INFORMATICA, 2013, Vol. 24, No. 1, 1–12

Authentication Protocols for Reliable Information Provision Systems with Low Computational-Ability Devices

Ya-Fen CHANG[1], Wei-Liang TAI[2], Chia-Chen CHEN[3] *

[1]*Department of Computer Science and Information Engineering*
National Taichung University of Science and Technology, Taichung, Taiwan
[2]*Department of Information Communications, Chinese Culture University, Taipei, Taiwan*
[3]*Department of Management Information Systems, National Chung Hsing University*
No. 250, Kuo Kuang Rd., Taichung 402, Taiwan
e-mail: cyf@cs.ccu.edu.tw, taiwl@cs.ccu.edu.tw, tr.emily@gmail.com

Received: June 2011; accepted: July 2012

Abstract. Wireless communication techniques provide convenience for users to get desired information. Construction and management costs of information provision systems with low computational-ability devices, such as RFID devices, are low so lightweight authentication protocols are required for information security. In this paper, two lightweight authentication protocols are proposed for reliable information provision systems with low computational-ability devices. The first protocol is for public information, and the other ensures that only authorized users can get information.

Keywords: RFID, the LPN problem, wireless communications, NP-completeness.

1. Introduction

Nowadays, people are used to applying network applications to dealing with routines for convenience. Conventional services allow people to handle specific affairs remotely with computers, but people are constrained to stay in the place of computers. Wireless communications become a hot research topic for ubiquitous services. Pager, WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Area Network), Bluetooth, ZigBee, RFID (Radio Frequency Identity), 1G, 2G, 3G, GPRS, and 3.5G are common wireless communication techniques to provide different types of services.

Among the mentioned wireless communication techniques, RFID is popular to be used in plenty of applications. RFID tags, a reader and a back-end application system compose an RFID system. A reader is connected to the back-end application system, and a reader can obtain data stored in tags via wireless technologies (Finkenzeller, 2002). Thereupon, the back-end application system can use the received data. RFID tags are divided into two categories: (1) passive tags and (2) active tags. Passive RFID tags do

*Corresponding author.

not need batteries plugged. Instead, they transfer energy sent by the reader to operation power. Because of this special characteristic, passive RFID tags possess advantages of small size, low cost, and low power consumption. On the other hand, active RFID tags need batteries plugged such that their transmission range is further than passive ones.

Like other wireless technologies, RFID needs to withstand some security threats. Consequently, some cryptographic protocols for RFID systems were proposed (Ohkubo *et al.*, 2004; Sarma, *et al.*, 2002; Vajda and Buttyan, 2003; Weis *et al.*, 2004). These protocols aim to have only the legal reader get information stored in tags so the reader needs to be authenticated by tags. Hopper and Blum (2001) proposed a light-weight authentication protocol, HB protocol, based on the learning parity with noise (LPN) problem. Unlike previous protocols, only dot product operation of binary vectors is required in HB protocol such that its computation load is light. As a result, HB protocol suits devices with low computational-ability such as passive RFID tags. Juels and Weis (2005) showed that HB protocol could not defend against active attacks and proposed an improvement, HB+ protocol. However, Katz and Shin (2005) and Gilbert *et al.* (2005) indicated that HB and HB+ protocols are insecure. Bringer *et al.* (2006) and Piramuthu (2006) proposed modified HB+ protocol to resist attacks. Munilla and Peinado (2007) proposed HB-MP′ and HB-MP protocols to improve the computation load of HB+ protocol and to withstand active attacks. Munilla and Peinado claimed that HB-MP′ protocol was still vulnerable to man-in-the-middle attacks while HB-MP protocol could defend against active attacks.

