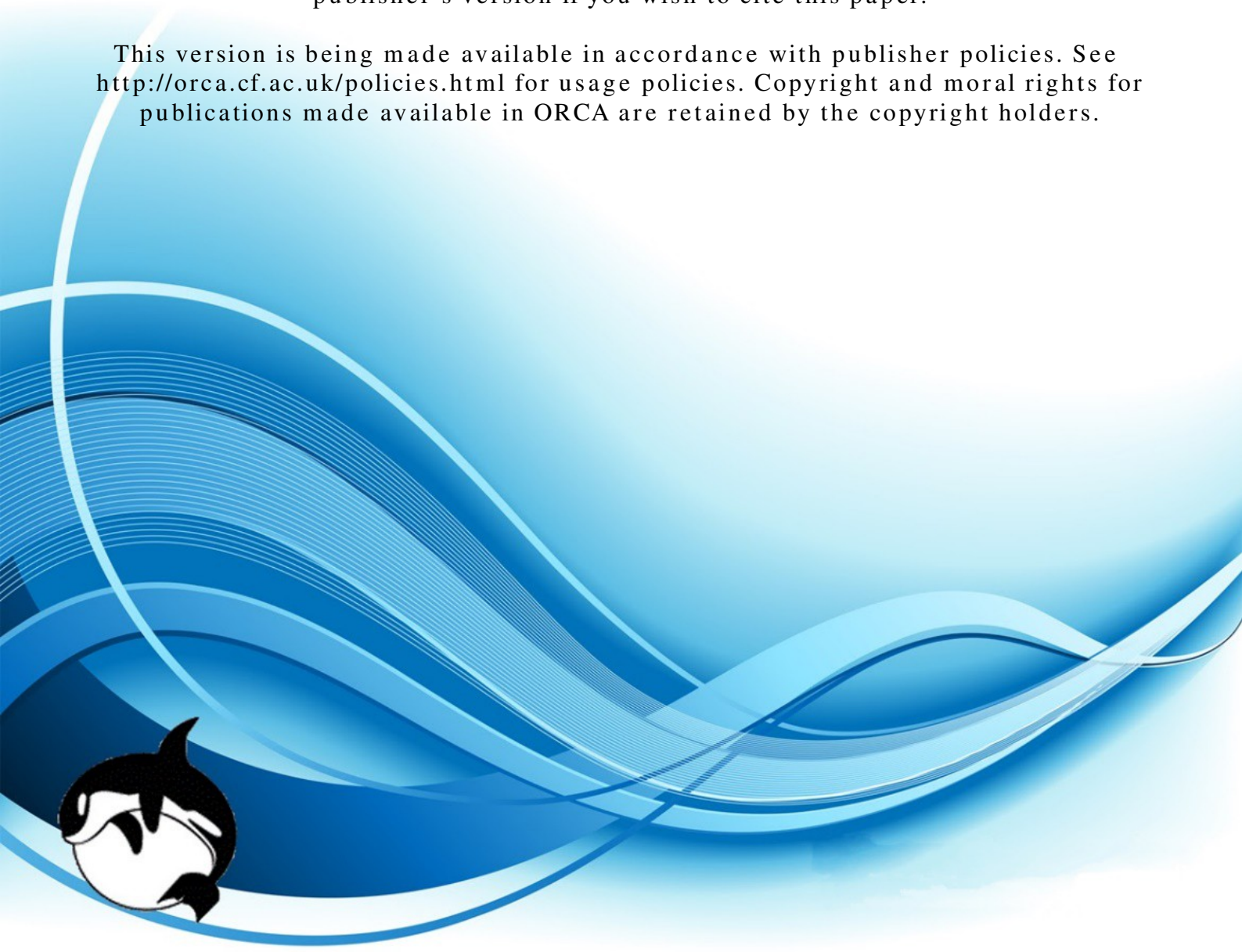

A Provably Secure Authentication Scheme for RFID-enabled UAV Applications

Prosanta Gope[1*], Owen Millwood[1], and Neetesh Saxena[2]

[1]Department of Computer Science

Univeristy of Sheffield, Regent Court, 211 Portobello Sheffield S1 4DP, United Kingdom.

Email: prosanta.nitdgp@gmail.com/p.gope@sheffield.ac.uk

[2] School of Computer Science and Informatics, Cardiff University, United Kingdom.

Abstract

Advantages of Physically Uncloneable Functions (PUFs) have led to appearing a substantial number of novel identification and authentication based systems such as Radio frequency identification (RFID), which is expected to replace the conventional bar-code identification system due to its advantages such as real-time recognition of a considerable number of objects. For example, RFID can be used to identify an unmanned aerial vehicle (UAV) when it is attached with a tag. In this article, we propose a novel anonymous authentication scheme for RFID-enabled UAV applications using Physically Unclonable Functions. Security and the performance analyses demonstrate that our proposed scheme is secure and efficient. Hence, it can be useful for several RFID-based secure application systems.

Keywords. *Unmanned aerial vehicle* , *Physically Uncloneable Functions*, *Fuzzy extractor*, *Realistic anonymous authentication.*

1 Introduction

Radio Frequency Identification, or RFID, has already become an imperative technology for identifying and tracking objects [1-5]. RFID uses a two-way radio signal receiver and transmitter (reader) for the interrogators. Radio signals are sent to the tag attached to the physical object and the interrogator

or reader is responsible for response. An RFID reader device is a network connected device (mobile or fixed) along with an antenna which is responsible to transmit power, data as well as commands to the objects tags.The versatility of RFID technology makes it ideal for use in the identification and authentication of UAVs in both commercial and/or military scenarios. Here we propose the example of a military scenario where a UAV must be authenticated before being allowed to operate within a secure airspace. In modern warfare, UAV drones are a commonly utlised resource that can perform reconnaissance and other useful tasks. Due to their widespread use, military personnel must be able to ensure that drones entering secure airspace are not being operated by their adversaries. In this case, these drones can be fitted with RFID tags and be required to pass through a reader checkpoint whereby the tag is scanned and it's credentials sent to a secure server unit for verification. Either the drone is authenticated, or if not, it can be intercepted. This scenario is also shownin Fig. 1. With the resource-constrained nature of RFID providing a requirement for protocols with limited computational overhead, we propose a solution utilising Physically Uncloneable Functions to reduce cost and complexity while retaining sufficient security for UAV-based authentication scenarios.

