An improved RFID protocol based on quadratic residues

Ching-Hung Huang[*]

Abstract

Nowadays, RFID has become very popular technology and applications in various fields. Restrictions of computation cause RFID have a security problem due to its light, fortunately, there is a lot of experts have proposed a number of ways to solve these problems such that the issues have been addressed. In 2008 "Computer Network", Chen et. al. proposed a novel mutual authentication scheme based on quadratic residues. Unfortunately, the paper is implicit some of the security problems, furthermore, the scheme may also be suffered from tracking problem. Therefore, we points out the weakness of CCS protocol and proposes a more secure RFID protocol.

1 Introduction

RFID is a contactless wireless communication technology allows devices to automatically identify people and objects by using radio frequency. RFID system was first applied in British on the military's IFF (Identification Friend or Foe,) its function is used to distinguish between enemy aircraft and our aircraft. Initially, RFID is not very popular till WalMart Stores requires suppliers to embed RFID tags on goods, to substitute the traditional bar codes in order to save time, logistics cost and warehouse management. Recently, application of RFID in industry, academia, more and more, is widely used in various fields, such SCM (Supply Chain Management), animal identification, passports, libraries and transportation payments etc. EPC Global Inc. has also developed EPC (Electric Product Code) and ISO standards. Through the use of ONS (Object Naming Service,) it can obtain item serial number and related information. In the next few years, RFID will continue to increase in demand. In RFID widely used, the privacy and security have paid more attention.

The rest of this paper is organized as follows. Section 2 shows the detail of RFID system and privacy and security requirement. Section 3 is to introduce the related works. In section 4, we describe the improved protocol we proposed. In the next section 5 is security analysis and the last section 6 is conclusion.

2 RFID System

RFID system is composed of tags, readers and back-end system with middleware and database. A tag consists of the antenna and the integrated circuit, used for storages, calculations, modulates and demodulate radio frequency signal. A tag communicates with the backend system through the reader. The backend system processes the information from tag via the reader and applies the information to service.

[*] Graduate Institute of Electrical Engineering, National Taipei University, Taipei County 237, Taiwan. E-mail: {s79682308@webmail.ntpu.edu.tw}.

2.1 RFID tag categories

In general, according to supply mode of RFID tags, it can be divided into three categories.

1. Active RFID Tag: The Active RFID Tag has its own battery. It can take the initiative to send signals to the reader. Active RFID Tags has a wide range of communications and has enough power to do more complex calculations, but the volume compared to passive tags is to large, and its prices is higher than Passive tags.

2. Passive RFID Tag : A passive RFID tag not have their own battery, it just rely on the signal transmitted by reader into enough energy to do calculations and return to the reader. Short communication range and cannot do the complex calculations are the disadvantage. The advantage is lightweight and inexpensive.

3. Battery assisted Tag: Between active and passive tag, the Battery assisted Tag has its own battery, and strikes a balance between function and size.

In different frequency bands have different applications and standards, the following is the classification of the RFID frequency.

1. LF(under 135KHz): The effective transmission distance is less than 1 meter, and often used in pet identification. The corresponding ISO standard is ISO18000.

2. HF(13.56MHz): The effective transmission distance is up to about 1.5 meters, and often used in access control cards. It often used in public transportation cards, identification cards or electronic passports. The corresponding ISO standard is 14443 A / B and ISO 15693.

3. UHF(860-960MHz): The optimum transmission distance of about 10 meters, often applied to the container warehousing and supply chain management. The corresponding ISO standard is ISO 18000.

4. Microware(2.45-5.8GHz): The effective transmission distance of about 100 meters, but less penetrating. It often used in ETC (Electronic Toll Collection) system. The corresponding ISO standard is ISO 18000.

2.2 Privacy and Security Requirement

Generally, RFID attacks can classified into four major groups[15]. (1) Attack on authenticity is to obtain the certification from backend system. (2) Attack on integrity, for the data stored in the tag and backend database, the RFID system need to ensure the correctness and completeness of the information. (3) Attack on confidentiality, the purpose of this attack is attempting to obtain personal and Tags information. (4) Attacks on availability is to make RFID system doesnt work. The attacks and personal privacy are closely related with system security. The following will address the privacy and security requirement.

