k-Strong Privacy for RFID Authentication Protocols Based on Physically Unclonable Functions

Süleyman Kardaş, Serkan Çelik, Muhammed Ali Bingöl, Mehmet Sabir Kiraz, Hüseyin Demirci, Albert Levi

TÜBİTAK BİLGEM UEKAE, Kocaeli, Turkey
Sabancı University, Faculty of Engineering and Natural Sciences, İstanbul, Turkey

Abstract. This paper examines Vaudenay's privacy model, which is one of the first and most complete privacy models featured the notion of different privacy classes. We enhance this model by introducing two new generic adversary classes, k-strong and k-forward adversaries where the adversary is allowed to corrupt a tag at most k times. Moreover, we introduce an extended privacy definition that also covers all privacy classes of Vaudenay's model. In order to achieve highest privacy level, we study low cost primitives such as Physically Unclonable Functions (PUFs). The common assumption of PUFs is that their physical structure is destroyed once tampered. This assumption works only in the ideal case because the tamper resistance depends on the ability of the attacker and the quality of the PUF circuits. In this paper, we have weaken this assumption by introducing a new definition *k-resistant PUFs*. k-PUFs are tamper-resistant against at most k attacks, i.e., their physical structure remains still functional and correct until at most k^{th} physical attack. Furthermore, we prove that strong privacy can be achieved without public-key cryptography using k-PUF based authentication. We finally prove that our extended proposal achieves both reader authentication and k-strong privacy.

Keywords: RFID, Security, Privacy, Physically Unclonable Function

1 Introduction

Radio Frequency IDentification (RFID) technology has benefited increasing attention as an emerging solution for automatically identifying and/or authenticating distant objects and individuals. A typical RFID system generally consists of tags, i.e., a microcircuit with an antenna, readers, which allow to remotely query the tags, and a back-end server that manages all the information related to each tag. The tag transfers its coded data when queried by a reader. The reader consigns the packets collected from the tag to the back-end server in order to perform the identification and/or authentication process.

Recently, many technologies based on RFID have been rapidly deployed in several daily life applications such as payment, access control, ticketing, e-passport, and etc. The security and privacy are two major concerns in these

applications because the communication between tags and readers runs on an insecure wireless channel. These concerns are definitely critical points when tags are required to provide a proof of identity. The most conspicuous privacy risk is the tracking of the tag owner that allows the creation and abuse of particular tag owner profiles. Therefore, an RFID system should provide confidentiality of the tag identity along with untraceability of the tag owner even the internal state of the tag has been disclosed [41]. Besides, an RFID system should be resistant against the traditional authentication and identification threats such as tag impersonation, tag cloning and denial of service attack [9]. Mitigating these problems requires the researchers to design identification/authentication protocols that include cryptographic mechanisms. On the other hand, most of RFID tags have limited memory and computational capability; therefore, the existing privacy-preserving mechanisms, which require high computational costs, are not applicable to many restricted RFID systems. Furthermore, most of RFID tags are not tamper resistant against strong adversarial attacks. Namely, physical attacks on tag's chip allow the adversary to learn the secrets stored in the tag. Thus, the design of a privacy preserving and cost-efficient RFID authentication protocol is a challenging task for industrial applications. To fulfill these needs, several authentication mechanisms have been proposed in the literature [6, 14, 21, 26, 32, 35, 41, 44].

The design of a privacy-preserving RFID authentication protocols is desperate for an suitable security and privacy model in order to admit of a careful security analysis of the protocol. A large number of frameworks have been proposed to formalize security and privacy in the context of RFID system [5, 9, 10, 12, 19, 22, 24, 29, 48, 49]. The shortcomings of these frameworks are addressed in [11] and the Vaudenay's model [49] is one of the most evolved and well defined privacy model. Moreover, Paise et al. [37] extended the Vaudenay's privacy model (PV-model), where PV-model additionally offers reader authentication. Later, Armknecht et al. [3] showed that it is impossible to achieve both reader authentication and any reasonable notion of RFID privacy in the PV-Model (where the target tags are vulnerable to corruption). On the other hand, Habibi and Araf [20] claimed that the privacy definition and adversary goal presented by Armknecht et al. is completely different from the PV-Model and the highest achievable privacy level in the Armknecht et al.'s privacy model is *narrow weak* privacy.

In this paper, we address two privacy notions of Vaudenay's model: *forward* and *strong* privacy. A forward adversary is allowed to corrupt the tag and once corruption is performed, the system is considered destructed, and now it can use only information of the memory of the target tag. A strong adversary has no restriction on any interactions with the target tag. However, the following

attack game is not considered in the Vaudenay's privacy model. Assume that an RFID tag is still functional against a number of physical attacks (say k) on a target tag, after k^{th} corruption the tag is no longer usable. During the period of k corruptions, the adversary can interact with the tags and can still get its internal state correctly. In the Vaudenay's model, the privacy of such a scenario is not ensured. This is the starting point of our work, in which we define the security and privacy levels between weak and strong privacy.

The strongest achievable notion of privacy in the Vaudenay's model, which is *strong privacy*, entails expensive public-key cryptography. This requirement generally exceeds the computational capabilities of current cost-efficient RFID tags. In order to achieve the highest privacy levels using only low cost cryptography, Physically Unclonable Functions (PUFs) have been studied. In the literature, several PUF based authentication protocols have been proposed [18, 41, 45]. The security of these protocols rely on tamper-resistant structure of PUF devices which assumes that an attempt to measure physical parameters of PUF will definitely make it unusable. This assumption works only in the ideal world whereas in the real case the PUF devices may be usable up to a number of physical attacks. If the PUF is usable after the first successful physical attack, the security of such protocols would be questionable. Therefore, it is not simple to decide whether the security of the system should rely on the protocol or on the tamper resistance of the device. Indeed, ultimate care is required for designing privacy-preserver protocols that the security relies on the tamper resistance of a device. We study these types of PUFs and introduce a new PUF definition, k-resistant PUF, which provides resistance against physical attacks at most k times where the integer value of k depends on the capability of adversary and manufacturing quality of PUFs. We show that the use of k-PUF helps to resolve the above-mentioned privacy issues in the Vaudenay model.

Our Contributions. Our contributions are multiple. We first revisit the Vaudenay's model and introduce two new privacy notions, k-strong privacy and k-forward privacy. Namely, we group all privacy classes of Vaudenay's model into two generic privacy classes. With this methodology, we construct a new privacy class between strong and destructive privacy.

In order to achieve highest security levels with only low-cost primitives, we study Physically Unclonable Functions (PUFs). We note that the security of the system relies on the assumption that physically tampering a PUF will immediately destroy its physical structure and making it unusable. This is, actually, an assumption commonly used in the literature. However, in the real world, this assumption is not always correct because tamper resistance depends on the ability of the attacker and the quality of the manufacture and the design of the PUF circuit. The circuit may not be destroyed until some number of physical attacks

(say k). Moreover, the structure of the PUF might be destroyed when unexpected environmental changes such as voltage, temperature changes occur and this destruction makes the PUF unreliable [34]. Therefore, we introduce a new extended PUF definition what we called k-resistant PUF (k-PUF). These PUFs are resistant against at most k number of physical attacks. After the k-th attack, the structure of the k-PUF is destroyed and can no longer be evaluated correctly. Also, k-PUF functions are more reliable against the k number of unexpected changes.

To illustrate our new privacy model, we analyzed two recent PUF based authentication protocols and show their security and privacy levels in our model [26, 41]. We show that these protocols do not achieve k-strong privacy for $k > 1$.

Next, we propose an efficient unilateral RFID authentication protocol based on k-PUFs. We prove that our protocol achieves k-strong privacy with low-cost cryptographic primitives such as hash functions and PUFs. When we choose k to be zero, 0-strong privacy implies weak privacy in Vaudenay's model, and when k is infinite, ∞-strong privacy implies strong privacy in Vaudenay's model. Therefore, to the best our knowledge, this is the first attempt to achieve strong privacy of Vaudenay's model only using symmetric cryptographic primitives.

Finally, we adapt and extend our generic authentication protocol to a mutual authentication. We prove that this extended protocol achieves both k-strong privacy and reader authentication.

Outline of the paper. The organization of the paper is as follows: In Section 2, we first briefly describe PUF functions and its characteristics. Then we discuss the problem on the common PUF assumption and give our new PUF definition. Section 3 introduces our extended privacy model. Section 4 introduces two recent PUF based RFID protocols and analyze their security and privacy levels. In section 5, we propose a simple generic PUF based RFID authentication protocol and analyze it with the help of our model. In section 6, we prove that it is possible to provide both k-strong privacy and reader authentication in a RFID scheme. Section 7 concludes the paper.

2 Preliminaries

In this section, we emphasize the current PUF function problems and provide an overview of related work and our new PUF function definition.

2.1 Physical Unclonable Functions (PUFs)

A Physical Unclonable Function (PUF) is a disordered physical structure implementing a unique function that maps challenges to responses. These responses

depend on the nano-scale structural disorder of the PUF that is assumed to be unclonable or not even reproducible by the PUF's manufacturer. Namely, the PUF functions are embodied in a physical structure in a complex way upon several physical properties that the manufacturers cannot control, and they are easy to be computed, but difficult to be predicted, characterize and model the mappings.

The first attempt to exploit the physical properties of the devices for authentication purposes were done in [7, 42, 43]. Naccache and Fremanteau [36] later proposed an authentication mechanism for memory cards which uses these physical properties. The concept of PUFs is first introduced by Pappu [38, 40]. Their PUF functions were based on an optical principle of operation. In these PUFs, transparent tokens include randomly distributed scattering particles and are illuminated by a laser light with a specific angle, distance and wavelength. The resulted speckle patterns from multiple scattering of laser in an incoherent optical medium are used for unique and unpredictable identifier. The challenge of the PUF can be the angle of incidence, the local distance or the wavelength of the laser. The responses can be hash value of digitized image of the speckle pattern. Afterward, several papers considered various hardware structures of PUF [17, 23, 28, 33].

Besides, for a given challenge c, a typical PUF P may produce a slightly different response r ($r \leftarrow P(c)$) because the response depends on the physical characteristics that could be affected by environmental noises such as temperature, light and supply voltage variations. This obstacle can be eliminated by a small circuit, called Fuzzy Extractor and with help of additional help input w [15, 16]. Moreover, even though two PUFs are implemented on the same device with the same structure, they both give independent responses with overwhelming probability for the same given challenges. Armknecht et al. proposed a formal foundation for such security primitives based on PUFs in [4].

The usage of PUFs in the authentication mechanisms has led to an increase in the security of existing RFID systems. They provide a new way for cost-efficient privacy preserving authentications based on the unclonable physical properties. In [17], PUFs are shown how they can be used to establish a shared secret with a specific physical device. Namely, PUFs are embedded into a microchip. One of the first attempts to embody PUF functions into RFID based authentication protocols is proposed in [13, 39]. In these studies, a set of challenge/response is derived from the PUF for each tag. The challenge/response pairs are stored in a secure database. The RFID reader selects a random challenge from the database and broadcasts it to the environment. Then, the received responses of the tags are interpreted by simply looking up the database. The main obstacle of the scheme is that the challenge cannot be used anymore since

it results to replay attacks. Another obstacle is storing huge amount of challenge/response in the database.

