Boolean Composition of Visual Secret Sharing Schemes

Hans Ulrich Simon
Fakultät für Mathematik, Ruhr-Universität Bochum, D-44780 Bochum, Germany
hans.simon@rub.de

Topic Classification: Visual Cryptography

Abstract

In this paper, we analyze the disjunction and the conjunction of two access structures for visual secret sharing schemes. The latter operation, when applied to k-out-of-n schemes, leads to schemes with multiple thresholds. We precisely determine the maximum relative contrast for schemes of this type. As in the case of classical schemes with a single threshold, the analysis proceeds by revealing a central relation between the relative contrast in a visual secret sharing scheme and the error-term in a related problem of approximation-theoretic flavor.

1 Introduction

Visual Cryptography and k-out-of-n secret sharing schemes (so-called threshold schemes) are notions introduced by Naor and Shamir [5]. A sender wishing to transmit a secret message distributes n transparencies among n participants of the scheme, where the single transparencies contain seemingly random pictures. A k-out-of-n scheme achieves the following situation. If any k participants stack their transparencies together, then a secret message is revealed visually. On the other hand, if only $k-1$ participants stack their transparencies, or analyze them by any other means, they are not able to obtain any information about the secret message.

The basic model by Naor and Shamir has been extended and generalized in several directions. For example, the concept of "general access structures" [1] allows for a flexible specification of the sets of participants who are qualified for the visual disclosure of the secret. Another variation are the schemes with "perfect reconstruction of black pixels". They are motivated by studies on visual perception and were suggested first in [2]. The main results in this paper are as follows:

1. We consider the conjunction (resp. disjunction) Γ of two given access structures Γ' and Γ'' and show that the corresponding best possible

relative contrast values satisfy the relation $\alpha \geq \frac{1}{2}\alpha'\alpha''$ (resp. $\alpha \geq \min\{\alpha', \alpha''\}$).

2. We show that these relations hold with equality for every disjunction of two arbitrary schemes and every conjunction of two threshold schemes.

3. We extend these results to the Boolean composition of more than two access structures.

In order to show the main result about conjunction of two threshold schemes, we apply the same key techniques that had been used for the determination of the maximum relative contrast, say $\alpha(k, n)$, achievable in a k-out-of-n scheme:
By means of *symmetrization*, it was shown in [3] that $\alpha(k, n)$ can be cast as the maximum gain in a (cleverly designed) linear program. By means of *dualization*, it was shown in [4] that $\alpha(k, n)$ can be cast as the minimum error in a well-known approximation-theoretic problem.
We show that these techniques, when properly used, lead to a tight analysis for threshold schemes with multiple thresholds. The connections to approximation theory that are uncovered on the way may find some interest in their own right.

The intimate relations between visual cryptography and approximation theory provide us with versatile and powerful instruments for the analysis of visual secret sharing schemes. In particular, upper bounds on the maximum relative contrast are found simply by providing feasible solutions for the corresponding (dual) approximation-theoretic problems. A meta-goal in this paper is to bundle the known key techniques and to demonstrate their amazing power.

2 Definitions, Notations and Facts

Let us first fix some general notation. For positive integers n and $n_1 \leq n_2$, $[n]$ denotes the set $\{1, \ldots, n\}$ and, more generally, $[n_1 : n_2]$ denotes the set $\{n_1, n_1 + 1, \ldots, n_2\}$. The least common multiple of two positive integers a, b is denoted $\mathrm{lcm}(a, b)$. The powerset of a set S is denoted 2^S. We say a set T is *maximal* in a collection $K \subseteq 2^S$ of subsets of S, if T belongs to K but no proper superset of T does. δ denotes the Kronecker symbol, i.e., $\delta(a, b) = 1$ if $a = b$, and $\delta(a, b) = 0$ otherwise. For a matrix A with k rows, $A^\top$ denotes its transpose, $A[i]$ denotes its i-th row, and, for every $I \subseteq [k]$, $A[I]$ denotes the submatrix formed by the rows $A[i]$ such that $i \in I$. The entry of A located in the i-th row and the j-th column is denoted $A[i, j]$. For vectors $u, v \in \mathbb{R}^m$, $\langle u, v\rangle$ denotes their scalar product, i.e., $\langle u, v\rangle = \sum_{i=1}^{m} u_i v_i$. For a given decomposition $k = k_1 + k_2$ of the number k of rows, a block-decomposition $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$ implicitly means that A_1 consists of the first k_1 rows of A, and A_2 consists of the last k_2 rows of A. The analogous convention holds for vectors. For Boolean vectors $v, w \in \{0,1\}^m$, $H(w) = \sum_{i=1}^m w_i$ denotes the Hamming-weight of w and $v \vee w = (v_i \vee w_i)_{i \in [m]}$ denotes the entry-wise Boolean disjunction of v and w. A vector with non-negative real coefficients that sum-up to 1 is called a *probability vector*. $\mathcal{P}_k$ denotes the set of univariate polynomials of degree at most k over the reals.

2.1 Visual Secret Sharing Schemes

In this subsection, we recall the definition of general access structures and visual secret sharing schemes from [1].

A *general access structure for a set* $[n]$ *of participants* is pair $\Gamma = (\mathcal{Q}, \mathcal{F})$ such that $\mathcal{Q}, \mathcal{F} \subseteq 2^{[n]}$ and $\mathcal{Q} \cap \mathcal{F} = \emptyset$. $\mathcal{Q}$ contains the so-called *qualified sets*, and $\mathcal{F}$ contains the so-called *forbidden sets*. $\mathcal{F}$ is monotonically decreasing (i.e., every subset of a forbidden set is forbidden too). $\mathcal{F}_0$ denotes the maximal forbidden sets. We consider two examples that will play a major role in this paper:

Example 2.1 *For $\mathcal{Q} = \{X \subseteq [n] : |X| = k\}$, a set is qualified iff it consists of k participants. Clearly, $\mathcal{F}_0 = \{X \subseteq [n] : |X| = k-1\}$.*

Example 2.2 *Let $n = n_1 + n_2$ and $\mathcal{Q} = \{X \subseteq [n] : |X \cap [n_1]| = k_1, |X \cap [n_1 + 1 : n_2]| = k_2\}$. Here a set is qualified if it contains k_1 participants from the "first group" (with numbers between 1 and n_1) and k_2 participants from the second (with numbers between $n_1 + 1$ and n_2). Note that $\mathcal{F}_0$ consists of all sets with either $k_1 - 1$ participants from the first group and all participants from the second, or with $k_2 - 1$ participants from the second group and all participants from the first.*

Let $\Gamma = (\mathcal{Q}, \mathcal{F})$ be an access structure for n participants. A (Γ, m)-*scheme* is given by two multisets of $(n \times m)$-matrices, $\mathcal{C}_0, \mathcal{C}_1$, a function $t : \mathcal{Q} \to [m]$, and a parameter $0 < \alpha \leq 1$ such that the following holds:

1. For every $X \in \mathcal{Q}$ and all $A \in \mathcal{C}_0, B \in \mathcal{C}_1$, $H(\vee_{i \in X} A[i]) \leq t(X) - \alpha m$ and $H(\vee_{i \in X} B[i]) \geq t(X)$.
2. For every $X \in \mathcal{F}$, the multisets $\mathcal{C}_0[X] = \{A[X] : A \in \mathcal{C}_0\}$ and $\mathcal{C}_1[X] = \{B[X] : B \in \mathcal{C}_1\}$ contain the same matrices with the same frequencies.

