Combinatorial Characterisation of ℓ-Optimal Authentication Codes with Arbitration

Yejing Wang, Reihaneh Safavi-Naini
School of IT and CS, University of Wollongong, Northfields Ave.,
Wollongong 2522, Australia
email: [ywl7,rei]@uow.edu.au
Dingyi Pei
Graduate School at Beijing of USTC, Beijing 100039, China
email: dypei@sun.ihep.ac.cn

January 25, 2001

Abstract

We study combinatorial structure of ℓ-optimal A^2-codes that offer the best protection for spoofing of order up to ℓ and require the least number of keys for the transmitter and the receiver. We prove that for such codes the transmitter's encoding matrix is a strong partially balanced resolvable design, and the receiver's verification matrix corresponds to an α-resolvable design with special properties.

1 Introduction

In a traditional authentication code (A-code) there are three participants: a *transmitter*, a *receiver* and an *opponent*. The transmitter and receiver are trusted. The opponent attempts to *impersonate* the transmitter by injecting a fraudulent message into the channel, or to *substitute* a message sent to the receiver with one of his own making. Simmons [15] extended this model by removing the assumption of trustworthiness of the transmitter and the receiver and included possible attacks from them. He introduced a fourth participant, called the *arbiter*, who is trusted and arbitrates if there is a dispute between the transmitter and the receiver. This is called an*authentication code with arbiter* (A^2-code). The model and constructions for A^2-code were further studied by Johansson [5], Desmedt at al [2] and Kurosawa [8].

In this paper we study the combinatorial structure of ℓ-optimal A^2-codes. These are codes that have the best protection for spoofing of order up to ℓ and have the least number of keys. Similar studies for traditional A-codes were reported in [10] and [17]. The paper is organized as follows. In section 2 we introduce the model and in section 3 derive information-theoretic bounds for spoofing of order i. We also obtain necessary and sufficient conditions for A^2-codes that achieve the bounds with equality. In section 4 we prove combinatorial lower bounds on the size of transmitter's and receiver's key spaces and derive necessary and sufficient conditions for achieving the bounds with equality. In section 5, we study the combinatorial structure of the transmitter's encoding matrix and receiver's verification matrix, and establish the relationship between optimal codes and some known classes of designs.

2 Definitions and Notations

An A^2-code is an asymmetric authentication system defined by two sets of functions: a set of encoding functions used by transmitter to generate an *authenticated message*, and a set of verification functions used by the receiver to *verify* authenticity of a received message. The set of encoding functions is indexed by the *transmitter's key*, e_t, and the set of verification functions is indexed by the *receiver's key*, e_r. The transmitter uses his *secret key*, $e_t \in E_T$, to select an *encoding function* f, and encode a *source state* $s \in S$, to obtain an *authenticated message*, $m \in M$, that is sent to the receiver.

$$f : E_T \times S \to M$$

The receiver uses his *secret key*, $e_r \in E_R$, to determine the *verification function* g to verify authenticity of the received message,

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

Decoding may result in acceptance of the message as a particular source state, or complete rejection of it and declaring it fraudulent.

We assume a probability distribution on S and one on $E_T \times E_R$, denoted by $p(s)$ and $p(e_t, e_r)$ respectively. Using $p(e_t, e_r)$ we can calculate the probability distribution of E_T and E_R, denoted by $p(e_t)$ and $p(e_r)$, respectively. The keys for transmitter and receiver are chosen such that if $f(e_t, s) = m$ and $p(e_t, e_r) > 0$, then $g(e_r, m) = s$ for all $s \in S$. Further, if $g(e_r, m_1) = s_1, g(e_r, m_2) = s_2, \cdots, g(e_r, m_i) = s_i$, then there is a e_t such that $f(e_t, s_1) = m_1, \cdots, f(e_t, s_i) = m_i$ and $p(e_t, e_r) > 0$. Key generation for the system can be coordinated by the arbiter in a number of ways. For example, the transmitter may select his key, e_t, securely forward it to the arbiter who will choose a key e_r with the required properties and securely forward it to the receiver. Key generation process can also be started by the receiver, who will send his chosen key to the arbiter. Arbiter will choose a secret key for the transmitter and secretly deliver it to him. Finally, keys can be generated by the arbiter and delivered to the transmitter and receiver. In all cases the arbiter will end up knowing both transmitter and receiver keys.

The collection of encoding functions define an *encoding matrix* where the rows are labelled by $e_t \in E_T$, columns are labelled by $s \in S$ and the (e_t, s) element is $m = f(e_t, s) \in M$. The collection of verification functions define a *verification matrix* where rows are labelled by e_r, columns are labelled by $m \in M$, and the (e_r, m) element is $s \in S$ or '-' if $g(e_r, m) = s$ or '-', respectively, and '-' means *reject*. We use the following notations.

S^i set of sequences of i source states $(s_1, s_2, \cdots, s_i)$, where s_j's are pairwise distinct;

M^i set of sequences of i messages $(m_1, m_2, \cdots, m_i)$, where m_j's are pairwise distinct.

Also

$$\begin{aligned}
M(e_r) &= \{m \in M : g(e_r, m) \in S\} \\
M(e_r, s) &= \{m \in M : g(e_r, m) = s\} \\
E_R(m_1, \cdots, m_i) &= \{e_r \in E_R : g(e_r, m_j) \in S \text{ and } g(e_r, m_j) \text{ are pairwise} \\
&\qquad \text{distinct, } 1 \le j \le i\} \\
E_R(e_t) &= \{e_r \in E_R : p(e_t, e_r) > 0\} \\
E_T(m_1, \cdots, m_i) &= \{e_t \in E_T : \exists s_j \in S \text{ such that } f(e_t, s_j) = m_j, 1 \le j \le i\} \\
E_T(e_r) &= \{e_t \in E_T : p(e_t, e_r) > 0\} \\
E_T \circ E_R &= \{(e_t, e_r) : p(e_t, e_r) > 0\}
\end{aligned}$$

3 Bounds on probability of success

We study three types of attack and derive lower bounds on the success probabilities of attacker in each case. Proofs of the theorems are omitted as they are essentially the same as proofs of Theorems 4.1-4.5 in [5] and Theorem 1 in [10].

Attack O_i: An opponent observes a sequence of i distinct messages, $m^i = (m_1, m_2, \cdots, m_i)$, sent by the transmitter and attempts to construct another message $m \neq m_j$, $1 \le j \le i$, which is acceptable by the receiver. The opponent is successful if receiver accepts m as authentic.

