https://doi.org/10.52326/ic-ecco.2022/SEC.02

Privacy and Mutual Authentication under Temporary State Disclosure in RFID Systems

Ferucio Laurențiu Țiplea [1], ORCID: 0000-0001-6143-3641
Cristian Hristea [2], ORCID: 0000-0003-0132-9310
Rodica Bulai [3], ORCID: 0000-0002-7878-2431
[1] "Alexandru Ioan Cuza" University of Iasi, Iasi, Romania, ferucio.tiplea@uaic.ro
[2] Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania, cristi.hristea@gmail.com
[3] Technical University of Moldova, Chisinau, Republic of Moldova, rodica.bulai@ati.utm.md

***Abstract*—Privacy and mutual authentication are two significant requirements for real-life applications of RFID schemes. These two requirements have been studied for a long time only for adversaries that cannot corrupt the temporary internal state of the tags. Recently, however, it has been shown that corrupting the temporary internal state of the tag is practically possible. This raises the question: do the current RFID protocols that ensure mutual authentication and privacy keep these properties in the temporary state disclosure model? The answer is negative and thus it justifies the effort to propose new RFID protocols that are secure under temporary state disclosure.**

In this paper, we amply discuss how temporary state disclosure affects mutual authentication and privacy of RFID protocols, and illustrate this on two well-known protocols. We argue then in favor of using the PUF technology in order to achieve mutual authentication and a reasonable enough level of privacy under temporary state disclosure. We close by presenting two RFID schemes that achieve destructive privacy, one of the most important levels of privacy in the context of the physical corruption of tags.

Keywords – Authentication, privacy, PUF, RFID system.

I. INTRODUCTION

The radio frequency identification (RFID) technology has been implemented in many significant areas such as toll collection systems, identification, and tracking of various kinds of objects, consumer products, or access control. With the increasing usage of healthcare, electronic passports, and personal ID cards, the potential security threats and compliance risks have become enormous. In such a context, the need for secure and private communication protocols between readers and tags becomes crucial. Moreover, when developing such protocols, an account must be taken of the adversary model to which they should resist.

Traditionally, the RFID adversarial models did not take into account the tag corruption capability revealing the temporary state of tags. However, it has recently been shown that temporary state disclosure is practically possible. This raises the alarm about the security of the existing RFID protocols: are they still secure and private? A quick analysis of the protocols in [1], which achieve mutual authentication, shows that none of them achieve the claimed privacy level under corruption with temporary state disclosure. This does not even happen [2] with newer protocols like those in [3] and [4].

Contribution: In this paper, we develop an analysis of the security and privacy properties of RFID protocols under temporary state disclosure in Vaudenay's model. Thus, we discuss two fundamental protocols that ensure mutual authentication but lose the property of privacy when the adversary can obtain the temporary states of the tags (Section 3). Our analysis highlights the essence of the problem we face.

We then turn our attention to PUF technology (Section 4), which is probably the only one that can help obtain mutual authentication property and a good level of privacy under temporary state disclosure.

Finally (Sections 5 and 6), we discuss the level of destructive privacy and briefly present two of our recently developed schemes.

Related work: The pseudo-random function (PRF) based RFID scheme in [1] achieves weak privacy and mutual authentication in Vaudenay's model. It is straightforward to see that the proof in [1] works even in the case of corruption with temporary state disclosure. The first PUF-based RFID scheme that achieves destructive privacy and mutual authentication in Vaudenay's model (where corruption does not disclose the temporary state of tags) was proposed in [2], as an extension of the scheme in [5], [6] (that only achieves unilateral authentication).

In [3], [4], two PUF-based RFID schemes have been proposed and claimed that they achieve (narrow) destructive privacy and mutual authentication in Vaudenay's model with temporary state disclosure. Unfortunately, neither of them reaches even the narrow forward privacy level [2]. The RFID scheme in [2] provides mutual authentication and destructive privacy in Vaudenay's model. Moreover, [7] proposes a general method by which the RFID schemes from [3] and [4] can be fixed in terms of privacy. Undoubtedly, the most efficient RFID scheme that provides mutual authentication and destructive privacy in Vaudenay's model with temporary state disclosure is the one in [8]. A new novel RFID scheme that achieves mutual authentication and destructive privacy in Vaudenay's model with temporary state disclosure was recently proposed [9].

