Key Updates for RFID Distance-Bounding Protocols: Achieving Narrow-Destructive Privacy

Cristina Onete

CASED & TU Darmstadt
cristina.onete@gmail.com

Abstract. Distance-bounding protocols address man-in-the-middle (MITM) in authentication protocols: by measuring response times, verifiers ensure that the responses are not purely relayed. Dürholz et al. [13] formalize the following attacks against distance-bounding protocols: (1) mafia fraud, where adversaries must authenticate to the verifier in the presence of honest provers; (2) terrorist fraud, where malicious provers help the adversary (in offline phases) to authenticate (however, the adversary shouldn't authenticate on its own); (3) distance fraud, where a malicious prover must convince the verifier that it is closer to it than in reality; (4) impersonation security, where the prover must authenticate to the verifier in the rounds where response times are not measured. A scenario where distance-bounding can be successfully deployed is RFID authentication, where the provers and RFID tags, and the verifiers are RFID readers.
Security models and most distance-bounding schemes designed so far are static, i.e. the used secret key is never updated. The scenario considered by [13] features a single reader and a single tag. However, a crucial topic in RFID authentication is privacy, as formalized by Vaudenay [32]. Adversaries against privacy can corrupt tags and learn the secret keys; in this scenario, key updates ensure better privacy. In this paper we extend distance-bounding security to include key updates, and show a compiler that preserves mafia, distance, and impersonation security, and turns a narrow-weak private distance-bounding protocol into a narrow-destructive private distance-bounding protocol as in [32]. We discuss why it is much harder to attain terrorist fraud resistance, for both stateless and stateful scenarios. We optimize our compiler for cases where (i) the underlying distance-bounding protocol does *not* have reader authentication; (ii) impersonation security is achieved (by using a pseudorandom function) before the distance-bounding phase; or (iii) the prover ends by sending a MAC of the transcript. We also use our compiler on the enhanced construction in [13].

1 Introduction

RFID Security and Privacy. Radio Frequency Identification (RFID) is a popular, cost-efficient platform to run authentication protocols, useful in logistics, public transport, and even personal identification. In RFID authentication, RFID tags interact with readers and prove their legitimacy. Since most RFID tags are resource-limited, with reduced computation and communication possibilities, authentication is usually done with lightweight protocols, e.g., the HB protocol and its variants [19,14,12,3,26,23].

The usual security notion in authentication is impersonation security, i.e. no adversary should impersonate a legitimate prover. However, a rising concern lately has been privacy. Privacy in authentication is defined as follows: an adversary must not distinguish which valid tag interacts with the reader. An early RFID privacy model was introduced by Juels and Weis [20]; their notion was based on tag indistinguishability

(an adversary cannot tell which of two valid tags is authenticated). In 2007, Vaudenay [32] formalized an RFID security and privacy model where adversaries can corrupt tags and learn secret keys; this model was later refined by Paise and Vaudenay, [27], and Ng et al. [25]. Vaudenay introduced eight types of adversaries, where narrow-weak adversaries coincide somewhat with Juels and Weis' adversaries, as they do not corrupt tags. The goal, however, remains to achieve better privacy.

Vaudenay showed that his notion of strong privacy cannot be achieved. Thus, if the adversary can corrupt tags at any point *and* learn the output of authentication sessions, it always breaks privacy. *Narrow* strong privacy, i.e., when the adversary does *not* learn authentication output, requires key agreement, which in turn requires public key cryptography, a primitive deemed too expensive for most RFID tags[1]. However, Vaudenay shows how to achieve so-called narrow-destructive privacy, where the adversary destroys the tags upon corruption (as is the case when the adversary damages tags to learn their secret keys): namely, to use key updates, thus ensuring that corruption only reveals an ephemeral secret, and no further information about the past states of the key.

Distance Bounding. General authentication security assumes an adversary cannot relay messages between honest readers and tags. Such man-in-the-middle (MITM) adversaries always succeed in impersonation attacks. Introduced in 1988 by Desmedt [10], pure relaying of messages is called mafia fraud, and implementations of such MITM attacks are shown in e.g. [16,6,11,15]. In 1993, Brands and Chaum [2] introduced distance-bounding as a countermeasure against mafia fraud, using the fact that pure relaying introduces a processing delay for the adversary, which the reader can detect if equipped with a clock. Following the formal description of [13], distance-bounding protocols consist of communication phases which are either lazy (if the clock is not used) or time-critical (if the clock detects pure relay).

In fact, the recent model of Dürholz et al. [13] formalizes the following four main attacks:

Mafia Fraud. The adversary impersonates the tag in the presence of an honest reader and an honest tag. However, any pure relaying is detected by the reader's clock.

Terrorist Fraud. The adversary impersonates the tag *with the tag's consent and (offline) aid* to an honest reader. The restriction is that the adversary is unable to impersonate the tag after the tag has withdrawn its support.

Distance Fraud. The adversary – a malicious tag – tries to cheat the reader's clock and prove it is closer to the reader than it really is.

Impersonation Security. The adversary attempts to impersonate the tag during the lazy phases, but without pure relay.

RFID distance-bounding protocols abound in the literature [2,31,17,4,1,29,21,22], addressing two or more of the above threats. The implementability of RF distance-

[1] Notably, more expensive tags *do* enable elliptic curve cryptography; however, passive and semi-active tags generally cannot run public key cryptography.

bounding was recently investigated in [28], and Dürholz et al. [13] have assessed the security properties of an enhanced variant of the protocol due to Kim and Avoine [21].

However, most distance-bounding protocols do not address the problem of privacy. An exception is the Swiss-Knife protocol due to Kim et al. [22], where tags have a secret identifier by which they are identified by the reader. However, this protocol does not achieve forward privacy, as the identifier is never updated.

Our contributions. In this work, we formalize distance-bounding with key updates. Concretely we show — to our knowledge for the first time in the literature — a *formal model* capturing the notion of distance-bounding in the setting of key updates. Towards this goal we define long-term completeness (i.e. availability) for distance-bounding. Also, we show a compiler that turns any mafia fraud, distance fraud, and impersonation resistant, narrow-*weak* private distance-bounding RFID protocol into a narrow-*destructive* private distance-bounding RFID protocol with the same distance-bounding properties and long-term completeness. Our construction also requires that the key generation algorithm of the underlying distance-bounding protocol outputs pseudorandom keys K [2]. Concretely, we wrap a construction like Vaudenay's narrow-destructive protocol [32] around an underlying distance-bounding scheme, such that the reader and tag both update state by using a pseudorandom function (PRF). Also, in order to address attacks where adversaries just drop messages, the reader only updates state upon receiving a final authentication message from the tag. Contrary to Vaudenay's construction [32], the reader *does* update state, but only if the tag succeeds in (a) an initial authentication phase; (b) the distance-bounding authentication steps; and (c) the final verification. Thus, we prevent denial-of-service (DoS) attacks and gain *availability* and efficiency in the reader's computations for the compiled protocol (compared to the initial scheme in [32]).

Concretely, we (1) formalize availability (DoS resistance), then (2) describe a compiler where the reader and tag update state at each successful authentication. Though the adversary may force the tag to update before the reader, the reader can "catch up" at the next honest authentication attempt. This is an efficiency improvement with respect to the construction in [32], where the reader must always catch up from scratch with the original key. Also, if the adversary drops a valid message from the communication, the reader only accepts with negligible probability, and so does not update state. We (3) prove that our compiler preserves mafia, distance, and impersonation security in the sense of [13]. We furthermore discuss why our compiler does *not* provably preserve terrorist fraud resistance. Namely, it is hard to formalize how a simulator may use partial update-information that the adversary receives from the tag. Note also that many distance-bounding protocols do not address this attack [2,17,21,1]; also, no protocol *claiming* to achieve terrorist fraud resistance has, in fact, been *proved* terrorist fraud resistant in the sense of [13]. We also (4) discuss optimizations of our compiler for three particular cases, namely for distance-bounding protocols which do not use reader authentication, for protocols with reader authentication and an initial

[2] This is not a very strong assumption, as such algorithms are usually required to produce pseudorandom outputs.

lazy phase achieving impersonation security by a pseudorandom function (PRF), and for protocols ending with a PRF computation on the protocol transcript. Finally, we (5) apply an optimized compiler to the protocol presented in [13] and quantify the security properties of the compiled protocol.

Related Work. The security and privacy model due to Vaudenay [32] defines privacy in terms of a blinder. Simply put, the adversary interacts in four main ways: it can create and draw honest and dishonest tags; it can communicate to the reader; communicate with the tag; or it can corrupt the tag. The adversary breaks the privacy of a protocol if it can distinguish a particular tag better than a trivial adversary (for which the blinder simulates everything except corruption queries). We review this framework briefly in section 2.5.

