NFC Communications-based Mutual Authentication Scheme for the Internet of Things

Yanna Ma

(Corresponding author: Yanna Ma)

Zhejiang University of Water Resources and Electric Power, Zhejiang 310000, China
(Email: helenmayanna@163.com.)

(Received May 10, 2016; revised and accepted Sept. 3 & Sept. 25, 2016)

Abstract

The integration of Near Field Communication (NFC) into consumer electronics devices has opened up opportunities for the internet of things applications such as electronic payment, electronic ticketing and sharing contacts, etc.. Meanwhile, various security risks should not be ignored. Therefore, all kinds of different protocols have been released with the purposing of securing NFC communications. Lately, a pseudonym-based NFC protocol for the consumer Internet of things was presented. They claimed that their scheme could withstand man-in-the middle attack headed from their scheme could provide mutual authentication. This study presents a security analysis on their scheme and finds that their scheme is not really secure against man-in-the-middle attack. Subsequently, this paper proposes an enhancement for purpose of thwarting this security attack. The security and performance analyses show that the enhancement is secure and efficient while keeping privacy preserving.

Keywords: Authentication; Key Establishment; Smart Cards; Wireless Communications

1 Introduction

Several wireless communications techniques and protocols are available in the market, such as Bluetooth, ZigBee, RFID, Wi-Fi and Infrared, which have different working frequencies and ranges. A more recent technology for short-range wireless (up to 10 cm) is the Near Field Communication (NFC) [16] that enables an easy, fast and secure communication between two devices in proximity. Its communication occurs with 13.56 MHz operating frequency while providing a high-level safety than other well-known wireless technologies, e.g. Bluetooth [3, 6]. The primary characteristic of NFC, leading to its widespread use and popularity is the advent of touch-less transactions, which leads to no cards, no coins and no laborious connections and network setup [2]. NFC thus enables the long awaited Internet-of-Things (IoT) [13], changing the interactions with the world in subtle but pervasive ways while providing digitally immersive experience. Although the communication range of NFC is limited to a few centimeters, NFC alone does not ensure secure communications, especially authentication between the sender and the recipient. One of the most important properties for data communication is mutual authentication which is defined as the ability that both communicating parties can authenticate with each other, thus preventing man-in-the-middle attack and replay attack [11, 14, 17]. In order to be secure NFC, the NFC security standards have been proposed in order to define data exchange format, tag types, and security protocols, e.g., a key agreement protocol [8, 9, 10]. In the process of key agreement, Certificate Authority (CA) as the Trusted Third Party (TTP) is in charge of generating the public key of the correspondents.

Recently, Eun et al. [5] proposed an authentication scheme for NFC communications to prevent replay and man-in-the-middle attack by providing mutual authentication based on a trusted service manager. The scheme was based on asymmetric cryptography and hash functions. By using an asymmetric cryptographic system, it was possible to address several security threats such as an evil twin attack, hotspot or captive portal eavesdropping, and even man-in-the-middle attacks [15]. However, He et al. [7] found that the scheme of Eun et al. could not resist impersonation attack. As a counter measure to these sufferings, He et al. presented a modified authentication NFC protocol to amend aforementioned security weaknesses. Unfortunately, this study showed that He et al.'s modification was not secure against the man-in-the-middle attack. As a result, a secure NFC mutual authentication scheme with privacy preservation for the Internet of things was designed in this paper.

The remainder of the paper is arranged as follows. In Section 2, a brief review of He et al.'s security protocol. In Section 3, man-in-the-middle attack is developed to analyze Eun et al.'s protocol. In Section 4, the proposed NFC communication-based protocol. Security and performance analyses results are given in Sections 5 and 6, respectively. Section 7 concludes this paper.

2 Review of He et al.'s Scheme

This part concisely review the NFC mutual authentication scheme by He et al. in 2014. For ease of presentation, Table I shows some intuitive abbreviations and notations.

Table 1: Notations

ID_X	the identity of the user X
TSM	a trusted service manager
G	the base point of the elliptic curve
KDF	a key derivation function
d_X	the private key of the user X
Q_X	the public key of the user X, where $Q_X = d_X G$
SK	exclusive-or operation
$E_K(m)$	symmetric encryption of using the key K
$h(\cdot), f(\cdot)$	hash functions
$Sig_K(m)$	signature of m using the key K

Once receiving the user A's request, the TSM generates n pseudonyms and delivers them to A via a private channel. The TSM also stores the user A's identity and pseudonyms into its database. Next, the TSM computes $PN_A^i = \{Q_A^i, E_{d_{TSM}}(ID_A, Q_A^i), ID_{TSM}, S_{TSM}^i\}$ and $S_{TSM}^i = Sig_{d_{TSM}}(Q_A^i, E_{d_{TSM}}(ID_A, Q_A^i), ID_{TSM})$, where $Q_A^i = q_A^i G$ is the public key of A, $d_A^i = q_A^i + h(ID_{TSM}, PN_A^i)d_{TSM}$ is A's private key, and S_{TSM}^i is the TSM's signature on the ith message.

