New Results on Unconditionally Secure Multi-receiver Manual Authentication*

Shuhong Wang and Reihaneh Safavi-Naini

Center for Computer and Information Security Research
TITR, University of Wollongong, Australia
{shuhong, rei@uow.edu.au}

Abstract. Manual authentication is a recently proposed model of communication motivated by the settings where the only trusted infrastructure is a low bandwidth authenticated channel, possibly realized by the aid of a human, that connects the sender and the receiver who are otherwise connected through an insecure channel and do not have any shared key or public key infrastructure. A good example of such scenarios is pairing of devices in Bluetooth. Manual authentication systems are studied in computational and information theoretic security model and protocols with provable security have been proposed. In this paper we extend the results in information theoretic model in two directions. Firstly, we extend a single receiver scenario to multireceiver case where the sender wants to authenticate the same message to a group of receivers. We show new attacks (compared to single receiver case) that can launched in this model and demonstrate that the single receiver lower bound $2\log(1/\epsilon)+O(1)$ on the bandwidth of manual channel stays valid in the multireceiver scenario. We further propose a protocol that achieves this bound and provides security, in the sense that we define, if up to c receivers are corrupted. The second direction is the study of non-interactive protocols in unconditionally secure model. We prove that unlike computational security framework, without interaction a secure authentication protocol requires the bandwidth of the manual channel to be at least the same as the message size, hence non-trivial protocols do not exist.

Key words: manual channel, (interactive) multireceiver authentication, security.

1 Introduction

Message authentication systems provide assurance for the receiver about the authenticity of a received message. Unconditionally secure authentication systems in symmetric key and asymmetric key models were introduced by Simmons [1] and later studied and extended to by a number of authors [2, 3]. Information theoretic bounds on the success probability of an adversary relates the success

* This work is in part supported by the Australian Research Council under Discovery Project grant DP0558490.

chance to the key entropy [4] and provides a lower bound on number of key bits that are required for achieving a certain level of protection. Gemmell and Naor [5] proposed an interactive protocol for authentication and showed that the key length can be reduced for the same level of protection [1].

As an extension of two-party authentication, MRA (multi-receiver authentication) aims at providing the integrity of a message sent from one sender to $n > 1$ receivers. MRA is very important for many applications, such as network control, TV broadcast, and other distributed systems. A trivial yet inefficient approach for MRA might be to run n copies of the two-party authentication protocol. Significant efforts have been made to construct nontrivial (more efficient and/or more secure) MRAs. Existing work on them in the information theoretic model includes [8–10], providing unconditional security. Note that all the existing MRAs were done in the shared key communication model where secrets are pre-distributed to participants.

Recently a new communication model for message authentication, motivated by scenarios such as pairing of devices in Bluetooth protocol [11], has been proposed. In this model sender and receiver do not have a shared key but in addition to the insecure channel that they are using for communication of messages, they are also connected through a low bandwidth authenticated channel, called *manual channel*. Messages sent over the manual channel cannot be modified. Also the attacker cannot inject a new message over this channel. However the attacker can change the synchronization of the channel and can delay or replay a sent message over this channel. The bandwidth of the manual channel is a scarce resource and has the same role as the key length in a symmetric or asymmetric key model and efficiency analysis of the protocols shows how efficiently the bandwidth has been used for providing protection against forgery.

Authentication in manual channel model has been studied in both computational and unconditionally secure frameworks [12, 13]. Vaudenay proposed a formal model for analysis of protocols in this model. Naor, Sergev and Smith studied protocols in this model using unconditionally secure framework. Naor et al's protocol is interactive and is shown to limit the success chance of the forger to ϵ by using a manual channel with bandwidth $2\log\epsilon + O(1)$.

In computational model there are also non-interactive protocols, referred to as NIMAP (Non-interactive Manual Authentication Protocol). NIMAPs [14, 15] are particularly interesting because they do not require the receive to be live and as long as what is received through the public channel *matches* what is received over the manual channel, the received message is considered authentic.

Our contribution

In this paper we extend the two party manual authentication scenario of [13] to a *multireceiver manual authentication* (MRMA), i.e., a scenario where there is one sender and multiple receivers, some possibly corrupted, and the sender does not have shared secret with receivers. The sender however has a low bandwidth manual channel with each receiver. We assume receivers are connected through

[1] The original version of their protocol was shown insecure [6]. The corrected version in [7] provides the claimed security.

a trusted infrastructure. In particular we assume there is a trusted initializer that provides key information to receivers. The adversary can corrupt up to c receivers. We will show that in the above MRMA system the $2\log(1/\epsilon) + O(1)$ lower bound on manual channel bandwidth holds for constant c. More specifically, we propose an interactive protocol for multireceiver case that limits the success chance of the forger to ϵ by using a manual channel with bandwidth $2\log(1/\epsilon) + O(\log c)$.

We also consider NIMAPs in unconditionally secure framework and show a lower bound on the bandwidth of the manual channel that effectively implies secure NIMAPs can only exist if the message is directly sent over the manual channel, i.e. trivial case. This demonstrates that unlike computational security framework interaction is necessary for secure manual authentication.

The paper is organized as follows. In Section 2 we present a communication model and a definition for multireceiver manual authentication (MRMA) under the model. We assume the strongest adversary in our model. In Section 3 we extend the Naor et al's protocol to multireceiver case. We first show that a straightforward extension cannot be secure in our strong adversary model, and then propose an secure extension, resulting in an interactive multireceiver manual authentication protocol. In Section 4 we show that non-interactive manual authentication in the unconditionally secure setting is not possible unless the message itself is sent over the manual channel. There, interaction is necessary in for unconditionally secure manual authentication. Finally, the paper is concluded in Section 5.

2 A model for multi-receiver manual authentication

We consider a setting where there are a sender $\mathcal{S}$ and a group of receivers denoted by $\mathcal{R} =: \{\mathcal{R}_1, \mathcal{R}_2, \cdots, \mathcal{R}_n\}$. The sender and receivers are connected via two types of channels (insecure and manual). Receivers are connected among themselves via one type of channels (insecure). However there is a trusted infrastructure among receivers. A motivating scenario is when a group leader is connected to each group member through a manual channel, and group members have some secret key information that enables them to have secure communication among themselves.

Communication between sender and receivers
The sender is connected to the receivers through an *insecure multicast* channel that is used to transmit the same message to all the receivers. Such an insecure multicast channel could be implemented by letting each receiver has a point to point channel to the sender. All these channels are insecure and are controlled by the adversary. In particular the adversary can control the link between the sender and each receiver independently, and read, inject, modify, remove and delay traffic as he wishes (similar to multicast over the Internet).

In addition to the public channel, we assume that there is a *manual multicast channel* that connects the sender to the receivers. This channel can be seen as n (unidirectional) manual channels, each connecting the sender to a receiver, that

can be individually controlled by the adversary. The sender uses the multicast channel to send the same message to all receivers but the adversary's control can result in the message to have different synchronisation tampering for different receivers.

An example of a manual multicast channel is a display that is visible by all group members (e.g a classroom) and is used to show a short string to all group members (although in this example the tampering will be the same on all individual manual channels). Following the terminology in A-codes, such a short string is called as *manual tag* and sometimes *tag* without making confusion.

Communication among receivers
Receivers can communicate with each other through insecure point-to-point public channels. We assume there is a trusted initializer that securely distribute keys to receivers, hence allowing them to use traditional cryptographic primitives.

The adversary
Adversary has full control over public channels can target one or more channels (but not all). He can can read, modify or delay messages; he can prevent them from being delivered; he can also replay old messages or insert new ones at any time. The adversary can control one or more manual channels between the sender and receivers. He is however restricted to tampering with synchronisation information; i.e. read, remove, delay, reply of sent messages.