Tuyls et al. [45] used PUF functions as secure key derivation mechanism since PUF behaves like a hidden pseudo-random functions. Whenever a key hidden by PUF is needed during an authentication, it is simply derived by evaluating the PUF on the chip. Tuyls et al. assumed that as the adversary tries to evaluate a PUF or an IC, for instance, by using the probes to measure the wire delays, the characteristics of that particular PUF are changed. Thus, the intrinsic structure of the PUFs yields resistance against tampering and this reduces the capability of an adversary to clone an RFID tag. Moreover, they also demonstrated that PUF circuit can easily be realized on a RFID chip with less than 1000 gates [45].

In [8], another way of using PUF within a privacy-preserving RFID authentication scheme was proposed. In this scheme, for each ID of tag, the database of the reader stores the vector $\{ID, P(ID), P^2(ID), \ldots, P^t(ID))\}$ where t is the threshold for authentication of a tag. Whenever the reader interrogates a tag, the tag evaluates its PUF with its identifier ID. The response is sent to the reader and the tag updates its ID with this response. The reader simply looks up the database, identifies the tag and removes the used response from the database. The main bottleneck of this protocol is that the system should store a huge amount of data for a large t. It also suffers from Denial of Service(DOS) attacks as the tag must be re-initialized after at most t sessions.

Sadeghi et al. [41] proposed a destructive private RFID authentication protocol based on PUF, which is similar to PUFs functions of [45]. Whenever a strong adversary performs a physical attack, such as side channel on PUFs of RFID tags, these PUF functions are destroyed and cannot be evaluated anymore. Later, Kardas et al. also introduced a new usage of PUF functions with a weaker assumption, where the adversary can reach all the internal state of the tags whenever she does a physical attack [26]. They also proposed a destructive private authentication protocol for RFID systems. Furthermore, recently, several new authentication mechanisms based on PUF functions have been proposed in order to enhance their security and privacy levels [1, 27, 30, 31, 50].

In this paper, we introduce a new PUF function definition (k-PUFs) that are resistant to at most number of k number of physical attacks. Contrary to the PUF of [26, 41, 45], after the k^{th} physical attack on the chip, the PUF inside the tag cannot be evaluated anymore because the structure of the PUF is destroyed with overwhelming probability. Similar to [26], we also assume that an adversary can reach to volatile and non-volatile memory of the tag in the case of physical attacks.

In this study, we prove that the protocol proposed in [41] achieves 0-strong (implies weak privacy in the Vaudenay model [49]) privacy in our model. Similarly, we prove that the protocol proposed in [26] achieves 1-strong privacy, which implies destructive privacy in the Vaudenay model.

2.2 Motivation and Problem Statement

Vaudenay defines several adversary classes which cover almost all of the privacy levels in his seminal work [49]. Nevertheless, the following privacy issues are not considered in the model. Suppose that an adversary corrupts a target tag k times where k is an integer. During (and after) these attacks, the tag is still functional and the adversary can still interact with it and the privacy of the tag is satisfied. However, after the $k+1$-th corruption, the privacy of the tag is not satisfied. The security and privacy of this scenario is not addressed in the Vaudenay's model. Note that when k goes to infinity, if the privacy of the tag is ensured against such an attack, then the strong privacy of Vaudenay's model is achieved. If k is equal to 1 and the privacy is still ensured, then the destructive privacy of Vaudenay's model is achieved. Similarly, if k is equal to 0, the weak privacy of Vaudenay's model is achieved. However, the privacy levels are not defined in the Vaudenay's model in case of $k \geq 2$. This is the starting point of our work, in which we define the security and privacy levels between weak and strong privacy notions for the first time in the literature.

We would like to highlight that the strong privacy of Vaudenay's model requires expensive public key cryptography. The driving motive behind this paper is achieving security levels of $k \geq 1$ using only low cost primitives. In this context, we have studied PUF functions and the common assumption on the PUFs. Then, we defined a new generic PUF function, which we call k-PUF. With this new k-PUF function, we show that the security levels described above can be achieved.

Now, let us look at the assumption. A large body of literature dedicated to PUFs assumes that any attempt to tampering the PUF circuit in order to observe its internal states will *most likely* alter these variables or even destroy the structure of the circuit [2, 18, 33, 45–47]. Here, *most likely* means that in practice *some* circuits may stay working as usual after *a number of* physical attacks. In fact, it depends on the manufacturing structure of the circuit and the ability of the attacker. Therefore, it is a strong assumption to postulate that any PUF circuit will destroy after a single attack. In what follows, we examine this problem and give a more general statement for realistic circumstances by weakening this assumption.

Let p be the destruction probability of a given PUF after a single physical attack. The value of p depends on the attacker's capability and chip's level of

strength against the physical attacks. The PUF circuit is assumed to be destructed if $p \geq P_{dest}$ where P_{dest} denotes a threshold value. If $p \geq P_{dest}$ after the first corruption then the circuit fulfills the best tamper-resistance property which corresponds to the ideal PUF case. More generally, let $P(X = i)$ denote the event of tag's evaluating not correctly after i-th corruption, then the probability of tag's not evaluating correctly at most k physical attack is

$$\sum_{i=1}^{k} P(X = i) = p \sum_{i=0}^{k-1} (1-p)^i = 1 - (1-p)^k$$

where $k \geq 1$, $k \in \mathbb{Z}$. Thus, the tag cannot evaluate correctly if the condition below is satisfied

$$1 - (1-p)^k \geq P_{dest} \Rightarrow k \geq \frac{\ln(1 - P_{dest})}{\ln(1-p)}.$$

Note that the basic case of $k = 1$ corresponds to the ideal PUF. In the next section, we generalize the definition of ideal PUF by extending it to a more realistic sense by allowing limited number of attempts to tamper without destruction (up to a level of k).

2.3 A New Definition: k-PUF

Let us denote $s \in_R S$ for choosing a value s uniformly at random from the set S. $y \in \{0,1\}^{\alpha}$ means y is any natural number such that y's bit length is at most α. For the case $\alpha = *$, there is no restriction on bit length of y; i.e., y can be any natural number.

A mapping $f : \{0,1\}^{\alpha} \rightarrow \{0,1\}^{\beta}$ means that f maps elements from $\{0,1\}^{\alpha}$ to $\{0,1\}^{\beta}$. $Pr(E)$ denotes the probability of event E occurring. $MSB_a\{k\}$ denotes the most significant a bits of binary representation of k.

We are now ready to present our new definition of PUF as follows:

Definition 1. *(k-resistant PUF (k-PUF)) Let $\kappa \in \mathbb{N}$ be a security parameter such that $\beta, \theta \in \mathbb{N}$ are polynomially bounded in κ. Define an evaluation function of k-resistant PUF (k-PUF) $P_k : \{0,1\}^{\beta} \rightarrow \{0,1\}^{\theta}$. Then, P_k has the following properties:*

- *Same inputs always give same output result, i.e, let $P_k(a_1) = b_1$ and $P_k(a_2) = b_2$, if $a_1 = a_2$ then $Pr(b_1 = b_2) = 1$.*
- *Any probabilistic polynomial time adversary has at most negligible success probability to distinguish between output of P_k and a random value.*
- *k-PUF is resistant against any physical attack at most k times (e.g., invasive attack). Namely, P_k cannot be evaluated correctly anymore after k physical attacks.*

2.4 Practicality of *k*-PUF

In this section, we are going to provide some intuition about how to create a *k*-PUF structure. The coating PUF modeled by Tuyls et al. in [47] has a self destructing capability control where an invasive attack would probably cause to destroy PUF structure. This control detects the attack whenever the level of noise caused by the attack in the output of the PUF exceeds some threshold; so, if not detected, the PUF will not be destructed. This makes coating PUF non-ideal in real life. If the PUF is destroyed after the first attack, this PUF could be considered as a natural example of *k*-PUF where $k = 1$. Our construction of *k*-PUF is inspired by the above-mentioned observation on [47] is described as follows.

The coating PUF can be built as top layer of an Integrated Circuit (IC) by applying circuit paths and laid out in a comb shape. These paths will be encased by a material that is randomly doped with dielectric particles of different size and dielectric strength. Each pair of circuit paths forms a capacitor with random capacitance, which again is unlikely to be controllable by the manufacturer. Random capacitor allows PUF to give a response with noise for a given challenge. In order to clean the noise from the response (i.e., error correction), helper data algorithm/fuzzy extractor is used for the reconstruction of secret keys [15, 16]. Tuyls et al. [34, 47] show that coating PUFs are resistant to an adversary who has the following optical and invasive methods.

- Optical inspection equipment to look into memory cells.
- Etching methods (e.g. chemical) to remove protective layers.
- Focused Ion Beam (FIB) to make holes in protective layers and allow for probing (of e.g. memory).

Since the coating is opaque, it is not so possible to look into the digital memory optically without damaging the coating [47]. Tuyls et al. [47] presented an advanced attack on the coating PUF where an adversary uses FIB to make an hole in the coating. The adversary uses her micro-probe(s) to retrieve the key bits during the reconstruction phase of the key. The use of FIB and micro-probes might give damage on the PUF. This damage causes the extracted key bits with more noise. It is stated that during reconstruction phase, the extracted keys are checked with a signature. If the level of the noise is very high, then the computed signature would not be valid and the PUF would be destroyed by the controller. However, the adversary gets key bits with some noise during the attack. For example, if the PUF produces key length of 128-bits then the attacker can recover the complete bits with 2^{51} trials (we refer to [47] for further details.). We highlight that the level of noise in the PUF response is not

only affected by the physical attacks but also affected by the unexpected significant environmental changes such as temperature, voltage changes. Thus, this environmental situation makes PUF unreliable.

The proposed k-PUF design is described as follows. We employ an additional counter, which is initialized to zero in the PUF control. The counter enables the PUF to limit the number of invasive attacks applied to the circuit. For example, a similar attack described above is performed, the PUF's control would detect the attack and it increments the counter by one because the attack causes the circuit to produce key bits with higher noise and Fuzzy Extractor is not able to produce a valid key and the signature would not be correct. When the counter is greater than or equal to $k-2$, the control in the PUF immediately destroys the circuit. In the worst case, in each attack, the adversary is assumed to recover a different key. In total she can gain at most $k-1$ different keys but in the k^{th} attack the structure of the PUF is destroyed. Hence the security of the our PUF is still protected. Moreover, our PUF functions are also vulnerable to environmental changes but they are reliable against number of $k-1$ unexpected changes.

