Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **4**, October **2014**

Pitfalls in an ECC-based Lightweight Authentication Protocol for Low-Cost RFID

Chien-Ming Chen[1,2,a], Shuai-Min Chen[3,b], Xinying Zheng[1,c]
Lijun Yan[1,d], Huaxiong Wang[4,e], and Hung-Min Sun[3,f]

[1]Innovative Information Industry Research Center
School of Computer Science and Technology
Shenzhen Graduate School, Harbin Institute of Technology
Shenzhen, 518055, China

[2]Shenzhen Key Laboratory of Internet Information Collaboration
Shenzhen, 518055, China

[3]Department of Computer Science
National Tsing Hua University
Hisnchu, 30013, Taiwan, R.O.C.

[4]Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore

[a]dr.chien-ming.chen@ieee.org, [b]sean@is.cs.nthu.edu.tw, [c]xinying_15@163.com,
[d]yanlijun@126.com, [e]hxwang@ntu.edu.sg, [f]hmsun@cs.nthu.edu.tw

Received October, 2013; revised November, 2013

Abstract. *RFID technology has become popular in many applications; however, most of the RFID products lack security related functionality due to the hardware limitation of the low-cost RFID tags. In 2009, Chien and Laih proposed an RFID authentication protocol based on error correction codes (ECC) to secure RFID systems with untraceability, which is one of the most critical privacy issues on RFID. In this paper, we demonstrate that their scheme is insecure against two kinds of tracing attacks. We also analyze the success probability of our attacks.*

Keywords: RFID, Security, Privacy , Error correction code

1. **Introduction.** RFID (**R**adio **F**requency **ID**entification) is a technique used to identify objects via radio frequency. It has became very popular in many applications such as access control systems, supply chain management systems, transportation, ticketing systems, animal identification and industrial electronics.

Although RFID technology brings people a convenient life, security and privacy issues are still been concerned mostly in RFID applications. As a result, researchers have proposed many RFID protocol to achieve several security requirements. However, with limited computational ability and insufficient memory storage on its embedded chip, low-cost RFID protocol design still remains a challenge. Previous studies showed that the number of logic gates available for security functionality on a low-cost RFID tag is 400 to 4000[1], which is not enough to implement most public key or symmetric key cryptosystems. Therefore, an RFID protocol should be as computationally lightweight as possible.

In 2009, Chien and Laih[2] proposed an error correction code based RFID protocol to secure RFID systems with mutual authentication, untraceability, anonymity and resistance to denial-of-service attacks. Since the protocol requires only pseudo random number generators and simple bit operations, it is lightweight enough to be implemented on low-cost RFID tags. Unfortunately, we found their scheme is not as secure as they claimed.

In this paper, we demonstrate that Chien and Liah's protocol[2] is vulnerable to two kinds of tracing attacks. Our attacks are able to correlate two messages and determine if both of them were generated from the same tag. Hence, with this information, an attacker can trace the tag and eavesdrop on messages. This violates privacy by leaking the tag owner's location. We also analyze the success probability of our attacks.

2. **Related Work.** With the rapidly growth of network technology, security issues have been concerned in various network environments [3, 4, 5, 6, 7, 8, 9]. In the RFID environment, security and privacy issues also receive increasing attention recently.

Lightweight authentication protocols for RFID aim to achieve mutual authentication through simple operations like bitwise XOR and binary addition. In 2005, Juels and Weis proposed a multi-round lightweight authentication protocol called HB$^+$[10], which is an improvement of *HumanAut*, a human-to-computer authentication protocol designed by Hopper and Blum[11]. Nevertheless, Gilbert and Robshaw proved that the HB$^+$ protocol is vulnerable to a man-in-the-middle attack[12]. There are currently many improvements of the HB$^+$ protocol. For example, the HB^{++} protocol proposed by Bringer *et al.* in 2006[13], the HB-MP protocol proposed by Munilla and Peinado in 2007[14], and the HB# protocol proposed by Gilbert *et al.* in 2008[15].

