Some Results on the Existence of t-All-or-Nothing Transforms Over Arbitrary Alphabets

Navid Nasr Esfahani, Ian Goldberg, Douglas R. Stinson

Dedicated to the memory of Solomon W. Golomb (1932–2016)

***Abstract*—A (t, s, v)-all-or-nothing transform is a bijective mapping defined on s-tuples over an alphabet of size v, which satisfies the condition that the values of any t input co-ordinates are completely undetermined, given only the values of any $s - t$ output co-ordinates. The main question we address in this paper is: for which choices of parameters does a (t, s, v)-all-or-nothing transform (AONT) exist? More specifically, if we fix t and v, we want to determine the maximum integer s such that a (t, s, v)-AONT exists. We mainly concentrate on the case $t = 2$ for arbitrary values of v, where we obtain various necessary as well as sufficient conditions for existence of these objects. This includes computer searches that establish the existence of $(2, q, q)$-AONT for all odd primes not exceeding 29. We also show some connections between AONT, orthogonal arrays and resilient functions.**

I. Introduction and Previous Results

RIVEST defined all-or-nothing transforms in [9] in the setting of computational security. Stinson considered unconditionally secure all-or-nothing transforms in [11]. More general types of unconditionally secure all-or-nothing transforms have been recently studied in [3], [5], [14].

We begin with some relevant definitions.

Definition I.1. Let X be a finite set of cardinality v, called an *alphabet*. Let s be a positive integer, and suppose that $\phi : X^s \to X^s$. We will think of ϕ as a function that maps an input s-tuple, say $\mathbf{x} = (x_1, \ldots, x_s)$, to an output s-tuple, say $\mathbf{y} = (y_1, \ldots, y_s)$, where $x_i, y_i \in X$ for $1 \leq i \leq s$. Let $1 \leq t \leq s$ be an integer. Informally, the function ϕ is an (unconditionally secure) (t, s, v)-*all-or-nothing transform* provided that the following properties are satisfied:

1) ϕ is a bijection.
2) If any $s - t$ of the s output values $y_1, \ldots, y_s$ are fixed, then the values of any t inputs are completely undetermined, in an information-theoretic sense.

We will denote such a function as a (t, s, v)-AONT, where $v = |X|$.

We note that any bijection from X^s to itself is an (s, s, v)-AONT, so the case $s = t$ is trivial.

Manuscript received February 23, 2017; revised September 22, 2017

All three authors are with David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

I. Goldberg's research is supported by NSERC discovery grant RGPIN-03858

D. Stinson's research is supported by NSERC discovery grant RGPIN-03882

The work of Rivest [9] and Stinson [11] concerned the case $t = 1$. Rivest's original motivation for AONT involved block ciphers. The idea is to apply a $(1, s, v)$-AONT to s plaintext blocks, where each plaintext block is treated as an element over an alphabet of size v. After the AONT is applied the resulting s blocks are then encrypted. The AONT property ensures that all s ciphertext blocks must be decrypted in order to obtain any information about any single plaintext block.

Other applications of AONT are enumerated in [3], where AONT (and "approximations" to AONT) for $t \geq 2$ were first studied. The paper [3] mainly considers the case $t = v = 2$. Additional results in this case are found in [14] and [5]; the latter paper also contains some results for $t = 2$, $v = 3$. In this paper, we study AONT for arbitrary values of v and t, obtaining our most detailed results for the case $t = 2$.

All of the above work is primarily concerned with deterministic AONT. We should also mention that randomized AONT have been studied in the context of "exposure-resilient cryptography"; see [1], [4]. However, there is no connection between the (randomized) AONT considered in that setting and the problems we study in this paper.

The definition of AONT can be rephrased in terms of the entropy function H. Let

$$\mathbf{X_1}, \ldots, \mathbf{X_s}, \mathbf{Y_1}, \ldots, \mathbf{Y_s}$$

be random variables taking on values in the finite set X. These $2s$ random variables define a (t, s, v)-AONT provided that the following conditions are satisfied:

1) $\mathsf{H}(\mathbf{Y_1}, \ldots, \mathbf{Y_s} \mid \mathbf{X_1}, \ldots, \mathbf{X_s}) = 0$.
2) $\mathsf{H}(\mathbf{X_1}, \ldots, \mathbf{X_s} \mid \mathbf{Y_1}, \ldots, \mathbf{Y_s}) = 0$.
3) For all $\mathcal{X} \subseteq \{\mathbf{X_1}, \ldots, \mathbf{X_s}\}$ with $|\mathcal{X}| = t$, and for all $\mathcal{Y} \subseteq \{\mathbf{Y_1}, \ldots, \mathbf{Y_s}\}$ with $|\mathcal{Y}| = t$, it holds that

$$\mathsf{H}(\mathcal{X} \mid \{\mathbf{Y_1}, \ldots, \mathbf{Y_s}\} \setminus \mathcal{Y}) = \mathsf{H}(\mathcal{X}). \tag{1}$$

Definition I.2. Let $\mathbb{F}_q$ be a finite field of order q. An AONT with alphabet $\mathbb{F}_q$ is *linear* if each y_i is an $\mathbb{F}_q$-linear function of $x_1, \ldots, x_s$. Then, we can write

$$\mathbf{y} = \phi(\mathbf{x}) = \mathbf{x}M^{-1} \quad \text{and} \quad \mathbf{x} = \phi^{-1}(\mathbf{y}) = \mathbf{y}M, \tag{2}$$

where M is an invertible s by s matrix with entries from $\mathbb{F}_q$.

Subsequently, when we refer to a "linear AONT", we mean the matrix M that transforms $\mathbf{y}$ to $\mathbf{x}$, as specified in (2).

