Multireceiver Authentication Codes: Models, Bounds, Constructions and Extensions

R. Safavi-Naini *
H. Wang
School of IT and CS
University of Wollongong, Northfields Ave
Wollongong 2522, Australia
Email: [rei, hw13]@uow.edu.au

August 29, 1998

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 and flexible constructions for such codes. Finally we extend the basic model to the case that multiple messages are sent and the case that the sender can be any member of the group.

1 Introduction

Multireceiver authentication codes (MRA-codes) are introduced by Desmedt, Frankel and Yung (DFY) [6] as an extension of Simmons' model of unconditionally secure authentication [18]. In an MRA-code, a sender wants to authenticate a message for a group of receivers such that each receiver can verify authenticity of the received message. The 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 codes 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 is based on unproven assumptions and the attackers have finite amount of computational resources. In this paper, we will be only concerned with the unconditionally secure model, that is, 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 and to send an authenticated

*Support for this project was partly provided by Australian Research Council Grant A49703076.

message, 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 enable them to construct 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 $w-1$ ($w < n$), 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 basic motivation of studying MRA-codes that are more efficient than the trivial one described above. DFY gave two constructions for (w, n) MRA-codes based on polynomials over finite fields and finite geometries. DFY description of MRA-code is basically an operational description of the system, that is the way the system works. Kurosawa and Obana (KO) [13] studied (w, n) MRA-code, again using the operational description of these codes, 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. They showed that DFY polynomial construction is in fact an optimal (smallest sizes of transmitter and receiver keys) construction.

In this paper we start by giving a formal definition of an MRA-code and use it to derive information theoretic bounds on the probability of success in impersonation and substitution attack against a single receiver for a general MRA-code. These bounds are used to obtain lower bounds on the the number of keys of transmitter and receivers, and also lower bound on the length of the transmitted codeword in terms of deception probability of the system. This is followed by a review of the known constructions of MRA-codes, pointing out their shortcomings and giving constructions that alleviate these shortcomings. Finally we discuss two extensions of MRA-codes, codes for multiple message transmissions and codes with dynamic senders, and give constructions for each. In the concluding section we propose possible extensions for this work.

The paper is organised as follows. Section 2 provides basic definitions and reviews known results. In section 3 we define MRA-codes and derive information theoretic and combinatorial bounds. In section 4 we first review DFY polynomial construction and then propose a more flexible construction by combining an arbitrary A-code with a cover-free family. In section 5 we consider two generalisations of our basic system and give an efficient construction for each. Finally in Section 6 we summarise our results and discuss open problems. Results presented in this paper were in part presented at Eurocrypt '98.

2 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 $f(e, s)$ from a set M and sends it to the receiver who can verify its authenticity using his knowledge of the

key.

Definition 2.1 *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 he calculates for s using his 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 accepted 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 and requires enemy's best strategy to be randomly selecting one of the remaining codewords such that the source state is different from the observed one. For Cartesian A-codes the probability of success of the intruder is $P_S = \frac{1}{|\mathcal{T}|}$.

An extension of this model, proposed by Desmedt, Frankel and Yung (DFY) [6], 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, $E_2..,E_n$ denote the set of decoding rules of receivers $R_1, \cdots R_n$, and S and M denote the set of source states and senders codewords, respectively. We will also use X to denote a random variable defined on a set X.

Definition 2.2 *([13]) We say that $(S, M, E_1, \cdots, E_n)$ is a (w, n) multireceiver A-code if for $\forall(E_{i_1}, \cdots, E_{i_w})$ and $\forall(e_1, \cdots, e_w)$,*

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

Probabilities of success in impersonation and substitution attacks, P_I and P_S, for (w, n) MRA-codes are then defined as

$$P_I = \max_{R_i} \max_{m} P(R_i \text{ accepts } m)$$

$$P_S = \sum_{m} P(m) \max_{R_i} \max_{m'} P(R_i \text{ accepts } m' | R_i \text{ accepts } m)$$

where maximum is taken over m' such that the source state of m' is different from that of m. With these definitions, they derived the following bounds. Assume $\ell = |M|/|S|$.

Theorem 2.1 *(Theorem 9 [13]) In a (w,n) MRA-code, $P_I \geq 1/\sqrt[w]{\ell}$. Equality holds if and only if $P(R_{i_1},\ldots,R_{i_w}\ accept\ m) = 1/\ell$ and $P(R_j\ accepts\ m) = 1/\sqrt[w]{\ell}$ for any m and any R_j.*

Theorem 2.2 *(Theorem 10 [13]) In a (w,n) MRA-code without secrecy, if $P_I = 1/\sqrt[w]{\ell}$, then $P_S \geq 1/\sqrt[w]{\ell}$. Equality holds if and only if*

$$P(R_{i_1},\ldots,R_{i_k}\ accept\ m' | R_{i_1},\ldots,R_{i_k}\ accept\ m) = 1/\ell$$

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

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

Theorem 2.3 *(Theorem 11 [13]) In a (w,n) MRA-code without secrecy, if $P_I = P_S = 1/\sqrt[w]{\ell}$, then $|E_j| \geq (\sqrt[w]{\ell})^2$ for $\forall j$. If equality holds, then each rule of E_j is used with equal probability.*

KO characterised Cartesian MRA-codes that satisfy $P_I = P_S = 1/\sqrt[w]{\ell}$ 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 size for the authenticator.

Definition 2.2 does not specify the relationship between the encoding functions of the transmitter and the receivers and only requires the independence of receivers' keys for any set of w receivers. This independence, as shown in Lemma 3.1, is sufficient to ensure that the probability of success in impersonation attack by any $w-1$ receivers against another receiver is the same as that by an (outside) opponent. We give a general definition of MRA-codes in terms of commutative mappings, and for (w,n) MRA-codes only require the success probability of attackers in impersonation and/or substitution attacks to be less than one. However we do allow coalition of insiders to have higher chance of success compared to an outsider. KO's definition of (w,n) MRA-codes corresponds to our definition of (w,n) MRA-codes that are perfect for impersonation (see Lemma 3.1).

3 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 $X_1, \ldots X_n$, and by p_i the projection mapping of $X_1 \times \cdots \times X_n$ on X_i. That is, $p_i : X_1 \times \cdots \times X_n \longrightarrow X_i$ defined by $p_i(x_1, x_2, \ldots, x_n) = x_i$. 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 $g_1 \times g_2$, where $g_1 \times g_2 : X_1 \times X_2 \longrightarrow Y_1 \times Y_2$ is 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 3.1 *Let $C = (S, M, E, f)$ and $C_i = (S, M_i, E_i, f_i)$, $i = 1, 2, \ldots, n$, be authentication codes. We call $(C; C_1, C_2, \ldots, C_n)$ 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 $\tau_i : E \longrightarrow E_i$ and $\pi_i : M \longrightarrow M_i$ are surjective. We also assume that for each code C_i the probability distribution on the source states of C_i 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 $R_1, \ldots, R_n$ denote the n receivers. In order to authenticate a message, the sender and 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, $1 \leq i \leq n$.

