mathematics

MDPI

Article

Analysis and Correction of the Attack against the LPN-Problem Based Authentication Protocols

Siniša Tomović [1,2,*] and Milica Knežević [1,2] and Miodrag J. Mihaljević [1]

[1] Mathematical Institute of the Serbian Academy of Sciences and Arts, Kneza Mihaila 36, 11000 Belgrade, Serbia; mknezevic@mi.sanu.ac.rs (M.K.); miodragm@turing.mi.sanu.ac.rs (M.J.M.)
[2] Faculty of Technical Sciences, University of Novi Sad, Trg Dositeja Obradovića 6, 21000 Novi Sad, Serbia
* Correspondence: sinisatom@mi.sanu.ac.rs

Abstract: This paper reconsiders a powerful man-in-the-middle attack against Random-HB# and HB# authentication protocols, two prominent representatives of the HB family of protocols, which are built based on the Learning Parity in Noise (LPN) problem. A recent empirical report pointed out that the attack does not meet the claimed precision and complexity. Performing a thorough theoretical and numerical re-evaluation of the attack, in this paper we identify the root cause of the detected problem, which lies in reasoning based on approximate probability distributions of the central attack events, that can not provide the required precision due to the inherent limitations in the use of the Central Limit Theorem for this particular application. We rectify the attack by employing adequate Bayesian reasoning, after establishing the exact distributions of these events, and overcome the mentioned limitations. We further experimentally confirm the correctness of the rectified attack and show that it satisfies the required, targeted accuracy and efficiency, unlike the original attack.

Keywords: lightweight cryptography; authentication; HB-family; man-in-the-middle attack; cryptanalysis; Poisson-binomial distribution; LPN problem

Citation: Tomović, S.; Knežević, M.; Mihaljević, M.J. Analysis and Correction of the Attack against the LPN-Problem Based Authentication Protocols. *Mathematics* **2021**, *9*, 573. https://doi.org/10.3390/math9050573

Received: 4 February 2021
Accepted: 4 March 2021
Published: 8 March 2021

1. Introduction

The construction of lightweight and secure authentication protocols for RFID (Radio Frequency IDentification) devices is an important task of contemporary cryptography. These devices are employed in supply-chain management, payment and transportation systems, for the tracking of goods and other applications, and are rapidly becoming one of the most pervasive technologies. An RFID system usually consists of two entities—a resource-constrained Tag attached to a physical object and a more computationally powerful Reader, which communicate using authentication protocol in order to validate Tag by the Reader. Reaching high security requirements for such validation while minimizing its resources cost is a very active research area [1–3]. One of the important families of authentication protocols for RFID systems is the HB family.

The HB family originates from a lightweight protocol called HB that was proposed by Hopper and Blum [4] and is built over the hardness of the Learning Parity in Noise (LPN) problem. Informally, the LPN problem could be considered as a problem of solving an overdefined system of consistent linear equations over GF(2), the field with two elements, where certain equations are available only in a corrupted form. While the HB protocol resists passive (eavesdropping) attacks, it is shown to be vulnerable against an active adversary who can impersonate a reader and interact with legitimate tags. A modified protocol named HB+ [5,6] was proposed with the aim of addressing this weakness. Soon after, it was shown that the HB+ protocol is defenseless against a stronger adversary who can modify the messages sent by the reader [7]. This attack is known as the GRS man-in-the-middle (MIM) attack. In order to avoid the GRS-MIM attack, different protocol variants were proposed (see, for example, HB++ [8] and HB-MP [9]). However, they were shown to be vulnerable [10], until the HB# and Random-HB# protocols were introduced in [11] and

proven to be secure against GRS-MIM. Shortly thereafter, Ouafi, Overback and Vaudenay proposed a more general MIM attack (OOV, by authors' initials) [12] against HB# and Random-HB#. The attack implies an adversary that can modify the messages exchanged in both directions between the tag and the reader. Moreover, OOV can be regarded as a generic attack against the HB-family. The OOV attack remains one of the keystones in the analysis of HB-like authentication schemes and it is recognized as essential in the security evaluation of any novel HB-like protocol [1].

Some other HB-protocol variants are: HB-MP+ [13], HB-MP++ [14], HB-MP* [15], Trusted-HB [16], NLHB [17], HB^N [18], GHB# [19], HB+PUF [20], PUF-HB [21], and Tree-LSHB [22,23]. However, many of these HB-family protocols have been shown to be vulnerable against several cryptanalysis techniques and MIM attacks [1,7,10,12]. For a detailed overview of the HB-protocols and analysis based on their efficiency and resistance against attacks, see, for example, [24].

Motivation for the work. Recent results presented in [25] showed that the OOV attack is significantly less successful than it was claimed in [12] and pointed out malfunctioning in the core component of the attack. The estimated complexity of the attack is 18% higher for HB# and 55% for Random-HB# than the claimed, in the case of the standard parameter set II. This is a significant increase having in mind the overall complexity and time consumption of the attack, which is claimed to be $2^{29.4}$ for Random-HB#, and 2^{21} for HB#. In this paper, we continue on this investigation path and revise the theoretical and numerical analysis behind the attack provided in [12], in order to determine the cause of the mentioned problem and try to solve it, if possible.

Summary of the results. This paper revises the cryptanalysis from [12] providing proof and explaining why the approximations of the probability distributions employed in the core component of the attack are inappropriate in the considered context, which results in lower precision and higher complexity of the OOV attack [12]. Further, this paper provides a derivation of the correct probability distributions on the number of successful authentications that leaks secret information, which can be used to recover secret keys. Finally, a correction of the OOV attack is proposed, which uses the derived, correct probability distributions, satisfying the targeted performances/complexity.

Organization of the work. Section 2 provides background on the HB# and Random-HB# protocols and the OOV attack. Section 3 brings a thorough revision of theoretical analysis behind the OOV attack and points to the critical omissions in it. Section 4 introduces the corrected attack and analyze its performance. Section 5 provides results of experimental analysis. In Section 6, the findings and results presented in the paper are briefly summarized.

2. Preliminaries

A list containing notation used throughout the remainder of the paper is given below.

- Variables are denoted with normal, bold or capital bold letters (e.g., x, $\mathbf{x}$ and $\mathbf{X}$) if they represent single elements, vectors, or matrices, respectively
- $\mathbb{Z}_2^m$: set of all m-dimensional binary vectors
- $\mathbb{Z}_2^{k\times m}$: set of all $k \times m$-dimensional binary matrices
- $\mathbf{x}_i$: i-th element of binary vector $\mathbf{x}$
- $\mathbf{1}_i$: binary vector with all zeros, except on the position i
- $\mathbf{x} \oplus \mathbf{y}$: bitwise XOR operation of two binary vectors $\mathbf{x}$ and $\mathbf{y}$
- $\|\mathbf{x}\|$: the Hamming weight of binary vector $\mathbf{x}$ (sum of its elements)
- $x \xleftarrow{\$} X$: sampling a value x which follows uniform distribution over a finite set X
- $Pr[A]$: probability of an event A
- Ber_τ: Bernoulli distribution with parameter τ. $x \leftarrow Ber_\tau$ is sampling of value x such that $P(x = 1) = \tau$, $P(x = 0) = 1 - \tau$
- $Bin(n, p)$: Binomial distribution of n experiments with success probability p of each experiment
- $\mathbf{e} \leftarrow Ber_\tau^m$: sampling binary vector $\mathbf{e} \in \mathbb{Z}_2^m$ such that $\mathbf{e}_i \leftarrow Ber_\tau, i = 1, \ldots, m$

- $\mathcal{N}(\mu, \sigma^2)$: Normal distribution with mean μ and variance σ^2
- $\Phi(x)$: standard normal cumulative distribution function
- $erfc(x) = 2\Phi(-x\sqrt{2})$: complementary error function
- $X_n \xrightarrow{\mathcal{D}} \mathcal{X}$: sequence of random variables $X_1, X_2, \ldots X_n$ converges weakly (in distribution) to a distribution $\mathcal{X}$ as $n \to \infty$
- $P(\bar{w})$: probability of acceptance during the OOV attack when the Adversary adds noise vector $\bar{\mathbf{e}}, \|\bar{\mathbf{e}}\| = \bar{w}$ to a regular noise vector $\mathbf{e}$ in a protocol session, that is, $P(\bar{w}) = Pr[\|\mathbf{e} \oplus \bar{\mathbf{e}}\| \leq thr]$
- $P_{OOV}(\bar{w}) := \Phi(\frac{thr-(m-\|\bar{e}\|)\tau-\|\bar{e}\|(1-\tau)}{\sqrt{m\tau(1-\tau)}})$: approximation of $P(\bar{w})$ used in the OOV attack [12].

The HB family of authentication protocols has attracted a lot of attention because of their simple implementations and the provable security based on the well-known hard problem—Learning Parity with Noise (LPN). Random-HB# and HB# are prominent representatives of this family. Their authentication procedure consists of the following steps [11]—first, the Tag sends a random blinding vector $\mathbf{b}$ to the Reader to initiate the authentication and the Reader responds with a random challenge vector $\mathbf{a}$ to the Tag. Then Tag sends $\mathbf{z} = \mathbf{aX} \oplus \mathbf{bY} \oplus \mathbf{e}$ to the Reader, where $\mathbf{e}$ is a noise vector whose bits independently follow Bernoulli distribution with coefficient τ, and $\mathbf{X} \in \mathbb{Z}_2^{k_X \times m}, \mathbf{Y} \in \mathbb{Z}_2^{k_Y \times m}$ are their shared secret keys (random matrices for Random-HB# and so-called Toeplitz matrices for HB#). The Reader validates the Tag, that is, accepts its response, if and only if the Hamming weight $\|\mathbf{aX} \oplus \mathbf{bY} \oplus \mathbf{z}\|$ falls under a certain threshold value (see Figure 1). Standard parameters' values for these protocols are given in Table 1.

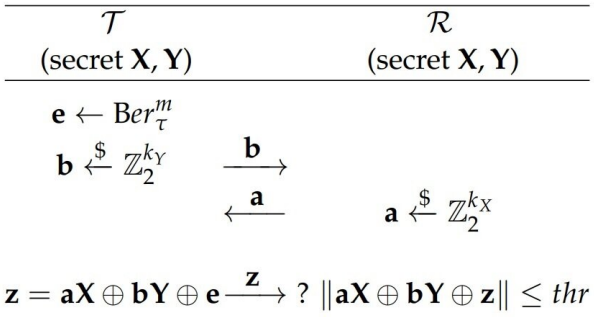


Figure 1. Random-HB# and HB# authentication protocols.

Table 1. Standard parameter sets I and II for HB# and Random-HB# proposed in [11]. Number l of secret bits is $(k_x + k_y)m$ for Random-HB#, while it is $k_x + k_y + 2m - 2$ for HB#.

Parameter Set	k_x	k_y	m	τ	thr
I	80	512	1164	0.25	405
II	80	512	441	0.125	113

The mechanism of the OOV attack proposed in [12] is shown in Figure 2. The adversary:

1. Collects a triplet $(\bar{\mathbf{a}}, \bar{\mathbf{b}}, \bar{\mathbf{z}} = \bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} \oplus \bar{\mathbf{e}})$ of messages exchanged between the Tag and the Reader by eavesdropping one of their communication sessions
2. Replaces each triplet $(\mathbf{a}, \mathbf{b}, \mathbf{z})$ of messages between the Tag and the Reader during n following communication sessions with a triplet $(\mathbf{a} \oplus \bar{\mathbf{a}}, \mathbf{b} \oplus \bar{\mathbf{b}}, \mathbf{z} \oplus \bar{\mathbf{z}})$
3. Counts the number c of "ACCEPT" decisions of the Reader at the end of those n sessions.

$\mathcal{T}$ (secret $\mathbf{X}, \mathbf{Y}$)	$\mathcal{A}$ triplet $(\bar{\mathbf{a}}, \bar{\mathbf{b}}, \bar{\mathbf{z}})$	$\mathcal{R}$ (secret $\mathbf{X}, \mathbf{Y}$)
$\mathbf{e} \leftarrow Ber_{\tau}^{m}$		
$\mathbf{b} \xleftarrow{\$} \mathbb{Z}_2^{k_Y}$	$\xrightarrow{\hat{\mathbf{b}} = \mathbf{b} \oplus \bar{\mathbf{b}}}$	
	$\xleftarrow{\hat{\mathbf{a}} = \mathbf{a} \oplus \bar{\mathbf{a}}}$	$\mathbf{a} \xleftarrow{\$} \mathbb{Z}_2^{k_X}$
$\mathbf{z} = \hat{\mathbf{a}}\mathbf{X} \oplus \mathbf{b}\mathbf{Y} \oplus \mathbf{e}$	$\xrightarrow{\hat{\mathbf{z}} = \mathbf{z} \oplus \bar{\mathbf{z}}}$	$? \ \|\mathbf{a}\mathbf{X} \oplus \hat{\mathbf{b}}\mathbf{Y} \oplus \hat{\mathbf{z}}\| \leq thr$

Figure 2. The OOV attack against Random-HB# and HB#.

The acceptance rate $\frac{c}{n}$, as it turns out, leaks the critical information which reveals the secret values. More precisely, the theoretical analysis from [12] shows that:

$$\frac{c}{n} \approx \Phi\left(\frac{thr - (m - \|\bar{\mathbf{e}}\|)\tau - \|\bar{\mathbf{e}}\|(1-\tau)}{\sqrt{m\tau(1-\tau)}}\right),$$

where Φ is the standard normal cumulative distribution function. This formula allows the adversary to estimate the Hamming weight $\|\bar{\mathbf{e}}\|$ using solely the empirical value $\frac{c}{n}$, for n large enough (Algorithm 1 from [12]).

