hHB: A Harder HB$^+$ Protocol

Ahmad Khoureich Ka
Dept. of Computer Science, Alioune Diop University of Bambey, Bambey, Senegal

Keywords: RFID, Authentication, LPN, HB$^+$, Man-In-the-Middle.

Abstract: In 2005, Juels and Weis proposed HB$^+$, a perfectly adapted authentication protocol for resource-constrained devices such as RFID tags. The HB$^+$ protocol is based on the *Learning Parity with Noise* (LPN) problem and is proven secure against active adversaries. Since a man-in-the-middle attack on HB$^+$ due to Gilbert et *al*. was published, many proposals have been made to improve the HB$^+$ protocol. But none of these was formally proven secure against general man-in-the-middle adversaries. In this paper we present a solution to make the HB$^+$ protocol resistant to general man-in-the-middle adversaries without exceeding the computational and storage capabilities of the RFID tag.

1 INTRODUCTION

Radio-frequency identification (RFID) belongs to the family of Automatic Identification systems. RFID system consists of tags and readers that communicate wirelessly. The RFID tag attached to an object can be used for access control, product tracking, identification, etc. Since the tag is programmable, a malicious person can then create counterfeit tags and benefit from it. Hence the need to secure the protocol run between the tag and the reader.

RFID tags have a low computational and storage capacity. Therefore, it is impossible to use classical cryptographic algorithms to secure the protocol they execute. At Crypto 2005, Juels and Weis proposed HB$^+$ (Juels and Weis, 2005), a perfectly adapted authentication protocol for resource-constrained devices such as RFID tags. The protocol consists of a number of rounds of challenge-response authentication. HB$^+$ is based on the *Learning Parity with Noise* (LPN) problem — which is known to be NP-Hard — and is proven secure against active adversaries (Katz and Shin, 2006; Juels and Weis, 2005). Since a simple man-in-the-middle attack on HB$^+$ due to Gilbert et *al* (Gilbert et al., 2005). was published, many proposals (Bringer et al., 2006; Duc and Kim, 2007; Munilla and Peinado, 2007; Bringer and Chabanne, 2008; Leng et al., 2008) have been made to improve the HB$^+$ protocol. But none of these was formally proven secure against general man-in-the-middle adversaries (Gilbert et al., 2008b; Frumkin and Shamir, 2009; Ouafi et al., 2008).

In this paper we present a solution to make HB$^+$ resistant to general man-in-the-middle adversaries without exceeding the computational and storage capabilities of the RFID tag.

Our paper is organized as follow: (1) we give a definition of the LPN problem, (2) we describe the HB$^+$ protocol, (3) we present our protocol based on HB$^+$ and provide security proofs, (4) we conclude with some observations and future work.

2 THE LPN PROBLEM

The LPN problem is a very known one (Blum et al., 1994; Kearns, 1998; Hopper and Blum, 2000; Hopper and Blum, 2001; Blum et al., 2003; Regev, 2009; Berlekamp et al., 1978). Let $\mathsf{hw}(v)$ denote the Hamming weight of a binary vector v.

Definition 2.1. *Let A be a random $q \times k$ binary vector matrix, let x be a random k-bit vector, let $\varepsilon \in]0, \frac{1}{2}[$ be a constant noise parameter, and let ν be a random q-bit vector such that $\mathsf{hw}(\nu) < \varepsilon q$. Given A, ε, and $z = (A \cdot x) \oplus \nu$, find a k-bit vector x' such that $\mathsf{hw}(A \cdot x' \oplus z) \leq \varepsilon q$.*

The difficulty of finding x (solving the LPN) comes from the fact that each bit of $A \cdot x$ is flipped independently with probability ε, thus making hard to get a system of linear correct equations in x which can be easily solved using the Gaussian elimination.

Let Ber_ε denote the Bernoulli distribution with parameter ε, (i.e. $\nu \leftarrow \mathsf{Ber}_\varepsilon$, $\Pr[\nu = 1] = 1 - \Pr[\nu =$

Khoureich Ka A..
hHB: A Harder HB+ Protocol.
DOI: 10.5220/0005500001630169
In *Proceedings of the 12th International Conference on Security and Cryptography* (SECRYPT-2015), pages 163-169
ISBN: 978-989-758-117-5

$0] = \varepsilon$) and let $A_{x,\varepsilon}$ be the distribution define by $\{a \leftarrow \{0,1\}^k; \nu \leftarrow \mathsf{Ber}_\varepsilon : (a, a \cdot x \oplus \nu)\}$. One consequence of the hardness of the LPN problem with noise parameter ε is that $A_{x,\varepsilon}$ is indistinguishable from the uniform distribution U_{k+1} on $(k+1)$-bit strings; see (Katz and Shin, 2006).

