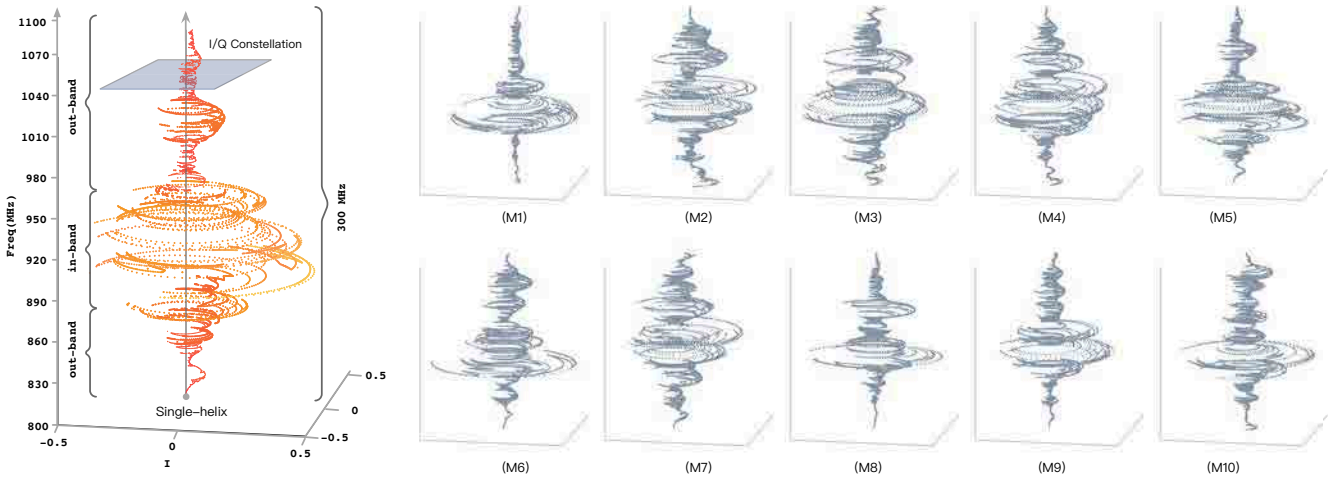
RF-DNA: Large-Scale Physical-layer Identifications of RFIDs via Dual Natural Attributes

Qingrui Pan†, Zhenlin An†, Xueyuan Yang, Xiaopeng Zhao, Lei Yang
†Co-primary Authors
Department of Computing, The Hong Kong Polytechnic University
{pan,an,xueyuan,zhao,young}@tagsys.org



(a) RF-DNA Structure

(b) RF-DNA examples acquired from ten different types of RFID tags

Fig. 1: Illustration of RF-DNA. The RF-DNA is a helical chain containing millions of DNA, each of which is a pair of I and Q components of a tag's intrinsic response when it is challenged at some frequency. (a) shows the structure of RF-DNA. An arbitrary cross-section of the RF-DNA is an I/Q constellation diagram representing the tag's intrinsic response at a frequency; (b) shows examples of (undersampled) RF-DNA acquired from ten different types of tags (M1~M10), exhibiting remarkably different spatial structures.

Abstract

Physical-layer identification aims to identify wireless devices during RF communication by exploiting the imperfections of their radio circuitry, i.e., hardware fingerprint. Previous work proposed several hardware fingerprints for RFIDs (e.g., TIE, ABD, PSD, etc). However, these proposed fingerprints suffer from either unscalability or acquisition inefficiency. This work presents RF-DNA, a new hardware fingerprint composed of millions of Dual Natural Attributes (DNA) organized in a helical structure, where a pair of DNA represents a tag's intrinsic response at some frequency. We take advantage of the frequency agnostic phenomenon that a commercial RFID tag can respond within a wider band than the regulated, to acquire 10× more features than previous fingerprints. At the heart of this work are the context-free acquisition approach to extracting DNA from backscatter signals; and the accurate DNA matching algorithm for verifying a tag's identity. A total of 160,000 RF-DNA instances were collected from 16,000 tags using a customized automatic acquisition system. We subsequently carried out large-scale experiments to test the identification accuracy of RF-DNA and previously proposed fingerprints. Our comprehensive evaluation reveals that RF-DNA can achieve a mean accuracy of 95.98%. In contrast, those of previous fingerprints fall to 60% below when in face of thousands of tags.

ACM MobiCom '22, October 17–21, 2022, Sydney, NSW, Australia

ACM ISBN 978-1-4503-9181-8/22/10…$15.00
https://doi.org/10.1145/3495243.3517028

CCS Concepts

• **Networks → Mobile and wireless security**.

Keywords

Security, RFID, Physical-layer Identification

ACM Reference Format:
Qingrui Pan†, Zhenlin An†, Xueyuan Yang, Xiaopeng Zhao, Lei Yang. 2022. RF-DNA: Large-Scale Physical-layer Identifications of RFIDs via Dual Natural Attributes. In *The 28th Annual International Conference On Mobile Computing And Networking (ACM MobiCom '22), October 17–21, 2022, Sydney, NSW, Australia.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3495243.3517028

1 Introduction

Radio Frequency IDentification (RFID) tags are becoming increasingly key components of the Internet of Things (IoT) and are widely adopted in many systems such as electronic passports, mobile payment, and supply chain systems. According to the report from

Table 1: Comparisons to the state-of-the-art

Solution	Fingerprint(s)	Comp.[1]	Scale(#)[2]	Accuracy[3]	Time
ETH[8]	TIE+ABP	Ant.+IC	50	98.7% → 26.08%	20ms
Geneprint[9]	ExTIE+PSD	Ant.+IC	150	99.68% → 56.08%	20ms
TagPrint[10]	Phase	Ant.	2,000	80.39% → 24.93%	20ms
Eingerp.[12]	PT	IC	200	91.60% → 77.80%	60s
Ours	RF-DNA	Ant.+IC	16,000	95.98%	20ms

[1] Comp. indicates which components (antenna and/or IC) affect the fingerprint
[2] Scale means how many tags were tested in the related work.
[3] $p_1 \rightarrow p_2$: p_1 is the accuracy originally reported by the related work and p_2 is the accuracy of the solution re-evaluated using our large-scale tag set.

IDTechEx [1], 17.5 billion RFID tags are sold in 2018. The security of RFIDs attracts much attention from the industry and academia. A large number of security protocols were proposed for RFID authentication [2–4], key management [5], and privacy preservation [6]. However, these protocols are rarely used in practice because the extremely limited power of RFID tags cannot meet their intensive computation demands.

Physical layer identification (PLI) is the process of fingerprinting the analog circuitry of a device by analyzing the device's wireless communication at the physical layer to identify a wireless device or a group of wireless devices [7]. PLI is based on the insight that the circuitry imperfections introduced during the manufacturing processing which affect the transmitted RF signals. PLI is tamper-proof, measurable, and needless of extra computations. All these merits highly fit the security demand of RFID system. For example, PLI is a very effective way to counteract cloning and spoofing attacks. It can be used in many applications that require a high level of security like valuable assets management and user identification. However, PLI was rarely studied in the field of RFID [8–10], among which a detailed comparison summary is presented in Table 1 (see §2 for more details). The typical work [8] employs backscatter link frequency (BLF) (equivalent to time interval error, TIE) as fingerprint, which is derived from the clock drifts of tags. However, this fingerprint is distinguishable only on a very small scale (i.e., dozens of RFID tags) because the EPCglobal GEN 2 protocol [11] already regulates such hardware discrepancy. Specifically, the protocol specifies that the BLFs of tags are only allowed to vary within 21.24 (±10.62%) Hz on average (refer to Table 6.9 of [11]). Non-conforming tags are not allowed to sell on the market. The work [8] only analyzed TIEs over 50 different tags, resulting in a mean accuracy of 71.4%. This drawback that the hardware imperfection is constrained in a small range by communication protocols is also observed in other previously proposed fingerprints. Thus, regardless of distinguishability or scalability, the previously proposed fingerprints are completely unsatisfied in face of billions of deployed RFIDs.

Can we identify a large number of RFID tags in the physical layer? Answering this question requires us to explore an entirely new type of scalable fingerprint for RFID systems. We found that the previously proposed fingerprints are exploited at in-band frequencies that the related agencies assign to an RFID system, i.e., 902-928 MHz in the US. The recent work [13, 14] discovered the frequency agnostic phenomenon that today's commercial RFID tags can backscatter the incoming RF signal in the 300 MHz bandwidth from 800-1100 MHz, which is around 10× larger than the specified ISM band. This results from the reality that tags are designed flat across regions and countries (e.g., 902-928 MHz in USA, 865-868 MHz in China) to support the worldwide logistics [15]. This phenomenon inspires us to exploit a fingerprint, which is present not only at in-band frequencies but also at out-of-band frequencies. Actually, tags behave more freely, diversely and unexpectedly in out-of-band frequencies since no regulations are defined there.

In this work, we present RF-DNA, an RFID fingerprint composed of millions of Dual Natural Attributes (DNA) organized in a helical structure. Fig. 1 illustrates the basic idea of RF-DNA. Specifically, we collect a tag's *intrinsic response caused by the hardware imperfection at some frequency* as the DNA. [1] The intrinsic response is a complex exponential number (i.e., $ae^{J\theta}$), which can be further decomposed into the I and Q components (i.e., $I = a\cos\theta$ and $Q = a\sin\theta$) based on the Euler formula. Thus, a DNA is a pair consisted of the $I(f)$ and $Q(f)$ components at frequency f. By traversing the whole 300 MHz responsive bandwidth, a chain of DNA called RF-DNA is obtained, including one million pairs of DNAs (which is in the same order of magnitude as an escherichia coli's biological DNA). The value space of RF-DNA is up to 0.1 trillion in theory given that the physical-layer signals are represented using 10 bits in the IQ channels, which is sufficient to uniquely distinguish each single deployed RFID tag around the world.

Utilizing RF-DNA for physical-layer identification involved two main challenges. First, when viewing a tag as an equivalent RLC circuit, its response to an input signal at some frequency is called *intrinsic response*, which carries the invariant caused by the circuitry imperfections. However, separating the intrinsic response from a tag's context-aware backscatter signals is quite challenging. To deal with this issue, a context-free DNA profiling algorithm is proposed to eliminate the influence from the surrounding reflections, the reader configuration, and the modulated data in §5. Second, the RF-DNA instances acquired on the spot is actually an 'imperfect' invariant of the one stored in the DNA database because it may be confused with DNA mutations due to the instantaneous interference, multiple-effect, or signal loss. As a result, the simple Euclidean distance based matching algorithm fails to compute the similarity of two RF-DNA instances. Therefore, a two-phase matching algorithm powered by deep neural network (DNN) was resorted to addressing the challenges in §6.