Security of HB-family is based on the computational hardness of the LPN problem (Blum *et al.*, 1994), and it has been proven to be an NP-complete problem (Berlekamp *et al.*, 1978). However, Chang found that HB-MP protocol is insecure by showing how to cheat the verifier without solving the secret keys with high probability by mounting active attacks on it (Chang, 2010). With deep insight into Chang's attack, the security flaw results from regular operations on involved secret keys. To preserve the advantages of HB-family and overcome the possible threat, two LPN-problem-based authentication protocols are proposed for reliable information provision systems. The first proposed LPN-problem-based authentication protocol is for public information such that users can ensure the received information is reliable and correct. Public information provision systems suit application for free and public information – tourist guides for example. The other protocol is for information provided for only authorized users. User-specific information provision systems suit application for privileged or charged data access. Because systems of both types need to make their users believe that the obtained information is reliable, tags must be authenticated by the reader. In public information provision systems, the reader does not need to be authenticated by tags because the stored information is public and free. On the other hand, the reader needs to be authenticated by tags because the stored information is privileged or charged in the other information provision systems. That is, the second protocol for information provided for only authorized users ensures mutual authentication.

The remainder of this paper is organized as follows. Section 2 reviews the LPN problem, HB-MP protocol and the security flaw of HB-MP protocol. The proposed authentication protocols are shown in Section 3 followed by security analyses in Section 4. At last, some conclusions are drawn in Section 5.

2. Reviews of Related Works

The LPN problem, HB-MP protocol, and the security flaw of HB-MP protocol are reviewed in Sections 2.1 to 2.3, respectively.

2.1. *The LPN Problem*

Before giving the definition of the LPN problem, the concept of learning parity without noise and how to find the secret share are first introduced. The used notations are listed as follows:

x: a binary vector of length i;
y, z: binary vectors of length n;
g_k: binary vectors of length i, where $k \in [1, n]$;
A: a binary matrix composed of $g_1, g_2, \ldots, g_n$;
ν: noise, a 1-bit value, and $\nu = 1$ with probability $p \in [0, 1/2]$;
$\oplus$: XOR operation;
y_k: the dot product of $x \cdot g_k (\mathrm{mod}\, 2)$;
$x \cdot g_k$: the shorthand of $x \cdot g_k (\mathrm{mod}\, 2)$.

For simplicity, shorthand $x \cdot g_k$ for $x \cdot g_k (\mathrm{mod}\, 2)$ is used throughout this paper. A linear system with binary matrices A, x and y is as follows.

$$Ax = \begin{vmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{vmatrix} \cdot x = y.$$

When A and y are known and there is no noise, x can be solved by Gaussian elimination. When noise ν is taken into consideration, it is known as the LPN problem, which has been proven to be an NP-complete problem (Berlekamp *et al.*, 1978), and the time complexity to get x is $2^{O(n/\log n)}$ (Blum *et al.*, 2003). For given A, x, y and z, we have the followings.

$$y_k = x \cdot g_k,$$
$$z_k = y_k \oplus \nu.$$

According to the above two equations, the definition of the LPN problem is as follows.

The LPN problem. *With given g_k, z_k and the probability p, solve x.*

2.2. *A Review of HB-MP Protocol*

Munilla and Peinado (2007) proposed HB-MP protocol to withstand man-in-the-middle attack which HB-MP′ protocol suffered from. In HB-MP protocol, two secret keys are

shared by the tag and the reader. Moreover, the length of these shared secret keys is not the same as that of exchanged messages. Notations used in HB-MP protocol are as follows:

x, y: secret keys shared between the reader and the tag;
k: the length of shared secret keys x and y;
m: the length of exchanged messages;
x'_m: the m least significant bits of x', which is an m-bit binary vector;
a, b: random binary vectors of length m;
ν: random noise, a 1-bit value, $\nu = 1$ with probability $p \in [0, 1/2]$;
$\oplus$: XOR operation;
$a{\cdot}x$: the dot product of vectors a and x, which is the shorthand for $a{\cdot}x (\mathrm{mod}\ 2)$;
rotate(x, y_k): a bitwise left rotate operation denoting x is left rotated with y_k bits.

HB-MP protocol consists of q rounds. The ith round is shown as follows:

Step 1. The reader chooses and sends one random binary vector a of length m to the tag.
Step 2. After receiving the binary vector a, the tag computes $x' = \text{rotate}(x, y_i)$ and $z = a{\cdot}x'_m \oplus \nu$, where y_i is the ith bit of y. Then, the tag selects an m-bit binary vector b satisfying $b{\cdot}x'_m = z$ and sends b to the reader.
Step 3. After getting b, the reader computes $x' = \text{rotate}(x, y_i)$, where y_i is the ith bit of y, and checks whether $a{\cdot}x'_m = b{\cdot}x'_m$ holds or not.

