# Improved Security Notions and Protocols for Non-transferable Identification

Carlo Blundo[1], Giuseppe Persiano[1], Ahmad-Reza Sadeghi[2], and Ivan Visconti[1]

[1] Dipartimento di Informatica ed Applicazioni, Università di Salerno, Italy
[2] Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany

**Abstract.** Different security notions and settings for identification protocols have been proposed so far, considering different adversary models where the main objective is the non-transferability of the proof.

In this paper we consider one of the strongest non-transferability notions, namely resettable non-transferable identification introduced by Bellare et al. This notion aim at capturing security with respect to powerful adversaries that have physical access to the device that proves its identity, and thus can potentially reset its internal state. We discuss some limitations of existing notions for secure identification protocols as well as different impossibility results for strong notions of non-transferability. We introduce a new strong and achievable notion for resettable non-transferable identification that reflects real scenarios more adequately and present a generic protocol that satisfies this notion. We then show how to efficiently instantiate our construction and discuss how our protocol can improve the current proposals for the next generation of electronic passports (e-passports).

**Keywords:** Non-transferability, reset attacks, e-passports.

## 1 Introduction

Identification protocols are mechanisms that enable one party $V$, called the *verifier*, to gain assurance that the claimed identity of another party $P$, called the *prover*, is legitimate. $P$ holds a secret key corresponding to a public key known by $V$, and $P$ proves that she is the owner of the secret key. The main security requirement is to prevent an adversary $A$ from impersonating the prover $P$, and making the verifier $V$ believe it is interacting with $P$. Traditionally, this is achieved by means of a zero-knowledge proof of knowledge [1,2], i.e., $P$ proves knowledge of the secret key in zero-knowledge. This guarantees that the prover is legitimate and that the verifier gains no information about the secret key.

A stronger security notion for identification protocols is that of *non-transferability*; that is, an adversarial verifier $A$ shall not be able to exploit the fact that she successfully runs the identification protocol with $P$ to convince a honest verifier $V$ that he is indeed $P$. In the rest of the paper we will also say that $A$ is a *man-in-the-middle* (MiM, for short).

In this paper, we consider very powerful MiM adversaries. Specifically, we allow the adversary to run several instances of the identification protocol with

S. Jajodia, and J. Lopez (Eds.): ESORICS 2008, LNCS 5283, pp. 364–378, 2008.

the prover; and we do not restrict the adversary to run the same protocol with $P$ and $V$. In some contexts, an important security property is the protection against *reset attacks* that deals with adversaries capable of resetting the internal state of the prover thus forcing the prover to use the same randomness for more than one run of the protocol. Security against reset attacks is of special interest for applications that use identification protocols and have sophisticated security and privacy requirements like the *electronic passport* also called *e-passport* [3,4,5]. We consider e-passports as our running example throughout this paper.

*Related work.* Non-transferability of proofs has been considered in the literature in the designated verifier/confirmer framework [6,7]. In this framework, a proof is linked to a verifier, and hence cannot be transferred. The issue here is that these approaches are based on public-key infrastructures (PKI) linking public keys to verifiers. Unfortunately, this is not practical (or even impossible) in large scale applications. Specifically, in the case of our running example (i.e., e-passports) it would be very difficult to manage the revocation lists of the readers' (verifiers) side (see also a similar discussion in [8]).

Security issues against adversaries with reset capabilities were considered by Goldreich et al. [9]. They introduced the concept of *resettable security* for zero-knowledge proofs. This notion has been investigated further in other papers (e.g., [10,11]) which mainly focus on having feasibility results and efficient constructions for zero-knowledge proofs requiring public-key for the verifiers.

Monnerat et al. [8] recently proposed identification protocols that consists in non-transferable signatures of knowledge. An important feature of their protocol is that they do not require PKI on the verifier's side. The proposed solutions are based on identification protocols that are zero-knowledge, and security is guaranteed under the assumption that the MiM does not work on-line. The protocol of [8] can be made secure against reset attacks by using resettable zero-knowledge. However, the known resettable zero-knowledge protocols that can work in their setting (i.e., without setup assumptions) are inefficient and cannot guarantee the proof of knowledge property (in the black-box sense).

To our knowledge, formal security notions capturing reset attacks for identification protocols have been first given by Bellare et al. [10]. They distinguish between two notions termed as `CR1` and `CR2` where `CR` stands for *concurrent-reset*. The `CR1` notion allows MiM to interact with prover instances (concurrently) having the goal to impersonate the prover at a later time (off-line attack). The `CR2` notion is stronger and allows the adversary to interact with prover instances and simultaneously attempt to impersonate the prover (on-line attack).

Basically, `CR2` security is impossible to achieve since the adversary can simply relay (copy) all messages between the prover and the verifier. In [10] the authors discuss this issue and argue that such attacks do not harm, since in fact the verifier was talking to the actual prover. Hence they do not consider these attacks as successful attacks in their security definition (which is based on *matching session ids*). However, this restriction is not necessary: First, it does not adequately reflect real scenarios in practice where the MiM could then get the benefit of an access obtained through the prover. Secondly it can be removed

by other means in practice, e.g., through techniques such as *distance bounding* protocols [12,13,14,15] allowing the prover to ensure that the MiM cannot play other protocols at the same time, i.e., the protocol is performed with the prover in one shot and in isolation. Moreover, as we show in Section 2, even when using techniques like distance bounding, the CR1 notion of [10] would not suffice to capture attacks where the MiM succeeds in transferring the proof by suspending and resuming the verifier before and after resettably interacting with the prover.

