New Results on Multi-receiver Authentication Codes

R. Safavi-Naini
H. Wang

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

Abstract. Multi-receiver authentication is an extension of traditional point-to-point message authentication in which a sender broadcasts a single authenticated message such that all the receivers can independently verify the authenticity of the message, and malicious groups of up to a given size of receivers can not successfully impersonate the transmitter, or substitute a transmitted message. This paper presents some new results on unconditionally secure multi-receiver authentication codes. First we generalize a polynomial construction due to Desmedt, Frankel and Yung, to allow multiple messages be authenticated with each key. Second, we propose a new flexible construction for multi-receiver A-code by combining an A-code and an (n, m, k)-cover-free family. Finally, we introduce the model of multi-receiver A-code with dynamic sender and present an efficient construction for that.

Keywords: Authentication code, Multi-receiver authentication code.

1 Introduction

Conventional authentication systems deal with *point-to-point* message authentication. 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 keys belonging to a set E. To authenticate a message, called a *source state* and denoted by $s \in \mathcal{S}$, transmitter forms a codeword $f(e, s)$ and sends it to the receiver who can verify its authenticity using his knowledge of the key. We are only concerned with *systematic Cartesian A-codes* in which the codeword constructed for s using $e \in E$ is the concatenation of s and $f(e, s)$, that is $(s, f(e, s))$, and $f(e, s)$ is called *authentication tag*, or simply *tag*. The receiver will detect a fraudulent codeword (s, t) if $t \neq f(e, s) \in \mathcal{T}$, where $\mathcal{T}$ denotes the set of all tags.

The opponent can perform an *impersonation attack*, or a *substitution attack*, by constructing a fraudulent codeword that would be 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 the tag and in the case of Cartesian A-codes, his probability of success is $P_0 = \frac{1}{|T|}$. Perfect protection for substitution is defined in a similar way and for Cartesian A-code the probability of success of the intruder is $P_1 = \frac{1}{|T|}$.

An extension of this model, proposed by Desmedt, Frankel and Yung (DFY) [5], is when there are multiple receivers who can not all be trusted. 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. In an (k, n) multi-receiver authentication system there are n receivers such that in any group of k receivers, there is at least one honest receiver. In other words the largest coalition of cheating receivers can have $k - 1$ members. The system provides perfect protection against impersonation, or substitution, if the best chance of success in the corresponding attacks is $1/q$, where q is the common size of tag space for all the receivers.

A multi-receiver authentication code can be constructed from a traditional A-code by allowing transmitter to use n authentication keys for the n receivers and broadcast a codeword that is simply a concatenation of the codewords for each receiver. The length of the combined tag is n times the length of the individual receiver tags, and the transmitter's key is n times the size of a receiver's key. This is a very uneconomical method of authenticating a message as such a system can prevent attacks by even $n - 1$ colluding receivers, while the assumption is that in every group of k receivers there is at least one honest receiver. The question is whether it is possible to have more efficient systems with shorter tags and shorter transmitter's key. Desmedt, Frankel and Yung [5] gave a positive answer to this question by constructing a (k, n) multi-receiver A-code in which the size of the tag and the size of the transmitter's key are significantly less than that of the naive solution. Kurosawa and Obana [10] showed that, these are the smallest sizes of the transmitted tag, and the transmitter's and the receiver's key for the given deception probabilities.

In this paper we present a number of new results on multi-receiver A-codes.

- We extend DFY polynomial construction to authenticate w messages. The construction reduces the key storage of the transmitter by a factor of 2, compared to the repeated use of the DFY system.
- We give a new construction for multi-receiver A-codes by combining an arbitrary A-code and a special combinatorial structure called (n, m, k)-cover-free family. The construction is particularly useful when the number of receivers, or the size of the source is large. In DFY construction the numbers of bits needed for the tag and the keys for the transmitter and receivers are both

at least $\log q$ (in this paper, all logs are in base 2), where q is a prime power that is not less the number of receivers and the size of the source states. This is an unnecessary constraint which is removed in our construction.

- Finally we extend the model of multi-receiver A-code to the case where the transmitter is not determined beforehand. This model is useful for authenticated conference communication. An interesting property of this model is separating message authentication and entity authentication. Again it is possible to have a trivial construction by giving each participant the required key information for the transmitter in a multi-receiver system, but the result will be a very inefficient system. We give a construction which is much more efficient than this elementary construction.

In section 2 after recalling DFY construction, we give the extension to multiple messages. In section 3 we give the new construction for multi-receiver A-codes and finally in section 4 we give the model and construction of multi-receiver A-code with dynamic receiver. Section 5 concludes the paper.

2 Generalization of DFY Scheme to Multiple Messages

In a multi-receiver A-code, there is a trusted *Key Distribution Centre* (KDC) that generates and distributes the required keys. The system has three phases:

1. **Key distribution:** The KDC privately sends to the sender, and each receiver, their individual keys.
2. **Broadcast:** For a source state s, the sender generates an authenticated message using his/her key and broadcasts the authenticated message.
3. **Verification:** Each user can verify the authenticity of the authenticated message.

