Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 225 (2023) 3996–4005

Procedia Computer Science

www.elsevier.com/locate/procedia

27th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2023)

# Efficient RFID Scheme in Healthcare Systems

Ferucio Laurențiu Țiplea[a]*, Cristian Hristea[b], Daniela Gifu[a]

[a]*Faculty of Computer Science, "Alexandru Ioan Cuza" University of Iasi, General Berthelot, 16, 700483, Romania*
[b]*Simion Stoilow Institute of Mathematics of the Romanian Academy, Calea Griviței, 21, 010702, Bucharest, Romania*

**Abstract**

Healthcare offers a rich palette of potential applications of RFID technology. Healthcare provides a rich palette of possible applications of RFID technology. Besides traditional uses such as tracking medical equipment and devices or access control, healthcare can benefit even more significantly from RFID technology. However, using the RFID technology in healthcare raises various problems of scalability, timely identification of tags, security, privacy, and efficient implementation in practice. That is because such systems contain many tags, operate with private personal data, and must respond promptly in concrete, practical situations to avoid malfunctions (errors in the decision process, traffic congestion, and so on). This paper discusses the fundamental requirements of RFID systems raised by healthcare and the limitations of existing schemes. Then, we propose a new RFID scheme that achieves mutual authentication, strong privacy, and constant-time identification in the HPVP model. The scheme employs a secure symmetric-key encryption scheme, making it very efficient in implementation and physically unclonable functions (PUFs) to protect the secret key against adversaries with corruption capabilities.



*Keywords:* RFID system; security; privacy;

## 1. Introduction

Healthcare offers a rich palette of potential radio frequency identification (RFID) applications. Besides traditional uses such as tracking medical equipment and devices or access control, healthcare can benefit even more significantly from RFID technology. The misidentification of patients, drugs, blood bags, and so on, frequently occurring in hospitals, constitutes a real threat to patients' safety [1]. An RFID-based infrastructure would allow

* Corresponding author. Tel.: +40 742 019 593
*E-mail address:* ferucio.tiplea@uaic.ro


10.1016/j.procs.2023.10.395

medical staff to alleviate this issue and significantly reduce medical errors. Likewise, tracking the movement of patients and visitors throughout the hospital through RFID bracelets has also been proven to help prevent infectious diseases [2; 1]. It would be desirable for the next generation of RFID healthcare services to ensure continuous patient monitoring, whether in the hospital or discharged (but not in total health). Despite all these advantages, the adoption process of RFID technology in healthcare systems has stagnated over the past decade. There are several reasons for this, but probably the most important reason is that the scientific and technological research was not yet sufficiently mature to offer fully secure and private RFID systems at affordable implementation costs [2; 3; 4; 1]. The foremost vital properties that healthcare RFID schemes must satisfy are:

- Efficient, or even constant, identification time: healthcare systems can be extensive (millions of tags), and thus, linear identification time proportional to the size of the database can lead to frequent system crashes and dysfunctionalities;
- Good security properties to avoid identity or personal data theft, even when corrupting the tag;
- Good privacy level to avoid illegal tracking or monitoring of patients, drugs, and so on, even when corrupting the tag;
- Efficient software and hardware implementation: the operations performed by tags, including the communication protocol, must be performed promptly to avoid the system's congestion.

Suppose we translate these properties into the HPVP security and privacy RFID model [5]. In that case, we see that we are interested in building RFID schemes to ensure efficient or even constant-time tag identification, security against strong adversaries, a strong level of privacy, and efficient (software and hardware) implementation. By efficient implementation, we understand, among others, that the RFID schemes we are interested in should avoid public-key cryptography (PKC), which is still very expensive [6], primarily if implemented on low-power devices.

Thus, the main goal of our paper is to design an RFID scheme that achieves mutual authentication, strong privacy, constant-time tag identification, and efficient implementation in practice. In addition, the model in which we want these properties to be satisfied is the HPVP model. Why this model? Because it is based on indistinguishability, a common approach to discussing secure encryption and other properties of standard cryptographic primitives.

### 1.1. Related work

As far as we know, no RFID scheme fulfills the above four properties in the HPVP model. Over time, RFID schemes have been proposed to satisfy one or more of these properties, but not all simultaneously. In what follows, we will survey this effort in Vaudenay's and the HPVP model.

**Efficient identification but loss of privacy**: In any RFID protocol, the tag transmits certain information from which the reader extracts a specification and initiates the tag identification process in its backend database. This specification is named *tag identifier* [7]. Several authors have developed RFID schemes in which the tag identifier is updated only at the end of the communication protocol (tag identifiers with this property are called *constant tag identifiers* [8; 9; 10; 11; 12; 13; 7]). The great advantage of using constant tag identifiers is that the time complexity of identification is proportional to $\log n$, where $n$ is the database size [7]. Some authors have proposed particular database organizing techniques for better identification time than $\log n$ [10]. But what is very clear about such RFID schemes is that they dramatically lose privacy. A general approach has recently shown this [7]: no stateful RFID scheme with constant tag identifiers achieves any form of privacy in Vaudenay's model (with or without temporary state disclosure).

