Combinatorial Designs and Cryptography, Revisited

Douglas R. Stinson[*]

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

Abstract

In the study of cryptography and information security, combinatorial structures arise in a natural and essential way, especially in the context of unconditional security (also termed information-theoretic security). In this expository paper, I will discuss several interesting examples of interactions between cryptography and combinatorics.

1 Introduction

In 1993, I gave an invited talk at the *Fourteenth British Combinatorial Conference*. The paper [25] I wrote to accompany my talk was entitled "Combinatorial Designs and Cryptography." It contained the following introduction:

> Recent years have seen numerous interesting applications of combinatorics to cryptography. In particular, combinatorial designs have played an important role in the study of such topics in cryptography as secrecy and authentication codes, secret sharing schemes, and resilient functions. The purpose of this paper is to elucidate some of these connections. This is not intended to be an exhaustive survey, but rather a sampling of some research topics in which I have a personal interest.

I was also an invited speaker at the 23rd, 33rd, 43rd and 48th Southeastern Conferences, and in each case my talks explored some aspect of combinatorial cryptography. For example, my 2002 talks at the 33rd Southeastern Conference were entitled "Combinatorial Structure Lurks Everywhere: the Symbiosis of Combinatorics and Cryptography". Clearly this has been an ongoing theme of my research for many years!

[*] The author's research is supported by NSERC discovery grant RGPIN-03882.

Now, 26 years after my talk at the 14th BCC, to honour the occasion of the *50th Anniversary Southeastern International Conference on Combinatorics, Graph Theory & Computing*, I am writing another paper on the same topic. A considerable amount of research in combinatorial cryptography has taken place in the intervening years, so there is much work to draw from. In the interests of space, I will just write about a few topics that have been of particular interest to me.

First, I will discuss the connections between the One-time Pad, perfect secrecy and latin squares in Section 2. I think it is fair to say that this classical material can be regarded as the origin of combinatorial cryptography. In the later sections of this chapter, I will dwell on three topics of continuing and/or recent interest, namely, threshold and ramp schemes, in Section 3; all-or-nothing transforms, in Section 4; and algebraic manipulation codes, in Section 5. For each of these topics, along with other results, I will provide some *combinatorial characterizations* which state that a certain cryptographic primitive exists if and only if a particular combinatorial structure exists.

2 The One-time Pad and Shannon's Theory

Any discussion of the interaction of combinatorics and cryptography must begin with the famous *One-time Pad* of Vernam [30], which was proposed in the mid-1920's. It is quite simple to describe. A message, or *plaintext*, consists of an n-bit binary vector $\mathbf{x} \in (\mathbb{Z}_2)^n$. The value of n is fixed.

The *key* K is also an n-bit binary vector. K should be chosen uniformly at random from the set $(\mathbb{Z}_2)^n$ of all possible keys. It should be shared "ahead of time" in a secure manner by the two parties wishing to communicate, who are traditionally named *Alice* and *Bob*.

Now, at a later time, when Alice wants to send a "secret message" to Bob, she computes the *ciphertext* $\mathbf{y} \in (\mathbb{Z}_2)^n$ using the formula $\mathbf{y} = \mathbf{x} + K$, where addition is performed in $(\mathbb{Z}_2)^n$. (Equivalently, she computes the exclusive-or of the bit-strings $\mathbf{x}$ and K.) When Bob receives $\mathbf{y}$, he decrypts it using the formula $\mathbf{x} = \mathbf{y} + K$.

After its proposal, it was conjectured for many years that the One-time Pad was "unbreakable." Let's consider what this actually means. The setting is that there is an eavesdropper (named *Eve*, say) who observes the ciphertext $\mathbf{y}$ but who does not know the value of K. It is desired that Eve should not be able to compute "any information" about the plaintext $\mathbf{x}$ after observing $\mathbf{y}$.

It is important to point out that K must only be used to encrypt a single message (that is why it is called the One-time Pad, after all). For, if K is used to encrypt two messages, say $\mathbf{x}$ and $\mathbf{x}'$, then the two corresponding ciphertexts are $\mathbf{y} = \mathbf{x} + K$ and $\mathbf{y}' = \mathbf{x}' + K$. From these equations, it is easy to see that $\mathbf{x} + \mathbf{x}' = \mathbf{y} + \mathbf{y}'$. Thus, Eve can compute the exclusive-or of the two plaintexts given only the two ciphertexts, which would be considered a serious loss of security.

Now, given that the key K is used to to encrypt only one message, how do we argue that the One-time Pad is secure? It might be helpful to look at a small example, say for $n = 3$. We construct the *encryption matrix* $M = (m_{\mathbf{x},K})$ for the scheme. The rows of this matrix are indexed by the eight possible plaintexts, the columns are indexed by the eight possible keys, and the entry $m_{\mathbf{x},K}$ is the ciphertext $\mathbf{x} + K$. The following encryption matrix is obtained:

	K							
$\mathbf{x}$	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

Suppose Eve observes the ciphertext $\mathbf{y} = 110$. She can easily identify all occurrences of 110 in the encryption matrix:

	K							
$\mathbf{x}$	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	$\boxed{110}$	111
001	001	000	011	010	101	100	111	$\boxed{110}$
010	010	011	000	001	$\boxed{110}$	111	100	101
011	011	010	001	000	111	$\boxed{110}$	101	100
100	100	101	$\boxed{110}$	111	000	001	010	011
101	101	100	111	$\boxed{110}$	001	000	011	010
110	$\boxed{110}$	111	100	101	010	011	000	001
111	111	$\boxed{110}$	101	100	011	010	001	000

It is clear that the encryption matrix is a latin square of order 8 and the boxed entries form a transversal. Thus, for every possible value of the plaintext $\mathbf{x}$, there is a unique key K (depending on $\mathbf{x}$) such that the encryption of $\mathbf{x}$ with this key yields the observed ciphertext. Consequently, every possible value of the plaintext is compatible with the given ciphertext. Intuitively, this provides some compelling evidence that Eve cannot determine any information about the plaintext simply by observing the ciphertext.

The above informal argument might be fairly convincing, but it is not a rigorous proof. In fact, the first mathematical proof of the security of the One-time Pad was given by Shannon [24] in 1949. Shannon's insight was to introduce probability distributions on the plaintexts and keys, which in turn induce a probability distribution on the ciphertexts. Shannon showed that the One-time Pad satisfied the property of *perfect secrecy*, which states that

$$\mathbf{Pr}[\mathbf{X} = \mathbf{x} \mid \mathbf{Y} = \mathbf{y}] = \mathbf{Pr}[\mathbf{X} = \mathbf{x}]$$

for all $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}_2)^n$, where $\mathbf{X}, \mathbf{Y}$ are random variables corresponding to the plaintext and ciphertext, respectively. That is, the *a priori* probability that the plaintext takes on any particular value is the same as the *a posteriori* probability that it takes on the same value, given that a particular ciphertext has been observed.

Shannon observed that, in any cryptosystem achieving perfect secrecy, the number of keys is at least the number of ciphertexts, which is in turn at least the number of plaintexts. Further, he established the following characterization concerning "minimal" codes that satisfy the perfect secrecy property.

Theorem 2.1. *[24] Suppose a cryptosystem has the same number of keys, plaintexts and ciphertexts. Then the cryptosystem provides perfect secrecy if and only if the encryption matrix is a latin square.*

The encryption matrix of the One-time Pad is the group operation table of $(\mathbb{Z}_2)^n$, which, as we have already noted, is a latin square of order 2^n.

