Privacy-Preserving NFC-Based Authentication Protocol for Mobile Payment System

Ali M. Allam[1*]
[1]Associate Professor, Communications, and Electronics Engineering Department, Faculty of Engineering, Helwan University, Egypt
[e-mail: ali_allam@h-eng.helwan.edu.eg]
[*]Corresponding author: Ali M. Allam

Received March 7, 2022; revised November 1, 2022; accepted May 11, 2023;
published May 31, 2023

Abstract

One of the fastest-growing mobile services accessible today is mobile payments. For the safety of this service, the Near Field Communication (NFC) technology is used. However, NFC standard protocol has prioritized transmission rate over authentication feature due to the proximity of communicated devices. Unfortunately, an adversary can exploit this vulnerability with an antenna that can eavesdrop or alter the exchanged messages between NFC-enabled devices. Many researchers have proposed authentication methods for NFC connections to mitigate this challenge. However, the security and privacy of payment transactions remain insufficient. We offer a privacy-preserving, anonymity-based, safe, and efficient authentication protocol to protect users from tracking and replay attacks to guarantee secure transactions. To improve transaction security and, more importantly, to make our protocol lightweight while ensuring privacy, the proposed protocol employs a secure offline session key generation mechanism. Formal security verification is performed to assess the proposed protocol's security strength. When comparing the performance of current protocols, the suggested protocol outperforms the others.

Keywords: Near Field Communication, Mobile Payment System, Third Party Authentication, Privacy-Preserving, Anonymity.

http://doi.org/10.3837/tiis.2023.05.009 **ISSN : 1976-7277**

1. Introduction

Many devices already include NFC, allowing for short-range communication and small data transfers. The usage of information and communication technology (ICT) is widespread worldwide [22]. However, NFC systems focus solely on communication speed, disregarding security aspects such as source and destination authentication [1–2] due to the minimal range of communications (about 10 cm). Due to this vulnerability in the NFC protocol, the authors in [3- 4] demonstrated that an adversary exploiting an NFC reader with a particular antenna might acquire confidential financial data from NFC bank cards or NFC-enabled devices within its (NFC reader) operational range. Many researchers [5-6] have discussed NFC's flaws, including authentication, protecting against replay, and man-in-the-middle attacks (MITM). Different methods have been suggested to provide party authentication in mobile payment systems using NFC technology [7–11].

El Madhoun et al. [7] devised a safe authentication system based on cloud infrastructure for NFC payment to solve security flaws revealed in the Europay, Mastercard, and Visa (EMV) protocols, which is the standard for securing contact and contactless NFC payment transactions. Asymmetric encryption is used in [7] to offer mutual authentication between an NFC-enabled device and an NFC-enabled point of sale (PoS) terminal. Also, symmetric encryption ensures bank data security during the authentication process. El Madhoun et al. [7] used the Scyther tool to confirm the security strength of the protocol. Unfortunately, there is a flaw in the protocol exchanged messages where users' IDs and transaction requests are sent in plaintext, allowing an eavesdropper to carry out a tracking attack and violate the parties' privacy.

Badra et al. [8] proposed detecting risks and weaknesses in the air interface between NFC-enabled smartphones and PoS terminals, as well as a method for securing NFC-based financial transactions using mobile devices. The suggested scheme is lightweight (due to the use of symmetric cryptosystem), simple, scalable, cost-effective, and has little computer processing overhead.

Sethia et al. [9] proposed a mutual authentication and verification system for the Internet of Things (IoT) access using NFC technology. The authors [9] deployed a cloud-based Trusted Certified Authority (TCA) to manage all cryptographic credentials and storage. In addition, the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool verifies the suggested protocol.

Authentication protocol was proposed by Sethia et al. [10] for protecting mobile health cards. The suggested protocol prevented replay threats, impersonating, and other types of attacks. For confidentiality, this protocol uses both asymmetric and symmetric cryptography.

For the Europay, Mastercard, and Visa (EMV) protocol, Al-Haj et al. [11] presented an enhanced security mechanism. The suggested protocol's management and authentication server authenticate the financial transactions and mutual authentication between the NFC-enabled device and the PoS terminal. Mutual authentication, non-repudiation, data integrity, secrecy, and data privacy are all security aspects of the protocol.