II. RFID SYSTEMS

RFID schemes: Let *R* be a *reader identifier* and *T* be a set of *tag identifiers* whose cardinal is polynomial in some security parameter λ. An RFID *scheme over* (*R,T*) [1], [10] is a triple *S = (SetupR, SetupT, Ident)* of PPT algorithms, where *SetupR* initializes the reader and its database *DB*, *SetupT* initializes a tag and stores a corresponding entry in *DB*, and *Ident* is an interactive protocol between the reader identified by *R* (with database *DB*) and a tag identified by *ID* (with state *S*). An *Ident* instance ends with output from both the reader (*ID* or ⊥) and the tag (⊥ or *OK*).

For mutual authentication RFID schemes, *correctness* 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, and the tag outputs *OK* with overwhelming probability.

Adversarial model: There have been several proposals for an adversarial model [1], [10], [11], [12], [13] for RFID schemes. In this paper, we follow *Vaudenay's model* [1], [10]. In this model, a tag can be either *drawn* or *free* based on adversarial access to the tag (proximity). An adversary can access a drawn tag only through a temporary unique identifier *vtag*.

The adversarial capabilities are modeled through oracles. The adversary can create tags (*CreateTag*), move a tag between the drawn and the free set of tags (*DrawTag*,*Free*), eavesdrop and manipulate de communication (*SendTag, SendReader*), obtain the internal state of a tag (*Corrupt*), and learn whether a particular protocol instance was successful (*Result*).

Based on access to the *Corrupt* oracle, adversaries are classified into: *weak* (no access to *Corrupt*), *forward* (no other oracles can be used after *Corrupt*), *destructive* (after corrupting a tag it is considered destroyed), and *strong* (no restrictions). Another class of adversaries, called *narrow*, is created when the adversary is denied access to the *Result* oracle. Combining this with the previous classes we obtain four more classes of adversaries: *narrow weak*, *narrow forward*, *narrow destructive*, and *narrow strong*.

Security: *Security* for RFID schemes is composed of two complementary notions: *tag authentication* and *reader authentication*. An RFID scheme has the property of *tag authentication* if no strong adversary has more than a negligible advantage in causing the reader to authenticate an uncorrupted legitimate tag in a protocol instance where the reader had no conversation with that tag to lead upon its authentication. An RFID scheme has the property of *reader authentication* if no strong adversary has more than a negligible advantage in causing an uncorrupted legitimate tag to authenticate the reader in a protocol instance where the tag had no conversation with the reader to lead upon its authentication.

Privacy: *Privacy* in Vaudenay's model generalizes anonymity (which means that the tag ID cannot be inferred) and untraceability (which means that the equality of two tags cannot be inferred). Thus, privacy requires that no adversary can infer non-trivial tag ID relations from the protocol messages. The information provided by a protocol is trivial when the adversary may learn it without making effective use of the protocol messages. To formalize this, Vaudenay's model introduces the concept of a *blinder* that simulates the protocol for adversary without knowing any secret information of the tags or the reader. If this simulation does not change the adversary's output compared to the case when the adversary plays with the real protocol, then the protocol achieves privacy.

III. PRIVACY AND MUTUAL AUTHENTICATION UNDER TEMPORARY STATE DISCLOSURE

When Vaudenay's model was proposed [10], it was somewhat unclear whether the *Corrupt* oracle returns the full (i.e., permanent and temporary) tag state or only the permanent one. This has also remained unclear in the next year's paper [1] on mutual authentication. While the distinction between full and permanent state did not have a negative impact on the results already obtained in the case of unilateral authentication, it highlighted several wrong results in the case of mutual authentication [14].

In the very interesting paper [14] a series of impossibility results were established, with respect to the privacy and mutual authentication in RFID schemes. One of them, namely Theorem 1, says that there is no RFID scheme that achieves both reader authentication and narrow forward privacy in Vaudenay's model with temporary state disclosure. The argument is as follows. Given a blinder *B*, one may construct an adversary *A* against reader authentication so that, if the scheme is narrow forward private then *A* has a non-negligible advantage to authenticate itself as a valid reader. Going inside the proof, we remark that it is

crucial the *Corrupt* oracle returns the full state of a tag in order to allow an adversary to perform the test by which the tag authenticates the reader. By this test, the adversary distinguishes with a non-negligible probability between the real privacy game and the blinded one.

In conclusion, none of the random oracle (RO) or public-key cryptography (PKC) based RFID schemes in [1] achieves mutual authentication and the privacy level claimed in [1] if Vaudenay's model allows corruption with temporary state disclosure.

