Single shift-register for RFID tag secrecy

Bruno B. Albert, F. M. de Assis and Marcus V. C. Rodrigues
Electrical Engineering Department, Iquanta
Federal University of Campina Grande
Campina Grande, Brazil
emails: albert,fmarcos@dee.ufcg.edu.br mvinicius1@terra.com.br

***Abstract*— In this paper we present a new privacy scheme against passive adversaries based on the message modulation instead of classical cryptographic models for low cost wireless devices, such as an RFID tag. The idea is to become the adversary in disadvantage related to the reader-tag communication channel, for example, by reducing her signal-to-noise ratio.**

Keywords*— *RFID, privacy/security, random modulation, PRG.

I. Introduction

In recent years, Radio Frequency Identification (RFID) technology has become a subject of main attention. RFID systems are wireless devices used to reveal both the nature and the location of physical objects or even persons. A typical RFID system consists of two main components: a *reader* and a *tag*. The reader is responsible to transmit information and also energy to the tag. Tags are small wireless devices that answer to a RFID reader query. In general, tags are passive elements, i.e., they receive all of their operating energy from the reader. RFID technology is used to simplify and to automate many processes, such as a supply chain. The low computational power associated with low cost of the tags imposes to privacy/security specialists extra difficulties. However, generally, the primary concern in such systems is protecting the privacy of data. Some privacy issues include the following: personal items could be scanned without authorization or even knowledge; clandestine tracking of people; might reveal patient's medical information; consumers might become classified by vendors; people could be compelled through automatic object reactions [1]. In response to these issues, the security and privacy research community has proposed schemes aiming the prevention of unauthorized access to RFID tags.

In this paper, we address privacy issues considering a passive eavesdropper. We propose a new system based on a modulation scheme instead of classical cryptographic models. This scheme is founded on the increasing of noisy transmission of the adversary's channel in terms of signal-to-noise rate. We enhanced a system presented in [2] using only one shift-register instead of two.

The paper is organized as follows. In Section II we present an overview of the related works with our proposal. In Section III we describe the proposed system. Section IV discusses the performance and the restrictions of the suggested protocol. Finally, we present a conclusion of the work in Section V.

II. Preliminaries

Since RFID devices use a wireless interface to communicate, they are subject to eavesdropping. For that reason, requirements for security and privacy are so important in this domain. The common method to achieve privacy in RFID systems is using conventional cryptosystems together with a shared secret key. Perfect secrecy systems were defined by Shannon [3] and must satisfy three conditions: 1) the encryption/decryption key must be kept secret; 2) the key length must have the same length of the message, and; 3) the key must be used only one time. However, these three conditions are generally impracticable.

The first arising question is how to share the secret key. *A. Wyner* [4], in 1975, was a pioneer in the investigation of the transmission of a secret key over an insecure noisy channel. In his model Alice transmits a message to Bob, the two authorized parties, by a discrete memoryless channel (DMC), and Bob is wired-tapper by Eve through another DMC, with crossover probabilities $P_{Y|X}$ and $P_{Z|Y}$ respectively, where Eve represents the adversary, as can be seen in the Figure 1.

Fig. 1. Wyner wire-tap channel.

The idea, in this model, is to design an encoder/decoder in such a way that maximizes the transmission rate to Bob, and also maximizes the equivocation of the data seen by Eve.[1]

I. Csiszár and *J. Körner* [6], in 1978, generalized the *Wyner*'s model. They defined a broadcast channel with confidential messages, i.e., there was a common message sent by Alice to Bob and Eve and a separated message sent to Bob in a way that Eve has a maximum equivocation about it. Notice that *Wyner* solved this problem considering that the Eve's channel is worst than Bob's channel and no common message was sent. Csisár-Körner model is presented in Figure 2 assuming Alice sends messages to Bob and to Eve through two discrete memoryless channels, characterized by the crossover probabilities $P_{Y|X}$ and $P_{Z|X}$.

