BULL. AUSTRAL. MATH. SOC. 94A60, 05B05, 05A15
VOL. 69 (2004) [203–215]

ISOMORPHISM CLASSES OF AUTHENTICATION CODES

RONGQUAN FENG, JIN HO KWAK AND E. KEITH LLOYD

In this paper, we give several kinds of characterisations of isomorphic authentication codes by examining a correspondence between optimal authentication codes and some combinatorial designs. The isomorphism classes of some kinds of authentication codes are also enumerated.

1. INTRODUCTION

Let $\mathcal{S}$, $\mathcal{E}$ and $\mathcal{M}$ be three non-empty sets and let $f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$ be a map. The four tuple $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$ is called an *authentication code* ([**13**]) if

(1) the map $f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$ is surjective, and

(2) for each $e \in \mathcal{E}$, the map $f(\cdot, e) : \mathcal{S} \to \mathcal{M}$ defined by $s \mapsto f(s,e)$ is injective.

For an authentication code $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$, we say that the sets $\mathcal{S}$, $\mathcal{E}$ and $\mathcal{M}$ are the set of *source states*, the set of *encoding rules*, and the set of *messages*, respectively, and the map f is the *encoding map*. If $m = f(s,e)$ for $s \in \mathcal{S}$, $e \in \mathcal{E}$ and $m \in \mathcal{M}$, then we say that the source state s is encoded into the message m using the encoding rule e, and that for convenience, the message m is valid under the encoding rule e. The cardinals $|\mathcal{S}|$, $|\mathcal{E}|$, $|\mathcal{M}|$ are called the *size parameters* of the code. An authentication code with the size parameters $|\mathcal{S}| = k$, $|\mathcal{E}| = b$ and $|\mathcal{M}| = v$ is denoted by $AC(k,b,v)$.

An $AC(k,b,v)$ can be represented by a $b \times k$ matrix, called the *encoding matrix*, where the rows are indexed by encoding rules, the columns are indexed by source states, and the entry in row e and column s is $f(s,e)$. It is clear from the definition that the k entries in a row are all distinct, and every $m \in \mathcal{M}$ appears in the encoding matrix at least once. Conversely, if a matrix satisfies the above conditions, then it is the encoding matrix of an authentication code. Clearly, an authentication code is uniquely determined by its encoding matrix.

Authentication codes are used in communication channels where, besides the transmitter and the receiver, there may be individuals who want to deceive the receiver by

Received 3rd June, 2003
The first author was supported by NSF of China under No. 10001005. The second author was supported by Com^{2}MaC-KOSEF. The authors would like to thank Prof. Zhe-xian Wan for his suggestions regarding this paper.

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9727/04 $A2.00+0.00.

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press

either impersonating or substituting messages. By *impersonate* we mean that the deceiver sends a message through the channel to the receiver and hopes the receiver will accept it as authentic, that is, as a message sent by the transmitter. By *substitute* we mean that after the deceiver intercepts a message sent by the transmitter to the receiver, he/she sends another message instead and hopes the receiver will accept it as authentic. To protect against these deceits, the transmitter-receiver may use an authentication code which is publicly known and choose a fixed encoding rule e which is known only by the transmitter and the receiver. The set of information which the transmitter would like to transmit to the receiver should be identified with the set of source states of the code. Suppose that the transmitter wants to send a source state s to the receiver. To do this, the transmitter first encodes s into a message m using the encoding rule e, that is, $m = f(s,e)$, and then sends m to the receiver. After receiving a message m', the receiver first has to judge whether m' is authentic, that is, whether m' is valid under the fixed encoding rule e. If m' is valid under e, then m' is regarded as authentic and can be decoded by e to get a source state s', where $m' = f(s',e)$. If m' is not valid under e then m' is regarded as a false message. The object of the deceiver is to choose a message and send it to the receiver so that the probability of deceiving the receiver, that is, of causing the receiver to accept a message not sent by the transmitter as authentic, is as large as possible. We denote by P_I and P_S, respectively, the largest probabilities that the deceiver could deceive the receiver by impersonating and by substituting a message. We call them the probabilities of a successful impersonation and of a successful substitution, respectively. Throughout this paper, we *assume* that the source states and the encoding rules are chosen according to a uniform probability distribution.

For any $s \in \mathcal{S}$, let $\mathcal{M}(s) = \{f(s,e) \mid e \in \mathcal{E}\}$ and for any $e \in \mathcal{E}$, let $\mathcal{M}(e) = \{f(s,e) \mid s \in \mathcal{S}\}$. That is, $\mathcal{M}(e)$ is the set of messages which are valid under e. Furthermore for any $m \in \mathcal{M}$, let $\mathcal{E}(m) = \{e \in \mathcal{E} \mid m \in \mathcal{M}(e)\}$. The following lemma is elementary (see [**14**]).

Lemma 1. *For an authentication code $(\mathcal{S},\mathcal{E},\mathcal{M};f)$, we have*

$$P_I = \max_{m\in\mathcal{M}} \frac{|\mathcal{E}(m)|}{|\mathcal{E}|} \quad \textit{and} \quad P_S = \max_{m\neq m'\in\mathcal{M}} \frac{|\mathcal{E}(m)\cap\mathcal{E}(m')|}{|\mathcal{E}(m)|}.$$

The following well-known results ([**9, 12, 16**]) give conditions under which the deceiver can do no better.

Lemma 2. *In an $AC(k,b,v)$, we have*

$$P_I \geqslant \frac{k}{v} \quad \text{and} \quad P_S \geqslant \frac{k-1}{v-1}.$$

Furthermore,

(i) $P_I = k/v$ *if and only if* $|\mathcal{E}(m)| = bk/v$ *for any* $m \in \mathcal{M}$;

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press

(ii) *$P_I = k/v$ and $P_S = (k-1)/(v-1)$ if and only if $|\mathcal{E}(m)| = bk/v$ for any $m \in \mathcal{M}$ and $|\mathcal{E}(m) \cap \mathcal{E}(m')| = (bk(k-1))/(v(v-1))$ for any distinct $m, m' \in \mathcal{M}$.*

If $P_I = k/v$, we say that P_I is *optimal*, and if $P_S = (k-1)/(v-1)$, we say that P_S is *optimal*.

