A new class of 2-fold perfect 4-splitting authentication codes*

Miao Liang[1] Sufang Jiang[2] Beiliang Du[2]

1 Foundation Department, Suzhou Vocational University, Suzhou 215104, P.R. China
2 Department of Mathematics, Soochow University (Suzhou University), Suzhou 215006, P.R. China

Abstract Restricted strong partially balanced t-designs were first formulated by Pei, Li, Wang and Safavi-Naini investigation of authentication codes with arbitration. We in recent proved that optimal splitting authentication codes that are multi-fold perfect against spoofing can be characterized in terms of restricted strong partially balanced t-designs. This article investigates the existence of optimal restricted strong partially balanced 2-design ORSPBD$(v, 2 \times 4, 1)$, and shows that there exists an ORSPBD$(v, 2 \times 4, 1)$ for even v. As its application, we obtain a new infinite class of 2-fold perfect 4-splitting authentication codes.

Keywords: restricted strong partially balanced t-designs, splitting authentication codes, splitting group divisible designs

1 Introduction

Let $\mathcal{S}$ denote a finite set of source states (or plaintexts), $\mathcal{M}$ a finite set of messages (or ciphertexts), and $\mathcal{E}$ a finite set of encoding rules (or keys). Using an encoding rule $e \in \mathcal{E}$, the transmitter encrypts a source state $s \in \mathcal{S}$ to obtain the message $m = e(s)$ to be sent over the channel. The encoding rule is communicated to the receiver via a secure channel prior to any messages being sent. When it is possible that more than one message can be used to communicate a particular source state $s \in \mathcal{S}$ under the same encoding rule $e \in \mathcal{E}$, then the authentication code is said to have splitting. In this case, a message $m \in \mathcal{M}$ is computed as $m = e(s, r)$, where r denotes a random number chosen from some specified finite set $\mathcal{R}$. If we define

*This work was supported by the National Natural Science Foundation of China (Grant No. 11171248).

Correspondence to: Beiliang Du, Department of Mathematics, Soochow University (Suzhou University), Suzhou 215006, China, E-mail: dubl@suda.edu.cn

$$e(s) := \{m \in \mathcal{M} : m = e(s,r) \text{ for some } r \in \mathcal{R}\}$$

for each encoding rule $e \in \mathcal{E}$ and source state $s \in \mathcal{S}$, then splitting means that $|e(s)| > 1$ for some $e \in \mathcal{E}$ and some $s \in \mathcal{S}$. A splitting authentication code is called c-splitting if $|e(s)| = c$ for every encoding rule $e \in \mathcal{E}$ and every source $s \in \mathcal{S}$.

We address the scenario of a spoofing attack of order r: Suppose that an opponent observes $r \geq 0$ distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message m' (being distinct from the r messages already sent), hoping to have it accepted by the receiver as authentic. The cases $r = 0$ and $r = 1$ are called impersonation game and substitution game, respectively.

For any r, the deception probability P_r denotes the probability that the opponent can deceive the transmitter/receiver with a spoofing attack of order r. We have the following information-theoretic lower bounds on deception probabilities, and a information-theoretic lower bound on the size of encoding rules for splitting authentication codes that are multi-fold secure against spoofing. We define

$$\mathcal{M}^r = \{m^r = (m_1, m_2, \cdots, m_r) : m_i \in \mathcal{M}, 1 \leq i \leq r\}$$

and write E and M^r for the random variables describing the splitting authentication code and taking vales e and m^r in $\mathcal{E}$ and $\mathcal{M}^r$, respectively.

Lemma 1.1 [15, 16] In a splitting authentication code, for every $0 \leq r \leq t-1$, the deception probabilities are bounded below by

$$P_r \geq 2^{H(E|M^{r+1})-H(E|M^r)}.$$

A splitting authentication code is called *t-fold key-entropy minimal* if the deception probabilities meet the lower bounds with equality for all $0 \leq r \leq t-1$.

Lemma 1.2 [15, 16] If a splitting authentication code is t-fold key-entropy minimal, then the number of encoding rules is bounded below by

$$|\mathcal{E}| \geq (P_0 P_1 \cdots P_{t-1})^{-1}.$$

Analogously, we call a splitting authentication code *t-fold perfect* if the number of encoding rules meets the lower bound with equality.

We [11] in recent proved that optimal splitting authentication codes that are multi-fold perfect against spoofing can be characterized in terms of restricted strong partially balanced t-designs. Let v, b, u, k, λ, t be positive integers and $t \leq u$. A *restricted partially balanced t-design* RPBD$(v, b, u \times k; \lambda, 0)$ is a pair $(X, \mathcal{B})$ where X is a v-set (of *points*) and $\mathcal{B}$ is a collection of b subsets of X (called *blocks*) with size uk such that the following properties are satisfied:

1. every $B \in \mathcal{B}$ is expressed as a disjoint union of u subblocks of size k: $B = B_1 \cup B_2 \cup \cdots \cup B_u$,
2. for every t-subset $\{x_1, x_2, \cdots, x_t\}$ of X either occurs together in exactly λ blocks $B = B_1 \cup B_2 \cup \cdots \cup B_u$ such that $x_1 \in B_{i_1}, x_2 \in B_{i_2}, \cdots, x_t \in B_{i_t}$ $(i_j, j = 1, 2, \cdots, t$, different in any two) or does not occur in any block.