We refer to the first (resp. second) condition as the "visibility condition" (resp. "security condition"). Note that it suffices to check the security condition for all $X \in \mathcal{F}_0$. The parameter m is called the *pixel expansion* of the scheme; α is called the *relative contrast.* If there exist matrices $G_0, G_1 \in \{0,1\}^{n\times m}$ such that, for $b = 0,1$, $\mathcal{C}_b$ consists of the $m!$ matrices obtained from G_b by a permutation of the columns, we say that the scheme has *generator matrices* G_0, G_1. If the function $t : \mathcal{Q} \to [m]$ assigns value m to every set $X \in \mathcal{Q}$, we say the scheme *perfectly reconstructs black pixels.* A scheme for the access structure from Example 2.1 is simply called *k-out-of-n* or *(k,n)-scheme* in this paper. A scheme for the access structure from Example 2.2 is called $(k_1,n_1;k_2,n_2)$-scheme. The maximum relative contrast achievable in a (k,n)-scheme (resp. $(k_1,n_1;k_2,n_2)$-scheme) is denoted $\alpha(k,n)$ (resp. $\alpha(k_1,n_1;k_2,n_2)$).

A *(Γ,m)-scheme* is used as follows to achieve the situation described in the introduction. A (black or white) pixel of a secret image is decomposed into m subpixels which are arranged in a fixed pattern (e.g., a rectangle). If the sender wishes to transmit a white pixel, she randomly chooses a matrix $A \in \mathcal{C}_0$ and transmits $A[i]$ to the i-th participant. The handling of black pixels is analogous: the i-th participant obtains the row $B[i]$ of a matrix B randomly chosen from $\mathcal{C}_1$. The security condition makes sure that, for forbidden sets of participants, the transmission of a white pixel is statistically indistinguishable from the transmission of a black pixel. The visibility condition makes sure that participants of a qualified set may stack their transparencies together so that a black pixel has a fraction of black subpixels (actually fraction 1 in case of perfect reconstruction) that exceeds the fraction of black sub-pixels of a white pixel by at least α. It is obviously desirable to maximize the relative contrast.[1]

2.2 Contrast as Objective Function in a Linear Program

The following result casts the problem of maximizing the relative contrast as an instance of Linear Programming:

Theorem 2.3 ([3]) *$\alpha(k,n)$ equals the maximal value of*

$$\alpha = \sum_{j=0}^{n-k} \binom{n-k}{j} \binom{n}{j}^{-1} (x_j - y_j) \tag{1}$$

subject to the following constraints:

(1-LP1) *x and y are probability vectors.*

(1-LP2) *For all $l = 0,\dots,k-1$, $\sum_{j=l}^{n-k+l+1} \binom{n-k+1}{j-l}\binom{n}{j}^{-1}(x_j - y_j) = 0$.*

[1] In this paper, we sweep the conflicting goal of minimizing the pixel expansion under the carpet.

The essential features of the linear program from Theorem 2.3 are nicely captured by the following definition of a linear program $\mathrm{LP}_{c,A}(k,n)$:

Maximize $\langle c, x-y\rangle = \sum_{j=0}^{n} c_j(x_j - y_j)$

subject to (1-LP1) and $A(x-y) = 0$.

Here, c, x, y are vectors with components c_j, x_j, y_j, respectively, and with j ranging from 0 to n. A is an arbitrary real-valued matrix with k rows and $1+n$ columns. We say $\mathrm{LP}_{c,A}(k,n)$ is of *type 1-BAP (with polynomials $P \in \mathcal{P}_k$ and $Q_0, \ldots, Q_{k-1} \in \mathcal{P}_{k-1}$ as "witnesses")* if the following conditions are satisfied:

(1-BAP1) For all $j = 0, \ldots, n$, $c_j = P(j)$.

(1-BAP2) For all $l = 0, \ldots, k-1$ and all $j = 0, \ldots, n$, $A[l,j] = Q_l(j)$.

(1-BAP3) Every polynomial of degree at most $k-1$ is a linear combination of the polynomials $Q_0, \ldots, Q_{k-1}$.

We denote the value of an optimal solution for $\mathrm{LP}_{c,A}(k,n)$ by $\alpha_{c,A}(k,n)$ in what follows.

Theorem 2.4 ([4]) *Maximizing the value of α in (1) subject to the constraints (1-LP1), (1-LP2) is of type 1-BAP.*

Note that $\alpha_{c,A}(k,n)$ collapses to $\alpha(k,n)$ — the maximum relative contrast achievable by a (k,n)-scheme — when c and A are chosen so as to obtain the linear program from Theorem 2.3.
For every $P \in \mathcal{P}_k$, we define the following function in k, n:

$$\beta_P(k,n) = \min_{Q \in \mathcal{P}_{k-1}} \max_{j=0,\ldots,n} |P(j) - Q(j)| \tag{2}$$

A polynomial in $\mathcal{P}_{k-1}$ that minimizes the right hand-side of (2) is called a *best approximating polynomial in $\mathcal{P}_{k-1}$ for $P \in \mathcal{P}_k$*. The following result links together visual cryptography and approximation theory:

Theorem 2.5 ([4]) *If $\mathrm{LP}_{c,A}(k,n)$ is of type 1-BAP and P is the polynomial which witnesses (1-BAP1), then $\alpha_{c,A}(k,n) = 2 \cdot \beta_P(k,n)$.*

3 The Composition of Two Access Structures

Let Γ' and Γ'' be two access structures with disjoint sets of participants. The access structure $\Gamma' \wedge \Gamma'' = (\mathcal{Q}, \mathcal{F})$, called the *(Boolean) conjunction of* Γ' *and* Γ'', is given by $\mathcal{Q} = \{X \cup Y : X \in \mathcal{Q}' \wedge Y \in \mathcal{Q}''\}$ and $\mathcal{F} = \{X \cup Y : X \in \mathcal{F}' \vee Y \in \mathcal{F}''\}$. The (Boolean) disjunction (already discussed in [1]) is defined analogously by setting $\mathcal{Q} = \{X \cup Y : X \in \mathcal{Q}' \vee Y \in \mathcal{Q}''\}$ and $\mathcal{F} = \{X \cup Y :$

$X \in \mathcal{F}' \wedge Y \in \mathcal{F}''\}$. Note that the access structure for a $(k_1, n_1; k_2, n_2)$-scheme is the conjunction of the access structure for a (k_1, n_1)-scheme and the access structure for a (k_2, n_2)-scheme. The *r-fold replication of a multiset* $\mathcal{C}$ of matrices is the multiset $\mathcal{C}(r) = \{[C_1|\cdots|C_r] : C_1, \ldots, C_r \in \mathcal{C}\}$ where the multiplicity of the composed matrix is the product of the multiplicities of the r building blocks. The *r-fold replication of a* (Γ, m)*-scheme* given by $\mathcal{C}_0, \mathcal{C}_1$ is the (Γ, rm)-scheme given by $\mathcal{C}_0(r), \mathcal{C}_1(r)$. r-fold replication increases the pixel expansion by factor r but leaves the relative contrast unchanged. The first main result in this paper is as follows:

Theorem 3.1 *A* (Γ', m')*-scheme achieving relative contrast* α' *and a* (Γ'', m'')*-scheme achieving relative contrast* α'' *can be transformed into a* $(\Gamma' \wedge \Gamma'', 2 \cdot \mathrm{lcm}(m', m'')^2\})$*-scheme (called the* conjunction of the two given schemes*) achieving relative contrast* $\frac{1}{2}\alpha'\alpha''$*. Moreover this transformation preserves perfect reconstruction of black pixels, i.e., if the given two schemes perfectly reconstruct black pixels then the composed scheme does this too.*