The RO-based RFID scheme in [1], [10] needs a detailed discussion in order to understand why Theorem 1 applies to this case as well. To define this scheme, two public random oracles F and G that run two random functions, one from $\{0,1\}^{k+\ell}$ to $\{0,1\}^k$ and the other one from $\{0,1\}^k$ to $\{0,1\}^k$, are needed. The *SetupT(pk, ID)* algorithm creates a tag with the identity *ID* and a (permanent) state consisting of a key $K \leftarrow \{0,1\}^k$. The pair (*ID, K*) is stored in the reader's database *DB*. The reader and all tags are granted (secure) access to the oracles F and G. One may also think that copies of these oracles are distributed to the reader and all tags. The interactive protocol *Ident* is pictorially represented in Figure 1.

Now, we have to clarify what corruption means in the case of this protocol. As F and G are public random oracles, the adversary is granted access to them as well.

The *Corrupt* oracle returns only the tag state but not the internal structure of the oracles F and G (which are thought of as black boxes). Therefore, an adversary that corrupts a tag and gets a state $G(K)$ will not be able to "inverse" this value or to do any other computation derived from the internal structure of these oracles, except with negligible probability. This is somewhat opposite to pseudo-random functions whose internal structure is supposed to be known. For instance, if we consider the candidate pseudo-random function $DES = (DES_K)_{K\in\{0,1\}^{64}}$, a key K, and a cyphertext $c = DES_K(x)$, one may efficiently compute the plaintext x.

	Reader (DB, F, G)		**Tag** (F, G, K)
1	$x \leftarrow \{0,1\}^\ell$	$\xrightarrow{x}$	
2		$\xleftarrow{z}$	$z = F(0, K, x)$, $w' = F(1, K, x)$, $K = G(K)$
3	If $\exists (ID, K) \in DB$ and $0 \le i < t$ s.t. $z = F(0, G^i(K), x)$ then output ID, $K = G^i(K)$, $K' = K$ else output $\perp$, $K' \leftarrow \{0,1\}^k$ $w = F(1, K', x)$	$\xrightarrow{w}$	
			If $w = w'$ then output OK else output $\perp$

Figure 1. RO based RFID scheme in [1]

In conclusion, an adversary that corrupts a tag and gets its key K may get $F(K, x)$ and $G(K)$ by querying the oracles F and G (but not by corrupting them). Therefore, the tag can perfectly be simulated by an adversary, and Theorem 1 in [14] can be applied in this case (in fact, the adversary only needs to know w' in order to do the tag's test in the last step).

IV. RFID DESIGN BASED ON PUF TAGS

A *physically unclonable function* (PUF) can be seen as 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* (indistinguishable on their challenge/response behavior), *unpredictable* (infeasible to predict the response to an unknown challenge), and *tamper-evident* (any attempt to physically access the PUF irreversible changes its behavior).

From a theoretical point of view, a 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 λ, such that P is computationally indistinguishable from U and any attempt to physically tamper with the object implementing P results in the destruction of P (P cannot be evaluated any more).

The newest RFID technologies allow *PUF tags* that are tags with PUFs inside them. In order to adapt Vaudenay's model (with or without temporary state disclosure) to RFID schemes with PUF tags, we have to clarify what corruption means in this case. At least two main scenarios are possible:

1) Any corruption on a PUF tag destroys the tag. By corruption, one gets the (full) state except for the values computed by the PUF (assuming that they were not saved in the tag's memory);
2) The PUF tag is destroyed by corrupting it, but some values returned by its PUFs are obtained (an example in this sense is the *cold boot attack* in [15] according to which the tag may be frozen at some time to obtain the PUF value).

The first scenario is the most used one and it is the one adopted in our paper. As the corruption of PUF-based tags

does not reveal the full tag state, PUF tags cannot generally be simulated by adversaries. Working in this scenario, Theorem 1 in [14], at least in its present form, cannot be applied to RFID schemes with PUF tags. This leaves open the invitation to design RFID schemes that achieve mutual authentication and higher privacy levels than narrow forward in Vaudenay's model with temporary state disclosure. As we have already said, such schemes cannot be based on ordinary tags. A good choice is to use PUF tags, as it was done in [2], [3], [4], [5], [6]. However, the use of PUF tags does not mean that the schemes are immune to corrupting adversaries. This is because an adversary might not need the entire tag state to attack the scheme. An example in this sense is provided in [2] where it was shown that the RFID schemes proposed in [3], [4] do not achieve mutual authentication and (narrow) destructive privacy in Vaudenay's model with temporary state disclosure, as it was claimed by authors, although they use PUF tags. The proof exploits the fact that these schemes use volatile variables to carry values between protocol steps.