*Our contribution.* In this paper, we propose a strong notion of security for identification protocols, termed CR+, which we believe to adequately model the non-transferability properties of identification protocols under reset attacks. Comparing CR+ with the notions of security CR1 and CR2 of Bellare et al. [10], we stress that CR+ allows the adversary to play different protocols with the prover and with the honest verifier. In addition, we allow the adversary to start and suspend the interaction with the verifier, start a resetting attack on the prover, and finally, resume the interaction with the verifier. The notion CR1 of [10] instead only considers adversaries that interact with the verifier after they have interacted with the prover.

We then propose a general identification protocol and prove that it is CR+ secure. Specifically, our general protocol is an argument of knowledge[1] and guarantees CR+ security with respect to any other identification protocol that is an argument of knowledge. In addition, our protocol makes minimal set-up assumption and it does not require PKI on the verifier side. We also give an *efficient* instantiation of our protocol based on the hardness of discrete logarithms.

Moreover, we apply our results to the current proposal for enhanced e-passports *Extended Access Control* (EAC) [16,5]. We point out the conceptual weaknesses of the chip authentication within EAC with respect to the requirements mentioned above and to our framework CR+. More concretely, we describe a simple attack on the Chip Authentication protocol which shows that the protocol is not CR+ secure, and propose our efficient instantiation as a possible substitute for the Chip Authentication protocol.

## 2 Identification Protocols Secure Against Reset Attacks

*Requirement analysis.* Given the previous discussion, we focus on the following requirements.

1. **Non-transferability.** An adversarial verifier should not be able to exploit in any useful way the fact that a prover successfully proved his identity to her. Since the strong on-line attack is unavoidable when the adversary controls the communication channel, one has to make some physical/setup assumptions or deploy techniques such as distance bounding [12,13,14,15]

[1] An argument of knowledge is a proof of knowledge that is secure against polynomial-time adversarial provers. This is a widely used security notion for identification schemes since here the prover has to prove knowledge of a secret information that corresponds to its identity.

that help to decrease the viability of these attacks, and reduce it to an off-line attack. A non-transferable protocol should be resilient to such MiM attacks.

2. **Resettability.** Standard security notions do not work anymore when the adversary has access to the device that is running the honest party protocol, in particular when the adversary can manipulate it – e.g., reset the internal state of the prover (see, e.g., [9,10]). These attacks are actually possible when the adversary has physical control of the device. This happens for instance when an e-passport is given to someone else for performing an identity control.[2] Concretely, e-passports are often physically given to someone who performs identity checks. Moreover, the random number generation of some RFID chips have already been successfully attacked due to their weak implementations. Therefore an identification protocol must resilient even to an adversary who can reset the proving device to a previous state.
3. **Practical setup assumptions.** In many large scale applications, one desires practical setup assumptions and key management to avoid strong overhead. Solutions such as the framework of designated verifier proofs require the existence and the deployment of a public-key infrastructure (PKI) for managing the keys of the verifiers. For e-passport for instance, having a PKI on the verifier (reader) side is often an additional and strong overhead, since it is not practical to manage revocation lists and other updates. Note that the current proposal for e-passport [16,5] heavily uses PKI, also on the verifier side. A design goal for identification protocols is therefore the use of practical setup assumptions and thus no PKI should be used on the verifier side.
4. **Efficiency.** Many of the settings where such identification protocols are employed, consider low-powered devices (smart cards, RFID chips) and thus there are important efficiency requirements concerning the round, communication, and computational complexities of the proposed protocols. Beyond general feasibility results, another goal is the design of protocols that are both secure and efficient.

*Security notion.* We follow (and slightly adapt to our setting) the notation used by Bellare et al. [10]. We assume that the number $m(k)$ of moves for an instance of the protocol with security parameter $k$ is odd so that the prover is the first and the last to move. We denote by $\mathsf{pk}$ the public key of the prover and by $\mathsf{sk}$ the associated secret key. Each party computes the next message as a function of its keys, random tape and conversation prefix. More specifically, for identification protocol $\mathcal{ID}()$, message $\mathsf{msg}_{2j+1}$, for $j$ integer and $1 \leq 2j+1 \leq m(k)$, is computed by the prover as $\mathsf{msg}_{2j+1} \leftarrow \mathcal{ID}(\mathsf{prvmsg}, \mathsf{crs}, \mathsf{sk}, \mathsf{msg}_1, \cdots, \mathsf{msg}_{2j}; R_P)$ where $\mathsf{crs}$ is the public parameter, $R_P$ is the random tape of the prover and $\mathsf{msg}_1, \cdots, \mathsf{msg}_{2j}$ is the current conversation prefix. On the other hand, message

[2] This certainly depends on the assumptions one makes with regard to the underlying device. If one assumes a tamper proof true random number generator (based on hardware) then the adversary cannot enforce the same physical environment and consequently the same randomness.

$\mathsf{msg}_{2j}$, for $j$ integer and $2 \leq 2j \leq m(k) - 1$, is computed by the verifier as $\mathsf{msg}_{2j} \leftarrow \mathcal{ID}(\mathsf{vrfmsg}, \mathsf{crs}, \mathsf{pk}, \mathsf{msg}_1, \cdots, \mathsf{msg}_{2j-1}; R_V)$ where $\mathsf{crs}$ is the public parameter, $R_V$ is the random tape of the verifier and $\mathsf{msg}_1, \cdots, \mathsf{msg}_{2j-1}$ is the current conversation prefix. The following keywords are used in the notation of the identification protocols: $\mathsf{prvmsg}$ used to denote message from $P$ to $V$, and $\mathsf{vrfmsg}$ for message from $V$ to $P$; $\mathsf{crsgen}$ is used to generate public parameters on input the security parameter $1^k$; $\mathsf{keygen}$ is used to generate the pair of public and secret key of the prover on input of the security parameter $1^k$ and the public parameters $\mathsf{crs}$, and $\mathsf{vrfdec}$ is used by the verifier to decide whether to accept or not on input of the public parameter $\mathsf{crs}$, the public key $\mathsf{pk}$ and the entire conversation.

