

On the equivalence of authentication codes and robust $(2, 2)$ -threshold schemes*

Maura B. Paterson¹ and Douglas R. Stinson^{†2}

¹Department of Economics, Mathematics and Statistics, Birkbeck, University of London, Malet Street, London WC1E 7HX, UK

²David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

October 12, 2019

Abstract

In this paper, we show a “direct” equivalence between certain authentication codes and robust secret sharing schemes. It was previously known that authentication codes and robust secret sharing schemes are closely related to similar types of designs, but direct equivalences had not been considered in the literature. Our new equivalences motivate the consideration of a certain “key-substitution attack.” We study this attack and analyze it in the setting of “dual authentication codes.” We also show how this viewpoint provides a nice way to prove properties and generalizations of some known constructions.

1 Introduction

We begin by giving some relevant definitions for authentication codes and threshold schemes. We should emphasize that we are only considering unconditionally secure cryptographic protocols in this paper.

1.1 Authentication Codes

We follow Simmons’ model for authentication [12]. A key K determines an *encoding rule* e_K , which is a possibly randomized mapping $e_K : \mathcal{S} \rightarrow \mathcal{M}$. Elements in \mathcal{S} are called *sources* and elements of \mathcal{M} are *messages*. In general, we

*This research was supported by a “Research in Pairs” grant from the London Mathematical Society.

[†]D.R. Stinson’s research is supported by NSERC discovery grant RGPIN-03882.

view $e_K(s)$ as a set of messages in the case that encoding is randomized (this is often called *authentication with splitting*). The key K is chosen from a *keyspace* \mathcal{K} . The key and the source can be treated as independent random variables. If $|e_K(s)| = c$ for all $s \in \mathcal{S}$ and all $K \in \mathcal{K}$, the code is called a *c-splitting* authentication code.

Given a key K and a message m , at most one source should be “possible.” That is, for every key K , we require that $e_K(s) \cap e_K(s') = \emptyset$ if $s \neq s'$. This ensures that the receiver, who has the key K and a message $m \in e_K(s)$, can uniquely determine the source s .

For any key K , denote

$$\mu(K) = \bigcup_s e_K(s).$$

The set $\mu(K)$ consists of all the messages that are valid encodings of a source under key K .

Also, for any message m , denote

$$\kappa(m) = \{K : m \in \mu(K)\}.$$

The set $\kappa(m)$ consists of all the keys for which m is a valid encoding of some source.

The *encoding matrix* of an authentication code is a matrix E in which the rows are indexed by the keys in \mathcal{K} and the columns are indexed by the sources in \mathcal{S} . The entry $E(k, s)$ is simply the set (of messages) $e_K(s)$. The entries $E(k, s)$ in the encoding matrix are singletons if and only if the code has no splitting, i.e., $c = 1$.

We are primarily interested in authentication codes having *perfect secrecy*, i.e., codes having the property that a message reveals no information about the source to an adversary who does not know the key. We also often want authentication codes that are secure against both message-substitution and key-substitution attacks. These attacks are defined as follows.

In a *message-substitution attack* (also called a *substitution attack*), the adversary sees a message m and replaces it with a message $m' \neq m$. The adversary wins if $m' \in e_K(s')$ and $m \in e_K(s)$, where K is the (unknown) secret key and $s' \neq s$. This is often just called a *substitution attack*; these types of attacks have been considered for many years.

In a *key-substitution attack*, the adversary sees a key K and replaces it with a key $K' \neq K$. The adversary wins if $m \in e_K(s)$ and $m \in e_{K'}(s')$, where m is the (unknown) message and $s' \neq s$. This is perhaps a less natural type of attack to consider than a message-substitution attack. In fact, we are not aware of any previous study of unconditionally secure authentication codes that considers key-substitution attacks. However, we should note that a similar attack has been studied in the setting of systematic algebraic manipulation detection (AMD) codes; see [3].

There is another attack that is often studied for authentication codes, namely, an *impersonation attack*. In this attack, the adversary chooses a message, without seeing a “previous” message, hoping that it is an encoding of some source under the (unknown) key K .

The *success probability* of an attack (impersonation, message-substitution or key-substitution) is the probability that the adversary wins the corresponding “game.” This probability is computed over a random choice of key, source, and message encoding (if encoding of messages is randomized, i.e., in the case of a code with splitting) according to the probability distributions specified on them. Throughout this paper, we assume that the probability distributions defined on the keys and message encodings are uniform. That is, $\text{Prob}[K] = 1/b$ for all keys $K \in \mathcal{K}$, and in a c -splitting code, for a given key $K \in \mathcal{K}$ and source $s \in \mathcal{S}$, we have $\text{Prob}[m] = 1/c$ for all $m \in e_K(s)$.

Source probability distributions are often (but not always) assumed to be uniform. Also, in all of the attacks we study, we assume that a key is used to encode only one message.

The adversary’s optimal success probability for an impersonation attack is often denoted by P_{d_0} and their optimal success probability for a message-substitution attack is denoted by P_{d_1} . For c -splitting authentication codes, the following bounds are known.

Theorem 1.1. [12, 4, 1] *Suppose a c -splitting authentication code for k sources has v messages. Then $P_{d_0} \geq ck/v$ and $P_{d_1} \geq c(k-1)/(v-1)$.*

For a code without splitting (i.e., $c = 1$), the bounds obtained from Theorem 1.1 are $P_{d_0} \geq k/v$ and $P_{d_1} \geq (k-1)/(v-1)$. This bound on P_{d_1} was first proved by Massey [7].

The following two results will be used several times later in the paper. They do not assume equiprobable sources.

Lemma 1.2. *Suppose a c -splitting authentication code for k sources has v messages, b equiprobable keys and equiprobable message encoding. Then $P_{d_0} = ck/v$ if and only if $|\kappa(m)| = bck/v$ for all messages m .*

Proof. Let K be the key that was chosen by the sender/receiver. The message m chosen by the attacker will be accepted as valid if and only if $K \in \kappa(m)$. Since there are b possible keys, the choice of m will be a successful impersonation with probability $|\kappa(m)|/b$.

Define

$$A = \{(K, m) : K \in \kappa(m)\}.$$

Clearly

$$|A| = \sum_{m \in \mathcal{M}} |\kappa(m)|.$$

However, we also have

$$|A| = \sum_{K \in \mathcal{K}} |\mu(K)| = bck.$$

Therefore,

$$\max\{|\kappa(m)| : m \in \mathcal{M}\} \geq \frac{bck}{v},$$

and equality occurs if and only if $|\kappa(m)| = bck/v$ for all messages m .

The adversary's optimal attack is to choose m so that $|\kappa(m)|$ is maximized. Hence, the maximum success probability of an impersonation attack is at least ck/v , and equality occurs if and only if $|\kappa(m)| = bck/v$ for all messages m . \square

Theorem 1.3. *Suppose a c -splitting authentication code for k sources has v messages, b equiprobable keys and equiprobable message encoding. Consider the following three conditions:*

1. $P_{d_0} = ck/v$;
2. the code achieves perfect secrecy;
3. within each column of the encoding matrix, every message occurs the same number of times.

