

General Access Structures in Audio Cryptography

Daniel Socek

Department of Computer Science and Engineering
Florida Atlantic University
Boca Raton, Florida 33431-0991
Email: dsocek@brain.math.fau.edu

Spyros S. Magliveras

Department of Mathematical Sciences
Florida Atlantic University
Boca Raton, Florida 33431-0991
Email: spyros@fau.edu

Abstract

We propose and analyze a new type of cryptographic scheme, which extends principles of secret sharing to Morse code-like audio signals. The proposed “audio cryptography scheme” (ACS) is perfectly secure and easy to implement. It relies on the human auditory system for decoding. “Audio sharing schemes” (ASS) proposed earlier were based on disguising secret binary message with a cover sound. Moreover, only 2-out-of- n audio sharing schemes have ever been proposed. Our scheme correlates strongly, and is analogous to schemes in well-studied visual cryptography. Consequently, we were able to use the existing visual cryptography constructions and obtain not only k -out-of- n audio sharing schemes, but also the most general audio cryptography schemes for qualified subsets. In audio cryptography scheme for qualified subsets, a subset of participants can recover the secret audio signal only if some qualified subset of participants is its subset.

1. Introduction

Cryptographic schemes that do not rely on computers or other hardware to perform encryption or decryption represent an important area of study [6]. *Visual cryptography* studies cryptographic schemes that rely on the human visual system to reveal secret messages. Similarly, *audio cryptography* relies on the human auditory system to decrypt messages. For people with visual disabilities this is obviously a preferred scheme. Some *audio secret sharing* (ASS) schemes have been proposed recently. However, these are based on audio shares which use “cover sound” to disguise a secret binary message [6, 7]. Moreover, only up to 2-out-of- n such audio sharing schemes have ever been proposed, and the general k -out-of- n audio sharing schemes were still an open research problem. In 1998, Desmedt, Hou and Quisquater [6] proposed an audio secret sharing scheme that uses a “cover sound” (harmonic sound or high-quality

music) to embed a secret binary message. This scheme was further improved in 2003 by Lin, Lai and Yang [7] who proposed two methods based on *time division*. The method used a single cover sound for a 2-out-of- n ASS scheme, as opposed to the original scheme requiring $\lceil \log_2 n \rceil$ cover sounds. The ASS schemes from [6] and [7] are all based on the idea of sound interference. The effect of this is that when enough shares are played simultaneously the human auditory system can detect changes in the sound volume. Destructive interference results in low volume, while constructive interference results in high volume. The changes in the sound volume reveal the secret binary message, in the sense that the high volume segment corresponds to 1 and the low volume segment corresponds to 0. Our scheme is based on a different principle. Instead of using sound interference, we focus on using two types of flat frequencies (beeps): the short beep and the long beep. This kind of sound is similar to a Morse code signal.

An *audio cryptography scheme*, ACS for short, for a set \mathcal{P} of n participants can be defined as a method for encoding a secret audio signal \mathcal{S} into n audio signals (*shares*) so that each participant from \mathcal{P} receives exactly one unique share, and only certain qualified subsets of \mathcal{P} can recover \mathcal{S} by simultaneously playing their shares. A k -out-of- n audio cryptography scheme, denoted by (k, n) -ACS, where $2 \leq k \leq n$, is an audio cryptography scheme in which the qualified subsets are all subsets of cardinality at least k . In other words, simultaneously playing any k shares reveals the secret audio signal \mathcal{S} , while simultaneously playing fewer than k shares gives no information about \mathcal{S} .

A truly innovative type of secret sharing, *visual cryptography*, was introduced by Naor and Shamir at the EUROCRYPT '94 [1]. Naor and Shamir considered the general k -out-of- n visual cryptography schemes, denoted by (k, n) -VCS, and gave optimal constructions for $(2, n)$ -VCS and (n, n) -VCS. However, their constructions for cases when $2 < k < n$ were quite inefficient. These inefficient constructions were improved in [2] and [3]. In addition, the constructions of visual schemes for *qualified* subsets of $[1, n]$

were proposed by Ateniese, Blundo, De Santis and Stinson [3]. In this paper we were able to achieve a much closer analogy between audio and visual cryptography by using Morse code-like audio messages. We present not only the k -out-of- n audio cryptography schemes, but also the most general audio cryptography schemes for qualified subsets.