The following lemma from [3] characterizes linear all-or-nothing transforms in terms of submatrices of the matrix M.

Lemma I.1. *[3, Lemma 1] Suppose that q is a prime power and M is an invertible s by s matrix with entries from $\mathbb{F}_q$.*

Then M defines a linear (t, s, q)-AONT if and only if every t by t submatrix of M is invertible.

Example I.1. *A linear $(2, 3, 3)$-AONT:*

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

Remark I.1. Any invertible s by s matrix with entries from $\mathbb{F}_q$ defines a linear (s, s, q)-AONT.

An s by s *Cauchy matrix* can be defined over $\mathbb{F}_q$ if $q \geq 2s$. Let $a_1, \ldots, a_s, b_1, \ldots, b_s$ be distinct elements of $\mathbb{F}_q$. Let $c_{ij} = 1/(a_i - b_j)$, for $1 \leq i \leq s$ and $1 \leq j \leq s$. Then $C = (c_{ij})$ is the Cauchy matrix defined by the sequence $a_1, \ldots, a_s, b_1, \ldots, b_s$. The most important property of a Cauchy matrix C is that any square submatrix of C (including C itself) is invertible over $\mathbb{F}_q$.

Cauchy matrices were briefly mentioned in [11] as a possible method of constructing 1-AONT. It was noted in [3] that, when $q \geq 2s$, Cauchy matrices immediately yield the strongest possible all-or-nothing transforms, as stated in the following theorem.

Theorem I.2. *[3, Theorem 2] Suppose q is a prime power and $q \geq 2s$. Then there is a linear transform that is simultaneously a (t, s, q)-AONT for all t such that $1 \leq t \leq s$.*

We observe that, in general, the existence of a (t, s, q)-AONT does not necessarily imply the existence of a $(t - 1, s, q)$-AONT or a $(t + 1, s, q)$-AONT.

We next review some results on general (i.e., linear or nonlinear) AONT. Let A be an N by k array whose entries are elements chosen from an alphabet X of size v. We will refer to A as an (N, k, v)-*array*. Suppose the columns of A are labelled by the elements in the set $C = \{1, \ldots, k\}$. Let $D \subseteq C$, and define A_D to be the array obtained from A by deleting all the columns $c \notin D$. We say that A is *unbiased* with respect to D if the rows of A_D contain every $|D|$-tuple of elements of X exactly $N/v^{|D|}$ times.

The following result characterizes (t, s, v)-AONT in terms of arrays that are unbiased with respect to certain subsets of columns.

Theorem I.3. *[3, Theorem 34] A (t, s, v)-AONT is equivalent to a $(v^s, 2s, v)$-array that is unbiased with respect to the following subsets of columns:*

1) $\{1, \ldots, s\}$,
2) $\{s + 1, \ldots, 2s\}$, *and*
3) $I \cup \{s+1, \ldots, 2s\} \setminus J$, *for all $I \subseteq \{1, \ldots, s\}$ with $|I| = t$ and all $J \subseteq \{s + 1, \ldots, 2s\}$ with $|J| = t$.*

An $\mathrm{OA}_\lambda(t, k, v)$ (an *orthogonal array*) is a $(\lambda v^t, k, v)$-array that is unbiased with respect to any subset of t columns. If $\lambda = 1$, then we simply write the orthogonal array as an $\mathrm{OA}(t, k, v)$.

The following corollary of Theorem I.3 is immediate.

Corollary I.4. *[3, Corollary 35] If there exists an OA$(s, 2s, v)$, then there exists a (t, s, v)-AONT for all t such that $1 \leq t \leq s$.*

For prime powers q, the existence of $(1, s, q)$-AONT has been completely determined in [11].

Theorem I.5. *[11, Corollary 2.3] There exists a linear $(1, s, q)$-AONT for all prime powers $q > 2$ and for all positive integers s.*

When $q = 2$, we have the following.

Theorem I.6. *[11, Theorem 3.5] There does not exist a $(1, s, 2)$-AONT for any integer $s > 1$.*

A. Organization of the Paper

Section II presents our new theoretical results on AONT. Section II-A concerns linear AONT with $t = 2$, where we obtain various lower bounds (constructions) and upper bounds (necessary conditions). Section II-B examines linear (t, s, q)-AONT for arbitrary values of t and shows a connection with linear t-resilient functions. Then Section II-C shows some relations between general (linear or nonlinear) AONT, orthogonal arrays and resilient functions.

In Section III, we turn to computational results. Section III-A reports the results of our exhaustive computer searches for linear $(2, q, q)$-AONT for all prime powers $q \leq 11$. Section III-B discusses our searches for a class of AONT, which we call cyclic τ-skew-symmetric AONT, for odd primes $q \leq 29$. Then Section III-C summarizes the upper and lower bounds we have obtained for AONT with $q = 2$.

Finally, Section IV provides a list of open problems.

II. New Theoretical Results

A. Linear AONT with $t = 2$

In this section, we give several results on linear $(2, s, q)$-AONT, including both constructions and bounds (necessary conditions for existence). We begin with a construction.