On the other hand, the protocols using only simple bitwise operations on the tags are called ultralightweight protocols. [16, 17]. In 2007, Chien proposed an ultralightweight RFID authentication protocol:[18]. Initially, each tag shares a static identification, a pseudonym and two keys with the server. However, studies[19, 20] showed that SASI is vulnerable to desynchronizing and tracing attacks. In 2012, Tian et al.[21] proposed a new ultra-lightweight RFID protocol named RAPP. RAPP utilize a new bitwise operation called permutation in the protocol. The authors claimed that RAPP can withstand various attacks and provide strong data confidentiality and integrity. Unfortunately, several research have demonstrate that RAPP[22, 23, 24, 25] is vulnerable various kinds of attacks.

3. **Reviewing Chien-Laih's Protocol.** There are three entities in their protocol, a backend database server S, an RFID reader R, and a set of tags T. It is assumed that the communication channel between the server and the reader is secure, but the wireless communication channel between the reader and the tags is insecure. Each tag is assigned with a unique identity, denoted by T_i. Initially, S publishes a random number generator $g()$ and constructs a secret linear code $C(n, k, d)$ over $GF(2)$, which is specified by a generator matrix G. For each tag T_i, S assigns s row vectors $G[j]$ into it, where $j = (i-1) \times s + 1, \ldots, i \times s$. Then S stores the corresponding information of each tag in its database, including the tag's identity T_i, a secret key k_i and the indices of the assigned rows of G. Finally, S writes $g()$, T_i, k_i and the corresponding row vectors $G[j]$ into the memory of T_i. The detailed steps of Chien-Laih's protocol are listed as follows.

1. R sends a query to T_i by a random challenge N_R.

2. T_i randomly generates a non-zero codeword C_i from the pre-assigned row vectors, and randomly chooses an error vector e with Hamming weight $t = \lfloor (d-1)/2 \rfloor$. T_i then computes the masked codeword $\tilde{C}_i = C_i + e$ and a verifier message $\tilde{V}_T =$

```
1. $R \longrightarrow T$ : Send a query to $T_i$ by a random number $N_R$
2. $T$                   : Randomly generate a non-zero codeword $C_i$ from the assigned row vectors.
                           Randomly choose $e$ with Hamming weight $t$.
                           Compute $\tilde{C_i} = C_i + e$ and $\tilde{V_T} = g(e \oplus g(N_R \oplus k_i))$
                           Choose two random numbers $(\hat{C_i}, \hat{V_T})$ that
                           have the same bit length as that of $(\tilde{C_i}, \tilde{V_T})$
3. $R \longleftarrow T$  : Randomly arrange the order of $\{(\tilde{C_i}, \tilde{V_T}), (\hat{C_i}, \hat{V_T})\}$ and send to the reader.
4. $R$                   : For each set from $\{(\tilde{C_i}, \tilde{V_T}), (\hat{C_i}, \hat{V_T})\}$, decode $C_i$ to derive $(m_i, e)$
                           Use $m_i$ to identify $T_i$ and $K_i$
                           IF $V_T = g(e \oplus g(N_R \oplus k_i))$ is correct
                             Compute $V_S = g(N_R \oplus g(e \oplus k_i))$
                           ELSE
                             Set $V_S$ = random value
5. $R \longrightarrow T$ : $V_S$
6. $T$                   : Verify if $V_S = g(N_R \oplus g(e \oplus k_i))$ or not
```

Figure 1. Chien's ECC-Based Protocol

$g(e \oplus g(N_R \oplus k_i))$. After that, T_i generates a meaningless random number set $(\hat{C_i}, \hat{V_T})$, which has the same bit length as $(\tilde{C_i}, \tilde{V_T})$. Finally, T_i randomly determines the order of the two messages $\{(\tilde{C_i}, \tilde{V_T}), (\hat{C_i}, \hat{V_T})\}$, and sends this message set to R.

3. R decodes both masked codewords of the received message set $\{(\tilde{C_i}, \tilde{V_T}), (\hat{C_i}, \hat{V_T})\}$. Since only one message from the set is meaningful, R can derive exactly one plaintext m_i and error vector e from $\tilde{C_i}$. Then, R uses m_i to search the lookup table for the corresponding T_i and k_i from the database in S. After that, R checks if the condition $\tilde{V_T} = g(e \oplus g(N_R \oplus k_i))$ holds. If any one of the sets satisfies the condition, R computes a verified message $V_S = g(N_R \oplus g(e \oplus k_i))$; otherwise, R sets V_S as a random number. Finally, R sends V_S to T_i.

