ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-201901.00172

Lightweight RFID Mutual Authentication Protocol Resistant to Desynchronization Attacks (Postprint)

Authors: Liu Yi, Chen Tianxiao, Hongzhou

Date: 2019-01-28T00:00:00+00:00

Abstract

To address the issue of insufficient security in existing RFID authentication protocols arising from design flaws during the security authentication process, this paper proposes a lightweight RFID authentication protocol enhanced with synchronized random numbers and PUF. First, a desynchronization attack method against RFID protocols is presented, and its underlying causes are analyzed. Subsequently, by establishing a synchronized random number at both the tag and reader ends, the protocol' s resistance to desynchronization attacks is strengthened. Finally, PUF is incorporated into the tag, leveraging the unclonability of PUF to enhance the attack resilience of the tag' s secret key. The analysis results indicate that the proposed protocol can effectively withstand various attacks while achieving higher security with reasonable efficiency and overhead.

Full Text

Preamble

Vol. 37 No. 4
Application Research of Computers
ChinaXiv Partner Journal

Lightweight RFID Two-Way Authentication Protocol with Anti-Synchronization Attack

Liu Yi[1], Chen Tianxiao[1], Hong Zhou[2]
(1. School of Computer Science & Technology, Guangdong University of Technology, Guangzhou 510006, China;
2. Office of Academic Research, Guangzhou City Polytechnic, Guangzhou 510405, China)

Abstract: Existing RFID authentication protocols suffer from insufficient security due to design flaws in their security authentication processes. This paper proposes an improved lightweight RFID authentication protocol utilizing synchronized random numbers and Physical Unclonable Functions (PUF). First, we present a desynchronization attack method against RFID protocols and analyze its root causes. Then, we enhance the protocol' s resistance to desynchronization attacks by establishing a synchronized random number at both the tag and reader ends. Finally, we introduce PUF into the tag, leveraging its unclonability to improve the tag' s key resistance against attacks. Analysis results demonstrate that the new protocol can effectively resist multiple attack vectors while maintaining higher security with acceptable efficiency and overhead.

Keywords: RFID; lightweight; physical unclonable function; mutual authentication; CRC

0 Introduction

Radio Frequency Identification (RFID), also known as wireless radio frequency identification, is a non-contact recognition technology that can identify specific targets and read/write relevant data via radio signals without physical contact. RFID has been widely applied in numerous fields such as logistics, military, and transportation. An RFID system typically consists of three components: tags, readers, and a backend database. The communication channel between the backend database and reader is generally considered secure and reliable [1]. However, the channel between reader and tag uses wireless connections that lack protection, making it extremely vulnerable to eavesdropping and spoofing.

With the development of RFID technology, security concerns have received increasing attention. Designing a secure RFID authentication protocol is crucial for safeguarding RFID systems. RFID tags require low-cost implementation, resulting in limited computational capabilities. Traditional public-key cryptographic algorithms such as RSA are unsuitable for RFID protocols. Consequently, designing secure, low-cost, and efficient lightweight RFID authentication protocols has become a prominent research focus.

Maintaining the lightweight nature of RFID tags is essential. References [2,3] applied traditional cryptographic tools to RFID protocols. While these approaches offered good security, they failed to consider the limited computational power of tags. Reference [2] proposed a hash function and timestamp-based authentication protocol that used timestamps to prevent replay attacks but did not optimize the hash function, leading to excessive computational costs for tags. Reference [3] presented a lightweight protocol based on CRC and pseudo-random number generators, which used CRC' s one-way property for encryption during message transmission and cross-combined the high bits of one message with the low bits of another. However, the tag employed a pseudo-random number generator, which proved inefficient due to the computational limitations of RFID

tags.