Contributions. We developed an automatic acquisition system and used it to acquire 160,000 RF-DNA instances from 1,600 COTS tags with ten different models. Our comprehensive evaluation reveals that RF-DNA can be used to classify tags based on their models with 98.4% accuracy and to identify individual tags with 95.98% accuracy. In summary, the following contributions are made: We first introduce the out-of-band backscatter response as a powerful hardware fingerprint for the physical-layer identification of RFID tags. Second, we develop a novel context-free profiling algorithm to acquire RF-DNA from tags in real-world environments. Third, we take advantage of deep neural networks to tackle the imperfections of RF-DNA caused by the acquisition settings and fully exploit the hidden information of RF-DNA. Finally, we successfully extend the capability of physical layer identification to tens of thousands of tags for the first time.

2 Related Work

Physical-layer identification or fingerprint has been investigated on several hardware platforms [7]. However, only a small percentage

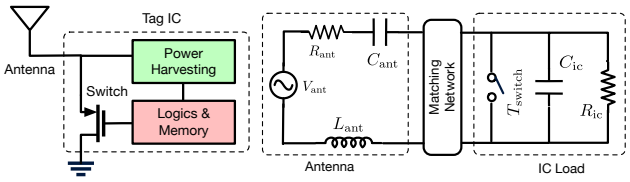
[1] A metaphor to the biological DNA in form.

of existing studies have explored the physical-layer identifications of RFID tags although they have been investigated for years [8–10, 16–22]. Related works have discovered various types of hardware imperfections as fingerprints: **(F1)** the time interval error (TIE) caused by the clock drift of tags relative to an ideal clock [8, 18], **(F2)** the extended TIE (ExTIE) defined as the correlation of two tags' RF preambles (equivalent to the correlation of two TIEs) [9], **(F3)** the average baseband power (ABP) defined as the average power of the baseband signal per cycle [8, 18], **(F4)** the minimum activating power (MAP) used to power up a tag at a distance [19], **(F5)** phase shift (Phase) caused by the diversity [10], **(F6)** the power spectrum density (PSD) defined as the power distribution in the frequency domain [9], and **(F7)** the persistence time (PT) defined as the discharging time of a tag takes after losing power [12]. We list the recent works in Table 1 for comparison. Different from F1-F7, a new fingerprint called RF-DNA is proposed herein. The differences lie in two main aspects. First, RF-DNA depends on the characteristics of both antenna and IC imperfections. By contrast, F7 is only on the IC imperfection. Second, past fingerprints were previously tested on a considerably small scale (50-2,000 tags). When being re-evaluated over a large-scaled testing set including 16,000 tags, their accuracy drops significantly, as indicated by our report in §8. Eingerprint seems attractive for its 77.8% accuracy. However, the information entropy for the Eingerprint is very limited and thus Eingerprint can only work with a small number of tags. In addition, taking persistence time as fingerprints is bound to be less time-efficient for tag running out of power. Unfortunately, its application takes nearly one minute to acquire from a single tag [12], which is thus more time-consuming than RF-based fingerprints adopted in practice. RF-DNA not only enlarges the information entropy of fingerprints for large-scale identification but also reduces the identification time. Regardless of the accuracy and efficiency, our solution shows distinct advantages.

Our work is also related to the frequency agnostic phenomenon of RFID tags [13, 14, 23]. RFind first reported this phenomenon and utilized it to improve the RFID localization [13]. Turbotrack [23] used wideband OFDM backscattering for high accurate robot localization. RFEats [24] further explored the food and liquid sensing applications by using such a wideband frequency response. TiFi uses this feature to achieve cross-frequency communication with Wi-Fi devices [14]. By contrast, we take advantage of this phenomenon to explore a new type of RFID fingerprint rather than localization or communication. Besides works in the RFID area, prior works are using out-of-band frequency response for authenticating other IoT devices [25, 26]. For example, [25] identifies the ZigBee devices by analyzing their out-of-band harmonic emission. However, since the harmonics is limited in band and can not fully explore the hardware differences, it can not achieve an acceptable accuracy in real-world environments. In comparison, RF-DNA's dual-frequency design can comprehensively analyze the frequency response differences and push the accuracy to an adequate level.

3 Background

In this section, we introduce the background of RFID and further explore the rationale behind RF-DNA.



(a) Tag Architecture (b) Equivalent circuit

Fig. 2: Internal Structure of an RFID Tag

3.1 Tag Architecture

A battery-free RFID tag consists of three key components, namely, an antenna, a matching network, and an integrated circuit (IC). The tag harvests the over-the-air continuous wave (CW) to power up the IC and modulates data by reflecting the incoming CW. The antenna and the IC are bridged by the matching network. Fig. 2(a) shows a simplified internal architecture of the tag, where the switch is controlled by the logic, resulting in two states.

- *Non-reflective*. When the switch is off, the incoming signal flows into IC, enabling the tag to harvest power. In this state, the tag is absorptive and non-reflective.
- *Reflective*. When the switch is on, the antenna is connected to the ground rather than to IC, enabling the tag to reflect the incoming signal, thus it is reflective.

A tag modulates the bit zero and bit one by switching in the above two states. As studied in [13], the matching between the IC and the antenna is not perfect in practice. The tag does not switch in the two states as perfectly reflective or perfectly absorptive. Instead, it might switch in intermediate states (i.e., more-reflective or less-reflective). The property results in the *frequency agnostic phenomenon* that the tag can backscatter not only at in-band frequencies but also at out-of-band frequencies.

3.2 Frequency Response Function

Each transistor acts as a frequency-dependent unique load due to its intrinsic imperfections [27], making two arbitrary tags distinguishable. There are more than 400,000 transistors in a tag's IC as reported in [28]. We treat them as a whole and stimulate them using a wireless exciting signal. Thus, hardware discrepancy among different tags can be exactly observed in the reflected signal. Mathematically, a tag can be simplified as an equivalent serial RLC circuit as shown in Fig. 2(b). The IC is reduced to a resistance connected in series with a capacitance. The antenna inductance L_{ant} and the IC capacitance L_{IC} together form a resonant circuit. Suppose the tag is stimulated with a single-tone signal at the frequency f. Then, the response Z is expressed as follows:

$$Z(f) = (R_{\text{ant}} + R_{\text{IC}}) + \mathbf{J}(2\pi f L_{\text{ant}} + \frac{1}{2\pi f C_{\text{IC}}}) \quad (1)$$

where $\mathbf{J}$ denotes the imaginary unit. Clearly, the resonant frequency is determined by the antenna inductance and IC resistance and capacitance, in which any tiny difference will cause a totally different response. As a result, a tag behaves as a *frequency response function* (FRF). Being challenged at a frequency f, FRF outputs an intrinsic response $Z(f)$. Next, let us analyze the characteristics of FRF in two bands.

In-band FRF. Each wireless communication system is designed to operate at predefined frequencies (aka *in-band frequencies*). The

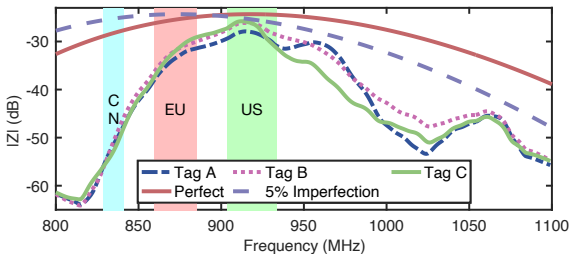


Fig. 3: Frequency Response Function. The operating spectrum assigned to RFID systems in China, Europe and USA are highlighted in blue, red and green respectively.

majority of UHF RFID standards adopt primarily three bands, 902-928 MHz (USA/China), 865-868 MHz (Europe) and 840-845 (China). The wireless terminals for the inter-communication must perform consistently to establish a wireless channel. The hardware imperfection may violate such consistency. To address this issue, all air protocols restrict severely the hardware discrepancy to vary within a small tolerable range. For example, Gen2 [11] specifies that the frequency variance of reflected signals from a tag must be less than ±10.62% Hz of the desired BLF. In consideration of this rule, tag manufactures must design a special matching circuitry to smooth the hardware discrepancy. Therefore, although the hardware imperfection is present at in-band frequencies, it is strictly under control. Hence, *the previously proposed fingerprints extracted at in-band frequencies (e.g., [8–10]) cannot distinguish a large number of tags.*

Out-of-band FRF. An ideal wireless system should not respond to any out-of-band request signal to avoid interference with other types of devices. Thus, out-of-band response should be suppressed severely inside wireless systems. However, many past works [13, 14] reported that a commercial RFID tag actually responds in a 10× wider bandwidth than the regulated band. The absence of out-of-band response suppression inside RFID tags is reasonable, because it not only saves cost (which is important for ten-cent devices) but also helps accommodate different regulations across countries and regions for world-wide logistics. Nevertheless, the matching circuitry for smoothing hardware discrepancy targets in-band frequencies only. Consequently, the FRF at out-of-band frequency is beyond the scope of regulation and thus more facilitate to fingerprint tags.

Verification. The discussion so far assumes that the hardware discrepancy is more evident at out-of-band frequencies than the in-band frequencies. To verify the above hypothesis, we measure the in-band and out-band FPF of three Impinj Monza 4 tags [29] in the same environmental setting. In the experiment, we transmit a single-tone CW at 926 MHz to query each tag. Simultaneously, a chirp signal is swept from 800MHz to 1100 MHz to acquire the FRF of the tag. The amplitude of the response (i.e., $|Z|$) was plotted in Fig. 3. The three primary bands were highlighted. It can be seen that the in-band response is more consistent than the out-of-band response. The datasheet suggests that the tag's IC impedance is $1000\Omega||2.48$pF and the best-fit antenna impedance at 915 MHz is $4.9||j70\Omega$ [29]. We substituted these parameters into Eqn. 1 and emulated the FRF with and without 10% variation in R_{IC}. The theoretical results also confirmed our hypothesis.