More recently, the authors of [14] have proposed a PUF-based RFID scheme that achieves constant time tag identification. They also claimed that the scheme achieves destructive privacy in Vaudenay's model with temporary state disclosure. Unfortunately, this is not true, as shown in [15]. As the scheme uses hash functions, random number generators (RNGs), a PUF, and the XOR operation to build messages transmitted between reader and tag, we may say that it achieves a certain degree of practical efficiency. However, sending secrets XOR-ed with "random" strings raises the issue of the generator's security [16]. That is because lightweight tags may only implement short-length RNGs and thus are susceptible to prediction. For instance, the EPC-compliant Class-1

Generation-2 standard [17] states that RFID tags should accommodate RNGs capable of providing 16-bit long random numbers. However, this might not be entirely secure. More secure RNGs require more than 1000 gate equivalents (GEs). But this is more than the GEs needed to implement lightweight symmetric-key ciphers [18].

**Efficient identification and strong privacy but inefficient implementation**: An elegant RFID protocol that allows constant-time identification is proposed in [19; 20] and based on PKC. The main idea is quite simple. Each tag has the reader's public key and can send its identity encrypted. Only the reader can decrypt the message, extract the tag's identity, and convert it into a hash index. Thus, the database search can be implemented in constant time (by hash indices). Vaudenay's PKC-based RFID scheme achieves strong privacy in the HPVP model [5; 21]. However, it uses PKC, which is still costly, primarily if implemented on low-power devices like RFID tags [6].

**Strong privacy but inefficient identification**: When Vaudenay's model was proposed, finding an RFID scheme to provide destructive privacy was an open problem. Using PUFs, [22] solved the problem. The scheme uses pseudo-random functions (PRFs), PUFs, and pseudo-random generators (PRGs), providing a certain degree of practical efficiency. The scheme appears to achieve strong privacy in the HPVP model. However, the scheme provides only unilateral authentication, and tag identification is inefficient, having linear time complexity in the database size.

### 1.2. Contribution

This paper proposes a PUF-based RFID scheme that achieves mutual authentication, strong privacy, and constant-time identification in the HPVP model with temporary state disclosure. Moreover, our scheme is very efficient in practical implementation. The scheme employs a secure symmetric-key encryption scheme. To protect the secret key on tags, we mask it with PUF values. We use the reader-first authentication approach to avoid using temporary variables that might compromise privacy, where the tag authenticates the reader first.

The use of PUFs should not be an inconvenience to our scheme. That is because reader authentication and narrow forward privacy are not possible by employing standard cryptography when corruption with temporary state disclosure is allowed [23]. The only technique known so far to bypass this limitation is by PUFs [22; 24; 14; 15; 25]. On the other hand, PUF technology is becoming increasingly mature, with a wide variety of hardware implementations at the moment [26; 27] (see Section 6).

Because the scheme employs only a symmetric-key encryption scheme and a PUF, it is efficient in practical implementation. We also emphasize that the scheme does not need RNGs on tags (please see our discussion above on RNGs).

### 1.3. Paper structure

The paper consists of seven sections, the first being the introductory section. The basic concepts and notations used in this paper are presented in Sections 2 and 3 (the latter being dedicated to RFID systems). Section 4 discusses general issues regarding tag identification complexity. In Section 5, we propose our main RFID scheme and prove its security and destructive privacy. The last two sections focus on implementation issues, comparison with other schemes, and conclude the paper. Due to the lack of space, the paper does not include our scheme's security and privacy proofs.

## 2. Basic Definitions and Notation

We recall in this section a few concepts from cryptography. For details, we refer the reader to standard textbooks, such as [28]. An adversary is a *probabilistic polynomial time* (PPT) algorithm [29] that can consult oracles. An oracle is a black box that can perform a particular computation. When considering an oracle, we do not care about its implementation or how it works. Whenever a PPT algorithm A sends a value x to some oracle $O$, the oracle returns a given value in O(1) time, which can be used further by A.

Given a set A, $a \leftarrow A$ means that a is chosen randomly from A under the uniform distribution. The asymptotic approach to security uses security parameters, denoted by $\lambda$ in our paper. A positive function $f(\lambda)$ is called negligible if for any positive polynomial $poly(\lambda)$ there exists $n_0$ such that $f(\lambda) < 1/poly(\lambda)$, for any $\lambda \geqslant n_0$.

