On Zigzag Functions and Related Objects in New Metric

An Braeken[1], Ventzislav Nikov[2], and Svetla Nikova[1]

[1] ESAT/SCD/COSIC, Katholieke Universiteit Leuven,
Kasteelpark Arenberg 10, B-3001 Leuven, Belgium
an.braeken,svetla.nikova@esat.kuleuven.ac.be
[2] vnikov@mail.com

Key words: Cryptography, Zigzag functions, Quorum systems, Orthogonal array Self-intersecting codes.

1 Introduction

For any two binary vectors $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_2^n$, define the sets $\delta(x, y) = \{i : x_i \neq y_i\}$ and $\sup(x) = \{i : x_i \neq 0\}$. Denote the size of a set A with $|A|$. Then the Hamming distance between the binary vectors x and y is equal to $d(x, y) = |\delta(x, y)|$ and the Hamming weight of x is $wt(x) = |\sup(x)|$. Instead of using the Hamming distance $d(x, y)$ and norm $wt(x)$, we will work with the metric defined by $\delta(x, y)$ and the corresponding norm $\sup(x)$. In this way, many definitions and properties will be expressed by sets instead of numbers, which in fact corresponds to the cardinality of certain sets. For this purpose monotone increasing and monotone decreasing sets are considered. Consequently, this leads to a better description of the properties. This approach has already been applied in [?] to codes (e.g. minimum distance, generator and parity-check matrix, minimal codeword, etc.) and in [?] to Boolean functions (e.g. resilient, with propagation characteristics, etc.).
In this paper we will investigate the properties of zigzag functions. The zigzag functions, introduced in [?] and used for efficient oblivious transfer in [?] were later generalized to s-zigzag functions for $2 \leq s \leq n$ in [?]. Zigzag functions are related to self-intersecting codes and orthogonal arrays as it is shown in [?] and [?]. We generalize the notion of zigzag functions and prove a connection with a subclass of Δ-resilient functions, introduced in [?]. This new definition results in a better understanding of the properties of zigzag functions and provides a better insight in the space defined by the new metric.

2 Background

Define the set $\mathcal{P}_n = \{1, \ldots, n\}$ and denote the power set of $\mathcal{P}_n$ by $P(\mathcal{P}_n)$. Call the set which contains all $\binom{n}{k}$ subsets of weight k from $\mathcal{P}_n$ by $\mathcal{P}_{k,n}$ for $1 \leq k \leq n$. Recall that the Hamming distance between the binary vectors x and y is equal to $d(x, y) = |\delta(x, y)|$ and the Hamming

weight of x is $\mathrm{wt}(x) = |\sup(x)|$. It was noted in [?] that $\delta(x, y)$ has similar properties as a metric and $\sup(x)$ has similar properties as a norm. Notice that $\sup(x)$ and $\delta(x, y) = \sup(x - y)$ are subsets of $\mathcal{P}_n$ and that $\mathcal{P}_n$ is partially ordered (i.e., $x \preceq y$ if and only if $\sup(x) \subseteq \sup(y)$).
In order to work in the metric defined by $\delta(x, y)$ and the corresponding norm $\sup(x)$, we will use the notion access structure (Γ, Δ), or shortly denoted by Γ. The set Γ ($\Gamma \subseteq P(\mathcal{P}_n)$) is monotone increasing and the set Δ ($\Delta \subseteq P(\mathcal{P}_n)$) is monotone decreasing. A monotone increasing set Γ can be described efficiently by the set Γ^- consisting of the minimal elements (sets) in Γ, i.e., the elements in Γ for which no proper subset is also in Γ. Similarly, the set Δ^+ consists of the maximal elements (sets) in Δ, i.e., the elements in Δ for which no proper superset is also in Δ. We set $\Gamma = \Delta^c$ ($\Delta^c = P(\mathcal{P}_n) \setminus \Delta$). Note that Γ is monotone increasing if and only if Δ is monotone decreasing.
The dual sets $\Delta^\perp$ and $\Gamma^\perp$ to Γ and Δ, respectively, are defined by $\Gamma^\perp = \{A : A^c \in \Delta\}$ and $\Delta^\perp = \{A : A^c \in \Gamma\}$. It is easy to see that $\Delta^\perp$ is monotone decreasing and $\Gamma^\perp$ is monotone increasing. For two monotone decreasing sets Δ_1 and Δ_2 define $\Delta_1 \uplus \Delta_2 = \{A = A_1 \cup A_2; A_1 \in \Delta_1, A_2 \in \Delta_2\}$. Note that $\Delta_1 \uplus \Delta_2$ is again a monotone decreasing set. We refer to the case $\Delta = \{A : |A| \leq t\}$ as a threshold case.

