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 based on the computational assumption that ICR hash functions exist. It performs better than message authentication protocols that are based on computational assumptions. 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 Non-interactive Message Authentication Protocol (NIMAP) in the literature. In other words, if we send the same amount of information over the authenticated channel, we can allow much stronger adversaries compared to the existing protocols 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.

Keywords: Two-channel Cryptography, Authenticated Channel, Message Authentication, Hash Functions.

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.

An ad-hoc network is a network where some of the users are part of the network only for a short period of time.

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, entity authentication, and data confidentiality. However, these properties might not be equally desirable compared to one another. For instance, it might be less important to provide entity authentication, as compared to message authentication, because an ad hoc network permits

Date: August 24, 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

.

users to easily join the network or leave the network. This fact has led the research in this area more towards providing tools for message authentication.

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 [9] 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 other's 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 [3] and [2].

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 [9] 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.** Hash based NIMAPs first appeared in [10] as fingerprints of public keys in PGP. Later, Balfanz et al proposed a NIMAP in [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.

Gehrmann, Mitchell and Nyberg [2] proposed several protocols which they called MANA I, MANA II, etc. The original version of this protocol is not a NIMAP and requires confidentiality in the authenticated channel. Vaudenay proposed a noninteractive version of MANA I in [11]. He has also proved that a "stall-free" authenticated channel is enough to ensure the security of MANA I.

The next NIMAP was proposed by Pasini and Vaudenay [8] 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 [5] and [6] 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 [5] and [6].

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. For instance, having a bidirectional channel may cost more than a unidirectional channel, or devices may have different computational capabilities, allowing one device to be the master and the other be the slave in the communication. However, we note that NIMAPs achieve a strictly weaker notion of security when compared to IMAPs. This is because NIMAPs provably cannot protect against replay attacks of the authenticated flow, while IMAPs can.

The IMAP presented in this paper is based on a computational assumption. As a result, we can only compare its security and efficiency to similar IMAPs that are based on computational assumptions. There are unconditionally secure IMAPs in the literature; see for example [7].

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. We note that, the possibility that the adversary does online computations has not been considered in this protocol.

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. Both substitution and impersonation attacks are analyzed in this 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. In the ACPA model, the adversary has offline computational power and can make the users send messages of adversary's choice. In this paper, we give further power to the adversaries by allowing them to have online

computational power. That is, they are allowed to do hash function computations, or make oracle queries, while they are in the middle of an attack.

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 a better level of security, while benefitting from an efficient structure and having to send fewer bits over the authenticated channel. To reiterate, if we want to send the same amount of information, then we can assume much stronger adversaries in terms of online computational complexity.

The rest of this paper is organized as follows. In Section 2, the attack model, i.e., adversarial goal and capabilities, are defined. In Section 3, Interactive-Collision Resistance (ICR), a new notion for hash function security, is defined and analyzed. Finally, an IMAP based on ICR hash functions is proposed. We prove in Section 4 that our IMAP is secure given that we use ICR hash functions. The security of our IMAP is analyzed in Section 4. Finally, we comment on parameter sizes for our IMAP in 5. We conclude with listing the advantages of our IMAP in 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. Moreover, the adversary can replay a previous flow of 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). This message M could be a key that is going to be used for further communication.

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 M' was never sent from Alice. 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 authenticated flow cannot be substituted according to the model, and hence any potential changes occur in the broadband channel. There are two types of substitution attacks; see Section 4.

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 more powerful and results in a stronger level of security. The adaptive chosen plaintext attack (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 $T_{\text{off}} = 2^{t_{\text{off}}}$ of an adversary up to and including the information gathering stage. The term *online complexity* refers to the computational complexity $T_{\text{on}} = 2^{t_{\text{on}}}$ of an adversary during the deception stage of a substitution attack. Furthermore, the number of messages sent by Alice to Bob during the information gathering stage is denoted by q.

In the information gathering stage, the adversary is allowed to adaptively choose q messages and make 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 happens after the information gathering phase. 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. A new Interactive Message Authentication Protocol.

We begin by defining new notions of hash function security called Interactive-Collision Resistance (ICR). We continue by introducing a new IMAP based on ICR hash functions. The security of this IMAP is based on the hardness of the ICR problems.

3.1. **Interactive-Collision Resistance.**

In this section, we begin by defining Interactive-Collision Resistance I, II and III (ICRI, ICRII, and ICRIII respectively) for hash functions. Then, we state and prove three lemmas about the security of ICRI, ICRII, and ICRIII hash functions.

To our knowledge, this is the first time that the problem of finding interactive-collisions of type I, II, and III are being investigated. We analyze the ICRI, ICRII, and ICRIII Games in the Random Oracle Model. This analysis yields some insight about the hardness of these games

compared to Collision Resistance (CR)[1] or Second-Preimage Resistance (SPR)[2]. Note that, we do not have any concrete constructions for designing such hash functions in the standard model. We pose this as an open problem.

Definition 1. *A hash function H is* **Interactive-Collision Resistant** I (ICRI) *if the game of Figure 1 is hard to win, for fixed values of ℓ_1, ℓ_2, and ℓ_3. In addition, the pair $(M\|K\|R', M'\|K'\|R)$ is called an interactive-collision of type* I. *Furthermore, we call H a $(T_{\text{off}}, \epsilon_1)$-ICR*I hash function if an adversary, who can make up to T_{off} hash function computations, wins the ICRI game with probability at most ϵ_1.

