INTERACTIVE TWO-CHANNEL MESSAGE AUTHENTICATION BASED ON INTERACTIVE-COLLISION RESISTANT HASH FUNCTIONS

ATEFEH MASHATAN[1] AND DOUGLAS R. STINSON[2]

Abstract. We propose an interactive message authentication protocol (IMAP) using two channels: an insecure broadband channel and an authenticated narrow-band channel. We consider the problem in the context of ad hoc networks, where it is assumed that there is neither a secret key shared among the two parties, nor a public-key infrastructure in place. The security of our IMAP is based on the existence of Interactive-Collision Resistant (ICR) hash functions, a new notion of hash function security.

Our IMAP is performing better than IMAPs and non-interactive message authentication protocols (NIMAPs) proposed so far. That is, while achieving the same level of security, the amount of information sent over the authenticated channel in our IMAP is smaller than the most secure IMAP and NIMAP in the literature. Moreover, our IMAP benefits from a simple structure and works under fewer security assumptions compared to other IMAPs in the literature. The efficient and easy-to-use structure of our IMAP makes it very practical in real world ad hoc network scenarios.

Date: January 11, 2007.

[1] Department of Combinatorics and Optimization
amashatan@uwaterloo.ca
[2] David R. Cheriton School of Computer Science
dstinson@uwaterloo.ca
University of Waterloo
Waterloo, Ontario CANADA N2L 3G1

.

1. Introduction

Message authentication, entity authentication, and data confidentiality are the cornerstones of secure communication and constitute the fundamental goals of cryptography. When communicating over a potentially insecure channel, the parties would like to be assured of the authenticity of information they obtain, as well as the identity of the sender.

Standard models of public-key cryptography and secret-key cryptography have addressed the three fundamental goals of cryptography by means of public-key infrastructures, secure channels, etc. However, in ad hoc networks where some users are part of the network only for a short period of time, assuming these traditional settings might not be practical. For instance, presuming a public-key infrastructure or any secure channel may not be cost efficient.

In search of a solution to the problem of message authentication in ad hoc networks, Rivest and Shamir [10] suggested using the human voice in an authentication protocol. They consider a scenario where the two parties want to authenticate a key in the absence of any trusted third party or previously distributed shared secret. Their authentication protocol is based on the assumption that the two parties can recognize each others' voices. Rivest and Shamir proposed incorporating human abilities in designing authentication protocols in 1984 and, indeed, such a communication assumption can be applied to many real life scenarios. However, this idea did not receive serious attention from researchers until very recently.

To make our protocols more useful in a practical ad hoc setting, we consider a model where no public-key infrastructure exists and no shared secret is assumed. Two small devices wish to establish a secure key in such an environment by communicating over an insecure broadband channel and an authenticated narrow-band channel. The authenticated channel might be based on information transmitted by human beings as users of the two devices. This short string is going be used to authenticate the information sent over the broadband channel. This model is described in detail in [2] and [3].

Reading a short string from one device and inputting it into the other device, or comparing two short strings from two devices, are examples of human aided authenticated channels. Infrared (IR), laser, near field communication (NFC) developed by Sony and Phillips, or visible light between the two devices can be used to send a short string. One can also require the two devices to physically touch each other. There is a cost associated to equipping the devices with the appropriate signal transmitter and receiver. However, using these signals has the advantage of essentially eliminating the human error factor.

Following the idea of Rivest and Shamir [10] in using human aided channels as the authenticated channel, there have been interactive message authentication protocols (IMAP) and noninteractive message authentication protocols (NIMAP) proposed in the literature.

1.1. Previous NIMAPs.

The first NIMAP was proposed by Balfanz, Smetters, Stewart, and Wong [1]. They require to send 160 bits over the narrow-band channel. It is desirable to reduce the amount of information sent over the authenticated channel.

Next, MANA I, MANA II, and MANA III were proposed by Gehrmann, Mitchell and Nyberg [3]. MANA stands for "manual authentication" which refers to the human aided authenticated channel. The MANA series reduce the amount of information sent over the narrow-band channel. However, a stall-free channel is required to be used as the narrow-band channel.

The next NIMAP was proposed by Pasini and Vaudenay [9] using second-preimage resistant hash functions and commitment schemes in the Common Reference String (CRS) model, where it is assumed that a random key K_p is previously distributed to all users. The key K_p, like any other public key, must be authenticated. Moreover, the use of commitment schemes makes

this NIMAP somewhat complicated, especially when compared to other NIMAPs that just use hash functions.

Mashatan and Stinson [7] recently provided a formal model for NIMAPs in general, along with a new NIMAP. They explored the essential properties of a general NIMAP using two channels and proved that any NIMAP having certain properties will be secure. The particular NIMAP proposed by them relies on a new property of hash functions named "hybrid-collision resistance". This NIMAP achieves the level of security of the Pasini and Vaudenay NIMAP, while it benefits from an efficient and easy to use structure. For further analysis and comparison among NIMAPs, we refer the reader to Mashatan and Stinson [7].

1.2. **Previous IMAPs.** A noninteractive protocol is, in general, preferred to an interactive protocol if they are achieving the exact same goals. In other words, interactive protocols are supposed to either achieve better security or be more efficient than their noninteractive competitors, otherwise, one would choose to implement noninteractive protocols and obtain the same results.

Hoepman [4] proposed an authenticated key agreement protocol that uses both a bidirectional narrow-band channel and a bidirectional broadband channel. This interactive protocol consists of a commitment exchange, an authentication exchange, and finally a decisional Diffie-Hellman problem in a group G. The security is based on the hardness of the decisional Diffie-Hellman problem in G and on two hash functions H_1 and H_2 having a very specific structure. In [11], it is discussed that instances of such hash functions may not exist at all.

