

BUPLE: Securing Passive RFID Communication Through Physical Layer Enhancements

Qi Chai and Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
{q3chai, ggong}@uwaterloo.ca

Abstract. Although RFID systems offer many noteworthy characteristics, security and privacy issues associated with them are not easy to address. In this paper, we investigate how to solve the eavesdropping, modification and one particular type of relay attacks toward the tag-to-reader communication in passive RFID systems without requiring lightweight ciphers or secret credentials shared by legitimate parties using a physical layer approach. To this end, we propose a novel physical layer scheme, called *Backscatter modulation- and Uncoordinated frequency hopping-assisted Physical Layer Enhancement* (BUPLE). The idea behind it is to use the amplitude of the carrier to transmit messages as normal, while to utilize its periodically varied frequency to hide the transmission from the eavesdropper/relayer and to exploit a random sequence modulated to the carrier's phase to defeat malicious modifications. We further improve its eavesdropping resistance through the coding in the physical layer as BUPLE ensures that the tag-to-eavesdropper channel is strictly noisier than the tag-to-reader channel. Three practical Wiretap Channel Codes (WCCs) for passive tags are then proposed: two of them are constructed from linear error correcting codes, and the other one is constructed, for the first time to the best of our knowledge, from resilient vector Boolean functions. The security and usability of BUPLE in conjunction with WCCs are further confirmed by our proof of concept implementation and testing on the software defined radio platform with a programmable WISP tag.

Keywords: RFID security, eavesdropping, backscatter, frequency hopping, wiretap channel

1 Introduction

Radio Frequency Identification (RFID), which allows remote identification of objects automatically, is one of the most promising technologies to enable ubiquitous computing and Internet of Things (IoT). The modest computation/storage capabilities of passive or battery-free tags and the necessity to keep their prices low constitute a challenging problem that goes beyond the well-studied problems of modern cryptography. Typical risks are (1) the reader-tag communication via

a radio channel is susceptible to *eavesdropping*, *modification* and *relay*, which are the concerns in this paper; (2) each RFID tag has a unique or fixed identity, which, once it has been captured by a malicious reader, leaks the geometric location of the tag, and invades the privacy of the tag holder; moreover, (3) the lack of tamper-resistant memory makes fabricating or counterfeiting a tag effortless.

To mitigate attacks in (1), this work presents a marked departure from the existing paradigm such as *lightweight cryptography* [8, 2, 19, 14] – we focus on defeating eavesdropping, modification and one particular type of relay attacks toward the tag-to-reader communication in passive RFID systems without requiring on-tag ciphers or secret credentials to be shared by legitimate parties. Our solution exploits the physical layer resources of passive RFID systems, i.e., backscatter modulation, uncoordinated frequency hopping and the coding for the wiretap channel, exhibiting a promising way to provide security functions while keeping the hardware cost of the reader and the tag almost unchanged, as expected in many RFID applications.

1.1 Problem Statement and Security Model

Assuming that a powerful RFID reader shares a common RF channel with a passive tag which is computation and storage-constrained, no secrets or authentication materials are shared by these two entities. We address the following problem: *how could confidentiality, authenticity and integrity of the tag-to-reader communication be preserved in the presence of a budget-limited adversary \mathcal{A} ?* Here, by “confidentiality”, we mean that given an eavesdropped version of the raw signal, to \mathcal{A} , the entropy of the message from the tag does not decrease. By “authenticity”, we mean that the reader should be clear who the sender of the message is. By “integrity”, we mean that malicious modifications to the message can be detected by the reader. By “budget-limited”, we mean that \mathcal{A} ’s RF devices are effective in a narrow frequency band.

We assume that the two communicating entities are legitimate and are not compromised; otherwise, little can be done from the physical layer (issues caused by a malicious reader or an impersonated tag are beyond the scope of this paper). We adopt a Dolev-Yao-alike model that \mathcal{A} controls the communication which allows him to conduct the following actions:

- **Eavesdropping:** \mathcal{A} intercepts tag-to-reader signals, demodulates and decodes to get communicated messages.
- **Modification:** \mathcal{A} either adds to the channel a signal, which converts bit “0” into “1” (called *bit flipping* [7]), or adds to the channel a signal representing a bit string different from the one sent by the tag with a significantly higher power than that of the original signal (called *signal overshadowing* [7]). However, \mathcal{A} is unable to eliminate energy from any channel.
- **Relay:** \mathcal{A} places an active radio device in between a valid reader and a victim tag, e.g., [11], which generates new signals in a narrow frequency band to

answer the valid reader according to the format of backscatter modulation after querying the victim tag.¹

1.2 Our Contributions

To thwart the aforementioned threats, we present the following contributions:

1. We propose a novel physical layer scheme, called *Backscatter modulation- and Uncoordinated frequency hopping-assisted Physical Layer Enhancement* (BUPLE), for passive RF communication. The idea is to use the amplitude of the carrier wave to transmit messages as normal, while to utilize its periodically varied frequency to hide the transmission from the eavesdropper/relayer and to exploit a random sequence modulated to the carrier's phase to defeat malicious modifications. Our rigorous security analysis shows that BUPLE achieves desired security goals without affecting the cost of the reader and the passive tag.
2. BUPLE ensures that \mathcal{A} receives a noisier signal than that of the valid reader, which presents a potential opportunity to further improve its eavesdropping resistance through the coding in the physical layer. Three Wiretap Channel Codes (WCCs) with practical parameters for passive tags and with trade-offs in the *information rate* (the proportion of the data-stream that is non-redundant), the *equivocation rate* (the degree to which the eavesdropper is confused) and the cost of implementation, are given – two of them are constructed from linear error correcting codes, and the other one is constructed, for the first time to the best of our knowledge, from resilient vector Boolean functions.
3. BUPLE and the proposed WCCs are implemented on the software defined radio platform (served as an RFID reader) and a programmable WISP tag. Results from our experimental data well support our theoretic hypothesis and security analysis. Additionally, performance comparison of the proposed WCC encoders with four lightweight ciphers from literature suggests that WCCs consume much less resource and have much higher throughput.

1.3 Related Work

There are a very few physical layer schemes targeting communication confidentiality and integrity in the context of RFID. To construct an unidirectional covert channel from the tag to the reader, cooperative-jamming methods are introduced in [16, 5] for the key distribution. However, bitwise synchronization and required pre-shared secrets between the reader and the friendly jammer may be problematic in real-world applications. Moreover, Savry *et al.* in [25] designed a noisy

¹ There exists another type of relay, for which a malicious passive tag wired with a malicious reader is placed in between the valid reader and the victim tag to relay the communication. Technically, this attack is one kind of tag impersonation, which violates our assumptions made to physical layer schemes thus is not considered here.

reader by exploiting the fact that a passive tag modulates a noisy carrier generated by a reader during its reply. Nevertheless, the noisy carrier could cause severe disruption of all nearby RFID systems. To enable message integrity protection in general wireless communication, [7] presents variants of the Manchester code which make the communication immune to bit flipping and signal overshadowing attacks. By leveraging the physical characteristic that “nothing travels faster than light”, the family of distance bounding protocols, e.g., [13, 18, 1, 29], provides a potential way to solve the relay attack. However, besides the security vulnerabilities discovered in [18, 1], this special-purpose protocol introduces additional communication overhead, and, the authenticity and integrity of the exchanged messages are ensured by symmetric cryptographic primitives.