After the adversary discovers the Hamming weight of the noise vector $\bar{\mathbf{e}}$, he can reconstruct the vector by flipping its bits (more precisely, he flips $\bar{\mathbf{z}} = \bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} \oplus \bar{\mathbf{e}}$ which secretly contains $\bar{\mathbf{e}}$) and measures weight of $\bar{\mathbf{e}}$ after the flipping. If the weight has increased, the flipped bit was 0, otherwise, it was 1. This way, he reconstructs the noise vector $\bar{\mathbf{e}}$ and obtains the linear combination $\bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y}$ since $\bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} = \bar{\mathbf{z}} \oplus \bar{\mathbf{e}}$ (Algorithm 2 from [12]). The whole previous procedure is repeated also for other modification triplets $(\bar{\mathbf{a}}_\mathbf{i}, \bar{\mathbf{b}}_\mathbf{i}, \bar{\mathbf{z}}_\mathbf{i} = \bar{\mathbf{a}}_\mathbf{i}\mathbf{X} \oplus \bar{\mathbf{b}}_\mathbf{i}\mathbf{Y} \oplus \bar{\mathbf{e}}_\mathbf{i})$ obtained by eavesdropping, until the adversary collects enough of these linear combinations $\bar{\mathbf{a}}_\mathbf{i}\mathbf{X} \oplus \bar{\mathbf{b}}_\mathbf{i}\mathbf{Y} = \bar{\mathbf{z}}_\mathbf{i} \oplus \bar{\mathbf{e}}_\mathbf{i}$ to form a full system of linear equations. The secret keys $\mathbf{X}$ and $\mathbf{Y}$ are then recovered as the solution to this system.

As illustrated above, in each corrupted communication session, the Reader computes:

$$\begin{aligned} \|\mathbf{a}\mathbf{X} \oplus \hat{\mathbf{b}}\mathbf{Y} \oplus \hat{\mathbf{z}}\| &= \|\mathbf{a}\mathbf{X} \oplus (\mathbf{b} \oplus \bar{\mathbf{b}})\mathbf{Y} \oplus (\mathbf{z} \oplus \bar{\mathbf{z}})\| \\ &= \|(\mathbf{a}\mathbf{X} \oplus \mathbf{b}\mathbf{Y} \oplus \mathbf{z}) \oplus (\bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} \oplus \bar{\mathbf{z}})\| \\ &= \|\mathbf{e} \oplus \bar{\mathbf{e}}\| \end{aligned}$$

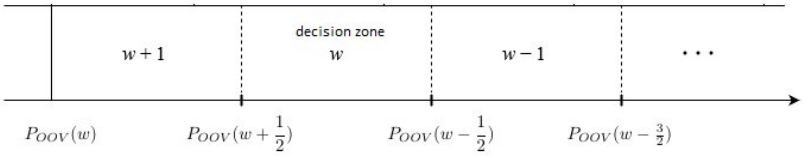
and the Tag successfully authenticates iff $\|\mathbf{e} \oplus \bar{\mathbf{e}}\| \leq thr$, whereas in a regular session, the Tag successfully authenticates iff $\|\mathbf{e}\| \leq thr$. This way, by creating the cumulative noise $\mathbf{e} \oplus \bar{\mathbf{e}}$, the adversary manipulates the verification criterion of the Reader and changes its theoretical acceptance rate from $Pr[\|\mathbf{e}\| \leq thr]$ to $P(\bar{w}) := Pr[\|\mathbf{e} \oplus \bar{\mathbf{e}}\| \leq thr] \approx \Phi\left(\frac{thr-(m-\|\bar{e}\|)\tau-\|\bar{e}\|(1-\tau)}{\sqrt{m\tau(1-\tau)}}\right)$.

Let us provide a simple and useful characterization of the OOV attack Algorithm 1 [12] output by introducing the notion of "decision zones."

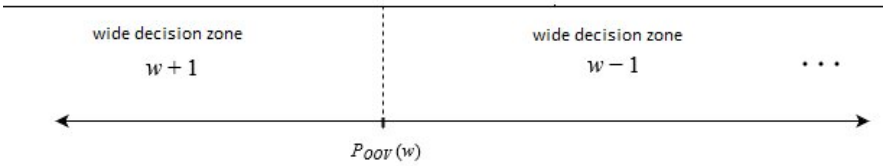
Definition 1. *("OOV decision zones"). OOV $\bar{w}$-decision zone is an interval $I_{\bar{w}}^{OOV}$ such that OOV Algorithm 1 estimates $\|\bar{\mathbf{e}}\|$ as $\bar{w}$ iff $\frac{c}{n} \in I_{\bar{w}}^{OOV}$.*

After eavesdropping a triplet, the adversary considers all weights of the noise vector $\bar{\mathbf{e}}$ possible. He decides that $\|\bar{\mathbf{e}}\|$ is $\bar{w} \iff \bar{w} - \frac{1}{2} \leq P_{OOV}^{-1}(\frac{c}{n}) < \bar{w} + \frac{1}{2} \iff \frac{c}{n} \in I_{\bar{w}}^{OOV} = (P_{OOV}(\bar{w} + \frac{1}{2}), P_{OOV}(\bar{w} - \frac{1}{2})]$, since P is a monotone decreasing function (see Figure 3a).

After flipping a bit in the noise vector, whose weight is previously estimated as $\bar{w}$, the adversary considers only two weights possible: $\bar{w} - 1$ and $\bar{w} + 1$, so there are two decision zones — $I_{\bar{w}-1}^{OOV} = (P_{OOV}(\bar{w}), \infty)$ and $I_{\bar{w}+1}^{OOV} = (-\infty, P_{OOV}(\bar{w})]$ (see Figure 3b).



(**a**) After eavesdropping



(**b**) After flipping a bit

Figure 3. Decision making of the OOV attack Algorithm 1.

In [12], the complexity of the OOV attack is estimated as an overall number of modified authentication sessions, which is minimized if the expected noise vector weight w_{exp} coincides with the so-called *optimal weight* when it is polynomial (for weights not near enough the optimal one, it becomes exponential). To achieve this, different strategies are introduced in [12], such as flipping the adequate number of last bits when $w_{exp} \leq w_{opt}$ before weight measurement, or removing the already recovered 1-bits when $w_{exp} \geq w_{opt}$.

Also, ref [12] provides an optimized version of the attack which uses flipping block-by-block in the noise vector recovery process instead of bit-by-bit. However, it is observed empirically in [25] that the actual benefit that this optimized version brings is somewhat overestimated. An explanation was offered that it uses insufficient sample sizes for decision making when measuring the weights, which are further away from the optimal one.

3. Revision of the OOV Attack

The previous work [25] has shown that the OOV attack predominantly incorrectly estimates weights of noise vectors. The probability of key recovery, that is, efficiency of the attack, is shown to be significantly lower compared to the values claimed in [12]. For the standard parameter set II, the probability of correct key recovery is shown to be 0.158 in the case of HB# and 10^{-7} in the case of Random-HB#. The analysis presented in [25] reveals that, in order to achieve the precision of key recovery claimed in [12], it is necessary to increase the number of intercepted authentications by 18% in the case of HB# and by 55% in the case of Random-HB#. Since the number of intercepted authentication sessions is the unit of the attack complexity, the complexity increases accordingly. Furthermore, the analysis from [25] shows that the weight estimation error cannot be corrected by taking a larger "sample" n, i.e., larger number of intercepted authentication sessions. On the contrary, by increasing the sample, the quality of the weight estimate worsens. So, for example, experimental evaluation on the standard parameter set II shows that the percentage of correctly estimated weights is only 5%, even if a very large number of modifications is used (for more details, see Section 4.4 in [25]).

This has led us to conduct a thorough revision of cryptanalysis from [12], which we provide in this Section. We shall prove that the attack's erroneous output is caused by inadequate, non-Bayesian inference over improper, approximate probability distributions of acceptance rates, which cannot be improved due to Central limit theorem application limitations for these protocols. We identify the exact distributions and the exact error of the approximations from [12]. Then we employ Bayesian reasoning over the exact distributions to construct proper decision zones, and show how OOV weight decision making proposed in [12] deviates significantly from the proper, Bayesian one.

3.1. Revision of the Theoretical Analysis behind the OOV Weight Estimate

Here, we revise the derivation of approximations of acceptance rates used in the OOV weight estimate process and report their significant imprecision. Specifically, this derivation is given in the "Correctness" paragraph, Section 2.1 in [12].

3.1.1. Incorrect Claim that Cumulative Noise Vector $\mathbf{e} \oplus \bar{\mathbf{e}}$ Follows Binomial Distribution

The mentioned paragraph begins with calculation of the probability that i-th bit of cumulative noise vector $\mathbf{e} \oplus \bar{\mathbf{e}}$ is 1:

$$Pr[(\mathbf{e} \oplus \bar{\mathbf{e}})_\mathbf{i} = 1] = \begin{cases} \tau, \bar{\mathbf{e}}_\mathbf{i} = 0 \\ 1 - \tau, \bar{\mathbf{e}}_\mathbf{i} = 1 \end{cases}$$

Then it says (exact quotation): "Hence, $m - \bar{w}$ bits of $\mathbf{e} \oplus \bar{\mathbf{e}}$ follow a Bernoulli distribution of parameter τ and the other $\bar{w}$ bits follow a Bernoulli distribution of parameter $1 - \tau$, **thus** $\|\mathbf{e} \oplus \bar{\mathbf{e}}\|$ follows a binomial distribution." [12].

However, that is not correct: $\|\mathbf{e} \oplus \bar{\mathbf{e}}\|$ does not follow binomial distribution, because that is by definition a distribution of sum of independent and *identically distributed* Bernoulli trials i.e., of *the same* parameter (probability of success). Here, the Hamming weight of cumulative noise $\|\mathbf{e} \oplus \bar{\mathbf{e}}\| = \sum_{i=1}^{m} (\mathbf{e} \oplus \bar{\mathbf{e}})_\mathbf{i}$, as we can see, is a sum of Bernoulli trials of mixed parameter values τ or $1 - \tau$ and actually corresponds to a more general so-called *Poisson-Binomial Distribution*. We elaborate more on this distribution in the upcoming Section 3.2.

3.1.2. Approximation of Acceptance Rates $P(\bar{w}) \approx P_{OOV}(\bar{w})$ without Error Estimation

The "Correctness" paragraph [12] continues with the calculations of the expected weight of the vector $\mathbf{e} \oplus \bar{\mathbf{e}}$ as $\mu = E(\|\mathbf{e} \oplus \bar{\mathbf{e}}\|) = \bar{w}(1 - \tau) + (m - \bar{w})\tau$ and its variance $\sigma^2 = Var(\|\mathbf{e} \oplus \bar{\mathbf{e}}\|) = m\tau(1 - \tau)$, which are correct, and derives approximation of acceptance rate during the attack:

$$P(\bar{w}) = Pr[\|\mathbf{e} \oplus \bar{\mathbf{e}}\| \leq thr] \approx \Phi\left(\frac{thr - (m - \bar{w})\tau - \bar{w}(1 - \tau)}{\sqrt{m\tau(1 - \tau)}}\right), \tag{1}$$

where Φ is the standard normal cumulative distribution function, by referring to the Central Limit Theorem (CLT)—Formula (1) in [12].

Here, ref [12] applies CLT to sum $\|\mathbf{e} \oplus \bar{\mathbf{e}}\|$ without discussing the magnitude of error of this approximation—the theorem itself only points to its convergence when $m \to \infty$.

3.1.3. Unknown Error Bound of the Weight Estimate Process

In the rest of the "Correctness" paragraph [12], the authors merge previous approximation (1) with the second one (which is a consequence of the Law of large numbers):

$$\frac{c}{n} \approx P(\bar{w}) \tag{2}$$

to conclude that:

$$\frac{c}{n} \approx \Phi\left(\frac{thr - (m - \bar{w})\tau - \bar{w}(1 - \tau)}{\sqrt{m\tau(1 - \tau)}}\right) =: P_{OOV}(\bar{w}). \tag{3}$$

The idea behind the merging of the two approximations can be explained in the following way: c/n converges to $P(\bar{w})$ when $n \to \infty$ (by the Law of large numbers), while $|P_{OOV}(\bar{w}) - P(\bar{w})|$ converges to 0 when $m \to \infty$ (by the Central Limit Theorem). Thus, c/n gets arbitrarily close to $P_{OOV}(\bar{w})$, if both n and m are large enough. This can be represented as:

$$\frac{c}{n} \xrightarrow[n \to \infty]{\text{Law of large numbers}} P(\bar{w}) \xleftarrow[m \to \infty]{\text{CLT}} P_{OOV}(\bar{w}) \implies \frac{c}{n} \approx P_{OOV}(\bar{w}).$$

Unlike $P(\bar{w}) \approx P_{OOV}(\bar{w})$, ref [12] actually does derive error for $\frac{c}{n} \approx P(\bar{w})$ approximation, and how large n should be in order to make the error negligible:

$\frac{c}{n} \in (P(\bar{w}) - |rP'(\bar{w})|, P(\bar{w}) + |rP'(\bar{w})|)$ with probability $1 - erfc(\theta)$ for $n(r, \bar{w}) = \frac{\theta^2}{r^2} R(\bar{w})$ (Formula (2) in [12]) where $erfc(\theta)$ gets exponentially small as θ (i.e., n) increases asymptotically. Therefore, $\frac{c}{n}$ is used to estimate $P(\bar{w})$ for n large enough.

However, as the final approximation (3) contains estimate $P(\bar{w}) \approx P_{OOV}(\bar{w})$ whose error was not assessed in [12], its error is also unknown. The bound of the error for (3) is essential, because if these approximate values $P_{OOV}(\bar{w})$ deviate too much from the actual $P(\bar{w})$ values, it could lead to the wrong decision of $\bar{w}$. Let us remember that in the OOV attack the weight of noise vector $\bar{\mathbf{e}}$ is $\bar{w}$, if $P_{OOV} - 1(\frac{c}{n})$ is closest to $\bar{w}$, for all possible values of $\bar{w}$.

3.1.4. Main Conclusions

We summarize the mistakes in the theoretical analysis behind the OOV attack from [12], found in the analysis given above, which will turn out as crucial for high error rate of the OOV weight estimate:

- The distribution of the Hamming weight of cumulative noise vector is wrongly assessed as Binomial,
- Approximation $P(\bar{w}) \approx P_{OOV}(\bar{w})$ lacks error estimation,
- The error of the weight estimate procedure is unknown. Since error bound of $P(\bar{w}) \approx P_{OOV}(\bar{w})$ is unknown, this consequently also stands for the final approximation $\frac{c}{n} \approx P_{OOV}(\bar{w})$ which produces the output of weight estimate procedure.

In the following sections, we introduce our research process to overcome the listed omissions.