After q rounds, the reader accepts the tag if $q * p$ or less rounds to verify b's are failed.

2.3. *Security Flaw of HB-MP Protocol*

In HB-family, HB, HB+ and HB-MP′ protocols have been proven to suffer from active attacks or man-in-the-middle attacks. Only HB-MP protocol was claimed to be secure (Chang, 2010). Chang found that HB-MP protocol is still vulnerable to active attacks even if two secret keys are used. In the following, how an attacker cheats the reader with high probability is demonstrated. Note that there are two secret keys x and y are shared between the reader and the tag in HB-MP protocol. In the ith round of HB-MP protocol, a tag and the reader need to compute $x' = \text{rotate}(x, y_i)$, where y_i denotes the ith bit of secret key y. If a malicious user wants to cheat the reader, he only needs to obtain where two consecutive zeros appear in x instead of knowing x thoroughly. The attack is as follows:

Step 1. The malicious user impersonates a RFID tag and guesses the jth and $(j-1)$th bits of x are zero. Note that $j - 1 = k$ when $j = 1$.
Step 2. After receiving the binary vector a from the RFID reader, the malicious user executes Chang's binary-vector-modification algorithm to get one binary vector b and sends b to the reader. Note that Step 2 will be executed q times.
Step 3. If the malicious user is authenticated by the reader successfully, it denotes that $x_j x_{j-1} = 00$ occurs with high probability. The malicious user regards $x_j x_{j-1} = 00$.

From now on, the malicious user can use Chang's binary-vector-modification algorithm to modify the binary vector a to cheat the RFID reader.

Chang's binary-vector-modification algorithm

Input: one m-bit binary vector $a = a_m a_{m-1} \dots a_1$ and position j and $(j-1)$, where $j-1=k$ if $j=1$
Output: one m-bit binary vector b

Step 1. Modify $a_j a_{j-1}$ to be $a'_j a'_{j-1}$.
Case 1: If $a_j a_{j-1} = 00$, $a'_j a'_{j-1} = 10$.
Case 2: If $a_j a_{j-1} = 01$, $a'_j a'_{j-1} = 11$.
Case 3: If $a_j a_{j-1} = 10$, $a'_j a'_{j-1} = 00$.
Case 4: If $a_j a_{j-1} = 11$, $a'_j a'_{j-1} = 01$.
Step 2: $b = a$.

3. Proposed Authentication Protocols

In this section, two LPN-problem-based authentication protocols are proposed for reliable information provision systems to preserve the advantages of HB-family and overcome the possible threat. The used notations are listed in Section 3.1. The first protocol for public information and the second protocol for information provided for only authorized users are shown in Sections 3.2 and 3.3, respectively.

3.1. *Notations*

x, y: secret keys shared between the reader and the tag;
k: the length of shared secret keys x and y;
m: the length of exchanged messages;
x'_m: the m least significant bits of x', which is an m-bit binary vector;
a, b, c, d: random binary vectors of length m;
ν: random noise, a 1-bit value, $\nu = 1$ with probability $p \in [0, 1/2]$;
$\oplus$: XOR operation;
$a{\cdot}x$: the dot product of vectors a and x, which is the shorthand for $a{\cdot}x \pmod 2$;
rotate(x, P_i): a bitwise left rotate operation denoting x is left rotated with P_i bits, where $P_i = \sum_{j=1}^{i} y_j$ and y_j is the jth bit of y.

3.2. *The Proposed Authentication Protocol for Public Information*

This protocol consists of q rounds. The ith round is illustrated in Fig. 1. The details are shown as follows:

Step 1. The reader randomly chooses and sends one binary vector a of length m to the tag.

Step 2. After getting a, the tag computes $x' = \text{rotate}(x, P_i)$ and $z = a{\cdot}x'_m \oplus \nu$, where $P_i = \sum_{j=1}^{i} y_j$ and y_j is the jth bit of y. Then, the tag selects an m-bit binary vector b such that $b \neq a$ and $b{\cdot}x'_m = z$ and sends b to the reader.