The opponent's probability of success is

$$p(R \text{ accepts } m \mid R \text{ accepts } m^i).$$

Define,

$$P_{O_i} = \max_{m^i \in M^i} \max_{m \in M} p(R \text{ accepts } m \mid R \text{ accepts } m^i).$$

For a random variable X with probability distribution $p(X)$ let $H(X) = -\sum_x p(x) \log p(x)$ denote the *entropy* function.

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

$$\frac{p(e_r | \textit{ R accepts } m^i)}{p(e_r | \textit{ R accepts } m^i, m)}$$

is independent of m^i, m and e_r, where $e_r \in E_R(m^i, m)$ and $E_R(m^i, m) \neq \emptyset$. In the case of the equality,

$$P_{O_i} = p(R \textit{ accepts } m \mid R \textit{ accepts } m^i) = \frac{p(e_r | \textit{ R accepts } m^i)}{p(e_r | \textit{ R accepts } m^i, m)}.$$

Attack R_i: Receiver, after receiving a sequence of i valid messages, $m^i = (m_1, m_2, \cdots, m_i)$, claims it has received a message m different from $m_1, m_2, \cdots, m_i$ It is successful if the arbiter approves receiver's claim. Arbiter accepts m from the receiver if m is valid under the transmitter's key.

Receiver's probability of success is,

$$p(m \text{ is valid for } T \mid T \text{ generates } m^i, e_r).$$

Define,

$$P_{R_i} = \max_{m^i \in M^i, e_r \in E_R} \max_{m \in M} p(m \text{ is valid for } T \mid T \text{ generates } m^i, e_r).$$

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

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

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

$$P_{R_i} = p(m \textit{ is valid for } T \mid T \textit{ generates } m^i, e_r) = \frac{p(e_t \mid T \textit{ generates } m^i, e_r)}{p(e_t \mid T \textit{ generates } m^i, m, e_r)}.$$

Attack T: T sends a message m, and later denies it. He is successful if the receiver accepts m as authentic. If T uses e_t, his success probability is,

$$p(m \text{ is valid } \mid e_t),$$

where m is valid means that m is acceptable by R and could not be generated by T using e_t. Define,

$$P_T = \max_{e_t \in E_T} \max_{m \in M \setminus M(e_t)} p(m \text{ is valid } \mid e_t).$$

Theorem 3.3 *([5])* $P_T \geq 2^{H(E_R|M,E_T)-H(E_R|E_T)}$.
Equality holds if and only if,

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

is independent of e_t, m and e_r, where $e_r \in E_R(m)$ assuming $E_R(m) \neq \emptyset$, $p(e_t, e_r) > 0$ and $m \notin M(e_t)$. In the case of equality,

$$P_T = p(R \textit{ accepts } m \mid e_t) = \frac{p(e_r \mid e_t)}{p(e_r \mid R \textit{ accepts } m, e_t)}.$$

4 Bounds on the sizes of the key spaces

An A^2-code is *secure against spoofing of order i* if P_{O_i}, P_{R_i} and P_T are all less than 1. We will consider an A^2-code which is secure against spoofing of order up to ℓ and use the following assumption throughout the rest of the papeı.

Assumption: *The probability distribution on $E_T \circ E_R$ is uniform.*

We consider the case that $P_{O_i}, P_{R_i} (0 \leq i \leq \ell)$ and P_T all achieve their lower bounds derived in Theorems 3.1, 3.2 and 3.3. In this case we can calculate probabilities in the following way.

$$\begin{aligned} P_{O_i} &= p(R \text{ accepts } m \mid R \text{ accepts } m^i) \\ &= \frac{p(R \text{ accepts } m^i, m)}{p(R \text{ accepts } m^i)} \\ &= \frac{\sum_{e_r \in E_R(m^{i+1})} p(e_r)}{\sum_{e_r \in E_R(m^i)} p(e_r)}. \end{aligned} \tag{1}$$

We also have,

$$\begin{aligned} P_{R_i} &= \frac{p(e_t \mid T \text{ generates } m^i, e_r)}{p(e_t \mid T \text{ generates } m^i, m, e_r)} \\ &= \frac{\sum_{e_t \in E_T(m^{i+1}) \cap E_T(e_r)} p(e_t, e_r)}{\sum_{e_t \in E_T(m^i) \cap E_T(e_r)} p(e_t, e_r)} \end{aligned} \tag{2}$$

Theorem 4.1 *In an A^2-code if P_{O_i} and P_{R_i} achieve their lower bounds, we have*

$$|E_T| \geq (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{R_i})^{-1}. \tag{3}$$

Equality holds if and only if,
(i) $|E_T(m^{\ell+1}) \cap E_T(e_r)| = 1$;
(ii) $|E_R(m^{\ell+1})| = |E_R(e_t)|$;
for any $m^{\ell+1}, e_t, e_r$ with $E_R(m^{\ell+1}) \neq \emptyset$, $E_T(m^{\ell+1}) \cap E_T(e_r) \neq \emptyset$; and
(iii) *the probability distribution on E_T is uniform.*

Proof: From equation (1) and (2) we have,

$$\begin{aligned}
(\prod_{i=0}^{\ell} P_{O_i})(\prod_{i=0}^{\ell} P_{R_i}) &= \sum_{e_r \in E_R(m^{\ell+1})} p(e_r)\frac{|E_T(m^{\ell+1}) \cap E_T(e_r)|}{|E_T(e_r)|} \\
&\geq \sum_{e_r \in E_R(m^{\ell+1})} p(e_r)\frac{1}{|E_T(e_r)|} \qquad (4)\\
&= \sum_{e_r \in E_R(m^{\ell+1})} p(e_r)p(e_t \mid e_r) \\
&= \sum_{e_r \in E_R(m^{\ell+1})} p(e_t, e_r) \\
&\geq \frac{|E_R(m^{\ell+1})|}{|E_T||E_R(e_t)|} \text{ (for some } e_t). \qquad (5)
\end{aligned}$$

Now choose $m^{\ell+1}$ and e_t such that $m^{\ell+1}$ is incident with e_t (could be generated by e_t). Then any $e_r \in E_R(e_t)$ must accept $m^{\ell+1}$. So $| E_R(m^{\ell+1}) |\geq| E_R(e_t) |$. Therefore $|E_T| \geq (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{R_i})^{-1}$. Equality holds if and only if $|E_R(m^{\ell+1})| \geq |E_R(e_t)|$ and inequalities (4) and (5) become equalities. Achieving equality in (4) is euivalent to $|E_T(m^{\ell+1}) \cap E_T(e_r)| = 1$. Achieving equality in (5) being euivalent to $|E_R(e_t)|$ is a constant for all e_t. It is also equivalent to that the probability distribution on E_T is uniform. □

Theorem 4.2 *In an A^2-code if $P_{O_i}, P_{R_i}, 0 \leq i \leq \ell$, and P_T achieve their lower bounds, and $|E_T| = (\prod_{i=0}^{\ell} P_{O_i})^{-1}(\prod_{i=0}^{\ell} P_{R_i})^{-1}$, then*

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

Equality holds if and only if

1. $|E_R(m) \cap E_R(e_t)| = 1$ *for any* e_t *and* m *such that* $m \notin M(e_t)$ *and* $E_R(m) \cap E_R(e_t) \neq \emptyset$.

