An application of covering designs: determining the maximum consistent set of shares in a threshold scheme

R. S. Rees*
Department of Mathematics and Statistics
Memorial University of Newfoundland
St. John's Newfoundland, A1C 5S7
Canada

D. R. Stinson† and R. Wei
Department of Combinatorics and Optimization
University of Waterloo
Waterloo Ontario, N2L 3G1
Canada

G. H. J. van Rees‡
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, R3C 2N2
Canada

Abstract

The shares in a (k, n) Shamir threshold scheme consist of n points on some polynomial of degree at most $k-1$. If one or more of the shares are faulty, then the secret may not be reconstructed correctly. Supposing that at most t of the n shares are faulty, we show how a suitably chosen covering design can be used to compute the correct secret. We review known results on coverings of the desired type, and give some new constructions. We also consider a randomized algorithm for the same problem, and compare it with the deterministic algorithm obtained by using a particular class of coverings.

*research supported by NSERC grant OGP # 333195
†research supported by NSERC grants IRC # 216431-96 and RGPIN # 203114-98
‡research supported by NSERC grant OGP # 0003558

1 Introduction

Suppose we have a (k, n) threshold scheme, say a Shamir scheme (see, e.g., [6]) implemented in $\mathbb{F}_q$. Let

$$S = \{(x_i, y_i) : 1 \leq i \leq n\} \subseteq \mathbb{F}_q \times \mathbb{F}_q$$

be the set of n shares, and assume that at most t of the shares are faulty. In other words, there exists a polynomial $p_0(x) \in \mathbb{F}_q[x]$ of degree at most $k-1$ such that $y_i = p_0(x_i)$ for at least $n-t$ of the n shares. The secret, which can be reconstructed from any k non-faulty shares, is the value $p_0(0)$. The problem we consider in this note is to find an efficient algorithm to compute p_0, given that some unspecified subset of t of the n shares are faulty.

Denote $\mathsf{G} = \{i : y_i = p_0(x_i)\}$ (the *good shares*) and $\mathsf{B} = \{1, \ldots, n\} \backslash \mathsf{G}$ (the *bad shares*). Then $|\mathsf{G}| = n - t$ and $|\mathsf{B}| = t$.

For any $T \subseteq \{1, \ldots, n\}$ such that $|T| = k$, there is a unique polynomial p_T of degree at most $k-1$ such that $p_T(x_i) = y_i$ for all $i \in T$. The polynomial p_T can easily be computed by Lagrange interpolation. The following two facts are obvious:

1. If $T \subseteq \mathsf{G}$, then $p_T = p_0$.
2. If $T \cap \mathsf{B} \neq \emptyset$, then $p_T \neq p_0$.

Now, for $T \subseteq \{1, \ldots, n\}$, $|T| = k$, define $C_T = \{i : p_T(x_i) = y_i\}$. Then it is clear that $|C_T| \geq n - t$ if $T \subseteq \mathsf{G}$. On the other hand, if $T \cap \mathsf{B} \neq \emptyset$, then $|C_T| \leq k + t - 1$, since $|C_T \cap \mathsf{B}| \leq |\mathsf{B}| \leq t$ and $|C_T \cap \mathsf{G}| \leq k - 1$.

If $n - t \leq k + t - 1$, then there could exist a polynomial $p_T \neq p_0$ of degree at most $k - 1$ such that at least $n - t$ shares lie on p_T. Therefore, in order to guarantee that our problem can be solved, it must be the case that $n - t > k + t - 1$, or $n \geq 2t + k$. We will assume that this inequality holds for the rest of this note.

In the remaining sections of this paper, we show how a suitably chosen covering design can be used to compute the correct secret. We review known results on coverings of the desired type, and give four new constructions — two direct constructions and two recursive constructions. We also consider a randomized algorithm for the same problem, and compare it with the deterministic algorithm obtained by using a particular class of coverings.

2 An algorithm to find the polynomial p_0

Let $\mathcal{T}$ be a set of k-subsets of $\{1, \ldots, n\}$, called *blocks*. The following algorithm will compute the polynomial p_0 if the set system $\mathcal{T}$ is chosen appropriately.

Algorithm 1

Input $\mathcal{T}$, $\mathcal{S}$, n, k and t.