Step 3. After getting b, the reader first checks if $b \neq a$. If it holds, the reader computes $x' = \text{rotate}(x, P_i)$, where $P_i = \sum_{j=1}^{i} y_j$ and y_j is the jth bit of y, and checks whether $a{\cdot}x'_m = b{\cdot}x'_m$ holds or not.

After q rounds, the reader accepts the tag if $q * p$ or less rounds to verify b's are failed.

Reader		Tag
$x = x_k x_{k-1} \dots x_1$		$x = x_k x_{k-1} \dots x_1$
$y = x_k y_{k-1} \dots y_1$		$y = x_k y_{k-1} \dots y_1$
	$\xrightarrow{a}$	
		$x' = \text{rotate}(x, P_i)$
		$z = a{\cdot}x'_m \oplus \nu$
		choose $b \mid b{\cdot}x'_m = x$
	$\xleftarrow{b}$	
check if $b \neq a$		
$x' = \text{rotate}(x, P_i)$		
check if $a{\cdot}x'_m =? b{\cdot}x'_m$		
$q * p$ failures are accepted		

Fig. 1. The proposed authentication protocol for public information.

Reader		Tag
$x = x_k x_{k-1} \dots x_1$		$x = x_k x_{k-1} \dots x_1$
$y = x_k y_{k-1} \dots y_1$		$y = x_k y_{k-1} \dots y_1$
	$\xrightarrow{a}$	
		$x' = \text{rotate}(x, P_i)$
		$z = a{\cdot}x'_m \oplus \nu$
		choose $b \mid b{\cdot}x'_m = x$
	$\xleftarrow{b,c}$	
check if $b \neq a,\ c \neq a$ and $c \neq b$		
$x' = \text{rotate}(x, P_i)$		
$w = c{\cdot}x'_m \oplus \nu$		
choose $d \mid d{\cdot}x'_m = w$		
check if $a{\cdot}x'_m =? b{\cdot}x'_m$		
$q * p$ failures are accepted		
	$\xrightarrow{d}$	
check if $d \neq c$		
check if $d{\cdot}x'_m =? c{\cdot}x'_m$		
$q * p$ failures are accepted		

Fig. 2. The proposed authentication protocol for information provided for authorized users.

3.3. *The Proposed Authentication Protocol for Information Provided for Authorized Users*

This protocol consists of q rounds. The ith round is illustrated in Fig. 2. The details are shown as follows:

Step 1. The reader randomly chooses and sends one m-bit binary vector a to the tag.

Step 2. After getting a, the tag computes $x' = \text{rotate}(x, P_i)$ and $z = a{\cdot}x'_m \oplus \nu$, where

$P_i = \sum_{j=1}^{i} y_j$ and y_j is the jth bit of y. Then, the tag selects an m-bit binary vector b such that $b \neq a$ and $b{\cdot}x'_m = z$ and chooses a random m-bit binary vector c, where $c \neq a$ and $c \neq b$. The tag sends b and c to the reader.

Step 3. After getting b and c, the reader first checks if $b \neq a, c \neq a$ and $c \neq b$. If they all hold, the reader computes $x' = \text{rotate}(x, P_i)$ and $w = c{\cdot}x'_m \oplus \nu$, where $P_i = \sum_{j=1}^{i} y_j$ and y_j is the jth bit of y. The reader selects an m-bit binary vector d such that $d \neq c$ and $d{\cdot}x'_m = w$. The reader checks whether $a{\cdot}x'_m = b{\cdot}x'_m$ holds or not. The reader sends d to the tag.

Step 4. After getting d, the tag first checks if $d \neq c$. If it holds, the tag checks whether $d{\cdot}x'_m = c{\cdot}x'_m$ holds or not.

After q rounds, the reader accepts the tag if $q * p$ or less rounds to verify b's are failed, and the tag accepts the reader if $q * p$ or less rounds to verify d's are failed.

4. Security Analyses

In this section, security analyses of the proposed protocols are given by the following theorems.