2.2.1 Privacy requirement

There are some privacy issues to be concerned. We discuss it as follows.

1. Tracking: To track individual movements, or the movement of goods, which are likely to violate personal privacy. For example, to track Hong Kong Octopus Cards, Taipei Easy Card, and even a personal identity card or passport and so on.
2. Inventorying: Construction of shopping habits of individuals, firms inventory, are privacy and confidential information of people and vendor.

2.2.2 Security requirement

There are some security requirements to be considered as list as follows.

1. Forward security: In the system running for some time, even if adversary crack the password, he has no way to use the password to know about the past information.
2. Eavesdropping: Because RFID is a wireless transmission equipment, all of the information is carried by radio waves through air; therefore, the communication between the tag and the reader may be eavesdropped.
3. Man-in-the-middle attack: Man-in-the-middle attack is an attack between the reader and the tag. Within the area of the intersection of the transmission in the reader and the tag, the adversary can play an intermediary to launch Man-in-the-middle attack.
4. Denial of service(DoS): The system receives too many messages from the adversary cause the system cannot work. In generally, the DoS attack in RFID system can be divided into two categories: One is to cause RFID tag unable to work. The other is for the RFID Backend system. the adversary made it impossible to provide services by sending numerous messages.
5. Spoofing: Spoofing is using a fake tag to masquerade as a valid tag to gain unlawful benefits such as forging identity cards, passport or student identity card.
6. Replay attack: In the replay attack, attacker will record the useful information from the tag and reader, then the attacker replies the duplicate to backend system attempts to obtain certification.
7. Virus: If there have an tag emits the message with malicious SQL syntax to the backend system, and the backend system may be suffered from SQL injection attack.
8. Power analysis: Professor Adi Shamirs paper[14] pointed out the power of RFID tags consumes is different in password correct and incorrect. Under the electricity consumption, the attacker can guess the correct password.

So far, there are many scheme[2-5,9-13] have been proposed to prevent security attacks for RFID system, but still some are not perfect. In next section, we aim to describe the Chen et. al.s scheme including how it works and be destroyed.

3 CCS Protocol

In [1], Chen et. al. proposed a novel mutual authentication scheme based on quadratic residues. In their paper, Chen et. al. using the Chinese Remainder Theorem to evaluate quadratic residues in order to achieve mutual authentication. This method will be described in the following.

Step 1: In the beginning of each round, the reader generates a random challenge $s \in Z_n$ and sends the *hello* message with challenge s to the tag.

Step 2: Received the challenge s, the tag calculates $x = h(TID) \oplus r \oplus s$, $X = x^2 \mathrm{mod} n$ and $R = r^2 \mathrm{mod} n$ and sends the information $\langle X, R, h(x), h(r) \rangle$ back to the reader.

Step 3: The reader forwards the information $\langle X, R, h(x), h(r), \rangle$ with challenge s to server.

Step 4: After receiving $\langle X, R, h(x), h(r), \rangle$, the server evaluates $X = x^2 \mathrm{mod} n$ and $R = r^2 \mathrm{mod} n$ by using Chinese Remainder Theorem and obtain the four roots (x_1, x_2, x_3, x_4) and (r_1, r_2, r_3, r_4). The server is necessary to compare which $h(x_i)$ and $h(r_i)$ is equal to the $h(x)$ and $h(r)$ tag sent, where $i = 1$ to 4, in order to determine the available x and r. Then the server calculates $h(TID) = x \oplus r \oplus s$ and use $h(TID)$ to search out the TID with r stored in the database. If it is not found, then the server will interrupt the session and authentication failed. Otherwise, the server verifies is the r as same as the servers. If it is the same, then the server calculates $x_{ack} = TID \oplus r$ and sends it to the tag. In the meanwhile, the server updates r_{old} as r and r as $PRNG(r)$ in the database.

Step 5: After receiving the $\langle h(x_{ack}) \rangle$, the tag verifies is the $\langle h(x_{ack}) \rangle$ equal to the received $\langle h(x_{ack}) \rangle$. If yes, then updates r as $PRNG(r)$.