The adversary can also corrupt up to c receivers and have them deviate from the protocol in anyway he defines, but of course subject to restrictions in the communication model.

2.1 Extending Naor *et al* protocol to MRMA

Our aim is to extend Naor *et al* protocol to allow a sender to authenticate a message m to a group of receivers when the communication structure is defined as above.

A basic approach would be to use the trusted infrastructure to reduce the group of receivers $\mathcal{R}$ into a single entity (i.e., a single receiver) and use the single receiver protocol of Naor *et al* [13] between the sender and this *combined receiver*.

We first show that without assuming a trusted infrastructure and using a direct application of the protocol, a single dishonest receiver can subvert the system. In Subsection 3.1 we describe two attacks that show how an adversary can use a man-in-middle strategy to forge a message with or without manipulating synchronization of messages. We next consider a model assuming receivers can be initialized by a *trusted initializer* who can provide some secret information (hence a trusted infrastructure) to them. Hence our model can be viewed as a combination of manual channel model between sender and receiver, and a trusted initializer model among receivers. See also Figure 1.

Similar to the single receiver model of [13], the input of the sender $\mathcal{S}$ is a message m, which she wishes to authenticate to the set of receivers $\mathcal{R}$. In the first round, $\mathcal{S}$ sends the message and an authentication tag $A^1_{\mathcal{S}}$ over the

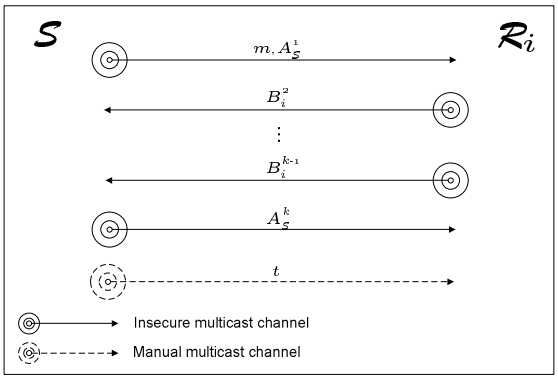

Fig. 1. The multireceiver manual authentication (MRMA) model.

insecure multicast channel. In the following rounds only a tag $A_{\mathcal{S}}^j$ (or B_i^j) is sent over the insecure channel, meaning that the tag is from $\mathcal{S}$ (or from $\mathcal{R}_i$). All communications over public channel can be controlled by the adversary. He can inject or modify the input message m. The replaced message $\widehat{m}_i$ is received by the receiver $\mathcal{R}_i, i = 1, 2, \cdots, n$. He receives all of the tags $A_{\mathcal{S}}^j$ and can replace them with $\widehat{A}_i^j$ of his choice intending for $\mathcal{R}_i$. The adversary also receives each of the tags B_i^j and can replace them with $\widehat{B}_i^j$ before they arrive $\mathcal{S}$. Finally, $\mathcal{S}$ manually authenticates a short *manual tag* t, i.e., sent over the manual channel.

For reading ease, we list the notations represent what are sent and received at each player's end in Table 1.

$\mathcal{S}$ side sending		receiving $\mathcal{R}_i$ side
m	$\longrightarrow$	$\widehat{m}_i$
$A_{\mathcal{S}}^j$	$\longrightarrow$	$\widehat{A}_i^j$
$\widehat{B}_i^j$	$\longleftarrow$	B_i^j

Table 1. Notations reflects changes. j specifies the round.

Notice that in the presence of a computationally unbounded adversary, we can assume w.l.g that the manually authenticated string is sent in the last round. As being pointed out in [13], this is true also in the computational setting, under the assumption that distributively one-way functions do not exit. And similarly, we also allow the adversary to control the synchronization of the protocol's execution. That is, the adversary can carry on two separate, possibly asynchronous conversations, one with the sender and one with the receivers. However, the party that is supposed to send a message waits until it receives the adversary's message from the previous round. For example, the sender $\mathcal{S}$ will only send his $A_{\mathcal{S}}^{j+1}$ after he has obtained all the $\widehat{B}_i^j$ $(i = 1, 2, \cdots, n)$ from the receivers.

We assume the adversary can corrupt a subset $\mathcal{C} \subset \mathcal{R}$ of the receivers and $c = |\mathcal{C}|$.

Definition 1. *An unconditionally (n, c)-secure (a, b, k, ϵ)-manual authentication protocol is a k-round protocol in the communication model described above, in which the sender wishes to authenticate an a-bit input message to n receivers, while manually authenticating at most b-bits to over a multireceiver manual channel. The following requirement must hold:*

- *Completeness: For all input message m, when there is no interference by the adversary in the execution and all the players honestly follow, every receiver accepts with probability at least 1/2.*
- *Unforgeability: For any computationally unbounded adversary, for any $\mathcal{C}$ of size c receivers corrupted by the adversary, and for all input messages m, if the adversary replaces m with a different message $\widehat{m}_i$ for any $\mathcal{R}_i \notin \mathcal{C}$, then $\mathcal{R}_i$ accepts $\widehat{m}_i$ with probability at most ϵ.*

Lower bound on bandwidth
Obviously when $n = 1$, our model reduces to the basic model of Naor *et al* [13] and so the lower bound for our model cannot be less than that. By constructing a protocol that uses a manual channel with bandwidth being only $2\log(1/\epsilon) + O(\log c)$, we show that the lower bound for the our MRMA model is in fact equal to $2\log(1/\epsilon) + O(1)$ for constant c, the same lower bound of the basic model. This is particularly the case for small groups.

3 Interactive MRMA protocols

At first, we show that a straightforward extension of a single-receiver scheme is not secure in the multi-receiver setting due to existence of strong attacks. This result is consistent to other known results on multi-receiver authentications in the shared-key communication model. More precisely, that is a straightforward extension of a single receiver scheme (A-code) is not secure in the multi-receiver setting. We note that this consistence is however due to different reasons (of course both due to distrust among receivers). In the shared-key model, the insecurity is due to the difference that the sender and receiver in A-codes is symmetric while in secure MRA-codes should be asymmetric. But in the manual channel model (always asymmetric), the insecurity is due to the difference that a single-receiver will generate a truly random for himself, while a group of receivers may not voluntarily generate a truly random for the group (traitors exist).

Then we present two attacks to show that a single traitor is enough to subvert the protocol completely and thus new technique must employed to secure the protocol. And in Subsection 3.2 we show that by using commitment schemes, the group of receivers can be forced to play honestly, in the sense that dishonest behavior (of up to $c = n - 1$ corrupted receivers) can cheat no honest receiver.

3.1 A straightforward extension

In the following, we present a straightforward extension of the interactive protocol P_k of [13], from the single receiver setting to the multi-receiver setting. A brief description of the P_k [13] is given in the Appendix A. Denote the resulting protocol by P_k^n. We show how an inside attacker (e.g., corrupted by the adversary) can fool the other receivers in P_k^n. Note that P_k^n is quite efficient in the sense that generating and sending a message to all the receivers is once-off in every round. It is obvious that a trivial multi-receiver solution by repeating a single-receiver protocol multiple times does not enjoy this computation and communication efficiency.

For simplicity, let $n = 2$ and $k = 2$, thus the round index j can be omitted. The $\mathrm{P}_{n=2}^{k=2}$ protocol is described as below, where f (more exactly f^j) is defined in Section 3.2, which is the function C^j in [13]. Note that for any equivalent tasks of $\mathcal{R}_1$ and of $\mathcal{R}_2$, the order of performing them can be either.