3 Threshold Schemes and Ramp Schemes

Suppose $1 \leq t \leq n$, where t and n are integers. A (t, n)-*threshold scheme* (invented independently by Blakley [2] and Shamir [23] in 1979) allows secret information (called *shares*) to be distributed to n players, so that any t (or more) of the n players can compute a certain *secret*, but no subset of $t-1$ (or fewer) players can determine the secret. The integer t is called the *threshold*. The shares are computed by a *dealer* and distributed to the players using a secure channel. At some later time, a threshold of t players can "combine" their shares using a certain *reconstruction algorithm* and thereby obtain the secret.

It is well-known that the number of possible shares in a threshold scheme must be greater than or equal to the number of possible secrets. If these two numbers are equal, the scheme is an *ideal* threshold scheme.

Shamir's original construction yields ideal (t, n)-threshold schemes. Let's denote the dealer by D and the n players by $P_1, \ldots, P_n$. The scheme is based on polynomial interpolation over a finite field $\mathbb{F}_q$, where $q \geq n + 1$. In an initialization phase, D chooses n distinct, non-zero elements of $\mathbb{F}_q$, denoted x_i, where the value x_i is associated with P_i, $1 \leq i \leq n$.

Suppose $K \in \mathbb{F}_q$ is the secret that D wants to share. D secretly chooses (independently and uniformly at random) values $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$. Then, for $1 \leq i \leq n$, D computes $y_i = a(x_i)$, where

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j .$$

Finally, D gives the share y_i to P_i, for $1 \leq i \leq n$.

The reconstruction algorithm is just polynomial interpolation. Given t points on the polynomial $a(x)$, which has degree at most $t-1$, it is a simple matter to use the Lagrange interpolation formula to determine $a(x)$. Then the secret is obtained as $K = a(0)$. To see that no information about K is revealed by $t-1$ shares, it suffices to observe that any possible value of K is consistent with any $t-1$ shares. That is, given any $t-1$ shares and given a "guess" $K = K_0$, there is a unique polynomial $a_0(x)$ of degree at most $t-1$ such that it agrees with the $t-1$ shares and $a_0(0) = K_0$.

Here are a few details about how reconstruction can be accomplished efficiently using polynomial interpolation. Remember that all computations are to be done in the field $\mathbb{F}_q$. Given t shares, say $y_{i_1}, \dots, y_{i_t}$, the *Lagrange interpolation formula* states that

$$a(x) = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}} \right). \tag{1}$$

However, the t players $P_{i_1}, \dots, P_{i_t}$ do not need to compute the entire polynomial $a(x)$; it is sufficient for them to determine the constant term $K = a(0)$. Hence, they can directly compute K as follows:

$$K = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \right).$$

The above formula is obtained by substituting $x = 0$ into (1).

Now, suppose we define

$$b_j = \prod_{1 \leq k \leq t, k \neq j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}},$$

$1 \leq j \leq t$. These values can be precomputed, and their values are independent of the secret K. Then we have the simplified formula

$$K = \sum_{j=1}^{t} b_j y_{i_j}. \tag{2}$$

Hence, the key is a linear combination (in $\mathbb{F}_q$) of the t shares, where the coefficients $b_1, \dots, b_t$ are public.

Now, whenever I see a combinatorial structure defined by evaluating points on a polynomial, I naturally think of a Reed-Solomon code, or more generally, any orthogonal array with $\lambda = 1$. So I will pause briefly to define orthogonal arrays. An *orthogonal array*, denoted $\mathrm{OA}_\lambda(t, k, v)$, is a λv^t by k array A, defined on a symbol set $\mathcal{X}$ of cardinality v, such that any t of the k columns of A contain all possible t-tuples from $\mathcal{X}^t$ exactly λ times.

It is not difficult to see that an $\mathrm{OA}_1(t, n+1, v)$ gives rise to an ideal (t, n)-threshold scheme with shares (and secret) from an alphabet of size v. Let A be an $\mathrm{OA}_1(t, n+1, v)$ defined on symbol set $\mathcal{X}$ of size v. Label the $n+1$ columns of A with the n players and the dealer, D. Each row of A is a *distribution rule*, where the secret K is the value in column D. Given a desired value for K, D

chooses a random row r in A such that the entry in column D is K (there are v^{t-1} such rows to choose from). Then D distributes the remaining n entries in row r to the n players.

As an example, here is an $\mathrm{OA}_1(2,4,3)$, which gives rise to a $(2,3)$-threshold scheme with shares and secrets in $\{0,1,2\}$. There are nine distribution rules, three for each possible value of the secret.

P_1	P_2	P_3	D
0	0	0	0
1	1	1	0
2	2	2	0
0	1	2	1
1	2	0	1
2	0	1	1
0	2	1	2
1	0	2	2
2	1	0	2

Given an $\mathrm{OA}_1(t,n+1,v)$, say A, it is not hard to see that the above process yields a (t,n)-threshold scheme. First, t shares determine a unique row r of A, which then allows the secret to be computed as $A(r,D)$. If a subset of players only have access to $t-1$ shares and they guess a value K_0 for the secret, this again determines a unique row of A. Thus any set of $t-1$ shares is “consistent” with any possible guess for the secret.

Interestingly, the converse is also true. That is, if there exists an ideal (t,n)-threshold scheme defined on an alphabet of size v, then the distribution rules of the threshold scheme form an $\mathrm{OA}_1(t,n+1,v)$. This more difficult fact was first shown by Keith Martin in 1991 in his PhD thesis [17], and it was also proven independently by Dawson, Mahmoodian and Rahilly [8]. This is summarized as follows.

Theorem 3.1. *[8, 17] There exists an ideal (t,n)-threshold scheme on an alphabet of size v if and only if there exists an $OA_1(t,n+1,v)$.*

3.1 Ramp Schemes

A generalization of a threshold scheme, called a ramp scheme, was invented by Blakley and Meadows [3] in 1984. Suppose $0 \leq s < t \leq n$. *An (s,t,n)-ramp scheme* has two thresholds: the value s is the *lower threshold* and t is the *upper threshold*. It is required that t of the n players can compute the secret, but no subset of s players can determine any information about the secret. Note that a $(t-1,t,n)$-ramp scheme is identical to a (t,n)-threshold scheme.

Ramp schemes provide a tradeoff between security and storage. This is because the size of the secret (relative to the sizes of the shares) can be larger in the case of a ramp scheme, as compared to a threshold scheme. More precisely, it can be shown that, in an (s,t,n)-ramp scheme with shares from a set of size v, there can be as many as v^{t-s} possible secrets. If this bound is met with equality, then the ramp scheme is *ideal*. (Note that the definition of "ideal" for a $(t-1, t, n)$-ramp scheme coincides with the notion of an ideal (t, n)-threshold scheme.)

There is a fairly obvious way to construct an ideal (s, t, n)-ramp scheme from an $\mathrm{OA}_1(t, n+t-s, v)$. The idea is to label n columns of the OA with the n players and label the remaining $t-s$ columns (collectively) with D. A row of the OA comprises a distribution rule for the $(t-s)$-tuple in the columns labelled by D.

