HB^{++}: a Lightweight Authentication Protocol Secure against Some Attacks

Julien Bringer, Hervé Chabanne, Emmanuelle Dottax
SAGEM Défense Sécurité

Abstract

At Crypto'05, Juels and Weis introduce HB$^+$, an enhancement of the Hopper and Blum (HB) authentication protocol. This protocol HB$^+$ is proven secure against active attacks, though preserving HB's advantages: mainly, requiring so few resources to run that it can be implemented on an RFID tag. However, in a wider adversarial model, Gilbert, Robshaw and Sibert exhibit a very effective attack against HB$^+$.

We here show how a simple modification of the HB$^+$ protocol thwarts Gilbert et al's attack. The resulting protocol, HB^{++}, remains a good candidate for RFID tags authentication.

Keywords. HB$^+$ protocol, active attacks, RFID.

1 Introduction

The problems of security and privacy for Radio Frequency Identification (RFID) have recently attracted many technical research.

RFID systems are made of three components: some tags, a reader, and a database which contains information on the tagged objects. Tags (transponders) follow the ISO and EPC [8] standards and communicate with the reader (transceiver) over the air. One main constraint here is that these tags have to be quite inexpensive (the order of magnitude is US cents) and thus they can embed only scarce resources, of which only some part is dedicated to security. Typically, computations are hardwired and some thousands of logic gates are kept for cryptography. This means that tags seem, at first glance, difficult targets for the implementation of classical cryptographic schemes, even if Feldhofer, Dominikus and Wolkerstorfer [9] have described an implementation of the AES algorithm which looks promising. Anyway, the introduction of new cryptographic schemes, requiring less resources, is today tempting.

In the typical setting, each tag comes with a unique identifier and an adversary should not be able to counterfeit tag responses. Many authentication protocols for RFID tags have been proposed so far (see e.g. in 2003 [18, 23], [12, 13, 16, 22] in 2004, [1, 3, 7, 20] in 2005, see also Juels [17] for a general survey and [2] for fresh references). Notably, at Crypto'05, HB^+, a lightweight cryptographic authentication scheme very well suited for low-cost hardware implementation, was introduced by Juels and Weis [19]. It provides a symmetric-key protocol allowing tags to identify themselves on the reader (the reader does not need to know a priori which tags and secrets are involved for the protocol to work). HB^+ is presented as an improvement of the HB protocol, which had been introduced in [14]. The security of the HB protocol does not rely on classical symmetric key cryptography solutions, but rather on the hardness of the computational Learning Parity with Noise (LPN) problem [4, 5, 15]. While the HB protocol is made to be secure against passive attacks only, the aim of HB^+ is to be resistant to active attacks. A proof of security is provided but at the same time, Gilbert, Robshaw and Sibert [10] describe a man-in-the-middle attack on HB^+ not covered by the corresponding security model.

The principal contribution of our work is to improve the HB^+ protocol in order to avoid the attack of [10], while keeping its design principles and, thus, its advantages. We call HB^{++} our new protocol. In fact, HB^{++} can be seen as running HB^+ twice under independent secrets but with correlated challenges. A function shared by all the tags and readers is introduced to link together challenges of the protocol. At the end, the HB^{++} protocol seems to us a good susbtitute for HB^+ for RFID tags authentication.

The paper is organised as follows. In Sect. 2, we recall the HB^+ protocol. In Sect. 3, we summarize Gilbert et al's attack of the HB^+ protocol [10]. In Sect. 4, we introduce our protocol HB^{++}. We here show that it is at least as secure as the HB^+ protocol and even resists some kind of generalizations of the active attack [10]. Section 5 concludes.

2 The HB^+ protocol

A brief description of one round of the HB^+ protocol is given by Fig. 1 where $a.x$ stands for the scalar product of the binary vectors a and x, and $\oplus$ is the exclusive or.

The two k-bit vectors x and y are secret keys shared by the tag and the reader. Note that an extra noise is added to the response $a.x \oplus b.y$ by the tag, this error bit ν equals 1 with probability η.

