RCID: Fingerprinting Passive RFID Tags via Wideband Backscatter

Jiawei Li[*], Ang Li[*], Dianqi Han[*], Yan Zhang[*], Tao Li[†], Yanchao Zhang[*]
[*] Arizona State University, [†] Indiana University–Purdue University Indianapolis
{jwli, anglee, dqhan, yanzhangyz, yczhang}@asu.edu, tli6@iupui.edu

IEEE INFOCOM 2022 - IEEE Conference on Computer Communications | 978-1-6654-5822-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/INFOCOM48880.2022.9796663

***Abstract*—Tag cloning and spoofing pose great challenges to RFID applications. This paper presents the design and evaluation of RCID, a novel system to fingerprint RFID tags based on the unique reflection coefficient of each tag circuit. Based on a novel OFDM-based fingerprint collector, our system can quickly acquire and verify each tag's RCID fingerprint which are independent of the RFID reader and measurement environment. Our system applies to COTS RFID tags and readers after a firmware update at the reader. Extensive prototyped experiments on 600 tags confirm that RCID is highly secure with the authentication accuracy up to 97.15% and the median authentication error rate equal to 1.49%. RCID is also highly usable because it only takes about 8 s to enroll a tag and 2 ms to verify an RCID fingerprint with a fully connected multi-class neural network. Finally, empirical studies demonstrate that the entropy of an RCID fingerprint is about 202 bits over a bandwidth of 20 MHz in contrast to the best prior result of 17 bits, thus offering strong theoretical resilience to RFID cloning and spoofing.**

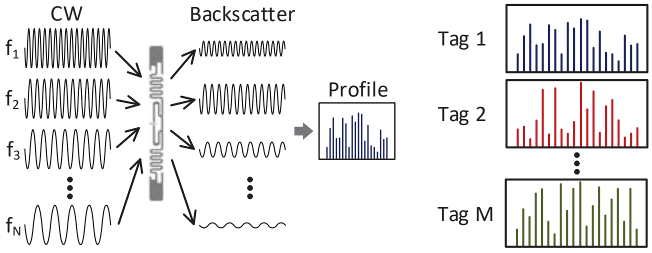
***Index Terms*—RFID, Fingerprinting, Authentication, Wireless Security**

I. Introduction

Passive ultra-high frequency (UHF) RFID tags are dominating the RFID market, and most commodity UHF RFID tags do not support cryptographic operations. To the best of our knowledge, NXP's UCODE DNA RAIN RFID [1] is the only product that supports cryptographic authentication checks. These crytographic tags cost about 70¢ in contrast to the typical price of 5¢ to 15¢ for crypto-less tags. Therefore, most existing and new UHF RFID systems still rely on crypto-less tags which are the focus of this paper. For brevity only, we omit the term "crypto-less passive UHF" hereafter whenever no confusion may arise.

Tag cloning poses possibly the greatest challenge to RFID systems. In particular, since there is no mutual authentication between the RFID reader and tags, a capable attacker can directly interrogate an RFID tag or sniff the unencrypted reader-tag communications. The attacker can then exploit the acquired information such as the EPC to clone and then impersonate legitimate RFID tags. Although many crypto-based countermeasures such as [2]–[4] have been proposed, they do not apply to commodity crypto-less UHF RFID tags.

RFID fingerprinting [5]–[13] is widely believed to be an effective anti-cloning technique. An RFID fingerprint refers to some unique hardware-based tag features caused by manufacturing imperfection and is hard to duplicate. Existing RFID fingerprinting schemes often have a small feature space subject to brute-force attacks. For example, the entropy of the RFID fingerprint proposed in the state of the art [12] is estimated to be about 17 bits (Section VI-F), which may be insufficient against dedicated attackers.



(a) frequency dependence (b) tag dependence

Fig. 1: Motivation: frequency-dependent and tag-dependent backscatter-power profiles of RFID tags.

In this paper, we propose **R**eflection **C**oefficient-based RF**ID** Fingerprint (RCID), a novel method to fingerprint RFID tags. RCID is motivated by the following observations.

- **Fact 1: the power of backscattered RFID signals is frequency-dependent**. Specifically, each RFID tag communicates with the reader via signal backscattering. The backscattered signal power (or equivalently the amount of reflected incident power) depends on the *reflection coefficient* that relates to the impedance of the tag circuit. Since some frequency-dependent capacitive and inductive electronic components compose the tag circuit, the reflection coefficient and thus the resulting backscattered signal power are also frequency-dependent. Fig. 1a gives an example where the backscattered signal power varies a lot for continuous-wave (CW) signals of different frequencies and the same incident power, leading to a unique *frequency-dependent backscatter-power profile*.
- **Fact 2: each RFID tag has a unique reflection coefficient due to manufacturing imperfection.** Therefore, each tag may reflect a different amount of power for the same CW signal. As exemplified in Fig. 1b, such unique reflection coefficients lead to distinguishable *tag-dependent backscatter-power profiles* for the same CW signal at different tags.

RCID explores the two observations above to well characterize the *frequency-dependent, tag-dependent* backscatter-power profiles of RFID tags over a wide frequency band. The key component of RCID is an *RCID collector* based

978-1-6654-5822-1/22/$31.00 ©2022 IEEE

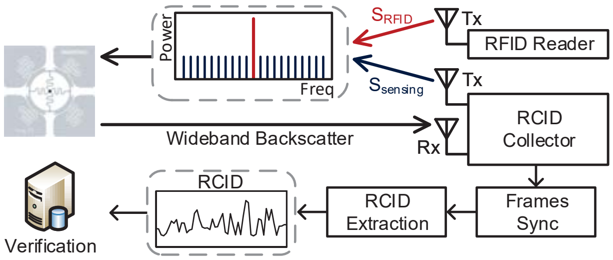


Fig. 2: RCID system architecture and workflow.

on orthogonal frequency-division multiplexing (OFDM). The RCID collector measures the backscattered signal power at each CW frequency to that of a reference frequency. Using the relative power makes each RCID fingerprint independent of the reader-tag distance and the reader's transmission power. In addition, the RCID collector measures the multi-path effects and channel response for each reader and use these measurements to calibrate each RCID fingerprint for achieving both reader and environment independence. Moreover, the RCID collector uses OFDM to simultaneously obtain the fingerprint elements at multiple carrier frequencies, so it can significantly accelerate the fingerprinting process. The RCID collector can be implemented either as a cheap auxiliary device or as a firmware update to existing RFID readers.

We prototype the entire RCID system on USRP X310 and thoroughly evaluate its efficacy and security. Our studies involve 600 COTS RFID tags, one of the largest experiments of its kind. According to our empirical results, the entropy of each RCID fingerprint can be up to 202 bits in contrast to the best prior result of 17 bits [12]. In addition, the authentication accuracy of RCID is 97.15% with the mean and median authentication error rates equal to 2.9% and 0.1%, respectively, which are comparable to the best prior work. Finally, it takes about 8 s to enroll a tag and 2 ms to verify an RCID fingerprint with a fully connected multi-class neural network to achieve a 97.15% authentication accuracy.

The rest of this paper is organized as follows. Section II gives an overview of the RCID system. Section III illustrates the definition of RCID fingerprints. Section IV details the RCID system design. Section VI evaluates the RCID system with prototyped experiments. Section VII outlines the related work. Section VIII concludes this paper.