First, we briefly review DFY scheme for multi-receiver authentication. Assume there is a sender T and n receivers $R_1, \ldots, R_n$. The key for T consists of two random polynomials $P_0(x)$ and $P_1(x)$, of degree at most $k-1$, 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 [5] that in this scheme no group of $k-1$ receivers can perform an impersonation or substitution attacks against a single receiver, with a probability greater than $\frac{1}{q}$.

Extending DFY to multiple messages authentication
Assume q is larger than, or equal to, the number of possible messages and $q \geq n$. The scheme has the following steps:

1. **Key distribution:** The KDC randomly generates $w+1$ polynomials $P_0(x)$, $P_1(x), \cdots, P_w(x)$ of degree at most $k-1$ and chooses n distinct elements $x_1, x_2, \cdots, x_n$ of $GF(q)$. KDC makes x_is public and sends privately $(P_0(x)$, $P_1(x), \cdots, P_w(x))$ to the sender T, and $(P_0(x_i), P_1(x_i), \cdots, P_w(x_i))$ to the receiver R_i.

2. **Broadcast:** For a source state s, T computes $A_s(x) = P_0(x) + sP_1(x) + \cdots + s^w P_w(x)$ and broadcasts $(s, A_s(x))$.
3. **Verification:** R_i accepts $(s, A_s(x))$ as authentic if $A_s(x_i) = P_0(x_i)+sP_1(x_i)+ \cdots + s^w P_w(x_i)$.

The above scheme is a multi-receiver authentication code in which each key can be used to authenticate up to w messages. To prove the security of the scheme, we consider the scenario where for a given key $(P_0(x), P_1(x), \cdots, P_w(x))$, w source states $s_1, s_2, \cdots, s_w$ have been authenticated and there are $k-1$ receivers who want to construct a fraudulent codeword that is acceptable by one of the other receivers. Without loss of generality, we may assume that the malicious receivers are $R_1, R_2, \cdots, R_{k-1}$.

Let $P_i(x) = a_{i0} + a_{i1}x + \cdots, +a_{ik-1}x^{k-1}$, $0 \le i \le w$. Since $s_1, s_2, \cdots, s_w$ have been sent, $A_{s_1}(x), A_{s_2}(x), \cdots, A_{s_w}(x)$ are publicly known where,

$$A_{s_j}(x) = b_{j0} + b_{j1}x + \cdots + b_{jk-1}x^{k-1}, \text{ for all } 1 \le j \le w.$$

and the $k-1$ receivers $R_1, R_2, \cdots, R_{k-1}$ know their keys

$$(P_0(x_1), P_1(x_1), \cdots, P_w(x_1)), \ \cdots, \ (P_0(x_{k-1}), P_1(x_{k-1}), \cdots, P_w(x_{k-1})),$$

It follows that the malicious receivers know the following two matrix equations

$$\begin{bmatrix} a_{00} & a_{10} & \cdots & a_{w0} \\ a_{01} & a_{11} & \cdots & a_{w1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{0k-1} & a_{1k-1} & \cdots & a_{wk-1} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ s_1 & s_2 & \cdots & s_w \\ \cdots & \cdots & \cdots & \cdots \\ s_1^w & s_2^w & \cdots & s_w^w \end{bmatrix} = \begin{bmatrix} b_{10} & b_{11} & \cdots & b_{1k-1} \\ b_{20} & b_{21} & \cdots & b_{2k-1} \\ \cdots & \cdots & \cdots & \cdots \\ b_{w0} & b_{w1} & \cdots & b_{wk-1} \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & x_1 & \cdots & x_1^{k-1} \\ 1 & x_2 & \cdots & x_2^{k-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & x_{k-1} & \cdots & x_{k-1}^{k-1} \end{bmatrix} \begin{bmatrix} a_{00} & a_{10} & \cdots & a_{w0} \\ a_{01} & a_{11} & \cdots & a_{w1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{0k-1} & a_{1k-1} & \cdots & a_{wk-1} \end{bmatrix} = \begin{bmatrix} P_0(x_1) & \cdots & P_w(x_1) \\ P_0(x_2) & \cdots & P_w(x_2) \\ \cdots & \cdots & \cdots \\ P_0(x_{k-1}) & \cdots & P_w(x_{k-1}) \end{bmatrix}.$$

The above two equations can be rewritten as

$$AM_w = B \tag{1}$$

$$X_{k-1}A = C \tag{2}$$

where A, M_w, B, X_{k-1} and C denote the corresponding matrices in an obvious manner.

We first give a lemma, which says that knowing M_w, X_{k-1}, B and C cannot determine A. In other words, the matrix satisfying (1) and (2) is not unique.