Then the code satisfies conditions 1. and 2. if and only if it satisfies condition 3.

Proof. For any $s \in \mathcal{S}$ and $m \in \mathcal{M}$, define

$$\kappa(m, s) = \{K : m \in e_K(s)\}.$$

Thus $\kappa(m, s)$ contains the keys for which m is a valid encoding of s . We observe that

$$\text{Prob}[m | s] = \frac{|\{K : m \in e_K(s)\}|}{b} = \frac{|\kappa(m, s)|}{b}. \quad (1)$$

Suppose the code satisfies 2. Perfect secrecy is achieved if and only if

$$\text{Prob}[s | m] = \text{Prob}[s]$$

for all $s \in \mathcal{S}$ and all $m \in \mathcal{M}$. By Bayes' Theorem, this is equivalent to proving

$$\text{Prob}[m | s] = \text{Prob}[m] \quad (2)$$

for all $s \in \mathcal{S}$ and all $m \in \mathcal{M}$.

For a given message m , equations (1) and (2) imply that $|\kappa(m, s_1)| = |\kappa(m, s_2)|$ for all sources s_1, s_2 .

It is clear that

$$\kappa(m) = \bigcup_{s \in \mathcal{S}} \kappa(m, s),$$

where the sets $\kappa(m, s)$ ($s \in \mathcal{S}$) are disjoint. Therefore

$$|\kappa(m)| = \sum_{s \in \mathcal{S}} |\kappa(m, s)| = k \times |\kappa(m, s)| \quad (3)$$

for any fixed source $s \in \mathcal{S}$.

Now, assume additionally that the code satisfies condition 1. From Lemma 1.2, we have $|\kappa(m)| = bck/v$. Hence, it follows that

$$|\kappa(m, s)| = \frac{bc}{v} \quad (4)$$

for every $m \in \mathcal{M}$, $s \in \mathcal{S}$. Therefore, condition 3. holds.

Conversely, suppose condition 3. holds. Let $s \in \mathcal{S}$. Then $|\kappa(m_1, s)| = |\kappa(m_2, s)|$ for all $m_1, m_2 \in \mathcal{M}$. We have

$$\sum_{m \in \mathcal{M}} |\kappa(m, s)| = bc,$$

since there are b rows in the encoding matrix and each cell contains c messages. Therefore, equation (4) holds for all $s \in \mathcal{S}$ and all $m \in \mathcal{M}$. Hence, from (1),

$$\text{Prob}[m | s] = \frac{bc}{b} = \frac{c}{v}$$

for all $s \in \mathcal{S}$ and all $m \in \mathcal{M}$. Then

$$\begin{aligned} \text{Prob}[m] &= \sum_{s \in \mathcal{S}} (\text{Prob}[m | s] \times \text{Prob}[s]) \\ &= \sum_{s \in \mathcal{S}} \left(\frac{c}{v} \times \text{Prob}[s] \right) \\ &= \frac{c}{v}, \end{aligned}$$

so $\text{Prob}[m | s] = \text{Prob}[m]$ for all $s \in \mathcal{S}$ and $m \in \mathcal{M}$. Therefore, equation (2) holds and we have perfect secrecy.

To see that $P_{d_0} = ck/v$, we use equation (3), which is satisfied because we have perfect secrecy. Since (4) holds, we have

$$|\kappa(m)| = k \times \frac{bc}{v} = \frac{bck}{v}$$

for all $m \in \mathcal{M}$. Then $P_{d_0} = ck/v$ from Lemma 1.2. \square

1.2 Threshold Schemes

A $(2, 2)$ -threshold scheme enables a *secret* s to be “split” into two *shares* v_1 and v_2 in such a way that

1. v_1 and v_2 uniquely determine s via a *reconstruction function*. We express this as $\text{Reconstruct}(v_1, v_2) = s$.
2. No individual share yields any information about the secret. That is,

$$\text{Prob}[s | v_1] = \text{Prob}[s | v_2] = \text{Prob}[s].$$

More generally, a (k, n) -threshold scheme enables a secret s to be split into n shares in such a way that any k shares permit the secret to be reconstructed, but no set of $k - 1$ or fewer shares yield any information about the secret.

In a *robust* $(2, 2)$ -threshold scheme, we consider the scenario where one player may modify their share, hoping that Reconstruct will then yield an incorrect

secret. So we consider a setting where `Reconstruct` either returns a secret or \perp , where the latter indicates that no secret can be reconstructed from the two given shares. Suppose that the first player, P_1 , alters their share as $v_1 \rightarrow v'_1$ (P_1 does not have any information about the value of the other share, v_2). Suppose $\text{Reconstruct}(v_1, v_2) = s$. Then P_1 *wins* this deception game if

$$\text{Reconstruct}(v'_1, v_2) = s'$$

where $s' \neq s$. P_1 *loses* the game if

$$\text{Reconstruct}(v'_1, v_2) = s \quad \text{or} \quad \text{Reconstruct}(v'_1, v_2) = \perp .$$

Similarly, if P_2 alters their share as $v_2 \rightarrow v'_2$, then they win the deception game if $\text{Reconstruct}(v_1, v'_2) = s'$ where $s' \neq s$.

A *robust* $(2, 2)$ -threshold scheme is ϵ -*secure* if no strategy by P_1 or P_2 will allow them to win the deception game with probability exceeding ϵ .

1.3 Background and Our Contributions

There has been previous work, for example in [9, 8], discussing constructions for “optimal” authentication codes and robust (threshold) secret sharing schemes using combinatorial structures such as BIBDs, difference sets, external BIBDs (EBIBDs), external difference families (EDFs) and splitting BIBDs. In the context of authentication codes, “optimal” means that the deception probabilities are as small as possible and the number of encoding rules (or keys) is also as small as possible. For a robust threshold scheme, “optimal” means that the deception probabilities meet a specified bound that is expressed in terms of the number of possible shares and the number of possible secrets. Additionally, [9, 8] proved some partial converses showing that optimal authentication codes and robust secret sharing schemes imply the existence of some of the above-mentioned combinatorial structures. Without going into details, the following are the main results along this line:

- In [9] it is shown that a robust threshold scheme can be constructed from an EDF with $\lambda = 1$. (This construction incorporates a Shamir threshold scheme as an ingredient.) Conversely, certain robust threshold schemes give rise to certain EBIBDs.
- In [8] it is shown that a robust threshold scheme can be constructed from a difference set. (This construction also incorporates a Shamir threshold scheme as an ingredient.) Conversely, certain robust threshold schemes give rise to certain SBIBDs.
- In [9], a construction is given for splitting authentication codes from EDFs with $\lambda = 1$. This paper also constructs certain authentication codes from splitting BIBDs with $\lambda = 1$, as well as proving a converse result.

The above results suggest that there are connections between authentication codes and robust secret sharing schemes, as they are closely related to similar (and sometimes identical) types of designs. For example, the combinatorial designs generated by EDFs (which include difference sets as a special case) can be used to construct both robust threshold schemes and authentication codes.

