Practical Unconditionally Secure Two-channel Message Authentication

In Honour of Spyros Magliveras' 70th Birthday

Atefeh Mashatan
The Security and Cryptography Laboratory
EPFL
CH-1015 Lausanne, Switzerland
atefeh.mashatan@epfl.ch

Douglas R. Stinson*
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
dstinson@uwaterloo.ca

December 8, 2009

Abstract

We investigate unconditional security for message authentication protocols that are designed using two-channel cryptography. (Two-channel cryptography employs a broadband, insecure wireless channel and an authenticated, narrow-band manual channel at the same time.) We study both noninteractive message authentication protocols (NIMAPs) and interactive message authentication protocols (IMAPs) in this setting.

First, we provide a new proof of nonexistence of nontrivial unconditionally secure NIMAPs. This proof consists of a combinatorial counting argument and is much shorter than the previous proof by Wang and Safavi-Naini, which was based on probability distribution arguments. We also prove a new result which holds in a weakened attack model.

Further, we propose a generalization of an unconditionally secure 3-round IMAP due to Naor, Segev and Smith. The IMAP is based on two ϵ-Δ universal hash families. With a careful choice of parameters, our scheme improves that of Naor *et al.* Our scheme is very close to optimal for most parameter situations of practical interest. Finally, a variation of the 3-round IMAP is presented, in which only one hash family is required.

1 Introduction

In this paper, we focus on using two-channel cryptography to design unconditionally secure message authentication protocols suitable for networks consisting of devices with limited resources. In particular, we look at noninteractive message authentication protocols (NIMAPs) and interactive

*Research supported by NSERC discovery grant 203114-06

message authentication protocols (IMAPs). Previous protocols and proofs are reviewed and some are improved.

Standard models of public-key cryptography and secret-key cryptography have addressed the problem of message authentication by means of assuming availability of public-key infrastructures or secure channels. In some scenarios, however, assuming the traditional settings of public-key and secret-key cryptography might not be practical and, indeed, using these techniques may be very costly. Mobile ad hoc networks (MANET), wireless sensor networks (WSN), and pervasive networks in general are examples of scenarios in which traditional cryptographic protocols may not be suitable, or not even possible, to implement.

In search of a solution to this problem, researchers realized that when the devices come in close geographic proximity of each other, it is possible to make use of a *manual channel*, as well as the usual wireless channel. Instances of the manual channel are typically more expensive to operate compared to the wireless channel. However, they provide some level of security. For example, the channel may provide authenticity of short messages, but may not be confidential. The aim is to employ a (broadband and insecure) wireless channel and a (somewhat secure and narrow-band) manual channel at the same time and attain a security objective, message authentication for instance. This motivated the term *two-channel cryptography*. In 1984, Rivest and Shamir [22] first proposed incorporating human participation in authentication protocols. However, this idea did not receive serious attention from researchers until very recently.

1.1 Communication Model of Two-channel Cryptography

We first describe the communication model of two-channel cryptography, where it is assumed that two channels are accessible for communication: an *insecure broadband channel*, denoted by "$\rightarrow$", and an *authenticated narrow-band channel*, denoted by "$\Rightarrow$". Communication over the authenticated channel is usually more expensive and less convenient. Hence, the messages sent over the authenticated channel are usually much shorter than those sent over the insecure channel. The goal of two-channel cryptography is, then, to achieve a certain cryptographic objective by means of the two channels, while optimizing the cost.

An insecure wireless channel is an example of the broadband channel. The narrow-band channel is usually used to send a short string. Instances of the narrow-band channel include voice-over-internet-protocol (VoIP), data imprinting or data comparison by a user, near field communication (NFC), infrared (IR), laser, or visible light between two devices. For a recent usability study of various types of authenticated channels, see [9].

The following are common assumptions on what an adversary can and cannot do in two-channel cryptography.

- The adversary has full control over the broadband channel. That is, the adversary can listen to any messages sent over the broadband channel, modify the messages sent via this channel, stall a message from being delivered, and insert a new message into this channel at any time.
- On the other hand, we assume that the adversary's control over the authenticated channel is limited. In particular, the adversary cannot modify the information transmitted over the authenticated channel, i.e., data integrity is ensured in this channel. Some works have allowed the adversary to "store" an authenticated flow from one session and replay it in another session. In this paper, however, we only consider "one-session" attacks where the adversary does not alter any flow over an authenticated channel.

Moreover, the authenticated channel is equipped with user authenticating features such that the recipient of the information can be sure about who sent it. In other words, an adversary cannot initiate a flow over this channel. On the other hand, the adversary is able to replay a previous flow sent through this channel. However, replaying a previous flow sent by Alice to Bob is not going to help Eve, when she wants to deceive another party, Charlie. That is, when Bob receives an authenticated flow, he can check if he was the intended recipient or not.

1.2 Two-channel Cryptography Applications

Two-channel cryptography techniques have several applications, especially in constrained environments where secure channels or trusted infrastructures do not exist or are very costly to provide. Moreover, these techniques are useful in networks that are composed of constrained devices which cannot handle heavy computations such as public-key computations.

With new technological advancements in miniaturizing devices and the emerging smart homes and buildings projects [2], the problem of designing light-weight cryptographic protocols for low-end devices has attracted a lot of attention both in the academic community and in industry. In scenarios such as personal area networks (PAN) [6] and telemedicine (remote health care where medical personnel can monitor the patients from a distance) [3], where the devices are naturally attended by users, the idea of employing the manual channel is even more appealing. This approach is especially attractive when it enables researchers to design more cost-efficient and easy-to-implement protocols.

Another important application is disaster recovery, when a trusted infrastructure is compromised. The use of two-channel cryptography allows for temporary, yet speedy, relief before the infrastructure is fully recovered. Full recovery usually takes a lot longer and security providers need to be vigilant in the meantime.

1.3 Message Authentication in Ad hoc Networks

The problem of authentication is an important aspect of secure communication. Typically, communicating parties would like to be assured of the authenticity of information they obtain via potentially insecure channels.

An ad hoc network is a network where some of the users are part of the network only for a short period of time. Typically, users may join or leave the network at will. For practical reasons, it should be possible to quickly add new users to an ad hoc network. In this network, like any other network, it is desirable to have message authentication so that users may be confident that information they receive has not been tampered with. However, assuming traditional settings for cryptographic tools might not be practical. For example, a public-key infrastructure may not exist, in which case digital signatures cannot be employed. Secondly, secure channels might not be present, so secret keys cannot be exchanged between parties. Finally, communication bandwidth may be severely limited, which means that protocols must be very careful to limit the amount of information transmitted by users in the network.

As an example, consider the following scenario presented by Balfanz *et al* [1] which motives this setting: a traveller in an airport lounge would like to print a sensitive document from his or her laptop to one of the many printers set up in the airport lounge. The lounge does not have a secure universal naming infrastructure for the printers. The traveller wants to choose a particular printer and make sure the document gets printed by *that* particular printer (and no other printer), using

the insecure wireless channel. The traveller's laptop and a printer need to be securely introduced while there is no public-key infrastructure or secure channel available. This is also known as the *pairing problem* [24].

In order to overcome these difficulties in an ad hoc network and still be able to provide message authentication, one can employ two-channel cryptographic techniques when designing protocols.

1.4 Attack Model

We focus on message authentication protocols which deploy both narrow-band and broadband channels between a claimant Alice and a verifier Bob. In the normal operation of the protocol, Alice chooses a message $M \in \mathcal{M}$, where $\mathcal{M}$ denotes the space of all acceptable messages, and sends it to Bob using a NIMAP or an IMAP. At the end of the protocol, Bob either outputs (Alice, M'), where $M' \in \mathcal{M}$, or he rejects. In the absence of an active adversary, denoted as Eve, the message M sent from Alice should be recovered by Bob, making him accept and output (Alice, M). (For example, this message M could be the hash of a shared Diffie-Hellman key that is going to be used for further communication.) Eve's goal is to make Bob accept a message M' along with the identity of Alice, when Alice has never sent M'.