A very interesting question is to ask if a converse result holds (as it does for threshold schemes). The first progress in this direction is found in the 1996 paper by Jackson and Martin [13]. It is shown in [13, Theorem 9] that a *strong ideal* (s, t, n)-ramp scheme is equivalent to an $\mathrm{OA}_1(t, n+t-s, v)$. Unfortunately, the definition of a strong ramp scheme is rather complicated and it is perhaps not what would be considered a "natural" definition. So this result is not completely satisfying. Indeed, in [13], the authors ask if it is possible to construct ideal ramp schemes that are not strong.

This was a question that intrigued me for many years, and I worked on it sporadically. Most of my effort was spent trying to prove that any ideal (s, t, n)-ramp scheme is equivalent to an $\mathrm{OA}_1(t, n+t-s, v)$, i.e., to remove the "strong" requirement from [13, Theorem 9]. I was not successful in proving the modified result because it is not true! I eventually came to the realization the the right way to look at the problem was to work with the "obvious" combinatorial structure (which is somewhat weaker than an orthogonal array) that captures the desired properties of an ideal ramp scheme. Thus, I ended up defining a structure that I termed an "augmented orthogonal array." As far as I am aware, this definition had not previously appeared in the literature (for example, I could not find it in Hedayat, Sloane and Stufken [10], which is the standard reference for orthogonal arrays).

Thus, I defined an *augmented orthogonal array*, denoted $\mathrm{AOA}(s, t, n, v)$, to be a v^t by $n+1$ array A that satisfies the following properties:

1. the first n columns of A form an orthogonal array $\mathrm{OA}(t, n, v)$ on a symbol set $\mathcal{X}$ of size v
2. the last column of A contains symbols from a set $\mathcal{Y}$ of size v^{t-s}
3. any s of the first n columns of A, together with the last column of A, contain all possible $(s+1)$-tuples from $\mathcal{X}^s \times Y$ exactly once.

I proved the following result in [27] in 2016.

Theorem 3.2. *[27] There exists an ideal (s, t, n)-ramp scheme with shares chosen from a set of size v if and only if there exists an* $\mathrm{AOA}(s, t, n, v)$.

Note that Theorem 3.2 by itself does not answer the question posed by Jackson and Martin. In order to fully answer their question, it is necessary to consider the relation between OAs and AOAs. It is rather obvious that the existence of an $\mathrm{OA}_1(t, n+t-s, v)$ implies the existence of an $\mathrm{AOA}(s, t, n, v)$, as it suffices to "group" the last $t-s$ columns of the OA and treat the entries in these columns as $(t-s)$-tuples. But what about the converse? It turns out that it is possible to construct infinite classes of $\mathrm{AOA}(s,t,n,v)$ for parameter situations where it can be proven that $\mathrm{OA}_1(t, n+t-s, v)$ do not exist. I provided some constructions in my paper [27], and additional results of this type can be found in Wang *et al.* [31] and Chen *et al.* [4].

Here is a small example, from [27], of an $\mathrm{AOA}(1,3,3,3)$. Let $\mathcal{X} = \mathbb{F}_3$ and $\mathcal{Y} = \mathbb{F}_3 \times \mathbb{F}_3$. The AOA has 27 rows of the form

α	β	γ	$(\alpha+\beta, \alpha+\gamma)$

where $\alpha, \beta, \gamma \in \mathbb{F}_3$. The entire $\mathrm{AOA}(1,3,3,3)$ is as follows:

0	0	0	$(0,0)$
0	0	1	$(0,1)$
0	0	2	$(0,2)$
0	1	0	$(1,0)$
0	1	1	$(1,1)$
0	1	2	$(1,2)$
0	2	0	$(2,0)$
0	2	1	$(2,1)$
0	2	2	$(2,2)$

1	0	0	$(1,1)$
1	0	1	$(1,2)$
1	0	2	$(1,0)$
1	1	0	$(2,1)$
1	1	1	$(2,2)$
1	1	2	$(2,0)$
1	2	0	$(0,1)$
1	2	1	$(0,2)$
1	2	2	$(0,0)$

2	0	0	$(2,2)$
2	0	1	$(2,0)$
2	0	2	$(2,1)$
2	1	0	$(0,2)$
2	1	1	$(0,0)$
2	1	2	$(0,1)$
2	2	0	$(1,2)$
2	2	1	$(1,0)$
2	2	2	$(1,1)$

However, as noted in [27], an $\mathrm{OA}(3,5,3)$ does not exist, because the parameters violate the classical Bush bound.

Finally, I would like to point out a nice alternative characterization of AOAs given by Wang *et al.* [31].

Theorem 3.3. *[31, Theorem 1.3] There exists an* $\mathrm{AOA}(s,t,n,v)$ *if and only if there exists an* $\mathrm{OA}(t,n,v)$ *that can be partitioned into* v^{t-s} $\mathrm{OA}(s,n,v)$.

4 All-or-nothing Transforms

In 1997, Rivest [22] introduced *all-or-nothing transforms.* His motivation was to slow down potential exhaustive key searches by someone trying to break a cryptosystem. In general, a *block cipher* encrypts plaintext in fixed-size chunks, e.g., in 128-bit *blocks.* A list of s plaintext blocks, say $x_1, \dots, x_s$, will be encrypted using a key K to obtain s ciphertext blocks, say $z_1, \dots, z_s$. Perhaps each z_i is the encryption of x_i using K, i.e., $z_i = e_K(x_i)$ for $1 \leq i \leq s$ (this is called *electronic codebook mode* or *ECB mode*). Alternatively, a more sophisticated *mode of operation*, such as cipher-block chaining, might be used. However, most commonly used modes of operation will allow an attacker to obtain one particular plaintext block by trial decryption of one particular ciphertext block using all possible keys (this is called an "exhaustive key search").

Rivest's idea was to develop a technique whereby no individual plaintext block could be computed without first decrypting every ciphertext block (thus he coined the term "all-or-nothing transform"). So, if $s = 1000$, for example, this would slow down the adversary's exhaustive key search by a factor of 1000. In [22], Rivest described methods for achieving this goal in the standard cryptographic setting of computational security. One such method involves a pre-processing step in which $x_1, \dots, x_s$ is converted into $y_1, \dots, y_s$ using an appropriate public bijective transformation, followed by an encryption of $y_1, \dots, y_s$ in ECB mode.

I thought it would be interesting to consider whether Rivest's objective could be achieved in the setting of unconditional security. I presented a simple positive answer to this question in a 2001 paper [26]. Mainly, I considered *linear* all-or nothing transforms, where every y_i is a linear function of $x_1, \dots, x_s$. Before stating the main result from [26], I will give a formal mathematical definition.

Let $\mathcal{X}$ be a finite set of cardinality v. Let $s > 0$ and suppose that $\phi : \mathcal{X}^s \rightarrow \mathcal{X}^s$. Then ϕ is an *(s, v)-all-or-nothing transform* (or *(s, v)-AONT*) provided that:

1. ϕ is a bijection, and
2. Suppose $(y_1, \dots, y_s) = \phi(x_1, \dots, x_s)$. If any $s - 1$ of the s output values $y_1, \dots, y_s$ are fixed, then the value of any one input x_i ($1 \leq i \leq s$) is completely undetermined.

The following easy result was stated in [26].

