Ideal Threshold Schemes from Orthogonal Arrays

Josef Pieprzyk and Xiam-Mo Zhang

Centre for Advanced Computing – Algorithms and Cryptography
Department of Computing, Macquarie University
Sydney , NSW 2109, AUSTRALIA
josef,xianmo@ics.mq.edu.au

Abstract. The work investigates the design of ideal threshold secret sharing in the context of cheating prevention. We showed that each orthogonal array is exactly a defining matrix of an ideal threshold scheme. To prevent cheating, defining matrices should be nonlinear so both the cheaters and honest participants have the same chance of guessing of the valid secret. The last part of the work shows how to construct nonlinear secret sharing based on orthogonal arrays.

Key Words: Threshold Secret Sharing, Orthogonal Arrays, Cheating Detection, Nonlinear Functions.

1 Introduction

Secret sharing is one of basic cryptographic algorithms that is of great importance for cryptographic services where actions are controlled by groups. It is a well known fact that linear secret sharing is vulnerable to cheating attacks. In these attacks, dishonest participants submit forged shares to the combiner who returns an invalid secret. The cheaters, knowing the invalid secret and their valid shares, are able to recover the valid secret. As the result, the cheaters hold the valid secret while the honest participants are left with the invalid one distributed by the combiner.

This paper explores how (nonlinear) orthogonal arrays can be used to build ideal threshold schemes that are immune against cheating. The immunity against cheating springs from the fact that, in nonlinear secret sharing, a cheater is unable to obtain the valid secret. More precisely, the probability of guessing the valid secret by the cheater and honest participants are the same.

This work is structured as follows. The basic concepts of secret sharing are introduced in Section 2. In Section 3, we define a perfect secret sharing scheme using defining matrices. An ideal secret sharing scheme is a perfect scheme for which the set of secrets and the set of shares have the same size. We investigate some properties of ideal secret sharing in Section 4. In Section 5, we introduce orthogonal arrays and show how they can be used to construct ideal threshold schemes. In Section 6, we study properties of such ideal threshold schemes and their applications for cheating prevention. In Section 7 we demonstrate the existence of orthogonal arrays that are defining matrices of ideal threshold schemes. Section 8 examines how cheating attacks can be prevented in secret sharing based on orthogonal arrays and constructions of secret sharing immune against cheating are given. Conclusions close the work.

2 Access Structures

Secret sharing is a method to share a secret among a set of participants $\mathbf{P} = \{P_1, \ldots, P_n\}$. Let $\mathbf{K}$ denote the set of *secrets* and $\mathbf{S}$ denote the set of *shares*. The secret sharing includes two algorithms: the distribution algorithm (dealer) and the recovery algorithm (combiner). The dealer assigns shares $s_1, \ldots, s_n$ to all the participants $P_1, \ldots, P_n$, respectively, or in other words, it creates the secret sharing system. After that the participants collectively hold the secret until there is a big enough subset of participants who wish to recover the secret by calling the recovery algorithm. Assume that the currently active participants are $P_{j_1}, \ldots, P_{j_\ell}$ and that they submit their shares to the combiner in order to recover the secret. Their shares $s_{j_1}, \ldots, s_{j_\ell}$ can determine a secret if and only if $\{P_{j_1}, \ldots, P_{j_\ell}\}$ is a qualified subset of $\mathbf{P}$, i.e., the set of currently active participants belongs to the access structure Γ. It turns out that any access control is *monotone* or any superset of qualified set of participants belongs to the access structure, or more precisely

$$\text{if } \mathcal{A} \in \Gamma \text{ and } \mathcal{A} \subseteq \mathcal{B} \subseteq \mathbf{P} \text{ then } \mathcal{B} \in \Gamma \tag{1}$$

We can describe secret sharing with the access structure Γ by an $m \times (n+1)$ matrix M^*, as shown in [2,3]. The matrix M^* has $n+1$ columns indexed by $0, 1 \ldots, n$. The number m of rows of M^* depends on a particular scheme. We index the m rows by $1, \ldots, m$. For a row of M^*, the entry in the 0th position holds a secret and the entry in the ith position ($i = 1, \ldots, n$) contains the corresponding share of P_i. Denote the entry on the ith row and the jth column of M^* by $M^*(i, j)$. The matrix M^* is called a *defining matrix* of secret sharing with the access scheme Γ. The matrix M obtained from M^* by removing the 0th column is called the *associated matrix* of the scheme.

The dealer works in two stages. In the first stage, it creates the defining matrix M^* for secret sharing with the access structure Γ. The matrix is made public. In the second stage, the dealer randomly chooses a row of the matrix M^*. Let the row chosen be indexed by the integer i. The secret is $K = M^*(i, 0)$ and shares are $s_j = M^*(i, j)$, $j = 1, \ldots, n$. The shares are distributed to the corresponding participants via secure channels.