The protocol $\mathrm{P}_{n=2}^{k=2}$

1. S multicasts m to the receivers through the insecure channel.
2. $\mathcal{R}_1$ receives the message as $\widehat{m}_1$ and $\mathcal{R}_2$ receives the message as $\widehat{m}_2$.
   (a) $\mathcal{S}$ chooses $A_{\mathcal{S}} \in_R \mathrm{GF}[Q]$ and multicasts it to $\mathcal{R}_1, \mathcal{R}_2$.
   (b) $\mathcal{R}_1$ receives $\widehat{A}_1$, then chooses $B_1 \in_R \mathrm{GF}[Q]$ and sends it to $\mathcal{S}$ and $\mathcal{R}_2$.
   (c) $\mathcal{R}_2$ receives $\widehat{A}_2$, then chooses $B_2 \in_R \mathrm{GF}[Q]$ and sends it to $\mathcal{S}$ and $\mathcal{R}_1$.
   (d) After receiving the $\widehat{B}_1$ and $\widehat{B}_2$, $\mathcal{S}$ computes $\widehat{B} = \widehat{B}_1 + \widehat{B}_2$ and computes $m_{\mathcal{S}} = \langle \widehat{B}, f_{\widehat{B}}(m) + A_{\mathcal{S}} \rangle$.
   (e) $\mathcal{R}_1$ receives B_2, then computes $B = B_1 + B_2$ and $m_1 = \langle B, f_B(\widehat{m}_1) + \widehat{A}_1 \rangle$.
   (f) $\mathcal{R}_2$ receives B_1, then computes $B = B_1 + B_2$ and $m_2 = \langle B, f_B(\widehat{m}_2) + \widehat{A}_2 \rangle$.
3. $\mathcal{S}$ multicasts $m_{\mathcal{S}}$ to $\mathcal{R}_1, \mathcal{R}_2$ through the manual multicast channel.
4. $\mathcal{R}_1$ accepts if and only if $m_{\mathcal{S}} = m_1$; $\mathcal{R}_2$ accepts if and only if $m_{\mathcal{S}} = m_2$.

Fig. 2. An insecure extension of Naor et al's P_k to MRMA model

Clearly the sum B (resp. $\widehat{B}$) plays exactly the role of the random number selected by the single receiver (resp. what received by the sender) of P_k. The protocol P_k is proved to be secure, but P_k^n is not secure any more. In order to better understand our construction, in the following we show two attacks on the protocol P_k^n below.

As illustrated in Figure 3, the *asynchronous* attack is named from that the dishonest $\mathcal{R}_2$ (or considering that he is corrupted by an adversary) runs the protocol *non-synchronically* (i.e., separately) with the sender $\mathcal{S}$ and the other receiver $\mathcal{R}_1$ who are both honest. When running the protocol with $\mathcal{S}$, $\mathcal{R}_2$ impersonates $\mathcal{R}_1$ sending an arbitrary $\widehat{B}_1$ and also sending his own $\widehat{B}_2$. Then $\mathcal{S}$ will send the supposed manual tag $t = \langle \widehat{B}, f_{\widehat{B}}(m) + A \rangle$ through the manual channel. Now $\mathcal{R}_2$ delays the manual tag, and impersonates $\mathcal{S}$ to run the protocol with

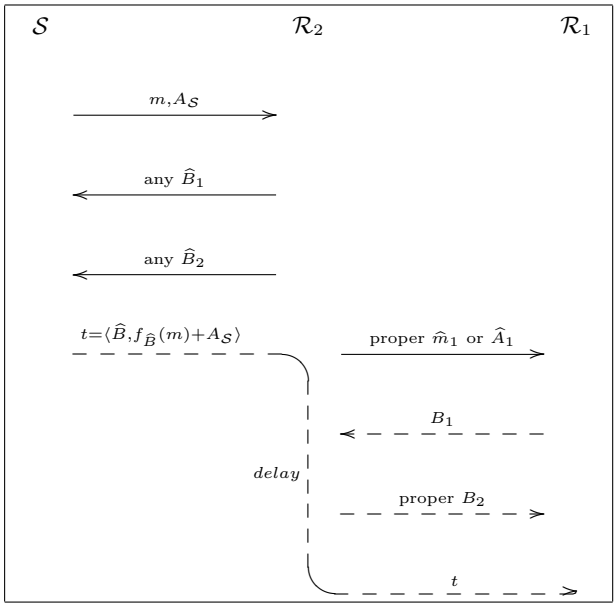

Fig. 3. An attack with manipulating synchronization.

$\mathcal{R}_1$. He can choose a proper $\widehat{A}_1$ for an arbitrary message $\widehat{m}_1$ or vice versa such that $f_{\widehat{B}}(\widehat{m}_1) + \widehat{A}_1 = f_{\widehat{B}}(m) + A$. On receiving $\widehat{m}_1, \widehat{A}_1$ the receiver $\mathcal{R}_1$ sends B_1 to $\mathcal{R}_2$ and thus $\mathcal{R}_2$ can simply sends $B_2 = \widehat{B}_1 + \widehat{B}_2 - B_1$ to $\mathcal{R}_1$. And then $\mathcal{R}_2$ let the tag t get through to $\mathcal{R}_1$ (recall that $\mathcal{R}_2$ is not able to modify the manual tag over the manual channel). It is easy to see that $\mathcal{R}_1$ will accept $\widehat{m}_1$ as authentic from $\mathcal{S}$.

As illustrated in Figure 4, the *dependent* attack does not use an asynchronous conversation, instead, it merely make use of the fact that $\widehat{B}_2$ and B_2 can be *dependent* on $\widehat{B}_1$ and B_1 (i.e. $\mathcal{R}_2$ can choose the former after he knows the latter). In fact, for any $m, A_{\mathcal{S}}$ and any $\widehat{m}_1, \widehat{A}_1$, $F(x) := (f_x(m) + A_{\mathcal{S}}) - (f_x(\widehat{m}_1) + \widehat{A}_1)$ is a polynomial of the variable x. Denote x_0 a root of $F(x)$, then $\mathcal{R}_2$ can simply compute and send $\widehat{B}_2 = x_0 - \widehat{B}_1$ and $B_2 = x_0 - B_1$. One can easily verify that $\mathcal{R}_1$ would accept the tag t sent by $\mathcal{S}$.

3.2 An interactive protocol

In a multireceiver manual authentication system the sender is trusted but some of the receivers can be corrupted by the adversary. Our protocol, Π_k, as described below is secure against such a strong adversary.

The main observation from the above section is that to ensure security of the protocol, one needs to ensure the sum $B^j = \sum_{i=1}^{n} B_i^j$ remains unpredictable (cannot be engineered by the adversary). We use unconditionally secure non-

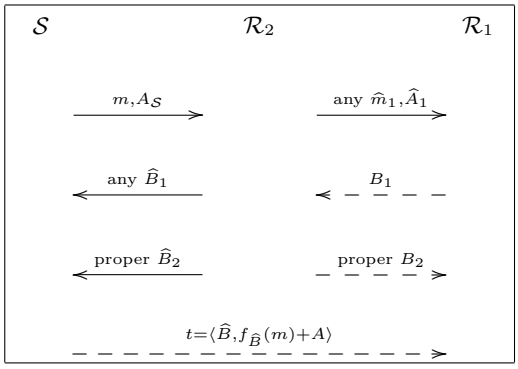

Fig. 4. An attack without manipulating synchronization.

interactive commitment schemes (USNIC) to achieve this goal. Examples of such commitment schemes include the ones by Rivest [16] and by Blundo *et al* [17].

We denote the USNIC scheme working in finite field GF[Q] by USNIC[Q] and choose it to be the scheme of Blundo *et al*. To make the paper self-contained, we briefly review their scheme in Appendix B.