We require an identification to be complete in the sense that if prover and verifier follow the protocol then the verifier accepts except with some negligible probability.

CR+ *security.* To define the security of an identification protocol we strengthen the notion of CR1 introduced by [10]. Our new notion captures security in the following scenario. We have an adversary $\mathcal{A}$ that interacts with multiple instances of an honest prover that are all running on input $\mathsf{pk}$ and using the same public information $\mathsf{crs}$. $\mathcal{A}$ is allowed to reset any of the instances to any state and we do not want $\mathcal{A}$ to gain enough information from this interaction to successfully complete an identification protocol with an honest verifier on input $\mathsf{pk}$. In the CR1 notion of [10] the two phases did not overlap in time (with the interaction with the honest provers to be completed before the interaction with the honest verifiers will start) and the adversary $\mathcal{A}$ was playing the same protocol with honest provers and honest verifier[3].

We get a stronger security notion by considering more powerful adversaries. Specifically, we allow the adversary to start the interaction with the verifier; the adversary can suspend the interaction with the verifier and start a resetting attack with the provers; finally, the adversary can resume the interaction with the verifier. We stress that, similarly to the CR1 notion of [10], we do not allow the adversary to interact with the provers and the verifier at the same time. Indeed, if this kind of attacks were allowed, then the adversary could simply relay messages between the honest prover and the honest verifier and no protocol can be secure against this attack. In [10] these stronger attacks where considered in the notion CR2, however, their CR2 secure protocols work assuming that each interaction uses a different session ID. We do not follow this approach since in practice nothing prevents the adversary from using the same ID in all protocols as it does in the simple relay attack where the adversary copies all messages: For instance in the CR2-secure construction in [10] the identity is a public-key $\mathsf{pk}$ of a CCA2 encryption scheme. The verifier sends a CCA2 encryption of a challenge $c$ and the prover answers by sending back the plaintext $m$. Obviously the MiM

[3] Obviously $\mathcal{A}$ could play with many verifiers but this would not add extra power since any succeeding adversary $\mathcal{A}$ that plays with many verifiers can be reduced to a succeeding adversary $\mathcal{A}'$ that plays with just one verifier, by simply emulating internally all other verifiers required by $\mathcal{A}$.

can obtain $c$ from the verifier, send $c$ to the prover thus obtaining $m$, and finally can give $m$ back to the verifier.

Therefore, given that the adversary has an easy strategy to win, we simply observe that there is no possible defense against on-line MiM attacks when they are mounted, and thus it is anyway necessary to resort to physical means to make sure that the adversary will not play protocols with other verifiers when it is also playing with a prover. In this context one may use some additional techniques such as distance bounding [12,13,14,15] where one can guarantee that the protocol played by the prover with the MiM will be executed in one shot, and it is isolated from the surrounding environment. Once we have this guarantee, we can focus on weaker and *achievable* security definitions.

Moreover, there is another important improvement to CR1 that we consider in the definition of CR+. Indeed, we also allow the adversary $\mathcal{A}$ to play different identification protocols with the provers and with the verifiers. This covers the case in which one can design an identification protocol that can be successfully executed by an adversary (even without knowing the secret key) if an adversary has access to the prover of a different identification protocol. The notion of [10] instead considered an adversary successful only if it manages to use the same identification protocol against itself and thus would guarantee security only if the same public key was used in only one type of identification protocol.

Therefore, having specified that the relay of messages is a successful attack and having extended the notions of CR1 and CR2 by assuming that the protocol played by the adversary with the prover can be different from the one played with the verifier, we have that when left and right protocols are the same, then CR2 $\Rightarrow$ CR+ $\Rightarrow$ CR1, moreover CR1 $\not\Rightarrow$ CR+ $\not\Rightarrow$ CR2, and CR2 is impossible to achieve. Our goal is to achieve CR+ security, and this will correspond to CR2 with the restriction that the adversary can have access only once to the prover and can access it with resetting capabilities, while it is isolated from other verifiers.

*Formal definition.* We consider probabilistic polynomial-time adversaries $\mathcal{A}$ that are a three-phase adversaries. In the first phase, $\mathcal{A}$ can issue a SendVer query which takes a message msg that is sent to an instance of a honest verifier of identification protocol $\mathcal{IDR}$ and the reply to the query is the next verifier message. In the second phase the adversary $\mathcal{A}$ mounts a resetting attack on protocol $\mathcal{ID}$ in which $\mathcal{A}$ can start any number of instances of the prover of $\mathcal{ID}$ on input public key pk. In the third phase, $\mathcal{A}$ can resume the instance of protocol $\mathcal{IDR}$ started in the first phase. We say that $\mathcal{A}$ is successful if the instance of protocol $\mathcal{IDR}$ is completed successfully. We stress that throughout the attack $\mathcal{A}$ is allowed to start exactly one instance[4] of protocol $\mathcal{IDR}$ in which $\mathcal{A}$ acts as a prover on input pk. In particular, the verifier of $\mathcal{IDR}$ cannot be reset.