Now, as a localizer and tracker, the RFID-based system [3] outperforms other localization systems; however, it is vulnerable to anonymity and location privacy attacks [4], [5] because the RFID tags transmit their identification and location information to RFID readers as plain-text. Therefore, any attacker can easily track the tags by their identifications. Securing RFID-based systems is a challenging task due to the computational capability of the RFID tags is very limited [6], [7]. Furthermore, existing solutions often use low cost tags without considering hardware protection mechanisms. As a consequence, secrets stored in these tags can be recovered through basic side channel and invasive attacks [27], which allows for forging of the information of the tag (such as debit balance of the ticket). To address this issue, recently the concept of Physically Unclonable Function (PUF) technology [8-9] has been introduced. A PUF is a function derived from a physical characteristic and basic purpose of PUFs is to produce a device specific output for any input like as a fingerprint. Emergence of PUF has provided new flavour in Radio frequency identification (RFID) technology. With the inclusion of PUF, RFID can ensure hardware security.

1.1 Possible Security Threats in RFID Systems

There are many attacks that threaten the RFID systems and hence reveal user's privacy. Therefore, for ensuring a secure RFID systems we need to consider the following attacks:

- **Illicit Tracking Attack:** Since each object in the RFID-based applications is identified uniquely using the RFID tag, the adversary can mark each of these objects by their unique identities, which are transmitted frequently in the query/reply messages, and then track the objects and define their locations even with encrypted replies.

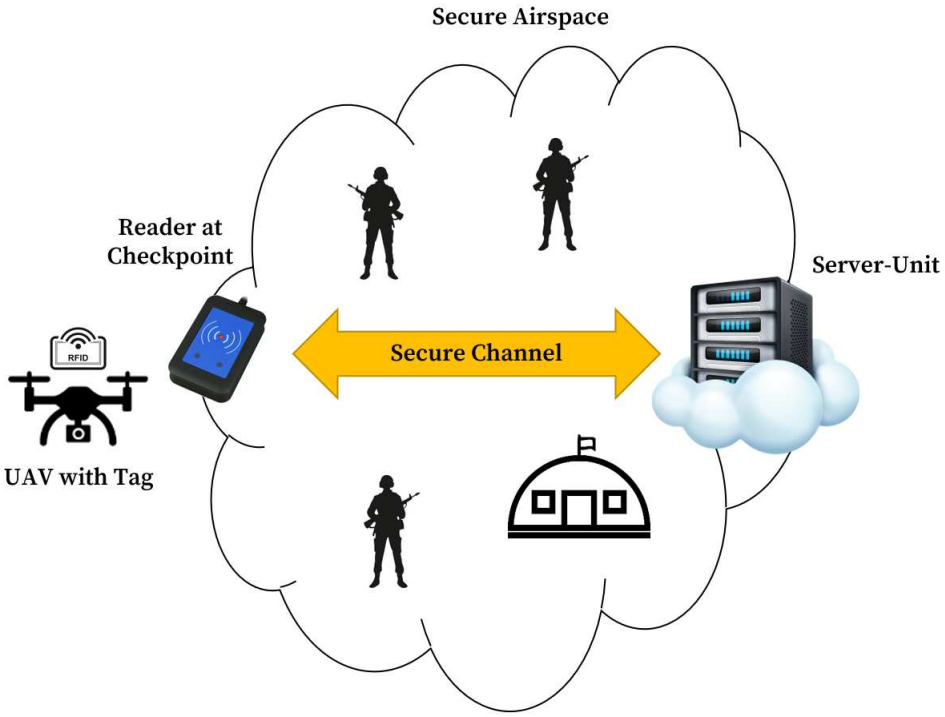

Figure 1: Example of UAV use within military airspace

- **Eavesdropping Attack:** Adversary listens to and records the communications among RFID tags and readers, in order to get critical information about the tagged objects.
- **Replay Attack:** Is a kind of Man in the Middle attack (MITM) who initiates the communication between the two parties then replay the subsequent messages to both parties.
- **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, to ensure forward secrecy both the backend server and tag need to update their secret security credentials. Now, if the response message from the backend server is blocked then the tag cannot ensure 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 [4].
- **Backward Secrecy Attack:** If an adversary gains access to the secret keys, then he/she should be able to trace back all the previous communications of the tag.
- **Physical attacks:** An adversary compromises a tag and should be able to obtain secure information such as secret key from the tag's memory through cold boot attacks, which is a kind of side channel attack. In this regard, an attacker with physical access to tag is able to retrieve some useful information stored in the tag. Then, the attacker may try to trace all previous communications of the tag's users. Many of the existing RFID authentication protocols are vulnerable to this attack.

- **Cloning attack:** Most tags are not tamper proof, hence an attacker can build a cloned tag which will be interpreted by the reader as a legitimate tag.

1.2 Related Work and Motivation

In general, the concept of PUF technology can be utilized to ensure higher degree of security and efficiency. In the last few years, some interesting PUF-based authentication schemes have been proposed. We can divide them into two categories: i)ideal PUF-based schemes [10-17], ii) noisy PUF based schemes [18-20]. Bringer et al. introduced an ideal-PUF-based scheme authentication protocol using ideal PUFs in [10]; however, the protocol fails to provide security against DoS and impersonation attacks [11]. Sadeghi et al. [11] applied an ideal-PUF in constructing RFID authentication to guarantee destructive privacy by considering the Vaudenay security model [16]. Soon after that, Kulseng et al. [12] proposed a new scheme that used the combination of PUF and a linear feedback shift register (LFSR). The protocol consists of four rounds and for each round the tag encodes it's identity by using XOR operation and a shared secret key. At the end of each session, the key is updated by both the server and tags; however, its security was re-examined and enhanced in view of ID protection (confidentiality) and desynchronized attack [13-14]. In 2015, Lee et al. proposed a new scheme under a new privacy setting [15]; however, its construction is based on a secure public-key encryption. In 2017, a new scheme was proposed by Pandey et al. The authors utilised the combination of PUF with a threshold cryptography. Here, the authors suggested the secret sharing technique for thwarting tag compromising attacks [17]; however, in their protocol the tag needs to perform some computationally expensive operation, which is infeasible for resource constrained tag devices. Although differential design mechanisms can improve reliability, noise still presents as a factor in PUF design, which may cause several of the output bits to be incorrect for any given challenge. Herrewege et al. [18] proposed an authentication protocol by considering noisy PUF condition; however, after thoroughly investigating their approach, we found the following weaknesses in these schemes. For instance, in [18], a tag needs to reveal its identity in order to help the verifier in finding a previous PUF output z , therefore this scheme fails to ensure anonymity property. In 2014, Moriyama et al. [19] suggested a new authenitcation protocol for RFID systems using PUF. The protocol allows a reader to update random status secret s, and then a tag receives s for each session; but in their scheme a tag needs to store helper data for output reconstruction, which will cause high storage overhead at the tag side. In addition, implementing the output reconstruction on the PUF-based device is a disadvantage in many applications. Recently, Gope et al. proposed a new authentication protocol [26] using noisy PUF condition; but like [19], in their scheme a tag requires to execute the computationally expensive reconstruction function and store helper data for output reconstruction, which will cause a high storage cost as well. To resolve this issue, in CHES 2015, Aysu et al. introduced a new PUF-based protocol [20] using reverse fuzzy ex-