1.4 Organization

In Section 2, we introduce basic concepts and definitions. In Section 3, we present BUPLE and its security analysis. In Section 4, we give our constructions of the wiretap channel codes for passive tags. A prototype implementation and experimental results are shown in Section 5, including a performance comparison with some lightweight ciphers. We conclude the paper in Section 6.

2 Preliminaries

In this section, we briefly introduce gradients for our scheme: the backscatter modulation, uncoordinated frequency hopping and Wyner’s wiretap channel.

2.1 Backscattering for Passive RF Communication

Radar principles tell us that the amount of energy reflected by an object is proportional to the reflective area of the object. A passive RFID system is principally a radar system in which the reader provides an RF signal for communication in both directions, i.e., from the reader to the tag and the tag to the reader. To be specific, we consider a passive tag composed of an antenna with impedance Z_a and a load with impedance Z_l . The impedance is often a complex quantity, where the real part is the resistance (i.e., R_a, R_l), and the imaginary part is the reactance (i.e., X_a, X_l). According to the *maximum power theorem* in RLC circuit theory [15], if the antenna’s impedance is matched to that of the load (i.e., $R_a = R_l$), no reflection occurs at the interface. On the contrary, if the load is shorted, total reflection occurs and the power is re-radiated by the antenna. Thus by switching between the two states, a backscattered signal is in fact modulated by the Amplitude Shift Keying (ASK).

2.2 Availability of Uncoordinated Frequency Hopping in Passive RFID Systems

Frequency Hopping (FH) communication [26], in which the carrier frequency of a transmitted signal constantly changes according to a pre-shared pseudorandom

sequence, was developed to defeat unintended listeners. *Uncoordinated Frequency Hopping* (UFH) indicates that two entities establish FH communication without sharing any secret. Strasser *et. al.* in [23] considered applying UFH for fighting against a hostile jammer and proposed a hash-chain based pre-authentication scheme. However, implementing this probabilistic scheme is challenging, because: (1) the sender and receiver have less chance to “meet” in a particular channel at a certain time especially when the hopping set is large; (2) synchronization of the sender and the receiver is non-trivial when the hop rate is high, e.g., synchronization signals are vulnerable to jamming.

Nevertheless, we observed that UFH can be practically realized in passive RFID systems due to the following property: the reader changes the carrier frequency, while the tag only has to modulate responses on the carrier and reflect it without concerning which carrier frequency it uses. The reader is then able to center at the right frequency to capture the backscattered signal. Besides, the imperfect time synchronization, which is the main issue in a FH system, can be trivially solved, since the returned signal from the tag is strictly Δt second later than the emitted signal, where Δt is the sum of the tag’s processing time and the signal’s propagation delay in a small distance ($< 20\text{m}$). Finally, FH mechanism is standardized in EPCglobal UHF Class-1 Gen-2 [9] (EPC C1G2) as an optional strategy to eliminate interference in dense reader scenarios and implemented in commercial products. In the light of UFH, our scheme brings confidentiality, authenticity and integrity to the tag-to-reader communication for free. Note that although employing FH to avoid session hijacking was briefly mentioned in [34], the problem that FH signals are usually unable to power up passive tags is not considered, which is addressed in Section 3 of this paper.

2.3 Wiretap Channel

The wiretap channel model, as shown in Figure 1, is introduced by Wyner [33] and extended in [20, 6]. In this model, when the main channel is better than the wiretap channel, i.e., $p_0 < p_w$, where p_0 and p_w are the error probabilities of the main channel and the wiretap channel respectively, it is possible through a particular coding to establish an (almost) perfectly secure source-destination link without relying on any pre-shared keys.

As shown in Figure 1, to send an m -bit message $\mathbf{s} = (s_1, \dots, s_m) \in \mathbb{F}_2^m$, the sender first encodes it into an n -bit codeword \mathbf{x} , which is then propagated through the main channel and wiretap channel simultaneously. The legitimate receiver, e.g., RFID reader, received a corrupted version $\mathbf{y} \in \mathbb{F}_2^n$ of \mathbf{x} while the eavesdropper receives an even more strongly corrupted binary stream $\mathbf{z} \in \mathbb{F}_2^n$. After decoding, all information of \mathbf{s} is expected to be learnt by the legitimate receiver at a code rate as high as possible, while no information about \mathbf{s} is leaked to the eavesdropper. Stated in another way, a wiretap channel has an *achievable secrecy* (R, L) , $0 \leq R, L \leq 1$, if there is an encode-decoder pair such that for any $\eta > 0$ the following is true:

$$\frac{1}{m} \text{Prob}\{\mathbf{s} \neq \mathbf{s}''\} \leq \eta, \quad \frac{m}{n} \geq R - \eta, \quad \Delta = \frac{H(\mathbf{s}|\mathbf{z})}{m} \geq L - \eta \quad (1)$$

where Δ is the equivocation rate and $H(\mathbf{s}|\mathbf{z})$ is the conditional entropy of \mathbf{s} given \mathbf{z} . Wyner exhibited the set of achievable (R, L) pairs always forms a region $\{(R, L) : 0 \leq R, L \leq 1, R \times L \leq h(p_w) - h(p_o)\}$, where $h(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)$ is called the *binary entropy function* of p , and, $h(p_w) - h(p_o)$ is the *secrecy capacity* meaning the maximum rate of a code under which perfect secrecy can be achieved.

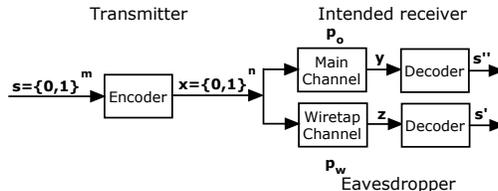


Fig. 1. Wiretap Channel Model [33, 6]

Although this model offers a potential opportunity to achieve Shannon's perfect secrecy (i.e., $\Delta = 1$) without a pre-shared key, two strong assumptions make it less appealing to practitioners: (1) two channels are distinct and the main channel is apparently better. This is difficult to realize in reality; (2) given p_o and p_w , there must exist a code satisfying Eq. (1) (we call such a code *Wiretap Channel Code* or (n, m) -WCC hereafter). Note that general constructions of WCCs (especially those with satisfactory information rate, equivocation rate and finite codeword length) remain an open problem [28].

As shown in Section 3 and 4, our work firstly closes the gap between this theoretic model and practice as: (1) UFH is exploited to significantly degrade the tag-to-eavesdropper channel by increasing p_w ; and (2) three WCCs with small codeword length, targeting practical security, are given which can be implemented in tags with modest computation/storage capability.

3 BUPLE and Its Security

For the rest of the paper, we keep the following notations.

