XOR-based visual cryptography schemes


Designs, Codes and Cryptography, 37, 169–186, 2005

XOR-based Visual Cryptography Schemes

P. TUYLS pim.tuyls@philips.com
Philips Research Laboratories, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands

H. D. L. HOLLMANN
Philips Research Laboratories, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands

J. H. VAN LINT
Eindhoven University of Technology, Department of Mathematics and Computer Science, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

L. TOLHUIZEN
Philips Research Laboratories, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands

Communicated by: P. Wild

Received August 8, 2003; Revised September 15, 2004; Accepted September 27, 2004

Abstract. A recent publication introduced a Visual Crypto (VC) system, based on the polarisation of light. This VC system has good resolution, contrast and colour properties. Mathematically, the VC system is described by the XOR operation (modulo two addition). In this paper we investigate Threshold Visual Secret Sharing schemes associated to XOR-based VC systems. Firstly, we show that n out of n schemes with optimal resolution and contrast exist, and that $(2, n)$ schemes are equivalent to binary codes. It turns out that these schemes have much better resolution than their OR-based counterparts. Secondly, we provide two explicit constructions for general k out of n schemes. Finally, we derive bounds on the contrast and resolution of XOR-based schemes. It follows from these bounds that for $k < n$, the contrast is strictly smaller than one. Moreover, the bounds imply that XOR-based k out of n schemes for even k are fundamentally different from those for odd k.

Keywords: Threshold visual secret sharing schemes, XOR, MDS codes

AMS Classification: 94A60

1. Introduction

The idea of using the human visual system for security purposes was first mentioned in [1]. Independently of [1], the basic Visual Cryptography (VC) principles were studied by Naor et al. [7,8]. The main idea is to split an image into two random shares (printed on transparencies) which separately reveal no information on the original image. The original image can be reconstructed by superimposing the two shares. In [7,8] it is shown that this system is equivalent to a One Time Pad encryption scheme based on the boolean OR function and therefore unconditionally secure. Later, the associated secret sharing problem and its physical properties as contrast, resolution and colour were extensively studied by Stinson [3,10], Droste [4], and Verheul and Van Tilborg [12].

Although the above mentioned visual crypto systems can be made unconditionally secure, they are not satisfactory from a practical point of view. Firstly, because of the One Time Pad property of the scheme, a key can be used only once. Since transparencies are static objects, a user has to carry a pile of transparencies with him to update the keys. Secondly, the bad physical properties (colour, resolution, contrast) [7,10,12] make the system not very well suited for practical purposes. In [11], a new visual crypto system is introduced that uses the polarisation of light. With this new VC system, decryption can be done with a small, cheap and light-weight decryption display which has a flexible key-updating mechanism. Moreover, the system has good colour, contrast and resolution properties. The operation of the VC system is mathematically described by an XOR operation, that is, a modulo two addition.[1] This motivates the investigation of Threshold Visual Secret Sharing (TVSS) schemes for XOR-based VC in the present paper. Other polarisation-based VC systems were studied in [2] and [9]. Biham and Itzkovitz [2] investigate VC schemes based on passive light polarisers. This way of doing is more flexible than the Naor–Shamir schemes but can not be modelled by an XOR. They present $(2, n)$ and (n, n) black–white schemes and shows how general (k, n) schemes can be derived from (k, n) Naor–Shamir schemes. Furthermore an example of an efficient coloured $(2, n)$ scheme is given. De Santis [9] investigates the pixel expansion and contrast of $(2, n)$ VC schemes for general boolean recombination functions.

The paper is organised as follows. In Section 2, the secret sharing problem is formally defined. We give an almost trivial example of an (n, n) scheme that has a much better resolution than any (n, n) scheme for an OR-based VC system, and show the equivalence of $(2, n)$ schemes and binary coding theory. Things get more complicated in Section 3, where we give two explicit constructions of general k out of n schemes. The first construction seems to yield very efficient schemes. It seems not easy to find manageable expressions for the parameters of the schemes so obtained, but we are able to do so for some specific examples. The second construction is based on MDS codes (known from coding theory, [6, Ch. 11]), and explicit formulas are derived for the parameters of the k out of n schemes obtained with this construction. In Section 4, we derive bounds on resolution and contrast properties of TVSS schemes. It turns out that TVSS schemes for XOR-based VC systems for even k are fundamentally different from those for odd k. This phenomenon does not occur with TVSS schemes for OR-based VC systems.

2. Threshold Visual Secret Sharing Schemes

2.1. Definitions

In this section, we define TVSS schemes for XOR-based VC systems, and give examples of such schemes for certain parameter values. We restrict ourselves to images consisting of black and white pixels. The schemes are meant for sharing a single black or white pixel. In order to share a complete image, the pixel scheme has to be applied to all pixels in the image.

Following the notation from [12], a k out of n (or (k,n)) TVSS scheme $\mathsf{S} = (\mathscr{C}_0, \mathscr{C}_1)$ consists of two collections of $n \times b$ binary matrices $\mathscr{C}_0$ and $\mathscr{C}_1$. To share a white (black) pixel, the dealer randomly chooses one of the matrices in $\mathscr{C}_0$ ($\mathscr{C}_1$) and distributes its rows as shares among the n participants of the system. Any k users can determine whether their shares originated from a matrix in $\mathscr{C}_0$ or from $\mathscr{C}_1$ by XOR-ing them. Any $k-1$ or less users have no information whatsoever on whether a black or a white pixel was shared. The next definition makes the above more precise.

Definition 1. Let k, n, b, h, l be positive integers satisfying $1 \le k \le n$ and $b \ge h > l$. A $[(k,n); b, h, l]$ TVSS scheme consists of two collections of $n \times b$ boolean matrices $\mathscr{C}_0$ and $\mathscr{C}_1$ such that:

1. For any $M \in \mathscr{C}_0$, the *XOR* of any k of the n rows of M has at least h zeroes.
2. For any $M \in \mathscr{C}_1$, the *XOR* of any k of the n rows of M has at most l zeroes.
3. For any $i_1 < i_2 < \cdots < i_t$ in $\{1, 2, \ldots, n\}$ with $t < k$, the two collections of $t \times b$ matrices $\mathscr{D}_0$ and $\mathscr{D}_1$, obtained by restricting each $n \times b$ matrix in $\mathscr{C}_0$ and $\mathscr{C}_1$, respectively, to rows $i_1, i_2, \ldots, i_t$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The numbers h and l are called the white-level and black-level, respectively, of the scheme. The parameter b is called the block length or pixel expansion[2] and determines the resolution of the scheme. The contrast $c = c(\mathsf{S})$ of the scheme is defined as $c = (h-l)/(h+l)$.

