Weaknesses in Two Recent Lightweight RFID Authentication Protocols

Pedro Peris-Lopez[1], Julio C. Hernandez-Castro[2], Juan M. E. Tapiador[3], Tieyan Li[4], and Jan C.A. van der Lubbe[1]

[1] Department of Information and Communication, Delft University of Technology
[2] School of Computing, University of Portsmouth
[3] Department of Computer Science, University of York
[4] Institute for Infocomm Research, A*STAR Singapore

Abstract. The design of secure authentication solutions for low-cost RFID tags is still an open and quite challenging problem, though many algorithms have been published lately. In this paper, we analyze two recent proposals in this research area. First, Mitra's scheme is scrutinized, revealing its vulnerability to cloning and traceability attacks, which are among the security objectives pursued in the protocol definition [1]. Later, we show how the protocol is vulnerable against a full disclosure attack after eavesdropping a small number of sessions. Then, we analyze a new EPC-friendly scheme conforming to EPC Class-1 Generation-2 specification (ISO/IEC 180006-C), introduced by Qingling and Yiju [2]. This proposal attempts to correct many of the well known security shortcomings of the standard, and even includes a BAN logic based formal security *proof*. However, notwithstanding this formal security analysis, we show that Qingling et al.'s protocol offers roughly the same security as the standard they try to improve, is vulnerable to tag and reader impersonation attacks, and allows tag traceability.

Keywords: RFID, EPC, Cloning, Traceability, Impersonation, Cryptanalysis, BAN, Proof

1 Introduction

Many authors have recently focused their attention on low-cost RFID tags, because designing secure solutions within their restricted capabilities is a great challenge. The solutions proposed can be categorized with respect to three main criteria. First, some proposals are based on the learning parity with noise (LPN) problem, initially examined by Hopper and Blum [3] and introduced by Juels in the context of RFID systems [4]. Secondly, other authors severely restrict the assumed set of operations supported by tags to very simple and efficient operations: The SASI [5] and Gossamer [6] protocols are two proposals in this direction, where tag capabilities are limited to bitwise operations and rotations. These protocols have been christened ultra-lightweight protocols, in Chien's classification [5]. When we add to the described tags the requirement of supporting Pseudo Random Number Generators (PRNGs), we then call these proposals lightweight. For example, EPC Class-1 Generation-2 (Gen-2 in short) compliant tags support a 16-bit PRNG and a 16-bit Cyclic Redundancy Check (CRC) [7].

In this paper, we successfully cryptanalyse two recent lightweight authentication protocols. First, Mitra's scheme [1] is explored, discovering that its two main objectives (anti-cloning and untraceability) are not guaranteed. After that, we present a full disclosure attack that points out the protocol fails short of the security level required for the intended applications. Then, a new scheme under the EPC Gen-2 framework is scrutinized. As is already well-known, the Gen-2 specification has some important security drawbacks. In [2], Qingling et al. made an attempt to correct many of them in their proposed scheme, but we show that the authors failed, just as those of many other previous protocols [8–11], despite providing a formal security *proof*.

2 Mitra's Protocol

In 2008, Mitra proposed a new scheme (in the following called TC-RFID for short) that attempts to protect tags against traceability and cloning [1]. The author assumes that tags support an on-chip PRNG. Tags are also able to compute simple operations, particulary multiplication and addition. Operations in readers are limited to the computation of a modulo. Regarding communication channels, both the forward (reader-to-tag) and the backward (tag-to-reader) can be eavesdropped by an adversary. As for memory requirements, each tag stores a static identifier $\{EPC_i\}$ and a key $\{K_i\}$. This key is shared between the tag and legitimate readers (and the back-end database) registered in the system.

The author proposed this simple protocol, in which only tags ($\mathcal{T}$) are authenticated by readers ($\mathcal{R}$):

Step 1: $\mathcal{R} \rightarrow \mathcal{T}_i$ The reader sends a request message to tag i.

Step 2: $\mathcal{T}_i$ (Tag i) computes an *encrypted* and/or *anonymized* version of its static identifier:

$$E_i(n) = RND(n) * K_i + EPC_i \qquad (1)$$

where RND is a random number, the output after the n^{th}-call to the on-chip PRNG, and K_i is the shared key between $\mathcal{T}_i$ and $\mathcal{R}$.