Different simulation-based privacy frameworks were introduced in [24,8,9], the latest one describing a very strong Zero-knowledge based notion of privacy. Very recently, a game-based security and privacy model was introduced by Hermans et al. [18]. However, simulation-based privacy is stronger than game-based privacy, capturing the notion that the adversary should not only be unable to distinguish a legitimate tag (with or without corruption), but it should, in fact, be unable to tell anything about this tag (including whether it is legitimate or not). Whereas such strong privacy is desirable, achieving destructive privacy in the framework of Vaudenay [32] is an important first step in achieving privacy for distance-bounding protocols.

Privacy can also be achieved as shown in 2009 by Sadeghi et al. [30], i.e., by means of anonymizers, which are corruptible third parties in the setting of [32]. As anonymizers are independent parties – not necessarily trusted – in RFID networks, the security model needs to include the communication between tags and anonymizers. The construction proposed by Sadeghi et al. [30] includes three actors: readers, tags, and anonymizers, and two protocols: anonymization and identification. Thus, a parallel approach to ours could use anonymization instead of internal key updates in a similar way as we describe here.

Finally, Cremers et al. [7] introduced a further attack against distance-bounding protocols, i.e., distance hijacking attacks, where a malicious tag commits distance fraud in the presence of an honest tag. As our paper focuses on privacy, we do not address this attack, but we stress that a formalized model for the single-reader multiple-tags scenario is highly desirable, and in such a setting, hijacking attacks are essential.

2 Preliminaries

In this paper, we extend the single-reader-single-tag, stateless scenario of [13] to a stateful single-reader-multiple-tag scenario with key updates. We consider distance-bounding security as in [13] and privacy as in [32]. However, key updates enable denial-of-service (DoS) attacks, where the adversary tries to desynchronize the reader and resp. tag states, such that an honest tag cannot authenticate. Such attacks also often break privacy in authentication. Resistance to DoS attacks, or long-term completeness, is here called availability.

We first briefly recall the definition of distance-bounding authentication protocols from [13], then shortly review the models for mafia, distance, and impersonation security, from [13]. Finally, we review the privacy model due to Vaudenay. The additional notion of availability is defined in section 4.

2.1 Distance-bounding Authentication

Though the framework of [13] refers to general distance-bounding between provers and verifiers, they note that distance-bounding is often used for RFID authentication, where the provers are RFID tags and the verifiers are RFID readers. Furthermore, in [13], the reader outputs a single bit (0/1 or reject/accept); thus, though they refer to distance-bounding *identification*, Dürholz et al. achieve *authentication* instead. The single reader and single tag share here a key K generated by a key generation algorithm Kg. Furthermore, the reader is associated with a clock.

Definition 1 ([13]). *An* authentication scheme for timing parameters $(t_{\max}, T_{\max}, E_{\max}, N_c)$ *is a triplet of efficient algorithms* $\mathcal{ID} = (\mathsf{Kg}, \mathcal{R}, \mathcal{T})$ *with:*

KEY GENERATION. *For parameter* $n \in \mathbb{N}$, Kg *generates a secret key* K.
AUTHENTICATION. *The joint execution of algorithms* $\mathcal{T}(K)$ *and* $\mathcal{R}(K)$ *generates, depending on* $t_{\max}$, $T_{\max}$, $E_{\max}$, N_c, *a verifier output* $b \in \{0, 1\}$.

Completeness is assumed: for any $n \in \mathbb{N}$ *and any key* $K \leftarrow \mathsf{Kg}(1^n)$, *the decision bit* b *produced by honest party* $\mathcal{R}(K)$ *interacting with honest party* $\mathcal{T}(K)$ *under the requirements following from the timing parameters, is* 1 *with probability (negligibly close to)* 1.

In the setting of stateful protocols, the key generated by Kg is in fact only an initial key. In fact, we will consider readers and tags having a state $\mathsf{st}_{\mathcal{R}}$ and resp. $\mathsf{st}_{\mathcal{T}}$, which are initialized with the value K at the tag's initialization. These states are updated, either at the end of honest interaction between the reader and the tag, or after an adversary's attack. In this setting thus, it is not always the case that the reader's and the tag's internal states coincide.

We consider distance-bounding protocols consisting of phases, which are either time-critical (the reader uses its clock) or lazy (the clock is not used). The total number of time-critical rounds N_c is a system parameter, which must be small for resource-constrained RFID. As in [13] we consider thresholds $T_{\max}$ and $E_{\max}$ for the number of time-critical rounds where communication takes longer than $t_{\max}$, resp. where the response is erroneous.

2.2 Communication Model

As in [13], we model communication between the reader and tag in sessions with unique identifiers sid. These can be one of the following: reader-tag sessions (here the honest reader interacts with the honest tag, and the adversary observes the interaction); reader-adversary sessions (here the adversary impersonates the tag to an honest

reader); and adversary-tag sessions (where the adversary impersonates the reader to the honest tag). To each session we associate a transcript, which either ends in $\perp$ (if the session is aborted) or in an authentication bit b.

2.3 Mafia and Distance Fraud Resistance

The precise formalization of mafia and distance fraud resistance, as well as impersonation security, can be found in detail in [13]. The notions are exact, in the sense that Dürholz et al. quantify the adversary's efficiency with respect to the following parameters: (1) the time t the adversary run before it halts; (2) the number of reader-tag, reader-adversary, and resp. adversary-tag sessions $q_{\text{OBS}}, q_{\mathcal{R}}$, resp. $q_{\mathcal{T}}$ it runs; and (3) the adversary's advantage of succeeding in a mafia or distance fraud attack. In the following we give only a brief overview of the definitions, referring the reader to [13] for more details.

Mafia fraud Resistance. In this scenario, the adversary attempts to authenticate to the reader in the presence of a tag. The adversary is essentially a man-in-the-middle (MITM), who can open concurrent reader-adversary and adversary-tag sessions sid, resp. sid^*, but *cannot* relay the exact transmissions between homologous phases of sid and sid^*. The definition of Dürholz et al. is very strong in the sense that only pure relay is excluded. An adversary is allowed to flip bits or guess challenges in advance; the attack is only invalidated if both the order *and* the contents of the rounds coincide in the two sessions. A round of pure relaying is called *tainted*. We refer to [13] for more details.

The definition of mafia fraud resistance naturally carries over to the stateful scenario with key updates.

Distance Fraud Resistance. In distance fraud, the adversary *is* the malicious tag, and its goal is to fool the reader into thinking that the tag is closer to it than in reality. In this setting, Dürholz et al. require the adversary to *commit* to the responses of each time-critical phase in advance. This models the idea that the only way to cheat the verifier's clock is to guess the challenges for every time-critical round in advance. Here, rounds are tainted if the adversary does not commit to the responses of time-critical rounds in advance.

Like mafia fraud resistance, distance fraud resistance extends naturally to stateful distance-bounding protocols: in this setting, the key update is essentially irrelevant, since the adversary is the tag itself, and will thus update the state honestly.

2.4 Impersonation Security

Impersonation security is the basic requirement of authentication protocols: adversaries should not authenticate as legitimate provers (apart from pure relays). Note that pure relay is not possible during time-critical phases (where the clock can detect relaying). In early distance-bounding literature, impersonation security was only achieved during the time-critical rounds; therefore, the number N_c of time-critical rounds needs to be

large. However, Avoine and Tchamkerten noted a large value of N_c may not be physically sustained by resource-constrained hardware, like passive and semi-active RFID tags. Thus, lazy-phase impersonation should also be considered. In the framework of Dürholz et al. [13], impersonation security only concerns lazy phases. In particular, impersonation adversaries must authenticate during the lazy phases of a protocol, without purely relaying messages.

2.5 Review of Privacy Model

We briefly review the privacy framework of Vaudenay [32], which considers RFID systems consisting of a single reader, but multiple tags. For the privacy game, tags are associated with handles called *virtual tags* (vtags). The adversary can send messages to the reader and to virtual tags, it can "draw" and "free" vtags (thus assigning them to tags), it can observe honest reader-tag interactions, and it can also corrupt tags (i.e., learn their state). Vaudenay models adversary interactions by means of a number of oracles that $\mathcal{A}$ can access; we refer to the original paper [32] for more details about the formalization of this model.

The four major adversary classes in [32] differ in the way an adversary may corrupt tags (see below). Furthermore, adversaries are *narrow* if they don't know the protocol output (i.e., whether a tag has been accepted or not). Narrowness is an additional property, which can be combined with any of the subsequent four adversary classes:

Weak adversaries. They cannot corrupt tags.

Forward adversaries. Once they have used the tag corruption oracle, forward adversaries may only use this oracle, on other virtual tags.

Destructive adversaries. These adversaries destroy the vtag upon corrupting it, but they are still allowed to interact with the RFID system arbitrarily with respect to other tags.

Strong adversaries. They may use all the articles arbitrarily.

