On Privacy Models for RFID

Serge Vaudenay

EPFL
CH-1015 Lausanne, Switzerland
http://lasecwww.epfl.ch

Abstract. We provide a formal model for identification schemes. Under this model, we give strong definitions for security and privacy. Our model captures the notion of a powerful adversary who can monitor all communications, trace tags within a limited period of time, corrupt tags, and get side channel information on the reader output. Adversaries who do not have access to this side channel are called narrow adversaries. Depending on restrictions on corruption, adversaries are called strong, destructive, forward, or weak adversaries. We derive some separation results: strong privacy is impossible. Narrow-strong privacy implies key agreement. We also prove some constructions: narrow-strong and forward privacy based on a public-key cryptosystem, narrow-destructive privacy based on a random oracle, and weak privacy based on a pseudorandom function.

1 The Privacy Issue in RFID Schemes

RFID protocols are used to identify cheap tags through wireless channels. However, putting tags in wearable items leads to privacy concerns. Although several privacy models exist so far, all have their own limitations, and finally, the classes of protocols that achieve privacy for one model or the other are not always comparable. A widely accepted flexible model permitting to establish a common measure of the performance of identification protocol is still under construction. We aim at contributing to this effort. To do so, we propose formal definitions of RFID schemes and adversaries and consider a twofold characterization of a scheme in terms of *security* and *privacy*. The former assesses the soundness of tag authentication. The latter property is for the ability to resist to adversaries aiming at identifying, tracing, or linking tags.

In a nutshell, we formalize several types of privacy and study inherent limitations for RFID applications. We discuss which restrictions we can assume regarding tag corruption and availability of side channels. We show how to achieve those levels of privacy and what must be used in terms of conventional vs. public-key cryptography or stateless vs. rewritable tags. We show that the strongest possible level of privacy implies key agreement, thus mandating the use of some public-key cryptography techniques. We present a simple protocol for that.

We assume a *powerful adversary* who can control all communications and interfere with the system. Cheap tags are not tamper-resistant so we analyze the ability to assure privacy and security even when an adversary is allowed to *corrupt* tags and retrieve the internal state. One novelty of our models is that they provide some kind of "exposure slots". Namely, adversaries can trace a tag within a limited time period during which this tag remains at the vicinity of the adversary. During this period, they can refer to the tag by using a temporary identity. In practice, this temporary identity can be the 32-bit number that is used in ISO/IEC 14443-3 norm [22] in singulation protocols for collision avoidance [4]. It can also be some tag named from its radiation pattern signature [21]. Exposure time periods are indeed unavoidable.

We consider several types of restrictions regarding tag corruption. The weakest model does not allow corruption. The relevant model for the so-called *forward privacy* allows corruption, but only at the end of the attack so that no further active action happens after corruption.[1] One less restrictive (thus stronger) model tolerates corruption at any time, but assumes that opening a tag destroys it so that it no longer circulates in nature. This model is called *destructive*. Our strongest model allows corruption at any time and even to put the tag back to nature so that tracing it is still considered as a threat. Although the purpose for distinguishing those two latter models is not clear, we prove that they separate.

Another question, as studied in Juels-Weis [24], is whether the adversary has access to the protocol partial output or not. Namely, can we consider that the adversary knows whether a reader succeeded to identify a legitimate tag or not? We call *narrow* adversaries those who do not have access to this information while "wider" adversaries can get it from side channels (e.g. the question whether a door opens or not). It is well known that security or privacy can collapse in such a case (e.g. for the HB+ protocol [17,23,25] or the OSK protocol [24,30]). It happens to be quite orthogonal to the corruption variants so that we obtain an array of $4 \times 2 = 8$ adversarial models. We prove that those privacy models are pairwise different.

Related work. Many simple challenge-response protocols have been proposed without addressing corruption [14,28,39]. The Ohkubo-Suzuki-Kinoshita protocol (OSK) [30,31] (see also [3,12,32]) made forward privacy possible. A few attempts have been made to really formalize privacy in RFID protocols. One of the first attempts was made by Avoine-Dysli-Oechslin [3], later extended in the Thesis of Avoine [2]. Following their model, privacy is formalized by the ability to distinguish two known tags. The model excludes the availability of side-channel information such as whether a protocol instance on the reader did succeed. Juels and Weis [24] extended this model using side-channel information and making the two target tags chosen by the adversary. Another model was proposed by Burmester, van Le, and de Medeiros [8,26]. In all these models, corrupted tags cannot be the target of privacy adversaries. Another approach by Damgård-Østergaard [10] studies RFID schemes "with symmetric cryptography only" to focus on the tradeoffs between complexity and security.

[1] Note that some authors call this notion *backward privacy* [27]. Their notion of *forward privacy* is included in our notion of strong privacy.

Our contribution. In this paper we present a complete formalism for defining RFID schemes, their security, and build a hierarchy of privacy models. Our definition for security is equivalent to Damgård-Østergaard [10]. We prove that security against strong adversaries can be easily achieved using a pseudorandom function family. We prove that strong privacy is impossible. We show that an RFID scheme that achieves narrow-strong privacy can efficiently be transformed into a key agreement protocol, meaning that this type of privacy essentially needs public-key cryptography techniques. On the other hand, we show that a public-key cryptosystem that resists to adaptively chosen ciphertext attacks can be used to define a simple narrow-strong private and forward private protocol. We further prove the narrow-destructive privacy of an OSK-like protocol [31] in the random oracle model and the weak privacy of a classical challenge-response protocol based on a pseudorandom function. This work follows up some joint work during the Thesis of Bocchetti [7].

2 Definitions

In the sequel, a function in terms of a security parameter s is said *polynomial* if there exists a constant n such that it is $\mathcal{O}(s^n)$. Similarly, a function is said *negligible* if there exists a constant $x > 0$ such that it is $\mathcal{O}(x^{-s})$. For the sake of readability we concentrate on asymptotic complexities and security although all our results can be written with more precise bounds.

The tag is a passive transponder identified by a unique ID. We typically focus on a cheap tag which is *passive*: it has no batteries, it can operate just when interrogated by a reader and only for a short time. It has *limited memory*: each tag has only a few Kbit of memory on board. It has *limited computational abilities*. Each tag can perform only basic cryptographic calculations: hash calculations [15], pseudorandom generation [35], symmetric encryption [14]. Some elliptic-curve arithmetic [5] and zero-knowledge identification [9,18,19] may fit, as well as public-key cryptography [1,16,38], but remain expensive so far. It is *not tamper proof*. It communicates at up to a limited *distance*: the communication Tag→Reader is limited to a few meters (if not centimeters).

The reader is a device composed by one or more transceivers and a backend processing subsystem. Security issues within the reader are not addressed in this work, moreover we focus on single backend readers. Note however that sometimes in literature "reader" denotes the transceiver alone. The purpose of the reader is to interact with tags so that it can tell legitimate tags (i.e. tags which are registered in the database) and unknown tags apart, and further identify (i.e. infer their ID) legitimate tags.

Definition 1 (RFID Scheme). *An RFID scheme is composed by*

– *a setup scheme* $\mathsf{SetupReader}(1^s)$ *which generates a private/public key pair* (K_S, K_P) *for the reader depending on a security parameter* s*. The key* K_S *is to be stored in the reader backend. The key* K_P *is publicly released. Throughout this paper we assume that* s *is implicitly specified in* K_P *so that there is no need to mention* s *any longer.*

– *a polynomial-time algorithm* $\mathsf{SetupTag}_{K_P}(\mathsf{ID})$ *which returns* (K, S)*: the tag specific secret* K *and the initial state* S *of the tag. The pair* (ID, K) *is to be stored in the reader backend when the tag is legitimate.*
– *a polynomial-time interactive protocol between a reader and a tag in which the reader ends with a tape* Output*.*

An RFID scheme is such that the output is correct except with a negligible probability for any polynomial-time experiment which can be described as follows.