In this paper, we show a “direct” equivalence between certain authentication codes and robust secret sharing schemes. We also study a key-substitution attack for authentication codes and interpret it in light of what we term “dual authentication codes.”

Robust (k, n) -threshold schemes were introduced by Tompa and Woll [14]. They have been constructed in the past by a two-step process: First, the secret is “encoded” using a suitable combinatorial structure such as a difference set [8], EDF [9] or AMD code [3]. Second, the encoded secret is shared using a traditional Shamir threshold scheme. However, if we consider a $(2, 2)$ -threshold scheme, then the second step is not required and consequently we can show a direct equivalence between authentication codes and $(2, 2)$ -threshold schemes.

The rest of this paper is organized as follows. In Section 2, we prove our main equivalence result. Constructions for authentication codes that satisfy the necessary hypotheses are studied in Section 3. The notion of “dual authentication codes” is introduced and explored in Section 4. Finally, some closing remarks are given in Section 5.

2 Equivalences

In the next subsections, we show the equivalence of certain authentication codes and robust $(2, 2)$ -threshold schemes.

2.1 Threshold Scheme to Authentication Code

Given an ϵ -secure robust $(2, 2)$ -threshold scheme, we construct an authentication code. This is somewhat similar to the the construction used by Kurosawa, Obana and Ogata in [6, Theorem 15].

For any ordered pair of shares (v_1, v_2) such that $\text{Reconstruct}(v_1, v_2) = s$, define $v_2 \in e_{v_1}(s)$. First, we note that $e_{v_1}(s) \neq \emptyset$ for all v_1 and all s . This holds because the share v_1 does not provide any information about the secret. Hence, for all choices of v_1 and s , there must be at least one value v_2 such that $\text{Reconstruct}(v_1, v_2) = s$.

The probability distribution on the sources in the authentication code should be the same as the probability distribution on the shares of the threshold scheme. Also, note the following correspondences:

threshold scheme		authentication code
source s	\longleftrightarrow	secret s
share v_1	\longleftrightarrow	key K
share v_2	\longleftrightarrow	message m .

We show that the resulting authentication scheme satisfies various properties now.

Message-substitution attack. Suppose an adversary replaces $m \in e_K(s)$ with $m' \neq m$ in the authentication code. This corresponds to modifying share v_2 (the second share) from m to m' in the robust secret sharing scheme. Because the threshold scheme is robust, we know that

$$\text{Prob}[\text{Reconstruct}(K, m') = s' \neq s] \leq \epsilon.$$

In other words,

$$\text{Prob}[m' \in e_K(s') \text{ and } s' \neq s] \leq \epsilon.$$

Therefore, the probability of a successful message-substitution attack is at most ϵ .

Key-substitution attack. Suppose an adversary replaces K with $K' \neq K$ in the authentication code, where $m \in e_K(s)$. This corresponds to modifying share v_1 (the first share) from K to K' in the robust secret sharing scheme. Because the threshold scheme is robust, we know that

$$\text{Prob}[\text{Reconstruct}(K', m) = s' \neq s] \leq \epsilon.$$

In other words,

$$\text{Prob}[m \in e_{K'}(s') \text{ and } s' \neq s] \leq \epsilon.$$

Therefore, the probability of a successful key-substitution attack is at most ϵ .

Perfect Secrecy. The threshold scheme has the property that one share yields no information about the value of the secret. Therefore, in particular,

$$\text{Prob}[s \mid v_2] = \text{Prob}[s].$$

Suppose the share v_2 is fixed but we have no information about the share v_1 . Then we have no information about the secret s . In the corresponding authentication code, this means that the message $m = v_2$ provides no information about the source s when the key $K = v_1$ is not known, so we have perfect secrecy.

It is also possible to construct authentication codes with similar properties from any robust (k, n) -threshold scheme with $k \geq 2$. For example, see [8]. The idea is to fix shares for the first $k - 2$ players, say, by choosing some $(k - 2)$ -tuple of shares that occurs with probability greater than 0. Consider the subset of distribution rules such that the first $k - 2$ shares take on the specified values. Retain the shares for the next two players, but throw away the shares that would be given to the last $n - k$ players. This gives rise to a $(2, 2)$ -threshold scheme, which can then be used to construct an authentication code using the above-described technique.

2.2 Authentication Code to Threshold Scheme

The construction in the previous subsection can easily be reversed. Now we start with an authentication code having perfect secrecy and we assume that message-substitution and key-substitution attacks have success probability at most ϵ . We construct a $(2, 2)$ -threshold scheme as follows: shares for P_1 are keys in the authentication code, shares for P_2 are messages in the authentication code, and secrets are sources in the authentication code. Note that P_1 and P_2 have shares of the same size if and only if the number of keys is the same as the number of messages (in the authentication code).

For every $m \in e_K(s)$, construct a distribution rule $(K, m; s)$, i.e., $v_1 = K$, $v_2 = m$ and

$$\text{Reconstruct}(v_1, v_2) = \text{Reconstruct}(K, m) = s.$$

We need to show that the resulting set of distribution rules defines an ϵ -secure $(2, 2)$ -threshold scheme.

Secret reconstruction. Suppose that we have two distribution rules $(K, m; s)$ and $(K, m; s')$ with $s' \neq s$. Then $m \in e_K(s) \cap e_K(s')$ in the authentication code, which is not allowed. Thus, two shares determine at most one secret.

Information revealed by one share. We want to prove that

$$\text{Prob}[s \mid v_1] = \text{Prob}[s \mid v_2] = \text{Prob}[s].$$

If $v_1 = K$ is given, then this yields no information about s because K and s are independent in the authentication code. If $v_2 = m$ is given, then this yields no information about s because the authentication code has perfect secrecy.

Modifying v_1 . Suppose P_1 replaces their share $v_1 = K$ with $v'_1 = K' \neq K$. This corresponds to a key-substitution attack in the authentication code. We know that

$$\text{Prob}[m \in e_{K'}(s') \text{ and } s' \neq s] \leq \epsilon,$$

so

$$\text{Prob}[\text{Reconstruct}(K', m) = s' \neq s] \leq \epsilon.$$

Modifying v_2 . Suppose P_2 replaces their share $v_2 = m$ with $v'_2 = m' \neq m$. This corresponds to a message-substitution attack in the authentication code. We know that

$$\text{Prob}[m' \in e_K(s') \text{ and } s' \neq s] \leq \epsilon,$$

so

$$\text{Prob}[\text{Reconstruct}(K, m') = s' \neq s] \leq \epsilon.$$

2.3 Main Theorem

Summarizing the results in the two previous subsections, we have our main equivalence theorem. For simplicity, we assume equiprobable distributions of sources (in the authentication code) and secrets (in the threshold scheme).

Theorem 2.1. *There exists an authentication code with perfect secrecy for k uniformly distributed sources that is ϵ -secure against message-substitution and key-substitution attacks if and only if there exists an ϵ -secure $(2, 2)$ -threshold scheme for k uniformly distributed secrets.*

3 Combinatorial Constructions

In this section, we look at various constructions for authentication codes that are based on combinatorial designs, paying particular attention to the properties (namely, perfect secrecy and key-substitution attacks) that are relevant for the construction of robust $(2, 2)$ -threshold schemes using Theorem 2.1. Throughout this section, we assume standard design-theoretic definitions that can be found, for example, in [2].