To be illustrative, the CCS protocol is shown in Figure 1.

3.1 The weakness of CCS protocol

In CCS protocol, we found that the adversary can counterfeit the tag and spoofs the server if the information tag emitted was recorded. Below, we describes how crack the scheme step by step. the weakness of CCS protocol is shown in Figure 2.

Step 1: The adversary generates a challenge $s_0 = [000...000]$ and sends the s_0 with hello message to the tag. After receiving the s_0, the tag will calculate $x = h(TID) \oplus r \oplus s_0$, $X = x^2 \mathrm{mod} n$ and $R = r^2 \mathrm{mod} n$ and sends the $\langle X, R, h(x), h(r) \rangle$ back to the adversary.

Step 2: The adversary also generates a challenge $s_1 = [000...001]$ and sends the s_1 with hello message to the tag. After receiving the s_1, the tag will calculate $x = h(TID) \oplus r \oplus s_1$, $X = x^2 \mathrm{mod} n$ and $R = r^2 \mathrm{mod} n$ and sends the $\langle X, R, h(x), h(r) \rangle$ back to the adversary.

Step 3: After collecting that information, the adversary starts to solve the two equations. The adversary has $Y = h(TID) \oplus r$ and $A = Y^2 \mathrm{mod} n$ and $B = (Y+1)^2 \mathrm{mod} n$; then the adversary calculates the Y.

$$B = Y^2 + 2Y + 1$$

$$A = Y^2$$

$$2Y + 1 = B - A$$

$$Y = \frac{B - A - 1}{2}$$

Then the adversary gets $Y = h(TID) \oplus r$; furthermore, the adversary also records the R and $h(r)$.

Step 4: Next, the adversary plays the legal tag to authenticate by the server. After receiving the hello message with challenge s from the reader, the adversary calculates $X = (Y \oplus s)^2 \mathrm{mod} n$ and sends the $\langle X, R, h(x), h(r) \rangle$ back to the reader.

Step 5: The reader forwards the $\langle X, R, h(x), h(r), s \rangle$ to the server.

Step 6: After receiving the message $\langle X, R, h(x), h(r), s \rangle$, the server verifies the $h(TID)$ and r in the database is correct; therefore, the fake tag is authenticated by the server.

Because of the weakness, CCS protocol is not applicable. Hence we improved CCS protocol to achieve full security in the next section.

4 Proposed Protocol

In this paper, we propose a more secure protocol to resolve the weakness of CCS protocol. The protocol will be described in the following.

In the initialization phase, the server first choose two large prime numbers p and q and calculates $n = pq$. Then the p, q and n are stored in the database. And the n is also stored in the tag.

Step 1: When the tag approaches the reader, the tag receives a hello message with random challenge s from reader.

Step 2: After receiving challenge s, the tag first generates a random number r_T and calculates $x = h(TID) \oplus r \oplus r_T \oplus s$, $X = x^2 \mathrm{mod} n$ and $R = (r \oplus r_T)^2 \mathrm{mod} n$; then, the tag sent the information $\langle X, R, h(x), h(r \oplus r_T), h(r_T) \rangle$ back to the reader.

Step 3: The reader forwards $\langle X, R, h(x), h(r \oplus r_T), h(r_T) \rangle$ with challenge s to the server.

Step 4: After receiving $\langle X, R, h(x), h(r \oplus r_T), h(r_T), s \rangle$, the server evaluates $X = x^2 \mathrm{mod} n$, $R = (r \oplus r_T) \mathrm{mod} n$ by using Chinese Remainder Theorem and obtains the four roots (x_1, x_2, x_3, x_4) and (r_{T_1}, r_{T_2}, r_{T_3}, r_{T_4}). For determine the available value x and $r \oplus r_T$, the server compare which $h(x_i)$ and $h((r \oplus r_T)_i)$ is equal to the $h(x)$ and $h(r \oplus r_T)$ tag sent, where $i = 1$ to 4.

Step 5: Then the server calculates $h(TID) = x \oplus r \oplus r_T \oplus s$ and use $h(TID)$ to search out the TID with r stored in the database. If it is not found, then the server interrupt the session and authentication failed.