Vaudenay [11] proposed an IMAP based on equivocable or extractable commitment schemes. This protocol achieves a good level of security. However, the only efficient commitment schemes, with the specific properties required here, are in the random oracle model. There are other instances of such commitment schemes in the standard model, but the number of rounds is logarithmic in terms of the security parameters and it involves zero-knowledge proofs. Also, there are some efficient commitment schemes with the appropriate properties in the Common Random String (CRS) model. However, the CRS model might not be suitable in an ad hoc setting where it is not practical to authentically distribute a random string to every user.

Laur, Asokan and Nyberg [5] proposed a Mutual Interactive Message Authentication Protocol (MIMAP) called MA-3 (for 3 round mutual authentication). It requires the authenticated channel to be bidirectional. Their protocol is in the CRS model and requires non-malleable commitment schemes to exist. Later Laur and Nyberg [6] proposed a protocol family in the CRS model using keyed hash functions and commitment schemes.

Naor, Segev and Smith [8] have recently proposed an unconditionally secure IMAP using evaluation of polynomials over finite fields. This IMAP is unconditionally secure. However, it requires the number of rounds to be an increasing function of the length of the message which is being authenticated. This is not desirable in an ad hoc setting.

1.3. **Our contributions.** We construct a new IMAP using two channels based on Interactive-Collision Resistant (ICR) hash functions. Our protocol has a very simple structure and does not require any long strings to be distributed ahead of time. We allow offline attacks by an adversary, as well as replay attacks. The attack model is the adaptive chosen plain-text attack (ACPA) model. The ACPA model is a strong model, and as a result, a scheme that is proven secure in this model does not require authenticated channels that have any unusual properties.

The simplicity of the structure and the generality of the security model makes our protocol applicable in a wide variety of real-world settings where ad hoc networks have no trusted infrastructure. For instance, it can be used in pairing of wireless devices such as Wireless

USB and Bluetooth, in Personal Area Networks (PANs), or in a disaster case where a trusted infrastructure has been compromised.

We analyze the security and efficiency of our IMAP and show that the performance of our IMAP is better than other IMAPs and NIMAPs proposed so far. In other words, our IMAP achieves the same level of security, while benefitting from an efficient structure and having to send fewer bits over the authenticated channel.

The rest of this paper is organized as follows. In Section 2, the attack model, i.e., adversarial goal and capabilities, are defined. Section 3 is devoted to briefly examining previous IMAPs. Their security is analyzed in our model. In Section 4, Interactive-Collision Resistance (ICR), a new notion for hash function security, is defined. Finally, an IMAP based on ICR hash functions is proposed. We prove in Section 5 that our IMAP is secure given that the ICR Game is hard to win. Furthermore, the simplicity of the structure, security, and the amount of information sent over both channels are noted. Finally, Section 6 contains some concluding remarks.

2. The communication Model and The Attack Model

We assume that two channels are accessible for communication: an insecure broadband channel, denoted by $\rightarrow$, and an authenticated narrow-band channel, denoted by $\Rightarrow$. The latter is sometimes referred to as the manual channel. Communication over the authenticated channel is usually more expensive and less accessible. Hence, the messages sent over the authenticated channel are ideally much shorter than those sent over the insecure channel. The goal is to employ both of these channels in a message authentication protocol.

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 the message from being delivered, and initiate a new message in 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. However, it is still possible to read, delay or remove the message from this channel. Furthermore, the authenticated channel is equipped with user authenticating features such that the recipient of the information can be sure about who sent it.

NIMAPs and IMAPs deploy both narrow-band and broadband channels between a claimant Alice and a verifier Bob. Alice chooses a message $M \in \mathcal{M}$, the space of all acceptable messages, and sends it to Bob using a NIMAP or an IMAP. At the end, Bob either outputs (Alice, M'), where $M' \in \mathcal{M}$, or he rejects. In the absence of an active adversary, the message M sent from Alice should be recovered by Bob, making him accept and output (Alice, M).

We now define the attack model, adversarial goal and capabilities. The adversary is trying to make Bob accept a message M' along with the identity of Alice, when in fact the message M' was never sent by Alice to Bob. That is, the *adversarial goal* is to make Bob output (Alice, M') when he was supposed to reject. There are two main types of attacks to consider: *impersonation* attacks and *substitution* attacks.

In an impersonation attack, the adversary initiates a session and tries to convince Bob that a message M' is sent from Alice, while in fact Alice is not involved in this session and M' was never sent from her even before this session. In our model, the attacker cannot initiate a new authenticated flow. Hence, the authenticated flow in an impersonation attack constitutes of a replay of a previous authenticated flow sent by Alice.

On the other hand, a substitution attack occurs when Alice initiates a session with Bob, and tries to send him a message M. Then, the attacker substitutes M' instead of M, so,

Bob receives M' and not M. The adversary may have changed part or all of M to get M'. The authenticated flow cannot be substituted according to the model, and hence the potential changes occur in the broadband channel.

Moreover, we assume that the adversary can make Alice send a message that the adversary has chosen. This ability of the adversary may not be considered in all models. We do consider it in our model since it makes the adversary stronger and results in a stronger level of security. In other words, the adaptive chosen plaintext attack (ACPA) model is considered here. The ACPA model is very strong and desirable compared to other models. It consists of two stages: an *information gathering* stage and a *deception* stage. In addition, we assume that the attacker has precomputing capabilities and is able to mount "dictionary-type" attacks.

The term *offline complexity* is used to refer to the computational complexity T of an adversary. The term *online complexity* refers to the number q of messages sent by Alice to Bob during the information gathering stage.

In the information gathering stage, the adversary adaptively chooses q messages and makes Alice send them to Bob. The communication is then recorded for further use. The adversary hopes that this stage of an attack gradually reveals information about the unknown aspects of the protocol.

The deception stage usually happens after the information gathering phase. To consider stronger adversaries, we allow the last query of the information gathering stage to happen concurrently with the deception stage. The attacker tries to make Bob accept a message M' along with the identity of Alice, when he was supposed to reject. We note that the message M' should be different from all the messages previously sent by Alice, otherwise, we consider the "attack" only a "replay".

