

# Hu-Fu: Replay-Resilient RFID Authentication

Ge Wang<sup>ID</sup>, Member, IEEE, Haofan Cai<sup>ID</sup>, Member, IEEE, Chen Qian, Member, IEEE, Jinsong Han<sup>ID</sup>, Senior Member, IEEE, ACM, Shouqian Shi<sup>ID</sup>, Member, IEEE, Xin Li<sup>ID</sup>, Han Ding<sup>ID</sup>, Member, IEEE, Wei Xi, Member, IEEE, ACM, and Jizhong Zhao, Member, IEEE, ACM

**Abstract**—We provide the first solution to an important question, “how a physical-layer authentication method can defend against signal replay attacks”. It was believed that if an attacker can replay the exact same reply signal of a legitimate authentication object (such as an RFID tag), any physical-layer authentication method will fail. This paper presents Hu-Fu, the first physical layer RFID authentication protocol that is resilient to the major attacks including tag counterfeiting, signal replay, signal compensation, and brute-force feature reply. Hu-Fu is built on two fundamental ideas, namely inductive coupling of two tags and signal randomization. Hu-Fu does not require any hardware or protocol modification on COTS passive tags and can be implemented with COTS devices. We implement a prototype of Hu-Fu and demonstrate that it is accurate and robust to device diversity and environmental changes, including locations, distance, and temperature. Hu-Fu provides a new direction of battery-free/low-power device authentication that enables numerous IoT applications.

**Index Terms**—Internet of Things, RFID, device authentication.

## I. INTRODUCTION

BATTERY-FREE wireless communication, in particular passive RFID, is a promising solution of the Internet of Things (IoT), due to its energy efficiency and low cost [1]–[18]. In recent years, security issues of IoT devices have drawn increasing attentions. Among these issues, device authentication is one of the most important problems. IoT device authentication aims to validate whether a device is indeed the legitimate one which has been registered in the system. It is a crucial task in many applications such as the

Manuscript received January 5, 2019; revised August 21, 2019; accepted December 23, 2019; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor W. Lou. Date of publication January 30, 2020; date of current version April 16, 2020. This work was supported in part by the National Key Research and Development Program of China under Grant 2018AAA0100500, in part by the NSFC under Grant 61832008, Grant 61872285, Grant 61751211, Grant 61772413, and Grant 61802299, in part by the Fundamental Research Funds for the Central Universities, and in part by the Research Institute of Cyberspace Governance in Zhejiang University. The work of Haofan Cai, Chen Qian, Shouqian Shi, and Xin Li was supported in part by the National Science Foundation under Grant 1932447, Grant 1717948, and Grant 1750704. (*Corresponding author: Jinsong Han*)

Ge Wang, Han Ding, Wei Xi, and Jizhong Zhao are with the Department of Computer Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: wangge@stu.xjtu.edu.cn; dinghan@mail.xjtu.edu.cn; xiwei@mail.xjtu.edu.cn; zjz@mail.xjtu.edu.cn).

Haofan Cai, Chen Qian, Shouqian Shi, and Xin Li are with the Department of Computer Engineering, University of California Santa Cruz, Santa Cruz, CA 95064 USA (e-mail: hcai10@ucsc.edu; cqian12@ucsc.edu; sshi27@ucsc.edu; xli178@ucsc.edu).

Jinsong Han is with the School of Cyber Science and Technology, Zhejiang University, Hangzhou 310027, China, and also with the Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies, Hangzhou 310007, China (e-mail: hanjinsong@zju.edu.cn).

This article has supplementary downloadable material available at <http://ieeexplore.ieee.org>, provided by the authors.

Digital Object Identifier 10.1109/TNET.2020.2964290

access control to an area or event, electronic payment, and tamper-evident packaging. However, the limited computing capability of battery-free devices restricts the execution of cryptographic algorithms such as hashing and encryption. In fact, commodity off-the-shelf (COTS) passive RFID tags do not support strong cryptographic operation and current UHF tags have no cryptographic capabilities.<sup>1</sup> Hence many classic security solutions are impossible to use on commodity passive tags. In addition, since a tag is simple and cheap, its memory may not be securely protected. If an attacker obtains the secret, it can easily produce unlimited counterfeits.

To this end, many researchers investigate to utilize physical-layer information of RFID tags for identification/authentication tasks [20]–[23]. Physical-layer identification methods are based on the fact that different tags may include hardware differences due to manufacturing imperfection. Hence a tag can be verified using certain physical features and a counterfeited tag is unlikely to have highly similar physical features with the legitimate one [20], [21], [23]. However, it is known that physical-layer identification/authentication is vulnerable to several major attacks, and whether there exists a solution to defend against them was considered an “open question” [22].

**Major Attacks:** We summarize four major attacks to physical layer authentication.

- 1) *Tag counterfeiting*; the attacker uses an unauthorized tag to let it carry the same ID of a legitimate tag. For example, a thief takes a fake entrance card and tries to play as a staff to open the door.
- 2) *Signal replay*; the attacker eavesdrops the physical signals of a legitimate tag, captures them in a digital form, and then replays the exactly same signals towards the reader [22], [24]. For example, a dishonest man eavesdrops and records the communication process between the metro card and the subway system. Then he/she tries to get on the subway by just replaying the same signals with an RF transmitter.
- 3) *Signal compensation*; the attacker obtains a signal that can pass the authentication, called a valid signal. Then during the authentication process, it compensates the current signal in the environment to become the valid signal [25]. For example, a robber uses an invalid entrance card and tries to open the door. At the same time, he/she uses a powerful RF radio to send a well-designed signal and make the entrance guard system mistake him/her for a legitimate user.
- 4) *Brute-force feature replay*; Assuming the attacker knows the feature extraction algorithm and owns sufficiently

<sup>1</sup>To our knowledge, the only tag with a cryptographic function is the recently announced NXP UCODE DNA RFID [19]. However all related documents are for commercial purposes. Hence we are not clear about its cryptographic strategy, reliability, and other characteristics.

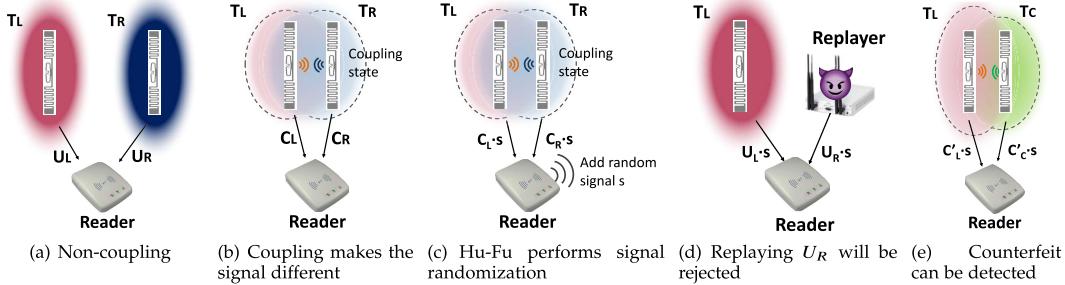


Fig. 1. Utilize coupling state and signal randomization to defend against various attacks.

many tags, it extracts the feature of every tag until getting one tag that presents a feature close enough to the legitimate tag [22]. For example, a bad man tries numerous times to find out a fake card that has very similar features with that of the valid bank card.

All prior physical-layer identification methods mainly defend against tag counterfeiting, but are vulnerable to the remaining three attacks [24]. Traditional network protocols using a cryptographic nonce to defend against replay attacks but passive tags are obviously unable to use it. Signal and feature replay has been considered as an ultra-weapon to physical-layer authentication. A recent work [23] states “*To our knowledge, no existing work can effectively defend against such an attack (signal replay), including our work*”. In [24] it states “*Signal replay makes the attacker frames almost indistinguishable from the genuine frames... Whether such impersonation detection (of signal or feature replay) is feasible, is an open question.*”

In this paper, we provide the first answer to such an open question, **a new direction of physical-layer authentication that is resilient to the attacks listed above**. The proposed authentication method is called Hu-Fu.<sup>2</sup> Hu-Fu is based on two ideas. First, we observe the fact of *inductive coupling* of two adjacent tags [26], [27] from real experiments, that if we place two tags in close positions (*e.g.*, in 2cm), the backscatter signal from either tag would be different from the signal by putting the tag alone. The coupling signal of a tag also depends on the other tag. Hence we use a tag, called the Retained Tag (or Left Tag)  $T_L$ , along with the reader as the authenticator. When an authenticatee, called the Right Tag  $T_R$ , is presented,  $T_R$  should be put to a position close to  $T_L$  and an inductive coupling state is created. The system validates whether the features from the physical signals of  $T_R$  and  $T_L$  are consistent to the signals collected previously using the legitimate tag  $T_R$ . As shown in Fig. 1(a), if  $T_L$  and  $T_R$  are separate, they will reply non-coupling signals  $U_L$  and  $U_R$ . However, if they are close enough, in Fig. 1(b) their signals will become  $C_L$  and  $C_R$ . The authentication features are extracted from  $C_L$  and  $C_R$ . The second idea, called *signal randomization*, which is introduced in a recent work [28], is to allow the reader sends a one-time random signal  $s(t)$  that changes with time  $t$ . Then the backscatter signal  $C_R$  become  $C_R \cdot s(t)$ , which appears random to an eavesdropper who has no information of  $s(t)$ , shown in Fig. 1(c). The eavesdropper is even unable to tell whether a tag is transmitting or not. But the reader is able to

<sup>2</sup>Hu-Fu, also called tiger tallies, were authentication seals used by ancient Chinese emperors to command and dispatch the army. The right piece was retained by the emperor and the left piece was issued to the general of the army. When a messenger sends a imperial command to the general, he must show the right tally that matches exactly to the left piece. Hu-Fu was famous for the tale of Lord Xinling in *The Records of the Grand Historian*.

remove  $s(t)$  for decoding. Hu-Fu makes an attacker incapable to capture, replay, or compensate the signal or feature that can pass the authentication, because  $C_L$  and  $C_R$  are hidden. For example in Fig. 1(d), if an attacker records  $U_R$  by querying  $T_R$  using an unauthorized reader, even if it replays  $U_R$ , Hu-Fu will find the difference between  $\langle C_L, C_R \rangle$  and  $\langle U_L, U_R \rangle$  and reject the replay. As in Fig. 1(e), since the attacker does not know  $C_R$ , the signal from a counterfeit  $C'_c$  will highly likely to be different from  $C_R$  and it cannot get accepted.

Both inductive coupling and signal randomization are essential components of Hu-Fu. They work together to block the access of attackers to valid signals and features from legitimate tags. Without inductive coupling, an attacker can easily get the reply signal from a legitimate tag by querying it using an unauthorized reader. Then the attacker replays it to the reader. Without signal randomization, the attacker can eavesdrop on  $C_L$  and  $C_R$  and try to use signal compensation or brute-force feature replay to re-build the signals.

Hu-Fu effectively protects the following information, which is the basis of the major attacks to physical-layer authentication. 1) The coupling signal of the pair of tags; 2) The feature of a legitimate tag, even though the attacker knows the feature extraction algorithm; 3) What signal can pass the authentication process. By cutting the source of these attacks, Hu-Fu effectively ensures the success of physical-layer authentication.

