

# Good Variants of $\text{HB}^+$ are Hard to Find

Henri Gilbert, Matthew J.B. Robshaw, and Yannick Seurin

Orange Labs,  
38–40 rue du General Leclerc, Issy les Moulineaux, France  
{henri.gilbert,matt.robshaw,yannick.seurin}@orange-ftgroup.com

**Abstract.** The strikingly simple  $\text{HB}^+$  protocol of Juels and Weis [11] has been proposed for the authentication of low-cost RFID tags. As well as being computationally efficient, the protocol is accompanied by an elegant proof of security. After its publication, Gilbert *et al.* [8] demonstrated a simple man-in-the-middle attack that allowed an attacker to recover the secret authentication keys. (The attack does not contradict the proof of security since the attacker lies outside the adversarial model.) Since then a range of schemes closely related to  $\text{HB}^+$  have been proposed and these are intended to build on the security of  $\text{HB}^+$  while offering resistance to the attack of [8]. In this paper we show that many of these variants can still be attacked using the techniques of [8] and the original  $\text{HB}^+$  protocol remains the most attractive member of the  $\text{HB}^+$  family.

**Key words:**  $\text{HB}^+$ , RFID tags, authentication, LPN.

## 1 Introduction

The extension of cryptographic functions to low-cost RFID tags is an active area of research. The combination of novel security requirements and demanding physical environments provides a major incentive to the development of new designs and techniques.

Juels and Weis introduced  $\text{HB}^+$  at Crypto 2005 [11]. The protocol is a multi-round symmetric key authentication protocol where each round consists of three communications between the reader and the tag. On the tag,  $\text{HB}^+$  is computationally lightweight since it requires only simple bit-wise operations. Furthermore, the protocol is supported by a proof of security against an active attacker in what the  $\text{HB}^+$  designers call the *detection-based* model. In this model adversaries can interrogate a tag in any way they wish, and then they must try and pass themselves off as an authentic tag to a legitimate reader. In loose terms, Juels and Weis show that for such an attack to succeed the attacker would be able to break an instance of the *Learning Parity with Noise (LPN)* problem which is believed to be hard.

However, if we allow the attacker to do a little more—*i.e.* if we leave the detection-based model—then  $\text{HB}^+$  becomes susceptible to a simple attack. In particular, if an attacker can slightly modify messages from the reader and observe whether the legitimate reader still accepts the legitimate tag, then the

attacker can recover secret key information. This is, in essence, the attack of Gilbert *et al.* [8] which we will refer to as the GRS attack in what follows. Some commentators suggest that interfering with the tag-reader communication would be technically difficult. Others claim that forbidding such manipulation during analysis ignores the full characteristics of a potential attack and makes potentially dangerous assumptions on the limitations of an attacker. However this is not the concern of this paper. Instead we will focus on the body of research that has evolved from both  $\text{HB}^+$  and the GRS attack.

In his paper introducing the block cipher RC5, Rivest states that “... a simpler structure is perhaps more interesting to analyze and evaluate ...” [19]. This is now a well-established principle in cryptographic design and the simplicity of both the original  $\text{HB}^+$  proposal and the GRS attack have given rise to a number of  $\text{HB}$ -related protocols in the literature. The goal of these protocols is that they retain some of the successful properties of  $\text{HB}^+$  while also resisting the GRS attack. In this paper we will take a critical look at such variants. We can show that despite claims to the contrary, the GRS attack can often be applied or extended to these new variants. Thus the tolerance of the new schemes to the GRS attack is often equivalent to that of  $\text{HB}^+$  and yet, at the same time, they suffer from additional complexity and/or reduced practicality. In short, we show that  $\text{HB}^+$  variants that resist the GRS attack are not that easy to come by.

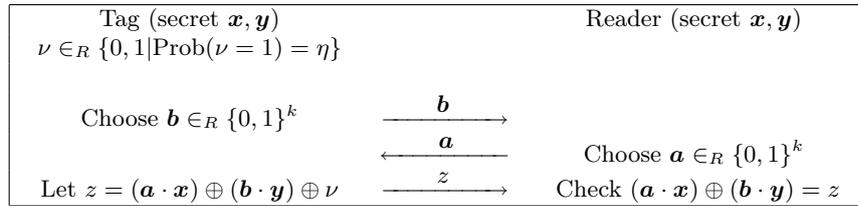
Our paper is organised as followed. After introducing the  $\text{HB}^+$  protocol we turn our attention to the variants  $\text{HB}^{++}$ ,  $\text{HB}^*$ ,  $\text{HB-MP}'$ , and  $\text{HB-MP}$ . These are treated in the order they appear in the literature and in Sections 3, 4 and 5 we provide a description and security analysis of each. We then discuss the implications of our work in Section 6 and draw our conclusions. It should be noted that our work is not concerned with the proofs of security for  $\text{HB}^+$  or its variants. Instead our focus is on applications of the GRS attack.

Throughout we aim to use established notation. There will be some interplay between vectors  $\mathbf{x} \in \{0, 1\}^k$  and scalars in  $\mathbb{F}_2$  and we use bold type  $\mathbf{x}$  to indicate a vector while scalars  $x$  are written in normal text. The *scalar product* of two vectors  $\mathbf{x}$  and  $\mathbf{y}$  will be written as  $\mathbf{x} \cdot \mathbf{y}$  while their bitwise addition will be denoted using  $\oplus$  just as for single bits. We denote the *Hamming weight* of  $\mathbf{x}$  by  $\text{Hwt}(\mathbf{x})$ . Several protocols require a rotation of  $\mathbf{x}$  by  $i$  bit positions to the left; we denote this operation by  $\text{ROT}_i(\mathbf{x})$ .

## 2 The $\text{HB}^+$ Protocol and the GRS Attack

There are now several protocols based on  $\text{HB}^+$  and these offer a variable level of security and practicality. We start by reviewing the original protocol, though all depend for their security on the conjectured hardness of the *Learning Parity with Noise* (LPN) problem [11].

**LPN Problem.** Let  $A$  be a random  $(q \times k)$ -binary matrix, let  $\mathbf{x}$  be a random  $k$ -bit vector, let  $\eta \in ]0, \frac{1}{2}[$  be a noise parameter, and let  $\boldsymbol{\nu}$  be a random  $q$ -bit vector such that  $\text{Hwt}(\boldsymbol{\nu}) \leq \eta q$ . Given  $A$ ,  $\eta$ , and  $\mathbf{z} = A \cdot \mathbf{x}^t \oplus \boldsymbol{\nu}^t$ , find a  $k$ -bit vector  $\mathbf{y}^t$  such that  $\text{Hwt}(A \cdot \mathbf{y}^t \oplus \mathbf{z}) \leq \eta q$ .



**Fig. 1.** One single round of  $\text{HB}^+$  [11]. The entire authentication process requires  $r$  rounds and, in this basic form, each round consists of the three passes shown. Provided the tag fails less than some threshold  $t$  number of rounds, the tag is authenticated.

We will not consider the intractability of the LPN problem directly in this paper, though we observe that the problem is not as difficult as was originally thought [7,15]. This means that the parameters for  $\text{HB}^+$  and its variants often need to be increased.