3. Previous Message Authentication Protocols

As it was mentioned in Sections 1.1 and 1.2, there have been many NIMAPs and IMAPs proposed in the literature. For the analysis and performance of NIMAPs we refer the reader to [7]. Authenticated key agreement of Hoepman [4] is analyzed in [11]. Here, we only analyze one IMAP, mainly Vaudenay IMAP.

3.1. **Vaudenay IMAP.**

Vaudenay [11] was the first to formalize the narrow-band authenticated channel and also proposed a three round interactive IMAP with three flows on the broadband channel and one last flow on the authenticated channel. This protocol, depicted in Figure 1, is in the Common Reference String (CRS) model. In other words, it is assumed that a random string K_p has been previously distributed to everyone.

There are three algorithms employed in Vaudenay IMAP:

- *setup* generates the random parameter K_p and k_s. K_p is public whereas K_s is a private variable.
- $commit(m, r)$ is usually a randomized algorithm that produces two values: a commit value c and an decommit value d.
- $open(m, c, d)$ is a deterministic algorithm that either outputs r or an error signal.

The algorithms *open* and *commit* are designed in a way that whenever there is a value r so that $commit(m, r) = (c, d)$, the output of $open(m, c, d)$ is going to be r.

The probability of an adversary attacking this protocol , with online complexity $q = 1$, is proven to be ϵ, where $k \approx \log(1/\epsilon)$, under the assumption that a certain type of commitment schemes exist. In [5] Laur, Asokan and Nyberg showed that a non-malleable commitment scheme will guarantee the security of Vadenay IMAP. There are some proposals for

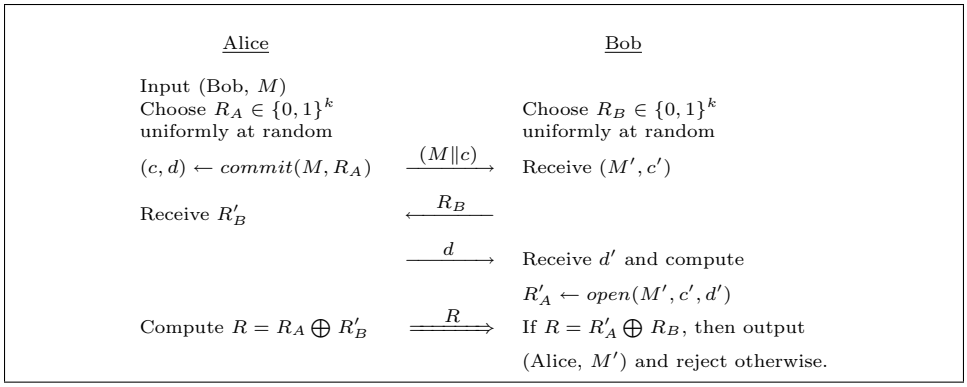

FIGURE 1. Vaudenay IMAP

non-malleable commitment schemes in the literature, but either the construction is inefficient or it requires a trusted infrastructure which is not practical for an ad hoc network.

4. A new Interactive Message Authentication Protocol.

In this section, we begin by defining Interactive-Collision Resistance (ICR) for hash functions. Then, we continue by analyzing the problem of finding Interactive-Collisions. Finally, we introduce a new IMAP based on Interactive-Collision Resistant hash functions. The security of this IMAP is based on the hardness of the ICR problem.

4.1. **Interactive-Collision Resistance.**

A hash function H is said to be Interactive-Collision Resistant (ICR) if the game of Figure 2 is hard to win, for fixed values of l_1 and l_2. In addition, H is a (T, ϵ)-ICR hash function if an adversary with computational complexity T wins the ICR game with probability at most ϵ.

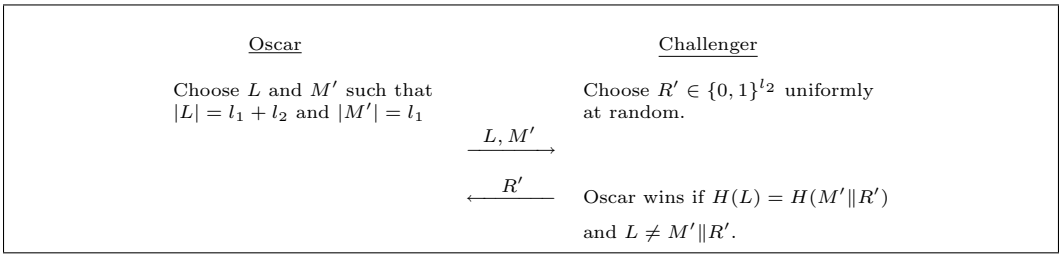

FIGURE 2. ICR Game

Furthermore, the pair $(L, M'\|R')$ is called an *interactive-collision*.

Note that, if $l_2 = 0$, then ICR is equivalent to Collision Resistant (CR)[1]. This suggests that finding collisions is not harder than finding interactive-collisions.

4.2. **On the difficulty of the ICR Game.**

To our knowledge, this is the first time that the problem of finding interactive-collisions is being investigated. We analyze the ICR Game in the Random Oracle Model. This analysis yields some insight about the hardness of the ICR Game compared to CR or Second-Preimage Resistant (SPR)[2].

[1]A hash function is collision resistant if it is hard to find two inputs that hash to the same output

[2]A hash function h is Second-Preimage Resistant, if given an input x, it is hard to find another input, y, $x \neq y$, such that $h(x) = h(y)$.

Let $\mathcal{X} = \{0,1\}^{l_1+l_2}$ be the set of all possible binary strings of size $l_1 + l_2$. Consider a hash function H chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$. In the random oracle model, we are only permitted oracle access to H. In other words, the only way to know the value of $H(x)$ is to query the value of x to the oracle. We assume that the adversary can access the Random Oracle for up to $T = 2^t$ times. We now find an upper bound on the probability ϵ of Oscar winning the ICR Game.

