Article

Efficient and Secure NFC Authentication for Mobile Payment Ensuring Fair Exchange Protocol

Chalee Thammarat

Faculty of Information Science and Technology, Mahanakorn University of Technology, Bangkok 10530, Thailand; tchale32@mut.ac.th

Received: 22 July 2020; Accepted: 25 September 2020; Published: 9 October 2020

Abstract: The standard protocol of near field communication (NFC) has concentrated primarily on the speed of communication while ignoring security properties. Message between an NFC-enabled smartphone and a point of sale are exchanged over the air (OTA), which is a message considered an authentication request for payment, billing, ticketing, loyalty services, identification or access control. An attacker who has an antenna can intercept or manipulate the exchanged messages to take advantage of these. In order to solve this problem, many researchers have suggested authentication methods for NFC communications. However, these remain inadequate transaction security and fairness. In this paper, we will propose a technique that ensures mutual authentication, security properties, and strong fairness. Mutual authentication is a security property that prevents replay attacks and man-in-the-middle attacks. Both fair exchange and transaction security are also significant issues in electronic transactions with regards to creating trust among the parties participating in the transaction. The suggested protocol deploys a secure offline session key generation technique to increase transaction security and, importantly, make our protocol lightweight while maintaining the fairness property. Our analysis suggests that our protocol is more effective than others regarding transaction security, fairness, and lightweight protocol. The proposed protocol checks robustness and soundness using Burrows, Abadi and Needham (BAN) logic, the Scyther tool, and automated validation of internet security protocols and applications (AVISPA) that provide formal proofs for security protocols. Furthermore, our protocol can resolve disputes in case one party misbehaves.

Keywords: NFC; near field communication; mutual authentication; fairness; fair exchange protocol

1. Introduction

Until recently, many smartphones have built-in near field communication (NFC) to allow short-range communication and small data transfers. Due to the severely short range of communications (short range is around 10 cm), NFC implementations concentrate only on the speed of communication, ignoring security properties, in particular, the authentication of the sender and the recipient [1–4]. Many techniques have been proposed to offer authentication of transactions through NFC [5–9].

El Madhoun et al. [5] proposed a secure authentication protocol for contactless-NFC payment based on a Cloud infrastructure to solve security vulnerabilities detected in the Europay Mastercard Visa (EMV) protocols. Asymmetric encryption is used to provide mutual authentication (with non-repudiation) between a near field communication (NFC) smartphone and an NFC point of sale terminal. Symmetric encryption is utilized the confidentiality of bank data in the authentication steps. This proposed protocol uses the Scyther tool to verify security protocols.

Badra et al. [6] suggested identifying threats and vulnerabilities of the air interface between NFC-enabled devices and the point of sale system, and a solution to secure NFC-based payment transactions with mobile phones. The proposed method gives lightweight (using symmetric cryptography), simple, scalable, cost-effective, and incurs minimal computational processing overheads.

Sethia et al. [7] recommended framework for the NFC secure element (SE)-based mutual authentication and attestation for Internet of things (IoT) access. A cloud-based trusted certified authority (TCA) is used to manage all cryptographic credentials and stores. The security protocol is verified by automated validation of internet security protocols and applications (AVISPA) tool. Moreover, this protocol is robust and lightweight as compared to the others protocols.

Sethia et al. [8] offered mutual authentication for securing mobile health card. The proposed protocol can ensure prevention against the kind of attacks such as relay attacks, masquerading and so on. This protocol applies asymmetric encryption and symmetric encryption to secure transactions.

Al-Haj et al. [9] introduced improve security layer in Europay, Mastercard and Visa (EMV) protocol. The management, authentication server (MAS) in this protocol provides authentication of the payment transactions, and to achieve mutual authentication between parties, both the NFC-enabled mobile device and the point of sale terminal. The protocol ensures security properties like mutual authentication, non-repudiation, data integrity, confidentiality, and data privacy. Moreover, the proposed protocol offers advantages including scalability, simplicity, cost-effectiveness, and low computational processing.

Nonetheless, those NFC authentication protocols that have been proposed do not possess sufficient fairness and security properties. Our present method attempts to ensure mutual authentication, fairness and security properties such as confidentiality, integrity, mutual authentication, non-repudiation, brute force attacks, replay attacks, man-in-the-middle (MITM) attacks, eavesdropping, and data manipulation. In addition, the proposed protocol deploys a secure offline session key generation technique to enhance the protocol's security.

2. Backgrounds

NFC [1,2] is a short-range wireless communication technology that is operating at 13.56 MHz. It can quickly send data rate links of 106, 212 and 424 Kbps inside a range of 10 cm. NFC equipment can execute a speedy pairing with various other devices, consumes little power and transmits small amounts of data. NFC is comprised of three operating modes. In the card emulation mode, NFC works as a radio frequency identification (RFID) tag installed in portable hardware. It can be operated as a contactless card according to ISO14443 and FeliCa. In the reader/writer mode, NFC can run as an NFC reader and writer. In the NFC-enabled peer-to-peer (P2P) mode, the system can communicate directly with each other, sharing data.

NFC is designed primarily on the speed of communication. Consequently, NFC lacks the encryption of data between two devices at the hardware level. Many researchers have discussed the weaknesses of NFC, which one of the essential security services is authentication, which protects against replay attack and man-in-the-middle attack (MITM).

Many security threats include [3,4] an eavesdropping type of attack, where communication between two NFC devices can be intercepted and read data by using the large antenna as NFC does not possess any countermeasures against eavesdropping. Data manipulation: an attacker intercepts and alters data throughout the communication, which can be separated into three different types: data alteration, data insertion, and data destruction. Relay attack: a relay attack is widely understood as man in the middle attack (MITM), which implementations focus on ISO 14443 and ISO18092 systems on network security. Data transmitted between two NFC devices can be intercepted by an attacker who both reads and records or manipulates the data before sending it to the receiving device.

To overcome the limitations of existing protocols [5–9], we will propose a new protocol that ensures mutual authentication, security properties, and fairness. In our proposed protocol, using a secure offline session key generation technique is to be employed. This can enhance transaction security and make the protocol lightweight while maintaining strong fairness. Our analysis demonstrates that our protocol is more efficient than others' regarding security, fairness and lightweight protocol.

3. The Proposed Protocol

In this study, we suggest an authentication protocol for NFC communications in order to untangle the issues and to overcome restrictions such as authentication and the fairness of current protocols [5–9] by applying [10–12] model to complete the fairness protocol. In [12], the suggested mobile payment protocol based on an NFC communication. The protocol possesses comprehensive properties of both fair exchange and transaction security, such as confidentiality of transactions, integrity of transactions, authentication of transactions, Non-repudiation of transactions, and resistance to attacks like double-spending, man-in-the-middle, replay attacks. This protocol uses cryptography algorithms such as symmetric, asymmetric and hash function, and the technique of offline session key generation is used to enhance security of the protocol. Fairness property of this protocol can resolve any dispute in case one party misbehaves. Burrows, Abadi and Needham (BAN logic) and the Scyther tool are utilized to verify security of the protocol.

Our protocol is based on symmetric key encryption, using a secure session key distribution to improve the protocol [13]. Many session key generation techniques have been suggested [14,15]. One technique was suggested by [13], which is not only secured key compromise attacks but can also operate purely offline. The engaged parties perform their tasks that do not need to send session keys throughout the network. The technique was chosen to secure session key generation technique our protocol. There are four phases of the proposed protocol comprised of initiation phase, registration phase, authentication phase, and dispute resolution phase.

