An addition to the paper "A polarisation based visual crypto system and its secret sharing schemes"

Henk D. L. Hollmann, J.H. van Lint, L.M.G. Tolhuizen, P. Tuyls,
Philips Research Laboratories
Prof. Holstlaan 4, 5656 AA Eindhoven
The Netherlands

December 18, 2002

Abstract

An (n,k)-pair is a pair of binary $n \times m$ martices (A,B) such that the weight of the modulo-two sum of any i rows, $1 \leq i \leq k$, from A or B is equal to a_i or b_i, respectively, independent of the choice of rows, and moreover, $a_i = b_i$ for $1 \leq i < k$ while $a_k \neq b_k$. In this note, we first show how to construct an (n,k) Threshold Visual Secret Sharing scheme from an (n,k)-pair. Then we explicitely construct an (n,k)-pair for all n and k with $1 \leq k \leq n$.

1 Introduction

We begin by introducing some notation. If M is an $n \times m$ matrix and $S \subseteq \{1, \ldots, n\}$, then we denote the restriction of M to the rows with row number in S by $M(S)$. Similarly, for a family $\mathcal{M}$ of $n \times m$ matrices and for any set $S \subseteq \{1, \ldots, n\}$, we will write $\mathcal{M}(S)$ to denote the collection of all matrices $M(S)$ for $M \in \mathcal{M}$. Note that we consider $\mathcal{M}(S)$ as a *multiset*.

Suppose that we are given two positive integers n and k with $1 \leq k \leq n$. Our aim is to explicitly construct two collections of $n \times m$ binary matrices $\mathcal{A}$ and $\mathcal{B}$ for which there exist numbers h and l with $h > l$ such that the following properties hold.

1. For any A in $\mathcal{A}$, the sum of any k of the rows of A contains at least h zeroes;
2. For any B in $\mathcal{B}$, the sum of any k of the rows of B contains at most l zeroes;
3. For any $S \subseteq \{1, \ldots, n\}$ with $|S| < k$, we have that $\mathcal{A}(S) = \mathcal{B}(S)$ as a multiset.

A pair of collections $\mathcal{A}$, $\mathcal{B}$ as above will be called a Threshold Visual Secret Sharing scheme or TVSS. To stress the values of the parameters, we will sometimes refer to such a pair of collections as a TVSS$(n, k; m, h, l)$. The *contrast* of such a scheme is defined as $(h - l)/(h + l)$.

2 Preliminaries

For a binary vector v, of length m, say, we let $w(v)$ denote the *weight* of v, the number of ones in v, and we write $z(v)$ for the number $m - w(v)$ of zeroes in v. In addition, we define the *unbalance* $d(v)$ of v by $d(v) = z(v) - w(v)$. Note that $d(v) = m - 2w(v)$. For later use we also observe that

$$d(v) = \sum_j (-1)^{v_j}. \tag{1}$$

With each binary $n \times m$ matrix A we will associate two vectors $d(A)$ and $N(A)$ of length 2^n, with the components indexed by vectors in $\{0, 1\}^n$, that is, by binary vectors of length n. For each binary vector x of length n, the x-th component $d_x(A)$ of $d(A)$ will be defined as $d_x(A) = d(x^\top A)$, the unbalance of the sum of the rows in A whose index i satisfies $x_i = 1$; also, the x-th component $N_x(A)$ of $N(A)$ will denote the number of columns of A that are equal to the vector x.

In the next section we will provide a construction that will show the existence of TVSS schemes for all pairs (k, n). This construction will be based on the observation that the vector $N(A)$ can be computed from the vector $d(A)$. We will now make this precise. Define the $2^n \times 2^n$ matrix H by letting

$$H(x, y) = (-1)^{(x,y)}, \tag{2}$$

where x, y are binary vectors of length n and $(x, y) = \sum_i x_i y_i$ denotes the inner product of x and y. Then we have the following.

Lemma 2.1 *(i) The matrix H is a Hadamard matrix, that is, $HH^\top = 2^n I$.*
(ii) The vectors $d(A)$ and $N(A)$ are related by $d(A) = HN(A)$.