Oscar begins by querying $X_1, X_2, \ldots, X_T$ to the random oracle, where $|X_i| = l_1 + l_2$ for $1 \leq i \leq T$. Without loss of generality, we can assume that $X_i \neq X_j$, for $1 \leq i, j \leq T$, $i \neq j$. Let the pair $(L, M'\|R')$ be the interactive-collision found by Oscar. We write every X_i in the form of $X_i = M_i\|K_i$, where $|K_i| = l_2$ and $|M_i| = l_1$. There are two cases to consider here:

Case 1. L, M', and R' are all random values and it happens that L collides with $M'\|R'$, where $L \neq M'\|R'$.
Case 2. L and $M'\|R'$ are precomputed values, X_i and X_j yielding a collision, for some i and j, $1 \leq i, j \leq T$ and $X_i \neq X_j$.

We denote the probability of Case 1 and 2 occurring by ϵ_1 and ϵ_2, respectively. Clearly, $\epsilon \leq \epsilon_1 + \epsilon_2$.

Given random values L and M', the probability that $H(M'\|R') = y$ for a random value of R' is 2^{-k}, where $y = H(L)$. Hence, $\epsilon_1 \leq 2^{-k}$.

When L and $M'\|R'$ are precomputed by Oscar, it means that a collision has occurred among the T queried values. That is, a colliding pair (X_i, X_j) exists. The probability of a collision occurring among T random values is $\binom{T}{2}/2^k$. When $T = 2^t$, this can be written as 2^{2t-k-1}. Having found the pair (X_i, X_j), Oscar may let $L = X_i$ and $M'\|K' = X_j$, or $L = X_j$ and $M'\|K' = X_i$. Now, having found a colliding pair L and (M', R'), Oscar can only hope that R' is the value chosen by the challenger. The probability that the "correct" R' is chosen is 2^{-l_2}. Hence, we conclude that $\epsilon_2 \leq 2^{2t-k-l_2}$. Therefore, we have proven the following.

Lemma 1. *Let $\mathcal{X} = \{0,1\}^{l_1+l_2}$ be the set of all possible binary strings of size $l_1 + l_2$. Consider a hash function H chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$. Then, H is a $(2^t, \epsilon)$-ICR hash function in the Random Oracle model, where $\epsilon = 2^{-k}(1 + 2^{2t-l_2})$. In other words, any player with computational complexity $T = 2^t$ against the challenger of the ICR Game depicted in Figure 2 has a probability of success at most $\epsilon = 2^{-k}(1 + 2^{2t-l_2})$.*

4.3. **A new Interactive Message Authentication Protocol using ICR hash functions.** Let H be a (T, ϵ)-ICRHF and l_1 and l_2 be fixed parameters. We propose the following IMAP:

1. On input (M, Bob), Alice sends M over the insecure channel.
2. Bob receives M'.
3. Bob chooses $R \in \{0,1\}^r$ uniformly at random and he sends it to Alice.
4. Alice receives R'.
5. Alice computes $h = H(M\|R')$ and sends it over the authenticated channel.
5. Bob receives h'.
6. Bob computes $H(M'\|R)$.
7. Bob outputs (Alice, M') if $h' = H(M'\|R)$, and he rejects otherwise.

This IMAP is also illustrated in Figure 3. Next, we prove that this IMAP is secure given that the game on Figure 2 is hard to win. In other words, H is a (T, ϵ)-ICR hash function.

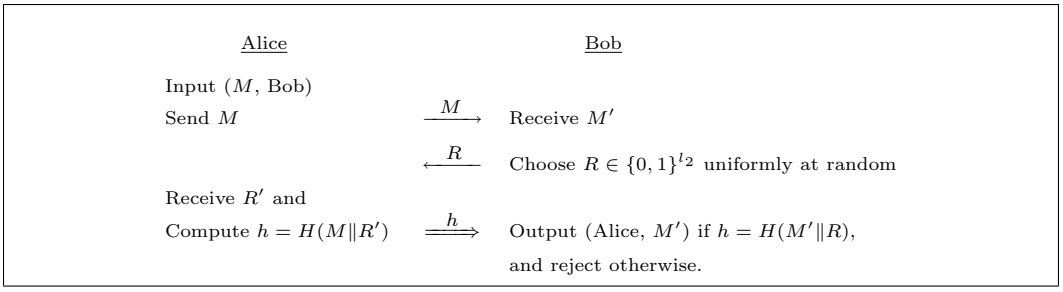

FIGURE 3. Interactive Message Authentication Protocol

5. Security Analysis

In this section, we analyze the security of the IMAP presented in Figure 3. The analysis begins by showing the equivalence between impersonation attacks and substitution attacks in our model. Then, it continues by introducing the IMAP Game in which winning this game is equivalent to attacking our proposed IMAP. Finally, the reduction of the ICR Game to the IMAP Game is shown.

5.1. **The equivalence of Substitution and Impersonation attacks.**

As it was mentioned previously, the goal of the adversary in attacking a MAP is to make the verifier, Bob, accept a message M' along with the identity of the claimant, Alice, when he was supposed to reject and, indeed, the message M' was never sent by Alice to Bob. There are two main ways of achieving this goal: by mounting impersonation attacks or substitution attacks.

5.1.1. *Impersonation Attack.* Figure 4 depicts the impersonation attack against our IMAP. Here, the attacker initiates a session herself and tries to convince Bob that a message M' is sent from Alice, while in fact M' was generated by herself and Alice has never sent M' to Bob.