tractor; however, according to [26], the protocol presented in [20] cannot provide privacy, which is one of the major security requirements in RFID-based system. Furthermore, in all the above PUF-based anonymous authentication protocols (including [18-20]), to identify the device, the reader-server unit requires to perform an exhaustive search operation; therefore, they are not suitable for the large-scale database application scenarios.

In a nutshell, in all the aforementioned schemes, the server needs to perform exhaustive search to identify the tag, which is not suitable for the applications with larger databases. The aim of this article is to address all the aforementioned issues by proposing a realistic privacy-preserving authentication protocol using PUF. We can summarize our contribution of this article as follows:

- We propose a novel authentication scheme for a noisy-PUF condition.
- Our proposed scheme will be able to ensure various important security features such as anonymity, protection against DoS attacks, etc., which are imperative for any IoT application and services.
- One of the notable properties of the proposed scheme is that, in our scheme the server will be able to identify the tag without performing any exhaustive search operation.

1.3 Fuzzy Extractor

A Fuzzy Extractor is a combination of two functions i.e., FE.Gen(.) [Key generation] and FE.Rec(.) [reproduction function]. We can consider FE.Gen(.) as a probabilistic algorithm for generating a key K and helper data hd, i.e., (K, hd) = FE.Gen(R) on a given input bit string R. FE.Rec(.) is a deterministic function, which takes a noisy input R' and the helper data hd and then it generates the key K i.e., K = FE.Rec ($R^{'}$, hd,) i.e., K = FE.Rec ($R^{'}$, hd) when the hamming distance between R' and R is at most d.

1.4 Reverse Fuzzy Extractor

In order to ensure fast implementation of secure sketch and fuzzy extractors, the concept of a reverse fuzzy extractor can be used. In this context, the PUF-enabled RFID devices do not require to execute any computationally intensive reconstruction algorithm. Instead, the device needs to execute the helper data generation algorithm.

1.5 Physically Uncloneable Function

A Physically Uncloneable Function (PUF) is a physical system, that for a given input - the challenge - provides an output - the response - that can serve as a secure unique identifier (digital fingerprint) for devices. Each response generated for any given challenge is entirely unique and unpredictable. The

entropy for a PUFs challenge/response pairs (CRPs) is attributed to the physical micro-variance in each chip caused during the manufacturing process that create unique behavioral differences between each individual PUF, making them very difficult to clone. The result of this is secure generation of challenges and responses that need not rely on complex and expensive cryptography. This lightweight nature of PUFs make them very suitable for enabling secure authentication for resource-constrained systems such as RFID.

We can define PUF as a pair of CRPs. For a given input challenge C, the PUF outputs a random string R i.e., $R = P(C)$. A PUF P is said to be $(d, n, l, \lambda, \epsilon)$-secure if the following conditions hold:

1. Conceive, there are two PUFs $P_1(\cdot)$ and $P_2(\cdot)$, and for any given input $C_1 \in \{0,1\}^k$, $\Pr[\mathrm{HD}(P_1(C_1), P_2(C_1)) > d] \geq 1 - \varepsilon$. Here, the parameter HD denotes the hamming distance.

2. For a given PUF $P_i(\cdot)$ and for any input $C_1, \cdots, C_n \in \{0,1\}^k$, $\Pr[\mathrm{HD}(P_i(C_1), P_i(C_2)) > d] \geq 1 - \varepsilon$.

3. Given, two PUFs $P_i(\cdot)$ and $P_{i*}(\cdot)$, and for any inputs $C_1, \cdots, C_n \in \{0,1\}^k$, $\Pr[\hat{H_\infty}(P_i(C_k), P_i*(C_j))_{1 \leq j,k \leq n, i \neq} \lambda] \geq 1 - \varepsilon$.

1.6 Pseudo Random Function

A pseudo random 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 $\mathcal{M} \epsilon \{0,1\}^*$ as input and provides an arbitrary string PRF(K, $\mathcal{M}$) which is indistinguishable from random string. Now, assume 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.

2 Our Proposed Scheme

This section introduces our realistic anonymous authentication scheme, which comprises of two phases: Setup Phase, and Authentication Phase.