In [12], Thammarat has provided an authentication protocol for mobile payment between the merchant and the buyer in the presence of an authentication server to carry out the authentication process between them, as well as a trusted third party for the dispute resolution process if the merchant or buyer does not accept the transaction. The protocol is composed of four stages. In the first two stages, symmetric keys are distributed among all the system users. Following that, an authentication process between the seller and the buyer used plaintext IDs, resulting in a tracking attack and a plaintext transaction requested, resulting in a breach of the parties' privacy.

For NFC-based proximity payments, the authors presented the security and privacy-preserving mobile commerce (SPPMC) framework [13]. They claimed that their protocol protects the user's privacy and anonymity; however, this isn't true because the participants' certificates contain all their information. Furthermore, these certificates were sent as plaintext between parties during the protocol phases.

A public key cryptography-based NFC mobile payment mechanism was presented by the authors of [21]. In [23], the authors proposed a Secure Protocol for Mobile Transaction (NSPMT) protocol based on NFC that included a Defense in Depth approach. Their Defense-in-depth approach consisted of three levels: defense at the hardware level, defense at the application level, and defense at the communication level.

In general, the current proposed NFC-based authentication solutions do not provide adequate privacy and anonymity for users' identities, leading to tracking attacks. To protect the payment process based on NFC technology, this paper presented a secure authentication protocol for the user authentication step in the mobile payment system. The suggested authentication system depended on three parties' communications: the Client (C), Merchant (M), and Trusted Service Manager (TSM). The client and merchant must mutually authenticate each other as part of the protocol design. Existing payment protocols can be immediately applied to perform payment transactions at the payment transaction stage. As a result, the method of the payment transaction step isn't covered in this article.

In this paper, we introduce the following contribution:

- An NEC-based mobile payment system environment is designed and suggested for users with NFC-enabled devices to promote users' privacy and anonymity of their identity and security robustness and system performance.
- A secure Anonymous authentication mechanism is being developed to allow mobile payments based on an NFC-enabled device. The proposed authentication protocol creates and uses a unique session key for each communicating session—moreover, this session key is from an offline procedure to increase the protocol's security.
- A formal security verification is used to verify the security properties of our suggested protocol. The suggested protocol grants security, mutual authentication, forward and backward secrecy, and protection against five common attacks: tracking, passive eavesdropping, replay, man-in-the-middle (MITM), and impersonation.
- Performance comparison between current protocols shows that the suggested protocol is more efficient than the other solutions.

The remainder of the paper is arranged as follows. The system architecture presents in section 2. In section 3, our proposed authentication protocol is discussed. The formal security analysis for our solution is introduced in section 4. Section 5 gives the performance analysis of our protocol. Finally, section 6 concludes the paper.

2. System Architecture

The relationships between different parties throughout mobile payment transactions are illustrated in **Fig. 1**. The architecture proposed in [14] has given rise to our system.

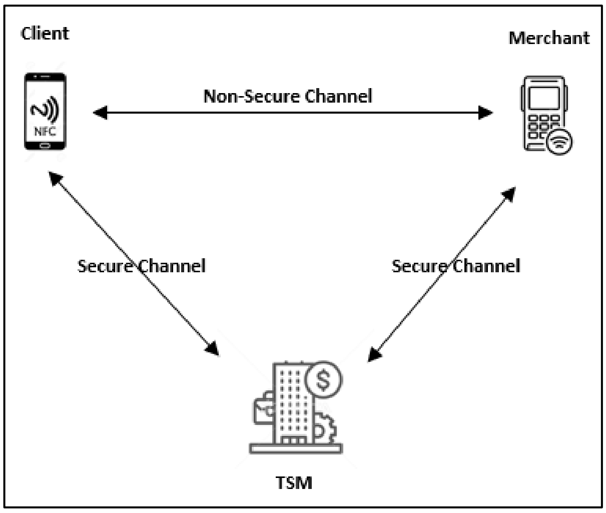


Fig. 1. System Architecture.

Fig. 1 represents the suggested system design. The system architecture consists of three components: Client, Merchant, and Trusted Service Manager. The client and the merchant communicated via an insecure NFC channel. A secure Internet link connects the merchant to the Trusted Service Manager. In addition, the client uses a secure channel to communicate with the Trusted Service Manager.

One of the primary components of the suggested payment system is the client's NFC-enabled device. The client's device has a Secure Element (SE) that performs the cryptographic operation and stores confidential financial data. As shown in **Fig. 1**, the client will use NFC technology to connect to and communicate with the merchant.

The merchant uses an NFC-enabled Point-of-Sale (PoS) device. The merchant's PoS is connected to a secure Internet link to back-end processing services, such as the Trusted Service Manager.

