Securing RFIDs by Randomizing the Modulation and Channel

Haitham Hassanieh, Jue Wang, and Dina Katabi, *Massachusetts Institute of Technology; Tadayoshi Kohno, University of Washington*

https://www.usenix.org/conference/nsdi15/technical-sessions/presentation/hassanieh
Securing RFIDs by Randomizing the Modulation and Channel

Haitham Hassanieh  Jue Wang  Dina Katabi  Tadayoshi Kohno
MIT  MIT  MIT  University of Washington

Abstract—RFID cards are widely used in sensitive applications such as access control and payment systems. Past work shows that an eavesdropper snooping on the communication between a card and its legitimate reader can break their cryptographic protocol and obtain their secret keys. One solution to this problem is to install stronger encryption on the cards. However, RFIDs’ size, power, and cost limitations do not allow for strong encryption protocols. Further, changing the encryption on the cards requires revoking billions of cards in consumers’ hands, which is impracticable.

This paper presents RF-Cloak, a solution that protects RFIDs from the above attacks, without any changes to today’s cards. RF-Cloak achieves this performance using a novel transmission system that randomizes both the modulation and the wireless channels. It is the first system that defends RFIDs against MIMO eavesdroppers, even when the RFID reader has no MIMO capability. A prototype of our design built using software radios demonstrates its ability to protect commercial RFIDs from both single-antenna and MIMO eavesdroppers.

1. INTRODUCTION

Ultra-low power RFIDs are widely used in a variety of sensitive applications such as access control, payment systems, and asset tracking [21, 51, 71]. Some of the most well-known examples include the U.S. Passport Card, Zipcar key, MasterCard PayPass, RFID-equipped pharmaceuticals, and MBTA subway cards [38, 44, 45, 55, 72]. As a result of their ultra-low cost, ultra-low power requirements, these systems typically adopt weak encryption protocols [34, 59] or lack encryption altogether [63], leaving them widely exposed to security threats [38, 49].

Past attacks on commercial RFID systems have employed passive eavesdropping [10, 22, 58, 67]. In these attacks, an adversary snooping on the wireless medium intercepts the conversation between a legitimate RFID reader and an RFID card to obtain the sensitive data transmitted by the card. For example, the secret key in over one billion MIFARE Classic cards, widely used in access control and ticketing systems, can be obtained in real-time from an overheard conversation [22]. Similarly, the cipher used in RFID-based anti-theft devices for modern cars has been broken in under 6 minutes using eavesdropped information [67].

In theory, eavesdropping attacks can be addressed with more sophisticated encryption protocols than those typically used in RFIDs. Such an approach, however, would translate into more expensive, power-consuming cards, which goes against the main goal of the RFID industry, namely to dramatically reduce the size and cost of RFIDs so as to allow ubiquitous use [21]. Further, replacing the encryption requires revoking billions of RFIDs in consumers’ hands, an impractical and costly endeavor.

In this paper, we introduce RF-Cloak, a system that defends RFIDs against eavesdroppers, without requiring any modifications to the RFID cards. RF-Cloak exploits that RFID cards do not generate their own transmission signal; they communicate by reflecting the signal transmitted by the RFID reader. In today’s RFID systems, the reader transmits a constant waveform $c(t)$, and a nearby card multiplies (i.e., modulates) this waveform by its data $x$ through reflection, producing $x \cdot c(t)$. In RF-Cloak, we replace the reader’s constant waveform, $c(t)$, by a random signal, $r(t)$, which also makes the card’s reflected message, $x \cdot r(t)$, appear random. Since the eavesdropper does not know the random waveform, he cannot extract the card’s data from what he hears. In contrast, the reader is the one who generates the random waveform, and thus is able to decode by removing its effect. We refer to this technique as random modulation. We formally analyze it and characterize its security guarantees.

Random modulation is effective at defending against a single-antenna eavesdropper. However, random modulation alone cannot defend against a more powerful MIMO eavesdropper. This vulnerability is due to the fact that a MIMO system with $n$ receivers can separate $n$ signals [36, 65], which allows a MIMO eavesdropper to separate the card’s signal from that of the reader. This is a fundamental problem with defending against MIMO eavesdroppers. The solution to this problem is to use a MIMO system on the reader that has at least as many transmitters as there are receivers on the MIMO eavesdropper [36]. Such a solution, however, creates a MIMO battle between the reader and the eavesdropper, where the reader has to keep increasing its MIMO transmitters to match the eavesdropper’s MIMO capability.

In RF-Cloak, we present a novel solution that enables a reader with no MIMO capability to securely communi-
cate with insecure cards, even in the presence of MIMO eavesdroppers. Specifically, a MIMO system relies on the channels being relatively static within a packet to be able to decode. Our key idea is to randomize the wireless channels from the reader to the MIMO eavesdropper to prevent it from correctly decoding. We analyze the impact of channel randomization and prove that it enables a reader with no MIMO capability to overcome a MIMO eavesdropper, even if it has a very large MIMO system.

To implement channel randomization in practice, we leverage recent results in wireless communication which show that, due to multipath, even small motion of the antenna can create large variations in the wireless channel [2, 50]. Thus, our system uses a rotating frame with multiple antennas, and randomly switches between the antennas using rapid switches.\(^1\) We empirically show that this creates fast varying channels with a random distribution. We note that our design uses a single transmit chain on the reader — i.e., no MIMO. However, it provides the channel diversity of a MIMO transmitter with a huge number of antennas, which renders a MIMO eavesdropper unable to decode.

We study RF-Cloak’s security guarantees both analytically and empirically. In particular, we implement the RF-Cloak reader on USRP software radios and evaluate it with commercial RFIDs in both the HF and UHF bands. Our evaluation reveals the following:

- **Random modulation is effective at protecting RFIDs from single-antenna eavesdroppers.** When the eavesdropper uses the optimal decoder which is the maximum likelihood decoder, he experiences a mean bit error rate of 49.8% for HF RFIDs and 50.3% for UHF RFIDs (and a standard deviation of 0.8% for HF and 2.3% for UHF), which is similar to the bit error rate of a random guess. On the other hand, the trusted RF-Cloak reader continues to be able to decode the RFID message.

- **Combining random modulation with channel randomization, an RF-Cloak reader with no MIMO capability causes the mean bit error rate of a MIMO eavesdropper to be 50%, even if the eavesdropper has a MIMO system with 3, 4 or 5 receivers.** The standard deviation ranges between 1.2% and 2.9%, depending on the number of receivers at the eavesdropper. Hence, RF-Cloak provides an effective mechanism to defend against a MIMO eavesdropper.

**Contributions:** This paper presents the first system that protects unmodified RFID cards from eavesdropping attacks, even if the eavesdropper has a large MIMO system and the reader has no MIMO capability. The paper introduces novel algorithms that randomize both the modulation and the wireless channels to the eavesdropper. It analytically proves its security guarantees and empirically demonstrates the benefits of its design. We believe that RF-Cloak addresses a real world problem that threatens the security of commercial RFIDs such as those used in car anti-theft solutions [67], and MBTA subway payment control [22].

