Advances in Mathematics of Communications
Volume 5, No. 1, 2011, 59–68

doi:10.3934/amc.2011.5.59

INFINITE FAMILIES OF OPTIMAL SPLITTING AUTHENTICATION CODES SECURE AGAINST SPOOFING ATTACKS OF HIGHER ORDER

Yeow Meng Chee and Xiande Zhang

Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
21 Nanyang Link, Singapore 637371

Hui Zhang

Department of Mathematics
Zhejiang University
Hangzhou, Zhejiang 310027, China

(Communicated by Iwan Duursma)

Abstract. We consider the problem of constructing optimal authentication codes with splitting. New infinite families of such codes are obtained. In particular, we establish the first known infinite family of optimal authentication codes with splitting that are secure against spoofing attacks of order two.

1. Introduction

In the standard model of authentication theory [13, 14, 15, 18], a *transmitter* wants to send some information to a *receiver* across an insecure channel while an *opponent* with access to the channel wants to deceive the receiver. The opponent can either insert new messages into the channel, or intercept messages from the transmitter and modify them into his own. In each case, the opponent's goal is to deceive the receiver into believing that the new messages are authentic (coming from the transmitter). The first attack based on insertion of new messages is known as *impersonation* and the second attack based on modification of messages from the transmitter is known as *substitution*.

More formally, let $\mathcal{S}$ denote the set of all *source states*, $\mathcal{M}$ be the set of all *messages*, and $\mathcal{E}$ be the set of all *encoding rules*. All these are finite sets. A source state is the information the transmitter wishes to communicate to the receiver. An encoding rule is an injection from $\mathcal{S}$ to $2^{\mathcal{M}}$. The transmitter and receiver agree beforehand on a secret encoding rule $e \in \mathcal{E}$. To communicate a source state $s \in \mathcal{S}$, the transmitter determines $M = e(s)$ (note that $M \subseteq \mathcal{M}$) and chooses a message $m \in M$ to send to the receiver. The receiver accepts the received message as authentic if there exists an M in the image of e containing the received message.

2000 *Mathematics Subject Classification:* Primary: 05B30, 94A60, 94C30; Secondary: 11T22.

Key words and phrases: Authentication code, splitting authentication code, splitting t-design.

Y. M. Chee and X. Zhang are supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03. Y. M. Chee is also supported in part by the Nanyang Technological University under Research Grant M58110040.

For the receiver to recover the source state, each encoding rule must satisfy the condition

$$e(s) \cap e(s') = \varnothing, \quad \text{for distinct } s, s' \in \mathcal{S}.$$

The triple $(\mathcal{S}, \mathcal{M}, \mathcal{E})$ is called an *authentication code*, or *A-code* in short.

An A-code $(\mathcal{S}, \mathcal{M}, \mathcal{E})$ can be represented by an $|\mathcal{E}| \times |\mathcal{S}|$ matrix, whose rows are indexed by authentication rules, and columns indexed by source states, such that the entry in row $e \in \mathcal{E}$ and column $s \in \mathcal{S}$ is $e(s)$.

For k an integer and X a finite set, we denote by $\binom{X}{k}$ the set of all k-subsets of X. Research on authentication codes have focused on the case when every encoding rule is an injection from $\mathcal{S}$ to $\binom{\mathcal{M}}{c}$, for some positive c. Such an A-code is called *a c-splitting A-code*. A 1-splitting A-code is also known as an *A-code without splitting*, and a c-splitting A-code with $c \geq 2$ is known as an *A-code with splitting*. A-codes with splitting are useful for the analysis of authentication with arbitration [9], an extended model of authentication introduced by Simmons [16, 17] for the scenario when the transmitter and receiver may both be deceptive.

In a *spoofing attack of order* i [10], the opponent observes i distinct messages sent by the transmitter through the insecure channel under the same encoding rule. The opponent then inserts a new message (distinct from the i messages already sent), hoping to have it accepted by the receiver as authentic. Within this framework, impersonation and substitution attacks are just spoofing attacks of order zero and one, respectively. While these attacks have been rather well studied for A-codes, less is known for the case of spoofing attacks of order $i \geq 2$, especially on c-splitting A-codes when $c \geq 2$.