Theorem 1. *A malicious user can be authenticated successfully in one round by modifying h bits of the challenge binary vector with probability $1/2$, where $1 \leqslant h \leqslant m$.*

Proof. A malicious user may modify h bits of the challenge binary vector a/c and send b/d to the other party, where $1 \leqslant h \leqslant m$. For $h = 1$, the attack may succeed in the following two cases.

Case 1-1: $v = 1$ and $x'_{m,r1} = 1$, where $x'_{m,r1}$ is the $r1$th bit of x'_m.

Case 1-2: $v = 0$ and $x'_{m,r1} = 0$.

The probability of Case 1-1 is $p \times 1/2 = p/2$, and that of Case 1-2 is $(1-p) \times 1/2 = (1-p)/2$. From above, we have the probability to authenticate the malicious user successfully is $1/2$ for $h = 1$. For $h = 2$, the attack may succeed in the following four cases.

Case 2-1: $v = 1, x'_{m,r1} = 0$, and $x'_{m,r2} = 1$, where $x'_{m,r2}$ is the $r2$th bit of x'_m.

Case 2-2: $v = 1, x'_{m,r1} = 1$, and $x'_{m,r2} = 0$.

Case 2-3: $v = 0, x'_{m,r1} = 0$, and $x'_{m,r2} = 0$.

Case 2-4: $v = 0, x'_{m,r1} = 1$, and $x'_{m,r2} = 1$.

The probability of Case 2-1 and Case 2-2 is $p \times 1/2 = p/2$, and that of Case 2-3 and Case 2-4 is $(1-p) \times 1/2 = (1-p)/2$. From above, we have the probability to authenticate the malicious user successfully is $1/2$ for $h = 2$. For $3 \leqslant h \leqslant m$, the attack may succeed in the following two cases.

Case 3-1: $v = 1$ and the number of $x'_{m,rj} = 1$ is odd, where $x'_{m,rj}$ is the rjth bit of x'_m and $1 \leqslant j \leqslant h$.

Case 3-2: $v = 0$ and the number of $x'_{m,rj} = 1$ is even.

The probability of Case 3-1 is $p \times \frac{C_1^h + C_3^h + \cdots + C_{\lceil \frac{h}{2} \rceil \times 2-1}^h}{2^h} = p \times 1/2 = p/2$, and that of Case 3-2 is $(1-p) \times \frac{C_0^h + C_2^h + \cdots + C_{\lfloor \frac{h}{2} \rfloor \times 2}^h}{2^h} (1-p) \times 1/2 = (1-p)/2$. From above, we have the probability to authenticate the malicious user successfully is $1/2$ for $3 \leqslant h \leqslant m$. From above, we have the probability of a malicious user can be authenticated successfully in one round by modifying h bits of the challenge binary vector with probability $1/2$, where $1 \leqslant h \leqslant m$.

Theorem 2. *A malicious user can be authenticated successfully by modifying h bits of the challenge binary vector with probability at most $1/2$, where $1 \leqslant h \leqslant m$.*

Proof. In each round, $x' = \text{rotate}(x, P_i)$, $z = a \cdot x'_m \oplus \nu$, and $b \cdot x'_m = z$, where $\nu = 1$ with probability p and $P_i = \sum_{j=1}^{i} y_j$. For $j = 1$ to k, $\Pr[y_j = 1]$ is $1/2$, where $\Pr[E]$ denotes the probability of the specific event E. Thus, $\Pr P_i = P_{i-1}] = \Pr[P_i \neq P_{i-1}] = 1/2$. When a malicious user wants to mount attack, he needs to modify the binary vector a in the ith round. In the $(i-1)$th round, rjth bits of a are modified, where $1 \leqslant j \leqslant h$. In the ith round, the malicious user has two chooses. (1) Modify $(rj+1)$th bits of a4 (2) Modify rjth bits of a. Note that a's in different rounds are different. In the ith round, the malicious user can be authenticated successfully in the following four cases.

Case 4-1: Modify $(rj+1)$th bits of a when $P_i \neq P_{i-1}$ and the result of the $(i-1)$th round is correct.

Case 4-2: Modify $(rj+1)$th bits of a when $P_i = P_{i-1}$ and the result of the $(i-1)$th round is wrong.