Step 6: Otherwise, the server verifies is the $h(r_T)$ as same as the servers. If it is the same, then the server calculates $x_{ACK} = TID \oplus r$ and sends the $h(x_{ACK})$ it to the tag. In the meanwhile, the server updates r_{old} as r and r as $PRNG(r)$ in the database.

Step 7: After receiving the $h(x_{ACK})$, the tag verifies is the $h(TID \oplus r)$ equal to the received $h(x_{ACK})$. If yes, then updates r as $PRNG(r)$.

To be illustrative, the proposed protocol is shown in Figure 3.

5 Security Analysis

In this section, we analyze our protocol is able to resist the adversary attacks and tracking problem.

1) Mutual Authentication
   In the improved protocol, the tag and reader will verify the argument of each other. The reader will check the calculated $h(r_T)$ is equal to the $h(r_T)$ received from the tag. If so, then the tag with the database stored in the r is the same. In step 6, tag also checks the $h(x_{ack})$ sent from the reader whether equal to the $h(x_{ack})$ tag computed.

2) Tracking Problem
   Because the information $\langle\, X,\, R,\, h(x),\, h(r \oplus r_T),\, h(r_T)\,\rangle$ tag generated is unfixable. It is no way to use the adversary eavesdrops all information from tag emitting. Therefore, the tag is impossible to be tracked by the adversary.

6 Conclusion

This paper not only points out the weakness of CCS protocol but also proposed a protocol to improve the scheme, furthermore, we are also to solve the tracking problem. This paper provides a more secure RFID protocol although the information transferred between the tag and server is a bit much.

References

[1] Yalin Chen, Jue-Sam Chou and Hung-Min Sun ”A novel mutual authentication scheme based on quadratic residues”, in *Computer Network*, Vol. 52, no. 12, pp. 2373-2380, August 2008.

[2] K. Rhee, J. Kwak, S. Kim, D. Won, Challenge-response based RFID authentication protocol for distributed database environment, in *International Conference on Security in Pervasive Computing SPC* 2005, pp. 7084.

[3] J. Yang, J. Park, H. Lee, K. Ren, K. Kim, Mutual authentication protocol for low-cost RFID, in *Handout of the Encrypt Workshop on RFID and Lightweight Crypto*, 2005.

[4] A. Juels, Yoking-Proofs for RFID tags, in *Proceedings of IEEE International Conference Digital Object Identifier,* 2004, pp. 138143.

[5] S. Karthikeyan, M. Nesterenko, RFID security without extensive cryptography, in *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2005, pp. 6367.

[6] H.Y. Chien, C.H. Chen, Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards, Computer Standards & Interfaces (2006).

[7] Kirk H.M. Wong, Patrick C.L. Hui, Allan C.K. Chan, Cryptography and authentication on RFID passive tags for apparel products, Computer in Industry 57 (2005) 342349.

[8] A. Juels, RFID Security and Privacy: A Research Survey, Selected Areas in Communications, IEEE Journal on Publication Date: Feb. 2006 Volume: 24, Issue: 2 On page(s): 381- 394

[9] A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFIDenabled banknotes. In R. Wright, editor, *Financial Cryptography 03*, volume 2742 of Lecture Notes in Computer Science, pages 103121. Springer-Verlag, 2003.

[10] Dong Seong Kim, Taek-Hyun Shin, and Jong Sou Park " A Security Framework in RFID Multi-domain System", in *Second International Conference on Availability, Reliability and Security* (ARES'07).

[11] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *Conference of Cryptographic Hardware and Embedded Systems*, 2004. Proceedings, pp. 357370. Springer 2004.

[12] X. Gao, Z. Xiang, H. Wang, J. Shen, J. Huang, and S. Song. "An approach to security and privacy of RFID system for supply chain," *CEC-East*, pp. 164168, IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), 2004.

[13] M. Aigner and M. Feldhofer. Secure symmetric authentication for RFID tags. *Telecommunication and Mobile Computing*, March 2005.

[14] R. Merritt, Cellphone could crack RFID tags, says cryptographer, EE Times, February 14, 2006. [Online]. http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=180201688

[15] Qinghan Xiao, Cam Boulet, Thomas Gibbons, "RFID Security Issues in Military Supply Chains," ares, pp.599-605, The Second International Conference on Availability, Reliability and Security (ARES'07), 2007.