The probability distribution on the set of source states $\mathcal{S}$ induces a probability distribution on $\binom{\mathcal{S}}{i}$, $i \geq 0$. Given these probability distributions, the transmitter and receiver choose a probability distribution on $\mathcal{E}$, called an *encoding strategy*. For any $s \in \mathcal{S}$ and $e \in \mathcal{E}$, the transmitter also chooses a probability distribution on $e(s)$, called a *splitting strategy*. The opponent is assumed to know the encoding and splitting strategies. The transmitter and receiver chooses the encoding and splitting strategies to minimize the probability of being deceived by the opponent. We denote by P_{d_i} the probability that the opponent can deceive the receiver with a spoofing attack of order i. The following lower bound on P_{d_i} is known.

Proposition 1.1 (Huber [7]). *In a c-splitting A-code* $(\mathcal{S}, \mathcal{M}, \mathcal{E})$,

$$P_{d_i} \geq c \cdot \frac{|\mathcal{S}| - i}{|\mathcal{M}| - i},$$

for every $i \geq 0$.

A c-splitting A-code is said to be $(t-1)$*-fold secure against spoofing* if $P_{d_i} = c(|\mathcal{S}| - i)/(|\mathcal{M}| - i)$, for all i, $0 \leq i < t$. For succinctness, we call such a code a (t, c)*-splitting A-code*.

Huber [7] also showed that the number of encoding rules must be large enough if an A-code is to be $(t-1)$-fold secure against spoofing.

Proposition 1.2 (Huber [7]). *In a* (t, c)*-splitting A-code* $(\mathcal{S}, \mathcal{M}, \mathcal{E})$,

$$|\mathcal{E}| \geq \frac{1}{c^t} \cdot \frac{\binom{|\mathcal{M}|}{t}}{\binom{|\mathcal{S}|}{t}}.$$

For efficiency, we want the number of encoding rules in an A-code to be as small as possible. We call a (t, c)-splitting A-code *optimal* if the lower bound in Proposition 1.2 is met with equality.

The main contribution of this paper is on the construction of optimal (t, c)-splitting A-codes with three source states, for $c \geq 2$ and $t \in \{2, 3\}$. In particular, we show that the following two new families of A-codes exist:

(i) $(2, 5)$-splitting A-codes with three source states and v messages, for all $v \equiv 1 \bmod 150$, $v \neq 301$.
(ii) $(3, 2)$-splitting A-codes with three source states and v messages, for all $v \equiv 2 \bmod 8$.

The $(3, 2)$-splitting A-codes we obtained is the first known infinite family of (t, c)-splitting A-codes with $t > 2$ and $c > 1$. We also prove that a $(2, c)$-splitting A-code with k source states and v messages exists for all sufficiently large v (with k and c fixed).

2. Preliminaries

This section serves to provide notions and results that are required for our construction in subsequent sections.

The ring $\mathbb{Z}/n\mathbb{Z}$ is denoted $\mathbb{Z}_n$.

2.1. Design-theoretic background.

Huber [7] defined *splitting t-designs*, generalizing the splitting 2-designs of Ogata *et al.* [12].

Definition 2.1. Let t, v, k, c, and λ be positive integers, with $t \leq k$ and $ck \leq v$. A *splitting t-design*, or more precisely, a *splitting t-$(v, k \times c, \lambda)$ design*, is a pair $(X, \mathcal{A})$ such that

(i) X is a set of v elements, called *points*;
(ii) $\mathcal{A}$ is a set of $k \times c$ arrays, called *blocks*, with entries from X, such that each point of X occurs at most once in each block;
(iii) for every $\{x_i : 1 \leq i \leq t\} \in \binom{X}{t}$, there are exactly λ blocks in which x_i, $1 \leq i \leq t$, occur in t different rows.

Note that a splitting t-$(v, k \times 1, \lambda)$ design coincides with the classical notion of a t-(v, k, λ) design. Huber [7] proved the equivalence between splitting t-designs and optimal splitting A-codes.