1: set up the reader
2: create many tags including a subject one named ID
3: execute a complete protocol between reader and tag ID

The output is correct if and only if $\mathsf{Output} = \perp$ *and tag* ID *is not legitimate, or* $\mathsf{Output} = \mathsf{ID}$ *and* ID *is legitimate.*

When $\mathsf{Output} = \perp$ but tag ID is legitimate, we have a *false negative*. When $\mathsf{Output} \neq \perp$ but tag ID is not legitimate, we have a *false positive*. When $\mathsf{Output} \notin \{\mathsf{ID}, \perp\}$ and tag ID is legitimate, we have an *incorrect identification*.

The RFID scheme is *stateless* if the tag state S is not allowed to change in time. Note that we do not a priori assume that tags know their ID nor their secret K: this is up to the protocol specification to make them extractable from S. We assume that a reader can run several concurrent instances of a protocol but that tags cannot. In this paper, we do not consider reader authentication so we do not consider any output on the side of the tag.[2]

In practice, some information about Output may leak from a side channel (e.g. by observing a door opening at a tag transit and deducing that authentication was successful). Having access to such an information could allow an adversary to gather information about tag identities. For simplicity, we focus here on passive tags which are exempt of side channel except by full corruption.

2.1 Adversaries

The characterization of the adversary is essentially done by specifying the actions that she is allowed to perform (i.e. the *oracles* she can query), the goal of her attack (i.e. the *game* she plays) and the way in which she can interact with the system (i.e. the *rules* of the game). We consider that, at every time, a tag can either be a *free tag* or a *drawn tag*. Drawn tags are the ones within "visual contact" to the adversary so that she can communicate while being able to link communications. Free tags are all the other tags. Two oracles are defined below to draw or free tags. We call *virtual tag* a unique reference (e.g. using a drawing sequence number or a nonce) to the action of drawing a tag. This plays the same role as a *temporary identity*. Note that two different virtual tags may refer to the same tag that has been drawn, freed, and drawn again.

[2] This model was extended for mutual authentication in the Thesis of Paise [33].

Definition 2 (Adversary). *An adversary is an algorithm which takes a public key K_P as input and runs by using the eight following oracles.*

- $\textsc{CreateTag}^b(\mathsf{ID})$*: creates a free tag, either legitimate ($b = 1$) or not ($b = 0$), with unique identifier* ID*. This oracle uses* $\mathsf{SetupTag}_{K_P}$ *algorithm to set up the tag and (for $b = 1$ only) to update the system database. By convention, b is implicitly 1 when omitted.*
- $\textsc{DrawTag}(\mathsf{distr}) \to (\mathsf{vtag}_1, b_1, \ldots, \mathsf{vtag}_n, b_n)$*: moves from the set of free tags to the set of drawn tags a tuple of tags at random following the probability distribution* distr *(which is specified by a polynomially bounded sampling algorithm). The oracle returns a vector of fresh identifiers* $(\mathsf{vtag}_1, \ldots, \mathsf{vtag}_n)$ *which allows to anonymously designate these tags. Drawing tags already drawn or not existing provoke the oracle to return $\perp$ in place of the respective virtual tag. We further assume that this oracle returns bits $(b_1, \ldots, b_n)$ telling whether the drawn tags are legitimate or not.*[3] *This oracle keeps a hidden table $\mathcal{T}$ such that $\mathcal{T}(\mathsf{vtag})$ is the* ID *of* vtag.
- $\textsc{Free}(\mathsf{vtag})$*: moves the virtual tag* vtag *back to the set of the free tags. This makes* vtag *unreachable. (That is, using* vtag *in oracle calls is no longer allowed.)*
- $\textsc{Launch} \to \pi$*: makes the reader launch a new protocol instance π.*
- $\textsc{SendReader}(m, \pi) \to m'$ *(resp.* $\textsc{SendTag}(m, \mathsf{vtag}) \to m'$*): sends a message m to a protocol instance π for the reader (resp. to virtual tag* vtag*) and receives the answer m' (that is meant to be sent to the counterpart). By convention we write* $\textsc{Execute}(\mathsf{vtag}) \to (\pi, \mathsf{transcript})$ *to group one* Launch *query and successive use of* SendReader *and* SendTag *to execute a complete protocol between the reader and the tag* vtag*. It returns the transcript of the protocol, i.e. the list of successive protocol messages.*
- $\textsc{Result}(\pi) \to x$*: when π is complete, returns 1 if* $\mathsf{Output} \neq \perp$ *and 0 otherwise.*
- $\textsc{Corrupt}(\mathsf{vtag}) \to S$*: returns the current state S of the tag. If* vtag *is no longer used after this oracle call, we say that* vtag *is* destroyed.

The adversary plays a game *which starts by setting up the RFID system and feeding the adversary with the public key. The adversary uses the oracle following some* rules *of the game and produces an output. Depending on the rules, the adversary* wins *or* looses.

Definition 3 (Strong, destructive, forward, weak, and narrow adversary). *We consider polynomial-time adversaries. Let* STRONG *be the class of adversaries who have access to the above oracles. Let* DESTRUCTIVE *be the class of adversaries who never use* vtag *again after a* $\textsc{Corrupt}(\mathsf{vtag})$ *query (i.e. who destroy it). Let* FORWARD *be the class of adversaries in which* Corrupt *queries can only be followed by other* Corrupt *queries. Let* WEAK *be the class of adversaries who do no* Corrupt *query. Let* NARROW *be the class of adversaries who do no* Result *query.*

[3] Namely, we assume that adversaries always have means to deduce whether a tag is legitimate or not by side channels.

Clearly, we have $\mathsf{WEAK} \subseteq \mathsf{FORWARD} \subseteq \mathsf{DESTRUCTIVE} \subseteq \mathsf{STRONG}$.

2.2 Security of RFID Schemes

Definition 4 (Security). *We consider any adversary in the class* STRONG*. We say the adversary wins if at least one protocol instance* π *on the reader identified an uncorrupted legitimate tag* ID *but* π *and* ID *did not have any matching conversation, i.e. they exchanged well interleaved and faithfully (but maybe with some time delay) transmitted messages until* π *completed. We call* ID *a target tag and* π *a target instance. We say that the RFID scheme is secure if the success probability of any such adversary is negligible.*

All protocols that we study here are two-pass protocols in which the reader starts by sending a random challenge a and the tag produces a response c depending on a. This way, attacks leading to matching protocol transcripts but badly interleaved messages have negligible probability of success.

We use the following lemma to prove security of RFID schemes in our paper.

Lemma 5 (Simple security for special RFID scheme). *We consider an RFID scheme for which the reader protocol satisfies the following structure. First, the communication messages from the reader do not depend on the database. Second, there is a predicate* R *and a sampling algorithm* $\mathcal{S}$ *such that the output is computed by running* $\mathcal{S}$ *on the set* $\mathcal{E}$ *of all* ID *corresponding to a database entry* (ID, K) *verifying* $R(\mathsf{ID}, K; \tau)$*, where* τ *is the protocol transcript. We assume that* R *and* $\mathcal{S}$ *do not use the database (but may use the secret key* K_S*). Third, the selected database entry may be updated by an extra algorithm not depending on other database entries or* K_S*. The algorithm* $\mathcal{S}$ *is such that*

- *if* $\mathcal{E} = \emptyset$ *then* $\mathcal{S}(\mathcal{E}) = \perp$
- *if* $\mathcal{E} \neq \emptyset$ *then* $\mathcal{S}(\mathcal{E})$ *outputs an element of* $\mathcal{E}$*.*

Finally, we assume that there exists an easily computable predicate R' *such that if a tag* ID *and the reader have a matching conversation with transcript* τ *and if* (ID, K) *is a database entry then* $R(\mathsf{ID}, K; \tau) \iff R'(n)$ *where* n *is the number of previously completed protocol executions on the tag* ID *side since the last succeeded one. (A protocol execution with* ID *is called succeeded if it has a matching conversation with the reader with output* ID*.) We consider adversaries who*

- *create (and draw) a single tag* ID
- *use* Launch*,* SendReader*,* SendTag
- *use an oracle who checks the predicate* R *on inputs different from* ID
- *use an oracle simulating* $\mathcal{S}$
- *end on a final* SendReader *to an instance* π*.*