Lemma 1. *There exists q different matrices D such that $DM_w = B$ and $X_{k-1}D = C$.*

Proof. See Appendix

Theorem 1. *The above scheme is a (k,n) unconditionally secure multi-receiver authentication code in which every key can be used to authenticate up to w messages.*

Proof. We only consider the substitution attack, the proof for the impersonation is similar. The malicious receivers $P_1,\ldots,P_{k-1}$, want to generate a valid codeword $(s_{w+1}, b_0+b_1x+\cdots b_{k-1}x^{k-1})$ such that it is accepted by R_k. What they try to do is to guess the value of $P_0(x_k)+s_{w+1}P_1(x_k)+\cdots+s_{w+1}^wP_w(x_k)$ and construct a polynomial $A(x)=b_0+b_1x+\cdots+b_{k-1}x^{k-1}$ such that

$$b_0+b_1x_k+\cdots+b_{k-1}x_k^{k-1}=P_0(x_k)+s_{w+1}P_1(x_k)+\cdots+s_{w+1}^wP_w(x_k).$$

In the following we will show that the information held by the colluders allows them to calculate q equally likely different tags for s_{w+1} and hence their probability of success is $1/q$.
From Lemma 1 we know that there are q different matrices D such that $DM_w=B$ and $X_{k-1}D=C$. This implies that there are q different$(w+1)$-tuples of polynomials $(Q_0(x),Q_1(x),\cdots,Q_{w+1}(x))$ such that each of them is equally likely to be the key of the sender. Now we note that **(1)** *the q different $(w+1)$-tuples of polynomials give rise to q different possible keys for R_k.* Indeed, suppose that $Q[x]=(Q_0(x),Q_1(x),\cdots,Q_{w-1}(x))$ and $Q'[x]=(Q'_0(x),Q'_1(x),\cdots,Q'_{w-1}(x))$ are two different keys of T, and their corresponding matrices are D and D'. Then

$$C_k=(Q_0(x_k),Q_1(x_k),\cdots,Q_{w+1}(x_k))=(1,x_k,\cdots,x_k^{k-1})D,$$

and

$$C'_k=(Q'_0(x_k),Q'_1(x_k),\cdots,Q'_{w+1}(x_k))=(1,x_k,\cdots,x_k^{k-1})D',$$

are their corresponding keys for R_k. By Lemma 1, we know that $X_{k-1}D=X_{k-1}D'=C$. It follows that $X_kD=\begin{pmatrix}C\\C_k\end{pmatrix}$ and $X_kD'=\begin{pmatrix}C\\C'_k\end{pmatrix}$. X_k is a Vandermonde matrix and so is invertible. Using the assumption that $D\neq D'$, implies that $C_k\neq C'_k$.
Next, **(2)** *we prove that* $C_k(1,s_{w+1},\cdots,s_{w+1}^w)^T\neq C'_k(1,s_{w+1},\cdots,s_{w+1}^w)^T$, where G^T denotes the transpose of the matrix G. Again, by Lemma 2.1, we have $C_kM_w=C'_kM_w$. Now if $C_k(1,s_{w+1},\cdots,s_{w+1}^w)^T\neq C'_k(1,s_{w+1},\cdots,s_{w+1}^w)^T$ then $C_kM_{w+1}=C'_kM_{w+1}$. But M_{w+1} is an invertible matrix too, it follows that $C_k=C'_k$ which is a contradiction.
Combining **(1)** and **(2)** above we have that for a given s_{w+1}, there are q different values $C_k(1,s_{w+1},\cdots,s_{w+1}^w)^T$ that all are equally likely to be acceptable by R_k. So the probability of the $k-1$ receivers correctly guessing $A(x)$ is $1/q$.

To authenticate w consecutive messages using DFY scheme, $2w$ polynomials are required while in our scheme we only need $w+1$ polynomials. So the key storages for the sender $((w+1)k\log q)$ and receivers $((w+1)\log q)$ are reduced to $\frac{w+1}{2w}$ times of that of DFY scheme, while the lengths of the authentication tag for both constructions are the same $(k\log q)$.

3 A Construction Based on (n, m, k)-Cover-Free Family

In this section we present a general construction for multi-receiver authentication by combining an A-code and a (n, m, k)- *cover-free Family.*

As noted before, a trivial solution for multi-receiver authentication is to give each receiver a shared secret key with the sender, and to transmit a concatenation of the individual authenticated messages to all the receivers. The disadvantage of this solution is that it requires the sender to store many key bits and requires 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 in this scheme the order of the field $GF(q)$ must be bigger than the size of the source and the number of the receivers. Moreover success probabilities of impersonation and substitution attacks, the size of the key storage and the length of the authentication tag are all determined by q. Although it is acceptable to have the key storage, and length of the tag, a function of the probability of success, having the number of receivers and the size of the source bound by this probability is not reasonable. In this case when the size of the source or the number of the receivers are very large, the key storage of the sender and the receivers, as well as the length of authentication tag will become too large. In practice, we may deal with the scenarios that we are satisfied with deception probabilities higher than $1/q$, but have limitation on the key storage or communication bandwidth. So it is desirable to look at construction methods that meet such trade-offs.