2. *The probability distribution on* E_R *is uniform*

Proof: From Theorem 3.3 and 4.1 we can write P_T in the following way.

$$\begin{aligned} P_T &= p(R \text{ accepts } m \mid e_t) \\ &= \sum_{e_r \in E_R(m) \cap E_R(e_t)} p(e_r \mid e_t) = p(e_r \mid e_t)|E_R(m) \cap E_R(e_t)| \\ &= \frac{|E_R(m) \cap E_R(e_t)|}{|E_R(e_t)|} \end{aligned}$$

So we have

$$\begin{aligned} (\prod_{i=0}^{\ell} P_{O_i})P_T &= \sum_{e_r \in E_R(m^{\ell+1})} p(e_r) \frac{|E_R(m) \cap E_R(e_t)|}{|E_R(e_t)|} \\ &= \sum_{e_r \in E_R(m^{\ell+1})} \sum_{e_t \in E_T(e_r)} p(e_t, e_r) \frac{|E_R(m) \cap E_R(e_t)|}{|E_R(e_t)|} \\ &= \sum_{e_r \in E_R(e_t)} \sum_{e_t \in E_T(e_r)} p(e_t, e_r) \frac{|E_R(m) \cap E_R(e_t)|}{|E_R(e_t)|} \quad \text{(by Theorem 4.1)} \\ &= \sum_{e_t \in E_T(e_r)} \sum_{e_r \in E_R(e_t)} p(e_t, e_r) \frac{|E_R(m) \cap E_R(e_t)|}{|E_R(e_t)|} \\ &= \frac{|E_T(e_r)||E_R(e_t)|}{|E_T \circ E_R|} \frac{|E_R(m) \cap E_R(e_t)|}{|E_R(e_t)|} \\ &= \frac{|E_T(e_r)|}{|E_T \circ E_R|} |E_R(m) \cap E_R(e_t)| \end{aligned}$$

The above value is independent of e_t, e_r, m. So we can choose an e_r such that $\frac{|E_T(e_r)|}{|E_T \circ E_R|} \geq \frac{1}{|E_R|}$. Then we get

$$|E_R| \geq (\prod_{i=0}^{\ell} P_{O_i})^{-1} P_T^{-1} |E_R(m) \cap E_R(e_t)| \tag{6}$$

$$\geq (\prod_{i=0}^{\ell} P_{O_i})^{-1} P_T^{-1} \tag{7}$$

$|E_R| = (\prod_{i=0}^{\ell} P_{O_i})^{-1} P_T^{-1}$ if and only if inequalities (6), (7) become equalities. (6) becomes equality if and only if $|E_T(e_r)|$ is independent of e_r. It is equivalent

to the probability distribution on E_R is uniform.
(7) becomes equality if and only if $|E_R(m) \cap E_R(e_t)| = 1$ for all m and e_t with $m \notin M(e_t)$. □

Corollary 4.1 *If $|E_T|, |E_R|$ achieve their lower bounds, then we have*

$$|E_T \circ E_R| = (\prod_{i=0}^{\ell} P_{O_i})^{-1} (\prod_{i=0}^{\ell} P_{R_i})^{-1} P_T^{-1}.$$

Proof: In the case that $|E_T|, |E_R|$ achieve lower bounds, we have

$$(\prod_{i=0}^{\ell} P_{O_i})(\prod_{i=0}^{\ell} P_{R_i}) P_T = \frac{|E_R(m^{\ell+1})|}{|E_R|} \frac{1}{|E_T(e_r)|} \frac{|E_R(m) \cap E_R(e_t)|}{|E_R(e_t)|} = \frac{1}{|E_T \circ E_R|}$$

□

An A^2-code, for which $P_{O_i}, P_{R_i}, 0 \leq i \leq \ell, P_T, |E_R|, |E_T|$ all achieve their lower bounds, is called *ℓ-optimal code.* In the rest of this paper we study combinatorial structure of these codes.

Corollary 4.2 *In an ℓ-optimal code, for any $i, 1 \leq i \leq \ell + 1$, we have the following:*

1. *$|E_T(m^i) \cap E_T(e_r)|$ is independent of m^i and e_r if $E_T(m^i) \cap E_T(e_r) \neq \emptyset$.*
2. *$|E_T(m^i)|$ is independent of m^i if $E_T(m^i) \neq \emptyset$. Especially, $|E_T(m^{\ell+1})| = 1$.*
3. *$|E_R(m^i) \cap E_R(e_t)|$ is independent of m^i and e_t if $E_R(m^i) \cap E_R(e_t) \neq \emptyset$.*
4. *$|E_R(m^i)|$ is independent of m^i if $E_R(m^i) \neq \emptyset$.*

Proof: From (i), (iii) of Theorem 4.1 and equality (2) we have

$$\prod_{j=0}^{i-1} P_{R_j} = \frac{|E_T(m^i) \cap E_T(e_r)|}{|E_T(e_r)|}.$$

So $|E_T(m^i) \cap E_T(e_r)|$ is independent of m^i and e_r. The first statement is true. From (ii), (iii) of Theorem 4.1 and equality (1) we have

$$\prod_{j=0}^{i-1} P_{O_j} = \sum_{e_r \in E_R(m^i)} p(e_r) = \frac{|E_R(m^i)|}{|E_R|}.$$

So $|E_R(m^i)|$ is independent of m^i for any i. The last statement is true. From

$$|E_R(m^i)| \cdot |E_T(m^i) \cap E_T(e_r)| = |E_T(m^i)| \cdot |E_R(e_t)| \tag{8}$$

we know $|E_T(m^i)|$ is independent of m^i. Especially, by Theorem 4.1, (i), (ii) $|E_T(m^\ell)| = 1$. The second statement is true. In the similar way the third one can be proved.