Tag (x, y)		**Reader**
$\nu \in \{0, 1 \| \mathbb{P}(\nu = 1) = \eta\}$		
Random blinding vector $b \in_R \{0,1\}^k$	$\xrightarrow{\quad b \quad}$	
	$\xleftarrow{\quad a \quad}$	Random challenge $a \in_R \{0,1\}^k$
Compute $z = a.x \oplus b.y \oplus \nu$	$\xrightarrow{\quad z \quad}$	Check $a.x \oplus b.y \approx_\eta z$

Figure 1: One round of HB$^+$

The HB$^+$ round described by Fig. 1 is repeated r times and the tag is successfully authenticated if the check fails at most ηr times (this is what is denoted by $\approx_\eta$ in Fig. 1 and in the following).

Remark 1 *The principal difference between the* HB$^+$ *and* HB *protocols is the introduction of y and b in the* HB$^+$ *protocol in order to avoid active attacks.*

In [19], the authors define a security model, and then show how to reduce an attack of HB to an attack of HB$^+$.

The security of the HB protocol is based on the Learning Parity with Noise (LPN) problem. Juels and Weis extend this result in their security model to HB$^+$ and explain how an attack of HB$^+$ can be used to solve an instance of the LPN problem (see Sec. 4.3 for an extension to HB^{++}).

Unfortunately, they do not take into account the extra information given by the result (positive or negative) of the protocol and this is exploited during the attack [10] (see Sec. 3).

3 A man-in-the-middle attack against HB$^+$

In [10], an attack is described against the HB$^+$ protocol. It is a linear-time man-in-the-middle attack where an adversary located between the reader and the tag is able to modify the challenge at every round. The adversary chooses a vector δ in $\{0,1\}^k$ and when a challenge a is sent by the reader, he intercepts the challenge and makes a switch to $a + \delta$ (see Fig. 2). Hence, at the end of the round, the reader will receive $z = (a + \delta).x \oplus b.y \oplus \nu$ from the tag.

This is repeated along all the rounds in order to deduce information from the success or failure of the authentication. Indeed, if the authentication succeeds (resp. fails), we have $\delta.x = 0$ (resp. $\delta.x = 1$) with a high probability. So one can recover x "bit after bit" by varying δ progressively.

Tag (x, y)		**Reader**
$\nu \in \{0, 1 \vert \mathbb{P}(\nu = 1) = \eta\}$		
Blinding vector $b \in_R \{0,1\}^k$	$\xrightarrow{\;b\;}$	
	$\xleftarrow{a' = a+\delta} \cdots \xleftarrow{\;a\;}$	Random challenge $a \in_R \{0,1\}^k$
Compute $z = a'.x \oplus b.y \oplus \nu$	$\xrightarrow{\;z\;}$	Check $a.x \oplus b.y \approx_\eta z$

Figure 2: An effective attack against HB^+

Remark 2 *This attack holds to recover y too, as an adversary can send $b + \delta$ instead of b to the reader.*

4 Proposed solution

4.1 Description of HB^{++}

The protocol HB^{++} needs two new secrets x', y', and f a permutation of the set $\{0,1\}^k$ as described in the following. This protocol simply consists in computing corresponding responses to given challenges (a, b), $(f(a), f(b))$ and for the tag to send these responses together with independent errors ν and ν', i.e. $z = a.x \oplus b.y \oplus \nu$ and $z' = f(a).x' \oplus f(b).y' \oplus \nu'$ (see Fig. 3).

Tag (x, y, x', y')		**Reader**
$\nu, \nu' \in \{0, 1 \vert \mathbb{P}(\nu = 1) = \eta\}$		
Blinding vector $b \in_R \{0,1\}^k$	$\xrightarrow{\;b\;}$	
	$\xleftarrow{\;a\;}$	Random challenge $a \in_R \{0,1\}^k$
$\begin{cases} z = a.x \oplus b.y \oplus \nu \\ z' = f(a).x' \oplus f(b).y' \oplus \nu' \end{cases}$	$\xrightarrow{(z,z')}$	$\begin{cases} \text{Check } a.x \oplus b.y \approx_\eta z \\ \text{Check } f(a).x' \oplus f(b).y' \approx_\eta z' \end{cases}$

Figure 3: One round of HB^{++}

4.2 Choice of f

We primarily choose f in order to thwart the attack presented in [10] but f has also to be taken with a low complexity and must not desequilibrate the distribution of scalar products.