Definition 1. *[?] A monotone decreasing set Δ is called $\mathcal{Q}^2$ if for all sets $A, B \in \Delta \Rightarrow A \cup B \subsetneq P$. More general, Δ is called $\mathcal{Q}^s$ if the union of every s sets do not cover the whole set. A monotone increasing set Γ is called $\mathcal{Q}^s$ if and only if $\Delta = \Gamma^c$ is $\mathcal{Q}^s$ for $2 \leq s \leq n$.*

The property $\mathcal{Q}^2$ could be rephrased as follows: there exists no set A in Δ whose complement also belongs to Δ. For $\mathcal{Q}^2$ systems, the following relation is easy to derive.

Theorem 1. *$\Delta^\perp$ is $\mathcal{Q}^2$ if and only if $\Delta^\perp \subseteq \Delta$ (and thus if and only if $\Gamma \subseteq \Gamma^\perp$).*

Let Γ and Γ' be access structures on $\mathcal{P}_n$. It is said that Γ' *dominates* Γ if and only if $\Gamma' \subseteq \Gamma$.

Definition 2. *A monotone decreasing set Δ is said to be self-dual if $\Delta^\perp = \Delta$. Analogously, a monotone increasing set is called self-dual if $\Gamma = \Gamma^\perp$.*

A $\mathcal{Q}^2$ access structure Γ is called *minimal* $\mathcal{Q}^2$ if for every access structure Γ' which dominates Γ, it follows that Γ' is not $\mathcal{Q}^2$. A $\mathcal{Q}^2$ monotone structure Δ is called *maximal* $\mathcal{Q}^2$ if $\Gamma = \Delta^c$ is a minimal $\mathcal{Q}^2$ access structure. It is easy to derive the following lemma.

Lemma 1. *An access structure Γ is minimal $\mathcal{Q}^2$ if and only if Γ is self-dual.*

3 Zigzag functions

We start with a generalization of the definition of vector resilient functions introduced in [?,?]. After proving that zigzag functions are a special type of vector resilient functions, we derive some bounds on the parameters of the zigzag functions. This is followed by two constructions of zigzag functions. Finally, relations with orthogonal arrays, intersecting codes and quorum systems are pointed out.

3.1 Definition

Definition 3. *Let f be a vector function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$. The function f is said to be resilient or unbiased with respect to the subset $T = \{i_1, \ldots, i_t\} \subseteq \mathcal{P}_n$ if for any $(a_1, \ldots, a_t) \in \mathbb{F}_2^t$ and $\beta \in \mathbb{F}_2^k$ holds that*

$$|\{x | x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n, x_{j_1} = a_1, \ldots, x_{j_n} = a_t, f(x) = \beta\}| = 2^{n-t-k}.$$

If f is resilient with respect to all sets of weight less or equal than t, then f is said to be an (n, k, t)-resilient function. An $(n, k, 0)$-resilient function is called balanced vector function.

The definition of (n, k, t)-resilient functions can be easily generalized to the definition of (n, k, Δ)-resilient functions, following the approach of [**?**].

Definition 4. *A vector function f from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$ is called (n, k, Δ)-resilient if f is resilient for all sets $A \in \Delta$.*

When $\Delta = \{A : |A| \leq t\}$ the definitions of Δ-resilient and t-resilient function coincide.