□

5 Combinatorial Structures of the Key Spaces

In this section we study the relationship between l-optimal A^2-code and combinatorial design. We only consider *Cartesian* (*without secrecy*) A^2-codes. In a Cartesian A^2-code for a fixed $m \in M$, there is a unique s and one or more $e_t \in E_T$ that satisfy $f(e_t, s) = m$, and at most one s and one or more $e_r \in E_R$ that satisfy $g(e_r, m) = s$.

5.1 Two Kinds of Combinatorial Designs

Definition 5.1 *A* block design *is a pair* (V, B)*, where* V *is a set of* v *points and* 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 5.2 *([8]) A block design is called* α-resolvable *if the block set 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.*

Obana and Kurosawa showed an example of this design [8]. 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, $1 \leq i \leq \ell + 1$.

(P2) For any ℓ+1 blocks $B_{j_1}, B_{j_2}, \cdots, B_{j_{\ell+1}}$ from different classes $C_{j_1}, C_{j_2}, \cdots, C_{j_\ell}$ 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 $B \in C_u \backslash \{B_u\}$, $|B_{j_1} \cap \cdots \cap B_{j_{\ell+1}} \cap B| = 1$.

Definition 5.3 *([10]) A* partially balanced t-design *is a block design* (V, 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 5.4 *A $t-(v,k;\{\lambda,0\})$-design (V,B) is a* strong partially balanced t-design *if it is also an $i-(v,k;\{\lambda_i,0\})$-design, for any i, $1 < i < t$, and 1-design.*

Example 5.1 *(Existence of strong partially balanced t-design)*

Let $\mathbf{F_q}$ be a field of q elements, and l be a positive integer less than $q-1$.

$$V = \mathbf{F_q}^2$$

For fixed $a_i \in \mathbf{F_q}$, $a_i \neq 0$, define a subset $C \subseteq V$ as follows:

$$C = \{(x,y) : y = \sum_{i=0}^{l} a_i x^i, a_i \in \mathbf{F_q}, a_l \neq 0\}.$$

Let B be the family of all subsets defined above. For any i different points $(x_1,y_1),(x_2,y_2),\cdots,(x_i,y_i) \in V$, if they are in a subset C, then they satisfy

$$\begin{array}{rcl} a_l x_1^l + a_{l-1}x_1^{l-1} + \cdots + a_1 x_1 + a_0 & = & y_1 \\ a_l x_2^l + a_{l-1}x_2^{l-1} + \cdots + a_1 x_2 + a_0 & = & y_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots & & \\ a_l x_i^l + a_{l-1}x_i^{l-1} + \cdots + a_1 x_i + a_0 & = & y_i \end{array}$$

This is a system of linear equations with unknown $a_0, a_1, \cdots, a_l$. The rank of the coefficient matrix is i. So for $1 \leq i \leq l$, it has $q^{l-i}(q-1)$ solutions $(a_l, a_{l-1}, \cdots, a_0)$ with $a_l \neq 0$. If $i = l+1$ there is a unique solution. Therefore (V,B) is a strong $(l+1)-(q^2,q;\{1,0\})$-design with $\lambda_i = q^{l-i}(q-1), 1 \leq i \leq l$.

Definition 5.5 *A $t-(v,k;\{\lambda,0\})$-design (V,B) is a* resolvable partially balanced t-design *if the block set can be partitioned into classes $C_1, C_2, \cdots, C_{n'}$ with the property that for each $j(1 \leq j \leq n')$, (V, C_j) is a $t-(v',k;\{\lambda',0\})$-design.*

Definition 5.6 *A* strong partially balanced $t-(v,k;\{\lambda,0\})$-design (V,B) *is resolvable if it is resolvable with classes $C_1, C_2 \cdots, C_{n'}$ and the property that for each $j, 1 \leq j \leq n', (V, C_j)$ is a strong partially balanced $t-(v',k;\{\lambda',0\})$-design.*

Now we show how to derive resolvable partially balanced t-design from an α-resolvable design with properties **(P1)** and **(P2)**.

Lemma 5.1 *Let (V, B) be an α-resolvable design in which B, $|B| = b$, is partitioned into $C_1, C_2, \cdots, C_n$ with property* **(P1)**. *Suppose all classes include the same number of blocks. Then*

$$|\{(B_{j_1}, \cdots, B_{j_i}) : \cap_{u=1}^{i} B_{j_u} \neq \emptyset, B_{j_u} \in C_u, 1 \leq u \leq i\}| = \frac{b}{n} \cdot \frac{\mu_1}{\mu_i} \alpha^{i-1},$$

where $1 < i \leq \ell + 1$.

Proof: We use an induction argument to prove this lemma. First consider a block B_1 in C_1. Using property **(P1)**, for each point $p \in B_1$, there are α blocks B_2's in C_2 such that $p \in B_1 \cap B_2$. Now $|B_1| = \mu_1, |B_1 \cap B_2| = \mu_2$, and so for a fixed B_1,

$$|\{(B_1, B_2) : B_1 \cap B_2 \neq \emptyset, B_2 \in C_2\}| = \frac{\mu_1}{\mu_2} \alpha.$$

If B_1 runs through C_1, then because $|C_i| = b/n$ we have,

$$|\{(B_1, B_2) : B_1 \cap B_2 \neq \emptyset, B_1 \in C_1, B_2 \in C_2\}| = \frac{b}{n} \cdot \frac{\mu_1}{\mu_2} \alpha.$$

Now suppose for i blocks we have,

$$|\{(B_{j_1}, \cdots, B_{j_i}) : \cap_{u=1}^{i} B_{j_u} \neq \emptyset, B_{j_u} \in C_u, 1 \leq u \leq i\}| = \frac{b}{n} \cdot \frac{\mu_1}{\mu_i} \alpha^{i-1}.$$

