2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON) | 978-1-6654-8643-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/SECON55815.2022.9918585

# ReaderPrint: A Universal Method for RFID Readers Authentication Based on Impedance Mismatch

Yinan Zhu*, Chunhui Duan†✉, Xuan Ding*, Zheng Yang*
*School of Software and BNRist, Tsinghua University, China
†School of Computer Science and Technology, Beijing Institute of Technology, China
Email: zhuyn1997@gmail.com, duanch@bit.edu.cn, {dingxuan,yangzheng}@tsinghua.edu.cn (✉Corresponding author)

***Abstract*—Unauthorized access attack has always been a critical problem in RFID systems since any illegitimate reader can conduct access commands on tags without authorization and leave no trace. Past solutions for reader authentication require either modifications on EPC-global Gen2 protocol, which are inapplicable to existing infrastructures, or numerous extra customized devices as communication monitors, which incur high overhead. In this paper, we present a universal, low-cost and effective system to authenticate RFID readers, namely *ReaderPrint*, which only requires an extra passive tag array and is fully compatible with Gen2 protocol. The key insight behind ReaderPrint is that the impedance mismatch degrees (IMD) of different reader antennas across channels are distinguishable. We verify this mechanism through empirical studies using vector network analyzer and further propose two brand-new forms of hardware fingerprints, *i.e.*, IMD-induced transmission power attenuation (ITPA) and phase shifts (IPS) across channels to quantify the IMD. Besides, to address the negative impacts of environmental changes, well-refined fingerprint matching algorithms are designed accordingly. We implement a prototype of ReaderPrint and evaluate it on 96 different readers in three indoor scenarios. Experimental results show that ReaderPrint can achieve fairly high authentication accuracy of up to 97.2%, regardless of environmental or device conditions.**

***Index Terms*—RFID, Unauthorized access attack, Reader hardware fingerprint, Impedance mismatch**

## I. Introduction

Today, as one of the key technologies in the Internet of Things, radio frequency identification (RFID) has gained popularity in a wide range of applications, such as warehouse inventory, baggage handling and unmanned retail [1], [2]. Passive RFID tags with no battery equipped, which exploit backscatter communication and store critical information (*e.g.*, electronic product code) in their memory banks, are commonly used to label items for identification purposes [3].

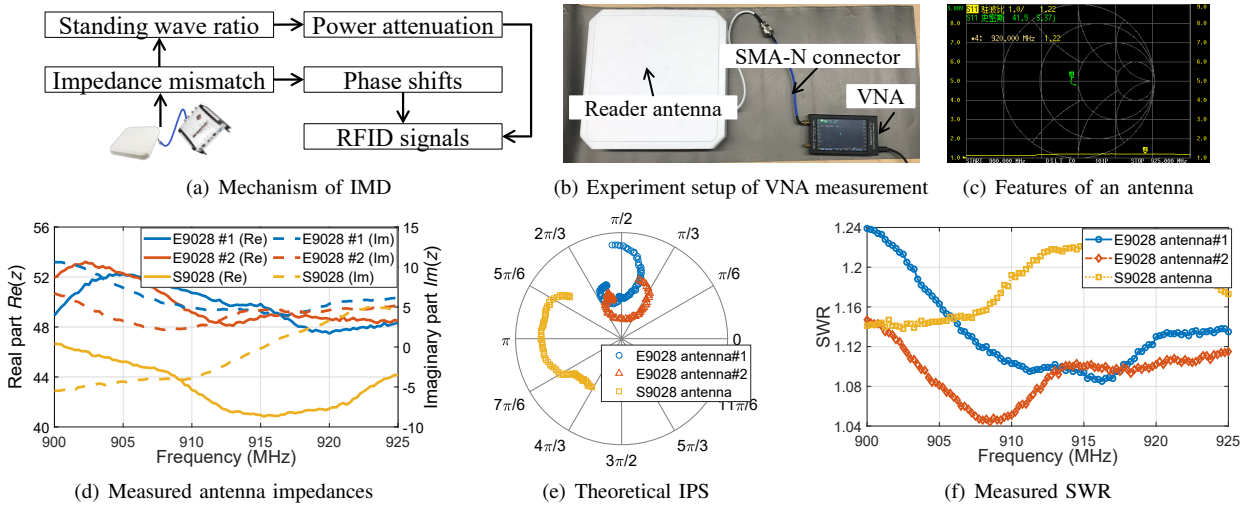
With the extensive adoption of RFIDs in people's everyday life, the security problems of existing RFID systems have drawn increasing attention [4]–[6] recently. One of the most urgent issues is *unauthorized access attack* [7]. As we know, the communication between commodity tags and interrogators should follow the EPC-global Class 1 Generation 2 air interface protocol [8] (abbreviated as "C1G2 protocol" hereafter), which however does not support reader authentication functionality. Illegitimate readers can easily establish a communication channel and access the tag memories without being authorized, thereby conducting malicious attacks (*e.g.*, retrieving or tampering the private information stored in tags attached to valuables, or even inactivating tags to disable the total RFID systems permanently) while leaving no traces. As a matter of fact, we have successfully exploited the `Read`, `Write` and `Kill` commands to perform the aforementioned attacks on certain airline baggage tags [9] and a part of item tags in Decathlon stores [10] using self-owned commercial off-the-shelf (COTS) readers (see Fig. 1). Therefore, validating reader legitimacy is vitally necessary, especially for some critical applications such as vaccines and chemicals management, where a great loss of life, time or property would be incurred once the attack happens.


(a) Baggage tag of an airline (b) Item tag in a store

**Fig. 1: Commodity RFID tags in real-world applications. Most of them are vulnerable to unauthorized access attack from illegitimate readers.**

In order to reinforce the security of RFID systems, existing related literature mainly focuses on designing authentication protocols based on cryptographic algorithms [11], [12]. However, these protocols are difficult to apply in practice because they require modifications of either hardware or C1G2 protocol, thus incompatible with commercial RFID devices. To overcome such limitation, state-of-the-art work Arbitrator [7], [13] proposes to leverage readers' hardware fingerprints inside physical-layer transmission signal fragments for authentication. Despite its promising advantages, Arbitrator has the following two notable weaknesses: (i) to acquire physical-layer signals, dedicated devices like software defined radio (SDR)-based monitors are required to be deployed in the vicinity of each reader, which is inflexible to restrict the readers' locations during authentication, and also incurs extra high deployment costs and maintenance efforts in the meantime; (ii) Arbitrator fails to work when the illegitimate reader locates very close to tags with a low transmission power or multiple readers are simultaneously accessing tags. As a result, it still remains to be an open problem to develop a more ubiquitous solution for reader authentication.

