New Combinatorial Designs and their Applications to Authentication Codes and Secret Sharing Schemes

Wakaha Ogata[1] Kaoru Kurosawa[2] Douglas R. Stinson[3]
Hajime Saido[4]

[1] Center for Research on Advanced Financial Technology,
Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152, Japan
wakaha@ss.titech.ac.jp

[2] Department of Computer and Information Sciences,
Ibaraki University
4-12-1 Nakanarusawa, Hitachi, Ibaraki, 316-8511, Japan
kurosawa@cis.ibaraki.ac.jp

[3] School of Computer Science
University of Waterloo
Waterloo Ontario, N2L 3G1, Canada
dstinson@uwaterloo.ca

[4] Department of Communication and Integrated Systems,
Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152, Japan

Abstract. This paper introduces three new types of combinatorial designs, which we call external difference families (EDF), external BIBDs (EBIBD) and splitting BIBDs. An EDF is a special type of EBIBD, so existence of an EDF implies existence of an EBIBD.

We construct optimal splitting A-codes by using EDF. Then we give a new bound on the number of shares required in robust secret sharing schemes (i.e., schemes secure against cheaters). EDF can be used to construct robust secret sharing schemes that are optimal with respect to the new bound. We also prove a weak converse, showing that if there exists an optimal secret sharing scheme, then there exists an EBIBD.

Finally, we derive a Fisher-type inequality for splitting BIBDs. We also prove a weak equivalence between splitting BIBDs and splitting A-codes. Further, it is shown that an EDF implies a splitting BIBD.

Keywords. combinatorial design, difference family, BIBD, authentication code, secret sharing scheme.

1 Introduction

Combinatorial designs have played an important role in cryptology. In this paper, we introduce three types of new combinatorial designs, external difference families (EDF), external BIBDs (EBIBD) and splitting BIBDs and show their applications to splitting authentication codes and secret sharing schemes secure against cheaters.

An EDF can be considered as an extension of difference sets and difference families. An EBIBD is a generalization of a balanced incomplete block design (BIBD). These concepts are defined in the next section, where we prove that an EDF is equivalent to an EBIBD having a particular automorphism group. In the remainder of the paper, we discuss applications of these designs to authentication codes and robust secret sharing schemes.

An authentication code (A-code) is called *splitting* if a message is not uniquely determined by the plaintext (*source state*) and the key. This concept is very important in the context of authentication codes with arbitration (see [11, 12, 4, 6, 7, 8, 9]). For splitting A-codes, lower bounds on cheating probabilities [5, 1] and a lower bound on the size of keys [13, 2] are known. However, no schemes were known which meet both these bounds. We show that splitting A-codes with perfect secrecy which meet both of these bounds can be obtained by using EDF.

In a (k, n) secret sharing scheme, a secret s is distributed to n participants, $P_1, \ldots, P_n$. A piece of information given to P_i is called a *share* and is denoted by v_i. Tompa and Woll [14] considered the following scenario. Suppose that $k-1$ participants $P_1, \ldots, P_{k-1}$ want to cheat the kth participant P_k by opening forged shares $v'_1, \ldots, v'_{k-1}$. They succeed if the secret s' reconstructed from $v'_1, \ldots, v'_{k-1}$ and v_k is different from the original secret s.

Recently, a lower bound on the size of shares for this problem was derived in [10]. There it was shown that $|\mathcal{V}_i| \geq (|\mathcal{S}|-1)/\delta + 1$, where $\mathcal{V}_i$ denotes the set

Table 1

	0	1	3
0	-	1	3
1	6	-	2
3	4	5	-

Table 2

	0	1	0	2	0	3
0	-	1				
1	6	-				
0			-	2		
2			5	-		
0					-	3
3					4	-

Table 3

	0	1	2	4
0			2	4
1			1	3
2	7	8		
4	5	6		

of possible shares for participant P_i, $\mathcal{S}$ denotes the set of possible secrets, and δ denotes the cheating probability.

This bound can be met with equality if $\delta \geq 1/|\mathcal{S}|$. However, if $\delta < 1/|\mathcal{S}|$, then the bound cannot be met. Here we present a new lower bound on $|\mathcal{V}_i|$ in the case where $\delta < 1/|\mathcal{S}|$. We show that

$$|\mathcal{V}_i| \;\geq\; 1 + \frac{|\mathcal{S}| - 1}{|\mathcal{S}|\delta^2}.$$

Then we show that secret sharing schemes which meet the new bound can be obtained by using EDF. Further, we prove a weak converse, namely that if there exists a secret sharing scheme which meets our bound, then there exists an EBIBD.

Finally, we derive a Fisher-type inequality for splitting BIBDs. We also prove a weak equivalence between splitting BIBDs and splitting A-codes. Further, it is shown that an EDF implies a splitting BIBD.

2 New Combinatorial Designs

In this section, we introduce two new types of combinatorial designs, external difference families (EDF) and external BIBDs (EBIBD), and we show that an EDF is equivalent to an EBIBD with a particular automorphism.

2.1 External Difference Family (EDF)

First, we give definitions of difference sets and difference families.

Definition 2.1 [3] Let $(X, +)$ be an Abelian group of order v. A subset $D \subseteq X$ is a (v, c, λ)-*difference set* if $|D| = c$ and the multiset

$$\{x - y : x, y \in D, x \neq y\} = \lambda(X \backslash \{0\}).$$

Example 2.1 $D = \{0, 1, 3\}$ is a $(7, 3, 1)$-difference set in the group $(\mathbf{Z}_7, +)$. Indeed, the differences modulo 7 are

$$1 - 0 = 1,\ 3 - 0 = 3,\ 3 - 1 = 2,\ 0 - 1 = 6,\ 0 - 3 = 4,\ 1 - 3 = 5.$$

This is also shown in Table 1, where the (i, j) entry is $d_i - d_j \bmod 7$. Each element in $\mathbf{Z}_7 \setminus \{0\}$ appears exactly once in Table 1.

Definition 2.2 [3] Let $(X, +)$ be an Abelian group of order v. A (v, c, λ)-*difference family* over X is a collection of u subsets of X, $\{D_1, \ldots, D_u\}$, such that $|D_1| = \cdots = |D_u| = c$ and the multiset union

$$\bigcup_i \{x - y : x, y \in D_i, x \neq y\} = \lambda(X \backslash \{0\}).$$

Example 2.2 $D_1 = \{0, 1\}, D_2 = \{0, 2\}$ and $D_3 = \{0, 3\}$ form a $(7, 2, 1)$-difference family over $\mathbf{Z}_7$, where $u = 3$. This is shown in Table 2, where each element in $\mathbf{Z}_7 \setminus \{0\}$ appears exactly once in the diagonal submatrices.

Now we define a new combinatorial design that we call an external difference family (EDF).

Definition 2.3 Let $(X, +)$ be an Abelian group of order v. A (v, c, λ) u-*EDF* (or, *external difference family*) over X is a collection of u subsets of X, denoted $\{D_1, \ldots, D_u\}$, such that (1) $|D_1| = \cdots = |D_u| = c$ and (2) the multiset union

$$\bigcup_{i \neq j} (D_i - D_j) = \lambda(X \backslash \{0\}),$$

where $D_i - D_j$ is the multiset $\{x - y : x \in D_i, y \in D_j\}$.

Example 2.3 $D_1 = \{0, 1\}$ and $D_2 = \{2, 4\}$ form a $(9, 2, 1)$ 2-EDF over $\mathbf{Z}_9$. This is shown in Table 3, where each element in $\mathbf{Z}_9 \setminus \{0\}$ appears exactly once in the off-diagonal submatrices.

Example 2.4 $D_1 = \{0, 1, \ldots, t-1\}$ and $D_2 = \{t, 2t, \ldots, t^2\}$ form a $(2t^2+1, t, 1)$ 2-EDF over $\mathbf{Z}_{2t^2+1}$.