Proof: (i) For all binary vectors x, y of length n, we have that

$$\begin{aligned} HH^\top(x,y) &= \sum_z (-1)^{(x,z)}(-1)^{(y,z)} \\ &= \sum_z (-1)^{(x+y,z)} \\ &= \begin{cases} 2^n, & \text{if } x = y; \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

(ii) We will use the expression (1) for the unbalance. By definition of $d_x(A)$, a column y contributes 1 or -1 to $d_x(A)$ according to whether this column contains an even or an odd number of ones in the rows whose index i satisfies $x_i = 1$. So if $v = x^\top A$ denotes the (modulo two) sum of these rows, then we have

$$\begin{aligned} (HN(A))_x &= \sum_y H(x,y)N_y(A) \\ &= \sum_y (-1)^{(x,y)} N_y(A) \\ &= \sum_{j=0}^{m-1} (-1)^{v_j} \\ &= d_x(A). \end{aligned}$$

□

Our construction of an (n, k) TVSS will be based on the constructions of pairs of $n \times m$ matrices A and B with the following two properties. There are numbers $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ such that for each i with $1 \le i \le k$, the weight of the sum of any i rows of A is equal to a_i and the sum of any i rows of B equals b_i; moreover, $a_i = b_i$ for $1 \le i < k$ and $a_k \ne b_k$. Let us call such a pair of matrices an (n, k)*-pair*. Now as a consequence of Lemma 2.1, we have the following.

Theorem 2.2 *Let A and B be an (n, k)-pair of $n \times m$ matrices as above. Let the collection $\mathcal{A}$ be obtained from A by letting the full permutaion group S_m of order m act on the columns of A, and let $\mathcal{B}$ be obtained from B in a similar way. Then the pair of collections $\mathcal{A}$ and $\mathcal{B}$ constitute an (n, k) TVSS scheme.*

Proof: Fix any t rowindices $i_0, \ldots, i_{t-1}$ with $t < k$. Let $\bar{A}$ and $\bar{B}$ denote the restrictions of A and B to these t rows. According to the assumptions, for any binary vector x of length t, we have that $d_x(\bar{A}) = m - 2a_{w(x)} = m - 2b_{w(x)} = d_x(\bar{B})$. Hence by Lemma 2.1, the number of columns $N_y(\bar{A})$ in $\bar{A}$ and the number of columns $N_y(\bar{B})$ in $\bar{B}$ of type $y = (y_0, \ldots, y_{t-1})$ are equal, for all binay vectors y of length t. As a consequence, the matrices

$\bar{A}$ and $\bar{B}$ are equal up to a column permutation; hence the collections $\mathcal{A}(\{i_0,\ldots,i_{t-1}\})$ and $\mathcal{B}(\{i_0,\ldots,i_{t-1}\})$ are equal. Since $a_k \neq b_k$, it follows that the pair $(\mathcal{A},\mathcal{B})$ indeed is an $(n,k;m,h,l)$ TVSS scheme with $h=\max(m-a_k,m-b_k)$ and $l=\min(m-a_k,m-b_k)$. $\square$

3 An explicit construction of (n,k) TVSS schemes

We will now discuss an explicit construction of (n,k) TVSS schemes for all n and all k with $1\le k\le n$. According to Theorem 2.2, it is sufficient to construct (n,k)-pairs for all such n and k. We will obtain such pairs of matrices A and B by concatenation of matrices from a fixed collection of building blocks. For each n and w, we let the $n\times\binom{n}{w}$-matrix $C_w^{(n)}$ consists of all the $\binom{n}{w}$ different 0-1 column vectors of weight w. For example, $C_0^{(n)}$ is the $n\times 1$ zero vector, $C_1^{(n)}$ the $n\times n$ identity matrix; also, note that $C_{n-w}^{(n)}$ is the complement of $C_w^{(n)}$. The collection of building blocks $\mathcal{C}_n$ will consist of all matrices $C_w^{(n)}$ with $0\le w\le n$. In what follows, we will consider n fixed and ommit all references to n in the notation. So we will write C_w for the w-th building block and we will denote the collection of all building blocks for this n by $\mathcal{C}$.

In the sequel we will need an explicit expression for the weight of the sum of some j rows from C_w. In the next lemma, we state the result. Here and in what follows, we will use the standard convention that $\binom{n}{k}=0$ whenever $k<0$ or $k>n$. Under this convention, it is true that

$$\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k} \tag{3}$$

for all n and k.

