Generalized Zig-zag Functions and Oblivious Transfer Reductions

Paolo D'Arco[1] and Douglas Stinson[2]

[1] Dipartimento di Informatica ed Applicazioni
Università di Salerno, 84081 Baronissi (SA), Italy
paodar@dia.unisa.it
[2] Department of Combinatorics and Optimization
University of Waterloo, Waterloo Ontario, N2L 3G1, Canada
dstinson@uwaterloo.ca

Abstract. In this paper we show some *efficient* and *unconditionally secure* oblivious transfer reductions. Our main tool is a class of functions that *generalizes* the Zig-zag functions, introduced by Brassard, Crepéau, and Sántha in [6]. We show necessary and sufficient conditions for the existence of such generalized functions, and some characterizations in terms of well known combinatorial structures. Moreover, we point out an interesting relation between these functions and ramp secret sharing schemes where each share is a single bit.

Keywords: Oblivious Transfer, Zig-zag Functions, Ramp Schemes.

1 Introduction

The oblivious transfer is a well known cryptographic primitive. Introduced by Rabin in [24], and subsequently defined in different forms in [16, 5], it has found many applications in cryptographic studies and protocol design. One of the most common forms in which the oblivious transfer is used is the following[1] [5]: Let $\mathcal{S}$, the Sender, and let $\mathcal{R}$, the Receiver, be two players. Assume that $\mathcal{S}$ holds n secrets of ℓ bits and $\mathcal{R}$ is interested in one of them, say the i-th one. An oblivious transfer protocol enables $\mathcal{R}$ to receive the i-th secret out of the n $\mathcal{S}$ holds in such a way that

- $\mathcal{S}$ does not know which of the n secrets $\mathcal{R}$ has received
- $\mathcal{R}$ does not receive any information on the other secrets $\mathcal{S}$ holds.

We will refer to such a protocol as to an $\binom{n}{1}$-OT$^\ell$. All the oblivious transfer definitions [24, 16, 5] were shown to be equivalent [12, 4, 13, 6]. Moreover, Kilian, in [21], showed that the oblivious transfer is *complete*; in other words, it can be used to construct *any* other cryptographic protocol. Due to the importance

[1] Recently, it has been pointed out that Wiesner independently developed a similar concept in 1970, unpublished until [27].

of the oblivious transfer many papers [6, 12, 11, 13, 14, 22, 23], assuming that an $\binom{n}{1}$-OT$^\ell$ is available, have been focusing on designing protocols that realize an $\binom{N}{1}$-OT^L, where $N \geq n$ and $L \geq \ell$, using in an efficient way the given $\binom{n}{1}$-OT$^\ell$. Such kind of protocols are usually referred to as oblivious transfer reductions.

In [14], *unconditionally secure* oblivious transfer reductions have been studied. Lower bounds on the number of times an $\binom{n}{1}$-OT$^\ell$ oblivious transfer protocol must be called to realize an $\binom{N}{1}$-OT^L one, as well as on the number of random bits needed to implement such a reduction, have been proven. The bounds were shown to be tight when the parameter $L = \ell$. Unfortunately, when $L > \ell$, the trivial extension of the described protocol leaks some information. Actually, a cheating receiver is able to obtain pieces of different secrets.

In this paper we focus our attention on unconditionally secure reductions of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$. We show how to modify the protocol proposed in [14] in order to avoid information leakage. To this aim, we investigate the properties of a class of functions that *generalizes* the Zig-zag function class introduced by Brassard, Crepéau, and Sántha in [6] in order to reduce in an unconditionally secure way $\binom{2}{1}$-OT$^\ell$ to $\binom{2}{1}$-OT^1. Using these generalized Zig-zag functions we set up an unconditionally secure oblivious transfer reduction of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$, which is optimal up to a small multiplicative constant with respect to the number of invocations of the smaller oblivious transfer needed to implement such a reduction [14].

Zig-zag functions have been deeply studied in the last years. The authors of [6] showed that linear Zig-zag functions are equivalent to a special class of codes, the self-intersecting codes [9]. Moreover, they described several efficient methods to construct these codes. On the other hand, Stinson, in [25], found bounds and combinatorial characterizations both for linear and for non-linear Zig-zag functions. Applying techniques developed in [25, 26], we show necessary and sufficient conditions for the existence of generalized Zig-zag functions, and some characterizations in terms of orthogonal arrays and large set of orthogonal arrays as well.

Then, we show that the reduction presented in [14] can be viewed as a two-stage process, and using a ramp secret sharing scheme [1] in the first stage, we set up a reduction of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$, which is optimal with respect to the number of invocations of the available $\binom{n}{1}$-OT$^\ell$, up to a factor 2.

Finally, we point out an interesting relation between generalized Zig-zags and ramp secret sharing schemes where the size of each share is exactly one bit.

2 Oblivious Transfer

The following definitions were given by Brassard, Crepéau, and Sántha in [6] and were used, in a slightly simplified form[2] in [14]. We refer the reader to [6] for more details.

[2] The goal of that paper was to find out lower bounds and the awareness condition does not influence them in any way

Assume that $\mathcal{S}$ and $\mathcal{R}$ hold two programs, S and R respectively, which specify the computations to be performed by the players to achieve $\binom{N}{1}$-OT^L. These programs encapsulate, as black box, *ideal* $\binom{n}{1}$-OT$^\ell$. Hence, during the execution, $\mathcal{S}$ and $\mathcal{R}$ are able to carry out many times unconditionally secure $\binom{n}{1}$-OT$^\ell$. In order to model dishonest behaviours, where one of the player tries to obtain unauthorized information from the other, we assume that a cheating $\mathcal{S}$ (resp. $\mathcal{R}$) holds a modified version of the program, denoted by $\overline{S}$ (resp. $\overline{R}$).

