RF-Mehndi: A Fingertip Profiled RF Identifier

Cui Zhao*‡†, Zhenjiang Li§, Ting Liu†*, Han Ding*, Jinsong Han¶‖, Wei Xi*, and Ruowei Gui*‡
*School of Electronic and Information Engineering, Xi'an Jiaotong University, China
†Ministry of Education Key Lab for Intelligent Netwroks and Network Security
‡Shaanxi Provincial Key Laboratory of Computer Network
§Department of Computer Science, City University of Hong Kong, Hong Kong
¶Institute of Cyberspace Research, College of Computer Science and Technology, Zhejiang University, China
‖Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies

***Abstract*—This paper presents RF-Mehndi, a passive commercial RFID tag array formed identifier. The key RF-Mehndi novelty is that when the user's fingertip touching on the tag array surface during the communication, the backscattered signals by the tag array become user-dependent and unique. Hence, if we enhance the communication modality of many personal cards nowadays by RF-Mehndi, in case that a card gets lost or stolen, it cannot be used illegally by the adversaries. To harvest such a benefit, we have two key observations in designing RF-Mehndi. The first observation is when tags are nearby, their interrogated currents can change each other's circuit characteristics, based on which unique phase features can be obtained from backscattered signals. The second observation is that when the user's fingertip touches the tag array surface during communication, the phase feature can be further profiled by this user. Based on these observations, the card and its holder can be potentially authenticated at the same time. To transfer the RF-Mehndi idea to a practical system, we further address technical challenges. We implement a prototype system. Extensive evaluations show the effectiveness of RF-Mehndi, achieving excellent authentication performance.**

I. Introduction

Nowadays people likely own a bank of personal cards. With a proliferation of the miniature chips inside these cards of near-field communication capabilities, *e.g.*, by Blue tooth [1], radio-frequency identification (RFID) [2], acoustic waves [17], etc., many of them, especially issued by certain associations or organizations, essentially serve as a kind of granted rights for us to access certain restricted spaces (*e.g.*, door entrance card), services (*e.g.*, membership card), e-accounts (*e.g.*, transportation card), etc. This could largely benefit aspects of our daily life. In practice, however, during the authentication process, we can hardly ensure that the current card holder is the legal user, as we lack an *on-site* relation verification for the card itself and holder's identity. Hence, if a card gets lost or stolen (likely to happen), it can be used illegally [4].

A natural countermeasure is to ask for explicitly verifying such a relation, *e.g.*, inputing the card's password as well [13]. However, it suffers two major limitations. First, the authentication can be dramatically slowed down, which may not be acceptable in many applications with a latency concern, *e.g.*, the e-payment. Second, this verification is a "loose" protection. For instance, if the password is compromised by an adversary, the card can still be illegally used as well. Moreover, multiple cards of one user may share the same password. Once the password is compromised, a potential security risk rises for a batch of cards. Of course, we can introduce some advanced sensors to replace the passwords, which, however, naturally lead to the high costs of system deployment and maintenance.

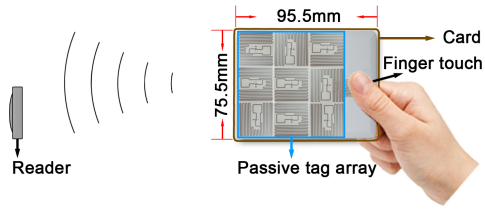


Fig. 1. Illustration of RF-Mehndi design. With a fingertip on the RF-Mehndi tag array, the backscattered signals convey user-dependent and unique features, so that the card and the holder's identity can be authenticated simultaneously.

In this paper, we make a pioneer attempt aiming to tackle this crucial issue in practice, by designing an RFID tag array based solution, as illustrated in Fig. 1, which can be easily attached to various types of cards. As we use *passive* commercial off-the-shelf (COTS) RFID tags and leverage their near-field capabilities, we envision this design can be conveniently integrated into smart card systems in near future.

The key novelty of this paper is that with our proposed techniques, when the user has a simple fingertip touching on the tag array surface (beneath a thin film to protect the tags' circuits) during the authentication, as illustrated in Fig. 1, the backscattered signals by the tag array become *user-dependent* and *unique*. Thus, if the system database has such a record, we can authenticate both the card and its holder simultaneously. In this case, even the card gets lost, it cannot be used illegally, as another person's touching will generate a different identifier or fingerprint, and thus cannot pass the authentication.

To harvest such a promising opportunity, we present RF-Mehndi in this paper with two key technical components. We first observe an interesting inductive effect for a group of tags nearby, *e.g.*, in a tag array. It suggests that when tags are in a vicinity, their interrogated currents (by reader) could change each other's circuit characteristics. As a result, we could obtain unique phase features from the received backscattered signals. Moreover, we further observe that after the user has a fingertip touching the tag array during its communication to the reader, the unique phase features can be further profiled (reshaped) by this user. Such a phase feature reshaping is user-dependent and unique, as the fingertip introduces a user-specific impedance

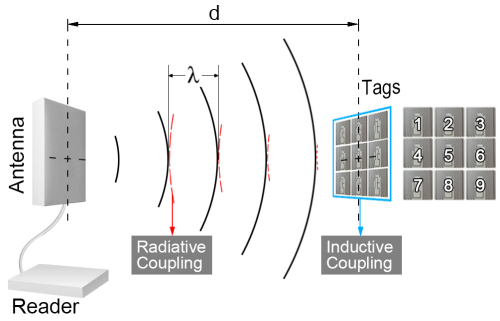


Fig. 2. Radiative coupling and inductive coupling of RFID tags.

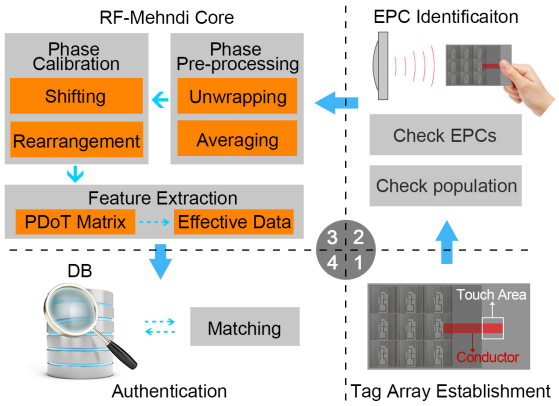


Fig. 3. The working flow of the RF-Mehndi system.

to the tags' circuits. As a result, the card and its holder can be authenticated simultaneously.

