ELSEVIER

Information Processing Letters 75 (2000) 255–259

Information Processing Letters

www.elsevier.com/locate/ipl

Visual cryptography for grey level images

Carlo Blundo [a,*], Alfredo De Santis [a], Moni Naor [b]

[a] *Dipartimento di Informatica ed Applicazioni, Università di Salerno, 84081 Baronissi (SA), Italy*

[b] *Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel*

Received 29 September 1999; received in revised form 23 May 2000

Communicated by A. Tarlecki

Abstract

Visual cryptography is a cryptographic paradigm introduced by Naor and Shamir [Lecture Notes in Comput. Sci., Vol. 950, Springer, Berlin, 1995, p. 1]. Some predefined set of participants can decode a secret message (a black and white image) without any knowledge of cryptography and without performing any cryptographic computation: Their visual system will decode the message.

In this paper we define and analyze visual cryptography schemes for grey level images whose pixels have g grey levels ranging from 0 (representing a white pixel) to $g-1$ (representing a black pixel). Moreover, we give a necessary and sufficient condition for such schemes to exist.

Keywords: Cryptography; Visual cryptography; Data security

1. Introduction

A visual cryptography scheme for a set $\mathcal{P}$ of n participants is a method to encode a secret image SI into n shadow images called shares, where each participant in $\mathcal{P}$ receives one share. Certain qualified subsets of participants can "visually" recover the secret image, but other, forbidden, sets of participants have no information (in an information-theoretic sense) on SI. A "visual" recovery for a set $X \subseteq \mathcal{P}$ consists of xeroxing the shares given to the participants in X onto transparencies, and then stacking them. The participants in a qualified set X will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation. Visual cryptography schemes are characterized by two parameters: The *pixel expansion*, which is the number of subpixels each pixel of the original image is encoded into, and the *relative difference* which measures the "difference" between a black and a white pixel in the reconstructed image.

This cryptographic paradigm has been introduced by Naor and Shamir [10]. They analyzed the case of a k out of n threshold visual cryptography scheme, in which the secret image is visible if and only if any k transparencies are stacked together. The model by Naor and Shamir has been extended in [1,3] to general access structures (an access structure is a specification of all qualified and forbidden subsets of participants), where general techniques to construct visual cryptography schemes for any access structure have been proposed. Although visual cryptography has been introduced only recently, is has received

* Corresponding author.

E-mail addresses: carblu@dia.unisa.it (C. Blundo), ads@dia.unisa.it (A. De Santis), moni@weizmann.ac.il (M. Naor).

0020-0190/00/$ – see front matter
PII: S0020-0190(00)00108-3

considerable attention by several researchers (see, for instance, [1–3,5,7,8,12]).

Alternative reconstruction methods for visual cryptography schemes based on "opaque" shares [11] and on polarized filters [4] have been recently proposed. Both models make assumptions different from ours on the way the shares combine. Authentication and identification methods for human users based on visual cryptography have been considered [9]. Recently, the randomness needed in visual cryptography schemes has been analyzed in [6].

A natural extension for visual cryptography, suggested in [10], is to consider images whose pixels have g grey levels ranging from 0 (representing a white pixel) to $g-1$ (representing a black pixel).

In this paper we define and analyze visual cryptography schemes for grey levels images. We provide a general technique to realize, for any access structure, visual cryptography schemes encoding grey level images. Moreover, we give a necessary and sufficient condition for such schemes to exist.

2. The model

Let $\mathcal{P} = \{1, \ldots, n\}$ be a set of elements called *participants*, and let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. Let $\Gamma_{\text{Qual}} \subseteq 2^{\mathcal{P}}$ and $\Gamma_{\text{Forb}} \subseteq 2^{\mathcal{P}}$, where $\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset$. We refer to members of Γ_{Qual} as *qualified sets* and we call members of Γ_{Forb} *forbidden sets*. The pair $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is called the *access structure* of the scheme.

We assume that the secret image consists of a collection of pixels, where to each pixel is associated a grey level ranging from white to black and each pixel is handled separately. Each pixel appears in n versions called *shares*, one for each transparency. Each share is a collection of m black and white subpixels. (The value m is referred to as the *pixel expansion* of the scheme.) The resulting structure of the shares can be described by an $n \times m$ Boolean matrix $S = [s_{ij}]$ where $s_{ij} = 1$ iff the jth subpixel in the ith transparency is black. Therefore the grey level of the combined share, obtained by stacking the transparencies $i_1, \ldots, i_s$, is proportional to the Hamming weight $w(V)$ of the m-vector $V = OR(r_{i_1}, \ldots, r_{i_s})$, where $r_{i_1}, \ldots, r_{i_s}$ are the rows of S associated with the transparencies we stack. This grey level is interpreted by the visual system of the participants as black, as grey, or as white according to some rule of contrast.