The merchant's device interacts with the client's device to complete the payment transaction during the payment process. First, through the Trusted Service Manager, the merchant confirms the validity of the relevant client's machine. Then, the merchant will finish the payment transaction once the authenticity of the related client's device is verified.

The Trusted Service Manager (TSM) plays a vital role in data security by acting as a mediator. Multiple parties collaborate to coordinate technical and business exchanges, including Mobile Network Operators (MNOs), banks and other service providers, ticketing agencies, and other issuing authorities. These companies can communicate with one another according to the TSM. Users can also download apps and services to their mobile devices using it. The significant responsibility of a TSM is to deliver all of these services securely, using encryption and authentication. It also allows secure and validated data installation into the Secure Element (SE) without holding the mobile device.

3. The Proposed Protocol

In this part, we propose a mobile payment authentication protocol based on NFC technology to disentangle the issues and overcome current protocols' limitations such as anonymity and privacy preservation [10 – 13]. Client (C), Merchant (M), and Trusted Service Manager (TSM) are all involved in the proposed authentication protocol. **Table 1** lists the notations used in this paper.

Table 1. Notations

Notation	Definition
ID_C	The unique identity of a client (C)
ID_M	The unique identity of a merchant (M)
$E_{K_x}\{\cdot\}$	Symmetric encryption by shared long-term key K_x
$H_1(\cdot)$	One-way hash function
$H_2(\cdot, K_x)$	A Message authentication code (MAC) value of a message with K_x
K_1	Shared long-term key between C & TSM
K_2	Shared long-term key M & TSM
N_1	Nonce generated by C
N_2	Nonce generated by M
TS_1	Timestamp generated by C
TS_2	Timestamp generated by M
TS_3	Timestamp generated by TSM
$Request_x$	A message is considered a payment request message generated by x
$Response$	A message is considered a payment response message.
PK_C	Public Key of C
PK_M	Public Key of M
SK_C	Secret Key of C
SK_M	Secret Key of M
K_S	Session Key
$f_1(\cdot)$	Elliptic Curve P-192 function
$f_2(\cdot)$	HMAC SHA-192

The proposed protocol comprises three phases: enrollment, authentication, and offline key exchange.

3.1 Enrollment Phase

The client and the merchant should register their mobile phones with their respective banks before completing any transaction to activate the service through an application, as shown in [14]. In addition, each party device must install a financial assistance provider-specific application during this phase. Finally, when the application is installed on the party's device, the party registers with the TSM via a secure channel like transport layer security (TLS). The purpose of registration is to provide the party with his financial information and a long-term shared key with TSM. This sensitive information will be stored in the secure element of the entity device. At this point, both C and M shared with TSM $K_1$and K_2 , respectively. TSM held the shared long-term key with the hashed value of the party's unique ID to achieve anonymity for all the parties.

3.2 Authentication Phase

During this phase, the proposed protocol depends on the TSM to provide mutual authentication between C and M. The proposed authentication protocol's execution sequence is illustrated in **Fig. 2** for all parties.

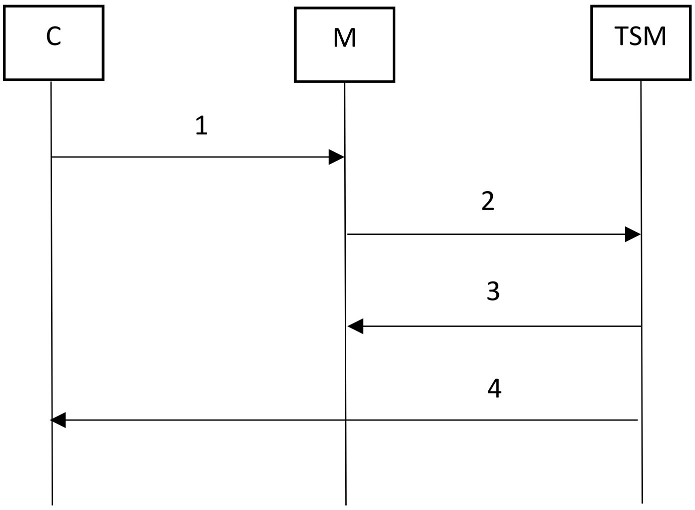


Fig. 2. The Protocol’s execution sequence

1. C→ M: Msg_1

$$Msg_1 = H_1(ID_C), E_{K_1}\{ID_C, Request_C, N_1, TS_1\}$$

2. M → TSM:Msg_1, Msg_2

$$Msg_2 = H_1(ID_M), E_{K_2}\{ID_M, Request_M, N_2, TS_2\}$$

3. TSM → M: Msg_3

$$Msg_3 = E_{K_2}\{Response, PK_C, H_2((Request_M, Response), K_2), H_1(ID_C), N_2, TS_3\}$$