2. The Basic Model

In any Morse code audio message, there are two types of sounds: the short beep and the long beep. When making an analogy between audio and visual cryptography, the short beep corresponds to a white pixel, whereas the long beep corresponds to a black pixel. Mathematically, we represent the short beep by 0 and the long beep by 1. We also make use of the visually logical representation of beeps where “-” (the dash) denotes a long beep, and “.” (the dot) denotes a short beep. Unfortunately, Morse code is not a prefix code, and pauses are needed to distinguish between symbols. Since we want to minimize the amount of information needed for encoding, Morse coded audio messages are consequently not suitable for our scheme. Instead, we would probably use a prefix code, possibly a Huffman encoding scheme based on the probability distribution of the symbols. Thus, an audio signal represented in the long-beep short-beep fashion is hereby referred to as *Prefix Binary Code* (PBC) audio signal. One can think of a PBC audio signal as a binary string.

The basic idea of our scheme can be best described by considering a $(2, 2)$ -ACS case. Let us consider a PBC audio message \mathcal{S} which contains exactly m beeps. The dealer creates two audio shares (binary sequences), S_1 and S_2 , consisting of exactly $2m$ beeps.

A beep b from \mathcal{S} is expanded into two beeps in each of the two shares. A short beep b is encoded with the same scheme in both shares, i.e, either $S_1(b) = S_2(b) = \cdot-$ or $S_1(b) = S_2(b) = \cdot\cdot$, depending on a coin flip. This will ensure that the simultaneous playback of the two shares contains a short beep. On the other hand, a long beep b is encoded with opposite schemes in the two shares. That is, either $S_1(b) = \cdot-$ and $S_2(b) = \cdot\cdot$, or $S_1(b) = \cdot\cdot$ and $S_2(b) = \cdot-$, depending on a coin flip. The effect of this is that simultaneously playing the two shares produces two long beeps. Thus, the superposition of a short beep with a second short beep in a particular time frame is perceived as a short beep, while the superposition of two beeps, at least one of which is long, is perceived as a long beep.

Example 2.1 Let the secret message be “..._____”. The dealer tosses a coin 9 times and the result turns out to be THHTHHHTH. Then, the corresponding two shares are:

·- ·- ·- ·- ·- ·- ·- ·- ·- ·-

Beep	Coin Toss	Share S_1	Share S_2	Playing S_1 and S_2
·	H	·-	·-	·-
	T	·-	·-	·-
-	H	·-	·-	——
	T	·-	·-	——

Table 1. Encoding of a beep in $(2, 2)$ -ACS.

·- ·- ·- ·- ·- ·- ·- ·- ·- ·-

When played simultaneously, the two shares produce the following sound:

·- ·- ·- — — — — ·- ·- ·-

Clearly, this reveals the secret plaintext, while observing the two shares individually gives no information about it. Note that the resulting sound corresponds to the bitwise OR of the two binary shares.

The $(2, 2)$ -ACS from above can be represented in a Boolean matrix form. Let \mathcal{C}_0 and \mathcal{C}_1 be the following two collections of matrices:

$$\mathcal{C}_0 = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\},$$

$$\mathcal{C}_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

To share a short beep, the dealer randomly selects one of the matrices in \mathcal{C}_0 , and to share a long beep, the dealer randomly selects one of the matrices in \mathcal{C}_1 . The first row of the chosen matrix is used for share S_1 , and the second for share S_2 . For example, a row $(1\ 0)$ defines the long-short scheme in a share. Throughout this paper \mathcal{C}_0 and \mathcal{C}_1 will denote the collections of matrices used to randomly select a share scheme to expand a short or long beep (respectively) from the original audio signal. Similar collections of matrices are used in visual cryptography to define sharing of white or black pixels [1, 3].

