Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2016, Article ID 9289050, 9 pages
http://dx.doi.org/10.1155/2016/9289050

Research Article

A Protocol for Provably Secure Authentication of a Tiny Entity to a High Performance Computing One

Siniša Tomović,[1] Miodrag J. Mihaljević,[1] Aleksandar Perović,[2] and Zoran Ognjanović[1]

[1]*Mathematical Institute, Serbian Academy of Sciences and Arts, Kneza Mihaila 36, 11000 Belgrade, Serbia*
[2]*Faculty of Transport and Traffic Engineering, University of Belgrade, Vojvode Stepe 305, 11000 Belgrade, Serbia*

Correspondence should be addressed to Miodrag J. Mihaljević; miodragm@turing.mi.sanu.ac.rs

Received 25 December 2015; Accepted 24 March 2016

Academic Editor: Zoran Obradovic

The problem of developing authentication protocols dedicated to a specific scenario where an entity with limited computational capabilities should prove the identity to a computationally powerful Verifier is addressed. An authentication protocol suitable for the considered scenario which jointly employs the learning parity with noise (LPN) problem and a paradigm of random selection is proposed. It is shown that the proposed protocol is secure against active attacking scenarios and so called GRS man-in-the-middle (MIM) attacking scenarios. In comparison with the related previously reported authentication protocols the proposed one provides reduction of the implementation complexity and at least the same level of the cryptographic security.

1. Introduction

Expansion of Internet of Things (IoT) and Machine-to-Machine (M2M) communications has implied additional challenges regarding the information security issues. In a number of scenarios at least one of the entities involved is a tiny device with very limited computational capabilities and heavy restriction regarding power consumption. Accordingly, a challenge is developing of the information security techniques which minimize the computational and power consumption overheads implied by the security requirements.

Authentication of one entity, called Prover, to another, called Verifier, has been well recognized as one of the cornerstones for achieving the desired level of information security (as well as cybersecurity). Authentication protocols for restricted implementation scenarios have been considered in a number of papers including [1–3]. This is also in line with a discussion recently reported in [4].

This paper considers an authentication approach suitable for scenarios where an entity with highly constrained computational capabilities should in a secure way perform authentication to the verification party with high performance computational capabilities.

The reported protocols appear as not enough suitable because either (i) they are not enough lightweight for a tiny party of an authentication protocol and do not take into account the asymmetrical implementation constraints (ii) or/and they do not provide the desired level of cryptographic security.

Consequently, in this paper, we jointly employ certain elements of the reported protocols to achieve our main goal: development of the authentication protocols with asymmetric implementation complexity at Prover and Verifier sides which provides desired provable level of cryptographic security.

2. Background

2.1. Family of HB Authentication Protocols. The origin of a family of authentication protocols based on hardness of learning parity with noise (LPN) problem is a lightweight

two-pass authentication protocol called the HB protocol reported in [5]. Simplicity of the approach and its provable security implied by the fact that the LPN problem is NP-complete (see [6]) have attracted much interest. The HB protocol requires only basic AND and XOR operations and it has been proved to be secure against passive attacks via reduction to the LPN problem. However, it is insecure against a stronger adversary, active adversary, who has ability to impersonate a reader and interact with legitimate tags. In order to address this weakness, a modified HB protocol called the HB+ protocol has been reported in [7–9]. The HB+ protocol has been proved to be secure against active attacks, but it has been shown in [10] that the HB+ protocol is insecure against a man-in-the-middle (MIM) attack. Specifically, in [10], a linear time MIM attack against the HB+ protocol that is called the GRS-MIM attack has been reported. Later on a number of variants of the HB+ protocol have been proposed to prevent the GRS-MIM attack (including [11, 12]), but all of them were shown to be insecure later. After a number of unsuccessful attempts, [13] has extended the HB+ protocol and proposed a new protocol called the HB# that only requires three-pass communication and is secure against GRS-MIM attacks. While two vectors are shared by the Prover and the Verifier as the secret keys in the HB+ protocol, two matrices are shared by the parties as the secret keys in the HB# protocol: by increasing the size of secret keys, the HB# protocol achieves stronger security and reduces the communication complexity. However, [14] has described an MIM attack against the HB# protocol. After that, several three-pass protocols that resist MIM attacks were proposed. Three-pass authentication protocols which have stronger security had been well studied. From a practical aspect, however, two-pass authentication protocol is more desirable than three-pass authentication protocol. Construction of a two-pass authentication scheme with even the active security had been open problem for a long time. In [15] a two-pass authentication protocol called the AUTH protocol has been proposed. The AUTH protocol is the first two-pass protocol which achieves the active security and yields a large improvement in terms of round complexity. Also [15] has reported two variants of the AUTH protocol, which could be called the AUTH+ protocol and the AUTH# protocol. In the AUTH+ protocol, the computational complexity decreases in exchange for increasing the number of secret keys. In the AUTH# protocol, the communication complexity decreases in exchange for the increasing the size of secret keys like the HB# protocol. Later on in [16] the active security of the AUTH# protocol has been proved employing a modular approach, which simplifies the proof: for this proof, a new computational assumption has been introduced and called the MSLPN assumption.

2.2. HB# Authentication Protocol. HB# authentication protocol is a three-round challenge-response protocol which has been proposed and analyzed in [13]. Random-HB# is a generalization of HB+ where the form of the secrets $\mathbf{x}$ and $\mathbf{y}$ has been changed from k-bit vectors into $(k_X \times m)$- and $(k_Y \times m)$-binary matrices $\mathbf{X}$ and $\mathbf{Y}$. Random-HB# protocol is displayed as follows.

Parameters: k_x, k_Y, m, τ, u

$$
\begin{array}{lcl}
\mathscr{P}(\text{secret } \mathbf{X}, \mathbf{Y}) & & \mathscr{V}(\text{secret } \mathbf{X}, \mathbf{Y}) \\
\mathbf{e} \leftarrow \mathrm{Ber}_\tau^m & & \\
\mathbf{b} \xleftarrow{\$} \mathbb{Z}_2^{k_Y} & \xrightarrow{\mathbf{b}} & \\
 & \xleftarrow{\mathbf{a}} & \mathbf{a} \xleftarrow{\$} \mathbb{Z}_2^{k_X} \\
\mathbf{z} = \mathbf{aX} + \mathbf{bY} + \mathbf{e} & \xrightarrow{\mathbf{z}} & ?\|\mathbf{z} \oplus \mathbf{aX} \oplus \mathbf{bY}\| \le mu.
\end{array}
$$

For an additional explanation of the notations, please refer to Section 3.2.

While Random-HB# has a number of similarities with the HB+ protocol, there are important differences as well. In particular, the final verification by the reader consists of the comparison of two m-bit vectors $\mathbf{a} \cdot \mathbf{X} \oplus \mathbf{b} \cdot \mathbf{Y}$ and $\mathbf{z}$.

2.3. Authentication Employing Random Selection. Design and security evaluation of authentication protocols based on random selection paradigm have been initially reported in [17–19]. The principle of random selection can be described as follows. Suppose that the Verifier Alice and the Prover Bob run a challenge-response authentication protocol which uses a lightweight symmetric encryption operation

$$E : \{0,1\}^n \times \mathscr{K} \longrightarrow \{0,1\}^m \tag{1}$$

of block length n, where $\mathscr{K}$ denotes an appropriate key space. Suppose further that E is weak in the sense that a passive adversary can efficiently compute the secret key $K \in \mathscr{K}$ from samples of the form $(u, E_K(u))$. This is obviously the case if E is linear.

Random selection denotes a method for compensating the weakness of E by using the following mode of operation. Instead of holding a single $K \in \mathscr{K}$, Alice and Bob share a collection $K_1, \ldots, K_L$ of keys from $\mathscr{K}$ as their common secret information, where $L > 1$ is a small constant.