**Definition 1.** *Let $\mathcal{ID}$ and $\mathcal{IDR}$ be two identification protocol. We say that $\mathcal{ID}$ is* CR+ secure with respect to $\mathcal{IDR}$ *if for all probabilistic polynomial-time adversaries $\mathcal{A}$ the probability that experiment* $\mathsf{IDCR+}^{\mathcal{A}}_{\mathcal{ID},\mathcal{IDR}}(k)$ *of Figure 1 returns* 1 *is negligible in $k$.*

[4] As we previously discussed, there is no extra power starting more such instances.

$\mathsf{IDCR}+^{\mathcal{A}}_{\mathcal{ID},\mathcal{IDR}}(k)$: **Trusted Parameter Initialization:**

1. $\mathsf{crs} \leftarrow \mathcal{ID}(\mathsf{crsgen}, 1^k)$; ‖Generate trusted parameters.‖

**Users Initialization:**

1. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{ID}(\mathsf{keygen}, \mathsf{crs}, 1^k)$; ‖Pick keys via randomized key generation algorithm. ‖
2. Choose tape $R_V$ for verifier at random; $C_V \leftarrow 0$; ‖Coins and message counter for verifier.‖
3. $\mathsf{trans} = \emptyset$;

**Execute adversary** $\mathcal{A}$ on input $\mathsf{pk}, \mathsf{crs}$;

- **Phase I:**
  Reply to $\mathcal{A}$'s $\mathsf{SendVer}(\mathsf{msg})$ queries as follows:
  1. $C_V = C_V + 2$, $\mathsf{trans} = \mathsf{trans} \circ \mathsf{msg}$;
  2. if $C_V \leq m(k) - 1$ then $\mathsf{msg}_{C_V} \leftarrow \mathcal{IDR}(\mathsf{vrfmsg}, \mathsf{crs}, \mathsf{pk}, \mathsf{trans}; R_V)$; $\mathsf{trans} = \mathsf{trans} \circ \mathsf{msg}_{C_V}$; **return**$(\mathsf{msg}_{C_V})$;
  3. if $C_V = m(k) - 1$ then $\mathsf{dec} \leftarrow \mathcal{IDR}(\mathsf{vrfdec}, \mathsf{crs}, \mathsf{pk}, \mathsf{trans}; R_V)$; **return**$(\mathsf{dec})$;
  4. if $C_V > m(k) - 1$ then **return**$(\perp)$;
- **Phase II:**
  $p \leftarrow 0$; ‖ Number of active prover instances. ‖ Reply to $\mathcal{A}$'s $\mathsf{WakeNewProver}$ queries as follows:
  ‖ Activate a new prover instance. ‖
  1. $p \leftarrow p + 1$; Pick a tape $R_p$ at random;
  2. **return**$(p)$;

  Reply to $\mathcal{A}$'s $\mathsf{SendPro}(i, \mathsf{msg}_1, \cdots, \mathsf{msg}_{2j+1})$ queries, with $0 \leq 2j < m(k)$ and $1 \leq i \leq p$, as follows: ‖ Send a message to $i$-th prover instance. ‖
  1. $\mathsf{msg}_{2j+1} \leftarrow \mathcal{ID}(\mathsf{prvmsg}, \mathsf{crs}, \mathsf{sk}, \mathsf{msg}_1, \cdots, \mathsf{msg}_{2j}; R_i)$[a].
  2. **return** $(\mathsf{msg}_{2j+1})$.
- **Phase III:** exactly like Phase I.

**return**$(\mathsf{dec})$.

[a] In a reset attack this message can be sent several times with the same $R_i$.

**Fig. 1.** Experiment for the execution of protocol $\mathcal{ID}$ with security parameter $k$ in the CR+ setting and resetting adversary $\mathcal{A}$ playing protocol $\mathcal{IDR}$ in the right

In Section 3 we give an identification protocol that is an argument of knowledge and is CR+ non-transferable with respect to all identification protocols that are arguments of knowledge.

*Generalizing* CR+ *to multiple accesses.* While it is reasonable to assume that by using some physical assumptions, one can be sure that the protocol executed by the prover is run in one shot, it is not immediately clear while the adversary should not be able to get again access to prover's device in the future, then again

interacting with the verifier and so on. Such extra power makes the attack of the adversary as strong as the CR2 attack, and thus it is impossible to obtain a secure identification protocol. Indeed, observe that the restriction that the adversary plays with the prover in one shot, does not hold anymore as the adversary can then play some messages with the verifier and can later reset the prover. This concretely simulates the CR2 attack and allows the adversary to be a proxy that copies to the verifier all messages played with the prover. This extension of CR+ is therefore impossible to achieve.

An important question is therefore whether the extra power of the adversary in this extension of CR+ is always possible in real scenarios, and thus there would be no reason to study CR+ anymore. However, consider the following example. Since the interaction with $V$ is non-resetting, it does make sense to consider a scenario where the adversary suspends the execution with $V$, plays in one shot with $P$ and then continues again the protocol with $V$. Indeed, since the interruption in practice can be just for a very short time, concrete timeouts of $V$ do not expire. A similar and more concrete example is that of the use of an e-passport at the border control.

## 3 Resettably Non-transferable Identification

*Overview.* In this section we present an efficient identification protocol $\mathcal{ID}$ that considers the security issues previously discussed. We then analyze its security properties. Our starting point for obtaining CR+ security is the approach used by [8] for the off-line setting (i.e., the MiM does not work simultaneously with provers and verifier) with PKI-less verifiers. Indeed, the proposed protocol is a zero-knowledge[5] proof of knowledge and as such it enjoys a satisfying security notion for both prover (i.e., the zero knowledge property) and verifier (i.e., the proof of knowledge property). Moreover the zero-knowledge property preserves the non-transferability of the protocol even in case the adversary will play with the verifier both before and after playing with the prover.