3.1. Notations and Assumptions

Table 1, shown below, demonstrates the details of notations that are used in the proposed protocol.

3.2. Initiation Phase

In this phase, the goal is to exchange key distribution parameters between parties—P, S, TP and V. The details of the initiation phase are shown as follows: P and S exchange $\{K_{P-S}, DK_{P-S}, m_{P-S}\}$ through the secure channel such as transport layer security (TLS). Both P and S can create a set of session keys, SK_{P-Sj} , where $j = 1, \dots, m_{P-S}$, by using the session key creation technique described in [13].

P and trusted third party (TP) exchange $\{K_{P-TP}, DK_{P-TP}, m_{P-TP}\}$ through a secure channel such as TLS. Both P and TP can create a set of session keys SK_{P-TPj} , where $j = 1, \dots, m_{P-TP}$, by using the session key creation technique described in [13].

P and V exchange $\{K_{P-V}, DK_{P-V}, m_{P-V}\}$ through a secure channel such as TLS. Both P and V can create a set of session keys SK_{P-Vj} , where $j = 1, \dots, m_{P-V}$, by using the session key creation technique described in [13].

S and TP exchange $\{K_{S-TP}, DK_{S-TP}, m_{S-TP}\}$ through a secure channel such as TLS. Both S and TP can create a set of session keys, SK_{S-TPj} , where $j = 1, \dots, m_{S-TP}$, by using the session key creation technique described in [13].

S and V exchange $\{K_{S-V}, DK_{S-V}, m_{S-V}\}$ through a secure channel such as TLS. Both S and V can create a set of session keys, SK_{S-Vj} , where $j = 1, \dots, m_{S-V}$, by using the session key creation technique described in [13].

TP and V exchange $\{K_{TP-V}, DK_{TP-V}, m_{TP-V}\}$ through a secure channel such as TLS. Both TP and V can create a set of session keys, SK_{TP-Vj} , where $j = 1, \dots, m_{TP-V}$, by using the session key creation technique described in [13].

Table 1. Notations.

Notation	Description
N	A user utilizing an NFC-enabled smartphone in card emulation mode
P	A sales station providing NFC equipment
S	An authentication server
TP	A trusted third party. TP by itself is not involved in the transaction but helps to keep a record of all transactions that have taken place for each engaged party for future verification. Note that TP is a semi-TP. Semi-TP may misbehave on its own. However, it will not collide with any of the participating parties.
V	The external party is a party that is not relevant to the particular transaction
$\{DK_{A-B}, K_{A-B}, m_{A-B}\}$	The key distribution parameters that are shared between the parties, where K_{A-B} is a long-term key, DK_{A-B} is a distributed key and m_{A-B} is a random number. m_{A-B} is used to specify the number of keys that will be generated.
ID_A	An identity of user A.
SK_{A-B}	A session key shared between party A and party B.
$\{msg\}_{SK}$	A message msg symmetrically encrypted with key SK.
$h(msg)$	Hash value of message msg.
$h(msg, SK_{A-B})$	A message authentication code (MAC) value of message msg with key SK_{A-B}
Request	A message is considered a request message like payment, billing, ticketing, loyalty services, identification or access control, and so on.
Response	A message is considered a response message like payment, billing, ticketing, loyalty services, identification or access control, and so on.
T_1	The timestamp is given when authentication is requested.
T_2	The timestamp is given when a feedback message is provided.
msg_1, msg_2	The concatenation of message msg_1 and message msg_2
h_{N-TP}	$h(ID_N, T_1, request)$ denotes hash value of $ID_N, T_1, request$
h_{P-TP}	$h(ID_N, ID_P, T_1, request)$ denotes hash value of $ID_N, ID_P, T_1, request$
h_{S-TP}	$h(ID_N, ID_P, T_1, T_2, response)$ denotes hash value of $ID_N, ID_P, T_1, T_2, response$

3.3. Registration Phase

In this phase, each smartphone user needs to install an application dependent on the proposed protocol. At the point when the application has been completely installed, the user needs to perform registration through a secure channel such as TLS. The object of registration is to exchange $\{K_{N-S}, DK_{N-S}, m_{N-S}\}$, $\{K_{N-P}, DK_{N-P}, m_{N-P}\}$, $\{K_{N-TP}, DK_{N-TP}, m_{N-TP}\}$, and $\{K_{N-V}, DK_{N-V}, m_{N-V}\}$ between the N and S, between N and P, between N and TP, and between N and V through the secure channel such as TLS. The details of the registration phase are shown as follows:

Both N and S can create a set of session keys, SK_{N-Sj} , where $j = 1, \dots, m_{N-S}$, by using the session key creation technique described in [13].

Both N and P can create a set of session keys, SK_{N-Pj} , where $j = 1, \dots, m_{N-P}$, by using the session key creation technique described in [15]. Both N and TP can create a set of session keys, SK_{N-TPj} , where $j = 1, \dots, m_{N-TP}$, by using the session key creation technique described in [13].

Both N and V can create a set of session keys, SK_{N-Vj} , where $j = 1, \dots, m_{N-V}$, by using the session key creation technique described in [13].

3.4. Authentication Phase

In this phase, the proposed protocol provides authentication between N and P, between N and S through P, and between P and S. Note that P communicates with an NFC reader through a

secure channel. From Figure 1 displays the transaction flow of authentication protocol of all parties, including N, P, S and TP.

- M1:** $N \rightarrow P$: $ID_N, T_1, request, h(ID_N, T_1, Request, SK_{N-S_j}), h(ID_N, T_1, request, h(ID_N, T_1, request, SK_{N-S_j}), \{h_{N-TP}\}_{SK_{N-TP_j}}, SK_{N-P_j}), \{h_{N-TP}\}_{SK_{N-TP_j}}$
- M2:** $P \rightarrow S$: $ID_N, ID_P, T_1, request, h(ID_N, T_1, request, SK_{N-S_j}), h(ID_P, h(ID_N, T_1, request, SK_{N-S_j}), SK_{P-S_j}), \{h_{N-TP}\}_{SK_{N-TP_j}}, \{h_{P-TP}\}_{SK_{P-TP_j}}$
- M3:** $S \rightarrow TP$: $\{h_{N-TP}\}_{SK_{N-TP_j}}, \{h_{P-TP}\}_{SK_{P-TP_j}}, \{h_{S-TP}\}_{SK_{S-TP_j}}$
- M4:** $TP \rightarrow S$: $\{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{N-TP_j+1}}, \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{P-TP_j+1}}, \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{S-TP_j+1}}$
- M5:** $S \rightarrow P$: $T_2, response, h(T_1, T_2, response, SK_{N-S_{j+1}}), h(h(T_1, T_2, response, SK_{N-S_{j+1}}), SK_{P-S_{j+1}}), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{N-TP_j+1}}, \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{P-TP_j+1}}$
- M6:** $P \rightarrow N$: $T_2, response, h(T_1, T_2, response, SK_{N-S_{j+1}}), h(h(T_1, T_2, response, SK_{N-S_{j+1}}), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{N-TP_j+1}}, SK_{N-P_{j+1}}), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{N-TP_j+1}}$

Figure 1. Transaction flow of authentication protocol.