For each $T \in \mathcal{T}$, perform the following steps:

1. compute p_T
2. compute C_T
3. if $|C_T| \geq n - t$, then set $p_0 = p_T$ and QUIT

In order for Algorithm 1 to succeed, we require the following property (*) to be satisfied by the set system $\mathcal{T}$:

For any $B \subseteq \{1, \ldots, n\}$, $|B| \leq t$, there exists a block $T \in \mathcal{T}$ such that $B \cap T = \emptyset$.

A collection $\mathcal{T}$ of k-subsets of $\{1, \ldots, n\}$ (called *blocks*) is an (n, k, t)-*covering* if every t-subset of $\{1, \ldots, n\}$ is contained in at least one block. The following lemma is obvious.

Lemma 1 *A set system $\mathcal{T}$ satisfies (*) if and only if the set system*

$$\{\{1, \ldots, n\} \backslash T : T \in \mathcal{T}\}$$

is an $(n, n-k, t)$-covering.

3 Coverings

Let $C(v, k, t)$ denote the minimum number of blocks in a (v, k, t)-covering. Then, $C(n, n-k, t)$ provides an upper bound on the number of iterations required by Algorithm 1. Some results on covering numbers of this form can be found in Mills [2], Sidorenko [3, 4, 5] and Todorov [7]. We briefly summarize some known results now.

Theorem 2 [2, eq. (2.16), p. 221] *If $n \geq k(t+1)$, then $C(n, n-k, t) = t+1$.*

For $n \geq k(t+1)$, the set $\mathcal{T}$ can be taken to be $t+1$ disjoint k-subsets of $\{1, \ldots, n\}$. It is clear that this collection of subsets satisfies property (*), since any element of a t-subset is contained in at most one of the given blocks.

Theorem 3 [2, eq. (2.17), p. 221] *If $k(t+1) > n \geq k(t + 1/2)$, then $C(n, n-k, t) = t+2$.*

For $k(t+1) > n \geq k(t+1/2)$ and k even, we can construct the set $\mathcal{T}$ as follows. First, take $t-1$ disjoint k-subsets of $\{1, \ldots, n\}$. Then, construct three further k-subsets on a disjoint set of $3k/2$ points, such that each of the $3k/2$ points occurs in two of the three blocks. (This can be done since $n \geq k(t+1/2) = k(t-1) + 3k/2$.) We show that this collection of blocks satisfies property (*). First, $t-1$ points are required to hit the $t-1$ disjoint blocks. Then, since any additional point hits only two of the remaining three blocks, (*) is satisfied.

In general, from [2, Theorem 2.4] we have the following result.

Theorem 4 *Suppose s and t are integers such that $3 \leq s \leq (t+3)/2$, and suppose that*

$$k\left(t - \frac{s-3}{2}\right) \leq n < k\left(t - \frac{s-4}{2}\right). \tag{1}$$

If k is odd and

$$k\left(t - \frac{s-3}{2}\right) \leq n < k\left(t - \frac{s-3}{2}\right) + \frac{s-3}{2},$$

then $C(n, n-k, t) \geq t+s+1$. Otherwise, $C(n, n-k, t) = t+s$.

If (1) is satisfied and k is even, then we can construct the set $\mathcal{T}$ by generalizing the construction given after Theorem 3, as follows. First, take $t-2s+3$ disjoint k-subsets, say $A_1, \ldots, A_{t-2s+3}$. Next, for $1 \leq i \leq s-1$, let B_i, C_i, D_i be disjoint $(k/2)$-subsets, and construct blocks $B_i \cup C_i$, $C_i \cup D_i$, and $D_i \cup B_i$. We have a collection $\mathcal{T}$ of $t-2s+3+3(s-1) = t+s$ blocks of size k. Further, the cardinality of the union of these blocks is

$$k(t-2s+3) + \frac{3k(s-1)}{2} = k\left(t - \frac{s-3}{2}\right) \leq n.$$

We show that $\mathcal{T}$ satisfies property (*). First, $t-2s+3$ points are required to hit the blocks $A_1, \ldots, A_{t-2s+3}$. Then, for $1 \leq i \leq s-1$, we require two points to hit the three blocks $B_i \cup C_i$, $C_i \cup D_i$, and $D_i \cup B_i$. Hence, any set of $t-2s+3+2(s-1)-1 = t$ points is disjoint from at least one block in $\mathcal{T}$.