3.2. Error Estimation of Acceptance Rates Approximation $P(\bar{w}) \approx P_{OOV}(\bar{w})$

First, we infer the standard upper error bound of $P(\bar{w}) \approx P_{OOV}(\bar{w})$ by applying Berry-Esseen inequality for CLT approximations. The obtained result indicates that distance between $P(\bar{w})$ and $P_{OOV}(\bar{w})$ could be too high and thus prevent a correct weight estimation. Then, we proceed to infer the exact distribution of the acceptance rates and the exact error of this approximation.

3.2.1. Standard Upper Error Bound for CLT Approximations

Approximation $P(\bar{w}) = Pr[\|\mathbf{e} \oplus \bar{\mathbf{e}}\| \leq thr] \approx P_{OOV}(\bar{w}) = \Phi(\frac{thr - (m-\bar{w})\tau - \bar{w}(1-\tau)}{\sqrt{m\tau(1-\tau)}})$ was derived in [12] using the CLT, which only implies its convergence when $m \to \infty$. The Berry-Eseen inequality further refines this result by providing bound on its maximal error. Here, we show that the sum $\|\mathbf{e} \oplus \bar{\mathbf{e}}\|$ follows Poisson-Binomial distribution, not the plain Binomial distribution as claimed in [12]. Then we apply a general CLT for non-identical random variables to this distribution in order to obtain $P(\bar{w}) \approx P_{OOV}(\bar{w})$, and we estimate its precision using the Berry-Eseen inequality.

Definition 2. *Poisson-Binomial distribution is a probability distribution of a sum $\sum_{i=0}^{n} X_i$ of independent Bernoulli random variables $X_1, \ldots, X_n$ with possibly different probabilities of success $p_1, \ldots, p_n$, and we denote it by $\mathcal{PB}(p_1, \ldots, p_n)$. Binomial distribution is a special case of the Poisson-Binomial distribution where $X_1, \ldots, X_n$ share the same probability of success.*

Lemma 1. *The Hamming weight of cumulative noise vector $\|\mathbf{e} \oplus \bar{\mathbf{e}}\|$, where $\|\bar{\mathbf{e}}\| = \bar{w}$, which the Reader computes in the verification phase after MIM modification $(\bar{\mathbf{a}}, \bar{\mathbf{b}}, \bar{\mathbf{z}} = \bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} \oplus \bar{\mathbf{e}})$ of Random HB# or HB# protocol session, follows Poisson-Binomial distribution*
$\mathcal{PB}(\underbrace{1-\tau, \ldots, 1-\tau}_{\bar{w}}, \underbrace{\tau, \ldots, \tau}_{m-\bar{w}})$.

Proof. Since a new noise vector $\mathbf{e} \leftarrow Ber_{\tau}^{m}$ is being generated in each modification session, and $\bar{\mathbf{e}} \leftarrow Ber_{\tau}^{m}$ remains fixed during all modifications, notice that:

$$\|\mathbf{e} \oplus \bar{\mathbf{e}}\| = \sum_{k=1}^{m} (\mathbf{e_k} \oplus \bar{\mathbf{e}}_\mathbf{k}) = \sum_{\substack{k=1 \\ \bar{\mathbf{e}}_\mathbf{k}=1}}^{m} (\mathbf{e_k} \oplus 1) + \sum_{\substack{k=1 \\ \bar{\mathbf{e}}_\mathbf{k}=0}}^{m} \mathbf{e_k} = \sum_{k=1}^{\bar{w}} \tilde{s}_k + \sum_{k=1}^{m-\bar{w}} s_k, \tag{4}$$

where s_k and $\tilde{s}_k$ are Bernoulli random variables, such that $Pr[s_k = 1] = \tau$ and $Pr[\tilde{s}_k = 1] = 1 - \tau$ (see Figure 4).

Therefore, $\|\mathbf{e} \oplus \bar{\mathbf{e}}\| \leftarrow \mathcal{PB}(\underbrace{1-\tau, \ldots, 1-\tau}_{\bar{w}}, \underbrace{\tau, \ldots, \tau}_{m-\bar{w}})$. □

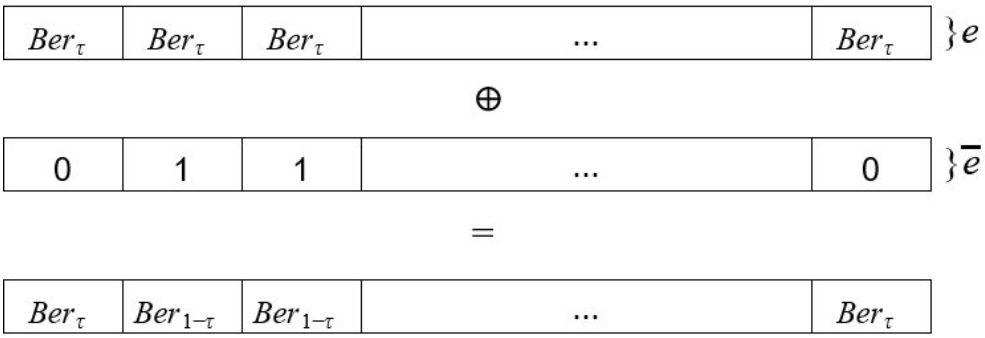


Figure 4. Distribution structure of the cumulative noise vector $\mathbf{e} \oplus \bar{\mathbf{e}}$.

Theorem 1 (General CLT, Lyapunov condition [26])**.** *Let $X_1, X_2 \ldots$ be a sequence of independent (and not necessarily identical) random variables such that $EX_i = \mu_i$, $VarX_i = \sigma_i^2 < \infty$ and $D_n^2 = Var(\sum_{i=1}^{n} X_i) = \sum_{i=1}^{n} \sigma_i^2$. If there is $\delta > 0$ such that:*

$$\lim_{n\to\infty} \frac{1}{D_n^{2+\delta}} \sum_{i=1}^{n} E(|X_i - \mu_i|)^{2+\delta} = 0 \quad \textbf{\textit{(Lyapunov condition)}}$$

then the distributions of $\frac{\sum_{i=1}^{n} X_i - \sum_{i=1}^{n} \mu_i}{D_n}$ converge weakly to $\mathcal{N}(0,1)$ as $n \to \infty$, that is,

$$\frac{\sum_{i=1}^{n} X_i - \sum_{i=1}^{n} \mu_i}{D_n} \xrightarrow{\mathcal{D}} \mathcal{N}(0,1).$$

Theorem 2 (General CLT for Poisson-Binomial distribution)**.** *If random variable X follows Poisson-Binomial distribution i.e., $X = \sum_{i=1}^{n} X_i$, $X_i \leftarrow Ber_{p_i}$, where $D_n^2 = Var(X) = \sum_{i=1}^{n} p_i(1-p_i)$, and $D_n \to \infty$ $(n \to \infty)$, then:*

$$\frac{X - \sum_{i=1}^{n} p_i}{D_n} \xrightarrow{\mathcal{D}} \mathcal{N}(0,1).$$

Proof of Theorem 2. Let $\mu_i = E(X_i) = p_i$. We prove the Lyapunov condition is satisfied for $\delta = 1$.

Since $X_i : \begin{pmatrix} 1 & 0 \\ p_i & 1-p_i \end{pmatrix}$, $|X_i - \mu_i|^3 : \begin{pmatrix} (1-\mu_i)^3 & \mu_i^3 \\ p_i & 1-p_i \end{pmatrix}$, we have that:

$$\begin{aligned} E|X_i - \mu_i|^3 &= (1-\mu_i)^3 p_i + \mu_i^3 (1-p_i) \\ &= (1-p_i)^3 p_i + p_i^3 (1-p_i) \\ &= p_i(1-p_i)[(1-p_i)^2 + p_i^2] \\ &= p_i(1-p_i)[1 - 2p_i(1-p_i)] \leq p_i(1-p_i), i = 1, \ldots, n. \end{aligned}$$

Therefore $\sum_{i=1}^{n} E(|X_i - \mu_i|)^3 \leq \sum_{i=1}^{n} p_i(1-p_i) = D_n^2$ and

$$\frac{1}{D_n^3}\sum_{i=1}^{n} E(|X_i - \mu_i|)^3 \leq \frac{D_n^2}{D_n^3} = \frac{1}{D_n} \to 0\,(n \to \infty).$$

□

Since $\mu = E(\|\mathbf{e} \oplus \bar{\mathbf{e}}\|) = \bar{w}(1-\tau) + (m-\bar{w})\tau$ and $Var(\|\mathbf{e} \oplus \bar{\mathbf{e}}\|) = m\tau(1-\tau)$, as a direct consequence of Theorem 2 and Lemma 1, we have that:

Lemma 2. *For the cumulative noise vector* $\mathbf{e} \oplus \bar{\mathbf{e}}$ *it holds that:*

$$\frac{\|\mathbf{e} \oplus \bar{\mathbf{e}}\| - (m-\bar{w})\tau - \bar{w}(1-\tau)}{\sqrt{m\tau(1-\tau)}} \xrightarrow{\mathcal{D}} \mathcal{N}(0,1), m \to \infty.$$

In order to estimate the precision of this approximation, we proceed to use the standard error measure for general CLT:

Theorem 3 (Berry-Eseen inequality for non-identical random variables [27])**.** *Let* $X_1, \ldots, X_n$ *be independent random variables such that* $EX_i = 0$, $VarX_i = \sigma_i^2$, *and* $D_n^2 = Var(\sum_{i=1}^{n} X_i) = \sum_{i=1}^{n} \sigma_i^2$. *Then for every n there is an absolute constant C such that:*

$$\sup_{x \in \mathbb{R}} \left| Pr\left[\frac{X}{D_n} \leq x\right] - \Phi(x) \right| \leq C \cdot \frac{\sum_{i=1}^{n} E|X_i|^3}{D_n^3}.$$

It was proven that $0.4097 \approx \frac{\sqrt{10}+3}{6\sqrt{2\pi}} = C_0 \leq C \leq C_1 = 0.5600$ ([28]). C_0 is the biggest known lower bound and C_1 the smallest known upper bound for C in literature, to the best of our knowledge.

Theorem 4 (Berry-Eseen inequality for Poisson-Binomial distribution)**.** *If random variable X follows Poisson-Binomial distribution, that is,* $X = \sum_{i=1}^{n} X_i$, $X_i \leftarrow \mathrm{Ber}_{p_i}$, *where* $D_n^2 = Var(X) = \sum_{i=1}^{n} p_i(1-p_i)$, *and* $D_n \to \infty\,(n \to \infty)$, *then for every n there is a constant* $C \in [C_0, C_1]$ *such that:*

$$\sup_{x \in \mathbb{R}} \left| Pr\left[\frac{X - \sum_{i=1}^{n} p_i}{D_n} \leq x\right] - \Phi(x) \right| \leq C \cdot \frac{\sum_{i=1}^{n} p_i(1-p_i)[(1-p_i)^2 + p_i^2]}{D_n^3}$$

Proof. Let $Y_i = X_i - \mu_i$, $\mu_i = EX_i = p_i$. Then $EY_i = 0$, $Var(Y_i) = p_i(1-p_i)$ and $E|Y_i|^3 = p_i(1-p_i)[(1-p_i)^2 + p_i^2]$ (see proof of Theorem 2). The claim follows directly by applying Berry-Eseen inequality to random variables $Y_1, \ldots, Y_n$. □

Lemma 3. *For the cumulative noise vector* $\mathbf{e} \oplus \bar{\mathbf{e}}$ *it holds that:*

$$\sup_{x \in \mathbb{R}} \left| Pr\left[\frac{\|\mathbf{e} \oplus \bar{\mathbf{e}}\| - (m-\bar{w})\tau - \bar{w}(1-\tau)}{\sqrt{m\tau(1-\tau)}} \leq x\right] - \Phi(x) \right| \leq C \cdot \frac{[(1-\tau)^2 + \tau^2]}{\sqrt{m\tau(1-\tau)}},$$

where $C \in [C_0, C_1]$.

Proof. This is a direct consequence of the inequality above, taken in consideration that:
$\|\mathbf{e} \oplus \bar{\mathbf{e}}\| = \sum_{i=1}^{m} X_i$, $X_i \leftarrow \mathrm{Ber}_{p_i}$, $p_i = \begin{cases} 1-\tau, i = 1, \ldots, \bar{w} \\ \tau, i = \bar{w}+1, \ldots, m \end{cases}$,
$\sum_{i=1}^{m} p_i = (m-\bar{w})\tau + \bar{w}(1-\tau)$,
$D_m^2 = Var(X) = m\tau(1-\tau)$,
$\sum_{i=1}^{n} p_i(1-p_i)[(1-p_i)^2 + p_i^2] = m\tau(1-\tau)[(1-\tau)^2 + \tau^2] = D_m^2[(1-\tau)^2 + \tau^2]$. □

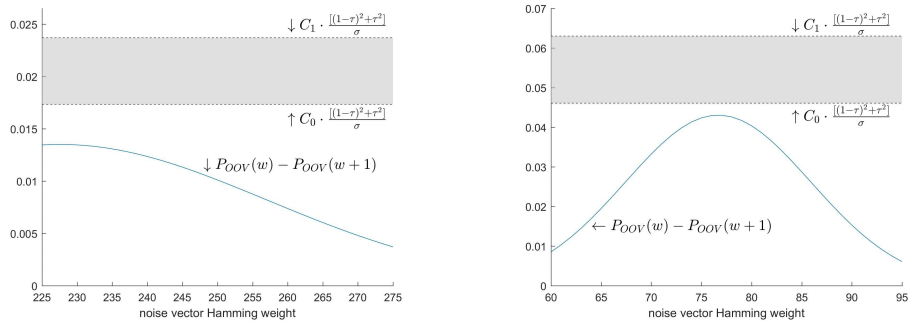
As a consequence of this Lemma, by taking $x = \frac{thr-\mu}{\sigma}$, $\mu = (m-\bar{w})\tau + \bar{w}(1-\tau)$ and $\sigma^2 = m\tau(1-\tau)$, the standard Berry-Eseen upper bound estimate for the error of the approximation $P(\bar{w}) \approx P_{OOV}(\bar{w})$ is:

$$\left| Pr[\|\mathbf{e} \oplus \bar{\mathbf{e}}\| \leq thr] - \Phi\left(\frac{thr-\mu}{\sigma}\right) \right| \leq \bar{C}, \tag{5}$$

where $\bar{C} \in [C_0 \cdot \frac{[(1-\tau)^2+\tau^2]}{\sigma}, C_1 \cdot \frac{[(1-\tau)^2+\tau^2]}{\sigma}]$.