The adversary's success is measured with respect a simulator $\mathcal{B}$ called a Blinder, which simulates all queries except corruption queries to the blinded adversary $\mathcal{A}^{\mathcal{B}}$. The adversary's goal is to distinguish between the real RFID system and an interaction with the blinder, after playing a two-phase game. In the attack phase, $\mathcal{A}$ interacts with all oracles arbitrarily, subject to corruption query restrictions; then, in the analysis phase, the adversary does not access any of the oracles, but receives the secret table containing the correspondence between tag identities and the respective handles. Finally, the adversary returns a bit denoting its success ($b = 1$) or failure in the attack ($b = 0$). Write $\mathcal{A}$ for the adversary, and $\mathcal{A}^{\mathcal{B}}$ for the blinded adversary, and denote:

$$\mathbf{Adv}^{\mathsf{priv}}_{\mathcal{ID}}(\mathcal{A}) = \mathrm{Prob}[\,\mathcal{A}\text{ wins}] - \mathrm{Prob}\left[\,\mathcal{A}^{\mathcal{B}}\text{ wins}\right]$$

Privacy is then defined as follows [32].

Definition 2 (Privacy). *Let $\mathcal{ID}$ be a distance-bounding authentication scheme $\mathcal{ID}$ with timing parameters $(t_{\max}, T_{\max}, E_{\max}, N_c)$. Let $\mathcal{P}$ denote one of the adversary classes defined above. $\mathcal{ID}$ is $\mathcal{P}$-private if for any adversary $\mathcal{A}$ there exists a blinder $\mathcal{B}$ such that $\boldsymbol{Adv}^{\mathsf{priv}}_{\mathcal{ID}}(\mathcal{A})$ is negligible.*

3 Availability; a Compiler for Key Updates

We begin by introducing the notion of long-term completeness for stateful protocols, where both the reader and the tag use key update, which we call availability.

3.1 Availability

In the context of key updates, the notion of completeness – i.e. the property that a reader always accepts a legitimate tag – is no longer static: the adversary can cause a desynchronisation between reader and tag states, such that a legitimate tag is unable to authenticate. Many authentication protocols featuring key updates are vulnerable to these so-called denial-of-service (DoS) attacks, e.g. the two protocols based on YA-TRAP of Chatmon et al. [5]. Note that DoS attacks are one successful way of breaching privacy as defined in the previous section.

We define *availability* as long-term completeness. The adversary may interact arbitrarily with the tag and the reader, also relaying messages. In particular, adversaries may choose to drop messages from honest reader-tag communication. At some point, the adversary stops, and the tag and reader interact in a single round (the adversary is in observation mode). We say that the adversary wins if the (honest) reader outputs a 0 bit. In other words, the adversary wins if (by arbitrary interaction with the reader and the tag), it makes the honest tag unable to authenticate in an honest session with the reader.

Definition 3 (Availability). *Let $\mathcal{ID}$ be an identification scheme $\mathcal{ID}$ with timing parameters $(t_{\max}, T_{\max}, E_{\max}, N_c)$. A $(t, q_{\mathcal{R}}, q_{\mathcal{T}}, q_{\text{OBS}})$ adversary $\mathcal{A}$ wins against availability if the reader rejects in one of the q_{OBS} reader-tag sessions* sid. *We denote by $\boldsymbol{Adv}^{\mathsf{avbl}}_{\mathcal{ID}}(\mathcal{A})$ the probability of $\mathcal{A}$ winning.*

3.2 Our compiler

We proceed to describe a compiler preserving impersonation resistance, as well as mafia and distance fraud resistance, while attaining narrow destructive privacy and availability. In particular, the compiler we present does *not* provably preserve terrorist fraud resistance. We discuss the difficulties of attaining this very strong property after we describe the construction, and we note that attempting to gain terrorist fraud resistance would come at greater computational cost and a compromise in security. Notably, however, whereas the construction presented in [13] (an enhancement of the Kim and Avoine protocol in [21]) is provably mafia and distance fraud resistant, as well as impersonation secure, no other protocol in the literature is, to this date, terrorist

fraud resistant. In fact, [13] show that it might in fact be hard to achieve provable terrorist fraud resistance.

We consider a general distance-bounding authentication scheme $(\mathsf{Kg}, \mathcal{R}, \mathcal{T})$ for parameters $(N_c, t_{\max}, T_{\max}, E_{\max})$ as outlined in the model of Dürholz et al. [13]. Here the reader and each legitimate tag share a key K generated by Kg. As discussed in section 1, there are two additional requirements for this protocol: (1) We require that the outputs of Kg are pseudorandom (i.e. indistinguishable from random), but make no assumption regarding the structure of this protocol; and (2) the protocol must be narrow-weak private in the sense of [32]. Our compiler can be used on such generic protocols to build new distance-bounding protocols $(\mathsf{Kg}^*, \mathcal{R}^*, \mathcal{T}^*)$ for parameters $(N_c, t_{\max}, T_{\max}, E_{\max})$ which are destructive-private in the sense of Vaudenay [32]. Our compiler preserves (the exact levels of) mafia and distance fraud resistance, as well as impersonation security, and grants the new protocol availability (long term completeness).

Efficient Compiler – Description. The compiler takes as input a distance protocol $(\mathsf{Kg}, \mathcal{R}, \mathcal{T})$ with the following properties: (1) $(t^{\text{mafia}}, q_{\mathcal{R}}^{\text{mafia}}, q_{\mathcal{T}}^{\text{mafia}}, q_{\text{OBS}}^{\text{mafia}}, \epsilon^{\text{mafia}})$ resistant to mafia fraud attacks; (2) $(t^{\text{mafia}}, q_{\mathcal{R}}^{\text{dist}}, \epsilon^{\text{dist}})$ resistant to distance fraud attacks; (3) $(t^{\text{imp}}, q_{\mathcal{R}}^{\text{imp}}, q_{\mathcal{T}}^{\text{imp}}, q_{\text{OBS}}^{\text{imp}}, \epsilon^{\text{imp}})$ secure against impersonations; and (4) narrow-weak private in the sense of Vaudenay [32]. Additionally, we require that the values K output by the key generation algorithm Kg are pseudorandom. The compiler outputs a protocol $(\mathsf{Kg}^*, \mathcal{R}^*, \mathcal{T}^*)$ having the same properties (1) – (3), as well as being (4^*) destructive private in the sense of Vaudenay [32]. The latter property also implies availability.

Our idea is to tweak the destructive-private construction due to Vaudenay [32] in order to achieve availability more efficiently and wrap it around the underlying protocol. In particular, we use the following three tricks: (1) the tag updates state early, before the distance-bounding protocol is run (2) the reader only updates states at every successful authentication session; (3) in the initial phase of the protocol, the reader uses lazy phase authentication to "catch up" with the tag: i.e. if the tag has updated state more often than the reader, the reader now catches up with the current state of the tag. Informally, these three strategies help us achieve availability.

Due to trick number (3), the adversary can only desynchronise the tag and reader if the tag does *not* update state, while the reader *does* update state (else, the reader and tag can catch up at the next honest session). Since we use trick number (1), this can only occur if the tag does *not* engage in the distance-bounding protocol. However, due to trick number (2) this implies that the adversary needs to authenticate on its own to the reader, a fact prevented by the mafia *and* impersonation security of the underlying distance-bounding protocol.

Apart from availability, there is an additional problem that must be considered when designing the compiler, and which is a direct consequence of its generality. In particular, in protocols like that of Kim and Avoine [21], the reader $\mathcal{R}$ generates its time-critical round input based on the secret key. Thus, in order to run an underlying, stateless protocol as a black box, the reader must know which state the tag is in before running the protocol. In our compiler, this is achieved by having a round of PRF-based authentication before running the distance-bounding protocol. This step,

however, is not necessary if the underlying protocol can be run (up to the verification steps) without knowledge of the secret key. We thus show some optimizations of the compiler after describing and discussing the general construction. We also note that the tag updates state just after this state recognition step.

Let $\mathcal{ID} = (\mathsf{Kg}, \mathcal{R}, \mathcal{T})$ be a distance-bounding authentication scheme. We describe the compiled scheme $\mathcal{ID}^* = (\mathsf{Kg}^*, \mathcal{R}^*, \mathcal{T}^*)$. The key generation algorithm Kg^* runs Kg as a black box, generating the pseudorandom key K. The tag and reader keep internal states both instantiated with K, i.e. $\mathsf{st}_{\mathcal{T}} = K$ and resp. $\mathsf{st}_{\mathcal{R}} = K$. Then Kg^* also generates a key sk, which is shared by the reader and tag. The algorithms $\mathcal{R}^*$ and $\mathcal{T}^*$ are changed as depicted in Fig. 3.2. Let F and G denote two pseudo-random functions (PRF) independent of any other PRFs used by the distance-bounding protocol. The short notation $\mathcal{R}^{NA}$ denotes the exact running of the reader protocol $\mathcal{R}$ without the verification steps and the (generation of the) authentication bit. By $\mathcal{R}^A(\mathsf{st}_{\mathcal{R}})$ we denote the run of the verification steps as in $\mathcal{R}$ for the secret key stored in $\mathsf{st}_{\mathcal{R}}$; we also write $b \leftarrow \mathcal{R}^A(\mathsf{st}_{\mathcal{R}})$ to denote that the verification output is a bit b. Denote by $\tau(\mathcal{T})$ the transcript of the messages received and sent by the tag in the current authentication session.