Theorem 4.1. *[26, Theorem 2.1] Suppose that q is a prime power and M is an invertible s by s matrix with entries from $\mathbb{F}_q$ such that no entry of M is equal to* 0. *Then the function $\phi : (\mathbb{F}_q)^s \rightarrow (\mathbb{F}_q)^s$ defined by $\phi(x_1, \dots, x_s) = (x_1, \dots, x_s)M^{-1}$ is a linear (s, q)-all-or-nothing transform.*

Various examples of matrices M satisfying the conditions of Theorem 4.1 are discussed in [26], including Hadamard matrices, Vandermonde matrices and Cauchy matrices.

Now I jump forward abut 15 years. Jeroen van de Graaf was visiting the University of Waterloo and he asked me if anyone had studied more general versions of AONT in which no information about any t inputs could be obtained from any $s - t$ outputs (the original definition is just the special case $t = 1$ of this more general definition). Such a function defined over an alphabet of a size v will be termed a *(t, s, v)-all-or-nothing transform* (or *(t, s, v)-AONT*).

I thought this was an intriguing question and it has led to a number of recent research papers by myself (in conjunction with various co-authors) and others. I will now survey a few of the known results on this more general problem.

First, the generalization of Theorem 4.1 to $t > 1$ is the following.

Theorem 4.2. *[7] Suppose that q is a prime power and M is an invertible s by s matrix with entries from $\mathbb{F}_q$, such that every $t \times t$ submatrix of M is invertible. Then the function $\phi : (\mathbb{F}_q)^s \rightarrow (\mathbb{F}_q)^s$ defined by $\phi(x_1, \dots, x_s) = (x_1, \dots, x_s)M^{-1}$ is a linear (t, s, q)-all-or-nothing transform.*

Cauchy matrices provide useful examples of linear (t, s, q)-AONTs for arbitrary values of t. An s by s *Cauchy matrix* can be defined over $\mathbb{F}_q$ whenever $q \geq 2s$. Let $a_1, \ldots, a_s, b_1, \ldots, b_s$ be distinct elements of $\mathbb{F}_q$. Define $c_{ij} = 1/(a_i - b_j)$, for $1 \leq i \leq s$ and $1 \leq j \leq s$. Then the Cauchy matrix $C = (c_{ij})$ has the property that any square submatrix of C (including C itself) is invertible over $\mathbb{F}_q$. The next result follows immediately.

Theorem 4.3. *[7, Theorem 2] Suppose q is a prime power, $q \geq 2s$ and $1 \leq t \leq s$. Then there is a linear (t, s, q)-AONT.*

4.1 Binary AONT with $t = 2$

The cases not covered by Theorem 4.3 are when $s > q/2$. When $q = 2$, this result does not say anything useful, so the paper by D'Arco, Esfahani and Stinson [7] investigated this case in detail, concentrating on $t = 2$. It is not difficult to prove that there is no linear $(2, s, 2)$-AONT if $s > 2$, so our paper [7] studied how "close" one could get to a $(2, s, 2)$-AONT. More precisely, $R_2(s)$ was used to denote the maximum density of invertible 2×2 submatrices in an invertible $s \times s$ binary matrix, where "density" is computed as the number of invertible 2×2 submatrices, divided by $\binom{n}{2}^2$. (Here, invertibility refers to invertibility in $\mathbb{F}_2$.)

First, observe that there are exactly six 2 by 2 invertible 0-1 matrices:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

As an example, we showed in [7] that $R_2(3) = 7/9$, and this bound is met by the following matrix:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

It is easy to see that seven of the nine 2×2 submatrices of this matrix are invertible. Further, a short case argument can be used to show that this is best possible.

Using quadratic programming, we proved in [7, Corollary 19] that

$$R_2(s) \leq \frac{5s}{8(s-1)}.$$

Thus the asymptotic density of invertible 2×2 submatrices is at most 5/8. Later, the upper bound on $R_2(s)$ was improved by Zhang, Zhang, Wang and Ge [34], where it was shown that $\lim_{s \to \infty} R_2(s) \leq 0.5$.

Existence results comprise both random methods and deterministic constructions. We observed in [7] that a random 2 by 2 binary matrix, in which every entry equals 1 with probability $\sqrt{1/2}$, is invertible with probability 1/2. Thus, a random s by s binary matrix that is constructed in the same fashion has an expected density equal to 0.5. Such a matrix may or may not be invertible, but a non-invertible matrix can be adjusted slightly to obtain an invertible matrix, by altering some of the entries on the main diagonal (see [34]). This does not affect the asymptotic density.

Various types of deterministic constructions have been considered in [7, 34]. We suggested to use the incidence matrix of a symmetric (v, k, λ)-BIBD in [7]. It is straightforward to count the exact number of invertible 2×2 submatrices in such an incidence matrix, and thereby compute the density. It turns out that the resulting density is close to $1/2$ when the ratio k/v is "close" to $\sqrt{1/2}$.

The points and hyperplanes of the m-dimensional projective geometry over $\mathbb{F}_3$ yield a

$$\left(\frac{3^{m+1}-1}{2}, \frac{3^m-1}{2}, \frac{3^{m-1}-1}{2}\right)\text{-SBIBD.}$$

We noted in [7] that the incidence matrix of this design is invertible and has density equal to

$$\frac{40 \times 3^{2m-3}}{(3^{m+1}-1)(3^m-1)},$$

which asymptotically approaches $40/81 \approx .494$.

We also proposed in [7] to use cyclotomic classes in $\mathbb{Z}_p$, where $p = 4f + 1$ is prime and f is even, to construct a certain binary matrix. After doing some computations involving the cyclotomic numbers of order 4, we showed that the matrices thus obtained have asymptotic density equal to $63/128 \approx .492$, which is not quite as good as the projective geometry example (the matrices also might not be invertible, but they can be "adjusted" using the method from [34]). An identical approach involving cyclotomic numbers of order 7 was subsequently used in [34] to obtain matrices with asymptotic density equal $1200/2401 \approx 0.4997917$. This is the best deterministic construction known at the present time.

4.2 General AONT with $t = 2$

Esfahani, Goldberg and I studied the existence of $(2, s, v)$-AONTs in [9], with particular emphasis on the case of linear AONT defined over a finite field $\mathbb{F}_q$. By using a connection with orthogonal arrays, we showed that a $(2, s, v)$-AONT can exist only if $s \leq v + 1$ (see [9, Corollary 25]). In the linear case, we showed a stronger result, namely that, for a prime power $q > 2$, a linear $(2, s, q)$-AONT defined over $\mathbb{F}_q$ can exist only if $s \leq q$ (see [9, Theorem 14]). As I already mentioned, a Cauchy matrix defined over $\mathbb{F}_q$ can be used to construct a linear $(2, s, q)$-AONT whenever $s \leq q/2$, so the cases of interest are where $q/2 < s \leq q$.

We observed in [9] that it is easy to construct a q by q matrix with entries from $\mathbb{F}_q$ such that any 2 by 2 submatrix is invertible over $\mathbb{F}_q$. The matrix $M = (m_{r,c})$ where $m_{r,c} = r + c$ (for all $r, c \in \mathbb{F}_q$) has this property. Unfortunately, this matrix M is not invertible, so it does not give rise to an AONT.

In [9], we provided some structural results for linear $(2, q, q)$-AONT defined over $\mathbb{F}_q$ and we performed some computer searches for small values of q. We found examples of linear $(2, p, p)$-AONT defined over $\mathbb{Z}_p$ for all odd primes $p \leq 29$. We posed several questions in [9], one of which was to determine if linear $(2, p, p)$-AONT exist for all odd primes $p \geq 3$. This question was answered in the affirmative by Wang, Cui and Ji in [32], who gave a very nice direct construction that we describe now.

