Designs, Codes and Cryptography, 22, 133–138, 2001.


# Something About All or Nothing (Transforms)

D. R. STINSON dstinson@cacr.math.uwaterloo.ca
*Department of Combinatorics and Optimization, University of Waterloo, Waterloo Onatrio, N2L 3G1, Canada*

**Communicated by:** S. Gao

*Received September 23, 1998; Revised June 25, 1999; Accepted July 12, 1999*

**Abstract.** In this short note, we study all-or-nothing transforms, which were recently proposed by Rivest as a mode of operation for block ciphers. We study transforms of this type that provide unconditional security. A simple construction for linear transforms is given, and some existence and non-existence results for general transforms are derived from a combinatorial characterization of these objects.

## 1. Introduction

Let $X$ be a finite set, called an *alphabet*. Let $s$ be a positive integer, and suppose that $\phi$: $X^s \rightarrow X^s$. We will think of $\phi$ 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 $1 \leq i \leq s$. Informally, the function $\phi$ is an *all-or-nothing transform* provided that the following properties are satisfied:

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

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

The above definition can be rephrased in terms of the entropy function, $\mathsf{H}$, as follows. Let $X_1, \ldots, X_s, Y_1, \ldots, Y_s$ be random variables taking on values in the finite set $X$. (The variables $X_1, \ldots, X_s$ need not be independent, or uniformly distributed.) Then these $2s$ random variables define an AONT provided that the following conditions are satisfied:

1. $\mathsf{H}(Y_1, \ldots, Y_s \mid X_1, \ldots, X_s) = 0$.
2. $\mathsf{H}(X_1, \ldots, X_s \mid Y_1, \ldots, Y_s) = 0$.
3. $\mathsf{H}(X_i \mid Y_1, \ldots, Y_{j-1}, Y_{j+1}, \ldots, Y_s) = \mathsf{H}(X_i)$ for all $i$ and $j$ such that $1 \leq i \leq s$ and $1 \leq j \leq s$ .

All-or-nothing transforms were defined in [6] by Rivest. Our definition differs from Rivest's only in that we are studying transforms that are unconditionally secure, as compared to the computationally secure schemes considered in [6].

Rivest suggests using all-or-nothing transforms as a preprocessing step for encrypting data with a block cipher. Suppose that $e_K$ is the encryption function for a block cipher, where $K$ is the secret key. We will regard $e_K$ as a bijective function defined on a finite alphabet

$X$. (For example, in the case of DES, $X = \{0,1\}^{64}$.) Now, suppose we are given $s$ blocks of plaintext, say $x_1, \ldots, x_s$, where $x_1, \ldots, x_s \in X$, and a publicly known $(s, v)$-AONT, $\phi$, where $v = |X|$. The *package transform* consists of the following two steps:

1. Compute $(y_1, \ldots, y_s) = \phi(x_1, \ldots, x_s)$.
2. Compute $z_i = e_K(y_i)$, for $1 \le i \le s$.

The $s$ blocks of ciphertext, $(z_1, \ldots, z_s)$, are transmitted to the receiver. The receiver can decrypt these ciphertexts to obtain $(y_1, \ldots, y_s)$, and then use the public inverse transform $\phi^{-1}$ to restore the original plaintexts, $(x_1, \ldots, x_s)$.

The use of the all-or-nothing transform affords a certain amount of addtional security (over and above the block cipher being used) because it requires an adversary to decrypt all $s$ blocks of ciphertext (by means of an exhaustive key search, say) in order to determine any one block of plaintext. As such, it can be thought of as an additional mode of operation that could be used instead of the usual ECB, CFB, CBC or OFB modes (see, for example, [5, Section 7.2.2]).

## 2. Linear Transforms

Let $\mathbb{F}_q$ be a finite field of order $q$. An $(s, q)$-AONT with alphabet $\mathbb{F}_q$ is *linear* if each $y_i$ is an $\mathbb{F}_q$-linear function of $x_1, \ldots, x_s$. The following theorem provides an easy method of constructing linear all-or-nothing transforms.

