A^3-Codes Under Collusion Attacks

Reihaneh Safavi-Naini and Yejing Wang
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, Australia
email: [rei,yejing]@uow.edu.au

January 23, 2002

Abstract

An A^3-code is an extension of an A-code in which none of the three participants, transmitter, receiver and arbiter, is trusted. In this paper we extend the previous model of A^3-codes by allowing the transmitter and the receiver to not only individually attack the system, but also collude with the arbiter against the other. We derive information-theoretic lower bounds on success probability of various attacks, and combinatorial lower bounds on the size of key spaces. We also study combinatorial structure of optimal A^3-code against collusion attacks and give a construction of an optimal code.

Keywords: A^3-codes, optimal A^3-codes, α-resolvable designs, partially balanced t-designs

1 Introduction

Authentication codes (A-codes) [8] provide protection for two trustworthy participants against an active spoofer tampering with the messages sent by a *transmitter* to a *receiver* over a public channel. In this model transmitter and receiver are assumed trusted. An extension of this model is an *authentication codes with arbitration* [9], or A^2-codes for short, in which transmitter and receiver are not trusted: transmitter may deny a message that he/she has sent, and receiver may attribute a fraudulent message to the transmitter. In an A^2-code a trusted third party, called the *arbiter*, resolves the dispute between transmitter and receiver. A^2-codes have been studied by various authors [6, 4, 12, 5].

Brickell and Stinson [1] introduced authentication code with dishonest arbiter(s), or A^3-code, where the arbiter may tamper with the communication but they will remain trusted in their arbitration. In an A^3-code each participant has some secret key information which is used to protect him/her against attacks in the system. These codes have also been studied in [3, 10, 4], where some constructions were given.

Collusion attacks in A-codes have been studied in various extensions of A-codes, such as multisender schemes [2] where unauthorised groups of senders can collude to construct a fraudulent message that is attributed to an authorised group, and multireceiver schemes where unauthorised groups of receivers collude to construct a fraudulent message that is attributed to the transmitter. The model studied in [4] is an extension of multireceiver schemes where the transmitter can collude with unauthorised groups of receivers. In the first two cases no arbitration is required as at least one side in the communication, that is receiver in a multisender scheme and transmitter in a multireceiver scheme, is assumed honest. However in the last case neither transmitter(s) nor the receiver(s) are assumed honest and dispute may arise between the two sides. To resolve the dispute either an honest arbiter is employed or a majority vote of participants will be used. The suggestion for resolving the dispute is to either include a trusted arbiter or, take the majority vote of the receivers.

In this paper we extend the attack model of A^3-codes to include collusion between arbiter and transmitter or receiver, against the other participants. For example, the arbiter may collude with the transmitter to construct a message that the transmitter can later deny sending it, or she may collude with the receiver to impersonate the transmitter or substitute a message that he has sent. We assume that the arbiter always honestly follows the arbitration rules. These rules are public and collusion with a participant effectively means that the arbiter will make her key information available to that participant. An extended abstract version of this paper, where proofs were omitted because of page limit, was published in [11]. In this paper we use a slightly different model (details in section 2), which in essence is the model proposed in [4] enhanced with the collusion attack, and prove a number of results on performance and structure of the codes.

The rest of this paper is organised as follows. In section 2 we introduce the model. In section 3 we derive information-theoretic bounds on success probabilities of various attacks. Combinatorial bounds on the size of key spaces for each participant are given in section 4. Section 5 and section 6 define optimal A^3-codes and Cartesian A^3-codes, respectively. We give

properties of Cartesian optimal A^3-codes. Section 7 gives combinatorial structure of Cartesian optimal A^3-codes. In section 8 we conclude the paper.

2 Model and Bounds

There are three participants: a *transmitter* T, a *receiver* R and an *arbiter* A, none of them is assumed trusted. T wants to send a source state s, $s \in S$, to R over a public channel. Each participant has some secret *key*. T uses his key information to construct a message $m \in M$ for a source state s to be sent over the channel. R uses her key information to verify authenticity of a received message and finally A who does not know the key information of T and R will use her key information to resolve a dispute between the two. Transmitter's key e_t is determined by an encoding function

$$f : E_T \times S \longrightarrow M.$$

The receiver's key e_r is determined by a verification function

$$g : E_R \times M \longrightarrow S \cup \{reject\}$$

and so each e_r determines a subset of M that the receiver will accept as valid message. The arbiter's key e_a is determined by an arbitration function

$$h : E_A \times M \longrightarrow S \cup \{reject\}$$

and so each e_a determines a subset of M that the arbiter will accept as valid.

There is also an *outsider* O, who has no key information. A colluding group of attackers in general use their knowledge of the system, their key information and all the previous communicated messages to construct fraudulent messages.

The system has the following stages.

Key Distribution: A triplet (e_t, e_r, e_a) of keys for the three participants T, R and A is generated and each participant securely receives his/her key. This stage may be performed by a trusted party, or through a secure distributed protocol among participants T, R, A.

Authentication: T uses his key e_t to construct an authentic message m for a source state s.

Verification: A message is acceptable by R if R accepts the message as authentic.

We note that in [11] a message was considered acceptable if it is acceptable by R and A both while in this paper, similar to [4], it is only required to be acceptable by R.

Arbitration: A dispute occurs if T sends a message and later denies it, or receiver tries to impersonate T or substitute a message that she has received. The arbiter accepts the message if it is valid under e_a. Hence when T attempts to deny a message and the receiver asks for arbitration, T looses if the message is acceptable by the arbiter. Similarly if R tries to attribute a message to T and T asks for arbitration, R looses if the message is not acceptable by the arbiter.

We assume the following types of attacks.