Proof: Let $m = \mathrm{lcm}(m', m'')$. Thanks to the replication trick, we easily get a (Γ', m)- and a (Γ'', m)-scheme, say the former is given by $\mathcal{C}_0', \mathcal{C}_1'$ and the latter by $\mathcal{C}_0'', \mathcal{C}_1''$. (Recall that replication leaves the relative contrast unchanged.) For a matrix M with m columns, $R_0(M), \ldots, R_{m-1}(M)$ denote the m matrices obtained from M by cyclic rotations of the columns. We now define the multisets of matrices, $\mathcal{C}_0$ and $\mathcal{C}_1$, that represent the desired $(\Gamma' \wedge \Gamma'', 2m^2\})$-scheme. Let A' (resp. B', A'', B'') range over all matrices in $\mathcal{C}_0'$ (resp. $\mathcal{C}_1', \mathcal{C}_0'', \mathcal{C}_1''$). Then, by definition, $\mathcal{C}_0$ contains all matrices of the form

$$A = \left[\begin{array}{c|c|c|c|c|c} A' & \cdots & A' & B' & \cdots & B' \\ R_0(A'') & & R_{m-1}(A'') & R_0(B'') & & R_{m-1}(B'') \end{array}\right] \tag{3}$$

and all matrices that are mirror-images of (3) in the sense that the final m blocks in (3) come first and the first m blocks in (3) come last. Similarly, $\mathcal{C}_1$ contains all matrices of the form

$$B = \left[\begin{array}{c|c|c|c|c|c} A' & \cdots & A' & B' & \cdots & B' \\ R_0(B'') & & R_{m-1}(B'') & R_0(A'') & & R_{m-1}(A'') \end{array}\right] \tag{4}$$

together with the corresponding mirror images. In both multisets, the multiplicity of the composed matrix is, by definition, the product of the multiplicities of A', B', A'', B'', respectively. The theorem is now obtained from the following

Claim 1: $\mathcal{C}_0, \mathcal{C}_1$ satisfy the security condition and achieve relative contrast $\frac{1}{2}\alpha'\alpha''$. Moreover, if $\mathcal{C}_0', \mathcal{C}_1'$ and $\mathcal{C}_0'', \mathcal{C}_1''$ perfectly reconstruct black pixels, then $\mathcal{C}_0, \mathcal{C}_1$ does this too.

The proof of the claim is found in Section A of the appendix. •

The transformation in Theorem 3.1 creates very large multisets $\mathcal{C}_0, \mathcal{C}_1$. Fortunately, these multisets can often be stored succinctly by means of an implicit representation. An example illustrating implicit representations and, of course, the transformation itself is found in Section B of the appendix.

As proved in Section C of the appendix, a result analogous to Theorem 3.1 holds for the disjunction of two access structures. Here, the relative contrast achieved by the composed scheme is $\min\{\alpha', \alpha''\}$.
The following result is an immediate consequence of Theorem 3.1:

Corollary 3.2 *Let Γ' (resp. Γ'') be an access structure with maximum relative contrast α'_{max} (resp. α''_{max}). Then, the maximum relative contrast α_{max} of a scheme for $\Gamma' \wedge \Gamma''$ satisfies $\alpha_{max} \geq \frac{1}{2}\alpha'_{max}\alpha''_{max}$. This relation holds correspondingly for schemes that perfectly reconstruct black pixels.*

4 Conjunction of Two Threshold-Schemes

The main result in this section, Theorem 4.6, implies that the transformation from Theorem 3.1 is "contrast-optimal" (i.e., transforms two schemes achieving the maximum relative contrast, respectively, into a composed scheme which does this too) whenever it is applied to threshold schemes. The corresponding result for the disjunction of two arbitrary schemes is found in Section C of the appendix. The following result is the counterpart to Theorem 2.3:

Theorem 4.1 *$\alpha(k_1, n_1; k_2, n_2)$ equals the maximal value of*

$$\alpha = \sum_{j_1=0}^{n_1-k_1} \sum_{j_2=0}^{n_2-k_2} \binom{n_1-k_1}{j_1} \binom{n_2-k_2}{j_2} \binom{n_1}{j_1}^{-1} \binom{n_2}{j_2}^{-1} (x_{j_1,j_2} - y_{j_1,j_2}) \quad (5)$$

subject to the following constraints:

(2-LP1) *x and y are (doubly indexed) probability vectors.*

(2-LP2) *For all $l_1 = 0, \ldots, k_1 - 1$ and all $l_2 = 0, \ldots, n_2$,*

$$\sum_{j_1=l_1}^{n_1-k_1+l_1+1} \binom{n_1-k_1+1}{j_1-l_1} \binom{n_1}{j_1}^{-1} (x_{j_1,l_2} - y_{j_1,l_2}) = 0 \ .$$

For all $l_1 = 0, \ldots, n_1$ and all $l_2 = 0, \ldots, k_2 - 1$,

$$\sum_{j_2=l_2}^{n_2-k_2+l_2+1} \binom{n_2-k_2+1}{j_2-l_2} \binom{n_2}{j_2}^{-1} (x_{l_1,j_2} - y_{l_1,j_2}) = 0 \ .$$

The proof of this theorem is found in Section D of the appendix.

The essential features of the linear program from Theorem 4.1 are nicely captured by the following definition of a linear program $\mathrm{LP}_{c,A}(k_1, n_1; k_2, n_2)$:

Maximize $\langle c, x - y\rangle = \sum_{j_1=0}^{n_1} \sum_{j_2=0}^{n_2} c_{j_1,j_2}(x_{j_1,j_2} - y_{j_1,j_2})$

subject to (2-LP1) and $A(x - y) = 0$.

Here c, x, y are vectors (viewed as one-dimensional) with components c_{j_1,j_2}, x_{j_1,j_2}, y_{j_1,j_2}, respectively, and with j_b ranging from 0 to n_b for $b = 1, 2$. A is an arbitrary real-valued matrix with $(1+n_1)(1+n_2)$ columns. The columns of A are addressed by the double indices j_1, j_2 so that the format of the rows of A fits with the format of x and y. We say $\mathrm{LP}_{c,A}(k_1, n_1; k_2, n_2)$ is of *type 2-BAP* if there exist vectors $c^{(1)} \in \mathbb{R}^{1+n_1}$, $c^{(2)} \in \mathbb{R}^{1+n_2}$ and matrices $A'_1 \in \mathbb{R}^{k_1\times n_1}$, $A'_2 \in \mathbb{R}^{k_2\times n_2}$ such that following holds:

1. $\mathrm{LP}_{c^{(1)},A'_1}(k_1, n_1)$ is of type 1-BAP, say with witnesses $P_1 \in \mathcal{P}_{k_1}$ and $Q_0, \ldots, Q_{k_1-1} \in \mathcal{P}_{k_1-1}$.

2. $\mathrm{LP}_{c^{(2)},A'_2}(k_2, n_2)$ is of type 1-BAP, say with witnesses $P_2 \in \mathcal{P}_{k_2}$ and $R_0, \ldots, R_{k_2-1} \in \mathcal{P}_{k_2-1}$.

3. For all $j_1 = 0, \ldots, n_1$ and all $j_2 = 0, \ldots, n_2$,
$$c_{j_1,j_2} = c^{(1)}_{j_1} \cdot c^{(2)}_{j_2} = P_1(j_1) \cdot P_2(j_2) \ . \tag{6}$$

4. A can be written in the form $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$ such that the following holds:

   (a) The rows of A_1 are addressed (l_1, l_2) with l_1 ranging from 0 to $k_1 - 1$ and l_2 ranging from 0 to n_2. For every row (l_1, l_2) of A_1,
   $$A_1[(l_1, l_2), (j_1, j_2)] = A'_1[l_1, j_1] \cdot \delta(l_2, j_2) = Q_{l_1}(j_1) \cdot \delta(l_2, j_2) \ . \tag{7}$$

   (b) The rows of A_2 are addressed (l_1, l_2) with l_1 ranging from 0 to n_1 and l_2 ranging from 0 to $k_2 - 1$. For every row (l_1, l_2) of A_2,
   $$A_2[(l_1, l_2), (j_1, j_2)] = A'_2[l_2, j_2] \cdot \delta(l_1, j_1) = R_{l_2}(j_2) \cdot \delta(l_1, j_1) \ . \tag{8}$$

We denote the value of an optimal solution for $\mathrm{LP}_{c,A}(k_1, n_1; k_2, n_2)$ by $\alpha_{c,A}(k_1, n_1; k_2, n_2)$ in what follows. We briefly note that the second equalities in (6), (7), (8), respectively, are redundant as they are implied by the first two conditions. We included them explicitly for ease of later reference.