Step 3: $\mathcal{T}_i \rightarrow \mathcal{R}$ The tag sends the reader $E_i(n)$, which serves as an authentication token.

3 Vulnerabilities of Mitra's Protocol

In this section we analyze the most relevant weaknesses of the TC-RFID protocol.

3.1 Cloning Attack

As mentioned in the last section, nowadays tags often respond to reader's queries without requiring any authentication at all. Tags can even transmit their static identifier $\{EPC_i\}$ over the channel in plaintext. In it case, an adversary can snoop this publicly available information and transfer it to a clone device (i.e. another tag or a more sophisticated emulator).

Symmetric-key cryptography can be used to avoid tag cloning attacks. Specifically, a challenge-response mechanism like the following can be employed. We assume the tag ($\mathcal{T}_i$) shares a secret key $\{K_i\}$ with the reader ($\mathcal{R}$). Afterwards, the following messages are exchanged:

Step 1: $\mathcal{R} \rightarrow \mathcal{T}_i$ The reader generates a fresh random number ($RND(n)$, a nonce challenge) and transmits it to the tag.

Step 2: $\mathcal{T}_i \rightarrow \mathcal{R}$ The tag computes $H_i(n) = g(K_i, RND(n))$ and sends it back to the reader.

Step 3: $\mathcal{R}$ The reader locally computes $H_i'(n) = g(K_i, RND(n))$ and checks if its value is identical to tag's answer H_i.

The g function can be implemented by using any hash or encryption algorithm. Note that the protocol security is highly dependent on that of the g function. As low-cost RFID tags have severe resource limitations, the use of standard cryptographic primitives is not possible. Particularly, Mitra proposed the use of multiplication and summation operands for the g function ($H_i(n) = E_i(n) = RND(n) * K_i + EPC_i$), which is vulnerable to cloning attacks. An attacker can collect a number of encrypted messages, and compute their difference:

$$\Delta = E_i(n) - E_i(n+1) = (RND(n) - RND(n+1)) * K_i \tag{2}$$

Then, she will compute the greatest common divisor of these differences. The attacker concludes this value is the secret key $\{K_i\}$ of the target tag.

Additionally, an attacker that eavesdrops on two (non necessarily consecutive) authentication sessions ($\{E_i(n), E_i(n+p)\}$) between the target tag ($\mathcal{T}_i$) and a legitimate reader ($\mathcal{R}$) is able to supplant a tag indefinitely by sending $E_i' = E(n) + RND_r(q) * \Delta$ as its authentication token, where $\Delta = E_i(n) - E_i(n+p) = (RND(n) - R(n+p)) * K_i$.

3.2 Traceability Attack

The traceability problem has been studied by many researchers lately. In [12], Juels and Weis give a formal definition of the untraceability model. The same definition, though in a style more commonly used to formally define the properties of security protocols, is described by Phan in his recent attack against the SASI protocol [13], and used in the following.

In RFID systems, tags ($\mathcal{T}$) and readers ($\mathcal{R}$) interact in protocol sessions. In general terms, the adversary ($\mathcal{A}$) controls the communications between all the participants and interacts passively or actively with them. In our case, we can succeed in the traceability attack by only using passive means. Specifically, $\mathcal{A}$ can run the following queries:

- Execute($\mathcal{R}$, $\mathcal{T}$, i) query. This models a passive attacker. $\mathcal{A}$ eavesdrops on the channel, and gets read access to the exchanged messages between $\mathcal{R}$ and $\mathcal{T}$ in session i of a genuine protocol execution.
- Test(i, $\mathcal{T}_0$, $\mathcal{T}_1$) query. This does not model any ability of $\mathcal{A}$, but it is necessary to define the untraceability test. When this query is invoked in session i, a random bit is generated $b \in \{0, 1\}$. Then, $E_b(n)$, from the set $\{E_0(n), E_1(n)\}$ corresponding to tags $\{\mathcal{T}_0, \mathcal{T}_1\}$ is given to $\mathcal{A}$.

Upon definition of the adversary's abilities, the untraceability problem can be defined as a game $\mathcal{G}$. We now show why the TC-RFID scheme does not achieve untraceability. Specifically, the TC-RFID protocol, in an RFID system (S= $\{R_i$, $\mathcal{T}_0$, $\mathcal{T}_1$, ...$\}$ in which an adversary $\mathcal{A}$ can invoke two Execute($\mathcal{R}$, $\mathcal{T}$, i) queries and one Test(i, $\mathcal{T}_0$, $\mathcal{T}_1$) query, is vulnerable to traceability attacks, since the advantage for an adversary is significant: $Adv_{\mathcal{A}}^{UNT}(t, r = 2) = 0.5 \gg \varepsilon(t, 2)$, t being a security parameter (i.e. the bit length of the secret key) and $\varepsilon(.)$ some negligible function.