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's 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 3.1 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 $R_1, \ldots, R_n$. Let $L = \{i_1, \ldots i_\ell\} \subseteq \{1, \ldots, n\}$, $E_L = E_{i_1} \times \cdots \times E_{i_\ell}$ and $R_L = \{R_{i_1}, \cdots, R_{i_\ell}\}$. 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

$$P_I[i, L] = \max_{e_L \in E_L} \max_{m \in M} P(m \text{ is accepted by } R_i \mid e_L) \tag{1}$$

where $i \notin L$.

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,

$$P_S[i, L] = \max_{e_L \in E_L} \max_{m \in M} \max_{m' \neq m \in M} P(R_i \text{ accepts } m' | m, e_L) \quad (2)$$

The following two bounds are generalisations of Simmons' bound [18] and Brickell's bound [4], when the attack is from a group of insiders who have access to part of the key information.

Theorem 3.1 *Let $P_I[i, L]$ and $P_S[i, L]$ be defined as in equation (1) and (2). Assume that $M' \neq M$, then*

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 given in the Appendix I.

Corollary 3.1

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

Proof: The corollary follows from Theorem 3.1 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 subset of $w - 1$ receivers can construct a fraudulent codeword accepted 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 for 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 for 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.

Lemma 3.1 *A sufficient condition for a (w, n) MRA-code to be perfect for impersonation is that $P(e_i | e_L) = P(e_i)$ for all w-subsets $L \cup \{i\}$, $i \notin L$ of $\{1, \ldots, n\}$.*

Proof: Consider the A-code $C_i = (S, M_i, E_i)$, we define an authentication 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 $P(\pi_i(m) \text{ is valid in } C_i) = \sum_{e_i \in E_i} \chi(\pi_i(m), e_i) P(e_i)$. By the definition of $\chi_I(m, e_i, e_L)$ (see Appendix I), we know that for any given e_L in accordance with $\tau_L(e) = e_L$ and $\tau_i = e_i$, $\chi(\pi_i(m), e_i) = \chi_I(m, e_i, e_L)$. Thus we have

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

□

In the above lemma, $P_I[i]$ is success probability of an outsider in impersonation attack and is given by

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

It should also be noted that a (w, n) MRA-code which is perfect for impersonation is not necessarily perfect for substitution.

Let $(C; C_i, \ldots, C_n)$ 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 maximum is taken over all possible w-subsets $L \cup \{i\}$ $(i \notin L)$ of $\{1, 2, \ldots, n\}$. 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.

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

Theorem 3.2 *Let $(C; C_1, \ldots, C_n)$ be a (w, n) MRA-code. Assume that $P_D \leq 1/q$ and there is a uniform probability distribution on the source states S. Then*

(i) $|E_i| \geq q^2$, *for each* $i \in \{1, \ldots, n\}$.

(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: (i) For each $(w-1)$-subset L of $\{1, \ldots, n\}$ and any $i \in \{1, \ldots, n\}$ where $i \notin L$, by Theorem 3.1 and Corollary 3.1 we have

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

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

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

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

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 $I(M;E) \geq I(M; E_1, \ldots, E_w)$. It follows that

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

where $Q_i = \{1, \ldots, i-1\}$. 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,

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

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 it is easy to verify that they are satisfied by the DFY polynomial construction. In this construction (briefly recalled in the next section), we have $P_D = 1/q$, $|E_i| = q^2$, for all $1 \leq i \leq n$, $|E| = q^{2w}$ and $|M| = q^w |S|$ and so the lower bounds are satisfied with equality.

□

Comparison of the bounds with KO's bounds: Theorem 3.2 gives combinatorial bounds on the size of the transmitter's and receivers' key spaces for general (w, n) MRA-codes with or without secrecy when probability of deception is known. It also lower bounds the required redundancy in terms of the deception probabilities.

KO derived a similar set of bounds (Theorem 9, 10, 11 in [13]) which only apply to (w, n) MRA-codes without secrecy that are perfect for impersonation. In Appendix II we give a detailed comparison of the two sets of bounds.

4 Constructions

4.1 DFY Polynomial Construction

In [6], Desmedt, Frankel and Yung gave two constructions for MRA-codes: one is based on polynomials and the other based on finite geometries. We briefly review DFY's polynomial construction because generalisations of this scheme will be discussed in later sections of this paper. Details of the geometric construction can be found in [6].

Assume there is a sender T, and n receivers $R_1, \ldots, R_n$. DFY polynomial scheme works as follows. The key for T consists of two random polynomials $P_0(x)$ and $P_1(x)$, each of degree at most $w-1$, with coefficients in $GF(q)$, where $q > \max\{|S|, n\}$. 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 [6] that the construction results in a MRA-code with $P_D = 1/q$ and the following parameters:

$$|S| = \frac{1}{q},\ |E_i| = q^2, \forall i \in \{1, \ldots, n\},\ |E| = 2^{2w},\ \text{and } |M| = q^w |S|.$$

Hence the bounds in Theorem 3.2 can be achieved with equality.

A trivial construction for MRA-codes, as mentioned in the introduction, requires the sender to store many key bits and produces a long tag for the authenticated message. DFY scheme significantly reduces the size of the key storage and the length of the authentication tag. However the order of the field $GF(q)$ must be chosen bigger than the size of the source space and the number of the receivers. In fact q, which can be thought of as the security parameter of the system, ($P_I = P_S = 1/q$), determines the size of the key storage and the length of the authentication tag. This makes the construction very restrictive because although it is acceptable to have the key storage, and length of the tag, a function of the security parameter of the system, but having the number of receivers and the size of the source bounded by it, is not reasonable. In particular when the size of the source or the number of the receivers are very large, P_I and P_S will be unnecessarily small and the key storage of the sender and the receivers, together with the length of the authentication tag will become prohibitively large.

In practice, we may deal with the scenarios where we are satisfied with deception probabilities higher than $1/q$, but have limitation on key storage or communication bandwidth. So it is desirable to look for constructions that can cater for such trade-offs. In Section 4.2 we will give a construction that accommodates this situation.

4.2 A construction based on (n, m, w)-cover-free family

In this section we present a general construction for (w, n) MRA-codes by combining an arbitrary A-code with an (n, m, w)-*cover-free Family*.

