

Faculty of Informatics

Faculty of Informatics - Papers

University of Wollongong

Year 2005

An exposure property of block designs

Y. Wang* J. Seberry† B. J. Wysocki‡
T. A. Wysocki** L. C. Tran††
Y. Zhao‡‡ T. Xia§

*University of Wollongong

†University of Wollongong, jennie@uow.edu.au

‡University of Wollongong, bjw@uow.edu.au

**University of Wollongong, wysocki@uow.edu.au

††University of Wollongong, LCT71@UOW.EDU.AU

‡‡University of Wollongong, yz03@uow.edu.au

§University of Wollongong, txia@uow.edu.au

This article was originally published as Wang, Y, Seberry, J, Wysocki, BJ et al, An exposure property of block designs, Australasian Journal of Combinatorics, 33, 2005, 147-156.

This paper is posted at Research Online.

<http://ro.uow.edu.au/infopapers/297>

An exposure property of block designs

YEJING WANG JENNIFER SEBERRY

*Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522
Australia
{yejing, jennie}@uow.edu.au*

BEATA J. WYSOCKI TADEUSZ A. WYSOCKI LE CHUNG TRAN

*School of Electrical, Computer and Telecommunications Engineering
University of Wollongong
Wollongong 2522
Australia
beata@elec.uow.edu.au {wysocki, lct71}@uow.edu.au*

YING ZHAO TIANBING XIA

*Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522
Australia
{yz03, txia}@uow.edu.au*

Abstract

An exposure property of block designs is defined and investigated in this paper. The families of c -exposed designs are shown for $c = 2$ and $c = 3$. A sufficient condition for a c -exposed design is derived.

1 Introduction

We introduce an exposure property of block designs, which is interesting from a combinatorial point of view. This property is motivated by traitor tracing schemes, a research area of cryptography.

For a given block design, we consider a ‘false block’ which (i) is included in the union of up to a certain number of blocks of the design, and (ii) has the same size of intersection with each block involved in the union. The family of the blocks in the

union is called *exposed* if every other block has an intersection, with the false block, of size smaller than the above given size of intersections.

In this paper we first define the exposure property and show examples in Section 2. We derive a sufficient condition for the parameters of a block design being exposed in Section 3, and the existence of the designs satisfying the condition is shown in Sections 4 and 5. We discuss possible application of *c*-exposed designs in Section 6.

2 Definitions and 2-exposed block designs

A (v, k) block design is a pair of (X, \mathcal{B}) where X is a set of v elements and \mathcal{B} is a family of k -subsets of X . Each of these k -subsets is called a block. For a (v, k) block design (X, \mathcal{B}) and $\mathcal{C} = \{B_1, B_2, \dots, B_c\} \subseteq \mathcal{B}$, consider a k -subset $F \subseteq X$ such that

$$\begin{cases} |F \cap B_1| = |F \cap B_2| = \dots = |F \cap B_c| \\ F \subseteq B_1 \cup B_2 \cup \dots \cup B_c \end{cases} \tag{1}$$

Define a family $\tilde{\mathcal{C}}$ to be as follows

$$\tilde{\mathcal{C}} = \{F \subseteq X : F \text{ satisfies (1) and } |F| = k\}.$$

A family $\mathcal{C} \subseteq \mathcal{B}$ is called exposed if

$$\{B \in \mathcal{B} : |F \cap B| = \max_{B_i \in \mathcal{B}} |F \cap B_i|\} = \mathcal{C}$$

holds for every $F \in \tilde{\mathcal{C}}$.

Obviously, \mathcal{C} is exposed if $\tilde{\mathcal{C}} = \emptyset$, and we call it trivial.

Example 2.1 Let (X, \mathcal{B}) be the following block design

$$\begin{aligned} X &= \{1, 2, \dots, 9\} \\ \mathcal{B} &= \{123, 456, 789, 147, 258, 369, 159, 168\} \end{aligned}$$

Let $\mathcal{C} = \{123, 147\}$. Then

$$\tilde{\mathcal{C}} = \{124, 127, 134, 137\}$$

This \mathcal{C} is exposed.