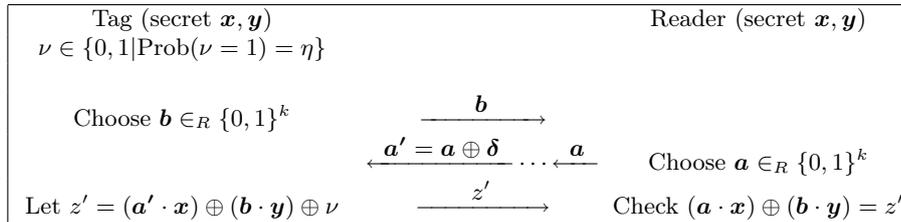
## 2.1 The $\text{HB}^+$ protocol

The  $\text{HB}^+$  protocol is outlined in Figure 1. The tag and the reader share two  $k$ -bit secrets  $\mathbf{x}$  and  $\mathbf{y}$ . One round of  $\text{HB}^+$  is as follows: the tag selects a random  $k$ -bit blinding vector  $\mathbf{b}$  and sends it to the reader. The reader challenges the tag with a random  $k$ -bit vector  $\mathbf{a}$ . The tag computes the response  $z = (\mathbf{a} \cdot \mathbf{x}) \oplus (\mathbf{b} \cdot \mathbf{y}) \oplus \nu$ , where  $\nu$  is a random noise bit taking the value 1 with probability  $\eta \in ]0, \frac{1}{2}[$ . This is repeated for  $r$  rounds, and the tag is authenticated if the number of errors (*i.e.*  $z$  distinct from  $(\mathbf{a} \cdot \mathbf{x}) \oplus (\mathbf{b} \cdot \mathbf{y})$ ) is less than a threshold  $t = ur$  where  $u \in ]\eta, \frac{1}{2}[$ . The difficulty of the LPN problem [7,11,13,15] is related to both  $k$  and the parameter  $\eta$  which governs how much noise is added to the correct computations by a valid tag. In its original state  $\text{HB}^+$  consists of multiple rounds each of three passes. The parallel version of  $\text{HB}^+$ —for which a proof of security also exists [13,14]—compresses the multiple rounds into one single three-pass round.

Immediately one can see that  $\text{HB}^+$  requires very modest on-tag computation. Leaving aside generating  $\mathbf{b}$  and the bit  $\nu$ , computation on the tag is reduced to a dot-product, which can be computed bit-wise, and a single bit exclusive-or. The novelty and simplicity of  $\text{HB}^+$  immediately generated considerable interest. Katz and Shin [13] closed gaps and extended the original proof of security while follow-on work by Katz and Smith [14] considered different noise levels.

## 2.2 An active attack on $\text{HB}^+$

A simple active attack on  $\text{HB}^+$  is provided in [8]. The attack applies equally to the serial and the parallel versions of  $\text{HB}^+$ . For this attack it is assumed that an adversary can manipulate challenges sent by a legitimate reader to a legitimate tag during authentication. Further, we assume that the adversary learns whether such manipulation leads to an authentication failure or not.



**Fig. 2.** The attack of [8] on  $\text{HB}^+$ . The adversary modifies the communications between reader and tag (by adding some perturbation  $\boldsymbol{\delta}$  and notes whether authentication is still successful. This reveals one bit of secret information.

The attack consists of choosing a constant  $k$ -bit vector  $\boldsymbol{\delta}$  and using it to perturb the challenges sent by a legitimate reader to the tag;  $\boldsymbol{\delta}$  is exclusive-or'ed to each authentication challenge for each of the  $r$  rounds of authentication. If the authentication process is successful then we must have that  $\boldsymbol{\delta} \cdot \mathbf{x} = 0$  with overwhelming probability. Otherwise  $\boldsymbol{\delta} \cdot \mathbf{x} = 1$  with overwhelming probability. Thus we gain one bit of secret information. The attack is illustrated in Figure 2 for one round of the  $\text{HB}^+$  protocol.

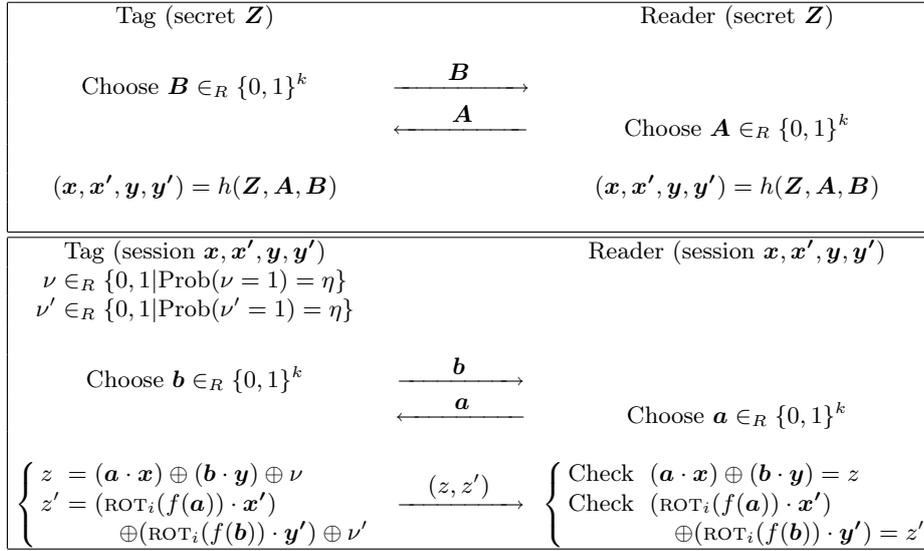
To retrieve the  $k$ -bit secret  $\mathbf{x}$  one can repeat the attack  $k$  times for linearly independent  $\boldsymbol{\delta}$ 's and solve the resulting system. Conveniently, an adversary can choose  $\boldsymbol{\delta}$ 's with a single non-zero bit. With  $\mathbf{x}$  an attacker can impersonate the tag by setting  $\mathbf{b} = \mathbf{0}$ . Alternatively, an attacker can emulate a false tag using  $\mathbf{x}$ , send a chosen blinding factor  $\mathbf{b}$  to a legitimate reader, and return  $\mathbf{a} \cdot \mathbf{x}$  to the challenge  $\mathbf{a}$ . If successful  $\mathbf{b} \cdot \mathbf{y} = 0$ , otherwise  $\mathbf{b} \cdot \mathbf{y} = 1$ , with overwhelming probability. Thus  $\mathbf{y}$  can be recovered with  $k$  linearly independent  $\mathbf{b}$ .

The attack is mathematically simple though it is not covered by the existing proof of security since the attacker needs to manipulate challenges and know whether authentication is successful [11]. Yet, despite the technical difficulties of interfering in a tag-reader exchange, the attack should be viewed as *certificational*. Certainly a variant of  $\text{HB}^+$  that is both computationally simple and resistant to the GRS attack would be of some considerable interest.

All the variants to  $\text{HB}^+$  we will consider in the following sections share some properties with  $\text{HB}^+$ . In particular, they all consist of the repetition of  $r$  basic rounds. An honest tag interacting with an honest reader may be rejected with a probability we denote  $P_{\text{FR}}$  (false rejection probability). An adversary answering randomly at each round will be authenticated with a probability we denote  $P_{\text{FA}}$  (false acceptance probability). For  $\text{HB}^+$  these are given by  $P_{\text{FR}} = \sum_{i=t+1}^r \binom{r}{i} \eta^i (1-\eta)^{r-i}$  and  $P_{\text{FA}} = \frac{1}{2^r} \sum_{i=0}^t \binom{r}{i}$ .