Remarks:

1. Theorems 2, 3 and 4 were proved independently by Sidorenko [3], using the terminology of Turán systems.

2. There are more known results about the covering numbers $C(n, n-k, 2)$ in [2]. For example, it is shown there that $C(n, n-k, 2) = 5$ for $\frac{5}{2}k > n \geq \frac{9}{4}k$; and $C(n, n-k, 2) = 6$ for $\frac{9}{4}k > n \geq \frac{7}{4}k$.

3. Sidorenko [4] shows that $C(n, n-4, t) = 3t+3-\lfloor \frac{n}{2} \rfloor$ whenever $3t+4 \leq n < 4t+4$.

Observe that Theorems 2, 3 and 4 leave a finite interval of covering numbers undetermined for any fixed values of k and t. For "small" values of k and t, the missing numbers can be found in the tables presented in [1]. As an example, consider the case $t = k = 3$. We have that $C(n, n-3, 3) = 4$ for $n \geq 12$, by Theorem 2, $C(11, 8, 3) = 5$ by Theorem 3, $C(10, 7, 3) = 6$ by Theorem 4. The remaining values of $C(n, n-3, 3)$ are found in [1]: $C(9, 6, 3) = 7$, $C(8, 5, 3) = 8$, $C(7, 4, 3) = 12$ and $C(6, 3, 3) = 20$.

For the case $k = 4$ and $t = 3$, we have $C(n, n-4, 3) = 4$ for $n \geq 16$ from Theorem 2; $C(n, n-4, 3) = 5$ for $n = 14, 15$ from Theorem 3; and $C(n, n-3, 3) = 6$ for $n = 12, 13$ from Theorem 4. The remaining covering numbers can be found in [1]: $C(11, 7, 3) = 8, C(10, 6, 3) = 10$.

4 New constructions of coverings

In this section, we present some new constructions for coverings. These constructions will not, in general, produce optimal coverings. However, they provide a simple, uniform method of obtaining coverings which are often reasonablely close to being optimal.

Our first construction is described in the following theorem.

Theorem 5 *Suppose $n \geq k + st$. Then*

$$C(n, n-k, t) \leq \binom{t + \lceil \frac{k}{s} \rceil}{\lceil \frac{k}{s} \rceil}.$$

Proof. Let $\mathcal{A} = \{A_1, A_2, \dots, A_{t+\lceil \frac{k}{s} \rceil}\}$ be a set of disjoint subsets of $\{1, \dots, n\}$ such that $|A_i| = s-1$ for $i = 1, 2, \cdots, s\lceil \frac{k}{s} \rceil - k$ and $|A_i| = s$ otherwise. This is possible because

$$n \geq st + k = (s-1)\left(s\left\lceil \frac{k}{s} \right\rceil - k\right) + s\left(\left\lceil \frac{k}{s} \right\rceil + t - s\left\lceil \frac{k}{s} \right\rceil + k\right).$$

Now, let $\mathcal{T}$ be formed by taking all unions of $\lceil \frac{k}{s} \rceil$ subsets in $\mathcal{A}$. We show that $\mathcal{T}$ satisfies property (*). In fact, a set B of t points hits at most t subsets in $\mathcal{A}$. Hence, at least $\lceil \frac{k}{s} \rceil$ subsets in $\mathcal{A}$ are disjoint from B, so there is a block $T \in \mathcal{T}$ which is disjoint from B.

It can be verified that the size of any block in $\mathcal{T}$ is at least k; this follows because

$$(s-1)\left(s\left\lceil \frac{k}{s} \right\rceil - k\right) + s\left(\left\lceil \frac{k}{s} \right\rceil - s\left\lceil \frac{k}{s} \right\rceil + k\right) = k.$$

We can delete points from any blocks in $\mathcal{T}$ that have size greater than k, obtaining a set of blocks of size k that satisfies property (*). $\square$

In general, Theorem 5 does not produce optimal coverings. However, one case in which Theorem 5 does yield optimal coverings is $s = k$, when the covering resulting from Theorem 5 is the same as that of Theorem 2.

