RF-Rock: Intermodulation-based RFID Unauthorized Identification Attack without Tag Activation

Chen Gong[ℙ], Bo Liang[ℙ], Purui Wang[𝕄], Xiaoyu Ji[ℤ], Yin Chen[ℝ], Chenren Xu[ℙ𝕂✉*]
[ℙ]School of Computer Science, Peking University [𝕄]Massachusetts Institute of Technology [ℤ]Zhejiang University
[ℝ]Reitaku University [𝕂]Key Laboratory of High Confidence Software Technologies, Ministry of Education (PKU)

ABSTRACT

Following the broad prospect of Radio Frequency Identification (RFID) technology is the security concern of unauthorized tag identification, which poses threats to the privacy of both objects and users. In this paper, we propose RF-Rock, the first RFID unauthorized identification attack that operates without tag activation, thereby evading almost all existing defenses. This attack exposes the vulnerabilities of current RFID networks in identification legitimacy and privacy. It is based on the intermodulation effect originating from intrinsic nonlinearity within tag circuits. To this end, we explore the distinctness and consistency of the intermodulation-based physical layer fingerprint of RFID tags with theoretical analysis and empirical validation, and optimize the attack accuracy and efficiency with delicate excitation plan. Real-world experiments show that RF-Rock achieves an attack success rate of 93.2% on average under various conditions. The entropy of our proposed fingerprint is 15.5 bits and implies sufficient capacity in practical attacks.

CCS CONCEPTS

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

KEYWORDS

Security, RFID, Physical-layer Identification

ACM Reference Format:
Chen Gong, Bo Liang, Purui Wang, Xiaoyu Ji, Yin Chen, Chenren Xu. 2025. RF-Rock: Intermodulation-based RFID Unauthorized Identification Attack without Tag Activation. In *The 31st Annual International Conference on Mobile Computing and Networking (ACM MOBICOM '25), November 4–8, 2025, Hong Kong, China.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3680207.3765262

*✉: chenren@pku.edu.cn

ACM MOBICOM '25, November 4–8, 2025, Hong Kong, China

ACM ISBN 979-8-4007-1129-9/25/11…$15.00
https://doi.org/10.1145/3680207.3765262

1 INTRODUCTION

Automatic object identification boosts the efficiency of commodity circulation and asset supervision in pervasive networked systems [1, 2], as well as enhances the security guarantee of access control and hazardous material management [3]. Among available technologies, RFID is a widely deployed low-cost solution and its market is predicted to reach 23 billion by 2036 [4]. RFID operates by interrogating tags attached to objects via RF signals and protocol commands emitted by readers. Tags are *powered* by the RF signals, *activated* by compliant commands, and backscatter a unique Electronic Product Code (EPC) identifier, which the reader decodes to identify the object. Due to its precise and efficient identification capability, RFID has been widely used in various scenarios, such as passport checking [5], vehicle monitoring [6] and self-checkout [7].

Despite the convenience of RFID technology, it has brought about privacy risks when the tag is activated and its identifier is exposed to unauthorized readers [8, 9]. By sniffing the presence of target RFID tags, such as the one embedded in passports or locomotives, attackers can reveal the whereabouts of passport holders, rail passengers, or cargo [10]. The privacy and security of both individuals and organizations are jeopardized by this *unauthorized identification attack*.

To counteract this threat, various defensive mechanisms have been developed to safeguard the activated tag responses containing identifiers and prevent unauthorized identification. One common practice is to encrypt the tag response with cryptographic algorithms [11–13] and there have been RFID tags with cryptographic capability [14]. Other defenses include randomizing tag response [15], blocking tag activation [16, 17], and checking the legitimacy of readers attempting to activate tags [18, 19]. Since the legible activated tag responses are unavailable to the adversaries, these tag-activation-oriented defenses can prevent existing unauthorized identification attacks aimed at obtaining tag identifiers.

In this paper, we aim to answer the research question: *Can we launch an identification attack against RFID tags without tag activation to sidestep existing defenses?*

Recent advances in RFID tag physical-layer fingerprinting [20–34] shed light on the feasibility. These studies focus on the physical-layer signal properties rather than extracting the digital identifier, thus bypassing the cryptographic

algorithms. The backscattered signals are affected by *inevitable hardware variance* introduced during tag manufacturing. However, *all* existing physical-layer fingerprinting techniques rely on responses of activated tags and fail to work as a practical identification attack when the tag activation is restricted by current defenses. To this end, we aim to design a physical-layer identification attack that addresses the following challenges (C1-C3):

Attack resilience against existing defenses (C1). The activated tags use ON-OFF state switching to generate dynamic signals that are differentiable from static ambient interference. Consequently, defense mechanisms that block tag activation [16, 17] preclude tag signal separation and disable current physical-layer fingerprint extraction approaches. Furthermore, tag activation monitoring [18, 19] and response randomization [15] prevent fingerprint extraction by eavesdropping on legitimate tag responses. These defenses render identification attacks that merely repurpose existing physical-layer authentication techniques infeasible.

Specific to the physical-layer fingerprinting, there arise two other challenges for an effective identification attack:

Attack scalability to tag amount (C2). For a physical-layer property to function as tag fingerprint, it should meet the primary criterion of *distinctness* across a vast amount of tags. While earlier studies tend to depend on incrementally larger datasets, ranging from thousands [22, 24] to hundreds of thousands [21], to demonstrate the distinctness of their suggested physical-layer fingerprints, their distinctness lacks a solid theoretical foundation. This leaves ambiguities about the maximum number of unique fingerprints, and the relatively unexplored mechanisms behind fingerprint production and enhancement cast doubt on the viability of physical layer fingerprinting as a trustworthy identification attack.

Attack consistency across various environments (C3). Fingerprint consistency within each tag under different conditions is another vital prerequisite for successful identification. The signal variance resulting from tag hardware imperfection is minor compared with the impact of complex and dynamic wireless propagation environment. Prior research relying on the signal difference with tag activation and state switching to exclude environmental interference is no longer applicable when confronted with the stealthiness challenge C1. The necessary yet unresolved consistency urges for a new solution to eliminate the effect of wireless propagation.

To overcome the above challenges, we propose an RFID identification attack without tag activation by employing the *intrinsic nonlinearity* of tag circuits. Specifically, the RF-Rock attack leverages the nonlinear intermodulation effect inside a tag [35, 36]. When excited by attacker-generated signals, circuit components within the tag (*e.g.,* diodes) generate new frequency components that are absent from both the incident signals and environmental reflections, enabling activation-free identification of the tag (C1). We then leverage circuit-level simulations, pilot experiments, and entropy analysis to fully validate the distinctness (C2) of intermodulation fingerprints across diverse tags. Finally, we present an intermodulation signal model and suppress environmental interference (C3) by signal differences between different groups of intermodulation products. In summary, our contributions include:

- We present RF-Rock, the first-of-its-kind approach for unauthorized RFID tag identification without activation. It can fingerprint tags while they are asleep, undermining the assumption that deactivation guarantees privacy.
- We highlight fingerprint distinctness with a combination of theoretical analysis, including circuit simulations, empirical testing and entropy estimation. This analytical framework establishes robust theoretical foundations and can be reused for future research.
- We propose an advanced propagation elimination algorithm for fingerprint consistency and provide comprehensive performance evaluation across diverse conditions.
- Extensive evaluations validate the efficacy and resilience of RF-Rock. It achieves an identification accuracy of 93.2% across 20,800 instances from 100 tags and remains reliable with environmental variations. The entropy of the intermodulation-based fingerprint is 15.5 bits, which is sufficient for the majority of attack contexts.

Our dataset and code are available at https://github.com/gcc17/RF-Rock.

2 THREAT MODEL

The RF-Rock attack enables tracking of sensitive RFID-tagged objects by establishing unique physical-layer fingerprints. It circumvents cryptographic protections and other activation-oriented defenses, thereby introducing privacy risks. The attack chain comprises three steps:

(1) **Fingerprint Acquisition:** Capture fingerprints in close contact with the tag.
(2) **(One-time) Target Association:** Link unique tag fingerprints to specific targets (e.g., an ambassador with an RFID-tagged passport) through manual observation or automated visual recognition. The one-time nature of this process ensures that once the association is established, it can be reliably used for subsequent identification attacks.
(3) **Trajectory Reconstruction:** Aggregate tag fingerprint detections across time and space to infer the target movement.

We focus on operational environments where the close proximity necessary for legitimate tag scanning can be exploited for covert fingerprint acquisition: In border control and public transportation systems, an adversary can deploy RF-Rock transceivers near automated passport gates and ticket validators to capture tag fingerprints around mandatory scans. For retail systems, the adversary can place devices

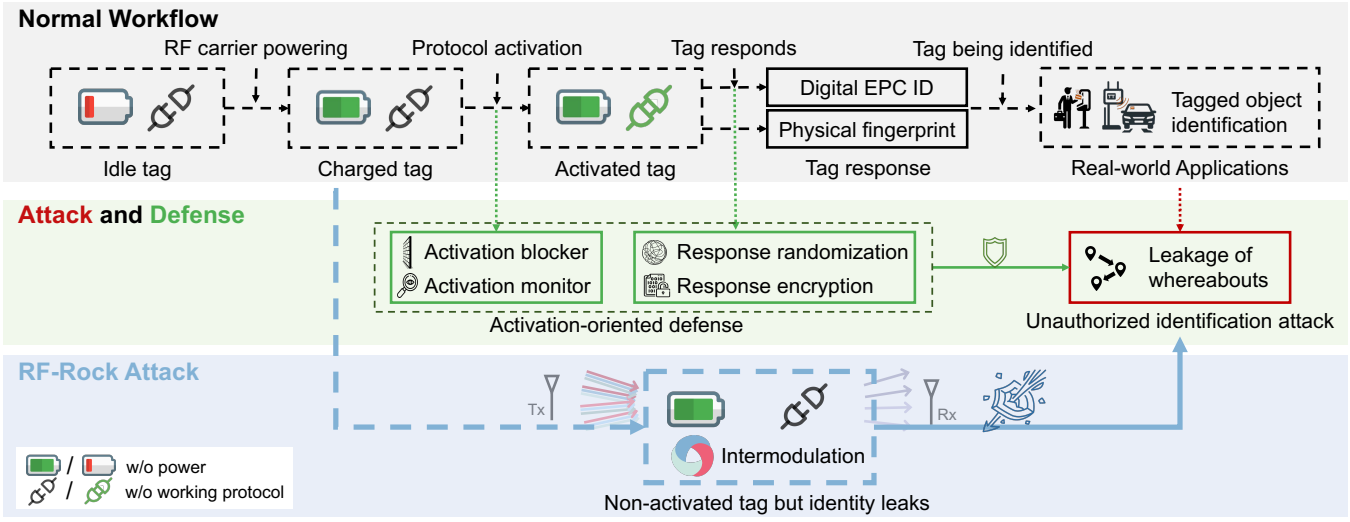
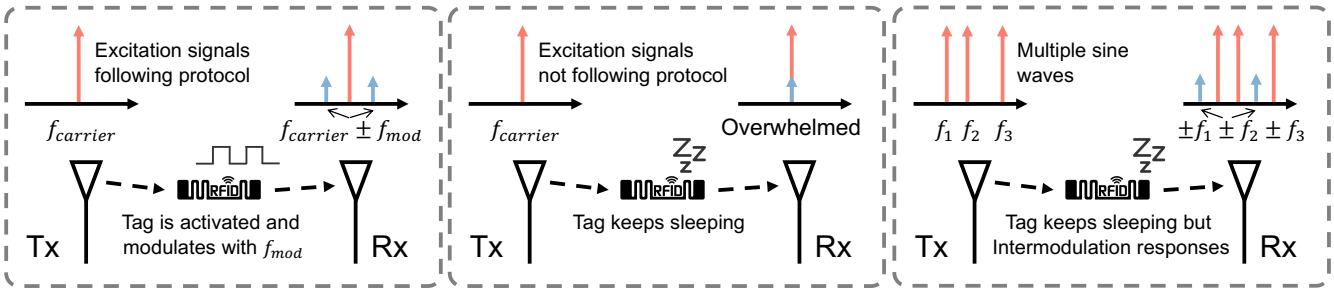


Figure 1: Comparison between existing unauthorized identification attacks and our approach.



