The Multireceiver Commitment Schemes

Shuhong Wang

Sumavision Technologies Co., Ltd.
godintears@gmail.com

Abstract. Existing commitment schemes were addressed under the classic two-party scenario. However, popularity of the secure multi-party computation in today's lush network communication is motivating us to adopt more sophisticate commitment schemes. In this paper, we study for the first time multireceiver commitment in unconditionally secure setting, i.e., one committer promises a group of verifiers a common secret value (in computational setting it is trivial). We extend the Rivest model for this purpose and present a provably secure generic construction using multireceiver authentication codes (without secrecy) as a building block. Two concrete schemes are proposed as its immediate implementations, which are almost as efficient as an optimal MRA-code. Furthermore, to affirmatively answer the open question of Pinto, Souto, Matos and Antunes, we present also a generic construction (for two-party case) using only an A-code with secrecy. Finally, we show the possibility of constructing multireceiver commitment schemes using other primitives such as verifiable secret sharing. We leave open problems and believe the work will open doors for more interesting research.

1 Introduction

Commitment schemes were first introduced by Blum [2]. To the best of our knowledge, commitment scheme in the unconditionally secure setting was first studied by Rivest [13] (using noiseless channels only). Then Blundo *et al* [3] gave the first mathematical formalization of an unconditionally secure commitment scheme, followed by Pinto *et al* [12] presenting a relation between which and unconditionally secure authentication schemes (A-codes). That is, an unconditionally secure commitment scheme can be built from such an A-code and an unconditionally secure cipher system, and in the opposite, a resolvable design (/optimal) commitment scheme is a composition of an A-code and a cipher system.

However, all the previous commitment schemes, both computationally secure ones [9] and unconditionally secure ones[1], were studied in the traditional two-party scenarios. The aim of this paper is to investigate the possibility of multi-party (esp. multireceiver) commitment schemes where a committer wants to commit himself to a value to a group of receivers. We will only focus on the unconditionally secure settings for the following reason: In computationally secure settings, the security of commitment schemes are based on the hardness of efficiently solving some computational problems, and most often are non-interactive. Thus any two-party commitment scheme is automatically a multireceiver commitment scheme.

In the unconditionally secure settings, however, it is well known (and easy to see) that *in a two-player scenario with only noiseless communication OT [Oblivious Transfer] and BC [Bit Commitment] with information-theoretic security is not possible, even if only passive cheating is assuming, and players are allowed infinite computing power [6].* This is the reason why Rivest introduced the so-called *trusted initializer* model where the dependence

[1] Including [11] in which either the committer or the receiver, but not both, has infinite computational power.

on the trusted party is minimized. We will also talk about MRC (multireceiver commitment) schemes under a similar extended model, assuming multicast channel exits.

More specifically, there are three different roles in the model: a trusted initializer Ted, a committer Alice and a group of receivers Bobs $\mathcal{R} = \{\mathcal{R}_1, \mathcal{R}_2, \cdots, \mathcal{R}_n\}$ ($n = 1$ in traditional cases [13, 3, 12]). Ted is only involved in the *initialization* phase, distributing secrets to Alice and $\mathcal{R}$, and then keeps inactive. When Alice wants to commit to a secret value x (of her choice) to all the receivers, she sends some *commitment* information, say y, to $\mathcal{R}$, by multicasting rather than repeatedly sending to each receiver. To disclosure the secret x, Alice sends (multicasts) some extra *decommitment* information z. Using y, z and his own secret, every receiver $\mathcal{R}_i \in \mathcal{R}$ should be able to make decision *independently* on accepting or rejecting the disclosure made by Alice and recover x on acceptance. Formal definition and properties of MRC will be given in the next section.

A trivial MRC scheme could be as simple as n copies of single receiver commitment schemes, which provides the strongest security. That is, any number of participants cannot collude to cheat the others successfully. However its inefficiency would not be acceptable and there seems no direct way to gain more efficiency for even weaker security, for instance, against $\omega < n$ colluders. In our generic construction of MRC, we will provide an option of the number ω of colluders. And we propose two concrete instances of the generic scheme, whose efficiency (of computation and communication both) is much better than the aforementioned trivial approach. This is true for even $\omega = n$ (out of the $n + 1$ participants including Alice and n Bobs).

Contributions: In brief, our contribution can be summarized as the following. We present for the first time the concept of *multi-party commitment* in the unconditionally secure setting, which is useful for the emerging popular multi-party computations. We address especially the *multireceiver commitment* (MRC for short) schemes in more details. The analogue concepts of *multi-sender commitment* and even *multi-initializer commitment* can be defined in a similar manner.

We construct a generic MRC scheme which achieves information-theoretic security against any certain number of colluders, and two concrete MRC schemes which are more efficient and flexible than running the traditional two-party commitment scheme separately with each receivers. More specifically, the computation of a commitment for n receivers is only one additive operation over $\mathbb{F}$, and the computation of an individual verification is as efficient as the one in optimal MRA-codes (i.e., one evaluation of a degree ω polynomial over $\mathbb{F}$). And sizes of secret keys for Alice and Bob's are only $O(\omega)$ with the hidden constant being 1 and 2 field elements, respectively.

We also point out for this new topic some possible issues as future research directions. Hopefully, more interesting issues and applications of MRC schemes will be found in the future. As initial attempts in some directions, we propose another generic MRC scheme using VSS (verifiable secret sharing) as a building block instead of using MRA-codes (multireceiver authentication codes). It is worthy to notice that one of the two concrete implementations under the first generic construction can also be viewed as an implementation under the latter seemingly completely different framework. This naturally propose an interesting question to investigate the fundamental relation among MRC, MRA and VSS primitives.

Back to the two party commitment scenario, we further propose an attractive solution different from all the existing constructions. Our construction bases on only an A-code with secrecy, which affirmatively answers the question of Pinto et al [12] – whether an A-code with secrecy only can be used to construct an unconditionally secure commitment scheme.