Next, we present a variation on the above construction.

Theorem 6 *Suppose $k \equiv l \bmod s, 0 < l < s < k$. Then*

$$C(n, n-k, t) \leq \binom{t + \lfloor \frac{k}{s} \rfloor}{\lfloor \frac{k}{s} \rfloor} + \binom{t + \lfloor \frac{k}{s} \rfloor - 1}{\lfloor \frac{k}{s} \rfloor} x,$$

where $x = t - 1$ if $n \geq k + s + lt$ and $x = t$ otherwise.

Proof. Take a set $\mathcal{A} = \mathcal{A}' \cup \{A\}$ of $t + \lfloor \frac{k}{s} \rfloor$ disjoint subsets of $\{1, 2, \cdots, n\}$, where each set in $\mathcal{A}'$ has s elements and A has $s + l$ elements. We can do this because

$$\left(t + \left\lfloor \frac{k}{s} \right\rfloor - 1\right) s + (s + l) = st + k \leq n,$$

since $s = \lfloor \frac{n-k}{t} \rfloor$. Let $\mathcal{T}$ consist of two types of k-subsets of $\{1, 2, \cdots, n\}$, as follows:

Type I The unions over all $(\lfloor \frac{k}{s} \rfloor - 1)$-subsets of $\mathcal{A}'$ together, in turn, with the set A.

Type II For each subset $\mathcal{S} \subset \mathcal{A}'$ with $|\mathcal{S}| = \lfloor \frac{k}{s} \rfloor$, choose $t + 1$ disjoint l-subsets of

$$\{1, 2, \cdots, n\} \setminus (\bigcup_{A_i \in \mathcal{S}} A_i).$$

We can do this because

$$\left\lfloor \frac{k}{s} \right\rfloor s + (t+1)l = k + lt < k + st \leq n.$$

Then take the unions of each of these l-subsets, in turn, with the elements of $\cup_{A_i \in \mathcal{S}} A_i$ as the required k-subsets.

We show that $\mathcal{T}$ satisfies property (*). Let T be a t-subset of $\{1, 2, \cdots, n\}$. If $T \cap A = \emptyset$, then one of the k-subsets of Type I must be disjoint from T, since T hits at most t sets in $\mathcal{A}'$. If $T \cap A \neq \emptyset$, then T hits at most $t - 1$ sets in $\mathcal{A}'$. Thus there is a subset $\mathcal{S} \subset \mathcal{A}'$ with $|\mathcal{S}| = \lfloor \frac{k}{s} \rfloor$ such that $T \cap (\cup_{A_i \in \mathcal{S}} A_i) = \emptyset$ and there is also an l-subset disjoint from T. Therefore there is a k-subset of Type II disjoint from T. The number of the k-subsets of Types I and II is

$$\binom{t + \lfloor \frac{k}{s} \rfloor - 1}{\lfloor \frac{k}{s} \rfloor - 1} + \binom{t + \lfloor \frac{k}{s} \rfloor - 1}{\lfloor \frac{k}{s} \rfloor}(t+1) = \binom{t + \lfloor \frac{k}{s} \rfloor}{\lfloor \frac{k}{s} \rfloor} + \binom{t + \lfloor \frac{k}{s} \rfloor - 1}{\lfloor \frac{k}{s} \rfloor} t.$$

Now suppose that $n \geq k + s + lt$. Then we can modify the Type II blocks to Type II' blocks, as follows.

Type II' For each subset $\mathcal{S} \subset \mathcal{A}'$ with $|\mathcal{S}| = \lfloor \frac{k}{s} \rfloor$, choose t disjoint l-subsets of

$$\{1,2,\cdots,n\}\backslash(\bigcup_{A_i \in \mathcal{S}} A_i \cup A).$$

Then take the unions of each of these l-subsets, in turn, with the elements of $\cup_{A_i \in \mathcal{S}} A_i$ as the required k-subsets.