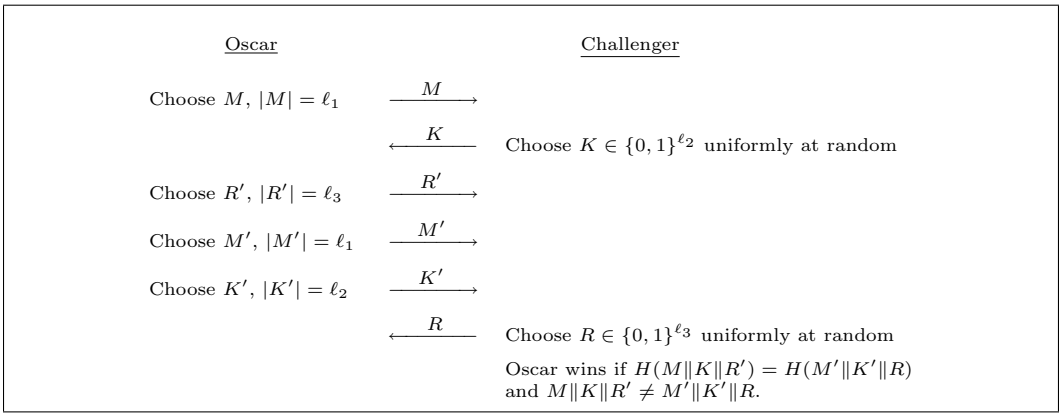

FIGURE 1. ICRI Game

Note that, if $\ell_2 = \ell_3 = 0$, then ICRI is equivalent to Collision Resistance (CR). Further, if $\ell_1 = \ell_3 = 0$, then ICRI is equivalent to Second-Preimage Resistant (SPR). In fact, ICRI is interpolating between CR and SPR. This suggests that, solving ICRI Game is harder than finding collisions, but not harder than finding second-preimages.

We can analyze the security of ICRI hash functions, or in other words the hardness of the ICRI Game, in the random oracle model. This will give us an intuition on how difficult this game is, as compared to former notions of hash function security. Let $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$ denote the set of all functions from a domain $\mathcal{X}$ to a range $\mathcal{Y}$.

Lemma 1. *Let $\mathcal{X} = \{0,1\}^{\ell_1+\ell_2+\ell_3}$ be the set of all possible binary strings of size $\ell_1 + \ell_2 + \ell_3$. Consider a hash function H chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$. Then, H is a $(2^{t_{\text{off}}}, \epsilon_1)$-ICR*I hash function in the Random Oracle model, where $\epsilon_1 = 2^{-k}(2 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3})$. In other words, any player with computational complexity $T_{\text{off}} = 2^{t_{\text{off}}}$ against the challenger of the ICRI Game has a probability of success at most $\epsilon_1 = 2^{-k}(2 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3})$.

We consider $\mathcal{X} = \{0,1\}^{\ell_1+\ell_2+\ell_3}$, the set of all possible binary strings of size $\ell_1 + \ell_2 + \ell_3$, and let a hash function H be chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$.

Assume that we are only permitted oracle access to H, that is we are working in the random oracle model. We let the adversary have access to the Random Oracle for $T_{\text{off}} = 2^{t_{\text{off}}}$ times. Given these conditions, we are looking for the probability ϵ_1 of Oscar winning the ICRI Game.

[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 $\mathcal{X} = \{X_1, X_2, \ldots, X_{T_{\text{off}}}\}$ be the queries of Oscar to the random oracle, where $|X_i| = \ell_1 + \ell_2 + \ell_3$ for $1 \leq i \leq T_{\text{off}}$. Without loss of generality, we assume that X_is are distinct, for $1 \leq i, j \leq T_{\text{off}}$.

Consider the pair $(Y, Y') = (M\|K\|R', M'\|K'\|R)$, the interactive-collision found by Oscar, and write X_is in the form of $X_i = M_i\|K_i\|R_i'$, where $|M_i| = \ell_1$, $|K_i| = \ell_2$ and $|R_i'| = \ell_3$.

Let E denote the event that $H(Y) = H(Y')$ and D denote the event that a colliding pair (X_i, X_j) exists, $X_i, X_j \in \mathcal{X}$. We want to find an upper bound on $\Pr[E]$. We will do this by conditioning on the event D:

$$\begin{aligned}\Pr[E] &= \Pr[\neg D] \times \Pr[E|\neg D] + \Pr[D] \times \Pr[E|D] \\ &\leq \Pr[E|\neg D] + \Pr[D] \times \Pr[E|D] \\ &= \Pr[E|\neg D] + \Pr[D \text{ and } E].\end{aligned}$$

Denote $\epsilon_{11} = \Pr[E|\neg D]$ and $\epsilon_{12} = \Pr[D \text{ and E}]$. We will compute upper bounds on ϵ_{11} and ϵ_{12}.

Let D_1 denote the event that $Y \notin \mathcal{X}$, yet it collides with $Y' = X_k$, for some $X_k \in \mathcal{X}$.

$$\begin{aligned}\epsilon_{11} &= \Pr[E|\neg D] \\ &= \Pr[\neg D_1] \times \Pr[E|\neg D \text{ and } \neg D_1] + \Pr[D_1] \times \Pr[E|\neg D \text{ and } D_1] \\ &\leq \Pr[E|\neg D \text{ and } \neg D_1] + \Pr[D_1] \times \Pr[E|\neg D \text{ and } D_1].\end{aligned}$$

The probability that $H(Y) = H(Y')$ when Y does not collide with any of the precomputed values is 2^{-k} due to the properties of random oracles. Hence, $\Pr[E|\neg D \text{ and } \neg D_1] = 2^{-k}$.

The probability that Y is not a precomputed value, yet it collides with a precomputed value $Y' = X_k$, is $T_{\text{off}} = 2^{t_{\text{off}}} 2^{-k}$. At this point Oscar hopes that he gets the "correct" R value from the Challenger. Hence, $\Pr[E|\neg D \text{ and } \neg D_1] = 2^{t_{\text{off}} - k - \ell_3}$. Hence, we obtain $\epsilon_{11} \leq 2^{-k} + 2^{t_{\text{off}} - k - \ell_3}$

Let D_2 denote the event that $Y \in \{X_i, X_j\}$ and $Y' \in \{X_i, X_j\} \setminus Y$.

$$\begin{aligned}\epsilon_{12} &= \Pr[D \text{ and E}] \\ &= \Pr[\neg D_2] \times \Pr[D \text{ and E}|\neg \text{D}_2] + \Pr[\text{D}_1] \times \Pr[\text{D and E}|\text{D}_2] \\ &\leq \Pr[D \text{ and } E|\neg D_1] + \Pr[D_2] \times \Pr[D \text{ and } E|D_2] \\ &= \Pr[D \text{ and } E|\neg D_2] + \Pr[E \text{ and } D \text{ and } \text{D}_2].\end{aligned}$$

When there is a colliding pair in $\mathcal{X}$, yet the colliding pair is not equal to neither (Y, Y') nor (Y', Y), the probability that $H(Y) = H(Y')$ is 2^{-k} in the random oracle model. Hence, $\Pr[D \text{ and } E|\neg D_2] = 2^{-k}$.