As f is taken as a bijection, the last point is always true, the distribution of values does not change:

$$\forall x \in \{0,1\}^k,\ \mathbb{P}(c \in \{c|f(c).x = 0\}) = \mathbb{P}(c \in \{c|c.x = 0\}).$$

Henceforth, we focus on the first point. In order to avoid the attack [10], f is chosen such that Δ_f is small with:

$$\Delta_f = \max_{\delta \neq 0, \gamma} |\{a \in \{0,1\}^k | f(a+\delta) + f(a) = \gamma\}|.$$

In fact, this comes to force f to respect only a small number of linear relations, such that ultimately no linear relation holds for all the rounds.

Definition 1 *Let $f : \mathbb{F}_2^k \to \mathbb{F}_2^k$ be a vectorial boolean function, for $u \neq 0, v \in \mathbb{F}_2^k$, let*

$$\delta_f(u,v) = \left|\{a \in \{0,1\}^k | f(a+u) + f(a) = v\}\right|.$$

Remark 3 *This $\delta_f(u,v)$ has been introduced in [6] to measure the resistance of an S-box against differential cryptanalysis. We have*

$$\Delta_f = \max_{u \neq 0, v} \delta_f(u,v).$$

And for instance, the lower the value Δ_f will be, the more resistant against differential cryptanalysis the function f will be.

Proposition 1 ([21]) *Let $f : \mathbb{F}_2^k \to \mathbb{F}_2^k$, then $\Delta_f \geq 2$. In case of equality, f is said to be* Almost Perfect Nonlinear (APN).

Proposition 2 ([11]) *Let $s = 2^j + 1$, known as a Gold exponent, with* $\gcd(k,j) = 1$. *If k is odd, the power function F defined as $F : x \mapsto x^s$ over $\mathbb{F}_{2^k}$ is a permutation and APN.*

Let $(\alpha_1, \ldots, \alpha_k)$ be a basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$, and $\varphi : (x_i)_{i=1..k} \in \mathbb{F}_2^k \mapsto \sum_i x_i \alpha_i$ the associated isomorphism. Let $s = 2^j + 1$ be a Gold exponent, F the corresponding power function over $\mathbb{F}_{2^k}$ and $f = \varphi^{-1} \circ F \circ \varphi : \mathbb{F}_2^k \to \mathbb{F}_2^k$. Hence f is a permutation and APN, that is $\Delta_f = 2$. Moreover, it is easy to see that f is a quadratic function. But, even if it is quadratic, f has a large complexity in terms of elementary operations, for a large k.

A way to reduce the complexity is to use a composition of functions defined over subspaces of $\mathbb{F}_2^k$. In particular, in the following case, the value Δ_f is easy to compute.

Proposition 3 *Let* $k = k_1 + k_2$*,* $f : \mathbb{F}_2^k \to \mathbb{F}_2^k$ *defined for* $a = (a_1, a_2) \in \mathbb{F}_2^{k_1} \times \mathbb{F}_2^{k_2}$ *by* $f(a) = (f_1(a_1), f_2(a_2))$ *with* $f_i : \mathbb{F}_2^{k_i} \to \mathbb{F}_2^{k_i}$*. We have*

$$\Delta_f = \max(\Delta_{f_1}\Delta_{f_2}, \Delta_{f_1}2^{k_2}, \Delta_{f_2}2^{k_1}).$$

For example, we can use this construction with a "good" function $g : \mathbb{F}_2^{k_1} \to \mathbb{F}_2^{k_1}$ with low complexity (e.g. a Gold power function over a small field) and define $f : \mathbb{F}_2^k \to \mathbb{F}_2^k$ as $f(a_1, \dots, a_j) = (g(a_1), \dots, g(a_j))$ where $k = jk_1$. For well-chosen parameters, this function f satisfies all the conditions to design the HB^{++} protocol: f is a permutation, has a low complexity and $\Delta_f = \Delta_g \times 2^{(j-1)k_1}$ is small compared to 2^k.

An example of construction is given for realistic parameters in Appendix A.

Remark 4 *As shown in Appendix B,* $\Delta_{f^{-1}} = \Delta_f$*. When* Δ_f *is small, the attack can not be extended to* f^{-1}*.*

