Achieving protection against man-in-the-middle attack in HB family protocols implemented in RFID tags

Aisha Aseeri and Omaimah Bamasag
King Abdulaziz University, Jeddah Saudi Arabia

Received 4 March 2016
Revised 4 March 2016
Accepted 7 July 2016

Abstract

Purpose – In the past few years, HB-like protocols have gained much attention in the field of lightweight authentication protocols due to their efficient functioning and large potential applications in low-cost radio frequency identification tags, which are on the other side spreading so fast. However, most published HB protocols are vulnerable to man-in-the-middle attacks such as GRS or OOV attacks. The purpose of this research is to investigate security issues pertaining to HB-like protocols with an aim of improving their security and efficiency.

Design/methodology/approach – In this paper, a new and secure variant of HB family protocols named HB-MP* is proposed and designed, using the techniques of random rotation. The security of the proposed protocol is proven using formal proofs. Also, a prototype of the protocol is implemented to check its applicability, test the security in implementation and to compare its performance with the most related protocol.

Findings – The HB-MP* protocol is found secure against passive and active adversaries and is implementable within the tight resource constraints of today's EPC-type RFID tags. Accordingly, the HB-MP* protocol provides higher security than previous HB-like protocols without sacrificing performance.

Originality/value – This paper proposes a new HB variant called HB-MP* that tries to be immune against the pre-mentioned attacks and at the same time keeping the simple structure. It will use only lightweight operations to randomize the rotation of the secret.

Keywords HB protocols, Lightweight authentication, Man-in-the-middle attack, RFID authentication, RFID security

Paper type Research paper

1. Introduction

There is no doubt that radio frequency identification (RFID) technology has received a great demand through the Past decade in different Application fields such as transport, travel, health and many others. Accordingly, this raised the researchers' concern toward the safety of this technique, especially with the fact that RFID tags respond to reader interrogation without alerting their owner (Juels, 2006). This enables unauthorized readers to record tag's responses, and use them later to impersonate a legitimate tag. To solve most of the security problems and to increase privacy in RFID systems, a particular interest has been paid to the issue of authentication to ensure that only authorized readers can read from or write to the tag's memory, as well as only legitimate tags can convince the reader of their authenticity (Duc *et al.*, 2009; Feldhofer *et al.*, 2004).

International Journal of Pervasive Computing and Communications
Vol. 12 No. 3, 2016
pp. 375-390

1742-7371
DOI 10.1108/IJPCC-03-2016-0015

To apply authentication on RFID systems, we need to use lightweight authentication protocols because complex implementations are too expensive for such low-cost devices and thus cannot be used for RFID tags. Over the past few years, several protocols were proposed and evaluated. Perhaps the most prominent of these protocols are the HB-like protocols and that is because they are very efficient to implement on extremely low-cost hardware imposing only bitwise operations (Duc and Kim, 2007). HB's first protocol member was proposed by Hopper and Blum (2001) and then several variants were issued, each of which to fix weaknesses in their predecessors.

However, all previous HB protocols are vulnerable to a man-in-the-middle attack either in the GRS model or in the OOV model (Li *et al.*, 2010).

In this paper, we propose a new HB variant called HB-MP* that tries to be immune against the pre-mentioned attacks and at the same time keeping the simple structure. It will use only lightweight operations to randomize the rotation of the secret.

The rest of the paper is organized as follows: Section 2 contains a definition of the LPN problem, and a review of HB family history including their possible attacks. Then, definitions of some of the HB-like protocols related to the one we are proposing are provided in Section 3. After that, Section 4 introduces the HB-MP* protocol as a solution to the discussed security issues. This is followed by a detailed security analysis through informal and formal methods in Sections 5 and 6, besides a performance analysis in Section 7. Section 8 provides an implementation of the proposed protocol and the possible attacks to validate practically its applicability and security. Finally, Section 9 concludes the work.

2. Background

2.1 HB family history

HB family is originally introduced by Hopper and Blum (2001). It aims at authenticating RFID tags to a reader using very lightweight operations requiring only dot product and some basic XOR operations (Piramuthu, 2006). Trying to achieve high security in protocols with simple operations is considered a difficult task. Accordingly, there were many published HB schemes attempting to attain that. The HB authentication schemes base their security on the hardness of the learning parity with noise problem. Most of the schemes are multiple-round protocols.

The first scheme, HB protocol, was introduced by Hopper and Blum (2001). Later, in 2005, Juels and Weis (2005) proved that HB is effective only in defending passive attacks. As a result, they proposed a modified version named HB+ to resist active attacks. In the same year, Gilbert *et al.* (2004) presented a form of man-in-the-middle attack named GRS attack that breaks the HB+ security. Many protocols afterwards were proposed with the soul of resisting this kind of attack but later on, they were cracked by the same attack. Examples of these protocols are HB++ (Bringer *et al.*, 2006), HB* (Duc and Kim, 2007), HB-MP' and HB-MP (Munilla and Peinado, 2007), modified HB+ (Piramuthu and Tu, 2007) and Trusted-HB (Bringer and Chabanne, 2008). HB# (Gilbert *et al.*, 2008b) was one of them claiming security against GRS attack, but a new form of man-in-the-middle attacks called OOV attack was presented by Oaufi *et al.* that breaks not only HB# but also many of the HB-like schemes (Ouafi *et al.*, 2008). Other protocols proposed were HB-MP+ (Xuefei *et al.*, 2008) and HB-MP++ (Bongno *et al.*, 2009), which were considered as an enhancement to the HB-MP, but the description of provided function in HB-MP+ was abstract and without any details, while

HB-MP++ includes another kind of weakness mentioned later in this paper. Also, PUF-HB (Hammouri and Sunar, 2008) was another variant that uses a physical unclonable function but does not carry any proof of security against man-in-the-middle attacks. At last, three other protocols, namely, NLHB (Madhavan *et al.*, 2010), RCHB (Ali *et al.*, 2011) and the work by Lyubashevsky and Daniel (2013) were proposed recently, aiming to increase security in passive attacks but did not mention active attacks.