The commitment scheme is used in each round, by each receiver to commit to a random value of his choice to all the other receivers[2] to provide assurance for other receivers that their random values are not captured for subverting the protocol (See the dependent attack in Subsection 3.1, Figure 4 for detail). In other words the sum $B^j = \sum_{i=1}^{n} B_i^j$ is unpredictable (has full entropy). We note that this can be achieved even if only one receiver is honest, i.e., if one B_i^j is truly randomly. This lets us to treat the group of the receivers as one entity and thus the security of our MRMA protocol reduces to the security of Naor et al's protocol P_k [13].

To reduce the length of manual tag, similar to the protocol in [13], we use a sequence of compression function families $f^1, f^2, \cdots, f^{k-1}$ in an k-round interactive protocol. More precisely, given the length, a, of the input message and the upper bound, $(c+1)\epsilon$, on the adversary's forgery probability, $k-1$ finite fields $Q_j, j = 1, \cdots k-1$, are chosen such that $\frac{2^{k-j}a_j}{\epsilon} \leq Q_j < \frac{2^{k-j+1}a_j}{\epsilon}$, where $a_1 = a$ and $a_{j+1} = \lceil 2 \log Q_j \rceil$. Then each f_x^j chosen from the family f^j maps an a_j-bit message m into GF[Q_j] in the following way: firstly the message is split as $m = m_1 m_2 \cdots m_d$ (concatenation of d strings) with each $m_i \in \mathrm{GF}[Q_j]$, and then the function is evaluated as $f_x^j(m) = m_1 x + m_2 x^2 + \cdots + m_d x^d \mod Q_j$. The splitting methods, and equivalently the function family f^j, is public known for all $j = 1, 2, \cdots, k-1$.

The protocol Π_k:

1. S multicasts $m_{\mathcal{S}}^1 = m$ to the receivers through the insecure channel.

[2] It is an interesting open problem to construct more sophistic schemes for committing to multiple messages, so that the trusted initializer is invoked only once.

2. For $i = \{1, 2, \cdots, n\}$, $\mathcal{R}_i$ obtains the message $m_i^1 = \widehat{m}_i$.
3. For $j = 1$ to $k - 1$.
   (a) If j is odd, then
      i. $\mathcal{S}$ chooses $A_{\mathcal{S}}^j \in_R \mathrm{GF}[Q_j]$ and multicasts it to $\mathcal{R}$, through the insecure multicast channel.
      ii. For $i = \{1, 2, \cdots, n\}$, $\mathcal{R}_i$ receives $\widehat{A}_i^j$. Then he chooses and commits to (using USNIC$[Q_j]$) a random $B_i^j \in_R \mathrm{GF}[Q_j]$ all the other receivers $\mathcal{R} \setminus \mathcal{R}_i$. After receiving all the commitments from other receivers, he sends B_i^j to $\mathcal{S}$ and opens the his commitment to other receivers.
      iii. After receiving all the $\widehat{B}_i^j$, $\mathcal{S}$ computes $\widehat{B}^j = \sum_{i=1}^n \widehat{B}_i^j$ and $m_{\mathcal{S}}^{j+1} = \langle \widehat{B}^j, f_{\widehat{B}^j}^j(m_{\mathcal{S}}^j) + A_{\mathcal{S}}^j \rangle$.
      iv. When all the commitments are correctly opened, $\mathcal{R}_i$ computes $B^j = \sum_{i=1}^n B_i^j$ and $m_i^{j+1} = \langle B^j, f_{B^j}^j(m_i^j) + \widehat{A}_i^j \rangle$.
   (b) If j is even, then
      i. For $i = \{1, 2, \cdots, n\}$, $\mathcal{R}_i$ chooses $B_i^j \in \mathrm{GF}[Q_j]$ and commits to it to other receivers using USNIC$[Q_j]$ scheme. After received all the commitments, he sends B_i^j to $\mathcal{S}$ and reveals his commitment.
      ii. After receiving all the $\widehat{B}_i^j$, $\mathcal{S}$ chooses $A_{\mathcal{S}}^j \in_R \mathrm{GF}[Q_j]$ and multicasts it to $\mathcal{R}$. Then he computes $\widehat{B}^j = \sum_{i=1}^n \widehat{B}_i^j$ and $m_{\mathcal{S}}^{j+1} = \langle A_{\mathcal{S}}^j, \widehat{B}^j, f_{A_{\mathcal{S}}^j}^j(m_{\mathcal{S}}^j) + \widehat{B}^j \rangle$.
      iii. For $i = \{1, 2, \cdots, n\}$, $\mathcal{R}_i$ computes $B^j = \sum_{i=1}^n B_i^j$ when all the commitments are correctly opened and then computes $m_i^{j+1} = \langle \widehat{A}_i^j, f_{\widehat{A}_i^j}^j(m_i^j) + B^j \rangle$ on receiving $\widehat{A}_i^j$.
4. $\mathcal{S}$ multicasts $m_{\mathcal{S}}^k$ to $\mathcal{R}$ through the manual multicast channel.
5. For $i = \{1, 2, \cdots, n\}$, $\mathcal{R}_i$ accepts if and only if $m_{\mathcal{S}}^k = m_i^k$.

Theorem 1. *For any $1 \leq c < n$ colluders, the above protocol Π_k is an (n, c)-secure $(a, b, k, (c+1)\epsilon)$-manual authentication protocol in the MRMA model, with $b \leq 2\log(1/\epsilon) + 2\log^{k-1} a + O(1)$.*

Proof (sketch). See Appendix C for the detailed proof.

The proof is analogous to that of the protocol P_k in [13] where the B^j is randomly chosen by a single receiver after receiving $\widehat{A}^j$. In our protocol B^j is the sum (or any function depending on all) of the random variables B_i^j chosen by $\mathcal{R}_i$, $i = 1, 2, \cdots, n$. Thus to prove the security of our protocol, it is sufficient to prove that the B^j that $\mathcal{R}_i \notin \mathcal{C}$ computes is truly random and plays the same role of B^j [illegible] he single receiver protocol. For instance in case of j odd, to prove that the sum B^j, after $\mathcal{R}_i$ received $\widehat{A}_i^j$ from the adversary, is truly random we note that since B^j depends on B_i^j which is chosen after $\mathcal{R}_i$ received $\widehat{A}_i^j$, it is sufficient to prove that the adversary can not control B^j. This is obviously true (except with a probability $\leq c/Q_j$) because the security of underlying commitment scheme USNIC$[Q_j]$ (see Appendix C), For the case of even j, the conclusion holds similarly. So the total cheating probability is bounded by $\sum_{j=1}^{k-1}(\frac{c}{Q_j} + \frac{\epsilon}{2^{k-j}}) \leq (c+1)\epsilon$.

Since by using USNIC schemes, we are able to handle a group $\mathcal{R}$ of receiver as a single receiver, thus the number of bits sent over the manual channel is actually same to the single receiver case, that is $b \leq 2\log(1/\epsilon)+2\log^{k-1} a+O(1)$ by claim 17 in [13]. And if there exists some $1 \leq j \leq k-2$ such that $a_j \leq \frac{2^{k-j}}{\epsilon}$, we can choose $Q_{k-1} = \Theta(1/\epsilon)$ instead of $Q_{k-1} = \Theta((1/\epsilon)\log(1/\epsilon))$ and achieves $b = 2\log(1/\epsilon) + O(1)$. □

Corollary 1. *An (n, c)-secure (a, b, k, ϵ)-manual authentication protocol in the MRMA model exists for all $a, k, 1 \leq c \leq n-1$, $0 < \epsilon < 1$ and $b \leq 2\log(1/\epsilon) + 2\log^{k-1} a + O(\log c)$.*

Proof. By replacing $(c+1)\epsilon$ with ϵ in Theorem 1, we have $b \leq 2\log((c+1)/\epsilon) + 2\log^{k-1} a + O(1) = 2\log(1/\epsilon) + 2\log^{k-1} a + 2\log(c+1) + O(1)$. □

In case $a_j \leq \frac{(c+1)2^{k-j}}{\epsilon}$ for some $j = 1, \cdots, k-2$, we immediately have a lower bound for the MRMA model $2\log(1/\epsilon) + O(\log c)$. This is the same bound as the single receiver model for constant c, that is $2\log(1/\epsilon) + O(1)$. It is however not known for large c, whether $2\log(1/\epsilon) + O(\log c)$ is the tight bound.