N sends an authentication request message M1 to P which contains the following: $h(ID_N, T_1, Request, SK_{N-S_j})$: the hash value is considered as a message authentication code (MAC), which is an authentication token between N and S, which will be transmitted to S through P, and ensures the integrity of the message. This message P cannot generate since P does not know the session key SK_{N-S_j} . Hence, only N constructs this message. $h(ID_N, T_1, Request, h(ID_N, T_1, Request, SK_{N-S_j}), \{h_{N-TP}\}_{SK_{N-TP_j}}, SK_{N-P_j})$: the hash value is considered as a MAC, which is an authentication token between N and P, and ensures the integrity of the message. Moreover, this message P uses to verify the authenticity of N. N cannot deny that it did not originate this message as the possession of both SK_{N-S_j} and SK_{N-P_j} . $\{h_{N-TP}\}_{SK_{N-TP_j}}$: the message encrypted with the session key SK_{N-TP_j} shared between N and TP, which will be transmitted to TP through S. This message P cannot generate because P does not know the session key SK_{N-TP_j} . Therefore, N is original of this message. Note that T_1 is generated by N to prevent replay attack.

On receiving message M1 from N, P will verify the authentication request message $h(ID_N, T_1, request, h(ID_N, T_1, request, SK_{N-S_j}), \{h_{N-TP}\}_{SK_{N-TP_j}}, SK_{N-P_j})$ of N, if the message is invalid, P rejects N's request. If not, P forwards N's authentication request to S in the message M2. P sends message M2 to S. It contains the following: $h(ID_P, h(ID_N, T_1, request, SK_{N-S_j}), SK_{P-S_j})$: the hash value is considered as a MAC, which is an authentication token between P and S, and ensures the integrity of the message. Besides, this message S uses to verify the authenticity of P. $\{h_{P-TP}\}_{SK_{P-TP_j}}$: the message encrypted with the session key SK_{P-TP_j} shared between P and TP which will be transmitted to TP through S. This message S cannot generate because S does not know the session key SK_{P-TP_j} . Therefore, P is original of this message.

On receiving the message M2 from P, S will check the correctness of the authentication request message $h(ID_P, h(ID_N, T_1, request, SK_{N-S_j}), SK_{P-S_j})$ of P, if the message is invalid, S rejects P's request. If not, S will check the correctness of authentication request message $h(ID_N, T_1, request, SK_{N-S_j})$ of N.

If the message is successful, S sends response message back to N and P. Otherwise, S rejects P's request. Then, S sends the message M3 to TP.

On receiving message M3 from S, TP will process three things: TP decrypts the message $\{h_{N-TP}\}_{SK_{N-TPj}}$ using SK_{N-TPj} keeps the hash value, decrypts the message $\{h_{P-TP}\}_{SK_{P-Sj}}$ using SK_{P-TPj} , keeps the hash value, decrypts the message $\{h_{S-TP}\}_{SK_{S-TPj}}$ using SK_{S-TPj} keeps the hash value. Next, TP encrypts three hash values, encrypts the hash value of h_{N-TP} , h_{P-TP} , h_{S-TP} using $SK_{N-TPj+1}$. Encrypts the hash value of h_{N-TP} , h_{P-TP} , h_{S-TP} using $SK_{P-TPj+1}$. Encrypts the hash value of h_{N-TP} , h_{P-TP} , h_{S-TP} using $SK_{S-TPj+1}$. Then, TP sends messages M4 to S.

On receiving the message M4 from TP, S decrypts the message $\{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{S-TPj+1}}$ with $SK_{S-TPj+1}$ and keeps the hash value as proof if a dispute arises. Then, S sends messages M5 to P. The message M5 contains the following: $h(T_1, T_2, \text{response}, SK_{N-Sj+1})$: the hash value is considered as a message as MAC, which is an authentication token between N and S which will be transmitted to N through P, and ensures the integrity of the message. This message P will not generate since P does not know the session key SK_{N-Sj+1} . Hence, only S constructs this message. $h(h(T_1, T_2, \text{response}, SK_{N-Sj+1}), SK_{P-Sj+1})$: the hash value is considered as MAC, which is an authentication token between P and S, and ensures the integrity of the message. Moreover, the message P uses to verify the authenticity of S. S cannot deny that it did not originate this message as the possession of both SK_{N-Sj+1} and SK_{P-Sj+1} . $\{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{N-TPj+1}}$: this message will forward to N via P. $\{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{P-TPj+1}}$: this message will send to P.

On receiving the message M5 from S, P will verify the authentication response message $h(h(T_1, T_2, \text{response}, SK_{N-Sj+1}), SK_{P-Sj+1})$ of S, if the message is invalid, P rejects S's response. Unless, P decrypts the message $\{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{P-TPj+1}}$ and keeps the hash value as proof if a dispute arises. Then, P sends the message M6 to N.

On receiving the message M6 from P, N will verify the authentication result message $h(h(T_1, T_2, \text{response}, SK_{N-Sj+1}), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{N-TPj+1}}, SK_{N-Pj+1})$ of P, if the message is invalid, N rejects P's response. Unless, N will verify the authentication result message $h(T_1, T_2, \text{Yes/No}, SK_{N-Sj+1})$ of S, if the message is invalid, N rejects P's response. If not, N decrypts the message $\{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SK_{N-TPj+1}}$ with $SK_{N-TPj+1}$ and keeps the hash as proof if a dispute arises. Note that T_2 is generated by S to prevent a replay attack.

It can be seen that N with S via P can provide mutual authentication for all engaged parties. Each message in this protocol can be used to identify the sender and the recipient of the message. Thus, our protocol ensures mutual authentication for N, P, and S. This protocol contains only symmetric cryptographic operations, MAC and a hash function, which leads to lightweight operations. Therefore, it is appropriate for NFC communications. Additionally, using a secure offline session key generation technique will enhance the security of the protocol.

3.5. Dispute Resolution Phase

There are two sub-phases: N requests dispute, and P requests dispute. After the transaction is complete, if N or P is not satisfied with the transaction, N or P can request a dispute resolution to V, the dispute resolution protocol. Consider the protocols below:

3.5.1. N Requests Dispute

N sends the hash value $h(h_{N-TP}, h_{P-TP}, h_{S-TP})$ of the transaction to V. Upon receiving the hash value of N, V sends the requested hash value of the TP. After receiving the hash value from the TP, V compares the hash value of N with the hash value from the TP. If the hash values do not match, V rejects N's request; if not, V sends a notification of dispute resolution to P and S. From Figure 2 shows transaction flow of N request dispute protocol of all parties including N, P, S, V and TP. The details of this protocol are outlined below.

Figure 2. Transaction flow of N request dispute.

- M1:** $N \rightarrow V: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKN-V_j}$
M2: $V \rightarrow TP: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKV-TP_j}$
M3: $TP \rightarrow V: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKV-TP_j+1}$
M4: $V \rightarrow P: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKP-V_j}$
M5: $V \rightarrow S: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKS-V_j}$
M6: $V \rightarrow N: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKN-V_j+1}$

3.5.2. P Requests Dispute

P sends the hash value $h(h_{N-TP}, h_{P-TP}, h_{S-TP})$ of the transaction to V. Upon receiving the hash value of P, V sends the requested hash value of the TP. After receiving the hash value from the TP, V compares the hash value of N with the hash value from the TP. If the hash values do not match, V rejects P's request; if not, V sends a notification of dispute resolution to N and S. Figure 3 shows the transaction flow of P request dispute protocol of all parties including N, P, S, V and TP. The details of this protocol are outlined below.