We show that a similar equation holds for $i + 1$ blocks, hence completing the induction step. Consider a point $p \in \cap_{u=1}^{i} B_{j_u}$. There are α blocks $B_{j_{i+1}}$ in $C_{j_{i+1}}$ such that $p \in \cap_{u=1}^{i+1} B_{j_u}$. Because $|\cap_{u=1}^{i} B_{j_u}| = \mu_i$ and $|\cap_{u=1}^{i+1} B_{j_u}| = \mu_{i+1}$, we have

$$\begin{aligned} |\{(B_{j_1}, \cdots, B_{j_{i+1}}) : \cap_{u=1}^{i+1} B_{j_u} \neq \emptyset, B_{j_u} \in C_u, 1 \leq u \leq i+1\}| &= \frac{b}{n} \cdot \frac{\mu_1}{\mu_i} \alpha^{i-1} \cdot \frac{\mu_i}{\mu_{i+1}} \alpha \\ &= \frac{b}{n} \cdot \frac{\mu_1}{\mu_{i+1}} \alpha^{i}, \end{aligned}$$

which proves the Lemma. □

Lemma 5.2 *Let (V, B) be an α-resolvable design in which B is partitioned into $C_1, C_2, \cdots, C_n$ and satisfies property* **(P1)**. *Suppose all classes include the same number of blocks. Then for i blocks $B_{j_1} \in C_{j_1}, \cdots, B_{j_i} \in C_{j_i}$ with $\cap_{u=1}^{i} B_{j_u} \neq \emptyset$, we have*

$$|\{(B_{j_{i+1}}, \cdots, B_{j_{\ell+1}}) : \cap_{u=1}^{\ell+1} B_{j_u} \neq \emptyset, B_{j_u} \in C_u, i+1 \leq u \leq \ell+1\}| = \frac{\mu_i}{\mu_{\ell+1}} \alpha^{\ell-i+1},$$

where $1 < i < \ell + 1$.

Proof: For any $p \in \cap_{u=1}^{i} B_{j_u}$ there are α blocks $B_{j_{i+1}}$ in $C_{j_{i+1}}$ such that $p \in \cap_{u=1}^{i+1} B_{j_u}$. By **(P1)** we know $| \cap_{u=1}^{i} B_{j_u}| = \mu_i$ and $| \cap_{u=1}^{i+1} B_{j_u}| = \mu_{i+1}$. So $|\{B_{j_{i+1}} \in C_{j_{i+1}} : \cap_{u=1}^{i+1} B_{j_u} \neq \emptyset\}| = \frac{\mu_i}{\mu_{i+1}}\alpha$. Similar argument for $i+1$ blocks, $B_{j_1}, B_{j_2}, \cdots, B_{j_{i+1}}$, results in $|\{B_{j_{i+2}} \in C_{j_{i+2}} : \cap_{u=1}^{i+2} B_{j_u} \neq \emptyset\}| = \frac{\mu_{i+1}}{\mu_{i+2}}\alpha$. Repeating the argument we have

$$\begin{aligned} & |\{(B_{j_{i+1}}, \cdots, B_{j_{\ell+1}}) : \cap_{u=1}^{\ell+1} B_{j_u} \neq \emptyset, B_{j_u} \in C_u, i+1 \leq u \leq \ell+1\}| \\ = \;& \frac{\mu_i}{\mu_{i+1}}\alpha \cdot \frac{\mu_{i+1}}{\mu_{i+2}}\alpha \cdots \frac{\mu_\ell}{\mu_{\ell+1}}\alpha \\ = \;& \frac{\mu_i}{\mu_{\ell+1}}\alpha^{\ell-i+1}, \end{aligned}$$

which proves the Lemma. □

Lemma 5.3 *Let (V, B) be an α-resolvable design in which B is partitioned into $C_1, C_2, \cdots, C_n$. Suppose all classes have the same number of blocks. For i blocks $B_{j_1} \in C_{j_1}, \cdots, B_{j_i} \in C_{j_i}$ with $1 \leq i \leq \ell$, and $p \in \cap_{u=1}^{i} B_{j_u}$, we have*

$$|\{(B_{j_{i+1}}, \cdots, B_{j_{\ell+1}}) : p \in \cap_{u=1}^{\ell+1} B_{j_u}, B_{j_u} \in C_u, 1 \leq u \leq \ell+1\}| = \alpha^{\ell-i+1}.$$

Proof: It follows from Definition 5.2. □

Theorem 5.1 *Suppose there exists an α-resolvable design (V, B) in which B is partitioned into $C_1, C_2, \cdots, C_n$, with properties* **(P1)** *and* **(P2)**, *and such that all classes have the same number of blocks. Then there exists an $(\ell+1)-(|B|, n; \{1, 0\})$-design (U, E) which is strong resolvable and has parameters,*

$$\lambda_i = \frac{\mu_i}{\mu_{\ell+1}}\alpha^{\ell-i+1}, \lambda_i' = \alpha^{\ell-i+1}.$$

Proof: We construct a resolvable partially balanced $(\ell+1)$-design. Let U be the set of $|B|$ points. Fix $\ell+1$ classes, say $C_1, C_2, \cdots, C_{\ell+1}$. From property **(P2)**, for any $\ell+1$ blocks $B_1 \in C_1, B_2 \in C_2, \cdots, B_{\ell+1} \in C_{\ell+1}$, with $B_1 \cap B_2 \cap \cdots \cap B_{\ell+1} \neq \emptyset$, and any $u, \ell+1 < u \leq n$, there exists a unique block $B_u \in C_u$ such that $B_1 \cap \cdots \cap B_{\ell+1} \cap B_u = B_1 \cap \cdots \cap B_{\ell+1}$. In this case there exists only one group $B_{\ell+2} \in C_{\ell+2}, \cdots, B_n \in C_n$ such that

$$B_1 \cap \cdots \cap B_{\ell+1} \cap B_{\ell+2} \cap \cdots \cap B_n = B_1 \cap \cdots \cap B_{\ell+1}.$$

Now we define a block (n-subset of U)

$$E_{B_1, \cdots, B_{\ell+1}} = \{m_1, \cdots, m_{\ell+1}, m_{\ell+2}, \cdots, m_n\}. \qquad (9)$$

From Lemma 5.1, we get in total $\frac{b}{n}\frac{\mu_1}{\mu_{\ell+1}}\alpha^\ell$ blocks which form a block set E. Using this construction we know that any $\ell+1$ points of U either occur in one block or does not occur in any block. From Lemma 5.2 we know that any i points of U either occur in $\frac{\mu_i}{\mu_{\ell+1}}\alpha^{\ell-i+1}$ blocks or do not occur in any block. So (U,E) is an $(\ell+1)-(|B|,n;\{1,0\})$-design with parameters $\lambda_i = \frac{\mu_i}{\mu_{\ell+1}}\alpha^{\ell-i+1}, 1 \le i \le \ell$.