Theorem 2.2 (Huber [7])**.** *There exists a splitting t-$(v, k \times c, 1)$ design if and only if there exists an optimal (t, c)-splitting A-code for k equiprobable source states, having v messages and $\binom{v}{t}/c^t\binom{k}{t}$ encoding rules.*

The *necessary divisibility conditions* for the existence of splitting t-designs are as follows.

Proposition 2.1 (Huber [7])**.** *The necessary conditions for the existence of a splitting t-$(v, k \times c, \lambda)$ design are*

$$\lambda\binom{v-s}{t-s} \equiv 0 \bmod c^{t-s}\binom{k-s}{t-s}, \quad \text{for all } s,\ 0 \leq s \leq t.$$

Sometimes, the points of a splitting t-design $(X, \mathcal{A})$ can be identified with the elements of an additive group Γ, so that $X = \Gamma$. If the set of blocks $\mathcal{A}$ can be generated by a set $\mathcal{B} \subseteq \mathcal{A}$, that is,

$$\mathcal{A} = \cup_{B \in \mathcal{B}}\{B + g : g \in \Gamma\},$$

then $\mathcal{B}$ is called a *set of base blocks* of $(X, \mathcal{A})$.

Example 2.1. Let $X = \mathbb{Z}_{151}$. The set containing the single array

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 5 & 13 & 59 & 105 & 118 \\ 28 & 67 & 73 & 112 & 134 \end{pmatrix}$$

as a base block, generates the set of blocks $\mathcal{A}$ for a splitting 2-$(151, 3 \times 5, 1)$ design $(X, \mathcal{A})$.

Our constructions for splitting t-designs also rely on group divisible designs (GDD). Let t, k, and v be nonnegative integers. A *group divisible t-design of order v and block size k*, denoted GDD(t, k, v), is a triple $(X, \mathcal{G}, \mathcal{A})$ satisfying the following properties:

(i) X is a set of v elements, called *points*;
(ii) $\mathcal{G} = \{G_1, \dots, G_s\}$ is a partition of X into subsets, called *groups*;
(iii) $\mathcal{A} \subseteq \binom{X}{k}$, whose elements are called *blocks*, such that each $A \in \mathcal{A}$ intersects any group $G \in \mathcal{G}$ in at most one point;
(iv) every $T \in \binom{X}{t}$ containing at most one point from each group is contained in exactly one block.

The *type* of a GDD(t, k, v) $(X, \mathcal{G}, \mathcal{A})$ is the multiset $[|G| : G \in \mathcal{G}]$. We use the exponential notation to describe the type of a GDD: a GDD of type $g_1^{n_1} \cdots g_s^{n_s}$ is a GDD where there are exactly n_i groups of size g_i, $1 \le i \le s$.

We require the following result.

Theorem 2.3 (Hanani [4], Brouwer *et al.* [1], Mills [11], Ji [8])**.**

(i) There exists a GDD$(2, 3, gn)$ *of type* g^n *if and only if* $n \ge 3$*,* $(n-1)g \equiv 0 \bmod 2$*, and* $n(n-1)g^2 \equiv 0 \bmod 6$*.*
(ii) There exists a GDD$(2, 4, gn)$ *of type* g^n *if and only if* $n \ge 4$*,* $(n-1)g \equiv 0 \bmod 3$*, and* $n(n-1)g^2 \equiv 0 \bmod 12$*, with the exception of* $(g, n) \in \{(2, 4), (6, 4)\}$*.*
(iii) For $n > 3$*,* $n \ne 5$*, a* GDD$(3, 4, gn)$ *of type* g^n *exists if and only if* $gn \equiv 0 \bmod 2$ *and* $(n-1)(n-2)g \equiv 0 \bmod 3$*. A* GDD$(3, 4, 5g)$ *of type* g^5 *exists when* $g \equiv 0 \bmod 2$*,* $g \ne 2$*, and* $g \not\equiv 10, 26 \bmod 48$*.*

Analogous to splitting t-designs, a “splitting” version of a GDD can be defined. This has been done by Wang [19] for $t = 2$. Here, we extend it to general t. A *splitting group divisible t-design*, denoted splitting GDD$(t, k \times c, v)$, is a triple $(X, \mathcal{G}, \mathcal{A})$ satisfying the following properties:

(i) X is a set of v elements, called *points*;
(ii) $G = \{G_1, \dots, G_s\}$ is a partition of X into subsets, called *groups*;
(iii) $\mathcal{A}$ is a set of $k \times c$ arrays, called *blocks*, with entries from X, such that each point of X occurs at most once in each block;
(iv) for every $\{x_i : 1 \le i \le t\} \in \binom{X}{t}$ containing at most one point from each group, there is exactly one block in which x_i, $1 \le i \le t$, occur in t different rows.