Let $[\mathbf{P}_0, \mathbf{P}_1](a)(b)$ be the random variable representing the *output* obtained by $\mathcal{S}$ and $\mathcal{R}$ when they execute together their own programs, P_0 held by $\mathcal{S}$ and P_1 held by $\mathcal{R}$, with private inputs a and b, respectively. Moreover, let $[\mathbf{P}_0, \mathbf{P}_1]^*(a)(b)$ be the random variable that describes the *total information* acquired during the execution of the protocol on input a and b, and let $[\mathbf{P}_0, \mathbf{P}_1]^*_{\mathcal{S}}(a)(b)$ (resp. $[\mathbf{P}_0, \mathbf{P}_1]^*_{\mathcal{R}}(a)(b)$) be the random variable obtained by restricting $[\mathbf{P}_0, \mathbf{P}_1]^*(a)(b)$ to $\mathcal{S}$ (resp. to $\mathcal{R}$). These restrictions are the *view* each player has while running the protocol.

Finally, let W be the set of all length N sequences of L-bit secrets, and, for any $w \in W$, let w_i be the i-th secret of the sequence. Denoting by $\mathbf{W}$ the random variable that represents the choice of an element in W, and by $\mathbf{T}$ the random variable representing the choice of an index i in $T = \{1, \ldots, N\}$, we can define the conditions that an $\binom{N}{1}$-OT^L oblivious transfer protocol must satisfy as follows:

Definition 1. *The pair of programs* $[S, R]$ *is* correct *for* $\binom{N}{1}$-OT^L *if for each* $w \in W$ *and for each* $i \in T$

$$\mathcal{P}([\mathbf{S}, \mathbf{R}](w)(i)) \neq (\epsilon, w_i)) = 0, \tag{1}$$

and, for any program $\overline{S}$*, there exists a probabilistic program Sim such that, for each* $w \in W$ *and* $i \in T$

$$([\overline{\mathbf{S}}, \mathbf{R}](w)(i)|\mathcal{R} \textit{ accepts }) = ([\mathbf{S}, \mathbf{R}](Sim(w))(i)|\mathcal{R} \textit{ accepts }). \tag{2}$$

Notice that condition (1) means that two honest players always complete successfully the execution of the protocol. More precisely, $\mathcal{R}$ receives w_T, the secret in which he is interested, while $\mathcal{S}$ receives nothing. The output pair (ϵ, w_i), where ϵ denotes the empty string, describes this situation. On the other hand, condition (2), referred to as the awareness condition, means that, when $\mathcal{R}$ does not abort, a dishonest $\mathcal{S}$ cannot induce on $\mathcal{R}$'s output a distribution that he could not induce by changing the input (*Sim(w)*) and being honest. As explained in [6], this condition is necessary for future uses of the output of the protocol.

Assuming that both $\mathcal{S}$ and $\mathcal{R}$ are aware of the joint probability distribution $\mathcal{P}_{W,T}$ on W and T, the probability with which $\mathcal{S}$ chooses the secrets in W and $\mathcal{R}$ chooses an index $i \in T$, and using the *mutual information*[3] between two random variables, the privacy property of $\binom{N}{1}$-OT^L can be defined as follows:

[3] The reader is referred to Appendix A for the definition and some basic properties of the concept of mutual information.

Definition 2. *The pair of programs* $[S,R]$ *is* private *for* $\binom{N}{1}$*-*OT^L *if for each* $w \in W$ *and* $i \in T$*, for any program* $\overline{S}$

$$I(\mathbf{T};[\overline{\mathbf{S}},\mathbf{R}]^*_{\mathcal{S}}(w)(i)|\mathbf{W}) = 0, \tag{3}$$

while, for any program $\overline{R}$*, there exists a random variable* $\overline{\mathbf{T}} = f(\mathbf{T})$ *such that*

$$I(\mathbf{W};[\mathbf{S},\overline{\mathbf{R}}]^*_{\mathcal{R}}(w)(i)|\mathbf{T},\mathbf{W}_{\overline{T}}) = 0. \tag{4}$$

These two conditions ensure that a dishonest $\mathcal{S}$ does not gain information about $\mathcal{R}$'s index; and a dishonest $\mathcal{R}$ infers at most one secret among the ones held by $\mathcal{S}$.

3 Unconditionally Secure Reductions

In the literature can be found many unconditionally secure reductions of more "complex" OT to "simpler" ones [11, 12, 4, 14]. The efficiency of such reductions has been careful analyzed in [14]. Therein, the authors considered two types of reductions: reductions for *strong* $\binom{N}{1}$-OT^L, where condition (4) of Definition 2 holds, and reductions for *weak* $\binom{N}{1}$-OT^L, where condition (4) is substituted by the following condition:

for any program $\overline{R}$ *and* $i \in T$*, it holds that*

$$I(\mathbf{W};[\mathbf{S},\overline{\mathbf{R}}]^*_{\mathcal{R}}(w)(i)) \leq L. \tag{5}$$

Roughly speaking, in a weak reduction, a dishonest $\mathcal{R}$ can gain partial information about several secrets, but at most L bits overall. Besides, they termed *natural* reductions the reductions where the receiver $\mathcal{R}$ sends no messages to the sender $\mathcal{S}$. This automatically implies that condition (3) of Definition 2 is satisfied. Using the above terminology, they showed the following lower bounds on the number α of invocations the $\binom{N}{1}$-OT^L protocol must do of the ideal $\binom{n}{1}$-OT$^\ell$ sub-protocol, and on the number of random bits required to implement the $\binom{N}{1}$-OT^L.