4. TSM → C: Msg_4

$$Msg_4 = E_{K_1}\{Response, PK_M, H_2((Request_C, Response), K_1), H_1(ID_M), N_1, TS_3\}$$

C sends an authentication request Msg_1 to M, which contains the client’s concealed identity $H_1(ID_C)$ to avoid tracking attacks and provide anonymity. The second part of the message $H_1(ID_C), E_{K_1}\{ID_C, Request_C, N_1, TS_1\}$ is encrypted by a shared key between C and TSM to ensure authenticity and confidentiality. C can't dispute that he didn't send this message because of the possession of K_1.
When M received a message Msg_1 from C, he passed it to TSM along with his authentication message Msg_2, which has the same security features as Msg_1 for M.
On receiving messages M1 and M2 from M, TSM will process the following:
1- From hashed ID for each party, pick up the corresponding long-term shared key.
2- Decrypt each authenticated request and check its correctness.
3- If it accepts the request, it sends the authenticated response $H_2((Request_C, Response), K_1)$, ensuring the integrity of the response and the non-repudiation of the transaction. Besides the distribution of parties’ public keys in a session key calculation.
All the nonce and timestamps in the protocol are used to prevent replay attacks.

3.3 Session Key Exchange

At this point, both customer C and merchant M can compute offline, Diffie-Helman key K_{DH}.

For customer C:

$$K_{DH} = f_1(SK_C, PK_M)$$

For merchant M:

$$K_{DH} = f_1(SK_M, PK_C)$$

Then, both compute session key K_S

$$K_S = f_2(K_{DH}, N_1, N_2, H\{ID_C\}, H\{ID_M\})$$

Finally, C and M can execute mutual authentication using a trusted third-party TSM. This proposed authentication protocol uses only symmetric cryptographic operations, MAC, and a hash function, resulting in lightweight processes. As a result, it is suitable for NFC-enabled devices. Furthermore, using a secure offline session key generation approach will improve the protocol's security.

4. Security Analysis

This section explores the proposed authentication protocol for a mobile payment system using NFC technology in terms of security. First, the proposed protocol's security is evaluated in its ability to defend against replay attacks, eavesdropping, man-in-the-middle attacks, and tracking attacks. Then we utilized the Scyther tool to check the proposed protocol's security.

4.1 Security Characteristics

A few potential attacks are presented here to assess the security of the proposed protocol.

4.1.1 Replay Attack

A replay attack occurs when an adversary obtains a copy of an authenticated message and then resends it to the receiving party. A session key based on nonce values is generated in the proposed protocol for communication between client C and merchant M. The nonce value changes with each session, so the session key generation mechanism eliminates replay attacks.

4.1.2 Eavesdropping

An adversary utilizes an appropriate antenna and gets close enough to obtain or modify payment information, such as credit card numbers. Establishing a secure channel between two NFC devices can prevent eavesdropping; our suggested protocol can prevent eavesdropping by using symmetric cryptography and incorporating the hash function of messages in each step.

4.1.3 Main-In-The-Middle Attack

Our proposed protocol can mitigate a MITM attack by combining symmetric-key cryptographic procedures and the hash function. As a result, there is no exposure of confidential information, the reuse of authentication information is limited, and our protocol provides mutual authentication to identify both the transmitter and the receiver.

4.1.4 User Anonymity

As a result of the wireless transmission in NFC-based applications, an adversary can control the communication channel between users. Consider the possibility that an opponent intercepts the transmitted messages Msg_1, Msg_2 between client C and Merchant M. The hash values $H_1(ID_C)$and $H_1(ID_M)$ represent the identities of C and M, respectively because a hash value represents the user identity. Even if the adversary obtains the masked user identity, it is useless because the identity-hashed value does not expose the user's true identity. As a result, no attacker can deduce the true identities of the client and merchant from the intercepted messages. In that case, the suggested protocol guarantees user anonymity and avoids the tracking attack.