(a) Activated Tag Response. **(b) Sleep and No Response.** **(c) Intermodulation Leaks Identity.**

Figure 2: How tag interacts with different signals. RF-Rock leverages intermodulation products of inactivated tags.

near self-checkout stations to capture fingerprints, even after payment when tags are deactivated to prevent triggering alarms [37]. Similarly, warehouse inventory systems could be targeted by placing malicious readers near conveyor belt scanners to collect fingerprints from tagged assets.

To achieve the aforementioned attack in these scenarios, the adversary has the following capabilities:

Deployment of Lightweight Transceivers. The adversary can deploy a radio transceiver that can transmit and receive multi-sine signals to excite and capture intermodulation products at the desired positions. One choice is HackRF One [38] with 120 × 75 mm, 201 grams and less than $120.

Working Range. Our investigation concentrates on sparse tag deployments with predictable proximity patterns, such as sequenced passport controls or retail checkout queues. Although the effective operational range is currently limited to 30 cm, which is shown in our range evaluation in §7.2.1, this limitation is adequate for targeted tracking in the specified scenarios. Notably, RF-Rock maintains functionality even when encountering killed tags, facilitating tag identification attacks across varying operational states.

3 BACKGROUND AND OVERVIEW

3.1 RFID Work Flow

In standard RFID work flow (depicted in Fig. 1), the reader sends RF signals and query commands to power and activate the tags. Once powered and activated, tags will reflect and modulate signals from the reader with ON and OFF state switching. The tag responses contain both digital EPC ID and physical-layer fingerprint. The tag responses are modulated on two sidebands of the carrier, as shown in Fig. 2a. The sideband modulation enables the reader to isolate tag response from ambient noise and reflection.

Current defenses against unauthorized identification protect different phases of tag activation, as shown in Fig. 1. They can be roughly divided into three categories according to tag activation phases. The first defense blocks the tag activation [16, 17] and the tags are powered yet inactivated, which either utilizes RF channel blockers [16] or permanently deactivates tags with the `kill` command[1]. The second defense monitors the legitimacy of readers requesting tag activation and jams unauthorized readers [18, 19].

[1]According to the EPC UHF GEN II Air Interface Protocol [39], RFID tags are rendered permanently inactive upon receiving the `Kill` command and subsequently reject to respond to any query.

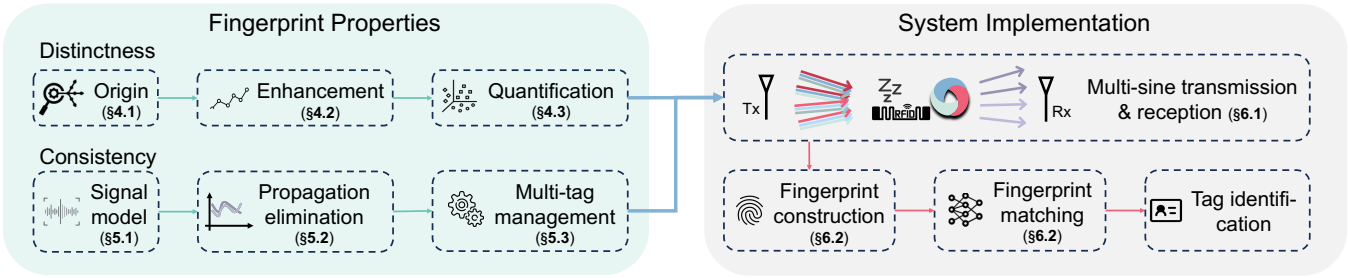


Figure 3: RF-Rock Overview.

The last defense encrypts [11–13] or randomizes [15] the activated tag responses.

Suppose an adversary adapts existing physical-layer fingerprint techniques to avoid tag activation and bypass defenses, she sends signals not following protocols. The inactivated tag only backscatters the signal without modulation, which is overshadowed by direct path interference and environmental reflections, as depicted in Fig. 2b. Such indistinguishable tag signal makes existing approaches ineffective.

3.2 Intermodulation

Intermodulation is a phenomenon when RF signals with multiple frequency components, for example, f_1, f_2, and f_3, are inputted to a nonlinear RF device, like a diode which is a component of RFID tag circuit. The intermodulation effect will result in new 'mixed' frequencies, known as intermodulation products (*e.g.,* $f_1 + f_2 - f_3$ and $2f_1 - f_3$), which is rooted in the non-linear response functions of these devices. The current-voltage function of an ideal diode is an exponential function [40] and can be expanded with Taylor expansion:

$$I = I_s\left(e^{\frac{1}{nV_T}V} - 1\right) = I_s\left(\frac{1}{nV_T}V + \frac{1}{2nV_T}V^2 + \frac{2}{3nV_T}V^3 + \cdots\right)$$
$$= \alpha V + \beta V^2 + \gamma V^3 + \cdots$$

where I_s is the reverse saturation current, n is the ideality factor, and V_T is thermal voltage. The high-order terms of voltage V generate cross terms for incident frequencies, leading to new frequency components in the output current. Given the input frequencies f_1, f_2, and f_3 with amplitude A_1, A_2, and A_3, the intermodulation product of $f_1 + f_2 - f_3$ is:

$$\begin{aligned}&\gamma\left(A_1\cos(2\pi f_1 t) + A_2\cos(2\pi f_2 t) + A_3\cos(2\pi f_3 t)\right)^3\\ &= \cdots + 3\gamma/2 \cdot A_1A_2A_3\cos\left(2\pi(f_1 + f_2 - f_3)t\right) + \cdots\end{aligned} \tag{1}$$

The RFID energy harvesting module, responsible for voltage rectification (*i.e.,* AC to DC) and amplification, consists of a chain of diodes. This module exhibits a spectrum of intermodulation products with new frequencies that encodes tag-specific information (*e.g.,* $\gamma_{(f_1,f_2,f_3)}$), as depicted in Fig. 2c. Since the frequencies of intermodulation products differ from the input signals, they stand out from ambient reflections, which have the same frequencies as the input signals.

3.3 RF-Rock Overview

RF-Rock is an unauthorized identification attack against RFID tags, which does not activate tags and escapes existing defenses of unauthorized RFID reading by leveraging the inherent nonlinearity in RFID tag chips. In the following sections, we will elaborate on the excitation signal plan for intermodulation. The plan is aimed at distinctness and consistency guarantee for a practical and reliable fingerprint. We explore the distinctness origin, enhancement and quantification in §4 and ensure the consistency with established signal model and propagation effect elimination in §5. The system implementation strategy is discussed in §6. The RF-Rock overview is shown in Fig. 3.

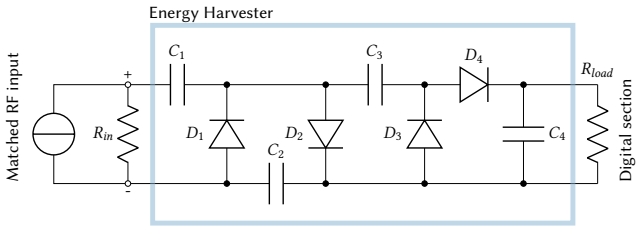
4 INTERMODULATION PRODUCT DISTINCTNESS

To use the intermodulation products of RFID tags as unique identifiers, it is essential to ensure that each tag produces distinct intermodulation signatures. This section addresses the questions of whether these intermodulation products exhibit distinguishable features and how their distinctiveness can be enhanced. To explore this, we conducted simulations at the chip circuit level, performed controlled real-world experiments, and carried out entropy analysis.

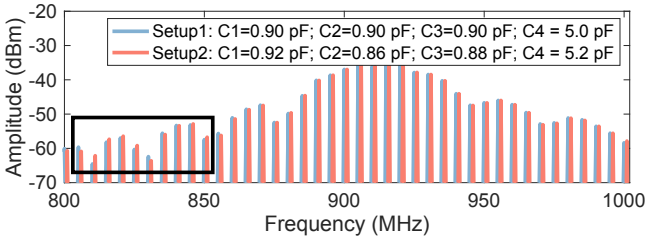
4.1 Distinctness Origin

The intermodulation effect mainly comes from the energy harvesting module within the tag circuit, where the distinctness of intermodulation is rooted in the circuit-level difference. The difference comes from inevitable hardware imperfection introduced in the manufacturing process, called manufacturing tolerance. Practical RFID chips adopt simple processes (*e.g.,* 130 nm [41]) and as public records indicate, the manufacturing tolerance for capacitance during the RFID chip CMOS process can exceed 10% [42]. Such intrinsic variations from circuit tolerances are the fundamental reason for the intermodulation product distinctness across tags.

In our preliminary exploration, we construct a circuit-level simulation of a two-stage voltage doubler energy harvester with popular simulator LTSpice [43], as illustrated in Fig. 4a. The circuit structure and its parameters (*setup 1* in Fig. 4b) align with established RFID tag circuit design studies [44,



(a) A Two-stage Energy Harvester in RFID IC.



(b) Intermodulation Product Diversity with Hardware.

Figure 4: Circuit Simulation with LTSpice.