An access structure $\Gamma = \{\mathcal{A} \mid \#\mathcal{A} \geq t\}$ is called a (t, n)-*threshold access structure*, where $\#X$ denotes the cardinality of the set X (i.e., the number of elements in the set X) and the integer t is called the *threshold* of secret sharing, where $t \leq n$. Secret sharing schemes with the (t, n)-threshold access structure are called (t, n)-threshold schemes.

It should be noticed that a defining matrix uniquely determines a secret sharing scheme but a secret sharing scheme has more defining matrices. Permuting the rows of a defining matrix of secret sharing does not give a new scheme. Clearly, two secret sharing schemes are considered to be the same if the defining matrix of the one can be obtained from the other by permuting the rows of its defining matrix. Permuting the columns of defining matrices of secret sharing is equivalent to changing the indices of participants. In other words, access structures of secret sharing with permuted columns are different but one access structure can be derived from the other by permuting the participants. For this reason, we do not regard the the resulting scheme as a new one. We say that the resulting scheme is *equivalent* to the original one.

It should be pointed out once again that a defining matrix of a secret sharing scheme is public. The dealer chooses at random a single row of the matrix. The shares are communicated to the corresponding participants via secure channels so the share s_i is known to the participant P_i only $(i = 1, \ldots, n)$.

3 Perfect Secret Sharing

We say that secret sharing with the access structure $\mathit{\Gamma}$ is perfect if the following two conditions are satisfied:

(1) If $\mathcal{A} \in \mathit{\Gamma}$ then the participants in $\mathcal{A}$ can uniquely determine the secret by pooling their shares together.
(2) if $\mathcal{A} \notin \mathit{\Gamma}$ then the participants from $\mathcal{A}$ can determine nothing about the secret (in an information theoretic sense).

As argued in [2], Conditions (1) and (2) can be translated into conditions that need to be satisfied in the context of the defining matrix.

(a) Let $\mathcal{A} \in \mathit{\Gamma}$. If $M^*(i,j) = M^*(i',j)$ for every $P_j \in \mathcal{A}$ then $M^*(i,0) = M^*(i',0)$.
(b) Let $\mathcal{A} \notin \mathit{\Gamma}$. For any $1 \leq i_0 \leq m$ and any $K \in \mathbf{K}$, there exists some i with $1 \leq i \leq m$ such that $M^*(i,j) = M^*(i_0,j)$ for all $P_j \in \mathcal{A}$ and $M^*(i,0) = K$.
(b') Let $\mathcal{A} = \{P_{j_1}, \ldots, P_{j_\ell}\} \notin \mathit{\Gamma}$. For any $s_{j_1}, \ldots, s_{j_\ell} \in \mathbf{S}$ and any $K \in \mathbf{K}$,

$$\#\{i \mid M^*(i,j_u) = s_{j_u} \text{ for all } P_{j_u} \in \mathcal{A} \text{ and } M^*(i,0) = K\}$$

is independent to the choice of K.

It is easy to verify that (b') implies (b). For the case of a (t,n)-threshold scheme, Conditions (a), (b), and (b') can be rewritten as follows:

(c) Let $\#\mathcal{A} \geq t$. If $M^*(i,j) = M^*(i',j)$ for every $P_j \in \mathcal{A}$ then $M^*(i,0) = M^*(i',0)$.
(d) Let $\#\mathcal{A} < t$. For any $1 \leq i_0 \leq m$ and any $K \in \mathbf{K}$, there exists some i with $1 \leq i \leq m$ such that $M^*(i,j) = M^*(i_0,j)$ for all $P_j \in \mathcal{A}$ and $M^*(i,0) = K$.

(d') Let $\mathcal{A} = \{P_{j_1}, \ldots, P_{j_\ell}\}$ with $\ell < t$. For any $s_{j_1}, \ldots, s_{j_\ell} \in \mathbf{S}$ and any $K \in \mathbf{K}$,

$$\#\{i \mid M^*(i, j_u) = s_{j_u} \text{ for all } P_{j_u} \in \mathcal{A} \text{ and } M^*(i, 0) = K\}$$

is independent to the choice of K.

Similarly, (d') implies (d).

Definition 1. *A secret sharing scheme satisfying (a) and (b) is called* weakly perfect*, while it is called* perfect *if it satisfies (a) and (b') [2]. Alternatively, a (t, n)-threshold scheme satisfying (c) and (d) is called* weakly perfect*, while it is called* perfect *if it satisfies (c) and (d').*

Threshold schemes were first introduced by Blakley [1] and Shamir [6]. Ito et al [5] generalized threshold secret sharing for arbitrary monotonic access structures.