The second scenario was touched on by several research papers such as [3], [4], and [15]. We are not aware of any formal treatment of this scenario in Vaudenay's model. To implement this scenario in Vaudenay's model, the *Corrupt* oracle should be changed to return snapshots of the tag's state during its computation (recall that the standard *Corrupt* oracle returns the tag's state before or after a protocol step). A formal and complete treatment of such corruption seems hard to reach; on the other side, such corruption is very strong, and probably no PUF-based RFID scheme may achieve a privacy level higher than (narrow) weak under such corruption. However, special cases may be relevant. One of them is the cold boot attack mentioned above. To defeat it, a PUF double evaluation technique was proposed in [15], which consists of two evaluations in a row of the same PUF. If the attack is applied immediately after the first PUF evaluation, the second PUF evaluation is lost, and vice-versa. This technique was implemented in two RFID schemes [3], [4]. Unfortunately, the authors did not pay much attention to the volatile variables, which made their schemes not achieve even the narrow forward privacy level [2].

Recall that a (narrow) strong adversary may corrupt a tag multiple times. However, working in the first corruption scenario mentioned above (with PUF tags), (narrow) strong adversaries become in fact (narrow) destructive. This is because corruption destroys the PUF tag and, therefore, it cannot be further used. Therefore, Vaudenay's model (with or without temporary state disclosure) for RFID schemes with PUF tags is limited to at most (narrow) destructive privacy.

The PRF-based RFID scheme in [1] achieves mutual authentication and weak privacy in Vaudenay's model with temporary state disclosure. This simply follows from the proof in [1] together with the remark that weak adversaries are not allowed to corrupt tags.

V. DESTRUCTIVE PRIVACY AND READER-FIRST AUTHENTICATION

An interesting question that arises when designing mutual authentication RFID schemes is whether the tag or the reader should be authenticated first. We have thus two approaches: *tag-first* and *reader-first authentication*, respectively [16]. The *tag-first authentication* has some advantages with respect to desynchronization: the tag computes its new state and sends information about it to the reader. However, the tag state is updated only when the reader authenticates the tag and confirms the new state to the tag. The disadvantage of this approach is that the tag should provide some information to the reader before it is confident of the reader's identity.

The *reader-first authentication* might enhance the tag privacy because the tag gives private information to the reader when it is confident of its identity. This also might help prevent adversaries from tracking tags. Another advantage is when the tag is designed only for a limited number of authentications. In such a case, the reader-first approach prevents a form of denial of service attack that would "consume" all the tag's authentication answers.

In [9], a destructive private and mutual authentication RFID scheme in Vaudenay's model with temporary state disclosure was proposed. For mutual authentication it follows the reader-first approach and, according to our discussion in Section 3, all tags are endowed with PUFs.

To describe our scheme, let us assume that λ is a security parameter, $\ell_1(\lambda)$ and $\ell_2(\lambda)$ are two polynomials, and $F = (F_K)_{K \in \mathcal{K}}$ is a pseudo-random function, where $F_K : \{0, 1\}^{2\ell_1(\lambda)+2} \rightarrow \{0, 1\}^{\ell_2(\lambda)}$ for all $K \in \mathcal{K}_\lambda$. Each tag is equipped with a (unique) PUF $P : \{0, 1\}^{p(\lambda)} \rightarrow \mathcal{K}_\lambda$ and has the capacity to compute F, where $p(\lambda)$ is a polynomial. The internal state of the tag consists of a pair (s, x), where $s \in \{0, 1\}^{p(\lambda)}$ is randomly chosen as a seed to evaluate P, and $x \in \{0, 1\}^{\ell_1(\lambda)}$ is a random string used as a "dynamic" identifier of the tag. The reader maintains a database *DB* with entries for all legitimate tags. Each entry is a vector (ID, K, x), where *ID* is the tag's identity and $K = P(s)$, where P is the tag's PUF and (s, x) is its state.

The mutual authentication protocol is given in Figure 2. Remark that if the reader does not update x (because it rejects the tag), then it will do so in step 2 of the next protocol session (with the same tag). Therefore, the desynchronization between reader and tag is at most one step.