In this paper, we present ReaderPrint, a universal and lightweight approach to authenticate RFID readers with high accuracy purely utilizing COTS RFID devices. To achieve




(a) Mechanism of IMD (b) Experiment setup of VNA measurement (c) Features of an antenna

(d) Measured antenna impedances (e) Theoretical IPS (f) Measured SWR

**Fig. 2: Reader antenna measurement using VNA. (a) shows the mechanism how antenna impedance mismatch affect RFID signals. (b) shows the experiment setup and (c) shows an example of measured antenna features (*e.g.*, smith charts). (d)-(f) detailedly show the distributions of measured antenna impedance across channels, theoretically calculated IPS and measured standing wave ratios across channels.**

the goal, we innovatively propose two brand-new hardware fingerprints related to the *impedance mismatch degree* (IMD) of a reader antenna for authentication: IMD-induced reader's transmission power attenuation (ITPA) and IMD-induced phase shift (IPS). The basic idea is that commercial reader antennas possess a crucial parameter of *input impedance*, which defines the ratio of the voltage and current at the pair of the antenna input terminals, at a specified frequency. Ideally, in order to achieve a maximum power transfer, manufacturers always expect to make the antenna's input impedance purely resistive and perfectly match the *characteristic impedance* of the transmission line (*e.g.*, feeder line). Unfortunately, due to manufacturing imperfections, no two RFID reader antennas could have exactly the same electronic circuits. Each antenna owns its unique IMD that is private, hardware-related and unable to be controlled even by the manufacturers, inherently exhibiting the qualities as a fingerprint. We further utilize a vector network analyzer (VNA) to measure the antenna impedance across channels and verify its feasibility. Moreover, to quantify the impedance mismatch degrees of various antennas, two forms of fingerprints are introduced, namely the coarse-grained ITPA and fined-grained IPS, extracted from the communication link between a pair of reader antenna and tag. Based on this, we can differentiate illegitimate readers by comparing the extracted ITPA and IPS across channels with the registered ones of legitimate devices. In addition, practical environmental varieties in complicated indoor scenarios, including the location and orientation of reader, reader-tag distance and tag heterogeneity, may influence the collected signal features (*e.g.*, phase shifts) and even impair the accuracy of fingerprint validation. To deal with this, we design a series of well-refined fingerprint matching algorithms to circumvent the negative impacts of environmental changes on raw signal features and further the extracted ITPA and IPS. In conclusion, our IMD-based reader authentication system ReaderPrint, only requires an extra COTS tag array to validate hardware fingerprints, and thus is much more universal and low-cost as compared to existing solutions.

Our contributions are summarized as follows:

- To the best of our knowledge, we introduce the first universal solution ReaderPrint to authenticate RFID readers and prevent unauthorized access of illegitimate ones, only using a COTS tag array without customized devices or any modification on the existing C1G2 specification.
- We present two brand-new hardware fingerprints, ITPA and IPS, related to antenna impedance mismatch. By harnessing carefully-designed fingerprint matching algorithms with collected signal features as input, the proposed fingerprints are able to maintain robustness regardless of most environmental factors.
- We implement a prototype of ReaderPrint and evaluate it on 96 readers in three indoor scenarios under different environmental settings. Experimental results demonstrate that our approach can achieve a fairly high authentication accuracy of up to 97.2% and also high resolution to distinguish different readers with the same antenna model.

The rest of this paper is organized as follows. Section II presents two kinds of reader hardware fingerprints along with empirical verification. Section III introduces our system design and fingerprint matching algorithms. We evaluate ReaderPrint in Section IV. Section V overviews the related works of reader authentication and Section VI finally concludes this paper.

## II. Mechanism Verification of ReaderPrint

Antenna manufacturers always utilize simulation tools (*e.g.*, HFSS [14]) to determine electronic components in RF circuits according to the expected antenna performance. However, antenna impedance mismatch is an inevitable phenomenon in real world [15], though reader antenna's input impedance obtained in simulation is pure resistance (*i.e.*, the imaginary

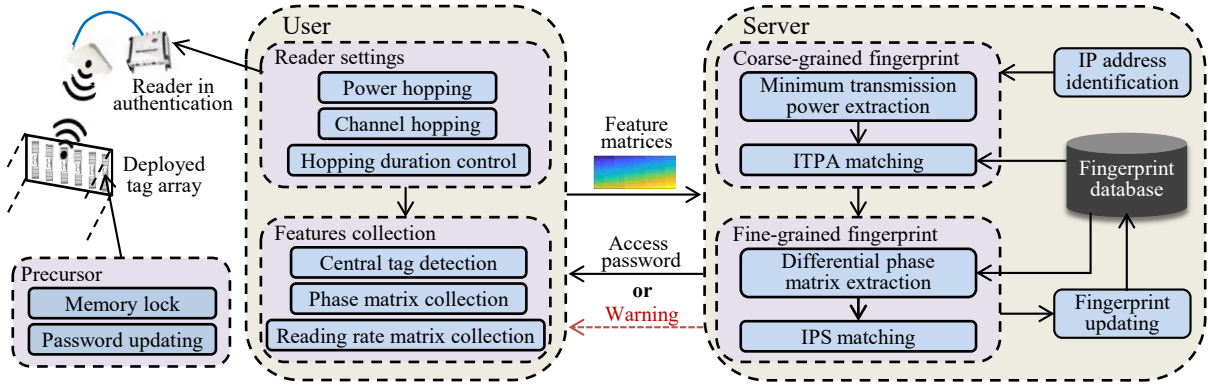



**Fig. 3: System overview of ReaderPrint**

part is zero). The reader antenna's input impedance cannot always match the characteristic impedance of the feeder line connecting the reader's power source, especially on different frequency channels, since the resistors and capacitors shall change with frequency. Due to the manufacturing imperfection of electronic components, no two reader antennas could have exactly the same IMD across channels. Even if manufacturers intend to adjust IMD by altering electronic components, they are unable to control IMD on all channels. Thus, each reader's IMD across channels is unique and private. Standing wave ratio (SWR), another antenna feature representing the capability how much proportion of power transmitted from the feeder line will be reflected, is essentially related to IMD and further incurs attenuation of reader's transmission power to active tags. The ideal situation that SWR equals one on each channel without power attenuation is hard to achieve and no two antennas could have the same ITPA across channels. From another aspect, IMD can induce the time delay of reader's transmitted signal, thereby incurring phase shifts when communication. Similarly, it is almost impossible that IPS on all channels are zero and each two antennas' IPS across channels are different. Both ITPA and IPS can be extracted from signal features COTS devices collect and this provides the probability for fingerprinting readers, as shown in Fig. 2(a).

To verify this mechanism, We utilize a VNA to measure three antennas' input impedance and standing wave ratios as shown in Fig. 2(b), where two antennas' model is E9028PCRNF and Laird S9028PCL (*i.e.*, E9028 and S9028 in the figures) respectively. Fig. 2(d) shows the antenna impedance obtained from smith charts in Fig. 2(c) and we can find that the antennas' IMDs are extremely distinguishable when their models are different. Even if the antenna models are the same, there also exists diversity in antennas' IMDs across channels. Considering the following relationship between IMD and IPS [16], we can compute the theoretical IPS across channels (see Fig. 2(e)) based on the measured antenna impedance. The difference of IPS between two antennas with different models can reach 76.10%, and IPS of the same antenna model can also exist a large diversity of up to 41.97%. Similar to IPS, in terms of measured SWR that demonstrates evident differences as shown in Fig. 2(f), different antennas' ITPA across channels and also their tendencies shall exhibit diversity. Through measurements, we can derive the conclusion that IPS and ITPA across channels show great potential to uniquely fingerprint reader antennas.