A block design (X, \mathcal{B}) is called *c*-exposed if \mathcal{C} is exposed for all $\mathcal{C} \subseteq \mathcal{B}$ with $|\mathcal{C}| \leq c$.

Example 2.2 The following $(9, 3, \{0, 1\})$ block design

$$\begin{aligned} X &= \{1, 2, \dots, 9\} \\ \mathcal{B} &= \{123, 456, 789, 147, 258, 369\} \end{aligned}$$

is 2-exposed. Table 1 shows this.

C, \tilde{C}	$ F \cap B , F \in \tilde{C}, B \in \mathcal{B}$	$ F \cap B , F \in C, B \in \mathcal{B}$
$C_1 = \{123, 456\}$		$ 125 \cap 123 = 125 \cap 258 = 2$
$\tilde{C}_1 = \emptyset$		$ 125 \cap 456 = 125 \cap 147 = 1$
$C_2 = \{123, 789\}$		$ 125 \cap 789 = 125 \cap 369 = 0$
$\tilde{C}_2 = \emptyset$		
$C_3 = \{456, 789\}$		$ 128 \cap 123 = 128 \cap 258 = 2$
$\tilde{C}_3 = \emptyset$		$ 128 \cap 789 = 128 \cap 147 = 1$
$C_4 = \{147, 258\}$		$ 128 \cap 456 = 128 \cap 369 = 0$
$\tilde{C}_4 = \emptyset$		
$C_5 = \{147, 369\}$		$235 \cap 123 = 235 \cap 258 = 2$
$\tilde{C}_5 = \emptyset$		$235 \cap 456 = 235 \cap 369 = 1$
$C_6 = \{258, 369\}$		$235 \cap 789 = 235 \cap 147 = 0$
$\tilde{C}_6 = \emptyset$		
		$238 \cap 123 = 238 \cap 258 = 2$
		$238 \cap 789 = 238 \cap 369 = 1$
		$238 \cap 456 = 238 \cap 147 = 0$
		$136 \cap 123 = 136 \cap 369 = 2$
		$136 \cap 456 = 136 \cap 147 = 1$
		$136 \cap 789 = 136 \cap 258 = 0$
		$139 \cap 123 = 139 \cap 369 = 2$
		$139 \cap 789 = 139 \cap 147 = 1$
		$139 \cap 456 = 139 \cap 258 = 0$
		$236 \cap 123 = 236 \cap 369 = 2$
		$236 \cap 456 = 236 \cap 258 = 1$
		$236 \cap 789 = 236 \cap 147 = 0$
		$239 \cap 123 = 239 \cap 369 = 2$
		$239 \cap 789 = 239 \cap 258 = 1$
		$239 \cap 456 = 239 \cap 147 = 0$
$C_7 = \{123, 147\}$		
$\tilde{C}_7 = \{124, 127, 134, 137\}$		
		$ 124 \cap 123 = 124 \cap 147 = 2$
		$ 124 \cap 456 = 124 \cap 258 = 1$
		$ 124 \cap 789 = 124 \cap 369 = 0$
		$ 127 \cap 123 = 127 \cap 147 = 2$
		$ 127 \cap 789 = 127 \cap 258 = 1$
		$ 127 \cap 456 = 127 \cap 369 = 0$
		$ 134 \cap 123 = 134 \cap 147 = 2$
		$ 134 \cap 456 = 134 \cap 369 = 1$
		$ 134 \cap 789 = 134 \cap 258 = 0$
		$ 137 \cap 123 = 137 \cap 147 = 2$
		$ 137 \cap 789 = 137 \cap 369 = 1$
		$ 137 \cap 456 = 137 \cap 258 = 0$

Table 1.

Table 1. (Cont.)