- $\{f_1, \dots, f_M\}$ represents a *hop set* with M possible frequencies and $W = \max(\{f_1, \dots, f_M\}) - \min(\{f_1, \dots, f_M\})$ is the *hopping band*.
- In one hop, t_h is the signal duration, called *hop duration*, (we ignore the transient *switching time* in this paper for simplicity) and W_h is the bandwidth for each frequency channel.
- v_T is the tag's data rate, while v , $v \gg v_T$, is the rate of a random binary sequence generated by the reader, and v_{cmd} is the data rate of reader's commands.
- τ_0 is the power-up time in second for a tag.

VIII

- Total bandwidth $W = 100\text{MHz}$.
- Size of hop set $M = 200$.
- Bandwidth for each frequency channel $W_h = 500\text{kHz}$.
- Hop duration $t_h = 20\mu\text{s}$.

BUPLE-S vs. BUPLE-W: As a result of spreading the power of the signal to hide the transmission, a technical challenge arises: FH signals are usually unable to power up a passive tag – providing the power of FH signals is strong enough to power up a tag, it is also detectable by \mathcal{A} 's envelope detector (even \mathcal{A} is unaware of the carrier's frequency). To address this problem, BUPLE takes different values of E_b , which leads to the following *two sub-schemes*.

- BUPLE-S (“S” for strong): E_b is a great positive float to the extent that CW_i provides enough power for passive tags to operate, i.e., $\int_0^{\tau_0} \sqrt{2E_b} v_T dt > V_{in}$, where V_{in} is the tag's minimum operating voltage, e.g., $V_{in} = 1.8\text{v}$ for WISP v4.1 tags.
- BUPLE-W (“W” for weak): E_b has small numerical values such that CW_i is not detectable by the eavesdropper.

These two sub-schemes differ in several aspects as listed in Table 1: BUPLE-S provides more functionalities while BUPLE-W offers more security properties. For example, although BUPLE-W can neither power up tags nor issue commands, it has full resistance to eavesdropping in tag-to-reader communication when executed right after BUPLE-S. As confirmed by our experiments, few rounds of BUPLE-W could be executed immediately following one round execution of BUPLE-S. This is because the passive tag's capacitor stores constraint energy, which supplies the tag's circuit for a short while even without (enough) power supply from the reader. Depending on the design of upper protocols, BUPLE-S can be used independently, or with BUPLE-W alternatively.

Table 1. Functionalities V.S. security properties of BUPLE-S and BUPLE-W.

	power-up tags	issue cmd	anti-modification	anti-eavesdropping	anti-relay
BUPLE-S	✓	✓	✓	limited	✓
BUPLE-W ^a	×	×	✓	✓	✓

^a when BUPLE-W is executed right after BUPLE-S.

3.2 Security Analysis

Using the adversary model introduced in Section 1.1, we have the following analytical results.

Eavesdropping BUPLE-W: Generally speaking, the detection of FH signals is hard and all existed detectors exploit the known structure of signals [35],

e.g., the hopping sequence is repeated after a short while. With the specified parameters, here we estimate the required *Signal-to-Noise Ratio* (SNR) to detect the presence of signals in BUPLE-W in terms of different types of FH detectors. Following the calculations in [26], given the probability of detection $P_D = 0.7$ and the probability of false alarm $P_{FA} = 10^{-6}$, we have³ (1) for a *wideband radiometer*, the required SNR at \mathcal{A} 's receiver is $SNR_{req} \approx 132\text{dB}$; (2) for a *partial-band filter bank combiner* (PB-FBC) with 50 branches, the required SNR for each channel $SNR_{req,I} \approx 128\text{dB}$; and (3) for an *optimum detector* with exact M branches, e.g., the legitimate reader, $SNR_{req} \approx 123\text{dB}$. This data suggests that \mathcal{A} 's wideband radiometer (PB-FBC resp.) has 9dB (4dB resp.) disadvantage relative to the optimum receiver owned by a legitimate reader. Thus, given the noise power spectrum in a specific environment, if E_b is carefully chosen, only the intended reader is able to receive messages backscattered by tags.

Eavesdropping BUPLE-S: Although BUPLE-S offers a poor eavesdropping resistance, it does differentiate the tag-to-reader channel and the tag-to-eavesdropper channel in the sense that the error probability of the latter is enlarged. Let a backscattered signal be $\widehat{CW}_i = \sqrt{2E_{b,k}V_t} \cos(2\pi f_i t)$, if $k = 0$ or 1 is sent by the tag (ignore the MSK-modulated sequence for the time being). According to the *minimum distance detection* [21], the bit error probability for the tag-to-reader channel is:

$$p_o = Q\left(\frac{\sqrt{E_{b,1}} - \sqrt{E_{b,0}}}{\sqrt{N_o}}\right). \quad (2)$$

where Q is the Gaussian cumulative distribution function.

Providing the eavesdropper listens at a wrong frequency, the received signal is passed through a band-pass filter, which leads a degradation, denoted as δ in dB, $\delta \leq 0$, to both $E_{b,0}$ and $E_{b,1}$, i.e., $E'_{b,0} = 10^{\delta/10} E_{b,0}$, $E'_{b,1} = 10^{\delta/10} E_{b,1}$. Thus the bit error probability for the tag-to-eavesdropper channel is:

$$p_w = Q\left(\frac{10^{\delta/20}(\sqrt{E_{b,1}} - \sqrt{E_{b,0}})}{\sqrt{N_o}}\right), \quad (3)$$

which is greater than p_o as Q is a decreasing function. Given an numerical example, let $E_{b,0} = 4$, $E_{b,1} = 25$, $\delta = -20$ and $N_o = 1$, we have $p_o = 0.0013$ for the intended receiver while $p_w = 0.3821$ for the eavesdropper.

Message Modification: First of all, the *signal overshadowing* is prevented: to inject a high amplitude signal to the channel, \mathcal{A} has to know at which frequency the reader's receiver is working at; otherwise, the inserted signal will be filtered. In BUPLE, the attacker has $\frac{1}{M}$ chance to hit the right frequency. Transmitting the same message N times in different hops further decreases this

³ To enable a tractable analysis, we assume: (1) the tag-to-eavesdropper channel is *Additive White Gaussian Noise* (AWGN); (2) $\{f_1, f_2, \dots, f_M\}$, W , t_{msg} , M , t_h and W_h are public; and (3) \mathcal{A} has exact knowledge of both the time at which a transmission originates and stops; otherwise, \mathcal{A} has 1dB extra disadvantage [26].

probability to $\frac{1}{M^N}$, which is negligible when N is large⁴. Secondly, the *bit flipping* could be eliminated: in order to change “ $r_j = 1$ ” to “ $r_j = 0$ ”, \mathcal{A} needs to modify “10” to “01” in the channel (note that “00” or “11” are illegal codewords that help the reader to detect modification). To change the first bit in “10”, \mathcal{A} has to predict the shape of its carrier and sends the inverted signal to cancel it out. However, this is impossible since, besides the carrier frequency is unknown, the phase of the backscattered carrier is randomized by the MSK-modulated sequence and the channel condition is unpredictable as analyzed in [7].

