Int. J. Inf. Secur. (2013) 12:151–154
DOI 10.1007/s10207-012-0188-z

REGULAR CONTRIBUTION

On the security of AUTH, a provably secure authentication protocol based on the subspace LPN problem

Panagiotis Rizomiliotis · Stefanos Gritzalis

Published online: 30 December 2012

Abstract At the 2011 Eurocrypt, Kiltz et al., in their best paper price awarded paper, proposed an ultra-lightweight authentication protocol, called $AUTH$. While the new protocol is supported by a delicate security proof based on the conjectured hardness of the learning parity with noise problem, this security proof does not include man-in-the-middle attacks. In this paper, we show that $AUTH$ is weak against MIM adversaries by introducing a very efficient key recovery MIM attack that has only linear complexity with respect to the length of the secret key.

Keywords Authentication protocol · Key recovery attack · RFID · LPN problem

1 Introduction

Low-cost radio frequency identification (RFID) technology uses radio frequency signals for the communication, through a reader, between an electronic tag, called RFID tag, attached to a physical object, and a back-end system that stores information related to this object. RFID tags is expected to be the most pervasive device in history and constitutes a fundamental part of what is known as the Internet of Things (IoT). In the IoT vision, the Internet extends into our everyday lives through a wireless network of uniquely identifiable objects or "things." Using RFID tags, each object is related to both current and historical information on that object's physical properties, origin, ownership.

Applications like supply-chain management, smart-home devices and tele-medicine are already taking advantage of the RFID technology. However, this rapid proliferation of RFID tags raises several security and privacy concerns. Together, in order to sustain the cost of the tag as low as possible, the resources that are available for security purposes are very limited. Thus, it was identified early on that new lightweight cryptographic protocols have to be designed, and several new schemes have been proposed in the last few years [1].

Authentication has been recognized as one of the most important cryptographic tasks, and the design of lightweight protocols supported by a security proof has gained a lot of attention by the cryptographic research community. In the context of RFID technology, the most promising proposals are based on the hardness of the so-called learning parity with noise (LPN) problem.

Definition 1 (*LPN Problem*) Let $\boldsymbol{A}$ be a random $(q \times k)$-binary matrix, let $\boldsymbol{x}$ be a random k-bit vector, let $\eta \in (0, 1/2)$ be a noise parameter, and let $\boldsymbol{v}$ be a random q-bit vector such that $wt(\boldsymbol{v}) \leq \eta q$. Given $\boldsymbol{A}$, η, and $\boldsymbol{z} = \boldsymbol{A} \cdot \boldsymbol{x}^t + \boldsymbol{v}^t$, find a k-bit vector $\boldsymbol{y}^t$ such that $wt(A \cdot \boldsymbol{y}^t + \boldsymbol{z}) \leq \eta q$.

Starting with the *HB* protocol [7], a work of Hopper and Blum, and mainly its extension HB^+ [8], several LPN-based authentication protocols have been proposed. HB^* [4], $HB^\#$ [6], HB^{++} [2], *HB-MAC* [15], modified-HB^{++} [14], *Trusted-HB* [3], *HB-MP* [11], *HB-MP*$^+$ [10], *HB-MP*$^{++}$ [16] are only a few of them. All these protocols are symmetric, that is, the tag and the back-end system share a common secret key, and most of them are ultra-lightweight performing just a few dot product and bit exclusive or computations between the secret key and randomly selected and publicly known binary vectors.