When D, D_2 and E occur at the same time, it means that $Y = M\|K\|R'$ and $Y' = M'\|K'\|R$ are among the precomputed values by Oscar. That is a collision is found among the T_{off} queried values, Oscar is sending M, M', K', and R', and he is hoping to get the "correct" R and K from the Challenger. We know that the probability of finding a collision among T_{off} random values is $\binom{T_{\text{off}}}{2}/2^k$. This is approximately equal to $2^{2t_{\text{off}} - k - 1}$ when $T_{\text{off}} = 2^{t_{\text{off}}}$. Having found a colliding pair (X_i, X_j), Oscar lets $(Y, Y') = (X_i, X_j)$ or $(Y, Y') = (X_j, X_i)$. Then, the probability that the "correct" K and R are chosen is $2^{-\ell_2 - \ell_3}$. Hence, we conclude that $\Pr[E \text{ and } D \text{ and } D_2] = 2^{2t_{\text{off}} - k - \ell_2 - \ell_3}$. This concludes that $\epsilon_{12} \leq 2^{-k} + 2^{2t_{\text{off}} - k - \ell_2 - \ell_3}$.

The above discussion concludes the proof of Lemma 1. To reiterate the Lemma, one can say that any player with computational complexity $T_{\text{off}} = 2^{t_{\text{off}}}$ against the challenger of the ICRI Game has a probability of success at most $\epsilon_1 = 2^{-k}(2 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3})$.

We now define Interactive-Collision Resistance II.

Definition 2. *A hash function H is* **Interactive-Collision Resistant** II (ICRII) *if the game of Figure 2 is hard to win, for fixed values of ℓ_1, ℓ_2, and ℓ_3. The pair $(M\|K\|R', M'\|K'\|R)$ is called an interactive-collision of type* II. *Furthermore, we call H a $(T_{\text{off}}, T_{\text{on}}, \epsilon_2)$-ICR*II hash function if an adversary with offline complexity T_{off} and online complexity T_{on} wins the ICRII Game with probability at most ϵ_2.

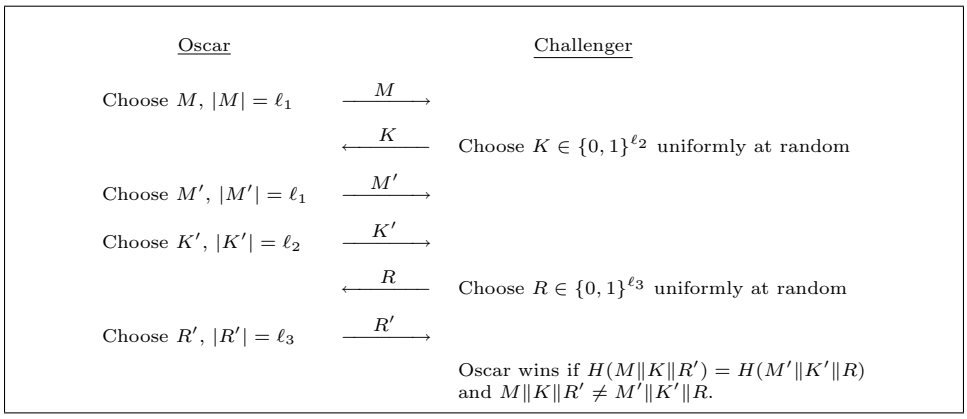

FIGURE 2. ICRII Game

Next, we define Interactive-Collision Resistant III (ICRIII).

Definition 3. *A hash function H is* **Interactive-Collision Resistant** III (ICRIII) *if the game of Figure 3 is hard to win, for fixed values of ℓ_1, ℓ_2, and ℓ_3. The pair $(M\|K\|R', M'\|K'\|R)$ is called an interactive-collision of type* III. *Furthermore, we call H a $(T_{\text{off}}, T_{\text{on}}, \epsilon_3)$-ICR*III hash function if an adversary with offline complexity T_{off} and online complexity T_{on} wins the ICRIII Game with probability at most ϵ_3.

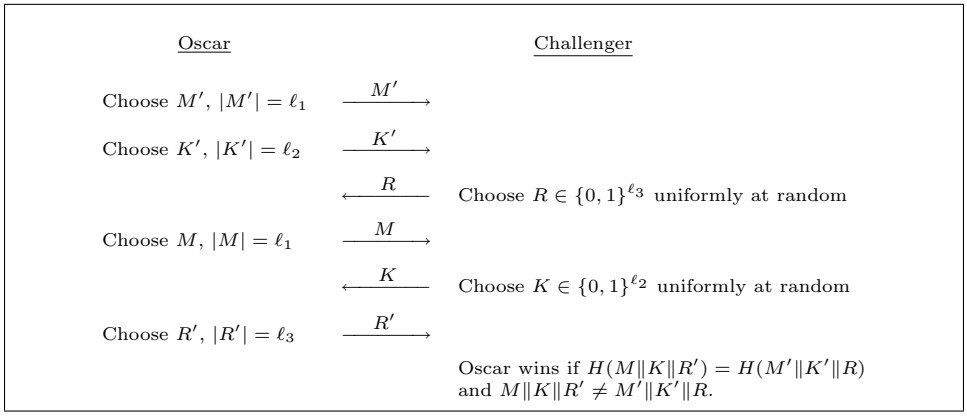

FIGURE 3. ICRIII Game

As in ICRI, if $\ell_2 = \ell_3 = 0$, then ICRII and ICRIII are equivalent to Collision Resistance. As a result, we conclude that finding collisions is not harder than finding interactive-collisions of type II and III.