II. RCID System Overview and Threat Model

Our RCID system targets many typical RFID application scenarios such as access control, asset tracking, and inventory management. For example, when a user with an RFID access card approaches a gate-control device, or when RFID-tagged physical objects are transported on a conveyor belt through a checkpoint, the RFID tag can be placed at or pass through a given location where its RCID fingerprint can be extracted and validated. Fig. 2 shows the RCID architecture and workflow, which consist of a backend server, RFID readers, and RFID tags. Each RFID reader is associated with an RCID collector which can be implemented either as a cheap auxiliary device or as a firmware update to commodity RFID readers with technical support from the reader manufacturer.

Each tag is associated with a physical entity such as a unique person or product and must be enrolled into the system by being brought to the vicinity of an arbitrary RFID reader along with the RCID collector. The RFID reader uses a conventional signal $\mathrm{S}_{\mathrm{RFID}}$ to interrogate and power the tag. The RCID collector transmits a low-power OFDM sensing signal $\mathrm{S}_{\mathrm{sensing}}$ and also receives the wideband backscattered signals from the tag. Subsequently, the Frame Synchronization module is invoked to synchronize backscattered RFID and OFDM signals and then outputs the OFDM symbols that contain the RCID fingerprint. Next, the RCID Extraction module outputs the RCID fingerprint after eliminating the impact of the radio environment (e.g., multi-path effects) and the RFID reader hardware from received OFDM symbols. Finally, the backend server trains a classifier based on the RCID fingerprint and stores it along with the standard tag information (e.g., EPC). In the later verification phase, the RCID fingerprint of each tag is extracted by any RFID reader in the same way and sent to the backend server for verification with the trained classifier.

Threat Model. We assume that the attacker acquires the data such as the EPC of a legitimate RFID tag, e.g., by sniffing the unencrypted reader-tag communications or impersonating a legitimate RFID reader to directly interrogating the tag. As mentioned before, commodity crypto-less RFID tags cannot deal with such data stealing. The attacker knows exactly how RCID works and can create many clones by writing the data on different writable RFID tags it owns. RFID cloning is quite easy and cheap to conduct, as a commodity writable RFID tag normally costs only a few cents.

III. Formulation of RCID Fingerprints

In the passive UHF RFID system we target, the reader continuously sends queries and transmits continuous wave (CW) to power the RFID tag. The tag replies with its unique EPC after being activated and receiving the query message. The tag communicates with the reader via backscatter [14], which is a passive communication method.

RCID fingerprints depend on a key RF circuit parameter called the reflection coefficient [15] denoted by Γ, which indicates the amount of reflected RF power caused by the impedance discontinuity of transmission media. Γ varies when the tag is in the backscatter or non-backscatter state. Since the RFID tag circuit contains many frequency-dependent components, Γ also varies with the frequency of the incident signal. Given the incident power P_{in} of the reader's CW signals, the reflected power P_{ref} by the RFID tag can be represented by $P_{\mathrm{ref}} = P_{\mathrm{in}}|\Gamma|^2$, which depends on both P_{in} and the frequency of the CW signal. In addition, no two RFID tags have identical circuits due to manufacturing imperfection, so P_{ref} of different tags also varies for the same CW signal.

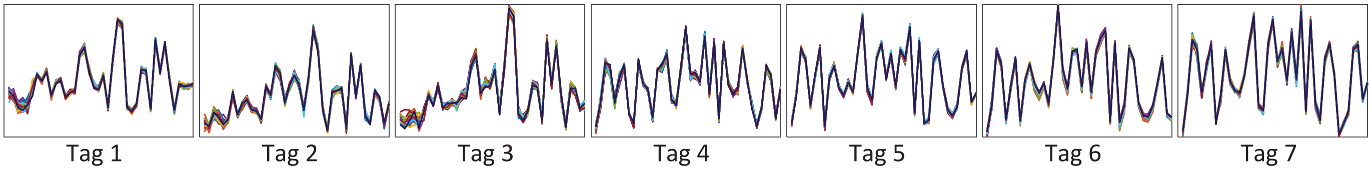


Fig. 3: Preliminary experimental results.

Based on the above motivation, We first formulate the power of backscatter signals in RFID systems. According to the free-space path loss model, the backscattered signal power is

$$P_{\rm rx} = P_{\rm tx} \frac{G_{\rm tx} G_{\rm rx} G_{\rm tag}^2 c^4}{(4\pi)^4 d^4 f^4} |\Gamma_f|^2 + P_L, \tag{1}$$

where $P_{\rm tx}$ is the power of CW sent by the reader, P_L is the leakage signal of CW, $G_{\rm tx}$ and $G_{\rm rx}$ are the gain of the reader's transmitting and receiving antenna, $G_{\rm tag}$ is the gain of the tag antenna, c is the speed of light, f is the carrier frequency, d is the distance between the reader and tag, and Γ_f is the reflection coefficient at the carrier frequency f. This backscatter-power model is more complicated than the commonly used one for RFID sensing [16]–[19], which mostly focuses on a single frequency in the operating band of RFID tags. It is more suitable for our need for a fine-grained power profile over a wide frequency band.

In existing methods [20], [21], the power of backscatter signals is the difference between the power received in the backscatter and non-backscatter states. Denoting the total gain of system by $G_0 = G_{\rm tx} G_{\rm rx} G_{\rm tag}^2$, we can rewrite the backscattered signal power as

$$P_B = P_{{\rm rx},2} - P_{{\rm rx},1} = P_{\rm tx} \frac{G_0 c^4}{(4\pi)^4 d^4 f^4} (|\Gamma_{2,f}|^2 - |\Gamma_{1,f}|^2), \tag{2}$$

where $P_{{\rm rx},1}$ and $P_{{\rm rx},2}$ denote the backscatter power in the backscatter and non-backscatter states, respectively. Define $\delta_f = |\Gamma_{2,f}|^2 - |\Gamma_{1,f}|^2$. Eq. (2) can be rewritten as

$$\delta_f = \frac{P_B}{P_{tx}} \frac{(4\pi)^4 d^4 f^4}{G_0 c^4}, \tag{3}$$

where P_B and $P_{\rm tx}$ can both be measured at the reader for a given carrier frequency f. In contrast, G_0 and d are hard to measure in the real scenarios.

In our design, the RCID fingerprint of a tag is collected over a wide frequency band from f_{-N} to f_N with step f_Δ, by sweeping the carrier frequency f with the same transmission power $P_{\rm tx}$. We normalize δ_{f_n} by δ_{f_0} as

$$\bar{\delta}_{f_n} = \frac{\delta_{f_n}}{\delta_{f_0}} = \frac{P_{B_n}}{P_{B_0}} (\frac{f_n}{f_0})^4, \tag{4}$$

where P_{B_n} and P_{B_0} denote the backscattered signal power at f_n and f_0, respectively. Doing normalization helps mitigate the impact of $P_{\rm tx}$, G_0, and d, which can vary a lot across different RFID readers and verification instances. Finally, the **RCID fingerprint** of an RFID tag is defined as

$$\bar{\Delta} = [\bar{\delta}_{f_{-N}}, \ldots, \bar{\delta}_{f_{-1}}, 1, \bar{\delta}_{f_1}, \ldots, \bar{\delta}_{f_N}]. \tag{5}$$

Preliminary Experiments. We conduct a simple experiment to highlight the feasibility of RCID fingerprints. To obtain the feature vector in Eq. (5), we simply sweep the CW carrier frequency from 905 to 925 MHz with step 500 KHz. Our experiment uses a USRP X310 [22] with two VERT900 antennas and the GNURadio RFID module [23] as the reader whose transmission power is set to 20 dBm. We test 7 Alien 9640 UHF RFID tags, and the reader-tag distance is fixed to 15 cm. The tests are conducted multiple times for each tag. We randomly select the results of 50 runs for each tag to derive and plot the RCID fingerprints $\bar{\Delta}$. Fig. 3 shows the experimental result, where the X-axis denotes the CW frequency, and the Y-axis represents $\bar{\delta}_{f_n}$. As we can see, the RCID fingerprint of each tag is highly consistent across the 50 runs and is also quite different from those of other tags.