The only weakness of the protocol proposed in [8] concerns the fact that they restrict the adversary to sequential interactions with the prover. This, however, does work in some scenarios where the adversary has physical access to the device and can mount concurrent and reset attacks against the prover. If one tries to strengthen the protocol of [8] to make it secure against concurrent/resetting adversaries, then the efficiency of their transformations is immediately lost (indeed, there is currently no efficient concurrent/resettable zero-knowledge proof system in their setting). Moreover, there is no hope to preserve the proof of knowledge property (at least for the black-box sense) against a resetting adversary.

We therefore play with the set-up assumptions in order to strengthen their solution still keeping it viable in several applications, and in particular for the one that they proposed, i.e., citizens identification through e-passports.

[5] Notice that zero knowledge implies other security properties as witness indistinguishability and witness hiding.

The setup assumption that we consider is the use of trusted parameters that we assume are known when parties run the protocol. Our trusted parameters do not correspond to a verifier public key, therefore we keep the PKI-less feature on the verifier side. For verifier security, by appropriately using the trusted parameters we achieve the argument of knowledge property while at the same time the adversary can mount reset attacks. Notice that the argument of knowledge property along with security against reset attacks is impossible to achieve without some setup assumption (the adversary would be as strong as the extractor), therefore this justifies the use of trusted parameters. For prover security, we show that resettable witness indistinguishability sufficies against transferability attacks (similar approaches were used in [10]). Even though our protocol also achieves resettable zero knowledge in the trusted parameters model, we follow the approach of [10] and consider resettable witness indistinguishability since in general resettable zero knowledge could be a requirement that only increases the complexity of a non-transferable protocol. Concretely, our protocol is a special argument of knowledge that is CR+ non-transferable with respect to any argument of knowledge. Our protocol achieves a general (rather than self) non-transferability property and works in a setting that admits wide applications.

The CR+ security proof of our protocol $\mathcal{ID}$ works as follows.

1. We include in the set of trusted parameters the parameters of a trapdoor commitment scheme[6]; this will let us to prove the argument of knowledge property, indeed the extractor will use a secret associated to the commitment parameters, and this is not known to the resetting adversary.
2. We include in the trusted parameters another public key $\mathsf{pk}$'; this will be used to reach a contradiction (see Section 3.1).
3. We run the experiment of CR+ by using in $\mathcal{ID}$ the secret that corresponds to $\mathsf{pk}$' instead of the one corresponding to $\mathsf{pk}$; by the resettable witness indistinguishability of $\mathcal{ID}$ the adversary will not notice any difference.
4. We assume that the adversary transfers a proof from $\mathcal{ID}$ to $\mathcal{IDR}$.
5. We run the extractor of $\mathcal{IDR}$ obtaining the secret key associated to $\mathsf{pk}$[7] thus breaking $\mathsf{pk}$ (if we instead always obtain $\mathsf{pk}'$ we can run a symmetric game where we break $\mathsf{pk}'$).

In order to design the resettable witness indistinguishable argument of knowledge $\mathcal{ID}$, we will try to be as much general as possible, therefore we will present a general protocol based on the popular $\Sigma$-protocols. These protocols exist for many useful languages and often admit efficient instantiations. We will then suggest an instantiation based on Schnorr's protocol [18] and argue its applicability to the e-passport framework.

*Generic protocol.* Let $1^k$ be the security parameter. The crsgen procedure outputs as public parameters a randomly chosen hard instance $\mathsf{pk}'$ of a language $L'$

[6] Such commitment schemes when defined in the trusted parameters model allow a party to open a commitment as any valid messages, in case it knows the trapdoor associated to the trusted parameters. See [17] for formal definitions.

[7] This step requires that $\mathcal{IDR}$ is an argument of knowledge.

admitting a $\Sigma$-protocol $\Pi_{\Sigma'}$ and the public parameters $tc$ of a trapdoor commitment scheme.

The keygen procedure outputs as public key pk of $P$ a randomly chosen hard instance for a language $L$ admitting a $\Sigma$ protocol $\Pi_{\Sigma}$, along with the corresponding NP witness sk as secret key.

The protocol can be described as follows. We consider the OR-composition of the two $\Sigma$-protocols obtained using the techniques of [19] and that produces another $\Sigma$-protocol $\Pi_{\Sigma_\vee}$, which 3 rounds are denoted $(a, c, z)$. Protocol $\mathcal{ID}$ that we propose starts by requiring that $V$ uses $tc$ to send a commitment $\hat{c}$ of the challenge $c$ of $\Pi_{\Sigma_\vee}$. Then $P$ uses a pseudorandom function to obtain the randomness to use in the next steps. $P$ computes and sends the first message $a$ of $\Pi_{\Sigma_\vee}$. Then $V$ opens to $c$ the commitment $\hat{c}$. Then $P$ sends the last message $z$ of $\Pi_{\Sigma_\vee}$. Finally $V$ runs the decision procedure of $\Pi_{\Sigma_\vee}$ thus accepting or rejecting the proof. The protocol is illustrated in Figure 2.

**Security parameter:** $k$.
**Tools:** pseudorandom function $f$, trapdoor commitment scheme $(\mathtt{Gen}, \mathtt{Com}, \mathtt{TCom}, \mathtt{TDec}, \mathtt{Ver})$.
**Common input:** the public information $(\mathsf{pk}', tc)$ and the public key of the prover pk.
$P$**'s private input:** sk that is an NP witness for pk in $L$.
$P$**'s randomness**: randomly pick a seed $s$; the randomness of $P$ will be taken from the output of $f(s, \hat{c})$ where $\hat{c}$ is the first message received from $V$.