4. T_i authenticates R by checking whether the received V_S is equal to $g(N_R \oplus g(e \oplus k_i))$.

In Chien-Laih's protocol, each tag can generate $2^s - 1$ non-zero codewords. Since every tags store distinct row vectors of G, their set of codewords is disjoint. According to the authors' claim, an adversary may try to collect all the codewords from a tag and use them to trace the tag. To prevent this happening, a set of random numbers $(\hat{C_i}, \hat{V_T})$ is added in each session to confuse the adversary.

4. **Crypoanalysis on Chien-Laih's Protocol.** The tracing attack means the adversary correlates a previous obtained message with the currently eavesdropped one, and determine whether they are generated from the same tag or not. If these two messages are the same or from the same codeword set, it means the tag nearby right now is the same with the previous known tag. With more readers being placed in different locations, the adversary can continuously trace the movements of tags till it received a specific tag's response. Moreover, because tags are carried by human, the tracing of the tags is equal to trace its possessor. This violates the serious problem of location privacy of users. In this section, a basic version of our tracing attack is proposed. We also provide a variant attack which will be applied to different application scenario. For example, when a tag attached to a book borrowed from a library is traced by an attacker, the privacy of the

borrower would be invaded. Another example is that if a thief can trace a tag-attached valuable item stored inside a public locker, then the thief would break the locker and steal that valuable item.

4.1. **A Tracing Attack.** The goal of our attack is to trace a specific target tag T_X without invoking any valid R or S. We first state the fundamental theorem (Theorem 1) used in our attack scenario.

Theorem 4.1. *For any two codewords $C_i, C_j \in C(n,k,d)$, the Hamming weight of $(C_i + e_i) + (C_j + e_j) \leq 2t$ if $C_i = C_j$, where e_i and e_j are error vectors with each Hamming weight $\leq t$.*

Proof. Let Hw() be the Hamming weight function. If $C_i = C_j$, $\mathrm{Hw}((C_i+e_i)+(C_j+e_j)) = \mathrm{Hw}(e_i + e_j) \leq \mathrm{Hw}(e_i) + \mathrm{Hw}(e_j) \leq 2t$. □

Recall that every two tags always generate distinct codewords since each of them stores distinct row vectors of G, and the number of codewords of a tag is limited to $2^s - 1$, where Chien and Laih suggest $s = 3$. In other words, a tag only stores 7 different codewords to use alternatively. Thus, it is likely that a codeword may be used more than once. We apply Theorem 4.1 to determine if these two masked codewords are generated from the same codeword. If the answer is true, we can conclude that these two masked codewords have a higher probability being generated from the same tag, and hence Chien-Laih's scheme fails to defend against the tracing attack. Based on the above idea, our tracing attack is as follows:

1. An adversary A eavesdrops on the communication channel between a valid reader R and its target tag T_X. When R reads T_X, A records the message set generated by T_X during Step 2 of Chien-Laih's protocol as $MS_X = \{(\bar{C}_{X,1}, \bar{V}_{X,1}), (\bar{C}_{X,2}, \bar{V}_{X,2})\}$.
2. For a time being after eavesdropping on the message, A uses its reader to broadcast queries here and there. Assume A receives a response message set $MS = \{(\bar{C}_{i,1}, \bar{V}_{i,1}), (\bar{C}_{i,2}, \bar{V}_{i,2})\}$ from a tag T_i.
3. A checks if the inequality $\mathrm{Hw}(\bar{C}_{X,j} + \bar{C}_{i,k}) \leq 2t$ holds for all $j, k = 1, 2$. If there exists two messages $\bar{C}_{X,j}$ and $\bar{C}_{i,k}$ that satisfies the inequality, the attack process is finished.
4. If there is no such message satisfying the inequality, repeat Step 2 and Step 3.

