RFID Authentication Protocol Resistant to the Man-in-the-Middle Attack

Li Zhai[1,2](✉) and ChuanKun Wu[1]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences,
Beijing 100093, China
{zhaili,ckwu}@iie.ac.cn
[2] University of Chinese Academy of Sciences,
Beijing 100190, China

Abstract. HB+ family protocols that based on LPN problem are effective and well suited for the Internet of Things. However, the HB+ family protocols have vulnerability on the man-in-the-middle attack. In this paper, we propose a new privacy preserving RFID authentication protocol based on the multiplication on Z_{2^k-1}. By analyzing the differential property on Z_{2^k-1}, we show that the protocol is resistant to the man-in-the-middle attack. Moreover, the performance analysis shows the protocol meets the demands of the large-scale RFID systems.

Keywords: RFID · Man-in-the-middle attack · Privacy · Internet of Things

1 Introduction

Radio Frequency Identification (RFID) is a technology that allows RFID readers automatically identification of RFID tags, and it is widely used in many applications. But low-cost RFID tags, in particular, have limited computational capabilities that render them unable to perform complicated cryptography operations.

Privacy preserving protocols based on symmetric key are faced a paradox. On one side, a tag must encrypt its identity with its secret key so that only authorized readers can extract the identity. On the other side, a tag cannot easily identify itself to reader. If the reader does not know any identity of the tag, it cannot determine which key is used to decrypt the protocol message [10]. Therefore, most symmetric-key protocols are using exhaustive search to determine the key.

Molnar and Wagner proposed a tree based RFID authentication protocols [14]. By using their method, a tag can be identified in $O(\log N)$ time. Their method is a tradeoff between the identification efficiency and privacy. Avoine et al. [3] discovered the tree based protocols have vulnerability on compromising attack. Song and Mitchell [16] proposed a constant-time identification protocols. However, their protocol have vulnerability on impersonation and tracking

This work was supported by China national 863 project under No. 2013AA014002.

J. Tian et al. (Eds.): SecureComm 2014, Part II, LNICST 153, pp. 41–47, 2015.
DOI: 10.1007/978-3-319-23802-9_6

attack [6]. Alomair et al. [1] proposed another constant-time identification protocols. Their protocol needs pre-computation and a large database. Moreover, the protocol has vulnerability on denial of service and tracking attack.

Juels and Weis [11] proposed HB+, the first RFID lightweight authentication protocol based on the learning parity problem. HB+ protocol is provable security under LPN problem, but it has security flaw on the man-in-the-middle attack. As Gilbert et al. showed in [8], the security of HB+ is compromised if the adversary is given the ability to modify messages transmitting between the reader and the tag. Karz et al. [12] gave a simpler proof of security for HB+, and proved security for parallel executions. Beinger et al. proposed HB++ [5] protocol.

However, all these protocols were proven to be insecure in the GRS model. They were successfully cryptanalyzed by Gilbert et al. in [7]. In fact, it has been shown in [7] that the secure authentication protocols based on the LPN problem are hard to find. Gilbert et al. proposed the HB# and Random-HB# [9] on the eurocrypt'08. Their protocol enhanced the security on the man-in-the-middle attack. But later, Ouafi et al. present a man-in-the-middle attack against HB# and Random-HB# [15]. Recently, more HB-like protocols are proposed, but they were all broken. Bosley et al. [4] proposed HBN protocol, but they were successfully cryptanalyzed by Avoine et al. [2].

Our Contribution. We proposed a new RFID authentication protocol which is secure under the man-in-the-middle attack. Our protocol does not rely on any cryptography ciphers, it is constructing directly from the multiplication on Z_{2^k-1}. We developed a new pseudorandom function based on the multiplication on Z_{2^k-1}. Due to the nonlinearity of our pseudorandom function, our protocol is secure on the GRS model. And we gives the multiplicative differential property of the Z_{2^k-1}. Based on these results, it shows that our protocol is resistant to the man-in-the-middle attack. Finally, we give the performance analysis of our protocols.

2 Our Protocol

In this section, we introduce our privacy preserving authentication protocol. In Table 1, we give the symbol definition used in this paper.

Initialization. Every tag T_i in the system is initialized with a secret key (x_i, y_i), which x_i and y_i are randomly drawn from G. The N secret keys of the tags are stored in a database. The reader uses a secure connection communicating with the database.