A similar argument shows that the collection $\mathcal{T}$ of all the blocks of Type I and Type II' satisfies property (*). The number of total subsets in Type I and II' is

$$\binom{t+\lfloor \frac{k}{s} \rfloor - 1}{\lfloor \frac{k}{s} \rfloor - 1} + \binom{t+\lfloor \frac{k}{s} \rfloor - 1}{\lfloor \frac{k}{s} \rfloor} t = \binom{t+\lfloor \frac{k}{s} \rfloor}{\lfloor \frac{k}{s} \rfloor} + \binom{t+\lfloor \frac{k}{s} \rfloor - 1}{\lfloor \frac{k}{s} \rfloor}(t-1).$$

□

We also can use recursive constructions to build the coverings, as in the following theorems.

Theorem 7 *Suppose* $k \equiv l \bmod s, 0 \leq l < s < k$. *Then*

$$C(n, n-k, t) \leq \binom{t+\lfloor \frac{k}{s} \rfloor - 1}{\lfloor \frac{k}{s} \rfloor - 1} + C(n-l-s, n-l-s-k, t-1).$$

Proof. Let $\mathcal{A}$ and the blocks of Type I be the same as in the proof of Theorem 6. Let the blocks of Type II be the complements of blocks in an $(n-l-s, n-l-s-k, t-1)$-covering based on the set $\cup_{A_i \in \mathcal{A}'} A_i$. It is readily checked that the set system satisfies the property (*). □

When $n \geq k + s + lt$, it is sometimes better to use the following variant of the previous theorem.

Theorem 8 *Suppose* $k \equiv l \bmod s, 0 < l < s < k$. *Then*

$$C(n, n-k, t) \leq \binom{t+\lfloor \frac{k}{s} \rfloor}{\lfloor \frac{k}{s} \rfloor} + C(n-l, n-l-k, t-1).$$

Proof. This time we slightly modify the sets described in the proof of Theorem 6 as follows: Let A be divided into two sets of size s and l. The set of size s becomes a set in $\mathcal{A}'$ and the set of size l becomes the new set A. The blocks of Type I are now unions over all $\lfloor \frac{k}{s} \rfloor$ subsets of $\mathcal{A}'$ together, in turn, with the set A. The blocks of Type II are complements of blocks in an $(n-l, n-l-k, t-1)$-covering based on the set $\cup_{A_i \in \mathcal{A}'} A_i$. Again it is readily checked that the set system satisfies the property (*). □

Let $s = n - k$ and $k \equiv l \bmod s$. If $l = 0$, then from Theorem 5 we have $C(n, n-k, 1) \leq \frac{n}{n-k}$. If $l > 0$, then from Theorem 6 we have $C(n, n-k, 1) \leq \lceil \frac{n}{n-k} \rceil$. These numbers are optimal according to the result of [2], and could be used as the base cases for a recursive algorithm based on Theorems 7 and 8.

For $t = 2$ and $t = 3$, we list values of $|T|$ in Tables 1 and 2 for small k and n. In a similar way, we list values of $|T|$ for $k = 3$ in Table 3. In these tables, we only list the values for $2t + k \leq n < k(t + 1)$.

The entries in these tables can be interpreted as follows:

- Values in parentheses are the exact covering numbers $C(n, n - k, t)$ from [2, 5] and the covering tables at the web page `http://sdcc12.ucsd.edu/ ~xm3dg/cover.html`
- In the upper right corner of each entry, a "1" means that the construction follows from Theorem 6, and a "2" means from Theorem 7 or Theorem 8. Otherwise the construction comes from Theorem 5.
- Optimal coverings produced by our constructions are marked by stars.

An easy computer program will produce covering designs with the number of blocks listed on the left in our tables.

5 A randomized algorithm

Next, we provide a randomized algorithm to compute p_0.

Algorithm 2

Input S, n, k and t.

REPEAT the following steps:

1. Let T be a random k-subset of $\{1, 2, \ldots, n\}$.
2. compute p_T
3. compute C_T
4. if $|C_T| \geq n - t$, then set $p_0 = p_T$ and QUIT; otherwise, proceed to the next iteration of the REPEAT loop.