1. **Attack O_i:** Observing a sequence of i messages $m_1, m_2, \cdots, m_i$, constructed under the same key, opponent places a message m into the channel. He is successful if the receiver accepts m as authentic.
2. **Attack R_i:** Receiving a sequence of i messages $m_1, m_2, \cdots, m_i$, constructed under the same key, and using her key e_r, R claims that she has received a message $m \neq m_1, m_2, \cdots, m_i$. She is successful if m can be generated by the transmitter under his key e_t.
3. **Attack A_i:** Observing a sequence of i messages $m_1, m_2, \cdots, m_i$, constructed under the same key, and using a key (an arbitrating rule) e_a, the arbiter puts another message m into the channel. She is successful if the message is valid for R.
4. **Attack T:** Using his key (an encoding rule) e_t, transmitter sends a fraudulent message m' which could not be generated by e_t. He succeeds if the receiver accepts this message.
5. **Collusion Attack $\overline{RA}_i$:** Having received a sequence of i messages $m_1, m_2, \cdots, m_i$, R and A collude to cheat against T. R, in collusion with A constructs a message and claims it has been sent by the transmitter. They succeed if m can be generated by the transmitter under his key e_t.
6. **Collusion Attack $\overline{TA}$:** A and T, using the keys e_t and e_a, respectively, collude to construct a message m' which is not incident with e_t but accepted by R.

This model of A^3-codes is similar to the model in [4] with the extension of considering collusion attacks. The difference with the model in [11] is

that in [11] the success in Attacks O_i and T was defined as R and A both accepting the message while in this paper, similar to [4], only R must need to accept the message.

Let E_T, E_R and E_A be the set of transmitter's, receiver's and arbiter's keys, respectively. We assume a probability distribution, $p(e_t, e_r, e_a)$, on $E_T \times E_R \times E_A$. A three tuple (e_t, e_r, e_a) has non-zero probability only if the following properties hold.

1. a message generated by e_t is valid under e_r and e_a both
2. a message valid for e_r and e_a determines e_t that is used for its generation.

The distributions: $p(e_r, e_a), p(e_t), p(e_r)$ and $p(e_a)$ on $E_R \times E_A$, E_T, E_R and E_A, respectively, can be calculated from $p(e_t, e_r, e_a)$. We assume there is a probability distribution $p(s)$ on the set of source states S. Support of $p(e_t, e_r, e_a)$ is denoted by $E_T \circ E_R \circ E_A$ and defined by

$$E_T \circ E_R \circ E_A = \{(e_t, e_r, e_a) : p(e_t, e_r, e_a) > 0\},$$

Similarly, support of $p(e_r, e_a)$ is defined by

$$E_R \circ E_A = \{(e_r, e_a) : p(e_r, e_a) > 0\}.$$

Let M be the set of all possible messages, M^i denote the set of sequences, m^i, of i distinct messages. We will also use the following notations.

$$\begin{aligned} E_{\overline{RA}}(m^i) &= \{(e_r, e_a) \in E_R \circ E_A : m^i \text{ is valid under } e_r, e_a \} \\ E_{\overline{RA}}(e_t) &= \{(e_r, e_a) \in E_R \circ E_A : p(e_t, e_r, e_a) > 0\}. \end{aligned}$$

Probability of success in various attacks can be defined as follows.

$$\begin{aligned} P_{O_i} &= \max_{m^i \in M^i} \max_{m \in M} p(R \text{ accepts } m \mid R \text{ accepts } m^i) \\ P_{R_i} &= \max_{m^i \in M^i, e_r \in E_R} \max_{m \in M} p(T \text{ generates } m \mid T \text{ generates } m^i, e_r) \\ P_{A_i} &= \max_{m^i \in M^i, e_a \in E_A} \max_{m \in M} p(R \text{ accepts } m \mid R \text{ accepts } m^i, e_a) \\ P_T &= \max_{e_t \in E_T} \max_{m' \notin M(e_t)} p(R \text{ accepts } m' \mid e_t) \\ P_{\overline{RA}_i} &= \max_{m^i \in M^i} \max_{(e_r, e_a) \in E_R \circ E_A} \max_{m \in M} p(T \text{ generates } m \mid T \text{ generates } m^i, e_r, e_a) \\ P_{\overline{TA}} &= \max_{e_t \in E_T} \max_{e_a \in E_A} \max_{m' \in M(e_a) \setminus M(e_t)} p(R \text{ accepts } m' \mid e_t, e_a) \end{aligned}$$

3 Information-theoretic bounds

We will use the following notations throughout the paper.

$$\begin{aligned} E_X(m^i) &= \{e_x \in E_X : m^i \text{ is available for } e_x\} \\ E_X(e_y) &= \{e_x \in E_X : p(e_x, e_y) > 0\} \\ M(e_y) &= \{m \in M : m \text{ is available for } e_y\}. \end{aligned}$$

We *assume* that if a sequence of i (up to $\ell + 1$) messages is valid under the receiver's key, then it could be generated by one transmitter's key.

Theorem 3.1 to 3.6 give information-theoretic bounds on success probability in the above attacks. Proofs of these theorems use an approach similar to [4] and are omitted here.

Theorem 3.1 $P_{O_i} \geq 2^{H(E_R \mid M^{i+1}) - H(E_R \mid M^i)}$, *for any* $i \geq 0$.
Equality holds if and only if,

$$\frac{p(e_r \mid R \text{ accepts } m^i)}{p(e_r \mid R \text{ accepts } m^i, m)}$$

is independent of m^i, m *and* $e_r \in E_R(m^i, m)$ *that satisfy* $E_R(m^i, m) \neq \emptyset$.

Theorem 3.2 $P_{R_i} \geq 2^{H(E_T \mid M^{i+1}, E_R) - H(E_T \mid M^i, E_R)}$ *for any* $i \geq 0$.
Equality holds if and only if,

$$\frac{p(e_t \mid T \text{ generates } m^i, e_r)}{p(e_t \mid T \text{ generates } m^i, m, e_r)}$$

is independent of $m^i, m, e_r \in E_R(m^i, m)$ *and* $e_t \in E_T(m^i, m)$, *where* $E_R(m^i, m) \neq \emptyset$, $E_T(m^i, m) \neq \emptyset$ *and* $p(e_t, e_r) > 0$.

