九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Applications of Algebraic Structures in Visual Cryptography

Adhikari, Avishek
Department of Pure Mathematics, Calcutta University

https://hdl.handle.net/2324/1434301

出版情報：MI lecture note series. 53, pp.93-101, 2013-12-26. 九州大学マス・フォア・インダストリ研究所
バージョン：
権利関係：

KYUSHU UNIVERSITY

Applications of Algebraic Structures in Visual Cryptography

Avishek Adhikari
Department of Pure Mathematics
Calcutta University
35 Ballygunge Circular Road, Kolkata 700019
E-mail : avishek.adh@gmail.com

Abstract

Most of the secret sharing schemes are based on algebraic calculations in their realizations. But there are some different realizations from ordinal secret sharing schemes. Visual cryptography is one such secret sharing scheme. In visual cryptography, the problem is to encrypt some written material (handwritten notes, printed text, pictures, etc.) in a perfectly secure way in such a manner that the decoding may be done visually, without any cryptographic computations. The concept of visual cryptography was first proposed by Naor and Shamir in 1994. Visual cryptographic scheme for a set P of n participants is a cryptographic paradigm that enables a secret image to be split into n shadow images called shares, where each participant in P receives one share. Certain qualified subsets of participants can "visually" recover the secret image with some loss of contrast, but other forbidden sets of participants have no information about the secret image. In this talk, we shall explore how linear algebra and statistical design theory play an important role in constructing visual cryptographic schemes. We further emphasize on some of the open problems related to visual cryptographic schemes for both (k, n)-threshold and general access structures.

References

[1] Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.

[2] Avishek Adhikari, M R Adhikari, *Basic Modern Algebra with Applications*, To be published by Springer.

[3] Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.

[4] Avishek Adhikari, M. R. Adhikari and Y. P Chaubey, *Contemporary Topics in Mathematics and Statistics with Applications*, Asian Books , India, 2013.

[5] Avishek Adhikari, *Linear Algebraic Techniques to Construct black and white Visual Cryptographic Schemes for General Access Structure and its Applications to Color Images*, Design, Codes and Cryptography, 2013, DOI 10.1007/s10623-013-9832-5.

[6] A. Shamir, *How to share a secret*, Communication of ACM, Vol. 22, No. 11, 612-613, 1979.

Applications of Algebraic Structures in Visual Cryptography

Avishek Adhikari

website: www.imbic.org/avishek.html

Research Team Members

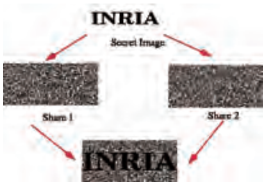
Partha Sarathi Roy, Angsuman Das, Ushnish Sarkar, Sabyasachi Dutta

Department of Pure Mathematics

University of Calcutta, Kolkata.

Secret Sharing for General Access Structure?

Example of (2, 2)-VCS



(2, 2)-VCS

For Black pixel

For White pixel

(2, 2)-VCS

For Black pixel

For White pixel

0	0	1	1
0	1	0	1
0	1	1	1

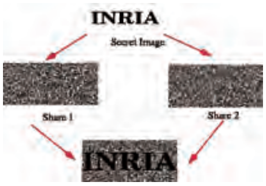
(2, 2)-VCS

For Black pixel

For White pixel

$S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$.

Example of $(2,2)$-VCS



Relative contrast

Let us consider a $(2,n)$-VCS on a set $\mathcal{P} = \{1, 2, \ldots, n\}$ of n participants with basis matrices S^0 and S^1 and having pixel expansion m. Then the *relative contrast* for the participants corresponding to X, $X \subseteq \mathcal{P}$, is denoted by $\alpha_X(m)$ and is defined as

$$\frac{w(S^1_X) - w(S^0_X)}{m}.$$

Secret Sharing for General Access Structure?