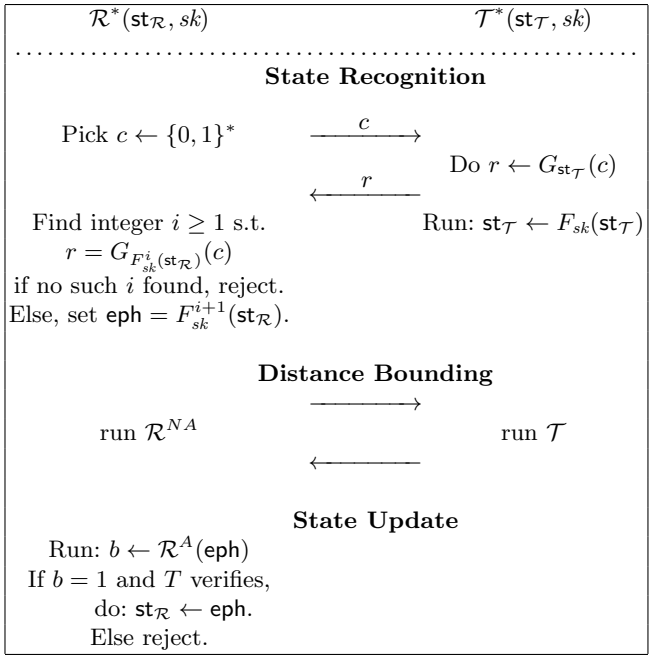

Fig. 1. Generic Compiler: preservation of impersonation security, mafia, and distance fraud resistance

This compiler is a modification of the narrow-destructive authentication protocol due to Vaudenay [32]. As previously noted, in [32] the tag updates state at every authentication attempt, but the reader's state remains set to the initial key K generated

by Kg. Our approach greatly improves the reader run-time (since the reader does not need to start its search for index i from 0 at every authentication attempt). We briefly give an intuition why the distance-bounding properties of the underlying protocol are preserved before giving a formal proof of the security statements. We also discuss why terrorist fraud resistance is *not* achieved.

Pseudorandomness of K. Once we introduce key updates, we have to ensure that the distance-bounding protocol still preserves its properties for the pseudorandom keys generated by iterating the PRF F. Thus, the updated keys must be indistinguishable from each other *and from the original key*. Note that it is possible to have a protocol that is mafia, distance, and impersonation resistant if the key generated by Kg is $K = \mathbf{0}^n$, i.e. the all-zero vector of dimension n, but not for another key. Thus, the initial instance of $(\mathsf{Kg}, \mathcal{R}, \mathcal{T})$ (for state K) is mafia, distance, and impersonation resistant, but no other instances are resistant to these attacks (as the state is updated).

Mafia Fraud Resistance. The protocol (Kg, $\mathcal{R}$, $\mathcal{T}$) is mafia fraud resistant. Since all the states, i.e. keys, are indistinguishable, an adversary against the mafia fraud resistance of the modified scheme $(\mathsf{Kg}^*, \mathcal{R}^*, \mathcal{T}^*)$, the adversary roughly succeeds in impersonating to $\mathcal{R}^*$ for one particular $\mathsf{st}_{\mathcal{T}}$ as it does for another. During the reduction, the adversary will simply have to guess which of the (polynomially many) states will be used for authentication.

Distance Fraud Resistance. This property is trivially preserved, as distance fraud adversaries know all the correct states, which are indistinguishable from one another (thus one session of distance fraud is as easy to attack as another).

Impersonation security. As for mafia fraud resistance, impersonation security is preserved because an adversary against the stateful protocol is as likely to succeed in impersonating the tag for one state as for another. The level of impersonation security is in fact increased, due to the initial authentication step, i.e. the state recognition.

We discuss more in detail why terrorist fraud resistance is not preserved after outlining the security properties of our compiler.

3.3 Compiler properties

Theorem 1. *Let $\mathcal{ID} = (\mathsf{Kg}, \mathcal{R}, \mathcal{T})$ be a distance-bounding protocol for timing parameters $(t_{\max}, N_c, E_{\max}, T_{\max})$, with the restriction that Kg outputs only pseudorandom keys. Let $\mathcal{ID}^* = (\mathsf{Kg}^*, \mathcal{R}^*, \mathcal{T}^*)$ be the distance-bounding protocol obtained by running the compiler in figure 3.2 on $\mathcal{ID}$. The following statements hold:*

Mafia Fraud. *For every $(t^{mafia}, q_{\mathcal{R}}^{mafia}, q_{\mathcal{T}}^{mafia}, q_{\text{OBS}}^{mafia}, \epsilon^{mafia})$-adversary $\mathcal{A}^*$ against the mafia fraud of $\mathcal{ID}^*$ there is an adversary $\mathcal{A}$ against the mafia fraud of $\mathcal{ID}$, running in time $\mathcal{O}((\,)\, t^{mafia})$ running: no eavesdropping sessions against $\mathcal{ID}$, at most* 1 *session with the tag, and at most $q_{\mathcal{R}}^{mafia}$ sessions with the reader, and winning with probability of at least (up to negligible terms) $\frac{1}{q_{\mathcal{T}}^{mafia} \cdot q_{\text{OBS}}^{mafia}} \epsilon^{mafia}$.*

Distance Fraud. *For every $(t^{dist}, q_{\mathcal{R}}^{dist}, \epsilon^{dist})$-adversary $\mathcal{A}^*$ against the distance fraud of $\mathcal{ID}^*$ there is an adversary $\mathcal{A}$ against the distance fraud of $\mathcal{ID}$, running in time*

$\mathcal{O}(()\, t^{dist})$ *running at most* $q_{\mathcal{R}}^{dist}$ *sessions with the reader, and winning with probability of at least (up to negligible terms)* ϵ^{dist}.

Impersonation Security. *For every* $(t^{imp}, q_{\mathcal{R}}^{imp}, q_{\mathcal{T}}^{imp}, q_{\text{OBS}}^{imp}, \epsilon^{imp})$*-adversary* $\mathcal{A}^*$ *against the impersonation security of* $\mathcal{ID}^*$ *there is an adversary* $\mathcal{A}$ *against the impersonation security of* $\mathcal{ID}$*, running in time* $\mathcal{O}(()\, t^{imp})$ *running: no eavesdropping sessions against* $\mathcal{ID}$*, at most* 1 *session with the tag, and at most* $q_{\mathcal{R}}^{imp}$ *sessions with the reader, and winning with probability of at least (up to negligible terms)* $\frac{1}{q_{\mathcal{T}}^{imp} \cdot q_{\text{OBS}}^{imp}} \epsilon^{imp}$.

Availability. *For every* $(t, q_{\mathcal{R}}, q_{\mathcal{T}}, q_{\text{OBS}}, \epsilon)$*-adversary* $\mathcal{A}^*$ *against the availability of* $\mathcal{ID}^*$ *there exist: an adversary* $\mathcal{A}^{\mathsf{PRF}}$ *against the pseudo-randomness of* G*; an adversary* $\mathcal{A}^{imp}$ *against the impersonation fraud of* $\mathcal{ID}$*; and an adversary* $\mathcal{A}^{mafia}$ *against the mafia-fraud resistance of* $\mathcal{ID}$ *such that:*

$$\boldsymbol{Adv}_{G}^{\mathsf{PR}}(\mathcal{A}^{\mathsf{PRF}}) \cdot \boldsymbol{Adv}_{\mathcal{ID}}^{imp}(\mathcal{A}^{imp}) \cdot \boldsymbol{Adv}_{\mathcal{ID}}^{mafia}(\mathcal{A}^{mafia}) \geq \epsilon.$$

Here, $\boldsymbol{Adv}_{G}^{\mathsf{PR}}(\mathcal{A}^{\mathsf{PRF}})$ *is the advantage of* $\mathcal{A}^{\mathsf{PRF}}$ *to win against the pseudo-randomness of* G*, and* $\boldsymbol{Adv}_{\mathcal{ID}}^{imp}(\mathcal{A}^{imp})$*, resp.* $\boldsymbol{Adv}_{\mathcal{ID}}^{mafia}(\mathcal{A}^{mafia})$ *are the advantages of* $\mathcal{A}^{imp}$*, resp.* $\mathcal{A}^{mafia}$ *to win against the impersonation security, resp. the mafia fraud resistance of* $\mathcal{ID}$.