Theorem 3.3 $P_{A_i} \geq 2^{H(E_R \mid M^{i+1}, E_A) - H(E_R \mid M^i, E_A)}$ *for any* $i \geq 0$.
Equality holds if and only if,

$$\frac{p(e_r \mid R \text{ accepts } m^i, e_a)}{p(e_r \mid R \text{ accepts } m^i, m, e_a)}$$

is independent of $m^i, m, e_r \in E_R(m^i, m)$ *and* $e_a \in E_A(m^i, m)$, *where* $E_R(m^i, m) \neq \emptyset$, $E_A(m^i, m) \neq \emptyset$ *and* $p(e_r, e_a) > 0$.

Theorem 3.4 $P_T \geq 2^{H(E_R \mid M', E_T) - H(E_R \mid E_T)}$.
Equality holds if and only if,

$$\frac{p(e_r \mid e_t)}{p(e_r \mid R \text{ accepts } m', e_t)}$$

is independent of e_t, e_r *if* $p(e_t, e_r) > 0$ *and* $m' \notin M(e_t)$.

Theorem 3.5 $P_{\overline{RA}_i} \geq 2^{H(E_T \mid M^{i+1}, E_R, E_A) - H(E_T \mid M^i, E_R, E_A)}$ *for any* $i \geq 0$.
Equality holds if and only if

$$\frac{p(e_t \mid T \text{ generates } m^i, e_r, e_a)}{p(e_t \mid T \text{ generates } m^i, m, e_r, e_a)}$$

is independent of $m^i, m, e_t \in E_T(m^i, m)$ *and* $(e_r, e_a) \in E_{\overline{RA}}(m^i, m)$, *where* $E_T(m^i, m) \neq \emptyset$, $E_{\overline{RA}}(m^i, m) \neq \emptyset$ *and* $p(e_t, e_r, e_a) > 0$.

Theorem 3.6 $P_{\overline{TA}} \geq 2^{H(E_R \mid M', E_T, E_A) - H(E_R \mid E_T, E_A)}$.
Equality holds if and only if

$$\frac{p(e_r \mid e_t, e_a)}{p(e_r \mid R \text{ accepts } m', e_t, e_a)}$$

is independent of e_t, e_r, e_a *with* $p(e_t, e_r, e_a) > 0$ *and* $m' \in M(e_a) \setminus M(e_t)$.

Using the above bounds we have a bound on size of the message space.

Corollary 3.1 $|M| \geq P_{O_0}^{-1} P_{\overline{RA}_0}^{-1} 2^{H(S)}$.
Equality holds if and only if P_{O_0} *and* $P_{\overline{RA}_0}$ *meet their lower bounds.*

Proof: From Theorem 3.1 and 3.5 we know that

$$\begin{aligned}
P_{O_0} P_{\overline{RA}_0} &\geq 2^{H(E_R,E_A|M) - H(E_R,E_A) + H(E_T|M,E_R,E_A) - H(E_T|E_R,E_A)} \\
&= 2^{H(E_R,E_A,M) - H(M) - H(E_R,E_A) + H(E_T,E_R,E_A,M) - H(E_R,E_A,M) - H(E_T,E_R,E_A) + H(E_R,E_A)} \\
&= 2^{-H(M) + H(M|E_T,E_R,E_A)} \\
&= 2^{-H(M) + H(M|E_T)} \\
&= 2^{-H(M) + H(S)}
\end{aligned}$$

The corollary is followed.

□

From Corollary 3.1 we know that when the probability distribution on S is uniform we have, $|M| \geq P_{O_0}^{-1} P_{\overline{RA}_0}^{-1} |S|$. Corollary 3.1 also tells us the size of message space is minimised when P_{O_0} and $P_{\overline{RA}_0}$ meet their bounds.

4 Combinatorial bounds on the size of key spaces

In this subsection we will derive the lower bounds on each participant's key space.

Theorem 4.1 $|E_T| \geq (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{R_i})^{-1}(\prod_{i=0}^{\ell} P_{\overline{RA}_i})^{-1}$.
Equality holds if and only if

1. $H(E_T \mid M^{\ell+1}, E_R, E_A) = 0$,
2. $H(E_T \mid M^{\ell+1}, E_R) = H(E_T \mid E_R, E_A)$,
3. $H(E_R \mid M^{\ell+1}) = H(E_R \mid E_T)$, *and*
4. *the probability distribution on* E_T *is uniform.*

Proof: Using theorems 3.1, 3.2 and 3.5 we have

$$
\begin{aligned}
& (\prod_{i=0}^{\ell} P_{O_i})(\prod_{i=0}^{\ell} P_{R_i})(\prod_{i=0}^{\ell} P_{\overline{RA}_i}) \\
\geq\ & 2^{H(E_R \mid M^{\ell+1}) - H(E_R) + H(E_T \mid M^{\ell+1}, E_R) - H(E_T \mid E_R) + H(E_T \mid M^{\ell+1}, E_R, E_A) - H(E_T \mid E_R, E_A)} \\
=\ & 2^{H(E_R \mid M^{\ell+1}) + H(E_T \mid M^{\ell+1}, E_R) + H(E_T \mid M^{\ell+1}, E_R, E_A) - H(E_R \mid E_T) - H(E_T) - H(E_T \mid E_R, E_A)}
\end{aligned}
$$

So

$$
\begin{aligned}
|E_T| \ &\geq\ 2^{H(E_T)} \\
&\geq\ 2^{H(E_R \mid M^{\ell+1}) + H(E_T \mid M^{\ell+1}, E_R) + H(E_T \mid M^{\ell+1}, E_R, E_A) - H(E_R \mid E_T) - H(E_T \mid E_R, E_A)} \\
&\quad \cdot (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{R_i})^{-1}(\prod_{i=0}^{\ell} P_{\overline{RA}_i})^{-1}
\end{aligned}
$$

Noting that $H(E_R \mid M^{\ell+1}) - H(E_R \mid E_T) \geq 0$, $H(E_T \mid M^{\ell+1}, E_R) - H(E_T \mid E_R, E_A) \geq 0$, then

$$
|E_T| \geq (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{R_i})^{-1}(\prod_{i=0}^{\ell} P_{\overline{RA}_i})^{-1}.
$$

Equality holds if and only if (i) $H(E_T \mid M^{\ell+1}, E_R, E_A) = 0$, (ii) $H(E_R \mid M^{\ell+1}) = H(E_R \mid E_T)$, (iii) $H(E_T \mid M^{\ell+1}, E_R) = H(E_T \mid E_R, E_A)$, and (iv) $|E_T| = 2^{H(E_T)}$. Clearly (iv) is equivalent to the probability distribution on E_T is uniform. The theorem is proved.