Definition 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, k)* Cover-Free Family *(CFF) if $B_0 \not\subseteq B_1 \cup \cdots \cup B_{k-1}$ for all $B_0, B_1, \ldots, B_{k-1} \in \mathcal{F}$, where $B_i \neq B_j$ if $i \neq j$.*

We note that a $(n, w, 2)$ CFF is exactly a Sperner family. CFF has been extensively studied by Erdös et al in [8] and [9]. A trivial CFF is the family consisting of single element subsets, in which $n = m$. Non-trivial CFFs are those with $n > m$. A good CFF is the one that for given m and k, n is as large as possible. Finding good CFFs is believed to be a hard combinatorial problem. Construction of good 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 a (n, m, k) CFF and (S, T, E, f) is an A-code without secrecy. We construct a (k, n) multi-receiver A-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 $\{e_j \mid \text{for all } j \text{ with } x_j \in B_i\}$, 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 of the underlying code C are P_I and P_S, respectively, and let $\alpha = \min\{|B_0 \backslash B_1 \cup \cdots \cup B_{k-1}|;\ \text{for all } B_0, \ldots, B_{k-1} \in \mathcal{F}\}$.

Theorem 2. *The above scheme is a (k,n) multi-receiver A-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 of $m\lceil\log|\mathcal{T}|\rceil$.

The following example compares this construction with that of DFY polynomial scheme. Assume that the size of source states is only one bit (for example, *yes* and *no*) and we need a $(2,70)$ multi-receiver authentication 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 attack 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 $C = (\mathcal{S}, \mathcal{T}, E, f)$ as follows. Let $\mathcal{S} = \mathcal{T} = GF(2)$, $E = GF(2)^2$, and $f : \mathcal{S} \times E \longrightarrow \mathcal{T}$ 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 attack are both 1/2.

Next, we assume that the size of the source state is very large, for example 2^{20} bits (*i.e.* $|S| = 2^{2^{20}}$). A direct computation shows that the DFY polynomial scheme for $(2,70)-$multi-receiver authentication 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 $1/2^{2^{20}}$. However, in many applications the deception probability of about $1/2^{20}$ might yield an acceptable security level. To this end, we choose an A-code that is constructed from universal hashing family (see [13]) with the following parameter: 2^{20} bits of source state, 445 bits of authentication keys, 20 bits of authentication tag and the probability of impersonation and substitution attacks is not greater than $1/2^{20}$. Combining with the $(70,8,2)$ CFF, our construction results in a $(2,70)-$multi-receiver A-code in which the key storages for the sender and each receiver are of 3560 bits and 1780 bits, respectively. The length of the authentication tag is 160 bits and the deception probability is bounded by $1/2^{20}$.

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

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

However, in [7] using a probabilistic method the authors proved that for small k, there exists $(n, O(\log n), k)$ CFFs. Finally, we point out that although in general the construction based on CFF does not provide perfect protection, it is more flexible than DFY polynomial scheme, since the underlying A-code can be chosen according to various requirements. For example, the A-code can be replaced by a universal hashing family, or an A-code for multiple authentication.

4 Multi-receiver Authentication with Dynamic Sender

In this section we study multi-receiver A-codes with dynamic sender. We consider the scenario where there is a KDC and a group of n users. The KDC privately distributes some secret information (key) to each user. At a later time, one of the users generates an authenticated message and broadcasts it such that every other user can verify *the origin* and *integrity* of the message and a collusion of up to a given size of the receivers cannot succeed in impersonation or substitution attacks on other receivers. We assume that in the key distribution phase, the KDC does not know which user is going to broadcast the authenticated message and hence each user is a potential sender or receiver. An obvious construction is by establishing a multi-receiver authentication system between each user, considered as the sender, and all the others, considered as receivers. For instance, for n users $P_1, \ldots, P_n$, using DFY $(k, n-1)$ multi-receiver authentication scheme, gives the following construction. During the key distribution phase, the KDC randomly chooses an n-tuple of polynomial pairs of degree less than k, $([f_1(x), g_1(x)], \ldots, [f_n(x), g_n(x)])$, and secretly gives user P_i, the tuples $[f_i(x), g_i(x)]$ and $([f_1(i), g_1(i)], \ldots, [f_{i-1}(i), g_{i-1}(i)], [f_{i+1}(i), g_{i+1}(i)], \ldots, [f_n(i), g_n(i)])$, for each $1 \leq i \leq n$. During broadcast, user P_i wants to generate an authenticated message for a source state $s \in GF(q)$, P_i calculates $M_i(x) = f_i(x) + sg_i(x)$ and broadcasts $(s, i, M_i(x))$. The user P_j accepts $(s, i, M_i(x))$ as authentic being sent from P_i if $M_i(j) = f_i(j) + sg_i(j)$. In this scheme the KDC must store $2kn\lceil\log q\rceil$ bits and each user to store $2(n+k-1)\lceil\log q\rceil$ bits. The length of the authentication tag for each message is $(k+1)\lceil\log q\rceil$ bits. Since the lengths of keys for KDC and each user are of order $O(n \log q)$, when the number of users is very large, the overhead for the key storage both at the KDC and each user becomes very large.