Relay: In this case, \mathcal{A} produces a well-formatted signal centered at f'_i carrying the relayed information to respond to the reader. The reader ignores this signal generated by the relay with probability $1 - \frac{1}{M}$ since the reader’s receiver always listens at f_i and filters out signals happening in other bands, where the probability, for \mathcal{A} , to have $f'_i = f_i$ is $\frac{1}{M}$. Multiple rounds of executions, say N , further decrease this probability to be negligible, i.e., $\frac{1}{M^N}$.

4 Enhanced BUPLE through Wiretap Channel Codes

As indicated by Eq. (2) and (3), if \mathcal{A} ’s receiver tunes to a wrong frequency, a portion of energy of the backscattered signal is filtered and the demodulated and decoded bit streams are apparently noisier than those received by the intended receiver. Therefore, the wiretap channel model is realized by BUPLE. In this section, we further enhance BUPLE by considering *how could BUPLE-S achieve immunity to eavesdropping to the practical maximum extent possible?*

Our solution relies on the wiretap channel code. As shown in Figure 3, the tag’s message is WCC-encoded before transmission and WCC-decoded by the reader launching BUPLE. Considering the moderate processing/storage capability of passive tags, we require a candidate WCC to have an equivocation rate close to 1 (rather than perfect secrecy), a relatively high information rate and a small codeword length n . In what follows, we assume both channels are *Binary Symmetric Channel* (BSC) with $p_o = 0$ and $p_w > 0$ for simplicity, otherwise a suitable error correction code can be employed to make $p_o = 0$ while keeping $p_w > 0$ (remember $p_w > p_o$). All “ \oplus ”s are addition operations in \mathbb{F}_2 unless otherwise stated and superscript T is the transpose of a vector.

4.1 Parameterized WCCs from Linear Error Correcting Codes

The *coset coding* based on linear error correcting codes with infinite codeword length was first used in Wyner’s proof [33] of the existence of a secrecy-capacity-achieving WCC (see Appendix A). Along this line, our first two constructions concentrate more on: (1) carefully selecting the underlying linear code to maximize the desired security with small n ; and (2) designing of a storage efficient

⁴ There is a confliction that repeated transmissions impair the eavesdropping resistance. In reality, which security property is more important depends on upper layer protocols, e.g., modification resistance is more imperative to protocols in HB⁺ family [19, 14].

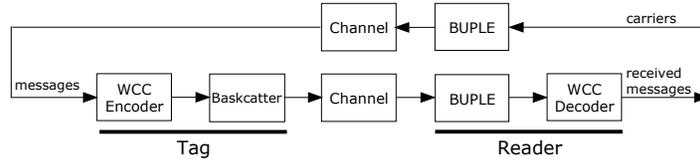


Fig. 3. Enhanced BUPLE Through Wiretap Channel Codes

encoding algorithm, i.e., reducing the storage complex from $O(2^{2m})$ to $O(2^m)$. We thus have the following constructions.

Construction I: (8, 1)-WCC The encoder works as follows: to transmit $\mathbf{s} \in \{0, 1\}$, the encoder outputs a random vector $\mathbf{x} = (x_1, \dots, x_8) \in \mathbb{F}_2^8$ satisfying $x_1 \oplus x_2 \oplus \dots \oplus x_8 = \mathbf{s}$. The decoder at the receiver's side evaluates $x_1 \oplus x_2 \oplus \dots \oplus x_8$ (or $z_1 \oplus z_2 \oplus \dots \oplus z_8$ for \mathcal{A}) to obtain \mathbf{s} (or $\mathbf{s} \oplus \sum_{i=1}^8 e_i$ resp.), where, as received by \mathcal{A} , $z_i = x_i \oplus e_i$ and e_i is an error bit introduced by the channel, i.e., $\text{Prob}\{e_i = 1\} = p_w$. We calculate its rate, equivocation rate and $R \times L$ for different p_w , which are listed in Table 2. Similarly, we could construct a (16, 1)-WCC.

Construction II: (8, 4)-WCC Let $g(\cdot) : \{0, 1\}^4 \mapsto i$, $0 \leq i \leq 15$ be a public injective function and H be the parity check matrix of a (8, 4)-extended hamming code \mathcal{C} , i.e.,

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Moreover, the *cosets* of \mathcal{C} is denoted as C_i , $0 \leq i \leq 15$.

To transmit a 4-bit message \mathbf{s} , the encoder randomly selects a code $\mathbf{c} \in \mathcal{C}$ and XOR it with the coset leader \mathbf{a} of $C_{g(\mathbf{s})}$ to produce \mathbf{x} . The decoder at the receiver's side evaluates $H\mathbf{x}^T$ (or $H\mathbf{z}^T = H(\mathbf{x} \oplus \mathbf{e})^T$ for \mathcal{A}) to obtain $H\mathbf{a}^T = \mathbf{s}$ (or $H(\mathbf{a} \oplus \mathbf{e})^T$ resp.). Here $H\mathbf{a}^T$ is called the *syndrome* of \mathcal{C} . In terms of implementation, this tag needs to store: (1) g of 64-bit; (2) \mathcal{C} of (8×16) -bit; (3) coset leaders of (8×16) -bit; and (4) the syndromes of (16×4) -bit in the tag's memory. That is 384 bits in all. We calculate its rate, equivocation rate and $R \times L$ for different p_w , which are listed in Table 2.

Security Analysis: It is intuitive that after decoding the noise-corrupted codeword $\mathbf{z} = (z_1, \dots, z_n)$, where each z_i can be seen as a random binary variable, \mathcal{A} is ignorant of $\mathbf{s} = (s_1, \dots, s_m)$ if and only if the output of the decoder appears (almost) equally likely ranging from $\underbrace{0 \dots 0}_m$ to $\underbrace{1 \dots 1}_m$. This is achieved by the

above WCCs because of the following theorem, the proof of which is deferred to the full version of this paper.