3.1 Symmetric BIBDs

First, we give a simple construction using symmetric BIBDs (i.e., SBIBDs). This is a slight generalization of constructions given in [9, 8] since we do not require that the SBIBD is generated from a difference set.

Suppose that (X, \mathcal{B}) is a (v, k, λ) -SBIBD (so $\lambda(v-1) = k(k-1)$). Suppose that $X = \{x_i : 1 \leq i \leq v\}$ is the set of points in the design and $\mathcal{B} = \{B_j : 1 \leq j \leq v\}$ is the set of blocks in the design. We can order each block B_j to obtain a k -tuple $C_j = (c_{1,j}, \dots, c_{k,j})$ in such a way that the following property is satisfied:

$$|\{j : c_{\ell,j} = x_i\}| = 1$$

for every i , $1 \leq i \leq v$, and every ℓ , $1 \leq \ell \leq k$. That is, we can write out the ordered blocks C_j ($1 \leq j \leq v$) as the rows of a v by k array E in such a way that every point occurs once in each column of the array E . Such an array is known as a *Youden square*; see, for example, [2, §VI.65].

A Youden square can be constructed from any SBIBD by using systems of distinct representatives. However, in the case where the SBIBD is generated from a difference set in an abelian group G , the Youden square occurs automatically if we arbitrarily order the base block and then generate the rest of the (ordered) blocks by developing the base block through the group G .

Suppose we use E as an encoding matrix for an authentication code. Thus, a key corresponds to a block in the design, or equivalently a row in E . The k sources are the k columns in E and the messages are the v points in the design. We assume that the sources are equiprobable.

It is not difficult to verify that this authentication code is $(k-1)/(v-1)$ -secure against message-substitution and key-substitution attacks (see the proof of Theorem 3.3 for additional detail). It is also clear that this authentication code provides perfect secrecy; this follows immediately from Theorem 1.3 using the “Youden square” property of the authentication matrix. This construction is in fact a special case of [9, Theorem 5.5], extended to include the perfect

secrecy property by using an appropriate ordering of the blocks, as described above.

Starting with this authentication code, we obtain from Theorem 2.1 an ϵ -secure $(2, 2)$ -threshold scheme for k equiprobable secrets, where $\epsilon = (k-1)/(v-1)$. Summarizing, we have the following theorem.

Theorem 3.1. *If there exists a (v, k, λ) -SBIBD, then there exists*

1. *an authentication code with perfect secrecy for k equiprobable sources that is $(k-1)/(v-1)$ -secure against message-substitution and key-substitution attacks, and*
2. *a $(k-1)/(v-1)$ -secure $(2, 2)$ -threshold scheme for k equiprobable secrets, in which the share sets for both players have size v .*

Example 3.1. A $(7, 3, 1)$ -SBIBD is just a projective plane of order 2, often called the Fano plane. The seven blocks in the design can be obtained from the base block $\{0, 1, 3\}$ by developing it in the group \mathbb{Z}_7 . After ordering the blocks appropriately, we obtain the following Youden square.

s_1	s_2	s_3
0	1	3
1	2	4
2	3	5
3	4	6
4	5	0
5	6	1
6	0	2

This Youden square is the encoding matrix for an authentication code with perfect secrecy having $P_{d_0} = 3/7$ and $P_{d_1} = 2/6 = 1/3$. The success probability of any key-substitution attack is also $1/3$. For example, if K_1 is replaced by K_2 , then the attack succeeds if and only if $m = 1$. The probability that $m = 1$ (given that K_1 is the key) is $1/3$ because the sources are equiprobable.

The corresponding $(2, 2)$ -threshold scheme is $(1/3)$ -secure and has the following 21 distribution rules:

v_1	v_2	s
0	0	s_1
1	1	s_1
2	2	s_1
3	3	s_1
4	4	s_1
5	5	s_1
6	6	s_1

v_1	v_2	s
0	1	s_2
1	2	s_2
2	3	s_2
3	4	s_2
4	5	s_2
5	6	s_2
6	0	s_2

v_1	v_2	s
0	3	s_3
1	4	s_3
2	5	s_3
3	6	s_3
4	0	s_3
5	1	s_3
6	2	s_3

Any deception carried out by P_1 or P_2 succeeds with probability $1/3$. For example, suppose $v_1 \rightarrow v'_1 = v_1 + 1 \pmod{7}$. This deception will succeed if and

only if $s = s_2$. In this case, $v_2 = v_1 + 1 \pmod{7}$ and then $\text{Reconstruct}(v'_1, v_2) = s_1$. The success probability of this deception is $\text{Prob}[s = s_2] = 1/3$ because the sources are equiprobable.

We should note that the authentication codes and robust threshold schemes obtained from Theorem 3.1 are optimal in various senses. In the case of the authentication code, the impersonation and message-substitution attacks have success probability that is as small as possible, according to Massey's bounds [7]. Also, the number of encoding rules (or keys) is as small as possible, from [11, Theorem 2.1].

For the threshold schemes, we have v possible shares, k possible secrets, and the scheme is ϵ -secure where $\epsilon = (k-1)/(v-1)$. This meets the bound proven in [8, Corollary 3.3]. In fact, as a result of our discussion above, we have shown the following strong characterization of these "optimal" $(2, 2)$ -threshold schemes.

Theorem 3.2. *There exists a (v, k, λ) -SBIBD if and only if there exists a $(k-1)/(v-1)$ -secure $(2, 2)$ -threshold scheme for k equiprobable secrets.*

3.2 BIBDs

More generally, we can use any BIBD (i.e, not necessarily a symmetric BIBD) to construct an authentication code. It has also been shown that the resulting authentication codes can provide perfect secrecy if obvious numerical conditions are satisfied; for example, see [13, Theorem 6.4]. Here is a "classical" construction of authentication codes from BIBDs.

Theorem 3.3. *Suppose there is a (v, b, r, k, λ) -BIBD where $r \equiv 0 \pmod{k}$. Then there is an authentication code for k equiprobable sources, having v messages and b equiprobable keys, which satisfies the following properties:*

1. $P_{d_0} = k/v$ and $P_{d_1} = (k-1)/(v-1)$,
2. the code provides perfect secrecy, and
3. if $r = k$, then the optimal key-substitution attack has success probability $(k-1)/(v-1)$, and if $\lambda = 1$, then the optimal key-substitution attack has success probability $1/k$.

Proof. First, we order each block in such a way that each element occurs exactly r/k times in each position. To do this, the technique used in the proof of [13, Theorem 6.4] can be applied (the proof of [13, Theorem 6.4] assumed $\lambda = 1$, but the method can be generalized easily to arbitrary λ). Then, Theorem 1.3 shows that the resulting authentication code has perfect secrecy and $P_{d_0} = k/v$.