Hu-Fu is also cost-efficient. It does not require any change on COTS tags. A Hu-Fu reader can be built with COTS wireless devices. It is also easy if a vendor wants to change its readers to be compatible to Hu-Fu. The authentication time is fast (< 1.5sec).

The major contributions of Hu-Fu are as follows:

- Hu-Fu is the **first tag authentication solution** to defend against counterfeiting, signal replay, signal compensation, and feature replay attacks that is compatible to the standard protocol. It provides a new direction of battery-free/low-power IoT device authentication.
- Hu-Fu is robust to the device and environment diversity. It uses environment- and reader-independent features, hence it can accurately authenticate tags that are registered at different places.
- We implement a working prototype of Hu-Fu and conduct extensive experiments to demonstrate its security and reliability.

In the rest of this paper, we first present the overview of Hu-Fu in Section II. We model and validate the inductive coupling of two tags in Section III, and introduce the propagation model in Section IV. In Section V, we present the detailed system design. The security analysis of our system is discussed in Section VI. The prototype implement

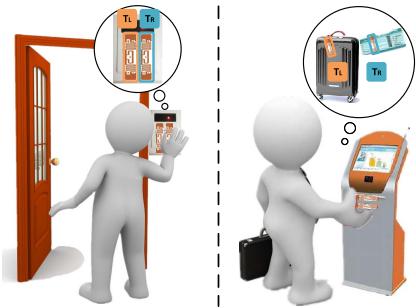


Fig. 2. Two typical applications of Hu-Fu. Left: static scenario; Right: dynamic scenario.

and evaluation of Hu-Fu are introduced in Section VII. The state-of-art RFID authentication methods and conclusion are discussed in Section VIII and IX.

## II. OVERVIEW

In this section we introduce the problem studied in this work, the system and security model, and the basic protocol work flow of Hu-Fu.

### A. System and Security Model

Hu-Fu solves the following fundamental problem in an RFID system. Given a tag reply that reports a registered tag ID (EPC), the RFID system needs to decide whether the reply was from the authorized tag that has been registered with this ID, called a *legitimate tag*, or from an attacker who does not hold the legitimate tag. The tag reply from an attacker could be transmitted from a different tag that carries the registered ID, called a *counterfeit*, or from a powerful device that can replay any signal it has previously heard, called a *replayer*.

Depending on the application requirements, Hu-Fu may be utilized in two situations, namely static scenarios and dynamic scenarios. In a **static scenario**, a legitimate tag is registered at the *check-in site* and its physical-layer feature is collected by the system. Later it is verified at the same place for authentication. Such a scenario is useful for applications like access control. As shown in the left of Fig. 2, one tag is fixed at an entrance guard and acts as the Left Tag  $T_L$ . A first-time user registers her Right Tag at the entrance by placing it together with the Left Tag and letting the system record the physical feature under certain security control. Later when the user requests for entrance, she places her Right Tag again with the Left Tag and let the system verify it. A Left Tag can be paired with multiple Right Tags for different users. In a **dynamic scenario**, the *authentication site* where a tag is verified may be different from the check-in site. Such scenario is useful for applications such as a baggage claim system. As shown in the right of Fig. 2, a user checks in her luggage by letting the system record the physical feature of a pair of coupled tags. Then a tag is attached to the luggage, acting as the Left Tag. The user carries the Right Tag. Later at the destination of the trip, the system verifies the features of the pair of tags and authenticate the Right Tag presented by the user before allowing her to pick up the luggage.

**Security Model:** We assume a powerful attacker. It can eavesdrop on any communication between the legitimate reader and tags (attacker can also be a MIMO eavesdropper), record any signal, and replay the *identical* physical signal of prior communication to the reader, at any location including the check-in and authentication sites. However, it cannot obtain the tags' features by some active attacks at check-in and

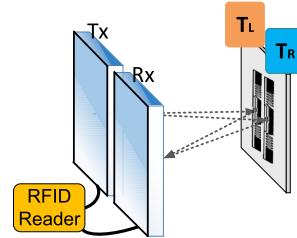


Fig. 3. The deployment of Hu-Fu.

authentication sites, *e.g.*, using an unauthorized reader to query the legitimate tags. Attackers cannot block the communication channel between the legitimate reader and tags. In the dynamic scenario, the Left Tag cannot be accessed anywhere with an unauthorized reader. This assumption has been used in prior work such as [28], and it is reasonable as there are a few practical and commercial solutions that can detect and prevent active attacks, including shielding sleeves [29], RFID blocking wallets [28] and RFID reader detectors [30], [31]. Right Tags do not have such a requirement. We further assume the attacker knows all authentication protocols and feature extraction algorithms.

Note that an attacker can gain from each false positive result of Hu-Fu, but it will also be penalized and pay non-trivial cost for every true negative result. When a negative result is obtained, the presenter of the right tag will be further interrogated and verified using next-level authentication method, such as being asked to show his/her personal ID, receipts, *etc.*. True negatives caused by attackers will hence be penalized. An attacker cannot try to use different counterfeited tags by infinitely many times and expect that one of them can pass Hu-Fu.

We mainly consider the four attacks presented in §I, namely 1) tag counterfeiting, 2) signal replay, 3) signal compensation, and 4) brute-force feature replay. The attacker is able to launch all of them. We focus on tag authentication and do not consider attacks that target on communication confidentiality, integrity, or availability.

To our knowledge, no prior work has considered such a powerful attacker and no prior work can defend against attacks 2), 3), and 4).

### B. Workflow of Hu-Fu

As shown in Fig. 3, a Hu-Fu instance includes an RFID reader carrying two directional antennas.<sup>3</sup> The Left Tag  $T_L$  sits face to the reader and is fixed. We assume  $T_L$  cannot be destroyed, replaced, nor its communication channel to the reader can be blocked. The reader and  $T_L$  are together acting as the Hu-Fu authenticator. A tag as the ‘authenticatee’ is denoted as the Right Tag  $T_R$ . Hu-Fu has two phases, namely registration phase and authentication phase. Every legitimate tag  $j$  should have been registered to the system. To register a tag, it should be placed to a position in 2cm distance to  $T_L$  and become the Right Tag  $T_R$ . Certain features of the physical signals from  $T_L$  and  $T_R$  will be collected and stored in a back-end server associated with  $T_R$ 's ID. Later if a tag claiming to be  $T_R$  is present and Hu-Fu needs to validate its authenticity, the tag will be putted to the place 2cm to  $T_L$  and become  $T_R$ . Their backscatter signals will be analysed in order to verify

<sup>3</sup>We use a USRP-based Software Defined Radio (SDR) to build the reader. In fact, Hu-Fu utilizes the raw received signals as the feature source, which can also be captured by COTS readers. Hence we believe Hu-Fu can be easily implemented on COTS readers by a vendor [32].

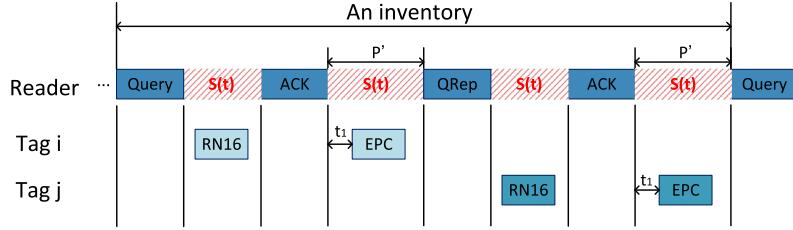


Fig. 4. The design of Hu-Fu.

the features are consistent to the record of  $T_R$  stored at the back-end server. **A Left Tag can be paired with multiple Right Tags.**

The main idea of Hu-Fu is utilizing both the **inductive coupling** phenomenon between two adjacent tags and **signal randomization**. A passive tag can be modeled as a kind of coil. When a tag is powered by the reader, a current will flow inside the coil. As we all know, a steady current on a circular can generate a magnetic field around it [26], [27], which may influence the current in adjacent circulars. That is why two close tags will inductive couple with each other. In addition, due to the manufacturing imperfection, the inductive coupling phenomena are not identical for different tag pairs. We utilize this characteristic of passive tags to perform authentication. Suppose tags  $T_L$  and  $T_R$  replies signals  $U_L$  and  $U_R$  respectively when they are not coupled. If they are in the coupling status,  $T_L$  and  $T_R$ 's signals will become  $C_L$  and  $C_R$  respectively, whose features are used for authentication. Hence an attacker cannot get  $C_R$  by using an unauthorized reader to query  $T_R$ . However, it may still eavesdrop on  $C_L$  and  $C_R$  during the registration or authentication process.

Hu-Fu is able to hide  $C_L$  and  $C_R$  during the registration or authentication process. As shown in Fig. 4, the RFID reader first broadcasts a *Query* command. Once the tag is powered up by the signals, it will randomly choose a slot to respond with a random number *RN16*. The reader will acknowledge the tag with an *ACK* command and append the received *RN16*. If the tag successfully recognizes the *ACK*, it will send back its ID, *i.e.*, the Electronic Product Code (*EPC*). In our design, as shown in Fig. 4, instead of transmitting a constant carrier wave, we let the reader sends a one-time random signal  $s(t)$  that changes with time  $t$ . Hence an attacker can only obtain  $C_L \cdot s(t)$  and  $C_R \cdot s(t)$  by eavesdropping on the registration/authentication process. The reader can easily extract and decode  $C_L$  and  $C_R$  since it knows  $s(t)$ . Since  $C_L$  and  $C_R$  are hidden, the attacker cannot extract the features from valid tags even if it knows the feature extraction algorithms. All attacks can be successfully defended by hiding both the valid signals and features. Note Hu-Fu does not need any hardware or protocol changes on COTS passive tags.

In addition, authenticating two tags as a unit is also helpful for extracting environment-independent features. For two tags that close with each other, the surrounding environments are very similar. This phenomenon can be applied in noise removal. Hu-Fu can effectively cope with environment diversity and achieve high accuracies in both static and dynamic scenarios.

### III. MODEL AND VALIDATE TAG COUPLING

We show that *inductive coupling* introduces significant signal difference to RFID tags, by modeling and experimental validation.