In addition to the innovate designs above, we also address a series of technical challenges to transfer the RF-Mehndi idea to a practical system. In particular, to extract the tag array's phase features, we propose an effective mechanism to exclude the impact of the distance between the reader and card. This can largely improve the design reliability and applicability. On the other hand, to profile the tag phase features by user's fingertip touching, we further introduce a conductor-based design to make the user's profiling consistent and robust.

We develop a RF-Mehndi prototype with a COTS RFID reader (Impinj R420), one directional patch antenna (Laird A9028), and several tag arrays formed by a number of passive tags (Alien-9629). As Fig. 1 illustrates, we adopt a 3×3 tag array in our current implementation and its size is only $75.5mm \times 75.5mm$, which can be easily made. The 3×3 array layout can produce more than 260K different unique phase features and the tag array can be authenticated by reader within $30cm$, which is sufficient in practice. Extensive evaluations with 15 volunteers show that RF-Mehndi can achieve promising authentication performance, *e.g.*, with higher than 99% accuracy. In addition, RF-Mehndi can be effectively against crucial attacks, like counterfeiting and impersonation attacks.

In summary, the contributions of this paper are as follows:

- We propose a fingertip profiled identifier using a passive RFID tag array to authenticate both its associated card and the holder's identity simultaneously.
- We leverage two insightful observations to enable the RF-Mehndi design and address a set of technical challenges to obtain a reliable and robust RF-Mehndi identifier.
- We develop a RF-Mehndi system and conduct extensive experiments to evaluate its performance. The results demonstrate the effectiveness of our design.

The rest of this paper is organized as follows. Section II states the design preliminary, system architecture and attack model. The RF-Mehndi design is detailed in Section III and we evaluate its performance in Section IV. Related works are reviewed in Section V before the conclusion Section VI.

II. Design Background and Overview

In this section, we introduce the design preliminary (§II-A), system architecture (§II-B) and attack model (§II-C).

A. Design Preliminary

Coupling of RFID Tags. In RFID systems, readers and tags communicate through the method of electromagnetic coupling. Coupling is to transfer the electrical energy from one device to another. There are two kinds of coupling in RFID systems: *inductive* and *radiative* couplings. The way that two circuits couple can determine the reading range of the system.

Inductive coupling: Inductive coupling employs the magnetic field of the device, which means that this coupling only occurs in the near field, *e.g.*, $1cm \sim 1m$.

Radiative coupling: Radiative coupling is also called backscatter. Most Ultra High Frequency (UHF) RFID systems use the backscatter to communicate between tag and reader. Backscatter is actually a communication method. Electromagnetic waves (*e.g.*, RF energy) are sent through the air from the reader antenna to activate the RFID tag. The tag modulates the information and reflects certain amount of energy back to reader. UHF tags that use backscatter can reach the read range of up to $6m$ in the indoor environments.

UHF Tag Structure. Generally, the tag can be divided into two components: the Integrated Circuit (IC) and the antenna. Most UHF tag antennas are designed with a dipole-type structure. The typical size for a half-dipole is around a half of the wavelength ($16cm$). To shorten the length, the Modified Half-Dipole is widely used, among which *Meander* is characterized by folding the antenna wires back and forth. As shown in Fig. 5, Alien-9629 SQUARE INLAY is a widely adopted RFID tag. With the meanders on the tag, Alien-9629 can keep the actual wire within the size of $2.25cm^2$.

Near-field capability: We note that UHF tag which has a small loop-shaped antenna in the middle will have near-field capabilities. In other words, the small loop antenna will act as a near-field antenna, *i.e.*, tags of this type will couple inductively to a nearby similar inductive tag. Hence, when UHF tags are placed in close proximity, both two types of coupling (*i.e.*, induction and backscatter) are present. As shown in Fig. 2, tags in our system will couple inductively to each other by loop antenna, and radiatively (backscatter) to the reader antenna by meanders. In §III, we leverage this phenomenon in the design.

B. System Architecture

Fig. 3 depicts the working flow of our proposed RF-Mehndi system, including the following 4 key steps.

• *Tag Array Establishment.* To use RF-Mehndi, we first need to establish an array of RFID tags, following certain layouts. Given each layout, RF-Mehndi also connects a conductor to one of the tags for providing a fixed touching area. The tag array is beneath a thin film to protect their circuits.

• *EPC Identification.* The reader interrogates the tag array following the EPC Gen 2 protocol [7], extracting information such as the tag ID and phase. The information is forwarded to backend PC to conduct the subsequent processing. RF-Mehndi checks the IDs and tag population for preliminary verification, *i.e.*, if such meta information is incorrect, the authentication can be early rejected without the following processing.

• *Phase Calibration and Fingerprint Extraction.* This step aims to tackle the phase's random jumping, removes the phase periodicity caused by the distance and prepares to extract the final phase-based identifier.

• *Authentication.* RF-Mehndi measures the extracted identifier and validates the user's identity with the stored records in the database. If the authentication is successful, both the tag array and holder's identity are verified at the same time.

C. Attack Model

We consider an attacker who attempts to steal the private information or impersonate the target user to conduct unauthorized operations. Specifically, we consider the following three popular and crucial categories of attacks.

• *Counterfeiting attack.* The attacker might be aware of the tag array's layout (*e.g.*, the number of tags and their relative locations) of an authorized user's credential (*i.e.*, the tag array) in advance. Then the attacker can make a replica with the same type of tags and layout to launch the attack.

• *Impersonation attack.* The attacker stealthily got the target user's credential and attempts to use the victim's tag array to hijack the authentication system.

• *Replay attack.* The attacker can be more advanced, trying to record the signals when the target user uses RF-Mehndi, and then retransmitting the recored signals to the system.

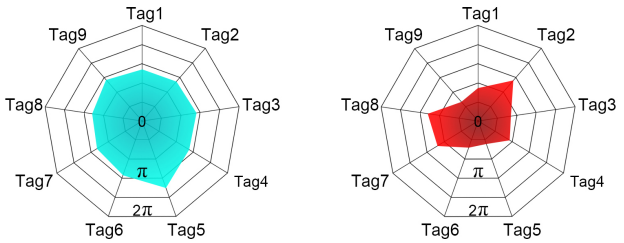
III. RF-Mehndi Design

In this section, we elaborate the RF-Mehndi design. We first extract the phase feature from the tag array (§III-A) and then incorporate the user's uniqueness (§III-B). Afterwards, we propose an effective algorithm to convert phase features to reliable identifier (§III-C), used for the authentication (§III-D).