Figure 3. Transaction flow of P request dispute.

- M1:** $P \rightarrow V: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKP-V_j}$
M2: $V \rightarrow TP: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKV-TP_j}$
M3: $TP \rightarrow V: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKV-TP_j+1}$
M4: $V \rightarrow N: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKN-V_j}$
M5: $V \rightarrow S: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKS-V_j}$
M6: $V \rightarrow P: \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}_{SKP-V_j+1}$

4. Security Analysis

4.1. Message Confidentiality

Our protocol satisfies the confidentiality problem by using symmetric key encryption to messages in each step of protocol to assure that only intended receiver can decrypt message sent to them.

4.2. Message Integrity

It can be seen that, in the proposed protocol, each message contains MAC. It is ensured by applying MAC that an attacker will not be able to alter or modify the message without being detected by the receiver.

4.3. Mutual Authentication

Each message in the protocol can be used to identify the sender and the receiver of the message, therefore ensuring authentication to N, P, and S. Our protocol be composed of symmetric cryptographic method, hash function, and Message Authentication Code (MAC) only. Moreover, with using the technique of offline session key generation and distribution. Only the sender and the receiver who share the same key will be able to encrypt and decrypt messages. It can be seen that, in the message M1, although N and P share the session key SK_{N-P_j} , P cannot generate this message $h(ID_N, T_1, request, SK_{N-S_j})$ by itself. This is because P cannot generate $h(ID_N, T_1, request, SK_{N-S_j})$ as the session key SK_{N-S_j} is shared between N and S. Only N knows both SK_{N-S_j} and SK_{N-P_j} . Hence this guarantees that N generated this message $h(ID_N, T_1, request, h(ID_N, T_1, request, SK_{N-S_j}), \{h_{N-TP}\}_{SK_{N-TP_j}}, SK_{N-P_j})$.

4.4. Non-Repudiation of Transactions

The proposed protocol uses symmetric encryption to encrypt message. It can satisfy the non-repudiation property by keeping evidence from each message that each party performed in each transaction. To show that our protocol satisfies the non-repudiation of transactions. In the message M1, it can be seen that N and P share the session key SK_{N-P_j} , but P cannot generate this message $h(ID_N, T_1, Request, SK_{N-S_j})$ by itself because the session key SK_{N-S_j} is shared between N and S. Only N knows both SK_{N-S_j} and SK_{N-P_j} , hence N cannot refuse that it did not originate this message as the possession of SK_{N-P_j} demonstrates clearly that only N can generate this message $h(ID_N, T_1, request, h(ID_N, T_1, request, SK_{N-S_j}), \{h_{N-TP}\}_{SK_{N-TP_j}}, SK_{N-P_j})$.

4.5. Brute Force Attack Prevention

The suggested protocol changes session keys every time at the completion of the transaction. It is hard to discover the correct session key. In addition, the technique of offline key generation and distribution is utilized in our protocol to resistance to brute force attacks.

4.6. Replay Attack Prevention

A replay attack is one in which an attacker obtains a copy of an authenticated message and later transmits it to the intended destination. Our proposed protocol use timestamps and limited-use session keys preventing replay attacks as the session keys used in this protocol are used only once.

4.7. MITM Attack

A MITM attack can be prevented with the combination of symmetric-key cryptographic operations including hash function. No confidential information is exposed, the reuse of authentication information is limited, and our protocol provides mutual authentication that can identify both its sender and recipient.

4.8. Eavesdropping

An attacker uses a suitable antenna and close enough in order to receive transferred information, such as credit card numbers, or manipulate payment information. Eavesdropping can be avoided by establishing a secure channel between two NFC devices, our proposed protocol can avoid eavesdropping by applying symmetric cryptography, including the hash function of messages in each step.

4.9. Data Manipulation

An attacker intercepts and alters data throughout the communication. This attack cannot occur successfully because the proposed protocol uses symmetric cryptography, including the hash function in all steps.

5. Discussions

5.1. Practicality of the Proposed Protocol

In this segment, we will compare the proposed protocol with previous protocols in [5–9] regarding performance, including fairness, security properties, cryptographic operations cost, energy consumption, time consumption, communication cost, and storage cost.

Table 2 displays a comparison of the fairness of NFC authentication protocols. We proposed a comparison between the NFC authentication protocols in [5–9] and our protocol. Regarding the model outlined in [10–12], the protocols proposed in [5,7–9] have no fairness because the trusted third party is not involved. In addition, the protocols proposed in [5,7–9] cannot resolve disputes in case one party misbehave because they do not contain the resolve disputes phase. The proposed protocol in [6] is weak in terms of fairness according to the model delineated in [10–12] as [6] cannot resolve conflicts in case one party misbehave because they do not contain the resolve dispute phase. It can be seen that the proposed protocol satisfies strong fairness according to the model suggested in [10–12].

Table 2. Compared fairness.

Protocol	A1	A2	A3	A4
[5]	No Fairness	No	Without TP	No
[6]	Weak Fairness	Yes	Online TP	No
[7]	No Fairness	No	Without TP	No
[8]	No Fairness	No	Without TP	No
[9]	No Fairness	No	Without TP	No
Our protocol	Strong	Yes	Online	Yes

A1: type of fairness; A2: use trusted third party (TP); A3: TP type; A4: dispute resolution.

Table 3 exhibits a comparison of the security properties of the protocols found in [5–9] with our protocol. It is clear that our protocol and [8] satisfy the necessary security properties and resistance to attacks, which are message confidentiality, message integrity, mutual authentication, non-repudiation of transactions, brute force attack prevention, replay attack prevention, MITM attacks, eavesdropping, and data manipulation.

5.2. Performance Analysis

From Table 4, Figures 4–6 demonstrate comparisons of cryptographic operations, energy consumption and time consumption between our protocol and the other protocols in [5–9]. The proposed protocol in [5,6,8,9] uses more energy consumption than our protocol. Our protocol uses more energy consumption than the protocol in [7]. Nevertheless, the protocol in [7] still lacks security property and strong fairness. The offered protocol in [5,8,9] takes more time consumption than our protocol. Our protocol takes more time consumption than the protocols in [6,7]. However, the protocol in [6,7] still lacks security properties and strong fairness. Note that time consumption is

derived from [16], which is proposed in [10,12]. Energy consumption is derived from [17], which is recommended in [18,19]. Table 5 demonstrates symbols, abbreviations and with their sizes in order to calculate communication cost, and storage cost of our protocol with previous protocols in [5–9]. In communication cost, Table 6 and Figure 7 show comparisons of communication cost between the previous protocols in [5–9] and the proposed protocol. It can be seen that the proposed protocol has a lower communication cost than the existing protocols in [5,9]. Nonetheless, the proposed protocol has a higher communication cost than the protocols in [6–8] but these protocols not satisfied security properties and strong fairness. In storage cost, Table 7 and Figure 8 represent comparisons of storage cost between the proposed protocol and the previous protocols in [5–9]. It is clear that the existing protocols in [5,8,9] have a higher storage cost than our proposed protocol. However, the existing protocols in [6,7] have a lower communication cost than the proposed protocols, but protocols in [6,7] cannot provide security properties and strong fairness.

Table 3. Comparison of security properties.