$V$: select a message $c$ for $\Pi_{\Sigma_\vee}$, compute and send $\hat{c} = \mathtt{Com}(c)$.
$P$: generate and send the first message $a$ for $\Pi_{\Sigma_\vee}$.
$V$: open $\hat{c}$ to $c$.
$P$: check that the opening of $\hat{c}$ to $c$ is correct and then compute and send the last message $z$ of $\Pi_{\Sigma_\vee}$.
$V$: accept iff $(a, c, z)$ is an accepting transcript for $\Pi_{\Sigma_\vee}$.

**Fig. 2.** $\mathcal{ID}$: CR+ Non-Transferable Identification

### 3.1 Analysis

We now show that the protocol depicted in Fig. 2 is CR+ secure. Completeness can be obtained by inspection since if $P$ follows the protocol, then $V$ trivially always accepts. For proving CR+ non-transferability we first show that the protocol is a resettable witness-indistinguishable (rWI) argument of knowledge. Then we will show that any adversary for the CR+ non-transferability property can be used to reach a contradiction.

*$\mathcal{ID}$ is a rWI argument of knowledge.* Completeness is straight-forward since by inspection we can observe that the honest verifier accepts the proof given by the honest prover on input the secret key.

The argument of knowledge property can be proved by showing an extractor $E$ that outputs a valid secret key with probability $p'$ such that $|p' - p| \leq \epsilon(k)$ for a negligible function $\epsilon$, whenever an adversarial prover $P^\star$ can succeed in convincing a honest verifier with probability $p$. $E$ runs on input the trapdoor that corresponds to the parameters $tc$ of the trapdoor commitment scheme.

$E$ runs the honest verifier algorithm with the following exception: it computes the commitment $c$ in the first round using the trapdoor. Notice that this experiment is indistinguishable from the real game played by $P^\star$ and the honest verifier $V$ since the trapdoor property of the trapdoor commitment scheme guarantees that commitments computed using the trapdoor are indistinguishable from commitments computed using the honest commitment function. Therefore, if $P^\star$ succeeds with honest $V$ with probability $p = p_0$, it will succeed with $E$ with probability $p_1$ where $|p_1 - p_0|$ is negligible in $k$. The extractor $E$ then goes back to the opening phase and instead of opening $\hat{c}$ to $c$, it opens $\hat{c}$ to a randomly chosen message $c'$. Here we have that the probability that $c = c'$ is negligible in $k$. Moreover, we have again that the trapdoorness of the trapdoor commitment scheme guarantees that $P^\star$ completes again successfully the proof with probability $p_2$ where $|p_2 - p_1|$ is negligible in $k$. Notice that by the special soundness property of $\Pi_{\Sigma_\vee}$, $E$ extracts from the two accepting transcripts either a valid secret key $\mathsf{sk}$ corresponding to $\mathsf{pk}$ or the witness $w$ for the hard instance $\mathsf{pk}' \in L'$. From the above discussion, the probability that $E$ extracts one of those two witnesses is $p_2 \leq p + \epsilon(k)$ for some negligible function $\epsilon$. Finally we have that if the extracted witness is with overwhelming probability $\mathsf{sk}$, then the extraction procedure is successful with probability $p'$. Instead, if with non-negligible probability the witness extracted corresponds to $\mathsf{pk}' \in L'$, we have that the previous game with non-negligible probability breaks the hard instance that is stored in the trusted parameters, thus contradicting the assumption that the instance is hard. This implies that $p' \leq p_2 + \epsilon(k)$ for some negligible function $\epsilon$ and thus it concludes the proof of the argument of knowledge property.

To prove the resettable witness-indistinguishable property we can use the general approach of [9] since our protocol follows the paradigm that they introduced to design rWI proof systems[8]. For the sake of clarifying the features of the protocol, we now give a sketched proof. First of all, notice that by Proposition 1 of [19] we have that $\Pi_{\Sigma_\vee}$ is witness indistinguishable. By adding a commitment of the challenge to the first round, we have only an additional constraint for the adversarial verifier and thus witness indistinguishability is trivially preserved. Moreover, it is known by [20,21] that witness indistinguishability is preserved under concurrent composition. In order to claim rWI, we have therefore only to consider the resets performed by $V^\star$. However, notice that the randomness used by the prover is the output of the pseudorandom function on input the first message of the verifier. Therefore, any reset of $V^\star$ where it feeds to $P$ a different commitment under a previously used randomness, will correspond to a

[8] The verifier first commits and then the only message it sends are openings of the committed messages. The prover uses as randomness the output of a pseudorandom function on input the commitment of the verifier and a random seed.

new incarnation of $P$ that will use new pseudorandom bits as randomness. The capability of $V^\star$ in succeeding in a reset attacks can therefore be converted to a distinguisher that distinguishes the use of random bits from the use of pseudorandom bits and therefore would break the pseudorandomness of the pseudorandom function. There is one more subtle point to consider: since the randomness of $P$ is fixed after the commitment of the first round, we have that in case $V$ manages to open the committed message in two different ways, it would run $P$ twice with the same pseudorandom bits but under different transcripts. This clearly would violate the preservation of the witness indistinguishability property. However, such a capability of $V$ with non-negligible probability $p$ would immediately correspond to an adversary that with non-negligible probability $p$ breaks the binding property of the trapdoor commitment scheme instantiated in the trusted parameters.