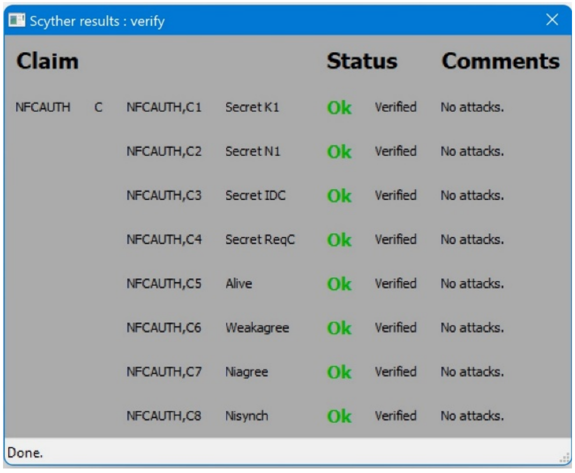
4.2 Formal Security Verification Using Scyther

In this section, our proposed mobile payment protocol is verified using a formal approach that proves the security properties and ensures that the protocol is free of various forms of attacks and vulnerabilities. Scyther [15] is a tool for analyzing security protocols using the perfect cryptography assumption, which assumes that all cryptographic functions are perfect. For example, the adversary can learn nothing from an encrypted communication unless he has the decryption key. Scyther employs an unbounded verification and validation technique, which seeks to show that a protocol is sound for all potential behaviors, including an opponent's existence [15]. It's a security protocol analysis tool that utilizes the security protocol description language (SPDL) as its basis [15, 16]. Several academics have now used the Scyther tool to verify security protocols; see [17, 18].

As a result, we constructed the suggested protocol in SPDL to validate authentication (with non-repudiation) and confidentiality of Scyther claims [15]. Our proposed protocol targeted five types of goals non-injective synchronization, non-injective agreement, weak agreement, secrecy, and the aliveness of all the participants. The Scyther tool's "verification claim" approach is used to verify our protocol.

As shown in **Fig. 2, 3**, and **4**, the protocol successfully guarantees all Scyther claims for C, M, and TSM, respectively, and no attacks are detected. Alive, Weakagree, Niagree, and Nisynch are authentication claims used to detect replay, relay, and man-in-the-middle attacks. Confidentiality claim Secret. [15] and [16] provide formal definitions for all Scyther claims.

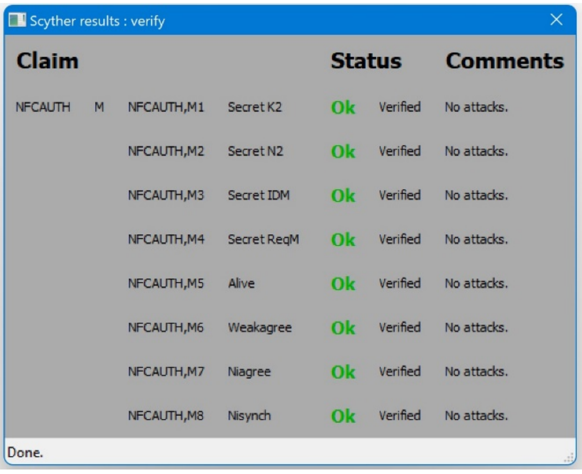
Six algorithms make up our suggested scheme. In this section, we will present the design of the scheme in detail.



Claim				Status		Comments
NFCAUTH	C	NFCAUTH,C1	Secret K1	Ok	Verified	No attacks.
		NFCAUTH,C2	Secret N1	Ok	Verified	No attacks.
		NFCAUTH,C3	Secret IDC	Ok	Verified	No attacks.
		NFCAUTH,C4	Secret ReqC	Ok	Verified	No attacks.
		NFCAUTH,C5	Alive	Ok	Verified	No attacks.
		NFCAUTH,C6	Weakagree	Ok	Verified	No attacks.
		NFCAUTH,C7	Niagree	Ok	Verified	No attacks.
		NFCAUTH,C8	Nisynch	Ok	Verified	No attacks.

Done.