(i) Upon receiving a challenge $u \in \{0,1\}^n$ from Alice, Bob chooses a random index $\ell \in \{1, 2, \ldots, L\}$ and outputs the response $y = E(u, K_\ell)$.

(ii) The verification of y with respect to u can be efficiently done by computing $E_{K_\ell}^{-1}(y)$ for all $\ell = 1, 2, \ldots, L$.

2.4. Security Evaluation of an Authentication Protocol. The common scenarios for security evaluation against impersonation attacks are as follows. The basic one is a passive attack scenario which proceeds in two phases: in the first phase the adversary eavesdrops a (large) number of interactions between P and V and then attempts to cause V to accept the authentication response in the second phase (where P is no longer available). In an active attack, the adversary is additionally allowed to interact with P in the first phase. The strongest and most realistic attack model is a man-in-the-middle attack (MIM), where the adversary can arbitrarily interact with P and V (with polynomially many concurrent executions allowed) in the first phase.

3. Proposal of a Dedicated Authentication Technique

This section proposes an authentication protocol with asymmetric implementation complexity which is suitable for authentication of a Prover with low computational capabilities to a Verifier with high performance computational capabilities.

3.1. Underlying Ideas for Design. Taking into account results on the authentication protocols reported in [13, 17–20], this paper proposes a novel authentication protocol which is based on a nontrivial hybridization and upgrading of certain previously reported results.

The initial observations regarding certain previously reported protocols are the following ones:

(i) The protocols reported in [13, 20] provide a number of interesting framework elements for developing highly secure authentication protocols, but they appear as not light enough for a number of M2M authentication scenarios and do not take into account asymmetric implementation constraints. It is desirable to reduce implementation complexity of certain authentication protocols with implementation potential in tiny Provers, like HB# authentication protocol [13].

(ii) The protocols reported in [17–19] employ an interesting paradigm of random selection but do not provide the desired level of cryptographic security.

Accordingly, the underlying ideas for developing the novel authentication protocols were the following ones:

(i) Employ framework elements of HB# authentication protocol and modify it in order to fit into implementation restrictions at a tiny Prover and asymmetric implementation and execution capabilities of Prover and Verifier sides.

(ii) Do not employ elements of the reported protocols which do not support lightweightness of the authentication at the party (usually the Prover) with tiny capabilities.

(iii) Employ the power of random selection approach to enhance cryptographic security of the protocol at the tiny party as a trade-off between the cryptographic security of the protocol and its increased implementation complexity at the more powerful party (usually the Verifier).

Particularly, note the following:

(i) Instead of employment of two secret keys $\mathbf{X}$ and $\mathbf{Y}$ as in the source HB# protocol, we propose employment of one secret key and the random selection paradigm for achieving the same security goals.

3.2. Notations. We use the following notations:

(i) $\mathbb{Z}_2^m$ and $\mathbb{Z}_2^{m\times n}$ denote, respectively, set of all m-dimensional binary vectors and set of binary matrices $m \times n$.

(ii) We use normal, bold, and capital bold letters such as x, $\mathbf{x}$, and $\mathbf{X}$ to denote single elements, vectors, and matrices.

(iii) For a vector $\mathbf{x}$, $\mathbf{x}[i]$ denotes the ith element of $\mathbf{x}$.

(iv) $\mathbf{x} \oplus \mathbf{y}$ is the bitwise XOR operation of two vectors $\mathbf{x}$ and $\mathbf{y}$; that is, $(\mathbf{x}\oplus\mathbf{y})[i] = \mathbf{x}[i]\oplus\mathbf{y}[i]$, for all i. Similarly, $\mathbf{X}\oplus\mathbf{Y}$ is defined as bitwise XOR of two binary matrices $\mathbf{X}$ and $\mathbf{Y}$.

(v) $\|\mathbf{x}\|$ denotes the Hamming weight of binary vector $\mathbf{x}$, which is the number of its nonzero elements $\mathbf{x}[i]$.

(vi) $x \xleftarrow{\$} X$ is the operation of sampling a value x from the uniform distribution on the finite set X.

(vii) Ber_τ represents the Bernoulli distribution with parameter τ, and $\nu \leftarrow \mathrm{Ber}_\tau$ means that for a bit ν, $\Pr[\nu = 1] = \tau$, and $\Pr[\nu = 0] = 1 - \tau$.

(viii) $\mathbf{e} \leftarrow \mathrm{Ber}_\tau^m$ means that the vector $\mathbf{e}$ was randomly chosen among all the vectors of length m, such that $e[i] \leftarrow \mathrm{Ber}_\tau$ and $\tau \in (0, 1/2)$, for $0 \le i \le m - 1$.

(ix) Let $\mathbf{e}^*$ be a vector of length m and weight Δ. *A circulant matrix* $\mathbf{E}^* = \mathrm{Circ}_n(\mathbf{e}^*)$ over the vector $\mathbf{e}^*$ is a matrix with n columns, whose first column is $\mathbf{e}^*$, and each next column is produced by a rotation of the previous column one position downwards.

The elements of the set $\mathbf{E}^*_{m,n,\Delta}$ of circulant matrices with n columns, generated over vectors of length m and weight Δ, can be ordered in the array $\mathbf{E}^*_{m,n,\Delta}[1], \ldots, \mathbf{E}^*_{m,n,\Delta}[\binom{m}{\Delta}]$.

(x) *$(m \times n)$-binary Toeplitz matrix* is a matrix where for each diagonal from upper-left to lower-right all the elements on the diagonal have the same value. Note that the entire matrix is specified by the top row and the first column, so it can be parametrized by $m + n - 1$ bits. Note that circulant matrices are also a kind of Toeplitz matrices. Toeplitz matrices can be generated efficiently and have good statistical properties [13].

An algorithm A is *probabilistic* if it makes random choices during its execution. A probabilistic algorithm A is *probabilistic polynomial-time* (PPT) if for any input the computation of algorithm terminates in at most polynomial number of steps in the length of input. We also use the term *efficient algorithm* as a synonym for PPT algorithm. A function $f(x)$ is *negligible* if for every positive polynomial p, with x being large enough, it holds that $f(x) < 1/p(x)$.

3.3. Proposal of the Authentication Protocol. The authentication protocol NHB# (Nondeterministic HB#) is displayed as follows:

Parameters: m, n, τ, thr

$$\begin{array}{ccc} \mathscr{P}(\text{secret } \mathbf{Y}) & & \mathscr{V}(\text{secret } \mathbf{Y}) \\ \mathbf{b} \overset{\$}{\leftarrow} \mathbb{Z}_2^m & \xrightarrow{\mathbf{b}} & \\ & \xleftarrow{\mathbf{a}} & \mathbf{a} \overset{\$}{\leftarrow} \mathbb{Z}_2^m \\ \mathbf{e} \leftarrow \mathrm{Ber}_\tau^m & & \\ \mathbf{e}^* \overset{\$}{\leftarrow} \mathbb{Z}_2^m, \|\mathbf{e}^*\| = \Delta & & \\ \mathbf{E}^* = \mathrm{Circ}_n(\mathbf{e}^*) & & \\ \mathbf{z} = \mathbf{aE} + \mathbf{bY} + \mathbf{e} & \xrightarrow{\mathbf{z}} & ?\|\mathbf{z} \oplus \mathbf{aE}^*[i] \oplus \mathbf{bY}\| \le \mathrm{thr} \\ & & \text{for some } i,\ 1 \le i \le \binom{m}{\Delta}, \\ & & \text{where } \mathbf{E}^*[i] = \mathbf{E}^*_{m,n,\Delta}[i]. \end{array}$$

This authentication protocol NHB# (Nondeterministic HB#) is an interactive protocol being executed between *Prover* $\mathscr{P}$ and *Verifier* $\mathscr{V}$ which are efficient algorithms. They share one secret key, a matrix $\mathbf{Y} \in \mathbb{Z}_2^{m \times n}$, which is produced by the key-generation algorithm $\mathrm{KG}(1^k)$, for the security parameter k. As a result of the protocol execution, Verifier $\mathscr{V}$ outputs indicator of acceptance value IND, such that IND = 1 if $\mathscr{V}$ confirms that the Prover is valid; otherwise the indicator value is set to IND = 0.