The interpretation of the white and black-level is the following. As the sub-pixels of a pixel lie close to each other, the human visual system averages over the black and white sub-pixels. This means that a pixel which has a majority of white (black) sub-pixels is interpreted as white (black) by the human visual system. Clearly, it is desirable to have a large contrast c, and a small block length b. Note that $c \in [0, 1]$ and that c is maximal when $l = 0$. Schemes with $l = 0$ are called *maximal contrast schemes*.

The proof of the following symmetry property is left as an easy exercise to the reader.

PROPOSITION 1. *Let* $\mathsf{S} = (\mathscr{C}_0, \mathscr{C}_1)$ *be a* $[(k,n); b, h, l]$ *TVSS scheme. Let* $\hat{\mathscr{C}}_i$ *be obtained from* $\mathscr{C}_i$ *by replacing zeroes by ones and vice versa. If* k *is even, then the scheme* $(\hat{\mathscr{C}}_0, \hat{\mathscr{C}}_1)$ *is a* $[(k,n); b, h, l]$ *scheme as well. If* k *is odd, then* $(\hat{\mathscr{C}}_1, \hat{\mathscr{C}}_0)$ *is a* $[(k,n); b, b-l, b-h]$ *scheme with contrast* $\hat{c}$ *given by*

$$\hat{c} = (h-l)/(2b-l-h).$$

It follows that $\hat{c} > c$ *whenever* $l + h > b$.

■

For OR-based VC systems, the minimum block length of a (2,2) TVSS scheme with contrast $c = 1$ is at least 2 [4, 7]. The following proposition—the proof of which is left as an easy exercise to the reader—explicitly describes, for each $n \geq 1$, an (n, n) scheme with block length $b = 1$ and contrast $c = 1$.

PROPOSITION 2. *Let $\mathscr{C}_0, \mathscr{C}_1$ be the set of all binary vectors of length n with an even, odd number of ones, respectively. Then $(\mathscr{C}_0, \mathscr{C}_1)$ is an $[(n, n); 1, 1, 0]$ TVSS scheme.*

2.2. *Equivalence of* $(2, n)$ *TVSS Schemes and Binary Error-Correcting Codes*

In this section, we show that $(2, n)$ TVSS schemes are equivalent to binary error-correcting codes. By a (b, n, d) code, we mean a binary code of length b, consisting of n words and with minimum Hamming distance at least d.

THEOREM 1. *Let b, l and h be positive integers such that $l < h \leq b$. The three following statements are equivalent.*

(i) *A $[(2, n); b, b, l]$ TVSS scheme exists.*

(ii) *A $[(2, n); b, h, l]$ TVSS scheme exists.*

(iii) *A binary $(b, n, b - l)$ code exists.*

Proof. It is clear that (i) implies (ii).

In order to show that (ii) implies (iii), let $\mathsf{S} = (\mathscr{C}_0, \mathscr{C}_1)$ be a $[(2, n); b, h, l]$ TVSS scheme. Take a matrix $A_1 \in \mathscr{C}_1$ and let C consist of the rows from A_1. As S is a $[(2, n); b, h, l]$ TVSS scheme, the Hamming distance between two words from C is at least $b - l$. Consequently, C is a $(b, n, b - l)$ code.

Finally, to show that (iii) implies (i), let C be a binary $(b, n, b - l)$ code. For $\mathbf{c} \in C$, let $A(\mathbf{c})$ denote the $n \times b$ matrix for which each row equals $\mathbf{c}$. Moreover, let B be an $n \times b$ matrix containing each word from C as a row, and for $0 \leq i \leq n - 1$, let $B(i)$ be the matrix obtained by a cyclic shift of the rows of B over i positions. We claim that $(\mathscr{C}_0, \mathscr{C}_1) = (\{A(\mathbf{c}) \mid \mathbf{c} \in C\}, \{B(0), B(1), \ldots, B(n - 1)\})$ is a $[(2, n); b, b, l]$ scheme. It is clear that both collections contain n matrices, and that in each row, each word from C occurs in one matrix from $\mathscr{C}_0$ and in one matrix from $\mathscr{C}_1$, showing the indistinghuisability. The sum of any two rows from a matrix in $\mathscr{C}_0$ equals $\mathbf{0}$. Finally, the Hamming distance between any two rows of a matrix from $\mathscr{C}_1$ is at least $b - l$, showing that the XOR of these two rows contains at most $b - (b - l) = l$ zeroes. ∎

We give a few examples of application of Theorem 1. If $n \leq 2^b$, a $(b, n, 1)$ code exists, which results in a $[(2, n); b, b, b - 1]$ TVSS scheme with contrast $c = 1/(2b - 1)$. If $n \leq 2^{b-1}$, a $(b, n, 2)$ code exists (consisting of words of even Hamming weight), resulting in a $[(2, n); b, b, b - 2]$ TVSS scheme with contrast $1/(b - 1)$. If

$b = 2^m$, with $m \geq 3$, a $(b, 2b, b/2)$ code exists (simplex code [6, Ch. 14]), resulting in a $[(2, 2b); b, b, b/2]$ TVSS scheme with contrast 1/3.

3. Construction of (*k, n*) Visual Secret Sharing Schemes

In the previous section, we constructed (n, n) schemes and $(2, n)$ schemes. In this section, we present two constructions showing that (k, n) TVSS schemes exist for all $2 \leq k \leq n-1$. In Subsection 3.1 we give some definitions and prove a theorem that is used in both constructions. The respective constructions are described in Subsections 3.2 and 3.3.

3.1. Constructing (k, n) TVSS Schemes from (k, n) Pairs of Matrices

For describing the constructions of (k, n) schemes, we use the following notation, due to Droste [4]. If A is a binary matrix, then $P(A)$ is the multi-set of matrices obtained by permuting the columns of A, that is, each column permutation corresponds to exactly one element of $P(A)$. Moreover, we use the concept of (k, n) pairs, defined as follows.

Definition 2. A pair (A, B) of binary $n \times b$ matrices is called a *(k,n) pair* if there exist numbers $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ such that

(1) for each i with $1 \leq i \leq k$, the weight of the sum of any i rows from A equals a_i and the weight of the sum of any i rows from B equals b_i, and

(2) $a_i = b_i$ for $1 \leq i < k$, and $a_k \neq b_k$.

The importance of this definition stems from the following theorem.