Similar to ICRI, we analyze the security of ICRII and ICRIII hash functions in the random oracle model to have an intuition on how difficult it is win ICRII or ICRIII Games.

Lemma 2. *Let $\mathcal{X} = \{0,1\}^{\ell_1+\ell_2+\ell_3}$ be the set of all possible binary strings of size $\ell_1 + \ell_2 + \ell_3$. Consider a hash function H chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$. Then, H is a $(2^{t_{\text{off}}}, 2^{t_{\text{on}}}, \epsilon_2)$-ICR*II hash function in the Random Oracle model, where $\epsilon_2 = 2^{-k}(1 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3} + 2^{t_{\text{on}}})$. In other words, any player with offline computational complexity $T_{\text{off}} = 2^{t_{\text{off}}}$ and online complexity $T_{\text{on}} = 2^{t_{\text{on}}}$ against the challenger of the ICRII Game has a probability of success at most $\epsilon_2 = 2^{-k}(2 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3} + 2^{t_{\text{on}}})$.

Lemma 3. *Let $\mathcal{X} = \{0,1\}^{\ell_1+\ell_2+\ell_3}$ be the set of all possible binary strings of size $\ell_1 + \ell_2 + \ell_3$. Consider a hash function H chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$. Then, H is a $(2^{t_{\text{off}}}, 2^{t_{\text{on}}}, \epsilon_3)$-ICR*III hash function in the Random Oracle model, where $\epsilon_3 = 2^{-k}(1 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3} + 2^{t_{\text{on}}})$. In other words, any player with offline computational complexity $T_{\text{off}} = 2^{t_{\text{off}}}$ and online complexity $T_{\text{on}} = 2^{t_{\text{on}}}$ against the challenger of the ICRIII Game has a probability of success at most $\epsilon_3 = 2^{-k}(2 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3} + 2^{t_{\text{on}}})$.

The proof of these lemmas are similar and we only prove Lemma 2 here.

Let H again be a random oracle and assume that the adversary can access the Random Oracle for up to $T_{\text{off}} = 2^{t_{\text{off}}}$ times before he receives the last flow from the Challenger, i.e. R in the ICRII and K in the ICRIII. Furthermore, he can access the Random Oracle for up to $T_{\text{on}} = 2^{t_{\text{on}}}$ times after he receives the last flow from the Challenger and before he sends the value of R'. We now find an upper bound on the probability ϵ_2 of Oscar winning the ICRII Game.

Let the pair $(Y, Y') = (M\|K\|R', M'\|K'\|R)$ be the interactive-collision of type II found by Oscar. Further, let $\mathcal{X} = \{X_1, \ldots, X_{T_{\text{off}}}\}$ be Oscar's inputs to the random oracle before he receives the value of R from the Challenger, and $\mathcal{Y} = \{Y_1, \ldots, Y_{T_{\text{on}}}\}$ be his inputs to the random oracle after he received the value of R. Without loss of generality, we assume that $X_1, \ldots, X_{T_{\text{off}}}, Y_1, \ldots, Y_{T_{\text{on}}}$ are all distinct. We write each X_i or Y_i in the form of $M_i\|K_i\|R'_i$, where $|M_i| = \ell_1$, $|K_i| = \ell_2$ and $|R'_i| = \ell_3$.

Let E denote the event that $H(Y) = H(Y')$ and D denote the event that a colliding pair (X_i, X_j) exists, $X_i, X_j \in \mathcal{X}$. We want to find an upper bound on $\Pr[E]$. This is done by conditioning on the event D:

$$\begin{aligned}\Pr[E] &= \Pr[\neg D] \times \Pr[E|\neg D] + \Pr[D] \times \Pr[E|D] \\ &\leq \Pr[E|\neg D] + \Pr[D] \times \Pr[E|D] \\ &= \Pr[E|\neg D] + \Pr[D \text{ and } E].\end{aligned}$$

Denote $\epsilon_{21} = \Pr[E|\neg D]$ and $\epsilon_{22} = \Pr[D \text{ and E}]$. We note that ϵ_{22} is found by the same argument we used in the proof of Lemma 1 for finding ϵ_{12}. Hence, $\epsilon_{22} \leq 2^{-k} + 2^{2t_{\text{off}}-k-\ell_2-\ell_3}$. We now find an upper bound on $\epsilon_{21} = \Pr[E|\neg D]$.

Let D_1 denote the event that $Y \notin \mathcal{X}$, yet it collides with $Y' = X_k$, for some $X_k \in \mathcal{X}$.

$$\begin{aligned}\epsilon_{11} &= \Pr[E|\neg D] \\ &= \Pr[\neg D_1] \times \Pr[E|\neg D \text{ and } \neg D_1] + \Pr[D_1] \times \Pr[E|\neg D \text{ and } D_1] \\ &\leq \Pr[E|\neg D \text{ and } \neg D_1] + \Pr[D_1] \times \Pr[E|\neg D \text{ and } D_1].\end{aligned}$$

The probability that Y is not a precomputed value, but collides with a precomputed value $Y' = X_k$, is $T_{\text{off}} = 2^{t_{\text{off}}} 2^{-k}$. At this point Oscar hopes that he gets the "correct" R value from the Challenger. Hence, $\Pr[E|\neg D \text{ and } \neg D_1] = 2^{t_{\text{off}}-k-\ell_3}$.

It remains to find $\Pr[E|\neg D \text{ and } \neg D_1]$. We find this by conditioning on the event D_2 which we define to be the case when $Y \in \mathcal{Y}$.

$$\begin{aligned}\Pr[E|\neg D \text{ and } \neg D_1] &= \Pr[D_2] \times \Pr[E|\neg D \text{ and } \neg D_1 \text{ and } D_2] \\ &\quad + \Pr[\neg D_2] \times \Pr[E|\neg D \text{ and } \neg D_1 \text{ and } \neg D_2] \\ &\leq \Pr[D_2] \times \Pr[E|\neg D \text{ and } \neg D_1 \text{ and } D_2] + \Pr[E|\neg D \text{ and } \neg D_1 \text{ and } \neg D_2]\end{aligned}$$

The probability that Y and Y' collide while $Y \notin \mathcal{X}$ and $Y \notin \mathcal{Y}$ is 2^{-k} in the random oracle model. Hence, $\Pr[E|\neg D \text{ and } \neg D_1 \text{ and } \neg D_2] = 2^{-k}$.