A *symmetric-key encryption* (SKE) scheme is a triple of PPT algorithms $S = (G, \mathcal{E}, D)$, where $G$ outputs a secret key $K$ when takes as input a security parameter $\lambda$, $\mathcal{E}$ outputs a ciphertext $y$ when takes as input a key $K$ and a message $x$, and $D$ is deterministic and outputs a plaintext when takes as input a key $K$ and a ciphertext, such that $x = D(K, y)$, for any $y \leftarrow \mathcal{E}(K, x)$. Usually, SKE schemes are obtained by iterating *block ciphers*. S is called IND-CPA secure if no PPT algorithm A that is allowed to query the encryption algorithm $\mathcal{E}$ of S has a non-negligible advantage to distinguish between two equally length plaintexts, given a ciphertext of one of them.

For the sake of simplicity, we use $\{x\}_K$ ($\{y\}_{K^{-1}}$) to denote encryption (decryption) of $x$ ($y$) by $K$. To concatenate two or more messages, we use " ‖ . "

## 3. (PUF Based) RFID Schemes and Systems

We recall basic notions regarding RFID systems in this section (please see [19; 20] for details). An RFID system typically comprises three main entities: a *reader*, a set of *tags*, and a radio frequency *communication protocol* between the reader and tags. The reader is a powerful device not computationally restricted to perform any cryptographic operation. It stores tag-related information in a database to which it has secure access. On the other side, tags are small devices that are resource constrained. Typically, a tag's memory is split into *permanent* (or *internal*), used to store the state values of the tag, and *temporary* (or *volatile*), used to carry out the calculations required by the communication protocol.

Let $R$ be a *reader identifier,* and $T$ be a set of *tag identifiers* whose cardinal is polynomial in some security parameter $\lambda$. An *RFID scheme over* $(R, T)$ [19; 20] is a triple $S = (SetupR, SetupT, Ident)$ of PPT algorithms, where:

1. $SetupR(\lambda)$ inputs a security parameter $\lambda$ and outputs a triple $(pk, sk, DB)$ consisting of a key pair $(pk, sk)$ and an empty database $DB$; $pk$ is public, while $sk$ is kept secret by the reader;
2. $SetupT(pk, ID)$ initializes the tag identified by $ID$. It outputs an initial tag state $S$ and a tag-specific secret $K$. The identity $ID$ together with $K$ is stored as a pair $(ID, K)$ in the reader's database;
3. $Ident(pk; R(sk, DB); ID(S))$ is an interactive protocol between the reader identified by $R$ (with its private key $sk$ and database $DB$) and a tag identified by $ID$ (with its state $S$ ) in which the reader ends with an output consisting of $ID$ or $\perp$. The tag may end with no output (*unilateral authentication*), or it may end with an output consisting of $OK$ or $\perp$ (*mutual authentication*).

The *correctness* of an RFID scheme means that, regardless of how the system is set up, after each complete execution of the interactive protocol between the reader and a legitimate tag, the reader outputs the tag's identity with overwhelming probability. For mutual authentication RFID schemes, *correctness* means that the reader outputs the tag's identity, and the tag outputs $OK$ with overwhelming probability.

An *RFID system* is an instantiation of an RFID scheme by a trusted *operator, I,* who establishes the reader identifier $R$, the set $T$ of tag identifiers, and runs an RFID scheme over $(R, T)$. In a given setting, the reader is initialized exactly once, while each tag is at most once. Thus, the reader's database does not store different entries for the same tag. However, various settings with the same RFID scheme may initialize the reader and the tags differently.

The newest technologies allow RFID systems with tags equipped with *physically unclonable functions* (PUFs) [30]. A PUF is a physical object that, when queried with a challenge $x$, generates a response $y$ that depends on both $x$ and the specific physical properties of the object. PUFs are typically assumed to be *physically unclonable* (it is infeasible to produce two PUFs that cannot be distinguished based on their challenge/response behavior), *unpredictable* (it is infeasible to predict the response to an unknown challenge), and *tamper-evident* (any attempt to physically access the PUF irreversible changes the challenge/response behavior).

Tags equipped with PUFs are called *PUF tags*. An RFID scheme with PUF tags is sometimes called a *PUF-based* one. The main advantage of using PUF tags is that the corruption on a PUF tag reveals the tag's permanent (and temporary) memory. Still, the values computed by PUFs cannot be obtained (except when saved in the permanent memory or non-local temporary variables).

## 4. Identification Time in RFID Schemes

With the increase in the applicability of RFID systems, the number of tags to be managed by the backend server has increased. That raises the problem of tag identification time by the reader. We thus face an online search problem for a specific record in an extensive database. The tag has to provide the reader with identification information, and the reader has to search the database for related information. The information provided by the tag for identification, generically called *tag identifier*, may facilitate more or less the identification process.

A tag identifier should not be confused with the tag's identity. It may be a tag identity, but it may also be a hash of a tag identity or any other information that uniquely identifies the tag without losing security and privacy. A tag identifier may also be a constant value (as in the case of the tag's identity), it may be derived from the tag's state or the tag's state and some message received from the reader. Therefore, a tag identifier may change dynamically, so the tag identification in the backend database might not always be very efficient.