### 3 The Variant $\text{HB}^{++}$

**Description of  $\text{HB}^{++}$ .** The protocol  $\text{HB}^{++}$  is proposed by Bringer *et al.* [3]. The complete proposal consists of two stages. In the first, illustrated in Figure 3,



**Fig. 3.** The  $\text{HB}^{++}$  protocol. Above: At the start of each authentication, a preliminary exchange of  $2k$  bits and the use of a universal hash function  $h$  are required to derive the session secrets  $\mathbf{x}, \mathbf{x}', \mathbf{y}, \mathbf{y}'$ . Below: One single round  $i$  of  $\text{HB}^{++}$ . The entire authentication process requires  $r$  rounds and, in this basic form, each round consists of the three passes shown. Provided the tag fails both tests less than some threshold  $t$  number of rounds, the tag is authenticated.

four  $k$ -bit secrets  $\mathbf{x}, \mathbf{x}', \mathbf{y}, \mathbf{y}'$  are derived by the tag and the reader from a shared secret  $\mathbf{Z}$ . These derived secrets might be viewed as session keys. Then  $\text{HB}^{++}$  consists of  $r$  rounds where each round consists of three passes, just as in  $\text{HB}^+$ .

A single round of  $\text{HB}^{++}$  is illustrated in Figure 3. We can see that things are slightly more complicated than in  $\text{HB}^+$ . In particular, once the blinding vector  $\mathbf{b}$  and the challenge  $\mathbf{a}$  have been sent, there are two on-tag computations.

The first looks like the  $\text{HB}^+$  on-tag computation and simply consists in computing  $z = (\mathbf{a} \cdot \mathbf{x}) \oplus (\mathbf{b} \cdot \mathbf{y}) \oplus \nu$ . The second involves a permutation  $f$  (which is in fact a layer of five-bit S-boxes) and also requires that  $k$ -bit quantities be rotated by  $i$  bit positions where  $i$  denotes the round (rounds are numbered from 0 to  $r - 1$ ). The second response bit is given by  $z' = (\text{ROT}_i(f(\mathbf{a})) \cdot \mathbf{x}') \oplus (\text{ROT}_i(f(\mathbf{b})) \cdot \mathbf{y}') \oplus \nu'$ . Both noise bits  $\nu$  and  $\nu'$  are randomly chosen according to the noise parameter  $\eta$ . For the tag to be authenticated, the number of erroneous  $z$  answers and the number of erroneous  $z'$  answers must be less than some threshold  $t = ur$ , where  $u \in ]\eta, \frac{1}{2}[$ . Consequently the false rejection and false acceptance probabilities are:

$$P_{\text{FR}} = 1 - \left( \sum_{i=0}^t \binom{r}{i} \eta^i (1 - \eta)^{r-i} \right)^2 \quad \text{and} \quad P_{\text{FA}} = \left( \frac{1}{2^r} \sum_{i=0}^t \binom{r}{i} \right)^2.$$

The proposed number of rounds is not given, but the parameters in [3], in particular  $k = 80$ , give a much-reduced level of security when compared to  $\text{HB}^+$ .

**Variant of Piramuthu.** Piramuthu [18] proposes a modification to  $\text{HB}^{++}$  but the details are unclear. The main difference with  $\text{HB}^{++}$  appears to be the removal of the first on-tag computation. However this means that what remains is equivalent to  $\text{HB}^+$  itself. Thus it will have all the characteristics of  $\text{HB}^+$  while at the same time possessing a heavier on-tag computation. We do not consider this variant further.

**Attacking  $\text{HB}^{++}$  without the renewed secrets.** We first show how to attack  $\text{HB}^{++}$  when the preliminary phase to renew the secrets  $(\mathbf{x}, \mathbf{x}', \mathbf{y}, \mathbf{y}')$  is omitted. We note that Wagner described an attack on a preliminary version of  $\text{HB}^{++}$  where the rotations are omitted, which was described in the original paper [3]. In this attack, the attacker guesses a short portion of the secrets  $\mathbf{x}$  and  $\mathbf{x}'$  and then modifies the challenges sent by the reader but also the answer returned by the tag accordingly to his guess. If the tag is authenticated, the attacker knows that with high probability his guess was right. Bringer *et al.* introduced the rotations to counter this attack. The rationale is that this way, even if the perturbation of  $\mathbf{a}$  is localized, the perturbation of  $f(\mathbf{a})$  will affect all bits of the secret  $\mathbf{x}'$ . It seems however that the following fact was overlooked: it is not necessary for the attacker to perturb *all* the rounds of the protocol but only a fixed fraction to be able to gain information through the decision of the reader. As we will show now, this leads to an efficient variant of the GRS attack.

Unlike the attack of Wagner, the attack we describe doesn't require that we modify the answers of the tag. As in the GRS attack, the attacker adds a fixed vector  $\boldsymbol{\delta}$  to the challenges  $\mathbf{a}_i$  sent by the reader, *but only for a fixed number of rounds*  $s < r$  (say the first  $s$  rounds). Let  $\sigma_i$  and  $\sigma'_i$  denote the total error vectors on the answers  $z_i$  and  $z'_i$  of the tag at round  $i$ . For rounds  $i = 0$  to  $s - 1$ , one has  $\sigma_i = \nu_i \oplus \boldsymbol{\delta} \cdot \mathbf{x}$  and  $\sigma'_i = \nu'_i \oplus \boldsymbol{\delta}'_i \cdot \mathbf{x}'$  where  $\boldsymbol{\delta}'_i = \text{ROT}_i(f(\mathbf{a}_i \oplus \boldsymbol{\delta}) \oplus f(\mathbf{a}_i))$ , whereas for rounds  $i = s$  to  $r - 1$ , one simply has  $\sigma_i = \nu_i$  and  $\sigma'_i = \nu'_i$ . Let  $N$  (resp.  $N'$ ) denote the number of answers  $z_i$  (resp.  $z'_i$ ) in error. The function  $f$  was chosen to satisfy good differential properties, meaning that for a fixed  $\boldsymbol{\delta}$  and a fixed  $\mathbf{c}$ ,  $\Pr_{\mathbf{a}}[f(\mathbf{a} \oplus \boldsymbol{\delta}) \oplus f(\mathbf{a}) = \mathbf{c}]$  is very small for most values of  $\boldsymbol{\delta}$ . Hence the noise bits  $\sigma'_i$  for rounds 0 to  $s - 1$  are close to uniformly distributed and we may assume<sup>1</sup> that, whatever  $\boldsymbol{\delta}$ ,  $N'$  is distributed as the sum of  $s$  Poisson trials taking the value 0 or 1 with probability  $\frac{1}{2}$  and  $r - s$  Poisson trials taking the value 0 with probability  $1 - \eta$  and 1 with probability  $\eta$ . The expected value of  $N'$  is  $\mu' = \frac{s}{2} + \eta(r - s) = \frac{1}{2}(1 - 2\eta)s + \eta r$ . Unlike  $N'$ , the distribution of  $N$  depends on the value of  $\boldsymbol{\delta} \cdot \mathbf{x}$ . When  $\boldsymbol{\delta} \cdot \mathbf{x} = 0$ , the answers  $z_i$  are undisturbed and  $N$  is distributed as the sum of  $r$  Poisson trials taking the value 0 with probability  $1 - \eta$

<sup>1</sup> Note that this is strictly speaking an approximation and that in fact the distribution of  $(\sigma'_0, \dots, \sigma'_{s-1})$  will be nearly uniform for an overwhelming fraction of  $\mathbf{x}'$  and  $\boldsymbol{\delta}$ . Concrete values will depend on the parameter  $\Delta_f$  defined in [3].

and 1 with probability  $\eta$ . The expected value of  $N$  in this case is  $\mu_0 = \eta r < t$ . When  $\delta \cdot \mathbf{x} = 1$ , the  $s$  first answers  $z_i$  are correct with probability  $\eta$  and incorrect with probability  $1 - \eta$ , while the  $r - s$  remaining rounds are undisturbed. In that case,  $N'$  is distributed as the sum of  $s$  Poisson trials taking the value 0 with probability  $\eta$  and 1 with probability  $1 - \eta$  and  $r - s$  Poisson trials taking the value 0 with probability  $1 - \eta$  and 1 with probability  $\eta$ . The expected value of  $N$  is  $\mu_1 = (1 - \eta)s + \eta(r - s) = (1 - 2\eta)s + \eta r$ . Consequently, if we choose  $s$  such that  $\mu' < t$ , and  $\mu_1 > t$ , the number of errors on  $z'$  will be less than  $t$  with high probability, and the reader's decision will indicate whether the number of errors on  $z$  was less or more than  $t$ , which in turn will indicate whether  $\delta \cdot \mathbf{x} = 0$  or 1.