To reduce tag costs and improve efficiency, early ultralightweight RFID authentication protocols employed simple operational functions and authentication steps, which improved efficiency but compromised security. Chien' s SASI protocol introduced Rot shift operations in the authentication process [4], but reference [5] subsequently identified DoS and tag tracking attacks against SASI. Reference [6] proposed the Gossamer protocol based on SASI with a similar structure, introducing MixBits operations in the key update phase to enhance security. However, Zeeshan demonstrated desynchronization attacks and other security vulnerabilities against this protocol in reference [7]. Tian et al. proposed an ultralightweight authentication protocol RAPP in 2012 [8], though Eyad et al. later identified a synchronization attack against RAPP in reference [9]. Reference [10] subsequently improved RAPP by proposing the PAPP protocol, which used the one-way property of the tag' s encryption algorithm to generate random numbers and prevent desynchronization attacks. This approach shared gate circuits within the tag, reducing overhead compared to direct random number generators.

The protocols in references [4-6,8,10] suffered from security issues due to their excessive simplicity. In reference [11], Zhang et al. conducted a detailed analysis of the protocol cycles and security strength of these ultralightweight authentication protocols, revealing that they employed overly simple operations with low complexity and weak attack resistance. They subsequently proposed an M-Hash function-based authentication protocol (MH protocol) featuring low hardware resource requirements and strong collision resistance. In the MH protocol, Zhang et al. also improved efficiency by reducing the logical operation bits of M-Hash. While their protocol achieved a balance between security and efficiency, M-Hash still required numerous gate circuits for implementation.

Yang proposed a new lightweight authentication protocol in reference [12] that employed CRC and cross-bit operations (Cro). This protocol exhibited extremely low computational and communication overhead, making it highly suitable for lightweight RFID systems. However, analysis revealed that the protocol could not resist desynchronization attacks, and relying solely on simple operations like CRC and Cro for key updates provided insufficient security.

To address the security issues in reference [12], this paper combines a synchronized random number and Physical Unclonable Function (PUF) to improve upon that protocol, proposing a new lightweight authentication protocol that maintains low cost while achieving higher security. A Physical Unclonable Function (PUF) is a function that maps input values to response values using physical characteristics [13]. PUF exhibits unclonability—each input yields a unique and unpredictable output, with different PUFs producing different outputs for the same input.

1.1 Symbol Description

- K_i^{old}: Shared key between tag and reader from previous round (i=1,2)
- K_i^{new}: Shared key between tag and reader for current round (i=1,2)
- ID: Tag' s real identity
- TID_{old}: Tag' s temporary identity from previous round
- TID_{new}: Tag' s temporary identity for current round
- N_i: Random numbers generated by reader (i=1,2)
- r_n: Initial synchronized random number between reader and tag
- A-E: Exchange messages between reader and tag
- $\oplus$: Bitwise XOR operation
- $Cro(X, Y)$: Cross-bit operation
- CRC-16(X): Cyclic redundancy check function for encrypting value X
- (G_n, G_{n+1}): Initial PUF verification pair
- $PUF(X)$: Random permutation function (implemented through PUF)

1.2 Description of Yang' s Protocol

Yang' s protocol is illustrated in Figure 1. The primary reason Yang' s protocol suffers from security issues is that within a certain period before tag updates, the response messages for every A and B message remain identical. This situation also enables tracking attacks. An attacker can block tag key updates during each authentication and subsequently send the same previous messages A and B to obtain identical responses, thereby achieving tracking attacks.

The typical improvement for such security issues involves adding a random number generator. Reference [14]' s protocol exhibited similar desynchronization problems, and reference [15] improved it using a random number generator. Although this approach utilized part of the encryption algorithm to generate random numbers, it still incurred certain computational overhead. This section improves upon Yang' s protocol using synchronized random numbers and Physical Unclonable Functions (PUF), proposing a new lightweight protocol.

---

2 New Protocol

The symbol definitions remain consistent with Section 1.1. The new protocol is illustrated in Figure 2 [Figure 2: see original paper].

Initialization Phase: The reader holds pre-generated PUF verification pairs (G_n, G_{n+1}), keys K_1, K_2, and synchronized random number r_n. The tag holds $\{ID, TID, K_1, K_2, r_n\}$.

Protocol Process:

1. **Hello:** The reader initiates authentication by sending a "Hello" signal to the tag, commencing the protocol authentication process.