Theorem 1. Let $\mathbf{s} = (s_1, \dots, s_m) \in \mathbb{F}_2^m$ be the message to be sent and let codewords in the dual of a linear code \mathcal{C} have minimum distance d and let $\text{wt}(H_i)$ be the hamming weight of the i -th row of the parity check matrix H of \mathcal{C} (thus

$wt(H_i) \geq d$). Above WCCs achieve:

$$\begin{aligned} \text{Prob}\{s_1 = 0|\mathbf{z}\} &= \sum_{j \text{ even}}^{wt(H_1)} \binom{wt(H_1)}{j} p_w^j (1-p_w)^{wt(H_1)-j} = \frac{1}{2} + \frac{1}{2}(1-2p_w)^{wt(H_1)} \\ \text{Prob}\{s_1 = 1|\mathbf{z}\} &= \sum_{j \text{ odd}}^{wt(H_1)} \binom{wt(H_1)}{j} p_w^j (1-p_w)^{wt(H_1)-j} = \frac{1}{2} - \frac{1}{2}(1-2p_w)^{wt(H_1)} \\ \text{Prob}\{s_i = 0|s_1, \dots, s_{i-1}, \mathbf{z}\} &= \frac{1}{2} \pm \frac{1}{2}(1-2p_w)^{wt(H_1 \oplus \dots \oplus H_{i-1})} = \frac{1}{2} \pm \frac{1}{2}(1-2p_w)^d, i > 1 \\ \text{Prob}\{s_i = 1|s_1, \dots, s_{i-1}, \mathbf{z}\} &= \frac{1}{2} \mp \frac{1}{2}(1-2p_w)^{wt(H_1 \oplus \dots \oplus H_{i-1})} = \frac{1}{2} \mp \frac{1}{2}(1-2p_w)^d, i > 1 \end{aligned}$$

$$\begin{aligned} \left(\frac{1}{2} - \frac{1}{2}(1-2p_w)^d\right)^m &\leq \text{Prob}\{s|\mathbf{z}\} = \text{Prob}\{s_1|\mathbf{z}\} \times \prod_{i=2}^m \text{Prob}\{s_i|s_1, \dots, s_{i-1}, \mathbf{z}\} \\ &\leq \left(\frac{1}{2} + \frac{1}{2}(1-2p_w)^d\right)^m. \end{aligned}$$

Therefore, above WCCs have an achievable secrecy (R, L) , as defined by Eq. (1), such that

$$R = \frac{m}{n}, \quad -\log_2\left(\frac{1}{2} + \frac{1}{2}(1-2p_w)^d\right) \leq L \leq 1.$$

4.2 WCCs Constructed from Resilient Boolean Functions

As we observed, the decoding process (e.g., $H(\mathbf{x} \oplus \mathbf{e})^T : \{0, 1\}^n \mapsto \{0, 1\}^m$ in Construction II) can be generalized as passing the noise-corrupted codeword through a well-designed S-box as shown below: when $(\mathbf{x} \oplus \mathbf{e})^T$ is not random as $p_w < 0.5$, the output of the S-box can be sufficiently random such that each output bit appears to be “0” and “1” (almost) equally likely. The tool of design for such an S-box is the *Boolean theory*, particularly, *vector resilient Boolean functions*. We refer the reader to [3] for unexplained definitions.

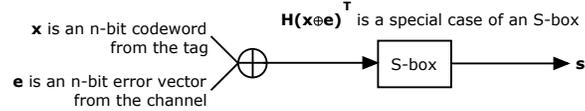


Fig. 4. The WCC decoder can be generalized as an S-box.

We propose the following theorem without proof here, which provides a striking connection between (n, m) -WCC and (n, m, t) -resilient vector Boolean functions for the first time to our best knowledge.

Theorem 2. *An (n, m, t) -resilient Boolean function $f(\cdot)$ can be used to construct an (n, m) -WCCs by letting the encoder be $f^{-1}(\cdot)$ and the decoder be $f(\cdot)$. All results in Theorem 1 is still valid by replacing d with $t + 1$.*

Theorem 2 generalizes the two aforementioned WCCs as there exists a linear (n, m, t) -resilient vector Boolean function if and only if there exists a $[n, m, d = t + 1]$ -linear code [3]. More importantly, we are interested in nonlinear WCCs with better overall performance, which is rooted in the fact that a nonlinear code with good parameters may exist while a linear function with the same parameters does not exist [24]. In light of the Kerdock code as studied in [24], we have the following novel construction of a WCC using the nonlinear code.

Construction III: (16, 8)-WCC Let $\mathbf{x} = (x_1, \dots, x_{16}) \in \mathbb{F}_2^{16}$, where $f(\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_8(\mathbf{x})) =$

$$\begin{aligned} & (x_9 \oplus (x_1 \oplus x_2 \oplus x_4 \oplus x_7 \oplus x_8 \oplus (x_1 \oplus x_5)(x_2 \oplus x_3 \oplus x_4 \oplus x_6) \oplus (x_2 \oplus x_3)(x_4 \oplus x_6)), \\ & x_{10} \oplus (x_2 \oplus x_3 \oplus x_5 \oplus x_1 \oplus x_8 \oplus (x_2 \oplus x_6)(x_3 \oplus x_4 \oplus x_5 \oplus x_7) \oplus (x_3 \oplus x_4)(x_5 \oplus x_7)), \\ & x_{11} \oplus (x_3 \oplus x_4 \oplus x_6 \oplus x_2 \oplus x_8 \oplus (x_3 \oplus x_7)(x_4 \oplus x_5 \oplus x_6 \oplus x_1) \oplus (x_4 \oplus x_5)(x_6 \oplus x_1)), \\ & x_{12} \oplus (x_4 \oplus x_5 \oplus x_7 \oplus x_3 \oplus x_8 \oplus (x_4 \oplus x_1)(x_5 \oplus x_6 \oplus x_7 \oplus x_2) \oplus (x_5 \oplus x_6)(x_7 \oplus x_2)), \\ & x_{13} \oplus (x_5 \oplus x_6 \oplus x_1 \oplus x_4 \oplus x_8 \oplus (x_5 \oplus x_2)(x_6 \oplus x_7 \oplus x_1 \oplus x_3) \oplus (x_6 \oplus x_7)(x_1 \oplus x_3)), \\ & x_{14} \oplus (x_6 \oplus x_7 \oplus x_2 \oplus x_5 \oplus x_8 \oplus (x_6 \oplus x_3)(x_7 \oplus x_1 \oplus x_2 \oplus x_4) \oplus (x_7 \oplus x_1)(x_2 \oplus x_4)), \\ & x_{15} \oplus (x_7 \oplus x_1 \oplus x_3 \oplus x_6 \oplus x_8 \oplus (x_7 \oplus x_4)(x_1 \oplus x_2 \oplus x_3 \oplus x_5) \oplus (x_1 \oplus x_2)(x_3 \oplus x_5)), \\ & \Sigma_{i=1}^{16} x_i). \end{aligned} \quad (4)$$

Let the encoder be $f^{-1}(\mathbf{x})$ and the decoder be $f(\mathbf{x})$. To transmit an 8-bit message \mathbf{s} , the encoder outputs a 16-bit random binary vector \mathbf{x} such that $f(\mathbf{x}) = \mathbf{s}$. The decoder at the receiver's side simply evaluates $f(\mathbf{x})$ (or $f(\mathbf{x} \oplus \mathbf{e})$ for \mathcal{A} given \mathbf{x} (or $\mathbf{x} \oplus \mathbf{e}$ resp.) is received. This construction is optimum as its $R \times L$ is closest to the secrecy capacity as shown in Table 2.

Table 2. Comparison of performances of proposed WCCs.