Definition 5. *[?] A function f from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$ is called* zigzag *if for all sets $A \subseteq \mathcal{P}_n$ the function f is resilient with respect to at least one of the sets $A \subseteq \mathcal{P}_n$ or $A^c = \mathcal{P}_n \setminus A$.*

3.2 Bounds on zigzag functions

A well known *trivial bound* for existence of (n, k, t)-resilient functions is $t \leq n - k$ [**?**,**?**]. Constructions of (n, k, t)-resilient functions can be found in [**?**]. We will prove that zigzag functions are a special type of vector resilient functions.

Theorem 2. *A function f is zigzag function if and only if f is an (n, k, Δ)-resilient function, for which $\Gamma^\perp$ is a $\mathcal{Q}^2$ structure.*

Proof. Consider a (n, k, Δ)-resilient function f. Then for any subset A we have either $A \in \Delta$ or $A \in \Gamma$. If $A \in \Delta$ then, by the definition of (n, k, Δ)-resilient function, f is resilient with respect to A. In the second case if $A \notin \Delta$ (i.e. $A \in \Gamma$) then by definition (of dual access structure) $A^c \in \Delta^\perp$. So, in order to have $A^c \in \Delta$ we need to require that $\Delta^\perp \subseteq \Delta$. But the relation $\Delta^\perp \subseteq \Delta$ is equivalent to $\Gamma \subseteq \Gamma^\perp$, which is equivalent $\Gamma^\perp$ to be $\mathcal{Q}^2$. On the other hand, a Δ-resilient function, such that $\Gamma^\perp$ is a $\mathcal{Q}^2$ structure, satisfies the zigzag property, as for all $A \subseteq \mathcal{P}_n$ either A or A^c belongs to Δ. $\square$

Remark 1. If f is resilient with respect to either A or A^c for all $A \subseteq \mathcal{P}$, but not to both, then f is a (n, k, Δ)-resilient function with Δ self-dual, because of the additional property $\Gamma^\perp \cap \Delta = \emptyset$ and thus $\Delta \subseteq \Delta^\perp$ should hold.

Thus for (n, k, Δ)-resilient function the trivial bound for existence can be restated as follows: $\Delta \subseteq P(\mathcal{P}_{n-k,n})$ or equivalently for any $A \in \Delta$ we have $|A| \leq n-k$. (see [?, Lemma 3.1]) Applying Theorem ?? to the threshold case, i.e. for (n, k, t)-resilient functions we get that $n - t - 1 \leq t$ (since $\Delta^\perp \subseteq \Delta$), hence $n \leq 2t + 1$. Now combining this fact with the trivial bound we get $\lceil \frac{n-1}{2} \rceil \leq t \leq n - k$, hence $n \geq 2k - 1$ which is [?, Lemma 3.2]. Therefore it follows that $t \geq k - 1$ (see [?, Theorem 3.3]). These results can be generalized as follows:

Theorem 3. *Let f be a zigzag function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$ then the following properties hold for the corresponding (n, k, Δ)-resilient function:*
(i) $\Delta^\perp \subseteq \Delta \subseteq P(\mathcal{P}_{n-k,n})$; *(ii)* $P(\mathcal{P}_{k-1,n}) \subseteq \Delta$; *(iii)* $2k - 1 \leq n$.

Proof. The first property follows from Theorem ?? and the existence property of resilient vector functions. For the second property, consider an element A of weight less or equal than $k - 1$. Let $A \notin \Delta$ (i.e. $A^c \in \Gamma$). Then $|A^c| \geq n - k + 1$ and thus $A^c \in \Gamma$ because of the first property. This is in contradiction with the definition of zigzag functions, since both A and A^c are in Γ. The condition on the dimension of the zigzag function is obtained by combining property (i) and (ii): $P(\mathcal{P}_{k-1,n}) \subseteq P(\mathcal{P}_{n-k,n})$ and hence $k - 1 \leq n - k$. □

3.3 Constructions

It is clear from the definition that any linear combination of the components of a $(\Delta-)$ resilient function is a $(\Delta-)$ resilient Boolean function. Some constructions of resilient Boolean functions can be immediately generalized for vector functions, which in their turn can be used in order to derive constructions for zigzag functions, as previously done in [?]. The connection between zigzag functions and (n, k, Δ)-resilient functions naturally leads to constructions of new zigzag functions from old.