The users A and B execute the establishment of the session key in the following manner:

Step 1: A computes $Q_A^{'} = r_A G$ and sends the message $\{PN_A^i, Q_A^{'}, N_A\}$ to B, where r_A and N_A are the random numbers generated by A, PN_A^i is a pseudonym selected by A.

Step 2: B computes $Q_B^{'} = r_B G$ and sends back the message $\{PN_B^j, Q_B^{'}, N_B\}$ to A, where r_B and N_B are the random numbers generated by B and PN_B^j is a pseudonym selected by B.

Step 3: After receiving the message, A computes $Z_A^1 = r_A Q_B^{'}$, $Z_A^2 = d_A^i(Q_B^j + h(ID_{TSM}, PN_B^j)Q_{TSM})$, $SK = KDF(N_A, N_B, ID_A, ID_B, Z_A^1, Z_A^2)$ and $MacTag_A = f(SK, ID_A, ID_B, Q_A^{'}, Q_A^2)$. Subsequently, A sends the message $\{MacTag_A\}$ to B.

Step 4: When receiving the message, B computes $Z_B^1 = r_B Q_A^{'}$, $Z_B^2 = d_B^j(Q_A^i + h(ID_{TSM}, PN_A^i)Q_{TSM})$, $SK = KDF(N_A, N_B, ID_A, ID_B, Z_B^1, Z_B^2)$ and verifies $f(SK, ID_A, ID_B, Q_A^{'}, Q_B^{'}) \stackrel{?}{=} MacTag_A$. If it holds, B computes $MacTag_B = f(SK, ID_A, ID_B, Q_A^{'}, Q_B^{'})$ and sets SK as the session key. Finally, B transmits the message $\{MacTag_B\}$ to A.

Step 5: Once receiving the message, A computes:

$$\begin{aligned} Z_A^1 &= r_A Q_B^{'} = r_A r_B G \\ &= r_B r_A G = r_B Q_A^{'}, \\ Z_A^2 &= d_A^i(Q_B^j + h(ID_{TSM}, PN_B^j)Q_{TSM}) \\ &= (q_A^i + h(ID_{TSM}, PN_A^i)d_{TSM}) \\ &\quad (q_B^j + h(ID_{TSM}, PN_B^j)d_{TSM})G \\ &= (q_B^j + h(ID_{TSM}, PN_B^j)d_{TSM}) \\ &\quad (q_A^i + h(ID_{TSM}, PN_A^i)d_{TSM})G \\ &= (q_B^j + h(ID_{TSM}, PN_B^j)d_{TSM}) \\ &\quad (q_A^i G + h(ID_{TSM}, PN_A^i)d_{TSM}G) \\ &= d_B^j(Q_B^j + h(ID_{TSM}, PN_B^j)Q_{TSM}). \end{aligned}$$

A computes SK and $f(SK, ID_A, ID_B, Q_A^{'}, Q_B^{'})$, then, A checks the correctness of the value $MacTag_B$. If it does not hold, A stops the session; Otherwise, A agrees on the session key SK with B.

3 Weaknesses of He et al.'s Scheme

He et al. declared that their improvements could resist the man-in-the-middle-attack due to their proposed scheme could provide the mutual authentication between A and B. Actually, a notable question is that A and B are unable to confirm the real identity of the other entity because of the absence of TSM during the execution of their scheme, thus giving a perfect opportunity for an adversary $\mathbb{A}$ to launch the man-in-the-middle attack.

The man-in-the-middle attack is a form of active eavesdropping in which $\mathbb{A}$ makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, while in fact the entire conversation is controlled by $\mathbb{A}$.

Let's describe the details of the attack as follows.

Step 1: When the message $M_1 = \{Q_A^{'}, PN_A^j, N_A\}$ is sent from A to B, $\mathbb{A}$ intercepts the message and computes $Q_A^* = r_{\mathbb{A}}^1 G$, and sends the forged message $M_1 = \{Q_A^*, PN_A^j, N_{\mathbb{A}}^1\}$ to B, where $r_{\mathbb{A}}^1$ and $N_{\mathbb{A}}^1$ are the random numbers of $\mathbb{A}$.