The adversary wins if the protocol instance π *on the reader identified tag* ID *but has no matching conversation. We say that the scheme is simply secure if the success probability of any such adversary is negligible. If the scheme is simply secure, then it is secure.*

Proof (Sketch). Let $\mathcal{A}$ be a strong adversary playing the security game. We can simulate DrawTag and Free queries and reduce to adversaries who draw tags once for all upon creation. Next, we can reduce to an adversary who guesses the first target tag ID upon creation, as well as the first target instance π. (The success probability is divided by a polynomially bounded factor.) Then, we can simulate all tags except ID so that only tag ID is really created. We show by induction that Output can be generated with same distribution (except on π) when the adversary knows all database entries except (ID, K). To compute $R(\mathsf{ID}, K; \tau)$ without knowing K, if τ is non-matching then R is not satisfied, otherwise R' can be used. We can thus simulate the reader and Result queries. One trick is not to send the last message to a reader instance if the simulated output is not ID and to send it otherwise so that the database entry can be updated. By using the simple security we deduce that $\mathcal{A}$ has negligible success probability. The scheme is thus secure. $\square$

2.3 Privacy of RFID Schemes

RFID schemes are given three cryptographic properties: correctness, security, and privacy. Depending on the application, not all properties may be required. Correctness is part of the definition of RFID schemes and is implicitly assumed. Security (i.e. soundness of tag identification) is defined in Section 2.2. We define privacy in terms of ability to infer non-trivial ID relations from protocol messages. This generalizes the notion of *anonymity* (for which the ID of tags cannot be inferred) and *untraceability* (for which the equality of two tags cannot be inferred).

Definition 6 (Privacy). *We consider adversaries who start with an attack phase allowing oracle queries then pursuing an analysis phase with no oracle query. In between phases, the adversary receives the hidden table $\mathcal{T}$ of the* DrawTag *oracle then outputs either* true *or* false*. The adversary wins if the output is* true*. We say that the RFID scheme is P-*private *if all such adversaries which belong to class P are trivial following Def. 7.*

Definition 7 (Blinder, trivial adversary). *A Blinder B for an adversary $\mathcal{A}$ is a polynomial-time algorithm which sees the same messages as $\mathcal{A}$ and simulates the* Launch, SendReader, SendTag, *and* Result *oracles to $\mathcal{A}$. The blinder does not have access to the reader tapes so does not know the secret key nor the database. A blinded adversary $\mathcal{A}^B$ is itself an adversary who does not use the* Launch, SendReader, SendTag, *and* Result *oracles. An adversary $\mathcal{A}$ is* trivial *if there exists a B such that $|\Pr[\mathcal{A} \text{ wins}] - \Pr[\mathcal{A}^B \text{ wins}]|$ is negligible.*

Informally, an adversary is trivial if it makes no effective use of protocol messages. Namely, these messages can be simulated without significantly affecting the success probability of the adversary. We stress that our privacy notion measures the privacy loss in the wireless link but not through tag corruption (since Corrupt queries are not blinded). In other words, we assume that corrupting a tag always compromise privacy and we only focus on wireless leakage.

Clearly, we have the following links between privacy notions.

$$
\begin{array}{ccccccc}
\text{strong} & \Rightarrow & \text{destructive} & \Rightarrow & \text{forward} & \Rightarrow & \text{weak} \\
\Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\
\text{narrow-strong} & \Rightarrow & \text{narrow-destructive} & \Rightarrow & \text{narrow-forward} & \Rightarrow & \text{narrow-weak}
\end{array}
$$

We will show separation between all those notions. We summarize below the non-implications with a reference to the appropriate notes.

$$
\begin{array}{ccccccc}
\text{strong} & & \text{destructive} & \overset{\text{Note 10}}{\not\Leftarrow} & \text{forward} & \overset{\text{Note 14}}{\not\Leftarrow} & \text{weak} \\
\not\Uparrow \text{ Note 10} & & \not\Uparrow \text{ Note 18} & & \not\Uparrow \text{ Note 18} & & \not\Uparrow \text{ Note 18} \\
\text{narrow-strong} & \overset{\text{Note 16}}{\not\Leftarrow} & \text{narrow-destructive} & \overset{\text{Note 17}}{\not\Leftarrow} & \text{narrow-forward} & \overset{\text{Note 14}}{\not\Leftarrow} & \text{narrow-weak}
\end{array}
$$

Some non-implication results may assume the existence of standard primitives such as IND-CCA public-key cryptosystems, random oracles, or pseudorandom functions. The non-implication of destructive privacy to strong privacy is equivalent to the feasibility of destructive privacy which is open so far.

In this model, corrupted tags can be the victims of tracing attacks, contrarily to the model of Juels-Weis [24] and Burmester-van Le-de Medeiros [8]. For instance, the protocol O-TRAP provides privacy in the sense of [8]. In this protocol, the reader sends a r^t_{sys} challenge to the tag and the tag answers with some random r_i and $h_{K_i}(r^t_{sys}, r_i)$ where h is a keyed hash function and K_i is a key which is permanently stored in the tag state. Clearly, corrupting the tag reveals K_i that was used in former protocols and enables to identified the tag in previous sessions. Hence, O-TRAP is not narrow-forward private.

We provide a useful lemma to get rid of Result queries.

Lemma 8. *We consider an RFID scheme with the property that whenever a legitimate tag and the reader have some matching conversation, the reader does not output $\perp$. If the scheme is secure, then narrow-forward (resp. narrow-weak) privacy implies forward (resp. weak) privacy.*

Proof (Sketch). Let $\mathcal{A}$ be a forward (resp. weak) adversary for privacy. W.l.o.g. we can assume that there is no Result query related to an instance that has a matching conversation with a legitimate tag (in such a case the answers is 1, due to the hypothesis). Since corruption (if any) are lately done, remaining Result queries are most likely to yield 0 due to security. Let B be a partial blinder for $\mathcal{A}$ who blinds all Result queries: for all such queries, the simulated answer 0 is returned. We further define an adversary $\mathcal{A}'$ playing the security game by simulating $\mathcal{A}$ and ending before the Corrupt queries. Let E be the event that one of the Result queries in $\mathcal{A}$ would answer 1. When E does not occur, $\mathcal{A}$ and $\mathcal{A}^B$ produce the same result. Since the scheme is secure, E occurs with negligible probability. We obtain that $\mathcal{A}$ is as effective as the narrow-forward (resp. narrow-weak) adversary $\mathcal{A}^B$. By blinding $\mathcal{A}^B$ due to the privacy hypothesis, we obtain that $\mathcal{A}$ is as effective as $\mathcal{A}^C$ for some blinder C. □

3 Separation Results

3.1 Strong Privacy is Impossible

Theorem 9. *A destructive-private RFID scheme is not narrow-strong private.*

Namely, no RFID scheme can achieve privacy with respect to the class

$$\mathsf{DESTRUCTIVE} \cup (\mathsf{NARROW} \cap \mathsf{STRONG}).$$

Note 10. As a consequence, strong privacy cannot be achieved. As another consequence, narrow-strong privacy (which is achieved by the scheme of Th. 19) does not imply strong privacy. Similarly, forward privacy (which is achieved by the same scheme) does not imply destructive privacy.

Proof. Let us consider the following destructive adversary $\mathcal{A}$ who simulates to the reader a tag with state S_b which is either forged (S_0) or the one of a corrupted legitimate tag (S_1). The adversary yields true if and only if the reader recognizes the right case (from RESULT).