A. Phase Feature from a Tag Array

Passive RFID tags communicate with the reader by backscattering. During the communication, the reader can acquire the tag information, including ID, RSS, and Phase. As illustrated in Fig. 2, the phase offset between the reader and tag depends on the round-trip transmitted distance ($2d$), as well as hardware-specific characteristics, which can be represented as:

$$\theta = (\frac{4\pi d}{\lambda} + \theta_{reader} + \theta_{tag}) \mod 2\pi, \quad (1)$$



(a) Phase of individual tags (b) Coupling phase of these tags

Fig. 4. Phase distribution w./w.o. inductive coupling by nearby tags.

where λ is the wavelength, and θ_{reader} and θ_{tag} denote the additional phase rotation induced by the reader's and tag's circuits, respectively [3].

1) Coupling Phase of a Tag Array: The basic idea of our system is to form a tag array as the authentication credential. Considering the 3×3 tag array in Fig. 2, we define that X-axis is parallel to the direction from the reader antenna plane to the center of the tag array. According to the standard phase-distance model (Eq. 1), phases of the tags in the array highly depend on the distance. We conduct experiments to investigate the model. We place the tag array 30cm away (along X-axis) from the reader antenna and collect each individual tag's phase one by one. The environment has tables and chairs around. Fig. 4(a) plots the corresponding phases. Since the distance difference between the reader to each individual tag is small, their phases appear almost alike (*i.e.*, around 3.5 radians).

The interesting observation in this measurement is that the phase of each tag changes distinctly, when it is placed close to other tags. As in Fig. 4(b), the phase jumps from 1.57 to 3.42 radians, which demonstrates that coupling from nearby tags will induce significant phase changes. The result also suggests coupling takes the dominant impact than the multipath effect.

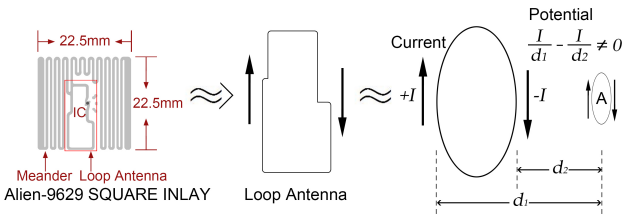
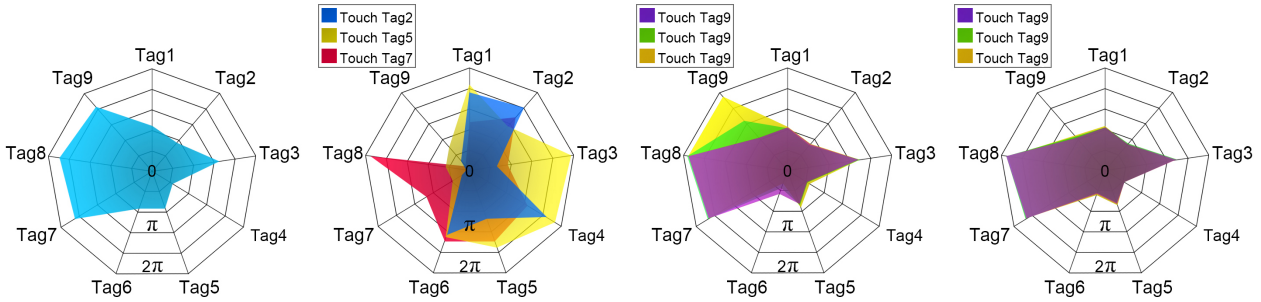


Fig. 5. Equivalent circuit of a tag due to the coupling effect.

Why does the phase change due to coupling? During the communication, the impinging waves from the reader antenna creates a voltage (as well as current) on the tag antenna. To the loop antenna part, the current from one side of the loop is with the same magnitude as that on the other side (of an opposite direction). Thus, the potentials from these two currents cancel with each other. However, when other loop antennas are close in distance, the backscattered signals will be changed.

An example is shown in Fig. 5. Suppose a second loop locates at position A, where A has offsets to the left and right



(a) Tags untouched (b) Touch different tags (c) Touch Tag9 three times without conductor (d) Touch Tag9 three times with conductor

Fig. 6. Tag phase changes w./w.o. the user's fingertip touching.

part of the existing loop by d_1 and d_2, respectively. Since the potential from the nearest part (*e.g.*, right part) of the loop is larger than another part, a significant residual potential exists. This potential can create an additional voltage to the second antenna, and affects this tag's backscattered electric field and signal, resulting in the changes of both phase and magnitude. In §III-C, we further show that very concrete phase features can be extracted based on this phenomenon.

2) Harnessing coupling phase effect: RF-Mehndi harnesses this effect using a tag array in RF-Mehndi. Therefore, we need to carefully design the array layout by considering:

Size of the array. The wavelength in a passive RFID system is about $32cm$. Thus, to reduce the probability that two tags in the array share the same phase, the maximum distance of any two tags should be within half of wavelength (due to the phase singularity) [3]. The tag we adopted (*e.g.*, Alien-9629) is $22.5mm$ long, implying we could arrange at most 7×7 tags.

Complexity of the coupling. In general, the coupling effect of loop antenna is substantial only for distances on a similar order of the loop size. For our design, more significant coupling each tag experiences, more unpredictable of its backscattered phase will be. Thus, we prefer to shorten the distance between tags for strengthening the coupling effect.

By considering above two criteria together, in our prototype of RF-Mehndi, we adopt a 3×3 tag array. The benefits are twofold. First, for portability, according to our experience, this array is smaller than the general size of personal cards or badges, so that it can be easily adopted in practice. Second, for complexity, the distance between all tags is minimized that phases of tags become more complex. In the rest of the paper, we use the 3×3 tag array to instrument our design, while the design principle can be directly applied to other configurations.

Note that the 3×3 tag array leads to 4^9 = 262,144 kinds of effective layouts (*e.g.*, each tag has four placement directions), implying 262K different phase features that can be potentially extracted. In other words, this tag array can support more than 262K users. We believe it is an acceptable population for most systems in practice.

B. Introducing Human Impedance

To further profile the phase changes by the individual users, we need to introduce user-specific characteristics into the backscattered signals. To this end, we find that when a user's fingertip touches the surface of a tag, its backscattered signal will change accordingly. To show how fingertip touch impacts tags' phases, we conduct a new proof-of-concept experiment.