4 Ideal Secret Sharing

Given an access structure Γ. A set $\mathcal{A} \in \Gamma$ is called *minimal* if all proper subsets of $\mathcal{A}$ do not belong to Γ. It is easy to see that $\mathcal{A}$ is minimal for a (t, n)-threshold access structure if and only if $\#\mathcal{A} = t$.

Lemma 1. $\#\mathbf{K} \leq \#\mathbf{S}$ *for any weakly perfect secret sharing scheme.*

Proof. Denote $\mathbf{K} = \{K_1, \ldots, K_\kappa\}$. We are going to consider the following two cases: every minimal $\mathcal{A} \in \Gamma$ satisfies $\#\mathcal{A} = 1$ and there exists a minimal $\mathcal{A}_0 \in \Gamma$ such that $\#\mathcal{A}_0 \geq 2$. The first case is trivial. For this case, let $M^*(i_1, 0) = K_1$ ..., $M^*(i_\kappa, 0) = K_\kappa$. Since $K_1, \ldots, K_\kappa$ are mutually distinct, due to Condition (a), $M^*(i_1, 1)$, ..., $M^*(i_\kappa, 1)$ must be mutually distinct. This proves that $\#\mathbf{S} \geq \#\mathbf{K}$. Consider the second case: there exists a minimal $\mathcal{A}_0 \in \Gamma$ such that $\#\mathcal{A}_0 \geq 2$. Let $\mathcal{A}_0 = \{P_{j_1}, \ldots, P_{j_\ell}\}$ where $j_1 < \cdots < j_\ell$. For fixed i_0th row of M^*, let $M^*(i_0, j_1) = s_{j_1}, \ldots, M^*(i_0, j_{\ell-1}) = s_{j_{\ell-1}}$. Since $\{P_{j_1}, \ldots, P_{j_{\ell-1}}\} \notin \Gamma$, according to Condition (b), for each K_r with $1 \leq r \leq \kappa$, there exists a row i_r of M^* such that $M^*(i_r, j_1) = s_{j_1}, \ldots, M^*(i_r, j_{\ell-1}) = s_{j_\ell - 1}$ and $M^*(i_r, 0) = K_r$, where $r = 1, \ldots, \kappa$. Since $M^*(i_1, 0) = K_1, \ldots, M^*(i_\kappa, 0) = K_\kappa$ are mutually distinct, due to Condition (a), $M^*(i_1, j_\ell), \ldots, M^*(i_\kappa, j_\ell)$ must be mutually distinct. This proves that $\mathbf{S}$ contains at least κ elements, i.e., $\#\mathbf{S} \geq \#\mathbf{K}$. □

A similar statement for perfect secret sharing appeared previously, for instance, in [3], that is, $\#\mathbf{K} \leq \#\mathbf{S}$ for any perfect secret sharing scheme. Since any perfect secret sharing is a special weakly perfect secret sharing, Lemma 1 is more general. In particular, if the equality in Lemma 1 holds, i.e., $\#\mathbf{K} = \#\mathbf{S}$, the perfect secret sharing scheme is said to be ideal.

Definition 2. *A perfect secret sharing scheme is said to be* ideal *if $\#\mathbf{K} = \#\mathbf{S}$, where $\mathbf{K}$ and $\mathbf{S}$ denote the set of secrets and the set of shares respectively. Alternatively, a perfect threshold scheme is said to be* ideal *if the set of secrets and the set of shares have the same cardinality.*

Using the same approach as in the proof of Lemma 1, we can prove the following lemma.

Lemma 2. *Let M be an associated matrix M of an ideal secret sharing scheme with an access structure $\mathit{\Gamma}$. Let $\mathcal{A}_0 = \{P_{j_1}, \dots, P_{j_\ell}\} \in \mathit{\Gamma}$, where $j_1 < \cdots < j_\ell$, be a minimal set. Then the submatrix of M, comprised of ℓ columns of M, indexed by $j_1, \dots, j_\ell$, contains each row vector $(s_1, \dots, s_\ell)$ where each $s_j \in \mathbf{S}$.*

In particular, we can formulate the following corollary.

Corollary 1. *Let M be an associated matrix of an ideal (t, n)-threshold scheme. Then a submatrix of M consisting of any t columns, contains all values of the vector $(s_1, \dots, s_t)$ where each $s_j \in \mathbf{S}$.*