Lemma 3.1 *The weight of the sum of any j rows, $1\le j\le n$, from C_w does not depend on the choice of rows and is equal to $M_{j,w}$, where*

$$M_{j,w}=\sum_{i\ \mathrm{odd}}\binom{j}{i}\binom{n-j}{w-i}. \tag{4}$$

Proof: Fix any j rows. There are precisely $\binom{j}{i}\binom{n-j}{w-i}$ vectors of weight w that have i ones in these j rows; these rows contribute one (zero) to the weight of the sum of these j rows precisely when i is odd (even). $\square$

Now let $\lambda=(\lambda_0,\ldots,\lambda_n)^\top$ be a vector of length $n+1$ with non-negative integer entries. We define the matrix $C(\lambda)$ to be the matrix consisting of the concatenation of λ_0 copies of C_0, λ_1 copies of C_1, ..., λ_n copies of the matrix C_n. According to Lemma 3.1, the weight of the sum of any j rows of $C(\lambda)$ equals $c_j(\lambda)$, where

$$c_j(\lambda)=\sum_w \lambda_w \sum_{i\ \mathrm{odd}}\binom{j}{i}\binom{n-j}{w-i}. \tag{5}$$

Moreover, the size (number of columns) of $C(\lambda)$ equals

$$c_0(\lambda) = \sum_w \lambda_w \binom{n}{w}. \tag{6}$$

So if we define $c(\lambda) = (c_0(\lambda), \ldots, c_n(\lambda))^\top$, then the above can also be written as $c(\lambda) = M\lambda$, where M is the $(n+1) \times (n+1)$ matrix with entries the $M_{j,w}$ as defined in Lemma 3.1 for $j \geq 1$ and with $M_{0,w} = \binom{n}{w}$.

In our construction of an (n, k) TVSS scheme, we will choose a pair λ, μ of non-negative integer vectors, and let $A = C(\lambda), B = C(\mu)$. Since we have $a_j = c_j(\lambda), b_j = c_j(\mu)$, it is then required that $c_j(\lambda) = c_j(\mu)$ for $j = 1, \ldots, k-1$, but not for $j = k$. Moreover, to ensure that A and B have the same size, we must require that $c_0(\lambda) = c_0(\mu)$. So if $\phi = \lambda - \mu$, we require that the vector $M\phi$ has a zero in components $0, 1, \ldots, k-1$, and a non-zero in component k. Conversely, if we can find an integer vector ϕ with this property, then writing $\phi = \phi^+ - \phi^-$ where ϕ^+ and ϕ^- are defined by requiring that $\phi^+, \phi^- \geq 0$ and $\phi_i^+ \phi_i^- = 0$ for $i = 0, \ldots, n$, we can take $\lambda = \phi^+, \mu = \phi^-$ to obtain an (n, k) pair and hence an (n, k) TVSS scheme. By using scaling, it is even sufficient to have a rational vector ϕ with these properties. In other words, if we define

$$\Phi_k = \{\phi \in \mathbf{Q}^{n+1} \mid \sum_w \phi_w \sum_{i \text{ odd}} \binom{j}{i}\binom{n-j}{w-i} = 0 \text{ for } j = 1, \ldots, k, \sum_w \phi_w \binom{n}{w} = 0\}, \tag{7}$$

then this construction will provide an (n, k) TVSS scheme for each $k = 1, \ldots, n$ if and only if $\Phi_{k-1} \setminus \Phi_k \neq \emptyset$ for $k = 1, \ldots, n$, that is, if and only if $\dim(\Phi_k) = n - k$, for all $k = 1, \ldots, n$.

We will need a result on binomial sums.

Lemma 3.2 *Let $m, v, s \geq 0$. Then*

$$(-1)^s \binom{m}{v+s} = \sum_j (-1)^j \binom{s}{j}\binom{m+j}{v+j}. \tag{8}$$

Proof: Induction on s. For $s = 0$, the claim is trivial. Moreover, if we assume that the claim holds for $s - 1$, then we have

$$\begin{aligned}
(-1)^s \binom{m}{v+s} &= (-1)^s \left[\binom{m+1}{v+s} - \binom{m}{v+s-1}\right] \\
&= -\sum_i (-1)^i \binom{s-1}{i}\binom{m+1+i}{v+1+i} + \sum_j (-1)^j \binom{s-1}{j}\binom{m+j}{v+j} \\
&= \sum_j (-1)^j \binom{s-1}{j-1}\binom{m+j}{v+j} + \sum_j (-1)^j \binom{s-1}{j}\binom{m+j}{v+j} \\
&= \sum_j (-1)^j \binom{s}{j}\binom{m+j}{v+j},
\end{aligned}$$

and the claim holds for s. $\square$

We will apply this lemma to obtain a more useful description of the vector spaces Φ_k defined above. Indeed, we have the following.