The fundamental reason of inductive coupling is the electromagnetic induction. According to the Biot-Savart Law [26],

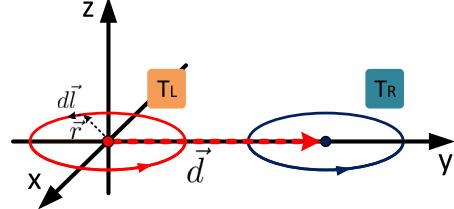


Fig. 5. Model of two coupling tags.

a steady current on a circular can generate a magnetic field around it. We specify it with the model shown in Fig. 5. According to the physical property of the dipole-aerial design, each tag can be modeled as a circular loop [26], [33]. We set the origin point as the center of the circular of the Left Tag  $T_L$ . Let vector  $\vec{d}$  denote the directional vector from the center of  $T_L$ 's circular to that of the Right Tag  $T_R$ . When a reader inventories the pair of tags and induces a current  $I_1$  on the circular of  $T_L$ , a magnetic field  $B_{21}$  will occur on  $T_R$ :

$$B_{21} = \frac{\mu_0}{4\pi} \oint_c \frac{I_1 d\vec{l} \times (\vec{d} - \vec{r})}{|\vec{d} - \vec{r}|^3}, \quad (1)$$

where  $\vec{r}$  is the radius vector from the circular center of  $T_L$  to the differential element  $d\vec{l}$  on the wire, the direction of  $d\vec{l}$  is defined as the same with the conventional current  $I_1$ , and  $\mu_0$  is the magnetic constant. As a result, the magnetic field  $B_{21}$  will introduce a magnetic flux  $\Phi_{21}$  that go through  $T_R$ 's loop. If the effective area of  $T_R$ 's loop is  $S_2$ , the magnetic flux  $\Phi_{21} = B_{21} \cdot S_2$ . In this way, we can further measure the mutual inductance  $M_{21}$  between  $T_L$  and  $T_R$ :

$$M_{21} = \frac{\Phi_{21}}{I_1} = \frac{\mu_0}{4\pi} \oint_c \frac{1}{|\vec{d} - \vec{r}|^2}. \quad (2)$$

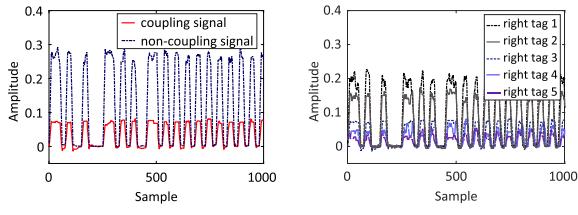
According to Eq. 2, we find that the mutual inductance  $M_{21}$  is independent of the current in the circular of either  $T_L$  or  $T_R$ . It is only related to the relative position ( $\vec{d}$ ) and the physical feature of the equivalent circular ( $\vec{r}$ ).

In this way, we can divide the electromotive force  $E'_2$  to  $T_R$  into two parts: the internal electromotive force  $E_2$  and the induced electromotive force  $E_{21}$ :

$$E'_2 = E_2 + E_{21} = E_2 + (-N_2 \frac{d\Phi_{21}}{dt}), \quad (3)$$

where  $N_2$  is the loop number of  $T_R$ ,  $E_2$  is the internal electromotive force of  $T_R$  in non-coupling case, and  $E_{21}$  represents the value that induced by the current in  $T_L$ 's circular. As a result, the current  $I'_2$  on the circular of  $T_R$  in non-coupling case will change to  $I'_2$  accordingly:

$$\begin{aligned} I'_2 &= \frac{E'_2}{R_2} = \frac{E_2}{R_2} + \frac{E_{21}}{R_2} \\ &= I_2 - \frac{N_2}{R_2} \cdot \frac{d\Phi_{21}}{dt} \end{aligned} \quad (4)$$



(a) Coupling and non-coupling signals of  $T_L$   
(b) The coupling signals of  $T_L$  with different  $T_R$

Fig. 6. The inductive coupling phenomenon.

Considering Eq. 4 and 2, we have:

$$I'_2 = I_2 - \frac{N_2}{R_2} \cdot \frac{dM_{21}}{dt} \cdot I_1. \quad (5)$$

In this way, we build a relationship between the influenced current  $I'_2$  in  $T_R$  with  $I_1$  and  $I_2$ , as well as the physical features of itself ( $N_2$ ,  $R_2$ , etc). Accordingly, the influenced current  $I'_1$  in  $T_L$ :

$$I'_1 = I_1 - \frac{N_1}{R_1} \cdot \frac{dM_{12}}{dt} \cdot I_2. \quad (6)$$

Therefore when a pair of tags are put together, the coupled signal from either of them depends on the physical features of both tags. The coupled signals are different for different pairs of tags. If the attacker replaces one of them, the influenced current  $I'_1/I'_2$  will change. To verify this fact, we conduct two experiments. In the first experiment, we collect the non-coupling signal of  $T_L$  and then put a right tag  $T_R$  close to  $T_L$  with 2cm distance. As shown in Fig. 6(a), with the interference of the right tag, the coupling signal of  $T_L$  has obvious difference to the non-coupling one *in amplitude*. We then change the right tag to four other different ones. We do not change any settings of the former experiment, including the parameters, environments and the tag's position. We show the coupling signal of the  $T_L$  in Fig. 6(b). We find that with the interference of different right tags, the coupling signals of the same left tag also have distinguishable differences in amplitude. Hence by querying  $T_L$  or  $T_R$  separately, the attacker cannot obtain the amplitude-based features that are used for authentication. Since the coupling signals are protected by randomization, the attacker is not able to obtain any valid signal or feature that can pass the authentication.

#### IV. PROPAGATION MODEL OF HU-FU

We divide the propagation process between the SDR reader and tags into two parts. One is from the transmitter end (Tx) of the reader to the tag pair, and another is from either of the tag to the receiver end (Rx). In this section, we will specify the signal propagation process between the reader and the tag pair.

First of all, the SDR reader emits an electronic wave with a transmitting power of  $P_R$ . When there is no other tags that is coupling with the tag  $T_i$ , its received power  $P_{T_i}$ <sup>4</sup> should be:

$$P_{T_i} = \gamma \cdot \frac{\lambda^2}{4\pi} \cdot \frac{P_R \cdot G_{Tx} \cdot G_{T_i}}{4\pi \cdot D_{R \leftrightarrow T_i}^2}, \quad (7)$$

where  $\gamma$  is the downlink attenuation parameter.  $D_{R \leftrightarrow T_i}$  represents the distance between reader's Tx to the tag  $T_i$ .  $G_{Tx}$

<sup>4</sup>The received data of the SDR reader is the I-Q values in a complex-number form. So we calculate the power  $P$  of the received signal and use it in the following analysis.

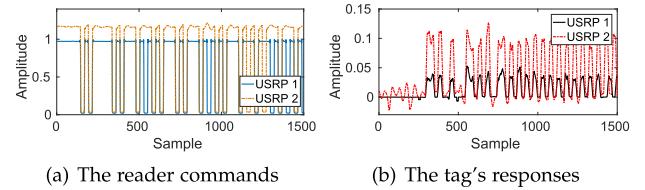


Fig. 7. The received signals of different devices.

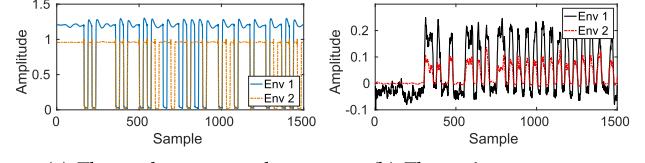


Fig. 8. The received signals of different places.

and  $G_{T_i}$  are the antenna gains of the reader and the tag  $T_i$ , respectively.

Once tag  $T_i$  is powered of  $P_{T_i}$ , the current along its circuit should be  $I_{T_i}$ . However, as we have aforementioned in Sec. III, when there is another tag, say tag  $T_j$ , inductive coupling with the tag  $T_i$ , the influenced current  $I'_{T_i}$  of tag  $T_i$  does not only determined by its received signal, but also be impacted by the tag  $T_j$ . In other words, the power of backscattered signal of tag  $T_i$  should be:

$$P'_{T_i} = I'_{T_i} \cdot U \cdot x(t), \quad (8)$$

where  $I'_{T_i}$  is the mutual inductance coupled current in tag  $T_i$ .  $U$  is the voltage, which is mainly determined by the reader's power and has nothing to do with the inductive coupling state of the tag. And  $x(t)$  represents the tag's data.

With the influence, the power of the received signal at Rx can be represented as:

$$P'_R = \gamma' \cdot P'_{T_i} \cdot G_{T_i} \cdot |\Gamma_{T_i}|^2 + N_G, \quad (9)$$

where  $\gamma'$  is the uplink attenuation parameter. And  $\Gamma_{T_i}$  is the modified reflection coefficient, which is determined by the antenna resistance and reactance of both reader and the tag.  $N_G$  is the Gaussian white noise introduced by devices. Observing the received signal  $P'_R$  of the tag tag  $T_i$ , we find that it is determined by four factors, the hardware characteristics of the reader and tag pairs, the environments and the relative position. We also conduct a series of experiments to validate our model. The first experiment is to change the SDR devices, *i.e.*, USRP, and observe the received signals. As depicted in Fig. 7, both of the reader's commands (also transmit by the same SDR device) and the tag's responses received by different devices are totally different. We also take an experiment in two different places and reach the same conclusion (as shown in Fig. 8). In other words, the received signals are highly related to the current environment, devices and other factors. In the following sections, we will specify how to remove other noises and extract environment and device independent features.

#### V. SYSTEM AND PROTOCOL DESIGN

To authenticate a tag presented to Hu-Fu, the system includes three modules to determine the result 'Accept' or 'Reject', namely signal collection, signal preprocessing, and feature extraction and comparison as shown in Fig. 9. The signal collection module aims to collect the signals from two coupling tags in a secure way with the reader. The signals are

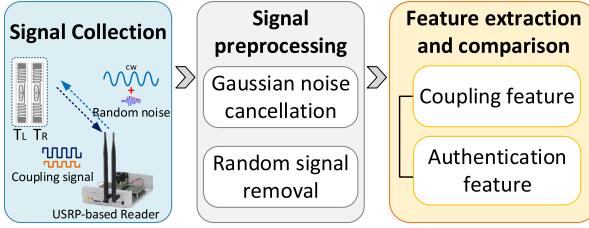


Fig. 9. System design.

then processed to remove the random signal and environmental noise, in the signal preprocessing module. Finally, in feature extraction and comparison module, we propose two types of features, namely coupling feature and authentication feature, which are used for authenticating the tag and detect different kinds of attacks. Our design is compliant to the existing EPC protocol [34] and requires no change on passive tags.

#### A. Signal Collection

In Hu-Fu the reader queries both the Left and Right Tags and then collects the backscatter signals from them. The deployment of Hu-Fu is shown in Fig. 3. We place the Tx and Rx antennas in a line. Both of them stand facing to the tag pair. In both the registration and authentication phases, Hu-Fu first collects the backscatter signal from  $T_L$  by keeping querying  $T_L$  for one second. Then  $T_R$  is placed within 2cm distance to  $T_L$  on the test board. Hu-Fu collects the backscatter signal from both  $T_L$  and  $T_R$  by keep querying them for another second.

To prevent attackers from eavesdropping and recording the coupling signals, the Hu-Fu reader sends a random signal instead of constant carrier waves during each tag response. As shown in Fig. 4, the reader transmits a random signal  $s(t)$  instead of the carrier waves ( $cw$ ). This mechanism has been introduced in RF-Cloak [28]. The authors of [28] have proved that this mechanism can overcome a single-antenna eavesdropper that uses the optimal decoder. For a MIMO eavesdropper, it may extract the coding of the legitimate tags. However, it is still not able to estimate the physical-layer features of each tag. The information it obtained is far from enough for recording, reconstructing and replying the original signals. We discuss it in Appendix A (supplementary material). Hence Hu-Fu can effectively prevent attackers from eavesdropping or recording the coupling signal. Without the knowledge about the coupling signal, attackers can hardly compensate uncoupling signals or find out a counterfeited tag that owns a similar hardware characteristic with the legitimate one.

In our implementation, we use a USRP radio to achieve these tasks. The entire process can also be implemented on a COTS reader without introducing much complexity, if a vendor wants to.