Using Formula (5) we derive that for the standard parameter set I, where $\tau = 0.25$ and $m = 1164$, the error upper bound lies in the interval $[0.017334, 0.023691]$, while for the standard parameter set II, where $\tau = 0.125$ and $m = 441$, the error upper bound is from the interval $[0.046091, 0.062994]$.

The exact $P(\bar{w})$ lies somewhere in the interval $[(P_{OOV}(\bar{w}) - \bar{C}, P_{OOV}(\bar{w}) + \bar{C}]$. Nevertheless, this interval is wider, i.e., covers the interval in which the adversary has to decide between adjacent weights $\bar{w}$ and $\bar{w}+1$ (see Figure 5). It is possible that the adversary is incapable to determine and decide accurately if $\frac{c}{n}$ is closest to $P(\bar{w})$ or $P(\bar{w}+1)$, which directly jeopardizes his decision making. For example, if $\frac{c}{n}$ is in the position marked in Figure 6, the adversary will decide that the weight is $\bar{w}$, because $P_{OOV}(\bar{w})$ is closest to it, but since $\frac{c}{n}$ is in a possible location of $P(\bar{w}+1)$, it could in fact be closest to $P(\bar{w}+1)$, and the actual weight could be $\bar{w}+1$. In order to investigate possibility of such scenarios of erroneous weight conclusions due to high error of approximation, in the next Section, we shall determine where precisely are $P(\bar{w})$ values.



(**a**) Standard parameter set I (**b**) Standard parameter set II

Figure 5. The approximation error upper bound is larger than the interval widths used in the attack. Thus, the adversary may not be capable to accurately estimate noise vectors weights.

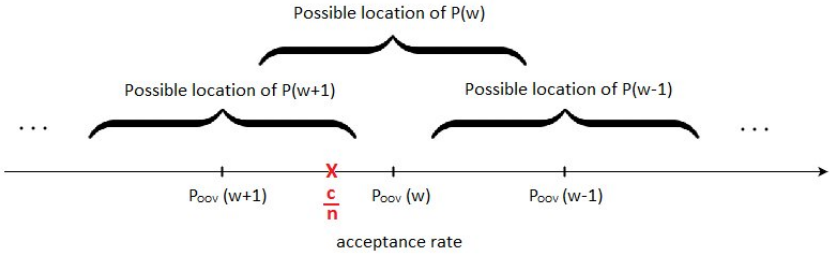


Figure 6. Localization of $P(w)$ values using Berry-Eseen upper error bound.

3.2.2. The Exact Distribution of the Acceptance Rates

Here, we calculate the exact acceptance rate of HB# and Random-HB# protocols while under the OOV attack, by using Lemma 1 from Section 3.2.1.

Theorem 5. *Let $P(\bar{w}) = P[\|\mathbf{e} \oplus \bar{\mathbf{e}}\| \leq thr]$ denote the probability of successful authentication after MIM modification using triplet $(\bar{\mathbf{a}}, \bar{\mathbf{b}}, \bar{\mathbf{z}} = \bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} \oplus \bar{\mathbf{e}})$ of exchanged messages caught in a Random HB# or HB# protocol session, where $\bar{w} = \|\bar{\mathbf{e}}\|$. Then:*

$$P(\bar{w}) = PB(\bar{w}) := \sum_{j=0}^{thr} \sum_{i=\max\{0, j+\bar{w}-m\}}^{\min\{\bar{w}, j\}} \binom{\bar{w}}{i} \binom{m-\bar{w}}{j-i} \tau^{\bar{w}+j-2i} (1-\tau)^{m-(\bar{w}+j-2i)}. \quad (6)$$

In addition, if c is the number of successful authentications after n MIM modifications, then for acceptance rate $\frac{c}{n}$ it holds that

$$\frac{c}{n} \leftarrow \frac{Bin(n, P(\bar{w}))}{n}.$$

Proof. Since:

$$\|\mathbf{e} \oplus \bar{\mathbf{e}}\| = \sum_{k=1}^{m} (\mathbf{e_k} \oplus \bar{\mathbf{e}}_\mathbf{k}) = \sum_{\substack{k=1 \\ \bar{\mathbf{e}}_\mathbf{k}=1}}^{m} (\mathbf{e_k} \oplus 1) + \sum_{\substack{k=1 \\ \bar{\mathbf{e}}_\mathbf{k}=0}}^{m} \mathbf{e_k} = \sum_{k=1}^{\bar{w}} \tilde{s}_k + \sum_{k=1}^{m-\bar{w}} s_k,$$

where $s_k \leftarrow Ber_\tau$, $\tilde{s}_k \leftarrow Ber_{1-\tau}$ (see Proof of Lemma 1) we have that:

$$\begin{aligned}
P(\bar{w}) &= Pr[\|\mathbf{e} \oplus \bar{\mathbf{e}}\| \leq thr] \\
&= \sum_{j=0}^{thr} Pr[\|\mathbf{e} \oplus \bar{\mathbf{e}}\| = j] \\
&= \sum_{j=0}^{thr} Pr[\sum_{k=1}^{\bar{w}} \tilde{s}_k + \sum_{k=1}^{m-\bar{w}} s_k = j] \\
&= \sum_{j=0}^{thr} \sum_{i=0}^{j} \left\{ Pr[\sum_{k=1}^{\bar{w}} \tilde{s}_k = i] \cdot Pr[\sum_{k=1}^{m-\bar{w}} s_k = j-i] \,|\, i \leq \bar{w}, j-i \leq m-\bar{w} \right\} \\
&= \sum_{j=0}^{thr} \sum_{\substack{i \leq \bar{w} \\ j-i \leq m-\bar{w} \\ i=0}}^{j} \left[\binom{\bar{w}}{i} (1-\tau)^i \tau^{\bar{w}-i} \right] \left[\binom{m-\bar{w}}{j-i} \tau^{j-i} (1-\tau)^{m-\bar{w}-j+i} \right] \\
&= \sum_{j=0}^{thr} \sum_{i=\max\{0, j+\bar{w}-m\}}^{\min\{\bar{w}, j\}} \binom{\bar{w}}{i} \binom{m-\bar{w}}{j-i} \tau^{\bar{w}+j-2i} (1-\tau)^{m-(\bar{w}+j-2i)}.
\end{aligned}$$

□

(Number of successes in $\bar{w}$ Bernoulli experiments can not exceed $\bar{w}$. Similarly for $m - \bar{w}$.)

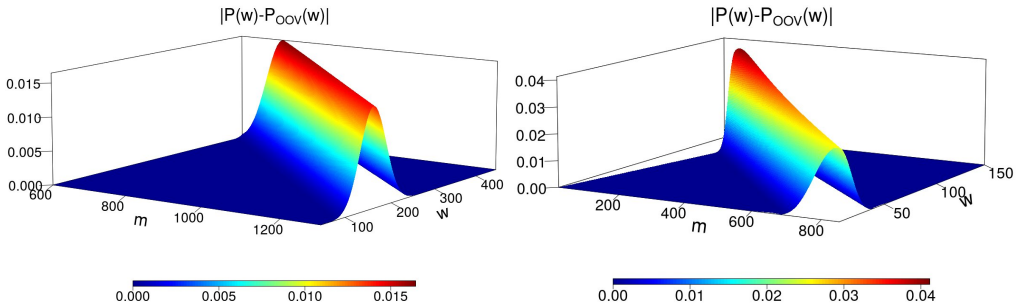
3.2.3. Exact Error of the Approximation $P(\bar{w}) \approx P_{OOV}(\bar{w})$

Finally, we are able to derive the exact error of the P_{OOV} approximation as:

$$|P(\bar{w}) - P_{OOV}(\bar{w})| = |\sum_{j=0}^{thr} \sum_{i=\max\{0, j+\bar{w}-m\}}^{\min\{\bar{w}, j\}} \binom{\bar{w}}{i} \binom{m-\bar{w}}{j-i} \tau^{\bar{w}+j-2i} (1-\tau)^{m-(\bar{w}+j-2i)} - \Phi\left(\frac{thr-\mu}{\sigma}\right)|, \quad (7)$$

where $\mu = (m-\bar{w})\tau + \bar{w}(1-\tau)$ and $\sigma^2 = m\tau(1-\tau)$.

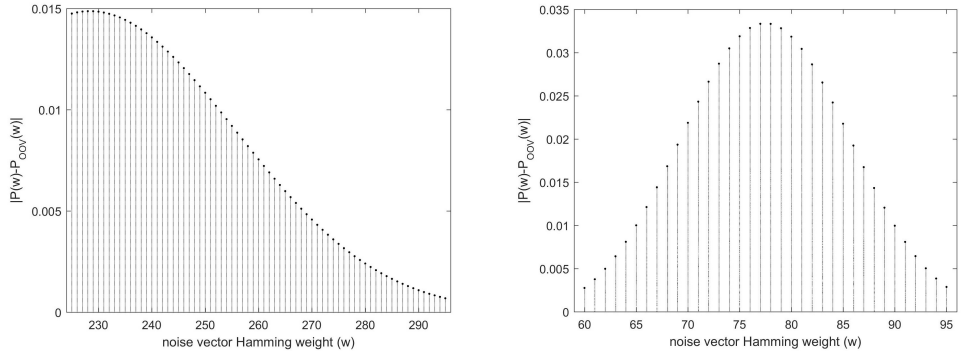
Although, in theory, this error diminishes for m large enough (see Figure 7), in the OOV attack m is the dimension of secret matrices. Thus, this error is a constant intrinsic to the protocol and the adversary is unable to manipulate it.



(**a**) Standard parameter set I (**b**) Standard parameter set II

Figure 7. Theoretically, the approximation error decreases as m increases by CLT (note the transition in color of the error peak). In the OOV attack, $m = 1164$ or $m = 441$, for standard parameter sets I or II, respectively.

The exact error values for standard protocol parameters are shown in Figure 8.



(**a**) Standard parameter set I (**b**) Standard parameter set II

Figure 8. The exact error of the P_{OOV} approximation.

Note that the error gets higher as $\bar{w}$ approaches the claimed optimal weight w_{opt}, where it reaches its maximum. This weight is 228 for the standard parameter set I, while it is 77 for the other one.

3.3. Proper Decision Zones

The OOV decision zones, which are based on the inverse function $P_{OOV}^{-1}(\frac{c}{n})$ values, have the following potential drawbacks, in general case:

- the inverse function might not preserve the ratios of distances, so, for example, it could be possible that $P^{-1}(\frac{c}{n})$ is closer to $\bar{w}$ than to $\bar{w}+1$, while $\frac{c}{n}$ is actually closer to $P(\bar{w}+1)$ than to $P(\bar{w})$,
- P_{OOV} is used as an approximation of exact acceptance rates P with unknown precision,
- $\bar{w}$ should be determined by considering which of the possible distributions is $\frac{c}{n}$ most likely sampled from, i.e., by probabilistic reasoning, instead of simply applying the inverse function to $\frac{c}{n}$ value.

We employ the Bayesian reasoning over the exact distributions of acceptance rates to construct proper decision zones. The noise vector weight $\|\bar{\mathbf{e}}\|$ is estimated as $\bar{w}$ if the observed empirical acceptance frequency $\frac{c}{n}$ most likely follows the exact distribution $\frac{Bin(n,P(\bar{w}))}{n}$, $\bar{w} \in W$, where W is the set of all the weights $\bar{w}$ the adversary considers possible.

As a general weight decision rule, $\bar{w} = \underset{w \in W}{\text{argmax}}\, Pr[\|\bar{\mathbf{e}}\| = w \mid \frac{c}{n} \text{ observed acceptance rate})]$

$= \underset{w \in W}{\text{argmax}}\{P(w)^{\frac{c}{n}}(1-P(w))^{1-\frac{c}{n}} \cdot P_{occur}(w)^{\frac{1}{n}}\}$, where $P_{occur}(w) = Pr[\|\bar{\mathbf{e}}\| = w]$ is the probability of occurrence of noise vector whose weight is w. By its logarithmic transformation, we obtain that the adversary decides the noise vector weight as $\bar{w}$ iff:

$$\bar{w} = \underset{w \in W}{\text{argmax}}\{F(c,n) = c_0(w) + c_1(w)\frac{c}{n}\},$$

where $c_0(w) = log(1-P(w)) + \frac{log(P_{occur}(w))}{n}$, $c_1(w) = log\frac{P(w)}{1-P(w)}$. After the mere eavesdropping, $P_{occur}(w) = \binom{m}{w}\tau^w(1-\tau)^{m-w}$. If the eavesdropped vector was flipped in f positions to reach optimal weight, $P_{occur}(w) = PB(f,m,\tau,w) - PB(f,m,\tau,w-1)$. When recovering bits, $P_{occur}(w-1) = \tau$ and $P_{occur}(w+1) = 1-\tau$. The values $P(w)$ and $P_{occur}(w)$ may be calculated in advance, so decision making is highly efficient.

However, when considering weights near w_{opt} and standard parameter sets, for n large enough, the decision making can be further simplified. Namely, after comparing variances $Var(w) = \frac{P(w)(1-P(w))}{n}$ of the exact distributions for the consecutive weights $w-1$, w and $w+1$ in such case, we have found their differences as insufficient to impact the Bayesian decision. Also, probabilities of occurrence of these weights produce negligible priors (observe division by n in $c_0(w)$).

Therefore, because these distributions $\frac{Bin(n,P(\bar{w}))}{n} \xrightarrow{\mathcal{D}} \mathcal{N}(P(\bar{w}), Var(\bar{w}))$ are almost symmetrical, for all practical purposes, $\bar{w}$-decision zones will be $(\frac{P(\bar{w})+P(\bar{w}+1)}{2}, \frac{P(\bar{w}-1)+P(\bar{w})}{2})$, $\bar{w} = 1, \ldots, m$ after eavesdropping, while they will be $(-\infty, \frac{P(\bar{w}-1)+P(\bar{w}+1)}{2})$ and $(\frac{P(\bar{w}-1)+P(\bar{w}+1)}{2}, \infty)$ when deciding between $\bar{w}+1$ and $\bar{w}-1$ after flipping a bit. We shall also call them *"PB-decision zones"*, since they use the exact values $P(\bar{w}) = PB(\bar{w})$. Figure 9 provides a graphical illustration of the PB-decision zones used in the processes of weight estimate after eavesdropping and bit recovery.