2.1 Setup Phase

The Server randomly generates a challenge C_i for the i-th round and also a set of emergency challenges C_{em}= $\{c_1, ..., c_n\}$, which we can use later to avoid any desynchronization between the reader-server

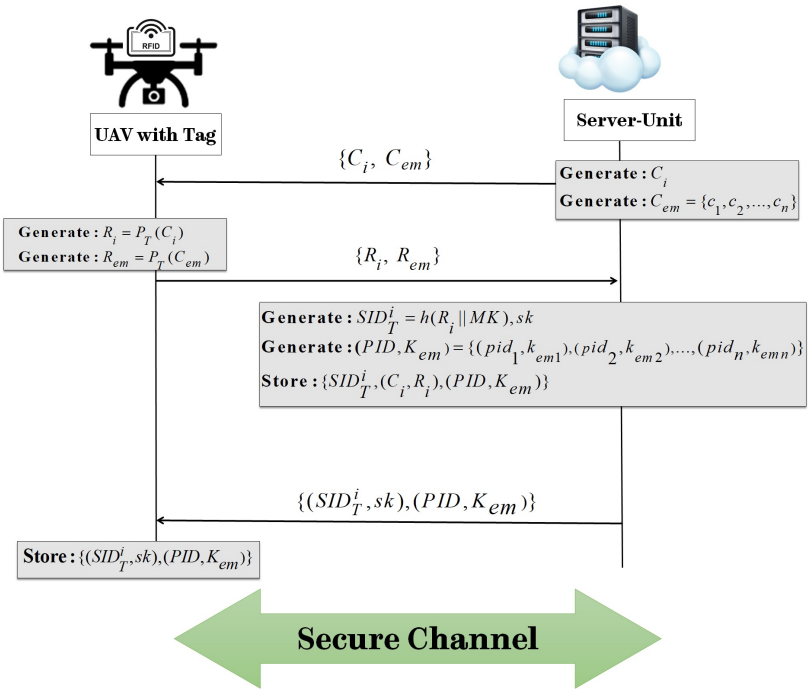

Figure 2: Setup Phase of the Proposed Scheme

unit and the tag. Then the server sends $\{C_i, C_{em}\}$ to the tag T. Hereafter, T extracts the PUF outputs: $R_i = P_T(C_i)$, $R_{em} = P_T(C_{em})$ and sends $\{R_i, R_{em}\}$ to the reader-server unit S. Next, S first generates a shadow identity $SID_T^i = h(R_i||MK)$, and a secret key sk, where MK denotes the master key of the server. Hereafter, S also generates a set of unique pseudo identity and emergency key pairs $(PID, K_{em}) = \{(sid_1, k_{em1}), ..., (sid_n, k_{emn})\}$ and sends $\{(SID_T^i, sk), (SID, K_{em})\}$ to the tag T. Finally, for each tag, S will store $\{(SID_T^i, sk), (C_i, R_i), (C_{em}, R_{em}), (PID, K_{em})\}$ in its database and the tag stores $\{(SID_T^i, sk), (PID, K_{em})\}$. Details of this phase is depicted in Fig. 2.

2.2 Authentication Phase

The Tag selects its i-th round shadow identity SID_T^i and then generates random number N_t and finally composes a request message M_1: $\{SID_T^i, N_t\}$ and sends it to S. Upon receiving the request message M_1, S first locates SID_T^i in its database and loads $\{(C_i, R_i), sk\}$ into its memory. Hereafter, S generates a nonce N_s and calculates $N_s^* = sk \oplus N_s$, *the key-hash output* $Res_S = h(N_t \,||\, sk \,||\, N_s^*)$ and sends $\{C_i, N_s^*, Res_S\}$ to the tag. Next, the tag extracts the PUF output $R_i' = P_T(C_i)$ and checks the key-hash output Res_S. If it is valid, the tag computes the following: $N_s = sk \oplus N_s^*$, $(K_i, hd_i) = \text{FE.Gen}(R_i')$, $hd^* = h(sk \,||N_s) \oplus hd_i$, $C_{i+1} = h(C_i||K_i)$, $R_{i+1}' = P_T(C_{i+1})$, $R_{i+1}^* = K_i \oplus R_{i+1}'$, $Res_T = h(N_s||K_i||R_{i+1}^*||hd^*)$, $SID_T^{i+1} = h(SID_T^i||K_i)$, $sk = h(sk \,||\, K_i)$. Next, the tag composes a response message M_3: $\{R_{i+1}^*, Res_T, hd^*\}$ and sends it to S.

Upon receiving the response message M_3, S first calculates $hd_i = h(sk \,||N_s) \oplus hd^*$, $K_i = \text{FE.Rec}(R_i,$