2.2 LPN

In simple, the learning parity with noise problem requires an attacker to recover a k-bit secret key x given q random binary k-bit strings a and q bits value representing $z_i = a_i.x \oplus v_i$ for some $x \in \{0,1\}k$, where $a.x$ denotes the binary inner product between a and x, ν is a noise bit equal to 1 with a probability $\epsilon\epsilon[0,1/2]$. It can be defined formally as follows, noting that the hamming weight of a vector x, is represented by $|x|$:

Definition 1 (Xuefei *et al.*, 2008): Let A be a random $q \times k$ binary matrix, let x be a random k-bit vector, let $\eta\epsilon[0,1/2]$ be a constant noise parameter and let v be a random q-bit vector such that $|v| < \eta q$. Given A, η and $z = (A.x) \oplus v$, find a k-bit vector x' such that $|(A \,.\, x') \oplus z| < \eta q$.

2.3 Attacks on HB-like protocols In the literature, there were number of known attacks that HB schemes suffer from and try to avoid. Here is a classification and definition of these types:

(1) *Passive attacks*: The adversary can only eavesdrop on the conversation between an honest tag and an honest reader, and then tries to impersonate the tag (Juels and Weis, 2005).

(2) *Active attacks*: This type of attack requires the attacker to be able to transmit data to one or both of the parties, or block the data stream in one or both directions. It can be formed in different ways, below are some of the tackled forms:

- *JW attack*: Proposed by Juels and Weis and targeting the tag only. The adversary first interacts with an honest tag up to a number of times (actively, but without access to the reader), and then tries to impersonate the tag (Juels and Weis, 2005).
- *Man-in-the-middle attack*: The adversary can manipulate the tag-reader conversation and observe whether the authentication is successful or not. Below are two types of this attack mentioned through literature:
  - *GRS attack*: Proposed by Gilbert, Robshow and Seurin. An attacker can slightly modify messages from the reader and observe whether the legitimate reader still accepts the legitimate tag, and then the attacker can recover secret key information (Gilbert *et al.*, 2004).
  - *OOV attack*: Proposed by Ouafi, Overbeck and Vaudenay. An attacker first eavesdrops on one successful execution of the protocol and uses the values to manipulate many executions of the protocol by XORing interactions on both directions with the eavesdropped values. Based on the overall success probability, the attacker can calculate the error-free bits. The adversary collects enough equations by changing a different bit in the tag response each time to recover the secrets (Ouafi *et al.*, 2008).

3. Related work

3.1 HB+ protocol

HB+ was proposed to overcome active attacks problem in the HB protocol. It includes an additional secret key y besides a blinding factor b compared to the HB protocol. It is also composed of q rounds, one of which is depicted in Figure 1, and described as follows: (using notations in Table I) (Juels and Weis, 2005)

Step 1: The tag chooses at random a k-bit vector b and sends it to the reader.
Step 2: The reader chooses at random a k-bit challenge a and sends it to the tag.
Step 3: The tag computes the value $z = a.x \oplus b.y \oplus v$.
Step 4: The tag sends the result z to the reader.
Step 5: The reader checks that $z = a.x \oplus b.y$.

The round given in Figure 1 is repeated q times and the tag is authenticated if check on the reader's side fails at most $q.\eta$ times.

3.1.1 Security issues. A new attack was found that imposes a threat against HB+. It is a form of man-in-the-middle attack called GRS, mentioned by Gilbret, Robshow and Surin (see Figure 2 for a description). In this attack, an adversary modifies the challenge a of all rounds by XORing it with δ, a fixed-value vector with a single non-zero bit, such that $a' = a \oplus \delta$. Then, it will observe the result of the authentication process. If it is authenticated, then it concludes that $\delta.x = 0$. Otherwise, $\delta.x = 1$. By repeating the process k-times for different independent values of δ, it can recover all k-bits of the secret x. A similar process can be applied on b to obtain the secret key y (Duc and Kim, 2007).

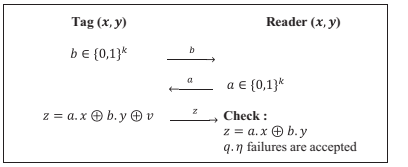

Figure 1.
A single round of HB+ protocol

k	Length of the secret keys
x	k-bit secret key
y	k-bit secret key
a	Random k-bit binary vector
b	Random k-bit binary vector
v	Noise bit; v=1 with probability $\eta \epsilon [0,1/2]$
.	Denotes scalar product of two vectors
$\oplus$	Denotes XOR operation

Table I.
Notations for HB+ protocol

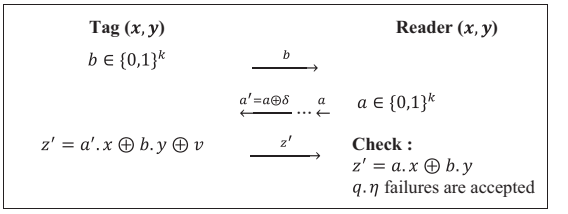

Figure 2.
GRS attack in general

3.2 HB-MP protocol

It was proposed to avoid the GRS attacks on HB-MP', by modifying the secret at each round using the rotation function. It contains an additional secret key y and composed of q-rounds. One of which is depicted in Figure 3, and described below: (using notations in Table II)

Step 1: The reader chooses at random a m-bit challenge a and sends it to the tag.

Step 2: The tag computes the x in the ith round by rotation as $x = Rot(x,y_i)$, where y_i presents the ith bit of the secret key y.

Step 3: The tag computes the value $= a.x_m \oplus v$, and then looks for a m-bit random vector b that satisfies the equation $b.x_m = z$.

Step 4: The tag sends b to the reader.

Step 5: The reader checks that b is different than a, and $a.x_m = b.x_m$.

In Step 5, the reader checks that b is different than a, as an adversary can send the same value of a to be authenticated by the reader without the need to know the secret.

The round given in Figure 3 is repeated q times and the tag is authenticated if check on the reader's side fails at most $q.\eta$ times.

3.2.1 Security issues. From the protocol description above, we can see that the secret key might have different values through rounds to help in randomizing the response. But, x_m will be the same for the same round through different authentication sessions, which makes x_m more predictable. Besides, an attacker can initiate repetitive authentication sessions restricted to the first round. Then, active attacks can be used to reveal the tag's first round x_m (Xuefei *et al.*, 2008).