Definition 4.1 *Let $X = \{x_1, \ldots, x_m\}$ and $\mathcal{F} = \{B_1, \ldots, B_n\}$ be a family of subsets of X. We call $(X, \mathcal{F})$ an* (n, m, w) Cover-Free Family *(CFF) if $B_0 \not\subset B_1 \cup \cdots \cup B_{w-1}$ for all $B_0, B_1, \ldots, B_{w-1} \in \mathcal{F}$, where $B_i \neq B_j$ if $i \neq j$.*

CFFs were introduced by Erdös et al in [8] and [9], further implicitly studied by Fujii, Kachen and Kurosawa in [11] in connection with MRA-codes. An $(n, w, 2)$ CFF is exactly a Sperner family. A trivial CFF is the family consisting of single element subsets, in which case $n = m$. Non-trivial CFFs are those with $n > m$. A good CFF is one that for given m and w, n is large. Finding good CFFs with the largest possible n is believed to be a hard combinatorial problem [7]. Construction of CFFs employs various areas of mathematics such as finite geometry, design theory and probability theory, and is beyond the scope of this paper.

Assume that $(X, \mathcal{F})$ is an (n, m, w) CFF and $(S, \mathcal{T}, E, f)$ is an A-code without secrecy. We construct a (w, n) MRA-code as follows

1. **Key Distribution:** The KDC randomly chooses an m-tuple of keys $(e_1, \ldots, e_m) \in E^m$, then privately sends $(e_1, \ldots, e_m)$ to the sender T and e_i to every receiver R_j for all j with $x_i \in B_j$, $1 \leq i \leq m$.

2. **Broadcast:** For a source state $s \in S$, the sender calculates $a_i = f(s, e_i)$ for all $1 \leq i \leq m$ and broadcast $(s, a_1, \ldots, a_m)$.

3. **Verification:** Since the receiver R_i holds the keys $\{e_j \mid$ for all j with $x_j \in B_i\}$, R_i accepts $(s, a_1, \ldots, a_m)$ as authentic if for all j satisfying $x_j \in B_i$, $a_j = f(s, e_j)$.

Assume that the probabilities of impersonation and substitution attacks for the underlying A-code, C, is P_I and P_S, respectively, and let $\alpha = \min\{|B_0 \backslash B_1 \cup \cdots \cup B_{w-1}|;$ for all $B_0, \ldots, B_{w-1} \in \mathcal{F}\}$.

Theorem 4.1 *The above scheme is a (w, n) MRA-code and the probabilities of impersonation and substitution attacks are $(P_I)^\alpha$ and $(P_S)^\alpha$, respectively.*

The proof of the theorem is straightforward. In this scheme the sender is required to store $m\lceil \log |E| \rceil$ bits, and the receiver R_i to store $|B_i| \lceil \log |E| \rceil$ bits. The authentication tag is of size $m\lceil \log |\mathcal{T}| \rceil$.

In [11], Fujii, Kachen and Kurosawa gave a definition of broadcast authentication which can be seen as a special case of DFY definition of MRA systems. Fujii *et al* also gave a construction for their broadcast authentication system which is a special case of the above construction, when the cover-free family has constant block size; that is $|B_i| = c, i = 1, \ldots, n$.

An important property of this construction is that it allows a complex system, such as a (w, n) MRA-code, to be constructed from two simpler ones, an A-code and a cover-free family, such that the security of the former can be described in terms of the properties and parameters of the latter. Another advantage of this construction is its flexibility in choosing system parameters. That is w and n are determined by the cover-free family while P_I and P_S are determined by the A-code and the cover-free family and so it is possible to fix w and n but change the A-code to obtain MRA-codes that provide the required protection. The following examples compare this construction with that of DFY polynomial scheme.

Example 4.1 *Assume that the size of the source state is only one bit (for example,* yes *and* no*) and we need a $(2, 70)$ MRA-code with the probabilities of impersonation and substitution attacks not greater than $1/2$. Using DFY polynomial scheme we need a finite field $GF(q)$ with $q \geq 70$; it follows that $\lceil \log q \rceil \geq 7$, and so the sender must store at least 28 bits and each receiver must store at least 14 bits. The length of the authentication tag is at least 14 bits, and the probabilities of impersonation and substitution attacks are $(\frac{1}{2})^7$. Now we use our construction. It is easy to see that the Sperner family consisting of all 4-subsets of a set of 8 elements gives a $(70, 8, 2)$ CFF. We define the underlying A-code $C = (S, \mathcal{T}, E, f)$ as follows. Let $S = \mathcal{T} = GF(2)$, $E = GF(2)^2$, and $f : S \times E \longrightarrow \mathcal{T}$ be given by $f(s, (e, e')) = e + se'$. Then C is an A-code with $P_I = P_S = \frac{1}{2}$. Applying our scheme, the sender and each receiver need to store only 16 bits and 8 bits, respectively. The length of authentication tag is of 8 bits and the probabilities of impersonation and substitution attacks are both 1/2.*

Example 4.2 *Assume that the size of the source is very large, for example 2^{20} bits* (i.e. $|S| = 2^{2^{20}}$*). A direct computation shows that the DFY polynomial scheme for $(2, 70)$ MRA-code requires that the sender and each receiver to store 2^{22} and 2^{21} bits, respectively. The length of authentication tag is 2^{21} bits while the probability of impersonation and substitution attacks is not greater that $1/2^{2^{20}}$. In many applications the deception probability of around $1/2^{20}$ is an acceptable security level. Consider an A-code that is constructed from a universal hashing family (see [22]) with the following parameter: 2^{20} bits of source state, 445 bits of authentication key, 20 bits of authentication tag and the probability of impersonation and substitution attacks is not greater than $1/2^{19}$. Combining with the $(70, 8, 2)$ CFF, our construction results*

in a $(2, 70)$ *MRA-code in which the key storages for the sender and each receiver are* 3560 *bits and* 1780 *bits, respectively. The length of the authentication tag is* 160 *bits and the deception probability is bounded by* $1/2^{19}$.

We note that this construction is only suitable for the case when the number of malicious receivers, compared to the total number of the receivers, is not very large. This is due to the following result.

Lemma 4.1 *([9]) In a non-trivial* (n, m, w) *CFF,* $\frac{w(w-1)}{2} \leq n$.

In [7], using probabilistic methods the authors proved that for small w, there exist $(n, O(\log n), w)$ CFFs . Finally, we point out that in general the constructions based on CFFs do not provide MRA-codes that are perfect for impersonation or substitution.

5 Generalisations

The basic MRA-code can be generalised in a number of ways. In this section we look at two possible generalisations.

5.1 MRA-codes for multiple message transmissions

In the basic model of MRA-codes, security analysis is for a single message transmission (only impersonation and substitution attacks are considered) and for a second message no protection is guaranteed. To provide protection for multiple message transmission one possibility is to use a new key after each message is broadcasted. This is a very inefficient solution both in terms of going through a key distribution phase after each message and the amount of key information required for each message. In the following section we propose systems that use a single key distribution phase for multiple message transmission, and compared to using a new key require less key information per communicated message.