3 Our Extended Security and Privacy Model

In this section, we first revisit the well-known definitions based on Vaudenay's privacy model [49]. Then, we extend this model by introducing a new class of adversary, namely, k-strong adversary where an adversary has the ability to corrupt a tag at most k times. After that, we introduce our k-strong privacy, which is extension of privacy definition of Vaudenay's model

3.1 Vaudenay's Privacy Model

In order to clearly describe our privacy definition, we first define the system procedures, adversary oracles and privacy experiments following the standard definitions of [49] for an RFID system. For the sake of simplicity, the reader and the server are assumed to be a single entity which are connected through a secure channel.

System Procedure An RFID scheme is defined by the following procedures.

- SETUPREADER(1^{ℓ}) : This algorithm first produces a public-private key pair (K_P, K_S) where ℓ is the security parameter, then initializes its database $\mathscr{DB}$.
- SETUPTAG$_{K_P}$(ID): This algorithm generates a tag secret K and the initial state S of a tag with identifier ID. If this tag is legitimate, the pair (ID,K) is inserted into the database.

– IDENT: An interaction protocol between a tag and the reader to complete the authentication transcript.

Adversary Oracles An adversary $\mathscr{A}$ can interact with the RFID system by the help of following generic oracles. First of all, $\mathscr{A}$ setups a new tag of identifier $\mathrm{ID}_{\mathscr{T}}$.

– CREATETAG($\mathrm{ID}_{\mathscr{T}}$) : It creates a free tag $\mathscr{T}$ with a unique identifier $\mathrm{ID}_{\mathscr{T}}$ by using $\mathbf{SetupTag}_{K_p}$. It also inserts $\mathscr{T}$ into $\mathscr{DB}$.
– LAUNCH()$\rightarrow \pi$: It makes the reader $\mathscr{R}$ start a new *Ident* protocol transcript π.
– SENDREADER(m,π)$\rightarrow m'$: This sends the message m to the reader $\mathscr{R}$ in the protocol transcript π and outputs the response m'.
– SENDTAG(m,π)$\rightarrow m'$: This sends the message m to $\mathscr{T}$ and outputs the response m'. Also, $\mathscr{A}$ asks for the reader's result of the protocol transcript π.
– DRAWTAG(distr)$\rightarrow(\mathscr{T}_1,b1,\ldots,\mathscr{T}_s,b_s)$: It randomly selects s free tags among all existing ones with distribution probability of distr. The oracle assigns a new pseudonym, $\mathscr{T}_i$ for each tag and changes their status to drawn. This oracle also returns bit b_i of tag i whether it is legitimate or not. The relations ($\mathscr{T}_i$,$\mathrm{ID}_{\mathscr{T}_i}$) are stored in a hidden table *Tab*. This hidden table is not seen by the adversary until the last step of the privacy game. Finally, the oracle returns all the generated tags in any order.
– FREE($\mathscr{T}$) : This oracle changes status of tag $\mathscr{T}$ from drawn to free, then $\mathscr{A}$ is no longer interact with $\mathscr{T}$.
– CORRUPT($vtag$)$\rightarrow S$: It returns volatile and non-volatile memory of the tag.
– RESULT(π)$\rightarrow x$: When π completes, returns $x=1$ if the tag is identified, $x=0$ otherwise.

Privacy Classes The Vaudenay model introduces five privacy classes of polynomial-time bounded adversary, determined by $\mathscr{A}$'s access to RESULT or CORRUPT oracles. These classes are defined as follows.

Definition 2. *(Adversary Classes [49]) An adversary $\mathscr{A}$ is a p.p.t. algorithm which has arbitrary number of accesses to the oracles described-above.* ***Weak*** *$\mathscr{A}$ uses all oracles except* CORRUPT *oracle.* ***Forward*** *$\mathscr{A}$ can only use* CORRUPT *oracle after her first call to this oracle.* ***Destructive*** *$\mathscr{A}$ cannot use any oracle against a tag after using* CORRUPT *oracle.* ***Strong*** *$\mathscr{A}$ uses all oracles described-above without any restrictions. Finally,* ***Narrow*** *$\mathscr{A}$ has no access to* RESULT *oracle.*

It is clearly seen that the following relation holds for these classes: WEAK$\subseteq$ FORWARD$\subseteq$ DESTRUCTIVE $\subseteq$STRONG.

Notion of Security and Privacy We are now ready to define security and privacy definitions of the Vaudenay model. The security definition given by the Vaudenay model considers attacks in which the adversary aims to impersonate or forge a legitimate tag but not security against cloning and availability.

Definition 3. *(Tag Authentication [49].) An RFID system achieves tag authentication if for every strong adversary, $\mathscr{A}^P$, where P is a class of adversary defined in Definition 2, is at most negligible.*

The privacy definition of Vaudenay is flexible and depends on the adversary classes in Definition 2, so it covers different notion of privacy. The privacy is simply based on the existence of a blinder $\mathscr{B}$, which is able to simulate each tag $\mathscr{T}$, and the reader $\mathscr{R}$ without knowing their secrets such that the adversary cannot distinguish whether it interacts with the real or simulated oracles. In the privacy game of the Vaudenay's model, a set of tags, a protocol transcript π, and the reader participate. The adversary can interact with tags and the reader by calling polynomial-bounded number of times any oracle according to her privacy class. The definition of the blinder is described as follows.

Definition 4. *(Blinder, trivial adversary [49]). A blinder $\mathscr{B}$ is a simulator which simulates* LAUNCH, SENDREADER, SENDTAG, *and* RESULT *oracles without having access to the real secret keys and the database. When a blinded adversary $\mathscr{A}^{\mathscr{B}}$ uses these oracles, she is answered through the blinder $\mathscr{B}$. An adversary $\mathscr{A}$ is trivial if there exists a blinded adversary $\mathscr{A}^{\mathscr{B}}$ such that Prob$[\mathscr{A}$ wins$]-$ Prob$[\mathscr{A}^{\mathscr{B}}$ wins$]$ is at most negligible.*

Remark 1. The blinder $\mathscr{B}$ is consistent and acts like a real reader in a way that if a protocol transcript's inputs are derived as a result of usage of oracles to $\mathscr{B}$. The answer given by $\mathscr{B}$ to the RESULT oracle on this protocol transcript is 1. If all inputs of a protocol transcript are not derived as a result of the usage of oracles to $\mathscr{B}$, then the answer given by $\mathscr{B}$ to the RESULT oracle on this protocol transcript depends on the appearance probability of missing inputs on protocol transcript. Besides, $\mathscr{B}$ keeps all its answers to the oracles used by $\mathscr{A}$ in its database and answers the new oracles depending on its database.

We now explicitly describe Vaudenay's privacy game by the following experiment $Exp^{prv-b}_{\mathscr{A}_{prv}}$:

Let ℓ be a given security parameter, $b \in_R \{0,1\}$ and $\mathscr{A}_{prv}$ be an adversary given in Definition 2. There two phases in the experiment: learning phase and

challenge phase. In the learning phase, $\mathscr{R}$ is first set with $(sk_{\mathscr{R}}, pk_{\mathscr{R}}, \mathscr{DB}) \leftarrow$SETUPREADER$(1^{\ell})$. Both A_{prv} and $\mathscr{B}$ also get the public key $pk_{\mathscr{R}}$. Then, $\mathscr{A}_{prv}$ arbitrarily inquiries all oracles defined in Section 3.1 but is limited to use the oracles according to her privacy class (See Definition 2). Whenever $b = 0$, A_{prv} simply calls real oracles. However, when $b = 1$, $\mathscr{B}$ receives and answers all queries to LAUNCH, SENDREADER, SENDTAG, and RESULT oracles. At this moment, $\mathscr{B}$ sees all oracles that are simulated by $\mathscr{B}$, but are made by A_{prv} ($\mathscr{B}$ sees what $\mathscr{A}_{prv}$ sees). These steps are done a polynomial number of times. In the challenge phase, $\mathscr{A}_{prv}$ can no longer interact with the oracles but the hidden table *Tab* of DRAWTAG oracle is revealed to her. Finally, $\mathscr{A}_{prv}$ is expected to return an answer bit b', which is denoted by $Exp^{prv-b}_{\mathscr{A}_{prv}} = b'$. The formal definition of privacy is given as follows.

Definition 5. *(Privacy[49]). Let C be an adversary class defined as in Definition 2. An RFID system is C-private if* $\forall \mathscr{A}_{prv} \in C$*, there exists a p.p.t. algorithm* $\mathscr{B}$ *such that the advantage*

$$Adv^{prv}_{\mathscr{A}_{prv}} = |Pr[Exp^{prv-0}_{\mathscr{A}_{prv}} = 1] - Pr[Exp^{prv-1}_{\mathscr{A}_{prv}} = 1]|$$

of $\mathscr{A}_{prv}$ *is at most negligible.* $\mathscr{B}$ *is the blinder, which simulates the* LAUNCH, SENDREADER, SENDTAG, *and* RESULT *oracles without having access to* $sk_{\mathscr{R}}$ *and* $\mathscr{DB}$*. Also, all oracles done by* A_{prv} *are sent to* $\mathscr{B}$

3.2 Our Extended Privacy Experiment

We first introduce two new notion of adversary classes: *k*-strong adversary and *k*-forward adversary. The *k* is defined as an integer for privacy level. *k*-strong adversary covers three privacy classes of Vaudenay's model. These are WEAK, DESTRUCTIVE and STRONG adversaries. We finally give the formal definitions of *k*-strong and *k*-forward privacy according to these two new adversary classes.

Definition 6. *(k-Strong adversary). Let a RFID system* $\mathscr{S}$ *and a target tag* $\mathscr{T}$ *be given. Let also k be defined as a privacy level, which is an integer in* $\mathscr{Z}^+ \cup \{0\}$*. k-strong adversary* $\mathscr{A}$ *has the following capabilities:*

- $\mathscr{A}$ *can use* CORRUPT *oracle on* $\mathscr{T}$ *at most k times.*
- $\mathscr{A}$ *cannot use any other oracles after* $\mathscr{A}$ *made its* k^{th} *corruption on the target tag.*
- $\mathscr{A}$ *can use all oracles if less than k* CORRUPT *oracles are used.*

Definition 7. *(k-Forward Adversary). Let an RFID system* $\mathscr{S}$ *and a target tag* $\mathscr{T}$ *be given. Let also k be defined as a privacy level which is an integer in* $\mathscr{Z}^+ \cup \{0\}$*. k-forward adversary* $\mathscr{A}$ *has the following capabilities:*

– $\mathscr{A}$ *can use any other oracles until* k^{th} CORRUPT *oracle on* $\mathscr{T}$.
– $\mathscr{A}$ *can use only* CORRUPT *oracle after* k^{th} CORRUPT *oracle on* $\mathscr{T}$.

Remark 2. For the case $k = 0$, $\mathscr{A}$ can not use CORRUPT oracle on any tag, but $\mathscr{A}$ can use all oracles except CORRUPT oracle without any limitation.

Next, we are now ready to define our privacy definition according to our new adversary classes. Note that this definition is almost similar to the Vaudenay's privacy game except its adversary classes.