## III. System Design

As shown in Fig. 3, our system mainly contains four modules: memory lock, signal features collection, ITPA matching and IPS matching. Memory lock of tags is the precursor module before ReaderPrint works and only readers that pass the follow-up authentication can obtain the access passwords as the evidence of authorization from the server and communicate with tags. Those failing the authentication shall be regarded as illegitimate readers and cannot access the tags without passwords.

The overall workflow of ReaderPrint is sketched below. The first step is to let readers hop power and channels to communicate with a pre-deployed passive tag array. Note that this tag array is only utilized for reader authentication and independent of existing tags in RFID applications. We can find the central tag that the reader faces in the tag array based on the received signal strength (RSS) readings. After that, we collect signal features, *i.e.*, phase matrix and reading rate matrix from the backscatter signals of the central tag. Then, the coarse-grained ITPA fingerprint is extracted from the reading rate matrix and compared to the registered one to filter out illegitimate readers. If the reader passes ITPA matching, we further extract the fine-grained IPS fingerprint from the phase matrix. According to both the ITPA and IPS matching results, the reader's legitimacy could be finally determined. If the reader is valid, we authorize it and send the access passwords; otherwise, the user shall receive a warning message. More details about each module are introduced in the following parts.

### A. Memory Lock

In C1G2 protocol, there are four types of tag lock status: unlocked, permanently unlocked, locked and permanently locked. Most tags lie in unlocked status, where any illegitimate reader can read, write or kill them if no operations are conducted. Permanently unlocked status is similarly vulnerable. Although permanently locked status can prevent the tags from malicious

attacks, this also makes legitimate readers unable to access tags, which limits many RFID functions (*e.g.*, scanning goods' expiration dates stored in tags' user memory bank [17], or inventorying tags' TID for valuables anti-counterfeiting). Therefore, the most reasonable status is locked but not permanently locked, where only authorized readers owning the correct 32-bit access password can access the tags. Regularly updating the password can also prevent brute-force attacks. This basic idea is adopted by some industrial applications and ReaderPrint as well.

However, authorizing readers only by checking their MAC/IP addresses is insecure since adversaries may forge a valid address to pass authentication. Thus, it is necessary to extract hardware fingerprints as the readers' uncloneable identifies for authentication.

### *B. Reader Setting and Feature Collection*

To extract feature matrices related to ITPA and IPS, we need to manipulate the reader to hop power and channels respectively. Taking ImpinJ R420 reader [18] in china region as an example, the power settings can range from $10\,\text{dBm}$ to $31\,\text{dBm}$ with a step length of $0.25\,\text{dBm}$ and the channel settings can range from $920.625\,\text{MHz}$ to $924.375\,\text{MHz}$ with a step length of $0.25\,\text{MHz}$. However, there exists a challenge that the query duration on the first few channels or last few channels may not be equal to others due to the hopping delay and undetermined query ending period, incurring inaccurate reading rate results. So, the total query duration of reader that can be preset, denoted as $T$, should be well controlled. We fix the Q value [19], set the antenna power to a large value, query the tags and record the query times on the $i$-th channel as $h_i(T)$. Then we try to optimize $T$ via binary search to achieve the minimum variance of query times as follows.

$$\hat{T} = \underset{h_l \le h_i(T) \le h_u, i \in [1,N]}{\arg\min} \sum_{i=1}^{N} \left( h_i(T) - \frac{1}{N} \sum_{k=1}^{N} h_k(T) \right)^2 \quad (1)$$

where $N$ denotes the number of hopped channels. $h_l$ is a lower bound to ensure that the last few channels are hopped and $h_u$ is an upper bound to avoid long query latency.

After reader settings, we collect the tag array's backscatter signals. Since the location of reader is unknown and more than one tag shall respond, we consider to find the central tag that the reader faces to evade the impacts of reader location on the following authentication. This also explains the reason why we need a tag array, rather than a single tag. Notice that the distance between the central tag and the reader is shortest and the antenna directivity towards the central tag is largest [15]. Thus the RSS readings of the central tag's backscatter signals should also be the largest among all the tags. Based on this, we detect the central tag in the array by selecting the one with the highest mean RSS value. We then exploit the `Select` command to filter out other tags and collect features only from the central tag, by setting its inventoried flag. Specifically,

$$\texttt{Select}\ (1,\ 4,\ 1,\ 32,\ 96,\ \texttt{Mask}). \quad (2)$$

Here the `Mask` field is set as the central tag's EPC.

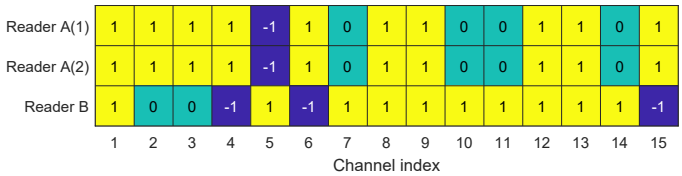



**Fig. 4: Two readers' changing tendency of ITPA. The first two rows show the similar experiment results of reader A at different locations. The last row shows the massive gap between reader A's ITPA and reader B's ITPA, even when the locations of two readers are same.**

Let $M$ be the number of hopped power levels, $r_{i,j}$ and $\theta_{i,j}$ be the reading rate and average phase value on the $i$-th channel with the $j$-th power respectively. After collecting signal features, we filter out useless phase data, *i.e.*, corresponding $r_{i,j} = 0$, and acquire the reading rate matrix $\mathbf{R}$ and phase matrix $\mathbf{\Theta}$ as below.

$$\mathbf{R} = \begin{pmatrix} r_{1,1} & \cdots & r_{1,M} \\ \vdots & \ddots & \vdots \\ r_{N,1} & \cdots & r_{N,M} \end{pmatrix}, \mathbf{\Theta} = \begin{pmatrix} \theta_{1,1} & \cdots & \theta_{1,M'} \\ \vdots & \ddots & \vdots \\ \theta_{N,1} & \cdots & \theta_{N,M'} \end{pmatrix} \quad (3)$$

Here $M'$ is the number of power levels after removing the useless data.

### *C. ITPA Matching*

After the server receives feature matrices, we try to extract ITPA across channels from $\mathbf{R}$. We first transform $\mathbf{R}$ to the reader's minimum transmission power (MTP) vector $P = \{p_1, p_2, ..., p_N\}$ to active the tag by the following rule: for the $i$-th channel and the smallest $j$ that satisfies $r_{i,j} > 0$, $p_i$ equals the $j$-th power level.