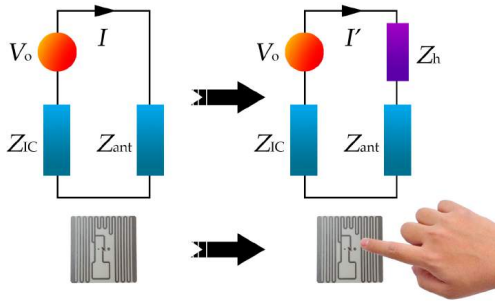


Fig. 7. Equivalent circuit of a tag w./w.o. the fingertip touching.

We place one 3×3 tag array in front of the reader antenna, about $25cm$ away. Fig. 6(b) shows the phases of 9 tags when the volunteer touches Tag 2, 5, 7 respectively. Compared with Fig. 6(a), phases change significantly when the finger touch is applied. Notice that not only the touched tag's phase changes, other tag phases change as well. The amount of change varies cross tags, either increases or decreases. The result suggests the fingertip touch indeed causes additional phase changes.

Why does phase change with fingertip touch? The tag can be modeled as an electrical circuit [5] with a voltage source V_0 connects the IC impedance Z_{IC} and antenna impedance Z_{ant}, where V_0 is derived from the incoming RF signal of the reader. The current induced in the tag antenna can be expressed as:

$$I = \frac{V_o}{Z_{IC} + Z_{ant}}. \tag{2}$$

Theoretically, our body can also be regarded as an equivalent resistance and capacitance [19]. When the fingertip touches the tag antenna, an additional impedance Z_h is virtually inserted into the tag circuit, as depicted in Fig. 7. Therefore, the current ($I^{'}$) flows in the tag in this case is changed, resulting in the radiation of the RF signal (both magnitude and phase) from the tag changed as well. In the tag array, due to the coupling among tags, the variation of the touched tag's impedance will also lead to the phase changes of nearby tags. Since the

internal resistances of different users are not the same, *e.g.*, varying about 300∼1,000 Ohms [15], which brings the chance to further distinguish different users.

One natural question then is *how to ensure the impedance consistency of the same person*? Extensive studies in biomedical science have shown that human impedance mainly depend on a series of factors, like body mass, age, muscles, skin, *etc.* Although the overall impedance of one person may gradually change (due to the varying of some factors), it has a minimal impact to RF-Mehndi. Because the effective impedance in Fig. 7 from the user is mainly due to a limb end local area, *i.e.*, fingertip. Its biometric features are simple, *e.g.*, a small part of the skin resistance, which hardly lead to obvious changes [9]. The introduced impedance is thus relatively stable, and our extensive evaluations also support this point as well.

However, even the introduced impedance from fingertip in principle is stable, there is still a practical challenge that can significantly impair the final consistency — the fingertip cannot be ensured to touch exactly the same position on the tag array, which however could incur further inconsistence. As shown in Fig. 6(c), Tag 9 (at bottom right corner) is touched 3 times (the user tries her best to touch the same location). The resulting phase changes are similar, whereas they are different (insufficient to confidently identify this user).

To overcome this issue, we propose to introduce a conductor to attach with the tag array. The conductor connects to a constant position of one tag antenna and extends outside of the array. The exposed area of the conductor fits the fingertip size to ensure a reliable touching. With this design, phase variations of the array will be overwhelmed by the introduced impedance that is distinguishable for different users. Thus, if an attacker uses an authorized user's tag array to cheat the system, the authentication is hardly to be succeeded.

C. Acquiring Phase Identifier

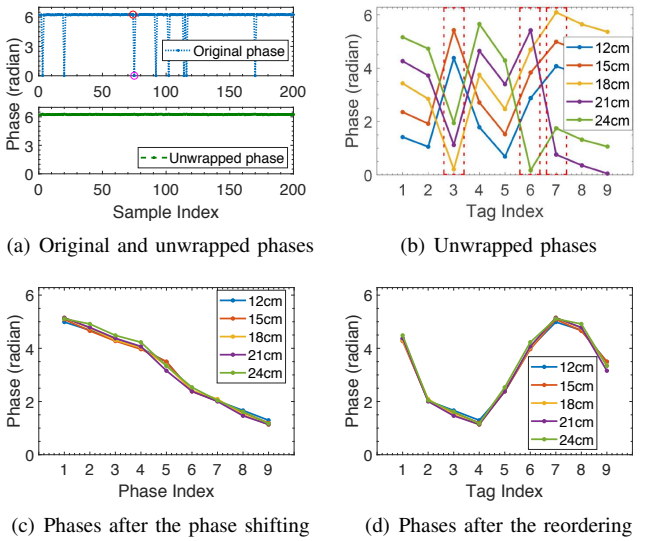
With observations obtained so far, we now introduce how to convert phase features to a reliable identifier, so that it can be used to fulfill the authentication. Even main phenomenons have been well explored in §III-A and §III-B, we find acquiring the phase identifier is still non-trivial, due to two reasons.

- Phase is a periodical function [10][24][26]. For one tag, if it locates at a specific position, its phase value could randomly jump from 0 to 2π or vice versa, due to the slight hand shaking.
- Phase is highly correlated with the distance [23][20]. When the array locates at different distances away from the reader, the phase values may vary.

To deal with above issues, we propose two techniques, namely phase calibration and identifier extraction.

1) Phase Calibration: Phase calibration is conducted in the registration and authentication stage. The user puts the array in front of the reader. The reader then continuously reads the tag array, and records all their phase responses for about $1s$.

Phase unwrapping: The phase reported by the reader varies from 0 to 2π. It is possible that at a certain distance, a tag phase randomly jumps from 0 to 2π or vice versa, which might introduce unnecessary errors. RF-Mehndi eliminates the phase jumping by unwrapping the phase sequences recorded for a period. As an example shown in Fig. 8(a), after unwrapping, the phase trend of this tag becomes continuous. In addition, to further mitigate the noise, we take the average phase of a short window (10 samples by default) for subsequent processing.



(a) Original and unwrapped phases (b) Unwrapped phases

(c) Phases after the phase shifting (d) Phases after the reordering

Fig. 8. Tag phases w./w.o. the calibration under different reader-to-tag distances.