Definition 8. *(k-Strong Privacy). Let* $\mathscr{A}_{prv}$ *be a k-strong adversary defined as in Definition 6. An RFID system is k-Strong private if* $\forall \mathscr{A}_{prv}$, $\exists$ *a p.p.t. algorithm* $\mathscr{B}$ *such that the advantage*

$$Adv^{prv}_{\mathscr{A}_{prv}} = |Pr[Exp^{prv-0}_{\mathscr{A}_{prv}} = 1] - Pr[Exp^{prv-1}_{\mathscr{A}_{prv}} = 1]|$$

of $\mathscr{A}_{prv}$ *is at most negligible.* $\mathscr{B}$ *is the blinder, which simulates the* LAUNCH,SENDREADER, SENDTAG, *and* RESULT *oracles without having access to* $sk_{\mathscr{R}}$ *and* $\mathscr{DB}$. *Also, all oracles done by* A_{prv} *are sent to* $\mathscr{B}$

Tag $\mathscr{T}_{ID}$ S		Reader $\mathscr{R}$ **DB =** $\{(\mathbf{ID}_1, \mathbf{K}_1), \ldots, (\mathbf{K}_n, \mathbf{ID}_n)\}$
$b \in_R \{0,1\}^\alpha$	$\xleftarrow{a}$	$a \in_R \{0,1\}^\alpha$
$K \leftarrow P(S)$		
$c \leftarrow F_K(a,b)$		
	$\xrightarrow{b,c}$	**If** $\exists$(ID,K) $\in \mathscr{DB}$
delete K, a, b, c		**s.t.** $c \stackrel{?}{=} F_K(a,b)$ **then**
		return ID
		else return $\perp$
		endif

Fig. 1: Sadeghi et al.'s authentication protocol [41].

Theorem 1. *When $k = 0$, 0-strong privacy implies* WEAK *privacy. When $k = 1$, 1-strong privacy implies* DESTRUCTIVE *privacy. When* $\lim_{k\to\infty}$*, k-strong privacy implies* STRONG *privacy.*

Proof. Let us start with the trivial cases. By remark 2, when $k = 0$, by definition, 0-strong privacy is equivalent to WEAK privacy. Moreover, when $k = 1$, by definition 2, 1-strong adversary cannot use any other oracles after the first CORRUPT oracle usage and the adversary can apply any oracle before the first CORRUPT oracle usage. Hence, this definition is equivalent to destructive adversary in Vaudenay's model.

For the $\lim_{k\to\infty}$, k-strong privacy case, we are going to prove the following claim.

Claim. $\lim_{k\to\infty}$ k-strong privacy implies that the tag privacy protected against any number of CORRUPT oracle usage.

Assume to the contrary the claim is wrong, then there exists integer k_0 such that after k_0 number of CORRUPT oracles are applied, the privacy of the tag is violated. However, by definition, $(k_0+1)-$strong privacy implies that the tag privacy is protected until $(k_0+1)^{th}$ CORRUPT oracle usage. Thus $\lim_{k\to\infty}$ k-strong privacy$\subset (k_0+1)-$strong privacy.

Claim. $(k_0+2)-$strong privacy$\subset \lim_{k\to\infty}$ k-strong privacy.

In fact, the problem is equivalent to the classical calculus problem, which is whether or not $(k_0+2) < \lim_{k\to\infty} k$. By undergraduate calculus, we know that $\lim_{k\to\infty} k$=∞, so the claim holds.

Therefore, we have $\lim_{k\to\infty}$ k-strong privacy $\subset (k_0+1)-th$ strong privacy $\subset$ $(k_0+2)-$strong privacy *subset* $\lim_{k\to\infty}$ k-strong privacy. This is a contradiction. Hence, the proposed claim holds.

Note that the tag's standing against any number of CORRUPT oracle usage corresponds to strong privacy in Vaudenay's model. Hence, $\lim_{k\to\infty}$, k-strong privacy in our model corresponds to strong privacy in Vaudenay's model.

Remark 3. Theoretically, one can claim that a tag can live forever regardless of how many times it has corrupted. However, in practice, it is impossible to create a tag standing against infinitely many number of corruptions physically. Hence, $\lim_{k\to\infty}$ k-strong privacy is more plausible to define for real world. For example, if a tag lives until t^{th} corruption, and until its destruction it gives no clue about privacy, then for this tag, $t-$strong privacy is equivalent to the strong privacy. However, this t value changes tag to tag so it is impossible to say that t-strong privacy is equivalent to strong privacy in Vaudenay's model for any $t \in \{Z\} - \infty$. This theoretical approach covers this need.

Moreover, one can claim that, if a tag lives until t corruption and until its destruction, it gives no clue about privacy, this tag also has $p-$strong privacy where $p >= t$. Therefore, according to this perspective, for all the tags in the system, the system satisfies $\lim_{k\to\infty}$ k-strong privacy.

There can be an adversary $\mathscr{A}$ such that $\mathscr{A}$ can corrupt a target tag k-times and $\mathscr{A}$ can interact with any oracle until its k^{th} corruption. In such case, the system should be private. Such a privacy is not handled in the Vaudenay's model; however, k-strong privacy captures this concern.

On the other hand, k-forward privacy is similarly defined if an adversary $\mathscr{A}_{prv}$ is defined according to the Definition 7.

Hence, the new relations between our privacy classes holds as follows: 0-FORWARD$\subseteq$0-STRONG $\subseteq \ldots \subseteq$K-FORWARD$\subseteq$K-STRONG.

4 Analysis of Two Recent Authentication Protocols in Our Extended Model

In this section, we analyze the security and privacy level of two recent PUF based authentication protocols according to our model.

4.1 Sadeghi et al.'s Authentication Protocol

Sadeghi et al. [41] use an ideal PUF (which corresponds to 1-PUF according to our model) in their proposed protocol. They assumed that whenever a strong adversary corrupts a tag, the adversary cannot reach to its temporary state and the structure of PUF would be destroyed. However, we assume that a PUF cannot be destroyed immediately after the first corruption. Tags may have a limited number of resistance against any strong attacks. We briefly describe their protocol, then analyze the protocol according to our model.

Let $\ell \in \mathbb{N}$ be a security parameter, $\alpha, \beta, \gamma, \kappa$ be polynomial bounded in ℓ. Let $F : \{0,1\}^{\kappa} \times \{0,1\}^{2\alpha} \to \{0,1\}^{\beta}$ be a pseudo-random function. Each tag $\mathscr{T}$ is equipped with an ideal unique PUF function $P : \{0,1\}^{\gamma} \to \{0,1\}^{\kappa}$ and stores a random state $S \in_R \{0,1\}^{\gamma}$. On the other hand, the reader's $\mathscr{R}$ database $\mathscr{DB}$ stores a set of records (ID,K) for each tag in the system, where $K = P(S)$. The authentication protocol steps are summarized in Figure 1.

In the protocol, $\mathscr{R}$ first sends a random challenge $a \in_R \{0,1\}^{\alpha}$ to a tag $\mathscr{T}$. Once $\mathscr{T}$ receives the challenge, $\mathscr{T}$ picks another random challenge $b \in_R \{0,1\}^{\alpha}$. $\mathscr{T}$ reconstructs the secret key K and computes response $c = F_K(a,b)$ sends b and c to $\mathscr{R}$. Then, $\mathscr{T}$ erases a, b, c, K from its volatile memory. Upon $\mathscr{R}$ receives b, c from $\mathscr{T}$, $\mathscr{R}$ recomputes $c' = F_K(a,b)$ for each record (K,S) in $\mathscr{DB}$

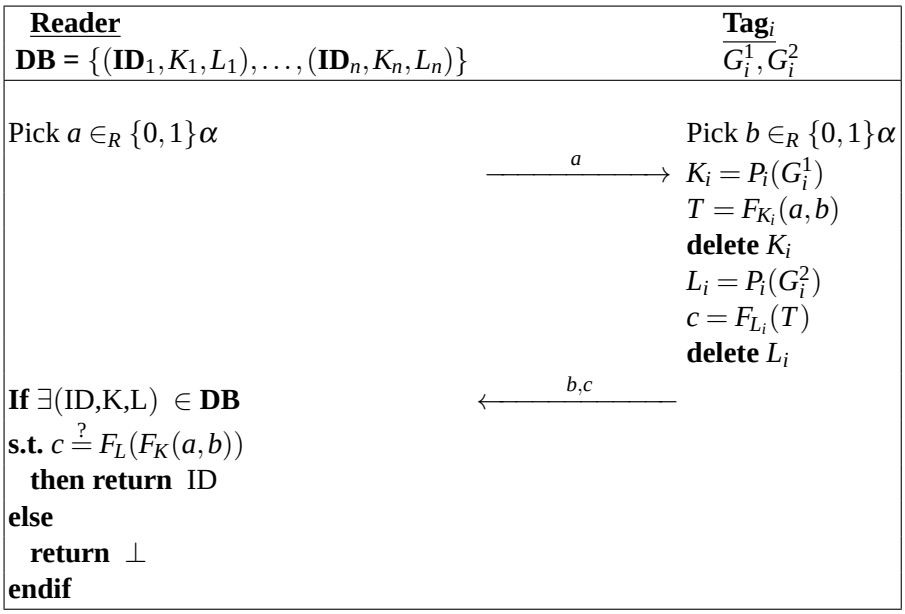

Fig. 2: Kardas et al.'s authentication protocol[26].

until $\mathscr{R}$ finds a match ($c' = c$). If a match is found, $\mathscr{R}$ sends the ID, otherwise sends $\perp$.

Remark 4. Note that output of a true random number generator and output of hash function in the random oracle model are indistinguishable. Therefore in practicality, outputs of pseudo-random functions and hash functions works similarly.

Theorem 2. *The RFID protocol demonstrated in Figure 1 achieves* 0*-strong privacy.*

Proof. Without loss of generality assume that there are one reader $\mathscr{R}$ and one tag in the system (note that it is shown in [25] that a system with many tags and one reader has at most negligible advantage). First of all, we show that, if adversary is not allowed to use CORRUPT oracle, then the adversary cannot distinguish $\mathscr{R}$ from the blinder $\mathscr{B}$. Then, we show that if the adversary is allowed to use CORRUPT oracle at least once, then the adversary can distinguish $\mathscr{R}$ from $\mathscr{B}$.

In the first case, the system runs m times by $\mathscr{R}$ or $\mathscr{B}$. During the runs, the adversary guesses number of t values for K and checks the corresponding guessed key values at any of previous runs. Note that both m and t are polynomially bounded in ℓ. In order to calculate the maximum success probability, we have

to consider two cases: (i) the probability that the adversary guesses the correct value of the key is $\frac{t}{2^\kappa}$. (ii) the probability that the adversary determines whether c is correct or not is $1-(1-(\frac{1}{2^\beta}))^m$. Since the values m and t are polynomially bounded the corresponding RFID scheme satisfies 0-strong privacy.