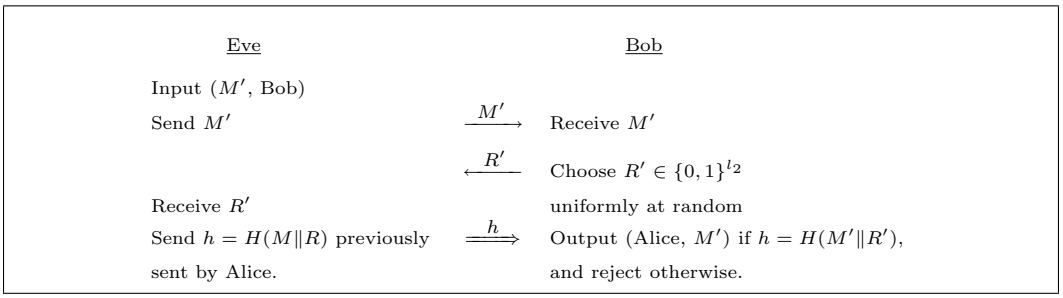

FIGURE 4. An Impersonation Attack Against IMAP

According to our model, the data sent over the authenticated channel, although public, cannot be modified by the adversary. Hence, Eve can only replay a previous flow sent by Alice, as shown in Figure 4.

5.1.2. *Substitution Attack.* Figure 5 is illustrating a substitution attack against our IMAP. In this attack, unlike the case of impersonation attack, Alice is the one who initiates the session with Bob and would like to authenticate M to him. The adversary, on the other hand, substitutes M' instead of M. Then, Bob receives M' and not M. The value of M' may be the result of a partial or total modification of M by the adversary. It is also possible that the

adversary changes R to R'. However, the value of h sent over the authenticated value cannot be substituted according to the model.

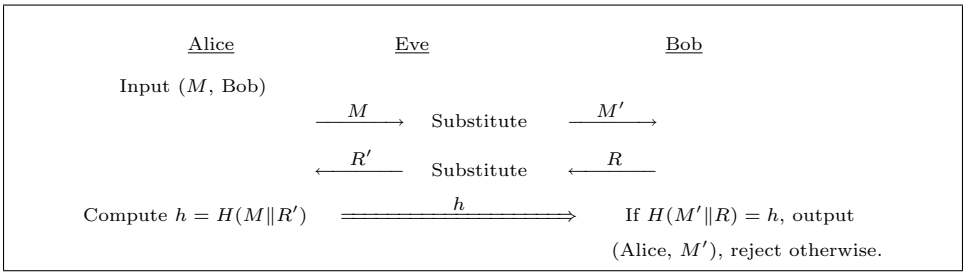

FIGURE 5. A Substitution Attack Against IMAP

5.1.3. *The Information Gathering Stage.* During the information gathering stage, the adversary can change the information sent over the broadband channel. For instance, the adversary may change R to R'. The value of R is supposed to be chosen by Bob, uniformly at random. The other value that is being sent over the broadband channel is the message M. However, our model allows the adversary to choose the message M to start with. Hence, there is no need for the adversary to intervene and change it to M'. This ability makes the adversary very strong. Since we are working in the ACPA model, the adversary can make Alice send q messages in the information gathering stage. This stage is depicted in Figure 6.

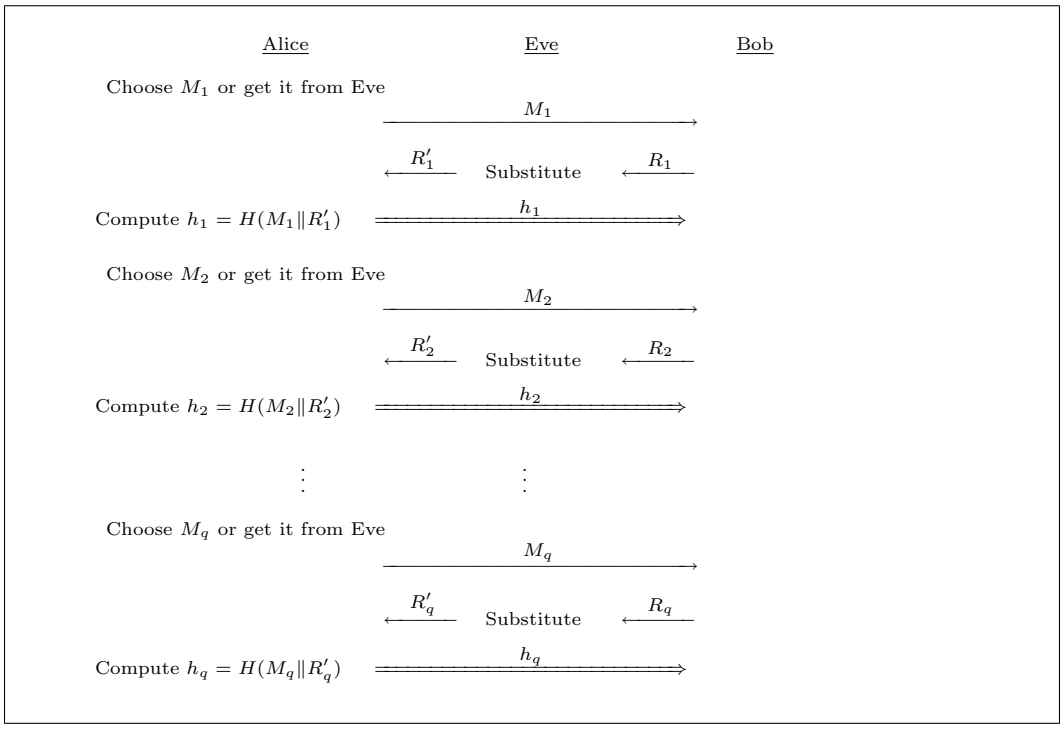

FIGURE 6. Information Gathering Phase of an Attack

5.1.4. *Equivalence of Impersonation and Substitution attacks in our Model.* Looking back at the substitution attack, the following is the order of flows happening in a substitution attack:

(1) Alice chooses M.
(2) Eve sends M' to Bob.
(3) Bob chooses a random value R.
(4) Eve chooses a random value R' and sends it to Alice.
(5) Alice computes $h = H(M\|R')$.
(6) Eve hopes that $h = H(M'\|R)$ and sends it to Bob.