4 Overview

4.1 Problem Definition

We use the output of FRF $Z(f)$, i.e., the intrinsic response caused by the hardware imperfection, as our fingerprint. This complex number $Z(f)$ can be extended by the Euler's formula as follows:

$$Z(f) = a(f)e^{\mathbf{J}\theta(f)} = \underbrace{a(f)\cos(\theta(f))}_{\mathrm{I}(f)} + \mathbf{J}\underbrace{a(f)\sin(\theta(f))}_{\mathrm{Q}(f)} \quad (2)$$

where $a(f)$ is the amplitude and the $\theta(f)$ is the phase. The components of $\mathrm{I}(f)$ and $\mathrm{Q}(f)$ are the real and imaginary parts, respectively. We use these two *dual natural attributes* (DNA) as our hardware fingerprint.

Definition 1 (DNA). *A tag's DNA is a pair including the I and the Q components of the intrinsic response at the frequency f, namely, DNA(f)=Z(f)=(I(f),Q(f)).*

The DNA is represented at the frequency domain, hence irrelevant to time-varying parameters. By acquiring the DNAs in the entire responsive band including the in-band and out-of-band frequencies, a DNA chain can be obtained, called RF-DNA, which is defined as follows:

Definition 2 (RF-DNA). *An RF-DNA is a 1D single helical chain containing a million pairs of DNAs acquired across the frequency band in which the tag can respond.*

Fig. 1 shows the structure and some examples of RF-DNA.The cross-section of an RF-DNA is actually an I/Q constellation diagram, which shows the intrinsic response (i.e., DNA) of the tag at the frequency. RF-DNA is sometimes called a DNA chain for convenience. The size of a DNA chain is equal to 300 MHz divided by the *resolution*, which is defined as the sweeping step in a unit of Hz. For example, given a 1 Hz resolution, our DNA chain contains 300 million pairs of DNAs. Note that the chains plotted in Fig. 1 are undersampled to avoid oversized pdf. Let λ denote an RF-DNA. It is formally expressed as below:

$$\lambda = \{Z(f_1), Z(f_2), \cdots, Z(f_K)\} \quad (3)$$

where K is the size of an RF-DNA.

4.2 Solution

To fingerprint a tag, at a high level we go through the following two issues: **(1) DNA Profiling**: We firstly propose a context-free DNA profiling approach to separate RF-DNA from the backscatter signals as well as the environmental reflections in §5. **(2) DNA Matching**: Given a DNA database storing pre-acquired DNA sequences of all tags of interest, we introduce a two-phase matching algorithm to find out the tag from the database by its DNA sequence acquired on the spot in §6. Next, we elaborate the two issues in the subsequent sections.

5 DNA Profiling

In biology, DNA profiling (aka DNA fingerprinting) is a technique by which individuals can be identified and compared via their respective DNA profiles. Similarly, we introduce how to profile RF-DNA from individual tags in this section.

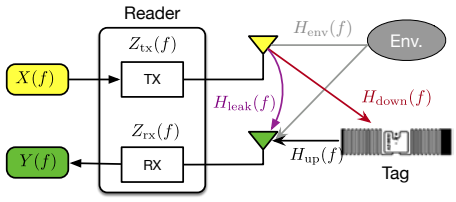


Fig. 4: Signal Model in an RFID system

5.1 Signal Model in an RFID System

Fig. 4 shows the signal model in an RFID system consisted of a reader and a tag. Specifically, the reader transmits a single-tone CW, denoted by $X(f)$, at the frequency f. Hence, this signal is reflected by the tag and finally received by the reader. The received signal is denoted by $Y(f)$. Since the tag has two states, namely, reflective and non-reflective states, the received signal also has two modalities as follows.

• **Modality 1 (Non-reflective):** The CW is not reflected by the tag when a bit zero is modulated. This modality of the received signal is denoted by $Y_0(f)$:

$$Y_0(f) = X(f)Z_{tx}(f)\left(H_{leak}(f) + H_{env}(f)\right)Z_{rx}(f) \tag{4}$$

Here, we use $Z(\cdot)$ and $H(\cdot)$ to denote an intrinsic response of a wireless component and a channel model, respectively. For example, $Z_{tx}(f)$ and $Z_{rx}(f)$ represent the intrinsic responses caused by the transmitter and the receiver of the reader. The H_{leak} represents the channel model of the leakage link propagated from the transmitter to the receiver directly. The CW is also reflected from surrounding obstacles such as the ceiling, walls, and so on. We model these reflections as a single combined signal and use a virtual channel model denoted by $H_{env}(f)$ to describe this link. Since the tag is in a non-reflective state, $Y_0(f)$ does not contain the intrinsic response of the tag.

• **Modality 2 (Reflective):** The CW is reflected by the tag when a bit one is modulated. This modality of the received signal is denoted by $Y_1(f)$:

$$\begin{aligned} Y_1(f) =& X(f)Z_{tx}(f)\left(H_{leak}(f) + H_{env}(f)\right)Z_{rx}(f) \\ &+ X(f)Z_{tx}(f)H_{up}(f)Z_{tag}(f)H_{down}(f)Z_{rx}(f) \\ =& Y_0(f) + X(f)Z_{tx}(f)H_{up}(f)Z_{tag}(f)H_{down}(f)Z_{rx}(f) \end{aligned} \tag{5}$$

where $H_{up}(f)$ and $H_{down}(f)$ represent the channel models of the uplink (transmitter → tag) and the downlink (tag → receiver), respectively. The $Z_{tag}(f)$ is the *intrinsic response* caused by the tag's hardware imperfection. Compared with the first modality, the received signal contains an additional term including intrinsic response that we are interested in. Suppose the environment keeps still in a short window, the received leaked signal and surrounding signal remain unchanged. The $Y_1(f)$ can be simplified by using $Y_0(f)$.

5.2 Context-free DNA Extraction

Clearly, the DNA is derived from $Z_{tag}(f)$ but the received backscatter signal is context-sensitive, namely, it contains other undesired variables dependent on the reader configuration and the environment. Thus, our task becomes to separate $Z_{tag}(f)$ from $Y_1(f)$. To do so, we propose a context-free extraction algorithm as follows:

First, we subtract the non-reflective signal from the reflective signal to eliminate the leaked signal and the environmental reflections as below:

$$Y_1(f) - Y_0(f) = X(f)Z_{tx}(f)H_{up}(f)Z_{tag}(f)H_{down}(f)Z_{rx}(f) \tag{6}$$

RFID protocols use Miller or FM0 encoding, which requires at least one transition during a bit. Thus, the two modalities must be present in a backscatter signal regardless of what data is backscattered from a tag

Second, we further eliminate $Z_{rx}(f)$ and $Z_{tx}(f)$ by dividing the above remainder by $Y_0(f)$ as shown below:

$$\begin{aligned} \xi(f) = \frac{Y_1(f) - Y_0(f)}{Y_0(f)} &= \frac{\cancel{X(f)Z_{tx}(f)Z_{rx}(f)}H_{up}(f)Z_{tag}(f)H_{down}(f)}{\cancel{X(f)Z_{tx}(f)Z_{rx}(f)}(H_{leak}(f) + H_{env}(f))} \\ &= \frac{H_{up}(f)H_{down}(f)}{H_{leak}(f) + H_{env}(f)}Z_{tag}(f) \end{aligned} \tag{7}$$

Clearly, the ratio removes $X(f)$ as well, making the final result irreverent to the CW. The ratio cannot still completely separate $Z_{tag}(f)$ due to the presence of the residual variables, i.e., $H_{up}(f)$, $H_{down}(f)$, $H_{leak}(f)$ and $H_{env}(f)$, which are only related to the propagation channels. Regarding these variables, we present a simple hypothesis as follows:

Hypothesis 1. *When $|f_i - f_j| \le \delta$ Hz, the channel models at frequencies of f_i and f_j are approximately identical if the environment remains unchanged.*

In summary, *the channel models are nearly identical for two wireless signals transmitted at very close-by frequencies under the same conditions.* Formally, when $|f_i - f_j| \le \delta$, $H_{up}(f_i) \approx H_{up}(f_j)$, $H_{down}(f_i) \approx H_{down}(f_j)$, $H_{leak}(f_i) \approx H_{leak}(f_j)$ and $H_{evn}(f_i) \approx H_{evn}(f_j)$. Suppose we acquire the backscatter signals at frequencies f_1 and f_2, then the phase difference caused by propagation over the same path equals $\Delta\theta = 2\pi d(f_1 - f_2)/c = 2\pi d\Delta f/c$ where c is the speed of light and d is the path length. To put this into perspective, if f_1 = 926 MHz, f_2 = 926.001 MHz and d = 5 m, then Δf = 1 kHz and $\Delta\theta$ = 0.0005 radians. Evidently, this phase difference resulted from the difference of carrier frequencies is ignorable compared with the phase shift caused by intrinsic response.

Finally, we can remove the path-related variables by dividing the two ratios at close-by frequencies as below:

$$\begin{aligned} \eta(f_k) = \frac{\xi(f_k)}{\xi(f_{k-1})} &= \frac{Y_1(f_k) - Y_0(f_k)}{Y_1(f_{k-1}) - Y_0(f_{k-1})} \cdot \frac{Y_0(f_{k-1})}{Y_0(f_k)} \\ &= \frac{\cancel{H_{up}(f_k)H_{down}(f_k)}}{\cancel{H_{leak}(f_k) + H_{env}(f_k)}} \cdot \frac{\cancel{H_{leak}(f_{k-1}) + H_{env}(f_{k-1})}}{\cancel{H_{up}(f_{k-1})H_{down}(f_{k-1})}} \cdot \frac{Z_{tag}(f_k)}{Z_{tag}(f_{k-1})} \\ &\approx \frac{Z_{tag}(f_k)}{Z_{tag}(f_{k-1})} \end{aligned} \tag{8}$$

Rather than the exact intrinsic response at a single frequency, the ratio $\eta(f_k)$ depicts the relation of the intrinsic responses at two adjacent frequencies. The $\eta(f_k)$ is free of the reader configuration and of the measurement environment, shortly, it is context-free. For instance, multi-path signals reflected by surrounding objects might have affected the performance as RF-DNA extracts hardware imperfections by analyzing the tag's wideband frequency response. However, multi-path cases should not have a significant impact on the system's accuracy with the aforementioned operation. This merit greatly facilitates the DNA measurement in practice. Thus,