□

Theorem 4.2 $|E_R| \geq (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{A_i})^{-1}(P_{\overline{TA}})^{-1}$.
Equality holds if and only if,

1. $H(E_R \mid M^{\ell+1}) = H(E_R \mid E_A)$,
2. $H(E_R \mid M^{\ell+1}, E_A) = H(E_R \mid E_T, E_A)$,
3. $H(E_R \mid M', E_T, E_A) = 0$, *and*
4. *probability distribution on* E_R *is uniform.*

Proof: Using theorems 3.1, 3.4 and 3.6 we have

$$\begin{aligned} & (\prod_{i=0}^{\ell} P_{O_i})(\prod_{i=0}^{\ell} P_{A_i})(P_{\overline{TA}}) \\ \geq\ & 2^{H(E_R \mid M^{\ell+1}) - H(E_R) + H(E_R \mid M^{\ell+1}, E_A) - H(E_R \mid E_A) + H(E_R \mid M', E_T, E_A) - H(E_R \mid E_T, E_A)} \end{aligned}$$

So

$$\begin{aligned} & |E_R| \geq 2^{H(E_R)} \\ \geq\ & 2^{H(E_R \mid M^{\ell+1}) + H(E_R \mid M^{\ell+1}, E_A) + H(E_R \mid M', E_T, E_A) - H(E_R \mid E_A) - H(E_R \mid E_T, E_A)} \\ & \cdot (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{A_i})^{-1}(P_{\overline{TA}})^{-1}. \end{aligned}$$

Since $H(E_R \mid M^{\ell+1}) - H(E_R \mid E_A) \geq 0$, $H(E_R \mid M^{\ell+1}, E_A) - H(E_R \mid E_T, E_A) \geq 0$, then

$$|E_R| \geq (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{A_i})^{-1}(P_{\overline{TA}})^{-1}.$$

Equality holds if and only if (i) $H(E_R \mid M^{\ell+1}) - H(E_R \mid E_A) = 0$, (ii) $H(E_R \mid M^{\ell+1}, E_A) - H(E_R \mid E_T, E_A) = 0$, (iii) $H(E_R \mid M', E_T, E_A) = 0$, and (iv) $|E_R| = 2^{H(E_R)}$. The theorem is proved.

□

To obtain the value of $|E_A|$ we first prove the following lemma.

Lemma 4.1 *Suppose all six attacks achieve their lower bounds, and* $|E_T|, |E_R|$ *also achieve their lower bounds. Then we have*

$$2^{H(E_T, E_R \mid E_A)} = (\prod_{i=0}^{\ell} P_{A_i})^{-1}(\prod_{i=0}^{\ell} P_{\overline{RA}_i})^{-1} P_{\overline{TA}}^{-1} \quad \textit{and} \tag{1}$$

$$2^{H(E_A \mid E_T)} = 2^{H(E_R \mid M', E_T) + H(E_A \mid E_T, E_R)}(P_T)^{-1}(P_{\overline{TA}}) \tag{2}$$

Proof: Using theorems 4.1 and 4.2 we have

$$
\begin{aligned}
& (\prod_{i=0}^{\ell} P_{A_i})(\prod_{i=0}^{\ell} P_{\overline{RA}_i})P_{\overline{TA}} \\
= \; & 2^{H(E_R \mid M^{\ell+1}, E_A) - H(E_R \mid E_A) + H(E_T \mid M^{\ell+1}, E_R, E_A) - H(E_T \mid E_R, E_A) + \\
& H(E_R \mid M', E_T, E_A) - H(E_R \mid E_T, E_A)} \\
= \; & 2^{H(E_R \mid E_T, E_A) - H(E_R \mid E_A) - H(E_T \mid E_R, E_A) - H(E_R \mid E_T, E_A)} \\
= \; & 2^{-H(E_T, E_R \mid E_A)}.
\end{aligned}
$$

Equality (1) is proved.

Using theorems 3.4, 3.6 and 4.2 we have

$$
\begin{aligned}
(P_T)(P_{\overline{TA}})^{-1} &\geq 2^{H(E_R \mid M', E_T) - H(E_R \mid E_T) - H(E_R \mid M', E_T, E_A) + H(E_R \mid E_T, E_A)} \\
&= 2^{H(E_R \mid M', E_T) - H(E_A \mid E_T) + H(E_A \mid E_T, E_R)}
\end{aligned}
$$

So

$$
2^{H(E_A \mid E_T)} = 2^{H(E_R \mid M', E_T) + H(E_A \mid E_T, E_R)} (P_T)^{-1} (P_{\overline{TA}}).
$$

Equation (2) is proved.

□

Theorem 4.3 *Suppose all six attacks achieve their lower bounds, and* $|E_T|, |E_R|$ *also achieve their lower bounds. Then we have*

$$
|E_A| \geq (P_T)^{-1} (\prod_{i=0}^{\ell} P_{O_i})^{-1} (\prod_{i=0}^{\ell} P_{R_i})^{-1} (\prod_{i=0}^{\ell} P_{A_i}) P_{\overline{TA}}.
$$

Equality holds if and only if

1. $H(E_R \mid M', E_T) = 0$,
2. $H(E_A \mid E_T, E_R) = 0$, *and*
3. *the probability distribution on* E_A *is uniform.*

Proof: Using above results we have

$$
\begin{aligned}
2^{H(E_A)} &= 2^{H(E_R \mid E_T, E_A)} \cdot 2^{H(E_A \mid E_T)} \cdot 2^{H(E_T)} \cdot 2^{-H(E_T, E_R \mid E_A)} \\
&= (P_{\overline{TA}})^{-1} \cdot 2^{H(E_R \mid M', E_T) + H(E_A \mid E_T, E_R)} (P_T)^{-1} (P_{\overline{TA}}) \cdot
\end{aligned}
$$

$$
\begin{aligned}
& (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{R_i})^{-1}(\prod_{i=0}^{\ell} P_{\overline{RA}_i})^{-1} \cdot (\prod_{i=0}^{\ell} P_{A_i})(\prod_{i=0}^{\ell} P_{\overline{RA}_i})P_{\overline{TA}} \\
= \; & 2^{H(E_R \mid M', E_T)+H(E_A \mid E_T, E_R)}(P_T)^{-1}(\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{R_i})^{-1}(\prod_{i=0}^{\ell} P_{A_i})P_{\overline{TA}} \\
\geq \; & (P_T)^{-1}(\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{R_i})^{-1}(\prod_{i=0}^{\ell} P_{A_i})P_{\overline{TA}}
\end{aligned}
$$

Equality holds if and only if $H(E_R \mid M', E_T) = H(E_A \mid E_T, E_R) = 0$. The theorem is proved.