The blocks of a t-design RPBD$(v, b, u \times k; \lambda, 0)$ will be displayed in the form $\{a_1^{(1)}, a_2^{(1)}, \cdots, a_k^{(1)}; a_1^{(2)}, a_2^{(2)}, \cdots, a_k^{(2)}; \cdots; a_1^{(u)}, a_2^{(u)}, \cdots, a_k^{(u)}\}$ in this paper. The number $\mid X \mid = v$ is called the order of restricted partially balanced t-design. It is easy to see that $b \leq \lfloor \frac{v}{uk} \lfloor \frac{v-1}{(u-1)k} \cdots \lfloor \frac{\lambda(v-t+1)}{(u-t+1)k} \rfloor \rfloor \rfloor$, where $\lfloor x \rfloor$ denotes the greatest integer satisfying $\lfloor x \rfloor \leq x$.

If a restricted partially balanced t-design RPBD$(v, b, u \times k; \lambda, 0)$ is a restricted partially balanced s-design RPBD$(v, b, u \times k; \lambda_s, 0)$ for $0 < s < t$ as well, then it is called a restricted strong partially balanced t-design and is denoted by t-design RSPBD$(v, b, u \times k; \lambda, 0)$. It is easy to see that a restricted strong partially balanced t-design is also a 1-design, that is $\lambda_1 = r_v$, the number of blocks which contain a fixed point.

Restricted strong partially balanced t-designs were first formulated by Pei, Li, Wang and Safavi-Nai [17] in investigation of authentication codes with arbitration (see, also, [15, 16]). We [11] in recent established its another application in splitting authentication codes.

Theorem 1.3 [11] Suppose there is a t-design RSPBD$(v, b, u \times k; 1, 0)$ with $t \geq 2$. Then there is a t-fold perfect k-splitting authentication code for u equiprobable source states, having v messages and b encoding rules. Conversely, if there is a t-fold perfect k-splitting authentication code for u source states, having v messages and b encoding rules, then there is a t-design RSPBD$(v, b, u \times k; 1, 0)$.

A restricted strong partially balanced t-design RSPBD$(v, b, u \times k; \lambda, 0)$ is optimal if b is the maximum number of blocks in all t-design RSPBD$(v, b, u \times k; \lambda, 0)$s (or equivalently, r_v is the maximum number of blocks which contain a fixed point in all t-design RSPBD$(v, b, u\times k; \lambda, 0)$s). An optimal restricted strong partially balanced 2-design is denoted briefly by ORSPBD$(v, u \times k, \lambda)$.

t-design ORSPBD$(v, b, u\times k; \lambda, 0)$s have been studied by many researchers (see, for example, Ogata, Kurosawa, Stinson and Saido [14], Du [5, 6], Liang and Du [9], Ge, Miao and Wang [7], Wang [18], Wang and Su [19] and Chee, Zhang and Zhang [1]). We [12, 13] have determined the existence of optimal restricted strong partially balanced 2-design ORSPBD$(v, u \times k, 1)$ with $u \times k = 2 \times 2, 2 \times 3$ and 3×2. From Theorem 1.3, we then established a class of 2-fold perfect 2-splitting authentication codes with 2 source states, a class of 2-fold perfect 3-splitting authentication codes with 2 source states and a class of 2-fold perfect 2-splitting authentication codes with 3 source states. We [10, 11] and Chee, Zhang and Zhang [1] also have obtained two classes of optimal restricted strong partially balanced 3-design ORSPBD$(v, b, 3 \times 2, 1)$ and then established two classes of 3-fold perfect 2-splitting authentication codes with 3 source states. In this article, we focus on the existence of the optimal restricted strong partially balanced 2-design ORSPBD$(v, 2 \times 4, 1)$ for even v.

An easy calculation shows that $r_v \leq \lfloor \frac{(v-1)}{k(u-1)} \rfloor$ for an optimal restricted strong partially balanced 2-design ORSPBD$(v, u \times k, 1)$. Let $m_v = \max \{m : m$ is a positive integer, $m \leq \lfloor \frac{(v-1)}{k(u-1)} \rfloor$ and $mv \equiv 0 \pmod{uk}\}$ and $v \equiv v_0 \pmod{k^2u(u-1)}$, $1 \leq v_0 \leq k^2u(u-1)$. For every case $v \equiv v_0 \pmod{k^2u(u-1)}$ and $1 \leq v_0 \leq k^2u(u-1)$, we calculate the maximum m which satisfied $m \leq \lfloor \frac{(v-1)}{k(u-1)} \rfloor$ and $mv \equiv 0 \pmod{uk}$. Then we have the following expression of m_v for $u \times k = 2 \times 4$.

$$m_v = \begin{cases} \frac{v}{4} - 1, & v_0 \equiv 0 \pmod 4, \\ \frac{v-v_0}{4} + 4, & v_0 = 18,\ 22,\ 26,\ 30, \\ \frac{v-v_0}{4}, & \text{otherwise.} \end{cases}$$

We shall prove $r_v = m_v$. That is, our main objective is to establish the following results.

Theorem 1.4 There exists an ORSPBD$(v, 2 \times 4, 1)$ for even v.

