Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions

Prosanta Gope, Jemin Lee, *Member, IEEE*, and Tony Q. S. Quek, *Fellow, IEEE*

***Abstract*— Radio frequency identification (RFID) has been considered one of the imperative requirements for implementation of Internet-of-Things applications. It helps to solve the identification issues of the things in a cost-effective manner, but RFID systems often suffer from various security and privacy issues. To solve those issues for RFID systems, many schemes have been recently proposed by using the cryptographic primitive, called physically uncloneable functions (PUFs), which can ensure a tamper-evident feature. However, to the best of our knowledge, none of them has succeeded to address the problem of privacy preservation with the resistance of DoS attacks in a practical way. For instance, existing schemes need to rely on exhaustive search operations to identify a tag, and also suffer from several security and privacy related issues. Furthermore, a tag needs to store some security credentials (e.g., secret shared keys), which may cause several issues such as loss of forward and backward secrecy and large storage costs. Therefore, in this paper, we first propose a lightweight privacy-preserving authentication protocol for the RFID system by considering the ideal PUF environment. Subsequently, we introduce an enhanced protocol which can support the noisy PUF environment. It is argued that both of our protocols can overcome the limitations of existing schemes, and further ensure more security properties. By analyzing the performance, we have shown that the proposed solutions are secure, efficient, practical, and effective for the resource-constraint RFID tag.**

***Index Terms*— Anonymity, lightweight, authentication, radio frequency identification (RFID), physically uncloneable functions (PUFs).**

Manuscript received November 24, 2017; revised March 15, 2018; accepted April 4, 2018. Date of publication May 3, 2018; date of current version May 23, 2018. This work was supported in part by SUTD-ZJU Research Collaboration under Grant SUTD-ZJU/RES/01/2016, in part by the National Research Foundation of Korea through the Korean Government (MSIP) under Grant 2017R1C1B2009280, and in part by the DGIST Research and Development Program of the Ministry of Science and ICT under Grant 18-EE-01. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yiorgos Makris. *(Corresponding author: Jemin Lee.)*

P. Gope was with iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design, Singapore 487372. He is now with the National University of Singapore, Singapore 119077 (e-mail: prosanta.nitdgp@gmail.com).

J. Lee is with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu 43016, South Korea (e-mail: jmnlee@dgist.ac.kr).

T. Q. S. Quek is with the Information Systems Technology and Design Pillar, Singapore University of Technology and Design, Singapore 487372 (e-mail: tonyquek@sutd.edu.sg).

This paper has supplementary downloadable material at http://ieeexplore.ieee.org, provided by the authors. The file consists of specification of the proposed scheme in high-level protocol specific language (HLPSL). The material is 112 KB in size.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2018.2832849

I. Introduction

RADIO frequency identification (RFID) technology is getting more involved in several IoT applications ranging from health-care to anti-counterfeiting protection. A typical RFID system consists of three components: RFID tag, reader, and a backend server. One of the key features of the RFID system is that a tag can be interrogated by a reader without line-of-sight contact. Therefore, RFID technology poses a great deal of security threats related to tag user's privacy, including the revelation of sensitive information and user location tracking [1]. In some cases, if a reader can be malicious then it can reveal the current location of the tag user to an adversary. Therefore, it is important that the interrogating process in the RFID system must be anonymous, where no one except the backend server should be able to know the exact identity of the tag.

In general, RFID tags are considered as the resource constrained devices, accordingly it is always feasible to use lightweight cryptographic primitives in designing anonymous authentication protocol for RFID system. Therefore, most of the RFID authentication protocols use symmetric-key system such as hash function. On the other hand, physically uncloneable functions (PUFs) [2] have gained popularity as an alternative primitive for providing security in RFID system. PUFs are the result of the manufacturing process of integrated circuits (ICs), which introduce random physical verifications into the micro structure of IC, to make it unique. PUFs are basically ICs which use their internal structures to provide one-way function that cannot be duplicated. The PUFs are easy to be constructed with a few number of gates [3] and their outputs are difficult to predict but easy to evaluate. This makes them to be a good choice for use as a security primitives for RFID system.

A. Possible Security Threats and Attacks in the RFID System

Since the communication channel between the tag and reader is insecure that makes the RFID system vulnerable to the flowing security threats and attacks.

1) Privacy Against Eavesdropper (PAE): Due to the insecure radio frequency channel, the communication between tag and reader can be easily eavesdropped. After eavesdropping, an attacker can monitor the tag to know user's location and movement, when the tag identifier is fixed, the user identity can be linked to the tag. To ensure security against PAE, it

is important that the entire tag interrogating process must be anonymous.

2) Attack Against Forward Secrecy: If an attacker somehow can manage the secrets of tags, then he/she will be able to trace all the previous communications of the tag. Therefore, a protocol which cannot handle this issue will be vulnerable to backward untraceability problem [4].

3) Desynchronization or DoS Attacks: An attacker can cause de-synchronization problem by blocking a message between tag and reader. Precisely, in many RFID-based authentication protocols, both the back end server and tag needs to update their secret security credentials to ensure forward secrecy. Hence, when the response message from the backend server is blocked then the tag cannot comprehend that whether the interrogation was successful or not. In this case, it is possible that the server updates its database, but tag does not. This will cause DoS attacks [5].

4) Impersonation Attacks: An attacker may try to impersonate as a legitimate tag user and send query to a reader and bypass the interrogation process. Similarly, the attacker can also try to impersonate as a legitimate reader. In this regard, one of the naive approach could be the attacker intercept the messages between tag and reader and reuses the message to impersonate as a legitimate tag or a legitimate reader.

5) Physical Attacks: The attacker compromises a tag and accesses the tag's memory to obtain secure information such as secret key through *cold boot attacks* [24]. This is a kind of side channel attack in which an attacker with physical access to tag is able to retrieve some useful informations stored in the tag. Then the attacker may try to trace all the previous communications of the tag user's. Most of the existing RFID authentication protocols are vulnerable to this attack.

6) Cloning Attack: Since most of the tags are not tamper-proof, an attacker can build a cloned tag which will be interpreted by the reader as a legitimate tag.

B. Related Work and Motivation

Over the past years, some interesting privacy preserving anonymous authentication schemes for RFID have been proposed, which can be divided into three categories: 1) public key crypto system (PKC), 2) error correction (EC), and 3) symmetric key or non-public key crypto system (NPKC) based schemes. Among PKC based schemes [6]–[11], most of them are designed on elliptic curve cryto systems, which is quite infeasible due to the expensive hardware cost. EC based schemes [12]–[16] can ensure security only when the error rate is less than a certain threshold value. Besides, these schemes are not scalable, since they can only support a limited number tags. The NPKC schemes can be divided into two categories i.e., hash based schemes [17]–[20] and PUF based schemes [21]–[26]. Hash based schemes can not guarantee security against any physical and cloning attacks. Because of that, PUF based schemes have gained more popularity in recent years. There are several works in the literature that utilized PUFs to ensure authentication for the RFID system. In 2008, Bringer *et al.* [21] proposed a tree-based authentication scheme using PUFs in. However, the protocol cannot ensure security against DoS and impersonation attacks [22]. Hereafter, Sadeghi *et al.* [22] proposed a new PUF-based scheme for RFID in, but Kardas *et al.* revealed that the scheme proposed in [22] is vulnerable to the cold boot attack [24]. An attacker after tampering a tag can easily impersonate it and even can trace its previous and future communications. Hereafter Akgun and Caglayan [23] proposed a tree based authentication protocol for RFID using PUFs. However, their protocol is also proven to be vulnerable cold boot attack presented in [24] and hence they cannot ensure the desired security properties. In 2012, Kardas *et al.* [25] proposed an RFID authentication protocol using PUFs, but the scheme cannot ensure forward secrecy and resilience of DoS attacks. Jung *et al.* proposed a HMAC-based RFID authentication scheme using PUF however, their scheme is also vulnerable to DoS attacks.

Recently, Akgun and Caglayan [26] proposed another PUF-based authentication scheme for RFID system. However, after thoroughly investigate we found that the scheme cannot ensure forward secrecy support, which is an imperative security requirement in RFID system. We also found that all the existing PUF-based RFID schemes can be impractical, where a reader needs to perform exhaustive search operation in order to identify a tag, which may impair the performance of the system. For instance, in [26], the proposed scheme encodes the identity of the tag T_i using a hash function. In that case, to identify the tag the backend server needs to try all possible combinations of the secrets a_i and b_i. The similar scenario can also be seen in other PUF-based authentication schemes. Furthermore, all the existing RFID schemes require to store secret keys on the tag memory. In that case, apart from the storage cost, once the tag is compromised, the attacker can obtain those secrets from the tag memory and perform several attacks.