Lemma 4.2

$$\alpha_{c,A}(k_1, n_1; k_2, n_2) \geq \frac{1}{2} \cdot \alpha_{c^{(1)},A'_1}(k_1, n_1) \cdot \alpha_{c^{(2)},A'_2}(k_2, n_2) \tag{9}$$

Proof: For $b = 1, 2$, let $x^{(b)}, y^{(b)}$ be an optimal solution for the linear program $\mathrm{LP}_{c^{(b)},A'_b}(k_b, n_b)$. Thus, $x^{(b)}$ and $y^{(b)}$ are probability vectors and $A'_b(x^{(b)} - y^{(b)}) = 0$. For $j_1 = 0, \ldots, n_1$ and $j_2 = 0, \ldots, n_2$, let

$$x_{j_1,j_2} = \frac{1}{2} \cdot (x^{(1)}_{j_1} x^{(2)}_{j_2} + y^{(1)}_{j_1} y^{(2)}_{j_2}) \text{ and } y_{j_1,j_2} = \frac{1}{2} \cdot (x^{(1)}_{j_1} y^{(2)}_{j_2} + y^{(1)}_{j_1} x^{(2)}_{j_2}) \ .$$

Note that

$$x_{j_1,j_2} - y_{j_1,j_2} = \frac{1}{2} \cdot (x^{(1)}_{j_1} - y^{(1)}_{j_1}) \cdot (x^{(2)}_{j_2} - y^{(2)}_{j_2}) \ . \tag{10}$$

The theorem is now obtained from the following

Claim 2: x, y is a feasible solution for the linear program $\mathrm{LP}_{c,A}(k_1, n_1; k_2, n_2)$, and the target function α evaluated at x, y yields the right hand-side of (9).

The proof of Claim 2 is found in Section E of the appendix. •

Theorem 4.3 *Maximizing the value of α in (5) subject to the constraints (2-LP1), (2-LP2) is of type 2-BAP.*

Proof: The problem is obviously of the form $\mathrm{LP}_{c,A}(k_1, n_1; k_2, n_2)$. In particular (compare with (5)),

$$c_{j_1,j_2} = \underbrace{\binom{n_1 - k_1}{j_1}\binom{n_1}{j_1}^{-1}}_{=:c^{(1)}_{j_1}} \cdot \underbrace{\binom{n_2 - k_2}{j_2}\binom{n_2}{j_2}^{-1}}_{=:c^{(2)}_{j_2}} \ . \tag{11}$$

Moreover (compare with (2-LP2)), A can be written in the form $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$ where

$$A_1[(l_1, l_2), (j_1, j_2)] = \underbrace{\binom{n_1 - k_1 + 1}{j_1 - l_1}\binom{n_1}{j_1}^{-1}}_{=:A'_1[l_1,j_1]} \cdot \delta(l_2, j_2) \ , \tag{12}$$

$$A_2[(l_1, l_2), (j_1, j_2)] = \underbrace{\binom{n_2 - k_2 + 1}{j_2 - l_2}\binom{n_2}{j_2}^{-1}}_{=:A'_2[l_2,j_2]} \cdot \delta(l_1, j_1) \ . \tag{13}$$

According to Theorem 2.4, the linear programs $\mathrm{LP}_{c^{(b)},A'_b}(k_b, n_b)$ are of type 1-BAP for $b = 1, 2$. Our discussion shows that the problem we started with is of type 2-BAP. •

According to Theorem 4.3 and its proof, $\alpha_{c,A}(k_1, n_1; k_2, n_2)$ collapses to $\alpha(k_1, n_1; k_2, n_2)$ when c is chosen according to (11) and $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$ is chosen according to (12), (13).

The next step is dualization. To this end, we consider again an arbitrary linear program of type 2-BAP (witnessed by polynomials $P_1, P_2, Q_0, \ldots, Q_{k_1-1}, R_0, \ldots, R_{k_2-1}$). The two equality constraints in (2-LP1) lead to the dual variables t_1 and t_2, respectively. As for the equality constraints $A(x-y) = 0$, we create the dual variable u_{l_1,l_2} for every row $(l_1, l_2) \in [0 : k_1 - 1] \times [0 : n_2]$ of A_1 and a dual variable v_{l_1,l_2} for every row $(l_1, l_2) \in [0 : n_1] \times [0 : k_2 - 1]$ of A_2. Now dualization leads to the following problem:

Minimize $t_1 + t_2$

subject to $A_1^\top u + A_2^\top v + (t_1, \ldots, t_1)^\top \geq c$ and $A_1^\top u + A_2^\top v - (t_2, \ldots, t_2)^\top \leq c$.

We refer to $A_1^\top u + A_2^\top v + (t_1, \ldots, t_1)^\top \geq c$ (resp. $A_1^\top u + A_2^\top v - (t_2, \ldots, t_2)^\top \leq c$) as the "$x$-constraints" (resp. "$y$-constraints") because they correspond to the primal variables x_{j_1,j_2} (resp. y_{j_1,j_2}).

The vector $A_1^\top u + A_2^\top v$ has an approximation-theoretic interpretation which becomes evident from the following calculation for an arbitrary but fixed index pair (j_1, j_2):

$$\begin{aligned}(A_1^\top u)_{j_1,j_2} &= \sum_{l_2=0}^{n_2} \sum_{l_1=0}^{k_1-1} u_{l_1,l_2} A_1[(l_1, l_2), (j_1, j_2)] \\ &\stackrel{(7)}{=} \sum_{l_2=0}^{n_2} \sum_{l_1=0}^{k_1-1} u_{l_1,l_2} Q_{l_1}(j_1) \delta(l_2, j_2) \\ &= \sum_{l_1=0}^{k_1-1} u_{l_1,j_2} Q_{l_1}(j_1) =: Q^{(j_2)}(j_1)\end{aligned}$$

Since u is a vector of unconstrained variables and $Q_0, \ldots, Q_{k_1-1}$ span the space of all polynomials of degree at most $k_1 - 1$, the outcome of our calculation, $Q^{(j_2)}(j_1)$, is an arbitrary polynomial of degree at most $k_1 - 1$ in variable j_1. It is important to note that there are $n_2 + 1$ such polynomials at our disposal: one for each value of j_2. A similar calculation shows that, for every fixed j_1, $(A_2^\top v)_{j_1,j_2}$ can be viewed as an arbitrary polynomial, say $R^{(j_1)}(j_2)$, of degree at most $k_2 - 1$ in variable j_2. It follows from this discussion and from $c_{j_1,j_2} = P_1(j_1)P_2(j_2)$ that the x_{j_1,j_2}-constraint (with $j_b = 0, \ldots, n_b$ for $b = 1, 2$) can be rewritten as

$$P_1(j_1)P_2(j_2) - (Q^{(j_2)}(j_1) + R^{(j_1)}(j_2)) \leq t_1 \ , \tag{14}$$

and, similarly, the y_{j_1,j_2}-constraint can be rewritten as

$$(Q^{(j_2)}(j_1) + R^{(j_1)}(j_2)) - P_1(j_1)P_2(j_2) \leq t_2 \ . \tag{15}$$

Consider the following approximation problem for given polynomials $P_1 \in \mathcal{P}_{k_1}$ and $P_2 \in \mathcal{P}_{k_2}$: find polynomials $Q^{(0)}, \ldots, Q^{(n_2)} \in \mathcal{P}_{k_1-1}$ and $R^{(0)}, \ldots, R^{(n_1)} \in \mathcal{P}_{k_2-1}$ which minimize

$$\max_{j_1=0,\ldots,n_1; j_2=0,\ldots,n_2} \left| P_1(j_1)P_2(j_2) - (Q^{(j_2)}(j_1) + R^{(j_1)}(j_2)) \right| \ . \tag{16}$$

The smallest possible value of (16) is denoted $\beta_{P_1,P_2}(k_1, n_1; k_2, n_2)$. With this notation, the following holds:

Lemma 4.4 *Consider a linear program* $\mathrm{LP}_{c,A}(k_1, n_1; k_2, n_2)$ *of type 2-BAP. Let* $P_1 \in \mathcal{P}_{k_1}$ *and* $P_2 \in \mathcal{P}_{k_2}$ *be the polynomials satisfying (6). Then the following holds:*

$$\alpha_{c,A}(k_1, n_1; k_2, n_2) = 2 \cdot \beta_{P_1,P_2}(k_1, n_1; k_2, n_2) \tag{17}$$

Proof: By duality, the optimal value of the primal, $\alpha_{c,A}(k_1, n_1; k_2, n_2)$, equals the optimal value of the dual. It is evident from (14) and (15) that the cost function in the dual, $t_1 + t_2$, measures the worst approximation error occurring on pairs $(j_1, j_2) \in [0 : n_1] \times [0 : n_2]$ when we try to approximate $P_1(j_1)P_2(j_2)$ by a polynomial of the form $Q^{(j_2)}(j_1) + R^{(j_1)}(j_2)$: t_1 (resp. t_2) accounts for errors where the approximation underestimates (resp. overestimates) the true value. The lemma now follows by observing that the constant terms in the polynomials $Q^{(j_2)}, R^{(j_1)}$ can be chosen so as to bring the two error terms, t_1 and t_2, into balance. •

Lemma 4.5 *For all polynomials* $P_1 \in \mathcal{P}_{k_1}$, $P_2 \in \mathcal{P}_{k_2}$, *the following holds:*

$$\beta_{P_1,P_2}(k_1, n_1; k_2, n_2) \le \beta_{P_1}(k_1, n_1) \cdot \beta_{P_2}(k_2, n_2)$$

Proof: For $b = 1, 2$, let $P_b^* \in \mathcal{P}_{k_b-1}$ denote the best approximating polynomial for P_b. For

$$Q^{(j_2)}(j_1) = P_2(j_2)P_1^*(j_1) \quad \text{and} \quad R^{(j_1)}(j_2) = P_2^*(j_2)(P_1(j_1) - P_1^*(j_1)) \ , \tag{18}$$

we get

$$P_1(j_1)P_2(j_2) - (Q^{(j_2)}(j_1) + R^{(j_1)}(j_2)) = (P_1(j_1) - P_1^*(j_1)) \cdot (P_2(j_2) - P_2^*(j_2)) \ .$$

Since the absolute value of the latter expression is bounded by $\beta_{P_1}(k_1, n_1) \cdot \beta_{P_2}(k_2, n_2)$ for all $j_1 = 0, \ldots, n_2$ and all $j_2 = 0, \ldots, n_2$, the lemma follows. •

We are ready now for the main result in this section:

Theorem 4.6 *The following equalities are valid:*

$$\beta_{P_1,P_2}(k_1,n_1;k_2,n_2) = \beta_{P_1}(k_1,n_1)\cdot\beta_{P_2}(k_2,n_2) \quad (19)$$

$$\alpha_{c,A}(k_1,n_1;k_2,n_2) = \frac{1}{2}\cdot\alpha_{c^{(1)},A_1'}(k_1,n_1)\cdot\alpha_{c^{(2)},A_2'}(k_2,n_2) \quad (20)$$

$$\alpha(k_1,n_1;k_2,n_2) = \frac{1}{2}\cdot\alpha(k_1,n_1)\cdot\alpha(k_2,n_2) \quad (21)$$

Proof: According to Lemma 4.5, $\beta_{P_1,P_2}(k_1,n_1;k_2,n_2) \le \beta_{P_1}(k_1,n_1)\cdot\beta_{P_2}(k_2,n_2)$. The converse direction is obtained as follows:

$$\beta_{P_1,P_2}(k_1,n_1;k_2,n_2) \overset{(17)}{=} \frac{1}{2}\cdot\alpha_{c,A}(k_1,n_1;k_2,n_2) \overset{(9)}{\ge}$$

$$\frac{1}{4}\cdot\alpha_{c^{(1)},A_1}(k_1,n_1\cdot\alpha_{c^{(2)},A_2}(k_2,n_2 \overset{(17)}{=} \beta_{P_1}(k_1,n_1)\cdot\beta_{P_2}(k_2,n_2)$$

Equation (20) follows directly from (19) and (17). According to Theorem 4.3, (21) is a special case of (20). •

An extension of our results to the Boolean composition of more than two access structures is found in Section F of the appendix.

We conjecture that the equalities in Theorem 4.6 hold correspondingly for schemes with perfect reconstruction of black pixels. But, although it easy to adjust the linear program accordingly, the resulting approximation-theoretic problem is surprisingly hard to analyze.

References

[1] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. Visual cryptography for general access structures. *Information and Computation*, 129(2):86–106, 1996.

[2] Eric R. Henk and Henk C. A. van Tilborg. Constructions and properties of k out of n visual secrete sharing schemes. *Design, Codes and Cryptography*, 11(2):179–196, 1997.

[3] Thomas Hofmeister, Matthias Krause, and Hans U. Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Theoretical Computer Science*, 240(2):471–485, 2000.

[4] Matthias Krause and Hans U. Simon. Determining the optimal contrast for secret sharing schemes in visual cryptography. *Combinatorics, Probability and Computing*, 12(3):285–299, 2003.

[5] Moni Naor and Adi Shamir. Visual cryptography. In *Proceedings of the Conference on Advances in Cryptology — EUROCRYPT '94*, pages 1–12. Springer-Verlag, LNCS 950, 1994.

A Proof of Claim 1

As for the security condition, let us consider a forbidden set $X \cup Y$ such that $X \in \mathcal{F}'$ or $Y \in \mathcal{F}''$. Let us assume that $X \in \mathcal{F}'$ and $Y \in \mathcal{Q}''$. (The other cases are similar.) Fix a matrix $A \in \mathcal{C}_0$ of the form (3). Then, $A[X \cup Y]$ equals

$$\left[\begin{array}{c|c|c|c|c|c} A'[X] & \multirow{2}{*}{\ldots} & A'[X] & B'[X] & \multirow{2}{*}{\ldots} & B'[X] \\ R_0(A'')[Y] & & R_{m-1}(A'')[Y] & R_0(B'')[Y] & & R_{m-1}(B'')[Y] \end{array} \right] . \tag{22}$$

(The case of the mirror image is similar.) If $A'[X]$ occurs m'_0 times in $\mathcal{C}'_0[X]$, $B'[X]$ occurs m'_1 times in $\mathcal{C}'_1[X]$, $A''[Y]$ occurs m''_0 times $\mathcal{C}''_0[Y]$, and $B''[Y]$ occurs m''_1 times in $\mathcal{C}''_1[Y]$, then, since $X \in \mathcal{F}'$, $A'[X]$ occurs m'_0 times in $\mathcal{C}'_1[X]$ and $B'[X]$ occurs m'_1 times in $\mathcal{C}'_0[X]$. Notice that $A''[Y] \neq B''[Y]$ because $Y \in \mathcal{Q}''$. It follows that $A[X \cup Y]$ occurs $m'_0 m'_1 m''_0 m''_1$ times in $\mathcal{C}_0[X \cup Y]$. Note that, since $A'[X]$ occurs m'_0 times in $\mathcal{C}'_1[X]$, we may alternatively think of $A'[X]$ as a sub-matrix of the form $\tilde{B}'[X]$ where $\tilde{B}' \in \mathcal{C}'_1$. Similarly, we may think of $B'[X]$ as a submatrix of the form $\tilde{A}'[X]$ where $\tilde{A}' \in \mathcal{C}'_0$. Performing these substitutions in (22), we arrive at a sub-matrix that is a mirror image of (4) (with $\tilde{A}'$ in the role of A' and $\tilde{B}'$ in the role of B'). The punchline of this discussion is that (22) occurs $m'_0 m'_1 m''_0 m''_1$ times in $\mathcal{C}_1[X \cup Y]$ (the same frequency that we had analyzed for $\mathcal{C}_0[X \cup Y]$). Thus, the security condition is satisfied.