5.1.1 Generalised DFY scheme for multiple messages

Assume messages are all distinct and $t < |S|$. The scheme consists of the following steps:

1. **Key distribution:** The KDC randomly generates $t + 1$ polynomials $P_0(x)$, $P_1(x), \ldots, P_t(x)$ of degree at most $w - 1$ and chooses n distinct elements $x_1, x_2, \cdots, x_n$ of $GF(q)$. KDC makes x_i's public and sends privately $(P_0(x), P_1(x), \cdots, P_t(x))$ to the sender T, and $(P_0(x_i), P_1(x_i), \cdots, P_t(x_i))$ to the receiver R_i.

2. **Broadcast:** For a source state s, T computes $A_s(x) = P_0(x) + sP_1(x) + \cdots + s^t P_t(x)$ and broadcasts $(s, A_s(x))$.

3. **Verification:** R_i accepts $(s, A_s(x))$ as authentic if $A_s(x_i) = P_0(x_i) + sP_1(x_i) + \cdots + s^t P_t(x_i)$.

Theorem 5.1 *[17] The above scheme is a* (w, n) *MRA-code in which every key can be used to authenticate up to* t *messages.*

To authenticate t consecutive messages, using basic DFY scheme, $2t$ polynomials are required while in the above scheme we only need $t+1$ polynomials. So the key storage for the sender and receivers are $(t+1)w\lceil \log q \rceil$ bits and $(w+1)\lceil \log q \rceil$ bits, respectively, and are reduced to around half of that of DFY scheme. The length of the authentication tag for both constructions are the same and equal to $tw\lceil \log q \rceil$ bits.

5.1.2 Using Cover-Free Family Construction

To extend the construction of Section 4.2 to support multiple messages it is only required to replace the underlying A-code by an A-code that provides protection against spoofing of order t, $t > 1$. In an *spoofing of order t attack* on an A-code, the enemy has access to t authenticated codewords and wants to constructs a fraudulent one. An A-code *provides perfect protection against spoofing of order t* if enemy's best strategy is randomly selecting one of the remaining codewords. It is straightforward to see that in the construction given in Section 4.2, using an A-code that provides protection against spoofing of order t ensures that probability of success in spoofing of order t (which can be defined similar to A-codes) is equal to $(P_t)^\alpha$, where P_t is the probability of success in spoofing of order t for the A-code used in the construction.

By replacing the underlying A-code with a Wegman-Carter type construction [1] one can obtain an MRA-code for multiple authentication using universal hash functions.

5.2 MRA-codes with dynamic sender

An interesting extension of the model of MRA-code is when the sender is not fixed and can be any member of the group. In this case key distribution is by a *Trusted Authority* (TA) who is only active during key distribution phase. We call the system *MRA-code with dynamic sender*. There are many applications for such systems. For example providing authentication in group communication where members of a group want to broadcast messages such that every other group member can verify the authenticity of the received messages. It is worth noting that providing authentication in group communication is much more difficult than providing confidentiality because in the former group members can participate in coordinated attack against other group members while in the latter protection is only provided against outsider's eavesdropping.

Allowing the sender to be dynamic introduces the notion of *authenticating with respect to a particular identity*. That is, to verify authenticity of a received message a receiver must first assume an identity for the sender and then verify the message with respect to this particular sender. An authenticated message in general carries information that indicates its *origin*, together with its *content information* and hence the system must provide *origin (entity) authentication* and *message authentication* both. In other words the success of an attacker(s) could be by replacing the identity information, or the message content.

5.2.1 The Model

In the model of MRA-code with dynamic sender, there are n users $\mathcal{P} = \{P_1, \ldots, P_n\}$, who want to communicate over a broadcast channel. The channel is subject to spoofing attack: that is a codeword can be inserted into the channel or, a transmitted

codeword can be substituted with a fraudulent one. An attack is directed towards a channel, consisting of a pair of users $\{P_i, P_j\}$, P_i as the sender and P_j as the receiver. A spoofer might be an outsider, or a coalition of $w-1$ users. The aim of the spoofer(s) is to construct a codeword that P_j accepts as being sent from P_i. We assume that the TA is only active during key distribution phase. The system has three phases.

1. **Key Distribution:** The TA generates and distributes secret information to each user.

2. **Broadcast:** One of the users generates an authenticated message for a source state of his/her choice, and broadcasts it.

3. **Verification:** Every user can verify authenticity of the broadcasted message using their own secret information.

Definition 5.1 *A (w, n) MRA-code with dynamic sender is a code for which no $w-1$ subset of users can perform impersonation and/or substitution attack on any other pair of users.*

For the sake of simplicity, we assume that after the key distribution phase, each user can only send at most a *single authenticated message.*

¿From the above definition, we make the following observations.

1. In a (w, n) MRA-code with dynamic sender during the key distribution phase, the TA does not know which user is going to broadcast. That is there are n users and everyone of them could be a sender.

2. A (w, n) MRA-code with dynamic sender is a (w', n) MRA-code with dynamic sender for any $w' \leq w$.

3. We assume that a message is sent only *once by a single sender.* So a possible attack is to change the origin information of codeword and leave the message content intact.

A straightforward construction based on conventional A-codes is to give each pair of users, $\{P_i, P_j\}$, a shared secret key. Note that now a user can generate the authenticators for a message using the secret keys he shares with all P_js, and broadcast the concatenation of them. In this case there are $n(n-1)/2$ pairs of users, which means that a user has to store $(n-1)$ keys, and the TA has to generate and store $(n-1)n/2$ keys. The disadvantages of this scheme are the large amount of keys stored by each user, together with the long tag for the authenticated message. Our aim is to give more efficient constructions which reduce the key management of both the TA and the users, and reduce the authenticator size, compared to this trivial scheme.

5.2.2 Lower Bounds

To define P_I and P_S in an MRA-code with dynamic sender, we note that because every user can be a sender, when a message is received by a user P_i, she/he must first assume an identity for the sender and then verify the authenticity of the message with respect to the assumed identity. The enemy is a set of $w-1$ malicious

users, $P_{l_1}, \ldots, P_{l_{w-1}}$, who attack *a pair* of other users. For example, targeting the pair $\{P_i, P_j\}$, results in P_j accepting a fraudulent messages as being sent from P_i. In impersonation attack, $P_{l_1}, \ldots, P_{l_{w-1}}$ collude and try to launch an attack against a pair of users P_i and P_j, by generating a message such that P_j accepts it as authentic and being sent from P_i. We denote the success probability in this case by $P_I[m; i, j; L]$, where $L = \{P_{l_1}, \ldots, P_{l_{w-1}}\}$. P_I is the best probability of success in such attacks and is defined by

$$P_I = \max_{\{L,i,j\}} \max_{m} P_I[m; i, j; L],$$

where $L \cup \{i, j\}$ runs through all $(w+1)$-subsets of $\{1, 2, \ldots, n\}$.

In the substitution attack, there are two distinct cases.