Constructions of authentication codes from some kinds of combinatorial designs have been obtained by Jimbo and Fuji-Hara (see [**7**]), Stinson (see [**14, 15, 16**]), and Rees and Stinson (see [**10**]). In [**14**], it was shown that the existence of optimal authentication codes is equivalent to the existence of some combinatorial designs. This will be reproved in Section 2 by a different description. In Section 3, isomorphic authentication codes are characterised and the relations of isomorphic authentication codes and corresponding isomorphic combinatorial designs are described. In Section 4, we enumerate the isomorphism classes of some special kinds of authentication codes.

2. Optimal authentication codes and combinatorial designs

Godlewski and Mitchell [4] gave the definition of several cryptosystems with secrecy (such as $U(L)$-secrecy, $S(L)$-secrecy, $O(L)$-secrecy, or $M(L)$-secrecy) and the characterisation of such systems with minimum number of encoding rules. In the following, the definition and some results on $U(L)$-secrecy are reviewed.

A subset $\mathcal{M}'$ of $\mathcal{M}$ is *allowable* if there exists an encoding rule e such that $\mathcal{M}' \subseteq \mathcal{M}(e)$. Given $L \geqslant 1$, an $AC(k,b,v)$ is said to provide *unordered perfect L-fold secrecy* (*$U(L)$-secrecy*) if, for every allowable L-subset $\mathcal{M}'$ of $\mathcal{M}$ and for every L-subset $\mathcal{S}'$ of $\mathcal{S}$, $p_{\mathcal{S}|\mathcal{M}}(\mathcal{S}'|\mathcal{M}') = p_{\mathcal{S}}(\mathcal{S}')$.

Theorem 1. [4] *If an $AC(k,b,v)$ provides $U(L)$-secrecy, then $b \geqslant (v/k) \cdot \binom{k}{L}$. Moreover, if $b = (v/k) \cdot \binom{k}{L}$ and $L \geqslant 2$, then for any two encoding rules e_1 and e_2 either $\mathcal{M}(e_1) = \mathcal{M}(e_2)$ or $\mathcal{M}(e_1)$ and $\mathcal{M}(e_2)$ are disjoint.*

It is easy to prove that if an $AC(k,b,v)$ provides $U(L)$-secrecy and $b = (v/k) \cdot \binom{k}{L}$ then P_I achieves its lower bound k/v. But if $L \geqslant 2$ in addition then $P_S = 1$. Therefore, in order to protect from the substitution attack, we are interested in $AC(k,b,v)$'s which provide $U(1)$-secrecy. Note that when $L = 1$ then all cryptosystems with secrecy defined in [4] coïncide and in fact equate to Shannon's notion of perfect secrecy [**11**]. So we call an $AC(k,b,v)$ which provides $U(1)$-secrecy an authentication code with *perfect secrecy*.

An important consideration in a construction of an authentication code is the number of its encoding rules. If there are b encoding rules, then $\log_2 b$ bits must be communicated in order to specify the encoding rule to be used. Hence, the number b is expected to be as small as possible. It is known from Theorem 1 that $b \geqslant v$ for any $AC(k,b,v)$ with perfect

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press

secrecy. It is said to be *(key-)minimal* if b achieves its lower bound v. The following theorem (Lemma 4.1 in [4]) gives a characterisation of a minimal authentication code with perfect secrecy.

Theorem 2. [4] *Let $(\mathcal{S},\mathcal{E},\mathcal{M};f)$ be an authentication code. Then it is minimal with perfect secrecy if and only if $|\mathcal{E}| = |\mathcal{M}|$ and for any $s \in \mathcal{S}$ and any $m \in \mathcal{M}$, there is an $e \in \mathcal{E}$ such that $m = f(s,e)$. In fact, such e exists uniquely.*

We say that an $AC(k,v,v)$ with perfect secrecy is *optimal* if both P_I and P_S are optimal. Such an authentication code can be characterised by a symmetric balanced incomplete block design, which is defined in the following.

A *balanced incomplete block design*, or a 2-(v,k,λ) design, is a pair $(X,\mathcal{B})$ which satisfies the following conditions:

(1) X is a set of *points* of cardinality v;

(2) $\mathcal{B}$ is a collection of k-subsets of X, called *blocks*;

(3) any two distinct points are contained in exactly λ blocks.

A balanced incomplete block design is called *symmetric* if the number of its points is equal to the number of its blocks. The following theorem can be found in [14]. For application of its structure information in Section 3, we reprove it by a different description.

Theorem 3. [14] *The existence of an $AC(k,v,v)$ with optimal P_I and optimal P_S is equivalent to the existence of a symmetric 2-(v,k,λ) design, where $\lambda = \big(k(k-1)\big)/(v-1)$.*

Proof: Suppose that $(\mathcal{S},\mathcal{E},\mathcal{M};f)$ is an $AC(k,v,v)$ with optimal P_I and optimal P_S. Let

$$X = \mathcal{M} \quad \text{and} \quad \mathcal{B} = \big\{\mathcal{M}(e) \mid e \in \mathcal{E}\big\}.$$

It is clear that $\big|\mathcal{M}(e)\big| = k$ for each $e \in \mathcal{E}$, and that for any message m, $m \in \mathcal{M}(e)$ if and only if $e \in \mathcal{E}(m)$. From Lemma 2, $(X,\mathcal{B})$ is a symmetric 2-(v,k,λ) design, where $\lambda = \big(k(k-1)\big)/(v-1)$. We call such a design the symmetric balanced incomplete block design *induced* from an $AC(k,v,v)$ with optimal P_I and optimal P_S.