Privacy. *Assuming that* $\mathcal{ID}$ *is narrow-weak private, the compiled scheme is narrow-destructive private in the sense of Vaudenay.*

Proof. **Mafia Fraud Resistance.** Assume that there exists a $(t, q_{\text{OBS}}, q_{\mathcal{R}}, q_{\mathcal{T}})$-mafia fraud adversary $\mathcal{A}^*$ winning against the compiled protocol $\mathcal{ID}^*$ with probability ϵ. We construct an adversary $\mathcal{A}$ against the mafia fraud resistance of $\mathcal{ID}$ that wins with probability at least $\frac{1}{q_{\text{OBS}} q_{\mathcal{T}}}\epsilon + \mathbf{Adv}_{F}^{\mathsf{PR}}(\mathcal{A}^*) + \mathbf{Adv}_{\mathsf{Kg}}^{\mathsf{PR}}(\mathcal{A}^*)$, where $\mathbf{Adv}_{F}^{\mathsf{PR}}(\mathcal{A}^*)$, resp. $\mathbf{Adv}_{\mathsf{Kg}}^{\mathsf{PR}}(\mathcal{A}^*)$ are the distinguishing advantage against the PRF F, resp. the output of Kg. Note that the game $\mathcal{A}$ plays against $\mathcal{ID}$ only uses a single state; thus for our reduction, the adversary $\mathcal{A}$ has to guess when adversary $\mathcal{A}^*$ makes its successful impersonation attempt.

In particular, $\mathcal{A}$ must guess which state the tag $\mathcal{T}^*$ and the reader $\mathcal{R}^*$ share when $\mathcal{A}^*$ succeeds in its impersonation attempt. For this state, $\mathcal{A}$ answers all of $\mathcal{A}^*$'s queries by forwarding them to $\mathcal{R}$ and resp. $\mathcal{T}$ (note that the initial state recognition is done in a lazy phase, thus it can be simply forwarded by the adversary $\mathcal{A}^*$). For all other states, $\mathcal{A}$ simulates the reader and tag protocols for a randomly chosen key (generated honestly through Kg). This simulation does not significantly affect $\mathcal{A}^*$'s success probability, due to the pseudorandomness of F, resp. of the keys output by Kg. In fact, $\mathcal{A}^*$'s success probability only decreases by $\mathbf{Adv}_{F}^{\mathsf{PR}}(\mathcal{A}^*) + \mathbf{Adv}_{\mathsf{Kg}}^{\mathsf{PR}}(\mathcal{A}^*)$ accounting for the distinguishing advantage against F and resp. the output of Kg.

In order to guess the shared state for the successful impersonation, $\mathcal{A}$ needs to guess exactly (a) how many reader-tag sessions $\mathcal{A}^*$ runs before the successful authentication (since reader-updates sessions make both $\mathcal{R}^*$ and $\mathcal{T}^*$ update state) and (b) how many successful adversary-tag sessions $\mathcal{A}^*$ runs after the last reader-tag session and before its successful impersonation (since adversary-tag sessions could, depending on the underlying protocol, change the tag's state making the reader catch up to a different state). Now $\mathcal{A}$ guesses both these values with probability $\frac{1}{q_{\text{OBS}}^{\text{mafia}} q_{\mathcal{T}}^{\text{mafia}}}$. If $\mathcal{A}^*$ initiates

another reader-tag session or another adversary-tag session before successfully authenticating, $\mathcal{A}$ outputs $\perp$ and halts (it fails). This happens if $\mathcal{A}$ has guessed either q_o or q_t incorrectly. During session q_t (which is an adversary-tag session), $\mathcal{A}$ must simulate the environment for $\mathcal{A}^*$. Upon receiving the challenge c, the adversary forwards a value r at random (this affects $\mathcal{A}^*$'s success probability by at most the distinguishing advantage against G) and during the distance-bounding phase, $\mathcal{A}$ forwards $\mathcal{A}^*$'s queries to $\mathcal{T}$ and then forwards $\mathcal{T}$'s responses. For every reader-adversary session that $\mathcal{A}^*$ initiates (note that there can be at most $q_{\mathcal{R}}^{\text{mafia}}$ such sessions), $\mathcal{A}$ opens a reader-adversary session and queries $\mathcal{R}$ as $\mathcal{A}^*$ queries $\mathcal{T}^*$. Now $\mathcal{A}^*$ wins with probability negligibly close to $\frac{\epsilon^{\text{mafia}}}{q_{\text{OBS}}q_{\mathcal{T}}}$ in one of the maximum $q_{\mathcal{R}}^{\text{mafia}}$ reader-adversary sessions, and so does $\mathcal{A}$. This yields the bound above for $\mathcal{A}^*$.

Impersonation security. The same applies for impersonation security, except that (intuitively) $\mathcal{A}$ also gains some security in future impersonation attempts (for the initial state recognition phase). The reduction works as before, with $\mathcal{A}$ simulating all but one session for $\mathcal{A}^*$.

Distance fraud resistance. This statement follows trivially: since distance fraud adversaries are malicious tags, they know the secret keys resp. states. Since the outputs of Kg are pseudorandom, the distance fraud level just transfers trivially.

Privacy. This proof follows the lines of the proof of theorem 15 in [32], with the following changes: (1) up to a negligible difference ($\mathbf{Adv}_F^{\mathsf{PR}}(\mathcal{A}^*) + \mathbf{Adv}_{\mathsf{Kg}}^{\mathsf{PR}}(\mathcal{A}^*)$) we disregard the key update step and assume that the same key is being used (this is possible since corrupted tags are destroyed, and since states are pseudorandom); thus we reduce destructive privacy to the narrow-weak privacy of the underlying protocol, thus (2) replacing the random c output by the blinder in simulated $\mathsf{SendTag}$ queries against $\mathcal{ID}^*$ by the responses given by the narrow-weak private blinder against $\mathcal{ID}$. Under the assumption of (1) this is a perfect simulation of $\mathsf{SendTag}$ queries. The rest of the proof is the same as in [32].

Availability. The scheme $\mathcal{ID}^*$ is available under the assumption of completeness for $\mathcal{ID}$. In this setting, adversaries can run reader-tag sessions where they observe communication, can interact either with the reader or with the tag separately, or they can run MITM attacks (even using pure relay). Note that it is only possible to break availability if the reader updates state but the tag does not. A reader-tag session will make both reader and tag update state; thus this will not help the adversary. If the adversary runs an adversary-tag session, the tag may update state, but the reader does not. If the adversary runs a reader-adversary session (without running a parallel adversary-tag session), if the adversary fails to authenticate, then the reader does not update state.

The adversary $\mathcal{A}$ can only win in a reader-adversary session, which can be run either in a MITM attack or in a separate reader-adversary interaction. If the adversary runs a MITM attack and forwards the tag a challenge (be it the reader's challenge or another challenge), the tag updates state, and thus the adversary fails. Therefore,

the adversary only wins if it wins in a reader-adversary interaction without querying the tag. Thus, the adversary must (i) pass the initial state recognition phase; (ii) authenticate during distance bounding. In order to achieve step (ii) the adversary must break both the impersonation security and the mafia-fraud resistance of the underlying distance-bounding protocol. The adversary passes the initial state recognition only if it can break the pseudorandomness of G. Thus we have the indicated bound. □

3.4 Optimizations

No mutual authentication. The initial state update computation in the compiler (which is quite computationally expensive) is required by protocols with no partial reader-authentication, as e.g. the protocol in [21]. However, many distance-bounding protocols, e.g. [17,1] do not feature reader authentication. In this case, the compiler can be simplified as in Figure 2. This compiler can be used if the underlying bounding protocol has properties (1-4) as in theorem 1, and (5) the partial reader protocol $\mathcal{R}^{NA}$ is independent of the state $\mathsf{st}_{\mathcal{R}}$ of the reader. Protocols fulfilling this conditions are, e.g. [2,17,1].