□

5 ℓ-optimal codes

An A^3-code is called *ℓ-optimal* if

(*i*) $P_{O_i}, P_{R_i}, P_{A_i}, P_T, P_{\overline{RA}_i}, P_{\overline{TA}}$ achieve their lower bounds, for $0 \leq i \leq \ell$; and

(*ii*) $|E_T|, |E_R|$ and $|E_A|$ achieve their lower bounds.

Theorem 4.3 shows that $H(E_A \mid E_T, E_R) = 0$ in an ℓ-optimal A^3-code. It means that the arbiter's key e_a is determined uniquely by pair of (e_t, e_r). We have seen from above subsection that in an ℓ-optimal A^3-code, the probability distributions on E_T, E_R, E_A are uniform. Further we *assume* that

(*iii*) the joint probability distributions on $E_T \circ E_R, E_R \circ E_A, E_T \circ E_R \circ E_A$ are uniform.

In the rest part of this paper, we always use this assumption without claiming. Under this assumption together with theorem 3.1 to theorem 3.6, the following theorem can be easily proved.

Theorem 5.1 *In an ℓ-optimal A^3-code the probabilities of attacks can be rewritten as follows,*

$$
\begin{aligned}
P_{O_i} &= \frac{|E_R(m^i, m)|}{|E_R(m^i)|}, \\
P_{R_i} &= \frac{|E_T(m^{i+1}) \cap E_T(e_r)|}{|E_T(m^i) \cap E_T(e_r)|},
\end{aligned}
$$

$$
\begin{aligned}
P_{A_i} &= \frac{|E_R(m^{i+1}) \cap E_R(e_a)|}{|E_R(m^i) \cap E_R(e_a)|}, \\
P_T &= p(e_r \mid e_l), \\
P_{\overline{RA_i}} &= \frac{|E_T(m^i, m) \cap E_T(e_r, e_a)|}{|E_T(m^i) \cap E_T(e_r, e_a)|}, \\
P_{\overline{TA}} &= p(e_r \mid e_l, e_a).
\end{aligned}
$$

Let $\mathcal{X}$ and $\mathcal{Y}$ be two sets and $p(x, y)$ denote a joint probability distribution on $\mathcal{X} \times \mathcal{Y}$. For $y \in \mathcal{Y}$, denote by $\mathcal{X}_y$ the set $\{x \in \mathcal{X} : p(x, y) > 0\}$.

Lemma 5.1 *Assume $p(x, y)$ and the marginal distributions on $\mathcal{X}$ and $\mathcal{Y}$ are uniform. If $|\mathcal{X}_y| < |\mathcal{X}|$ then there is a partition on the set $\mathcal{X}$ given by: $\mathcal{X} = \cup_y \mathcal{X}_y$ where all subsets $\mathcal{X}_y$ are of equal size.*

Proof: Consider a graph with vertex set given by $\mathcal{X} \cup \mathcal{Y}$ and an edge between x and y if $p(x, y) \neq 0$. It is easy to see that we have a bipartite graph where the number of edges incident with a node x in $\mathcal{X}$ is $|\mathcal{Y}_x|$, the number of edges incident with a node y in $\mathcal{Y}$ is $|\mathcal{X}_y|$ and we have $|\mathcal{X}| \times |\mathcal{Y}_x| = |\mathcal{Y}| \times |\mathcal{X}_y|$.

For $y^{(1)} \in \mathcal{Y}$, let $\mathcal{X}_1 = \mathcal{X}_{y^{(1)}}$, and

$$\mathcal{Y}_{\mathcal{X}_1} = \{y' : p(x, y') > 0 \text{ for some } x \in \mathcal{X}_1\}.$$

Then $\mathcal{Y}_{\mathcal{X}_1} \neq \mathcal{Y}$, as otherwise $|\mathcal{X}_1| \times |\mathcal{Y}_x| = |\mathcal{Y}| \times |\mathcal{X}_y|$ and so $|\mathcal{X}| = |\mathcal{X}_1|$ which contradicts the assumption.

Choose $y^{(2)} \in \mathcal{Y} \setminus \mathcal{Y}_{\mathcal{X}_1}$ and let $\mathcal{X}_2 = \mathcal{X}_{y^{(2)}}$. Then $\mathcal{X}_1 \cap \mathcal{X}_2 = \emptyset$.

Suppose we have chosen $\mathcal{X}_1 = \mathcal{X}_{y^{(1)}}, \cdots, \mathcal{X}_{d-1} = \mathcal{X}_{y^{(d-1)}}$ as above. If there exists $y' \in \mathcal{Y}$ such that $p(x, y') > 0$ and

$$y' \notin \{y : p(x, y) > 0 \text{ for some } x \in \mathcal{X}_1 \cup \cdots \cup \mathcal{X}_{d-1}\},$$

then we choose

$$y^{(d)} \in \mathcal{Y} \setminus (\mathcal{Y}_{\mathcal{X}_1} \cup \mathcal{Y}_{\mathcal{X}_2} \cup \cdots \cup \mathcal{Y}_{\mathcal{X}_{d-1}}),$$

and let $\mathcal{X}_d = \mathcal{X}_{y^{(d)}}$. Then $\mathcal{X}_1 \cap \mathcal{X}_2 \cap \cdots \cap \mathcal{X}_d = \emptyset$. Repeat above steps until,

$$\{y' : p(x, y') > 0 \text{ for some } x \in \mathcal{X}_1 \cup \cdots \cup \mathcal{X}_{d-1}\} = \mathcal{Y}.$$

Now we have a partition of $\mathcal{X} = \cup_i \mathcal{X}_i$, in which all $\mathcal{X}_i$ have the same size $p(x \mid y)^{-1}$.