Lemma 3.3 *We have that*

$$\sum_w \phi_w \sum_{i \text{ odd}} \binom{j}{i}\binom{n-j}{w-i} = 0 \text{ for } j = 1, \ldots, k \tag{9}$$

if and only if

$$\sum_w \phi_w \binom{n-j}{w-j} = 0 \text{ for } j = 1, \ldots, k. \tag{10}$$

Proof: Induction on k. First, if $k = 1$, then for $j = 1$ we have $M_{j,w} = \binom{n-1}{w-1}$, in agreement with the claim. Now suppose that the equations for $j = 1, \ldots, k-1$ are indeed equivalent to the equations $\sum_w \phi_w \binom{n-j}{w-j} = 0$ for $j = 1, \ldots, k-1$. Consider

$$N = \sum_w \phi_w \sum_{i \text{ odd}} \binom{k}{i}\binom{n-k}{w-i}. \tag{11}$$

By Lemma 3.2 with $m = n-k$, $s = k-i$, and $v = w-k$, we have that

$$(-1)^{k-i}\binom{n-k}{w-i} = \sum_j (-1)^j \binom{k-i}{j}\binom{n-k+j}{w-k+j}, \tag{12}$$

hence for $1 \le i \le k$, we have that $\binom{n-k}{w-i}$ is a linear combination of the binomial coefficients

$$\binom{n-k}{w-k}, \ldots, \binom{n-i}{w-i} \tag{13}$$

with coefficients independent of w. Moreover, the coefficient of $\binom{n-k}{w-k}$ in the expression for $\binom{n-k}{w-i}$ is $(-1)^{k-i}$, hence the coefficient of $\binom{n-k}{w-k}$ in $M_{k,w} = \sum_{i \text{ odd}} \binom{k}{i}\binom{n-k}{w-i}$ is equal to

$$\sum_{\substack{i=0 \\ i \text{ odd}}}^{n} \binom{k}{i}(-1)^{k-i} \neq 0, \tag{14}$$

so if we are given that $\sum_w \phi_w \binom{n-j}{w-j} = 0$ for $j = 1, \ldots, k-1$, then the quantity N defined above is zero if and only if $\sum_w \phi_w \binom{n-k}{w-k} = 0$. $\square$

According to the above lemma, to finish the proof that indeed $\dim(\Phi_k) = n-k$, for $k = 1, \ldots, n$, we must show that the $(n+1) \times (n+1)$ matrix R defined by

$$R_{k,w} = \binom{n-k}{w-k} \tag{15}$$

is invertible. To this end, define the $(n+1)\times(n+1)$ matrix S by

$$S_{i,j} = (-1)^{i+j}\binom{n-i}{j-i}. \tag{16}$$

Then we have the following.

Lemma 3.4 *The matrices R and S are inverses of each other.*

Proof: Note that both R and S are upper triangular. (Since also $R_{k,k}=1$ for all k, we immediately see that R is invertable.) We begin by observing that for $j \geq i$, we have that

$$\begin{aligned}
\binom{n-i}{w-i}\binom{n-w}{j-w} &= \frac{(n-i)!}{(w-i)!(n-w)!}\frac{(n-w)!}{(j-w)!(n-j)!} \\
&= \frac{(n-i)!}{(w-i)!(j-w)!(n-j)!} \\
&= \frac{(n-i)!(j-i)!}{(w-i)!(j-w)!(n-j)!(j-i)!} \\
&= \frac{(n-i)!}{(n-j)!(j-i)!}\frac{(j-i)!}{(w-i)!(j-w)!} \\
&= \binom{n-i}{j-i}\binom{j-i}{w-i}.
\end{aligned}$$

Using this, we obtain for $j \geq i$ that

$$\begin{aligned}
(RS)_{i,j} &= \sum_w (-1)^{w+j}\binom{n-i}{w-i}\binom{n-w}{j-w} \\
&= \sum_w (-1)^{w+j}\binom{n-i}{j-i}\binom{j-i}{w-i} \\
&= (-1)^{i+j}\binom{n-i}{j-i}\sum_w (-1)^{w-i}\binom{j-i}{w-i} \\
&= (-1)^{i+j}\binom{n-i}{j-i}\sum_v (-1)^{v}\binom{j-i}{v} \\
&= (-1)^{i+j}\binom{n-i}{j-i}(1-1)^{j-i} \\
&= (-1)^{i+j}\binom{n-i}{j-i}\delta_{i=j} \\
&= \delta_{i=j}.
\end{aligned}$$