Definition 2.1. Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure on a set of n participants and let $g \geqslant 2$ be an integer. The g collections (multisets) of $n \times m$ Boolean matrices $\mathcal{C}_0, \ldots, \mathcal{C}_{g-1}$ constitute a *visual cryptography scheme for g grey levels with pixel expansion m for* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ ($(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m, g)$-GVCS, for short), if there exist values $\alpha_0, \ldots, \alpha_{g-2}$ and sets $\{(X, t_{i,X})\}_{X \in \Gamma_{\text{Qual}}}$, for $i = 0, \ldots, g-2$, satisfying:

(1) *Any* (*qualified*) *set* $X = \{j_1, j_2, \ldots, j_p\} \in \Gamma_{\text{Qual}}$ *can recover the shared image by stacking their transparencies*.
Formally, for $i = 0, \ldots, g-2$ for any $M \in \mathcal{C}_i$, the "or" V of rows $j_1, j_2, \ldots, j_p$ satisfies $w(V) \leqslant t_{i,X} - \alpha_i \cdot m$; whereas, for any $M \in \mathcal{C}_{i+1}$ it results that $w(V) \geqslant t_{i,X}$.

(2) *Any* (*forbidden*) *set* $X = \{j_1, j_2, \ldots, j_p\} \in \Gamma_{\text{Forb}}$ *has no information on the shared image*.
Formally, the g collections of $p \times m$ matrices $\mathcal{D}_i$, with $i = 0, \ldots, g-1$, obtained by restricting each $n \times m$ matrix in $\mathcal{C}_i$ to rows $j_1, j_2, \ldots, j_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Notice that when $g = 2$ we are encoding black and white images. We will refer to such a scheme as a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$-VCS or, equivalently, as a visual cryptography scheme for the access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ (see, for instance, [1,3,10]).

Each pixel of the original image will be encoded into n pixels, each of which consists of m subpixels. To share a pixel having grey level ℓ, the dealer randomly chooses one of the matrices in $\mathcal{C}_\ell$, and distributes row i to participant i. Thus, the chosen matrix defines the m subpixels in each of the n transparencies.

The first property is related to the contrast of the image. It states that when any set of qualified participants stack their transparencies they can correctly recover the image shared by the dealer. The value α_i, for $i = 0, \ldots, g-2$, is referred to as the *relative difference* between the ith and the $(i+1)$th grey levels. The set $\{(X, t_X)\}_{X \in \Gamma_{\text{Qual}}}$ is called the *set of thresholds*. For $i = 0, \ldots, g-2$, we assume that α_i takes values on the rational numbers. The number $\alpha_i \cdot m$ is referred to as the *contrast* of the image. As we want the contrast to be as large as possible, we have that $\alpha_i \cdot m \geqslant 1$.

The second property is related to the *security* of the scheme, since it implies that, even by inspecting all their shares, any set of forbidden participants cannot gain any information on the value of the grey level of the shared pixel.

A convenient class of visual cryptography schemes for images having g grey levels is realized using $n \times m$ matrices, $G^0, \ldots, G^{g-1}$, referred to as *basis matrices* satisfying the following definition.

Definition 2.2. Let $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$ be an access structure on a set of n participants and let $g \geqslant 2$ be an integer. A $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}, m, g)$-GVCS with relative differences $\alpha_0, \ldots, \alpha_{g-2}$ and sets of thresholds $\{(t_{i,X}, X)\}_{X \in \Gamma_{\mathrm{Qual}}}$, for $i = 0, \ldots, g-2$, is realized using the $n \times m$ *basis matrices* $G^0, \ldots, G^{g-1}$ if the following two conditions hold.

(1) If $X = \{j_1, j_2, \ldots, j_p\} \in \Gamma_{\mathrm{Qual}}$ (i.e., if X is a qualified set), then, for $i = 0, \ldots, g-2$, the "or" V of rows $j_1, j_2, \ldots, j_p$ of G^i satisfies $w(V) \leqslant t_{i,X} - \alpha_i \cdot m$; whereas, for G^{i+1} it results that $w(V) \geqslant t_{i,X}$.

(2) If $X = \{j_1, j_2, \ldots, j_p\} \in \Gamma_{\mathrm{Forb}}$ (i.e., if X is a forbidden set), then the g $p \times m$ matrices obtained by restricting $G^0, \ldots, G^{g-1}$ to rows $j_1, j_2, \ldots, j_p$ are equal up to a column permutation.