Public Parameters

(i) $m, n \in \mathbb{N}$: dimensions of the secret matrix $\mathbf{Y}$, which depend on the security parameter k;

(ii) $\tau \in (0, 1/4)$: parameter of the Bernoulli distribution (Ber_τ);

(iii) thr: the acceptance threshold, such that $\mathrm{thr} \ll m/2$.

Key Generation. Algorithm $\mathrm{KG}(1^k)$ samples a random matrix $\mathbf{Y} \overset{\$}{\leftarrow} \mathbb{Z}_2^{m \times n}$ as a secret key and returns it to $\mathscr{P}$ and $\mathscr{V}$.

Protocol Specification

Phase I: the protocol initialization, executed by $\mathscr{P}$

$\mathbf{b} \overset{\$}{\leftarrow} \mathbb{Z}_2^m$;
$\mathbf{b} \mapsto \mathscr{V}$ ($\mathscr{P}$ sends message $\mathbf{b}$ to $\mathscr{V}$).

Phase II: challenge generation, executed by $\mathscr{V}$

$\mathbf{a} \overset{\$}{\leftarrow} \mathbb{Z}_2^m$;
$\mathbf{a} \mapsto \mathscr{P}$ ($\mathscr{V}$ sends message $\mathbf{a}$ to $\mathscr{P}$).

Phase III: response generation, executed by $\mathscr{P}$

$\mathbf{e} \leftarrow \mathrm{Ber}_\tau^n$;
$\mathbf{e}^* \overset{\$}{\leftarrow} \mathbb{Z}_2^m$, $\|\mathbf{e}^*\| = \Delta$;
$\mathbf{E}^* = \mathrm{Circ}_n(\mathbf{e}^*)$
$\mathbf{z} \coloneqq \mathbf{aE}^* + \mathbf{bY} + \mathbf{e}$;
$\mathbf{z} \mapsto \mathscr{V}$ ($\mathscr{P}$ sends $\mathbf{z}$ to $\mathscr{V}$).

Phase IV: the verification process, executed by $\mathscr{V}$

IND $\coloneqq$ 0, $i \coloneqq 1$;
while (IND = 0 and $i \le \binom{m}{\Delta}$) do
  if $\|\mathbf{z} \oplus \mathbf{aE}^*_{m,n,\Delta}[i] \oplus \mathbf{bY}\| \le \mathrm{thr}$ then IND $\coloneqq$ 1;
$\mathscr{V}$ outputs IND value.

Let us discuss the error rates of the protocol. The false rejection happens when a legitimate Prover gets rejected by the Verifier, that is, when the weight of vector $\mathbf{e} \leftarrow \mathrm{Ber}_\tau^n$ generated in the response phase is greater than thr value. Therefore, the probability of this event (the *completeness error*) is

$$P_{\mathrm{FR}} = \sum_{i=\mathrm{thr}+1}^{n} \binom{n}{i} \tau^i (1-\tau)^{n-i}. \tag{2}$$

The false acceptance occurs when an illegitimate Prover sends a randomly chosen response to the Verifier and gets authenticated, which happens with the following probability (the *soundness error*):

$$P_{\mathrm{FA}} = \frac{\binom{m}{\Delta}}{2^n} \sum_{i=0}^{\mathrm{thr}} \binom{n}{i} \tag{3}$$

taking into account the number of binary vectors of length n whose weight is at most thr and $\binom{m}{\Delta}$ different acceptance subcriteria of the Verifier.

Protocol Storage Optimization. Following the proposal in [13], the storage cost of the secret key $\mathbf{Y}$ may be reduced to $m+n-1$ bits, by using a Toeplitz matrix as $\mathbf{Y}$ instead of the random matrix. This type of storage reduction was applied in [13] to the Random-HB# protocol, resulting in the HB# protocol, which uses two Toeplitz matrices $\mathbf{X}$ and $\mathbf{Y}$ as secret keys. The security of HB# is based on the conjecture about hardness of the so-called Toeplitz-MHB Puzzle. In our case, the security of this optimized protocol version is based on the analogously plausible conjecture about hardness of the Toeplitz-MLPN problem (see Note 1, Section 5).

4. The Security Evaluation Framework

We consider two types of attack scenarios for our protocol: active and GRS-MIM scenarios. Both of them consist of two phases: the so-called *learning* and *forgery phases*. In the first phase, the adversary interacts with the Prover and/or Verifier, learning the information she needs in order to be successful in the second phase, where she interacts with the verifier trying to make him output IND = 1.

Definition 1. The *active attack* is being executed in two phases.

Phase 1. The adversary interacts only with the honest Prover $\mathscr{P}$ for a polynomial number of times q.

Phase 2. The adversary interacts with the Verifier trying to impersonate the Prover.

Definition 2. GRS-MIM attack is being executed in two phases.

Phase 1. The adversary interferes in q executions of the protocol. The adversary can eavesdrop or modify all messages between the honest Prover and honest Verifier and also gets the Verifier's decision, on each execution of protocol.

Phase 2. The adversary interacts with the Verifier trying to impersonate the Prover.

Let $\langle \mathcal{T}, \mathcal{V} \rangle$ denote a complete execution of NHB# protocol between a party $\mathcal{T}$ and the Verifier $\mathcal{V}$ and say that $\langle \mathcal{T}, \mathcal{V} \rangle$ takes value 1 if the execution ends with Verifier's acceptance (i.e., IND = 1) and takes value 0 otherwise (IND = 0).

Then we define the advantage of an active adversary $\mathcal{A}$ as

$$\begin{aligned} &\mathrm{Adv}_{\mathcal{A}}^{\mathrm{active}}(\tau, \mathrm{thr}, m, n) \\ &\quad = \left| \Pr\left[\langle \mathcal{A}, \mathcal{V} \rangle \longrightarrow 1 \mid \mathbf{Y} \xleftarrow{\$} \mathbb{Z}_2^{m \times n} \right] \right| \end{aligned} \tag{4}$$

and the advantage of a GRS-MIM adversary $\mathcal{A}$ as

$$\begin{aligned} &\mathrm{Adv}_{\mathcal{A}}^{\mathrm{MIM}}(\tau, \mathrm{thr}, m, n) \\ &\quad = \left| \Pr\left[\langle \mathcal{A}, \mathcal{V} \rangle \longrightarrow 1 \mid \mathbf{Y} \xleftarrow{\$} \mathbb{Z}_2^{m \times n} \right] \right|. \end{aligned} \tag{5}$$

If this advantage is nonnegligible, we say that the adversary $\mathcal{A}$ is *successful* in the given attack scenario against the protocol. The protocol is *secure against active attacks* if, for all efficient active adversaries $\mathcal{A}$, the advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{active}}(\tau, \mathrm{thr}, m, n, m)$ is negligible. Similarly, the protocol is *secure against MIM attacks* if, for all efficient MIM adversaries $\mathcal{A}$, the advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{MIM}}(\tau, \mathrm{thr}, m, n)$ is negligible.

5. Security Evaluation in the Active Attacking Scenario

LPN Problem. Let $\mathbf{x} \in \mathbb{Z}_2^m$ be a secret key, and $\tau \in (0, 1/2)$. We denote by $\Lambda_{\tau,m}(\mathbf{x})$ the probability distribution over $\mathbb{Z}_2^{m \times n}$ whose samples are pairs $(\mathbf{a}, \mathbf{a} \cdot \mathbf{x}^\top \oplus e)$, where $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_2^m$, $e \leftarrow \mathrm{Ber}_\tau$. Let $\Lambda_{\tau,m}(\mathbf{x})$ also denote the oracle taking a sample from distribution $\Lambda_{\tau,m}(\mathbf{x})$. U_{m+1} is the oracle taking samples from the uniform distribution over $\mathbb{Z}_2^{m+1}$. $\mathrm{LPN}_{\tau,m}$ problem consists of distinguishing the access to the oracle $\Lambda_{\tau,m}(\mathbf{x})$ from access to the oracle U_{m+1}.