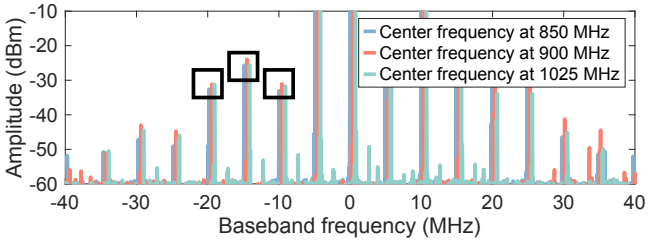
45]. We introduce a minor modification (under 5%) to the circuit capacitors, resulting in *setup 2*. Using sine waves at 905 MHz, 915 MHz, and 920 MHz as excitation signals, we obtain the intermodulation products in Fig. 4b. Peaks except the incident frequency components represent intermodulation products. *The circuit-level simulation can introduce adjustable and controllable variances to RFID energy harvesting circuits and show that even minor variations in circuit components can yield perceptible changes in the intermodulation products.*

4.2 Distinctness Enhancement

To scale up tag identification, the intermodulation products of RFID tags must demonstrate significant distinctness. Recent research indicates that common commercial RFID tags can respond over a broader frequency range (800-1100 MHz) compared to their designed ISM band (about 20 MHz) [46, 47], showing increased hardware distinctness in these extended bands [21] through large scale experiments. We wonder whether it is still effective in the context of intermodulation products. As the Berkeley diode model [48] used in our simulation does not account for frequency-dependent responses, it cannot reflect the intermodulation product variance across different bands. Instead, we analyze real-world tag chips (MONZA-2K [49]) with signals across diverse bands.

We capture intermodulation products using a custom test board with wired SMA connections, as shown in Fig. 5a. This setup eliminates wireless propagation effects across frequencies (addressed further in §5). Excitation signals with central frequencies of 850 MHz, 900 MHz, and 1025 MHz are used, with consistent baseband frequency offsets (-5, 0, and 10 MHz, e.g., 845, 850, and 860 MHz). Results in Fig. 5b reveal a 3 dB variation in intermodulation products across bands. *The controlled wired experiments demonstrate frequency-dependent variances in intermodulation products of commercial tags, highlighting the potential for large-scale identification.*

(a) Our Custom Wired RFID Test Board.



(b) Intermodulation Product Diversity across Bands.

Figure 5: Wired Measurement with Test Board.

4.3 Distinctness Quantification

We seek to advance beyond the *qualitative* intuition that a broader frequency band inherently provides more distinct features in RFID tags. To achieve this, we undertake a *quantitative* investigation to rigorously evaluate this assumption. While prior studies [21–24] have conducted large-scale experiments, they fail to conclusively demonstrate that incorporating arbitrary additional frequency components invariably enhances tag identification. A critical unresolved issue is the potential correlation between responses at different frequencies. If the response at one frequency can be predicted or 'extrapolated' from known frequencies [50], simply expanding the frequency spectrum may not enhance distinctiveness and could prove ineffective in scaling tag identification.

To better understand the relationship between intermodulation products of different frequencies, we calculate the entropy of intermodulation products to quantitatively describe the distinctness distribution. Entropy quantification is usually employed to measure the distinctiveness or predictability of a variable, especially in fingerprinting studies [51–53]. The Shannon entropy of a discrete random variable regarding its probability distribution is given as:

$$H(\mathbf{v}) = -\sum_{i}^{M} p(v_i) \log p(v_i)$$

Directly applying this formula to the entropy estimation of intermodulation products encounters two challenges: 1) *Correlated high dimensions.* The intermodulation products across wide bands result in high-dimensional (*e.g.,* 10k) features and risk the 'curse of dimensionality'. In such cases, feature vectors may become sparsely distributed across a vast space, and correlations between different dimensions can complicate the accurate estimation of probability distributions. 2) *Value continuity.* The values of intermodulation products are continuous. Although the summation operation

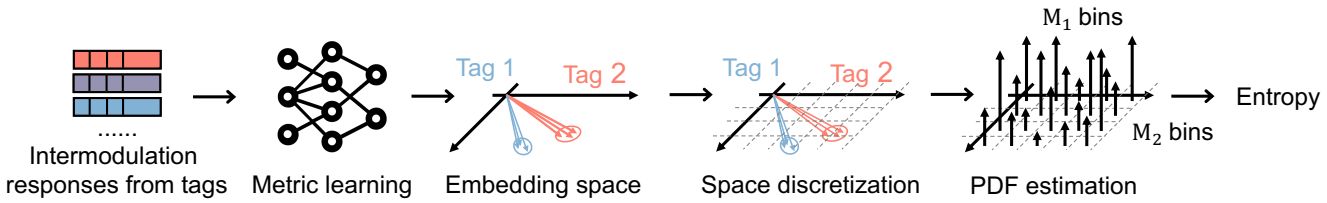


Figure 6: Entropy Estimation.

in entropy calculations can be adapted to integration for continuous variables, this approach necessitates a large dataset to achieve probability estimation with high confidence.

To address aforementioned issues in entropy calculation, we map the real-world tag intermodulation products into a *independent low-dimensional space*, and divide the space into *discrete regions* to enable the probability distribution estimation, as shown in Fig. 6. The workflow is as follows:

Data Collection. To inspect real-world tag intermodulation products and eliminate the effect of wireless signal propagation, we collected 7,800 intermodulation product instances from 100 Alien 9640 tags [54] from a fixed location. The intermodulation excitation signals included a variety of frequency components across 850 to 1025 MHz.

Dimension Reduction and Decoupling. Our objective is to eliminate internal correlations among the dimensions of intermodulation products and retain only the independent principal components. While principal component analysis (PCA) is a widely used method for this purpose, it does not inherently ensure the clustering of samples from the same tag and is unsuitable for our ultimate goal of tag identification. To address this, we employ deep metric learning for its dual role in supervised clustering and dimension reduction [55, 56]. The loss function of metric learning is defined as follows:

$$L = \sum_{v_a \in \mathsf{E}} \sum_{v_p \in \mathsf{P}_a} \sum_{v_n \in \mathsf{N}_a} \sum_{i=1}^{N} \|v_i^a - v_i^p\|_2^2 - \|v_i^a - v_i^n\|_2^2$$

The output from metric learning is an embedding vector of each data sample, represented as v^a belonging to the entire embedding set E, which falls within the space of $\mathcal{S} = [-1, 1]^N$. These vectors are expected to be closer to other vectors $v^p \in \mathsf{P}_a$ from the identical tag (positive sample set) than $v^n \in \mathsf{N}_a$ from different tags (negative sample set). During the training phase, we perform unsupervised clustering of the output embedding vectors, and measure mutual information between the output clusters and true labels. Higher mutual information indicates better clustering of data samples from the same tag and dispersal of samples from different tags. We adjust the dimension of output embedding vectors and observe the consequent mutual information. An 'elbow point' of the mutual information emerges at the embedding vector dimension of $N = 4$, leading to an empirical decision of mapping the intermodulation products into a 4-dimensional space.

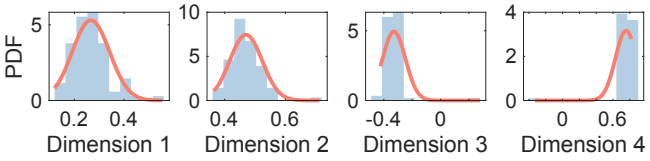


Figure 7: Samples from A Single Tag.

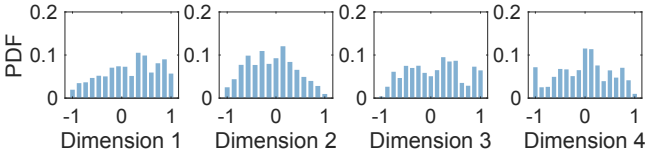


Figure 8: Sample Distributions in the Embedding Space.

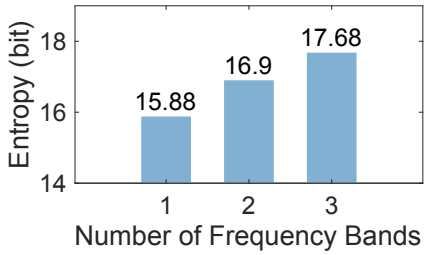


Figure 9: Entropy analysis for various number of intermodulation frequencies across different bands.

Discretization and PDF estimation. The next step for entropy calculation is to estimate the discrete probability distribution function (PDF) within the embedding vector space, both individually for each tag and collectively for all tags. To this end, we adopt the frequentist method [57], which infers probability based on observed frequencies in collected samples. As illustrated in Fig. 7, each tag's features in different measurements typically follow a normal distribution at each dimension i, denoted as $\mathcal{N}(\mu_i, \sigma_i)$. We can distinguish tags if their distribution difference is larger than a critical value known as the full width at half maximum (FWHM), mathematically expressed as $2\sqrt{2 \ln 2}\sigma = 2.3548\sigma$ [58]. This threshold serves as the 'resolution' for dividing space into M_i bins in dimension i. Once segmented, we determine the discrete probability function based on observed data in Fig. 8.

Findings. The entropy estimation results are depicted in Fig. 9. Specifically, the first bar represents the entropy within the single ISM band close to 900 MHz, while the latter two bars account for responses from the additional bands at 850 and 1025 MHz. From this analysis, we can infer two main

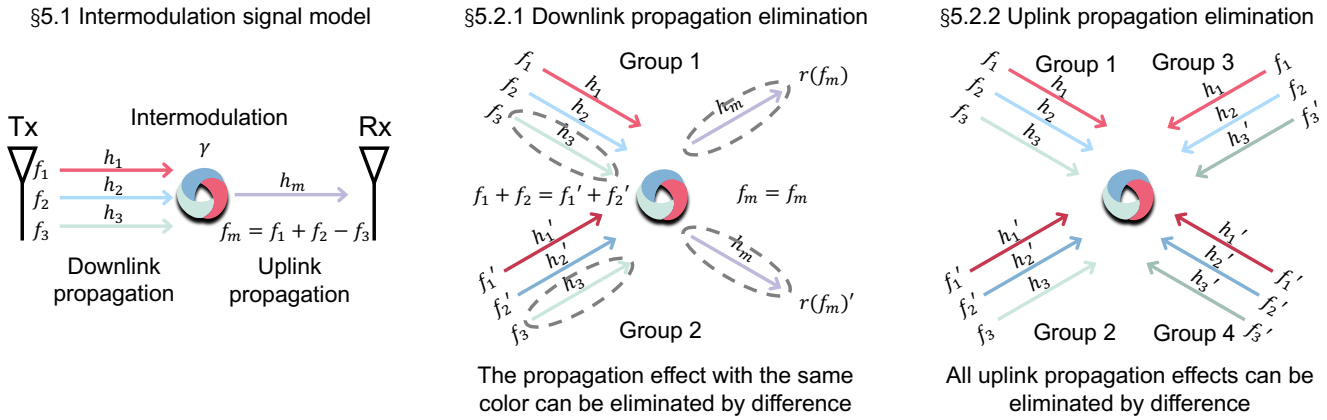


Figure 10: Group Difference Algorithm to Eliminate the Effect of Propagation.

observations: 1) Introducing more intermodulation frequencies notably enhances entropy by 1.02 and 0.78 bits. This result aligns with theoretical predictions of a 1-bit ($\log_2(2)$) increase and 0.59-bits ($\log_2(\frac{3}{2})$) increase, respectively. 2) Multiple frequency bands contribute to a more substantial increase in entropy than a single band. *Our entropy analysis shows that the intermodulation products at different bands are almost independent and we can increase the fingerprint distinctness by expanding the scanning bandwidth.*

In summary, we conduct simulations and pilot experiments to validate the intermodulation product distinctiveness arising from circuit tolerances and excitation frequencies. Furthermore, we employ entropy analysis to quantitatively assess the capacity of intermodulation-based fingerprint, showing its potential for large-scale tag identification.