Theorem 1. *[14] Any information-theoretical secure reduction of weak* $\binom{N}{1}$*-*OT^L *to* $\binom{n}{1}$*-*OT^ℓ *must have* $\alpha \geq \frac{L}{\ell} \cdot \frac{N-1}{n-1}$

Theorem 2. *[14] In any information-theoretic natural reduction of weak* $\binom{N}{1}$*-*OT^L *to* $\binom{n}{1}$*-*OT^ℓ *the sender must flip at least* $\frac{L(N-n)}{n-1}$ *random bits.*

When $L = \ell$, the bounds are tight both for the strong and the weak case, since they showed a protocol realizing $\binom{N}{1}$-OT$^\ell$ where $N > n$ which makes exactly $\frac{N-1}{n-1}$ invocations of the $\binom{n}{1}$-OT$^\ell$ and flips exactly $\frac{L(N-n)}{n-1}$ random bits [14]. However, for the case $L > \ell$, they gave a protocol (see Table 1), which is optimal with respect to condition (5), but which does not meet condition (4). The idea is simply to split each of the N secret strings in L/ℓ pieces of ℓ bits, and to run the

Protocol weakly reducing $\binom{N}{1}$-OT^L (with $L > \ell$) to $\binom{n}{1}$-OT$^\ell$. Assume that $\ell \mid L$. - Let $w = w_1, \ldots, w_N$ be the length N sequence of secrets $\mathcal{S}$ holds. For each $i = 1, \ldots, N$, w_i is a string of L bits. - Split the strings into $\frac{L}{\ell}$ pieces. More precisely, let $w_i = w_i^1, \ldots, w_i^{\frac{L}{\ell}}$, where, $w_i^j \in \{0,1\}^\ell$, for each $j = 1, \ldots, \frac{L}{\ell}$. - For $j = 1, \ldots, \frac{L}{\ell}$, execute an $\binom{N}{1}$-OT^ℓ oblivious transfer of *the j-th piece of* $w = w_1, \ldots, w_N$. In other words, compute $$\binom{N}{1}\text{-}OT^\ell \text{ on } (w_1^j, \ldots, w_N^j)$$ where the $\binom{N}{1}$-OT^ℓ is the reduction of $\binom{N}{1}$-OT$^\ell$ to $\binom{n}{1}$-OT$^\ell$ described in [14].

Table 1. Basic protocol for a weak reduction

available $\binom{N}{1}$-OT$^\ell$, optimal with respect to the use of the $\binom{n}{1}$-OT$^\ell$ black box, exactly $\frac{L}{\ell}$ times.

An honest $\mathcal{R}$ always obtains the secret in which he is interested in, recovering the "right" pieces at each execution. On the other hand, a *cheating* $\mathcal{R}$ is able to recover $\frac{L}{\ell}$ pieces of possibly *different* secrets among $w = w_1, \ldots, w_N$. We would like to modify this basic construction in order to achieve condition (4) without losing too much in efficiency.

Brassard, Crepéau, and Sántha solved a similar problem in [6]. They studied how to reduce $\binom{2}{1}$-OT$^\ell$ to $\binom{2}{1}$-OT^1 in an information theoretic secure way. Starting from the observation that trivial serial executions of ℓ $\binom{2}{1}$-OT^1 oblivious transfer, one for each bit of the two secret strings w_0 and w_1, didn't work, they pursued the idea of finding a function f where, given x_0 and x_1 such that $f(x_0) = w_0$ and $f(x_1) = w_1$, from two disjoint subsets of bits of x_0 and x_1 it is possible to gain information on *at most one* of w_0 and w_1. Using such a (public) function, the reduction would have been simple to implement (see Table 2).

The property of f ensures that an honest receiver is always able to recover one of the secrets, while a dishonest receiver can obtain information on at most one of the secrets. They called such functions *Zig-zag functions.*

Notice that we have to solve a very close problem: in our scenario, a cheating receiver is able to obtain *partial* information about *many* secrets. Our aim is to find out a class of functions where disjoint subsets of strings $x_1, x_2, \ldots$ give information about at most one of the secrets $w_1, w_2, \ldots$

Protocol strongly reducing $\binom{2}{1}$-OT$^\ell$ to $\binom{2}{1}$-OT^1

- $\mathcal{S}$ picks random $x_0, x_1 \in \{0,1\}^n$ such that $f(x_0) = w_0$ and $f(x_1) = w_1$
- For $i = 1, \ldots, n$, $\mathcal{S}$ performs a $\binom{2}{1}$-OT^1 on the pair (x_0^i, x_1^i)
- $\mathcal{R}$ recovers w_0 or w_1 by computing $f(x_0)$ or $f(x_1)$.

Table 2. Protocol for two secrets of ℓ bits

4 Generalized Zig-zag Functions

Let $X = GF(q)$, and let $X^n = \{(x_1, \ldots, x_n) : x_i \in X, \text{ for } 1 \le i \le n\}$. Moreover, for each $I = \{i_1, \ldots, i_{|I|}\} \subseteq \{1, \ldots, n\}$, denote by $x^I = (x_{i_1}, \ldots, x_{i_{|I|}})$ the subsequence of $x \in X^n$ indexed by I. Finally, let X^I be the set of all possible subsequences x^I for a given I.

A function is *unbiased* with respect to a subset I if the knowledge of the value of x^I does not give *any* information about $f(x)$. More formally, we have the following definition

Definition 3. *Suppose that $f : X^n \to X^m$, where $n \ge m$. Let $I \subseteq \{1, \ldots, n\}$. We say that f is* unbiased *with respect to I if, for all possible choices of $x^I \in X^I$, and for every $(y_1, \ldots, y_m) \in X^m$, there are exactly $q^{n-m-|I|}$ choices for $x^{\{1,\ldots,n\}\setminus I}$ such that $f(x_1, \ldots, x_n) = (y_1, \ldots, y_m)$.*

This concept has been introduced in [6]. Actually, the form in which it is stated here is the same as [25]. Since we are going to follow the same approach applied in [25] to study the properties of linear and nonlinear Zig-zag functions, we prefer this definition. The definition of Zig-zag functions relies on the unbiased property.