By broadcasting query messages rapidly, the adversary is able to collect the response message sets and determine if the target tag is nearby. If T_i is right the one of the target tag T_X, the received messages $\bar{C}_{i,k}$ and $\bar{C}_{X,j}$ must be generated from the same codeword by Theorem 4.1. The location privacy of the carrier is leaking. This concludes that our tracing attack is successful.

On the other hand, the Hamming weight of $(C_i + e_i) + (C_j + e_j)$ will be less than or equal to $2t$ even if $C_i \neq C_j$ under certain situations. Therefore, the attacker may misjudge another tag's response as the target one. This situation will occur whenever the error vectors satisfy some specific patterns. Denote $C' = C_i + C_j$ as a vector whose Hamming weight is not less than d and the vector $e' = e_i + e_j$ whose Hamming weight is t. There will be at least d bits and t bits of '1's in C' and e', respectively. Imagine that when these two vectors are combined together, any overlap on these '1's will reduce the Hamming weight of $C' + e' = (C_i + e_i) + (C_j + e_j)$ by 1, while in any position where the bit values in C' and e' are distinct, the Hamming weight will increase by 1. Eventually, if there are at least $x = \lfloor \frac{t}{2} \rfloor + 1$ bits overlaps, the Hamming weight of $(C_i + e_i) + (C_j + e_j)$ will be smaller than or equal to $2t$. The probability of this situation can be expressed as

$\frac{\sum_{i=x}^{t}(\binom{d}{i}\binom{n-d}{t-i})}{\binom{n}{t}}$. Recall that $x = \lfloor\frac{t}{2}\rfloor + 1$, d is the minimum Hamming distace, n is the code word length, and $t = \lfloor(d-1)/2\rfloor$. Briefly, we take the parameter set suggested by Chien and Laih as an example, this situation will occur with the probability 1.53×10^{-24}, which is relatively small and negligible. In other words, our tracing attack will succeed for a higher probability.

4.2. **A Variant Tracing Attack.** To reduce failure matching of the target tag, we propose another attack method as follows. Due to the mobility of the carrier, the target tag may be out of the reading range of an attacker's reader. Therefore, another attack scenario is provided. If the attacker finds a still (not moving) tag and decides to trace this tag as target hereafter. Now A continuously queries the tag; therefore, the tag will respond messages every time the attacker queries it. By this method, the attacker is able to collect as many messages as possible. Note that, although the responding message may be repeated according to the protocol, the attacker can query the tag again and again. Assume A by some means had repeated Step 1 of the basic attack and collected more message sets from the target tag T_X, denoted by $MS_{X,i}, i = 1, 2, \ldots$. For the time being, in Step 3, A compares the received message set MS with all message sets in $MS_{X,i}$, rather than just a single message set MS_X. The success probability of this tracing attack is increased with the amount of message sets that A had collected previously.

5. **Analysis.** Here we analyze the success probability of our attacks. Note that A is with a high probability to determine whether two masked codewords are generated from the same codeword set by applying Theorem 4.1. Therefore, a successful attack mainly depends on the case that a codeword is reused.

Our tracing attack will succeed whenever the number of times the adversary repeats Step 2 and Step 3 of our basic attack equals the number of repeated codeword used. Because memory space is limited on low-cost RFID tags and only few row vectors of G can be stored on a single tag; thus, the size of possible codewords set is bounded to a small number. In[2], the authors suggested $C(n = 2048, k = 1289, d = 139)$ and $s = 3$ as reasonable parameters. That is, a tag can only produce 7 codewords, so the probability of a codeword being reused is high. Therefore, a successful attack just requires repeating Step 2 and Step 3 for a few rounds.

For our variant attack, the success probability relies on the number of different codewords collected at Step 1. Here we adopt the formula of inclusion and exclusion. The principle of inclusion and exclusion is to find out the total number that each case appeared at least once. Let N be the number of masked codewords that A has collected from T_X, the probability that each codeword has appeared at least once is $\frac{\sum_{i=0}^{l}((-1)^i \times \binom{l}{i} \times (l-i)^N)}{l^N}$, where $l = 2^s - 1$. If $s = 3$, the success probability will exceed 0.5 when $N \geq 17$. When $N = 40$, the probability of success is increased to 0.98. Notice that A can collect all the information she needs when the target tag is nearby, and once she has acquired all these codewords, she can launch a successful tracing attack by sending a single query to the tag. This variant attack is more appropriate in most RFID applications.