4 Impossibility of noninteraction

Non-interactive Manual Authentication Protocols (NIMAPs) [14, 15] are particularly interesting in computational model because they do not require the receive to be live and as long as what is received through the public channel *matches* what is received over the manual channel, the received message is considered authentic. In this section we show a negative result that non-trivial NIMAPs do not exist in information theoretic model.

The information theoretic NIMAP model: The sender $\mathcal{S}$ sends the message m and some x over the insecure public channel, and a tag t over the manual channel. The receiver $\mathcal{R}$ decides wether or not accepts m as authentic from $\mathcal{S}$.

Advantage: The non-interactive protocol (if exists) has an obvious advantage over interactive protocol, that is, it is simple and efficient in communication. More importantly, there is an advantage that non-interactive protocol for single receiver also works for multiple receivers by replacing the unicast channels with multicast ones. The intrinsic reason is that non-interactive protocol needs no information from the receiver, no matter it is a single entity or a group. For this reason, we thereafter consider $\mathcal{R}$ as a single entity.

Impossibility: We, however, notice that non-interactive manual authentication protocol does not exists in the "pure" manual channel model (i.e., without secrets between sender and receiver, and without requirements such as stall-free on the manual channel) *unless* the manual channel has enough bandwidth to transmit the whole message. This can be roughly argued as follows.

Suppose now $|m| > |t|$, then there definitely exists some other message $\widehat{m}$ which is authenticated under the same manual tag t (under some $\widehat{x}$). Therefore,

on observing the authentication transcripts (m, x, t), the adversary simply replaces (m, x) with $(\widehat{m}, \widehat{x})$. The adversary can do so "online" by removing m, x and delaying t until he figures out such $(\widehat{m}, \widehat{x})$ and then inserts it into the insecure channel.

To formally prove the impossibility, we need the following formal definition of non-interactive manual authentication protocol.

Definition 2. *Let M, X, T denote the random variables overs the sets $\mathcal{M}, \mathcal{X}, \mathcal{T}$, respectively. A non-interactive manual protocol is given by a joint conditional distribution $P_{XT|M} : (\mathcal{X}, \mathcal{T}, \mathcal{M}) \to [0, 1]$, where the input message m is chosen according to the distribution $P_M : \mathcal{M} \to [0, 1]$ (by either the adversary or $\mathcal{S}$). The values (m, x) of (M, X) are sent over the insecure channel and the value t of T is sent over the manual channel. Finally, $\mathcal{R}$ receives $\widehat{m}, \widehat{x}, t$ and accepts $\widehat{m}$ as authentic if and only if $P_M(\widehat{m}) > 0$ [3] and $V(\widehat{m}, \widehat{x}, t) = 1$, where $V(\cdot)$ is a boolean-valued function $V(m, x, t) \in \{0, 1\}$ over $\mathcal{M} \times \mathcal{X} \times \mathcal{T}$.*

Typically, the distribution P_M is chosen to be the uniform distribution; the joint conditional distribution $P_{XT|M}$ is given in terms of efficiently computable randomized function $f : \mathcal{M} \times \Gamma \to \mathcal{X} \times \mathcal{T}$, where Γ is some finite se, such that $P_{.|M}$ is the distribution of $f(m, \gamma))$ for a uniformly random chosen $\gamma \in \Gamma$. This is often directly used as the definition of a manual authentication protocol, such as [19, 15], although they are in computational setting. The protocol of Naor *et al* [13] and ours in previous sections are also described in this typical manner. Note that this definition can be extended to cover the interactive manual authentication protocol by defining a series of joint conditional distributions. Due to the time and space limitation, we leave the extension as our future work.

We use the term "an input message m" to mean a message $m \in \mathcal{M}$ satisfying $P_M(m) > 0$, and denote the set of input messages by $\mathcal{M}^+$. Then for every $m \in \mathcal{M}^+$, define $\mathcal{T}_m = \{t \in \mathcal{T} : \exists x \in \mathcal{X}, s.t., P_{XT|M}(x, t|m) > 0\}$ and $\Delta_m = \{t \in \mathcal{T} : \exists x \in \mathcal{X}, s.t., V(m, x, t) = 1\}$. $\mathcal{T}_m$ is called the set of correct manual tags with regard to an input message m, and Δ_m is called the acceptable manual tags with regard to an input message m. Then we can use $t \in \mathcal{T}_m$ (resp. $t \in \Delta_m$) to refer to the event that "there exists an $x \in \mathcal{X}$ such that $P_{XT|M}(x, t|m) > 0$ (resp. $V(m, x, t) = 1$) holds for the input message m". Let $1/2 \leq \xi \leq 1$ and $0 \leq \epsilon < 1$ be two real number constants, and let $\epsilon(\widehat{m}|m, t)$ be the chance of an adversary, who observes the authentication transcripts[4] (m, x, t), in deceiving $\mathcal{R}$ into accepting a different message $\widehat{m}$ using his best strategy. We have the following definition for security of a non-interactive manual authentication protocol.

Definition 3. *A* non-interactive *manual authentication protocol is said to be information theoretically (ξ, ϵ)-secure if the following properties hold.*

[3] This can be looked as the message redundancy verification that excludes the messages meaningless. However, one can assume $P_M(m) > 0$ holds for all $m \in \mathcal{M}$ to omit this verification without impact on our impossibility result since, adding m with $P_M(m) = 0$ to $\mathcal{M}$ only increase its size, has no effect on its entropy $H(M)$.

[4] Which, by the definition of $\mathcal{T}_m$, implies $t \in \mathcal{T}_m$.

Completeness *The joint conditional distribution satisfies for every* $m \in \mathcal{M}^+$, $\sum_{x,t:V(m,x,t)=1} P_{XT|M}(x,t|m) \geq \xi$. *In other words, for all input message* m, *when there is no interference by the adversary in the execution, the receiver accepts* m *with probability at least* ξ.

Unforgeability *The joint conditional distribution satisfies* $\epsilon(\widehat{m}|m,t) \leq \epsilon$, *for all* $m \neq \widehat{m} \in \mathcal{M}^+$ *and* $t \in \mathcal{T}_m$. *In other words, for any computationally unbounded adversary, and for all input message* m, *if the adversary replaces* m *with a different message* $\widehat{m}$, *then* $\mathcal{R}$ *accepts* $\widehat{m}$ *with probability at most* ϵ.

By the definitions, the property of *perfect completeness* (i.e., $\xi = 1$) in Section 2 is guaranteed if and only if $V(m,x,t) = 1$ holds whenever $P_{XT|M}(x,t,m) > 0$.