Theoretically, MTP is related to the reader antenna gain $G_r$, tag's energy required for activation $E_t$, reader-tag distance $d$, communication frequency $f$ and other constant factors denoted by $a$ irrelevant to the reader hardware and frequency as follows,

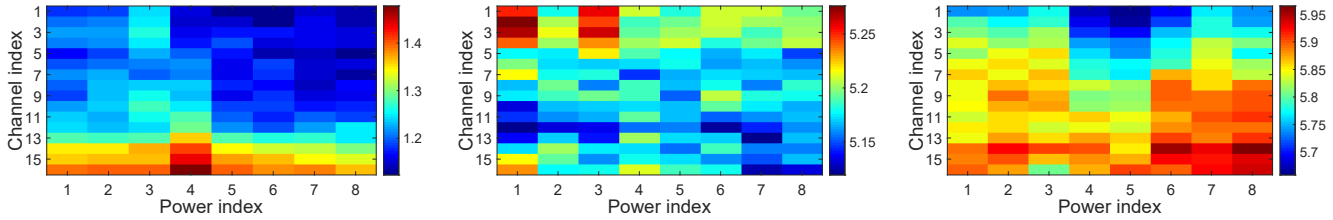
$$p = -2\log G_r(f) + E_t + 2\log d + 2\log f + a. \quad (4)$$

Here $G_r$ is also a function of $f$ and equals the production of *attenuation coefficient* $\eta$ (*i.e.*, ITPA) and directivity [16]. We can circumvent the impacts of $d$ by subtracting the adjacent elements in the MTP vector. That is,

$$p_{i+1} - p_i = -2\left(\log \eta(f_{i+1}) - \log \eta(f_i)\right) + 2\log\left(f_{i+1}/f_i\right), \quad (5)$$

where $G_r$ can be directly represented by $\eta$ since the impact of reader directivity has been removed. Besides, the reader orientation does not affect MPT theoretically [20]. So, the changing tendency of ITPA over channels can be obtained via MPT differences of each adjacent channels.

Practically, due to the low resolution of power levels (*e.g.*, $0.25\,\text{dBm}$), $p_{i+1}$ and $p_i$ may be the same for some channel-pairs. So we make the following rule to compare the magnitude of $p_{i+1}$ and $p_i$ when $p_{i+1} = p_i$: if $r_{i+1,j} - r_{i,j} \ge \delta$, we regard $p_{i+1} < p_i$; else if $r_{i+1,j} - r_{i,j} \le -\delta$, we regard $p_{i+1} > p_i$; otherwise, we regard $p_{i+1} = p_i$. Here $j$ is the corresponding index of MTP and $\delta$ is a pre-defined empirical parameter.




(a) Differential phase matrix of A(1) & A(2) (b) Differential phase matrix of A(1) & B (c) Differential phase matrix of A(1) & C

**Fig. 5: Three reader pairs' differential phase matrices, where A(1) and A(2) denote the same reader's measurements at two locations, B and C are another two different readers, and the antenna model of C is the same with A.**

In this way, we can obtain the magnitude relationship of each $(p_{i+1}, p_i)$. Note that, though $E_t$ may also change with channels and the central tag may not always be the same one, we demonstrate that tag heterogeneity shall not affect the magnitude relationship through extensive experiments. Therefore, it is reasonable to extract ITPA across channels as a coarse-grained fingerprint.

If the reader is legitimate, its ITPA shall be identical to the registered value, *i.e.* the mismatched number of channel-pairs $\epsilon$ should approach zero. Otherwise, the similarity of ITPA would be small. Fig. 4 shows an example of the obtained ITPA over 16 channels from two readers (A and B) in our experiments, where "1" indicates $p_{i+1} > p_i$, "-1" indicates $p_{i+1} < p_i$ and "0" indicates $p_{i+1} = p_i$ for $i = 1, 2, ..., N-1$ ($N = 16$). We can see that different readers' ITPA demonstrate clearly diverse patterns ($\epsilon = 10$), while ITPA of the same reader remains stable ($\epsilon = 0$) regardless of the reader's locations.

We leverage ITPA as a coarse-grained fingerprint to directly filter out some illegitimate readers so that the system latency of ReaderPrint could be reduced. Only those passing ITPA matching can continue to the next step of authentication.

### *D. IPS Matching*

To increase the authentication accuracy of our approach, we try to extract a more fine-grained fingerprint utilizing the phase matrix $\mathbf{\Theta}$. As is known, the RF phase of a tag's backscatter signal reported by commercial RFID readers can be expressed as [20]:

$$\theta_{i,j} = \theta_t(f_i, p_j) + \theta_{IPS}(f_i, p_j) + 2\pi \cdot \frac{2d}{\lambda_i} + \theta_o \bmod 2\pi, \quad (6)$$

where $\lambda_i$ is the wavelength of RFID signals and equals $c/f_i$, $d$ is the distance between the reader and tag, and $\theta_t$, $\theta_{IPS}$ and $\theta_o$ denote the phase rotations introduced by the tag's circuits, reader's hardware and reader's orientation respectively. $\theta_o$ equals the double intersection angle between the polarization directions of the reader antenna and tag, which is independent of channel or power.

We first compute the differential phase matrix of reader by subtracting its registered phase matrix as below.

$$\theta^{\text{dif}}_{i,j} = \theta^{\text{aut}}_{i,j} - \theta^{\text{reg}}_{i,j} = \theta^{\text{aut}}_{IPS}(f_i, p_j) - \theta^{\text{reg}}_{IPS}(f_i, p_j) + \theta^{\text{aut}}_o - \theta^{\text{reg}}_o + \frac{4\pi\,(d^{\text{aut}} - d^{\text{reg}})}{c} \cdot f_i \bmod 2\pi. \quad (7)$$

Here $d^{\text{aut}} - d^{\text{reg}}$ denotes the unknown reader-tag distance difference, $\theta^{\text{aut}}_o$ and $\theta^{\text{reg}}_o$ denote the orientation factors. $\theta^{\text{aut}}_{i,j}$ and $\theta^{\text{reg}}_{i,j}$ are elements in phase matrices for authentication and registration respectively. If the reader to be authenticated is legitimate, the IPS difference $\theta^{\text{aut}}_{IPS}(f_i, p_j) - \theta^{\text{reg}}_{IPS}(f_i, p_j)$ should be zero for each $i$ and $j$. Otherwise, $\theta^{\text{aut}}_{IPS}(f_i, p_j)$ is probably unequal to $\theta^{\text{reg}}_{IPS}(f_i, p_j)$ for any $i$ and $j$.

In this way, we can mitigate the impacts of tag heterogeneity and reader orientation since $\theta^{\text{aut}}_o - \theta^{\text{reg}}_o$ is a constant with no dependency on channel or power. From Eqn. 7, we can derive the following two properties:

- If IPS is matched, $\theta^{\text{dif}}_{i,j}$ would be a linear function of $f_i$, where the gradient relevant to distance difference is unknown but fixed; otherwise, the linearity should not hold.
- If IPS is matched, $\theta^{\text{dif}}_{i,j}$ should be independent of power index $j$, for each $i$; otherwise, there would be differences between $\theta^{\text{dif}}_{i,j}$ and $\theta^{\text{dif}}_{i,u} (u \neq j)$.