It was also found that HB-MP is vulnerable to a simple passive attack (Gilbert *et al.*, 2008a). In each round, a reader checks that $a.x_m = b.x_m$, which means $(a \oplus b).x_m = 0$. So, eavesdropping all a and b values through one execution can help an attacker to predict b using a besides the previous values of the same round, without the need to know the secret. For example, in the first round, if the reader sends a', it's easy to find b' that satisfies the equation $a \oplus b = a' \oplus b'$, noting that a and b are the eavesdropped values of the first round.

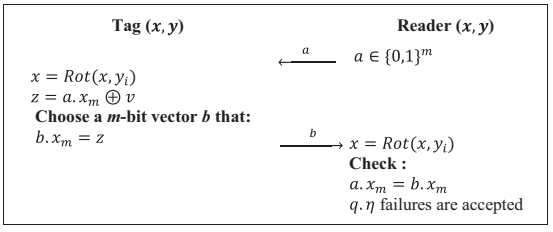

Figure 3.
A single round of HB-MP protocol

x,y	k-bit secret keys
a,b	Random m-bit binary vectors
m	Length of the message exchanged between the parties
$Rot(p,u)$	The operand p is left rotated by u positions
x_m	m-bit LSB of the secret x

Table II.
Notations for HB-MP

4. HB-MP* protocol description

By reviewing and critically analyzing the related protocols and their vulnerabilities in the previous section, we found that the HB-MP-like protocols are a good architecture to base our design on. This is because all HB-MP-like protocols do not include the tag computation result z through the communicated messages. This helps in a way to hide some information, as z can be used to retrieve the secrets x and y as in HB+. Furthermore, this feature can be used to avoid the OOV attack to a certain degree, as the OOV attack requires this value to be present to be mounted. This section will present a description of a new HB variant protocol. The design of the proposed protocol assumes that the low-cost RFID tag is passive and has a re-writable memory like EEPROM with reasonable size like EPC Class 1 Gen 2 of EPC Global.

The protocol is a multi-round symmetric key authentication protocol where each round consists of two communications between the reader and the tag. The goal of the protocol is to retain some of the successful properties of HB+ and HB-MP while also resisting the GRS and OOV attacks. It will have the same steps of the HB-MP, with some differences to avoid the previous explored attacks. These differences include having only one shared secret key instead of two and choosing it prime, multiplying the secret by a rotated version of itself instead of the challenge and encrypting the exchanged messages. The protocol is composed of q rounds, one of which is depicted in Figure 4, and described below: (using notations in Table III)

Step 1: The reader chooses at random a m-bit binary vector a where m is a prime number, and XOR it with x_m and send it to the tag. We use the XOR to make it harder for the adversary to know x or a.

Step 2: The tag computes $a = a' \oplus x_m$.

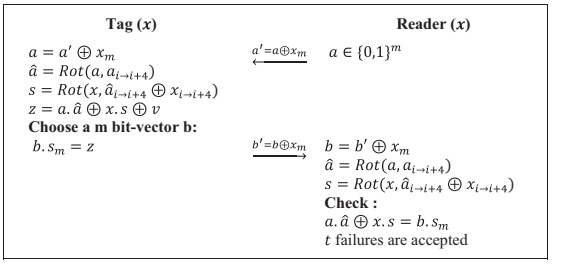

Figure 4.
A single round of HB-MP* protocol

k	Prime number representing the length of the secret key
x	k-bit secret key
a,b	Random m-bit binary vectors
v	Noise bit; $v = 1$ with probability $\eta \epsilon [0,1/2]$
t	Threshold, the accepted number of failures, equal to $q \cdot \eta$
.	Denotes scalar product of two vectors
$\oplus$	Denotes XOR operation
m	Prime number representing the length of messages, m < k
$Rot(p,u)$	The operand p is left rotated by u positions
x_m, s_m	m-bit LSB of the vectors x , s
$a_{i\to i+3}$, $x_{i\to i+3}$, $\hat{a}_{i\to i+3}$	Four bits from the vectors a, x, $\hat{a}$ starting from the ith bit to (i + 3) bit, where i is the round index

Table III.
Notations for HB - MP* protocol

Step 3: The tag and reader compute $\hat{a} = Rot(a,a_{i\to i+3})$, where $a_{i\to i+3}$ is four bits starting from the ith bit of the vector a and i is the round index (i takes values from 0 to q-1). Those four bits will give a number from 1 to 15, which will present the number of rotated positions.

Step 4: The tag and reader compute $s = Rot(x,\hat{a}_{i\to i+3} \oplus x_{i\to i+3})$, where $\hat{a}_{i\to i+3}$, $x_{i\to i+3}$ are also four bits starting from the ith bit of the vectors $\hat{a}$ and x. Two four-bit vectors will be XORed to get a number from 1 to 15, which will present the number of rotated positions.

Step 5: The tag computes z as follows: $z = a.\hat{a} \oplus x.s \oplus v$.

Step 6: The tag will then find a m-bit binary vector b such that $b.s_m = z$.

Step 7: The tag will XOR the b with the amount x_m and send it to the reader.

Step 8: The reader computes $b = b' \oplus x_m$ and checks that: $a.\hat{a} \oplus x.s = b.s_m$, and accepts it if failures are not more than t. t is a threshold equal to $q.\eta$., and can be adjusted to a value that is larger than $q.\eta$ to reduce the false rejection rate, and retain a low false acceptance rate at the same time according to Xuefei *et al.* (2008).

A neat algorithm on picking b when $\eta = 0.25$ for HB-MP protocol was mentioned by Munilla and Peinado (2007), and is reformed for the HB-MP* protocol here:

Algorithm 1
Input: a, x. Output: b such that $b.s_m = a.\hat{a} \oplus x.s \oplus v$, where $v = 1$ with probability 1/4.
Computes $z = a.\hat{a} \oplus x.s$
Generates at random a m-bit binary vector b
If $b.s_m = z$
Sends b
else
Generates and sends a new random m-bit vector b
end

From the algorithm, one can know that the possibility that $b \,.\, s_m = a \,.\, \hat{a} \oplus x \,.\, s$ is $0.5 \times 0.5 = 0.25$, that means $\varsigma = 0.25$.

As the HB-family protocols, including our protocol, are probabilistic approaches, there exist two types of authentication errors. A false negative (P_{FN}), that is the authentication of a legitimate entity being rejected, takes place when the number of incorrect responses exceeds the pass-threshold τ. By contrast, a false positive (P_{FP}) is defined such that the number of unmatched responses out of random bits is less than the pass-threshold τ. P_{FN} and P_{FP} are also referred to as the false negative rate and the false positive rate, respectively (Gilbert *et al.*, 2008a).