THEOREM 2. *If (A, B) is a (k, n)-pair of $n \times b$ matrices, then $(P(A), P(B))$ is a $[(k, n); b, h, l]$ TVSS scheme with $h = \max(b - a_k, b - b_k)$ and $l = \min(b - a_k, b - b_k)$. Here, a_k and b_k denote the weight of the sum of any k rows from A and B, respectively.*

We continue with a proof of Theorem 2, or in fact of a generalisation of it.

For a binary vector $\mathbf{v}$ of length b, we define $z(\mathbf{v})$ as the number of zeroes in $\mathbf{v}$, and $w(\mathbf{v})$ as its number of ones. Moreover, we define the *unbalance* $\delta(\mathbf{v})$ of v by $\delta(\mathbf{v}) = z(\mathbf{v}) - w(\mathbf{v})$. Note that $\delta(\mathbf{v}) = b - 2w(\mathbf{v})$. For later use, we also observe that

$$\delta(\mathbf{v}) = \sum_{j=1}^{b} (-1)^{v_j}. \tag{1}$$

With each binary $n \times b$ matrix A we associate two vectors $\delta(A)$ and $N(A)$ of length 2^n, with the components indexed by binary vectors of length n. For each binary vector $\mathbf{x}$ of length n, the $\mathbf{x}$-th component $\delta_{\mathbf{x}}(A)$ of $\delta(A)$ is defined as $\delta_{\mathbf{x}}(A) = \delta(\mathbf{x}^\top A)$, the unbalance of the sum of the rows in A whose index i satis-

fies $x_i = 1$; also, the $\mathbf{x}$-th component $N_{\mathbf{x}}(A)$ of $N(A)$ is defined as the number of columns of A that are equal to $\mathbf{x}$.

We will show that the vectors $\delta(A)$ and $N(A)$ can be computed from each other. To make this precise, we define the $2^n \times 2^n$ matrix H by

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

where $\mathbf{x}, \mathbf{y}$ are binary vectors of length n and $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} x_i y_i$ denotes the inner product of $\mathbf{x}$ and $\mathbf{y}$. Then we have the following.

LEMMA 1. *(i) The matrix H is a Hadamard matrix, that is, $HH^\top = 2^n I$.*
(ii) The vectors $\delta(A)$ and $N(A)$ are related by $\delta(A) = HN(A)$.

Proof. (i) For all binary vectors $\mathbf{x}, \mathbf{y}$ of length n, we have that

$$HH^\top(\mathbf{x}, \mathbf{y}) = \sum_{\mathbf{z}} (-1)^{(\mathbf{x},\mathbf{z})}(-1)^{(\mathbf{y},\mathbf{z})} = \sum_{\mathbf{z}} (-1)^{(\mathbf{x}+\mathbf{y},\mathbf{z})} = \begin{cases} 2^n, & \text{if } \mathbf{x} = \mathbf{y}; \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

(ii) Let $\mathbf{x}$ be a binary vector of length n. From equation (1), it follows that the contribution of a column $\mathbf{y}$ of A to $\delta_{\mathbf{x}}(A)$ equals $(-1)^{(\mathbf{x},\mathbf{y})}$. On the other hand, by definition, we have

$$(HN(A))_{\mathbf{x}} = \sum_{\mathbf{y}} (-1)^{(\mathbf{x},\mathbf{y})} N_{\mathbf{y}}(A). \qquad \blacksquare$$

We are now in a position to prove a generalisation of Theorem 2. Before we state it, we need one more notation: if A is an $n \times b$ matrix, then $w(A_I)$ denotes the weight of the sum of the rows of A indexed by I. Note that

$$w(A_I) = \frac{1}{2}(b - \delta_{\chi(I)}(A)), \tag{4}$$

where $\chi(I)$ is the characteristic vector of the set I.

THEOREM 3. *Let A and B be $n \times b$ matrices such that for each $I \subset \{1, 2, \ldots, n\}$ of size at most $k-1$, $w(A_I) = w(B_I)$. Assume moreover that there exist integers h and l such that $h > l$ and that for each $I \subset \{1, 2, \ldots, n\}$ of size k, $b - w(A_I) \geq h$ and $b - w(B_I) \leq l$. Then $(P(A), P(B))$ is an $[(k, n); b, h, l]$ TVSS scheme.*

Proof. The only non-trivial thing we have to prove is the indistinguishability. Let $I = \{i_1, \ldots, i_t\}$ be a subset of $\{1, 2, \ldots, n\}$ of size $t < k$. Let $\bar{A}$ and $\bar{B}$ denote the restrictions of A and B to the t rows indexed by I. Let $\mathbf{x} = (x_1, \ldots, x_t)$ be a binary vector of length t, and let $\tilde{\mathbf{x}}$ be the binary vector of length n for which entry i_j equals x_j for $j = 1, 2, \ldots, t$, and whose other entries equal zero. It is clear that $\delta_{\mathbf{x}}(\bar{A}) = \delta_{\tilde{\mathbf{x}}}(\bar{A})$. As $\tilde{\mathbf{x}}$ has weight at most t, we find, using equation (4) and the properties of A and B, that $\delta_{\mathbf{x}}(\bar{A}) = \delta_{\mathbf{x}}(\bar{B})$.

Hence by Lemma 1, the number of columns $N_{\mathbf{y}}(\bar{A})$ in $\bar{A}$ and the number of columns $N_{\mathbf{y}}(\bar{B})$ in $\bar{B}$ of type $\mathbf{y} = (y_0, \ldots, y_{t-1})$ are equal for all binary vectors $\mathbf{y}$ of

length t. As a consequence, the matrices $\bar{A}$ and $\bar{B}$ are equal up to a column permutation, which readily implies indistinguishability in the rows under consideration in the multi-sets $P(A)$ and $P(B)$. ■

3.2. *Construction 1*

We discuss an explicit construction of (k, n) TVSS schemes for all n and all k with $1 \le k \le n$. According to Theorem 2, it is sufficient to construct (k, n)-pairs for all such n and k. We will obtain such pairs by concatenation of matrices from a fixed collection of building blocks. For each n and w with $0 \le w \le n$, we let the $n \times \binom{n}{w}$-matrix $C_w^{(n)}$ consist of all the $\binom{n}{w}$ different 0–1 column vectors of weight w, in any order. The collection of building blocks $C^{(n)}$ consists of all matrices $C_w^{(n)}$ with $0 \le w \le n$. In what follows, we will consider n fixed and omit all references to n in the notation. More specifically, we will write C_w for the w-th building block. It is noteworthy that Droste [4] uses the same building blocks in his construction of TVSS schemes for OR-based VC systems.

