Bounds for resilient functions and orthogonal arrays

Extended Abstract

Jürgen Bierbrauer[1], K. Gopalakrishnan[2] and D. R. Stinson[2,3]

[1] Mathematisches Institut der Universität
Im Neuenheimer Feld 288, 69120 Heidelberg, Germany
[2] Department of Computer Science and Engineering
University of Nebraska - Lincoln, Lincoln, NE 68588
[3] Center for Communication and Information Science
University of Nebraska - Lincoln, Lincoln, NE 68588

Abstract. Orthogonal arrays (OAs) are basic combinatorial structures, which appear under various disguises in cryptology and the theory of algorithms. Among their applications are universal hashing, authentication codes, resilient and correlation-immune functions, derandomization of algorithms, and perfect local randomizers. In this paper, we give new bounds on the size of orthogonal arrays using Delsarte's linear programming method. Then we derive bounds on resilient functions and discuss when these bounds can be met.

1 Introduction

Orthogonal arrays (OAs) are basic combinatorial structures. They and some natural generalizations appear under various disguises in cryptology and the theory of algorithms. Among the applications we mention **universal hashing** and **authentication codes**, **resilient** and **correlation-immune functions**, **derandomization of algorithms** and **perfect local randomizers**.

Here, we concentrate on resilient functions, two possible applications of which are mentioned in [2] and [6]. The first application concerns the generation of shared random strings in the presence of faulty processors. The second involves renewing a partially leaked cryptographic key (one setting in which this would be relevant is quantum cryptography [1]). Correlation-immune functions are used in stream ciphers as combining functions for running-key generators that are resistant to a correlation attack (see, for example, Rueppel [13]).

In this abstract, we give new bounds on the size of orthogonal arrays using Delsarte's linear programming method. Then we derive bounds on resilient functions and discuss when these bounds can be met. Complete proofs of all results, as well as further related results, can be found in the full paper [10].

The concept of binary resilient functions was introduced and studied in the papers Chor *et al* [6], Bennett *et al* [2], Stinson [14] and Friedman [8]. An (n, m, t)-resilient function is a function $f : \{0,1\}^n \longrightarrow \{0,1\}^m$ such that every possible output m-tuple is equally likely to occur when the values of t arbitrary inputs are fixed by an opponent and the remaining $n-t$ input bits are chosen independently at random. More formally, the property can be stated as follows: For every t-subset $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$, for every choice of $z_j \in \{0,1\} (1 \le j \le t)$, and for every $(y_1, \ldots, y_m) \in \{0,1\}^m$, we have

$$Pr(f(x_1, \ldots, x_n) = (y_1, \ldots, y_m) | x_{i_j} = z_j, 1 \le j \le t) = \frac{1}{2^m}.$$

A basic problem is to maximize t given m and n, i.e., to determine the largest value of t such that an (n, m, t)-resilient function exists. It was proved by Chor et al in [6] that an $(n, 2, t)$ - resilient function exists if and only if $t < \lfloor \frac{2n}{3} \rfloor$. The corresponding question for $m = 3$ or higher remained open. As a consequence of our new bounds, we have completed the determination of the optimal resiliency of resilient functions with $m = 3$, and we have also done most of the cases for $m = 4$.

Here are some examples of resilient functions from [6] (all addition is modulo 2):

(1) $m = 1$, $t = n - 1$. Define $f(x_1, \ldots, x_n) = x_1 + \ldots + x_n$.
(2) $m = n - 1$, $t = 1$. Define $f(x_1, \ldots, x_n) = (x_1 + x_2, x_2 + x_3, \ldots, x_{n-1} + x_n)$.
(3) $m = 2$, $n = 3h$, $t = 2h - 1$. Define

$$f(x_1, \ldots, x_{3h}) = (x_1 + \ldots + x_{2h}, x_{h+1} + \ldots + x_{3h}).$$

2 Orthogonal Arrays

An *orthogonal array* $OA_\lambda(t, k, v)$ is a $\lambda v^t \times k$ array of v symbols, such that in any t columns of the array every one of the possible v^t ordered pairs of symbols occurs in exactly λ rows. Usually t is referred to as the *strength* of the orthogonal array, k is called the number of *factors*, v is called the number of *levels* and λ is called the *index* of the orthogonal array. An orthogonal array is said to be *simple* if no two rows are identical. Of course, an array with $\lambda = 1$ is simple. In this paper, we consider only simple arrays.