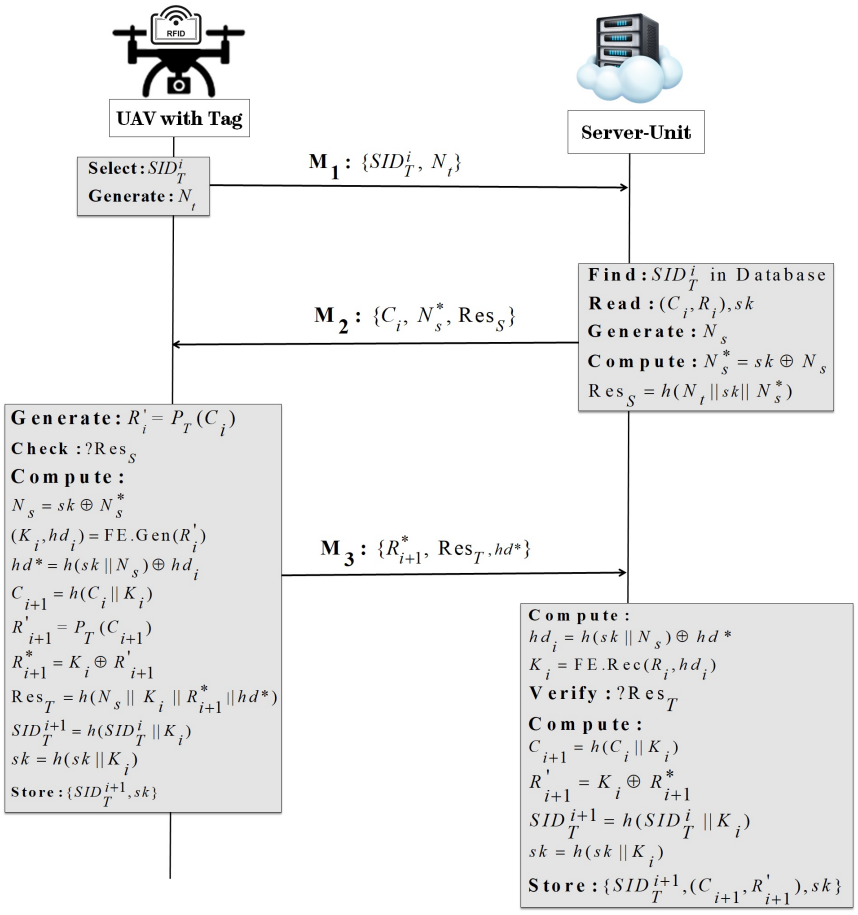

Figure 3: Proposed Authentication Scheme

hd_i) and then verifies the key-hash output Res_T. If the verification is successful, S calculates C_{i+1}= $h(C_i||K_i)$, R'_{i+1}= $K_i \oplus R^*_{i+1}$, SID_T^{i+1}=$h(SID_T^i \,||K_i)$, $sk = h(sk \,||\, K_i)$ and stores $\{SID_T^{i+1}, (C_{i+1}, R'_{i+1}), sk)$ for the next authentication round $(i+1)$. Otherwise, S terminates the authentication process and asks the tag to try again by using one of the unused pairs of $(pid_x, k_{emx}) \in (PID, K_{em})$. Each time a pair is used up, it is then needed to be deleted from both the ends. In this case, S will select one of the unused emergency CRPs from (C_{em}, R_{em}) and a new pseudo identity will be provided to the tag T. Finally, the used pair of emergency CRPs also needs to be deleted from (C_{em}, R_{em}).

In our proposed scheme, tag can only use t numbers of unused pairs of (PID, K_{em}) and (C_{em}, R_{em}), where $(t \leq n-1)$. After that, the tag needs to request for reloading. In that case, the tag needs to include its $(t+1)$ shadow identity along with the nonce N_t and the "Re-Load" message in the authentication request M_1. Then, after interrogating the tag, S will generate a set of new pairs and then use session key K_i to encode them and subsequently send them to the tag. Details of our authentication phase is presented in Fig. 3.

3 Security Analysis

In this section, we formally analyze the security of the proposed realistic lightweight anonymous authentication scheme on the major security requirements.

3.1 Security Model

We now consider Ouafi and Phan's security model [28] for analyzing both the security and privacy of the proposed scheme. This model allows an adversary $\mathcal{A}$ to eavesdrop on the radio link between the tag and readers. In addition, the adversary can also perform any active or passive attacks. In this regard, $\mathcal{A}$ needs to model the following queries in polynomial time.

- **Execute** ($\mathcal{S}$, $\mathcal{T}$, i): This query represents the modeling of the passive attacks. In this context, the adversary eavesdrops all the messages communicated between the tag $\mathcal{T}$ and the reader-server unit $\mathcal{S}$ in i-th session. Consequently, the attacker should be able to acquire all the exchanged data communicated between the tag $\mathcal{T}$ and reader-server unit $\mathcal{S}$.

- **Send** (U, V, m, i): This query denotes the modeling of the active attacks. Here, an adversary $\mathcal{A}$ is allowed to impersonate as a legitimate reader U in the i-th session and forwards a message m to a tag V.

- **Query**($\mathcal{T}$, m_1,m_2) : This query models the adversary's ability to investigate a tag. For this, $\mathcal{A}$ sends m_1 to $\mathcal{T}$ and receives m_2 from $\mathcal{T}$.

- **Block** ($\mathcal{A}$): This query models the adversary's ability to launch a DoS attack. Here, $\mathcal{A}$ is permitted to block a part of the protocol and break the synchronization between tag $\mathcal{T}$ and the backend server $\mathcal{S}$.

- **Corrupt** ($\mathcal{T}$, K): In this query, the attacker $\mathcal{A}$ has the permission to access secret information (K) stored in the tag's memory.

- **Test** ($\mathcal{T}_0$, $\mathcal{T}_1$, i): This query defines the indistinguishability-based notion of untraceable privacy (UPriv). If the party has accepted and is being asked a Test query, then depending on a randomly chosen bit $b \in \{0, 1\}$, $\mathcal{A}$ is given $\mathcal{T}_b$ from the set $\{\mathcal{T}_0, \mathcal{T}_1\}$. We say, $\mathcal{A}$ wins th game if he/she can correctly guess the bit b. In order for the notion to be meaningful, it is important that a **Test** session must be fresh in the sense of Definition 2.

Definition 1 (**Partnership & Session Completion**) We say that $\mathcal{A}$ *reader instance* $\mathcal{S}_j$ *and a tag instance* $\mathcal{T}_i$ *are partners if, and only if, both have output Accept*($\mathcal{T}_i$) *and Accept*($\mathcal{S}_j$) *respectively, that denotes the completion of the protocol session.*

Definition 2 (**Freshness**) *A party instance is said to be fresh if, and only if, at the end of execution of the identification protocol*

1. *it has output Accept with or without a partner instance,*

2. *both the instance and its partner instance (if such a partner exists) have not been sent a Corrupt query.*

Definition 3 (**Untraceable Privacy** (**UPriv**)) Defines the game $\mathcal{G}$ played between a malicious adversary $\mathcal{A}$ and a collection of reader and tag instances. $\mathcal{A}$ runs the game $\mathcal{G}$ whose setting is as follows.

- ***Learning phase*:** $\mathcal{A}$ is able to send any **Execute**, **Send**, and **Corrupt** queries and interact with the reader-server unit $\mathcal{S}$ and tag $\mathcal{T}_0$, $\mathcal{T}_1$that are chosen randomly.
- ***Challenge phase*:** The attacker selects two tags $\mathcal{T}_0$, $\mathcal{T}_1$ and forwards a Test query ($\mathcal{T}_0$, $\mathcal{T}_1$, i) to the challenger $\mathcal{C}$. After that, $\mathcal{C}$ randomly selects $b \in\{0, 1\}$ and the attacker determines a tag $\mathcal{T}_b\in\{\mathcal{T}_0, \mathcal{T}_1\}$ using *Execute* and *Send* queries.
- ***Guess phase*:** The attacker $\mathcal{A}$ finishes the game $\mathcal{G}$ and outputs a bit $b'\in\{0, 1\}$ as guess of b. The success of attacker $\mathcal{A}$ in the game $\mathcal{G}$ and consequently breaking the security of UPriv is quantified via $\mathcal{A}$'s advantage in recognizing whether attacker $\mathcal{A}$ received $\mathcal{T}_\mathbf{0}$ or $\mathcal{T}_1$, and denoted by $Adv_{\mathcal{A}}^{UPriv}(k) = |\Pr\left[b' = b\right] - \frac{1}{2}|$, where k is a security parameter.