- Secret sharing refers to method for distributing a secret, say K, amongst a set $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ of n participants , each of which is allocated a share of the secret in such a way that certain qualified set of participants can reconstruct the secret by combining their shares while certain set of participants gets no information about the secret even when they combine their shares.
- The set of participants who are qualified to reconstruct the share is called qualified set of participants, while the set of participants who are not qualified to reconstruct the secret is known as forbidden set of participants.
- The collection of all qualified sets of participants is denoted by Γ_{Qual} while the set of all forbidden sets of participants are known as Γ_{Forb}. Γ_0 denotes the set of minimal qualified sets of participants.
- $(\Gamma_{Qual}, \Gamma_{Forb})$ is known as an access structure on the set of participants $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$.

Basis Matrix

Definition

Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set $\mathcal{P}$ of n participants. A $(\Gamma_{Qual}, \Gamma_{Forb}, m)$-VCS with relative difference $\alpha(m)$ and a set of thresholds $\{t_X\}_{X \in \Gamma_{Qual}}$ is realized using the $n \times m$ basis matrices S^0 and S^1 if the following two conditions hold:

1. *If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$, then S^0_X, the "or" of the rows $i_1, i_2, \ldots, i_p$ of S^0, satisfies $w(S^0_X) \leq t_X - \alpha(m) \cdot m$; whereas, for S^1 it results in $w(S^1_X) \geq t_X$.*
2. *If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$, the two $p \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_p$ are equal up to a column permutation.*

$(2,n)$-VCS by Naor and Shamir

$$S^0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \textit{and} \quad S^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Here the *relative contrast* for any two participants is $\frac{1}{4}$ and the *pixel expansion* is 4.

Linear Algebraic Techniques to construct VCS for General Access Structures

- $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{\{1,2\},\{1,3\},\{1,4\},\{2,3,4\}\}$.
- $\{\{1,2\},\{1,3\}\}$ and $\{\{1,4\},\{2,3,4\}\}$.
- $\left.\begin{aligned} x_1 + x_2 &= 0 \\ x_1 + x_3 &= 0 \\ x_4 &= 0 \end{aligned}\right\} \cdots (1)$ and $\left.\begin{aligned} x_1 + x_2 &= 1 \\ x_1 + x_3 &= 1 \\ x_4 &= 0 \end{aligned}\right\} \cdots (2)$
- $\left.\begin{aligned} x_1 + x_4 &= 0 \\ x_2 + x_3 + x_4 &= 0 \end{aligned}\right\}$ (3) and $\left.\begin{aligned} x_1 + x_4 &= 1 \\ x_2 + x_3 + x_4 &= 1 \end{aligned}\right\} \cdots (4)$

$$S^0_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, S^1_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

$$S^0_2 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, S^1_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Linear Algebraic Techniques to construct VCS for General Access Structures

- $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{\{1,2\},\{1,3\},\{1,4\},\{2,3,4\}\}$.
- $$S^0 = S^0_1 || S^0_2 = \left[\begin{array}{cc|cccc} 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

$$S^1 = S^1_1 || S^1_2 = \left[\begin{array}{cc|cccc} 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

Main Theorem

Theorem

For any given strong strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ on a set $\mathcal{P} = \{1, 2, \ldots, n\}$ of n participants with $\Gamma_0 = \{B_1, B_2, \ldots, B_k\}$ where $B_i \subseteq \mathcal{P}, \forall\, i = 1, 2, \ldots, k$ and for any permutation $\sigma \in S_k$, the symmetric group of degree k, there exists a strong visual cryptographic scheme $(\Gamma_{Qual}, \Gamma_{Forb}, m)$ on $\mathcal{P}$ with $m = m_\sigma$, where m_σ is given as follows:

$$m_\sigma = \begin{cases} \sum_{i=1}^{l} 2^{|B_{\sigma(2i-1)} \cup B_{\sigma(2i)}|-2} & \text{if } k = 2l,\ l \geq 1 \\ \sum_{i=1}^{l} 2^{|B_{\sigma(2i-1)} \cup B_{\sigma(2i)}|-2} + 2^{|B_{\sigma(2l+1)}|-1} & \text{if } k = 2l+1,\ l \geq 0. \end{cases}$$