1: $(\cdot, S_0) \leftarrow \mathsf{SetupTag}_{K_P}(\mathsf{ID}_0)$
2: $\textsc{CreateTag}(\mathsf{ID}_1)$
3: $(\mathsf{vtag}_1, \cdot) \leftarrow \textsc{DrawTag}(\mathsf{ID}_1)$
4: $S_1 \leftarrow \textsc{Corrupt}(\mathsf{vtag}_1)$ (destroy it)
5: flip a coin $b \in \{0, 1\}$
6: $\pi \leftarrow \textsc{Launch}$
7: simulate tag of state S_b with π
8: $x \leftarrow \textsc{Result}(\pi)$
9: output whether $x = b$

The complexity of this adversary is polynomial. Clearly, if the protocol execution is correct, the adversary succeeds. Thus, $1-\Pr[\mathcal{A}\text{ wins}]$ is negligible. Hence, if we have destructive privacy, there must exist a blinder B such that $1-\Pr[\mathcal{A}^B\text{ wins}]$ is negligible as well. If we now look at a privacy game from the blinder perspective, it works as follows:

- blinder receives a public key K_P
- blinder gets one tag state S_1 (by looking at the answer from CORRUPT)
- blinder impersonates a reader to a tag whose state is either S_1 or some unknown S_0 depending on some unknown bit b
- with high probability, blinder guesses b

Indeed, a blinder is a distinguisher who never uses the secret key of the reader between a tag with known state and a random one. This means that for a destructive-private scheme, it must be possible to identify tags whose states are known a priori. We can use this blinder to construct the following narrow-strong adversary. Basically, the adversary creates and corrupt two legitimate tags, feeds the previous distinguisher with one of the tag states, and makes one of the two tags interact with it. If the distinguisher distinguishes well, the output is true.

1: create tag ID_0 and tag ID_1
2: draw both tags
3: corrupt both tags and get their states S_0 and S_1
4: free both tags
5: draw a random tag: $(\mathsf{vtag}, \cdot) \leftarrow \textsc{DrawTag}(\Pr[\mathsf{ID}_0] = \Pr[\mathsf{ID}_1] = \frac{1}{2})$
6: simulate B with input K_P, S_1, and interacting with vtag and get bit x

7: get $\mathcal{T}$ and output whether $\mathcal{T}(\mathsf{vtag}) = \mathsf{ID}_x$

This adversary $\mathcal{A}'$ has polynomial complexity and $1 - \Pr[\mathcal{A}' \text{ wins}]$ is negligible. Clearly, for any blinder B' we have $\Pr[\mathcal{A}'^{B'} \text{ wins}] = \frac{1}{2}$. Hence the scheme is not narrow-strong private. □

3.2 Narrow-Strong Privacy Requires Key Agreement

A key agreement protocol [11] is an interactive protocol between two participants Alice and Bob with common public input set to the security parameter s which ends with a common output bit (the *key*), except with negligible probability. We assume that Alice initiates the protocol and that Bob responds. The protocol is secure (against passive adversary) if the probability that any polynomial-time algorithm that is fed with the common input and the protocol transcript has a negligible advantage over $\frac{1}{2}$ to guess the key bit.

We recall that a 2-round key agreement protocol can define a public-key cryptosystem. Rudich [36] proved a separation between key agreement in $k+1$ rounds and key agreement in k rounds, for any k. That is, a separation exists between key agreement in k rounds (for $k \neq 2$) and a public-key cryptosystem. Nevertheless, we do not know any efficient key agreement protocol based on conventional cryptography only. We use this fact to show that RFID schemes which achieve narrow-strong privacy need more than conventional cryptography techniques.

Theorem 11. *A narrow-strong private RFID scheme can be transformed (in polynomial time) into a secure key agreement protocol with same number of rounds in which Alice simulates* SetupTag *and the reader and Bob simulates the tag.*

This means that any RFID scheme based on a pseudorandom function or a digital signature scheme only is unlikely to be narrow-strong private. Indeed, the tag workload should be at least the same as a responder Bob in a key agreement protocol of same number of rounds. For two-round protocols, this is equivalent to a public-key encryption algorithm (the reader does the decryption).

Proof. We construct a protocol that securely sends a key bit b from Bob to Alice. Intuitively, Alice first creates two legitimate tags and sends their initial states to Bob. Then, Alice simulates the reader and Bob simulates either tag depending on the key bit. By identifying the tag, Alice gets b.

1: Alice: $(K_P, K_S) \leftarrow \mathsf{SetupReader}(1^s)$
2: Alice: $(K_0, S_0) \leftarrow \mathsf{SetupTag}_{K_P}(\mathsf{ID}_0)$, $(K_1, S_1) \leftarrow \mathsf{SetupTag}_{K_P}(\mathsf{ID}_1)$
3: Alice sends (K_P, S_0, S_1) to Bob and simulates the reader protocol with database $\{(\mathsf{ID}_0, K_0), (\mathsf{ID}_1, K_1)\}$
4: Bob simulates the tag protocol with state S_b and interact with Alice
5: Alice sets a such that $\mathsf{ID}_a = \mathsf{Output}$

If the instance of the protocol is correct, Alice obtains $a = b$. This proves the correctness of the key agreement. Note that the number of message rounds is the same as in the RFID protocol. An adversary is an algorithm $\mathcal{P}$ which takes (K_P, S_0, S_1) and the transcript τ of the RFID protocol and returns a bit $\mathcal{P}(K_P, S_0, S_1, \tau)$. We can now define an adversary $\mathcal{A}$ against the RFID scheme.

1: create tag ID_0 and tag ID_1, draw them, corrupt them, get their states S_0 and S_1, and free them
2: draw a random tag $(\mathsf{vtag}, \cdot) \leftarrow \textsc{DrawTag}(\Pr[\mathsf{ID}_0] = \Pr[\mathsf{ID}_1] = \frac{1}{2})$
3: $(\cdot, \tau) \leftarrow \textsc{Execute}(\mathsf{vtag})$
4: set $a = \mathcal{P}(K_P, S_0, S_1, \tau)$
5: get $\mathcal{T}$ and output whether $\mathcal{T}(\mathsf{vtag}) = \mathsf{ID}_a$

Clearly, this is a narrow-strong adversary such that $\Pr[\mathcal{A} \text{ wins}] = \Pr[\mathcal{P} \text{ wins}]$. There must exist a blinder B such that $\Pr[\mathcal{A} \text{ wins}] - \Pr[\mathcal{A}^B \text{ wins}]$ is negligible. Clearly, $\mathcal{A}^B$ gets no information on whether ID_0 or ID_1 is drawn, so $\Pr[\mathcal{A}^B \text{ wins}] = \frac{1}{2}$. Hence, $\Pr[\mathcal{P} \text{ wins}] - \frac{1}{2}$ is negligible: the key agreement protocol is secure. □

We can similarly prove the following result.

Theorem 12. *A narrow-forward private stateless RFID scheme can be transformed into a secure key agreement with same number of rounds.*

This is why protocols like OSK [30] require tags to update their states.

Proof. We proceed as before and use the following adversary $\mathcal{A}$.

1: create tag ID_0 and tag ID_1
2: draw one tag at random $(\mathsf{vtag}, \cdot) \leftarrow \textsc{GetTag}(\Pr[\mathsf{ID}_0] = \Pr[\mathsf{ID}_1] = \frac{1}{2})$
3: $(\cdot, \tau) \leftarrow \textsc{Execute}(\mathsf{vtag})$
4: $\textsc{Free}(\mathsf{vtag})$
5: draw tag ID_0 and tag ID_1, corrupt them, get their states S_0 and S_1
6: set $a = \mathcal{P}(K_P, S_0, S_1, \tau)$
7: get $\mathcal{T}$ and output whether $\mathcal{T}(\mathsf{vtag}) = \mathsf{ID}_a$

We observe that $\textsc{Execute}$ does not modify the state of vtag. □

4 Case Studies

4.1 Weak Privacy based on a Pseudorandom Function

We first construct a weak-private and secure protocol based on a pseudorandom function family (PRF). Let $(F_{s,K})_{K \in \{0,1\}^{k(s)}}$ be a family of functions from $\{0,1\}^{\delta(s)}$ to $\{0,1\}^{\gamma(s)}$. We say it is a PRF if k, δ, γ are polynomially bounded, if $2^{-\delta(s)}$, and $2^{-\gamma(s)}$ are negligible, if $F_{s,K}(x)$ is computable in polynomial time, and if any distinguisher with polynomial complexity has a negligible advantage for distinguishing an oracle simulating $F_{s,K}$ initialized with a random K from an oracle initialized with a truly random function. For more readability we omit the parameter s.