5. Security analysis against passive and active attacks

We consider the proposed protocol presented above and evaluate its security against common threats, which are passive and active, including man-in-the-middle attacks.

5.1 Immunity against passive attacks

If an attacker tries to eavesdrop an execution recording all values of a and b, to impersonate a tag, similar to what is possible to happen with HB-MP as discussed in Section 3.4.3, it will be very difficult to predict b depending on a sent by the reader and the eavesdropped values from previous authentication sessions. This is because there is no common factor between the terms of a and b (i.e. a and b are multiplied by different

values). Besides, the structure of the computation equation does not allow knowing b without knowing the secrets.

5.2 Immunity against active and man-in-the-middle attacks

The protocol is immune against JW attacks, as each time the same challenge a is sent to the tag, it will give a different response due to the random b. Another act an adversary might do here is sending a certain value of a such as 0 that could get rid of some terms in the computation to reveal the secrets, but this will be hard to determine with the added amount x_m. For example, sending a zero will correspond to $(a \oplus x_m)$ and that means $(a = x_m)$, which will not help in any way. Even simplifying the equation will not work, as the lengths of x,s and x_m are different.

In a GRS attack, an attacker could modify the only message sent from reader to tag which is $(a \oplus x_m)$ by XORing it with δ, a single non-zero-bit vector to become $(a \oplus x_m \oplus \delta)$. The tag, thus, uses $(a \oplus \delta)$ instead of a in its computations, but this will not help to reveal any secret information because, originally, a was not multiplied by any of the secrets. On the other side, an attacker can also modify the message sent from tag to reader $(b \oplus x_m)$. In this case, it will succeed only if s_m has a fixed value through all rounds or at least for the same rounds in different sessions as in HB-MP, then it will be easy to reveal the secret by sending a modified message $(b \oplus x_m \oplus \delta)$ and observing the authentication result. However, this will be very difficult to happen, as s_m is changing through all rounds and sessions. That is because its value depends on three factors: the secret key x, the round index and the challenge a which is a random number changing on each round besides the fact that its value is unknown to the adversary unless he knows the secret x.

In an OOV attack, an attacker goes through two stages. In the first stage, an attacker eavesdrops on one successful execution and uses these values $(\bar{a}, \bar{b})$ to modify messages going on both directions. The goal of the first stage is to get an estimation of $wt(v \oplus \bar{v})$. In our case, there is the amount x_m that prevents using $a \oplus \bar{a}$ on the tag; instead, it will use $a \oplus \bar{a} \oplus x_m$. However, even if we assumed that we were able to use the amounts $a \oplus \bar{a}$ and $b \oplus \bar{b}$ on the tag and reader, we will find it difficult to complete the attack. As on the reader, we will get the equation $(a.\hat{a} \oplus x.s = b.s_m \oplus \bar{b}.s_m)$, which will not allow us to get $v \oplus \bar{v}$, even after compensation and reduction. That is because the values of s *and* s_m are different for the values of $a,b,\bar{a}$ *and* $\bar{b}$.

From the above, we can see that HB-MP* is secure against passive, active and man-in-the-middle attacks as long as it resists the GRS and OOV attacks.

6. Formal proof of security

To formally discuss HB-MP* security, we should define some security models. We will represent the tag-reader authentication system by two probabilistic functions $(T_{x,\eta,q}, \mathcal{R}_{x,q,\tau})$, namely, a tag and a reader function. Below are two security models that we will use in the formal proof, identical to the one used by Juels and Weis (2005), Li *et al.* (2009) and Li *et al.* (2010).

6.1 Definition 1 (DET model)

In the detection-based model, an attack is carried out in two phases as follows:

(1) *Phase 1*: An adversary A impersonating a reader interacts q times with the honest tag $T_{x,\eta,q}$. Where on the ith interaction, $T_{x,\eta,q}$ receives a vector from A as an

input interpreted as a challenge vector a_i XORed with a part of the secret key and outputs to A, a random generated blinding vector b_i that satisfies the equation $a_i \,.\, \hat{a_i} \oplus x \,.\, s = b_i \,.\, s_m$, but after encrypting it by XORing with the secret key. This phase simulates an active attacker querying a legitimate tag.

(2) *Phase 2*: Adversary A interacts with the reader $\mathcal{R}_{x,q,\tau}$, intending to impersonate the tag using the key extracted from the first phase.

6.2 Definition 2 (GRS model)

In the GRS model, an attack is carried out in two phases as follows:

(1) *Phase 1*: Adversary A modifies the encrypted challenges and blinding vectors exchanged between the tag $T_{x,\eta,q}$ and the reader $\mathcal{R}_{x,q,\tau}$ for q executions. Where on the ith invocation, $\mathcal{R}_{x,q,\tau}$ generates a random challenge a_i, encrypts it to $a_i^{'}$ and sends it to adversary A. Then, $T_{x,\eta,q}$ receives a modified challenge $a_i^{''}$ from A and generates a blinding vector b_i that satisfies the equation $a_i^{''} \,.\, \hat{a_i}^{''} \oplus x \,.\, s^{'} \oplus v = b_i \,.\, s_m^{'}$ and gives it to A after encryption. $\mathcal{R}_{x,q,\tau}$ takes a modified blinding vector $b_i^{'}$ from A, and checks if $\mathrm{Hwt}(a_i \,.\, \hat{a_i} \oplus x \,.\, s \oplus b_i^{'} \,.\, s_m) \leq \tau$. If it holds, $\mathcal{R}_{x,q,\tau}$ outputs "ACCEPT" to A; otherwise, it outputs "REJECT".

(2) *Phase 2*: Adversary A interacts with the reader $\mathcal{R}_{x,q,\tau}$, intending to impersonate the tag using the key extracted from the first phase.