2. **Threat Model**

We address passive eavesdropping attacks on commercial RFID cards in the HF and UHF bands, including cards with and without cryptographic protection.\(^2\) In this attack, an adversary listening on the wireless medium intercepts the conversation between a legitimate reader and an RFID card and seeks to obtain confidential information contained in the card. In the simplest case, the adversary can learn the ID of the card, which threatens the privacy of the party carrying the card and enables cloning attacks. The adversary may also obtain sensitive data transmitted by the card, such as biometric information and passwords. Further, the adversary can reverse engineer the encryption and extract the secret key based on the eavesdropped information [10, 22].

The adversary may use standard or custom-built hardware with high receiver sensitivity including multi-antenna MIMO devices. Also, he may be in any location with respect to the card and the reader.

We secure the communication from the RFID card to the reader. We assume the commands transmitted from the reader to the card do not contain sensitive information. This assumption is justified since for HF cards (e.g., MIFARE), listening to the reader’s messages alone does not allow the eavesdropper to extract the secret key and decode the card’s encrypted data [10, 22]. For UHF cards, this assumption is satisfied as long as the reader acknowledges cards using only their temporary IDs, an option readily available for today’s RFID readers [19].

We also assume that the reflected signal from the RFID card is significantly weaker than the direct signal from the reader. This assumption is valid for both HF and UHF systems [7, 18, 53]. In practice, the reflection is 20 to 30 dB weaker than the direct high power RF signal generated by the reader, because the card’s circuit reflects only a small portion of the power it receives [37, 56].

Finally, this paper focuses on passive attacks as opposed to active attacks, in which an adversary repeatedly queries an RFID card to infer the secret key or obtain confidential information. Active RFID attacks are harder to mount than passive attacks. First, they have a shorter range because the attacker needs to power the RFID card [28, 29, 38, 49]. For example, for HF RFIDs,\(^2\) eavesdropping attacks have been successfully mounted on a variety of RFIDs that employ cryptographic protection [10, 22].

---

\(^1\)Cheap switches [20] can switch every few microseconds, which is faster than individual bits in an RFID transmission.

\(^2\)Eavesdropping attacks have been successfully mounted on a variety of RFIDs that employ cryptographic protection [10, 22].
an active adversary needs to be within a few centimeters from the card whereas a passive eavesdropper can be more than 4 meters away [28]. Second, there are few practical and commercial solutions for protecting RFIDs from active attacks, including shielding sleeves which are used in US Passport Cards [38], RFID blocking wallets [52, 64], RFID reader detectors [43].

3. RFID Communication Primer

RFIDs mainly operate in two frequency bands: the High Frequency band (HF 13.56 MHz), where the communication range is about 10 cm [7], and the Ultra High Frequency band (UHF 902 MHz–928 MHz), where the communication range can reach a few meters [11]. RF-Cloak protects both types of RFIDs from eavesdropping attacks.

RFID cards do not generate their own transmission signals. Instead, they are powered and activated by the waveform coming from the RFID reader, through inductive coupling in the HF band [7] or RF backscatter communication in the UHF band [11]. In both UHF and HF systems, the reader continuously transmits a high power RF signal \( c(t) \), and a nearby RFID card conveys its message by switching on and off its reflection of the reader’s signal through a mechanism called load modulation. In particular, when the card switches on its load to reflect the reader’s signal, its signal on the air appears as \( x_1 \cdot c(t) \), where \( x_1 \) represents the fraction of the reader’s signal reflected by the card. When the card switches off its reflection via open circuit, its signal on the air appears as \( x_0 \cdot c(t) \), where \( x_0 \) is almost 0 and \( x_0 \ll x_1 \ll 1 \).

In current RFID systems, during the card’s reply, the reader’s baseband signal is a constant waveform \( x \cdot c(t) \), where \( x \) represents the fraction of the reader’s signal reflected by the card. When the card switches off its reflection via open circuit, its signal on the air appears as \( x_0 \cdot c(t) \), where \( x_0 \) is almost 0 and \( x_0 \ll x_1 \ll 1 \).

In current RFID systems, during the card’s reply, the reader’s baseband signal is a constant waveform \( c(t) \), where \( c(t) \) is the card’s data. Instead, it shows a few bits of the card’s reply while communicating with a conventional reader, as perceived by an eavesdropper. The card uses Manchester encoding, where a ‘0’ bit is expressed as a constant value followed by switching repeatedly between two states, whereas a ‘1’ bit is expressed as switching state followed by a constant value. The reader’s random signal \( r(t) \) when multiplied by \( x(t) \) should destroy these internal patterns of the card’s reflection. Hence, \( r(t) \) has to change faster than any transition in the card’s signal. Since the card’s data has a bandwidth slightly less than 2 MHz, \( r(t) \) should span a bandwidth of 2 MHz.

In our design, the RF-Cloak reader generates a sequence of 2 million random complex samples per second drawn from a complex Gaussian distribution with a variance equal to the average transmission power of the reader. Given this random modulation, Fig. 1(b) shows the time signal received by the eavesdropper for the same bits as in Fig. 1(a). Both the ‘0’ bits and the ‘1’ bits are now dispersed by the rapidly changing \( r(t) \) and hence have the appearance of random white noise on the air. The eavesdropper can no longer distinguish them to decode. Additionally, Fig. 1(c) shows the frequency profile of the eavesdropper’s received signal, which exhibits a flat profile characterizing white noise spanning 2 MHz.

We analytically show that even if the eavesdropper uses the optimal decoder (i.e., the maximum likelihood
given a random signal $r(t)$, the eavesdropper's optimal decoder and prove the following results. Specifically, in Appendix A, we derive the fact that a MIMO system with $n$ receivers can separate (and independently decode) $n$ signals transmitted concurrently on the wireless medium [23, 36]. Thus, a 2-receiver MIMO eavesdropper can separate the reader’s random modulation from the card’s signal, and decode the latter. Below we explain this challenge in detail and design a solution that overcomes MIMO eavesdroppers.

5. RF-CLOAK: RANDOMIZED CHANNEL

In this section, we focus on defending against MIMO (multi-input multi-output) eavesdroppers. The challenge in securing RFIDs against MIMO adversaries stems from the fact that a MIMO system with $n$ receivers can separate (and independently decode) $n$ signals transmitted concurrently on the wireless medium [23, 36]. Thus, a 2-receiver MIMO eavesdropper can separate the reader’s random modulation from the card’s signal, and decode the latter. Below we explain this challenge in detail and design a solution that overcomes MIMO eavesdroppers.