Definition 2.1 A solution to the k -out-of- n audio cryptography scheme consists of two collections of $n \times \ell$ Boolean matrices \mathcal{C}_0 and \mathcal{C}_1 , which define the sharing scheme for a PBC audio signal. The collections \mathcal{C}_0 and \mathcal{C}_1 constitute a (k, n) -ACS if the following two conditions are met:

1. Let $B_0 \in \mathcal{C}_0$ and $B_1 \in \mathcal{C}_1$, and let U be a proper subset of $[1, k]$ with $q = |U|$ (clearly $q < k$). The two matrices obtained by restricting B_0 and B_1 to rows corresponding to the elements of U are equal up to

a column permutation. Consequently, the bitwise OR, x , of any q rows of any matrix from \mathcal{C}_0 , and the bitwise OR, y , of any q rows of any matrix from \mathcal{C}_1 satisfy $H(x) = H(y)$ (where $H(z)$ denotes the Hamming weight of vector z).

2. The bitwise OR, x , of any k rows of any matrix from \mathcal{C}_0 , and the bitwise OR, y , of any k rows of any matrix from \mathcal{C}_1 satisfy $H(x) < H(y)$.

The first condition implies that analyzing encodings of a beep b in any $k - 1$ or fewer shares gives no information whatsoever about b . This ensures the secrecy afforded by the perfect sharing scheme. The second condition is important to distinguish between the long beep and the short beep if k shares are played simultaneously; i.e., it enables the recovery of a secret audio signal to qualified subsets.

Naor and Shamir defined the following three important parameters used to describe the quality of a visual sharing scheme [1]:

- m , the number of subpixels in a share encoding a pixel. This measures the loss of resolution from the original picture to the shared one. The smaller m , the better.
- α , the relative difference in weight between k combined shares arising from a white pixel and a black pixel in the original picture. This measures the loss in contrast. The larger α , the better.
- $r = \max\{|\mathcal{C}_0|, |\mathcal{C}_1|\}$. Although $|\mathcal{C}_0|$ and $|\mathcal{C}_1|$ could be different, one can always extend the smaller \mathcal{C}_i so that $|\mathcal{C}_0| = |\mathcal{C}_1|$ [1]. The value $\log r$ represents the number of random bits needed to encode each pixel. This parameter does not affect the quality of the picture.

We consider a similar, but smaller set of parameters important for the proposed audio cryptography schemes:

- ℓ , the number of beeps in a share. This measures the beep extension from the original audio to the shared one. The smaller ℓ , the better.
- p , the size of collections \mathcal{C}_0 and \mathcal{C}_1 . The value $\log p$ is the number of random bits needed to encode a beep.

Notice that we have dropped the audio equivalent to the α parameter. In the case of the human hearing system, perhaps it is preferred that the share combination representing the long beep contains no short beeps, and the share combination representing the short beep contains at least one short beep. However, in this paper we ignore audio contrast.

3. Constructing a $(2, n)$ -ACS

Let B_0 and B_1 denote the following two $n \times n$ matrices:

$$B_0 = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ \dots & & & & \\ 0 & 1 & 1 & \dots & 1 \end{pmatrix},$$

$$B_1 = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 1 \\ \dots & & & & \\ 1 & 1 & 1 & \dots & 0 \end{pmatrix}.$$

The general problem of constructing a 2 -out-of- n audio cryptography scheme can be solved with the following two $n \times n$ matrix collections:

$$\mathcal{C}_0 = \{\text{all matrices obtained by permuting the columns of } B_0\},$$

$$\mathcal{C}_1 = \{\text{all matrices obtained by permuting the columns of } B_1\}.$$

The dealer expands the beep b into $\ell = n$ beeps in each of the n shares. It is easy to observe that the bitwise OR of any two or more rows of a matrix from \mathcal{C}_0 contains a short beep. On the other hand, the bitwise OR of any two or more rows of a matrix from \mathcal{C}_1 does not contain a short beep. This is the key feature that distinguishes the short beep from the long beep in the decoding process by the human auditory system. Clearly, one share only does not reveal any information whatsoever about the secret audio message. The above construction of $(2, n)$ -ACS is identical to the construction of $(2, n)$ -VCS from [1].

4. Constructing an (n, n) -ACS

Let V_n denote the vector space of dimension n over the binary field, E_n the linear subspace of V_n consisting of all $v \in V_n$ of even weight, and $O_n = V_n - E_n$. Then, of course $O_n = E_n + u$, for any fixed $u \in V_n$ of odd weight. We state without proof the following easy lemma.