Step 2: When receiving the message, B computes $Q_B^{'} = r_B G$ and sends the message $M_2 = \{Q_B', PN_B^j, N_B\}$ to A.

Step 3: $\mathbb{A}$ intercepts the message M_2 and computes $Q_B^* = r_{\mathbb{A}}^2 G$ and sends the forged message $M_2 = \{Q_B^*, PN_B^j, N_{\mathbb{A}}^2\}$ to A, where $r_{\mathbb{A}}^2$ and $N_{\mathbb{A}}^2$ are the random numbers of $\mathbb{A}$.

Step 4: After receiving the message, A computes $Z_A^2 = d_A^1(Q_B^* + h(ID_{TSM}, PN_B^j)Q_{TSM})$, $Z_A^1 = r_A Q_B^*$, and the session key $SK = KDF(N_A, N_{\mathbb{A}}^2, ID_A, ID_B, Z_A^1, Z_A^2)$ and $MacTag_A =$

$f(SK, ID_A, ID_B, Q'_A, Q^*_B)$. Next, A sends the message $M_3 = \{MacTag_A\}$ to B.

Step 5: $\mathbb{A}$ eavesdrops this message and computes $Z^2_A = d^1_{\mathbb{A}}(Q'_B + h(ID_{TSM}, PN^j_B)Q_{TSM})$, $Z^1_A = r^1_{\mathbb{A}}Q'_B$, and the session key $SK = KDF(N_B, N^1_{\mathbb{A}}, ID_A, ID_B, Z^1_A, Z^2_A)$ and $MacTag_A = f(SK, ID_A, ID_B, Q^*_A, Q'_B)$. After that, $\mathbb{A}$ sends the forged message $M_3 = \{MacTag_A\}$ to B.

Step 6: When receiving the message M_3, B computes $Z^1_B = r_B Q^*_A$, $Z^2_B = d^1_B(Q^*_A + h(ID_{TSM}, PN^j_B)Q_{TSM})$ and $SK = KDF(N_B, N^1_{\mathbb{A}}, ID_A, ID_B, Z^1_B, Z^2_B)$. B verifies whether $f(SK, ID_A, ID_B, Q^*_A, Q'_B) \stackrel{?}{=} MacTag_A$ and it is obvious that the equation is true, because:

$$\begin{aligned}
Z^1_B &= r_B Q^*_A = r_B r^1_{\mathbb{A}} G \\
&= r^1_{\mathbb{A}} Q'_B = Z^1_A, \\
Z^2_B &= d^1_B(Q^*_A + h(ID_{TSM}, PN^j_B)Q_{TSM}) \\
&= (q^j_B + h(ID_{TSM}, PN^j_B)d_{TSM}) \\
&\quad (q^i_{\mathbb{A}}G + h(ID_{TSM}, PN^j_B)d_{TSM}G) \\
&= (q^i_{\mathbb{A}} + h(ID_{TSM}, PN^j_B)d_{TSM}) \\
&\quad (q^j_B + h(ID_{TSM}, PN^i_A)d_{TSM})G \\
&= d^1_{\mathbb{A}}(Q'_B + h(ID_{TSM}, PN^j_B)Q_{TSM}) \\
&= Z^2_A.
\end{aligned}$$

B computes $MacTag_B = f(SK, ID_A, ID_B, Q^*_A, Q'_B)$ and sends the message $M_4 = \{MacTag_B\}$ to A.

Step 7: $\mathbb{A}$ receives the message M_4 from B to A, $\mathbb{A}$ computes $Z^2_B = d^i_{\mathbb{A}}(Q^{'}_A + h(ID_{TSM}, PN^j_B)Q_{TSM})$, $Z^1_B = r^2_{\mathbb{A}}Q'_A$ and the session key $SK = KDF(N_A, N^2_{\mathbb{A}}, ID_A, ID_B, Z^1_B, Z^2_B)$ and $MacTag_B = f(SK, ID_A, ID_B, Q^{'}_A, Q^*_B)$. After that, $\mathbb{A}$ sends the forged message $M_4 = \{MacTag_B\}$ to A.

Step 8: When receiving the message, A checks the validness of $MacTag_B$ and it is sure that the equation will be equal to $f(SK, ID_A, ID_B, Q^{'}_A, Q^*_B)$. Therefore, A agrees on the session key SK as the common key aiming at encrypting the communication messages.

