Bounds and Constructions for Multireceiver Authentication Codes

R. Safavi-Naini and H. Wang

School of IT and CS
University of Wollongong, Northfields Ave
Wollongong 2522, Australia
Email: [rei, hw13]@uow.edu.au

Abstract. Multireceiver authentication codes allow one sender to construct an authenticated message for a group of receivers such that each receiver can verify authenticity of the received message. In this paper, we give a formal definition of multireceiver authentication codes, derive information theoretic and combinatorial lower bounds on their performance and give new efficient constructions for such codes, our constructions are based on the linear error-correcting codes.

Multireceiver authentication codes (MRA-codes) [4] extend Simmons' model of unconditionally secure authentication [16]. In an MRA-code [4], a sender wants to authenticate a message for a group of receivers such that each receiver can verify authenticity of the received message. Receivers are not trusted and may try to construct fraudulent messages on behalf of the transmitter. If the fraudulent message is acceptable by even one receiver the attackers have succeeded. This is a useful extension of traditional authentication code and has numerous applications. For example a director wanting to give instructions to employees in an organisation such that each employee is able to verify authenticity of the message. Providing such service using digital signature implies that security relies on unproven assumptions and the attackers have finite amount of computational resources. In unconditionally secure model, there is no computational assumptions or limitations on the attackers' resources.

A multireceiver A-code can be trivially constructed using traditional A-codes: the sender shares a common key with each receiver; to send an authenticated message it constructs n codewords, one for each receiver, concatenates them and broadcasts the result. Now each receiver can verify its own codeword and so authenticate the message. In this construction collaboration of even $n - 1$ receivers does not help them in constructing a message that is acceptable by the n^{th} receiver simply because the n codewords are independently constructed. If we assume that the size of the malicious groups cannot be too large, for example the biggest number of collaborators is $w - 1$ (where $w < n$), then we can expect to save on the size of the key and the length of the codeword because codewords can have dependencies. This is the basis of attempting to construct codes that are more efficient than the trivial one. The first two constructions of

(w, n) MRA-codes, given in [4], are based on polynomials over finite fields and finite geometries. DFY description of MRA-codes is basically a definition of its functionality: that is the way the code works. Kurosawa and Obana (KO) [10] studied (w, n) MRA-code, derived combinatorial lower bounds on the probability of success in impersonation and substitution attacks, and characterised Cartesian MRA-codes that satisfy the bound with equality.

In this paper we start by giving a more general definition of MRA-codes which is a natural generalisation of KO's definition. Next we derive the first information theoretic bounds on the probability of success in impersonation and substitution attacks. The bounds are used to obtain combinatorial bounds on the the number of keys of the transmitter and receivers and also the size of the tag. These latter bounds are generalisations of KO bounds to MRA-systems that are not perfect. Finally, we present two new constructions for MRA-codes using linear error-correcting codes (E-codes). The constructions are particularly important because they give MRA-codes from arbitrary E-codes and can be seen as extension of Johansson et al [9] work relating E-codes and A-codes. This established link allows us to apply bounds and constructions from the well-developed discipline of E-codes to the construction of new MRA-systems. Using maximum distance separable codes in the first construction, and special values for parameters in the second, results in new optimal MRA-codes that satisfy lower bounds on the size of keys and the tag. Besides DFY's original polynomial construction, these are the only other known optimal constructions for MRA-codes.

The paper is organised as follows. Section 1 provides basic definitions and reviews known results. In section 2 we define MRA-codes and derive information theoretic and combinatorial bounds. In section 3 we first recall DFY polynomial construction and then propose two efficient constructions from linear error-correcting codes. Finally in Section 4 we summarise our results.

1 Preliminaries

In Simmons' model of unconditionally secure authentication there are three participants: a *transmitter* (*sender*), a *receiver*, and an *opponent*. The transmitter and the receiver share a *secret key* and are both assumed honest. The message is sent over a public channel which is subject to active attack. Transmitter and receiver use an *authentication code* which is a set of authentication functions f , indexed by a *key* belonging to a set E . To authenticate a message called a *source state* and denoted by $s \in S$, using a key e , transmitter forms a codeword $f(e, s)$ and sends it to the receiver who can verify its authenticity using his knowledge of the key.

Definition 1. An authentication code C is a 4-tuple (S, M, E, f) , where f is a mapping from $S \times E$ to M ,

$$f : S \times E \longrightarrow M$$

such that $f(s, e) = m$ and $f(s', e) = m$ imply $s = s'$.

In a *systematic Cartesian A-code* the codeword corresponding to a source state s using $e \in E$ is the concatenation of s and an authentication tag $t \in \mathcal{T}$, that is $m = (s, t)$. The receiver will detect a fraudulent codeword (s, t) if the tag that it calculates for s using its secret key e is different from the received tag t .

The opponent can perform an *impersonation*, or a *substitution*, attack by constructing a fraudulent codeword and succeeds if the codeword is acceptable by the receiver. In impersonation the attacker has not seen any previous communication while in substitution he has seen one transmitted codeword. A code provides *perfect protection* against impersonation if enemy's best strategy is randomly guessing a codeword. In the case of Cartesian A-codes, enemy's probability of success is $P_I = \frac{1}{|\mathcal{T}|}$. Perfect protection for substitution is defined in a similar way, it requires the enemy's best strategy to be randomly selecting one of the remainder codewords. For Cartesian A-codes the probability of success of the intruder must be $P_S = \frac{1}{|\mathcal{T}|}$.

An extension of this model, proposed by Desmedt, Frankel and Yung (DFY) [4], is when there are multiple receivers. The system works as follows. First the key distribution centre (KDC) distributes secret keys to the transmitter and each receiver. Next the transmitter broadcasts a message to all the receivers who can individually verify authenticity of the message using their secret key information. There are malicious groups of receivers who use their secret keys and all the previous communications in the system to construct fraudulent messages. They succeed in their attack even if a single receiver accepts the message as being authentic.

KO formalisation of (w, n) MRA-codes is as follows. Let $E_1, E_2, \dots, E_n$ denote the set of decoding rules of receivers $R_1, \dots, R_n$, and S and M denote the set of source states and senders codewords, respectively.