Let p be prime, and define a p by p matrix $A = (a_{ij})$, where $0 \leq i, j \leq p - 1$, as follows:

$$a_{ij} = \begin{cases} 0 & \text{if } i = j \\ 1 & \text{if } j = 0,\ i \geq 1 \\ (i-j)^{-1} & \text{if } j > 0,\ i \neq j. \end{cases} \tag{3}$$

The following theorem is proven in [32].

Theorem 4.4. *[32] The matrix A defined in (3) is a linear $(2, p, p)$-AONT.*

Here is the linear $(2, 7, 7)$-AONT obtained from Theorem 4.4:

$$\begin{pmatrix} 0 & 6 & 3 & 2 & 5 & 4 & 1 \\ 1 & 0 & 6 & 3 & 2 & 5 & 4 \\ 1 & 1 & 0 & 6 & 3 & 2 & 5 \\ 1 & 4 & 1 & 0 & 6 & 3 & 2 \\ 1 & 5 & 4 & 1 & 0 & 6 & 3 \\ 1 & 2 & 5 & 4 & 1 & 0 & 6 \\ 1 & 3 & 2 & 5 & 4 & 1 & 0 \end{pmatrix}.$$

5 Algebraic Manipulation Detection Codes

Algebraic manipulation detection codes (or, *AMD codes*) were introduced by Cramer *et al.* [5] in 2008 (see also [6]). These codes are a type of information authentication code that protect against certain types of active attacks by an adversary. In this section, I will discuss results I proved with Maura Paterson in [21] and with Bill Martin in [18], as well as some new results by other authors.

Let $\mathcal{G}$ be an additive abelian group and let $\mathcal{A} = \{A_1, \dots, A_m\}$ consist of m pairwise disjoint k-subsets of G. Then the pair $(\mathcal{G}, \mathcal{A})$ is an *(n, m, k)-AMD code*, which can be used to encode information as follows. A *source* i, such that $1 \leq i \leq m$, is *encoded* by choosing an element $g \in_R A_i$. This notation means that $g \in A_i$ is chosen uniformly at random.[1] Clearly any $g \in \mathcal{G}$ is the encoding of at most one i.

It is desired that an AMD code has certain security properties. There are two flavours of AMD code that I will discuss; they are termed *weak* and *strong* AMD codes.

5.1 Weak and Strong AMD Codes

I will begin with the definition of a weak AMD code.

[1] Some authors have considered a more general definition, where this encoding is not done uniformly at random, but rather, according to a certain probability distribution.

Definition 1 (Weak AMD code)**.**

Suppose $(\mathcal{G}, \mathcal{A})$ *is an* (n, m, k)*-AMD code. Consider the following game:*

1. *The adversary chooses a value* $\Delta \in \mathcal{G} \setminus \{0\}$*.*
2. *The source* $i \in \{1, \ldots, m\}$ *is chosen uniformly at random.*
3. *The source is encoded by choosing* $g \in_R A_i$*.*
4. *The adversary wins if and only if* $g + \Delta \in A_j$ *for some* $j \neq i$*.*

The adversary is free to choose Δ in any manner that they wish, so it is natural to assume that the adversary chooses Δ in order to maximize their probability of winning the above game.

Now I will define strong AMD codes.

Definition 2 (Strong AMD code)**.**

Suppose $(\mathcal{G}, \mathcal{A})$ *is an* (n, m, k)*-AMD code. Consider the following game:*

1. *The source* $i \in \{1, \ldots, m\}$ *is specified and given to the adversary.*
2. *The adversary chooses a value* $\Delta \in \mathcal{G} \setminus \{0\}$*.*
3. *The source is encoded by choosing* $g \in_R A_i$*.*
4. *The adversary wins if and only if* $g + \Delta \in A_j$ *for some* $j \neq i$*.*

Observe that, in a strong AMD code, the adversary knows the source (but not the encoded source) before they choose Δ. On the other hand, in a weak AMD code, the adversary is required to choose Δ before the source is determined. The other difference between weak and a strong AMD codes is that the source is chosen uniformly at random in a weak AMD code, whereas there is no such restriction for a strong AMD code.

The main goal when designing AMD codes is to prevent the adversary from winning the above-described games. Later in this section, I will discuss some constructions for "optimal" AMD codes, which are AMD codes in which the adversary's probability of winning is minimized.

5.2 An Application of AMD Codes to Threshold Schemes

Constructing *robust* threshold schemes has been considered by various researchers, beginning with Tompa and Woll [28]. In 1996, Ogata and Kurosawa [19] suggested using difference sets in conjunction with a Shamir threshold scheme to provide an optimal solution to this problem. A similar construction using EDFs can be found in [20]. In fact, any AMD code can be used in this way, as noted by Cramer *et al.* in [5].

The problem that arises when using the basic Shamir threshold scheme (defined over $\mathbb{F}_q$) in the presence of cheaters is that a single dishonest player can release a bogus share and thereby influence the value of the reconstructed secret in a predictable way. Recall the formula (2) that players $P_{i_1}, \ldots, P_{i_t}$ use to compute the secret:

$$K = \sum_{j=1}^{t} b_j y_{i_j}.$$

Suppose that P_{i_1} claims that their share is y'_{i_j} instead of y_{i_j}. This will lead to the secret being incorrectly computed as

$$K' = b_1 y'_{i_1} + \sum_{j=2}^{t} b_j y_{i_j} = K + b_1(y'_{i_1} - y_{i_1}).$$

Thus, even though P_{i_1} does not know the value of K, they know that the value of the secret will be increased by the known quantity $b_1(y'_{i_1} - y_{i_1})$ as a result of the substitution $y_{i_1} \rightarrow y'_{i_1}$.

AMD codes provide a nice way to prevent (with some probability) a cheating player from carrying out a successful attack of this type. Suppose first that there are m possible secrets, denoted as $\{1, \ldots, m\}$. Next, suppose that $(\mathbb{F}_q, \mathcal{A})$ is an (n, m, k)-weak AMD code (note that we are assuming here that the group G is the additive group of a field). Suppose also that the m possible secrets $\{1, \ldots, m\}$ are equiprobable. Then consider the modified Shamir scheme which works as follows:

1. Given a secret $i \in \{1, \ldots, m\}$, D chooses an element $K \in_R A_i$.

2. D computes shares for K using the usual Shamir threshold scheme over $\mathbb{F}_q$.

To reconstruct a secret, t players proceed as follows:

1. The t players first determine K using (2).

2. Then they determine the value i such that $K \in A_i$.

Now consider what happens if a player P_{i_1} releases a bogus share y'_{i_1} instead of the correct share y_{i_1}. Then the value $K' = K + \Delta$ would be computed in the first stage of reconstruction where $\Delta = b_1(y'_{i_1} - y_{i_1})$. The adversary P_{i_1} would win if $K + \Delta \in A_j$ for some $j \neq i$. Thus, the security of the threshold scheme is determined by the security of the AMD code that is employed in the construction.

If the m possible sources have a nonuniform distribution, we could instead use a strong AMD code to thwart the adversary. A strong AMD code can protect against a cheating player if even if the secret happens to be completely determined ahead of time.