Among the LPN-based authentication protocols, the most interesting ones are those that are supported by a security proof, that is, a concrete reduction in the LPN problem to the security of the corresponding protocol. Three attack models

P. Rizomiliotis (✉)· S. Gritzalis
Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Karlovassi, Samos, Greece
e-mail: prizomil@aegean.gr

Fig. 1 The *AUTH* protocol

Tag $(\mathbf{x})$		**Reader** $(\mathbf{x})$
if $wt(\boldsymbol{a}) \neq l$, abort	$\xleftarrow{\boldsymbol{a}}$	$\boldsymbol{a} \in_R \mathbb{F}_2^{2l}$, $wt(\boldsymbol{a}) = l$
$\boldsymbol{R} \in_R \mathbb{F}_2^{l \times n}$; $\boldsymbol{\nu} \in_R Ber(n, \eta)$ $\boldsymbol{z} = \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \boldsymbol{a}} \oplus \boldsymbol{\nu}$	$\xrightarrow{\boldsymbol{z}, \boldsymbol{R}}$	If $rank(\boldsymbol{R}) \neq n$, reject If $wt(\boldsymbol{z} \oplus \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \boldsymbol{a}}) \leq \tau$, accept

have been mainly considered, namely passive, active, and man-in-the-middle (MIM) attacks. In the first model, the attacker can only eavesdrop the communication between legitimate tag and reader, while in the second model, she can also interrogate a legitimate tag. The strongest security notion is against MIM attacks where the adversary can interact with both the tag and the reader and learn the reader's accept or reject decision.

The *HB*$^+$ protocol was proved to be secure against passive and active attacks. However, the security proof did not cover MIM attacks. Thus, it came as no surprise that soon after the introduction of the *HB*$^+$, it was shown [5] that there is a MIM attack that can easily reveal the secret key. Almost all the variants of *HB*$^+$, that have a security proof, can resist passive and active attacks; however, these schemes have also been shown to be weak against a MIM attacker. The only exception constitutes the *HB*$^\#$ protocol that partially resists against MIM attacks. In more detail, the protocol is secure when the adversary is able to modify only the messages that the reader sends to the tag.

In 2011, Kiltz et al. [9], in their paper that was awarded with the Eurocrypt best paper price, introduced *AUTH*, the most recently proposed LPN-based authentication protocol and proved that given the hardness of the subspace LPN problem, a variant of the LPN problem [13], *AUTH* is secure against both passive and active attackers. However, the security proof does not include MIM adversaries. In this paper, we will show that *AUTH*, like practically all the variants of the *HB*$^+$ protocol, is weak against MIM attackers, by introducing an efficient MIM attack that reveals the secret key with linear computational and data complexity with respect to the size of the secret key. Recently, the protocol's weakness against a full MIM attack was demonstrated [12].

The paper is organized as follows. In Sect. 2, we briefly present the *AUTH* authentication protocol, and in Sect. 3, we introduce the proposed attack, and we evaluate its computational and data complexity. Finally, conclusions can be found in Sect. 4.

2 The AUTH protocol

First, we establish some notation. We use $\boldsymbol{b} \in_R \mathbb{F}_2{}^k$ to denote a random binary vector $\boldsymbol{b}$ with length k, $\boldsymbol{M} \in_R \mathbb{F}_2{}^{k \times n}$ to denote a random $k \times n$ binary matrix $\boldsymbol{M}$, and $wt(\boldsymbol{b})$ is the Hamming weight of $\boldsymbol{b}$, that is, the number of nonzero elements $b(i)$, for $1 \leq i \leq k$. Also, $Ber(\eta)$ stands for the Bernoulli distribution with parameter η, meaning that a bit $\nu \in Ber(\eta)$, when $Pr[\nu = 1] = \eta$ and $Pr[\nu = 0] = 1 - \eta$. A vector $\boldsymbol{\nu}$ randomly chosen among all the vectors with length m, such that $\nu(i) \in Ber(\eta)$ and $\eta \in (0, 1/2)$, for $0 \leq i \leq m - 1$, is denoted by $\boldsymbol{\nu} \in_R Ber(m, \eta)$. Finally, let $\boldsymbol{a}$ and $\boldsymbol{b}$ be two binary vectors with length l. We use $\boldsymbol{a}_{\downarrow \boldsymbol{b}}$ to denote the subvector of $\boldsymbol{a}$ obtained by deleting all bits of $\boldsymbol{a}$ where $\boldsymbol{b}$ equals 0 (for instance for $\boldsymbol{a} = 10101000$ and $\boldsymbol{b} = 00011010$, we have $\boldsymbol{a}_{\downarrow \boldsymbol{b}} = 010$).

