# VARIANTS OF HB PROTOCOLS FOR RFID SECURITY

**S. A. Ali [*], M. Hardan**

*Electrical Engineering Department, Faculty of Engineering, Assiut University*

Received 18 March 2013, accepted 7 April 2013

## ABSTRACT

Radio Frequency Identification (RFID) has received recently a great attention from large organizations and researchers due to the dropping tag costs and vigorous RFID standardization. They are becoming more common in daily use to identify, locate and track people, assets, and animals. Number of protocols has been proposed in the literature for the security of RFID against passive attacks. One of the well-known protocols is the HB family protocol which utilizes the complexity of decoding linear codes for RFID security against passive attacks. The nonlinear HB (NLHB) is one member of the HB family protocol which achieves high security by reducing the provably hard problem of decoding a class of nonlinear codes to passive attacks. This paper introduces Multi-Nonlinear Stages to the HB protocol to enhance its security against passive attacks. More specifically, the paper presents two Multi-Nonlinear versions of the HB protocol; Double-Nonlinear HB (DNLHB), and Triple-Nonlinear HB (TNLHB). The proposed protocols increase significantly the security of RFID systems against passive attacks at a lower implementation cost.

*Keywords:*HB family protocols, NLHB protocol, LPN problem, secure and efficient authentication protocol, passive attacks, RFID tags.

## 1. Introduction

RFID (Radio Frequency Identification) tags are small wireless devices that track objects in supply chains. They are working their way into the pockets, belongings and even the bodies of consumers. RFID is a technology for automated identification of physical entities using radio frequency transmissions. Typically, RFID systems consist of simple, low-cost tags that are attached to physical objects, and powerful readers that queue data from these tags. Billions of tags have been deployed; tens of billions are on their way, making RFID tags one of the most pervasive microchips in recent history [1]. The RFID can be used in many applications such as auto-makers, animal tracking, asset tracking in hospitals and pharmacies, Contactless payments such as American Express, Supply chain like Wal-Mart, etc. The low production cost of those pervasive devices is one of the reasons for the wide use in many application systems [2].

Security and privacy play important roles in the prevalence of RFID systems. Efficient authentication protocols are the natural approaches to address the counterfeiting problem, which imposes a serious threat to those low-cost pervasive computing devices. These devices, which lack the computation, storage, energy, and communication capacities necessary for most cryptographic authentication schemes, call for light-weight authentication approaches [3].

The HB protocol was first proposed in 2001 by Hopper and Blum [4]. It was modified by Juels and Weis in 2005 to include protection against active attacks from adversaries, it

* Corresponding author.

*E-mail address:* samya.hassan@eng.au.edu.eg, samia_fattah@yahoo.com

is called HB+ [5]. However, the HB+ protocol too was not completely secure for certain circumstances. Later in 2006, Bringer et al. modified the HB+ protocol to improve its security against active attacks with the HB++ protocol [6]. Also, Gilbert et al. have enhanced the security of the HB+ protocol with the introduction of the HB# protocol in 2008 [7]. Madhavan et al. in 2010 have upgraded the HB protocol to increase its security against passive attacks with the NLHB protocol by adding a single nonlinear stage to the coding process [8].

The principle assumption of the HB family protocols is that the reader and the tag share a secret key(s) that is (are) unknown for any other component in the system. The main weakness of the HB family protocols is the Learning from Parity with Noise (LPN) problem. In the literature, there exist many algorithms to solve the LPN problem to find the secret key(s) [9]. The NLHB protocol has added a single stage of non-linear stage to enhance the resistance to known passive attacks on the HB family protocols. The introduction of the nonlinearity stage by the NLHB protocol has resulted in higher key efficiency and cheaper implementation than the HB protocol. This is due to the decrease in the tag/reader coding process stage of the HB protocol by reducing the secret key size [10].

This paper proposes the concept of multi-nonlinear HB protocols, namely; Double Nonlinear HB (DNLHB) which imposes two nonlinear stages, and Triple Nonlinear HB (TNLHB) which introduces three nonlinear stages over the HB protocol. Theoretical analysis and experimental results illustrate that these proposed protocols outperform similar protocols in terms of efficiency and complexity. The main contribution of this paper is a low-cost, provably secure extension of the NLHB protocol with multiple stages of non-linear functions on parties. Increasing the security against passive attacks by increasing the degree of nonlinear stages introduced which resulted in higher key efficiency and cheaper implementations. Moreover, entropy derivation and its effect on the errors of the attacking algorithms which enhanced the security level of the proposed protocols are given.

This paper is organized as follows: the LPN problem is described in section 2. The NLHB protocol is introduced in section 3 and the nonlinear function used for encoding and its properties are presented in section 4. The proposed protocols and their implementation are described in section 5, while the experimental results of the proposed protocols versions are given in section 6. The presented work is concluded in section 7.

## 2. Learning Parity in the presence of Noise (LPN)

The LPN Problem, in machine learning theory, is described in the uniform distribution model where the algorithm only has access to a source of random samples. The LPN problem is an average-case version of the following problem: given a set of equations over a Generation Function, GF(2) find a vector S that maximally satisfies the given set of equations. This problem has been known as the decoding of a random linear code and has been proven to be NP-hard by Berlekamp et al. [12]. In the LPN problem, the instances (set of equations and values) may not represent the worst case of the problem, but studies of the average-case hardness of this problem have been presented in [4, 9, 13]. The LPN problem may also be formulated and referred to as the Minimum Disagreement Problem, or the problem of finding the closest vector to a random linear error-correcting code; also known as the syndrome decoding problem [3].

*Definition 1: LPN Problem*

Let A be a random N × K binary matrix, S be a random K-bit vector, ε ∈ ]0, ½[ be a constant noise parameter, and ν be a random q-bit vector such that |ν| ≤ ε N. Given A, ε, and Z = (S.A) ⊕ ν, find a K-bit vector X such that |(X.A)⊕ Z| ≤ ε N [9, 10, 12, 14].

The best known algorithm to solve random LPN instances is due to Blum, Kalai and Wasserman, and has a sub-exponential runtime of $2^{o\left(\frac{k}{\log k}\right)}$ [3]. All the HB family of protocols achieved the hardness of the Learning Parity in the Presence of Noise (LPN) problem. Some protocols produced two responses from a tag for the same reader response (HB-CM) [4], while others used nonlinear functions (NLHB) [15], etc. The HB family of protocols relied on a secret key(s) shared only between the tag and the reader. The LPN problem involves finding a vector X such that: |(A·X) + Z| ≤ εN, where Z represents a N×1 vector which is the response of the tag and A is a N × K matrix send by the reader to the tag [9, 10, 16, 17]. The LPN problem can be summarized as given A, ε, and Z an attacker is able to recover X.

## 3. The NLHB protocol

All the HB family of protocols depends upon the complexity of decoding linear codes for security against passive attacks. In contrast, security for the Nonlinear HB (NLHB) protocol is achieved by reducing the provably hard problem of decoding a class of nonlinear codes to prevent passive attacks. Figure 1 presents one session of the NLHB protocol. Here A is a K × n matrix, S is a K ×1 vector, and V is a D ×1vector, where D=n-p and p is the degree of the nonlinear function f. In this protocol, the Prover (tag) and Verifier (reader) share a K-bit secret key S. The Verifier transmits a random K × n challenge matrix A to the Prover. Upon receiving A, the Prover computes f (S.A), and then computes $Z = f(S.A) \oplus V$. The vector V is a noise-vector whose bits are all independently distributed according to Bernoulli distribution with parameter ε, similar to the noise vector in the HB protocol [18]. Here S.A is an N-bit vector and Z is a D-bit vector and D has to be large enough (~1000) and ε < έ <1/2. The triplet (D, ε, έ) has to meet the conditions satisfied by the HB protocol parameters (N, ε, έ) [19].Then upon the receiving of Z, the Verifier checks whether d (Z, *f* (S.A)) ≤ έ D where d (.) is the Hamming distance. The verifier returns “Accept” if and only if its check on the Prover response is true.

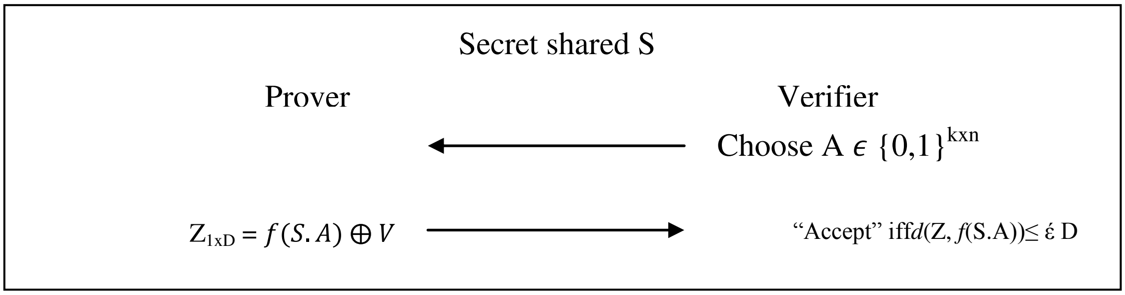
Secret shared S
Prover
Verifier
Choose A $\epsilon$ $\{0,1\}^{kxn}$
$Z_{1xD} = f(S.A) \oplus V$
“Accept” iff$d$(Z,$f$(S.A))≤ έ D

**Fig. 1.**Parallelized Version of the NLHB protocol.

## 4. The nonlinear function *f*

The main difference between the HB family of protocols and the NLHB family of protocols is the nonlinearity added through a nonlinear function applied to the Prover's response. The construction foundation of the nonlinear function f is presented in this section. Each bit yi; i∊ [1;….;D] of the output y = f(x); y∊{0,1}D; x∊ {0,1}n is computed as:

$$y_i = x_i + g([x_{i+1}; \ldots.; x_{i+p}]) \quad (1)$$

Where xi is the ith-bit of x and g: {0, 1}p⇒ {0,1} is a Boolean function composed of only nonlinear terms. The main properties of this class of nonlinear functions are given in [11, 17, 19] and summarized as follows:

$$f: \{0,1\}^n \Rightarrow \{0,1\}$$

*f* is a nonlinear function, for a uniformly distributed x$\epsilon\{0,1\}^n$, f(x) is uniformly distributed in $\{0,1\}^D$. To prove that f(x) is uniformly distributed in $\{0,1\}^D$, first it has to be proven that each bit of the output probability is balanced. Let the probability of yi = 1 be abbreviated as Pr [yi=1].

$$\text{Pr [yi} = 1] = \Pr[x_i + g(x_{i+1}, \ldots \ldots \ldots., x_{i+p}) = 1] \quad (2)$$

$$= \frac{1}{2}\Pr[g(x_{i+1}, \ldots \ldots \ldots., x_{i+p}) = 1|x_i = 0]$$

$$+ \frac{1}{2}\Pr[g(x_{i+1}, \ldots \ldots \ldots., x_{i+p}) = 0|x_i = 1] \quad (3)$$

Since the input vector is uniform, the bits of x are independent, therefore;

$$\Pr[y_i = 1] = \frac{1}{2}\Pr[g(x_{i+1}, \ldots \ldots \ldots., x_{i+p}) = 1] + \frac{1}{2}\Pr[g(x_{i+1}, \ldots \ldots \ldots., x_{i+p}) = 0] = \frac{1}{2} \quad (4)$$

Thus each bit of the output y is balanced. Now, let $y^i = [y^{D-i+1}, .., y^D]$to be the vector containing the last I bits of y (i.e.$y^D$ = y). Similarly, let $a = [a^1, \ldots, a^D]$be an arbitrary constant D-bit vector and $a^i = [a^{D-i+1}, .., a^D]$. Now consider the probability,$\Pr[y^D = a^D]$. Generalizing the above balance property gives:

$$\Pr[y^D = a^D] = \frac{1}{2^D}. \quad (5)$$

Some examples for such a class of nonlinear functions that satisfies the above properties are shown in Table1.