We now state a couple of fundamental properties of EDF. First, it is easy to see that if there exists a (v, c, λ) u-EDF, then

$$\lambda(v - 1) = k(k - c) = c^2 u(u - 1), \tag{1}$$

where $k = cu$.

Theorem 2.1 *In a (v, c, λ) u-EDF $(D_1, \ldots, D_u)$ over X, for all $a \in X$,*

$$N_a \stackrel{\triangle}{=} |\{x : x \in D_i, x - a \in D_j, i \neq j\}| \;=\; \begin{cases} 0 & \text{if } a = 0 \\ \lambda & \text{if } a \neq 0. \end{cases} \tag{2}$$

Proof. It is clear that $N_0 = 0$. For $a \neq 0$, from the definition, we have

$$\begin{aligned} \lambda &= |\{(x, y) : x - y = a, x \in D_i, y \in D_j, i \neq j\}| \\ &= |\{x : x \in D_i, x - a \in D_j, i \neq j\}| = N_a, \end{aligned}$$

letting $y = x - a$. ∎

2.2 External BIBD

The definition of a balanced incomplete block design (BIBD) is given as follows.

Definition 2.4 [3] A (v, b, r, l, λ)-*BIBD* is a pair $(X, \mathcal{B})$ in which X is a set of v elements called *points*, $\mathcal{B}$ is a set of b l-subsets of X called *blocks*, each point is contained in exactly r blocks, and each pair of distinct points is contained in exactly λ blocks. If $v = b$ (equivalently, if $r = k$), then the BIBD is called *symmetric*, and denoted (v, l, λ)-*SBIBD*. It is known that a (v, l, λ)-SBIBD can be characterized by the fact that, for every $A, B \in \mathcal{B}$, $|A \cap B| = \lambda$.

Now we define our second new combinatorial design, an external BIBD.

Definition 2.5 A (v, l, λ) c-*EBIBD* (or, *external BIBD*) is a pair $(X, \mathcal{B})$ such that $l = cu$ for some integer $u \geq 2$, and the following properties are satisfied:

1. $|X| = |\mathcal{B}| = v$.
2. Every $B \in \mathcal{B}$ is expressed as a disjoint union $B = B_1 \cup \cdots \cup B_u$, where $|B_1| = \cdots = |B_u| = c$, and $B \subseteq X$ (hence, $|B| = l$ for all $B \in \mathcal{B}$).
3. For each i, $1 \leq i \leq u$, we have that the multiset union $\displaystyle\bigcup_{B \in \mathcal{B}} B_i = cX$.
4. For every $A, B \in \mathcal{B}$, $A \neq B$, we have that $\displaystyle\sum_{i \neq j} |A_i \cap B_j| = \lambda$.

It can be shown that the parameters of an EBIBD are not independent; in fact, $\lambda(v-1) = l(l-c)$ as shown below.

Lemma 2.2 *Each element x appears in l blocks.*

Proof. Suppose that x appears in r blocks. Count in two ways the number of pairs (B, x) such that $x \in B$, where B is a block. Then we have

$$vl = vr$$

because $|X| = |\mathcal{B}| = v$ and $|B| = l$. Therefore, $r = l$. ∎

Theorem 2.3 *In a (v, l, λ) c-EBIBD,*

$$\lambda(v-1) = l(l-c).$$

Proof. Fix a block A arbitrarily. We count in two ways the number N of pairs (B, x), where $B \neq A$ is a block and x is an element such that $x \in A_i$ and $x \in B_j$ for some $i \neq j$.

First there are $v - 1$ blocks B other than A. For each $B \neq A$, the number of such x is λ from property 4. Therefore, $N = \lambda(v-1)$.

Next fix $x \in A$ arbitrarily and suppose that $x \in A_i$. From Lemma 2.2, x appears in l blocks. Further from property 3, we can see that the number of blocks B such that $x \in B_j$ with some $j \neq i$ is $l - c$. Therefore, $N = l(l-c)$.

Hence $\lambda(v-1) = l(l-c)$. ∎

Corollary 2.4 *In a (v, l, λ) c-EBIBD, there cannot exist two blocks A and B such that $A_i = B_i$, $1 \le i \le u$.*

Proof. Suppose that $A_i = B_i$, $1 \le i \le u$. Then $\lambda = 0$, and Theorem 2.3 implies that $l = c$, or equivalently, $u = 1$. This contradicts the condition that $u \ge 2$. $\square$

2.3 The Relation between EDF and EBIBD

In this subsection, we show that a (v, c, λ) u-EDF is equivalent to a (v, l, λ) c-EBIBD with a particular automorphism.

Suppose $(X, \mathcal{B})$ is a (v, l, λ) c-EBIBD. Let $\mathsf{Sym}(X)$ denote the symmetric group of all $v!$ permutations of the elements of X. A permutation $\gamma \in \mathsf{Sym}(X)$ is an *automorphism* of $(X, \mathcal{B})$ provided that there is a permutation of $\mathcal{B}$, say ρ, such that

$$\gamma(B_i) = (\rho(B))_i$$

for all $B \in \mathcal{B}$ and for $1 \le i \le u$. In other words, γ maps blocks to blocks in a way that respects the partitions $B = B_1 \cup \cdots \cup B_u$. The set of all automorphisms of $(X, \mathcal{B})$, denoted $\mathsf{Aut}(X, \mathcal{B})$, is a subgroup of $\mathsf{Sym}(X)$ that is called the *automorphism group* of $(X, \mathcal{B})$.

A subgroup Γ of $\mathsf{Sym}(X)$ is *sharply transitive* if, for every $x \in X$ and for every $x' \in X$, there exists a unique $\gamma \in \Gamma$ such that $\gamma(x) = x'$. Any additive abelian group, say $(X, +)$, has a natural representation as a sharply transitive subgroup of $\mathsf{Sym}(X)$. To be precise, each group element $g \in X$ corresponds to a permutation γ_g of X defined as follows: $\gamma_g(h) = g + h$ for all $h \in X$.

Suppose that $(X, +)$ is an abelian group and Γ is its representation as a sharply transitive subgroup of $\mathsf{Sym}(X)$. Further, suppose that $(X, \mathcal{B})$ is a (v, l, λ) c-EBIBD such that Γ is a subgroup of $\mathsf{Aut}(X, \mathcal{B})$. Then we say that $(X, \mathcal{B})$ has $(X, +)$ as a *sharply transitive automorphism group*.

After proving a preliminary lemma, we will state and prove the main theorem of this section.

Lemma 2.5 *Suppose $T_1, T_2 \subseteq X$, where $(X, +)$ is an additive Abelian group. Let $a \in X$. Then*

$$|T_1 \cap (T_2 + a)| = |\{(s, t) : s \in T_1, t \in T_2, s - t = a\}|.$$

Proof. Denote $D_a = \{(s, t) : s \in T_1, t \in T_2, s - t = a\}$. Suppose $x \in T_1 \cap (T_2 + a)$. Then $x \in T_1$ and $x - a \in T_2$, so $(x, x - a) \in D_a$. Conversely, if $(x, y) \in D_a$, then $x \in T_1 \cap (T_2 + a)$. Thus we have a bijection from $T_1 \cap (T_2 + a)$ to D_a. $\square$

Theorem 2.6 *Let $(X, +)$ be an additive Abelian group of order v. A (v, l, λ) c-EBIBD having $(X, +)$ as a sharply transitive automorphism group, say $(X, \mathcal{B})$, is equivalent to a (v, c, λ) u-EDF over X such that $l = cu$.*

Proof. Suppose $\{D_1, \ldots, D_u\}$ is a (v, c, λ) u-EDF over X. For $1 \le i \le u$ and for $g \in X$, define $B_i^g = D_i + g$. For $g \in X$, define $B^g = \bigcup_{i=1}^u B_i^g$ and then define the collection of blocks $\mathcal{B}$ to consist of the v blocks B^g, $g \in X$.