Phase shifting: Once the deployment of the array is established, the coupling effect will reach a stable state. For example, Fig. 8(b) shows the phases of nine tags in the array when we put the array at different distances to the reader. We observe the phase difference between tags (*e.g.*, especially Tag 1, 2, and Tag 7, 8, 9) are relatively regular and constant. But due to the periodicity, during the continuous movement, the phases of Tag 3, 6 ,7 all undergo the phase reversal.

To overcome this issue, RF-Mehndi conducts the proposed phase shifting algorithm (*i.e.*, Algorithm 1, where N denotes the number of tags in the array, *i.e.*, $N = 9$) to mitigate the phase ambiguity induced by the distance. The basic idea is to find a pair of adjacent phases, denoted by (θ_m, θ_n), that their difference is maximal among all other adjacent phases. Then moving all phases together until one of the phase in (θ_m, θ_n) is nearest to 2π and the other is nearest to 0. As shown in Fig. 8(c), after the phase shifting, the phase values of all distances fall into one period and become consistent.

2) Identifier Extraction: After the calibration, we rearrange the phases according to their original tag order, as in Fig. 8(d). Then RF-Mehndi computes the *Phase Difference of Tags* (PDoT) as the feature, which is more reliable than using absolute phase values directly. PDoT (beween two tags i to j) can be calculated as:

$$\Delta\theta_{ij} = \theta_i - \theta_j = (\frac{4\pi d_{ij}}{\lambda} + \Delta\theta_{tag}^{ij}) \mod 2\pi, \quad (3)$$

where d_{ij} is the reader-to-tag distance difference between tag i and j, and $\Delta\theta_{tag}^{ij}$ is the initial phase offset of tag i and j, which represents the tag hardware characteristics (*i.e.*, tag diversity).

Algorithm 1: Phase Shifting

Input: Unwrapped phase sequence: $\theta = (\theta_{t_1}, \theta_{t_2}, ...\theta_{t_n}), n \in [1, N]$

Output: Calibrated phase sequence: $\theta^{'} = (\theta^{'}_{t_1}, \theta^{'}_{t_2}, ..., \theta^{'}_{t_n})$

Descending sort: $\theta \leftarrow sort(\theta), i \in [1, N]$
$i \leftarrow 1$
while $i < N$ **do**
  $\delta_i \leftarrow \theta_{t_i} - \theta_{t_{i+1}}$
  if $i == N$ **then**
    $\delta_i \leftarrow \theta_{t_i} - \theta_{t_1} + 2\pi$
  end if
  $i \leftarrow i + 1$
end while
Obtain maximum of δ_i: $\delta^{ma} \leftarrow max(\delta_i), i \in [1, N]$
if $\delta^{ma} == \delta_N$ **then**
  $\theta^{'}_{t_i} \leftarrow (\theta_{t_i} - (\theta_{t_N} - \frac{1}{2}\delta^{ma}))\ mod\ 2\pi$
else if $\delta^{ma} == \delta_j, j \in [1, N-1]$ **then**
  $\theta^{'}_{t_i} \leftarrow (\theta_{t_i} + (2\pi - \theta_{t_{j+1}} - \frac{1}{2}\delta^{ma}))\ mod\ 2\pi$
end if
Descending sort: $\theta^{'} \leftarrow sort(\theta^{'}_{t_i}), i \in [1, N]$

Calculating PDoT for each pair of tags, we can derive a N×N (N = 9 in the implementation) PDoT array (namely, ΔP):

$$\Delta P = \begin{Vmatrix} \Delta\theta_{11} & \Delta\theta_{12} & ... & \Delta\theta_{1N} \\ \Delta\theta_{21} & \Delta\theta_{22} & ... & \Delta\theta_{2N} \\ \vdots & \vdots & ... & \vdots \\ \Delta\theta_{N1} & \Delta\theta_{N2} & ... & \Delta\theta_{NN} \end{Vmatrix} \quad (4)$$

ΔP is a symmetric matrix, and every element on the diagonal is zero. Therefore, there are $\binom{9}{2} = 36$ effective descriptors to comprehensively represent phase differences in total. RF-Mehndi arranges these 36 descriptors in the upper triangular matrix (excluding the diagonal) into a vector as the identifier.

Note that compared to Eq. 1, PDoT eliminates the reader circuit characteristic, while retains the tags'. The benefits are twofold. First, this property provides the scalability that RF-Mehndi can be applied to different sites (*e.g.*, equipped with different readers). Second, keeping tag diversity makes each credential (*i.e.*, array) uniquely binding up with its target user.

D. Authentication

For the authentication, we develop a classifier using Support Vector Machine (SVM) to validate the identifiers. We utilize Weka [12] to train the SVM using the Sequential Minimal Optimization (SMO) algorithm [18]. The SVM algorithm adopts the polynomial kernel. This classifier can handle the multi-class problem using the pairwise classification.

IV. Implementation and Evaluation

We implement a prototype of RF-Mehndi and evaluate its performance through extensive experiments in this section.

Hardware: RF-Mehndi is mainly built with a COTS RFID reader, *i.e.*, Impinj R420. One directional antenna (Laird A9028, with gain of 8dbi) is connected to the reader. We assemble the tag array using the Alien-9629 SQUARE INLAY tag, which is a common label tag on the market. The whole system works on the frequency of $922.38MHz$.

Fig. 9. Experimental setups to evaluate the performance of RF-Mehndi.

Software: The software of RF-Mehndi is implemented using C#, which adopts the Low-Level Reader Protocol (LLRP, specified by EPCglobal in its EPC Gen2 standard) to communicate with the reader. The software runs on a PC with an Intel Core i7-4600U 2.10GHz CPU and 8GB RAM.

Experimental setups: We conduct experiments in a typical office environment. Fig. 9 illustrates the default setups. Nine Alien-9629 tags are used to form each 3×3 tag array, separated by about $3mm$, which can be nicely put into a general badge. When performing the authentication, the user (facing the reader antenna) holds the badge and touches the designed conductor. The tag array is covered by a thin film for the protection. The default reader-to-tag distance is about $15cm$. The reader continuously interrogates tags and collects their IDs and phases. The information is forwarded via Ethernet to a backend PC that runs RF-Mehndi.