We move on to the visibility condition. Let us assume that $X \in \mathcal{Q}'$ and $Y \in \mathcal{Q}''$. It suffices to show that, for all matrices A, B of the form (3) resp. (4), the number of zero-columns in $A[X \cup Y]$ exceeds the number of zero-columns in $B[X \cup Y]$ by at least $\alpha' \alpha'' m^2$ (which leads to the desired relative contrast $\frac{1}{2}\alpha'\alpha''$). According to our assumptions, $B'[X]$ has at least $t'(X)$ nonzero-columns whereas the number of nonzero-columns in $A'[X]$ is at most $t'(X) - \alpha' m$. Let $s' = m - t'(X)$ and $s'' = m - t''(Y)$. With this notation, $A'[X]$ has at least $s' + \alpha' m$ zero-columns whereas the number of zero-columns in $B[X]$ is at most s'. The analogous remark applies to $A''[Y]$ and $B''[Y]$. Note that the rotations in (3) make sure that every zero-column in $A'[X]$ (resp. $B'[X]$) is aligned with every zero-column in $A''[Y]$ (resp. $B''[Y]$) exactly once. Similarly, the rotations in (4) make sure that every zero-column in $A'[X]$ (resp. $B'[X]$) is aligned with every zero-column in $B''[Y]$ (resp. $A''[Y]$) exactly once. It follows that $A[X \cup Y]$ has at least $(s' + \alpha' m) \cdot (s'' + \alpha'' m) + s's''$ zero-columns whereas the number of zero-columns in $B[X \cup Y]$ is at most $(s' + \alpha' m) \cdot s'' + (s'' + \alpha'' m) \cdot s'$. The difference between these values is at least $\alpha' \alpha'' m^2$, as desired. As for the preservation of perfectly reconstructing black pixels, we briefly observe that a scheme perfectly reconstructs black pixels iff, for every qualified set X and every $B \in \mathcal{C}_1$, the submatrix $B[X]$ does not contain any zero-column. Next, we observe that replication and rotation (of columns) preserve the matrix-property of not having any zero-column. We finally observe that the matrices from $\mathcal{C}_1$, like (4) or the corresponding mirror-image, have a (possibly rotated) matrix from either $\mathcal{C}_1'$ or $\mathcal{C}_1''$ in each of the $2m$ blocks. Thus these matrices do not contain any zero-column provided that none of the matrices from $\mathcal{C}_1$ or $\mathcal{C}_1''$ does this.

B Illustration of Theorem 3.1

We apply the transformation from Theorem 3.1 to a $(2,2)$-scheme $\mathcal{C}_0', \mathcal{C}_1'$ and a $(2,6)$-scheme $\mathcal{C}_0'', \mathcal{C}_1''$ and obtain a $(2,2;2,6)$-scheme $\mathcal{C}_0, \mathcal{C}_1$. As for the $(2,2)$-scheme resp. $(2,6)$-scheme), we may use the following generator matrices G_0', G_1' (resp. G_0'', G_1''):

$$G_0' = \begin{bmatrix} 10 \\ 10 \end{bmatrix} \quad , \quad G_1' = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$$

$$G_0'' = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \quad , \quad G_0'' = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Obviously, $m' = 2$, $\alpha' = 1/2$, $m'' = 4$, and $\alpha'' = 1/4$ so that $m = \mathrm{lcm}(m', m'') = 4$ and the matrices of the $(2,2)$-scheme have to be replicated twice. Instead of computing the multisets $\mathcal{C}_0', \mathcal{C}_1', \mathcal{C}_0'', \mathcal{C}_1''$ explicitly, we use the above matrices G_0', G_1', G_0'', G_1'' as implicit representations. In order to pick a matrix A of the form (3) at random from $\mathcal{C}_0$ (or a matrix B of the form (4) at random from $\mathcal{C}_1$), we may proceed as follows:

- A' (resp. B') is the horizontal concatenation of two matrices that, up to two independent random permutations of the columns, equal G_0' (resp. G_1').
- A'' (resp. B'') equals G_0'' (resp. G_1'') up to a random permutation of the columns.

The following is a possible outcome of this random experiment:

$$A' = \begin{bmatrix} 0110 \\ 0110 \end{bmatrix} \quad , \quad B' = \begin{bmatrix} 0101 \\ 1010 \end{bmatrix} \quad , \quad A'' = \begin{bmatrix} 1010 \\ 1010 \\ 1010 \\ 1010 \\ 1010 \\ 1010 \end{bmatrix} \quad , \quad B'' = \begin{bmatrix} 0011 \\ 0110 \\ 1010 \\ 0101 \\ 1001 \\ 1100 \end{bmatrix}$$

Finally, these matrices are composed according to (3) in case of a white pixel, and according to (4) in case of a black pixel. The resulting matrices A, B have 32 columns, and $32 = 2 \cdot \mathrm{lcm}(m', m'')^2$ is the claimed pixel expansion of the composed $(2,2;2,6)$-scheme, indeed. It is easily checked that, for each qualified set S for this access structure (with both participants of the first group $\{1,2\}$ and exactly 2 participants of the second group $\{3,\ldots,8\}$), the subarray $A[S]$ has 4 zero-columns whereas $B[S]$ has only 2, which leads to the relative contrast $(4-2)/32 = 1/16$ in the corresponding picture. This is consistent with the formula $\frac{1}{2}\alpha'\alpha''$ since, as already noted above, $\alpha' = 1/2$ and $\alpha'' = 1/4$.

C The Disjunction of Two Access Structures

The disjunction of two access structures had been considered already in [1], where the following is shown:

Theorem C.1 ([1]) *A (Γ', m')-scheme and a (Γ'', m'')-scheme can be transformed into a $(\Gamma' \vee \Gamma'', \max\{m', m''\})$-scheme.*

We briefly outline the proof. If the (Γ', m')-scheme (resp. the (Γ'', m'')-scheme) is given by $\mathcal{C}_0', \mathcal{C}_1'$ (resp. by $\mathcal{C}_0'', \mathcal{C}_1''$), the desired scheme for the disjunction of Γ' and Γ'' is obtained as follows:

Padding: Apply an obvious padding construction (e.g., adding zero-columns to matrices with fewer than $m = \max\{m', m''\}$ columns) so that $\mathcal{C}_0', \mathcal{C}_1', \mathcal{C}_0'', \mathcal{C}_1''$ become multisets of matrices with m columns, respectively.

Vertical Concatenation: For $b = 0, 1$, let the multiset $\mathcal{C}_b$ consist of all $((n' + n'') \times m)$-matrices with a matrix $C' \in \mathcal{C}_b'$ in the first n' rows and a matrix $C'' \in \mathcal{C}_b''$ in the last n'' rows. The multiplicity of such a matrix is the product of the multiplicity of C' in $\mathcal{C}_b'$ and the multiplicity of C'' in $\mathcal{C}_b''$.