Let M^* be a defining matrix of an ideal (t, n)-threshold scheme. Set $\mathbf{S}^t = \{(s_1, \dots, s_t) \mid s_1, \dots, s_t \in \mathbf{S}\}$. Let $1 \leq j_1 < \cdots < j_t \leq n$ and M_1 be the $m \times t$ submatrix of M, comprised of the t columns indexed by $j_1, \dots, j_t$. We now define a function, denoted by $\chi_{j_1,\dots,j_t}$, from $\mathbf{S}^t$ to $\mathbf{K}$ as follows. According to Corollary 1, for any $(s_1, \dots, s_t) \in \mathbf{S}^t$, there exists some i_0 with $1 \leq i_0 \leq m$ such that $M^*(i_0, j_1) = s_1, \dots, M^*(i_0, j_t) = s_t$. Let $M^*(i_0, 0) = K$. Note that according to Condition (d), if there exists another i_1 $(1 \leq i_1 \leq m)$ such that $M^*(i_1, j_1) = s_1, \dots, M^*(i_1, j_t) = s_t$, then $M^*(i_1, 0) = K$. Thus we can define K to be the image of $(s_1, \dots, s_t)$ and write $K = \chi_{j_1,\dots,j_t}(s_1, \dots, s_t)$. We call $\chi_{j_1,\dots,j_t}$ the *secret function* with respect to $j_1, \dots, j_t$. Secret functions play an important role as a tool against cheating. This will be elaborated later.

5 Ideal Threshold Schemes from Orthogonal Arrays

An $m \times n$ matrix with entries from b-set $\mathbf{B}$ is called an *orthogonal array*, denoted by (m, n, b, t), if its any $m \times t$ submatrix contains all b^t possible row vectors precisely λ times. Clearly $m = \lambda b^t$. The parameters m, t and λ are called the *size*, the *strength* and the *index* of the orthogonal array, respectively, while n is called the number of *constraints* and b is called the number of *levels*.

Lemma 3. *An orthogonal array (m, n, b, t) with an index λ is an orthogonal array (m, n, b, ℓ) with an index $\lambda b^{t-\ell}$ where ℓ is any integer with $1 \leq \ell \leq t$.*

In particular, we can formulate the following corollary.

Corollary 2. *Each column of an orthogonal array (m, n, b, t) with entries from a b-set $\mathbf{B}$ contains each element of $\mathbf{B}$ precisely λb^{t-1} times, where λ is the index of the orthogonal array.*

This following statement is obvious.

Lemma 4. *Let O_1 be an $m \times n_1$ submatrix of an orthogonal array (m, n, b, t) with an index λ. If $n_1 \geq t$ then O_1 is an orthogonal array (m, n_1, b, t) with an index λ.*

Orthogonal arrays with index $\lambda = 1$, i.e, orthogonal arrays (b^t, n, b, t) have many interesting properties. The following bounds on the number of constraints for orthogonal arrays (b^t, n, b, t) was proved by Bush [4]:

Lemma 5. *For an orthogonal array (b^t, n, b, t),*

(i) if $t \le b$ then $n \le b + t - 1$ (b is even) or $n \le b + t - 2$ (b is odd and $t \ge 3$),
(ii) if $b \le t$, then $n \le t + 1$.

Theorem 1. *An orthogonal array $(b^t, n+1, b, t)$ with entries from a b-set $\mathbf{B}$ is a defining matrix of an ideal (t, n)-threshold scheme with $\mathbf{K} = \mathbf{S} = \mathbf{B}$.*

Proof. Let O be an orthogonal array $(b^t, n+1, b, t)$ with entries from b-set $\mathbf{B}$. We index the columns of O by $j = 0, 1, \ldots, n$ and index the rows of O by i, $1 \le i \le b^t$. We write $O(i, j)$ to denote the entry of O in the i row and the j column. We now construct a (t, n)-threshold with participants $P_1, \ldots, P_n$ as follows. For an ith row, let $O(i, 0)$ be a secret, and $O(i, j)$ denote the share of participant of P_j, $j = 1, \ldots, n$. We next prove that this scheme satisfies Condition (c) and (d').

Let $\{P_{j_1}, \ldots, P_{j_\ell}\}$ be the set of currently active participants. For the case of $\ell \ge t$, if $O(i, j_1) = O(i', j_1), \ldots, O(i, j_\ell) = O(i', j_\ell)$, then it follows that $i = i'$, as the orthogonal array $(b^t, n+1, b, t)$ has index $\lambda = 1$. Thus Condition (c) is satisfied. For the case of $\ell < t$, let O_1 denote the $b^t \times (\ell + 1)$ submatrix of O, comprised of the $\ell + 1$ columns indexed by 0, j_1, …, j_ℓ. Note that $\ell + 1 \le t$. Let $K, s_{j_1}, \ldots, s_{j_\ell} \in \mathbf{B}$. According to Lemma 3, O_1 contains the row vector $(K, s_{j_1} \ldots, s_{j_\ell})$ precisely $b^{t-\ell-1}$ times, where $b^{t-\ell-1}$ is independent to the choice of K. This proves (d'). Thus O is a defining matrix of a perfect (t, n)-threshold scheme. Finally, due to Corollary 2, we conclude that $\mathbf{K} = \mathbf{S} = \mathbf{B}$. Hence the scheme is ideal. □

6 Properties of Threshold Schemes from Orthogonal Arrays

The *Hamming distance* of two vectors $\mu = (a_1, \ldots, a_n)$ and $\nu = (b_1, \ldots, b_n)$, denoted by $dist(\mu, \nu)$, is the value of $\#\{j \mid a_j \ne b_j,\ 1 \le j \le n\}$.