5 INTERMODULATION PRODUCT CONSISTENCY

Another important characteristic of a fingerprint is its consistency across diverse conditions. The backscattered signals from tags transmit through wireless channels and are prone to distortion from environmental impacts, including the transmission distance and ambient reflections. Prior fingerprinting studies [21–24] utilize the signal difference between activated tag state switching to cancel out the environmental factors, while the tag activation absence of our attack to evade defenses urges for new approaches to mitigate the propagation interference. In this section, we address this challenge by modeling the influences of downlink and uplink propagation and leveraging a group difference elimination algorithm in Fig. 10 to enable consistent fingerprinting.

5.1 Intermodulation Signal Model

We begin with constructing a model to profile the received intermodulation signal with the frequency $f_m = f_1 + f_2 - f_3$. This model describes the signal strength of the received intermodulation product by combining both the intermodulation generation modeled in Eqn. 1 and the propagation processes:

$$\underbrace{r(f_m)}_{\text{received signal}} = \underbrace{h_m}_{\text{uplink}} \cdot \underbrace{\gamma_{(f_1+f_2-f_3)}}_{\text{intermodulation}} \cdot \underbrace{h_1 h_2 h_3}_{\text{downlink}} \cdot \underbrace{A_1 A_2 A_3}_{\text{excitation}} \quad (2)$$

where h_i represents the channel response, including amplitude attenuation and multipath reflection, and A_i denotes the amplitude of the excitation signal with frequency f_i. With this model, two observations can be made. First, our fingerprint, the intermodulation coefficient γ, is intertwined with downlink and uplink signal propagation, which are influenced by the surrounding environment. Second, the intermodulation product with frequency f_m is influenced by all three initial signals of f_1, f_2, and f_3, whose channel responses are not uniform. In the following analysis, we leave out the controllable transmission signal amplitude A_i for brevity.

5.2 Propagation Elimination

Our goal is to derive γ from $r(f_m)$ in Eqn. 2, which serves as a unique intermodulation-based fingerprint for tags. To this end, we eliminate the effect of uplink and downlink with differences between a specially crafted set of signals.

Uplink Propagation Elimination. A common approach to eliminate the propagation effect is taking difference between signals with comparable propagation impacts [59, 60]. In our context, a crucial observation is that excitation signals with varying frequency components can yield intermodulation products of the same frequency, thereby having identical uplink channel responses. Specifically, we adopt a 2-round intermodulation excitation using signal groups (f_1, f_2, f_3) and (f_1', f_2', f_3), which satisfy $f_1 + f_2 = f_1' + f_2'$ and excite identical intermodulation product f_m. The resulting signals are:

$$\begin{aligned} r(f_m)_{(f_1,f_2,f_3)} &= h_m \cdot \gamma_{(f_1+f_2-f_3)} \cdot h_1 h_2 h_3, \\ r(f_m)_{(f_1',f_2',f_3)} &= h_m \cdot \gamma_{(f_1'+f_2'-f_3)} \cdot h_1' h_2' h_3 \end{aligned} \quad (3)$$

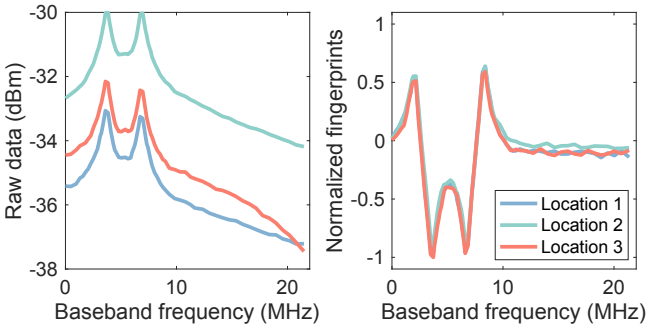


Figure 11: Performance of Elimination Algorithm.

By taking the ratio of $r(f_m)_{(f_1,f_2,f_3)}$ to $r(f_m)_{(f_1',f_2',f_3)}$, we suppress the downlink response of f_3 and uplink of f_m:

$$F_1 = \frac{r(f_m)_{(f_1,f_2,f_3)}}{r(f_m)_{(f_1',f_2',f_3)}} = \frac{\cancel{h_m}\gamma_{(f_1'+f_2'-f_3)}h_1h_2\cancel{h_3}}{\cancel{h_m}\gamma_{(f_1'+f_2'-f_3)}h_1'h_2'\cancel{h_3}} = \frac{\gamma_{(f_1+f_2-f_3)}\cdot h_1h_2}{\gamma_{(f_1'+f_2'-f_3)}\cdot h_1'h_2'} \tag{4}$$

Downlink Propagation Elimination. In Eqn. 4, the uplink influence is removed, leaving the downlink influences of h_1, h_2, h_1', and h_2' in ratio F_1. By transmitting another 2-round excitation signals, composed of identical (f_1, f_2) and (f_1', f_2') but different f_3', we derive another ratio F_1', and then we divide the two ratios:

$$F_1 = \frac{\gamma_{(f_1+f_2-f_3)}\cdot h_1h_2}{\gamma_{(f_1'+f_2'-f_3)}\cdot h_1'h_2'};\ F_1' = \frac{\gamma_{(f_1+f_2-f_3')}\cdot h_1h_2}{\gamma_{(f_1'+f_2'-f_3')}\cdot h_1'h_2'} \tag{5}$$

$$F_2 = \frac{F_1}{F_1'} = \frac{r(f_m)_{(f_1,f_2,f_3)}}{r(f_m)_{(f_1',f_2',f_3)}} \times \frac{r(f_m)_{(f_1',f_2',f_3')}}{r(f_m)_{(f_1,f_2,f_3')}} = \frac{\gamma_{(f_1+f_2-f_3)}}{\gamma_{(f_1'+f_2'-f_3)}} \times \frac{\gamma_{(f_1'+f_2'-f_3')}}{\gamma_{(f_1+f_2-f_3')}} \tag{6}$$

By choosing F_2 as the fingerprint feature, we ensure that only the intermodulation coefficients are involved, effectively eliminating propagation-related factors such as h_i and h_m. To better understand the efficacy of our algorithm, we conduct a microbenchmark test, where we collect the intermodulation product from the same tag but at different positions. As illustrated in Fig. 11, the raw data, shown in the left panel, displays variations in amplitude (due to differences in propagation attenuation) and occasionally discrepancies in the curve shape (resulting from complex interference and multipath effects). However, after applying the aforementioned propagation elimination process, the fingerprint F_2 remains consistent across different positions, as depicted in the right panel. Note that RF-Rock does not require tags to be stationary during reading. These groups, gathered within a millisecond, experience identical propagation effects even if the tag is in motion. In conclusion, by transmitting a sequence of 4-round 3-tone signals and computing the ratios of the received intermodulation product signal strength across these rounds, we effectively eliminate the impacts of signal propagation, maintaining the consistency of tag fingerprint.

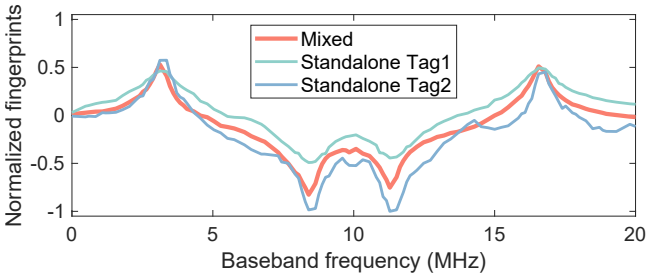


Figure 12: Fingerprint Distortion with Multiple Tags.

5.3 Multi-tag Coexistence Handling

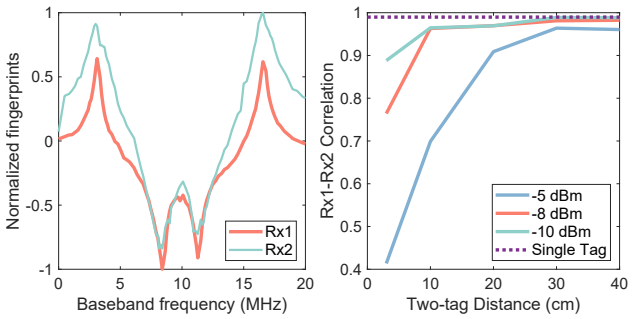
Our research has figured out extracting fingerprints from individual standalone tags. The complexity increases significantly when multiple tags are present. Given that our approach does not activate tags and coordinate their responses, all coexisting tags will produce intermodulation products simultaneously, and these signals mix at the receiver, complicating individual fingerprint extraction. Although multi-tag coexistence within the working range is rare in our targeted sequential scanning scenarios in §2, we delve into the impact of multi-tag coexistence and explore strategies to address it.

Multi-tag Coexistence Impact. We collect intermodulation products from two standalone tags and their coexistence (with the distance of 15 cm to Tx and Rx, tag spacing distance of 5 cm, marked as 'mixed') and repeat the propagation elimination process in §5.2. The results in Fig. 12 demonstrate that the mixed fingerprint exhibits distinct peak values compared to the individual tag fingerprints. To quantify fingerprint similarity, we employ 1D SSIM due to its superior sensitivity to extreme values relative to cross-correlation analysis [61]. The calculated correlation between mixed fingerprints and individual tags falls below 0.8. To clarify the dissimilarity, we examine the mixed ratio F_1 following Eqn. 5, within a two-tag coexistence context:

$$F_1(\text{mix}) = \frac{h_m\gamma_{(f_1+f_2-f_3)}h_1h_2h_3 + \tilde{h}_m\tilde{\gamma}_{(f_1+f_2-f_3)}\tilde{h}_1\tilde{h}_2\tilde{h}_3}{h_m\gamma_{(f_1'+f_2'-f_3)}h_1'h_2'h_3 + \tilde{h}_m\tilde{\gamma}_{(f_1'+f_2'-f_3)}\tilde{h}_1'\tilde{h}_2'\tilde{h}_3} \tag{7}$$

where h_i represents the transmission terms (downlink and uplink) of tag 1, $\tilde{h}_i$ for tag 2, and γ and $\tilde{\gamma}$ denote their intermodulation coefficients. This ratio F_1 is intertwined with transmission terms and cannot be used for tag identification. The intermodulation fingerprints fail to exhibit linear additivity, as the *intermodulation products of different tags undergo different channel propagation that cannot be eliminated.*

Multi-tag Detection with Dual-Rx. Apart from the difficulty of decomposing multi-tag signals, another challenge is to discern whether the received signals come from single or multiple tags. Inspired by the spatial diversity in MIMO [62], we propose to employ a dual-receiver (dual-Rx) setup to detect multi-tag coexistence. This approach leverages the principle that our propagation elimination algorithm is effective at mitigating the propagation effects from a single



(a) Rx Discrepancy. (b) Rx Correlation.