Conversely, suppose $(X,\mathcal{B})$ is a symmetric 2-(v,k,λ) design with $\lambda = \big(k(k-1)\big)/(v-1)$. It is clear that $|\mathcal{B}| = v$. Let $\mathcal{S}$ be any set with k elements, $\mathcal{E} = \mathcal{B} = \{B_1, B_2, \ldots, B_v\}$, and $\mathcal{M} = X = \{x_1, x_2, \ldots, x_v\}$. For any $B_i \in \mathcal{E}$, B_i is a k-element subset of $\mathcal{M}$. Since $|\mathcal{S}| = |B_i| = k$, there are bijections between $\mathcal{S}$ and B_i. For any $1 \leqslant i \leqslant v$, choose a bijection $g_i : \mathcal{S} \to B_i$ to order the elements of B_i. Define $f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$ by $f(s,B_i) = g_i(s)$ for any $s \in \mathcal{S}$ and any $B_i \in \mathcal{E}$. Since any two elements x_i, x_j of X are contained in the blocks in $\mathcal{E}(x_i) \cap \mathcal{E}(x_j)$, it follows easily that $(\mathcal{S},\mathcal{E},\mathcal{M};f)$ constructed above has optimal P_I and optimal P_S by Lemma 2. We call such an $AC(k,v,v)$ an authentication code *induced* from a symmetric 2-(v,k,λ) design. $\square$

Two authentication codes $(\mathcal{S}_i,\mathcal{E}_i,\mathcal{M}_i;f_i)$ $(i = 1,2)$ are said to be *isomorphic* [3] if

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press

there exist bijections

$$\sigma_{\mathcal{S}} : \mathcal{S}_1 \to \mathcal{S}_2, \quad \sigma_{\mathcal{E}} : \mathcal{E}_1 \to \mathcal{E}_2 \quad \text{and} \quad \sigma_{\mathcal{M}} : \mathcal{M}_1 \to \mathcal{M}_2$$

such that

$$f_2(\sigma_{\mathcal{S}}(s), \sigma_{\mathcal{E}}(e)) = \sigma_{\mathcal{M}}(f_1(s, e))$$

for any $s \in \mathcal{S}_1$ and any $e \in \mathcal{E}_1$. The triple $(\sigma_{\mathcal{S}}, \sigma_{\mathcal{E}}, \sigma_{\mathcal{M}})$ is called an *isomorphism* between the two authentication codes. It is clear that two isomorphic authentication codes have the same size parameters and the same probabilities of successful deceit. In particular, if one of them has optimal P_I and(or) optimal P_S, so does the other.

EXAMPLE. The symmetric balanced incomplete block design induced from an $AC(k, v, v)$ with optimal P_I and optimal P_S is unique. But we can construct more than one non-isomorphic $AC(k, v, v)$'s from a symmetric balanced incomplete block design. As an example, let $X = \{x_1, x_2, x_3\}$ and $\mathcal{B} = \{B_1, B_2, B_3\}$, where $B_1 = \{x_1, x_2\}$, $B_2 = \{x_2, x_3\}$, and $B_3 = \{x_3, x_1\}$. Then $(X, \mathcal{B})$ is a 2-$(3, 2, 1)$ design. Set $\mathcal{S} = \{s_1, s_2\}$, $\mathcal{E} = \{B_1, B_2, B_3\}$, $\mathcal{M} = \{x_1, x_2, x_3\}$, $f_1(s_1, B_1) = f_2(s_1, B_1) = x_1$, $f_1(s_2, B_1) = f_2(s_2, B_1) = x_2$, $f_1(s_1, B_2) = f_2(s_1, B_2) = x_2$, $f_1(s_2, B_2) = f_2(s_2, B_2) = x_3$, $f_1(s_1, B_3) = f_2(s_2, B_3) = x_3$ and $f_1(s_2, B_3) = f_2(s_1, B_3) = x_1$. Then $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f_1)$ and $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f_2)$ are non-isomorphic $AC(2, 3, 3)$'s induced from $(X, \mathcal{B})$, by noting that $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f_1)$ is an authentication code with perfect secrecy, but $(\mathcal{S}, \mathcal{E}, \mathcal{M};\ f_2)$ is not.

In general, we have the following theorem.

THEOREM 4. *At least one of the authentication codes induced from a symmetric balanced incomplete block design has perfect secrecy.*

PROOF: Let $(X, \mathcal{B})$ be a symmetric 2-(v, k, λ) design, where $\lambda = \big(k(k-1)\big)/(v-1)$. First, we construct a bipartite graph G having bipartition $(\mathcal{B}, X)$, where $\{B_i, x_j\}$, $B_i \in \mathcal{B}$, $x_j \in X$, is an edge if and only if $x_j \in B_i$. It is clear that G is a k-regular bipartite graph. By König's Theorem [8], the bipartite graph G is k-edge-colourable. Let G be edge-coloured by the colours $C_1, C_2, \ldots, C_k$ and let $\mathcal{S} = \{C_1, C_2, \ldots, C_k\}$. Set $\mathcal{E} = \mathcal{B}$ and $\mathcal{M} = X$. For any $e = B_i \in \mathcal{E}$, define a bijection $g_i : \mathcal{S} \to B_i$ as $g_i(s) = m$, where $\{e, m\}$ is an edge coloured by s. That is, the encoding map $f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$ is defined by $f(s, e) = m$ for any $s \in \mathcal{S}$ and $e \in \mathcal{E}$, where $\{e, m\}$ is an edge of the graph G coloured by s. Then, for any $m \in \mathcal{M}$ and any $s \in \mathcal{S}$, there is a unique edge incident with m and has colour s. The other end of this edge is an encoding rule e satisfying $m = f(s, e)$. By Lemma 2 and Theorem 2, the constructed code is an optimal one with perfect secrecy. ▯

Combined Theorems 3 and 4, we get that the existence of an $AC(k, v, v)$ with perfect secrecy is equivalent to the existence of a symmetric 2-(v, k, λ) design, where $\lambda = \big(k(k-1)\big)/(v-1)$.

Next, we consider Cartesian authentication codes. An authentication code is called a *Cartesian* one if for any message m, there is a source state $s \in \mathcal{S}$ such that $p(s \mid m) = 1$

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press

and $p(s' \mid m) = 0$ for any $s' \neq s$, that is, for any message m there is a unique source state s such that $m = f(s,e)$ for every encoding rule e under which m is valid. Therefore, a Cartesian authentication code provides no secrecy. The following lemma can be found in [**15**].