Theorem II.1. *Suppose $q = 2^n$, $q - 1$ is prime and $s \leq q - 1$. Then there exists a linear $(2, s, q)$-AONT over $\mathbb{F}_q$.*

Proof: Let $\alpha \in \mathbb{F}_q$ be a primitive element and let $M = (m_{r,c})$ be the s by s Vandermonde matrix in which $m_{r,c} = \alpha^{rc}$, $0 \leq r, c \leq s - 1$. Clearly M is invertible, so we only need to show that any 2 by 2 submatrix is invertible. Consider a submatrix M' defined by rows i, j and columns i', j', where $i \neq j$ and $i' \neq j'$. We have

$$\det(M') = \alpha^{ii'+jj'} - \alpha^{ij'+ji'},$$

so $\det(M') = 0$ if and only if $\alpha^{ii'+jj'} = \alpha^{ij'+ji'}$, which happens if and only if

$$ii' + jj' \equiv ij' + ji' \bmod (q - 1).$$

This condition is equivalent to

$$(i - j)(i' - j') \equiv 0 \bmod (q - 1).$$

Since $q - 1$ is prime, this happens if and only if $i = i'$ or $j = j'$. We assumed $i \neq j$ and $i' \neq j'$, so we conclude that M' is invertible. ∎

The above result requires that $2^n - 1$ is a (Mersenne) prime. Here are a couple of results on Mersenne primes from [7]. The first few Mersenne primes occur for

$$n = 2, 3, 5, 7, 13, 31, 61, 89, 107, 127.$$

At the time this paper was written, there were 49 known Mersenne primes, the largest being $2^{74207281}-1$, which was discovered in January 2016.

If we ignore the requirement that a linear AONT is an invertible matrix, then a construction for q by q matrices is easy in the case $t=2$.

Theorem II.2. *For any prime power q, there is a q by q matrix defined over $\mathbb{F}_q$ such that any 2 by 2 submatrix is invertible.*

Proof: Let $M=(m_{r,c})$ be the q by q matrix of entries from $\mathbb{F}_q$ defined by the rule $m_{r,c}=r+c$, where the sum is computed in $\mathbb{F}_q$ and the indices r and c each range over the q elements of $\mathbb{F}_q$. Consider a submatrix M' defined by rows i,j and columns i',j', where $i\neq j'$ and $i'<j'$. We have

$$\det(M')=ii'+jj'-(ij'+ji'),$$

so $\det(M')=0$ if and only if $ii'+jj'=ij'+ji'$. This condition is equivalent to

$$(i-j)(i'-j')=0,$$

which happens if and only if $i=i'$ or $j=j'$. We assumed $i\neq j$ and $i'\neq j'$, so we conclude that M' is invertible. ∎

We note that the above construction does not yield an AONT for $q>2$, because the sum of all the rows of the constructed matrix M is the all-zero vector and hence M is not invertible.

We next define a "standard form" for linear $(2,s,q)$-AONT.

Definition II.1. Suppose M is a matrix for a linear $(2,s,q)$-AONT. Clearly there can be at most one zero in each row and column of M. Then we can permute the rows and columns so that the 0's comprise the first μ entries on the main diagonal of M. If $\mu=0$, then we can multiply rows and columns by nonzero field elements so that all the entries in the first row and first column consist of 1's. If $\mu\neq 0$, we can multiply rows and columns by nonzero field elements so that all the entries in the first row and first column consist of 1's, except for the entry in the top left corner, which is a 0. Such a matrix M is said to be of *type μ standard form*.

Theorem II.3. *There is no linear $(2,q+1,q)$-AONT for any prime power $q>2$.*

Proof: Suppose M is a matrix for a linear $(2,q+1,q)$-AONT defined over $\mathbb{F}_q$. We can assume that M is in standard form. Consider the $q+1$ ordered pairs occurring in any two fixed rows of the matrix M. There are q symbols, which result in q^2 possible ordered pairs. However, the pair consisting of two zeros is ruled out, leaving q^2-1 ordered pairs. For two such ordered pairs $(i,j)^T$ and $(i',j')^T$, define $(i,j)^T\sim(i',j')^T$ if there is a nonzero element $\alpha\in\mathbb{F}_q$ such that $(i,j)^T=\alpha(i',j')^T$. Clearly $\sim$ is an equivalence relation, and there are $q+1$ equivalence classes, each having size $q-1$. We can only have at most one ordered pair from each equivalence class, so there are only $q+1$ possible pairs that can occur. Since there are $q+1$ columns, it follows that from each of these $q+1$ equivalence classes, exactly one will be chosen. Therefore, each row must contain exactly one 0 and thus M is of type $q+1$ standard form.

From the above discussion, we see that M has the following structure:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & \dots & 1 & 1\\ 1 & 0 & & & & & \\ 1 & & 0 & & & & \\ 1 & & & 0 & & & \\ \vdots & & & & \ddots & & \\ 1 & & & & & 0 & \\ 1 & & & & & & 0 \end{pmatrix}.$$

Now consider the lower right q by q submatrix M' of M. There is exactly one occurrence of each element of ${\mathbb{F}_q}^*$ in each column of M'. Now, compute the sum of all the rows in this matrix. Recall that the sum of the elements of a finite field $\mathbb{F}_q$ is equal to 0, provided that $q>2$. Therefore, regardless of the configuration of the remaining entries, the sum of the last q rows of M is the all-zero vector. Therefore, the matrix M is singular, which contradicts its being an AONT. ∎

Remark II.1. In [3, Example 16], it is shown that a linear $(2,3,2)$-AONT does not exist. This covers the exception $q=2$ in Theorem II.3.

We next obtain some structural conditions for linear $(2,q,q)$-AONT in standard form.