A *large set of orthogonal arrays* $LOA_\lambda(t, k, v)$ is a set of v^{k-t}/λ simple arrays $OA_\lambda(t, k, v)$ such that every possible k-tuple of symbols occurs in exactly one of the orthogonal arrays in the set.

The proof of the following theorem, which elucidates the connection between resilient functions and orthogonal arrays, can be found in [14].

Theorem 1. *An (n, m, t) - resilient function is equivalent to a large set of orthogonal arrays $LOA_{2^{n-m-t}}(t, n, 2)$.*

The correspondence between resilient functions and orthogonal arrays is as follows. For any $m-$tuple $(y_1, \ldots, y_m)$, the inverse image $f^{-1}(y_1, \ldots, y_m)$ of an (n, m, t) - resilient function, say f, is an orthogonal array $OA_{2^{n-m-t}}(t, n, 2)$; and the 2^m OA's thus obtained comprise a large set.

In view of Theorem 1, any necessary condition for the existence of an orthogonal array $OA_{2^{n-m-t}}(t, n, 2)$ is also a necessary condition for the existence of an (n, m, t) - resilient function. Classical bounds for orthogonal arrays include the Rao and Bush bounds; see [14] for their application to resilient functions.

3 Bounds based on Linear Programming

The most powerful bounds on orthogonal arrays are obtained from Delsarte's linear programming bound; this is the main theme of this section. While developing the bounds based on linear programming techniques, we will be using several standard results from coding theory without proof; the reader is referred to MacWilliams and Sloane [11] for background information on error-correcting codes.

An (n, M, d) binary error correcting code $\mathcal{C}$ is a set of M vectors of length n such that the Hamming distance between any two vectors in $\mathcal{C}$ is at least d. The *distance distribution* of the code is defined to be the sequence $(B_0, B_1, \ldots, B_n)$, where

$$B_i = \frac{1}{M}|\{(u, v) : u, v \in \mathcal{C}, d(u, v) = i\}|.$$

Note that $B_0 = 1$ and $B_0 + B_1 + \ldots + B_n = M$.

The *Krawtchouck transform* of the distance distribution is another sequence, denoted $(B_0^{'}, B_1^{'}, \ldots, B_n^{'})$, where

$$B_k^{'} = \frac{1}{M}\sum_{i=0}^{n} B_i P_k(i).$$

$P_k(i)$ is the value of the *Krawtchouk polynomial* $P_k(x)$ at the integer i and can be defined explicitly as

$$P_k(i) = \sum_{j=0}^{k}(-1)^j\binom{i}{j}\binom{n-i}{k-j}.$$

If $B_i^{'} = 0$ for $1 \leq i \leq d^{'} - 1$ and $B_{d^{'}}^{'} \neq 0$, then $d^{'}$ is called the *dual distance* of the code $\mathcal{C}$. This concept was defined by Delsarte [7]. It is a well known theorem that if we write the vectors in $\mathcal{C}$ as rows of an $M \times n$ array, then any set of $r \leq d^{'} - 1$ columns contains each r-tuple exactly $M/2^r$ times, and $d^{'}$ is the largest number with this property (see for example [11, p. 139], [7]). In other words $\mathcal{C}$ is an orthogonal array $OA_\lambda(d^{'} - 1, n, 2)$ where $\lambda = M/2^{d^{'}-1}$.

It is clear that for any code $\mathcal{C}$, we have $B_i \geq 0$ for $i = 0, 1, \ldots n$. On the other hand, it is a non-trivial theorem (see for example [11, p. 139],[7]) that $B_i^{'} \geq 0$ for $i = 0, 1, \ldots n$.