Specifically, an adversary $\mathcal{A}$ performs the following steps:

Phase 1 (Learning): $\mathcal{A}$ sends two Execute queries to $\mathcal{T}_0$. Consecutiveness in the queries is not necessary, which is handy because the target tag may have been read by a legitimate reader in between. $\mathcal{A}$ acquires the following messages:

$$E_0(n) = RND(n) * K_0 + EPC_0 \tag{3}$$

$$E_0(n + m) = RND(n + m) * K_0 + EPC_0 \tag{4}$$

Phase 2 (Challenge): $\mathcal{A}$ chooses two fresh tags whose associated identifiers are EPC_0 and EPC_1. Then he sends a Test(q, $\mathcal{T}_0$, $\mathcal{T}_1$) query. As a result, $\mathcal{A}$ is given a challenge cipher text $E_b(q)$ from the set $\{E_0(q), E_1(q)\}$, which depends on a chosen random bit $b \in \{0, 1\}$:

$$E_i(q) = \begin{cases} RND(q) * K_0 + EPC_0 \text{ if } b = 0 \\ RND(q) * K_1 + EPC_1 \text{ if } b = 1 \end{cases} \tag{5}$$

Phase 3 (Guessing) $\mathcal{A}$ finishes $\mathcal{G}$ and outputs a bit d ($d \in \{0, 1\}$) as his guess of the value b. In particular, we propose the following procedure to obtain value d:

1. $\mathcal{A}$ computes the difference between Equations 3, 4:

$$\begin{aligned} \Delta_1 &= |E_0(n) - E_0(n + m)| \\ &= |RND(n) * K_0 + EPC_0 - RND(n + m) * K_0 - EPC_0| \\ &= |(RND(n) - RND(n + m)) * K_0| \end{aligned} \tag{6}$$

2. $\mathcal{A}$ computes the difference between Equations 3, 5:

$$\Delta_2 = \begin{cases} |(RND(n) - RND(q)) * K_0| & \text{if } b = 0 \\ |RND(n) * K_0 - RND(q) * K_1 + EPC_0 - EPC_1| & \text{if } b = 1 \end{cases} \tag{7}$$

3. $\mathcal{A}$ uses the following decision rule:

$$d = \begin{cases} 0 & \text{if } gcd(\Delta_1, \Delta_2) \geq 2^{L/2} \\ 1 & \text{if } gcd(\Delta_1, \Delta_2) < 2^{L/2} \end{cases} \tag{8}$$

where gcd(.) symbolizes the greatest common divisor and L represents the length of the variables used. To be compatible with the common encodings schemes defined by EPCGlobal [14], we can fix L to 96 bits.

We have run 1000 experiments, with 2^{20} executions of the above game ($\mathcal{G}$) in each experiment, in order to obtain an approximation of the success probability of the adversary. From this experimentation, a probability of 1 was obtained. So, the $Adv_{\mathcal{A}}^{UNT}(t,r)$ is not only not negligible, but maximal. $\mathcal{A}$ wins $\mathcal{G}$, allowing him the traceability of tags: $Adv_{\mathcal{A}}^{UNT}(t,2) = |1 - \frac{1}{2}| = 0.5$. So the use of random numbers does not prevent the attacker from associating the tags's answers with its holder, with complete certainty.

3.3 Full Disclosure Attack

In this section, we show a much more harmful attack in which the attacker disclosures the secret key $\{K_i\}$ of the target tag. Once $\{K_i\}$ is made public, the static identifier $\{EPC_i = E_i(n+c) \mod K_i\}$ is compromised too. That is, all the private information of the tag is exposed by the adversary.