From Theorems 1.3, we then have the following result, where b is the number of the blocks of the ORSPBD$(v, 2 \times 4, 1)$ in Theorem 1.4.

Theorem 1.5 Let $v \equiv 0 \pmod 2$ and $v \geq 8$. Then there exists a 2-fold perfect 4-splitting authentication code with $|\mathcal{M}| = v$, $|\mathcal{E}| = b$, and $|\mathcal{S}| = 2$.

2 Preliminaries

In this section we shall define some of the auxiliary designs and some of the fundamental results which will be used later. The reader is referred to [2, 5, 14] for more information on designs, and, in particular, group divisible designs and splitting group divisible designs.

Let K and M be sets of positive integers. A *group divisible design* (GDD) GD$[K, 1, M; v]$ is a triple $(X, \mathcal{G}, \mathcal{B})$ where X is a v-set (of *points*), $\mathcal{G}$ is a collection of nonempty subsets of X (called *groups*) with cardinality in M and $\mathcal{B}$ is a collection of subsets of X (called *blocks*) with cardinality at least two, in K, such that the following properties are satisfied.

1. $\mathcal{G}$ partition X,
2. no block intersects any group in more than one point, and,
3. each pair set $\{x, y\}$ of points not contained in a group is contained in exactly one block.

The group-type (or type) of the GDD $(X, \mathcal{G}, \mathcal{B})$ is the multiset of sizes $|G|$ of the group $G \in \mathcal{G}$ and we usually use the "exponential" notation for its description: group-type $1^i 2^j 3^k \cdots$ denotes i occurrences of groups of size 1, j occurrences of groups of size 2, and so on.

We need to establish some more notations. We shall denote by GD$[k, 1, m; v]$ a GD$[\{k\}, 1, \{m\}; v]$. We shall sometimes refer to a GD$[K, 1, M; v]$ $(X, \mathcal{G}, \mathcal{B})$ as a K-GDD.

Lemma 2.1 There exists a $\{2\}$-GDD of type $m^u n^1$ for any positive integers m and n.

For our purpose we need to introduce the concept of splitting group divisible designs. Let u and k be positive integers and M be set of positive integers. A *splitting group divisible design* (splitting GDD) splitting GD$[u \times k, 1, M; v]$, is a triple $(X, \mathcal{G}, \mathcal{B})$ where X is a v-set (of *points*), $\mathcal{G}$ is a collection of nonempty subsets of X (called *groups*) with cardinality in M and $\mathcal{B}$ is a collection of subsets of X (called *blocks*) with cardinality uk such that the following properties are satisfied.

1. $\mathcal{G}$ partition X,
2. every $B \in \mathcal{B}$ is expressed as a disjoint union of u subblocks of size k: $B = B_1 \cup B_2 \cup \cdots \cup B_u$,

3. no block intersects any group in more than one subblock, and,
4. for each pair set $\{x, y\}$ of X not contained in a group, there exists exactly one block $B = B_1 \cup B_2 \cup \cdots \cup B_u$ such that $x \in B_i, y \in B_j$ $(i \neq j)$.

The group-type (or type) of the splitting GDD is the same as that of the GDD. We shall sometimes refer to a splitting GD$[u \times k, 1, M; v]$ $(X, \mathcal{G}, \mathcal{B})$ as a $u \times k$-splitting GDD.

For splitting group divisible designs, we can establish the following results which will be used later.

Lemma 2.2 [12] There exists a $2 \times k$-splitting GDD of type k^u for any $u \geq 2$.

Lemma 2.3 [12] Suppose that there exists a K-GDD of type $g_1 g_2 \cdots g_u$ and that for each $k' \in K$ there exists a $2 \times k$-splitting GDD of type $h^{k'}$. Then there exists a $2 \times k$-splitting GDD of type $(hg_1)(hg_2) \cdots (hg_u)$.

We shall illustrate the main technique that will be used throughout the remainder of the article, which is "Filling in Holes" construction. As the "Filling in Holes" construction will generally involve adjoining more than one infinite point to a splitting GDD, we will require the notation of an optimal restricted strong partially balanced design with an empty subdesign. Specifically, we write ORSPBD$(v, w; u \times k, 1)$ for a structure $(X, Y, \mathcal{B})$, where X is a set of v points, $Y \subset X$ is a set of w points (Y is called the *hole*), and $\mathcal{B}$ is a collection of subsets of X (called *blocks*), such that

1. every $B \in \mathcal{B}$ is expressed as a disjoint union of u subblocks of size k: $B = B_1 \cup B_2 \cup \cdots \cup B_u$,
2. for each pair set $\{x, y\}$ of X, there exists exactly one block $B = B_1 \cup B_2 \cup \cdots \cup B_u$ such that $x \in B_i$, $y \in B_j$ $(i \neq j)$ or does not occur in any block,
3. each pair set $\{x, y\}$ of Y do not occur in any block $B = B_1 \cup B_2 \cup \cdots \cup B_u$ such that $x \in B_i$, $y \in B_j$ $(i \neq j)$,
4. for each point of X, there exist exactly r_v blocks $B = B_1 \cup B_2 \cup \cdots \cup B_u$,
5. r_v is the maximum number of blocks which contain a fixed point in all RSPBD$(v,\ u \times k, 1)$.

Now we are in a position to give our main construction.