5.1 Challenge: The MIMO Game

MIMO transforms the RFID eavesdropping problem into a game between the eavesdropper and the reader:

$$\text{BER} = \frac{1}{2} - \epsilon \quad \text{where} \quad \epsilon < C \sqrt{\frac{\text{Power of RFID's signal}}{\text{Power of Reader's signal}}}$$

Since the power reflected by the RFID is much weaker than the reader’s direct signal power, $\epsilon \approx 0$ and the BER $\approx 1/2$. For typical scenarios, the card’s reflected signal is 20 to 30 dB weaker than the reader’s RF signal [7, 18, 53]. Hence, the eavesdropper’s BER assuming no channel noise is around 40%–47%. Further, our empirical results in §6.1 show that the eavesdropper’s mean BER is 49.8%. This higher BER is because in practice the wireless channel noise exacerbates the BER.

4.2 How Does the RF-Cloak Reader Decode?

The goal of the RF-Cloak reader’s decoder is to retrieve the card’s data $x(t)$ from the received signal $y(t)$. The reader received signal is:

$$y(t) = h_{\text{reader} \rightarrow \text{self}} \cdot r(t) + h_{\text{card} \rightarrow \text{reader}} \cdot x(t) \cdot r(t), \quad (3)$$

where $h_{\text{reader} \rightarrow \text{self}}$ is the channel of the reader’s self-interference, and $h_{\text{card} \rightarrow \text{reader}}$ is the channel of the card’s reflection at the reader.

To decode, the RF-Cloak reader needs to eliminate the effect of the random signal $r(t)$ in Eq. 3 to obtain $x(t)$. The first term in the above equation, $h_{\text{reader} \rightarrow \text{self}} \cdot r(t)$, is the reader’s self-interference over the wire. Canceling self-interference is a standard procedure in RFID readers [15, 57] since the reader has to receive the tag’s signal while transmitting its own signal (without which the RFID tag cannot transmit). The reader cancels its self-interference using a device called circulator [33], which eliminates most of the signal in the analog domain. It then processes the signal in the digital domain to eliminate any residual self-interference. This is done by subtracting $h_{\text{reader} \rightarrow \text{self}} \cdot r(t)$ from the received signal $y(t)$. The reader knows $r(t)$ since it generated the random signal. As for the channel, $h_{\text{reader} \rightarrow \text{self}}$, it is estimated using standard channel estimation methods [30].

Removing the self-interference term from Eq. 3 yields:

$$\tilde{y}(t) = h_{\text{card} \rightarrow \text{reader}} \cdot x(t) \cdot r(t) \quad (4)$$

Next, the reader divides $\tilde{y}(t)$ by $h_{\text{card} \rightarrow \text{reader}} \cdot r(t)$, which produces $x(t)$.\(^3\) The reader can do so because it knows $r(t)$ and can compute the channel $h_{\text{card} \rightarrow \text{reader}}$ using the known preamble in the card message. Once the reader has $x(t)$, it decodes the data bits as in standard RFID decoding.

\(\text{DIVIDING a noisy received signal by } r(t) \text{ can potentially increase the noise variance, due to the random structure of } r(t). \) One way to refine the decoding at low SNRs is to use a matched filter and correlate with $r(t)$ [24].
if the eavesdropper has a larger MIMO system than the reader, it can separate the reader’s random signal from the RFID’s signal and decode the latter. Thus, with random modulation alone, to win this game, the reader needs to keep adding MIMO transmitters to match or exceed the number of receivers on the MIMO eavesdropper. For example, in §4, we demonstrated that a single-transmitter reader transmitting a random signal, \( r(t) \), can defend against a single-receiver eavesdropper. Let us examine what happens if the reader continues to use one transmitter but the eavesdropper upgrades to a 2-receiver MIMO system.

A 2-receiver MIMO eavesdropper receives two signals, \( y_1(t) \) and \( y_2(t) \):

\[
\begin{align*}
y_1(t) &= (h_{\text{reader} \rightarrow \text{eave}} + h_{\text{card} \rightarrow \text{eave}} \cdot x(t)) \cdot r(t) \\
y_2(t) &= (h_{\text{reader} \rightarrow \text{eave}} + h_{\text{card} \rightarrow \text{eave}} \cdot x(t)) \cdot r(t),
\end{align*}
\]

where \( h_{\text{reader} \rightarrow \text{eave}} \) and \( h_{\text{card} \rightarrow \text{eave}} \) are the channels from the reader to the eavesdropper’s first and second receivers respectively, and \( h_{\text{card} \rightarrow \text{eave}} \) and \( h_{\text{card} \rightarrow \text{eave}} \) are the channels of the card’s reflected signal at the eavesdropper’s receivers.

The MIMO eavesdropper can first eliminate the random multiplier \( r(t) \) by dividing the two signals he receives:

\[
\frac{y_1(t)}{y_2(t)} = \frac{h_{\text{reader} \rightarrow \text{eave}} + h_{\text{card} \rightarrow \text{eave}} \cdot x(t)}{h_{\text{reader} \rightarrow \text{eave}} + h_{\text{card} \rightarrow \text{eave}} \cdot x(t)} \cdot \frac{x(t)}{x(t)}.
\]

Next, the eavesdropper tries to decode \( x(t) \) from Eq. 6, which has no random multiplier. Recall that the card’s message \( x(t) \) has only two states: \( x(t) = x_0 \) when the card’s load is off (i.e., open circuit), and \( x(t) = x_1 \) when the card’s load is on (i.e., reflecting the reader’s signal). Distinguishing these two states enables the eavesdropper to track the state transition and decode the card’s transmitted data \( x(t) \). Note that the ratio of the received signals in Eq. 6 takes only two values corresponding to the \( x(t) = x_0 \) state and the \( x(t) = x_1 \) state. We denote these two values of the ratio \( y_1/y_2 \) as \( \alpha_0 \) and \( \alpha_1 \). Thus, after computing the ratio \( y_1/y_2 \), the only ambiguity the eavesdropper has is in mapping the two observed values \( \alpha_0 \) and \( \alpha_1 \) to states \( x_0 \) and \( x_1 \). To resolve this ambiguity, the attacker checks which of the two mappings allows the decoded message to satisfy the checksum [19]. Thus, a 2-receiver MIMO eavesdropper can win the MIMO game over a single-transmitter reader, even if the latter uses random modulation.\(^4\)

We can gain a deeper insight into this MIMO game by looking at the received signal in a 2-dimensional space created by the two receivers on the eavesdropper, where one dimension is \( y_1(t) \), the signal received on his first receiver and the other dimension is \( y_2(t) \), the signal received on his second receiver. At any point in time \( t \), the received signals \( (y_1(t), y_2(t)) \) can be represented as one point in this 2-dimensional space. When \( x(t) = x_0 \), we know from above that \( y_1 = \alpha_0 y_2 \), which defines a line in this 2-dimensional space. Similarly, when \( x(t) = x_1 \), the received signals lie on a different line defined by \( y_1 = \alpha_1 y_2 \).