1. *Message substitution:* After seeing a valid message m broadcasted by P_i, the users $\{P_{l_1}, \ldots, P_{l_{w-1}}\}$ construct a new message m' $(m \neq m')$ such that P_j will accept m' as being sent ¿from P_i. We denote the success probability in this case by $P_S[m, m'; i, j; L]$, and the best probability of such an attack is denoted by $P_{S_{message}}$,
$$P_{S_{message}} = \max_{\{L,i,j\}} \max_{m' \neq m} P_S[m, m'; i, j; L],$$
where $L \cup \{i, j\}$ runs through all $(w+1)$-subsets of $\{1, 2, \ldots, n\}$

2. *Entity substitution:* After seeing a valid message m broadcasted by P_i, the users $\{P_{l_1}, \ldots, P_{l_{w-1}}\}$ construct a new message m', not necessarily different from m', such that P_j will accept m' as being sent ¿from $P_{i'}$, where $i \neq i'$. We denote the success probability in this case by $P_S[m, m'; i, i', j; L]$, and the best probability of such an attack by
$$P_{S_{entity}} = \max_{\{L,i,i',j\}} \max_{m',m} P_S[m, m'; i, i', j; L],$$
where $L \cup \{i, i', j\}$ runs through all $(w+2)$-subsets of $\{1, 2, \ldots, n\}$.

Now the probability of success in the substitution attack for the whole system is defined as

$$P_S = \max\{P_{S_{message}}, P_{S_{entity}}\}.$$

Theorem 5.2 *In a (w, n) MRA-code with dynamic sender, assume that $P_I = P_S \leq 1/q$ and assume there is a uniform probability distribution on the source states S. Then we have:*

(i) $|E_i| \geq q^{2w}$, *for each* $i \in \{1, 2, \ldots, n\}$,

(ii) $|M_i| \geq q^w |S|$, *for each* $i \in \{1, 2, \ldots, n\}$,

where E_i is the set of possible keys of P_i and M_i is the set of possible codewords when P_i is a sender, for all $i \in \{1, 2, \ldots, n\}$. These are tight bounds and there exists a system that satisfies them with equality.

Proof: For each i, $1 \leq i \leq n$, P_i is a possible sender and so the (w, n) MRA-system with dynamic sender induces a $(w, n-1)$ MRA-code, in which the probability of success in impersonation and substitution attacks are both $1/q$. By applying Theorem 3.2, we obtain the required results. In Section 5.2.3 we will show that the bounds are tight by giving a construction that meets them. □

5.2.3 An optimal construction

Now we give a construction for a (w, n) MRA-code with dynamic sender, which is based on symmetric polynomials in two variables. In [17] a (w, n) MRA-code with dynamic sender using Blom's key distribution scheme is proposed. The following construction is a slightly modified version of the construction given in [17]. We show that the construction has the minimum length of keys for users and the authenticator, and meets the bounds in Theorem 5.2 with equality. We first briefly review Blom key distribution scheme.

Blom key distribution scheme

Let $q \geq n$ be a prime power. The TA randomly chooses a symmetric polynomial, $F(x, y)$, with coefficients in $GF(q)$ and of degree less than w. For $1 \leq i \leq n$, the TA computes the polynomial $G_i(x) = F(x, i)$ and gives $G_i(x)$ to user P_i, i.e., $G_i(x)$ is the secret information of P_i. The key associated with the pair of users P_i and P_j is calculated as, $k_{ij} = G_i(j) = G_j(i)$. It is proved [2] that the scheme is unconditionally secure against the collusion of $w - 1$ users in the following sense: the coalition of any $w - 1$ out of n users, say $P_{i_1}, \ldots, P_{i_{w_1}}$, has no information about the key k_{ij} for the pair i, j, where $i, j \notin \{i_1, \ldots, i_w\}$.

(w, n) MRA-code with dynamic sender based on Blom's scheme

The (w, n) MRA-code with dynamic sender based on the Blom's scheme, works as follows. Let S be the set of source states and $q \geq \max\{|S|, n\}$ be a prime power.

1. **Key distribution:** The TA chooses n distinct numbers a_i in $GF(q)$ (associate a_i to user P_i, $1 \leq i \leq n$). These values are public and are used as identity information for users. Then the TA randomly chooses 2 symmetric polynomials of degree less than w with coefficients in $GF(q)$,

$$F_\ell(x, y) = (1, x, \ldots, x^{w-1}) A_\ell \begin{pmatrix} 1 \\ y \\ \vdots \\ y^{w-1} \end{pmatrix}, \quad \ell = 0, 1,$$

   where A_ℓ is a $w \times w$ symmetric matrix for $\ell = 0, 1$. For $1 \leq i \leq n$, the TA computes the polynomials

$$G_{\ell i}(x) = F_\ell(x, a_i) = (1, x, \ldots, x^{w-1}) A_\ell \begin{pmatrix} 1 \\ a_i \\ \vdots \\ a_i^{w-1} \end{pmatrix}, \quad \ell = 0, 1,$$

   and gives the 2-tuple of polynomials, $(G_{0i}(x), G_{1i}(x))$, to user P_i. This constitutes the secret information of P_i.

2. **Broadcast:** For $1 \leq i \leq n$, assume that the user P_i wants to generate the authenticated message for a source state $s \in S$. P_i computes the polynomial $M_i(x) = G_{0i}(x) + sG_{1i}(x)$ and broadcasts $(s, a_i, M_i(x))$.

3. **Verification:** The user P_j can verify the authenticity of the message in the following way. P_j accepts $(s, a_i, M_i(x))$ as authentic and being sent from P_i if $M_i(a_j) = G_{0j}(a_i) + sG_{1j}(a_i)$.

Theorem 5.3 *The above scheme is a (w, n) MRA-code with dynamic sender with $P_I = P_S = 1/q$.*

Proof: Assume that after seeing an authenticated message $(s, a_i, M_i(x))$ broadcasted by the user P_i, the users $P_1, \ldots, P_{w-1}$ want to generate a new message $(s', a_i, M_i'(x))$, where $s' \neq s$ such that the user P_j will accepts it as authentic, i.e. $M_i'(a_j) = G_{0j}(a_i) + s'G_{1j}(a_i)$. First, we observe that for each $m \in GF(q)$ each user, say P_t, can calculate the polynomial $G_{0t}(x) + mG_{1t}(x) = (1, x, \cdots, x^{w-1})(A_0 + mA_1) \begin{pmatrix} 1 \\ a_t \\ \vdots \\ a_t^{w-1} \end{pmatrix}$. It follows that for each $m \in GF(q)$, $P_1, \ldots, P_{w-1}$ can calculate a $w \times (w-1)$ matrix $D[m]$ such that the following identity holds

$$(A_0 + mA_1) \begin{bmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_{w-1} \\ \cdots & \cdots & \cdots \\ a_1^{w-1} & \cdots & a_{w-1}^{w-1} \end{bmatrix} = D[m]. \tag{3}$$

Since $(s, a_i, M_i(x))$ is broadcasted, it follows that $P_1, \ldots, P_{w-1}$ know the following polynomial

$$g(x) = (1, x, \cdots, x^{w-1})(A_0 + sA_1) \begin{pmatrix} 1 \\ a_i \\ \vdots \\ a_i^{w-1} \end{pmatrix}.$$