All the aforesaid schemes [21]–[26] are designed based on the assumption of the noise-resilient or ideal PUFs [31]–[32]. Recently, a few interesting PUF-based authentication protocols [33]–[35] and [38] have been proposed for RFID systems, where noise has been taken into account. However, there are some shortcomings in theses schemes. For example, in [33], during authentication, the tag discloses its identity for assisting the verifier to find a previous PUF output z, so this scheme cannot ensure the privacy of the tag. To address this issue, two other PUF-based authentication schemes [34]–[35] have been proposed, however, in these schemes, the server needs to launch an exhaustive search to identify the device. Hence, these schemes are not scalable especially for the applications with a large scale of database. Moreover, after carefully investigate we found that the scheme presented in [35] cannot ensure the untraceability property. In this regard, when a communication failure/error occurs, the device will generate and interact using the same authentication field value c as used in the previous communication, and this could be used to identify the tag. Furthermore, Huth *et al.* [38] revealed that in the scheme of [35], an attacker can obtain the helper data for each round since the symmetric key sk stored in non-volatile memory, could be exposed, and addressed this issue by proposing an improved protocol. However, the proposed

TABLE I
SYMBOLS AND CRYPTOGRAPHIC FUNCTION

Symbol	Definition
TID_T^i	Temporary identity of the tag T for i-th round
$CRP(C_i, R_i)$	Challenge-Response pair for the i-th round
K_i	Session key for the i-th round
PUF_T	Secure physically uncloneable functions for tag T
$h(.)$	One-way hash function
$\oplus$	Exclusive-OR operation
$\|$	Concatenation operation

protocol in [38] requires to perform an additional channel-based key agreement (CBKA) phase. Generally, the performance of CBKA is greatly depending on the environment, so they cannot work well, i.e., provide low key rate, especially when the channel fading is not dynamic such as indoor. Besides, similar to [34]–[35], the protocol presented in [38] needs to launch an exhaustive search operation in order to verify the prover.

This paper seeks to address all these issues including the accomplishing of untracebility property in a realistic way. For that, we first propose a novel privacy preserving authentication protocol for RFID systems in ideal PUF environments, which can deal with several security issues including the physical attacks. Then, we present our enhanced protocol which can be used in the noisy PUF environments. Subsequently, we evaluate the security of the proposed schemes through the formal analysis. Finally, we demonstrate the performance of our proposed protocols by comparing to that of other existing PUF-based authentication protocols for RFID. The key contributions of this article can be summarized as follows:

- The proposed authentication protocols can ensure several key security properties including anonymity, availability, resilience of DoS attacks, and forward secrecy, which are all desirable in several critical IoT applications and services.
- The proposed protocols can also guarantee higher degree of practicality and efficiency. Specifically, in our proposed scheme, the backend server need not to perform any exhaustive search operation to identify the tag. Moreover, it does not require any secret key to be stored on the tag device.

The rest of the article is organized as follows. In Section II, we first present our novel lightweight privacy preserving authentication protocol for ideal PUFs. Then we introduce our enhanced protocol for noisy PUF environment. Security of the proposed protocols are analyzed in Section III. A relevant discussion based on the performance of the proposed protocol is presented in Section IV. The symbols and cryptographic functions used in this article are defined in Table I.

II. PROPOSED SCHEME

In this section, we describe our proposed privacy-preserving anonymous authentication protocols for RFID system. Before describing our protocols, we give brief overview of the adversary model and some underlying assumptions for the proposed scheme.

A. Adversary Model

We consider two categories of adversaries: Type 1 and Type 2. Type 1 adversary denotes the typical Dolev-Yao intruder [27], who can eavesdrop on the radio link between a tag and a reader. This type of adversary can alter messages and also be able to block some messages from a tag reader, or vice verse. Type 2 adversary is stronger than the Type 1, who has all the capabilities of Type 1 and additionally can perform any physical or cloning attacks. Besides, we assume that there are several readers in the system, and the adversary has the control over a subset of them (i.e., rouge readers).

B. Assumptions

We make the following assumptions regarding our proposed protocol for RFID system.

1) An RFID tag consists of a micro controller attached to a PUF, where the PUF output depends on its unique physical characteristics. Any attempt to tamper with the PUF changes the behavior of the tag and that will eventually renders the tag useless. Considering PUF as a challenge-response pair (*CRP*), where the response of R of a challenge C in PUF_T can be represented as $R = PUF_T(C)$.
2) We assume that there is a secure connection between the reader and the backend server, so the adversary cannot access that link.
3) RFID tags have limited resources while backend servers are considered as legitimate and have no such limitation.

C. Proposed Anonymous Authentication Protocol for Ideal PUFs

1) Setup Phase of the Proposed Protocol for Ideal PUFs: Every tags need to be registered into the backend server. For that, first the server needs to randomly generate a challenge C_i and a set of emergency challenges $C_{em} = \{c_1, c_2, \ldots, c_n\}$, and then sends $\{C_i, C_{em}\}$ to the tag T. Hereafter, the tag produces the responses $\{R_i, R_{em}\}$ by using its unique embedded function PUF_T, and subsequently sends $\{R_i, R_{em}\}$ to the server. After that, the server generates a unique temporary identity TID_T^i for the i-th round, and a set of unique un-linkable pseudo identities $PID = \{pid_1, pid_2, \ldots, pid_n\}$, and sends $\{TID_T^i, PID\}$ to the tag. Finally, the server stores $\{TID_T^i, PID, (C_i,R_i), (C_{em},R_{em})\}$ for each tag, but each tag only stores its current temporary identity TID_T^i and PID for future interactions. Details of this phase is depicted in Fig.1.

2) Authentication Phase of the Proposed Protocol for Ideal PUFs: This phase accomplishes mutual authentication among the RFID tag, the reader, and the backend server. Since each reader is connected to the server through a secure link hence we consider them (Reader-Server) as a single unit S. This phase of the proposed scheme consists of the following steps:

Step 1: $T \rightarrow S$: M_1 :$\{TID_T^i, \text{COUNT}\}$.

The tag randomly generates a nonce, COUNT and then selects its i-th round temporary identity TID_T^i and sends $\{TID_T^i, \text{COUNT}\}$ to the S.

Step 2: $S \rightarrow T$: M_2 :$\{C_i, R_i^*, Res_S\}$.

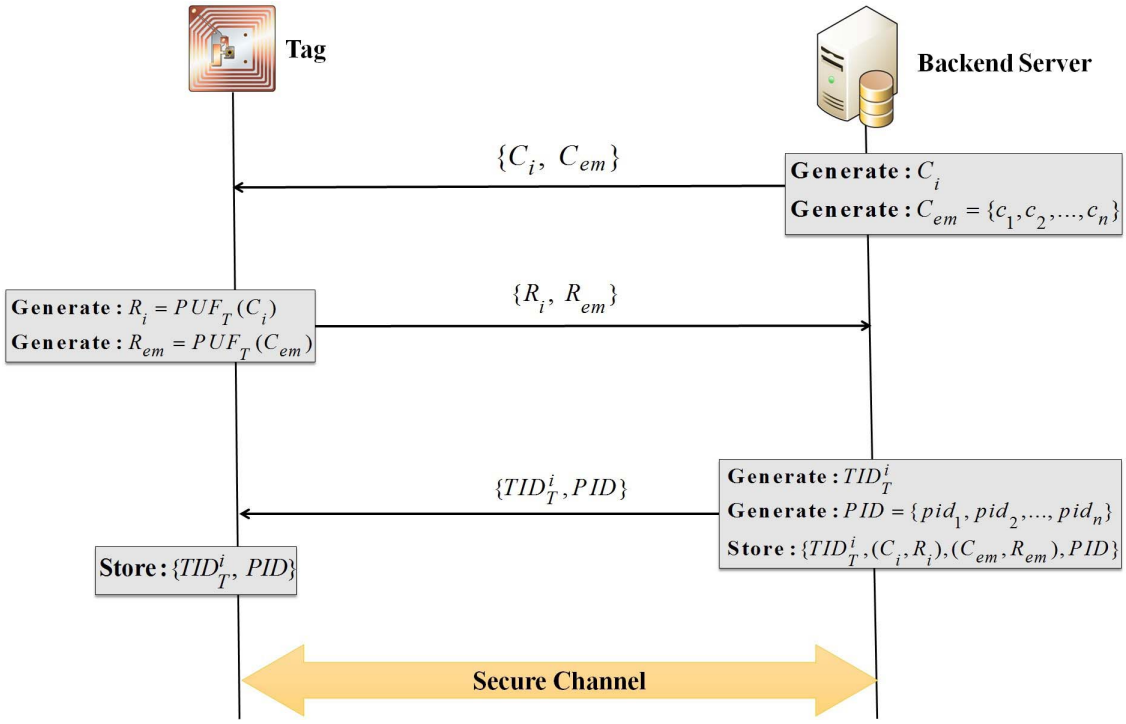

Fig. 1. Setup phase of the proposed authentication protocol for ideal PUFs.

After receiving the authentication request, S locates TID_T^i and reads (C_i, R_i) from its memory. Hereafter, S generates a random number N_S and computes $R_i^* = R_i \oplus N_S$, $Res_S = h(\text{COUNT} + 1||R_i||R_i^*)$. At last, S constitutes a response message $M_2 : \{C_i, R_i^*, Res_S\}$ and sends it to the tag T. If the search of TID_T^i is failed, the authentication requests will be rejected and then S needs to ask the tag to try again by using one of the un-used pseudo identities from $PID = \{pid_1, pid_2, \ldots, pid_n\}$. Once a pseudo identity is used up, it must be deleted from both the ends. In this case, during the authentication process, S will select one of the un-used emergency CRP from (C_{em}, R_{em}) and a new temporary identity TID_T^{new} will be provided to T for the next round in an encoded way. Finally, like the pseudo identity, S also needs to delete the used pair of emergency CRP from (C_{em}, R_{em}). In this way, we can resist DoS attacks [5] without compromising anonymity support.

Step 3: $T \rightarrow S$: $M_3 : \{R_{i+1}^*, Res_T\}$.