The collections $\mathcal{C}_0, \ldots, \mathcal{C}_{g-1}$ are obtained by permuting the columns of the corresponding basis matrix (G^i for $\mathcal{C}_i$, with $i = 0, \ldots, g-1$) in all possible ways. Note that, in this case, the size of the collections $\mathcal{C}_i$'s is the same and it is denoted by r. This technique was first introduced in [10]. The algorithm for the VCS based on the previous construction of the collections $\mathcal{C}_i$'s has small memory requirements (it keeps only the basis matrices G^i, with $i = 0, \ldots, g-1$) and it is efficient (to choose a matrix in $\mathcal{C}_i$ it only generates a permutation of the columns of G^i).

3. Schemes for grey level images

In this section we analyze visual cryptography schemes for grey level images by giving a necessary and sufficient condition for such schemes to exist.

In [5] it was shown that if there exists a k out of n threshold VCS Σ, realized using collections of $n \times m$ Boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$, having relative difference α, then there exists a k out of n threshold VCS realized by using basis matrices having the same relative difference as Σ. This result can be extended to $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}, m, g)$-GVCS as shown in the next lemma.

Lemma 3.1. *Let $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$ be an access structure on a set of n participants and let $g \geqslant 2$ be an integer. Let Σ be a $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}, m, g)$-GVCS with relative differences $\alpha_0, \ldots, \alpha_{g-1}$ realized by the collections of matrices $\mathcal{C}_0, \ldots, \mathcal{C}_{g-1}$. Then, there exists a $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}, m, g)$-GVCS realized by using basis matrices having relative differences $\alpha_0, \ldots, \alpha_{g-1}$.*

Proof. Without loss of generality we can assume that $r = |\mathcal{C}_0| = \cdots = |\mathcal{C}_{g-1}|$. (The proof that we can restrict our attention to GVCS for collections having the same cardinality can be obtained, in a straightforward way, from the one for VCS in Section 2.1 of [1].) Suppose that $\mathcal{C}_i = \{M^{i,1}, \ldots, M^{i,r}\}$, with $i = 0, \ldots, g-1$. It is immediate to check that, for $i = 0, \ldots, g-1$, the matrices $G^i = M^{i,1} \circ \cdots \circ M^{i,r}$, where $\circ$ denotes the concatenation of matrices, constitute the basis matrices of a $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}, m, g)$-GVCS having the same relative differences as Σ. □

Let M be a matrix in the collection $\bigcup_{i=0}^{g-1} \mathcal{C}_i$ of a $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}, m, g)$-GVCS on a set of participants $\mathcal{P} = \{1, \ldots, n\}$. For $X \subseteq \mathcal{P}$, let M_X denote the m-vector obtained by considering the *or* of the vectors corresponding to participants in X; whereas $M[X]$ denotes the $|X| \times m$ matrix obtained from M by considering only the rows corresponding to participants in X.

The next theorem provides a necessary and sufficient condition for GVCS to exist.

Theorem 3.2. *Let $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$ be an access structure on a set of n participants and let $g \geqslant 2$ be an integer. Let α^* be the maximum relative difference of a visual cryptography scheme for $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$. There exists a $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}, m, g)$-GVCS with relative differences $\alpha_0, \ldots, \alpha_{g-2}$ if and only if $\sum_{i=0}^{g-2} \alpha_i \leqslant \alpha^*$.*

Proof. Let $\mathcal{C}_0, \ldots, \mathcal{C}_{g-1}$ be the collections of Boolean matrices of a $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}, m, g)$-GVCS with relative differences $\alpha_0, \ldots, \alpha_{g-1}$. It is easy to see that $\mathcal{C}_0$ and $\mathcal{C}_{g-1}$ constitute a $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}}, m)$-VCS. The relative

difference of such a scheme is equal to $\sum_{i=0}^{g-2}\alpha_i$. Hence, we have that

$$\sum_{i=0}^{g-2}\alpha_i \leqslant \alpha^*.$$

Now, suppose that $\sum_{i=0}^{g-2}\alpha_i \leqslant \alpha^*$. We will show that there exists a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m, g)$-GVCS with relative differences $\alpha_0, \ldots, \alpha_{g-2}$. Let S^0 and S^1 be the basis matrices of a visual cryptography scheme for $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ with optimal relative difference α^* and let $\overline{m}$ be its pixel expansion (by Lemma 3.1 such a scheme always exists). Suppose that $\alpha_i = a_i/b_i$, for $i = 0, \ldots, g-2$, and that $\alpha^* = a/b$, where a, b, a_i, and b_i are positive integers. Let