We confirm this point empirically by letting a 2-receiver MIMO adversary (implemented using USRP software radios) eavesdrop on a conversation between a commercial UHF RFID and a USRP-based reader that employs random modulation. Fig. 2 shows a scatter plot of what the eavesdropper receives on its two antennas. Here, we plot the magnitude of the received samples, i.e., each point in the figure represents \((|y_1(t)|, |y_2(t)|)\) for a specific \( t \). We then use our ground truth knowledge of the actual bits transmitted by the RFID card to label samples corresponding to \( x_0 \) in blue and \( x_1 \) in red. Despite the fact that the received signal at each receiver is random, together \( y_1(t) \) and \( y_2(t) \) span only lines instead of the entire 2-dimensional space at the eavesdropper. Since the card’s data has only two states, we see two lines in the figure and hence the eavesdropper can decode by checking which line the received samples belong to.

The above can be generalized to larger-scale MIMO systems on the reader and eavesdropper. If the eavesdropper has \( n \) receive chains, he receives signals in an \( n \)-dimensional space. If the reader has \( k \) transmit chains \(( k < n )\) and transmits \( k \) signals from them, these signals will only span a \( k \)-dimensional subspace (lines, planes, etc.) in the eavesdropper’s \( n \)-dimensional space. Since the card has only two states \( x_0, x_1 \), the eavesdropper will observe two unique subspaces and hence he can decode. Thus, it comes down to a MIMO game between the reader and the eavesdropper. No matter how many transmit chains the reader uses, the eavesdropper can win the game by using more receive chains.

\(^4\)Note that the eavesdropper is able to decode without having to estimate any of the wireless channels in Eq. 5.

---

**Figure 2**—2-Dimensional space of a 2-receiver MIMO eavesdropper in RF-Cloak’s random modulation scheme: The figure shows a scatter plot of the samples received by a 2-receiver eavesdropper. Despite random modulation, a 2-receiver eavesdropper facing a single-transmitter reader sees two lines corresponding to two states of the RFID card, \( x_0 \) and \( x_1 \) which allows it to decode.
5.2 Change the Game: Channel Randomization

To overcome the MIMO game, let us go back to Fig. 2 and try to understand why we have separate slopes for the two states of the RFID signal. Recall that the slopes of the two lines in Fig. 2, $\alpha_0$ and $\alpha_1$, depend only on the channels from the reader to the eavesdropper receivers, as clear from Eq. 6. If the channels stay constant, the two lines $y_2 = \alpha_0 y_1$ and $y_2 = \alpha_1 y_1$ in Fig. 2 do not change over time. However, if the channels from the reader to the eavesdropper’s MIMO antennas are random, then the ratio $y_1/y_2$ will be random and the slope will be random for every transition in the state of the RFID’s signal. This prevents the eavesdropper from separating the points corresponding to the $x_0$ state of the RFID from the points corresponding to the $x_1$ state of the RFID. Thus, we can overcome a MIMO eavesdropper by randomizing the wireless channels to the eavesdropper.

We analytically show that if the channels from the reader to the eavesdropper are random, a MIMO eavesdropper that uses the optimal decoder (maximum likelihood decoder) will see a bit error rate close to 50%, which is no better than a random guess. Specifically, in Appendix B we prove the following lemma:

**Lemma 5.1.** There exists a constant $C < 1$ such that, given the wireless channels from the reader to the eavesdropper’s antennas are random complex Gaussians with zero mean and the channels change as fast as the bandwidth of $x(t)$, a MIMO eavesdropper with $n$ receivers using the optimal decoder achieves a bit error rate (BER):

$$\text{BER} = \frac{1}{2} - \epsilon \quad \text{where} \quad \epsilon < C \sqrt{n} \cdot \frac{\text{Power of RFID's signal}}{\text{Power of Reader's signal}}$$

Recall that the power reflected by the RFID is much weaker than the reader’s direct signal power. For a typical power ratio of $-30$ dB to $-20$ dB [56], assuming no channel noise, even a 20 antenna MIMO eavesdropper will have BER around 48% to 49.8%.

To build a system that randomizes the channels, RF-Cloak uses a combination of antenna motion and random rapid antenna switching. Specifically, past work shows that due to multipath effects, even small motion of the antenna can create large variations in the wireless channels [2, 41, 50, 54]. Hence, by leveraging antenna motion, we are able to span a large range of random channel instantiations. We further increase the randomization by combining antenna motion with rapid and random switching of antennas. Specifically, we use a rotating frame that holds multiple antennas, and we randomly switch between the antennas using rapid switches [20] that can switch every few microseconds. Random switching breaks the periodicity of rotation as well as any correlation in the channel instantiations over time. Note that while our reader uses switched antennas,
The entire space. No subspace is unique to the card’s dropper from decoding.

The eavesdropper’s received samples (\(|Y_1|, |Y_2|\)) almost span the entire space. No subspace is unique to the card’s \(x_0\) state (red) as opposed to the \(x_1\) state (blue), which prevents the eavesdropper from decoding.

5.3 How Does the RF-Cloak Reader Decode?

The RF-Cloak reader needs to be able to retrieve the card’s data despite the channel randomization. The reader receives the signal:

\[ y(t) = h_{\text{reader} \rightarrow \text{self}} \cdot r(t) + h_{\text{card} \rightarrow \text{reader}}(t) \cdot x(t) \cdot r(t), \tag{7} \]

where \(h_{\text{reader} \rightarrow \text{self}}\) is the reader’s self-interference channel and \(h_{\text{card} \rightarrow \text{reader}}(t)\) is the channel of the card’s reflected signal at the reader. The reader can cancel its self interference \(h_{\text{reader} \rightarrow \text{self}}\cdot r(t)\) as described in §4.2. Note that \(h_{\text{reader} \rightarrow \text{self}}\) is not random since it is the channel from the antenna to itself over the wire and hence it is not affected by motion. Once the reader eliminates its self interference and the random modulation \(r(t)\), what remains is:

\[ \tilde{y}(t) = h_{\text{card} \rightarrow \text{reader}}(t) \cdot x(t) \tag{8} \]

Since \(h_{\text{card} \rightarrow \text{reader}}(t)\) is random and cannot be estimated, the reader needs to decode based on the power. Recall that, when the card switches off its reflection via an open circuit, its state \(x_0 \approx 0\). And hence, by detecting the power when the card’s signal is in the \(x_1\) state, the reader can distinguish the two states and decode. In Appendix C, we derive the optimal decoder and BER and in §6.2 we empirically show that RF-Cloak can decode the RFID’s data.

6. Implementation & Evaluation

We built a prototype of RF-Cloak using USRP software radios [32] and used it to secure the communication of off-the-shelf RFID cards. We adopt a UHF reader code base developed in [11] and extend it to also work with HF RFIDs.