Utilizing this mechanism, when a tag responds its data, the reader transmits a random signal  $s(t)$  with the power of  $P_R(t)$ . We develop a model of the backscatter signal under such randomization using basic communication theory. Due to the space limitation, the detailed derivation is skipped. The power of the received signal  $P'_R$  from a tag at the receiver of the reader  $R$  can be modeled as follows:

$$P'_R(t) = \gamma \cdot \gamma' \cdot h(R, T_i, T_j) \cdot s(t) \cdot x(t) + N_G, \quad (10)$$

where  $h(R, T_i, T_j)$  is related to the hardware characteristics and relative positions of the reader  $R$  and two tags  $T_i$  and

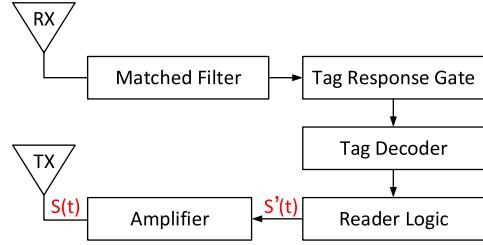


Fig. 10. The structure of SDR reader.

$T_j$ ,<sup>5</sup>  $\gamma$  and  $\gamma'$  are the attenuation parameters of the paths from the reader to tag and backwards,  $x(t)$  is the original tag signal, and  $N_G$  is the Gaussian white noise introduced by devices. According to the EPC C1G2 protocol [34], we retrieve the tag's EPC signal segment by cutting out the signal between each valid ACK and its next command (usually *QueryREP/QueryAdj/Query*), and use it as the received signal  $P'_R$ .

#### B. Signal Preprocessing

According to Eq. 10, we find that the received signal is influenced by many factors, including random signal, white noises and environment noises. To obtain the hardware-dependent features, we should first eliminate noises and remove the random signal  $s(t)$ . Hu-Fu processes the signal using two steps: Gaussian white noise cancellation and random signal removal.

*Gaussian Noise Cancellation (GNC):* Although we have no idea about the exact value of Gaussian white noise at a given time, the noise has a normal distribution in the time domain with an average value of zero, i.e.,  $G_N \sim \mathcal{N}(0, \sigma^2)$ . Hence we may employ a mean filter with a time window  $w$  to remove the Gaussian noise, i.e. :

$$P_1^*(t) = \text{MEAN}[P'_R(x)], x \in [t - w/2, t + w/2], \quad (11)$$

where  $t$  is the time point of a signal sample. The basic idea of the mean filter is that within a time window, the average value of Gaussian noise should be 0. While the other parts of signal  $P'_R$  are highly likely to be unchanged. Hence the signal  $P_1^*$  can be modeled as:

$$P_1^*(t) \approx \gamma \cdot \gamma' \cdot h(R, T_i, T_j) \cdot s(t) \cdot x(t). \quad (12)$$

Based on empirical experience, we choose the time window  $w$  as 10 samples, which is about half of a square wave.

*Random Signal Removal:* Then Hu-Fu removes the random signal that is used to hide the responses from tags. The inner structure of the reader (implemented by SDR in our prototype) is shown in Fig. 10 [35], [36]. We generate a random signal  $s'(t)$  in reader logic module and then send it instead of the constant carrier waves. However, before the SDR reader transmits  $s'(t)$ , it will put  $s'(t)$  into an amplifier, i.e.,  $s(t) = \alpha \cdot s'(t)$ , where  $\alpha$  represents the magnification times of the amplifier. In practice, we do not know the exact value of  $\alpha$  and have no idea about the exact value of  $s(t)$ . That introduces a challenge in this step.

<sup>5</sup>The detailed representation is  $\frac{P_R \cdot G_{T_i} \cdot G_{Tx} \cdot |\Gamma_{T_i}|^2 \cdot \lambda^2}{16\pi^2 \cdot D^2} \cdot [G_{T_i} - \frac{N_i}{R_i} \cdot \frac{dM_{ij}}{dt}] \cdot G_{Tj}$  where  $G_{Tx}$  and  $G_{T_i}$  are the antenna gains of the reader and the tag  $T_i$ ,  $\Gamma_{T_i}$  is the modified reflection coefficient, which is determined by the antenna resistance and reactance of both reader and the tag,  $D$  is the distance, and  $M_{ij}$  is the mutual inductance.

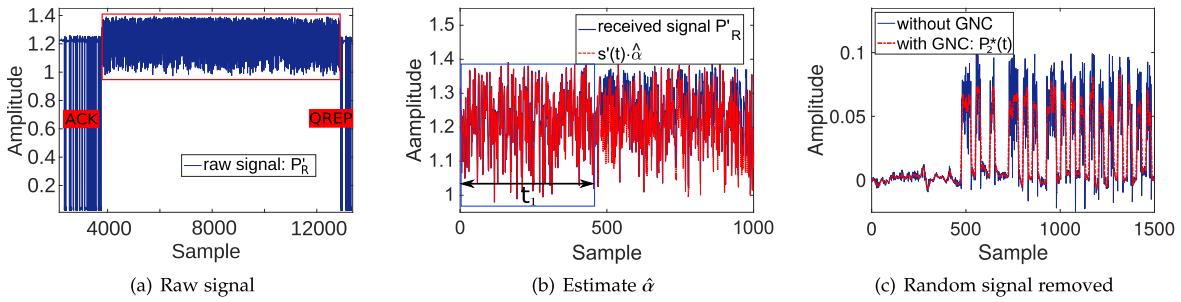


Fig. 11. Signal pre-processing. Due to signal overlaps, (b) and (c) are easier to read with colors.

Fortunately, we find that after the reader finishes transmitting *ACK* commands, a tag will wait for a relatively stable time period  $t_1$ , before it starts to respond. As shown in Fig. 4, the tag will not start to transmit the EPC during time  $[t_0, t_0 + t_1]$ , where  $t_0$  is the time when the reader finishes transmitting its *ACK*. Hence the signal during time  $[t_0, t_0 + t_1]$  can be expressed as follows:

$$P'_R(t) = \gamma^* \cdot h(R) \cdot s(t) + N_G, \quad (13)$$

where  $\gamma^*$  is the propagation parameter through the transmitting path, and  $h(R)$  is only related to the reader hardware. After canceling the Gaussian white noise, we can estimate amplifier coefficient  $\alpha$  as follows:

$$\hat{\alpha} = (P'_R(t) - N_G)/s'(t) = \gamma^* \cdot h(R) \cdot \alpha, \quad (14)$$

Utilizing the estimated amplifier parameter  $\hat{\alpha}$ , we can remove the random signal  $s(t)$  for the signal samples collected after time  $t_0 + t_1$ , i.e. :

$$P_2^*(t) = P_1^*(t)/(\hat{\alpha} \cdot s'(t)), \quad (15)$$

Based on Eq. 12 and 15,  $P_2^*(t)$  can be modeled as  $\frac{\gamma \cdot \gamma'}{\gamma^*} \cdot \frac{h(R, T_i, T_j)}{h(R)} \cdot x(t)$ . In practice, we can assume that the transmission channels stay unchanged in a very short time. As a result, the environment parameters, i.e.,  $\gamma \cdot \gamma'/\gamma^*$ , can be considered static when a tag responds its EPC, which costs just several microseconds. Even if the attacker can run the same preprocessing algorithm, it is not able to get  $P_2^*(t)$  because it has no information of  $s'(t)$ .

In Fig. 11, we show an example of the preprocessing module. The raw data received at Rx is as shown in Fig. 11(a), the entire time between *ACK* and *QREP* (marked by a red rectangle) is covered by a random signal and the EPC signal can't be recognized. We zoom in the red rectangle and show first 1000 samples in Fig. 11(b). The blue curve is the EPC signal, while the red dotted line is the estimated  $s(t)$ . We show in Fig. 11(c) the signal after removing the random signal (first 1500 samples in the red rectangle in Fig. 11(a)), and find that we can recover the tag's EPC segment effectively. Canceling the Gaussian noise is very necessary, for the signal after GNC (the red curve) is much easier for decoding.

*Outliers Removal:* During the signal collection, we receive multiple responses from the tags. To make the feature extraction more accurate, we try to find out and remove the outliers among all the received signals. To reach this goal, we first transform the signals into the frequency domain with FFT (Fast Fourier Transform). This process can help us to extract the main characteristics of the signals, and ignore the tiny differences in the noisy fluctuations of the signals. As shown in Fig. 12, to get rid of the errors introduced by the absolute values, we map the profiles after FFT of the two tags into

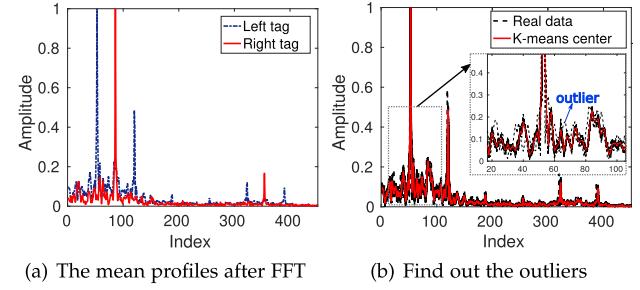


Fig. 12. The outlier removal with FFT.

a range of  $[0, 1]$ . Then we feed the processed signals into a k-means classifier. Fig. 12(a) shows the mean profiles (the center calculated by the k-means classifier) of the left tag and right tag in the k-means classifier. Then we compare the processed profiles of the received data (the dotted black line in Fig. 12(b)) with the k-means center (the red line in Fig. 12(b)), and find out the outliers by calculating their euclidean distances. Fig. 12(b) exhibits 10 profiles of the real data, and obviously, one of them (marked with 'outlier') has a nonnegligible difference with the profile of the k-means center. So we check the received signals and remove the outliers before feature extraction. The improvements in accuracy can be found in Sec. VII.

### C. Feature Extraction and Comparison

To defend against different types of attacks, we propose to use two features in Hu-Fu, namely the *coupling feature* and *authentication feature*. The coupling feature is to determine whether the Left Tag is indeed coupling with another tag, while authentication feature aims to verify whether the Right Tag is the legitimate one. The coupling feature can be used to detect signal replay and the authentication feature is effective to detect tag counterfeiting. Note that both the two features are insensitive to the environment, i.e., we can use them for tag authentication even if the registration phase and authentication phase happen at different locations.

*Extracting the Coupling Feature:* We first specify how to extract the coupling feature. In the signal collection module, Hu-Fu first collects the uncoupling signal of the Left Tag  $T_L$  and then records the coupling signals of both Left and Right Tags in the same situation. After pre-processing, let  $U_L$  denotes the signal of  $T_L$  in the non-coupling state,  $C_L$  and  $C_R$  denote the processed signals of  $T_L$  and  $T_R$  in the coupling state. Based on our model,

$$U_L(t) = \frac{\gamma \cdot \gamma'}{\gamma^*} \cdot \frac{h(R, T_L)}{h(R)} \cdot x(t)$$

$$C_L(t) = \frac{\gamma \cdot \gamma'}{\gamma^*} \cdot \frac{h(R, T_L, T_R)}{h(R)} \cdot x(t), \quad (16)$$

where  $h(R, T_L)$  represents the hardware characteristic parameters without inductive coupling, which can be modeled as  $\frac{\lambda^2 \cdot G_{Tx} \cdot G_{T_L}^2 \cdot |\Gamma_{T_L}|^2}{16\pi^2 \cdot D_R^2 \cdot T_L}$ . We define the coupling feature as:

$$F_c = \frac{\int_{t_s}^{t_e} C_L dt}{\int_{t_s}^{t_e} U_L dt}, \quad (17)$$

where  $t_s$  and  $t_e$  are the start and end time of the tag's EPC segment. We detect them by finding the sudden rising/falling edge of the received signal.  $F_c$  can be modeled as  $\int_{t_s}^{t_e} G_{T_L} \cdot [G_{T_L} - \frac{N_L}{R_L} \cdot \frac{dM_{LR}}{dt} \cdot G_{T_R}] dt$  according to Eq. 16 and 17. We find that  $F_c$  is independent of the environment and reader hardware. In addition,  $F_c$  can be used to detect signal replay attack. If the attacker uses a signal replayer but not the actual Right Tag at present, the Left Tag will transmit a non-coupling signal. Under this circumstance, the coupling feature  $F_c$  will be close to 1. However, if there is indeed exist a correct Right Tag, the coupling feature  $F_c$  is much less than 1. We also validate that different Right Tags may introduce different hardware parameter  $h(R, T_i, T_j)$ . Hence the coupling feature  $F_c$  is also able to authenticate the right tag. We further introduce the authentication feature that enhances the accuracy of detecting a different Right Tag.