The type of a splitting GDD is defined in a fashion similar to that for a GDD.

Splitting GDDs play an important role in the recursive constructions of splitting designs. The following is a straightforward extension of Wilson’s Fundamental Construction for GDDs [21, 22] to splitting GDDs.

Theorem 2.4 (Fundamental Construction)**.** *Let $(X,\mathcal{G},\mathcal{A})$ be a* GDD(t,k,v)*. Suppose that for each block $A\in\mathcal{A}$, there exists a splitting* GDD$(t,k'\times c,kc)$ *of type c^k, $(X_A,\mathcal{G}_A,\mathcal{B}_A)$, where*

$$\begin{aligned}X_A &= A\times\{1,\ldots,c\},\\ \mathcal{G}_A &= \{\{x\}\times\{1,\ldots,c\} : x\in A\},\end{aligned}$$

then there exists a splitting GDD$(t,k'\times c,vc)$ *of type $[c|G| : G\in\mathcal{G}]$ $(X',\mathcal{G}',\mathcal{A}')$, where*

$$\begin{aligned}X' &= X\times\{1,\ldots,c\},\\ \mathcal{G}' &= \{G\times\{1,\ldots,c\} : G\in\mathcal{G}\},\\ \mathcal{A}' &= \cup_{A\in\mathcal{A}}\mathcal{B}_A.\end{aligned}$$

Since the trivial splitting GDD$(t,k\times c,kc)$ of type c^k (containing only one block) always exists for any t, k, and c, we have the following.

Corollary 2.1. *If there exists a* GDD(t,k,v) *of type $g_1^{n_1}\ldots g_s^{n_s}$, then there exists a splitting* GDD$(t,k\times c,vc)$ *of type $(cg_1)^{n_1}\ldots(cg_s)^{n_s}$.*

As shown by Ge *et al.* [3], we can also fill in the groups of a splitting GDD with a splitting 2-design to obtain new splitting 2-designs.

Proposition 2.2 (Filling-In Groups)**.** *Let $(X,\mathcal{G},\mathcal{A})$ be a splitting* GDD$(2,k\times c,v)$*. If for each $G\in\mathcal{G}$, there exists a splitting* 2-$(|G|+1,k\times c,1)$ *design, then there exists a splitting* 2-$(v+1,k\times c,1)$ *design.*

2.2. State of affairs. The following theorem summarizes the state of knowledge on the existence of splitting t-designs with $\lambda=1$.

Theorem 2.5 (Du [2], Ge *et al.* [3], Wang [19], Wang and Su [20])**.** *The necessary divisibility conditions (of Proposition 2.1) are also sufficient for the existence of a splitting* 2-$(v,k\times c,1)$ *design when*

(i) $(k,c)=(2,2n)$*, for any positive integer n;*
(ii) $(k,c)=(2,3)$*, except for $v=10$;*
(iii) $(k,c)=(3,2)$*, except for $v=9$;*
(iv) $(k,c)=(3,3)$*, with the possible exception of $v=55$;*
(v) $(k,c)=(4,2)$*, with the possible exception of $v\in\{49,385\}$.*

In addition, there exists a 2-$(v,3\times 4,1)$ *design for all* $v\equiv 1 \bmod 96$.

3. Nonexistence and asymptotic existence

Let λ be a positive integer. The complete (loopless) multigraph on v vertices, denoted λK_v, is the graph where every pair of distinct vertices is connected by λ edges. Let G be a simple graph without isolated vertices. A *G-design of order v and index λ* is a partition of edge set of λK_v into subgraphs, each of which is isomorphic to G. If $e(G)$ denotes the number of edges in G, and $d(G)$ denotes the greatest common divisor of the degrees of vertices in G, then simple counting shows that the conditions

(i) $\lambda v(v-1)\equiv 0 \bmod 2e(G)$, and
(ii) $\lambda(v-1)\equiv 0 \bmod d(G)$

are necessary for the existence of a G-design of order v and index λ. A celebrated result of Wilson [23] states that these necessary conditions are also asymptotically sufficient.