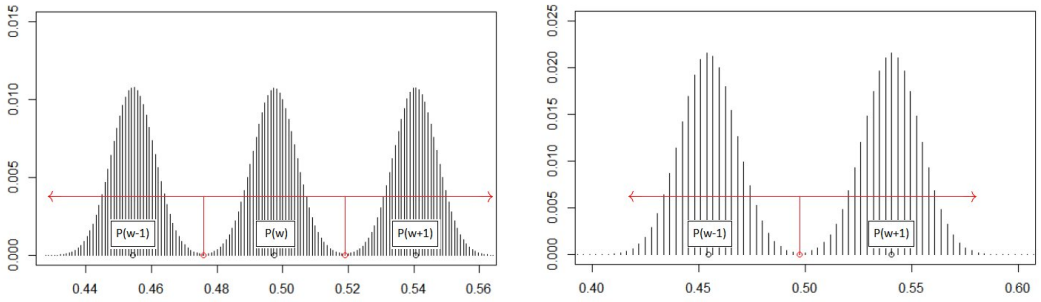


Figure 9. PB-decision zones used after eavesdropping (**left**) and for bit recovery (**right**).

Expressed more formally—probability that $\frac{c}{n}$ is sampled from $\mathcal{N}(P(\bar{w}), Var(\bar{w}))$ is $g(c,n,\bar{w}) = \frac{1}{\sqrt{2\pi Var(\bar{w})}} e^{-\frac{(\frac{c}{n}-P(\bar{w})^2)}{2Var(\bar{w})}} P_{occur}(\bar{w})$, so according to maximum a posteriori (MAP) test, we choose hypothesis $W = \bar{w}$ over $W = \bar{w}+i, i \in \{1,2\}$ iff $g(c,n,\bar{w}) > g(c,n,\bar{w}+i)$ that is,

$$\sqrt{\frac{Var(\bar{w}+i)}{Var(\bar{w})}} \cdot \frac{P_{occur}(\bar{w})}{P_{occur}(\bar{w}+1)} \geq e^{-\frac{(\frac{c}{n}-P(\bar{w}+i))^2}{2Var(\bar{w}+i)} + \frac{(\frac{c}{n}-P(\bar{w}))^2}{2Var(\bar{w})}} = e^{-\frac{n}{2}(\frac{(\frac{c}{n}-P(\bar{w}+i))^2}{P(\bar{w}+i)(1-P(\bar{w}+i))} - \frac{(\frac{c}{n}-P(\bar{w}))^2}{P(\bar{w})(1-P(\bar{w}))})},$$

that is, iff condition $(\frac{c}{n} - P(\bar{w}+i))^2 > \delta^2(\frac{c}{n} - P(\bar{w}))^2$ is satisfied, where $\delta^2 = \frac{P(\bar{w}+i)(1-P(\bar{w}+i))}{P(\bar{w})(1-P(\bar{w}))} = \frac{Var(\bar{w}+i)}{Var(\bar{w})}$, i.e., $\frac{c}{n} < B$ or $\frac{c}{n} > A$ when $\delta < 1$, or $A < \frac{c}{n} < B$ when $\delta > 1$, where $A = P(\bar{w}+i) + \frac{\delta}{\delta+1}(P(\bar{w}) - P(\bar{w}+i))$, $B = P(\bar{w}) + \frac{\delta}{\delta-1}(P(\bar{w}) - P(\bar{w}+i))$. However, since $B < 0$ for $\delta < 1$, and $B \geq 1$ for $\delta > 1$, for weights near the optimal one, the condition is equivalent

to $\frac{c}{n} > A$. Furthermore, $Pr\left[\frac{c}{n} \in (\frac{P(\bar{w})+P(\bar{w}+i)}{2}, A) \,\middle|\, \frac{c}{n} \xrightarrow{\mathcal{D}} \mathcal{N}(P(w), \sigma^2), w \in \{\bar{w}, \bar{w}+i\}\right]$ is negligible in such case, so we reduce this decision to condition $\frac{c}{n} > \frac{P(\bar{w})+P(\bar{w}+i)}{2}$, that is, that the observed frequency $\frac{c}{n}$ is closer to $P(\bar{w})$ than to $P(\bar{w}+i)$ (P is monotone decreasing function).

3.4. The Exact and the Approximate Probability Distribution Relation

We now show that the decisions the adversary makes about noise vectors weights can differ depending on whether he uses the OOV approximation or the exact distribution.

We have noticed that the OOV w-decision zones are substantially shifted to the left with respect to PB-w decision zones, and that they often largely overlap with the correct PB-$w+1$ decision zone (see Figure 10). As a consequence, there is a high chance that the OOV adversary decides the weight is w, while the actual weight is $w+1$.

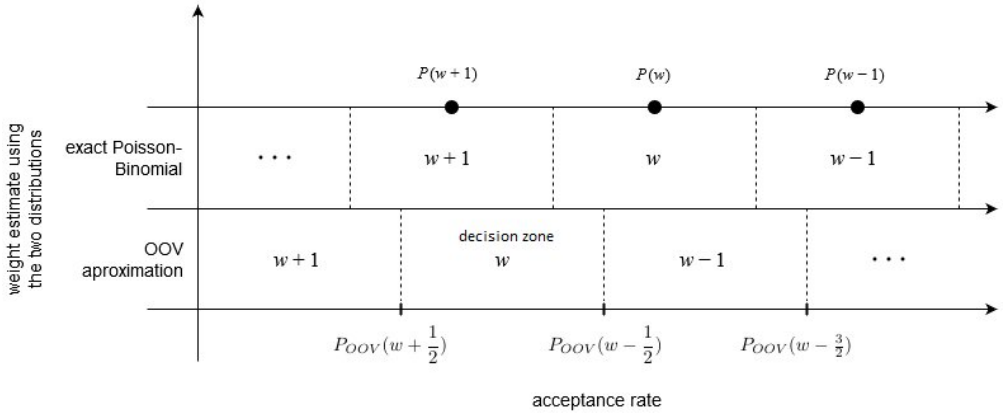


Figure 10. Different "decision zones" according to the OOV approximation and the exact Poisson-Binomial distribution.

This adverse phenomena is especially pronounced in the expected case—when $\bar{w}$ is near the optimal weight w_{opt}, since there is the biggest distance between $P(\bar{w})$ and $P_{OOV}(\bar{w})$—degrading significantly the precision of the weight estimate.

Furthermore, the shift of the OOV decision zones can not be repaired by employing larger "sample size" n, that is, number of intercepted authentications, because the approximation $P_{OOV}(\bar{w}) \approx P(\bar{w})$ has a high fixed error in this scenario (as shown in the previous Section). The convergence $\frac{c}{n} \to P_{OOV}(\bar{w})$ occurs only when both $m \to \infty$ and $n \to \infty$:

$$\frac{c}{n} \xrightarrow[n\to\infty]{} P(\bar{w}) \xleftarrow[m\to\infty]{} P_{OOV}(\bar{w}) \implies \frac{c}{n} \xrightarrow[n\to\infty, m\to\infty]{} P_{OOV}(\bar{w}).$$

However, in the context of the OOV attack, m is a constant protocol parameter and thus:

$$\frac{c}{n} \xrightarrow[n\to\infty]{} P(\bar{w}) \xleftarrow[\text{fixed distance}]{} P_{OOV}(\bar{w}) \implies |\frac{c}{n} - P_{OOV}(\bar{w})| \xrightarrow[n\to\infty]{} |P(\bar{w}) - P_{OOV}(\bar{w})|.$$

This explains the experimental observations from [25] that the weight estimate does not improve by increasing the sample size.

4. Correction of the OOV Attack

In this section, we give a correction of the OOV-MIM attack and show that it meets the targeted precision, unlike the original attack.

4.1. Correction of the OOV Attack Algorithm

In order to solve the problem of high error of the approximation $P_{OOV}(\bar{w}) \approx P(\bar{w})$, we eliminate this approximation altogether, since we have shown that it can not be improved. Instead we employ the acceptance rates obtained from the exact distribution. That is, instead of:

$$\frac{c}{n} \xrightarrow[n\to\infty]{} P(\bar{w}) \xleftarrow[m\to\infty]{} P_{OOV}(\bar{w}) \implies \frac{c}{n} \approx P_{OOV}(\bar{w}) = \Phi\left(\frac{thr-(m-\bar{w})\tau-\bar{w}(1-\tau)}{\sqrt{m\tau(1-\tau)}}\right),$$

we use Poisson-Binomial cumulative distribution function:

$$\frac{c}{n} \xrightarrow[n\to\infty]{} P(\bar{w}) \implies \frac{c}{n} \approx P(\bar{w}) = \sum_{j=0}^{thr} \sum_{i=\max\{0,j+\bar{w}-m\}}^{\min\{\bar{w},j\}} \binom{\bar{w}}{i}\binom{m-\bar{w}}{j-i}\tau^{\bar{w}+j-2i}(1-\tau)^{m-(\bar{w}+j-2i)}.$$

Then, we incorporate it in proper, Bayesian decision zones described in Section 3.3 with their corresponding optimal weights and modification samples. Noise vector $\bar{\mathbf{e}}$ Hamming weight will be estimated as $\bar{w}$ if and only if $\frac{c}{n}$ is nearest to $P(\bar{w})$, for all weights $w \in \{0,\ldots,m\}$ considered possible.

Hence, the pseudocode of the proposed correction of the weight estimate procedure is given in Algorithm 1:

Algorithm 1 PB-OOV weight estimate alg. Approximating $\bar{w} = \|\bar{\mathbf{e}}\|$

1: **Input:** $\bar{\mathbf{a}}, \bar{\mathbf{b}}, \bar{\mathbf{z}} = \bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} \oplus \bar{\mathbf{e}}, n$
2: **Output:** estimate of noise vector weight
$\bar{w} = \|\bar{\mathbf{a}}\mathbf{X} \oplus \bar{\mathbf{b}}\mathbf{Y} \oplus \bar{\mathbf{z}}\|$, where

$$P(\bar{w}) = \sum_{j=0}^{thr} \sum_{i=\max\{0,j+\bar{w}-m\}}^{\min\{\bar{w},j\}} \binom{\bar{w}}{i}\binom{m-\bar{w}}{j-i}\tau^{\bar{w}+j-2i}(1-\tau)^{m-(\bar{w}+j-2i)}$$

3: **Processing:**
4: $c = 0$
5: **for** $i = 1...n$ **do**
6: During i-th session, the adversary modifies and replaces messages:
7: $\mathbf{a}$ with $\hat{\mathbf{a}} = \mathbf{a} \oplus \bar{\mathbf{a}}$, $\mathbf{b}$ with $\hat{\mathbf{b}} = \mathbf{b} \oplus \bar{\mathbf{b}}$, $\mathbf{z}$ with $\hat{\mathbf{z}} = \mathbf{z} \oplus \bar{\mathbf{z}}$
8: **if** Verifier accepts the modified response **then**
9: $c = c + 1$
10: **end if**
11: **end for**
12: **return** $\bar{w} = \underset{w}{\operatorname{argmin}}\{|\frac{c}{n} - P(w)| \,|\, w = 0,\ldots,m\}$.

Since the PB Decision zone for $w \supset I = [P(w) - \bar{r}, P(w) + \bar{r}]$, where $\bar{r} = \frac{1}{2}min\{P(w) - P(w+1), P(w-1) - P(w)\}$ we have that:

$$Pr[\tfrac{c}{n} \in \text{PB Decision zone for } w] \geq Pr\left[\frac{c}{n} \in I \,\middle|\, \frac{c}{n} \xrightarrow{\mathcal{D}} \mathcal{N}(P(\bar{w}), \sigma^2)\right] = 1 - erfc(\theta), \theta = \frac{\bar{r}\cdot\sqrt{n}}{\sqrt{2P(\bar{w})(1-P(\bar{w}))}}.$$

Therefore, after the eavesdropping, PB-OOV adversary chooses sample of size $n_{PB} = 4\theta^2 R_{PB}(w)$, $R_{PB}(w) = 2\frac{P(w)(1-P(w))}{\bar{r}^2}$ to achieve the required precision $1 - erfc(\theta)$, which is based on exact values $PB(w)$ instead of approximate ones $P_{OOV}(w)$ as in Formula (2) from [12]. Accordingly, he uses optimal weight w_{opt}^{PB} which minimizes this sample across all weights and its value is 229 for parameter set I, and 78 for parameter set II. After the flipping, he will use samples of size $\theta^2 R_{PB}(w)$ to recover bits.

It should be noted that the values $P(w), w = 0,\ldots,m$ can be calculated in advance, as a part of the preprocessing step, and stored in a table to be later used during the attack.

4.2. Comparison of the OOV and PB-OOV Attack Success

In this section we analyze the probability of success of the OOV and PB-OOV attack. Namely, we derive the probability the OOV adversary will correctly reconstruct a noise vector (and consequently recover the key) and show that, as a consequence of the approximation employed, the OOV attack is significantly less efficient than claimed in [12]. Oppositely, the PB-OOV attack proposed in Section 4.1, achieves the desired precision and efficiency.

4.2.1. Noise Vector Hamming Weight Estimate

OOV adversary. First, let us observe the distribution of acceptance rate $\frac{c}{n}$ during the attack when $\|\bar{\mathbf{e}}\| = \bar{w}$:

$$c = \sum_{i=1}^{n} X_i, X_i \leftarrow Ber_{P(\bar{w})} \implies \frac{c}{n} \xrightarrow{\mathcal{D}} \mathcal{N}(P(\bar{w}), \sigma^2(\bar{w}, n)),$$

where $\sigma = \sigma(\bar{w}, n) := \sqrt{\frac{P(\bar{w})(1-P(\bar{w}))}{n}}$.