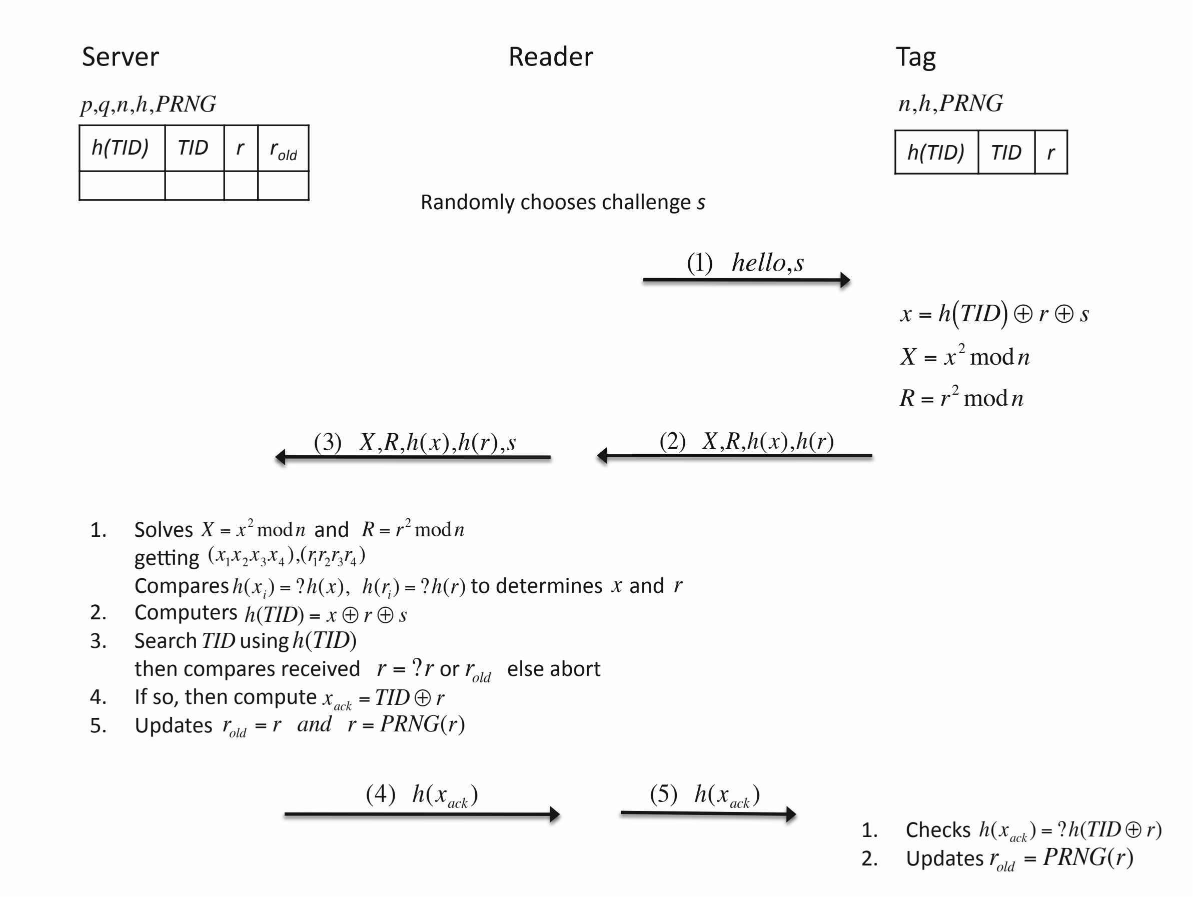