Theorem 5.1. ([9]) The RFID scheme in Figure 2 is correct ad achieves mutual authentication and destructive privacy in Vaidenay's model with temporary state disclosure, provided that F is a pseudo-random function and the tags are endowed with ideal PUFs.

VI. NARROW DESTRUCTIVE PRIVACY AND READER FIRST AUTHENTICATION

With little effort, the RFID scheme in Figure 2 can be simplified to a narrow destructive private and reader-first authentication RFID scheme in Vaudenay's model with temporary state disclosure. The mutual authentication protocol of this new RFID scheme is presented in Figure 3; all the other elements are as in Section 5, except that F_K is a function from $\{0,1\}^{\ell_1(\lambda)+2}$ to $\{0,1\}^{\ell_2(\lambda)}$ and t is polynomial in the security parameter. As one can see, there is no random generator on the tag. Because of this, the synchronization between tag and reader can be lost. The only thing we can do is to check (on the reader side) for a polynomial bounded desynchronization. Due to this, the scheme can be at most narrow destructive private: if an adversary desynchronizes the tag and reader sufficiently enough (for more than t steps), then it will be able to distinguish the real privacy game from the blinded one by means of the *Result* oracle. Roughly speaking, this is because in the real privacy game the *Result* oracle returns 0 (when the tag and reader are desynchronized for more than t steps), while in the blinded privacy game it returns 1.

	Reader (DB, F)		**Tag** (P, s, F, x)
1			$u \leftarrow \{0,1\}^{\ell_1(\lambda)}$, $K = P(s)$
		$\xleftarrow{u,z}$	$z = F_K(0,0,u,x)$
			erase K, u, z
2	If $\exists (ID, K, x) \in DB$ and $i \in \{0,1\}$		
	s.t. $z = F_K(0,0,u,x+i)$		
	then $v \leftarrow \{0,1\}^{\ell_1(\lambda)}$, $x = x + i$		
	$w = F_K(0,1,v,x)$		
	else $v \leftarrow \{0,1\}^{\ell_1(\lambda)}$, $w \leftarrow \{0,1\}^{\ell_2(\lambda)}$		
		$\xrightarrow{v,w}$	
3			$K = P(s)$, $w' = F_K(0,1,v,x)$
			If $w = w'$
			then $x = x + 1$, $w' = F_K(1,1,v,x)$
		$\xleftarrow{w'}$	else $w' \leftarrow \{0,1\}^{\ell_2(\lambda)}$
			erase K, v, w, w'
4	If $w' = F_K(1,1,v,x+1)$		
	then output ID, $x = x + 1$		
	else output $\perp$		

Figure 2. Destructive private and reader-first authentication PUF based RFID scheme in Vaudenay's model with temporary state disclosure

Theorem 6.1. ([9]) The RFID scheme in Figure 3 achieves mutual authentication and narrow destructive privacy in Vaudenay's model with temporary state disclosure, provided that F is a PRF and the tags are endowed with ideal PUFs.

It is good to remark that our RFID scheme in Figure 3 also provides an appropriate practical solution to the narrow destructive privacy in the plain Vaudenay's model, where the existing solution is based on random oracles.

A few more words on desynchronization are in order. If we look at the protocol in Figure 3 we remark that the desynchronization is a result of the fact that the tag and reader share a common variable x that is updated by the tag before authenticating the reader. This allows an adversary to query a tag more than t times and, therefore, to desynchronize the tag and the reader.

To prevent desynchronization between reader and tag in reader-first authentication RFID schemes, the tag should update the shared permanent variables after authenticating the reader, and not before.

VII. CONCLUSIONS

Modern applications of RFID systems ask for advanced security and privacy properties. For instance, tag destruction under corruption is an important requirement when the tag is used for access control. Likewise, the disclosure of temporary state under tag corruption is a serious threat in practice. Reader-first authentication [16] assures that the tag will give its private data only when it authenticates the reader. Therefore, tag tracking and data theft are prevented when the reader is fake. All these together mean that we need RFID schemes that provide destructive privacy and reader-first authentication under corruption with temporary state disclosure.

In this paper, we amply discussed how temporary state disclosure affects mutual authentication and privacy of RFID protocols. We argued then in favor of using the PUF technology in order to achieve mutual authentication and a reasonable enough level of privacy under temporary state disclosure. Finally, we presented two RFID schemes that achieve destructive

privacy, one of the most important levels of privacy in the context of the physical corruption of tags.

REFERENCES

[1] R.-I. Paise and S. Vaudenay, "Mutual authentication in RFID: Security and privacy," in Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '08. New York, NY, USA: ACM, 2008, pp. 292–299.