The attack model makes the following assumptions. Eve gives a message M to Alice. Then Alice will use the protocol to attempt to send M to Bob. Eve can observe all the flows sent during the protocol, and she can change the information sent in any flow that does not take place over the authenticated channel. Her goal is to make Bob accept a message $M' \neq M$, along with the identity of Alice

1.5 Interactive versus Noninteractive Protocols

A message authentication protocol may or may not require online interaction with Bob. There are numerous noninteractive as well as interactive message authentication protocols that have been considered in the literature. Noninteractive protocols have been proposed in Balfanz *et al* [1]; Pasini and Vaudenay [19]; Mashatan and Stinson [14]; and Reyhanitabar *et al* [21]. Interactive protocols have been discussed in many papers, including the following: the so-called MANA protocols were introduced in Gehrmann *et al* [5] and Gehrmann and Nyberg [6]; Hoepman [8]; the SAS protocol proposed by Vaudenay [27]; Pasini and Vaudenay [20]; Laur and Nyberg [11]; Laur and Pasini [12, 13]; and Mashatan and Stinson [15]. Group protocols are studied in Nguyen and Roscoe [18].

In a NIMAP, all flows are initiated by Alice. She sends some information over the broadband channel and some information over the narrow-band channel. Since there is no flow being initiated by Bob, the order in which Alice's flows are sent is irrelevant. As a result, we can combine all flows sent over the broadband channel into one single flow and, similarly, we can combine all flows sent over the narrow-band channel into one single flow. Hence, without loss of generality, we obtain a typical flow structure of a NIMAP as depicted in Fig. 1.

On the other hand, the flow structure of an IMAP can be more complicated. There is at least one flow initiated by Bob and, hence, the order in which flows are initiated matters. There may be more than one narrow-band flow. The authenticated channel may be bidirectional which means Bob can initiate a flow over the narrow-band channel as well. Illustrated in Fig. 2 is a possible flow structure of an IMAP. In this particular flow structure, the first flow is initiated by Alice on the broadband channel which is followed by a response from Bob on the same channel. Then, Alice

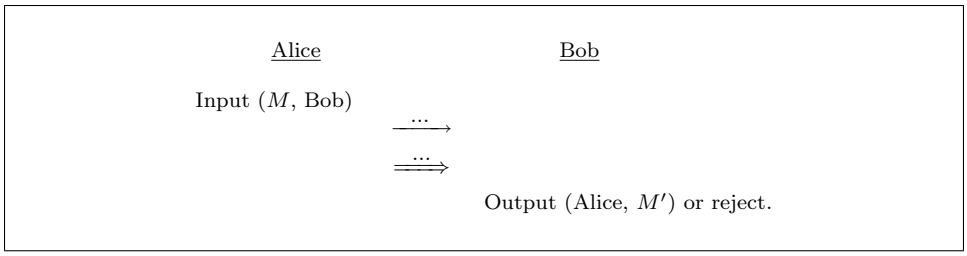

Figure 1: A Schematic NIMAP

sends one more flow over the broadband channel and her authenticated flow over the narrow-band channel.

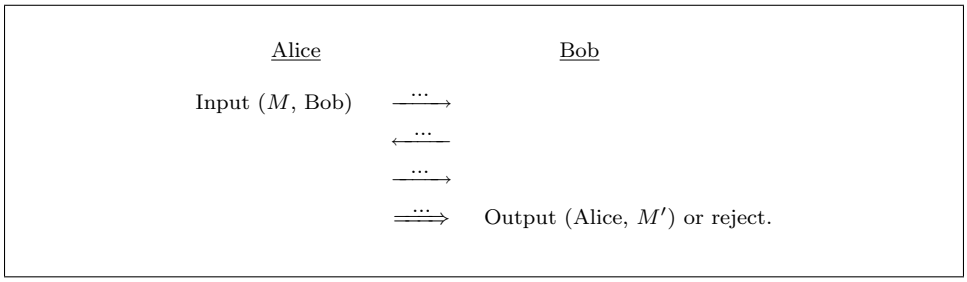

Figure 2: A Sample Schematic IMAP

NIMAPs are particularly interesting because they do not require the verifier to be online. On the other hand, interaction sometimes allows for more efficient protocols. Furthermore, some objectives may not be achievable in the noninteractive setting, but can be realized in an interactive setting.

1.6 Computational versus Unconditional Security

In the unconditional security setting, the adversary is assumed to have unlimited computational resources. In the computational security setting, on the other hand, the computational power of the adversary is bounded (typically, it is assumed to be polynomial-time, as a function of a certain security parameter). In order for a protocol to be considered computationally secure, the best currently-known methods to defeat a system or protocol should exceed the computational resources of the adversary by a comfortable margin. In the case of computationally secure NIMAPs or IMAPs, a successful adversary is reduced (in the sense of a Turing reduction) to an attacker against a well-known system or problem which is proven, or widely believed, to be secure. In the case of unconditionally secure NIMAPs or IMAPs, the adversary is permitted to use as much computation time as necessary in order to try to break the protocol.

1.7 Contributions of this Paper

First, we provide a new proof of nonexistence of nontrivial unconditionally secure NIMAPs. This proof consists of a combinatorial counting argument and is much shorter than the previous proof by Wang and Safavi-Naini[28], which was based on probability distribution arguments. We also prove a new result which holds in a weakened attack model.

Further, we propose a generalization of an unconditionally secure 3-round IMAP due to Naor, Segev and Smith [16, 17]. The IMAP is based on two ϵ-Δ universal hash families. With a careful choice of parameters, our scheme improves that of Naor *et al.* For most parameter situations of practical interest, our scheme requires an authenticated tag that is only 10 bits longer than the theoretical minimum proven in [16, 17]. Finally, a variation of the 3-round IMAP is presented, in which only one hash family is required.

2 On Unconditionally Secure NIMAPs

In the study of unconditionally secure NIMAPs, we assume the existence of adversaries who have access to unbounded amounts of time and resources. In this section, we show that the only NIMAPs which are secure in the presence of such unbounded adversaries are trivial protocols. In other words, the entire message has to be sent over the authenticated channel in order for a NIMAP to be unconditionally secure, and, therefore, nontrivial unconditionally secure NIMAPs do not exist. This result was first proved by Wang and Safavi-Naini [28] using probability distribution arguments. We provide a new proof in the form of a simple counting argument that can be viewed as an application of the pigeon-hole principle.

2.1 Wang and Safavi-Naini's Proof

Wang and Safavi-Naini [28] first showed the impossibility of designing nontrivial unconditionally secure NIMAPs. They used the following model to describe the unconditionally secure NIMAP:

The information theoretic NIMAP model: The sender S (Alice) sends the message M and a value r over the insecure public channel, and a tag s over the manual channel. The receiver R (Bob) decides whether or not to accept M as authentic from S.

Wang and Safavi-Naini showed that unconditionally secure NIMAPs do not exist without prior shared secrets between the sender and receiver, and without requirements such as stall-free on the narrow-band channel[1], unless the whole message is transmitted over the narrow-band channel. This results in a trivial protocol where the authenticated channel has enough bandwidth to transmit the whole message.

They suppose $|M| > |s|$ and propose an attack. First, they show that there definitely exists some other message M' such that M' can be authenticated under some r', possibly different from r, and the same tag s. Now, the adversary, on observing the authentication transcripts (M, r, s), replaces M and r with M' and r'. They further note that the adversary can mount this attack online by removing M and r from the broadband channel and delaying s on the narrow-band channel until she finds an appropriate M' and r'. Then, she sends M' and r' over the broadband channel and let s be transmitted over the narrow-band channel right after. In order to formally prove the effectiveness of their attack, for example when proving the existence of appropriate M' and r', they use probability distribution arguments involving Shannon entropies.

[1] In a stall-free channel, once a message is sent, it is either received by the recipient right away or it is never received.

2.2 A Simple Counting Argument

We now present a much shorter and simpler proof of nonexistence of nontrivial NIMAPs. Our proof is based on a counting argument.

We use the same model used by Wang and Safavi-Naini [28] and define $\mathcal{M}$ to be the set of all possible messages to be authenticated and $\mathcal{R}$ to be the set of all possible strings that could be sent on the first flow along with a possible message. Moreover, we let $\mathcal{S}$ be the set of all authenticating tags that are sent over the authenticated channel. An instance of a NIMAP in this model is as follows. A message $M \in \mathcal{M}$ is to be authenticated and it is sent over the broadband channel along with some information $r \in \mathcal{R}$. Later, an authenticating tag $s \in \mathcal{S}$ is sent over the narrow-band channel. Figure 3 depicts this NIMAP.