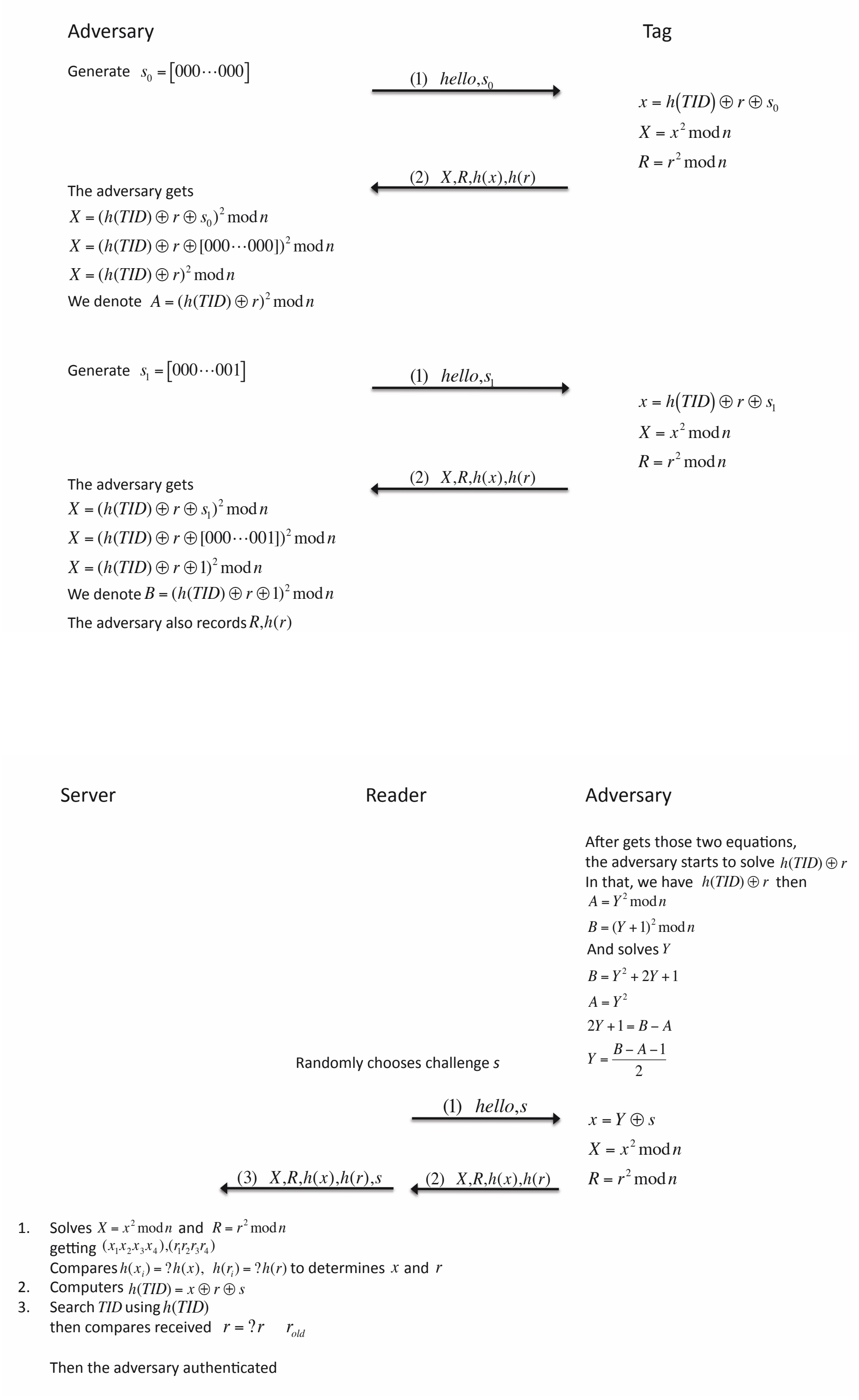