We construct an RFID scheme as depicted on Fig. 1 with $\alpha = \beta = \frac{\delta}{2}$. The algorithm $\mathsf{SetupTag}(\mathsf{ID})$ simply picks a random k-bit key K and sets $S = K$.

$$
\begin{array}{rcl}
\textbf{Tag} & & \textbf{System} \\
\textbf{state: } S & (S = K) & \{\ldots, (\mathsf{ID}, K), \ldots\} \\
\text{pick } b \in \{0,1\}^{\beta} & \xleftarrow{\quad a \quad} & \text{pick } a \in \{0,1\}^{\alpha} \\
c = F_S(a,b) & \xrightarrow{\quad b,c \quad} & \text{find } (\mathsf{ID}, K) \text{ s.t. } c = F_K(a,b) \\
 & & \textbf{output: } \mathsf{ID} \text{ or } \perp \text{ if not found}
\end{array}
$$

Fig. 1. A Weak-Private RFID Scheme based on PRF.

1. Reader picks a random α-bit string a and sends it to tag.
2. Tag with state S sends a random β-bit string b and $c = F_S(a,b)$ to reader.
3. Reader looks for (ID, K) in the database such that $c = F_K(a,b)$ and gets ID.

This protocol is essentially equivalent to the ISO/IEC 9798-2 3-pass mutual authentication protocol that is used in [14] and to the CR building block of [28], both without their third pass (the reader authentication pass). The randomized Hash-Lock identification scheme [39] is this one with no a. But this opens the door to delay attacks where the reader protocol is launched after the tag protocol completed (so conversation are no longer matching). ISO/IEC 9798-2 2-pass unilateral authentication is this protocol with no b [14]. But this opens the door to privacy threats by replaying a.

Theorem 13. *If F is a PRF, the above RFID scheme is secure and weak private.*

Note 14. The scheme is clearly not narrow-forward private since afterward corruption makes it possible to link tags. So, as corollary of this theorem, weak privacy does not imply forward privacy and narrow-weak privacy does not imply narrow-forward privacy.

Proof. Correctness. No false negative is possible here. False positives and incorrect identifications are possible when given the selected tag key K and (a,b) values, there exists $K' \neq K$ in the database such that $F_K(a,b) = F_{K'}(a,b)$. Let us assume that we have n legitimate tags in addition to a subject tag. We construct a distinguisher that simulates the creation of the n tags and simulates a protocol between the subject tag and the reader. To compute F_K on a given input with the subject tag, $\mathcal{A}$ sends the input to an oracle which returns the output. If the subject tag is correctly identified in the simulation, $\mathcal{A}$ answers 1, otherwise it answers 0. This is a distinguisher for F, so it has a negligible advantage. When the oracle implements a random function, the probability of incorrect identification is bounded by $n2^{-\gamma}$ which is negligible. Hence, the probability of incorrect identification with the right oracle is also negligible.

Security. We first note that the protocol suits the special form in Lemma 5 where $R(\mathsf{ID}, K; a, b, c) \iff F_K(a,b) = c$ and R' is always true. We can thus prove simple security and apply Lemma 5.

Let $\mathcal{A}$ be an adversary for simple security with a single tag ID. W.l.o.g. we assume that $\mathcal{A}$ does not call R since R can be simulated. Since database entries are never modified we can reduce to the case where only the target π is launched and others are simulated. $\mathcal{A}$ calls $\textsc{SendReader}(\pi) \to \hat{a}$ at time t and ends by $\textsc{SendReader}((\hat{b}, \hat{c}), \pi)$. $\mathcal{A}$ further calls $\textsc{SendTag}(a_i, \mathsf{ID}) \to (b_i, c_i)$ at time t'_i. $\mathcal{A}$ wins if $\hat{c} = F_K(\hat{a}, \hat{b})$ and for every i such that $t < t'_i$ we have $(a_i, b_i, c_i) \neq (\hat{a}, \hat{b}, \hat{c})$ (namely: conversations are not matching). As for correctness, let $\mathcal{A}'$ be an algorithm who simulates $\mathcal{A}$ and all oracles then looks whether the attack succeeded. To simulate $\textsc{SendTag}(a_i, \mathsf{ID})$, $\mathcal{A}'$ simply picks a random b_i and queries an oracle F with (a_i, b_i) to get c_i and returns (b_i, c_i). To determine whether the attack succeeded, $\mathcal{A}'$ queries the oracle F again. Clearly, $\mathcal{A}$ and $\mathcal{A}'$ interacting with an oracle simulating F_K have the same success probability. $\mathcal{A}'$ can be considered as a distinguisher between F and a truly random function. Since F is pseudorandom, the distinguisher has negligible advantage, so $\mathcal{A}'$ interacting with an oracle simulating a random function has similar success probability as $\mathcal{A}$. If $t'_i < t$, $\Pr[\hat{a} = a_i]$ is negligible. If now $t < t'_i$, wining cases are for $(a_i, b_i, c_i) \neq (\hat{a}, \hat{b}, \hat{c})$, $c_i = F(a_i, b_i)$, $\hat{c} = F(\hat{a}, \hat{b})$, thus $(a_i, b_i) \neq (\hat{a}, \hat{b})$. However, if $(a_i, b_i) \neq (\hat{a}, \hat{b})$, the value for $F(\hat{a}, \hat{b})$ before the final query is free so $\Pr[\hat{c} = F(\hat{a}, \hat{b})] = 2^{-k}$, which is negligible. Therefore, $\mathcal{A}$ succeeds with negligible probability. This proves simple security. Lemma 5 concludes.

Weak privacy. Thanks to Lemma 8, we only have to prove narrow-weak privacy. We want to prove that, for any narrow-weak adversary $\mathcal{A}$, there exists a blinder B such that $\mathcal{A}$ has no significant advantage over $\mathcal{A}^B$. Let B be the blinder who simulates $\textsc{SendTag}(a, \mathsf{vtag})$ by answering with a random (b, c).

Clearly, all $\textsc{Launch}$ and $\textsc{SendReader}$ queries can be perfectly simulated so we assume w.l.o.g. that these oracles are no longer used. We use the proof methodology of Shoup [37]. Let $\mathsf{game}_0 = \mathsf{game}_1(0)$ be the privacy game.

Let $\mathsf{game}_1(i)$ be the same game as $\mathsf{game}_1(i-1)$ in which the ith created tag is simulated using an ad-hoc random oracle F_i from $\{0,1\}^{\alpha+\beta}$ to $\{0,1\}^\gamma$ to compute $F_{K_i}(a, b) = F_i(a, b)$. Clearly, $|\Pr[\mathcal{A} \text{ wins } \mathsf{game}_1(i)] - \Pr[\mathcal{A} \text{ wins } \mathsf{game}_1(i-1)]|$ can be expressed as a distinguisher advantage for F so it is negligible. Let $\mathsf{game}_1 = \mathsf{game}_1(n)$ where n is the number of tags. Since n is polynomial, $|\Pr[\mathcal{A} \text{ wins } \mathsf{game}_1] - \Pr[\mathcal{A} \text{ wins } \mathsf{game}_0]|$ is negligible.

Let game_2 be the same game as game_1 in which the adversary wins when $\textsc{SendTag}$ never picked a duplicate b. This duplication happens with probability bounded by $q^2 \cdot 2^{-\beta}$ where q is the number of $\textsc{SendTag}$ queries. Clearly, this probability is negligible. Hence $|\Pr[\mathcal{A} \text{ wins } \mathsf{game}_2] - \Pr[\mathcal{A} \text{ wins } \mathsf{game}_0]|$ is negligible.

Using B, $|\Pr[\mathcal{A}^B \text{ wins } \mathsf{game}_2] - \Pr[\mathcal{A}^B \text{ wins } \mathsf{game}_0]|$ is negligible as well. Clearly, the B simulation is perfect when there is no duplicate b. This leads us to $|\Pr[\mathcal{A}^B \text{ wins } \mathsf{game}_2] - \Pr[\mathcal{A} \text{ wins } \mathsf{game}_2]|$ being negligible. Finally, we obtain that $|\Pr[\mathcal{A}^B \text{ wins } \mathsf{game}_0] - \Pr[\mathcal{A} \text{ wins } \mathsf{game}_0]|$ is negligible. Hence, $\mathcal{A}$ is a trivial adversary. $\square$

4.2 Narrow-Destructive Privacy in the Random Oracle Model

We now consider a new scheme based on two oracles F and G running random functions from $\{0,1\}^{\alpha+k}$ and $\{0,1\}^k$ to $\{0,1\}^k$, respectively. The tag generation algorithm $\mathsf{SetupTag}(\mathsf{ID})$ picks a random k-bit key K and sets the initial state to $S = K$. The protocol works as depicted on Fig. 2.