Lemma II.4. *Suppose M is a matrix for a linear $(2,q,q)$-AONT in standard form. Then M is of type q or type $q-1$.*

Proof: Suppose that M is of type μ standard form, where $\mu\leq q-2$. Then the last two rows of M contain no zeroes. We proceed as in the proof of Theorem II.3. The q ordered pairs in the last two rows must all be from different equivalence classes. However, there are only $q-1$ equivalence classes that do not contain a 0, so we have a contradiction. ∎

Therefore the standard form of a linear $(2,q,q)$-AONT looks like

$$M=\begin{pmatrix} 0 & 1 & 1 & 1 & \dots & 1 & 1\\ 1 & 0 & & & & & \\ 1 & & 0 & & & & \\ 1 & & & 0 & & & \\ \vdots & & & & \ddots & & \\ 1 & & & & & 0 & \\ 1 & & & & & & \chi \end{pmatrix},$$

where $\chi=0$ iff M is of type q and $\chi\neq 0$ iff M is of type $q-1$.

For the rest of this section, we will focus on linear $(2,q,q)$-AONT in type q standard form.

Definition II.2. Suppose M is a matrix for a linear $(2,q,q)$-AONT in type q standard form.. Define a linear ordering on the elements in the alphabet $\mathbb{F}_q$. If M also has the additional property that the entries in columns $3,\dots,q$ of row 2 are in increasing order (with respect to this linear order), then we say that M is *reduced*.

To summarize, the term "reduced" means that M is a linear $(2,q,q)$-AONT that satisfies the following additional properties:

- the diagonal of M consists of zeroes,

- the remaining entries in the first row and first column of M are ones, and
- the entries in columns $3, \ldots, q$ of row 2 of M are in increasing order.

Example II.1. *We present a linear $(2, 5, 5)$-AONT that is reduced with respect to the "natural" ordering $0 < 1 < 2 < 3 < 4$.*

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

Lemma II.5. *Suppose M is a matrix for a linear $(2, q, q)$-AONT in type q standard form. Then we can permute the rows and columns of M to obtain a reduced matrix M'.*

Proof: Let π be the permutation of $3, \ldots, q$, which, when applied to the columns of M, results in the entries in columns $3, \ldots, q$ of row 2 being in increasing order. Call this matrix M^π. Now, apply the same permutation π to the rows of M^π to construct the desired reduced matrix M'. ∎

B. Results on Linear AONT for Arbitrary Values of t

In this section, we present some additional results on linear AONT that hold for arbitrary values of t.

Theorem II.6. *If there exists a linear (t, s, q)-AONT with $t < s$, then there exists a linear $(t, s-1, q)$-AONT.*

Proof: Let M be a matrix for a linear (t, s, q)-AONT. Consider all the s possible $s-1$ by $s-1$ submatrices formed by deleting the first column and a row of m. We claim that at least one of these s matrices is invertible. For, if they were all noninvertible, then M would be noninvertible, by considering the cofactor expansion with respect the first column of M. ∎

We finish this section by showing that the existence of linear AONT imply the existence of certain linear resilient functions. We present the definition of resilient functions given in [6]. Let $|X| = v$. An (n, m, t, v)-*resilient function* is a function $g : X^n \to X^m$ which has the property that, if any t of the n input values are fixed and the remaining $n-t$ input values are chosen independently and uniformly at random, then every output m-tuple occurs with the same probability $1/v^m$.

Suppose q is a prime power. A (n, m, t, q)-resilient function f is *linear* if $f(x) = xM^T$ for some m by n matrix M defined over $\mathbb{F}_q$.

Theorem II.7. *Suppose there is a linear (t, s, q)-AONT. Then there is a linear $(s, s-t, t, q)$-resilient function.*

Proof: Suppose that the s by s matrix M over $\mathbb{F}_q$ gives rise to a linear (t, s, q)-AONT. Then, from Lemma I.1, every t by t submatrix of M is invertible. Construct an s by t matrix M^* by deleting any $s-t$ rows of M. Clearly any t columns of M^* are linearly independent. Let $\mathcal{C}$ be the code generated by the rows of M^* and let $\mathcal{C}'$ be the dual code (i.e., the orthogonal complement of $\mathcal{C}$). It is well-known from basic coding theory (e.g., see [8, Chapter 1, Theorem 10]) that the minimum distance of $\mathcal{C}'$ is at least $t+1$. Let N be a generating matrix for $\mathcal{C}'$. Then N is an $s-t$ by s matrix over $\mathbb{F}_q$. Since N generates a code having minimum distance at least $t+1$, the function $f(x) = xN^T$ is a a (linear) $(s, s-t, t, q)$-resilient function (for a short proof of this fact, see [13, Theorem 1]). ∎

Remark II.2. A resilient function implies the existence of a correlation-immune function (for a definition of these objects, see [10]) with certain parameters.

C. Results on General AONT for Arbitrary Values of t

In this section, we present a few results on "general" AONT (i.e., results that hold for any AONT, linear or not) for arbitrary t.

Theorem II.8. *Suppose there is a (t, s, v)-AONT. Then there is an OA(t, s, v).*

Proof: Suppose we represent an (t, s, v)-AONT by a $(v^s, 2s, v)$-array denoted by A. Let R denote the rows of A that contain a fixed $(s-t)$-tuple in the last $s-t$ columns of A. Then $|R| = v^t$. Delete all the rows of A not in R and delete the last s columns of A and call the resulting array A'. Within any t columns of A, we see that every t-tuple of symbols occurs exactly once, since the rows of A' are determined by fixing $s-t$ outputs of the AONT. But this says that A' is an OA(t, s, v). ∎

The following classical bound can be found in [2].

Theorem II.9 (Bush Bound)**.** *If there is an OA(t, s, v), then*

$$s \leq \begin{cases} v+t-1 & \text{if } t = 2, \text{ or if } v \text{ is even and } 3 \leq t \leq v \\ v+t-2 & \text{if } v \text{ is odd and } 3 \leq t \leq v \\ t+1 & \text{if } t \geq v. \end{cases}$$

Corollary II.10. *If there is a $(2, s, v)$-AONT, then $s \leq v+1$.*

We recall that we proved in Theorem II.3 that $s \leq v$ if a linear $(2, s, v)$-AONT exists; the above corollary establishes a slightly weaker result in a more general setting.