Construction 2.4 Suppose

1. there exists a 2×4-splitting GDD of type $g_1 g_2 \cdots g_u$, where $g_i \equiv 0 \pmod{32}$ for $1 \leq i \leq u$,
2. there exists an ORSPBD$(g_i + w, w; 2 \times 4, 1)$ for each $i, 1 \leq i < u$, where $w \in \{2, 6, 10, 14\}$,
3. there exists an ORSPBD$(g_u + w, 2 \times k, 1)$.

Then there exists an ORSPBD$(v, 2 \times k, 1)$, where $v = w + \sum_{1 \leq i \leq u} g_i$.

Proof We start with a 2×4-splitting GDD of type $g_1 g_2 \cdots g_u$ $(X, \mathcal{G}, \mathcal{B})$, where $\mathcal{G} = \{G_1, G_2, \cdots, G_u\}$, $|G_i| = g_i$, $1 \leq i \leq u$. For each G_i, $1 \leq i < u$, let $(G_i \cup W, \mathcal{A}_i)$ be the ORSPBD$(g_i + w, w; 2 \times 4, 1)$, where $|W| = w$ and $X \cap W = \emptyset$. Let $(G_u \cup W, \mathcal{A}_u)$ be the ORSPBD$(g_u + w, 2 \times 4, 1)$. Then the design we construct will have point set

$$X^* = X \cup W,$$

and the block set

$$\mathcal{B}^* = \mathcal{B} \cup (\textstyle\bigcup_{1 \leq i \leq u} \mathcal{A}_i),$$

It is easy to check that the $(X^*, \mathcal{B}^*)$ is an ORSPBD$(v, 2 \times 4, 1)$ with $r_v = \frac{v-w}{4} = m_v$. □

Construction 2.5 Suppose that u is odd, and

1. there exists a 2×4-splitting GDD of type $g_1 g_2 \cdots g_u$, where $g_i \equiv 16 \pmod{32}$ for $1 \leq i \leq u$,
2. there exists an ORSPBD$(g_i + w, w; 2 \times 4, 1)$ for each i, $1 \leq i < u$, where $w \in \{2, 6, 10, 14\}$,
3. there exists an ORSPBD$(g_u + w, 2 \times 4, 1)$.

Then there exists an ORSPBD($v, 2 \times 4, 1$), where $v = w + \sum_{1 \leq i \leq u} g_i$.

Proof It is the same as Construction 2.4 to get the design $(X^*, \mathcal{B}^*)$, and easy to check that it is an ORSPBD($v, 2 \times 4, 1$) with $v \equiv 16 + w \pmod{32}$ and $r_v = \frac{v-(w+16)+16}{4} = m_v$. □

3 ORSPBD$(v, 2 \times 4, 1)$s

In this section, we shall investigate the existence of ORSPBD($v, 2 \times 4, 1$).

Lemma 3.1 [12] There exists an ORSPBD($v, 2\times4, 1$) for any $v \equiv 0 \pmod 4$ and $v \geq 8$.

Lemma 3.2 There exists an ORSPBD($v, w; 2 \times 4, 1$) for $(v, w) = \{(34, 2), (38, 6), (42, 10), (46, 14)\}$.

Proof We construct directly the designs as follows:

ORSPBD($34, 2; 2 \times 4, 1$):

Point set: $X = Z_{34}$, $Y = Z_2$.

Block set: Develop the following blocks +2 mod 34:

$\{0, 1, 2, 3; 4, 5, 8, 9\}$, $\{0, 1, 2, 3; 12, 13, 16, 17\}$.

ORSPBD($38, 6; 2 \times 4, 1$):

Point set: $X = Z_{38}$, $Y = Z_6$.

Block set: $\{0, 1, 2, 3; 6, 7, 8, 9\}$, $\{0, 1, 2, 3; 22, 23, 24, 25\}$,

$\{0, 1, 2, 3; 10, 11, 12, 13\}$, $\{0, 1, 2, 3; 26, 27, 28, 29\}$, $\{0, 1, 2, 3; 14, 15, 16, 17\}$,

$\{0, 1, 2, 3; 30, 31, 32, 33\}$, $\{0, 1, 2, 3; 18, 19, 20, 21\}$, $\{0, 1, 2, 3; 34, 35, 36, 37\}$,

$\{4, 5, 6, 7; 8, 9, 10, 11\}$, $\{4, 5, 22, 23; 24, 25, 26, 27\}$, $\{4, 5, 6, 7; 12, 13, 14, 15\}$,

$\{4, 5, 22, 23; 28, 29, 30, 31\}$, $\{4, 5, 6, 7; 16, 17, 18, 19\}$, $\{6, 7, 8, 9; 26, 27, 28, 29\}$,

$\{4, 5, 8, 9; 20, 21, 22, 23\}$, $\{4, 5, 24, 25; 36, 37, 6, 7\}$, $\{4, 5, 22, 23; 32, 33, 34, 35\}$,

$\{6, 7, 8, 9; 30, 31, 32, 33\}$, $\{6, 7, 8, 9; 34, 35, 36, 37\}$, $\{8, 9, 10, 11; 16, 17, 18, 19\}$,