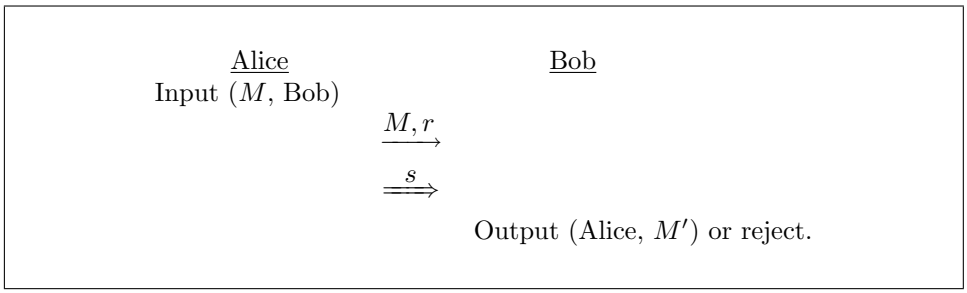

Figure 3: A General NIMAP

Let $\mathcal{V}$ be the set of all transcripts which result in Bob accepting a message, that is

$$\mathcal{V} = \{(M, r, s) : \text{ Bob accepts the triple } (M, r, s)\}.$$

Note that $\mathcal{V}$ is public knowledge and a computationally unbounded adversary can find or store $\mathcal{V}$ ahead of time.

If $|\mathcal{M}| \leq |\mathcal{S}|$, then there exists a trivial NIMAP where the whole message is transmitted over the authenticated channel. We assume that $|\mathcal{M}| > |\mathcal{S}|$ to consider nontrivial NIMAPs. For every tag $s \in \mathcal{S}$, we let $\mathcal{M}_s$ be the set of all messages such that there exists some r in which (M, r, s) results in an acceptance by Bob. In other words,

$$\mathcal{M}_s := \{M : (M, r, s) \in \mathcal{V} \text{ for some } r\}.$$

We let $\mathcal{U}$ be the set of all tags that can authenticate only one message; that is,

$$\mathcal{U} := \{s : |\mathcal{M}_s| = 1\}.$$

Furthermore, we let $\mathcal{M}_{\mathcal{U}}$ be the union of all $\mathcal{M}_s$ such that $s \in \mathcal{U}$. In other words,

$$\mathcal{M}_{\mathcal{U}} = \bigcup_{s \in \mathcal{U}} \mathcal{M}_s.$$

Since $|\mathcal{U}| \leq |\mathcal{S}| < |\mathcal{M}|$ and $|\mathcal{U}| \geq |\mathcal{M}_{\mathcal{U}}|$, we obtain that $|\mathcal{M}_{\mathcal{U}}| < |\mathcal{M}|$. Hence, there exists an $M \in \mathcal{M} \setminus \mathcal{M}_{\mathcal{U}}$ such that, for any $(M, r, s) \in \mathcal{V}$, there exists $(M', r', s) \in \mathcal{V}$ with $M \neq M'$.

The attack consists of Eve choosing any $M \in \mathcal{M} \setminus \mathcal{M}_{\mathcal{U}}$ and giving it to Alice. Note that Eve is computationally unbounded and can find such an M. Later, when Eve receives (M, r, s) from Alice,

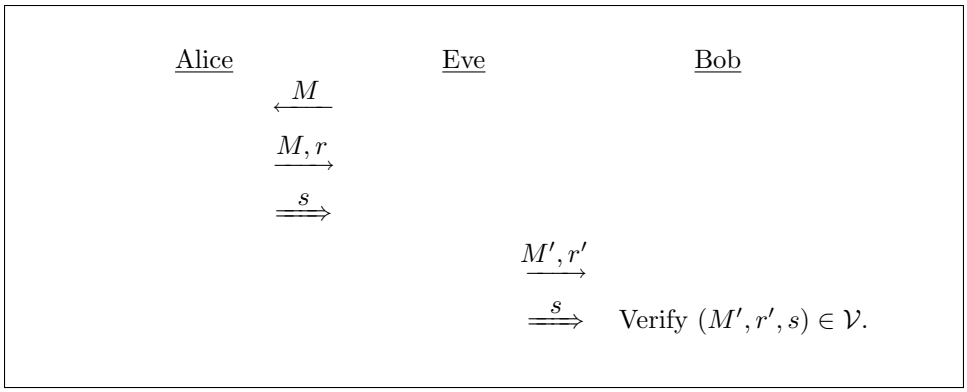

Figure 4: An Attack Against the General NIMAP

she replaces it with the appropriate (M', r', s), that we know exists. This attack, which succeeds with probability equal to 1, is depicted in Fig. 4.

We have proven the following theorem.

Theorem 2.1. *If the message space $\mathcal{M}$ of a NIMAP has greater cardinality than the tag space $\mathcal{S}$, then Eve can deceive Bob with probability equal to 1.*

Corollary 2.2. *Nontrivial unconditionally secure NIMAPs do not exist.*

The usual attack model allows Eve to select the message M that Alice will transmit to Bob. It is also interesting to consider a weaker attack model in which Alice chooses the message $M \in \mathcal{M}$ uniformly at random. (This is a natural situation to consider, for example in the setting where the message to be authenticated is a hash of a previously established Diffie-Hellman key.)

We have the following new result.

Theorem 2.3. *Suppose we have a NIMAP where Alice chooses the message $M \in \mathcal{M}$ uniformly at random, and the message space $\mathcal{M}$ has greater cardinality than the tag space $\mathcal{S}$. Then Eve can deceive Bob with probability at least $1 - |\mathcal{S}|/|\mathcal{M}|$.*

Proof. The analysis in this attack model is similar to the usual model. As before, Eve can successfully deceive Bob whenever $M \in \mathcal{M} \setminus \mathcal{M}_{\mathcal{U}}$. We showed above that $|\mathcal{M}_{\mathcal{U}}| \leq |\mathcal{S}|$. Under the assumption that Alice chooses the message $M \in \mathcal{M}$ uniformly at random, it follows that

$$\text{Prob}[M \in \mathcal{M} \setminus \mathcal{M}_{\mathcal{U}}] \geq 1 - \frac{|\mathcal{S}|}{|\mathcal{M}|}.$$

Therefore Eve can deceive Bob in this weaker attack model with probability at least $1 - |\mathcal{S}|/|\mathcal{M}|$. □

3 An Unconditionally Secure 3-Round IMAP

Naor, Segev and Smith [16, 17] proposed an unconditionally secure IMAP, with k rounds, using evaluation of polynomials over finite fields, for every integer k. To authenticate λ-bit message in k rounds, they require the length of the authenticated string to be about $2\log(1/\epsilon) + 2\log^{(k-1)}\lambda + O(1)$, where ϵ is the probability of success of the adversary. The length of the authenticated string

over the narrow-band channel is $2\log(1/\epsilon) + O(1)$ when $k = \log\lambda$. When $k = 3$, the length is $2\log(1/\epsilon) + 2\log\log\lambda + O(1)$. (Note that all logarithms are to the base 2.) Moreover, they proved that their protocol is close to optimal by proving a lower bound of $2\log(1/\epsilon) - 6$ on the required length of the authenticated string, for sufficiently long messages ([17, Theorem IV.4]).

In this paper, we focus on unconditionally secure IMAPs with three rounds. These are probably the IMAPs of greatest practical interest, since the communication structure is as simple as possible.

We present a construction for 3-round IMAPs based on ϵ-Δ universal hash families. This IMAP includes the Naor-Segev-Smith 3-round IMAP as a special case. We give a security analysis of our construction and analyze how to minimize the deception probability by choosing the hash families carefully. It turns out that the best IMAPs produced by this approach use hash families based on Reed-Solomon codes (essentially, the approach of Naor-Segev-Smith) but with different, optimized parameters. If a ν-bit authentication tag is sent in the third round, then we can achieve a deception probability of $2^{-\nu/2+2}$ for most parameter situations of practical interest (more precisely, whenever the message to be authenticated is not too long; see Theorem 3.6).

3.1 Hash Family Preliminaries

We will make essential use of certain types of hash families. The notion of an ϵ-Δ universal hash family (also known as an ϵ-ΔU hash family) was first given in Stinson [26], generalizing the idea of ϵ-almost xor universal hash families due to Krawczyk [10]. In this section, we review some old results and prove some new results that will be used in the rest of the paper. We begin with the following definition for ϵ-ΔU hash families.