Although the preliminary experiment above confirms the feasibility of RCID fingerprints, our basic prototype takes too much time to do frequency sweeping over a wide band. Take the UBX-160 [24] used on USRP X310 [22] as example. The frequency synthesizer MAX2871 [25] used on UBX-160 takes up to 100 μs[1] to set up a frequency according to the data sheet. In practice, we find that UBX-160 takes up to 300 ms to generate a stable, usable carrier frequency and needed 12.2 s in total to collect the RCID fingerprint over 40 CW frequencies. This latency is too long for many time-sensitive RFID applications such as access control, asset tracking, and conveyor belt systems. In addition, Eq. (4) relies on an important assumption that the reader-tag distance d remains unchanged during the fingerprinting process. Very long execution time like 12.2 s would invalidate this assumption. For example, it may be difficult to ask an RFID user to hold a tag steady for 12.2 s; RFID-tagged physical objects on a conveyor belt may quickly pass through the checkpoint. So we are motivated to propose a more effective method in Section IV to collect reliable RCID fingerprints in a very short time.

IV. RCID System Design

In this section, we explore OFDM to collect the RCID fingerprints over multiple subchannels simultaneously to significantly shortening the overall fingerprinting time.

A. Frame Design of RCID Collector

According to previous work [26], [27], the RFID tags can backscatter the ambient RF signals within their operating bandwidth. Therefore, if we deliver appropriate RF power over several subchannels concurrently, the backscatter occurs on

[1] It depends on the actual frequency.

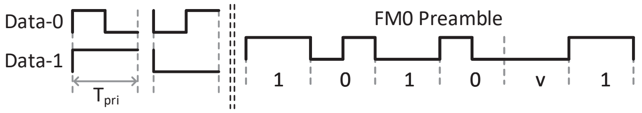


Fig. 4: FM0 baseband symbols and preamble.

all these subchannels. Therefore, if we let the RCID collector transmit OFDM signals along with the reader's query signal, the RFID tag would backscatter both signals.

To make OFDM signals compatible with the EPC Gen2 RFID standard, we need to solve the following challenges.

1. The first challenge is how to deliver the RF power on each subchannel using OFDM properly. According to Eq. (3), the transmitted power on each subchannel should be exactly the same in order to extract the RCID fingerprint. If we arrange the same value (e.g., '1') on all subchannels, the time-domain signal will be a sharp pulse followed by a long sequence filled with '0', which needs to be avoided when transmitting the wireless signal. Some existing OFDM training sequences can be used to construct the CW of RFID systems without worrying about the long strings of '0'. In particular, the Legacy Long Training Field (LLTF) of the 802.11n legacy preamble uses two continuous long training sequences (LTS) for channel estimation. The LTS is a vector filled with 52 "1" and "-1". Continuously transmitting the LTS can construct a "virtual CW" on each subchannel, which is filled with "1" and "-1" at different subcarriers. Therefore, the LTS can substitute the frequency-sweeping CW to collect RCID fingerprints.
2. The RFID and OFDM signals are transmitted at the same carrier frequency and thus may interfere with each other. According to the EPC UHF Gen2 Air Interface protocol [28], RFID tags can encode the baseband signal using either FM0 (bi-phase space) or miller encoding methods, selected by the RFID reader. The backscatter link frequency ranges from 40 KHz to 640 KHz. In this paper, we only consider the 40 KHz FM0-encoded baseband, our techniques can be easily extended to the miller-encoded baseband and also other backscatter link frequencies. Fig. 4 shows the FM0 baseband symbols consisting of data-0 and data-1 symbols. Both types of symbols invert their baseband phase at the boundary between each symbol, and the data-0 symbol has an extra mid-symbol phase inversion. In addition, both Data-0 and Data-1 symbols have high-voltage and low-voltage states, corresponding to the backscatter and non-backscatter states, respectively. The 40 KHz FM0 baseband signal can be treated as a 40 KHz square wave containing only the odd-integer harmonic frequency. If we only consider the 5th harmonic frequency, the bandwidth of the 40 KHz FM0 baseband signal is approximate 200 KHz. To avoid interference between RFID and OFDM signals, we leave the 12 central subchannels (312.5 KHz each) empty by shifting the LTS. By doing so, the OFDM and RFID signals do not have overlapping spectrums and can be easily separated by appropriate filters.
3. The RFID and OFDM signals are not synchronized. As shown in Fig. 5d, the OFDM symbols can occur during backscatter states, non-backscatter states, or the transitions between backscatter and non-backscatter states. The OFDM symbols during the transition states are corrupted and cannot be used for channel estimation. To make sure that there is at least one uncorrupted OFDM symbol in each backscatter or non-backscatter state, the duration of each OFDM symbol should be shorter than half of the minimum FM0 symbol duration in either state. In particular, let $T_{\mathrm{pri}}/2$ denote the minimum duration of an FM0 symbol, since the FM0 symbol "0" flips its state in the middle of the symbol duration. The duration of OFDM symbols should meet $T_{\mathrm{OFDM}} < T_{\mathrm{pri}}/4$.
4. Although OFDM symbols are used for RCID fingerprints collection instead of communication, they still need preambles for synchronization. We adopt the Legacy Short Training Field (LSTF) of IEEE 802.11 for frame synchronization. Each frame contains an LSTF and 100 OFDM symbols. The length of the LSTF is $2.5T_{\mathrm{OFDM}}$, so it does not overlap much with the backscatter signal.