Lemma 3. *For a Cartesian $AC(k,b,v)$ with optimal P_I, we have that k is a divisor of v, $|\mathcal{M}(s)| = v/k$ for any $s \in \mathcal{S}$, and $P_S \geqslant k/v$. The equality holds if and only if for any distinct messages m and m',*

$$|\mathcal{E}(m) \cap \mathcal{E}(m')| = \begin{cases} 0 & \text{if } m,\ m' \in \mathcal{M}(s) \text{ for an } s \in \mathcal{S}, \\ \dfrac{bk^2}{v^2} & \text{otherwise.} \end{cases}$$

Furthermore, if $P_I = P_S = k/v$, then $b \geqslant (v/k)^2$.

Hence, we say that a Cartesian authentication code is *optimal* if $P_I \doteq P_S = k/v$ and $b = (v/k)^2$.

A *transversal design* [**6**] $TD(k,\lambda,n)$ is a triple $(X,\mathcal{G},\mathcal{B})$ which satisfies the following conditions:

(1) X is a set of kn elements, called *points*;

(2) $\mathcal{G}$ is a partition of X into k subsets of n points, called *groups*;

(3) $\mathcal{B}$ is a set of λn^2 subsets of X, called *blocks*, such that a group and a block contain exactly one common point;

(4) every pair of points from distinct groups occurs in exactly λ blocks.

Theorem 5. [**15**] *The existence of an optimal Cartesian $AC(k,b,v)$ is equivalent to the existence of a transversal design $TD\big(k,1,(v/k)\big)$.*

Proof: Suppose that $(\mathcal{S},\mathcal{E},\mathcal{M};f)$ is an optimal Cartesian $AC(k,b,v)$. Let

$$X = \mathcal{M}, \quad \mathcal{G} = \{\mathcal{M}(s) \mid s \in \mathcal{S}\} \quad \text{and} \quad \mathcal{B} = \{\mathcal{M}(e) \mid e \in \mathcal{E}\}.$$

For any $s \in \mathcal{S}$ and any $e \in \mathcal{E}$, if $x,\ y \in \mathcal{M}(s) \cap \mathcal{M}(e)$, then $x = f(s,e) = y$, that is, $|\mathcal{M}(s) \cap \mathcal{M}(e)| = 1$. Therefore, $(X,\mathcal{G},\mathcal{B})$ is a $TD\big(k,1,(v/k)\big)$ by Lemma 3. We call it the transversal design *induced* from an optimal Cartesian $AC(k,b,v)$.

Conversely, let $(X,\mathcal{G},\mathcal{B})$ be a $TD(k,1,n)$ with $n = v/k$. Set

$$\mathcal{S} = \mathcal{G}, \quad \mathcal{E} = \mathcal{B} \quad \text{and} \quad \mathcal{M} = X.$$

For any $G_i \in \mathcal{G}$ and any $B_j \in \mathcal{B}$, let $G_i \cap B_j = \{x\}$. Define an encoding map $f : \mathcal{S} \times \mathcal{B} \to X$ by $f(G_i, B_j) = x$. It is easy to check from Lemma 3 that the $(\mathcal{S},\mathcal{E},\mathcal{M};f)$ constructed is an optimal Cartesian $AC(k,b,v)$. We call it the optimal Cartesian $AC(k,b,v)$ *induced* from a transversal design. $\square$

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press

3. Characterisations of isomorphic authentication codes

Feng and Wan [3] proved the following lemma.

Lemma 4. *Two authentication codes $(\mathcal{S}_i, \mathcal{E}_i, \mathcal{M}_i; f_i)$ $(i = 1, 2)$ are isomorphic if and only if $|\mathcal{M}_1| = |\mathcal{M}_2|$, and there are bijections $\sigma_\mathcal{S} : \mathcal{S}_1 \to \mathcal{S}_2$ and $\sigma_\mathcal{E} : \mathcal{E}_1 \to \mathcal{E}_2$ such that $f_2\big(\sigma_\mathcal{S}(s), \sigma_\mathcal{E}(e)\big) = f_2\big(\sigma_\mathcal{S}(s'), \sigma_\mathcal{E}(e')\big)$ whenever $f_1(s, e) = f_1(s', e')$ for any s, $s' \in \mathcal{S}_1$ and any e, $e' \in \mathcal{E}_1$.*

This characterisation for isomorphic authentication codes can be expressed in matrix form.

Theorem 6. *Let $(\mathcal{S}_1, \mathcal{E}_1, \mathcal{M}_1; f_1)$ and $(\mathcal{S}_2, \mathcal{E}_2, \mathcal{M}_2; f_2)$ be two $AC(k, b, v)$'s with encoding matrices A and B, respectively. Then $(\mathcal{S}_1, \mathcal{E}_1, \mathcal{M}_1; f_1)$ and $(\mathcal{S}_2, \mathcal{E}_2, \mathcal{M}_2; f_2)$ are isomorphic if and only if there exists a $b \times b$ permutation matrix P, a $k \times k$ permutation matrix Q and a bijection σ from $\mathcal{M}_1$ to $\mathcal{M}_2$ such that $B = P\sigma(A)Q$, where $\sigma(A) = \big(\sigma(a_{ij})\big)$ for $A = (a_{ij})$.*

Proof: Let $\mathcal{S}_\ell = \{s_j^{(\ell)} \mid 1 \leqslant j \leqslant k\}$ and $\mathcal{E}_\ell = \{e_i^{(\ell)} \mid 1 \leqslant i \leqslant b\}$ $(\ell = 1,\ 2)$. Suppose that $(\mathcal{S}_1, \mathcal{E}_1, \mathcal{M}_1; f_1)$ and $(\mathcal{S}_2, \mathcal{E}_2, \mathcal{M}_2; f_2)$ are isomorphic by an isomorphism $(\sigma_\mathcal{S}, \sigma_\mathcal{E}, \sigma_\mathcal{M})$. Define two square matrices $P = (p_{ij})$ and $Q = (q_{ij})$ by

$$p_{ij} = \begin{cases} 1 & \text{if } \sigma_\mathcal{E}(e_j^{(1)}) = e_i^{(2)}, \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad q_{ij} = \begin{cases} 1 & \text{if } \sigma_\mathcal{S}(s_i^{(1)}) = s_j^{(2)}, \\ 0 & \text{otherwise.} \end{cases}$$

Clearly, P and Q are permutation matrices, and $B = P\sigma_\mathcal{M}(A)Q$.