Let the adversary apply CORRUPT oracle at least once. Then, the adversary learns the value of K. For the consecutive protocol run, after getting values of a, b and c, the adversary computes the real value of c by using a, b and K and compares it with the given c value. The probability of distinguishing the real oracle from the blinder for only one protocol run is $1-\frac{1}{2^\beta}$. If the adversary observes more protocol runs, her success probability increases. Since the advantage is non negligible, in fact close to 1, the system does not achieve k-strong privacy for $k \geq 1$.

4.2 Kardas et al.'s Authentication Protocol

Kardas et al. [26] also proposed another PUF based authentication protocol and applied it into a distance bounding protocol and showed its security enhancements. Similar to Sadeghi et al.'s model, they also assume that whenever a strong adversary corrupts a tag, the PUF in the tag is destroyed; however, the adversary can reach its volatile memory only once. Their assumptions are weaker than Sadeghi et al.'s adversary model. In the following, we show that their protocol achieves 1-strong privacy according to our adversarial model. In this section, we first simplify Kardas et al.'s protocol without changing the core of the protocol. Then, we analyze its privacy level in our model. The authentication protocol steps are summarized in Figure 2.

Let $F : \{0,1\}^\ell \times \{0,1\}^{2\ell} \rightarrow \{0,1\}^{2\ell}$ be a one-way pseudo random function and $P_i : \{0,1\}^k \rightarrow \{0,1\}^\ell$ be an ideal PUF (1-PUF) function for tag $\mathscr{T}_i$. Each tag stores two random states $G'1_i, G_i^2 \in_R \{0,1\}^k$. On the other hand, the reader's database $\mathscr{DB}$ stores a set of records $(ID_i,\ K_i,\ L_i)$ for each tag $\mathscr{T}_i$ in the system, where $K_i = P_i(G_i^1)$ and $L_i = P_i(G_i^2)$. The authentication protocol is summarized in Figure 2.

The protocol starts with $\mathscr{R}$ sends a random challenge $a \in_R \{0,1\}^\alpha$ to a tag $\mathscr{T}_i$. Whenever $\mathscr{T}_i$ receives this challenge, it chooses another random challenge $b \in_R \{0,1\}^\alpha$. $\mathscr{T}_i$ reconstructs the secret key K_i and computes $T = F_K(a,b)$. Then, it deletes the K_i from its volatile memory. After that, $\mathscr{T}_i$ reconstructs the secret L_i by re-evaluating the PUF with G_i^2 ($L_i = P_i(G_i^2)$), calculates the response $c = F_{L_i}(T)$, and erases L_i from its volatile memory. $\mathscr{T}_i$ sends c along with b to $\mathscr{R}$. Once $\mathscr{R}$ receives b, c from $\mathscr{T}_i$, it recomputes $c' = F_{L_i}(F_{L_i}(a,b))$ for each record (ID_i, K_i, L_i) in $\mathscr{DB}$ until $\mathscr{R}$ a match ($c' = c$) is found. If a match is found, $\mathscr{R}$ sends the ID, otherwise sends $\perp$.

Theorem 3. *The RFID protocol demonstrated in Figure 1 achieves* 1*-strong privacy.*

Proof. Let there be one tag and one reader in the system [25]. We consider two cases. In the first case, the adversary is allowed to apply CORRUPT oracle at most once in order to maximize her success probability. As a second case, we investigate privacy issue when the adversary is allowed to use CORRUPT oracle more than once.

After the adversary applies the CORRUPT oracle, either the value of K or L is learned, but not both at the same time since the PUF P_i is 1-PUF, which means its function is destroyed after the 1*st* CORRUPT oracle usage. Similar to the calculations done in the proof of Theorem 2, if the system is run m times by blinder or the reader and the adversary guesses number of t values for the unrevealed key value (K or L). Then the maximum advantage that the adversary gets in distinguishing the reader from the blinder is $\frac{t}{2^\kappa} + 1 - (1 - (\frac{1}{2^\beta}))^m$. Since m and t values are polynomially bounded, then the system achieves 1-strong privacy.

If the adversary applies corrupt oracle more than once, then both K and L are revealed in the worst case scenario. Similar to the calculations done in the proof of Theorem 2, the advantage that adversary has in order to distinguish the reader from the blinder is $1 - \frac{1}{2^\beta}$, which is non-negligible. Thus, the system does not achieve k-strong privacy for $k \geq 2$.

5 *k*-Strong Private Authentication Protocol

Let κ be the security parameter of the system. Let $P_i : \{0,1\}^\beta \rightarrow \{0,1\}^\theta$ be a k-PUF of the i^{th} legitimate prover $\mathscr{P}_i$ where θ is polynomially bounded in κ. Let $\mathscr{H} : \{0,1\}^* \rightarrow \{0,1\}^\gamma$ be one-way collision resistant hash function where where γ is polynomially bounded in κ. The credentials database $\mathscr{DB}$ of the reader $\mathscr{R}$ stores the following tag related information $((K_1^1,\ldots,K_1^{k+1},ID_1),\ldots,(K_n^1,\ldots,K_n^{k+1},ID_n)$ for $j = 1,\ldots,k+1$, $K^j = P_i(G_i \oplus j)$ for random states $G_i \in_R \{0,1\}^\beta$ where β is polynomially bounded in κ. Our unilateral authentication protocol depicted in Figure 3 works as follows.

- First of all, $\mathscr{R}$ generates a nonce $a \in_R \{0,1\}^\alpha$ and sends it to $\mathscr{T}_i$.
- Upon receiving a, $\mathscr{T}_i$ generates a nonce $b \in_R \{0,1\}^\alpha$ and computes $H = \mathscr{H}(a,b)$. $\mathscr{T}_i$ reconstructs $K^j = P_i(G_i \oplus j)$ and computes $H = \mathscr{H}(K^j,H)$, then immediately deletes K^j from the memory where $j = 1,\ldots,k+1$. The final value of H is assigned to c and $\mathscr{T}_i$ sends c along with b to the verifier.
- Upon receiving b and c, for each record $(K^1,\ldots,K^{k+1},ID)$ in $\mathscr{DB}$, $\mathscr{R}$ does following steps. $\mathscr{R}$ first computes $H = \mathscr{H}(a,b)$, then updates $H = \mathscr{H}(K^j,H)$

Reader		**Tag$_i$**
$\mathscr{DB}$ = $\{(K_1^1,\ldots,K_1^k,K_1^{k+1}, \mathbf{ID}_1),$ $\ldots,(K_n^1,\ldots,K_n^k,K_n^{k+1}, \mathbf{ID}_n)\}$		G_i, $\mathbf{ID}_i$
1. Pick $a \in_R \{0,1\}^\alpha$		Pick $b \in_R \{0,1\}^\alpha$
2.	$\xrightarrow{a}$	$H = \mathscr{H}(a,b)$
3.		**for** $j = 1$ **to** $k+1$
4.		$K^j = P_i(G_i \oplus j)$
5.		$H = \mathscr{H}(K^j,H)$
6.		**delete** K^j
7.		**endfor**
8.		$c = H$
9. **If** $\exists(K^1,\ldots,K^{k+1},ID) \in \mathscr{DB}$	$\xleftarrow{b,c}$	Send b,c
10. **s.t.**		
11. $H = \mathscr{H}(a,b)$		
12. **for** $j = 1$ **to** $k+1$		
13. $H = \mathscr{H}(K^j,H)$		
14. **endfor**		
15. **and** $H = c$ **then**		
16. **return ID**		
17. **else return** $\perp$		
18. **endif**		

Fig. 3: A Generic PUF based Authentication Protocol.

$\forall j = 1,\ldots,k+1$. The last H value is assigned to b'. If a match ($c' = c$) is found, the authentication succeeded. Otherwise, $\mathscr{R}$ does these steps with another record in $\mathscr{DB}$. If no match is found, the authentication aborts.

5.1 Security Analysis

Throughout the paper, we utilize the following rule. Let $B = \{1,\ldots,k+1\}$ be a set and $B_i = B/\{i\}$, where $i \in \{1,\ldots,k+1\}$. When it is said that CORRUPT oracle applied by B_i, we mean that the adversary captures all key values except the value of i^{th} key K^i. Moreover, throughout all proofs of this section, we assume that a tag is destructed at k^{th} CORRUPT oracle usage. This assumption does not restricts role of the adversary whereas this assumption gives the adversary the opportunity to take advantage of performing maximum number of oracles to any tag.

Lemma 1. *Let $\mathscr{A}_d$ be a k-strong adversary, $\mathscr{T}$ be a target tag and $B = \{1,\ldots,k+1\}$ be a set. Let B_i be $B/\{i\}$, where $i \in \{1,\ldots,k+1\}$. Then, the advantage that $\mathscr{A}_d$ obtains by applying* CORRUPT *oracle on tag $\mathscr{T}$ by the rules of B_i (not getting K_i) and the advantage that the adversary gets by applying* CORRUPT *oracle on tag $\mathscr{T}$ by the rules of B_j with $i \neq j$ are equal.*

Proof. Note that a set with $k+1$ elements has $k+1$ subsets having k elements. Thus, we can choose such two subsets (B_i, B_j) in $\frac{k(k-1)}{2}$ ways. Let us fix two integers i_0 and j_0 with $i_0 \neq j_0$ and $i_0, j_0 \in \{1,\ldots,k+1\}$.

Let m and n be polynomially bounded positive integers in κ. If $\mathscr{A}_d$ applies CORRUPT oracle on tag $\mathscr{T}$ by rules of B_{i_0}, then after k^{th} CORRUPT oracle usage, in the worst case, $\mathscr{A}_d$ has the knowledge of $K^1,\ldots,K^{i_0-1},K^{i_0+1},\ldots,K^{k+1}$. If $\mathscr{A}_d$ observes number of m protocol runs until k^{th} CORRUPT oracle usage, $\mathscr{A}_d$ also has knowledge of $(a_1,b_1,c_1),\ldots,(a_m,b_m,c_m)$. Then, $\mathscr{A}_d$ can compute c_{m+1} value in three cases:

- If a_{m+1} is equal to any of a_l values for $l \in \{1,\ldots,m\}$, then with 1 probability, the adversary figures out the value of c_{m+1} by choosing $b_{m+1} = b_l$.
- If this is not the case, $\mathscr{A}_d$ guesses number of n values of K^{i_0} and checks her guesses in any of the previous runs.
- In the case of failure, eventually the adversary has to guess the value of K^{k+1} or K^{i_0} for the corresponding protocol run.

Thus, the success probability of $\mathscr{A}_d$ is $\frac{m}{2^\alpha} + \frac{2^\alpha - m}{2^\alpha}\left[\frac{n}{2^\theta} + \frac{2^\theta - n}{2^\theta}\left(\frac{1}{2^\gamma} + \frac{1}{2^\theta - n}\right)\right]$. Similarly, if the CORRUPT oracle usage applied by the rules of the set B_{j_0}, one deduces that $\mathscr{A}_d$ gets the same success probability. The result follows by the fact that i_0 and j_0 are chosen arbitrarily.