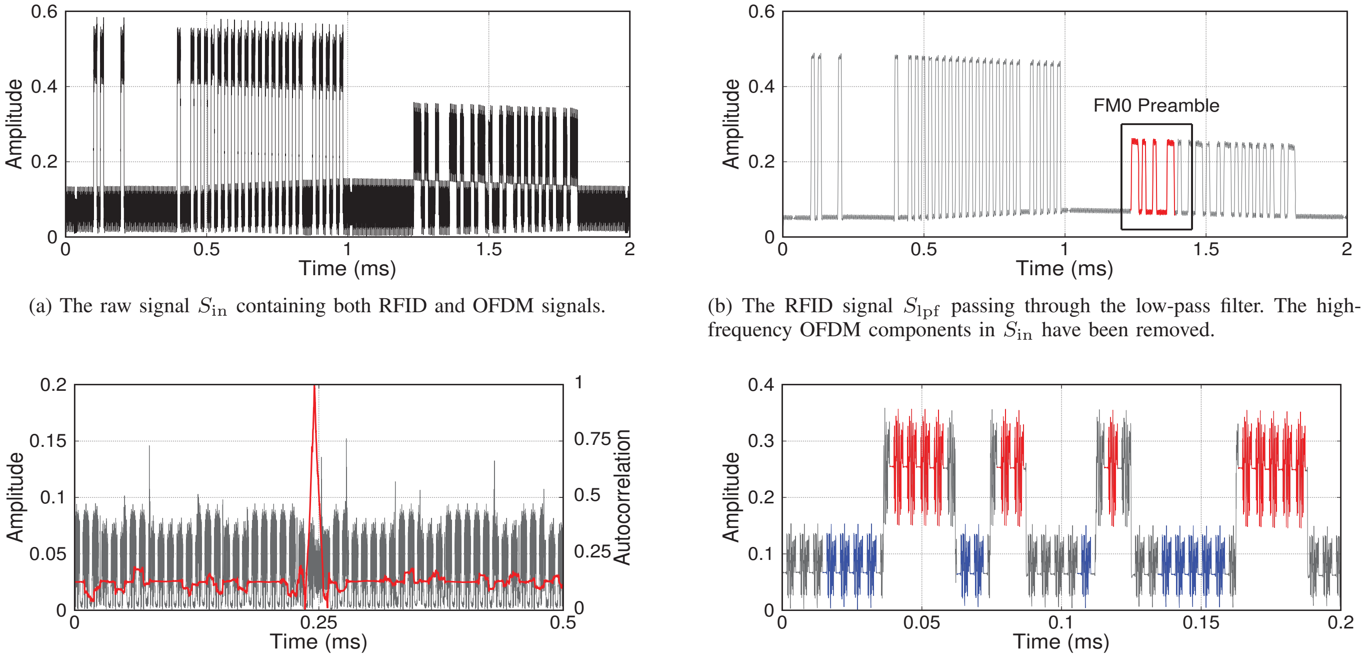
B. Frame Synchronization

The Frame Synchronization module is used to detect the preambles of backscattered RFID and OFDM frames. RFID frames contain the tag response, and OFDM frames contain the information for RCID fingerprints.

1) Preamble detection of RFID frames: Since the backscattered signals contain both RFID and OFDM signals, it is hard to apply the traditional preamble detection algorithms. An example is given in Fig. 5a, in which the received signal S_{in} is sampled at f_s. Recall that we leave the central 12 OFDM subchannels empty where RFID signals are dominating. So we use a low-pass filter with the cutoff frequency at 200 KHz to remove most OFDM signal. A K-points moving average filter is used to further smooth the signal. Fig. 5b shows the filtered signal S_{lpf} in which only a few OFDM signal above the cutoff frequency are still retrained.

We develop a basic algorithm to detect the RFID preamble. The target is to detect the FM0 preamble shown in Fig. 4. It takes five inputs, where S is the waveform vector, P_LEN is the vector recording the samples of each state in the FM0 preamble, L_{win} is the window length, L_{preamble} is the preamble length, S_{preamble} is the total number of preamble states, and ϵ is the tolerance for counting the samples in each preamble state. We use a sliding window to calculate the windowed average value whereby to judge the positive or negative state of the FM0 baseband signal. A finite state machine is used to decide whether the whole preamble is detected. Since the signal is interfered by the OFDM signal, we need to count the exact number of samples at each state.

We further propose a two-stage preamble strategy to significantly reduce the time complexity $O(n \log n)$ of the basic algorithm, where n denotes the total number of signal samples. If the basic algorithm is directly applied to the raw data with high sampling rate, it may take thousands of hours just for



(a) The raw signal S_{in} containing both RFID and OFDM signals.

(b) The RFID signal S_{lpf} passing through the low-pass filter. The high-frequency OFDM components in S_{in} have been removed.

(c) The gray waveform is the OFDM signal S_{hpf} through the high-pass filter. The red waveform is the normalized windowed autocorrelation ρ_n.

(d) The gray waveform is the raw signal S_{in}. The blue waveform $\mathbf{B}_L$ and red waveform $\mathbf{B}_H$ are detected OFDM symbols in different states.

Fig. 5: Signal processing for frame synchronization.

preamble detection. For example, n is equal to 2×10^7 for a one-second signal sampled at 20 MHz. In our approach, S_{lpf} is decimated at $f_{\text{FM0}} = 2$ MHz to S_{dec} in the coarse-grained detection stage. Then the basic algorithm is applied to S_{dec} to extract a coarse-grained set of the preamble's starting points, denoted by $\hat{\mathbf{p}} = [\hat{p_1}, \hat{p_2}, \ldots, \hat{p_N}]$, where N is the number of detected FM0 baseband preambles. In the subsequent fine-grained detection stage, The basic algorithm is reapplied to the samples in S_{lpf} with indices in $[\gamma\hat{p_n} - \epsilon, \gamma\hat{p_n} + L + \epsilon]$ to a fine-grained set of the preamble's starting points, denoted by $\mathbf{p}$, where $\gamma = f_s/f_{\text{FM0}}$ is the decimation coefficient, and $n \in [1, N]$. Since the K-point moving average filter causes a delay of $K/2$, $\mathbf{p}$ needs to be compensated by $K/2$. The detected preamble after this two-stage process is shown as the read line in Fig. 5b.

2) Preamble detection of OFDM frames: To detect the preamble of OFDM frames, we first apply a high-pass filter with the cutoff frequency at 200 KHz to remove the RFID signals. The filtered signal S_{hpf} is shown as the grey line in Fig. 5c. Since the LSTF is adopted, we can use the similar preamble detection method in IEEE 802.11. In particular, the windowed autocorrelation can be calculated by

$$C_n = \sum_{k=0}^{L_{\text{STS}}-1} S_{n+k} S^*_{n+k+L_{\text{FFT}}}, \tag{6}$$

where L_{STS} is the length of the STS symbol, and L_{FFT} is the FFT length. The signal energy in the processed window is

$$P_n = \sum_{k=0}^{L_{\text{STS}}-1} \left|S_{n+k}\right|^2. \tag{7}$$

The normalized windowed autocorrelation is

$$\rho_n = \frac{C_n}{P_n}. \tag{8}$$

The local peaks of ρ which are larger than the system threshold are the starting indices of OFDM preambles, represented by $\mathbf{q} = [q_1, q_2, \ldots, q_M]$, where M is the number of detected OFDM preambles. Fig. 5c plots ρ_n and S_{hpf}. There is a peak corresponding to the first sample in the preamble. Also note that the window length of the windowed autocorrelation function is L_{STS} instead of the standard value in IEEE 802.11, as we use an all-zeros cyclic prefix to suit our purpose.

3) Feature-symbol detection: The next step is to segment the OFDM symbols into one of the backscatter, non-backscatter, and transition states. This can be easily done based on the preamble positions of RFID and OFDM frames. The OFDM symbols in the backscatter state are extracted as $\mathbb{B}_H = [\mathbf{B}_{1|H}, \mathbf{B}_{2|H}, \ldots, \mathbf{B}_{K|H}]$, where K is the number of extracted symbols. There are much more OFDM symbols in the non-backscatter state than in the backscatter state. So we only extract the K most adjacent ones to $\mathbb{B}_H$, which are denoted by $\mathbb{B}_L = [\mathbf{B}_{1|L}, \mathbf{B}_{2|L}, \ldots, \mathbf{B}_{K|L}]$. In Fig. 5d, $\mathbb{B}_H$ and $\mathbb{B}_L$ are shown in red and blue lines, respectively.