□

Theorem 5.2 *In an ℓ-optimal A^3-code, the following conditions are satisfied:*

1. *If $E_T(m^i) \cap E_T(e_r, e_a) \neq \emptyset$, then $|E_T(m^i) \cap E_T(e_r, e_a)|$ is independent of m^i, e_r and e_a.*
2. *If $E_T(m^i) \cap E_T(e_r) \neq \emptyset$, then $|E_T(m^i) \cap E_T(e_r)|$ is independent of m^i, e_r.*
3. *If $E_R(m^i) \cap E_R(e_a) \neq \emptyset$, then $|E_R(m^i) \cap E_R(e_a)|$ is independent of m^i and e_a.*
4. *If $E_T(m^i) \neq \emptyset$, then $|E_T(m^i)|$ is independent of m^i.*
5. *If $E_R(m^i) \neq \emptyset$, then $|E_R(m^i)|$ is independent of m^i.*

Proof: The first three statements and the fifth are true because of theorem 5.1. Applying lemma 5.1 to $E_T \circ E_R \circ E_A, E_R \circ E_A$, we obtain a partition of $E_T = \cup_{(e_r,e_a)} E_T(e_r, e_a)$. So $|E_T(m^i)| = \sum_{(e_r,e_a)} |E_T(m^i) \cap E_T(e_r, e_a)|$ does not depend on m^i.

□

6 Cartesian A^3-codes

An A^3-code is *Cartesian* if for any message m, there is a unique source state s which can be encoded to m. This means that in a Cartesian code M can be partitioned into $M(s_1), M(s_2), \cdots$ such that all messages $m \in M(s_j)$ are obtained from encoding s_j. Formally, for $s \in S$, define

$$M(s) = \{m : s \text{ can be encoded to } m \text{ by some } e_t \in E_T\}.$$

Then by theorem 5.2, part 4, we know that $|M(s)| = \frac{|E_T|}{|E_T(m)|}$ is a constant and

$$\frac{|M|}{|S|} = |M(s)|, \ \forall s \in S$$

Define,

$$M(s, e_r) \ = \ \{m \in M : m \text{ is accepted as } s \text{ by } e_r\}.$$

Theorem 6.1 $|M(s, e_r)|$ *is independent of* s, e_r.

Proof: For given e_a and $e_r \in E_R(e_a)$, it is clear that

$$\sum_{m \in M(s,e_r)} p(R \text{ accepts } m \,|\, e_a) = 1.$$

We know in optimal codes, $P_{A_0} = p(R \text{ accepts } m \,|\, e_a)$ which is independent of m, e_a. So $|M(s,e_r)| = P_{A_0}^{-1}$ is independent of s and e_r.

□

The following theorem shows that success probabilities in higher order attacks are the same as those of impersonation attacks, and having access to extra message does not improve success chance of the attackers.

Theorem 6.2 *In an ℓ-optimal Cartesian A^3-code,*

1. $P_{O_0} = P_{O_1} = \cdots = P_{O_\ell}$;
2. $P_{R_0} = P_{R_1} = \cdots = P_{R_\ell}$;
3. $P_{A_0} = P_{A_1} = \cdots = P_{A_\ell}$;
4. $P_{\overline{RA}_0} = P_{\overline{RA}_1} = \cdots = P_{\overline{RA}_\ell}$.

Proof: From theorems 5.1 and 6.1 we know that,

$$P_{O_i} = \frac{|E_R(m^{i+1})|}{|E_R(m^i)|} \text{ and } P_{O_0} = \frac{|E_R(m)|}{|E_R|} = \frac{|M(s,e_r)|}{|M(s)|}.$$

We need to show that for all i,

$$\frac{|E_R(m^{i+1})|}{|E_R(m^i)|} = \frac{|M(s,e_r)|}{|M(s)|}.$$

It is true when $i = 0$. Suppose for some $i \geq 0$,

$$\frac{|E_R(m^i)|}{|E_R(m^{i-1})|} = \frac{|M(s,e_r)|}{|M(s)|}.$$

Consider the sequence of messages $m^i = (m_1, m_2, \cdots, m_i)$, from the sets $M(s_1), M(s_2), \cdots, M(s_i)$, respectively, and let $s \notin \{s_1, s_2, \cdots, s_i\}$. Consider the sum $\sum_{m \in M(s)} |E_R(m^i, m)|$. An $e_r \in E_R(m^i)$ in this sum is counted $|M(s,e_r)|$ times which by theorem 6.1 is independent of s and e_r and so,

$$\sum_{m \in M(s)} |E_R(m^i, m)| = |E_R(m^i)| \times |M(s,e_r)|.$$

Using theorem 5.2, part 5, we know that $|E_R(m^i, m)|, i < \ell$, is constant and we have

$$|E_R(m^i, m)| \times |M(s)| = |E_R(m^i)| \times |M(s, e_r)|,$$

and so the first statement is proved by induction.

The rest can be proved in a similar way.

□

7 Combinatorial designs and A^3-codes

In the following we describe combinatorial structure of E_T and E_R. First we do a few calculations in the following lemmas.