From properties **(P1)** and **(P2)**, a point $p \in V$ appears in α blocks of every class. Therefore

$$|\{(B_1, B_2, \cdots, B_{\ell+1}) : p \in \cap_{j=1}^{\ell+1} B_j\}| = \alpha^{\ell+1}.$$

That is, a point $p \in V$ corresponds to $\alpha^{\ell+1}$ blocks $e_1, \cdots, e_{\alpha^{\ell+1}}$ of (U,E). For each block, say e_j, we call (e_j, p) a valid pair. Now we partition the block set E. First choose one point $p_1 \in V$. There are $\alpha^{\ell+1}$ blocks e in E such that each (e, p_1) is a valid pair. Denote the collection of such e by E_1. Next if there is any point left, choose

$$p_2 \in V - \{p \in V : \exists e \in E_1,\ (e,p) \text{ is a valid pair}\}.$$

Then there are $\alpha^{\ell+1}$ blocks e in E such that (e, p_2) is a valid pair. Denote the collection of such e by E_2. Repeat the above steps until all the points are exhausted. At the dth step we choose

$$p_d \in V - \{p \in V : \exists e \in E_1 \cup E_2 \cup \cdots \cup E_{d-1},\ (e,p) \text{ is a valid pair}\}.$$

For p_d there are $\alpha^{\ell+1}$ blocks e in E such that (e, p_d) is a valid pair. The collection of all such e is E_d. The process stops when,

$$V - \{p \in V : \exists e \in E_1 \cup \cdots \cup E_u,\ (e,p) \text{ is a valid pair}\} = \emptyset.$$

Now we have a partition of $E = E_1 \cup \cdots \cup E_u$.

Furthermore, in each E_j, using Lemma 5.3 any $i, 1 \le i \le \ell$, points of U either occur in exactly $\alpha^{\ell-i+1}$ blocks or do not occur in any block. This implies (U,E) is a strong, resolvable partially balanced $(\ell+1)$-design with parameters $\lambda_i' = \alpha^{\ell-i+1}$. This proves the Theorem. □

5.2 Structure of E_R and E_T

In this section we will study the combinatorial structure of E_T and E_R which correspond to the combinatorial designs defined in the previous section. We assume all codes are ℓ-optimal Cartesian codes. In a Cartesian A^2-code M is partitioned into $M_1, M_2, \cdots, M_{|S|}$, where $M_j = \{m : \exists e_r \in E_R \text{ such that } g(e_r, m) = s_j\}$.

Lemma 5.4 *$|M(e_r, s)|$ and $|M(e_r)|$ are independent of e_r, s.*

Proof: For a given $e_r \in E_R$ and $s \in S$, all m in $\{m = f(e_t, s) : e_t \in E_T(e_r)\}$ are acceptable by e_r. So $|M(e_r, s)| \geq \frac{|E_T(e_r)|}{|E_T(m) \cap E_T(e_r)|}$. On the other hand if m can be accepted by e_r, then m can be generated by some $e_t \in E_T(e_r)$. So $|M(e_r, s)| \leq \frac{|E_T(e_r)|}{|E_T(m) \cap E_T(e_r)|}$. Therefore, $|M(e_r, s)| = \frac{|E_T(e_r)|}{|E_T(m) \cap E_T(e_r)|}$, which is independent of e_r and m using Corollary 4.2, 1. It follows that $|M(e_r)| = \sum_{s \in S} |M(e_r, s)| = |S| \cdot |M(e_r, s)|$ is independent of $e_r \in E_R$. □

Corollary 5.1 *$P_{R_0}^{-1} = |M(e_r, s)|$ is an integer.*

Proof: From the proof of Lemma 5.4 and equation (2). □

Lemma 5.5 $P_{R_0} = P_{R_1} = \cdots = P_{R_\ell}$.

Proof: From equation (2) $P_{R_0} = \frac{|E_T(m) \cap E_T(e_r)|}{|E_T(e_r)|}$. Now fix $s \in S$ and $e_r \in E_R$. Choose $m^i = (m_1, \cdots, m_i)$ such that $E_T(m^i) \cap E_T(e_r) \neq \emptyset$ and $m_1, \cdots, m_i \notin M(e_r, s)$. Then for $m \in M(e_r, s)$, m^i and m can be accepted by e_r. Hence m^i and m can be generated by some $e_t \in E_T(e_r)$. So

$$|E_T(m^i, m) \cap E_T(e_r)| \cdot |M(e_r, s)| = |E_T(m^i) \cap E_T(e_r)|.$$

Hence we get $|M(e_r, s)| = \frac{|E_T(m^i) \cap E_T(e_r)|}{|E_T(m^i, m) \cap E_T(e_r)|} = P_{R_i}^{-1}$. But we also know that $|M(e_r, s)| = \frac{|E_T(e_r)|}{|E_T(m) \cap E_T(e_r)|} = P_{R_0}^{-1}$. So $P_{R_0} = P_{R_1} = \cdots = P_{R_\ell}$. □

Lemma 5.6 $P_{O_0} = P_{O_1} = \cdots = P_{O_\ell}$.

Proof: Fix a $j, 1 \leq j \leq |S|$. For $i \leq \ell$ choose $m^i = (m_1, \cdots, m_i)$ such that $m_1, \cdots, m_i \notin M_j$ and $E_R(m^i) \neq \emptyset$. Then

$$\sum_{m \in M_j} \sum_{e_r \in E_R(m^i, m)} p(e_r) = |M(e_r, s_j)| \sum_{e_r \in E_R(m^i)} p(e_r).$$

So $P_{O_i} = |M(e_r, s_j)| \cdot |M_j|^{-1}$ and so all P_{O_i} are equal. □

Corollary 5.2 *There exists an integer c such that $|M| = c|S|$.*

Proof: In the proof of Lemma 5.6 we have seen that $|M_j| = |M(e_r, s)| P_{O_i}^{-1}$ holds for each $j, 1 \leq j \leq |S|$. So $|M_1| = |M_2| = \cdots = |M_{|S|}|$. Therefore $|M| = |M_1| \cdot |S|$. □

Lemma 5.7 *There is a partition on E_T given by $E_T = \cup_{e_r} E_T(e_r)$.*

The proof can be found in [13].

Lemma 5.8 *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 $E_R(m^{\ell+1}) = E_R(m^{\ell+1}, m_u)$.*

Proof: Suppose $E_R(m^{\ell+1}) \neq \emptyset$. Then there exists at least one $e_t \in E_T$ that generates $m^{\ell+1}$. Without loss of generality, we assume that $m^{\ell+1}$ comes from $M_1, \cdots, M_{\ell+1}$. Let $u > \ell+1$ and $f(e_t, s_u) = m_u$. Clearly $E_R(m^{\ell+1}, m_u) \subseteq E_R(m^{\ell+1})$. To prove $E_R(m^{\ell+1}, m_u) = E_R(m^{\ell+1})$, assume otherwise: that is $E_R(m^{\ell+1}, m_u) \neq E_R(m^{\ell+1})$ and so $|E_R(m^{\ell+1}, m_u)| < |E_R(m^{\ell+1})|$. From Theorem 4.1, (ii) we know $|E_R(m^{\ell+1})| = |E_R(e_t)|$. So $|E_R(m^{\ell+1}, m_u)| < |E_R(e_t)|$. But because of the way m_u, e_t are chosen, we know $E_R(e_t) \subseteq E_R(m^{\ell+1}, m_u)$. Hence $|E_R(e_t)| \leq |E_R(m^{\ell+1}, m_u)|$ which is a contradiction.