Specifically, in the TC-RFID protocol, an adversary that eavesdrops on t (non necessarily consecutive) authentication sessions $\{E_i(n+c_1), E_i(n+c_2), ..., E_i(n+c_t)\}$ between the target tag ($\mathcal{T}_i$) and a legitimate reader ($\mathcal{R}$) is able to disclosure the secret key $\{K_i\}$ by computing the greatest common divisor of the t–1 independent differences $\{|E_i(n+c_1) - E_i(n+c_2)|, ..., |E_i(n+c_1) - E_i(n+c_t)|\}$. The probability of success –from basic Number Theory [15]– is quite accurately given by the equation bellow:

$$Pr[\mathcal{A}\ reveals\ K_i] \approx \frac{1}{\zeta(t-1)} \tag{9}$$

where ζ is the Riemann zeta function.

We ran 10,000 experiments in order to estimate the Adversary's probability of success. We conducted this experiment for several numbers of eavesdropped sessions. In Figure 1, the good fitting between the theoretical and experimental results is depicted. We observe that after a low number [2 : 11] of eavesdropped sessions the attack is quite successful (60% – 100%). The attack just presented here is the most powerful and implies all those described in previous sections (i.e. privacy exposure, cloning, traceability, etc.).

4 Qingling et al.'s Protocol

In 2008, Quingling et al. proposed a minimalist mutual authentication protocol conforming with Gen-2 specification (QYY-Gen2 in short) [2]. A formal security

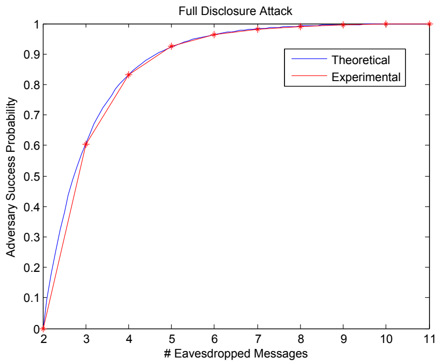

Fig. 1. Full Disclosure Attack

analysis was included in their proposal, which generated some hopes that it could be the first solution to really increase the security of the Standard. We have analyzed the scheme, and realized these hopes were overoptimistic, because the protocol has the same security weaknesses as the Gen-2 Standard it is intended to improve, as shown in Section 5.

The authors proposed a challenge-response protocol in which both tags ($\mathcal{T}_i$) and reader ($\mathcal{R}$) are authenticated. Each tag and reader (back-end database) share a 32-bit EPC unique identifier $\{TID^{Tag_i}\}$ and a 32-bit access password $\{APWD^{Tag_i}\}$. For simplicity, we condense readers and back-end database into a single entity as the communication channel between both entities is assumed to be secure. The subindex M and L are used to represent the 16 most and least significant bits of a variable (i.e. $X = X_L||X_M$). We outline the messages exchanged bellow:

Step 1: $\mathcal{R} \rightarrow \mathcal{T}_i$**:** $Query$**,** RND^{Rdr}

The reader first generates a random number RND^{Rdr} and sends $\{Query,$ $RND^{Rdr}\}$ to the target tag.

Step 2: $\mathcal{T}_i \rightarrow \mathcal{R}$**:** M^{Tag_i}**,** RND^{Tag_i}

Upon receiving reader's query, the tag also generates a nonce RND^{Tag_i} and computes: $M^{Tag_i} = M_L^{Tag_i}||M_M^{Tag_i}$

$$\begin{aligned} M_L^{Tag_i} &= CRC(TID_L^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag_i}) \oplus APDW_L^{Tag_i} \\ M_M^{Tag_i} &= CRC(TID_M^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag_i}) \oplus APDW_M^{Tag_i} \end{aligned} \tag{10}$$

Finally, the tag sends $\{M^{Tag_i}, RND^{Tag_i}\}$ to the reader.

Step 3: The reader verifies whether the equation $M^{Tag_i} \oplus APDW^{Tag_i} = CRC(TID_L^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag_i})||CRC(TID_M^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag})$ holds for any tag registered in the back-end database. If it can find a match, the tag is authenticated and the process continues; otherwise it stops the process, which ends in failure.

Step 4: $\mathcal{R} \rightarrow \mathcal{T}_i$**:** $M^{Rdr} = M_L^{Rdr}||M_M^{Rdr}$

The reader computes an authentication message and sends it to the tag.

$$\begin{aligned} M_L^{Rdr} &= CRC(TID_L^{Tag_i} \oplus RND^{Tag_i}) \oplus APDW_L^{Tag_i} \\ M_M^{Rdr} &= CRC(TID_M^{Tag_i} \oplus RND^{Tag_i}) \oplus APDW_M^{Tag_i} \end{aligned} \tag{11}$$

Step 5: On receiving M^{Rdr}, the tag verifies the equation $M^{Rdr} \oplus APDW^{Tag_i} = CRC(TID_L^{Tag_i} \oplus RND^{Tag_i})||CRC(TID_M^{Tag_i} \oplus RND^{Tag_i})$. If it holds, the reader is successful authenticated; otherwise it stops the process, which ends in failure.