Definition 2. ([10]) We say that $(S, M, E_1, \dots, E_n)$ is a (w, n) multireceiver A-code if for $\forall (E_{i_1}, \dots, E_{i_w})$ and $\forall (e_1, \dots, e_w)$,

$$P(E_{i_w} = e_w | E_{i_1} = e_1, \dots, E_{i_{w-1}} = e_{w-1}) = P(E_{i_w} = e_w).$$

The probabilities of impersonation and substitution attacks, P_I and P_S , for (w, n) MRA-code are then defined as the best chance of success in impersonation and substitution attacks, respectively, against a single (arbitrary) receiver.

With these definitions, they derived the following bounds. Assume $q = |M|/|S|$.

Theorem 3. (Theorem 9 [10]) In a (w, n) MRA-code, $P_I \geq 1/\sqrt[w]{q}$. The equality holds if and only if $P(R_{i_1}, \dots, R_{i_w} \text{ accept } m) = 1/q$ and $P(R_j \text{ accepts } m) = 1/\sqrt[w]{q}$ for any m and any R_j .

Theorem 4. (Theorem 10 [10]) In a (w, n) MRA-code without secrecy, if $P_I = 1/\sqrt[w]{q}$, then $P_S \geq 1/\sqrt[w]{q}$. The equality holds if and only if

$$P(R_{i_1}, \dots, R_{i_k} \text{ accepts } m' | R_{i_1}, \dots, R_{i_k} \text{ accepts } m) = 1/q$$

$$P(R_j \text{ accepts } m' | R_j \text{ accepts } m) = 1/\sqrt[w]{q}$$

for $\forall R_j, \forall m$ and $\forall m'$ such that the source state of m is different from that of m' .

Theorem 5. (Theorem 11 [10]) *In a (w, n) MRA-code without secrecy, if $P_I = P_S = 1/\sqrt[w]{q}$, then $|E_j| \geq (\sqrt[w]{q})^2$ for $\forall j$. If the equality holds, then each rule of E_j is used with equal probability.*

KO characterised Cartesian MRA-codes that satisfy $P_I = P_S = 1/\sqrt[w]{q}$ and observed that DFY polynomial construction is in fact an optimal construction and has the least number of keys for the transmitter and the receivers and requires the smallest tag size for the authenticator.

Definition 2 only requires that the set of keys for any set of w receivers be independent. This property ensures that the probability of success in impersonation attack by any $w - 1$ receivers against a single other receiver is the same as that by an (outside) opponent. However, it does not imply a similar property for substitution, as will be shown in Example 1. (Contrary to KO's claim in page 207 [10].) We give a more general definition for MRA-codes that has KO's definition as a special case, and derive information theoretic combinatorial lower bounds on P_I and P_S for such codes. These are the first information theoretic bounds for MRA-codes.

2 Model and Bounds

An MRA-System has three phases:

1. **Key distribution:** The KDC (key distribution centre) privately transmits the key information to the sender and each receiver(the sender can also be the KDC).
2. **Broadcast:** For a source state, the sender generates the authenticated message using his/her key and broadcasts the authenticated message.
3. **Verification:** Each user can verify the authenticity of the broadcast message.

Denote by $X_1 \times \cdots \times X_n$ the direct product of sets $X_1, \dots, X_n$, and by p_i the projection mapping of $X_1 \times \cdots \times X_n$ on X_i (i.e., $p_i : X_1 \times \cdots \times X_n \longrightarrow X_i$ defined by $p_i(x_1, x_2, \dots, x_n) = x_i$). Let $g_1 : X_1 \longrightarrow Y_1$ and $g_2 : X_2 \longrightarrow Y_2$ be two mappings; we denote the direct product of g_1 and g_2 by $g_1 \times g_2$ (i.e., $g_1 \times g_2 : X_1 \times X_2 \longrightarrow Y_1 \times Y_2$ defined by $g_1 \times g_2(x_1, x_2) = (g_1(x_1), g_2(x_2))$). The identity mapping on a set X is denoted by 1_X .

Definition 6. Let $C = (S, M, E, f)$ and $C_i = (S, M_i, E_i, f_i)$, $i = 1, 2, \dots, n$ be authentication codes. We call $(C; C_1, C_2, \dots, C_n)$ a multireceiver authentication code (MRA-code) if there exist two mappings $\tau : E \longrightarrow E_1 \times \cdots \times E_n$ and $\pi : M \longrightarrow M_1 \times \cdots \times M_n$ such that for any $(s, e) \in S \times E$ and any $1 \leq i \leq n$, the following identity holds

$$p_i(\pi f(s, e)) = f_i((1_S \times p_i \tau)(s, e)).$$

Let $\tau_i = p_i \tau$ and $\pi_i = p_i \pi$. Then we have for each $(s, e) \in S \times E$

$$\pi_i f(s, e) = f_i(1_S \times \tau_i)(s, e).$$

We assume that for each i the mappings $\tau_i : E \rightarrow E_i$ and $\pi_i : M \rightarrow M_i$ are surjective. We also assume that for each code C_i the probability distribution on the source states is the same with that in the A-code C , and the probability distribution on E_i is derived from that of E and the mapping τ_i .

Let T denote the sender and $R_1, \dots, R_n$ denote the receivers. In order to authenticate a message, the sender and the receivers follow the following protocol.

1. The KDC (or the sender) randomly chooses a key $e \in E$ and privately transmits e to T and $e_i = \pi_i(e)$ to the receiver R_i for all $1 \leq i \leq n$.
2. If T wants to send a source state $s \in S$ to all the receivers, T computes $m = f(s, e) \in M$ and broadcasts it to all receivers.
3. Receiver R_i checks whether a source state s such that $f_i(s, e_i) = \pi_i(m)$ exists. If such an s exists, the message m is accepted as authentic. Otherwise m is rejected.

We adopt the Kerckhoff principle that everything in the system except the actual keys of the sender and receivers is public. This includes the probability distribution of the source states and the sender's keys. From Definition 6 we know that the probability distribution of the sender's key induces a probability distribution on each receiver's key.