At this point, we do not know if these blocks are all distinct. We will prove that $(X, \mathcal{B})$ is a (v, l, λ) c-EBIBD having $(X, +)$ as a sharply transitive automorphism group (which shows that the blocks are, in fact, distinct).

Property 2 is satisfied since $D_i \cap D_j = \emptyset$ if $i \neq j$. Property 3 is also obvious since $B_i^g = D_i + g$ for all i and g.

Let's consider property 4. Let $g, h \in X$, $g \neq h$. We want to compute $\sum_{i \neq j} |B_i^g \cap B_j^h|$. Since $B_i^g = D_i + g$ and $B_j^h = D_j + h$, we have that

$$\begin{aligned} |B_i^g \cap B_j^h| &= |(D_i + g) \cap (D_j + h)| = |(D_i \cap (D_j + h - g)| \\ &= |\{(s,t) : s \in D_i, t \in D_j, s - t = h - g\}|, \end{aligned}$$

where the last equation is obtained by applying Lemma 2.5 with $T_1 = D_i$, $T_2 = D_j$ and $a = h - g$. Now, we have that

$$\sum_{i \neq j} |B_i^g \cap B_j^h| = \sum_{i \neq j} |\{(s,t) : s \in D_i, t \in D_j, s - t = h - g\}| = \lambda,$$

since $\cup_{i \neq j}(D_i - D_j)$ contains the element $h - g$ exactly λ times. Hence, we have proved property 4.

By property 4, there should be no two blocks A and B such that $A_i = B_i$ for $1 \le i \le u$. This implies property 1. Finally, it is obvious that $(X, \mathcal{B})$ has $(X, +)$ as a sharply transitive automorphism group by the way that $(X, \mathcal{B})$ was constructed.

Let's look now at the converse. Suppose that $(X, \mathcal{B})$ is a (v, l, λ) c-EBIBD having $(X, +)$ as a sharply transitive automorphism group. Pick any $A \in \mathcal{B}$, and define $D_i = A_i$, $1 \le i \le u$. We will show that $\{D_1, \ldots, D_u\}$ is a (v, c, λ) u-EDF.

Property 1 is obvious, so let's look at property 2. Let $g \in X$, $g \neq 0$, and denote by α_g the number of occurrences of g in $\cup_{i \neq j}(D_i - D_j)$. (We want to show that $\alpha_g = \lambda$.) Clearly, we have

$$\alpha_g = \sum_{i \neq j} |\{(s,t) : s \in A_i, t \in A_j, s - t = g\}| = \sum_{i \neq j} |(A_i \cap (A_j + g)|,$$

where we apply Lemma 2.5 with $T_1 = A_i$, $T_2 = A_j$ and $a = g$.

Now, since $(X, +)$ is a sharply transitive automorphism group of $(X, \mathcal{B})$ we see that $B = A + g \in \mathcal{B}$. Hence, $\alpha_g = \sum_{i \neq j} |A_i \cap B_j| = \lambda$ since $(X, \mathcal{B})$ is a (v, l, λ) c-EBIBD. ∎

3 Application to Splitting A-codes

In this section, we show that an optimal splitting A-code can be obtained from a (v, c, λ) u-EDF.

3.1 Splitting A-code

In the model of authentication codes (A-codes), the *transmitter* T and the *receiver* R share a common *encoding rule* (or *key*) e. The key e is chosen according to some specified probability distribution. Given a *source state* (plaintext) s, T computes a *message* $m = e(s)$ and sends m to R. R accepts or rejects m based on e.

It is possible that more than one message can be used to communicate a particular source state s; this is called *splitting*. In this case, a message m is computed as $m = e(s, r)$, where r is a random number chosen from some specified finite set. If we define

$$e(s) \stackrel{\triangle}{=} \{m : e(s,r) = m \text{ for some } r\},$$

then splitting means that $|e(s)| > 1$. Note also that $e(s) \cap e(\hat{s}) = \emptyset$ if $s \neq \hat{s}$, for otherwise decoding would be impossible.

Let

$$S \stackrel{\triangle}{=} \{s\}, \quad M \stackrel{\triangle}{=} \{m\}, \quad E \stackrel{\triangle}{=} \{e\}, \quad \text{and } \kappa(e) \stackrel{\triangle}{=} \bigcup_{s \in S} e(s).$$

We say that e *accepts* m if $m \in \kappa(e)$.

In an *impersonation attack*, the opponent O sends a message m to the receiver; O succeeds if $m \in \kappa(e)$. The impersonation attack probability P_I is defined as

$$P_I \stackrel{\triangle}{=} \max_{m \in M} \Pr(m \in \kappa(e)), \tag{3}$$

where the probability is computed over the set of keys E.

In a *substitution attack*, the opponent O observes a message m transmitted by T, and then substitutes m with another message $\hat{m}$. O succeeds if $m \in e(s)$ and $\hat{m} \in e(\hat{s})$, where $s \neq \hat{s}$. In other words, the receiver accepts $\hat{m}$ as authentic and is misled as to the state of the source. The substitution attack probability P_S is defined as follows.

$$P_S \stackrel{\triangle}{=} \sum_m \Pr(T \text{ sends } m) \max_{\hat{m} \in M} \Pr(m \in e(s), \hat{m} \in e(\hat{s}), s \neq \hat{s} \mid m \in \kappa(e)),$$

where the probability is computed over the set of keys E. Here are some known bounds on attack probabilities and the number of keys in a (splitting) A-code.

Proposition 3.1 *[5]* $P_I \geq \min_{e \in E} \dfrac{|\kappa(e)|}{|M|}$.

Proposition 3.2 *[5, 1]* $P_S \geq \min_{e \in E} \dfrac{|\kappa(e)| - \max_{s \in S} |e(s)|}{|M| - 1}$.

(The bound on P_S in [5] was corrected as stated above in [1].)

Proposition 3.3 *[13, 2]* $|E| \geq \dfrac{1}{P_I P_S}$.

Finally, we say that an A-code has *perfect secrecy* if the opponent O has no information about the source state s given a message m. Formally,

$$\Pr(S = s \mid M = m) = \Pr(S = s)$$

for all $s \in S$ and $m \in M$.

3.2 Optimum Splitting A-codes Constructed from EDF

In this subsection, we show that an optimal splitting A-code can be obtained from a (v, c, λ) u-EDF.

Theorem 3.4 *If there exists a* $(v, c, 1)$ u-EDF $\{D_1, \ldots, D_u\}$ *over an Abelian group* $(X, +)$*, then there exists a splitting A-code with perfect secrecy, which meets the bounds of Propositions 3.1, 3.2 and 3.3, such that*

$$|E| = |M| = v, \quad |S| = u, \quad \text{and } |e(s)| = c, \quad \forall e, s.$$

Proof. Consider a splitting A-code such that $E = M = X, S = \{1, \ldots, u\}$ and

$$e(i) = \{e + x : x \in D_i\}$$

for all $e \in X$ and all $i \in S$. Then we have:

$$|E| = |M| = |X| = v = c^2 u(u-1) + 1 \text{ (from eq.(1))},$$

$$|e(i)| = |D_i| = c, \text{ and}$$

$$|\kappa(e)| = \sum_{i \in S} |e(i)| = uc, \quad \forall e \in E. \tag{4}$$

Suppose that E and S are uniformly distributed. It is clear that this A-code has perfect secrecy because $m = e + x$ and e is uniformly distributed over X. Let's compute P_I.

$$P_I = \max_{m \in M} \Pr(m \in \kappa(e)) = \frac{\max_{m \in M} |\{e \in E : m \in \kappa(e)\}|}{|E|} = \frac{uc}{v}.$$

Since $|M| = v$, we have equality in Proposition 3.1.