Based on these observations, we propose a well-refined IPS matching algorithm. First, we apply linear regression to fit $\theta^{\text{dif}}_{i,j}$ with variable $f_i$ for each $j$ and obtain the fitting function $\gamma_j = \alpha_j f_i + \beta_j$ through the following equation:

$$[\alpha_j, \beta_j] = \arg\min \frac{1}{N} \sum_{i=1}^{N} \left(\alpha_j f_i + \beta_j - \theta^{\text{dif}}_{i,j}\right)^2, \ \forall j. \quad (8)$$

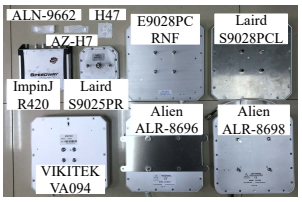
On one hand, we count how many pairs of $\theta_{i,j}$ and $\theta_{i+1,j}$ ($i = 1, ..., N-1, j = 1, ..., M'$) accord with the positive-negative property of $\alpha_j$ and put them into the set $\Omega$. That is, if $\alpha_j \cdot (\theta_{i+1,j} - \theta_{i,j}) < 0$, $\Omega = \Omega \cup \{\theta_{i,j}, \theta_{i+1,j}\}$. On the other hand, we calculate the variance $\sigma$ of $\alpha_j (j = 1, ..., M')$ after normalization to remove the dimensions of reader-tag distance differences.

$$\sigma = \frac{1}{M'} \sum_{j=1}^{M'} \left( \frac{M' \alpha_j}{\sum_{u=1}^{M'} \alpha_u} - 1 \right)^2 \quad (9)$$

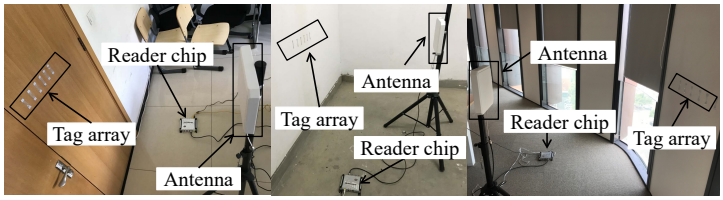
Whatever the reader-tag distance is, according to two properties, the average value of $|\Omega|$ over powers and value of $\sigma$ should both approach zero if IPS is matched. In this way, we can validate the reader legitimacy. For example, Fig. 5(a)$\sim$ 5(c) shows the differential phase matrix of three reader pairs and Table I shows the obtained average $|\Omega|$ and $\sigma$ from them. We can find that the average $|\Omega|$ and $\sigma$ between

**TABLE I: Similarity matching results of three readers**

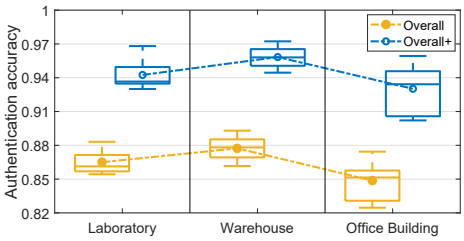
| Metric | A(1) & A(2) | A(1) & B | A(1) & C |
|---|---|---|---|
| Value of $\lvert\Omega\rvert/M'$ | **4.125** | 7 | 4.875 |
| Value of $\sigma$ | **0.05896** | 0.38667 | 0.13548 |
| Value of $\sigma$ (w/ weights) | **0.03965** | 0.39731 | 0.18522 |



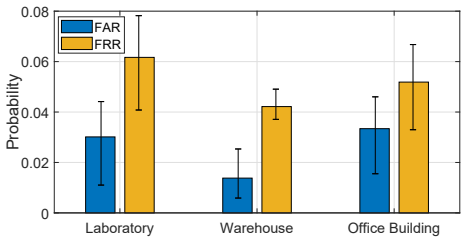

(a) Various RFID devices



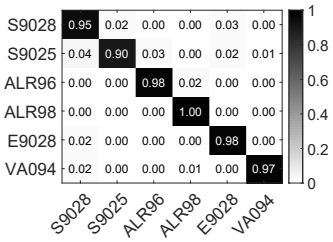

(b) System evaluation in three scenarios: laboratory, warehouse and office building




(c) Authentication accuracy




(d) FAR and FRR




(e) Reader types classification

**Fig. 6: Experiment setup and evaluation results of ReaderPrint**

different readers are much larger than those between same readers of $69.7\%$ and $555.9\%$ respectively. Even if the antenna model is same, we can also differentiate them by $|\Omega|$ and $\sigma$ where the difference ratios are $18.2\%$ and $129.8\%$ respectively.

Moreover, to obtain more robust matching results under environmental multipaths, we can compute the variance of collected phase matrix samples (around 87∼90 samples per second) as confidence level matrix and exploit it as weight in Eqn. 8 and Eqn. 9. After weighting, the difference ratio of $\sigma$ can further reach $902.04\%$. Apart from IPS, based on the confidences, we can also optimize the matching results of ITPA under multipaths by selecting the cleaner channels.

Eventually, with the similarity matching results of ITPA and IPS fingerprints, we can determine the authentication of readers, authorize the valid ones with access passwords for communication and alarm the invalid ones with warnings.

### *E. Practical Issues*

There are two practical issues of ReaderPrint as follows.

First, `Query` command is not a kind of `Access` command [8]. Though ReaderPrint can effectively prevent from unauthorized access, EPC (*i.e.*, tag ID) bank is a special case that cannot resist `Query` operation even if the tag is locked. Nevertheless, the public EPC offers us the opportunity to authenticate readers using tags' backscatter signal features.

Second, ReaderPrint mainly focuses on reader legitimacy to prevent unauthorized access attack. Other conventional security problems inside the system (*e.g.*, data streaming detection) can be solved using existing methods [21] in other fields.

## IV. Implementation and Evaluation

### *A. Prototype Implementation*

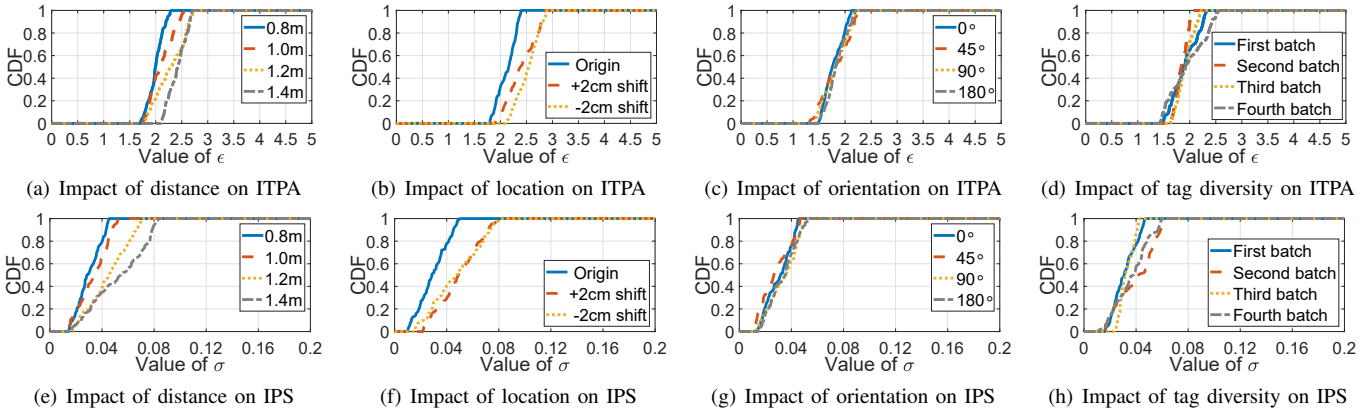
**Hardware:** As shown in Fig. 6(a), we adopt 96 different COTS RFID readers in total (more devices than Arbitrator [7]), consisting of six reader types with eight ImpinJ R420 reader chips and twelve Laird S9028PCL/Larid S9025PR/E9028PCRNF/Alien ALR-8698/Alien ALR-8696/VIKITEK VA094 antennas. Each reader is connected to one localhost through Ethernet, with antenna transmission power ranging from $10.0\,$dBm to $30.0\,$dBm and operating frequency band of $920.625 \sim 924.375$MHz, respectively. The size of deployed tag array is six and tag models include Alien ALN-9662, ImpinJ H47 and NXP AZ-H7 [18], [22].