Lemma 7.1 $|E_R(e_a)| = P_{A_0}^{-\ell-1} P_{\overline{TA}}^{-1}$ *holds in an ℓ-optimal Cartesian A^3-code.*

Proof:

$$\begin{aligned} |E_R(e_a)| &= \frac{|E_T \circ E_R \circ E_A|}{|E_T(e_r, e_a)| \times |E_A|} = \frac{|E_T \circ E_R(e_a)|}{|E_T(e_r, e_a)|} \\ &= (\prod_{i=0}^{\ell} P_{A_i})^{-1} (\prod_{i=0}^{\ell} P_{\overline{RA}_i})^{-1} P_{\overline{TA}}^{-1} (\prod_{i=0}^{\ell} P_{\overline{RA}_i}) = P_{A_0}^{-\ell-1} P_{\overline{TA}}^{-1}. \end{aligned}$$

□

Lemma 7.2 $|E_R(m^{\ell+1})| = |E_R(e_t)|$ *holds in an ℓ-optimal A^3-code.*

Proof: From theorem 4.1 we know that $H(E_R \,|\, M^{\ell+1}) = H(E_R \,|\, E_T) = \log |E_R(e_t)|$. Instead of values of P_{O_i}, P_{R_i} and $P_{\overline{RA}_i}$ in theorem 5.1 to calculate E_T as in theorem 4.1 we get

$$\begin{aligned} |E_T| &= (\prod_{i=0}^{\ell} P_{O_i})^{-1} (\prod_{i=0}^{\ell} P_{R_i})^{-1} (\prod_{i=0}^{\ell} P_{\overline{RA}_i})^{-1} \\ &= \frac{|E_R|}{|E_R(m^{\ell+1})|} \cdot \frac{|E_T(e_r)|}{|E_T(m^{\ell+1}) \cap E_T(e_r)|} \cdot \frac{|E_T(e_r, e_a)|}{|E_T(m^{\ell+1}) \cap E_T(e_r, e_a)|} \\ &= \frac{|E_R|}{|E_R(m^{\ell+1})|} \cdot \frac{|E_T(e_r)|}{|E_T(e_r, e_a)|} \cdot |E_T(e_r, e_a)| \quad \text{(by theorem 4.1)} \\ &= \frac{|E_T| \cdot |E_R(e_t)|}{|E_R(m^{\ell+1})|}. \end{aligned}$$

The lemma is followed.

□

Lemma 7.3 *If $E_T(m^i) \neq \emptyset$, then $|E_T(m^i)| = (P_{O_0})^{-\ell+i-1}(P_{R_0})^{-\ell+i-1}(P_{\overline{RA_0}})^{-\ell-1}$ in an ℓ-optimal Cartesian A^3-code, for $1 \leq i \leq \ell+1$.*

Proof: Based on above results, $|E_T(m^i)|$ can be calculated as follows.

$$\begin{aligned}
|E_T(m^i)| &= \frac{|E_R(m^i)| \cdot |E_T(m^i) \cap E_T(e_r)|}{|E_R(e_t)|} \\
&= \frac{|E_R(m^i)| \cdot |E_T(m^i) \cap E_T(e_r)|}{|E_R(m^{\ell+1})|} \quad \text{(by lemma 7.2)} \\
&= (P_{O_0})^{-\ell+i-1}(P_{R_0})^{-\ell+i-1} \cdot |E_T(e_r, e_a)| \\
&\qquad \text{(by theorems 4.1, 5.1 and 6.2)} \\
&= (P_{O_0})^{-\ell+i-1}(P_{R_0})^{-\ell+i-1}(P_{\overline{RA_0}})^{-\ell-1}|E_T(m^{\ell+1})|.
\end{aligned}$$

When $i = \ell+1$, it becomes

$$|E_T(m^{\ell+1})| = (P_{O_0})^0(P_{R_0})^0(P_{\overline{RA_0}})^{-\ell-1}|E_T(m^{\ell+1})| = (P_{\overline{RA_0}})^{-\ell-1}|E_T(m^{\ell+1})|$$

so $(P_{\overline{RA_0}})^{-\ell-1} = 1$. Therefore we obtain

$$|E_T(m^i)| = (P_{O_0})^{-\ell+i-1}(P_{R_0})^{-\ell+i-1}, \quad \text{for } i \leq \ell+1.$$

□

7.1 Combinatorial designs

To describe the structures of E_T and E_R we first give definitions of combinatorial designs used later.

Definition 7.1 *A block design is a pair $(V, \mathcal{B})$, where V is a set of v points and $\mathcal{B}$ is a family of k-subsets (called blocks) of V. A block design is called t-design if any t-subset of V occurs in exactly λ blocks.*

Definition 7.2 *([7]) A* partially balanced t-design *is a block design $(V, \mathcal{B})$ in which any t-subset of V either occurs in exactly λ blocks or does not occur in any block.*

We denote this design by $t-(v,k;\{\lambda,0\})$-design.

Definition 7.3 *([6]) A block design $(V,\mathcal{B})$ is called α-resolvable if the block family $\mathcal{B}$ can be partitioned into classes $C_1,C_2,\cdots,C_n$ with the property that in each class, every point occurs in exactly α blocks.*

We will be interested in α-resolvable design with the following properties: There is a positive integer $\ell < n$ such that

(P1) Any collection of i blocks from i different classes either intersect in μ_i points or do not intersect, $1 \le i \le \ell+1$;

(P2) For any $\ell+1$ blocks $B_{j_1},B_{j_2},\cdots,B_{j_{\ell+1}}$ from different classes $C_{j_1},C_{j_2},\cdots,C_{j_{\ell+1}}$ and any $u(\neq j_1,j_2,\cdots,j_{\ell+1})$, there exists a unique block $B_u \in C_u$ such that

$$B_{j_1}\cap\cdots\cap B_{j_{\ell+1}} = B_{j_1}\cap\cdots\cap B_{j_{\ell+1}}\cap B_u$$

if $B_{j_1}\cap\cdots\cap B_{j_{\ell+1}} \neq \emptyset$. Furthermore, for any $B \in C_u\backslash\{B_u\}$,

$$|B_{j_1}\cap\cdots\cap B_{j_{\ell+1}}\cap B| = 1.$$

7.2 E_T

Theorem 7.1 *In an ℓ-optimal Cartesian A^3-code, (M,E_T) is a strong partially balanced, resolvable $(\ell+1)-(|M|,|S|;\{\lambda,0\})$-design. The block set is partitioned into n' classes, $C_1,C_2,\cdots,C_{n'}$, and has following parameters:*

$\lambda = 1$,
$\lambda_i = (P_{O_0})^{-\ell+i-1}(P_{R_0})^{-\ell+i-1}$, $1 \le i \le \ell$,
$\lambda_i' = (P_{\overline{RA}_0})^{-\ell+i-1}$, $1 \le i \le \ell$.