Next, we compute P_S. Let $m, \hat{m} \in M$, $m \neq \hat{m}$. First, we observe that

$$\Pr(m \in e(i), \hat{m} \in e(j), i \neq j \mid m \in \kappa(e)) = \frac{|\{e \in E : m \in e(i), \hat{m} \in e(j), i \neq j\}|}{|\{e \in E : m \in \kappa(e)\}|}$$

$$= \frac{|\{e \in E : m - e \in D_i, \hat{m} - e \in D_j, i \neq j\}|}{|\{e \in E : m \in \kappa(e)\}|} = \frac{1}{uc},$$

since $m - \hat{m}$ occurs exactly once as a difference in $\cup_{i \neq j}(D_i - D_j)$. On the other hand, for any $e \in E$, we have

$$|\kappa(e)| - \max_{i \in S} |e(i)| = uc - c = c(u-1)$$

and

$$|M| - 1 = c^2 u(u-1),$$

so it follows that

$$\frac{|\kappa(e)| - \max_{i \in S} |e(i)|}{|M| - 1} = \frac{1}{uc}.$$

Hence we have equality in Proposition 3.2. Finally, we compute

$$\frac{1}{P_I P_S} = \frac{v}{uc} \times uc = v = |E|,$$

so we have equality in Proposition 3.3. ∎

4 Application to Secret Sharing Schemes

4.1 Definition of Security against Cheaters

In a (k, n) threshold secret sharing scheme, let $\mathcal{S}$ be the set of *secrets*. In the distribution phase, a dealer outputs a vector $(v_1, \ldots, v_n)$ on input $s \in \mathcal{S}$, where v_i is called a *share* of participant P_i. In the reconstruction phase, the following conditions must hold.

1. any k or more shares determine the secret s, and
2. no set of $k-1$ or fewer shares have any information on the secret s.

Let S denote a random variable distributed over a finite set $\mathcal{S}$. Let V_i denote the random variable induced by v_i and let

$$\mathcal{V}_i \stackrel{\triangle}{=} \{v_i : \Pr(V_i = v_i) > 0\}.$$

Definition 4.1 For $w \in \mathcal{V}_{i_1} \times \cdots \times \mathcal{V}_{i_k}$, define

$$Sec_{(i_1,\ldots,i_k)}(w) \stackrel{\triangle}{=} \begin{cases} s & \text{if } \exists s \text{ such that } \Pr(S = s \mid V_{i_1} \cdots V_{i_k} = w) = 1, \\ \perp & \text{otherwise.} \end{cases}$$

Note that we will usually omit the subscript $(i_1, \ldots, i_k)$ for readability.

Definition 4.2 Suppose that $k-1$ cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$ have $b = (v_{i_1}, \ldots, v_{i_{k-1}})$ as their shares, where v_{i_j} denotes the share of P_{i_j}. We say that P_{i_k} is *cheated* by the list of forged shares $b' = (v'_{i_1}, \ldots, v'_{i_{k-1}})$ if $Sec(b', v_{i_k}) \in \mathcal{S}$ and $Sec(b', v_{i_k}) \neq Sec(b, v_{i_k})$.

Definition 4.3 We define the *cheating probability* as follows:

$$Cheat(V_{i_1}, \ldots, V_{i_{k-1}}) \stackrel{\triangle}{=} \max_{b} \max_{b'} \Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1}, \ldots, P_{i_{k-1}} \text{ have } b)$$

We say that a (k, n) threshold scheme is δ-*secure* if

$$Cheat(V_{i_1}, \ldots, V_{i_{k-1}}) \leq \delta$$

for any $\{i_1, \ldots, i_{k-1}\} \subseteq \{1, \ldots, n\}$.

4.2 A New Bound on $|\mathcal{V}_i|$

Recently, the following lower bound on $|\mathcal{V}_i|$ was shown.

Proposition 4.1 *[10] In a δ-secure (k,n) threshold secret sharing scheme,*

$$|\mathcal{V}_i| \ \geq \ 1 + \frac{|\mathcal{S}|-1}{\delta}. \tag{5}$$

In this subsection, we derive a more tight lower bound on $|\mathcal{V}_i|$ for $\delta < 1/|\mathcal{S}|$.

Theorem 4.2 *Suppose that S is uniformly distributed in a δ- secure (k,n) threshold secret sharing scheme. Then*

$$|\mathcal{V}_i| \ \geq \ 1 + \frac{|\mathcal{S}|-1}{|\mathcal{S}|\delta^2}. \tag{6}$$

Proof. Assume that cheaters $P_{i_1}, \ldots, P_{i_{k-1}}$ have $b = (v_{i_1}, \ldots, v_{i_{k-1}})$ as their shares. Let

$$\hat{\mathcal{V}}_{i_k}(s,b) \ \stackrel{\triangle}{=} \ \{v_{i_k} : Sec(b, v_{i_k}) = s\}.$$

First, we prove that

$$|\hat{\mathcal{V}}_{i_k}(s,b)| \geq \frac{1}{|\mathcal{S}|\delta}, \tag{7}$$

for any $\{i_1, \ldots, i_{k-1}\} \subset \{1, \ldots, n\}, \forall b = V_{i_1} \times \cdots \times V_{i_{k-1}}$ and $\forall s \in \mathcal{S}$. Consider a cheaters' strategy as follows. The cheaters choose $\hat{s} \in \mathcal{S}$ arbitrarily and then choose $\hat{x} \in \hat{\mathcal{V}}_{i_k}(\hat{s}, b)$ such that $\Pr(V_{i_k} = \hat{x} \mid V_{i_1} \cdots V_{i_{k-1}} = b, S = \hat{s})$ is the maximum. Finally, they open b' such that $Sec(b', \hat{x}) \notin \{\hat{s}, \perp\}$ arbitrarily. P_{i_k} is cheated if he has $\hat{x}$ and $S = \hat{s}$. Therefore,

$$\begin{aligned}
&\max_{b'} \Pr(P_{i_k} \text{ is cheated by } b' \mid P_{i_1}, \ldots, P_{i_{k-1}} \text{ have } b) \\
&\quad \geq \ \Pr(S = \hat{s} \mid V_{i_1} \cdots V_{i_{k-1}} = b) \Pr(V_{i_k} = \hat{x} \mid V_{i_1} \cdots V_{i_{k-1}} = b, S = \hat{s}) \\
&\quad = \ \Pr(S = \hat{s}) \max_{x \in \hat{\mathcal{V}}_{i_k}(\hat{s}, b)} \Pr(V_{i_k} = x \mid V_{i_1} \cdots V_{i_{k-1}} = b, S = \hat{s}) \\
&\quad \geq \ (1/|\mathcal{S}|) \times (1/|\hat{\mathcal{V}}_{i_k}(\hat{s}, b)|).
\end{aligned}$$

Since we consider a δ-secure scheme,

$$\delta \geq \frac{1}{|\mathcal{S}||\hat{\mathcal{V}}_{i_k}(\hat{s}, b)|}.$$

Then we obtain eq.(7).