Lemma 4.1 *Projecting E_n (or O_n) onto a fixed set of s coordinates, $s < n$, yields a multiset of all vectors of V_s each with multiplicity 2^{n-s-1} .*

Let $B_{e,n}$ ($B_{o,n}$) be the $n \times 2^{n-1}$ binary matrix whose columns are the vectors of E_n (O_n) in some order. The problem of constructing an n -out-of- n audio cryptography scheme can be solved with the following two $n \times 2^{n-1}$ matrix collections:

$$\mathcal{C}_0 = \{\text{all matrices obtained by permuting the columns of } B_{e,n}\},$$

$$\mathcal{C}_1 = \{\text{all matrices obtained by permuting the columns of } B_{o,n}\},$$

In this scheme, the dealer expands the original beep into 2^{n-1} beeps in each of the n shares. The above collections \mathcal{C}_0 and \mathcal{C}_1 satisfy the criteria of Definition 2.1.

Lemma 4.2 *The above construction is an (n, n) -ACS with parameters $\ell = 2^{n-1}$ and $p = 2^{n-1}$.*

Proof: Clearly, matrix $B_{e,n}$ has exactly one column with all zeros, while matrix $B_{o,n}$ has no such columns. This satisfies condition 2. of Definition 2.1. Furthermore, deleting any $k > 0$ rows of $B_{e,n}$ ($B_{o,n}$) corresponds to projecting E_n (O_n) onto the remaining $s = n - k$ coordinates, hence by Lemma 4.1 in both cases we get up to a permutation of columns the same submatrix. This satisfies condition 1. of Definition 2.1. Q.E.D.

Naor and Shamir suggested the same construction mechanism for an (n, n) -VCS with parameters $m = 2^{n-1}$, $\alpha = 1/2^{n-1}$ and $r = 2^{n-1}$!. Now we extend some of the results presented in [1] to the audio cryptography schemes. Namely, we show that the above proposed audio cryptography scheme is optimal by using a slight modification of the corresponding proof given in [1].

Lemma 4.3 *If U is any proper subset of $[1, n]$, and A_1, \dots, A_n and B_1, \dots, B_n are two sequences of sets such that $|\bigcup_{i \in U} A_i| = |\bigcup_{i \in U} B_i|$, then $|\bigcap_{i \in U} A_i| = |\bigcap_{i \in U} B_i|$.*

Proof: Let A_1, \dots, A_n and B_1, \dots, B_n be two sequences of sets and suppose that for $W \subseteq U$, both proper subsets of $[1, n]$, $|\bigcup_{i \in W} A_i| = |\bigcup_{i \in W} B_i|$. Set $|U| = q$. Then, for any $i, j \in U$, $i \neq j$, we have that $|A_i \cup A_j| = |B_i \cup B_j|$. By the inclusion-exclusion principle we have $|A_i \cap A_j| = |A_i| + |A_j| - |A_i \cup A_j| = |B_i| + |B_j| - |B_i \cup B_j| = |B_i \cap B_j|$. Using this result, the fact that for distinct $i, j, k \in U$, $|A_i \cup A_j \cup A_k| = |B_i \cup B_j \cup B_k|$, and the inclusion-exclusion principle, we similarly show that $|A_i \cap A_j \cap A_k| = |B_i \cap B_j \cap B_k|$. Inductively we proceed to show that for $U = \{a_1, a_2, \dots, a_q\}$, we have that $|A_{a_1} \cap A_{a_2} \cap \dots \cap A_{a_q}| = |B_{a_1} \cap B_{a_2} \cap \dots \cap B_{a_q}|$. Q.E.D.

