# A Message Recognition Protocol Based on Standard Assumptions

Atefeh Mashatan and Serge Vaudenay

The Security and Cryptography Laboratory (LASEC), EPFL
CH-1015 Lausanne, Switzerland
http://lasecwww.epfl.ch/

**Abstract.** We look at the problem of designing Message Recognition Protocols (MRP) and note that all proposals available in the literature have relied on security proofs which hold in the random oracle model or are based on non-standard assumptions.
Incorporating random coins, we propose a new MRP using a pseudorandom function $F$ and prove its security based on new assumptions. Then, we show that these new assumptions are equivalent to the standard notions of preimage resistance, second preimage resistance, and existential unforgeability given that $F$ is a pseudorandom function.

**Key words:** Cryptographic Protocols, Authentication, Recognition, Pseudorandom Functions, Pervasive Networks, Ad Hoc Networks

## 1 Introduction

*Message recognition* is a notion that has recently been developed for small devices in ad hoc networks. In particular, the devices have low computational power, low communication bandwidth and low energy resources. Moreover, they are placed in an environment where no pre-established authentic information exists and without the presence of a trusted third party. Although chips in embedded systems are becoming more and more powerful, researchers have always been looking for lower complexity algorithms in the past 30 years.

In 2003, Weimerskirch and Westhoff [WW03], realized that achieving message authentication is not possible under such restrictive assumptions. The notion of *recognition* was later formalized by Hamell et al. [HWGW05] and motivated by Lucks et al. [LZWW08] with the following example. Alice and Bob are two complete strangers. They meet in a party. Therefore, they have the chance to briefly meet in person, before they depart. A few days later, Bob receives some message from a person who claims to be Alice. Now, obviously Bob would like to recognize the source of the message and make sure the message is sent from the same person who introduced herself as Alice in the party, and not from a malicious person, Eve, who is trying to deceive Bob.

As a real life application, one can think of Alice having a contactless smart badge who wants to buy several movies from a shop owned by Bob. For her first movie, she walks into the shop and pays using her contactless smart badge.

She would like to download the movie to her computer when she goes home. Moreover, she would like to buy and download more movies from home without having to walking to the shop in person. That is, Alice would like Bob to recognize her after the first in person encounter. Many other settings can be considered when Alice and Bob do not have public keys and do not have the required time to generate appropriate keys or agree on domain parameters when they meet for the first time.

More formally, we have two small devices, one sender and one receiver, who share no secret information and are in a setting where they can send authentic, but not confidential, information for a short period of time. Later, the sender wants the receiver to recognize the message it sends. The adversarial goal is to make the receiver accept a message as sent by the sender whereas the sender never sent that message. A message recognition protocol (MRP) is secure if the sender or the receiver detect the active adversary. A passive adversary is not considered harmful in this setting.

There have been many recent MRP proposals in the literature, see for example [GMS09,LZWW08,MS08,Mit03]. However, one can go back to 1998 to trace the first protocol [ABC$^{+}$98] which was designed to fulfill the notion of recognition, although such a term was not used then. Clearly, a digital signature scheme would suffice: Alice gives her public-key to Bob when they first meet and, later, signs her messages. However, in message recognition protocols, one is looking for a cheaper primitive, such as message authentication codes, as opposed to having to compute modular exponentiations. In the case of this paper, the message recognition protocol requires one MAC computation and one pseudorandom function computation. We are unaware of any public-key based solution that could compete with such efficiency.

### 1.1 Literature Review

There has been considerable recent interest in designing security protocols for devices who do not share a secret key which are placed in an environment that does not provide a public-key infrastructure. One proposal is the use of a narrow-band authenticated channel, along with a broadband insecure channel, in order to achieve *message authentication* in such an environment has been investigated in several recent papers, see for example [GN04,MS09,SA99,Vau05]. In such solutions, the narrow-band channel is available all the time and can be used at least once for every message. In this paper however, we are focusing on a more restricted case where the narrow-band channel is only available once at the beginning at the initialization step. To distinguish between the two, the literature refers to the more restricted case as *recognition*, as opposed to *authentication*.

We now briefly go over the already existing message recognition protocols and mention their advantages and disadvantages compared to one another.

‘Guy Fawkes’ protocol, designed by Anderson et al. [ABC$^{+}$98], seems to be the first in line in proposing a protocol achieving recognition, but not authentication. The first variant requires a time-stamping authority and the second variant uses digital signatures for authentication. Hence, the practicality of either variants for restricted devices in restricted environments is under question.

'Remote User Authentication' protocol, proposed by Mitchell [Mit03], uses a message authentication code to authenticate the sender. Hence, does not need a trusted third party. However, it requires computing and sending $2t$ MAC values and sending $r$ secret keys for every message. The suggested parameters are $t \geq 35$ and $r \approx t/2$. Therefore, in terms of computation and communication, it is costly and not suitable for low power and low communication bandwidth devices.

'Zero Common-Knowledge' (ZCK) protocol, by Weimerskirch et al. [WW03], seemed to be the first to admit all the required properties. Implemented by Hammell et al. [HWGW05], the ZCK protocol proved to be practical for devices with restrictive properties such as low computational power, low code space, low communication bandwidth, low energy resources. However, Lucks et al. [LZWW08] found an attack against ZKC which pointed out a flaw in its security proof.

'Jane Doe' protocol, designed by Lucks et al. [LZWW08], uses the idea of using values of a hash chain as keys for MACs to authenticate messages. The Jane Doe protocol exhibits all the preferred properties for small devices placed in a hostile environment. Its security proof is based on the assumption that preimage resistance, second preimage resistance, and their hash chain equivalents, hold for a hash function. Moreover, it makes use of a message authentication code that exhibits existential unforgeability and its hash chain equivalent. The hash chain equivalent properties are non-standard ones. On the other hand, although provably secure, the Jane Doe protocol has a recoverability problem: with one move Eve can bring Alice and Bob out of their synchronized states for the life time of these devices. As a result, they will never be able to communicate again.

Goldberg et al. proposed a self-recoverable MRP [GMS09] to overcome Jane Doe's shortcoming in synchronization. They modified the assumptions of the Jane protocol a little bit, however, they still need to assume the non-standard hash chain assumptions.

Mashatan and Stinson proposed a message recognition protocol [MS08] which does not make use of a hash chain. As a result, they claim that the security assumptions they need become *closer* to the standard notions of preimage resistance and second preimage resistance. However, the assumptions are not exactly standard yet, and it comes with a communication cost of sending about twice as long messages in each flow. Since these protocols are considered in the context of small devices, power consumption is an issue. One should avoid unnecessary communication in order to minimize the power consumption.

Hence, the problem of designing a message recognition protocol based on standard assumptions which exhibits low computational power, low code space, low communication bandwidth, and low energy resources is yet unsolved. This is what we try to achieve in this paper. Alongside of other papers in this area, we do not target any particular device and only specify that low computational power, low code space, low communication bandwidth, and low energy resources are the constraints that our devices are dealing with.

### 1.2 Our Contribution

We propose an MRP and *for the first time* prove its security in the standard model and based on the existence of pseudorandom functions. The essential idea in our protocol consist in adding random coins in every step of the Jane Doe protocol or its self-recoverable variant due to Goldberg et al. [GMS09].

The MRP presented in this paper is based on the same design principle of the protocols by Lucks et al. [LZWW08] and Goldberg et al. [GMS09] which instructs Alice to send a message $m$ along with a commitment $d$ of $m$ to Bob. Then, Bob is to make Alice recognize him followed by Alice revealing the key in which the commitment was computed with. We use the same design principle, but we use different primitives, e.g., a pseudorandom function. Moreover, the only source of the randomness in the latter two proposals is the root of a hash chain, whereas we insert randomness per key while building the hash chain. Furthermore, using appropriate primitives along with more randomness, we end up *not* requiring the non-standard security assumptions that both Lucks et al. [LZWW08] and Goldberg et al. [GMS09] need to assume. Instead, we prove the security of our MRP based on standard assumptions. Note that the logic of our protocol is similar to the protocol due to Goldberg et al. [GMS09], as opposed to the original Jane Doe protocol, to obtain self-recoverability.

We make use of two primitives, a function $F : \{0,1\}^{s+k} \rightarrow \{0,1\}^s$ and a message authentication code $\mathrm{MAC} : \{0,1\}^s \times \{0,1\}^* \rightarrow \{0,1\}^c$. We define new notions of security for our primitives, $F$ and MAC, namely degree-$i$ preimage resistance and degree-$i$ second preimage resistance for $F$, and $F$-degree-$i$ existential unforgeability for MAC. Next, we show that these new notions are equivalent to preimage resistance, second preimage resistance, and existential unforgeability under the assumption that $F$ is a pseudorandom function.

In each protocol instance, Alice and Bob are only required to exchange one $F$ output during their encounter (when they meet in the party). This output can be as short as 80 bits.

As in the Jane Doe protocol, one instance of our MRP provides the message recognition primitive from Alice to Bob. This is not considered as a limitation since one uses two separate protocol instances, one in each direction, to achieve message recognition in both directions. Moreover, the total number of messages to be recognized is required to be preset, both in the Jane Doe protocol and in ours, but we propose the last message to be recognized to simulate a new 'key exchange during a party' which enables Alice and Bob to execute the protocol for another set of messages (see Section 3.2). This is possible whenever message recognition is in place in both directions.

The rest of the paper is organized as follows. In Section 2, we list and analyze the properties we require for the function $F$ and the message authentication code MAC and reduce them to the standard notions. Section 3 is dedicated to our MRP and proves its security based on the assumptions analyzed earlier.

## 2 Our Security Assumptions and Pseudorandom Functions

Suppose we have a function $F : \{0,1\}^{s+k} \rightarrow \{0,1\}^s$ and a message authentication code MAC : $\{0,1\}^s \times \{0,1\}^* \rightarrow \{0,1\}^c$. We now present three non-standard security notions for $F$ and MAC. Later, we show that these notions are equivalent to standard notions based on the assumption that pseudorandom functions exist.

By *$F$ is pseudorandom* we mean that *the $F_r$ family defined by $F_r(\rho) = F(\rho, r)$ is a pseudorandom function family.* In other words, an oracle initialized with a random $r$ and implementing $F_r$ would be indistinguishable from another implementing a random function after a polynomial number of queries. Note that we only require indistinguishability after a single query, and not multiple queries.

**Definition 1.** *For randomly chosen secrets $r_1, \dots, r_i$, each having $k$ bits, and randomly chosen secret $\rho_0$, of size $s$, let secret $\rho_1, \dots, \rho_{i-1}$ and known $\rho_i$ be such that $\rho_j = F(\rho_{j-1}, r_j)$, where $1 \leq j \leq i$. The function $F$ is a* **degree-$i$ preimage resistant ($i$-PR)** *function if it is infeasible to find $\pi$, of size $s + k$, such that $\rho_i = F(\pi)$.*

We note that the notion of degree-$i$ preimage resistance is similar to the well known notion of *one-way on iterates* first introduced by Levin [Lev85]. Variations of this notion was used later by other authors, see for example [GKL93]. We use our variation of 'one-way on iterates' and give it the new name 'degree-$i$ preimage resistance' to be consistent with the later security notions of this paper and also the literature on message recognition protocols.

The notion of degree-$i$ preimage resistance is illustrated in Figure 1 as a game between a player Oscar and a challenger.

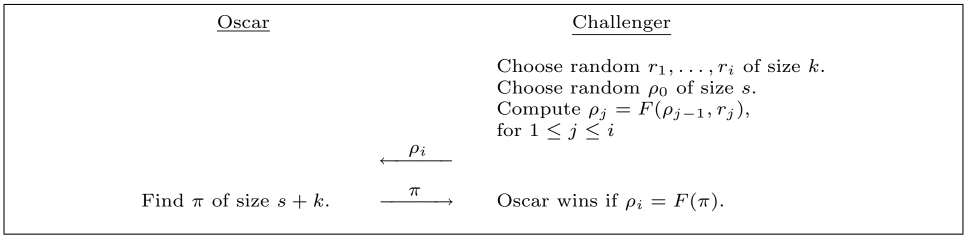

Oscar
Challenger
Choose random $r_1, \dots, r_i$ of size $k$.
Choose random $\rho_0$ of size $s$.
Compute $\rho_j = F(\rho_{j-1}, r_j)$,
for $1 \leq j \leq i$
$\xleftarrow{\rho_i}$
Find $\pi$ of size $s + k$.
$\xrightarrow{\pi}$
Oscar wins if $\rho_i = F(\pi)$.

**Fig. 1.** Degree-$i$ Preimage Resistant Game

Note that we obtain the classical notion of preimage resistance when $i = 0$. Moreover, for $k = 0$, we obtain the depth-$i$ preimage resistance considered by Lucks et al. [LZWW08]. In other words, we are considering extra randomness for each round, whereas they rely on the randomness of the root element of the hash chain for the entire life time of the protocol.

**Definition 2.** *For randomly chosen secrets $r_1, \ldots, r_{i-1}$, each having $k$ bits, and randomly chosen secret $\rho_0$, of size $s$, let secret $\rho_1, \ldots, \rho_{i-2}$ and known $\rho_{i-1}$ be such that $\rho_j = F(\rho_{j-1}, r_j)$, where $1 \leq j \leq i-1$. The function $F$ is a* **degree-$i$ second preimage resistant ($i$-SPR)** *function if, given a random $r_i$ of size $k$, it is infeasible to find $\pi$, of size $s+k$, such that $F(\rho_{i-1}, r_i) = F(\pi)$.*

Figure 2 depicts this notion as a game between a player and a challenger.

| Oscar | | Challenger |
|---|---|---|
| | | Choose random $r_1, \ldots, r_i$ of size $k$.<br>Choose random $\rho_0$ of size $s$.<br>Compute $\rho_j = F(\rho_{j-1}, r_j)$,<br>for $1 \leq j \leq i-1$ |
| | $\xleftarrow{\rho_{i-1}, r_i}$ | |
| Find $\pi$ of size $s+k$. | $\xrightarrow{\pi}$ | Oscar wins if $F(\rho_{i-1}, r_i) = F(\pi)$. |

**Fig. 2.** Degree-$i$ Second Preimage Resistant Game

Again, note that for $i = 1$, we obtain the classical notion of second preimage resistance. Furthermore, if we consider the case of $k = 0$, the case when the only source of randomness is $\rho_0$, we obtain the depth-$i$ second preimage resistance of Lucks et al. [LZWW08].

**Definition 3.** *For randomly chosen secrets $r_1, \ldots, r_i$, each having $k$ bits, and randomly chosen secret $\rho_0$, of size $s$, let secret $\rho_1, \ldots, \rho_{i-1}$ and known $\rho_i$ be such that $\rho_j = F(\rho_{j-1}, r_j)$, where $1 \leq j \leq i$. A message authentication code MAC is* **$F$-degree-$i$ existentially unforgeable ($i$-EU)** *if, knowing $\rho_i$, it is infeasible to mount an existential forgery against $MAC_{\rho_{i-1}}$ in an adaptive chosen message attack scenario.*

### 2.1 Pseudorandom Functions Satisfy $i$-PR

We now show that if $F$ is a pseudorandom function, then the notion of degree-$i$ preimage resistance for $F$ is equivalent to the notion of preimage resistance.

**Theorem 1.** *Consider a pseudorandom function $F : \{0,1\}^{s+k} \to \{0,1\}^s$ and let $i$ be polynomial in $s$ and $k$. Then, the function $F$ is preimage resistant if and only if it is degree-$i$ preimage resistant.*

We actually show a stronger result: if the distribution of $F(\rho, \pi)$, for $(\rho, \pi) \in_R \{0,1\}^{s+k}$, is computationally indistinguishable from the uniform distribution using a single sample, then $F$ is preimage resistant if and only if it is degree-$i$ preimage resistant.

Note that for $k = 0$, as in the case of properties introduced by Lucks et al. [LZWW08], this property can only be true if almost all elements of $\{0,1\}^s$ have a single preimage under $F$. For a random function $F$, the probability of every value to have no preimage is roughly $e^{-1}$. Hence, this property is almost never achieved. And, this argument justifies the introduction of random values $r_i$.

*Proof.* Define the success probability of a polynomially bounded player Oscar in the $i$PR game to be

$$Succ^i_{\mathrm{PR}} := \Pr(F(\pi) = \rho_i),$$

where the probability is taken over all random choices of Oscar and the Challenger. In other words, $F$ is an $i$-PR if and only if $Succ^i_{\mathrm{PR}}$ is negligible. We are going to first find an upperbound for $|Succ^i_{\mathrm{PR}} - Succ^{i-1}_{\mathrm{PR}}|$ and use triangle inequality to find an upper bound for $|Succ^i_{\mathrm{PR}} - Succ^1_{\mathrm{PR}}|$.

Moreover, for a variable $x$ of size $s$, define the degree-$i$ distribution to be

$$\mathcal{D}^i_{\mathrm{PR}}(x) := \Pr_{r_0, r_1, \ldots, r_i}[\rho_i = x].$$

Note that $\mathcal{D}^0_{\mathrm{PR}}$ is just the uniform distribution.

Consider a player, Charlie, who wants to distinguish a $\rho$ following either $\mathcal{D}^i_{\mathrm{PR}}$ or $\mathcal{D}^{i-1}_{\mathrm{PR}}$. As illustrated in Figure 3, Charlie can use Oscar as a black-box. His advantage is

$$Adv^i_{\mathrm{PR}} := |Succ^i_{\mathrm{PR}} - Succ^{i-1}_{\mathrm{PR}}|.$$

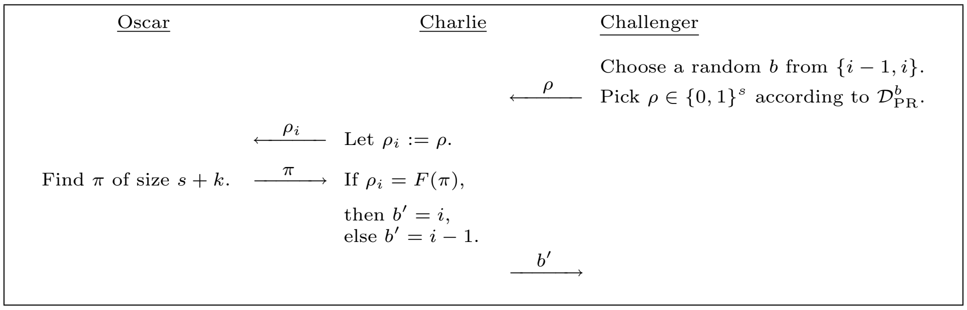

Oscar
Charlie
Challenger
Choose a random $b$ from $\{i-1, i\}$.
$\rho$
Pick $\rho \in \{0,1\}^s$ according to $\mathcal{D}^b_{\mathrm{PR}}$.
$\rho_i$
Let $\rho_i := \rho$.
Find $\pi$ of size $s + k$.
$\pi$
If $\rho_i = F(\pi)$,
then $b' = i$,
else $b' = i - 1$.
$b'$

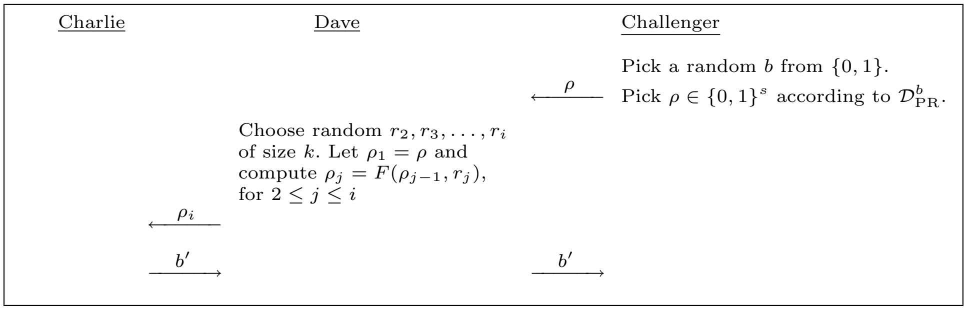
**Fig. 3.** Degree-$i$ Distinguishing Game

On the other hand, Charlie can be transformed into a distinguisher Dave between $\mathcal{D}^1_{\mathrm{PR}}$ and $\mathcal{D}^0_{\mathrm{PR}}$. To see this, consider a player Dave who, given $\rho$, uses Charlie as a black-box. This game is illustrated in Figure 4.

The advantage of Dave is equal to $Adv^i_{\mathrm{PR}}$. Therefore, $Adv^i_{\mathrm{PR}} = |Succ^i_{\mathrm{PR}} - Succ^{i-1}_{\mathrm{PR}}|$ must be negligible. Now applying the triangle inequality $i-1$ times, we obtain that $|Succ^i_{\mathrm{PR}} - Succ^1_{\mathrm{PR}}|$ is negligible.

Note that $Succ^1_{\mathrm{PR}}$ is simply the success probability of the adversary in winning the standard notion of preimage resistance for our function $F$. On the other hand, if the function $F$ is pseudorandom, then the advantage of any polynomial time distinguisher between $\mathcal{D}^1_{\mathrm{PR}}$ and $\mathcal{D}^0_{\mathrm{PR}}$ must be negligible. Therefore, we have shown that $F$ is $i$-PR if and only if it is PR.

□



Pick a random $b$ from $\{0,1\}$.
Pick $\rho \in \{0,1\}^s$ according to $\mathcal{D}^b_{\text{PR}}$.

Choose random $r_2, r_3, \ldots, r_i$ of size $k$. Let $\rho_1 = \rho$ and compute $\rho_j = F(\rho_{j-1}, r_j)$, for $2 \leq j \leq i$

**Fig. 4.** Reducing Degree-1 Distinguishing Game to Degree-$i$ Distinguishing Game

### 2.2 Pseudorandom Functions Satisfy $i$-SPR

Similarly to the previous section, we show that the notions of degree-$i$ second preimage resistance and second preimage resistance are equivalent for a pseudorandom function $F$.

**Theorem 2.** *Consider a pseudorandom function $F : \{0,1\}^{s+k} \to \{0,1\}^s$ and let $i$ be polynomial in $s$ and $k$. Then, the function $F$ is second preimage resistant if and only if it is degree-$i$ second preimage resistant.*

Again, we prove a slightly stronger statement than the Theorem. We prove that if the distribution of $F(\rho, \pi)$, for $(\rho, \pi) \in_R \{0,1\}^{s+k}$, is computationally indistinguishable from the uniform distribution using a single sample, then $F$ is second preimage resistant if and only if it is degree-$i$ second preimage resistant.

*Proof.* We define the success probability of a computationally bounded player Oscar in the $i$SPR game to be

$$Succ^i_{\text{SPR}} := \Pr(F(\pi) = F(\rho_{i-1}, r_i)),$$

where the probability is taken over all random choices of Oscar and Challenger.

To show that $F$ is $i$SPR, we need to show that $Succ^i_{\text{SPR}}$ is negligible. We first find an upperbound for $|Succ^i_{\text{SPR}} - Succ^{i-1}_{\text{SPR}}|$ and, then, using the triangle inequality find an upperbound for $|Succ^i_{\text{SPR}} - Succ^1_{\text{SPR}}|$.

Now consider Charlie who wants to distinguish $\rho$ following either $\mathcal{D}^{i-1}_{\text{PR}}$ or $\mathcal{D}^{i-2}_{\text{PR}}$. Figure 5 is depicting Charlie when he is using Oscar as a black-box to distinguish between a random value and $\rho_{i-1}$. This reduction implies that $|Succ^i_{\text{SPR}} - Succ^{i-1}_{\text{SPR}}|$ is the advantage for distinguishing $\mathcal{D}^{i-1}_{\text{PR}}$ from $\mathcal{D}^{i-2}_{\text{PR}}$.

We conclude like in the proof of Theorem 1.

□

### 2.3 Existential Unforgeable MACs Are $i$-EU

In this section, given a pseudorandom functions $F$ and a secure message authentication code MAC, we show that MAC is also degree-$i$ existentially unforgeable.

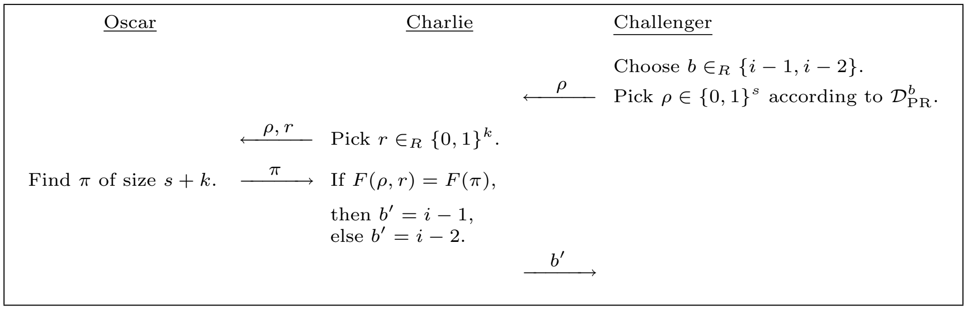

Oscar
Charlie
Challenger
Choose $b \in_R \{i-1, i-2\}$.
Pick $\rho \in \{0,1\}^s$ according to $\mathcal{D}^b_{\mathrm{PR}}$.
$\rho$
$\rho, r$
Pick $r \in_R \{0,1\}^k$.
Find $\pi$ of size $s+k$.
$\pi$
If $F(\rho, r) = F(\pi)$,
then $b' = i-1$,
else $b' = i-2$.
$b'$

**Fig. 5.** Degree-$i$ Distinguishing Game

**Theorem 3.** *Consider a message authentication code* MAC : $\{0,1\}^s \times \{0,1\}^* \rightarrow \{0,1\}^c$ *and a function* $F : \{0,1\}^{s+k} \rightarrow \{0,1\}^s$*, where* $k \geq 2s$*. If* $i$ *is polynomial in* $s$ *and* $k$*, and* $F$ *is a pseudorandom function, then, the notions of existential unforgeability and* $F$*-degree-*$i$ *existential unforgeability are equivalent.*

*Proof.* For a variable $x$, of size $s$, we define the following distribution

$$\mathcal{D}^i_\rho(x) = \Pr_r[F(\rho, r) = x].$$

We need to show that for all $\rho$, $\mathcal{D}^i_\rho$ is indistinguishable from the uniform distribution, using a single sample. This comes from $(F(.,r))_{r \in \{0,1\}^k}$ being a pseudorandom function. As in the analysis in the previous proofs, $i$-EU is equivalent to 1-EU. We now show that 1-EU is equivalent to EU.

Let Oscar be a player who finds standard existential forgeries, and Charlie be a player who is trying to distinguish between $\mathcal{D}^1_\rho$ and the uniform distribution. Now, Charlie uses Oscar as a black box, as illustrated in Figure 6. Note that with $b = 1$, Oscar is a 1-EU adversary. On the other hand, with $b = 0$, Oscar is a regular EU adversary (who is given a useless $x$). Let $Succ_{b=0}$(Oscar) be the success probability of Oscar when $b = 0$ and $Succ_{b=1}$(Oscar) be his success probability when $b = 1$.

For every $\rho$, the advantage of Charlie in distinguishing between $\mathcal{D}^1_\rho$ and the uniform distribution is negligible. Hence, on average, the advantage is negligible too. As a result, $|Succ_{b=0}(\text{Oscar}) - Succ_{b=1}(\text{Oscar})|$ is negligible. Thus, we obtain that $Succ_{b=1}$(Oscar) is negligible if and only if $Succ_{b=0}$(Oscar) is negligible, that is if MAC is existentially unforgeable.

□

### 2.4 Separation between PR and *i*-PR

We show that there is a separation between preimage resistance and degree-$i$ preimage resistance. This implies that considering both assumptions is necessary. Let $\ell : \{0,1\}^s \rightarrow \{1, 2, \ldots, s\}$ be defined as $\ell(x) =$ the number of leading zeros of $x$. Consider a preimage resistant hash function $H$ and define

$$F(x, r) := \mathrm{trunc}_s(0^{\ell(x)+1} 1 \| H(x \| r)),$$

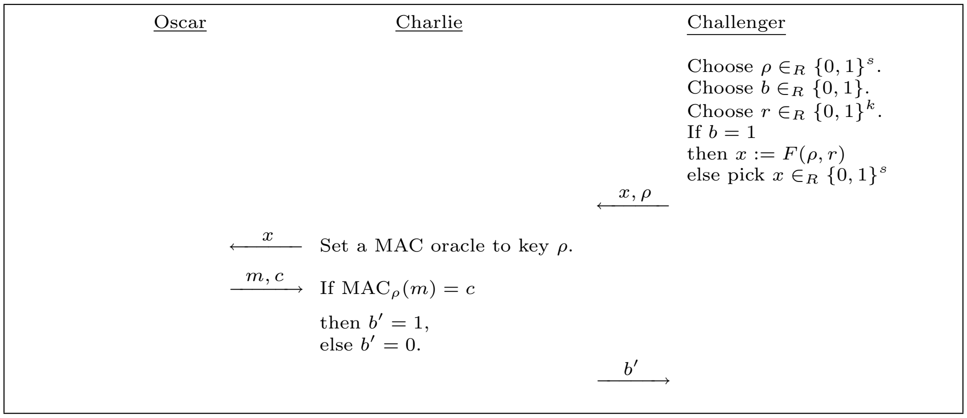

Oscar
Charlie
Challenger
Choose $\rho \in_R \{0,1\}^s$.
Choose $b \in_R \{0,1\}$.
Choose $r \in_R \{0,1\}^k$.
If $b = 1$
then $x := F(\rho, r)$
else pick $x \in_R \{0,1\}^s$
$x, \rho$
$x$
Set a MAC oracle to key $\rho$.
$m, c$
If $\mathrm{MAC}_\rho(m) = c$
then $b' = 1$,
else $b' = 0$.
$b'$

**Fig. 6.** Reducing 1-EU to EU

where $\mathrm{trunc}_s$ outputs the first $s$ bits of the input. Since $H$ is preimage resistant, $F$ is also preimage resistant. However, $F$ is not degree-$s$ preimage resistant. One can make similar constructions for degree-$i$ second preimage resistance.

## 3 A Message Recognition Protocol Based on Pseudorandom Functions

Consider a pseudorandom function $F : \{0,1\}^{s+k} \to \{0,1\}^s$ and a message authentication code $\mathrm{MAC} : \{0,1\}^s \times \{0,1\}^* \to \{0,1\}^c$ with typical parameters $s \geq 80$, $k \geq 2s$, and $c \geq 30$. Moreover, let the maximum number of messages to be authenticated be fixed to be $n$.

Alice randomly chooses $a_0, a_1, \ldots, a_{n-1}$ of size $k$ and $\alpha_0$ of size $s$, and forms a chain of the form $\alpha_i = F(\alpha_{i-1}, a_{i-1})$, $i = 1, \ldots, n$. Analogously, Bob chooses random $b_0, b_1, \ldots, b_{n-1}$ of size $k$ and $\beta_0$ of size $s$, and forms his chain of the form $\beta_i = F(\beta_{i-1}, b_{i-1})$, $i = 1, \ldots, n$.

They start with index $n$ and go downward in the $\alpha$ and $\beta$ chains, revealing elements of hash chains and the random keys in a descending order. In each session $i$, Alice and Bob, respectively, use the random $a_i$ and $b_i$ as keys for the MAC values they compute. On the other hand, they use $\alpha_i$ and $\beta_i$ in session $i+1$ to commit to $a_i$ and $b_i$ of session $i$.

The protocol starts with an initialization phase, illustrated in Figure 7, in which Alice and Bob exchange $\alpha_n$ and $\beta_n$ over an authenticated channel. Eve is passive at this stage, hence, the channel is denoted by $\Rightarrow$.

We first present a high level description of our protocol, depicted in Figure 8 based on the logic of the Jane Doe protocol. Although this high level presentation does not include the details of our proposal, it helps in signifying the differences and it gives a better big picture on how the hash chaining technique is modified in order to obtain a security proof based on standard assumptions.

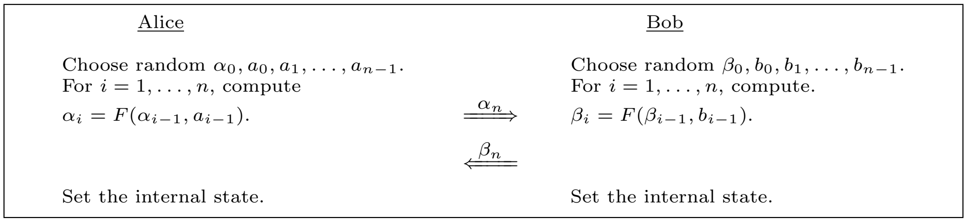

Alice
Bob
Choose random $\alpha_0, a_0, a_1, \ldots, a_{n-1}$.
For $i = 1, \ldots, n$, compute
$\alpha_i = F(\alpha_{i-1}, a_{i-1})$.
$\xrightarrow{\alpha_n}$
$\xleftarrow{\beta_n}$
Choose random $\beta_0, b_0, b_1, \ldots, b_{n-1}$.
For $i = 1, \ldots, n$, compute.
$\beta_i = F(\beta_{i-1}, b_{i-1})$.
Set the internal state.
Set the internal state.

**Fig. 7.** Initialization Phase

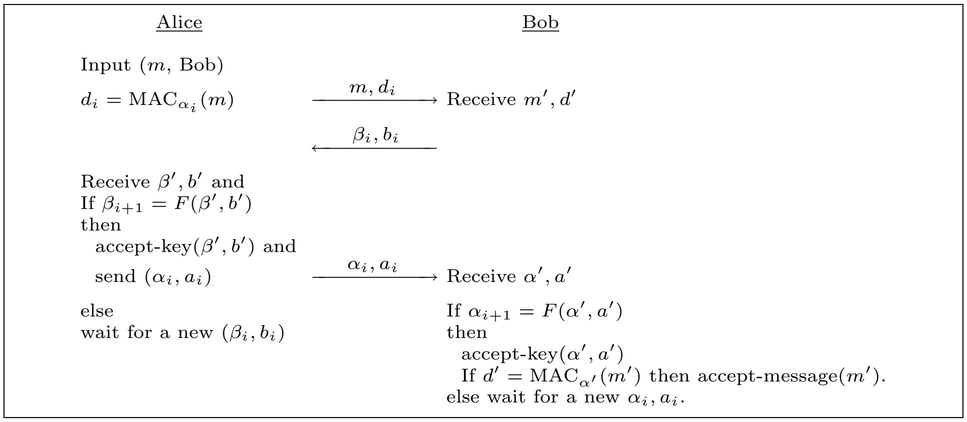

Alice
Bob
Input ($m$, Bob)
$d_i = \text{MAC}_{\alpha_i}(m)$
$\xrightarrow{m, d_i}$
Receive $m', d'$
$\xleftarrow{\beta_i, b_i}$
Receive $\beta', b'$ and
If $\beta_{i+1} = F(\beta', b')$
then
accept-key($\beta', b'$) and
send ($\alpha_i, a_i$)
$\xrightarrow{\alpha_i, a_i}$
Receive $\alpha', a'$
else
wait for a new ($\beta_i, b_i$)
If $\alpha_{i+1} = F(\alpha', a')$
then
accept-key($\alpha', a'$)
If $d' = \text{MAC}_{\alpha'}(m')$ then accept-message($m'$).
else wait for a new $\alpha_i, a_i$.

**Fig. 8.** High Level Description of our Message Recognition Protocol

Alice uses $\alpha_i$ as the key for the MAC value, but also to make Bob recognize her. Bob uses $\beta_i$, so Alice will recognize him. However, $b_i$s are not used to send a message. Note that the role of Alice, as the claimant, and the role of Bob, as the verifier are not reversible. In other words, if Bob wishes to authenticate messages to Alice, they should fix another pair of random keys. Indeed, if the same $\alpha_i$ and $\beta_i$ are used, a man-in-the-middle attack is possible.

In order to present the details of the logic of our proposed protocol, we adapt the approach of Goldberg et al. [GMS09] to obtain a self-recoverable MRP. Note that our building blocks are different from theirs and, more importantly, our security assumptions are different. The point in adapting the logic of the protocol is to ensure self-recoverability of the protocol.

The internal state of Alice includes (along with each variable's initial value):
- $i_A := n - 1$: the position of Alice in her chain.
- $i_{accA} := n$: the last index of Bob's chain that was accepted by Alice.
- $\beta_A := \beta_n$: the last value of Bob's chain that was accepted by Alice.
- $b_A := Null$: the last value for Bob's randomness accepted by Alice.
- $M := Null$: the input message to be authenticated in the current session.
- a one-bit flag, to distinguish the program states **A0** and **A1**.

Similarly, Bob's internal state is as follows:

- $i_B := n - 1$: the position of Bob in his chain.
- $i_{accB} := n$: the last index of Alice's chain that was accepted by Bob.
- $\alpha_B := \alpha_n$: the last value of Alice's chain that was accepted by Bob.
- $a_B := Null$: the last value for Bob's randomness accepted by Alice.
- $e' := Null$: the MAC value received in the current session, supposedly from Alice.
- $M' := Null$: the message received in the current session, supposedly from Alice.
- a one-trit flag, to distinguish the program states **B0**, **B1**, and **B2**.

We write commit-message$(M, i_A)$ to indicate that Alice is committing herself to sending the message $M$ to Bob in session $i_A$. We let $T$ be the maximum amount of time Alice waits to receive a response from Bob, and vice versa. Alice and Bob start in program states **A0** and **B0**.

**A0** is executed as follows:

```
If $i_A \leq 0$ then Abort.
Receive input $(M)$.
Compute $e_{i_A} := \mathrm{MAC}_{\alpha_{i_A}}(i_A \| M)$.
Send $[e_{i_A}, M]$ to Bob and goto A1.
```

**B0** is executed as follows:

```
If $i_B \leq 0$ then Abort.
Wait to receive $[e', M']$, then goto B1.
```

**B1** has the following description:

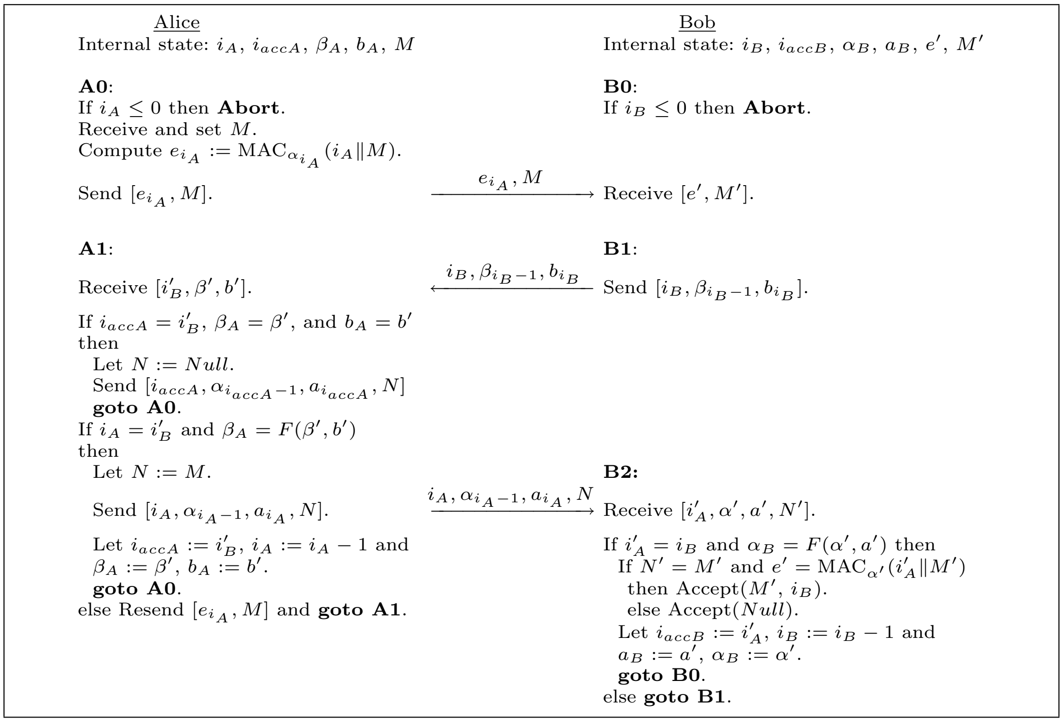
```
Send $[i_B, \beta_{i_B - 1}, b_{i_B}]$ to Alice and goto B2.
```

**A1** is performed in the following manner:

```
Wait at most time $T$ to receive $[i'_B, \beta', b']$.
If $[i'_B, \beta', b']$ is received, then
    If $i_{accA} = i'_B$, $\beta_A = \beta'$, and $b_A = b'$ (Bob has not received the last flow
    of the previous session) then
        Let $N := Null$.
        Send $[i_{accA}, \alpha_{i_{accA}-1}, a_{i_{accA}}, N]$ and goto A0.
    If $i_A = i'_B$ and $\beta_A = F(\beta', b')$ then (Alice and Bob seem to be synchronized.)
        Let $N := M$.
        Send $[i_A, \alpha_{i_A - 1}, a_{i_A}, N]$ to Bob.
        Let $i_{accA} := i'_B$, $i_A := i_A - 1$, $\beta_A := \beta'$, $b_A := b'$. (Alice updates her
        state.)
        goto A0.
    else Resend $[e_{i_A}, M]$ to Bob and goto A1.
If timeout then
Resend $[e_{i_A}, M]$ to Bob and goto A1.
```

**B2** is performed as follows:

```
Wait at most time $T$ to receive $[i'_A, \alpha', a', N']$.
If $[i'_A, \alpha', a', N']$ is received, then
    If $i'_A = i_B$ and $\alpha_B = F(\alpha', a')$ then (Alice and Bob seem to be synchronized.)
        If $N' = M'$ and $e' = \mathrm{MAC}_{\alpha'}(i'_A \| M')$ then
            Accept($M'$, $i_B$).
        else Accept($Null$).
        Let $i_{accB} := i'_A$, $i_B := i_B - 1$, $\alpha_B := \alpha'$, $a_B := a'$. (Bob updates his state.)
        goto B0.
    else goto B1.
If timeout, then goto B1.
```



| Alice | | Bob |
|---|---|---|
| Internal state: $i_A$, $i_{accA}$, $\beta_A$, $b_A$, $M$ | | Internal state: $i_B$, $i_{accB}$, $\alpha_B$, $a_B$, $e'$, $M'$ |
| **A0**:<br>If $i_A \leq 0$ then **Abort**.<br>Receive and set $M$.<br>Compute $e_{i_A} := \mathrm{MAC}_{\alpha_{i_A}}(i_A \| M)$. | | **B0**:<br>If $i_B \leq 0$ then **Abort**. |
| Send $[e_{i_A}, M]$. | $\xrightarrow{e_{i_A}, M}$ | Receive $[e', M']$. |
| **A1**: | | **B1**: |
| Receive $[i'_B, \beta', b']$. | $\xleftarrow{i_B, \beta_{i_B - 1}, b_{i_B}}$ | Send $[i_B, \beta_{i_B - 1}, b_{i_B}]$. |
| If $i_{accA} = i'_B$, $\beta_A = \beta'$, and $b_A = b'$ then<br>Let $N := Null$.<br>Send $[i_{accA}, \alpha_{i_{accA} - 1}, a_{i_{accA}}, N]$<br>**goto A0**.<br>If $i_A = i'_B$ and $\beta_A = F(\beta', b')$ then<br>Let $N := M$. | | **B2:** |
| Send $[i_A, \alpha_{i_A - 1}, a_{i_A}, N]$. | $\xrightarrow{i_A, \alpha_{i_A - 1}, a_{i_A}, N}$ | Receive $[i'_A, \alpha', a', N']$. |
| Let $i_{accA} := i'_B$, $i_A := i_A - 1$ and $\beta_A := \beta'$, $b_A := b'$.<br>**goto A0**.<br>else Resend $[e_{i_A}, M]$ and **goto A1**. | | If $i'_A = i_B$ and $\alpha_B = F(\alpha', a')$ then<br>If $N' = M'$ and $e' = \mathrm{MAC}_{\alpha'}(i'_A \| M')$<br>then Accept($M'$, $i_B$).<br>else Accept($Null$).<br>Let $i_{accB} := i'_A$, $i_B := i_B - 1$ and $a_B := a'$, $\alpha_B := \alpha'$.<br>**goto B0**.<br>else **goto B1**. |

**Fig. 9.** Proposed Message Recognition Protocol

Figure 9 illustrates the common case of our protocol. It is worth mentioning that since we are basing our protocol on the logic of the message recognition protocol of Goldberg et al. [GMS09], the security analysis, specially the reductions, are similar to those presented in their paper. For example, our protocol directly inherits the self-recoverability property of their protocol. Hence, we do not discuss self-recoverability. On the other hand, we stress that we are using different assumptions and primitives to start with. Hence, we obtain a different protocol and it deserves its own security analysis.

### 3.1 Security Result

In Appendix A, we prove the following theorem which is analogous to the Security and Self-recoverability Theorem of Goldberg et al. [GMS09].

**Theorem 4.** *A successful adversary against the protocol of Section 3 who efficiently deceives Bob into accepting ($M'$,$i$), where $M'$ is not $Null$ and Alice did not send $M'$ in session $i$, implies an efficient algorithm that finds degree-$i$ preimages or degree-$i$ second preimages, or creates degree-$i$ existential forgeries. Moreover, the adversary cannot stop Alice and Bob from successfully executing the protocol unless she is actively disrupting the communication for the lifetime of Alice and Bob.*

The above theorem together with the theorems of Section 2, namely Theorems 1, 2, and 3, imply the following theorem.

**Theorem 5 (Final result).** *Consider a pseudorandom function $F : \{0,1\}^{s+k} \to \{0,1\}^s$, $k \geq 2s$, and a message authentication code* $\mathrm{MAC} : \{0,1\}^s \times \{0,1\}^* \to \{0,1\}^c$. *Moreover, let $i$ be polynomial in $s$ and $k$. If $F$ is preimage resistant and second preimage resistant, and if $MAC$ is existentially unforgeable, then there is no efficient adversary against the $i$th session of the protocol of Section 3.*

The condition on $i$ being a polynomial in $s$ and $k$ is unavoidable to get negligible advantage for the distinguishers in Theorems 1, 2, and 3. On the other hand, note that $i \leq n$ to begin with and, hence, this assumption is reasonable.

### 3.2 Discussion

Our MRP shares some similarities with protocols based on hash chains (e.g., TESLA [HPJ02], OTP (S/Key) [HMNS98], Lamport authentication [Lam81]). These protocols can adapt to different data structures such as hash trees (see for example, Merkle signatures [Mer89] and Merkle tree traversal [Szy04]) and can be turned into dynamic ones (consult Naor and Yung [NY89]).

Once our MRP is in place in both directions, using two separate pairs of chains, we can use the last two iterations to authenticate some new $\alpha_n$ and $\beta_n$ to be able to continue. Note that using the same pair of hash chains in both directions results in man-in-the-middle type of attacks.

## 4 Conclusion

Incorporating random coins in every step of a hash chain, we proposed the first MRP which is provably secure in the standard model and based on standard assumptions. Our protocol uses two primitives, a pseudorandom function $F : \{0,1\}^{s+k} \rightarrow \{0,1\}^s$ and an existential unforgeable message authentication code $\mathrm{MAC} : \{0,1\}^s \times \{0,1\}^* \rightarrow \{0,1\}^c$.

We defined new notions of security for our primitives, $F$ and MAC, namely degree-$i$ preimage resistance and degree-$i$ second preimage resistance for $F$, and $F$-degree-$i$ existential unforgeability for MAC. Then, we showed that these new properties are equivalent to the standard notions of preimage resistance, second preimage resistance, and existential unforgeability under the assumption that $F$ is a pseudorandom function.

## References

[ABC$^+$98] Ross Anderson, Francesco Bergadano, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas, and Roger Needham. A new family of authentication protocols. In *ACMOSR: ACM Operating Systems Review*, volume 32, pages 9–20, 1998.

[Geh98] Christian Gehrmann. Multiround unconditionally secure authentication. *Designs, Codes, and Cryptography*, 15(1):67–86, 1998.

[GKL93] Oded Goldreich, Hugo Krawczyk, and Michael Luby. On the existence of pseudorandom generators. *SIAM J. Comput.*, 22(6):1163–1175, 1993.

[GMS09] Ian Goldberg, Atefeh Mashatan, and Douglas R. Stinson. A new message recognition protocol with self-recoverability for ad hoc pervasive networks. In Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, and Damien Vergnaud, editors, *ACNS*, volume 5536 of *Lecture Notes in Computer Science*, pages 219–237, 2009.

[GN04] Christian Gehrmann and Kaisa Nyberg. Security in personal area networks. *Security for Mobility, IEE, London*, pages 191–230, 2004.

[HMNS98] N. Haller, C. Metz, P. Nesser, and M. Straw. A One-Time Password System. RFC 2289, February 1998.

[HPJ02] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. In Ian F. Akyildiz, Jason Yi-Bing Lin, Ravi Jain, Vaduvur Bharghavan, and Andrew T. Campbell, editors, *MOBICOM*, pages 12–23. ACM, 2002.

[HWGW05] Jonathan Hammell, André Weimerskirch, Joao Girao, and Dirk Westhoff. Recognition in a low-power environment. In *ICDCSW '05: Proceedings of the Second International Workshop on Wireless Ad Hoc Networking (WWAN)*, pages 933–938, Washington, DC, USA, 2005. IEEE Computer Society.

[Lam81] Leslie Lamport. Password authentification with insecure communication. *Commun. ACM*, 24(11):770–772, 1981.

[Lev85] L A Levin. One-way functions and pseudorandom generators. In *STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 363–365, New York, NY, USA, 1985. ACM.

[LZWW08] Stefan Lucks, Erik Zenner, André Weimerskirch, and Dirk Westhoff. Concrete security for entity recognition: The Jane Doe protocol. In *Progress in Cryptology—INDOCRYPT 2008*, volume 5365 of *Lecture Notes in Computer Science*, pages 158–171. Springer, 2008.

[Mer89] Ralph C. Merkle. A certified digital signature. In Gilles Brassard, editor, *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 218–238. Springer, 1989.

[Mit03] Chris J. Mitchell. Remote user authentication using public information. In Kenneth G. Paterson, editor, *IMA Int. Conf.*, volume 2898 of *Lecture Notes in Computer Science*, pages 360–369. Springer, 2003.

[MS08] Atefeh Mashatan and Douglas R. Stinson. A new message recognition protocol for ad hoc pervasive networks. In Matthew K. Franklin, Lucas Chi Kwong Hui, and Duncan S. Wong, editors, *CANS*, volume 5339 of *Lecture Notes in Computer Science*, pages 378–394. Springer, 2008.

[MS09] Atefeh Mashatan and Douglas R. Stinson. Interactive two-channel message authentication based on interactive-collision resistant hash functions. *Int. J. Inf. Secur.*, 8(1):49–60, 2009.

[NY89] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *STOC*, pages 33–43. ACM, 1989.

[SA99] Frank Stajano and Ross Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In B. Christianson, B. Crispo, , and M. Roe, editors, *Security Protocols, 7th International Workshop Proceedings*, Lecture Notes in Computer Science, 1999.

[Szy04] Michael Szydlo. Merkle tree traversal in log space and time. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 541–554. Springer, 2004.

[Vau05] Serge Vaudenay. Secure communications over insecure channels based on short authenticated strings. In Victor Shoup, editor, *Advances in Cryptography, CRYPTO 05: The 25th Annual International Cryptology Conference*, volume 3621 of *Lecture Notes in Computer Science*, pages 309–326, Santa Barbara, California, U.S.A., August 2005. Springer-Verlag.

[WW03] André Weimerskirch and Dirk Westhoff. Zero common-knowledge authentication for pervasive networks. In *Selected Areas in Cryptography*, volume 3006 of *Lecture Notes in Computer Science*, pages 73–87. Springer, 2003.

## A Proof of Theorem 4

We list all possible attacks against our protocol and show that they are all infeasible when the assumptions listed in Section 2 hold. This discussion is similar to what is presented by Goldberg et al. [GMS09].

Eve remains passive for a period of time and, at some point, she gets active to carry out her attack. Since Eve was a passive observer before the attack, it holds that $i_A = i_B$ before she starts her attack. Let $i := i_A = i_B$ and observe that at the start of session $i$ we have $i_{accA} = i_{accB} = i+1$, $a_B = a_{i+1}$, $b_A = b_{i+1}$, $\alpha_B = \alpha_i$, $\beta_A = \beta_i$.

We adapt the approach of Gehrmann [Geh98] in listing all possible attacks by considering different orderings of the flows. Gehrmann labels a flow by **A** when the recipient is Alice. Analogously, a flow is labelled as **B**, if the recipient is Bob. One distinguishes between the attacks that are started in one session and are completed in the same session versus the attacks that are started in one session and completed in a later session, named multi-session attacks.

We first analyze single-session attacks. Recall that Eve has been passive before the session the attack takes place and was only observing the activities. Hence, the attack is started and completed in session $i$. Gehrmann [Geh98] has showed that there are only $\binom{4}{2} = 6$ different single-session attacks for a three flow protocol. In his notation, these attacks are labelled as AABB, ABAB, BBAA, ABBA, BABA, and BAAB. We will reduce the AABB and BBAA attack scenarios to degree-$i$ preimage resistant or degree-$i$ second preimage resistant games. Moreover, we reduce the ABAB attack scenario to degree-$i$ existential forgeries, degree-$i$ preimage resistant, or degree-$i$ second preimage resistant games.

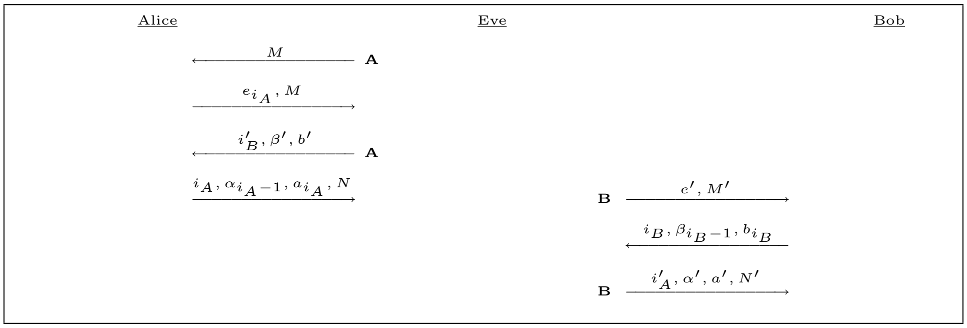


**Fig. 10.** AABB Attack

**AABB Attack.** This attack scenario is depicted in Figure 10. Recall that up until the start of this session, Alice and Bob were synchronized having $i_A = i_B = i$. Hence, Eve has to set $i'_A := i$, otherwise Bob will detect Eve, and $i'_B := i$, otherwise Alice will detect Eve. Moreover, recall that $\beta_A = \beta_i$ and $\alpha_B = \alpha_i$. Alice sends $i_A, \alpha_{i_A-1}, a_{i_A}, N$ to Eve if and only if $i'_B, \beta', b'$ are verified. It implies that unless $\beta_A = F(\beta', b')$, Alice will not cooperate with Eve. Hence, having seen $\beta_i$ and not having seen $\beta_{i-1}, b_i$, Eve has to find $\beta'$ and $b'$ such that $\beta_i = F(\beta', b')$. That is, Eve has to win the degree-$i$ preimage resistant game of Definition 1.

**BBAA Attack.** This scenario is shown in Figure 11. For Eve not to be detected by Bob, she has to find $i'_A, \alpha', a'$, and $N'$ such that they get verified by Bob. Note that Eve has $\alpha_B = \alpha_i$ from the previous session. This implies that, not having seen $\alpha_{i-1}, a_i$, Eve has to find $\alpha'$ and $a'$ such that $\alpha_i = F(\alpha', a')$. Again, if Eve successfully finds such $\alpha'$ and $a'$, then she can win the degree-$i$ preimage resistant game of Definition 1.

**ABAB Attack.** Figure 12 illustrates this scenario. Eve first receives $\beta_{i_B-1} = \beta_{i-1}$ and $b_{i_B} = b_i$. Then, she has the choice between setting $(\beta', b') = (\beta_{i-1}, b_i)$ or $(\beta', b') \neq (\beta_{i-1}, b_i)$. Let us assume that she sets $(\beta', b') \neq (\beta_{i-1}, b_i)$. In order for Eve not to get detected by Alice, Eve must find $\beta'$ and $b'$ such that

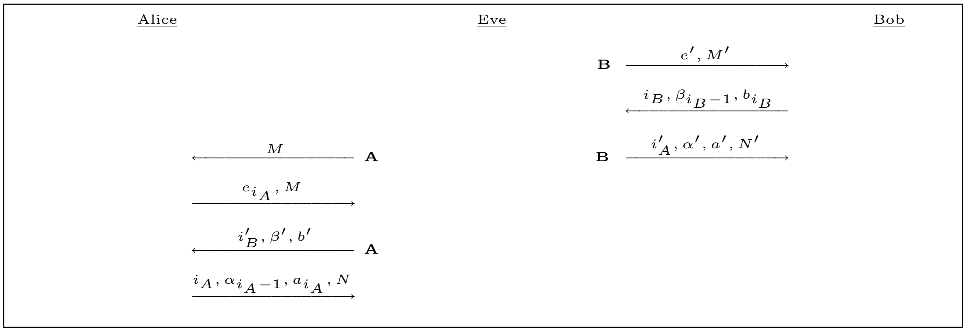


**Fig. 11.** BBAA Attack

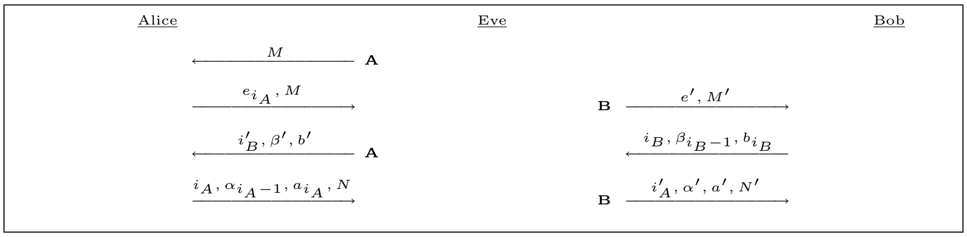


**Fig. 12.** ABAB Attack

$F(\beta', b') = F(\beta_{i-1}, b_i)$. This implies that she has to win the degree-$i$ second preimage resistant game of Definition 2.

Now, assume that $(\beta', b') = (\beta_{i-1}, b_i)$. Alice will verify $\beta'$ and $b'$ and, then, send $i_A, \alpha_{i_A-1}, a_{i_A}, N$. Again, Eve has the choice between setting $(\alpha', a') = (\alpha_{i-1}, a_i)$ or $(\alpha', a') \neq (\alpha_{i-1}, a_i)$. In order to set $(\alpha', a') \neq (\alpha_{i-1}, a_i)$ and not get detected by Bob, she has to win the degree-$i$ second preimage resistant game of Definition 2. Let us now assume that she chooses $(\alpha', a') = (\alpha_{i-1}, a_i)$. For Eve not to get detected by Bob, she has to first set $N' := M'$. Moreover, *not knowing* $a'$, Eve must have set $e' := \mathrm{MAC}_{\alpha'}(i'_A \| M')$, for $M'$ to be verified by Bob. Hence, Eve has to perform a degree-$i$ existential forgery, introduced in Definition 3.

It can be shown that the remaining three attack scenarios are reduced to the former three scenarios. In particular, one can reduce the BABA attack to the ABBA attack. Next, the ABBA attack is reduced to the ABAB attack. Last, but not least, one reduces the BAAB attack to the ABAB attack. It remains to take care of multi-session attacks against our protocol. Analogous to the analysis presented by Goldberg et.al [GMS09], one can show that multi-session attacks and show that they reduce to single-session attacks. The reductions for our protocol are analogous to the reductions presented by Goldberg et.al [GMS09], hence, we do not repeat them here.