**Table1.**
Examples for nonlinear functions satisfying balance property.

| | Function | Degree |
|---|---|---|
| 1 | $y_i = x_i \oplus x_{i+1}x_{i+2}$ | 2 |
| 2 | $y_i = x_i \oplus x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1}$ | 3 |
| 3 | $y_i = x_i \oplus x_{i+1}x_{i+2} \oplus x_{i+3}x_{i+1}$ | 3 |
| 4 | $y_i = x_i \oplus x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+4}$ | 4 |

The uniform distribution property for p = 3 can be readily verified by exhaustively determining the joint distribution of $\{y_i, y_{i+1}, y_{i+2}, y_{i+3}\}$ for a fixed i. When p is set to be three, the function f takes an n-bit vector x and maps it onto a D = (n − 3) bit response vector. As it easily can be seen that members of this family similar to the ones described in table 1 of the third degree, p=3, require for implementation only three AND gates and three XOR gates. Therefore, these types of nonlinear functions are easily accommodated into any RFID system tags.

## 5. The proposed protocols

This paper proposes a Multi-Nonlinear HB (MNLHB) family of protocols. The main idea of the proposed family of protocols is the addition of two or more stages of nonlinear functions over the HB protocol. This has the effect of increasing the complexity of the decoding process which in turn hardens the passive attacker job. The proposed protocols achieve higher security at smaller key sizes against normal passive attacks such as BKW, LF1, LF2, and novel [10, 20, 21] as well as special nonlinear passive attack as the equivalent HB attack [22].

In this paper two types of multi-nonlinear HB protocols are presented; Double Nonlinear HB (DNLHB) protocol which added one more nonlinear stage over the NLHB, and Triple Nonlinear HB (TNLHB) protocol which added another nonlinear stage over the DNLHB protocol. The added stages of nonlinearity may be of the same degree or different degrees. The two cases will be discussed in this paper. Three different versions for the DNLHB protocol are treated. In the first version, the two nonlinear stages have an equal degree of three. In the second version, the degree of the latter nonlinear stage is one higher than the degree of the first stage. While, in the last version the degree of the latter nonlinear stage is one less than the degree of the first stage. The TNLHB protocol versions are constructed by adding one more stage of nonlinearity on top of the prescribed DNLHB protocol versions.

### *5.1. DNLHBprotocol versions*

The DNLHB protocol is based on the NLHB protocol [11] with one more stage of nonlinearity on its top to increase the efficiency against passive attacks. Figure 2 shows one session of the proposed DNLHB protocol.

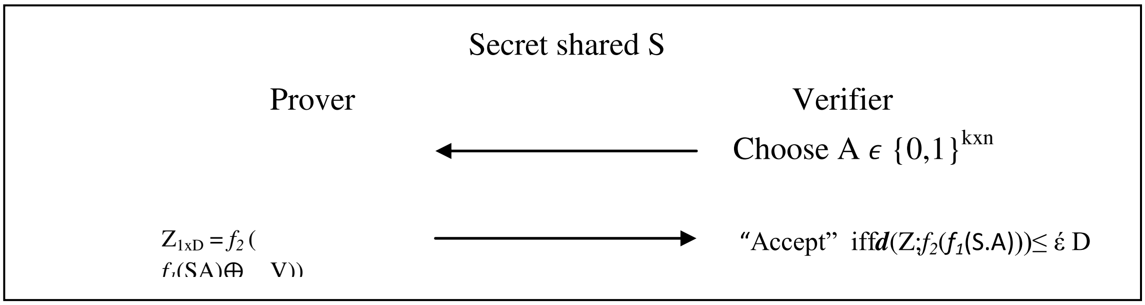
Secret shared S
Prover
Verifier
Choose A ϵ {0,1}^kxn
Z_1xD = f_2( f_1(SA)⊕ V))
"Accept" iff d(Z;f_2(f_1(S.A)))≤ έ D

**Fig. 2.**Parallelized version of the proposed DNLHB protocol.

The Prover (tag) and Verifier (reader) share a K-bit secret key S. The Verifier transmits a random $K \times n$ challenge matrix A to the Prover. In the HB family of protocols, the Prover computes Z=S.A⊕V, while, the Prover of the NLHB family of protocols computes Z= *f*(S.A)⊕V. However, the Prover in the DNLHB protocol first computes $f_1$(S.A) followed by the computation of Z = $f_2$($f_1$(S.A)⊕V), where V is a noise-vector whose bits are all independently distributed according to Bernoulli distribution with parameter ε, similar to the noise vector in the HB protocol [23] and the NLHB protocol [11].Then the verifier returns "Accept" if and only if its check on the Prover response is true. The size of the A matrix in the HB family of protocols is greater than the A matrix of NLHB by a number of times equal to the degree of the nonlinear function f used by the NLHB protocol. Similarly, the DNLHB protocol reduces the size of the utilized A matrix by the sum of the degrees of the two nonlinear functions; f1 and f2 with respect to the A matrix used by the HB protocol, and by the degree of f2 with respect to the A matrix employed in the NLHB protocol. Therefore, the DNLHB protocol is capable of achieving the same level of security against passive attacks as HB family protocols and NLHB protocol but with much lower sizes of the A matrix. In other words, the proposed DNLHB protocol achieves higher level of security against attacks for the same size of the A matrix than both the HB and the NLHB protocols as will be shown in more detail in section 6.

### *5.1.1.Hardnessof DNLHB protocol*

The NLHB protocol has been proven in [11] to be an NP hard. In this section, we show that the proposed DNLHB protocol is an NP hard as well. The proof is very similar to the proof provided for the hardness of the NLHB protocol. All it is necessary to do is to show that an instance of NLHB is reducible to an instance of DNLHB.

Lemma 1: The NLHB protocol is reducible to the proposed DNLHB protocol, and hence the proposed DNLHB protocol is an NP hard.

Proof: Follows directly from the proof of theorem 1 in [11] after replacing p by p1+p2 and replacing $y = f(\mathrm{SA}) \oplus v'$by $y = f_2(f_1(\mathrm{SA}) \oplus v')$. Thus the NLHB protocol is reducible to the proposed DNLHB protocol, and hence the proposed DNLHB protocol is an NP hard.

### *5.1.2. Implementation of the DNLHB protocol versions*

To evaluate the proposed DNLHB protocol an implementation is in order to construct the two nonlinear functions, $f_1$, and $f_2$. The following equations describe two possible nonlinear functions $f_1$ and $f_2$ which can be used in an implementation for the DNLHB protocol.

$$f_{1i} = f_1(x_i, x_{i+1}, x_{i+2}, \dots, x_{i+p_1}); 1 \le i \le (D - p_1) \quad (6)$$

$$y_i = f_{1i} \oplus v_i \quad (7)$$

$$f_{2i} = f_2(y_i, y_{i+1}, y_{i+2}, \dots, y_{i+p_2}; 1 \le i \le (D - p_1 - p_2) \quad (8)$$

The following discussion demonstrates how the low-cost candidates f1 and f2 given in equations (6- 8) perform on passive attacks. A security efficiency comparison is held between both the HB and the NLHB protocols and the DNLHB protocol for the same passive attacks. Due to the double nonlinearity introduced by the DNLHB, passive attacks required more time to succeed in invading the security of DNLHB protocol than for either the HB or NLHB protocols. Moreover, a comparison for the Prover complexity of HB, NLHB and DNLHB protocols, demonstrates that the DNLHB Prover requires less computations than the Prover for either of HB or NLHB for achieving the same level of security.

### 5.1.3. The DNLHBv1 protocol

The first version of the proposed DNLHB protocol, DNLHBv1, employs two nonlinear functions of the third degree;p1= p2=p=3. The two functions f1 and f2 are given in equations (9- 11).

$$f_{1i} = x_i \oplus x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1};\ 1 \le i \le (D - p_1) \quad (9)$$

$$y_i = f_{1i} \oplus v_i \quad (10)$$

$$f_{2i} = y_i \oplus y_{i+1}y_{i+2} \oplus y_{i+1}y_{i+3};\ 1 \le i \le (D - p_1 - p_2) \quad (11)$$

Next we have to show how the proposed DNLHBv1performs against any of the four popular attacking algorithms (BKW [20], LF1, LF2 [10], Novel [21]).Let x = [x1,..,xn] = S.A = [s.a1,.., s.an], where [a1,.., an] are the columns of the A matrix. Also, Let m = f1(x) and y = m ⊕V. Then, the passive adversary to DNLHBv1 has access to Z=f2(y).