Definition 3.1. *Suppose that a hash family $\mathcal{H}$ has keyspace $\mathcal{K}$, and $h_K : \mathcal{X} \to \mathcal{Y}$ for all $k \in \mathcal{K}$. We assume that $(\mathcal{Y}, +)$ is an abelian group. The hash family $\mathcal{H}$ is an* ϵ-ΔU hash family *if for all choices of $M, M' \in \mathcal{X}$ and all $s \in \mathcal{Y}$, it holds that*

$$\Pr[h_k(M) - h_k(M') = s] \leq \epsilon,$$

where the probability is computed over a randomly chosen key $k \in \mathcal{K}$. Equivalently,

$$|\{k \in \mathcal{K} : h_k(M) - h_k(M') = s\}| \leq \epsilon|\mathcal{K}|.$$

We will denote the hash family $\mathcal{H}$ as an ϵ-$\Delta U(N; n, m)$ hash family *if $N = |\mathcal{K}|$, $n = |\mathcal{X}|$, and $m = |\mathcal{Y}|$.*

We next present some bounds and constructions on ϵ-ΔU hash families.

Lemma 3.1. *Suppose there exists an ϵ-$\Delta U(N; n, m)$ hash family. Then $\epsilon \geq \max\{1/m, 1/N\}$.*

Proof. It is shown in [26, Theorem 4.1] that $\epsilon \geq 1/m$, so we need only show that $\epsilon \geq 1/N$. Let the hypothesized hash family $\mathcal{H}$ have keyspace $\mathcal{K}$, and assume $h_k : \mathcal{X} \to \mathcal{Y}$ for all $k \in \mathcal{K}$. Let $M, M' \in \mathcal{X}$, $M \neq M'$. Define $\mathcal{Y}_{M,M'} = \{h_k(M) - h_k(M') : k \in \mathcal{K}\}$. Observe that $|\mathcal{Y}_{M,M'}| \leq |\mathcal{K}| = N$. For any $y \in \mathcal{Y}_{M,M'}$, let

$$a_y = |\{k \in \mathcal{K} : h_k(M) - h_k(M') = y\}|.$$

Then $a_y \leq \epsilon N$ for all $y \in \mathcal{Y}_{M,M'}$, so

$$\sum_{y \in \mathcal{Y}_{M,M'}} a_y \leq \epsilon N^2.$$

On the other hand,

$$\sum_{y \in \mathcal{Y}_{M,M'}} a_y = N.$$

It therefore follows that $N \leq \epsilon N^2$, so $\epsilon \geq 1/N$. □

Lemma 3.2. *Suppose there exists an ϵ-$\Delta U(N; n, m)$ hash family, where $\epsilon = 1/m$. Then $N \geq n$.*

Proof. See [26, Theorem 4.3]. □

We now present a class of hash families based on Reed-Solomon codes. These hash families were first described in [26, Theorem 4.8]. The IMAP of Naor, Segev and Smith [16, 17] makes essential use of these hash families.

Lemma 3.3. *[26] Suppose q is a prime power and $1 \leq t \leq q-1$. Define $\mathcal{K} = \mathbb{F}_q$, $\mathcal{X} = (\mathbb{F}_q)^t$ and $\mathcal{Y} = \mathbb{F}_q$. For any $k \in \mathcal{K}$ and any $(x_1, \ldots, x_t) \in \mathcal{X}$, define*

$$h_k(x_1, \ldots, x_t) = \sum_{i=1}^{t} x_i k^i.$$

Then $\mathcal{RS}(q,t) = \{h_k : k \in \mathcal{K}\}$ is a $\frac{t}{q}$-$\Delta U(q; q^t, q)$ hash family.

3.2 The IMAP

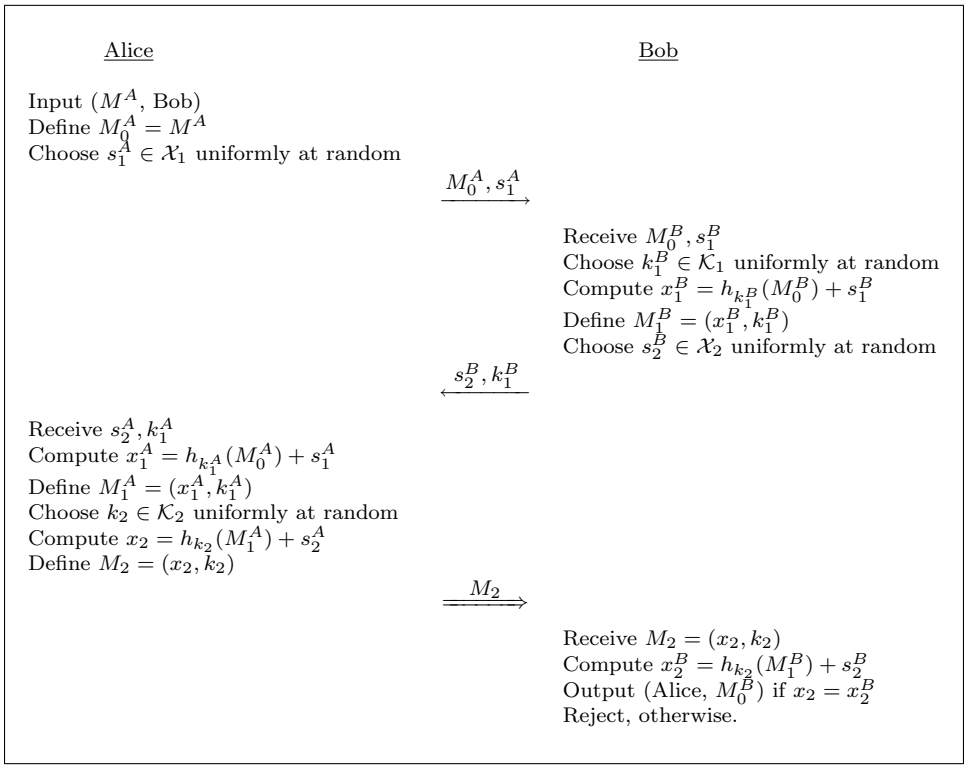

Figure 5: A Generalization of Naor-Segev-Smith IMAP

Figure 5 illustrates our generalization of the protocol proposed by Naor *et al.* In our protocol, we use the following notation and assumptions:

1. Let $\mathcal{M}$ be the set of all possible messages, and denote $\mathcal{M}_0 = \mathcal{M}$.
2. We use two families of hash functions, $\mathcal{H}_1$ and $\mathcal{H}_2$. For $i = 1, 2$, $\mathcal{H}_i$ is an ϵ_i-$\Delta U(N_i; n_i, m_i)$ hash family.
3. For $i = 1, 2$, let the keyspace of $\mathcal{H}_i$ be denoted by $\mathcal{K}_i$. For every $k_i \in \mathcal{K}_i$, the hash function $h_{k_i} : \mathcal{M}_{i-1} \to \mathcal{X}_i$.
4. $\mathcal{X}_1 \times \mathcal{K}_1 \subseteq \mathcal{M}_1$ (hence $n_2 \geq N_1 m_1$).
5. Define $\mathcal{X}_2 \times \mathcal{K}_2 = \mathcal{M}_2$. The number of bits sent over the authenticated channel is $\log |\mathcal{M}_2| = \log |\mathcal{K}_2| + \log |\mathcal{X}_2|$.

There are two hash function computations performed in this protocol. First, $x_1 = h_{k_1}(M_0) + s_1$. Then $M_1 = (x_1, k_1)$ and $x_2 = h_{k_2}(M_1) + s_2$. Finally, $M_2 = (x_2, k_2)$ is sent over the authenticated channel. Observe that Alice and Bob both compute x_1 and x_2 during the protocol.

3.3 Possible Attacks Against a 3-round Protocol

Before we analyze the protocol presented in Figure 5, we discuss the possible attacks we must consider. Figure 6 depicts a 3-round generic IMAP (3GIMAP) having the same flow structure as the one considered in Figure 5. We denote the messages transmitted in the protocol as follows:

- A_0 denotes the initial input received by Alice
- A_1 denotes the message sent by Alice in response to A_0
- A_2 denotes the second message received by Alice
- A_3 denotes the message sent by Alice over the authenticated channel in response to A_2
- B_1 denotes the first message received by Bob
- B_2 denotes the message sent by Bob in response to B_1
- B_3 denotes the final message received by Bob (over the authenticated channel).