$$m = \operatorname{lcm}\{b_0, \ldots, b_{g-2}\} \cdot a \cdot \overline{m}.$$

For $i = 0, \ldots, g-2$, define $r_i = (a_i \cdot b \cdot m)/(b_i \cdot a \cdot \overline{m})$. Let

$$d = m - \sum_{i=0}^{g-2} r_i \cdot \overline{m}.$$

Since $\sum_{i=0}^{g-2}\alpha_i \leqslant \alpha^*$, then $d \geqslant 0$. Finally, let D be a $n \times d$ matrix whose entries are all equal to 0. For $i = 0, \ldots, g-1$, the following $n \times m$ matrices G^i define a $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m, g)$-GVCS.

$$G^i = \underbrace{S^0 \circ \cdots \circ S^0}_{\sum_{j=i}^{g-2} r_j} \circ \underbrace{S^1 \circ \cdots \circ S^1}_{\sum_{j=0}^{i-1} r_j} \circ D.$$

(Notice that the matrix S^1 does not appear in G^0; whereas, the matrix S^0 does not appear in G^{g-1}.) Indeed, for any $X \in \Gamma_{\text{Qual}}$ and for $i = 1, \ldots, g-1$, we have that

$$\begin{aligned}
&\frac{w(G^i_X) - w(G^{i-1}_X)}{m} \\
&\quad = \frac{r_{i-1}[w(S^1_X) - w(S^0_X)]}{m} \\
&\quad = \frac{1}{m} \cdot \frac{a_{i-1} \cdot b \cdot m}{b_{i-1} \cdot a \cdot \overline{m}}\big[w(S^1_X) - w(S^0_X)\big] \\
&\quad = \alpha_{i-1}\frac{w(S^1_X) - w(S^0_X)}{\alpha^* \cdot \overline{m}} \\
&\quad \geqslant \alpha_{i-1}.
\end{aligned}$$

Therefore, setting $t_{i-1,X} = w(G^i_X)$ we get that property (1) of Definition 2.1 is satisfied. It is immediate to check that for any $X \in \Gamma_{\text{Forb}}$ it results that the g matrices obtained by restricting $G^0, \ldots, G^{g-1}$ to the rows indexed by X are equal up to a column permutation. Thus, the theorem holds. □

Notice that when all the α_i are equal, then the scheme proposed in this paper reduces to the one proposed by Naor and Shamir [10] for k out of n visual cryptography schemes. A k out of n visual cryptography scheme is a scheme where

$$\Gamma_{\text{Qual}} = \big\{X \subseteq \{1, \ldots, n\}\colon |X| = k\big\}$$

and

$$\Gamma_{\text{Forb}} = \big\{X \subseteq \{1, \ldots, n\}\colon |X| < k\big\}.$$

For any integers k, n, and g such that $1 \leqslant k \leqslant n$ and $g \geqslant 2$, we denote with (k, n, m, g)-GVCS a k out of n visual cryptography scheme for g grey level images.

Here is a small example to illustrate the construction of $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m, g)$-GVCS given in Theorem 3.2.

Example 3.3. The following basis matrices define a two out of two visual cryptography scheme for 4 grey levels. In such a scheme we have that $\alpha_0 = \alpha_1 = \alpha_2 = 1/6$.

$$G^0 = \begin{bmatrix} 111000 \\ 111000 \end{bmatrix}, \qquad G^1 = \begin{bmatrix} 111000 \\ 011100 \end{bmatrix},$$

$$G^2 = \begin{bmatrix} 111000 \\ 001110 \end{bmatrix}, \qquad G^3 = \begin{bmatrix} 111000 \\ 000111 \end{bmatrix}.$$

The next corollary is an immediate consequence of Theorem 3.2.

Corollary 3.4. *In any (k, k, m, g)-GVCS, with relative differences $\alpha_0, \ldots, \alpha_{g-2}$, it holds that*

$$\min\{\alpha_0, \ldots, \alpha_{g-2}\} \leqslant \frac{1}{(g-1)2^{k-1}}$$

and

$$m \geqslant (g-1)2^{k-1}.$$

Proof. It is known (see [10]) that in any k out k threshold visual cryptography scheme the relative difference is upper bounded by $1/2^{k-1}$. From Theorem 3.2 we have that

$$\sum_{i=0}^{g-2}\alpha_{(i)} \leqslant \frac{1}{2^{k-1}}.$$

Let $\alpha = \min\{\alpha_0, \ldots, \alpha_{g-2}\}$. Since

$$\alpha(g-1) \leqslant \sum_{i=0}^{g-2} \alpha_i,$$

we get that

$$\alpha \leqslant \frac{1}{(g-1)2^{k-1}}.$$

Since the contrast is at least one, i.e., $\alpha \cdot m \geqslant 1$, it results that $m \geqslant (g-1)2^{k-1}$. □