4.3 HB^{++} Security

4.3.1 Protection against a generalization of Gilbert et al's attack

One can try to extend the attack [10] by corrupting (a, b) with $G(a, b) = (g_1(a, b), g_2(a, b))$, where $G \neq Id$, and sending $g_2(a, b)$ to the reader and $g_1(a, b)$ to the tag such that the reader will check if

$$\left\{ \begin{array}{lcl} g_1(a,b).x \oplus b.y \oplus \nu & \approx_\eta & a.x \oplus g_2(a,b).y \\ f(g_1(a,b)).x' \oplus f(b).y' \oplus \nu' & \approx_\eta & f(a).x' \oplus f(g_2(a,b)).y' \end{array} \right.$$

i.e if

$$\left\{ \begin{array}{lcl} (g_1(a,b) + a, b + g_2(a,b)).(x,y) \oplus \nu & \approx_\eta & 0 \\ (f(g_1(a,b)) + f(a), f(b) + f(g_2(a,b))).(x',y') \oplus \nu' & \approx_\eta & 0 \end{array} \right. \tag{1}$$

Fortunately, an adversary does not know the result of this comparison but only the result of the authentication which depends on the results of all the r rounds of the protocol. So, if one wants to obtain some information on the secrets via this method, (1) has to be independent of a and b. We suppose also that an adversary has not any knowledge of x, y, x' and y' and so they have to be considered as random vectors. In consequence, to achieve an attack, $\delta_1^{(x,y)}, \delta_2^{(x,y)}, \lambda_1^{(x',y')}$ and $\lambda_2^{(x',y')}$ have to be chosen such that the following equalities stand for all the r rounds:

$$\begin{cases} g_1(a,b) & = & a + \delta_1^{(x,y)} \\ g_2(a,b) & = & b + \delta_2^{(x,y)} \\ f(g_1(a,b)) & = & f(a) + \lambda_1^{(x',y')} \\ f(g_2(a,b)) & = & f(b) + \lambda_2^{(x',y')} \end{cases}$$

If $\{(a_i, b_i)\}_{i=1..r}$ is the set of all the values used during the r rounds, those equalities induce two linear relations involving f: $\forall i \in \{1, \ldots, r\}$,

$$f(a_i + \delta_1^{(x,y)}) + f(a_i) = \lambda_1^{(x',y')},$$
$$f(b_i + \delta_2^{(x,y)}) + f(b_i) = \lambda_2^{(x',y')}.$$

As $\Delta_f = \max_{\delta \neq 0, \gamma} \left| \{a \in \{0,1\}^k | f(a+\delta) + f(a) = \gamma\} \right|$ is small, this relations are verified during all the rounds only with a small probability. So it is possible to deduce something on the secrets from the success or failure of the authentication only with a small probability $\mathbb{P}$, which verifies:

$$\mathbb{P} \leq \left(\frac{\Delta_f}{2^k} \right)^r.$$

Consequently, the smaller Δ_f is, the smaller $\mathbb{P}$ is, and whenever $\left(\frac{\Delta_f}{2^k}\right)^r$ is negligible, we have the following result:

Proposition 4 *The* HB^{++} *protocol is secure against generalizations of the active attack described in [10].*

4.3.2 Security reduction to HB$^+$ in the active adversarial model of [19]

Proposition 5 *An adversary who has the capability of breaking a random sequence of challenges of* HB^{++} *can successfully attack* HB$^+$*.*

Proof. Indeed, if an adversary $\mathcal{A}$ obtains a sequence of challenges $\mathcal{S} = \{a_i.x \oplus b_i.y \oplus \nu_i\}_{i \in I}$ from successive rounds of the HB$^+$ protocol between a tag $\mathcal{T}_{x,y}$ and a reader $\mathcal{R}$, then, by randomly picking x', y' and a variable ν' such that $\mathbb{P}(\nu' = 1) = \eta$, he can simulate a sequence of challenges $\{(a_i.x \oplus b_i.y \oplus \nu_i, f(a_i).x' \oplus f(b_i).y' \oplus \nu'_i)\}_{i \in I}$ of successive rounds of the HB^{++} protocol between $\mathcal{R}$ and a tag $\mathcal{T}_{x,y,x',y'}$. Thus his ability to cryptanalyse the HB^{++} protocol allows $\mathcal{A}$ to recover the value of x, y, x' and y' given a sufficiently large number of challenges, and so to gain the knowledge of the secrets of the original tag $\mathcal{T}_{x,y}$. □

If $\mathcal{A}$ needs to use an active attack for this last point, the only constraint is to obtain the sequence $\mathcal{S}$ of challenges by applying the same modification on a and b during the rounds of HB$^+$ as if he was trying the attack on HB^{++}.

Hence the model of active security standing for the HB$^+$ protocol in [19] can be translated to HB^{++}.