For a fixed protocol, i.e., a fixed joint conditional distribution $P_{XT|M}(x,t|m)$, the maximal chance ϵ of success of an adversary could be calculated as

$$\epsilon = \max_{m,t\in\mathcal{T}_m} \max_{\widehat{m}\neq m} \epsilon(\widehat{m}|m,t).$$

Since the adversary has computationally unbounded power, then

$$\begin{aligned}\epsilon(\widehat{m}|m,t) &= \Pr[V(\widehat{m},*,t) = 1 | t \in \mathcal{T}_m] \\ &= \Pr[t \in \Delta_{\widehat{m}} | t \in \mathcal{T}_m] = \Pr[t \in \mathcal{T}_m \cap \Delta_{\widehat{m}}] \\ &= \begin{cases} 1 & \text{if } t \in \Delta_{\widehat{m}}, \\ 0 & \text{if } t \notin \Delta_{\widehat{m}}. \end{cases}\end{aligned}$$

is a boolean-valued function and is only defined for $m, \widehat{m} \in \mathcal{M}^+$.

Theorem 2. *For any information theoretically secure* (ξ,ϵ) *non-interactive manual authentication protocol,* $|\mathcal{M}^+| \leq |\mathcal{T}|$. *Furthermore, if* $\xi = 1$, *then* $H(M) \leq H(T)$, *where* $H(\cdot)$ *denotes the Shannon entropy function.*

Proof. We observe that $\Pr[t \in \mathcal{T}_m \cap \Delta_{\widehat{m}}] \leq \epsilon < 1$ is equivalent to $\Pr[t \in \mathcal{T}_m \cap \Delta_{\widehat{m}}] = 0$ since it is a boolean function. That is to say $\mathcal{T}_m \cap \Delta_{\widehat{m}} = \emptyset$ for all $m \neq \widehat{m} \in \mathcal{M}^+$. Because $\Delta_m \subseteq \mathcal{T}_m$, we further have $\Delta_m \cap \Delta_{\widehat{m}} = \emptyset$ for all $m \neq \widehat{m} \in \mathcal{M}^+$. And, thanks to the completeness property, we know $\Delta_m \neq \emptyset$ for all $P_M(m) > 0$. Together, we can claim that $\{\Delta_m\}_{m\in\mathcal{M}^+}$ forms a partition of a subset of $\mathcal{T}$. So we immediately have $|\mathcal{M}^+| \leq |\mathcal{T}|$. But $|\mathcal{M}| \leq |\mathcal{T}|$ is not necessarily true if there exist some messages m with $P_M(m) = 0$. Instead, we show $H(M) \leq H(T)$ as below.

Denote by P_{MXT} the joint distribution over $\mathcal{M}, \mathcal{X}, \mathcal{T}$ determined by P_M and $P_{XT|M}$. Then $P_{MXT}(m,x,t)$ is computed as $P_M(m) \cdot P_{XT|M}(x,t|m)$. Artificially define a conditional probability

$$\Pr[m|t] = \begin{cases} 1 & \text{if } t \in \Delta_m; \\ 0 & \text{otherwise,} \end{cases}$$

then $H(M|t) = -\sum_{\Pr[m|t]>0} \Pr[m|t] \cdot \log_2 \Pr[m|t] = 0$, which implies $H(M,T) = H(T)$. Following the fact that the joint entropy of two variables is not smaller

than the entropy of either variable, i.e., $H(M,T) \geq H(M)$, we easily arrive at the conclusion $H(T) \geq H(M)$. If $\Pr[m|t]$ matches the conditional distribution $P_{M|T}$ deducted from P_{MXT}, then the conclusion also holds for the protocol.

In the following, we show that for perfect complete non-interactive protocol, $\Pr[m|t]$ does match the conditional distribution $P_{M|T}$ defined by the protocol. In fact, we have for the general case that,

$$\begin{aligned} P_{M|T}(m,t) &= \sum_{x\in\mathcal{X}} \frac{P_{MXT}(m,x,t)}{P_T(t)} = \frac{\sum_{x\in\mathcal{X}} P_M(m)\cdot P_{XT|M}(x,t,m)}{\sum_{m\in\mathcal{M}}\sum_{x\in\mathcal{X}} P_M(m)\cdot P_{XT|M}(x,t|m)} \\ &= \frac{\sum_{x\in\mathcal{X}} P_M(m)\cdot P_{XT|M}(x,t,m)}{\sum_{x\in\mathcal{X}} P_M(m)\cdot P_{XT|M}(x,t,m) + \sum_{m\neq\widehat{m}\in\mathcal{M}}\sum_{x\in\mathcal{X}} P_M(\widehat{m})\cdot P_{XT|M}(x,t,\widehat{m})} \\ &= \begin{cases} 0 & \text{if } m\notin\mathcal{M}^+ \text{ or } t\notin\mathcal{T}_m; \\ p\in(0,1) & \text{if } t\in\mathcal{T}_m\setminus\Delta_m; \\ 1 & \text{if } t\in\Delta_m. \end{cases} \end{aligned}$$

Then we can conclude the proof by noticing that $\mathcal{T}_m = \Delta_m$ for a perfect completeness protocol and thus $\mathcal{T}_m \setminus \Delta_m = \emptyset$. □

5 Conclusions

Manual authentication captures numerous real life scenarios where a sender wants to send a message to a receiver with whom he does not have any pre-distribute keys, however he an use a low bandwidth auxiliary channel to send short strings authentically. We propose an extension of this model where the sender wants to send the message to a group of receivers. We introduce multireceiver manual channel to model devices such as a display used to display a short string to a group of people, or a speaker is used to send a short string to a group. Such a manual channel can be seen as a collection of manual channels, one for each receiver. Our model of adversary is the most powerful one, allowing the adversary to control independently each manual channel. We gave the construction of a protocol that achieves optimal security assuming a trusted infrastructure among receivers. We also showed nontrivial NIMAP in unconditionally secure framework does not exist. An interesting question is to consider extensions of multireceiver manual authentication systems where receivers are connected through other types of trusted mechanisms (e.g. manual channels).

References

1. Simmons, G.J.: Authentication theory/coding theory. In Blakley, G.R., Chaum, D., eds.: CRYPTO. Volume 196 of Lecture Notes in Computer Science., Springer (1984) 411–431
2. Simmons, G.J.: Message authentication with arbitration of transmitter/receiver disputes. In Chaum, D., Price, W.L., eds.: EUROCRYPT. Volume 304 of Lecture Notes in Computer Science., Springer (1987) 151–165