2. **TID:** Upon receiving the request, the tag sends its temporary identity TID to the reader. The reader forwards this TID to the backend database for lookup. If a matching TID is found, the backend database sends the corresponding keys K_i to the reader, and the tag and reader enter the mutual authentication phase. If the TID does not exist in the database, authentication fails and must restart.

3. **A and B:** During mutual authentication, the reader generates two random numbers N_1, N_2, computes A and B, and sends them to the tag to request PUF-based verification. After sending, the reader computes $r_{n+1} = CRC(r_n \oplus N_1)$. The tag extracts G_n from A using keys K_1, K_2 for subsequent PUF computation, then computes random number N_1 from B using K_1, K_2, G_n.

4. **R and C:** The tag uses the $PUF()$ function with the received G_n to compute $PUF(G_n)$ and obtain G_{n+1}, then computes $G_{n+2} = PUF(G_{n+1})$ and $r_{n+1} = CRC(r_n \oplus N_1)$. Using keys K_1, K_2, random numbers $N_1, r_{n+1}, G_{n+1}, G_{n+2}$, the tag computes R and C and sends them to the reader. The reader first extracts G_{n+1} from R and compares it with its own G_{n+1}. If they match, the reader successfully authenticates the tag; otherwise, authentication fails.

5. **D and E:** The reader computes D and E using the previously generated random number N_2 and sends them to the tag. The tag extracts N_2 from D, computes E', and compares it with E. If they match, the tag successfully authenticates the reader, confirming that the reader possesses G_{n+2} and the correct r_{n+1}. The tag then updates its keys using random numbers N_1, N_2 and $r_{n+1}, G_{n+1}, G_{n+2}$, concluding the protocol. If they do not match, authentication fails and keys are not updated.

Update Operations: After successful authentication, the reader uses $K_1, K_2, N_1, r_{n+1}, G_{n+1}$ to compute G_{n+2} from C. The pair (G_{n+1}, G_{n+2}) serves as the PUF verification pair for the next round of reader authentication and tag verification, after which the reader updates its keys.

The new protocol resists desynchronization attacks by synchronizing a random number between tag and reader without requiring the tag to transmit it, thereby reducing communication overhead. PUF usage enhances protocol security—even if an attacker obtains (G_n, G_{n+1}) in a given round, they cannot reverse-engineer previously used verification pairs or derive future ones, making tag authentication more secure than previous CRC-based key updates.

---

3 Security Analysis

This section analyzes the improved protocol' s security across eight dimensions: impersonation attacks, information leakage attacks, tracking attacks, cloning attacks, replay attacks, desynchronization attacks, forward/backward security, and mutual authentication. We also demonstrate why the new protocol resists the previously described desynchronization attack.

1) Impersonation Attack
An impersonation attack occurs when an attacker poses as a tag or reader to obtain useful authentication information. In the improved protocol, any modification is detectable by both tag and reader because K_i, N_1, N_2, r_{n+1}, and PUF-generated verification pairs all change dynamically. Each protocol step enables mutual verification, and attackers lacking the appropriate K_i and verification pairs cannot complete full authentication. At best, an attacker might obtain TID, which is merely a temporary identity that changes after each successful authentication round and holds no practical value. Thus, the protocol resists impersonation attacks.

2) Information Leakage Attack
Information leakage attacks involve attackers modifying messages from the reader to extract protocol information from tag responses [13]. Since every step in this protocol is encrypted or randomized, and all values $N_1, N_2, r_{n+1}, G_{n+1}, G_{n+2}$ are transmitted using CRC and Cro encryption, both reader and tag verify each received message. If verification fails, the protocol terminates. Therefore, any attempt to modify protocol information will be detected, causing protocol termination. The protocol thus resists information leakage attacks.

3) Tracking Attack
The protocol exclusively uses the tag' s temporary TID as its identity identifier throughout, never revealing the tag' s real ID. Consequently, attackers cannot obtain the tag' s true identity from intercepted protocol content and cannot track the ID. If an attacker attempts to track a captured TID, they will fail because TID is updated each round using random numbers N_1, N_2 and G_{n+1}. The protocol therefore resists tracking attacks.