The tag identification time in the backend database depends on how the tag identifiers are viewed as search indices [31]. There are two main approaches along this line: *ordered* and *hash indices*.

An *ordered index* is a pair that consists of a search key value and a pointer to the corresponding record or a disk block containing it in the backend database. The search key value sorts ordered indices. Therefore, the identification time of a tag is proportional to $\log n$ ($n$ being the database size). When the tag is identified and its state is updated, as it is, for instance, in [8; 9; 19; 20; 13; 15; 25], the tag identifier changes. Therefore, the index structure has to be updated as well. This can be done by deleting the old index entry and inserting the new one in the right position, which takes time proportional to $\log n$. Therefore, the entire process is proportional to $\log n$. Remark that the new index entry is obtained from the old one by replacing the search key value (the pointer remains unaltered).

The sequential organization of indices has the main disadvantage in that performance degrades as the index file grows. In such a case, one may think of organizing indices on multiple levels or as a $B^+$-tree. Lookup on $B^+$-trees is efficient; deletion and insertion are somewhat more complicated but still efficient. Thus, if the number of pointers in a non-leaf node is $k$, the height of the $B^+$-tree is proportional to $\log_k n$, and the identification and updating time is proportional to $\log_{k/2} n$. The value of $k$ is often around 50 or 100 [31].

The *hash organization* of a database uses a hash function that maps the search key value to the address of the desired record or to a *bucket* containing it (a bucket is a unit of storage containing one or more records; typically, a bucket is a disk block). In such a case, the lookup time is usually a constant, independent of the database size. This approach can be used with all RFID schemes for which the tag identifier is constant, such as the PKC-based RFID scheme in [19].

There is also another approach based on hash indices. Namely, we compute hash indices for all possible search keys of each tag, associate the corresponding pointers to the database records, view the hash index (the hash file structure) obtained in this way as secondary (hash) indices, and use the first hashing approach to search within it. However, the search time might not be constant.

In this paper, we will look for constant-time identification using tag identifiers. That will also allow for scalability. However, the constant tag identifiers need encapsulating to avoid loss of privacy. In [19, 20], the PKC-based RFID scheme does this using PKC. To get more efficiency, we would like to do this through SKC. The details follow in the next section.

## 5. Strong Privacy and Constant-Time Identification

Now is the time to talk about the security and privacy properties of RFID systems. Our discussion is informal, but for details, we ask the reader to consult [19; 20; 5; 21]. These properties are essentially studied through well-established models, such as Vaudenay's [19; 20] or the HPVP model [5; 21]. There are other models, but these are the ones that best capture the security and privacy properties. Within these, the adversary can consult certain oracles that allow him to interact with the reader and tags. There are two oracles of significant importance in these models. One will enable the adversary to corrupt tags, and another allows him to know the reader's decision when he has ended a session with a tag.

The security property guarantees unilateral or mutual authentication within RFID systems. The privacy property guarantees non-tracking, anonymity, unlinkability, etc. Strong privacy guarantees privacy against all unrestricted adversaries.

The PKC-based RFID scheme proposed in [20] achieves forward privacy and mutual authentication in Vaudenay's model. Moreover, it allows constant-time identification of tags in the reader's database. That is because the reader has a public key distributed to all tags while keeping the corresponding private key. Therefore, each tag can safely send its identity encrypted by the reader's public key. The search procedure in the database may then be organized using hash indices computed on tag identities (as discussed in Section 4).

This idea cannot be implemented only by SKC because the secret key is necessary for both encryption and decryption. Sharing the secret key to all tags and the reader raises severe security and privacy problems: corruption of a tag reveals the secret key, and the entire system is compromised. However, if PUFs protect the secret key, it may act as a master key known only to tags and the reader. Trying to extract the key from tags by corruption destroys the tags without disclosing the key.

[14] proposed the first attempt to design a destructive private and mutual authentication RFID scheme using PUF-protected secret keys. Unfortunately, the scheme uses temporary variables to carry crucial information from one tag step to another; therefore, it leaks information by corruption. The reader is referred to [15] for a detailed attack on the scheme.

However, suppose we combine the idea in [14] of using PUF-protected secret keys with the idea in [25] of using a reader-first authentication approach to avoid using temporary variables. In that case, we arrive at an RFID scheme that achieves good privacy and mutual authentication under temporary state disclosure while allowing constant-time identification of tags in the backend database.