A multi-receiver A-system with dynamic sender has three phases: *Key distribution*, *Broadcast* and *Verification*.

To define P_I and P_S, 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 $k-1$ malicious users, $P_{l_1}, \ldots, P_{l_{k-1}}$, 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 the impersonation attack, $P_{l_1}, \ldots, P_{l_{k-1}}$ 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 as being sent from P_i. We denote the successful probability in this case by

$P_I[m;i,j;L]$, where $L = \{P_{l_1},\dots,P_{l_{k-1}}\}$. P_I is the best probability of all 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 the $(k+1)$-subsets of $\{1,2,\dots,n\}$
In substitution attack, there are two distinct cases:

1. *Message substitution:* After seeing a valid message m broadcasted by P_i, the users $\{P_{l_1},\dots,P_{l_{k-1}}\}$ 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 the $(k+1)$-subsets of $\{1,2,\dots,n\}$
2. *Entity substitution:* After seeing a valid message m broadcasted by P_i, the users $\{P_{l_1},\dots,P_{l_{k-1}}\}$ 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 the $(k+2)$-subsets of $\{1,2,\dots,n\}$.

Now the probability of the substitution attack for the system is defined as

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

In the following we present a construction for such systems. Let S be the set of source states and assume $S \subset GF(q)$ and $q \geq |S| + n$.

1. **Key distribution:** The KDC chooses n distinct numbers a_i in $GF(q)\backslash S$, and gives a_i to user P_i ($1 \leq i \leq n$). These values are public knowledge and are used as identity information for users. Then the KDC randomly chooses 3 symmetric polynomials of degree less than k with coefficients in $GF(q)$,

$$F_\ell(x,y) = (1,x,\dots,x^{k-1})A_\ell \begin{pmatrix} 1 \\ y \\ \vdots \\ y^{k-1} \end{pmatrix}, \quad \ell = 0,1,2,$$

where A_ℓ is a $k \times k$ symmetric matrix for all $0 \leq \ell \leq 2$. For $1 \leq i \leq n$, the KDC computes the polynomials

$$G_{\ell i}(x) = F_\ell(x,a_i) = (1,x,\dots,x^{k-1})A_\ell \begin{pmatrix} 1 \\ a_i \\ \vdots \\ a_i^{k-1} \end{pmatrix}, \quad \ell = 0,1,2,$$

and gives the 3-tuple of polynomials, $(G_{0i}(x), G_{1i}(x), G_{2i}(x))$, 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 $M_1(x) = G_{0i}(x) + a_i G_{1i}(x) + a_i^2 G_{2i}(x)$ and $M_2(x) = G_{0i}(x) + sG_{1i}(x) + s^2 G_{2i}(x)$ and broadcasts $(s, a_i, M_1(x), M_2(x))$.
3. **Verification:** The user P_j can verify the authenticity of the message in the following way. P_j accepts $(s, a_i, M_1(x), M_2(x)$ as authentic being sent from P_i if $M_1(a_j) = G_{0j}(a_i) + a_i G_{1j}(a_i) + a_i^2 G_{2j}(a_i)$ and $M_2(a_j) = G_{0j}(a_i) + sG_{1j}(a_i) + s^2 G_{2j}(a_i)$.

Theorem 3. *The above scheme is a (k, n) multi-receiver authentication code with $P_I = \frac{1}{q^2}$ and $P_S = P_{S_{message}} = P_{S_{entity}} = \frac{1}{q}$.*

The proof is given in the Appendix. Here we give some intuition behind the proof. Assume that after seeing an authenticated message $(s, a_i, M_1(x), M_2(x))$ broadcasted by the user P_i, the malicious users $P_1, \ldots, P_{k-1}$ want to commit a message substitution attack on the user P_j. They want to generate a polynomial $M(x)$ of degree less than k and a source state $s' \in S, s' \neq s$, such that $M(a_j) = G_{0j}(a_i) + s'G_{1j}(a_i) + s'^2 G_{2j}(a_i) = F(a_i, a_j) + s'F_1(a_i, a_j) + s'^2 F_2(a_i, a_j)$. Using the idea of Blom's key distribution scheme in [1] (for the polynomial representation of Blom's scheme see [2] and [14]), we know that $P_1, \ldots, P_{k-1}$, by pooling their secret information $\{(F_0(x, a_i), F_1(x, a_i), F_2(x, a_i)) \mid i = 1, \ldots, k-1\}$ together can not obtain any information about $(F_0(a_i, a_j), F_1(a_i, a_j), F_2(a_i, a_j))$, and so it is easy to see that even if they know $M_1(a_j))$ and $M_2(a_j)$ the probability that they correctly guess the value of $M(a_j)$ is $1/q$. The contribution of our proof is that it remains true even $P_1, \ldots, P_{k-1}$ know $M_1(x)$ and $M_2(x)$.