Attackers could be *outsiders* who do not have access to any key information, or *insiders* who have some key information. We only need to consider the latter group as it is at least as powerful as the former. We consider the systems that protect against the coalition of groups of up to a maximum size of receivers, and study impersonation and substitution attacks.

Assume there are n receivers $R_1, \dots, R_n$. Let $L = \{i_1, \dots, i_\ell\} \subseteq \{1, \dots, n\}$, $E_L = E_{i_1} \times \dots \times E_{i_\ell}$ and $R_L = \{R_{i_1}, \dots, R_{i_\ell}\}$. We consider the attack from R_L on a receiver R_i , where $i \notin L$.

Impersonation attack: R_L , after receiving their secret keys, send a message m to R_i . R_L is successful if m is accepted by R_i as authentic. We denote by $P_I[i, L]$ the success probability of R_L in performing an impersonation attack on R_i . This can be expressed as

$$P_I[i, L] = \max_{m \in M} P(m \text{ is accepted by } R_i \mid e_L)$$

where $e_L \in E_L$.

Substitution attack: R_L , after observing a message m that is transmitted by the sender, replace m with another message m' . R_L is successful if m' is accepted by R_i as authentic. We denote by $P_S[i, L]$, the success probability of R_L in performing a substitution attack on R_i . We have,

$$P_S[i, L] = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} P(R_i \text{ accepts } m' \mid m, e_L)$$

The following two bounds are generalisation of Simmons' [16] bound and Brickell's bound [2], when attack is from a group of insiders who have access to part of the key information.

Theorem 7. Let $P_I[i, L]$ and $P_S[i, L]$ be defined as above.

1. $P_I[i, L] \geq 2^{-I(M; E_i | E_L)}$.
2. $P_S[i, L] \geq 2^{-I(M'; E_i | M, E_L)}$.

Proof is omitted due to the lack of space, and it can be found in [15].

Corollary 8.

$$P_S[i, L] \geq 2^{-H(E_i | M, E_L)}.$$

Proof. The corollary follows from Theorem 7 by noting that $I(M'; E_i | M, E_L) = H(E_i | M, E_L) - H(E_i | M', M, E_L)$.

A (w, n) MRA-code is an MRA-code in which there are n receivers such that no set of $w - 1$ receivers can construct a fraudulent codeword acceptable by another receiver. We note that in this definition, the only requirement is that the chance of success of the attackers is less than one but it is possible that some coalition of attackers can have a better chance of success than an outsider. A (w, n) MRA-code is *perfect against impersonation* if the chance of success of any group of up to $w - 1$ receivers in an impersonation attack is the same as an outsider. Similarly a (w, n) MRA-code is *perfect against substitution* if the chance of success for any group of up to $w - 1$ receivers in a substitution attack is the same as an outsider.

Let $(C; C_i, \dots, C_n)$ be an MRA-code. Define P_I and P_S as follows.

$$P_I = \max_{L \cup \{i\}} \{P_I[i, L]\}$$

$$P_S = \max_{L \cup \{i\}} \{P_S[i, L]\}$$

where the maximum is taken over all possible w -subsets $L \cup \{i\}$ ($i \notin L$) of $\{1, 2, \dots, n\}$. In other words, P_I and P_S are the best chance of a group of $w - 1$ receivers to succeed in impersonation or substitution attacks against a single receiver, respectively.

Let $P_I[i]$ and $P_S[i]$ denote the success probabilities for an outsider in impersonation and substitution attacks, respectively. Then

$$P_I[i] = \max_{m \in M} P(R_i \text{ accepts } m) = \max_{m \in M} P(\pi_i(m) \text{ is valid in } C_i)$$

$$\begin{aligned} P_S[i] &= \max_{m' \neq m \in M} P(R_i \text{ accepts } m' \mid m \text{ is valid in } C) \\ &= \max_{m' \neq m \in M} P(\pi_i(m') \text{ is valid in } C_i \mid m \text{ is valid in } C) \end{aligned}$$

Thus a (w, n) MRA-code is perfect against impersonation if and only if Condition (a): $P_I[i, L] = P_I[i]$ holds; and it is perfect against substitution if and only if Condition (b): $P_S[i, L] = P_S[i]$ holds.

Lemma 9. *A sufficient condition for a (w, n) MRA-code to be perfect against impersonation is that $P(e_i|e_L) = P(e_i)$ for all w -subsets $L \cup \{i\}$ ($i \notin L$) of $\{1, \dots, n\}$.*

Proof is given in the Appendix I.

It should also be noted that an (w, n) MRA-code which is perfect for impersonation is not necessarily perfect for substitution, as the following example shows.

Example 1. Similar to the DFY polynomial scheme, the sender randomly chooses two polynomials $f(x), g(x)$ of degree at most $w - 1$ and secretly transmits $f(i), g(i)$ to receiver R_i ($i \neq 0$). For a source state $s \in GF(q)$ the sender calculates $h(x) = f(x) + sg(x)$ and broadcasts $(s, g(0), h(x))$. Each receiver R_i can verify the authenticity of the broadcasted message by checking if $h(i) = f(i) + sg(i)$. Now for any group of $w - 1$ receivers $L = \{P_{i_1}, \dots, P_{i_{w-1}}\}$ and $i \notin L$, $P_I[i, L] = 1/q$, since L has not information about the key $(f(i), g(i))$ of R_i . But, $P_S[i, L] = 1$, since, after seeing the broadcasted message, L can calculate $f(0) = h(0) - sg(0)$, so L knows $(f(i_1), g(i_1)), \dots, (f(i_{w-1}), g(i_{w-1}))$ and $(f(0), g(0))$. Thus L can calculate $f(x)$ and $g(x)$, and so $P_S[i, L] = 1$.

We define the *deception probability* of a (w, n) MRA-system as $P_D = \max\{P_I, P_S\}$.