Note that Algorithm 2 is a Las Vegas type algorithm, since it terminates if and only if the correct polynomial p_0 has been found. In any iteration,

Table 1: Covering numbers $C(n, n-k, 2)$

$n\backslash k$	3	4	5	6	7	8	9
7	$*5(5)^1$						
8	$*4(4)^2$	$*6(6)$					
9		$6(5)$	$9(6)^1$				
10		$*4(4)^2$	$7(6)^1$	$10(9)$			
11		$*4(4)^2$	$*6(6)$	$10(6)$	$14(11)^1$		
12			$*5(5)^1$	$*6(6)$	$11(9)^2$	$15(12)$	
13			$*4(4)^2$	$*6(6)$	$8(6)^2$	$14(10)^2$	$19(13)^2$
14			$*4(4)^2$	$*5(5)^1$	$7(6)^2$	$9(6)^2$	$16(12)^2$
15				$*4(4)^2$	$*6(6)$	$8(6)^1$	$*10(10)$
16				$*4(4)^2$	$6(5)$	$*6(6)$	$10(6)$
17				$*4(4)^2$	$*5(5)^1$	$*6(6)$	$7(6)^2$
18					$*4(4)^2$	$6(5)$	$7(6)^2$
19					$*4(4)^2$	$*5(5)^1$	$*6(6)$
20					$*4(4)^2$	$*4(4)^2$	$*6(6)$
21						$*4(4)^2$	$*5(5)^1$
22						$*4(4)^2$	$*5(5)^1$
23						$*4(4)^2$	$*4(4)^2$
24							$*4(4)^2$
25							$*4(4)^2$
26							$*4(4)^2$

Table 2: Covering numbers $C(n, n-k, 3)$

$n\backslash k$	3	4	5	6
9	10(7)[1]			
10	*6(6)[2]	*10(10)		
11	*5(5)[2]	10(8)	17(11)[2]	
12		8(6)[2]	13(11)[2]	20(15)
13		7(6)[2]	11(10)[2]	20(13)
14		*5(5)[2]	9(8)[2]	16(11)[2]
15		*5(5)[2]	8(6)[2]	*10(10)
16			7(6)[2]	10(8)
17			*6(6)[2]	9(7)[2]
18			*5(5)[2]	7(6)[2]
19			*5(5)[2]	7(6)[2]
20				*6(6)[2]
21				*5(5)[2]
22				*5(5)[2]
23				*5(5)[2]

Table 3: Covering numbers $C(n, n-3, t)$

$n\backslash t$	2	3	4	5	6
7	*5(5)[1]				
8	*4(4)[2]				
9		10(7)[1]			
10		*6(6)[2]			
11		*5(5)[2]	11(9)[2]		
12			10(8)[2]		
13			9(7)[2]	16(11)[2]	
14			9(6)[2]	11(10)[2]	
15				10(9)[2]	18(13)[2]
16				9(8)[2]	16(12)[2]
17				9(7)[2]	*11(11)[2]
18					*10(10)[2]
19					*9(9)[2]
20					9(8)[2]

the algorithm is successful if T contains no bad shares. If there are exactly t bad shares, this happens with probability

$$p = \frac{\binom{n-t}{k}}{\binom{n}{k}}.$$

Hence, the expected number of iterations of Algorithm 2 is

$$\beta_r = \frac{1}{p} = \frac{\binom{n}{k}}{\binom{n-t}{k}} = \frac{n(n-1)\cdots(n-k+1)}{(n-t)(n-t-1)\cdots(n-t-k+1)}.$$

6 Comparison of the two algorithms

The value β_r derived above is an average computed over all possible random choices made in Algorithm 2. In order to compare this with Algorithm 1, we should compute the average-case complexity of Algorithm 1. This requires specifying a particular set system $\mathcal{T}$, and we will use the set system from Theorem 2. Since Algorithm 1 is a deterministic algorithm, we compute the average number of iterations over all possible t-subsets B.

Suppose $n \geq k(t+1)$, and Let $\mathcal{T} = \{T_1, T_2, \ldots, T_{t+1}\}$ be the set system containing $t+1$ disjoint k-subsets of $\{1, \ldots, n\}$, in which $T_i = \{(i-1)k + 1, \ldots, ik\}$ for $1 \leq i \leq t+1$. For a t-subset B, define

$$i_{\mathsf{B}} = \min\{i : \mathsf{B} \cap T_i = \emptyset\}.$$

Let $\psi(j)$ denote the number of t-subsets B such that $i_{\mathsf{B}} = j$. Then the average number of iterations required for Algorithm 1 is