Normally, the attacker repeatedly adds the columns of the A matrix, and obtains the response corresponding to this new matrix by adding the responses corresponding to the added columns [20]. The following discussion examines the results when the attacker performs an addition for one such matrix A. Now, assume that the attacker has modified matrix A and it becomes $A'$ = [a1,…, aj⊕ak,…,an] through the addition of the kth column to the jth column of A. The corresponding matrix product of S and $A'$; y’ = [y1, y2,…,yj⊕yk,…, yn]. Note that $y'$ is the same as y except that the jth position value is yj⊕yk. Now, the attacker computes $z'$= f2($y'$), it is easily noting that only the output bits getting affected by the change of the A matrix are the ones with indices (j-3); (j-2); (j-1) and j as indicated below (see equations 12-19).

$$z_{i-3} = y_{i-3} \oplus y_{i-2}y_{i-1} \oplus y_{i-2}y_i \quad (12)$$

$$z_{i-2} = y_{i-2} \oplus y_{i-1}y_i \oplus y_{i-1}y_{i+1} \quad (13)$$

$$z_{i-1} = y_{i-1} \oplus y_iy_{i+1} \oplus y_iy_{i+2} \quad (14)$$

$$z_i = y_i \oplus y_{i+1}y_{i+2} \oplus y_{i+1}y_{i+3} \quad (15)$$

$$z'_{i-3} = y_{i-3} \oplus y_{i-2}y_{i-1} \oplus y_{i-2}y_i \oplus y_{i-2}y_k \quad (16)$$

$$z'_{i-2} = y_{i-2} \oplus y_{i-1}y_i \oplus y_{i-1}y_K \oplus y_{i-1}y_{i+1} \quad (17)$$

$$z'_{i-1} = y_{i-1} \oplus y_iy_{i+1} \oplus y_ky_{i+1} \oplus y_iy_{i+2} \oplus y_ky_{i+2} \quad (18)$$

$$z'_i = y_i \oplus y_k \oplus y_{i+1}y_{i+2} \oplus y_{i+1}y_{i+3} \quad (19)$$

Comparing equations (12) through (15) for z with the corresponding equations (16) through (19) for$z'$ , it can be easily concluded that there is an extra term in each equation. Therefore, the attacker will not be able to deduce the noiseless response z from $z'$.

In order to evaluate the performance of the DNLHBv1, the entropy is estimated to show how far the attacker will be off from the correct response. The entropy is defined to be the probability of zero error. The error equations, Ei’s can be found through subtracting the corresponding equation for $z_i$ from $z'_i$ to find $E_i$ equation. The probability of zero error equations can easily be found as:

$$\Pr[f_{1(i-3)} = 1] = 0.4375$$

$$\Pr[v_{i-3} = 1] = \varepsilon = 0.25$$

$$\Pr[(f_{1(i-3)} \oplus v_{i-3}) = 1] = \Pr[f_{1(i-3)} \cup v_{i-3}] - \Pr[f_{1(i-3)} \cap v_{i-3}]$$

$$\Pr[(f_{1(i-3)} \oplus v_{i-3}) = 1]$$
$$= \text{Max}(\Pr[f_{1(i-3)} = 1], \Pr[v_{(i-3)} = 1])$$
$$- \min(\Pr[f_{1(i-3)} = 1], \Pr[v_{(i-3)} = 1])$$

$$\Pr[(f_{1(i-3)} \oplus v_{i-3}) = 1] = 0.4375 - 0.25 = 0.1875$$

$$\Pr[y_{i-3} = 1] = 0.1875$$

$$\Pr[y_{i-3} = 0] = 1 - 0.1875 = 0.8125$$

$$\Pr[E_{i-3} = 1] = \Pr[y_{i-2}y_k = 1] = 0.035$$

$$\Pr[E_{i-3} = 0] = 0.965$$

$$\Pr[E_{i-2} = 1] = \Pr[y_{i-1}y_k = 1] = 0.035$$

$$\Pr[E_{i-2} = 0] = 0.965$$

$$\Pr[E_{i-1} = 1] = y_k(y_{i+1} \oplus y_{i+2}) = 0.1875 * 0.1797 = 0.03369375$$

$$\Pr[E_{i-1} = 0] = 1 - 0.03369375 = 0.96630625 \approx 0.966$$

$$\Pr[E_i = 0] = \Pr[y_k = 0] = 1 - 0.1875 = 0.8125$$

The error bits $E_{i-3}, E_{i-2}, E_{i-1}$ and $E_i$ for the bits ($z_{i-3}$, $z_{i-2}$, $z_{i-1}$, $z_i$) of Z and the corresponding bits ($z'_{i-3}$, $z'_{i-2}$, $z'_{i-1}$, $z'_i$) of Z' are given in Table 2.

**Table 2.**

Error bits and the corresponding entropy values for the proposed DNLHBv1 protocol.

| Error equation | Entropy |
|---|---|
| $E_{i-3} = z'_{i-3} - z_{i-3} = y_{i-2}y_k$ | 0.965 |
| $E_{i-2} = z'_{i-2} - z_{i-2} = y_{i-1}y_K$ | 0.965 |
| $E_{i-1} = z'_{i-1} - z_{i-1} = y_k y_{i+1} \oplus y_k y_{i+2}$ | 0.9663 |
| $E_i = z'_i - z_i = y_K$ | 0.8125 |

The maximum entropy, Emax, equals to the sum of entropies ($E_{i-3}$ ,$E_{i-2}$,$E_{i-1}$,$E_i$ ).

$$E_{max}(\text{DNLHBv1}) = E_i + E_{i-1} + E_{i-2} + E_{i-3} = 3.7 \quad (20)$$

### *5.1.4. The DNLHBv2 protocol*

Similar to the first DNLHB version, the second DNLHB version, DNLHBv2 utilizes two nonlinear functions but with different degrees; p1=3, p2=4. These two nonlinear functions, $f_1$ and $f_2$, are given in equations (21- 23).

$$f_{1i} = x_i \oplus x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1}; 1 \leq i \leq (D - p_1) \quad (21)$$

$$y_i = f_{1i} \oplus v_i \quad (22)$$

$$f_{2i} = y_i + y_{i+1}y_{i+2} + y_{i+2}y_{i+3} + y_{i+3}y_{i+4}; 1 \leq i \leq (D - p_1 - p_2) \quad (23)$$

Similar treatment as for the DNLHBv1protocol is followed to show the performance of the DNLHBv2 protocol against the four popular attacking algorithms. Equations (24 –33) indicate the output bits getting affected by the change of the A matrix due to the introduction of two nonlinear functions given in equations (22) and (24) for DNLHBv2.

$$z_{i-4} = y_{i-4} + y_{i-3}y_{i-2} + y_{i-2}y_{i-1} + y_{i-1}y_i \tag{24}$$

$$z_{i-3} = y_{i-3} + y_{i-2}y_{i-1} + y_{i-1}y_i + y_iy_{i+1} \tag{25}$$

$$z_{i-2} = y_{i-2} + y_{i-1}y_i + y_iy_{i+1} + y_{i+1}y_{i+2} \tag{26}$$

$$z_{i-1} = y_{i-1} + y_{i+1}y_i + y_{i+2}y_{i+1} + y_{i+2}y_{i+3} \tag{27}$$

$$z_i = y_i + y_{i+1}y_{i+2} + y_{i+2}y_{i+3} + y_{i+3}y_{i+4} \tag{28}$$

$$z'_{i-4} = y_{i-4} + y_{i-3}y_{i-2} + y_{i-2}y_{i-1} + y_{i-1}y_i + y_{i-1}y_K \tag{29}$$

$$z'_{i-3} = y_{i-3} + y_{i-2}y_{i-1} + y_{i-1}y_i + y_iy_{i+1} + y_{i-1}y_K + y_Ky_{i+1} \tag{30}$$

$$z'_{i-2} = y_{i-2} + y_{i-1}y_i + y_iy_{i+1} + y_{i-1}y_K + y_Ky_{i+1} + y_{i+1}y_{i+2} \tag{31}$$

$$z'_{i-1} = y_{i-1} + y_{i+1}y_i + y_{i+1}y_K + y_{i+2}y_{i+1} + y_{i+2}y_{i+3} \tag{32}$$

$$z'_i = y_i + y_k + y_{i+1}y_{i+2} + y_{i+2}y_{i+3} + y_{i+3}y_{i+4} \tag{33}$$

Comparing equations (24) through (28) for z with the corresponding equations (29) through (33) for z', it can be easily recognizes that there is an extra term in each equation. Thus, the attacker will not be able to obtain the noiseless response z from z'.

In order to evaluate the performance of the proposed DNLHBv2 protocol, the entropy is estimated to illustrate how far the attacker will be off from the correct response. The probability of zero error equations can be written as:

$$\Pr[f_{1(i-4)} = 1] = 0.4375$$

$$\Pr[v_{i-4} = 1] = \varepsilon = 0.25$$

$$\Pr[(f_{1(i-4)} \oplus v_{i-4}) = 1] = \Pr[f_{1(i-4)} \cup v_{i-4}] - \Pr[f_{1(i-4)} \cap v_{i-4}]$$

$$\begin{aligned}\Pr[(f_{1(i-4)} \oplus v_{i-4}) = 1] &\\ &= \mathrm{Max}(\Pr[f_{1(i-4)} = 1], \Pr[v_{(i-4)} = 1]) \\ &\quad - \min(\Pr[f_{1(i-4)} = 1], \Pr[v_{(i-4)} = 1])\end{aligned}$$

$$\Pr[(f_{1(i-4)} \oplus v_{i-4}) = 1] = 0.4375 - 0.25 = 0.1875$$

$$\Pr[y_{i-4} = 1] = 0.1875$$

$$\Pr[y_{i-4} = 0] = 1 - 0.1875 = 0.8125$$

$$\Pr[E_{i-4} = 1] = \Pr[y_{i-1}y_k = 1] = 0.035$$

$$\Pr[E_{i-4} = 0] = 0.965$$

$$\Pr[E_{i-3} = 1] = y_k(y_{i+1} \oplus y_{i-1}) = 0.1875 * 0.1797 = 0.03369375$$

$$\Pr[E_{i-3} = 0] = 1 - 0.03369375 = 0.96630625 \approx 0.966$$

$$\Pr[E_{i-2} = 1] = y_k(y_{i+1} \oplus y_{i-1}) = 0.1875 * 0.1797 = 0.03369375$$

$$\Pr[E_{i-2} = 0] = 1 - 0.03369375 = 0.96630625 \approx 0.966$$

$$\Pr[E_{i-1} = 1] = \Pr[y_ky_{i+1} = 1] = 0.035$$

$$\Pr[E_{i-1} = 0] = 0.965$$

$$\Pr[E_i = 0] = \Pr[y_k = 0] = 1 - 0.1875 = 0.8125$$

The error bits $E_{i-4}, E_{i-3}, E_{i-2}, E_{i-1}$ and $E_i$ for the bits ($z_{i-4}$,$z_{i-3}$, $z_{i-2}$, $z_{i-1}$, $z_i$) of Z and the corresponding bits ($z'_{i-3}$, $z'_{i-2}$, $z'_{i-1}$, $z'_i$) of Z' can be found as given in Table3.