The $\mathrm{LPN}_{\tau,m}$ advantage of a distinguisher $\mathcal{D}$ is defined as

$$\begin{aligned} \mathrm{Adv}_{\mathcal{D}}^{\mathrm{LPN}}(\tau, m) = \Big| &\Pr\left[\mathcal{D}^{\Lambda_{\tau,m}(\mathbf{x})} \longrightarrow 1 \mid \mathbf{x} \xleftarrow{\$} \mathbb{Z}_2^m \right] \\ &- \Pr\left[\mathcal{D}^{U_{m+1}} \longrightarrow 1 \right] \Big|. \end{aligned} \tag{6}$$

Definition 3 (LPN problem). $\mathrm{LPN}_{\tau,m}$ problem is (t, q, ϵ)-*hard* if for every distinguisher $\mathcal{D}$ running in time t and making q queries, the advantage $\mathrm{Adv}_{\mathcal{D}}^{\mathrm{LPN}}(\tau, m)$ is less than ϵ. In asymptotic terms, $\mathrm{LPN}_{\tau,m}$ is hard if for every efficient $\mathcal{D}$, the advantage $\mathrm{Adv}_{\mathcal{D}}^{\mathrm{LPN}}(\tau, m)$ is negligible.

Matrix LPN (MLPN) Problem. The matrix LPN problem is defined analogously to the LPN problem, with the difference that the secret key is now a matrix, not a vector.

Let $\mathbf{X} \in \mathbb{Z}_2^{m \times n}$ be a secret key, and $\tau \in (0, 1/2)$. We denote by $\widetilde{\Lambda}_{\tau,m,n}(\mathbf{X})$ the probability distribution $\mathbb{Z}_2^{m \times n}$ with samples $(\mathbf{a}, \mathbf{aX} \oplus \mathbf{e})$, where $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_2^m$ and $\mathbf{e} \leftarrow \mathrm{Ber}_\tau^m$. Let $\widetilde{\Lambda}_{\tau,m,n}(\mathbf{X})$ also denote the oracle producing samples from $\widetilde{\Lambda}_{\tau,m,n}(\mathbf{X})$. $\widetilde{U}_{m+n}$ is the oracle taking samples from the uniform distribution over $\mathbb{Z}_2^{m+n}$. $\mathrm{MLPN}_{\tau,m,n}$ problem, that is, the matrix variant of $\mathrm{LPN}_{\tau,m,n}$ problem, is to distinguish the access to the oracle $\widetilde{\Lambda}_{\tau,m,n}(\mathbf{X})$ from access to the oracle $\widetilde{U}_{m+n}$.

For a distinguisher $\mathcal{D}$, we define $\mathrm{MLPN}_{\tau,m,n}$ advantage of $\mathcal{D}$ as

$$\begin{aligned} &\mathrm{Adv}_{\mathcal{D}}^{\mathrm{MLPN}}(\tau, m, n) \\ &\quad = \left| \Pr\left[\mathcal{D}^{\widetilde{\Lambda}_{\tau,m,n}(\mathbf{X})} \longrightarrow 1 \mid \mathbf{X} \xleftarrow{\$} \mathbb{Z}_2^{m \times n} \right] \right. \\ &\quad \left. - \Pr\left[\mathcal{D}^{\widetilde{U}_{m+n}} \longrightarrow 1 \right] \right|. \end{aligned} \tag{7}$$

Definition 4 (MLPN problem). $\mathrm{MLPN}_{\tau,m,n}$ problem is (t, q, ϵ)-*hard* if, for all distinguishers $\mathcal{D}$ running in time t and making q queries, the advantage $\mathrm{Adv}_{\mathcal{D}}^{\mathrm{MLPN}}(\tau, m, n)$ is less than ϵ. In asymptotic terms, $\mathrm{MLPN}_{\tau,m}$ is hard if all efficient distinguishers $\mathcal{D}$ achieve a negligible $\mathrm{Adv}_{\mathcal{D}}^{\mathrm{MLPN}}(\tau, m, n)$ advantage.

Theorem 5 (equivalence to LPN). *If $\mathrm{LPN}_{\tau,m}$ problem is (t, q, ϵ)-hard, then $\mathrm{MLPN}_{\tau,m,n}$ problem is $(t', q, \epsilon n)$-hard; $t' = t - poly(q, m)$.*

Proof. We slightly adapt the proof of Proposition 2 in [16]. As usual, we will assume that there exists a distinguisher $\mathcal{D}_{\mathrm{MLPN}}$ with $\mathrm{MLPN}_{\tau,m,n}$-advantage $n\epsilon$ and use it as a subroutine to construct a distinguisher $\mathcal{D}_{\mathrm{LNP}}$ using $\mathcal{D}_{\mathrm{MLPN}}$ as a subroutine and prove that the corresponding $\mathrm{LPN}_{\tau,m}$-advantage is equal to ϵ, which contradicts the hardness assumption of $\mathrm{LPN}_{\tau,m}$.

Let $\mathbf{X} \in \mathbb{Z}_2^{m \times n}$ be a matrix with columns $\mathbf{x}_1^\top, \ldots, \mathbf{x}_n^\top$, and $i \in \{0, \ldots, n\}$. We define the probability distribution $\widetilde{\Lambda}_{\tau,m,n}^i(\mathbf{X})$ over $\mathbb{Z}_2^{m \times n}$ whose samples are pairs $(\mathbf{a}, \mathbf{z})$, where $\mathbf{z} = (\mathbf{a} \cdot \mathbf{x}_1^\top \oplus e_1, \ldots, \mathbf{a} \cdot \mathbf{x}_i^\top \oplus e_i, a_{i+1}, \ldots, a_n)$, for $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_2^m$, $e_j \leftarrow \mathrm{Ber}_\tau$ $(j = 1, \ldots, i)$, and $a_k \xleftarrow{\$} \mathbb{Z}_2$ $(k = i+1, \ldots, n)$.

For $i = 0, \ldots, n$, we denote by p_i the probability that distinguisher $\mathcal{D}_{\mathrm{MLPN}}$ outputs 1, when its input is a sample $\widetilde{\Lambda}_{\tau,m,n}^i(\mathbf{X})$:

$$p_i = \Pr\left[\mathcal{D}_{\mathrm{MLPN}}^{\widetilde{\Lambda}_{\tau,m,n}^i(\mathbf{X})} \longrightarrow 1 \mid \mathbf{X} \xleftarrow{\$} \mathbb{Z}_2^{m \times n} \right]. \tag{8}$$

Note that $\widetilde{\Lambda}_{\tau,m,n}^0(\mathbf{X})$ is the same as a sample from $\widetilde{U}_{m+n}$, and $\widetilde{\Lambda}_{\tau,m,n}^n(\mathbf{X})$ is the same as a $\widetilde{\Lambda}_{\tau,m,n}(\mathbf{X})$ sample. Therefore

$$\begin{aligned} p_0 &= \Pr\left[\mathcal{D}_{\mathrm{SLPN}}^{\widetilde{U}_{m+n}} \longrightarrow 1 \right], \\ p_n &= \Pr\left[\mathcal{D}_{\mathrm{MLPN}}^{\widetilde{\Lambda}_{\tau,m,n}(\mathbf{X})} \longrightarrow 1 \mid \mathbf{X} \xleftarrow{\$} \mathbb{Z}_2^{m \times n} \right]. \end{aligned} \tag{9}$$

The distinguisher $\mathscr{D}_{\mathrm{LPN}}$ will forward the samples $\widetilde{\Lambda}^{i}_{\tau,m,n}(\mathbf{X})$ for $i \xleftarrow{\$} \{0,\ldots,n\}$ as input to the distinguisher $\mathscr{D}_{\mathrm{MLPN}}$. Each sample will contain a sample from the unknown oracle that $\mathscr{D}_{\mathrm{LPN}}$ communicates with ($\Lambda_{\tau,m}(\mathbf{x})$ or U_{m+1}). Then, $\mathscr{D}_{\mathrm{LPN}}$ will produce the same output as $\mathscr{D}_{\mathrm{MLPN}}$. Now follows the precise description of actions taken by $\mathscr{D}_{\mathrm{LPN}}$ algorithm:

(1) Take a sample $(\mathbf{a},\mathbf{z}) \in \mathbb{Z}_2^{m\times n}$ from an unknown oracle $\mathcal{O}$.