Conversely, suppose that there exists a $b \times b$ permutation matrix P, a $k \times k$ permutation matrix Q and a bijection σ from $\mathcal{M}_1$ to $\mathcal{M}_2$ such that $B = P\sigma(A)Q$. Let $P = (p_{ij})$ and $Q = (q_{ij})$. Define $\sigma_\mathcal{S} : \mathcal{S}_1 \to \mathcal{S}_2$ by $\sigma_\mathcal{S}(s_i^{(1)}) = s_j^{(2)}$ if $q_{ij} = 1$ for any $s_i^{(1)} \in \mathcal{S}_1$. Define $\sigma_\mathcal{E} : \mathcal{E}_1 \to \mathcal{E}_2$ by $\sigma_\mathcal{E}(e_j^{(1)}) = e_i^{(2)}$ if $p_{ij} = 1$ for any $e_j^{(1)} \in \mathcal{E}_1$. Let $\sigma_\mathcal{M} = \sigma$. Then $f_2\big(\sigma_\mathcal{S}(s_j), \sigma_\mathcal{E}(e_i)\big) = \sigma_\mathcal{M}\big(f_1(s_j, e_i)\big)$ for any $s_j \in \mathcal{S}_1$ and any $e_i \in \mathcal{E}_1$. That is, $(\mathcal{S}_1, \mathcal{E}_1, \mathcal{M}_1; f_1)$ and $(\mathcal{S}_2, \mathcal{E}_2, \mathcal{M}_2; f_2)$ are isomorphic. ∎

Two balanced incomplete block designs $(X_1, \mathcal{B}_1)$ and $(X_2, \mathcal{B}_2)$ are said to be *isomorphic* [1] if there is a bijection α from X_1 onto X_2 which induces a bijection from $\mathcal{B}_1$ onto $\mathcal{B}_2$, that is, for any $B \in \mathcal{B}_1$, $\alpha(B) = \big\{\alpha(x) : x \in B\big\} \in \mathcal{B}_2$. In this case, we call α an *isomorphism* between these two balanced incomplete block designs. Similarly, two transversal designs $(X_1, \mathcal{G}_1, \mathcal{B}_1)$ and $(X_2, \mathcal{G}_2, \mathcal{B}_2)$ are said to be *isomorphic* if there is a bijection $\alpha : X_1 \to X_2$ which induces bijections from $\mathcal{G}_1$ onto $\mathcal{G}_2$ and from $\mathcal{B}_1$ onto $\mathcal{B}_2$.

Theorem 7. *The two symmetric balanced incomplete block designs induced from two isomorphic optimal minimal authentication codes with perfect secrecy are isomorphic.*

Proof: Let $(\mathcal{S}_i, \mathcal{E}_i, \mathcal{M}_i; f_i)$ $(i = 1,\ 2)$ be two isomorphic optimal minimal authentication codes with perfect secrecy and let $(\sigma_\mathcal{S}, \sigma_\mathcal{E}, \sigma_\mathcal{M})$ be an isomorphism between

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press

them. Let $(X_i, \mathcal{B}_i)$ $(i = 1,\ 2)$ be the balanced incomplete block designs induced from $(\mathcal{S}_i, \mathcal{E}_i, \mathcal{M}_i; f_i)$. As in the proof of Theorem 3, $X_i = \mathcal{M}_i$ and $\mathcal{B}_i = \{\mathcal{M}(e) \mid e \in \mathcal{E}_i\}$. Let $\alpha = \sigma_{\mathcal{M}}$. Then α is a bijection from X_1 onto X_2. Furthermore, for any $\mathcal{M}(e) \in \mathcal{B}_1$ with $e \in \mathcal{E}_1$,

$$\begin{aligned}\alpha(\mathcal{M}(e)) &= \sigma_{\mathcal{M}}(\mathcal{M}(e)) \\ &= \{\sigma_{\mathcal{M}} f_1(s, e) \mid s \in \mathcal{S}_1\} \\ &= \left\{f_2(\sigma_{\mathcal{S}}(s), \sigma_{\mathcal{E}}(e)) \mid s \in \mathcal{S}_1\right\} \\ &= \left\{f_2(t, \sigma_{\mathcal{E}}(e)) \mid t \in \mathcal{S}_2\right\} \\ &= \mathcal{M}(\sigma_{\mathcal{E}}(e)) \in \mathcal{B}_2.\end{aligned}$$

Thus, α induces a bijection from $\mathcal{B}_1$ onto $\mathcal{B}_2$. That is, $(X_1, \mathcal{B}_1)$ and $(X_2, \mathcal{B}_2)$ are isomorphic. □

Authentication codes induced from a symmetric balanced incomplete block design cannot be unique. However, we have the following theorem.

Theorem 8. *Let $(X_i, \mathcal{B}_i)$ $(i = 1,\ 2)$ be two isomorphic symmetric balanced incomplete block designs. Then, for any optimal minimal authentication code with perfect secrecy induced from $(X_1, \mathcal{B}_1)$, there is an optimal minimal authentication code with perfect secrecy induced from $(X_2, \mathcal{B}_2)$ which is isomorphic to it.*