$\mathcal{C}, \tilde{\mathcal{C}}$	$ F \cap B , F \in \tilde{\mathcal{C}}, B \in \mathcal{B}$	
$\mathcal{C}_{14} = \{789, 258\}$ $\tilde{\mathcal{C}}_{14} = \{278, 289, 578, 589\}$	$ 278 \cap 789 = 278 \cap 258 = 2$ $ 278 \cap 123 = 278 \cap 147 = 1$ $ 278 \cap 456 = 278 \cap 369 = 0$	
	$ 289 \cap 789 = 289 \cap 258 = 2$ $ 289 \cap 123 = 289 \cap 369 = 1$ $ 289 \cap 456 = 289 \cap 147 = 0$	
	$ 578 \cap 789 = 578 \cap 258 = 2$ $ 578 \cap 456 = 578 \cap 147 = 1$ $ 578 \cap 123 = 578 \cap 369 = 0$	
	$ 589 \cap 789 = 589 \cap 258 = 2$ $ 589 \cap 456 = 589 \cap 369 = 1$ $ 589 \cap 123 = 589 \cap 147 = 0$	
	$\mathcal{C}_{15} = \{789, 369\}$ $\tilde{\mathcal{C}}_{15} = \{379, 389, 679, 689\}$	$ 379 \cap 789 = 379 \cap 369 = 2$ $ 379 \cap 123 = 379 \cap 147 = 1$ $ 379 \cap 456 = 379 \cap 258 = 0$
		$ 389 \cap 789 = 389 \cap 369 = 2$ $ 389 \cap 123 = 389 \cap 258 = 1$ $ 389 \cap 456 = 389 \cap 147 = 0$
		$ 679 \cap 789 = 679 \cap 369 = 2$ $ 679 \cap 456 = 679 \cap 147 = 1$ $ 679 \cap 123 = 679 \cap 258 = 0$
		$ 689 \cap 789 = 689 \cap 369 = 2$ $ 689 \cap 456 = 689 \cap 258 = 1$ $ 689 \cap 123 = 689 \cap 147 = 0$

For a block design (X, \mathcal{B}) and an integer $i > 1$, we denote

$$\lambda = \max_{B_1, B_2 \in \mathcal{B}} |B_1 \cap B_2|$$

$$\mu_i = \min_{B_1, \dots, B_i \in \mathcal{B}} |B_1 \cap \dots \cap B_i|$$

Theorem 2.1 *A block design (X, \mathcal{B}) is 2-exposed if $k > 4\lambda - 2\mu_3$.*

Proof: Let $\mathcal{C} = \{B_1, B_2\} \subseteq \mathcal{B}$. For any third block $B \in \mathcal{B}$ and any $F \in \tilde{\mathcal{C}}$, the following inequality holds.

$$\begin{aligned} |F \cap B| &= |F \cap B \cap B_1 \cap B_2| + |F \cap B \cap B_1 \setminus B_2| + |F \cap B \cap B_2 \setminus B_1| \\ &\leq |B \cap B_1 \cap B_2| + |B \cap B_1 \setminus B_2| + |B \cap B_2 \setminus B_1| \\ &= |B \cap B_1| + |B \cap B_2 \setminus B_1| \end{aligned}$$

$$\begin{aligned}
 &= |B \cap B_1| + |B \cap B_2| - |B \cap B_1 \cap B_2| \\
 &\leq 2\lambda - \mu_3 < \frac{k}{2}
 \end{aligned}$$

It is obvious that $|F \cap B_1| = |F \cap B_2| \geq k/2$. So $|F \cap B| < |F \cap B_1|, |F \cap B_2|$. Hence \mathcal{C} is 2-exposed. □

Example 2.3 *The $(21, 5, 1)$ -SBIBD is 2-exposed. The blocks of $(21, 5, 1)$ -SBIBD are*

$$B_i = \{0 + i, 1 + i, 6 + i, 8 + i, 18 + i\}, \quad 0 \leq i \leq 20.$$

and $\mu_3 = |B_0 \cap B_{13} \cap B_{18}| = 0$.

3 c -exposed designs ($c > 2$)

Let (X, \mathcal{B}) be a block design, $\mathcal{C} = \{B_1, B_2, \dots, B_c\} \subseteq \mathcal{B}$, $B \in \mathcal{B} \setminus \mathcal{C}$. For each $h, 1 \leq h \leq c$,

$$\begin{aligned}
 \lambda &\geq |B \cap B_h| \\
 &= |B \cap B_1 \cap \dots \cap B_c| + \\
 &\quad \sum_{\substack{1 \leq s \leq c-1 \\ \{h, i_1, \dots, i_{c-1}\} \\ = \{1, \dots, c\}}} |B \cap B_h \cap B_{i_1} \cap \dots \cap B_{i_{s-1}} \setminus (B_{i_s} \cup \dots \cup B_{i_{c-1}})|
 \end{aligned} \tag{2}$$