**Table 3.**

Error bits and the corresponding entropy values for the proposed DNLHBv2 protocol.

| Error equation | Entropy |
|---|---|
| $E_{i-4} = z'_{i-4} - z_{i-4} = y_{i-1}y_k$ | 0.965 |
| $E_{i-3} = z'_{i-3} - z_{i-3} = y_k y_{i+1} \oplus y_k y_{i-1}$ | 0.9663 |
| $E_{i-2} = z'_{i-2} - z_{i-2} = y_k y_{i+1} \oplus y_k y_{i-1}$ | 0.9663 |
| $E_{i-1} = z'_{i-1} - z_{i-1} = y_k y_{i+1}$ | 0.965 |
| $E_i = z'_i - z_i = y_K$ | 0.8125 |

The maximum entropy, Emax equals to the sum of entropies ($E_{i-4}, E_{i-3}$ ,$E_{i-2}$,$E_{i-1}$,$E_i$ ).

$$E_{max}(\mathrm{DNLHBv2}) = E_i + E_{i-1} + E_{i-2} + E_{i-3} + E_{i-4} = 4.675 \qquad (34)$$

### *5.1.5. The DNLHBv3 protocol*

The third proposed version of the DNLHB protocol, DNLHBv3, also employs two nonlinear functions with different degrees; p1=3, p2=2. The two used nonlinear functions $f_1$ and $f_2$ are given in equations (35- 37).

$$f_{1i} = x_i \oplus x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1};\ 1 \le i \le (D - p_1) \qquad (35)$$

$$y_i = f_{1i} \oplus v_i \qquad (36)$$

$$f_{2i} = y_i y_{i+2} \oplus y_{i+1} y_i;\ 1 \le i \le (D - p_1 - p_2) \qquad (37)$$

The performance of the proposed DNLHBv3 protocol for the four popular attacking algorithms is evaluated similar to the two other protocol versions. The attacker computes $z' = f_2(y')$; the output bits getting affected by the change of the A matrix due to the introduction of the two nonlinear functions in equation (35) and (37) are:

$$z_{i-2} = y_{i-1}y_{i-2} \oplus y_i y_{i-2} \qquad (38)$$

$$z_{i-1} = y_i y_{i-1} \oplus y_{i-1} y_{i+1} \qquad (39)$$

$$z_i = y_{i+1} y_i \oplus y_{i+2} y_i \qquad (40)$$

$$z'_{i-2} = y_{i-1}y_{i-2} \oplus y_{i-2}y_K \oplus y_{i-2}y_i \qquad (41)$$

$$z'_{i-1} = y_i y_{i-1} \oplus y_k y_{i-1} \oplus y_{i-1} y_{i+1} \qquad (42)$$

$$z'_i = y_{i+1}y_i \oplus y_{i+2}y_i \oplus y_{i+1}y_k \oplus y_{i+2}y_k \qquad (43)$$

Comparing equations (38) through (40) for z with the corresponding equations (41) through (43) for z', it can be easily recognized that there is an extra term in each equation. Therefore, the attacker will not be able to get the noiseless response z from z'.

The entropy for the proposed DNLHBv3 is estimated to illustrate how far the attacker will be off from the correct response. The error equations can be found by subtracting the two equations for z from z' to find the equation for E. The probability equations can easily be written as:

$$\Pr[f_{1(i-2)} = 1] = 0.4375$$
$$\Pr[v_{i-2} = 1] = \varepsilon = 0.25$$
$$\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] = \Pr[f_{1(i-2)} \cup v_{i-2}] - \Pr[f_{1(i-2)} \cap v_{i-2}]$$
$$\begin{aligned}\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] \\ &= \mathrm{Max}(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1]) \\ &- \min(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1])\end{aligned}$$
$$\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] = 0.4375 - 0.25 = 0.1875$$
$$\Pr[y_{i-2} = 1] = 0.1875$$
$$\Pr[y_{i-2} = 0] = 1 - 0.1875 = 0.8125$$
$$\Pr[E_{i-2} = 1] = \Pr[y_{i-2}y_k = 1] = 0.035$$
$$\Pr[E_{i-2} = 0] = 0.965$$
$$\Pr[E_{i-1} = 1] = \Pr[y_{i-1}y_k = 1] = 0.035$$
$$\Pr[E_{i-1} = 0] = 0.965$$
$$\Pr[E_i = 1] = y_k(y_{i+1} \oplus y_{i+2}) = 0.1875 * 0.1797 = 0.03369375$$
$$\Pr[E_i = 0] = 1 - 0.03369375 = 0.96630625 \approx 0.966$$

The error bits $E_{i-2}, E_{i-1}$ and $E_i$ for the bits ($z_{i-2}$, $z_{i-1}$, $z_i$) of Z and the corresponding bits ($z'_{i-2}$, $z'_{i-1}$, $z'_i$) of z' are given in Table 4.

**Table 4.**
Error bits and the corresponding entropy values for the proposed DNLHBv3 protocol.

| Error equation | Entropy |
|---|---|
| $E_{i-2} = z'_{i-2} - z_{i-2} = y_{i-2}y_K$ | 0.965 |
| $E_{i-1} = z'_{i-1} - z_{i-1} = y_{i-1}y_K$ | 0.965 |
| $E_i = z'_i - z_i = y_k y_{i+1} \oplus y_k y_{i+2}$ | 0.9663 |

The maximum entropy, Emax equals to the sum of entropies ($E_{i-2}$,$E_{i-1}$, and $E_i$ ).

$$E_{max}(\mathrm{DNLHBv3}) \quad = E_i + E_{i-1} + E_{i-2} = 2.89 \qquad (44)$$

Thus it can be concluded that the entropy varies with the degrees of the two utilized nonlinear functions to be 3.7, 4.675, and 2.89 respectively for the proposed DNLHBv1, DNLHBv2, and DNLHBv3.

### *5.2. The TNLHB protocol versions*

The proposed TNLHB protocol is of the same category as both the NLHB and DNLHB protocols; its security is built upon the use of nonlinear functions. The TNLHB protocol added two more levels of nonlinear functions over the NLHB protocol and one more level of nonlinear function over the DNLHB protocol. Thus, the proposed TNLHB protocol achieves the same security as NLHB and DNLHB protocol but at much smaller secret key size. Figure 3shows one session for the proposed TNLHB protocol.

The Prover (tag) and Verifier (reader) share a K-bit secret S. The Verifier transmits a random K×n challenge matrix A to the Prover. The TNLHB protocol's Prover (tag) computes $\mathrm{Z} = \mathrm{f}_3(\mathrm{f}_2(\mathrm{f}_1(\mathrm{S.A})\oplus\mathrm{v}_1)\oplus\mathrm{v}_2)$,where $\mathrm{v}_1$and$\mathrm{v}_2$ are noise-vectors whose bits are all independently distributed according to Bernoulli distribution with parameter ε. Then the verifier returns "Accept" if and only if its check on the Prover response is true.

The proposed TNLHB protocol reduces the size of the utilized A matrix by the sum of the degrees of $\mathrm{f}_1$, $\mathrm{f}_2$,and $\mathrm{f}_3$ with respect to the A matrix used by the HB protocols, by the sum of the degrees of $\mathrm{f}_1$ and $\mathrm{f}_2$ with respect to the A matrix employed by the NLHB protocol, and by the degree of $\mathrm{f}_3$ with respect to the A matrix utilized in the DNLHB protocol. It worth noting that the size of the A matrix for both DNLHB and TNLHB can be equal depending on the degrees of the nonlinear functions, $\mathrm{f}_1$, $\mathrm{f}_2$, and $\mathrm{f}_3$, used by both proposed protocols. Therefore, the TNLHB protocol is capable of achieving the same level of security against attacks with lower size of the matrix A and a higher level of security against attacks for the same size of the A matrix than either HB, or NLHB , or DNLHB as will be shown later in section 6.

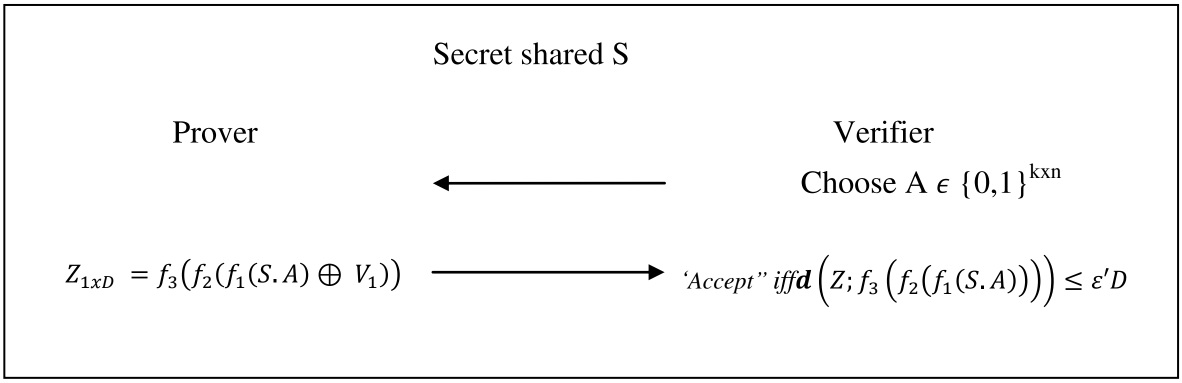
Secret shared S
Prover
Verifier
Choose A $\epsilon$ $\{0,1\}^{\mathrm{kxn}}$
$Z_{1xD} = f_3(f_2(f_1(S.A) \oplus V_1))$
'Accept" iff$\mathbf{d}\left(Z; f_3\left(f_2(f_1(S.A))\right)\right) \leq \varepsilon' D$

**Fig. 3.**Parallelized version of the proposed TNLHB protocol.

### *5.2.1 Hardness of TNLHB protocol*

The proposed TNLHB protocol can be shown to be an NP hard. Also, the proof is very similar to the proof provided for the hardness of the NLHB protocol in [11]. All one has to do is to show that an instance of NLHB or DNLHB is reducible to an instance of TNLHB.

Lemma 2: The NLHB and the DNLHB protocols are reducible to the proposed TNLHB protocol, and hence the proposed TNLHB protocol is an NP hard.

Proof: Follows directly from the proof of theorem 1 in [11] after replacing p by p1+p2+p3 and replacing $y = (f(SA))\oplus v)$. by $y = (f_3(f_2(f_1(SA)))\oplus v)$. Therefore, the NLHB protocol is reducible to the proposed TNLHB protocol, and hence the proposed TNLHB protocol is an NP hard.