Server
Reader
Tag
$p,q,n,h,PRNG$
h(TID) | TID | r | r_{old}
$n,h,PRNG$
h(TID) | TID | r
Randomly chooses challenge s
(1) $hello,s$
$x = h(TID) \oplus r \oplus s$
$X = x^2 \bmod n$
$R = r^2 \bmod n$
(2) $X,R,h(x),h(r)$
(3) $X,R,h(x),h(r),s$
1. Solves $X = x^2 \bmod n$ and $R = r^2 \bmod n$ getting $(x_1x_2x_3x_4),(r_1r_2r_3r_4)$ Compares $h(x_i) = ?h(x)$, $h(r_i) = ?h(r)$ to determines x and r
2. Computers $h(TID) = x \oplus r \oplus s$
3. Search TID using $h(TID)$ then compares received $r = ?r$ or r_{old} else abort
4. If so, then compute $x_{ack} = TID \oplus r$
5. Updates $r_{old} = r$ and $r = PRNG(r)$
(4) $h(x_{ack})$
(5) $h(x_{ack})$
1. Checks $h(x_{ack}) = ?h(TID \oplus r)$
2. Updates $r_{old} = PRNG(r)$

Figure 1: CCS Protocol[1]



Adversary

Tag

Generate $s_0 = [000 \cdots 000]$

(1) $hello, s_0$

$x = h(TID) \oplus r \oplus s_0$

$X = x^2 \bmod n$

$R = r^2 \bmod n$

(2) $X, R, h(x), h(r)$

The adversary gets

$X = (h(TID) \oplus r \oplus s_0)^2 \bmod n$

$X = (h(TID) \oplus r \oplus [000 \cdots 000])^2 \bmod n$

$X = (h(TID) \oplus r)^2 \bmod n$

We denote $A = (h(TID) \oplus r)^2 \bmod n$

Generate $s_1 = [000 \cdots 001]$

(1) $hello, s_1$

$x = h(TID) \oplus r \oplus s_1$

$X = x^2 \bmod n$

$R = r^2 \bmod n$

(2) $X, R, h(x), h(r)$

The adversary gets

$X = (h(TID) \oplus r \oplus s_1)^2 \bmod n$

$X = (h(TID) \oplus r \oplus [000 \cdots 001])^2 \bmod n$

$X = (h(TID) \oplus r \oplus 1)^2 \bmod n$

We denote $B = (h(TID) \oplus r \oplus 1)^2 \bmod n$

The adversary also records $R, h(r)$

Server

Reader

Adversary

After gets those two equations,
the adversary starts to solve $h(TID) \oplus r$
In that, we have $h(TID) \oplus r$ then