4.3.3 Security reduction to the LPN problem in the passive adversarial model

The reduction to the Learning Parity with Noise problem, which ensures the security of HB and HB$^+$ against a passive attack, is always true for the HB^{++} protocol.

Let wt_H stand for the hamming weight.

Definition 2 (LPN problem) *Let A be a random $q \times k$ binary matrix, let X be a random k-bit vector, let η be a constant noise parameter, and let $\vec{\nu}$ be a random q-bit vector such that* $\mathrm{wt}_H(\vec{\nu}) \leq \eta q$.

Given A, η, and $\vec{z} = AX \oplus \vec{\nu}$, find a k-bit vector X' such that $\mathrm{wt}_H(AX' \oplus \vec{z}) \leq \eta q$.

Proposition 6 *If a "passive" attacker has the capacity of breaking* HB^{++} *with 4 secrets of size k, he can also solve a random instance of the LPN problem of size $2k$.*

Proof. The attacker $\mathcal{A}$ can recover the secrets given a sufficiently large sequence.

Let A a random $q \times 2k$ binary matrix, X a random $2k$-bit vector, $\vec{\nu}$ a random q-bit vector such that $\mathrm{wt}_H(\vec{\nu}) \leq \eta q$ and $\vec{z} = AX \oplus \vec{\nu}$. $\mathcal{A}$ can construct the k-bit vectors x, y, a_i, b_i for $i \in \{1, \ldots, q\}$ such that:

$$X = \begin{pmatrix} x \\ y \end{pmatrix}$$

and

$$A = \begin{pmatrix} a_1 & b_1 \\ \vdots & \vdots \\ a_i & b_i \\ \vdots & \vdots \\ a_q & b_q \end{pmatrix}$$

The attacker $\mathcal{A}$ can interpret $\vec{z} = (a_i.x \oplus b_i.y \oplus \nu_i)_{i=1\ldots q}$ as challenges of the HB$^+$ protocol. As in the HB^{++} protocol the errors ν_i are independant of the errors ν'_i, by taking random vectors $x', y', \vec{\nu'}$ and by computing $\vec{z'} = (f(a_i).x' \oplus f(b_i).y' \oplus \nu'_i)_{i=1\ldots q}$, then $(\vec{z}, \vec{z'})$ can be viewed as challenges of the HB^{++} protocol which allows $\mathcal{A}$ to recover $X = \begin{pmatrix} x \\ y \end{pmatrix}$. $\square$

5 Conclusion

The main contribution of this paper is to present HB^{++}, a new identification protocol which can be used as a replacement of HB$^+$ for low-cost pervasive computing devices. At the price of making twice more computations than in HB$^+$, it allows to achieve security in a stronger adversarial model than HB$^+$ as it is resistant to the attack [10] and at least as secure as HB$^+$ in its adversarial model. This point was left as "an essential line for future work" in [19]. In fact, with HB^{++}, we switch from the "detection security model" to a more classical one (i.e. a "prevention-based" model).

The way we improve HB$^+$, i.e. forcing challenges to a specific form, is, to the best of our knowledge, new.

Its security reduction, against any man-in-the-middle attack, to a hard problem is left as an open question.

Acknowledgments. The authors thank Jonathan Katz for his comments on a preliminar version of this paper.

References

[1] G. Ateniese, J. Camenisch, and B. de Medeiros. Untraceable RFID tags via insubvertible encryption. In *Conference on Computer and Communications Security – CCS'05*. ACM Press, 2005.

[2] G. Avoine. `http://lasecwww.epfl.ch/~gavoine/rfid/`.

[3] G. Avoine and P. Oechslin. A scalable and provably secure hash based RFID protocol. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 110–114. IEEE Computer Society Press, 2005.

[4] A. Blum, M. L. Furst, M. J. Kearns, and R. J. Lipton. Cryptographic primitives based on hard learning problems. In *Advances in Cryptology*

– *CRYPTO'93*, Lecture Notes in Computer Science, pages 278–291. Springer-Verlag, 1993.

[5] A. Blum, A. Kalai, and H. Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. In *STOC 2000*, pages 435–440, 2000.

[6] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In A. D. Santis, editor, *Advances in Cryptology – EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 356–365. Springer-Verlag, 1994.

[7] S. Dominikus, E. Oswald, and M. Feldhofer. Symmetric authentication for RFID systems in practice. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[8] EPC. Electronic product code global inc. `http://www.epcglobalinc.org/`.