(n, m)	underlying code	rate	equivocation rate	$R \times L$
$p_w = 0.20$, secrecy capacity = $h(p_w) = 0.721928094887$				
(8, 1)	parity check	0.1250	0.99979649036	0.12497456129
(8, 4)	ext. hamming	0.5000	0.96977096204	0.48488548102
(16, 8)	Kerdock	0.5000	0.98711512719	0.49355756360
$p_w = 0.10$, secrecy capacity = $h(p_w) = 0.468995593589$				
(8, 1)	parity check	0.1250	0.97959953172	0.12244994146
(8, 4)	ext. hamming	0.5000	0.78495689709	0.39247844855
(16, 8)	Kerdock	0.5000	0.82311413681	0.41155706840
$p_w = 0.05$, secrecy capacity = $h(p_w) = 0.286396957116$				
(8, 1)	parity check	0.1250	0.86186434726	0.10773304341
(8, 4)	ext. hamming	0.5000	0.53233802320	0.26616901160
(16, 8)	Kerdock	0.5000	0.55356866398	0.27678433199

4.3 Visualize the Security of Proposed WCCs

We calculate the information rate, the exact equivocation rate and $R \times L$ of each WCC with different p_w , which are listed in Table 2. As seen, there is no one-size-fits-all WCC: Construction I is an extreme case when confidentiality is

to be taken care of, with an imperative shortcoming in its lowest transmission rate; Construction II and Construction III are rate-efficient codes at the cost of lower equivocation rates.

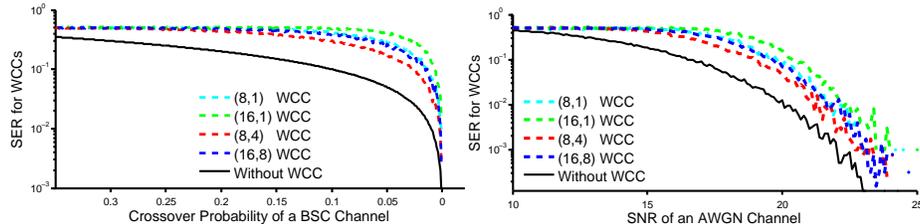


Fig. 5. Simunlink Simulation for RFID systems

To observe the real-world effects of the proposed WCCs, with Simulink, we built a digital communication system composing of a random message generator, a WCC encoder/decoder, an ASK modulator with 915MHz carrier, a BSC or AWGN channel and an envelope detector. The Symbol Error Rate (SER) is simulated and calculated to validate that WCCs further improves the eavesdropping resistance. As shown in Figure 5, the SER in BSC increases with p_w if no coding is involved (the given plots use a logarithmic scale for the y-axis). An interesting result is that the distance or resiliency of each WCC can be visualized as its maximum geometric distance away from the solid line. Besides, the plot of SER in AWGN on the right shows that the intended receiver has approximately 5dB advantage of SNR (relative to the eavesdropper) to achieve the same SER.

5 Proof-of-Concept Implementation and Testing

In the following, we present our proof-of-concept implementation and testing of BUPLE and proposed WCCs.

5.1 Experiment Setup

We built a physical-layer programmable reader using the Universal Software Radio Peripherals (USRP v1.0) [10] together with two RFX900 daughter boards (with the filters bypassed to get a 500mW peak output power): we use one RFX900 with a VERT900 antenna [30] to serve as the frontend of the transmitter (call them RFX900-Tx hereafter) and another RFX900 with a circular polarity panel antenna [4] to be the frontend of a narrowband receiver (call them RFX900-Rx hereafter). In the receiving path, RFX900-Rx samples raw UHF signals by an ADC and then converts them to baseband signals by a digital downconverter (DDC). The baseband digital signals out of USRP are sent via USB 2.0 interface to the Thinkpad T410 laptop running GNU Radio [12], a free software toolkit

for signal processing from the physical layer, under the 32-bit Ubuntu 10.04. The transmission path is similar, but consists of digital upconverters (DUC) and a DAC. Parallel to this, a DP07104 digital phosphor oscilloscope is used for measurements.

To observe behaviors of a passive tag, the WISP v4.1 tag [32], is employed. The reasons for the selection are: (1) it is programmable due to its 16-bit general purpose MSP430F2132 microcontroller. Programs for MSP430F2132 are written in embedded C and compiled, debugged and profiled with IAR Embedded Workbench 5.10.4, in conjunction with TI FET430UIF debugger; (2) it simulates every aspect of a passive tag in terms of limited and ephemeral energy storage and backscatter communication; (3) it implements a significant portion of EPC C1G2 commands, e.g., QUERY and QUERYREP.

Table 3. Actual measures of the output voltages at port TX/RX of RFX900 with respect to the scale factor.

scale factor	output voltage	scale factor	output voltage
10	0.00mv	5000	2.124v
500	144mv	10000	2.880v
1000	396mv	25000	3.208v
2000	864mv	32767	3.312v

In what follows, we use an integer called *scale factor* in $[-2^{16} + 1, 2^{16} - 1]$ to represent the amplitude of a signal without unit. The actual measures of the output voltages at port TX/RX of RFX900 (without antenna) with respect to this scale factor is provided shown in Table 3.

5.2 Our Implementation

In our implementation, BUPLE-W and BUPLE-S are executed alternatively. We first developed a signal processing block for GNU Radio, in conjunction with our customized FPGA firmware, to generate a two leveled carrier signal with period 0.5s, where the high level of the amplitude 25000 represents BUPLE-S while the low level of the amplitude 3000 represents BUPLE-W (this amount, as we tested in an independent session, cannot drive the tag). In addition, our block randomly tunes the frequency of both RFX900-Tx and RFX900-Rx every 0.5s. Finally, we wrote a Python script to create and control *signal flow graphs*, in which, the gain of the receiver's antenna is set to 20dB, and the received signal is decimated by USRP with a factor of 32; right before demodulation, the decimated signals are again filtered by an 8-th order low-pass filter with gain 2, cutoff frequency of 400KHz. Therefore a narrowband receiver is realized. Note that here the specified hop rate cannot be implemented as there are many delays along the digitization path of USRP such as RF frontend settling time, FPGA FIFO filling time, USB transferring time, etc..



Fig. 6. Devices employed in our implementation and testing: one DP07104 oscilloscope, one USRP (v1.0), two RFX900 daughterboards, one VERT900 antenna, one circular polarity panel antenna, one WISP tag (v4.1) and one TI FET430UIF debugger.

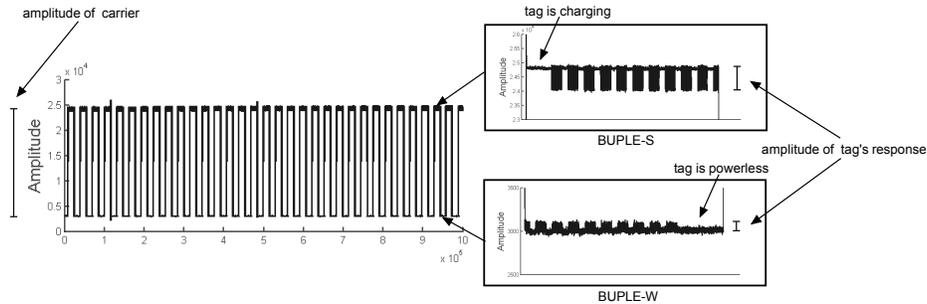


Fig. 7. Time domain measurements when BUPLE works with a WISP tag.