Lemma 6. *Any two distinct row vectors of an orthogonal array (b^t, n, b, t) have a Hamming distance at least $n - t + 1$.*

Proof. Denote the orthogonal array by O. We prove the lemma by contradiction. Assume that there exist two rows of O, row L_i and L_j of O, satisfying $dist(L_i, L_j) \le n-t$. Then L_i and L_j have at least t same corresponding coordinations. This contradicts the fact that the submatrix, comprised of any t columns, contains a row vector precisely once as O is an orthogonal array (b^t, n, b, t) with index $\lambda = 1$. Therefore we have proved the lemma. □

Consider (t, n)-threshold secret sharing whose defining matrix O is an orthogonal array $(b^t, n+1, b, t)$. Assume that the dealer chooses an i_0 row vector

$(s_1, \dots, s_n)$ of O and assigns $s_1, \dots, s_n$ to participants $P_1, \dots, P_n$, respectively. Let $\{P_{j_1}, \dots, P_{j_\ell}\}$ for $t \leq \ell \leq n$ be a subset of active participants. Let O_1 be the $b^t \times \ell$ submatrix of O, containing ℓ columns indexed by $j_1, \dots, j_\ell$. According to Lemma 4, O_1 is an orthogonal array (b^t, ℓ, b, t). Denote the ith row of O_1 by L_i. According to Lemma 6, any two distinct row vectors L_i and L_j of O_1 satisfy

$$dist(L_i, L_j) \geq \ell - t + 1 \tag{2}$$

Clearly, the row i_0 of O_1 is $L_{i_0} = (s_{j_1}, \dots, s_{j_\ell})$. Let there exist u cheaters, among the active participants $P_{j_1}, \dots, P_{j_\ell}$, who submit modified shares to the combiner while the honest active participants submit correct shares to the combiner. Assume that the combiner receives the shares $s'_{j_1}, \dots, s'_{j_\ell}$ sent by $P_{j_1}, \dots, P_{j_\ell}$, where $s'_{j_i} = s_{j_i}$ if and only if P_{j_i} is honest. Write $L' = (s'_{j_1}, \dots, s'_{j_\ell})$. Clearly, $dist(L', L_{i_0}) = u$.

We show that cheating can be checked when $1 \leq u \leq \ell - t$. We assume that the combiner (recovery algorithm) knows the defining matrix O and then O_1. Thus the combiner can calculate

$$d_m = \min\{dist(L', L_i) \mid 1 \leq i \leq b^t\}$$

Since $dist(L', L_{i_0}) = u$ and $1 \leq u \leq \ell - t$, it follows that $1 \leq d_m \leq \ell - t$. Although the combiner does not know L_{i_0}, from $1 \leq d_m \leq \ell - t$ and (2), he can conclude that $L' = (s'_{j_1}, \dots, s'_{j_\ell})$ is not a row of O_1 and thus it is incorrect.

Furthermore we indicate that the correct shares can be found and the cheaters can be identified when $1 \leq u \leq \lfloor \frac{1}{2}(\ell - t) \rfloor$, where $\lfloor \frac{1}{2}(\ell - t) \rfloor$ denotes the greatest integer not larger than $\frac{1}{2}(\ell - t)$. The combiner can find a row L_{i_1} of O_1 such that $dist(L', L_{i_1}) = d_m$. Then L_{i_1} is identical with $L_{i_0} = (s_{j_1}, \dots, s_{j_\ell})$. In fact $dist(L_{i_1}, L_{i_0}) \leq dist(L_{i_1}, L') + dist(L', L_{i_0}) \leq 2u \leq \ell - t$. Since both L_{i_0} and L_i are rows of O_1, due to (2), we conclude that L_{i_1} is identical with $L_{i_0} = (s_{j_1}, \dots, s_{j_\ell})$. Thus the correct shares have been found. Comparing L' and L_{i_0}, the combiner (recovery algorithm) can determine who are cheaters.

The above discussions uses basic facts of coding theory. The reader interested in more details is referred to any book on the subject.