Theorem 4. *[?] Let f be a zigzag function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ and g be a balanced vector function from $\mathbb{F}_2^m$ into $\mathbb{F}_2^k$, then $g \circ f$ is a zigzag function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$.*

Proof. The theorem follows immediately from the fact that $(\Delta$-) resiliency is kept invariant after applying a balanced transformation on the output. See also [?, Theorem 16]. □

Theorem 5. *[?] Let $f_1 : \mathbb{F}_2^{n_1} \to \mathbb{F}_2^k$ and $f_2 : \mathbb{F}_2^{n_2} \to \mathbb{F}_2^k$. Then the function $f : \mathbb{F}_2^{n_1+n_2} \to \mathbb{F}_2^k :$ $(x, y) \mapsto f(x, y) = f_1(x) + f_2(y)$ is a zigzag function if and only if at least one of the two functions f_1 or f_2 are zigzag functions.*

Proof. Let f_1 be a zigzag function, which implies that f_1 is (n, k, Δ_1)-resilient with $\Gamma_1 \subseteq \Gamma_1^\perp$ and let f_2 be just an (n, k, Δ_2)-resilient function. Then as proven in [**?**], f is an $(n, k, \Delta = \Delta_1 \uplus \Delta_2 \uplus S)$-resilient function where $S = \{\emptyset, \{1\}, \cdots, \{n_1\}, \{n_1+1\}, \cdots, \{n_2+n_1\}\}$. Moreover, it holds that $\Gamma \subseteq \Gamma^\perp$, or f is a zigzag function. □

Remark 2. The previous theorem also holds for the direct sum of an arbitrary number r with $r \geq 2$ functions. If at least one of these r functions are zigzag, the direct sum is also a zigzag function.

3.4 Relation with Orthogonal arrays

For the threshold case, the connection between zigzag functions, resilient functions and large set of orthogonal arrays was derived in [**?**, Theorem 3.5],[**?**, Theorem 5.1], and [**?**, Theorem 5.2]. We now generalize these results in the new metric. Let us first generalize the concepts of orthogonal array and large set of orthogonal arrays.

Definition 6. *An* orthogonal array*, denoted by $OA(M, n, q, \Delta)$, is an $M \times n$ matrix V with entries from a set of q elements, strength Δ which is a decreasing monotone set and index μ. Any set $A \in \Delta^+$ of columns of V contains all $q^{|A|}$ possible row vectors exactly $\mu = Mq^{-|A|}$ times. A* large set of orthogonal arrays *$OA(M, n, q, \Delta)$, denoted by $LOA(M, n, q, \Delta)$ is a set of q^n/M simple $OA(M, n, q, \Delta)$ such that every n-tuple occurs as a row in exactly one of the orthogonal arrays in the set.*

Note that for $\Delta = \{A : |A| \leq t\}$, these definitions coincide with the definitions of $OA(M, n, q, t)$ and $LOA(M, n, q, t)$. From property (ii) of Theorem **??**, we immediately derive:

Corollary 1. *If there exists a zigzag function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$ with $k \geq 2$, which corresponds to a Δ-resilient function, then there exists a $LOA(2^{n-k}, n, 2, \Delta)$ and hence also an $OA(2^{n-k}, n, 2, \Delta)$ exists.*

In the case of zigzag function with respect to self-dual access structure Δ, we get the following equivalence relation:

Theorem 6. *A zigzag function f from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$ with $k \geq 2$, which corresponds to a Δ-resilient function, where Δ is self-dual, exists if and only if there exists a $LOA(2^{n-k}, n, 2, \Delta)$ and thus an $OA(2^{n-k}, n, 2, \Delta)$.*

Proof. The derivation of the existence of a LOA from a zigzag function follows immediately from Corollary **??**. Conversely, consider a $LOA(2^{n-k}, n, 2, \Delta)$. Analogously as in the proof of [**?**, Theorem 2.1], define the sets $A_y = A_{(y_1,\ldots,y_k)}$ which contain the elements of the 2^k orthogonal arrays in the large set for all $y \in \mathbb{F}_2^k$. Then the function defined by $f(x_1, \ldots, x_n) = (y_1, \ldots, y_k) \Leftrightarrow (x_1, \ldots, x_n) \in A_{(y_1,\ldots,y_k)}$ represents a zigzag function since $\Delta = \Delta^\perp$. □

4 Relation with Intersecting Codes and Quorum system

In [?], the connections with linear zigzag functions and self-intersecting codes were considered. A *self-intersecting code* [?] is a code for which $sup(x) \cap \sup(y) \neq 0$ for all nonzero codewords x, y. On the other hand (weakly) self-dual codes are defined as follows. Code $\mathcal{C}$ is called *weakly self-dual* if $\mathcal{C} \subsetneqq \mathcal{C}^{\perp}$, a code $\mathcal{C}$ is called *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp}$. It is easy to see that for a weakly self-dual code $\mathcal{C}$ there exists a non-invertible matrix W such that $WH = G$, where G and H are the generator and parity check matrices of the code, while for self-dual code $\mathcal{C}$ one has $H = G$. For a code $\mathcal{C}$ the *set of possible (allowed) distances* is defined in [?] by $\Gamma(\mathcal{C}) = \{A :$ there exist x, y in $\mathcal{C},\ x \neq y$ such that $\delta(x, y) \subseteq A\}$ and the *set of forbidden distances* is defined by $\Delta(\mathcal{C}) = \Gamma(\mathcal{C})^c$. It is easy to see that $\Delta(\mathcal{C})$ is monotone decreasing and that $\Gamma(\mathcal{C})$ is monotone increasing. If $\Delta(\mathcal{C}) = \{A : |A| < d\}$ then $\mathcal{C}$ is an $[n, k, d]$ code.

Theorem 7. *[?] The function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^k$ defined by $f(x) = xM^T$ is a linear zigzag function if and only if M is the generator matrix of an $[n, k, d]$ self-intersecting code $\mathcal{C}$.*

In [?] the authors show that any weakly self-dual code corresponds to an access structure with $\mathcal{Q}^2$ property, while any self-dual code corresponds to an access structure which satisfies the minimal $\mathcal{Q}^2$-property. However, it is still an open problem whether the inverse also holds, i.e. whether to any $\mathcal{Q}^2$ or minimal $\mathcal{Q}^2$ access structure corresponds a weakly self-dual code or self-dual code respectively. Since there exists a relation between the monotone span programs of access structures and the generator matrices of the corresponding codes, this property could be used to derive new constructions of zigzag functions.

Quorum set system and quorum access structures have been used in the study of problems related to mutual exclusion [?], data selective dissemination of information [?], distributed access control, digital signatures [?], multi party computation [?], etc.

Definition 7. *[?] A* set system *$\mathbb{Q}$ is a collection of subsets $Q_i \subseteq \mathcal{P}_n$. A* quorum system *is a set system $\mathbb{Q}$ that has the* intersection property*: $Q_i \cap Q_j \neq \emptyset$ for all $Q_i, Q_j \in \mathbb{Q}$. The sets of the system are called* quorums.