4) Cloning Attack
Against cloning attacks, this protocol employs PUF-generated verification pairs for reader authentication each round. Due to PUF' s unclonable nature, attackers cannot forge an identical PUF to that in the tag and cannot clone a tag containing a legitimate PUF. The protocol thus resists cloning attacks.

5) Replay Attack
Upon successful protocol completion, keys K_i, synchronized random number r_n, and TID all change in both reader and tag. If an attacker impersonates a reader to conduct a replay attack by first replaying "Hello," the tag returns an updated TID. Replaying previous round' s messages A, B will fail because

the keys K_i within them no longer correspond to the updated TID. Even if attackers intercept previous authentication information, replay attacks cannot succeed. The protocol therefore resists replay attacks.

6) Desynchronization Attack
The improved protocol resists the previously described desynchronization attack through a synchronized random number r_n shared between tag and reader. During each round' s third step, the reader computes a new $r_{n+1} = CRC(r_n \oplus N_1)$. When the tag receives the reader' s request, it computes the same r_{n+1}, ensuring that message C differs each round and granting the new protocol desynchronization resistance.

Under the previous desynchronization attack scenario:
a) During the n-th authentication, block protocol step 5 so the reader updates keys and temporary identity TID while the tag does not. The reader holds $(TID_{n+1}^{new}, TID_n^{old}, K_i^{new}, K_i^{old}, G_{n+1}, G_{n+2}, r_{n+1}, ID)$, while the tag holds $(TID_n^{old}, ID, r_{n+1})$. The attacker eavesdrops on messages $Hello_n$, $A||B_n$, C_n, R_n, $D||E_n$. At this point, tag and reader can still mutually authenticate.

b) During the $(n+1)$-th authentication, again block step 5. The reader holds $(TID_{n+2}^{new}, TID_n^{new}, K_i^{old}, K_i^{new}, G_{n+2}, G_{n+3}, r_{n+2}, ID)$, while the tag holds $(TID_n^{new}, K_i^{old}, K_i^{new}, ID, r_{n+2})$.

c) Replay the messages from step 1: The reader sends $Hello_n$, the tag returns its TID_n^{old}, then sends $A||B_n$. However, unlike before, the tag' s response incorporates the new synchronized random number r_{n+3}. When the attacker replays $D||E_n$ from step 1, E_n contains the old synchronized random number r_{n+1}, causing verification failure and protocol termination. This blocks the desynchronization attack.

7) Forward and Backward Security
Even if an attacker obtains keys K_i, G_n, G_{n+1} from a specific round, they cannot continuously track the tag. After several authentications, the tag and reader will have updated K_i, G_n, G_{n+1} and other information, rendering previously obtained keys and verification pairs useless. The key update process uses CRC, Cro, random numbers N_1, N_2, r_{n+1}, and G_{n+1}, G_{n+2} to compute new keys, preventing attackers from deriving future keys from current ones, thus ensuring forward security.

Throughout the protocol, each round' s random numbers are unpredictable, ensuring all messages differ per authentication round. Attackers cannot reverse-engineer previous verification pairs like G_{n+1} from G_{n+2}. Therefore, attackers cannot use information obtained from current attacks to deduce previous protocol authentication messages, guaranteeing backward security.

8) Mutual Authentication
The new protocol achieves mutual authentication between reader and tag. The reader authenticates the tag' s legitimacy using its generated random numbers $TID, N_1, (G_n, G_{n+1})$ and keys K_i, while the tag verifies the reader' s legitimacy

using its PUF-computed G_{n+1}, r_{n+1} and keys K_i, satisfying mutual authentication requirements.

Table 1 compares the new protocol with Yang' s protocol, where Y indicates resistance to an attack and N indicates vulnerability. The new protocol demonstrates significantly higher security than Yang' s protocol.

---

4 Performance Analysis

This section discusses the new protocol' s performance in terms of tag computational operations, storage space, and communication cost. Assuming all messages in the protocol have length L:

Computational Cost: Compared with the original protocol, the new protocol adds one PUF operation in addition to CRC, Cro, and $\oplus$ operations. All four operations are lightweight with minimal computational overhead, easily implementable in tags. The protocol places the more expensive random number generation on the reader side, improving computational efficiency.