This scheme requires the KDC to store $\frac{3k(k+1)}{2}\lceil \log q \rceil$ bits and each user to store $3k\lceil \log q \rceil$ bits. The length of the authentication tag for each message is $(2k+1)\lceil \log q \rceil$ bits. Compared with the construction based on DFY scheme, we see that the key storages of the KDC and the receivers are both reduced. The length of the authentication tag in this construction is about twice of the DFY scheme. The system allows message substitution and entity substitution to be separated. It is possible to halve the size of the authentication tag at the cost of only being able to detect fraudulent messages but not distinguishing the type of fraud (message versus entity).

Generalization

1. The above scheme can be easily generalized for multiple message transmission, in the following way. Instead of 3 symmetric polynomials, by choosing $(w+2)$ $(w \geq 1)$ symmetric polynomials of degree less than k, using a construction similar to that of Section 2, we can generalize the scheme such that the sender (one of the users) can broadcast w authenticated messages.

2. An interesting generalization of the model of multi-receiver A-code with a dynamic sender is to allow more than one user to broadcast authenticated messages in the broadcast stage. It is easy to see that the straightforward generalization of

DFY scheme allows each user to broadcast one message, so a total of n messages can be authenticated in the system. However, if we allow only up to $t(t \leq n)$ users send authenticated messages, it is possible to reduce the key storage and the length of authentication tag. We observe that if more than one sender is allowed, then for each pair of users, for example P_i and P_j, the key information contributing to authentication from P_i to P_j must be different from that used for authentication from P_j to P_i. Otherwise after seeing a broadcast authenticated message from P_i, anyone can perform an attack on P_i by resending the observed message to P_i himself and claiming that this is sent from P_j. Thus the construction based on symmetric polynomial will not be suitable for multiple senders. Rather, the KDC may use polynomials in two variables and of suitable degrees to produce the required key information. Details of this construction will be given in a future paper.

5 Conclusion

In this paper first we generalized DFY polynomial scheme for multi-receiver A-code so that it can be used to authenticate multiple messages instead of a single message. Next we suggested a flexible construction for multi-receiver A-codes by combining an A-code and an (m, n, k) cover-free family. Finally we introduced the model of multi-receiver A-codes with dynamic sender and presented a construction that is much more efficient than the naive method.

Acknowledgements

1. The authors thank Yvo Desmedt for several valuable comments.
2. This work is supported in part by Australian Research Council.

References

1. R. Blom, *An optimal class of symmetric key generation systems*, Lecture Notes in Computer Science, **209**(1985), 335-338 (Advances in Cryptology–Eurocrypt '84)
2. 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).
3. B. den Boer, *A simple and key-economical unconditional authentication scheme*, Journal of Computer Security **2**(1993), 65-71.
4. Y. Desmedt and Y. Frankel, *Shared generation of authenticators and signatures*, Adv. in Cryptology - Crypto '91, Lecture Notes in Comput. Sci., **576**, 457-469.
5. Y. Desmedt, Y. Frankle and M. Yung, *Multi-receiver/Multi-sender network security: efficient authenticated multicast/feedback*, IEEE Infocom'92, (1992) 2045-2054.
6. Y. Desmedt and M. Yung, *Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks*, Lecture Notes in Computer Science, **537**(1991), 177-188 (Advances in Cryptology - Crypto '90).
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. Erdős, 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. Erdős, P. Franlkl, 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. K. Kurosawa and S. Obana, *Characterization of (k,n) multi-receiver authentication*, Information Security and Privacy, ACISP'97, Lecture Notes in Comput. Sci. **1270**,(1997) 204-215.
11. J. L. Massey, *Cryptography - a selective survey*, Digital Communications, North Holland(pub) (1986)3-21.
12. 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.
13. D. R. Stinson, *Universal hashing and authentication codes*, Designs, Codes and Cryptography, **4**(1994), 369-380.
14. D. R. Stinson, *On some methods for unconditionally secure key distribution and broadcast encryption*, Designs, Codes and Cryptography, **12**(1997), 215-243.