Proof: Let α be an isomorphism between $(X_1, \mathcal{B}_1)$ and $(X_2, \mathcal{B}_2)$, and let $(\mathcal{S}_1, \mathcal{E}_1, \mathcal{M}_1; f_1)$ be an optimal minimal authentication code with perfect secrecy induced from $(X_1, \mathcal{B}_1)$. Then $\mathcal{S}_1$ is a set with k elements, $\mathcal{E}_1 = \mathcal{B}_1$ and $\mathcal{M}_1 = X_1$. For each $B_j^{(1)} \in \mathcal{B}_1$, let $g_j^{(1)}$ be the bijection chosen from $\mathcal{S}_1$ onto $B_j^{(1)}$, that is, $f_1(s, B_j^{(1)}) = g_j^{(1)}(s)$. Take $\mathcal{S}_2 = \mathcal{S}_1$, $\mathcal{E}_2 = \mathcal{B}_2$ and $\mathcal{M}_2 = X_2$. For any $B_i^{(2)} \in \mathcal{E}_2$, let $B_j^{(1)} = \alpha^{-1}(B_i^{(2)})$ and define $g_i^{(2)} = \alpha \circ g_j^{(1)}$. Then $g_i^{(2)}$ is a bijection from $\mathcal{S}_2$ $(= \mathcal{S}_1)$ onto $B_i^{(2)}$. Define an encoding map $f_2 : \mathcal{S}_2 \times \mathcal{E}_2 \to \mathcal{M}_2$ as $f_2(s, B_i^{(2)}) = g_i^{(2)}(s)$ for any $s \in \mathcal{S}_2$. It is clear that $(\mathcal{S}_2, \mathcal{E}_2, \mathcal{M}_2; f_2)$ is an optimal minimal authentication code with perfect secrecy induced from $(X_2, \mathcal{B}_2)$. Let

$$\sigma_{\mathcal{S}} = 1_{\mathcal{S}_1}, \quad \sigma_{\mathcal{E}} = \sigma_{\mathcal{M}} = \alpha.$$

Then, for any $s \in \mathcal{S}_1$, $B_j^{(1)} \in \mathcal{B}_1$, we have

$$\begin{aligned}f_2(\sigma_{\mathcal{S}}(s), \sigma_{\mathcal{E}}(B_j^{(1)})) &= f_2(s, B_i^{(2)}) \\ &= g_i^{(2)}(s) \\ &= \alpha(g_j^{(1)}(s)) \\ &= \sigma_{\mathcal{M}}(f_1(s, B_j^{(1)})).\end{aligned}$$

Thus, $(\mathcal{S}_2, \mathcal{E}_2, \mathcal{M}_2; f_2)$ is isomorphic to $(\mathcal{S}_1, \mathcal{E}_1, \mathcal{M}_1; f_1)$. □

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press

Similarly, for an optimal Cartesian authentication code, we have the following theorem.

Theorem 9. *Two optimal Cartesian authentication codes are isomorphic if and only if the induced transversal designs are isomorphic.*

4. Numbers of some kinds of authentication codes

The classification of authentication codes, or the enumeration of the isomorphism classes of authentication codes is one of the most important problems in the study of authentication theory. In the following, let $n \geqslant 2$.

Theorem 10. *There exists one and only one optimal Cartesian $AC(2, n^2, 2n)$ for each $n \geqslant 2$.*

Proof: Existence Let $\mathcal{S} = \{s_1, s_2\}$, $\mathcal{E} = \{e_1, e_2, \dots, e_{n^2}\}$ and $\mathcal{M} = \{(s_i, j) \mid 1 \leqslant i \leqslant 2,\ 1 \leqslant j \leqslant n\}$. The encoding matrix

$$(1)\qquad \left[\underbrace{\begin{matrix}(s_1,1) & \cdots & (s_1,1)\\ (s_2,1) & \cdots & (s_2,n)\end{matrix}}_{n}\ \underbrace{\begin{matrix}(s_1,2) & \cdots & (s_1,2)\\ (s_2,1) & \cdots & (s_2,n)\end{matrix}}_{n}\ \begin{matrix}\cdots\\ \cdots\end{matrix}\ \underbrace{\begin{matrix}(s_1,n) & \cdots & (s_1,n)\\ (s_2,1) & \cdots & (s_2,n)\end{matrix}}_{n}\right]^t$$

gives an optimal Cartesian $AC(2, n^2, 2n)$.

Uniqueness. For an optimal Cartesian $AC(2, n^2, 2n)$, $|\mathcal{E}(m)| = n$ for any $m \in \mathcal{M}$ by Lemma 2, $|\mathcal{M}(s)| = n$ for any $s \in \mathcal{S}$, and any two messages which correspond to different source states are contained in a unique encoding rule simultaneously by Lemma 3. Suppose that $\mathcal{M} = \{m_\ell : 1 \leqslant \ell \leqslant 2n\}$. By interchanging the rows of its encoding matrix if necessary, we can assume that its first column is of the form

$$(\underbrace{m_1, \dots, m_1}_{n}, \underbrace{m_2, \dots, m_2}_{n}, \dots, \underbrace{m_n, \dots, m_n}_{n})^t$$

The subblock in the second column corresponding to subblock $(\underbrace{m_i, \dots, m_i}_{n})$ $(1 \leqslant i \leqslant n)$ in the first column is a permutation of $m_{n+1}, m_{n+2}, \dots, m_{2n}$. By interchanging the rows in this encoding matrix again, we can assume that its second column is

$$(m_{n+1}, \dots, m_{2n}, m_{n+1}, \dots, m_{2n}, \dots, m_{n+1}, \dots, m_{2n})^t.$$

Since the authentication code obtained by interchanging the rows of the encoding matrix is isomorphic to the original one, every optimal Cartesian $AC(2, n^2, 2n)$ is isomorphic to one whose encoding matrix is of the form (1). So any two optimal Cartesian $AC(2, n^2, 2n)$'s are isomorphic. □

Next, we enumerate the isomorphism classes of $AC(2, n, n)$'s with perfect secrecy. Clearly, there exists such an $AC(2, n, n)$. Also, we know that $P_I = 2/n$ for any $AC(2, n, n)$

with perfect secrecy (see [**2**]). In the encoding matrix of an $AC(2,n,n)$ with perfect secrecy, each column is a permutation of the n messages. For convenience, let the messages be 1, 2, ..., n. Suppose the first column of its encoding matrix is $(i_1, i_2, \ldots, i_n)^t$ and the second one is $(j_1, j_2, \ldots, j_n)^t$. Then the $AC(2,n,n)$ with perfect secrecy can be represented by the permutation

$$P = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}.$$

We call P the *permutation representation* of the code $AC(2,n,n)$.