Theorem 3.1 (Wilson [23]). *Let G be a simple graph without isolated vertices. Then there exists a constant v_0 depending only on G and λ such that a G-design of order v and index λ exist for all $v \geq v_0$ satisfying $\lambda v(v-1) \equiv 0 \bmod 2e(G)$ and $\lambda(v-1) \equiv 0 \bmod d(G)$.*

Let $K_{k\times c}$ denote the complete k-partite graph, with each part having c vertices. A splitting 2-$(v, k \times c, \lambda)$ design $(X, \mathcal{A})$ is equivalent to a $K_{k\times c}$-design of order v and index λ through the following correspondence:

(i) a point in X corresponds to a vertex in λK_v,

(ii) a block $A \in \mathcal{A}$ corresponds to the complete k-partite graph, where the i-th part contains c vertices corresponding to the c entries in row i of A, $1 \leq i \leq k$.

Applying Theorem 3.1 with $G = K_{k\times c}$ then gives the following result on the asymptotic existence of splitting 2-designs.

Corollary 3.1. *There exists a constant v_0 depending only on k, c, and λ, such that a splitting 2-$(v, k \times c, \lambda)$ design exists for all $v \geq v_0$ satisfying $\lambda v(v-1) \equiv 0 \bmod c^2k(k-1)$ and $\lambda(v-1) \equiv 0 \bmod c(k-1)$.*

We end this section with a nonexistence result. Huang [6] has shown that the number of complete k-partite graphs required to partition the edge set of K_v is at least $\lceil (v-1)/(k-1) \rceil$. This has the following consequence.

Proposition 3.1. *There does not exist a splitting 2-$((k-1)c^2+1, k \times c, 1)$ design, for all $k, c \geq 2$.*

Proof. Suppose a splitting 2-$((k-1)c^2+1, k\times c, 1)$ design exists. The number of blocks in this splitting 2-design is $((k-1)c^2+1)/k$. This would mean that we can partition the edge set of $K_{(k-1)c^2+1}$ into $((k-1)c^2+1)/k$ complete k-partite subgraphs. This is impossible by Huang's result, since $\lceil (k-1)c^2/(k-1) \rceil = c^2 > ((k-1)c^2+1)/k$. □

The definite exceptions in Theorem 2.5 are special cases of Proposition 3.1.

4. Splitting 2-designs

In this section, we establish the existence of an infinite family of splitting 2-$(v, 3 \times 5, 1)$ designs, and remove $v = 385$ as a possible exception from Theorem 2.5(v).

Proposition 4.1. *There exists a splitting 2-$(v, 3 \times 5, 1)$ design for all $v \equiv 1 \bmod 150$, except possibly when $v = 301$.*

Proof. A splitting 2-$(151, 3\times 5, 1)$ design is exhibited in Example 2.1, so let $v \geq 451$. Write $v = 150m+1$, for some integer $m \geq 3$. A GDD$(2, \{3\}, 30m)$ of type 30^m exists by Theorem 2.3(i). Apply Corollary 2.1 to obtain a splitting GDD$(2, 3\times 5, 150m)$ of type 150^m. Now fill in the groups of this splitting GDD with a splitting 2-$(151, 3 \times 5, 1)$ design (which has been constructed in Example 2.1) to obtain a splitting 2-$(150k+1, 3\times 5, 1)$ design. □

Proposition 4.2. *There exists a splitting 2-$(385, 4 \times 2, 1)$ design.*

Proof. A GDD$(2, \{4\}, 192)$ of type 48^4 exists by Theorem 2.3(ii). Apply Corollary 2.1 to obtain a splitting GDD$(2, 4\times 2, 384)$ of type 96^4. Now fill in the groups of this splitting GDD with a splitting 2-$(97, 4\times 2, 1)$ design (which exists by Theorem 2.5) to obtain a splitting 2-$(385, 4 \times 2, 1)$ design. □

5. Splitting 3-designs

In this section, we establish the existence of the first known infinite family of splitting 3-designs with $c > 1$.