7 Simple Construction

According to Theorem 1, the design of threshold schemes is equivalent to the construction of corresponding orthogonal arrays. In this section, we are interested in orthogonal arrays with elements in a finite field, or simply, orthogonal arrays *over* a finite field. Let $q = p^v$ where p is a prime number and v is a positive integer. We write $GF(q)$ or $GF(p^v)$ to denote the finite field of $q = p^v$ elements, and $GF(q)^n$ or $GF(p^v)^n$ to denote the vector space of n tuples of elements from $GF(q)$. Each vector $\alpha \in GF(q)^n$ can be expressed as $\alpha = (a_1, \dots, a_n)$ where $a_1, \dots, a_n \in GF(q)$. The integer $a_1 q^{n-1} + \dots + a_{n-1} q + a_n$ is called the *integer representation* of vector $\alpha = (a_1, \dots, a_n)$, where each a_j and the sum are regarded real-valued. Thus we can index all vectors in $GF(q)^n$:

$$\alpha_0, \alpha_1, \dots, \alpha_{q^n - 1}$$

where j is the integer representation of α_j. A *function* f on $GF(q)^n$ is a mapping from $GF(q)^n$ to $GF(q)$. The function f can be expressed as $f(x)$ or $f(x_1, \ldots, x_n)$, where $x = (x_1, \ldots, x_n) \in GF(q)^n$. The *truth table* of f is the sequence $f(\alpha_0), f(\alpha_1)$, $\ldots$, $f(\alpha_{q^n-1})$. If each element of $GF(q) = GF(p^v)$ appears in the truth table of f precisely q^{n-1} times then f is called *balanced.* If f can be expressed as $f(x_1, \ldots, x_n) = c + a_1x_1 + \cdots + a_nx_n$ then f is called an *affine function.* In particular, the affine function f is called *linear* if $c = 0$. It is easy to see that non-constant affine functions are balanced.

For any integer t, n and prime power q with $1 \leq t \leq n+1 \leq q-1$, we next construct an orthogonal array $(q^t, n+1, q, t)$ over $GF(q)$. Since $n+1 \leq q-1$, we can collect $n+1$ nonzero elements of $GF(q)$: $\lambda_1, \ldots, \lambda_{n+1}$. For each λ_j, $1 \leq j \leq n+1$, define a vector $\beta_j = (1, \lambda_j, \ldots, \lambda_j^{t-1})$, $j = 1, \ldots, n+1$, and a liner function ψ_j on $GF(q)^t$ such that $\psi_j(x) = \langle \beta_j, x \rangle$ where $x = (x_1, \ldots, x_t) \in GF(q)^t$ and $\langle , \rangle$ denotes the inner product of two vectors. We now construct a $q^t \times (n+1)$ matrix O. We index the columns of O by $j = 0, 1. \ldots, n$, and define the j column vector of O to be the truth table of ψ_{j+1} where $j = 0, 1, \ldots, n$. According to the results given in [4], O is an orthogonal array $(q^t, n+1, q, t)$ over $GF(q)$. Therefore, by Theorem 1, O is a defining matrix of an ideal (t, n)-threshold scheme.

The above orthogonal arrays have a property as follows.

Lemma 7. *Let O be the orthogonal array $(q^t, n+1, q, t)$ over $GF(q)$, constructed previously in this section. Then for any fixed $1 \leq j_1 < \cdots < j_t \leq n$, $\chi_{j_1,\ldots,j_t}$ is a linear function.*

Proof. It is not hard to verify that any t vectors $\beta_{j_1}, \ldots, \beta_{j_t}$, where each β_j has been defined previously in this section, are linearly independent. Thus $\{\beta_{j_1}, \ldots$ $, \beta_{j_t}\}$ is a basis of $GF(q)^t$ and thus the 0th column is a linear combination of the j_1th, $\ldots$, the j_tth columns. If we denote the jth columns of O by η_j, then $\eta_0 = c_1\eta_{j_1} + \cdots + c_t\eta_{j_t}$ where each $c_j \in GF(q)$. Thus $O(i, 0) = c_1O(i, j_1) + \cdots + c_t0(i, j_t)$, $i = 1, \ldots, q^t$. By definition, $\chi_{j_1,\ldots,j_t}(s_1, \ldots, s_t) = c_1s_1 + \cdots + c_ts_t$, for any $s_1, \ldots, s_t \in GF(q)$. This proves the lemma. □

Using the same approach as shown by Tompa and Woll [7] for Shamir's scheme [6], due to Lemma 7, we can demonstrate that the Tompa-Woll attack works also for the scheme constructed above. For this reason, we will improve this construction in the next section.

8 Ideal Threshold Schemes with Nonlinear Secret Functions

We address the weakness discussed in the previous section by removing linearity from the orthogonal array $(q^t, n+1, q, t)$. Being more specific, we make sure that the 0th column (secret) is described by a nonlinear function of other columns (shares).