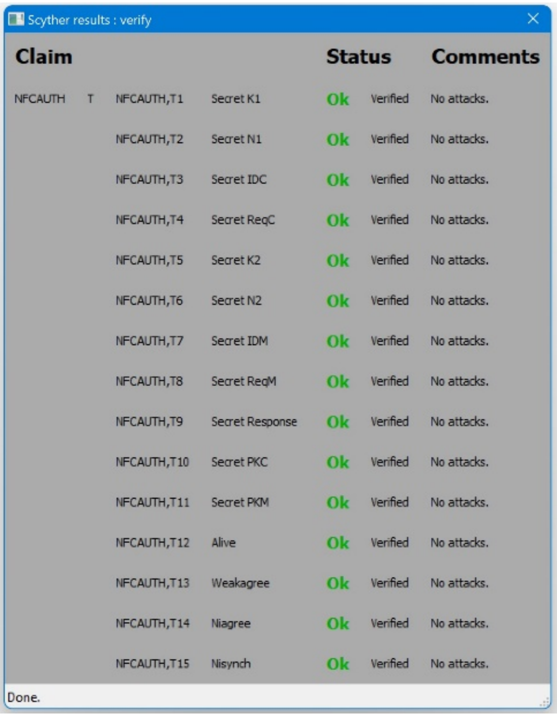
Fig. 2. Scyther results for the Client



```
Claim                                        Status        Comments

NFCAUTH   M   NFCAUTH,M1   Secret K2         Ok  Verified  No attacks.
              NFCAUTH,M2   Secret N2         Ok  Verified  No attacks.
              NFCAUTH,M3   Secret IDM        Ok  Verified  No attacks.
              NFCAUTH,M4   Secret ReqM       Ok  Verified  No attacks.
              NFCAUTH,M5   Alive             Ok  Verified  No attacks.
              NFCAUTH,M6   Weakagree         Ok  Verified  No attacks.
              NFCAUTH,M7   Niagree           Ok  Verified  No attacks.
              NFCAUTH,M8   Nisynch           Ok  Verified  No attacks.
Done.
```

Fig. 3. Scyther results for the Merchant



```
Claim                                        Status        Comments

NFCAUTH   T   NFCAUTH,T1   Secret K1         Ok  Verified  No attacks.
              NFCAUTH,T2   Secret N1         Ok  Verified  No attacks.
              NFCAUTH,T3   Secret IDC        Ok  Verified  No attacks.
              NFCAUTH,T4   Secret ReqC       Ok  Verified  No attacks.
              NFCAUTH,T5   Secret K2         Ok  Verified  No attacks.
              NFCAUTH,T6   Secret N2         Ok  Verified  No attacks.
              NFCAUTH,T7   Secret IDM        Ok  Verified  No attacks.
              NFCAUTH,T8   Secret ReqM       Ok  Verified  No attacks.
              NFCAUTH,T9   Secret Response   Ok  Verified  No attacks.
              NFCAUTH,T10  Secret PKC        Ok  Verified  No attacks.
              NFCAUTH,T11  Secret PKM        Ok  Verified  No attacks.
              NFCAUTH,T12  Alive             Ok  Verified  No attacks.
              NFCAUTH,T13  Weakagree         Ok  Verified  No attacks.
              NFCAUTH,T14  Niagree           Ok  Verified  No attacks.
              NFCAUTH,T15  Nisynch           Ok  Verified  No attacks.
Done.
```

Fig. 4. Scyther results for the TSM

The proposed protocol achieves all of the defined objectives. As a result, each side has met the requirements for secure mutual authentication.

5. Performance Analysis

The proposed and existing authentication protocols for the mobile payment system are compared regarding security characteristics and performance in this section. In addition, the proposed authentication protocol is compared to several current authentication protocols [11, 12, 13, 21, 23].

Table 2 compares the proposed authentication protocol to current protocols in several security aspects. As a result, as shown in **Table 2**:

- Ahamad et al. protocol [13] and our suggested protocol hide the user's identity. In [13], the identity of the user is not used. Instead, the certificate of the user is used in cipher form. Despite this, the recipient of an encrypted message in a symmetric system without sending the user's identity faces a hurdle in selecting the appropriate decryption key, which requires time-consuming searching to find the correct key. Instead, we use the hashed ID to protect user privacy and detect the corresponding key more quickly to overcome this challenge.
- In comparison to the other authentication protocols, Thammarat's protocol [12] and our proposed protocol enable backward/forward secrecy of the session key.
- Our protocol is the only protocol to mitigate the tracking attack due to the hashed identity in the exchanged message.