*Extracting the Authentication Feature:* The coupling feature  $F_c$  is used by Hu-Fu to determine whether the Left Tag  $T_L$  is indeed coupled with another Right Tag. If the attacker utilizes a counterfeited Right Tag, it is likely that  $F_c$  will be different. However, in some cases, Hu-Fu may observe similar  $F_c$  for different Right Tags. Hence we propose two metrics as the authentication feature. The first metric is defined as the specific value of energy spectrum of the Left and Right Tags, i.e. :

$$F_e = \frac{\int_{t_s}^{t_e} C_L dt}{\int_{t_s}^{t_e} C_R dt}, \quad (18)$$

Based on Eq. 16,  $F_e$  can be modeled as

$$F_e = \frac{h(T_L, T_R) \cdot \int_{t_s}^{t_e} x_L(t) dt}{\int_{t_s}^{t_e} x_R(t) dt},$$

where  $h(T_L, T_R)$  is  $\frac{G_{T_L} \cdot |\Gamma_{T_L}|^2}{G_{T_R} \cdot |\Gamma_{T_R}|^2} \cdot \frac{G_{T_L} - \frac{N_L}{R_L} \cdot \frac{dM_{LR}}{dt} \cdot G_{T_R}}{G_{T_R} - \frac{N_R}{R_R} \cdot \frac{dM_{RL}}{dt} \cdot G_{T_L}}$ , only depending on the hardware characteristic of the two tags, and  $x_L(t)$  and  $x_R(t)$  are the data-dependent signal functions of the Left and Right Tags, respectively. We find that  $F_e$  is independent of the environment or reader. In addition to the hardware characteristics of  $T_L$  and  $T_R$ ,  $F_e$  also takes the data-dependent signal functions  $x(t)$  into consideration. However even though two Right Tags carry the same data, Hu-Fu will measure different values of the integral results (and hence different  $F_e$ ), because the BLF of different tags is different. We will show that even if the attacker utilizes a counterfeited Right Tag that owns the same ID as the legitimate one, it cannot pass the authentication.

To further improve the authentication accuracy of Hu-Fu, we propose another authentication metric, namely Power Spectral Density (PSD). The PSD feature reflects the distribution of power into frequency components composing that signal [37]. The second authentication metric  $F_p$  is defined as:

$$F_p(T_i) = \left| \int_{t_s}^{t_e} e^{-j2\pi f_i t} C_i(t) dt \right|^2, \quad (19)$$

where  $i$  can be 'L' or 'R'.  $f_L$  and  $f_R$  represent the corresponding frequencies of the Left and Right Tags. Hu-Fu calculates and records both  $F_p(T_L)$  and  $F_p(T_R)$  from each EPC segment of the two tags.

In practice, the surrounding moving objects may also introduce unpredictable errors. To tackle this problem, we pair each  $C_L$  and  $C_R$  that collected in an inventory round (as shown in Fig. 4), which have very adjacent reply time to calculate the authentication features.

We further define a vector  $[F_e, F_p(T_L), F_p(T_R)]$ . For an authenticatee tag, Hu-Fu calculates the *Cross Correlation Coefficient* (CORR) of the two authentication vectors collected at the registration and authentication phases.

*Authentication Logic:* The authentication of a presented tag returns either 'Accept' or 'Reject'. If the coupling feature  $F_c$  is larger than a threshold  $\varepsilon$  determined by empirical results, Hu-Fu immediately returns 'Reject'. Otherwise, Hu-Fu calculates CORR of the two authentication vectors collected at the registration and authentication phases. If CORR is larger than another threshold  $\rho$ , Hu-Fu returns 'Accept'. Note the choice of both  $\varepsilon$  and  $\rho$  is **universal** in a system: each of them uses one single value for all tags in a Hu-Fu system. We do not need to determine them for each individual tag.

## VI. SECURITY ANALYSIS

### A. Defend Against the Major Attacks

In this section, we provide the detailed analysis on how Hu-Fu defends against the four major attacks, namely tag-counterfeiting, signal replay, signal compensation, and brute-force feature replay. In addition, we also talk about the ability of Hu-Fu on coping with two crucial problems in RFID systems, namely the tag tracking attack and the signal modeling.

*Tag Counterfeiting:* Tag counterfeiting refers to that the attacker uses its own tag to carry the ID of a legitimate tag, and wants to get access to some region or resource. Tag counterfeiting attack is the most common attack in RFID systems. And most existing physical-layer authentication methods can defend against this type of attack. By analyzing the physical features from the signal from a tag, physical-layer authentication decides whether the presented tag has very similar features of the legitimate tag with the ID. In our design, both of the coupling feature and the authentication features are effective in distinguishing counterfeit tags. As aforementioned, due to the imperfection in the manufacturing, different tags have different physical-layer signals. In other words, the counterfeit tag is likely to have totally different coupling signal  $C_R$ . In addition, as we have proved in Sec. III and IV, the coupling signals of the left tag, i.e.,  $C_L$ , will also change if we use a different right tag. According to the feature definitions in Eq. 17 ~ 19, the counterfeit tag will have a different coupling feature  $F_c$ , and the authentication features  $F_e$  and  $F_p$  with that of the legitimate tags.

To demonstrate that the feature used in Hu-Fu is unique and can be used for authentication purpose, we conduct the following experiments. We use 101 ALN-9840 tags, pick one tag as the Left Tag, and use the other 100 tags as the Right Tag. We calculate the feature CORR of all pairs among the 100 Right tags, which are coupled with the same Left tag under the same situation. As shown in Fig. 13, we find that 84% features have distinctly different features ( $CORR < 0.5$ ). Only 0.55% of the CORR values show similar features of two Right Tags ( $CORR > 0.74$ , where 0.74 is the default value of threshold and can be set higher). We use other Right tags,

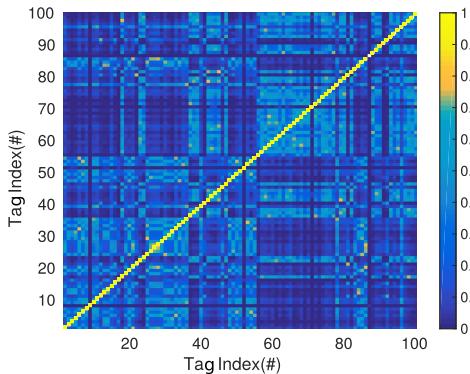


Fig. 13. CORR among 100 tags.

which show similar results. Hence Hu-Fu can successfully detect counterfeited tags that carry the same ID but different physical features. One potential problem of defending against tag counterfeiting is that, if the registration and authentication happens in different environments, including location changes and dynamic moving objects. We will show Hu-Fu is robust to environmental changes in §VII-C. An advanced tag counterfeiting attack is brute-force feature replay, which will be discussed later.

**Signal Replay Attack:** The attacker first eavesdrops on the backscatter communication of a legitimate tag, either during the registration/authentication period or using an unauthorized reader to query the tag. Then the attacker replays the identical signal to cheat the authenticator. Compared to tag counterfeiting, this attack requires a more powerful device at the attacker, which can replay signals. Existing methods are difficult in defending against signal replay. One unique advantage of Hu-Fu is that, even if an attacker can eavesdrop on all communication of a legitimate tag. None of these signals can pass Hu-Fu. The attacker can record the signal  $U_R$  of the legitimate tag in a non-coupling state, but  $U_R$  cannot pass Hu-Fu as shown in Fig. 1(d). It can also record the coupling signals  $C_L \cdot s$  and  $C_R \cdot s$  but replaying them does not work either, because next time the random signal is different. In addition, since simply replaying the signal will not make  $T_L$  in a coupling state, Hu-Fu can also detect signal replay if it finds  $T_L$  still transmits  $U_L \cdot s$ . Even if the attack may use both signal replay and a counterfeited tag, it still has no way to produce  $C_L \cdot s$  and  $C_R \cdot s$ . As a result, after the random signal removal, Hu-Fu will not have the right coupling signals  $C_L$  and  $C_R$  from the replay signals. Obviously, the wrong signals will eventually lead to invalid features, specifically,  $F_c$  and  $F_p$ .

**Signal Compensation Attack:** In signal compensation, the attacker knows the signal that can pass the authentication, denoted as  $\mathfrak{S}$ . Assume the current signal in the environment is  $\mathfrak{S}'$ . The attacker can compensate the existing signal  $\mathfrak{S}'$  to make it become  $\mathfrak{S}$ . Signal compensation might work if Hu-Fu is not protected by signal randomization. For example, the attacker eavesdrops on a prior registration or authentication of the legitimate tag and records  $C_L$  and  $C_R$ . Then it uses a faked tag and compensates any signal to make the signals be  $C_L$  and  $C_R$ . In Hu-Fu,  $C_L$  and  $C_R$  are protected by the one-time random signal  $s$ . The attacker can only get  $C_L \cdot s$  and  $C_R \cdot s$ , which will fail to pass the next authentication because Hu-Fu will use another random signal. The attacker has no idea about the coupling signals, not to mention reconstructing them. Similar to the signal replay attack, attackers that can

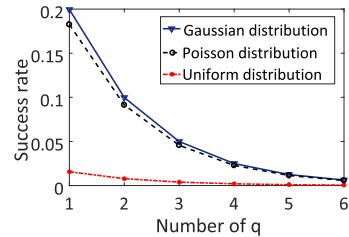


Fig. 14. Success rate that the attacker hit the right start point in a slot.

not provide the identical coupling signals  $C_L$  and  $C_R$  will not pass the system.

There is another reason that signal compensation to Hu-Fu is difficult. The RFID tags comply slotted-ALOHA-based communication protocol [34]. Based on the protocol, after receiving the slot number, *i.e.*,  $2^q$ , from the reader, tags will randomly select one slot to response. At that slot, a tag will wait for an uncertain time  $t_1$  and then start to transmit the backscatter signal. According to the protocol [34], the range of  $t_1$  is roughly from  $184\mu s$  to  $216\mu s$ . In other words, the tag may start to respond at any time during the  $32\mu s$ . Because Hu-Fu transmits a random signal during tag's backscatter, attackers have to guess at which time point the tag will start to transmit. To discuss the success possibility of attackers to hit the right start point and reconstruct the coupling signal, we conduct a simulation. In fact, we have no idea about the exact probabilistic model of  $t_1$ . So we use three common models, namely Gaussian distribution, Poisson distribution and Uniform distribution, to simulate it. As shown in Fig. 14, the success probability goes down with the increased number of slots. However, even under the worst case, *i.e.*, there are only 2 slots ( $q = 1$ ) in each inventory round and the values of  $t_1$  follow a Gaussian distribution, the attackers only have less than 20% probability to compensate the signal to the expected one successively.