C. RCID Fingerprint Extraction

The last step is to extract reliable RCID fingerprints from the retrieved OFDM symbols $\mathbb{B}_H$ and $\mathbb{B}_L$. RFID system may be deployed in both indoor and outdoor environments with rich location-dependent multi-path effects. In addition, in a large system with many RFID readers, the RCID fingerprint of the same tag may be collected and verified at different locations. Furthermore, each RFID reader has RF fingerprint that may have large impact on RCID fingerprint. So it is critical to eliminate the impact of multi-path effects and the RFID reader hardware to make RCID fingerprints both environment-independent and reader-independent.

For this purpose, we let the RCID collector measure the channel-response vector $\mathbf{h}_d$ of the reader's transceiver and $\mathbf{h}_e$ of the multi-path environment by transmitting an OFDM pilot signal alone before acquiring the RCID fingerprint. The received backscattered signal is represented by

$$\mathbf{y}_0 = \mathbf{h}_d \mathbf{h}_e \mathbf{t} + \mathbf{n} \tag{9}$$

where $\mathbf{t}$ is the training sequence, and $\mathbf{n}$ represents the i.i.d. Gaussian white noise. Define $\mathbf{h}_0 = \mathbf{h}_d \mathbf{h}_e$. Using the common least squares estimator, we can estimate $\mathbf{h}_0$ as $\hat{\mathbf{h}_0} = \mathbf{y}_0 \mathbf{t}^{-1}$.

The receiving vectors $\mathbf{y}_H$ and $\mathbf{y}_L$ can be obtained by removing the unused sub-carriers from $\mathcal{F}(\mathbf{B}_H)$ and $\mathcal{F}(\mathbf{B}_L)$. By doing so, the leakage signal P_L in Eq. (1) in the center of the spectrum can be removed. Define the channel vectors of tag in the backscatter and non-backscatter states as $\mathbf{h}_H$ and $\mathbf{h}_L$, respectively. We have

$$\mathbf{y}_H = \mathcal{F}(\mathbf{B}_H) = \mathbf{h}_d \mathbf{h}_e \mathbf{t}(\mathbf{h}_H + \mathbf{1}) + \mathbf{n} \tag{10}$$

and

$$\mathbf{y}_L = \mathcal{F}(\mathbf{B}_L) = \mathbf{h}_d \mathbf{h}_e \mathbf{t}(\mathbf{h}_L + \mathbf{1}) + \mathbf{n}. \tag{11}$$

Define $\hat{\mathbf{h}}_{\text{tag}} = \hat{\mathbf{h}}_H - \hat{\mathbf{h}}_L = \hat{\mathbf{h}}_{\text{tag}} = (\mathbf{y}_H - \mathbf{y}_L)\mathbf{t}^{-1}\hat{\mathbf{h}}_0^{-1}$. Then we can compute $\Delta = \left|\hat{\mathbf{h}}_{\text{tag}}\right|^2$ and further normalize it per Eq. (4) to obtain the eventual RCID fingerprint $\bar{\Delta}$.

D. Authentication (Classification and Identification)

We build a fully connected multi-class neural network with one hidden layer and 256 perceptrons for RCID fingerprint classification. This neural network is trained and used at the backend server. It takes $\bar{\Delta}$ as input and outputs a vector s containing the confidence scores for each class. In the experiment, we observe from a commercial spectrum analyzer that there can be some other devices in the ISM band that transmit periodically. To eliminate the sudden interference in backscattered signals, η confidence scores vector are summed up. The predicted result $\hat{p}$ is the tag with the highest score

$$\hat{p} = \arg\max_i \sum_{k=1}^{\eta} s_{k,i}. \tag{12}$$

If the other information such as EPC of tag $\hat{p}$ matches the retrieved from the tag being authenticated, the system considers the tested tag a genuine one and otherwise a clone.

V. Security Analysis

Now we analyze the resilience of RCID against various attacks launched by the adversary denoted by $\mathcal{A}$.

Tag cloning. In this attack, $\mathcal{A}$ makes a fake tag with the same EPC as the genuine tag. According to our experimental results, RCID achieves the overall authentication accuracy up to 97.15% and the FPR less than 0.1%. So it is highly unlikely for $\mathcal{A}$'s fake tag to have a very similar RCID fingerprint to the genuine one.

Brute force. In this attack, $\mathcal{A}$ keeps making and trying different fake tags with the genuine EPC. According to our empirical studies, the entropy of the RCID fingerprints over a 20 MHz bandwidth is about 202 bits. So it takes $\mathcal{A}$ about 2^{202} tries to make a tag with an RCID fingerprint highly similar to the genuine one and 2^{101} tries to find two RFID tags with highly similar RCID fingerprints. Such brute-force attacks occur in the physical world and can also be mitigated by rate-limiting authentication failures.

Signal replay. In this attack, $\mathcal{A}$ relays the sniffed backscatter signals from the genuine tag to the RFID reader. The replayed signal inevitably contains the RF fingerprint of $\mathcal{A}$'s device, so the RCID fingerprint measured by our system fails to match the genuine one with overwhelming probability.

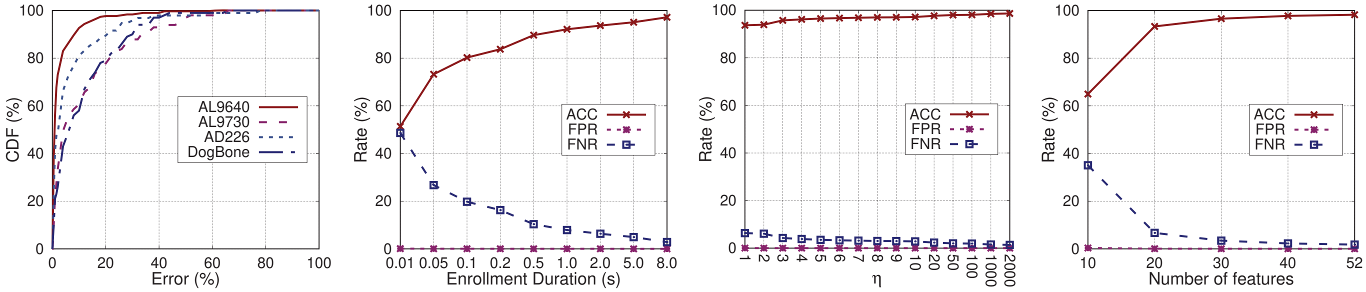
Signal forgery. In this attack, $\mathcal{A}$ tries to forge a backscattered RFID signal in the hope of inducing an RCID fingerprint that closely matches genuine one. According to Eq. 9, the RCID collector needs to estimate the channel-response vector $\mathbf{h}_d$ of the reader's transceiver and that $\mathbf{h}_e$ of the multi-path environment to generate an authentic fingerprint that is both reader-independent and environment-independent. Since the RCID collector is a software module inside the RFID reader, it is almost infeasible for external $\mathcal{A}$ to acquire $\mathbf{h}_d$ and $\mathbf{h}_e$ for fine-tuning its forged signal to produce a valid RCID fingerprint measured by the RCID collector.

To sum up, our RCID system offers very strong resilience to the tag cloning, brute force, signal replay, and signal forgery attacks, which are all common attacks on RFID authentication systems. Same as all the other RFID fingerprinting techniques, RCID cannot deal with denial-of-service (DoS) attacks aiming to prevent the acquisition and authentication of valid RCID fingerprints. There is no practical solution to such DoS attacks.