Next consider a cheaters' strategy as follows. P_{i_1} opens $v'_{i_1} \in \mathcal{V}_{i_1} \setminus \{v_{i_1}\}$ randomly. That is,

$$\Pr(v'_{i_1}) = \begin{cases} 1/(|\mathcal{V}_{i_1}| - 1) & \text{if } v'_{i_1} \neq v_{i_1} \\ 0 & \text{if } v'_{i_1} = v_{i_1}. \end{cases}$$

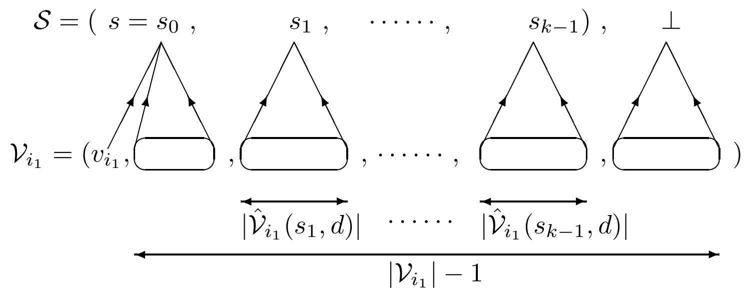

Figure 1:

$P_{i_2}, \ldots, P_{i_{k-1}}$ open their shares honestly. Suppose that P_{i_k} has $v_{i_k} = x$. We then consider

$$\Pr(P_{i_k} \text{ is cheated} \mid P_{i_1}, \ldots, P_{i_{k-1}} \text{ have } b).$$

Since the probability is taken over v'_{i_1} and x, we have

$$\begin{aligned}
& \Pr(P_{i_k} \text{ is cheated} \mid P_{i_1}, \ldots, P_{i_{k-1}} \text{ have } b) \\
= \ & E_{v'_{i_1}}[\Pr_x(P_{i_k} \text{ is cheated by } v'_{i_1} \mid P_{i_1}, \ldots, P_{i_{k-1}} \text{ have } b)] \\
= \ & E_x[\Pr_{v'_{i_1}}(P_{i_k} \text{ is cheated } \mid P_{i_1}, \ldots, P_{i_{k-1}} \text{ have } b, P_{i_k} \text{ has } x)] \\
= \ & E_x\left[\sum_{s \in \mathcal{S}} \Pr(S = s) \Pr_{v'_{i_1}}(P_{i_k} \text{ is cheated } \mid P_{i_1}, \ldots, P_{i_{k-1}} \text{ have } b, P_{i_k} \text{ has } x, S = s)\right] \\
= \ & |\mathcal{S}|^{-1} E_x\left[\sum_{s \in \mathcal{S}} \Pr_{v'_{i_1}}(P_{i_k} \text{ is cheated } \mid V_{i_2} \cdots V_{i_k} = d, S = s)\right], \qquad (8)
\end{aligned}$$

where $d = (v_{i_2}, \ldots, v_{i_{k-1}}, x)$. From figure 1, we see that

$$\Pr_{v'_{i_1}}(P_{i_k} \text{ is cheated } \mid V_{i_2} \cdots V_{i_k} = d, S = s) \ \geq \ \frac{\sum_{s' \neq s} |\hat{\mathcal{V}}_{i_1}(s', d)|}{|\mathcal{V}_{i_1}| - 1}. \qquad (9)$$

Therefore, by subsituting eq.(9) into eq.(8), we obtain that

$$\begin{aligned}
& \Pr(P_{i_k} \text{ is cheated} \mid P_{i_1}, \ldots, P_{i_{k-1}} \text{ have } b) \\
\geq \ & |\mathcal{S}|^{-1}(|\mathcal{V}_{i_1}| - 1)^{-1} E_x\left[\sum_{s \in \mathcal{S}} \sum_{s' \neq s} |\hat{\mathcal{V}}_{i_1}(s', d)|\right]. \qquad (10)
\end{aligned}$$

Finally, we prove eq.(6). In a δ-secure scheme, for any cheaters' strategy,

$$\delta \ \geq \ \max_b \Pr(P_{i_k} \text{ is cheated} \mid P_{i_1}, \ldots, P_{i_{k-1}} \text{ have } b)$$

where the probability is taken over the randomness of the cheaters as well as v_{i_k}. Hence, from eq.(7) and (10),

$$\begin{aligned}
\delta &\geq \max_b |\mathcal{S}|^{-1}(|\mathcal{V}_{i_1}|-1)^{-1} E_x\left[\sum_{s\in\mathcal{S}}\sum_{s'\neq s}|\hat{\mathcal{V}}_{i_1}(s',d)|\right] \\
&\geq \max_b |\mathcal{S}|^{-1}(|\mathcal{V}_{i_1}|-1)^{-1} E_x\left[\sum_{s\in\mathcal{S}}\sum_{s'\neq s}\frac{1}{|\mathcal{S}|\delta}\right] \\
&= \frac{|\mathcal{S}|-1}{|\mathcal{S}|(|\mathcal{V}_{i_1}|-1)\delta}.
\end{aligned}$$

Therefore, we obtain eq.(6). $\square$

Observe that the right hand side of eq.(6) is bigger than that of eq.(5) if $\delta < 1/|\mathcal{S}|$. In the next subsection, we show that the bound of Theorem 4.2 can be met with equality.

Remark: We can not remove the condition that S is uniformly distributed from Theorem 4.2 because there exists a counterexample. Consider a $(2,2)$ threshold secret sharing scheme such as follows.

Let $\mathcal{S} = \{0,1\}$ and suppose that $\Pr(S=0) = 1/4, \Pr(S=1) = 3/4$. Let $\mathcal{V}_1 = \mathcal{V}_2 = \mathbf{Z}_7$. In what follows, all operations are done over $GF(7)$. First, the dealer D chooses $v_1 \in \mathcal{V}_1$ uniformly. Next, if $s = 0$ then let $v_2 = -v_1$. Otherwise, choose $a \in \{1,2,3\}$ uniformly at random and let $v_2 = a - v_1$. The secret is reconstructed as

$$s = \begin{cases} 0 & \text{if } v_1 + v_2 = 0, \\ 1 & \text{if } v_1 + v_2 \in \{1,2,3\}, \\ \perp & \text{otherwise.} \end{cases}$$

We will show that this scheme is 1/4-secure. On the other hand, the right hand side of eq.(6) is

$$1 + 4^2(2-1)/2 \ = \ 9,$$

which is larger than $|\mathcal{V}_1| = 7$.

First in this scheme,

$$\Pr(V_2 = -v_1 \mid V_1 = v_1) = \Pr(S = 0 \mid V_1 = v_1) = 1/4$$

for any $v_1 \in \mathcal{V}_1$ because $\mathcal{V}_1$ is uniformly distributed. Similarly, we have

$$\begin{aligned}
\Pr(V_2 = 1 - v_1 \mid V_1 = v_1) &= 1/4, \\
\Pr(V_2 = 2 - v_1 \mid V_1 = v_1) &= 1/4, \\
\Pr(V_2 = 3 - v_1 \mid V_1 = v_1) &= 1/4
\end{aligned}$$

for all $v_1 \in \mathcal{V}_1$.

Next suppose that a malicous P_1 opens $v_1' = v_1 + 1$ instead of v_1. If P_2 has $v_2 = -v_1$, then the secret is $s = 0$. In this case, however,

$$v_1' + v_2 = v_1 + 1 - v_1 = 1.$$

Therefore, P_2 reconstrcuts $s' = 1$. Hence P_2 is cheated. We can further see that if P_2 has $v_2 = 1 - v_1$ or $2 - v_1$ or $3 - v_1$, then P_2 is not cheated. Therefore,

$$\begin{aligned}&\Pr(P_2 \text{ is cheated by } v_1 + 1 \mid V_1 = v_1)\\ &= \Pr(V_2 = -v_1 \mid V_1 = v_1)\\ &= 1/4.\end{aligned}$$

Similarly, we can show that

$$\Pr(P_2 \text{ is cheated by } v_1' \mid V_1 = v_1) \leq 1/4$$

for all $v_1' (\neq v_1)$. Therefore, this scheme is 1/4-secure.

4.3 Optimal Secret Sharing Scheme Constructed from EDF

In this subsection, we show that an optimal secret sharing scheme secure against cheaters can be obtained by using a $(v, c, 1)$ u-EDF.

Theorem 4.3 *Suppose that there exists a $(v, c, 1)$ u-EDF such that v is a prime power. Then there exists a δ-secure (k, n) threshold scheme which meets the bound of Theorem 4.2 such that $|\mathcal{S}| = u$ and $\delta = 1/(cu)$ for any $k \leq n < v$.*

Proof. Let $(D_1, \ldots, D_u)$ be a $(v, c, 1)$ u-EDF. Consider the following secret sharing scheme. The set of secrets is $\mathcal{S} = \{1, \ldots, u\}$. S is uniformly distributed over $\mathcal{S}$. In what follows, all operations are done over $GF(v)$.