Note that, the last query of the information gathering stage can happen concurrently with the deception stage. Considering this fact, we can break the substitution attack into two parts: the first part is the last query of the information gathering stage and the second part is an impersonation attack belonging to the deception stage. This is done by relabelling the flows of the substitution attack as follows. Consider the last query of the information gathering stage to be

(1) Alice chooses M.
(4) Eve chooses a random value R' and sends it to Alice.
(5) Alice computes $h = H(M\|R')$.

And, let the deception stage be

(2) Eve sends M' to Bob.
(3) Bob chooses a random value R.
(6) Eve replays $h = H(M\|R')$.

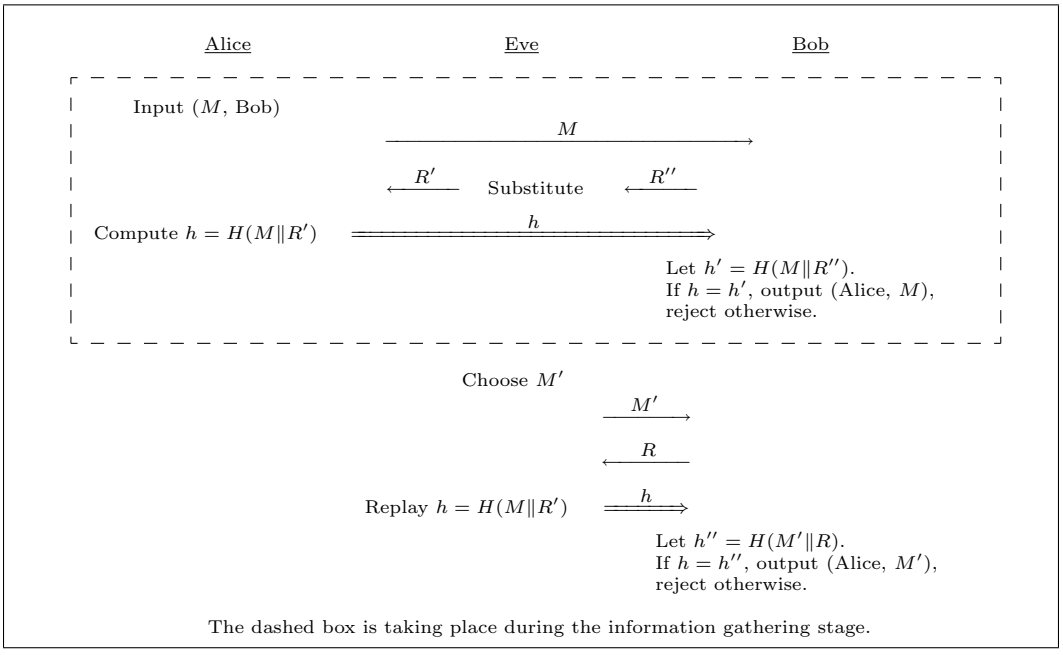

FIGURE 7. Equivalence of Impersonation and Substitution Attacks

This relabelling is illustrated in Figure 7. We note that the last query of the information gathering ends before the deception stage is completed.

The above discussion allows us, without loss of generality, to consider only impersonation attacks. This brings us to the deception stage where the attacker tries to impersonate Alice by sending M' and a replay of one of $h_1, \ldots, h_q$. Given that Alice has never sent M', the adversarial goal is achieved if Bob accepts. This stage is depicted in Figure 8.

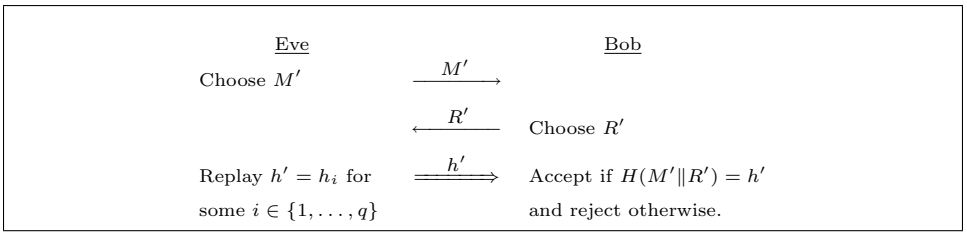

FIGURE 8. Deception Phase of an Attack

5.2. **IMAP Game.** We now prove that our IMAP is secure given that H is a (T, ϵ)-ICR hash function. In other words, an adversary who can attack the IMAP with non-negligible probability can also win the ICR Game with non-negligible probability.