In this way, $\mathbb{A}$ is successfully authenticated by A and B, respectively. That is, $\mathbb{A}$ shares a session key $SK = KDF(N_A, N^2_{\mathbb{A}}, ID_A, ID_B, Z^1_B, Z^2_B)$ with A, at the same time, he shares a session key $SK = KDF(N_B, N^1_{\mathbb{A}}, ID_A, ID_B, Z^1_A, Z^2_A)$ with B. However, both of A and B do not know that they are communicating with an attacker at all. They believe they successfully have finished the handshake agreement with each other.

4 The Proposed Scheme

This section will present the proposed scheme as Figure 1.

After receiving the user A's request for pseudonyms, the TSM generates n pseudonyms and sends them to A via a secret channel. The TSM also stores the user A's identity and pseudonyms into its database. There are four parties in a pseudonym PN^i_A : the A's public key, A's private key, the TSM's identity and the TSM's signature.

$$\begin{aligned}
PN^i_A &= \{Q_A i, Enc(\{ID_A, Q_A i\}, d_{TSM}), ID_{TSM}, S^i_{TSM}\}, \\
S^i_{TSM} &= Sig(d_{TSM}, Q^i_A, Enc(Q^i_A, d_{TSM}), ID_{TSM}), \\
d^i_A &= d_{TSM} + h(ID_A, r_{S-A})h(ID_A, PN^i_A).
\end{aligned}$$

As the same method, the user B could get its pseudonyms and corresponding private key $d^j_B = d_{TSM} + h(ID_B, r_{S-B})h(ID_B, PN^j_B)$ and public key $d^j_B G$.

4.1 Establishment of the Session Key

When A and B attempts to establish the handshake, they perform as follows:

Step 1: A computes $Q^{'}_A = r_A G$, $Q^{''}_A = r_A d^j_B G$, where r_A is a nonce generated by A. Then, A sends $\{Q^{'}_A, Q^{''}_A\}$ to B.

Step 2: When receiving the message, B computes $(d^j_B)^{-1}Q^{''}_A = Q^{'}_A$, $Q^{'}_B = r_B G$, and $Q^{''}_B = r_B d^i_A G$, where $d^i_A G$ is the public key of A. Finally, B returns $\{Q^{'}_B, Q^{''}_B\}$ to A.

Step 3: Once receiving the message, A computes $(d^i_A)^{-1}Q^{''}_B = Q^{'}_B$, $Z^{'}_A = r_A Q^{'}_B$, $Z^{''}_A = d^i_A(Q_{TSM} + h(ID_B, PN^j_B)Q^i_A)$, $SK = KDF(ID_A, ID_B, Z^{'}_A, Z^{''}_A)$ and $MacTag_A = f(ID_A, ID_B, SK, Q^{'}_B)$. At last, A sends back the message $\{MacTag_A\}$ to B.

Step 4: When receiving the messages, B computes $Z^{'}_B = r_B Q^{'}_A$, $Z^{''}_B = d^j_B(Q_{TSM} + h(ID_A, PN^i_A)Q^j_B)$, $SK = KDF(ID_A, ID_B, Z^{'}_B, Z^{''}_B)$ and verifies whether $f(ID_A, ID_B, SK, Q^{'}_B) \stackrel{?}{=} MacTag_A$. If it is equal, B sets SK as the session key and computes $MacTag_B = f(ID_A, ID_B, SK, Q^{'}_A)$. After that, B delivers back the message $\{MacTag_B\}$ to A.

Step 5: When receiving the message, A checks whether $f(ID_A, ID_B, SK, Q^{'}_A) \stackrel{?}{=} MacTag_B$. If it holds, A successfully negotiates the session key SK with B.

5 Security Analysis

This section analyze the security of the proposed scheme, which includes achieving users' anonymity, mutual authentication, perfect forward session key security, and withstanding relay attack, impersonation attack. The details describe below.