Let t, k, and v be nonnegative integers. A (t, k) *candelabra system* of order v is a quadruple $(X, S, \mathcal{G}, \mathcal{A})$ that satisfies the following properties:

(i) X is a set of v elements, called *points*;
(ii) $S \subseteq X$, called the *stem*;
(iii) $\mathcal{G} = \{G_1, \ldots, G_m\}$ is a partition of $X \setminus S$ (elements of $\mathcal{G}$ are called *groups*);
(iv) $\mathcal{A} \subseteq \binom{X}{k}$, whose elements are called *blocks*;
(v) every $T \in \binom{X}{t}$ with $|T \cap (S \cup G_i)| < t$ for all i, is contained in a block in $\mathcal{A}$.

The *type* of a (t, k) candelabra system $(X, S, \mathcal{G}, \mathcal{A})$ is the multiset $[|G| : G \in \mathcal{G}]$. A (t, k) candelabra system of type $g_1^{n_1} \cdots g_r^{n_r}$ with a stem of size s is denoted (t, k)-CS$(g_1^{n_1} \cdots g_r^{n_r} : s)$.

Here, we introduce the notion of splitting candelabra systems.

A *splitting* $(t, k \times c)$ *candelabra system* of order v is a quadruple $(X, S, \mathcal{G}, \mathcal{A})$ that satisfies the following properties:

(i) X is a set of v elements, called *points*;
(ii) $S \subseteq X$, called the *stem*;
(iii) $\mathcal{G} = \{G_1, \ldots, G_m\}$ is a partition of $X \setminus S$ (elements of $\mathcal{G}$ are called *groups*);
(iv) $\mathcal{A}$ is a set of $k \times c$ arrays, called *blocks*, with entries from X, such that each point of X occurs at most once in each block;
(v) for every $\{x_i : 1 \leq i \leq t\} \in \binom{X}{t}$ with $|T \cap (S \cup G_i)| < t$ for all i, there is exactly one block in which x_i, $1 \leq i \leq t$, occur in t different rows.

We use the same notation for splitting (t, k) candelabra systems as those for (t, k) candelabra systems.

The following theorem is an extension of Hartman's Fundamental Construction [5] from $(3, k)$ candelabra systems to splitting $(3, k \times c)$ candelabra systems.

Theorem 5.1. *If there exist a* $(3, k)$-CS$(g_1^{n_1} \cdots g_r^{n_r} : s)$*, a splitting* $(3, k' \times c)$-CS$(m^{k-1} : a)$*, and a splitting* GDD$(3, k' \times c, mk)$ *of type* m^k*, then there exists a splitting* $(3, k' \times c)$-CS$((g_1 m)^{n_1} \cdots (g_r m)^{n_r} : m(s-1) + a)$.

Proof. Let $(X, S, \mathcal{G}, \mathcal{A})$ be a $(3, k)$-CS$(g_1^{n_1} \cdots g_r^{n_r} : s)$, and let ∞ be a distinguished point in S. For $Y \subseteq X$, define the set of points

$$P(Y) = ((Y \setminus \{\infty\}) \times \mathbb{Z}_m) \cup (\{\infty\} \times \mathbb{Z}_a).$$

Further define

$$S' = ((S \setminus \{\infty\}) \times \mathbb{Z}_m) \cup (\{\infty\} \times \mathbb{Z}_a),$$
$$\mathcal{G}' = \{G \times \mathbb{Z}_m : G \in \mathcal{G}\}.$$

For each $A \in \mathcal{A}$ containing the point ∞, let

$$(P(A), \{\infty\} \times \mathbb{Z}_a, \{\{x\} \times \mathbb{Z}_m : x \in A \setminus \{\infty\}\}, \mathcal{B}_A)$$

be a splitting $(3, k' \times c)$-CS$(m^{k-1} : a)$, and for each $A \in \mathcal{A}$ not containing the point ∞, let

$$(A \times \mathbb{Z}_m, \{\{x\} \times \mathbb{Z}_m : x \in A\}, \mathcal{C}_A)$$

be a splitting GDD$(3, k' \times c, mk)$ of type m^k.