Figure 13: Multi-tag Distortion Detection and Solution.

tag, thereby ensuring consistent fingerprints across different locations, as shown in Fig. 11. However, this algorithm fails with multiple tags and there is large discrepancy across antennas in Fig. 13a. By analyzing the correlation of dual-Rx fingerprints and comparing it against a predetermined threshold (empirically set at 0.96), we can determine the presence of multiple tags within the operational range.

Distortion Mitigation. Fingerprint correlation across different antennas serves not only as a threshold for detecting multiple tags, but also as an indicator of interference on the target tag from surrounding tags. A high correlation suggests that the received signals are predominantly from the nearest tag, with minimal interference from distant tags. This scenario is analogous to the near-far problem in traditional communication systems [63]. To mitigate signal distortion, we optimize the transceiver location and transmission power to make the target tag as the closest one, and primarily excite its intermodulation products while reducing the influence of interfering tags. In a case study where the distance between the Rxs and the farther tag is varied relative to the closer tag, we adjust the transmission power and compare the correlation between the two Rxs. The results, presented in Fig. 13b, demonstrate the feasibility of eliminating the impact of interfering tags by using appropriate transmission power when the distance between the transceivers and the interfering tags is twice that of the target tag.

In real-world attack scenarios, an adversary can adjust the transceiver placement and transmission power based on the target tag's location and the anticipated tag density to mitigate multi-tag interference. Note that while optimizing the two factors is a core principle, fully addressing multi-tag interference requires iterative strategies informed by dual-Rx feedback. The complexity of such an approach exceeds the scope of our current research, which focuses on exposing vulnerabilities in existing defenses and identifying tags in sequential scanning scenarios.

To summarize, we develop a signal propagation model for intermodulation products. We utilize a 4-round 3-tone excitation signal plan, along with a power adaptation strategy, to minimize the effects of signal propagation. These innovations ensure the consistency of tag fingerprints.

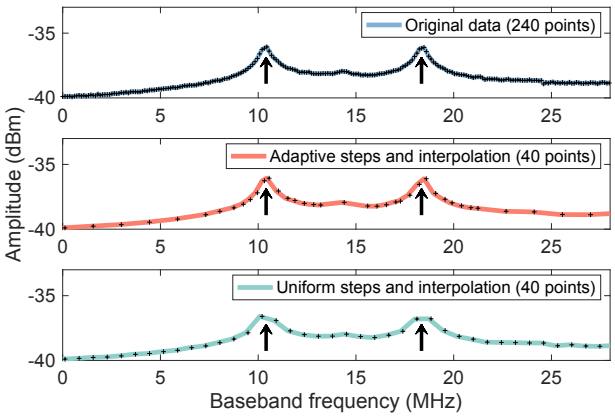


Figure 14: Comparison of f_3-sweeping Schemes.

6 ATTACK IMPLEMENTATION

As observed in §4, wideband intermodulation products result in increased entropy and distinctness. Further, in §5, we elaborate a group difference algorithm to eliminate the propagation effect and ensure fingerprint consistency. In this section, we combine these findings to devise an excitation signal plan for the attack, balancing accuracy and efficiency. We also present our prototype platform of RF-Rock.

6.1 Excitation Signals

The fingerprint feature should incorporate both frequency-dependent distinctness and propagation-suppressing consistency to ensure identification *accuracy*.

4-Round 3-Tone Excitation and f_3-Sweeping. In the propagation elimination algorithm, our excitation signals are grouped into 4-round 3-tone transmission (f_1, f_2, f_3), (f_1', f_2', f_3), (f_1, f_2, f_3'), and (f_1', f_2', f_3') with the constraint of $f_1 + f_2 = f_1' + f_2'$. Without specific demands for f_3, we choose f_3s across a range of continuous frequencies and reuse f_1, f_2.

Band Broadening. As demonstrated in §4.3, expanding beyond the ISM band augments the fingerprint distinctness. Therefore, we exploit the entire frequency spectrum of typical RFID tags and gather intermodulation products across three bands: 850-875 MHz, 950-975 MHz, 1025-1050 MHz.

Power Selection. To minimize sensitivity to position variations and tag density, we transmit the excitation signals at three distinct power levels. Based on empirical observations within the work range, we adopt excitation powers of low (-12 dBm), medium (-8 dBm), and high (-4 dBm).

We further refine the excitation plan towards to finish fingerprint collection within a reasonable amount of time.

Further reuse of (f_1, f_2). One group of excitation signals f_1, f_2, f_3 actually generates multiple intermodulation products besides $f_1 + f_2 - f_3$, such as $2f_1 - f_3$. Given that our propagation elimination algorithm does not assume the exact form of the intermodulation products, careful selection of (f_1, f_2) pairs will generate more exploitable intermodulation products as fingerprints: so long as the intermodulation

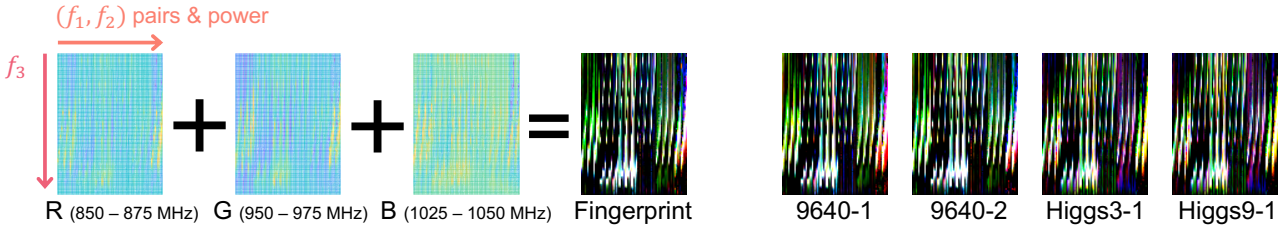


Figure 15: Fingerprint Construction, Examples of Fingerprints, and Their Corresponding Embeddings.

products have the same frequency f_m, the propagation effect can be eliminated as Eqn. 4 and Eqn. 5.

Adaptive f_3-Sweeping. As depicted in Fig. 11, the curves composed of intermodulation products exhibit richer features at the peaks. Recognizing the peak positions ($f_3 = f_1$ or f_2)[2], we adaptively choose the step of f_3-sweeping: f_3s closer to f_1 and f_2 are sampled with a finer granularity, while others adopt coarser steps. A comparison between adaptive f_3-sweeping with complete f_3s is presented in Fig. 14: their similarity proves the feasibility of adaptive sweeping, while the non-selective uniform down-sampling performs worse.

Benefiting from the above efficiency enhancement, we cut down the number of interactions required for single tag identification, from initial 122,400 interactions to mere 7,200 with a 94.1% decrease. The collection of one intermodulation product takes 1/800 s[3]. The trade-off between data collection time and identification accuracy is further analyzed in §7.3.

6.2 Identification Feature Processing

Input Format. Inspired by advances in neural network-based image processing, we structure the intermodulation products analogous to RGB images. Each color channel corresponds to a frequency band. Within a single channel, one dimension corresponds to the sweeping frequency f_3, and the other dimension incorporates both the combinations of (f_1, f_2) and their respective power levels, as illustrated in the left part of Fig. 15.

Identification Algorithm. For tag identification, we utilize the metric learning, the same as our entropy analysis in §4.3 to cluster the fingerprint features from the same tag and disperse different tags. This technique extracts embedding vectors for fingerprints and the distance between these vectors represents the similarity of original inputs. The right part of Fig. 15 shows four fingerprints and their 4-dimensional embedding vectors. The tag identification is achieved by matching current embedding to the closest one in database.

6.3 Prototype Platform

Hardware. We implement the RF-Rock transceiver with a software defined radio platform y790 [64] equipped with

[2]One possible explanation: according to the signal model in Eqn. 2, when $f_3 \approx f_1$, the incident power scales with the factor $(2A_1)A_2(2A_3)/A_1A_2A_3 = 4$, resulting in stronger intermodulation products.

[3]RF-Rock accumulates 150 cycles of the periodic signals to boost SNR.

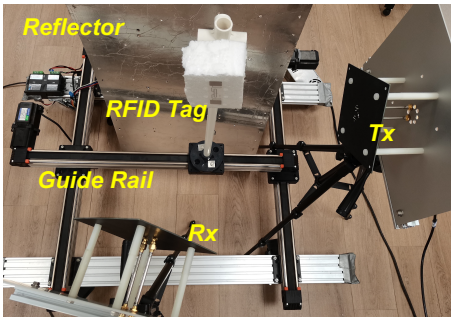


Figure 16: Testbed Setup.

a ZU47DR RFSoC chip [65] for signal transmission and reception with 245.76 MHz sample rate. We employ a recent variant [66] of wideband patch antenna [67] and adapt it with HFSS software[68] for 700-1100 MHz bands. We use a guide rail to move the tags in two horizontal directions, as shown in Fig. 16, where the metal reflector is used for multipath evaluation.

Software. Signals captured by SDR platform are sent to a PC host with E5-2698b v3@2.00 GHz CPU through PCIe connection, and transformed to frequency domain with FFTW library [69]. The metric learning model uses ResNet18 [70] pretrained on ImageNet and connected to a fully-connected layer for 8-dimensional embedding vector, implemented with Pytorch [71] and trained on NVIDIA RTX 3090 GPU. The training process converges in 200 epochs in 60 minutes.

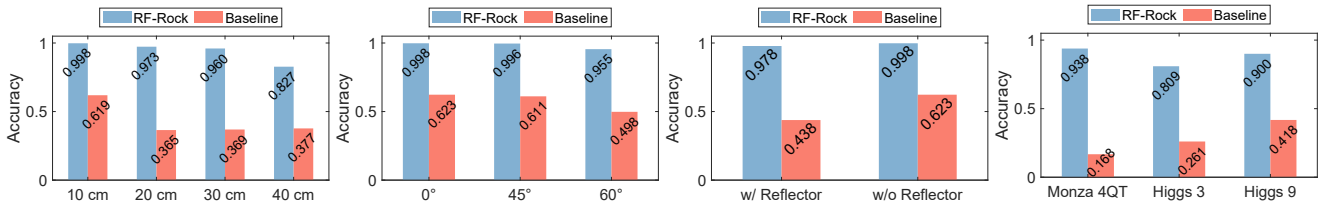
Data Augmentation. As detailed in §6.1, we employ three power levels-high, mid, and low-to excite the tag. During the data collection, we further refine these power levels by adjusting them up or down by 1 dB so we obtain 3 samples for each power level. By combining these samples, we generate $3 \times 3 \times 3 = 27$ unique combinations and enrich our dataset.

7 EXPERIMENTAL EVALUATION

In this section, we evaluate the identification accuracy and the impact of environmental factors, tag models and multi-tag interference. We also weigh the trade-offs between accuracy and efficiency. With the consistency guarantee, we re-calculate the fingerprint entropy to conduct simulations for large scale tag identification accuracy.

7.1 Identification Accuracy

Dataset. Our primary dataset consists of 20,800 instances collected from 100 Alien 9640 tags, gathered across 12 distinct



(a) Distance. **(b) Orientation.** **(c) Multipath.** **(d) Tag Model.**

Figure 17: Impact of Environmental Factors and Tag Models.

positions as detailed in Tab. 1. These positions are categorized into four groups based on the distances between the transmitter and the tag. Note that this experiment focuses solely on single-tag scenario.