In the sequel, we will need an explicit expression for the weight of the sum of any 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 $k > n$.

LEMMA 2. *The weight of the sum of any j rows, $1 \le j \le n$, from C_w does not depend on the choice of the rows and is equal to $M_{j,w}$, where*

$$M_{j,w} = \sum_{i \text{ odd}} \binom{j}{i} \binom{n-j}{w-i}. \tag{5}$$

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). ■

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. It is clear that $c_0(\lambda)$, the number of columns of $C(\lambda)$, satisfies

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

According to Lemma 2, the weight of the sum of any j rows of $C(\lambda)$ equals $c_j(\lambda)$, where

$$c_j(\lambda) = \sum_w \lambda_w \sum_{i \text{ odd}} \binom{j}{i} \binom{n-j}{w-i}. \tag{7}$$

Hence, 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 2 for $j \geq 1$ and with $M_{0,w} = \binom{n}{w}$. Now suppose that λ and μ are non-negative integer vectors such that $M\lambda$ and $M\mu$ agree in positions 0,1, ... ,$k-1$, but differ in position k. Then $(C(\lambda), C(\mu))$ is a (k, n) pair of matrices to which we can apply Theorem 2. The way to find such vectors λ and μ is described in Theorem 4, that uses Lemma 3, Corollary 1 and Lemma 4 below.

LEMMA 3. *For $1 \leq j \leq n$, $1 \leq w \leq n$, we have that $M_{j,w} = \sum_{k \geq 1} (-2)^{k-1} \binom{j}{k} \binom{n-k}{w-k}$.*

Proof. Let $f(z) := (1+z)^{n-j}(1-z)^j$. It is clear that

$$f(z) = \sum_i \binom{j}{i} (-1)^i z^i \sum_k \binom{n-j}{k} z^k. \tag{8}$$

As $f(z) = (1+z)^{n-j}((1+z)-2z)^j$, we have that

$$f(z) = \sum_k \binom{j}{k} (-2z)^k (1+z)^{n-k} = \sum_k \binom{j}{k} (-2z)^k \sum_i \binom{n-k}{i} z^i. \tag{9}$$

By comparing the coefficients of z^w in $f(z)$ in equations (8) and (9), we see that

$$\sum_i \binom{j}{i} (-1)^i \binom{n-j}{w-i} = \sum_k \binom{j}{k} (-2)^k \binom{n-k}{w-k}. \tag{10}$$

By comparing the coefficients of z^w in the expansions of $(1+z)^j (1+z)^{n-j} = (1+z)^n$, we obtain the well-known Vandermonde identity,

$$\sum_i \binom{j}{i} \binom{n-j}{w-i} = \binom{n}{w}. \tag{11}$$

The lemma is obtained by subtracting equation (10) from (11). ■

The following is a direct consequence of Lemma 3.

COROLLARY 1. *Let R and L be the $(n+1) \times (n+1)$ matrices defined as*

$$R_{k,w} = \binom{n-k}{w-k} \quad \text{for } 0 \leq k, w \leq n, \text{ and}$$

$$L_{0,0} = 1, L_{i,0} = L_{0,i} = 0 \quad \text{if } i > 0, \text{ and } L_{j,k} = (-2)^{k-1} \binom{j}{k} \quad \text{if } 1 \leq j, k \leq n.$$

Then $M = LR$.

We define the $(n+1) \times (n+1)$ matrix S by

$$S_{i,j} = (-1)^{i+j} \binom{n-i}{j-i}. \tag{12}$$

The following result is surely well-known, but we could not find a reference. The result can be derived from [13, Ch. 2, (4a)].

LEMMA 4. *The matrices R and S are inverses of each other.*

Proof. As R and S are upper triangular matrices with ones on their diagonals, RS is an upper triangular matrix with ones on its diagonal. If $0 \le i < j$, then we have that

$$(RS)_{i,j} = \sum_w \binom{n-i}{w-i}(-1)^{w+j}\binom{n-w}{j-w} = \sum_w (-1)^{w+j}\binom{n-i}{n-j}\binom{j-i}{w-i}$$
$$= \binom{n-i}{n-j}(-1)^{i+j}\sum_v (-1)^v \binom{j-i}{v} = \binom{n-i}{n-j}(-1)^{i+j}(1-1)^{j-i} = 0 \quad \blacksquare$$

We are now in a position to describe our construction, that we cast in the form of a theorem.

THEOREM 4. *Let $1 \le k \le n-1$. Let $\theta = (\theta_0, \theta_1, \ldots, \theta_n)$ be an integer-valued vector such that $\theta_j = 0$ if $0 \le j \le k-1$, and $\theta_k \ne 0$, and let $\phi := S\theta$. For $0 \le j \le n$, we define*

$$\lambda_j = \max(0, \phi_j) \text{ and } \mu_j = -\min(0, \phi_j).$$

Then λ and μ are vectors with non-negative integer entries, and $(C(\lambda), C(\mu))$ is a (k, n) pair.
The parameters of the corresponding $[(k, n); b, h, l]$ TVSS scheme satisfy the following equations:

$$b = \frac{1}{2}\sum_{w=0}^{n} |\phi_w| \binom{n}{w}, \; h - l = 2^{k-1}|\theta_k|, \text{ and } h + l = b + \frac{1}{2}\sum_{w=0}^{n} |\phi_w| \sum_i (-1)^i \binom{k}{i}\binom{n-k}{w-i}.$$

Proof. As S has integer entries, ϕ has integer entries, whence λ and μ have non-negative integer entries. Using Corollary 1, Lemma 4, and the fact that $\phi = \lambda - \mu$, we find that

$$c(\lambda) - c(\mu) = M\lambda - M\mu = M(\lambda - \mu) = M\phi = LRS\theta = L\theta.$$

As L is a lower triangular matrix, and $\theta_j = 0$ if $j < k$, it follows that $c_j(\lambda) = c_j(\mu)$ if $0 \le j \le k-1$, and that $h - l = |c_k(\lambda) - c_k(\mu)| = |(L)_{k,k}\theta_k| = 2^{k-1}|\theta_k|$.
Moreover, $2b = c_0(\lambda) + c_0(\mu) = c_0(\lambda + \mu) = c_0(|\phi|)$, and similarly $(b - h) + (b - l) = c_k(\lambda + \mu) = c_k(|\phi|)$. $\blacksquare$

The construction above shows the existence of (k, n) pairs for all pairs of integers k and n. There is ample choice for the vector θ. We will discuss three choices for it.