5.1 Users' Anonymity

In the proposed scheme, the users' identities ID_A and ID_B are respectively implied in $MacTag_{A(B)} =$

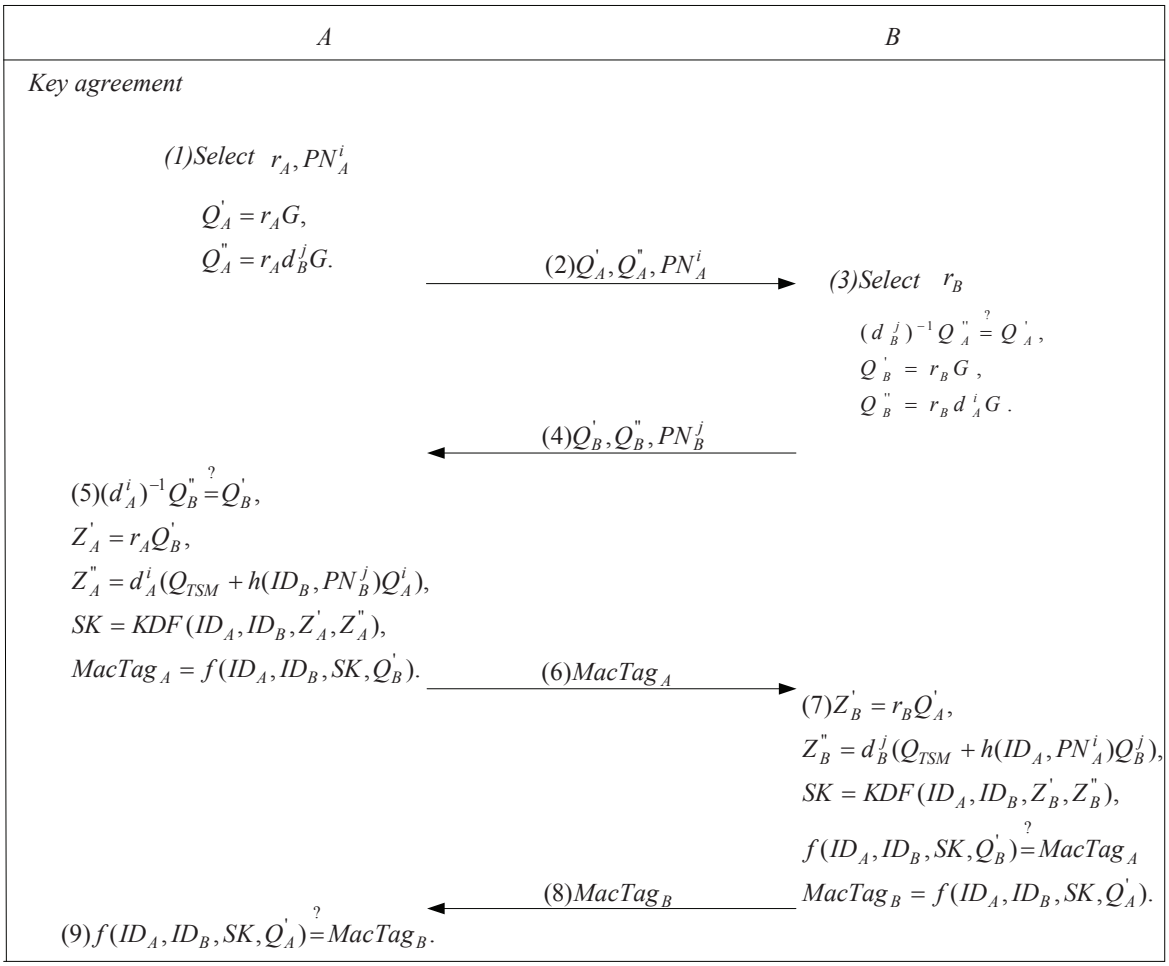

Figure 1: Mutual authentication and key agreement of our scheme

$f(ID_A, ID_B, SK, Q_{B(A)}^{'})$, where SK is the session key, $Q_{B(A)}^{'} = r_{B(A)} d_{A(B)}^{i(j)} G$, $r_{B(A)}$ and $d_{A(B)}^{i(j)}$ are the random numbers and the private keys. Therefore, ID_A is not able to be derived from $Z_A^{''}$ without knowing the users' private key, owing to the one-way property of the hash function. Therefore, the proposed scheme preserves identity privacy.

5.2 Mutual Authentication

In the proposed scheme, A authenticates A by checking $Q_A^{'} = (d_B^j)^{-1} Q_A^{''}$ and $MacTag_A = f(ID_A, ID_B, SK, Q_B^{'})$, where $SK = KDF(ID_A, ID_B, r_B Q_A^{'}, d_B^j d_A^i G)$. Additionally, A authenticates B by verifying whether $Q_B^{'} \stackrel{?}{=} (d_A^j)^{-1} Q_B^{''}$ and $MacTag_B \stackrel{?}{=} f(ID_A, ID_B, SK, Q_A^{'})$, where $SK = KDF(ID_A, ID_B, r_A Q_B^{'}, d_A^i d_B^j G)$.