For the tag side, we slightly modified the firmware of the WISP tag to let it intermittently answers “10101010101010”⁵ at $v_T = 250\text{KHz}$ followed each time by a sleep, when it has enough power, rather than implementing the command-based reader-tag interaction. This is because our physical layer scheme is essentially independent from upper layer protocols. Figure 7 exhibits how our scheme works in a standard office setting with the tag placed in between the transceiver and receiver – it is 9.8cm away from RFX900-Tx’s antenna and 131cm away from RFX900-Rx’s antenna. As we can see, the backscatter communication carries out normally in BUPLE-S while it can only last for a while in BUPLE-W before the tag uses up its power. As long as the execution time of BUPLE-W is reduced, it is possible to keep the tag always alive.

Eavesdropping BUPLE Enhanced Communication: To further investigate the eavesdropper’s performance while BUPLE is running, we conducted the following tests in the same physical environment: centering RFX900-Tx at 915MHz while centering RFX900-Rx at frequencies ranging from 915MHz to 918MHz, we measured the amplitudes of the backscattered signals on BUPLE-S

⁵ This actually transmits a “1”: the tag encodes “1” as “11111111” with the (8,1)-WCC, and each “1” in “11111111” is mapped to “10” as specified by BUPLE.

and BUPLE-W respectively, which are expected to exhibit the loss of communication reliability if the eavesdropper works at a wrong frequency.

We tabulated the results in Table 4. In both BUPLE-S and BUPLE-W, the carrier’s amplitudes as well as those of the tag’s responses drop quickly if the eavesdropper’s receiver is not centered at the right frequency. By “N/A”, we mean the signal is submerged in noise and cannot be observed. The experimental evidences support the theoretic hypothesis that to detect the presence of frequency hopped signals in BUPLE-W is non-trivial, let alone demodulate and decode them. We conducted this experiment for reader/tag/eavesdropper with varying distances/angles and get the similar results.

Table 4. Amplitudes of signals captured by the eavesdropper working at 915MHz to 918MHz.

Rx’s Freq.	BUPLE-S		BUPLE-W	
	amp. of carrier	amp. of tag’s response	amp. of carrier	amp. of tag’s response
915MHz	24700	564	2980	91
916MHz	6000	389	600	N/A
917MHz	4300	210	270	N/A
918MHz	300	N/A	200	N/A

Implementing On-tag WCC Encoders: To evaluate the cost of WCC encoders, we implemented them on the MSP430F2132 of a WISP tag (without WISP’s firmware since the firmware itself consumes a considerable portion of SRAM [27]) and tested memory consumption and throughput. We employ a 23-stage LFSR with each stage in \mathbb{F}_2^8 as the random source for each WCC. To be mentioned, the encoding processes of (8,1)-WCC and (8,4)-WCC are implemented using pre-computed lookup tables while that of (16,8)-WCCs is computed on-the-fly by the underlying Boolean calculations. This is because when $n = 16$, the desired lookup table (of size 128KB) is far greater than the memory provided. To generate the code with maximal speed, we set the optimization level to be “high-speed” for the compiler. We then record the cycle counts through the FET debugger by letting the encoders execute at 8MHz on MSP430F2132 for 1000 times with random messages as inputs.

Table 5. Performance comparison of the proposed WCC encoders and four lightweight ciphers from literature. Note that PRESENT is implemented on a different-but-similar microcontroller platform – Atmel AVR ATmega163.

	SRAM [byte]	Flash [byte]	Initialization [cycle]	Throughput [bits/sec]
(8,1)-WCC	690	0	0	740,936
(8,4)-WCC	732	0	0	621,346
(16,8)-WCC	1,348	0	0	86,776
Hummingbird[8]	1,064	0	9,667	53,024
AES[17]	13,448	92	1,745	199,377
KASUMI[17]	9,541	64	1,381	90,395
PRESENT [22]	2,398	528	–	53,361

Table 5 summarizes the performance of WCC encoders, together with that of four lightweight ciphers implemented on the same or similar microcontroller platforms. Thanks to the simple operations, WCCs consume less resource and have higher throughput. The (16, 8)-WCC encoder is resource-hungry because the pure embedded C code, as we used, is inefficient to process Boolean functions such as Eq. (4). Appropriate mixing of inline assembly code will allow the consumed resource be further decreased; this is part of our future work. Another noteworthy merit is that WCCs are more survivable in a frequent-loss-of-power environment since (1) they have the zero initialization time; and (2) they have a very small computation granularity, e.g., the only operation needed is a simple mapping from $\{0, 1\}^m$ to $\{0, 1\}^n$. On the contrary, an on-tag cipher, composing of many operations in series, is more likely to be interrupted. In all, together with Table 2, we found that (8, 4)-WCC makes the information rate, the security and the implementation cost well-balanced, which is a favorable choice for practitioners.

6 Conclusion

Given the likely importance of RFID technology in practice, security and privacy problems should be solved before worldwide deployment. In this paper, we propose to enhance the physical layer of the passive RFID communication. The security and usability are further confirmed by our implementations and testing results. Through the BUPLE scheme and proposed WCCs, a confidentiality-, authenticity- and integrity-preserving channel is created for tag-to-reader communication. It is also worth emphasizing that our solutions are designed for, but not limited to passive RFID systems, e.g. it is applicable to the backscatter wireless sensor network, e.g., [31], for establishing secret communication.

References

1. G. Avoine, C. Floerkemeier and B. Martin, RFID distance bounding multistate enhancement, *Progress in Cryptology, INDOCRYPT'09*, LNCS 5922, Springer-Verlag, pp. 290-307, 2009.
2. A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin and C. Vikkelsoe, PRESENT: an ultra-lightweight block cipher, *Cryptographic Hardware and Embedded Systems, CHES'07*, pp. 450-466, 2007.
3. C. Carlet, *Vectorial Boolean Functions For Cryptography*, Cambridge University Press, 2010.
4. Circular Polarity Pane Antenna, <http://www.arcadianinc.com/datasheets/4123.pdf>.
5. C. Castelluccia and G. Avoine, Noisy tags: a pretty good key exchange protocol for RFID tags, *International Conference on Smart Card Research and Advanced Applications*, LNCS 3928, Springer-Verlag, pp. 289-299, 2006.
6. I. Csiszar, J. Korner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339-348, 2002.
7. M. Cagalj, S. Capkun, R. Rengaswamy, I. Tsigkogiannis, M. Srivastava and J.P. Hubaux, Integrity (I) codes: message integrity protection and authentication over