Paper organization: The remainder of the paper is organized as follows. In the next section (Section 2) we present the formal definition of (non-interactive) multireceiver commitment (MRC) schemes secure against up to ω colluders. Then in Section 3 some useful primitives are recalled, followed by a generic construction of MRC scheme in Section 4.1, whose security is reduced to the underlying primitives. Two efficient instances of the generic scheme are given in Section 4.2. In Seciton 5 we show how to construct commitment schemes (for either single receiver or multireceiver cases) using other primitives (i.e., A-code with secrecy in Section 5.1 and verifiable secret sharing in Section 5.2, respectively). Finally in Section 6 we end this work with some conclusive remarks.

2 MRC model and definitions

For the reason aforementioned, all issues addressed in this section is under the information-theoretical settings and for reading convenience, we always use calligraphic letters for domains/sets, the corresponding lowercase letters for their elements and the uppercase letters for random variables over respective domains/sets.

As in the basic commitment model of [13], there are three roles in our multireceiver commitment model, namely the trusted-initializer role, the sender role and the receiver role. Although we focus only on multireceiver case, every role could be played by multiple players. To facilitate reading, we call the single trusted-initializer Ted and the single sender Alice, but denote the group of players playing the receiver role by $\mathcal{R} = \{\mathcal{R}_1, \mathcal{R}_2, \cdots, \mathcal{R}_n\}$.

Assume Ted is connected to Alice and $\mathcal{R}$ with secure (both confidential and authentic) channels, while Alice and $\mathcal{R}$ are connected by insecure channels, i.e., an adversary is able to eavesdrop, delay, modify and insert messages over the channels. We assume *broadcast/multicast*[2] is allowed from Alice to the receivers $\mathcal{R}$. Also, we assume all the communication channels in use are noiseless. In our (non-interactive) model, connections among $\mathcal{R}$ is not necessary, but these connections may exist such that part of the dishonest players are able to collude. What property the colluding connections satisfy is out of our scope.

Remark 1. In the definition of *broadcast*, Agarwal *et al* observed that *since the [broadcast] value can then be correctly determined using majority voting on the other end, such values are always perfectly reliably transmitted. Since corruptions that occur during broadcasts are easy to detect, in the sequel we (Agarwal, Cramer and de Haan) assume without loss of generality that broadcasts occur without any corruptions on the channels [1].* However, using majority voting needs the players *on the other end* interactively communicate, which is not desirable in our model. Thus *corruptions that occur during broadcasts* are possible. Nevertheless the corruptions as such can be modelled by dishonest Alice which is the case we considered in this paper.

The formal model (information flows) of MRC schemes is illustrated in Figure 1 below. The trusted initializer Ted pre-distributes the secret keys to each participants in advance of even Alice yet deciding the value to commit to and keeps off-line after the initialization phase.

[2] As defined in [1], a value is said to be broadcasted/multicasted if it is simultaneously sent over all communication channels. We do not care whether the message simultaneously arrives at the receivers.

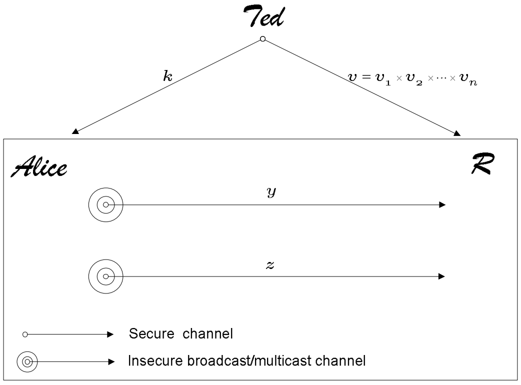
Ted
k
$v = v_1 \times v_2 \times \cdots \times v_n$
Alice
$\mathcal{R}$
y
z
Secure channel
Insecure broadcast/multicast channel

Fig. 1. The trusted initializer MRC model.

Now a (non-interactive) multireceiver commitment scheme can be formally defined as follows.

Definition 1. *A (non-interactive) multireceiver commitment scheme MRC=($\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, $\mathcal{K}$, $\mathcal{V}$) is composed of four algorithms* $(\mathsf{Gen}, \mathsf{Com}, \mathsf{Dcm}, \mathsf{Ver})$ *described below. Where $\mathcal{X}$ denotes the set of values to be committed, $\mathcal{Y}$ the set of commitments, $\mathcal{Z}$ the set of decommitments, $\mathcal{K}$ the set of keys for Alice and $\mathcal{V} = \mathcal{V}_1 \times \cdots \times \mathcal{V}_n$ is the direct production of the sets of verification keys for receivers $\mathcal{R} = \{\mathcal{R}_1, \cdots, \mathcal{R}_n\}$.*

Ted uses Gen*, a probabilistic algorithm, to generate the pair $(k, v) \in \mathcal{K} \times \mathcal{V}$ of which k is securely sent to Alice and v to $\mathcal{R}$; The algorithm* $\mathsf{Com} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ *is used when Alice wants to commit to a value $x \in \mathcal{X}$ using her secret k. Its output y is sent to $\mathcal{R}$ as a commitment to the value x; The algorithm* $\mathsf{Dcm} : \mathcal{K} \times \mathcal{X} \to \mathcal{Z}$ *is invoked to produce the decommitment information z when Alice wants to reveal the value x and the algorithm* $\mathsf{Ver} = \mathsf{Ver}_1 \times \cdots \times \mathsf{Ver}_n$ *where each* $\mathsf{Ver}_i : \mathcal{V}_i \times \mathcal{Y} \times \mathcal{Z} \to \{0, 1\} \times \mathcal{X}$ *is used by the receiver $\mathcal{R}_i$ to verify the correctness of decommitment z with respect to the commitment y and to recover the value x.*

Correctness: *When all players are honest, every receiver will accept and recover the committed value correctly. That is, for all (k, v) generated by* Gen *and for all $x \in \mathcal{X}$, $y = \mathsf{Com}(k, x)$ and $z = \mathsf{Dcm}(k, x)$, the equality $\mathsf{Ver}_i(v_i, y, z) = (1, x)$ holds for all $i \in \{1, 2 \cdots, n\}$.*

In this paper, we assume full trust on Ted but no trust at all on Alice and $\mathcal{R}$. That is, Ted always securely distributes correct secrets k and v to Alice and $\mathcal{R}$, respectively and would neither mount attacks to other players nor collude with any player. However, Alice may collude with some receivers to cheat other receivers (fooling them to accept the commitment as to a value different from x) and a subset of receivers may collude to cheat Alice (recovering the value x before receiving z) or even the remaining receivers. For simplicity of presentation, let $\mathcal{N}$ be the set of indices $\{1, 2, \cdots, n\}$ and $\mathcal{C}$ a subset of $\mathcal{N}$ of size not bigger than ω. Thus $\mathcal{R}_\mathcal{C} := \{\mathcal{R}_i : i \in \mathcal{C}\}$ denotes the subset of receivers who collude and $\mathcal{V}_\mathcal{C} := \{v_i : i \in \mathcal{C}\}$ denotes the secret information of the colluders.