It is easy to see that the resulting multisets $\mathcal{C}_0, \mathcal{C}_1$ represent a scheme with pixel expansion $\max\{m', m''\}$ for the disjunction of Γ' and Γ''. A similar construction leads to the following

Corollary C.2 *A (Γ', m')-scheme achieving relative contrast α' and a (Γ'', m'')-scheme achieving relative contrast α'' can be transformed into a $(\Gamma' \vee \Gamma'', \mathrm{lcm}(m', m''))$-scheme achieving relative contrast $\min\{\alpha', \alpha''\}$. Moreover, this transformation preserves perfect reconstruction of black pixels.*

Proof: Let $m = \mathrm{lcm}(m', m'')$. In the transformation described above, we replace "Padding" by "Replication" because replication preserves the relative contrast whereas padding does not. Thus (as in the proof of Theorem 3.1), we easily get a (Γ', m)-scheme achieving relative contrast α' and a

(Γ'', m)-scheme achieving relative contrast α''. Then these two schemes are vertically concatenated (as described above). It is easy to see that the result is a $(\Gamma' \vee \Gamma'', m)$-scheme achieving relative contrast $\min\{\alpha', \alpha''\}$. Recall that a scheme perfectly reconstructs black pixels iff, for every qualified set X and every $B \in \mathcal{C}_1$, the submatrix $B[X]$ does not contain any zero-column. Since replication and vertical concatenation preserve the matrix-property of not containing any zero-column, the described transformation preserves perfect reconstruction of black pixels. •

The following result shows that the transformation from Corollary C.2 is contrast-optimal:

Theorem C.3 *Let Γ' (resp. Γ'') be an access structure with maximum relative contrast α'_{max} (resp. α''_{max}). Then, the maximum relative contrast α_{max} of a scheme for $\Gamma' \vee \Gamma''$ equals $\min\{\alpha'_{max}, \alpha''_{max}\}$.*

Proof: $\alpha_{max} \geq \min\{\alpha'_{max}, \alpha''_{max}\}$ follows from Corollary C.2. The reverse direction is obvious because a scheme for $\Gamma' \vee \Gamma''$ restricted to the participants for Γ' (resp. Γ'') is a scheme for Γ' (resp. Γ'') that achieves relative contrast α_{max} (where the restriction of a scheme $\mathcal{C}_0, \mathcal{C}_1$ to a set P of participants is the scheme $\mathcal{C}_0[P], \mathcal{C}_1[P]$ with $\mathcal{C}_b[P] = \{C[P] : C \in \mathcal{C}_b\}$). •

D Proof of Theorem 4.1

The proof is based on symmetrization, a technique that we describe first. Let $n = n_1 + n_2$. A matrix $A \in \{0,1\}^{n \times m}$ is called (n_1, n_2)-*symmetric* if the following holds for every $0 \leq j_1 \leq n_1$ and every $0 \leq j_2 \leq n_2$: every vector $\begin{bmatrix} v \\ w \end{bmatrix}$ such that $H(v) = j_1$ and $H(w) = j_2$ occurs with the same absolute frequency, say $f_{j_1,j_2}(A)$, as column in A. Thus, up to column permutations, such a matrix is completely characterized by the values $f_{j_1,j_2}(A)$. Obviously, the following relation holds:

$$\sum_{j_1=0}^{n_1} \sum_{j_2=0}^{n_2} \binom{n_1}{j_1} \binom{n_2}{j_2} f_{j_1,j_2}(A) = m \tag{23}$$

Fix subsets $P_1 \subseteq [n_1]$, $P_2 \subseteq [n_1 + 1 : n_1 + n_2]$. Let $p_1 = |P_1|$ and $p_2 = |P_2|$. For every $0 \leq l_1 \leq p_1$ and every $0 \leq l_2 \leq p_2$, let $c^{p_1,p_2}_{l_1,l_2}(A)$ be the number of columns $\begin{bmatrix} v \\ w \end{bmatrix}$ in $\begin{bmatrix} A_{P_1} \\ A_{P_2} \end{bmatrix}$ such that $H(v) = l_1$ and $H(w) = l_2$. It is easy to see that

$$c^{p_1,p_2}_{l_1,l_2}(A) = \binom{p_1}{l_1} \binom{p_2}{l_2} \sum_{j_1=l_1}^{n_1-p_1+l_1} \sum_{j_2=l_2}^{n_2-p_2+l_2} \binom{n_1 - p_1}{j_1 - l_1} \binom{n_2 - p_2}{j_2 - l_2} f_{j_1,j_2}(A) \ . \tag{24}$$

In particular, $c_{l_1,l_2}^{p_1,p_2}(A)$ depends on the sizes p_1, p_2 of the sets P_1, P_2, respectively, but not on the specific choice of these sets (which, in retrospect, justifies our notation with p_1, p_2 as upper indices instead of P_1, P_2). A $(k_1, n_1; k_2, n_2)$-scheme is called *symmetric* if it has (n_1, n_2)-symmetric generator matrices.

Lemma D.1 *Every $(k_1, n_1; k_2, n_2)$-scheme can be made symmetric without changing its relative contrast.*

Proof: For every $M \in \{0,1\}^{s\times t}$ and every permutation σ of $[s]$, let $\sigma(M)$ denote the matrix obtained from M by permuting its rows according to σ. Let $A = \left[\begin{array}{c} A_1 \\ A_2 \end{array}\right] \in \{0,1\}^{n\times m}$ and, for $b = 1, 2$, let $\sigma_b^{(1)}, \ldots, \sigma_b^{(n_b!)}$ be a fixed list containing all permutations of $[n_b]$. Then, the $(n \times n_1!n_2!m)$-matrix $\mathrm{symm}(A)$ given by

$$\left[\begin{array}{c|c|c|c|c|c|c} \sigma_1^{(1)}(A_1) & \multirow{2}{*}{$\ldots$} & \sigma_1^{(1)}(A_1) & \cdots & \sigma_1^{(n_1!)}(A_1) & \multirow{2}{*}{$\ldots$} & \sigma_1^{(n_1!)}(A_1) \\ \sigma_2^{(1)}(A_2) & & \sigma_2^{(n_2!)}(A_2) & \cdots & \sigma_2^{(1)}(A_2) & & \sigma_2^{(n_2!)}(A_2) \end{array}\right]$$

is obviously (n_1, n_2)-symmetric. Now, the lemma is proved as follows. Fix a $(k_1, n_1; k_2, n_2)$-scheme, say with pixel expansion m, given by multisets $\mathcal{C}_0, \mathcal{C}_1$. According to an observation in [1], we may assume that $\mathcal{C}_0$ and $\mathcal{C}_1$ contain the same number r of matrices (counted with multiplicities). For $b = 0, 1$, let $G_b \in \{0,1\}^{n\times rm}$ be the matrix obtained by writing all r matrices in $\mathcal{C}_b$ side by side. It is easy to verify that the $(k_1, n_1; k_2, n_2)$-scheme generated by $\mathrm{symm}(G_0), \mathrm{symm}(G_1)$, is symmetric and achieves the same relative contrast as the original scheme. •

We now come back to the proof of Theorem 4.1. In order to show that the optimal value of α in (5) is lower-bounded by $\alpha(k_1, n_1; k_2, n_2)$, we proceed as follows. Fix a $(k_1, n_1; k_2, n_2)$-scheme that achieves the maximum relative contrast $\alpha(k_1, n_1; k_2, n_2)$. According to Lemma D.1, we may assume that this scheme has (n_1, n_2)-symmetric generator matrices $G_0, G_1 \in \{0,1\}^{n\times m}$. Then the security condition can be written as follows:

$$c_{l_1,l_2}^{k_1-1,n_2}(G_0) = c_{l_1,l_2}^{k_1-1,n_2}(G_1) \quad \text{and} \quad c_{l_1,l_2}^{n_1,k_2-1}(G_0) = c_{l_1,l_2}^{n_1,k_2-1}(G_1) \tag{25}$$

In the first equation, l_1 ranges from 0 to $k_1 - 1$ and l_2 ranges from 0 to n_2. In the second equation, l_1 ranges from 0 to n_1 and l_2 ranges from 0 to $k_2 - 1$. It is furthermore easy to see that

$$\alpha(k_1, n_1; k_2, n_2) = \frac{1}{m}\left(c_{0,0}^{k_1,k_2}(G_0) - c_{0,0}^{k_1,k_2}(G_1)\right) \stackrel{(24)}{=}$$

$$\frac{1}{m}\sum_{j_1=0}^{n_1-k_1}\sum_{j_2=0}^{n_2-k_2}\binom{n_1-k_1}{j_1}\binom{n_2-k_2}{j_2}\left(f_{j_1,j_2}(G_0) - f_{j_1,j_2}(G_1)\right) \ . \tag{26}$$

Consider the following setting of the parameters x, y:

$$x_{j_1,j_2} = \frac{1}{m}\binom{n_1}{j_1}\binom{n_2}{j_2} f_{j_1,j_2}(G_0) \quad , \quad y_{j_1,j_2} = \frac{1}{m}\binom{n_1}{j_1}\binom{n_2}{j_2} f_{j_1,j_2}(G_1) \qquad (27)$$