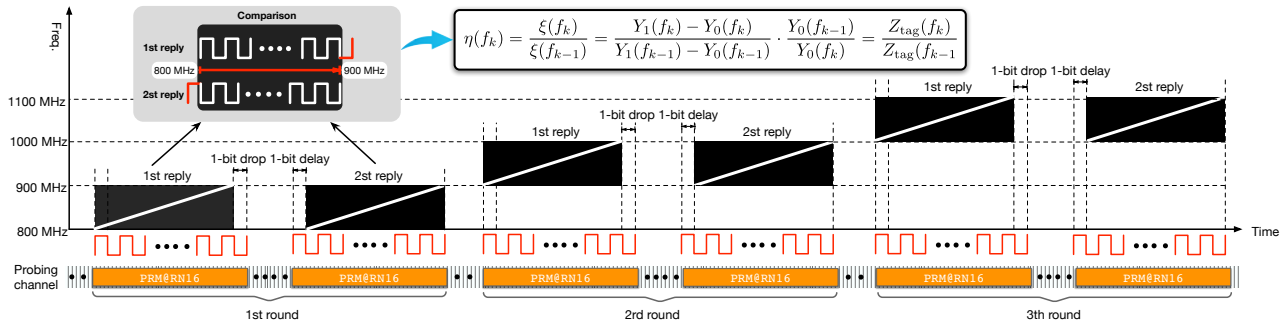


Fig. 5: Fast Batch DNA Extraction. The whole procedure requires a tag to repeat RN16 reply for six times and involves three rounds, each of which contains two replies. In each round, the reader repeats to sweep 100 MHz bandwidth twice exactly during the two reply window. However, the chirp is delayed by one bit later in the second reply compared with the first reply. In this way, two samples in the opposite states can be acquired as shown in the left-top corner.

we redefine DNA chain λ *using* $\eta(f_k)$ as follows:

$$\lambda = \{\eta(f_2), \eta(f_3), \eta(f_4), \cdots, \eta(f_K)\} = \{\frac{Z_{\text{tag}}(f_2)}{Z_{\text{tag}}(f_1)}, \frac{Z_{\text{tag}}(f_3)}{Z_{\text{tag}}(f_2)}, \frac{Z_{\text{tag}}(f_4)}{Z_{\text{tag}}(f_3)} \cdots, \frac{Z_{\text{tag}}(f_K)}{Z_{\text{tag}}(f_{K-1})}\} \quad (9)$$

Note that $\eta(f_1)$ is non-existent. Ideally, we prefer $\delta = 1$ Hz and acquire 300 million pairs of DNA. This resolution setting requires a higher reader configuration and leads to heavy computations in DNA matching. Our empirical study suggests setting $\delta < 1$ kHz (see more discussions in §8).

5.3 Single-Pair DNA Extraction

The next issue is *how could we extract a tag's DNA through the current air protocol?* A naive approach is to request the response of a tag with a desired frequency f and then separate $Y_0(f)$ and $Y_1(f)$ from the backscatter signal. However, the CW at out-of-band frequency might fail to power up the tag because the energy harvester of the tag is designed to work at in-band frequencies. To address the issue, a similar dual-channel solution is adopted as proposed in [13, 14]. Fig. 6 illustrates the acquisition procedure. Specifically, the reader transmits the Query related commands through the *query channel*, which operates at an in-band frequency f_q (e.g., 926 MHz). The query channel aims to power up the tag and trigger it to backscatter RN16 reply. Simultaneously, the reader transmits another single-tone CW through the *probing channel*. The probing channel is to acquire the tag's response at an arbitrary frequency f_k. In this way, the tag backscatters its RN16 reply at two frequencies simultaneously. After receiving an RN16 reply, the reader filters out two signals at the two frequencies, denoted by RN16@f_q and RN16@f_k. Then, the reader decodes the bits using RN16@f_q. Based on the decoding results, the reader can classify the samples from RN16@f_k into two clusters, namely, $Y_0(f_k)$ and $Y_1(f_k)$. Surely, EPC replies can be also used for this end; and collisions should be discarded.

5.4 Fast Batch DNA Extraction

Our ultimate goal is to obtain a sequence of DNA from 800 MHz to 1100 MHz. A 500 Hz resolution requires performing 300 MHz/500 Hz = 600,000 times DNA extractions from a single tag, which tends to cost a long time to acquire a complete DNA chain. To address this issue, we propose the chirp-based batch DNA extraction approach. Specifically, the reader transmits a chirp based CW in the probing

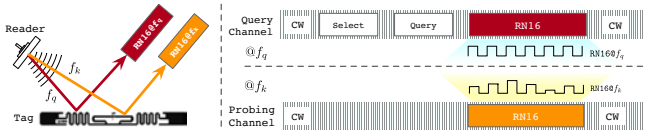


Fig. 6: Single-pair DNA extraction. Two channels, namely, query and probing channels exist. The query channel at in-band frequency f_q is to power up the tag and trigger it to backscatter RN16 reply. The probing channel aims to acquire the reply at the frequency f_k.

channel. If the chirp is swept from 800 MHz to 1100 MHz, each sample received by the reader through the probing channel is a response at a different frequency, allowing us to acquire a complete DNA chain within a single RN16 reply.

However, we face practical issues: first, constrained on the capabilities of our underlying RF daughter board, we are only allowed to sweep 100 MHz bandwidth at a time. Thus, we must launch three rounds to sweep the whole 300 MHz, that is, sweeping 800-900 MHz in the first round, 900-1000 MHz and 1000-1100 MHz in the second and third round. Second, each sample is a measurement of the response at a different frequency, thus either $Y_1(f)$ or $Y_0(f)$ but we need both to compute $\xi(f)$. To address this issue, we request the RN16 reply twice in each round. Unlike the first reply, the start of the chirp is postponed for one bit in the second reply. Fig. 5 illustrates the entire extraction procedure. The reader requests a tag to repeatedly backscatter its RN16 for six times through broadcasting Select plus Query commands in the query channel. The whole procedure is divided into three rounds. Each round contains two RN16 replies. In the 1st reply, the chirp is started from the first bit of the pilot-tone, which is a part of the preamble and composed of 136×2 alternatively appeared bit ones and bit zeros. In the 2nd reply, the chirp starts from the second bit, namely, the start of chirp is postponed for one bit in the 2nd reply than the 1st reply. As shown in the top-left corner, by comparing the two replies, we can acquire a pair of samples at the same frequency, which are in opposite states (i.e., $Y_1(f)$ and $Y_0(f)$), and then use them to compute $\xi(f)$.

Suppose the BLF is set to 40 kHz, each bit lasts 12.5 μs and the total length of the pilot-tone is $136 \times 2 \times 12.5 = 3.4$ ms, resulting in about $3.4 \times 6 + 100 = 120.4$ ms time cost totally (100 ms for other cost). When adopting 100 MHz IQ sampling rate, we can then acquire 3.4 ms × 100 MHz = 340,000 samples totally from the pilot-tone. Given a 100 MHz sweeping bandwidth, each two adjacent samples are spaced 100 MHz/340,000 ≈ 300 Hz. Assuming that

time cost remains the same for acquisition in a 500Hz-resolution condition mentioned at the beginning of this section, 600,000 times query processes cost $600000 * 2 * (0.0167 + 0.0034)/3600 \approx 6.7$ hours. Therefore, our approach can reduce the acquisition time from 6.7 hours to about 120.4 ms on extracting a complete DNA chain from a tag. Even if RFID scanners with poor frequency sweep function can not scan that fast, just like the USRP with an underperforming PC, collecting features with 10MHz is an acceptable choice cost only 1 second. In exchange, the size of an RF-DNA is shrunk to 300 MHz/300 Hz = 1 M.

6 DNA Matching

In this section, we discuss how we can use RF-DNA to find out a tag out of a DNA database that stores DNA sequences of tags of interest. This procedure is called DNA matching.

6.1 Preprocessing

Before diving into the details of matching algorithm, we should preprocess two practical issues.

6.1.1 Pre 1: Resolution Alignment

Given the limited sampling capability, the on-site reader may be incapable of acquiring the high-resolution RF-DNA as those stored in database, leading to the resolution misalignment. For example, given the following two DNA chains, which are stored in the database (denoted by λ_d) and acquired on the spot (denoted by λ_s) :

$$\begin{cases} \lambda_d = \{\eta_d(f_2), \eta_d(f_3), \eta_d(f_4), \eta_d(f_5), \eta_d(f_6) \dots\} \\ \lambda_s = \{\quad \times \quad, \eta_s(f_3), \quad \times \quad, \eta_s(f_5), \quad \times \quad, \dots\} \end{cases} \tag{10}$$

where $\times$ means the DNA loss at the non-sampled frequencies. Suppose the resolutions of λ_d and λ_s are 1 Hz and 2 Hz, respectively. Evidently, the two chains differ in size. We can simply resize λ_s by filling with zeros at the missing frequencies. Recall that DNA $\eta(f_k)$ is redefined as the relation of the intrinsic responses at two adjacent frequencies (see Eqn. 8), thus λ_d and λ_s are inconsistent in the calculation. To be more specific, $\eta_d(f_k)$ and $\eta_s(f_k)$ are defined as:

$$\eta_d(f_k) = \frac{Z_{\text{tag}}(f_k)}{Z_{\text{tag}}(f_{k-1})} \text{ and } \eta_s(f_k) = \frac{Z_{\text{tag}}(f_k)}{Z_{\text{tag}}(f_{k-2})} \tag{11}$$

Clearly, $\eta_d(f_k) \neq \eta_s(f_k)$ even if two DNA chains are acquired from the same tag because the denominators are different. Thus, before making the comparison, the resolution of a DNA chain stored in database should be downgraded to align with the on-site DNA chain. Generally, if the resolution of λ_d is m-fold than λ_s, we can downgrade the resolution of λ_d to align with λ_s as follows:

$$\begin{aligned} \eta'_d(f_k) &= \frac{Z_{\text{tag}}(f_k)}{Z_{\text{tag}}(f_{k-m})} = \frac{Z_{\text{tag}}(f_k)}{Z_{\text{tag}}(f_{k-1})} \cdot \frac{Z_{\text{tag}}(f_{k-1})}{Z_{\text{tag}}(f_{k-2})} \cdot \dots \cdot \frac{Z_{\text{tag}}(f_{k-m+1})}{Z_{\text{tag}}(f_{k-m})} \\ &= \eta_d(f_k) \cdot \eta_d(f_{k-1}) \cdot \dots \cdot \eta_d(f_{m+1}) \end{aligned} \tag{12}$$

where $\eta_d(f_k)$ and $\eta'_d(f_k)$ denote the original item and its downgraded version respectively. The downgrading is done by aggregating the original m adjacent items with multiplication. Replacing Eqn. 12 into Eqn. 10, we obtain two new DNA chains consistent in calculation and dimension for the subsequent matching:

$$\begin{cases} \lambda'_d = \{0, \eta_d(f_3)\eta_d(f_2), 0, \eta_d(f_5)\eta_d(f_4), 0, \eta_d(f_7)\eta_d(f_6), \dots\} \\ \lambda_s = \{0, \eta_s(f_3), \quad 0, \eta_s(f_5), \quad 0, \eta_s(f_7), \quad \dots\} \end{cases} \tag{13}$$

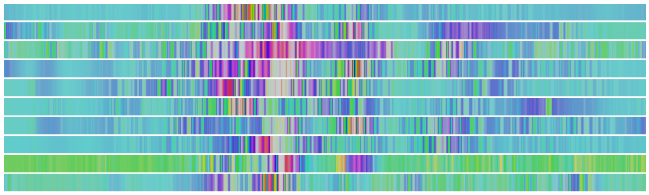


Fig. 7: DNA sequencing. The above ten stripes shows the DNA sequences of the ten tags shown in Fig. 1. Each stripe is repeated vertically for better visualization.