Theorem 10. *Let $(C; C_1, \dots, C_n)$ be a (w, n) MRA-code. Assume that $P_D \leq 1/q$ and suppose there is a uniform probability distribution on the source states S . Then*

- (i) $|E_i| \geq q^2$, for each $i \in \{1, \dots, n\}$.
- (ii) $|E| \geq q^{2w}$.
- (iii) $|M| \geq q^w |S|$.

The bounds are tight and there exists a system that satisfies the bounds with equality.

Proof is given in the Appendix I

Comparison of the bounds with KO's bounds: Theorem 10 gives combinatorial bounds for general (w, n) MRA-codes on the size of the transmitter and receivers' key when probability of deception is known. It also lower bounds the required redundancy in terms of the deception probabilities. KO's bounds only apply to (w, n) MRA-codes that are perfect against impersonation and can be seen as special cases of the combinatorial bounds derived above. Appendix II we give a more detailed comparison of the two sets of bounds.

3 Constructions

DFY [4] gave two constructions for MRA-codes: one based on polynomials and the other based on finite geometries. KO showed that the polynomial construction is optimal and has the minimum number of keys for transmitter and receivers (Theorem 9 and 11 in [10] and produces the shortest length tag for the

codewords. No other optimal construction is known so far. In this section we use error correcting codes (E-codes) to construct MRA-codes. First, we present two constructions which can be used to derive an MRA-code from an *arbitrary* E-code and then show that the constructions result in new optimal MRA-codes. An linear $[n, k]$ code C over $GF(q)$ is a linear subspace of $GF(q)^n$ with dimension k . The *minimum distance* d_C of C is defined by $d_C = \min_{0 \neq \mathbf{u} \in C} w(\mathbf{u})$, where $w(\mathbf{u})$ is the number of nonzero coordinates of $\mathbf{u}$. A $k \times n$ matrix G over $GF(q)$ is called a *generator matrix* of C if its row vectors generate the linear subspace C . For a linear code C its dual code, denoted by $C^\perp$, is defined by

$$C^\perp = \{\mathbf{u} \in GF(q)^n; \mathbf{u}\mathbf{v}^T = 0 \text{ for all } \mathbf{v} \in C\}.$$

We briefly recall DFY's polynomial construction as it makes it easier to describe Construction I.

DFY polynomial construction: Assume there is a sender T , and n receivers $R_1, \dots, R_n$. The key for T consists of two random polynomials $P_0(x)$ and $P_1(x)$, of degree at most $w - 1$, with coefficients in $GF(q)$. The key for R_i consists of $P_0(i)$ and $P_1(i)$. For a source state $s \in GF(q)$, T broadcasts $(s, A(x))$ where $A(x) = P_0(x) + sP_1(x)$. R_i accepts $(s, A(x))$ as authentic if $A(i) = P_0(i) + sP_1(i)$. It is proved in [4] that no group of $w - 1$ receivers can perform an impersonation or substitution attacks against a single receiver, with a probability greater than $1/q$, the construction provides the following parameters $P_I = P_S = 1/q$, $|E_i| = q^2$, for all $1 \leq i \leq n$, $|E| = q^{2w}$ and $|M| = q^w |S|$.

3.1 Construction I

Let C be a linear $[n, k]$ code over $GF(q)$ with a generator matrix $G \in GF(q)^{k \times n}$. We construct an MRA-code with n receivers from C in the following way. Assume that $S = GF(q)$ is the set of source states and G is publicly known.

1. *Key distribution* T randomly chooses $(\alpha, \beta) \in GF(q)^k \times GF(q)^k$, where $\alpha, \beta \in GF(q)$. T then calculates the codewords $\alpha G = \mathbf{u} = (u_1, \dots, u_n)$ and $\beta G = \mathbf{v} = (v_1, \dots, v_n)$, and privately transmits (u_i, v_i) to the receiver R_i for each $1 \leq i \leq n$, which consists of the secret key of R_i .
2. *Broadcast* To authenticate a message $s \in S$, the sender T computes $\gamma = \alpha + s\beta$ and broadcasts (s, γ) to all the receivers.
3. *Verification* For each i , R_i accepts (s, γ) as authentic if $y_i = u_i + sv_i$, where $\mathbf{y} = (y_1, \dots, y_n) = \gamma G$.

Lemma 11. *In the above construction, let the probability distribution on the source and sender's key space be uniform. Let $L = \{i_1, \dots, i_\ell\} \subseteq \{1, \dots, n\}$ and $i \notin L$. Then $P_I[i, L] = P_S[i, L] = \frac{1}{q}$ if and only if there exists a codeword $\mathbf{c} = (c_1, \dots, c_n) \in C$ such that $c_{i_1} = \dots = c_{i_\ell} = 0$ and $c_i = 1$.*

Proof. (Sketch)

Sufficiency: Assume that there exists a codeword $\mathbf{c} \in C$ satisfying the required property of the theorem. Let $\mathbf{u} = \alpha G, \mathbf{v} = \beta G$, where (α, β) is the key chosen

by the sender T . Because of the linearity of the E-code, we know that for any $t, t' \in GF(q)$ we have $\mathbf{u} + t\mathbf{c}, \mathbf{v} + t'\mathbf{c} \in C$. Since R_L have the key information $((u_{i_1}, \dots, u_{i_\ell}), (v_{i_1}, \dots, v_{i_\ell}))$, then for all $t, t' \in GF(q)$ $(u_{i_1}, \dots, u_{i_\ell}, u_i + t)$, and $(v_{i_1}, \dots, v_{i_\ell}, v_i + t')$ produce all possible keys of $R_{L \cup \{i\}}$. It follows that R_L have no information about R'_i 's key, and hence $P_I[i, L] = P_S[i, L] = \frac{1}{q}$.

