On the (im)possibility of receiving security beyond 2^l using an l-bit PRNG: the case of Wang *et. al.* protocol

Masoumeh Safkhani[1], Nasour Bagheri[1], Mehdi Hosseinzadeh[2], Mojtaba Eslamnezhad Namin[2], Samad Rostampour[2]

[1] Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran, Postal code: 16788-15811, Tel/fax:+98-21-2297006. Safkhani@srttu.edu
[2] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran, Postal code: 16788-15811, Tel/fax:+98-21-2297006. NBagheri@srttu.edu
[3] Department of Computer Engineering, Science and Research branch, Islamic Azad University, Tehran, Iran. {m.eslamnezhad,s.rostampour,hosseinzadeh}@srbiau.ac.ir

Abstract. Recently,Wang *et al.* analyzed the security of two EPC C1-G2 compliant RFID authentication protocols, called RAPLT and SRP^{+}, and proved that these protocols are vulnerable against de-synchronization and secret disclosure attacks. The time complexity of their attacks were $O(2^{16})$. In addition, they proposed an improved version of SRP^{+} entitled SRP^{++}, for which they claim the security would be $O(2^{32})$. However, in this letter, we analyze the security of SRP^{++} and show that the complexity of retrieving all secret parameters of a given tag is $O(2^{16})$, similar to its predecessor protocol.

Keywords: RFID; EPC-C1-G2; Authentication; Security Vulnerabilities.

1 Introduction

Nowadays, Radio Frequency Identification (RFID) systems are used in many applications [6,11]. In this technology, generally, authentication process is used to increase the security of RFID systems [3,5]. An authentication process allows a sender and receiver of information to validate each other. In this direction, many researchers have proposed their solutions for passive tags that are compliant with EPC C1-G2. Two examples of such attempts are a proposal by Jeon and Yoon named RAPLT [4] and a proposal by Pang *et al.* called SRP^{+} [7]. The designer of SRP^{+} claims that this protocol is robust against well-known RFID attacks as well as passive disclosure attacks with the exhaustive search complexity of $O(2^{32})$. However, recently Wang *et al.* analyzed these two protocols and presented successful attacks with the complexity of $O(2^{16})$ [10] against these protocols. In addition, they improved the SRP^{+} and presented a new protocol called SRP^{++}, which conforms to the EPC C1-G2 standard. Wang *et al.* claimed that their protocol can resist disclosure attacks up to the complexity of $O(2^{32})$.

In this paper, we argue that SRP^{++} is not secure and cannot resist against disclosure attacks. The remainder of this paper is organized as follows. In the Section 2, we review the SRP^{++} protocol. In Section 3, we analyze the security level of SRP^{++} and implement an attack on it. Finally, conclusions are drawn in Section 4.

2 Review of SRP^{++} protocol

Wang *et al.* improved SRP^{+} protocol and called it SRP^{++}. They just used XOR and PRNG functions in their method and removed CRC function, which has been used in SRP^{+}. Their protocol has two phases: initialization and mutual authentication.

1. **Initialization phase**
   In this phase, some information are shared between the tag and reader. The notations of SRP^{++} protocol are listed in Table (1).

2. **Mutual authentication phase**
The mutual authentication phase, that is shown in Figure (1), is implemented as follows:

(a) First, the reader generates a random number N_1 and sends it to the tag.
(b) Upon receiving N_1, the tag generates a random number N_2, computes M_1 and M_2 and sends M_1, M_2 and C_i to the reader, where:
$M_1 = N_2 \oplus PRNG(EPC_S \oplus K_i \oplus N_1)$
$M_2 = PRNG(EPC_S \oplus N_2 \oplus C_i) \oplus K_i$

(c) After receiving M_1, M_2 and C_i, the reader does as below:

- The reader looks up its database for a $C_{i,new}$ or $C_{i,old}$ equals to the received C_i and collects EPC_S and corresponding $K_i = K_{old}$ or K_{new} of the correct tag.
- The reader obtains the temporary random number $N_2 = M_1 \oplus PRNG(K_i \oplus EPC_S \oplus N_1)$ and checks whether the equation $M_2 \oplus K_i = PRNG(EPC_S \oplus N_2 \oplus C_i)$ holds or not.
- The reader repeats the search until the matched tag is found. If it can not find a matched tag, the reader stops this session.
- After the reader authenticates the tag successfully, it computes and sends M_3 to the tag and updates the secret records, as follows:
$M_3 = PRNG(K_i \oplus N_2) \oplus PRNG(EPC_S)$,
$C_{i,old} \leftarrow C_i$,
$C_{i,new} \leftarrow PRNG(N_1 \oplus EPC_S) \oplus PRNG(N_2 \oplus K_i \oplus C_i)$,
$K_{i,old} \leftarrow K_i$,
$K_{i,new} \leftarrow K_i \oplus PRNG(N_2)$