Going into details, we will compute the advantage of the attacker guessing  $\delta \cdot \mathbf{x} = 0$  when the reader accepts and  $\delta \cdot \mathbf{x} = 1$  when the reader rejects. Denoting WG the event that the guess is wrong, we will upper bound the probability of WG as follows:

$$\begin{aligned}
\Pr[\text{WG}] &= \frac{1}{2} (\Pr[\text{WG} \mid \delta \cdot \mathbf{x} = 0] + \Pr[\text{WG} \mid \delta \cdot \mathbf{x} = 1]) \\
&= \frac{1}{2} (\Pr[\mathcal{R} \text{ rejects} \mid \delta \cdot \mathbf{x} = 0] + \Pr[\mathcal{R} \text{ accepts} \mid \delta \cdot \mathbf{x} = 1]) \\
&= \frac{1}{2} (\Pr[(N > t) \vee (N' > t) \mid \delta \cdot \mathbf{x} = 0] \\
&\quad + \Pr[(N \leq t) \wedge (N' \leq t) \mid \delta \cdot \mathbf{x} = 1]) \\
&\leq \frac{1}{2} (\Pr[N' > t] + \Pr[N > t \mid \delta \cdot \mathbf{x} = 0] + \Pr[(N \leq t) \mid \delta \cdot \mathbf{x} = 1]) \\
&\leq \frac{1}{2} \left( e^{-\frac{(t-\mu')^2}{3\mu'}} + e^{-\frac{(t-\mu_0)^2}{3\mu_0}} + e^{-\frac{(\mu_1-t)^2}{2\mu_1}} \right)
\end{aligned}$$

where the last inequalities come from the Chernoff bounds (see Appendix). According to the expressions of  $\mu'$  and  $\mu_1$ , the condition on  $s$  to have  $\mu' < t$  and  $\mu_1 > t$  is

$$\frac{t - \eta r}{1 - 2\eta} < s < 2 \frac{t - \eta r}{1 - 2\eta}.$$

Whether such  $s$  exist will depend on the parameters of the scheme, however we note that in order for the protocol to have a low false rejection probability,  $t$  has to be sufficiently distinct from  $\eta r$ . In particular, taking  $t = \lceil \eta r \rceil$  yields  $P_{\text{FR}} \simeq 0.4$  (see Section 6), which is unacceptable. Hence, it is arguable that such  $s$  will exist. However, concrete values in the formulae show that it is uncertain for the attacker to make a guess when the reader rejects, as the probability for this to happen when  $\delta \cdot \mathbf{x} = 0$  (due to  $N' > t$ ) may be quite high when  $\mu'$  is close to  $t$ . A much better strategy is to make a guess only when the reader accepts, guessing that  $\delta \cdot \mathbf{x} = 0$ . In this case, the probability of a wrong guess is given by  $\Pr[\text{WG}_a] = \Pr[\delta \cdot \mathbf{x} = 1 \mid \mathcal{R} \text{ accepts}] = \frac{1}{2} P_a^{-1} \Pr[\mathcal{R} \text{ accepts} \mid \delta \cdot \mathbf{x} = 1]$ , where  $P_a$  is the probability that the reader accepts for a random  $\delta$ .  $\Pr[\text{WG}_a]$  decreases with  $s$  as the gap between  $t$  and  $\mu_1$  increases. The cost is that a higher number of attempts will be required to retrieve  $\mathbf{x}$ , namely  $O(k \cdot P_a^{-1})$ , which may become impractical as  $s$  tends to  $r$  since  $P_a$  becomes negligible. However,

for  $s = \left\lfloor 2 \frac{t-\eta r}{1-2\eta} \right\rfloor$ ,  $\mu' \simeq t$  so that  $N'$  is more or less than  $t$  with probability roughly  $1/2$ , and hence the reader accepts with probability roughly  $1/4$ . We computed concrete values for different set of parameters. For example, when  $(r, t, \eta) = (80, 30, 0.25)$  we obtain, with  $s = 40$ ,  $\Pr[\text{WG}_a] \simeq 0.007$  and  $P_a^{-1} \simeq 3.62$ , whereas for  $(r, t, \eta) = (160, 60, 0.25)$ , we obtain, with  $s = 80$ ,  $\Pr[\text{WG}_a] \simeq 0.0002$  and  $P_a^{-1} \simeq 3.73$ .

Once  $\mathbf{x}$  has been retrieved with high confidence,  $\mathbf{x}'$  can be obtained by adding to the  $i$ -th challenge a vector  $\delta_i$  such that  $\delta_i \cdot \mathbf{x} = 0$  and  $\text{ROT}_i((f(\mathbf{a}_i \oplus \delta_i) \oplus f(\mathbf{a}_i)))$  is constant, which will give linear equations on  $\mathbf{x}'$ .

**Attacking  $\text{HB}^{++}$  with renewed secrets.** Let us now consider the situation where  $\text{HB}^{++}$  is operated with renewed secrets at each authentication, as recommended by the authors of [3]. We show that while secret renewal apparently protects  $\text{HB}^{++}$  against a simple application of the GRS attack, a slightly more complex attack remains.

To explain this attack, we need to introduce the function  $h$  that is used to derive the 320-bit temporary authentication key  $(\mathbf{x}, \mathbf{x}', \mathbf{y}, \mathbf{y}')$  from a permanent 768-bit secret  $\mathbf{Z}$ . This function is derived from the hash functions family WH, a variant of the hash functions family NH on which the UMAC message authentication code is based [2] and which was proposed by Kaps *et al.* in [12].

The instance of WH used to construct  $h$  is defined as follows: given two 160-bit words  $\mathbf{K} = (K_1, \dots, K_n) \in (\mathbb{F}_{2^{16}})^n$ , and  $\mathbf{M} = (M_1, \dots, M_n) \in (\mathbb{F}_{2^{16}})^n$ , where  $n = 10$ , the 16-bit word  $\text{WH}_{\mathbf{K}}(\mathbf{M})$  is defined as

$$\text{WH}_{\mathbf{K}}(\mathbf{M}) = \sum_{i=1}^{n/2} (M_{2i-1} + K_{2i-1}) \cdot (M_{2i} + K_{2i}) \cdot c_i,$$

where the  $c_i$  are  $\mathbb{F}_{2^{16}}$  constants defined in [12]. The function  $h$  results from  $t = 20$  invocations of this instance of WH, according to the construction of a hash function family with a larger key and output size named  $\text{WH}^T$  proposed in [12]. Given  $\mathbf{Z} = (Z_1, \dots, Z_{n+2(t-1)}) \in (\mathbb{F}_{2^{16}})^{n+2(t-1)} = (\mathbb{F}_{2^{16}})^{48}$ , and  $\mathbf{M} = (M_1, \dots, M_n) \in \mathbb{F}_{2^{16}}^n = (\mathbb{F}_{2^{16}})^{10}$ , the  $t$ -uple  $\text{WH}_{\mathbf{Z}}^T(\mathbf{M})$  of  $\mathbb{F}_{2^{16}}$  words is defined as  $\text{WH}_{\mathbf{Z}}^T(\mathbf{M}) = (\text{WH}_{Z_1 \dots Z_n}(\mathbf{M}), \text{WH}_{Z_3 \dots Z_{n+2}}(\mathbf{M}), \dots, \text{WH}_{Z_{2t-1} \dots Z_{n+2t-2}}(\mathbf{M}))$ . With the previous notation  $h$  is defined as  $h(\mathbf{Z}, \mathbf{A}, \mathbf{B}) = \text{WH}_{\mathbf{Z}}^T(\mathbf{M})$  where  $\mathbf{M} = (\mathbf{A} \parallel \mathbf{B})$ .