Proposition 1 *The proposed scheme is secure against any traceability attacks.*

Proof. In our proposed scheme, after a successful authentication, the tag updates its secrets sk. Besides, the pseudo identity PID changes in each session. Therefore, it will be difficult for an adversary to perform any traceability attack by performing the following phases:

Learning phase: In the i-th round, the attacker $\mathcal{A}$ sends an *Execute* query ($\mathcal{S}$, $\mathcal{T}_0$, i) and obtains the parameters $\{SID_i^{\mathcal{T}_0}, Res_{T,i}^{\mathcal{T}_0}\}$.

***Challenge phase*:** $\mathcal{A}$ selects two fresh tags $\mathcal{T}_0$, $\mathcal{T}_1$and sends a Test query ($\mathcal{T}_0$, $\mathcal{T}_1$, i+1). Next, according to the randomly chosen bit $b\in\{0, 1\}$, the attacker is given a tag $\mathcal{T}_b\in\{\mathcal{T}_0, \mathcal{T}_1\}$. After that the attacker $\mathcal{A}$ sends an Execute query ($\mathcal{S}$, $\mathcal{T}_b$, i+1) and obtains $\{SID_{i+1}^{\mathcal{T}_b}, Res_{T,i+1}^{\mathcal{T}_b}\}$.

Guess phase: In the *Learning phase* the tag $\mathcal{T}_0$ updates its secret sk, therefore for the two subsequent sessions i and i+1 the parameter $Res_{T,i}^{\mathcal{T}_0}$ and $Res_{T,i+1}^{\mathcal{T}_b}$ are calculated as follows: $Res_{T,i}^{\mathcal{T}_0} = h(N_s||K_{\mathcal{T}_0,i}||R^*_{\mathcal{T}_0,i+1}||hd^*)$, $Res_{T,i+1}^{\mathcal{T}_b} = h(R_{\mathcal{T}_b,(i+1)+1}||hd^*||K_{\mathcal{T}_b,(i+1)+1}||N_s)$. Since $R^*_{\mathcal{T}_0,i+1}\neq R_{\mathcal{T}_b,(i+1)+1}$, $K_{\mathcal{T}_0,i}\neq K_{\mathcal{T}_b,(i+1)+1}$, and $SID_i^{\mathcal{T}_0} \neq SID_{i+1}^{\mathcal{T}_b}$ therefore the adversary needs make a random guess. In this context, the advantage of the adversary recognizing $\mathcal{T}_\mathbf{0}$ or $\mathcal{T}_1$, can be denoted by $Adv_{\mathcal{A}}^{UPriv}(k)$ $= |\Pr\left[b' = b\right] - \frac{1}{2}|\leq\epsilon$.

Proposition 2 *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 $\mathcal{C}$. In this proof, we consider (Reader-Backend Server) as a single unit $\mathcal{S}$.

(1)$\mathcal{C}$ selects a valid backend server $\mathcal{S}$ and a tag $\mathcal{T}$.

(2)$\mathcal{A}$ calls the following oracles: *Send, Query, and Execute* on $\mathcal{S}$ and $\mathcal{T}$ 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 $\mathcal{A}$ needs to respond to the interrogation of the backend server $\mathcal{S}$. For that, $\mathcal{A}$ needs to send a valid one-time pseudo identitySID_T^i and also needs to generate a valid response message $Res_T = h(N_s||K_i||R_{i+1}^*||hd^*)$. In this case, $\mathcal{A}$ must know the secret parameter i.e., K_i. However, $\mathcal{A}$ cannot expose the secret K_i which implies she cannot impersonate as a legitimate tag. On the other hand, to be authenticated as a backend server, $\mathcal{A}$ needs to invoke a Query oracle in (4) and also needs to sends a valid response message $Res_S = h(N_t \;||\; sk \;||\; N_s^*)$. As a result, $\mathcal{A}$ cannot infer sk, hence cannot produce the valid key-hash response Res_S. Accordingly, $\mathcal{A}$ cannot impersonate as a legitimate $\mathcal{S}$.

Proposition 3 *The proposed scheme can ensure the resilience of DoS or desynchronization attacks.*

Proof. As discussed, in the proposed scheme, to address desynchronization or DoS attacks, where during regiestration S also generates a set of unique shadow identity and emergency key pairs (SID, K_{em}) =$\{(sid_1,k_{em1}),...,\ (sid_n,\ k_{emn})\}$ and server maintains t numbers of unused pairs of (PID, K_{em}) and (C_{em}, R_{em}), where $(t \leq n-1)$.

Now, if $\mathcal{A}$ calls the *Block* oracle, the backend server does not receive the response message M_3:$\{R_{i+1}^*,\ Res_T,\ hd^*\}$ and accordingly cannot obtain R_{i+1}^* for the next round. To address this issue, the tag needs select one of the unused pair of $(sid_j,k_{emj}) \in (PID,\ K_{em})$ and continue the authentication process. At the end of the authentication process, both the tag and server delete (pid_j,k_{emj}) from their memory. In this way, we ensure security against DoS to desynchronization attacks.

Proposition 4 The proposed scheme is secure agianst replay attacks.

Proof. In the proposed scheme, an adversary cannot reuse the message M_1: $\{SID_T^i\ ,\ N_t\}$ since the pseudo identity SID_T^i changes in each session. The adversary cannot resend the message $\{C_i,\ N_s^*,\ Res_S\}$ since the secret sk changes in each session. Similarly, an adversary cannot resend M_3:$\{R_{i+1}^*,\ Res_T,\ hd^*\}$, since the parameter Res_T is associated with the nonce N_s, which changes in each session.

Proposition 5 *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 *Corrupt* oracle.