(d) Finally, after receiving M_3, the tag checks whether the equation $M_3 \oplus PRNG(EPC_S) = PRNG(K_i \oplus N_2)$ holds or not. If it holds, the tag authenticates the server successfully, and updates the records as follows and if it does not hold, the tag stops the session:
$C_i \leftarrow PRNG(N_1 \oplus EPC_S) \oplus PRNG(K_i \oplus N_2 \oplus C_i)$,
$K_i \leftarrow K_i \oplus PRNG(N_2)$.

3 Secret disclosure attack against SRP^{++}

In this section, we show that SRP^{++} protocol cannot resist against the disclosure attack with the exhaustive search complexity of $O(2^{16})$. We obtain secret parameters of the tag with $2 * 2^{16}$ evaluations of the PRNG function and prove that SRP^{++} cannot provide the desired security level with the complexity of $O(2^{32})$. The proposed attack is implemented as follows:

Table 1. The notations are used in the Wang *et al.*'s scheme i.e. SRP^{+}

Notation	Description
EPC_S	A 96-bit value which is built by XORing six 16-blocks of the EPC code.
K_i	The authentication key shared by the tag and reader, used to authenticate the tag at $(i+1)^{th}$ authentication.
C_i	The pseudonym of an RFID tag
K_{old}, K_{new}	The old and new authentication keys stored in the reader
C_{old}, C_{new}	The old and new pseudonyms stored in the reader
$PRNG()$	The pseudo random number generator with 16-bit output length
$\oplus$	The XOR operation

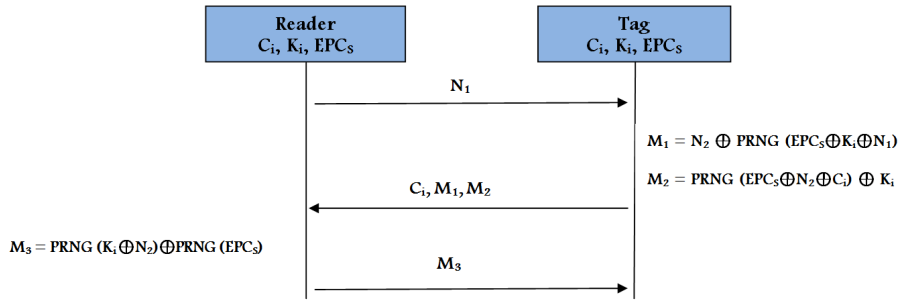

Fig. 1. Overview of SRP^{++} protocol

1. The adversary $\mathcal{A}$ initiates two consequence sessions of protocol by sending the same random value N_1 to the tag and stores all transferred messages includes: $(N_1, C_i, M_1 = N_2 \oplus PRNG(EPC_S \oplus K_i \oplus N_1), M_2 = PRNG(EPC_S \oplus N_2 \oplus C_i) \oplus K_i)$ and $(N_1, C_i, M_1' = N_2' \oplus PRNG(EPC_S \oplus K_i \oplus N_1), M_2' = PRNG(EPC_S \oplus N_2' \oplus C_i) \oplus K_i)$.
2. $\mathcal{A}$ calculates $\Delta N_2 = M_1 \oplus M_1' = N_2 \oplus N_2'$ and $\Delta M_2 = M_2 \oplus M_2' = PRNG(EPC_S \oplus N_2 \oplus C_i) \oplus PRNG(EPC_S \oplus N_2' \oplus C_i)$
3. $\forall\ i = 0, \ \ldots, \ 2^{16} - 1$ $\mathcal{A}$ does as follows:
   - $EPC_S \oplus N_2 \oplus C_i \longleftarrow i$,
   - $EPC_S \oplus N_2' \oplus C_i \longleftarrow i \oplus \Delta N_2$,
   - If $\Delta M_2 = PRNG(i) \oplus PRNG(i \oplus \Delta N_2)$ then $\mathcal{A}$ returns i as $EPC_S \oplus N_2 \oplus C_i$.
4. $K_i \longleftarrow PRNG(EPC_S \oplus N_2 \oplus C_i) \oplus M_2$
5. $EPC_S \oplus N_2 \longleftarrow EPC_S \oplus N_2 \oplus C_i \oplus C_i$
6. $x = EPC_S \oplus PRNG(EPC_S \oplus K_i \oplus N_1) \longleftarrow EPC_S \oplus N_2 \oplus M_1$
7. $\forall\ i = 0, \ \ldots, \ 2^{16} - 1$, and the extracted K_i and x in Step 4 and 6, $\mathcal{A}$ does as follows:
   - $EPC_S \longleftarrow i$,
   - If $x = i \oplus PRNG(x \oplus K_i \oplus N_1)$ then $\mathcal{A}$ returns i as EPC_s.
8. $N_2 \longleftarrow M_1 \oplus PRNG(EPC_S \oplus k_i \oplus N_1)$.
9. $\mathcal{A}$ uses M_1', M_2 and M_2' to verify the extracted values.
10. $\mathcal{A}$ returns the values of K_i, EPC_S and N_2.