[2] C. Hristea and F. L. Țiplea, "Destructive privacy and mutual authentication in Vaudenay's RFID model," Cryptology ePrint Archive, Report 2019/073, 2019, https://eprint.iacr.org/2019/073.

[3] S. Kardaş, S. Ç elik, M. Yildiz, and A. Levi, "PUF-enhanced offline RFID security and privacy," J. Netw. Comput. Appl., vol. 35, no. 6, pp. 2059–2067, Nov. 2012.

[4] M. Akgun and M. U. Ç aglayan, "Providing destructive privacy ¨ and scalability in RFID systems using PUFs," Ad Hoc Netw., vol. 32, no. C, pp. 32–42, Sep. 2015.

[5] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, "PUF-enhanced RFID security and privacy," in Workshop on secure component and system identification (SECSI), vol. 110, 2010.

[6] ——, Enhancing RFID Security and Privacy by Physically Unclonable Functions. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 281–305.

[7] F. L. Țiplea and C. Hristea, "PUF protected variables: A solution to rfid security and privacy under corruption with temporary state disclosure," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 999–1013, 2021.

[8] F. L. Țiplea and C. Hristea, "Practically efficient RFID scheme with constant-time identification," in Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021, July 6-8, 2021, S. D. C. di Vimercati and P. Samarati, Eds. SCITEPRESS, 2021, pp. 495–506. [Online]. Available: https://doi.org/10.5220/0010544804950506

[9] F. L. Țiplea, C. Hristea, and R. Bulai, "Privacy and reader-first authentication in Vaudenay's RFID model with temporary state disclosure," Computer Science Journal of Moldova, vol. (to appear).

[10] S. Vaudenay, "On privacy models for RFID," in Proceedings of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security, ser. ASIACRYPT'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 68–87.

[11] A. Juels and S. A. Weis, "Defining strong privacy for RFID," ACM Trans. Inf. Syst. Secur., vol. 13, no. 1, pp. 7:1–7:23, Nov. 2009.

[12] J. Hermans, F. Pashalidis, Andreasand Vercauteren, and B. Preneel, "A new RFID privacy model," in Computer Security – ESORICS 2011, V. Atluri and C. Diaz, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 568–587.

[13] J. Hermans, R. Peeters, and B. Preneel, "Proper RFID privacy: Model and protocols," IEEE Transactions on Mobile Computing, vol. 13, no. 12, pp. 2888–2902, Dec 2014.

[14] F. Armknecht, A.-R. Sadeghi, A. Scafuro, I. Visconti, and C. Wachsmann, "Impossibility results for RFID privacy notions," in Transactions on Computational Science XI, M. L. Gavrilova, C. J. K. Tan, and E. D. Moreno, Eds. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 39–63.

[15] S. Kardaş, M. S. Kiraz, M. A. Bingol, and H. Demirci, "A novel ¨ RFID distance bounding protocol based on physically unclonable functions," in RFID. Security and Privacy, A. Juels and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 78–93.

[16] R. Peeters, J. Hermans, and J. Fan, "IBIHOP: Proper privacy preserving mutual RFID authentication," in The 2013 Workshop on Radio Frequency Identification/Internet of Things Security (RFIDsec'13 Asia), ser. Cryptology and Information Security Series, C. Ma and J. Weng, Eds., vol. 11. IOS Press, 2013.

	Reader (DB, F)		**Tag** (P, s, F, x)
1		$\xleftarrow{z}$	$K = P(s)$ $z = F_K(0, 0, x)$ erase K, z $x = x + 1$
2	If $\exists (ID, K, x) \in DB$ and $0 \leq i < t$ s.t. $z = F_K(0, 0, x + i)$ then $x = x + i$, $w = F_K(0, 1, x + 1)$ else $w \leftarrow \{0, 1\}^{\ell_2(\lambda)}$	$\xrightarrow{w}$	
3		$\xleftarrow{w'}$	$K = P(s)$ If $w \neq F_K(0, 1, x)$ then $w' = F_K(1, 1, x)$ else $w' \leftarrow \{0, 1\}^{\ell_2(\lambda)}$ erase K, w, w'
	If $w' = F_K(1, 1, x + 1)$ then output ID, $x = x + 1$ else output $\perp$		

Figure 3. Narrow destructive private and reader-first authentication PUF based RFID scheme in Vaudenay's model with temporary state disclosure