[9] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In M. Joye and J.-J. Quisquater, editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370, Boston, Massachusetts, USA, August 2004. IACR, Springer-Verlag.

[10] H. Gilbert, M. Robshaw, and H. Sibert. An active attack against HB^+ - a provably secure lightweight authentication protocol. Cryptology ePrint Archive, Report 2005/237, 2005. `http://eprint.iacr.org/`.

[11] R. Gold. Maximal recursive sequences with 3-valued crosscorrelation functions. *IEEE Trans. on Inform. Theory*, 14:154–156, 1968.

[12] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. In T. Okamoto, editor, *The Cryptographers' Track at the RSA Conference – CT-RSA*, volume 2964 of *Lecture Notes in Computer Science*, pages 163–178. Springer-Verlag, 2004.

[13] D. Henrici and P. Müller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In R. Sandhu and R. Thomas, editors, *International Workshop on Pervasive Computing and Communication Security – PerSec 2004*, pages 149–153. IEEE Computer Society, 2004.

[14] N. J. Hopper and M. Blum. Secure human identification protocols. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 52–66. Springer-Verlag, 2001.

[15] J. Håstad. Some optimal inapproximability results. In *STOC 1997*, pages 1–10, 1997.

[16] A. Juels. “yoking-proofs” for RFID tags. In R. Sandhu and R. Thomas, editors, *International Workshop on Pervasive Computing and Communication Security – PerSec 2004*, pages 138–143. IEEE Computer Society, 2004.

[17] A. Juels. RFID security and privacy: A research survey. To appear in the *IEEE Journal on Selected Areas in Communication*, 2006.

[18] A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In V. Atluri, editor, *Conference on Computer and Communications Security – ACM CCS*, pages 103–111. ACM Press, 2003.

[19] A. Juels and S. Weis. Authenticating pervasive devices with human protocols. In V. Shoup, editor, *Advances in Cryptology – CRYPTO’05*, volume 3126 of *Lecture Notes in Computer Science*, pages 293–308. Springer-Verlag, 2005.

[20] D. Molnar, A. Soppera, and D. Wagner. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In B. Preneel and S. Tavares, editors, *Selected Areas in Cryptography – SAC 2005*, Lecture Notes in Computer Science. Springer-Verlag, 2005.

[21] K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. In E. F. Brickell, editor, *Advances in Cryptology – CRYPTO’92*, volume 740 of *Lecture Notes in Computer Science*, pages 566–574. Springer-Verlag, 1992.

[22] J. Saito, J.-C. Ryou, and K. Sakurai. Enhancing privacy of universal re-encryption scheme for RFID tags. In L. Jang, M. Guo, G. Gao, and N. Jha, editors, *Embedded and Ubiquitous Computing – EUC 2004*, volume 3207 of *Lecture Notes in Computer Science*, pages 879–890. Springer-Verlag, 2004.

[23] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In D. Hutter, G. Müller, W. Stephan, and M. Ullmann, editors, *International Conference on Security in Pervasive Computing – SPC 2003*, volume 2802 of *Lecture Notes in Computer Science*, pages 454–469. Springer-Verlag, 2003.

A An example of construction of f

Let $k = 225$. This corresponds to the actual key length of HB, HB^+ and HB^{++}; as for $k \geq 224$, the best known algorithm to solve the relying LPN problem has a computational runtime greater than 2^{80} [19].

Let $k_1 = 5$, $j = 45$ and $(\alpha_1, \ldots, \alpha_{k_1})$ be a basis of $\mathbb{F}_{2^{k_1}}$ over $\mathbb{F}_2$, and $\varphi : \mathbb{F}_2^{k_1} \to \mathbb{F}_{2^{k_1}}, (x_i)_{i=1..k_1} \mapsto \sum_i x_i\alpha_i$ the associated isomorphism.

We construct $f : \mathbb{F}_2^k \to \mathbb{F}_2^k$ thanks to the power function

$$g : \begin{array}{ccc} \mathbb{F}_{2^{k_1}} & \to & \mathbb{F}_{2^{k_1}} \\ x & \mapsto & x^3 \end{array}$$

by

$$f(a_1, \ldots, a_j) = (\tilde{g}(a_1), \ldots, \tilde{g}(a_j)),$$

for $a = (a_1, \ldots, a_j) \in (\mathbb{F}_2^{k_1})^j$ and $\tilde{g}(x) = \varphi^{-1} \circ g \circ \varphi(x)$.