	[5]	[6]	[7]	[8]	[9]	Our Protocol
B1	Y	Y	Y	Y	Y	Y
B2	Y	N	Y	Y	Y	Y
B3	Y	N	Y	Y	Y	Y
B4	N	N	Y	Y	Y	Y
B5	N	Y	N	Y	N	Y
B6	Y	Y	Y	Y	Y	Y
B7	Y	Y	Y	Y	Y	Y
B8	Y	Y	Y	Y	Y	Y
B9	Y	Y	Y	Y	Y	Y

B1: message confidentiality; B2: message integrity; B3: mutual authentication; B4: non-repudiation of transactions; B5: brute force attack prevention; B6: replay attack prevention; B7: man-in-the-middle attack; B8: eavesdropping; B9: data manipulation.

Figure 4. Cryptographic operations cost.

Table 4. Protocol comparisons of cryptographic operations cost, energy consumption, and time consumption.

Protocol	Cryptographic Operations	Energy Consumption			Total	Time Consumption			Total
		C1	C2	C3		C4	C5	C6	
[5]	TS7 + TA4 + TH3 = 14	8.47	2186	2.28	2196.75	11.97	60.84	3.84	76.65
[6]	TS1 + TA1 + TH0 = 2	1.21	546.5	0	547.71	1.71	15.21	0	16.92
[7]	TS6 + TA0 + TH5 = 11	7.26	0	3.8	11.06	10.26	0	6.4	16.66
[8]	TS0 + TA5 + TH2 = 7	0	2732.5	1.52	2734.02	0	76.05	2.56	78.61
[9]	TS2 + TA2 + TH2 = 6	2.42	1093	1.52	1096.94	3.42	30.42	2.56	36.4
Our Protocol	TS6 + TA0 + TH10 = 16	7.26	0	7.6	14.86	10.26	0	12.8	23.06

C1 = AES (1.21 μ J/byte); C2 = RSA (546.5 μ J/byte); C3 = SHA1 (0.76 μ J/byte); C4 = AES (1.71 ms/byte); C5 = RSA (15.21 ms/byte); C6 = SHA1 (1.28 ms/byte); TS: a symmetric encryption or decryption operation time cost; TA: an asymmetric encryption or decryption operation time cost; TH: a one-way hash operation time consumption.

Figure 5. Energy Consumption. **Figure 6.** Time Consumption.

Table 5. Symbols and abbreviations.

Symbol	Definition	Bits
P/S/C/IB/AB/ID _{SE} /ID _r /ID _c /ID _C /ID _R /ID _m /ID _N /ID _P	Identity number	80
RP ₁ /RP ₂ /RS ₁ /RS ₂ /RV _{SE} /RV _{POS} /RAND _C /RAND _R /RM/RS/RBIs	Random number	80
TS/T ₁ /T ₂	Time-stamp	80
Cert(P)/Cert(S)/Cert(AB)/Cert(IB)/CertPOS/CertBAq	Certification	1024
ReqS/ReqP/ReqM/ReqPOS/ReqK/ReqM2	Authentication request message	128
ReqSession	Session request	128
Confirm/ConfirmPOS/ConfirmM	Confirmation authenticity message	56
H/h	One way hashing function	160
KMaster	Master session key	128
X	Banking data stored on the secure element	-
Cert _{POS}	Certification	1024
session_key/SK _{POS-SE} /KUD/KDS/KUS/KS/kpm	Symmetric session key	128
IdVU/IdVD	Virtual identity	80
NU/ND	Nonce	128
pwb	Password	128
KPbr/KPbc	Public key	1024
Loc _C /Loc _R	Location information	80
TData	-	-
BankData	Banking Data	1024
Request	Authentication request message	128
Response	Authentication response message	128

Table 6. Protocol comparison of communication cost.

Protocol	Communication Cost (bits)
[5]	$(1) + (2) + (3) + (4) + (5) + (6) + (7) = (80 + 80 + 80 + 80 + 1024 + 1024 + 128 + 160) + (80 + 80 + 80 + 80 + 1024 + 1024 + 128 + 160 + 80 + 80 + 128 + 128) + (80 + 80 + 80 + 80 + 80 + 80 + 56 + 1024 + 128) + (80 + 80 + 80 + 80 + 128 + 1024 + 1024 + 160 + 80 + 80 + 80 + 80 + 80) + (80 + 80 + 80) + (80 + 80 + 80 + 80) + (80 + 80 + 80 + 80 + 160) = 11,521$
[6]	$(1) + (2) + (3) + (4) = (80 + 80) + (80 + 80 + 1024 + 80) + (128 + 128) + (80 + 128) = 1888$
[7]	$(1) + (2) + (3) + (4) + (5) = (80 + 128 + 128 + 160) + (80 + 80 + 128 + 128) + (128 + 128 + 160 + 160) + (128 + 128 + 160) + (160) = 2064$
[8]	$(1) + (2) + (3) + (4) = (1024 + 80 + 160) + (1024 + 80 + 160 + 80 + 80 + 80) + (80 + 80 + 80 + 80 + 80) + (128 + 80 + 80) = 3456$
[9]	$(1) + (2) + (3) + (4) + (5) + (6) = (128 + 1024 + 1024 + 160) + (128 + 1024 + 1024 + 160 + 80 + 128 + 128 + 80) + (80 + 80 + 56 + 128 + 80 + 80 + 56 + 128 + 1024 + 160) + (80 + 80 + 56 + 128 + 80 + 80 + 1024 + 160) + (80 + 80 + 56 + 1024 + 160 + 128) + (80 + 80 + 80 + 56) = 10,472$
Our Protocol	$(1) + (2) + (3) + (4) + (5) + (6) = (80 + 80 + 128 + 160 + 160 + 160) + (80 + 80 + 80 + 128 + 160 + 160 + 160 + 160) + (160 + 160 + 160) + (160 + 160 + 160) + (80 + 128 + 160 + 160 + 160) + (80 + 128 + 160 + 160 + 160) = 4112$

Figure 7. Communication cost.

Table 7. Protocol comparison of storage cost.

Protocol	Storage Cost (bits)
	NFC-Enabled Smartphone
[5]	$(1) + (2) + (3) + (4) + (5) + (6) + (7) = (80 + 80 + 80 + 80 + 1024 + 1024 + 128 + 160) + (80 + 80 + 80 + 80 + 1024 + 1024 + 128 + 160 + 80 + 80 + 128 + 128) + (80 + 80 + 80 + 80 + 80 + 80 + 56 + 1024 + 128) + (80 + 80 + 80 + 80 + 128 + 1024 + 1024 + 160 + 80 + 80 + 80 + 80 + 80) + (80 + 80 + 80) + (80 + 80 + 80 + 80) + (80 + 80 + 80 + 80 + 160) = 11,521$
[6]	$(1) + (4) = (80 + 80) + (80 + 128) = 368$
[7]	$(1) + (4) + (5) = (80 + 128 + 128 + 160) + (128 + 128 + 160) + (160) = 1072$
[8]	$(1) + (2) + (3) + (4) = (1024 + 80 + 160) + (1024 + 80 + 160 + 80 + 80 + 80) + (80 + 80 + 80 + 80 + 80) + (128 + 80 + 80) = 3456$
[9]	$(1) + (2) + (3) + (4) = (128 + 1024 + 1024 + 160) + (128 + 1024 + 1024 + 160 + 80 + 128 + 128 + 80) + (80 + 80 + 56 + 128 + 80 + 80 + 56 + 128 + 1024 + 160) + (80 + 80 + 56 + 128 + 80 + 80 + 1024 + 160) = 8648$
Our Protocol	$(1) + (6) = (80 + 80 + 128 + 160 + 160 + 160) + (80 + 128 + 160 + 160 + 160) = 1456$

Figure 8. Storage cost.