Suppose an $OA_\lambda(t, n, 2)$ exists. Let M be the number of rows in this orthogonal array. A lower bound on M can be obtained by solving a suitable linear programming problem (see [11, §4 of Ch.17], [7] for similar approaches to a different problem), if we view the rows of this orthogonal array as codewords of a code

$\mathcal{C}$. Let $(B_0, B_1, \ldots, B_n)$ be the distance distribution of $\mathcal{C}$ and $(B_0', B_1', \ldots, B_n')$ be its transform. Then

$$M = B_0 + B_1 + \ldots + B_n.$$

Also

$$\begin{aligned} B_k' &= \frac{1}{M} \sum_{i=0}^{n} B_i P_k(i) \\ &= \frac{1}{M} \left(\sum_{i=1}^{n} B_i P_k(i) + \binom{n}{k} \right). \end{aligned}$$

As $B_k' \geq 0$, we get

$$\sum_{i=1}^{n} B_i P_k(i) \geq -\binom{n}{k} \text{ for } 1 \leq k \leq n.$$

Note further that the dual distance of this code $\mathcal{C}$ is at least $t+1$ (as it is an orthogonal array of strength t). So we can formulate the following linear programming problem which we will refer to as **LP1**:

Minimize $B_1 + B_2 + \cdots + B_n$ subject to $\sum_{i=1}^{n} B_i P_k(i) = -\binom{n}{k}$ for $1 \leq k \leq t$ $\sum_{i=1}^{n} B_i P_k(i) \geq -\binom{n}{k}$ for $t+1 \leq k \leq n$ $B_i \geq 0$ for $1 \leq i \leq n$

Let $B = B(n,t)$ be the optimal solution to the above linear programming problem. Then we have

$$M = \sum_{i=0}^{n} B_i \geq 1 + B \tag{1}$$

Now let us return to our original problem of establishing stronger upper bounds for the optimal value of t. In view of Theorem 1, an (n, m, t) resilient function exists if only if $LOA_{2^{n-m-t}}(t, n, 2)$ exists. Clearly $LOA_{2^{n-m-t}}(t, n, 2)$ exists only if an $OA_{2^{n-m-t}}(t, n, 2)$ exists. The number of rows in this orthogonal array is given by

$$M = 2^{n-m-t} 2^t = 2^{n-m}.$$

In view of the bound of inequality (1), this immediately implies that

$$m \leq n - \log_2(1 + B).$$

Thus we have an upper bound for the optimal value of m, given n and t. The upper bound for the optimal value of t for a given n and m can be trivially computed once we have a table of upper bounds for the optimal value of m.

4 Explicit bounds

The disadvantage of the linear programming bound is that one needs to solve a different LP for every parameter situation. Thus it is of interest to try to derive explicit bounds as corollaries of the LP bound. We will pursue this idea in this section.

Let us first form the dual of the linear programming problem **LP1**. We will refer to the dual as **LP2**.

$$\boxed{\begin{array}{l} \text{Maximize } \displaystyle\sum_{i=1}^{n} x_i \binom{n}{i} \\ \\ \text{subject to} \\ \\ \displaystyle\sum_{i=1}^{n} x_i P_i(k) \geq -1 \text{ for } k = 1 \text{ to } n \\ \\ x_1, x_2, \ldots x_t \text{ unrestricted} \\ x_{t+1}, x_{t+2}, \ldots x_n \leq 0 \end{array}}$$

It is a standard theorem in the theory of linear programming that in a pair of primal-dual linear programs the optimal value of the minimization problem will always be greater than or equal to the value attained by the objective function of the maximization problem at any feasible solution vector. So any feasible solution to the dual linear program **LP2** yields a lower bound on the size of the orthogonal array of strength t and length n and consequently an upper bound on m of t-resilient functions on n-tuples.

Consider the solution vector

$$x_i = 1 - \frac{i}{t+1}.$$

We will first show that this is indeed a feasible solution. In the proof, we will make use of the following standard properties (see problem 45 in page 153 of [11]) of the Krawtchouk polynomials.

$$\sum_{i=0}^{n} P_i(k) = 2^n \delta_{k,0}, \tag{2}$$

$$\sum_{i=0}^{n} i P_i(k) = 2^{n-1} \left(n\delta_{k,0} - \delta_{k,1} \right), \tag{3}$$

where $\delta_{r,s}$ is the Kronecker symbol defined by $\delta_{r,s} = 1$ if $r = s$ and $\delta_{r,s} = 0$ if $r \neq s$.