Definition 4. *A function $f : X^n \to X^m$ is said to be a* Zig-zag *function if, for every $I \subseteq \{1, \ldots, n\}$, f is unbiased with respect to at least one of I and $\{1, \ldots, n\} \setminus I$.*

We would like some "generalized" Zig-zag property, holding for different disjoint subsets of indices. Roughly speaking, a generalized Zig-zag function should be unbiased with respect to at least $s-1$ of the subsets $I_1, \ldots, I_s$ into which $\{1, \ldots, n\}$ is partitioned (for all possible partitions). More formally, we can state the following

Definition 5. *Let s be an integer such that $2 \le s \le n$. A function $f : X^n \to X^m$ is said to be an s-*Zig-zag *function if, for every set of s subsets $I_1, \ldots, I_s \subseteq \{1, \ldots, n\}$, such that $\cup_i I_i = \{1, \ldots, n\}$, and $I_j \cap I_j = \emptyset$ if $i \ne j$, f is unbiased with respect to at least $s-1$ of $I_1, \ldots, I_s$.*

In an s-Zig-zag function, if $\mathcal{R}$ collects information about s x_i's, for some s, then he can get information on at most one w_i. If the above property is satisfied *for every* $2 \leq s \leq n$, then we say that f is *fully Zig-zag* (see Appendix B for an example of such a function). Fully Zig-zag functions enable us to apply the same approach developed in [6] in order to substitute the real secrets w_i with some pre-images x_i of w_i. The generalized property of the function *ensures* the privacy of the transfer.

Note: The functions $f : X^n \to X^m$ we are looking for must be *efficient to compute*. Moreover, there must exist an *efficient procedure* to compute a *random pre-image* $x \in f^{-1}(y)$, for each $y \in X^m$.

4.1 Zig-zag and Fully Zig-zag Functions.

We briefly review some definitions and known results about Zig-zag. A Zig-zag (resp. s-Zig-zag, fully Zig-zag) function is said to be *linear* if there exists an $m \times n$ matrix M with entries from $GF(q)$ such that $f(x) = xM^T$ for all $x \in GF(q)^n$.

The following results have been shown in [25] and are recalled here since they will be used in the following subsection. The next lemma shows an upper bound on the size of the set of index I with respect to a function can be unbiased.

Lemma 1. *[25] If $f : X^n \to X^m$ is unbiased with respect to I, then $|I| \leq n - m$.*

As a consequence, it is possible to show a lower bound on the size n of the domain of the function, given the size m of the codomain.

Lemma 2. *[25] If $f : X^n \to X^m$ is a Zig-zag function, then $n \geq 2m - 1$.*

The following theorem establishes that a Zig-zag function is unbiased with respect to all the subsets of size $m - 1$.

Theorem 3. *[25] If $f : X^n \to X^m$ is a Zig-zag function, then f is unbiased with respect to I for all I such that $|I| = m - 1$.*

Moreover, notice that it is not difficult to prove the following result

Lemma 3. *If $f : X^n \to X^m$ is unbiased with respect to I, then f is unbiased with respect to all $I^{'} \subseteq I$.*

Using the above results, we can prove our main result of this section: an equivalence between certain fully Zig-zag functions and Zig-zag functions.

Theorem 4. *Let $n \geq 2m - 1$. Then $f : X^n \to X^m$ is a fully Zig-zag function if and only if f is a Zig-zag function.*

Proof. We give the proof for $n = 2m - 1$. The if part is straightforward. Indeed, if f is fully Zig-zag, then *for each* partition $I_1, \ldots, I_s$ of $\{1, \ldots, n\}$ f is unbiased with respect to at least $s - 1$ subsets out of the s in the partition. Hence, it is unbiased with respect to at least 1 subset out of the 2 for any possible bipartition of $\{1, \ldots, n\}$. Therefore, f is Zig-zag.

Assume now that f is Zig-zag. Hence, by definition, for each $I \subseteq \{1, \ldots, n\}$, f is unbiased with respect to at least one of I and $\{1, \ldots, n\} \setminus I$.

Let $I_1, \ldots, I_s$ be a partition of $\{1, \ldots, n\}$. We can consider two cases.

a) There exists a subset I_i of the partition such that $|I_i| > n - m$. Consider this subset. Since f is Zig-zag, by Lemma 1, f is unbiased with respect to $\{1, \ldots, n\} \setminus I_i$. But $\{1, \ldots, n\} \setminus I_i = \cup_{j \neq i} I_j$. Hence, applying Lemma 3, we can conclude that f is unbiased with respect to all I_j, for $j \neq i$.
b) For each $i = 1, \ldots, s$, $|I_i| \leq n - m$. Notice that, since $n = 2m - 1$,

$$|I_i| \leq n - m \Leftrightarrow |I_i| \leq 2m - 1 - m \Leftrightarrow |I_i| \leq m - 1.$$

Since f is a Zig-zag function, applying Theorem 3, we can say that f is unbiased with respect to all $I_i : |I_i| = m - 1$. Therefore, by Lemma 3, we can conclude that f is unbiased with respect to all of $I_1, \ldots, I_s$.

Therefore, f is fully Zig-zag. □

The proof for $n > 2m - 1$ is similar. Therefore, we can conclude saying that Zig-zag and fully Zig-zag definitions define the *same class of functions*. Therefore, the known constructions for Zig-zag functions enable us to improve the protocol described in Table 1 by substituting the secrets with the pre-images of a Zig-zag functions, as done in the protocol described in Table 2 for two secrets. A complete description of our protocol can be found in Table 3. Moreover, since both in [6] and in [25], has been shown that for each m there exist functions $f : X^n \to X^m$, where $n = \Theta(m)$ and the asymptotic notation hides a small constant, the modified protocol is still efficient and optimal with respect to the bound obtained in [14] up to a small multiplicative constant [4].

Protocol strongly reducing $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$

Let $f : X^P \to X^L$ be a fully Zig-zag function such that $\ell | P$.