An adversary's advantage is a measure of how successfully it can attack a cryptographic algorithm, by distinguishing it from an idealized version of that type of algorithm (Zhang and Kitsos, 2009). A cryptographic algorithm is considered secure if the advantage of any computationally bounded adversary is a negligible function of the security parameter (Bellare *et al.*, 1997). The success probability of an adversary impersonating a tag in Phase 2 of both models, by replying a random vector, is presented by the false positive rate P_{FP}. This is the best soundness error that could be achieved by the HB-MP* protocol. The advantage of an adversary A attacking HB-MP* in the DET model and in the GRS model is defined as the overall success probability over P_{FP} in impersonating the tag:

$$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{DET}}(k,\ \eta,\ n, \tau) \overset{\mathrm{def}}{=} \Pr\left[x \overset{\$}{\rightarrow} \mathrm{S}^k, A^{T_{x,\eta,n}}(1^k) : \langle A, \mathcal{R}_{x,n,\tau} \rangle = AAC\right] - P_{\mathrm{FP}}$$

$$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{GRS}}(k,\ \eta,\ n, \tau) \overset{\mathrm{def}}{=} \Pr\left[x \overset{\$}{\rightarrow} \mathrm{S}^k, A^{T_{x,\eta,n},\mathcal{R}_{x,n,\tau}}(1^k) : \langle A, \mathcal{R}_{x,n,\tau} \rangle = AAC\right] - P_{\mathrm{FP}}$$

If an adversary only achieves a negligible advantage against an HB-like protocol in a model, we can claim that the protocol is secure in this model.

To proceed in our proof, we need to prove the following two lemmas which will be needed in the next sections.

Lemma 1: If a is a p-length binary vector and p is a prime number, then shifting the vector t-times where $0 < t < p$ will never give the same original vector.

Proof. Let: $a_i = (a_0, a_1, \ldots, a_{p-1-t}, a_{p-t}, a_{p-t+1}, \ldots, a_{p-1})$.

Shifting the vector t-times will generate:

$$a_{(i+t) \bmod p} = (a_t,\ a_{t+1},\ \ldots,\ a_{p-1},\ a_0,\ a_1,\ \ldots,\ a_{t-1})$$

Let's assume that $a_i = a_{(i+t) \bmod p}$

This implies that $a_0 = a_{t \bmod p} = a_{2t \bmod p} = a_{3t \bmod p} = \ldots = a_{(p-1)t \bmod p}$, representing p numbers.

We want to show that these are p different numbers. So, let's take the indexes and show that they are pair-wise different.

$\{0, t \bmod p, 2t \bmod p, 3t \bmod p [\ldots][\ldots]., (p-1)t \bmod p\}$

Assuming that we have $i \neq j$ and $0 \leq j < i \leq (p-1)$, which means that:

$$0 < i - j < p$$

$(it) \bmod p = (jt) \bmod p \rightarrow it = s_1 p + q$ and $jt = s_2 p + q$

$\rightarrow s_1 p + q = s_2 p + q \rightarrow (s_1 p + q) - (s_2 p + q) = (s_1 - s_2)p = s^{'} p$

So we get to: $(it) - (jt) = s^{'} p$, which means that $it - jt = (i-j)t$ is divisible by p.

This implies that either $(i-j)$ or t is divisible by p and this gives us a contradiction, as we assumed that $(i-j)$ and t is less than p. So, none of them is divisible by p and this proves that all p numbers in $\{0, t \bmod p, 2t \bmod p, 3t \bmod p [\ldots][\ldots]., (p-1)t \bmod p\}$ are different, which on the other side proves that $a_i \neq a_{(i+t) \bmod p}$.

Lemma 2:

If a is a p-length binary vector and p is a prime number, then shifting the vector t-times where $0 < t < p$ will generate a linearly independent vector with a.

Proof. Let: $a_i = (a_0, a_1, \ldots, a_{p-1-t}, a_{p-t}, a_{p-t+1}, \ldots, a_{p-1})$.

And let $a_{(i+t) \bmod p} = (a_t, a_{t+1}, \ldots, a_{p-1}, a_0, a_1, \ldots, a_{t-1})$, be A t-times sifted version of a_i.

We want to prove that a_i and $a_{(i+t) \bmod p}$ are linearly independent.

a_i and $a_{(i+t) \bmod p}$ are said to be linearly dependent if and only if there exists two values n and m both of which are not zero such that $n.a_i + m.a_{(i+t) \bmod p} = 0$.

This will be achieved only if $a_i = a_{(i+t) \bmod p}$.

From Lemma 1, we can see that it's impossible that a_i and $a_{(i+t) \bmod p}$ will be equal, so a_i and $a_{(i+t) \bmod p}$ are linearly independent.

6.3 HB-MP security in the GRS model*

Theorem 1: If there exists an adversary A attacking the HB-MP* protocol in the GRS model, modifying at most q executions of the protocol between an honest tag and an honest reader, running in time t and achieving $\mathrm{Adv}_{\mathrm{A}}^{\mathrm{GRS}}(k,n,\eta,u) \geq \delta$. Then there exists an adversary A' attacking the HB-MP* protocol in the DET model, interacting at most q oracle queries, running in time O(t) and achieving $\mathrm{Adv}_{\mathrm{A}'}^{\mathrm{DET}}(k,n,\eta,\tau) \geq \delta - q\epsilon(P_{FP} + \delta)$ for some negligible function.

Hence, assuming HB-MP* is secure in the DET model, HB-MP* is provably secure in the GRS model.

Proof. In Phase 1, as A' has access to $\mathrm{T}_{x,\eta,n}$, it can easily simulate the honest tag to A. Accordingly, the main challenge lies on how to simulate the reader $\mathcal{R}_{x,n,\tau}$. Similar to the proof method for the Random-HB# protocol (Gilbert *et al.*, 2008b), A' launches Phase 1 of adversary A, and simulates the tag and the reader for q times as follows:

- A' sends a random vector a_i as the challenge of the simulated reader. A modifies it into $a_i^{'}$ and sends it to the simulated tag. A' forwards $a_i^{'}$ to the real tag.
- The real tag receives $a_i^{'}$ and calculates $a_i^{''} = a_i^{'} \oplus x_m$, trying to decrypt a. It responds with $b_i^{'} = b_i \oplus x_m$ to A', where b_i satisfies $b_i.s_m^{''} = a_i^{''}.\hat{a}_i^{''} \oplus x.s^{''} \oplus v$. A' sends $b_i^{'}$ as the blinding vector of the simulated tag. A modifies it into $b_i^{''}$, and sends it to the simulated reader.

- If $a_i \oplus a_i^{'} = 0^{(m)}$ and also $b_i^{'} \oplus b_i^{''} = 0^{(m)}$, A' outputs "Accept" to A as the authentication result of the simulated reader; otherwise, it outputs "Reject".