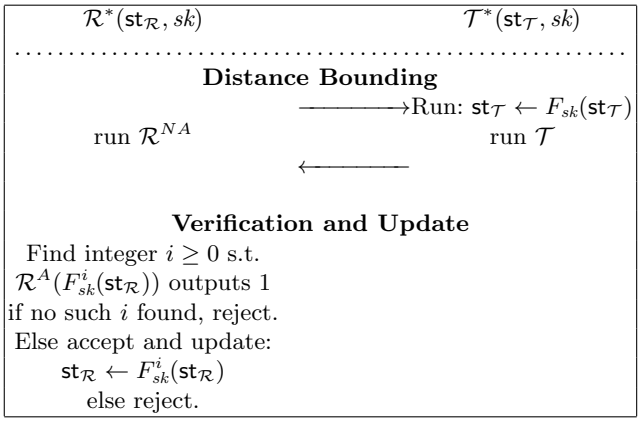

Fig. 2. Compiler for protocols with no mutual authentication

Merging authentication steps. Even if some reader authentication is used, we can gain efficiency by merging the state recognition step with impersonation security. Some distance-bounding schemes, e.g. [1], have some PRF-based lazy-phase authentication preceding the time-critical rounds. In particular, we require that the underlying scheme $\mathcal{ID}$ has phases $1, \ldots, n$ such that there is a (lazy) phase l where $\mathcal{T}$ sends a (part of the) output of a PRF function G^* computed on state information $\mathsf{st}_{\mathcal{T}}$ (for static protocols, this can be the key generated by Kg) to the reader *and* there is no phase $1, \ldots, l-1$ in $\mathcal{R}^{NA}$ that depends on $\mathsf{st}_{\mathcal{R}}$. Then, we tweak the compiler using the partial output of G^* for state recognition, replacing G by G^*.

3.5 Why Terrorist Resistance doesn't Work

Mafia and impersonation resistance are preserved despite the key update since the adversary has no inside information about the updating process. Thus, the adversary has only an outside view on the keys (which are indistinguishable from one another). In the mafia and impersonation fraud proofs, we argue that, except with negligible probability, an adversary learns as much information for one state as he does for another. For distance fraud, the adversary is the tag itself. As the keys are, except with negligible probability, indistinguishable from each other, the adversary has as much probability to succeed in a single instance of the secret key as it does for multiple keys.

For terrorist fraud resistance, the adversary is at neither of the two extremes, i.e. it *may* learn some insider information about the states and about the updating process, but it does *not* have complete information about it (else, it can then authenticate without the malicious tag). Dürholz et al. [13] define terrorist fraud resistance in terms of a simulator. Informally, once an adversary having offline contact with a malicious tag succeeds, the simulator also gets as many attempts as the adversary to authenticate to the reader. The simulator, however, only has access to the adversary's transcripts. A protocol is terrorist fraud resistant if for any adversary that succeeds with probability $p_{\mathcal{A}}$, there exists a simulator $\mathcal{S}$ that, once the adversary is successful, runs as many impersonation attempts as $\mathcal{A}$ and wins with probability $p_{\mathcal{S}} \geq p_{\mathcal{A}}$. Intuitively, the information given by the malicious tag to the adversary not only helps it authenticate in a specific impersonation attempt, but the adversary can then also authenticate without the tag's help with at least as much probability.

Our compiler does not preserve terrorist fraud resistance in a provable way, because the malicious tag could reveal some partial information about the secret key sk (though not the entire key), thus giving the adversary some insight for a particular state, but not for others; thus the simulator cannot authenticate with equal probability afterwards. It seems therefore hard to find a compiler that preserves terrorist fraud resistance for *all* distance-bounding protocols.

We also note that in general, terrorist fraud resistant constructions must provide a back door for the simulator (since we want *provable* terrorist fraud resistance in a very strong sense, and the simulator must account for all possible malicious-tag-strategies). This back door, however, may be inefficient to achieve in practice. Furthermore, the protocol may lose some of its mafia and distance fraud security (since the back door could be used by the adversary in, say, distance fraud). We leave it an open question to achieve a generic compiler that preserves terrorist fraud resistance for distance-bounding protocols.

4 Application: enhanced Kim-Avoine

We apply our compiler to the protocol presented in [13], which is an extension of the original scheme in [21]. This scheme uses a PRF *and* mutual authentication. We apply the optimized compiler with merged authentication steps from section 3.4, and show

the result in figure 4. Due to space limitations, we only show the protocol below and give the security statements and the proof of narrow weak privacy in the appendix. This, combined with the results of [13] prove that the compiled protocol is narrow-destructive private as in [32].

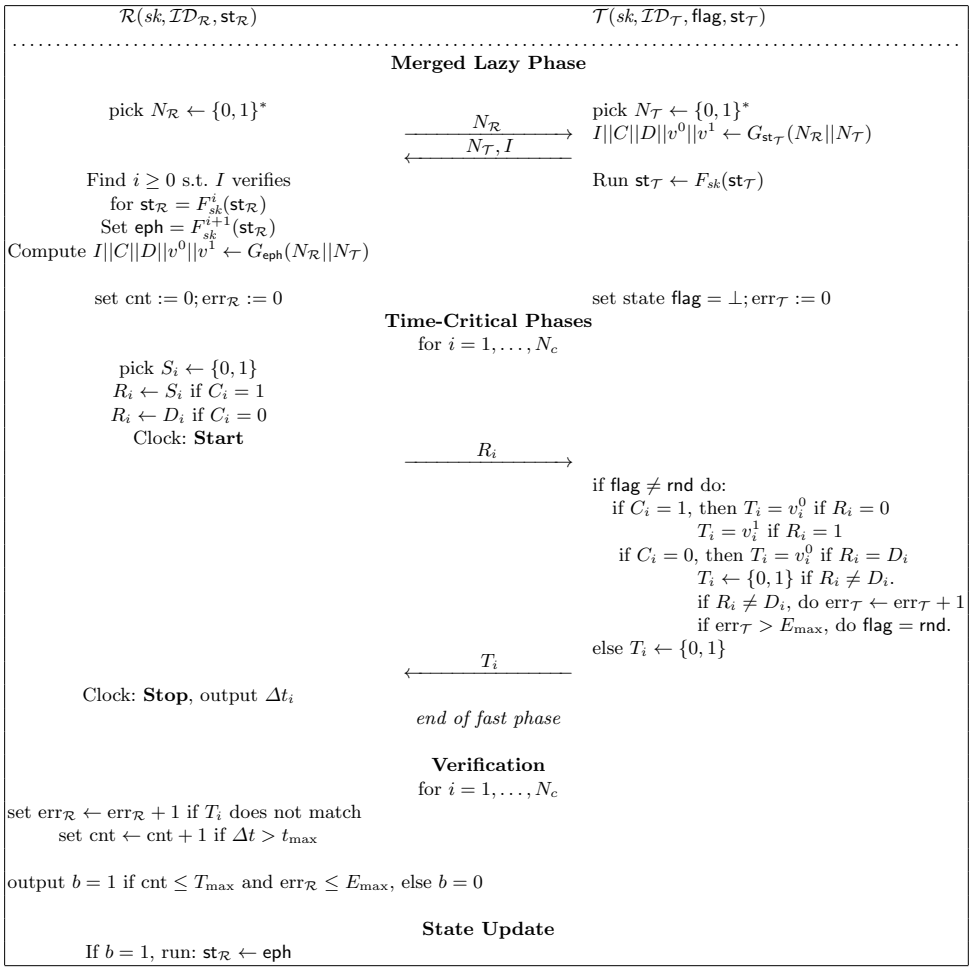

Fig. 3. Compiled enhanced Kim/Avoine protocol.

References

1. Avoine, G., Tchamkerten, A.: An efficient distance bounding RFID authentication protocol: Balancing false-acceptance rate and memory requirement. In: Information Security. Lecture Notes in Computer Science, vol. 5735, pp. 250–261. Springer-Verlag (2009)
2. Brands, S., Chaum, D.: Distance-bounding protocols. In: Advances in Cryptology — Eurocrypt'93. pp. 344–359. Lecture Notes in Computer Science, Springer-Verlag (1993)