Construction of Basis Matrices

- Suppose we want to construct a scheme on a set of 6 participants $\mathcal{P} = \{1, 2, 3, 4, 5, 6\}$ in which the minimal qualified set is $\Gamma_0 = \{\{1,2,3\},\{2,3,4\},\{2,4,5\},\{1,2,5\},\{1,3,6\},\{2,4,6\},\{3,4,5\}\}$.
- Note that $\Gamma_0 =$ $\{\{1,2,3\},\{1,2,5\},\{2,4,3\},\{2,4,6\},\{2,4,5\},\{3,4,5\},\{1,3,6\}$
- Let us start with $\{1, 2, 3\}$ and $\{1, 2, 5\}$. Consider the following two associated system of linear equations over the binary field $\mathbf{Z_2}$

$$\begin{array}{rcl} x_1 + x_2 + x_3 & = & 0 \\ x_1 + x_2 + x_5 & = & 0 \\ x_4 & = & 0 \end{array} \quad ---(3) \qquad \begin{array}{rcl} x_1 + x_2 + x_3 & = & 1 \\ x_1 + x_2 + x_5 & = & 1 \\ x_4 & = & 0 \end{array} \quad ---(4)$$

$$G_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad \begin{array}{c} \leftarrow 1 \rightarrow \\ \leftarrow 2 \rightarrow \\ \leftarrow 3 \rightarrow \\ \leftarrow 5 \rightarrow \end{array} \quad \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = G_1$$

Important Observations

- $\{\{1,2,3\},\{1,2,5\},\{2,4,3\},\{2,4,6\},\{2,4,5\},\{3,4,5\},\{1,3,6\}\}$
- $G_0 =$

$$\begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \left[\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right]$$

- $G_1 =$

$$\begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \left[\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

Open Problem: Find a suitable permutation to get minimum pixel expansion.

(k, n)-Threshold Scheme: as a particular case

Theorem

Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set $\mathcal{P} = \{1, 2, \ldots, n\}$ of n participants with $\Gamma_0 = \{A \subseteq \mathcal{P} : |A| = k\}, 2 \leq k \leq n$. Then there exists a strong (k, n)-VCS with

$$m_{our} = \begin{cases} l \cdot 2^{k-2}, & \text{if } l = \binom{n}{k} \text{ is even} \\ (l+1) \cdot 2^{k-2}, & \text{if } l = \binom{n}{k} \text{ is odd} \end{cases}$$

and relative contrast $\alpha(m) = \frac{1}{m_{our}}$.

$(4, 5)$-Threshold Scheme: An Efficient Construction

Let us consider the $(4, 5)$-VCS with $\{\{1,2,3,4\},\{1,2,3,5\},\{1,2,4,5\},\{1,3,4,5\},\{2,3,4,5\}\}$.

$$s^0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ & *^1 & *^2 & *^3 & *^4 & & & & & *^5 & *^6 & *^7 & *^8 & & & & & & & & & & & *^9 \end{bmatrix}$$

$$s^1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ *^7 & & & *^9 & & & & *^8 & *^3 & & & & & & & *^4 & & & & *^1 & & *^2 & *^5 & *^6 \end{bmatrix}$$

$$S^0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix},$$

$$S^1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Open Problem: For a future problem, one may think of finding exact number of common columns in S^0 and S^1.

Open Problems

- $\Gamma_0 = \{\{1,2\},\{2,3\},\{3,4\},\{1,4\}\}$.
- $$\left.\begin{array}{l} x_1 + x_2 = 0 \\ x_2 + x_3 = 0 \\ x_3 + x_4 = 0 \end{array}\right\} \cdots (5) \text{ and } \left.\begin{array}{l} x_1 + x_2 = 1 \\ x_2 + x_3 = 1 \\ x_3 + x_4 = 1 \end{array}\right\} \cdots (6).$$
- $S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Open Problem: Characterize a given access structure on which we can take 3 equations together to get less pixel expansion.

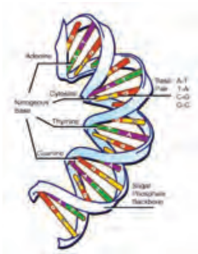
Introduction

- Secret Sharing Schemes,
- DNA Computing,
- Mathematics.