Although many algorithms solving the LPN problem has been published (Blum et al., 2003; Levieil and Fouque, 2006; Fossorier et al., 2006), the current most efficient one due to Blum, Kalai, and Wasserman (Blum et al., 2003) has a runtime of $2^{O(\frac{k}{\log k})}$.

3 THE HB$^+$ PROTOCOL

HB$^+$ is an authentication protocol based on the LPN problem and designed for low-cost devices like RFID tags. The protocol consists of $r = r(k)$ challenge-response authentication rounds between the reader and the tag who share two random secrets keys x and y of length k. A round consists of the following steps (see fig 1 for a graphical representation):

1. the tag randomly chooses and sends to the reader a vector $b \leftarrow \{0,1\}^k$ called "blinding factor",
2. the reader randomly chooses and sends to the tag a challenge vector $a \leftarrow \{0,1\}^k$
3. the tag gets a bit ν following Ber_ε and responses to the reader by sending a bit $z = a \cdot x \oplus b \cdot y \oplus \nu$,
4. the reader accepts the authentication round if $a \cdot x \oplus b \cdot y = z$.

The parameters of HB$^+$ are: the shared secrets x and y each of length k, the number of rounds $r = r(k)$, the Bernoulli parameter ε and the threshold $\mathsf{u} = \mathsf{u}(k)$. The threshold u is such that it is greater than $\varepsilon \cdot r$ so the reader accepts the tag if the number of rounds for which Verify $a \cdot x \oplus b \cdot y = z$ returns false is less than u. Because of ν in the response z of the tag, the probability that an authentication round be unsuccessful even for the honest tag is not null. Therefore the event called false rejection that the reader rejects an honest tag happens with probability

$$P_{FR} = \sum_{i=\mathsf{u}+1}^{r} \binom{r}{i} \varepsilon^i (1-\varepsilon)^{r-i}.$$

At the same time an adversary sending random responses z to the reader can be accepted with probability

$$P_{FA} = \frac{1}{2^r} \sum_{i=0}^{u} \binom{r}{i}.$$

This event is called false acceptance. Fortunately these probabilities (P_{FR} and P_{FA}) are negligible in k because $r = r(k)$ (the use of Chernoff bound helps to see it).

3.1 Attacks on HB$^+$

HB$^+$ is in fact an improvement of an earlier protocol named HB (Hopper and Blum, 2001) which is secure against passive attack but vulnerable to active ones. In an active attack the adversary plays the role of a reader and tries to get the secrets from an honest tag. HB$^+$ is proven secure against this type of attack (Katz and Shin, 2006; Juels and Weis, 2005) but is defenseless against more powerful adversaries like man-in-the-middle (MIM). In such attacks the adversary stays between the reader and the tag and have the abilities to tamper with messages exchanged between them.

In (Gilbert et al., 2005) Gilbert, Robshaw, and Silbert present a MIM-attack against HB$^+$ called GRS attack. The attack is depicted in fig 2. In the GRS attack, in order to reveal the secret x, the adversary does not need to modify all the messages exchanged between the tag and the reader but only the challenge vector a. The adversary adds a perturbation δ on the challenge vector a and looks if the whole authentication process will be successful or not. The reader will verify if $a' \cdot x \oplus b \cdot y = z$ that is if $\delta \cdot x \oplus \nu = 0$. If the honest tag continues to be authenticated normally *i.e.* with negligible fails (P_{FR}) then the whole authentication process is not disturbed and it means that $\delta \cdot x = 0$ otherwise $\delta \cdot x = 1$. By using $\delta = e_i$ the vector with 1 at position i and 0s elsewhere, the adversary gets the bit x_i of x. By repeating the attack k times with different δ the adversary gets the whole secret x.

Much work (Bringer et al., 2006; Duc and Kim, 2007; Munilla and Peinado, 2007; Bringer and Chabanne, 2008; Leng et al., 2008) has been done in order to propose a protocol based on the LPN problem and resistant to the GRS attack. But none of these has been formally proven secure against general man-in-the-middle attacks (Gilbert et al., 2008b; Frumkin and Shamir, 2009; Ouafi et al., 2008).

4 OUR PROPOSAL

Intuitively we believe that the weakness of HB$^+$ to the man-in-the-middle attack is due to the fact that the secret x does not change. This intuition is reinforced by our observation of RANDOM-HB$^\#$ (Gilbert et al., 2008a) — partially resistant to this type of attack (GRS attack), see (Ouafi et al., 2008) — which can be viewed as an HB$^+$ protocol where the secret x varies in each round (although in fact parallel) but remains fixed for each instance of the protocol.