Baseline. To assess the necessity of propagation elimination algorithm, we compare RF-Rock with a baseline approach that directly inputs the amplitude of the received intermodulation products into the metric learning model.

Table 1: Position Setups.

Position	1	2	3	4	5	6	7	8	9	10	11	12
$d_{\text{Tx-Tag}}$ (cm)	8			8.5			9.5			12		
$d_{\text{Rx-Tag}}$ (cm)	15	17	18	13	15	17	13	14	17	13	14	15

Metric. We employ a 4-fold cross-validation, using three groups for training and the remaining group for testing to ensure the independence between the training and testing sets. We present the top-1 and top-5 accuracy in Tab. 2.

Table 2: Overall Identification Accuracy (%).

Testing set	RF-Rock		Baseline	
Positions	Top-1 Acc	Top-5 Acc	Top-1 Acc	Top-5 Acc
1, 2, 3	90.29	94.12	31.78	36.23
4, 5, 6	95.67	98.02	26.94	31.58
7, 8, 9	92.65	95.62	28.71	34.79
10, 11, 12	94.38	96.96	23.23	26.38
Average	93.22	96.18	27.67	32.25

Findings. We can derive the following findings: 1) The distinctness of intermodulation products can support a high success rate of the identification attack under various conditions, where the average top-1 accuracy is higher than 93%. 2) Our consistency algorithm enables universality for across different positions. The baseline approach, which directly applies metric learning to raw data, has an identification accuracy less than 40%. The poor performance suggests that the tag position has great impact and makes it difficult for metric learning model to generalize across positions with raw data. On the contrary, RF-Rock eliminates the effect of propagation and ensures consistency for identification.

7.2 Microbenchmark

We analyze the impact of three environmental factors: distance between the tag and antennas, tag orientation, and multipath effect. We also evaluate the identification performance

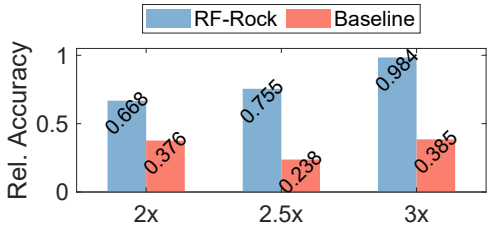


Figure 18: Accuracy with Interfering Distance.

across tag models. In each setup, we compare RF-Rock to the baseline approach, ensuring that the observed generalization capability is not merely attributed to the metric learning, but is inherently rooted in the propagation elimination.

Training Set. The dataset involves 10 tags in each setup to enable fast profiling of the influence factors. In total, the training set consists of 5,200 instances.

Testing Set. The testing set is gathered separately, based on new environmental conditions corresponding to the factors to be evaluated. The new data with different environmental factors is not included in the training set.

7.2.1 Distance. We maintain consistent tag-Tx and tag-Rx distances, aligning with the configuration of commercial RFID readers. The identification accuracy of RF-Rock is evaluated at distances of 10 to 40 cm, as depicted in Fig. 17a. The results demonstrate that the performance of RF-Rock remains relatively stable as the distance increases up to 30 cm, whereas the baseline performance degrades significantly. The observed performance decline at 40 cm suggests the operational range limit of our current system implementation, constrained by transmission power and device sensitivity.

7.2.2 Tag Orientation. The orientation involves both the azimuth and elevation angle between the tag and antenna. The RFID tags in our study are fitted with dipole antennas, whose radiation pattern is invariant to the azimuth angle. Therefore, we only evaluate the impact of polarization misalignment at elevation angles. The results are shown in Fig. 17b. The accuracy remains high even when the misalignment is 60°.

7.2.3 Multipath. We set up an aluminum sheet behind the tag to construct a multipath-rich environment as shown in Fig. 16 and the results are shown in Fig. 17c. The performance gap between RF-Rock and the baseline is evident.

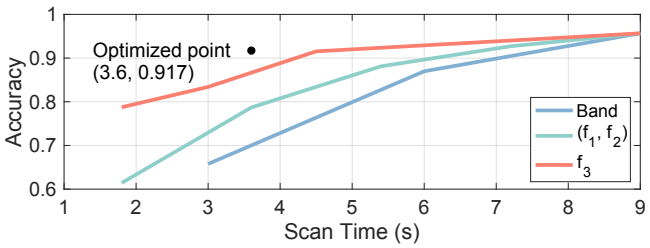


Figure 19: Efficiency-Accuracy Trade-offs.

7.2.4 Tag Model. To demonstrate the wide applicability of our approach, we evaluate RF-Rock with different tag models and show the identification accuracy in Fig. 17d. RF-Rock remains superior to the baseline approach and shows good generalization capability across different tag models.

7.2.5 Multiple Tags. To evaluate the feasibility of our attack in multi-tag interference scenarios, we fix the distance between the target tag and the transceivers at 20 cm while varying the distance of the interfering tag relative to the target tag. We measure the relative identification accuracy of the target tag in the presence of interference compared to scenarios without interference. As shown in Fig. 18, the results demonstrate that when the interfering tag is in close proximity to the target tag, the extracted fingerprints are disrupted, leading to identification failure of the target tag, with performance similar to raw data. However, a turning point occurs when the interfering tag is positioned at a distance three times that of the target tag, where the performance is nearly equivalent to the interference-free case.

7.3 Attack Efficiency

Dataset. We re-use the dataset in §7.1 to evaluate the trade-offs between identification accuracy and fingerprint acquisition time. We reduce the number of intermodulation products and observe the corresponding identification accuracy.

Metric. The intermodulation products are decided by 3 factors as shown in Fig. 15, including the number of frequency bands, (f_1, f_2) pairs and f_3s in excitation signals. We evaluate the impact of each factor while fixing the other two (lines in Fig. 19), and jointly adjust the three variables to obtain a Pareto point for optimal efficiency-accuracy tradeoff.

Findings. The results are shown in Fig. 19. Reduction in the number of intermodulation products invariably impacts identification performance. The performance degradation aligns with our previous assessments in §4.3: 1) The frequency band is vital for distinctness. Reducing from 3 to 2 frequency bands sees accuracy drop from above 95% to below 90%. 2) The adaptive f_3-sweeping has minor impact on identification performance. Reducing the sampled f_3 by half still yields an accuracy rate exceeding 90%. 3) An optimized efficiency-effectiveness trade-off is achieved at 3.6 seconds with 20 f_3 and 4 (f_1, f_2), maintaining an accuracy of 91.7%.

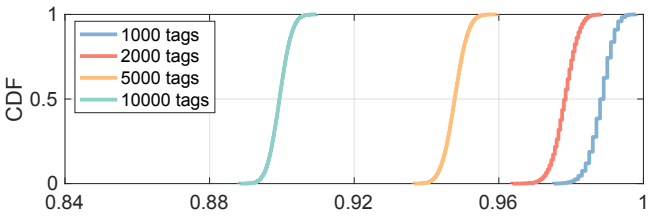


Figure 20: Accuracy in Large Scale Simulation

7.4 Entropy and Large Scale Simulation.

We revisit entropy estimation with the complete dataset composed of fingerprints with the consistency guarantee to explore the maximum discrimination capability of RF-Rock. The approach is similar to our discussion in §4.3 but results are more accurate due to: 1) fingerprint consistency from our propagation elimination algorithm; 2) proper embedding length. As indicated in Tab. 3, the embedding length between 4 to 8 marks an elbow point, achieving near-optimal identification accuracy. Using 4 as the embedding dimension, we update the estimated entropy to 15.5 bits.

Table 3: Embedding Length v.s. Accuracy.

Length	2	3	4	8	16	32	64	128	256
Accuracy (%)	14.2	64.5	88.8	95.7	93.8	95.2	93.9	94.6	94.4

Conducting thorough accuracy tests across a large number of tags requires substantial engineering work and experimental effort. Moreover, such testing yields limited statistical value, as it produces only several data points. The fingerprint misidentification is analogous to hash collisions, particularly known as the multi-collision birthday paradox [72]. This analogy opens up new analytical approaches to handle large-scale scenarios with closed-form analysis and simulation. Specifically, we employ a Monte Carlo simulation approach, which generates multiple samples with equal probability from a value space of $2^{15.5\ \text{(bits)}}$ possibilities and estimates the collision probability. As shown in Fig. 20, we conduct 10,000 Monte Carlo simulations across various tag amounts, resulting in an accuracy cumulative distribution function (CDF). In a scenario like a convenience store with 10,000 RFID-tagged items, our model suggests a median identification accuracy of 89.93%. Although the simulation assumes perfect fingerprint consistency and may overestimate accuracy, it highlights the fingerprint capacity based on our current implementation. Optimizing the excitation signal plan holds the potential for increased entropy and improved accuracy.

8 DISCUSSION

Countermeasures. Apart from physically damaging or sealing tags, another defense is spectrum sensing. However, intermodulation-based fingerprints can be sampled across different bands, allowing adversaries to agilely switch working bands or even replicate waveforms of established protocols like 2G GSM. Besides, the interference from coexisting

tags can combat our attack to some extent. This defense may turn out to be a blessing for adversaries: adversaries equipped with multiple Rxs can detect multi-tag coexistence, move transceivers and adapt power to obtain the fingerprint of each tag, increasing the chances of target identification.

Identification versus Reading. RFID tags contain limited memory storage for additional information. RF-Rock is only a physical-layer identification attack and cannot obtain the additional information without reading the tag memory.

Multi-tag Signal Separation. RF-Rock cannot utilize multiple access supported by MAC layer protocol to deal with the situation of multiple-tag coexistence. Therefore, we have employed power adaption to address the multi-tag interference. Another option is to separate the intermodulation products of different tags, such as blind signal separation with antenna arrays [73, 74] and we leave it for future research.

Working Range. Certain practical RFID-related scenarios, as detailed in our threat model, operate in a limited range. Our working distance aligns with most existing physical-layer fingerprinting [21, 24, 25], maintaining high accuracy within 30 cm. The operational range is primarily limited by FCC transmission power regulations for non-ISM bands, while an adversary could violate these regulations and extend the attack range by employing higher transmission power and more sensitive components like directional antenna and low-noise amplifiers.

Attack More Devices. RF-Rock framework offers extensibility to general identification beyond RFID. Prior work E-Eye [75] detects electronic devices with their nonlinear responses to millimeter-wave excitation, indicating the widespread nonlinearity in electronic devices. Our methods for distinctness and consistency are not tied to RFID tags and can be adapted to other electronic devices.

9 RELATED WORK

RFID Identification Attacks and Defenses. Unauthorized identification in RFID systems can occur through accessing digital identifiers in tag memory or exploiting physical fingerprints. Despite existing defense mechanisms, various counter-strategies have been developed to bypass these protections, as summarized in Tab. 4: cryptographic measures can be circumvented through targeted cracking [76, 77], tag blockers can be bypassed by polling target tags and analyzing responses strategically, and tag killing operations can be reversed by sophisticatedly overwriting tag memory [78, 79]. However, existing attacks share a common limitation of reliance on tag activation, which makes them detectable through activation monitoring and prevents them from extracting tag responses with modulation and channel randomization. In contrast, RF-Rock does not depend on tag activation and is uniquely resilient against existing defenses.