Case 4-3: Modify rjth bits of a when $P_i \neq P_{i-1}$ and the result of the $(i-1)$th round is wrong.

Case 4-2: Modify rjth bits of a when $P_i = P_{i-1}$ and the result of the $(i-1)$th round is correct.

According to Theorem 1, the probability for the attacker to be authenticated successfully in one round is $1/2$. After q rounds, authentication is successful when $q * p$ or less rounds to verify b's are failed. Thus, the success probability is

$$\frac{C_q^q + C_{q-1}^q + \cdots + C_{q-\lfloor q \times p \rfloor}^q}{2^q} \leqslant \frac{C_q^q + C_{q-1}^q + \cdots + C_{\lceil q/2 \rceil}^q}{2^q}$$
$$= \frac{(C_0^q + C_q^q)/2 + (C_1^q + C_{q-1}^q)/2 + \cdots + (C_{\lceil q/2 \rceil}^q + C_{q-\lceil q/2 \rceil}^q)/2}{2^q} \approx 1/2.$$

Theorem 3. *A malicious user can be authenticated successfully by mounting reflection attack with probability* 0.

Proof. Reflection attack is a special case of relay attack. Via this attack, an attacker sends a received challenge to the verifier immediately for authentication. In the first authentication protocol, the reader checks if $b \neq a$ to prevent an attacker from sending the challenge back immediately. If an attacker sends the challenge a to the reader immediately, the authentication protocol will be terminated instantly.

In the second authentication scheme, the reader first checks if $b \neq a,\ c \neq a$ and $c \neq b$ to prevent an attacker from sending the challenge a back immediately. The tag's challenge c satisfying $c \neq a$ and $c \neq b$ makes no malicious user send b or a immediately to the tag for successful authentication as a legal reader. After getting the response d for a challenge c, the tag checks if $d \neq c$ to prevent an attacker from sending the challenge c immediately. If a challenge and the corresponding response are the same, the authentication protocol will be terminated instantly.

By above analyses, an attacker cannot be authenticated successfully by sending a received challenge back to a verifier immediately because the verifier checks whether a challenge and its response are equal while receiving the response. The probability that a malicious user is authenticated successfully by mounting reflection attack is 0.

Theorem 4. *A malicious user has no advantage to be authenticated successfully by mounting replay attack after gathering previous authentication challenges and corresponding responses.*

Proof. An attacker may intercept challenges and responses in a number of authentication sessions. Noise $\nu = 1$ with probability p so each challenge-response pair yields a successful authentication round with probability $(1 - p)$. Suppose α gathered challenge-response pairs are applied for one authentication session because the fresh challenges are the same as those of gathered challenge-response pairs. By Theorem 1, the attacker only can send a correct response back with probability $1/2$ in the other $(q - \alpha)$ rounds. Note that $(q - \alpha) = 0$ with probability τ which is negligible. Because the probability p of $\nu = 1$ is in $[0, 1/2]$, the probability of a challenge-response pair to yield a successful authentication round is in $[1, 1/2]$. When $p = 1/2$, the probability that an attacker can be authenticated successfully is $\frac{C_q^q + C_{q-1}^q + \cdots + C_{\lceil q/2 \rceil}^q}{2^q} \approx 1/2$. When $p = 1$, the probability that an attacker can be authenticated successfully is $\frac{1}{2^{q-\alpha}}$. From above, we have the probability β that an attacker can be authenticated successfully by mounting replay attack after gathering previous authentication challenges and corresponding responses is in $[\frac{1-\tau}{2^{q-\alpha}} + \tau, 1/2]$. By Theorem 2, a malicious user can be authenticated successfully by modifying h bits of the challenge binary vector with probability at most $1/2$, where $1 \leqslant h \leqslant m$. The advantage for an attacker to be authenticated successfully by mounting replay attack after gathering previous authentication challenges and corresponding responses can be presented by $\mathrm{Adv}_1[\beta] = (\beta - 1/2) \times 2$. By this transformation, we formalize the advantage of the specific attack such that the result is in $[-1, 1]$. When the result is in (0, 1], it denotes that an attacker has advantage. When the result is in $[-1, 0]$, it denotes that an attacker has no advantage. Because β is in $[\frac{1-\tau}{2^{q-\alpha}} + \tau, 1/2]$ and $\frac{1-\tau}{2^{q-\alpha}} + \tau \approx \frac{1}{2^{q-\alpha}}$, $\mathrm{Adv}_1[\beta]$ is in $[\frac{1}{2^{q-\alpha-1}} - 1, 0]$. Because $(q - \alpha) \neq 0$, $\mathrm{Adv}_1[\beta]$ is in $[-1, 0]$ such that the attacker has no advantage to be authenticated successfully by mounting replay attack after gathering previous authentication challenges and corresponding responses.