The main idea is to let the reader choose a random k-bit secret x and then sends it to the tag in a secure way. Our protocol denoted *h*HB for harder HB$^+$ con-

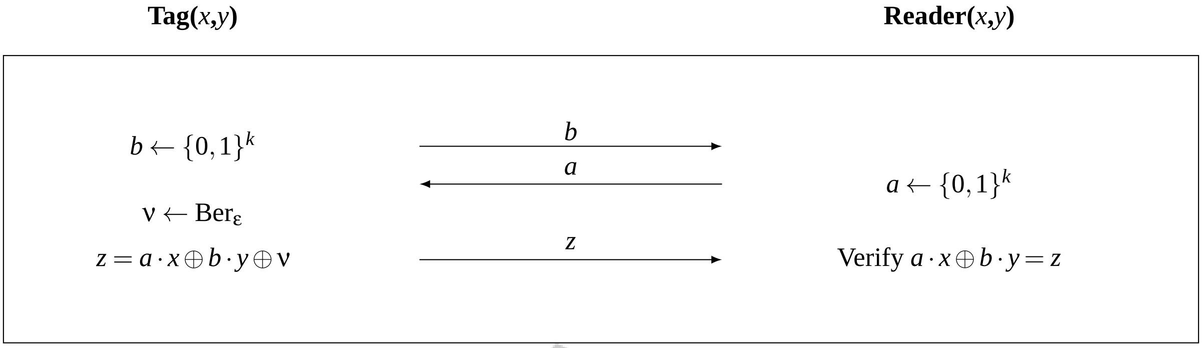

Figure 1: A round of the HB^+ Protocol.

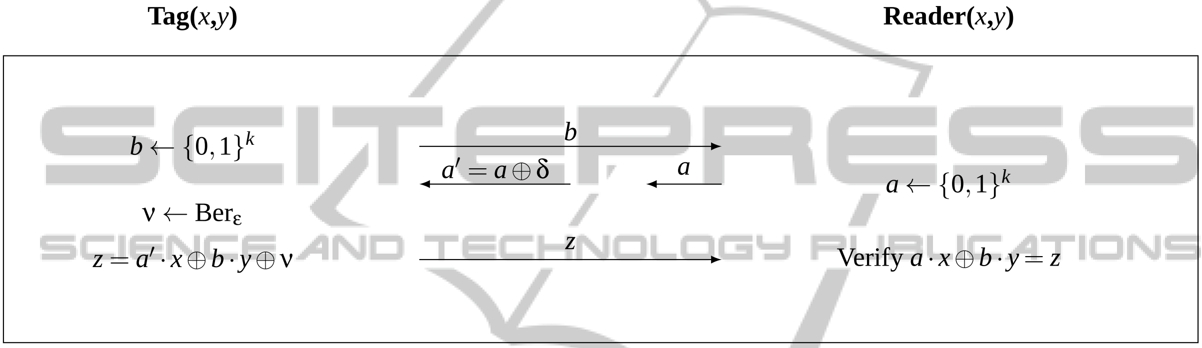

Figure 2: The GRS attack. The adversary adds a perturbation on the challenge vector a and looks if the whole authentication process will be disturbed or not.

sists of two stages. In the first stage the reader selects a random secret x that it transmits to the tag and in the second stage hHB is identical to HB^+. The secret x is transmitted bit by bit from the reader to the tag. The reader randomly selects three bits (τ, ξ_0, ξ_1) and sets the value x_i (a bit of x) to ξ_τ. After that the three bits are randomly permuted by a function f_s (see Algorithm 1 and 2) and securely communicated to the tag using the vector $s \oplus p_i$ where s is a shared secret and p_i a vector obtained from the prefix of length i of x, $p_i = x_1x_2...(x_i)^{(|s|-i+1)}$. This operation is repeated $|x|+1$ times. The hHB protocol is outlined in figure 3. The first triplet transmitted is used for the initialization of p_0 and the following triplets for the transmission of x. In order to cancel the effet of a MIM attack on the first triplet, the c_i vectors used for the second triplet (only for this one) are chosen such that their Hamming weight are even. The second stage of hHB is identical to a round of HB^+ and is run r times. An authentication round is successful if Verify $a \cdot x \oplus b \cdot y = z$ returns true. The reader accepts the tag if the number of unsuccessful rounds is less than a threshold u.