Lemma 3.1 *For $2 \leq h \leq c$,*

$$\begin{aligned}
 &\sum_{\substack{1 \leq s \leq c-h \\ \{1, \dots, h, i_1, \dots, i_{c-h}\} \\ = \{1, \dots, c\}}} |B \cap B_h \cap B_{i_1} \cap \dots \cap B_{i_{s-1}} \setminus (B_{i_s} \cup \dots \cup B_{i_{c-h}} \cup (\cup_{p=1}^{h-1} B_p))| \\
 &\leq \lambda - |B \cap B_1 \cap \dots \cap B_c|
 \end{aligned}$$

Proof:

$$\begin{aligned}
 &\sum_{\substack{1 \leq s \leq c-h \\ \{1, \dots, h, i_1, \dots, i_{c-h}\} \\ = \{1, \dots, c\}}} |B \cap B_h \cap B_{i_1} \cap \dots \cap B_{i_{s-1}} \setminus (B_{i_s} \cup \dots \cup B_{i_{c-h}} \cup (\cup_{p=1}^{h-1} B_p))| \\
 &\leq \sum_{\substack{1 \leq s \leq c-1 \\ \{h, i_1, \dots, i_{c-1}\} = \{1, \dots, c\}}} |B \cap B_h \cap B_{i_1} \cap \dots \cap B_{i_{s-1}} \setminus (B_{i_s} \cup \dots \cup B_{i_{c-1}})| \\
 &\leq \lambda - |B \cap B_1 \cap \dots \cap B_c|
 \end{aligned}$$

the last inequality is from (2). The lemma is proved. \square

For $1 \leq h \leq c-1$, denote by

$$N_h = \sum_{\substack{1 \leq s \leq c-h \\ \{1, \dots, h, i_1, \dots, i_{c-h}\} \\ = \{1, \dots, c\}}} |B \cap B_{i_1} \cap \dots \cap B_{i_s} \setminus (B_{i_{s+1}} \cup \dots \cup B_{i_{c-h}} \cup (\cup_{p=1}^h B_p))|$$

Then we have

$$\begin{aligned} N_h &= \sum_{\substack{1 \leq s \leq c-h \\ \{1, \dots, h, i_1, \dots, i_{c-h}\} \\ = \{1, \dots, c\}}} |B \cap B_{i_1} \cap \dots \cap B_{i_s} \setminus (B_{i_s} \cup \dots \cup B_{i_{c-h}} \cup (\cup_{p=1}^h B_p))| \\ &= \sum_{\substack{1 \leq s \leq c-h-1 \\ \{1, \dots, h+1\} \\ \cup \{i_1, \dots, i_{c-h-1}\} \\ = \{1, \dots, c\}}} |B \cap B_{h+1} \cap B_{i_1} \cap \dots \cap B_{i_{s-1}} \setminus (B_{i_s} \cup \dots \cup B_{i_{c-h-1}} \cup (\cup_{p=1}^h B_p))| \\ &\quad + \sum_{\substack{1 \leq s \leq c-h-1 \\ \{1, \dots, h+1\} \\ \cup \{i_1, \dots, i_{c-h-1}\} \\ = \{1, \dots, c\}}} |B \cap B_{i_1} \cap \dots \cap B_{i_s} \setminus (B_{i_{s+1}} \cup \dots \cup B_{i_{c-h-1}} \cup (\cup_{p=1}^{h+1} B_p))| \\ &\leq \lambda - \mu_{c+1} + N_{h+1} \quad (\text{from lemma 3.1}) \end{aligned}$$

That is

$$N_h \leq \lambda - \mu_{c+1} + N_{h+1} \quad (3)$$

Lemma 3.2 $N_1 \leq (h-1)(\lambda - \mu_{c+1}) + N_h$, for $1 \leq h \leq c-1$.