By combining the two reasons, Hu-Fu is resilient to the signal compensation attack.

**Brute-Force Feature Replay Attack:** Assuming the attacker knows the feature extraction algorithms and obtains sufficiently many tags, it extracts the feature of every tag until getting one tag that presents a feature close enough to the legitimate tag. Then that tag can be used as a strong counterfeit. Hu-Fu is also resilient to brute force attack. Since Hu-Fu randomizes the communication channel between the reader and the legitimate tags, the coupling signals are difficult to obtain. Hence the attacker does not know the valid features, even if the attacker knows the feature extraction algorithms. It is impossible to find an unknown feature from the tags owned by the attacker. In other words, the attackers do not know exactly what the coupling signals  $C_L$  and  $C_R$  are, not to mention find out a fake tag that has the similar coupling feature  $F_c$  and authentication features  $F_e$  and  $F_p$  with that of the legitimate one.

**Tag Tracking Attack:** Tag tracking does not target on the authenticity of an RFID system, but on the privacy. Hence as an authentication method, Hu-Fu does not need to be resilient to tag tracking, but it still worths discussion. Current COTS passive tags have no ability to protect their replies being eavesdropped by an attacker. The tag locations and moving trajectories can be tracked. In §VII-B we use experiments to show that a single-antenna eavesdropper is unable to decode any ID information from the signal that being covered by randomization. Hence Hu-Fu also improves the tag privacy.

**Signal Modeling:** A crucial concern is that whether an attacker can model the interactions between legitimate tags if he could obtain their uncoupling signals. Our answer is that modeling and reconstructing the coupling signals of the legitimate tags are extremely difficult. There are two reasons: 1) As aforementioned in Section. II-A, we assume the Left tag is always under higher security protection. Hence the attacker cannot access the uncoupling signals of the Left tag. Only obtaining the uncoupling signal of the Right tag is not enough to infer their interactions. 2) There remains a huge gap between molding the interaction of a tag pair and obtaining their uncoupling signals. Due to the complexity of indoor environments, both the signal collection and reply are vulnerable to the environment changes. Even if the attacker can extract the corresponding characteristics of the Right tags, they are not able to infer the environment variation at the current moment. During the authentication process, the signal from the Left tag includes environment factors and an attacker is difficult to create the coupling signals of both Left and Right tags.

### B. Feature Space Analysis

Intuitively, utilizing two tags, instead of using one tag, as a entirety for authentication will increase the authentication feature space. The feature space refers to the number of categories the system can distinguish. For example, if the feature space of one-tag-case is  $\mathfrak{R}$ , there are at least two tags that can not be successfully distinguished with each other when the tag population is larger than  $\mathfrak{R}$ . In this section, we will discuss the feature space of Hu-Fu.

In fact, the feature space of Hu-Fu is highly related to the use case and requirements. We consider this problem according two aspects, one is the usage mode of the left tag and another is the impact of different ID numbers. For the first aspects, we consider two usage modes of the left, *i.e.*, one left tag mode and multiple left tag mode. For example, some scenarios only employ one left tag to authenticate all the users, *e.g.*, entrance guard. In contrast, some use cases need multiple left tags, *e.g.*, baggage claim, where each user has one left tag and one right tag. In this case, different users use different left tags as the authenticator. Only if the features of both of the two tags are identical to the records in our system, the user can pass the authentication process. Hence, in the multiple-left-tag case, both the left tag and right tag have a feature space of  $\mathfrak{R}$ . And eventually, the multi-left-tag case has a feature space of  $\mathfrak{R}^2$ .

Another aspect is the impact of different ID numbers.<sup>6</sup> As aforementioned, if we have more than  $\mathfrak{R}$  tags, at least two tags can not be distinguished by our system, *i.e.*, will be classified into the same category. However, if we set the tags that in the same category with different IDs, their features may also show tiny differences. As long as the tiny differences make their similarity reduced and lower than the threshold  $T$ , the tags even in the same category will also be distinguished. We discuss the feature spaces under these two situations and show them in Table. I. The calculation details can be found in Appendix B (supplementary material). The results show that Hu-Fu has a significant larger feature space than single-tag-based authentication systems.

## VII. IMPLEMENTATION AND EVALUATION

### A. Prototype Implementation

We implement a prototype system of Hu-Fu with a USRP N210 equipped with an SBX daughter-board and two Laird

<sup>6</sup>The RFID reader can change the tag ID to a 96-bit hexadecimal string.

TABLE I  
THE FEATURE SPACE OF HU-FU

	One $T_L$	Multiple $T_L$
with the same ID	$\mathfrak{R}$	$\mathfrak{R}^2$
with different IDs	$[2 \cdot T] \cdot \mathfrak{R}$	$([2 \cdot T] \cdot \mathfrak{R})^2$

S9028-PCL directional antennas. The center frequency of USRP-based SDR reader [35], [36], [38] varies among [905MHz, 910MHz, 915MHz, 920MHz, 925MHz]. Note that in practice, we can randomly select center transmitting frequency from 902MHz to 928MHz. The sampling rate is 2MHz, and the transmission gain and receiving gain are both 25dB. The distance between the reader and tag pairs is 20cm. We have verified that most main-stream brands and models of passive RFID tags have the inductive coupling phenomenon and can be used in Hu-Fu, including ALN-9740, ImpinJ E41C/B, and Alien 964X. The prototype is compatible to the standard EPC Class 1 Generation 2 protocols (C1G2) [34]. In our experiments, we run our prototype at a Dell desktop, which equips Intel Core i7-7700 CPU at 3.6 GHz and 16G memory.

As aforementioned, Hu-Fu has the registration phase and authentication phase. At the registration phase of a tag  $T_R$ , Hu-Fu collects the features introduced in § V-C. Then the features are stored in a database running on a back-end server, indexed by the tag ID. At the authentication phase of the tag, Hu-Fu calculates its features and compared them to the stored features of the same tag ID. Hu-Fu returns either ‘Accept’ or ‘Reject’.

### B. Evaluation of Randomization

**Methodology:** We evaluate whether an attacker can obtain any useful information from Hu-Fu to conduct signal or feature replay attacks. Since tag replies will be covered by a one-time random signal, replaying the same signal will absolutely result in a ‘Reject’ because the random signal is different. We further ask an easier question to the attacker: whether it is able to decode or infer any bit from the tag replies covered by random signals. Note even if an attacker can decode the bits, it is still not able to conduct a successful reply attack. We conduct a set of experiments that use Hu-Fu to query 50 commercial tags in different models for 1000 times in total. The experiments are conducted in both static and dynamic scenarios. In static scenarios (St), registration and authentication happen at the same place. In dynamic scenarios (Dy), they happen in different places. We allow an eavesdropper to obtain the signal of the entire communication, which then tries to decode the signal by reading the rising and falling edges. We measure the Bit Error Rate (BER) of the eavesdropper.

Fig. 16 shows the cumulative distribution of the BER for the eavesdropper in St and Dy as well as the random guess (*i.e.*, amplitude  $> 50\%$  to 1 and  $\leq 50\%$  to 0). We find the BER for all three cases are extremely close to 50%, which implies they provide almost no information of the bits of tag replies. The average BER for St and Dy are 52.85% and 53.18%, with a standard deviation of 1.27% and 1.79%, respectively. The eavesdropper is not obviously better than a random guess. On the other hand, the BER of Hu-Fu in all 100 experiments is always 0.

### C. Evaluation of Authentication Quality

**Methodology:** We first evaluate the authentication accuracy of Hu-Fu in both static and dynamic scenarios. We define

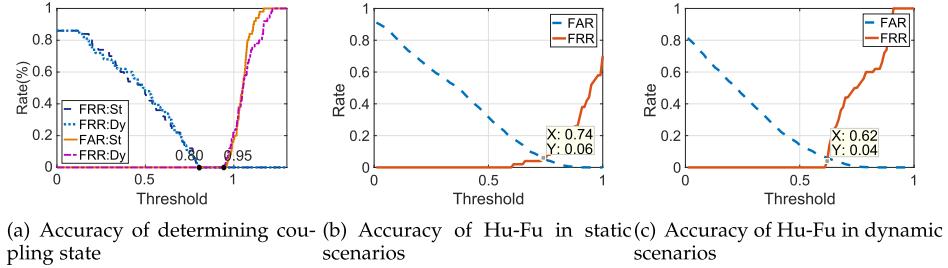


Fig. 15. Accuracy of Hu-Fu.

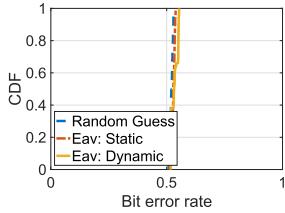


Fig. 16. BER of an eavesdropper.

two accuracy metrics of physical-layer authentication, namely *False Accept Rate* (FAR) and *False Reject Rate* (FRR):

$$FAR = n_a/n_n; \quad FRR = n_r/n_l$$

where  $n_n$  is the number of tests that use non-legitimate tags,  $n_a$  is the number of ‘Accept’ results among tests using non-legitimate tags,  $n_l$  is the number of tests that use legitimate tags, and  $n_r$  is the number of ‘Reject’ results among tests using legitimate tags. FRR is also equal to  $1 - \text{Recall}$ . Note in practice, false acceptances are usually considered more harmful and critical than false rejections. It is because the users that are falsely rejected will usually go through other off-line and more reliable authentication processes, such as verifying their photo IDs or other certificates. On the other hand, false acceptance will allow an illegal user to get access to the protected area/objects. In addition to FAR and FRR, we use the *classification accuracy*, a metric that has been used by existing physical-layer identification methods [21], [23] for comparison. These experiments work as follows. Each method collects the testing features from a number of tags and classify each feature to one of the existing stored features that were from these tags. The accuracy is the rate of features that are correctly classified.

Note in the experiments, we give a huge advantage to the attacker by assuming the tag ID matching is always correct. However in actual cases since Hu-Fu hides the tag replies, the attacker has no information of the tag ID (see results in §VII-B) if we can protect the Right Tag carefully from being queried by a malicious reader. **Hence even though the results show some level of FAR, the actual FAR of a practical attacker is still almost 0 if it has no information of the tag ID.**

**Accuracy of Determining a Coupling Tag:** The first step of the authentication logic is to compare the coupling feature  $F_c$  with the threshold  $\varepsilon$ . Fig. 15(a) exhibits the FRR and FAR of Hu-Fu for determining the coupling state. Note that the FRR and FAR here are not calculated based on the final authentication results, but only the middle results for determining the coupling state of the Left Tag. We find that FAR and FRR in both St and Dy drop to 0 when  $\varepsilon$  is in the range of [0.8, 0.95]. This result is robust to different models of tags. Hence determining a coupling Left Tag is highly accurate. In other experiments, we set the threshold  $\varepsilon$  as 0.85.