Remark 2. Notice that the randomness of algorithm Gen automatically introduces randomness on k and v; and together with the randomness of x, further introduce randomness on y, z, b_i and x_i, where $(b_i, x_i) := \mathsf{Ver}_i(v_i, y, z)$. As stated in the beginning of this section, we denote the random variables associating with these values by respectively K, V, X, Y, Z, B_i, X_i and the corresponding probability distributions by $\mathcal{D}_K, \mathcal{D}_V, \cdots, \mathcal{D}_{X_i}$. We will simplify the probability, say $\Pr[X = x]$, using $\Pr[x]$ as shorthand if without making confusion.

Definition 2. *An MRC scheme is said to be information-theoretically* (α, β, γ)-secure against up to ω colluders *if it satisfies the following properties, even if the colluders $\mathcal{R}_\mathcal{C}$ have unbounded computational power:*

- $(1-\alpha)$-binding: *Alice cannot change her mind after sending the commitment y except with at most a probability α of success, even with the help of the colluders $\mathcal{R}_\mathcal{C}$. That is, for any $y = \mathsf{Com}(k, x)$, the conditional probability $\Pr[b_i = 1, x_i \neq x | k, \mathcal{V}_\mathcal{C}] \leq \alpha$ holds for every $z \in \mathcal{Z}$ and every $i \in \mathcal{N} \setminus \mathcal{C}$* [3]*, where $(b_i, x_i) = \mathsf{Ver}_i(v_i, y, z)$ and $y = \mathsf{Com}(k, x)$.*
- $(1-\beta)$-origin: *The colluders of up to ω receivers should not be able to impersonate Alice making commitment acceptable by any receiver with a probability bigger than β. That is, the probability $\max_{i \in \mathcal{N} \setminus \mathcal{C}} \max_{y,z} \Pr[b_i = 1 | \mathcal{V}_\mathcal{C}] \leq \beta$. Remember $(b_i, *) = \mathsf{Ver}_i(v_i, y, z)$.*
- $(1-\gamma)$-hiding: *The colluders $\mathcal{R}_\mathcal{C}$ can not learn more than* a priori *information of the committed value x from the commitment y, except with at most a probability γ. That is, the equality $\Pr[x | y, \mathcal{V}_\mathcal{C}] = \Pr[x]$ holds with probability at least $1-\gamma$, where $y = \mathsf{Com}(k, x)$.*

An simpler alternation of *(α, β, γ)-security against up to ω colluders* is $(\alpha, \beta, \gamma : \omega)$-*security.* Most often, we can have commitment schemes with $\gamma = 0$ and therefore we particularly name them to be (α, β)-*secure* or $(\alpha, \beta : \omega)$-*secure* if up to ω colluders are allowed. We say a commitment scheme provides *perfect hiding* or is *concealing* [4] as per the terminology for single receiver setting [3] if it is (α, β)-secure.

Note that a single receiver concealing commitment providing with $(1-\alpha)$-binding property is an $(\alpha, \perp, 0 : 1)$-secure scheme using our terminology, since β does not exist at all and $\omega = 1$ only makes sense for binding property. Therefore simplified as above, merely α-security or (α, γ)-security is enough for define the security for single receiver commitment schemes. This shows that the multireceiver setting is much more complicated than the single receiver setting.

3 Preliminaries

We recall in this section some useful primitives.

An *encryption* system $ENC = (\mathcal{X}, \mathcal{Y}, \mathcal{S})$ is composed of two functions $(\mathsf{Enc}, \mathsf{Dec})$. Where $\mathcal{X}$ is the set of plaintext, $\mathcal{Y}$ the set of the ciphertext and $\mathcal{S}$ the set of the secret keys. The function $\mathsf{Enc} : \mathcal{S} \times \mathcal{X} \to \mathcal{Y}$ maps every plaintext x to a ciphertext y under the secret s while the function $\mathsf{Dec} : \mathcal{S} \times \mathcal{Y} \to \mathcal{X}$ decrypts y to the plaintext x using the same secret. Note that for every s, the function $\mathsf{Enc}_s(\cdot) := \mathsf{Enc}(s, \cdot)$ should be injective and well defined for all

[3] When such i does not exist, i.e., $\mathcal{N} \setminus \mathcal{C} = \emptyset$, we artificially set as zero the not well-defined probability. This way we can uniformly have $0 \leq \omega \leq n$.

[4] Concealing or perfect hiding can also be equivalently defined as $H(X|Y, V_\mathcal{C}) = H(X)$ where $V_\mathcal{C}$ denotes the random variable associate to colluders' secrets $v_\mathcal{C}$ and $H(X)$ denotes the Shannon entropy of the random variable X.

$x \in \mathcal{X}$. For an information-theoretical secure encryption system ENC, the random variables X, S and $Y = \mathsf{Enc}(S, X)$ satisfies $H(X|S) = H(X)$.

A *multireceiver authentication code* (MRA-code) $MRA = (\mathcal{S}, \mathcal{M}, \mathcal{E}, \mathcal{V})$ is composed of three algorithms $(\mathsf{EGen}, \mathsf{Tg}, \mathsf{Vf})$. Where $\mathcal{S}$ denotes the set of source states; $\mathcal{M}$ denotes the set of authentication messages which is also written as $\mathcal{S} \times \mathcal{T}$ for a cartesian MRA-code, i.e., MRA-code without secrecy; $\mathcal{E}$ denotes the set of keys for the sender (alias Alice) and $\mathcal{V} = \mathcal{V}_1 \times \cdots \times \mathcal{V}_n$ denotes the direct production of the sets of keys for the receivers $\mathcal{R}$.