Given that $|\bigcap_{i \in U} A_i| = |\bigcap_{i \in U} B_i|$, we are interested to know how different the cardinalities $|\bigcup_{i=1}^n A_i|$ and $|\bigcup_{i=1}^n B_i|$ are. More precisely we would like to find a bound for $||\bigcup_{i=1}^n A_i| - |\bigcup_{i=1}^n B_i||$. This problem was solved by Linial and Nisan, who noticed that the problem is scalable in the sense that multiplying each size by a constant would change the difference by that constant [5]. Thus, one can divide each size by the size of the ground set (that we previously denoted by G) to obtain a probability representation. To use this representation, Linial and Nisan defined $E(k, n)$, and $D(k, n)$ in [5] as follows:

Definition 4.1

$$E(k, n) = \sup \left(P\left(\bigcup_{i=1}^n A_i\right) - P\left(\bigcup_{i=1}^n B_i\right) \right), \quad (1)$$

where $P(X)$ is a probability of an event X .

Definition 4.2

$$D(k, n) = \inf \left(\max_{m \in [0, n]} (|f(m) - 1|) \right), \quad (2)$$

where the infimum ranges over all polynomials f of degree at most k and zero constant term.

Furthermore, in [5], Linial and Nisan proved the following useful lemma:

Lemma 4.4

$$E(k, n) = \frac{2D(k, n)}{1 + D(k, n)}. \quad (3)$$

Finally, we make use of the following major result shown in [5]:

Theorem 4.5

$$D(n-1, n) = \frac{1}{2^{n-1} - 1}.$$

Applying Theorem 4.5 to Lemma 4.4 we get the following corollary:

Corollary 4.6

$$E(n-1, n) = \frac{1}{2^{n-1}}.$$

Theorem 4.7 *In any n -out-of- n audio cryptography scheme $\ell \geq 2^{n-1}$.*

Proof: Consider an (n, n) -ACS with parameters ℓ and p . Let the two collections of $n \times \ell$ matrices that satisfy Definition 2.1 be $\mathcal{C}_0 = \{S_1^0, S_2^0, \dots, S_p^0\}$ and $\mathcal{C}_1 = \{S_1^1, S_2^1, \dots, S_p^1\}$. Note that S_i^j is an $n \times \ell$ Boolean matrix. Let $G = [1, p] \times [1, \ell]$. We now construct two sequences of subsets of G , A_1, A_2, \dots, A_n and B_1, B_2, \dots, B_n as follows:

$$(x, y) \in A_i \Leftrightarrow S_x^0[i, y] = 1,$$

$$(x, y) \in B_i \Leftrightarrow S_x^1[i, y] = 1.$$

Let U be a proper subset of $[1, n]$ and $|U| = q$ (therefore $q < n$). By the definition of \mathcal{C}_0 and \mathcal{C}_1 , taking the bitwise OR of any q rows of any matrix S_i^0 ($i \in [p]$) results in an ℓ -binary vector that is equal up to a cyclic shift to an ℓ -binary vector obtained by taking the bitwise OR of any q rows of any matrix S_j^1 ($j \in [p]$). This implies that $|\bigcup_{i \in U} A_i| = |\bigcup_{i \in U} B_i|$. By Lemma 4.3 this implies that $|\bigcap_{i \in U} A_i| = |\bigcap_{i \in U} B_i|$. Corollary 4.6 actually states that when $k = n - 1$, then $\sup(P(\bigcup_{i=1}^n A_i) - P(\bigcup_{i=1}^n B_i)) = \frac{1}{2^{n-1}}$ which implies the following:

$$\left| \bigcup_{i=1}^n A_i - \bigcup_{i=1}^n B_i \right| \leq |G| \cdot \frac{1}{2^{n-1}} = p \cdot \ell \cdot \frac{1}{2^{n-1}}.$$

Notice that if for all matrices in \mathcal{C}_0 and \mathcal{C}_1 the difference of Hamming weight of bitwise OR of all of their rows is larger than $\ell \cdot \frac{1}{2^{n-1}}$, then that would contradict Corollary 4.6. Therefore, there exist a matrix S_a^0 and a matrix S_b^1 for which the difference of Hamming weight of bitwise OR of all of their rows is at most $\ell \cdot \frac{1}{2^{n-1}}$. Since by the definition of collections \mathcal{C}_0 and \mathcal{C}_1 it follows that for any matrix from \mathcal{C}_0 and any matrix from \mathcal{C}_1 the bitwise OR of all of their rows must differ by a strictly positive integer, then ℓ must be at least 2^{n-1} since otherwise for the two matrices S_a^0 and S_b^1 the difference of Hamming weight of bitwise OR of all of their rows would be less than 1. Q.E.D.