The $AUTH$ protocol is a symmetric key authentication protocol supported by a security proof under the hardness of the subspace LPN problem [9]. After some initialization phase, the reader $\mathcal{R}$ and the tag $\mathcal{T}$ share a secret key $\boldsymbol{x}$ with length $2l$. The basic steps of the protocol go as follows (Fig. 1):

1. The reader $\mathcal{R}$ generates a random bit-string $\boldsymbol{a}$ with length $2l$ and sends it to tag $\mathcal{T}$. The Hamming weight of the $\boldsymbol{a}$ must be l.
2. The tag $\mathcal{T}$ verifies that the Hamming weight of $\boldsymbol{a}$ is l and generates a full rank $l \times n$ random binary matrix $\boldsymbol{R}$ and a bit-string $\boldsymbol{\nu} \in Ber(n, \eta)$. Then, it computes $\boldsymbol{z} = \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \boldsymbol{a}} \oplus \boldsymbol{\nu}$ and sends to the reader both $\boldsymbol{z}$ and the matrix $\boldsymbol{R}$. If $\boldsymbol{a} \neq l$, it aborts the execution of the protocol.
3. The reader first verifies that matrix $\boldsymbol{R}$ has rank n, and then it accepts the tag as authentic if $wt(\boldsymbol{z} \oplus \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \boldsymbol{a}}) \leq \tau$, where $n\eta \leq \tau \leq \frac{n}{2}$ and $\boldsymbol{R}^T$ is the transpose of $\boldsymbol{R}$. If the rank is not correct or the condition is not satisfied, the tag is rejected.

It is assumed that the reader communicates with the back-end server over a secure channel, while the tag and the reader communicate over an insecure channel.

Typically, the false rejection rate P_{FR} of the protocol; that is, the probability to reject a legitimate tag, equals the probability $wt(\boldsymbol{\nu}) > \tau$, and it is given by

$$P_{FR} = \sum_{i=\tau+1}^{n} \binom{n}{i} \eta^i (1 - \eta)^{n-i}.$$

Finally, the false acceptance rate P_{FA}; that is, the probability to accept a randomly selected response $\boldsymbol{z}$, can be computed

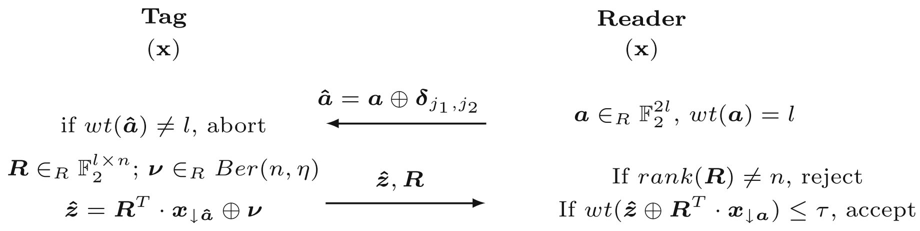
Tag
$(\mathbf{x})$
Reader
$(\mathbf{x})$
$\hat{\boldsymbol{a}} = \boldsymbol{a} \oplus \boldsymbol{\delta}_{j_1, j_2}$
$\boldsymbol{a} \in_R \mathbb{F}_2^{2l}$, $wt(\boldsymbol{a}) = l$
if $wt(\hat{\boldsymbol{a}}) \neq l$, abort
$\boldsymbol{R} \in_R \mathbb{F}_2^{l \times n}$; $\boldsymbol{\nu} \in_R Ber(n, \eta)$
$\hat{\boldsymbol{z}} = \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \hat{\boldsymbol{a}}} \oplus \boldsymbol{\nu}$
$\hat{\boldsymbol{z}}, \boldsymbol{R}$
If $rank(\boldsymbol{R}) \neq n$, reject
If $wt(\hat{\boldsymbol{z}} \oplus \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \boldsymbol{a}}) \leq \tau$, accept

Fig. 2 The attack against *AUTH* protocol

as follows:

$$P_{FA} = \sum_{i=0}^{\tau} \binom{n}{i} 2^{-n};$$

that is, it is equal to the number of binary vectors with length n and Hamming weight at most τ.