RFID Physical-layer Fingerprinting. RF-Rock is inspired by physical-layer fingerprinting based on signal properties

Table 4: RFID Identification Attacks and Defenses.

	Activation		Response	
Attacks	Blocker	Monitor	Randomization	Encryption
Tag reactivation [78, 79]	✸	🛡	🛡	🛡
Blocked identification [80, 81]	✸	🛡	🛡	🛡
Re-encryption cracking [76]	🛡	🛡	🛡	✸
Physical fingerprint [20]-[34]	🛡	🛡	🛡	✸
RF-Rock	✸	✸	✸	✸

✸ represents that the attack can circumvent the defense, whereas 🛡 denotes that the defense is capable of detecting the attack.

from inevitable hardware imperfections. Past studies leverage diverse properties: modulation shape [28–31], state switching time [32], wavelet coefficients [82], energy distribution [26, 32, 33], persistent time [27], multi-tag interaction [25, 34], frequency drift [22, 23], and wideband responses [21, 24]. Their dependency on tag activation renders them vulnerable to defenses of tag activation blocking and monitoring. Instead, RF-Rock can evade the defenses and identify tags.

Benefit from Intermodulation. Intermodulation has been utilized in various applications, including circuit model classification (*e.g.,* distinguishing between cordless phones and wireless microphones [83]) and radar systems [84]. Additionally, it has been employed to mitigate backscatter self-interference, thereby enhancing the performance of communication [85], sensing [86], power harvesting [36, 87], and RFID tag localization [88]. RF-Rock introduces two advancements: 1) It can distinguish RFID tags even if they share the same circuit model by maximizing distinctiveness and consistency, while existing studies on intermodulation-based classification are limited to different circuit models. 2) It utilizes intermodulation to identify tags without activation, while prior research relies on coordinated tag activation to assist normal communication and sensing.

10 CONCLUSION

In this paper, we introduce an unauthorized RFID tag identification attack without tag activation. Our investigation into the intermodulation-based identification reveals the deficiencies of current defenses focusing on tag activation protection, highlighting the urgent need for improved mechanisms to safeguard tag identification. We develop a comprehensive analytical framework for distinctness and consistency to transform the intermodulation effect into a usable physical-layer fingerprint. We hope the framework including theoretical analysis and empirical validation can be a foundation for future research in physical-layer fingerprinting.

ACKNOWLEDGMENTS

This work is supported by National Key R&D Program of China (Grant No.2023YFF0725004) and National Natural Science Foundation of China (Grant No.62272010 and 62061146001). Chenren Xu is the corresponding author.

REFERENCES

[1] Duncan McFarlane and Yossi Sheffi. The impact of automatic identification on supply chain operations. 2003.

[2] Lu Yan, Yan Zhang, Laurence T. Yang, and Huansheng Ning. *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*. Auerbach Publications, USA, 1st edition, 2008.

[3] Ireneusz Miciula and Henryk Wojtaszek. Automatic hazard identification information system (AHIIS) for decision support in inland waterway navigation. In Imre J. Rudas, János Csirik, Carlos Toro, János Botzheim, Robert J. Howlett, and Lakhmi C. Jain, editors, *Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 23rd International Conference KES-2019, Budapest, Hungary, 4-6 September 2019*, volume 159 of *Procedia Computer Science*, pages 2313–2323. Elsevier, 2019.

[4] Rfid forecasts, players and opportunities 2026-2036. https://www.idtechex.com/en/research-report/rfid/1114.

[5] G. Matthew Ezovski and Steve E. Watkins. The electronic passport and the future of government-issued rfid-based identification. In *2007 IEEE International Conference on RFID*, pages 15–22, 2007.

[6] Omid Abari, Deepak Vasisht, Dina Katabi, and Anantha Chandrakasan. Caraoke: An e-toll transponder network for smart cities. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, page 297–310, New York, NY, USA, 2015. Association for Computing Machinery.

[7] Uniqlo's parent company bets big on tiny rfid chips. https://www.wsj.com/articles/uniqlos-parent-company-bets-big-on-tiny-rfid-chips-600b124f.

[8] A. Juels. Rfid security and privacy: a research survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, 2006.

[9] Gerhard P. Hancke. Practical eavesdropping and skimming attacks on high-frequency rfid tokens. *J. Comput. Secur.*, 19(2):259–288, apr 2011.

[10] Günter Karjoth and Paul A. Moskowitz. Disabling rfid tags with visible confirmation: clipped tags are silenced. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, WPES '05, page 27–30, New York, NY, USA, 2005. Association for Computing Machinery.

[11] Mike Burmester and Jorge Munilla. Lightweight rfid authentication with forward and backward security. *ACM Trans. Inf. Syst. Secur.*, 14(1), jun 2011.

[12] Kai Fan, Nan Ge, Yuanyuan Gong, Hui Li, Ruidan Su, and Yintang Yang. An ultra-lightweight rfid authentication scheme for mobile commerce. *Peer-to-Peer Networking and Applications*, 10:368–376, 2017.

[13] Ari Juels. Minimalist cryptography for low-cost rfid tags (extended abstract). In Carlo Blundo and Stelvio Cimato, editors, *Security in Communication Networks*, pages 149–164, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[14] Ucode dna: Uhf tag ic for secure authentication. https://www.nxp.com/products/rfid-nfc/ucode-rain-rfid-uhf/ucode-dna-uhf-tag-ic-for-secure-authentication:SL3S5002N0FUD. Accessed: 2024-02-02.

[15] Haitham Hassanieh, Jue Wang, Dina Katabi, and Tadayoshi Kohno. Securing rfids by randomizing the modulation and channel. In *Proceedings of the 12th USENIX Conference on Networked Systems Design and Implementation*, NSDI'15, page 235–249, USA, 2015. USENIX Association.

[16] Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: Selective blocking of rfid tags for consumer privacy. In *Proceedings of the 10th ACM Conference on Computer and Communications Security*, CCS '03, page 103–111, New York, NY, USA, 2003. Association for Computing Machinery.

[17] Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips. Guidelines for securing radio frequency identification (rfid) systems. *NIST Special publication*, 80:1–154, 2007.

[18] Han Ding, Jinsong Han, Yanyong Zhang, Fu Xiao, Wei Xi, Ge Wang, and Zhiping Jiang. Preventing unauthorized access on passive tags. In *2018 IEEE Conference on Computer Communications, INFOCOM 2018, Honolulu, HI, USA, April 16-19, 2018*, pages 1115–1123. IEEE, 2018.

[19] Han Ding, Jinsong Han, Cui Zhao, Ge Wang, Wei Xi, Zhiping Jiang, and Jizhong Zhao. Arbitrator2.0: Preventing unauthorized access on passive tags. *IEEE Trans. Mob. Comput.*, 21(3):835–848, 2022.

[20] Boris Danev, Thomas S. Heydt-Benjamin, and Srdjan Čapkun. Physical-layer identification of rfid devices. In *Proceedings of the 18th Conference on USENIX Security Symposium*, SSYM'09, page 199–214, USA, 2009. USENIX Association.

[21] Qingrui Pan, Zhenlin An, Xueyuan Yang, Xiaopeng Zhao, and Lei Yang. Rf-dna: Large-scale physical-layer identifications of rfids via dual natural attributes. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, MobiCom '22, page 419–431, New York, NY, USA, 2022. Association for Computing Machinery.

[22] Qingrui Pan, Zhenlin An, Xiaopeng Zhao, and Lei Yang. Revisiting backscatter frequency drifts for fingerprinting rfids: A perspective of frequency resolution. In *2023 20th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 124–132, 2023.

[23] Qingrui Pan, Zhenlin An, Xiaopeng Zhao, and Lei Yang. The power of precision: High-resolution backscatter frequency drift in rfid identification. *IEEE Transactions on Mobile Computing*, 2023.

[24] Jiawei Li, Ang Li, Dianqi Han, Yan Zhang, Tao Li, and Yanchao Zhang. Rcid: Fingerprinting passive rfid tags via wideband backscatter. In *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, page 700–709. IEEE Press, 2022.

[25] Ge Wang, Haofan Cai, Chen Qian, Jinsong Han, Xin Li, Han Ding, and Jizhong Zhao. Towards replay-resilient rfid authentication. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, MobiCom '18, page 385–399, New York, NY, USA, 2018. Association for Computing Machinery.

[26] Jinsong Han, Chen Qian, Panlong Yang, Dan Ma, Zhiping Jiang, Wei Xi, and Jizhong Zhao. Geneprint: Generic and accurate physical-layer identification for uhf rfid tags. *IEEE/ACM Transactions on Networking*, 24(2):846–858, 2016.

[27] Xingyu Chen, Jia Liu, Xia Wang, Haisong Liu, Dong Jiang, and Lijun Chen. Eingerprint: Robust energy-related fingerprinting for passive rfid tags. In *USENIX NSDI*, 2020.

[28] Boris Danev, Thomas S. Heydt-Benjamin, and Srdjan Čapkun. Physical-layer identification of rfid devices. In *Proceedings of the 18th Conference on USENIX Security Symposium*, SSYM'09, page 199–214, USA, 2009. USENIX Association.

[29] Chinnappa Gounder Periaswamy, Dale R. Thompson, H.P. Romero, Senthilkumar Chinnappa, G. Periaswamy, Dale R. Thompson, and H.P. Romero. Fingerprinting radio frequency identification tags using timing characteristics. 2009.

[30] Henry P. Romero, Kate A. Remley, Dylan F. Williams, and Chih-Ming Wang. Electromagnetic measurements for counterfeit detection of radio frequency identification cards. *IEEE Transactions on Microwave Theory and Techniques*, 57(5):1383–1387, 2009.

[31] Davide Zanetti, Pascal Sachs, and Srdjan Capkun. On the practicality of uhf rfid fingerprinting: How real is the rfid tracking problem? In *Proceedings of the 11th International Conference on Privacy Enhancing Technologies*, PETS'11, page 97–116, Berlin, Heidelberg, 2011. Springer-Verlag.

[32] Davide Zanetti, Boris Danev, and Srdjan Capkun. Physical-layer identification of uhf rfid tags. In *Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking*, MobiCom '10, page 353–364, New York, NY, USA, 2010. Association for Computing Machinery.

[33] Senthilkumar Chinnappa Gounder Periaswamy, Dale R. Thompson, and Jia Di. Fingerprinting rfid tags. *IEEE Transactions on Dependable and Secure Computing*, 8(6):938–943, 2011.

[34] Kai Zhang, Jiuwu Zhang, Xin Xie, Xinyu Tong, Xiulong Liu, and Keqiu Li. Frequency- and orientation-related phase fingerprints for rfid tag authentication. In *2022 19th Annual IEEE International Conference on*

Sensing, Communication, and Networking (SECON), 2022.