Upon receiving the response message from S, tag T uses its PUF to generate the response R_i using the challenge C_i and then validates the response parameter Res_S. If the validation is successful then T computes $N_S = R_i \oplus R_i^*$, $C_{i+1} = h(\text{COUNT} + 2||N_S||R_i)$, $R_{i+1} = PUF_T(C_{i+1})$, $K_i = h(R_i||N_S)$, $R_{i+1}^* = K_i \oplus R_{i+1}$, $Res_T = h(\text{COUNT}+2||K_i||R_{i+1}^*)$, $TID_T^{i+1} = h(TID_T^i||R_{i+1})$ and sends $M_3 : \{R_{i+1}^*, Res_T\}$ to S.

Step 4: $Verification\ at\ Reader - Server\ Unit\ S$.

After receiving the response from the tag, S first computes $K_i = h(R_i||N_S)$ and subsequently verifies the response parameter Res_T. If the verification is successful then S computes the following: $R_{i+1} = K_i \oplus R_{i+1}^*$, $C_{i+1} = h(\text{COUNT} + 2||N_S \| R_i)$, $TID_T^{i+1} = h(TID_T^i||R_{i+1})$. At last, S stores $\{TID_T^{i+1}, (C_{i+1}, R_{i+1})\}$ in its memory for the next round (i.e., $i+1$th) communication.

If there is any failure in the validation process of the aforementioned steps, then this phase of the proposed authentication scheme will be terminated. On the other hand, successful completion of this phase indicates that both T and S mutually authenticate each other. Besides, it should be noted that, to ensure higher degree of privacy in the proposed authentication protocol, the server needs to maintain the secrecy of the stored information. In that case, the server requires to encode the responses $\{R_i, R_{em}\}$ by using its master key MK, which is stored in secure ROM-BIOS of the server. Once the tag produces the a valid TID_T^i, then only the server decodes the encoded response parameter. The details of the MAKA phase are also depicted in Fig. 2.

D. Proposed Enhanced Anonymous Authentication Protocol for Nosiy PUFs

Although differential design methodologies improve reliability, the noise in the PUF could still be an issue. Therefore, in this subsection, we present our enhanced protocol that can support the noisy PUF environments. In this regard, we utilize the concept of fuzzy extractor FE $(d,\ y)$ which composes with two algorithms: key generation algorithm FE.Gen and reconstruction algorithm FE.Rec. The FE.Gen algorithm takes R_i as input and outputs a key K_i and helper data hd_i. Then, the FE.Rec recovers the key K_i from the input variable R_i' and the helper data hd_i, if the hamming distance between the R_i' and R_i is at most d. FE ensures security if the min-entropy of the input R_i is at the minimum y, K_i is close to a uniformly random in $\{0, 1\}^k$. Since repeated exposure of the helper data may result in additional min-entropy loss [36].

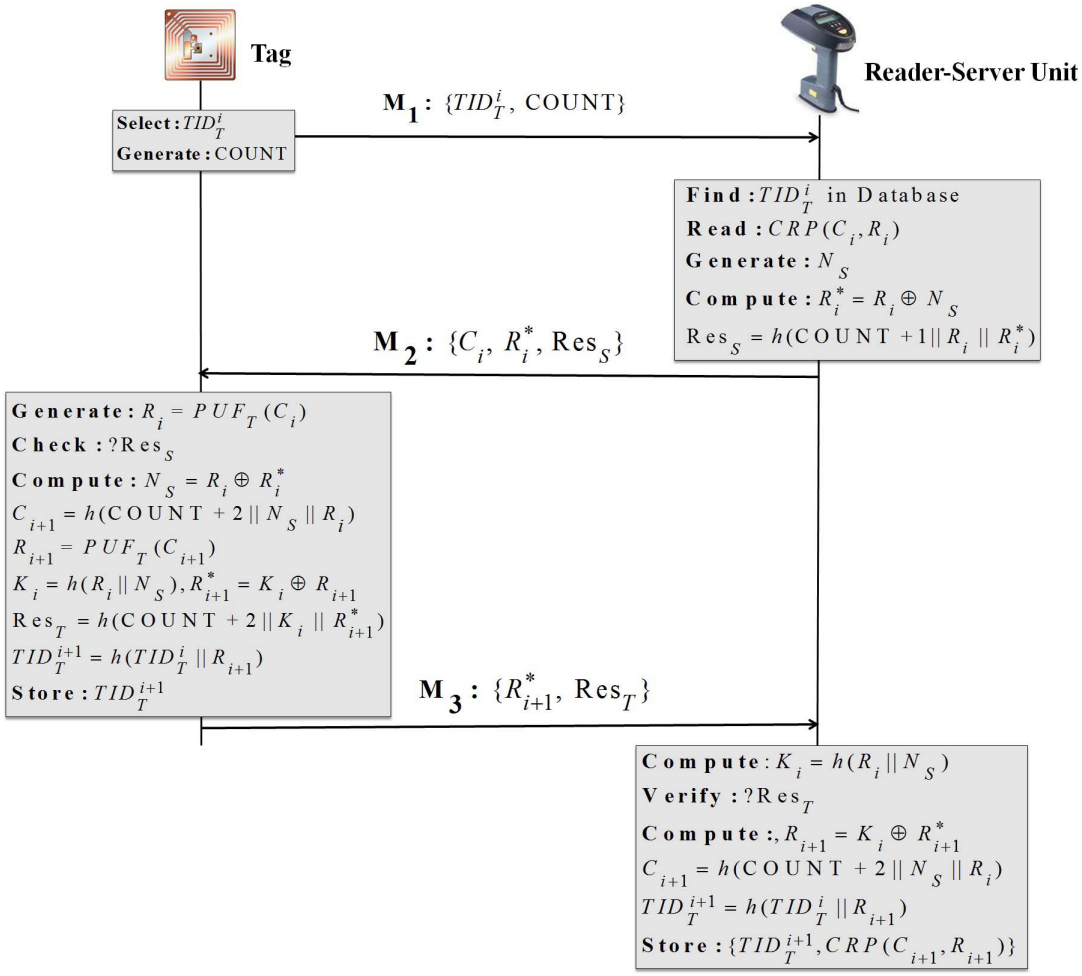

Fig. 2. The proposed lightweight and practical anonymous authentication protocol for ideal PUF-based RFID system.

Therefore, during execution of the authentication protocol, the helper data should not be exposed.

1) Setup Phase of the Enhanced Protocol: The server randomly generates a challenge C_i and a set of emergency challenges $C_{em} = \{c_1, c_2, \ldots, c_n\}$ and sends $\{C_i, C_{em}\}$ to the tag T. After that, tag produces $\{R_i, R_{em}\}$ by using its unique embedded function PUF_T and then sends $\{R_i, R_{em}\}$ to the server. Hereafter, the server generates a unique temporary identity TID_T^i for the i-th round. Then the server also generates a set of unique un-linkable pseudo identity $PID = \{pid_1, pid_2, \ldots, pid_n\}$, and calculates $(K_i, hd_i) = \text{FE.Gen}(R_i)$, $(K_{em}, hd_{em}) = \text{FE.Gen}(R_{em})$, and sends $\{TID_T^i, PID, (C_i, hd_i), (C_{em}, hd_{em})\}$ to the tag. Finally, the server stores $\{TID_T^i, PID, (C_i, K_i), (C_{em}, K_{em})\}$ for each tag for future interactions. Details of this phase is depicted in Fig. 3.

2) Authentication Phase of the Enhanced Protocol: Similar to our proposed ideal PUF-based scheme, we consider as single unit S. This phase of the enhanced protocol consists of the following steps:

Step 1: The tag randomly generates a nonce COUNT and selects its i-th round temporary key TID_T^i and sends $\{TID_T^i, \text{COUNT}\}$ to the S.

Step 2: Upon receiving the authentication request, S searches for TID_T^i and reads (C_i, K_i) for the tag from its memory. After that, S generates a nonce N_S and calculates $N_S^* = K_i \oplus N_S$, $Res_S = h(\text{COUNT} + 1||K_i||N_S^*)$. Finally, S composes a response message M_{E_2}: $\{C_i, N_S^*, Res_S\}$ and sends it to the tag T.

Step 3: After receiving the response message from S, tag T first searches its memory for C_i and picks the helper data hd_i. After that, T uses its PUF to generate R_i' by using the challenge C_i, and then calculates $K_i = \text{FE.Rec}(R_i', hd_i)$ and validates the response parameter Res_S. If the validation is successful, T calculates $N_S = K_i \oplus N_S^*$, $C_{i+1} = h(\text{COUNT} + 2||N_S||K_i)$, $R_{i+1}' = PUF_T(C_{i+1})$, $R_{i+1}^* = K_i \oplus R_{i+1}'$, $Res_T = h(N_s||K_i||R_{i+1}^*)$, and sends M_{E_3}: $\{R_{i+1}^*, Res_T\}$ to S.

Step 4: Upon receiving the response from the tag, S first validates the parameter Res_T. If the validation is successful then S computes $R_{i+1}' = K_i \oplus R_{i+1}^*$, $(K_{i+1}, hd_{i+1}) = \text{FE.Gen}(R_{i+1}')$, $C_{i+1} = h(\text{COUNT}+2||N_S||K_i)$, $hd_{i+1}^* = h(\text{COUNT}+3||K_i) \oplus hd_{i+1}$, $V_s = h(hd_{i+1}^*||K_i)$, $TID_T^{i+1} = h(TID_T^i||K_i)$ and sends $\{hd_{i+1}^*, V_s\}$ to the tag T. Finally, S stores $\{TID_T^{i+1}, (C_{i+1}, K_{i+1})\}$ for the next round communication.