EXAMPLE 1. *Take*

$$\theta = (0, \ldots, 0, 1, 2, \ldots, n-k, n-k+1)^\top. \tag{13}$$

As $\phi = S\theta$, we have by definition

$$\phi_i = \sum_{v=k-i-1}^{n-i} (-1)^v \binom{n-i}{v}(v-k+i+1).$$

After some computations (see Appendix A), it follows that

$$\begin{aligned} &\phi_i = (-1)^{i+k}\binom{n-2-i}{k-2-i} \quad \text{if } 0 \le i \le k-2, \\ &\phi_i = 0 \quad \text{if } k-1 \le i \le n-2, \quad \phi_{n-1} = -1, \text{ and } \phi_n = n-k+1. \end{aligned} \tag{14}$$

It does not seem easy to obtain manageable formulas for the length b and the contrast c of the resulting schemes. We work out the special cases $k=3$ and $k=4$.

Case 1. $k=3$.
If $k=3$, then $\phi = (2-n, 1, 0, 0, \ldots, -1, n-2)$. Consequently, $\lambda = (0, 1, 0, \ldots, 0, n-2)$ and $\mu = (n-2, 0, \ldots, 0, 1, 0)$. That is to say, $A = C(\lambda)$ consists of the $n \times n$ identity matrix and $n-2$ columns of weight n, while $B = C(\mu)$ consists of $n-2$ all-zero columns and furthermore contains each column of weight $n-1$ once. It is clear that A and B both contain $2n-2$ columns. Straightforward computations show that $a_1 = b_1 = n-1$, $a_2 = b_2 = 2$, $a_3 = n+1$, $b_3 = n-3$. As a consequence, we obtain a

$[(3, n); 2n-2, n+1, n-3]$ TVSS scheme with $c = 2/(n-1)$.

Case 2. $k=4$.
If $k=4$, then $\phi = (\binom{n}{2} - 2n + 3, 3-n, 1, 0, \ldots, 0, -1, n-3)$. Consequently, $\lambda = (\binom{n}{2} - 2n + 3, 0, 1, 0, \ldots, 0, n-3)$ and $\mu = (0, n-3, 0, \ldots, 0, 1, 0)$. That is to say, $A = C(\lambda)$ consists of $\binom{n}{2} - 2n + 3$ all-zero columns, $n-3$ all-one columns, and contains each vector of weight 2 exactly once. The matrix $B = C(\mu)$ consists of $n-3$ copies of the identity matrix, and contains each column of weight $n-1$ exactly once. It is clear that A and B both contain $n(n-2)$ columns. Straightforward computations show that $a_1 = b_1 = 2n-4$, $a_2 = b_2 = 2n-4$, $a_3 = b_3 = 4n-12$, $a_4 = 4n-16$, $b_4 = 4n-8$. As a consequence, we obtain a

$[(4, n); n^2-2n, n^2-6n+16, n^2-6n+8]$ TVSS scheme with $c = 4/(n^2-6n+12)$.

EXAMPLE 2. *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*

$$\lambda_{2i} = \binom{n-2i}{k-2i}, \qquad \lambda_{2i+1} = 0, \qquad \mu_{2i} = 0, \qquad \mu_{2i+1} = \binom{n-2i-1}{k-2i-1}, \tag{15}$$

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

$$\lambda = \left(\binom{n}{3}, 0, n-2, 0, \ldots, 0\right) \text{ and } \mu = \left(0, \binom{n-1}{2}, 0, 1, 0, \ldots, 0\right). \tag{16}$$

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 both matrices have* $b = \frac{2}{3}n(n-1)(n-2)$ *columns. Straightforward computations show that*

$$a_1 = b_1 = (n-1)(n-2),\ a_2 = b_2 = 2(n-2)^2,\ a_3 = 3n^2 - 15n + 18, b_3 = 3n^2 - 15n + 22$$

Consequently, we have obtained a

$$[(3,n); \frac{2}{3}n(n-1)(n-2), (2n^3 - 15n^2 + 49n - 54)/3,$$
$$(2n^3 - 15n^2 + 49n - 66)/3]\ \textit{TVSS scheme , with}\ c = 6/(2n^3 - 15n^2 + 49n - 60).$$

Clearly, the $(3,n)$ scheme from Example 1 has better parameters.
The parameters of the obtained TVSS scheme can be computed for all k and n. Indeed, the following proposition holds (for a proof, see Appendix B).

PROPOSITION 3. *The parameters of the* $[(k,n); b, h, l]$ *TVSS scheme obtained in Example 2 are given by*

$$b = 2^{k-1}\binom{n}{k},\ h = 2^{k-2}\left[\binom{n}{k} + \binom{n-k}{k} + 1\right],\ \textit{and}\ l = 2^{k-2}\left[\binom{n}{k} + \binom{n-k}{k} - 1\right].$$

EXAMPLE 3. *We apply Construction 1 for obtaining* $2m-1$ *out of* $2m$ *schemes. We take for* θ *the vector (0,0, ... ,0,1,m). The computations in Appendix C imply that we obtain a*

$$\left[(2m-1, 2m); m\binom{2m-1}{m}, \frac{m}{2}\binom{2m-1}{m} + 2^{2m-3}, \frac{m}{2}\binom{2m-1}{m} - 2^{2m-3}\right]$$
$$\textit{TVSS scheme, with}\ c = 2^{2m-2} \ / \ m\binom{2m-1}{m}.$$

Application of Stirling's formula shows that for large m, the contrast behaves like $\sqrt{\frac{\pi}{4m}}$.

3.3. Construction 2

In general, it seems hard to give manageable expressions for the physical parameters (block-length, white level and black level) of the schemes obtained with Construction 1. In this section, we give an explicit construction of (k,n) TVSS schemes for all k and n with $2 < k < n$ that has the virtue that the physical parameters of these schemes can readily be computed. However, the physical parameters of the schemes obtained with Construction 1 (whenever we could compute them) seem to be far superior to those of the schemes obtained with Construction 2.

Again, we construct a (k, n) TVSS scheme from a (k, n) pair of matrices. For constructing these matrices, we use MDS codes over GF(q), the finite field with q elements. An $[n, k]$ MDS code over GF(q) consists of q^k vectors of length n with entries from GF(q) such that any two codewords have Hamming distance at least $n-k+1$. It is known that such a code exists whenever $q+1 \geq n$ [6, Ch. 11, Thm. 9]. Therefore, we choose $q \geq n-1$.