We now prove 3, which treats the special cases of (1) SBIBDs and (2) BIBDs with $\lambda = 1$. First, we look at authentication codes derived from an SBIBD. The encoding matrix has one occurrence of each message in each column. Suppose we replace any key K_i with any other key K_j . There are exactly λ messages that occur in both K_i and K_j , and each such message occurs in a different position

in K_i and K_j . Thus the attack is successful if and only if the message m is one of these λ messages. The sources are equiprobable, so the success probability is $\lambda/k = (k-1)/(v-1)$.

Suppose now that the code is derived from a BIBD with $\lambda = 1$. Suppose the attacker replaces a key K_i with another key K_j . Observe that there is at most one message that occurs in both K_i and K_j . If K_i and K_j contain no common message, or if they contain a common message in the same column, the attack will not succeed. Therefore the attacker should choose K_j so that K_i and K_j contain a common message that occurs in different columns. Given a message m in row K_i , there are $r - r/k = r(k-1)/k$ rows in which m occurs in a different column than it does in K_i . Since $\lambda = 1$ and there are k messages in row K_i , the number of rows K_j such that K_i and K_j contain a common message that occurs in different columns is precisely $kr(k-1)/k = r(k-1)$. The optimal attack is to choose one of these $r(k-1)$ rows; the success probability is

$$\frac{r(k-1)/k}{r(k-1)} = \frac{1}{k}.$$

□

Computing the success probability of a key-substitution attack is, in general, more complicated, as blocks of a BIBD might intersect in different numbers of points. There were two types of BIBDs considered in part 3 of Theorem 3.3. Suppose we then construct a robust $(2, 2)$ -threshold scheme from the authentication code using the transformation given in Section 2. The success of modifying share v_1 is quantified by the success of the key-substitution attack in the authentication code setting, whereas the success of modifying share v_2 is the same as the success of the message-substitution attack in the authentication code setting. In general, the success probabilities of the two share-modification attacks will be different; however, if we start with an SBIBD, the probabilities are the same. Theorem 3.1 is fact just the specialization of Theorem 3.3 to symmetric BIBDs.

Applying Theorem 2.1, we have the following.

Theorem 3.4. *If there exists a $(v, k, 1)$ -BIBD, then there exists*

1. *an authentication code with perfect secrecy for k equiprobable sources that is $(1/k)$ -secure against message-substitution and key-substitution attacks, and*
2. *a $(1/k)$ -secure $(2, 2)$ -threshold scheme for k equiprobable secrets.*

Proof. We showed in Theorem 3.3 that the authentication code arising from a $(v, k, 1)$ -BIBD is $(k-1)/(v-1)$ -secure against message-substitution attacks and $(1/k)$ -secure against key-substitution attacks. Since we have

$$\frac{k-1}{v-1} \leq \frac{1}{k}$$

if a $(v, k, 1)$ -BIBD exists, the authentication code is $(1/k)$ -secure against both attacks. Then the stated result follows directly from Theorem 2.1. □

We note that the $(2, 2)$ -threshold scheme arising from part 2. of Theorem 3.4 has share sets (for the two players) of different sizes, unless the BIBD is a projective plane.

3.3 External difference families

A construction for splitting authentication codes using external difference families (or EDFs) was given in [9]. First, we define EDFs. Let G be an additive abelian group of order n having identity 0 . An (n, k, c, λ) -external difference family is a set of k c -subsets of G , say D_1, \dots, D_k , such that the following multiset equation holds.

$$\{x - y : x \in D_i, y \in D_j, i \neq j\} = \lambda(G \setminus \{0\}).$$

That is, when we look at the differences of elements from different c -subsets in the EDF, we see every non-zero value occurring exactly λ times. Therefore, a necessary condition for existence of an (n, k, c, λ) -EDF is that the following equation holds:

$$\lambda(n - 1) = c^2 k(k - 1). \quad (5)$$

The following theorem is a straightforward generalization of [9, Theorem 3.4], which only addressed the case $\lambda = 1$ and did not explicitly discuss key-substitution attacks.

Theorem 3.5. *Suppose there is an (n, k, c, λ) -EDF. Then there is a c -splitting authentication code E for k equiprobable sources, having n messages and n equiprobable keys, such that*

1. *the code provides perfect secrecy,*
2. *$P_{d_0} = ck/n$ and $P_{d_1} = c(k - 1)/(n - 1)$, and*
3. *the optimal key-substitution attack has success probability $c(k - 1)/(n - 1)$.*

Proof. We first specify an arbitrary ordering of the k c -subsets in the EDF and then we develop the EDF through the abelian group G , maintaining the same ordering (as is done in Example 3.2). This yields the encoding matrix of a c -splitting authentication code. In each column of the encoding matrix, we see exactly c occurrences of each element of G . From Theorem 1.3, we have perfect secrecy and $P_{d_0} = ck/n$.

In a message-substitution attack, a message m is substituted with m' . There are precisely λ rows of E that contain m and m' in different c -subsets; these are the keys for which the particular substitution will succeed. Also, there are kc rows that contain m . Since the sources are equiprobable, the probability of a successful message substitution is

$$\frac{\lambda}{kc} = \frac{c(k - 1)}{n - 1},$$

by applying (5).

For a key-substitution attack, a key K is given to the attacker and the attacker must choose a different key K' . Because the encoding matrix is generated from an EDF, there is a value $d \in G$, $d \neq 0$, such that $e_{K'}(s) = e_K(s) + d$ for all s . From this fact, it is not hard to see that

$$\{m : m \in e_K(s) \cap e_{K'}(s'), s \neq s'\} = \{m : m \in e_K(s), m - d \in e_K(s'), s \neq s'\}.$$

Hence, there are exactly λ messages m such that the attack where K is replaced by K' is successful. Since there are kc possible messages $m \in \mu(K)$, and these values of m are equally likely, the key-substitution attack has success probability $\lambda/(kc) = c(k-1)/(n-1)$. \square

Observe that the values of P_{d_0} and P_{d_1} in Theorem 3.5 are optimal, by Theorem 1.1. Also, we have shown that the optimal message-substitution and key-substitution attacks in the above-constructed code have the same success probability, namely $c(k-1)/(n-1)$. Thus, if we apply Theorem 2.1, we obtain a $c(k-1)/(n-1)$ -secure $(2, 2)$ -threshold scheme for k secrets.