Corollary II.11. *If there is a $(3, s, v)$-AONT, then $s \leq v+2$ if $v \geq 4$ is even, and $s \leq v+1$ if $v \geq 3$ is odd.*

Lastly, we prove a generalization of Theorem II.7 which shows that any AONT (linear or nonlinear) gives rise to a resilient function. This result is based on a characterization of resilient functions which says that they are equivalent to "large sets" of orthogonal arrays. Suppose $\lambda = v^r$ for some integer r. A *large set of OA$_{v^r}(t, n, v)$* consists of v^{n-r-t} distinct OA$_{v^r}(t, n, v)$, which together contain all v^n possible n-tuples exactly once.

We will make use of the following result of Stinson [12].

Theorem II.12. *[12, Theorem 2.1] An (n, m, t, v)-resilient function is equivalent to a large set of OA$_{q^{n-m-t}}(t, n, v)$.*

Theorem II.13. *Suppose there is a (t, s, v)-AONT. Then there is an $(s, s-t, t, v)$-resilient function.*

Proof: We use the same technique that was used in the proof of Theorem II.8. Let A be the $(v^2, 2s, v)$-array representing the AONT. For any $(s-t)$-tuple $\mathbf{x}$, let $R_{\mathbf{x}}$ be

the rows of A that contain $\mathbf{x}$ in the last $s-t$ columns of A. Let $A'_{\mathbf{x}}$ denote the submatrix of A indexed by the columns in $R_{\mathbf{x}}$ and the first s columns. Theorem II.8 showed that $A'_{\mathbf{x}}$ is an $\mathrm{OA}(t,s,v)$.

Now, consider all v^{s-t} possible $(s-t)$-tuples $\mathbf{x}$. For each choice of $\mathbf{x}$, we get an $\mathrm{OA}(t,s,v)$. These v^{s-t} orthogonal arrays together contain all v^s s-tuples, since the array A is unbiased with respect to the first s columns. Thus we have a large set of $\mathrm{OA}_1(t,s,v)$. Applying Theorem II.12, this large set of OAs is equivalent to an $(s,s-t,t,v)$-resilient function (note that $m=s-t$ because $v^{s-m-t}=1$). ∎

III. Computational Results for Linear $(2,q,q)$-AONT

In this section, we describe the outcomes of some exhaustive computer searches that we have carried out to find linear $(2,q,q)$-AONT. We first performed exhaustive searches for linear $(2,q,q)$-AONT for all prime powers $q \leq 11$ and then we tested the resulting matrices for equivalence. The results are reported in Section III-A. Then we did an exhaustive search for a special subclass of linear $(2,q,q)$-AONT, for all primes $q \leq 29$; see Section III-B (these AONT are termed "cyclic τ-skew-symmetric AONT").

A. Search for Linear $(2,q,q)$-AONT For All Prime Powers $q \leq 11$

We performed exhaustive searches for linear $(2,q,q)$-AONT for all prime powers $q \leq 11$. To speed up the search, we only considered reduced $(2,q,q)$-AONT (which are a certain kind of linear AONT in type q standard form; see Definition II.2). From Lemma II.5, there is no loss of generality in assuming that a linear $(2,q,q)$-AONT of type q standard form is reduced. We also performed an exhaustive search for linear $(2,q,q)$-AONT in type $q-1$ standard form for $q \leq 11$, but we did not find any examples of these.

The results of our searches for reduced $(2,q,q)$-AONT are found in the second column of Table I. One perhaps surprising outcome is that, while there exists a (reduced) $(2,4,4)$-AONT (see Example III.1), there are no examples of linear $(2,q,q)$-AONT for $q=8,9$. A linear $(2,8,9)$-AONT is given in Example III.2 and a linear $(2,7,8)$-AONT can be constructed using Theorem II.1.

Example III.1. *A linear $(2,4,4)$-AONT, defined over the finite field $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$:*

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

Example III.2. *A linear $(2,8,9)$-AONT, defined over the finite field $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$:*

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & x & x+1 & x+2 & 2x \\ 1 & 1 & 0 & 2x+1 & x+1 & x+2 & 2 & x \\ 1 & 2x & x & 0 & x+2 & 2 & 2x+1 & x+1 \\ 1 & x+2 & 2 & x & 0 & 1 & 2x & 2x+1 \\ 1 & x+1 & x+2 & 2x & 2x+1 & 0 & 1 & 2 \\ 1 & x & x+1 & 1 & 2 & 2x+1 & 0 & x+2 \\ 1 & 2 & 2x+1 & x+1 & 1 & 2x & x & 0 \end{pmatrix}$$

TABLE I
Number of reduced and inequivalent linear $(2,q,q)$-AONT, for prime powers $q \leq 11$

q	reduced $(2,q,q)$-AONT	inequivalent $(2,q,q)$-AONT
3	2	1
4	3	2
5	38	5
7	13	1
8	0	0
9	0	0
11	21	1

Even though we generated reduced $(2,q,q)$-AONT, it is still possible that some of these matrices of a given order q are "equivalent", where the notion of equivalence is defined as follows.

Definition III.1. Suppose M and M' are linear (t,s,q)-AONT. We say that M and M' are *equivalent* if M can be transformed into M' by performing a sequence of operations of the following type:

- row and column permutations,
- multiplying a row or column by a nonzero constant, and
- transposing the matrix.