[1]Equivocation is defined by the conditioned entropy $H(X|Z)$, where X stands for the random variable that represents the message and Z is the Eve's knowledge. For more details about information measures we point the reader to [5]

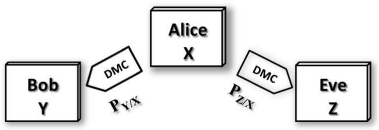

Fig. 2. Csiszár-Körner channel.

In 1993, *U. Maurer* [7] improved the previous model, showing that a secret key agreement was possible for the following scenario: Alice, Bob and Eve receive the output of a random binary source *S* over three independent DMCs, even when Eve's channel was better than the other two channels. A restriction was that the discussion between Alice and Bob is realized over a perfect (but not secure) channel, i.e., Eve has total access to this channel, see Figure 3. Our

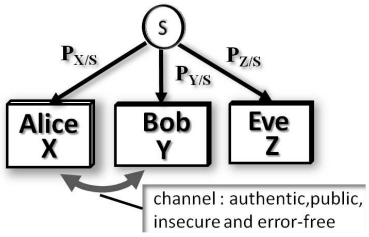

Fig. 3. U. Maurer channel.

system is based on the results obtained by *Brassard* in 1983 [8]. Brassard's protocol (see Figure 4) makes use of two secret keys. The first one, $Y^{(l)}$, specifies a fixed universal-2 hash function $h \in \mathscr{H}$, where $l = \lceil \log |\mathscr{H}| \rceil$. The second specifies the seed $X^{(n)} \in \mathbb{Z}_2^n$, for a PRG, a sequence of *n* bits. Additional details on hash functions will be examined later in this paper. Notice that $\mathscr{H}$ stands for the set of hash functions.

In comparison with a prior scheme proposed by *Wegman* and *Carter* [9], the Brassard's protocol is more effective because it allows the use of a relatively short seed of a Pseudo-Random Generator (PRG). The price paid is that now only computational security is offered. On the other hand, the effectiveness of the protocol is highly dependent on the quality of the PRG. Generally this quality is evaluated by the hardness to discriminate the pseudo-random sequence output of the PRG from a truly random sequence. Alternatively the hardness to find out the seed from the observation of the PRG output can be used to evaluate its quality. In [10] it is shown that under specific conditions,

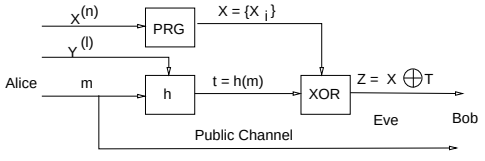

Fig. 4. Brassard's Protocols with two keys and hash function.

a scheme similar to the Brassard's one can assure security

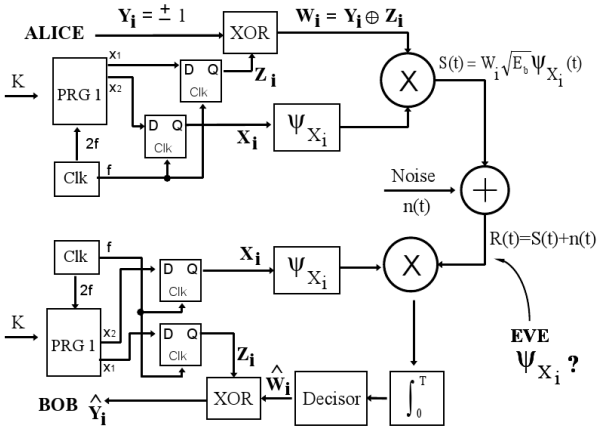

Fig. 5. RFID pseudo-random modulation security scheme.

using a simple PRG. The main requirements are that the information accessible to Eve is kept below a specific level and that the sequence to be protect is not too long. This idea is adapted in our propose in two ways: only one short secret key is adopted and a very simple PGR based on linear feedback shift-register (LFSR) is used.