$\{22, 23, 24, 25; 18, 19, 20, 21\}$, $\{22, 23, 24, 25; 10, 11, 12, 13\}$,

$\{24,25,26,27;28,29,30,31\}$, $\{24,25,26,27;32,33,34,35\}$,
$\{10,11,12,13;20,21,30,31\}$, $\{26,27,28,29;36,37,14,15\}$,
$\{26,27,28,29;16,17,18,19\}$, $\{10,11,30,31;28,29,36,37\}$,
$\{12,13,14,15;16,17,36,37\}$, $\{28,29,30,31;32,33,20,21\}$,
$\{30,31,32,33;34,35,18,19\}$, $\{16,17,18,19;20,21,36,37\}$,
$\{10,11,12,13;32,33,34,35\}$, $\{26,27,14,15;12,13,20,21\}$,
$\{14,15,16,17;18,19,34,35\}$, $\{32,33,34,35;36,37,20,21\}$,
$\{22,23,24,25;14,15,16,17\}$, $\{8,9,10,11;12,13,14,15\}$.

ORSPBD$(42,10;2\times 4,1)$:
Point set: $X = Z_{42}$, $Y = Z_{10}$.
Block set: $\{0,1,2,3;10,11,12,13\}$, $\{0,1,2,3;26,27,28,29\}$,
$\{0,1,2,3;14,15,16,17\}$, $\{0,1,2,3;30,31,32,33\}$, $\{0,1,2,3;18,19,20,21\}$,
$\{0,1,2,3;34,35,36,37\}$, $\{0,1,2,3;22,23,24,25\}$, $\{0,1,2,3;38,39,40,41\}$,
$\{4,5,6,7;10,11,12,13\}$, $\{4,5,6,7;26,27,28,29\}$, $\{4,5,6,7;14,15,16,17\}$,
$\{4,5,6,7;30,31,32,33\}$, $\{4,5,6,7;18,19,20,21\}$, $\{4,5,6,7;34,35,36,37\}$,
$\{30,31,32,33;20,21,22,23\}$, $\{20,21,22,23;24,25,40,41\}$,
$\{12,13,14,15;22,23,24,25\}$, $\{28,29,30,31;38,39,40,41\}$,
$\{30,31,32,33;36,37,18,19\}$, $\{14,15,16,17;36,37,38,39\}$,
$\{16,17,18,19;24,25,40,41\}$, $\{32,33,34,35;40,41,24,25\}$,
$\{8,9,14,15;10,11,12,13\}$, $\{10,11,12,13;16,17,18,19\}$,
$\{8,9,34,35;30,31,32,33\}$, $\{10,11,12,13;32,33,34,35\}$,
$\{8,9,10,11;22,23,24,25\}$, $\{26,27,28,29;20,21,22,23\}$,
$\{8,9,26,27;38,39,40,41\}$, $\{26,27,28,29;32,33,34,35\}$,
$\{8,9,22,23;18,19,20,21\}$, $\{10,11,12,13;20,21,30,31\}$,
$\{8,9,38,39;34,35,36,37\}$, $\{26,27,28,29;16,17,18,19\}$,
$\{8,9,30,31;26,27,28,29\}$, $\{36,37,38,39;40,41,24,25\}$,
$\{8,9,18,19;14,15,16,17\}$, $\{26,27,28,29;36,37,14,15\}$,
$\{4,5,6,7;38,39,40,41\}$, $\{10,11,12,13;36,37,38,39\}$,

$\{4,5,6,7;22,23,24,25\}$, $\{14,15,16,17;20,21,34,35\}$.

ORSPBD$(46,14;2\times 4,1)$:

Point set: $X = Z_{46}$, $Y = Z_{14}$.

Block set: $\{0,1,2,3;14,15,16,17\}$, $\{0,1,2,3;30,31,32,33\}$,
$\{0,1,2,3;18,19,20,21\}$, $\{0,1,2,3;34,35,36,37\}$, $\{0,1,2,3;22,23,24,25\}$,
$\{0,1,2,3;38,39,40,41\}$, $\{0,1,2,3;26,27,28,29\}$, $\{0,1,2,3;42,43,44,45\}$,
$\{4,5,6,7;14,15,16,17\}$, $\{4,5,6,7;30,31,32,33\}$, $\{4,5,6,7;18,19,20,21\}$,
$\{4,5,6,7;34,35,36,37\}$, $\{4,5,6,7;22,23,24,25\}$, $\{4,5,6,7;38,39,40,41\}$,
$\{18,19,20,21;28,29,38,39\}$, $\{34,35,36,37;44,45,22,23\}$,
$\{36,37,38,39;40,41,42,43\}$, $\{22,23,24,25;28,29,44,45\}$,
$\{24,25,28,29;26,27,42,43\}$, $\{40,41,44,45;42,43,26,27\}$.
$\{12,13,16,17;28,29,30,31\}$, $\{12,13,32,33;44,45,14,15\}$,
$\{30,31,32,33;18,19,20,21\}$, $\{16,17,18,19;20,21,22,23\}$,
$\{16,17,18,19;24,25,26,27\}$, $\{32,33,34,35;40,41,42,43\}$,
$\{20,21,22,23;24,25,26,27\}$, $\{38,39,40,41;44,45,28,29\}$,
$\{8,9,10,11;14,15,16,17\}$, $\{12,13,30,31;32,33,34,35\}$,
$\{8,9,10,11;30,31,32,33\}$, $\{12,13,30,31;36,37,38,39\}$,
$\{8,9,10,11;22,23,24,25\}$, $\{12,13,14,15;24,25,26,27\}$,
$\{8,9,10,11;42,43,44,45\}$, $\{12,13,14,15;16,17,18,19\}$,
$\{8,9,10,11;18,19,20,21\}$, $\{12,13,14,15;20,21,22,23\}$,
$\{8,9,10,11;34,35,36,37\}$, $\{12,13,30,31;40,41,42,43\}$,
$\{8,9,10,11;38,39,40,41\}$, $\{14,15,16,17;34,35,36,37\}$,
$\{8,9,10,11;26,27,28,29\}$, $\{32,33,34,35;36,37,38,39\}$,
$\{4,5,6,7;26,27,28,29\}$, $\{4,5,6,7;42,43,44,45\}$. □