5.3 Combinatorial Analysis of AMD Codes

AMD codes have been studied in a number of papers over the years, and various interesting connections with combinatorial structures have been pointed out, e.g., in [5, 6]. Maura Paterson and I thought it would be of interest to investigate *optimal* AMD codes from a combinatorial viewpoint, which what we did in our 2016 paper [21]. Roughly speaking, the term "optimal" means that the AMD code has the property that the adversary's probability of winning the game described in Definition 1 is minimized.

To be more precise, consider the following analysis. For any source i, there are exactly $k(m-1)$ values of $\Delta \neq 0$ for which the adversary will win this game. It follows that a random choice of $\Delta \neq 0$ will result in the adversary winning the game with probability $k(m-1)/(n-1)$, since sources are equiprobable. We defined a weak (n, m, k)-AMD code to be *R-optimal* if the adversary's optimal strategy is a random choice of $\Delta \neq 0$.

There are interesting connections between R-optimal weak AMD codes and certain types of difference families, which I will describe now. The following definition from [20] is relevant to the subsequent discussion. (I should mention that the more general concept of a *difference system of sets* was defined earlier, by Levenshtein, in [15].)

Definition 3 (External difference family)**.** *Let $\mathcal{G}$ be an additive abelian group of order n. An (n, m, k, λ)-external difference family (or (n, m, k, λ)-EDF) is a set of m disjoint k-subsets of $\mathcal{G}$, say $A_1, \ldots, A_m$, such that the following multiset equation holds:*

$$\bigcup_{\{i,j : i \neq j\}} \{g - h : g \in A_i, h \in A_j\} = \lambda(\mathcal{G} \setminus \{0\}).$$

In words, the multiset of differences obtained from elements in different A_i's yields every non-zero element of $\mathcal{G}$ exactly λ times.

It is obvious that, if an (n, m, k, λ)-EDF exists, then $n \geq mk$ and

$$\lambda(n-1) = k^2 m(m-1). \qquad (4)$$

Also, note that an $(n, m, 1, \lambda)$-EDF is the same thing as an (n, m, λ) difference set.

Here is a nice infinite class of EDFs due to Tonchev.

Theorem 5.1. *[29] Suppose that $q = 2u\ell + 1$ is a prime power, where u and ℓ are odd. Let $\alpha \in \mathbb{F}_q$ be a primitive element and let C be the subgroup of ${\mathbb{F}_q}^*$ having order u and index 2ℓ. Then the ℓ cosets $\alpha^{2i}C$ $(0 \leq i \leq \ell - 1)$ comprise a $(q, u, \ell, (q - 2\ell - 1)/4)$-EDF in $\mathbb{F}_q$.*

The following example illustrates Theorem 5.1.

Example 5.1. *Let $\mathcal{G} = (\mathbb{Z}_{19}, +)$. Then $\alpha = 2$ is a primitive element and $C = \{1, 7, 11\}$ is the (unique) subgroup of order 3 in ${\mathbb{Z}_{19}}^*$. A $(19, 3, 3, 3)$-EDF is given by the three sets $\{1, 7, 11\}$, $\{4, 9, 6\}$ and $\{16, 17, 5\}$.*

Given a weak (n, m, k)-AMD code, because the source is chosen equiprobably, it is not hard to see that the adversary's optimal choice of Δ is the most frequently occurring element in the multiset of differences

$$\bigcup_{\{i,j:i \neq j\}} \{g - h : g \in A_i, h \in A_j\}. \tag{5}$$

Therefore, in order to minimize the adversary's probability of winning the game, all non-zero elements of $\mathcal{G}$ should occur equally often in (5). But this happens precisely when the AMD code is an EDF. Thus, the following theorem is obtained.

Theorem 5.2. *[21, Theorem 3.10] An R-optimal weak (n, m, k)-AMD code is equivalent to an (n, m, k, λ)-EDF.*

We also showed in [21] that "optimal" strong AMD codes can be characterized in terms of certain types of difference families named "strong external difference families." (A related but more general object, called a *differential structure*, was defined in [6].)

Definition 4 (Strong external difference family)**.** *Let $\mathcal{G}$ be an additive abelian group of order n. An $(n, m, k; \lambda)$-strong external difference family (or $(n, m, k; \lambda)$-SEDF) is a set of m disjoint k-subsets of $\mathcal{G}$, say $A_1, \ldots, A_m$, such that the following multiset equation holds for every i, $1 \leq i \leq m$:*

$$\bigcup_{\{j:j \neq i\}} \{g - h : g \in A_i, h \in A_j\} = \lambda(\mathcal{G} \setminus \{0\}). \tag{6}$$

The next theorem is an immediate consequence of Theorems 4.10 and 4.11 from [21].

Theorem 5.3. *An R-optimal strong (n, m, k)-AMD code is equivalent to an (n, m, k, λ)-SEDF.*

There did not seem to be any study of SEDF prior to our 2016 paper [21]. However, it is a natural problem to consider, and several researchers have since obtained interesting results on these structures. I will now discuss some of the known results on SEDF.

First, it is easy to see that a (n, m, k, λ)-SEDF is an $(n, m, k, m\lambda)$-EDF. Therefore, from (4), a necessary condition for existence of an (n, m, k, λ)-SEDF is that

$$\lambda(n - 1) = k^2(m - 1). \tag{7}$$

Here are some fairly trivial examples of SEDFs that we presented in [21].

Example 5.2. *Let $\mathcal{G} = (\mathbb{Z}_{k^2+1}, +)$, $A_1 = \{0, 1, \ldots, k-1\}$ and $A_2 = \{k, 2k, \ldots, k^2\}$. This is a $(k^2 + 1, 2; k; 1)$-SEDF.*

Example 5.3. *Let $\mathcal{G} = (\mathbb{Z}_n, +)$ and $A_i = \{i\}$ for $0 \leq i \leq n - 1$. This is a $(n, n; 1; 1)$-SEDF.*

The following result states that these two examples are the only SEDFs with $\lambda = 1$. It is proven using elementary counting arguments.

Theorem 5.4. *[21, Theorem 2.3] There exists an $(n, m, k, 1)$-SEDF if and only if $m = 2$ and $n = k^2 + 1$, or $k = 1$ and $m = n$.*

When we first defined SEDFs, I thought they would not be difficult to find, e.g., using cyclotomic classes, in a manner similar to Theorem 5.1. I wrote a short computer program to search for examples of this type in finite fields $\mathbb{Z}_p$ for primes $p < 1000$. But my searches were unsuccessful, surprisingly to me at least. So, at the end of our paper [21], we asked if there are examples of strong external difference families with $k > 1$ and $m > 2$.

The first progress on this question occurred when Bill Martin visited me in September 2016. Bill suggested that we use character theory to try and learn more about possible existence or non-existence of SEDF. This turned out be an excellent idea and we were able to prove a few non-existence results which were reported in [18]. The most important result we proved is the following.

Theorem 5.5. *[18, Theorem 3.9] If v is prime, $k > 1$ and $m > 2$, then there does not exist a (v, m, k, λ)-SEDF.*

After Bill and I posted the preprint version of [18] on ArXiV in October, 2016, there was a flurry of activity by several researchers on the topic of SEDFs (see [1, 11, 12, 14, 33]). Several additional nonexistence results were obtained, e.g., when v is the product of two odd primes or the square of an odd prime (see [1, 14] for these and other nonexistence results). But perhaps the biggest surprise was that two groups of researchers independently found a non-trivial example of an SEDF with $m > 2$.