3 Security analysis

In [9], the authors prove that the protocol is secure against passive and active attacks based on the hardness of the recently introduced subspace LPN problem [13]. However, the main problem that it was identified to practically all LPN-based authentication protocols is the vulnerability against MIM attacks. Next, we demonstrate that the $AUTH$ protocol does not constitute an exception.

3.1 Attack steps

In a MIM attack, the adversary is able to modify all communication between a legitimate tag and the reader. In our case, we will show that it suffices to alter only one message, the challenge send by the reader (Fig. 2). The attack consists of two phases. In the first phase, the attacker discloses two elements of the secret key $\boldsymbol{x}$ that are equal to zero. In the second phase, she uses this information to reveal the whole key. We use $\boldsymbol{\delta}_{j_1, j_2}$ to denote the vector with length $2l$ that is all zeros except elements $\delta(j_1) = \delta(j_2) = 1$, $1 \leq j_1 < j_2 \leq 2l$.

Phase I Choose a pair of element indexes (j_1, j_2) of the key $\boldsymbol{x}$, $1 \leq j_1 < j_2 \leq 2l$.

1. Observe the value of $\boldsymbol{a}$. When $a(j_1) \neq a(j_2)$ complement the two bits of $\boldsymbol{a}$ and replace the vector by the produced vector $\hat{\boldsymbol{a}} = \boldsymbol{a} \oplus \boldsymbol{\delta}_{j_1, j_2}$.
2. Observe the result of the authentication.
3. Repeat the previous steps for the same pair (j_1, j_2). If the tag is rejected with probability higher than the false reject rate P_{FR}, then choose a new pair of indexes (j_1, j_2) and repeat the procedure. Otherwise, assume that $x(j_1) = x(j_2) = 0$ and exit *Phase I*.

Thus, from *Phase I*, we have $x(j_1) = x(j_2) = 0$ for some $1 \leq j_1 < j_2 \leq 2l$. Next, we compute the rest $2l - 2$ bits of $\boldsymbol{x}$.

Phase II For each $1 \leq j \leq 2l$ and $j \neq j_1, j_2$ do,

1. Observe the value of $\boldsymbol{a}$. When $a(j_1) \neq a(j)$ complement the two bits of $\boldsymbol{a}$ and replace the vector by the produced vector $\hat{\boldsymbol{a}} = \boldsymbol{a} \oplus \boldsymbol{\delta}_{j_1, j_2}$.
2. Observe the result of the authentication.
3. Repeat the previous steps for the same pair (j_1, j). If the tag is rejected with probability higher than the false reject rate P_{FR}, then $x(j) = 1$. Otherwise, assume that $x(j) = 0$.

Note 1 *Phase I* delivers more information that we actually use in the described attack. In detail, when the tag is rejected with probability higher than the false reject rate P_{FR}, then it holds that at least one of $x(j_1)$ and $x(j_2)$ is non-zero. In other words, it holds that $1 + x(j_1) + x(j_2) + x(j_1)x(j_2) = 0$. Hence, by repeating the *Phase I*, each time with a different pair of indexes (j_1, j_2), we derive either the values of these elements, when both are zero, or a quadratic equation. In this way, we can build a system of quadratic equations and solve it, for instance with the linearization method, and reveal the secret key.