In the distribution phase, for a secret $s \in \mathcal{S}$, the dealer chooses $d \in D_s$ randomly. Then, he chooses a random polynomial $f(x)$ of degree $k - 1$ such that $f(0) = d$. The share of P_i is $v_i = f(i)$. In the reconstruction phase, k or more participants compute the constant term d of $f(x)$ by using the Lagrange interpolation formula. They accept s as the secret iff $d \in D_s$ for some D_s.

We show that the above scheme satisfies our requirements. Without loss of generality, suppose that $P_1, \ldots, P_{k-1}$ have shares $b = (v_1, \ldots, v_{k-1})$ and P_k has share v_k. Fix a list of forged shares $b' = (v_1', \ldots, v_{k-1}')$. From the Lagrange formula, we have

$$\sum_{j=1}^{k-1} \beta_j v_j + \beta_k v_k = d \in D_s, \tag{11}$$

where $\beta_j = \prod_{l \neq j, 1 \leq l \leq k} \frac{-l}{j - l}$ for $1 \leq j \leq k$. Define

$$\begin{aligned}T &\triangleq \{x : \sum_{j=1}^{k-1} \beta_j v_j + \beta_k x \in D_i \text{ for some } i\}, \quad \text{and}\\ \tilde{\mathcal{V}}_k(b \to b') &\triangleq \{v_k : \ P_k \text{ is cheated by } b'\}.\end{aligned}$$

Thus T is the set of possible values of v_k (given b), and $\tilde{\mathcal{V}}_k(b \to b')$ represents the possible values of v_k that will lead to P_k being cheated.

Note that there is a bijection between T and $\bigcup_i D_i$ for a fixed b since $\beta_k \neq 0$. Also, v_k is uniformly distributed over T because d is uniformly distributed over $\bigcup_i D_i$. Therefore, we have

$$\Pr(P_k \text{ is cheated by } b' \mid P_1, \ldots, P_{k-1} \text{ have } b) \;=\; \frac{|\tilde{\mathcal{V}}_k(b \to b')|}{|T|}. \tag{12}$$

Now, we have

$$|T| = \sum_{i=1}^{u} |D_i| = cu, \tag{13}$$

and

$$\begin{aligned} |\tilde{\mathcal{V}}_k(b \to b')| &= |\{x : Sec(b', x) \in \mathcal{S}, Sec(b', x) \neq Sec(b, x)\}| \\ &= \left|\{x : \sum_{j=1}^{k-1} \beta_j v_j + \beta_k x \in D_i, \sum_{j=1}^{k-1} \beta_j v'_j + \beta_k x \in D_{i'}, i \neq i'\}\right| \\ &= \left|\{d : d \in D_i, d - \sum_{j=1}^{k-1} \beta_j v_j + \sum_{j=1}^{k-1} \beta_j v'_j \in D_{i'}, i \neq i'\}\right| = 1 \text{ or } 0, \end{aligned}$$

from Theorem 2.1 since $\lambda = 1$. Hence,

$$\Pr(P_k \text{ is cheated by } b' \mid P_1, \ldots, P_{k-1} \text{ have } b) \;=\; \frac{1}{cu} \text{ or } 0,$$

and

$$\delta = Cheat(V_1, \ldots, V_{k-1}) \;=\; \frac{1}{cu} \;=\; \frac{1}{c|\mathcal{S}|}.$$

Finally, from eq.(1) since $|\mathcal{S}| = u$ for $\forall j$, we have

$$|\mathcal{V}_j| = v = c^2 u(u-1) + 1 = \frac{|\mathcal{S}| - 1}{\delta^2 |\mathcal{S}|} + 1.$$

$\square$

4.4 EBIBD from Secret Sharing Schemes

In this subsection, we prove a weak converse of Theorem 4.3. Recall that a (v, c, λ) u-EDF is equivalent to a (v, l, λ) c-EBIBD with a particular automorphism from Theorem 2.6.

Theorem 4.4 *For a uniformly distributed S, suppose that there exists a δ-secure (k, n) threshold scheme which meets the bound of Theorem 4.2 for all i. That is, for all i,*

$$|\mathcal{V}_i| = 1 + \frac{|\mathcal{S}| - 1}{|\mathcal{S}|\delta^2}.$$

Also, suppose that $c \stackrel{\triangle}{=} 1/(\delta|\mathcal{S}|)$ *is an integer. Then there exists a* $(v, c|\mathcal{S}|, 1)$ *c-EBIBD such that*

$$v \stackrel{\triangle}{=} 1 + |\mathcal{S}|(|\mathcal{S}| - 1)c^2. \tag{14}$$

Proof. Note that $|\mathcal{V}_j| = v$ for any j. Let $\mathcal{S} = \{1, 2, \ldots, |\mathcal{S}|\}$ and $\mathcal{V} \stackrel{\triangle}{=} \{1, 2, \ldots, v\} = \mathcal{V}_j$ for any j. Fix $v_2, \ldots, v_{k-1}$ arbitrarily. For each $i \in \mathcal{V}$, define

$$\begin{aligned} B_{i,s} &\stackrel{\triangle}{=} \{v_k : Sec(i, v_2, \ldots, v_{k-1}, v_k) = s\}, \text{and} \\ B_i &\stackrel{\triangle}{=} \bigcup_{s \in \mathcal{S}} B_{i,s} \\ &= \{v_k : Sec(i, v_2, \ldots, v_{k-1}, v_k) \in \mathcal{S}\}. \end{aligned}$$

We will show that $(\mathcal{V}, \{B_i\})$ is the desired EBIBD. Property 1 is obvious. To prove property 2, first we show that

$$|B_{i,s}| = c \quad \text{for } \forall (i, s). \tag{15}$$

If the equality of eq.(6) is satisfied, then the equality of eq.(7) must be satisfied from the proof of Theorem 4.2. Therefore,

$$|\hat{\mathcal{V}}_k(s, (i, v_2, \ldots, v_{k-1}))| = \frac{1}{\delta|\mathcal{S}|} = c \quad \text{for } \forall (i, s). \tag{16}$$

This means eq.(15) because $B_{i,s} = \hat{\mathcal{V}}_k(s, (i, v_2, \ldots, v_{k-1}))$.

Further, since k participants can determine the secret uniquely, it must be that $B_{i,s} \cap B_{i,\hat{s}} = \phi$ if $s \neq \hat{s}$. Hence, property 2 is satisfied for $u = |\mathcal{S}|$ because $B_i = \bigcup_{s \in \mathcal{S}} B_{i,s}$.

Let's now consider property 3. Define

$$\hat{B}_{i,s} \stackrel{\triangle}{=} \{v_1 : Sec(v_1, v_2, \ldots, v_{k-1}, i) = s\}.$$

We can prove that

$$|\hat{B}_{i,s}| = c \quad \text{for } \forall (i, s) \tag{17}$$

in the same way as eq.(15). Then for all $s \in \mathcal{S}$, it follows that the multiset union $\bigcup_{i \in \mathcal{V}} B_{i,s} = c\mathcal{V}$ because $v_k = i$ appears in $|\hat{B}_{i,s}| = c$ blocks for any $i \in \mathcal{V}$. Hence, property 3 is satisfied.