The three algorithms are used in the three phases of an MRA scheme. We briefly explain them as follows. In the initialization phase, a trusted initializer (alias, Ted) runs EGen to generate the encoding rule $e \in \mathcal{E}$ for Alice and verification rules $v \in \mathcal{V}$ for all the receivers. In the authentication (of source state s) phase Alice calculates $t = \mathsf{Tg}(e, s)$ and sends/broadcasts the message $m := (s, t)$ to R. Then each receiver $\mathcal{R}_i$, using his own verification rule v_i, is able to verify the authenticity of m by the function $\mathsf{Vf}_i(v_i, m) \in \{0, 1\}$.

We say that an MRA-code is an (ω, n)-MRA-code if up to ω-out-of-the-n receivers colluding is not able to learn any information about the *verification key* of any other receiver [10], or equivalently if the chance of success of any group of up to ω receivers in an impersonation (as well as a substitution) attack is the same as an outsider [14]. We denote these chances as P_I (and P_S) respectively.

Remark 3. There are two differences comparing to the definitions in [10, 14]. One is that we distinguish the secret keys held by Alice and the receivers, while [10, 14] assume Alice knows the keys of all receivers. Second is that in order to simplify the notations, we define the (ω, n)-MRA-code to be against ω, instead of $\omega - 1$ in the later, colluders. Another thing worthy pointing out is that Safavi-Naini and Wang extended the definition of an (ω, n)-MRA-code to be an MRA-code in which no subset of ω (again, slightly revised) receivers can construct a *fraudulent message* accepted by another receiver. For completeness, we recall below the definition of an MRA-code of [14] which is based on basic A-codes. The following notations needs explanation. Let p_i be the projection mapping defined by $p_i(x_1, x_2, \cdots, x_n) := x_i$, $1_{\mathcal{S}}$ be the identity mapping on $\mathcal{S}$ and $g_1 \times g_2$ the direct product of two mappings $g_1 : \mathcal{X}_1 \to \mathcal{Y}_1$ and $g_2 : \mathcal{X}_2 \to \mathcal{Y}_2$ defined as $(g_1 \times g_2)(x_1, x_2) := (g_1(x_1), g_2(x_2))$.

> Definition 3.1 of [14]. Let $A = (\mathcal{S}, \mathcal{M}, \mathcal{E}, f)$ and $A_i = (\mathcal{S}, \mathcal{M}_i, \mathcal{E}_i, f_i), i = 1, 2, \cdots, n$, be authentication codes. We call $(A; A_1, A_2, \cdots, A_n)$ an MRA-code if there exist two mappings $\tau : \mathcal{E} \to \mathcal{E}_1 \times \cdots \times \mathcal{E}_n$ and $\pi : \mathcal{M} \to \mathcal{M}_1 \times \cdots \times \mathcal{M}_n$ such that for any $(s, e) \in \mathcal{E}$ and any $1 \leq i \leq n$, the following identity holds
>
> $$p_i(\pi \circ f(s, e)) = f_i((1_{\mathcal{S}} \times p_i \tau)(s, e)).$$

4 MRC constructions using cartesian MRA-codes

4.1 A generic construction

Given an encryption system $ENC = (\mathcal{X}, \mathcal{Y}, \mathcal{S}, \mathsf{Enc}, \mathsf{Dec})$ and a multireceiver authentication scheme $MRA = (\mathcal{S}, \mathcal{M}, \mathcal{E}, \mathcal{V}, \mathsf{EGen}, \mathsf{Tg}, \mathsf{Vf})$ without secrecy, i.e., $\mathcal{M} = \mathcal{S} \times \mathcal{T}$, there is a generic multireceiver commitment scheme GMRC with domains $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{K}, \mathcal{V})$ where $\mathcal{K} = \mathcal{Z} = \mathcal{S} \times \mathcal{T}$ and algorithms $(\mathsf{Gen}, \mathsf{Com}, \mathsf{Dcm}, \mathsf{Ver})$ described as the following:

1. *Initialization:* A trusted initializer (TI) pre-distributes secrets $(k, v) := (m, v) \in \mathcal{M} \times \mathcal{V}$ generated by Gen to participants. For this purpose, TI runs EGen to obtain $(e, v) \in_R \mathcal{E} \times \mathcal{V}$ and randomly chooses a source state $s \in_R \mathcal{S}$, computes $t = \mathsf{Tg}(e, s) \in \mathcal{T}$. Then $m = (s, t)$ is sent to Alice and v_i is sent to the receiver $\mathcal{R}_i$, both through secure channels.
2. *Commitment:* To commit a value $x \in \mathcal{X}$, Alice calculates $y = \mathsf{Enc}(s, x)$ (i.e., $\mathsf{Com}(k, x) = \mathsf{Enc}(s, x)$) and multicasts[5] it to the receivers $\mathcal{R}$.
3. *Decommitment:* To reveal the value x, Alice multicasts $z = \mathsf{Dcm}(k, x) = k = m = (s, t)$ to $\mathcal{R}$. Then $\mathcal{R}_i$ accepts if $\mathsf{Vf}_i(v_i, m) = 1$ and recovers the committed value $x = \mathsf{Dec}(s, y)$, that is, $\mathsf{Ver}_i(v_i, m) = (\mathsf{Vf}_i(v_i, m), \mathsf{Dec}(s, y))$.

Theorem 1. *Suppose the underlying encryption system is perfect secure and the MRA-code is a (ω, n) MRA-code, then the generic MRC scheme constructed above is $(P_S, P_I : \omega)$-secure, where P_I, P_S denote respectively the maximal probability of an adversary succeeding in the impersonation and the substitution attacks in the MRA-code.*

Proof (sketch). We reduce the security of our scheme to the corresponding security of the underlying MRA-code. The reduction is performed as below on the three properties separately.