5.3 Perfect Forward Security of the Session Key

Given $Q_A^{'}, Q_A^{''}$, $Q_B^{'}, Q_B^{''}$ and $d_A^i d_B^j$, the session key $SK = KDF(ID_A, ID_B, r_A Q_B^{'}, d_A^i d_B^j G)$ cannot be calculated without the knowledge of r_A and r_B, owing to the Diffie-Hellman problem. Additionally, given $MacTag_A = f(ID_A, ID_B, SK, Q_B^{'})$ and $MacTag_B = f(ID_A, ID_B, SK, Q_A^{'})$. SK cannot be determined due to the one-way property of the hash function and no knowledge of users' identities. Therefore, the session key cannot be derived from the revealed messages in the proposed scheme.

5.4 Known Session Key Security

In the proposed scheme, the session key is computed as $SK = KDF(ID_A, ID_B, r_A r_B G, d_A^i d_B^j G)$, which does not give any useful information for computing the next session keys because r_A and r_B are randomly generated in different runs and are independent of each other among scheme executions. Therefore, the proposed scheme has the property of known-key security.

5.5 Resistance to relay attack

Relay Attack is also popularly known as "man in the middle attack" in network security. An attacker acts as a middleman between two NFC devices to intercept the data

Table 2: Computational cost comparison

	Eun et al. [5]	He et al. [7]	The Proposal
A	$3T_{ecm} + 1T_{eca} + 2T_h + 2T_{mm} + 1T_{kdf}$ ≈ 0.6552	$4T_{ecm} + 1T_{eca} + 2T_h + 1T_{kdf}$ ≈ 0.2214	$4T_{ecm} + 1T_{mi} + 2T_h + 1T_{kdf}$ ≈ 0.2391
B	$3T_{ecm} + 1T_{eca} + 2T_h + 2T_{mm} + 1T_{kdf}$ ≈ 0.2583	$4T_{ecm} + 1T_{eca} + 3T_h + 1T_{kdf}$ ≈ 0.1845	$4T_{ecm} + 1T_{mi} + 2T_h + 1T_{kdf}$ ≈ 0.1107
Total	$6T_{ecm} + 2T_{eca} + 4T_h + 4T_{mm} + 2T_{kdf}$ ≈ 0.6921	$8T_{ecm} + 2T_{eca} + 5T_h + 2T_{kdf}$ ≈ 0.369	$8T_{ecm} + 2T_{mi} + 4T_h + 2T_{kdf}$ ≈ 0.3498

without the knowledge of the two NFC devices. The attacker either reads and records or manipulates the data before relaying it to the receiving device [18]. If an adversary intends to impersonate as a legal user to cheat A and B, he cannot accomplish his well as he wished. Because A and B each hold the data which is only verified by the other side, any forgery data will be detected by the receiver. Specifically, A sends $Z_A^{''} = d_A^i d_B^j G$ which is concealed in the session key and $Q_A^{''} = r_A d_B^j G$ to B, where $d_B^j G$ is a secret value of B. After verifying the correctness of the two values, B judges whether the sender is the real A. Similarly, A can also authenticate the validity of B by checking $Z_B^{''} = d_B^j d_A^i G$ and $Q_B^{''} = r_B d_A^i G$.

5.6 Resistance to Impersonation Attack

In the establishment of the session key, A transmits $Q_A^{''} = r_A d_B^j G$ to B, where d_B^j is the secret key of B, only B knows d_B^j. Others are impossible to know the value of $d_B^j G$ and cannot compute $Z_A^{''}$. Without the value of $Z_A^{''}$, an adversary cannot pass the authentication of B. Meanwhile, B also sends back the value $d_A^i G$ which is hidden in $Q_B^{''} = r_B d_A^i G$, where $d_A^i G$ is the secret information only known by of A and B, and only A knows d_A^i. That is, any unauthorized user cannot compute the correct $Z_B^{''}$ and hence cannot be verified by A without the value of $d_A^i G$. In this way, the proposed scheme can withstand the impersonation attack.

5.7 No Key Control

In the proposed scheme, both A and B jointly compute the session key $SK = KDF(ID_A, ID_B, r_A r_B G, d_A^i d_B^j G)$ and therefore, A fails to predetermine a session key since SK contains r_B and d_B^j, where r_B and d_B^j are the secret values of B and independent among scheme executions. In other word, A or B cannot determine a session key alone and hence, the proposed scheme provides the no key control property.