5 Vulnerabilities of Qingling's Protocol

In this section we analyze the most relevant weaknesses of the QYY-Gen2 protocol. The authors use a Cyclic Redundancy Check (CRC) function as if it were a "strong" primitive despite its well-known security problems due to its linearity [16, 17]. Basically, the security of the proposed scheme is incorrectly based on the assumption that CRC functions are one-way functions.

CRC functions possess some properties that are undesirable from a security point of view. We show one of them, which will be enough to prove that the QYY-Gen2 protocol fails short of its security objectives, being as insecure as the original Gen-2 specification it is intended to improve on. For any CRC (independently of its generator polynomial) and for any values A, B: $CRC(A \oplus B) = CRC(A) \oplus CRC(B)$.

5.1 Tag/Reader Impersonation Attack

Tags are authenticated by checking the equation: $M^{Tag_i} \oplus APDW^{Tag_i} \overset{?}{=} CRC(TID_L^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag_i})||CRC(TID_M^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag_i})$. The authors claim that only genuine tags can compute correct answers to the readers's queries because private information shared between these two entities is employed in message generation. However, we show how an attacker can supplant a tag without needing to know any private information. A passive attacker, after eavesdropping one authentication session between an authentic tag ($\mathcal{T}_i$) and a genuine reader ($\mathcal{R}$), can impersonate the target tag by sending message $M_L^{Tag_i} \oplus CRC(\alpha)||M_M^{Tag_i} \oplus CRC(\alpha), RND_{new}^{Tag_i}$, where $\delta = RND_{new}^{Tag_i} \oplus RND^{Tag_i}$, $\gamma = RND_{new}^{Rdr} \oplus RND^{Rdr}$, and $\alpha = \delta \oplus \gamma$. The adversary is thus authenticated as a legitimate tag, without knowing any of the tag's private information.

Similarly, the authors point out that an attacker cannot respond to tag queries due to their ignorance of the private information and the use of fresh random nonces in each authentication session. However, we show an attacker can impersonate a reader using similar arguments as in the tag impersonation attack. On capturing messages transmitted in a valid authentication session between an authentic tag ($\mathcal{T}_i$) and a genuine reader ($\mathcal{R}$), an adversary can supplant a reader by sending message $M_L^{Rdr} \oplus CRC(\delta)||M_M^{Tag_i} \oplus CRC(\delta)$, where

$\delta = RND_{new}^{Tag_i} \oplus RND^{Tag_i}$. The tag cannot, therefore, detect the ploy and authenticates the adversary as a genuine reader.

We must emphasize that these attacks are very efficient, since passive capture of messages in just one legitimate authentication session is all that is required for their success.

5.2 Traceability Attack

The authors argue that the proposed protocol guarantees untraceability due to the use of new nonces in each session. However, in this section we show how an attacker is able to track a tag by making some simple computations over the tag's response. To do this, we use the traceability game defined in Section 3.2.

Specifically, QYY-Gen2 protocol, in an RFID system (S= $\{R_i, \mathcal{T}_0, \mathcal{T}_1, ...\}$ in which an adversary $\mathcal{A}$ can invoke one Execute($\mathcal{R}$, $\mathcal{T}$, i) and Test(i, $\mathcal{T}_0$, $\mathcal{T}_1$) query in an untraceability game $\mathcal{G}$, is vulnerable to traceability attacks, since the advantage for an adversary to win $\mathcal{G}$ is not negligible: $Adv_{\mathcal{A}}^{UNT}(t, r = 1) \simeq 0.499999 \gg \varepsilon(t, 1)$, t being a security parameter (i.e. the bit length of the access and key password) and $\varepsilon(.)$ some negligible function.