Corollary 4.8 *The above constructed (n, n) -ACS is optimal.*

5. Generalizing to Audiovisual Cryptography

So far, we saw that the constructions for ACS's that we defined are mathematically identical to the constructions of VCS's. In the previous section we provided a construction for (n, n) -ACS, an audio sharing scheme that was not known to exist. In this section, we provide the further generalization that will reveal constructions not only for the general (n, k) -ACS, but also audio cryptography schemes for general qualified subsets of $[1, n]$, all of which were not known to exist [6, 7].

Definition 5.1 [1, 2, 3, 4] *A solution to the k -out-of- n visual cryptography scheme consists of two collections of $n \times \ell$ Boolean matrices \mathcal{C}_0 and \mathcal{C}_1 . The collections \mathcal{C}_0 and \mathcal{C}_1 constitute a (k, n) -VCS if for some nonnegative integers h and m , $h > m$, the following conditions are met:*

1. *The bitwise OR x of any k of the rows in \mathcal{C}_0 satisfies $H(x) \leq \ell - h$.*
2. *The bitwise OR x of any k of the rows in \mathcal{C}_1 satisfies $H(x) \geq \ell - m$.*
3. *For any $i_1 < i_2 < \dots < i_s$ in $[1, n]$ with $s < k$, the matrices obtained by restricting \mathcal{C}_0 and \mathcal{C}_1 to rows i_1, i_2, \dots, i_s are equal up to a column permutation.*

Lemma 5.1 *Existing constructions of (n, k) visual cryptography schemes are also constructions for (n, k) audio cryptography schemes, with $m = \ell$ and $p = r$.*

Proof: Note that the constraints of Definition 2.1 comply to the constraints of Definition 5.1. Q.E.D.

Therefore, the construction schemes that already exist for (n, k) -VCS also work for (n, k) -ACS. The first such constructions are proposed by Naor and Shamir [1], but more efficient constructions are presented in [2] and [3]. Details of these constructions are omitted due to complexity and lack of space.

In [3], Ateniese et al. proposed construction schemes for general qualified subsets of $[1, n]$. This is the ultimate generalization in visual secret sharing. For example, the possible qualified subsets in VCS with $n = 4$ shares could be only the subsets of $\{1, 2, 3, 4\}$ that contain sets $\{1, 2\}$, $\{2, 3\}$, and $\{3, 4\}$. Notice that, for example, $\{1, 3\}$ is non-qualified set. It turns out that the proposed visual cryptography schemes for arbitrary qualified subsets are also applicable to audio cryptography.

Let us recall some definitions from [3]. A *monotone access structure* Γ is a subset of $2^{[1, n]} \setminus \{\emptyset\}$, such that if $A \in \Gamma$ and $A \subseteq A' \subseteq [1, n]$ then $A' \in \Gamma$. Let Γ be a monotone access structure, a set $C \in \Gamma$ is a *minimal set* of Γ if it does not contain any set in $\Gamma \setminus \{C\}$. A *basis* Γ_0 of Γ is the family of all minimal sets of Γ . Note that in a (k, n) -VCS, $\Gamma_0 = \{B \subseteq [1, n] : |B| = k\}$.

Definition 5.2 [3] *Let Γ be an access structure on a set of n participants. Two collections of $n \times m$ Boolean matrices \mathcal{C}_0 and \mathcal{C}_1 constitute a visual cryptography scheme (Γ, m) -VCS if there exist positive values $\alpha(m)$ and $\{t_X\}_{X \in \Gamma_0}$ such that:*

1. *Any qualified set $X = \{i_1, i_2, \dots, i_p\} \in \Gamma_0$ can recover the shared secret. That is, for any $S \in \mathcal{C}_0$, the bitwise OR x of rows i_1, i_2, \dots, i_p satisfies $H(x) \leq t_X - \alpha(m) \cdot m$, while for any $S \in \mathcal{C}_1$, the bitwise OR y of rows i_1, i_2, \dots, i_p satisfies $H(y) \geq t_X$.*
2. *Any non-qualified set $X = \{i_1, i_2, \dots, i_p\} \notin \Gamma$ has no information about the shared secret. That is, the two collections of $p \times m$ matrices \mathcal{D}_0 and \mathcal{D}_1 obtained by restricting each $n \times m$ matrix in \mathcal{C}_0 and \mathcal{C}_1 respectively to rows i_1, i_2, \dots, i_p are equal up to a column permutation.*

We now similarly define a (Γ, ℓ) -ACS.