5.8 Verification Using Scyther Tool

Scyther is a tool for the automatic verification of security protocols. In this part, we use Scyther-w32-v1.1.3 [4] to analyze the proposed scheme. Figure 1 shows a summary of the claims in the proposed scheme. The verification result (Figuer 2) shows our scheme is correct.

6 Performance Comparisons

This section will evaluate the performance of the proposed scheme, and compare it with other related schemes [5, 7] for performance and functionality aspects. In order to facilitate the analysis of the performance, some notations was defined as below:

- T_{ecm}: the time consumption for an elliptic curve point multiplication operation;
- T_h: the time consumption for a hash function operation;
- T_{eca}: the time consumption for an elliptic curve point addition operation;
- T_{kdf}: the time consumption for a key derivation function operation;
- T_{mm}: the time consumption for a modular multiplication operation;
- T_{mi}: The time consumption for a modular inversion operation.

Generally, T_{mm} is far greater than T_{ecm}, T_{eca} and T_h. According to [1], under the environment of 2.2 GHz CPU and 2.0GB RAM, T_{ecm} and T_{eca} are 2.226 and 0.0288 ms, T_{mi}, T_{mm} and T_h are 5.565, 1.855 and 2.3 μs, respectively.

Table 2 demonstrates that the proposed scheme has less computational efficiency as compared with He et al. [7] but a slighter higher than Eun et al. [5] schemes, where the computational cost for executing the scheme once is only half of the time needed for other related scheme due to the proposed scheme needs more elliptic curve point multiplication computation than Eun et al.'s scheme, and employ modular inversion computation instead of elliptic curve point addition computation.

Table 3 shows the functionality analysis of the proposed scheme with Eun et al.'s [5] and He et al.'s [7] schemes. It is observed that the proposed scheme outperforms as compared to He et al.'s and Eun et al.'s schemes as the proposed scheme supports extra features listed in

```
hashfunction H;hashfunction KDF;

const Add: Function;const Mul: Function;

usertype String;const IDa,IDb: String;
protocol lu(A,B)
{      role A{  fresh Ra, G, PNa, PNb, Qtsm: Nonce;

               var Qa1, Qa2, Qb1, Qb2, Za1, Za2: Nonce;

               var SK, MacTaga, MacTagb: Nonce;

               match(Qa1,Mul(Ra, G));match(Qa2,Mul(Ra,pk(B)));

               send_!1(A,B,Qa1,Qa2,PNa);recv_!2(B,A,Qb1,Qb2,PNb);

               match(Za1,Mul(Ra,Qb1));match(Za2,{Add(Mul(H(IDb,PNb),Qa1),Qtsm)}sk(A));

               match(SK,KDF(IDa, IDb, Za1, Za2));

               match(MacTaga,H(IDa, IDb, SK, Qb1));send_!3(A,B,MacTaga);
               recv_!4(B,A,MacTagb);claim_A1(A,Secret,MacTaga);claim_A2(A,Secret,Qa1);

               claim_A3(A,Secret,Qa2);claim_A4(A,Secret,Qb1);

               claim_A5(A,Secret,Qb1);claim_A6(A,Alive);

               claim_A7(A,Weakagree);claim_A8(A,Niagree);

               claim_A9(A,Nisynch);}
role B{ fresh Rb, G, PNa, PNb, Qtsm: Nonce;

               var Qa1, Qa2, Qb1, Qb2, Zb1, Zb2: Nonce;

               var SK, MacTaga, MacTagb: Nonce;

               recv_!1(A,B,Qa1,Qa2,PNa);match(Qb1,Mul(Rb, G));

               match(Qb2,Mul(Rb,pk(A)));send_!2(B,A,Qb1,Qb2,PNb);

               recv_!3(A,B,MacTaga);match(Zb1,Mul(Rb,Qa1));

               match(Zb2,{Add(Mul(H(IDa,PNb),Qb1),Qtsm)}sk(B));

               match(SK,KDF(IDa, IDb, Zb1, Zb2));

               match(MacTagb,H(IDa, IDb, SK, Qa1));

               send_!4(B,A,MacTagb);claim_B1(B,Secret,MacTagb);

               claim_B2(B,Secret,Qa1);claim_B3(B,Secret,Qa2);

               claim_B4(B,Secret,Qb1);claim_B5(B,Secret,Qb1);

               claim_B6(B,Alive);claim_B7(B,Weakagree);

               claim_B8(B,Niagree);claim_B9(B,Nisynch);}}
```

Figure 2: The scheme description

Table 3: Comparison of functionality features

	Eun et al. [5]	He et al. [7]	The Proposal
Mutual authentication	Yes	Yes	Yes
User anonymity	Yes	Yes	Yes
No key control	Yes	Yes	Yes
Known session key security	Yes	Yes	Yes
Impersonation attack	No	Yes	Yes
Perfect forward security of the session key	-	-	Yes
Relay attack	-	No	Yes

Figure 3: Test result.

this table and is also more secure than He et al.'s scheme. As a result, the proposed scheme is much suitable for practical applications as compared to the recently proposed He et al.'s scheme.