Aim of Our Work

Suppose we want to distribute a secret binary string to a set $\{P_1, P_2, \ldots, P_n\}$ of n participants in such a way that certain designated set of participants can reveal the secret by pulling their shares, but no forbidden set of participants has any information about the secret binary string.

Why DNA?

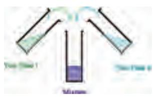


- The very small size,
- The huge storage capacity,
- Easy to carry or hide,
- Made up of A, T, G, C,
- Huge parallel computing,
- Stable as a DNA double strand,
- High longevity,
- Easy to get synthesized DNA

DNA encoding of binary strings

- a binary string can be represented as a set of integers that corresponds the positions where the bits are 1 from left to right.
- 1011 can be represented as a set $\{1,3,4\}$,
- each integer i can be represented in a DNA double strand notation as follows $ds_i = \updownarrow (GAATT)^i$.
- if $\alpha = 1011$, the DNA double strand representation of α is the test tube $T[\alpha] = \{ds_1,\ ds_3,\ ds_4\}$.

Mixing operation



- Take the content of two test tubes.
- Mixing can be done by dehydrating the tube contents (if not already in solution) and then combining the fluids together into a new tube, by pouring and pumping.

Bio-mathematical operations

1011
"or"
1001
1011

- Boolean *"or"* operation between two binary strings
- if $\alpha = 1011$ and $\beta = 1001$,
- the binary *"or"* of two strings will be 1011.
- $T[\alpha]$ ($T[\beta]$) the test tube corresponding to the binary string α (β).
- pore the contents of the two test tubes to get binary *"or"*.

Automated DNA Sequencing

- To read the DNA double strands in the test tube we need the process called DNA sequencing.

Outlay of our scheme

- Consider the secret sharing scheme on $\mathcal{P} = \{1, 2, 3, 4\}$ of 4 participants, where $\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{2, 4\}, \{1, 4\}\}$.
- $\Gamma_{Qual} = \{Y \subseteq \mathcal{P} : X \subseteq Y \text{for some } X \in \Gamma_0\}$ and $\Gamma_{Forb} = 2^{\mathcal{P}} \setminus \Gamma_{Qual}$.
- let the secret binary string be $x = x_1x_2x_3 = 011$.
- Assume that the DNA encoding, the mixing process are public.

Share Distribution

- The dealer chooses two Boolean matrices
$$G_0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } G_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$
- Since $x_1 = 0$, the dealer considers the matrix G_0 and apply a random permutation to the columns of G_0 and produces a matrix M_1.
- Similarly, for x_2 and x_3 on G_1 to produce matrices M_2 and M_3.
- Assume that the DNA encoding, the mixing process are public.

Share Distribution

- Let $M = M_1||M_2||M_3$.
- first row of M is $\alpha_1 = 010110101010$. Similarly $\alpha_2 = 010101100110$, $\alpha_3 = 010010001000$ and $\alpha_4 = 000100010001$.
- dealer converts the binary strings to DNA representations to get the test tubes
$T[\alpha_1] = \{ds_2, ds_4, ds_5, ds_7, ds_9, ds_{11}\}$,
$T[\alpha_2] = \{ds_2, ds_4, ds_6, ds_7, ds_{10}, ds_{11}\}$,
$T[\alpha_3] = \{ds_2, ds_4, ds_5, ds_9\}$,
$T[\alpha_4] = \{ds_4, ds_8, ds_{12}\}$,

Share Distribution

- $T[\alpha_i]$ is given to the participants P_i, $i = 1, 2, \ldots, n$ through a secret channel.
- Also the values $m = 4$ and $k = 3$ are given to the participants even through an insecure channel.

Decryption by the Qualified participants

- Let P_1, P_2 come together.
- They use mixing procedure with test tubes $T[\alpha_1]$ and $T[\alpha_2]$ to get $T[\alpha_1] \cup T[\alpha_2] = \{ds_2, ds_4, ds_5, ds_6, ds_7, ds_9, ds_{10}, ds_{11}\}$.
- Execute automated DNA sequencing method to read the DNA double strands.
- With the knowledge of decoding the DNA representation to the binary string, the values of $k = 3$ and $m = 4$, the participants P_1 and P_2 can convert the DNA representation to the binary string $y = 010111101110$.