The way this secret key is shared by the two legitimated parties, Reader and Tag, follows the ideas of *Gander* and *Maurer* paper [11]. In their work, they made use of a noisy channel to achieve perfect secrecy between the sender and the receiver by a very simple protocol. They obtained lower bounds on the secret key rate of binary random sequences even when the adversary channel is better than the Reader-Tag channel. The results of Gander and Maurer protocol is applied to the Cascade protocol introduced by *Brassard* and *Savail* in [12] and modified by *Charbanne* and *Fumaroli* in [13]. Finally, we use the results of *K. Yüksel* [14] work on universal hash functions to improve the privacy of the shared secret key. He defined a variant of NH hash function family [15] named Weighted NH-Polynomial with Reduction (WH) using a Toeplitz approach which is adequated for implementing in ultra-low-power devices.

III. Proposed System

Consider, initially, two parties, a Reader ($\mathscr{R}$) and a Tag ($\mathscr{T}$), who would like to exchange information securely over an insecure channel to which a passive eavesdropper Eve ($\mathscr{E}$) has access. Our proposed system, called RFID Pseudo-Random Modulation Privacy, is shown in Figure 5. A short secret key K, shared by $\mathscr{R}$ and $\mathscr{T}$, represented in Figure 5 by Alice and Bob respectively, feeds a Pseudo-Random Generator (PRG). The PRG is a general linear feedback shift register of length v with a clock that is at least twice the transmission rate. The details of how to share the secret key is described in Subsection III-A. Let $\{X_0, Z_0, X_1, Z_1, \ldots\}$ denote a pseudo-random number sequence generated by the PRG. The $i-$th number $X_i \in \{0, 1, 2, \ldots, L-1\}$ from the PRG is used to choose a basis for encoding information bits. Let $\{Y_0, Y_1, \ldots\}$ be the information bits to be sent by $\mathscr{R}$ to

$\mathscr{T}$. $\{W_0, W_1, \ldots\}$ represents the encoded XOR output, $W_i = Y_i \oplus Z_i$. The $i-$th bit $W_i \in \{-1, +1\}$ is encoded/modulated for transmission by

$$S(t) = S(X_i, W_i, t) = W_i \sqrt{E_b} \Psi_{X_i}(t), \quad 0 \le t < T \quad (1)$$

where T is the pulse duration, E_b is the energy per bit and Ψ_{X_i} represents one of the L orthogonal basis that can be chosen as a function of X_i.

This system works as follows: $\mathscr{E}$ does not know which basis is being used, then she has to choose some strategy in order to estimate W_i; under her point of view, information about W_i is very noisier than for $\mathscr{T}$ (Bob). It can be shown that $\mathscr{E}$ channel became worst as the number of basis L increases. We intend to analyze this scheme in terms of bit error probability.

A. Key Distribution

This subsection is concerned with $\mathscr{R}$ and $\mathscr{T}$ achieving a secret key K, even when they have no such a key initially. The key distribution protocol is based on the noisy channel.

The first part of the proposed protocol is based on *Gander* and *Maurer* paper [11] and is named *distillation phase* where the two legitimate parties take advantage related to the adversary. The second part is based on Cascade protocol introduced by *Brassard* and *Savail* in [12] and modified by *Charbanne* and *Fumaroli* in [13] and called *reconciliation phase* where $\mathscr{R}$ and $\mathscr{T}$ shares a common key about which $\mathscr{E}$ has partial information. The last part of the protocol uses the results of *Yüksel* [14] for *privacy amplification*, where another key is generated, applying a universal hash function and $\mathscr{E}$ almost has no information of the common key.

Suppose $\mathscr{R}$ send a random n-bit string to $\mathscr{T}$ over a noisy channel, this n-bit string may be eavesdropped by $\mathscr{E}$ over another independent noisy channel.

Let $\mathscr{R}$, $\mathscr{T}$, and $\mathscr{E}$ be given random variables $R = \{R_0, R_1, \ldots, R_{n-1}\}$, $T = \{T_0, T_1, \ldots, T_{n-1}\}$, and $E = \{E_0, E_1, \ldots, E_{n-1}\}$ respectively. Sequence R is generated by an unbiased discrete memoryless source. The two independent binary symmetric channels, with crossover probabilities $P_{T|R} = p_T$ and $P_{E|R} = p_E$ generate T and E sequences respectively, damaged versions of R sequence. After this initial phase, it is assumed that $\mathscr{R}$ and $\mathscr{T}$ can communicate over an insecure zero error channel, $\mathscr{E}$ is still present.