| | **Reader** $(DB, K_m)$ | | **Tag** $(ID, x, K'_m, P, s)$ |
|---|---|---|---|
| 1 | | | $K = P(s)$, $K_m = K'_m \oplus K$,<br>$x = x + 1$, $z = \{x \parallel ID\}_{K_m}$ |
| | | $\xleftarrow{z}$ | erase $K$, $K_m$ |
| 2 | $\{z\}_{K_m^{-1}} = x \parallel ID$<br>If $\exists (ID, y) \in DB$ and $y < x$<br>then $y = x - 1$, $v \leftarrow \{0,1\}^\ell$, $w = \{v \parallel (y+1)\}_{K_m}$<br>else $w \leftarrow \{0,1\}^{2\ell}$ | | |
| | | $\xrightarrow{w}$ | |
| 3 | | | $K = P(s)$, $K_m = K'_m \oplus K$,<br>$\{w\}_{K_m^{-1}} = v' \parallel x'$<br>If $x = x'$<br>then output $OK$,<br>$x = x + 1$, $w' = \{x \parallel (v'+1)\}_{K_m}$<br>else output $\perp$<br>$x = x + 1$, $w' = \{x \parallel (v'+2)\}_{K_m}$ |
| | | $\xleftarrow{w'}$ | erase $K$, $K_m$ |
| 4 | If $w' = \{(y+2) \parallel (v+1)\}_{K_m}$<br>then output $ID$, $y = y + 2$<br>else output $\perp$ | | |

Fig. 1. Strong privacy and reader-first authentication RFID scheme in the HPVP model with temporary state disclosure.

We thus propose an RFID scheme based on an SKE scheme $\{\cdot\}_{K_m}$ whose block length and key length are $\ell$, where $\ell$ is polynomial in the security parameter $\lambda$. The secret key $K_m$, also called the *master key* of the scheme, is stored on the reader and all tags. However, to avoid key disclosure by tag corruption, $K_m$ is stored on tags in a masked form $K'_m = K_m \oplus P(s)$, where $P$ is a PUF and $s$ is a seed, both specific to the tag.

Each tag is identified by its identity $ID$ and is initially endowed with a random value, $x$, needed to randomize the encryption. The value $x$ is incremented each time a tag is queried. For the simplicity of the exposition, we assume that $ID$, $x$, $s$, and $P(s)$ are all of the same length $\ell$. The mutual authentication protocol is represented in Figure 1. The tag evaluates its PUF $P$ on $s$, extracts $K_m$ from $K'_m$ with the help of $P(s)$, and sends its encrypted credentials $(x, ID)$

to the reader. Remark that $x$ is the first block to be encrypted (using some operation mode) because it will get a new value the next time the protocol is initiated. In this way, the encryption gets randomized†.

When the reader receives the message from the tag, it decrypts it and looks for a corresponding record in its database. If this is found, which means that the reader identified the tag, an "authentication code" $w$, obtained from a random $v$ and $x$, is returned (remark that $v$ is the first block to be encrypted). The tag decrypts $w$ and checks the $x$-values. If they match, it authenticates the reader and prepares an "authentication code" $w'$ for the reader. Note again that $w'$ is built by placing x in the first position after it has been incremented. When receiving $w'$, the reader checks it against the value $\{(y + 2) \| (v + 1)\}_{K_m}$ computed by itself. If they match, the tag is authenticated, and $x$ is synchronized (by incrementing it) with the corresponding value on the tag. It is straightforward to check the correctness of this scheme. We list below a few properties of it:

1. The x-value gets greater than (but never less than) the corresponding value stored in the database, querying the tag multiple times without completing the protocol. However, the reader synchronizes its $x$-value with the one used by the tag to compose the message $w$ when identifies the tag;
2. The scheme does not use temporary variables to carry information from one protocol step to another. So the scheme does not depend on temporary state disclosure;
3. The tag identification process takes constant time if the database uses hash indices computed on tag identities;
4. The scheme does not use RNGs on tags, which might be a source of insecurity if they are not sufficiently long. Secure RNGs require more than 1000 GEs [18];
5. There are lightweight block ciphers that are sufficiently secure and can efficiently be implemented on RFID tags (please see the last section of the paper for more details on this).

We will now focus on the security and privacy of our RFID scheme. First of all, we idealize PUFs. *An ideal PUF* is a physical object with a challenge/response behavior that implements a function $P$: $\{0, 1\}^p \rightarrow \{0, 1\}^k$, where $p$ and $k$ are of polynomial size in $\lambda$, such that:

1. $P$ is computationally indistinguishable from a random function (that is, no PPT algorithm can decide with more than a negligible probability whether a given value is an output of $P$ or is uniformly at random chosen);
2. Any attempt to physically tamper with the object implementing P results in P's destruction, so the adversary cannot evaluate P anymore.

We have the following result (due to the lack of space, we omit the proof).

**Theorem 5.1.** *The RFID scheme in Figure 1 achieves tag authentication, reader authentication, and strong privacy in the HPVP model, as long as the SKE scheme is secure and the PUFs are ideal.*

We can easily transform the RFID scheme in Figure 1 into a weak private scheme: we must remove the PUF from each tag and keep the master key $K_m$ in the tag's permanent memory. Although this might seem a good idea from the constant-time identification point of view, this solution should be taken with care. This is because disclosure of $K_m$ compromises the entire scheme. One can see that in our RFID scheme in Figure 1, the messages have a length of $2\ell$. According to our assumption, each message to be encrypted consists of two blocks. Therefore, the SKE scheme must be IND-CPA secure for such messages. However, although the messages consist of only two blocks, some operation mode has to be used. When we proposed the scheme, we considered the CBC operation mode. Under this operation mode, the incrementation of $x$ and the random choice of $v$ randomizes the first block of the ciphertext. This block then encrypts the next message block, so the entire encryption gets randomized.