THEOREM 2.1 *Suppose that $q$ is a prime power, and $M$ is an invertible $s$ by $s$ matrix with entries from $\mathbb{F}_q$, such that no entry of $M$ is equal to 0. Then the function $\phi$: $(\mathbb{F}_q)^s \to (\mathbb{F}_q)^s$ defined by $\phi(\mathbf{x}) = \mathbf{x}M^{-1}$ is a linear $(s, q)$-AONT.*

*Proof.* If $\mathbf{y} = \mathbf{x}M^{-1}$, then $\mathbf{x} = \mathbf{y}M$. Since every entry of $M$ is non-zero, each $x_j$ $(1 \le j \le s)$ depends on all $s$ of the $y_i$'s. More precisely, if $n-1$ of the $y_i$'s are fixed and the remaining value, say $y_{i_0}$, is allowed to vary, then any $x_j$ can take on any possible value in $\mathbb{F}_q$, depending on the value of $y_{i_0}$. ∎

We give some examples to illustrate. Our first application uses Hadamard matrices. A *Hadamard matrix* of order $n$ is an $n$ by $n$ matrix, with entries in the set $\{1, -1\}$, such that $HH^T = n\,I_n$, where $I_n$ is an $n$ by $n$ identity matrix and the matrix product is computed over the real numbers. For a summary of information on Hadamard matrices, see [3, §IV.24]. (We note here that a Hadamard matrix can exist only if $n = 1$, $n = 2$, or $n \equiv 0 \bmod 4$. It is conjectured that Hadamard matrices exist for all orders $n \equiv 0 \bmod 4$. Currently the smallest $n \equiv 0 \bmod 4$ for which a Hadamard matrix of order $n$ is not known to exist is $n = 428$.)

COROLLARY 2.2 *Suppose $p > 2$ is prime, $s \equiv 0 \bmod 4$, and there exists a Hadamard matrix of order $s$. Then there exists a linear $(s, p)$-AONT.*

*Proof.* Let $H$ be a Hadamard matrix of order $s$, and define $M$ to be the matrix formed by reducing the entries of $H$ modulo $p$. Then the matrix $M^{-1} = c\,M^T$, where $c = s^{-1} \bmod p$. Hence, $M$ satisfies the conditions of Theorem 2.1 and the result follows. ∎

It is straightforward to find applications of Theorem 2.1 that will work in any finite field (except $\mathbb{F}_2$; see Section 2.1). This can be done, for example, by taking $M$ to be a Vandemonde matrix (see [4, p. 116]) or a Cauchy matrix (see [4, p. 323]). Implementing the resulting transforms, however, requires a substantial amount of finite field arithmetic and might be too slow for a practical application. Therefore, we describe a construction due to J. Bierbrauer that is more efficient computationally.

COROLLARY 2.3 [1] *Suppose $q > 2$ is a prime power and $s$ is a positive integer. Then there exists a linear $(s, q)$-AONT.*

*Proof.* Let $q = p^k$ where $p$ is prime and $k$ is a positive integer. Let $\lambda \in \mathbb{F}_q$ be such that $\lambda \notin \{s - 1 \bmod p, s - 2 \bmod p\}$ (this can be done since $q > 2$). Since $\lambda \neq s - 1 \bmod p$, we can define $\gamma = (s - 1 - \lambda)^{-1}$. Now, define $M$ to be the following symmetric matrix:

$$M = \begin{pmatrix} 1-\gamma & -\gamma & -\gamma & \dots & -\gamma & \gamma \\ -\gamma & 1-\gamma & -\gamma & \dots & -\gamma & \gamma \\ -\gamma & -\gamma & 1-\gamma & \dots & -\gamma & \gamma \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -\gamma & -\gamma & -\gamma & \dots & 1-\gamma & \gamma \\ \gamma & \gamma & \gamma & \dots & \gamma & -\gamma \end{pmatrix}.$$

It is straightforward to verify that $M$ is invertible; indeed, we have

$$M^{-1} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 1 & 1 & 1 & \dots & 1 & \lambda \end{pmatrix}.$$