6.1.2 Pre 2: DNA Sequencing

To facilitate the DNA processing with DNN technique, which is well-established in processing images, we convert a DNA chain into a 1D image called *DNA sequence*. This preprocessing is correspondingly called *sequencing*. Formally, the value of the k^{th} pixel equals $\text{HSV}(|I(\eta(f_k))|, |Q(\eta(f_k))|, 1)$ where $\text{HSV}(\cdot)$ represents the color model. Fig. 7 shows the sequencing results of the ten DNA chains shown in Fig. 1. In terms of the features, a DNA chain and a DNA sequence are equivalent. To improve the network efficiency, we further divide a DNA sequence into 1000 segments uniformly and merge them into a 2D image with 1000×1000 pixels since the convolution neural network (CNN, a type of DNN) is much more efficient in processing 2D images.

6.2 DNA Matching with Neural Networks

The naive solution for DNA matching is to compare the similarity of RF-DNA between the candidate RF-DNA chosen from the database and the test RF-DNA acquired on the spot using the Euclidean distance. The RF-DNA stored in the database are acquired perfectly, but the on-site RF-DNA might be distorted, skewed or even partially ruined for three reasons. **(1) DNA Mutation**. Our context-free DNA extraction can eliminate the relatively long-term ambient interference but cannot defend against the instant interference that lasts less than one bit. In addition, the multipath effect might distort the DNA chains due to the superimposed propagation. Both cases will introduce some random DNA mutations (i.e., distorted DNA values). **(2) DNA Loss**. The reader sometimes suffers from acquisition failures due to the frequency-selective "black hole" on which the tag's backscatter signals cannot be received on account of the destructive superimposing, resulting in DNA losses at some frequencies. **(3) DNA Shifting**. This on-site reader is certainly not synchronized to the reader employed for building DNA database, which results in the carrier frequency offset and corresponding DNA shiftings between the candidate and test RF-DNA instances. Clearly, the traditional Euclidean distance based algorithm fails to deal with these complex situations.

Instead, we resort to DNN, which has shown significant power in object classification and similarity matching like face and signature recognition [30, 31]. Particularly, convolutional neural network (CNN, a classical DNN) is known for discovering the inherent and hidden features robust to the ambient interference, skews and distortions in images. Because of such task comparability, we mainly adopt CNNs for our problem. Specifically, we propose a two-phase matching algorithm, which takes the inter-family recognition task and then takes the intra-family recognition task in the two phases accordingly. The DNN architecture is shown in Fig. 8.

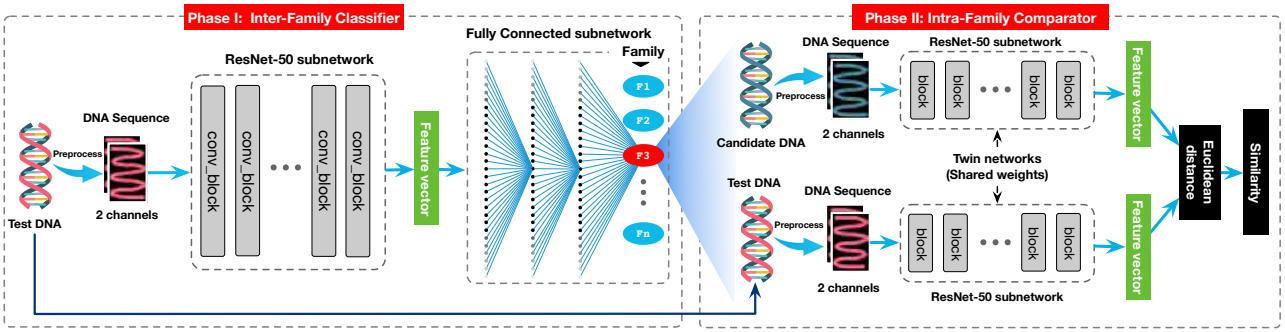
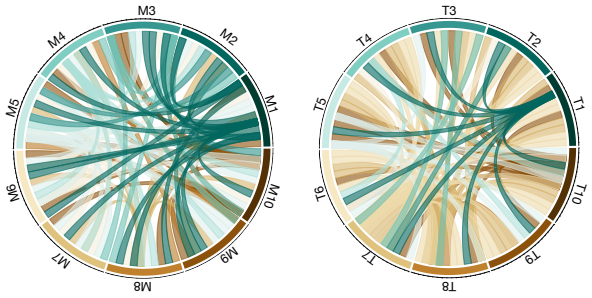


Fig. 8: Two-phase DNA Matching. In the first phase, we employ a ResNet-50 followed by an FCN to classify the test DNA sequence into a family. In the second phase, we adopt a siamese network to distinguish it from others in the classified family.



(a) Inter-family (b) Intra-family

Fig. 9: Genome mapping among inter-family and intra-family DNA chains. (a) shows the DNA chains of ten tags from different models; (b) shows the DNA chains of ten tags from the same model.

The intuition behind the two-phase design is from the comparison of genome mapping diagram shown in Fig. 9. Genome mapping diagrams are widely adopted in biology for exploring the similarity among different species. Here, we employ it to show the dissimilarity among different tags because we mean to distinguish two tags using their DNA chains. In a chord diagram, ten DNA chains are arranged in a circle where each chain is further uniformly divided into 30 segments called genomes. A line inside the circle connects the most dissimilar genomes between two DNA chains. The dissimilarity is computed as the farthest Euclidean distance of two genomes. Fig. 9(a) and Fig. 9(b) plots the connections of ten tags from different models and from the same model respectively. It is easy to find many dissimilarity connections in Fig. 9(a) but quite less connections in Fig. 9(b). This demonstrates that the task for family classification is relatively simple, but a fine-grained approach is expected to discriminate tags of the same models. Therefore, in the first phase, we use a CNN network to classify a tag into a model based family. In the second phase, we use a siamese network to discriminate two tags from the same family.

6.2.1 Phase I: Inter-Family Classification

In the first phase, we use a RestNet-50 network (a type of CNN) [32] followed by a three-layer fully connected network (FCN) to classify a DNA sequence into a model-based group called *family*, in which all tags are of the same model (e.g., ImpinJ ER62 and Alien 9962). The classification is inspired by the insight that tags of the same models are assembled using same components and fabricated by a same pipeline, thereby showing extremely similar fingerprints as children from the same family, which shows 90% above similarity in biological DNAs. The main purpose of the RestNet-50 is to extract a hidden and compressed feature with 2048 elements from a DNA sequence. The FCN is used to classify a tag into a family using the hidden feature. The network accepts the invariant of DNA sequence and outputs its family indicator. The whole network is optimized by minimizing the following cross entropy loss function:

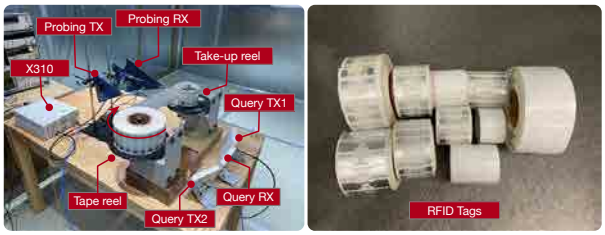
$$\arg\min_{\Theta} -\frac{1}{N}\sum_{\lambda\in\Delta}\sum_{c=1}^{M} B(\lambda,c)\cdot\log(h_1(\lambda,c;\Theta)) \tag{14}$$

where Δ is the training set and $|\Delta| = N$. The $B(\lambda, c)$ is a binary function where one and zero represent that λ is acquired from a tag of family c or not. The $h_1(\lambda, c; \Theta)$ denotes the network where Θ is the network parameters and the output is the probability that the λ is acquired from a tag of family c. The M is the number of families. For example, our dataset contains ten models of tags (Table 2) thus the network can classify a tag into one of the ten families (i.e., $M = 10$).

One may argue that why not train a network that can classify tags into single-tag groups such that the network can output a tag's ID directly? This solution is indeed used in some applications when the number of items is limited, because the network must be re-trained once a new item is added into the database. Clearly, we face thousands of and even millions of tags, so the solution is unscalable for us.

6.2.2 Phase II: Intra-Family Recognition

The second phase is to discriminate a tag from others in the same family. To this end, we adopt the popular neural network called *siamese network* which aims to compute the similarity of two inputs. A siamese neural network is a class of neural network architectures that contain two identical twin subnetworks, which share the same weights, but take distinct DNA sequences as inputs. The right of Fig. 8 shows the architecture of our Siamese neural network. Specifically, the two twin subnetworks are established using a shared ResNet-50. The parameters between the twin subnetworks are tied, which guarantees that *two extremely similar DNA sequences are mapped by each subnetwork to a close distance and different DNA are mapped to a far distance in feature space.* The Euclidean distance of the two features extracted from the two ResNet-50 subnetworks is computed as the similarity of the two input DNA sequences. Given a test DNA sequence, it is recognized as the candidate tag which has the highest similarity among all tags from the same family.