We now describe a simple process to test for equivalence of reduced $(2,q,q)$-AONT. The idea is to start with a specific reduced $(2,q,q)$-AONT, say M. Given M, we can generate all the reduced $(2,q,q)$-AONT that are equivalent to M. After doing this, it is a simple matter to take any other reduced $(2,q,q)$-AONT, say M' and see if it occurs in the list of reduced $(2,q,q)$-AONT that are equivalent to M.

The algorithm presented in Figure 1 generates all the reduced $(2,q,q)$-AONT that are equivalent to M. After executing the first five steps, we have a list of q^2-q reduced $(2,q,q)$-AONT, each of which is equivalent to M (this includes M itself). After transposing the original matrix, we repeat the same five steps, which gives q^2-q additional equivalent AONT. The result is a list of $2q^2-2q$ equivalent AONT, but of course there could be duplications in the list.

We have used this algorithm to determine the number of inequivalent $(2,q,q)$-AONT for prime powers $q \leq 11$. We started with the list of all the reduced $(2,q,q)$-AONT and then we eliminated equivalent matrices using our algorithm as described above. The results are presented in the third column of Table I.

B. Cyclic τ-skew-symmetric AONT

It does not seem feasible to continue the exhaustive searches beyond $q=11$. Therefore, it is helpful to identify a particular subclass of $(2,q,q)$-AONT in which exhaustive searches can be performed for larger values of q. We observed that, for prime orders $3,5,7,11$, there exists a $(2,q,q)$-AONT having a very interesting structure, which we define now.

Definition III.2. Let M be a matrix for a $(2,q,q)$-AONT in type q standard form (we do not require that M is reduced).

1. Pick two distinct rows r_1, r_2. Interchange rows 1 and r_1 of M and interchange rows 2 and r_2 of M. Then interchange columns 1 and r_1 and interchange columns 2 and r_2 of the resulting matrix.
2. Multiply columns $2, \ldots, q$ by constants to get $(0\,1\,1\,\cdots\,1)$ in the first row.
3. Multiply rows $2, \ldots, q$ by constants to get $(0\,1\,1\,\cdots\,1)^T$ in the first column.
4. Permute columns $3, \ldots, q$ so the entries in row 2 in these columns are in increasing order (there is a unique permutation π that does this).
5. Apply the same permutation π to rows $3, \ldots, q$.
6. Transpose M and apply the first five steps to the transposed matrix.

Fig. 1. Generating the reduced $(2, q, q)$-AONT that are equivalent to a given reduced $(2, q, q)$-AONT, M

Let $\tau \in \mathbb{F}_q \setminus \{0\}$. We say that M is *τ-skew-symmetric* if, for any pair of cells (i, j) and (j, i) of M, where $2 \leq i, j \leq q$ and $i \neq j$, it holds that $m_{ij} + m_{ji} = \tau$.

Furthermore, we say that M is *cyclic* if M_1 (the lower right $q-1$ by $q-1$ submatrix of M) is a cyclic matrix.

Another way to define the τ-skew-symmetric property is to say that $M_1 + {M_1}^T = \tau(J - I)$, where J is the all-ones matrix and I is the identity matrix. Notice that the τ-skew-symmetric property implies that the matrix M_1 contains no entries equal to τ, since the only zero entries are on the diagonal.

Example II.1 depicts a cyclic 4-skew-symmetric $(2, 5, 5)$-AONT. This example also happens to be reduced, but this is not a required property.

After observing that cyclic τ-skew-symmetric AONT exist for prime orders $3, 5, 7, 11$, we decided to perform a specialized search for cyclic τ-skew-symmetric AONT for larger prime orders. It turns out that we can fix the value of τ to be any desired nonzero value, as a consequence of the following lemma.

Theorem III.1. *If there is a cyclic τ_0-skew-symmetric $(2, q, q)$-AONT for some $\tau_0 \in \mathbb{F}_q \setminus \{0\}$, then there is a cyclic τ_1-skew-symmetric $(2, q, q)$-AONT for all $\tau_1 \in \mathbb{F}_q \setminus \{0\}$.*

Proof: We show that, for any nonzero values τ_0 and τ_1, a τ_0-skew-symmetric AONT can be used to obtain a 1-skew-symmetric AONT, and a τ_1-skew-symmetric AONT can be derived from a 1-skew-symmetric AONT. For every $\tau_0 \neq 0, 1$, we can multiply all the columns, other than the first column, by τ_0^{-1}, and then multiply the first row by τ_0 in order to return the matrix to type q standard form. This way, we get a cyclic 1-skew-symmetric AONT because

1) all the elements in the cyclic part are multiplied by a constant factor, so that part remains cyclic, and
2) $\tau_0^{-1}(m_{ij} + m_{ji}) = 1$ for all $i \neq j$ where $2 \leq i, j \leq q$.

Then, given a cyclic 1-skew-symmetric AONT, all of its columns except for the first one can be multiplied by τ_1, and then the first row can be multiplied by τ_1^{-1}, to get a cyclic τ_1-skew-symmetric AONT. ∎

As mentioned above, we are searching for cyclic τ-skew-symmetric AONT for odd prime orders q. Because the AONT M is cyclic, we only need to construct the first row of M_1. However, the τ-skew-symmetric property forces some additional structure.

Lemma III.2. *Suppose we denote the last $q-2$ entries in the first row of M_1 in the form of a vector $(a_1, \ldots, a_{q-2})$. Then this vector satisfies the following properties:*

1) $a_{(q-1)/2} = \tau/2$,
2) $a_i + a_{q-1-i} \equiv \tau \pmod q$, *for* $i = 1, \ldots, (q-3)/2$, *and*
3) $(a_1, \ldots, a_{q-2})$ *is a permutation of the set* $\mathbb{Z}_q \setminus \{0, \tau\}$.