TABLE II  
ACCURACY COMPARISON

	Hu-Fu	[COV,PSD]	[TIE,ABP]	Spectral
St	95%	99%	96%	99.6%
Dy	90%	77.8%	36.24%	37.6%

TABLE III  
HU-FU ACCURACY WITH MOBILITY

Coupling state	Authentication (FAR,FRR)
	(0%, 0%)

**Accuracy of Hu-Fu :** After verifying the coupling state, Hu-Fu determines whether the CORR of authentication features that collected at registration and authentication phases is larger than the threshold  $\rho$ . It returns ‘Accept’ if  $\text{CORR} > \rho$  and ‘Reject’ otherwise. We show the FRR and FAR for static cases in Fig. 15(b) and for dynamic cases in Fig 15(c), by varying the threshold  $\rho$ . We find that when  $\rho = 0.74$  in St, both the FAR and FRR are 6%. We set  $\rho = 0.83$  to make FAR  $< 2\%$  and allow 10% FRR. When  $\rho = 0.62$  in Dy, both the FAR and FRR are 4%. However, to make FAR  $< 2\%$ , FRR may be a slightly higher than 10%.

**Comparison to Existing Methods:** We compare Hu-Fu to existing physical-layer identification methods, including the COV and PSD method used in Geneprint [23], the time interval error (TIE), average baseband power (ABP), and spectral feature (SP) proposed by Zanetti *et al.* [21], [39]. We perform these methods in both static and dynamic cases, and use a Bayesian classifier to classify 50 tags. We conduct multiple production experiments for every tag. The classification results are shown in Table II. In St, all methods have high accuracy. Hu-Fu has a little lower accuracy than other methods. That is because signal processing, including the Gaussian noise and random signal removal, will more or less distort the tag’s signals and introduce unpredictable errors in authentication. However, in Dy, only Hu-Fu can maintain a high accuracy and other methods are not resilient to environment changes. Note none of the prior methods can defend against reply attacks. Hu-Fu achieves an extra advantage of accuracy in Dy, because it can use a pair of tags to eliminate environmental factors.

**Accuracy After Outlier Removal:** In Sec. V, we propose to remove the outliers among the received signals before feature extraction. In Tab. IV, we elaborates the accuracies with or without outlier removal. We reuse the experiments data in Tab. II and find that with the outlier removal, we have a 2% or 3% improvement on the accuracy in the static case and dynamic case, respectively. Hence the outlier removal is very effective and necessary.

**Time Cost of Hu-Fu :** Hu-Fu is fast. In our experiments, all authentication decisions are made within 1.5 seconds. Existing work do not mention their authentication times. We believe

TABLE IV  
ACCURACY WITH OUTLIER REMOVAL

Performance	w/o outlier removal	w/ outlier removal
St	95%	97%
Dy	90%	93%

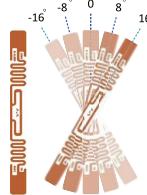


Fig. 17. The intersection angle of two tags.

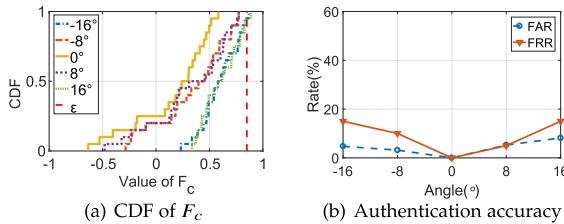


Fig. 18. Accuracy by varying the angle.

that 1.5 seconds is an acceptable time for authentication applications.

#### D. Impact of Environmental Factors

In this section, we evaluate the performance of Hu-Fu under the impacts of practical factors. Note that we do not alter the system threshold. Because we have no idea about the environmental factors at each moment.

**In Mobility Environments:** Moving persons and objects around the reader usually cause unstable signals due to multipath reflection [16]. To evaluate the robustness of Hu-Fu with moving objects, we conduct the experiments by allowing a person walking around the reader with a speed of  $1 \sim 2$ m/s. We first register 50 right tags in one place, and then authenticate them at another place. The results are shown in Table III. We find that Hu-Fu still achieves 100% accuracy in determining a coupling Left Tag. The FAR and FRR of authentication the right tag do not increase much.

**Varying Tag Angles:** We evaluate the performance of Hu-Fu when the Right Tag is not fully parallel to the Left Tag. We define the intersection angle between Left and Right Tags as the angle between their antenna directions as shown in Fig. 17. The separation distance between two tags' centers is 2cm. We first collect the signals when the left tag is fully parallel to the right tags as the registration record, and then utilize the signals when the two tags have intersection angles as the authentication data. We exhibit the values of the coupling feature  $F_c$  for different angles in Fig. 18. The red dashed line is the threshold. When the angle is no more than  $\pm 8^\circ$ , all  $F_c$  values are smaller than the threshold, which means the coupling determination is always correct. For tags that with  $\pm 16^\circ$  intersection angles, Hu-Fu has a FAR of 5%. The authentication error rates are shown in Fig. 18(b). We find that the FARs are no more than 5% and the FRRs are no more than 10%, when the angle is between  $-16^\circ$  to  $8^\circ$ . According to the results, we can safely infer that an intersection angle smaller than about  $8^\circ$  may not impact the results significantly. Intersection angles larger than  $8^\circ$  are very obvious and easy to correct.

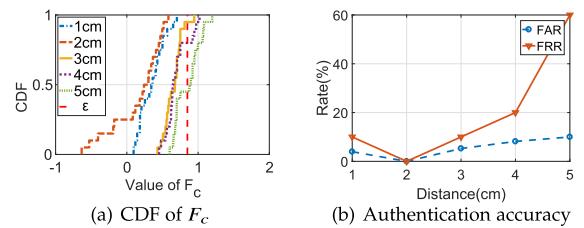


Fig. 19. Accuracy by varying the distances.

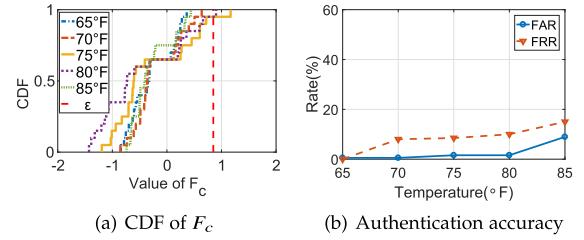


Fig. 20. Accuracy by varying the temperature.

**Varying Tag Distances:** We evaluate whether the separation distance between the Left and Right Tags is a factor that may influence the authentication results. We use the records that the two tags have a 2cm separation distance as the registration data. Then we move the right tag with a separation distance from 1cm to 5cm. Fig. 19(a) exhibits the CDF of coupling feature  $F_c$  by varying the distances. We find that the coupling features of tags with a distance smaller than 4cm are mostly smaller than the threshold  $\varepsilon$ . The authentication error rates are shown in Fig. 19(b), the FARs for 1cm to 3cm distances are all smaller than 10%. Hence by slightly moving the Right Tag, the results are still reliable.

**Varying the Temperature:** The outside temperature may change the hardware characteristic of the RFID tag and make its signals distort. In this set of experiments, we will discuss the impact of temperature on the system's performance. We first collect registration data at  $18.3^\circ\text{C}$  ( $65^\circ\text{F}$ ) and then heat the room to conduct authentication at  $21.1^\circ\text{C}$  ( $70^\circ\text{F}$ ),  $23.9^\circ\text{C}$  ( $75^\circ\text{F}$ ),  $26.7^\circ\text{C}$  ( $80^\circ\text{F}$ ), and  $29.4^\circ\text{C}$  ( $85^\circ\text{F}$ ), respectively. As shown in Fig. 20, most coupling states can be accurately determined when the temperature changes. The authentication FAR and FRR for different temperatures  $\leq 80^\circ\text{F}$  are extremely low ( $\leq 1.5\%$  and  $\leq 10\%$ ), but increase for  $\leq 85^\circ\text{F}$ . As long as the system operator keeps the temperature  $\leq 80^\circ\text{F}$ , Hu-Fu has stable accuracy.

## VIII. RELATED WORK

Recent effort has been made to authenticating RFID tags. Most existing solutions fall into two categories: crypto-based and physical-layer approaches.

Crypto-based approaches aim to utilize conventional cryptographic algorithms to perform the authentication. After allowing each tag to share a secret key with the reader, the reader will accept a tag as a valid one only if the tag can replay a cipher depending on the secret [40]–[44]. Feldhofer *et al.* propose a low-power authentication protocol using the AES Algorithm in [40] and analyze the standardized cryptographic algorithms like SHA-256, SHA-1 and AES-128 in RFID system in [42]. Engels *et al.* [41] present a lightweight encryption scheme, which can provide designed security with small block size and is resistant to the attacks such as linear and differential cryptanalysis. And tag authentication protocols based on randomized skip lists-based authentication (RSLA), and Randomized Skip Graphs-Based Authentication (RSGA) are also discussed in [43] and [44]. However, Crypto-based

methods suffer from several drawbacks. First, it is difficult for these methods to be implemented on COTS passive tags as they are commonly with a need of changing the current industrial standards and introducing non-trivial financial cost and labor cost. To our knowledge, the only tag claimed with a cryptographic function is the NXP UCODE DNA RFID [19], but its price is much higher than COTS tags (\$67,000 for 77K tags, not available for purchase under 77K tags). Its performance and actual security level are unclear to the public, because there is no report from its users. Using tags with a cryptographic function may have several limitations. First, the current main-stream COTS tags need to be replaced, which introduce non-trivial financial cost and labor cost. Second, the process of storing secret key on tags may also be vulnerable to some eavesdropping and active attacks. Third, if the secret keys are stolen, it will be easy for attackers to produce unlimited counterfeit tags. In contrast, Hu-Fu does not need to modify the protocol or substitute the deployed tags. In addition, it is infeasible for an attacker to produce many counterfeits that can pass the authentication. Our conclusion is, even if on-chip cryptographic passive tags would be available in future, Hu-Fu still has its unique advantages.

Physical-layer identification approaches leverage the hardware diversity of tags [20], [21], [23], [45], [46] caused by manufacturing imperfection. Danev *et al.* [20] show the feasibility of using the physical-layer information to detect cloned or counterfeit RFID tag. Zanetti *et al.* [21] further propose physical-layer identification of UHF RFID using the time interval error (TIE), average baseband power (ABP) and spectral feature as the fingerprints. Periaswamy *et al.* [47] use a specific device to extract the Minimum Power Response of RF signals as the fingerprint. Geneprint [23] utilizes the covariance among the square waves of two tags' signals as the fingerprint, which reduces the cost of feature extraction. These methods name themselves as 'identification' rather than 'authentication' and they are not robust against the signal-replay, brute force, and signal compensation attacks [24]. Physical-layer identification has also been investigated for other wireless devices such as 802.11 and 802.15.4 [22], but there is no effective solution for the attacks mentioned in §I. RF-Cloak [28] is a recent solution that protects tags from eavesdropping. It is the first work to introduce signal randomization. However, it mainly focuses on providing confidentiality and does not validate tag authenticity.

## IX. CONCLUSIONS

Hu-Fu is a physical layer authentication method for battery-free IoT devices, in particular, passive RFID tags. Hu-Fu is the first solution that is resilient to a number of major attacks to physical layer authentication, including tag counterfeiting, signal replay, signal compensation, and brute-force feature reply. We build a prototype of Hu-Fu and the results show that Hu-Fu can achieve reliable accuracy under environmental changes.

## ACKNOWLEDGMENT

The authors thank the anonymous reviewers for their suggestions and comments.