Finally, let's consider property 4. Recall that

$$\begin{aligned} B_{1,s} &= \{v_k : P_k \text{ computes } s \text{ when } P_1 \text{ opens } 1\}, \\ B_{h,\hat{s}} &= \{v_k : P_k \text{ computes } \hat{s} \text{ when } P_1 \text{ opens } h\}, \\ B_1 &= \cup_{s \in \mathcal{S}} B_{1,s}, \quad \text{and} \\ |B_1| &= c|\mathcal{S}| \quad \text{(from eq.(15))}. \end{aligned}$$

Without loss of generality, suppose that P_1 has $v_1 = 1$ as his original share. Then we have

$$\begin{aligned}
&\Pr(P_k \text{ is cheated when } P_1 \text{ opens } h) \\
&= \sum_{s \neq \hat{s}} \frac{|B_{1,s} \cap B_{h,\hat{s}}|}{|B_1|} = \sum_{s \neq \hat{s}} \frac{|B_{1,s} \cap B_{h,\hat{s}}|}{c|\mathcal{S}|}.
\end{aligned} \tag{18}$$

Define a binary $(v-1) \times c|\mathcal{S}|$ matrix $G = (g_{h,j})$ as follows:

$$g_{h,j} = \begin{cases} 1 & \text{if } j \in B_{1,s} \cap B_{h+1,\hat{s}} \text{ for some } s \neq \hat{s} \\ 0 & \text{otherwise.} \end{cases}$$

Let H denote the Hamming weight. Let w_j be the j-th column of G. Suppose that $j \in B_{1,s}$. Then from eq.(17), we have

$$\begin{aligned}
H(w_j) &= \sum_{\hat{s} \neq s} |\hat{B}_{j,\hat{s}}| = c(|\mathcal{S}| - 1), \\
H(G) &= c|\mathcal{S}| \times c(|\mathcal{S}| - 1) = c^2 |\mathcal{S}|(|\mathcal{S}| - 1).
\end{aligned}$$

Next, let u_h be the h-th row of G. Then

$$\max_h H(u_h) \geq \frac{c^2|\mathcal{S}|(|\mathcal{S}| - 1)}{v - 1}.$$

Further, it is easy to see that

$$H(u_h) = \sum_{i \neq j} |B_{1,i} \cap B_{h+1,j}|.$$

Therefore,

$$\max_{h \geq 2} \sum_{i \neq j} |B_{1,i} \cap B_{h,j}| \geq \frac{c^2|\mathcal{S}|(|\mathcal{S}| - 1)}{v - 1}.$$

Then from eq.(18), we obtain that

$$\delta \geq \frac{c(|\mathcal{S}| - 1)}{v - 1}.$$

On the other hand, from eq.(14), we see that

$$\delta = 1/(c|\mathcal{S}|) = c(|\mathcal{S}| - 1)/(v - 1), \tag{19}$$

since $c = 1/(\delta|\mathcal{S}|)$. Hence it must be that

$$\sum_{i \neq j} |B_{1,i} \cap B_{h,j}| = \frac{c^2|\mathcal{S}|(|\mathcal{S}| - 1)}{v - 1} = 1$$

for any h. (The last equality comes from Eq. (19).) Therefore, property 4 is satisfied. $\square$

5 Splitting BIBD and Fisher-type Inequality

In this section, we introduce a notion of splitting BIBDs and derive a Fisher-type inequality. Then we show a weak equivalence with splitting A-codes. Finally, it is shown that an EDF implies a splitting BIBD.

5.1 Definition

Definition 5.1 A $(v, b, l = cu, \lambda)$-splitting BIBD is a pair $(V, \mathcal{B})$ such that the following properties are satisfied, where $B_i \in \mathcal{B}$ is called a block and $B_i \subseteq V$.

1. $|V| = v,\ |\mathcal{B}| = b$.
2. Every $B_i \in \mathcal{B}$ is expressed as a disjoint union $B_i = B_{i,1} \cup \cdots \cup B_{i,u}$, where $|B_{i,1}| = \cdots = |B_{i,u}| = c$ and $|B_i| = l = cu$.
3. For each $x, y \in V$ $(x \neq y)$, there exist exactly λ blocks $B_i = B_{i,1} \cup \cdots \cup B_{i,u}$ such that
$$x \in B_{i,j},\ y \in B_{i,k},\ j \neq k.$$

Example 5.1 *We show a* $(9, 9, 4 = 2 \times 2, 1)$*-splitting BIBD.*

$$\begin{aligned}
V &= \{1,2,3,4,5,6,7,8,9\},\\
B_1 &= \{\{1,2\},\ \{3,5\}\},\\
B_2 &= \{\{2,3\},\ \{4,6\}\},\\
B_3 &= \{\{3,4\},\ \{5,7\}\},\\
B_4 &= \{\{4,5\},\ \{6,8\}\},\\
B_5 &= \{\{5,6\},\ \{7,9\}\},\\
B_6 &= \{\{6,7\},\ \{8,1\}\},\\
B_7 &= \{\{7,8\},\ \{9,2\}\},\\
B_8 &= \{\{8,9\},\ \{1,3\}\},\\
B_9 &= \{\{9,1\},\ \{2,4\}\}.
\end{aligned}$$

For example, for $x = 1$ *and* $y = 2$ *or* 4, B_9 *satisfies property 3.*

5.2 Fisher-type Inequality

We first prove the following lemma.

Lemma 5.1 *In a* $(v, b, l = cu, \lambda)$*-splitting BIBD, each element of* V *is contained in exactly*
$$r = \lambda(v-1)/(l-c) \tag{20}$$
blocks. Further,
$$b = \lambda v(v-1)/l(l-c). \tag{21}$$

Proof. First for any $x \in V$, count in two ways the number of pairs (y, B_i), where $y \in V$ and B_i is a block such that $x \in B_{i,j}$ and $y \in B_{i,k}$ with $j \neq k$. Then

$$\lambda(v-1) = r(l-c).$$

Therefore,

$$r = \lambda(v-1)/(l-c).$$

Next count in two ways the number of pairs $((x,y), B_i)$, where $x \neq y$ and B_i is a block such that $x \in B_{i,j}$ and $y \in B_{i,k}$ with $j \neq k$. Then

$$\lambda\binom{v}{2} = b\frac{l(l-c)}{2}.$$

Therefore,

$$b = \lambda v(v-1)/l(l-c).$$

$\square$

The right hand sides of eq.(20) and eq.(21) must be integers if a splitting BIBD exists. We next show a Fisher-type inequality for splitting BIBDs, which is also a necessary condition for the existence of splitting BIBDs.

Theorem 5.2 *If there exists a $(v, b, l = cu, \lambda)$-splitting BIBD $(V, \mathcal{B})$, then*

$$b \geq v/u.$$

Proof. For

$$V = \{x_1, \ldots, x_v\},$$

let

$$\begin{aligned}
\overline{x}_1 &\triangleq (1, 0, \ldots, 0),\\
\overline{x}_2 &\triangleq (0, 1, \ldots, 0),\\
&\vdots\\
\overline{x}_v &\triangleq (0, 0, \ldots, 1).
\end{aligned}$$

Define $\tilde{V}$ to be the v-dimensional real vector space having basis $\{\overline{x}_1, \ldots, \overline{x}_v\}$. For each $B_{i,j}$, define a vector

$$\overline{B_{ij}} \triangleq \sum_{x_k \in B_{i,j}} \overline{x}_k$$

Let $\tilde{V}'$ be the subspace of $\tilde{V}$ spanned by the vectors $\overline{B_{ij}}$,

$$\tilde{V}' \triangleq \{\overline{B_{ij}} : 1 \leq i \leq b, 1 \leq j \leq u\}$$

It is clear that $\tilde{V}' \subseteq \tilde{V}$. We will show that $\tilde{V} \subseteq \tilde{V}'$. Let

$$
\begin{aligned}
\overline{B_i} &\triangleq \sum_j \overline{B_{ij}}, \\
\overline{v}_{x_j} &\triangleq \sum_{B_i : x_j \in B_i} \overline{B}_i \quad \text{for } x_j \in V, \\
\overline{X} &\triangleq \sum_{x_i \in V} \overline{x}_i = \frac{1}{r} \sum_{i,j} \overline{B_{ij}}. \quad \text{(from Lemma 5.1)}
\end{aligned}
\tag{22}
$$