Theorem 5.6. *[14, 33] There exists a $(243, 11, 22, 20)$-SEDF.*

The construction of the $(243, 11, 22, 20)$-SEDF is fairly simple. Let C_0 be the subgroup of ${\mathbb{F}_{3^5}}^*$ having order 22, and let $C_1, \dots, C_{10}$ be its cosets. $\{C_0, \dots, C_{10}\}$ forms the desired SEDF.

The parameters of the SEDF constructed in Theorem 5.6 satisfy the equation $n = km + 1$ and thus they have been termed *near-complete*. The parameter set $(243, 11, 22, 20)$ is quite special; the following result concerning near-complete SEDF was proven by Jedwab and Li in [14].

Theorem 5.7. *[14] If there exists a near-complete (n, m, k, λ)-SEDF, then $(n, m, k, \lambda) = (v, 2, (v-1)/2, (v-1)/4)$ for some $v \equiv 1 \bmod 4$, or $(n, m, k, \lambda) = (243, 11, 22, 20)$.*

Here is one more interesting result. Huczynska and Paterson [11] used combinatorial techniques to prove the following.

Theorem 5.8. *[11] Suppose $\lambda \geq 2$, $m \geq 3$ and $k \geq \lambda + 1$. Then an (n, m, k, λ)-SEDF exists only if*

$$\lambda(k-1)(m-2) \leq (\lambda - 1)k(m-1).$$

Using this theorem, Huczynska and Paterson [11] gave a substantially complete treatment of the case $\lambda = 2$.

5.4 Nonuniform AMD Codes

In [21], we also considered a more general definition of AMD codes, in which the sets $A_1, \ldots, A_m$ are not all required to be the same size. We will call an AMD code of this type a *nonuniform* AMD code.

A study of optimal nonuniform weak AMD codes by Huczynska and Paterson [12] introduced the notion of *reciprocally-weighted external difference families*. These structures can be defined combinatorially (as in [12]), but a more concise definition can be given using the group ring $\mathbb{Q}[G]$. We write elements of $\mathbb{Q}[G]$ as polynomials with rational coefficients and exponents in G. Associated with a subset $A \subseteq G$ we have $A(x) \in \mathbb{Q}[G]$ defined as $A(x) = \sum_{g \in A} x^g$. We also define $A(x^{-1}) = \sum_{g \in A} x^{-g}$ and $G(x) = \sum_{g \in G} x^g$.

Using this notation, we can define EDFs and SEDFs as follows:

- m disjoint k-subsets of $\mathcal{G}$, say $A_1, \ldots, A_m$, comprise an (n, m, k, λ)-EDF if
$$\sum_{i=1}^{m} \sum_{j=1,\ldots,m, j \neq i} A_i(x)A_j(x^{-1}) = \lambda(G(x) - x^0).$$
- m disjoint k-subsets of $\mathcal{G}$, say $A_1, \ldots, A_m$, comprise an (n, m, k, λ)-SEDF if
$$\sum_{j=1,\ldots,m, j \neq i} A_i(x)A_j(x^{-1}) = \lambda(G(x) - x^0)$$
for $j = 1, \ldots, m$.

The above two definitions also make sense in the group ring $\mathbb{Z}[G]$. However, the definition of reciprocally-weighted external difference families, which we give next, is more natural in $\mathbb{Q}[G]$.

Definition 5 (Reciprocally-weighted external difference family)**.** *Let $\mathcal{G}$ be an additive abelian group of order n. An (n, m, λ)-reciprocally-weighted external difference family (or (n, m, λ)-RWEDF) is a set of m disjoint subsets of $\mathcal{G}$, say $A_1, \ldots, A_m$ (of possibly different sizes), such that the following equation holds in $\mathbb{Q}[G]$:*
$$\sum_{i=1}^{m} \sum_{j=1,\ldots,m, j \neq i} \frac{1}{|A_i|} A_i(x)A_j(x^{-1}) = \lambda(G(x) - x^0).$$
(Note that, in this definition, λ is not required to be an integer.) The notation $(n, m; k_1, \ldots, k_m; \lambda)$-RWEDF is also used, where $|A_i| = k_i$ for $1 \leq i \leq m$.

We note that an $(n, m; k; \lambda)$-EDF is equivalent to an $(n, m; k, \ldots, k; \lambda/k)$-RWEDF Here is a nonuniform example.

Example 5.4. *[21, Example 3.1] Let $\mathcal{G} = (\mathbb{Z}_{10}, +)$ and let $A_1 = \{0\}$, $A_2 = \{5\}$, $A_3 = \{1, 9\}$ and $A_4 = \{2, 3\}$. We verify that this is a* $(10, 4; 1, 1, 2, 2; 2)$-

RWEDF:

$$\begin{array}{rcl}
A_1(x)(A_2(x^{-1})+A_3(x^{-1})+A_4(x^{-1})) & = & x^1+x^5+x^7+x^8+x^9\\
A_2(x)(A_1(x^{-1})+A_3(x^{-1})+A_4(x^{-1})) & = & x^2+x^3+x^4+x^5+x^6\\
\frac{1}{2}A_3(x)(A_1(x^{-1})+A_2(x^{-1})+A_4(x^{-1})) & = & \frac{1}{2}x^1+\frac{1}{2}x^4+x^6+\frac{1}{2}x^7+\frac{1}{2}x^8+x^9\\
\frac{1}{2}A_4(x)(A_1(x^{-1})+A_2(x^{-1})+A_3(x^{-1})) & = & \frac{1}{2}x^1+x^2+x^3+\frac{1}{2}x^4+\frac{1}{2}x^7+\frac{1}{2}x^8.
\end{array}$$

Summing the polynomials on the right sides of these four equations, we obtain $2(\mathbb{Z}_{10}(x)-x^0)$, as claimed.

Huczynska and Paterson [12] proved the following equivalence.

Theorem 5.9. *[12, Theorem 1.10] An R-optimal weak nonuniform (n, m)-AMD code is equivalent to an (n, m, λ)-RWEDF.*

Turning now to strong AMD codes, the R-optimal codes can be characterized in terms of the generalized strong external difference families that Paterson and I defined in [21]. Here I give the group ring definition.

Definition 6 (Generalized strong external difference family)**.** *Let $\mathcal{G}$ be an additive abelian group of order n. An $(n, m; \lambda_1, \dots, \lambda_m)$-generalized strong external difference family (or $(n, m; \lambda_1, \dots, \lambda_m)$-GSEDF) is a set of m disjoint subsets of $\mathcal{G}$, say $A_1, \dots, A_m$ (of possibly different sizes), such that the following equation holds in $\mathbb{Z}[G]$:*

$$\sum_{j=1,\dots,m, j\neq i} A_i(x)A_j(x^{-1}) = \lambda_i(G(x)-x^0)$$

for $i = 1, \dots, m$, where the λ_i's are positive integers. It is sometimes convenient to use the notation $(n, m; k_1, \dots, k_m; \lambda_1, \dots, \lambda_m)$-GSEDF, where $|A_i| = k_i$ for $1 \leq i \leq m$.

It is clear that an $(n, m; k; \lambda)$-SEDF is equivalent to an $(n, m; k, \dots, k; \lambda, \dots, \lambda)$-GSEDF. Here is a nonuniform example.