The first two properties enumerated in Lemma III.2 establish that the first row of M_1 is completely determined by the values $a_1, \ldots, a_{(q-3)/2}$.

Example III.3. *Consider $q = 7$ and suppose $\tau = 6$. Suppose we have chosen $a_1 = 2$ and $a_2 = 5$. Then the first row of M_1 would be* $0\quad 2\quad 5\quad 3\quad 1\quad 4$. *The matrix M would be*

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

As a consequence of the above discussion, the search algorithm only needs to generate and check matrices M that arise from a list of $(q-3)/2$ values $a_1, \ldots, a_{(q-3)/2}$. We will take $\tau = q - 1$, which we can do without loss of generality. Then it follows from Lemma III.2 that

$$\{a_i : 1 \leq i \leq q-2\} = \{1, \ldots, q-2\}.$$

We can partition $\{1, \ldots, q-2\} \setminus \{(q-1)/2\}$ into two sets A_1 and A_2, each of size $(q-3)/2$, such that $a \in A_1$ if and only $q - 1 - a \in A_2$, for all $a \in \{1, \ldots, q-2\} \setminus \{(q-1)/2\}$.

It is easy to see that there are $2^{(q-3)/2}$ possible partitions to consider. However, because the transpose of a τ-skew-symmetric AONT is also a τ-skew-symmetric AONT, we can stipulate without loss of generality that any particular element is in A_1. We decided to specify that $(q-3)/2 \in A_1$. This reduces the number of possible partitions to $2^{(q-5)/2}$.

Now, given a partition determined by A_1 and A_2, we would consider the $((q-3)/2)!$ permutations of A_1. A permutation of A_1 determines a permutation of A_2, in view of property 2 from Lemma III.2.

In summary, the number of possible vectors $(a_1, \ldots, a_{q-2})$ to be tested is

$$2^{(q-5)/2} \times \left(\frac{q-3}{2}\right)!$$

Example III.4. *Let $q = 7$ and $\tau = 6$. We assume that $2 \in A_1$. There are $2^{(7-5)/2} = 2$ partitions to consider, namely $A_1 = \{1, 2\}$, $A_2 = \{4, 5\}$ and $A_1 = \{2, 5\}$, $A_2 = \{1, 4\}$. For each*

TABLE II
CYCLIC $(q-1)$-SKEW-SYMMETRIC AONT FOR ODD PRIMES q, $5 \le q \le 29$.

q	$a_1, \ldots, a_{(q-3)/2}$												
5													1
7												2	5
11										1	4	8	3
13									11	3	10	5	4
17							7	1	14	6	3	5	4
19						8	6	7	13	3	2	17	14
23				7	14	17	2	6	3	4	10	9	1
29	7	11	1	4	12	10	20	5	25	22	9	2	13

partition, there are $\left(\frac{7-3}{2}\right)! = 2$ *possible permutations. There are therefore four possible first rows of* M_1 *to consider:*

0	1	2	3	4	5
0	2	1	3	5	4
0	2	5	3	1	4
0	5	2	3	4	1

It turns out that exactly one of these possible first rows generates an AONT, namely

$$0 \quad 2 \quad 5 \quad 3 \quad 1 \quad 4.$$

The matrix M *presented in Example III.3 is the resulting AONT.*

We implemented his algorithm and we ran it on the CrySP RIPPLE Facility using 160 hyperthreads on 80 physical cores, for $q = 3, 5, 7, 11, 13, 17, 19, 23$ and 29. For each of these values of q, Table II lists values $a_1, \ldots, a_{(q-3)/2}$ which give rise to cyclic $(q-1)$-skew-symmetric AONT.

For the case $q = 29$, the search took about five weeks. Based on the number of possible first rows to be searched, the current approach would take about 28 times as long to handle the next case $q = 31$, which makes such a search too costly.

For each q, we found all the solutions, and then tested the resulting AONT for equivalence. It turned out that, up to equivalence, there was exactly one $(q-1)$-skew-symmetric $(2, q, q)$-AONT for each value $q \in \{3, 5, 7, 11, 13, 17, 19, 23, 29\}$.

Finally, we should note that exhaustive searches showed that there are no examples of τ-skew-symmetric $(2, q, q)$-AONT for $q = 16, 25, 27$.

C. Summary of Existence Results for linear $(2, s, q)$-AONT

Given a prime power q, define

$$\mathcal{S}(q) = \{s : \text{there exists a linear } (2, s, q)\text{-AONT}\}.$$

From Remark I.1, we have that $2 \in \mathcal{S}(q)$, so $\mathcal{S}(q) \neq \emptyset$. Also, from Theorem II.3, Remark II.1 and Theorem II.6, there exists a maximum element in $\mathcal{S}(q)$, which we will denote by $M(q)$. In view of Theorem II.6, we know that a linear $(2, s, q)$-AONT exists for all s such that $2 \le s \le M(q)$. We summarize upper and lower bounds on $M(q)$ in Table III.

TABLE III
UPPER AND LOWER BOUNDS ON $M(q)$

bound	authority
$\lfloor q/2 \rfloor \le M(q) \le q$ for all prime powers q	Theorem I.2 and II.3
$M(q) \ge q - 1$ if $q = 2^n$ and $q - 1$ is prime	Theorem II.1
$M(q) = q$ for $q = 5, 7, 11, 13, 17, 19, 23, 29$	Table II
$M(3) = 3$	Example I.1
$M(4) = 4$	Example III.1
$M(8) = 7$	Theorem II.1, computer search
$M(9) = 8$	Example III.2, computer search

IV. OPEN PROBLEMS

In this paper, we have begun a study of t-all-or-nothing transforms over alphabets of arbitrary size. There are many interesting open problems suggested by the results in this paper. We list some of these now.