Gehrmann [4] looked at different possible attacks against a generic k-round protocol and proved that there are in total $\binom{k+1}{\frac{k+1}{2}}$ distinct attacks. He used the following notation to label these attacks. A flow initiated by the adversary is labelled as **A** if it sent to Alice, and, similarly, a flow sent by the adversary is labelled as **B** if the recipient is Bob. According to his result, there are $\binom{4}{2} = 6$ possible attacks against a three round protocol, namely, AABB, ABBA, BABA, ABAB, BBAA, and BAAB attacks.

The last flow of 3GIMAP is an authenticated flow sent by Alice to Bob. According to the communication model of two-channel cryptography, the adversary can only replay this last flow. As a result, the only possible attacks against 3GIMAP are the ones that end with a flow sent to

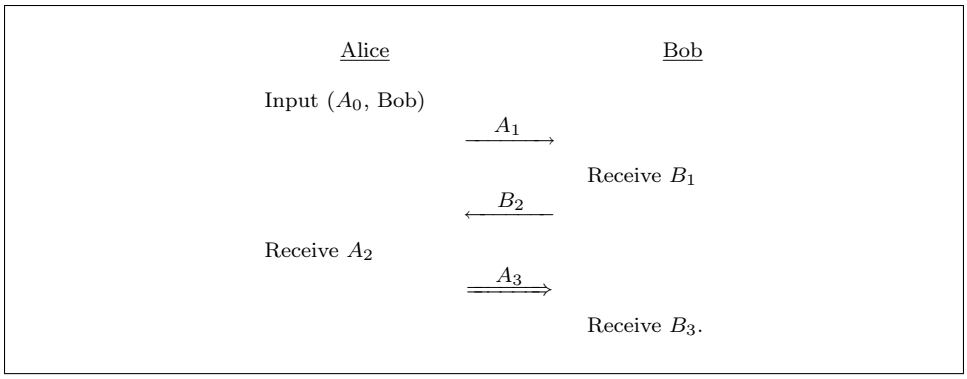

Figure 6: 3GIMAP

Bob, namely AABB, ABAB, and BAAB. These attacks, when applied to the protocol in Figure 5, are depicted in Figures 7, 8, and 9.

It would perhaps be of interest to give a self-contained proof that there are only three attacks that need to be considered, so we do this now. An execution of the protocol will consist of a certain ordering of the seven messages A_0, A_1, A_2, A_3, B_1, B_2, B_3 in the presence of Eve. However, not all orderings are possible. Clearly $A_0 < A_1 < A_2 < A_3$ and $B_1 < B_2 < B_3$, where "$<$" denotes that one message must precede another message.

Now we can assume without loss of generality that

- A_1 immediately follows A_0,
- A_3 immediately follows A_2, and
- B_2 immediately follows B_1.

This is easily seen because Eve can always wait for these responses before carrying out her next action (she can ignore the responses if she chooses to do so).

As well, $A_3 < B_3$ since this the authenticated flow that cannot be altered. Consequently, B_3 must be the very last flow in any complete execution of the protocol.

As a consequence of the above analysis, we can define four "message units" as follows:

- let A^1 denote A_0A_1
- let A^2 denote A_2A_3
- let B^1 denote B_1B_2, and
- let B^2 denote B_3.

Now it is easily seen, in view of the above restrictions, that there are in fact only three orderings (attacks) to consider:

- $A^1A^2B^1B^2$ (which we term AABB)
- $A^1B^1A^2B^2$ (which we term ABAB), and
- $B^1A^1A^2B^2$ (which we term BAAB).

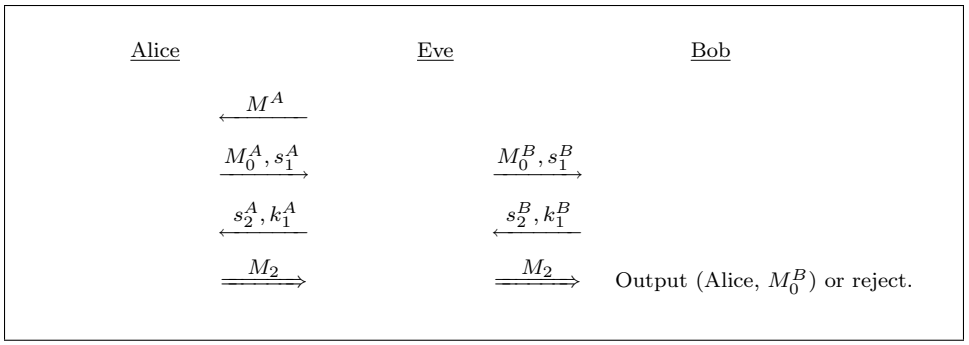

Figure 7: Attack of Type ABAB

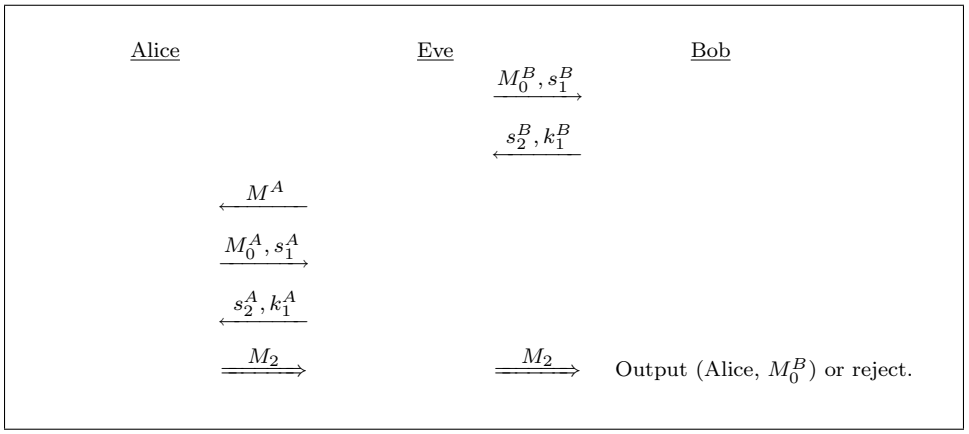

Figure 8: Attack of Type BAAB

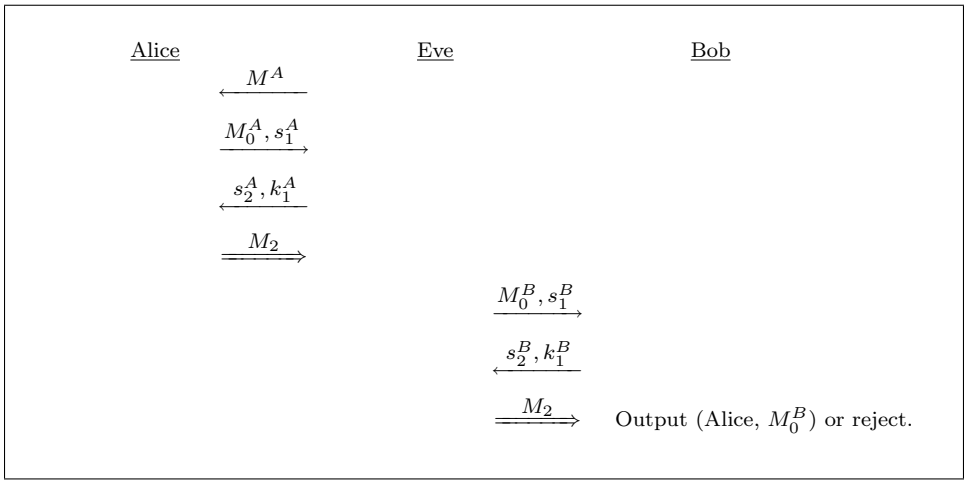

Figure 9: Attack of Type AABB

3.4 Analysis of the IMAP

Now we are in a position to analyze the attacks on the protocol presented in Figure 5. In a successful attack, it is required that $M_0^A \neq M_0^B$ and $x_2 = x_2^B$. We distinguish two cases:

(i) $M_1^A = M_1^B$

(ii) $M_1^A \neq M_1^B$.