From now on, when it is said that a tag is corrupted, it should be understood that it is corrupted by rules of $B_{k+1} = B/\{k+1\} = \{1,\ldots,k\}$.

Lemma 2. *Let $\mathscr{A}_d$ be a k-strong adversary and $\mathscr{T}_t$ be the target tag. Then $\mathscr{A}_d$'s analyzing the system with many tags including $\mathscr{T}_t$ gives him at most negligible advantage over her analyzing the system with only $\mathscr{T}_t$.*

Proof. Assume that there are one reader and n tags in the system, where n is polynomially bounded in κ. For every $i \in \{1,\ldots,n\}$, the reader and tag $\mathscr{T}_i$ realize the number of m_i protocol runs before k^{th} corruption. Note that our aim is to observe the adversarial advantage difference between the analyzing the systems with multiple tags and single tag. Thus, we have to figure out how much $\mathscr{A}_d$ gets advantage by guessing the value of c_{m_t+1} after corrupting $\mathscr{T}_i$ and observing the protocol runs realized by $\mathscr{T}_i$, $i \in \{1,\ldots,t-1,t+1,\ldots,n\}$. Since the value of G_i and the PUF function P_i differ from tag to tag, the only advantage of $\mathscr{A}_d$ is to find relations among the keys or the resulting c values. By letting $m = \max\{m_1,\ldots,m_{t-1},m_{t+1},\ldots,m_n\}$, the total advantage is at most $km(n-1)\frac{1}{2^\theta} + m(n-1)\frac{1}{2^{2\theta}} + m(n-1)\frac{1}{2^\gamma}$. Since n, k and m are polynomially bounded in κ and θ is sufficiently large, the advantage is at most negligible.

From now on, in the theorems stated below, we assume there are only one reader R and one tag $\mathscr{T}$, target tag, in the system.

Theorem 4. *The RFID protocol demonstrated in Figure 3 achieves tag authentication for a k-strong adversary $\mathscr{A}_k$.*

Proof. Let κ be the security parameter in the RFID system. According to Lemma 2, there are only one tag, $\mathscr{T}$ and one reader, $\mathscr{R}$ in the system. Note that the adversary does not need to apply CREATETAG, DRAWTAG and FREE oracles. $\mathscr{A}_k$ can use SENDREADER(π) oracle to start a protocol run either between $\mathscr{R}$ and $\mathscr{T}$ or between $\mathscr{R}$ and himself. Furthermore, $\mathscr{A}_k$ can use RESULT oracle polynomially bounded in κ number of times by sending b and c values to the reader for corresponding a values, which are sent by $\mathscr{R}$ as a result of the usage of SENDREADER(π) oracle. Moreover, $\mathscr{A}_k$ can use SENDTAG oracle polynomially bounded in κ number of times to send a challenge value a to $\mathscr{T}$. Besides, $\mathscr{A}_k$ can use CORRUPT oracle at most k times and we assume that the adversary exactly applies CORRUPT oracle k times to increase her chance to destroy tag authentication.

By Lemma 1, we assume that $\mathscr{A}_k$ applies CORRUPT oracle by rules of the set B_{k+1}. Moreover, we us assume that $\mathscr{A}_k$ observed number of m_1 protocol runs between $\mathscr{R}$ and $\mathscr{T}$ and queried SENDREADER(π) oracle m_2 times to start protocol run between $\mathscr{R}$ and $\mathscr{T}$. Furthermore, $\mathscr{A}_k$ uses SENDTAG oracle m_3 times.

Note that m_1, m_2, m_3 are polynomially bounded integers in κ and in order to increase the success probability of $\mathscr{A}_k$'s destroying tag authentication, we assume that in all protocol runs, occurred as a result of above oracle usages and observation, different a values are used. Moreover, assume that SENDREADER(π) oracle is used m_4 times to start protocol run between the reader and the adversary. After k^{th} corruption, $\mathscr{A}_k$ uses number of m_5 SENDREADER(π) oracles to start protocol run between the reader and herself. In each of these runs $\mathscr{A}_k$ receives a different a values, then she generates a pair (b,c) and $\mathscr{A}_k$ sends this pair to the reader and finally $\mathscr{A}_s$ uses RESULT oracle for triple (a,b,c). Assume the adversary has y chances to impersonate the corresponding tag without using any oracle where y is polynomial bounded in κ. Moreover, $\mathscr{A}_k$ is allowed to prepare p_i triples (K^{k+1},b_i,c_i) for corresponding impersonation trial i. Note that these triples are prepared according to guesses of $\mathscr{A}_k$ on the value of the missing key. $\mathscr{A}_k$ checks if any of the triples is true or false based on the protocol transcripts reached so far at each impersonation round. If $\mathscr{A}_k$ has no success at p_i triples, then the adversary just guesses the values of b and c. Let us denote $M = m_1 + m_2 + m_3 + m_4 + m_5$ and $P = \max\{p_1,\ldots,p_y\}$. Note that M and P are polynomially bounded in κ. Let us figure out the success probability of the adversary at i^{th} impersonation trial. The reader sends a_i as a challenge to the adversary. If a_i is equal to any of the a values that were used at previous successful protocol transactions observed or created by oracle usage, then with 1 probability, the adversary succeeds. However, the probability of realization of this scenario is at most $\frac{M}{2^\alpha}$. In case of failure, then $\mathscr{A}_k$ checks correctness of each p_i triple. However, the success probability of $\mathscr{A}_k$ in this case is at most $\sum_{l=(i-1)P-1}^{iP-2}[(\prod_{j=0}^{l}(1-\frac{1}{2^\theta-j}))\frac{1}{2^\theta-l-1}]$. If the adversary fails after two cases discussed above, then she guesses the values of b and c. At each trial, the success probability is $\frac{1}{2^\gamma-P}$.

Thus, maximum success probability of $\mathscr{A}_k$ at the end of y^{th} impersonation trial is smaller than $\frac{yM}{2^\alpha}+(1-\frac{M}{2^\alpha})[\frac{1}{2^\theta}+\sum_{i=0}^{yP-2}[(\prod_{j=0}^{i}(1-\frac{1}{2^\theta-j}))\frac{1}{2^\theta-i-1}]]+(\frac{y}{2^\gamma-P})$. Let us denote above probability by B. Then,

$$\begin{aligned} B &\leq \frac{yM}{2^\alpha} + \sum_{i=0}^{yP-2}\frac{1}{2^\theta-i-1} + \frac{y}{2^\gamma-P} \\ &\leq y\left[\frac{M}{2^\alpha} + \frac{P}{2^{\theta-1}} + \frac{1}{2^\gamma-P}\right] \end{aligned} \tag{1}$$

The resulting probability is negligible since y, M and P are polynomially bounded and α, θ and γ are big enough. Thus the system satisfies tag authentication.

Theorem 5. *The RFID protocol demonstrated in Figure 3 achieves k-strong privacy.*

Proof. Assume to the contrary, the system does not satisfy k-strong privacy. Then, there exists an adversary $\mathscr{A}_k$, who can distinguish between the real RFID system and the system simulated by a blinder $\mathscr{B}$ with non-negligible probability. By definition, $\mathscr{B}$ simulates LAUNCH, SENDTAG, SENDREADER and RESULT oracles without knowing the tag and the reader secrets.

Let us start with how $\mathscr{B}$ evaluates the oracles:

- LAUNCH(): $\mathscr{B}$ evaluates this oracle in a trivial way.
- SENDREADER(π): The output is $a \in_R \{0,1\}^\alpha$.
- SENDTAG(a): The output is $b \in_R \{0,1\}^\alpha$, $c \in_R \{0,1\}^\gamma$.
- SENDREADER($(b,c),\pi$): returns no output.
- RESULT(π): If π is generated by LAUNCH oracle and the protocol transcript is generated by SENDTAG and SENDREADER oracles, the output is 1. If one of the conditions does not hold, then the output is 0.

By Lemma 2, we assume that there are only one tag and one reader in the system. Moreover, for simplicity and to increase the success probability of $\mathscr{A}_k$ to destroy the privacy, we assume the database of the reader is not updated throughout the proof. Let the system run for n times only by real RFID system or the blinder $\mathscr{B}$, where n is polynomially bounded integer in κ. In other words, all usable oracles defined at Section 3.1 is used at most n times. Moreover, by Lemma 1, assume that CORRUPT oracle is applied by the rules of the set B_{k+1}.

There are three cases to consider: The first case is guessing of the value of K^{k+1}. The probability of this happening is $\frac{1}{2^\theta}$. The second case is $\mathscr{A}_k$ to determine the correct value of c in at least one of the protocol runs. The probability of this case is $1-(1-\frac{1}{2^\gamma})^n$. The last case is $\mathscr{A}_k$ to guess the value that is produced by the RESULT oracle is correct or wrong successfully.

By contradiction assumption, since $\mathscr{A}_k$ destroys the privacy, either one of two probabilities given above is non-negligible or the probability of realization of the last case is non-negligible. However, with sufficiently large θ and γ values, first two probabilities are negligible. Thus, the success probability of $\mathscr{A}_k$ to guess the value that is produced by the RESULT oracle is correct or wrong is non-negligible. However, this contradicts with Theorem 4, namely, contradicts to the tag authentication.

6 Adapting Our Protocol to Reader Authentication

The privacy definition given by Paise and Vaudenay (P-V) is based on the anonymity of the tags and unlink-ability of the interactions. The privacy of an

RFID scheme is broken when an adversary identifies a victim tag or links its interactions [37]. Nevertheless, Armknecht et al. define privacy as the ability of an adversary to distinguish real oracles from the blinder $\mathscr{B}$ [3]. The concept of privacy in the P-V model is based on distinguishing between different tags, whereas in the Armknecht et al.'s model the privacy is defined based on the notion of (left-or-right) or (0-or-1) indistinguishability game. Therefore, their results on the privacy with reader authentication are different.

By using [3] approach, Habibi et al. claim that the highest achievable privacy level is narrow-weak privacy with reader authentication [20]. However, in this section, we prove that it is possible to achieve *k*-strong privacy and reader authentication by introducing a PUF based RFID mutual authentication protocol. This is the first attempt to provide both these security and privacy properties in the literature. For our proposed mutual authentication protocol, we first give definitions of two functions, $\mathscr{F}_{tag}$, $\mathscr{F}_{reader}$ which combine some steps of computation at tag and reader side respectively. These functions make our next protocol more readable. The function $\mathscr{F}_{tag}$ requires two random challenges (a,b), the initial nonce G and the number of k internal steps. $\mathscr{F}_{tag}$ does the computation from step 2 to step 6 at the tag side (see Figure 3). The process depicted in Figure 4.