One can see from the former equations that given any fixed pair  $(\mathbf{A}, \mathbf{B})$ ,  $h(\mathbf{Z}, \mathbf{A}, \mathbf{B})$  is a known quadratic function of  $(Z_1, \dots, Z_{48})$ . However, the security advantage that results from having a quadratic expression rather than a linear one is quite marginal for this particular function. This is due to the following property that immediately results from the definition of WH: for all  $(\mathbf{A}, \mathbf{B})$  pairs, each of the  $t$  16-bit words of  $h(\mathbf{Z}, \mathbf{A}, \mathbf{B})$  can be expressed as a known affine function with  $\mathbb{F}_{2^{16}}$  coefficients of only 15 unknown words, namely 10 consecutive values of the sequence  $(Z_1, \dots, Z_{48})$  and 5 of the 24 products  $Z_1 \cdot Z_2, Z_3 \cdot Z_4, \dots, Z_{47} \cdot Z_{48}$ . Equivalently, if we consider equations over  $\mathbb{F}_2$  instead of  $\mathbb{F}_{2^{16}}$ , each bit of  $h(\mathbf{Z}, \mathbf{A}, \mathbf{B})$  can be expressed for all  $(\mathbf{A}, \mathbf{B})$  pairs as a known

affine function of only 240 unknown bits, namely 160  $\mathbf{Z}$  bits and 80 quadratic functions of  $\mathbf{Z}$  bits. We call hereafter such unknown bits *expanded key bits*.<sup>2</sup>

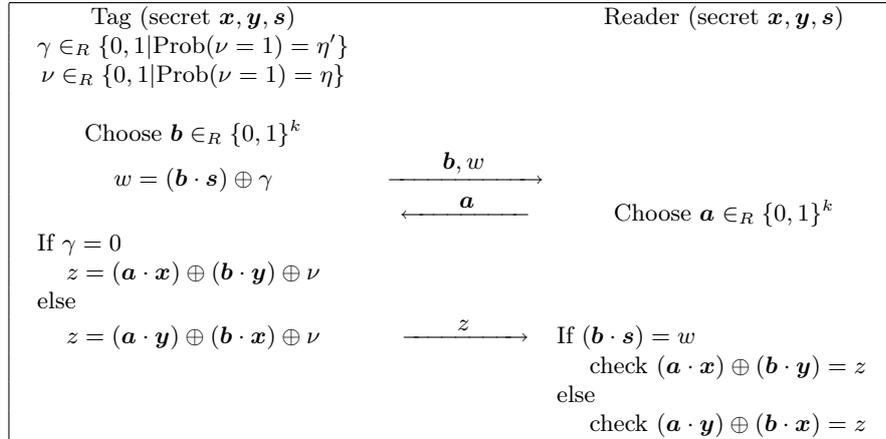
We now present the cryptanalysis of  $\text{HB}^{++}$ . We have shown in the former section that, by disturbing a subset of  $s$  rounds of an authentication and exploiting the authentication success or failure information for the disturbed protocol, an adversary is capable of getting approximate linear equations involving a subset of the bits of  $\mathbf{x}$ , say the 16 first bits of  $\mathbf{x}$  (which all linearly depends on the same 240 expanded key bits). If we collect a sufficient number  $m$  of such equations, relating to  $m$  temporary values  $\mathbf{x}$ , we get an LPN problem in 240 expanded key bits. According to the previous analysis, the error parameter for this LPN problem will typically not be more than 0.01. Leveil and Fouque [15] estimate that such instances of the LPN problem can be solved with about  $2^{30}$  noisy samples and  $2^{41}$  steps of computation and bytes of memory. Thus 240 bits of the expanded key can be recovered by solving an LPN problem of medium complexity. The same method can be applied to recover 240-bit portions of the expanded key allowing the attacker to predict the other 16-bit words of  $\mathbf{x}$ . Once this is done,  $\mathbf{x}$  can be predicted by the adversary for each authentication. This renders the derivation of  $m$  approximate linear equations on  $\mathbf{x}'$  bits even easier than the initial derivation of approximate equations on  $\mathbf{x}$  bits and therefore the parts of the expanded key that allow the attacker to compute the value of  $\mathbf{x}'$  at each authentication can now be derived.

At this stage, the adversary has enough information to impersonate the tag without having to derive the rest of the expanded key and derive  $\mathbf{y}$  and  $\mathbf{y}'$ . The adversary can re-use the masking vectors  $\mathbf{b}$  used by the tag in a successful authentication along with its knowledge of  $\mathbf{x}$  and  $\mathbf{x}'$  to correct the  $z$  and  $z'$  values in an appropriate way. All in all,  $\text{HB}^{++}$  can be cryptanalyzed by solving 10 LPN problems of size 240 bits with small noise parameters. The total number of authentications needed is multiplied by  $P_a^{-1} \simeq 4$  as only authentications where the reader accepts are used. For example, for  $(r, t, \eta) = (80, 30, 0.25)$ , the noise parameter of the LPN problem is roughly 0.01 so that the total number of authentications needed is  $4 \times 10 \times 2^{30} \simeq 2^{35}$  and the total complexity is about  $2^{44}$ . Moreover, it is possible to reduce the number of authentications needed at the expense of an increased complexity. Hence  $\text{HB}^{++}$  offers a much reduced level of security considering the complexity of the operations it requires.

## 4 The Variant $\text{HB}^*$

**Description of  $\text{HB}^*$ .** The variant  $\text{HB}^*$  is proposed by Duc and Kim [5]. Again it consists of  $r$  rounds where each round consists of three passes. This is illustrated in Figure 4. There is an additional secret  $\mathbf{s}$  which is used to secretly transmit from the tag to the reader a random bit  $\gamma$ , which is 1 with probability  $\eta' \in ]0, \frac{1}{2}]$ , and which determines whether the right answer is computed as  $(\mathbf{a} \cdot \mathbf{x}) \oplus (\mathbf{b} \cdot \mathbf{y})$  or  $(\mathbf{a} \cdot \mathbf{y}) \oplus (\mathbf{b} \cdot \mathbf{x})$ . As in  $\text{HB}^+$ , the tag is authenticated if the

<sup>2</sup> Thus the function  $h$  involves 1152 expanded key bits in overall, namely 768  $\mathbf{Z}$  bits and 384 quadratic functions of the  $\mathbf{Z}$  bits.



**Fig. 4.** One single round of HB\*. The entire authentication process requires  $r$  rounds and, in this basic form, each round consists of the three passes shown. Provided the tag fails less than some threshold  $t$  number of rounds, the tag is authenticated.

number of errors is less than some threshold  $t = ur$ , where  $u \in ]\eta, \frac{1}{2}[$ . Note that the false rejection and false acceptance probabilities  $P_{\text{FR}}$  and  $P_{\text{FA}}$  are given by the same formulas as in the case of HB+. In particular these probabilities are independent of  $\eta'$ . The on-tag computation is roughly twice that of HB+ (but less than that required in HB++) while resistance to the GRS attack is claimed. In the next section we apply the GRS attack to HB\* and show that HB\* offers no advantage over HB+.