(2) Choose $i \xleftarrow{\$} \{0,\ldots,n\}$, $\mathbf{x}_j \xleftarrow{\$} \mathbb{Z}_2^m$, $e_j \leftarrow \mathrm{Ber}_\tau$ $(j = 1,\ldots,i-1)$, $a_k \xleftarrow{\$} \mathbb{Z}_2$ $(k = i+1,\ldots,n)$.

(3) Make a sample $(\widetilde{\mathbf{a}},\widetilde{\mathbf{z}})$, where

$$\widetilde{\mathbf{a}} = \mathbf{a},$$
$$\widetilde{\mathbf{z}} = \left(\mathbf{a}\cdot\mathbf{x}_1^{\top} \oplus e_1,\ldots,\mathbf{a}\cdot\mathbf{x}_{i-1}^{\top} \oplus e_{i-1}, \boxed{\mathbf{z}}, a_{i+1},\ldots,a_n\right) \tag{10}$$

and forward $(\widetilde{\mathbf{a}},\widetilde{\mathbf{z}})$ as input to distinguisher $\mathscr{D}_{\mathrm{MLPN}}$.

(4) Output the same output value IND (0 or 1) returned by $\mathscr{D}_{\mathrm{MLPN}}$.

Note that if $\mathcal{O}$ is the oracle $\Lambda_{\tau,m}(\mathbf{x})$, then $(\widetilde{\mathbf{a}},\widetilde{\mathbf{z}})$ produced in Step (3) is a sample $\widetilde{\Lambda}^{i}_{\tau,m,n}(\mathbf{X})$. If $\mathcal{O}$ is the oracle U_{m+1}, then $(\widetilde{\mathbf{a}},\widetilde{\mathbf{z}})$ is a sample $\widetilde{\Lambda}^{i-1}_{\tau,m,n}(\mathbf{X})$.

In particular, $\mathrm{LPN}_{\tau,m}$ advantage of distinguisher $\mathscr{D}_{\mathrm{LPN}}$ can be computed as follows:

$$\begin{aligned}
\mathrm{Adv}^{\mathrm{LPN}}_{\mathscr{D}}(\tau,m) &= \left|\Pr\left[\mathscr{D}^{\Lambda_{\tau,m}(\mathbf{x})}_{\mathrm{LPN}} \longrightarrow 1 \mid \mathbf{x} \xleftarrow{\$} \mathbb{Z}_2^m\right]\right.\\
&\quad \left. - \Pr\left[\mathscr{D}^{U_{m+1}}_{\mathrm{LPN}} \longrightarrow 1\right]\right|\\
&= \left|\sum_{j=1}^{n}\left(\Pr\left[\mathscr{D}^{\Lambda_{\tau,m}(\mathbf{x})}_{\mathrm{LPN}} \longrightarrow 1 \mid \mathbf{x} \xleftarrow{\$} \mathbb{Z}_2^m,\ i=j\right]\right.\right.\\
&\quad \left.\left. \cdot \Pr[i=j] - \Pr\left[\mathscr{D}^{U_{m+1}}_{\mathrm{LPN}} \longrightarrow 1 \mid i=j\right]\Pr[i=j]\right)\right|\\
&= \frac{1}{n}\left|\sum_{j=1}^{n}\left(\Pr\left[\mathscr{D}^{\widetilde{\Lambda}^{j}_{\tau,m,n}(\mathbf{X})}_{\mathrm{MLPN}} \longrightarrow 1 \mid \mathbf{X} \xleftarrow{\$} \mathbb{Z}_2^{m\times n}\right]\right.\right.\\
&\quad \left.\left. - \Pr\left[\mathscr{D}^{\widetilde{\Lambda}^{j-1}_{\tau,m,n}(\mathbf{X})}_{\mathrm{MLPN}} \longrightarrow 1 \mid \mathbf{X} \xleftarrow{\$} \mathbb{Z}_2^{m\times n}\right]\right)\right|\\
&= \frac{1}{n}\left|\sum_{j=1}^{n}\left(p_j - p_{j-1}\right)\right| = \frac{1}{n}\left|p_n - p_0\right| \geq \epsilon.
\end{aligned} \tag{11}$$

Thus, distinguisher $\mathscr{D}_{\mathrm{LPN}}$ achieves $\mathrm{LPN}_{\tau,m}$ advantage greater or equal to ϵ, which contradicts that $\mathrm{LPN}_{\tau,m}$ is (t,q,ϵ)-hard. □

Note 1. Similarly as in Conjecture 1 [13], the hardness of the Toeplitz variant of MLPN problem can be conjectured, where the Toeplitz matrix is used as the secret key instead of a random matrix.

Theorem 6. *Let $n = \Theta(k)$, $0 < \tau < 1/4$, and $thr = \tau^{+}\cdot n$, where τ^{+} is a constant satisfying $\tau < \tau^{+} < 1/4$. If $LPN_{\tau,m}$ problem is hard, then the protocol NHB#(τ, thr, m, n) is safe against active attacks.*

Proof. The proof consists of the following four parts: (i) specification of a contradiction scenario which is a framework for security evaluation where an active adversary $\mathscr{A}$ exists; (ii) design of a distinguishing algorithm $\mathscr{D}$ which provides learning of $\mathscr{A}$ for solving a hard problem; (iii) procedure for distinguishing between two oracles; and (iv) estimation of the success rate of $\mathscr{D}$ in the distinguishing phase.

(i) We assume the opposite from Theorem 6 statement; that is, the protocol is not actively secure and an active adversary exists achieving a nonnegligible advantage, but that will contradict the hardness assumption of $\mathrm{MLPN}_{\tau,m,n}$ problem. The addressed scenario is formally specified in the following claim.

Claim. Suppose that there is an active adversary $\mathscr{A}$ interacting with Prover $\mathscr{P}$ in at most q executions of NHB# protocol, running in time t and achieving advantage $\mathrm{Adv}^{\mathrm{active}}_{\mathscr{A}}(\tau,\mathrm{thr},m,n) = \delta$. Then there exists a PPT algorithm $\mathscr{D}$, running in time $\mathcal{O}(t)$ and making $\Theta(k)$ oracle queries, such that

$$\begin{aligned}
&\left|\Pr\left[\mathscr{D}^{\widetilde{\Lambda}_{\tau,m,n}(\mathbf{Y})} \longrightarrow 1 \mid \mathbf{Y} \xleftarrow{\$} \mathbb{Z}_2^{m\times n}\right]\right.\\
&\quad \left. - \Pr\left[\mathscr{D}^{\widetilde{U}_{m+n}} \longrightarrow 1\right]\right| \geq \delta^2 - \frac{\binom{m}{\Delta}^2}{2^n}\sum_{i=0}^{2\cdot\mathrm{thr}}\binom{n}{i}.
\end{aligned} \tag{12}$$

(ii) The learning phase: at first, $\mathscr{D}$ initializes the learning phase of the adversary $\mathscr{A}$, while simulating the honest Prover $\mathscr{P}^{\mathrm{sim}}$ of protocol NHB#:

(1) $\mathscr{D}$ takes the sample $(\mathbf{b},\overline{\mathbf{z}})$ from oracle.