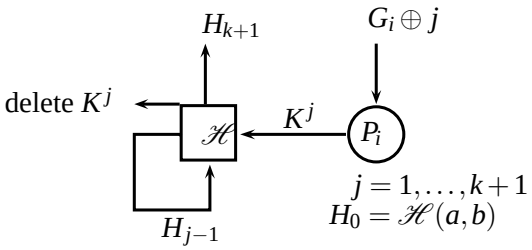

Fig. 4: A Generic function $\mathscr{F}_{tag}(a,b,G_i,k+1) = H_{k+1}$

$\mathscr{F}_{reader}$ takes two challenges (a,b) and the secret keys of a tag $(K^1,\ldots,K^{k+1})$ and produces the output H. It simply does the computation from step 11 to step 14 at the reader side(see Figure3). The process depicted in Figure 5.

Note that the notations used in the protocol are already described in Section 5. The extended mutual authentication protocol works as follows. First of all, $\mathscr{R}$ generates a random nonce a and sends it to $\mathscr{T}_i$. As receiving a, $\mathscr{T}_i$ generates a random nonce b and computes $c = \mathscr{F}_{tag}(a,b,G_i,k+1)$ and sends c along with b to the reader. Then, for each record $(K_j^1,\ldots,K_j^{k+1},ID_j)$ in $\mathscr{DB}$ where $j \in \{1,\ldots,n\}$, $\mathscr{R}$ computes $c = \mathscr{F}_{reader}(a,b,K_j^1,\ldots,K_j^{k+1})$. If a match

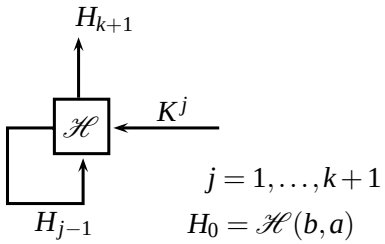

Fig. 5: $\mathscr{F}_{reader}(b,a,K^1,\ldots,K^{k+1}) = H_{k+1}$

($c' = c$) is found, then the tag authentication succeeds and $\mathscr{R}$ computes $d = \mathscr{F}_{reader}(b,a,K_j^1,\ldots,K_j^{k+1})$ and sends d to $\mathscr{T}_i$. If no match is found in $\mathscr{DB}$, $\mathscr{R}$ sends random bits to $\mathscr{T}_i$. Finally, upon receiving d, $\mathscr{T}_i$ computes $d' = \mathscr{F}_{tag}(b,a,G_i,k+1)$ and if d is equal to d', then the reader authentication succeeds.

Reader		**Tag**$_i$
$\mathscr{DB}$ = $\{(K_1^1,\ldots,K_k^1,K_{k+1}^1,\mathbf{ID}^1),$ $\ldots,(K_1^n,\ldots,K_k^n,K_{k+1}^n,\mathbf{ID}^n)\}$		G_i, $\mathbf{ID}_i$
1. Pick $a \in_R \{0,1\}^\alpha$		Pick $b \in_R \{0,1\}^\alpha$
2.	$\xrightarrow{a}$	$c = \mathscr{F}_{tag}(a,b,G_i,k+1)$
3.		Send b,c
4. **If** $\exists(K_j^1,\ldots,K_j^{k+1},ID_j) \in \mathscr{DB}$	$\xleftarrow{b,c}$	
5. **s.t.** $c \stackrel{?}{=} \mathscr{F}_{reader}(a,b,K_j^1,\ldots,K_j^{k+1})$		
6. **then**		
7. **return** $d = F_{reader}(b,a,K_j^1,\ldots,K_j^{k+1})$		
8. **else return** $d \in_R \{0,1\}^\gamma$		
9. **endif**		
10.	$\xrightarrow{d}$	$d \stackrel{?}{=} \mathscr{F}_{tag}(b,a,G_i,k+1)$

Fig. 6: A Generic PUF based Mutual Authentication Protocol.

6.1 Security and Privacy Analysis

In this section, we first prove that our protocol achieves reader authentication. Then we utilize this proof in order to prove the protocol also provides k-strong privacy. Note that, throughout all proofs of this section, we assume that a tag is

destructed at k^{th} CORRUPT oracle usage. This assumption gives the adversary the opportunity to take advantage of performing maximum number of oracles to any tag.

Theorem 6. *The RFID protocol demonstrated in Figure 6 achieves reader authentication for k-strong adversary $\mathscr{A}_k$.*

Proof. By Lemma 2, let there be one reader, $\mathscr{R}$ and one tag, $\mathscr{T}$ in the system. Also, the adversary $\mathscr{A}$ has applied CORRUPT oracle to $\mathscr{T}$ k times with rules of B_{k+1}. Besides, A_k observes the number of m_1 protocol runs between $\mathscr{R}$ and $\mathscr{T}$. Also assume that A_k applies following oracles with given number of times before authentication game as described below:

1. m_1 times: no oracle usage, the adversary just watches protocol run between $\mathscr{R}$ and $\mathscr{T}$
2. m_2 times: SENDREADER(π) oracle to start protocol run between $\mathscr{R}$ and $\mathscr{T}$
3. m_3 times: SENDTAG(a) oracle and SENDREADER(b,c) , where SENDTAG$(a) \rightarrow (b,c)$
4. m_4 times: A_k derives (b,c) and uses SENDREADER(b,c) and RESULT(d) oracles, where SENDREADER$(b,c) \rightarrow d$.

In order to increase the success probability of A_k, let us assume that the value of a that is sent to tag by the adversary or derived as a result of SENDREADER(π) oracle is fixed. Moreover, let us assume that different b,c values are used by the adversary or the tag as a result of SENDTAG(a) oracle usage).

Let the adversary have the number of y chances in order to impersonate the corresponding reader without using any oracle. Moreover, $\mathscr{A}_k$ is allowed to prepare p_i pairs (K_j^{k+1}, d_j^i), $j = 1,\ldots,p_i$, for corresponding impersonation trial i. Note that these pairs are prepared according to guesses of $\mathscr{A}_k$ on value of missing key. $\mathscr{A}_k$ checks if any pair created is true or false based on the protocol transcripts reached so far at each impersonation round. If $\mathscr{A}_k$ has no success at p_i pairs, then the adversary just guesses the values of d^i.

Let us denote $M = m_1 + m_2 + m_3 + m_4$ and $P = \max\{p_1,\ldots,p_k\}$ where M and P are polynomially bounded positive integers in κ. Let us figure out the success probability of the adversary at i^{th} impersonation trial. Assume that the adversary sends a to the tag. If the tag responds with (b,c) pair value that was used previously while using the oracles defined above, then the adversary succeeds with probability 1. If this is not the case, then A_k checks the correctness of each (K_j^{k+1}, d_j^i), $j = 1,\ldots,p_i$. However, the success probability of $\mathscr{A}_k$ in this

case is at most $\sum_{l=(i-1)P-1}^{iP-2}\left[\left(\prod_{j=0}^{l}\left(1-\frac{1}{2^{\theta}-j}\right)\right)\frac{1}{2^{\theta}-l-1}\right]$. If the adversary fails after two cases discussed above, then she guesses the values of d^i. At this trial the success probability is $\frac{1}{2^{\gamma}-P}$.

Thus, maximum success probability of $\mathscr{A}_k$ at the end of y^{th} impersonation trial is smaller than

$$\frac{1}{2^{\theta}}\left(1-\frac{M}{2^{\alpha}}\right)+\sum_{i=0}^{yP-2}\left[\left(\prod_{j=0}^{i}\left(1-\frac{1}{2^{\theta}-j}\right)\right)\frac{1}{2^{\theta}-i-1}\right] + \frac{yM}{2^{\alpha}}+\left(\frac{y}{2^{\gamma}-P}\right)$$

Let us denote above probability by B. Then,

$$\begin{aligned} B &\leq \frac{yM}{2^{\alpha}}+\sum_{i=0}^{yP-2}\frac{1}{2^{\theta}-i-1}+\frac{y}{2^{\gamma}-P} \\ &\leq y\left[\frac{M}{2^{\alpha}}+\frac{P}{2^{\theta-1}}+\frac{1}{2^{\gamma}-P}\right] \end{aligned} \tag{2}$$

The resulting probability is negligible by the same argument since y, M and P are polynomially bounded in κ and α, θ and γ are big enough. Thus the system achieves reader authentication.

Theorem 7. *The RFID protocol demonstrated in Figure 6 achieves both k-strong privacy and reader authentication.*

Proof. Note that by Theorem 6 the system achieves reader authentication. Thus, we only need to prove k-strong privacy.

Assume to the contrary, there exists an adversary $\mathscr{A}_k$ who can distinguish the real RFID system and the system simulated by the blinder $\mathscr{B}$. The blinder simulates the oracles as it is defined at proof of Theorem 5 except SENDREADER$((b,c),\pi)$ oracle. In this case, $\mathscr{B}$ evaluates this oracle and it outputs $d \in_R \{0,1\}^{\gamma}$. Moreover, there is one more oracle $SendTag(d,\pi,end)$ simulated by $\mathscr{B}$. The blinder returns no output to this oracle.

By Lemma 2, let there be one tag and one real reader in the system. Moreover, let us assume that the reader is not updated throughout the proof. Let $\mathscr{A}_k$ apply the CORRUPT oracle k times by the rules of the set B_{k+1} by Lemma 1 and the system runs y times before distinguish-ability phase.

There are four cases to consider. The first case, as indicated at proof of Theorem 6, is the value of K^{k+1} or the value of c is determined correctly by the adversary $\mathscr{A}_k$ at least one protocol run by obtained information. However, the probabilities are $\frac{1}{2^{\theta}}$ and $1-(1-\frac{1}{2^{\gamma}})^y$ respectively.

The second case is to make $\mathscr{A}_k$ to determine the answers given from usage of RESULT oracle true or false after receiving $d \leftarrow$SENDREADER(b,c). Nonetheless, this is possible only if $\mathscr{A}_k$ knows the value of K^{k+1} but this can only happen with probability of $\frac{1}{2^\theta}$. The third case is that the correct value of d is determined by $\mathscr{A}_k$'s at least in one of the protocol runs. This probability is $1-(1-\frac{1}{2^\gamma})^y$. The last case is the value of c or d is guessed correctly by $\mathscr{A}_k$. However, the success probability is $\frac{1}{2^{\gamma-1}}$.

As all calculated probabilities are negligible and finite sum of negligible numbers are negligible. Thus we have a contradiction. Namely, $\mathscr{A}_k$ has at most negligible advantage at distinguishing the real system from the blinder. Thus, the system satisfies *k*-strong privacy.

7 Conclusion

In this paper, we revisited Vaudenay's privacy model, which is one of the well-known models in RFID frameworks. We went one step further and introduced two new notions of adversary classes, *k*-strong adversary and *k*-forward adversary. These two adversary classes cover all the classes defined by the Vaudenay's model and yield two new privacy classes, *k*-strong privacy and *k*-forward privacy. Contrary to Vaudenay's model, our model covers the security level between destructive and strong privacy.