An adversary $\mathcal{A}$ performs the following steps to track tags in the QYY-Gen2 protocol:

Phase 1 (Learning): $\mathcal{A}$ sends an Execute query to $\mathcal{T}_0$. $\mathcal{A}$ acquires the random numbers used in the session and the tag's authentication message: RND^{Rdr}, $RND_q^{Tag_0}$, $M^{Tag_0} = M_L^{Tag_0} || M_M^{Tag_0}$.

$$\begin{aligned} M_L^{Tag_0} &= CRC(TID_L^{Tag_0} \oplus RND^{Rdr} \oplus RND_q^{Tag_0}) \oplus APDW_L^{Tag_0} \\ M_M^{Tag_0} &= CRC(TID_M^{Tag_0} \oplus RND^{Rdr} \oplus RND_q^{Tag_0}) \oplus APDW_M^{Tag_0} \end{aligned} \tag{12}$$

Phase 2 (Challenge): $\mathcal{A}$ chooses two fresh tags whose associated identifiers are TID^{Tag_0} and TID^{Tag_1}. Then he sends query Test(q, $\mathcal{T}_0$, $\mathcal{T}_1$). As a result, $\mathcal{A}$ is given two random number messages RND_{new}^{Rdr}, $RND_{q+1}^{Tag_i}$, and an authentication message M^{Tag_i} from the set $\{M^{Tag_0}, M^{Tag_1}\}$, which depends on a chosen random bit $b \in \{0, 1\}$:

$$M^{Tag_i} = \begin{cases} CRC(TID_L^{Tag_0} \oplus RND_{new}^{Rdr} \oplus RND_{q+1}^{Tag_0}) \oplus APDW_L^{Tag_0} || \text{ if } b = 0 \\ \quad CRC(TID_M^{Tag_0} \oplus RND_{new}^{Rdr} \oplus RND_{q+1}^{Tag_0}) \oplus APDW_M^{Tag_0} \\ CRC(TID_L^{Tag_1} \oplus RND_{new}^{Rdr} \oplus RND_{q+1}^{Tag_1}) \oplus APDW_L^{Tag_1} || \text{ if } b = 1 \\ \quad CRC(TID_M^{Tag_1} \oplus RND_{new}^{Rdr} \oplus RND_{q+1}^{Tag_1}) \oplus APDW_M^{Tag_1} \end{cases} \tag{13}$$

Phase 3 (Guessing) $\mathcal{A}$ finishes $\mathcal{G}$ and outputs a bit d ($d \in \{0, 1\}$) as its conjecture of value b. Specifically, we propose the following procedure to obtain d:

1. From Equation 12 and CRC linearity, the following constant value univocally associated with $\mathcal{T}_0$ is obtained by the adversary: $X = X_L || X_M$

$$\begin{aligned} X_L = M_L^{Tag_0} \oplus CRC(RND^{Rdr}) \oplus CRC(RND_q^{Tag_0}) = \\ = CRC(TID_L^{Tag_0}) \oplus APDW_L^{Tag_0} \\ X_M = M_M^{Tag_0} \oplus CRC(RND^{Rdr}) \oplus CRC(RND_q^{Tag_0}) = \\ = CRC(TID_M^{Tag_0}) \oplus APDW_M^{Tag_0} \end{aligned} \qquad (14)$$

2. By the same mathematical reasoning, $\mathcal{A}$ calculates the constant value associated with Equation 13:

$$Y = \begin{cases} CRC(TID_L^{Tag_0}) \oplus APDW_L^{Tag_0} || \text{ if } b = 0 \\ \ CRC(TID_M^{Tag_0}) \oplus APDW_L^{Tag_0} \\ CRC(TID_L^{Tag_1}) \oplus APDW_L^{Tag_1} || \text{ if } b = 1 \\ \ CRC(TID_L^{Tag_1}) \oplus APDW_L^{Tag_1} \end{cases} \qquad (15)$$

3. $\mathcal{A}$ utilizes the following simple decision rule:

$$d = \begin{cases} 0 & \text{if } X = Y \\ 1 & \text{if } X \neq Y \end{cases} \qquad (16)$$

As tags are randomly initialized, there is a negligible probability for the value $CRC(TID_L^{Tag_i}) \oplus APDW_L^{Tag_i} || CRC(TID_M^{Tag_i}) \oplus APDW_L^{Tag_i}$ to be equal for different tags (i.e. $\mathcal{T}_0$ and $\mathcal{T}_1$). Specifically, for the parameters proposed by the authors, with variables set to a 32-bit length and a CRC function of 16 bits, we have a $1/2^{32}$ probability of collision, assumed independence and uniformity in the secret values $\{TID^{Tag_i}, APWD^{Tag_i}\}$ linked to each tag. Therefore the advantage of $\mathcal{A}$ in distinguishing whether the adversary interacts with $\mathcal{T}_0$ or $\mathcal{T}_1$ is: $Adv_{\mathcal{A}}^{UNT}(t, 1) = |Pr[d = b] - \frac{1}{2}| = \frac{1}{2} - \frac{1}{2^{32}}$.