$$\begin{aligned}
\sum_{i=1}^{n} x_i P_i(k) &= \sum_{i=1}^{n} \left(1 - \frac{i}{t+1}\right) P_i(k) \\
&= \sum_{i=1}^{n} P_i(k) - \frac{1}{t+1} \sum_{i=1}^{n} i P_i(k) \\
&= 2^n \delta_{k,0} - 1 - \frac{2^{n-1}}{t+1} \left(n\delta_{k,0} - \delta_{k,1}\right) \\
&= -1 + \frac{2^{n-1}}{t+1} \delta_{k,1} \text{ as } k \neq 0 \text{ in our case} \\
&\geq -1.
\end{aligned}$$

Clearly $x_{t+1} = 0$. As the x_i's form a decreasing sequence, it follows that the condition $x_{t+1}, \ldots, x_n \leq 0$ is also satisfied by the above solution vector. Now that we have shown that the x_i's form a feasible solution, let us compute the value of the objective function at this solution vector.

$$\begin{aligned}
\sum_{i=1}^{n} x_i \binom{n}{i} &= \sum_{i=1}^{n} \left(1 - \frac{i}{t+1}\right) \binom{n}{i} \\
&= \sum_{i=1}^{n} \binom{n}{i} - \frac{1}{t+1} \sum_{i=1}^{n} i \binom{n}{i} \\
&= 2^n - 1 - \frac{1}{t+1} \sum_{i=1}^{n} n \binom{n-1}{i-1} \\
&= 2^n - 1 - \frac{n}{t+1} \sum_{j=0}^{n-1} \binom{n-1}{j} \\
&= 2^n - 1 - \frac{n 2^{n-1}}{t+1}
\end{aligned}$$

Hence it follows that

$$M \geq 1 + B \geq 2^n - \frac{n 2^{n-1}}{t+1}. \tag{4}$$

As a consequence, we get the following Theorem, which was first proved by Friedman [8] using very different methods.

Theorem 2. *If an (n, m, t)-resilient function exists, then*

$$t \leq \left\lfloor \frac{2^{m-1} n}{2^m - 1} \right\rfloor - 1.$$

Similarly, by proving that the vector

$$x_i = 1 - \frac{\lceil \frac{i}{2} \rceil}{\lceil \frac{t+1}{2} \rceil}.$$

is a feasible solution to the dual linear program **LP2**, we can show that

$$M \geq 1 + B \geq 2^n - \frac{2^{n-2}(n+1)}{\lceil \frac{t+1}{2} \rceil}. \tag{5}$$

As a consequence, we get the following new bound, which complements the bound of Theorem 2.

Theorem 3. *If an* (n, m, t)*-resilient function exists, then*

$$t \leq 2 \left\lfloor \frac{2^{m-2}(n+1)}{2^m - 1} \right\rfloor - 1.$$

The bounds of inequalities (4) and (5) are easily computed. Also for many parametric situations, these two bounds are as powerful as the linear programming bound itself. We record this fact as the following Theorem; however, the proof is omitted due to space limitations.

Theorem 4. *When t is odd and $t+1 \leq n \leq 2t+1$, the bound of equation (4) is as powerful as the linear programming bound. When t is even and $t+1 \leq n \leq 2t+2$, the bound of equation (5) is as powerful as the linear programming bound.*

The result of Theorem 2 was conjectured in [6], where it was shown to be true for $m = 1, 2$ (and in these cases, the bound is tight). Theorem 2 establishes that the conjecture is true for arbitrary m.

By considering a slightly different (but equivalent) version of the linear programming problem, we can exhibit a duality between codes and orthogonal arrays in the sense that each bound on block codes which can be derived from Delsarte's LP-bound yields a bound on orthogonal arrays as well. In this sense the trivial bound $M \geq 2^t$ is the dual of the Singleton bound for codes, the Rao bound is the dual of the sphere packing bound for codes, and the bounds of inequalities (4) and (5) are the dual of the Plotkin bounds for codes.

The MRRW-bound on codes (see [12]), or at least the easier part of it, also follows from the LP-bound. So this bound also carries over to orthogonal arrays. We state an asymptotic version, as applied to resilient functions:

Theorem 5. *If there is an infinite series of resilient functions with parameters (n, m, t), where $n \longrightarrow \infty, t/n \longrightarrow \delta$, then m/n is asymptotically bounded by $H_2(\frac{1}{2} - \sqrt{\delta(1-\delta)})$, where H_2 is the binary entropy function. In particular, positive rates m/n can be attained asymptotically only if $\delta < 1/2$.*

5 Optimal Resilient Functions

Any method of construction of resilient functions yields a lower bound on the optimal value of t. The most important construction method for resilient functions uses linear error correcting codes. A resilient function constructed in this way is said to be a *linear* resilient function.