- $\mathcal{S}$ picks random $x_0, x_1, \ldots, x_{N-1} \in \{0,1\}^P$ such that, for $i = 0, \ldots, N-1$, $f(x_i) = w_i$.
- $\mathcal{S}$ performs the protocol described in Table 1, using $x_0, x_1, \ldots, x_{N-1}$ instead of the real secrets $w_0, \ldots, w_{N-1}$.
- $\mathcal{R}$ recovers x_i, and computes $w_i = f(x_i)$.

Table 3. General protocol, depending on f.

[4] After the submission of this extended abstract to the conference, we found out that Dodis and Micali, working on the journal version of the paper presented at Eurocrypt '99, have independently obtained the same reduction, which will appear in the full version of their paper.

4.2 On the Existence of s-Zig-zags.

A question coming up to mind now is the following: Zig-zag functions are equivalent to fully Zig-zag functions. But these functions, according to Lemma 2, exist only if $n \geq 2m-1$. Do s-Zig-zag functions exist when $n < 2m-1$? The example reported in Appendix C shows that the answer is again affirmative. It is interesting to investigate some necessary and sufficient conditions for the existence of such generalized functions. The following lemma extends Lemma 2:

Lemma 4. *If an s-Zig-zag function $f : X^n \to X^m$ exists, then*

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

Proof. Notice that, by definition, f must be unbiased with respect to at least $s-1$ subsets of each possible s-partition. It is not difficult to check that the worst case we have to consider is when a partition has $s-2$ subsets of size 1 and two subsets of essentially the same size. Therefore, f must be unbiased with respect to at least one of the two "big" subsets. Hence, applying Lemma 1, it follows that

$$\lfloor \frac{n-(s-2)}{2} \rfloor \leq n - m. \tag{6}$$

The result follows by simple algebra. □

An interesting relation between s-Zig-zag and t-Zig-zag, where $t \geq s$, is stated by the following lemma, whose proof can be obtained essentially noticing that a t-partition is a refinement of an s-partition.

Lemma 5. *If $f : X^n \to X^m$ is s-Zig-zag, then f is t-Zig-zag for every $s < t \leq n$.*

4.3 A Combinatorial Characterization.

Let t be an integer such that $1 \leq t \leq k$ and $v \geq 2$. An *orthogonal array* $OA_\lambda(t,k,v)$ is a $\lambda v^t \times k$ array A of v symbols, such that within any t columns of A, every possible t-tuple of symbols occurs in exactly λ rows of A. An orthogonal array is *simple* if it does not contain two identical rows. A *large set* of orthogonal arrays $OA_\lambda(t,k,v)$, denoted $LOA_\lambda(t,k,v)$, is a set of v^{k-t}/λ simple $OA_\lambda(t,k,v)$, such that every possible k-tuple occurs as a row in exactly one of the orthogonal arrays in the set (see [20] for the theory and applications of these structures).

Theorem 5. *If $f : X^n \to X^m$ is an s-Zig-zag function where n and s have different parity, and $m > \lfloor \frac{n}{2} \rfloor + \lfloor \frac{s-2}{2} \rfloor$ then f is unbiased with respect to all the subsets of size $\lfloor \frac{n-(s-2)}{2} \rfloor$.*

Proof. Notice that, our assumptions imply $\lceil \frac{n-(s-2)}{2} \rceil > \lfloor \frac{n-(s-2)}{2} \rfloor$. By definition, f is unbiased with respect to at least $s-1$ subsets of each s-partition of $\{1, \ldots, n\}$. Suppose there exists a subset I_i such that $|I_i| = \lfloor \frac{n-(s-2)}{2} \rfloor$ with respect to f is biased. Then, it would be possible to define an s-partition having $s-2$ subsets of size 1, the subset I_i, and a subset R having size

$$|R| = n - (s-2) - \lfloor \frac{n-(s-2)}{2} \rfloor = \lceil \frac{n-(s-2)}{2} \rceil.$$

Since f is biased with respect to I_i, then f must be unbiased with respect to R. This is possible only if

$$|R| = \lceil \frac{n-(s-2)}{2} \rceil \leq n - m \iff m \leq n - \lceil \frac{n-(s-2)}{2} \rceil.$$

Since $\lceil \frac{n-(s-2)}{2} \rceil = \lceil \frac{n}{2} \rceil - \lfloor \frac{s-2}{2} \rfloor$ the above inequality is satisfied only if $m \leq \lfloor \frac{n}{2} \rfloor + \lfloor \frac{s-2}{2} \rfloor$. But $m > \lfloor \frac{n}{2} \rfloor + \lfloor \frac{s-2}{2} \rfloor$ and, hence, we have a contradiction. □

The following theorem establishes a necessary and sufficient condition for the existence of certain s-Zig-zag functions.

Theorem 6. *An s-Zig-zag function $f : X^n \to X^m$, where n and s have different parity, and $m > \lfloor \frac{n}{2} \rfloor + \lfloor \frac{s-2}{2} \rfloor$ exists if and only if a large set of orthogonal arrays $LOA_\lambda(\lfloor \frac{n-(s-2)}{2} \rfloor, n, q)$ with $\lambda = q^{n-m-\lfloor \frac{n-(s-2)}{2} \rfloor}$ exists.*

Proof. The necessity of the condition derives from Theorem 5, analyzing the arrays containing the pre-images of f, as done in [25]. The sufficiency can be proved as follows: label each of the q^m arrays of the large set with a different element of $y \in X^m$. Denote such array with A_y. Then, define a function $f : X^n \to X^m$ as

$$f(x_1, \ldots, x_n) = y \iff (x_1, \ldots, x_n) \in A_y.$$

The properties of the arrays and the condition $m > \lfloor \frac{n}{2} \rfloor + \lfloor \frac{s-2}{2} \rfloor$ assure that f is s-Zig-zag. □

On the other hand, using the same proof technique, it is possible to show a *sufficient* condition for the existence of an s-Zig-zag for *any* n and $2 \leq s \leq n$. More precisely, we can state the following