Example 5.5. *[21, Example 2.7] Let $\mathcal{G} = (\mathbb{Z}_7, +)$ and let $A_1 = \{1\}$, $A_2 = \{2\}$, $A_3 = \{4\}$ and $A_4 = \{0, 3, 5, 6\}$. It is straightforward to check that this is a $(7, 4; 1, 1, 1, 4; 1, 1, 1, 2)$-GSEDF.*

In fact, Example 5.5 is a special case of the following more general theorem that we proved in [21].

Theorem 5.10. *[21, Theorem 2.4] Suppose $A_1, \dots, A_m$ is a partition of an abelian group $\mathcal{G}$ of order n, where $|A_i| = k_i$ for $1 \leq i \leq m$. Then $A_1, \dots, A_m$ is an $(n, m; k_1, \dots, k_m; \lambda_1, \dots, \lambda_m)$-GSEDF if and only if A_i is an $(n, k_i, k_i - \lambda_i)$-difference set in $\mathcal{G}$, for $1 \leq i \leq m$.*

In Example 5.5, A_1, A_2 and A_3 are difference sets with $\lambda = 0$, while A_4 is a difference set with $\lambda = 2$.

Theorem 5.11. *[21, Theorems 4.10 and 4.11] An R-optimal strong nonuniform (n, m)-AMD code is equivalent to an $(n, m; \lambda_1, \ldots, \lambda_m)$-GSEDF.*

For additional existence and nonexistence results on GSEDF, see [16, 21].

6 Conclusion and Open Problems

There are many other topics that could be included in a survey paper such as this one. The topics I chose are all research areas of current interest in which there are interesting unsolved problems to investigate. Here are four open problems that I find particularly interesting.

1. Construct further example of $\mathrm{AOA}(s, t, n, v)$ in parameter situations where the corresponding $\mathrm{OA}_1(t, n + t - s, v)$ do not exist.
2. Find a deterministic construction which shows that $R_2(s) \rightarrow 0.5$ as $s \rightarrow \infty$.
3. Determine if there exist (nonlinear) $(2, v + 1, v)$-AONT.
4. Determine if there exist any additional (other than the example provided in Theorem 5.6) nontrivial (n, m, k, λ)-SEDF with $m > 2$.

References

[1] J. Bao, L. Ji, R. Wei and Y. Zhang. New existence and nonexistence results for strong external difference families. *Discrete Mathematics* **341** (2018), 1798–1805.

[2] G.R. Blakley. Safeguarding cryptographic keys. *Proceedings AFIPS 1979 National Computer Conference*, pp. 313–317.

[3] G.R. Blakley and C. Meadows. Security of ramp schemes. *Lecture Notes in Computer Science* **196** (1985), 242–268 (Advances in Cryptology: Proceedings of CRYPTO '84).

[4] G. Chen, C. Shi and Y. Guo. Ideal ramp schemes and augmented orthogonal arrays. *Discrete Mathematics* **342** (2019), 405–411.

[5] 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.)

[6] R. Cramer, S. Fehr and C. Padró. Algebraic manipulation detection codes. *Science China Mathematics* **56** (2013), 1349–1358.

[7] P. D'Arco, N. Nasr Esfahani and D.R. Stinson. All or nothing at all. *Electronic Journal of Combinatorics* **23(4)** (2016), paper #P4.10, 24 pp.

[8] E. Dawson, E.S. Mahmoodian and A. Rahilly. Orthogonal arrays and ordered threshold schemes. *Australasian Journal of Combinatorics* **8** (1993), 27–44.

[9] N. Nasr Esfahani, I. Goldberg and D.R. Stinson. Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets. *IEEE Transactions on Information Theory* **64** (2018), 3136–3143.

[10] A.S. Hedayat, N.J.A. Sloane and J. Stufken. *Orthogonal Arrays: Theory and Applications.* Springer, 1999.

[11] S. Huczynska and M.B. Paterson. Existence and non-existence results for strong external difference families. *Discrete Mathematics* **341** (2018), 87–95.

[12] S. Huczynska and M.B. Paterson. Weighted external difference families and R-optimal AMD codes. *Discrete Mathematics* **342** (2019), 855–867.

[13] W.A. Jackson and K.M. Martin. A combinatorial interpretation of ramp schemes. *Australasian Journal of Combinatorics* **14** (1996), 51–60.

[14] J. Jedwab and S. Li. Construction and nonexistence of strong external difference families. *Journal of Algebraic Combinatorics* **49** (2019), 21–48.

[15] V.I. Levenshtein. One method of constructing quasilinear codes providing synchronization in the presence of errors. *Problems of Information Transmission* **7** (1971), 215–222.

[16] X. Lu, X. lei Niu and H. Cao. Some results on generalized strong external difference families. *Designs, Codes and Cryptography* **86** (2018), 2857–2868.

[17] K.M. Martin. *Discrete Structures in the Theory of Secret Sharing.* PhD Thesis, University of London, 1991.

[18] W.J. Martin and D.R. Stinson. Some nonexistence results for strong external difference families using character theory. *Bulletin of the ICA* **80** (2017), 79–92.

[19] W. Ogata and K. Kurosawa. Optimum secret sharing scheme secure against cheating. *Lecture Notes in Computer Science* **1070** (1996), 200–211. (Advances in Cryptology — EUROCRYPT '96.)

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

[21] M.B. Paterson and D.R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. *Discrete Mathematics* **339** (2016), 2891–2906.

[22] R.L. Rivest. All-or-nothing encryption and the package transform. *Lecture Notes in Computer Science* **1267** (1997) pp. 210–218. (Fast Software Encryption, 1997.)

[23] A. Shamir. How to share a secret. *Communications of the ACM* **22** (1979), 612–613.

[24] C. E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal* **28** (1949), 656-715.

[25] D.R. Stinson. Combinatorial designs and cryptography. In "Surveys in Combinatorics, 1993", Cambridge University Press, 1993, pp. 257–287 (*London Mathematical Lecture Note Series*, vol. 187).

[26] D.R. Stinson. Something about all or nothing (transforms). *Designs, Codes and Cryptography* **22** (2001), 133–138.

[27] D.R. Stinson. Ideal ramp schemes and related combinatorial objects. *Discrete Math.* **341** (2018), 299–307.

[28] M. Tompa and H. Woll. How to share a secret with cheaters. *Journal of Cryptology* **1** (1989), 133–138.

[29] V.D. Tonchev. Difference systems of sets and code synchronization. *Rendiconti del Seminario Matematico di Messina Series II* **9** (2003), 217–226.

[30] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the American Institute of Electrical Engineers* **55** (1926), 109-115.

[31] X. Wang, L. Ji, Y. Li and M. Liang. Constructions of augmented orthogonal arrays. *Journal of Combinatorial Designs* **26** (2018), 547–559.

[32] X. Wang, J. Cui and L. Ji. Linear $(2, p, p)$-AONTs exist for all primes p. *Designs, Codes and Cryptography*, to appear.

[33] J. Wen, M. Yang, F. Fu and K. Feng. Cyclotomic construction of strong external difference families in finite fields. *Designs, Codes and Cryptography* **86** (2018), 1149–1159.

[34] Y. Zhang, T. Zhang, X. Wang and G.Ge. Invertible binary matrices with maximum number of 2-by-2 invertible submatrices. *Discrete Mathematics* **340** (2017), 201–208.