1. Reader picks a random α-bit string a and sends it to tag.
2. Tag with state S sends $c = F(S, a)$ then refreshes its state S with $G(S)$.
3. Reader looks for (ID, K) in the database such that $c = F(G^i(K), a)$ with $i < t$, gets ID, and replaces (ID, K) by $(\mathsf{ID}, G^i(K))$ in the database.

Note that after t iterations without the reader a tag can no longer be identified. Thus, this scheme does not satisfy the hypothesis of Lemma 8. (See also Note 18.) As opposed to the previous construction, F and G cannot be just PRFs since the adversary can get the code of F and G by corrupting a tag.

Tag		**System**
state: S	$(S = K)$	$\{\ldots, (\mathsf{ID}, K), \ldots\}$
	$\xleftarrow{\quad a \quad}$	pick $a \in \{0,1\}^\alpha$
$c = F(S, a)$	$\xrightarrow{\quad c \quad}$	find (ID, K) and i s.t.
replace S by $G(S)$		$c = F(G^i(K), a)$ and $i < t$
		replace K by $G^i(K)$
		output: ID or $\perp$ if not found

Fig. 2. A Narrow-Destructive-Private RFID Scheme based on a Random Oracle.

The OSK protocol [30,31] uses no a, so delay attacks can be made. Avoine et al. [3] proposed to add a random a and use $c = F(S \oplus a)$. Dimitriou [12] proposed to add a (useless) b and to send $F(S)$ and b in addition to $c = F(S, a, b)$.[4]

Theorem 15. *Assuming that k and t are polynomially bounded and that 2^{-k} is negligible, the above scheme is a secure and narrow-destructive private RFID scheme in the random oracle model.*

Note 16. This is not narrow-strong private since early corruption enables to link tags. So, narrow-destructive privacy does not imply narrow-strong privacy.

Note 17. We can artificially tweak the protocol of Th. 15 to get narrow-forward privacy but not narrow-destructive privacy, which separates the two models. To do so, we add in all tag states a common secret K_s such that when a tag receives $a = K_s$ it outputs $c = S$. Readers should not select $a = K_s$ but narrow-destructive adversaries could do so after a tag is sacrificed to leak K_s. Obviously, the scheme is no longer narrow-destructive private. Nevertheless, it is still narrow-forward private since corruption output cannot be used in interaction.

[4] Sending $F(S)$ is used to decrease the workload in optimistic cases.

Note 18. As pointed out in Juels-Weis [24], a weak adversary against the scheme of Fig. 2 could run a sort of denial of service. The adversary proceeds as follows.

$\textsc{CreateTag}(\mathsf{ID}_0)$, $\textsc{CreateTag}(\mathsf{ID}_1)$
$\mathsf{vtag}_0 \leftarrow \textsc{DrawTag}(\mathsf{ID}_0)$
for $i = 1$ to $t + 1$ **do**
  pick a random x
  $\textsc{SendTag}(x, \mathsf{vtag}_0)$
end for
$\textsc{Free}(\mathsf{vtag}_0)$
$(\mathsf{vtag}, \cdot) \leftarrow \textsc{DrawTag}(\Pr[\mathsf{ID}_0] = \Pr[\mathsf{ID}_1] = \frac{1}{2})$
$(\pi, \cdot) \leftarrow \textsc{Execute}(\mathsf{vtag})$
$x \leftarrow \textsc{Result}(\pi)$
get $\mathcal{T}$ and output whether $\mathcal{T}(\mathsf{vtag}) = \mathsf{ID}_x$

Clearly, $\Pr[\mathcal{A} \text{ wins}] = 1$, but for any blinder B, we have $\Pr[\mathcal{A}^B \text{ wins}] = \frac{1}{2}$. So this weak adversary is not trivial. Hence, narrow-destructive privacy does not imply weak privacy.

Proof. Correctness. False negatives are not possible. False positives and wrong identifications are possible when given K, a, b, and i, there exist K' and $j < t$ such that $K' \neq K$ and $F(G^i(K), a, b) = F(G^j(K'), a, b)$. In the random oracle model, the probability of such event is at most $nt^2 2^{-k}$, which is negligible.

Security. We apply Lemma 5 where oracle $R(\mathsf{ID}, K; a, c)$ simply checks that there exists $i < t$ such that $F(G^i(K), a) = c$ and $R'(n) \iff n < t$. By using standard random oracle techniques, we can assume that $\mathcal{A}$ never queries F with $G^i(K)$ for $i = 0, \ldots, t + n - 1$ and n is the number of $\textsc{SendTag}$ queries.

We proceed as in the proof of Th. 13 with same notations. If $t'_i < t$, $\Pr[\hat{a} = a_i]$ is negligible. If $t < t'_i$, wining cases are for $(a_i, c_i) \neq (\hat{a}, \hat{c})$ and $\hat{c} = F(G^j(K), \hat{a})$ for some j smaller than t. Since $\mathcal{A}$ never queried F with any $G^j(K)$ and the tag did not query it with any $(G^j(K), \hat{a})$, the values of $F(G^j(K), \hat{a})$ are free so $\Pr[\hat{c} = F(G^j(K), \hat{a}); j < t] = t2^{-k}$, which is negligible.

Narrow-destructive privacy. Clearly, all $\textsc{Launch}$ and $\textsc{SendReader}$ queries are trivial to simulate since no $\textsc{Result}$ query is allowed. So, we assume w.l.o.g. that no such query is made. We want to prove that, for any adversary $\mathcal{A}$ there exists a blinder B such that $\mathcal{A}$ has no significant advantage over $\mathcal{A}^B$.

Let E (resp. E') be the event that at least one of the queries by $\mathcal{A}$ to the F or the G oracles equals one query made (resp. that should have been made if it was not blinded) by some $\textsc{SendTag}(a, \mathsf{vtag})$ query.

$\textsc{SendTag}$ queries are simulated by B by returning a random c. Note that there is no $\textsc{SendTag}$ query to corrupted tags since adversaries are destructive. This simulation is perfect (in the sense that the adversary and the blinded adversary recover the same information about the virtual tag from the protocol transcript) when the event E does not occur. Namely, $\Pr[\mathcal{A} \text{ wins}|\neg E] = \Pr[\mathcal{A}^B \text{ wins}|\neg E']$ and $\Pr[E] = \Pr[E']$.

Hence, $|\Pr[\mathcal{A} \text{ wins}] - \Pr[\mathcal{A}^B \text{ wins}]| \leq \Pr[E]$. If q queries to F and G were made by $\mathcal{A}$, in the worst case $\mathcal{A}$ knows that all $G^i(K)$'s are in a set of $2^k - q$ values. Note that no Corrupt query gives information on any $G^i(K)$ that can be used by any SendTag query. The probability to pick one is at most $\frac{tn}{2^k - q}$ where n is the number of tags. Hence, E occurs with probability at most $\frac{tnq}{2^k - q}$, which is negligible. □

4.3 Narrow-Strong and Forward Privacy based on a PKC

We now achieve narrow-strong and forward privacy using public-key cryptography. We use the standard definitions of public-key cryptosystems (PKC), IND-CPA and IND-CCA security [6,13,20,29,34]. A PKC consists of a key generator, a probabilistic encryption algorithm, and a deterministic decryption algorithm. It must be correct in the sense that the decryption of the encryption of any x is always x. The scheme is IND-CPA-secure (resp. IND-CCA-secure) is all polynomial-time adversaries win the IND-CPA (resp. IND-CCA) with negligible advantage. In the IND-CPA game, the adversary receives a public key, submits two plaintexts, receives the encryption of one of the two, and tries to guess which plaintext was encrypted. In the IND-CCA game, the adversary can query a decryption oracle, except on the received ciphertext.

$$
\begin{array}{ccl}
\textbf{Tag} & & \qquad\textbf{System} \\
\textbf{state: } K_P, \mathsf{ID}, K & (K = F_{K_M}(\mathsf{ID})) & \textbf{secret keys: } K_S, K_M \\
 & \xleftarrow{\quad a \quad} & \text{pick } a \in \{0,1\}^\alpha \\
c = \mathsf{Enc}_{K_P}(\mathsf{ID}||K||a) & \xrightarrow{\quad c \quad} & \text{parse } \mathsf{Dec}_{K_S}(c) = \mathsf{ID}||K||a' \\
 & & \text{check } a = a' \\
 & & \text{check } K = F_{K_M}(\mathsf{ID}) \\
 & & \textbf{output: } \mathsf{ID} \text{ or } \perp \text{ if failed}
\end{array}
$$

Fig. 3. A Narrow-Strong and Forward -Private RFID Scheme based on a PKC.