VI. Evaluation

A. Implementation

We implement a simplified EPC UHF Gen2 Air Interface Protocol and an RCID collector on USRP X310 [22] with two UBX160 [24] daughter boards and three VERT900 vertical antennas. Both the RFID reader and RCID collector run on a single X310 using different RF channels. The X310 connects with an Intel X520-DA2 10 Gigabit Ethernet card on the host workstation via an SFP+ cable to ensure the high throughput. We implement a GNURadio workflow for signal Tx/Rx and files I/O. Generating transmission samples and processing received signals are all done by Matlab in non-real-time. All communication with USRP, signal processing, and training models are performed by a workstation equipped with AMD 3960X 24 cores CPU, 128 GB RAM, and 2 NVIDIA Titan RTX GPU.



(a) CDF of authentication errors for each tag model

(b) Impact of enrollment time

(c) Impact of authentication time

(d) Impact of # of features

Fig. 6: Authentication performance with dataset D1.

More implementation and evaluation settings are as follows. The RFID reader works at 915 MHz with the transmission power of -5 dBm and the sampling rate of 1 MHz. The OFDM-based RCID collector works at 915 MHz with the transmission power of -15 dBm and used 64-point FFT, 1/2 length cyclic prefix with zero padding, and a bandwidth of 20 MHz. The transmission power of both the RFID reader and the OFDM-based RCID collector comply the FCC regulation [29]. We test 600 UHF RFID tags involving four models of different antenna shapes: Alien 9640 (300 pieces), Alien 9730 (100 pieces), SMARTRAC DogBone (100 pieces), and Avery Dennison AD-226iM (100 pieces).

We implement the multi-class neural network via PyTorch, which has one hidden layer and 256 perceptions. Typical performance metrics for machine learning research are used and include the accuracy (ACC), the false positive rate (FPR), and the false negative rate (FNR). Since all the datasets have multiple classes, we calculate the macro-average on each metric. Unless stated otherwise, k-fold cross-validation ($k = 5$) is used to eliminate the unbalance of all datasets; $\eta = 5$ is used to eliminate the sudden interference from ambient transmissions in the ISM band; and all the experiments are conducted in a bedroom with the tag-reader distance of 15 cm.

B. Dataset Description

We collect 2 datasets for different experimental purposes.

D1: All 600 tags are used in this dataset. The samples in D1 were all collected with the same experimental setup, and the duration of each sample was 10 s.

D2: 50 Alien 9640 tags are used to evaluate the impact of four factors: hardware, environment, distance, and orientation. We change every single factor while fixing the rest. The duration of each sample was 2 s.

The data-collection procedures are controlled by a bash script to realize accurate timing control. Each signal sample is an 8-bytes single-precision complex number. The raw I/Q data rate for each tag is 160 Mbps, and the total data volume is more than 2.2 TB.

C. Overall Performance

1) Authentication accuracy: We first evaluate the authentication accuracy of RCID with D1. Table I shows the results for each tag model and the overall performance. Fig. 6a also shows the CDF of RCID's authentication errors for each tag model. The overall authentication accuracy is 97.15%, and the mean and median of the authentication error rates are 2.9% and 0.1%, respectively. The results of each tag model show that the RCID performance is closely related to the complexity of the antenna shape and also the size of each tag. Dogbone tags have the simplest antenna design, so they have the lowest authentication accuracy. Although Alien 9730 tags have a complex antenna, their tiny size make them easily suffer from interference and poor SNR, leading to the average authentication accuracy. Alien 9640 tags have a relatively complex antenna and a reasonable size as well, so they achieve the highest authentication accuracy.

TABLE I: Authentication accuracy of different tag models.

Alien 9640	Alien 9730	AD-226iM	DogBone	Overall
99.01%	94.96%	97.08%	93.43%	97.15%

2) Enrollment time: We next evaluate the relation between the enrollment time and authentication accuracy. The enrollment time are proportional to the number of training samples. Fewer training samples can translate into higher system usability, and vice versa. By controlling the number of training samples, we test the following nine enrollment time settings in seconds: 0.01, 0.05, 0.1, 0.2, 0.5, 1.0, 2.0, 5.0, and 8.0. As shown in Fig. 6b, it is not surprising to see that the authentication accuracy increases with the enrollment time. We also notice that the FNR is always very low regardless of the authentication accuracy. So the system operator can freely adjust the enrollment time to suit the usability requirement without sacrificing the system security.

3) Authentication time: We further evaluate the impact of the authentication duration. The authentication module uses η continuous scores to mitigate the possible interference from ambient radio signals. The larger η, the longer the authentication time, the lower the system usability, and vice versa. In this experiment, we evaluate the authentication accuracy, the FPR, and the FNR over D1 with η ranging from 1 to 2000. As shown in Fig. 6c, the accuracy without interference elimination (i.e., $\eta = 1$) is 93.67% and reaches 97.15% for $\eta = 10$. But when η increases from 10 to 2,000, the accuracy

TABLE II: Accuracy with different hardware and environments.

Baseline	USRP 0, Bedroom 1, 15cm, $\eta = 5$
Accuracy	99.25%

Device	USRP 1	USRP 2
Accuracy	97.55%	96.95%

Location	Living Room 1	Living Room 2
Accuracy	98.40%	91.60%

Distance	15 cm	17.5 cm	20 cm	22.5 cm	25 cm
Accuracy	99.25%	90.90%	84.99%	76.42%	79.85%

only slightly improves by 1.48% to 98.63%. In our prototype system, RCID fingerprints can be extracted at an average rate of five features per millisecond, each corresponding to a different CW frequency. For $\eta = 10$ and $\eta = 2000$, the actual authentication delays are about 2ms and 0.4s, respectively. Both authentication delays are quite acceptable for practical applications. It is unwise to make η too large because it would significantly increase the computational load and time without many performance gains.

4) Impact of OFDM bandwidth: We also evaluate the impact of the OFDM signal bandwidth. Intuitively speaking, the larger the bandwidth, the more features in the RCID fingerprint with one for each carrier frequency, the higher the authentication accuracy, and vice versa. In this experiment, we selected a subset of features from the samples over 20 MHz and show the result in Fig. 6d. As expected, the authentication accuracy increases with the number of features or equivalently the OFDM signal bandwidth. In particular, since adjacent features are separated by a bandwidth of 312.5 kHz, the accuracy is already larger than 90% for 20 features corresponding to a bandwidth of 6.25 MHz.

5) False-positive rates (FPRs): Our previous evaluations reveal an extremely low FPR consistent in all experimental settings regardless of the achievable TPR and authentication accuracy. For example, Fig. 6b shows that the authentication error rate is about 25% with only 0.05 s enrollment duration, while the FPR is only 0.2%. This means that the RCID system is highly effective in rejecting inauthentic RFID tags, which is very important for security-sensitive applications.

D. Impact of Measurement Conditions

It is important to evaluate the robustness of RCID fingerprints to various measurement conditions. In this set of experiments, we first randomly select 50 tags from D1 as the enrollment samples to train the classifier. In each subsequent evaluation instant, we use these 50 tags to collect the fingerprint samples by taking turns varying each influence factor while fixing the others. It takes about 2 s to collect one fingerprint sample. The baseline experiment setups and accuracy results are shown in Table II.

Hardware. We first evaluate the impact of different RFID readers and RCID collectors. For this experiment, we collect the RCID fingerprints of the 50 tags with another two USRP X310 devices and obtain consistent performance results among the three X310 devices.

TABLE III: Performance comparison.