**Software:** Low level reader protocol (LLRP) [23] is used for communication between localhost and reader, including reader settings and signal features collection. We use Thinkpad PCs equipped with Intel Core i7 CPU at 2.00GHz and 16G memory as the clients and server. The algorithms are developed using Java and Matlab language.

**Experiment setup:** We first evaluate ReaderPrint on the above readers in three scenarios where tag arrays are attached on the wall or door (see Fig. 6(b)), in terms of the following metrics: average authentication accuracy, false accept rate (FAR) that indicates the ratio of illegitimate readers passing authentication, false reject rate (FRR) that indicates the ratio of legitimate readers failing authentication. Next, we control the environmental factors including reader-tag distance, reader location, reader orientation, tag heterogeneity and tag model to verify the robustness of our proposed two hardware fingerprints ITPA and IPS. In the end, we examine the performance under different parameter settings and that over the long term.

### *B. The Overall Authentication Performance*

If a reader is classified correctly by the similarity of our proposed fingerprints, we regard it as a successful authentication. Fig. 6(c) plots the results of authentication accuracy over 200 experiments, respectively in three scenarios. The "Overall" and "Overall+" indicate the accuracy of two cases when matching: whether considering the registered ones with same reader chip/antenna or not. It is reasonable to employ "Overall+" accuracy in real-world applications since illegitimate readers should not have legitimate components generally. We can find that the accuracy in each scenario is fairly high and reach as high as $97.23\%$. The difference between three scenarios' accuracy is probably incurred by diverse multipath effects in indoor environments. The "Overall" accuracy (up to $89.30\%$)




(a) Impact of distance on ITPA (b) Impact of location on ITPA (c) Impact of orientation on ITPA (d) Impact of tag diversity on ITPA

(e) Impact of distance on IPS (f) Impact of location on IPS (g) Impact of orientation on IPS (h) Impact of tag diversity on IPS

**Fig. 7: CDF curves to show robustness of ITPA and IPS under different environmental settings**

is only 8.15% lower than the "Overall+" accuracy, which also implicitly shows the uniqueness of our fingerprints. These positive results all verify the effectiveness of ReaderPrint.

Next, we treat each reader in authentication as illegitimate device and randomly assign it fingerprints of a registered reader whose MAC/IP address is different, thereby measuring the FAR. On the other hand, we treat each reader as legitimate and compare the fingerprints in authentication with its registered ones, thereby measuring the FRR. Fig. 6(d) shows the results of FAR and FRR over 100 experiments in three scenarios. It demonstrates that FAR does not exceed 4.60% and the minimum value reaches 0.59%; FRR is lower than 7.82% and can decrease to 3.30%. Both the FAR and FRR of ReaderPrint is fairly low. In real-world use, FAR is probably more important because legitimate readers can repeatedly request authentication if they fail, but once the illegitimate gets access authorization, great loss would be caused. The trade-off between FAR and FRR is introduced in following subsections.

Then, we study the accuracy of classifying different reader types based on the results in Fig. 6(c). If the obtained category of each reader in authentication is the correct type, we regard it as a successful matching. Fig. 6(e) shows the confusion matrix of matching results. The six reader types are denoted by #1∼#6. We can see that all the matching accuracy is higher than 90% and the ImpinJ R420 reader chip with ALR-8698 antenna reaches the highest accuracy of 100%. The accuracy of Alien antennas is higher than that of ImpinJ antennas, possibly due to the firmware fitness differences. In addition, most error cases are centered at antenna types from the same manufacturer and this also shows the uniqueness of antenna hardware.

### C. The Robustness to Environmental Impacts

We measure the robustness of ReaderPrint using one legitimate reader under different environment settings as follows.

**The impact of reader-tag distance.** As is well known, reader-tag distance exerts great impacts on signal features such as RSS and phase. So, we adjust the distance from 0.8 m to 1.4 m at four levels and observe the CDF curves of $\epsilon$ and $\sigma$ as shown in Fig. 7(a) and Fig. 7(e). It is demonstrated that the CDF curves are similar when reader-tag distance is short, and the mean values of $\epsilon$ are 2.00, 2.17, 2.29 and 2.42 for the four distance levels, while the mean values of $\sigma$ are 0.030, 0.033, 0.045 and 0.053 respectively. The variance is probably caused by stronger multipath effect in larger signal propagation space when the distance is longer. Even so, our fingerprints can generally remain stable within a distance range and the authentication results with default threshold settings of $\epsilon = 3$ and $\sigma = 0.1$ are stationary regardless of reader-tag distance.

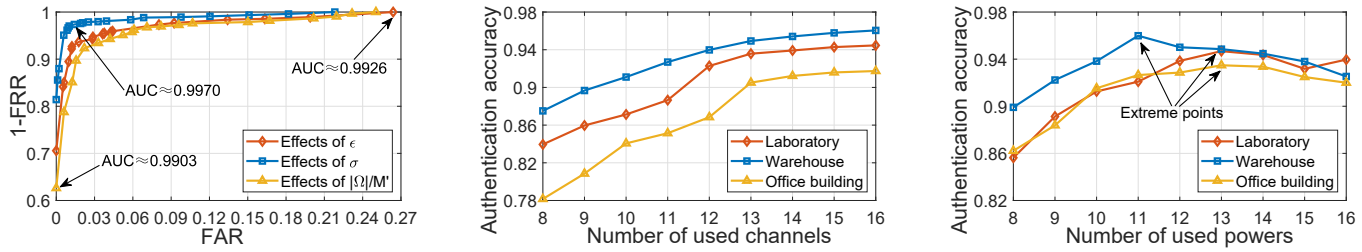
**The impact of reader location.** To measure whether reader location affects ITPA and IPS, we adjust the locations from the original location facing the central tag to new locations with 2 cm positive/negative displacements. Fig. 7(b) and Fig. 7(f) show that the similarity matching performance could be better at the original location but location displacements do not affect the authentication results. Note that the interval between adjacent tags in the array is not restricted because the inductive coupling effect [24] only changes $\theta_t$ which is eliminated in our matching algorithm.