When $Y \in \mathcal{Y}$, Oscar has $2^{t_{\text{on}}}$ choices for Y and then, the probability that Y collides with a determined Y' is $2^{t_{\text{on}}-k}$. Hence, $\Pr[D_2] \times \Pr[E|\neg D \text{ and } \neg D_1 \text{ and } D_2] = 2^{t_{\text{on}}-k}$.

This concludes that $\epsilon_{22} \leq 2^{t_{\text{off}}-k-\ell_3} + 2^{t_{\text{on}}-k} + 2^{-k}$.

This proves Lemma 2.

Finally, we define the notion of an Interactive-Collision Resistant hash function.

Definition 4. *A hash function H is* **Interactive-Collision Resistant (ICR)** *if the ICR*I, ICRII, and ICRIII Games are both hard to win.

Furthermore, H is said to be a $(T_{\text{off}}, T_{\text{on}}, \epsilon_1, \epsilon_2)$-ICR hash function if it is a $(T_{\text{off}}, \epsilon_1)$-ICRI hash function, a $(T_{\text{off}}, T_{\text{on}}, \epsilon_2)$-ICRII hash function, and a $(T_{\text{off}}, T_{\text{on}}, \epsilon_2)$-ICRIII hash function.

3.2. **A new Interactive Message Authentication Protocol using ICR hash functions.** Let H be a $(T_{\text{off}}, T_{\text{on}}, \epsilon_1, \epsilon_2)$-ICR hash function with fixed parameters ℓ_1, ℓ_2, and ℓ_3. We propose the following IMAP:

1. On input (M, Bob), Alice chooses $K \in \{0,1\}^{\ell_2}$ uniformly at random and sends $M\|K$ to Bob over the insecure channel.
2. Bob receives $M'\|K'$.
3. Bob chooses $R \in \{0,1\}^{\ell_3}$ uniformly at random and he sends it to Alice.
4. Alice receives R'.
5. Alice computes $h = H(M\|K\|R')$ and sends it over the authenticated channel.
5. Bob receives h'.
6. Bob computes $H(M'\|K'\|R)$.
7. Bob outputs (Alice, M') if $h' = H(M'\|K'\|R)$, and he rejects otherwise.

This IMAP is illustrated in Figure 4. Next, we prove that this IMAP is secure given that the three games on Figures 1, 2, and 3 are hard to win. In other words, if H is a $(T_{\text{off}}, T_{\text{on}}, \epsilon_1, \epsilon_2)$-ICR hash function, then the IMAP is secure.

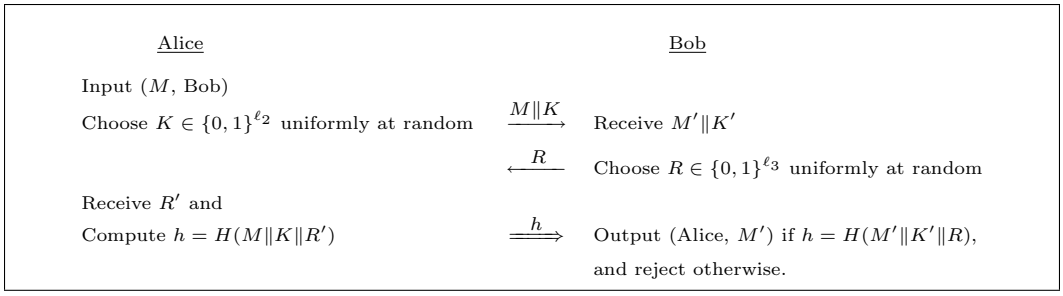

FIGURE 4. Interactive Message Authentication Protocol

4. Security Analysis

In this section, we analyze the security of the IMAP presented in Figure 4. We consider substitution and impersonation attacks separately. Associated with each attack scenario, an IMAP Game is introduced. Winning this game is equivalent to attacking our proposed IMAP. Finally, the reduction of the ICRI, and similarly ICRII and ICRIII, to the IMAP Game is shown.

As was mentioned earlier, the ACPA model consists of an information gathering stage and the deception stage.

4.1. **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', or K to K'. 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'. 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 5.

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. We will prove that a successful impersonation attack translates into winning the ICRI Game and a successful substitution attack is equivalent to winning either the ICRII Game or the ICRIII Game.

4.2. **Impersonation Attack.** Figure 6 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 the attacker and Alice never sent M' to Bob.

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 6. The attacker replays one of $h_1, \ldots, h_q$. Given that Alice has never sent M', the adversarial goal is achieved if Bob accepts.

4.2.1. *IMAP Game Against Impersonation Attacks.* We now prove that our IMAP is secure against impersonation attacks mounted by an adversary who has offline computational power T_{off} given that H is a $(T_{\text{off}}, \epsilon_1)$-ICRI hash function. In other words, an adversary who can attack the IMAP by mounting an impersonation attack with non-negligible probability can also win the ICRI Game with non-negligible probability.