To randomize the modulation, we customize the reader software to transmit a random signal generated as described in §4 instead of a constant waveform, during the card’s reply. For channel randomization, we connect the reader’s single transmit chain to 8 antennas using a programmable switch and randomly switch between them at the same rate as the card switches between its on and off states. The switch is built using three off-the-shelf multiplexers [20] controlled by a programmable micro-controller [6]. Furthermore, the transmit antennas are mounted on a circular frame which is rotated by a 1725 RPM fan motor.

A. UHF Devices

Reader: The UHF RF-Cloak reader is built using USRP N210 with RFX900 daughterboards and VERT900 omnidirectional antennas.

RFID Card: We use the Alien Squiggle General Purpose RFID Tags [4] as an example of UHF passive RFIDs.

Eavesdropper: The eavesdropper is implemented using the same hardware (USRP and antenna) as the RF-Cloak reader. The only difference is that, in the MIMO experiments, the eavesdropper uses multiple (up to 5) USRPs and receive antennas distributed across space.

B. HF Devices

Reader: The HF RF-Cloak reader is implemented using USRP1 software radio with LFTX and LFRX daughterboards operating in the 0-30 MHz frequency range and the DLP-RFID-ANT antennas [17].

RFID Card: We use the MBTA Charlie card [46] as an example of the widely used MIFARE Classic cards.

Eavesdropper: The eavesdropper is implemented using the same hardware (USRP and antenna) as the RF-Cloak reader.

C. Security Metric

We use the bit error rate (BER) experienced by the eavesdropper as a metric for the system’s security. Ideally, a fully secure system should maintain a 50% BER at the eavesdropper, which is equivalent to the result of a random guess. For both HF and UHF RFIDs, we run experiments at a variety of reader, card, and eavesdropper locations and average across 1000 runs to compute the mean BER for each placement.
6.1 Evaluation of Randomized Modulation

First, we investigate whether RF-Cloak’s random modulation can protect HF and UHF RFIDs from a single-receiver eavesdropper.

**Experiment:** The RF-Cloak reader queries the Charlie card or the commercial UHF tag for 1000 times in each run. To match the operating range in current RFID systems, the distance between the RF-Cloak reader and the RFID card is varied between 2–10 cm in the HF case, and 1–5 meters in the UHF case. During the RFID’s reply, the reader continuously transmits a random signal generated using the design in §4. In the case of the Charlie card (HF), the eavesdropper is placed 5–10 cm away from the card; in the UHF case, it is placed 0.2–5 meters away from the UHF RFID tag. The eavesdropper has a single receive chain and a single antenna. It tries to decode the tag’s message using the maximum-likelihood decoder described in Appendix A.

**Result 1 (BER at the Eavesdropper):** Fig. 6(a) plots the CDF of the eavesdropper’s bit error rates when the Charlie card is communicating with an RF-Cloak reader. The CDF is taken over all locations of the reader, Charlie card, and eavesdropper. For comparison, the red dashed curve is the CDF of the eavesdropper’s BER when it randomly guesses the bits without trying to make use of the eavesdropped information. The figure shows that, when the RF-Cloak reader randomizes the modulation, the eavesdropper’s BER is 49.8% on average, with a standard deviation of less than 0.8%, closely matching the result of a random guess.

**Figure 6—Effectiveness of random modulation against single-antenna eavesdroppers:** CDF of the eavesdropper’s BER. (a) For HF cards, the eavesdropper’s BER closely matches a random guess. (b) For UHF cards, the eavesdropper’s average BER is 50.3% with a standard deviation of 2.3%.

**Result 2 (Decoding Performance of RF-Cloak Reader):** Next, we verify that replacing the constant waveform with RF-Cloak’s randomized modulation does not affect the decoding at the reader. We use the signals from the same experiment above but now focus on the reader’s decoding BER.

Fig. 7(a) and Fig. 7(b) show the CDFs of the bit error rates at the RF-Cloak reader for the HF and UHF experiments respectively. For reference, the figure also shows the bit error rates of existing RFID readers that use a constant waveform instead of the random modulation, for the same placements of reader and card. The HF RF-Cloak reader has an average decoding BER of less than 0.01% and a maximum BER of 0.03%, whereas the UHF RF-Cloak reader has an average bit error rate of less than 0.01% and a maximum of 0.06%. These bit error rates are typical for RFID systems and on par with current RFID reader’s performance.

6.2 Evaluating RF-Cloak with MIMO Eavesdroppers

Next, we study RF-Cloak’s capability of protecting...
RFIDs from a MIMO eavesdropper employing multiple receive chains and antennas. Note that MIMO does not benefit eavesdroppers in HF RFID systems for the following reason. The ability of a MIMO eavesdropper to separate the reader’s random signal from the RFID’s signal hinges on the channels he perceives from the reader and the RFID being sufficiently different. However, in HF (13.56 MHz) RFID systems, the operating distance between the card and the reader is within 10 cm, significantly smaller than the wavelength (22 meters). In this case, it is well-known that MIMO techniques cannot separate their signals [65]. Hence, here, we focus on UHF RFIDs in our evaluation with MIMO eavesdroppers.

**Experiment (MIMO & Channel Randomization):** We repeat the same experiment performed in the previous section, after replacing the single-antenna eavesdropper by a MIMO eavesdropper and introducing channel randomization at the RF-Cloak reader, using one transmit chain with random antenna switching and rotation as described in §6. We vary the number of receive chains and antennas employed by the MIMO eavesdropper between 3, 4, and 5. The eavesdropper decodes as described in Appendix B.

**Result 1 (MIMO Eavesdropper v.s. Channel Randomization):** Fig. 8 plots CDFs of the BER experienced by 3-, 4-, and 5-antenna MIMO eavesdroppers when the RF-Cloak reader uses channel randomization. For reference, the BER result of a random guess is also plotted. The figure shows that the eavesdropper experiences a BER close to 50%, with a standard deviation ranging between 1.2% and 2.9%, depending on the number of receivers at the eavesdropper. Hence, the eavesdropper’s decoding in face of RF-Cloak’s channel randomization scheme is equivalent to a random guess. This is because the samples corresponding to $x_0$ and $x_1$ states are now indistinguishable in the multi-dimensional space.

**Result 2 (Decoding Performance of the RF-Cloak Reader with Channel Randomization):** Finally, we verify that the antenna switching/motion and the resulting channel randomization do not prevent the trusted RF-Cloak reader from decoding. Fig. 9 shows the BER from the same experiment as above but as perceived by an RF-Cloak reader that decodes the signal using our design in §5.2. As we can see, the RF-Cloak reader has an average decoding bit error rate of 0.2%. Note that the RFID packet length is typically short, since most of the communication involves transmitting 16-bit temporary IDs plus 5-bit checksum. In this case, a 0.2% bit error rate translates into a packet loss rate of around 4%, which is quite common and acceptable in RFID systems. If certain applications require an even lower BER, the reader can request the tags to transmit their data using longer codes, an option readily available in today’s commercial RFIDs [19].