Definition 8. *[?] Let $\mathbb{Q}$ be a quorum system. Let $\Gamma(\mathbb{Q}) = \{A : Q \subseteq A, Q \in \mathbb{Q}\}$ be the collection of sets containing some quorum, and let $\Delta(\mathbb{Q}) = \{B : B^c \in \Gamma(\mathbb{Q})\}$ be the collection of sets whose complement contains a quorum. The* quorum access structure *of $\mathbb{Q}$ is the tuple $(\Gamma(\mathbb{Q}), \Delta(\mathbb{Q}))$.*

Consider for instance the tuple $(\Gamma^{\perp}, \Delta)$. Beaver and Wool [?] proved that in the passive case multi-party computation is unconditionally secure provided that the tuple $(\Gamma^{\perp}, \Delta)$ is a quorum access structure, where the quorum system is $\mathbb{Q} = (\Gamma^{\perp})^{-}$.

Lemma 2. *The tuple $(\Gamma^{\perp}, \Delta)$ is a quorum access structure if and only if Δ satisfies the $\mathcal{Q}^2$ property.*

Proof. The $\mathcal{Q}^2$ property for Δ by definition states that $\forall A, B \in \Delta : A \cup B \neq \mathcal{P}$, then $\forall A^c, B^c \in \Gamma^{\perp} : A^c \cap B^c = (A \cup B)^c \neq \emptyset$. So, the quorum system $(\Gamma^{\perp})^-$ is equivalent to Δ being $\mathcal{Q}^2$. $\square$

This result leads to the following equivalence.

Theorem 8. *The access structure $(\Gamma(\mathcal{C}), \Delta(\mathcal{C})^{\perp})$ is a quorum system if and only if $\mathcal{C}$ is an intersecting code.*

5 s-Zigzag Functions

In [?] the authors generalized the notion of zigzag function to s-zigzag function, as follows.

Definition 9. *[?] Call $A_1, \ldots, A_s \in \Lambda$ an s-partition of $\mathcal{P}$ in Λ if $A_1 \cup \cdots \cup A_s = \mathcal{P}_n$ and $A_i \cap A_j = \emptyset$ for all $1 \leq i < j \leq s$. A function f from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$ is called s-zigzag if f is resilient with respect to at least $s-1$ subsets of any s-partition. A function is called fully zigzag if it satisfies s-zigzag property for $2 \leq s \leq n$.*

Thus zigzag functions are by definition 2-zigzag functions. Now we will generalize Theorem **??** to the new setting.

Theorem 9. *A function f is an s-zigzag function if and only if it is an (n, k, Δ)-resilient function, such that $\Gamma^{\perp}$ is a $\mathcal{Q}^s$ structure.*

Proof. Consider an (n, k, Δ)-resilient function f such that $\Gamma^{\perp}$ is a $\mathcal{Q}^s$ structure. Let us take an s partition of $\mathcal{P}_n$. For A_1, there are two possibilities. First, if $A_1 \in \Gamma^{\perp}$, it follows that $A_2 \cup \cdots \cup A_s \in \Delta$ and thus f is resilient with respect to $s-1$ sets. In the second case, $A_1 \notin \Gamma^{\perp}$, which implies that $A_1 \in \Delta^{\perp}$ and we need to consider the rest of the sets $A_2, \ldots, A_s$. For the set A_2, we have the same two possibilities. If $A_2 \in \Gamma^{\perp}$, then $A_1 \cup A_3 \cup \cdots \cup A_s \in \Delta$. Otherwise we need to proceed in the same way. In the worst case (when $A_1, A_2, \cdots, A_{s-1} \in \Delta^{\perp}$ we arrive at A_s and again we have two possibilities. First, if $A_s \in \Gamma^{\perp}$, it follows that $A_1 \cup A_2 \cdots \cup A_{s-2} \cup A_s \in \Delta$ and thus f is resilient with respect to $s-1$ sets. Or in the second case $A_s \in \Delta^{\perp}$ so all $A_i \in \Delta^{\perp}$ and $A_1 \cup \cdots \cup A_s = \mathcal{P}_n$, which is in contradiction with the $\mathcal{Q}^s$ property of $\Delta^{\perp}$. $\square$

Corollary 2. *Every s-zigzag function f is also an s'-zigzag function for $s \leq s' \leq n$. Thus every (2-) zigzag function f is fully zigzag function.*

Similar as for 2-zigzag functions, an s-zigzag function f is resilient with respect to exactly $s-1$ elements from the partition if and only if the additional property $\Gamma^{\perp} \cap \Delta = \emptyset$ holds.