[35] Ping Li, Zhenlin An, Lei Yang, Panlong Yang, and QiongZheng Lin. Rfid harmonic for vibration sensing. *IEEE Transactions on Mobile Computing*, 2021.

[36] Nai-Chung Kuo and Ali M. Niknejad. Rf-powered-tag intermodulation uplink with three-tone transmitter for enhanced uplink power. *IEEE RFID*, 2019.

[37] Introducing the rfid self checkout kiosk in nrf 2023. https://mishipay.com/blogs/introducing-the-rfid-self-checkout-kiosk-in-nrf-2023/.

[38] Low cost software defined radio hackrf. https://greatscottgadgets.com/hackrf/one/. Accessed: 2023-12-06.

[39] Epc™ radio-frequency identity protocols generation-2 uhf rfid standard. https://www.gs1.org/sites/default/files/docs/epc/gs1-epc-gen2v2-uhf-airinterface_i21_r_2018-09-04.pdf. Accessed: 2023-07-26.

[40] Ideal diode equation. https://eng.libretexts.org/Bookshelves/Materials_Science/Supplemental_Modules_(Materials_Science)/Solar_Basics/D._P-N_Junction_Diodes/3%3A_Ideal_Diode_Equation. Accessed: 2023-08-15.

[41] Yang Hong, Chi Fat Chan, Jianping Guo, Yuen Sum Ng, Weiwei Shi, Lai Kan Leung, Ka Nang Leung, Chiu Sing Choy, and Kong Pang Pun. Design of passive uhf rfid tag in 130nm cmos technology. In *APCCAS 2008-2008 IEEE Asia Pacific Conference on Circuits and Systems*, 2008.

[42] Foundry technologies 130-nm cmos and rf cmos. https://edg.uchicago.edu/projects/sampling_chip_review_2010/docs/130nm-techbrief01.pdf.

[43] ltspice-simulator. https://www.analog.com/en/design-center/design-tools-and-calculators/ltspice-simulator.html.

[44] Giuseppe De Vita and Giuseppe Iannaccone. Design criteria for the rf section of uhf and microwave passive rfid transponders. *IEEE transactions on microwave theory and techniques*, 2005.

[45] Dahmane Allane, Gianfranco Andia Vera, Yvan Duroc, Rachida Touhami, and Smail Tedjini. Harmonic power harvesting system for passive rfid sensor tags. *IEEE Transactions on microwave theory and techniques*, 2016.

[46] Yunfei Ma, Nicholas Selby, and Fadel Adib. Minding the billions: Ultra-wideband localization for deployed rfid tags. In *ACM MobiCom*, 2017.

[47] Towards deployable rfid localization system for logistics network: Hardware, firmware, and software of rf-chord. https://soar.group/projects/rfid/rfchord/.

[48] Surface mount microwave schottky detector diodes in sot-323 (sc-70). http://www.hp.woodshot.com/hprfhelp/4_downld/products/diodes/hsms285a.pdf.

[49] Monza x-2k dura tag chip datasheet. https://support.impinj.com/hc/en-us/articles/202765328-Monza-R6-Product-Brief-Datasheet. Accessed: 2023-08-05.

[50] Manfred R. Schroeder. Frequency-correlation functions of frequency responses in rooms. *Journal of the Acoustical Society of America*, 34:1819–1823, 1962.

[51] Peter Eckersley. How unique is your web browser? In *Privacy Enhancing Technologies: 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings 10*. Springer, 2010.

[52] Guillaume Celosia and Mathieu Cunche. Fingerprinting bluetooth-low-energy devices based on the generic attribute profile. In *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, 2019.

[53] Xiang-Yang Li, Huiqi Liu, Lan Zhang, Zhenan Wu, Yaochen Xie, Ge Chen, Chunxiao Wan, and Zhongwei Liang. Finding the stars in the fireworks: Deep understanding of motion sensor fingerprint. *IEEE/ACM Transactions on Networking*, 27(5):1945–1958, 2019.

[54] Alien 9640 rfid tag. http://www.alientechnology.com/wp-content/uploads/Alien-Technology-Higgs-3-ALN-9640-Squiggle.pdf. Accessed: 2023-08-12.

[55] Mehrtash Harandi, Mathieu Salzmann, and Richard Hartley. Joint dimensionality reduction and metric learning: A geometric take. In Doina Precup and Yee Whye Teh, editors, *Proceedings of the 34th International Conference on Machine Learning*, volume 70 of *Proceedings of Machine Learning Research*, pages 1404–1413. PMLR, 06–11 Aug 2017.

[56] Fei Wang and Jimeng Sun. Survey on distance metric learning and dimensionality reduction in data mining. *Data mining and knowledge discovery*, 29(2):534–564, 2015.

[57] Min-ge Xie and Kesar Singh. Confidence distribution, the frequentist distribution estimator of a parameter: A review. *International Statistical Review*, 81(1):3–39, 2013.

[58] Full width at half maximum. https://en.wikipedia.org/wiki/Full_width_at_half_maximum. Accessed: 2023-08-15.

[59] Hao Wang, Daqing Zhang, Yasha Wang, Junyi Ma, Yuxiang Wang, and Shengjie Li. Rt-fall: A real-time and contactless fall detection system with commodity wifi devices. *IEEE Transactions on Mobile Computing*, 16(2):511–526, 2016.

[60] Fusang Zhang, Jie Xiong, Zhaoxin Chang, Junqi Ma, and Daqing Zhang. Mobi2sense: empowering wireless sensing with mobility. In *ACM MobiCom*, 2022.

[61] Yuhan Liu and Ke Tu. Ts3im: Unveiling structural similarity in time series through image similarity assessment insights. In *2024 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2024.

[62] John G Proakis. *Digital communications*. McGraw-Hill, Higher Education, 2008.

[63] D.J. Goodman and A.A.M. Saleh. The near/far effect in local aloha radio communications. *IEEE Transactions on Vehicular Technology*, 36(1):19–27, 1987.

[64] V3 yunsdr y790. https://www.v3best.com/y790.

[65] Zynq ultrascale+ rfsoc zu47dr. https://docs.xilinx.com/v/u/en-US/ds890-ultrascale-overview. Accessed: 2023-08-12.

[66] Dong-Ze Zheng and Qing-Xin Chu. A wideband dual-polarized antenna with two independently controllable resonant modes and its array for base-station applications. *IEEE Antennas and Wireless Propagation Letters*, 16:2014–2017, 2017.

[67] Seong-Youp Suh, W.L. Stutzman, and W.A. Davis. Low-profile, dual-polarized broadband antennas. In *IEEE Antennas and Propagation Society International Symposium. Digest. Held in conjunction with: USNC/CNC/URSI North American Radio Sci. Meeting (Cat. No.03CH37450)*, volume 2, pages 256–259 vol.2, 2003.

[68] Hfss simulation software. https://www.ansys.com/products/electronics/ansys-hfss. Accessed: 2023-08-12.

[69] Fftw library for dft operation. https://www.fftw.org/. Accessed: 2023-08-12.

[70] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. *CoRR*, abs/1512.03385, 2015.

[71] Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, Alban Desmaison, Andreas Kopf, Edward Yang, Zachary DeVito, Martin Raison, Alykhan Tejani, Sasank Chilamkurthy, Benoit Steiner, Lu Fang, Junjie Bai, and Soumith Chintala. Pytorch: An imperative style, high-performance deep learning library. In *Advances in Neural Information Processing Systems 32*, pages 8024–8035. Curran Associates, Inc., 2019.

[72] Kazuhiro Suzuki, Dongvu Tonien, Kaoru Kurosawa, and Koji Toyota. Birthday paradox for multi-collisions. In *Information Security and Cryptology–ICISC 2006: 9th International Conference, Busan, Korea, November 30-December 1, 2006. Proceedings 9*. Springer, 2006.

[73] Asli F. Mindikoglu and Alle-Jan van der Veen. Separation of overlapping rfid signals by antenna arrays. In *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 2737–2740, 2008.

[74] Y. Deville, J. Damour, and N. Charkani. Multi-tag radio-frequency identification systems based on new blind source separation neural networks. *Neurocomputing*, 49(1):369–388, 2002.

[75] Zhengxiong Li, Zhuolin Yang, Chen Song, Changzhi Li, Zhengyu Peng, and Wenyao Xu. E-eye: Hidden electronics recognition through

mmwave nonlinear effects. In *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*, SenSys '18, page 68–81, New York, NY, USA, 2018. Association for Computing Machinery.

[76] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai. Enhancing privacy of universal re-encryption scheme for rfid tags. In Laurence T. Yang, Minyi Guo, Guang R. Gao, and Niraj K. Jha, editors, *Embedded and Ubiquitous Computing*, pages 879–890, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[77] Gildas Avoine, Etienne Dysli, and Philippe Oechslin. Reducing time complexity in rfid systems. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography*, pages 291–306, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[78] Christopher Bolan. Kill features of rfid tags in a medical environment: Boon or burden? 2007.

[79] Christopher Bolan. The lazarus effect: Resurrecting killed rfid tags. 2006.

[80] Xiulong Liu, Xin Xie, Xibin Zhao, Kun Wang, Keqiu Li, Alex X. Liu, Song Guo, and Jie Wu. Fast identification of blocked rfid tags. *IEEE Transactions on Mobile Computing*, 17(9):2041–2054, 2018.

[81] Xia Wang, Jia Liu, Yanyan Wang, Xingyu Chen, and Lijun Chen. Efficient missing tag identification in blocker-enabled rfid systems. *Computer Networks*, 164:106894, 2019.

[82] Crystal Bertoncini, Kevin Rudd, Bryan Nousain, and Mark Hinders. Wavelet fingerprinting of radio-frequency identification (rfid) tags. *IEEE Transactions on Industrial Electronics*, 59(12):4843–4850, 2012.

[83] Anthony F Martone and Edward J Delp. Characterization of rf devices using two-tone probe signals. In *2007 IEEE/SP 14th Workshop on Statistical Signal Processing*, pages 161–165. IEEE, 2007.

[84] Gregory J Mazzaro, Anthony F Martone, and David M McNamara. Detection of rf electronics by multitone harmonic radar. *IEEE Transactions on Aerospace and Electronic Systems*, 50(1):477–490, 2014.

[85] Deepak Vasisht, Guo Zhang, Omid Abari, Hsiao-Ming Lu, Jacob Flanz, and Dina Katabi. In-body backscatter communication and localization. In *SIGCOMM 2018*. ACM.

[86] Ashish Mishra, William McDonnell, Jing Wang, Daniel Rodriguez, and Changzhi Li. Intermodulation-based nonlinear smart health sensing of human vital signs and location. *IEEE access*, 2019.

[87] Nai-Chung Kuo, Bo Zhao, and Ali M. Niknejad. Novel inductive wireless power transfer uplink utilizing rectifier third-order nonlinearity. *IEEE Transactions on Microwave Theory and Techniques*.

[88] Hugo Gomes and Nuno Borges Carvalho. Rfid for location proposes based on the intermodulation distortion. *Sensors & Transducers*, 2009.