Proof: Since $|E_T(m^i)|$ is either 0 or a non-zero constant for all m^i and all $i, 1 < i \le \ell+1$, also $|E_T(m)|$ is a non-zero constant for all $m \in M$. So (M,E_T) is a strong $(\ell+1)-(|M|,|S|;\{\lambda,0\})$-design with parameters $\lambda_i = |E_T(m^i)|$, for $1 \le i \le \ell+1$. Lemma 7.3 gives the value of $|E_T(m^i)|$.

We have seen that E_T has a partition $E_T = \cup_{(e_r,e_a)}E_T(e_r,e_a)$. Clearly, for each pair (e_r,e_a), $(M,E_T(e_r,e_a))$ is still strong $(\ell+1)-(|M|,|S|;\{\lambda,0\})$-design with parameters $\lambda_i' = |E_T(m^i)\cap E_T(e_r,e_a)| = (P_{\overline{RA}_0})^{-\ell+i-1}$.

□

7.3 E_R

The following lemma 7.4 has been proved (lemma 5.8, [12]) in an A^2-code. Based on lemmas 7.2 and 7.3, it is easy to see that lemma 7.4 is still true in optimal A^3-code, and the proof is the same. We omit the proof here.

Lemma 7.4 *For a sequence of $\ell+1$ messages $m^{\ell+1}$ from $M_{i_1}, M_{i_2}, \cdots, M_{i_{\ell+1}}$ with $E_R(m^{\ell+1}) \neq \emptyset$, and $u \neq i_j$, $j = 1, 2, \cdots, \ell+1$ with $\ell+1 < |S|$, there exists a unique message $m_u \in M_u$ such that $E_R(m^{\ell+1}) = E_R(m^{\ell+1}, m_u)$.*

We have known that $|E_R(m)|$ is a constant for all $m \in M$. Therefore $(E_R, \{E_R(m) : m \in M\})$ forms a block design. For this block design we have the following theorem.

Theorem 7.2 *In an ℓ-optimal Cartesian A^3-code, design $(E_R, \{E_R(m) : m \in M\})$ is α-resolvable design with properties (P1) and (P2). It has parameters:*

$\alpha^{(R)} = (P_{A_0})^{-1}$;

$\mu_i^{(R)} = (P_{O_0})^{-\ell+i-1}(P_{A_0})^{-\ell-1}(P_{\overline{TA}})^{-1}$, $1 \leq i \leq \ell+1$.

Proof: Using theorem 6.1, we know that $(E_R, \{E_R(m) : m \in M\})$ is an α-resolvable design with $|S|$ classes and $\alpha^{(R)} = |M(s, e_r)| = P_{A_0}^{-1}$. From theorem 5.1 $\mu_i^{(R)} = |E_R(m^i)| = \prod_{j=0}^{i-1} P_{O_j} |E_R| = (P_{O_0})^{-\ell+i-1}(P_{A_0})^{-\ell-1}(P_{\overline{TA}})^{-1}$. So the design $(E_R, \{E_R(m) : m \in M\})$ has property (P1). Lemma 7.4 shows that (P2) is satisfied. The theorem is proved.

□

8 Conclusion

In this paper we introduced collusion attacks in A^3-codes, obtained information theoretic and combinatorial bounds on security and efficiency parameters of the codes, defined optimal codes and finally derived combinatorial structure of optimal Cartesian codes. Our study of the optimal A^3-codes is limited to Cartesian codes. Combinatorial structure of optimal A^3-codes in the general case is an open problem.

References

[1] E. F. Brickell and D. R. Stinson. Authentication codes with multiple arbiters. In *Advances in Cryptology - EUROCRYPT'88, Lecture Notes in Computer Science*, volume 330, pages 51–55. Springer-Verlag, Berlin, Heidelberg, New York, 1988.

[2] Y. Desmedt, Y. Frankel, and M. Yung. Multi-receiver/multi-sender network security: efficient authenticated multicast/feedback. In *IEEE Infocom*, pages 2045–2054, 1992.

[3] Y. Desmedt and M. Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks. In *Advances in Cryptology - CRYPTO'90, Lecture Notes in Computer Science*, volume 537, pages 177–188. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[4] T. Johansson. Further results on asymmetric authentication schemes. *Information and Computation*, 151:100–133, 1999.

[5] K. Kurosawa and S. Obana. Combinatorial bounds on authentication codes with arbitration. *Designs, Codes and Cryptography*, 22:265–281, 2001.

[6] S. Obana and K. Kurosawa. A^2-code=affine resolvable + BIBD. In *Proc. of ICICS, Lecture Notes in Computer Science,*, volume 1334, pages 118–129. Springer-Verlag, Berlin, Heidelberg, New York, 1997.

[7] D. Pei. Information-theoretic bounds for authentication codes and block designs. *Journal of Cryptology*, 8:177–188, 1995.

[8] G. J. Simmons. Authentication theory/coding theory. In *Advances in Cryptology - CRYPTO'84, Lecture Notes in Computer Science*, volume 196, pages 411–432. Springer-Verlag, Berlin, Heidelberg, New York, 1985.

[9] G. J. Simmons. A cartesian construction for unconditionally secure authentication codes that permit arbitration. *Journal of Cryptology*, 2:77–104, 1990.

[10] R. Taylor. Near optimal unconditionally secure authentication. In *Advances in Cryptology - EUROCRYPT'94, Lecture Notes in Computer*

Science, volume 950, pages 244–253. Springer-Verlag, Berlin, Heidelberg, New York, 1994.

[11] Y. Wang and R. Safavi-Naini. A^3-code under collusion attacks. In *Advances in Cryptology - ASIACRYPT'99, Lecture Notes in Computer Science*, volume 1716, pages 390–398. Springer-Verlag, Berlin, Heidelberg, New York, 1999.

[12] Y. Wang, R. Safavi-Naini, and D. Pei. Combinatorial characterisation of ℓ-optimal authentication codes with arbitration. *Journal of Combinatorial Mathematics and Combinatorial Computing*, Vol. 37:205–224, 2001.