	TIE+ABP	SP	HuFu	Eingerprint	RCID
St	96.0%	99.6%	95.0%	97.3%	99.25%
Dy	36.2%	37.6%	90.0%	96.2%	95.0%

Environment. Then we evaluate the impact of the measurement environment which incur different multi-path effects to backscattered signals. For this experiment, we collect the RCID fingerprints at another two living rooms. The resulting authentication accuracy in both locations is comparable with the original result.

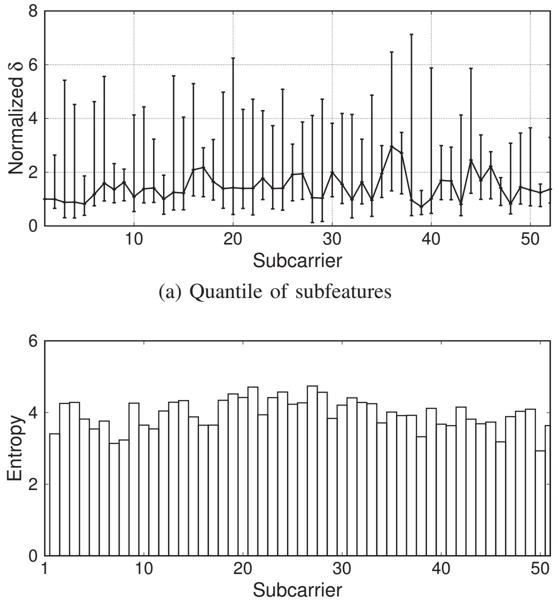
Distance. The tag-reader distance d affects the RSSI and phase of backscattered signals. In this experiment, we collect RCID fingerprints at four different distances and show the result in Table II. As d increases, backscattered signals experience a graduate attenuation, which leads to inaccurate RCID fingerprints and thus slightly reduces the authentication performance. But the overall performance is still quite acceptable for practical distance settings below 20 cm. For example, the RCID fingerprints can be verified when RFID users approach a gate-control device or when RFID-tagged physical objects are transported on a conveyor belt through a checkpoint.

E. Feature Space and Entropy

One of the most important issues for RFID fingerprinting is the dimension and entropy of the feature space, which determine the security and usability of the fingerprinting technique. Each feature in an RCID fingerprint relates to a normalized value at a unique OFDM subcarrier. We estimate the RCID feature space based on the 1,217,006 samples for 600 tags in D1. Fig. 7a is the 1st, 2nd and 3rd quantile plots of each feature. We can see that the feature values of most subcarriers cover a large range, which means the high distinctiveness of individual RCID fingerprints. We also compute the entropy for each subcarrier space and show the result in Fig. 7b. Each subcarrier space can offer 4 bits of information on average. Since there are 52 subcarriers over 20 MHz, the total entropy of the RCID fingerprints is about 202 bits which can guarantee sufficiently high security in practical settings.

F. Performance Comparison with Related Work

We compare the authentication accuracy of RCID with some representative UHF RFID fingerprinting schemes based on different hardware features, including the time interval error (TIE) and average baseband power (ABP) in the pioneering work, the spectrum (SP) feature proposed by Zanetti [30], the coupling feature between two tags in HuFu [10], and the charging duration feature in Eingerprint [12]. We use the same experiment setups in HuFu [10] for fair comparisons. In the stationary (St) case, the enrollment and authentication



(a) Quantile of subfeatures

(b) Entropy of subfeatures

Fig. 7: RCID feature space illustration.

are done in the same location, while in the dynamic (Dy) case these procedures are done in separate rooms. There are total 50 Alien 9640 tags tested in each case. The comparison results are shown in Table III. In the stationary case, all the techniques achieve comparably high authentication accuracy. For the dynamic scenario, RCID still achieves very high accuracy and is only slightly worse than Eingerprint [12]. This is because RCID extract the fingerprints with OFDM which is relatively more sensitive to the environment fluctuation.

We also briefly compare the entropy of our RCID feature space to that of two most relevant schemes. Note that the entropy of the feature space represents the capability of the maximum number of the tags can be distinguished. The pioneering work [5] uses the baseband signal power at a single frequency to fingerprint RFID tags, amounting to a single subcarrier feature in RCID fingerprints. This work can deliver an empirical entropy of 4.57 bits, which is comparable to the entropy of a single RCID subcarrier feature. In addition, Eingerprint [12] uses a one-dimension feature called persistence time for RFID fingerprinting. The standard variance of persistence time is about 0.1 s. The impinj reader they use can report timestamps in the granularity of µs. Therefore, Eingerprint can support at most 0.1s/1 µs = 100,000 devices, corresponding to an entropy of about 17 bits. In contrast, the empirical entropy of our RCID feature space is about 202 bits over a bandwidth of 20 MHz, representing a much higher level of security than all existing work.

VII. Related Work

There is significant effort on RFID security. Existing work can be divided into three categories by enhanced protocol designs, cryptography, and RF fingerprinting.

The solutions in the first category such as [8], [11], [31]–[33] normally secure the RFID systems by adding extra factors to the authentication procedures. Self-jamming [31], [33] is an effective method to prevent unauthorized querying and eavesdropping attacks. Both Yang [8] and Zhao [11] leverage the interrelationships between tags inside a federated tag array to authenticate tags. RF-Mehndi [11] adds a biometric authentication factor, and RF-Rhythm [32] uses RFID tags as a password-input method to induce a second authentication factor to the RFID system. Although these solutions can secure the RFID system and do not require modifications on either tags or the infrastructure, adding extra authentication factors inevitably diminishes convenience of the RFID systems.

The techniques in the second category apply elegant cryptographic designs [2]–[4], [34]–[36] to secure RFID systems. Although offering strong security against RFID spoofing and cloning, these techniques require significant updates to both tags and the infrastructure. Since the original EPC Gen2 protocol does not support the crypto functions, these cryptographic designs are not compatible with COTS UHF RFID devices. In contrast, the proposed RCID system applies to COST RFID tags and readers after a firmware update at the reader side or adding a very cheap auxiliary device.

The methods in the third category such as [5], [6], [9], [10], [12], [13], [37] explores the physical-layer features caused by manufacturing imperfection to fingerprint RFID tags. The pioneering work [5] combines the time-interval error (TIE) and the baseband signal power P_B of the backscattered signal to fingerprint 50 RFID tags. The empirical entropy for TIE and P_B are 5.84 bits and 4.57 bits, respectively. The impulse response of RFID tags has been tested in [5], [6] as well. Hu-Fu [10] uses the coupling features between two tags to identify tags. More recently, Eingerprint [12] fingerprints RFID tags by using the persistent time, which refers to the duration of a tag going from the fully charged state to the fully discharged state. Both tag coupling and persistence time only have a single feature space with limited entropy. In contrast, we have demonstrated that the RCID fingerprint involves an entropy of 202 bits over a 20 MHz bandwidth, which indicates the high resilience of our system to signal spoofing and cloning.

VIII. Conclusion

In this paper, we proposed RCID, a novel system to fingerprint RFID tags based on the unique reflection coefficient of each tag circuit. Based on a novel OFDM-based fingerprint collector, our system can quickly acquire and verify the RCID fingerprints of RFID tags which are independent of the RFID reader and measurement environment. Our system applies to COTS RFID tags and readers after installing a firmware update at the reader or adding a very low-cost auxiliary device. Extensive prototyped experiments confirm that RCID is highly secure against common attacks on RFID authentication systems and is also highly usable with very short tag-enrollment and authentication time.

Acknowledgment

This project was supported in part by US National Science Foundation under grants CNS-2055751/1933069/1824355.