Proof: We use induction on h . It is obviously true when $h = 1$. Assume that $N_1 \leq (h-1)(\lambda - \mu_{c+1}) + N_h$ is true for h . From (3) we obtain

$$N_1 \leq (h-1)(\lambda - \mu_{c+1}) + \lambda - \mu_{c+1} + N_{h+1} = h(\lambda - \mu_{c+1}) + N_{h+1}$$

The lemma is proved. \square

From lemma 3.2, we obtain

$$\begin{aligned} N_1 &\leq (c-2)(\lambda - \mu_{c+1}) + N_{c-1} \\ &= (c-2)(\lambda - \mu_{c+1}) + |B \cap B_c \setminus (B_1 \cup \dots \cup B_{c-1})| \\ &= (c-2)(\lambda - \mu_{c+1}) + |B \cap B_c| - |B \cap B_1 \cap \dots \cap B_c| \\ &\leq (c-1)(\lambda - \mu_{c+1}) \end{aligned} \quad (4)$$

Let $F \in \tilde{\mathcal{C}}$. For $1 \leq h \leq c$,

$$|F \cap B_h| \geq \frac{k}{c} \quad (5)$$

Consider $|F \cap B|$.

$$\begin{aligned}
 & |F \cap B| \\
 = & \sum_{\substack{1 \leq s \leq c \\ \{i_1, \dots, i_c\} \\ = \{1, \dots, c\}}} |F \cap B \cap B_{i_1} \cap \dots \cap B_{i_s} \setminus (B_{i_{s+1}} \cup \dots \cup B_{i_c})| \\
 \leq & \sum_{\substack{1 \leq s \leq c \\ \{i_1, \dots, i_c\} \\ = \{1, \dots, c\}}} |B \cap B_{i_1} \cap \dots \cap B_{i_s} \setminus (B_{i_{s+1}} \cup \dots \cup B_{i_c})| \\
 = & |B \cap B_1 \cap \dots \cap B_c| \\
 & + \sum_{\substack{1 \leq s \leq c-1 \\ \{i_1, i_2, \dots, i_{c-1}\} \\ = \{1, \dots, c\}}} |B \cap B_1 \cap B_{i_2} \cap \dots \cap B_{i_{s-1}} \setminus (B_{i_s} \cup \dots \cup B_{i_{c-1}})| \\
 & + \sum_{\substack{1 \leq s \leq c-1 \\ \{1, i_1, \dots, i_{c-1}\} \\ = \{1, \dots, c\}}} |B \cap B_{i_1} \cap \dots \cap B_{i_s} \setminus (B_{i_{s+1}} \cup \dots \cup B_{i_{c-1}} \cup B_1)| \\
 = & |B \cap B_1| + N_1 \\
 \leq & \lambda + (c-1)(\lambda - \mu_{c+1}) \quad (\text{from (2) and (4)}) \\
 = & c\lambda - (c-1)\mu_{c+1} \tag{6}
 \end{aligned}$$

Theorem 3.1 *A block design (X, \mathcal{B}) is c -exposed if*

$$k > c^2\lambda - c(c-1)\mu_{c+1} \tag{7}$$

Proof: Applying (7) to (5) and (6) results in $|F \cap B_h| > |F \cap B|$. □

4 Existence from SBIBDs

We will show in this section that SBIBDs with parameters satisfying (7) exist.

4.1 Family of 2-exposed SBIBDs

From theorem 2.1, we have obtained that a (v, k, λ) -SBIBD is 2-exposed if $k > 4\lambda$. By this we have the following 2-exposed SBIBDs.

Theorem 4.1 *Let q be a prime power and $n \geq 2$ be an integer.*

1. ([2], pp.244) *There exists a*

$$\left(\frac{q^{n+1} - 1}{q - 1}, \frac{q^n - 1}{q - 1}, \frac{q^{n-1} - 1}{q - 1} \right)\text{-SBIBD.}$$

2. The $\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right)$ -SBIBD is 2-exposed if $q > 4$.

Theorem 4.2 Let p^a and $q^b = 3p^a + 2$ be prime powers.

1. ([2], pp.280) Then there exists a

$$\left(p^a q^b, \frac{p^a q^b - 1}{4}, \frac{p^a q^b - 5}{16}\right)\text{-SBIBD}$$

provided that $(p^a q^b - 1)/4$ is an odd square.