(a) ADAS (b) Tags

Fig. 10: Illustration of the experimental setup

We train a siamese network for each a single family. Suppose there are N tags in the current family, their DNA sequences are denoted by $\{\lambda_1, \lambda_2, \ldots, \lambda_N\}$. The whole network is optimized by minimizing the contrastive loss function $\mathcal{L}(\cdot)$ [33]:

$$\arg\min_{\Theta} \sum_{\lambda_i, \lambda_j \in \Delta} \mathcal{L}(h_2(\lambda_i, \lambda_j; \Theta), B(\lambda_i, \lambda_j)) \tag{15}$$

where Θ and Δ denotes the network parameters and the training set, respectively. The $h_2(\cdot)$ denotes the network, which computes the similarity of two inputs. The $B(\cdot)$ is a binary function where one and zero represent that the two DNA sequences are acquired from a same tag or not. Clearly, $N(N-1)/2$ pairs of negative samples can be obtained (i.e., their similarity is zero). Meanwhile, positive samples (i.e., their similarity is one) are created using the multiple RF-DNA instances acquired from the same tag. Some variants are generated by randomly deleting, changing, or shifting a few percent of DNAs (i.e., $1\% \sim 20\%$) to emulate practical challenges mentioned above. In our dataset, each family contains $1000 \sim 2000$ tags, resulting in up to one million pairs of training pairs. To deal with this issue, we randomly choose 100k pairs for the training. Since the Siamese network uses the concept of one-shot learning and takes pairs as input for training [34], the amount of data required for training is much smaller than traditional convolutional neural networks for classification tasks.

7 Implementation

We implemented an automatic DNA acquisition system (ADAS) and collected RF-DNA instances from a total of 16,000 COTS tags. The experimental settings and the data collection details are described below:

• **DNA Acquisition**. Fig. 10(a) shows the ADAS deployed in our lab room. The tags are rolled up in a tape reel and moved to a take-up reel. We used a microchip to control the rolling of the tape reel. In each time, about ten tags are fully scanned by antennas between two reels. As mentioned earlier, two channels exist, namely, the probing and query channels. The probing channel is built with an Ettus USRP (i.e., X310) and a pair of log-periodic antennas, which are used to transmit and receive chirp signals respectively.[2] The query channel is built with another USRP and three directional antennas, among which two antennas are to transmit the single-tone CW at 926 MHz and the remaining antenna is to receive the backscatter signal. To be compliant with the RF power regulation [37], the transmitting power of the query channel is 30 dBm, and that of the probing channel is -15 dBm. One of the two transmitting antennas in query channel acts a backup in case that the tag is failed to be powered up from one angle. To avoid tag collision, the proposed fast batch DNA extraction uses the select command to assign only one tag for one collection slot. Only the tags between two reels are selected to reply `RN16`. The collecting time is linearly proportional to the scale of tags. *One might wonder if tags suffer from the coupling effect in such dense deployment condition.* The answer is affirmative. However, it does not affect our measurement. The coupling effect causes the backscatter signal to be multiplied by a coefficient. As indicated in Eqn. 8, this common coefficient can be eliminated from the division. Thus, our context-free DNA profiling approach is also free of coupling effect.

• **Dataset**. We successfully collect RF-DNAs from 16,000 COTS tags using the customized ADAS. To balance the number of tags from different manufacturers, the total number of Alien and NXP tags remains 5000. In addition, 1000 and 2000 are of the same order of magnitude and we believe this scale of datasets could closely or even equally evaluate the performance for a specific model. The pictures of the tags are shown in Fig. 10(b) and the detailed information is listed in Table 2. These tags are the most common COTS tags on the market that we can buy. Briefly, the dataset covers six different IC models from the three manufacturers and ten different antenna designs. Their size varies from 70×15 *mm* to 73.5×20.2 *mm*. We collected about 10 TB raw I/Q data with 10 M/s sampling rate. To test the robustness of RF-DNA, we acquired 10 RF-DNA instances from each tag in ten different environment settings. Thus, 160,000 instances were acquired from the 16,000 tags, among which 80% instances are used for the DNN training and the remaining 20% are for the testing. This dataset will be released in our website as open dataset.

• **Deep Learning**. We use PyTorch framework to develop the CNN and run it on a machine with an AMD 5900x (4.9 GHz) processor, 64 GB RAM and NVIDIA 2080Ti GPU. We adopt the top-performing CNN model in computer vision called ResNet-50. The detailed configuration can be found in [32]. The Stochastic Gradient Descent (SGD) optimizer with learning rate of 10^{-5}. The training well converges after 500 training epochs. The processing time of each DNA sequence is 0.006 s. The networks for inter-family classification are trained about 24 hours. Each siamese network is trained for about 20 hours in our settings. To further save the training time, one can use more GPU cards to train in parallel or use some pre-training policies to reduce the total training time when training the model for new cases.

Table 2: Collected Tags

#	MFR.	IC	Model	Size(mm^2) .	AMT.
M1		Monza 4QT	H47	50×50	2000
M2	Impinj	Monza R6	ER62	74×18	2000
M3		Monza R6	AZ-H63	49×114	2000
M4		Higgs 3	9662	70×17	1000
M5	Alien	Higgs 3	9640	94.8×8.25	2000
M6		Higgs 3	9654	93×19	1000
M7		Higgs 9	9962	73.5×20.2	1000
M8		Ucode8	U9627	96×27	2000
M9	NXP	UR108	U7015	70×15	2000
M10		Ucode7	U5030	50×30	1000

[2]For convenience, we use the USRP to implement the prototype of RF-DNA in our lab. While, both probing and query channels can be implemented with customized RF devices at a low cost. For example, a commercial RFID reader for query channel only costs 300 USD [35] and an RF sweep signal source generator for probing channel only costs 150 USD [36].

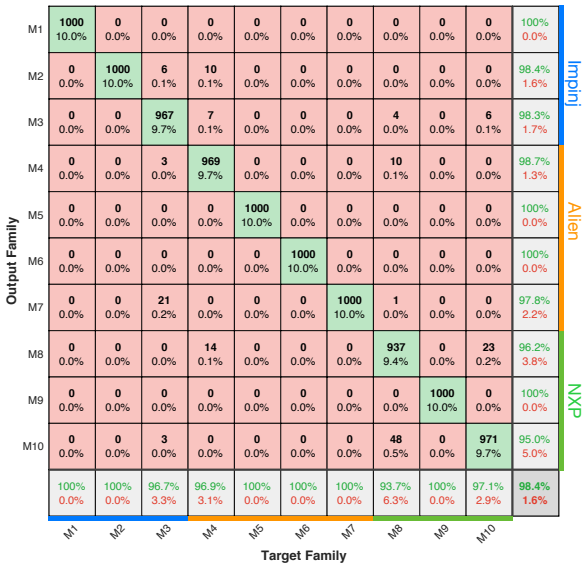


Fig. 11: Confusion Matrix of Inter-family Classification

8 Evaluation

In this section, we firstly demonstrate the matching accuracy of physical-layer identification using RF-DNA, which is evaluated in terms of inter-family classification (Phase I), inter-family recognition (Phase II) and overall identity verification (Phase I+Phase II), respectively. Then, we discuss the performance of the context-free profiling.

8.1 Inter-Family Classification Accuracy

Firstly, we seek to determine whether our fingerprints can be used to correctly classify a group of tags with the same model into a class called family (i.e., performance of Phase I). For this objective, we randomly pick up 1,000 RF-DNA instances per family from the test set. A total of 10,000 tags are input into the trained inter-family classifier (see Fig. 8). The resulting confusion matrix is plotted in Fig. 11. In the figure, the rows correspond to the predicted class (output family) and the columns correspond to the true class (Target family). The diagonal cells are the correctly classified results, while the off-diagonal cells are the incorrectly classified results. From the confusion matrix, we derive the following findings: **(1)** the column on the far right of the matrix shows the precision and false discovery rate (FDR), respectively. The precision (or FDR) is defined as the percentage of all the results predicted for each family that is correctly (or incorrectly) classified. We achieve 100% precision for the four families (M1, M5, M6, and M9). The lowest precision of 95% is observed for M10 because 48 tags from M8 are incorrectly predicated to be from M10. This relatively low precision results from the fact that both M8 and M10 tags are fabricated by NXP and they adopt a similar hardware configuration and antenna design. Nevertheless, the overall mean precision reaches up to 98.4%. **(2)** the row at the bottom of the matrix shows the true positive rate (TPR, i.e., recall) and false negative rate (FNR), respectively. TPR (or FNR) refers to the percentage of all results belonging to each family that is correctly (or incorrectly) classified. We achieve 100% recall for six families (M1-2, M5-7, M9). That is, 6,000 tags are correctly classified into their own families. The minimal recall (i.e., 93.7%) also occurs for M8 because of the 48 false negatives of M8. The recalls are above 96% in the other cases. **(3)** the precision values increase to 98.9%, 99.13%, and 97.07% if the classification is based on manufacturers (i.e., Impinj, Alien, and NXP). This finding suggests that the tags fabricated by different manufacturers are actually more distinguishable than their models.

8.2 Intra-Family Recognition Accuracy

Next, we evaluate the individual recognition accuracy inside a family (i.e., performance of Phase II) by temporarily ignoring the impact of the inter-family classification accuracy temporarily . To this end, we randomly choose 100 RF-DNA instances from each family. For each tag, we use its family's siamese network to determine the candidate tag whose RF-DNA has the highest and above-threshold similarity to the input RF-DNA. The result is positive if the tag is correctly found out; otherwise, it is negative. For each in-family test, we repeat 100 trials and report the TPR (i.e., percentage of positives). The accuracy results as a function of family are plotted in Fig. 12. In sum, we can achieve an overall TPR of 95.98% with an std of 1% across the 10 families; such TPR is nearly the same TPR as that of inter-family classification (i.e., 96%). As the Siamese network finds out the target out of a candidate set, its accuracy should be influenced by the set size to a certain extent. In the figure, the families including 2,000 tags (or 1,000 tags) are highlighted in dark blue (or dark red). We can clearly observe $1\% - 3\%$ higher TPRs in the small-sized families than in the large-sized ones. The mean TPRs by manufacturer are 95.09%, 96.64% and 95.96%, and they do not show any notable difference. In summary, discriminating an individual tag from a set of tags by using RF-DNA is a completely reliable approach.