Table 1: Performance Benchmarking based on Three Major Security Requirements

Schemes	Mutual Authentication	Untraceability	Scalability
Scheme Presented in [19]	✓	✓	×
Scheme Presented in [20]	✓	×	×
Proposed Tag-Identification Scheme	✓	✓	✓

Table 2: Performance Benchmarking based on the Computational Cost

Schemes	**UAV with Tag**	**Server Unit**
Scheme Presented in [19]	$2h$ + $2P$+FE.Rec+2RNG ≈19.68 ms	$3h$ +1RNG+FE.Gen ≈1.07 ms
Scheme Presented in [20]	$3h$ + $2P$+1RNG+FE.Gen+SKE ≈17.85 ms	$3h$ + 1RNG+FE.Rec+SKD ≈6.11 ms
Proposed Scheme	$5h$ + $2P$+1RNG+FE.Gen ≈14.58 ms	$5h$ + 1RNG+FE.Rec ≈3.73 ms
h :One-way Hash Operation; P : Secure PUF Operation; *RNG:* Random Number Generation;		
SKE/D:Private Key Operations; *FE.Gen/Rec*:Fuzzy Extractor Generation/Reconstruction		

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. Thus, 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 access to the RFID tag, she cannot compromise the security of the proposed protocol. Furthermore, since PUFs are safe against cloning, a PUF cannot be recreated by the adversary. 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.

4 Performance Benchmarking and Comparison

In this section, we show that the performance of our proposed scheme is better than the other two recently proposed noisy-puf-based anonymous authentication protocols for RFID: [19] and [20]. In

Table 3: Execution Time of Relevant Cryptographic Operations

Crypto-Operations	**UAV with Tag**	**Server Unit**
H(SHA-256)	1.48 ms	0.045 ms
SE(AES-CBC Encryption)	6.23 ms	-
SD(AES-CBC Decryption)	-	2.47 ms
PUF (SRAM PUF)	1. 12 ms	-
FE.Gen (.)	3.46 ms	0.89 ms
FE.Rec (.)	11.52 ms	3.46 ms

this regard, the performance of the proposed authentication scheme has been compared with [19] and [20], by considering three major security requirements (shown in Table I). From Table I, we see that the scheme presented in [20] cannot ensure the untraceability property (demonstrated in [26]). Furthermore, in [19] and [20] to identify the tag, the server needs to launch an exhaustive search operation; therefore, the protocols presented in [19] and [20] cannot ensure the scalability property. Whereas in our proposed authentication protocol, S can identify a valid user without launching any exhaustive search. Next, we consider the computation cost for analysing the performance of the proposed scheme. From Table II, we can see that in [19] the tag needs to perform the computationally intensive reconstruction operation, which will create a very large computational burden on the PUF-enabled RFID tags. Whereas in our proposed scheme and [20], the tag needs to implement much more efficient helper data generation phase. Thus, the computation overhead of the proposed scheme is quite similar to [20] (as shown in Table II). To evaluate the performance of the above three protocols, here we implement all the cryptographic operations used in these protocols on a Xilinx XC5VLX30 with the system clock 1.84 MHz and 16KByte of program memory (operating as a tag) and an Intel Core i5-4300 dual-core 2.60 GHz CPU machine (operating as the Reader-Server Unit). In this regard, for PUF operation we consider the SRAM PUF, where to evaluate our noisy-PUF-based solutions, before execution of each phase of the above protocols, we power cycle the device to re-initialize the SRAM-PUF. This gives us a real SRAM PUF noise profile. Here we construct the helper data from a (63,16,23)-BCH code. For the hash operation and symmetric key encryption/decryption operations, we consider the SHA-256, AES-CBC mode, respectively. From Table II, we can see that our proposed scheme takes less computational overhead at the tag (14.58 ms) as compared to others, which is imperative for the resource limited RFID tags. On the other hand, since our proposed scheme is reverse-FE-based, where server needs to perform the computationally expensive operations (FE.REC). Hence, computational cost of the proposed scheme at the server end is more than the [19]. Table III shows the details on the computation cost for each operation at the tag and the reader-server ends. To sum up, based on the above performance outcomes of the proposed scheme, we can argue that our proposed authentication protocol can be used to create several RFID-based practically realizable security solutions using PUFs.

5 Conclusion

RFID is a technology that allows over the air identification of objects, animals or persons. The central figure of an RFID system is a small resource constrained device called tag. It communicates through radio waves with an unconstrained device capable of much more computation, called reader. The reader is connected through a secure channel with a back-end database that contains information about all tags. The result of communication between reader and tag is the identification of the entity the tag

is attached to. In this article we present a new PUF-based privacy-preserving authentication protocol for an RFID-enabled UAV system, which can guarantee several imperative security properties such as the resilience against man-in-the-middle attacks, privacy against-eavesdropper, etc. (as discussed in Section 3), which are necessary for any RFID-based application. Security and the performance analysis demonstrate that our proposed authentication scheme is secure and efficient; hence, it can be useful for several RFID-based practically realisable security solutions using PUFs.

References

[1] A. Grover and H. Berghel "A Survey of RFID Deployment and Security Issues," Inf. Process. Syst., vol. 7, no. 4, pp. 561–580, dec 2011.

[2] J. Banks, D. Hanny, M. Pachano and L.Thompson "RFID Applied," Wiley, 2007.

[3] Want R.: An introduction to RFID technology. IEEE Pervasive Computing, vol. 5, no. 1, pp. 25–33, 2006.

[4] J. Kim, C. Yang, and J. Jeon J," A Research on Issues Related to RFID Security and Privacy" Boston, MA: Springer US, 2007, pp. 412–420.

[5] B. Preneel. "Cryptography best practices," [Online]. Available: https://secappdev.org/handouts-2018.html (2018, Feb).

[6] A. Khattab, Z. Jeddi, E. Amini, and M. Bayoumi, "RFID Security Threats and Basic Solutions," Cham: Springer International Publishing, 2017, pp. 27–41.

[7] P. Peris-Lopez P., J.C. Hernandez-Castro, J. M. Estevez-Tapiador and A. Ribagorda, "RFID Systems: A Survey on Security Threats and Proposed Solutions," Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 159–170.

[8] P.S. Ravikanth, "Physical One-Way Functions," Ph.D. thesis,. Massachusetts Institute of Technology, 2001.

[9] G. Suh, S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in: Design Automation Conference, 2007, DAC '07, 44th ACM/IEEE, 2007, pp. 9–14.

[10] J. Bringer, H. Chabanne, T. Icart, "Improved privacy of the tree-based hash protocols using physically unclonable function, " in: Proceedings of the 6th International Conference on Security and Cryptography for Networks, SCN '08, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 77–91.

[11] A.-R Sadeghi, I. Visconti, C. Wachsmann, " PUF-enhanced RFID security and privacy, " in: Secure Component and System Identification – SECSI'10, Cologne, Germany, 2010.