7 Conclusion

This paper have investigated the NFC communications-based mutual authentication scheme presented by He et al.. By cryptanalyzing studies, a fatal security weakness in He et al.'s scheme have been found. In order to remedy this flaw, an enhancement based on He et al.'s scheme have been presented. Based on the security analysis, the proposed scheme has been demonstrated to be satisfied both the verifiability and privacy of attributes. According to the performance comparison results, the efficiency and feasibility of the proposed scheme under different privacy requirements for the IOT have been shown.

References

[1] H. Arshad, and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for ses-

sion initiation protocol using ECC," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 181–197, 2016.

[2] G. Broll, S. Siorpaes, E. Rukzio, M. Paolucci, J. Hamard, M. Wagner and A. Schmidt, "Supporting mobile service usage through physical mobile interaction," in *5th Annual IEEE International Conference on Pervasive Computing and Communications*, White Plains, NY, USA. 2007.

[3] V. Coskun, K. Ok, and B. Ozdenizci, *Near Field Communication (NFC): From Theory to Practice*, London, Wiley, February, 2012.

[4] C. Cremers, *The Scyther Tool*, Apr. 4, 2014. (`https://www.cs.ox.ac.uk/people/cas.cremers/scyther/`)

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

[6] E. Hasoo, L. Hoonjung, S. Junggab, K. Sangjin, and O. Heekuck, "Conditional privacy preserving security protocol for NFC applications," in *IEEE International Conference on Consumer Electronics*, pp.380-381, 2012.

[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] ISO/IEC, *Information Technology-Security Methods-Cryptographic Methods Based on Elliptic Curves - Part 1: General*, ISO/IEC 15946-1, Apr. 2008.

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

[11] P. Kumar, A. Gurtov, J. Iinatti, and S. G. Lee, "Delegation-based robust authentication model for wireless roaming using portable communication devices," *IEEE Transaction on Consumer Electronics*, vol. 60, no.4, pp. 668-674, 2014.

[12] Y. Lu, X. Wu, X. Yang, "A secure anonymous authentication scheme for wireless communications using smart cards," *International Journal of Network Security*, vol. 17, no. 3, pp. 237–245, 2015.

[13] W. Lumpkins, and M. Joyce, "Near-field communication: It pays: Mobile payment systems explained and explored," *IEEE Consumer Electronics Magazine*, vol. 4, no. 2, pp. 49-53, 2015.

[14] G. Madlmayr, J. Langer, and C. Kantner, "NFC devices: Security and privacy," in *3th Annual IEEE International Conference on Availability, Reliability and Security*, pp. 642–647, 2008.

[15] A. Matos, D. Romao, and P. Trezentos, "Secure hotspot authentication through a near field communication side-channel," in *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 807–814, Oct. 2012.

[16] K. F. Warnick, R. B. Gottula, S. Shrestha, and J. Smith, "Optimizing power transfer efficiency and bandwidth for near field communication systems," *IEEE Transaction on Antennas and Propagation*, vol. 61, no. 2, pp. 927–933, 2013.

[17] T. Sunil, B. Rabin, and M. Sangman, "NFC and its application to mobile payment: Overview and comparison," in *2012 8th IEEE International Conference on Information Science and Digital Content Technology*, pp. 203–206, 2012.

[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 2015 IEEE International Conference on Information Networking*, pp. 133–138, 2015.

Biography

Yan-Na Ma received the B.S. degree in electrical engineering from Dalian University (DUT) of Technology, Dalian, China, in 2009 and the M.S. and Ph.D. degree in communications and integrated system from Tokyo Institute of Technology, Tokyo, Japan, in 2011 and 2014, respectively. Currently, she is a faculty member with School of Information Engineering and Art Design, Zhejiang University of Water Resources and Electric Power, China. Her research interests are speech signal processing, noise reduction, near field communication and their applications to communication devices.