6 Conclusions

In this paper the cryptanalysis of two recent lightweight protocols is proposed. Both of these protocols assume that tags support an on-chip PRNG and simple operations. In Mitra's protocol, operations are limited to multiplication and addition, paving the way towards a simple differential analysis of exchanged messages, and showing its lack of resistance to cloning and traceability attacks. Additionally, a full disclosure attack, which involves all the aforemention attacks, can be implemented with a high probability of success by applying some simple results from Number Theory. Qingling et al.'s protocol is on the other hand based on a CRC function and bitwise operations as dictated by the Gen-2 specification. The security of this scheme resides in the strength provided by CRC functions. However, the authors are not aware that CRCs are linear. These functions should be confined only to detect random transmission errors and must not be used for security purposes. Qingling et al. even included a formal BAN logic analysis in their paper. The whole analysis presented is incorrect because it assumes that a secure encryption algorithm is used in the protocol. However, the use of the combination $CRC() \oplus password$ is not at all secure, as shown in Section 5.

References

1. Mitra, M.: Privacy for RFID systems to prevent tracking and cloning. International Journal of Computer Science and Network Security **8**(1) (January 2008) 1–5
2. Qingling, C., Yiju, Z., Yonghua, W.: A minimalist mutual authentication protocol for RFID system & BAN logic analysis. In: Proc. of CCCM'08, IEEE Computer Society (2008) 449–453
3. Hopper, N.J., Blum, M.: Secure human identification protocols. In: Proc. of ASIACRYPT'01. Volume 2248 of LNCS., Gold Coast, Australia, Springer-Verlag (2001) 52–66
4. Juels, A., Weis, S.: Authenticating pervasive devices with human protocols. In: Proc. of CRYPTO'05. Volume 3126 of LNCS., IACR, Springer-Verlag (2005) 293–308
5. Chien, H.Y.: SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE Trans. Dependable Secur. Comput. **4**(4) (2007) 337–340
6. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In: Workshop on Information Security Applications. Volume 5379 of LNCS., Jeju Island, Korea, Springer-Verlag (September 2008)
7. EPCglobal: Class-1 generation 2 UHF air interface protocol standard version 1.2.0: "Gen 2". http://www.epcglobalinc.org/standards/ (2008)
8. Chien, H., Chen, C.: Mutual authentication protocol for RFID conforming to EPC class-1 generation-2 standards. Computer Standards and Interfaces, Elsevier Science Publishers **29**(2) (2007) 254–259
9. Han, D., Kwon, D.: Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 Standards. Computer Standards and Interfaces, Elsevier Science Publishers **31**(4) (2009) 648–652
10. Lim, T., Li, T.: Addressing the weakness in a lightweight RFID tag-reader mutual authentication scheme. In: Proc. of the IEEE Int'l Global Telecommunications Conference - GLOBECOM'07, IEEE Computer Society Press (2007) 59–63
11. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard. Computer Standards and Interfaces, Elsevier Science Publishers **31**(2) (2009) 372–380
12. Juels, A., Weis, S.: Defining strong privacy for RFID. In: Proc. of PerCom 2007, IEEE Computer Society Press (2007) 342–347
13. Phan, R.: Cryptanalysis of a new ultralightweight RFID authentication protocol - SASI. Dependable and Secure Computing, IEEE Transactions on **DOI: 10.1109/TDSC.2008.33** (2008)
14. EPCglobal: EPC Tag data standard version 1.4. http://www.epcglobalinc.org/standards/ (2008)
15. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Sixth edn. Oxford University Press (2008)
16. Anarchriz: CRC and how to reverse it. http://www.woodmann.com/fravia/crctut1.htm (1999)
17. Ranasinghe, D.C.: Lightweight Cryptography for Low Cost RFID. In: Networked RFID Systems and Lightweight Cryptography. Springer (2007) 311–346