Theorem 7. *If a large set of orthogonal arrays $LOA_\lambda(\lfloor \frac{n-(s-2)}{2} \rfloor, n, q)$ with $\lambda = q^{n-m-\lfloor \frac{n-(s-2)}{2} \rfloor}$ exists, then an s-Zig-zag function exists.*

5 Towards a General Reduction

The protocol described before can be conceptually divided in two phases: a first phase in which x_i is split into several pieces and $\mathcal{R}$ needs all the pieces to retrieve x_i; and a second phase where, once having obtained x_i, $\mathcal{R}$ recovers the secret by computing $y_i = f(x_i)$ for some function f. Since each piece gives partial knowledge of x_i, f needs to hide the value of y_i according to the definition of a correct and private reduction (i.e., the Zig-zag property). In this section, we show that using in the first phase an appropriate *ramp secret sharing scheme* [1] (see Appendix D for a brief review of the definition and some basic properties) to share x_i then, in the second phase the function f needs *weaker requirements* than the Zig-zag property. In this case, the pieces that $\mathcal{R}$ recovers from each transfer are not *substrings* of the value x_i he needs to compute the real secret $y_i = f(x_i)$, but *shares* that he has to combine according to the given ramp scheme in order to recover x_i.

Actually, notice that the splitting of the strings can be seen as a sharing according to a $(0, \frac{p}{\ell}, \frac{p}{\ell})$-RS, where p is $|x_i|$ and ℓ is the size of each share/piece. The questions therefore are: is it possible to design an overall better protocol, using in the first phase some *non trivial* ramp scheme to share x_i. Does there exist a *trade-off* between what we pay in the first phase and what we pay in the second phase? Using a generic (t_1, t_2, n)-RS, what properties does f need to satisfy in order to hide y_i from partial knowledge of x_i as required by our problem? It is not difficult to check that the condition f needs is the following.

Definition 6. *A function $f : X \to Y$ realizes an unconditionally secure oblivious transfer reduction if and only if, for each set of shares $\{x_1, \ldots, x_n\}$ for a secret $x \in X$ generated by a given (t_1, t_2, n)-RS, for every sequence of subsets $I_1, \ldots, I_s \subseteq \{1, \ldots, n\}$, such that $\cup_i I_i = \{1, \ldots, n\}$, and $I_i \cap I_j = \emptyset$ if $i \neq j$, it holds that*

$$H(Y|X_{I_i}) = H(Y)$$

for at least $s-1$ of $I_1, \ldots, I_s$.

The definition means that *at most one subset* of shares can give information about $f(x)$.

It is easy to see that, when the ramp secret sharing scheme used in the first phase of the protocol is the trivial $(0, p, p)$-RS (shares/pieces of one bit), Definition 6 is equivalent to fully Zig-zag functions.

An Almost Optimal Reduction. Using a $(\frac{n}{2}, n, n)$-RS it is immediate to see that, to acquire information on x_i, the adversary needs at least $\frac{n}{2} + 1$ shares. Hence, recovering partial information on one secret *rules out* the possibility of recovering partial information on another secret. Notice that with such a scheme, if each secret has size p and ℓ divides p, the bound on the size of the shares (see Appendix D) implies $n \geq \frac{2p}{\ell}$ (number of invocations of the given $\binom{N}{1}$-OT^{ℓ}). An implementation meeting the bound for several values of p and ℓ can be set up using, for example, the protocol described in [17]. In this case the function f used in the second phase can be simply the identity function!

6 Ramp Secret Sharing Schemes with Shares of One Bit

Fully Zig-zag, s-Zig-zag and Zig-zag functions give rise to ramp secret sharing schemes with shares of one bit. The idea is the following: the dealer, given one of these functions, say $f : X^n \to X^m$, chooses a secret $y \in X^m$ and computes a random pre-image $x \in f^{-1}(y)$. Then, he distributes the secret among the set of n participants giving, as a share, a single bit of the pre-image x to each of them. It is immediate to see that

- some subsets of participants do not gain *any* information about the secret, even if they pool together their shares. These subsets are the subsets of $\{1, \ldots, n\}$ with respect to the function f is *unbiased.*
- some subsets of participants are able to recover *partial* information about the secret. These are the subsets of $\{1, \ldots, n\}$ with respect to f is biased
- *all* the participants are able to recover the *whole* secret.

The idea of such constructions was recently described in [8] (see Remark 9) as an application of ℓ-AONT transforms. In that construction, however, the dealer distributes among the participants the *bits of the image* of the secret while we distribute the bits of a pre-image of the secret.

7 Conclusions

In this paper we have shown how to achieve efficient unconditionally secure reductions of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$, proving that Zig-zag functions can be used to reduce $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ *for each* $N \geq n$ and $L \geq \ell$. Finally, we have studied a generalization of these functions, identifying a combinatorial characterization and a relation with ramp schemes with shares of one bit. Some interesting questions arise from this study. To name a few:

– The constructions presented before are almost optimal but do not meet the bounds of Theorems 1 and 2 by equality. Hence, the question of how to reach (if it is possible) these bounds is still open.
– Do *cryptographic applications* of s-Zig-zag exist? We have pointed out the interesting relation with efficient ramp schemes, where each share is a single bit. Is it possible to say more?
– Linear Zig-zag are equivalent to *self-intersecting codes.* Is there any characterization in *terms of codes* for s-Zig-zag functions? And what about some *efficient constructions*? Is it possible, along the same line of [6], to set up any deterministic or probabilistic method?

Acknowledgements

This research was done while the first author was visiting the Department of Combinatorics and Optimization at the University of Waterloo. He would like to thank the Department for its hospitality. Moreover, he would like to thanks Yevgeniy Dodis for a helpful discussion.

D.R. Stinson's research is supported by NSERC grants IRC 216431-96 and RGPIN 203114-98.