- insecure channels, *29th IEEE Symposium on Security and Privacy, S&P'08*, pp. 279-294, 2006.
8. D. Engels, X. Fan, G. Gong, H. Hu and E. M. Smith, Hummingbird: ultra-lightweight cryptography for resource-constrained devices, *14th International Conference on Financial Cryptography and Data Security, FC'10*, pp. 3-18, 2010.
 9. EPC Global, Class 1 Generation 2 UHF air interface protocol standard v1.2, <http://www.epcglobalinc.org>, 2008.
 10. Ettus Research LLC, The USRP and RFX900 daughter boards, <http://www.ettus.com/products>.
 11. L. Francis, G. Hancke, K. Mayes and K. Markantonakis, Practical NFC peer-to-peer relay attack using mobile phones, *Workshop on RFID Security, RFIDSec'10*, LNCS 6370, Springer-Verlag, pp. 35-49, 2010.
 12. GNU Radio, <http://www.gnu.org/software/gnuradio>.
 13. G. Hancke and M. Kuhn, An RFID distance bounding protocol, *Conference on Security and Privacy for Emerging Areas in Communication Networks, SecureComm'06*, 2005.
 14. H. Gilbert, M.J.B. Robshaw and Y. Seurin, HB#: increasing the security and efficiency of HB⁺, *Advances in Cryptology, EUROCRYPT'08*, pp. 361-378, 2008.
 15. D.M. Dobkin, *The RF in RFID: passive UHF RFID in practice*, Newnes, 2007.
 16. A. Juels, R. L. Rivest and M. Szyldo, The blocker tag: selective blocking of RFID tags for consumer privacy, *10th ACM Conference on Computer and Communications Security, CCS'03*, pp. 103-111, 2003.
 17. Y. W. Law, J. Doumen and P. Hartel, Survey and benchmark of block ciphers for wireless sensor networks, *ACM Transactions on Sensor Networks*, vol. 2, no. 1, pp. 65-93, 2006.
 18. J. Munilla and A. Peinado, Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels, *Wireless Communications and Mobile Computing*, vol. 8, no. 9, pp. 1227-1232, 2008.
 19. K. Ouafi, R. Overbeck and S. Vaudenay, On the security of HB# against a Man-in-the-Middle attack, *Advances in Cryptology, ASIACRYPT'08*, pp. 108-124, 2008.
 20. L.H. Ozarow and A.D. Wyner, Wire-tap channel II, *Advances in Cryptology, EUROCRYPT'84*, pp. 33-50, 1985.
 21. M.B. Pursley, *Introduction to Digital Communications*, Pearson Prentice Hall, 2005.
 22. A. Poschmann, Lightweight cryptography - cryptographic engineering for a pervasive world, Ph.D. Thesis, Ruhr-Universitaet Bochum, Germany, 2009.
 23. M. Strasser, S. Capkun, C. Popper and M. Cagalj, Jamming-resistant key establishment using uncoordinated frequency hopping, *29th IEEE Symposium on Security and Privacy, S&P'08*, pp. 64-78, 2008.
 24. D.R. Stinson and J.L. Massey, An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions, *Journal of Cryptology*, vol. 8, no. 3, pp. 167-173, 1995.
 25. O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert and J. Reverdy, RFID noisy reader: how to prevent from eavesdropping on the communication?, *9th International Workshop on Cryptographic Hardware and Embedded Systems, CHES'07*, vol. 4727, pp. 334-345, 2007.
 26. M.K. Simon, J. K. Omura, R.A. Scholtz and B.K. Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill Professional Publishing, 2001.
 27. N. Saxena and J. Voris, We can remember it for you wholesale: implications of data remanence on the use of RAM for true random number generation on RFID tags, *Workshop on RFID Security, RFIDSec'09*, 2009.

28. A. Thangaraj, S. Dihidar, A.R. Calderbank, S.W. McLaughlin and J.M. Merolla, Applications of LDPC codes to the wiretap channel, *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933-2945, 2007.
29. R. Trujillo-Rasua, B. Martin and G. Avoine, The poulidor distance-bounding protocol, *Workshop on RFID Security, RFIDSec'10*, LNCS 6370, Springer-Verlag, pp. 239-257, 2010.
30. VERT900 Antenna, <http://www.ettus.com/downloads/VERT900.pdf>.
31. G. Vannucci, A. Bletsas and D. Leigh, A software-defined radio system for backscatter sensor networks, *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2170-2179, 2008.
32. Wireless Identification and Sensing Platform (WISP), <http://wisp.wikispaces.com>.
33. A.D. Wyner, The wire-tap channel, *Bell Systems Technical Journal*, vol. 54, pp. 1355-1387, 1975.
34. S. Weis, S. Sarma, R. Rivest and D. Engels, Security and privacy aspects of low-cost radio frequency identification systems, *Security in Pervasive Computing*, pp. 50-59, 2004.
35. S. Haykin, Cognitive radio: brain-empowered wireless communications, *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, 2005.

A Wyner's Coset Coding

Let \mathcal{C} be an $[n, n-m]$ binary linear code with the parity check matrix H . We can partition the n -bit vector space \mathbb{F}_2^n into 2^{n-m} subsets in the following fashion. For any fixed vector $\mathbf{a} \in \mathbb{F}_2^n$, the set,

$$C_i = \mathbf{a} \oplus \mathcal{C} = \{\mathbf{a} \oplus \mathbf{c} | \mathbf{c} \in \mathcal{C}\},$$

is called a *coset* of \mathcal{C} . Two cosets are either disjoint or coincide (partial overlap is impossible). The minimum weight vector in a coset is called the *coset leader*. It may have more than one coset leaders, then just randomly chooses one. In addition, let $g_1(\cdot) : \{0, 1\}^m \mapsto i$, $0 \leq i \leq 2^m - 1$, $g_2(\cdot) : \{0, 1\}^m \mapsto \{0, 1\}^m$ be two public injective functions.

To transmit an m -bit secret message \mathbf{s} , the sender propagates over the channel an n -bit vector \mathbf{x} , which is selected randomly among all vectors in $C_{g_1(\mathbf{s})}$. Let \mathbf{a} be the coset leader of $C_{g_1(\mathbf{s})}$. The intended receiver decodes by computing:

$$H\mathbf{x}^T = H(\mathbf{c}^T \oplus \mathbf{a}^T) = H\mathbf{a}^T, \quad \mathbf{s} = g_2(H\mathbf{a}^T),$$

where the second last identity comes from $H\mathbf{c}^T = \mathbf{0}$, which is the property of the linear code \mathcal{C} . On the other hand, after receiving $\mathbf{z} = \mathbf{x} + \mathbf{e}$ where $\mathbf{e} \in \mathbb{F}_2^n$ is a binary error vector introduced by the noisy channel, the eavesdropper does the following:

$$H(\mathbf{x} \oplus \mathbf{e})^T = H(\mathbf{c}^T \oplus \mathbf{a}^T \oplus \mathbf{e}^T) = H(\mathbf{a}^T \oplus \mathbf{e}^T), \quad \mathbf{s}' = g_2(H(\mathbf{a}^T \oplus \mathbf{e}^T)),$$

which implies that the transmitted message is masked by a true random sequence \mathbf{e} . In our implementations, $g_2(\cdot)$ is saved by arranging the syndrome in a proper order.