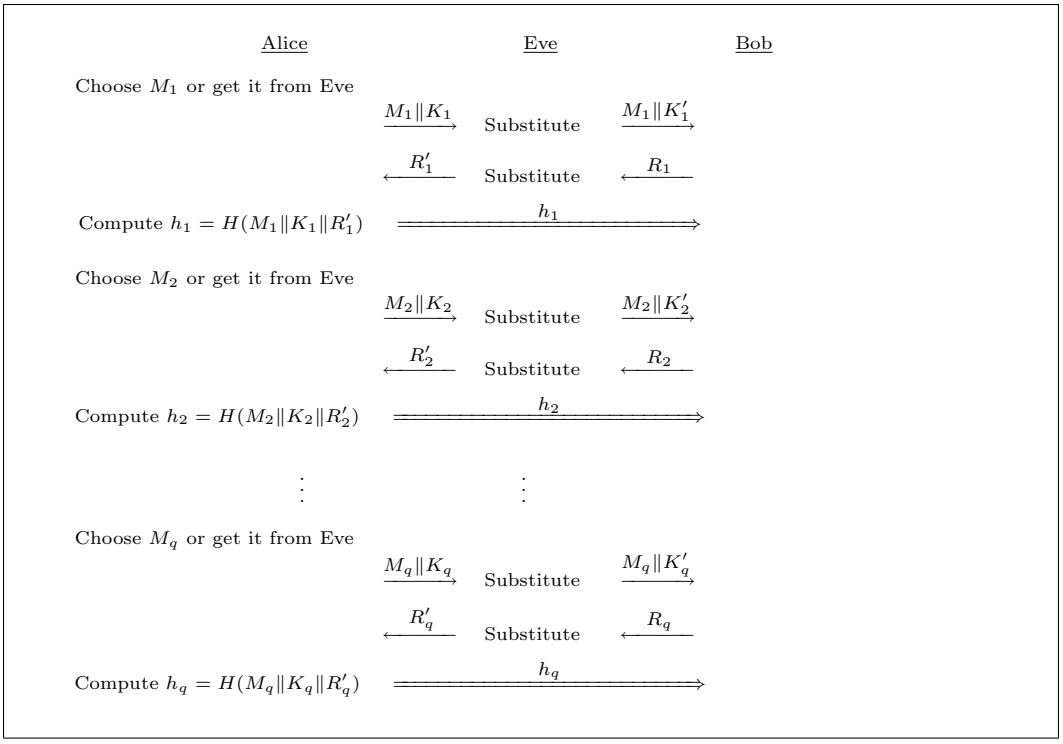

FIGURE 5. Information Gathering Phase of an Attack

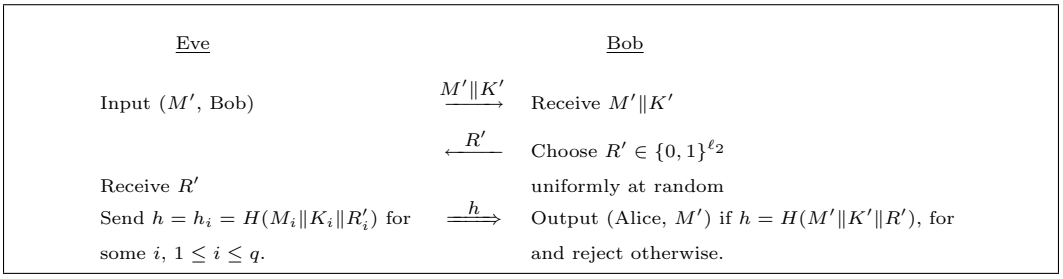

FIGURE 6. An Impersonation Attack Against IMAP

Consider the game illustrated in Figure 7. 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 K_i. This part is simulating the first flow sent by Alice.

Eve is allowed to change the values sent by Alice and Bob sent over the insecure channel, that is K_i and R_i. Note that $h_i = H(M_i\|K_i\|R_i')$. Hence, the values of K_i' and R_i are redundant in the analysis of the impersonation attack.

In the last round of the game, corresponding to the deception phase, Eve sends $M'\|K'$, $M' \neq M_i$ for every $i \in \{1, \ldots, q\}$. After receiving a random value R from the challenger, she

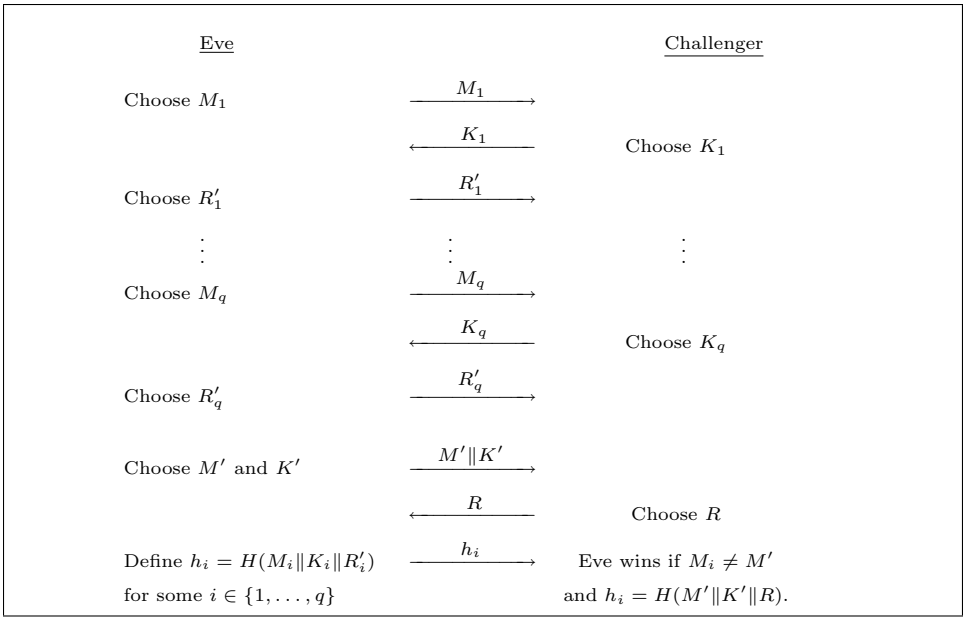

FIGURE 7. IMAP Game Against Impersonation Attacks

sends $h_i = H(M_i\|K_i\|R'_i)$, for some $i \in \{1, \ldots, q\}$. Eve wins the game if $h_i = H(M'\|K'\|R)$ for $M_i \neq M'$.

The following Theorem reduces the ICRI Game to the IMAP Game against impersonation attacks.