Then, $\overline{v}_{x_j} \in \tilde{V}'$, $\overline{X} \in \tilde{V}'$. On the other hand, from Eq. (22) and the definition of splitting BIBD, we have

$$
\begin{aligned}
\overline{v}_x &= \sum_{B_i : x \in B_i} \sum_j \overline{B_{ij}} \\
&= \sum_{B_i : x \in B_i} \left(\sum_{j : x \in B_{i,j}} \overline{B_{ij}} + \sum_{j : x \notin B_{i,j}} \overline{B_{ij}} \right) \\
&= \sum_{B_{i,j} : x \in B_{i,j}} \overline{B_{ij}} + \lambda(\overline{X} - \overline{x}), \\
\overline{x} &= \overline{X} - \frac{1}{\lambda}(\overline{v}_x - \sum_{B_{i,j} : x \in B_{i,j}} \overline{B_{ij}}).
\end{aligned}
$$

Therefore,

$$\overline{x} \in \tilde{V}'$$

for all $x \in V$. Hence $\tilde{V} = \tilde{V}'$. Then $bu \geq v$ because $\dim \tilde{V} = v$ and $\dim \tilde{V}'$ is at most bu. This means that $b \geq v/u$. $\square$

5.3 Weak Equivalence with Splitting A-codes

Definition 5.2 We say that a splitting A-code is c-splitting if

$$|e(s)| = c$$

for any $e \in E$ and any $s \in S$.

By using the notation of Sec. 3.1, let

$$|M| = v, \quad |S| = u, \quad |\kappa(e)| = l \ (= cu),$$

$$S = \{s_1, \ldots, s_u\},$$

$$e^{-1}(m) \triangleq s \text{ if } m = e(s, r) \text{ for some } r$$

for a c-splitting A-code.

From Proposition 3.1 and Proposition 3.2, we obtain the following corollary.

Corollary 5.3 *In a c-splitting A-code,*

$$P_I \geq l/v, \quad P_S \geq (l-c)/(v-1).$$

Now we show a connection between c-splitting A-codes and splitting BIBDs.

Theorem 5.4 *If there exists a c-splitting A-code which satisfies the equalities of Corollary 5.3, then*

$$|E| \geq \frac{v(v-1)}{l(l-c)}. \tag{23}$$

Further, the rows of the encoding matrix forms a $(v, |E|, l = cu, 1)$*-splitting BIBD if the above equality holds.*

Proof. If the equality of Proposition 3.2 is satisfied, then

$$|\{e : e^{-1}(m) \neq e^{-1}(m')\}| \geq 1$$

for any $m \neq m'$ from the proof of [1]. Now count the number of $\{m, m'\}$ such that $e^{-1}(m) \neq e^{-1}(m')$ for some e in two ways. Since each e accepts $l = c|S| = cu$ messages,

$$|E|l(l-c) \geq v(v-1).$$

Therefore, eq. (23) holds.

Next, if the equality of eq. (23) is satisfied, then

$$|\{e : e^{-1}(m) \neq e^{-1}(m')\}| = 1 \tag{24}$$

for any $m \neq m'$. Let

$$B_e \stackrel{\triangle}{=} e(s_1) \cup e(s_2) \cup \cdots \cup e(s_u).$$

Then $(V, \mathcal{B}) = (M, \{B_e \mid e \in E\})$ is a $(v, |E|, l = cu, 1)$-splitting BIBD from eq.(24). ∎

Theorem 5.5 *If there exists a* $(v, |E|, l = cu, 1)$*-splitting BIBD, then there exists a c-splitting A-code such that*

1. *all the equalities of Corollary 5.3 and Theorem 5.4 are satisfied.*
2. $|M| = v, \quad |S| = u.$
3. *Each source state occurs with equal probability.*

Proof. Let $|M| = v$. For each block

$$B = B_1 \cup \cdots \cup B_u,$$

define an encoding rule as

$$e(s_1) = B_1, \ \ldots, \ e(s_u) = B_u.$$

∎

Example 5.2 *We show an optimum* 2*-splitting A-code obtained from* $(9, 9, 4 = 2 \times 2, 1)$*-splitting BIBD.*

	s_1	s_2
e_1	$\{m_1, m_2\}$	$\{m_3, m_5\}$
e_2	$\{m_2, m_3\}$	$\{m_4, m_6\}$
e_3	$\{m_3, m_4\}$	$\{m_5, m_7\}$
e_4	$\{m_4, m_5\}$	$\{m_6, m_8\}$
e_5	$\{m_5, m_6\}$	$\{m_7, m_9\}$
e_6	$\{m_6, m_7\}$	$\{m_8, m_1\}$
e_7	$\{m_7, m_8\}$	$\{m_9, m_2\}$
e_8	$\{m_8, m_9\}$	$\{m_1, m_3\}$
e_9	$\{m_9, m_1\}$	$\{m_2, m_4\}$

5.4 EDF Implies Splitting BIBD

Theorem 5.6 *If there exists a* (v, c, λ) *u-EDF* $\{D_1, \ldots, D_u\}$ *over an Abelian group* $(X, +)$*, then there exists a* $(v, v, l = cu, \lambda)$*-splitting BIBD.*

Proof. For each $i \in X$, let

$$\begin{aligned} B_{i,j} &= \{i + z : z \in D_j\}, \\ B_i &= B_{1,1} \cup \cdots \cup B_{1,u}. \end{aligned}$$

Define $\mathcal{B} = \{B_1, \ldots, B_v\}$. We claim that $(X, \mathcal{B})$ is a $(v, v, l = cu, \lambda)$-splitting BIBD. Properties 1 and 2 are obvious.

Let's consider property 3. For any $x \neq y$, we can see that

$$\begin{aligned} & |\{B_i : x \in B_{i,j}, y \in B_{i,k}, j \neq k\}| \\ = & |\{B_i : x - i \in D_j, y - i \in D_k, j \neq k\}| \\ = & \lambda \end{aligned}$$

because $x - y$ occurs exactly λ times in $\cup_{j \neq k}(D_j - D_k)$. Hence we have proved property 3. ∎

References

[1] C. Blundo, A. De Santis, K. Kurosawa and W. Ogata. On a fallacious bound for authentication codes, *Journal of Cryptology* **12** (1999), 155–159.

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

[3] C. J. Colbourn and J. H. Dinitz, eds. *CRC Handbook of Combinatorial Designs*, CRC Press, Inc., 1996.

[4] Y. Desmedt and M. Yung. Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attack, *Lecture Notes in Computer Science* **537**, 177–188 (CRYPTO '90 Proceedings).

[5] M. De Soete. New bounds and constructions for authentication/secrecy codes with splitting, *Journal of Cryptology* **3** (1991), 173–186.

[6] T. Johansson. On the construction of perfect authentication codes that permit arbitration, *Lecture Notes in Computer Science* **773**, 343–354 (CRYPTO '93 Proceedings).

[7] T. Johansson. Lower bounds on the probability of deception in authentication with arbitration, *IEEE Transactions on Information Theory* **40** (1994), 1573–1585.

[8] K. Kurosawa. New bound on authentication code with arbitration, *Lecture Notes in Computer Science* **899**, 140–149 (CRYPTO '94 Proceedings).

[9] K. Kurosawa and S. Obana. Combinatorial bounds for authentication codes with arbitration, *Lecture Notes in Computer Science* **921**, 289–300 (EUROCRYPT '95 Proceedings).

[10] W. Ogata and K. Kurosawa. Optimum secret sharing scheme against cheating, *Lecture Notes in Computer Science* **1070**, 200–211 (EUROCRYPT '96 Proceedings).

[11] G. J. Simmons. Message authentication with arbitration of transmitter/receiver disputes, *Lecture Notes in Computer Science* **304**, 150–166 (EUROCRYPT '87 Proceedings).

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

[13] G. J. Simmons. Authentication theory/coding theory, *Lecture Notes in Computer Science* **196**, 411–431 (CRYPTO '84 Proceedings).

[14] M. Tompa and H. Woll. How to share a secret with cheaters, *Journal of Cryptology* **1** (1988), 133–138.