$A = Y^2 \bmod n$

$B = (Y+1)^2 \bmod n$

And solves Y

$B = Y^2 + 2Y + 1$

$A = Y^2$

$2Y + 1 = B - A$

$Y = \frac{B - A - 1}{2}$

Randomly chooses challenge s

(1) $hello, s$

$x = Y \oplus s$

$X = x^2 \bmod n$

$R = r^2 \bmod n$

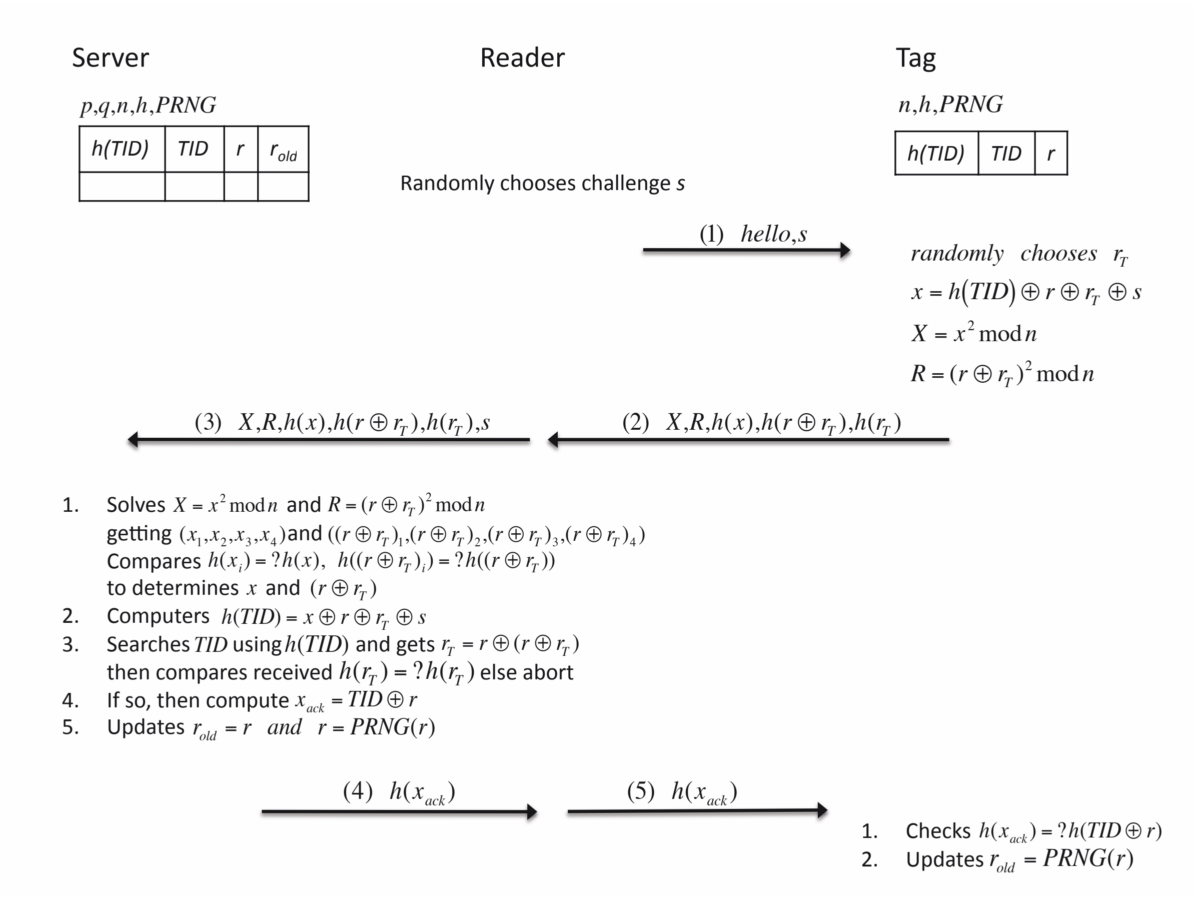
(3) $X, R, h(x), h(r), s$

(2) $X, R, h(x), h(r)$

1. Solves $X = x^2 \bmod n$ and $R = r^2 \bmod n$
   getting $(x_1 x_2 x_3 x_4), (r_1 r_2 r_3 r_4)$
   Compares $h(x_i) = ?h(x)$, $h(r_i) = ?h(r)$ to determines x and r
2. Computers $h(TID) = x \oplus r \oplus s$
3. Search TID using $h(TID)$
   then compares received $r = ?r$ r_{old}

Then the adversary authenticated

Figure 2: Attack on CCS Protocol


Server
Reader
Tag
$p,q,n,h,PRNG$
h(TID) | TID | r | r_{old}
$n,h,PRNG$
h(TID) | TID | r
Randomly chooses challenge *s*
(1) $hello,s$
$randomly \quad chooses \quad r_T$
$x = h(TID) \oplus r \oplus r_T \oplus s$
$X = x^2 \bmod n$
$R = (r \oplus r_T)^2 \bmod n$
(2) $X,R,h(x),h(r \oplus r_T),h(r_T)$
(3) $X,R,h(x),h(r \oplus r_T),h(r_T),s$
(4) $h(x_{ack})$
(5) $h(x_{ack})$

1. Solves $X = x^2 \bmod n$ and $R = (r \oplus r_T)^2 \bmod n$
   getting $(x_1,x_2,x_3,x_4)$and $((r \oplus r_T)_1,(r \oplus r_T)_2,(r \oplus r_T)_3,(r \oplus r_T)_4)$
   Compares $h(x_i) = ?h(x),\ h((r \oplus r_T)_i) = ?h((r \oplus r_T))$
   to determines x and $(r \oplus r_T)$
2. Computers $h(TID) = x \oplus r \oplus r_T \oplus s$
3. Searches TID using $h(TID)$ and gets $r_T = r \oplus (r \oplus r_T)$
   then compares received $h(r_T) = ?h(r_T)$ else abort
4. If so, then compute $x_{ack} = TID \oplus r$
5. Updates $r_{old} = r \quad and \quad r = PRNG(r)$

1. Checks $h(x_{ack}) = ?h(TID \oplus r)$
2. Updates $r_{old} = PRNG(r)$

Figure 3: Improved protocol