3.2 Proof of correctness

The attack is based on the following observation. When two bits $a(j_1)$ and $a(j_2)$ of $\boldsymbol{a}$, with $a(j_1) \neq a(j_2)$, are complemented, then the Hamming weight of the bit-sting remains the same; that is, $wt(\boldsymbol{a}) = wt(\hat{\boldsymbol{a}})$, where $\hat{\boldsymbol{a}} = \boldsymbol{a} \oplus \boldsymbol{\delta}_{j_1, j_2}$. Thus, when an attacker replaces the vector $\boldsymbol{a}$, the modified message $\hat{\boldsymbol{a}}$ is accepted by the tag.

Using $\hat{\boldsymbol{a}}$, the tag computes $\hat{z} = \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \hat{\boldsymbol{a}}} \oplus \boldsymbol{\nu}$ and sends it together with $\boldsymbol{R}$ to the reader. Then, the reader calculates

$$\begin{aligned} \boldsymbol{\omega}_{j_1, j_2} &= \hat{z} \oplus \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \boldsymbol{a}} = \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \hat{\boldsymbol{a}}} \oplus \boldsymbol{\nu} \oplus \boldsymbol{R}^T \cdot \boldsymbol{x}_{\downarrow \boldsymbol{a}} \\ &= x(j_1) R_{j_1}^T \oplus x(j_2) R_{j_2}^T \oplus \boldsymbol{\nu}. \end{aligned}$$

where R_i is the ith row of the random matrix $\boldsymbol{R}$.

If $x(j_1) = x(j_2) = 0$, then $\boldsymbol{\omega}_{j_1, j_2} = \boldsymbol{\nu}$, and the tag is rejected with probability equal to the false reject rate P_{FR}. Otherwise, $\boldsymbol{\omega}_{j_1, j_2}$ equals the sum of $\boldsymbol{\nu}$ with one or two random vectors $R_{j_1}^T$, $R_{j_2}^T$, and the tag is rejected with high probability equal to $1 - P_{FA}$.

Similarly, in *Phase II*, since $x(j_1) = 0$, for each element $j \neq j_1, j_2$, the reader computes $\boldsymbol{\omega}_{j_1, j} = x(j_2) R_{j_2}^T \oplus \boldsymbol{\nu}$.

If $x(j_2) = 0$, it is rejected with very small probability P_{FR}, and if $x(j_2) = 0$, it is rejected with high probability $1 - P_{FA}$.

3.3 Complexity issues

The first phase of the attack is repeated until a pair of bits $x(j_1), x(j_2)$ of the secret key is found that both elements are zero. Since the secret key has been randomly selected, the probability such a pair of elements to exist $p_0 = \frac{1}{4}$. At the same time, in step 1, approximately half of the times, the challenge vector $\boldsymbol{a}$ is inappropriate, that is, $a(j_1) = a(j_2)$, and the current protocol execution is discarded with probability $p_1 = \frac{1}{2}$. Finally, by observing ψ times the reader's decision in step 2 , the probability of correctly guessing the value of the two elements is $1 - (P_{FR})^{\psi}$. Since, for practical values of the protocol parameters, the false rejection rate P_{FR} is extremely small, close to zero (around 2^{-80}), the overall success probability of *Phase I* can be considered constant and approximately equal to $\frac{1}{8}$.

In *Phase II*, following the same argumentation, the success probability for each one of the other $2l-2$ secret key bits is again constant. Thus, the overall required modified executions of the protocol are just $\mathcal{O}(2l)$, that is, the complexity of the attack is linear with respect to the length of the secret key.

4 Remarks

The design of a lightweight authentication protocol that is based on the LPN problem and that can provably resist MIM attackers is an extremely difficult task, and it is out of the scope of this paper. Thus, enhancing in a provable way, the security of $AUTH$ is left as a future work. However, from our experience in studying the LPN-based lightweight protocols, we can derive some first guidelines.