[12] L. Kulseng, Z. Yu, Y.Wei, and Y. Guan, "Lightweight mutual authentication and ownership transfer for RFID systems, "in: Proceedings of the IEEE Conference on INFOCOM 2010, RFIDSec'11, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 251–255.

[13] M. Akgun, M. U Caglayan, "Puf based scalable private RFID authentication," in: Proceedings of the 20 11 Sixth International Conference on Availability/ Reliability and Security, ARES '11, IEEE Computer Society, Washington, DC, USA, 2011, pp. 473–478.

[14] S. Kardas S., S. elikc, M. Yıldız, A. Levi, "Puf-enhanced offline RFID security and privacy. " J. Netw. Comput. Appl. 35 (6) (2012) 2059–2067.

[15] K. Lee, J. G. Nieto, and C. Boyd, " A State-Aware RFID Privacy Model with Reader Corruption, "Cyberspace Safety and Security,LNCS Vol. 7672, pp. 324–338, Springer, 2015.

[16] S. Vaudenay, "On Privacy Models for RFID," AsiaCrypt 2007, LNCS Vol. 4833, pp. 68-87, Springer, (2007)

[17] S. Pandey, S. Deyati, A. Singh and A. Chatterjee, " Noise-Resilient SRAM Physically Unclonable Function Design for Security," IEEE 25th Asian Test Symposium (ATS), Hiroshima, 2016, pp. 55-60. doi: 10.1109/ATS.2016.65.

[18] A. V. Herrewege, S. Katzenbeisser, R. Maes, R. Peeters, et al. "Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs," In: Keromytis, A.D. (ed.) FC 2012. LNCS, vol. 7397, pp. 374–389. Springer, Heidelberg

[19] D. Moriyama, S. Matsuo, M. Yung, "PUF-based RFID authentication secure and private under complete memory leakage," IACR Cryptology ePrint Archive 2013, 712 (2013), http://eprint.iacr.org/2013/712.

[20] A. Aysu, E. Gulca, D. Moriyama, P. Schaumont, and M. Yung, " End-to-end Design of a PUF-based Privacy Preserving Authentication Protocol," *In: Cryptographic Hardware and Embedded Systems (CHES)* LNCS vol. 9293, pp.555-576, (2015).

[21] Y. Dodis, J. Katz, J., L. Reyzin, A. Smith, " Robust fuzzy extractors and authenticated key agreement from close secrets," *In: Advances in Cryptology (CRYPTO),* LNCS, vol. 4117, pp. 232–250. Springer (2006)

[22] Y. Dodis, L. Reyzin, A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, " *In: Advances in Cryptology (EUROCRYPT)* LNCS, vol. 3027, pp. 523–540 (2004)

[23] X. Boyen, "Reusable cryptographic fuzzy extractors," *In: ACM Conference on Computer and Communications Security (ACM CCS)* pp. 82–91. ACM (2004)

[24] C. Bosch, J. Guajardo, A.R Sadeghi, J. Shokrollahi, P. Tuyls, " Efficient helper data key extractor on FPGAs," *In: Cryptographic Hardware and Embedded Systems (CHES)*, LNCS, vol. 5154, pp. 181–197. Springer (2008)

[25] J. Delvau, D. Gu, I. Verbauwhede, M. Hiller, and J. Yu, " Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications," *In: Cryptographic Hardware and Embedded Systems (CHES)*. LNCS vol. 8913 pp. 412-430, Springer (2016).

[26] P. Gope, J. Lee, and T˜Q. S. Quek, "Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions," *IEEE Transactions on Information Forensics and Security,* vol. 13(11), pp. 2831-2843, 2018.

[27] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *in Proc. CRYPTO'99*, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.

[28] K. Ouafi and R. C.-W. Phan, Privacy of recent RFID authentication protocols, in: Information Security Practic and Experience, Springer, pp. 263-277, 2008.

Author(s) Biographies

Prosanta Gope is currently working as an Assistant Professor (Lecturer) in the Department of Computer Science (Cyber Security) at the University of Sheffield, UK. Dr. Gope served as a Research Fellow in the Department of Computer Science at National University of Singapore (NUS). Primarily driven by tackling challenging real-world security problems, he has expertise in lightweight anonymous authentication, authenticated encryption, access control, security of mobile communications, healthcare, Internet of Things, Cloud, RFIDs, WSNs, Smart-Grid and hardware security of the IoT devices. He has authored more than 75 peer-reviewed articles in several reputable international journals and conferences and has four filed patents. He received the *Distinguished Ph.D. Scholar* Award 2014 by National Cheng Kung University (Taiwan). Dr. Gope has served as TPC member in several international conferences such as IEEE GLOBECOM, ARES, etc. He currently serves as an Associate Editor for the IEEE INTERNET OF THINGS JOURNAL, IEEE SYSTEMS JOURNAL, IEEE SENSORS JOURNAL, the *Security and Communication Networks*, and the *Mobile Information Systems Journal.*

Owen JW Millwood recieved a BSc (Hons) in Computer Science from the University of Hull in 2019 and is currently working towards his PhD with the Security of Advanced Systems research group at the University of Sheffield. He is interested in

and currently researching Lightweight Authentication Schemes, Physically Uncloneable Functions and Machine Learning Attacks on Physically Uncloneable Functions.

Neetesh Saxena is currently an Assistant Professor (lecturer) with the School of Computer Science and Informatics at Cardiff University, UK with more than 14 years of teaching/research experience in academia. Before joining CU, he was an Assistant Professor with Bournemouth University, UK. Prior to this, he was a Post-Doctoral Researcher in the School of Electrical and Computer Engineering at the Georgia Institute of Technology, USA. He was also with the Department of Computer Science, The State University of New York (SUNY) Korea, South Korea as a Post-Doctoral Researcher and a Visiting Scholar at the Department of Computer Science, Stony Brook University, USA. He earned my PhD in Computer Science and Engineering from Indian Institute of Technology (IIT), Indore, India. He was a DAAD Scholar at Bonn-Aachen International Center for Information Technology (B-IT), Rheinische-Friedrich-Wilhelms UniversitÃ€t, Bonn, Germany and was also a TCS Research Scholar. His current research interests include cyber security and critical infrastructure security, including cyber-physical system security: smart grid, V2G and cellular communication networks.