APPENDIX

Lemma 2.1 *There exist q different matrices D such that $DM_w = B$ and $X_{k-1}D = C$.*

Proof. It is sufficient to prove that there exist q different matrices D such that $DM_w = 0$ and $X_{k-1}D = 0$. First, we observe that given an $n \times m$ matrix $D_0 = (d_{ij})$, we can associate it a polynomial over x, y

$$F(x,y) = (1, x, \cdots, x^{n-1})D_0 \begin{pmatrix} 1 \\ y \\ \vdots \\ y^{m-1} \end{pmatrix} \tag{3}$$

and conversely, every polynomial $F(x,y)$ can be written as the form (3) for some $n \times m$ matrix D_0. Now consider the polynomial

$$F(x,y) = (x - x_1)(x - x_2)\cdots(x - x_{k-1})(y - s_1)(y - s_2)\cdots(y - s_w).$$

Let $F(x,y) = (1, x, \cdots, x^{k-1})D \begin{pmatrix} 1 \\ y \\ \vdots \\ y^{w} \end{pmatrix}$, where D is a $k \times (w+1)$ matrix and $D \neq 0$. Clearly, $F(x_1, y) = F(x_2, y) = \cdots = F(x_{k-1}, y) = 0$ for all y. It follows

$$\begin{bmatrix} 1 & x_1 & \cdots x_1^{k-1} \\ 1 & x_2 & \cdots x_2^{k-1} \\ \cdots & \cdots & \cdots \ \cdots \\ 1 & x_{k-1} & \cdots x_{k-1}^{k-1} \end{bmatrix} D = 0.$$

Indeed, we may choose $(w+1)$ distinct elements $y_1, y_2, \cdots, y_{w+1}$ in $GF(q)$, then

$$F(x_1, y_i) = F(x_2, y_i) = \cdots = F(x_{k-1}, y_i) = 0, \quad \text{for all } 1 \leq i \leq w+1.$$

Thus we have

$$\begin{bmatrix} 1 & x_1 & \cdots & x_1^{k-1} \\ 1 & x_2 & \cdots & x_2^{k-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & x_l & \cdots & x_{k-1}^{k-1} \end{bmatrix} D \begin{bmatrix} 1 & 1 & \cdots & 1 \\ y_1 & y_2 & \cdots & y_{w+1} \\ \cdots & \cdots & \cdots & \cdots \\ y_1^w & y_2^w & \cdots & y_{w+1}^w \end{bmatrix} = 0$$

Since $\begin{bmatrix} 1 & 1 & \cdots & 1 \\ y_1 & y_2 & \cdots & y_{w+1} \\ \cdots & \cdots & \cdots & \cdots \\ y_1^w & y_2^w & \cdots & y_{w+1}^w \end{bmatrix}$ is a Vandermonde matrix, the desired result follows.

Similarly, we have

$$D \begin{bmatrix} 1 & 1 & \cdots & 1 \\ s_1 & s_2 & \cdots & s_w \\ \cdots & \cdots & \cdots & \cdots \\ s_1^w & s_2^w & \cdots & s_w^w \end{bmatrix} = 0.$$

For each $r \in GF(q)$, we also have $(rD)M_w = 0$ and $X_{k-1}(rD) = 0$. Thus there are q different matrices $\{rD \,|\, r \in GF(q)\}$ with the desired property. So we complete the proof of the lemma

Theorem 4.1 *The above scheme is a (k, n) multi-receiver authentication code with $P_I = \frac{1}{q^2}$ and $P_S = P_{S_{message}} = P_{S_{entity}} = \frac{1}{q}$.*

Proof. Assume that after seeing an authenticated message $(s, a_i, M_1(x), M_2(x))$ broadcasted by the user P_i, the users $P_1, \ldots, P_{k-1}$ want to generate a new message $(s', a_i, M_1(x), M_2'(x))$, where $s' \neq s$ such that the user P_j will accepts it as authentic, i.e. $M_2'(a_j) = G_{0j}(a_i) + s'G_{1j}(a_i) + s'^2 G_{2j}(a_i)$. First, we observe that for each $m \in GF(q)$ each user, P_t say, can calculate the polynomial

$$G_{0t}(x) + mG_{1t}(x) + m^2 G_{2t}(x) = (1, x, \cdots, x^{k-1})(a_0 + mA_1 + m^2 A_2) \begin{pmatrix} 1 \\ a_t \\ \vdots \\ a_t^{k-1} \end{pmatrix}.$$

It follows that for each $m \in GF(q)$, $P_1, \ldots, P_{k-1}$ can calculated a $k \times (k-1)$ matrix $D[m]$ such that the following identity holds

$$(A_0 + mA_1 + m^2 A_2) \begin{bmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_{k-1} \\ \cdots & \cdots & \cdots \\ a_1^{k-1} & \cdots & a_{k-1}^{k-1} \end{bmatrix} = D[m]. \qquad (4)$$

Since $(s, a_i, M_1(x), M_2(x))$ has been broadcasted. it follows that $P_1, \ldots, P_{k-1}$ know the following two polynomials $f(x) = (1, x, \cdots, x^{k-1})(A_0 + a_i A_1 + a_i^2 A_2) \begin{pmatrix} 1 \\ a_i \\ \vdots \\ a_i^{k-1} \end{pmatrix}$

and $g(x) = (1, x, \cdots, x^{k-1})(A_0 + sA_1 + s^2A_2)\begin{pmatrix} 1 \\ a_i \\ \vdots \\ a_i^{k-1} \end{pmatrix}$. By combining equation (4) and these two polynomials, $P_1, \ldots, P_{k-1}$ can also calculate matrices B and C such that the following equations hold.