□

As a result of this lemma, we have shown that $\phi \in \Phi_{k-1}\setminus\Phi_k$ if and only if $(R\phi)_j = 0$ for $j = 0,\ldots,k-1$ but $(R\phi)_k \neq 0$, which holds if and only if $\phi = S\theta$ with $\theta = (0,\ldots,0,e,\ldots)^\top$ (where $\theta_k = e$) for some $e \neq 0$. We will discuss two choices for the vector θ.

Example 3.5 *Take $\theta = e_k$, the k-th unit vector. Then ϕ is just the k-th column from S. This leads to vectors λ and μ with*

$$\lambda_{2i} = \binom{n-2i}{k-2i}, \qquad \lambda_{2i+1} = 0 \tag{17}$$

and

$$\mu_{2i} = 0, \qquad \mu_{2i+1} = \binom{n-2i-1}{k-2i-1}, \tag{18}$$

for $0 \le i \le k/2$. For example, if $k = 3$, then

$$\lambda = (\binom{n}{3}, 0, n-2, 0, \ldots, 0) \tag{19}$$

and

$$\mu = (0, \binom{n-1}{2}, 0, 1, 0, \ldots, 0). \tag{20}$$

So A consists of $\binom{n}{3}$ zero-columns followed by $n-2$ matrices C_2 of size $n \times \binom{n}{2}$, where C_2 consists of all columns of weight 2; similarly, B consists of $\binom{n-1}{2}$ copies of the $n \times n$ identity matrix followed by the $n \times \binom{n}{3}$-matrix consisting of all columns of weight 3. It is easily verified that we have

$$a_0 = \binom{n}{3} + (n-2)\binom{n}{2} \tag{21}$$

and

$$b_0 = \binom{n-1}{2} n + \binom{n}{3}, \tag{22}$$

so we have that

$$m = a_0 = b_0 = (2/3)n(n-1)(n-2) = (2n^3 - 6n^2 + 4n)/3. \tag{23}$$

Moreover, we have that

$$a_1 = (n-2) \cdot 1 \cdot (n-1), \qquad b_1 = \binom{n-1}{2} \cdot 1 + 1 \cdot \binom{n-1}{2} \tag{24}$$

so that $a_1 = b_1 = (n-1)(n-2)$,

$$a_2 = (n-2) \cdot 2 \cdot (n-2), \qquad b_2 = \binom{n-1}{2} \cdot 2 + 1 \cdot 2\binom{n-2}{2} = (n-2)(n-1+n-3), \tag{25}$$

so that $a_2 = b_2$, and finally

$$a_3 = (n-2) \cdot 3 \cdot (n-3) = 3n^2 - 15n + 18 \tag{26}$$

and

$$b_3 = \binom{n-1}{2} \cdot 3 + 3 \cdot \binom{n-3}{2} + 1 \cdot 1 = 3n^2 - 15n + 22, \tag{27}$$

Consequently, this scheme has

$$h = a_0 - a_3 = (2n^3 - 6n^2 + 4n)/3 - (3n^2 - 15n + 18) = (2n^3 - 15n^2 + 49n - 54)/3 \tag{28}$$

and

$$l = b_0 - b_3 = (2n^3 - 6n^2 + 4n)/3 - (3n^2 - 15n + 22) = (2n^3 - 15n^2 + 49n - 66)/3, \tag{29}$$

so the contrast $\gamma = (h - l)/(h + l)$ *is given by*

$$\gamma = 12/(4n^3 - 30n^2 + 98n - 120) = 6/(2n^3 - 15n^2 + 49n - 60). \tag{30}$$

Example 3.6 *Now, take*

$$\theta = (0, \ldots, 0, 1, 2, \ldots, n-k, n-k+1)^\top. \tag{31}$$

For $k = 3$*, this leads to the example from the paper. These schemes seem to have significantly higher contrast than the schemes constructed in Example 3.5.*

References

[1] P. Tuyls, H.D.L. Hollmann, J.H. v. Lint, L.M.G. Tolhuizen, *A polarisation based visual crypto system and its secret sharing schemes*, preprint.