**The impact of reader orientation.** We set the reader orientation to 0°, 45°, 90° and 180°. From Fig. 7(c) and Fig. 7(g), we can find that the CDF curves of $\epsilon$ and $\sigma$ are very close to each other. The mean values $\epsilon$ are 1.79, 1.83, 1.83 and 1.84, while the mean values of $\sigma$ are 0.031, 0.028, 0.033 and 0.033 respectively. The results indicate that reader orientation has very little impact on our fingerprints. Note that this conclusion can be applied to all reader antenna models because whatever the antenna polarization mode is, it can be approximated to the superposition of two orthogonal linear-polarization that exerts only a constant effect on phase shifts.

**The impact of tag heterogeneity.** Finally, we exam the stability of ITPA and IPS under different tags. On one hand, we alternate four batches of tags with the same tag model for measurement. Fig. 7(d) and 7(h) show the obtained CDF curves that are similar to each other. On the other hand, we change the tag models for measurement respectively and Table II shows their mean $\epsilon$ and $\sigma$ that are consistent with

**TABLE II: Impact of tag models on ITPA and IPS**

| Fingerprint | Alien AZ-9662 | ImpinJ H47 | NXP AZ-H7 |
|---|---|---|---|
| Mean $\epsilon$ | 1.993 | 1.781 | 2.147 |
| Mean $\sigma$ | 0.0259 | 0.0391 | 0.0530 |
| Accuracy | 95.11% | 94.08% | 87.20% |




(a) ROC curves vs. different thresholds settings (b) Impact of used channels' quantity (c) Impact of used powers' quantity

**Fig. 8: Effects of different parameter settings including thresholds and channels/powers' quantities**

each other, with the differences less than $0.366$ and $0.0271$ respectively. The results demonstrate that our fingerprints are resistant to tag heterogeneity.

From the above evaluation, we verify that ReaderPrint can work under many different environmental settings and maintain high accuracy and robustness.

### *D. Effects of Different Parameter Settings*

First, we adjust the similarity matching thresholds of $\epsilon$ (from $0$ to $8$), $|\Omega|/M'$ (from $0$ to $8$) and $\sigma$ (from $0.01$ to $0.3$) respectively, and repeat the same experiments above to obtain FAR and FRR. The receiver operating characteristic (ROC) curves are plotted in Fig. 8(a). We can see the trade-off between FRR and FAR, that is, FRR degrades with the growing value of FAR. It is reasonable because when the threshold is small, a legitimate reader may fail authentication though the risk of illegitimate reader passing authentication can be lowered. Taking the effect of $\sigma$ as an example, FRR is below $4.01\%$ when FAR exceeds $0.84\%$. We find that when FAR ranges from $0.93\%$ to $3.94\%$, FRR is always less than $4\%$, and both FAR and FRR are extremely low. Besides, the areas under curve (AUC) of each parameter $\epsilon$, $|\Omega|/M'$ and $\sigma$ all approach one and this demonstrates extremely high classification capability of ReaderPrint. The AUC of $\sigma$ is evidently larger than that of $\epsilon$ or $|\Omega|/M'$, which reveals that $\sigma$ is the most effective fingerprint. In fact, FAR indicates the diversity of reader fingerprints and FRR indicates the stability. We can see that in corner cases of thresholds settings, the maximum FRR $37.37\%$ is higher than the maximum FAR $26.39\%$. This reveals that the stability of legitimate readers' fingerprints is the major concern when authentication, considering the impacts on raw signal features from environmental noises.

Second, we measure the effects of selected channels and power levels respectively. Fig. 8(b) shows that more channels used would result in higher authentication accuracy, which conforms to our intuition that the hardware differences are enlarged with more channels. The authentication accuracy can be promoted by up to $13.58\%$ when the number of adopted channels ranges from $8$ to $16$. So, we recommend users to hop more channels. Different from channel hopping, more power levels may not increase the authentication accuracy, as shown in Fig. 8(c). The accuracy initially grows with the increasing number of power levels but declines later, and the maximum accuracy can be promoted by $9.05\%$. This is probably due to more severe multipath effects when transmission power becomes larger. In addition, when more channels or powers are used, the authentication latency shall be prolonged inevitably and the trade-off forms a part of our future work.

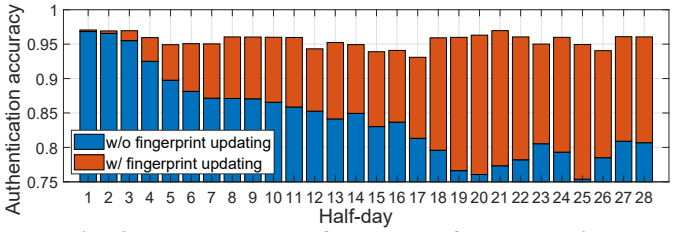



**Fig. 9: Long-term performance of ReaderPrint**

### *E. Long-term Performance*

To evaluate the long-term performance of ReaderPrint, we conduct a 14-days experiment where each reader is authenticated ten times per day. The fingerprint database is automatically updated when readers pass authentication and artificially updated per half-day to avoid accumulative errors. As shown in Fig. 9, the authentication accuracy with fingerprint updating maintains nearly $95\%$ even after two weeks, whereas the accuracy without fingerprint updating by only using the registered fingerprints on the first day degrades over time to less than $80\%$, probably due to the device aging and re-assembly phenomena that lead to the changes of IMD. This indicates the necessity of fingerprint updating to alleviate the impacts of device condition changes over the long term.

## V. Related Work

Past literature related to reader authentication can be classified into the following two categories.

**Cryptography-based solutions.** In the early stage, most works prefer exploiting cryptographic algorithms to encrypt the plaintext to avoid eavesdropping or tampering attacks. For example, some works utilize symmetric encryption algorithms [11] or physical uncloneable functions [12] to achieve mutual authentication. However, none of these cryptography-based solutions are realistic in real-world applications. This is because commodity tags cannot support such high computation cost [15], thereby necessitating hardware modifications, on one hand; they need to modify C1G2 protocol that most commodity tags follow, thereby making them incompatible with existing RFID infrastructure, on the other hand.

**Hardware fingerprint-based solutions.** Recent works explore the RFID devices' hardware diversity induced by man-

ufacturing imperfection and unique physical-layer signal features related to hardware diversity are leveraged as fingerprints for authentication [25]–[28], where most of them focus on tag anti-counterfeiting and few consider RFID reader legitimacy. In fact, many counterfeit attacks on tags are caused by illegitimate readers' unauthorized access that happens earlier and imperceptibly. Thus, reader legitimacy is the foremost problem to solve. The state-of-the-art works for reader authentication are Arbitrator [7] and Arbitrator2.0 [13], which solve this problem using universal software radio peripheral (USRP) devices as monitors to extract physical-layer fingerprints. However, Arbitrator is very hard to deploy in real world because SDR devices are always needed to locate nearby readers in authentication. On one hand, SDR devices themselves incur extra high deployment, operation and maintenance overhead. On the other hand, once the reader-tag distance is short (*e.g.*, $\leq$0.8m), the reader's transmission power is low (*e.g.*, $\leq$12dBm) or multiple readers simultaneously access, Arbitrator can not work with a finite number of SDR devices. Otherwise, countless SDR devices are needed. In addition, other works such as URTracker [29] can only judge whether the unauthorized access happens, but fail to validate the readers' legitimacy.