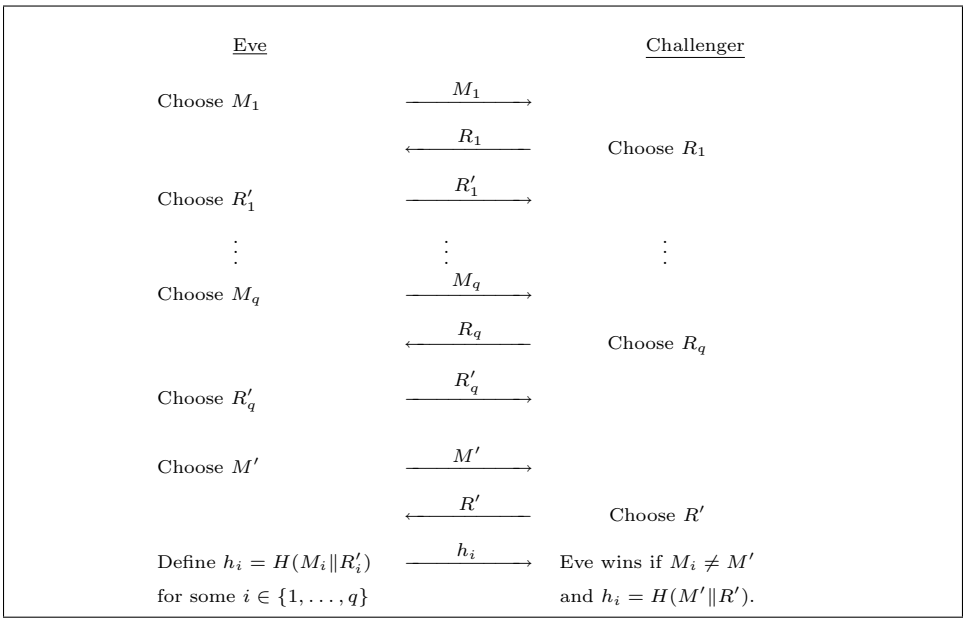

FIGURE 9. IMAP Game

Consider the game illustrated in Figure 9. If Eve wins this game with probability ϵ, then obviously we can translate the game into an attack against our IMAP with success probability ϵ. As a result, this game is named the "IMAP Game". Here, Eve is simulating the adversary of the IMAP and is facing a challenger who is simulating Alice and Bob at the same time.

The first q rounds, analogous to the information gathering stage of an attack, consist of Eve sending messages M_i and the challenger responding with R_i. Eve is allowed to change the values sent by Bob and as a result she responds with R'_i after each round. In the last round of the game, corresponding to the deception phase, Eve sends her messages M', $M' \neq M_i$

for every $i \in \{1, \ldots, q\}$. After receiving a random value R' from the challenger, she sends $h_i = H(M_i \| R_i)$, for some $i \in \{1, \ldots, q\}$. Eve wins the game if $h_i = H(M' \| R')$ for $M_i \neq M'$.

Assuming that Eve wins the IMAP Game of Figure 9 with non-negligible probability, we can employ her in the ICR Game depicted in Figure 2. This reduction is illustrated in Figure 10. In this reduction, Eve is playing against her IMAP Game Challenger and Oscar is playing against his ICR Game Challenger. The result of the IMAP Game, played by Eve, is going to be used in the ICR Game, played by Oscar. The dashed box highlights the the part corresponding to the ICR Game. Note, Eve does not see any difference between this game and the game of Figure 9.

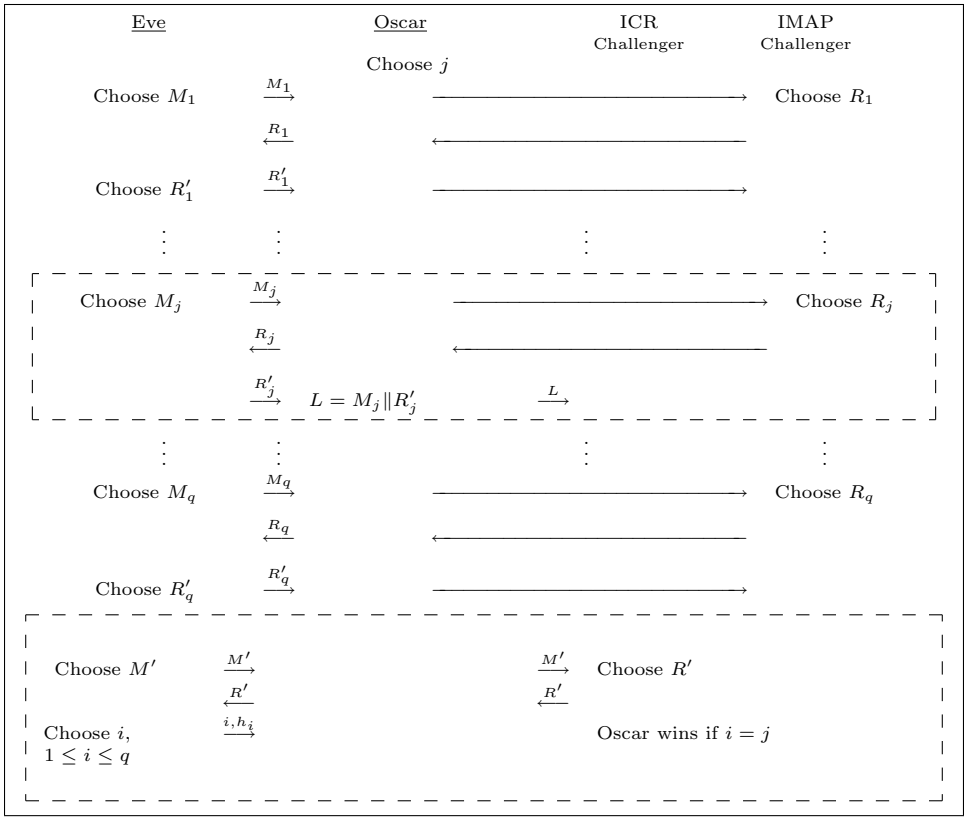

FIGURE 10. Reducing the ICR Game to the IMAP Game

Oscar begins by choosing a random value $j \in \{1, \ldots, q\}$. Then, he lets Eve continue playing against the IMAP Challenger by sending messages M_t, receiving R_t, and sending R'_t. The flows continue in this manner except when $t = j$. For $t = j$, Oscar forwards $L = M_j \| R'_j$ to the ICR Challenger.

At the deception stage, Eve sends a message M'. Oscar sends M' to his challenger and receives R'. He then sends R' to Eve. Eve responds with a value h_i, $i \in \{1, \ldots, q\}$. Eve wins if $h_i = H(M' \| R')$. If $i = j$ and Eve wins, then Oscar wins the ICR Game, and loses otherwise.

If we assume that Eve can win IMAP Game with probability ϵ, then Oscar wins the ICR Game with probability ϵ/q. Thus, we have proven the following.

