An Improvement of A Lightweight NFC Authentication Algorithm Based on Modified Hash Function

Min-Shiang Hwang
Department of Computer Science and Information Engineering
Asia University
Wufeng, Taichung 354, Taiwan (R.O.C.)
Email: mshwang@asia.edu.tw

Hou-Wen Li
The Ph.D. Program in Artificial Intelligence
Asia University
Wufeng, Taichung 354, Taiwan (R.O.C.)
Email: g935151@gmail.com

Cheng-Ying Yang*
Department of Computer Science
University of Taipei
Taipei, Taiwan (R.O.C.)
Email: cyang@utaipei.edu.tw
*Corresponding author: Prof. Cheng-Ying Yang

***Abstract*—In NFC applications, user privacy information must be protected first. Cao and Liu recently proposed a lightweight NFC authentication scheme based on an improved hash function to ensure that the user's private information will not be leaked. Although their method is highly efficient and has Mutual Authentication, Forward Security, Backward Security, and security against attacks such as Replay, Location, and Fake, once out of synchronization occurs, the method must re-establish synchronization data. Therefore, this article will propose a lightweight synchronization method.**

***Index Terms*—authentication algorithm, hash function, near field communication, privacy**

I. INTRODUCTION

The low cost of electronic tags in RFID systems, RFID is thus widely used in daily life [14], [19], [22]. However, limited by the computing power of electronic tags, RFID cannot perform complex cryptographic algorithms to protect user privacy information [6], [10], [15], [16]. To improve both the computing power of tags and protect users' privacy information, NFC technology is a feasible solution. Near Field Communication (NFC) can read information stored in objects at short distances without touching the object [12], [13], [20].

The communication of NFC is the same as that of RFID technology [18], [23]. The main difference between NFC and RFID is that the user equipment that stores information in the NFC device is no longer a simple tag but a mobile device with more computing capabilities, such as a mobile cell phone [4], [11]. Mobile cell phones have both high data storage capabilities and powerful computing [8]. In addition, they can perform en/decryption algorithms based on traditional cryptographic algorithms to protect user privacy information [2]. Therefore, mobile cell phones can use as traditional RFID tags and bring users great convenience [3], [7]. For example, users can produce the applications of electronic label records such as bus and bank cards on their mobile cell phones, reducing the number of items users carry when going out [9], [17], [21].

The paper is structured as follows. We then review the Cao-Liu scheme [1] in Section II. Section III proposes a lightweight NFC authentication algorithm based on an improved Cao-Liu scheme. Finally, we conclude the entire paper in Section IV.

Identify applicable funding agency here. If none, delete this.

II. REVIEW ON CAO-LIU SCHEME

In this section, we will briefly review the Cao-Liu NFC authentication scheme [1]. There are two entities in the NFC authentication scheme: S (The server and reader) and T (The mobile devices, cell phones, etc.). Their scheme can be divided into two stages: the initialization and the authentication stages. After the initialization stage, the server (S) will store the information $(K, K_{old}, K_{new}, T_{IDS}, T_{ID})$. In initial, $K_{old} = K_{new} = K$. The mobile device (MD) will store the information (K, T_{IDS}, T_{ID}).

The steps of the authentication stage of the Cao-Liu scheme are described as follows.

Step 1. The server S sends a start session command, ASK, to T.

Step 2. After receiving the ASK, the mobile device (T) sends its anonymous ID or pseudonym T_{IDS} to S as a response.

Step 3. After S receives the message, S looks out T_{IDS} in database. If T_{IDS} does not in the database, the T_{IDS} is fabricated. S will stop the authentication. If T_{IDS} does in the database, S will take the mobile device identity (T_{ID}) and generates a random number r_S. Next, S computes B and D as follows:

$$B = r_S \oplus T_{ID},$$
$$D = h(r_S, T_{ID}).$$

S sends (B, D) to the mobile devise T.

Step 4. After receiving (B, D), the mobile device T will derive the random number r_S:

$$r'_S = B \oplus T_{ID},$$

And verifies D as follows:

$$D \stackrel{?}{=} h(r'_S, T_{ID}).$$

If the above equation does not hold, the (B, D) was fabricated. Otherwise, the $r_S = r'_S$ and the (B, D) sent by the server S are correct. Next, the mobile device (T) generates a random number r_T and computes E and F as follows:

$$E = (r_S \& T_{ID}) \oplus r_T,$$
$$F = h(r_S \oplus K, K).$$

Here, & denotes a bitwise sum operation.