We see that $\gamma \neq 1$ because $\lambda \neq s - 2 \bmod p$. Therefore, $M$ satisfies the conditions of Theorem 2.1 and the result follows. ∎

The transform (and inverse transform) resulting from Corollary 2.3 can be implemented very efficiently. Given $\mathbf{x}$, we can compute $\mathbf{y}$ as follows:

1. For $1 \leq i \leq s - 1$, compute $y_i = x_i + x_s$.

2. Compute $x_s = x_1 + \cdots + x_{s-1} + \lambda x_s$.

Further, given $\mathbf{y}$, we can compute $\mathbf{x}$ as follows:

1. Compute $y_s = \gamma(x_1 + \cdots + x_{s-1} - y_s)$.

2. For $1 \leq i \leq s - 1$, compute $x_i = y_i - x_s$.

### 2.1. *Linear Transforms over* $\mathbb{F}_2$

It is clear that we cannot satisfy the conditions of Theorem 2.1 when $q = 2$ and $s \geq 2$, since the matrix in which all entries equal 1 is not invertible. We can come fairly close, however. Suppose that $s$ is even, and let $M$ be the matrix having all diagonal entries equal to 0 and all off-diagonal entries equal to 1. Then $M^{-1} = M$, where $M$ is considered as a matrix over $\mathbb{F}_2$. In this example, each $x_j$ will depend on all the $y_i$'s except for $y_j$.

This transform (and its inverse) is also particularly efficient to implement. We can first compute

$$t = x_1 + \cdots + x_s,$$

and then compute

$$y_i = t + x_i$$

for $1 \leq i \leq s$. The total number of addition operations required (over $(\mathbb{F}_2)^s$) is $2s - 1$.

## 3. General Transforms

In this section, we give a combinatorial characterization of general (i.e., linear or nonlinear) AONT over an arbitrary alphabet. We then use this characterization to provide some existence and nonexistence resuilts.

Let $A$ be an $N$ by $k$ array whose entries are elements chosen from an alphabet $X$ of order $v$. 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 AONT in terms of arrays that are unbiased with respect to certain subsets of columns.

THEOREM 3.1 *An $(s, v)$-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. $\{i\} \cup \{s + 1, \ldots, 2s\} \setminus \{s + j\}$, *for all* $1 \leq i \leq s$ *and all* $1 \leq j \leq s$.

*Proof.* Let $A$ be the hypothesized $(v^s, 2s, v)$-array on alphabet $X$. We construct $\phi$: $X^s \rightarrow X^s$ as follows: for each row $(x_1, \ldots, x_{2s})$ of $A$, define

$$\phi(x_1, \ldots, x_s) = (x_{s+1}, \ldots, x_{2s}).$$

The function $\phi$ is easily seen to be an $(s, v)$-AONT.

Conversely, suppose $\phi$ is an $(s, v)$-AONT. Define an array $A$ whose rows consist of all $v^s$ $2s$-tuples $(x_1, \ldots, x_{2s})$, where $\phi(x_1, \ldots, x_s) = (x_{s+1}, \ldots, x_{2s})$. $A$ is the desired $(v^s, 2s, v)$-array. ∎

An OA$(s, k, v)$ (*orthogonal array*) is a $(v^s, k, v)$-array that is unbiased with respect to any subset of $s$ columns. The following corollary of Theorem 3.1 is immediate.

COROLLARY 3.2 *If there exists an OA*$(s, 2s, v)$*, then there exists an* $(s, v)$*-AONT.*

In the case $s = 2$, the converse also follows from Theorem 3.1. Thus, we have

COROLLARY 3.3 *There exists an OA*$(2, 4, v)$ *if and only if there there exists a* $(2, v)$*-AONT.*

An OA$(2, 4, v)$ is equivalent to a pair of orthogonal latin squares of order $v$ (see, for example, [3, §II.2]). It is a well-known result of Bose, Shrikhande and Parker [2]) that a pair of orthogonal latin squares of order $v$ exist if and only if $v \neq 2, 6$. Thus we have the following.

THEOREM 3.4 *There exists a* $(2, v)$*-AONT if and only if* $v \neq 2, 6$.