From the definition of $\mathcal{Q}^s$, it is clear that for all $2 \le s \le n$, a $\mathcal{Q}^s$ structure implies a $\mathcal{Q}^\ell$ structure with $\ell \le s$. Note that $\Gamma^\perp$ being $\mathcal{Q}^s$ structure implies for Δ (changing the monotonicity) that any s-zigzag function is also an ℓ-zigzag function with $s \le \ell \le n$. Thus fully zigzag functions are equivalent to zigzag functions.

Note that the construction from Section **??** can also be applied to the construction of s-zigzag functions for any $2 \le s \le n$. Next, in the similar way as in [**?**, Theorem 5] we derive the following statement.

Theorem 10. *If f from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$ is an s-zigzag function where n and s have different parity and $k > \lfloor \frac{n}{2} \rfloor + \lfloor \frac{s-2}{2} \rfloor$, then f is (n,k,Δ)-resilient where $\mathcal{P}_{\lfloor \frac{n-(s-2)}{2} \rfloor, n} \subseteq \Delta$.*

Proof. Suppose f is resilient with respect to the set I_s of size $\left\lfloor \frac{n-(s-2)}{2} \right\rfloor$. Consider the s-partition which contains the set I_s, $s-2$ subsets of size 1, and a subset I_e with $n-(s-2)-\left\lfloor \frac{n-(s-2)}{2} \right\rfloor = \left\lceil \frac{n-(s-2)}{2} \right\rceil$ elements. Note that this partition is the worst case we have to consider. By the trivial bound for the existence of resilient functions, we derive that the f cannot be resilient with respect to I_e if and only if $|I_e| = \left\lceil \frac{n-(s-2)}{2} \right\rceil \ge n-k$. The last inequality can be rewritten as $k > \lfloor \frac{n}{2} \rfloor + \lfloor \frac{s-2}{2} \rfloor$. □

Combining Theorem **??** and the trivial bound $\Delta \subseteq P(\mathcal{P}_{n-k,n})$ (see property (i) of Theorem **??**), we derive a condition on the dimension n of the zigzag function f from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$. This generalizes and simplifies the proof of [**?**, Lemma 4].

$$n \ge \begin{cases} 2k-s+2, & \text{if } n,s \text{ are both odd or even;} \\ 2k-s+1, & \text{otherwise.} \end{cases}$$

Theorem **??** has a nice implication that a relation can be found between s-zigzag functions and orthogonal arrays. Similar to the proof of Theorem **??** we have:

Theorem 11. *[?] An s-zigzag function $f : \mathbb{F}_2^n \to \mathbb{F}_2^k$ where n and s have different parity and $k > \lfloor \frac{n}{2} \rfloor + \lfloor \frac{s-2}{2} \rfloor$, exists if and only if a $LOA(2^{n-k}, n, 2, \Delta)$ exists.*

We generalize the notion of quorum system (see Definition **??**) to *s-quorum system* as a system that has the s-intersection property namely $\cap_{j=1}^s Q_{i_j} \neq \emptyset$ for all Q_{i_j}. Then define an *s-quorum access structure* analogously to Definition **??**. Now it is easy to prove a relation between the $\mathcal{Q}^s$ property for Δ and the s-quorum systems.

Lemma 3. *The tuple $(\Gamma^\perp, \Delta)$ is an s-quorum access structure if and only if Δ satisfies the $\mathcal{Q}^s$ property.*

Thus the result of Hirt and Maurer [**?**] in the active case multi-party computation can be translated in this context as follows: every function can be securely computed, provided that the tuple $(\Gamma^\perp, \Delta)$ is a 3-quorum access structure, where the 3-quorum system is $\mathbb{Q} = (\Gamma^\perp)^-$.