† Formally, the encryption will be required to be IND-CPA secure.

What we have said above is just an explanation underpinning our scheme's construction. In general, it is sufficient to ask the SKE scheme to be IND-CPA secure to get the RFID scheme's security and privacy (without any other constraints on the operation mode).

## 6. Implementation Issues

The existence of lightweight symmetric-key encryption schemes conditions the practical implementation of the RFID scheme in the previous section. An RFID tag has very few gates, many taken by the logic required for basic operation. In [32], it was estimated that about 5,000 GEs are left over in a typical RFID tag for cryptographic functions. That allows compact implementations of the Advanced Encryption Standard (AES) cryptosystem on RFID tags, using around 2,400 GEs [33; 34]. However, with processors getting smaller and faster and more devices becoming mobile, the AES cryptosystem has become clunky, while RFID technology developers are seeking something that consumes a smaller area of about 2,000 GEs.

Much effort has been dedicated to proposing lightweight block ciphers for the last fifteen years. Among them, it is worth mentioning PRESENT [35], Piccolo [36], SIMON and SPECK [37], and Simeck [38]. There are similarities between Simon/Speck and Simeck. 32/64- (48/96-, 64/128-) bit size block ciphers require less than 580 (800, 1030) GEs. They also have comparable security properties. In conclusion, all of them can meet the area, power consumption, and throughput requirements of passive RFID tags. They are promising candidates for resource-constrained devices, such as passive RFID tags and wireless sensor networks.

PUFs have been integrated into various cryptographic protocols since their introduction. Usually, PUFs serve two primary purposes: identification and cryptographic key generation. A primary example of the former situation is [39], where a PUF has been integrated into an RFID tag. Key generation by PUFs is a bit more delicate because we need to overcome the PUF's noisy nature and lack of entropy. Therefore, additional mechanisms such as error correction codes, hash functions, and helper data algorithms are needed [40].

Fortunately, this situation changed recently when new PUF constructions with very low bit error rates were proposed [41; 42; 43; 44]. The PUF design in [43; 44], based on the randomness of the soft breakdown position of CMOS transistors, is such an example. Denoted as BD-PUF, it represents a prominent candidate for constructing PUF-based key generation mechanisms with good entropy.

## 7. Conclusions

| RFID Scheme | Efficiency | Ident. time | Auth. | Privacy |
|---|---|---|---|---|
| [22] (2010) | 1 PRF + 1 PUF + 1 RNG | Linear | Unilateral | Destructive private in V |
| [24] (2012) | 4 Hash + 2 PUF + 2 RNG | Linear | Mutual | Claimed destructive private in V_TSD but not even narrow forward private [15] |
| [14] (2015) | 4 Hash + 2 PUF + 1 RNG | Constant | Mutual | Claimed destructive private in V_TSD but not even narrow forward private [15] |
| This paper | 3 SKE + 2 PUF | Constant | Mutual | Strong private in HPVP |

Fig. 2. Comparisons between RFID schemes: V stands for Vaudenay's model, and V_TSD stands for Vaudenay's model with temporary state disclosure.

We have proposed in this paper an RFID scheme that achieves mutual authentication, strong privacy, constant-time identification, and practical efficiency. The scheme uses symmetric-key encryption. We have masked the keys by PUF values to avoid key disclosure on tags. To reach strong privacy in the HPVP model, we avoided using temporary variables by following the reader-first authentication approach. Constant-time identification follows from the fact that each tag sends its encrypted identity to the reader.

As far as we know, this is the first RFID scheme that meets these properties in the HPVP model: mutual authentication, strong privacy, constant-time identification, and efficient implementation. The table in Figure 2 compares our scheme and the closest schemes to ours.

## References


[1] Haddara, M., Staaby A. (2018) "RFID Applications and Adoptions in Healthcare: A Review on Patient Safety." *Procedia Computer Science* **138**: 80-88.

[2] Lahtela, A. (2009) "A Short Overview of the Rfid Technology in Healthcare." *2009 Fourth International Conference on Systems and Networks Communications*, IEEE, 165-169.

[3] Yao, W., Chu, C.-H., Li, Z. (2010) "The Use of RFID in Healthcare: Benefits and Barriers." *IEEE International Conference on RFID-Technology and Applications*, IEEE, 128-134.

[4] Yao, W., Chu, C.-H., Li, Z. (2012) "The Adoption and Implementation of RFID Technologies in Healthcare: A Literature Review." *Journal of Medical Systems*, **36 (6)**: 3507-3525.