Table 2. Comparison of Security Characteristics

Property	**[11]**	**[12]**	**[13]**	**[21]**	**[23]**	**Proposed Protocol**
Party's Identity Cloaking	No	No	Yes	No	No	Yes
Privacy Preservation	No	No	Yes	No	No	Yes
Mutual Authentication	Yes	Yes	Yes	Yes	Yes	Yes
Session Key Security	No	Yes	No	No	No	Yes
Backward/Forward Secrecy Of Session Key	No	Yes	No	No	No	Yes
Replay Attack Mitigation	Yes	Yes	Yes	Yes	Yes	Yes
Man-In-The-Middle (MITM) Attack Mitigation	Yes	Yes	Yes	Yes	Yes	Yes
Tracking Attack Mitigation	No	No	No	No	No	Yes

Table 3 lists the symbols and abbreviations that can be used to compare our procedure's performance to those of other protocols [11–13, 21, 23].

Table 3. Notations used for Performance Analysis

Notation	Description
T_H	Time cost to perform the one-way hash function
T_S	Time cost to perform encryption or decryption operation in a symmetric cryptosystem
T_A	Time cost to perform encryption or decryption operation in a public-key cryptosystem

Next, the execution time and energy consumption for various cryptographic processes [19, 20] are shown in **Table 4**.

Finally, **Table 5** compares the performance of the proposed authentication protocol to existing approaches [11, 12, 13, 21, 23]. In addition, **Table 5** shows the mathematical symbols that reflect the individual time and energy usage during various computing operations.

Table 4. The energy and time consumption of some cryptographic operations based on [19, 20]

Operation	Energy Consumption $(\mu J/byte)$	Time Consumption $(ms/byte)$
Encryption/decryption operation of symmetric cryptosystem (AES)	1.21	1.71
Encryption/decryption operation of asymmetric cryptosystem (RSA)	546.5	15.21
One-way hash function (SHA-1)	0.76	1.28

Table 5. Protocol comparisons of cryptographic operations cost, energy consumption, and execution time.

Protocol	Cryptographic operations	Energy Consumption $(\mu J/byte)$	Time Consumption $(ms/byte)$
[11]	$2T_S + 2T_A + 2T_H$	1096.94	36.4
[12]	$6T_S + 10T_H$	14.86	23.06
[13]	$6T_S + 3T_A + T_H$	1647.52	57.17
[21]	$5T_S + 7T_A + T_H$	3832.31	116.3
[23]	$4T_S$	4.84	6.84
Proposed protocol	$4T_S + 4T_H$	7.88	11.96

Based on **Table 5**, our protocol depends only on two cryptographic operations hash function and symmetric cryptosystems, leading to less time than existing protocols [11-13, 21]. The hash function process has been used in our proposed protocol to include novel security features like Party's Identity Cloaking and tracking attack mitigation as well as to satisfy the security criteria of the payment system described in [14]. However, the authors in [23] missed to meet the security standards for payment systems in favor of protocol effectiveness, in addition to their protocol's inability to protect user privacy.

According to the results, the proposed protocol consumes fewer resources. In addition, as compared to protocols in [11-13, 21, 23], the suggested protocol provides privacy preservation and mitigates tracking attacks.

6. Conclusions

This paper proposes a secure, lightweight authentication technique for mobile payment systems that use NFC-enabled devices. Compared to the corresponding current protocols, our proposed protocol has a lower computation time and less energy. It also enhances security and privacy throughout the mobile payment transaction procedure. Furthermore, the proposed protocol protects against well-known attacks, including passive eavesdropping, replay, tracking attack, and man-in-the-middle. In addition, the proposed protocol provides mutual authentication and session key backward/forward secrecy. Additionally, the proposed protocol's security and validity are ensured by using the Scyther tool to verify the security protocol.

We plan to improve this proposed solution in the future, create a prototype, and demonstrate its effectiveness in a real-world setting.

References

[1] V. Coskun, B. Ozdenizci and K. Ok, “The Survey on Near Field Communication,” *Sensors*, vol. 15, no. 6, pp. 13348-13405, 2015. Article (CrossRef Link).

[2] P. Vishwakarma, A. Tripathy, and S. Vemuru, “Cryptanalysis of Near Field Communication Based Authentication Protocol for Mobile Payment System,” *Wireless Personal Communications*, vol. 121, no. 1, pp. 963-983, 2021. Article (CrossRef Link).

[3] M. Emms and A. van Moorsel, “Practical attack on contactless payment cards,” in *Proc. of HCI2011 Workshop Health, Wealth and Identity Theft*, 2011.

[4] R. Lifchitz, “Hacking the NFC credit cards for fun and debit,” in *Proc. of Hackito Ergo Sum conference*, April 2012.

[5] S. Bojjagani, D. Brabin, and P. Rao, “PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification,” *Procedia Computer Science*, vol. 171, pp. 1110-1119, 2020. Article (CrossRef Link).