Storage Requirements: The new protocol reduces one key K_i due to PUF introduction but requires storing a synchronized random number. Tags must store $\{ID, TID, r_n, K_1, K_2\}$, maintaining the same storage volume of $5L$.

Communication Cost: The new protocol transmits one TID and messages R and C during a complete authentication process, totaling $3L$ communication overhead.

Table 2 compares the new protocol with other algorithms.

---

5 Conclusion

Since its inception, RFID technology has faced numerous security challenges. This paper analyzed security deficiencies in Yang' s lightweight RFID protocol and proposed an improved protocol using Physical Unclonable Functions (PUF). Analysis demonstrates that compared with the original protocol, the new protocol achieves higher security while maintaining efficiency and resisting more attack vectors. In summary, the new protocol features low cost, high efficiency, and robust security, making it highly suitable for lightweight RFID systems.

References

[1] Zhou Yongbin, Feng Dengguo. Design and analysis of cryptographic protocols for RFID [J]. Chinese Journal of Computers, 2006, 29 (4): 581-589.

[2] Yu Wenjin, Jiang Yixiang. Mobile RFID mutual authentication protocol based on hash function [C]// Proc of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Piscataway, NJ: IEEE Press, 2017: 358-361.

[3] Shi Zhicai, Chen Jiwei, Chen Shanshan, et al. A lightweight RFID authentication protocol with confidentiality and anonymity [C]// Proc of the 2nd IEEE Advanced Information Technology, Electronic and Automation Control Conference. Piscataway, NJ: IEEE Press, 2017: 1340-1344.

[4] Chien H Y. SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity [J]. IEEE Trans on Dependable and Secure Computing, 2007, 4 (4): 337-340.

[5] Cao Tianjie, Bertino E, Lei Hong. Security analysis of the SASI protocol [J]. IEEE Trans on Dependable and Secure Computing, 2009, 6 (1): 73-77.

[6] Peris-Lopez P, Hernandez-Castro J C, Tapiador J M. et al. Advances in ultralightweight cryptography for low-cost RFID tags: gossamer protocol [C]// Proc of the 9th International Workshop on Information Security Applications. Springer-Verlag, 2009: 56-58.

[7] Bilal Z, Masood A, Kausar F. Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: gossamer protocol [C]// Proc of International Conference on Network-Based Information Systems. Piscataway, NJ: IEEE Press, 2009: 260-267.

[8] Tian Yun, Chen Gongliang, Li Jianhua. A new ultralightweight RFID authentication protocol with permutation [J]. IEEE Communications Letters, 2012, 16 (5): 702-705.

[9] Taqieddin E, Sarangapani J. Vulnerability analysis of ultra-lightweight RFID authentication protocols: RAPP and gossamer [C]// Proc of the 7th International Conference for Internet Technology and Secured Transactions. Piscataway, NJ: IEEE Press, 2012: 80-86.

[10] Ma Qing, Guo Yajun, Zeng Qingjiang, et al. A new ultra-lightweight RFID mutual authentication protocol [J]. Netinfo Security, 2016 (5): 44-50.

[11] Zhang Xing, Li Chang, Han Dong, et al. Lightweight security authentication protocol for RFID based on hash functions [J]. Computer Engineering and Design, 2018, 39 (5): 1269-1275.

[12] Yang Xin, Ling Jie. Low-cost ultralightweight RFID mutual-authentication protocol [J]. Computer Science, 2016, 43 (4): 160-162.

[13] Liu Yi, Gu Guosheng. New mutual authentication for lightweight RFID protocols [J]. Computer Science, 2017, 44 (2): 206-208.

[14] Ma Yuanjia, Liu Daowei. An improved mutual authentication with backward security for RFID protocols [J]. Computer Engineering and Applications, 2017, 53 (9): 136-140.

[15] Wei Mianyu, Ou Yuyi. Improved resistance de-synchronization attack RFID security protocol [J]. Computer Engineering and Design, 2017, 38 (7): 1719-1723.

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv —Machine translation. Verify with original.