Lemma 3.3 There exists an ORSPBD$(v,2\times 4,1)$ for any $v \equiv v_0 \pmod{32}$, $v_0 \in \{2,6,10,14\}$.

Proof we begin with a 2-GDD of type 8^t, $t \geq 2$ (for whose existence, see Lemma 2.1), give the points weight 4, and apply Lemma 2.3 with the input design 2×4-splitting GDD of type 4^2 to obtain a 2×4-splitting GDD of type 32^t, $t \geq 2$. The desired result follows from Construction 2.4 with the input designs ORSPBD$(v, w; 2 \times 4, 1)$s for $(v, w) = \{(34, 2), (38, 6), (42, 10), (46, 14)\}$ (for whose existence, see Lemma 3.2). □

Lemma 3.4 There exists an ORSPBD$(v, w; 2 \times 4, 1)$ for $(v, w) = \{(18, 2), (22, 6), (26, 10)\}$.

Proof We construct directly the designs as follows:

ORSPBD$(18, 2; 2 \times 4, 1)$:

Point set: $X = Z_{18}$, $Y = Z_2$.

Block set: Develop the following blocks +2 mod 18: $\{0, 1, 2, 3; 4, 5, 8, 9\}$.

ORSPBD$(22, 6; 2 \times 4, 1)$:

Point set: $X = Z_{22}$, $Y = Z_6$.

Block set: $\{0, 1, 2, 3; 6, 7, 8, 9\}$, $\{0, 1, 2, 3; 10, 11, 12, 13\}$,

$\{0, 1, 2, 3; 14, 15, 16, 17\}$, $\{0, 1, 2, 3; 18, 19, 20, 21\}$, $\{4, 5, 10, 11; 6, 7, 8, 9\}$,

$\{4, 5, 14, 15; 10, 11, 12, 13\}$, $\{4, 5, 18, 19; 14, 15, 16, 17\}$,

$\{6, 7, 8, 9; 12, 13, 14, 15\}$, $\{12, 13, 20, 21; 16, 17, 18, 19\}$,

$\{4, 5, 6, 7; 18, 19, 20, 21\}$, $\{8, 9, 10, 11; 16, 17, 20, 21\}$.

ORSPBD$(26, 10; 2 \times 4, 1)$:

Point set: $X = Z_{26}$, $Y = Z_{10}$.

Block set: $\{0, 1, 2, 3; 10, 11, 12, 13\}$, $\{0, 1, 2, 3; 14, 15, 16, 17\}$,

$\{0, 1, 2, 3; 18, 19, 20, 21\}$, $\{0, 1, 2, 3; 22, 23, 24, 25\}$, $\{4, 5, 6, 7; 10, 11, 12, 13\}$,

$\{4, 5, 6, 7; 14, 15, 16, 17\}$, $\{4, 5, 6, 7; 18, 19, 20, 21\}$, $\{4, 5, 6, 7; 22, 23, 24, 25\}$,

$\{8, 9, 14, 15; 10, 11, 12, 13\}$, $\{8, 9, 18, 19; 14, 15, 16, 17\}$,

$\{8, 9, 10, 11; 22, 23, 24, 25\}$, $\{8, 9, 22, 23; 18, 19, 20, 21\}$,

$\{12, 13, 16, 17; 20, 21, 24, 25\}$. □

Lemma 3.5 There exists an ORSPBD$(v, 2 \times 4, 1)$ for any $v \equiv v_0 \pmod{32}$, $v_0 \in \{18, 22, 26\}$.

Proof we begin with a 2-GDD of type 4^{2t+1}, $t \geq 1$ (for whose existence, see Lemma 2.1), give the points weight 4, and apply Lemma 2.3 with the input design 2×4-splitting GDD of type 4^2 to obtain a 2×4-splitting GDD of type 16^{2t+1}, $t \geq 1$. The desired result follows from Construction 2.5 with the input designs ORSPBD$(v, w; 2 \times 4, 1)$s for $(v, w) = \{(18, 2), (22, 6), (26, 10)\}$ (for whose existence, see Lemma 3.4). □

Lemma 3.6 There exists an ORSPBD$(v, 2 \times 4, 1)$ $v \in \{30, 94\}$ and an ORSPBD$(62, 14; 2 \times 4, 1)$.

Proof We construct directly the designs as follows:

ORSPBD$(30, 2 \times 4, 1)$:

Point set: $X = Z_{30}$.