[6] N. Akinyokun and V. Teague, “Security and Privacy Implications of NFC-enabled Contactless Payment Systems,” in *Proc. of the 12th International Conference on Availability, Reliability, and Security*, pp. 1-10, 2017. Article (CrossRef Link).

[7] N. El Madhoun, F. Guenane, and G. Pujolle, “A cloud-based secure authentication protocol for contactless-NFC payment,” in *Proc. of 2015 IEEE 4th International Conference on Cloud Networking (CloudNet)*, 2015. Article (CrossRef Link).

[8] M. Badra and R. Badra, “A Lightweight Security Protocol for NFC-based Mobile Payments,” *Procedia Computer Science*, vol. 83, pp. 705-711, 2016. Article (CrossRef Link).

[9] D. Sethia, D. Gupta and H. Saran, “NFC Secure Element-Based Mutual Authentication and Attestation for IoT Access,” *IEEE Transactions on Consumer Electronics*, vol. 64, no. 4, pp. 470-479, 2018. Article (CrossRef Link).

[10] D. Sethia, D. Gupta, H. Saran, R. Aggarwal, and A. Gaur, "Mutual Authentication Protocol For Secure NFC Based Mobile Healthcard," *IADIS International Journal on Computer Science & Information Systems*, vol. 11, no. 2, pp. 195-202, 2016.

[11] A. Al-Haj and M. Al-Tameemi, "Providing security for NFC-based payment systems using a management authentication server," in *Proc. of 2018 4th International Conference on Information Management (ICIM)*, 2018. Article (CrossRef Link).

[12] C. Thammarat, "Efficient and Secure NFC Authentication for Mobile Payment Ensuring Fair Exchange Protocol," *Symmetry*, vol. 12, no. 10, p. 1649, 2020. Article (CrossRef Link).

[13] S. Ahamad and A. Pathan, "Trusted service manager (TSM) based privacy-preserving and secure mobile commerce framework with formal verification," *Complex Adaptive Systems Modeling*, vol. 7, no. 1, 2019. Article (CrossRef Link).

[14] S. Bojjagani, V. N. Sastry, C.-M. Chen, S. Kumari, and M. K. Khan, "Systematic survey of mobile payments, protocols, and Security Infrastructure," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 609-654, 2023. Article (CrossRef Link).

[15] C. J. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols," in *Proc. of 20th International Conference on Computer-Aided Verification (CAV'08)*, pp. 414–418, 2008. Article (CrossRef Link)

[16] C. Cremers and S. Mauw, "Operational semantics," *Operational Semantics and Verification of Security Protocols*, pp. 13–35, 2012. Article (CrossRef Link)

[17] D. G. Duguma, J. Kim, S. Lee, N.-S. Jho, V. Sharma, and I. You, "A Lightweight D2D security protocol with request-forecasting for next-generation mobile networks," *Connection Science*, vol. 34, pp. 362-386, 2022. Article (CrossRef Link).

[18] S. Szymoniak, "Amelia—A new security protocol for protection against false links," *Computer Communications*, Vol. 179, pp. 73-81, 2021. Article (CrossRef Link).

[19] X. Zheng, L. Yang, J. Ma, G. Shi, and D. Meng, "TrustPAY: Trusted mobile payment on security-enhanced ARM TrustZone platforms," in *Proc. of 2016 IEEE Symposium on Computers and Communication (ISCC)*, pp. 456-462, 2016. Article (CrossRef Link).

[20] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128-143, Feb. 2006. Article (CrossRef Link).

[21] Tafti, Forough Sadat, et al., "A New NFC Mobile Payment Protocol Using Improved GSM Based Authentication," *Journal of Information Security and Applications*, vol. 62, p. 102997, 2021.Article (CrossRef Link).

[22] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava and M. Abdallah, "B-Ride: Ride Sharing With Privacy-Preservation, Trust and Fair Payment Atop Public Blockchain," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1214-1229, 1 April-June 2021. Article (CrossRef Link).

[23] S. S. Ahamad, "A Novel NFC-Based Secure Protocol for Merchant Transactions," *IEEE Access*, vol. 10, pp. 1905-1920, 2022. Article (CrossRef Link).

Ali M. Allam received his Ph.D. degree in Communication Engineering from Helwan University in 2008. From 2016 to current works as associated professor in the communication department in Helwan University. His research interests include wireless communication, network security, and cryptography.