$(1 - P_S)$*-Binding:* That is $\max_{i \in \mathcal{N} \setminus \mathcal{C}} \max_{z'} \Pr[\mathcal{R}_i \text{ accepts } m' \text{ and } x' \neq x] \leq P_S$, where $m' = (s', t')$ and $x' = \mathsf{Dec}(s', y)$. This inequality is easy to see from the definition of MRA, $P_S = \max_{i \in \mathcal{N} \setminus \mathcal{C}} \max_{m'} \Pr[\mathcal{R}_i \text{ accepts } m' \text{ and } m' \neq m]$, and the observation that the event $(\mathcal{R}_i \text{ accepts } m') \wedge (x' \neq x)$ implies the event $(\mathcal{R}_i \text{ accepts } m') \wedge (m' \neq m)$ and that $m' \neq m$ is equivalent to $z' \neq z$. Thus $\max_{z'} \Pr[\mathcal{R}_i \text{ accepts } m' \text{ and } x' \neq x] \leq \max_{z'} \Pr[\mathcal{R}_i \text{ accepts } m' \text{ and } m' \neq m] = \max_{m'} \Pr[\mathcal{R}_i \text{ accepts } m' \text{ and } m' \neq m]$, and the conclusion follows.

$(1 - P_I)$*-Origin:* That is $\max_{i \in \mathcal{N} \setminus \mathcal{C}} \max_{y,z} \Pr[\mathsf{Ver}_i(v_i, m) = (1, *) | V_\mathcal{C} = \mathcal{V}_\mathcal{C}] \leq P_I$. This relation follows simply from that $\max_{y,z} \Pr[\mathsf{Ver}_i(v_i, m) = (1, *) | V_\mathcal{C} = \mathcal{V}_\mathcal{C}] = \max_m \Pr[\mathsf{Vf}_i(v_i, m) = 1 | V_\mathcal{C} = \mathcal{V}_\mathcal{C}]$, exactly the impersonation probability of the MRA-code.

Perfect Hiding: That is $H(X|Y, V_\mathcal{C}) = H(X)$, which follows from the perfect secrecy of the one-time-pad, the fact that $x \in \mathcal{X}$ is chosen by Alice independently to $v_\mathcal{N}$ distributed by Ted, and the security of the (ω, n)-MRA-code. In other words we have $H(X|Y) = H(X)$, $H(X|V_\mathcal{C}) = H(X)$ and $H(S|V_\mathcal{C}) = H(S)$ if only $|\mathcal{C}| \leq \omega$. Remember that in the generic scheme $s \in \mathcal{S}$ serves as the secret key of the one-time pad. Therefore $V_\mathcal{C}$ is independent to the whole encryption system and hence $H(X|Y, V_\mathcal{C}) = H(X|Y) = H(X)$. □

Complexity of the protocol: The computation complexity of the whole protocol equals to that of the encryption system and the MRA-code. However the communication complexity is only that of the MRA-code, since we do no need to distribute the encryption key which is part of the MRA-code (i.e., the source code). So for this construction, we can immediately have the bounds on the size of each domain as well as on α and β. The proof of the following theorem will be presented in the full version of the paper.

Theorem 2. *In the GMRC construction above, suppose TI distributes keys uniformly, then it holds that $|\mathcal{V}_i| \geq \frac{1}{\alpha\beta}$ and $|\mathcal{K}| \geq (\frac{1}{\alpha})^{\omega+1} |\mathcal{X}|$.*

[5] Alice may send different $y_i = \mathsf{Enc}(s, x_i)$ to $\mathcal{R}_i$ to commit to different values x_i.

These bounds are tight for MRC schemes derived from GMRC. Particularly, the scheme MRC1 in the next subsection achieves these bounds and therefore is optimal in sense of key sizes.

More than one commitments: By using the MRA-code with higher level, say ℓ, of security, Alice (the committer) can make more than one (i.e., ℓ) commitments without the necessity of changing verification secrets at the receivers sides. This is done by the TI distribute more messages $m_i = (s_i, t_i), 1 \leq i \leq \ell$ to Alice. But be careful, we need some specific redundance on the source states s_i, otherwise the Alice can easily change her mind by sending a different m_i in the open phase. To this end, we can require, for example, the last $\lceil \log_2 \ell \rceil$-bit of s_i to be the binary representation of number i, i.e., $s_i = s'_i || i \in \mathcal{S}$, and therefore any change of her mind implies a substitute attack of order ℓ on the underlying MRA-code.

4.2 Two concrete MRC schemes

MRC1 can be viewed as an extension of [12] in the viewpoint of composition of cipher system and authentication code (i.e, from A-code to (ω, n) MRA-code), while MRC2 can be viewed as an extension of [13] in the viewpoint of verifiable secret key sharing (i.e., from $(1, |\mathbb{F}|)$-sharing to $(\omega, |\mathbb{F}|)$-sharing).

We choose the cryptosystem to be the one-time pad over a finite Galois Field $\mathbb{F}$ (the addition, minus and product are denoted as $+, -$ and $\cdot$). That is $\mathcal{X} = \mathcal{Y} = \mathcal{S} = \mathbb{F}$. Then $\mathsf{Enc}(s, x) = s + x$ and obviously $\mathsf{Dec}(s, y) = y - s$.

MRC1:
We choose the MRA to be the polynomial based construction due to DFY [7]. The sender's encoding rule is two random polynomials $e = (f(X), g(X))$ of degree ω. Then for each receiver $\mathcal{R}_i$, whose verification rule $e_i = (f(i), g(i)) \in \mathbb{F}^2$ is generated by evaluating the polynomials at i (which could be public). To authenticate a source $s \in \mathbb{F}$, the sender calculates $t(X) = f(X) + s \cdot g(X)$ and sends $m = (s, t(X))$ to the receivers. Then $\mathcal{R}_i$ accepts s as authentic if and only if $t(i) = f(i) + s \cdot g(i)$.

Now the MRC scheme is constructed as follows. The TI distributes $k = m = (s, t(X))$ to Alice and $v_i = e_i = (f(i), g(i))$ to the receiver $\mathcal{R}_i$. In the commitment phase for a value $x \in \mathbb{F}$, Alice calculates $y = \mathsf{Enc}(s, x) = x + s$ and multicasts it to $\mathcal{R}$. In the decommitment phase, Alice multicasts $k = (s, t(X))$. $\mathcal{R}_i$ accepts if $t(i) = f(i) + s \cdot g(i)$ and in the positive case recovers the value $\mathsf{Dec}(s, y) = y - s = x$.

The secret keys of Alice and each receiver consists respectively of $(\omega + 2)$ and 2 elements in $\mathbb{F}$, in total $2n + \omega + 2$ elements. The bit length of message communicated (multicasted) is $(\omega + 3) \log_2 |\mathbb{F}|$.