By combining equation (3) and the polynomial $g(x)$, $P_1, \ldots, P_{w-1}$ can also calculate matrices B and C such that the following equations hold.

$$A_0 + sA_1 = C \tag{4}$$

$$(A_0 + mA_1) \begin{bmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_{w-1} \\ \cdots & \cdots & \cdots \\ a_1^{k-1} & \cdots & a_{w-1}^{w-1} \end{bmatrix} = D[m] \quad \text{for all } m \in GF(q) \tag{5}$$

We claim that in the equations (4) and (5) above, knowing C and $D[m]$ for all $m \in GF(q)$ can not determine the 2-tuple matrices (A_0, A_1). In fact, there exist q distinct 2-tuple matrices (A_0, A_1) satisfying equations (4) and (5). This is equivalent to the following statement: *There exists a 2-tuple matrices $(A_0, A_1) \neq (0, 0)$ such that the following equations hold*

$$A_0 + sA_1 = 0 \tag{6}$$

$$(A_0 + mA_1) \begin{bmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_{w-1} \\ \cdots & \cdots & \cdots \\ a_1^{w-1} & \cdots & a_{w-1}^{w-1} \end{bmatrix} = 0 \quad \textit{for all } m \in GF(q) \tag{7}$$

Indeed, consider the symmetric polynomial,

$$\begin{aligned} F(x,y) &= (x-a_1)\cdots(x-a_{w-1})(y-a_1)\cdots(y-a_{w-1}) \\ &= (1,x,\cdots,x^{w-1})A\begin{pmatrix} 1 \\ y \\ \vdots \\ y^{w-1} \end{pmatrix}, \end{aligned}$$

where A is a $w \times w$ symmetric matrix and $A \neq 0$. We define $A_0 = -sA$ and $A_1 = A$, then it is not difficult to verify that (A_0, A_1) satisfies the desired properties.

We note that since $(-sA, A)$ satisfy the equations (6), and (7), so is $(-rsA, rA)$ for all $r \in GF(q)$. This implies that there are q distinct 2-tuple symmetric polynomials which are equally likely to be chosen by the TA. For each 2-tuple matrices (A_0, A_1) of the from $(-rsA, rA)$, let

$$(1, a_j, \cdots, a_j^{w-1})(A_0 + s'A_1)\begin{pmatrix} 1 \\ a_i \\ \vdots \\ a_i^{k-1} \end{pmatrix} = d.$$

Then it is straightforward to verify that $d = 0$ if and only if $r = 0$. This is equivalent to that the q distinct possible 2-tuple polynomials $(F_0(x,y), F_1(x,y))$ chosen by the TA result in q distinct values of the form $F_0(a_i, a_j) + s'F_1(a_i, a_j)$. Therefore the probability of message substitution attack $P_{S_{message}}$ is $1/q$. Similarly, we can prove $P_{S_{entity}} = P_I = 1/q$. □

We see that in this construction the size of each user's key is $|E_i| = q^{2w}$, for all $1 \leq i \leq n$, and the size of codewords is $M_i = q^{w+1} = q^w|S|$. Thus we have shown that the bounds given in Theorem 5.2 are satisfied with equality.

6 Conclusions

Multireceiver authentication is an important cryptographic primitive in secure group communication. In this paper, we formally defined MRA-codes and derived information theoretic and combinatorial lower bounds on their performance. We reviewed other works in this area and showed their relations to our work. We have presented an efficient and flexible construction for MRA-codes by combination of a cover-free family and an A-code. This construction generalises an earlier work by Fujii, Kachen and Kurosawa. We also generalised Desmedt, Frankel and Yung (DFY) polynomial construction for multiple messages transmission. Finally, we introduced the model of multireceiver authentication code with dynamic sender, derived combinatorial bounds for key and message sizes of such a system, and gave an optimal construction that meets the bounds with equality. Deriving information theoretic bound for MRA systems with dynamic senders, and construction of systems with more than one dynamic sender are interesting open problems. Another important direction to generalise this work is to require MRA systems to provide secrecy against outsiders. Study of MRA systems so far has been in the context of systems without secrecy. Requiring secrecy of broadcasted message can also be seen as adding authenticity to the known model of broadcast encryption [10]. This means that we require general

multireceiver systems that reduce to MRA-codes and broadcast encryption systems when only authenticity, or only secrecy, is required. A successful generalisation will extend the known model of MRA-code by imposing an access structure on the set of receivers such that only the authorised set of receivers can verify authenticity of messages.

Acknowledgements We would like to thank the anonymous referee for insightful comments and suggestions on the original draft of this paper.

References

[1] M. Atici and D. R. Stinson, Universal Hashing and Multiple Authentication, *Lecture Notes in Comp. Sci.* **1109**(1996), 16-30. (Advances in Cryptology – Crypto '96)

[2] R. Blom, An optimal class of symmetric key generation systems, *Lecture Notes in Computer Science* **209**(1985), 335-338 (Advances in Cryptology–Eurocrypt '84).

[3] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, Perfectly secure key distribution for dynamic conferences. *Lecture Notes in Computer Science* **740**(1993), 471-486 (Advances in Cryptology – CRYPTO'92)

[4] E. F. Brickell, A few results in message authentication, *Congressus Numerantium,* Vol.43(1984), 141-154.

[5] T. Cover and J. Thomas, Elements of Information Theory, *New York; Wiley,* 1991.

[6] Y. Desmedt, Y. Frankel and M. Yung, Multi-receiver/Multi-sender network security: efficient authenticated multicast/feedback, *IEEE Infocom'92,* (1992) 2045-2054.

[7] M. Dyer, T. Fenner, A. Frieze and A. Thomason, On key storage in secure Networks. *Journal of Cryptology* **8**(1995), 189-200.

[8] P. Erdös, P. Frankl, and Z. Furedi, Families of finite sets in which no sets is covered by the union of two others, *Journal of Combinatorial Theory, Series A* **33**(1982), 158-166.

[9] P. Erdös, P. Frankl, and Z. Furedi, Families of finite sets in which no sets is covered by the union of r others, *Israel Journal of Mathematics* **51**(1985), 79-89.

[10] A. Fiat and M. Naor, Broadcast Encryption. In "Advances in Cryptology – Crypto '93", *Lecture Notes in Computer Science* **773** (1994), 480-491.

[11] H. Fujii, W. Kachen and K. Kurosawa, Combinatorial bounds and design of broadcast authentication, *IEICE Trans.*, VolE**79**-A, No. 4(1996)502-506.

[12] 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.

[13] K. Kurosawa and S. Obana, Characterisation of (k, n) multi-receiver authentication, *Information Security and Privacy, ACISP'97*, Lecture Notes in Cpmput. Sci. **1270**,(1997) 204-215.