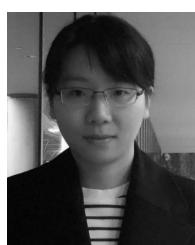
## REFERENCES

- [1] L. Shangguan, Z. Zhou, X. Zheng, L. Yang, Y. Liu, and J. Han, "Shop miner: Mining customer shopping behavior in physical clothing stores with COTS RFID devices," in *Proc. 13th ACM Conf. Embedded Netw. Sensor Syst.*, 2015, pp. 113–125.
- [2] S. Jog, J. Wang, J. Guan, T. Moon, H. Hassanieh, and R. R. Choudhury, "Many-to-many beam alignment in millimeter wave networks," in *Proc. NSDI*, 2019, pp. 783–800.
- [3] J. Wang, J. Zhang, R. Saha, H. Jin, and S. Kumar, "Pushing the range limits of commercial passive RFIDs," in *Proc. NSDI*, 2019, pp. 301–316.
- [4] X. Li, M. Wang, H. Wang, Y. Yu, and C. Qian, "Toward secure and efficient communication for the Internet of Things," *IEEE/ACM Trans. Netw.*, vol. 27, no. 2, pp. 621–634, Apr. 2019.
- [5] X. Li, M. Wang, S. Shi, and C. Qian, "VERID: Towards verifiable IoT data management," in *Proc. Int. Conf. Internet Things Design Implement. (IoTDI)*, 2019, pp. 118–129.
- [6] G. Wang *et al.*, "A (near) zero-cost and universal method to combat multipaths for RFID sensing," in *Proc. IEEE 27th Int. Conf. Netw. Protocols (ICNP)*, Oct. 2019, pp. 1–4.
- [7] G. Wang *et al.*, "Verifiable smart packaging with passive RFID," *IEEE Trans. Mobile Comput.*, vol. 18, no. 5, pp. 1217–1230, May 2019.
- [8] H. Cai, G. Wang, X. Shi, J. Xie, M. Wang, and C. Qian, "When tags 'read' each other: Enabling low-cost and convenient tag mutual identification," in *Proc. IEEE 27th Int. Conf. Netw. Protocols (ICNP)*, Oct. 2019, pp. 1–11.
- [9] X. Shi *et al.*, "TagAttention: Mobile object tracing without object appearance information by vision-RFID fusion," in *Proc. IEEE 27th Int. Conf. Netw. Protocols (ICNP)*, Oct. 2019, pp. 1–11.
- [10] Z. Li, Y. Xie, M. Li, and K. Jamieson, "Recitation: Rehearsing wireless packet reception in software," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, 2015, pp. 291–303.
- [11] C. Qian, H. Ngan, Y. Liu, and L. M. Ni, "Cardinality estimation for large-scale RFID systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 9, pp. 1441–1454, Sep. 2011.
- [12] Y. Zheng, M. Li, and C. Qian, "PET: Probabilistic estimating tree for large-scale RFID estimation," in *Proc. IEEE ICDCS*, Jun. 2011, pp. 37–46.
- [13] J. Ou, M. Li, and Y. Zheng, "Come and be served: Parallel decoding for COTS RFID tags," in *Proc. ACM MOBICOM*, 2015, pp. 500–515.
- [14] F. Adib, Z. Kabelac, and D. Katabi, "Multi-person localization via RF body reflections," in *Proc. USENIX NSDI*, 2015, pp. 279–292.
- [15] J. Wang and D. Katabi, "Dude, where's my card?: RFID positioning that works with multipath and non-line of sight," *SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 51–62, Aug. 2013.
- [16] 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 *Proc. 20th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2014, pp. 237–248.
- [17] H. Ding *et al.*, "Human object estimation via backscattered radio frequency signal," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 1652–1660.
- [18] T. Liu, L. Yang, Q. Lin, Y. Guo, and Y. Liu, "Anchor-free backscatter positioning for RFID tags with high accuracy," in *Proc. IEEE Conf. Comput. Commun.*, Apr./May 2014, pp. 379–387.
- [19] NXP UCODE DNA RFID. Accessed: Jan. 2019. [Online]. Available: <https://www.nxp.com/docs/en/fact-sheet/UCODEDNATRACKLF.pdf>
- [20] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of RFID devices," in *Proc. Usenix Secur. Symp.*, 2009, pp. 199–214.
- [21] D. Zanetti and B. Danev, "Physical-layer identification of UHF RFID tags," in *Proc. 16th Annu. Int. Conf. Mobile Comput. Netw.*, 2010, pp. 353–364.
- [22] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv.*, vol. 45, no. 1, pp. 1–29, Nov. 2012.
- [23] J. Han *et al.*, "GenePrint: Generic and accurate physical-layer identification for UHF RFID tags," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 846–858, Apr. 2016.
- [24] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. 3rd ACM Conf. Wireless Netw. Secur. (WiSec)*, 2010, pp. 89–98.
- [25] B. D. Danev, "Physical-layer identification wireless devices," Ph.D. dissertation, Dept. Comput. Sci., ETHZ, Zürich, Switzerland, 2011.
- [26] R. K. Wangness, *Electromagnetic Fields*. Hoboken, NJ, USA: Wiley, 1986, p. 608.
- [27] J. Han *et al.*, "Twins: Device-free object tracking using passive tags," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1605–1617, Jun. 2016.
- [28] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, "Securing RFIDs by randomizing the modulation and channel," in *Proc. NSDI*, 2015, pp. 235–249.

- [29] N. Marquardt and A. Taylor, "RFID reader detector and tilt-sensitive RFID tag," in *Proc. ACM CHI*, 2009.
- [30] H. Ding *et al.*, "Preventing unauthorized access on passive tags," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2018, pp. 1115–1123.
- [31] K. Koscher, A. Juels, V. Brajkovic, and T. Kohno, "EPC RFID tag security weaknesses and defenses: Passport cards, enhanced drivers licenses, and beyond," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, 2009, pp. 33–42.
- [32] *ThinkMagic Evaluation Kit*. Accessed: Jan. 2019. [Online]. Available: <https://www.jadaktech.com/products/thingmagic-rfid/>
- [33] X. Chen, F. Lu, and T. Y. Terry, "The 'weak spots' in stacked UHF RFID tags in NFC applications," in *Proc. IEEE RFID*, Apr. 2010, pp. 181–186.
- [34] *EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz*, EPC Global, Brussels, Belgium, 2005.
- [35] N. Kargas, F. Mavromatis, and A. Bletsas, "Fully-coherent reader with commodity SDR for Gen2 FM0 and computational RFID," *IEEE Wireless Commun. Lett.*, vol. 4, no. 6, pp. 617–620, Dec. 2015.
- [36] M. Buettner and D. Wetherall, "A software radio-based UHF RFID reader for PHY/MAC experimentation," in *Proc. IEEE Int. Conf. RFID*, Apr. 2011, pp. 134–141.
- [37] P. Stoica *et al.*, *Spectral Analysis of Signals*, vol. 1. Upper Saddle River, NJ, USA: Prentice-Hall, 2005.
- [38] L. Shangguan. *USRP Gen2 Reader*. Accessed: Mar. 3, 2016. [Online]. Available: <https://github.com/shanggdk/Gen2-UHF-RFID-Reader/>
- [39] D. Zanetti, P. Sachs, and S. Capkun, "On the practicality of UHF RFID fingerprinting: How real is the RFID tracking problem?" in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.* Berlin, Germany: Springer, 2011, pp. 97–116.
- [40] M. Feldhofer, "Comparison of low-power implementations of trivium and grain," in *Proc. State Art Stream Ciphers, Workshop Rec.*, Jun. 2007, pp. 236–246.
- [41] D. Engels, M.-J.-O. Saarinen, P. Schweitzer, and E. M. Smith, "The hummingbird-2 lightweight authenticated encryption algorithm," in *Proc. Int. Workshop Radio Freq. Identificat., Secur. Privacy*. Berlin, Germany: Springer, 2011, pp. 19–31.
- [42] M. Feldhofer and J. Wolkerstorfer, "Strong Crypto for RFID tags—A comparison of low-power hardware implementations," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2007, pp. 1839–1842.
- [43] 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 Trans. Dependable Secure Comput.*, vol. 13, no. 6, pp. 657–671, Nov. 2016.
- [44] Y. Komori, K. Sakai, and S. Fukumoto, "Fast and secure tag authentication in large-scale RFID systems using skip graphs," *Comput. Commun.*, vol. 116, pp. 77–89, Jan. 2018.
- [45] Y. Hou, J. Ou, Y. Zheng, and M. Li, "PLACE: Physical layer cardinality estimation for large-scale RFID systems," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 2702–2714, Oct. 2016.
- [46] G. Wang, C. Qian, H. Cai, J. Han, H. Ding, and J. Zhao, "Replay-resilient physical-layer authentication for battery-free IoT devices," in *Proc. 4th ACM Workshop Hot Topics Wireless HotWireless*, 2017.
- [47] S. C. G. Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID tags," *IEEE Trans. Depend. Sec. Comput.*, vol. 8, no. 6, pp. 938–943, Nov./Dec. 2011.



**Ge Wang** (Member, IEEE) received the Ph.D. degree from Xi'an Jiaotong University in 2019. She was a Visiting Student with the University of California Santa Cruz from 2017 to 2019. Her research interests include wireless sensor network, RFID, and mobile computing.



**Haofan Cai** (Member, IEEE) received the B.Eng. degree from the Southern University of Science and Technology in 2016. She is currently pursuing the Ph.D. degree with the University of California Santa Cruz. Her research interests include wireless sensor networks and RFID.



**Chen Qian** (Member, IEEE) received the Ph.D. degree from The University of Texas at Austin in 2013. He is currently an Assistant Professor with the Department of Computer Engineering, University of California Santa Cruz. His research interests include computer networking, data-center networks, software-defined networking, and mobile computing.



**Jinsong Han** (Senior Member, IEEE, ACM) received the Ph.D. degree in computer science from The Hong Kong University of Science and Technology in 2007. He is currently a Professor with Zhejiang University, and also with the Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies. His research interests focus on mobile computing, RFID, and wireless networks. He is a Senior Member of the ACM.



**Shouqian Shi** (Member, IEEE) received the B.Sc. degree from the University of Science and Technology of China. He is currently pursuing the Ph.D. degree with the Department of Computer Engineering, UC Santa Cruz. His research interests include computer networks and cloud computing.



**Xin Li** received the Ph.D. degree from the Department of Computer Engineering, University of California Santa Cruz. His research interests lie in computer networking, cloud computing, Internet of Things, and cybersecurity.



**Han Ding** (Member, IEEE) received the Ph.D. degree in computer science and technology from Xi'an Jiaotong University in 2017. She is currently an Assistant Professor with Xi'an Jiaotong University. Her research interests focus on RFID systems and smart sensing.



**Wei Xi** (Member, IEEE, ACM) received the Ph.D. degree in computer science and technology from Xi'an Jiaotong University in 2014. He is currently an Associate Professor with Xi'an Jiaotong University. His research interests focus on wireless networks, smart sensing, and mobile computing. He is a member of the CCF and ACM.



**Jizhong Zhao** (Member, IEEE, ACM) received the Ph.D. degree in computer science and technology from Xi'an Jiaotong University in 2001. His research interests focus on computer software, pervasive computing, distributed systems, and network security. He is a member of the CCF and ACM.