Necessity: Assume that there is no codeword $\mathbf{c}$ in C satisfying the required property of the theorem. We prove that $(u_{i_1}, \dots, u_{i_\ell})$ and $(v_{i_1}, \dots, v_{i_\ell})$ uniquely determine u_i and v_i . Clearly, there exist u_i and v_i such that $(u_{i_1}, \dots, u_{i_\ell}, u_i)$ and $(v_{i_1}, \dots, v_{i_\ell}, v_i)$ are subcodewords of C . We only need to show that such u_i and v_i are unique. Indeed, if there exist two subcodewords $(u_{i_1}, \dots, u_{i_\ell}, u_i)$, $(u_{i_1}, \dots, u_{i_\ell}, u'_i)$ in C , it follows that $(u_{i_1}, \dots, u_{i_\ell}, u_i) - (u_{i_1}, \dots, u_{i_\ell}, u'_i) = (0, \dots, 0, u_i - u'_i)$ is also a subcodeword in C , and so is $(0, \dots, 0, 1)$, which is a contradiction. In this case we have $P_I[i, L] = P_S[i, L] = 1$, proving the necessity.

Theorem 12. *Let C be a linear $[n, k]$ code over $GF(q)$ and let d' be the minimum distance of $C^\perp$, the dual code of C . Then Construction I results in a (w, n) MRA-code with $P_I = P_S = 1/q$, $w = d' - 1 \leq k$, and the following parameters:*

$$|S| = q, \quad |M| = q^k |S|, \quad |E| = q^{2k} \text{ and } |E_i| = q^2.$$

Proof. We show that the resulting MRA-code is a $(d' - 1, n)$ MRA-code, but not a (d', n) MRA-code. Let G be a generator matrix of C , and let d' be the minimum distance of $C^\perp$. Recall [11] that $C^\perp$ has the minimum distance d' if and only if every $d' - 1$ columns of G are linearly independent and some d' columns of G are linearly dependent. For each $d' - 1$ columns, indexed by $\{i_1, \dots, i_{d'-2}, i\}$, the restriction of G to these $d' - 1$ columns results in a $k \times (d' - 1)$ matrix $G_{\{i_1, \dots, i_{d'-2}, i\}}$. It follows that $e_i \in GF(q)^{d'-1}$ can be expressed as a linear combination of the k rows of $G_{\{i_1, \dots, i_{d'-2}, i\}}$, where $e_i \in GF(q)^{d'-1}$ is the vector with the i th entry being 1 and other entries being 0. This implies that there exists a codeword $\mathbf{c} = (c_1, \dots, c_n) \in C$ such that $c_{i_1} = \dots = c_{i_{d'-2}} = 0$ and $c_i = 1$. Thus, by Lemma 11 we have $P_I[i, L] = P_S[i, L] = 1/q$ for any $d' - 1$ subset $\{i\} \cup L$ of $\{1, \dots, n\}$ with $i \notin L$, and so the resulted MRA-code is a $(d' - 1, n)$ MRA-code with $P_I = P_S = 1/q$. In a similar manner, we can prove that there exists a d' -subset $L \cup \{i\}$ of $\{1, \dots, n\}$ such that $P_I[i, L] = P_S[i, L] = 1$, so it is not a (d', n) MRA-code.

In general the MRA-code derived from an E-code is not optimal and does not satisfy bounds in Theorem 10. In the following we will show that for a well-known class of E-codes the construction results in optimal MRA-codes.

A *maximum distance separable (MDS)* E-code has maximum possible minimum distance and its parameters satisfy $d_C = n - k + 1$. We are only interested in linear MDS codes. An important property of MDS codes is given in the following theorem.

Theorem 13. *(Theorem 2 page 318 in [11]) If C is MDS so is the dual $C^\perp$.*

This means that for an MDS code $d' = n - (n - k) + 1 = k$, or $k = d' - 1$. That is the resulting (w, n) MRA-code can protect against the largest size set of cheaters. Using this result and theorem 12 it is straightforward to prove the following.

Corollary 14. *If the linear code C in Construction I is an $[n, k]$ MDS code over $GF(q)$, then Construction I results in an optimal (k, n) MRA-code with $P_I = P_S = 1/q$. It has the following parameters*

$$|S| = q, \quad |M| = q^k |S|, \quad |E| = q^{2k} \text{ and } |E_i| = q^2.$$

A special class of MDS codes are *Reed-Solomon code* with the following generator matrix,

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{w-1} & x_2^{w-1} & \cdots & x_n^{w-1} \end{bmatrix},$$

where the x_i are n distinct elements in $GF(q)$.

Corollary 15. *If the linear code C in Construction I is an $[n, k]$ Reed-Solomon code, then Construction I coincides with DFY's construction.*

3.2 Construction II

Construction I can be seen as a generalisation of DFY's construction. Construction II is based on the properties of the dual code and can be used for large size sources which makes it of practical interest. We first describe the construction and then discuss its properties.

The basic idea is to use vectors of dual code for verification process. The sender's secret key is an $\ell \times w$ matrix U which defines the generator matrix $G = [I_\ell \mid U]$ of a linear code. To authenticate a source state $\mathbf{s} \in \mathcal{S}$ the sender generates the codeword $c = \mathbf{s}G$ and broadcasts it to the receivers. Each receiver R_i has a codeword d_i of the dual code. To verify authenticity of a broadcasted vector x , receiver R_i calculates $x \cdot d_i$ ($\cdot$ denotes vector inner product) and if it is zero, it accepts the codeword as authentic.

Let $S \subseteq GF(q)^\ell$ denote the set of source states obtained by defining an equivalence relation $\sim$ over $GF(q)^\ell \setminus \{0\}$ as follows: $\mathbf{s} \sim \mathbf{s}' \iff \mathbf{s} = r\mathbf{s}'$ for some $0 \neq r \in GF(q)$. It is easy to verify that this relation is in fact an equivalence relation. We define $\mathcal{S}$ as the set of equivalence classes obtained from $\sim$. It follows that $|S| = \frac{q^\ell - 1}{q - 1} = q^{\ell-1} + \cdots + q + 1$.

The three phases of Construction II are as follows.