Theorem 5. *A malicious user has no advantage to retrieve secrets.*

Proof. By Theorem 1, an attacker can be authenticated successfully in one round by modifying h bits of the challenge binary vector with probability $1/2$, where $1 \leqslant h \leqslant m$. By Theorem 2, an attacker can be authenticated successfully in one authentication session by modifying h bits of the challenge binary vector with probability at most $1/2$, where $1 \leqslant h \leqslant m$. By modifying the challenge binary vector, the attacker can obtain some information of secrets. The probability for an attacker to be authenticated successfully by sending a random response in one round is $1/2$. The probability for an attacker to be authenticated successfully by sending a random response in one authentication session is $\frac{C_q^q+C_{q-1}^q+\cdots+C_{q-\lfloor q\times p\rfloor}^q}{2^q} \leqslant \frac{C_q^q+C_{q-1}^q+\cdots+C_{\lceil q/2\rceil}^q}{2^q} = \frac{(C_0^q+C_q^q)/2+(C_1^q+C_{q-1}^q)/2+\cdots+(C_{\lceil q/2\rceil}^q+C_{q-\lceil q/2\rceil}^q)/2}{2^q} \approx 1/2$. Let δ denote the probability for an attacker to be authenticated successfully in one round or in one authentication session by modifying h bits of the challenge binary vector, where $1 \leqslant h \leqslant m$. Let σ denote the probability for an attacker to be authenticated successfully by randomly sending a response in one round or in one authentication session. The advantage for an attacker to retrieve secrets by the perceived information can be presented by $\mathrm{Adv}_2[\delta] = \delta - \sigma$. By this transformation, we formalize the advantage to retrieve secrets such that the result is in $[-1, 1]$. When the result is in (0, 1], it denotes that an attacker has advantage. When the result is in $[-1, 0]$, it denotes that an attacker has no advantage. Because $\delta = \sigma$, we have $\mathrm{Adv}_2[\delta] = 0$ such that the attacker has no advantage to retrieve secrets.

5. Conclusions

In this paper, two lightweight LPN-problem-based authentication protocols have been proposed for reliable information provision systems with low computational-ability devices. The first protocol is for public information, and the other ensures that only authorized users can get information. According to security analyses, the attacker can be authenticated successfully with probability at most $1/2$ when $p = 1/2$ by mounting relay attack or modification attack. When p is lower, attack succeeds with lower probability. Moreover, no attacker has advantage to retrieve secrets. Unlike previous protocols, no malicious attacker can get information of the shared secret keys in the proposed protocols even if the attack succeeds. This property ensures the security of the proposed protocols. Thus, the security of information provision systems with low computational-ability devices can be ensured by the proposed protocols.

Acknowledgements. This work was supported in part by National Science Council under the grants NSC 98-2221-E-025-007- and NSC 99-2410-H-025-010-MY2.

References

Berlekamp, E.R., McEliece, R.J., van Tillborg, H.C.A. (1978). On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3), 384–386.

Blum, A., Furst, M.L., Kearns, M.J., Lipton, R.J. (1994). Cryptographic primitives based on hard learning problems. In: *Advances in Cryptology (CRYPTO'93), Lecture Notes in Computer Science*, Vol. 773. Springer, Berlin, pp. 278–291.

Blum, A., Kalai, A., Wasserman, H. (2003). Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*, 50(4), 506–519.