(2) $\mathscr{D}$ as $\mathscr{P}^{\mathrm{sim}}$ sends $\mathbf{b}$ to adversary $\mathscr{A}$.

(3) The active adversary $\mathscr{A}$ forwards a challenge $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_2^m$ to $\mathscr{P}^{\mathrm{sim}}$.

$\mathscr{D}$ is taking the following actions:

(4) chooses a vector $\mathbf{e}^{*} \xleftarrow{\$} \mathbb{Z}_2^m$, $\|\mathbf{e}^{*}\| = \Delta$. Then it makes $\mathbf{E}^{*} = \mathrm{Circ}_n(\mathbf{e}^{*})$ and sets the value $\mathbf{z} := \mathbf{a}\mathbf{E}^{*} + \overline{\mathbf{z}}$;

(5) as $\mathscr{P}^{\mathrm{sim}}$ sends the value $\mathbf{z}$ to active adversary $\mathscr{A}$.

The previous steps are repeated for q times.

(iii) The oracle distinguishing phase: $\mathscr{D}$ is taking the following actions:

(1) initiates a communication with adversary $\mathscr{A}$ (after its learning phase) which sends a blinding message $\mathbf{b}$;

(2) chooses two different random vectors $\mathbf{a}_1, \mathbf{a}_2 \xleftarrow{\$} \mathbb{Z}_2^n$;

(3) sends the challenge $\mathbf{a}_1$ to adversary $\mathscr{A}$ and receives a response $\mathbf{z}_1$ in return;

(4) rewinds $\mathscr{A}$ (behind Step (1)), sends another challenge $\mathbf{a}_2$, and receives the answer $\mathbf{z}_2$;

(5) receives the answer $\mathbf{z}_2$ from $\mathcal{A}$;

(6) for $i, j = 1, \ldots, \binom{m}{\Delta}$ makes values

$$w_{ij} := \left\| \mathbf{z}_1 \oplus \mathbf{z}_2 \oplus \mathbf{a}_1 \mathbf{E}^*_{m,n,\Delta}[i] \oplus \mathbf{a}_2 \mathbf{E}^*_{m,n,\Delta}[j] \right\| \quad (13)$$

and sends IND = 1 as output if $w_{ij} \leq 2 \cdot \text{thr}$ for some i. Otherwise, IND = 0.

(iv) The success rate of $\mathcal{D}$ in the distinguishing phase: we analyze the success rate of the algorithm $\mathcal{D}$ in distinguishing the distribution used by the oracle $\mathcal{O}$.

(1) If $\mathcal{O}$ uses the uniform distribution, then $\overline{\mathbf{b}}$, $\overline{\mathbf{z}}$, and $\mathbf{z}$ are uniformly random. $\mathcal{D}$ outputs IND = 1 if $\mathbf{z}_1$ and $\mathbf{z}_2$ produced by the adversary $\mathcal{A}$ satisfy the condition $\|\mathbf{z}_1 \oplus \mathbf{z}_2 \oplus \mathbf{a}_1 \mathbf{E}^*_{m,n,\Delta}[i] \oplus \mathbf{a}_2 \mathbf{E}^*_{m,n,\Delta}[j]\| \leq 2 \cdot \text{thr}$ for some i, j. Since $\mathcal{A}$ did not learn correctly, we can assume that $\mathbf{z}_1$ and $\mathbf{z}_2$ are random, so the event IND = 1 has a nonnegligible probability $\left(\binom{m}{\Delta}^2 / 2^n\right) \sum_{i=0}^{2\cdot\text{thr}} \binom{n}{i}$.

(2) Suppose that $\mathcal{D}$ had access to oracle $\widetilde{\Lambda}_{\tau,m,n}(\mathbf{Y})$. Then $\overline{\mathbf{z}} = \mathbf{bY} \oplus \mathbf{e}$, so $\mathbf{z} = \mathbf{aE}^* \oplus \overline{\mathbf{z}} = \mathbf{aE}^* \oplus \mathbf{bY} \oplus \mathbf{e}$. Thus, $\mathcal{D}$ did simulate the $\mathcal{P}^{\text{sim}}$ correctly in the learning phase of $\mathcal{A}$, so the adversary authenticates to protocol with the nonnegligible probability δ. That means that δ^2 is the probability that for the answers $\mathbf{z}_1, \mathbf{z}_2$ of the adversary produced in Steps (3) and (4) of the oracle distinguishing phase; it holds that $\|\mathbf{z}_1 \oplus \mathbf{a}_1 \mathbf{E}^*_{m,n,\Delta}[i] \oplus \mathbf{bY}\| \leq \text{thr}$, and $\|\mathbf{z}_2 \oplus \mathbf{a}_2 \mathbf{E}^*_{m,n,\Delta}[j] \oplus \mathbf{bY}\| \leq \text{thr}$ for some i, j. Therefore, by the triangle inequality in the Hamming metrics, we get that $w_{ij} = \|\mathbf{z}_1 \oplus \mathbf{z}_2 \oplus \mathbf{a}_1 \mathbf{E}^*_{m,n,\Delta}[i] \oplus \mathbf{a}_2 \mathbf{E}^*_{m,n,\Delta}[j]\| \leq 2 \cdot \text{thr}$, so $\mathcal{D}$ outputs IND = 1.

Thus, depending on whether $\mathcal{D}$ was interacting with the uniform or the $\text{MLPN}_{\tau,m,n}$ oracle, we estimate the difference in probabilities of $\mathcal{D}$ producing IND = 1 as output:

$$\begin{aligned} &\text{Adv}^{\text{MLPN}}_{\mathcal{D}}(\tau, m, n) \\ &= \left| \Pr\left[\mathcal{D}^{\widetilde{\Lambda}_{\tau,m,n}(\mathbf{Y})} \longrightarrow 1 \mid \mathbf{Y} \xleftarrow{\$} \mathbb{Z}_2^{m \times n} \right] \right. \\ &\left. - \Pr\left[\mathcal{D}^{\widetilde{U}_{m+n}} \longrightarrow 1 \right] \right| \geq \delta^2 - \frac{\binom{m}{\Delta}^2 2^{2\cdot\text{thr}}}{2^n} \sum_{i=0}^{} \binom{n}{i}. \end{aligned} \quad (14)$$

Therefore, the distinguisher D is achieving a nonnegligible $\text{MLPN}_{\tau,m,n}$ advantage, which contradicts the hardness assumption of $\text{MLPN}_{\tau,m,n}$ problem. □

6. Security Evaluation in the Restricted Man-in-the-Middle Attacking Scenario

We prove the GRS-MIM security following the technique used in [13].

Lemma 7 (see [13]). *If $\mathbf{X} \in \mathbb{Z}_2^{m \times n}$ is a random matrix, d an integer in the interval $[1, \ldots, \lfloor n/2 \rfloor]$, and H the binary entropy function $H(x) = -x \log_2(x) - (1 - x)\log_2(1 - x)$, then for $y_{\min} = \min_{\mathbf{a} \neq 0, \mathbf{a} \in \mathbb{Z}_2^m} \|\mathbf{aX}\|$ it holds that*

$$\Pr[y_{\min} \leq d] \leq 2^{-(1 - m/n - H(d/n))n}. \quad (15)$$

The previous lemma also holds if $\mathbf{X}$ is a random Toeplitz matrix (Appendix C, [13]).

Theorem 8. *Suppose that there exists an efficient GRS-MIM adversary $\mathcal{A}$ attacking NHB#(τ, thr, m, n) protocol by modifying at most q executions of protocol between the Prover and the Verifier, running in time t and achieving advantage at least δ. Then, under an easily met condition on the parameter set, there is an active adversary $\mathcal{A}'$ attacking NHB#(τ, thr, m, n) interacting at most q times with honest Prover, running in time $O(t)$ and achieving a nonnegligible advantage.*

Proof. The proof consists of the following two parts: (i) specification of the learning phase of an MIM adversary and (ii) evaluation of the advantage which MIM adversary can achieve after the learning phase.