In conclusion, RF-Cloak’s channel randomization via rapid antenna switching and motion provides an effective mechanism to protect RFIDs from MIMO eavesdropping, without requiring MIMO capability at the reader.

### 7. Related Work

Past work on defending RFIDs against eavesdropping has mainly focused on improving the cryptographic protocols [1, 9, 13]. These schemes, however, are difficult to build in practice due to the severe energy, size and cost constraints on RFID cards. Thus, commercial RFIDs continue to use weak encryption schemes proven to be vulnerable [38, 51, 63].

RF-Cloak belongs to the class of physical layer security mechanisms that aim to defend against eavesdroppers without modifying the RFIDs. The closest to our work is the Noisy Reader proposal [60], in which the reader varies its own signal in an attempt to hide an HF RFID’s data. It generates one random number per card bit and uses it as the magnitude of the reader’s signal. It also tries to imitate the card’s internal bit pattern by making the reader periodically switch its signal phase by 180° at the same frequency the card switches between two states. The Noisy Reader scheme was studied analytically, yet we are unaware of any prior implementation or empirical evaluation. We implemented the Noisy Reader using the same USRP setup as RF-Cloak. Fig. 10
and cannot be applied directly to RFIDs. Standard jamming deals with wireless devices that transmit their own. Hence, the random signal multiples with the protected data. Because of this multiplicative model, directly applying jamming to RFIDs yields insecure systems like in the case of the Noisy Reader [60] described above in details.

Our work is also related to Near Field Communication (NFC) security on mobile phones [27, 48, 70]. These systems, however, operate in very close proximity and are not applicable to UHF RFIDs that operate at a distance of few meters away from the reader. RF-Cloak provides a solution that is applicable to both UHF RFIDs as well as near field HF RFIDs.

Finally, antenna motion has been recently exploited in wireless communication for interference management [2] as well as RF localization [39, 40, 47, 61, 68, 69] and WiFi Imaging [26]. Differing from these, RF-Cloak leverages antenna motion to randomize the wireless channels and enable a security construct for defending against MIMO eavesdropping.

8. CONCLUSION

Recent eavesdropping attacks have compromised the security of billions of deployed RFIDs worldwide. This paper asks whether one can secure these simple RFIDs from eavesdropping attacks, without modifying the cards. By only implementing changes on the RFID reader, RF-Cloak introduces random modulation and random channels to overcome powerful MIMO eavesdroppers. We demonstrated that randomizing the modulation via reflection, and randomizing the wireless channels by using antenna motion and rapid switching can effectively protect today’s widely used commercial RFIDs from eavesdroppers. Further, we believe the channel randomization technique can be combined with many existing security primitives, which opens doors to a variety of new designs in wireless security beyond the scope of RFID communication.

Acknowledgments:
The authors would like to thank the shepherd Deepak Ganesan as well as Lixin Shi, Fadel Adib, Deepak Vassishit, Badih Ghazi, Swarun Kumar, and Hariharan Rahul for their insightful feedback and comments.

APPENDIX

A. PROOF OF LEMMA 4.1

The eavesdropper receives the signal $y(t)$ in Eq. 2. Since $h_{\text{reader} \rightarrow \text{eve}}$ is constant, we can normalize $y(t)$ by it to get:5

$$y'(t) = r(t) \cdot \left[ 1 + \frac{h_{\text{card} \rightarrow \text{eve}}}{h_{\text{reader} \rightarrow \text{eve}}} \cdot x(t) \right]$$

Figure 10—Noisy Reader trace: The eavesdropper’s received signal of the Charlie card communicating with the Noisy Reader still exhibits two clear patterns corresponding to the ‘0’ bits and ‘1’ bits. Despite the random magnitude in each bit and the phase shifting, the eavesdropper can still decode by comparing the first half and the second half of each bit. The ‘0’ bits have the same shape, while the ‘1’ bits have a different one.

shows the received signal at a single-antenna eavesdropper, when the Noisy Reader is protecting the Charlie card. Although each bit is scaled differently, we can still see that all the ‘0’ bits have the same shape, while the ‘1’ bits have a different shape. This is due to the multiplicative nature of the card’s signal and the Manchester encoding shown in Fig. 1(a) which is used by more than 80% of the HF cards today (ISO 14443 Type A [51]). Our experiments show that a single-antenna eavesdropper is able to fully decode the Charlie card’s data in 99.7% of the traces despite the Noisy Reader.

Another prior work in this category, BUPLE [14], tries to hide the RFID’s message using frequency hopping at the reader. However, given the frequency band that commercial backscatter RFIDs operate in (i.e., 902 MHz – 928 MHz), any typical receiver (e.g., USRP) with a bandwidth larger than 26 MHz can easily identify the center frequency at any point in time and decode the RFID’s signal. Other physical layer solutions to eavesdropping attacks, such as the Noisy Tag [12], require modifying the cards to use wireless signals to exchange a key with the reader.

Past theoretical work from the information theory community has also explored the use of antenna switching for secure physical layer communication [3, 16, 31, 42, 66]. These papers use large switched antenna arrays to maintain a decodable signal towards the direction of the intended receiver (i.e., a constant main beam of the antenna array), but scramble the signal at undesired directions (i.e., sidelobes of the array pattern) to prevent the eavesdropper from decoding. Such techniques do not work in the context of passive RFID communication, where the RFID reflects the reader’s signal to all directions regardless of the reader signal’s directionality.

RF-Cloak also builds on jamming-based systems [25, 60, 62]. However, these solutions use standard jamming and cannot be applied directly to RFIDs. Standard jamming deals with wireless devices that transmit their own signal, in which case the random jamming signal adds up to the protected data. RFIDs, on the other hand, reflect the reader’s signal without transmitting a signal of their own. Hence, the random signal multiples with the protected data. Because of this multiplicative model, directly applying jamming to RFIDs yields insecure systems like in the case of the Noisy Reader [60] described above in details.

5 In this derivation, we ignore wireless channel noise, since it will only increases the BER of the eavesdropper.
The RFID card’s signal $x(t)$ has two states: $x_0$ when the card has an open circuit and $x_1$ when the card turns on its load to reflect the reader’s signal. To convey a ‘0’ or ‘1’ bit, the card transmits different patterns of $x_0$’s and $x_1$’s of length $k$. Thus, for each card bit $b$, the eavesdropper receives $k$ samples in $y'(t)$ denoted by $\{Y_1, Y_2, \ldots, Y_k\}$:

$$Y_i = \begin{cases} R_i \cdot (1 + p_i^0) & \text{if } b = 0 \\ R_i \cdot (1 + p_i^1) & \text{if } b = 1 \end{cases}$$

where $\{p_1^0, \ldots, p_k^0\}$ is the pattern when the card transmits a ‘0’ bit and $\{p_1^1, \ldots, p_k^1\}$ is the pattern when the card transmits a ‘1’ bit. $R_i$ is a sample in the reader’s random signal $r(t)$ which is drawn from a complex normal distribution with zero mean and standard deviation $\sigma$. Note that, since the bandwidth of $r(t)$ is the same as $x(t)$, there is a single $R_i$ for each state of the RFID’s signal. We will assume the eavesdropper knows the bit boundaries i.e. he knows which $Y_i$ samples correspond to the same bit.