Definition 5.3 *Let Γ be an access structure on a set of n participants. Two collections of $n \times \ell$ Boolean matrices \mathcal{C}_0 and \mathcal{C}_1 constitute an audio cryptography scheme (Γ, m) -ACS if there exist positive values a and $\{t_X\}_{X \in \Gamma_0}$ such that:*

1. *Any qualified set $X = \{i_1, i_2, \dots, i_q\} \in \Gamma_0$ can recover the shared secret. That is, for any matrix from \mathcal{C}_0 , the bitwise OR x of rows i_1, i_2, \dots, i_q satisfies $H(x) \leq t_X - a$, while for any matrix from \mathcal{C}_1 , the bitwise OR y of rows i_1, i_2, \dots, i_q satisfies $H(y) \geq t_X$.*
2. *Any non-qualified set $X = \{i_1, i_2, \dots, i_q\} \notin \Gamma$ has no information about the shared secret. That is, the two collections of $q \times \ell$ matrices \mathcal{D}_0 and \mathcal{D}_1 obtained by restricting each $n \times \ell$ matrix in \mathcal{C}_0 and \mathcal{C}_1 respectively to rows i_1, i_2, \dots, i_q are equal up to a column permutation.*

Lemma 5.2 Existing constructions for (Γ, m) -VCS are also constructions for (Γ, ℓ) -ACS, with $m = \ell$ and $p = r$.

Proof: The constraints from Definition 5.3 comply to the constraints of Definition 5.2. Q.E.D.

6. Conclusions

We presented a new kind of audio cryptography, the one that possesses a strong parallel to the well-studied visual cryptography. In doing so, we were able to construct audio sharing schemes that no one was able to construct up until now. In fact we applied the existing visual cryptography schemes to obtain the corresponding audio cryptography schemes. Finally, we concluded that the sharing schemes for visual cryptography are also the sharing schemes for audio cryptography, and perhaps such schemes should be referred to as the *audiovisual cryptography schemes*.

References

- [1] M. Naor and A. Shamir, *Visual Cryptography*, Advances in Cryptology - EUROCRYPT '94, A. De Santis (Ed.), volume **950** of Lecture Notes in Computer Science, Springer-Verlag, Berlin, Germany, pp 1–12, 1995.
- [2] S. Droste, *New Results on Visual Cryptography*, in CRYPTO '96, Lecture Notes in Computer Science vol. 1109, pages 401–415. Springer-Verlag, 1996.
- [3] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, *Constructions and Bounds for Visual Cryptography*, in proc. 23rd International Colloquium on Automata, Languages and Programming, F.M. auf der Heide and B. Monien (Ed.), volume **1099**, Springer-Verlag, Berlin, Germany, pp 416–428, 1996.
- [4] P.A. Eisen and D.R. Stinson, *Threshold Visual Cryptography Schemes With Specified Whiteness Levels of Reconstructed Pixels*, Designs, Codes and Cryptography, volume **25**, pp 15–61, 2002.
- [5] N. Linial and N. Nisan, *Approximate inclusion-exclusion*, the Internet resource available at <http://www.cs.huji.ac.il/~nati/>
- [6] Y. Desmedt, S. Hou, and J.-J. Quisquater, *Audio and Optical Cryptography*, Advances in Cryptology - ASIACRYPT '98, K. Ohta and D. Pei (Ed.), volume **1514** of Lecture Notes in Computer Science, Springer-Verlag, Beijing, China, pp 392–404, 1998.
- [7] C.-C. Lin, C.-S. Laih, and C.-N. Yang, *New Audio Secret Sharing Schemes With Time Division Technique*, Journal of Information Science and Engineering, volume **19(4)**, Institute of Information Science, Academia Sinica, Taipei, Taiwan, pp 605–614, 2003.