CR+ *non-transferability.* Assume there is a MiM $\mathcal{A}$ that succeeds in transferring a proof during a CR+ attack with non-negligible probability $p_0$. We show how to use $\mathcal{A}$ for reaching a contradiction. First of all, we run $\mathcal{A}$ with fake but perfectly indistinguishable parameters $(\mathsf{pk}', tc)$ and public key $\mathsf{pk}$. Protocol $\mathcal{IDR}$ is played by running the honest verifier algorithm. Protocol $\mathcal{ID}$ instead is played by running the honest prover algorithm of $\Pi_\Sigma$ but using as witness the one corresponding to $\Pi_{\Sigma'}$ protocol (which instance $\mathsf{pk}'$ is in the trusted parameters). Notice that $\mathcal{A}$ will still succeed in $\mathcal{IDR}$ with probability $p_1$ such that $|p_1 - p_0|$ is negligible in $k$, otherwise it would immediately contradict the rWI property of $\mathcal{ID}$ that we have proved above.

We can then replace the verifier of $\mathcal{IDR}$ by the corresponding extractor. Its execution still guarantees that $\mathcal{A}$ succeeds in $\mathcal{IDR}$ with probability $p_2$ such that $|p_2 - p_1|$ is negligible. The execution of the extraction procedure will potentially require multiple rewinds and consequently multiple executions of $\mathcal{ID}$. Finally, in case the extractor $\mathcal{IDR}$ will give as output one $\mathsf{sk}$. we have that $\mathcal{A}$ can be used to break an hard instance of $L$. Instead, in case we have that the extraction procedure fails, notice that the only difference between the real game where $\mathcal{A}$ succeeds and this game, consists in the different witness used by the prover of $\mathcal{ID}$. Therefore, either the extraction procedure on $\mathcal{IDR}$ succeeds and we break an hard instance of $L$, or it fails and in this case we have a distinguisher for the resettable witness indistinguishable property of $\mathcal{ID}$. However, since we have already proved the resettable witness indistinguishable property of $\mathcal{ID}$, we have reached a contradiction. This ends the proof.

## 4 Efficient Instantiation and Application to E-Passports

The CR+-secure identification protocol $\mathcal{ID}$ that we have shown can be instantiated very efficiently in the following way. The trapdoor commitment scheme can be Pedersen's commitment scheme, which requires a $k$-bit prime $q$, a prime $p = 2q + 1$ and two generators $g, h$ of the subgroup $G$ of $Z_p^\star$ of $q$ elements for the trusted parameters. The trapdoor will be the discrete logarithm $\alpha$ of $h$ with base $g$ mod $p$. For language $L'$ and an hard instance $\mathsf{pk}'$ we can simply consider

**Security Parameter:** $k$.
**Tools:** pseudorandom function $f$.
**Common input:** The public information $(p, q, g, h, \mathsf{pk}')$.
$P$**'s identity:** $\mathsf{pk} \in G_q$.
$P$**'s private input:** $\mathsf{sk}$ such that $g^{\mathsf{sk}} = \mathsf{pk} \pmod p$.
$P$**'s randomness**: randomly pick a seed $s$; the randomness of $P$ will be taken from the output of $f(s, \hat{C})$ where $\hat{C}$ is the first message received from $V$.

$V$: Randomly pick $C \in Z_q$ and commit to $c$ by computing $\hat{C} = g^C h^r$ for a random $r \in Z_q$. Send $\hat{C}$ to $P$.
$P$: Randomly pick $s_0, C_1, Z_1 \in Z_q$, and set $A_0 = g^{s_0}$ and $A_1 = g^{Z_1}\mathsf{pk}^{-C_1} \pmod q$. Send $A_0$ and $A_1$ to $V$.
$V$: Upon receiving $(A_0, A_1)$, open commitment $\hat{C}$ by sending $(C, r)$.
$P$: Check that the opening is correct and then compute $Z_0$ as follows: $C_0 = C - C_1 \pmod q$, $Z_0 = s_0 + C_0\mathsf{sk} \pmod q$. Send $(Z_0, C_0, Z_1, C_1)$.
$V$: Accept if $C_0 + C_1 = C \pmod q$ and if $g^{Z_0} = A_0\mathsf{pk}^{C_0} \pmod p$ and $g^{Z_1} = A_1\mathsf{pk}'^{C_1} \pmod p$.

**Fig. 3.** Efficient CR+ Non-Transferable Identification Protocol $\mathcal{ID}_{DLOG}$

$G$ and a random element $\mathsf{pk} \in G$. A randomly chosen pair of public and secret keys can be respectively a pair $(\mathsf{pk}, \mathsf{sk})$ where $g^{\mathsf{sk}} = \mathsf{pk} \pmod p$. $\Pi_{\Sigma'}$ and $\Pi_{\Sigma}$ will coincide with Schnorr's $\Sigma$ protocol. The protocol is illustrated in Figure 3.

We consider such a protocol as a possible substitute for the Chip Authentication protocol of EAC [16,5] to be used in the next generation of e-passports. The next generation of e-passports will make use of public-key cryptography for identification and cloning prevention and it is assumed that the owner will hand over his passport to the border control guard that thus has physical control of the device for a time interval. Therefore, the e-passport could in general be subject to reset attacks where the malicious inspection system will try to gain as much information as it can in order to impersonate that identity later. Moreover, it is also possible that the inspection system initiated an identification protocol with a verifier before starting his slot in the border control system and will try to continue it as soon as he will finish his slot. The CR+ notion of non-transferability perfectly fits the setting of the e-passports.