Algorithm 1: Function f_s that permutes elements of a triplet (λ_1, λ_2, λ_3).

function $f_s(\lambda_1, \lambda_2, \lambda_3, p_i)$
  $c_1 \leftarrow \{0,1\}^k \quad t_1 = c_1 \cdot (s \oplus p_i) \oplus \lambda_1$
  $c_2 \leftarrow \{0,1\}^k \quad t_2 = c_2 \cdot (s \oplus p_i) \oplus \lambda_2$
  $c_3 \leftarrow \{0,1\}^k \quad t_3 = c_3 \cdot (s \oplus p_i) \oplus \lambda_3$
  if $\lambda_1 \oplus \lambda_2 \oplus \lambda_3 = 0$ **then**
    return $((c_3,t_3),(c_1,t_1),(c_2,t_2))$
  end if
  if $\lambda_1 \oplus \lambda_2 \oplus \lambda_3 = 1$ **then**
    return $((c_2,t_2),(c_3,t_3),(c_1,t_1))$
  end if
end function

5 SECURITY PROOFS

5.0.1 Notation and Security Definitions

We call negl any negligible function, that is which tends to zero faster than any inverse polynomial. That is, for any polynomial $p(\cdot)$ there exist an N such that for all integer n greater than N we have $\mathsf{negl}(n) < \frac{1}{p(n)}$.

The parameters of hHB are: the shared secrets s

Tag(s,y)		**Reader(s,y)**
		$\tau \leftarrow \{0,1\}\ \xi_0 \leftarrow \{0,1\}\ \xi_1 \leftarrow \{0,1\}$
$(\tau,\xi_0,\xi_1) = f_s^{-1}(\alpha,\beta,\gamma,0^{\lvert s\rvert})$	$\xleftarrow{(\alpha,\beta,\gamma)}$	$(\alpha,\beta,\gamma) = f_s(\tau,\xi_0,\xi_1,0^{\lvert s\rvert})$
$\theta = \xi_\tau$		$\theta = \xi_\tau$
$p_0 = \theta^{\lvert s\rvert}$		$p_0 = \theta^{\lvert s\rvert}$
Repeat k times		
		$\tau \leftarrow \{0,1\}\ \xi_0 \leftarrow \{0,1\}\ \xi_1 \leftarrow \{0,1\}$
$(\tau,\xi_0,\xi_1) = f_s^{-1}(\alpha,\beta,\gamma,p_{i-1})$	$\xleftarrow{(\alpha,\beta,\gamma)}$	$(\alpha,\beta,\gamma) = f_s(\tau,\xi_0,\xi_1,p_{i-1})$
$x_i = \xi_\tau$		$x_i = \xi_\tau$
$p_i = x_1x_2\ldots(x_i)^{(\lvert s\rvert-i+1)}$		$p_i = x_1x_2\ldots(x_i)^{(\lvert s\rvert-i+1)}$
Repeat r times. $x = x_1x_2\ \ldots\ x_k$		
$b \leftarrow \{0,1\}^k$	$\xrightarrow{b}$	
	$\xleftarrow{a}$	$a \leftarrow \{0,1\}^k$
$\nu \leftarrow \mathrm{Ber}_\varepsilon$		
$z = a\cdot x \oplus b\cdot y \oplus \nu$	$\xrightarrow[z]{}$	Verify $a\cdot x \oplus b\cdot y = z$

Figure 3: The *h*HB authentication protocol.

and y, the one-time secret x is of length k, the number of rounds $r = r(k)$ of its second part, the Bernoulli parameter ε and the threshold $\mathsf{u} = \mathsf{u}(k)$. The parameters ε, r and u are the same as for the HB^+ protocol.

Let $\mathcal{T}_{s,y,\varepsilon,r}$ and $\mathcal{R}_{s,y,\varepsilon,\mathsf{u},r}$ denote the algorithms respectively run by the honest tag and the honest reader in the *h*HB protocol. Let k denote the security parameter. An active attack is by definition performed in two stages: first the adversary interacts $q(k)$ times with the tag, second she tries to authenticate to the reader. Man-in-the-middle attacks requires more power than active attacks. There the adversary can tamper with all messages going from the reader to the tag and vice versa for $q(k)$ executions of the protocol, and after that tries to authenticate to the reader. The adversary's advantage according to the model of attack can be defined as follow