The Learning Phase of MIM Adversary. In order to provide a valid learning phase for the adversary $\mathcal{A}$, the adversary $\mathcal{A}'$ takes the roles of simulated honest Prover and honest Verifier, denoted by $\mathcal{P}^{\text{sim}}$ and $\mathcal{V}^{\text{sim}}$.

The honest Prover $\mathcal{P}$ sends a blinding vector $\mathbf{b}$ to $\mathcal{A}'$, and $\mathcal{A}'$ playing as $\mathcal{P}^{\text{sim}}$ forwards b to $\mathcal{A}$.

$\mathcal{A}'$ playing as $\mathcal{V}^{\text{sim}}$ sends a random vector $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_2^m$ as a challenge to $\mathcal{P}^{\text{sim}}$.

$\mathcal{A}$ modifies $\mathbf{a}$ to $\widehat{\mathbf{a}} = \mathbf{a} \oplus \overline{\mathbf{a}}$ and sends $\widehat{\mathbf{a}}$ to $\mathcal{P}^{\text{sim}}$, and $\mathcal{A}'$ forwards $\widehat{\mathbf{a}}$ to the honest $\mathcal{P}$.

$\mathcal{P}$ returns $\mathbf{z} = \widehat{\mathbf{a}}\mathbf{E}^* \oplus \mathbf{bY} \oplus \mathbf{e}$ to $\mathcal{A}'$.

$\mathcal{A}'$ as $\mathcal{P}^{\text{sim}}$ forwards $\mathbf{z}$ to $\mathcal{V}^{\text{sim}}$.

If $\overline{\mathbf{a}}$ is the all-zero vector, $\mathcal{V}^{\text{sim}}$ sets IND = 1; otherwise IND = 0.

The previous procedure is being repeated in q iterations.

The Advantage of MIM Adversary. We consider that the adversary $\mathcal{A}$ has achieved successful learning if $\mathcal{P}^{\text{sim}}$ and $\mathcal{V}^{\text{sim}}$ were executed correctly in each iteration of the learning phase, that is, if they behaved like honest $\mathcal{P}$ and $\mathcal{V}$.

Since $\mathcal{P}^{\text{sim}}$ forwards directly the responses of honest $\mathcal{P}$ to the received queries, $\mathcal{P}^{\text{sim}}$ works correctly in each simulation step.

On the other hand, the behaviours of the honest $\mathcal{V}$ and $\mathcal{V}^{\text{sim}}$ do not have to match in all circumstances.

This happens in two cases: when $\mathcal{V}^{\text{sim}}$ accepts the response which gets rejected by $\mathcal{V}$, or when $\mathcal{V}^{\text{sim}}$ rejects the response which gets accepted by $\mathcal{V}$.

In the first situation, since $\mathcal{V}^{\text{sim}}$ accepts the response, it means that it is the response of honest $\mathcal{P}$ which is rejected by $\mathcal{V}$, so the probability of this event is equal to the completeness error of the protocol; that is, $\Pr[V^{\text{sim}}(\text{IND} = 1), V(\text{IND} = 0)] = P_{\text{FR}}$.

The second case, when in some iteration $\mathcal{V}^{\text{sim}}$ rejects the response which is accepted by $\mathcal{V}$, means that it is the response $\widehat{\mathbf{z}}$ where $\overline{\mathbf{a}}$ is not all-zero, but still this response gets accepted by honest $\mathcal{V}$.

The probability of this acceptance is the probability that the following holds for some i (where $\mathbf{E}^*[i] = \mathbf{E}^*_{m,n,\Delta}[i]$):

$$\left\|\hat{\mathbf{z}} \oplus \mathbf{a}\mathbf{E}^*[i] \oplus \mathbf{b}\mathbf{Y}\right\| \leq \text{thr}. \tag{16}$$

That is, $\|\hat{\mathbf{z}} + \mathbf{a}\mathbf{E}^*[i] + \mathbf{b}\mathbf{Y}\| = \|\mathbf{a}\mathbf{E}^*[i] + \bar{\mathbf{a}}\mathbf{E}^*[i] + \mathbf{b}\mathbf{Y} + \mathbf{e} + \mathbf{a}\mathbf{E}^*[i] + \mathbf{b}\mathbf{Y}\| = \|\bar{\mathbf{a}}\mathbf{E}^*[i] \oplus \mathbf{e}\| \leq \text{thr}$.

Let us denote by $\mathbf{y}_{\bar{\mathbf{a}}}$ the vector $\bar{\mathbf{a}}\mathbf{X} \oplus \beta$. Then in vector $\mathbf{y}_{\bar{\mathbf{a}}} \oplus \mathbf{e}$, $(n - \|y_{\bar{a}}\|)$ bits follow the distribution Ber^n_τ, and the rest $\|y_{\bar{a}}\|$ follow the distribution $\text{Ber}^n_{1-\tau}$. Therefore $\mu(\|y_{\bar{a}}\|) = E(\|\mathbf{y}_{\bar{\mathbf{a}}} \oplus \mathbf{e}\|) = \|y_{\bar{a}}\|(1 - \tau) + (n - \|\mathbf{y}_{\bar{\mathbf{a}}}\|)\tau$. Since μ is a linear function of $\|\mathbf{y}_{\bar{\mathbf{a}}}\|$, it holds that $\mu \geq \text{thr}$ for each $\|y_{\bar{a}}\| \geq x_0$, where $x_0 = 1 + \lfloor(\text{thr} - \tau n)/(1 - 2\tau)\rfloor$.

Therefore, according to Chernoff bound, event $\|\mathbf{y}_{\bar{\mathbf{a}}} \oplus \mathbf{e}\| \leq \text{thr}$ has the probability at most $e^{-(\mu-\text{thr})^2}/2\mu$ when $\|\mathbf{y}_{\bar{\mathbf{a}}}\| \geq d$, for each $d \geq x_0$.

Suppose that $y_{\min} = \min_{\bar{\mathbf{a}}\neq 0, \bar{\mathbf{a}} \in \mathbb{Z}_2^m} \|\bar{\mathbf{a}}\mathbf{E}^*_{m,n,\Delta}[i]\|$.

Let FAIL denote the event $V^{\text{sim}}(\text{IND} = 0),\ V(\text{IND} = 1)$. Therefore for each $d \geq x_0$ it holds

$$\begin{aligned}
\Pr_{\mathbf{E}^*[i],\mathbf{e}}[\text{FAIL}] &= \Pr_{\mathbf{e}}\left[\text{FAIL} \mid y_{\min} > d\right] \cdot \Pr_{\mathbf{E}^*[i]}\left[y_{\min} > d\right] \\
&\quad + \Pr_{\mathbf{e}}\left[\text{FAIL} \mid y_{\min} \leq d\right] \\
&\quad \cdot \Pr_{\mathbf{E}^*[i]}\left[y_{\min} \leq d\right] \\
&\leq \Pr_{\mathbf{e}}\left[\text{FAIL} \mid y_{\min} > d\right] + \Pr_{\mathbf{E}^*[i]}\left[y_{\min} \leq d\right] \qquad (17) \\
&= \Pr_{\mathbf{e}}\left[\left\|\mathbf{y}_{\bar{\mathbf{a}}} \oplus \mathbf{e}\right\| \leq \text{thr} \mid y_{\min} > d\right] \\
&\quad + \Pr_{\mathbf{E}^*[i]}\left[y_{\min} \leq d\right] \\
&\leq e^{-(\mu-\text{thr})^2/2\mu} + 2^{-(1-m/n-H(d/n))n}.
\end{aligned}$$

Suppose that $k > 0$ is some positive constant, and x_0 is the least integer such that $\mu > (1 + k)\text{thr}$ for $\|\mathbf{y}_{\bar{\mathbf{a}}}\| \geq x_0$. Then, for all $d \geq x_0$, when $y_{\min} > d$, we have $e^{-(\mu-\text{thr})^2/2\mu} \leq e^{-\text{thr}\cdot k^2/2(1+k)}$, so the first term in the upper bound is negligible.