Note that the current proposal for chip authentication protocol in Extended Access Control [5] of e-passport is not CR+ secure (and thus transferable). Consider our attack from Section 2 on resettable identification scheme with CCA2 encryption from [10]. Then we obtain an attack on the Chip Authentication Protocol by simply replacing the identity of the prover with a Diffie-Hellman contribution $A$ (representing the static public key in the chip authentication protocol of EAC). The message of the verifier will be a randomized Diffie-Hellman contribution $B$ and the identification of the prover is concluded by means of the passive authentication step $C$ that consists in a message sent by the prover according to the Diffie-Hellman exchanged key $K$. Therefore, by replacing $\mathsf{pk}$

with $A$, $c$ with $B$ and $m$ with $C$, we can mount precisely the same attack. Notice further that in our attack we did not have to resort to any reset. This implies that the EAC chip authentication protocol is transferable even if the adversary can not perform resets.

The protocol that we have proposed works in the trusted parameters model. Notice that this is not an extra assumption for the application to e-passports as passports by their own nature assume a trusted authority. Indeed, e-passports are made by governments and readers at the border control already trust the parameters decided by those governments (i.e., they accept as valid the identities certified through digital signatures and digital certificates by those governments). Therefore there is no extra assumption when in the context of e-passport a government also appends to its public information the parameters that we require as trusted parameters.

Another feature of our candidate implementation for e-passports is that there is no public-key requirement on the verifier side. Note that the current proposal for e-passport heavily uses PKI and hence, for e-passports, the management of a PKI is problematic as it should include a key-revocation management that would be difficult to implement.

## 5 Conclusion

In this paper, we have proposed a new security notion for identification protocols, termed `CR+`, which we believe to adequately model the achievable non-transferability properties of identification protocols under reset attacks.

We then have proposed as identification protocol an argument of knowledge in the trusted parameters model that is `CR+` secure with respect to any other argument of knowledge. In addition, our protocol makes minimal set-up assumption, does not require PKI on the verifier side and can be efficiently instantiated with all languages admitting $\Sigma$-protocols.

We have also applied our results to the current proposal for enhanced e-passports pointing out the conceptual transferability weaknesses of the chip authentication protocol. Finally we have proposes an efficient instantiation of out general result as a possible substitute for the Chip Authentication protocol.

*Acknowledgments.* The work of the authors has been supported in part by the European Commission through the FP7 Information Communication Technologies programme, under Contract FET-215270 FRONTS (Foundations of Adaptive Networked Societies of Tiny Artefacts) and in part by the European Commission through the IST program under Contract IST-2002-507932 ECRYPT.

## References

1. Goldwasser, S., Micali, S., Rackoff, C.: The Knowledge Complexity of Interactive Proof-Systems. SIAM J. on Computing 18, 186–208 (1989)
2. Bellare, M., Goldreich, O.: On Defining Proofs of Knowledge. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 390–420. Springer, Heidelberg (1993)

3. Organization, I.C.A.: Machine Readable Travel Documents, Doc 9303, Part 1 Machine Readable Passports (Fifth Edition) (2003)
4. MRTD/NTWG, I.T.: Biometrics Deployment of Machine Readable Travel Documents, Technical Report (2004), http://www.icao.int/mrtd
5. BSI: (Advanced security mechanisms for machine readable travel documents – extended access control), http://www.bsi.bund.de/fachthem/epass/EACTR03110_v110.pdf
6. Chaum, D.: Designated confirmer signatures. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 86–91. Springer, Heidelberg (1995)
7. Jakobsson, M., Sako, K., Impagliazzo, R.: Designated verifier proofs and their applications. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 143–154. Springer, Heidelberg (1996)
8. Monnerat, J., Vaudenay, S., Vuagnoux, M.: About machine-readable travel documents – privacy enhancement using (weakly) non-transferable data authentication. In: International Conference on RFID Security (2007)
9. Canetti, R., Goldreich, O., Goldwasser, S., Micali, S.: Resettable Zero-Knowledge. In: STOC 2000, pp. 235–244. ACM, New York (2000)
10. Bellare, M., Fischlin, M., Goldwasser, S., Micali, S.: Identification protocols secure against reset attacks. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 495–511. Springer, Heidelberg (2001)
11. Di Crescenzo, G., Persiano, G., Visconti, I.: Constant-Round Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 237–253. Springer, Heidelberg (2004)
12. Brands, S., Chaum, D.: Distance-bounding protocols. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994)
13. Bussard, L., Roudier, Y.: Embedding distance bounding protocols within intuitive interactions. In: Proceedings of the First International Conference on Security in Pervasive Computing (SPC 2003), Boppard (2003)
14. Hancke, G.P., Kuhn, M.G.: An rfid distance bounding protocol. In: Proceedings of IEEE/Create-Net SecureComm 2005 (2005)
15. Singele, D., Preneel, B.: Distance bounding in noisy environments. In: Security and Privacy in Ad-hoc and Sensor Networks, pp. 101–115. Springer, Heidelberg (2007)
16. Justice, H.A.: Eu standard specifications for security features and biometrics in passports and travel documents. Technical report, EU (2006)
17. Catalano, D., Visconti, I.: Hybrid Trapdoor Commitments and Their Applications. In: Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 298–310. Springer, Heidelberg (2005)
18. Schnorr, C.P.: Efficient Signature Generation for Smart Cards. Journal of Cryptology 4, 239–252 (1991)
19. Cramer, R., Damgard, I., Schoenmakers, B.: Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 174–187. Springer, Heidelberg (1994)
20. Feige, U., Shamir, A.: Witness indistinguishable and witness hiding protocols. In: STOC 1990, pp. 416–426. ACM, New York (1990)
21. Feige, U., Lapidot, D., Shamir, A.: Multiple Non-Interactive Zero Knowledge Proofs Under General Assumptions. SIAM J. on Computing 29, 1–28 (1999)