1) Are there infinitely many primes p for which there exist linear $(2, p, p)$-AONT?
2) Are there infinitely many primes p for which there exist (cyclic) skew-symmetric $(2, p, p)$-AONT?
3) Are there any prime powers $q = p^i > 4$ with $i \ge 2$ for which there exist linear $(2, q, q)$-AONT?
4) As mentioned in Section III, we performed exhaustive searches for linear $(2, q, q)$-AONT in type $q-1$ standard form, for all primes and prime powers $q \le 11$, and found that no such AONT exist. We ask if there exists any linear $(2, q, q)$-AONT in type $q - 1$ standard form.
5) For $p = 3, 5$, there are easily constructed examples of *symmetric* linear $(2, p, p)$-AONT in standard form (where "symmetric" means that $M = M^T$). But there are no symmetric examples for $p = 7$ or 11. We ask if there exists any symmetric linear $(2, p, p)$-AONT in standard form for a prime $p > 5$.
6) Theorem II.6 showed that a linear $(t, s-1, q)$-AONT exists whenever a linear (t, s, q)-AONT exists. Does an analogous result hold for arbitrary (linear or nonlinear) AONT?
7) We proved in Theorem II.3 that, if a linear $(2, s, q)$-AONT exists, then $s \le q$. On the other hand, for

arbitrary (linear or nonlinear) $(2, s, v)$-AONT, we were only able to show that $s \leq v + 1$ (Corollary II.10). Can this second bound be strengthened to $s \leq v$, analogous to the linear case?

8) In the case $t = 3$, we have one existence result (Theorem I.2) and one necessary condition (Corollary II.11). What additional results can be proven about existence or nonexistence of $(3, s, v)$-AONT?

ACKNOWLEDGEMENTS

This work benefitted from the use of the CrySP RIPPLE Facility at the University of Waterloo.

REFERENCES

[1] R. Canetti, Y. Dodis, S. Halevi, E. Kushilevitz and A. Sahai. Exposure-resilient functions and all-or-nothing transforms. *Lecture Notes in Computer Science* **1807** (2000), 453–469 (EUROCRYPT 2000).

[2] C.J. Colbourn and J.H. Dinitz, eds. *The CRC Handbook of Combinatorial Designs, Second Edition*, CRC Press, 2006.

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

[4] Y. Dodis, A. Sahai and A. Smith. On perfect and adaptive security in exposure-resilient cryptography. *Lecture Notes in Computer Science* **2045** (2001), 301–324 (EUROCRYPT 2001).

[5] N. Nasr Esfahani and D.R. Stinson. Computational results on invertible matrices with the maximum number of invertible 2×2 submatrices. *Australasian Journal of Combinatorics* **69** (2017), 130–144.

[6] K. Gopalakrishnan and D.R. Stinson. Three characterizations of non-binary correlation-immune and resilient functions. *Designs, Codes and Cryptography* **5** (1995), 241–251.

[7] Great Internet Mersenne Prime Search. https://www.mersenne.org. Page retrieved Feb. 20, 2017.

[8] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

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

[10] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic application. *IEEE Trans. Inform. Theory*, **IT-30** (1984), 776–780.

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

[12] D.R. Stinson. Resilient functions and large sets of orthogonal arrays. *Congressus Numerantium* **92** (1993), 105–110.

[13] D.R. Stinson and J.L. Massey. An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions. *Journal of Cryptology* **8** (1995), 167–173.

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

Navid Nasr Esfahani is a Ph.D. student in the Cheriton School of Computer Science at the University of Waterloo. He received his B.Sc. degree from the Isfahan University of Technology, Isfahan, Iran, and his M.Sc. degree from the University of Manitoba, Winnipeg, Canada. Currently, he is a member of the Cryptography, Security, and Privacy (CrySP) research group, working under the supervision of Prof. Stinson. His research interests include combinatorics, cryptography, information theoretic security, and privacy.

Ian Goldberg is a Professor and University Research Chair in the Cheriton School of Computer Science at the University of Waterloo, where he is a founding member of the Cryptography, Security, and Privacy (CrySP) research group. He holds a Ph.D. from the University of California, Berkeley, where he discovered serious weaknesses in a number of widely deployed security systems, including those used by cellular phones and wireless networks. He also studied systems for protecting the personal privacy of Internet users, which led to his role as Chief Scientist at Zero-Knowledge Systems, a Montreal-based startup. His research currently focuses on developing usable and useful technologies to help Internet users maintain their security and privacy. He is a Distinguished Member of the Association for Computing Machinery and a winner of the Early Researcher Award, the Outstanding Young Computer Science Researcher Award, and the Electronic Frontier Foundation's Pioneer Award.

Douglas R. Stinson received the B.Math. degree from the University of Waterloo, Waterloo, ON, Canada, in 1978, the M.Sc. degree from The Ohio State University, Columbus, in 1980, and the Ph.D. degree in combinatorics and optimization from the University of Waterloo in 1981. He previously held academic positions at the University of Manitoba and the University of Nebraska-Lincoln. Currently he holds the position of University Professor in the David R. Cheriton School of Computer Science at the University of Waterloo and he is a Fellow of the Royal Society of Canada. His research interests include cryptography and computer security, combinatorics and coding theory, and applications of discrete mathematics in computer science. He is the author of over 300 research papers as well as several books, including the popular textbook Cryptography: Theory and Practice.