**Attacking HB\*.** We show that HB\* remains vulnerable to an extremely close variant of the GRS attack. The first phase of the attack aims to gather information on  $\boldsymbol{\delta} \cdot \mathbf{x}$  and  $\boldsymbol{\delta} \cdot \mathbf{y}$  for independent vectors  $\boldsymbol{\delta}$ . For this, the adversary proceeds exactly as in the GRS attack and modifies the challenges sent by the reader by adding a vector  $\boldsymbol{\delta}$  to  $\mathbf{a}$ . When  $\boldsymbol{\delta} \cdot \mathbf{x} = 0$  and  $\boldsymbol{\delta} \cdot \mathbf{y} = 0$ , the protocol is undisturbed and the tag will be authenticated with high probability. In all other cases, the authentication will be less likely to succeed, so that the output of the reader gives information about  $\mathbf{x}$  and  $\mathbf{y}$ . More precisely, depending on the values of  $\boldsymbol{\delta} \cdot \mathbf{x}$  and  $\boldsymbol{\delta} \cdot \mathbf{y}$ , each round of the protocol will be successful or not with the following probabilities:

1. if  $\boldsymbol{\delta} \cdot \mathbf{x} = 0$  and  $\boldsymbol{\delta} \cdot \mathbf{y} = 0$ , then none of the  $r$  rounds of the protocol are disturbed. The response of the tag is incorrect each time  $\nu = 1$ , hence with probability  $\tau_1 = \eta$  and the reader accepts with probability  $1 - P_{\text{FR}}$  and rejects with probability  $P_{\text{FR}}$ .
2. if  $\boldsymbol{\delta} \cdot \mathbf{x} = 0$  and  $\boldsymbol{\delta} \cdot \mathbf{y} = 1$ , the response of the tag is incorrect each time ( $\gamma = 0, \nu = 1$ ) or ( $\gamma = 1, \nu = 0$ ), hence with probability

$$\tau_2 = (1 - \eta)\eta' + (1 - \eta')\eta = \eta + (1 - 2\eta)\eta' > \eta.$$

3. if  $\boldsymbol{\delta} \cdot \boldsymbol{x} = 1$  and  $\boldsymbol{\delta} \cdot \boldsymbol{y} = 0$ , the response of the tag is incorrect each time ( $\gamma = 0, \nu = 0$ ) or ( $\gamma = 1, \nu = 1$ ), hence with probability

$$\tau_3 = (1 - \eta)(1 - \eta') + \eta\eta' = \eta + (1 - 2\eta)(1 - \eta') > \eta.$$

4. if  $\boldsymbol{\delta} \cdot \boldsymbol{x} = 1$  and  $\boldsymbol{\delta} \cdot \boldsymbol{y} = 1$ , the response of the tag is incorrect each time  $\nu = 0$ , whatever  $\gamma$ , hence with probability  $\tau_4 = 1 - \eta = \eta + (1 - 2\eta) > \eta$ .

Note that  $\tau_1 < \tau_2 \leq \frac{1}{2} \leq \tau_3 < \tau_4$ . Note also that when  $\eta' \rightarrow 0$  ( $\eta' = 0$  corresponds to the classical HB<sup>+</sup> protocol),  $\tau_2 \rightarrow \tau_1$  and  $\tau_3 \rightarrow \tau_4$ , whereas when  $\eta' \rightarrow \frac{1}{2}$ ,  $\tau_2 \rightarrow \frac{1}{2}$  and  $\tau_3 \rightarrow \frac{1}{2}$ . In each of the cases 2, 3 and 4, the reader will reject with probability greater than  $P_{\text{FR}}$ , namely  $P_i^{\text{rej}} = \Pr[\mathcal{R} \text{ rejects} \mid \text{case } i] = \sum_{j=t+1}^r \binom{r}{j} \tau_i^j (1 - \tau_i^{r-j})$ .

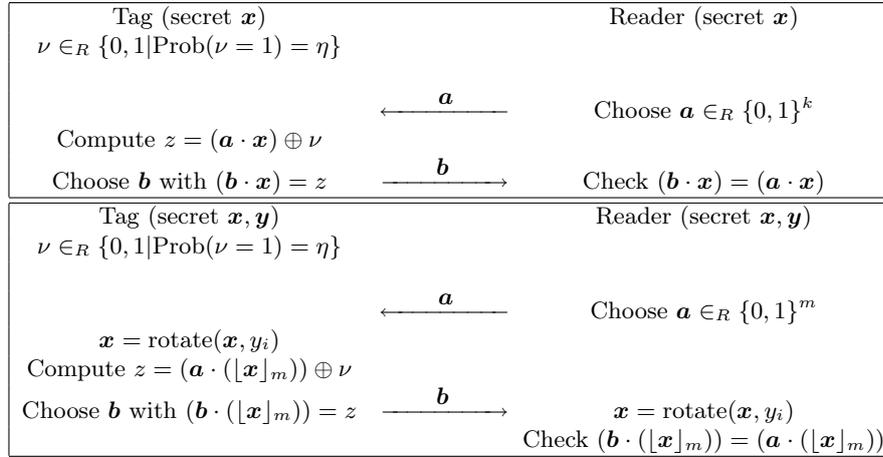
According to the Chernoff bound (see Appendix), the adversary will be able to discriminate between case  $i$  and  $j$  as soon as  $|P_i^{\text{rej}} - P_j^{\text{rej}}|$  is non-negligible. We have to distinguish two cases: either  $\tau_2 \leq u$ , or  $\tau_2 > u$ .

When  $\tau_2 \leq u$ , *i.e.*  $\eta' \leq \frac{u-\eta}{1-2\eta}$ , we are “almost” in the HB<sup>+</sup> case: the reader will accept with overwhelming probability when  $\boldsymbol{\delta} \cdot \boldsymbol{x} = 0$  and reject with overwhelming probability when  $\boldsymbol{\delta} \cdot \boldsymbol{x} = 1$ , independently of  $\boldsymbol{\delta} \cdot \boldsymbol{y}$ . The GRS attack applies as it is, meaning that the adversary can retrieve  $\boldsymbol{x}$  with high probability in linear time. Once this is done, it can impersonate a tag by sending  $(\boldsymbol{b}, \omega) = (\mathbf{0}, 0)$  as first message.

When  $\tau_2 > u$ , *i.e.*  $\eta' > \frac{u-\eta}{1-2\eta}$ , the attacker can only discriminate case 1 from cases 2, 3, and 4. Indeed the reader will accept with overwhelming probability when  $\boldsymbol{\delta} \cdot \boldsymbol{x} = 0$  and  $\boldsymbol{\delta} \cdot \boldsymbol{y} = 0$ , and reject with overwhelming probability in the three other cases. However this does not prevent a slight variant of the GRS attack as follows.