MRC2:
The TI distributes to Alice a random polynomial $f(X)$ over $\mathbb{F}$ of degree ω and, to each receiver $\mathcal{R}_i$ a random point $v_i = (x_i, y_i)$ on the polynomial (i.e., $y_i = f(x_i)$). Let $s = f(0)$ denote the constant term of the polynomial f. Note that s is uniformly distributed in $\mathbb{F}$ when f is uniformly chosen at random.

Then Alice multicasts the ciphertext [6] $y = \mathsf{Enc}(s, x) = s + x$ as the commitment to the value $x \in \mathbb{F}$, and simply reveals her secret $f(X)$ as decommitment. For each $\mathcal{R}_i$, he accepts if v_i is on the polynomial and the value x is then recovered to be $\mathsf{Dec}(f(0), y) = x$.

The secret keys of the sender Alice and every receiver consists of $(\omega + 1)$ and 2 elements in $\mathbb{F}$, respectively. In total $2n + \omega + 1$ elements. The length of message communicated is $(\omega + 2) \log_2 |\mathbb{F}|$.

Following the security proof for the generic construction, we immediately have the corollary below.

Corollary 1. *Let $q = |\mathbb{F}|$. The schemes MRC1 and MRC2 both are $(\frac{1}{q}, \frac{1}{q} : \omega)$-secure.*

If one chooses to trivially run n copies of the Rivest protocol, there will be $2n$ field elements in the secret key of Alice. This is true even for any ω. It is obvious inefficient compared to both of our schemes, especially for small ω cases. Furthermore, the length of messages communicated is almost 3 times of our schemes. Actually, a straightforward but non-trivial extension of the Rivest protocol can be constructed as follows (MRC0), resulting in an MRC scheme equivalent to at least ω copies of the Rivest protocol. Its sender secret key is twice of MRC1 or MRC2. And MRC0 becomes the trivial approach in case of largest number of colluders, i.e., $\omega = n - 1$.

MRC0:
The trusted initializer generates two polynomials $f(X)$ and $g(X)$ of degree ω, over $\mathbb{F}$. Then the key values for the sender Alice and the receiver $\mathcal{V}_i$ are respectively $(f(X), g(X))$ and (x_i, y_i) where $x_i \in_R \mathbb{F}$ and $y_i = f(i) + x_i \cdot g(i)$.

To commit to a value x, Alice constructs $F(X) = f(X) + x \cdot g(X)$ and sends $y = F(X)$ as her commitment. To open the commitment, she sends $z = (x, f(X), g(X))$. Then each receiver $\mathcal{V}_i$ checks whether the following two relations hold and accepts x if both checks succeed.

- $F(X) = f(X) + x \cdot g(X)$; that is the commitment and decommitment match.
- $y_i = f(X)|_{X=i} + x_i \cdot g(X)|_{X=i}$; that is the released information matches the secret key (x_i, y_i) of the receiver.

Theorem 3. *Let $q = |\mathbb{F}|$. The scheme MRC0 is $(\frac{1}{q}, \frac{1}{q}, \frac{\omega}{q} : \omega)$-secure.*

Proof (sketch). The security mainly follows the security of Rivest's commitment protocol for a single verifier. But there are subtle differences.

$(1 - \frac{1}{q})$-*Binding:* Suppose Alice (even with up to ω colluding receivers) wants to change her mind to $x' \neq x$. She substitutes $f(X), g(X)$ with $f'(X), g'(X)$ such that $f(X)|_{X=i} + x_i \cdot g(X)|_{X=i} = f'(X)|_{X=i} + x_i \cdot g'(X)|_{X=i}$ and $F(X) = f'(X) + x' \cdot g'(X)$. Unless with a probability $1/q$ she guesses x_i correctly, she has to chose f', g' such that $f(i) = f'(i)$ and $g(i) = g'(i)$. In this case Alice cannot be successful because $f(i), g(i)$ and $F(X)|_{X=i}$ uniquely determine the value $x = \frac{F(X)|_{X=i} - f(X)|_{X=i}}{g(X)|_{X=i}}$. Therefore unless with probability $1/q$, we always have $x' = \frac{F(X)|_{X=i} - f'(X)|_{X=i}}{g'(X)|_{X=i}} = x$. That is the binding property is satisfied.

[6] In the Rivest protocol $y = f(x)$ which has been shown [3] possessing a minor flaw - it is not *perfectly* hiding. Furthermore, one more element (i.e., x) has to be multicasted in the decommitment phase.

$(1-\frac{1}{q})$-*Origin:* Since $f(X), g(X)$ are polynomials of degree ω, with even up to ω points $(i, f(i), g(i))$ the polynomial f, g cannot be reconstructed. Much less is available with only $\{(c, x_c, y_c)\}_{c\in\mathcal{C}}$ for $|\mathcal{C}| \leq \omega$. So colluders $\mathcal{V}_{\mathcal{C}}$ completely have no idea what $f(X), g(X)$ and thus $f(i), g(i)$ are. A successful impersonation of Alice to $\mathcal{V}_i$ require at least a forged $f'(X), g'(X)$ such that $y_i = f'(X)|_{X=i} + x_i \cdot g'(X)|_{X=i}$. Without knowing x_i, the success probability is at most $1/q$. The origin property is also guaranteed.

$(1-\frac{\omega}{q})$-*Hiding:* First, we observe that for an honest Alice, the receiver $\mathcal{V}_c$ knows in 100 percent the secret value $x = x_c$ if $y|_{X=c} = y_c$. This happens with probability $\Pr[x_c = x] = 1/q$ for each $c \in \mathcal{C}$. Thus $\gamma \geq \omega/q$. Repeat the argument for *origin* property, the colluders obtain no information on $f(X)$ and $g(X)$. So $F(X) = f(X) + x \cdot g(X)$ leak no information of x if no $x_c = x$ for $c \in \mathcal{C}$. This proves $\gamma = \omega/q$. □

5 Constructions using other primitives

5.1 Using only an A-code with secrecy

We can also construct unconditionally secure commitment scheme using only an A-code with secrecy (i.e., without using an encryption system). Here we only talk about the two-party commitment case.