8.3 Overall Matching Accuracy

Next, we evaluate the overall matching accuracy of our approach (i.e., performance of Phase I + Phase II). In the experiment, we randomly choose 20,000 RF-DNA instances without knowing their family and then use the two-phase matching algorithm to identify them out of 16,000 tags. The accuracy is reported using the TPR. Fig. 14 shows the comparison of the results of our approach and those of state-of-the-art methods. Specifically, the grouping TPR indicates the accuracy of grouping tags based on their models. The overall TPR refers to the accuracy of identifying an individual tag out of all tags. From the figure, we obtain the following findings:

• **State-of-the-art approaches**: (1) ETH: This fingerprinting approach was introduced by the researchers from ETH [8], which proposed to use the PSD plus TIE as a combined fingerprint, as elaborated in §2. They studied the performance of this combined fingerprint across 200 tags and reported a mean TPR of 98.7%. However, we would find that its accuracy sharply drops to 26.08% across 16,000 tags. *This result is perfectly aligned with the average tolerance range of* 21.24% *defined in the Gen2 protocol* [11]. Thus, ETH is not a good solution when dealing with more than thousands of tags. (2) GenePrint: This approach uses the correlation between two tags' `RN16` preambles as the fingerprint [9]. The correlation difference is caused by the TIE, and thus, the approach is essentially a fingerprint extended from TIE. GenePrint offers 30% accuracy improvement to ETH regarding the overall accuracy. (3) TagPrint: This approach

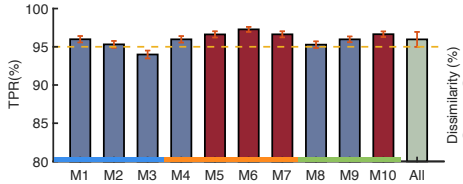


Fig. 12: Intra-family Recognition

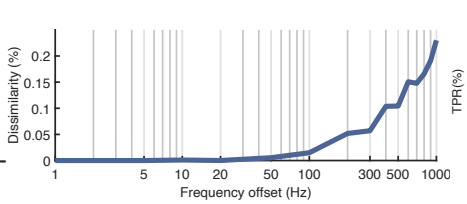


Fig. 13: Impact of Resolution

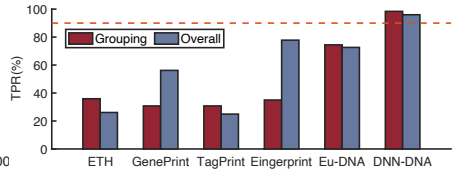


Fig. 14: Overall Classification

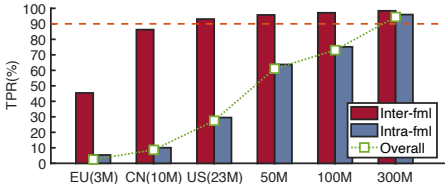


Fig. 15: Impact of Bandwidth

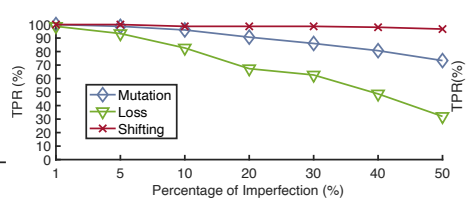


Fig. 16: Impact of Imperfection

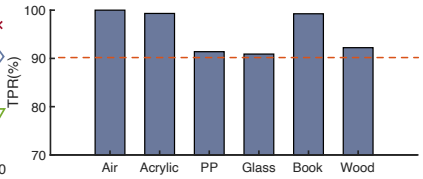


Fig. 17: Impact of Substrate

uses the phase diversity as a fingerprint [10], which is a half feature of our DNA. Our fingerprint not only considers the power but also the phase. TagPrint achieves 30.77% and 24.93% TPR in the two cases. (4) Eingerprint: Unlike other RF based fingerprints, this approach uses the uniqueness in discharging of IC as a fingerprint [12]. The work can achieve 77.8% TPR in identifying an individual tag, but is less able to group tags based on models (i.e., 35% TPR). The performance of Eingerprint seems attractive. Unfortunately, it requires to take about one minute to collect the fingerprint from every single tag. Such efficiency is nearly unacceptable in practice.

• **RF-DNA**: Finally, we report the accuracy of our fingerprint. (1) Eu-DNA. For comparison, we also use the Euclidean distance to compare the similarity of two RF-DNAs without the help of DNN. Specifically, we firstly use k-means to compute the center of ten clusters and the tag is grouped into the nearest cluster. Then the tag is found out by comparing the input RF-DNA with all candidate tags' RF-DNAs. As a result, this approach can achieve 77.44% and 72.61% accuracy in the two tasks. It outperforms the first three types of fingerprints by 46.53%, 16.43% and 47.68% respectively in terms of the overall accuracy. (2) DNN-DNA. After introducing DNN to the matching problem, the accuracy are further improved to 98.4% and 95.98% for two tasks respectively, which increases 21% and 23% on the basis of Eu-DNA thanks to the recent advances of DNN. In summary, regardless of the grouping task or individual recognition task, DNN-DNA demonstrates the great advantage in the accuracy and efficiency than the previously proposed fingerprints. Such merits mainly attribute to the out-of-band response features and the power AI in classfication task.

8.4 Impact of the Resolution

We formulate a hypothesis about resolution in DNA profiling. To verify this hypothesis, we compare the dissimilarities of the RF-DNAs acquired with different resolutions. Specifically, we first acquire the highest-resolution (i.e., 1 Hz) RF-DNA as a baseline denoted by λ_1, and then acquire the other-resolution RF-DNA denoted by λ_m, where m is the resolution. During the experiment, the environment remains unchanged. The dissimilarity is defined as $|(\lambda_m - \lambda_1)/\lambda_1|$, which suggests the percentage of λ_m that is different from λ_1. When computing the similarity, the resolution of λ_1 must be downgraded based on Eqn. 12. The dissimilarity is plotted in Fig. 13. As desired, the dissimilarity is lower than 0.2% even if the resolution is increased to 1 kHz. The result verifies the hypothesis.

8.5 Impact of Bandwidth

We emphasize that the uniqueness of RF-DNA mainly lies in the intrinsic responses at out-of-band frequencies. Thus, we aim to test the impact of bandwidth. To do so, we test the accuracy as a function of bandwidth in terms of the inter-family classification and intra-family recognition tasks. We collect the RF-DNA instances in the four sub-bands: EU (865–868 MHz), CN (840–845 MHz, 920–925 MHz), US (902–928 MHz), 875–925 MHz (50 M), and 860–960 MHz (100 M). The first three bands are adopted by Europe, China, and the US while the last two cover the bands regulated in other countries and regions. The results are plotted in Fig. 15. As desired, the accuracy is clearly increased as the bandwidth increases because many DNA features are expressed in a wider bandwidth. Interestingly, 23 M bandwidth is sufficient to achieve at least 93.07% TPR in the inter-family classification task. This result reconfirms our observation (see Fig. 9) that the family feature is much more evident than the individual feature. The overall accuracy is limited to 75% if only in-band DNA pairs are employed. In other words, the 250 M out-of-band feature can offer nearly 20% contributions to the overall accuracy. This result demonstrates again that the out-of-band fingerprints better depict individual tags than the in-band fingerprints.

8.6 Tolerance on DNA Imperfections

Finally, we evaluate the tolerance of our matching algorithm to DNA imperfections, including mutations, loss, and shifting. We randomly change and delete 1% $\sim$ 50% DNA pairs. Considering the common ±2.5 ppm clock drift and 1 GHz carrier frequency, we can observe a maximum of 2.5 kHz shifting in a DNA chain. Thus, we circularly shift RF-DNA by 1 $\sim$ 50% $\times$ 2.5 kHz. We plot the accuracy as a function of the percentage of DNA imperfection in Fig. 16. DNN has strong tolerance in the case of shifting. However, it can only tolerate 20% and 5% mutations and loss to maintain an accuracy of over 90%. This feature is because the DNA loss is equivalent to decreasing the acquisition bandwidth.

8.7 Impact of Substrate

In real-life scenarios, tags will be attached to objects and backing materials will alter the tag's impedance by coupling with it. In this experiment, we evaluate the impact of the substrate. Five common items are chosen, including acrylic, polypropylene (PP), glass cup, book and a wood board. For each case, 50 objects attached with tags are tested. Fig.17 shows the results where tags in default settings attached to paper tape is denoted as 'Air'. TPRs for each substrate are 100%, 99.32%, 91.39%, 90.9%, 99.25%, 92.22%, and the standard deviation is 4.42%. The identification accuracy for PP, glass and wood is lower than the others. This is mainly because the dielectric constant permittivity of these materials is higher than the others [38–40] and they have a greater coupling effect on tag's frequency response.

8.8 Impact of Context Settings

Next, we discuss the impact of the acquisition context settings including the tag orientation, distance, reader configuration, sampling rate, the multiple-path effect and the long-term persistence. To this end, we list nine different context combinations, i.e., C0-C9, in Fig 18. Taking C0 as a default setting, other combinations reveal possible impacts for different factors. For each setting, we randomly choose 50 tags to obtain their RF-DNA instances. Then, we compute the mean overall accuracy indicated by the TPR using the trained matching networks. We have the following finds:

Distance: C0-C3 shows the effects of distance. As we discussed before, the probing channel transmitting power is far below the query channel. Due to the USRP's poor noise control, the SNR of the received probing signal beyond 0.5 m is lower than the requirements of the accurate frequency response acquisition. Hence, we only test our system in a range of up to 0.5 m. As shown in Fig. 18, an apparent drop could be easily observed between C1 (TPR 100%), C2 (TPR 90.4%) and C3 (TPR 87.2%). This indicates that the ultra wideband hardware fingerprint is sensitive to SNR. To enlarge the operating range, one can boost the received SNR by using an external low-noise amplifier (LNA) on the receiver channel [24].

Orientation: C0, C4 and C5 are groups set up for the effect of the orientation of tag, including vertical, horizontal and one in between (45°). TPRs for three cases are 100%, 99.6% and 91.0%. In theory, our approach is orientation-insensitive. This is because the impact of the orientation can be modeled as a frequency independent coefficient on the whole fingerprint, which can also be eliminated from Eqn. 8. The loss of accuracy for different orientations in experiments is mainly due to the attenuation of signal strength. Here we use the Impinj H47 tags with the dual linear polarized antenna, which has poor gain in the 45° direction. Therefore, the TPR in this direction is lower than the others.