### *5.2.2.Implementation of TNLHB protocol versions*

This section shows how the TNLHB protocol is implemented and its prevalence against popular attacking algorithms is estimated next. The following equations (45-49) describe the three nonlinear functions f1, f2 and f3 used in the implementation of the TNLHB protocol:

$$f_{1i} = f_1(x_i, x_{i+1}, x_{i+2}, \dots, x_{i+p_1}); 1 \le i \le (D - p_1) \quad (45)$$

$$y_i = f_{1i}\oplus v_{1i}; 1 \le i \le D \quad (46)$$

$$f_{2i} = f_2(y_i, y_{i+1}, \dots, y_{i+p_2}); 1 \le i \le (D - p_1 - p_2) \quad (47)$$

$$l_i = f_{2i}\oplus v_{2i}; 1 \le i \le (D - p_1 - p_2 - p_3) \quad (48)$$

$$f_{3i} = f_3(l_i, l_{i+1}, l_{i+2}, \dots, l_{i+p_3}); 1 \le i \le (D - p_1 - p_2 - p_3) \quad (49)$$

The following discussion demonstrates how the low-cost candidates for $f_1$, $f_2$, and $f_3$ given in equations (47- 51) perform on passive attacks. A security efficiency comparison is held between the HB, NLHB, DNLHB protocols and the TNLHB protocol for the same passive attacks. Due to the multi-nonlinearity introduced by the TNLHB, passive attacks require more time to succeed in invading the security of TNLHB protocol than for the HB, NLHB, or DNLHB protocols.

### *5.2.3. The TNLHBv1 protocol*

The proposed TNLHBv1protocol utilizes three nonlinear function with degrees; p1=3, p2=3, and p3 =3, for $f_1$, $f_2$, and $f_3$ respectively for encoding the secret key to compute the output z. The used nonlinear functions $f_1$, $f_2$, and $f_3$ are given in equations (50- 54). Next, is a proof to show that the four popular attacking algorithms fail to break the security of the proposed TNLHBv1 protocol:

$$f_{1i} = x_i\oplus x_{i+1}x_{i+2}\oplus x_{i+2}x_{i+3}\oplus x_{i+3}x_{i+1}; 1 \le i \le (D - p_1) \quad (50)$$

$$y_i = f_{1i}\oplus v_i \quad (51)$$

$$f_{2i} = y_i\oplus y_{i+1}y_{i+2}\oplus y_{i+1}y_{i+3}; 1 \le i \le (D - p_1 - p_2) \quad (52)$$

$$l_i = f_{2i}\oplus v_i \quad (53)$$

$$f_{3i} = l_i\oplus l_{i+1}l_{i+2}\oplus l_{i+1}l_{i+3}; 1 \le i \le (D - p_1 - p_2 - p_3) \quad (54)$$

Normally, the attacker repeatedly adds the columns of the A matrix, and obtains the response corresponding to the new matrix by adding the responses corresponding to the added columns [10]. The following discussion examines the results when the attacker performs an addition for one such a matrix, A. Assume that the attacker has modified the A matrix and became $A'$= [a1,...,aj⊕ak, …, an], through the addition of the kth column to the jth column. The corresponding matrix product of S and $A'$;$l'$= [l1, l2, …, lj⊕lk, …, ln]. Note that,$l'$ matrix is the same as l matrix except for the jth position value which is lj⊕lkinstead of lj. Now, the attacker computes $z' = f_3(f_2(f_1(l')))$, only the output bits getting affected by the change of the A matrix are the ones with indices (j-3); (j-2); (j-1) and j as indicated below (see equations 55 to 62).

$$z_{i-3} = l_{i-3} \oplus l_{i-1} l_i \oplus l_{i-2} l_{i-1} \quad (55)$$

$$z_{i-2} = l_{i-2} \oplus l_{i+1} l_i \oplus l_{i-1} l_{i+1} \quad (56)$$

$$z_{i-1} = l_{i-1} \oplus l_i l_{i+1} \oplus l_{i+1} l_{i+2} \quad (57)$$

$$z_i = l_i \oplus l_{i+1} l_{i+2} \oplus l_{i+2} l_{i+3} \quad (58)$$

$$z'_{i-3} = l_{i-3} \oplus l_{i-2} l_i \oplus l_{i-2} l_k \oplus l_{i-2} l_{i-1} \quad (59)$$

$$z'_{i-2} = l_{i-2} \oplus l_{i-1} l_i \oplus l_{i-1} l_K \oplus l_{i-1} l_{i+1} \quad (60)$$

$$z'_{i-1} = l_{i-1} \oplus l_i l_{i+1} \oplus l_k l_{i+1} \oplus l_{i+1} l_{i+2} \quad (61)$$

$$z'_i = l_i \oplus l_k \oplus l_{i+1} l_{i+2} \oplus l_{i+2} l_{i+3} \quad (62)$$

Comparing equations (55) through (58) for Z with the corresponding equations (59) through (62) for Z', it can be easily concluded that there is an extra term in each equation. Thus, the attacker will not be able to obtain the noiseless response Z from Z'.

In order to evaluate the performance of the TNLHBv1, the entropy is estimated to show how far the attacker will be off from the correct response. The entropy is the probability of the error being zero. The error equations $E'_i$s, can be found through the subtraction of$z_i$ from $z'_i$. Thus the probability of error can easily be found as:

$$\Pr[f_{1(i-2)} = 1] = 0.4375$$
$$\Pr[v_{i-2} = 1] = \varepsilon = 0.25$$
$$\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] = \Pr[f_{1(i-2)} \cup v_{i-2}] - \Pr[f_{1(i-2)} \cap v_{i-2}]$$
$$\begin{aligned}\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] &\\ &= \mathrm{Max}(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1]) \\ &- \min(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1])\end{aligned}$$
$$\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] = 0.4375 - 0.25 = 0.1875$$
$$\Pr[y_{i-2} = 1] = 0.1875$$
$$\Pr[f_{2(i-2)} = 1] \approx 0.1875$$
$$\Pr[v_{2(i-2)} = 1] = \varepsilon = 0.25$$
$$\Pr[(f_{2(i-2)} \oplus v_{2(i-2)}) = 1] = \Pr[f_{2(i-2)} \cup v_{2(i-2)}] - \Pr[f_{2(i-2)} \cap v_{2(i-2)}]$$
$$\begin{aligned}\Pr[(f_{1(i-2)} \oplus v_{1(i-2)}) = 1] &\\ &= \mathrm{Max}(\Pr[f_{1(i-2)} = 1], \Pr[v_{1(i-2)} = 1]) \\ &- \min(\Pr[f_{1(i-2)} = 1], \Pr[v_{1(i-2)} = 1])\end{aligned}$$
$$\Pr[(f_{2(i-2)} \oplus v_{2(i-2)}) = 1] = 0.25 - 0.1875 = 0.0625$$
$$\Pr[l_{i-2} = 1] = 0.0625$$
$$\Pr[l_{i-2} = 0] = 1 - 0.0625 = 0.9375$$

$$\Pr[E_{i-3} = 1] = \Pr[l_{i-2}l_k = 1] = 0.00390625$$
$$\Pr[E_{i-3} = 0] = 1 - \Pr[E_{i-3} = 1] = 0.99609375$$
$$\Pr[E_{i-2} = 1] = \Pr[l_{i-1}l_k = 1] = 0.00390625$$
$$\Pr[E_{i-2} = 0] = 1 - \Pr[E_{i-2} = 1] = 0.99609375$$
$$\Pr[E_{i-1} = 0] = \Pr[l_k l_{i+1} = 0] = 0.99609375$$
$$\Pr[E_i = 0] = \Pr[l_k = 0] = 1 - 0.0625 = 0.9375$$

The error bits $E_{i-3}, E_{i-2}, E_{i-1}$ and $E_i$ for the bits ($z_{i-3}$, $z_{i-2}$, $z_{i-1}$, $z_i$) of Z and the corresponding bits ($z'_{i-3}$, $z'_{i-2}$, $z'_{i-1}$, $z'_i$) of Z' can be found as given in Table5.

**Table 5.**
Error bits and the corresponding entropy values for the proposed TNLHBv1.

| Error equation | Entropy |
|---|---|
| $E_{i-3} = z'_{i-3} - z_{i-3} = l_{i-2}l_K$ | 0.996 |
| $E_{i-2} = z'_{i-2} - z_{i-2} = l_{i-1}l_K$ | 0.996 |
| $E_{i-1} = z'_{i-1} - z_{i-1} = l_k l_{i+1}$ | 0.996 |
| $E_i = z'_i - z_i = l_K$ | 0.9375 |

The maximum entropy for TNLHBv1, Emax equals to the sum of entropies ($E_{i-3}$ ,$E_{i-2}$,$E_{i-1}$,$E_i$ ).

$$E_{max}(\text{TNLHBv1}) = E_i + E_{i-1} + E_{i-2} + E_{i-3} \approx 3.93 \quad (63)$$

### *5.2.4. The TNLHBv2 protocol*

Similar to TNLHBv1 three nonlinear functions are employed to implement the TNLHBv2 protocol. The three nonlinear functions $f_1$, $f_2$, and $f_3$ with degree p1=3, p2=3, and p3=4 are given in equations (64- 68).

$$f_{1i} = x_i \oplus x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1};\ 1 \le i \le (D - p_1) \quad (64)$$

$$y_i = f_{1i} \oplus v_{i1} \quad (65)$$

$$f_{2i} = y_i \oplus y_{i+1}y_{i+2} \oplus y_{i+2}y_{i+3};\ 1 \le i \le (D - p_1 - p_2) \quad (66)$$

$$l_i = f_{2i} \oplus v_{i2} \quad (67)$$

$$f_{3i} = l_i \oplus l_{i+1}l_{i+2} \oplus l_{i+1}l_{i+3} \oplus l_{i+3}l_{i+4};\ 1 \le i \le (D - p_1 - p_2 - p_3) \quad (68)$$

Also, it is easily proven that any attacker using any one of the four popular attacking algorithms finds it very hard to invade the security of the TNLHBv2 protocol. To do this similar what have been done for the TNLHBv1, the modified $A^{'}$ = [a1,…,aj⊕ak,….., an], is found through the addition of the kth column to the jthcolumn of A. The corresponding dot product matrix of S and$A^{'}$is l = [l1; l2;……;lj⊕ lk;………; ln]. Note that $l^{'}$ matrix is the same as l matrix except for the $j^{th}$ position value which is lj⊕lk. Now, the attacker computes $z^{'} = f_2(l^{'})$, it is clear that only the output bits getting affected by the change of the A matrix are the ones with indices (j-3); (j-2); (j-1) and j as indicated below (see equations 69 through 78).