The probability that the OOV adversary estimates that noise vector $\bar{\mathbf{e}}$ has weight w_{est}, when its weight is $\bar{w}$ (which may or may not be equal to w_{est}), using n modifications of authentication sessions is:

$$p_0(w_{est}, \bar{w}, n) = Pr\left[\frac{c}{n} \in \text{OOV Decision zone for } w_{est} \,\middle|\, \|\bar{\mathbf{e}}\| = \bar{w}\right]$$

$$= Pr\left[\frac{c}{n} \in (P_{OOV}(w_{est} + \frac{1}{2}), P_{OOV}(w_{est} - \frac{1}{2})) \,\middle|\, \frac{c}{n} \xrightarrow{\mathcal{D}} \mathcal{N}(P(\bar{w}), \sigma^2)\right]$$

$$= \Phi(\frac{P_{OOV}(w_{est} - \frac{1}{2}) - P(\bar{w})}{\sigma}) - \Phi(\frac{P_{OOV}(w_{est} + \frac{1}{2}) - P(\bar{w})}{\sigma}), \quad (8)$$

Therefore, the adversary makes correct decision when $\|\bar{\mathbf{e}}\| = \bar{w}$, using n modifications, with probability $p_0(\bar{w}, \bar{w}, n)$.

After evaluating Formula (8), we have found that the weight will either be estimated as one lower (when the adversary is wrong, which is the majority of the time for the weights near the expected ones) or make a correct guess, that is, all other cases will appear with negligible probability (see Table 2). This supports the experimental findings from [25]. Table 2 shows comparison between the claimed and real precision $p_0(\bar{w}, \bar{w}, n)$ of the OOV weight estimate (see Appendix A Table A1 for details on the parameters' values). It can be noticed that, for parameter set II, in the case of Random-HB#, the claimed precision is by two orders of magnitude smaller than the claimed. In all other cases, the discrepancy is somewhat smaller but, still, the real precision is by an order of magnitude smaller than the claimed.

Table 2. Comparison of the claimed and real precision of the OOV weight estimate showing that the real precision is remarkably smaller than the claimed one.

	Parameter Set I		**Parameter Set II**	
	HB#	**Random-HB#**	**HB#**	**Random-HB#**
claimed precision $= 1 - erfc(\theta)$	0.999315	0.999997	0.998641	0.999992
real precision $= p_0(w_{exp}, w_{exp}, 4n_{w_{exp}})$	0.087803	0.031017	0.038852	0.006860
$p_0(w_{exp} - 1, w_{exp}, 4n_{w_{exp}})$	0.912197	0.968983	0.961146	0.993139

PB-OOV adversary. Since $(\frac{P(w)+P(w+1)}{2}, \frac{P(w-1)+P(w)}{2}), w = 1, \ldots, m$ is PB-w decision zone after the eavesdropping, and PB-OOV adversary uses exact values $P(w)$ instead of the approximate ones $P_{OOV}(w)$, by analogous analysis as above, we obtain that he estimates the weight as w_{est} when its actual value is $\bar{w}$ with probability:

$$p'_0(w_{est}, \bar{w}, n) = \Phi(\frac{P(w_{est}-1) + P(w_{est}) - 2P(\bar{w})}{2\sigma}) - \Phi(\frac{P(w_{est}) + P(w_{est}+1) - 2P(\bar{w})}{2\sigma})$$

Unlike the OOV weight estimate, whose precision is shown to be remarkably lower than the claimed, precision of the PB-OOV weight estimate is within the given boundaries (see Table 3). This is also confirmed by the experimental results presented in Section 5.3.

Table 3. Precision of the proposed PB-OOV algorithm meets the targeted precision for weight estimate.

	Parameter Set I		**Parameter Set II**	
	HB#	**Random-HB#**	**HB#**	**Random-HB#**
targeted precision $= 1 - erfc(\theta)$	0.999315	0.999997	0.998641	0.999992
real precision $= p'_0(w_{exp}, w_{exp}, 4n_{w_{exp}})$	0.999506	0.999998	0.998641	0.999992

4.2.2. Noise Vector Bits Recovery

Here, we compare the success rate of the OOV adversary and PB-OOV adversary when it comes to the reconstruction of noise vectors, that is, bit recovery.

OOV adversary. After the adversary has estimated the weight of the observed vector $\bar{\mathbf{e}}$ as w_{est} after eavesdropping, he tries to recover its bits by flipping one by one each bit $\bar{\mathbf{e}}_\mathbf{i}$ and estimating new weight as $w_{est} - 1$ or $w_{est} + 1$. If the weight has decreased, he concludes the flipped bit is 1, otherwise, that the bit is 0. Therefore, he recovers a bit correctly, depending on its value, with probabilities:

$$= \begin{cases} Pr\left[\frac{c}{n} \in \text{OOV Decision zone for } w_{est} - 1\right], \bar{\mathbf{e}}_\mathbf{i} = 1 \\ Pr\left[\frac{c}{n} \in \text{OOV Decision zone for } w_{est} + 1\right], \bar{\mathbf{e}}_\mathbf{i} = 0 \end{cases}$$

$$= \begin{cases} Pr\left[\frac{c}{n} > P_{OOV}(w_{est}) \,\middle|\, \frac{c}{n} \xrightarrow{\mathcal{D}} \mathcal{N}(P(\bar{w}-1), \sigma^2(\bar{w}-1, n))\right], \bar{\mathbf{e}}_\mathbf{i} = 1 \\ Pr\left[\frac{c}{n} \leq P_{OOV}(w_{est}) \,\middle|\, \frac{c}{n} \xrightarrow{\mathcal{D}} \mathcal{N}(P(\bar{w}+1), \sigma^2(\bar{w}+1, n))\right], \bar{\mathbf{e}}_\mathbf{i} = 0 \end{cases}$$

$$= \begin{cases} p_{i_1}(w_{est}, \bar{w}, n) = 1 - \Phi(\frac{P_{OOV}(w_{est}) - P(\bar{w}-1)}{\sigma(\bar{w}-1, n)}), \bar{\mathbf{e}}_\mathbf{i} = 1 \\ p_{i_0}(w_{est}, \bar{w}, n) = \Phi(\frac{P_{OOV}(w_{est}) - P(\bar{w}+1)}{\sigma(\bar{w}+1, n)}), \bar{\mathbf{e}}_\mathbf{i} = 0. \end{cases} \quad (9)$$

The results of evaluation of Formula (9) are shown in Table 4. First, it should be noted that the probability for bit recovery is very asymmetrical, that is, the precision for 0-bit recovery is very different from the precision for 1-bit, while the claimed precision is uniform for both bit values. Secondly, when the weight is correctly estimated, the precision for 0-bit is much lower than the claimed and it would make reconstruction of the noise vector (and further the key recovery itself) practically impossible. This is in accordance with the experimental results from [25]. On the other hand, the OOV adversary has more success in bits recovery when the initial weight estimate is incorrect, since the relative change remains intact if the measured weights are both one lower than the actual ones. The two errors made in the weight estimate processes can neutralize each other; however,

even with this mutual cancellation of the errors, the claimed precision is not achieved. Namely, the precision for 1-bit recovery is lower than the targeted $1 - \frac{1}{2}erfc(\theta)$ and that lowers the probability of the attack success.

Table 4. Comparison of the claimed and real precision of the OOV bit recovery depending on the initial weight estimate.

	Parameter Set I		**Parameter Set II**	
	HB#	**Random-HB#**	**HB#**	**Random-HB#**
claimed precision $= 1 - \frac{1}{2}erfc(\theta)$	0.999658	0.9999986	0.999320	0.999996
$p_{i_1}(w_{exp}, w_{exp}, n_{w_{exp}})$	$1 - 4.4 \times 10^{-9}$	$1 - 1.1 \times 10^{-15}$	$1 - 5.5\times 10^{-9}$	$1 - 7.1\times 10^{-16}$
$p_{i_1}(w_{opt}, w_{opt}, n_{w_{opt}})$	$1 - 4.6 \times 10^{-13}$	$1 - 3.9 \times 10^{-23}$		
$p_{i_0}(w_{exp}, w_{exp}, n_{w_{exp}})$	0.858089	0.930114	0.764623	0.843169
$p_{i_0}(w_{opt}, w_{opt}, n_{w_{opt}})$	0.365592	0.317990		
$p_{i_1}(w_{exp} - 1, w_{exp}, n_{w_{exp}-1})$	0.991712	0.999518	0.993508	0.999740
$p_{i_1}(w_{opt} - 1, w_{opt}, n_{w_{opt}-1})$	0.999908	$1 - 1.3 \times 10^{-7}$		
$p_{i_0}(w_{exp} - 1, w_{exp}, n_{w_{exp}-1})$	0.999997	$1 - 2.8 \times 10^{-10}$	0.999957	$1 - 2.1\times 10^{-8}$
$p_{i_0}(w_{opt} - 1, w_{opt}, n_{w_{opt}-1})$	0.998863	0.999987		

Let us further consider the probability that the OOV adversary will successfully recover a complete noise vector. We observe the expected case $\|\bar{\mathbf{e}}\| = w_{exp}$ ($= w_{opt}$ for parameter set II). As we have already noted: (a) w_{est} is either $\|\bar{\mathbf{e}}\|$ or $\|\bar{\mathbf{e}}\| - 1$, and (b) the noise vector is practically impossible to recover when $w_{est} = \|\bar{\mathbf{e}}\|$ due to too high error for 0-bit. Thus, for parameter set II, the probability of the OOV Adversary successfully recovering a complete m-bit noise vector of weight $\|\bar{\mathbf{e}}\| = w_{opt}$ is:

$$pvr(w_{exp}) = pvr(w_{opt}) = p_0 p_{i_0}^{m-w_{opt}} p_{i_1}^{w_{opt}}, \tag{10}$$

where $p_0 = p_0(w_{opt} - 1, w_{opt}, 4\theta^2 R(w_{opt}))$, $p_{i_k} = p_{i_k}(w_{opt} - 1, w_{opt}, \theta^2 R(w_{opt} - 1)), k = 0, 1$.

Similarly, for parameter set I, the adversary needs to recover and remove $\Delta = w_{est} - w_{opt}$ errors in a noise vector in order to achieve the optimal weight. This is expected to happen after recovering Δ/τ bits, thus:

$$pvr(w_{exp}) = p_0 p_{i_0}^{*w_0} p_{i_0}^{m-w_{exp}-w_0} p_{i_1}^{*\Delta} p_{i_1}^{w_{exp}-\Delta}, \tag{11}$$

where: $p_0 = p_0(w_{exp} - 1, w_{exp}, 4\theta^2 R(w_{exp}))$, $p_{i_k}^* = p_{i_k}(w_{exp} - 1, w_{exp}, \theta^2 R(w_{exp} - 1))$, $p_{i_k} = p_{i_k}(w_{opt}, w_{opt} + 1, \theta^2 R(w_{opt}))$, $k = 0, 1$, $w_0 = \frac{\Delta(1-\tau)}{\tau} = \frac{(w_{exp}-1-w_{opt})(1-\tau)}{\tau}$.

Using Formulas (10) and (11) we can evaluate the probability that the OOV adversary will correctly recover a complete noise vector in the expected case, and compare the obtained probability with the claimed one, which is calculated based on the claimed probabilities of correct weight estimate and bit guess as $(1 - erfc(\theta))(1 - \frac{1}{2}erfc(\theta))^m$. Results of the comparison are given in Table 5. Although the difference between the claimed and real precision on the noise vector level does not seem remarkable for Random-HB#, it does make a significant impact on the key recovery probability, having in mind the number of noise vector that have to be reconstructed, which is 592. More details will be provided in the next Section 4.2.3.

Table 5. Comparison of the claimed and real precision of the OOV noise vector recovery showing that the real precision is smaller than the claimed one.

	Parameter Set I		**Parameter Set II**	
	HB#	**Random-HB#**	**HB#**	**Random-HB#**
claimed precision	0.670720	0.998314	0.739967	0.998306
$pvr(w_{exp})$	0.245168	0.932141	0.573019	0.973427

PB-OOV adversary. For the PB-OOV adversary, by replacing P_{OOV} with P, and $P_{OOV}(w_{est})$ with $\frac{P(w_{est}-1)+P(w_{est}+1)}{2}$ (i.e., by using proper PB $\bar{w}$-decision zones) in the derivation above, the probabilities of successful bit recovery, depending on its value are:

$$\begin{cases} p'_{i_1}(w_{est}, \bar{w}, n) = 1 - \Phi(\frac{P(\bar{w}+1)-P(\bar{w}-1)}{2\sigma(\bar{w}-1,n)}), \bar{\mathbf{e}}_\mathbf{i} = 1 \\ p'_{i_0}(w_{est}, \bar{w}, n) = \Phi(\frac{P(\bar{w}-1)-P(\bar{w}+1)}{2\sigma(\bar{w}+1,n)}), \bar{\mathbf{e}}_\mathbf{i} = 0. \end{cases} \tag{12}$$

Table 6 shows the precision the PB-OOV adversary achieves in the bit recovery process, when the standard parameter sets are employed. The results obtained by evaluating Formula (12) prove that the PB-OOV on the bit level does achieve the targeted precision using the OOV sample (i.e., the number of modifications). This is also confirmed by the experimental results presented in Section 5.3.

Table 6. Precision of the proposed PB-OOV algorithm meets the targeted precision for bit recovery.

	Parameter Set I		**Parameter Set II**	
	HB#	**Random-HB#**	**HB#**	**Random-HB#**
targeted precision $= 1 - \frac{1}{2}erfc(\theta)$	0.999658	0.9999986	0.999320	0.999996
$p'_{i_1}(w_{exp}, w_{exp}, n_{w_{exp}})$	0.999623	0.9999983	0.999345	0.999996
$p'_{i_1}(w_{opt}, w_{opt}, n_{w_{opt}})$	0.999660	0.9999986		
$p'_{i_0}(w_{exp}, w_{exp}, n_{w_{exp}})$	0.999874	0.9999998	0.999351	0.999996
$p'_{i_0}(w_{opt}, w_{opt}, n_{w_{opt}})$	0.999659	0.9999986		

Further, we analyze the probability that the PB-OOV adversary will successfully recover a complete noise vector. We observe the expected case $\|\bar{\mathbf{e}}\| = w_{exp} (= w_{opt}$ for parameter set II). For parameter set II, the probability is given by the formula:

$$pvr'(w_{opt}) = p'_0 p'^{m-w_{opt}}_{i_0} p'^{w_{opt}}_{i_1}, \tag{13}$$

where $p'_0 = p'_0(w_{opt}, w_{opt}, \theta^2 R w_{opt})), p'_{i_k} = p'_{i_k}(w_{opt}, w_{opt}, \theta^2 R(w_{opt})), k = 0, 1.$

Similarly, for parameter set I, we have that:

$$pvr'(w_{exp}) = p'_0 p'^{*w_0}_{i_0} p'^{m-w_{exp}-w_0}_{i_0} p'^{*\Delta}_{i_1} p'^{w_{exp}-\Delta}_{i_1} \tag{14}$$

where $p'_0 = p'_0(w_{exp}, w_{exp}, 4\theta^2 R(w_{exp})), p'^{*}_{i_k} = p'_{i_k}(w_{exp}, w_{exp}, \theta^2 R(\bar{w}_{exp})), p'_{i_k} = p'_{i_k}(w_{opt}, w_{opt}, \theta^2 R(\bar{w}_{opt})), k = 0, 1, w_0 = \frac{\Delta(1-\tau)}{\tau} = \frac{(w_{exp}-w_{opt})(1-\tau)}{\tau}$.