Example 3.2. The three sets $\{1, 7, 11\}$, $\{4, 7, 9\}$, $\{5, 16, 17\}$ form a $(19, 3, 3, 3)$ -EDF in \mathbb{Z}_{19} . We develop these sets modulo 19 to obtain the following encoding matrix for a 3-splitting authentication code:

	s_1	s_2	s_3
	$\{1, 7, 11\}$	$\{4, 6, 9\}$	$\{5, 16, 17\}$
	$\{2, 8, 12\}$	$\{5, 7, 10\}$	$\{6, 17, 18\}$
	$\{3, 9, 13\}$	$\{6, 8, 11\}$	$\{7, 18, 0\}$
	$\{4, 10, 14\}$	$\{7, 9, 12\}$	$\{8, 0, 1\}$
	$\{5, 11, 15\}$	$\{8, 10, 13\}$	$\{9, 1, 2\}$
	$\{6, 12, 16\}$	$\{9, 11, 14\}$	$\{10, 2, 3\}$
	$\{7, 13, 17\}$	$\{10, 12, 15\}$	$\{11, 3, 4\}$
	$\{8, 14, 18\}$	$\{11, 13, 16\}$	$\{12, 4, 5\}$
	$\{9, 15, 0\}$	$\{12, 14, 17\}$	$\{13, 5, 6\}$
	$\{10, 16, 1\}$	$\{13, 15, 18\}$	$\{14, 6, 7\}$
	$\{11, 17, 2\}$	$\{14, 16, 0\}$	$\{15, 7, 8\}$
	$\{12, 18, 3\}$	$\{15, 17, 1\}$	$\{16, 8, 9\}$
	$\{13, 0, 4\}$	$\{16, 18, 12\}$	$\{17, 9, 10\}$
	$\{14, 1, 5\}$	$\{17, 0, 3\}$	$\{18, 10, 11\}$
	$\{15, 2, 6\}$	$\{18, 1, 4\}$	$\{0, 11, 12\}$
	$\{16, 3, 7\}$	$\{0, 2, 5\}$	$\{1, 12, 13\}$
	$\{17, 4, 8\}$	$\{1, 2, 6\}$	$\{2, 13, 14\}$
	$\{18, 5, 9\}$	$\{2, 4, 7\}$	$\{3, 14, 15\}$
	$\{0, 6, 10\}$	$\{3, 5, 8\}$	$\{4, 15, 16\}$

The rows of E are indexed by K_0, \dots, K_{18} . The optimal success probability of a message-substitution attack or a key-substitution attack is $1/6$. The code also has perfect secrecy.

An EDF also gives rise to a robust $(2, 2)$ -threshold scheme by applying Theorem 2.1. The two share sets in the threshold scheme have the same size because the authentication code derived from the EDF has the same number of messages as keys.

Theorem 3.6. *If there exists an (n, k, c, λ) -EDF, then there exists a $c(k - 1)/(n - 1)$ -secure $(2, 2)$ -threshold scheme for k equiprobable secrets, in which the share sets for both players have size n .*

3.4 Splitting BIBDs

Splitting BIBDs were defined in [9]. A $(v, u \times c, 1)$ -splitting BIBD is a set system consisting of a set X of v points and a set \mathcal{B} of blocks of size uc , which satisfies the following properties:

1. each block B can be partitioned into u subsets of size c , which are denoted B_i , $1 \leq i \leq u$, and
2. given any two distinct points x and y , there is a unique block B such that $x \in B_i$ and $y \in B_j$, where $i \neq j$.

We note that $(v, u \times 1, 1)$ -splitting BIBD is the same thing as a $(v, u, 1)$ -BIBD.

A $(v, u \times c, 1)$ -splitting BIBD has replication number r and b blocks, where

$$r = \frac{v - 1}{(u - 1)c} \quad \text{and} \quad b = \frac{vr}{uc} = \frac{v(v - 1)}{u(u - 1)c^2}.$$

Of course r and b must be integers if a $(v, u \times c, 1)$ -splitting BIBD exists.

The following definition is new. A $(v, u \times c, 1)$ -splitting BIBD is *equitably ordered* if the multiset equation

$$\bigcup_{B \in \mathcal{B}} B_i = \frac{r}{u} X$$

is satisfied for all i , $1 \leq i \leq u$. If a splitting BIBD is equitably ordered, then it yields an authentication code with perfect secrecy, from Theorem 1.3.

It is shown in [10] that a $(v, u \times c, 1)$ -splitting BIBD can be equitably ordered only if

$$v \equiv 1 \pmod{(u(u - 1)c^2)}. \tag{6}$$

In the case $c = 1$, where a splitting BIBD is just a BIBD, the condition (6) is necessary and sufficient for the design to be equitably orderable. This fact follows from Theorem 3.3. However, when $c > 1$, it is not known if (6) is a sufficient condition for a splitting BIBD to be equitably orderable.

The following result is shown in [10].

Lemma 3.7. *Suppose that a $(v, u \times c, 1)$ -splitting BIBD is generated by base blocks over an abelian group of order v , and suppose every orbit of blocks has size v . Then the splitting BIBD can be equitably ordered.*

Example 3.3. A $(25, 3 \times 2, 1)$ -splitting BIBD is presented in [5]. It has points in \mathbb{Z}_{25} and it is generated from the base block

$$\{\{0, 1\}, \{2, 4\}, \{12, 20\}\}.$$

If we order the base block as

$$(\{0, 1\}, \{2, 4\}, \{12, 20\})$$

and maintain this ordering as the block is developed, we obtain the blocks

$$\begin{aligned} &(\{0, 1\}, \{2, 4\}, \{12, 20\}) \\ &(\{1, 2\}, \{3, 5\}, \{13, 21\}) \\ &\quad \vdots \\ &(\{24, 0\}, \{1, 3\}, \{11, 19\}). \end{aligned}$$

This is an equitable ordering of the splitting BIBD.

It is also shown in [10] that some infinite families of splitting BIBDs that are constructed recursively can be equitably ordered. Specifically, the cases $u = 2$ and $(u, c) = (3, 2), (3, 3), (3, 4)$ and $(4, 2)$ are almost completely solved (with a small number of possible exceptions). See [10] for additional details.

Theorem 3.8. *Suppose there is an equitably ordered $(v, u \times c, 1)$ -splitting BIBD. Then there is a c -splitting authentication code E for u equiprobable sources, having v messages and $b = v(v - 1)/(u(u - 1)c^2)$ keys, such that*

1. *the code provides perfect secrecy,*
2. *$P_{d_0} = cu/v$ and $P_{d_1} = c(u - 1)/(v - 1)$, and*
3. *the optimal key-substitution attack has success probability $1/(cu)$.*

Proof. Part 1 follows from Theorem 1.3 because the splitting BIBD is equitably ordered. Part 2 is shown in [9, Theorem 5.5]. Part 3 is proven as follows. Suppose K is the given key. Fix any message $m \in \mu(K)$. Since the splitting BIBD is equitably ordered, there are

$$r - \frac{r}{u} = \frac{v - 1}{cu}$$

keys K' such that $m \in e_K(s) \cap e_{K'}(s')$ with $s \neq s'$. Since $\lambda = 1$, the number of keys $K' \neq K$ such that there exists a message $m \in e_K(s) \cap e_{K'}(s')$ with $s \neq s'$ is

$$cu \times \frac{v - 1}{cu} = v - 1.$$

The attacker should replace K by one of these $v - 1$ keys. Since sources are equiprobable, the key-substitution attack will succeed with probability

$$\frac{\frac{v-1}{cu}}{v-1} = \frac{1}{cu}.$$

□

Applying Theorem 2.1, we have the following.