The results show that the proposed protocol uses fewer resources. Even though our protocol uses a hash function rather than an encrypted protocol, the proposed protocol still has security and strong fairness compared with protocols in [5–9].

6. Formal Security Verification

6.1. Using Scyther

The Scyther tool is a formal proof for security protocols. It is an automated security protocol analysis tool based on the security protocol description language (SPDL) [20,21]. Many researchers have now utilized the Scyther tool to validate security protocols; see [22,23]. Our protocol is verified using the “verification claim” scheme in the Scyther tool. It can be seen that status (OK) for all the claims are utilized to verify the security properties and no attacks are discovered within bounds. It shown in Figure 9.

6.2. Using AVISPA

The automated validation of internet security protocols and applications (AVISPA) tool is a formal verification tool for network security protocols. AVISPA is developed by [24] and can be found in [25,26] used for verifying network security protocols. We simulate and check the proposed protocol under both, on-the-fly model-checker (OFMC) and constraint logic-based attack searcher (CL-ATSE)

back-ends. It can be seen that simulation reports of OFMC and CL-ATSE reports of our protocol in AVISPA are safe, as shown in Figure 10.

Claim	Status	Comments
FairnessNFCAuthen, N	Niagree	Ok Verified No attacks.
FairnessNFCAuthen, N3	Nisynch	Ok Verified No attacks.
FairnessNFCAuthen, N4	Alive	Ok Verified No attacks.
FairnessNFCAuthen, N5	Weakagree	Ok Verified No attacks.
FairnessNFCAuthen, N6	P	Niagree Ok Verified No attacks.
FairnessNFCAuthen, P3	Nisynch	Ok Verified No attacks.
FairnessNFCAuthen, P4	Alive	Ok Verified No attacks.
FairnessNFCAuthen, P5	Weakagree	Ok Verified No attacks.
FairnessNFCAuthen, P6	S	Niagree Ok Verified No attacks.
FairnessNFCAuthen, S3	Nisynch	Ok Verified No attacks.
FairnessNFCAuthen, S4	Alive	Ok Verified No attacks.
FairnessNFCAuthen, S5	Weakagree	Ok Verified No attacks.
FairnessNFCAuthen, S6	TP	Niagree Ok Verified No attacks.
FairnessNFCAuthen, TP3	Nisynch	Ok Verified No attacks.
FairnessNFCAuthen, TP4	Alive	Ok Verified No attacks.
FairnessNFCAuthen, TP5	Weakagree	Ok Verified No attacks.
FairnessNFCAuthen, TP6		

Figure 9. The result of our protocol verification using the Scyther.

Figure 10. The result of on-the-fly model-checker (OFMC) and constraint—logic-based attack searcher (CL-AtSe) of verification using the automated validation of internet security protocols and applications (AVISPA).

6.3. Using BAN

In this fragment, The BAN logic [27] is a well-known formal model, which is used to examine the security of mutual authentication using the widely-accepted works [28,29]. The notations used in BAN logic [27] are defined in Table 8.

Table 8. Burrows, Abadi and Needham (BAN) logic notations.

Symbol	Definitions
X, Y	Statement
P, Q	Parties
$P \models X$	P believes in X
$P \triangleleft X$	P sees X
$P \sim X$	P once said X
$P \Rightarrow X$	P has the jurisdiction over X
$\#(X)$	The formula X is fresh
$P \stackrel{K}{\leftrightarrow} Q$	P and Q may use the shared key K to communicate
$P \stackrel{X}{\leftrightarrow} Q$	The formula Y is a secret known only to P and Q
$\{X\}_K$	The formula X is encrypted under the key K
$(X)_K$	The hash value of X using K as a key

Moreover, the proposed protocols use six rules of BAN logic to prove a security protocol:

- R1. Message-meaning rule: $\frac{P \models P \stackrel{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \models Q \sim X}, \frac{P \models P \stackrel{K}{\leftrightarrow} Q, P \triangleleft (X)_K}{P \models Q \sim X}$
- R2. Nonce-verification rule: $\frac{P \models \#(X), P \models Q \sim X}{P \models Q \models X}$
- R3. Jurisdiction rule: $\frac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$
- R4. Freshness rule: $\frac{P \models \#(X)}{P \models \#(X, Y)}$
- R5. Belief rule: $\frac{P \models (X), P \models Y}{P \models (X, Y)}$
- R6. Decryption rule: $\frac{P \models Q \stackrel{K}{\leftrightarrow} P, P \triangleleft \{X\}_K}{P \triangleleft X}$

We analyze mutual authentication using BAN logic to show that our protocol guarantee a secure mutual authentication of all parties.

6.3.1. Idealized Form

- M1:** $N \rightarrow P$: $ID_N, T_1, \text{request}, h(ID_N, T_1, \text{request}, N \stackrel{SK_{N-Sj}}{\longleftrightarrow} S), h(ID_N, T_1, \text{request}, h(ID_N, T_1, \text{request}, N \stackrel{SK_{N-Sj}}{\longleftrightarrow} S), \{h_{N-TP}\}N \stackrel{SK_{N-TPj}}{\longleftrightarrow} TP, N \stackrel{SK_{N-Pj}}{\longleftrightarrow} P), \{h_{N-TP}\}N \stackrel{SK_{N-TPj}}{\longleftrightarrow} TP$
- M2:** $P \rightarrow S$: $ID_N, ID_P, T_1, \text{request}, h(ID_N, T_1, \text{request}, N \stackrel{SK_{N-Sj}}{\longleftrightarrow} S), h(ID_P, h(ID_N, T_1, \text{request}, N \stackrel{SK_{N-Sj}}{\longleftrightarrow} S), \{h_{N-TP}\}N \stackrel{SK_{N-TPj}}{\longleftrightarrow} TP, \{h_{P-TP}\}P \stackrel{SK_{P-TPj}}{\longleftrightarrow} TP$
- M5:** $S \rightarrow P$: $T_2, \text{response}, h(T_1, T_2, \text{response}, N \stackrel{SK_{N-Sj+1}}{\longleftrightarrow} S), h(h(T_1, T_2, \text{response}, N \stackrel{SK_{N-Sj+1}}{\longleftrightarrow} S), P \stackrel{SK_{P-Sj+1}}{\longleftrightarrow} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}N \stackrel{SK_{N-TPj+1}}{\longleftrightarrow} TP, \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}P \stackrel{SK_{P-TPj+1}}{\longleftrightarrow} TP$
- M6:** $P \rightarrow N$: $T_2, \text{response}, h(T_1, T_2, \text{response}, N \stackrel{SK_{N-Sj+1}}{\longleftrightarrow} S), h(h(T_1, T_2, \text{response}, N \stackrel{SK_{N-Sj+1}}{\longleftrightarrow} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}N \stackrel{SK_{N-TPj+1}}{\longleftrightarrow} TP, N \stackrel{SK_{N-Pj+1}}{\longleftrightarrow} P), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}N \stackrel{SK_{N-TPj+1}}{\longleftrightarrow} TP$