1. *Key distribution* The sender T randomly chooses an $\ell \times w$ matrix $G \in GF(q)^{\ell \times w}$ (and so $[I_\ell \mid U]$ is the generator matrix of a linear $[\ell + w, \ell]$ code

in its systematic form). Assume that $q \geq n$ (this assumption is not necessary¹). T chooses n distinct elements $x_1, \dots, x_n \in GF(q)$ (these elements are public and are used as the identities of the receivers), and then calculates and secretly transmits $U(1, x_i, \dots, x_i^{w-1})^T = \alpha_i \in GF(q)^{\ell \times 1}$ to R_i , which consists of the secret key of $R_i, i = 1, \dots, n$.

2. *Broadcast* To authenticate a source state $\mathbf{s} = (s_1, \dots, s_\ell) \in \mathcal{S}$, T computes $\mathbf{s}U = \mathbf{t} = (t_1, \dots, t_w) \in GF(q)^w$ and broadcasts $(\mathbf{s}, \mathbf{t})$.
3. *Verification* For each i , R_i accepts $(\mathbf{s}, \mathbf{t})$ as authentic if $\mathbf{s}\alpha_i = \mathbf{t}(1, x_i, \dots, x_i^{w-1})^T$.

Theorem 16. *Construction II results in a (w, n) multireceiver A-code with $P_I = P_S = 1/q$. It has the following parameters*

$$|S| = \frac{q^\ell - 1}{q - 1}, \quad |M| = q^w |S|, \quad |E| = q^{\ell w} \quad \text{and} \quad |E_i| = q^\ell.$$

Proof. First, we prove that $P_I = P_S = 1/q$. It is sufficient to show that for each $L \subseteq \{1, \dots, n\}$ with $|L| = w - 1$ and $i \notin L$, $P_I[i, L] = P_S[i, L] = 1/q$. Without loss of generality, assume that $L = \{1, \dots, w - 1\}$ and $i = w$, and that after the key distribution R_L hold their keys

$$U(1, x_1, \dots, x_1^{w-1})^T = \alpha_1, \quad \dots, \quad U(1, x_{w-1}, \dots, x_{w-1}^{w-1})^T = \alpha_{w-1}.$$

Let

$\mathcal{F} = \{U \in GF(q)^{\ell \times w}; U(1, x_1, \dots, x_1^{w-1})^T = \alpha_1, \dots, U(1, x_{w-1}, \dots, x_{w-1}^{w-1})^T = \alpha_{w-1}\}$. That is, $\mathcal{F}$ is the set of possible authentication keys of the sender T in accordance with the keys of R_L . We define a mapping $\phi: \mathcal{F} \rightarrow GF(q)^{\ell \times 1}$ by

$$\phi(U) = U(1, x_w, \dots, x_w^{w-1})^T, \quad \forall U \in \mathcal{F}.$$

It is straightforward to verify that ϕ is one-to-one from $\mathcal{F}$ onto $GF(q)^{\ell \times 1}$. This also implies that R'_w 's key $U(1, x_w, \dots, x_w^{w-1})^T = \phi(U)$ is independent of the keys of R_L .

In the impersonation attack, R_L generates a codeword $(\mathbf{s}, \mathbf{t}), \mathbf{s} \in \mathcal{S}$ and $\mathbf{t} \in \mathcal{T} = GF(q)^w$, and hope that it will be accepted by R_w as authentic. It follows

$$\begin{aligned} P_I[w, L] &= \max_{(\mathbf{s}, \mathbf{t}) \in \mathcal{S} \times \mathcal{T}} \frac{|\{U; U \in \mathcal{F} \text{ and } \mathbf{s}U(1, x_w, \dots, x_w^{w-1})^T = \mathbf{t}(1, x_w, \dots, x_w^{w-1})^T\}|}{|\mathcal{F}|} \\ &= \frac{q^{\ell-1}}{q^\ell} \\ &= \frac{1}{q}. \end{aligned}$$

In the substitution attack, R_L , after seeing a broadcast authenticated codeword $(\mathbf{s}, \mathbf{t})$, generates a new codeword $(\mathbf{s}', \mathbf{t}'), \mathbf{s}' \neq \mathbf{s}$, and hope that $(\mathbf{s}', \mathbf{t}')$ will be accepted by R_w as authentic. It follows that

$$\begin{aligned} &P_S[w, L] \\ &= \max_{\mathbf{s}' \neq \mathbf{s}} \frac{|\{U; U \in \mathcal{F}, \mathbf{s}U(1, \dots, x_w^{w-1})^T = \mathbf{t}(1, \dots, x_w^{w-1})^T, \mathbf{s}'U(1, \dots, x_w^{w-1})^T = \mathbf{t}'(1, \dots, x_w^{w-1})^T\}|}{|\{U; U \in \mathcal{F}, \mathbf{s}U(1, x_w, \dots, x_w^{w-1})^T = \mathbf{t}(1, x_w, \dots, x_w^{w-1})^T\}|} \\ &= \frac{q^{\ell-2}}{q^{\ell-1}} \\ &= \frac{1}{q}. \end{aligned}$$

¹ Instead, the sender may choose a $w \times n$ matrix $M = (M_1, \dots, M_n)$ over $GF(q)$ such that any w columns of M are linearly independent and the secret key of R_i is $\begin{pmatrix} -U \\ I \end{pmatrix} M_i$

Similarly, we have $P_I[i, L] = P_S[i, L] = 1/q$ for any w subset $\{i\} \cup L$ of $\{1, \dots, n\}$ with $i \notin L$. Thus we have proved that $P_I = P_S = 1/q$. The proof of the cardinality parameters are obvious.

Corollary 17. *Let $q \geq n$ be a prime power. There exists a (w, n) multireceiver A-code with the following parameters*

$$|\mathcal{S}| = q + 1, \quad |M| = q^w |\mathcal{S}|, \quad |E| = q^{2w}, \quad \text{and} \quad |E_i| = q^2,$$

and the probability of success in each attack is $P_I = \frac{1}{q}$ and $P_S = \frac{1}{q}$.

The corollary follows from the theorem when $\ell = 2$. the resulting MRA-code meets the bounds of Theorem 10 and hence is optimal.