3. Bringer, J., Chabanne, H.: Trusted-HB: A low-cost version of HB $^{+}$ secure against man-in-the-middle attacks. Transactions on Information Theory 54(9), 4339–4342 (2008)
4. Bussard, L., Bagga, W.: Distance-bounding proof of knowledge to avoid real-time attacks. IFIP International Federation for Information Processing, vol. 181, pp. 222–238. Springer-Verlag (2005)
5. Chatmon, C., van Le, T., Burmester, M.: Secure anonymous rfid authentication protocols. Florida State University, Department of Computer Science, Tech Report (2006)
6. Clulow, J., Hancke, G.P., Kuhn, M.G., Moore, T.: So near and yet so far: Distance-bounding attacks in wireless networks. In: European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks. Lecture Notes in Computer Science, vol. 4357, pp. 83–97. Springer-Verlag (2006)
7. Cremers, C., Rasmussen, K.B., Čapkun, S.: Distance hijacking attacks on distance bounding protocols. Cryptology ePrint Archive, Report 2011/129 (2011), ePRINTURL
8. Deng, R.H., Li, Y., Yung, M., Zhao, Y.: A new framework for RFID privacy. In: Proceedings of the 15th European Symposium on Research in Computer Security, (ESORICS'10). Lecture Notes in Computer Science, vol. 6514, pp. 1–18. Springer-Verlag (2010)
9. Deng, R.H., Li, Y., Yung, M., Zhao, Y.: A zero-knowledge based framework for RFID privacy. In: Journal of Computer Security, (JSC), IOS 2011 (2011)
10. Desmedt, Y.: Major security problems with the 'unforgeable' (feige)-fiat-shamir proofs of identity and how to overcome them. In: SecuriCom. pp. 15–17. SEDEP Paris, France (1988)
11. Drimer, S., Murdoch, S.J.: Keep your enemies close: distance bounding against smartcard relay attacks. In: Proc. of the 16-th USENIX Security Symposium on USENIX Security Symposium, article no. 7. ACM Press (2007)
12. Duc, D., Kim, K.: Securing HB+ against GRS man-in-the-middle attacks. In: Symposium on Cryptography and Information Security (SCIS). The Institute of Electronics, Information and Communication Engineers (2007)
13. Dürholz, U., Fischlin, M., Kasper, M., Onete, C.: A formal approach to distance bounding RFID protocols. In: Proceedings of the 14$^{\text{th}}$ Information Security Conference ISC 2011. pp. 47–62. Lecture Notes in Computer Science, Springer-Verlag (2011)
14. Gilbert, H., Robshaw, M., Sibert, H.: An active attack against HB+ - a provably secure lightweight authentication protocol. Cryptology ePrint Archive, Report 2005/237 (2005), ePRINTURL
15. Haataja, K., Toivanen, P.: Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures. Transactions on Wireless Communications 9(1), 384–392 (2010)
16. Hancke, G.P.: A practical relay attack on ISO 14443 proximity cards (2005)
17. Hancke, G.P., Kuhn, M.G.: An RFID distance bounding protocol. In: SECURECOMM. pp. 67–73. ACM Press (2005)
18. Hermans, J., Pashalidis, A., Vercauteren, F., Preneel, B.: A new RFID privacy model. In: Proceedings of the 16th European Symposium on Research in Computer Security, (ESORICS'11). Lecture Notes in Computer Science, vol. 6879, pp. 568–587. Springer-Verlag (2011)
19. Hopper, N.J., Blum, M.: Secure human identification protocols. In: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security ADVCRYPTO. Lecture Notes in Computer Science, vol. 2248, pp. 52–66. Springer-Verlag (2001)
20. Juels, A., Weis, S.A.: Defining strong privacy for RFID. In: International Conference on Pervasive Computing and Communications - Workshops (PerCom Workshops). pp. 342–347. IEEE Computer Society Press (2007)
21. Kim, C.H., Avoine, G.: RFID distance bounding protocol with mixed challenges to prevent relay attacks. In: Proceedings of the 8th International Conference on Cryptology and Networks Security (CANS 2009). Lecture Notes in Computer Science, vol. 5888, pp. 119–131. Springer-Verlag (2009)
22. Kim, C.H., Avoine, G., Koeune, F., Standaert, F.X., Pereira, O.: The swiss-knife RFID distance bounding protocol. In: Proceedings of the 14$^{\text{th}}$ Information Security Conference ISC 2011. pp. 98–115. Lecture Notes in Computer Science, Springer-Verlag (2009)
23. Leng, X., Mayes, K., Markantonakis, K.: HB-MP+ protocol: An improvement on the HB-MP protocol. In: International Conference on RFID. pp. 118–124. IEEE Computer Society Press (2008)
24. Ma, C., Li, Y., Deng, R.H., Li, T.: RFID privacy: relation between two notions, minimal condition, and efficient construction. In: Proceedings of the 16th ACM conference on Computer and communications security, (CCS'09). pp. 54–65. ACM Press (2009)

25. Ng, C.Y., Susilo, W., Mu, Y., Safavi-Naini, R.: RFID privacy models revisited. In: Proceedings of the 13th European Symposium on Research in Computer Security, (ESORICS'08). Lecture Notes in Computer Science, vol. 5283, pp. 251–266. Springer-Verlag (2008)
26. Ouafi, K., Overbeck, R., Vaudenay, S.: On the security of HB# against a man-in-the-middle attack. In: Advances in Cryptology — Asiacrypt 2008. Lecture Notes in Computer Science, vol. 5350, pp. 108–124. Springer (2008)
27. Paise, R.I., Vaudenay, S.: Mutual authentication in rfid: Security and privacy. In: ASIACCS. pp. 292–299. ACM Press (2008)
28. Rasmussen, K.B., Čapkun, S.: Realization of RF distance bounding. In: Proceedings of the USENIX Security Symposium, 2010 (2010)
29. Reid, J., Nieto, J.M.G., Tang, T., Senadji, B.: Detecting relay attacks with timing-based protocols. In: ASIACCS. pp. 204–213. ACM Press (2007)
30. Sadeghi, A.R., Visconti, I., Wachsmann, C.: Anonymizer-enabled security and privacy for RFID. In: Advances in Cryptology — Asiacrypt'08. Lecture Notes in Computer Science, vol. 5888, pp. 292–299. Springer-Verlag (2009)
31. Trujillo-Rasua, R., Martin, B., Avoine, G.: The poulidor distance-bounding protocol. In: RFIDSec 2010. pp. 239 – 257
32. Vaudenay, S.: On privacy models for rfid. In: Advances in Cryptology — Asiacrypt'07. Lecture Notes in Computer Science, vol. 4883, pp. 68–87. Springer-Verlag (2007)

A Appendix

A.1 The Kim and Avoine Protocol Extension

We give a brief overview of the enhancement shown in [13] of the well-known scheme due to Kim and Avoine in [21]. The notation in the original paper is modified slightly to reflect the notation we use in this paper. We refer the reader to [13] for more details and for a proof of the security statement.

Theorem 2 (Security Properties). *The distance bounding protocol $\mathcal{ID}$ in Fig. 4 with parameters $(T_{\max}, t_{\max}, E_{\max}, N_c)$ has the following properties:*

- *It is not terrorist-fraud resistant.*
- *For any $(t, q_{\mathcal{R}}, q_{\mathcal{T}}, q_{\text{OBS}})$-impersonation adversary $\mathcal{A}$ against $\mathcal{ID}$ there exists a (t', q')-distinguisher $\mathcal{A}'$ against G (with $t' = t + O(n)$ and $q' = q_{\mathcal{R}} + q_{\mathcal{T}} + q_{\text{OBS}}$) such that,*

$$\boldsymbol{Adv}^{imp}_{\mathcal{ID}}(\mathcal{A}) \leq q_{\mathcal{R}} \cdot 2^{-|I|} + \boldsymbol{Adv}^{\mathsf{PR}}_{G}(\mathcal{A}') + \binom{q_{\mathcal{T}}}{2} \cdot 2^{-|N_{\mathcal{T}}|} + \binom{q_{\mathcal{R}} + q_{\text{OBS}}}{2} \cdot 2^{-|N_{\mathcal{R}}|}.$$

- *For any $(t, q_{\mathcal{R}}, q_{\mathcal{T}}, q_{\text{OBS}})$-distance-fraud adversary $\mathcal{A}$ against $\mathcal{ID}$ there is a (t', q')-distinguisher $\mathcal{A}'$ against G (where $t' = t + O(n)$ and $q' = q_{\mathcal{R}} + q_{\mathcal{T}} + q_{\text{OBS}}$) such that, for $N_t = T_{\max} + E_{\max}$*

$$\boldsymbol{Adv}^{dist}_{\mathcal{ID}}(\mathcal{A}) \leq q_{\mathcal{R}} \cdot \binom{N_c}{N_t} \left(\frac{7}{8}\right)^{N_c - N_t} + \binom{q_{\mathcal{R}} + q_{\text{OBS}}}{2} \cdot 2^{-|N_{\mathcal{R}}|} + \boldsymbol{Adv}^{\mathsf{PR}}_{G}(\mathcal{A}').$$