After receiving $\{hd_{i+1}^*, V_s\}$ from S, the tag T first checks the parameter V_s. If the verification is successful, T calculates

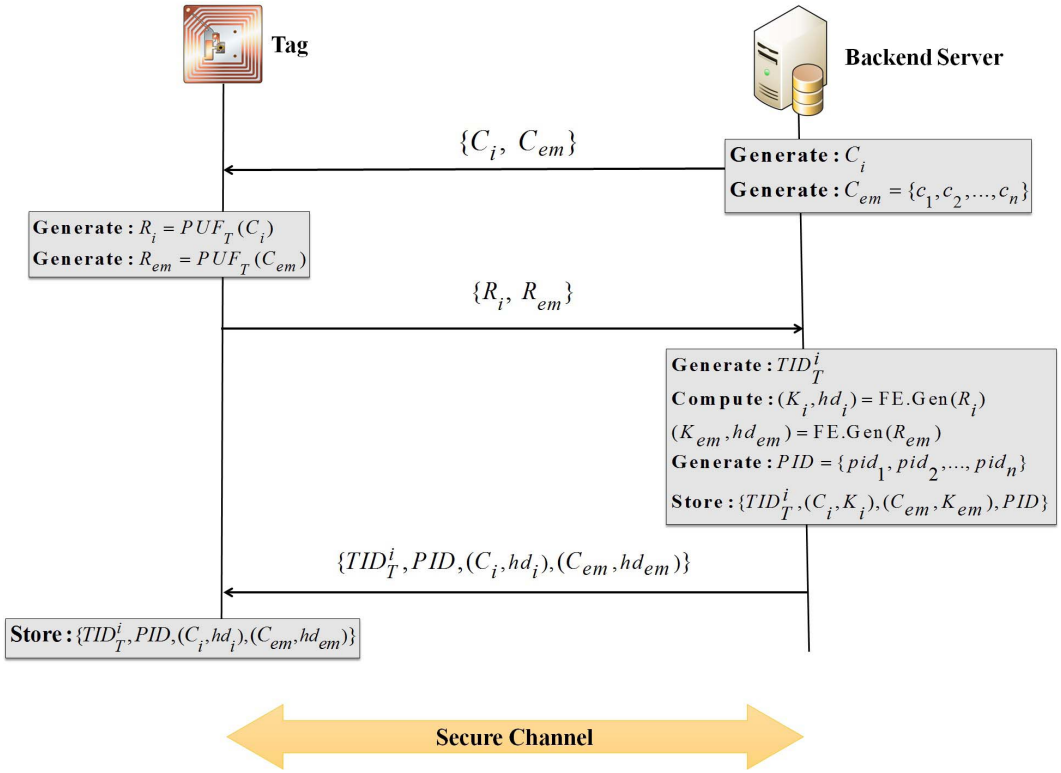

Fig. 3. Setup phase of the enhanced anonymous authentication protocol for noisy-PUF-based RFID system.

$hd_{i+1} = h(\text{COUNT}+3||K_i) \oplus hd_{i+1}^*$, $TID_T^{i+1} = h(TID_T^i||K_i)$ and stores $\{TID_T^{i+1}, (C_{i+1}, hd_{i+1})\}$ for the next round interaction with S. If there is any failure in the verification process of the above steps, this phase of the enhanced scheme will be terminated. In the case of loss of synchronization or DoS attacks, that can be comprehended if the response message M_{E_2} or M_{E_4} has been interrupted, so that the tag cannot receive the message within a specific time period. In that case, the tag T needs to use one of the un-used pseudo identities $pid \in PID$, and similarly S will select an unused pair of $(c_j, k_j) \in (C_{em}, K_{em})$ and uses (c_j, k_j) in composing the response message M_{E_2}. At the end of the authentication process, the tag T will delete (c_j, hd_j) from its memory and S will delete (c_j, k_j) from its database. The details of this phase of our enhanced scheme is depicted in Fig. 4.

It should note that to provide desired security level in the PUF-based authentication scheme, it is imperative that the PUF response should be stable and uniform. When PUF response is unstable and biased, helper data may leak information about seed (entropy loss). In addition, it will be difficult to extract entropy from unstable response. One of the conventional methods for extracting stable and uniform response from unstable and biased PUFs is debiasing. Debiased response can ensure full-entropy and it is applied to PUF response prior to FE. Recently, Aysu *et al.* [39] and Suzuki *et al.* [40] independently introduced two debiasing methods for lightweight PUFs while Wang *et al.* [41] proposed a new PUF design called locally enhanced defectivity physically unclonable function (LEDPUF), which can ensure higher degree of stability in the PUF design. Unlike the conventional parametric PUFs, LEDPUF does not require any kinds of correction schemes.

Now, similar to [34]–[35] and [38], in our proposed scheme, we assume that the PUF response to be stable and uniform. However, to strengthen our scheme to work even in the environment where PUF responses may not be stable and uniform, we can adopt the idea of [39]–[40] or [41]. For instance, in designing the ideal PUF-based anonymous authentication scheme (presented in Section II-C), we can consider LEDPUF [41]. On the other hand, for secure key generation in the construction of the noisy PUF-based anonymous authentication scheme (presented in Section II-D), we can use the debiasing methods ([39] or [40]) to PUF response prior to FE (as shown in Fig. 5).

III. Formal Security Analysis

In this section, we formally analyze our ideal PUFs-based lightweight anonymous authentication scheme on the major security requirements. Similarly, we can also analyze the formal security of the enhanced protocol.

A. Adversarial Model

We consider an adversary $\mathcal{A}$ who has the control over the radio communication channel between a tag T and the (Reader-Server) unit S. $\mathcal{A}$ needs to model the following set of queries in polynomial time.

- `Send`(S, `m1`, `x1`, `m2`) : This query models the adversary's ability to act like a legitimate tag. In this regard, $\mathcal{A}$ sends `m1` and receives `x1` from S and then replies `m2` to S.

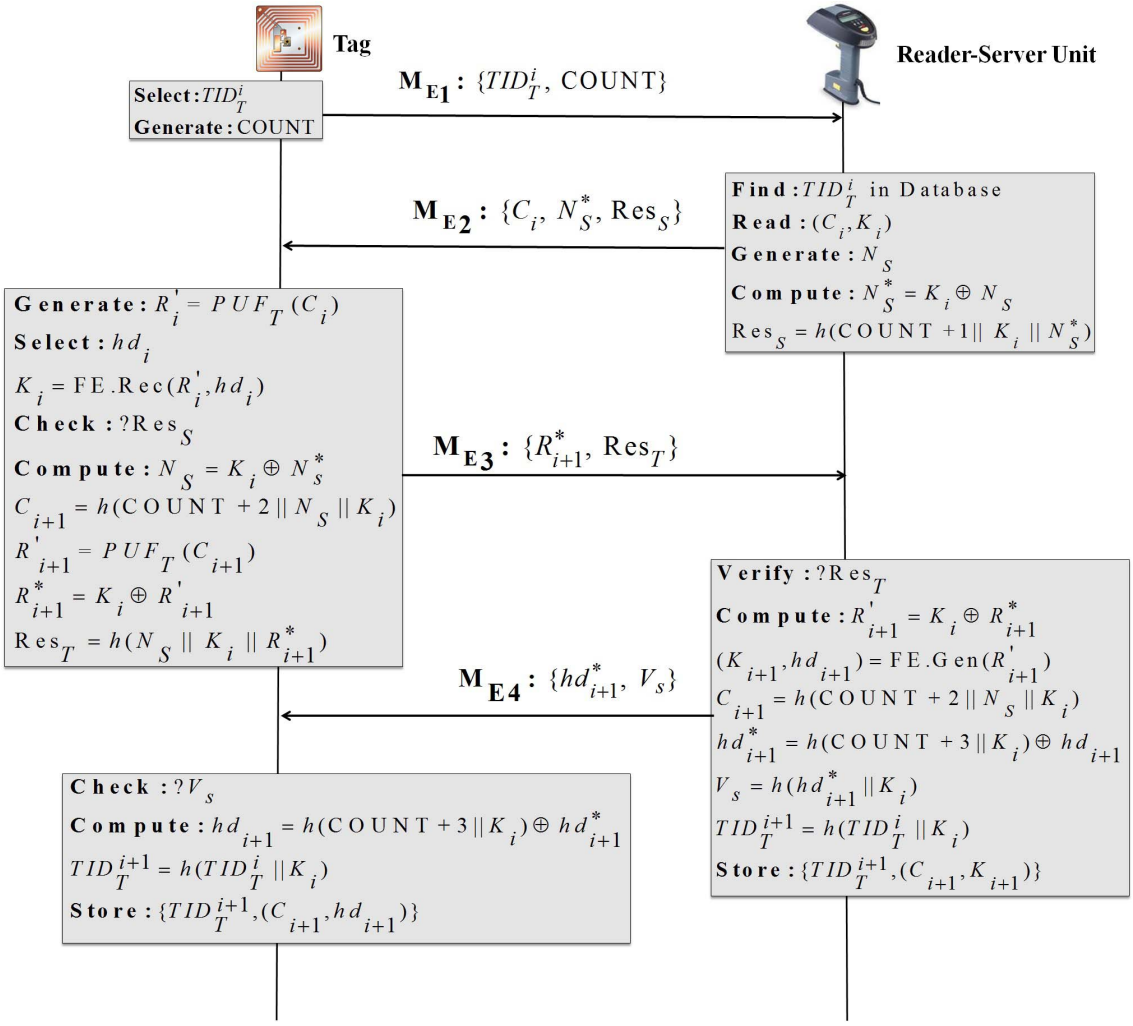

Fig. 4. Enhanced lightweight and practical anonymous authentication protocol for noisy-PUF-based RFID system.