In case (i), we have $k_1^A = k_1^B = k_1$ (say), and $x_1^A = x_1^B$, so

$$h_{k_1}(M_0^A) + s_1^A = h_{k_1}(M_0^B) + s_1^B,$$

which simplifies to

$$h_{k_1}(M_0^A) - h_{k_1}(M_0^B) = s_1^B - s_1^A. \tag{1}$$

In case (ii), we have $x_2 = x_2^B$, and it follows that

$$h_{k_2}(M_1^A) - h_{k_2}(M_1^B) = s_2^B - s_2^A, \tag{2}$$

where $M_1^A \neq M_1^B$.

We now analyze each of the three attacks.

ABAB attack

Case (i) Here, M_0^A, M_0^B, s_1^A and s_1^B are fixed before k_1 is chosen by Bob. Therefore, the probability that (1) holds is at most ϵ_1, because $\mathcal{H}_1$ is an ϵ_1-ΔU hash family.

Case (ii) Here, M_1^A, M_1^B, s_2^A and s_2^B are fixed before k_2 is chosen by Alice. Therefore, the probability that (2) holds is at most ϵ_2, because $\mathcal{H}_2$ is an ϵ_2-ΔU hash family.

The probability of success of an ABAB attack is therefore at most $\epsilon_1 + \epsilon_2$.

BAAB attack

Case (i) Here, k_1, M_0^A, M_0^B and s_1^B are fixed before s_1^A is chosen by Alice. Therefore, (1) holds if and only if

$$s_1^A = s_1^B - h_{k_1}(M_0^A) + h_{k_1}(M_0^B),$$

where the right side of this equality is a fixed quantity. Since Alice chooses s_1^A uniformly at random from $\mathcal{X}_1$, the probability that (1) holds is $1/|\mathcal{X}_1|$.

Case (ii) Here, M_1^A, M_1^B, s_2^A and s_2^B are fixed before k_2 is chosen by Alice. Therefore, the probability that (2) holds is ϵ_2.

The probability of success of a BAAB attack is therefore at most $1/|\mathcal{X}_1| + \epsilon_2$.

AABB attack

Case (i) Eve has to choose k_1^A before Bob chooses k_1^B. The probability that $k_1^A = k_1^B$ is $1/|\mathcal{K}_1|$.

Case (ii) Here, k_2, M_1^A, M_1^B and s_2^A are fixed before s_2^B is chosen by Bob. Therefore, (2) holds if and only if

$$s_2^B = s_2^A + h_{k_2}(M_1^A) - h_{k_2}(M_1^B),$$

where the right side of this equality is a fixed quantity. Since Bob chooses s_2^B uniformly at random from $\mathcal{X}_2$, the probability that (2) holds is $1/|\mathcal{X}_2|$.

The probability of success of an AABB attack is therefore at most $1/|\mathcal{K}_1| + 1/|\mathcal{X}_2|$.

Summary

Now, whatever Eve chooses to do, the sequence of messages that she inserts into the channel will correspond to one of the three attacks (AABB, ABAB or BAAB). So the analysis of the three attacks covers all the possibilities. Hence, if we consider all three attacks, we see that Eve succeeds with probability

$$\max\left\{\epsilon_1+\epsilon_2, \frac{1}{|\mathcal{X}_1|}+\epsilon_2, \frac{1}{|\mathcal{K}_1|}+\frac{1}{|\mathcal{X}_2|}\right\}.$$

It follows from Lemma 3.1 that $\epsilon_1 \geq 1/|\mathcal{X}_1|$, $\epsilon_1 \geq 1/|\mathcal{K}_1|$ and $\epsilon_2 \geq 1/|\mathcal{X}_2|$. Therefore,

$$\max\left\{\epsilon_1+\epsilon_2, \frac{1}{|\mathcal{X}_1|}+\epsilon_2, \frac{1}{|\mathcal{K}_1|}+\frac{1}{|\mathcal{X}_2|}\right\} = \epsilon_1+\epsilon_2.$$

Therefore, we have proven the following theorem.

Theorem 3.4. *Suppose there exists an ϵ_i-$\Delta U(N_i; n_i, m_i)$ hash family, for $i = 1, 2$, where $n_2 \geq N_1 m_1$. Then the protocol presented in Figure 5 manually authenticates an $\log_2 n_1$-bit message with an $(\log_2 N_2 + \log_2 m_2)$-bit tag, where the deception probability of an adversary is at most $\epsilon \leq \epsilon_1 + \epsilon_2$.*

3.5 Specific Constructions for Unconditionally Secure IMAPs

The following application of Theorem 3.4 uses the hash families constructed in Lemma 3.3. It is similar to the construction in [16, 17], specialized to three rounds, but with more general parameters. The three-round version of the Naor *et al.* construction, which uses formulas given in [17, page 2414], is a special case of this corollary.

Corollary 3.5. *Suppose that λ, μ and ν are positive integers such that $\lambda > \mu > \nu/2$. Then a λ-bit message can be manually authenticated with a ν-bit tag using a 3-round IMAP in which*

$$\epsilon \leq \left\lceil \frac{\lambda}{\mu} \right\rceil 2^{-\mu} + \left\lceil \frac{4\mu}{\nu} \right\rceil 2^{-\nu/2}. \tag{3}$$

Proof. Define

$$n_1 = 2^{\mu\left\lceil \frac{\lambda}{\mu} \right\rceil}, \quad m_1 = 2^{\mu}, \quad N_1 = 2^{\mu}, \quad \epsilon_1 = \left\lceil \frac{\lambda}{\mu} \right\rceil 2^{-\mu}$$

and

$$n_2 = 2^{\frac{\nu}{2}\left\lceil \frac{4\mu}{\nu} \right\rceil}, \quad m_2 = 2^{\nu/2}, \quad N_2 = 2^{\nu/2}, \quad \text{and} \quad \epsilon_2 = \left\lceil \frac{4\mu}{\nu} \right\rceil 2^{-\nu/2}.$$

The required hash families exist from Lemma 3.3 and it is easy to verify that $n_2 \geq 2^{2\nu} = N_1 m_1$. □

In our computations, it will be useful to note that we have the following in Corollary 3.5:

- M_0 is λ bits in length,
- $x_1 = h_{k_1}(M_0)$ is μ bits in length,
- $M_1 = (x_1, K_1)$ is 2μ bits in length,
- $x_2 = h_{k_2}(M_1)$ is $\nu/2$ bits in length, and

- $M_2 = (x_2, K_2)$ is ν bits in length.

The value of μ in Corollary 3.5 would be chosen to minimize the resulting value of ϵ. Denote $t = \lceil \frac{4\mu}{\nu} \rceil$. Observe that $\mu > \nu/2$, so $t > 2$.

We will assume that 2μ is an integer multiple of the integer value $\nu/2$, and λ is an integer multiple of μ. It follows that $4\mu/\nu$ is an integer, so we have $t = 4\mu/\nu$. Writing $\mu = \nu t/4$, we can express the bound (3) as follows:

$$\epsilon \leq \frac{4\lambda}{\nu t} 2^{-\nu t/4} + t\, 2^{-\nu/2}. \tag{4}$$

For fixed λ and ν, denote the right side of (4) by $f(t)$. Recalling that t is an integer, it is possible to determine the value of t that maximizes $f(t)$ by computing

$$f(t+1) - f(t) = \frac{4\lambda}{\nu(t+1)} 2^{-\nu(t+1)/4} + (t+1)\, 2^{-\nu/2} - \left(\frac{4\lambda}{\nu t} 2^{-\nu t/4} + t\, 2^{-\nu/2} \right).$$

After some simplification, it can be verified that

$$f(t+1) \geq f(t) \Leftrightarrow \lambda \leq \frac{\nu\, 2^{\nu(t-1)/4}}{4\left(\frac{2^{\nu/4}}{t} - \frac{1}{t+1} \right)}.$$

It follows that it is optimal to use $t = 3$ whenever

$$\lambda \leq \frac{\nu\, 2^{\nu/2}}{\frac{4}{3} 2^{\nu/4} - 1}. \tag{5}$$

When $t = 3$, we have $\mu = 3\nu/4$. We want λ to be a multiple of μ, so we denote $t_1 = \lambda/\mu$. Observing that

$$\left\lfloor \frac{2^{\nu/2}}{2^{\nu/4} - 1} \right\rfloor = 2^{\nu/4},$$

and using the fact that t_1 is an integer, we can refine (5) as follows:

$$t_1 \leq \left\lfloor \frac{\lambda}{\mu} \right\rfloor \leq \left\lfloor \frac{2^{\nu/2}}{2^{\nu/4} - 1} \right\rfloor = 2^{\nu/4} = 2^{\mu/3}.$$

Table 1 lists the maximum value of λ such that $t = 3$ is optimal, for various values of ν, along with the corresponding values of μ, t_1 and $\log_2 \epsilon$. We have that $t_1 = 2^{\nu/4}$, $\mu = 3\nu/4$ and $\lambda = \nu t_1$. Observe that $\log_2 \epsilon = -\nu/2 + 2$; this can be verified algebraically using (4), since

$$\frac{4\lambda}{\nu t} 2^{-\nu t/4} + t\, 2^{-\nu/2} = 2^{\nu/4} \times 2^{-3\nu/4} + 3 \times 2^{-\nu/2} = 2^{-\nu/2+2}.$$

It can be seen that the resulting λ values cover many if not most practical applications of IMAPs.