[5] Hermans, J., Pashalidis, A., Vercauteren, F., Preneel, B. (2011) "A New RFID Privacy Model." V. Atluri, C. Diaz (Eds.), *Computer Security – ESORICS 2011*, Springer Verlag, Berlin, Heidelberg, 568-587.

[6] Preneel, B. (2018) "Cryptography Best Practices." [Online]. Available: https://secappdev.org/handouts-2018.html

[7] C. Hristea, C., Țiplea, F.L. (2019) "Privacy of Stateful RFID Systems with Constant Tag Identifiers." *IEEE Transactions on Information Forensics and Security* **15**: 1920-1934. DOI: 10.1109/TIFS.2019.2953398.

[8] Dimitriou, T. (2005) "A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks." *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, SECURECOMM '05, IEEE Computer Society, Washington, DC, USA, 59-66.

[9] Tsudik, G. (2006) "YA-TRAP: Yet Another Trivial RFID Authentication Protocol." *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, PERCOMW '06, IEEE Computer Society, Washington, DC, USA, 640-643.

[10] Alomair, B., Lazos, L., Poovendran, R. (2010) "Securing Low-Cost RFID Systems: An Unconditionally Secure Approach." *Cryptology and Information Security Series*, **4**: 1–17. DOI: 10.3233/978-1-60750-485-6-1.

[11] Lu, L., Liu, Y., Li, X.-Y. (2010) "Refresh: Weak Privacy Model for RFID Systems." *Proceedings of the 29th Conference on Information Communications*, INFOCOM '10, IEEE Press, Piscataway, NJ, USA, 704–712.

[12] Alomair, B., Clark, A., Cuellar, J., Poovendran, R. (2012) "Scalable RFID Systems: A Privacy-Preserving Protocol with Constant-Time Identification." *IEEE Transactions on Parallel and Distributed Systems*, **3 (8)**: 1536-1550.

[13] Hristea, C., Tiplea, F.L. (2019) "A PUF-Based Destructive Private Mutual Authentication RFID Protocol." J.-L. Lanet, C. Toma (Eds.), *Innovative Security Solutions for Information Technology and Communications*, Springer Intern. Publishing.

[14] Akgun, M. (2015) "Caglayan M.U. Providing Destructive Privacy and Scalability in RFID Systems using PUFs." *Ad Hoc Netw.*, **32**: 32-42. DOI: 10.1016/j.adhoc.2015.02.001.

[15] Hristea, C., Tiplea, F.L. (2019) "Destructive Privacy and Mutual Authentication in Vaudenay's RFID Model." *Cryptology ePrint Archive*, Report 2019/073.

[16] Arslan, A., Kardas, S., C¸olak, S.A., Ertürk, S. (2018) "Are RNGs Achilles' Heel of RFID Security and Privacy Protocols?" *Wireless Personal Communications*, **100 (4)**: 1355-1375.

[17] *** (2016) "Interoperability Test System for EPC Compliant Class-1 Generation-2 UHF RFID Devices." *Tech. Rep.*, GS1 EPCglobal Inc. (Feb.).

[18] Armknecht, F., Hamann, M., Mikhalev, V. (2014) "Lightweight Authentication Protocols on Ultra-Constrained RFIDs – Myths and Facts." N. Saxena, A.-R. Sadeghi (Eds.), *Radio Frequency Identification: Security and Privacy Issues*, Springer International Publishing, Cham, 1-18.

[19] Vaudenay, S. (2007) "On Privacy Models for RFID." *Proceedings of the Advances in Cryptology 13th International Conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT '07, Springer-Verlag, Berlin, Heidelberg, 68-87.

[20] Paise, R.-I., Vaudenay, S. (2008) "Mutual Authentication in RFID: Security and Privacy." *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, ASIACCS '08, ACM, NY, USA, 292–299. DOI: 10.1145/1368310.1368352.

[21] Hermans, J., Peeters, R., Preneel, B. (2014) "Proper RFID Privacy: Model and Protocols." *IEEE Transactions on Mobile Computing*, **13 (12)**: 2888-2902. DOI: 10.1109/TMC.2014.2314127.

[22] Sadeghi, A.-R., Visconti, I., Wachsmann, C. (2010) "PUF-Enhanced RFID Security and Privacy." *Workshop on Secure Component and System Identification* (SECSI), **110**.

[23] Armknecht, F., Sadeghi, A.-R., Scafuro, A., Visconti, I., Wachsmann, C. (2010) "Impossibility Results for RFID Privacy Notions." M.L. Gavrilova, C.J.K. Tan, E.D. Moreno (Eds.), *Transactions on Computational Science*, **XI**, Springer-Verlag, Berlin, Heidelberg, 39-63.