We assume that  $\boldsymbol{x}$  and  $\boldsymbol{y}$  are linearly independent. For a random  $\boldsymbol{\delta}$ , case 1 happens with probability  $\frac{1}{4}$ , so that the adversary will be able to find with  $\Theta(4k)$  attempts  $k - 2$  independent vectors  $\boldsymbol{\delta}$  such that  $\boldsymbol{\delta} \cdot \boldsymbol{x} = 0$  and  $\boldsymbol{\delta} \cdot \boldsymbol{y} = 0$ . Put a different way, he is able to learn the two-dimensional vectorial space  $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ . Let  $\boldsymbol{c}_1, \boldsymbol{c}_2$  and  $\boldsymbol{c}_3$  denote the three non-null vectors in this vectorial space. Once they are found, the adversary can directly impersonate a valid tag with probability roughly  $\frac{1}{8}$  by choosing at random two vectors among  $(\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3)$  (say  $\boldsymbol{c}_1$  and  $\boldsymbol{c}_2$ ), fixing two arbitrary values for  $(\boldsymbol{b}, \omega)$  that he will send at each round, and then answering  $(\boldsymbol{c}_1 \cdot \boldsymbol{a}) \oplus (\boldsymbol{c}_2 \cdot \boldsymbol{b})$  at each round. The adversary will be successfully authenticated when  $(\boldsymbol{b} \cdot \boldsymbol{s} = \omega, \boldsymbol{c}_1 = \boldsymbol{x}, \boldsymbol{c}_2 = \boldsymbol{y})$  or  $(\boldsymbol{b} \cdot \boldsymbol{s} \neq \omega, \boldsymbol{c}_1 = \boldsymbol{y}, \boldsymbol{c}_2 = \boldsymbol{x})$ , which happens with probability  $\frac{1}{8}$ .

Alternatively, the adversary can do a little more work and identify from the three values  $(\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3)$  the one which is equal to  $\boldsymbol{x} \oplus \boldsymbol{y}$ . For this, the attacker queries the honest tag with challenges  $\boldsymbol{a}$  systematically equal to the blinding vector  $\boldsymbol{b}$  sent by the tag. That way, the answer of the tag is always equal to  $\boldsymbol{b} \cdot (\boldsymbol{x} \oplus \boldsymbol{y}) \oplus \nu$  and the attacker deduces that  $\boldsymbol{x} \oplus \boldsymbol{y}$  is the value  $\boldsymbol{c}_i$  such that the number of  $\boldsymbol{b}$ 's such that  $\boldsymbol{b} \cdot \boldsymbol{c}_i$  is equal to the answer of the tag is maximal. Once this is done, the adversary knows the unordered set  $\{\boldsymbol{x}, \boldsymbol{y}\}$ . This is enough to impersonate the tag with probability  $\frac{1}{2}$ . Assume that the vector  $\boldsymbol{c}_3$  has been



**Fig. 5.** Round  $i$  of HB-MP' (above) and HB-MP (below). The entire authentication process requires  $r$  rounds and, in this basic form, each round consists of the two passes shown. Provided the tag fails less than some threshold  $t$  number of rounds, the tag is authenticated. For HB-MP  $\lfloor \mathbf{x} \rfloor_m$  denotes the  $m$  least significant bits of  $\mathbf{x}$  and  $y_i$  is the  $i^{\text{th}}$  bit of  $\mathbf{y}$  which is used as the argument to a bitwise rotation.

ruled out as being  $\mathbf{x} \oplus \mathbf{y}$ . The adversary randomly fixes values for  $(\mathbf{b}, \omega)$  that he will send at each round, and then answers  $(\mathbf{c}_1 \cdot \mathbf{a}) \oplus (\mathbf{c}_2 \cdot \mathbf{b})$  at each round. The adversary will be successfully authenticated when  $(\mathbf{b} \cdot \mathbf{s} = \omega, \mathbf{c}_1 = \mathbf{x}, \mathbf{c}_2 = \mathbf{y})$  or  $(\mathbf{b} \cdot \mathbf{s} \neq \omega, \mathbf{c}_1 = \mathbf{y}, \mathbf{c}_2 = \mathbf{x})$ , which happens now with probability  $\frac{1}{2}$ . Note that whatever the outcome of this first attempt, the adversary will successfully pass the following attempt with probability 1. If the first attempt succeeded he can reuse the same  $(\mathbf{b}, \omega)$  and answer  $(\mathbf{c}_1 \cdot \mathbf{a}) \oplus (\mathbf{c}_2 \cdot \mathbf{b})$  at each round. If the first attempt failed, use the same  $(\mathbf{b}, \omega)$  but answer  $(\mathbf{c}_2 \cdot \mathbf{a}) \oplus (\mathbf{c}_1 \cdot \mathbf{b})$  at each round; the answer will always be correct and the tag will be successfully impersonated.

## 5 The Variants HB-MP' and HB-MP

**Description of HB-MP' and HB-MP.** Another prominent protocol due to Munilla and Peinado is HB-MP [17]. In a departure from the HB<sup>+</sup> approach, each of the  $r$  rounds consists of only a two-pass communication between the tag and the reader. This is illustrated in Figure 5 where two variants are depicted; the first variant HB-MP' is claimed to be resistant to chosen challenges (presumably against the tag) while the second HB-MP is claimed to resist the GRS attack.

While HB-MP' and HB-MP are reasonably lightweight, we show in the next section that both are less secure than HB<sup>+</sup> since they are vulnerable to a passive attack. These are the attacks that HB<sup>+</sup> provably resists and so HB-MP' and HB-MP are not good alternatives.

**Table 1.** Error rates and transmission costs for HB<sup>+</sup> and different parameter choices.

$r$	$\eta$	$k$	False reject	False accept	Transmission cost (bits)	
			rate	rate	[ $k = 224$ ]	[ $k = 512$ ]
100	0.25	224	0.45	$3 \times 10^{-7}$	44,900	102,500
80	0.25	224	0.44	$4 \times 10^{-6}$	35,920	82,000
60	0.25	224	0.43	$6 \times 10^{-5}$	26,984	61,500
40	0.25	224	0.42	$1 \times 10^{-3}$	17,960	41,000

**Attacking HB-MP' and HB-MP.** In their paper, Munilla and Peinado claim that HB-MP is immune to passive attacks, but also active and man-in-the-middle attacks of the GRS type. However, there is a very simple passive attack which enables an adversary which simply eavesdrops the  $r$  rounds of one execution of the protocol to impersonate a valid tag with probability  $1 - P_{FR}$ .

Note that the verification done by the reader consists in checking that  $(\mathbf{a} \oplus \mathbf{b}) \cdot (\lfloor \mathbf{x} \rfloor_m) = 0$ . This equation is always verified when  $\mathbf{b} = \mathbf{a}$ , so that Munilla and Peinado recommend that the reader rejects a tag as soon as it answers  $\mathbf{a}$  in any round. However, for an adversary which has eavesdropped the  $r$  rounds of a previous execution of the protocol, it is easy to compute a vector  $\mathbf{b}$  different from  $\mathbf{a}$  and such that  $(\mathbf{a} \oplus \mathbf{b}) \cdot (\lfloor \mathbf{x} \rfloor_m) = 0$  with high probability as follows.

The adversary simply records the  $r$  pairs  $(\mathbf{a}_i, \mathbf{b}_i)$  which are exchanged between the honest tag and the honest reader. Then we know that with probability  $(1 - \eta)$ ,  $(\mathbf{a}_i \oplus \mathbf{b}_i) \cdot (\lfloor \mathbf{x} \rfloor_m) = 0$ . Hence, for any other challenge  $\mathbf{a}'_i$ , the answer  $\mathbf{b}'_i = \mathbf{a}'_i \oplus \mathbf{a}_i \oplus \mathbf{b}_i$  is different from  $\mathbf{a}'_i$  (because  $\mathbf{b}_i \neq \mathbf{a}_i$ ) and  $(\mathbf{a}'_i \oplus \mathbf{b}'_i) \cdot (\lfloor \mathbf{x} \rfloor_m) = (\mathbf{a}_i \oplus \mathbf{b}_i) \cdot (\lfloor \mathbf{x} \rfloor_m)$ . Hence the adversary is authenticated as soon as the tag was authenticated in the eavesdropped execution of the protocol. The attack works exactly in the same way against HB-MP'.