The complexity of the given attack is to initiate two sessions with the target tag and doing 2×2^{16} evaluations of the $PRNG$-function. However, in the given attack, the adversary succeeds in its attack if it comes up with only one pre-image in each of Steps 4 and 7 (it must be noted that the existence of at least one pre-image in each step is guaranteed). Otherwise, the adversary should repeat the attack several times to come up with a unique solution. In this case, four runs of protocol should be fairly enough to extract all given parameters.

Following the given attack, the tag's all secret parameters have been extracted. Given secret parameters, it is easy to apply any other attacks against the protocol. Hence, we prove that the exact security level of Wang *et al.* protocol is 2^{16}, same as its predecessors.

4 Conclusion

In this paper, we analyzed SRP^{++} authentication protocol, which is presented by Wang *et al.*. They claimed that SRP^{++} can resist against the exhaustive search attack with the complexity of $O(2^{32})$ by using 16-bit PRNG function. We demonstrated that SRP^{++} is not robust against the secret disclosure attacks with the exhaustive search complexity of $O(2^{16})$. We obtained secret parameters of the tag by doing $2 * 2^{16}$ evaluations based on the short length of the used PRNG-function.

This work together with the previous works [2, 9], show the impossibility of receiving a security level beyond the security of building blocks of the design by linear combinations of components. In fact, this work shows that receiving security level more than 2^{16} by employing a 16-bit PRNG functions may not be feasible. On the other hand, there are many interesting PRNG functions and block ciphers with enough large output length that can be implemented in an EPC-C1-G2 tag, for example SIMON [1] and LAMED [8]. Hence, we suggest to use such primitives to design a secure protocol when an application needs high security margin.

References

1. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. `http://eprint.iacr.org/`.
2. J. Black, M. Cochran, and T. Shrimpton. On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions. In R. Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 526–541. Springer, 2005.
3. L. Gao, M. Ma, Y. Shu, F. Lin, L. Zhang, and Y. Wei. A Low-Cost RFID Authentication Protocol Against Desynchronization with a Random Tuple. *Wireless Personal Communications*, 79(3):1941–1958, 2014.
4. I.-S. Jeon and E.-J. Yoon. A New Ultra-lightweight RFID Authentication Protocol using Merge and Separation Operations. *International Journal of Mathematical Analysis*, 7(52):2583–2593, 2013.
5. Y.-P. Liao and C.-M. Hsiao. A Secure ECC-based RFID Authentication Scheme Integrated with ID-verifier Transfer Protocol . *Ad Hoc Networks*, 18(0):133 – 146, 2014.
6. I.-C. Lin, H.-H. Hsu, and C.-Y. Cheng. A Cloud-Based Authentication Protocol for RFID Supply Chain Systems. *Journal of Network and Systems Management*, pages 1–20, 2014.
7. L. Pang, L. He, Q. Pei, and Y. Wang. Secure and Efficient Mutual Authentication Protocol for RFID Conforming to the EPC C-1 G-2 Standard. In *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, pages 1870–1875, April 2013.
8. P. Peris-Lopez, J. C. H. Castro, J. M. Estévez-Tapiador, and A. Ribagorda. LAMED - A PRNG for EPC Class-1 Generation-2 RFID specification. *Computer Standards & Interfaces*, 31(1):88–97, 2009.
9. P. Rogaway and J. Steinberger. Security/Efficiency Tradeoffs for Permutation-Based Hashing. In N. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008, Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 220–236. Springer, 2008.
10. S. Wang, S. Liu, and D. Chen. Security Analysis and Improvement on Two RFID Authentication Protocols. *Wireless Personal Communications*, pages 1–13, 2014.
11. X. Zhuang, Y. Zhu, and C.-C. Chang. A New Ultralightweight RFID Protocol for Low-Cost Tags:R^2AP. *Wireless Personal Communications*, 79(3):1787–1802, 2014.