It is easy to check that $(P(X), S', \mathcal{G}', \mathcal{A}')$, where

$$\mathcal{A}' = \left(\bigcup_{A \in \mathcal{A} : \infty \in A} \mathcal{B}_A \right) \cup \left(\bigcup_{A \in \mathcal{A} : \infty \notin A} \mathcal{C}_A \right),$$

is the required splitting $(3, k' \times c)$-CS$((g_1 m)^{n_1} \cdots (g_r m)^{n_r} : m(s-1)+a)$. □

We can also fill in the groups of a splitting candelabra system by splitting 3-designs to obtain larger splitting 3-designs.

Proposition 5.1. *If there exists a splitting* $(3, k \times c)$-CS$(g_1^{n_1} \cdots g_r^{n_r} : s)$, *where* $s \leq 2$, *and there exists a splitting* 3-$(g_i + s, k \times c, 1)$ *design for each* i, $1 \leq i \leq r$, *then there exists a splitting* 3-$(s + \sum_{i=1}^{r} g_i n_i, k \times c, 1)$ *design.*

Proof. Let $(X, S, \mathcal{G}, \mathcal{A})$ be a splitting $(3, k \times c)$-CS$(g_1^{n_1} \cdots g_r^{n_r} : s)$, where $s \leq 2$. For each $G \in \mathcal{G}$, let $(G \cup S, \mathcal{B}_G)$ be a splitting 3-$(|G| + s, k \times c, 1)$ design. Then $(X, \mathcal{A} \cup (\cup_{G \in \mathcal{G}} \mathcal{B}_G))$ is the required splitting 3-$(s + \sum_{i=1}^{r} g_i n_i, k \times c, 1)$ design. □

To apply Theorem 5.1 and Proposition 5.1, we require some splitting candelabra systems to start with.

Lemma 5.2. *There exist a splitting* $(3, 3 \times 2)$-CS$(8^2 : 0)$ *and a splitting* $(3, 3 \times 2)$-CS$(8^2 : 2)$.

Proof. Let $X = \mathbb{Z}_{16}$ and $\mathcal{G} = \{\{2i + j : 0 \leq i \leq 7\} : j \in \{0, 1\}\}$. Let

$$\mathcal{B} = \left\{ \begin{pmatrix} 0 & 4 \\ 6 & 9 \\ 7 & 11 \end{pmatrix}, \begin{pmatrix} 0 & 14 \\ 1 & 4 \\ 11 & 13 \end{pmatrix}, \begin{pmatrix} 0 & 5 \\ 8 & 10 \\ 13 & 15 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 4 & 1 \\ 7 & 15 \end{pmatrix}, \begin{pmatrix} 0 & 13 \\ 1 & 15 \\ 2 & 12 \end{pmatrix}, \begin{pmatrix} 0 & 13 \\ 1 & 9 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 0 & 6 \\ 9 & 7 \\ 14 & 15 \end{pmatrix} \right\}.$$

Then $(X, \mathcal{G}, \varnothing, \mathcal{A})$, where $\mathcal{A} = \cup_{B \in \mathcal{B}} \{B + 2i \bmod 16 : 0 \leq i < 8\}$, is a splitting $(3, 3 \times 2)$-CS$(8^2 : 0)$.

Now let $S = \{x, y\}$ be such that $S \cap X = \varnothing$, and let

$$\mathcal{C} = \left\{ \begin{pmatrix} x & y \\ 2i & 2i + 2 \\ 2j + 1 & 2j + 3 \end{pmatrix} : i, j \in \{0, 2, 4, 6\} \right\}.$$

Then $(X \cup \{x, y\}, S, \mathcal{G}, \mathcal{A} \cup \mathcal{C})$ is a splitting $(3, 3 \times 2)$-CS$(8^2 : 2)$. □

We now establish an infinite family of splitting 3-designs.

Theorem 5.3. *A splitting* 3-$(v, 3 \times 2, 1)$ *design exists if and only if* $v \equiv 2 \bmod 8$.

Proof. Necessity of the condition $v \equiv 2 \bmod 8$ follows from Proposition 2.1.