## 6 Discussion and Implications

The computational challenges posed by low-cost RFID tags have generated many cryptographic proposals which rely exclusively on the simplest (typically bitwise) operations. While some might express the view that some security is better than no security, even claims for “some security” need to be verified. Weaknesses in some of the simpler RFID protocols has already been demonstrated before, *e.g.* [4], and will undoubtedly be demonstrated in the future.

Those working in the field of RFID security are correct when claiming that one doesn't necessarily need full security for a deployment. This is why a proposal like HB<sup>+</sup> is actually rather successful: it doesn't claim to protect against all adversaries, but for adversaries with a minimum technical capability it provides a reasonable level of security. HB<sup>+</sup> does as claims and no more. The variants described in this note have attempted to do more and have, arguably, delivered less. It is difficult to do a lot with such basic operations.

This is not to say, however, that  $\text{HB}^+$  is currently ideal. While the on-tag computation is low, the GRS attack may be practically important to some (*i.e.* it might be more than certificational). Furthermore, the communication overheads for  $\text{HB}^+$  are substantial while the false acceptance and false rejection rates are not suitable for deployment. These are shown in Table 1 for the parameter  $k = 224$  and acceptance threshold  $r\eta$  proposed in  $\text{HB}^+$  [11]. Based on the work of [15] we also consider the data transmission costs when  $k = 512$  which is a more appropriate value to use if we are seeking 80-bit security.

These are unfortunate barriers for any practical deployment of  $\text{HB}^+$ . Nevertheless, the computational complexity and simplicity of  $\text{HB}^+$  are very attractive and it nicely complements other work that seeks to extend more conventional forms of cryptography [1,6,10,16]. It is therefore an interesting challenge to find the right variant of  $\text{HB}^+$  that simultaneously improves both security and efficiency: one such proposal has been named  $\text{HB}^\#$  by the authors [9].

## 7 Conclusions

In this paper we have considered variants to  $\text{HB}^+$ . While they were designed with the sole intention of resisting the GRS attack on  $\text{HB}^+$ , all of  $\text{HB}^{++}$ ,  $\text{HB}^*$ ,  $\text{HB-MP}'$ , and  $\text{HB-MP}$  are vulnerable to GRS-style attacks. In addition these variants sacrifice much of the simplicity and elegance of the original  $\text{HB}^+$ . Despite some questions on the practical implementation of  $\text{HB}^+$  and the existence of the GRS attack, the computational efficiency and theoretical foundations of  $\text{HB}^+$  are impressive. And while the work in this paper suggests that good variants to  $\text{HB}^+$  are very hard to find, the right variant might offer a particularly interesting—and successful—solution to the problem of low-cost tag authentication.

**Acknowledgements.** We would like to thank Stanislaw Jarecki for his thoughtful feedback on a previous version of this paper.

## References

1. A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In P. Paillier and I. Verbauwhede, editors, *Proceedings of CHES 2007*, Lecture Notes in Computer Science, vol. 4727, 450–466, Springer, 2007.
2. J. Black, S. Halevi, H. Krawczyk, T. Krovetz and P. Rogaway. UMAC: Fast and Secure Message Authentication. In M. J. Wiener, editor, *Proceedings of CRYPTO '99*, Lecture Notes in Computer Science, vol. 1666, 216–233, Springer, 1999.
3. J. Bringer, H. Chabanne, and E. Dottax.  $\text{HB}^{++}$ : A Lightweight Authentication Protocol Secure Against Some Attacks. In P. Georgiadis, J. Lopez, S. Gritzalis, and G. Marias, editors, *Proceedings of SecPerU 2006*, 28–33, IEEE Computer Society Press, 2006.
4. B. Defend, K. Fu, and A. Juels. Cryptanalysis of Two Lightweight RFID Authentication Schemes. In *International Workshop on Pervasive Computing and Communication Security, PerSec 2007*, 211–216, IEEE Computer Society Press, 2007.

5. D.N. Duc and K. Kim. Securing HB<sup>+</sup> Against GRS Man-in-the-Middle Attack. In *Institute of Electronics, Information and Communication Engineers, Symposium on Cryptography and Information Security*, Jan. 23–26, 2007.
6. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems Using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, *Proceedings of CHES 2004*, Lecture Notes in Computer Science, vol. 3156, 357–370, Springer, 2004.
7. M.P.C. Fossorier, M.J. Mihaljevic, H. Imai, Y. Cui, and K. Matsuura. A Novel Algorithm for Solving the LPN Problem and its Application to Security Evaluation of the HB Protocol for RFID Authentication. Available from <http://eprint.iacr.org/2006/197.pdf>.
8. H. Gilbert, M.J.B. Robshaw, and H. Sibert. An Active Attack Against HB<sup>+</sup>: A Provably Secure Lightweight Authentication Protocol. *IEE Electronics Letters*, vol. 41, number 21, 1169–1170, 2005.
9. H. Gilbert, M.J.B. Robshaw, and Y. Seurin. HB<sup>#</sup>: Increasing the Security and Efficiency of HB<sup>+</sup>. In *Proceedings of Eurocrypt 2008*, to appear. Full version available from <http://eprint.iacr.org/2008/028>
10. M. Girault, G. Poupard and J. Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. *Journal of Cryptology*, vol. 19, number 4, 463–488, 2006.
11. A. Juels and S.A. Weis. Authenticating Pervasive Devices With Human Protocols. In V. Shoup, editor, *Advances in Cryptology - Crypto 05*, Lecture Notes in Computer Science, vol. 3126, 293–198, Springer, 2005.
12. J.-P. Kaps, K. Yüksel and B. Sunar. Energy Scalable Universal Hashing. *IEEE Trans. on Computers*, vol. 54, number 12, 1484–1495, 2005.
13. J. Katz and J. Shin. Parallel and Concurrent Security of the HB and HB<sup>+</sup> Protocols. In S. Vaudenay, editor, *Advances in Cryptology - Eurocrypt 2006*, Lecture Notes in Computer Science, vol. 4004, 73–87, Springer, 2006.
14. J. Katz and A. Smith. Analysing the HB and HB<sup>+</sup> Protocols in the “Large Error” Case. Available from <http://eprint.iacr.org/2006/326.pdf>.
15. E. Leveil and P.-A. Fouque. An Improved LPN Algorithm. In R. De Prisco and M. Yung, editors, *Proceedings of SCN 2006*, Lecture Notes in Computer Science, vol. 4116, 348–359, Springer, 2006.
16. M. McLoone and M.J.B. Robshaw. Public Key Cryptography and RFID. In M. Abe, editor, *CT-RSA 2007*, Lecture Notes in Computer Science, vol. 4377, 372–384, Springer, 2007.
17. J. Munilla and A. Peinado. HB-MP: A Further Step in the HB-family of Lightweight Authentication Protocols. *Computer Networks* 51, 2262–2267, 2007.
18. S. Piramuthu. HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication. *COLLECTeR Europe Conference*, June 2006.
19. R.L. Rivest. The RC5 Encryption Algorithm. In B. Preneel, editor, *Proceedings of FSE 1994*, Lecture Notes in Computer Science, vol. 1008, 86–96, Springer, 1995.

## A Chernoff Bounds

We recall here the classical Chernoff bounds. Let  $X_1, \dots, X_n$  be independent Poisson trials such that  $\Pr[X_i = 1] = p_i$ . Let  $X = \sum_{i=1}^n X_i$  and  $\mu$  be the expected value of  $X$ . Then for any  $t < \mu$  and  $t' > \mu$ ,

$$\Pr[X \leq t] \leq e^{-\frac{(\mu-t)^2}{2\mu}} \quad \text{and} \quad \Pr[X \geq t'] \leq e^{-\frac{(t'-\mu)^2}{3\mu}}.$$