Equipment: C6 changes reader B from reader A in C0 as the receiver equipment to evaluate the effect of frequency response in different devices. Performance of this setting verifies the performance of step denoted as Equ.7 that remove $Z_t x$ and $Z_r x$ caused by transmission devices. TPR equals 98.1% which shows an acceptable decline.

Sampling rate: For a USRP reader, a higher sample rate means wider one-shot sweeping bandwidth and can effectively increase the acquisition speed. To evaluate how the sample rate impacts the identification accuracy, we increase the sampling rate to the maximum, 25 MS/s. While, compared with 10 MS/s, the TPR for 25 MS/s drops 5.4%. This is because higher frequency bandwidth also brings in a higher level of background noise. One shall balance the acquisition speed and the accuracy by adjusting the sampling rate in practical application.

#	Orient.	Dist.	RX	SR.	MP.	LT.	Accuracy
C0	↑	0.1m	A	10M	N	N	100%
C1	↑	0.2m	A	10M	N	N	100%
C2	↑	0.3m	A	10M	N	N	90.4%
C3	↑	0.5m	A	10M	N	N	87.2%
C4	↗	0.1m	A	10M	N	N	91.0%
C5	→	0.1m	A	10M	N	N	99.6%
C6	↑	0.1m	B	10M	N	N	98.1%
C7	↑	0.1m	A	25M	N	N	94.6%
C8	↑	0.1m	A	10M	Y	N	96.0%
C9	↑	0.1m	A	10M	N	Y	100%

Fig. 18: Impact of Context

Multipath: Multipath effect makes the background frequency response complicated and might interfere with the DNA acquisition. To evaluate how well our system resists the multipath, we create a multipath environment by adding two reflecting metal objects around the tags. TPR in this setting is 96%, which indicates our context-free extraction can effectively eliminate the environment scattering.

Persistence: Sampling time of configuration C9 is 24 hours after sampling data of C0 to verify time persistence. Without changing the environment and RFID tag itself, frequency response should be consistent. TPR remains 100% to support the point.

In short, the mean TPR for all nine different settings is 95.69% and the standard deviation is 4.71% apart from C2 and C3. This shows that our DNA profiling is indeed context-free and robust. While, the working distance is limited in the current hardware setting, which still requires further improvement.

9 Conclusion

The study on RF-DNA creates a new perspective on the backscatter device security through the exploration of abundant out-of-band RF hardware information. This work first attempts to build a clear and informative genetic map for an RFID tag with a low-cost wireless measurement. By mining the vast amount of information contained in the genetic map, we demonstrate that RF-DNA can support the accurate physical-layer identification of over 10,000 tags. We believe that RF-DNA will inspire plenty of new applications in wireless ecosystems. RF-DNA also leaves room for further investigations, including enlarging the working range and increasing the training efficiency.

Acknowledgments

This study is supported in NSFC Excellent Young Scientists Fund (Hong Kong and Macau) (No. 62022003), NSFC General Program (No. 61972331), UGC/GRF (No. 15204820), UGC/GRF (No. 15215421), NSFC Key Program (No. 61932017), and National Key R&D Program of China 2019YFB2103000. We thank all the anonymous reviewers and the shepherd, for their valuable comments and helpful suggestions.

References

[1] "RFID Forecasts, Players and Opportunities 2019-2029," https://www.idtechex.com/en/research-report/rfid-forecasts-players-and-opportunities-2019-2029/700, accessed on 2021-7-10.

[2] G. Wang, H. Cai, C. Qian, J. Han, S. Shi, X. Li, H. Ding, W. Xi, and J. Zhao, "Hufu: Replay-resilient rfid authentication," *IEEE/ACM Transactions on Networking*, vol. 28, no. 2, pp. 547–560, 2020.

[3] H.-Y. Chien, "Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity," *IEEE transactions on dependable and secure computing*, vol. 4, no. 4, pp. 337–340, 2007.

[4] B. Song and C. J. Mitchell, "Rfid authentication protocol for low-cost tags," in *Proc. of ACM WiSec*, 2008, pp. 140–147.

[5] A. Juels, R. Pappu, and B. Parno, "Unidirectional key distribution across time and space with applications to rfid security." in *Proc. of USENIX security symposium*, 2008, pp. 75–90.

[6] M. Terrovitis and N. Mamoulis, "Privacy preservation in the publication of trajectories," in *Proc. of IEEE MDM*. IEEE, 2008, pp. 65–72.

[7] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, pp. 1–29, 2012.

[8] D. Zanetti, B. Danev, and S. sapkun, "Physical-layer identification of uhf rfid tags," in *Proc. of ACM MobiCom*, 2010, pp. 353–364.

[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, 2015.

[10] L. Yang, P. Peng, F. Dang, C. Wang, X.-Y. Li, and Y. Liu, "Anti-counterfeiting via federated rfid tags' fingerprints and geometric relationships," in *Proc. of IEEE INFOCOM*. IEEE, 2015, pp. 1966–1974.

[11] "EPC Gen2, EPCglobal." 2021, accessed on 2021-5-18. [Online]. Available: www.gs1.org/epcglobal

[12] X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Eingerprint: Robust energy-related fingerprinting for passive rfid tags," in *Proc. of USENIX NSDI*, 2020, pp. 1101–1113.

[13] Y. Ma, N. Selby, and F. Adib, "Minding the billions: Ultra-wideband localization for deployed rfid tags," in *Proc. of ACM MobiCom*, 2017.

[14] Z. An, Q. Lin, and L. Yang, "Cross-frequency communication: Near-field identification of uhf rfids with wifi!" in *Proc. of ACM MobiCom*, 2018, pp. 623–638.

[15] Global Frequencies Regulations for RFID. https://tagitsolutions.com/knowledge-base/global-frequency-regulations-for-rfid/.

[16] B. Danev, S. Capkun, R. Jayaram Masti, and T. S. Benjamin, "Towards practical identification of hf rfid devices," *ACM transactions on Information and System Security (TISSEC)*, vol. 15, no. 2, pp. 1–24, 2012.

[17] J. Han, C. Qian, Y. Yang, G. Wang, H. Ding, X. Li, and K. Ren, "Butterfly: Environment-independent physical-layer authentication for passive rfid," *Proc. of ACM on IMWUT*, vol. 2, no. 4, pp. 1–21, 2018.

[18] D. Zanetti, P. Sachs, and S. Capkun, "On the practicality of uhf rfid fingerprinting: How real is the rfid tracking problem?" in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2011, pp. 97–116.

[19] S. C. G. Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting rfid tags," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 938–943, 2010.

[20] G. Wang, C. Qian, H. Cai, J. Han, H. Ding, and J. Zhao, "Replay-resilient physical-layer authentication for battery-free iot devices," in *Proc. of ACM HotWireless*, 2017, pp. 7–11.

[21] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. of ACM WiSec*, 2010, pp. 89–98.

[22] G. Wang, H. Cai, C. Qian, J. Han, X. Li, H. Ding, and J. Zhao, "Towards replay-resilient rfid authentication," in *Proc. of ACM MobiCom*, 2018, pp. 385–399.

[23] Z. Luo, Q. Zhang, Y. Ma, M. Singh, and F. Adib, "3d backscatter localization for fine-grained robotics," in *Proc. of USENIX NSDI*, 2019, pp. 765–782.

[24] U. Ha, J. Leng, A. Khaddaj, and F. Adib, "Food and liquid sensing in practical environments using rfids," in *Proc. of USENIX NSDI*, 2020, pp. 1083–1100.

[25] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2091–2106, 2016.

[26] A. Elmaghbub, B. Hamdaoui, and A. Natarajan, "Widescan: Exploiting out-of-band distortion for device classification using deep learning," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[27] T. Björninen, L. Sydänheimo, and L. Ukkonen, "Development and validation of an equivalent circuit model for uhf rfid ic based on wireless tag measurements," in *Proc. of AMTA Symp*, vol. 6, 2012, pp. 21–26.

[28] "Deep Construction of RFID Tags." https://rfid4u.com/dig-deep-construction-of-rfid-tags/, accessed on 2021-05-13.

[29] "Impinj Monza 4 Datasheet," https://support.impinj.com/hc/en-us/articles/202756908-Monza-4-Datasheet, accessed on 2021-7-2.

[30] I. Masi, Y. Wu, T. Hassner, and P. Natarajan, "Deep face recognition: A survey," in *Proc. of SBC SIBGRAPI*. IEEE, 2018, pp. 471–478.

[31] B. Ribeiro, I. Gonçalves, S. Santos, and A. Kovacec, "Deep learning networks for off-line handwritten signature recognition," in *Iberoamerican Congress on Pattern Recognition*. Springer, 2011, pp. 523–532.

[32] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. of IEEE CVPR*, 2016, pp. 770–778.

[33] R. Hadsell, S. Chopra, and Y. LeCun, "Dimensionality reduction by learning an invariant mapping," in *Proc. Of IEEE CVPR*, vol. 2. IEEE, 2006, pp. 1735–1742.

[34] L. Fei-Fei, R. Fergus, and P. Perona, "One-shot learning of object categories," *IEEE transactions on pattern analysis and machine intelligence*, vol. 28, no. 4, pp. 594–611, 2006.

[35] "Keonn advanreader-10 usb rfid reader (1-port) (fcc) [clearance]," accessed on 2022-1-2. [Online]. Available: https://www.atlasrfidstore.com/keonn-advanreader-10-usb-rfid-reader-1-port-fcc-clearance/

[36] "Analog devices inc. eval-adf4351eb1z," accessed on 2022-1-3. [Online]. Available: https://www.digikey.hk/products/zh?keywords=Analog%20Devices%20Inc.%20EVAL-ADF4351EB1Z

[37] F. C. Commission *et al.*, "Understanding the fcc regulations for low-power, non-licensed transmitters," *Office of Engineering and Technology*, vol. 34, 1993.

[38] "Relative permittivity - wikipedia 2022," 2022, accessed on 2022-1-3. [Online]. Available: https://en.wikipedia.org/wiki/Relative_permittivity

[39] P. Thomas, R. E. Ravindran, and K. Varma, "Dielectric properties of poly(methyl methacrylate) (pmma)/cacu3ti4o12 composites," in *2012 IEEE 10th International Conference on the Properties and Applications of Dielectric Materials*, 2012, pp. 1–4.

[40] W. James, "Dielectric properties of wood and hardboard: variation with frequency, moisture content and grain orientation," *USDA for Serv. Res. Pap. FPL-245, Madison, WI*, 1975.