An (n, m, d) *linear code* is an m-dimensional subspace C of $[GF(2)]^n$ such that the Hamming distance between any two vectors in C is at least d. Let G be an $m \times n$ matrix whose rows form a basis for C; G is called a *generating matrix* for C. The following construction for resilient functions was given in [6, 2]:

Theorem 6. *Let G be a generating matrix for an (n, m, d) linear code C. Define a function $f : [GF(2)]^n \longrightarrow [GF(2)]^m$ by the rule $f(x) = xG^T$. Then f is an $(n, m, d-1)$ - resilient function.*

The *simplex code* $\mathcal{S}_m$ is the dual of the Hamming code $\mathcal{H}_m$. The generator matrix of $\mathcal{S}_m$ is of size $m \times 2^m - 1$ and has all non-zero binary m-tuples as its columns. It is not too difficult to see that each non-zero codeword of the simplex code has weight 2^{m-1}. Thus $\mathcal{S}_m$ is a linear constant-weight code with parameters $(2^m - 1, m, 2^{m-1})$. We shall make use of the simplex code in the proof of the following theorem.

Theorem 7. *Suppose there exists an (n, m, t) linear resilient function which is optimal by virtue of meeting one of the two bounds of Theorem 2 and Theorem 3. Then there exists an $(n + 2^m - 1, m, t + 2^{m-1})$ linear resilient function which is also optimal by virtue of meeting the same bound.*

Proof. Since the (n, m, t) resilient function is linear, it must have been constructed from an $(n, m, t+1)$ linear code $\mathcal{C}$. Now consider the linear code $\mathcal{C}'$ whose generating matrix is obtained by pasting the generating matrices of the code $\mathcal{C}$ and the simplex code $\mathcal{S}_m$, i.e.,

$$G_{\mathcal{C}'} = [G_{\mathcal{C}} \mid G_{\mathcal{S}_m}]$$

Clearly $\mathcal{C}'$ is a linear $(n+2^m-1, m, t+1+2^{m-1})$ code and from this code we can construct a linear resilient function with parameters $(n + 2^m - 1, m, t + 2^{m-1})$.

By assumption the (n, m, t) resilient function is optimal as the parameters meet one of the two bounds derived in the last section. If we increase n by $2^m - 1$, both the bounds go up by 2^{m-1} and so it immediately follows that the linear resilient function with parameters $(n + 2^m - 1, m, t + 2^{m-1})$ is also optimal by virtue of meeting the same bound. $\square$

The simplex code itself yields a $(2^m - 1, m, 2^{m-1} - 1)$ linear resilient function, which meets the bound of Theorem 2 and hence is optimal. Applying Theorem 7, we see that optimal linear resilient functions exist whenever $n \equiv 0 \bmod 2^m - 1$, a result first shown by Friedman [8].

In view of Theorem 6, whenever a linear (n, m, d) code exists, so does an $(n, m, d-1)$ resilient function. Brouwer and Verhoeff [4] provides a compilation of best known linear binary codes. It so happens that when $m = 3$ and $4 \leq n \leq 10$, the linear resilient functions constructed from the best known linear codes are optimal by virtue of meeting one of the two bounds of Theorem 2 and Theorem 3. In fact the bound of Theorem 2 is always met except when $n = 9$, in which case the bound of Theorem 3 is met. This fact coupled with Theorem 7 completely determines the optimal resiliency of resilient functions with $m = 3$. We record the result as the following theorem.

Theorem 8. *The optimal resiliency t of resilient functions with $m = 3$ is*

$$\lfloor \tfrac{4n}{7} \rfloor - 1 \text{ if } n \not\equiv 2 \bmod 7 \text{ and}$$

$$\lfloor \tfrac{4n}{7} \rfloor - 2 \text{ if } n \equiv 2 \bmod 7.$$

Similar analysis settles the question for $m = 4$ in all cases except for two congruence classes modulo 15, as described in the following theorem.