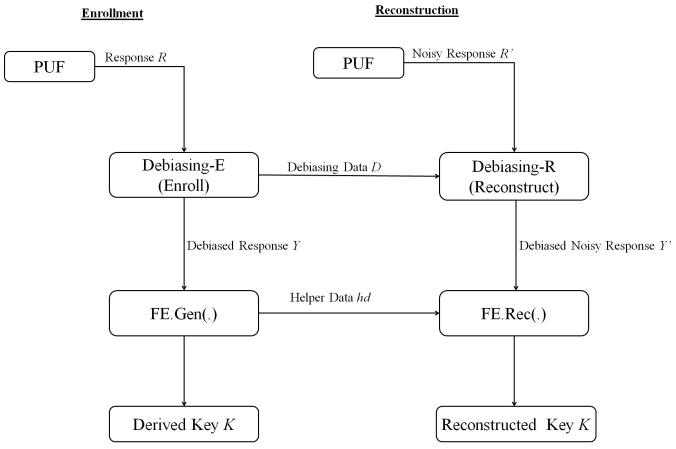

Fig. 5. Debiasing PUF-based key generator.

- `Query`(T, `x2`, `m2`) : This query models the adversary's ability to investigate a tag. For that, $\mathcal{A}$ sends `x2` to T and receives `m2` from T.
- `Execute`(T, S) : This query models the adversary's ability to continuously observe the radio channel between T and S. In this context, $\mathcal{A}$ needs to intercept on the channel during the execution of an instance of the protocol between T and S.
- `Block`($\mathcal{A}$): This query models the adversary's ability to launch DoS attack. In this regard, $\mathcal{A}$ is allowed to block a part of the protocol and break the synchronization between T and S.
- `Reveal`(T): Modeling this query $\mathcal{A}$ obtains the contents of the tag's memory. In other words, this query models adversary's ability to corrupt a tag and obtains the secrets stored in its memory.

It should be noted that $\mathcal{A}$ can call `Send`, `Query`, `Execute`, and `Block` queries any polynomial number of times but can call `Reveal` query only once. Furthermore, based on the definitions of adversaries as discussed in Section II.A and the above formal adversarial model, a Type 1 adversary can call all the oracle queries except `Reveal` oracle. On the other hand, a Type 2 adversary has the ability to invoke all the oracle queries including the `Reveal` oracle.

B. Assumptions

1) Uncloneability Assumption: We make standard assumption, where it is impossible to predict the behavior of PUF without having the physical device. Consider a PUF, which can

be defined as *PUF:* $\{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$ that on input of length l_1 produces a random string of the length l_2. Security of this function can be determined through the following *challenge-response game,* which consists of two phases*:*

Phase 1: An adversary $\mathcal{A}$ randomly chooses a challenge C_i and obtains the PUF response R_i.

Challenge: Now $\mathcal{A}$ selects a challenge C_x that has not been queried before.

Phase 2: $\mathcal{A}$ can query the PUF for challenges other than C_x.

Response: Finally, $\mathcal{A}$ outputs its guess for R'_x for PUF's response to $R_x = PUF(C_x)$.

$\mathcal{A}$ wins the game if $R'_x = R_x$, which can be denoted as $Adv^{puf}_{\mathcal{A}}(l_2) = \Pr\left[R_x = R'_x\right]$.

2) Pseudo Random Function Assumption: A pseudorandom function PRF:$\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^{k'}$ which takes a secret security parameter $K\epsilon\{0,1\}^k$ and a message $M\epsilon\{0,1\}^*$ as input and provides an arbitrary string PRF(K, M) which is indistinguishable from random string. Now, assuming that h be a polynomial-time computable pseudorandom function. For distinguishing h, a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ may request polynomial bounded queries with its selected inputs and obtain the outputs computed by h for training. After the training phase, $\mathcal{A}$ is given a function, which is either h or a truly random function. We say that h is a pseudo-random function, if it is indistinguishable from a truly random function under $\mathcal{A}$. Namely, $\mathcal{A}$ is given either h or a truly random function according to a random bit $\{0, 1\}$ and it has only the probability $\frac{1}{2} + \varepsilon$, to distinguish h.

C. Security Analysis

Lemma 1: In the proposed ideal PUFs-based lightweight anonymous authentication protocol the secret data of a tag cannot be revealed any secret even calling the `Reveal` oracle.

Proof: A legitimate tag needs to request with the updated temporary identity TID^i_T, and responds to a reader's query with the valid response parameter $Res_T = h(\text{COUNT}+2||K_i||R^*_{i+1})$, $R^*_{i+1} = K_i \oplus R_{i+1}$. In these messages, the session key K_i is used as a key security parameter, which is generated based on the secret response parameter R_i. Without knowing R_i, the adversary $\mathcal{A}$ cannot generate K_i. Now, in our proposed scheme, tag need not to store any secret security credential, therefore, if the adversary calls a `Reveal` oracle to obtain secret from the tag memory, then she may only manage to obtain TID^i_T. With that she cannot pass the reader's interrogation process. Most importantly, since any authorized attempt to access the PUF will change its *CRP* behavior, then that will eventually renders the tag useless. ■

Lemma 2: In the proposed scheme the temporary identities of the tag cannot be correlated without calling the `Reveal` oracle.

Proof: Since each temporary identity TID^{i+1}_T (valid only for the i+1-th round) is generated from the random response R_{i+1} and one-way hash function h i.e., $TID^{i+1}_T = h(TID^i_T||R_{i+1})$. Hence, it will be difficult for an adversary to correlate TID^i_T with the temporary identity for the next round TID^{i+1}_T as well as with the original one, unless $\mathcal{A}$ calls the `Reveal` oracle. ■

Theorem 1 (Untraceability): In the proposed authentication protocol, tags are universally untraceable.

Proof: In RFID system, a tag is universally untraceable [4], if an adversary $\mathcal{A}$ cannot correlate two of its successful authentication requests and responses with a valid reader-server unit S. This can be modeled by the following game between a challenger $\mathcal{C}$ as a RFID system and the adversary $\mathcal{A}$. It is assumed that the power of both $\mathcal{C}$ and $\mathcal{A}$ is not more than polynomial-time algorithm:

1) $\mathcal{C}$ selects a valid reader-server unit S and two tags T_1 and T_2.
2) $\mathcal{A}$ calls the following oracles: `Send`, `Query`, `Execute`, and `Block` on S and T_1 and T_2 for a polynomial number of times.
3) After finishing calling the oracles $\mathcal{A}$ notifies $\mathcal{C}$.
4) $\mathcal{C}$ randomly chooses one of the tags T.
5) $\mathcal{A}$ calls the following oracles: `Send`, `Query`, `Execute`, and `Block` on S and T.
6) $\mathcal{A}$ predicts her guess T' and wins the game if $T' = T$.

In this case, the advantages of successfully guessing is defined as $Adv_{\mathcal{A}} = 2 \times \left(\Pr\left[T' = T\right] - \frac{1}{2}\right)$. Tags are claimed to be untraceable if the the adversary $\mathcal{A}$ does not have any advantages on the random guess and for that $\Pr(T' = T) = \frac{1}{2}$ and hence $Adv_{\mathcal{A}}$ is zero.

Now, we follow the above game to ensure universal untraceability of the tags in the proposed authentication protocol. In this context, we assume $\mathcal{C}$ successfully carries out the authentication process between each tags, T_1 and T_2, and the reader-server unit S. Then, $\mathcal{C}$ randomly chooses one of the tags T and gives it to $\mathcal{A}$. $\mathcal{A}$ predicts her guess T'after calling the following oracles `Send`, `Query`, `Execute`, and `Block`. Since, $\mathcal{A}$ cannot infer the secret response of the i-th round i.e., R_i so that she cannot produce the correct temporary identity TID^{i+1}_T for the i+1th round (by Lemma1). Accordingly, she cannot correlate the temporary identities to each other (by Lemma 2). Therefore, $\mathcal{A}$ has only one choice i.e., a random guess $\left(\Pr\left[T' = T\right] - \frac{1}{2}\right)$ and based on the above equation of $Adv_{\mathcal{A}}$ the advantage of the adversary is zero. So, our proposed lightweight anonymous authentication protocol can ensure universal untracebility. ■

Theorem 2: The proposed ideal PUFs-based lightweight anonymous authentication protocol can ensure forward secrecy with backward untraceability support.