It is interesting to note that for $w = n = 1$, the above construction results in a conventional (one-sender to one-receiver) A-code with the following parameters

$$|\mathcal{S}| = \frac{q^\ell - 1}{q - 1}, \quad |M| = q|\mathcal{S}|, \quad |E| = |E_1| = q^\ell,$$

and the probability of success in impersonation and substitution is given by $P_I = \frac{1}{q}$ and $P_S = \frac{1}{q}$, respectively. Conventional A-code with these parameters has been constructed from finite geometries [1]. In particular, for $\ell = 2$, The A-code has the same parameters as the A-code due to Gilbert, MacWilliams and Sloane [7].

We note that Construction II is more suitable for MRA-codes with large source space. In the DFY construction and Construction I, the order of the field $GF(q)$ determines the lower bound on the success probabilities in impersonation and substitution, and at the same time bounds the size of the source that can be used in the system ($|\mathcal{S}| \leq q$). This can result in inefficient constructions for larger sources. For example a source of size 2^{100} results in probability of deception lower bounded by 2^{-100} which is unnecessarily low. The price paid for this low probability is bigger key sizes which for practical applications is not acceptable. This restriction is removed in Construction II, and by choosing appropriate ℓ the size of source can be increased to the required level.

4 Conclusions

MRA-codes are an important cryptographic primitive in secure group communication. In this paper, we gave a formal definition of MRA-codes and derived the first information theoretic bounds on their performance. The bounds result in combinatorial lower bounds which are generalisations of the previously known combinatorial bounds. We established a link between E-codes and MRA-codes by giving two constructions that can be used to derive MRA-codes from E-codes. The constructions are used to give new optimal MRA-codes.

References

1. A. Beutelspacher, Perfect and essentially perfect authentication systems, *Lecture Notes in Computer Science* **304**(1988), 167-170. (Advances in Cryptology–Eurocrypt ’87).
2. E. F. Brickell, A few results in message authentication, *Congressus Numerantium*, Vol.43(1984), 141-154.
3. T. Cover and J. Thomas, Elements of Information Theory, *New York; Wiley*, 1991.
4. Y. Desmedt, Y. Frankel and M. Yung, Multi-receiver/Multi-sender network security: efficient authenticated multicast/feedback, *IEEE Infocom’92*, (1992) 2045-2054.
5. A. Fiat and M. Naor, Broadcast Encryption. In “Advances in Cryptology – Crypto ’93”, *Lecture Notes in Computer Science* **773** (1994), 480-491.
6. H. Fujii, W. Kachen and K. Kurosawa, Combinatorial bounds and design of broadcast authentication, *IEICE Trans.*, Vol**E79**-A, No. 4(1996)502-506.
7. E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, Codes which detect deception, *The Bell System Technical Journal*, Vol.33, No.3, 405-424(1974).
8. T. Johansson, Lower Bounds on the Probability of Deception in Authentication with Arbitration, *IEEE Trans. on Information Theory*, Vol.40, No.5, (1994) 1573-1585.
9. T. Johansson, G. Kabatianskii and B. Smeets, On the relation between A-codes and codes correcting independent errors. In “Advances in Cryptology – Eurocrypt ’93”, *Lecture Notes in Computer Science* **765** (1993), 1-11.
10. K. Kurosawa and S. Obana, Characterisation of (k, n) multi-receiver authentication, *Information Security and Privacy, ACISP’97*, Lecture Notes in Comput. Sci. **1270**, (1997) 204-215.
11. F. J. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*, New-York; NorthHolland, 1977.
12. J. L. Massey, Cryptography - a selective survey, *Digital Communications*, North Holland(pub) (1986)3-21.
13. D. Pei, Information-Theoretic Bounds for Authentication Codes and Block Designs, *J. of Cryptology*, 8(1995)177-188.
14. R. Safavi-Naini and H. Wang, New results on multi-receiver authentication codes, *Advances in Cryptology – Eurocrypt ’98*, Lecture Notes in Comp. Sci., 1403(1998), 527-541.
15. R. Safavi-Naini and H. Wang, Multireceiver Authentication Codes: Model, Bounds, Constructions and Extensions, *Information and Computation*, to appear.
16. G. J. Simmons, Authentication theory/coding theory, Lecture Notes in Comput. Sci., **196** 411-431. (Crypto ’84).
17. G. J. Simmons, A survey of information authentication, in *Contemporary Cryptology, The Science of Information Integrity*, G.J. Simmons, ed., IEEE Press, (1992), 379-419.
18. B. Smeets, Bounds on the Probability of Deception in Multiple Authentication, *IEEE Trans. of Information Theory*, Vol.40, No.5, (1994)1586-1591.
19. D. R. Stinson, The combinatorics of authentication and secrecy codes, *J. Cryptology* **2**, (1990), 23-390.
20. D. R. Stinson, Universal Hashing and authentication codes, *Designs, Codes and Cryptography* **4** (1994), 369-280.
21. D. R. Stinson, On some methods for unconditionally secure key distribution and broadcast encryption. *Designs, Codes and Cryptography*, **12**(1997), 215-243.
22. M. N. Wegman and J. L. Carter, New hash functions and their use in authentication and set equality, *J. of Computer and System Science* **22**(1981), 265-279.

APPENDIX I

Proof of Lemma 9: Consider the A-code $C_i = (S, M_i, E_i)$, we define an authenticate function $\chi(m_i, e_i)$ on $M_i \times S_i$ as

$$\chi_S(m_i, e_i) = \begin{cases} 1 & \text{if } m_i \text{ is authentic for the key } e_i \\ 0 & \text{otherwise.} \end{cases}$$

We have $P(\pi_i(m) \text{ is valid in } C_i) = \sum_{e_i \in E_i} \chi(\pi_i(m), e_i)P(e_i)$. We define an impersonation characteristic function χ_I on $M \times E_i \times E_L$ by

$$\chi_I(m, e_i, e_L) = \begin{cases} 1 & \text{if } m \text{ is a valid for } e \in E \text{ in } C \\ & \text{such that } \tau_i(e) = e_i \text{ and } \tau_L(e) = e_L \\ 0 & \text{otherwise} \end{cases}$$