After Phase 1, A' launches Phase 2 of A. And as Phase 2 in the DET model is identical to that in the GRS model, A' just replicates A's behavior with the real reader, to simulate the tag $T_{x,\eta,n}$. Accordingly, if A achieves $\mathrm{Adv}_{A}^{GRS}(k,n,\eta,u) \geq \delta$, then the probability of A' successfully impersonating a valid tag is the same as the success probability of A, i.e. $P_{FP} + \delta$, on the condition that the reader is correctly simulated by A' in Phase 1.

Therefore, to calculate the probability of A' successfully simulating the reader for A in Phase 1, we will consider one execution of the protocol in Phase 1. To simplify the security proof for HB-MP*, we rule out a trivial case of $a_i \oplus a_i^{'} = 1^{(m)}$ and $b_i^{'} \oplus b_i^{''} = 1^{(m)}$. When $a_i \oplus a_i^{'} = 0^{(m)}$ and $b_i^{'} \oplus b_i^{''} = 0^{(m)}$, A' fails at simulating the reader with a probability equal to the false negative rate P_{FN}. For the case of $a_i \oplus a_i^{'} \neq 0^{(m)}$ or $b_i^{'} \oplus b_i^{''} \neq 0^{(m)}$, as we suppose that $a_i \oplus a_i^{'} \neq 1^{(m)}$ and $b_i^{'} \oplus b_i^{''} \neq 1^{(m)}$, the resulting equation $b_i.s_m^{''} = a_i^{''}.\hat{a}_i^{''} \oplus x.s^{''} \oplus v$ is uniformly distributed over $\{0,1\}^n$, because all terms are linearly independent. As a result, the probability of A' wrongly outputting "REJECT" is exactly the same as the false positive rate P_{FP}. Overall, A' fails at simulating the reader in one execution at most with probability $\varepsilon = \max(P_{FN}, P_{FP})$. The probability of A' correctly simulating the reader in Phase 1 would be not less than $1\text{-}q\varepsilon$, and adversary A' can impersonate a valid tag with success probability not less than $(P_{FP} + \delta)(1\text{-}q\varepsilon)$. Therefore, A' can achieve advantage:

$$\mathrm{Adv}_{A'}^{DET}(k,\eta,n,\tau) \geq (P_{FP} + \delta)(1 - q\varepsilon) - P_{FP} = \delta - q\varepsilon(P_{FP} + \delta)$$

If δ is non-negligible, then $q\varepsilon(P_{FP} + \delta) \leq \delta/2$ for k is big enough, and $\mathrm{Adv}_{A'}^{DET}(k,\eta,n,\tau) \geq \delta/2$ is non-negligible. Thus, if HB-MP* is secure in the DET model, HB-MP* is secure in the GRS model. In other words, if HB-MP* is vulnerable to the GRS attack, then it must be vulnerable to the DET attack.

6.4 HB-MP security in the DET model*

We cannot provide a strict reduction from the LPN problem to HB-MP* security in the DET model. Instead, we conjecture that the HB-MP* protocol is secure in the DET model.

Claim 1: In the DET model, the HB-MP* protocol is as secure as the HB+ protocol.

Justification: Let's recall the HB+ protocol, which is provably secure in the DET model (Juels and Weis, 2005; Katz and Shin, 2006). The tag first generates a random blinding vector b and sends it to the reader; then, the reader selects a challenge vector a at random. After receiving a, the tag computes and sends the one-bit response z, computed by equation (1). Vector x is of k_a bits and vector y is of k_b bits.

$$z = a.x \oplus b.y \oplus v \tag{1}$$

As for the HB-MP* protocol, we could define $a = a, x = \hat{a}, b = s$ and $y = x$, as these terms are uniformly distributed because they are linearly independent according to Lemma 1 and 2. Then, the response bit is equivalently computed by:

$$z = a_i.\hat{a}_i \oplus x.s \oplus v \tag{2}$$

The HB-MP* and HB+ protocols are very alike, except that instead of sending the z as in HB+, HB-MP* generates a vector b and sends it, which satisfies $z = b.s_m$. This will help the reader to get the value of z without the need to expose its value, which might further help in exposing the secret keys, this is the major difference.

Let's compare (1) for HB+ with (2) for HB-MP* side-by-side for security level. In Phase 1, the adversary can freely choose the challenges. When setting $a = 0^{k_a}$ in (1) against HB+, the adversary can get an LPN instance $(b, z = (b.y) \oplus v)$. Therefore, as concluded by Levieil and Fouque (2006), the hardness of HB+ against a DET adversary only relies on the k_b-bit LPN instances. In contrast, even if choosing $a = 0^{k_a}$ in (2) against HB-MP*, the adversary obtains an LPN instance $(b \oplus x_m)$. Consequently, the hardness of HB-MP* depends on the m-bit LPN instances, no matter what challenges the adversary chooses. Similarly, as for Phase 2, in which the adversary can choose arbitrary blinding vectors, k_a in HB+ has to be at least d to guarantee d-bit security (Levieil and Fouque, 2006), while the adversary against HB-MP* is confronting the whole amount $a_i \,.\, \hat{a}_i \oplus x \,.\, s$, which actually provides $(m + k_a)$-bit security.

Therefore, HB-MP* is at least as secure as the HB+ protocol in the DET model.

6.5 HB-MP security in the OOV model*

OOV attack involves more than manipulating the challenge or blending vector messages, it manipulates the response z as well. Although HB-MP* contains only two communicated messages which when modified by an OOV attack could be considered in general under the GRS model, it still needs to clearly state a proof of security in the OOV model or alternatively against general MIM adversaries allowed to perturb any message of the protocol. Though we do not have a formal proof of such a result, we have provided in Section 5 a heuristic analysis to argue in favor of the resistance of HB-MP* against arbitrary OOV-MIM adversaries. This will assess the claim that could be extended in future work with a formal proof supporting the informal one.

7. Performance analysis

In this section, the performance of the proposed HB-MP* will be analyzed in terms of storage, computation and communication requirements.

Regarding storage requirement, HB-MP* requires only one shared secret key between tag and reader, which makes it very efficient for low-cost tags compared to HB+ and HB-MP. So if we propose the key size is k bits, HB-MP* will need only k bits for storage on tag, while HB+ and HB-MP will need $2k$ bits.