The following protocol exploits such a situation. For one iteration:

1) $\mathscr{R}$ and $\mathscr{T}$ group their bits by pair;
2) $\mathscr{R}$ and $\mathscr{T}$ tell each other the parity of each pair over a public channel;
3) If the parities do not match
   a) Then $\mathscr{R}$ and $\mathscr{T}$ discard their bits pair
4) Otherwise
   a) They keep the first bit of the pair

Notice that $\mathscr{E}$ (Eve) knows all the procedure. The reliability of the bits increases as the number of iterations increases at the expense of shrinking the string. This fact is proved in [11].

After the phase of advantage distillation, $\mathscr{R}$ string still has some errors related to $\mathscr{T}$ string. Charbanne and Fumaroli in [13] showed how Brassard and Sailvail's Cascade protocol can be modified in order to reduce the hardware implementation cost while still maintaining adequate correction rate and tolerable leaked information during the reconciliation phase. They suggested two changes: the same block size is set for every pass, and a permutation which is set once and for all. The permutation is cabled inside the $\mathscr{T}$ and $\mathscr{R}$. Let n be the length of the strings to be reconciled; k be the block size width ; n/k be the number of the blocks; σ be a pre-cabled permutation in the set of all bijections of $\{0, 1, ..., n-1\}$ x_0 be $\mathscr{R}$ string at the beginning of the protocol and; y_0 be $\mathscr{T}$ string at the beginning of the protocol. The flowchart of the protocol is shown in Figure 6 and is described as follows. In the i-th pass:

1) $x_i = \sigma(x_{i-1})$ in $\mathscr{R}$.
   $y_i = \sigma(y_{i-1})$ in $\mathscr{T}$.
2) x_i is divided in n/k blocks in $\mathscr{R}$,
   y_i is divided into n/k blocks in $\mathscr{T}$.
3) $x_i(j)$ is the j-th block of the *string* x_i.
   $y_i(j)$ is the j-th block of the *string* y_i.
4) Parity testing:
   a) If the parity of $x_i(j)$ = parity of $y_i(j)$, $\mathscr{R}$ and $\mathscr{T}$ continue testing the parity of the next block (or the next step if all the blocks has been already tested).
   b) If the parity of $x_i(j) \neq$ parity of $y_i(j)$ is started a dichotomic search to find the position l which $x_i(j)[l] \neq y_i(j)[l]$. Then $\mathscr{R}$ reverses $x_i(j)[l]$ to correct the error.

We introduced a stop condition in the reconciliation protocol proposed by Charbanne and Fumaroli. Let p, in Figure 6, denote the number of steps without finding parity error.

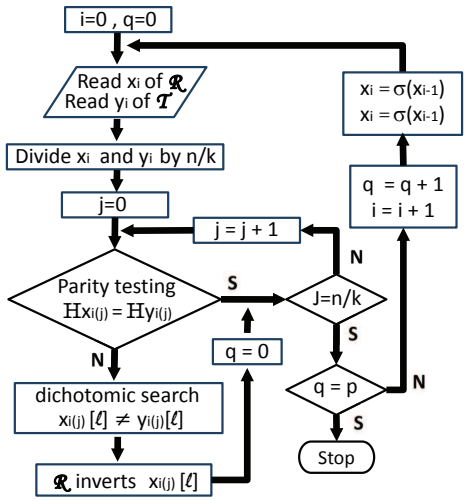

Fig. 6. Reconciliation phase flowchart.