The components of x and y are obviously non-negative, and an application of (23) shows that they sum-up to 1, respectively. Thus, x, y satisfy (2-LP1). An application of (24) and (25) shows that they satisfy (2-LP2) too. Last, an application of (26) shows that α in (5) evaluates to $\alpha(k_1, n_1; k_2, n_2)$.
In order to show that $\alpha(k_1, n_1; k_2, n_2)$ is lower-bounded by the optimal value of α in (5), we can argue as follows. Consider a basic feasible solution x_{j_1,j_2}, y_{j_1,j_2}. Note that x_{j_1,j_2} and y_{j_1,j_2} are non-negative rational numbers. It follows that there exists a choice for m such that the following holds: $f_{j_1,j_2}(G_0)$ and $f_{j_1,j_2}(G_1)$ chosen according to (27) are non-negative integers. We can therefore design $(k_1, n_1; k_2, n_2)$-symmetric generator matrices G_0 and G_1 whose characteristic values actually are $f_{j_1,j_2}(G_0)$ and $f_{j_1,j_2}(G_1)$, respectively. The generated symmetric $(k_1, n_1; k_2, n_2)$-scheme achieves a relative contrast equal to the value α of the feasible solution we started with.

E Proof of Claim 2

Obviously, x, y satisfy condition (2-LP1). The following calculation, focusing on a fixed row (l_1, l_2) of A_1, verifies the condition $A_1(x - y) = 0$:

$$\begin{aligned}
(A_1(x-y))_{l_1,l_2} \quad &= \quad \sum_{j_2=0}^{n_2}\sum_{j_1=0}^{n_1} A_1[(l_1,l_2),(j_1,j_2)](x_{j_1,j_2} - y_{j_1,j_2}) \\
&\overset{(7),(10)}{=} \quad \frac{1}{2}\cdot(x^{(2)}_{l_2} - y^{(2)}_{l_2})\cdot \sum_{j_1=0}^{n_1} Q_{l_1}(j_1)\cdot(x^{(1)}_{j_1} - y^{(1)}_{j_1}) \\
&\overset{(1-BAP2)}{=} \quad \frac{1}{2}\cdot(x^{(2)}_{l_2} - y^{(2)}_{l_2})\cdot(A'_1(x^{(1)} - y^{(1)}))_{l_1} = 0
\end{aligned}$$

Condition $A_2(x - y) = 0$ can be verified analogously. The proof is now completed by the following calculation:

$$\begin{aligned}
2\cdot\langle c, x-y\rangle \quad &= \quad 2\cdot\left(\sum_{j_1=0}^{n_1}\sum_{j_2=0}^{n_2} c_{j_1,j_2}(x_{j_1,j_2} - y_{j_1,j_2})\right) \\
&\overset{(6),(10)}{=} \quad \prod_{b=1,2}\left(\sum_{j_b=0}^{n_b} P_b(j_b)\cdot(x^{(b)}_{j_b} - y^{(b)}_{j_b})\right) \\
&\overset{(1-BAP1)}{=} \quad \left\langle c^{(1)}, x^{(1)} - y^{(1)}\right\rangle \cdot \left\langle c^{(2)}, x^{(2)} - y^{(2)}\right\rangle
\end{aligned}$$

Since $x^{(b)}, y^{(b)}$ was chosen as an optimal solution for $\mathrm{LP}_{c^{(b)},A'_b}(k_b, n_b)$, the latter expression coincides with $\alpha_{c^{(1)},A'_1}(k_1, n_1)\cdot\alpha_{c^{(2)},A'_2}(k_2, n_2)$.

F Composition of Several Access Structures

Let $\Gamma_1 = (\mathcal{Q}_1, \mathcal{F}_1), \ldots, \Gamma_s = (\mathcal{Q}_s, \mathcal{F}_s)$ be access structures with pairwise disjoint sets of participants. The access structure $\Gamma_1 \wedge \cdots \wedge \Gamma_s = (\mathcal{Q}, \mathcal{F})$, called the *conjunction* (resp. *disjunction*) of $\Gamma_1, \ldots, \Gamma_s$, is given by $\mathcal{Q} = \{X_1 \cup \cdots \cup X_s : X_1 \in \mathcal{Q}_1 \wedge \cdots \wedge X_s \in \mathcal{Q}_s\}$ and $\mathcal{F} = \{X_1 \cup \cdots \cup X_s : X_1 \in \mathcal{F}_1 \vee \cdots \vee X_s \in \mathcal{F}_s\}$ (resp. given by $\mathcal{Q} = \{X_1 \cup \cdots \cup X_s : X_1 \in \mathcal{Q}_1 \vee \cdots \vee X_s \in \mathcal{Q}_s\}$ and $\mathcal{F} = \{X_1 \cup \cdots \cup X_s : X_1 \in \mathcal{F}_1 \wedge \cdots \wedge X_s \in \mathcal{F}_s\}$). By iterative application of Theorem 3.1, we immediately obtain the

Corollary F.1 *One can transform (Γ_i, m_i)-schemes achieving relative contrast α_i, where $i = 1, \ldots, s$, into a scheme for $\Gamma_1 \wedge \cdots \wedge \Gamma_s$ that achieves relative contrast $2^{-(s-1)}\alpha_1 \cdots \alpha_s$. Moreover this transformation preserves perfect reconstruction of black pixels.*

Similarly, we obtain by iterative application of Corollary C.2 and Theorem C.3 the

Corollary F.2 *One can transform (Γ_i, m_i)-schemes achieving relative contrast α_i, where $i = 1, \ldots, s$, into a scheme for $\Gamma_1 \vee \cdots \vee \Gamma_s$ that achieves relative contrast $\min\{\alpha_1 \cdots \alpha_s\}$. Moreover this transformation is contrast-optimal and preserves perfect reconstruction of black pixels.*

The conjunction of (k_i, n_i)-schemes, $i = 1, \ldots, s$, yields a $(k_1, n_1; \ldots; k_s, n_s)$-scheme (with the obvious definition of the latter). The maximum relative contrast achievable for such a scheme can again be cast as the objective function of a linear program. The approximation problem resulting from dualization then reads as follows:
Given polynomials $P_1 \in \mathcal{P}_{k_1}, \ldots, P_s \in \mathcal{P}_{k_s}$, find polynomials $Q^{[1]}_{j_2,\ldots,j_s} \in \mathcal{P}_{k_1-1}, \ldots, Q^{[s]}_{j_1,\ldots,j_{s-1}} \in \mathcal{P}_{k_s-1}$ such that the error-term

$$\max_{j_1=0,\ldots,n_1;\ldots;j_s=0,\ldots,n_s} \left| P_1(j_1) \cdots P_s(j_s) - \left(Q^{[1]}_{j_2,\ldots,j_s}(j_1) + \cdots + Q^{[s]}_{j_1,\ldots,j_{s-1}}(j_s) \right) \right| \tag{28}$$

is minimized. The smallest possible error is denoted $\beta_{P_1,\ldots,P_s}(k_1, n_1; \ldots; k_s, n_s)$. The counterpart to Theorem 4.6 reads as follows:

Theorem F.3 *The following equalities are valid:*

$$\begin{aligned}
\beta_{P_1,\ldots,P_s}(k_1, n_1; \ldots; k_s, n_s) &= \beta_{P_1}(k_1, n_1) \cdots \beta_{P_s}(k_s, n_s) \\
\alpha_{c,A}(k_1, n_1; \ldots; k_s, n_s) &= 2^{-(s-1)} \cdot \alpha_{c^{(1)},A'_1}(k_1, n_1) \cdots \alpha_{c^{(s)},A'_s}(k_s, n_s) \\
\alpha(k_1, n_1; \ldots; k_s, n_s) &= 2^{-(s-1)} \cdot \alpha(k_1, n_1) \cdots \alpha(k_s, n_s)
\end{aligned}$$