Using Formulas (13) and (14), we can evaluate the probability that the PB-OOV adversary will correctly recover a complete noise vector in the expected case. Table 7 shows the results of this evaluation, which confirm that the PB-OOV attack does meet the targeted precision.

Table 7. Precision of the proposed PB-OOV algorithm meets the targeted precision for noise vector recovery.

	Parameter Set I		**Parameter Set II**	
	HB#	**Random-HB#**	**HB#**	**Random-HB#**
claimed precision	0.670720	0.998314	0.739967	0.998306
$pvr'(w_{exp})$	0.698279	0.998538	0.749770	0.998443

4.2.3. Secret Keys Recovery Comparison

Finally, let us compare the precision of the OOV attack and PB-OOV attack. We observe the expected case $\bar{w} = w_{exp} (= w_{opt}$ for parameter set II). Let l be the number of secret bits, that is, secret key length and m be the noise vector length. The claimed probability of key recovery in [12] is calculated as $ckr = (1 - erfc(\theta))^{\lceil \frac{l}{m} \rceil}(1 - \frac{1}{2}erfc(\theta))^{l}$. This probability is equal 0.37.

As we have shown in Section 4.2.2, the PB-OOV attack achieves the claimed precision on bit level, therefore it can recover the secret key with probability 0.37. Let us further compare this value with the probability that the OOV adversary recovers the key. In the case of Random-HB#, the number of secret bits is $l = (k_x + k_y)m$ and the adversary has to recover $k_x + k_y = 592$ complete noise vectors of length m. The probability of a key recovery can be calculated using the values from Table 5 as $pvr(w_{exp})^{592}$. For parameter set I, the probability of key recovery is 8.6×10^{-19}, and for parameter set II, it is equal 1.2×10^{-7}. This is remarkably smaller than the claimed 0.37. In the case of HB#, the adversary has to recover $\lfloor \frac{l}{m} \rfloor$ complete noise vectors and additional $l \mod m$ bits. For parameter set I, the probability of key recovery for HB# is 0.024, and for parameter set II, it is 0.159.

More formally, the OOV attack reconstructs the secret keys if it recovers:

- $\lfloor \frac{l}{m} \rfloor$ whole m-bit noise vectors—which happens with probability $pvr(\bar{w})^{\lfloor \frac{l}{m} \rfloor}$,
- and then the remaining $l \mod m$ bits, by guessing incorrectly one more noise vector weight, and recovering each one of them—which happens with probability $pvrest(\bar{w}) = p_0 p_{i_1}^{(l \mod m)\tau} p_{i_0}^{(l \mod m)(1-\tau)}$ for parameter set II and $pvrest(\bar{w}) = p_0^* p_{i_1}^{*\Delta} p_{i_0}^{*\frac{\Delta(1-\tau)}{\tau}} p_{i_1}^{(l \mod m - \frac{\Delta}{\tau})\tau} p_{i_0}^{(l \mod m - \frac{\Delta}{\tau})(1-\tau)}$ for parameter set I, since $\frac{\Delta}{\tau} < l \mod m$.

Therefore, the probability of successful recovery of secret keys using OOV attack will be:

$$Pr[\text{OOV-Attack success}] = pvr(\bar{w})^{\lfloor \frac{l}{m} \rfloor} pvrest(\bar{w}) \tag{15}$$

and similarly, probability of successful recovery of secret keys using PB-OOV attack is:

$$Pr[\text{PB-OOV-Attack success}] = pvr'(\bar{w})^{\lfloor \frac{l}{m} \rfloor} pvrest'(\bar{w}), \tag{16}$$

where $pvrest'$ is the same as $pvrest$, but with symbols p' instead of p.

Complexity comparison. The complexity of the OOV attack needed to achieve the required (claimed) key recovery rate is $Compl^{OOV} = \underset{n}{\text{argmin}}\{Pr[\text{OOV-Attack success}](n) \geq ckr\}$. By increasing the number of modifications n until the claimed key recovery rate is reached, we have estimated that the complexity of the OOV attack is higher than the claimed—for parameter set II by 55% in the case of Random-HB# and by 18% for HB# (this supports the results from [25] based on experimental evaluation), and for parameter set I by 150% in the case of Random-HB# and 35% for HB#. On the other hand, since the PB-OOV attack achieves the required precision on a bit recovery level targeted in [12], its precision and complexity is in accordance with the one claimed for the original OOV attack.

5. Experimental Results and Discussion

5.1. Evaluation of the Acceptance Rates

We have conducted a set of experiments to confirm the convergence of experimentally obtained acceptance rates to the corresponding PB values. There were 4 rounds of tests, for $n = 2500$, $n = 5000$, $n = 10{,}000$ and $n = 15{,}000$. For each n, we generated 500 noise vectors and flipped the appropriate number of their last bits, so that the expected weight of the noise vectors is optimal, that is, 78. For each test vector e_i, we measured the acceptance rate and analyzed how it relates to $P_{OOV}(\|e_i\|)$ and $PB(\|e_i\|)$. In general, it can be noted that the experimental acceptance rates lie above the corresponding OOV points, but compared to the corresponding PB points, they are evenly distributed above and bellow (see Figure 11). It can also be noticed that as n increases, the experimental points concentrate around the PB points, as expected. This further explains and confirms that the OOV algorithm relaying on the OOV approximation has high error rate when it comes to weight estimate, while the corrected PB-OOV algorithm gives much better results.

Furthermore, we compare experimentally obtained acceptance rates $\frac{c(e_i)}{n}$ with OOV and PB reference points, i.e., $P_{OOV}(\|e_i\|)$ and $PB(\|e_i\|)$, using a standard error measure—Mean absolute error (MAE), and show how it relates to the correctness of weight estimates. That is, for a set $\{e_i\}_{i=1}^{N}$ of test noise vectors, we observe the MAE between the acceptance rates $\frac{c(e_i)}{n}$, where n is the number of intercepted authentication sessions (i.e., modifications), and $P_{OOV}(\|e_i\|)$ and $PB(\|e_i\|)$:

$$Avg\_dist_n^{OOV} = \frac{1}{N}\sum_{i=1}^{N}|\frac{c(e_i)}{n} - P_{OOV}(\|e_i\|)|,$$

$$Avg\_dist_n^{PB} = \frac{1}{N}\sum_{i=1}^{N}|\frac{c(e_i)}{n} - PB(\|e_i\|)|.$$

From the previous theoretical analysis given in Section 4.1, we have that $\frac{c(e_i)}{n} \xrightarrow[n\to\infty]{} PB(\|e_i\|), i = 1, \ldots, N$. Therefore:

$$Avg\_dist_n^{OOV} \xrightarrow[n\to\infty]{} \frac{1}{N}\sum_{i=1}^{N}|PB(\|e_i\|) - P_{OOV}(\|e_i\|)|,$$

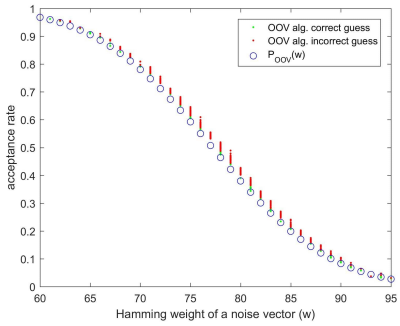
$$Avg\_dist_n^{PB} \xrightarrow[n\to\infty]{} 0.$$

Consequently, the expected MAE value for the OOV points, across all possible weights $\|e_i\|$, as $n \to \infty$, converges to:

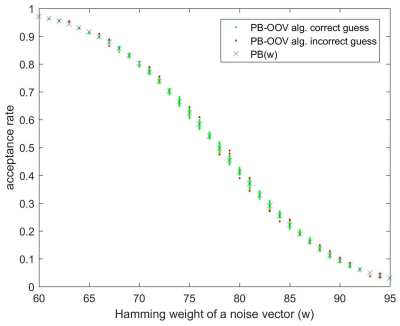
$$E(Avg\_dist_\infty^{OOV}) = \frac{1}{N}\sum_{i=1}^{N}\sum_{w=1}^{m}|PB(w) - P_{OOV}(w)|(PB(f,m,\tau,w) - PB(f,m,\tau,w-1)),$$

since $Pr[\|e_i\| = w] = PB(f,m,\tau,w) - PB(f,m,\tau,w-1)$, after flipping f last bits in e_i, while for the PB points they converge to: $E(Avg\_dist_\infty^{PB}) = 0$.

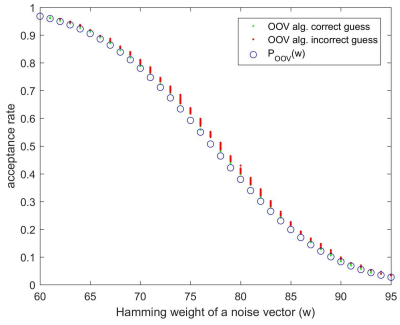
This is in accordance with the experimental results shown in Figure 12, for different number of modifications n. Furthermore, Figures 12 and 13 show that there is an inverse correlation between the distance (between the experimental and OOV points, i.e., PB points, respectively) and the accuracy of weight estimation.



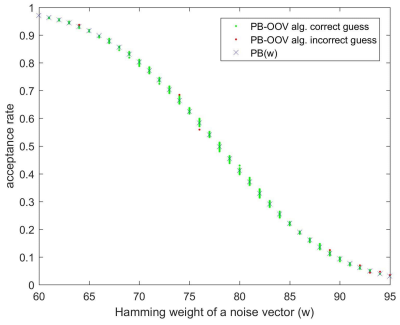
(**a**) OOV alg. and $n = 2500$



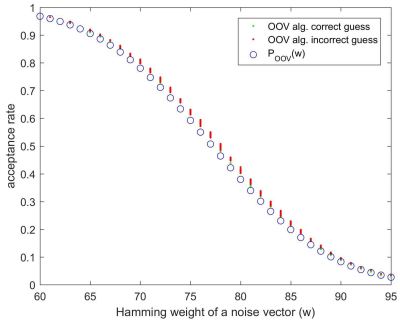
(**b**) PB-OOV alg. and $n = 2500$



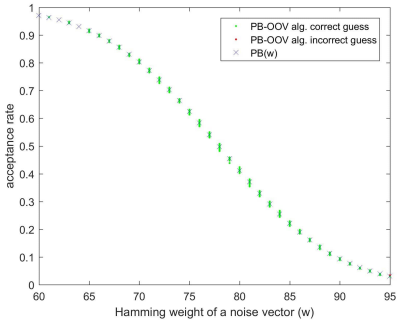
(**c**) OOV alg. and $n = 5000$



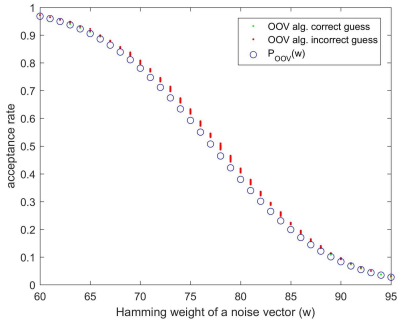
(**d**) PB-OOV alg. and $n = 5000$



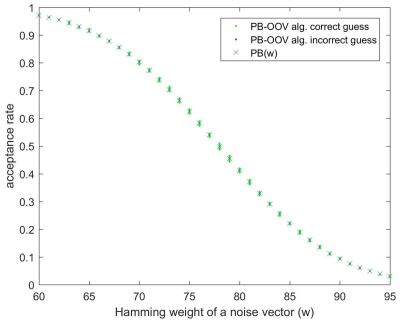
(**e**) OOV alg. and n = 10,000



(**f**) PB-OOV alg. and n = 10,000



(**g**) OOV alg. and n = 15,000



(**h**) PB-OOV alg. and n = 15,000

Figure 11. Comparison of the experimentally obtained acceptance rates and the corresponding $P_{OOV}(\|e_i\|)$ and $PB(\|e_i\|)$ points for n = 2500, 5000, 10,000, 15,000.

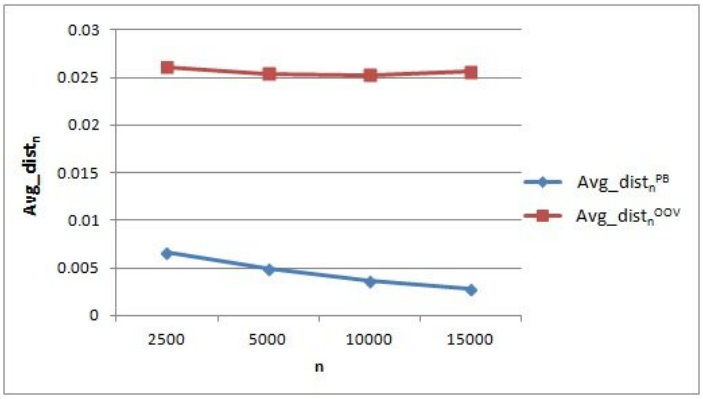


Figure 12. MAE between the experimentally obtained acceptance rates and the OOV and PB points, respectively, for n = 2500, 5000, 10,000 and 15,000.