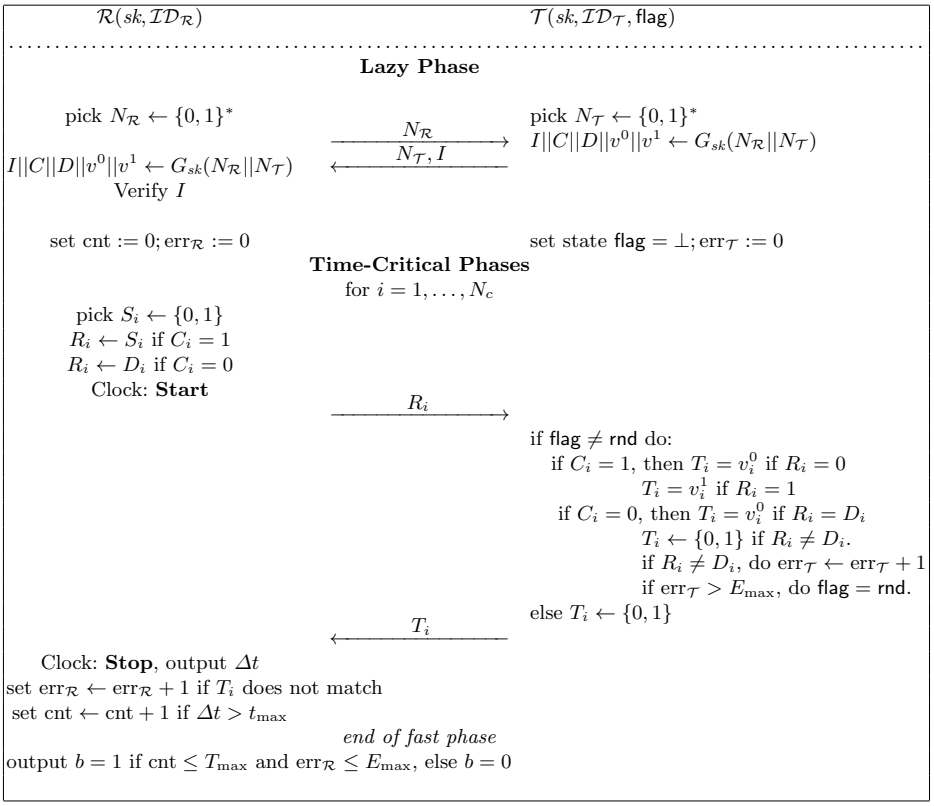

Fig. 4. Enhanced Kim/Avoine protocol.

– *For any $(t, q_\mathcal{R}, q_\mathcal{T}, q_{\mathrm{OBS}})$-Mafia-fraud adversary $\mathcal{A}$ against $\mathcal{ID}$ there exists a (t', q')-distinguisher $\mathcal{A}'$ against G (where $t' = t + O(n)$ and $q' = q_\mathcal{R} + q_\mathcal{T} + q_{\mathrm{OBS}}$) such that, for $N_t = T_{\max} + 2E_{\max}$*

$$\begin{aligned}\boldsymbol{Adv}^{mafia}_{\mathcal{ID}}(\mathcal{A}) \leq \tfrac{5}{8} \cdot q_\mathcal{R} \binom{N_c}{N_t} \cdot (N_c - N_t + 2) \cdot 2^{-(N_c - N_t)} \\ + \binom{q_\mathcal{T}}{2} \cdot 2^{-|N_\mathcal{T}|} + \binom{q_\mathcal{R} + q_{\mathrm{OBS}}}{2} \cdot 2^{-|N_\mathcal{R}|} \\ + \boldsymbol{Adv}^{dist}_{\mathsf{PRF}}(\mathcal{A}').\end{aligned}$$

A.2 Security Properties of the Compiled Kim-Avoine Scheme

Lemma 1. *Let $\mathcal{ID} = (\mathsf{Kg}, \mathcal{R}, \mathcal{T})$ be the distance-bounding protocol for timing parameters $(t_{\max}, N_c, E_{\max}, T_{\max})$ shown in [13], with the restriction that Kg outputs only pseudorandom keys. Then the compiled protocol shown in Figure 4 has the following properties:*

– *For any $(t, q_\mathcal{R}, q_\mathcal{T}, q_{\mathrm{OBS}})$-impersonation adversary $\mathcal{A}$ against $\mathcal{ID}$ there exist: a (t', q')-distinguisher $\mathcal{A}'$ against G and a (t'', q'')-distinguisher $\mathcal{A}''$ against F (with $t' =$*

$t + O(n)$, $t'' = t + O(n)$ *and* $q' = q'' = q_{\mathcal{R}} + q_{\mathcal{T}} + q_{\text{OBS}}$*) such that,*

$$\boldsymbol{Adv}^{imp}_{\mathcal{ID}}(\mathcal{A}) \leq (q_{\text{OBS}} q_{\mathcal{T}})[q_{\mathcal{R}} \cdot 2^{-|I|} + \boldsymbol{Adv}^{dist}_{\mathsf{PRF}}(\mathcal{A}') + \binom{q_{\mathcal{R}} + q_{\text{OBS}}}{2} \cdot 2^{-|N_{\mathcal{R}}|} + \binom{q_{\mathcal{T}}}{2} \cdot 2^{-|N_{\mathcal{T}}|} + \boldsymbol{Adv}^{\mathsf{PR}}_{F}(\mathcal{A}'') + \boldsymbol{Adv}^{\mathsf{PR}}_{G}(\mathcal{A}').$$

– *For any* $(t, q_{\mathcal{R}}, q_{\mathcal{T}}, q_{\text{OBS}})$*-distance-fraud adversary* $\mathcal{A}$ *against* $\mathcal{ID}$ *there exist: a* (t', q')*-distinguisher* $\mathcal{A}'$ *against* G *and a* (t'', q'')*-distinguisher* $\mathcal{A}''$ *against* F *(with* $t' = t + O(n)$, $t'' = t + O(n)$ *and* $q' = q'' = q_{\mathcal{R}} + q_{\mathcal{T}} + q_{\text{OBS}}$*) such that, for* $N_t = T_{\max} + E_{\max}$*,*

$$\boldsymbol{Adv}^{dist}_{\mathcal{ID}}(\mathcal{A}) \leq q_{\mathcal{R}} \cdot \binom{N_c}{N_t} \left(\frac{7}{8}\right)^{N_c - N_t} + \boldsymbol{Adv}^{dist}_{G}(\mathcal{A}') + \binom{q_{\mathcal{R}} + q_{\text{OBS}}}{2} \cdot 2^{-|N_{\mathcal{R}}|} + \boldsymbol{Adv}^{\mathsf{PR}}_{F}(\mathcal{A}'').$$

– *For any* $(t, q_{\mathcal{R}}, q_{\mathcal{T}}, q_{\text{OBS}})$*-Mafia-fraud adversary* $\mathcal{A}$ *against* $\mathcal{ID}$ *there exist: a* (t', q')*-distinguisher* $\mathcal{A}'$ *against* G *and a* (t'', q'')*-distinguisher* $\mathcal{A}''$ *against* F *(with* $t' = t + O(n)$, $t'' = t + O(n)$ *and* $q' = q'' = q_{\mathcal{R}} + q_{\mathcal{T}} + q_{\text{OBS}}$*) such that, for* $N_t = T_{\max} + 2E_{\max}$

$$\boldsymbol{Adv}^{mafia}_{\mathcal{ID}}(\mathcal{A}) \leq (q_{\text{OBS}} q_{\mathcal{T}})[\tfrac{5}{8} \cdot q_{\mathcal{R}} \binom{N_c}{N_t} \cdot (N_c - N_t + 2) \cdot 2^{-(N_c - N_t)} + \binom{q_{\mathcal{T}}}{2} \cdot 2^{-|N_{\mathcal{T}}|}] + \binom{q_{\mathcal{R}} + q_{\text{OBS}}}{2} \cdot 2^{-|N_{\mathcal{R}}|} + \boldsymbol{Adv}^{dist}_{G}(\mathcal{A}') + \boldsymbol{Adv}^{\mathsf{PR}}_{F}(\mathcal{A}'').$$

– *For every* $(t, q_{\mathcal{R}}, q_{\mathcal{T}}, q_{\text{OBS}}, \epsilon)$*-adversary* $\mathcal{A}^*$ *against the availability of* $\mathcal{ID}^*$ *there exist: an adversary* $\mathcal{A}^{\mathsf{PRF}}$ *against the pseudo-randomness of* G*; an adversary* $\mathcal{A}^{imp}$ *against the impersonation fraud of* $\mathcal{ID}$*; and an adversary* $\mathcal{A}^{mafia}$ *against the mafia-fraud resistance of* $\mathcal{ID}$ *such that:*

$$\boldsymbol{Adv}^{\mathsf{PR}}_{G}(\mathcal{A}^{\mathsf{PRF}}) \cdot \boldsymbol{Adv}^{imp}_{\mathcal{ID}}(\mathcal{A}^{imp}) \cdot \boldsymbol{Adv}^{mafia}_{\mathcal{ID}}(\mathcal{A}^{mafia}) \geq \epsilon.$$

– *Privacy It is narrow-destructive private in the sense of Vaudenay [32].*

Proof. We use the results in Theorem 1 to prove these security properties. The statements regarding mafia, distance, and impersonation resistance, as well as availability, result from the proof of Theorem 1 and from the security properties outlined for the original scheme in [13]. In order to prove narrow-destructive privacy for the compiled protocol, we need to prove that the underlying protocol is narrow-weak private in the sense of Vaudenay. This follows because we can build a blinder that simply forwards the adversary random values of appropriate length for every SendReader or SendTag query. Note that this gives the adversary no significant advantage, since the values exchanged between the reader and the tag are either pseudorandom or the outputs of a pseudorandom function. □