Theorem 2. *Let O be the orthogonal array $(q^t, n+1, q, t)$ over $GF(q)$, constructed in Section 7. We replace the 0th column by the truth table of function $\sigma(x) = \langle \beta_1, x\rangle^p$, where p is the characteristic of $GF(q)$, i.e., $q = p^v$. Denote the resulting matrix by O'. Then O' is also an orthogonal array $(q^t, n+1, q, t)$. Alternatively, we obtain an ideal (t, n)-threshold scheme with the defining matrix O'.*

Proof. Let O'_1 (O_1) be a $q^t \times t$ submatrix of O' (O), consisting of any t columns of O' (O), indexed by $j_1, \dots, j_t$, where $0 \le j_1 < \cdots < j_t \le n$. Let $(a_1, a_2, \dots, a_t)$ be a t-dimensional vector where each $a_j \in GF(q)$. There two cases to be considered: $j_1 \neq 0$ and $j_1 = 0$. For the first case: $j_1 \neq 0$, clearly $O'_1 = O_1$ is a submatrix of O. Thus $O'_1 = O_1$ contains $(a_1, a_2, \dots, a_t)$ as a row vector precisely once. We next consider the second case: $j_1 = 0$. It is easy to verify that $c_1 = c_2$, where $c_1, c_2 \in GF(q)$, if and only if $c_1^p = c_2^p$. Thus, there exists an unique element $c \in GF(q)$ such that $c^p = a_1$. Recall that O is an orthogonal array $(q^t, n+1, q, t)$ with index $\lambda = 1$. Thus O_1 contains the row vector $(c, a_2, \dots, a_t)$ precisely once. It follows that O'_1 contains the row vector $(a_1, a_2, \dots, a_t)$ precisely once. Summarising the two cases, we have proved that O' is also an orthogonal array $(q^t, n+1, q, t)$. According to Theorem 1, we obtain an ideal (t, n)-threshold scheme with the defining matrix O'. □

Theorem 3. *Let O' be the orthogonal array $(q^t, n+1, q, t)$ in Theorem 2. For any $1 \le j_1 < \cdots < j_t \le n$, $\chi_{j_1,\dots,j_t}$ is a nonlinear function.*

Proof. Recall that for each j with $1 \le j \le n$, the jth column of O' is the truth table of a linear function on $GF(q)^t$. On the other hand, the 0th column of O' is the truth table of the function $\sigma(x) = \langle \beta_1, x\rangle^p$, that contains nonlinear terms. Thus the 0th column of O' is not a linear combination of other columns. This proves that $\chi_{j_1,\dots,j_t}$ is a nonlinear function. □

9 Constructions of Ideal Threshold Schemes

The construction in Section 7 demonstrates the existence of secret sharing based on orthogonal arrays. In this section, we show how to construct secret sharing from a known orthogonal array.

Theorem 4. *Let O be the orthogonal array (m, n, b, t) with elements from a b-set $\mathbf{B}$. For a permutation π on $\mathbf{B}$ and a uth column of O, we replace each entry c in the uth column by $\pi(c)$. Denote the resulting matrix by O'. Then O' is also an orthogonal array (m, n, b, t). Alternatively, we obtain an ideal threshold scheme based on the defining matrix O'.*

Proof. The proof is similar to the proof of Theorem 2. Let O'_1 (O_1) be an $m \times t$ submatrix of O' (O), consisting of the t columns of O' (O), indexed by $j_1, \dots, j_t$, where $1 \le j_1 < \cdots < j_t \le n$. Let $(a_1, a_2, \dots, a_t)$ be a t-dimensional vector where each $a_j \in GF(q)$. There two cases to be considered: $u \notin \{j_1, \dots, j_t\}$ and

$u \in \{j_1, \dots, j_t\}$. For the first case: $u \notin \{j_1, \dots, j_t\}$, clearly $O'_1 = O_1$ is a submatrix of O. Thus $O'_1 = O_1$ contains $(a_1, a_2, \dots, a_t)$ as a row vector precisely once. We next consider the second case: $u \in \{j_1, \dots, j_t\}$. Let $u = j_r$ and then assume that $j_1 < \cdots < j_{r-1} < j_r < j_{r+1} < \cdots < j_t$. Since π is a permutation on $\mathbf{B}$, there exists an unique element $c \in \mathbf{B}$ such that $\pi(c) = a_{j_r}$. Recall that O is an orthogonal array (m, n, b, t) with index $\lambda = 1$. Thus, O_1 contains the row vector $(a_1, \dots, a_{j_{r-1}}, c, a_{j_{r+1}}, \dots, a_t)$ precisely once. It follows that O'_1 contains the row vector $(a_1, \dots, a_{j_{r-1}}, a_{j_r}, a_{j_{r+1}}, \dots, a_t)$ precisely once. Summarising the two cases, we have proved that O' is also an orthogonal array (m, n, b, t). Alternatively, we obtain an ideal threshold scheme with the defining matrix O'. □

Repeatedly applying Theorem 4, we obtain more orthogonal arrays and more ideal threshold schemes. Moreover, the theorem gives ideal threshold schemes with different properties.