Block set: Develop the following blocks +2 mod 30: $\{0, 1, 2, 3; 4, 5, 8, 9\}$.

ORSPBD$(94, 2 \times 4, 1)$:

Point set: $X = Z_{94}$.

Block set: Develop the following blocks +2 mod 94:

$\{0, 1, 2, 3; 4, 5, 8, 9\}$, $\{0, 1, 2, 3; 12, 13, 16, 17\}$, $\{0, 1, 2, 3; 20, 21, 24, 25\}$,

$\{0, 1, 2, 3; 28, 29, 32, 33\}$, $\{0, 1, 2, 3; 36, 37, 40, 41\}$.

ORSPBD$(62, 14; 2 \times 4, 1)$:

Point set: $X = Z_{62}$, $Y = Z_{14}$.

Block set: $\{0, 1, 2, 3; 30, 31, 32, 33\}$, $\{0, 1, 2, 3; 46, 47, 48, 49\}$,

$\{0, 1, 2, 3; 14, 15, 16, 17\}$, $\{0, 1, 2, 3; 34, 35, 36, 37\}$, $\{0, 1, 2, 3; 50, 51, 52, 53\}$,

$\{0, 1, 2, 3; 18, 19, 20, 21\}$, $\{0, 1, 2, 3; 38, 39, 40, 41\}$, $\{0, 1, 2, 3; 54, 55, 56, 57\}$,

$\{0, 1, 2, 3; 22, 23, 24, 25\}$, $\{0, 1, 2, 3; 42, 43, 44, 45\}$, $\{0, 1, 2, 3; 58, 59, 60, 61\}$,

$\{0, 1, 2, 3; 26, 27, 28, 29\}$, $\{4, 5, 6, 7; 30, 31, 32, 33\}$, $\{4, 5, 6, 7; 46, 47, 48, 49\}$,

$\{4, 5, 6, 7; 14, 15, 16, 17\}$, $\{4, 5, 6, 7; 34, 35, 36, 37\}$, $\{4, 5, 6, 7; 50, 51, 52, 53\}$,

$\{4, 5, 6, 7; 18, 19, 20, 21\}$, $\{4, 5, 6, 7; 38, 39, 40, 41\}$, $\{4, 5, 6, 7; 54, 55, 56, 57\}$,

$\{4, 5, 6, 7; 22, 23, 24, 25\}$, $\{4, 5, 6, 7; 42, 43, 44, 45\}$, $\{4, 5, 6, 7; 58, 59, 60, 61\}$,