Metrics: To characterize the RF-Mehndi's performance, we adopt three main metrics, namely False Accept Rate (FAR), False Reject Rate (FRR), and Accuracy. FAR is the measure of the likelihood that RF-Mehndi will incorrectly accept an access attempt by an unauthorized user (*i.e.*, an unauthorized array), which is calculated as:

$$FAR = \frac{false\ positives}{false\ positives + true\ negatives} \quad (5)$$

FRR is the measure of the likelihood that RF-Mehndi incorrectly rejects an access of an authorized user by:

$$FRR = \frac{false\ negatives}{true\ positives + false\ negatives} \quad (6)$$

A. Performance of RF-Mehndi

Note that to authenticate an user, our system will always first check IDs of tags in the array. If the IDs are registered, then RF-Mehndi performs the physical layer identifier (that derived from both the tag array characteristics and the human biometrics) based verification. Since the ID checking is simple, in the following we mainly focus on the authentication, using the extracted phase-based identifiers.

Efficiency of distinguishing different users: We first evaluate the overall performance of distinguishing various users. We

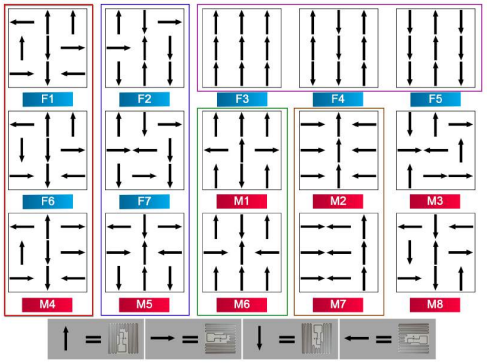


Fig. 10. Illustration of 15 tag layouts used in the experiment.

invite 15 volunteers to participate in this experiment, among which 7 are females and 8 are males. Each user has a unique tag array as his/her credential. We choose 15 representative tag array layouts, as illustrated in Fig. 10. The deployments of arrays marked in the box of same color are similar. We collect 200 groups of data for each user and perform the validation.

Fig. 11 plots the results. RF-Mehndi is shown to achieve an average accuracy exceeds 99%. Observe that for most users (11 out of 15), the FAR rates are even 0, meaning that RF-Mehndi can correctly recognize all illegal user 100% of the time. We also introduce challenging settings for several users (*e.g.*, F1, F2, F6, F7, M8). Specifically, the layouts of F1 vs. F6 and F2 vs. F7 are similar (*i.e.*, with only 1 or 2 tag direction differences). In addition, users F1, F6 and F2, F7 also have similar physical characteristics, *e.g.*, almost same age, height and weight. As a result, their FAR and FRR slightly increase, while they are still less than 4% and 3% respectively. This actually inspires the possibility to further optimize tag array assignments by both the tag layouts and user's characteristics, which will be studied as a future work of this paper.

Resisting impersonation attack: RF-Mehndi involves the human biometrics for authentication, which provides the ability that if an attacker tries to use an authorized user's credential to access the system, RF-Mehndi should be able to detect it. To evaluate the efficiency of resisting such impersonation attack, we investigate the distinguishability of the introduced impedance. We let ten volunteers perform the authentication using a same tag array. They stand at the same position towards the antenna, and the reader collects the phases of tags. Fig. 12 shows the average FAR and FRR of each volunteer.

We can see that FAR is below 0.05 for all, and the maximum FRR is still below 0.1. The results reveal that RF-Mehndi will refuse an unauthorized attacker with the probability above 95% even the attacker holds an valid array. It suggests that (1) each user brings distinguishable impedances, which can effectively identify each individual user. (2) RF-Mehndi can resist the impersonation attack as aforementioned in §II-C.

Resisting counterfeiting attack: We assume the attacker has the knowledge about the layout of an authorized user's array in this experiment. We examine whether the attacker can produce a counterfeited array with the same tag model and layout to

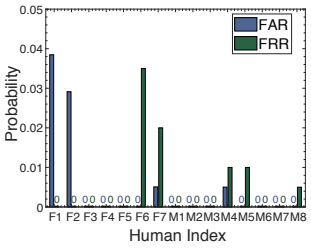


Fig. 11. Overall FAR and FRR performance of 15 users.

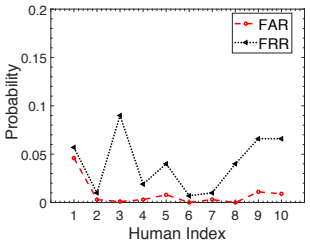


Fig. 12. Performance of resiting the impersonation attack.

pass the authentication. To this end, we choose 90 Alien-9629 tags and form 10 arrays. The layout is the same to that of F3's (in Fig. 10). We execute SVM to classify their identifiers. Fig. 13 compares the FAR and FRR. The FAR is less than 0.005, and the average FRR is less than 0.01, revealing that tags have hardware difference that will reflect in phases. Since *Phase Difference of Tags* (PDoT) keeps the tag differences, our proposed identifiers can well represent a unique array.

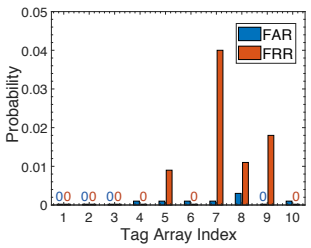


Fig. 13. Performance of resiting the counterfeiting attack.

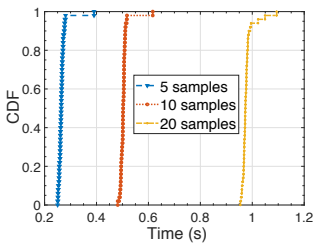


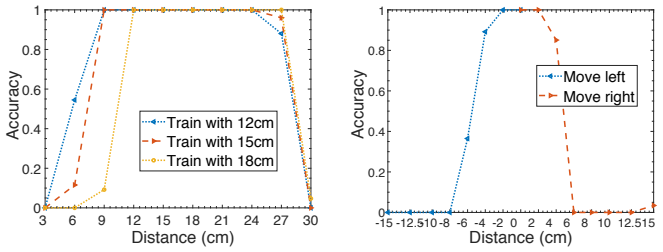
Fig. 14. Latency of RF-Mehndi under different settings.

Latency: In the implementation, the time consumption of RF-Mehndi mainly comes from three components: data collection, feature extraction, and fingerprint matching. Latter two components consume constant time in our system, nevertheless when using different phase samples to calculate the identifier, the data collection time will change. Thus, to evaluate the latency, we measure the time RF-Mehndi takes for authentication when varying the number of collected samples (*e.g.*, 5, 10, and 20 samples). Fig. 14 plots the CDF of latency from 50 measurements. The average values are $0.26s$, $0.50s$, $0.97s$ for 5, 10, 20 samples respectively. We believe it is sufficient for most access control application scenarios.