3. Simmons, G.J.: A survey of information authentication. In Simmons, G.J., ed.: Contemporary Cryptology, The Science of Information Integrity. IEEE Press (1992) 379–419 Preliminary version appeared in Proceedings of the IEEE 76 (1988):603-620.
4. Shannon, C.E.: A mathematical theory of communication. Mobile Computing and Communications Review **5**(1) (2001) 3–55
5. Gemmell, P., Naor, M.: Codes for interactive authentication. In Stinson, D.R., ed.: CRYPTO. Volume 773 of Lecture Notes in Computer Science., Springer (1993) 355–367
6. Gehrmann, C.: Cryptanalysis of the gemmell and naor multiround authentication protocol. In Desmedt, Y., ed.: CRYPTO. Volume 839 of Lecture Notes in Computer Science., Springer (1994) 121–128
7. Gehrmann, C.: Secure multiround authentication protocols. In: EUROCRYPT. (1995) 158–167
8. Desmedt, Y., Frankel, Y., Yung, M.: Multi-receiver/multi-sender network security: Efficient authenticated multicast/feedback. In: INFOCOM. (1992) 2045–2054
9. Kurosawa, K., Obana, S.: Characterisation of (k, n) multi-receiver authentication. In Varadharajan, V., Pieprzyk, J., Mu, Y., eds.: ACISP. Volume 1270 of Lecture Notes in Computer Science., Springer (1997) 204–215
10. Safavi-Naini, R., Wang, H.: New results on multi-receiver authentication codes. In: EUROCRYPT. (1998) 527–541
11. Hoepman, J.H.: The ephemeral pairing problem. In Juels, A., ed.: Financial Cryptography. Volume 3110 of Lecture Notes in Computer Science., Springer (2004) 212–226
12. Vaudenay, S.: Secure communications over insecure channels based on short authenticated strings. In Shoup, V., ed.: CRYPTO. Volume 3621 of Lecture Notes in Computer Science., Springer (2005) 309–326
13. Naor, M., Segev, G., Smith, A.: Tight bounds for unconditional authentication protocols in the manual channel and shared key models. In Dwork, C., ed.: CRYPTO. Volume 4117 of Lecture Notes in Computer Science., Springer (2006) 214–231
14. Peyrin, T., Vaudenay, S.: The pairing problem with user interaction. In Sasaki, R., Qing, S., Okamoto, E., Yoshiura, H., eds.: SEC, Springer (2005) 251–266
15. Pasini, S., Vaudenay, S.: An optimal non-interactive message authentication protocol. In Pointcheval, D., ed.: CT-RSA. Volume 3860 of Lecture Notes in Computer Science., Springer (2006) 280–294
16. Rivest, R.L.: Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer. Unpublished manuscript (November 1999) `http://citeseer.ifi.unizh.ch/rivest99unconditionally.html/`.
17. Blundo, C., Masucci, B., Stinson, D.R., Wei, R.: Constructions and bounds for unconditionally secure non-interactive commitment schemes. Design Codes and Cryptography **26**(1-3) (2002) 97–110
18. Wang, S.: Unconditionally secure multi-receiver commitment schemes. Manuscript (2007)
19. Mashatan, A., Stinson, D.R.: Noninteractive two-channel message authentication based on hybrid-collision resistant hash functions (2006)

Appendix

A Description of P_k [13]

For ease of reading and self-completeness, we give a brief description of the single-receiver ($\mathcal{R}$) protocol P_k due to Naor, Segev and Smith [13]. To uniform the notations, we replace C^j with f^j, $i^j_{\mathcal{S}}$ with $A^j_{\mathcal{S}}$, and $i^j_{\mathcal{R}}$ with $B^j_{\mathcal{R}}$.

The protocol P_k:

1. $\mathcal{S}$ sends $m^1_{\mathcal{S}} = m$.
2. For $j = 1$ to $k - 1$.
   (a) If j is odd, then
      i. $\mathcal{S}$ chooses $A^j_{\mathcal{S}} \in_R \mathrm{GF}[Q_j]$ and sends it to $\mathcal{R}$.
      ii. $\mathcal{R}$ receives $\widehat{A}^j_{\mathcal{S}}$, chooses $B^j_{\mathcal{R}} \in_R \mathrm{GF}[Q_j]$, and sends it to $\mathcal{S}$.
      iii. $\mathcal{S}$ receives $\widehat{B}^j_{\mathcal{R}}$, and computes $m^{j+1}_{\mathcal{S}} = \langle \widehat{B}^j_{\mathcal{R}}, f^j_{\widehat{B}^j_{\mathcal{R}}}(m^j_{\mathcal{S}}) + A^j_{\mathcal{S}} \rangle$.
      iv. $\mathcal{R}$ computes $m^{j+1}_{\mathcal{R}} = \langle B^j_{\mathcal{R}}, f^j_{B^j_{\mathcal{R}}}(m^j_{\mathcal{R}}) + \widehat{A}^j_{\mathcal{S}} \rangle$.
   (b) If j is even, then
      i. $\mathcal{R}$ chooses $B^j_{\mathcal{R}} \in_R \mathrm{GF}[Q_j]$ and sends it to $\mathcal{S}$.
      ii. $\mathcal{S}$ receives $\widehat{B}^j_{\mathcal{R}}$, chooses $A^j_{\mathcal{S}} \in_R \mathrm{GF}[Q_j]$, and sends it to $\mathcal{R}$.
      iii. $\mathcal{R}$ receives $\widehat{A}^j_{\mathcal{S}}$, and computes $m^{j+1}_{\mathcal{R}} = \langle \widehat{A}^j_{\mathcal{S}}, f^j_{\widehat{A}^j_{\mathcal{S}}}(m^j_{\mathcal{R}}) + B^j_{\mathcal{R}} \rangle$.
      iv. $\mathcal{S}$ computes $m^{j+1}_{\mathcal{S}} = \langle A^j_{\mathcal{S}}, f^j_{A^j_{\mathcal{S}}}(m^j_{\mathcal{S}}) + \widehat{B}^j_{\mathcal{R}} \rangle$.
3. $\mathcal{S}$ manually authenticates $m^k_{\mathcal{S}}$ to $\mathcal{R}$.
4. $\mathcal{R}$ accepts if and only if $m^k_{\mathcal{S}} = m^k_{\mathcal{R}}$.

Fig. 5. The k-round authentication protocol [13]

B Description of USNIC[p] [17]

Unconditionally secure non-interactive commitment scheme is suggested by Revist [16] and then formally addressed by Blundo, Masucci, Stinson and Wei [17]. As commitment schemes in computational setting, a USNIM scheme provides also two aspects of security. That is *concealing* and *binding* properties. Roughly speaking, concealing means the receiver learns nothing about the committed value before the reveal/open phase and binding means the sender can not change this value after committed. But different to computational setting, USNIM schemes works only in trusted initializer (TI) model – TI trusted by both the sender $\mathcal{S}$ and the receiver $\mathcal{R}$. For more information, please refer to their original work.

Fig. 6 is a brief description of the Affine Plane Commitment Scheme working in $\mathrm{GF}[p] = \mathbb{Z}_p$. We use the notation USNIC[p] to imply that any similar commitment scheme is applicable for our MRMA protocol in Subsection 3.2.

USNIC[p] Scheme:

initialize TI chooses $a, b, x_1 \in_R \mathbb{Z}_p$.
He computes $y_1 = (ax_1 + b) \mod p$.
Then he privately sends (a, b) to $\mathcal{S}$ and (x_1, y_1) to $\mathcal{R}$.

commit Suppose $\mathcal{S}$ wants to commit to the value $x_0 \in \mathbb{Z}_p$.
She computes $y_0 = (x_0 + a) \mod p$ and sends y_0 to $\mathcal{R}$.

reveal $\mathcal{S}$ sends (a, b) and x_0 to $\mathcal{R}$.
$\mathcal{R}$ verifies that $ax_1 + by_1 \mod p$ and $x_0 + a = y_0 \mod p$.
If both congruences hold, $\mathcal{R}$ accepts x_0 and otherwise rejects.

Fig. 6. The USNIC[p] commitment scheme from [17]

The following theorem shows that $\mathcal{R}$'s probability of guessing the value of x_0 after the commit protocol is the same as his probability of randomly guessing it.

Theorem 3 (THEOREM 4.1 of [17]). *The USNIC[p] scheme in Fig. 6 is concealing.*

The following theorem says that the probability of $\mathcal{S}$ cheating $\mathcal{R}$ into accepting a different x_0 is less that $1/p$.

Theorem 4 (THEOREM 4.2 of [17]). *In the USNIC[p] scheme in Fig. 6, the binding probability is equal to* $1 - 1/p$.

C The proof of Theorem 1

Proof. Given an uncorrupted receiver $\mathcal{R}_i \in \mathcal{R} \backslash \mathcal{C}$ who was cheated into accepting a fraudulent message $\widehat{m}_i (= m_i^1) \neq m (= m_{\mathcal{S}}^1)$, it holds that $m_i^j \neq m_{\mathcal{S}}^j$ but $m_i^{j+1} = m_{\mathcal{S}}^{j+1}$ for some $1 \leq j \leq k-1$. As in [13], denote this event by D_j. We similarly prove $\Pr[D_j] \leq \frac{(c+1)\epsilon}{2^{k-j}}$ and therefore the cheating probability is bounded by $\sum_{j=1}^{k-1} \Pr[D_j] \leq \sum_{j=1}^{k-1} \frac{(c+1)\epsilon}{2^{k-j}} \leq (c+1)\epsilon$.