$$\mathsf{Adv}^{\mathsf{active}}_{\mathcal{A}}(\varepsilon,\mathsf{u},\mathsf{r}) \stackrel{\text{def}}{=} \mathsf{Pr}\Big[s \leftarrow \{0,1\}^k; y \leftarrow \{0,1\}^k; \mathcal{A}^{\mathcal{T}_{s,y,\varepsilon,r}}(1^k) : \langle \mathcal{A}, \mathcal{R}_{s,y,\varepsilon,\mathsf{u},r}\rangle = \mathsf{accept}\Big],$$
$$\mathsf{Adv}^{\mathsf{mim}}_{\mathcal{A}}(\varepsilon,\mathsf{u},\mathsf{r}) \stackrel{\text{def}}{=} \mathsf{Pr}\Big[s \leftarrow \{0,1\}^k; y \leftarrow \{0,1\}^k; \mathcal{A}^{\mathcal{T}_{s,y,\varepsilon,r},\mathcal{R}_{s,y,\varepsilon,\mathsf{u},r}}(1^k) : \langle \mathcal{A}, \mathcal{R}_{s,y,\varepsilon,\mathsf{u},r}\rangle = \mathsf{accept}\Big],$$

where $\langle \mathcal{A}, \mathcal{R}_{s,y,\varepsilon,\mathsf{u},r}\rangle$ denote an attempt of $\mathcal{A}$ to authenticate to the reader.

Algorithm 2: Function f_s^{-1}.

```
function f_s^{-1}((c1,t1),(c2,t2),(c3,t3),p_i)
    λ1 = c1 · (s ⊕ p_i) ⊕ t1
    λ2 = c2 · (s ⊕ p_i) ⊕ t2
    λ3 = c3 · (s ⊕ p_i) ⊕ t3

    if λ1 ⊕ λ2 ⊕ λ3 = 0 then
        return (λ2, λ3, λ1)
    end if
    if λ1 ⊕ λ2 ⊕ λ3 = 1 then
        return (λ3, λ1, λ2)
    end if
end function
```

5.1 Security of the *h*HB Protocol against Active Attacks

Theorem 5.1. *If* HB^+ *with parameters* $0 < \varepsilon < \frac{1}{2}$, $r = r(k)$ *and* $\mathsf{u} > \varepsilon \cdot r$ *is secure against active attacks then hHB with the same settings of parameters is secure against active attacks.*

Proof. Let $\mathcal{A}$ be a probabilistic polynomial-time adversary interacting with the *h*HB tag in at most q executions of the protocol and achieving $\mathsf{Adv}^{\mathsf{active}}_{\mathcal{A}}(\varepsilon,\mathsf{u},\mathsf{r}) = \delta$.

We construct a probabilistic polynomial-time adversary $\mathcal{A}'$ who performs an active attacks on HB$^+$ and uses $\mathcal{A}$ as a sub-routine. For the first phase of the attack, $\mathcal{A}'$ simulates for $\mathcal{A}$ the *h*HB tag for q times as follows:

1. $\mathcal{A}'$ receives the triplets $(\alpha_i, \beta_i, \gamma_i)$ for $i = 1..k+1$ sent by $\mathcal{A}$.
2. $\mathcal{A}'$ forwards b sent by the honest HB$^+$ tag to $\mathcal{A}$,
3. $\mathcal{A}$ replies to $\mathcal{A}'$ by sending a challenge vector a which is then forwarded by $\mathcal{A}'$ to the honest HB$^+$ tag,
4. $\mathcal{A}'$ forwards z sent by the honest tag HB$^+$ to $\mathcal{A}$,

Steps 2., 3. and 4. are run r times. For the second phase of the attack, $\mathcal{A}'$ simulates for $\mathcal{A}$ the *h*HB reader as follows:

5. $\mathcal{A}'$ generates $k+1$ triplets $(\alpha_i, \beta_i, \gamma_i)$ and sends it to $\mathcal{A}$,
6. $\mathcal{A}$ sends b to $\mathcal{A}'$ which it forwards to the honest HB$^+$ reader,
7. $\mathcal{A}'$ sends to $\mathcal{A}$ the challenge vector a which it received from the honest HB$^+$ reader,
8. $\mathcal{A}$ sends z to $\mathcal{A}'$ which it forwards to the honest HB$^+$ reader,

Steps 6., 7. and 8. are run r times. It is not difficult to see that the view of $\mathcal{A}$ when run as a sub-routine by $\mathcal{A}'$ is distributed identically to the view of $\mathcal{A}$ when performing an active attack on *h*HB (Because even if $\mathcal{A}$ has carefully chosen the triplets $(\alpha_i, \beta_i, \gamma_i)$ it has sent in step 1, the blinding vector b prevents it to distinguish the effects of its choices in the value of z). So,

$$\mathsf{Adv}^{\mathsf{active}}_{\mathcal{A}}(\varepsilon,\mathsf{u},\mathsf{r}) = \delta = \mathsf{Adv}^{\mathsf{active}}_{\mathcal{A}',\mathsf{HB}^+}(\varepsilon,\mathsf{u},\mathsf{r}).$$