References

1. G.R. Blakley, Security of Ramp Schemes, *Advances in Cryptology: Crypto '84*, pp. 547-559, LNCS Vol. 196, pp. 242-268, 1984.
2. M. Bellare and S. Micali, Non-interactive Oblivious Transfer and Applications, *Advances in Cryptology: Crypto '89*, Springer-Verlag, pp. 547-559, 1990.
3. M. Blum, How to Exchange (Secret) Keys, *ACM Transactions of Computer Systems*, Vol. 1, No. 2, pp. 175-193, 1993
4. G. Brassard, C. Crepéau, and J.-M. Roberts, Information Theoretic Reductions Among Disclosure Problems, *Proceedings of 27th IEEE Symposium on Foundations of Computer Science*, pp. 168-173, 1986.
5. G. Brassard, C. Crepéau, and J.-M. Roberts, All-or-Nothing Disclosure of Secrets, *Advances in Cryptology: Crypto '86*, Springer-Verlag, Vol. 263, pp. 234-238, 1987.
6. G. Brassard, C. Crepéau, and M. Sántha, Oblivious Transfer and Intersecting Codes, *IEEE Transaction on Information Theory*, special issue in coding and complexity, Vol. 42, No. 6, pp. 1769-1780, 1996.
7. C. Blundo, A. De Santis, and U. Vaccaro, Efficient Sharing of Many Secrets, *Proceedings of STACS*, LLNCS Vol. 665, pp.692-703, 1993.
8. R. Canetti, Y. Dodis, S. Halevi, E. Kushilevitz, and A. Sahai, Exposure-Resilient Functions and All-or-Nothing Transforms, *Advances in Cryptology: Proceedings of EuroCrypt 2000*, Springer-Verlag, LLNCS vol. 1807, pp. 453-469, 2000.
9. G. Cohen and A. Lempel, Linear Intersecting Codes, *Discrete Mathematics*, Vol. 56, pp. 35-43, 1985.
10. T. M. Cover and J. A. Thomas, Elements of Information Theory, *John Wiley & Sons*, 1991.
11. C. Crepéau, A Zero-Knowledge Poker Protocol that Achieves Confidentiality of the Players' Strategy or How to Achieve an Electronic Poker Face, *Advances in Cryptology: Proceedings of Crypto '86*, Springer-Verlag, pp. 239-247, 1987.
12. C. Crepéau, Equivalence between to flavors of oblivious transfers, *Advances in Cryptology: Proceedings of Crypto '87*, Springer-Verlag, vol. 293, pp. 350-354, 1988.
13. C. Crepéau and J. Kilian, Achieving Oblivious Transfer Using Weakened Security Assumptions, *Proceedings of 29th IEEE Symposium on Foundations of Computer Science*, pp. 42-52, 1988.
14. Y. Dodis and S. Micali, Lower Bounds for Oblivious Transfer Reduction, *Advances in Cryptology: Proceedings of Eurocrypt '99*, vol. 1592, pp. 42-54, Springer Verlag, 1999.
15. S. Even, O. Goldreich, and A. Lempel, A Randomized Protocol for Signing Contracts, *Advances in Cryptology: Proceedings of Crypto '83*, Plenum Press, New York, pp. 205-210, 1983.
16. M. Fisher, S. Micali, and C. Rackoff, A Secure Protocol for the Oblivious Transfer, *Journal of Cryptology*, vol. 9, No. 3, pp. 191-195, 1996.
17. M. Franklin and M. Yung, Communication Complexity of Secure Computation, *Proceedings of the 24th Annual Symposium on Theory of Computing*, pp. 699-710, 1992.
18. O. Goldreich, S. Micali, and A. Wigderson, How to play ANY mental game or: A Completeness Theorem for Protocols with Honest Majority, *Proceedings of 19th Annual Symposium on Theory of Computing*, pp. 20-31, 1987.
19. W.-A. Jackson and K. Martin, A Combinatorial Interpretation of Ramp Schemes, *Australasian Journal of Combinatorics*, vol. 14, pp. 51-60, 1996.

20. A. Hedayat, N.J.A. Sloane, and J. Stufken, Orthogonal Arrays : Theory and Applications, *Springer Verlag*, 1999.
21. J. Kilian, Founding Cryptography on Oblivious Transfer, *Proceedings of 20th Annual Symposium on Theory of Computing*, pp. 20-31, 1988.
22. M. Naor and B. Pinkas, Computationally Secure Oblivious Transfer, available at *http://www.wisdom.weizmann.ac.il/ naor/onpub.html*
23. M. Naor and B. Pinkas, Efficient Oblivious Transfer Protocols, available at *http://www.wisdom.weizmann.ac.il/ naor/onpub.html*
24. M. Rabin, How to Exchange Secrets by Oblivious Transfer, *Technical Memo TR-81, Aiken Computation Laboratory*, Harvard University, 1981.
25. D.R. Stinson, Some Results on Nonlinear Zig-zag Functions, *The Journal of Combinatorial Mathematics and Combinatorial Computing*, No. 29, pp. 127-138, 1999.
26. D.R. Stinson, Resilient Functions and Large Set of Orthogonal Arrays, *Congressus Numerantium*, Vol. 92, 105-110, 1993.
27. S. Wiesner, Conjugate Coding, *SIGACT News*, Vol. 15, pp. 78-88, 1983.

A Information Theory Elements

This appendix briefly recalls some elements of information theory (the reader is referred to [10] for details).