We now consider the case $v = 2$. We earlier noted that there is no linear $(s, 2)$-AONT. We extend this result to general AONT, as follows.

THEOREM 3.5 *There does not exist an* $(s, 2)$*-AONT for any* $s \geq 2$.

*Proof.* For $s = 2$, the result was already shown in Theorem 3.4. Hence, we suppose that $s \geq 3$. Suppose there exists a $(2^s, 2s, 2)$-array, $A$, on alphabet $\{0, 1\}$, that satisfies the properties enumerated in Theorem 3.1. Since $A$ is unbiased with respect to its last $s$ columns, it follows that $A$ contains four rows of the following form:

| $1$ | $2$ | $\cdots$ | $s$ | $s+1$ | $s+2$ | $s+3$ | $\cdots$ | $2s$ |
|---|---|---|---|---|---|---|---|---|
| $c_1$ | $c_2$ | $\cdots$ | $c_s$ | 0 | 0 | 0 | $\cdots$ | 0 |
| | | | | 0 | 1 | 0 | $\cdots$ | 0 |
| | | | | 1 | 0 | 0 | $\cdots$ | 0 |
| | | | | 1 | 1 | 0 | $\cdots$ | 0 |

where $c_1, \ldots, c_s$ are column binary 4-tuples. For $1 \leq j \leq s$, denote $c_j = (c_j^1, c_j^2, c_j^3, c_j^4)^T$. Now, let $1 \leq j \leq s$. Since $A$ is unbiased with respect to the set of columns $\{j, s+2, \ldots, 2s\}$, it follows that $c_j^1 \neq c_j^3$ and $c_j^2 \neq c_j^4$. Similarly, since $A$ is unbiased with respect to the set of columns $\{j, s+1, s+3, \ldots, 2s\}$, it follows that $c_j^1 \neq c_j^2$ and $c_j^3 \neq c_j^4$. Therefore it follows that

$$c_j \in \left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

for all $1 \leq j \leq s$. From this, we see that $A$ is not unbiased in the set of columns $\{1, \ldots, s\}$. Hence, an $(s, 2)$-AONT does not exist. ∎

## 4. Randomized Transforms

Rivest suggests in [6] that all-or-nothing transforms are most useful when they are randomized, in part to prevent known- or chosen-plaintext attacks. Randomization can be easily accomplished in the unconditionally secure model we are studying. We refer to the package transform as described in Section 1. Assume that we have a publicly known $(s, v)$-AONT defined over an alphabet $X$, as before. Let $r < s$. Given $r$ plaintext blocks $x_1, \ldots, x_r \in X$, we will choose $s-r$ values $x_{r+1}, \ldots, x_s \in X$ uniformly at random. Then proceed as before.

The randomness introduced into the encryption process yields a data expansion of $s/r$. However, on the positive side, it makes it unlikely that identical sequences of $r$ blocks of plaintext encrypt to the same $s$ blocks of ciphertext: the probability of this happening is $v^{s-r}$. This quantity can be made as small as desired, for fixed $v$ and $r$, by choosing $s$ sufficiently large.

## Acknowledgments

I would like to thank the referee for reading the manuscript carefully and for providing several helpful suggestions. Also, thanks to Jürgen Bierbrauer for his comments, and especially for providing the construction used in Corollary 2.3.

The author's research is supported by the Natural Sciences and Engineering Research Council of Canada through the following grants: NSERC-IRC #216431-96 and NSERC-RGPIN #203114-98.

## References

1. J. Bierbrauer, Private communication, January 13, 1999.
2. R. C. Bose, S. S. Shrikhande and E. T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.*, Vol. 12 (1960) pp. 189–203.
3. C. J. Colbourn and J. H. Dinitz, eds., *The CRC Handbook of Combinatorial Designs*, CRC Press (1996).
4. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland (1977).
5. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press (1996).
6. R. L. Rivest, All-or-nothing encryption and the package transform, In *Fast Software Encryption 1997*, (E. Biham, ed.), Lecture Notes in Computer Science, 1267 (1997) pp. 210–218.