Theorem 9. *The optimal resiliency t of resilient functions with $m = 4$ is*

$$\lfloor \tfrac{8n}{15} \rfloor - 1 \text{ if } n \not\equiv 2, 3, 4, 6 \text{ or } 10 \bmod 15 \text{ and}$$

$$\lfloor \tfrac{8n}{15} \rfloor - 2 \text{ if } n \equiv 2, 6 \text{ or } 10 \bmod 15.$$

Here, it turns out that the bound of Theorem 2 is met in those cases when $n \not\equiv 2, 3, 4, 6, 10 \bmod 15$, and the bound of Theorem 3 is relevant for $n \equiv 2, 6, 10 \bmod 15$. The two congruence classes $n \equiv 3, 4 \bmod 15$ are unsolved at present.

It is also possible to determine other classes of parameters for which the optimal resiliency can be computed, by using the method of *anticodes* [11, Ch. 17, §6]. For each fixed m, we get many infinite classes of optimal resilient functions. The following is one theorem that can be proved by these methods.

Theorem 10. *Let m be a fixed integer. Let $m > u_1 \geq u_2 \geq 1$. Then for the following values of n, the upper bound on resiliency given in Theorem 2 is tight and it can be attained by linear resilient functions.*

$$\begin{aligned} &n = s(2^m - 1) - 2^{u_1} + 1 \text{ for all } s \geq 1 \\ &n = s(2^m - 1) - 2^{u_1} - 2^{u_2} + 2 \\ &\qquad \text{for } s = 1 \text{ if } u_1 + u_2 \leq m, \text{ and for all } s \geq 2. \end{aligned}$$

6 Related results

Most of the techniques used in this paper are applicable mutatis mutandis to non-binary orthogonal arrays and resilient functions. Some results on non-binary resilient functions are proved in [9]. As well, the following bound on non-binary orthogonal arrays is proved in [3]:

Theorem 11. *If there exists an $OA_\lambda(t, n, v)$, then*

$$M \geq v^n \left(1 - \frac{(v-1)n}{v(t+1)}\right).$$

Acknowledgements

Research of the second and third authors is supported by NSF grant CCR-9121051.

References

1. C. H. Bennett, G. Brassard, and A. K. Ekert. Quantum cryptography. *Scientific American*, **267(4)** (1992), 26–33.
2. C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. *SIAM J. Computing*, **17** (1988), 210–229.
3. J. Bierbrauer. Bounds on orthogonal arrays and codes. Preprint.
4. A. E. Brouwer and Tom Verhoeff. An updated table of minimum-distance bounds for binary linear codes. *IEEE Transactions on Information Theory*, **39** (1993), 662–677.
5. P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Advances in Cryptology - CRYPTO '91*, pages 86–100. Springer Verlag, 1992.
6. Benny Chor, Oded Goldreich, Johan Håstad, Joel Friedman, Steven Rudich, and Roman Smolensky. The bit extraction problem or $t-$resilient functions. *IEEE Symposium on Foundations of Computer Science*, pages 396–407, 1985.
7. P. Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Information and Control*, **23** (1973), 407–438.
8. J. Friedman. On the bit extraction problem. *Proc. 33rd IEEE Symposium on Foundations of Computer Science*, pages 314–319, 1992.
9. K. Gopalakrishnan and D. R. Stinson. Characterizations of non-binary correlation-immune and resilient functions. Technical Report UNL - CSE - 93 - 010, University of Nebraska - Lincoln, Lincoln, NE 68588, March 1993. Submitted to *Designs, Codes and Crytography.*
10. K. Gopalakrishnan, D. R. Stinson and J. Bierbrauer. Orthogonal arrays, resilient functions, error correcting codes and linear programming bounds. Preprint.
11. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, 1977.
12. R. J. McEliece, E. R. Rodemich, H. Rumsey and L. R. Welch. New upper bounds on the rate of a code via the Delsarte-McWilliams inequalities. *IEEE Trans. on Information Theory*, **23** (1977), 157–166.
13. Rainer A. Rueppel. *Analysis and Design of Stream Ciphers.* Springer-Verlag, 1986.
14. D. R. Stinson. Resilient functions and large sets of orthogonal arrays. *Congressus Numerantium*, **92** (1993), 105–110.

This article was processed using the LaTeX macro package with LLNCS style