$$\frac{\sum_{j=1}^{t+1} j\,\psi(j)}{\binom{n}{t}}.$$

By a simple application of the inclusion-exclusion principle, we have

$$\psi(j) = \sum_{i=1}^{j} (-1)^{i+1} \binom{n-ik}{t} \binom{j-1}{i-1}$$

for $1 \leq j \leq t+1$. Therefore, it follows that

$$\begin{aligned}
\sum_{j=1}^{t+1} j\,\psi(j) &= \sum_{j=1}^{t+1} j \sum_{i=1}^{j} (-1)^{i+1} \binom{n-ik}{t} \binom{j-1}{i-1} \\
&= \sum_{i=1}^{t+1} (-1)^{i+1} \binom{n-ik}{t} \sum_{j=i}^{t+1} j \binom{j-1}{i-1}
\end{aligned}$$

$$= \sum_{i=1}^{t+1}(-1)^{i+1}\binom{n-ik}{t}i\sum_{j=i}^{t+1}\binom{j}{i}$$

$$= \sum_{i=1}^{t+1}(-1)^{i+1}\binom{n-ik}{t}i\binom{t+2}{i+1}.$$

Hence, the average number of iterations required for Algorithm 1 is

$$\beta_d = \sum_{i=1}^{t+1}(-1)^{i+1}i\binom{n-ik}{t}\binom{t+2}{i+1}\Big/\binom{n}{t}.$$

Table 4 lists some of the values of β_r and β_d. These values are very close, especially for large n. Also, observe that $\beta_d < \beta_r$ for all values computed. Thus the average-case complexities of the two algorithms are similar, and indeed, there is no real advantage in using the randomized algorithm, at least when $n \geq k(t+1)$. For $n < k(t+1)$, the randomized algorithm could be considered since the required coverings become more difficult to construct and there is no uniform description of "good" coverings for all parameters in this range.

Acknowledgement

Part of this work was done while R.S.Rees and G.H.J. van Rees were visiting the Department of Combinatorics and Optimization at the University of Waterloo. They would like to thank the department for its hospitality.

References

[1] D. M. Gordon, G. Kuperberg and O. Patashnik. New constructions for covering designs, *J. Combin. Designs* **3** (1995), 269–284.

[2] W. H. Mills. Covering designs I: coverings by a small number of subsets, *Ars Combin.* **8** (1979), 199–315.

[3] A. F. Sidorenko. *Extremal constants and inequalities for distributions of sums of random vectors*, (in Russian), PhD Thesis, Moscow State University, 1982.

[4] A. F. Sidorenko. Precise values of Turán numbers, *Math. Notes* **42** (1987), 913–918.

[5] A. F. Sidorenko. What we know and what we do not know about Turán numbers, *Graphs Combin.* **11** (1995), 179–199.

[6] D. R. Stinson. *Cryptography Theory and Practice*. CRC Press. Inc.. 1995.

[7] D. T. Todorov. On some covering designs. *J. Combin. Theory* A **39** (1985). 83–101.

Table 4: Comparison of the deterministic and randomized algorithms

n	t	k	β_d	β_r	$\frac{\beta_d}{\beta_r}$
9	2	3	1.833	2.400	.764
10	2	3	1.733	2.143	.809
11	2	3	1.655	1.964	.842
12	2	3	1.591	1.833	.868
13	2	3	1.538	1.733	.888
59	2	3	1.105	1.111	.995
109	2	3	1.056	1.058	.998
159	2	3	1.038	1.039	.999
209	2	3	1.029	1.029	1.000
12	2	4	1.818	2.357	.771
13	2	4	1.744	2.167	.805
14	2	4	1.681	2.022	.831
15	2	4	1.629	1.909	.853
16	2	4	1.583	1.818	.871
62	2	4	1.134	1.144	.992
112	2	4	1.073	1.076	.997
162	2	4	1.050	1.051	.999
262	2	4	1.031	1.031	1.000
16	3	4	2.036	2.545	.800
17	3	4	1.956	2.378	.823
18	3	4	1.887	2.242	.842
19	3	4	1.828	2.130	.858
20	3	4	1.775	2.036	.872
66	3	4	1.196	1.210	.989
116	3	4	1.108	1.112	.996
216	3	4	1.057	1.058	.999
316	3	4	1.039	1.039	1.000