THEOREM 11. *Two $AC(2,n,n)$'s with perfect secrecy are isomorphic if and only if their permutation representations have the same cycle type.*

PROOF: Suppose that two $AC(2,n,n)$'s $(\mathcal{S}_i, \mathcal{E}_i, \mathcal{M}_i; f_i)$ $(i = 1,2)$ with perfect secrecy are isomorphic by an isomorphism $(\sigma_{\mathcal{S}}, \sigma_{\mathcal{E}}, \sigma_{\mathcal{M}})$. Let $\mathcal{S}_i = \{s_1^{(i)}, s_2^{(i)}\}$ $(i = 1,2)$ and let the permutation representation of $(\mathcal{S}_1, \mathcal{E}_1, \mathcal{M}_1; f_1)$ be

$$P = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}.$$

If $\sigma_{\mathcal{S}}(s_1^{(1)}) = s_1^{(2)}$, then the permutation representation of $(\mathcal{S}_2, \mathcal{E}_2, \mathcal{M}_2; f_2)$ is

$$Q = \begin{pmatrix} \sigma_{\mathcal{M}}(i_1) & \sigma_{\mathcal{M}}(i_2) & \cdots & \sigma_{\mathcal{M}}(i_n) \\ \sigma_{\mathcal{M}}(j_1) & \sigma_{\mathcal{M}}(j_2) & \cdots & \sigma_{\mathcal{M}}(j_n) \end{pmatrix}.$$

Since $\sigma_{\mathcal{M}}$ is a bijection, P and Q have the same cycle type. If $\sigma_{\mathcal{S}}(s_1^{(1)}) = s_2^{(2)}$, then the permutation representation of $(\mathcal{S}_2, \mathcal{E}_2, \mathcal{M}_2; f_2)$ is

$$Q^{-1} = \begin{pmatrix} \sigma_{\mathcal{M}}(j_1) & \sigma_{\mathcal{M}}(j_2) & \cdots & \sigma_{\mathcal{M}}(j_n) \\ \sigma_{\mathcal{M}}(i_1) & \sigma_{\mathcal{M}}(i_2) & \cdots & \sigma_{\mathcal{M}}(i_n) \end{pmatrix}.$$

Since Q^{-1} and Q have the same cycle type, so do P and Q^{-1}.

Conversely, suppose that the permutation representations P_1 and P_2 of two $AC(2,n,n)$'s with perfect secrecy $(\mathcal{S}_i, \mathcal{E}_i, \mathcal{M}_i; f_i)$ $(i = 1,2)$ have the same cycle type. Let $\mathcal{S}_i = \{s_1^{(i)}, s_2^{(i)}\}$, $\mathcal{E}_i = \{e_1^{(i)}, e_2^{(i)}, \ldots, e_n^{(i)}\}$, $\mathcal{M}_i = \{1^{(i)}, 2^{(i)}, \ldots, n^{(i)}\}$, and let the cyclic representations of P_1 and P_2 be

$$P_1 = \left(i_1^{(1)} i_2^{(1)} \cdots i_t^{(1)}\right) \left(i_{t+1}^{(1)} i_{t+2}^{(1)} \cdots i_\ell^{(1)}\right) \cdots \left(i_{s+1}^{(1)} i_{s+2}^{(1)} \cdots i_n^{(1)}\right),$$
$$P_2 = \left(j_1^{(2)} j_2^{(2)} \cdots j_t^{(2)}\right) \left(j_{t+1}^{(2)} j_{t+2}^{(2)} \cdots j_\ell^{(2)}\right) \cdots \left(j_{s+1}^{(2)} j_{s+2}^{(2)} \cdots j_n^{(2)}\right).$$

Define $\sigma_{\mathcal{S}}$, $\sigma_{\mathcal{E}}$ and $\sigma_{\mathcal{M}}$ by

$$\sigma_{\mathcal{S}} : s_i^{(1)} \mapsto s_i^{(2)}, \quad i = 1,2,$$
$$\sigma_{\mathcal{E}} : e_{i_r}^{(1)} \mapsto e_{j_r}^{(2)}, \quad 1 \leqslant r \leqslant n,$$
$$\sigma_{\mathcal{M}} : i_r^{(1)} \mapsto j_r^{(2)}, \quad 1 \leqslant r \leqslant n.$$

From Lemma 4, it can be proved that $(\sigma_S, \sigma_{\mathcal{E}}, \sigma_{\mathcal{M}})$ is an isomorphism between these two codes. □

The number of the cycle types of permutations on n elements is the number of partitions of n into positive parts and is normally denoted by $p(n)$. A recurrence formula for calculating $p(n)$ and its values up to $n = 100$ can be found in [5]. It is also the number of non-negative integer solutions $(\ell_1, \ell_2, \dots, \ell_n)$ of the equation $\sum_{i=1}^{n} i\ell_i = n$. For the permutation representation of an $AC(2,n,n)$ with perfect secrecy, $\ell_1 = 0$. If $\ell_2 \neq 0$, then its encoding matrix has two rows containing i, j and j, i, respectively, and these two messages i and j do not appear in other rows. So, $\mathcal{E}(i) = \mathcal{E}(j)$ and then $P_S = 1$. If $\ell_2 = 0$, then each pair of messages appear in at most one row. Therefore, $P_S = 1/2$. That is,

$$P_S = \begin{cases} 1 & \text{if } \ell_2 \neq 0, \\ \dfrac{1}{2} & \text{if } \ell_2 = 0. \end{cases}$$

Denote, by $N_k(n)$, the number of non-negative integer solutions $(\ell_k, \ell_{k+1}, \dots, \ell_n)$ of the equation $\sum_{i=k}^{n} i\ell_i = n$. So $p(n) = N_1(n)$. Since $N_k(n)$ is the number of partitions of n with smallest part at least k and $N_{k+1}(n)$ is the number of partitions of n with smallest part at least $k+1$, it follows that $N_k(n) - N_{k+1}(n)$ is the number of partitions of n with smallest part exactly k. By removing one part of size k from each such partition, it can be seen that there is a one-one correspondence between these partitions and the partitions of $n-k$ with smallest part at least k. Hence

$$N_k(n) - N_{k+1}(n) = N_k(n-k),$$

so

$$N_{k+1}(n) = N_k(n) - N_k(n-k). \tag{2}$$

By repeated use of (2), we have $N_2(n) = p(n) - p(n-1)$ and $N_3(n) = p(n) - p(n-1) - p(n-2) + p(n-3)$. Therefore, we have the following theorem.