B. Impacts of various factors

Recalling that RF-Mehndi leverages the phase identifier in the design. We thus further consider and examine a series of practical factors that might change the phase.

Impact of distance: The array in our system has a maximum read range about $30cm$. A longer distance results in weaker signals, hence more noisy phase reading. In addition, distance will also involve the phase jumping issue. To understand how friendly RF-Mehndi can be utilized for users, we investigate the relationship between the distance and accuracy. Here we test two kinds of distances, vertical and horizontal distances.



(a) Vertical distance (b) Horizontal distance

Fig. 15. Accuracy vs. distances.

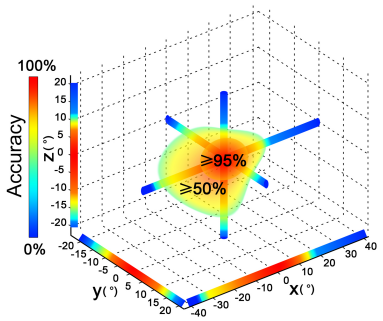


Fig. 16. Accuracy vs. rotations.

Vertical distance is the reader-to-tag distance along the direction from the reader antenna to the tag array. Horizontal distance is the offset perpendicular to the vertical distance.

We first vary the vertical distance form $3cm$ to $30cm$, with the step length of $3cm$. We use the data of one distance as the training set, then test if data from other distances can be classified as the same label with the training distance. Fig. 15(a) shows the average accuracy under each distance. The results reveal that our system has an effective authentication range of about $15cm$ (close to the training distance) along the vertical direction, within which the accuracy is 100%. With the vertical distance of $12cm$, we then vary the horizontal distance. The results in Fig. 15(b) demonstrate a $\pm 4cm$ region that can achieve the accuracy above 90%.

Impact of rotation: Fig. 16 shows the authentication accuracy of RF-Mehndi when the array is hold at varying angles w.r.t. the plane of the reader antenna. The reader antenna and tag array are put along the positive x-axis, paralleling to the y-z plane. Observe that along both y and z-axis, RF-Mehndi can achieve the authentication accuracy above 90% within $8.5°$. This is because according to the antenna design, RFID tags have angular sensitivity. When rotating in y or z-axis, the relative read range of the tag varies as well as the backscattered phase. On the other hand, the tolerance in x-axis is about $12.5°$. The range is limited because our system works in the distance shorter than $30cm$, within this distance (one wavelength), we cannot regard the reader transmitted CW as plane waves. Hence, rotating along x-axis will also introduce phase variations. But this is acceptable since rotating along x-axis, for example, with $90°$, the array will become a new array that might represent another user. For higher efficiency, when performing the authentication, we suggest the user to put the tag array parallel to the reader antenna plane.

C. Security Analysis

Our system aims at user authentication, hence, it is easy to think of that attackers would counterfeit an authorized user's credential (*i.e.*, tag array), steal the credential, or replay the signal of the credential. In this section, we summarize how RF-Mehndi deals with above three major threats.

***Counterfeiting attack*:** The attacker may learn the IDs and layout of a legitimate array in advance, and then establish an array with the attacker's own tags. Most physical-layer signal based authentication systems focus on solving this problem. As shown by existing works [11][6], by analyzing the physical fingerprints caused by hardware difference, the counterfeiting tags can be recognized. Experiments and results in Fig. 13 further demonstrate that RF-Mehndi can also successfully detect counterfeiting tag arrays that carry the same IDs and layout of the authorized credential.

***Impersonation attack*:** The user's card or credential may be lost or stolen. In this case, can the attacker outtrick RF-Mehndi with the user's card? To the best of our knowledge, we rarely find other RFID-field works could tackle this problem, since they only focus on device authentication. RF-Mehndi introduces the human biometric features and authenticates the device and the user identity at the same time. We have proved in Fig. 12 that when different persons touch the array, they will induce different amount of impedance to the tag antenna, resulting them to be distinguishable.

***Replay attack*:** An attacker first eavesdrops on the legitimate array's signal then replays it to cheat the system. Compared to other attacks, this attack requires more powerful or dedicated devices. Most fingerprint based works cannot stop this attack. For RF-Mehndi, due to the coupling of tags, the effective read range is shortened into about $30cm$, which increases the difficulty of the eavesdropping.

V. Related Work

User authentication: The concept of using biometrics for individual identification is widely adopted in many aspects of our life. Biometrics is a technology incorporates sensors that capture the biological characteristics (like fingerprints, finger and palm vein patterns, iris and voice) to recognize its original owner. It builds on the concept of replacing "something you have" with "who you are". However, general biometric based authentication systems extract static biometric features (*e.g.*, a fingerprint capture device electronically captures fingerprint images), that are easy to be copied. Recently, researchers explored voice-based [8] and heartbeat-based [21] methods to improve the efficiency. These emerging techniques have their tailored applications, while they may not be suitable for our targeted scenarios, like for lightweight personal cards, as they need dedicated sensors and devices to support.

Device authentication: Authenticating commercial RFID tags can be mainly divided into two categories: Crypto-based and Physical-layer signal based approaches.

The former type aims to utilize cryptographic techniques to protect the tag from illegal accessing [16][22]. However, due to the limited computational capability of COTS passive tags, most of these methods require the modification of either the commercial communication protocol or the hardware of tags, making them hard to be applied to the lightweight passive tags. In addition, if an attacker build a cloned tag with the same data, there is no mechanism to differentiate the legal one and the cloned one. Recently, leveraging physical-layer signals for authentication has been proved to be effective [14][6][25]. The rationale is that difference of circuit characteristics will reflect in the tag backscattered signal. D. Zanetti *et al.* [28] extract the Time Interval Error (TIE) and Average Baseband Power (ABP) from the tag physical signal to conduct tag authentication. Geneprint [11] utilizes the similarity of tag RN16 waveforms to resist counterfeit tags. Tagprint [27] exploits the phase fingerprint to acquire the geometric relationships and validate the genuineness of tags. All these solutions aim to authenticate the device (*i.e.*, the tag) itself. They are vulnerable to impersonation attacks that the system will fail if the attacker has the physical control of the legitimate device.