Protocol. Our scheme is a n-round challenge response protocol. Figure 1 illustrates a round of our protocol. Each authentication consists of n rounds, where n is a security parameter. The protocol works as follows:

1. The reader first draw a random element a from G and sends it to the tag.
2. Upon the tag receipt a, it draw a random element b from G, and compute $z = f(a * x) \oplus f(b * y)$, sends (b, z) to reader.

Table 1. Symbol definition

Symbols	Descriptions
k	Security parameter, k is an integer and $2^k - 1$ is prime
r	Security parameter, the number of rounds in our protocol
N	The number of tags on the system
G	Multiplicative group on the $Z^*_{2^k-1}$
$*$	Multiplication on the $Z^*_{2^k-1}$
a, b, x, y	Elements on the group G
$\oplus$	Exclusive or operator
$[x]_i$	The i-th bit of the x binary representation (least significant bit first)
$f(x)$	$f(x) = \bigoplus_{i=1}^{k} [x]_i$

3. The reader receipt (b, z). Then reader exhaustive search the key pair (x_i, y_i), and compute $z' = f(a_i * x) \oplus f(b_i * y)$. If $z' = z$, put (x_i, y_i) into the candidates key set; otherwise exclude (x_i, y_i) immediately.

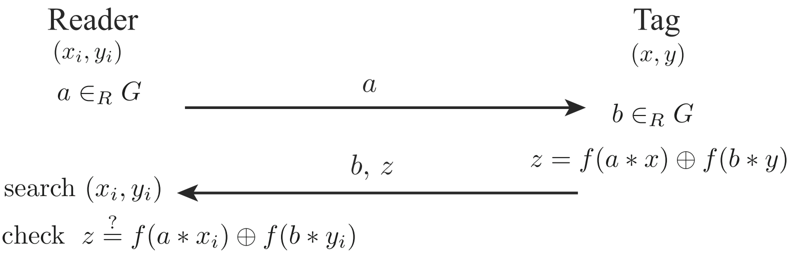
Reader
(x_i, y_i)
$a \in_R G$
a
Tag
(x, y)
$b \in_R G$
$b,\ z$
$z = f(a * x) \oplus f(b * y)$
search (x_i, y_i)
check $z \overset{?}{=} f(a * x_i) \oplus f(b * y_i)$

Fig. 1. The basic authentication step of our protocol.

By repeating for n rounds, if reader found a key passed the verification on all rounds, the reader authenticates the tag successfully. The output of the function $f(a*x)$ is balance. Thus a naive adversary can guess the correct bit of one round is 1/2, so the probability of the adversary can be authenticated by reader is 2^{-n}.

3 Security Analysis

3.1 Differential Property of the Function $f(X * a)$

In this section, we will show the differential property of the function $f(X*a)$. The resistance of the man-in-the-middle attacks is generally relied on the differential probability of pseudorandom function. If the differential probability of a function is 1/2, that function is perfectly resistance to the differential attack.

Definition 1 (δ-differential probability of the function $f(X * a)$). *Let $q = 2^k - 1$ be a prime, a, δ be two constant on Z_q^*. Let X be a random variable, X is uniformly distributed over Z_q^*. Let $*$ denote the multiplication operator on the Z_q^*.The δ-differential probability $p(a, \delta)$ of the function $f(X * a)$ is defined as*

$$p(a, \delta) \overset{def}{=} \Pr[X \in_R Z_q^* : f((X + \delta) * a \ mod \ q) \oplus f(X * a \ mod \ q) = 0]$$

Definition 2. *Let us define a mapping $\phi(a)$ from Z_{2^k-1} to a vector, where $\phi(a) = m_{a_k} m_{a_{k-1}} \ldots m_{a_1} v$. Let $\phi(a, i)$ be the i-th element of $\phi(a)$, a be a constant on Z_{2^k-1}, a_i be the i-th bit of a's binary representation. The definition of m_0, m_1, v are as follows:*

$$m_0 = \begin{pmatrix} 1 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}, m_1 = \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & 0 & 1 & 0 \end{pmatrix}, v = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

The following theorem gives the differential probability of our pseudorandom function. The computational complexity of Theorem 1 is $O(k)$.