2. The $\left(p^a q^b, \frac{p^a q^b - 1}{4}, \frac{p^a q^b - 5}{16}\right)$ -SBIBD is 2-exposed.

Theorem 4.3 Let q be a prime power, d be a positive integer.

1. ([2], pp.280) There exists a

$$\left(q^{d+1}(q^d + \dots + q + 2), q^d(q^d + \dots + q + 1), q^d(q^{d-1} + \dots + q + 1)\right)\text{-SBIBD}$$

2. The $\left(q^{d+1}(q^d + \dots + q + 2), q^d(q^d + \dots + q + 1), q^d(q^{d-1} + \dots + q + 1)\right)$ -SBIBD is 2-exposed if $q > 4$.

4.2 Family of 3-exposed SBIBDs

From theorem 3.1 we have obtained that a (v, k, λ) -SBIBD is 3-exposed if $k > 9\lambda$. Therefore we have 3-exposed SBIBDs below.

Theorem 4.4 There exist 3-exposed SBIBDs.

1. The $\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right)$ -SBIBD is 3-exposed if $q \geq 9$.
2. The $\left(q^{d+1}(q^d + \dots + q + 2), q^d(q^d + \dots + q + 1), q^d(q^{d-1} + \dots + q + 1)\right)$ -SBIBD is 3-exposed if $q > 9$.

5 Existence from Steiner systems

In this section we shall show the existence of 2-exposed designs with parameters satisfying (7) and $\mu_3 > 0$. Let $S(t, k, v)$ be a Steiner system, where v is the size of X and k is the size of blocks, every t points of X occur in exactly one block.

Theorem 5.1 Let $S(3, k, v)$ be a Steiner system. Its complement is 2-exposed if

$$\frac{v(v-1)}{k(k-1)} > 4\frac{v-2}{k-2} - 2 \tag{8}$$

Proof: Let (X, \mathcal{B}) be the Steiner system. It is also a $2 - (v, k, \lambda)$ -design with $\lambda = (v - 2)/(k - 2)$ and $b \geq v$. Each point occurs in $r = v(v - 1)/k(k - 1)$ blocks.

Consider its complementary (X', \mathcal{B}') . The size of each block is $k' = v(v - 1)/k(k - 1)$. Every three blocks intersect in exactly $\mu'_3 = 1$ point. Every two blocks intersect in exactly $\lambda' = (v - 2)/(k - 2)$ points. Theorem 2.1 and (8) indicates that (X', \mathcal{B}') is 2-exposed. □

Example 5.1 ([1], pp.67) *There are known families of Steiner systems:*

1. $S(3, q + 1, q^n + 1)$, q is a prime power, $n \geq 2$;
2. $S(3, q + 1, u^\ell q^n + 1)$, q is a prime power, u a prime power satisfying the standard divisibility conditions, $\ell \geq 0$, and $n \geq n_0$, n_0 is a constant depending only on q, u .

6 A note on application

The c -exposure property of a block design provides a capability of revealing all the blocks used to build a false block. Revealing the block(s) that built a false block is expected in a traitor tracing schemes (eg [3, 4]). However, to apply a c -exposed block design to a c -traceability scheme we need an assumption that every block (representing a traitor) has an equal contribution to the false block (representing a pirate decoder). In this case up to c blocks are able to be identified provided that the traitors choose the strategy of avoiding being the sole traitor identified. This strategy is likely as any pirate decoder who provides more contributions would be identified before, or instead of, fellow traitors.

References

- [1] C. J. Colbourn and J. H. Dinitz, Eds. *CRC Handbook of Combinatorial Designs*. CRC Press, 1996.
- [2] J. H. Dinitz and D. Stinson. *Contemporary Design Theory, A Collection of Surveys*. A Wiley Interscience Publications, John Wiley & Sons, 1992.
- [3] D. Stinson and R. Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM Journal on Discrete Mathematics* **11** (1998), 41–53.
- [4] D. R. Stinson and R. Wei. Key preassigned traceability schemes for broadcast encryption. In *Proceedings of SAC'98, Lecture Notes in Computer Science*, **1556** (1999), 144–156. Springer-Verlag, Berlin, Heidelberg, New York.