The privacy amplification phase consists of distilling a highly secret shared key, from a larger sequence of shared

partially secret information. Consider that $\mathscr{R}$ and $\mathscr{T}$ share a common random variable S, a sequence of m bits. $\mathscr{E}$ has a correlated random variable W providing at most v bits of information about S, and $v < m$. Let $\{0,1\}^n$ represent all binary strings of length n. $\mathscr{R}$ and $\mathscr{T}$ wish to publicly choose a compression function $h : \{0,1\}^m \rightarrow \{0,1\}^r$, $r < m$, such that $\mathscr{E}$ has complete information on $h(.)$ and her partial information on S give her little information about the key $K_S = h(S)$. The compression function $h(.)$, in practical terms, is chosen from a universal class of hash functions as defined by [14].

Definition 1: The set of hash functions $\mathscr{H} = \{h : A \rightarrow B\}$ is said to be universal if for all pairs $(a_1, a_2) \in A$ and $a_1 \neq a_2$, the probability that the event $h(a_1) = h(a_2)$ occurs is at most $1/|B|$ when $h(.)$ is chosen completely at random in $\mathscr{H}$, where $|B|$ represents the cardinality of the set B.

For our purpose, the universal class of hash functions WH-64 with Toeplitz approach as defined in [14], is an appropriated choice because it is quite easy to be implemented in devices such a tag. The weighted NH-polynomial with reduction hash function family with Toeplitz approach WH_K^T is a variation of the NH hash function family construction. The index K is a key of length $\omega(n+2(t-1))$ bits defining one hash function, where t stands for Toeplitz iteration count. So $K = (k_1, k_2, \ldots, k_{n+2(t-1)})$, where each k_i is a word of length ω. We define $WH_K^T(M)$ as follows.

Definition 2: Let $M = (m_1, \ldots, m_n) \in A$ be a message string and m_i has a length of ω then

$$WH_K^T(M) = (WH_{K_{1\ldots n}}, WH_{K_{3\ldots n+2}}, \ldots, WH_{K_{2t-1\ldots n+2t-2}}),$$

where $K_{i\ldots j} = (k_i, k_{i+1}, \ldots, k_j)$ and WH_k is defined bellow.

Definition 3: Let M be defined as in Definition 2 and $K = (k_1, \ldots, k_n)$ where m_i and $k_i \in GF(2^\omega)$, for any even $n \geq 2$, and an irreducible polynomial $p \in GF(2^\omega)$ we have

$$WH_K(M) = \sum_{i=1}^{n/2} (m_{2i-1} + k_{2i-1})(m_{2i} + k_{2i}) x^{(\frac{n}{2}-i)\omega} \mod p.$$

In the next Section we will make some considerations about the performance of the proposed system.

IV. Performance Analysis

To compute the bit error probability for the Reader-Tag and Reader-Eve channel we assume that the only degradation source is due to AWGN (Additive White Gaussian Noise).

Initially, consider only two orthogonal basis, Ψ_0 and $\Psi_1$as defined bellow

$$\Psi_0 = \sqrt{2/T}\cos(2\pi f_c t) \quad \text{and} \tag{2}$$

$$\Psi_1 = \sqrt{2/T}\sin(2\pi f_c t) \quad 0 \leq t < T. \tag{3}$$

Without loss of generality, consider that Ψ_0 basis was chosen by PRG. The receiver is constituted by a coherent detector model as shown previously in Figure 5. Assume that the transmitted signals in this basis, $S_{0i}(t), \quad i = 0, 1,$ are equiprobable antipodal signals that can be characterized in an unidimensional space of signals.

$$S_{00} = -\sqrt{E_b}\Psi_0 \quad \text{and} \tag{4}$$

$$S_{01} = \sqrt{E_b}\Psi_0 \quad 0 \leq t < T. \tag{5}$$

The received signal $R_{0i}(t)$ is

$$R_{0i}(t) = S_{0i}(t) + N(t), \tag{6}$$

where $N(t)$ is the zero-mean white Gaussian random process. Let $Z_0(T)$ be the correlator output, in this case, the detector uses the following decision rule