Uniqueness: If there exist two messages $m_u, m_u^{'} \in M_u$ such that

$$E_R(m^{\ell+1}, m_u) = E_R(m^{\ell+1}, m_u^{'}) = E_R(m^{\ell+1})$$

then there exist $e_t, e_t^{'} \in E_T$ such that $m^{\ell+1}, m_u$ can be generated by e_t, and $m^{\ell+1}, m_u^{'}$ can be generated by $e_t^{'}$. As both $m_u, m_u^{'}$ are in M_u, $e_t \neq e_t^{'}$. So $|E_T(m^{\ell+1})| \geq 2 > 1$, which contradicts Corollary 4.2, 2. □

Note that Lemma 5.8 tells us that if a sequence of $\ell+1$ messages,

$$m_1 \in M_1, \cdots, m_{\ell+1} \in M_{\ell+1}$$

is acceptable under the same key, then there exists a unique sequence $m_{\ell+2} \in M_{\ell+2}, \cdots, m_{|S|} \in M_{|S|}$ such that

$$E_R(m_1, \cdots, m_{\ell+1}) = E_R(m_1, \cdots, m_{\ell+1}, m_{\ell+2}, \cdots, m_{|S|}).$$

Furthermore from Theorem 3.1 and 4.2, for any m such that $m \neq m_{\ell+2}, \cdots, m_{|S|}$, we have $E_R(m_1, \cdots, m_{\ell+1}, m) = E_R(m_1, \cdots, m_{\ell+1}) \cap E_R(m) = E_R(e_t) \cap E_R(m)$. So $|E_R(m_1, \cdots, m_{\ell+1}, m)| = 1$. This means that the system will not be secure after ℓ messages are transmitted.

The structures of E_R and E_T are given as follows. Let E_R be a point set. From Corollary 4.2, 4 we have $|E_R(m)|$ independent of m. So $(E_R, \{E_R(m) : m \in M\})$ forms a block design. In this design the block set can be partitioned into $|S|$ classes $C_1, C_2, \cdots, C_{|S|}$ such that if $g(e_r, m) = s_i$ then the block $E_R(m)$ is in C_i.

The following theorem gives the structure of E_R.

Theorem 5.2 *In an ℓ-optimal Cartesian A^2-code, the design $(E_R, \{E_R(m)\})$ is α-resolvable with properties (***P1***) and (***P2***). The block set is partitioned into $|S|$ classes, $C_1, C_2, \cdots, C_{|S|}$, and has following parameters:*

1. $\alpha = P_{R_0}^{-1}$.
2. $\mu_i = |E_R| \prod_{j=0}^{i-1} P_{O_j}$ *for any* i, $1 \leq i \leq \ell + 1$.

Proof: From Corollary 5.1, 4.2 and Lemma 5.8 it can be derived that $(E_R, \{E_R(m)\})$ is α-resolvable with properties (**P1**) and (**P2**). Corollary 5.1 shows that $\alpha = P_{R_0}^{-1}$, and equation (1) shows that $\mu_i = |E_R(m^i)| = |E_R| \prod_{j=0}^{i-1} P_{O_j}$. □

Now we consider E_T. Let M be the point set, and for each $e_t \in E_T$ consider a block $\{f(e_t, s) : s \in S\}$. Then $(M, \{f(e_t, S) : e_t \in E_T\})$ forms a block design which is denoted by (M, E_T).

Theorem 5.3 *In an ℓ-optimal Cartesian A^2-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:*

1. $\lambda = \lambda_{\ell+1} = 1$, *and*
   $\lambda_i = (P_{O_0}^{-1})^{\ell-i+1}(P_{R_0}^{-1})^{\ell-i+1}, \ 1 \leq i \leq \ell;$
2. *For a class C_j, (M, C_j) has parameters $\lambda' = \lambda'_{\ell+1} = 1$, and*
   $\lambda'_i = (P_{R_0}^{-1})^{\ell-i+1}, \ 1 \leq i \leq \ell,$

where $n' = |E_T|/|E_T(e_r)|$.

Proof: Lemma 5.7 and Corollary 4.2 show that (M, E_T) is a strong partially balanced, resolvable $(\ell + 1) - (|M|, |S|; \{\lambda, 0\})$-design. The parameters are as follows.

$$\begin{aligned}
\lambda_i &= |E_T(m^i)| = \frac{|E_R(m^i)|}{|E_R(e_t)|}|E_T(m^i) \cap E_T(e_r)| \quad \text{(from (8))} \\
&= \frac{|E_R(m^i)|}{|E_R(m^{\ell+1})|}\frac{|E_T(m^i) \cap E_T(e_r)|}{|E_T(m^{\ell+1}) \cap E_T(e_r)|} \quad \text{(from theorem 4.1)} \\
&= (P_{O_0}^{-1})^{\ell-1+1}(P_{R_0}^{-1})^{\ell-i+1} \quad \text{(from (1), (2), lemma 5.5, 5.6)}
\end{aligned}$$

and

$$\lambda'_i = |E_T(m^i) \cap E_T(e_r)| = \frac{|E_T(m^i) \cap E_T(e_r)|}{|E_T(m^{\ell+1}) \cap E_T(e_r)|} = (P_{R_0}^{-1})^{\ell-i+1}.$$

□

5.3 Constructing ℓ-optimal A^2-codes from Designs

In this subsection we show how to construct an ℓ-optimal Cartesian A^2-code from an α-resolvable design.