An A-code with secrecy [17, 4, 8] is an A-code $(\mathcal{S}, \mathcal{M}, \mathcal{E})$ satisfying that observing a message $m \in \mathcal{M}$ does not help the adversary to determine the source state $s \in \mathcal{S}$ (1-folder secrecy [17]), where $m = e(s)$ is generated using the secret encoding rule $e \in \mathcal{E}$ shared by the sender and the receiver. Obviously, the m cannot be the form of (s, t) as in the Cartesian A-code [16] (without secrecy). The legal receiver can recover the source state as $s = e^{-1}(m)$ and accepts it as authentic if $s \in \mathcal{S}$. Stinson defined a notion of *perfect L-fold secrecy* if for every set M_L of at most L messages observed in the channel, and for every set S_L of at most L source states, we have $H(S_L|M_L) = H(S_L)$. That is observing a set of at most L authentication messages does not help the adversary determine the source states. The security against *spoofing of order* ℓ can also be defined accordingly, we refer the readers to [17] for more details.

Using only an A-code with perfect 2-fold secrecy, a traditional two-party commitment scheme $(\mathcal{S}, \mathcal{M}, \mathcal{E}, \mathcal{E}, \mathcal{M})$ can be described as follows. Note that here the secret keys distributed to Alice (the committer) and Bob (the receiver) is dual to that in the "ENC+A-code" case. This answers affirmatively the open question in [12].

1. *Initialization:* Ted (the trusted initializer) chooses randomly an encoding rule $e \in \mathcal{E}$ and a source state $s_0 \in \mathcal{S}$. He computes the message $m_0 = e(s_0) \in \mathcal{M}$. Then he securely distributes e to Alice and m_0 to Bob.
2. *Commitment:* When Alice wants to commits to a value $s \in \mathcal{S}$, she computes and sends $m = e(s)$ to Bob. For simplicity we assume $s \neq s_0$ and thus $m \neq m_0$.
3. *Decommitment:* Alice sends e to Bob to reveal the value s. Bob accepts the reveal if both $e^{-1}(m)$ and $e^{-1}(m_0)$ belongs to $\mathcal{S}$. And on acceptance, Bob recovers the value $s = e^{-1}(m)$.

Discussion on security: By definition, the perfect 2-fold secrecy of the A-code guarantees that Bob cannot obtain any information on s from his secret key m_0 and the commitment m.

But on the other hand, in order to provide perfect binding property, we require the A-code to have absolutely no secrecy if 3 messages are observed. Let $\mathcal{E}(m) = \{e \in \mathcal{E} : e^{-1}(m) \in \mathcal{S}\}$ and $\mathcal{E}(M_L) = \cap_{m \in M_L} \mathcal{E}(m)$, where $M_L \in \mathcal{M}^L$ denotes the set of L different messages. Then the perfect 2-fold secrecy means $|\mathcal{E}(M_2)| > 1$ for all $M_2 \in \mathcal{M}^2$; while the 3-fold non-secrecy means $|\mathcal{E}(M_3)| \leq 1$ for all $M_3 \in \mathcal{M}^3$.

More generally, the commitment scheme above enables Alice to commit to L values if the underlying A-code is perfect L-fold secret but $(L+1)$-fold non-secret. However, different to the multiple commitments in Section 4.1 where the commitments can be opened one after another, the L commitments in this scheme can only be opened in the end, because open of one commitment implies the open of all the others

5.2 Using verifiable secret sharing

Verifiable secret sharing (VSS) schemes are extensively studied in computational and information theoretic settings, for example [5, 9, 18]. There are a dealer and n holders in a VSS, each holder of a share of the secret can verify that the share is consistent with the other shares. Thus dealer and other participants can be verified in such a scheme. There are two aspects of the security in a VSS. One is the security of the secret and the other is the security of the verification.

More specifically, a VSS consists of two phases, i.e. Share and $\mathsf{Reconstruction}$, and a verification function Verify. In the Share phase, for a secret $s \in \mathcal{S}$, the dealer generates shares $s_i \in \mathcal{V}$ for each holder. Each holder can determine the validity of the share using the function Verify. In the $\mathsf{Reconstruction}$ phase, with $\omega + 1$ shares the holders can recover a secret s'. Then the security of the secret requires that with up to ω valid shares, one cannot obtain any information of the secret; the security of the verification requires that for every $\geq \omega + 1$ valid shares, an unique s' will be recovered. For more formal definition, please refer to [18].

Given an encryption system ENC$= (\mathcal{X}, \mathcal{Y}, \mathcal{S}, \mathsf{Enc}, \mathsf{Dec})$ and an $(\omega, n+\omega+1)$-VSS scheme with the set $\mathcal{S}$ for secrets and set $\mathcal{V}$ for shares, the MRC scheme $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{K}, \mathcal{V}^n)$, where $\mathcal{Z} = \mathcal{K} = \mathcal{V}^{\omega+1}$, is described below:

1. *Initialization:* A trusted initializer (TI) randomly chooses a secret $s \in \mathcal{S}$ and generates $n + \omega + 1$ shares as in the VSS Share phase. He securely distributes $k = (s_1, \cdots, s_{\omega+1})$ to Alice and $v_i = s_{\omega+i}$ to the receiver $\mathcal{R}_i$.
2. *Commitment:* To commit a value $x \in \mathcal{X}$, Alice reconstructs $s = \mathsf{Reconstruction}(k)$ and calculates $y = \mathsf{Enc}(s, x)$ (i.e., $\mathsf{Com}(k, x) = \mathsf{Enc}(s, x)$). She multicasts it to the receivers $\mathcal{R}$.
3. *Decommitment:* To reveal the value x, Alice multicasts $z = \mathsf{Dcm}(k, x) = k = (s_1, \cdots, s_{\omega+1})$ to $\mathcal{R}$. Each $\mathcal{R}_i$ accepts if all s_j $(j = 1, \cdots, \omega+1)$ are valid shares (passing the test Verify). On acceptance, $\mathcal{R}_i$ reconstructs s with any $\omega + 1$ shares and recovers the committed value as $x = \mathsf{Dec}(s, y)$.