Bringer, J., Chabanne, H., Dottax, E. (2006). HB++: a lightweight authentication protocol secure against some attacks. In: *Proceedings of IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06)*, pp. 28–33.

Chang, Y.F. (2010). Real understanding of LPN-problem-based lightweight authentication protocols. *Information Technology and Control*, 39(3), 236–240.

Finkenzeller, K. (2002). *RFID Handbook*, 2nd edn. Wiley, New York.

Gilbert, H., Robshaw, M., Silbert, H. (2005). An active attack against HB+− a provable secure lightweight authentication protocol. *Cryptology ePrint Archive, Report 2005/237*. `http://eprint.iacr.org`.

Hopper, N.J., Blum, M. (2001). Secure human identification protocols. In: *Advances in Cryptology (ASYACRYPT' 2001), Lecture Notes in Computer Science*, Vol. 2248. Springer, Berlin, pp. 52–66.

Juels, A., Weis, S. (2005). Authenticating pervasive devices with human protocols. In: *Advances in Cryptology (Crypto2005), Lecture Notes in Computer Science*, Vol. 3621. Springer, Berlin, pp. 293–308.

Katz, J., Shin, J.S. (2005). Parallel and concurrent security of the HB and HB+ protocols. *Cryptology ePrint Archive, Report 2005/461*. `http://eprint.iacr.org`.

Munilla, J., Peinado, A. (2007). HB-MP: a further step in the HB-family of lightweight authentication protocols. *Computer Networks*, 51(9), 2262–2267.

Ohkubo, M., Suzuki, K., Kinoshita, S. (2004). Efficient hash-chain based RFID privacy protection scheme. In: *Proceedings of Ubiquitous Computing*.

Piramuthu, S. (2006). HB and related lightweight authentication protocols for secure RFID tag/reader authentication. In: *Proceedings of CollECTeR Europe Conference*, Basel, Switzerland.

Sarma, S.E., Weis, S.A., Engels, D.W. (2002). RFID systems and security and privacy implications. In: *Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science*, Vol. 2523. Springer, Berlin, pp. 454–469.

Vajda, I., Buttyan, L. (2003). Lightweight authentication protocols for low-cost RFID tags. In: *Proceedings of Ubiquitous Computing*.

Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. *Security in Pervasive Computing, Lecture Notes in Computer Science*, Vol. 2802. Springer, Berlin, pp. 201–212.

Y.-F. Chang is an associate professor of Department of Computer Science and Information Engineering at National Taichung University of Science and Technology in Taiwan. She received her BS degree in computer science and information engineering from National Chiao Tung University and PhD degree in computer science and information engineering from National Chung Cheng University, Taiwan. Her current research interests include electronic commerce, information security, cryptography, mobile communications, image processing, and data hiding.

W.-L. Tai is an assistant professor of Department of Information Communications at Chinese Culture University. He received his MS and PhD degrees in computer science and information engineering from National Chung Cheng University, Taiwan. His current research interests include information security, information communications, steganography, data hiding, signal processing, and image retrieval.

C.-C. Chen is an assistant professor of Department of Management Information Systems at National Chung Hsing University, Taiwan. Her current research interests include RFID, context awareness, wireless and sensor network, e-learning, and smart living. Dr. Chen's research is published or is forthcoming in *Information Sciences*, *Computer and Education*, *Journal of Educational Technology&Society*, *The Electronic Library*, *International Journal of Mobile Communications*, *Expert Systems with Applications*, *International Journal of Information Technology and Management*, and a number of national and international conference proceedings.

Patikimų informacijos teikimo sistemų, sudarytų iš mažų skaičiavimo galimybių įrenginių, autentifikavimo protokolai

Ya-Fen CHANG, Wei-Liang TAI, Chia-Chen CHEN

Belaidžio ryšio metodai įgalina vartotojus patogiai gauti reikalingą informaciją. Straipsnyje pasiūlyti du autentifikavimo protokolai, skirti patikimoms informacijos teikimo sistemoms, sudarytoms iš mažų skaičiavimo galimybių įrenginių. Pirmasis protokolas skirtas gauti informaciją visiems vartotojams, o antrasis protokolas informaciją pateikia tik tiems vartotojams, kuriems ji yra skirta.