[14] J. L. Massey, Cryptography - a selective survey, *Digital Communications*, North Holland(pub) (1986)3-21.

[15] C. J. Mitchell and F. C. Piper, Key storage in secure networks. *Discrete Applied Mathematics* **21**(1988), 215-228.

[16] K. A. S. Quinn, Some constructions for key distribution patterns, *Designs, Codes and Cryptography* **4**(1994), 177-191.

[17] 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.

[18] G. J. Simmons, Authentication theory/coding theory, Lecture Notes in Comput. Sci., **196** 411-431. (Crypto '84).

[19] 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.

[20] B. Smeets, Bounds on the Probability of Deception in Multiple Authentication, *IEEE Trans. of Information Theory* ,Vol.40, No.5, (1994)1586-1591.

[21] D. R. Stinson, The combinatorics of authentication and secrecy codes, *J. Cryptology* **2**, (1990), 23-390.

[22] D. R. Stinson, Universal Hashing and authentication codes, *Designs, Codes and Cryptography* **4** (1994), 369-280.

[23] D. R. Stinson, On some methods for unconditionally secure key distribution and broadcast encryption. *Designs, Codes and Cryptography*, **12**(1997), 215-243.

[24] 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 Theorem 3.1

1. 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

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

For given $L \subseteq \{1, \ldots, n\}$ and $i \notin L$, let $P(m, e_i, e_L)$ be the joint probability distribution induced by the system. If $\chi_I(m, e_i, e_L) = 0$ then $P(m, e_i, e_L) = 0$. Indeed, if $P(m, e_i, e_L) \neq 0$ then m is a valid message for e with $\tau_i(e) = e_i$ and $\tau_L(e) = e_L$, which contradicts with the definition of $\chi_I(m, e_i, e_L)$.

$$
\begin{aligned}
& I(M; E_i|E_L) \\
= \; & E_{P(m,e_i,e_L)} \tfrac{P(M,E_i|E_L)}{P(M|E_L)P(E_i|E_L)} \\
= \; & \sum_{m \in M, e_i \in E_i, e_L \in E_L} P(m, e_i, e_L) \log \tfrac{P(m,e_i|e_L)}{P(m|e_L)P(e_i|e_L)} \\
= \; & \sum_{m \in M, e_i \in E_i, e_L \in E_L} P(m, e_i, e_L) \log \tfrac{P(e_i|m,e_L)P(m|e_L)}{P(m|e_L)P(e_i|e_L)} \\
= \; & \sum_{\substack{m \in M, e_L \in E_L \\ P(m,e_L) \neq 0}} P(m, e_L) \left(\sum_{e_i \in E_i} P(e_i|m, e_L) \log \tfrac{P(e_i|m,e_L)}{P(e_i|e_L)} \right).
\end{aligned}
$$

For each pair (m, e_L) with $P(m, e_L) \neq 0$, if $\chi_I(m, e_i,e_L) = 0$ then $P(e_i|m, e_L) = 0$. In this case, $P(e_i|m, e_L) \log \frac{P(e_i|m,e_L)}{P(e_i|e_L)} = 0$. It follows that the summation taking over E_i in the above identity is restricted to all e_i for which $\chi_I(m, e_i, e_L)= 1$. Thus we have

$$
\begin{aligned}
& I(M; E_i|E_L) \\
= \; & \sum_{\substack{m \in M, e_L \in E_L \\ P(m,e_L) \neq 0}} P(m, e_L) \left(\sum_{e_i \in E_i} P(e_i|m, e_L)\chi_I(m, e_i, e_L) \right. \\
& \qquad \left. \cdot \log \tfrac{P(e_i|m,e_L)\chi_I(m,e_i,e_L)}{P(e_i|e_L)\chi_I(m,e_i,e_L)} \right).
\end{aligned}
$$

By log-sum inequality we have

$$
\begin{aligned}
& I(M; E_i|E_L) \\
\geq \; & \sum_{\substack{m \in M, e_L \in E_L \\ P(m,e_L) \neq 0}} P(m, e_L) \left(\sum_{e_i \in E_i} P(e_i|m, e_L)\chi_I(m, e_i, e_L) \right) \\
& \qquad \cdot \log \frac{\sum_{e_i \in E_i} P(e_i|m,e_L)\chi_I(m,e_i,e_L)}{\sum_{e_i \in E_i} P(e_i|e_L)\chi_I(m,e_i,e_L)}.
\end{aligned}
$$

For each pair (m, e_L), as we have noted before, if $P(m, e_L) \neq 0$ and $\chi_I(m, e_i,e_L) = 0$, then $P(e_i|m, e_L) = 0$. It follows that

$$
\sum_{e_i \in E_i} P(e_i|m, e_L)\chi_I(m, e_i, e_L) = 1.
$$

and

$$\sum_{e_i \in E_i} P(e_i|e_L)\chi_I(m, e_i, e_L) = P(\pi_i(m) \text{ is valid in } C_i|e_L)$$

We obtain

$$\begin{aligned} & I(M; E_i|E_L) \\ \geq & -\sum_{m\in M, e_L \in E_L} P(m, e_L) \log P(\pi_i(m) \text{ is valid in } C_i|e_L) \\ = & -\sum_{e_L \in E_L} P(e_L) \sum_{m\in M} P(m|e_L) \log P(\pi_i(m) \text{ is valid in } C_i|e_L). \end{aligned}$$

Since

$$\begin{aligned} & P_I[i, L] \\ \geq & \sum_{e_L \in E_L} P(e_L) \left[\max_{m\in M} P(\pi_i(m) \text{ is valid in } C_i|e_L)\right] \\ \geq & \sum_{e_L \in E_L} P(e_L) \left[\sum_{m\in M} P(m|e_L) P(\pi_i(m) \text{ is valid in } C_i|e_L)\right], \end{aligned}$$

by Jensen inequality, it follows

$$\begin{aligned} & \log P_I[i, L] \\ \geq & \sum_{e_L \in E_L} P(e_L) \sum_{m\in M} P(m|e_L) \log P(\pi_i(m) \text{ is valid in } C_i|e_L) \\ \geq & -I(M; E_i|E_L). \end{aligned}$$

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

2. In the substitution attack R_L, receives their keys from the sender, observe a message m that is transmitted by T and substitutes another message m' for m. R_L succeed if m' is accepted by R_i as authentic. We denote by $P_S[i, L]$ the successful probability that R_L perform substitution attack on R_i. We have

$$P_S[i, L] = \max_{e_L \in E_L} \max_{m\in M} \max_{m'\neq m\in M} P(\pi_i(m) \text{ is valid in } C_i|m, e_L)$$

Now we define a substitution characteristic function $\chi_S(m', m, e_i, e_L)$ by

$$\chi_S(m', m, e_i, e_L) = \begin{cases} 1 & \chi_I(m', e_i, e_L) = 1 \text{ and } \chi_I(m, e_i, e_L) = 1, m' \neq m, \\ 0 & \text{otherwise.} \end{cases}$$