$$z_{i-4} = l_{i-4} \oplus l_{i-2} l_{i-1} \oplus l_{i-3} l_{i-1} \oplus l_{i-1} l_i \quad (69)$$

$$z_{i-3} = l_{i-3} \oplus l_{i-1} l_{i-2} \oplus l_{i-2} l_i \oplus l_i l_{i+1} \quad (70)$$

$$z_{i-2} = l_{i-2} \oplus l_{i-1} l_i \oplus l_{i-1} l_{i+1} \oplus l_{i+1} l_{i+2} \quad (71)$$

$$z_{i-1} = l_{i-1} \oplus l_i l_{i+1} \oplus l_i l_{i+2} \oplus l_{i+2} l_{i+3} \quad (72)$$

$$z_i = l_i \oplus l_{i+1} l_{i+2} \oplus l_{i+1} l_{i+3} \oplus l_{i+3} l_{i+4} \quad (73)$$

$$z'_{i-4} = l_{i-4} \oplus l_{i-2} l_{i-1} \oplus l_{i-3} l_{i-2} \oplus l_{i-1} l_i \oplus l_{i-1} l_k \quad (74)$$

$$z'_{i-3} = l_{i-3} \oplus l_{i-1} l_{i-2} \oplus l_{i-2} l_i \oplus l_i l_{i+1} \oplus l_{i-2} l_k \oplus l_k l_{i+1} \quad (75)$$

$$z'_{i-2} = l_{i-2} \oplus l_{i-1} l_i \oplus l_{i-1} l_{i+1} \oplus l_{i+1} l_{i+2} \oplus l_{i-1} l_k \quad (76)$$

$$z'_{i-1} = l_{i-1} \oplus l_i l_{i+1} \oplus l_i l_{i+2} \oplus l_{i+2} l_{i+3} \oplus l_k l_{i+1} \oplus l_k l_{i+2} \quad (77)$$

$$z'_i = l_i \oplus l_k \oplus l_{i+1} l_{i+2} \oplus l_{i+1} l_{i+3} \oplus l_{i+3} l_{i+4} \quad (78)$$

Comparing equations (69) through (73) for Z with the corresponding equations (74) through (78) for Z', it is concluded that there is an extra term in each equation. Thus, the attacker will not be able to obtain the noiseless response Z from Z'.

In order to evaluate the performance of the TNLHBv2, the entropy is estimated to illustrate how far the attacker will be off from the correct response. The entropy is the probability of error being zero. Errors equations can be found by subtract $z_i$equation from $z'_i$ equation to find $E_i$ equation. The probability equations can easily be found as:

$$\Pr[f_{1(i-2)} = 1] = 0.4375$$
$$\Pr[v_{i-2} = 1] = \varepsilon = 0.25$$
$$\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] = \Pr[f_{1(i-2)} \cup v_{i-2}] - \Pr[f_{1(i-2)} \cap v_{i-2}]$$
$$\begin{aligned}\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] &\\ &= \mathrm{Max}(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1]) \\ &\quad - \min(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1])\end{aligned}$$
$$\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] = 0.4375 - 0.25 = 0.1875$$
$$\Pr[y_{i-2} = 1] = 0.1875$$
$$\Pr[f_{2(i-2)} = 1] \approx 0.1875$$
$$\Pr[v_{2i-2} = 1] = \varepsilon = 0.25$$
$$\Pr[(f_{2(i-2)} \oplus v_{2i-2}) = 1] = \Pr[f_{2(i-2)} \cup v_{2i-2}] - \Pr[f_{2(i-2)} \cap v_{2i-2}]$$
$$\begin{aligned}\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] &\\ &= \mathrm{Max}(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1]) \\ &\quad - \min(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1])\end{aligned}$$

$\Pr[(f_{2(i-2)} \oplus v_{2(i-2)}) = 1] = 0.25 - 0.1825 = 0.0625$
$\Pr[l_{i-2} = 1] = 0.0625$
$\Pr[l_{i-2} = 0] = 1 - 0.0675 = 0.9375$
$\Pr[E_{i-4} = 0] = 1 - \Pr[E_{i-4} = 1] = 0.99609375 \approx 0.996$
$\Pr[E_{i-3} = 1] = \Pr[l_k(l_{i+1} \oplus l_{i-2}) = 1] = 0.0625(0.01992) = 0.001245$
$\Pr[E_{i-3} = 0] = 1 - 0.001245 = 0.998755 \approx 1$
$\Pr[E_{i-2} = 1] = \Pr[l_{i-1}l_k = 1] = 0.00390625$
$\Pr[E_{i-2} = 0] = 1 - \Pr[E_{i-2} = 1] = 0.99609375 \approx 0.996$
$\Pr[E_{i-1} = 0] = 0.998755 \approx 1$
$\Pr[E_i = 0] = \Pr[l_k = 0] = 1 - 0.0675 = 0.9375$

The error bits $E_{i-3}, E_{i-2}, E_{i-1}$ and $E_i$ for the bits ($z_{i-4}$,$z_{i-3}$, $z_{i-2}$, $z_{i-1}$, $z_i$) of Z and the corresponding bits ($z'_{i-4}$,$z'_{i-3}$, $z'_{i-2}$, $z'_{i-1}$, $z'_i$) of Z' can be found as given in Table 6:

**Table 6.**
Error bits and the corresponding entropy values for the proposed TNLBHv2 protocol.

| Error equation | Entropy |
|---|---|
| $E_{i-4} = z'_{i-4} - z_{i-4} = l_{i-1}l_K$ | 0.996 |
| $E_{i-3} = z'_{i-3} - z_{i-3} = l_{i-2}l_k \oplus l_kl_{i+1}$ | 1 |
| $E_{i-2} = z'_{i-2} - z_{i-2} = l_{i+1}l_k$ | 0.996 |
| $E_{i-1} = z'_{i-1} - z_{i-1} = l_kl_{i+1} \oplus l_kl_{i+2}$ | 1 |
| $E_i = z'_i - z_i = l_K$ | 0.9375 |

The maximum entropy, $E_{max}$,is equal to the sum of entropies ($E_{i-3}$ ,$E_{i-2}$,$E_{i-1}$,$E_i$ ).

$$E_{max}(\text{TNLHBv2}) = E_i + E_{i-1} + E_{i-2} + E_{i-3} \approx 4.93 \quad (79)$$

### *5.2.5. The TNLHBv3 protocol*

Similar to both TNLHBv1 and TNLHBv2, three nonlinear functions are used to implement the TNLHBv3 protocol. The three nonlinear functions $f_1$, $f_2$, and $f_3$ with degrees: $p_1 = 3$,$p_2$=2, and $p_3$=3 are given in equations (80- 84) below.

$$f_{1i} = x_i \oplus x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1}; 1 \le i \le (D - p_1) \quad (80)$$

$$y_i = f_{1i} \oplus v_i \quad (81)$$

$$f_{2i} = y_i \oplus y_{i+1}y_{i+2}; 1 \le i \le (D - p_1 - p_2) \quad (82)$$

$$l_i = f_{2i} \oplus v_i \quad (83)$$

$$f_{3i} = l_i \oplus l_{i+1}l_{i+2} \oplus l_{i+1}l_{i+3}; 1 \le i \le (D - p_1 - p_2 - p_3) \quad (84)$$

Using the three functions $f_1$, $f_2$, and $f_3$ given in equations (81, 82, and- 84), it will be shown that any attacker using any one of the four popular attacking algorithms fails with high probability to invade the security of the TNLHBv3 protocol. The following discussion examines the results when the attacker performs addition on the A matrix to compute the output Z. The attacker has modified the A matrix by the performed addition and obtained instead $A' = [a1, \ldots aj \oplus ak, \ldots \ \ an]$, through the addition of the kth column to the jth column of A. The corresponding dot matrix product of S and$A'$is: $l' = [l1, l2, \ldots, lj \oplus lk, \ldots, ln]$. Note that matrix $l'$ is the same as the l matrix with the expectation of the jth position value which is $lj \oplus lk$. Now, the attacker computes $Z' = f2(l')$, only the output bits getting affected by the change of the A matrix are the ones with indices (j-3); (j-2); (j-1) and j as indicated below (see equations 85 through 92).

$$z_{i-3} = l_{i-3} \oplus l_{i-1} l_i \oplus l_{i-2} l_{i-1} \tag{85}$$

$$z_{i-2} = l_{i-2} \oplus l_{i+1} l_i \oplus l_{i-1} l_{i+1} \tag{86}$$

$$z_{i-1} = l_{i-1} \oplus l_i l_{i+1} \oplus l_i l_{i+2} \tag{87}$$

$$z_i = l_i \oplus l_{i+1} l_{i+2} \oplus l_{i+2} l_{i+3} \tag{88}$$

$$z'_{i-3} = l_{i-3} \oplus l_{i-2} l_i \oplus l_{i-2} l_k \oplus l_{i-2} l_{i-1} \tag{89}$$

$$z'_{i-2} = l_{i-2} \oplus l_{i-1} l_i \oplus l_{i-1} l_K \oplus l_{i-1} l_{i+1} \tag{90}$$

$$z'_{i-1} = l_{i-1} \oplus l_i l_{i+1} \oplus l_k l_{i+1} \oplus l_i l_{i+2} \oplus l_k l_{i+2} \tag{91}$$

$$z'_i = l_i \oplus l_k \oplus l_{i+1} l_{i+2} \oplus l_{i+2} l_{i+3} \tag{92}$$

Comparing equations (85) through (88) for Z with the corresponding equations (89) through (92) for Z', it can be easily noticed that there is an extra term in each equation. Thus, the attacker will not be able to get the noiseless response Z from Z'.