Theorem 1. *Let H be a (T, ϵ)-ICR hash function. Then, any adversary against the IMAP of Figure 3, with offline complexity T and online complexity q, has a probability of success p at most $q\epsilon$.*

When $q = 1$, adversaries with probability of success 2^{-k} clearly exist, and hence, the reduction is tight. For $q \neq 1$, the probability of success is $q2^{-k}$. This factor q appears as a consequence of considering strong adversaries who can request q messages to be sent by Alice. Some papers only consider $q = 1$ resulting in a weaker notion of security[3]. However, the approach of many other papers is similar to our paper[4].

Putting Lemma 1 and Theorem 1 together, we obtain the following corollary.

Corollary 1. *Let $\mathcal{X} = \{0,1\}^{l_1+l_2}$ be the set of all possible binary strings of size $l_1 + l_2$ and H be a hash function chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$. Then, any adversary against the IMAP of Figure 3, with offline complexity T and online complexity q, has a probability of success $p \leq q2^{-k}(1 + 2^{2t-l_2})$.*

5.3. **Parameter sizes.** Let us assume that the adversary is allowed to carry out $T = 2^t$ hash computations and make Alice send q messages to Bob. In other words, T and q are the offline and online complexities of the attacker, respectively. Moreover, H be a (T, ϵ)-ICR hash function of output size k.

Corollary 1 says that an adversary attacking our proposed IMAP, using T hash computations and q messages, has probability of success p at most $q2^{-k}(1 + 2^{2t-l_2})$.

We target typical[5] parameters $q \leq 2^{10}$, $t \leq 70$, and $p \leq 2^{-20}$. If we take $l_2 \geq 160$, then we can basically ignore the factor $(1 + 2^{2t-l_2})$. We note that, since the random values R are being sent over the insecure channel, this assumption does not have any impact on the analysis or usefulness of our protocol.

With the parameters of interest, we require $k \geq 30$ to obtain a success probability $p \leq 2^{-20}$. Note that, these choices of parameters require only 30 bits to be transmitted over the narrow-band channel. This is a distinct improvement over the previous NIMAPs and IMAPs.

5.4. **Advantages of the proposed IMAP.** The proposed IMAP of Figure 3 has three flows and utilizes hash functions instead of commitment schemes. This yields an advantage of having a simple and easy to implement structure.

Our security assumptions are reasonable and are based on the existence of an ICR hash function. We do not require any previously distributed public parameters, which are needed in the CRS model.

The amount of information sent over the authenticated channel is smaller than the most secure IMAP proposed so far, while achieving the same level of security.

6. Conclusion

Working in the ACPA model, we assumed that the communication is taking place over two different channels: an insecure broadband channel and an authenticated narrow-band channel.

Having examined the most secure and efficient IMAPs and NIMAPs found in the literature, we proposed a new IMAP based on ICR hash functions, a new notion that we have defined. Given a secure ICR hash function, we proved that our IMAP is secure.

Our IMAP performs better than other IMAPs and NIMAPs in the literature. While achieving the same level of security, the amount of information required to be sent over the authenticated channel in our IMAP is smaller. Moreover, our IMAP works under fewer security assumptions compared to other IMAPs in the literature.

[3]See [8] for instance.

[4]For instance, in [11], it is assumed that $q \leq 2^{10}$ and the reduction is not tight. They also get the same probability of success, p/q.

[5]See for instance [7] and [9].

Acknowledgements

Douglas R. Stinson's research is supported by NSERC discovery grant 203114-06. Atefeh Mashatan is supported by an NSERC PGSD Scholarship. Part of this research was done when A. Mashatan was visiting the Fields Institute, Research in Mathematical Sciences, in Toronto, Canada.

References

[1] Dirk Balfanz, Diana K. Smetters, Paul Stewart, and H. Chi Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *Network and Distributed Sytem Security Symposium*, San Diego, California, U.S.A., February 2002.

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

[3] Christian Gehrmann, Chris J. Mitchell, and Kaisa Nyberg. Manual authentication for wireless devices. *RSA Cryptobytes*, 7(1):29–37, January 2004.

[4] Jaap-Henk Hoepman. The ephemeral pairing problem. In *Financial Cryptography*, pages 212–226, 2004.

[5] Sven Laur, N. Asokan, and Kaisa Nyberg. Efficient mutual data authentication using manually authenticated strings: Preliminary version. Cryptology ePrint Archive, Report 2005/424, 2005. Shorter more compact version was published at CANS 2006.

[6] Sven Laur and Kaisa Nyberg. Efficient mutual data authentication using manually authenticated strings. In *The 5th International Conference on Cryptology and Network Security, CANS 2006, Suzhou, Dec. 8 - 10, 2006*, volume 4301 of *Lecture Notes in Computer Science*. Springer, 2006. To appear. It is a shortened version of ePrint Report 2005/424.

[7] Atefeh Mashatan and Douglas R. Stinson. Noninteractive two-channel message authentication based on hybrid-collision resistant hash functions. Cryptology ePrint Archive, Report 2006/302, 2006. http://eprint.iacr.org/.

[8] M. Naor, G. Segev, and A. Smith. Tight bounds for unconditional authentication protocols in the manual channel and shared key models. *In Advances in Cryptology - CRYPTO '06*, pages 214–231, 2006.

[9] Sylvain Pasini and Serge Vaudenay. An optimal non-interactive message authentication protocol. In David Pointcheval, editor, *Topics in Cryptography*, volume 3860 of *Lecture Notes in Computer Science*, pages 280–294, San Jose, California, U.S.A., February 2006. Springer-Verlag.

[10] Ronald L. Rivest and Adi Shamir. How to expose an eavesdropper. *Commun. ACM*, 27(4):393–394, 1984.

[11] Serge Vaudenay. Secure communications over insecure channels based on short authenticated strings. In Victor Shoup, editor, *Advances in Cryptography*, volume 3621 of *Lecture Notes in Computer Science*, pages 309–326, Sanra Barbara, California, U.S.A., August 2005. Springer-Verlag.