Theorem 1 (Differential probability on the Z_{2^k-1}). *Let X be a random variable distributed uniformly over Z_q, where $q = 2^k - 1$. Let a be a constant value on Z_q. Then the differential probability $p(a, \delta)$ is*

$$\begin{aligned} &p(a, \delta) \\ &= \frac{2^k \phi(a, f(a) + 1) + 2^k \phi(a + 1, 4 - f(a + 1)) + \theta(0, a) + \theta(q, a) + \theta(q - a, a) - 3}{q - 1} \end{aligned}$$

where $\theta(x, a) = f(x + a \ mod \ 2^k) \oplus f(x \ mod \ 2^k)$.

3.2 Man-in-the-Middle Attack of Our Protocol

We assumed a man-in-the-middle adversary has the following abilities: he can fully control the messages between reader and tag; he can modify or replay the message, and look up the protocol result that is succeeded or failed. Without loss of generality, we consider the adversary modifying the message a:

1. Reader sends message a to tag.
2. Adversary intercept the message, changing a to $a' = a + \delta$, and sends a' to tag.
3. Upon tag receipt the message a' from the adversary, tag generate b uniformly at random, and compute $z' = f(a' * x) \oplus f(b * y)$, tag sends (b, z') to reader.
4. Upon receipt (b, z'), reader calculate $z = f(a * x) \oplus f(b * y)$. If $z = z'$ then reader accept the tag, otherwise reader reject the tag.
5. Adversary view the output of the reader and deduce the secret key.

The above attacking method is the famous GRS attack [8,13]. It successfully crack many HB-family protocols. Now we shows that our protocol can resistant GRS attack. According to the assumption, adversary can get the protocol result. If reader accepted tag, then adversary can conclude that $z = z'$, if reader rejected tag then $z = z' \oplus 1$. We can calculate the probability of reader accepting tag while adversary intercepting the messages:

$$\begin{aligned}
&\Pr[\text{Reader Accept Tag}] \\
=&\Pr[z = z'] \\
=&\Pr[f(a * x) \oplus f(b * y) = f(a' * x) \oplus f(b * y)] \\
=&\Pr[f(a * x) \oplus f(a' * x) = 0] \\
=&\Pr[f(a * x) \oplus f((a + \delta) * x) = 0] \qquad (1)
\end{aligned}$$

We can see the probability (1) is the differential probability defined in Definition 1. If the x and δ are fixed, the probability (1) is fixed. Thus every tag on the systems has a unique differential probability. Adversary can attack our protocol by utilizing the uniqueness of differential probability. Adversary repeats the above process to get many samples of $f(a*x) \oplus f((a+\delta)*x)$. Then he can use the maximize like hood method to approximate the differential probability (1).

For convenience, we denote the probability (1) as $2^{-1} \pm 2^{-m}$, which m is a positive value about k. By using the Theorem 1, given x, δ, we can calculate m. If we choose the key length to 127-bit($2^{127} - 1$ is a prime), then m is approximating to 40. According to the Chernoff bound, if the probability of adversary succeeded is η, then adversary needs at least n samples to approximate the differential probability, where $n \geq 2^{2m} \ln \frac{1}{\sqrt{\eta}}$. Then adversary needs $O(2^{80})$ samples to get a distinguish attack against our protocol. On the practical environment, adversary cannot get a large amount of samples, and therefore our protocol is secure against these attack.

4 Performance Analysis

In this section, we give the performance analysis of our protocol. We can proof that a reader can exclude a wrong tag within 2 rounds on average. Thus a reader identify a tag needs to run $2N$ times sub-protocol on average, where N is the number of tags on the system. The Algorithm 1 shows the identification process. n is the number of rounds of the protocol. The algorithm's input $(b_1, z_1), \ldots, (b_n, z_n)$ is an array of the tag's output.

Assuming the tag's output z_i is uniformly distributed. If the reader chooses the right key, the verification processes will success in all rounds. If the reader choose the wrong key, the probability of a wrong key passing the verification on i-round is 1/2. Then the probability of a wrong key just rejected on i-round is (i.e., passed the first $i - 1$ rounds, and rejected on i-th round):

$$p_i = \frac{1}{2^{i-1}} * \frac{1}{2} = \frac{1}{2^i}$$

Algorithm 1. SearchKey $((b_1, z_1), \ldots, (b_n, z_n))$

```
for $j = 1$ to $N$ do
  for $i = 1$ to $n$ do
    if $z_i \neq f(a_i * x_j) \oplus f(b_i * y_j)$ then
      reject key $(x_j, y_j)$ and break
    end if
  end for
  if $i = n$ then
    accept key $(x_j, y_j)$ and return $ID_j$
  end if
end for
return $ID_{error}$
```

The random variable X_i denoted the number of rounds of a wrong key excluded by reader. The random variable X denoted the number of all wrong keys excluded by reader. According to linearity of expectation, $E(X)$ is:

$$E(X) = \sum_{i=1}^{N} E(X_i) = N \sum_{i=1}^{\infty} i * p_i = 2N$$

Protocol Parameter. The basic requirement of the key length is 80-bit, otherwise the adversary can break the protocol by brute force. According to the analysis on Sect. 3.2, we choose the key length of our protocol to be 127-bit.