Because HB$^+$ is secure against active attack, there is a negligible function negl such that

$$\mathsf{Adv}^{\mathsf{active}}_{\mathcal{A}',\mathsf{HB}^+}(\varepsilon,\mathsf{u},\mathsf{r}) \leq \mathsf{negl}(k).$$

This implies that δ is negligible in k and completes the proof. □

5.2 Security of the *h*HB against MIM Attacks on the Second Stage of the Protocol

The second stage of the *h*HB protocol is identical to HB$^+$.

Theorem 5.2. *Assume the* LPN_ε *problem is hard, where* $0 < \varepsilon < \frac{1}{2}$. *Then the* *h*HB *protocol with parameters* $r = r(k)$ *and* $\mathsf{u} > \varepsilon \cdot r$ *is secure against man-in-the-middle attacks on its second stage.*

Proof. Let $\mathcal{A}$ be a probabilistic polynomial-time adversary tempering with messages of the second stage of *h*HB in at most q executions of the protocol and achieving $\mathsf{Adv}^{\mathsf{MIM}}_{\mathcal{A}}(\varepsilon,\mathsf{u},\mathsf{r}) = \delta$.

In the first phase of its attack, $\mathcal{A}$ eavesdrops and modifies messages at will in order to gain informations on secret x by correlating its actions with the decision of the reader (acceptance or rejection). For the second phase of the attack, we say for simplicity that $\mathcal{A}$ uses values $b = 0$.

$\mathcal{A}$ has the probability δ of being authenticated by the reader. This means with probability δ, $\mathcal{A}$ does a good guess of the value of z in at least $r - \mathsf{u}$ rounds. Therefore the probability that $\mathcal{A}$ gets an equation in the secret x is at least $\delta^{\frac{1}{r-\mathsf{u}}}$. On the other hand, because each bit x_i of x comes from one element of a triplet (α, β, γ), $\mathcal{A}$ gets a correct equation in x if she finds the element of (α, β, γ) which corresponds to x_i. Let $\mathsf{GoodChoice}$ denote the event *find the good element in the triplet*, F_1 the event *all the elements in the triplet are equal*, F_2 the event *two elements in the triplet are equal* and F_3 the event *all the elements in the triplet are distinct*. Since the way in which x is transmitted to the tag is an instance of the LPN problem and the application of f_s, we have:

$$\begin{aligned}
\Pr[\mathsf{GoodChoice}] =& \Pr[\mathsf{GoodChoice}|\mathsf{F}_1]\cdot\Pr[\mathsf{F}_1] + \Pr[\mathsf{GoodChoice}|\mathsf{F}_2]\cdot\Pr[\mathsf{F}_2] \\
&+ \Pr[\mathsf{GoodChoice}|\mathsf{F}_3]\cdot\Pr[\mathsf{F}_3] \\
=& \frac{1}{(2^{k_s+1})^2}\left[1 + \frac{3}{2}(2^{k_s+1}-1) + \frac{1}{3}(2^{k_s+1}-1)(2^{k_s+1}-2)\right] \\
=& \frac{1}{3} + \frac{1}{2^{k_s+2}} + \frac{1}{6(2^{k_s+1})^2} \\
\leq& \frac{1}{3} + \frac{1}{2^{k_s+1}},
\end{aligned}$$

where k_s is the length of s.

It follows that $\delta^{\frac{1}{r-\mathsf{u}}} \leq \frac{1}{3} + \frac{1}{2^{k_s+1}}$, this implies that $\delta \leq (\frac{1}{3} + \frac{1}{2^{k_s+1}})^{r-\mathsf{u}}$. Since k_s and $r - \mathsf{u}$ are functions of k, $(\frac{1}{3} + \frac{1}{2^{k_s+1}})^{r-\mathsf{u}}$ is negligible in k then δ itself is negligible. This completes the proof. □

5.3 Security of the *h*HB against MIM Attacks on the First Stage of the Protocol

The first stage of the *h*HB protocol consists of the transmission of the secret x from the reader to the tag.

Lemma 5.3. *Let* M *be a square* $(n \times n)$ *matrix over* $\mathbb{F}_2$. *If the Hamming weight of each row vector of* M *is even then* $det(M) = 0$.

Proof. For $n = 1$ and $n = 2$, it is easy to verify that the lemma is true. Let's prove it for $n \geq 3$.