LEMMA 5. *Let C be an $[n, k]$ MDS code over GF(q). In any set of k positions, each of the q^k possible patterns occurs in exactly one of the words of C.*

Proof. Fix k positions. Two codewords that agree in these positions, differ in at most $n-k$ positions. We conclude that each of the q^k patterns agrees with at most one codeword. As the number of patterns equals the number of codewords, each pattern agrees with exactly one codeword in the given positions. ■

Let C be an $[n, k]$ MDS code over GF(q). Let $U(C)$ be an $n \times q^k$ matrix over GF(q) in which each word from C occurs as a column once, and let $A(C)$ be the binary $n \times q^k$ matrix obtained from $U(C)$ by replacing each non-zero symbol in GF(q) by a '1', and the zero-symbol in GF(q) by a '0'.

PROPOSITION 4. *Let $1 \leq j \leq k$. The sum of any j rows of $A(C)$ has weight $\frac{1}{2}q^{k-j}\left[q^j - (2-q)^j\right]$.*

Proof. Consider j rows from $U(C)$. Lemma 5 implies that each of the q^j possible patterns occurs in these j positions in q^{k-j} words from C. The number of patterns with w non-zero elements equals $\binom{j}{w}(q-1)^w$. Each such pattern yields a column in $A(C)$ with exactly w ones in the j prescribed rows. Consequently, the number of ones in the sum of the j rows from $A(C)$ under consideration equals

$$q^{k-j} \sum_{w \text{ odd}} \binom{j}{w}(q-1)^w = \frac{1}{2}q^{k-j}\left((q-1+1)^j - (-1)^j(q-1-1)^j\right). \quad ■$$

PROPOSITION 5. *The sum of any $k+1$ rows of $A(C)$ has weight*

$$\frac{1}{2q}(q^{k+1} - (2-q)^{k+1}) - \frac{q-1}{q}2^k.$$

Proof. Consider $k+1$ positions in C. Any two distinct words from C differ in at least two of these positions. That is, restricted to these $k+1$ positions, C is a $[k+1, k, 2]$ code over GF(q). According to [6, Ch. 11, Thm. 6], the number of words of weight w in such a code equals

$$b_w = \binom{k+1}{w}(q-1)\sum_{j=0}^{w-2}(-1)^j\binom{w-1}{j}q^{w-2-j} = \binom{k+1}{w}\left(\frac{(q-1)^{w-1} - (-1)^{w-1}}{q}\right).$$

The weight of the sum of the rows of $A(C)$ corresponding to the $k+1$ chosen positions is obtained by summing the above expressions for b_w over all odd w. ■

THEOREM 5. *Let $2 \le k \le n-1$, and let q be a prime power not smaller than $n-1$. There exists a*

$$[(k,n); q^k, \frac{1}{2}(q^k + (-1)^k(q-2)^k + (q-1)2^k), \frac{1}{2}(q^k + (-1)^k(q-2)^k)] \text{ TVSS scheme,}$$

with contrast $(q-1)2^{k-1} / \left[q^k + (-1)^k(q-2)^k + (q-1)2^{k-1}\right]$.

Proof. Let C be an $[n,k]$ MDS code over GF(q), and let D be an $[n,k-1]$ MDS code over the same field. In the notation of this section, let A equal $A(C)$, and let B equal the concatenation of q copies of $A(D)$. By combining the above results, (A,B) is a (k,n) pair, and $(P(A),P(B))$ is a TVSS scheme with parameters as claimed in the theorem. ■

4. Bounds on the Parameters *b*, *h* and *l*

In this section, we provide bounds on the parameters of (k,n) TVSS schemes. As shown in Subsection 2.2, a $[(2,n); b, b, l]$ TVSS scheme exists if and only if a binary code of length b with n words and minimum Hamming distance $b-l$ exists. Therefore, for the case $k=2$ we can use the well-established results on error-correcting codes, e.g. [6]. For this reason, we will concentrate on the case that $k \ge 3$.

We start by proving that maximal contrast schemes ($l = 0$) do not exist. We note that for OR-based systems maximal contrast schemes can always be constructed [12].

PROPOSITION 6. *Let $3 \le k < n$. There exists neither a $[(k,n); b, h, 0]$ TVSS scheme, nor a $[(k,n); b, b, l]$ scheme.*

Proof. Let $\mathsf{S} = (\mathscr{C}_0, \mathscr{C}_1)$ be a $[(k,n); b, h, 0]$ TVSS scheme and let $B \in \mathscr{C}_1$. Denote by σ^1, σ^2 two arbitrary rows in B. Since $n-2 \ge k-1$, B contains (at least) $k-1$ more rows. We denote these rows by $\sigma^3, \ldots, \sigma^{k+1}$. Since S is a threshold scheme with $l=0$, the XOR of $\sigma^1, \sigma^3, \sigma^4, \ldots, \sigma^{k+1}$ is the all-one vector, as is the XOR of $\sigma^2, \sigma^3, \sigma^4, \ldots, \sigma^{k+1}$. It follows that $\sigma^1 = \sigma^2$, so all rows of B are equal.

Next, let $A \in \mathscr{C}_0$ and consider row i and j of A. As $k \ge 3$, the indistinguishability property of Definition 1 implies that there is a $B \in \mathscr{C}_1$ that agrees with A in these rows. As all rows of B are equal, the i-th and j-th row of A are equal. Since i and j are arbitrary, all rows of A are equal, so $A = B$, a contradiction.
The second statement follows from an analogous reasoning. ■

Note that Proposition 6 implies that $[(k,n); 1, h, l]$ TVSS schemes do not exist for $1 < k < n$. Moreover, it is noteworthy that $[(2,n); b, b, l]$ TVSS schemes with $l > 0$ exist while $[(2,n); b, h, 0]$ TVSS schemes do not exist.

The next two propositions show that TVSS schemes with odd and even k fundamentally differ.