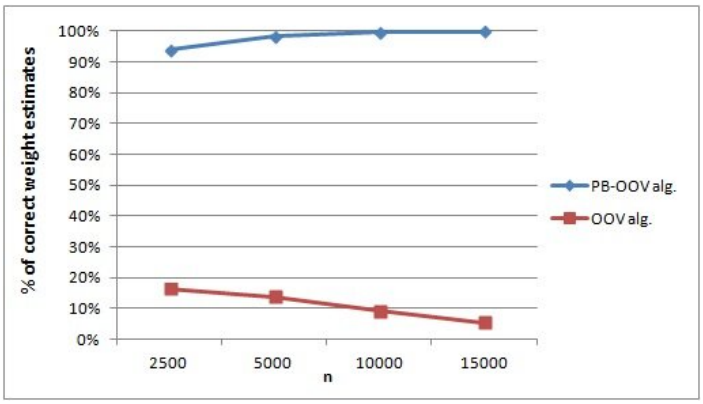
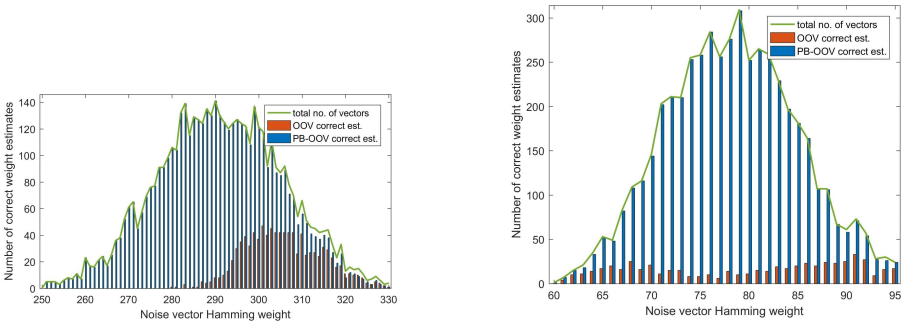


Figure 13. Percentage of correct weights estimates based on acceptance rates using the PB distribution and OOV approximation respectively, for n = 2500, 5000, 10,000 and 15,000.

5.2. Precision Comparison of the OOV and PB-OOV Weight Estimate: Experimental

Here, the differences in the weight estimate quality between the original OOV Algorithm 1 and the PB-OOV Algorithm 1 proposed in Section 4.1 are experimentally proven. We have analyzed and compared effectiveness of the two algorithms for different Hamming weights. For the standard parameter set I, 99% of all noise vectors have the weight between 250 and 330. The comparison of the algorithms is based on the sample of 5000 noise vectors whose Hamming weight is from that interval. The number of modifications employed for weight estimation corresponds to the HB# scenario. The success rate of the OOV algorithm is 20% and for the PB-OOV it is 98%. Detailed results are given in Figure 14a. For the standard parameter set II, 99% of all noise vectors have the weight between 60 and 95 (this is after flipping $(w_{opt} - m\tau)/(1 - 2\tau)$ bits to obtain a vector of the optimal weight from a vector of the expected weight) and the comparison of the two algorithms is based on the sample of 5000 noise vectors with the Hamming weight in this interval. The number of modifications employed for weight estimation corresponds to the HB# scenario. The experimental results again show that the success rate of the OOV algorithm is much worse than PB-OOV (11% in contrast to 99%). Details are given in Figure 14b.



(**a**) Standard parameter set I (**b**) Standard parameter set II

Figure 14. Precision comparison of the weight estimate using the OOV and PB-OOV algorithms.

5.3. Evaluation of the PB-OOV Attack Precision

In Section 2.1 from [12], the authors derive the error formula and calculate the number of modifications n that should provide the aimed accuracy of the OOV attack, that is, of the weight estimate and bit recovery. However, the analysis given in Section 4.2 shows that the precision deviates significantly from the one claimed. The analysis provides the theoretical proof that supports the experimental findings presented in [25]. On the other hand, the analysis of the proposed PB-OOV algorithm given in Section 4.2, shows that this algorithm does achieve the desired precision and efficiency. We have conducted a series of experiments in order to experimentally verify the correctness of the PB-OOV attack. The experimental results presented in this section support the conclusions of the theoretical analysis.

The tests are conducted for both HB# and Random-HB# protocols and parameter set II. The number of modifications used ("sample size") is the one from the [12]. For the HB# protocol we have tested the weight estimate and bit recovery precision for 2000 randomly generated noise vectors of the optimal weight. The weights of two noise vector were incorrectly estimated as 79, since the obtained acceptance rates were 0.473227 and 0.475217. This gives success rate of 0.999 in weight estimation step. When the weight of a vector is incorrectly guessed, it further causes high error rate in the bit recovery process, since the algorithm relies on the initial weight estimate w_{est} and chooses between $w_{est} - 1$ and $w_{est} + 1$ after flipping the observed bit. However, when the weight estimate is correct, targeted bit precision is $1 - \frac{1}{2}erfc(\theta)$, and our tests verify that the PB-OOV attack complies with this. Namely, in the set of noise vectors whose weight is correctly estimated, the average bit guessing success rate in our test is 0.999342, compared to the targeted 0.999320. For Random-HB#, we have randomly generated 25,000 noise vectors of the optimal weight. The PB-OOV attack correctly estimated all weights, while the achieved average bit guessing success rate was 0.999996, which is in line with the targeted precision. An interesting finding regarding the OOV attack is that the bit guessing precision may significantly differ for 0-bits and 1-bits, for example, in the case of HB# and parameter set II, precision for 0-bit is 0.764623, while for 1-bit it is remarkably higher and equal $1 - 5.5 \times 10^{-9}$ (see Table 4). On the other hand, the proposed PB-OOV algorithm does not have this strong and distinct bias. Table 8 summarizes the results of the tests.

Table 8. PB-OOV experimentally obtained precision.

	HB#	**Random-HB#**
num. tests	2000	25,000
targeted OOV weight est. precision $= 1 - erfc(\theta)$	0.998641	0.999992
experimentally obtained weight est. precision	0.999	1
targeted OOV bit precision $= 1 - \frac{1}{2}erfc(\theta)$	0.999320	0.999996
experimentally obtained avg. bit precision	0.999342	0.999996
experimentally obtained 0-bit precision	0.999344	0.999996
experimentally obtained 1-bit precision	0.999333	0.999995

6. Conclusions

This paper provides a detailed examination of the OOV attack reported in [12] against the LPN based authentication protocols known as HB# and Random-HB#. We have found that the problem of discrepancy between the theoretically estimated performances and complexity in [12] and the experimentally evaluated ones in [25] arises from non-Bayesian reasoning with inadequate approximations of the probability distributions on the acceptance rates during the attack, which can not be improved due to the limitations of Central limit theorem use in the attack context. We give a correction of the attack by employing proper, Bayesian inference after establishing the exact underlying probability distributions, and prove that the new version of the attack, unlike the original one, achieves the targeted precision and complexity.

Since the OOV attack is recognized as one of the cornerstones in the analysis of any HB-like authentication protocol, our correction of the OOV attack is not only significant against Random-HB# and HB#, but also for practical security analysis of all new members of the HB-family. An interesting future direction could be a design of improved MIM attacks against HB-like protocols, which could be based on the corrected version of the OOV attack proposed in this paper.

Author Contributions: Conceptualization, S.T., M.K. and M.J.M.; formal analysis, S.T. and M.K.; funding acquisition, S.T., M.K. and M.J.M.; investigation, S.T., M.K.; methodology, S.T., M.K., and M.J.M.; software, M.K., S.T.; validation, S.T. and M.K.; writing—original draft, S.T., M.K. and M.J.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been supported by the Ministry of education, science and technological development, Government of Serbia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Parameters' values used in the OOV and PB-OOV attack.

	Parameter Set I		Parameter Set II	
	HB#	**Random-HB#**	**HB#**	**Random-HB#**
θ	2.401	3.308	2.265	3.164
$R(w_{exp})$	16,780.41 *		269.39	
$R(w_{opt})$	2742.61			
$R(w_{exp}-1)$	15,789.60		270.95	
$R(w_{opt}-1)$	2743.75			
$n_{w_{exp}} = \theta^2 R(w_{exp})$	96,736	183,626	1382	2697
$n_{w_{opt}} = \theta^2 R(w_{opt})$	15,811	30,012		
$n_{w_{exp}-1} = \theta^2 R(w_{exp}-1)$	91,024	172,783	1390	2712
$n_{w_{opt}-1} = \theta^2 R(w_{opt}-1)$	15,817	30,024		

* R_{exp} is calculated using Formula (2) from the OOV paper [12].

References

1. Avoine, G.; Carpent, X.; Hernandez-Castro, J. Pitfalls in ultralightweight authentication protocol designs. *IEEE Trans. Mob. Comput.* **2015**, *15*, 2317–2332 [CrossRef]
2. Baashirah, R.; Abuzneid, A. Survey on prominent RFID authentication protocols for passive tags. *Sensors* **2018**, *18*, 3584. [CrossRef] [PubMed]
3. D'Arco, P. Ultralightweight cryptography. In *International Conference on Security for Information Technology and Communications*; Springer: Cham, Switzerland, 2018; pp. 1–16.
4. Hopper, N.J.; Blum, M. Secure Human Identification Protocols. In *Advances in Cryptology—ASIACRYPT 2001. ASIACRYPT 2001. Lecture Notes in Computer Science*; Boyd, C., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2248.
5. Katz, J.; Shin, J.S. Parallel and Concurrent Security of the HB and HB$^+$ Protocols. In *Advances in Cryptology—EUROCRYPT 2006. EUROCRYPT 2006. Lecture Notes in Computer Science*; Vaudenay, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4004.
6. Katz, J.; Shin, J.S.; Smith, A. Parallel and concurrent security of the HB and HB+ protocols. *J. Cryptol.* **2010**,*23*, 402–421. [CrossRef]
7. Gilbert, H.; Robshaw, M.; Sibert, H. Active attack against HB+: A provably secure lightweight authentication protocol. *Electron. Lett.* **2005**, *41*, 1169–1170. [CrossRef]
8. Bringer, J.; Chabanne, H.; Dottax, E. HB++: A Lightweight Authentication Protocol Secure against Some Attacks. In Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06), Lyon, France, 29 June 2006; IEEE Computer Society: Washington, DC, USA, 2006; pp. 28–33.
9. Munilla, J.; Peinado, A. HB-MP: A further step in the HB-family of lightweight authentication protocols. *Comput. Netw.* **2007**, *51*, 2262–2267. [CrossRef]
10. Gilbert, H.; Robshaw, M.J.; Seurin, Y. Good variants of HB+ are hard to find. In *Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 156–170.
11. Gilbert, H.; Robshaw, M.J.B.; Seurin, Y. HB#: Increasing the Security and Efficiency of HB$^+$. In *Advances in Cryptology—EUROCRYPT 2008. Lecture Notes in Computer Science*; Smart, N., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; Volume 4965.
12. Ouafi, K.; Overbeck, R.; Vaudenay, S. On the Security of HB# against a Man-in-the-Middle Attack. In *Advances in Cryptology—ASIACRYPT 2008. Lecture Notes in Computer Science*; Pieprzyk, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5350.
13. Leng, X.; Mayes, K.; Markantonakis, K. HB-MP+ protocol: An improvement on the HB-MP protocol. In Proceedings of the 2008 IEEE International Conference on RFID, Las Vegas, NV, USA, 16–17 April 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 118–124.
14. Yoon, B.; Sung, M.Y.; Yeon, S.; Oh, H.S.; Kwon, Y.; Kim, C.; Kim, K.H. HB-MP++ protocol: An ultra lightweight authentication protocol for RFID system. In Proceedings of the 2009 IEEE International Conference on RFID, Orlando, FL, USA, 27–28 April 2009; IEEE Computer Society: Washington, DC, USA, 2009; pp. 186–191.
15. Aseeri, A.; Bamasak, O. HB-MP*: Towards a Man-in-the-Middle-Resistant Protocol of HB Family. In *2nd Mosharaka International Conference on Mobile Computing and Wireless Communications (MIC-MCWC 2011)*; Mosharaka for Research and Studies: Amman, Jordan, 2011; Volume 2, pp. 49–53.
16. Bringer, J.; Chabanne, H. Trusted-HB: A low-cost version of HB+ secure against man-in-the-middle attacks. *IEEE Trans. Inf. Theory* **2008**, *54*, 4339–4342. [CrossRef]

17. Madhavan, M.; Thangaraj, A.; Sankarasubramanian, Y.; Viswanathan, K. NLHB: A non-linear HopperBlum protocol. In Proceedings of the 2010 IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 2498–2502.
18. Bosley, C.; Haralambiev, K.; Nicolosi, A. HB^N: An HB-like protocol secure against man-in-the-middle attacks. *IACR Cryptol. ePrint Arch.* **2011**, *2011*, 350.
19. Rizomiliotis, P.; Gritzalis, S. GHB#: A provably secure HB-like lightweight authentication protocol. In *International Conference on Applied Cryptography and Network Security*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 489–506.
20. Hammouri, G.; Öztürk, E.; Birand, B.; Sunar, B. Unclonable lightweight authentication scheme. In *International Conference on Information and Communications Security*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 33–48.
21. Hammouri, G.; Sunar, B. PUF-HB: A tamper-resilient HB based authentication protocol. In *International Conference on Applied Cryptography and Network Security*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 346–365.
22. Deng, G.; Li, H.; Zhang, Y.; Wang, J. Tree-LSHB+: An LPN-based lightweight mutual authentication RFID protocol. *Wirel. Pers. Commun.* **2013**, *72*, 159–174. [CrossRef]
23. Qian, X.; Liu, X.; Yang, S.; Zuo, C. Security and privacy analysis of tree-LSHB+ protocol. *Wirel. Pers. Commun.* **2014**, *77*, 3125–3314. [CrossRef]
24. Karrothu, A.; Scholar, R.; Norman, J. An analysis of LPN based HB protocols. In Proceedings of the 2016 Eighth International Conference on Advanced Computing (ICoAC), Chennai, India, 19–21 January 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 138–145.
25. Knežević, M.; Tomović, S.; Mihaljević, M.J. Man-In-The-Middle Attack against Certain Authentication Protocols Revisited: Insights into the Approach and Performances Re-Evaluation. *Electronics* **2020**, *9*, 1296. [CrossRef]
26. Koralov, L.; Sinai, Y.G. *Theory of Probability and Random Processes*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 131–134.
27. Shiganov, I.S. Refinement of the upper bound of the constant in the central limit theorem. *J. Math. Sci.* **1986**, *35*, 2545–2550. (translated from *Stab. Probl. Stoch. Models* **1982**, 105–115.) [CrossRef]
28. Shevtsova, I.G. An improvement of convergence rate estimates in the Lyapunov theorem. *Dokl. Math.* **2010**, *82*, 862–864. [CrossRef]