We initialize the scheme by generating a private/public key pair (K_S, K_P) for the $\mathsf{Enc}/\mathsf{Dec}$ PKC. The tag generation algorithm $\mathsf{SetupTag}(\mathsf{ID})$ picks a random k-bit key K and sets the initial state to $S = (K_P, \mathsf{ID}, K)$. We assume that k and α are polynomial. The protocol works as depicted on Fig. 3.

1. Reader sends an identification request with an α-bit random a.
2. Tag calculates $c = \mathsf{Enc}_{K_P}(\mathsf{ID}||K||a)$ and sends c to the reader.
3. Reader gets $\mathsf{ID}||K||a = \mathsf{Dec}_{K_S}(c)$ and checks that a is correct and that (ID, K) is in database.[5]

[5] Using $K = F_{K_M}(\mathsf{ID})$ as depicted on Fig. 3 given a PRF F and a master secret K_M does not modify our result. The same simplification could apply to the scheme of Fig. 1 as well, in order to shrink the database.

Theorem 19. *If the public-key cryptosystem is IND-CPA-secure then the above RFID scheme is narrow-strong private. If the cryptosystem is IND-CCA-secure and 2^{-k} is negligible, the RFID scheme is further secure and forward private.*

Namely, with an IND-CCA PKC, this RFID scheme achieves privacy with respect to the class

$$\mathsf{FORWARD} \cup (\mathsf{NARROW} \cap \mathsf{STRONG}).$$

Due to Th. 9, this scheme is not strong private so narrow-strong privacy does not imply strong privacy and forward privacy does not imply strong privacy.

Proof. Correctness. This comes from the correctness of the cryptosystem.

Narrow-strong privacy. We prove that for any narrow-strong adversary $\mathcal{A}$ there exists a blinder B such that $\mathcal{A}$ has no significative advantage over $\mathcal{A}^B$. Since the reader just sends random a and no Result query is allowed, every Launch and SendReader query can be simulated in a trivial way so we can assume without loss of generality that no such query is done. We construct the blinder by using standard hybrid arguments. We consider the hybrid blinder B_i which works as follows: any of the i first SendTag queries with input a, returns the encryption c of a random r of same length as $\mathsf{ID}||K||a$. Other SendTag queries by $\mathcal{A}$ are forwarded to the SendTag oracle.

The adversary, hybrid blinders, and tags can be simulated without using K_S. Let S_i be a simulator for the $\mathcal{A}^{B_i}$ attack except for the ith SendTag query which is indeed released. We use S_i to play the IND-CPA game. At the beginning, S_i receives K_P and runs the simulator for $\mathcal{A}^{B_i}$. At the moment of the ith query a, S_i computes $m_0 = \mathsf{ID}||K||a$ as B_{i-1} would do to simulate the tag, computes $m_1 = r$ as B_i would do, and submits m_0 and m_1 to the IND-CPA game. S_i receives an encrypted value c of either m_0 or m_1 that is used to respond the query and continues the simulation. At the end, S_i looks whether $\mathcal{A}^{B_i}$ won the privacy game or not. If it won, S_i outputs 0. Otherwise, S_i outputs 1. Clearly $\mathcal{A} = \mathcal{A}^{B_0}$, $\mathsf{Adv}^{\mathsf{IND}}(S_i) = \Pr[\mathcal{A}^{B_{i-1}} \text{ wins}] - \Pr[\mathcal{A}^{B_i} \text{ wins}]$, and $B = B_{q_T}$ is a full blinder where q_T is the number of SendTag queries. The complexity of S_i is polynomial. Due to IND-CPA security, $|\Pr[\mathcal{A} \text{ wins}] - Pr[\mathcal{A}^B \text{ wins}]|$ is negligible.

Security. The protocol suits the special form in Lemma 5 where $R(\mathsf{ID}, K; a, c)$ means $\mathsf{Dec}_{K_S}(c) = \mathsf{ID}||K||a$ and R' is always true. We can thus prove simple security and apply Lemma 5.

Let $\mathcal{A}$ be an adversary for the simple security game with a single tag ID and a single instance π (others are simulated). W.l.o.g. $\mathcal{A}$ does not query $R(\cdot; \cdot, c)$ when there is a protocol transcript $(\cdot, c)$. (The first input of R queries cannot be ID thus R cannot be satisfied.) $\mathcal{A}$ queries SendReader$(\pi) \to \hat{a}$ at time t, SendTag$(a_i, \mathsf{ID}) \to c_i$ at time t'_i, and ends by SendReader$(\hat{c}, \pi)$. If $t'_i < t$, $\Pr[a_i = \hat{a}]$ is negligible. If $t < t'_i$, wining cases are for $(\hat{a}, \hat{c}) \neq (a_i, c_i)$, $\mathsf{Dec}_{K_S}(\hat{c}) = \mathsf{ID}||K||\hat{a}$, and $\mathsf{Dec}_{K_S}(c_i) = \mathsf{ID}||K||a_i$. Hence, w.l.o.g. we can assume that $\hat{c} \neq c_i$ for all i.

We construct a partial blinder B_i as before. We construct a simulator S_i for $\mathcal{A}^{B_i}$ playing the IND-CCA game as before. S_i terminates by determining whether $\mathcal{A}$ succeeded by calling $\hat{c}$ to a decryption oracle. Finally, by using the IND-CCA security, we obtain a blinded adversary $\mathcal{A}^B$ such that $|\Pr[\mathcal{A}\text{ wins}] - Pr[\mathcal{A}^B\text{ wins}]|$ is negligible. Clearly, if the tag is no longer used and the reader leaks no information, making it identify the tag reduces to guessing the tag key K which can only happen with probability 2^{-k}, which is negligible.

Forward privacy. Narrow-forward privacy implies forward privacy thanks to Lemma 8, □

5 Conclusion

We have proven that public-key cryptography can assure the highest level of feasible privacy in RFID: narrow-strong and forward privacy, even with stateless protocols. We have shown narrow-destructive privacy for an OSK-like protocol in the random oracle model. Finally, we have proven weak privacy for a simple challenge-response protocol. The problem of achieving destructive privacy or forward privacy without public-key techniques are left open.

Acknowledgment. I thank Gildas Avoine for providing many useful references.