Let M be as in the lemma. $M = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix}$ where $r_i = \begin{bmatrix} m_{i1} \; m_{i2} \; \cdots \; m_{in} \end{bmatrix}$. We sometimes use the same letter M to denote the set of row vectors of the matrix M.

Assume toward a contradiction that $det(M) \neq 0$. Let $\mathcal{P}_k$ be the set of k-combinations of the set of integers $\{1, 2, \ldots, n\}$. Consider

$$S_M = \bigcup_{P \in \mathcal{P}_k;\, 2 \leq k \leq n} \left\{ \sum_{i \in P} r_i \, ; \quad r_i \text{ the } i\text{-th row vector of } M \right\}$$

the set of sums of row vectors of M. $|S_M| = \sum_{k=2}^{n} \binom{n}{k} = 2^n - n - 1$. Let E denotes the set of vectors of even Hamming weight of $\mathbb{F}_2^n$. Since the sum of binary vectors of even Hamming weight is a vector of even weight and $det(M) \neq 0$, the set S_M is a subset of $E \setminus M$. $|E \setminus M| = 2^{n-1} - n$. For $n \geq 3$ we have $|S_M| > |E \setminus M|$, the pigeonhole principal tells us that there must be at least two elements of S_M which are equal thus the vectors of M are linearly dependent contradicting the assumption that $det(M) \neq 0$. This completes the proof of the lemma. □

Theorem 5.4. *Assume the* LPN_ε *problem is hard, where* $0 < \varepsilon < \frac{1}{2}$*. Then the h*HB *protocol with parameters* $r = r(k)$ *and* $\mathsf{u} > \varepsilon \cdot r$ *is secure against man-in-the-middle attacks on its first stage.*

Proof. In a the man-in-the-middle attack on the first stage of the *h*HB protocol, two cases can be considered:

Case 1. *The adversary perturbs the first triplet which is used to initialize* p_0*:* This perturbation can lead the tag to receive $\overline{\theta}$ instead of θ, and to consider without loss of generality that $x_1 = c_1 \cdot (s \oplus \overline{\theta}^{|s|}) \oplus t_1$, while for the reader $x_1 = c_1 \cdot (s \oplus \theta^{|s|}) \oplus t_1$. The effect of this perturbation is canceled when c_1 is chosen such that $c_1 \cdot \overline{\theta}^{|s|} = c_1 \cdot \theta^{|s|}$. This means the Hamming weight of c_1 is even. Therefore by choosing the elements of the second triplet with even Hamming weight, the perturbation the adversary adds in the first triplet will have no effect on the protocol.

Case 2. *The adversary perturbs triplets that carry bits of x:* Suppose the adversary adds a perturbation δ to each c in the $(i+1)$-th triplet, $1 \leq i \leq k$. This leads the tag to consider without loss of generality that $x_i = (c_1 \oplus \delta) \cdot (s \oplus p_{i-1}) \oplus t_1$ while the reader takes $x_i = c_1 \cdot (s \oplus p_{i-1}) \oplus t_1$. If the reader no longer authenticates the honest tag normally *i.e.* with negligible fails (P_{FR}) then the whole authentication process is disturbed and it means that $\delta \cdot s \oplus \delta \cdot p_{i-1} = 1$ otherwise $\delta \cdot s \oplus \delta \cdot p_{i-1} = 0$. Each of these equations in s contains a noise parameter $\delta \cdot p_{i-1}$. There are two subcases to consider:

1. *The adversary chooses a perturbation* δ *of odd Hamming weight:* In this case, without loss of generality suppose the perturbation is added to the second triplet. Then the noise parameter $\delta \cdot p_0$ will be equal to θ which is randomly chosen from $\{0, 1\}$. Thus in order to find the secret s the attacker has to solve the LPN_ε problem.
2. *The adversary chooses a perturbation* δ *of even Hamming weight:* If a perturbation of even Hamming weight is added to the second triplet (without loss of generality) then $\delta \cdot p_0 = 0$. The attacker gets a clean equation in s but in the light of lemma 5.3 he will not be able to obtain a system of equations consisting of linearly independent vectors δ. Therefore he can't compute the secret bits of s.

This means the adversary can't benefit from a man-in-the-middle attack on the first stage of the *h*HB protocol and completes the proof. □

5.4 *h*HB Security Settings

We respectively denote by k_s, k_x and k_y the length of the secrets s, x and y. The first phase of *h*HB consists of the secure transmission of the secret x which relies on the LPN problem with secret s and $\varepsilon \in [0.49, 0.5[$. Taking into account the recommendations of Levieil et *al* (Levieil and Fouque, 2006), we can use $k_s = 256$ to achieve at least 88 bits security. For the second phase of the *h*HB protocol corresponding to an execution of the HB^+ with $\varepsilon = 0.25$ the same recommendations from (Levieil and Fouque, 2006) can be applied, that is $k_x = 80$ and $k_y = 512$ to achieve 80 bits security. Using $r = 1164$ and $\mathsf{u} = 0.348 \times r$, the probability of false acceptance and false rejection are respectively 2^{-80} and 2^{-40}.