Proof: To ensure forward secrecy with backward untraceability support we model a game which is similar to the universally untraceable one, except that in the last phase the adversary needs to invoke the `Reveal` oracle on the tag. $\mathcal{C}$ selects a valid reader-server unit S and two tags T_1 and T_2 and provides them to $\mathcal{A}$. Now, $\mathcal{A}$ calls the following oracles: `Send`, `Query`, `Execute`, and `Block` on S and T_1 and T_2 for a polynomial number of times. Hereafter, $\mathcal{C}$ successfully carries out the authentication process between each tags, T_1 and T_2, and the reader-server unit S. Then $\mathcal{C}$ randomly chooses one of the tags T and gives it to $\mathcal{A}$. Then $\mathcal{A}$ invokes the `Reveal` oracle on the tag T obtains all the current data from the tag memory i.e., the current temporary identity. Finally, $\mathcal{A}$ outputs her guess T'. Since, the current temporary identity is generated from the hash of the previous one, so $\mathcal{A}$ cannot

inverse the hash function. Besides, each *CRP* is randomly generated, hence they are expected to be independent to each other. Furthermore, it should be noted that in our proposed scheme we do not store any secrets such as key in the tag memory. To sum up, since all the secrets used in the proposed protocol is one-time hence, if the adversary can manage the current temporary identity and *CRP*, however $\mathcal{A}$ still cannot trace the tag owner by using the compromised information. The adversary will not have any advantage over random guess. Hence, the proposed scheme can ensure forward secrecy with backward untraceability support. ■

Theorem 3: The proposed protocol accomplishes mutual authentication.

Proof: The adversary $\mathcal{A}$ may try to authenticate herself as a legitimate tag, which can be modeled by the following game between the $\mathcal{A}$ and the challenger $\mathcal{C}$.

1) $\mathcal{C}$ selects a valid reader-server unit S and a tag T.
2) $\mathcal{A}$ calls the following oracles: `Send`, `Query`, `Execute`, and `Block` on S and T for a polynomial number of times.
3) After finishing calling oracles $\mathcal{A}$ notifies $\mathcal{C}$.
4) $\mathcal{A}$ invokes the `Send` oracle to impersonate a tag.
5) If $\mathcal{A}$ can authenticate herself as a legitimate tag then $\mathcal{A}$ wins the game.

Now, to prove her legitimacy $\mathcal{A}$ must responds to the interrogation of the reader-server unit S. For that, $\mathcal{A}$ needs to send a valid temporary identity TID_T^i and also needs to generate a valid response message $Res_T = h(\text{COUNT} + 2||K_i||\ R_{i+1}^*)$. In that case, $\mathcal{A}$ must know the secret response of the i-th round i.e., R_i. However, by Lemma 1, $\mathcal{A}$ cannot expose the secret response R_i and that implies she cannot impersonate as a legitimate tag. On the other hand, to be authenticated as a reader-server unit, $\mathcal{A}$ needs to invoke a `Query` oracle in (4) and also needs to sends a valid *CRP* with the legitimate response message $Res_S = h(\text{COUNT} + 1||R_i||\ R_i^*)$. Since $\mathcal{A}$ cannot infer R_i, hence cannot produce the valid Res_S. Accordingly, $\mathcal{A}$ cannot impersonate as a legitimate reader. In our proposed scheme only a legitimate tag and reader-server unit can mutually authenticate each other with the support of valid *CRP*. ■

Lemma 3: The proposed scheme can ensure the resilience of DoS attacks.

Proof: In our proposed protocol, to deal with DoS attack we utilize the concept of set of unlinkable pseudo identities *PID* and emergency $CRP(C_{em},R_{em})$. Now, we assume that the adversary $\mathcal{A}$ invokes the `Block` oracle and due to that backend server cannot receive the response message M_3 :$\{R_{i+1}^*,Res_T\}$and hence cannot obtain the *CRP* for the next round i.e., (C_{i+1},R_{i+1}). To deal with this issue, the tag needs to use one of the pseudo identity from $PID = \{pid_1, pid_2, \ldots, pid_n\}$. Once the server receives pid_i instead of TID_T^i then it selects one of the un-used emergency *CRP* from (C_{em},R_{em}) and continue the authentication process with that. In this way, we ensure security against DoS to desynchronization attacks. ■

Lemma 4: The proposed RFID authentication scheme can ensure security against any physical and cloning attack.

Proof: Since an attacker can get access secrets stored in the RFID device through `Reveal` oracle. Hence, it is desirable that tags should not store any secret within its memory. However, most of the existing RFID authentication protocols rely on one or more secrets (in the form of keys) to be stored in the tag's memory. Hence, this approach can lead to leakage of key. In our proposed scheme, we do not store any keys in the tag memory. Besides, the PUF and micro-controller of the tag are considered as inseparable. Accordingly, we can argue that even if an adversary has the access of RFID tag, but she cannot compromise the security of the proposed protocol. Furthermore, since PUFs are safe against cloning and a PUF cannot be recreated [3]. In our proposed scheme we require each tag device to be equipped with PUF. Hence, the proposed RFID authentication protocol can be regarded safe against cloning attacks. ■

IV. Performance Analysis and Comparison

In general, RFID tags have limited resources, so it is important that apart from security, any designed protocol for RFID system should consider the efficiency in terms of memory footprint, and storage, computation and communication overhead. In this section, we first compare the performance of the proposed ideal PUF-based anonymous authentication protocol with some of the recently proposed RFID authentication protocols such as [22], [23], [25], and [26] for the same environment. Subsequently, we compare our enhanced anonymous authentication protocol with a recently proposed RFID authentication protocol [35] for the noisy PUF environment.

Now, we compare the performance of the proposed ideal PUF-based scheme based on some important security properties for RFID system as shown in Table II. From Table II, we can see that our proposed ideal PUF-based scheme can satisfy all the important required security requirements of the RFID system, while other proposed protocols for the same environment cannot guarantee several security requirements. For instance, none of the ideal PUF-based existing schemes can ensure forward secrecy (i.e., SP4) with the resistance of DoS attacks. Besides, even though these schemes are based on PUF, they are still vulnerable to physical attacks since a tag needs to store all required security credentials (i.e., secret key). Therefore, by intelligent side-channel attacks [28], the attacker can easily access those secret credentials stored in the RFID device. Then, the attacker can easily trace back all the previous communications of the tag as the existing schemes cannot ensure forward secrecy. Furthermore, in the existing schemes, the backend server needs to do exhaustive search to identify the tag, which makes those schemes not scalable.

We also compare the performance of the proposed ideal PUF-based scheme in terms of the computation cost as shown in Table III. Table III shows the numbers of operations including hash (denoted by h), random number generator (denoted by RNG), and PUF (denoted by P), those operations are required by our proposed scheme and existing ideal PUF-based schemes for RFID system. From Table III, we can clearly see that the computation overhead of the proposed ideal PUF-based scheme is similar to that of the existing schemes for the

TABLE II

PERFORMANCE COMPARISON BASED ON THE REQUIRED SECURITY PROPERTIES (SP)

	Schemes	SP1	SP2	SP3	SP4	SP5	SP6	SP7	SP8
Ideal PUF Case	**Sadeghi et al. [22]**	No	Yes	No	No	NA	Yes	No	Yes
	Akgun et al. [23]	Yes	No	No	No	No	Yes	No	Yes
	Kardas et al. [25]	Yes	Yes	No	No	No	Yes	No	Yes
	Akgun et al. [26]	Yes	Yes	No	No	NA	Yes	No	Yes
	Proposed Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Noisy PUF Case	**Aysu et al. [35]**	Yes	No	No	Yes	Yes	Yes	Yes	Yes
	Huth et al. [38]	Yes	Yes	No	Yes	Yes	Yes	Yes	No
	Proposed Scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

SP1: Mutual Authentication; **SP2:** Untraceability; **SP3:** Scalability; **SP4:** Forward Secrecy; **SP5:** Resilience of DoS Attacks; **SP6:** Uncloneability; **SP7:** Security Against Physical Attacks; **SP8:** Without Additional Key-agreement Support;

TABLE III

PERFORMANCE COMPARISON BASED ON THE COMPUTATIONAL COST

	Schemes	Tag	Reader-Server Unit
Ideal PUF Case	**Sadeghi et al. [22]**	$4h + 2P + RNG$	$5h + RNG$
	Akgun et al. [23]	$4h + P + RNG$	$4h + RNG$
	Kardas et al. [25]	$5h + 2P + RNG$	$4h + RNG$
	Akgun et al. [26]	$4h + 2P + RNG$	$4h + RNG$
	Proposed Scheme	$4h + 2P + RNG$	$4h + RNG$
Noisy PUF Case	**Aysu et al. [35]**	$3h + 2P + RNG + FE.Gen + SKE$	$3h + RNG + FE.Rec + SKD$
	Huth et al. [38]	CBKA (CM+Q+IR+PA) + $3h + 2P + RNG + FE.Gen + SKE$	CBKA (CM+Q+IR+PA)+$3h + RNG + FE.Rec + SKD$
	Proposed Scheme	$5h + 2P + RNG + FE.Rec$	$5h + RNG + FE.Gen$

h : Hash Operations; P : PUF Operations; RNG : Random number generator;
SKE/D : Symmetric Key Encryptions/Decryption; $FE.Gen/Rec$: Fuzzy Extractor Generation/Reconstruction;
CM : Channel Mesurement; Q : Quantization; IR : Information Reconcilation; PA : Privacy Amplification;

TABLE IV

PERFORMANCE COMPARISON BASED ON THE OTHER COST

	Schemes	Tag Memory Footprint	Tag Storage Overhead	Communication Cost
Ideal PUF Case	**Sadeghi et al. [22]**	768-bit	640-bit	1280-bit
	Akgun et al. [23]	768-bit	384-bit	1280-bit
	Kardas et al. [25]	640-bit	768-bit	1408-bit
	Akgun et al. [26]	640-bit	512-bit	896-bit
	Proposed Scheme	576-bit	128 + $n\times$64-bit	832-bit
Noisy PUF Case	**Aysu et al. [35]**	1392-bit	192-bit	2476-bit
	Huth et al. [38]	1392-bit	1804-bit	4140-bit
	Proposed Scheme	1264-bit	1456 + $n\times$1392-bit	2154-bit

same environment even it provides better security as shown earlier in Table II.