Theorem 1. *Let H be a $(T_{\text{off}}, \epsilon_1)$-ICRI hash function. Then, any adversary against the IMAP of Figure 4 with offline complexity T_{off} who makes q message queries and mounts an impersonation attack, has a probability of success p at most $q\epsilon_1$.*

Assuming that Eve wins the IMAP Game of Figure 7 with non-negligible probability, we can employ her in the ICRI Game depicted in Figure 1. In this reduction, Eve is playing against her IMAP Game Challenger and Oscar is playing against his ICRI Game Challenger. The result of the IMAP Game, played by Eve, is going to be used in the ICRI Game, played by Oscar. Oscar begins by choosing a random value $j \in \{1, \ldots, q\}$. Then, he lets Eve continue playing against the IMAP Challenger. Oscar does not interrupt the flows between Eve and her challenger except when $t = j$. For $t = j$, Oscar forwards M_j to the ICRI Challenger. Then, the challenger responds with K. Oscar sends $K = K_j$ to Eve. Oscar gets R' from Eve and sends it to the ICRI Challenger.

At the deception stage, Eve sends M' and K'. 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 $h_i = H(M'\|K'\|R)$. If $i = j$ and Eve wins, then Oscar wins the ICRI Game, and Oscar loses otherwise.

If we assume that Eve can win IMAP Game with probability ϵ, then Oscar wins the ICRI Game with probability ϵ/q.

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 $\mathcal{X} = \{0,1\}^{\ell_1+\ell_2+\ell_3}$ be the set of all possible binary strings of size $\ell_1+\ell_2+\ell_3$ 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 4, with offline complexity $T_{\text{off}} = 2^{t_{\text{off}}}$ who makes up to q message queries and mounts an impersonation attack, has a probability of success $p \leq q2^{-k}(2+2^{2t_{\text{off}}-\ell_2-\ell_3}+2^{t_{\text{off}}-\ell_3})$.*

4.3. **Substitution Attack.** In the substitution attack, unlike the case of impersonation attack, Alice is actively involved and she would like to authenticate M to Bob. The adversary, on the other hand, wishes to authenticate M' to Bob along with the identity of Alice. There are two cases possible here.

The first case is when Alice initiates a session and tries to authenticate M to Bob. Then, Eve substitutes M' instead of M. As a result, Bob receives M' and not M. The value of M' may be the result of a partial or total modification of M by Eve. After receiving R from Bob, Eve tries to find a suitable value R' which will make Bob accept after receiving h. Figure 8 is illustrating this scenario against our IMAP.

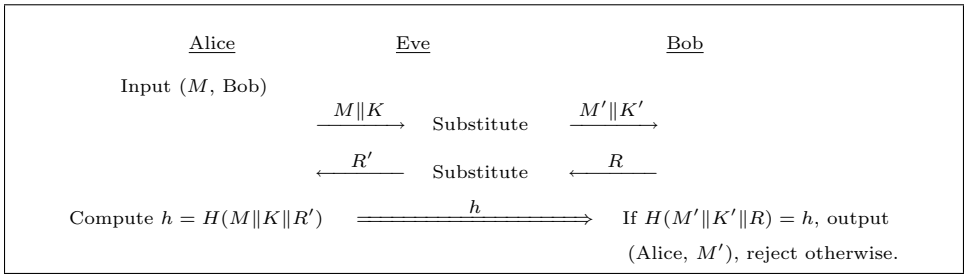

FIGURE 8. Substitution Attack of Type A Against Our IMAP

The second case is when Eve initiates a flow with Bob while pretending to be Alice. Eve tries to authenticate M' to Bob. After receiving R, she does her computations to find a suitable M. Then, she will make Alice initiate a session with Bob with input M. Eve will use the authenticated flow of this session in her original session with Bob.

4.3.1. *The IMAP Game Against Substitution Attacks.* Examining the substitution attack of type A, illustrated in Figure 8, we can write down the following as the order of the flows:

(1) Alice chooses M or gets it from Eve. Eve gets K from Alice.
(2) Eve sends M' and K' to Bob.
(3) Bob chooses a random value R and sends it to Eve.
(4) Eve chooses a random value R' and sends it to Alice.
(5) Alice computes $h = H(M\|K\|R')$, which is sent to Bob.

Note that the a successful substitution attack of type A directly translates into a successful player against the ICRII Game. As a result, we get the following theorem.

[3]See [7] 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.

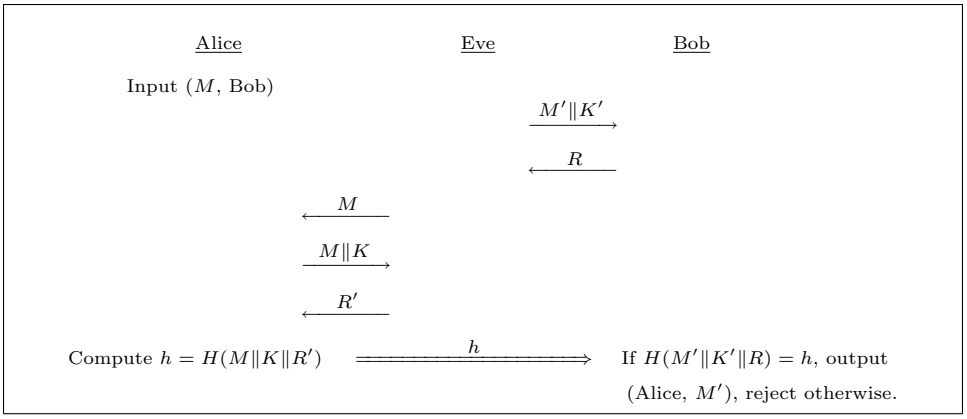

FIGURE 9. Another Substitution Attack of Type B Against Our IMAP

Theorem 2. *Let H be a $(T_{\text{off}}, T_{\text{on}}, \epsilon_2)$-ICR*II hash function. Then, any adversary against our IMAP with offline complexity T_{off} and online complexity T_{on}, who is mounting a substitution attack of type A has a probability of success $p = \epsilon_2$.