From the definition of the impersonation attack we can express $P_I[i, I]$ as

$$\begin{aligned} P_I[i, L] &= \max_{m \in M} P(\pi_i(m) \text{ is valid in } C_i | e_L \in E_L) \\ &= \max_{m \in M} \sum_{e_i \in E_i} \chi_I(m, e_i, e_L) P(e_i | e_L). \end{aligned}$$

It follows that for any given e_L in accordance with $\tau_L(e) = e_L$ and $\tau_i = e_i$, we know $\chi(\pi_i(m), e_i) = \chi_I(m, e_i, e_L)$. Thus we have

$$\begin{aligned} P_I[i, L] &= \max_{m \in M} P(m \text{ is accepted by } R_i | e_L) \\ &= \max_{m \in M} \sum_{e_i \in E_i} \chi_I(m, e_i, e_L) P(e_i | e_L) \\ &= \max_{m \in M} \sum_{e_i \in E_i} \chi(\pi_i(m), e_i) P(e_i | e_L) \\ &= \max_{m \in M} \sum_{e_i \in E_i} \chi(\pi_i(m), e_i) P(e_i) \\ &= P_I[i] \end{aligned}$$

Proof of Theorem 10: (i) For each $(w-1)$ -subset L of $\{1, \dots, n\}$ and any $i \in \{1, \dots, n\}$ where $i \notin L$, by Theorem 7 and Corollary 8 we have

$$\begin{aligned} \left(\frac{1}{q}\right)^2 &\geq P_D^2 \geq P_I[i, L] P_S[i, L] \geq 2^{-(I(M; E_i | E_L) + H(E_i | E_L, M))} = 2^{-H(E_i | E_L)} \\ &\geq 2^{-H(E_i)} \geq 2^{-\log |E_i|} = \frac{1}{|E_i|}. \end{aligned}$$

It follows that $|E_i| \geq q^2$.

(ii) Assume that $L_i = \{1, \dots, i-1, i+1, \dots, w\}, i = 1, \dots, w$. We have,

$$\begin{aligned} \left(\frac{1}{q}\right)^{2w} &\geq \prod_{i=1}^w P_I[i, L_i] P_S[i, L_i] \geq 2^{\sum_{i=1}^w H(E_i | E_{L_i})} \\ &\geq 2^{-\sum_{i=1}^w H(E_i | E_1, \dots, E_{i-1})} = 2^{-H(E_1, \dots, E_w)} \\ &\geq 2^{-H(E)} \geq 2^{-\log |E|} = \frac{1}{|E|}. \end{aligned}$$

Therefore, $|E| \geq q^{2w}$.

(iii) Since $\tau : E \longrightarrow E_1 \times \cdots \times E_n$ induces a mapping from E to $E_1 \times \cdots \times E_w$, we have $I(M; E) \geq I(M; E_1, \dots, E_w)$. It follows that

$$\begin{aligned} 2^{-I(M; E)} &\leq 2^{-I(M; E_1, \dots, E_w)} = 2^{-\sum_{i=1}^w I(M; E_i | E_1, \dots, E_w)} \\ &= 2^{-\sum_{i=1}^w I(M; E_i | E_1, \dots, E_{i-1})} \\ &= \prod_{i=1}^w 2^{-I(M; E_i | E_1, \dots, E_{i-1})} \leq \prod_{i=1}^w P_I[i, Q_i], \end{aligned}$$

where $Q_i = \{1, \dots, i-1\}$. Since for each $1 \leq i \leq w$, we have $P_I[i, Q_i] \leq P_I[i, L_i] \leq \frac{1}{q}$, it follows that,

$$2^{-I(M; E)} = 2^{-(H(M) - H(M|E))} = 2^{-H(M)} 2^{H(M|E)} \leq \left(\frac{1}{q}\right)^w.$$

Since S is assumed to be uniformly distributed, we know that $H(M|E) = H(S) = \log |S|$. Hence $|M| = 2^{\log |M|} \geq 2^{H(M)} \geq q^w |S|$, which proves (iii).

The bounds are tight as in the next sections we will give constructions that meet them with equality.

APPENDIX II

In the following we give we comparison between bounds obtained in Theorem 10 and the bounds derived by Kurosawa and Obana in [10]. Let $\ell = \frac{|M|}{|S|}$.

1. In [10] the first part of Theorem 9 proves that $P_I \geq 1/\sqrt[w]{\ell}$. We show that our Theorem 10 (iii) implies that $P_D = \max\{P_I, P_S\} \geq 1/\sqrt[w]{\ell}$. This is because assuming $P_D = \max\{P_I, P_S\} = 1/q$ and using Theorem 10 (iii), we have $|M| \geq q^w |S| \implies P_D = 1/q \geq \sqrt[w]{|S|/|M|} = 1/\sqrt[w]{\ell}$. This is similar to KO result but uses different assumption: KO result only applies to MRA-codes that are perfect for impersonation while our result is for general MRA-codes.
2. Theorem 10 and 11 in [10] in fact prove the following result(see also the introduction in [10]).

Theorem 18. (*KO [10]*) For (w, n) MRA-code without secrecy, if $P_I = P_S = \frac{1}{\sqrt[w]{\ell}}$, then $|E| \geq \ell^2$ and $|E_i| \geq (\sqrt[w]{\ell})^2$ for all $1 \leq i \leq n$.

This result can be also obtained from Theorem 10. Indeed, since $P_I = P_S = \frac{1}{\sqrt[w]{\ell}}$, we have $P_D = \frac{1}{\sqrt[w]{\ell}} = \frac{1}{q}$, where $q = \sqrt[w]{\ell}$. By our Theorem 10 (i) and (ii) it follows that $|E_i| \geq q^2 = (\sqrt[w]{\ell})^2$. and $|E| \geq q^{2w} = (\sqrt[w]{\ell})^{2w} = (\ell)^2$ proving the desired result.

This result applies to *all* (w, n) MRA-codes and does not require the code to be perfect for impersonation, or the assumption that the code is without secrecy.

3. The second parts of Theorem 9, 10 and 11 in [10] do not have any counterpart in this paper.