Further we generalize intersecting codes to *s-intersecting codes*, namely we say that a code is *s-intersecting code* for $s \geq 2$ if the intersection of any s non-zero codewords is not empty. Analogous theorem for relation between s-intersecting codes and s-quorum systems can be proven.

Theorem 12. *The access structure $(\Gamma(\mathcal{C}), \Delta(\mathcal{C})^{\perp})$ is an s-quorum system if and only if $\mathcal{C}$ is an s-intersecting code.*

References

1. C. Bennett, G. Brassard, J. -M. Roberts, Privacy Amplification by Public Discussion, *SIAM J.Comput.*, Vol. 17 (2), 1988, pp. 210-229.
2. G. Brassard, D. Crepeau, M. Santha, Oblivious Transfers and Intersecting Codes, *IEEE Trans. on IT, Special Issue in Coding and Complexity*, Vol. 42 (6), 1996, pp. 1769-1780.
3. A. Braeken, V. Nikov, S. Nikova, B. Preneel, On Boolean Functions with Generalized Cryptographic Properties, *Indocrypt 2004*, LNCS 3348, pp. 119-134, full version - *Cryptology ePrint Archive*: Report 2004/259.
4. D. Beaver, A. Wool, Quorum-Based Secure Multi-Party Computation, *Eurocrypt 1998*, LNCS 1403, 1998, pp. 25-35.
5. L. Chen, F. -W. Fu, V. Wei, On the Constructions of Highly Nonlinear Zigzag Functions and Unbiased Functions, *Inf. Proc. Letters*, Vol. 79 (3), 2001, pp. 135-140.
6. B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, R. Smolensky, The Bit Extraction Problem of t-resilient Functions, *FOCS 1985*, 1985, pp. 396-407.
7. G. Cohen, A. Lempel, Linear Intersecting Codes, *Discrete Mathematics* 56, 1985, pp. 35-43.
8. P. D'Arco, D. Stinson, Generalized Zig-zag Functions and Oblivious Transfer Reductions, *SAC 2001*, LNCS 2259, 2001, pp. 87-102.
9. K. Gopalakrishan, D. Stinson, Three Characterizations of non binary correlation-immune and Resilient function, *Design, Codes and Cryptography*, Vol. 5 (3), 1995, pp. 241-151.
10. M. Hirt, U. Maurer, Complete characterization of adversaries tolerable in secure multi-party computation, *PODC 1997*, pp. 25-34.
11. M. Herlihy, Methods for Abstract Data Types, *Ph.D Thesis MIT*, 1984, MIT/LCS/TR-319.
12. V. Nikov, S. Nikova, On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Schemes, *Cryptology ePrint Archive*: Report 2003/210.
13. D. Peleg, A. Wool, The Availability of Crumbling Wall Quorum Systems, *IT-36* (2), 1990, pp. 443.
14. M. Rabin, How to Exchange Secrets by Oblivious Transfer, Technical *Memo TR-81*, 1984.
15. M. Raynal, Algorithms for Mutual Exclusion, *MIT press*, 1986.
16. D. Stinson, Combinatorial Designs and Cryptography, *Surveys in Combinatorics*, 1993, pp. 257-287.
17. D. Stinson, Resilient Functions and Large Sets of Orthogonal Arrays, *Congressus Numerantium* 92, 1993, pp. 105-110.
18. D. Stinson, Some Results on Nonlinear Zigzag Functions, *JCMCC* 29, 1999, pp. 127-138.
19. T. Yan, H. Garcia-Molina, Distributed Selective Dissemination of Information, *Proc. Parallel and Distributed Information Systems*, 1994, pp. 89-98.
20. X.M. Zhang, Y. Zheng, Cryptographically Resilient Functions, *IEEE Trans. on IT*, Vol. 43 (5), 1997, pp. 1740–1747.