We also proposed a new extended PUF definition *k*-PUFs. Ideal PUFS are assumed to be destroyed once tampered. However, our proposal extends this assumption to the real case, , i.e., these types of PUFS are tamper proof up to *k* corruptions. This new type of PUFs seems to be more plausible than prior proposals. This approach can also be considered as a more realistic scenario to analyze RFID authentication protocols.

Next, we give two robust PUF based authentication protocols to illustrate different privacy levels in our new extended model. In our first protocol, we prove that the strong privacy (∞-strong privacy in our model) in the Vaudenay model can be achieved by only using symmetric encryption and PUF functions. In our second protocol, we prove that both strong privacy and reader authentication can be achieved in our model (as it was not possible in the Paise Model previously).

8 Acknowledgment

We would like to thank anonymous referees for their invaluable comments that have significantly improved the article. Also, we would like to thank Berk Sunar and Unal Kocabas for their technical contributions especially on Sect. 2.4.

Bibliography

[1] Akgun M, Caglayan M (2011) Puf based scalable private rfid authentication. In: Availability, Reliability and Security (ARES), 2011 Sixth International Conference on, pp 473 –478

[2] Armknecht F, Maes R, Sadeghi AR, Sunar B, Tuyls P (2009) Memory leakage-resilient encryption based on physically unclonable functions. In: Advances in Cryptology – ASIACRYPT 2009, Lecture Notes in Computer Science, vol 5912, Springer Berlin Heidelberg, pp 685–702, DOI 10.1007/978-3-642-10366-7_40

[3] Armknecht F, Sadeghi AR, Visconti I, Wachsmann C (2010) On rfid privacy with mutual authentication and tag corruption. In: Proceedings of the 8th international conference on Applied cryptography and network security, Springer-Verlag, Berlin, Heidelberg, ACNS'10, pp 493–510

[4] Armknecht F, Maes R, Sadeghi AR, Standaert FX, Wachsmann C (2011) A formalization of the security features of physical functions. In: Proceedings of the 2011 IEEE Symposium on Security and Privacy, IEEE Computer Society, Washington, DC, USA, SP '11, pp 397–412, DOI 10.1109/SP.2011.10

[5] Avoine G (2005) Adversarial model for radio frequency identification. Tech. rep., Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC

[6] Avoine G, Oechslin P (2005) A scalable and provably secure hash-based rfid protocol. In: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops, IEEE Computer Society, Washington, DC, USA, PERCOMW '05, pp 110–114

[7] Bauder DW (1983) An Anti-Counterfeiting Concept for Currency Systems. Research report PTK- 11990. Sandia National Labs

[8] Bolotnyy L, Robins G (2007) Physically unclonable function-based security and privacy in rfid systems. In: Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications, IEEE Computer Society, Washington, DC, USA, pp 211–220

[9] Burmester M, van Le T, de Medeiros B (2006) Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols. In: Securecomm and Workshops, 2006, pp 1 –9

[10] Canard S, Coisel I, Etrog J, Girault M (2010) Privacy-preserving rfid systems: Model and constructions. URL

[11] Coisel I, Martin T (2011) Untangling rfid privacy models. Cryptology ePrint Archive, Report 2011/636,

[12] Deng RH, Li Y, Yung M, Zhao Y (2010) A new framework for rfid privacy. In: Proceedings of the 15th European conference on Research in computer security, Springer-Verlag, Berlin, Heidelberg, ESORICS'10, pp 1–18

[13] Devadas S, Suh E, Paral S, Sowell R, Ziola T, Khandelwal V (2008) Design and Implementation of PUF-Based 'Unclonable' RFID ICs for Anti-Counterfeiting and Security Applications. In: RFID, 2008 IEEE International Conference on, pp 58–64

[14] Dimitriou T (2005) A lightweight rfid protocol to protect against traceability and cloning attacks. In: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, IEEE Computer Society, Washington, DC, USA, pp 59–66

[15] Dodis Y, Ostrovsky R, Reyzin L, Smith A (2008) Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J Comput 38(1):97–139

[16] Dodis Y, Ostrovsky R, Reyzin L, Smith A (2008) Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J Comput 38(1):97–139

[17] Gassend B, Clarke D, van Dijk M, Devadas S (2002) Silicon physical random functions. In: Proceedings of the 9th ACM conference on Computer and communications security, ACM, New York, NY, USA, CCS '02, pp 148–160

[18] Guajardo J, Kumar S, Schrijen GJ, Tuyls P (2007) Physical unclonable functions and public-key crypto for fpga ip protection. In: Field Programmable Logic and Applications, 2007. FPL 2007. International Conference on, pp 189–195

[19] Ha J, Moon S, Zhou J, Ha J (2008) A new formal proof model for rfid location privacy. In: Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, Springer-Verlag, Berlin, Heidelberg, ESORICS '08, pp 267–281

[20] Habibi MH, Aref MR (2011) Two RFID privacy models in front of a court. Cryptology ePrint Archive, Report 2011/625

[21] Henrici D, Müller P (2004) Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, IEEE Computer Society, Washington, DC, USA, PERCOMW '04, pp 149–

[22] Hermans J, Pashalidis A, Vercauteren F, Preneel B (2011) A new rfid privacy model. In: Proceedings of the 16th European conference on Research

in computer security, Springer-Verlag, Berlin, Heidelberg, ESORICS'11, pp 568–587

[23] Holcomb DE, Burleson WP, Fu K (2007) Initial sram state as a fingerprint and source of true random numbers for rfid tags. In: In Proceedings of the Conference on RFID Security

[24] Juels A, Weis SA (2009) Defining strong privacy for rfid. ACM Trans Inf Syst Secur 13:7:1–7:23

[25] Kardaş S, Çelik S, Yildiz M, Levi A (2012) PUF-enhanced offline RFID security and privacy. Journal of Network and Computer Applications 11(12):1–11, DOI 10.1016/j.jnca.2012.08.006

[26] Kardaş S, Kiraz MS, Bingöl MA, Demirci H (2012) A novel rfid distance bounding protocol based on physically unclonable functions. In: Juels A, Paar C (eds) RFID. Security and Privacy, Springer Berlin / Heidelberg, Lecture Notes in Computer Science, vol 7055, pp 78–93

[27] Koeberl P, Li J, Rajan A, Vishik C, Wu W (2011) A practical device authentication scheme using sram pufs. In: Trust and Trustworthy Computing, vol 6740, Springer Berlin / Heidelberg, pp 63–77

[28] Kumar S, Guajardo J, Maes R, Schrijen GJ, Tuyls P (2008) Extended abstract: The butterfly puf protecting ip on every fpga. In: Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on, pp 67–70

[29] Lai J, Deng RH, Li Y (2010) Revisiting unpredictability-based rfid privacy models. In: Proceedings of the 8th international conference on Applied cryptography and network security, Springer-Verlag, Berlin, Heidelberg, ACNS'10, pp 475–492

[30] Lee YS, Park Y, Lee S, Kim T, Lee HJ (2011) Rfid mutual authentication protocol with unclonable rfid-tags. In: Mobile IT Convergence (ICMIC), 2011 International Conference on, pp 74 –77

[31] Li Z, Gong G (2011) Computationally efficient mutual entity authentication in wireless sensor networks. Ad Hoc Networks 9(2):204 – 215

[32] Lim CH, Kwon T (2006) Strong and robust rfid authentication enabling perfect ownership transfer. In: ICICS, pp 1–20

[33] Maes R, Tuyls P, Verbauwhede I (2008) Intrinsic pufs from flip-flops on reconfigurable devices. In: 3rd Benelux Workshop on Information and System Security (WISSec 2008), Eindhoven,NL, p 17

[34] Maubach S, Kevenaar T, Tuyls P (2006) Information-theoretic analysis of coating pufs

[35] Molnar D, Wagner D (2004) Privacy and security in library rfid: issues, practices, and architectures. In: Proceedings of the 11th ACM conference on Computer and communications security, ACM, New York, NY, USA, CCS '04, pp 210–219

[36] Naccache D, Fremanteau P (1994) Unforgeable identification device, identification device reader and method of identification. Patent-EP0583709
[37] Paise RI, Vaudenay S (2008) Mutual authentication in rfid: security and privacy. In: Proceedings of the 2008 ACM symposium on Information, computer and communications security, ACM, New York, NY, USA, ASIACCS '08, pp 292–299
[38] Pappu RS, Recht B, Taylor J, Gershenfeld N (2002) Physical one-way functions. Science 297:2026–2030
[39] Ranasinghe DC, Engels DW, Cole PH (2004) Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In: Systems, Proc. Auto-ID Labs Research Workshop
[40] Ravikanth P (March 2001) Physical One-Way Functions. PhD thesis, Massachusetts Institute of Technology
[41] Sadeghi AR, Visconti I, Wachsmann C (2010) PUF-Enhanced RFID Security and Privacy. In: Secure Component and System Identification – SECSI'10, Cologne, Germany
[42] Simmons G (1991) Identification of data, devices, documents and individuals. In: Security Technology, 1991. Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on, pp 197 –218
[43] Simmons GJ (1984) A system for verifying user identity and authorization at the point-of sale or access. Cryptologia 8(1):1–21
[44] Song B, Mitchell CJ (2008) Rfid authentication protocol for low-cost tags. In: Proceedings of the first ACM conference on Wireless network security, ACM, New York, NY, USA, WiSec '08, pp 140–147
[45] Tuyls P, Batina L (2006) RFID-Tags for Anti-counterfeiting. In: Topics in Cryptology – CT-RSA 2006, LNCS, vol 3860, pp 115–131
[46] Tuyls P, Skoric B (2006) Secret key generation from classical physics: Physical uncloneable functions. In: Mukherjee S, Aarts R, Roovers R, Widdershoven F, Ouwerkerk M (eds) AmIware Hardware Technology Drivers of Ambient Intelligence, Philips Research, vol 5, Springer Netherlands, pp 421–447, DOI 10.1007/1-4020-4198-5_20
[47] Tuyls P, Schrijen GJ, Škorić B, van Geloven J, Verhaegh N, Wolters R (2006) Read-proof hardware from protective coatings. In: Proceedings of the 8th international conference on Cryptographic Hardware and Embedded Systems, Springer-Verlag, Berlin, Heidelberg, CHES'06, pp 369–383, DOI 10.1007/11894063_29
[48] Van Deursen T, Mauw S, Radomirović S (2008) Untraceability of rfid protocols. In: Proceedings of the 2nd IFIP WG 11.2 international conference on Information security theory and practices: smart devices, convergence and next generation networks, Springer-Verlag, Berlin, Heidelberg, WISTP'08, pp 1–15

[49] Vaudenay S (2007) On privacy models for rfid. In: Proceedings of the Advances in Crypotology 13th international conference on Theory and application of cryptology and information security, Springer-Verlag, Berlin, Heidelberg, ASIACRYPT'07, pp 68–87

[50] Yang K, Zheng K, Guo Y, Wei D (2011) Puf-based node mutual authentication scheme for delay tolerant mobile sensor network. In: Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, pp 1 –4