PROPOSITION 7. *Let k be odd, and let $k<n$. For each $\epsilon>0$, there are integers b, l and h such that $l/b<\epsilon$ and a $[(k,n); b, h, l]$ TVSS scheme exists.*

Proof. Construction 2 of Section 3.3 yields for each prime power $q>n-1$ a $[(k,n); b, h, l]$ TVSS scheme for which

$$\frac{l}{b}=\frac{1}{2}(1-(1-\frac{2}{q})^k).$$ ■

PROPOSITION 8. *Let k be even, and let $k<n$. If a $[(k,n); b, h, l]$ TVSS scheme exists, then $l/b \geq 1/(k+1)$.*

Proof. Let $(\mathscr{C}_0, \mathscr{C}_1)$ be a $[(k,n); b, h, l]$ TVSS scheme. Choose a matrix $B \in \mathscr{C}_1$. Let $\hat{B}$ be a set of $k+1$ arbitrarily chosen rows in B. Let α_1 denote the number of positions in which the rows of $\hat{B}$ all have the same coordinate and let α_2 denote the number of positions in which not all of the $k+1$ rows of $\hat{B}$ have the same coordinate. Note that $\alpha_1+\alpha_2=b$. Consider the $k+1$ subsets of k elements of $\hat{B}$ and compute the sum vector of each of the subsets of k elements. The total number of zeroes z in all these sum vectors together satisfies

$$(k+1)l \geq z \geq (k+1)\alpha_1+\alpha_2 \geq \alpha_1+\alpha_2=b.$$ ■

COROLLARY 2. *For even $k<n$, the contrast of a k out of n TVSS scheme is at most $k/(k+2)$.*

Proof. Let S be a $[(k,n); b, h, l]$ scheme. By definition, the contrast c is equal to $(h-l)/(h+l)$. It is clear that c is increasing in h, and so $c \leq (b-l)/(b+l)$. As $(b-l)/(b+l)$ is decreasing in l, we obtain an upper bound on c by plugging in the upper bound for l from Proposition 8. ■

Just like we wish l to be small, we wish h to be large. If $k=2$, then h can be as large as b (see Section 2.2). For larger k, Construction 2 (combined with Proposition 1, if k is odd) yields (k,n) schemes with h/b arbitrarily close to 1.

To prove Proposition 9, we need two lemmas.

LEMMA 6. *Let k be an even integer. Let B be a binary matrix with n rows such that the sum of any k rows from B differs from $\mathbf{0}$. Then B has at least $n-k+2$ distinct rows.*

Proof. By induction on k. The result is obvious for $k=2$. Now assume that $k \geq 4$, and that B has two equal rows (otherwise we are done). By removing these two rows from B, we obtain a matrix B^* with $n-2$ rows. The sum of any $k-2$ rows

from B^* differs from $\mathbf{0}$, as otherwise these $k-2$ rows and the two removed rows would add up to $\mathbf{0}$. The induction hypothesis implies that B^* (and so surely B) has at least $(n-2)-(k-2)+2=n-k+2$ distinct rows. ■

LEMMA 7. *Let $(\mathscr{C}_0, \mathscr{C}_1)$ be a $[(k,n); b, h, l]$ TVSS scheme with $k \geq 3$, and let c_1 and c_2 be two rows of a matrix in $\mathscr{C}_0$ and hence also two rows of some matrix in $\mathscr{C}_1$. Then, the Hamming distance between c_1 and c_2 satisfies*

$$d(c_1, c_2) \leq \min\{2l, 2(b-h)\}.$$

Proof. Let B be a share matrix in $\mathscr{C}_1$ containing the rows c_1, c_2 and let c denote the sum of $k-1$ other rows. Then, with $\mathbf{1}$ the all-one vector), we have that

$$\begin{aligned} d(c_1, \mathbf{1} \oplus c) = &\text{ the number of zeroes in } (c \oplus c_1) \leq l, \\ &\text{and similarly } d(c_2, \mathbf{1} \oplus c) \leq l. \end{aligned} \tag{17}$$

Combining equation (17) with the triangle inequality, we find that $d(c_1, c_2) \leq 2l$.

A similar reasoning with a matrix $A \in \mathscr{C}_0$ containing the shares c_1, c_2 and the sum $\hat{c}$ of $k-1$ other rows yields that $d(c_1, c_2) \leq 2(b-h)$. ■

PROPOSITION 9. *Let k be even, $k \geq 4$. If a $[(k,n); b, h, l]$ TVSS scheme exists, then*

$$n-k+1 \leq \sum_{i=0}^{\min(l, 2(b-h))} \binom{b}{i}.$$

Proof. Let k be even, $k \geq 4$, and let $\mathsf{S} = (\mathscr{C}_0, \mathscr{C}_1)$ be a $[(k,n); b, h, l]$ scheme. Let B be a matrix in $\mathscr{C}_1$. As $l \neq b$, no k rows of B add to the all-zero word. Lemma 6 implies that B has at least $n-k+2$ distinct rows. Since according to Lemma 7, all rows from B have Hamming distance at most $2(b-h)$ to its top row, we obtain

$$n-k+2 \leq \sum_{i=0}^{2(b-h)} \binom{b}{i}.$$

Now, we assume without loss of generality that the top $n-k+1$ rows of B are distinct. Let $\mathbf{c}$ be the sum of the $k-1$ bottom rows of B. For $1 \leq i \leq n-k+1$, the sum of $\mathbf{c}$ and the i-th row of B contains at most l ones; that is to say, the i-th row of B has Hamming distance at most l to the complement of $\mathbf{c}$. As the $n-k+1$ top rows of B are distinct, $n-k+1$ is at most the number of vectors at distance at most l from the complement of $\mathbf{c}$, so

$$n-k+1 \leq \sum_{i=0}^{l} \binom{b}{i}.$$ ■

Appendix A

Computations for Example 1

By defintion, we have

$$\phi_i = \sum_j S_{i,j}\theta_j = \sum_{j=k}^{n}(j-k+1)(-1)^{i+j}\binom{n-i}{j-i} = \sum_{v=0}^{n-k}(-1)^{i+n+v}(n-k+1-v)\binom{n-i}{v}.$$

According to [14, equation (5.25)], we have for all integers $l, m, p \geq 0$

$$\sum_{v\leq p}\binom{p-v}{m}\binom{s}{v-q}(-1)^v = (-1)^{l+m}\binom{s-m-1}{p-m-q} \tag{18}$$

Note that equation (18) also holds for binomial coefficients of the form $\binom{r}{j}$ with negative r; it is then used that [14, equation (5.14)]

$$\binom{r}{j} = (-1)^j\binom{j-r-1}{j} \text{ for integer } j \text{ and arbitrary } r \tag{19}$$

By applying equation (18) with $m=1, q=0, s=n-i$, and $p=n-k+1$, we obtain that

$$\phi_i = (-1)^{i+k}\binom{n-i-2}{n-k}. \tag{20}$$

This is indeed the claimed result. Note that $\binom{n-i-2}{n-k}=0$ if $0\leq n-i-2<n-k$, that is, $\phi_i=0$ if $k-1\leq i\leq n-2$, and application of equation (19) yields that $\phi_{n-1}=-1$ and that $\phi_n = n-k+1$.