6.3.2. Initial Assumptions

- A1. $S \models N \stackrel{SK_{N-Sj}}{\longleftrightarrow} S$ A2. $N \models N \stackrel{SK_{N-Sj}}{\longleftrightarrow} S$
- A3. $S \models N \stackrel{SK_{N-Sj+1}}{\longleftrightarrow} S$ A4. $N \models N \stackrel{SK_{N-Sj+1}}{\longleftrightarrow} S$
- A5. $P \models N \stackrel{SK_{N-Pj}}{\longleftrightarrow} P$ A6. $N \models N \stackrel{SK_{N-Pj}}{\longleftrightarrow} P$
- A7. $P \models N \stackrel{SK_{N-Pj+1}}{\longleftrightarrow} P$ A8. $N \models N \stackrel{SK_{N-Pj+1}}{\longleftrightarrow} P$
- A9. $P \models P \stackrel{SK_{P-Sj}}{\longleftrightarrow} S$ A10. $S \models P \stackrel{SK_{P-Sj}}{\longleftrightarrow} S$

- A11. $P \models P \xleftrightarrow{SK_{P-Sj+1}} AS$ A12. $S \models P \xleftrightarrow{SK_{P-Sj+1}} S$
 A13. $N \models \#(T_1)$ A14. $P \models \#(T_1)$
 A15. $S \models \#(T_1)$ A16. $N \models \#(T_2)$
 A17. $P \models \#(T_2)$ A18. $S \models \#(T_2)$

6.3.3. The Goals of the Analysis

- G1. $S \models h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S)$ from M1
 G2. $P \models h(ID_N, T_1, request, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), \{h_{N-TP}\}N \xleftrightarrow{SK_{N-TPj}} TP, N \xleftrightarrow{SK_{N-Pj}} P)$ from M1
 G3. $S \models h(ID_P, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), P \xleftrightarrow{SK_{P-Sj}} S)$ from M2
 G4. $P \models h(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), P \xleftrightarrow{SK_{P-Sj+1}} S)$ from M5
 G5. $N \models h(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}N \xleftrightarrow{SK_{N-TPj+1}} TP, N \xleftrightarrow{SK_{N-Pj+1}} P)$ from M6
 G6. $N \models h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S)$ from M6

6.3.4. Details of the Proof

- G1. $S \models h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S)$ from M1
 $S \triangleleft h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S)$ 1
1, R1: $S \models h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S)$ 2
2, R2, R4, A1, A15: $S \models S$ has $(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S)$ 3
3, R5: $S \models h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S) = h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S)$ 4
4: $S \models h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S)$ 5
 G2. $P \models h(ID_N, T_1, request, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), \{h_{N-TP}\}N \xleftrightarrow{SK_{N-TPj}} TP, N \xleftrightarrow{SK_{N-Pj}} P)$ from M1
 $P \triangleleft h(ID_N, T_1, request, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), \{h_{N-TP}\}N \xleftrightarrow{SK_{N-TPj}} TP, N \xleftrightarrow{SK_{N-Pj}} P)$ 1
1, R1: $P \models h(ID_N, T_1, request, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), \{h_{N-TP}\}N \xleftrightarrow{SK_{N-TPj}} TP, N \xleftrightarrow{SK_{N-Pj}} P)$ 2
2, R2, R4, A5, A14: $P \models P$ has $(ID_N, T_1, request, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), \{h_{N-TP}\}N \xleftrightarrow{SK_{N-TPj}} TP, N \xleftrightarrow{SK_{N-Pj}} P)$ 3
3, R5: $P \models h(ID_N, T_1, request, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), \{h_{N-TP}\}N \xleftrightarrow{SK_{N-TPj}} TP, N \xleftrightarrow{SK_{N-Pj}} P) = h(ID_N, T_1, request, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), \{h_{N-TP}\}N \xleftrightarrow{SK_{N-TPj}} TP, N \xleftrightarrow{SK_{N-Pj}} P)$ 4
4: $P \models h(ID_N, T_1, request, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), \{h_{N-TP}\}N \xleftrightarrow{SK_{N-TPj}} TP, N \xleftrightarrow{SK_{N-Pj}} P)$ 5
 G3. $S \models h(ID_P, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), P \xleftrightarrow{SK_{P-Sj}} S)$ from M2
 $S \triangleleft h(ID_P, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), P \xleftrightarrow{SK_{P-Sj}} S)$ 1
1, R1: $S \models h(ID_P, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), P \xleftrightarrow{SK_{P-Sj}} S)$ 2
2, R2, R4, A10, A15: $S \models S$ has $(ID_P, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), P \xleftrightarrow{SK_{P-Sj}} S)$ 3
3, R5: $S \models h(ID_P, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), P \xleftrightarrow{SK_{P-Sj}} S) = h(ID_P, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), P \xleftrightarrow{SK_{P-Sj}} S)$ 4
4: $S \models h(ID_P, h(ID_N, T_1, request, N \xleftrightarrow{SK_{N-Sj}} S), P \xleftrightarrow{SK_{P-Sj}} S)$ 5
 G4. $P \models h(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), P \xleftrightarrow{SK_{P-Sj+1}} S)$ from M5
 $P \triangleleft h(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), P \xleftrightarrow{SK_{P-Sj+1}} S)$ 1
1, R1: $P \models h(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), P \xleftrightarrow{SK_{P-Sj+1}} S)$ 2
2, R2, R4, A11, A17: $P \models P$ has $(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), P \xleftrightarrow{SK_{P-Sj+1}} S)$ 3
3, R5: $P \models h(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), P \xleftrightarrow{SK_{P-Sj+1}} S) = h(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), P \xleftrightarrow{SK_{P-Sj+1}} S)$ 4
4: $P \models h(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), P \xleftrightarrow{SK_{P-Sj+1}} S)$ 5
 G5. $N \models h(h(T_1, T_2, response, N \xleftrightarrow{SK_{N-Sj+1}} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\}N \xleftrightarrow{SK_{N-TPj+1}} TP, N \xleftrightarrow{SK_{N-Pj+1}} P)$ from M6

$N \triangleleft h(h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\})N \xleftrightarrow{SK_{N-TPj+1}} TP, N \xleftrightarrow{SK_{N-Pj+1}} P)$	1
1, R1: $N \models h(h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\})N \xleftrightarrow{SK_{N-TPj+1}} TP, N \xleftrightarrow{SK_{N-Pj+1}} P)$	2
2, R2, R4, A8, A16: $N \models h(h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\})N \xleftrightarrow{SK_{N-TPj+1}} TP, N \xleftrightarrow{SK_{N-Pj+1}} P)$	3
3, R5: $N \models h(h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\})N \xleftrightarrow{SK_{N-TPj+1}} TP, N \xleftrightarrow{SK_{N-Pj+1}} P) = h(h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\})N \xleftrightarrow{SK_{N-TPj+1}} TP, N \xleftrightarrow{SK_{N-Pj+1}} P)$	4
4: $N \models h(h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S), \{h(h_{N-TP}, h_{P-TP}, h_{S-TP})\})N \xleftrightarrow{SK_{N-TPj+1}} TP, N \xleftrightarrow{SK_{N-Pj+1}} P)$	5
G6: $N \models h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S)$ from M6	
$N \triangleleft h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S)$	1
1, R1: $N \models h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S)$	2
2, R2, R4, A4, A16: $N \models N \text{ has } (T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S)$	3
3, R5: $N \models h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S) = h(T_1, T_2, \text{response}, N \xleftrightarrow{SK_{N-Sj+1}} S)$	4
4: $N \models h(T_1, T_2, \text{response}, NS)$	5

All established goals are successfully proven in the proposed protocol. Thus, it can be concluded that every party has satisfied a secure mutual authentication.