The transmission cost of x is $3(k_x + 1)(k_s + 1)$. For *h*HB that transmission cost is added to that of HB^+. When $k_x = 80$ and $k_s = 256$, the transmission cost of x is equal to 62451 bits which is substantially high. Nevertheless, the storage and computation cost of *h*HB remain low thus suited for low-cost hardware implementation.

6 CONCLUSIONS

In this paper we have presented a new protocol *h*HB which is a solution to thwart the man-in-the-middle attack against HB^+. The transmission cost of our protocol is quite high. But the *h*HB tag remains a tag as it is not overloaded (the storage and computation cost are substantially the same as for HB^+). Does securing HB^+ worth that transmission cost ? We say yes, but it would be very interesting to find a way to lower it while keeping the same level of security.

REFERENCES

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

Blum, A., Furst, M., Kearns, M., and Lipton, R. J. (1994). Cryptographic primitives based on hard learning problems. In *Advances in cryptologyCRYPTO93*, pages 278–291. Springer.

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

Bringer, J. and Chabanne, H. (2008). Trusted-HB: a low-cost version of HB^+ secure against man-in-the-middle attacks. *arXiv preprint arXiv:0802.0603*.

Bringer, J., Chabanne, H., and Dottax, E. (2006). HB^{++}: a lightweight authentication protocol secure against some attacks. In *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on*, pages 28–33. IEEE.

Duc, D. N. and Kim, K. (2007). Securing HB^+ against GRS man-in-the-middle attack. In *Institute of Electronics, Information and Communication Engineers, Symposium on Cryptography and Information Security*.

Fossorier, M. P., Mihaljević, M. J., Imai, H., Cui, Y., and Matsuura, K. (2006). An algorithm for solving the LPN problem and its application to security evaluation of the HB protocols for RFID authentication. In *Progress in Cryptology-INDOCRYPT 2006*, pages 48–62. Springer.

Frumkin, D. and Shamir, A. (2009). Un-trusted-HB: Security vulnerabilities of trusted-HB. *IACR Cryptology ePrint Archive*, 2009:44.

Gilbert, H., Robshaw, M., and Sibert, H. (2005). Active attack against HB^+: a provably secure lightweight authentication protocol. *Electronics Letters*, 41(21):1169–1170.

Gilbert, H., Robshaw, M. J., and Seurin, Y. (2008a). : Increasing the security and efficiency of HB^+. In *Advances in Cryptology–EUROCRYPT 2008*, pages 361–378. Springer.

Gilbert, H., Robshaw, M. J., and Seurin, Y. (2008b). Good variants of HB^+ are hard to find. In *Financial Cryptography and Data Security*, pages 156–170. Springer.

Hopper, N. J. and Blum, M. (2000). A secure human-computer authentication scheme. In *Technical Report CMU-CS-00-139*. Carnegie Mellon University.

Hopper, N. J. and Blum, M. (2001). Secure human identification protocols. In *Advances in cryptologyASIACRYPT 2001*, pages 52–66. Springer.

Juels, A. and Weis, S. A. (2005). Authenticating pervasive devices with human protocols. In *Advances in Cryptology–CRYPTO 2005*, pages 293–308. Springer.

Katz, J. and Shin, J. S. (2006). Parallel and concurrent security of the HB and HB^+ protocols. In *Advances in Cryptology-EUROCRYPT 2006*, pages 73–87. Springer.

Kearns, M. (1998). Efficient noise-tolerant learning from statistical queries. *Journal of the ACM (JACM)*, 45(6):983–1006.

Leng, X., Mayes, K., and Markantonakis, K. (2008). HB-MP^+ protocol: An improvement on the HB-MP protocol. In *RFID, 2008 IEEE International Conference on*, pages 118–124. IEEE.

Levieil, É. and Fouque, P. A. (2006). An improved LPN algorithm. In *Security and Cryptography for Networks*, pages 348–359. Springer.

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

Ouafi, K., Overbeck, R., and Vaudenay, S. (2008). On the security of $HB^\#$ against a man-in-the-middle attack. In *Advances in Cryptology-ASIACRYPT 2008*, pages 108–124. Springer.

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34.