RF-Mehndi verifies the legitimacy of the tag array based on both the physical feature of the tags and the biological feature of the holder, which effectively tackles above issues. In addition, the implementation of RF-Mehndi depends on COTS readers and tags, enabling the seamless adoption by real applications in the near future.

VI. Conclusions

In this paper, we present RF-Mehndi, a user's fingertip profiled passive RFID tag based identifier, which is designed to enhance communication modalities of many personal cards nowadays, so that the card and holder's identity can be authenticated simultaneously. The RF-Mehndi design is based on two key observations — unique phase features from backscattered signals when tags are nearby and the user-specific profiling on such features when fingertip touches on the tags. In addition to these two observations, we further address technical challenges for developing a practical system. We evaluate RF-Mehndi by extensive experiments. Results show the effectiveness of RF-Mehndi, achieving excellent authentication performance.

Acknowledgements

This work is partially supported by NSFC Grant No. 61872285, 61802299, 61572396, 61751211, 61772413, 61672424, U1766215, Project funded by China Postdoctoral Science Foundation No. 2018M643663, Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies, GRF grant from Research Grants Council of Hong Kong No. CityU 11217817, and ECS grant from Research Grants Council of Hong Kong No. CityU 21203516. Ting Liu is Corresponding Author.

References

[1] Linear Bluepass Access Control Solution. http://www.nortekcontrol.com/bluepass/. Nortek Security & Control, 2018.

[2] Next-Gen Payment Processing Tech: Contactless RFID Credit Card. TREND MICRO, Security Technology, 2015.

[3] *Speedway Revolution Reader Application Note: Low Level User Data Support*. 2010.

[4] C. Bessette. How Serious a Crime Is Credit Card Theft and Fraud. https://www.nerdwallet.com/blog/credit-cards/credit-card-theft-fraud-serious-crime-penalty/. Nerdwallet, 2018.

[5] H. Ding, J. Han, C. Qian, F. Xiao, G. Wang, N. Yang, W. Xi, and J. Xiao. Trio: Utilizing Tag Interference for Refined Localization of Passive RFID. In *IEEE INFOCOM*, 2018.

[6] H. Ding, J. Han, Y. Zhang, F. Xiao, W. Xi, G. Wang, and Z. Jiang. Preventing Unauthorized Access on Passive Tags. In *IEEE INFOCOM*, 2018.

[7] EPCglobal. *Specification for RFID Air Interface EPC: Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz*, 2008.

[8] H. Feng, K. Fawaz, and K. G. Shin. Continuous Authentication for Voice Assistants. In *ACM Mobicom*, 2017.

[9] J. Gregory, S. Tang, Y. Luo, and Y. Shen. Bio-impedance Identification of Fingertip Skin for Enhancement of Electro-tactile-based Preference. *International Journal of Intelligent Robotics and Applications*, 1(3):327–341, 2017.

[10] J. Han, H. Ding, C. Qian, W. Xi, Z. Wang, Z. Jiang, L. Shangguan, and J. Zhao. CBID: A Customer Behavior Identification System using Passive Tags. *IEEE/ACM Transactions on Networking*, 24(5):2885–2898, 2016.

[11] J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, and J. Zhao. Generic and Accurate Physical-layer Identification for UHF RFID Tags. *IEEE/ACM Transactions on Networking*, 24(2):846–858, 2016.

[12] G. Holmes, A. Donkin, and I. Witten. WEKA: A Machine Learning Workbench. In *IEEE ANZIIS*, 1994.

[13] L. Irby. Setting a Secure Credit Card PIN and Password. https://www.thebalance.com/create-secure-credit-card-pin-or-password-960788. The balance, Fraud & ID Theft, 2018.

[14] X. Ji, J. Wang, M. Liu, Y. Yan, P. Yang, and Y. Liu. Hitchhike: Riding Control on Preambles. In *IEEE INFOCOM*, 2014.

[15] T. R. Kuphaldt. *Chapter 3: Electrical Safety. Lessons In Electric Circuits*. 2017.

[16] T. Li, W. Luo, Z. Mo, and S. Chen. Privacy-preserving RFID Authentication based on Cryptographical Encoding. In *IEEE INFOCOM*, 2012.

[17] R. Nandakumar, K. K. Chintalapudi, and N. Venkata. Dhwani: Secure Peer-to-Peer Acoustic NFC. In *ACM SIGCOMM*, 2013.

[18] J. Platt. Fast Training of Support Vector Machines using Sequential Minimal Optimization. In *Advances in Kernel Methods - Support Vector Learning*. MIT Press, 1998.

[19] S. Pradhan, E. Chai, K. Sundaresan, L. Qiu, M. A. Khojastepour, and S. Rangarajan. RIO: A Pervasive RFID-based Touch Gesture Interface. In *ACM MobiCom*, 2017.

[20] l. Shangguan, Z. Yang, A. X. Liu, Z. Zhou, and Y. Liu. STPP: Spatial-Temporal Phase Profiling-Based Method for Relative RFID Tag Localization. *IEEE/ACM Transactions on Networking*, 25(1):596–609, 2017.

[21] C. Song, F. Lin, Y. Zhuang, W. Xu, C. Li, and K. Ren. Cardiac Scan: A Non-Contact and Continuous Heart-Based User Authentication System. In *ACM Mobicom*, 2017.

[22] M.-T. Sun, K. Sakai, W.-S. Ku, T. H. Lai, and A. V. Vasilakos. Private and Secure Tag Access for Large-Scale RFID Systems. *IEEE Transactions on Dependable and Secure Computing*, 13(6):657–671, 2016.

[23] F. Xiao, Z. Wang, N. Ye, R. Wang, and X.-Y. Li. One More Tag Enables Fine-Grained RFID Localization and Tracking. *IEEE/ACM Transactions on Networking*, 26(1):161–174, 2018.

[24] L. Xie, C. Wang, A. X. Liu, J. Sun, and S. Lu. Multi-Touch in the Air: Concurrent Micromovement Recognition Using RF Signals. *IEEE/ACM Transactions on Networking*, 26(1):231–244, 2018.

[25] P. Xie, J. Feng, Z. Cao, and J. Wang. GeneWave: Fast Authentication and Key Agreement on Commodity Mobile Devices. In *IEEE ICNP*, 2017.

[26] 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 *ACM MobiCom*, 2014.

[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 *IEEE INFOCOM*, 2015.

[28] D. Zanetti, B. Danev, and C. Srdjan. Physical-layer Identification of UHF RFID Tags. In *ACM Mobicom*, 2010.