Theorem 5.4 *Suppose there exists an α-resolvable design (V, B) in which M is partitioned into $C_1, C_2, \cdots, C_n$ with properties* **(P1)** *,* **(P2)** *and such that all classes have the same number of blocks. Then there exist an ℓ-optimal Cartesian A^2-code The code has the following parameters:*

1. *The number of source states is n;*
2. *The number of messages is $|B|$;*
3. $|E_R| = |V|, |E_T| = \frac{|B|}{n} \cdot \frac{\mu_1}{\mu_{\ell+1}}\alpha^\ell, |E_T \circ E_R| = \frac{|B|}{n}\mu_1\alpha^\ell$;
4. $P_{O_i} = \frac{\mu_{i+1}}{\mu_i}, P_{R_i} = \frac{1}{\alpha}, P_T = \frac{1}{\mu_{\ell+1}}, 0 \leq i \leq \ell.$

Proof: Using theorem 5.1 we obtain an $(\ell + 1) - (|B|, n; \{0, 1\})$ design (U, E). Now the A^2-code will have the message space $M = U$, source state space $S = \{s_1, s_2, \cdots, s_n\}$, $E_R = V$ and $E_T = E$.

For each $v \in V$ define a verification function g such that

$$g(v, m) = \begin{cases} s_i & \text{if } v \in B_i \\ - & \text{if } v \notin B_i \end{cases}$$

For each $e \in E$ define an encoding function f such that $f(e, S)$ is (9).

Because of property **(P1)** $P_{O_i} = \frac{\mu_{i+1}}{\mu_i}$. From the proof of Theorem 5.1 we know $P_{R_i} = \frac{\lambda'_{i+1}}{\lambda'_i} = \frac{1}{\alpha}$, and from property **(P2)** and construction of E_T we have $P_T = \frac{1}{\mu_{\ell+1}}$. All calculations are independent of the chosen message, encoding function or verification function. So P_{O_i}, P_{R_i}, P_T meet their lower bounds.

Noting the construction of E_T in the proof of Theorem 5.1 we know that $E_R(m^{\ell+1}) = E_R(e_t)$ and $|E_T(m^{\ell+1}) \cap E_T(e_r)| = 1$. So by using Theorem 4.1 $|E_T|$ achieves its lower bound. From property **(P2)** we know for any m such that $m \notin M(e_t)$,

$$|E_R(m) \cap E_R(e_t)| = |E_R(m) \cap E_R(m_1, \cdots, m_{\ell+1})| = |E_R(m_1, \cdots, m_{\ell+1}, m)| = 1$$

and so by using Theorem 4.2 $|E_R|$ achieves its lower bound. Hence the code is optimal. □

Example 5.2 *An 1-optimal A^2-code*

Encoding matrix E_T:

			s	
		1	2	3
e_t	1	1	6	9
	2	1	5	10
	3	2	6	10
	4	2	5	9
	5	1	8	11
	6	1	7	12
	7	2	8	12
	8	2	7	11
	9	3	6	11
	10	3	5	12
	11	4	6	12
	12	4	5	11
	13	3	8	9
	14	3	7	10
	15	4	8	10
	16	4	7	9

Verification matrix E_R:

							m						
		1	2	3	4	5	6	7	8	9	10	11	12
e_r	1	1	1	-	-	2	2	-	-	3	3	-	-
	2	1	1	-	-	-	-	2	2	-	-	3	3
	3	-	-	1	1	2	2	-	-	-	-	3	3
	4	-	-	1	1	-	-	2	2	3	3	-	-
	5	-	1	-	1	2	-	2	-	3	-	3	-
	6	-	1	-	1	-	2	-	2	-	3	-	3
	7	1	-	1	-	2	-	2	-	-	3	-	3
	8	1	-	1	-	-	2	-	2	3	-	3	-

$E_T \circ E_R$:

		e_r							
		1	2	3	4	5	6	7	8
	1	√							√
	2	√						√	
	3	√					√		
	4	√				√			
	5		√						√
	6		√					√	
	7		√				√		
e_t	8		√			√			
	9			√					√
	10			√				√	
	11			√			√		
	12			√		√			
	13				√				√
	14				√			√	
	15				√		√		
	16				√	√			

In this code, $P_{O_0}=1/2$, $P_{O_1}=1/2$, $P_{R_0}=1/2$, $P_{R_1}=1/2$, $P_T=1/2$.
Note that $E_T \circ E_R$ corresponds a partially balanced 2 design.

References

[1] Y. Desmedt and J. Seberry, *Practical Proven Secure Authentication with Arbitration*, Advances in cryptology–AUSCRYPT'92, 27-32.

[2] Y. Desmedt and M. Yung, *Arbitrated Unconditionally Secure Authentication Can Be Unconditionally Protected against Arbiter's attacks*, Advances in Cryptology-CRYPTO'90, 177-188 (1991).

[3] J. H. Dintiz and D. Stinson, *Contemporary Design Theory, A collection of Surveys*, A Wiley Interscience Publications, John Wiley & Sons, INC(1992).

[4] E. N. Gilbert, F. J. MacWilliams and N. J. A. Slone, *Codes which detect deception*, Bell system technical journal 53(1974), 405-424.

[5] T. Johansson, *Contributions to unconditionally secure authentication*, Ph.D Thesis, 1994, Lund University, Sweden.

[6] T. Johansson, *Authentication codes for nontrusting parties obtained from rank metric codes*, Designs, Codes, and Cryptography, 6, 205-218(1995).

[7] K. Kurosawa, *New bound on authentication code with arbitration*, Advances in cryptology–CRYPTO'94, Lecture note in computer science 839(1994), 140-149

[8] S. Obana and K. Kurosawa, *A^2-code=Affine resolvable + BIBD*, Proc. of ICICS, Lecture note in computer science 1334, 118-129(1997).

[9] J. L. Massey, *Contemporary cryptology: an introduction*, Contemporary cryptology, the science of information integrity, 1-39(1992).

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

[11] D. Pei and X. Wang, *Authentication-secrecy code based on conics over finite fields*, Sci. China Ser. E39(1996), No.5, 471-484.

[12] R. S. Rees and D. R. Stinson, *Combinatorial characterisations of authentication codes II*, Designs, codes and cryptography 7(1996),239-259.

[13] R. Safavi-Naini and Y. Wang, *Combinatorial structure of A^3-codes against collusion attacks*, preprint.

[14] G. J. Simmons, *Authentication theory/coding theory*, Advances in cryptology–CRYPTO'84, Lecture notes in computer science 196(1985), 411-432.

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

[16] G. J. Simmons, *A survey of information authentication*, in Contemporary Cryptology, The science of information integrity, ed. G. J. Simmons, IEEE Press, New York, 1992.

[17] D. R. Stinson, *The combinatorics of authentication and secrecy codes*, Journal of cryptology 2(1990), 23-49.

[18] R. Taylor, *Near Optimal Unconditionally Secure Authentication*, Advances in Cryptology–EUROCRYPT'94, 245-255.