**Comparison.** Compared to cryptography-based solutions, hardware fingerprint-based solutions can have higher ubiquity. However, the state-of-the-art solution Arbitrator still needs SDR devices deployment and remains many limitations. Our solution, ReaderPrint extracts hardware fingerprints only from signal features COTS devices can collect, thereby greatly improving the ubiquity and further lowering the overhead, though it can not actively interrupt the access of illegitimate readers like Arbitrator. Besides, ReaderPrint can support simultaneous authentication of multiple readers and retain higher parallelism than Arbitrator. Comprehensively, ReaderPrint is a universal, low-cost and effective solution for reader authentication.

## VI. Conclusion

In this work, we present two brand-new hardware fingerprints of RFID readers related to antenna impedance mismatch and the first universal, low-cost and effective system ReaderPrint to authenticate readers with well-refined fingerprint matching algorithms and defend against unauthorized access, only requiring an extra COTS tag array. ReaderPrint is fully compatible with C1G2 protocol and existing commercial RFID infrastructure, making it a promising system for real-world deployment. Experiments show the fairly high authentication accuracy of up to $97.2\%$ and also high resolution to distinguish readers with the same antenna model. We believe ReaderPrint explores a new view to extract hardware fingerprints and can boost the development of RFID authentication systems.

## Acknowledgment

This work is supported partially by the National Key Research and Development Program of China (Grant No.2018YFB0803403), the National Natural Science Foundation of China (Grant No.61902212), and the Beijing Institute of Technology Research Fund Program for Young Scholars.

## References

[1] C. Duan, J. Liu, X. Ding, Z. Li, and Y. Liu, "Full-dimension relative positioning for rfid-enabled self-checkout services," *Proceedings of the ACM IMWUT*, vol. 5, no. 1, pp. 1–23, 2021.
[2] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-time tracking of mobile rfid tags to high precision using cots devices," in *Proceedings of ACM MobiCom*, 2014, pp. 237–248.
[3] Z. An, Q. Lin, X. Zhao, L. Yang, D. Zheng, G. Wu, and S. Chang, "One tag, two codes: identifying optical barcodes with nfc," in *Proceedings of ACM MobiCom*, 2021, pp. 108–120.
[4] A. Juels, "Rfid security and privacy: A research survey," *IEEE JSAC*, vol. 24, no. 2, pp. 381–394, 2006.
[5] D. Zanetti, B. Danev, and S. Mapkun, "Physical-layer identification of uhf rfid tags," in *Proceedings of ACM MobiCom*, 2010, pp. 353–364.
[6] J. Li, C. Wang, A. Li, D. Han, Y. Zhang, J. Zuo, R. Zhang, L. Xie, and Y. Zhang, "Rf-rhythm: Secure and usable two-factor rfid authentication," in *Proceedings of IEEE INFOCOM*, 2020, pp. 2194–2203.
[7] H. Ding, J. Han, Y. Zhang, F. Xiao, W. Xi, G. Wang, and Z. Jiang, "Preventing unauthorized access on passive tags," in *Proceedings of IEEE INFOCOM*, 2018, pp. 1115–1123.
[8] E. Global, "Specification for rfid air interface epc radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz-960 mhz," Technical report, GS1, Tech. Rep., 2008.
[9] "Hainan airlines," https://www.hainanairlines.com/US/US/Home.
[10] "Decathlon," https://www.decathlon.co.uk/.
[11] T. Van Le, M. Burmester, and B. De Medeiros, "Universally composable and forward-secure rfid authentication and authenticated key exchange," in *Proceedings of ACM ASIACCS*, 2007, pp. 242–252.
[12] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight mutual authentication and ownership transfer for rfid systems," in *Proceedings of IEEE INFOCOM*, 2010, pp. 1–5.
[13] H. Ding, J. Han, C. Zhao, G. WANG, W. Xi, Z. Jiang, and J. Zhao, "Arbitrator2.0: Preventing unauthorized access on passive tags," *IEEE TMC*, 2020.
[14] Z. Cendes, "The development of hfss," in *Proceedings of IEEE USNC-URSI Radio Science Meeting*, 2016, pp. 39–40.
[15] D. M. Dobkin, *The RF in RFID: UHF RFID in practice*. Newnes, 2012.
[16] S. Pradhan and L. Qiu, "Rtsense: Passive rfid based temperature sensing," in *Proceedings of ACM SenSys*, 2020, pp. 42–55.
[17] J. Liu, X. Chen, H. Liu, H. Gong, Y. Wang, and L. Chen, "Time-efficient range detection in commodity rfid systems," in *Proceedings of IEEE ICNP*, 2020, pp. 1–10.
[18] "Impinj inc," http://www.impinj.com.
[19] Q. Lin, L. Yang, C. Duan, and Z. An, "Tash: Toward selective reading as hash primitives for gen2 rfids," *IEEE/ACM ToN*, vol. 27, no. 2, pp. 819–834, 2019.
[20] C. Jiang, Y. He, X. Zheng, and Y. Liu, "Omnitrack: Orientation-aware rfid tracking with centimeter-level accuracy," *IEEE TMC*, vol. 20, no. 2, pp. 634–646, 2019.
[21] J. M. Kizza, *Computer network security*. Springer Science & Business Media, 2005.
[22] "Alien technology," http://www.alientechnology.com.
[23] E. EPCglobal, "Low level reader protocol (llrp)," 2010.
[24] J. Guo, T. Wang, Y. He, M. Jin, C. Jiang, and Y. Liu, "Twinleak: Rfid-based liquid leakage detection in industrial environments," in *Proceedings of IEEE INFOCOM*, 2019, pp. 883–891.
[25] J. Han, C. Qian, Y. Yang, G. Wang, H. Ding, X. Li, and K. Ren, "Butterfly: Environment-independent physical-layer authentication for passive rfid," *Proceedings of the ACM IMWUT*, vol. 2, no. 4, pp. 1–21, 2018.
[26] X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Eingerprint: Robust energy-related fingerprinting for passive rfid tags," in *Proceedings of USENIX NSDI*, 2020, pp. 1101–1113.
[27] 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 *Proceedings of IEEE INFOCOM*, 2015, pp. 1966–1974.
[28] C. Zhao, Z. Li, T. Liu, H. Ding, J. Han, W. Xi, and R. Gui, "Rf-mehndi: A fingertip profiled rf identifier," in *Proceedings of IEEE INFOCOM*, 2019, pp. 1513–1521.
[29] D. Sun, Y. Cui, Y. Feng, J. Xie, S. Wang, and Y. Zhang, "URTracker: Unauthorized reader detection and localization using COTS RFID," in *Proceedings of WASA*. Springer, 2021, pp. 339–350.