In Table IV, we now compare the efficiency of our proposed ideal PUF-based scheme to the existing schemes in terms of tag memory footprint size, tag storage overhead, and communication cost. Here, the tag memory footprint size denotes the amount of the memory required during the execution of an authentication protocol. Table IV shows that the tag memory footprint size for the proposed ideal PUF-based scheme is 576-bit, which is reasonably less than other existing schemes for the same environment. Besides, the proposed protocol is more efficient than other schemes in terms of storage requirements. For the normal execution of our proposed protocol, a tag needs to store its current temporary identity only (not previous ones), and this causes 128-bit of storage cost, which is significantly less than those of other schemes. Furthermore, from Table IV, we can also notice that the communication cost of the proposed noise-resilient PUF-based protocol is also less than those of other schemes for the same environment.

Note that to handle DoS attacks in our proposed ideal PUF-based protocol, we need to store a few number (i.e., n) of un-linkable pseudo identities of 64-bits. In this regard, the tag can use at most t number of pseudo identities where $t \leq n - 1$. After that, the tag needs to request the server for re-loading pseudo identities. For that in the request message M_1, tag needs to include its $t + 1$th pseudo identity, nonce (COUNT), and "Re-Loading". After authenticating the tag, the system generates a set of new ($t + 1$) un-linkable pseudo identities, encrypts them using the session key K_i, and sends it to the tag. An attackers may continuously interrupt the interrogations to destroy the unlinkability. This kind of attack can be prevented with sufficient pseudo identities, but there will be more cost in terms of storage and maintaining the identities. Here, we assume the tag has relatively enough pseudo identities to limit the failure for reloading new set of un-linkable pseudo identities and temporary identity. When all the pseudo identities are used up and the tag fails to reload pseudo identities, the tag will execute the setup phase of the

proposed scheme and reload itself with the new set of unlinkable pseudo identities and temporary identity.

Furthermore, we also consider the *"Usability Problem"*, where an attacker has a temporary access (say, for a few minutes) of the device, and then he/she may try to deplete all pseudo identities before the owner comes back. Here the device owner can maintain a hash of a secret code in the device and the secret code needs to be remembered by the owner. Now, while the attacker or the device owner wants to utilize the $(t + 1)$-th pseudo identity, he/she needs to input the secret code. The device will check the validity with the hash of the secret code stored in its memory. Whenever the device owner wants to change his/her secret code, he/she must submit the old secret code first, so that the device can validate the old secret code. If the validation is successful, the device owner will be allowed to update his/her secret code with the new one.

Next, we compare our proposed protocol with existing protocols in [35] and [38] for the noisy PUF environment. From Table II, we can see that our enhanced scheme for noisy PUF environment can ensure all the security properties, whereas the protocol presented in [35] cannot support untraceability and scalability properties (discussed in Section IB). On the other hand, in [38], the protocol needs to perform the CBKA phase prior execution of the authentication phase, which will cause additional overhead. In addition, the similar to [35], the protocol cannot support scalability property as for identifying a tag, the server needs to perform exhaustive search operation.

We have also compared our proposed protocol with the schemes in [35] and [38] in terms of costs for computation, communication, storage, and tag memory footprint. First, Table III shows the comparison result based on the computational cost, and we can see that the protocol presented in [35] requires an additional cryptographic primitive i.e., symmetric key encryption/decryption. On the other hand, the protocol presented in [38] needs to bear the additional overhead of the CBKA phase. In Table IV, we compare our enhanced scheme with [35] and [38] in terms of the communication cost, storage cost and tag memory footprint, as compared to our enhanced scheme. Here, we consider the length of each variable as similar as mentioned in [35, Table I]. From the bottom part of Table IV, we can see that our enhanced scheme requires less communication cost and tag memory footprint than the protocol in [35] and [38]. The protocol presented in [38] requires additional 208-bytes of communication cost. Next, we consider the storage overhead of the proposed scheme. Here, we consider the sizes of the temporary identity as 128-bit, pseudo identity as 64-bit, helper data as 1264-bit (as mentioned in [35, Table I]), and he challenge variable C_i as 64-bit (as mentioned in [35, Table I]). Therefore, in the case of normal execution, the storage overhead of our noisy PUF-based scheme is $TID_T^i + hd_i + C_i = 1456$-bit. On the other hand, for handling DoS attacks and in case of n synchronous executions, the storage overheard of our noisy PUF-based scheme is $n \times PID + hd_{em} + C_i = n \times 1392$-bit. From Table IV, we can see that, our proposed scheme needs larger tag storage than that of the protocol in [35]. Hence, the enhanced scheme can be suitable for the RFID tags with large storage capacity based [37] such as IQC 37, IQC 42, IQC 43, etc.

```
% OFMC %
Version of 2006/02/13
SUMMARY SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/avispa/web-interface-computation/
./tempdir/workfilegyKvlF.if.
GOAL
as_specified
BACKEND OFMC
COMMENTS STATISTICS
parseTime: 0.00s searchTime: 0.10s visited
Nodes: 208 nodes depth: 11 plies
```

Fig. 6. Outcome of the analysis of our proposed scheme using OFMC.

A. Formal Security Verification Using AVISPA Tool

The proposed authentication protocol for ideal PUF is also evaluated by using the formal verification tool, Automated Validation of Internet Security Protocols and Applications (AVISPA) [29]–[30], which provides automated validation of the security sensitive protocols and applications. It contains four backends and abstraction-based methods that are integrated through the high level protocol specific language (HLPSL). The outcome of the formal security verification of our proposed scheme using On-the-fly Model-Checker (OFMC) backend is shown in Fig. 6 which shows that our proposed scheme is safe. The details of the implementation process of the proposed scheme are provided in the supplementary material.

V. Conclusion

In this article, we first proposed a lightweight anonymous authentication protocol for RFID system using ideal PUF. Subsequently, considering the noise at PUF, we proposed an enhanced protocol which can support the noisy PUF environment. We analyzed the security and the performance of the proposed schemes. Analyses show that our protocols still remains safe even if an adversary has a physical access to an RFID tag. The proposed protocols ensures the desired security properties efficiently by exploiting the inherent security feature of PUFs. Specifically, tags do not require to store any secret (such as key). Overall, the performance of the proposed schemes are better than those of other existing PUF-based authentication protocols for RFID. Therefore, our proposed approaches is more suitable for designing a secure RFID system.

References

[1] P. Gope and T. Hwang, "Untraceable sensor movement in distributed IoT infrastructure," *IEEE Sensors J.*, vol. 15, no. 9, pp. 5340–5348, Sep. 2015.