Let $T(x)$ be the time at which the variable x is fixed. Namely, $T(A_{\mathcal{S}}^j)$ denotes the time in which $\mathcal{S}$ sent the tag $A_{\mathcal{S}}^j$, and $T(\widehat{A}_i^j)$ denotes the time in which $\mathcal{R}_i$ received the tag $\widehat{A}_i^j$ from the adversary, corresponding to $A_{\mathcal{S}}^j$; Similarly, $T(\widehat{B}^j)$ denotes the time in which $\mathcal{S}$ received the last $\widehat{B}_l^j$, $l \in [n]$, and $T(B_i^j)$ denote the time in which $\mathcal{R}_i$ opened his commitment for B_i^j.

From the description of the protocol, it holds that all the B_l^j's were chosen before $T(B_i^j)$. So, thanks to the security of the commitment scheme, B_l^j is unchangeable except with a probability $1/Q_j$ (binding property of USNIC[Q_j]) and the other B_l^j's ($l \neq i$) were chosen *independently to* B_i^j (concealing property of USNIC[Q_j]). In the exception case we regard the adversary as being successful, which happens with a probability at most $c/Q_j \leq \frac{c\epsilon}{2^{k-j}}$ (accumulated among all the corrupted users).

In the following we assume the commitment scheme has zero probability for both binding and secrecy. Denote by $\overline{D}_j$ the event D_j under the assumption, the conclusion follows as long as $\Pr[\overline{D}_j] \leq \frac{\epsilon}{2^{k-j}}$ is proved. Under the assumption, we easily have $\Pr_{B_i^j \in_R \mathrm{GF}[Q_j]}[B^j \ (i.e., \sum_{l=1}^{n} B_l^j) = B] = \frac{1}{Q_j}$ for any constant $B \in \mathrm{GF}Q_j]$ and no matter how B_l^j's $(l \neq i)$ were chosen.

Now suppose j is odd, we have the following possible cases:

1. $\mathbf{T}(\widehat{\mathbf{B}}^{\mathbf{j}}) < \mathbf{T}(\mathbf{B}_{\mathbf{i}}^{\mathbf{j}})$: In this case, the receiver $\mathcal{R}_i$ opens the randomly chosen B_i^j only after the adversary chooses $\widehat{B}^j$. Therefore,

$$\Pr[\overline{D}_j] \leq \Pr_{B_i^j \in_R \mathrm{GF}[Q_j]}[\widehat{B}^j = B^j] = \frac{1}{Q_j} \leq \frac{\epsilon}{2^{k-j}}.$$

2. $\mathbf{T}(\widehat{\mathbf{B}}^{\mathbf{j}}) \geq \mathbf{T}(\mathbf{B}_{\mathbf{i}}^{\mathbf{j}})$ and $\mathbf{T}(\widehat{\mathbf{A}}_{\mathbf{i}}^{\mathbf{j}}) \geq \mathbf{T}(\mathbf{A}_{\mathcal{S}}^{\mathbf{j}})$: In this case, the adversary chooses $\widehat{B}^j$ not before the receiver opens the random B_i^j. Then the sum B^j may be known to the adversary. If the adversary chooses $\widehat{B}^j \neq B^j$, then $m_{\mathcal{S}}^{j+1} \neq m_i^{j+1}$, i.e., $\Pr[D_j] = 0$. Now suppose that the adversary chooses $\widehat{B}^j = B^j$. Since j is odd, $\mathcal{R}_i$ chooses (and then opens) B_i^j only after he receives $\widehat{A}_i^j$ from the adversary, therefore $T(B_i^j) > T(\widehat{A}_i^j) \geq T(A_{\mathcal{S}}^j) > T(m_{\mathcal{S}}^j)$, and also $T(B_i^j) > T(m_i^j)$. This means that $m_i^j, m_{\mathcal{S}}^j, \widehat{A}_i^j$ and $A_{\mathcal{S}}^j$ are chosen independently to B_i^j. Define $F(x) := f_x^j(m_{\mathcal{S}}^j) + A_{\mathcal{S}}^j - f_x^j(m_i^j) - \widehat{A}_i^j$, which is a polynomial of degree $d \in [1, \lceil \frac{a_j}{\log Q_j} \rceil]$ (since by assumption $m_{\mathcal{S}}^j \neq m_i^j$). Therefore,

$$\Pr[\overline{D}_j] \leq \Pr_{B_i^j \in_R \mathrm{GF}[Q_j]}[f_{B^j}^j(m_{\mathcal{S}}^j) + A_{\mathcal{S}}^j = f_{B^j}^j(m_i^j) + \widehat{A}_i^j]$$

$$= \Pr_{B_i^j \in_R \mathrm{GF}[Q_j]}[B^j \text{ is a root of } F(x)] = \frac{d}{Q_j} \leq \frac{\epsilon}{2^{k-j}}.$$

3. $\mathbf{T}(\widehat{\mathbf{B}}^{\mathbf{j}}) \geq \mathbf{T}(\mathbf{B}_{\mathbf{i}}^{\mathbf{j}})$ and $\mathbf{T}(\widehat{\mathbf{A}}_{\mathbf{i}}^{\mathbf{j}}) < \mathbf{T}(\mathbf{A}_{\mathcal{S}}^{\mathbf{j}})$: As in the previous case, we can assume that the adversary chooses $\widehat{B}^j = B^j$. It always holds that $T(A_{\mathcal{S}}^j) > T(m_{\mathcal{S}}^j)$ and $T(B^j) > T(B_i^j) > T(m_i^j)$. Since j is odd, $\mathcal{R}_i$ sends (before he opens) B_i^j only after he receives $\widehat{A}_i^j$, therefore $T(\widehat{A}_i^j) < T(B_i^j)$. And we can assume $T(B_i^j) < T(A_{\mathcal{S}}^j)$ (otherwise we have $T(B_i^j) > \{T(A_{\mathcal{S}}^j), T(\widehat{A}_i^j), T(m_{\mathcal{S}}^j), T(m_i^j)\}$ as in case 2). This implies that $\mathcal{S}$ chooses $A_{\mathcal{S}}^j \in_R \mathrm{GF}[Q_j]$ when $m_{\mathcal{S}}^j, m_i^j, \widehat{A}_i^j$ and B^j are fixed. As a result,

$$\Pr[\overline{D}_j] = \Pr_{A_{\mathcal{S}}^j \in_R \mathrm{GF}[Q_j]}[A_{\mathcal{S}}^j = f_{B^j}^j(m_i^j) + \widehat{A}_i^j - f_{B^j}^j(m_{\mathcal{S}}^j)] = \frac{1}{Q_j} \leq \frac{\epsilon}{2^{k-j}}.$$

When j is even, the conclusion follows in the same way. We just need to change the roles of A and B in classifying the possible cases. That is, i) $T(\widehat{A}_i^j) < T(A_{\mathcal{S}}^j)$; ii) $T(\widehat{A}_i^j) \geq T(A_{\mathcal{S}}^j)$ and $T(\widehat{B}^j) \geq T(B_i^j)$; and iii) $T(\widehat{A}_i^j) \geq T(A_{\mathcal{S}}^j)$ and $T(\widehat{B}^j) < T(B_i^j)$. Also refer to [13] for more details. □