Summarizing, we have the following.

Theorem 3.6. *Suppose $\lambda \leq 3\nu\, 2^{\nu/4-2}$. Then a λ-bit message can be manually authenticated with a ν-bit tag using a 3-round unconditionally secure IMAP in which $\epsilon \leq 2^{-\nu/2+2}$.*

Table 1: Parameters for which $t = 3$ is optimal

λ	μ	ν	t_1	$\log_2 \epsilon$
6144	24	32	256	-14
30720	30	40	1024	-18
147456	36	48	4096	-22
688128	42	56	16384	-26
3145728	48	64	65536	-30
14155776	54	72	262144	-34

Remark: The value of ν in Theorem 3.6 can be expressed as $\nu = 2\log(1/\epsilon) + 4$, which is only 10 bits more than the lower bound $\nu \geq 2\log(1/\epsilon) - 6$ which holds for sufficiently large n ([16, 17]).

Example 3.1. *Suppose we wish to construct a 3-round IMAP with a 48-bit authenticated tag. Then we take* $\nu = 48$ *in Theorem 3.6. The deception probability of the IMAP will be at most* 2^{-22} *provided that the message to be authenticated is at most* 147456 *bits in length. The scheme has* $\mu = 36$*, so the hash family* $\mathcal{H}_2$ *is a* $3/2^{24}$*-*$\Delta U(2^{24}; 2^{72}, 2^{24})$ *hash family. The hash family* $\mathcal{H}_1$ *is an* ϵ_1*-*$\Delta U(2^{36}; 2^{\lambda}, 2^{36})$ *hash family, where* $\lambda \leq 147456$ *and* $\epsilon_1 = \frac{\lambda}{36}\, 2^{-36} \leq 2^{-24}$*. Implementation of the scheme requires evaluating a polynomial of degree* $\lambda/36$ *over the field* $\mathbb{F}_{2^{36}}$*, and a polynomial of degree* 3 *over the field* $\mathbb{F}_{2^{24}}$*.*

Example 3.2. *We present an example of the Naor-Segev-Smith scheme. As in the previous example, we take* $\lambda = 147456$ *and* $\epsilon = 2^{-22}$*. We apply the formulas in [17, p. 2414]. Using our notation, we would obtain*

$$\mu = \lceil 2 + \log 147456 + 22 \rceil = 42$$

and

$$\nu = 2\ \lceil 1 + \log 84 + 22 \rceil = 60.$$

Thus their scheme uses a 60*-bit tag whereas a* 48*-bit tag is sufficient in our scheme.*

4 Another Unconditionally Secure 3-Round IMAP

The IMAP analyzed in the previous section made use of two hash function families, and a message is hashed twice during the protocol. It might be of interest to study simpler protocols that only require one hash computation to be performed.

Figure 10 illustrates another unconditionally secure 3-round IMAP. This IMAP requires only one evaluation of a hash function instead of two. It is most useful in the authentication of relatively short messages. We use one hash function family, $\mathcal{H}$, which is an ϵ-$\Delta U(N; n, m)$ hash family. Let the keyspace of $\mathcal{H}$ be denoted by $\mathcal{K}$, and for every $k \in \mathcal{K}$, there is a hash function $h_k : \mathcal{M} \to \mathcal{X}$. The number of bits sent over the authenticated channel is $\log|\mathcal{K}| + \log|\mathcal{X}|$.

In a BAAB attack, Eve is required to set $k^A = k^B$, otherwise she will be detected. Eve is successful if and only if

$$h_{k^B}(M^A) + s^A = h_{k^B}(M^B) + s^B.$$

In other words, Eve succeeds if and only if $s^A = h_{k^B}(M^B) + s^B - h_{k^B}(M^A)$. In the BAAB attack, s^A is randomly chosen by Alice after k^B is chosen by Bob, so Eve succeeds with probability $1/|\mathcal{X}|$.

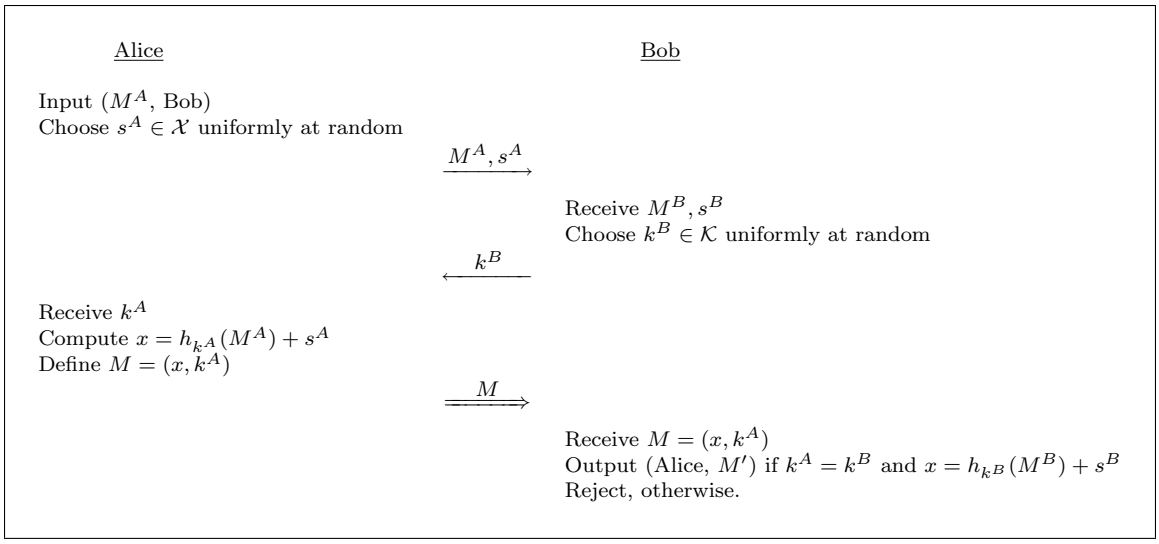

Figure 10: Another 3-Round IMAP

In an AABB attack, on the other hand, Eve first obtains the values M^A, s^A and she has to guess the key k^B ahead of time in order to set $k^A = k^B$. Later, she can choose M^B and s^B such that $h_{k^B}(M^A) + s^A = h_{k^B}(M^B) + s^B$. The probability that Eve guesses the right key k^B is $1/|\mathcal{K}|$.

Finally, in an ABAB attack, Eve receives M^A, s^A and fixes M^B, s^B before k^B is chosen by Bob. Since $k^A = k^B$, Eve is successful in her attack if and only if $h_{k^B}(M^A) - h_{K^B}(M^B) = s^B - s^A$. Note that $s^B - s^A$ is a predetermined fixed value. Hence, since $\mathcal{H}$ is an ϵ-ΔU hash family, Eve succeeds with probability at most ϵ.

If we summarize the above three attacks, we see that Eve succeeds with probability

$$\max\{\epsilon, |\mathcal{X}|^{-1}, |\mathcal{K}|^{-1}\}.$$

From Lemma 3.1, we have $\max\{\epsilon, |\mathcal{X}|^{-1}, |\mathcal{K}|^{-1}\} = \epsilon$. Therefore we have the following.