Step 5. After S receives the message, S derives and contains r_T as follows:

$$r_T = E \oplus (r_S \& T_{ID}).$$

Next, S identifies the K is K_{old} or K_{new} as follows: If $F = h(r_T \oplus K_{old}, K_{old})$, the K is K_{old}. In this case, the S will renews and updates K_{new} and T_{IDS}^{new} in database:

$$K_{new} = h(K_{old}, r_R \& r_T),$$
$$T_{IDS}^{new} = h(T_{IDS}, r_R \& r_T).$$

If $F = h(r_T \oplus K_{new}, K_{new})$, the K is K_{new}. In this case, the S will renews and updates K_{new} and T_{IDS}^{new} in database:

$$K_{old} = K_{new},$$
$$K_{new} = h(K_{new}, r_R \& r_T),$$
$$T_{IDS}^{new} = h(T_{IDS}, r_R \& r_T).$$

Next, S computes $M = (r_S, r_T)$ and sends M to the mobile device.

Step 6. After T receives M, T verifies M by $M' = h(r_S, r_T)$. If $M = M'$, T renews and updates K_{new} and T_{IDS}^{new} in database:

$$K_{new} = h(K, r_R \& r_T),$$
$$T_{IDS}^{new} = h(T_{IDS}, r_R \& r_T).$$

III. The Improved of Cao-Liu Scheme

In this section, we will show the weakness of Cao-Liu scheme and the improvement of a lightweight NFC authentication scheme based on a modified hash function.

A. The Weakness of Cao-Liu Scheme

The main weakness of the Cao-Liu scheme is that it fails to synchronize the new pseudonym T_{IDS}. As a result, once the attacker interrupts the transmission data in Step 5, accidental disconnection or other factors result in T not receiving $M = (r_S, r_T)$. In this case, T will not update K_{new} and T_{IDS}^{new} in the database. Therefore, T will have no new anonymous ID T_{IDS}^{new} to send to S as a response in Step 2 in the next authentication stage.

B. The Improved Cao-Liu Scheme

In this section, we will propose an improvement of Cao-Liu NFC authentication scheme. There are also two entities in the NFC authentication scheme: S (The server and reader) and T (The mobile devices, cell phones, etc.). There are two stages in the proposed scheme: The initialization and the authentication stages. After the initialization stage, the server (S) will store the information $(K, K_{old}, K_{new}, T_{IDS}^{old}, T_{IDS}^{new}, T_{ID})$. In initial, $K_{old} = K_{new} = K$ and $T_{IDS}^{old} = T_{IDS}^{new}$. The mobile device (MD) will store the information (K, T_{IDS}, T_{ID}).

The steps of the authentication stage of the proposed scheme are shown in Figure 1 and described as follows.

Step 1. The server S sends a start session command message ASK to T.

Step 2. After receiving ASK, the mobile device T sends its anonymous ID or pseudonym T_{IDS} to S as a response.

Step 3. After S receives the message, S looks out T_{IDS} in the database. If T_{IDS} does not match T_{IDS}^{old} or T_{IDS}^{new} in the database, the T_{IDS} is fabricated. S will stop the authentication. If T_{IDS} does in the database, S will take the mobile device identity (T_{ID}) and generates a random number r_S. Next, S computes B and D as follows:

$$B = r_S \oplus h(T_{ID}),$$
$$D = h(r_S, T_{ID}).$$

Here, $h(\cdot)$ denotes a one hash function with the length of r_S.

If $T_{IDS} = T_{IDS}^{old}$, the S will renews and updates T_{IDS}^{new} in database:

$$T_{IDS}^{new} = h(T_{IDS}, r_S).$$

If $T_{IDS} = T_{IDS}^{new}$, the S will renews and updates T_{IDS}^{old} and T_{IDS}^{new} in database:

$$T_{IDS}^{old} = T_{IDS}^{new}$$
$$T_{IDS}^{new} = h(T_{IDS}, r_S).$$

Next, S sends (B, D) to the mobile devise T.

Step 4. After receiving (B. D), T will derive the random number r_S:

$$r'_S = B \oplus h(T_{ID}),$$

And verifies D as follows:

$$D \stackrel{?}{=} h(r'_S, T_{ID}).$$

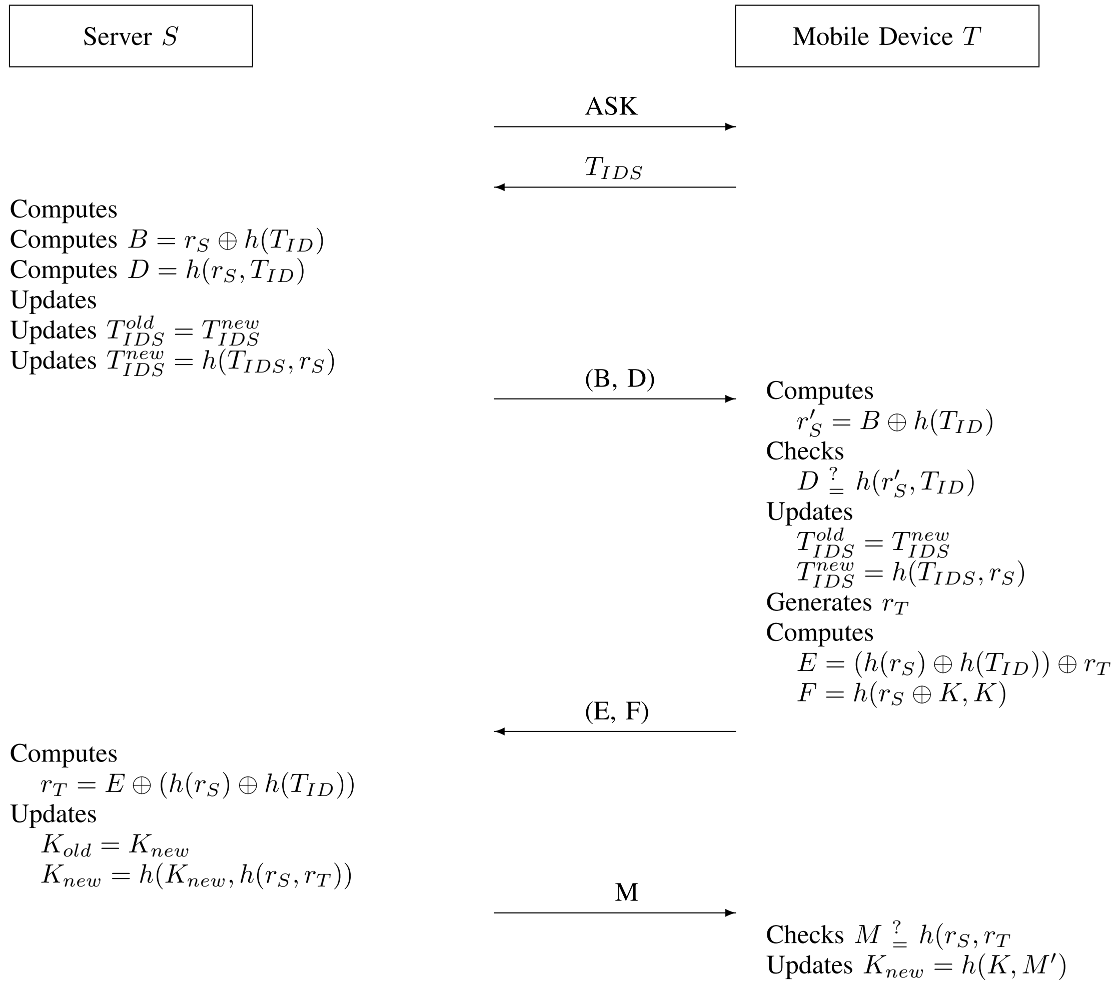

Fig. 1. The authentication stage of the proposed scheme

If the above equation does not hold, the (B, D) was fabricated. Otherwise, the $r_S = r'_S$ and the (B, D) was send by the server S are correct. The mobile device (T) will renews and updates T_{IDS}^{old} and T_{IDS}^{new} in database:

$$
\begin{aligned}
T_{IDS}^{old} &= T_{IDS}^{new} \\
T_{IDS}^{new} &= h(T_{IDS}, r_S).
\end{aligned}
$$

Next, T generates a random number r_T and computes E and F as follows:

$$
\begin{aligned}
E &= (h(r_S) \oplus h(T_{ID})) \oplus r_T, \\
F &= h(r_S \oplus K, K).
\end{aligned}
$$

Next, T sends (E, F) to the server S.

Step 5. After S receives the message, S derives and contains r_T as follows:

$$r_T = E \oplus (h(r_S) \oplus h(T_{ID})).$$

Next, S identifies the K is K_{old} or K_{new} as follows: If $F = h(r_T \oplus K_{old}, K_{old})$, the K is K_{old}. In this case, the S will renews and updates K_{new} in database:

$$K_{new} = h(K_{old}, h(r_S, r_T)),$$

If $F = h(r_T \oplus K_{new}, K_{new})$, the K is K_{new}. In this case, the S will renews and updates K_{new} in database:

$$
\begin{aligned}
K_{old} &= K_{new}, \\
K_{new} &= h(K_{new}, h(r_S, r_T)).
\end{aligned}
$$

Next, S computes $M = h(r_S, r_T)$ and sends M to the mobile device.

Step 6. After T receives M, T verifies M by $M' = h(r_S, r_T)$. If $M = M'$, T renews and updates K_{new} in database:

$$K_{new} = h(K, M').$$

IV. Conclusion

In this article, we have shown the weakness of the lightweight NFC authentication scheme by Cao-Liu [1]. The main weakness of Cao-Liu's scheme is that it fails to synchronize the new pseudonym T_{IDS}. To against the above weakness, we propose improving Cao-Liu's lightweight NFC authentication scheme.