References

[1] "MIFARE SAM AV3 for NTAG 5, ICODE DNA and UCODE DNA," 2020. [Online]. Available: https://www.nxp.com/docs/en/application-note/AN12698.pdf

[2] T. Li, W. Luo, Z. Mo, and S. Chen, "Privacy-preserving RFID authentication based on cryptographical encoding," in *IEEE INFOCOM*, 2012.

[3] L. Fu, X. Shen, L. Zhu, and J. Wang, "A low-cost UHF RFID tag chip with AES cryptography engine," *Security and Communication Networks*, vol. 7, no. 2, pp. 365–375, May 2014.

[4] L. Yang, Q. Lin, C. Duan, and Z. An, "Analog on-tag hashing: Towards selective reading as hash primitives in Gen2 RFID systems," in *ACM MobiCom*, 2017.

[5] D. Zanetti and B. Danev, "Physical-layer identification of UHF RFID tags," in *ACM Mobicom*, Chicago, Illinois, September 2010.

[6] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of RFID devices," in *USENIX Security*, Montreal, Canada, August 2009, pp. 199–214.

[7] S. Periaswamy, D. Thompson, and J. Di, "Fingerprinting RFID tags," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 06, pp. 938–943, November 2011.

[8] L. Yang, P. Peng, F. Dang, C. Wang, X. Li, and Y. Liu, "Anti-counterfeiting via federated RFID tags' fingerprints and geometric relationships," in *IEEE INFOCOM*, Kowloon, Hong Kong, April 2015.

[9] J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, and J. Zhao, "GenePrint: Generic and accurate physical-layer identification for UHF RFID tags," *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, pp. 846–858, April 2016.

[10] G. Wang, H. Cai, C. Qian, J. Han, X. Li, H. Ding, and J. Zhao, "Towards replay-resilient RFID authentication," in *ACM MobiCom*, 2018.

[11] C. Zhao, Z. Li, T. Liu, H. Ding, J. Han, W. Xi, and R. Gui, "RF-mehndi: A fingertip profiled RF identifier," in *IEEE INFOCOM*, Paris, France, April 2019.

[12] X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Eingerprint: Robust energy-related fingerprinting for passive rfid tags," in *NSDI*, Santa Clara, California, February 2020.

[13] J. Han, C. Qian, Y. Yang, G. Wang, H. Ding, X. Li, and K. Ren, "Butterfly: Environment-independent physical-layer authentication for passive RFID," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 4, pp. 1–21, December 2018.

[14] C. Boyer and S. Roy, "Backscatter communication and rfid: Coding, energy, and mimo analysis," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 770–785, March 2014.

[15] J. Griffin and G. Durgin, "Complete link budgets for backscatter-radio and rfid systems," *IEEE Antennas and Propagation Magazine*, vol. 51, no. 2, pp. 11–25, July 2009.

[16] L. Yang, Y. Li, Q. Lin, X.-Y. Li, and Y. Liu, "Making sense of mechanical vibration period with sub-millisecond accuracy using backscatter signals," in *ACM Mobicom*, New York City, New York, October 2016.

[17] H. Jin, J. Wang, Z. Yang, S. Kumar, and J. Hong, "Wish: Towards a wireless shape-aware world using passive RFIDs," in *ACM MobiSys*, Munich, Germany, June 2018.

[18] C. Wang, J. Liu, Y. Chen, H. Liu, L. Xie, W. Wang, B. He, and S. Lu, "Multi-touch in the air: Device-free finger tracking and gesture recognition via COTS RFID," in *IEEE INFOCOM*, Honolulu, HI, April 2018.

[19] H. Jin, Z. Yang, S. Kumar, and J. Hong, "Towards wearable everyday body-frame tracking using passive RFIDs," in *ACM UBICOMP*, Singapore, October 2018.

[20] C. Wang, L. Xie, W. Wang, T. Xue, and S. Lu, "Moving tag detection via physical layer analysis for large-scale RFID systems," in *IEEE INFOCOM*, San Francisco, CA, April 2016.

[21] T. Wei and X. Zhang, "Gyro in the air: tracking 3D orientation of batteryless internet-of-things," in *ACM Mobicom*, New York City, New York, October 2016.

[22] "UBX 10-6000 MHz Rx/Tx (160 MHz, X Series only)." [Online]. Available: https://www.ettus.com/all-products/x310-kit/

[23] N. Kargas, F. Mavromatis, and A. Bletsas, "Fully-coherent reader with commodity SDR for Gen2 FM0 and computational RFID," *IEEE Wireless Communications Letters*, pp. 617–620, 2015.

[24] "Ubx 10-6000 mhz rx/tx (160 mhz, x series only)," 2021. [Online]. Available: https://www.ettus.com/all-products/ubx160/

[25] "MAX2871 23.5MHz to 6000MHz Fractional/Integer-N Synthesizer/VCO." [Online]. Available: https://www.maximintegrated.com/en/products/comms/wireless-rf/MAX2871.html

[26] Y. Ma, N. Selby, and F. Adib, "Minding the billions: Ultra-wideband localization for deployed RFID tags," in *ACM Mobicom*, Snowbird, Utah, October 2017.

[27] Z. Luo, Q. Zhang, Y. Ma, M. Singh, and F. Adib, "3d backscatter localization for fine-grained robotics," in *NSDI*, Boston, Massachusetts, February 2019.

[28] "EPC UHF Gen2 Air Interface Protocol." [Online]. Available: https://www.gs1.org/standards/epc-rfid/uhf-air-interface-protocol

[29] "47 CFR § 15.231 - Periodic operation in the band 40.66-40.70 MHz and above 70 MHz." [Online]. Available: https://www.law.cornell.edu/cfr/text/47/15.231

[30] D. Zanetti, P. Sachs, and S. Capkun, "On the practicality of uhf rfid fingerprinting: How real is the rfid tracking problem?" in *Privacy Enhancing Technologies*, Waterloo, Canada, July 2011.

[31] H. Ding, J. Han, Y. Zhang, F. Xiao, W. Xi, G. Wang, and Z. Jiang, "Preventing unauthorized access on passive tags," in *IEEE INFOCOM*, Honolulu, HI, April 2018.

[32] J. Li, C. Wang, A. Li, D. Han, Y. Zhang, J. Zuo, R. Zhang, L. Xie, and Y. Zhang, "RF-Rhythm: secure and usable two-factor RFID authentication," in *IEEE INFOCOM*, Jun. 2020.

[33] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, "Securing RFIDs by randomizing the modulation and channel," in *NSDI*, Oakland, CA, May 2015.

[34] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight mutual authentication and ownership transfer for RFID systems," in *IEEE INFOCOM*, Pisa, Italy, March 2010.

[35] H.-J. Chae, M. Salajegheh, D. J. Yeager, J. R. Smith, and K. Fu, "Maximalist cryptography and computation on the WISP UHF RFID tag," in *Wirelessly Powered Sensor Networks and Computational RFID*, J. R. Smith, Ed. Springer, 2013, ch. 10, pp. 175–187.

[36] M. Chen and S. Chen, "Etap: Enable lightweight anonymous RFID authentication with o (1) overhead," in *IEEE ICNP*, San Francisco, California, March 2015.

[37] G. DeJean and D. Kirovski, "RF-DNA: Radio-frequency certificates of authenticity," in *International Workshop on Cryptographic Hardware and Embedded Systems*, Vienna, Austria, September 2007.