$$\text{decides} \quad S_{00}(t) \quad \text{if} \quad Z_0(T) < 0 \tag{7}$$

$$\text{decides} \quad S_{01}(t) \quad \text{otherwise.} \tag{8}$$

Two types of error can occur. (1) $S_{00}(t)$ was transmitted and $Z_0(T) > 0$, and (2) $S_{01}(t)$ was transmitted and $Z_0(T) < 0$. With these conditions, the bit error probability P_b is given by

$$P_b = \int_{\sqrt{\frac{2E_b}{N_0}}}^{\infty} \frac{1}{\sqrt{2\pi}} e^{\frac{-z^2}{2}}\, dz = Q\left(\sqrt{\frac{2E_b}{N_0}}\right), \tag{9}$$

where $N_0/2$ is the two sided power spectral density of the noise. A similar analysis can be done for the other basis Ψ_1.

Now, for the Reader-Eve (or Tag-Eve) channel we assume that $\mathscr{E}$ knows the bases used by $\mathscr{R}$ and $\mathscr{T}$ transmissions (however, she does not know which basis is used for each time of symbol transmission), and she has a receptor to capture the signals exchanged between $\mathscr{R}$ and $\mathscr{T}$. It can be shown that the best choice for her is to use a basis with 45 degrees from the orthogonal bases Ψ_0 and Ψ_1 when the two bases have the same probability to be selected, shown in Figure 7. Note that this is the same situation as before

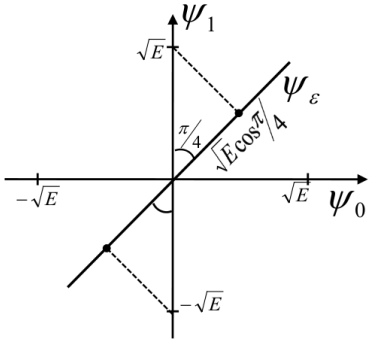

Fig. 7. Eve reception basis.

with the antipodal signals S_{E0} and S_{E1} seen by Eve defined by

$$S_{E0} = -\sqrt{E_b}\cos(\pi/4)\Psi_i \quad \text{and} \tag{10}$$

$$S_{E1} = \sqrt{E_b}\cos(\pi/4)\Psi_i \quad 0 \leq t < T, \tag{11}$$

no matter which basis was chosen. Thus, $\mathscr{E}$ bit error probability P_E can be written as

$$P_E = Q\left(\sqrt{\frac{E_b}{N_0}}\right). \quad (12)$$

In terms of signal-to-noise ratio (SNR) this result represents a loss of 3 dB for $\mathscr{E}$ message reception related to $\mathscr{R} \leftrightarrow \mathscr{T}$ message reception.

If L is the number of basis used by $\mathscr{R}$ and $\mathscr{T}$ communication, then, using the same procedure as before for two basis, with $\mathscr{E}$ choosing the best reception basis, the two antipodal signals S_{E0} and S_{E1} seen by Eve now, will be

$$S_{E0} = -\sqrt{E_b}[\cos(\pi/4)]^{L-1}\Psi_i \quad \text{and} \quad (13)$$

$$S_{E1} = \sqrt{E_b}[\cos(\pi/4)]^{L-1}\Psi_i \quad 0 \le t < T, \quad (14)$$

no matter which basis was chosen. In this case, the signal-to-noise rate on $\mathscr{E} \leftrightarrow \mathscr{R}$ channel, $SNR(\mathscr{E})$, is given by

$$SNR(\mathscr{E}) = SNR(\mathscr{T}) - 10\log L, \quad (15)$$

where $SNR(\mathscr{T})$ is the signal-to-noise rate of the $\mathscr{R} \leftrightarrow \mathscr{T}$ channel.

The proposed PRG is vulnerable for an Berlekamp-Massey algorithm attack [16] [17] [18]. However, for binary numbers, if $\mathscr{E}$ tries to guess the PRG seed by using Berlekamp-Massey algorithm she has to keep her basis in one of the random basis, for example, Ψ_0, but if she did it she will be unable to detect about half of the encoded message bits. Furthermore, she will get only half of the PRG bit output sequence, since the clock rate is twice the transmission rate. Note that a new seed is generated every time $\mathscr{R}$ and $\mathscr{T}$ exchange a new message.