Theorem 5. *Let O be the orthogonal array $(q^t, n+1, q, t)$ over $GF(q)$, constructed in Section 7. Let a permutation π on $GF(q)$ satisfy $\pi(0) \neq 0$. For a uth $(1 \leq u \leq n)$ column of O, we replace each entry c in the uth column by $\pi(c)$, and replace the 0th column by the truth table of function $\sigma(x) = \langle \beta_1, x \rangle^p$, where $q = p^v$. Denote the resulting matrix by O'. Then*

(i) O' is also an orthogonal array (q^t, n, q, t). Alternatively, we obtain an ideal threshold scheme with the defining matrix O',

(ii) all the row vectors of the orthogonal array O' do not form a linear subspace of $GF(q)^n$,

(iii) for any $1 \leq j_1 < \cdots < j_t \leq n$, $\chi_{j_1, \dots, j_t}$ is a nonlinear function.

Proof. According to Theorems 2 and 4, (i) is true. We denote the jth column of O (O') by η_j (η'_j). From the construction of O mentioned in Section 7, $O(0, u) = 0$. Thus $O'(0, u) = \pi(0) \neq 0$. This means that η'_u is not the true table of a linear function. We have proved (ii). We next prove (iii). There exist two cases to be considered: $u \notin \{j_1, \dots, j_t\}$ and $u \in \{j_1, \dots, j_t\}$. In the first case: $u \notin \{j_1, \dots, j_t\}$. According to the same arguments as in the proof of Theorem 3, (iii) is true in the first case. We consider the second case: $u \in \{j_1, \dots, j_t\}$. Let $u = j_r$. We prove (iii) by contradiction. Assume that $\chi_{j_1, \dots, j_t}$ is a linear function. By definition,

$$\eta'_0 = c_1 \eta'_{j_1} + \cdots + c_{r-1} \eta'_{j_{r-1}} + c_r \eta'_{j_r} + c_{r+1} \eta'_{j_{r+1}} + \cdots + c_t \eta'_{j_t}$$

for some $c_1, \dots, c_t \in GF(q)$. Since $\eta'_j = \eta_j$ for $j \neq 0, j_r$, we have

$$\eta'_0 = c_1 \eta_{j_1} + \cdots + c_{r-1} \eta_{j_{r-1}} + c_r \eta'_r + c_{r+1} \eta_{j_{r+1}} + \cdots + c_t \eta_{j_t} \tag{3}$$

From the proof of Theorem 3, we know that η'_0 is not a linear combination of η_{j_1}, …, $\eta_{j_{r-1}}$, $\eta_{j_{r+1}}$, …, η_{j_t}. Thus we conclude that $c_r \neq 0$. On the other hand, $O'(0, 0) = 0$, $O(0, j_1) = 0$, …, $O(0, j_{r-1}) = 0$, $O(0, j_{r+1}) = 0$, …, $O(0, j_t) = 0$ but $O'(0, j_r) \neq 0$. This means that (3) does not hold. The contradiction proves (iii) in the second case. □

It is easy to see that all row vectors of the orthogonal array $(q^t, n+1, q, t)$, constructed in Section 7, form a linear subspace. Usually, this is not a desirable property from a security point of view as the corresponding secret sharing may be subject to the Tompa-Woll attack. In contrast to the construction in Section 7, the construction in Theorem 5 provides secret sharing that is resistant against cheating.

10 Conclusions

In this work we have applied orthogonal arrays to construct threshold schemes and have shown that all these schemes are not only perfect but also ideal. We have indicated that such ideal threshold schemes have an ability to detect cheating and also, can identify cheaters and recover correct shares. Besides cheating detection and identification, we have also shown that the secret functions must be nonlinear to prevent cheating using the Tompa-Woll attack.

11 Acknowledgement

The work was in part supported by Australian Research Council grant A00103078.

References

1. G. R. Blakley. Safeguarding cryptographic keys. In *Proc. AFIPS 1979 National Computer Conference*, pages 313–317. AFIPS, 1979.
2. E. F. Brickell and D. M. Davenport. On the Classification of Ideal Secret Sharing Schemes. J. Cryptology, 4: 123 - 134, 1991.
3. E. F. Brickell and D.R. Stinson. Some Improved Bounds on Information Rate of Perfect Sharing Schemes J. Cryptology, 5: 153 - 166, 1992.
4. K. A. Bush. Orthogonal arrays of index unity. In *Annals of Mathematical Statistics.* 23, 426-434.
5. M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. In *Proceedings IEEE Globecom '87*, pages 99–102. IEEE, 1987.
6. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, November 1979.
7. M. Tompa and H. Woll. How to share a secret with cheaters. *Journal of Cryptology*, 1(2):133–138, 1988.