The on-tag computation is simple and applicable for such low-cost devices, as it uses only lightweight operations such as dot product, XOR and Rotation. There is a slight increase in the number of required gates compared to HB+ and HB-MP, but it is considered acceptable as long as they are lightweight and increasing the security.

The communication cost is decreased compared to HB+, by reducing the number of exchanged messages to two instead of three, besides decreasing the message size to m. This will be the same compared to HB-MP. The total number of exchanged bits is only $2mq$ in HB-MP*, while HB+ needs $2kq+q$ noting that $(m < k)$.

8. Implementation

In this section, we present a prototype implementation of the proposed protocol HB-MP* through a given scenario besides implementing the most known attack. The primary goal for implementing this prototype is twofold: first, to test the protocol immunity

against the pre-mentioned attacks by running communication between the two parties (a reader and a tag) and launching the corresponding attack. Second, to measure the execution time for both the proposed protocol and the most related HB+ protocol to compare their performance. This will help in analyzing the protocol security and applicability for authentication.

The reason behind using a prototype instead of implementing a real environment using physical tags and readers is that RFID tags control logic comes programmed using a special RFID compiler, which makes it very difficult to be reprogrammed. Therefore, implementing our environment requires building a tag from scratch, which is beyond the scope and the time constrain of this study. Besides, what is being tested is the authentication process between the tag and reader and the packets sent between the two parties. These packets can still be examined irrespective of the communication medium being used.

The prototype platform we have implemented is a basic platform that models the tags and readers in an RFID system as a collection of entities. It was written entirely in the C# programming language. A collection of classes simulating the implementation of the HB+ and HB-MP* protocols were constructed to test the communication and to compare results. Communication between the two RFID components (the reader and the tag) was established through an instance from the class protocol.

From the results, we can see that GRS attackers will be able to guess tag secrets about 45 per cent of the times an attack is launched, while it will be very difficult to reveal any of them using the HB-MP* protocol (Figure 5). That is because the secret was not multiplied by the modified challenge of an attacker, which prevents a GRS attacker from revealing any secret information and accordingly prevents the GRS attack from being successful. Also, we can see from the figure that an attacker with a calculated secret will pass the impersonation phase of an attack process using HB+ protocol with a percentage of 57 per cent compared to the HB-MP* protocol, where it will be only 6 per cent. The high percentage of a successful impersonation in HB+ protocol is due to the false acceptance rate, which represents the percentage of an attacker is accepted by randomly guessing the secret. In general, both results prove the security of HB-MP*.

A secure protocol will try to minimize the number of both wrongly rejected and wrongly accepted tags. Accordingly, we have computed these numbers using parameters $q = 100$, Key = 223, epsi = 0.25, var = 0.10 (Threshold = 0.25 + 0.10 = 0.35), and found that both

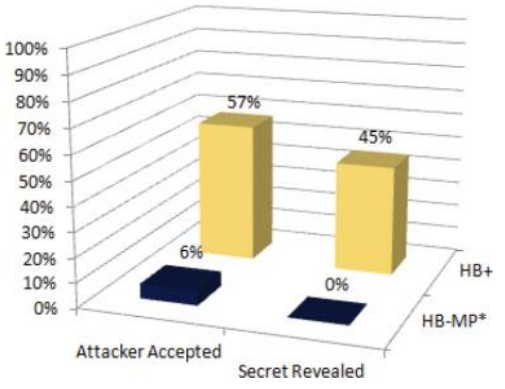

Figure 5.
Success percentage rate of an attacker

false accepted and false rejected tags were minimized using the HB-MP* compared to the HB+ protocol, which also counts for the HB-MP* security (Figure 6).

A universal measurement of performance is to count the time required to accomplish a certain task. Accordingly, we computed the time needed (in seconds) to accomplish one iteration of both protocols and also the time needed to conduct 100 authentication sessions. We can see that HB-MP* shows a slight increase in the time required for an authentication process to complete compared to an HB+ protocol. This overhead is expected and reasonable due to the increase in the required computations compared to the HB+, and as a cost of the increased security (Figure 7).

9. Conclusion

HB family protocols are one of the most attractive schemes in the lightweight authentication field. Most of the HB family protocols are vulnerable to the GRS attack, which is a type of man-in-the-middle attack. Accordingly, HB-MP*, an enhanced version of HB family, is proposed to reduce the vulnerability and keep the simplicity of the original protocol.

Security evaluation of the proposed protocol was conducted both theoretically and using a formal proof. It was shown that HB-MP* is secure under the DET model and the GRS model through different steps.

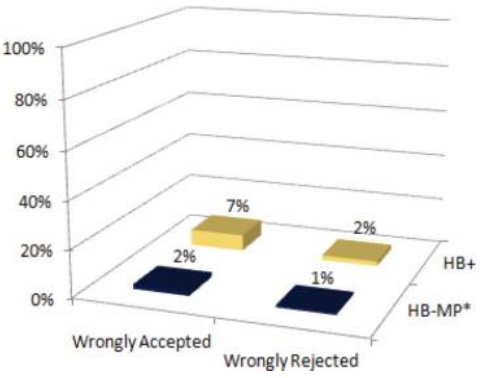

Figure 6.
False rejected and false accepted tags out of 100

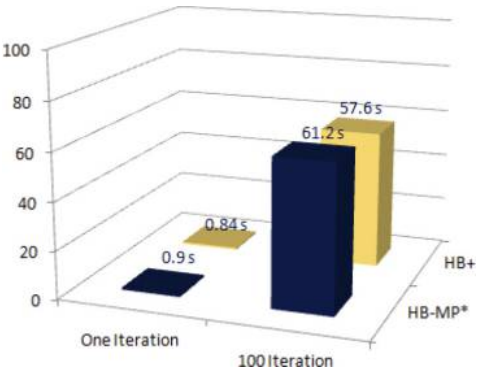

Figure 7.
Elapsed time for the authentication process

To show the applicability of the proposed protocol, its security and performance were evaluated using a prototype to quickly and realistically generate results. Results show a clear improvement in the security especially against GRS attacks, besides a decrease in the rate of false negatives and false positives. Regarding performance, results show a slight increase in time of computation, which interprets a slight increase in the number of required gates compared to HB+. This increase is considered neglected, given the provided security. In general, all results show that HB-MP* enjoys a great improvement in terms of security and performance.