Our system is based on a secret key shared by $\mathscr{R}$ and $\mathscr{T}$, the key distribution protocol described in Subsection III-A requires a noisy channel to work. An analysis of the key distribution protocol is partially done in [13].

V. Conclusion

In this paper we addressed privacy issues in using of RFID systems. We analyzed a modulation scheme, in terms of bit error probability, to give some privacy protection to RFID technology consumers instead of the use of highly complex cryptosystems. We focus on prejudicing the adversary (Eve) communication channel by decreasing her signal-to-noise rate. The proposed system is an enhancement of the system to be presented in [2], here we use one PRG instead of two, and at the same time we increase the difficult of the adversary to guess the PRG seed.

Our initial investigation shows that the proposed scheme can be have a physical implementation without high costs. Antennas with two polarizations is somewhat easy to achieve. The gates to be put into the tag, like shift-registers, etc., is also a feasible task.

For future works we need to compute the colliding probability of the privacy amplification phase when we use a fixed value key for the hash function instead of a random value. Evaluate the vulnerability of the PRG is also required. We also intend to make a comparison of our scheme with others proposed schemes.

Acknowledgment

This work was supported by the Capes-Cofecub Project No. 599/08.

References

[1] S. Spiekermann and S. Evdokimov, "Critical RFID Privacy-Enhancing Technologies," *Computing in Science and Engineering*, vol. 7, no. 2, pp. 56–62, 2009.

[2] B. Albert, F. M. Assis, M. V. Rodrigues, and S. Tedjini, "Performance analysis of a random modulation privacy algorithm," in *WSIM 2010*, Campina Grande, Brazil, May 2010.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systen Technicl Journal*, vol. 28, pp. 656–715, Oct. 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[5] Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*. New York, USA: John Wiley & Sons, Inc., 1991.

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, pp. 339–348, May 1978.

[7] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, pp. 733–742, 1993.

[8] G. Brassard, "On computationally secure authentication tags requiring short secret shared keys," in *Proc. CRYPTO 82*, R. L. Rivest, A. Sherman, and D. Chaum, Eds. New York: Plenum Press, 1983, pp. 79–86.

[9] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *JCSS*, vol. 22, pp. 265–279, 1981.

[10] F. Assis, P. Mateus, Y. Omar, and I. CEMAPRE, "Quantum Authentication of Classical Messages with Perfect Security," *Arxiv preprint arXiv:0806.1231*, 2008.

[11] Gander and Maurer, "On the secret-key rate of binary random variables," in *ISIT: Proceedings IEEE International Symposium on Information Theory, sponsored by The Information Theory Society of The Institute of Electrical and Electronic Engineers*, 1994.

[12] G. Brassard and L. Salvail, "Secret key reconciliation by public discussion," *Lecture Notes in Computer Science*, vol. 765, pp. 410–423, 1994.

[13] H. Chabanne and G. Fumaroli, "Noisy cryptographic protocols for low-cost RFID tags," *IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3562–3566, 2006.

[14] K. Yuksel, "Universal hashing for ultra-low-power cryptographic hardware applications [electronic resource]." Master's thesis, Worcester Polytechnic Institute, 2004. [Online]. Available: http://www.wpi.edu/Pubs/ETD/Available/etd-0428104-195331;http://worldcat.org/oclc/55848122

[15] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and secure message authentication," in *Advances in Cryptology–CRYPTO*, vol. 99. Springer, 1999, pp. 216–233.

[16] A. Sidorenko and B. Schoenmakers, "State Recovery Attacks on Pseudorandom Generators," in *Western European Workshop on Research in Cryptology, Lectures Notes in Informatics (LNI)*, vol. 74. Citeseer, 2005, pp. 53–63.

[17] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. IT-15, pp. 122–127, 1969.

[18] Klapper, "On the existence of secure feedback registers," in *EUROCRYPT: Advances in Cryptology: Proceedings of EUROCRYPT*, 1996.