[24] Kardaş, S., ÇElik, S., Yıldız, M., Levi, A. (2012) "PUF-Enhanced Offline RFID Security and Privacy." *J. Netw. Comput. Appl.*, **35 (6)**: 2059-2067. DOI: 10.1016/j.jnca.2012.08.006.

[25] Tiplea, F.L., Hristea, C. (2019) "Privacy and Reader-First Authentication in Vaudenay's RFID Model with Temporary State Disclosure." *Cryptology ePrint Archive*, Report 2019/113, https://eprint.iacr.org/2019/113.

[26] Maes, R., Verbauwhede, I. (2010) "Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions." Springer Verlag, Berlin, Heidelberg, 3-37.

[27] Delvaux, J., Peeters, R., Gu, D., Verbauwhede, I. (2015) "A Survey on Lightweight Entity Authentication with Strong PUFs." *ACM Comput. Surv.*, **48 (2)**: 26:1-26:42. DOI: 10.1145/2818186.

[28] Katz, J., Lindell, Y. (2014) "Introduction to Modern Cryptography." 2nd Edition, Chapman & Hall/CRC.

[29] Sipser, M. (2012) "Introduction to the Theory of Computation", Cengage Learning.

[30] Maes, R. (2013) "Physically Unclonable Functions: Constructions, Properties and Applications", Springer Verlag, Berlin, Heidelberg.

[31] Silberschatz, A., Korth, H., Sudarshan, S. (2010) "Database Systems Concepts," 6th Edition, McGraw-Hill Education, Inc., NY, USA.

[32] Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W. (2004) "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems." D. Hutter, G. M¨uller, W. Stephan, M. Ullmann (Eds.), *Security in Pervasive Computing*, Springer Verlag, Berlin, Heidelberg, 201-212.

[33] Moradi, A., Poschmann, A., Ling, S., Paar, C., Wang, H. (2011) "Pushing the Limits: A Very Compact and a Threshold Implementation of AES." K. G. Paterson (Ed.), *Advances in Cryptology – EUROCRYPT 2011*, Springer Verlag, Berlin, Heidelberg, 69-88.

[34] Banik, S., Bogdanov, A., Regazzoni, F. (2016) "Atomic-AES: A Compact Implementation of the AES Encryption/Decryption Core." *INDOCRYPT*.

[35] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C. (2007) "PRESENT: An Ultra-Lightweight Block Cipher." P. Paillier, I. Verbauwhede (Eds.), *Cryptographic Hardware and Embedded Systems – CHES 2007*, Springer Verlag, Berlin, Heidelberg, 450–466.

[36] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T. (2011) "Piccolo: An Ultra-Lightweight Blockcipher." B. Preneel, T. Takagi (Eds.), *Cryptographic Hardware and Embedded Systems – CHES 2011*, Springer Verlag, Berlin, Heidelberg, 342–357.

[37] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L. (2015) "The SIMON and SPECK Lightweight Block Ciphers." *Proceedings of the 52Nd Annual Design Automation Conference*, DAC '15, ACM, NY, USA, 175:1-175:6. DOI: 10.1145/2744769.

[38] Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G. (2015) "The Simeck Family of Lightweight Block Ciphers." T. G¨uneysu, H. Handschuh (Eds.), *Cryptographic Hardware and Embedded Systems – CHES 2015*, Springer Verlag, Berlin, Heidelberg, 307-329.

[39] Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., Khandelwal, V. (2008) "Design and implementation of PUF-based unclonable RFID ICs for anticounterfeiting and security applications." *IEEE International Conference on RFID*, 58-64.

[39] Delvaux, J., Gu, D., Schellekens, D., Verbauwhede, I. (2015) "Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **34 (6)**: 889-902.

[40] Yoshimoto, Y., Katoh, Y., Ogasahara, S., Wei, Z., Kouno, K. (2016) "A ReRAM-Based Physically Unclonable Function with Bit Error Rate ¡ 0.5% after 10 Years at 125◦ c for 40nm Embedded Application." *2016 IEEE Symposium on VLSI Technology*, 1-2.

[41] Liu, R., Wu, H., Pang, Y., Qian, H., Yu, S. (2015) "Experimental Characterization of Physical Unclonable Function Based on 1 kb Resistive Random-Access Memory Arrays." *IEEE Electron Device Letters*, **36 (12)**: 1380-1383.

[42] Chuang, K.-H., Bury, E., Degraeve, R., Kaczer, B., Groeseneken, G., Verbauwhede, I., Linten, D. (2017) "Physically Unclonable Function Using CMOS Breakdown Position." *2017 IEEE International Reliability Physics Symposium* (IRPS), 4C-1.

[43] Chuang, K.-H., Bury, E., Degraeve, R., Kaczer, B., Linien, D., Verbauwhede, I. (2018) "A Physically Unclonable Function with 0% ber Using Soft Oxide Breakdown in 40-nm CMOS." *2018 IEEE Asian Solid-State Circuits Conference* (A-SSCC), 157-160.