Acknowledgment

The Ministry of Science and Technology partially supported this research, Taiwan (ROC), under contract no.: MOST 109-2221-E-468-011-MY3 and MOST 111-2622-8-468-001 -TM1.

References

[1] F. M. Cao, D. W. Liu, "A Lightweight NFC Authentication Algorithm Based on Modified Hash Function," *International Journal of Network Security*, vol. 24, no. 3, pp. 436-443, 2022.

[2] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.

[3] Y. C. Chen, W. L. Wang, M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection", in *The 9th International Conference on Advanced Communication Technology*, pp. 255-259, 2007.

[4] Y. L. Chi, C. H. Chen, I. C. Lin, M. S. Hwang, "The Secure Transaction Protocol in NFC Card Emulation Mode," *International Journal of Network Security*, vol. 17, no. 4, pp. 431-438, 2015.

[5] T. H. Feng, M. S. Hwang, and L. W. Syu, "An authentication protocol for lightweight NFC mobile sensors payment," *Informatica*, vol. 27, no. 4, pp. 723–732, 2016.

[6] Y. Y. Hsieh, L. H. Chang, A. Y. H. Liao, C. Y. Yang, and M. S. Hwang, "The System Adoption Evaluation of RFID Safety Management System on Campus," *International Journal of Network Security*, vol. 24, no. 1, pp. 176-180, 2022.

[7] M. S. Hwang, C. H. Wei, C. Y. Lee, "Privacy and security requirements for RFID applications", *Journal of Computers*, vol. 20, no. 3, pp. 55–60, Oct. 2009.

[8] M. S. Hwang and W. P. Yang, "Conference key distribution protocols for digital mobile communication systems", *IEEE Journal on Selected Areas in Communications*, vo1. 13, no. 2, pp. 416-420, Feb. 1995.

[9] C. H. Lee, M. S. Hwang, W. P. Yang, "A novel application of the phone card and its authentication in mobile communications", *Journal of Information Science and Engineering*, vol. 15, no. 4, pp. 471-484, 1999.

[10] Y. Z. Li, W. T. Zuo, and D. W. Liu, "Tag Group Coexistence Protocol for Verifiable RFID System," *International Journal of Network Security*, vol. 24, no. 6, pp. 1056-1063, 2022.

[11] J. Ling, Y. Wang, W. Chen, "An Improved Privacy Protection Security Protocol Based on NFC," *International Journal of Network Security*, vol. 19, no. 1, pp. 39-46, 2017.

[12] Y. Ma, "NFC Communications-based Mutual Authentication Scheme for the Internet of Things," *International Journal of Network Security*, vol. 19, no. 4, pp. 631-638, 2017.

[13] Z. Wang, W. Wang, J. Zhang, and T. Yang, "NFC-Defender: SVM-based Attack Detection on NFC-enabled Mobile Device," *International Journal of Network Security*, vol. 23, no. 3, pp. 379-385, 2021.

[14] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "A secure privacy and authentication protocol for passive RFID tags," *International Journal of Mobile Communications*, vol. 15, no. 3, pp. 266–277, 2017.

[15] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "Security analysis of an enhanced mobile agent device for RFID privacy protection," *IETE Technical Review*, vol. 32, no. 3, pp. 183–187, 2015.

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

[17] C. H. Wei, M. S. Hwang, Augustin Y. H. Chin, "An authentication protocol for low-cost RFID tags", *International Journal of Mobile Communications*, vol. 9, no. 2, pp. 208–223, 2011.

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

[19] C. H. Wei, CY Yang, and M. S. Hwang, "Cryptanalysis of the Serverless RFID Authentication and Search Protocols," *Advances in Intelligent, Interactive Systems and Applications*, vol. 885, 2019.

[20] Y. Wei and J. Chen, "Tripartite Authentication Protocol RFID/NFC Based on ECC," *International Journal of Network Security*, vol. 22, no. 4, pp. 664-671, 2020.

[21] H. J. Wu, Y. H. Chang, M. S. Hwang, I. C. Lin, "Flexible RFID location system based on artificial neural networks for medical care facilities", *ACM SIGBED Review*, vol. 6, no. 2, pp. 1-8, 2009.

[22] S. H. Xu, D. W. Liu, and W. T. Zuo, "A Mobile RFID Authentication Protocol Based on Self-assembling Cross-bit Algorithm," *International Journal of Network Security*, vol. 25, no. 1, pp. 1-9, 2023.

[23] S. H. Zhan and C. Q. Yu, "Mobile RFID Authentication Protocol Based on Permutation Cross Synthesis for Anti Counterfeit Attack," *International Journal of Network Security*, vol. 24, no. 2, pp. 305-313, 2022.