References

1. J.-Ph. Aumasson, M. Finiasz, W. Meier, S. Vaudenay. TCHo: a Hardware-Oriented Trapdoor Cipher. In *Information Security and Privacy (ACISP'07)*, Townsville, Australia, Lecture Notes in Computer Science 4586, pp. 184–199, Springer-Verlag, 2007.
2. G. Avoine. Cryptography in Radio Frequency Identification and Fair Exchange Protocols. PhD Thesis no. 3407, EPFL, 2005. http://library.epfl.ch/theses/?nr=3407
3. G. Avoine, E. Dysli, P. Oechslin. Reducing Time Complexity in RFID Systems. In *Selected Areas in Cryptography'05*, Kingston, Ontario, Canada, Lecture Notes in Computer Science 3897, pp. 291–306, Springer-Verlag, 2006.
4. G. Avoine, P. Oechslin. RFID Traceability: A Multilayer Problem. In *The 9th International Conference on Financial Cryptography (FC'05)*, Roseau, The Commonwealth of Dominica, Lecture Notes in Computer Science 3570, pp. 125–140, Springer-Verlag, 2005.
5. L. Batina, N. Mentens, K. Sakiyama, B. Preneel, I. Verbauwhede. In *Security and Privacy in Ad-Hoc and Sensor Networks (ESAS'06)*, Hamburg, Germany, Lecture Notes in Computer Science 4357, pp. 6–17, Springer-Verlag, 2006.
6. M. Bellare, A. Desai, D. Pointcheval, P. Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. In *Advances in Cryptology CRYPTO'98*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 1462, pp. 26–45, Springer-Verlag, 1998.
7. S. Bocchetti. Security and Privacy in RFID Protocols. Master Thesis, 2006.

8. M. Burmester, T. van Le, B. de Medeiros. Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols. In *Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm'06)*, Baltimore, MA, USA. IEEE, 2006.
9. B. Calmels, S. Canard, M. Girault, H. Sibert. Low-Cost Cryptography for Privacy in RFID Systems. In *Smart Card Research and Advanced Applications (CARDIS'06)*, Tarragona, Spain, Lecture Notes in Computer Science 3928, pp. 237–251, Springer-Verlag, 2006.
10. I. Damgård, M. Østergaard. RFID Security: Tradeoffs between Security and Efficiency. Technical report 2006/234, IACR, 2006. http://eprint.iacr.org/2006/234
11. W. Diffie, M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, 1976.
12. T. Dimitriou. A Lightweight RFID Protocol to Protect against Traceability and Cloning Attacks. In *Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm'05)*, Athens, Greece, IEEE, 2005. http://ieeexplore.ieee.org/iel5/10695/33755/01607559.pdf?arnumber=1607559
13. D. Dolev, C. Dwork, M. Naor. Non-Malleable Cryptography. In *Proceedings of the 23rd ACM Symposium on Theory of Computing*, New Orleans, Louisiana, U.S.A., pp. 542–552, ACM Press, 1991.
14. M. Feldhofer, S. Dominikus, J. Wolkerstorfer. Strong Authentication for RFID Systems using the AES Algorithm. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES'04)*, Boston, MA, USA, Lecture Notes in Computer Science 3156, pp. 357–370, Springer-Verlag, 2004.
15. M. Feldhofer, C. Rechberger. A Case against Currently used Hash Functions in RFID Protocols. In *On the Move to Meaningful Internet Systems 2006: OTM'06 Workshops, including the First International Workshop on Information Security (IS'06)*, Montpelier, France, Lecture Notes in Computer Science 4277, pp. 372–381, Springer-Verlag, 2006.
16. M. Finiasz, S. Vaudenay. When Stream Cipher Analysis Meets Public-Key Cryptography. (Invited Talk.) To appear in the proceedings of SAC'06. Lecture Notes in Computer Science, Springer, 2006.
17. H. Gilbert, M. Robshaw, H. Sibert. An Active Attack Against HB+: A Provably Secure Lightweight Authentication Protocol. *IEE Electronic Letters*, vol. 41, pp. 1169–1170, 2005.
18. M. Girault, D. Lefranc. Public Key Authentication with One (Online) Single Addition. In *Cryptographic Hardware and Embedded Systems CHES'04*, Worcester, MA, USA, Lecture Notes in Computer Science 3156, pp. 413–427, Springer-Verlag, 2004.
19. M. Girault, G. Poupard, J. Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. *Journal of Cryptology*, vol. 19, pp. 463–487, 2006.
20. S. Goldwasser, S. Micali. Probabilistic Encryption. *Journal of Computer and System Sciences*, vol. 28(2), pp. 270–299, 1984.
21. J. Hall, M. Barbeau, E. Kranakis. Detecting Rogue Devices in Bluetooth Networks using Radio Frequency Fingerprinting. In *Proceedings of the Third IASTED International Conference on Communications and Computer Networks (CCN'06)*, Lima, Peru, pp. 108–113, IASTED/ACTA Press, 2006.
22. ISO/IEC 14443-3. Identification Cards — Contactless Integrated Circuit(s) Cards — Proximity Cards. Part 3: Initialization and Anticollision. ISO. 2001.
23. A. Juels, S. Weis. Authenticating Pervasive Devices with human Protocols. In *Advances in Cryptology CRYPTO'05*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 3621, pp. 293–308, Springer-Verlag, 2005.

24. A. Juels, S. Weis. Defining Strong Privacy for RFID. Technical report 2006/137, IACR, 2006. http://eprint.iacr.org/2006/137
25. J. Katz, J. S. Shin. Parallel and Concurrent Security of the HB and HB+ Protocols. In *Advances in Cryptology EUROCRYPT'06*, St. Petersburg, Russia, Lecture Notes in Computer Science 4004, pp. 73–87, Springer-Verlag, 2006.
26. T. van Le, M. Burmester, B. de Medeiros. Universally Composable and Forward Secure RFID Authentication and Authenticated Key Exchange. In *Proceedings of the 2007 ACM Symposium on Information, Computer and Communications Security (ASIACCS'07)*, Singapore, pp. 242–252, ACM, 2007.
27. C. H. Lim, T. Kwon. Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer. In *Proceedings of Information and Communications Security (ICICS'06)*, Raleigh, NC, USA, Lecture Notes in Computer Science 4307, pp. 1–20, Springer-Verlag, Springer. 2006
28. D. Molnar, D. Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In *11th ACM Conference on Computer and Communications Security*, Washington, DC, USA, pp. 210–219, ACM Press, 2004.
29. M. Naor, M. Yung. Public-Key Cryptosystems Provably Secure against Chosen Ciphertext Attacks. In *Proceedings of the 22nd ACM Symposium on Theory of Computing*, Baltimore, Maryland, U.S.A., pp. 427–437, ACM Press, 1990.
30. M. Ohkubo, K. Suzuki, S. Kinoshita. Cryptographic Approach to a Privacy Friendly Tag. Presented at the *RFID Privacy Workshop*, MIT, USA, 2003.
31. M. Ohkubo, K. Suzuki, S. Kinoshita. Efficient Hash-Chain based RFID Privacy Protection Scheme. Presented at the *International Conference on Ubiquitous Computing (Ubicomp'04), Workshop Privacy: Current Status and Future Directions*, Nottingham, UK, 2004.
32. M. Ohkubo, K. Suzuki. RFID Privacy Issues and Technical Challenges. *Communications of the ACM*, vol. 48, pp. 66–71, 2005.
33. R.-I. Paise. A Privacy Model for Mutual Authentication in Radio Frequency Systems. Master Thesis, 2007.
34. C. Rackoff, D. Simon. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In *Advances in Cryptology CRYPTO'91*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 576, pp. 433–444, Springer-Verlag, 1992.
35. M.J.B. Robshaw. Searching for Compact Algorithms: CGEN. In *First International Conference on Cryptology in Vietnam (Vietcrypt'06)*, Hanoi, Vietnam, Lecture Notes in Computer Science 4341, pp. 37–49, Springer-Verlag, 2006.
36. S. Rudich. The Use of Interaction in Public Cryptosystems. In *Advances in Cryptology CRYPTO'91*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 576, pp. 242–251, Springer-Verlag, 1992.
37. V. Shoup. Sequences of Games: A Tool for Taming Complexity in Security Proofs. Technical report 2004/332, IACR, 2004. http://eprint.iacr.org/2004/332
38. S. Vaudenay. RFID Privacy based on Public-Key Cryptography. (Invited Talk.) In *International Conference on Information Security and Cryptography ICISC'06*, Busan, Korea, Lecture Notes in Computer Science 4296, pp. 1–6, Springer-Verlag, 2006.
39. S. Weis, S. Sarma, R. Rivest, D. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *International Conference on Security in Pervasive Computing (SPC'03)*, Boppard, Germany, Lecture Notes in Computer Science 2802, pp. 454–469, Springer-Verlag, 2003.