$$A_0 + a_iA_1 + a_i^2A_2 = B \tag{5}$$

$$A_0 + sA_1 + s^2A_2 = C \tag{6}$$

$$(A_0 + mA_1 + m^2A_2)\begin{bmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_{k-1} \\ \cdots & \cdots & \cdots \\ a_1^{k-1} & \cdots & a_{k-1}^{k-1} \end{bmatrix} = D[m] \text{ for all } m \in GF(q) \tag{7}$$

We claim that in the above equations (5), (6) and (7), knowing B, C, and $D[m]$ for all $m \in GF(q)$ can not determine the 3-tuple matrices (A_0, A_1, A_2). In fact, there exists q distinct 3-tuple matrices (A_0, A_1, A_3) satisfying equations (5), (6) and (7). This is equivalent to the following statement *There exists a 3-tuple matrices* $(A_0, A_1, A_2) \neq (0, 0, 0)$ *such that the following equations hold*

$$A_0 + a_iA_1 + a_i^2A_2 = 0 \tag{8}$$

$$A_0 + sA_1 + s^2A_2 = 0 \tag{9}$$

$$(A_0 + mA_1 + m^2A_2)\begin{bmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_{k-1} \\ \cdots & \cdots & \cdots \\ a_1^{k-1} & \cdots & a_{k-1}^{k-1} \end{bmatrix} = 0 \textit{ for all } m \in GF(q) \tag{10}$$

Consider the symmetric polynomial over x, y

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

where A is a $k \times k$ symmetric matrix and $A \neq 0$. Let $f(x) = (x - a_i)(x - s) = x^2 - (a_i + s)x + a_is$. We define $A_0 = a_isA, A_1 = -(a_i + s)A$ and $A_3 = A$, then it is not difficult to verify that A_0, A_1, A_2 satisfy the desired properties.

We note that if (A_0, A_1, A_3) satisfy the equations (8), (9) and (10) , so is (rA_0, rA_1, rA_3) for all $r \in GF(q)$. This implies that there are q distinct 3-tuple symmetric polynomials which are equally likely to be chosen by the KDC. But, of course, one of them is exactly chosen . Now let the 3-tuple matrices (A_0, A_1, A_2)

satisfy the equations (8), (9) and (10), we claim that for each $s' \neq s, a_i$ in $GF(q)$

$$(1, a_j, \cdots, a_j^{k-1})(A_0 + s'A_1 + s'^2 A_2) \begin{pmatrix} 1 \\ a_i \\ \vdots \\ a_i^{k-1} \end{pmatrix} = d \neq 0$$

Indeed, we have

$$\begin{bmatrix} 1 & a_1 & \cdots & a_1^{k-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & a_{k-1} & \cdots & a_{k-1}^{k-1} \\ 1 & a_j & \cdots & a_j^{k-1} \end{bmatrix} (A_0 + s'A_1 + s'^2 A_2) \begin{bmatrix} 1 & \cdots & 1 & 1 \\ a_1 & \cdots & a_{k-1} & a_i \\ \cdots & \cdots & \cdots & \cdots \\ a_1^{k-1} & \cdots & a_{k-1}^{k-1} & a_i^{k-1} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & a_1 & \cdots & a_1^{k-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & a_{k-1} & \cdots & a_{k-1}^{k-1} \\ 1 & a_j & \cdots & a_j^{k-1} \end{bmatrix} (a_i s - (a_i + s)s' + s'^2)A \begin{bmatrix} 1 & \cdots & 1 & 1 \\ a_1 & \cdots & a_{k-1} & a_i \\ \cdots & \cdots & \cdots & \cdots \\ a_1^{k-1} & \cdots & a_{k-1}^{k-1} & a_i^{k-1} \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 \\ 0 & d \end{bmatrix}$$

Since $f(s') = (s'-s)(s'-a_i) \neq 0$, we have $d = f(s')F(a_i, a_j) \neq 0$. It follows that q distinct 3-tuple matrices give rise to q distinct possible value of d. This is equivalent to that the q distinct possible 3-tuple polynomials $(F_0(x,y), F_1(x,y), F_2(x,y))$ chosen by the KDC results in q distinct values of the form $F_0(a_i, a_j) + s'F_1(a_i, a_j) + s^2 F_2(a_i, A_j)$. Therefore the probability of message substitution attack $P_{S_{message}}$ is $1/q$. Similarly, we can prove that the probability of entity substitution attack $P_{S_{entity}}$ is also $1/q$, and the probability of impersonation attack P_I is $1/q^2$.