Discussion on security: The MRC2 in Section 4.2 can be viewed as an implementation of the above construction. The VSS is a *probabilistic variant* of Shamir secret sharing [15]. That is the share for $\mathcal{R}_i$ is generated by randomly choosing an x_i and then computing $y_i = f(x_i)$, while in the conventional case $x_i = i$ is fixed and known to all the participants. The Verify

function is evaluated on $s_{\omega+i}$ and the $\omega + 1$ shares (or equally $f(X)$, with which $\mathcal{R}_i$ can generate as many shares as he wants) sent by the committer. In fact $\mathsf{Verify}(s_{\omega+1}, z) = 1$ if and only if all $\mathsf{Reconstruction}(S_{\omega+1})$ results in the same s', where $S_{\omega+1}$ denotes a subset of arbitrary $\omega + 1$ elements in $\{s_1, \cdots, s_\omega, s_{\omega+i}\}$. The verification function defined in this way is actually weaker than what required in a VSS. The reason is that the share $s_{\omega+i}$ of $\mathcal{R}_i$ generated by the trusted initializer is always valid.

From the discussion above, two requirements on the VSS is necessary. One is the Share phase must be probabilistic. The other is that given the secret, one (e.g., the committer) can not know the share of an honest receiver with a probability more than $\frac{1}{|\mathcal{V}|-\omega-1}$ or $\frac{1}{|\mathcal{V}|-2\omega-1}$ (colluding with ω dishonest receivers). And with above two properties being satisfied, the Verify function can be constructed easier, e.g., $\mathsf{Verify}(\geq \omega + 1 \text{ shares}) = 1$ if and only if $\mathsf{Reconstruction}((every)\omega + 1 \text{ shares})$ consistent with each other.

6 Conclusive remarks

In this paper, we studied for the first multireceiver commitment in unconditionally secure setting. That is a committer can make commitments to a group of verifiers. Different from in computational setting given the (noninteractive) two party commitment, multireceiver commitment (MRC) is trivial, commitment in information theoretic setting can only exist with a trusted infrastructure. We extended the two-party model of Rivestto multireceiver case and presented generic constructions using respectively multireceiver authentication codes (without secrecy) (MRA-codes) and verifiable secret sharing (VSS) schemes. We presented two concrete implementations of the generic constructions. In the traditional two-party commitment, we affirmatively answered the open question of Pinto, Souto, Matos and Antunes by presenting a genric construction based on only an A-code with secrecy.

However, there is still a lot of work to do. We believe that our work will initiate a couple of new interesting researches and hopefully, more applications off multireceiver commitment schemes will be found in the near future. Particularly, they are interesting problems to study the fundamental relation among the related primitives, such as MRC, MRA-code (with or without secrecy) and VSS, to investigate bounds on keys of committer as well as receivers, and to explore perhaps other extensions (e.g., efficient commitments for dynamic sender). These will be our future work.

References

1. Saurabh Agarwal, Ronald Cramer, and Robbert de Haan. Asymptotically optimal two-round perfectly secure message transmission. In Cynthia Dwork, editor, *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 394–408. Springer, 2006.
2. Manuel Blum. Coin flipping by telephone - a protocol for solving impossible problems. In *COMPCON*, pages 133–137. IEEE Computer Society, 1982.
3. Carlo Blundo, Barbara Masucci, Douglas R. Stinson, and Ruizhong Wei. Constructions and bounds for unconditionally secure non-interactive commitment schemes. *Design Codes and Cryptography*, 26(1-3):97–110, 2002.
4. L. R. A. Casse, Keith M. Martin, and Peter R. Wild. Bounds and characterizations of authentication/secrecy schemes. *Des. Codes Cryptography*, 13(2):107–129, 1998.
5. Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract). In *FOCS*, pages 383–395. IEEE, 1985.

6. Ivan Damgård, Joe Kilian, and Louis Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In *EUROCRYPT*, pages 56–73, 1999.
7. Yvo Desmedt, Yair Frankel, and Moti Yung. Multi-receiver/multi-sender network security: Efficient authenticated multicast/feedback. In *INFOCOM*, pages 2045–2054, 1992.
8. Cunsheng Ding, Arto Salomaa, Patrick Solé, and Xiaojian Tian. Three constructions of authentication/secrecy codes. In Marc P. C. Fossorier, Tom Høholdt, and Alain Poli, editors, *AAECC*, volume 2643 of *Lecture Notes in Computer Science*, pages 24–33. Springer, 2003.
9. Paul Feldman. A practical scheme for non-interactive verifiable secret sharing. In *FOCS*, pages 427–437. IEEE, 1987.
10. Kaoru Kurosawa and Satoshi Obana. Characterisation of (k, n) multi-receiver authentication. In Vijay Varadharajan, Josef Pieprzyk, and Yi Mu, editors, *ACISP*, volume 1270 of *Lecture Notes in Computer Science*, pages 204–215. Springer, 1997.
11. Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Secure commitment against a powerful adversary. In Alain Finkel and Matthias Jantzen, editors, *STACS*, volume 577 of *Lecture Notes in Computer Science*, pages 439–448. Springer, 1992.
12. Alexandre Pinto, André Souto, Armando Matos, and Luís Antunes. Galois field commitment scheme. Cryptology ePrint Archive, Report 2006/410, 2006. `http://eprint.iacr.org/`.
13. Ronald L. Rivest. 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/`.
14. Reihaneh Safavi-Naini and Huaxiong Wang. Multireceiver authentication codes: Models, bounds, constructions, and extensions. *Inf. Comput.*, 151(1-2):148–172, 1999.
15. Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
16. Gustavus J. Simmons. A survey of information authentication. In G. J. Simmons, editor, *Contemporary Cryptology, The Science of Information Integrity*, pages 379–419. IEEE Press, 1992. Preliminary version appeared in Proceedings of the IEEE 76 (1988):603-620.
17. Douglas R. Stinson. A construction for authentication/secrecy codes from certain combinatorial designs. In Carl Pomerance, editor, *CRYPTO*, volume 293 of *Lecture Notes in Computer Science*, pages 355–366. Springer, 1987.
18. Douglas R. Stinson and Ruizhong Wei. Unconditionally secure proactive secret sharing scheme with combinatorial structures. In Howard M. Heys and Carlisle M. Adams, editors, *Selected Areas in Cryptography*, volume 1758 of *Lecture Notes in Computer Science*, pages 200–214. Springer, 1999.