Decryption by the Qualified participants

- Since, the value of m is known to the participants, P_1 and P_2 can break y as $y = (0101)(1110)(1110)$.
- Next they will find the value of w as 3 and then they will compute $z = 011$, as $BW(0101) < 3$, $BW(1110) = 3$. Thus P_1 and P_2 can recover the secret 011.

Forbidden set of participants

- Let $Y = \{P_3, P_4\}$ come together.
- They use mixing procedure with test tubes $T[\alpha_3]$ and $T[\alpha_4]$ to get $T[\alpha_1] \cup T[\alpha_2] = \{ds_2, ds_4, ds_5, ds_8, ds_9, ds_{12}\}$.
- they will convert the DNA representation to the binary string $y = (0101)(1001)(1001)$.
- Thus looking at those it is not possible to predict whether they correspond to 0 or 1.

DNA Microarray

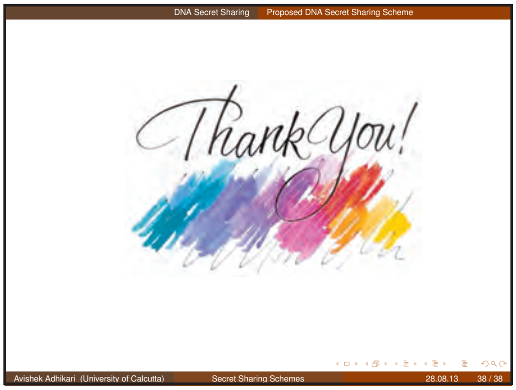
- Affymetrix chips has more than 3,50,000 oligos per chip
- Around 48,000 different DNA spots can fit on a glass of this array.
- Statistical data analysis using computers gives less error.

Bibliography

- Avishek Adhikari, *Linear Algebraic Techniques to Construct black and white Visual Cryptographic Schemes for General Access Structure and its Applications to Color Images*, Design, Codes and Cryptography, 2013, DOI 10.1007/s10623-013-9832-5.
- Avishek Adhikari, "DNA Secret Sharing", IEEE World Congress on Evolutionary Computation 2006, CEC 2006, July 16-21, 1407-1411, 2006.
- Avishek Adhikari and Bimal Roy, *On some constructions of monochrome visual cryptographic schemes*, Page(s): 1-6, Digital Object Identifier 10.1109/INFTECH.2008.4621609, appeared in the IEEE Conference Proceedings, 1st International Conference on Information Technology, Faculty of Electronics, Telecommunications & Informatics Gdansk University of Technology, Poland, May 18-21, 2008.
- Avishek Adhikari, M. Bose, D. Kumar and Bimal Roy, *Applications of Partially Balanced and Balanced IncompleteBlock Designs in developing Visual Cryptographic Schemes*, IEICE TRANS. FUNDAMENTALS, Japan, Vol. E-90A, No. 5, pp. 949-951, May 2007.
- Avishek Adhikari, and M. Bose, "A New Visual Cryptographic Scheme Using Latin Squares," IEICE Transactions on Fundamentals, E87-A, No. 5, 1998-2002, 2004.
- Avishek Adhikari, T. K. Dutta, and B Roy, *A New Black and White Visual Cryptographic Scheme for General Access Structures*, Recent Advances in Cryptology : Indocrypt 2004, Lecture Notes in Computer Science, Springer, 2004, 399-413.
- Avishek Adhikari, and S. Sikdar, "A New (2, n) Color Visual Threshold Scheme for Color Images," Indocrypt'03, Lecture Notes in Computer Science, Springer-Verlag, 2904, 148-161, 2003.
- Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.
- Avishek Adhikari, M R Adhikari, *Basic Modern Algebra with Applications*, To be published by Springer.

Questions

Questions???


DNA Secret Sharing
Proposed DNA Secret Sharing Scheme
Thank You!
Avishek Adhikari (University of Calcutta)
Secret Sharing Schemes
28.08.13
38 / 38