Computational Cost. Our protocol is based on the multiplication on the Z_{2^k-1}. We implement our pseudorandom function(127-bit) in a personal computer having Intel 2.6 GHz G1610 Celeron Dual Core processor, 4 GB RAM and Linux Debian - 64-bit operating system. By running our pseudorandom function 10^8 times, it cost 350 ms. Our protocol needs to run 2N times PRF to identify a tag on average, where N is the number of tags on the system. On a system have 10^8 tags, we needs 700 ms to identify one tag.

5 Conclusion

In this paper, we construct a new privacy preserving authentication RFID protocol that does not rely on the traditional cryptography ciphers. Our protocol is consist of multiple sub protocols, this structure can be used to speed up the process of searching key on server-side. Furthermore, we give an analysis on differential property of the multiplicative group of the Z_{2^k-1}. According to our analysis, the protocol is secure on the man-in-the-middle attack.

References

1. Alomair, B., Clark, A., Cuellar, J., Poovendran, R.: Scalable RFID systems: a privacy-preserving protocol with constant-time identification. IEEE Trans. Parallel Distrib. Syst. **23**(8), 1536–1550 (2012)

2. Avoine, G., Carpent, X.: Yet another ultralightweight authentication protocol that is broken. In: Hoepman, J.-H., Verbauwhede, I. (eds.) RFIDSec 2012. LNCS, vol. 7739, pp. 20–30. Springer, Heidelberg (2013)
3. Molnar, D., Soppera, A., Wagner, D.: A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 276–290. Springer, Heidelberg (2006)
4. Bosley, C., Haralambiev, K., Nicolosi, A.: HBN: an HB-like protocol secure against man-in-the-middle attacks. IACR Cryptology ePrint Arch. **2011**, 350 (2011)
5. Bringer, J., Chabanne, H., Dottax, E.: Hb++: a lightweight authentication protocol secure against some attacks. In: Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing. SecPerU 2006, pp. 28–33. IEEE (2006)
6. Erguler, I., Anarim, E.: Scalability and security conflict for RFID authentication protocols. Wireless Pers. Commun. **59**(1), 43–56 (2011)
7. Gilbert, H., Robshaw, M., Seurin, Y.: Good variants of HB+ are hard to find. In: Tsudik, G. (ed.) FC 2008. LNCS, vol. 5143, pp. 156–170. Springer, Heidelberg (2008)
8. Gilbert, H., Robshaw, M., Sibert, H.: Active attack against HB+: a provably secure lightweight authentication protocol. Electron. Lett. **41**(21), 1169–1170 (2005)
9. Gilbert, H., Robshaw, M., Seurin, Y.: HB#: Increasing the security and efficiency of HB+. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 361–378. Springer, Heidelberg (2008)
10. Juels, A.: RFID security and privacy: a research survey. IEEE J. Sel. Areas Commun. **24**(2), 381–394 (2006)
11. Juels, A., Weis, S.A.: Authenticating pervasive devices with human protocols. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 293–308. Springer, Heidelberg (2005)
12. Katz, J., Shin, J.S., Smith, A.: Parallel and concurrent security of the HB and HB+ protocols. J. Cryptol. **23**(3), 402–421 (2010)
13. Lyubashevsky, V., Masny, D.: Man-in-the-middle secure authentication schemes from LPN and weak PRFs. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 308–325. Springer, Heidelberg (2013)
14. Molnar, D., Wagner, D.: Privacy and security in library RFID: issues, practices, and architectures. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, p. 219 (2004)
15. Ouafi, K., Overbeck, R., Vaudenay, S.: On the security of HB# against a man-in-the-middle attack. In: Pieprzyk, J. (ed.) asiacrypt 2008. LNCS, vol. 5350, pp. 108–124. Springer, Heidelberg (2008)
16. Song, B., Mitchell, C.J.: Scalable RFID security protocols supporting tag ownership transfer. Comput. Commun. **34**(4), 556–566 (2011)