As explained in Sect. 4.2, g is a permutation and $\Delta_g = 2$ ($s = 3$ is a Gold exponent, so g is an APN function). Hence, f is a permutation and

$$\Delta_f = 2^{(j-1)k_1+1} = 2^{k-4}.$$

Thus, the probability for an active attack, like the one described in [10], to succeed is lower than $(2^{-4})^r$. For $r \geq 20$, the probability of success is smaller than 2^{-80}.

One remaining constraint has to be checked: f must have a low complexity.

We set the representation of the field $\mathbb{F}_{2^{k_1}}$ as $\mathbb{F}_{2^{k_1}} = \mathbb{F}_2[X]/(P)$ where $P = X^5 + X^2 + 1$ is an irreducible polynomial over $\mathbb{F}_2$. For α a root of P in $\mathbb{F}_{2^{k_1}}$, let $(\alpha_1, \ldots, \alpha_{k_1}) = (1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ be the canonical basis of $\mathbb{F}_{2^{k_1}}$. For this basis, a description of $\tilde{g} : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ is given below.

$$\begin{aligned}
\tilde{g} : (x_0, x_1, x_2, x_3, x_4) \longmapsto (&x_0 \oplus x_1x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_0x_4, \\
&x_0x_1 \oplus x_2 \oplus x_0x_3 \oplus x_3 \oplus x_3x_4 \oplus x_4, \\
&x_0x_2 \oplus x_0x_1 \oplus x_1x_2 \oplus x_2x_4 \oplus x_0x_4 \oplus x_3x_4 \oplus x_4, \\
&x_1 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_3 \oplus x_0x_4 \oplus x_4, \\
&x_0x_4 \oplus x_1x_2 \oplus x_0x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_3 \oplus x_3x_4 \oplus x_1x_4 \oplus x_2x_4)
\end{aligned}$$

The computation of $\tilde{g}$ requires the evaluation of 10 AND and 29 XOR.

Remark 5 *It is even possible to construct a function f with a smaller complexity, by taking $k_1 = 3$. The corresponding power function $\tilde{g}$ defined over $\mathbb{F}_8$ would take only 3 AND and 7 XOR. The induced probability for an active attack to succeed would still be lower than $(2^{-2})^r$.*

B Case of f^{-1}

When f is chosen to thwart the attack, as described previously, the resistance of f^{-1} is the same, i.e.

$$\Delta_f = \Delta_{f^{-1}}.$$

Indeed, for $u, v \in \mathbb{F}_2^k$, as f is a permutation of $\mathbb{F}_2^k$, we have the following equalities

$$\begin{aligned}
\{a \in \mathbb{F}_2^k | f(a+u)+f(a)=v\} &= \{b \in \mathbb{F}_2^k | f(f^{-1}(b)+u)+f(f^{-1}(b))=v\} \\
&= \{b \in \mathbb{F}_2^k | f(f^{-1}(b)+u)+b=v\} \\
&= \{b \in \mathbb{F}_2^k | f(f^{-1}(b)+u)=b+v\} \\
&= \{b \in \mathbb{F}_2^k | f^{-1}(f(f^{-1}(b)+u))=f^{-1}(b+v)\} \\
&= \{b \in \mathbb{F}_2^k | f^{-1}(b)+u=f^{-1}(b+v)\} \\
&= \{b \in \mathbb{F}_2^k | f^{-1}(b+v)+f^{-1}(b)=u\}.
\end{aligned}$$

Hence $\delta_f(u,v) = |\{a \in \mathbb{F}_2^k | f(a+u)+f(a)=v\}| = \delta_{f^{-1}}(v,u)$, $\forall u, v \in F_2^k$. Moreover, note that $\delta_f(0,v) = |\{a \in \mathbb{F}_2^k | f(a)+f(a)=v\}| = 0$ if $v \neq 0$, so

$$\begin{aligned}
\Delta_f &= \max_{u \neq 0, v} \delta_f(u,v) \\
&= \max_{(u,v) \neq (0,0)} \delta_f(u,v).
\end{aligned}$$

The same holds for f^{-1}. Then,

$$\Delta_f = \max_{(u,v)\neq(0,0)} \delta_f(u,v) = \max_{(u,v)\neq(0,0)} \delta_{f^{-1}}(v,u) = \Delta_{f^{-1}}.$$