Now we examine the substitution attack of type B, illustrated in Figure 9. The following is the order of the flows as they happen in this attack scenario:

(1) Eve sends M' and K' to Bob.
(2) Bob chooses a random value R and sends it to Eve.
(3) Eve provides Alice with M.
(4) Alice sends M and K to Eve.
(5) Eve chooses a random value R' and sends it to Alice.
(6) Alice computes $h = H(M\|K\|R')$, which is sent to Bob.

A successful substitution attack of type B yields a successful player against the ICRIII Game. Hence, the following theorem follows.

Theorem 3. *Let H be a $(T_{\text{off}}, T_{\text{on}}, \epsilon_2)$-ICR*III hash function. Then, any adversary against our IMAP with offline complexity T_{off} and online complexity T_{on}, who is mounting a substitution attack of type B has a probability of success $p = \epsilon_2$.

Now combining Lemmas 2 and 3 with Theorems 2 and 3, we obtain the following corollary.

Corollary 2. *Let $\mathcal{X} = \{0,1\}^{\ell_1+\ell_2+\ell_3}$ be the set of all possible binary strings of size $\ell_1+\ell_2+\ell_3$ and H be a hash function chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$. Then, any adversary against our IMAP, with offline complexity $T_{\text{off}} = 2^{t_{\text{off}}}$ and online complexity $T_{\text{on}} = 2^{t_{\text{on}}}$, who is mounting a substitution attack, has a probability of success $p = 2^{-k}(2 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3} + 2^{t_{\text{on}}})$.*

4.4. **Security of our IMAP.** The adversary against our IMAP will either mount a substitution attack or an impersonation attack. Hence, the following theorem is a consequence of Corollary 1 and Corollary 2.

Theorem 4. *Let $\mathcal{X} = \{0,1\}^{\ell_1+\ell_2+\ell_3}$ and H be a hash function chosen randomly from $\mathcal{F}^{\mathcal{X},\mathcal{Y}}$, where $|\mathcal{Y}| = 2^k$. Then, any adversary against our IMAP, with offline complexity $T_{\text{off}} = 2^{t_{\text{off}}}$ and online complexity $T_{\text{on}} = 2^{t_{\text{on}}}$ who can make q message queries, has a probability of success*

$$p \leq 2^{-k} \max(q(2 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3}), 2 + 2^{2t_{\text{off}}-\ell_2-\ell_3} + 2^{t_{\text{off}}-\ell_3} + 2^{t_{\text{on}}}).$$

5. Parameter sizes

Theorem 4 says that an adversary attacking our proposed IMAP, using $2^{t_{\text{off}}}$ hash computations before the deception stage, $2^{t_{\text{on}}}$ hash computations during the deception stage, and q message queries, has a probability of success at most $2^{-k}\max(q(2+2^{2t_{\text{off}}-\ell_2-\ell_3}+2^{t_{\text{off}}-\ell_3}), 2+2^{2t_{\text{off}}-\ell_2-\ell_3}+2^{t_{\text{off}}-\ell_3}+2^{t_{\text{on}}})$.

Here, we first target typical[5] values for $q \leq 2^{10}$, $t_{\text{off}} \leq 70$, and $p \leq 2^{-20}$.

If we take $\ell_2, \ell_3 \geq 80$, then we can basically ignore the factors $(2+2^{2t_{\text{off}}-\ell_2-\ell_3})$ and $2^{t_{\text{off}}-\ell_3}$. We note that, since R and K are being sent over the insecure channel, this assumption does not have any impact on the analysis or usefulness of our protocol. We now can simplify the result of Theorem 4 to $p \leq 2^{-k}\max(q, 2^{t_{\text{on}}})$.

Since we want the overall success probability of the adversary be less than or equal to 2^{-20}, we require that $\max(q, 2^{t_{\text{on}}}) \leq 2^{k-20}$.

Hence, letting $t_{\text{on}} = 10$ along with typical parameters $q \leq 2^{10}$, $t_{\text{off}} \leq 70$, and $p \leq 2^{-20}$, we get that $k \geq 30$. This is a distinct improvement over the previous works.

In [11], $k \geq 50$ is required while the same typical parameters are targeted. If we let $k = 50$, then we can tolerate much stronger adversaries, compared to [11], [6], and [8], having $t_{\text{on}} = 30$ and $q \leq 2^{30}$ and still get the same overall success probability of $p \leq 2^{-20}$. Note that, we can allow t_{off} to get bigger as well by just choosing $\ell_2 + \ell_3$ according to the size of t_{off}.

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 IMAP 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.

The proposed IMAP of Figure 4 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 for commitment schemes.

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. Allowing the same amount of information to be sent over the authenticated channel, we can tolerate much stronger adversaries.

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 System Security Symposium*, San Diego, California, U.S.A., February 2002.

[5] See for instance [5] and [8].

[2] Christian Gehrmann, Chris J. Mitchell, and Kaisa Nyberg. Manual authentication for wireless devices. *RSA Cryptobytes*, 7(1):29–37, January 2004.
[3] Christian Gehrmann and Kaisa Nyberg. Security in personal area networks. *Security for Mobility, IEE, London*, pages 191–230, 2004.
[4] Jaap-Henk Hoepman. The ephemeral pairing problem. In *Financial Cryptography*, pages 212–226, 2004.
[5] 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/.
[6] Atefeh Mashatan and Douglas R. Stinson. Noninteractive two-channel message authentication based on hybrid-collision resistant hash functions. *IET Proceedings Information Security*, 2007. To Appear. [This is an updated version of [5]].
[7] Moni Naor, Gil Segev, and Adam 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.
[8] 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.
[9] Ronald L. Rivest and Adi Shamir. How to expose an eavesdropper. *Commun. ACM*, 27(4):393–394, 1984.
[10] Frank Stajano and Ross Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In B. Christianson, B. Crispo, , and M. Roe, editors, *Security Protocols, 7th International Workshop Proceedings*, Lecture Notes in Computer Science, 1999.
[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, Santa Barbara, California, U.S.A., August 2005. Springer-Verlag.