Huber [7] has shown the existence of a splitting 3-$(10, 3 \times 2, 1)$ design, so we consider $v > 10$. Write $v = 8m + 2$, for some $m \geq 2$. Let X be a set of $m + 1$ points, containing ∞ as a distinguished point. It is easy to verify that $(X, \{\infty\}, \{\{x\} : x \in X \setminus \{\infty\}\}, \binom{X}{3})$ is a $(3, 3)$-CS$(1^m : 1)$. Apply Theorem 5.1 with a splitting $(3, 3 \times 2)$-CS$(8^2 : 2)$ (which exists by Lemma 5.2) and a splitting GDD$(3, 3 \times 2, 24)$ of type 8^3 (whose existence is implied by the trivial GDD$(3, 3, 12)$ of type 4^3 and Corollary 2.1) to obtain a splitting $(3, 3 \times 2)$-CS$(8^m : 2)$. Now apply Proposition 5.1 to this splitting $(3, 3 \times 2)$-CS$(8^m : 2)$ with a splitting 3-$(10, 3 \times 2, 1)$ design to obtain a splitting 3-$(8m + 2, 3 \times 2, 1)$ design. □

6. Conclusion

Determining the existence of optimal c-splitting authentication codes with k source states that are $(t-1)$-fold secure against spoofing is a difficult problem, when k, c and t are large. New constructions, both direct and recursive, need to be developed in order to make further progress on the problem.

Acknowledgment

The authors would like to thank Gennian Ge and Alan Ling for helpful discussions.

References

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

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

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

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

[5] A. Hartman, *The fundamental construction for 3-designs*, Discrete Math., **124** (1994), 107–132.

[6] Q. X. Huang, *On the decomposition of* K_n *into complete* m*-partite graphs*, J. Graph Theory, **15** (1991), 1–6.

[7] M. Huber, *Combinatorial bounds and characterizations of splitting authentication codes*, Crypt. Commun., **2** (2010), 173–185.

[8] L. Ji, *An improvement on* H *design*, J. Combin. Des., **17** (2009), 25–35.

[9] K. Kurosawa and S. Obana, *Combinatorial bounds on authentication codes with arbitration*, Des. Codes Crypt., **22** (2001), 265–281.

[10] J. L. Massey, *Cryptography, a selective survey*, in "Digital Communications '85: Proceedings of the Second Tirrenia International Workshop on Digital Communications" (eds. E. Biglieri and G. Prati), Elsevier, (1986), 3–25.

[11] W. H. Mills, *On the existence of* H *designs*, in "Proceedings of the Twenty-first Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1990)," **79** (1990), 129–141.

[12] 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.

[13] G. J. Simmons, *A game theory model of digital message authentication*, Congr. Numer., **34** (1982), 413–424.

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

[15] G. J. Simmons, *Authentication theory/coding theory*, in "Advances in Cryptology – CRYPTO '84" (eds. G.R. Blakely and D. Chaum), Springer-Verlag, (1985), 411–432.

[16] G. J. Simmons, *Message authentication with arbitration of transmitter/receiver disputes*, in "Advances in Cryptology – EUROCRYPT '87," Springer-Verlag, (1987), 151–165.

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

[18] G. J. Simmons, *A survey of information authentication*, in "Contemporary Cryptology — The Science of Information Integrity "(ed. G.J. Simmons), IEEE Press, (1992), 379–419.

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

[20] 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.

[21] R. M. Wilson, *An existence theory for pairwise balanced designs. I. Composition theorems and morphisms*, J. Combin. Theory Ser. A, **13** (1972), 220–245.

[22] R. M. Wilson, *An existence theory for pairwise balanced designs. II. The structure of PBD-closed sets and the existence conjectures*, J. Combin. Theory Ser. A, **13** (1972), 246–273.

[23] R. M. Wilson, *Decompositions of complete graphs into subgraphs isomorphic to a given graph*, in "Proceedings of the Fifth British Combinatorial Conference (Univ. Aberdeen, Aberdeen, 1975)," Winnipeg, Man., (1976), 647–659.

Received May 2010; revised November 2010.

E-mail address: ymchee@ntu.edu.sg
E-mail address: xiandezhang@ntu.edu.sg
E-mail address: z_h1984@126.com