Let $\mathbf{X}$ be a random variable taking values on a set X according to a probability distribution $\{P_{\mathbf{X}}(x)\}_{x \in X}$. The *entropy* of $\mathbf{X}$, denoted by $H(\mathbf{X})$, is defined as

$$H(\mathbf{X}) = -\sum_{x \in X} P_{\mathbf{X}}(x) \log P_{\mathbf{X}}(x),$$

where the logarithm is to the base 2. The entropy satisfies

$$0 \leq H(\mathbf{X}) \leq \log |X|,$$

where $H(\mathbf{X}) = 0$ if and only if there exists $x_0 \in X$ such that $Pr(\mathbf{X} = x_0) = 1$; whereas, $H(\mathbf{X}) = \log |X|$ if and only if $Pr(\mathbf{X} = x) = 1/|X|$, for all $x \in X$. The entropy of a random variable is usually interpreted as

- a measure of the equidistribution of the random variable
- a measure of the amount of information given on average by the random variable

Given two random variables $\mathbf{X}$ and $\mathbf{Y}$ taking values on sets X and Y, respectively, according to the joint probability distribution $\{P_{\mathbf{XY}}(x, y)\}_{x \in X, y \in Y}$ on their cartesian product, the *conditional entropy* $H(\mathbf{X}|\mathbf{Y})$ is defined as

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y \in Y} \sum_{x \in X} P_{\mathbf{Y}}(y) P_{\mathbf{X}|\mathbf{Y}}(x|y) \log P_{\mathbf{X}|\mathbf{Y}}(x|y).$$

It is easy to see that

$$H(\mathbf{X}|\mathbf{Y}) \geq 0.$$

with equality if and only if X is a function of Y. The conditional entropy is a measure of the amount of information that $\mathbf{X}$ still has, once given $\mathbf{Y}$.

The *mutual information* between $\mathbf{X}$ and $\mathbf{Y}$ is given by

$$I(\mathbf{X};\mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}),$$

and it enjoys the following properties,

$$I(\mathbf{X};\mathbf{Y}) = I(\mathbf{Y};\mathbf{X}), \text{ and } I(\mathbf{X};\mathbf{Y}) \geq 0.$$

The mutual information is a measure of the common information between $\mathbf{X}$ and $\mathbf{Y}$.

B A Fully Zig-zag Function

In this section, we show an example of a fully Zig-zag function. Let $X = GF(2)$, and let $f : X^6 \to X^3$ be the function defined by $f(x) = xM^T$ where

$$M = \begin{bmatrix} 1\,0\,1\,1\,0\,0 \\ 1\,1\,0\,0\,1\,0 \\ 0\,1\,1\,0\,0\,1 \end{bmatrix}$$

To prove that f is fully Zig-zag it is necessary to show that, for any $1 < s \leq 6$, for each partition of $\{1,\ldots,6\}$ into s parts, f is unbiased with respect to at least $s-1$ of them. An easy proof can be obtained using the following theorem, which can be found in [25].

Theorem 8. *Let M be a generating matrix for an $[n,m]$ q-ary code, $\mathcal{C}$, and let H be a parity-check matrix for $\mathcal{C}$. The function $f(x) = xM^T$ is unbiased with respect to $I \subseteq \{1,\ldots,n\}$ if and only if the columns of H indexed by I are linearly independent.*

The parity-check matrix H for the generating matrix M is

$$H = \begin{bmatrix} 1\,0\,0\,1\,1\,0 \\ 0\,1\,0\,0\,1\,1 \\ 0\,0\,1\,1\,0\,1 \end{bmatrix}$$

Applying the above theorem, it is not difficult to see that f is unbiased with respect to

a) any subset of size 1.
b) any subset of size 2.
c) any subset of size 3, except $\{1,2,5\},\{1,3,4\},\{2,3,6\}$, and $\{4,5,6\}$.

Therefore, for any $2 \leq s \leq 6$, and for any s-partition, f is unbiased with respect to at least $s-1$ subsets of the s subsets.

C An Example of an s-Zig-zag

In this Appendix we show an example of a 3-Zig-zag function (where $n < 2m-1$). Let $X = GF(2)$, and let $f : X^4 \to X^3$ be the function defined by $f(x) = xM^T$ where

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

In this case, the parity-check matrix H for the generating matrix M is simply

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

Applying Theorem 8, it is easy to see that f is unbiased with respect to each subset of size 1. Since any 3-partition contains 2 subsets of size 1 and a subset of size 2, it follows that f is unbiased with respect to exactly 2 subsets.

Hence, s-Zig-zag functions can exist where Zig-zag functions and fully Zig-zag functions cannot exist.

D Ramp Secret Sharing Schemes

A ramp secret sharing schemes ((t_1, t_2, n)-RS, for short) is a protocol by means of which a dealer distributes a secret s among a set of n participants $\mathcal{P}$ in such a way that subsets of $\mathcal{P}$ of size greater than or equal to t_2 can reconstruct the value of s, any subset of $\mathcal{P}$ of size less than or equal to t_1 cannot determine anything about the value of the secret, while a subset of size $t_1 < t < t_2$ can recover *some* information about the secret [1]. Using information theory, the three properties of a (linear) (t_1, t_2, n)-RS can be stated as follows. Assuming that P denotes both a subset of participants and the set of shares these participants receive from the dealer to share a secret $s \in S$, and denoting the corresponding random variables in bold, it holds

- *Any subset of participants of size less than or equal to t_1 has no information on the secret value:* Formally, for each subset $P \in \mathcal{P}$ of size $|P| \leq t_1$, $H(\mathbf{S}|\mathbf{P}) = H(\mathbf{S})$.
- *Any subset of participants of size $t_1 < |P| < t_2$ has some information on the secret value:* Formally, for each subset $P \in \mathcal{P}$ of size $t_1 < |P| < t_2$, $H(\mathbf{S}|\mathbf{P}) = \frac{|P|-t_1}{t_2-t_1} H(\mathbf{S})$.
- *Any subset of participants of size greater than t_2 can compute the whole secret:* Formally, for each subset $P \in \mathcal{P}$ of size $|P| \geq t_2$, $H(\mathbf{S}|\mathbf{P}) = 0$.

In a (t_1, t_2, n)-RS, the size of each share must be greater than or equal to $\frac{H(\mathbf{S})}{t_2-t_1}$ (see [7, 19]).