In order that the second term also gets negligible, we choose $d \geq x_0$ such that $1 - m/n - H(d/n)$ is always positive; that is, $H(d/n) < 1 - m/n$ (that condition is easily met for the usual parameter values [13]).

Therefore, we have that the probability of incorrect simulation in a single iteration is

$$\begin{aligned}
p_r &= \Pr\left[V^{\text{sim}}(\text{IND} = 1), V(\text{IND} = 0)\right] \\
&\quad + \Pr\left[V(\text{IND} = 0), V^{\text{sim}}(\text{IND} = 1)\right] \qquad (18) \\
&\leq P_{\text{FR}} + e^{-(\mu-\text{thr})^2/2\mu} + 2^{-(1-m/n-H(d/n))n}.
\end{aligned}$$

Thus, the probability that all q iterations are correct, that is, that the learning phase is successfully conducted, is $(1 - p_r)^q$, which has the asymptotic value of 1.

We conclude that the advantage of the active adversary $\mathcal{A}'$ attacking NHB#(τ, thr, m, n) is $\delta' = \delta(1 - p_r)^q$, which is a nonnegligible value, so this contradicts the active security of that protocol. □

7. A Concluding Discussion

This paper proposes an authentication protocol with asymmetric implementation complexity which is suitable for authentication of a Prover with low computational capabilities to a Verifier with high performance computational capabilities. The protocol is based on a trade-off between the execution overheads at Prover and Verifier: more computational efforts are required at the side of Verifier in order to maintain the desired level of the authentication security.

The proposed protocol originates from HB# protocol [13], but it provides reduction of the required secret key dimension to the half of the one required in HB# protocol. Reduction of the required secret key dimension and the asymmetric computational overheads at Prover and Verifier appear as a consequence of employment the random selection paradigm. Security of the proposed authentication protocol results from joint employment of the LPN problem and random selection paradigms. In this paper, security of the proposed authentication protocol has been proved in active attacking and restrictive MIM (so called GRS-MIM) attacking scenarios. We conjecture that protocol could achieve security in MIM attacking scenarios stronger than GRS-MIM, and this is one of the directions for the related future work.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

The Ministry of Education, Science and Technological Development, Serbia, has partially funded this work.

References

[1] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, 2006.

[2] S. Piramuthu, "Lightweight cryptographic authentication in passive RFID-Tagged systems," *IEEE Transactions on Systems, Man and Cybernetics—Part C: Applications and Reviews*, vol. 38, no. 3, pp. 360–376, 2008.

[3] J. L. Hernandez-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a lightweight authentication and authorization framework for smart objects," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 4, pp. 690–702, 2015.

[4] I. Ratković, N. Bežanić, O. S. Ünsal, A. Cristal, and V. Milutinović, "An overview of architecture-level power- and energy-efficient design techniques," *Advances in Computers*, vol. 98, pp. 1–57, 2015.

[5] N. J. Hopper and M. Blum, "Secure human identification protocols," in *Advances in Cryptology—ASIACRYPT 2001*, C. Boyd, Ed., vol. 2248 of *Lecture Notes in Computer Science*, pp. 52–66, Springer, Heidelberg, Germany, 2001.

[6] E. R. Berlekamp, R. J. McEliece, and H. C. van Tilborg, "On the inherent intractability of certain coding problems," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. IT-24, no. 3, pp. 384–386, 1978.

[7] A. Juels and S. A. Weis, "Authenticating pervasive devices with human protocols," in *Advances in Cryptology—CRYPTO 2005*, V. Shoup, Ed., vol. 3621 of *Lecture Notes in Computer Science*, pp. 293–308, Springer, Heidelberg, Germany, 2005.

[8] J. Katz and J. S. Shin, "Parallel and concurrent security of the HB and HB$^+$ protocols," in *Advances in Cryptology—EUROCRYPT 2006*, S. Vaudenay, Ed., vol. 4004 of *Lecture Notes in Computer Science*, pp. 73–87, Springer, Heidelberg, Germany, 2006.

[9] J. Katz, J. S. Shin, and A. Smith, "Parallel and concurrent security of the HB and HB$^+$ protocols," *Journal of Cryptology*, vol. 23, no. 3, pp. 402–421, 2010.

[10] H. Gilbert, M. Robshaw, and H. Sibert, "Active attack against HB+: a provably secure lightweight authentication protocol," *Electronics Letters*, vol. 41, no. 21, pp. 1169–1170, 2005.

[11] J. Munilla and A. Peinado, "HB-MP: a further step in the HB-family of lightweight authentication protocols," *Computer Networks*, vol. 51, no. 9, pp. 2262–2267, 2007.

[12] J. Bringer and H. Chabanne, "Trusted-HB: a low-cost version of HB+ secure against man-in-the-middle attacks," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4339–4342, 2008.

[13] H. Gilbert, M. J. B. Robshaw, and Y. Seurin, "HB$^\#$: increasing the security and efficiency of HB$^+$," in *Advances in Cryptology—EUROCRYPT 2008*, N. Smart, Ed., vol. 4965 of *Lecture Notes in Computer Science*, pp. 361–378, Springer, Heidelberg, Germany, 2008.

[14] K. Ouafi, R. Overbeck, and S. Vaudenay, "On the security of HB$^\#$ against a man-in-the-middle attack," in *Advances in Cryptology—ASIACRYPT 2008*, J. Pieprzyk, Ed., vol. 5350 of *Lecture Notes in Computer Science*, pp. 108–124, Springer, Heidelberg, Germany, 2008.

[15] E. Kiltz, K. Pietrzak, D. Cash, A. Jain, and D. Venturi, "Efficient authentication from hard learning problems," in *Advances in Cryptology—EUROCRYPT 2011*, K. G. Paterson, Ed., vol. 6632 of *Lecture Notes in Computer Science*, pp. 7–26, Springer, Heidelberg, Germany, 2011.

[16] E. Kosei and N. Kunihiro, "On the security proof of an authentication protocol from Eurocrypt 2011," in *Advances in Information and Computer Security*, M. Yoshida and K. Mouri, Eds., vol. 8639 of *Lecture Notes in Computer Science*, pp. 187–203, Springer, Heidelberg, Germany, 2014.

[17] J. Cichoń, M. Klonowski, and M. Kutyłowski, "Privacy protection for RFID with hidden subset identifiers," in *Pervasive Computing*, J. Indulska, D. J. Patterson, T. Rodden, and M. Ott, Eds., vol. 5013 of *Lecture Notes in Computer Science*, pp. 298–314, 2008.

[18] Z. Gołębiewski, K. Majcher, and F. Zagórski, "Attacks on CKK family of RFID authentication protocols," in *Ad-Hoc, Mobile and Wireless Networks*, D. Coudert, D. Simplot-Ryl, and I. Stojmenovic, Eds., vol. 5198 of *Lecture Notes in Computer Science*, pp. 241–250, 2008.

[19] M. Krause and M. Hamann, "The cryptographic power of random selection," in *Selected Areas in Cryptography, SAC 2011*, vol. 7118 of *Lecture Notes in Computer Science*, pp. 134–150, Springer, New York, NY, USA, 2012.

[20] V. Lyubashevsky and D. Masny, "Man-in-the-middle secure authentication schemes from LPN and weak PRFs," in *Advances in Cryptology—CRYPTO 2013*, R. Canetti and J. A. Garay, Eds., vol. 8043 of *Lecture Notes in Computer Science*, pp. 308–325, Springer, Heidelberg, Germany, 2013.