Theorem 3.9. *If there exists an equitably ordered $(v, u \times c, 1)$ -splitting BIBD, then there exists*

1. *a c -splitting authentication code with perfect secrecy for u equiprobable sources that is $(1/cu)$ -secure against message-substitution and key-substitution attacks, and*
2. *a $(1/cu)$ -secure $(2, 2)$ -threshold scheme for k equiprobable secrets.*

Proof. We showed in Theorem 3.8 that the authentication code arising from a $(v, u \times c, 1)$ -splitting BIBD is $c(u-1)/(v-1)$ -secure against message-substitution attacks and $(1/cu)$ -secure against key-substitution attacks. In the proof of Theorem 3.8 it is shown that $b \geq v$, so

$$v - 1 \geq u(u - 1)c^2,$$

or

$$\frac{c(u - 1)}{v - 1} \leq \frac{1}{cu}.$$

Hence the authentication code is $(1/cu)$ -secure against both attacks and the stated result follows directly from Theorem 2.1. \square

4 Dual Authentication Codes

Suppose we have an authentication code with sources \mathcal{S} , messages \mathcal{M} , and keyspace \mathcal{K} . The encoding matrix is denoted by E . Then we can construct another authentication code, which we call the *dual code*, by simply interchanging the roles of messages and keys. Thus, the encoding matrix of the dual code is the matrix F having entries

$$F(m, s) = \{K \in \mathcal{K} : m \in e_K(s)\},$$

where $s \in \mathcal{S}$ and $m \in \mathcal{M}$. The keys in the dual code are the same as the messages in the original code.

It is not hard to see that a key-substitution attack in an authentication code is “equivalent” to a message-substitution attack in the dual code.

Theorem 4.1. *A message-substitution attack in an authentication code is successful if and only if the corresponding key-substitution attack is successful in the dual authentication code.*

Note that the probability of a “key” in the dual code is the same as the probability of the corresponding message in the original code. Thus, keys in the dual code will be equiprobable if and only if messages in the original code are equiprobable. In all the examples we consider, we will assume that condition 3. of Theorem 1.3 holds. This will ensure that a code and its dual both have equiprobable keys and messages.

Theorem 4.1 provides an alternative method to compute success probabilities of key-substitution attacks. We illustrate by reconsidering some of the constructions from Section 3, where we computed these success probabilities from first principles.

If we begin with an authentication code having an encoding matrix that is a (v, k, λ) -SBIBD, then the rows of the encoding matrix of the dual code, considered as sets, forms the *dual design* of the SBIBD. It is a classical result in design theory that the dual design of an SBIBD is again a (v, k, λ) -SBIBD. Thus, Theorem 4.1 provides a quick way to see that the optimal success probabilities of the key-substitution and message-substitution attacks are identical in this particular situation (as we showed previously in Theorem 3.1).

Example 4.1. We return to Example 3.1, where we constructed an authentication code from a $(7, 3, 1)$ -SBIBD. We display the encoding matrices of the code and the dual code:

$$E = \begin{array}{|c|c|c|} \hline s_1 & s_2 & s_3 \\ \hline 0 & 1 & 3 \\ \hline 1 & 2 & 4 \\ \hline 2 & 3 & 5 \\ \hline 3 & 4 & 6 \\ \hline 4 & 5 & 0 \\ \hline 5 & 6 & 1 \\ \hline 6 & 0 & 2 \\ \hline \end{array} \quad F = \begin{array}{|c|c|c|} \hline s_1 & s_2 & s_3 \\ \hline K_0 & K_6 & K_4 \\ \hline K_1 & K_0 & K_5 \\ \hline K_2 & K_1 & K_6 \\ \hline K_3 & K_2 & K_0 \\ \hline K_4 & K_3 & K_1 \\ \hline K_5 & K_4 & K_2 \\ \hline K_6 & K_5 & K_3 \\ \hline \end{array}$$

The rows of E are indexed by K_0, \dots, K_6 and the rows of F are indexed by $0, \dots, 6$. The rows of F comprise the blocks of the dual $(7, 3, 1)$ -SBIBD.

Suppose we start with an authentication code E arising from an EDF and then we construct the dual authentication code, F . Let D_1, \dots, D_k be the c -subsets in the original EDF. It is not hard to see that the dual authentication code F is generated from the EDF consisting of the k sets $-D_1, \dots, -D_k$. The dual authentication code F satisfies the same properties as E because it is also obtained from an (n, k, c, λ) -EDF. Thus we see immediately from Theorem 4.1 that the success probability of a key-substitution attack in E is $c(k-1)/(n-1)$ (as we showed previously in Theorem 3.5).

To illustrate, we present a small example.

Example 4.2. We have already noted in Example 3.2 that the three sets $\{1, 7, 11\}$, $\{4, 7, 9\}$, $\{5, 16, 17\}$ form a $(19, 3, 3, 3)$ -EDF in \mathbb{Z}_{19} . We develop these sets modulo 19 to obtain the following encoding matrices for a 3-splitting authentication code and its dual code:

$$E = \begin{array}{|c|c|c|} \hline s_1 & s_2 & s_3 \\ \hline \{1, 7, 11\} & \{4, 6, 9\} & \{5, 16, 17\} \\ \hline \{2, 8, 12\} & \{5, 7, 10\} & \{6, 17, 18\} \\ \hline \{3, 9, 13\} & \{6, 8, 11\} & \{7, 18, 0\} \\ \hline \vdots & \vdots & \vdots \\ \hline \{0, 6, 10\} & \{3, 5, 8\} & \{4, 15, 16\} \\ \hline \end{array}$$

$$F = \begin{array}{c} \begin{array}{|c|c|c|} \hline s_1 & s_2 & s_3 \\ \hline \{K_8, K_{12}, K_{18}\} & \{K_{10}, K_{13}, K_{15}\} & \{K_2, K_3, K_{14}\} \\ \hline \{K_9, K_{13}, K_0\} & \{K_{11}, K_{14}, K_{16}\} & \{K_3, K_4, K_{15}\} \\ \hline \{K_{10}, K_{14}, K_1\} & \{K_{12}, K_{15}, K_{17}\} & \{K_4, K_5, K_{16}\} \\ \hline \vdots & \vdots & \vdots \\ \hline \{K_7, K_{11}, K_{17}\} & \{K_{10}, K_{13}, K_{15}\} & \{K_1, K_2, K_{13}\} \\ \hline \end{array} \end{array}$$

The rows of E are indexed by K_0, \dots, K_{18} and the rows of F are indexed by $0, \dots, 18$. We can view F as being generated from the EDF consisting of sets $\{8, 12, 18\}$, $\{10, 13, 15\}$, $\{2, 3, 14\}$.

Here is another example, which makes use of a BIBD with $\lambda = 1$ that is not a symmetric BIBD.