Theorem 12. *For $n \geqslant 3$, the number of isomorphism classes of $AC(2,n,n)$'s with perfect secrecy is*

$$\begin{cases} N_2(n-2) = p(n-2) - p(n-3) & \textit{if } P_S = 1, \\ N_3(n) = p(n) - p(n-1) - p(n-2) + p(n-3) & \textit{if } P_S = \dfrac{1}{2}, \\ 0 & \textit{otherwise}, \end{cases}$$

where $p(n)$ is the number of partitions of n and $p(0) = 1$.

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press

The numbers of isomorphism classes of $AC(2,n,n)$'s with perfect secrecy for a small n are listed in the following table.

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	$\cdots$
$P_S=1$	0	1	1	2	2	4	4	7	8	12	14	21	24	34	$\cdots$
$P_S=\frac{1}{2}$	1	1	1	2	2	3	4	5	6	9	10	13	17	21	$\cdots$
Total	1	2	2	4	4	7	8	12	14	21	24	34	41	55	$\cdots$

EXAMPLE. The encoding matrices of the four non-isomorphic $AC(2,8,8)$'s with perfect secrecy and $P_S=1$ are

$$\begin{bmatrix}1&2\\2&1\\3&4\\4&3\\5&6\\6&5\\7&8\\8&7\end{bmatrix},\quad \begin{bmatrix}1&2\\2&1\\3&4\\4&5\\5&3\\6&7\\7&8\\8&6\end{bmatrix},\quad \begin{bmatrix}1&2\\2&1\\3&4\\4&3\\5&6\\6&7\\7&8\\8&5\end{bmatrix}\quad\text{and}\quad \begin{bmatrix}1&2\\2&1\\3&4\\4&5\\5&6\\6&7\\7&8\\8&3\end{bmatrix}.$$

The encoding matrices of the three non-isomorphic $AC(2,8,8)$'s with perfect secrecy and $P_S=1/2$ are

$$\begin{bmatrix}1&2\\2&3\\3&1\\4&5\\5&6\\6&7\\7&8\\8&4\end{bmatrix},\quad \begin{bmatrix}1&2\\2&3\\3&4\\4&1\\5&6\\6&7\\7&8\\8&5\end{bmatrix}\quad\text{and}\quad \begin{bmatrix}1&2\\2&3\\3&4\\4&5\\5&6\\6&7\\7&8\\8&1\end{bmatrix}.$$

REFERENCES

[1] T. Beth, D. Jungnickel and H. Lenz, *Design theory* (Cambridge University Press, Cambridge, 1993).

[2] R. Feng and J.H. Kwak, 'Minimal authentication codes with perfect secrecy', (preprint).

[3] R. Feng and Z. Wan, 'A construction of cartesian authentication codes from vector space and dual authentication codes', *Northeast. Math. J.* **13** (1997), 63–72.

[4] P. Godlewski and C. Mitchell, 'Key-minimal cryptosystems for unconditional secrecy', *J. Cryptology* **3** (1990), 1–25.

[5] M. Hall, Jr., *Combinatorial theory*, (2nd Edition) (John Wiley and Sons Inc., New York, 1986).

[6] H. Hanani, 'On transversal designs', in *Theory of deisgns, finite geometry and coding theory*, Math. Centre Tracts **55**, 1974, **pp.** 42–52.

[7] M. Jimbo and R. Fuji-Hara, 'Optimal authentication systems and combinatorial designs', *IEEE Trans. Inform. Theory* **36** (1990), 54–62.

[8] D. König, 'Über Graphen und ihre Anwendung anf Determinantentheorie und Mengenlehre', *Math. Ann.* **77** (1916), 453–465.

[9] J.L. Massey, 'Cryptography – a selective survey', in *Digital Communications* (North-Holland, Amsterdam, 1986), **pp.** 3–21.

[10] R.S. Rees and D.R. Stinson, 'Combinatorial characterizations of authentication codes II', *Des. Codes Cryptogr.* **7** (1996), 239–259.

[11] C.E. Shannon, 'Communication theory of secrecy systems', *Bell System Technical Journal* **28** (1949), 656–715.

[12] G.L. Simmons, 'Message authentication: a game on hypergraphs', *Congr. Numer.* **45** (1984), 161–192.

[13] G.L. Simmons, 'Authentication theory/coding theory', in *Advances in Cryptology-Crypto'84*, (G.R. Blakley and D. Chaum, Editors), Lecture Notes in Computer Science **196** (Springer-Verlag, Berlin, 1985), **pp.** 411–431.

[14] D.R. Stinson, 'Some constructions and bounds for authentication codes', *J. Cryptology* **1** (1988), 37–51.

[15] D.R. Stinson, 'The combinatorics of authentication and secrecy codes', *J. Cryptology* **2** (1990), 23–49.

[16] D.R. Stinson, 'Combinatorial characterizations of authentication codes', *Des. Codes Cryptogr.* **2** (1992), 175–187.

LMAM, School of Mathematical Sciences
Peking University
Beijing 100871
People's Republic China
and
State Key Laboratory of Information Security
Graduate School of USTC
Beijing 100039
People's Republic of China
e-mail: fengrq@math.pku.edu.cn

Department of Mathematics
Pohang University of Science and Technology
Pohang 790-784
Korea
e-mail: jinkwak@postech.ac.kr

Faculty of Mathematical Studies
University of Southampton
Southampton SO17 1BJ
United Kingdom
e-mail: ekl@soton.ac.uk

https://doi.org/10.1017/S0004972700035942 Published online by Cambridge University Press