Theorem 4.1. *Suppose there exists an ϵ-$\Delta U(N; n, m)$ hash family. Then the protocol presented in Figure 10 manually authenticates an $\log_2 n$-bit message with an $(\log_2 N + \log_2 m)$-bit tag, where the deception probability of an adversary is at most ϵ.*

Using the hash families constructed in Lemma 3.3, we have the following theorem, which is a corollary of Theorem 4.1.

Corollary 4.2. *Suppose $\lambda \leq \nu(2^{\nu/2-1})$. Then a λ-bit message can be manually authenticated with a ν-bit tag using a 3-round unconditionally secure IMAP in which the deception probability $\epsilon \leq \lambda/(\nu 2^{\nu/2-1})$.*

Proof. Let $q = 2^{\nu/2}$ and $t = 2\lambda/\nu$. Since $\lambda \leq \nu(2^{\nu/2-1})$, we have that $t \leq 2 \times \nu(2^{\nu/2-1})/\nu = q$. Therefore, Lemma 3.3 establishes the existence of an ϵ-$\Delta U(q; q^t, q)$ hash family, where $\epsilon = t/q$. Now apply Theorem 4.1. The resulting IMAP authenticates a message of length $\log q^t = t \log q = (2\lambda/\nu) \times (\nu/2) = \lambda$ with a tag of length $2 \log q = \nu$. The deception probability is $\epsilon = t/q = t/2^{\nu/2} = (2\lambda/\nu)/2^{\nu/2} = \lambda/(\nu 2^{\nu/2-1})$. □

If we wish to have $\epsilon = 2^{-\nu/2+2}$, as in Theorem 3.6, then we must take $\lambda \leq 4\nu$ in Corollary 4.2. For this range of values of λ, we achieve the same security as Theorem 3.6 but we require only one hash function computation.

In related work, a somewhat similar protocol was given by Laur and Pasini in [13, Figure 5]. Their protocol makes use of a bidirectional authenticated channel, which is used in two flows of the protocol. Briefly, Alice chooses a random key K and hashes M, obtaining a hash value t. t is sent to Bob over the broadband channel. Bob sends an acknowledgement to Alice over the authenticated channel, and then Alice sends K to Bob over the authenticated channel.

In the Laur-Pasini proptocol, the hash family needs to withstand substitution attacks in the classical authentication framework of Simmons [23]. Therefore, the hash family should in fact be an ϵ-*almost strongly universal* hash family (see [25]) for a definition). It is shown in [26] that an ϵ-almost strongly universal hash family can be obtained from a ϵ-ΔU hash family by "encrypting" the tag (i.e., hash value) with a one-time pad which would form part of the key. Suppose an ϵ-almost strongly universal hash family is constructed in this fashion. Then the length of the key in the Laur-Pasini protocol is the same as the length of the key plus the length of the hash value in our protocol (Figure 10). Therefore the Laur-Pasini protocol achieves an efficiency level similar to our protocol in terms of the deception probability and the amount of information sent over the authenticated channel. However, as mentioned above, the Laur-Pasini protocol requires a bidirectional authenticated channel, which is a stronger requirement than our protocol.

5 Conclusion

We proved that nontrivial unconditionally secure NIMAPs do not exist, by using a simple counting argument. We also proposed a generalization of an unconditionally secure 3-round IMAP due to Naor, Segev and Smith [16, 17]. For most parameter situations of practical interest, our scheme requires an authenticated tag that is only 10 bits longer than the theoretical minimum proven in [16, 17]. This IMAP is based on two ϵ-Δ universal hash families. Finally, a variation of the IMAP is presented, in which only one hash family is required.

Acknowledgements

We would like to thank the referees for helpful suggestions that improved the presentation of the results in this paper.

References

[1] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: authentication in ad-hoc wireless networks. In *Network and Distributed System Security Symposium*, San Diego, California, U.S.A., February 2002.

[2] M. Chan, D. Estève, C. Escriba, and E. Campo. A review of smart homes-present state and future challenges. *Computer Methods and Programs in Biomedicine*, **91** (2008), 55–81.

[3] G. Demiris. Electronic home healthcare: concepts and challenges. *International Journal of Electronic Healthcare* **1** (2004), 4–16.

[4] C. Gehrmann. Multiround unconditionally secure authentication. *Designs, Codes, and Cryptography* **15** (1998), 67–86.

[5] C. Gehrmann, C. J. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *RSA Cryptobytes* **7** (2004), 29–37.

[6] C. Gehrmann and K. Nyberg. Security in personal area networks. In *Security for Mobility*, IEE, London, 2004, pages 191–230.

[7] S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing* **17** (1988), 281–308.

[8] J.-H. Hoepman. The ephemeral pairing problem. *Lecture Notes in Computer Science* **3110** (2004), 212–226 (Financial Cryptography).

[9] R. Kainda, I. Flechais and A. W. Roscoe. Usability and security of out-of-band channels in secure device pairing protocols. In *Symposium on Usable Privacy and Security (SOUPS 2009)*.

[10] H. Krawczyk. LFSR-based hashing and authentication. *Lecture Notes in Computer Science* **839** (1994), 129–139 (CRYPTO 1994).

[11] S. Laur and K. Nyberg. Efficient mutual data authentication using manually authenticated strings. *Lecture Notes in Computer Science* **4301** (2006), 90–107 (CANS 2006).

[12] S. Laur and S. Pasini. SAS-Based group authentication and key agreement protocols. *Lecture Notes in Computer Science* **4939** (2008), 197–213 (PKC 2008).

[13] S. Laur and S. Pasini. User-aided data authentication. *International Journal of Security and Networks* **4(1/2)** 2009, 69–86.

[14] A. Mashatan and D. R. Stinson. Noninteractive two-channel message authentication based on hybrid-collision resistant hash functions. *IET Information Security* **1** (2007), 111–118.

[15] A. Mashatan and D. R. Stinson. Interactive two-channel message authentication based on interactive-collision resistant hash functions. *International Journal of Information Security* **8** (2009), 49–60.

[16] M. Naor, G. Segev, and A. Smith. Tight bounds for unconditional authentication protocols in the manual channel and shared key models. *Lecture Notes in Computer Science* **4117** (2006), 214–231 (CRYPTO 2006).

[17] M. Naor, G. Segev, and A. Smith. Tight bounds for unconditional authentication protocols in the manual channel and shared key models. *IEEE Transactions on Information Theory* **54** (2008), 2408–2425.

[18] L. H. Nguyen and A. W. Roscoe. Authenticating ad hoc networks by comparison of short digests. *Information and Computation* **206** (2008), 250–271.

[19] S. Pasini and S. Vaudenay. An optimal non-interactive message authentication protocol. *Lecture Notes in Computer Science* **3860** (2006), 280–294 (CT-RSA 2006).

[20] S. Pasini and S. Vaudenay. SAS-Based Authenticated Key Agreement. *Lecture Notes in Computer Science* **3958** (2006), 395–409 (PKC 2006).

[21] M. R. Reyhanitabar, S. Wang, and R. Safavi-Naini. Non-interactive manual channel message authentication based on eTCR hash functions. *Lecture Notes in Computer Science* **4586** (2007), 385–399 (ACISP 2007).

[22] R. L. Rivest and A. Shamir. How to expose an eavesdropper. *Communications of the ACM* **27** (1984) , 393–394.

[23] G. J. Simmons. Authentication theory / coding theory. *Lecture Notes in Computer Science* **196** (1985), 411–431 (CRYPTO 1984).

[24] F. Stajano and R. Anderson. The resurrecting duckling: security issues for ad-hoc wireless networks. *Lecture Notes in Computer Science* **1796** (1999), 172–182 (Security Protocols, Seventh International Workshop).

[25] D. R. Stinson. Universal hashing and authentication codes. *Designs, Codes and Cryptography* **4** (1994), 369–380.

[26] D. R. Stinson. On the connections between universal hashing, combinatorial designs and error-correcting codes. *Congressus Numerantium* **114** (1996), 7–27 (Twenty-fifth Manitoba Conference on Combinatorial Mathematics and Computing).

[27] S. Vaudenay. Secure communications over insecure channels based on short authenticated strings. *Lecture Notes in Computer Science* **3621** (2005), 309–326 (CRYPTO 2005).

[28] S. Wang and R. Safavi-Naini. New results on unconditionally secure multireceiver manual authentication. Cryptology ePrint Archive, Report 2008/039, 2008.