References

Ali, S., Mohamed, R. and Fahim, M. (2011), "RCHB: Light-weight, provably-secure variants of the HB protocol using rotation and complementation", *Proceedings in 5th International Conference on Network and System Security, IEEE, Milan, 6-8 September 2011*, pp. 244-248.

Bellare, M., Desai, A., Jokipii, E. and Rogaway, P. (1997), "A concrete security treatment of symmetric encryption", *Proceedings of 38th Symposium on Foundations of Computer Science, IEEE Press, Miami Beach, Florida, 20-22 October 1997*, pp. 394-403.

Bongno, Y., Man, Y.S., Sujin, Y., Hyun, S.O., Yoonjoo, K., Chuljin, K. and Kyung-Ho, K. (2009), "HB-MP++ Protocol: an ultra light-weight authentication protocol for RFID System", *Proceedings of IEEE International Conference on RFID, Orlando, FL*, pp. 186-191.

Bringer, J., Chabanne, H. and Dottax, E. (2006), "HB++: a lightweight authentication protocol secure against some attacks", *Proceedings of IEEE International Conference on Privacy and Trust in Pervasive and Ubiquitous Computing SecPerU2006, Second International Workshop on Security, France*, pp. 28-33.

Bringer, J. and Chabanne, H. (2008), "Trusted-HB: a low-cost version of HB+ secure against man-in-the-middle attacks", *IEEE Transactions on Information Theory*, Vol. 54, pp. 4339-4342.

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

Duc, D., Lee, H. and Kim, K. (2009), *Toward Designing Provably Secure Cryptographic Protocols for RFID Tags*, Auto-ID Lab Whitepaper Series, Daejeon, March 2009.

Feldhofer, M., Dominikus, S. and Wolkerstorfer, J. (2004), *Strong Authentication for RFID Systems Using the AES Algorithm*, LNCS, 3156, Springer, Heidelberg, pp. 357-370.

Gilbert, H., Robshaw, M.J.B. and Sibert, H. (2004), "Active attack against HB+: a provably secure lightweight Authentication Protocol", *IEEE Electronics Letters*, Vol. 41, pp. 1169-1170.

Gilbert, H., Robshaw, M.J.B. and Seurin, Y. (2008a), "Good variants of HB+ are hard to find", *Proceedings of Financial Cryptography and Data Security (FC 2008), LNCS, 5143, Springer, Heidelberg*, pp. 156-170.

Gilbert, H., Robshaw, M.J.B. and Seurin, Y. (2008b), "HB#: increasing the security and efficiency of HB+", *Advances in Cryptology – Eurocrypt*, Vol. 4965, pp. 361-378.

Hammouri, G. and Sunar, B. (2008), "PUF-HB: a tamper-resilient HB based authentication protocol", *Proceedings of Applied Cryptography and Network Security (ACNS 2008), LNCS, 5037, Springer, Heidelberg*, pp. 346-365.

Hopper, N. and Blum, M. (2001), "Secure human Identification Protocols", *Proceedings of Advances in Cryptology-ASIACRYPT 2001, LNCS, 2248*, Springer, Heidelberg, pp. 52-66.

Juels, A. and Weis, S. (2005), "Authenticating pervasive devices with human protocols", *Proceedings Advances in Cryptology- CRYPTO 2005, LNCS, 3621*, *Springer*, *Heidelberg*.

Juels, A. (2006), "RFID security and privacy: a research survey", *IEEE Journal on Selected Areas in Communications*, Vol. 24 No. 2, pp. 381-394.

Katz, J. and Shin, J. (2006), "Parallel and concurrent security of the HB and HB+ Protocols", *Proceedings of Advances in Cryptology – EUROCRYPT 2006, LNCS, 4004*, *Saint Petersburg*, pp. 73-87.

Levieil, E. and Fouque, P. (2006), "An improved LPN algorithm", *Security and Cryptography for Networks (SCN 2006), LNCS, 4116*, pp. 348-359.

Li, Z., Gong, G. and Qin, Z. (2009), "Secure and efficient HB-CM entity authentication protocol", *Proceedings of IACR Cryptology ePrint Archive, 2009/444*.

Li, Z., Gong, G. and Qin, Z. (2010), "Secure and efficient LCMQ entity authentication protocol", Centre for Applied Cryptographic Research (CACR) Technical Reports, CACR, pp. 2010-2021.

Lyubashevsky, V. and Daniel, M. (2013), "Man-in-the-middle secure authentication schemes from LPN and weak PRFs", *Advances in Cryptology – CRYPTO 2013*, Springer, Berlin, Heidelberg, pp. 308-325.

Madhavan, M., Thangaraj, A., Sankarasubramanian, Y. and Viswanathan, K. (2010), "NLHB: a non-linear Hopper Blum protocol", *Proceedings of IEEE National Conference on Communications (NCC)*, *Austin, TX*.

Munilla, J. and Peinado, A. (2007), "HB-MP: A further step in the HB-family of lightweight authentication protocols", *Computer Networks*, Vol. 51 No. 9, pp. 2262-2267.

Ouafi, K., Overbeck, R. and Vaudenay, S. (2008), "On the security of HB# against a Man-in the-Middle Attack", *Proceedings of Advances in Cryptology – ASIACRYPT 2008, LNCS, 5350*, *Springer*, *Heidelberg*.

Piramuthu, S. (2006), "HB and related lightweight authentication protocols for secure RFID Tag/ Reader Authentication", *Proceedings of CollECTeR Europe Conference*, *Basel, Switzerland*.

Piramuthu, S. and Tu, Y. (2007), "Modified HB Authentication Protocol", *Proceedings of Western European Workshop on Research in Cryptology*, *Germany*, pp. 41-44.

Xuefei, L., Keith, M. and Konstantinos, M. (2008), "HB-MP+ protocol: an improvement on the HB-MP Protocol", *Proceedings of IEEE International Conference on RFID*, *Las Vegas, Nevada*, pp. 118-124.

Zhang, Y. and Kitsos, P. (2009), *Security in RFID and Wireless Sensor Networks*, Edited by: Yan Zhang and Paris Kitsos, Auerbach Publications, Taylor & Francis Group, Journal Publication.

Corresponding author
Omaimah Bamasag can be contacted at: obamasek@kau.edu.sa