7. Conclusions

In this paper, we introduced a protocol that ensures mutual authentication for NFC mobile payment to all engaged parties using lightweight cryptographic operations for running on mobile devices. The proposed protocol satisfies the necessary transaction security and strong fairness for NFC communications, which are significant issues in mobile payment transactions regarding creating trust among the parties participating in the transaction. We have demonstrated that our proposed protocol is more effective compared to existing protocols regarding transaction security, fairness, and lightweight protocol. In case that one party misbehaves, the proposed protocol can resolve disputes. Furthermore, the robustness and soundness of the proposed protocol is ensured through use of BAN logic, the Scyther tool, and AVISPA to verify the security protocol.

Funding: This research was funded by the Faculty of Information Science and Technology, Mahanakorn University of Technology, Bangkok, Thailand.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Coskun, V.; Ozdenizci, B.; Ok, K. The survey on near field communication. *Sensors* **2015**, *15*, 13348–13405. [[CrossRef](#)] [[PubMed](#)]
2. Singh, N.K. Near-field Communication (NFC). *Inf. Technol. Libr.* **2020**, *39*, 2259–2294.
3. Thammarat, C.; Chokngamwong, R.; Techapanupreeda, C.; Kungpisdan, S. A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys. In Proceedings of the 29th Information Networking, Krong Siem Reap, Cambodia, 12–14 January 2015; pp. 133–138.
4. Singh, M.M.; Adzman, K.A.A.K.; Hassan, R. Near Field Communication (NFC) technology security vulnerabilities and countermeasures. *Int. J. Eng. Technol.* **2017**, *7*, 298–305.
5. El Madhoun, N.; Guenane, F.; Pujolle, G. A cloud-based secure authentication protocol for contactless-NFC payment. In Proceedings of the 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), Niagara Falls, ON, Canada, 5–7 October 2015; pp. 328–330.
6. Badra, M.; Badra, R.B. A lightweight security protocol for NFC-based mobile payments. *Procedia Comput. Sci.* **2016**, *83*, 705–711. [[CrossRef](#)]
7. Sethia, D.; Gupta, D.; Saran, H. NFC secure element-based mutual authentication and attestation for IoT access. *IEEE Trans. Consum. Electron.* **2018**, *64*, 470–479. [[CrossRef](#)]

8. Sethia, D.; Gupta, D.; Saran, H.; Agrawal, R.; Gaur, A. Mutual authentication protocol for secure NFC based mobile healthcard. *IADIS Int. J. Comput. Sci. Inf. Syst.* **2016**, *11*, 195–202.
9. Al-Haj, A.; Al-Tameemi, M.A. Providing security for NFC-based payment systems using a management authentication server. In Proceedings of the 2018 4th International Conference on Information Management (ICIM), Oxford, UK, 25–27 May 2018; pp. 184–187.
10. Thammarat, C.; Kurutach, W. A secure fair exchange for SMS-based mobile payment protocols based on symmetric encryption algorithms with formal verification. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 6953160. [[CrossRef](#)]
11. Thammarat, C.; Kurutach, W.; Phoomvuthisarn, S. A secure lightweight and fair exchange protocol for NFC mobile payment based on limited-use of session keys. In Proceedings of the 2017 17th International Symposium on Communications and Information Technologies (ISCIT), Cairns, Australia, 25–27 September 2017; pp. 1–6.
12. Thammarat, C.; Kurutach, W. A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification. *Int. J. Commun. Syst.* **2019**, *32*, e3991. [[CrossRef](#)]
13. Kungpisdan, S.; Metheekul, S. A secure offline key generation with protection against key compromise. In Proceedings of the 13th World Multiconference on Systemics, Cybernetics, and Informatics, Orlando, FL, USA, 10–13 July 2009.
14. Dandash, O.; Wang, Y.; Le, P.D. Fraudulent internet banking payments prevention using dynamic key. *J. Netw.* **2008**, *3*, 25–34. [[CrossRef](#)]
15. Ngo, H.H.; Wu, X.; Le, P.D.; Wilson, C.; Srinivasan, B. Dynamic key cryptography and applications. *Int. J. Netw. Secur.* **2010**, *10*, 161–174.
16. Zheng, X.; Yang, L.; Ma, J.; Shi, G.; Meng, D. TrustPAY: Trusted mobile payment on security-enhanced ARM TrustZone platforms. In Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 27–30 June 2016; pp. 456–462.
17. Potlapally, N.R.; Ravi, S.; Raghunathan, A.; Jha, N.K. A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *Trans. IEEE. Mob. Comput.* **2006**, *5*, 128–143. [[CrossRef](#)]
18. Zhang, L.; Ma, M. Secure and efficient scheme for fast initial link setup against key reinstallation attacks in IEEE 802.11 ah networks. *Int. J. Commun. Syst.* **2020**, *33*, e4192. [[CrossRef](#)]
19. Gupta, A.; Tripathi, M.; Sharma, A. A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN. *Comput. Commun.* **2020**, *160*, 311–325. [[CrossRef](#)]
20. Cremers, C. The scyther tool: Verification, falsification, and analysis of security protocols. In *International Conference on Computer Aided Verification*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 414–418.
21. Cremers, C.; Sjouke, M. *Operational Semantics and Verification of Security Protocols*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2012.
22. Shehada, D.; Yeun, C.Y.; Zemerly, M.J.; Qutayri, M.L.; Hammadi, Y.L.; Damiani, E.; Hu, J. BROSMAP: A novel broadcast based secure mobile agent protocol for distributed service applications. *Secur. Commun. Netw.* **2017**, *2017*, 414–418. [[CrossRef](#)]
23. Genge, B.; Haller, P.; Duka, A.V. Engineering security-aware control applications for data authentication in smart industrial cyber–physical systems. *Future Gener. Comput. Syst.* **2019**, *91*, 206–222. [[CrossRef](#)]
24. Armando, A.; Basin, D.; Boichut, Y.; Chevalier, Y.; Compagna, L.; Cuellar, J.; Drielsma, P.H.; Heám, P.C.; Kouchnarenko, O.; Mantovani, J.; et al. The AVISPA tool for the automated validation of internet security protocols and applications. In *International Conference on Computer Aided Verification*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 281–285.
25. Khedr, W.I. Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol. *J. Inf. Secur. Appl.* **2018**, *39*, 41–57. [[CrossRef](#)]
26. Cao, J.; Li, H.; Ma, M.; Li, F. UPPGHA: Uniform privacy preservation group handover authentication mechanism for mMTC in LTE-A networks. *Secur. Commun. Netw.* **2018**, 6854612. [[CrossRef](#)]
27. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [[CrossRef](#)]

28. Chandrakar, P.; Om, H. A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. *Comput. Commun.* **2017**, *110*, 26–34. [[CrossRef](#)]
29. Kumari, S.; Das, A.K.; Wazid, M.; Li, X.; Wu, F.; Choo, K.K.R.; Khan, M.K. On the design of a secure user authentication and key agreement scheme for wireless sensor networks. *Concurr. Comput. Pract. Exp.* **2017**, *29*, e3930. [[CrossRef](#)]

© 2020 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).