$\{12, 13, 58, 59; 54, 55, 56, 57\}$, $\{24, 25, 27, 29; 42, 44, 60, 61\}$,

$\{30, 31, 32, 33; 36, 37, 38, 39\}$, $\{46, 47, 48, 49; 52, 53, 54, 55\}$,

$\{12,13,30,31;42,43,44,45\}$, $\{12,13,46,47;58,59,60,61\}$,

$\{30,31,34,35;48,49,50,51\}$, $\{46,47,50,51;16,17,18,19\}$,

$\{30,31,35,36;52,53,54,55\}$, $\{46,47,51,52;20,21,22,23\}$,

$\{30,31,33,34;40,41,46,47\}$, $\{46,47,49,50;56,57,14,15\}$,

$\{14,15,19,20;36,37,38,39\}$, $\{30,31,36,37;56,57,58,59\}$,

$\{14,15,20,21;40,41,42,43\}$, $\{30,31,37,38;60,61,16,21\}$,

$\{14,15,21,22;44,45,48,53\}$, $\{32,33,34,35;42,43,44,45\}$,

$\{16,17,18,19;26,27,28,29\}$, $\{32,33,35,36;60,61,16,17\}$,

$\{16,17,19,20;44,45,48,49\}$, $\{32,33,36,37;50,22,23,24\}$,

$\{16,17,20,21;34,54,55,56\}$, $\{32,33,37,38;55,25,26,27\}$,

$\{16,17,21,22;39,57,58,59\}$, $\{34,35,36,39;25,26,27,28\}$,

$\{18,19,20,23;57,58,59,60\}$, $\{34,35,38,39;56,57,58,59\}$,

$\{18,19,22,23;40,41,42,43\}$, $\{36,37,38,39;40,41,44,45\}$,

$\{20,21,22,23;24,25,28,29\}$, $\{40,41,42,43;44,45,56,61\}$,

$\{24,25,26,27;28,29,40,45\}$, $\{40,41,43,45;58,60,28,29\}$,

$\{46,47,52,53;24,25,26,27\}$, $\{46,47,53,54;28,29,32,37\}$,

$\{48,49,50,51;58,59,60,61\}$, $\{48,49,51,52;28,29,32,33\}$,

$\{48,49,52,53;18,38,39,40\}$, $\{48,49,53,54;23,41,42,43\}$,

$\{50,51,52,55;41,42,43,44\}$, $\{50,51,54,55;24,25,26,27\}$,

$\{52,53,54,55;56,57,60,61\}$, $\{56,57,58,59;60,61,24,29\}$,

$\{8,9,10,11;46,47,48,49\}$, $\{12,13,50,51;46,47,48,49\}$,

$\{8,9,10,11;50,51,52,53\}$, $\{12,13,38,39;34,35,36,37\}$,

$\{8,9,10,11;54,55,56,57\}$, $\{12,13,54,55;50,51,52,53\}$,

$\{8,9,10,11;58,59,60,61\}$, $\{12,13,42,43;38,39,40,41\}$,

$\{8,9,10,11;26,27,28,29\}$, $\{12,13,34,35;30,31,32,33\}$,

$\{8,9,10,11;30,31,32,33\}$, $\{12,13,18,19;14,15,16,17\}$,

$\{8,9,10,11;14,15,16,17\}$, $\{12,13,22,23;18,19,20,21\}$,

$\{8,9,10,11;34,35,36,37\}$, $\{12,13,26,27;22,23,24,25\}$,

$\{8,9,10,11;18,19,20,21\}$, $\{12,13,14,15;26,27,28,29\}$,

$\{8,9,10,11;38,39,40,41\}$, $\{14,15,16,17;20,21,22,23\}$,

$\{8,9,10,11;22,23,24,25\}$, $\{14,15,17,18;24,25,30,31\}$,

$\{8,9,10,11;42,43,44,45\}$, $\{14,15,18,19;32,33,34,35\}$,

$\{4,5,6,7;26,27,28,29\}$, $\{56,57,59,61;26,28,44,45\}$. □

Lemma 3.7 There exists an ORSPBD$(v, 2\times 4, 1)$ for any $v \equiv 30 \pmod{32}$.

Proof ORSPBD$(30, 2\times 4, 1)$, ORSPBD$(62, 2\times 4, 1)$ and ORSPBD$(94, 2\times 4, 1)$ see Lemma 3.6. For the other values of v, we begin with a 2-GDD of type $12^{2t}s^1$, $s = 4, 12, 20$ and $t \geq 1$ (for whose existence, see Lemma 2.1), give the points weight 4, and then apply Lemma 2.3 with the input design 2×4-splitting GDD of type 4^2 to obtain a 2×4-splitting GDD of type $48^{2t}(4s)^1$. The desired result follows from Construction 2.5 with the input designs ORSPBD$(62, 14; 2\times 4, 1)$ and ORSPBD$(4s+14, 2\times 4, 1)$ (for whose existence, see Lemma 3.6). □

Proof of Theorem 1.4 By Lemma 3.1, Lemma 3.3, Lemma 3.5 and Lemma 3.7 we complete the proof of Theorem 1.4.

References

[1] Y.M. Chee, X. Zhang and H. Zhang, *Infinite families of optimal splitting authentication codes secure against spoofing attacks of higher order*, Adv. Math. Commun., **5** (2011), 59-68.

[2] Th. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Bibliographisches Institut, Zurich, 1985.

[3] A.E. Browwer, A. Schrijver and H. Hanani, *Group divisible designs with block size* 4, Discrete Math., **20** (1977), 1-10.

[4] C.J.Colbourn, D.G.Hoffman, and R. Rees, *A new class of group divisible designs with block size three*, J. Combin. Theory Ser A **59** (1992), 73-89.

[5] B. Du, *Splitting balanced incomplete block designs with block size* 3×2, J. Combin. Designs, **12** (2004), 404-420.

[6] B. Du, *Splitting balanced incomplete block designs*, Australas. J. Combin., **31** (2005), 287-298.

[7] G. Ge, Y. Miao and L. Wang, *Combinatorial constructions for optimal splitting authentication codes*, SIAM J. Discrete Math., **18** (2005), 663-678.

[8] H. Hanani, *Balanced incomplete block designs and related designs*, Discrete Math., **11** (1975), 255-369.

[9] M, Liang and B. Du, *Splitting balanced incomplete block designs with block size* 2×4, J. Combin. Math. Combin. Computing, **63** (2007), 159-172.

[10] M, Liang and B. Du, *A new class of splitting* 3*-designs*, , Des. Codes Cryptogr., **60** (2011), 283-290.

[11] M, Liang and B. Du, *A new class of* 3*-fold perfect splitting authentication codes*, Des. Codes Cryptogr., **62** (2012), 109-119.

[12] M, Liang and B. Du, *Existence of optimal restricted strong partially balanced designs*, Utilitas Math., to appear.

[13] M, Liang and B. Du, *A new class of* 2*-fold perfect splitting authentication codes*, preprint.

[14] W. Ogata, K. Kurosawa, D.R. Stinson and H. Saido, *New combinatorial designs and their applications to authentication codes and secret sharing schemes*, Discrete Math., **279** (2004), 383-405.

[15] D. Pei, *Information-theoretic bounds for authentication codes and block designs*, J. Cryptology, **8** (1995), 177-188.

[16] D. Pei, *Authentication Codes and Combinatorial Designs*, Chapman Hall/CRC, Boca Raton, FL, 2006.

[17] D. Pei, Y. Li, Y. Wang and R. Safavi-Naini, *Characterization of authentication codes with arbitration*, Lecture Notes in Computer Science, **1587** (1999), Springer-Verlag, Berlin-Heidelberg-New York, pp. 303-313.

[18] J. Wang, *A new class of optimal* 3*-splitting authentication codes*, Des. Codes Cryptogr., **38** (2006), 373-381.

[19] J. Wang and R. Su, *Further results on the existence of splitting BIBDs and application to authentication codes*, Acta Appl. Math., **109** (2010), 791-803.