We introduce a random variable M' which only takes values when $\chi_S(m', m, e_i$ $, e_L) = 1$. It follows that there is a joint probability distribution $P(m', m, e_i, e_L)$ such that $P(m, e_i, e_L)$ is the probability distribution given in the system and such that if $\chi_S(m', m, e_i, e_L) = 0$ and $P(m, e_i, e_L) \neq 0$ then $P(m', e_i, e_L) = 0$.

$$
\begin{aligned}
& I(M'; E_i|M, E_L) \\
= \quad & E_{P(m',m,e_i,e_L)}) \log \tfrac{P(M',E_i|M,E_L)}{P(M'|M,E_L)P(E_i|M,E_L)} \\
= \quad & \sum_{\substack{m'\in M', m\in M \\ e_i\in E_i, e_L\in E_L}} P(m', m, e_i, e_L) \log \tfrac{P(m',e_i|m,e_L)}{P(m'|m,e_L)P(e_i|m,e_L)} \\
= \quad & \sum_{\substack{m'\in M', m\in M \\ e_i\in E_i, e_L \in E_L}} P(m', m, e_L) P(e_i|m', m, e_L) \log \tfrac{P(m'|m,e_L)P(e_i|m',m,e_L)}{P(m'|m,e_L)P(e_i|m,e_L)} \\
= \quad & \sum_{\substack{m'\in M', m\in M \\ e_L\in E_L, P(m,m,e_L)\neq 0}} P(m', m, e_L) \sum_{e_i\in E_i} P(e_i|m', m, e_L) \\
& \qquad \cdot \log \tfrac{P(m'|m,e_L)P(e_i|m',m,e_L)}{P(m'|m,e_L)P(e_i|m,e_L)}
\end{aligned}
$$

If $P(m', m, e_L) \neq 0$ then $\chi_S(m', m, e_i, e_L) = 0$ implies $P(e_i|m', m, e_L) = 0$, and so

$$
P(e_i|m', m, e_i, e_L) \log \frac{P(e_i|m', m, e_L)}{P(e_i|m, e_L)} = 0.
$$

Thus the summation taking over E_i in the above identity is restricted to all e_i for which $\chi_S(m',m, e_i, e_L) = 1$. By log-sum inequality, we have

$$
\begin{aligned}
& I(M'; E_i|M, E_L) \\
= \quad & \sum_{\substack{m'\in M, m\in M \\ e_L\in E_L, P(m',m,e_L)\neq 0}} P(m', m, e_L) \sum_{e_i\in E_i} P(e_i|m', m, e_L)\chi_S(m', m, e_i, e_L) \\
& \qquad \cdot \left(\log \tfrac{P(e_i|m',m,e_L)\chi_S(m',m,e_i,e_L)}{P(e_i|m,e_L)\chi_S(m',m,e_i,e_L)} \right) \\
\geq \quad & \sum_{\substack{m'\in M, m\in M \\ e_L\in E_L, P(m',m,e_L)\neq 0}} P(m', m, e_L) \sum_{e_i\in E_i} P(e_i|m', m, e_L)\chi_S(m', m, e_i, e_L) \\
& \qquad \cdot \left(\log \frac{\sum_{e_i\in E_i} P(e_i|m',m,e_L)\chi_S(m',m,e_i,e_L)}{\sum_{e_i\in E_i} P(e_i|m,e_L)\chi_S(m',m,e_i,e_L)} \right)
\end{aligned}
$$

Again, if $P(m', m, e_L) \neq 0$ and $\chi_S(m', m, e_i, e_L) = 0$ then $P(e_i|m', m, e_L) = 0$. It follows that

$$
\sum_{e_i\in E_i} P(e_i|m', m, e_L)\chi_S(m', m, e_i, e_L) = 1
$$

and

$$\sum_{e_i \in E_i} P(e_i|m, e_L)\chi_S(m', m, e_i, e_L) = P(\pi_i(m') \text{ is valid in } C_i|m, e_L\ )$$

So we have

$$\begin{aligned} & I(M'; E_i|M, E_L) \\ \geq\ & -\sum_{m' \in M', m \in M, e_L \in E_L} P(m', m, e_L) \log P(\pi_i(m') \text{ is valid in } C_i|m, e_L) \\ =\ & -\sum_{m \in M, e_L \in E_L} P(m, e_L) \sum_{m' \in M'} P(m'|e_L, m) \log P(\pi_i(m') \text{ is valid in } C_i|m, e_L) \end{aligned}$$

Since

$$\begin{aligned} & P_S[i, L] \\ \geq\ & \sum_{e_L \in E_L} P(e_L) \sum_{m \in M} P(m|e_L) \sum_{m' \in M'} P(m'|m, e_L) P(\pi_i(m') \text{ is valid in } C_i|m, e_L) \\ \geq\ & \sum_{e_L \in E_L, m \in M} P(e_L, m) \sum_{m' \in M'} P(m'|m, e_L) P(\pi_i(m') \text{ is valid in } C_i|m, e_L). \end{aligned}$$

By Jensen's inequality, it follows

$$\begin{aligned} & \log P_S[i, L] \\ \geq\ & \sum_{e_L, m \in M} P(e_L, m) \sum_{m' \in M'} P(m'|m, e_L) \log P(\pi_i(m') \text{ is valid in } C_i|M, e_L) \\ \geq\ & -I(M'; E_i|M, E_L). \end{aligned}$$

We obtain

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

APPENDIX II

In the following we give we comparison between bounds obtained in Theorem 3.2 and the bounds derived by Kurosawa and Obana in [13]. Let $\ell = \frac{|M|}{|S|}$.

1. In [13] the first part of Theorem 9 proves that

$$P_I \geq \frac{1}{\sqrt[w]{\ell}}.$$

We show that our Theorem 3.2 (iii) implies that

$$P_D = \max\{P_I, P_S\} \geq \frac{1}{\sqrt[w]{\ell}}.$$

This is because assuming $P_D = \max\{P_I, P_S\} = 1/q$ and using Theorem 3.2 (iii), we have

$$|M| \geq q^w |S| \Longrightarrow P_D = \frac{1}{q} \geq \sqrt[w]{\frac{|S|}{|M|}} = \frac{1}{\sqrt[w]{\ell}}.$$

Our result applies to general MRA-codes. KO result is stronger as $P_S \geq 1/q$ implies $P_D \geq 1/q$, but only applies to MRA-codes that are perfect for impersonation.

2. Theorem 10 and 11 in [13] in fact prove the following result(see also the introduction in [13]).

Theorem .1 *(KO [13]) 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 3.2. 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 3.2 (i) and (ii) it follows that

$$|E_i \geq q^2 = (\sqrt[w]{\ell})^2.$$

$$|E| \geq q^{2w} = (\sqrt[w]{\ell})^{2w} = (\ell)^2$$

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 [13] do not have any counterpart in this paper.