In [9], in the second part of the paper, the authors present a LPN-based Message Authentication Code (MAC) that is provably secure against MIM attacks. Then, they propose the adaption of the MAC for the secure authentication of the tag. The protocol requires the presence of a secure hash function, that must be kept secret, as part of the secret key, and, clearly, such a construction a little "heavier" than lightweight. However, it gives us valuable lessons. More precisely, we believe that the main reason that practically all LPN-based authentication protocols, at least the ones supported by a security proof, fail to resist against MIM attacks is the absence of nonlinearity, a conscious decision that all the designers made in order to keep the protocols as lightweight as possible. Thus, our current work is in the direction of using low cost nonlinearity to enhance the security of LPN-based protocols.

References

1. Avoine, G.: RFID Security and Privacy Lounge. Available at http://www.avoine.net/rfid/
2. Bringer, J., Chabanne, H., Dottax, E.: HB^{++}: a Lightweight Authentication Protocol Secure against Some Attacks. In: Proceedings of the IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing—SecPerU (2006)
3. Bringer, J., Chabanne, H.: Trusted-HB: a low-cost version of HB secure against man-in-the-middle attack. IEEE Trans. Inf. Theory **54**, 4339–4342 (2008)
4. Duc, D.N., Kim, K.: Securing HB^{+} against GRS Man-in-the-Middle Attack. In: Proceedings of the Symposium on Cryptography and Information, Security (SCIS2007) (2007)
5. Gilbert, H., Robshaw, M., Silbert, H.: An active attack against HB^{+}-a provable secure lightweighted authentication protocol. In: Cryptology ePrint Archive, Report 2005/237, (2005). http://eprint.iacr.org
6. Gilbert, H., Robshaw, M., Seurin, Y.: $HB^{\#}$: increasing the security and efficiency of HB^{+}. In: Proceedings of Eurocrypt 2008, Springer LNCS, 4965, pp. 361–378 (2008)
7. Hopper, N.J., Blum, M.: Secure human identification protocols. In: Proceedings of Asiacrypt 2001, Springer LNCS, 2248, pp. 52–66 (2001)
8. Juels, A., Weis, S.A.: Authenticating pervasive devices with human protocols. In: Proceedings of Crypto 2005, Springer LNCS, 3126, pp. 293–308 (2005)
9. Kiltz, E., Pietrzak, K., Cash, D., Jain, A., Venturi, D.: Efficient authentication from hard learning problems. In: Proceedings of the Eurocrypt 2011, LNCS Springer, pp. 7–26 (2011)
10. Leng, X., Mayes, K., Markantonakis K.: HP-MP^{+}: an improvement on the HB-MP protocol. In: Proceedings of the IEEE International Conference on RFID 2008, IEEE Press, pp. 118–124 (2008)
11. Munilla, J., Peinado, A.: HP-MP: a further step in the HB-family of lightweight authentication protocols. Computer Networks **51**, 2262–2267 (2007)
12. Ouafi, K., Overbeck, R., Vaudenay, S.: On the security of $HB\#$ against a man-in-the-middle attack. In: Proceedings of Asiacrypt 2008, Springer LNCS, 5350, pp. 108–124 (2008)
13. Pietrzak, K.: Subspace LWE. http://homepages.cwi.nl/pietrzak/publications/SLWE.pdf (2011)
14. Piramuthu, S.: HB and related lightweight authentication protocols for secure RFID tag/reader authentication. In: Proceedings of CollECTeR Europe Conference, Basel, 9–10 June (2006)
15. Rizomiliotis, P.: HB-MAC: improving the random—$HB^{\#}$ authentication protocol. In: Proceedings of the 6th International Conference on Trust, Privacy and Security in Digital Business (TrustBus), LNCS Springer, pp. 159–168 (2009)
16. Yoon, B., Sung, M.Y., Yeon, S., Oh, H.S., Kwon, Y., Kim, C., Kim, K.-H.: HB-MP^{++} protocol: an ultra light-weight authentication protocol for RFID system. In: Proceedings of the IEEE International Conference on RFID, pp. 186–191 (2009)