Example 4.3. We construct an authentication code from a $(13, 3, 1)$ -BIBD. This design has $r = 6$, and $6 \equiv 0 \pmod{3}$, so we can ensure that the corresponding authentication code has perfect secrecy. The 26 blocks of the design can be generated from the two base blocks $\{0, 1, 4\}$ and $\{0, 2, 8\}$ by developing them modulo 13. The 26 by 3 encoding matrix E of the code is as follows:

s_1	s_2	s_3
0	1	4
1	2	5
2	3	6
3	4	7
4	5	8
5	6	9
6	7	10
7	8	11
8	9	12
9	10	0
10	11	1
11	12	2
12	0	3

s_1	s_2	s_3
0	1	8
1	2	9
2	3	10
3	4	11
4	5	12
5	6	0
6	7	1
7	8	2
8	9	3
9	10	4
10	11	5
11	12	6
12	0	7

The dual code has the following 13 by 3 encoding matrix F :

s_1	s_2	s_3
$\{K_0, K_{13}\}$	$\{K_{12}, K_{25}\}$	$\{K_9, K_{18}\}$
$\{K_1, K_{14}\}$	$\{K_0, K_{13}\}$	$\{K_{10}, K_{19}\}$
$\{K_2, K_{15}\}$	$\{K_1, K_{14}\}$	$\{K_{11}, K_{20}\}$
$\{K_3, K_{16}\}$	$\{K_2, K_{15}\}$	$\{K_{12}, K_{21}\}$
$\{K_4, K_{17}\}$	$\{K_3, K_{16}\}$	$\{K_0, K_{22}\}$
$\{K_5, K_{18}\}$	$\{K_4, K_{17}\}$	$\{K_1, K_{23}\}$
$\{K_6, K_{19}\}$	$\{K_5, K_{18}\}$	$\{K_2, K_{24}\}$
$\{K_7, K_{20}\}$	$\{K_6, K_{19}\}$	$\{K_3, K_{25}\}$
$\{K_8, K_{21}\}$	$\{K_7, K_{20}\}$	$\{K_4, K_{13}\}$
$\{K_9, K_{22}\}$	$\{K_8, K_{21}\}$	$\{K_5, K_{14}\}$
$\{K_{10}, K_{23}\}$	$\{K_9, K_{22}\}$	$\{K_6, K_{15}\}$
$\{K_{11}, K_{24}\}$	$\{K_{10}, K_{23}\}$	$\{K_7, K_{16}\}$
$\{K_{12}, K_{25}\}$	$\{K_{11}, K_{24}\}$	$\{K_8, K_{17}\}$

As can be seen, the dual code is 2-splitting. The rows of E are indexed by K_0, \dots, K_{25} and the rows of F are indexed by $0, \dots, 12$. Theorem 3.3 states that the optimal success probability of a key-substitution attack for E is $1/3$. This is of course the same as the optimal success probability of a message-substitution attack for F , by Theorem 4.1.

We now explore some additional properties relating authentication codes to their duals.

Theorem 4.2. *Suppose a c -splitting authentication code for u sources has b equiprobable keys, equiprobable message encoding, v messages, perfect secrecy, and $P_{d_0} = cu/v$. Then the dual authentication code is a (bc/v) -splitting authentication code for u sources that has v equiprobable keys, equiprobable message encoding, b messages, perfect secrecy, and $P_{d_0} = cu/v$.*

Proof. The proof of Theorem 1.3 establishes that equation (4) holds, i.e., every message m occurs bc/v times in each column s of the encoding matrix E . This immediately implies that the dual code is (bc/v) -splitting. Therefore the dual code is a (bc/v) -splitting authentication code for u sources having v equiprobable keys and equiprobable message encoding. Each “message” in the dual code occurs c times in each column s of F (where F is the the encoding matrix of the dual code). Therefore, from Theorem 1.3, the dual code has perfect secrecy and

$$P_{d_0} = \frac{\frac{bc}{v} \times u}{b} = \frac{cu}{v}.$$

□

We note that the hypotheses of Theorem 4.2 are satisfied whenever we construct an authentication code from an equitably ordered BIBD or splitting BIBD.

The authentication code presented in Example 4.3 satisfies the hypotheses of Theorem 4.2 with $v = 13$, $b = 26$, $u = 3$, $c = 1$. Thus, the dual code is 2-splitting with perfect secrecy, each “message” K_i occurs once in each column of F . The code and dual code both have $P_{d_0} = 3/13$.

5 Summary and Discussion

Our goal in this paper has been to develop some theory to better understand various connections between authentication codes and threshold schemes, as well as how certain combinatorial designs can be used to construct these cryptographic objects. To this end, we have proven a simple direct equivalence of certain authentication codes and $(2, 2)$ -threshold schemes. Further, we have introduced the notion of a key-substitution attack and observed that it is identical to a message-substitution attack in a “dual authentication code.”

We have already mentioned that robust (k, n) -threshold schemes are usually constructed by “combining” an algebraic object such as a difference set, EDF, or AMD code with a Shamir threshold scheme. These objects all live in a finite group and, consequently, the construction of the resulting threshold schemes is algebraic. The main equivalence result we have proven (Theorem 2.1) is a purely combinatorial result. It would be of interest to extend our equivalence theorem in some way to handle robust (k, n) -threshold schemes in a strictly combinatorial setting. There is a purely combinatorial analogue of Shamir threshold schemes—namely, orthogonal arrays—so this is perhaps possible.

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] C.J. Colbourn and J.H. Dinitz, eds. *Handbook of Combinatorial Designs, Second Edition*. Chapman & Hall/CRC, 2007.
- [3] R. Cramer, Y. Dodis, S. Fehr, C. Padró and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. *Lecture Notes in Computer Science* **4965** (2008), 471–488 (Eurocrypt 2008).
- [4] M. De Soete. New bounds and constructions for authentication/secret codes with splitting. *Journal of Cryptology* **3** (1991), 173–186.
- [5] G. Ge, Y. Miao and L. Wang. Combinatorial constructions for optimal splitting authentication codes. *SIAM J. Discrete Math.* **18** (2005), 663–678.
- [6] K. Kurowawa, S. Obana and W. Ogata. t -cheater identifiable (k, n) threshold secret sharing schemes. *Lecture Notes in Computer Science* **963** (1995), 410–423. (CRYPTO ’95 Proceedings.)

- [7] J.L. Massey. Cryptography—a selective survey. in “Digital Communications,” 1986, pp. 3–21.
- [8] W. Ogata, K. Kurowawa and D.R. Stinson. Optimum secret sharing scheme secure against cheating. *SIAM J. Discrete Math.* **20** (2006), 79–95.
- [9] W. Ogata, K. Kurowawa, 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.
- [10] M.B. Paterson and D.R. Stinson. Algebraic manipulation detection codes and authentication codes with perfect secrecy. Preprint.
- [11] R.S. Rees and D.R. Stinson. Combinatorial characterizations of authentication codes II. *Designs, Codes and Cryptography* **7** (1996), 239–259.
- [12] G.J. Simmons. Authentication theory / coding theory. *Lecture Notes in Computer Science* **196** (1985), 411–431. (CRYPTO '84 Proceedings.)
- [13] D.R. Stinson. The combinatorics of authentication and secrecy codes. *Journal of Cryptology* **2** (1990), 23–49.
- [14] M. Tompa and H. Woll. How to share a secret with cheaters. *Journal of Cryptology* **1** (1988), 133–138.