In order to evaluate the performance of the TNLHB, the entropy is estimated to show how far the attacker will be off from the correct response. The entropy is the probability of the error being zero. Errors equations can be found by subtracting $z_i$ equation from$z'_i$equation to find $E_i$ equation. The probability equations can be written as:

$$\Pr[f_{1(i-2)} = 1] = 0.4375$$
$$\Pr[v_{i-2} = 1] = \varepsilon = 0.25$$
$$\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] = \Pr[f_{1(i-2)} \cup v_{i-2}] - \Pr[f_{1(i-2)} \cap v_{i-2}]$$
$$\begin{aligned}\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] \\ &= \mathrm{Max}(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1]) \\ &\quad - \min(\Pr[f_{1(i-2)} = 1], \Pr[v_{(i-2)} = 1])\end{aligned}$$
$$\Pr[(f_{1(i-2)} \oplus v_{i-2}) = 1] = 0.4375 - 0.25 = 0.1875$$
$$\Pr[y_{i-2} = 1] = 0.1875$$
$$\Pr[f_{2(i-2)} = 1] = 0.1525$$
$$\Pr[v_{2(i-2)} = 1] = \varepsilon = 0.25$$

$$\Pr\left[\left(f_{2(i-2)} \oplus v_{2(i-2)}\right) = 1\right] = \Pr\left[f_{2(i-2)} \cup v_{2(i-2)}\right] - \Pr\left[f_{2(i-2)} \cap v_{2(i-2)}\right]$$

$$\begin{aligned}\Pr\left[\left(f_{1(i-2)} \oplus v_{1(i-2)}\right) = 1\right] \\ &= \mathrm{Max}\left(\Pr\left[f_{1(i-2)} = 1\right], \Pr\left[v_{1(i-2)} = 1\right]\right) \\ &- \min\left(\Pr\left[f_{1(i-2)} = 1\right], \Pr\left[v_{1(i-2)} = 1\right]\right)\end{aligned}$$

$$\Pr\left[\left(f_{2(i-2)} \oplus v_{2(i-2)}\right) = 1\right] = 0.25 - 0.1525 = 0.0975$$

$$\Pr[l_{i-2} = 1] = 0.0975$$

$$\Pr[l_{i-2} = 0] = 1 - 0.0975 = 0.9025 \cong 0.9$$

$$\Pr[E_{i-3} = 0] = \Pr[l_{i-2} l_K = 0] \approx 0.99$$

$$\Pr[E_{i-2} = 1] = \Pr[l_{i-1} l_k = 1] = 0.00950625$$

$$\Pr[E_{i-2} = 0] = 1 - \Pr[E_{i-2} = 1] = 1 - 0.0095 \cong 0.9905 \approx 0.99$$

$$\Pr[E_{i-1} = 0] = \Pr[l_{i-1} l_K = 0] \approx 0.99$$

$$\Pr[E_i = 0] = \Pr[l_k = 0] = 1 - 0.09765625 = 0.90234375 \cong 0.9$$

The error bits $E_{i-3}, E_{i-2}, E_{i-1}$ and $E_i$ for the bits ($z_{i-3}$, $z_{i-2}$, $z_{i-1}$, $z_i$) of Z and the corresponding bits ($z'_{i-3}$, $z'_{i-2}$, $z'_{i-1}$, $z'_i$) of Z' can be found as given in Table 7.

The maximum entropy, Emax equals to the sum of entropies ($E_{i-3}$ ,$E_{i-2}$,$E_{i-1}$,$E_i$ ).

$$E_{max}(\mathrm{TNLHBv3}) = E_i + E_{i-1} + E_{i-2} + E_{i-3} \cong 3.87 \qquad (93)$$

In summary this section presented three versions for the TNLHB protocol which are based on the NLHB and DNLHB protocols. Each of the three versions has employed three nonlinear functions; $f_1$, $f_2$, and $f_3$ but with varying degrees; p1, p2, and p3. The entropy for the three proposed versions is estimated to be 3.93, 4.93, and 3.87 respectively for TNLHBv1, TNLHBv2, and TNLHBv3. It is clear that the entropy and hence the achieved security of each of the proposed TNLHB protocol versions is dependent upon the chosennonlinear functions degrees; the higher the degree of the chosen nonlinear function the higher the achieved security by the protocol.

**Table 7.**
Error bits and the corresponding entropy values for the proposed TNLHBv3 protocol.

| Error equation | Entropy |
|---|---|
| $E_{i-3} = z'_{i-3} - z_{i-3} = l_{i-2} l_K$ | 0.99 |
| $E_{i-2} = z'_{i-2} - z_{i-2} = l_{i-1} l_K$ | 0.99 |
| $E_{i-1} = z'_{i-1} - z_{i-1} = l_k l_{i+1} \oplus l_k l_{i+2}$ | 0.99 |
| $E_i = z'_i - z_i = l_K$ | 0.90 |

## 6. Performance of proposed protocols against popular attacks

The proposed protocols as well as the NLHB protocol are exposed to two types of attacks that must defend themselves against them. The first type is a direct passive attack, in which the nonlinear protocol is attacked as if it was a linear protocol. While in the other type the attacker converts the nonlinear protocol to a linear protocol and then attacks it. Next, a description for the two types of attacks is presented and comparisons are held between the security of the HB, the NLHB, and the proposed protocols for the two attack types.

### *6.1 Direct Passive Attacks*

The four popular attacking algorithms impersonate the HB and NLHB families to obtain the secret key by repeatedly adding the columns of the A matrix and compute the response corresponding to the new A matrix. Table 9 shows the equations which are used to calculate the security level in terms of the security bits for every protocol [10, 20]. Since the NLHB protocol adds a nonlinear function stage over the HB protocol therefore, every security bit in the HB protocol is multiplied by the entropy value of the added nonlinear function of the third degree to produce an entropy value of 2.5. However, the DNLHB protocol versions have added another stage of nonlinearity over The NLHB protocol. Thus increasing the value of the entropy for the proposed DNLHBv1with a third degree, functions over the two stages and produce an entropy value of 3.7. Furthermore, adding onemore stage of nonlinear function with equal degree to construct the TNLHBv1 protocol and produce an entropy value of 3.94. Table 8 compares the entropies for the HB, NLHB, the three versions of DNLHB, and the three versions of TNLHB for the four popular attacker algorithms.

From Figures 4 and 5, it is easy to notice that the security level for the HB protocol at K=512 is higher than 80bits which is considered to be acceptable security level [8]. However, the NLHB protocol achieves the same level of security at K=128 and the proposed protocols the DNLHB and TNLHB achieve the 80 bits security level at K=64. Thus the proposed protocols; DNLHB and TNLHB reduce the size of the secret key to one fourth of that for HB and one half of that required by the NLHB and hence reducing the hardware required for their implementations.

**Table 8.**
Security bits equations for BKW, LF1, LF2 and NOVEL attacking algorithms.

| Algorithm | HB Protocol | NLHB Protocol | DNLHB Protocols | | | TNLHB Protocols | | |
|---|---|---|---|---|---|---|---|---|
| | | | 1st | 2nd | 3rd | 1st | 2nd | 3rd |
| BKW | $Q=\mathrm{l\,og}_2(a^3 * 2^b * (1-2\varepsilon)^{-2^a})$ | 2.5Q | 3.7Q | 4.6Q | 2.89Q | 3.93Q | 4.93Q | 3.87Q |
| LF1 | $Q=\mathrm{l\,og}_2((8b+200)\cdot(1-2\varepsilon)^{-2^a}+2b(a-1))$ | 2.5Q | 3.7Q | 4.6Q | 2.89Q | 3.93Q | 4.93Q | 3.87Q |
| LF2 | $Q=\log_2(25 * (1\text{-}2\varepsilon)-2a+2b(a-1))$ | 2.5Q | 3.7Q | 4.6Q | 2.89Q | 3.93Q | 4.93Q | 3.87Q |
| Novel | $Q=(1-2\varepsilon)^{-w*2^{(k-2b)/2}}$ | 2.5Q | 3.7Q | 4.6Q | 2.89Q | 3.93Q | 4.93Q | 3.87Q |

Figure 4 shows the security bits for the HB, NLHB, and the three versions of the proposed protocols DNLHB, and TNLHB for the attacking algorithm BKW. In Fig.4 a=0.5 log2 (K), b = K/a, and w=2(a-1) where K is the length of the secret key. While Fig.5 presents a comparison for the security bits for the proposed protocols and similar protocols in the literature.

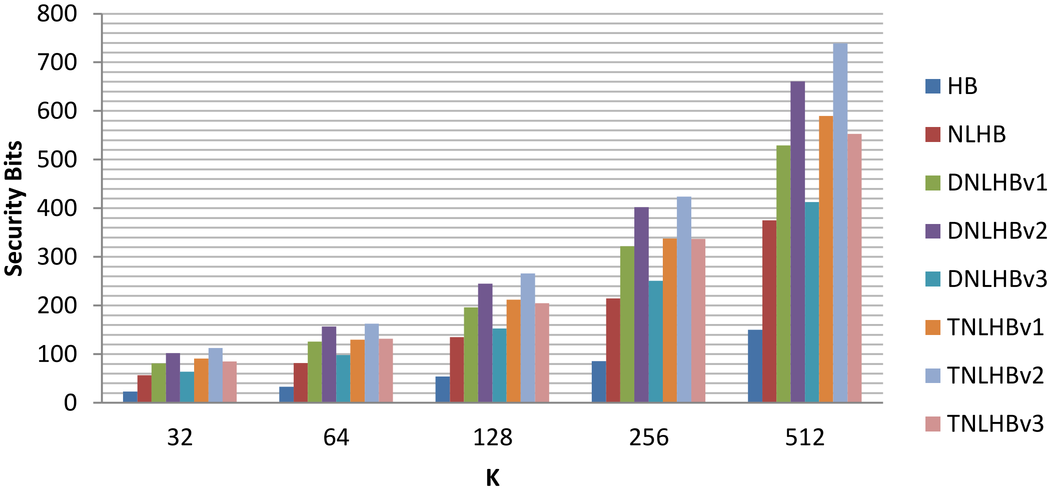

**Fig.4.** Number of security bits for the BKW algorithm at $\varepsilon = 0.25$ and $\varepsilon' = 0.35$.

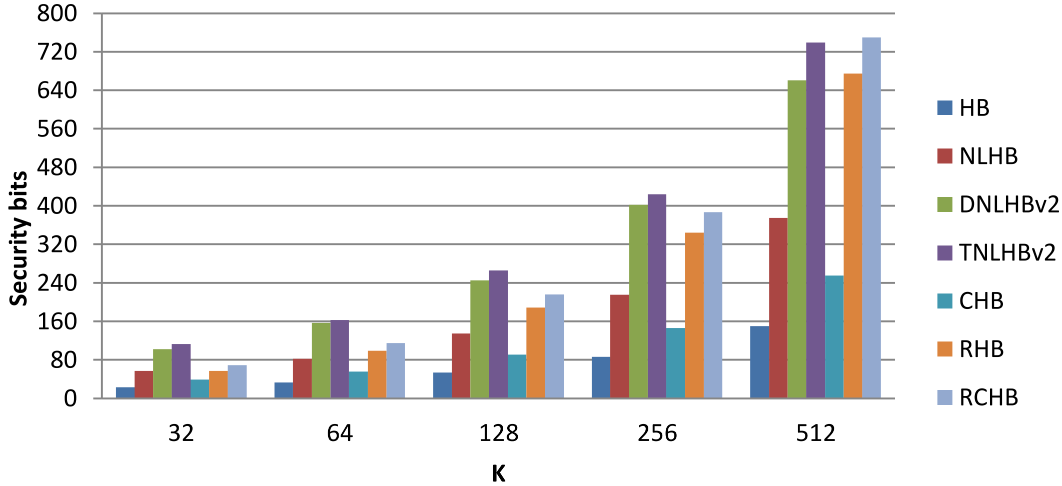

**Fig.5.** Security bits comparison for the protocols: HB, NLHB, DNLHB v2, TNLHBv2, CHB, RHB, and RCHB at $\varepsilon = 0.25$ and $\varepsilon' = 0.35$for the BKW attacking algorithm.