On the other hand, the Hamming weight of $(C_i+e_i)+(C_j+e_j)$ will be less than or equal to $2t$ even if $C_i \neq C_j$. Therefore, the attacker may mistake another tag's response as the targeted one. This situation occurs whenever the error vectors satisfy specific patterns. Denote vector $C' = C_i + C_j$ whose Hamming weight is not less than d and the vector $e' = e_i + e_j$ whose Hamming weight is t. There will be at least d bits and t bits of '1's in C' and e', respectively. Imagine when these two vectors are combined together, any overlap on these '1's will reduce the Hamming weight of $C' + e' = (C_i + e_i) + (C_j + e_j)$ by 1, while in any position where the bit values in C' and e' are distinct, the Hamming weight will increase by 1. Eventually, if there are at least $x = \lfloor \frac{t}{2} \rfloor + 1$ bits overlaps, the Hamming weight of $(C_i + e_i) + (C_j + e_j)$ will be less than or equal to $2t$. The probability of this situation can be express as $\frac{\sum_{i=x}^{t}\left(\binom{d}{i}\binom{n-d}{t-i}\right)}{\binom{n}{t}}$. Taking the parameter set suggested by Chien as an example, the probability is 1.53×10^{-24}, which is a relatively small value.

Furthermore, since $\tilde{V_T}$ is generated from hash function, there exists a small probability that the value decoded from the meaningless random message just matches with the valid codeword set. In this case, our tracing attack seems to have failed since the adversary recognizes another tag's message as her target one. However, this situation will occur only with the probability $\frac{(2^s - 1) \times \binom{n}{t}}{2^n}$, which is negligible when a larger n is chosen. Taking Chien-Laih's parameter set as the example again, the probability is 1.51×10^{-161}. This is undoubtedly a negligible value.

6. **Conclusions.** Security and privacy issues on RFID have been studied in recent years due to the rapid growth of RFID systems. In this paper, we show that Chien and Liah's protocol is vulnerable to two kinds of tracing attacks. The goal of tracing attack is to discover the presence of a specific tag. According to our analysis, our tracing attack will succeed for a higher probability.

Acknowledgement. The work of C.-M. Chen was supported in part by the Shenzhen Peacock Project, China, under Contract KQC201109020055A, and in part by Shenzhen Strategic Emerging Industries Program under Grant ZDSY20120613125016389. The work of H.-M. Sun was supported in part by the National Science Council, Taiwan, R.O.C., under Grant NSC 101-2221-E-007-026-MY3. The corresponding author is Prof. Hung-Min Sun.

REFERENCES

[1] D. Ranasinghe, D. Engels, and P. Cole, Low-Cost RFID systems: confronting security and privacy, *Auto-ID Labs Research Workshop*, pp. 54-77, 2004.

[2] H.-Y. Chien and C.-S. Laih, ECC-based lightweight authentication protocol with untraceability for Low-Cost RFID, *Journal of Parallel and Distributed Computing*, vol. 69, no. 10, pp. 848-853, 2009.

[3] T.-Y. Wu and Y.-M. Tseng, Further analysis of pairing-based traitor tracing schemes for broadcast encryption, *Security and Communication Networks*, vol. 6, no. 1, pp. 28-32, 2013.

[4] C.-M. Chen, K.-H. Wang, T.-Y. Wu, J.-S. Pan, and H.-M. Sun, A scalable transitive humanverifiable authentication protocol for mobile devices, *IEEE Trans. Information Forensics and Security*, vol. 8, no. 8, pp. 1318-1330, 2013.

[5] T.-Y. Wu and Y.-M. Tseng, Publicly verifiable multi-secret sharing scheme from bilinear pairings, *IET Information Security*, vol. 7, no. 3, pp. 239-246, 2013.

[6] T.-P. Hong, C.-W. Lin, K.-T. Yang, and S.-L.Wang, Using tf-idf to hide sensitive itemsets, *Applied Intelligence*, pp. 1-9, 2013.