Appendix B

Proof of Proposition 3

We prove Proposition 3 by employing Theorem 4. In Example 2, for each w we have that $|\phi_w| = \binom{n-w}{k-w}$, whence

$$b = \frac{1}{2}\sum_w \binom{n-w}{k-w}\binom{n}{w} = \frac{1}{2}\sum_w \binom{n}{k}\binom{k}{w} = \binom{n}{k}2^{k-1}.$$

As $\theta_k = 1$, $h-l = 2^{k-1}$. Application of Theorem 4 and equation (10) implies that

$$\begin{aligned} h+l &= b + \frac{1}{2}\sum_w \binom{n-w}{k-w}\sum_j \binom{k}{j}(-2)^j\binom{n-j}{w-j} \\ &= b + \frac{1}{2}\sum_j (-2)^j\binom{k}{j}\sum_w \binom{n-w}{k-w}\binom{n-j}{w-j}. \end{aligned}$$

As $\binom{n-w}{k-w}\binom{n-j}{w-j}=\binom{k-j}{w-j}\binom{n-j}{n-k}$, we obtain that

$$h+l=b+\frac{1}{2}\sum_j(-2)^j\binom{k}{j}\binom{n-j}{n-k}\sum_w\binom{k-j}{w-j}=b+\frac{1}{2}\sum_j(-2)^j\binom{k}{j}\binom{n-j}{n-k}2^{k-j}.$$

We apply equation (18) with the following substitutions: $p=n$, $v=j$, $m=n-k$, $s=k$, and $q=0$. Moreover, we apply equation (19) with $r=n-k$. We obtain that

$$h+l=b+2^{k-1}\binom{n-k}{k}=2^{k-1}\left[\binom{n}{k}+\binom{n-k}{k}\right].$$

Appendix C

Computations for Example 3

As $S_{i,2m-1}=(-1)^{i-1}(2m-i)$ and $S_{i,2m}=(-1)^i$, we have that $\phi_i=(-1)^{i+1}(m-i)$. According to Theorem 4, the block length b is given by

$$b=\frac{1}{2}\sum_w|m-w|\binom{2m}{w}.$$

If $m\le w\le 2m$, then $|m-w|\binom{2m}{w}=(w-m)\binom{2m}{w}=|m-(2m-w)|\binom{2m}{2m-w}$, and so

$$\begin{aligned}b&=\sum_{w=0}^{m}(m-w)\binom{2m}{w}=m\sum_{w=0}^{m}\binom{2m}{w}-2m\sum_{w=1}^{m}\binom{2m-1}{w-1}\\&=m\left(\frac{1}{2}\sum_w\binom{2m}{w}+\frac{1}{2}\binom{2m}{m}\right)-m\sum_{j=0}^{2m-1}\binom{2m-1}{j}=\frac{1}{2}m\binom{2m}{m}=m\binom{2m-1}{m}.\end{aligned}$$

For computing l and h, we note that, according to Theorem 4, $h-l=2^{k-1}\phi_k=2^{k-1}=2^{2m-2}$. Theorem 4 also implies that

$$\begin{aligned}h+l&=b+\frac{1}{2}\sum_w|m-w|\sum_i(-1)^i\binom{2m-1}{i}\binom{1}{w-i}\\&=b+\frac{1}{2}\sum_w|m-w|(-1)^w\left[\binom{2m-1}{w}-\binom{2m-1}{w-1}\right]\\&=b+\frac{1}{2}\sum_w|m-w|(-1)^w\ \frac{m-w}{m}\binom{2m}{w}.\end{aligned}$$

For $0\le w\le m$, we have that

$$|m-(2m-w)|(m-(2m-w))\binom{2m}{2m-w}=|w-m|(w-m)\binom{2m}{w}.$$

That is to say, the terms with w and $2m-w$ in the above sum cancel each other, whence $h+l=b$.

Conmemorative Note

Sadly, prof. Jack van Lint passed away on the 28th of September 2004. We have lost a great mathematician, an inspiring collaborator, and a dear friend.

Notes

1. Another Visual Crypto system using an XOR process has been recently introduced in [5]. Their system, being based on interferometric techniques and needing a Mach–Zehnder interferometer is less practical and more expensive.
2. In the literature the pixel expansion is often denoted by m.

References

1. B. Arazi and I. Dinstein, O. Kafri, Intuition, perception and secure communication, *IEEE Transactions on Systems, Man and Cybernetics*, Vol. 19 (1989) pp. 1016–1120.
2. E. Biham and A. Itzkovitz, *Visual Cryptography with Polarization*, http://www.cs.technion.ac.il/ biham/Reports/visual.ps.gz. (1997).
3. C. Blundo, A. De Santis and D. R. Stinson, On the contrast in visual cryptography schemes, *Journal Cryptology,* Vol. 12 (1999) 261–289.
4. C. Droste, *New Results on Visual Cryptography*, *Crypto 96*, LNCS, Vol. 1109, Springer-Verlag, pp. 401–415. (1996).
5. S -S. Lee, J -C. Na, S -W. Sohn, C. Park, D -H. Seo and S -J. Kim, Visual cryptography based on an interferometric encryption technique, *ETRI Journal*, Vol. 24, No. 5 (2002) pp. 373–380.
6. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam-New York-Oxford, North Holland (1977).
7. M. Naor and A. Shamir, *Visual Cryptography, Eurocrypt 94,* LNCS, Vol. 950, Springer-Verlag, pp. 1–12. (1994).
8. M. Naor and B. Pinkas, *Visual Authentication and Identification, Crypto 97*.
9. A. de Santis, *On Visual Cryptography Schemes*, *Proc. Information Theory Workshop*, Killarney, Ireland, (1998) pp. 154–155.
10. D. R. Stinson, *An Introduction to Visual Cryptography, presented at Public Key solutions '97*. Available at http://bibd.unl.edu/ stinson/VCS-PKS.ps. (1997).
11. P. Tuyls, T. Kevenaar, G. J. Schrijen, A. A. M. Staring and M. van Dijk, Visual crypto displays enabling secure communications, In *Security in Pervasive Computing*, LNCS2802, pp. 271–284. (2003).
12. E. Verheul and H. C. A. van Tilborg, Constructions and properties of k out of n Visual Secret Sharing Schemes, *Designs Codes and Cryptography*, Vol. 11 (1997) pp. 179–196.
13. J. Riordan, *Combinatorial Identities*, R. E. Krieger Publishing Company, Huntington, New York (1979).
14. R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley (1992).