It is easy to see that for any $g \geqslant 2$ and any $k \geqslant 2$ there exists a (k, k, m, g)-GVCS meeting both bounds of the previous corollary. Such a scheme is constructed by applying the construction provided by Theorem 3.2 using the basis matrices of the k out of k threshold visual cryptography scheme given in [10]. (The construction of a k out of k threshold provided in [10] is the following: S^0 is the matrix whose columns are all the Boolean k-vectors having an even number of '1's, and S^1 is the matrix whose columns are all the Boolean k-vectors having an odd number of '1's.)

The following scheme, to encode grey level images whose pixels have grey levels ranging from 0 to 255, can be obtained from the one proposed by Naor and Shamir [10] by arranging in a different way the subpixels of a pixel. The scheme is as follows: An original pixel with grey level ℓ is divided into a 15×17 array (referred to as *grey level table*) of ℓ black and $255 - \ell$ white subpixels. Then, each black and white subpixel is encoded separately by using a simple black and white visual cryptography scheme (for instance, we can use the scheme of [1,5,7,8,10, 12]). The resulting scheme has a pixel expansion equal to $255 \cdot m$ and relative differences $\alpha_0 = \cdots = \alpha_{254} = \alpha/255$ (where m and α are the pixel expansion and the relative difference, respectively, of the scheme we use to encode the pixels of the grey level table). In the case of (k, k, m, g)-GVCS, the pixel expansion and the relative differences we achieve in the above scheme are optimal because of Corollary 3.4.

4. Conclusion and open problems

In this paper we have defined and analyzed visual cryptography schemes for grey level images. We gave a necessary and sufficient condition for such schemes to exist. We proved the optimality of (k, k, m, g)-GVCS.

An interesting open problem which deserves further investigation is the encoding of grey level images for different models of VCS such as [11] and [4].

Acknowledgement

We would like to thank an anonymous referee for his/her useful comments.

References

[1] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform. and Comput. 129 (2) (1996) 86–106.

[2] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Extended schemes for visual cryptography, Theoret. Comput. Sci. 250 (2000) 143–161. Available on-line at http://www.dia.unisa.it /VISUAL/papers.html.

[3] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Constructions and bounds for visual cryptography, in: Proc. ICALP'96, Lecture Notes in Comput. Sci., Vol. 1099, Springer, Berlin, 1996, pp. 416–428.

[4] E. Biham, A. Itzkovitz, Visual cryptography with polarization, Talk given by Biham at the "Weizmann Workshop on Cryptography", Weizmann Institute, Rehovot, Israel, June 8–9, 1997.

[5] C. Blundo, A. De Santis, D.R. Stinson, On the contrast in visual cryptography schemes, J. Cryptology 12 (1999) 261–289.

[6] A. De Bonis, A. De Santis, Randomness in visual cryptography, in: Proc. STACS 2000, Lecture Notes in Comput. Sci., Vol. 1770, Springer, Berlin, 2000, pp. 627–638.

[7] S. Droste, New results on visual cryptography, in: Advances in Cryptology—CRYPTO'96, Lecture Notes in Comput. Sci., Vol. 1109, Springer, Berlin, 1996, pp. 401–415.

[8] T. Hofmeister, M. Krause, H.U. Simon, Contrast-optimal k out of n secret sharing schemes in visual cryptography, in: Proc. COCOON'97, Lecture Notes in Comput. Sci., Vol. 1276, Springer, Berlin, 1997, pp. 176–185.

[9] M. Naor, B. Pinkas, Visual authentication and identification, in: Advances in Cryptology—CRYPTO'97, Lecture Notes in Comput. Sci., Vol. 1294, Springer, Berlin, 1997, pp. 322–336.

[10] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology—EUROCRYPT'94, Lecture Notes in Comput. Sci., Vol. 950, Springer, Berlin, 1995, pp. 1–12.

[11] M. Naor, A. Shamir, Visual cryptography, II: Improving the contrast via the cover base, in: Security Protocols, Lecture Notes in Comput. Sci., Vol. 1189, Springer, Berlin, 1997, pp. 197–202.

[12] E.R. Verheul, H.C.A. van Tilborg, Constructions and properties of k out of n visual secret sharing schemes, Designs, Codes, and Cryptography 11 (2) (1997) 179–196.