The eavesdropper’s optimal decoder is a maximum likelihood decoder as derived in [8, 35]. The optimal decoder is the one that achieves the minimum bit error rate. Hence, an eavesdropper using any other strategy cannot extract more information than an eavesdropper using the optimal decoder. Given the $k$ received samples $\{Y_1, Y_2, \ldots, Y_k\}$ at the eavesdropper, the decoder is defined by the following hypothesis test:

$$Pr(b = 1|\{Y_1, \ldots, Y_k\}) \geq Pr(b = 0|\{Y_1, \ldots, Y_k\})$$

Because the card’s bits have equal probability of being ‘0’ or ‘1’ [19, 51], we can rewrite the hypothesis test as:

$$Pr(\{Y_1, \ldots, Y_k\}|b = 1) \geq Pr(\{Y_1, \ldots, Y_k\}|b = 0)$$

Given $b = 0$ or $b = 1$, the $k$ samples in $\{Y_1, \ldots, Y_k\}$ become independent Gaussians with zero mean and standard deviation $\sigma_b^0 = \sigma(1+p_i^0)$ or $\sigma_b^1 = \sigma(1+p_i^1)$. Hence, we can write:

$$Pr(Y|b) = \frac{1}{(2\pi)^{k/2}} \prod_{i=1}^k \sigma_i^{-2} \exp \left( -\sum_{i=1}^k \frac{|Y_i|^2}{\sigma_i^2} \right)$$

A similar equation can be derived for $b = 1$. Since the two patterns have the same number of $x_0$ samples, we have $\prod_{i=1}^k \sigma_i^0 = \prod_{i=1}^k \sigma_i^1$. The maximum-likelihood decoder can then be simplified to:

$$\sum_{i=1}^k \left( \frac{|Y_i|^2}{\sigma_i^0} \right)^2 \geq \sum_{i=1}^k \left( \frac{|Y_i|^2}{\sigma_i^1} \right)^2$$

Given the patterns $p^0$ and $p^1$ for UHF RFIDs [60], we can further simplify the UHF decoder to:

$$\begin{align*}
\frac{6}{p^0} &= \frac{\text{power of card signal} - x_0}{\text{power of card signal}} \quad \text{or} \\
\frac{6}{p^1} &= \frac{\text{power of card signal} - x_1}{\text{power of card signal}}
\end{align*}$$

Depending on the pattern used by the RFID card. For HF cards the patterns are $p^0 = \{0101010\}00000000$ and $p^1 = \{000000010101010\}$. For UHF cards with Miller 8 encoding the patterns are $p^0 = \{01010101010\}$ and $p^1 = \{01010101011\}$.

Similarly, given the patterns for HF RFIDs [60], we can simplify the HF decoder to:

$$\begin{align*}
|Y_1|^2 + |Y_2|^2 + |Y_3|^2 + |Y_4|^2 \\
\leq \frac{1}{6} \left( |Y_1|^2 + |Y_2|^2 + |Y_3|^2 + |Y_4|^2 \right)
\end{align*}$$

Given the above optimal decoders, we derive the bit error rate (BER) at the eavesdropper for the case of UHF RFID cards. The derivation is the same for the HF RFID cards.

Define the random variables $U$, $V$, and $Z$ such that $U = |Y_1|^2 + |Y_2|^2 + |Y_3|^2 + |Y_4|^2$, $V = |Y_5|^2 + |Y_6|^2 + |Y_7|^2 + |Y_8|^2$, and $Z = U - V$. Then, the bit error rate at the eavesdropper is defined as:

$$\text{BER} = \frac{1}{2} Pr(Z < 0|b = 0) + \frac{1}{2} Pr(Z > 0|b = 1)$$

Given $b = 0$, $\{Y_2, Y_4, Y_6, Y_8\}$ are independent complex gaussian random variables with zero mean and standard deviation $\sigma_U = \sigma(1 + x_1)$ while $\{Y_9, Y_{11}, Y_{13}, Y_{15}\}$ are the same but with standard deviation $\sigma_V = \sigma(1 + x_0)$. Thus, $U$ and $V$ have a Gamma distribution with degree 4 and rate of $2\sigma_U^2$ and $2\sigma_V^2$ [5]. We can now derive the distribution of $Z$ for $z \leq 0$ as:

$$Pr(Z|b) = \frac{\Gamma(\frac{z}{\beta})\beta^{\frac{z}{\beta}}}{\Gamma(3)} e^{-\frac{z^2}{6\beta}}$$

where $\beta = \frac{2\sigma_U^2 + 2\sigma_V^2}{\beta_1}$. In a similar manner, we can derive the distribution of $Z$ given $b = 1$ for $z \geq 0$. We can now integrate to calculate the probabilities in Eq. 11 and the BER as:

$$\text{BER} = 1 - \frac{\mu^4}{(1+\mu)^4} \left( \frac{20}{(1+\mu)^2} + \frac{10}{(1+\mu)^4} + \frac{4}{(1+\mu)} + 1 \right)$$

where $\mu = \frac{(1+x_1)^2}{(1+x_0)^2}$. Since $x_0 \approx 0$ and $x_1 \ll 1$, we get that $1/(1+\mu) \approx 1/(2(1+x_1))$. Using this, we can rewrite the above BER equation as:

$$\text{BER} = \frac{1}{2} - \epsilon \quad \text{where} \quad \epsilon < \frac{29}{32} x_1$$

Recall that, $x_1$ is the fraction of the reader’s signal reflected by the RFID. Hence, $x_1 = \sqrt{\frac{\text{Power of RFID’s signal}}{\text{Power of Reader’s signal}}}$

**B. Proof of Lemma 5.1**

An eavesdropper with $n$ antennas receives $n$ signals $y_1(t), \ldots, y_n(t)$ on each of its $n$ antennas:

$$\begin{align*}
y_1(t) &= \begin{pmatrix} h_{r_1}(t) \\ \vdots \end{pmatrix} + x(t) \cdot \begin{pmatrix} h_{c_1}(t) \\ \vdots \end{pmatrix} + r(t) \\
y_n(t) &= \begin{pmatrix} h_{r_n}(t) \\ \vdots \end{pmatrix} + x(t) \cdot \begin{pmatrix} h_{c_n}(t) \\ \vdots \end{pmatrix} + r(t)
\end{align*}$$

where $h_{r_i}(t)$ and $h_{c_i}(t)$ are the channel coefficients for the reader and card, respectively.
where \( h_r(t) \) is the random channel from RF-Cloak’s antenna to the eavesdropper’s i-th antenna, \( h_c(t) \) is the random channel from RFID card to the Eavesdropper’s j-th antenna, \( r(t) \) is the random modulation signal, and \( x(t) \) is the RFID card’s reply which takes two states \( x_0 \) and \( x_1 \). To simplify the analysis, we will ignore the random modulation \( r(t) \) in favor of the eavesdropper.