[7] C.-M. Chen, Y.-H. Chen, Y.-H. Lin, and H.-M. Sun, Eliminating rouge femtocells based on distance bounding protocol and geographic information, *Expert Systems with Applications*, vol. 41, no. 2, pp. 426-433, 2014.

[8] H.-M. Sun, H. Wang, K.-H. Wang, and C.-M. Chen, A native apisprotection mechanism in the kernel mode against malicious code, *IEEE Trans. Computers*, vol. 60, no. 6, pp. 813-823, 2011.

[9] C.-M. Chen, Y.-H. Lin, Y.-C. Lin, and H.-M. Sun, Rcda: recoverable concealed data aggregation for data integrity in wireless sensor networks, *IEEE Trans. Parallel and Distributed Systems*, vol. 23, no. 4, pp. 727-734, 2012.

[10] A. Juels and S. Weis, Authenticating pervasive devices with human protocols, *Advances in Cryptology-CRYPTO 2005*, vol. 3621, pp. 293-308, 2005.

[11] N. Hopper and M. Blum, Secure human identification protocols, *Proc. of the 7th International Conference on Theory and Application of Cryptology and Information Security*, pp. 52-66, 2001.

[12] H. Gilbert, M. Robshaw, and H. Sibert, Active attack against HB$^+$: a provably secure lightweight authentication protocol *IEEE Electronics Letters*, vol. 41, no. 21, pp. 1169-1170, 2005.

[13] J. Bringer, H. Chabanne, E. Dottax, and S. Securite, HB^{++}: a lightweight authentication protocol secure against some attacks, *Proc. of the 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, pp. 28-33, 2006.

[14] J. Munilla and A. Peinado, HB-MP: a further step in the HB-Family of lightweight authentication protocols, *Computer Networks*, vol. 51, no. 9, pp. 2262-2267, 2007.

[15] H. Gilbert, M. Robshaw, and Y. Seurin, HB#: Increasing the Security and Efficiency of HB+, *Proc. of the 27th International Conference on Theory and Applications of Cryptographic Techniques*, pp. 361-378, 2008.

[16] T. Li and R. Deng, Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol, *Proc. of the 2nd International Conference on Availability, Reliability and Security*, pp. 238-245, 2007.

[17] T. Li and G. Wang, Security analysis of two Ultra-Lightweight RFID authentication protocols, *Proc. of the IFIP TC-11 22nd International Information Security Conference*, vol. 232, pp. 109-120, 2007.

[18] H.-Y. Chien, SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity, *IEEE Trans. on Dependable and Secure Computing*, vol. 4, no. 4, pp. 337-340, 2007.

[19] H.-M. Sun, W.-C. Ting, and K.-H. Wang, On the security of Chiens ultralightweight RFID authentication protocol, *IEEE Trans. on Dependable and Secure Computing*, vol. 8, no. 2, pp. 315-317, 2009.

[20] R.-W. Phan, Cryptanalysis of a new ultralightweight RFID authentication protocol-SASI, *IEEE Trans. on Dependable and Secure Computing*, vol. 6, no. 4, pp. 316-320, 2009.

[21] Y. Tian, G. Chen, and J. Li, A new ultralightweight rfid authentication protocol with permutation, *IEEE Communications Letters*, vol. 16, no. 5, pp. 702-705, 2012.

[22] G. Avoine and X. Carpent, Yet another ultralightweight authentication protocol that is broken, *Radio Frequency Identication. Security and Privacy Issues*, Springer,Berlin-Heidelberg, Germany, pp. 20-30, 2013.

[23] W. Shao-hui, H. Zhijie, L. Sujuan, and C. Dan-wei, Security analysis of rapp an rfid authentication protocol based on permutation, Cryptology ePrint Archive, Report 2012/327, Technology Report, 2012.

[24] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, Desynchronization attack on rapp ultralightweight authentication protocol, *Information processing letters*, vol. 113, no. 7, pp. 205-209, 2013.

[25] X. Zhuang, Z.-H. Wang, C.-C. Chang, and Y. Zhu, Security analysis of a new ultra-lightweight rfidprotocol and its improvement, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 3, 2013.