### 6.2 Equivalent HB protocol attacks

The equivalent HB protocol attacker [22] gets around the nonlinearity of protocols such as NLHB protocol by getting a good approximate linear function for their nonlinear functions. However, for the DNLHB protocols, there are two levels of nonlinear functions, the equivalent HB attacker obtains an approximate linear function for the first level but there still a second nonlinear function with an entropy dependent on its degree (for *p*=3the Entropy is 2.5). Also, the TNLHB protocols have three levels of nonlinear functions; the equivalent HB attacker obtains a good approximate linear function of one level, however, there still two more nonlinear levels to protect the TNLHB protocols from such attacks. In other words, if the equivalent HB protocol attacker invades the DNLHB protocol it will convert it to NLHB protocol which has security higher than the HB protocol. Also, if it attacks the TNLHB protocol, it will convert to TNLHB protocol with one less stage or DNLHB protocol. Table 9 shows the securities at $\varepsilon = 0.05$ and $\varepsilon' = 0.29$ against the BKW attacker and its equivalent HB protocol for the NLHB and the proposed protocols; DNLHB with two nonlinear functions of degrees 3, and TNLHB with three nonlinear functions of degrees 3, 2, and 3.

**Table 9.**
Securities of proposed protocols against the BKW and equivalent HB protocol attacks.

| K | NLHB | | DNLHB | | TNLHB | |
|---|---|---|---|---|---|---|
| | BKW | equivalent HB Protocol | BKW | equivalent HB Protocol | BKW | equivalent HB Protocol |
| 32 | 45 | 18 | 62 | 50 | 64 | 54.4 |
| 64 | 65 | 43 | 96 | 70 | 100 | 83.2 |
| 128 | 117 | 65 | 162 | 122 | 170 | 140.8 |
| 256 | 337 | 102 | 266 | 342 | 280 | 230.4 |

## 7. Conclusion

In this paper we have introduced the concept of multiple nonlinear functions for the HB family in order to increase the security against passive attacks. We proposed DNLHB protocol which is mainly a new authentication protocol that is light in its computation demands. Light-weight requirements of DNLHB protocol makes it suitable for low power devices such as RFIDs. Three different versions for the DNLHB protocol have presented. First version, the two nonlinear stages have an equal degree of three. The second version, the latter nonlinear stage has a degree one less than the degree of the first stage. While in the third, the latter nonlinear stage has a degree one higher than the degree of the first stage. The discussion of the proposed protocol showed that adding double stages of nonlinearity has increased the entropy from 2.5 for NLHB protocol to 3.7 for the proposed DNLHB protocol. It has been shown that the DNLHB protocol with a small sized security key (e.g. 64 bits) achieves the same security level (80 bits) that can be achieved with large-sized key of previous protocols. The implementation for the proposed DNLHB protocol showed that it is highly effective, harder to be attacked and less demanding in terms of the hardware components.

A second TNLHB protocol has been proposed to enhance the performance of the proposed DNLHB protocol, which consists of three levels of nonlinear functions. Also, three versions of the TNLHB protocol have been presented with different degrees for the three nonlinear functions used in the implementation. The simulation results showed that TNLHB has improved the security against passive attacks significantly over DNLHB, NLHB and HB protocols at very reasonable complexity cost.

## 8. References

[1] Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J., Ribagorda, A.: M2AP:AMinimalist Mutual-Authentication Protocol for Low-Cost RFID Tags. In: Ubiquitous Intelligence and Computing. LNCS 4159 (2006) 912–923.

[2] K. Finkenzeller. RFID Handbook, second edition, Wiley & Sons, 2002.

[3] Juels, A. & Weis, S. A. (2005). Authenticating Pervasive Devices with Human Protocols, International Cryptology Conference, CRYPTO 2005: 293-308.

[4] Hopper, N. J. ;& Blum, M. (2001). Secure Human Identification Protocols, International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2001: 52-66.

[5] Gilbert, H., Robshaw M. J. B. &Seurin, Y. HB#: Increasing the Security and Efficiency of HB+, Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2008: 361-378.

[6] Piramuthu, S., \HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication," Proceedings of the Conference on Collaborative Electronic Commerce Technology and Research (CollECTer Europe), pp. 239-247, Basel, 2006.

[7] KhaledOuafi, Raphael Overbeck, Serge Vaudenay. On the Security of HB# Against a Man-in-the-Middle Attack. Advances in Cryptology - ASIACRYPT 2008 · Lecture Notes in Computer Science Volume 5350, 2008, pp 108-124.

[8] M. Madhavan, A. Thangaraj, K. Viswanathan, and Y. Sankarasubramaniam, NLHB : A Light-weight, Provably-secure Variant of the HB Protocol Using Simple Non-linear Functions, Authorized licensed use limited to: Hewlett-Packard via the HP Labs Research Library,2010

[9] Blum, A., Furst, M., Kearns, M., and Lipton, R. J. Cryptographic Primitives Based on Hard Learning Problems. In Advances in Cryptology – CRYPTO'93 (1994), vol. 773 of Lecture Notes in Computer Science, pp. 278–291.

[10] E. Levieil and P.A. Fouque. An Improved LPN Algorithm. Proceedings of SCN 2006, LNCS vol. 4116, 348-359, Springer, 2006.

[11] M. Madhavan, A. Thangaraj, Y. Sankarasubramaniam, and K. Viswanathan, "NLHB: A non-linear Hopper Blum protocol," ArXiv.org, 12 Feb 2010, http://arxiv.org/abs/1001.2140.

[12] E. R. Berlekamp, R. J. McEliece, V. Tilborg. On the Inherent Intractability of Certain Coding Problem. IEEE Transactions on Information Theory 24, 1978, pp. 384-386

[13] Marc P.C. Fossoriery, Miodrag J. Mihaljevi´c, Hideki Imai,YangCuiz and KantaMatsuuraz, A Novel Algorithm for Solving the LPN Problem and its Application to Security Evaluation of the HB Protocol for RFID Authentication, International Conference on Cryptology-INTDOCRYPT, PP. 48-62, 2006. DOI: 10.1007/11941378_5

[14] J. Hastad. Some Optimal Inapproximability Results, STOC '97 Proceeding of the twenty-ninth annual ACM Symposium on Theory of Computing, pp. 1-10, 1997.

[15] Crawford, J. M., Kearns, M. J., and Shapire, R. E. The Minimal Disagreement Parity Problem as a Hard Satisfiability Problem. Tech. rep., Computational Intelligence Research Laboratory and AT&T Bell Labs, February 1994.

[16] Chabaud, F. On the Security of Some Cryptosystems Based on Error-Correcting Codes. In Advances in Cryptology - EUROCRYPT (1995), vol. 950 of Lecture Notes in Computer Science, pp. 131–139.

[17] Crawford, J. M., Kearns, M. J., and Shapire, R. E. The Minimal Disagreement Parity Problem as a Hard Satisfiability Problem. Tech. rep., Computational Intelligence Research Laboratory and AT&T Bell Labs, February 1994.

[18] A. Blum, A. Kalai, and H.Wasserman. Noise-tolerant Learning, the Parity Problem, and the Statistical Query Problem Journal of the ACM 50, 4, July 2003, pp. 506-519.

[19] Kishan Chand Gupta and PalashSarkar, Construction of Perfect Nonlinear and Maximally Nonlinear Multiple-Output Boolean Functions Satisfying Higher Order Strict Avalanche Criteria. IEEE Trans. On Information Theory, Vol. 50, No. 11, Nov. 2004.pp. 2886 - 2893

[20] Kishan Chand Gupta and PalashSarkar, Construction of Perfect Nonlinear and Maximally Nonlinear Multiple-Output Boolean Functions Satisfying Higher Order Strict Avalanche Criteria. IEEE Trans. On Information Theory, Vol. 50, No. 11, Nov. 2004.

[21] A. Juels and S. Weis, Authenticating Pervasive Devices with Human Protocols,CRYPTO2005, Lecture Notes in Computer Science, vol. 3621, pp. 293-308, 2005.

[22] Mohammad Reza SohizadehAbyaneh, On the Security of Non-Linear HB (NLHB) Protocol against Passive Attack, Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on , vol., no., pp.523-528, 11-13 Dec.2010

[23] N. Hopper and M. Blum, A Secure Human-Computer Authentication Scheme. Technical Report CMU-CS-00-139, Carnegie Mellon University, 2000.

[24] Samia A. Ali, Rafeet Mohamed, and Mahmoud Hardan, RCHB: Light-weight, provably-secure variants of the HB protocol using rotation and complementation, Network and System Security (NSS), 2011 5th International Conference on 6-8 Sept. 2011, Page(s): 244 – 248.

## متغيرات من بروتوكولات الـ HBللأمن نظم الـ RFID

### الملخص:

تلقت أجهزةالـ RFIDفي الآونة الأخيرة إهتماما كبيرًا من المؤسسات الكبيرة والباحثين وهذا يرجع إلى نقص لتكاليف الـ Tag وأدخال القياسية على نظم الـRFID. لذلك أصبحت نظم الـRFIDأكثر شيوعا في الاستخدام اليومي لتحديد وتتبعالمواقع والأشخاص، والحيوانات. وقد اقترح عدد من البروتوكولات في المجلات العلمية لأمان ضد الهجمات السلبية على الـ RFID. أحد البروتوكولات المعروفة هو البروتوكول الذي يعتمد على الـHB بروتوكول وفك الرموز الخطية لأمان الـ RFID ضد الهجمات السلبية. والـ HBغير الخطي (NLHB) هو عضو منعائلة بروتوكول الـ HBالذي يحقق أمنية مشددة عن طريق الحد من المشكلة بصورة مبرهنة حيث أنه من الصعب فك الرموزمن الفئة الغير خطية ضد الهجمات السلبية على نظم الـ RFID.

هذا البحثيقدم بروتوكولات متعدد المراحل الغير الخطية على بروتوكول الـ HBلتعزيز أمنها ضد الهجمات السلبيةً. وبشكل أكثر تحديدًا، فإن البحثيقدمبروتوكولان متعددان اللاخطية وثلاث إصدارات مقدمع لكل منهم معتمدان على البروتوكول الـ HB.أحد البروتوكةلان مزدوجا اللاخطية (DNLHB)، والبروتوكول الثانى ثلاثي اللاخطية (TNLHB). البروتوكولات المقترحة تحقق زيادة كبيرة في أمن أنظمة الـRFIDضد الهجماتالسلبية بتكلفة أقل فى التنفيذ.