As described earlier, for each bit \( b \), the RFID transmits a pattern \( \{ p^b_i, \ldots, p^b_k \} \) where \( p^b_i = x_0 \) or \( x_1 \). Thus, the eavesdropper receives \( k \) samples per bit on each of its \( n \) antennas:

\[
\begin{bmatrix}
Y_{11} & \cdots & Y_{1k} \\
\vdots & \ddots & \vdots \\
Y_{n1} & \cdots & Y_{nk}
\end{bmatrix} = \begin{bmatrix}
H_{t1} & \cdots & H_{tk} \\
\vdots & \ddots & \vdots \\
H_{tn} & \cdots & H_{tk}
\end{bmatrix}
\begin{bmatrix}
p^b_1 \\
\vdots \\
p^b_k
\end{bmatrix}
\]

The random channels \( H_t \) and \( H_c \) are independent and follow a complex normal distribution with zero mean and standard deviation \( \sigma \). Similar to the random modulation, the optimal decoder is a maximum likelihood decoder based on the following hypothesis test:

\[
Pr(b = 1|\{Y_{11}, \ldots, Y_{nk}\}) \overset{1}{\approx} \frac{1}{\sqrt{2\pi}} Pr(b = 0|\{Y_{11}, \ldots, Y_{nk}\})
\]

Since the tags bits have equal probability of being ‘0’ or ‘1’, we can rewrite the above hypothesis test as:

\[
Pr(\{Y_{11}, \ldots, Y_{nk}\}|b = 1) \overset{1}{\approx} \frac{1}{\sqrt{2\pi}} Pr(\{Y_{11}, \ldots, Y_{nk}\}|b = 0)
\]

Given \( b = 0 \) or \( b = 1 \), the \( Y_i \) samples become independent complex Gaussians with zero mean and standard deviation \( \sigma^b_i = \sigma \sqrt{1 + |p^b_i|^2} \). Their joint probability is:

\[
Pr(Y|b) = \frac{1}{(2\pi)^{nk/2}} |\sigma^b_i|^{2n} \exp \left( -\sum_{i,j} \frac{|Y^b_i|^2}{\sigma^b_i} \right)
\]

The hypothesis test can now be simplified to:

\[
\sum_{i,j} \frac{|Y^b_i|^2}{\sigma^b_i} 2^{2n} \overset{1}{\approx} \sum_{i,j} \frac{|Y^b_i|^2}{\sigma^b_i} 2^{2n}
\]

Substituting the patterns for UHF RFID cards, we get:

\[
\sum_{j \in \{10,12,14,16\}} \sum_{i} |Y^b_i|^2 \overset{1}{\approx} \sum_{j \in \{9,11,13,15\}} \sum_{i} |Y^b_i|^2
\]

Given the above optimal decoder, we can derive the BER of the eavesdropper. Define \( Z \) as the difference between the left and right hand sides of the above hypothesis test. Then, \( Z \) is the difference between two random variables of a Gamma distribution with degree \( 4n \) and rates \( 2\sigma^2(1 + x_1^2) \) and \( 2\sigma^2(1 + x_0^2) \). Similar to Appendix A, we derive the distribution of \( Z \) use it to calculate the BER as:

\[
BER = \frac{1}{2} Pr(Z < 0|b = 0) + \frac{1}{2} Pr(Z > 0|b = 1)
\]

\[
= 1 - \mu^{4n} \sum_{i=0}^{4n-1} \left( 1 + \frac{4n-1}{4n-1} \right) \frac{1}{(1 + \mu)^i}
\]

where \( \mu = (1 + x_1^2)/(1 + x_0^2) \). Since \( x_0 \approx 0 \) and \( x_1 \ll 1, 1/(1 + \mu)^2 \approx 1/(4(1 + x_1^2)) \). Using the fact that \( \sum_{i=0}^{4n} (e^{\mu^2}) \frac{1}{2} = 2^\epsilon \) and Stirling’s bounds, we can simplify the BER to:

\[
BER = \frac{1}{2} - \epsilon \quad \text{where} \quad \epsilon < \frac{e}{2\pi} x_1^2 \sqrt{n}
\]

Recall that, \( x_1 \) is the fraction of the reader’s signal reflected by the RFID. Hence, \( x_1^2 \approx \text{Power of Reader’s signal} \).

C. RF-CLOAK’S OPTIMAL DECODER AND BER

After canceling the self interference and removing the random modulation, RF-Cloak’s received signal is:

\[
\tilde{y}(t) = h_r(t) \cdot x(t)
\]

where \( h_r(t) \) is the random channel from card to RF-Cloak’s receiver. For each bit \( b \), RF-Cloak receives \( k \) samples \( \{Y_1, \ldots, Y_k\} \) where \( Y_i = H_c p^b_i \). The random channels \( H_c \) are independent and follow a complex normal distribution with zero mean and standard deviation \( \sigma \). Hence, \( Y_i \) has a normal distribution with zero mean and standard deviation \( \sigma^b = |p^b_i| \). As before the decoder will be the maximum likelihood decoder and the hypothesis test can be written as:

\[
\sum_{i,j} \frac{|Y^b_i|^2}{\sigma^b_j} \overset{1}{\approx} \sum_{i,j} \frac{|Y^b_i|^2}{\sigma^b_j}
\]

which for for UHF cards is:

\[
|Y_{i0}|^2 + |Y_{i1}|^2 + |Y_{i2}|^2 + |Y_{i3}|^2 \overset{1}{\approx} \frac{1}{\sigma_0} |Y_{i0}|^2 + |Y_{i1}|^2 + |Y_{i2}|^2 + |Y_{i3}|^2
\]

And similar to before the BER will be:

\[
BER = 1 - \mu^{4n} \left( \frac{20}{(1 + \mu)^2} + \frac{10}{(1 + \mu)^2} + \frac{4}{1 + \mu} + 1 \right)
\]

where \( \mu = x_1^2 / x_0^2 \). Although, this BER equation is similar to that of the adversary, it only depends on the ratio of \( x_1 \) to \( x_0 \). Since, when the card does not reflect the reader’s signal its state \( x_0 \approx 0 \), the BER\( \approx 0 \). In fact, even when \( x_0 \approx 1/4 \), the BER is less than 0.04% which is typical for RFID communication.

9. REFERENCES


[17] DLP Design, Inc. DLP-RFID-ANT.


[19] EPCglobal Inc. EPCglobal Class 1 Generation 2 V.1.2.0. [http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2](http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2).


MBTA. Reusable, rechargeable charliecards.


J. Wang and D. Katabi. Dude, Where’s My Card?:

