On the (Im)possibility of Perennial Message Recognition Protocols without Public-Key Cryptography

Madeline González Muñiz
Cybernetica AS
Akadeemia 21
Tallinn, Estonia
madeline@cyber.ee

Peeter Laud
Cybernetica AS
Aleksandri 8a
Tartu, Estonia
peeter@cyber.ee

ABSTRACT

A message recognition protocol (MRP) aims to exchange authenticated information in an insecure channel. During the initialization session of the protocol, the parties exchange some authenticated information which the adversary can passively observe. Then, one party wants to send authenticated messages to the other party over an insecure channel. Such security requirements are often found in wireless sensor networks.

A *perennial* MRP is one that is able to recover from the adversarial interference, no matter how long the adversary has been active before it stops. MRPs based on hash chains are not perennial because after fixing the length of the hash chain in the initialization phase, authentic communication is not possible if the adversary interferes until all elements of the hash chain have been consumed.

Perennial MRPs can be trivially built from public-key primitives. In this paper we present very strong evidence that they cannot be constructed from "cheap" primitives. Namely, we show in the symbolic model of cryptography, perennial MRPs cannot be built using just hash functions and XORing. The result also covers other symmetric primitives, e.g. encryption. The result explains why all previous attempts to construct perennial MRPs from those primitives have failed. The result also has interesting implications regarding authentication protocols in general, and the gap between formal and computational models of cryptography.

Categories and Subject Descriptors

D.4.6,K.6.5 [**Security and Protection**]: [Authentication]

General Terms

algorithms, security

Keywords

message recognition, Dolev-Yao model, symmetric cryptography

SAC'11 March 21-25, 2011, TaiChung, Taiwan.

1. INTRODUCTION

When considering resource-restricted devices, public-key cryptographic protocols such as secret key exchanges and asymmetric encryption may not be practical. Without the use of a private channel, a MRP aims at achieving data integrity with respect to the data origin. That is, the purpose of a MRP is to allow authenticated communication of messages over insecure channels. In the scenario that we have in mind, there are two honest parties, Alice and Bob, with Alice sending messages in an authenticated way to Bob, while the adversary, Eve, interferes with the communication channel.

The protocol proceeds in two phases. Initially, Alice and Bob have no common knowledge. In the *intialization* phase of the protocol, the channel between Alice and Bob is authentic, but can be eavesdropped by Eve; hence, Eve cannot alter, delete, or withhold messages during this phase. In the *main* phase of the protocol, the channel is insecure, i.e. Eve can perform active attacks. As Eve would trivially succeed, we do not consider denial-of-service attacks where Eve stops the flow of messages permanently between Alice and Bob.

We are interested in protocols that provide *authenticity* and *perenniality*. Informally, an MRP is authentic if for any message M that Bob accepts, the transmission of M was previously initated by Alice. An MRP is perennial if all messages M, whose transmission was initiated by Alice, eventually will be accepted by Bob, provided that Eve stops active attacks at some point in the main phase. At no point in time will Alice and Bob know whether Eve has already stopped all active attacks, or will she intend to perform more of them in the future. Formal definitions of authenticity and perenniality will be provided below.

We continue the current paper with a brief survey of proposed MRPs and impossibility results in cryptography, after which we give a formalization for two-party protocols in the perfect cryptography (Dolev-Yao) model. We then give definitions of authenticity and perenniality for MRPs and show that, with the chosen set of cryptographic primitives, there can be no protocol satisfying both properties.

2. RELATED WORK

In the literature, there have been a number of proposals for MRPs. Motivated by the use of low-cost and low-power devices such as RFID tags, Lucks et al. proposed the *Jane Doe protocol* [19] (a modified version of this protocol has been proposed by Goldberg, Mashatan, and Stinson in [21]). Earlier work includes Anderson et al.'s *Guy Fawkes protocol* [2], Mitchell's *Remote User Authentication protocol* [23],

Stajano and Anderson's *Resurrecting Duckling protocol* [27], and Weimerskirch and Westhoff's *zero-common-knowledge protocol* [28].

The *Jane Doe protocol* uses a hash chain to authenticate a pre-determined number of messages. For a randomly chosen a_0 and hash function h, the hash chain generated is by $a_1 := h(a_0), \ldots, a_n := h(a_{n-1})$. Similar to the *Jane Doe protocol*, Weimerskirch and Westhoff's *zero-common-knowledge protocol* (ZCK) uses a hash chain. Unfortunately, ZCK is flawed due to Eve's ability to use a denial of service attack along with a lack of recoverability in order to convince Bob that she is Alice.

The *Guy Fawkes protocol* uses a commitment to a string that consists of the hash of a triple in the form (codeword, message, [hash of next codeword]). The first codeword needs to be bootstrapped by some external mechanism providing authentication (digital signature or some user-aided mechanism, e.g. [16]). The protocol assumes that Bob can see this commitment hash before the triple is revealed by Alice. In our setting, Eve controls the flow of messages between Alice and Bob. Since the protocol does not include a provision for Alice to be sure that Bob received the commitment hash, Eve simply has to wait for Alice to reveal her codeword in order to impersonate her.

Building on the *Guy Fawkes protocol*, Mitchell's *Remote User Authentication protocol* uses a set of message authentication codes (MACs) of a random data string under different keys to authenticate a particular user (not a message). Due to the number and size of MACs used, this protocol can be expensive in terms of computation and storage. The security of the scheme depends on computational assumptions about the parameters. The number of times that this protocol can be used is limited because denial of service attacks may cause the reuse of keys during resynchronization and allow Eve to impersonate Alice.

Stajano and Anderson's *Resurrecting Duckling protocol* assumes that Alice and Bob can share an initial secret during what they refer to as the "imprinting phase". The solution proposed is physical contact between the two devices that Alice and Bob represent which may not always be feasible. As Eve is a passive observer during the *intialization* (or imprinting) phase, any information exchanged by Alice and Bob can be eavesdropped by Eve.

More recent and in the same line of research, Mashatan and Stinson's *new message recognition protocol for ad hoc pervasive networks* [20] provides a MRP of fixed size. The protocol uses a hash function to create commitment values to a current and future "password". However, as shown in [13], the resynchronization process rendered does not provide the recoverability intended, and in fact, enables an adversary to create selective forgeries.

There are not many impossibility results in cryptography, and those that exist are mostly for cryptographic primitives and certain proof methods. There are some results on the impossibility of using black-box methods for constructing one primitive from another one, e.g. collision-resistant hash functions from one-way permutations [26] or time-stamping schemes and collision-resistant hash functions from each other [8, 6, 7]. For somewhat larger systems, Backes et al. [3, 5] show that certain primitives cannot be implemented in the universally composable cryptographic library in a certain reasonable way.

Regarding protocols, there is a well-known result stating that a fair exchange protocol cannot be built without a trusted third party [29]. Impagliazzo's and Rudich's result [14] on the impossibility of establishment of a common secret over an authentic channel is maybe the closest to what we achieve in the current paper, but in some sense, it is the weakest of the ones listed here — it shows that if one manages to prove that secret agreement is possible assuming only that one-way permutations exist, then one has proved $\mathbf{P} \neq \mathbf{NP}$. Another result on the non-existence of a certain class of protocols is by Pereira and Quisquater [24] which shows that Diffie-Hellman based group key exchange protocols cannot be constructed if the parties are constrained to perform only exponentiations in the underlying group, and only elements of the group may be exchanged between parties.

3. PROTOCOLS AND EXECUTION

3.1 Messages

To be able to show the non-existence of a certain class of protocols, we have to specify what a protocol is. We are working in the *symbolic cryptography* (or *Dolev-Yao*) model [10]. Messages are modeled as elements of a term algebra, the operations possible with the messages are explicitly listed, and the adversary is bound to the same list.

Let $\mathbf{R}$ be a countable set of *formal nonces*, $\mathbf{C}$ a countable set of *formal constants*, and $\mathbf{P}$ a countable set of *formal payloads*. Let the sets $\mathbf{R}$, $\mathbf{C}$ and $\mathbf{P}$ be mutually disjoint. Let $\mathbf{A} = \mathbf{R} \cup \mathbf{C} \cup \mathbf{P}$. The set of formal *pre-messages* $\Sigma^\#$ is defined as the smallest set satisfying $\mathbf{A} \subseteq \Sigma^\#$, $h(m_1, \ldots, m_k) \in \Sigma^\#$ if $m_1, \ldots, m_k \in \Sigma^\#$, and $(m_1 \oplus m_2) \in \Sigma^\#$ if $m_1, m_2 \in \Sigma^\#$. We say that $h(m_1, \ldots, m_k)$ is the *formal hash* of messages $m_1, \ldots, m_k$ and $(m_1 \oplus m_2)$ is the *exclusive or* (XOR) of the messages m_1, m_2.

The set of *formal messages* Σ is defined as the factor set $\Sigma^\# / \equiv$ where $\equiv$ relates two messages that we want to consider equal because of the properties of $\oplus$. We assume there is a fixed element $0 \in \mathbf{C}$. The relation $\equiv$ is the least congruence (with respect to the operations h and $\oplus$) that contains $x \oplus y \equiv y \oplus x$, $x \oplus x \equiv 0$, $0 \oplus x \equiv x$ and $(x \oplus y) \oplus z \equiv x \oplus (y \oplus z)$ for all $x, y, z \in \Sigma^\#$. In the set Σ, we consider $\oplus$ to be a long operation, taking any number of arguments, because of the associativity imposed by $\equiv$.

We define the relation "is submessage of" (denoted $\sqsubseteq$) on messages. We define $m \sqsubseteq m$ for all messages m, and if $m' \sqsubseteq m$, then also $m' \sqsubseteq h(\ldots, m, \ldots)$ and $m' \sqsubseteq (\ldots \oplus m \oplus \ldots)$.

Given a set of messages $\mathbf{M}$, we say that m can be constructed from $\mathbf{M}$ (denoted $\mathbf{M} \vdash m$), if $m \in \mathbf{M}$, $m \in \mathbf{C}$ or $m = h(m_1, \ldots, m_k)$ or $m = m_1 \oplus \cdots \oplus m_k$ with $\mathbf{M} \vdash m_i$ for all i. Denote $\langle \mathbf{M} \rangle = \{m \in \Sigma \mid \mathbf{M} \vdash m\}$.

Two messages can be compared for equality, and given a message, it is possible to check whether it is a constant or a payload. We assume that a nonce cannot be told apart from a formal hash (or their XOR). Indeed, they both model "random-looking" bitstrings.

Remark. In our setting, tupling is not a message constructor. We have made this choice because of difficulties in combining tupling and XOR. The lack of tupling is handled by making hashing a long operation, and by allowing parties to send tuples of messages to each other.

3.1.1 Modeling Symmetric Cryptography

When using perfect cryptography to model protocols, one

usually understands certain sets of cryptographic primitives under the notions of "symmetric cryptography" or "asymmetric cryptography". Symmetric cryptography usually includes not only symmetric encryption and hash functions, but also message authentication codes, (pseudo)random functions, and permutations. It may also include XOR or other computationally simple operations with data. On the other hand, asymmetric cryptography contains primitives like public-key encryption and signing using operations like exponentiation (to model Diffie-Hellman key exchange).

In the current paper, we explicitly consider only hash functions and the XOR operation. Nevertheless, we claim that we are still handling most of "symmetric cryptography" because other primitives under this label can be constructed from hashes and XORs. For example, (randomized) symmetric encryption (which also provides integrity in the symbolic model) can be defined as $\{m\}_K^r = (r, h(K, h(r, K, m)) \oplus m, h(r, K, m))$ [15]. A pseudorandom function can be defined as $PRF_K(m) = h(K, m)$. A message authentication code can be defined exactly in the same way. A pseudorandom permutation can be constructed from a pseudorandom function by using the Feistel construction [11, Sec. 3.7.2].

3.2 Alice and Bob

The MRP proceeds in rounds, i.e. we assume a global clock. The construction of protocols is generally easier in the synchronous model, hence this assumption strengthens our impossibility result. During a round, Alice and Bob read the messages sent to them during the previous round (possibly modified by Eve), generate new messages, and send them to each other (possibly captured by Eve). At the beginning of a round, Alice may receive a *payload* that she must somehow transmit to Bob. In addition to sending messages, Bob may also choose to *accept* payloads.

Recall that the protocol had two phases. During the initialization phase, Eve is not active. The end of the initialization phase is denoted by Alice (this is w.l.o.g. as Alice and Bob can discuss when to start with the main phase). During the main phase, Eve gives Alice payloads and interferes with the communication between Alice and Bob. At some point, Eve may decide to become inactive again. When this happens, Alice and Bob will get no notification.

Formally, the protocol role for Alice is defined by the following components:

- The set of *internal states* $\mathbf{S}_A$ (possibly infinite) and the initial state $S_{A0} \in \mathbf{S}_A$ of Alice.
- The *transition function* δ_A, subject to certain conditions.

The arguments to the transition function are the following:

- the current state $S_A^\circ \in \mathbf{S}_A$;
- the current *message store*, $\mathcal{M}^\circ \in \Sigma^*$ (where X^* denotes the set of finite sequences of elements of the set X);
- the sequence of messages $\mathcal{M}_{A\leftarrow B} \in \Sigma^*$ received at the beginning of the current round, presumably from Bob;
- the payloads $\mathcal{M}_{\mathrm{pl}} \in \mathbf{P}^*$ that Alice received from Eve to be transmitted to Bob (possibly empty).

Alice's transition function outputs the following components:

- new internal state $S_A^\bullet \in \mathbf{S}_A$;
- new store of messages $\mathcal{M}^\bullet \in \Sigma^*$;
  - We demand that $\mathcal{M}^\bullet = \mathcal{M}^\circ \cdot \mathcal{M}_{\mathrm{pl}} \cdot \mathcal{M}_{A\leftarrow B} \cdot \mathcal{N}$, where $\mathcal{N} \in \mathbf{R}$ is the sequence of formal nonces generated by Alice in the current round.
- the sequence of messages $\mathcal{M}_{A\to B} \in \Sigma^*$ to be sent to Bob;
- a Boolean b_{m} indicating whether the main phase of the protocol should start (this component is ignored after the main phase has started).

Similarly, Bob's role is defined by its set of internal states $\mathbf{S}_B$, the initial state $S_{B0} \in \mathbf{S}_B$ and the transition function δ_B. The inputs and outputs of δ_B are the same as of δ_A, except that there is no input $\mathcal{M}_{\mathrm{pl}}$ nor output b_{m}, but there is an additional output $\mathcal{M}_{\mathrm{acc}} \in \mathbf{P}^*$ of payloads Bob has accepted during the current round.

Remark. We have defined Alice and Bob to behave deterministically. In the symbolic model, randomized behaviour is commonly modeled as non-determinism (*possibilism*). As authenticity and perenniality are trace properties (required to hold on each possible trace of the protocol) and Eve is also allowed to behave non-deterministically, Alice's and Bob's non-determinism will not help them to defeat Eve, because Eve can nondeterministically guess their choices.

The conditions on δ_A and δ_B are inspired by the formal meaning of epistemic modalities in authentication logics [1]. Similarly to those models, Alice and Bob can only act upon the information that they actually have. Given two message stores that look the same to Alice, her outputs cannot allow her to distinguish these two stores. Two sequences of messages $\mathcal{M}$ and $\mathcal{M}'$ are indistinguishable (denoted $\mathcal{M} \approx \mathcal{M}'$) if there is an isomorphism from $\langle\mathcal{M}\rangle$ to $\langle\mathcal{M}'\rangle$ mapping each element in the sequence $\mathcal{M}$ to the element at the same position in $\mathcal{M}'$. A bijective mapping φ on messages is isomorphism, if it is identity on formal constants, maps payloads to payloads and preserves the message structure given by h and $\oplus$. As formal hashes and nonces cannot be told apart, an isomorphism is allowed to map a nonces to hashes and *vice versa*.

Let $S^\circ \in \mathbf{S}_A$ and let $\mathcal{M}^\circ, \mathcal{M}^{\circ\prime}, \mathcal{M}_{A\leftarrow B}, \mathcal{M}'_{A\leftarrow B}, \mathcal{M}_{\mathrm{pl}}, \mathcal{M}'_{\mathrm{pl}}$ be sequences of messages. Let

$$(S^\bullet, \mathcal{M}^\bullet, \mathcal{M}_{A\to B}, b) = \delta_A(S^\circ, \mathcal{M}^\circ, \mathcal{M}_{A\leftarrow B}, \mathcal{M}_{\mathrm{pl}})$$
$$(S^{\bullet\prime}, \mathcal{M}^{\bullet\prime}, \mathcal{M}'_{A\to B}, b') = \delta_A(S^\circ, \mathcal{M}^{\circ\prime}, \mathcal{M}'_{A\leftarrow B}, \mathcal{M}'_{\mathrm{pl}}) \ .$$

If $|\mathcal{M}^\circ| = |\mathcal{M}^{\circ\prime}|$, $|\mathcal{M}_{A\leftarrow B}| = |\mathcal{M}'_{A\leftarrow B}|$, $|\mathcal{M}_{\mathrm{pl}}| = |\mathcal{M}'_{\mathrm{pl}}|$, and $\mathcal{M}^\circ \cdot \mathcal{M}_{\mathrm{pl}} \cdot \mathcal{M}_{A\leftarrow B} \approx \mathcal{M}^{\circ\prime} \cdot \mathcal{M}'_{\mathrm{pl}} \cdot \mathcal{M}'_{A\leftarrow B}$, where the indistinguishability is realized by the isomorphism φ° then the we must have $S^\bullet = S^{\bullet\prime}$; $b = b'$; $|\mathcal{M}^\bullet| = |\mathcal{M}^{\bullet\prime}|$; $|\mathcal{M}_{A\to B}| = |\mathcal{M}'_{A\to B}|$, and $\mathcal{M}^\bullet \cdot \mathcal{M}_{A\to B} \approx \mathcal{M}^{\bullet\prime} \cdot \mathcal{M}'_{A\to B}$ where the indistinguishability can be realized by some isomorphism $\varphi^\bullet$ that extends φ°.

Similar condition (indistinguishable inputs lead to indistinguishable outputs) must hold for δ_B. The isomorphism on inputs obviously does not include $\mathcal{M}_{\mathrm{pl}}$, but the isomorphism on outputs also has to include $\mathcal{M}_{\mathrm{acc}}$.

3.3 Global Setup

The *global state* $\mathcal{S}$ of the protocol (between the rounds) consists of the following components (or parts):

- the states S_A, S_B and message stores $\mathcal{M}_A$, $\mathcal{M}_B$ (initially empty) of Alice and Bob;

- the set of messages $\mathbf{M}_E$ that Eve has seen or generated;
- the Booleans b_{m} (initially false) and b_{a} (initially true) indicating whether the protocol execution is in the main phase, and whether Eve is active;
- the sequences of messages $\bar{\mathcal{M}}_{A\leftarrow B}$ and $\bar{\mathcal{M}}_{B\leftarrow A}$ that Alice and Bob are about to receive;
- the sequence $\mathcal{M}_{\mathrm{pl}}$ of payloads that Alice should transmit to Bob.

We say that global state $\mathcal{S}$ is transformed to $\mathcal{S}'$ in a single round and write $\mathcal{S} \to \mathcal{S}'$ if the following holds. Let

$$(S'_A, \mathcal{M}'_A, \mathcal{M}_{A\to B}, b) = \delta_A(S_A, \mathcal{M}_A, \bar{\mathcal{M}}_{A\leftarrow B}, \mathcal{M}_{\mathrm{pl}})$$
$$(S'_B, \mathcal{M}'_B, \mathcal{M}_{B\to A}, \mathcal{M}_{\mathrm{acc}}) = \delta_B(S_B, \mathcal{M}_B, \bar{\mathcal{M}}_{B\leftarrow A}) \qquad (1)$$

Then $S'_A, S'_B, \mathcal{M}'_A, \mathcal{M}'_B$ must be components of $\mathcal{S}'$. The other components of $\mathcal{S}'$ must satisfy the following conditions.

- If $b_{\mathrm{m}} \wedge b_{\mathrm{a}}$ then there must exist a finite set of nonces and payloads $\mathbf{N} \subset \mathbf{R} \cup \mathbf{P}$ not occurring in $\mathcal{S}$, $\mathcal{M}'_A$ and $\mathcal{M}'_B$, such that $\mathbf{M}'_E = \langle \mathbf{M}_E \cup \mathcal{M}_{A\to B} \cup \mathcal{M}_{B\to A} \cup \mathbf{N} \rangle$. Otherwise $\mathbf{M}'_E = \langle \mathbf{M}_E \cup \mathcal{M}_{A\to B} \cup \mathcal{M}_{B\to A} \rangle$.
- $b'_{\mathrm{m}} = b_{\mathrm{m}} \vee b$.
- If b_{a} is false then b'_{a} must be false.
- If $b_{\mathrm{m}} \wedge b_{\mathrm{a}}$ then the components of the sequences of messages $\bar{\mathcal{M}}'_{A\leftarrow B}$ and $\bar{\mathcal{M}}'_{B\leftarrow A}$ belong to $\mathbf{M}'_E$. Otherwise $\bar{\mathcal{M}}'_{A\leftarrow B} = \mathcal{M}_{B\to A}$ and $\bar{\mathcal{M}}'_{B\leftarrow A} = \mathcal{M}_{A\to B}$.
- If $b_{\mathrm{m}} \wedge b_{\mathrm{a}}$ then $\mathcal{M}'_{\mathrm{pl}}$ is a possibly empty sequence of payloads that belong to $\mathbf{M}'_E$. Otherwise $\mathcal{M}'_{\mathrm{pl}}$ is empty.

We see that Eve acts only if both flags b_{m} and b_{a} are set. In this case she non-deterministically selects the messages received by A and B. If Eve does not act then $\mathcal{S}'$ is uniquely determined by $\mathcal{S}$.

A *protocol trace* is an infinite sequence $\mathcal{S}_0 \to \mathcal{S}_1 \to \cdots$, such that $\mathcal{S}_0$ is the initial global state described above and for each i we have $\mathcal{S}_{i-1} \to \mathcal{S}_i$.

3.4 Security Properties

We say that Bob *accepts* payload M at the step $\mathcal{S} \to \mathcal{S}'$ if in the equation (1), the component $\mathcal{M}_{\mathrm{acc}}$ contains M. We say that Alice *initiates* the payload M in the state $\mathcal{S}$, if the component $\mathcal{M}_{\mathrm{pl}}$ of that state contains M.

We say that the MRP is **authentic** if the following holds for all of its traces $\mathcal{S}_0 \to \mathcal{S}_1 \to \cdots$. If Bob accepts a payload M at the step $\mathcal{S}_i \to \mathcal{S}_{i+1}$ then there exists $j \in \{1, \ldots, i\}$, such that Alice initiates M in the state $\mathcal{S}_j$.

We say that the MRP is **perennial** if the following holds for all of its traces $\mathcal{S}_0 \to \mathcal{S}_1 \to \cdots$. If Alice initiates the payload M in some state $\mathcal{S}_i$, and there exists a state $\mathcal{S}_k$, where b_{a} is false, then there exists some j, such that Bob accepts M at the step $\mathcal{S}_j \to \mathcal{S}_{j+1}$.

THEOREM 1. *There exist no authentic perennial MRPs.*

Obviously, the theorem applies to our selection of cryptographic primitives.

4. PROOF OF THE THEOREM

Due to space constraints, we will give only a sketch of the proof here. We refer to [12] for the full proof.

We give a constructive proof, describing how Eve should attack the protocol. We explain how Eve must construct the messages received by Alice and Bob. As explained in the previous section, Eve is non-deterministic, hence our descriptions serve to point out a trace where either the authenticity or perenniality is violated.

Schmidt et al. [25] have shown that using just hashing and XOR, Alice and Bob cannot establish a common secret. We show that if Alice and Bob do not share secrets, then during the main phase of the protocol, Eve can force Alice to deplete the means with which she can prove the authenticity of her messages to Bob.

Proof for Language without XOR.

Suppose that the initialization phase of the protocol has just ended — at the step $\mathcal{S}_{i-1} \to \mathcal{S}_i$, Alice decided that the main phase should start. Let $\mathbf{Z}^0$ be the set of all messages that Alice and Bob have sent during the initialization phase. Consider the knowledge $\mathbf{M}_E$ of Eve in the state $\mathcal{S}_i$. Let $\mathbf{Z} = \{m' \mid m \in \mathbf{Z}^0, m' \sqsubseteq m\} \backslash \mathbf{M}_E$, i.e. $\mathbf{Z}$ contains all submessages of sent messages that Eve does not know. As there are no shared secrets, each element of $\mathbf{Z}$ is known to exactly one of Alice and Bob. Let $\mathbf{Z} = \mathbf{Z}_A \dot\cup \mathbf{Z}_B$, where $\mathbf{Z}_A$ [resp. $\mathbf{Z}_B$] is the set of messages in $\mathbf{Z}$ known only to Alice [resp. Bob].

W.l.o.g., we partition the set of formal nonces $\mathbf{R}$ into three countable sets $\mathbf{R}_A$, $\mathbf{R}_B$ and $\mathbf{R}_E$ and assume that whenever Alice, Bob, or Eve generates a new nonce, it comes from the respective set. Let $\mathbf{Y}_A = \mathbf{Z}_A \cup \mathbf{R}_A$ and $\mathbf{Y}_B = \mathbf{Z}_B \cup \mathbf{R}_B$. We now define mappings tr_A and tr_B from messages to messages as follows:

$$tr_A(m) = \begin{cases} m, & m \in \mathbf{Z}^0 \cup \mathbf{C} \\ \square^m, & m \in \mathbf{Y}_A \\ m', & m = \square^{m'}, m' \in \mathbf{Y}_B \\ h(tr_A(m_1), \ldots, tr_A(m_k)), & m = h(m_1, \ldots, m_k) \end{cases}$$

$$tr_B(m) = \begin{cases} m, & m \in \mathbf{Z}^0 \cup \mathbf{C} \\ \square^m, & m \in \mathbf{Y}_B \\ m', & m = \square^{m'}, m' \in \mathbf{Y}_A \\ h(tr_B(m_1), \ldots, tr_B(m_k)), & m = h(m_1, \ldots, m_k), \end{cases}$$

where the different cases have to be considered from top to bottom. Here $\square^m \in \mathbf{R}_E$ is a new nonce that Eve constructs the first time that she needs to consider the second case for the message m. Additionally, we state that tr_A is a permutation on payloads (but do not specify which one). The mapping tr_B is also a permutation on payloads and it is equal to the inverse of tr_A.

In the main phase of the protocol run, as long as Alice and Bob do not send each other the messages in $\mathbf{Z}$, the attack mounted by Eve consists of replacing all messages m sent by Alice with $tr_A(m)$, and all messages m sent by Bob with $tr_B(m)$. We explain below what happens if some message from the set $\mathbf{Z}$ is sent.

LEMMA 1. *Eve is capable of replacing all messages $m \notin \mathbf{Z}$ sent by Alice with $tr_A(m)$, and all messages sent by Bob with $tr_B(m)$.*

We show that Alice and Bob do not notice Eve replacing the exchanged messages m with $tr_A(m)$ or $tr_B(m)$. Let $\mathcal{S}^\circ$ and $\mathcal{S}^{\circ\prime}$ be two global states. Let $\mathbf{Z}^0$ be a set of messages that Alice, Bob, and Eve all know in $\mathcal{S}^\circ$ and $\mathcal{S}^{\circ\prime}$. Also, let each of the messages in $\mathbf{Z}^0$ appear in the message store of either Alice or Bob as a message from the other party.

Let $\mathbf{Z}$ be the set of submessages of $\mathbf{Z}^0$ unknown to Eve and known to exactly one of Alice and Bob. The sets $\mathbf{Z}^0$ and $\mathbf{Z}$ must look like the sets of messages and their submessages of an initial segment of a conversation between Alice and Bob. That is, there must exist an order on $\mathbf{Z}^0$ such that each message in $\mathbf{Z}^0$ can be constructed from previous messages of $\mathbf{Z}^0$, from the nonces in $\mathbf{Z}$, and from the nonces in $\mathbf{R}_E$.

Define tr_A and tr_B as above. Let the states be *isomorphic* (denoted $\mathcal{S} \cong \mathcal{S}'$), meaning that

- The internal states of Alice and Bob are the same in $\mathcal{S}^\circ$ and $\mathcal{S}^{\circ\prime}$;
- $\mathcal{M}^\circ \cdot \mathcal{M}_{\mathrm{pl}} \cdot \mathcal{M}_{A\leftarrow B} \approx \mathcal{M}^{\circ\prime} \cdot \mathcal{M}'_{\mathrm{pl}} \cdot \mathcal{M}'_{A\leftarrow B}$, where the isomorphism φ_A is the following:
  - $\varphi_A(x) = x$ if $x \in \mathbf{R}_A$ or $x \in \mathbf{P}$,
  - $\varphi_A(m) = tr_B(m)$ if m is a message received from Bob
    - in particular, $\varphi_A(m) = m$ for all $m \in \mathbf{Z}^0$

  (recall that message stores of Alice consist of nonces generated by her, payloads, and messages received from the network);
- the message stores of Bob must be isomorphic too, where the isomorphism φ_B is identity on nonces Bob has generated, and equals tr_A on messages received from Alice.

Let $\mathcal{S}^\circ \to \mathcal{S}^\bullet$, where the step corresponds to Eve not interfering with the messages Alice and Bob are sending to each other. Also let $\mathcal{S}^{\circ\prime} \to \mathcal{S}^{\bullet\prime}$ where the step corresponds to Eve applying tr_A to the messages Alice is sending, and tr_B to the messages Bob is sending, before forwarding them to the other party. Let $P[\,]$ denote a *message context* (a message with holes) and let $P[x_1, \ldots, x_n]$ denote the message where the holes of P have been filled with messages $x_1, \ldots, x_n$.

LEMMA 2. *Let the sets $\mathbf{Z}$ and $\mathbf{Z}^0$ be as defined above. Let $\mathcal{M}$ be a message store of Alice. Let φ be a mapping from $\mathcal{M}$ to the set of all messages Σ defined as follows: $\varphi(x) = x$ if $x \in \mathbf{R}_A$ or $x \in \mathbf{P}$, and $\varphi(x) = tr_B(x)$ otherwise. Let y be a message that satisfies the following:*

- *$y \notin \mathbf{Z}$.*
- *If $r \in \mathbf{Y}_A$ and $r \sqsubseteq y$, then exists $z \in \mathbf{Z}^0$, such that $r \sqsubseteq z \sqsubseteq y$. Such z exists for each occurrence of r in y.*

Let $P[\overrightarrow{x}] = y$ for a certain message context P and messages $\overrightarrow{x}$ in $\mathcal{M}$. Then $P[\overrightarrow{\varphi(x)}] = tr_B(y)$.

LEMMA 3. *If the messages sent by Alice and Bob in $\mathcal{S}^\circ$ and $\mathcal{S}^{\circ\prime}$ do not contain elements of $\mathbf{Z}$, then in states $\mathcal{S}^\bullet$ and $\mathcal{S}^{\bullet\prime}$, the messages in the set $\mathbf{Z}$ are still known by exactly one of Alice and Bob. Furthermore, $\mathcal{S}^\bullet$ and $\mathcal{S}^{\bullet\prime}$ are isomorphic, and the isomorphism between messages is related to tr_A and tr_B in the same way as for $\mathcal{S}^\circ$ and $\mathcal{S}^{\circ\prime}$.*

Lemma 3 shows that as long as Alice and Bob do not send elements of $\mathbf{Z}$ to each other, Eve is able to simulate them to each other. Indeed, Eve knows from the description of the protocol which messages Alice and Bob are going to send to each other — which message context they are applying to their message stores. Although Eve does not necessarily know the message m Alice is sending to Bob, she is capable of constructing the message $tr_A(m)$.

If (say) Alice sends to Bob a tuple of messages $(m_1, \ldots, m_k)$ where $m_i \in \mathbf{Z}$, then Eve redefines the sets $\mathbf{Z}$ and $\mathbf{Z}^0$, by moving from $\mathbf{Z}$ to $\mathbf{Z}^0$ the message m_i and any other elements of $\mathbf{Z}$ she is now capable of computing. In this way, the mappings tr_A and tr_B are also redefined. Eve now continues as before: applies tr_A to all messages sent by Alice and tr_B to all messages sent by Bob and forwards them to Bob and Alice, respectively. Of course, Bob now notices that Eve is performing an active attack. If Bob had also sent messages belonging to $\mathbf{Z}$, then Alice would have noticed it too.

If the following steps of Alice and Bob do not involve sending messages in the now smaller set $\mathbf{Z}$ to each other, then lemma 3 is again applicable — Eve can simulate Alice to Bob and Bob to Alice. We have that in order to have authenticity of messages, it is necessary for Alice and Bob to use up messages in $\mathbf{Z}$. Eventually, the set $\mathbf{Z}$ will become empty and no more authentic communication is possible.

Proof for the Full Language.

The definition of the set $\mathbf{Z}$ is complicated by $\oplus$-operations. For a set of messages $\mathbf{M}$, define its *linear hull* as $\langle\langle \mathbf{M} \rangle\rangle = \{m_1 \oplus \cdots \oplus m_k \,|\, m_1, \ldots, m_k \in \mathbf{M}\}$. Let $\mathbf{W}^0$ be the set of all messages that Alice and Bob have sent during the initialization phase. Let $\mathbf{W}$ be the set containing $\mathbf{W}^0$, as well as all submessages of messages in $\mathbf{W}^0$. Let $\mathbf{Z}^0$ contain all messages in $\langle\langle \mathbf{W} \rangle\rangle$ that are known to Eve at the end of the initialization phase. Let $\mathbf{Z} = \langle\langle \mathbf{W} \rangle\rangle \backslash \mathbf{Z}^0$. As before, $\mathbf{Z}_A \subseteq \mathbf{Z}$ is the set of messages in $\mathbf{Z}$ known only to Alice, and $\mathbf{Z}_B = \mathbf{Z} \backslash \mathbf{Z}_A$ is the set of messages in $\mathbf{Z}$ known only to Bob. As before, let $\mathbf{Y}_A = \mathbf{Z}_A \cup \mathbf{R}_A$ and $\mathbf{Y}_B = \mathbf{Z}_B \cup \mathbf{R}_B$. We now extend $tr_A(m)$ and $tr_B(m)$ as follows:

$$tr_A(m) = \begin{cases} \ldots \\ tr_A(m_1) \oplus \cdots \oplus tr_A(m_k), & m = m_1 \oplus \cdots \oplus m_k \end{cases}$$

$$tr_B(m) = \begin{cases} \ldots \\ tr_B(m_1) \oplus \cdots \oplus tr_B(m_k), & m = m_1 \oplus \cdots \oplus m_k \end{cases} .$$

Eve performs the attack by replacing messages m sent by Alice with $tr_A(m)$ and messages m sent by Bob with $tr_B(m)$, *as long as it is possible*. Without XOR, the last condition was just "messages do not contain elements from $\mathbf{Z}$". Now it is "the messages in $\mathbf{Z}^0$, together with the messages sent by Alice and Bob during the main phase do not allow Eve to find any message in $\mathbf{Z}$". If the replacement is no longer possible, then Eve has learned an element of $\mathbf{Z}$, decreasing its size.

The proof of the validity of such attack is based on the extensions of three lemmas before. Of those, only Lemma 2 becomes significantly more complex. It is now stated as follows.

LEMMA 2'. *Let $\mathbf{Z}$, $\mathbf{Z}^0$ and tr_B be defined as above. Let $\mathcal{M}$ be a message store of Alice. Let φ be a mapping on messages defined as in Lemma 2. Let y be a message satisfying the following:*

- *From y, messages in $\mathbf{Z}^0$, and messages received from Bob (in $\mathcal{M}$), it is impossible to derive any message in $\mathbf{Z}$.*
- *Adding y to the knowledge of Alice does not allow her to compute any more messages in $\mathbf{Z}$ compared to what she can compute just from $\mathcal{M}$.*

- *Second condition in Lemma 2: If $r \in \mathbf{Y}_A$ and $r \sqsubseteq y$, then exists $z \in \mathbf{Z}^0$, such that $r \sqsubseteq z \sqsubseteq y$. Such z exists for each occurrence of r in y.*

Let $P[\overrightarrow{x}] = y$ for a certain message context P and messages $\overrightarrow{x}$ in $\mathcal{M}$. Then $P[\overrightarrow{\varphi(x)}] = tr_B(y)$.

5. CONCLUSIONS

With advances in hardware, asymmetric cryptography is fast becoming a viable option for small devices [9, 18]. Nevertheless, we believe that there will always exist devices, ever smaller, with computational capabilities similar to the least powerful devices of today. Our results show that for these devices, certain forms of authentication are impossible.

We have shown that for a certain set of cryptographic primitives, the perennial authentication is impossible. An interesting future work, complementing [25] would be the determination of necessary and/or sufficient properties on symbolic cryptographic primitives for the possibility of authentication.

Our result has been established in the symbolic setting. Interestingly, it does *not* hold in the computational setting where signature schemes can be constructed from symmetric encryption [22] and one-way hash functions. This points out a gap between the two models, which according to our knowledge has not been recognized before. It would be interesting to study the gap and find out methods to reduce it, thereby finding symbolic model that better captures the essentials of cryptography. Regarding Merkle's construction, one of its main tools is decomposing messages to their constituent bits. The introduction of bits to the symbolic model is known to be very difficult [17].

Perenniality is a *liveness property*. So far, liveness properties have not received much attention for cryptographic protocols, except for protocols devised for certain narrowly defined tasks (e.g. fair exchange). In the computational setting even the existing definitions of liveness [4] may need to be significantly adapted.

6. ACKNOWLEDGMENTS

This research was supported by the European Regional Development Fund through the Estonian Center of Excellence in Computer Science, EXCS, and by the Estonian Science Foundation grant #8124.

7. REFERENCES

[1] M. Abadi and M. R. Tuttle. A Semantics for a Logic of Authentication (Extended Abstract). In *PODC*, pages 201–216, 1991.

[2] R. Anderson, F. Bergadano, B. Crispo, J.-H. Lee, C. Manifavas, and R. Needham. A New Family of Authentication Protocols. *Operating Systems Review*, 32(4):9–20, 1998.

[3] M. Backes and B. Pfitzmann. Limits of the Cryptographic Realization of Dolev-Yao-Style XOR. In *ESORICS 2005* (LNCS 3679), pages 178–196. Springer, 2005.

[4] M. Backes, B. Pfitzmann, M. Steiner, and M. Waidner. Polynomial fairness and liveness. In *CSFW*, pages 160–174. IEEE Computer Society, 2002.

[5] M. Backes, B. Pfitzmann, and M. Waidner. Limits of the BRSIM/UC Soundness of Dolev-Yao Models with Hashes. In *ESORICS 2006* (LNCS 4189). pages 404–423, Springer, 2006.

[6] A. Buldas and A. Jürgenson. Does Secure Time-Stamping Imply Collision-Free Hash Functions? In *ProvSec* (LNCS 4784), pages 138–150. Springer, 2007.

[7] A. Buldas and M. Niitsoo. Can We Construct Unbounded Time-Stamping Schemes from Collision-Free Hash Functions? In *ProvSec* (LNCS 5324), pages 254–267. Springer, 2008.

[8] A. Buldas and M. Saarepera. On Provably Secure Time-Stamping Schemes. In *ASIACRYPT* (LNCS 3329), pages 500–514. Springer, 2004.

[9] W. R. Claycomb, R. Lopes, D. Shin, and B. Kim. Key Establishment Using Group Information for Wireless Sensor Networks. In *Sensor Systems and Software* (LNICST 24), pages 51–65. Springer, 2010.

[10] D. Dolev and A. C.-C. Yao. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.

[11] O. Goldreich. *Foundations of Cryptography, Volume I - Basic Techniques*. Cambridge University Press, 2001.

[12] M. González Muñiz and P. Laud. On the (im)possibility of perennial message recognition protocols without public-key cryptography. Technical Report T-4-12, Cybernetica AS, 2010.

[13] M. González Muñiz and R. Steinwandt. Cryptanalysis of a Message Recognition Protocol by Mashatan and Stinson. In *ICISC '09: 12th International Conference on Information Security and Cryptology*, 2009.

[14] R. Impagliazzo and S. Rudich. Limits on the Provable Consequences of One-Way Permutations. In *STOC '89*, pages 44–61, New York, NY, USA, 1989. ACM.

[15] P. Laud. Implementing Cryptographic Primitives in the Symbolic Model. Submitted, 2010.

[16] S. Laur and S. Pasini. User-Aided Data Authentication. *International Journal of Security and Networks*, 4(1/2):69–86, 2009.

[17] P. Lincoln, J. C. Mitchell, M. Mitchell, and A. Scedrov. A probabilistic poly-time framework for protocol analysis. In *ACM Conference on Computer and Communications Security*, pages 112–121, 1998.

[18] A. Liu and P. Ning. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. In *IPSN '08: Proceedings of the 7th International Conference on Information Processing in Sensor Networks*, pages 245–256. IEEE Computer Society, 2008.

[19] S. Lucks, E. Zenner, A. Weimerskirch, and D. Westhoff. Concrete Security for Entity Recognition: The Jane Doe Protocol. In *INDOCRYPT 2008* (LNCS 5365), pages 158–171. Springer-Verlag, 2008.

[20] A. Mashatan and D. R. Stinson. A New Message Recognition Protocol for Ad Hoc Pervasive Networks. In *Cryptology and Network Security, 7th International Conference, CANS 2008* (LNCS 5339), pages 378–394. Springer, 2008.

[21] A. Mashatan, D. R. Stinson, and I. Goldberg. A New Message Recognition Protocol with Self-recoverability for Ad Hoc Pervasive Networks. In *Applied Cryptography and Network Security* (LNCS 5536), pages 219–237. Springer, 2009.

[22] R. C. Merkle. A Digital Signature Based on a Conventional Encryption Function. In *CRYPTO* (LNCS 293), pages 369–378. Springer, 1987.

[23] C. J. Mitchell. Remote User Authentication Using Public Information. In *Cryptography and Coding, 9th IMA International Conference* (LNCS 2398), pages 360–369. Springer-Verlag, 2003.

[24] O. Pereira and J.-J. Quisquater. On the Impossibility of Building Secure Cliques-Type Authenticated Group Key Agreement Protocols. *Journal of Computer Security*, 14(2):197–246, 2006.

[25] B. Schmidt, P. Schaller, and D. Basin. Impossibility Results for Secret Establishment. In *CSF*, pages 261–273. IEEE Computer Society, 2010.

[26] D. R. Simon. Finding Collisions on a One-Way Street: Can Secure Hash Functions Be Based on General Assumptions? In *EUROCRYPT* (LNCS 1403), pages 334–345. Springer, 1998.

[27] F. Stajano and R. Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Security Protocols, 7th International Workshop* (LNCS 1796), pages 172–182. Springer, 2000.

[28] A. Weimerskirch and D. Westhoff. Zero Common-Knowledge Authentication for Pervasive Networks. In *Selected Areas in Cryptography, 10th Annual International Workshop, SAC 2003* (LNCS 3006), pages 73–87. Springer, 2004.

[29] J. Zhou and D. Gollmann. A Fair Non-repudiation Protocol. In *IEEE Symposium on Security and Privacy*, pages 55–61. IEEE Computer Society, 1996.