[2] P. S. Ravikanth, "Physical one-way functions," Ph.D. dissertation, Dept. Media Arts Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2001.
[3] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf. (DAC)*, Jun. 2014, pp. 9–16.
[4] M. Asadpour and M. T. Dashti, "Scalable, privacy preserving radio-frequency identification protocol for the Internet of Things," *Concurr. Comput., Pract. Exp.*, vol. 27, no. 8, pp. 1932–1950, Jun. 2015.
[5] P. Gope, J. Lee, and T. Q. S. Quek, "Resilience of DoS attack in designing anonymous user authentication protocol for wireless sensor networks," *IEEE Sensors J.*, vol. 17, no. 2, pp. 498–503, Jan. 2017.
[6] D. Hein, J. Wolkerstorfer, and N. Felber, "ECC is ready for RFID—A proof in silicon," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science), vol. 5381. Aug. 2009, pp. 401–413.
[7] M. Hutter, M. Feldhofer, and T. Plos, "An ECDSA processor for RFID authentication," in *Radio Frequency Identification: Security and Privacy Issues* (Lecture Notes in Computer Science), vol. 6370. Sep. 2010, pp. 189–202.
[8] G. Avoine, M. A. Bingol, X. Carpent, and S. B. O. Yalcin, "Privacy-friendly authentication in RFID systems: On sublinear protocols based on symmetric-key cryptography," *IEEE Trans. Mobile Comput.*, vol. 12, no. 10, pp. 2037–2049, Oct. 2013.
[9] S. Kinoshita, M. Ohkubo, F. Hoshino, G. Morohashi, O. Shionoiri, and A. Kanai, "Privacy enhanced active RFID tag," in *Proc. Int. Workshop Exploiting Context Histories Smart Environ.*, May 2005, pp. 43–52.
[10] C. Ng, W. Susilo, Y. Mu, and R. Safavi-Naini, "New privacy results on synchronized RFID authentication protocols against tag tracing," in *Computer Security—ESORICS* (Lecture Notes in Computer Science), vol. 5789. Sep. 2009, pp. 321–336.
[11] C.-I. Lee and H.-Y. Chien, "An elliptic curve cryptography-based RFID authentication securing e-health system," *Int. J. Distrib. Sensor Netw.*, vol. 11, Dec. 2015, Art. no. 642425-1–642425-7.
[12] Y.-P. Liao and C. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," *Ad Hoc Netw*, vol. 18, pp. 133–146, Jul. 2014.
[13] H.-Y. Chien, "De-synchronization attack on quadratic residues-based RFID ownership transfer," in *Proc. AsiaJCIS*, May 2015, pp. 42–47.
[14] H.-Y. Chien, "Combining Rabin crypto-system and error correction codes to facilitate anonymous authentication with un-traceability for low-end devices," *Comput. Netw.*, vol. 57, no. 14, pp. 2705–2717, Jun. 2013.
[15] Y. Chen, J. S. Chou, and H. M. Sun, "A novel mutual authentication scheme based on quadratic residues for RFID systems," *Comput. Netw.*, vol. 52, no. 12, pp. 2373–2380, Aug. 2008.
[16] R. Doss, W. Zhou, S. Sundaresan, S. Yu, and L. Gao, "A minimum disclosure approach to authentication and privacy in RFID systems," *Comput. Netw.*, vol. 56, no. 15, pp. 3401–3416, Oct. 2012.
[17] C. C. Tan, B. Sheng, and Q. Li, "Secure and server-less RFID authentication and search protocols," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1400–1407, Apr. 2008.
[18] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID," in *Proc. Workshop RFID Lightweight Cryptograp.*, Sep. 2005, pp. 17–24.
[19] Z. Luo, T. Chan, and J. S. Li, "A lightweight mutual authentication protocol for RFID networks," in *Proc. IEEE Int. Conf. e-Business Eng.*, Oct. 2005, pp. 620–625.
[20] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," *Comput. Secur.*, vol. 55, pp. 271–280, Nov. 2015.
[21] J. Bringer, H. Chabanne, and T. Icart, "Improved privacy of the tree-based hash protocols using physically unclonable function," in *Proc. 6th Int. Conf. Secur. Cryptograp. Netw. (SCN)*, Sep. 2008, pp. 77–91.
[22] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, "PUF-enhanced offline RFID security and privacy," in *Proc. Secure Component Syst. Identificat.*, Cologne, Germany, Jun. 2010, pp. 102–106.
[23] M. Akgun and M. U. Caglayan, "Puf based scalable private RFID authentication," in *Proc. Int. Conf. Availability Rel. Secur.*, Washington, DC, USA, Aug. 2011, pp. 473–478.
[24] S. Kardas, M. S. Kiraz, M. A. Bing, and H. Demirci, "A novel RFID distance bounding protocol based on physically unclonable functions," in *Proc. Int. Conf. RFID Secur. Privacy*, Jun. 2012, pp. 78–93.
[25] S. Kardas *et al.*, "Puf-enhanced offline RFID security and privacy," *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 2059–2067, Nov. 2012.
[26] M. Akgun and M. U. Caglayan, "Providing destructive privacy and scalability in RFID systems using PUFs," *Ad Hoc Netw.*, vol. 32, pp. 32–42, Sep. 2015.
[27] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[28] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science Book), vol. 1666. Sep. 1999, pp. 388–397.
[29] (Nov. 25, 2016). *AVISPA Automated Validation of Internet Security Protocols and Applications*. [Online]. Available: http://www.avispa-project.org/
[30] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7124–7132, Nov. 2016.
[31] C. Bohm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. New York, NY, USA: Springer, Oct. 2012.
[32] S. Pandey, S. Deyati, A. Singh, and A. Chatterjee, "Noise-resilient SRAM physically unclonable function design for security," in *Proc. IEEE 25th Asian Test Symp. (ATS)*, Hiroshima, Japan, Nov. 2016, pp. 55–60, doi: 10.1109/ATS.2016.65.
[33] A. Van Herrewege *et al.*, "Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science), vol. 7397, A. D. Keromytis, Ed. Heidelberg, Germany: Springer, 2012, pp. 374–389.
[34] D. Moriyama, S. Matsuo, and M. Yung, "PUF-based RFID authentication secure and private under complete memory leakage," *IACR Cryptol. ePrint Arch.*, vol. 712, 2013. [Online]. Available: http://eprint.iacr.org/2013/712
[35] A. Aysu, E. Gulcan, D. Moriyama, P. Schaumont, and M. Yung, "End-to-end design of a puf-based privacy preserving authentication protocol," in *Proc. 17th Int. Conf. Cryptograph. Hardw. Embedded Syst. (CHES)*, vol. 9293. Saint-Malo, France, Sep. 2015, pp. 556–576.
[36] J. Delvaux, D. Gu, I. Verbauwhede, M. Hiller, and M.-D. Yu, "Efficient fuzzy extraction of puf-induced secrets: Theory and applications," in *Proc. 18th Int. Conf. Cryptograph. Hardw. Embedded Syst. (CHES)*, vol. 9813. Santa Barbara, CA, USA, Aug. 2016, pp. 412–431.
[37] *High-Capacity RFID Tags*. Accessed: Jan. 25, 2018. [Online]. Available: http://blog.pepperl-fuchs.us/high-capacity-rfid-tags
[38] C. Huth, A. Aysu, J. Guajardo, P. Duplys, and T. Güneysu, "Secure and private, yet lightweight, authentication for the IoT via PUF and CBKA," in *Proc. Int. Conf. Inf. Secur. Cryptol. (ICISC)*, 2017, pp. 28–48.
[39] A. Aysu, Y. Wang, P. Schaumont, and M. Orshansky, "New maskless debiasing method for lightweight physical unclonable function," in *Proc. IEEE Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2017, pp. 134–139.
[40] M. Suzuki, R. Ueno, N. Homma, and T. Aoki, "Multiple-valued debiasing for physically unclonable functions and its application to fuzzy extractors," in *Constructive Side-Channel Analysis and Secure Design* (Lecture Notes in Computer Science). Springer, 2017, pp. 248–263.
[41] W.-C. Wang, Y. Yona, S. N. Diggavi, and P. Gupta, "Design and analysis of stability-guaranteed PUFs," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 978–992, Apr. 2018.

Prosanta Gope received the M.Tech. degree in computer science and engineering from the National Institute of Technology, Durgapur, India, in 2009, and the Ph.D. degree in computer science and information engineering from National Cheng Kung University, Tainan, Taiwan, in 2015. He served over one year as a Post-Doctoral Research Fellow with the Singapore University of Technology and Design established in collaboration with the Massachusetts Institute of Technology. He is currently a Research Fellow with the Department of Computer Science, National University of Singapore. He has authored over 40 peer-reviewed articles in several reputable international journals and conferences, and has three filed patents. His research interests include lightweight authentication, authenticated encryption, access control system, and security in mobile communication, and hardware security of the IoT devices. He received the Distinguished Ph.D. Scholar Award in 2014 given by National Cheng Kung University.

Jemin Lee (S'06–M'11) received the B.S. (Hons.), M.S., and Ph.D. degrees in electrical and electronic engineering from Yonsei University, Seoul, South Korea, in 2004, 2007, and 2010, respectively. She was a Post-Doctoral Fellow with the Massachusetts Institute of Technology, Cambridge, MA, USA, from 2010 to 2013, and a Temasek Research Fellow at iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design, Singapore, from 2014 to 2016. She is currently an Assistant Professor with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea. Her current research interests include wireless communications, wireless security, intelligent networking, and machine-type communications.

Dr. Lee received the Chun-Gang Outstanding Research Award in 2011, the Temasek Research Fellowship in 2013, the IEEE ComSoc AP Outstanding Young Researcher Award in 2014, the IEEE WCSP Best Paper Award in 2014, and the IEEE ComSoc AP Outstanding Paper Award in 2017. She has served as a Guest Editor for the IEEE WIRELESS COMMUNICATIONS, special issue on LTE in Unlicensed Spectrum, in 2016, and *Physical Communication* (Elsevier), special issues on Physical Layer Security in 2016 and Heterogeneous and Small Cell Networks in 2014. She is currently an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE COMMUNICATIONS LETTERS.

Tony Q. S. Quek (S'98–M'08–SM'12–F'18) received the B.E. and M.E. degrees in electrical and electronics engineering from the Tokyo Institute of Technology, and the Ph.D. degree in electrical engineering and computer science from the Massachusetts Institute of Technology. He is currently a tenured Associate Professor with the Singapore University of Technology and Design (SUTD). He also serves as the Acting Head of ISTD Pillar and the Deputy Director of SUTD-ZJU IDEA. His main research interests include the application of mathematical, optimization, and statistical theories to wireless communication, networking, signal processing, and resource allocation problems. Specific current research interests include network intelligence, wireless security, Internet-of-Things, and big data processing.

He is a co-author of the book *Small Cell Networks: Deployment, PHY Techniques, and Resource Allocation* (Cambridge University Press, 2013) and the book *Cloud Radio Access Networks: Principles, Technologies, and Applications* (Cambridge University Press, 2017). He is currently an Elected Member of the IEEE Signal Processing Society SPCOM Technical Committee. He was an Executive Editorial Committee Member of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He has been actively involved in organizing and chairing sessions, and has served as a member of the Technical Program Committee and a symposium chair in a number of international conferences. He was an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE WIRELESS COMMUNICATIONS LETTERS.

Dr. Quek received the 2008 Philip Yeo Prize for Outstanding Achievement in Research, the IEEE GLOBECOM 2010 Best Paper Award, the 2012 IEEE William R. Bennett Prize, the 2015 SUTD Outstanding Education Awards–Excellence in Research, the 2016 IEEE Signal Processing Society Young Author Best Paper Award, the 2017 CTTC Early Achievement Award, the 2017 IEEE ComSoc AP Outstanding Paper Award, and the 2017 Clarivate Analytics Highly Cited Researcher. He is a Distinguished Lecturer of the IEEE Communications Society.