Connections Among Algebra, Statistical Designs and Secret Sharing Schemes

Adhikari, Avishek
Department of Pure Mathematics, Calcutta University

https://hdl.handle.net/2324/1434295

出版情報：MI lecture note series. 53, pp.9-17, 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：

Workshop

Connections Among Algebra, Statistical Designs and Secret Sharing Schemes

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

Abstract

Due to the recent development of computers and computer networks, huge amount of digital data can easily be transmitted or stored. But the transmitted data in networks or stored data in computers may easily be destroyed or substituted by enemies if the data are not enciphered by some cryptographic tools. So it is very important to restrict access of confidential information stored in a computer or in a certain nodes of a system. Access should be gained through a secret key, password or token. Again storing the secret key or password securely could be a problem. The best solution could be to memorize the secret key. But for large and complicated secret key, it is almost impossible to memorize the key. As a result, it should be stored safely. While storing data in a hard disk, the threats such as troubles of storage devices or attacks of destruction make the situation even worse. In order to prevent such attacks, we may make as many copies of the secret data as possible. But, if we have many copies of the secret data, the secret may be leaked out and hence the number of the copies should be as small as possible. Under this circumstances, it is desirable that the secret key should be governed by a secure key management scheme. If the key or the secret data is shared among several participants in such a way that the secret data can only be reconstructed by a significantly large and responsible group acting in agreement, then a high degree of security is attained. Shamir and Blakley, independently, addressed this problem in 1979 when they introduced the concept of a threshold secret sharing scheme. A (t,n)-threshold scheme is a method whereby n pieces of information, called shares, corresponding to the secret data or key K, are distributed to n participants so that the secret key can be reconstructed from the knowledge of any t or more shares and the secret key can not be reconstructed from the knowledge of fewer than t shares. This this we we further emphasize on a special type of secret sharing scheme known as visual secret sharing scheme. Visual cryptographic scheme, for a set $\mathcal{P}$ of n participants, is a cryptographic paradigm that enables us to split a secret image, which may be some

handwritten note, printed text, picture, etc., 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 with some loss of contrast, but other forbidden sets of participants have no information about the secret image. A "visual recovery" for a set $X \subseteq \mathcal{P}$ consists of photocopying the shares given to the participants in X onto the transparencies, and then stacking them. Since the reconstruction is done by human visual system, no computation is involved during decoding unlike traditional cryptographic schemes where a fair amount of computation is needed to reconstruct the plain text. In this talk, we shall describe how algebra and statistical designs play an important role in constructing visual cryptographic schemes.

References

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

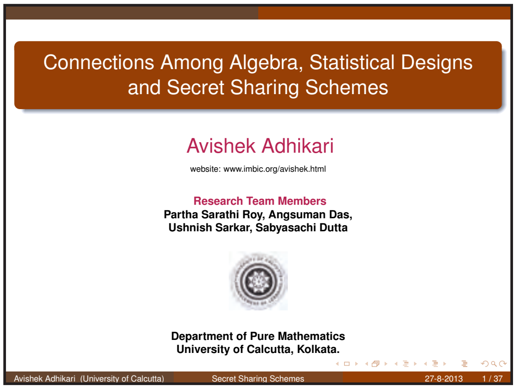
[2] Avishek Adhikari, M R Adhikari, *Basic Modern Algebra with Applications*, To be published by Springer.

[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.



Connections Among Algebra, Statistical Designs and Secret Sharing Schemes

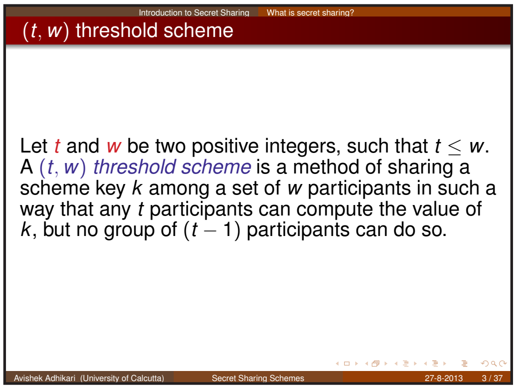
Avishek Adhikari

website: www.imbic.org/avishek.html

Research Team Members
Partha Sarathi Roy, Angsuman Das,
Ushnish Sarkar, Sabyasachi Dutta

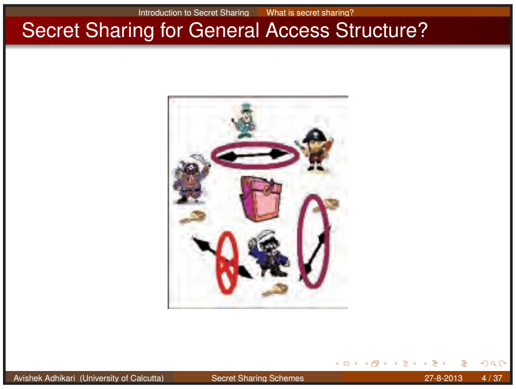
Department of Pure Mathematics
University of Calcutta, Kolkata.

What is secret sharing?

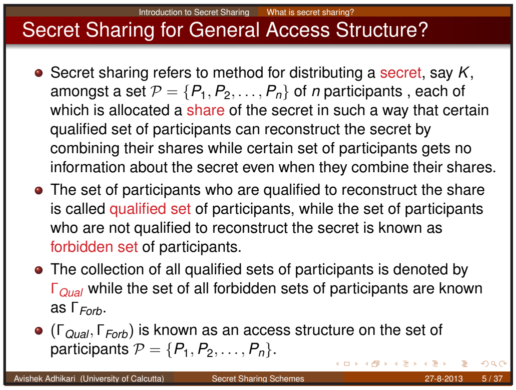


(t, w) threshold scheme

Let t and w be two positive integers, such that $t \leq w$. A (t, w) *threshold scheme* is a method of sharing a scheme key k among a set of w participants in such a way that any t participants can compute the value of k, but no group of $(t - 1)$ participants can do so.

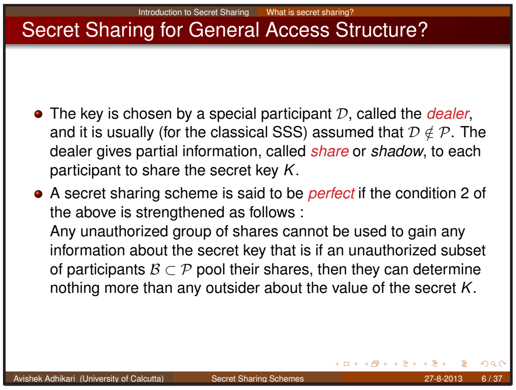


Secret Sharing for General Access Structure?



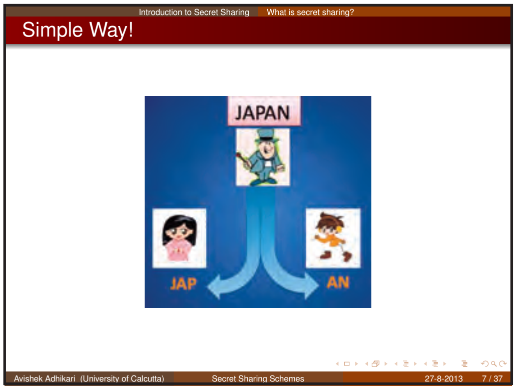
Secret Sharing for General Access Structure?

- 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}.
- $(\Gamma_{Qual}, \Gamma_{Forb})$ is known as an access structure on the set of participants $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$.



Secret Sharing for General Access Structure?

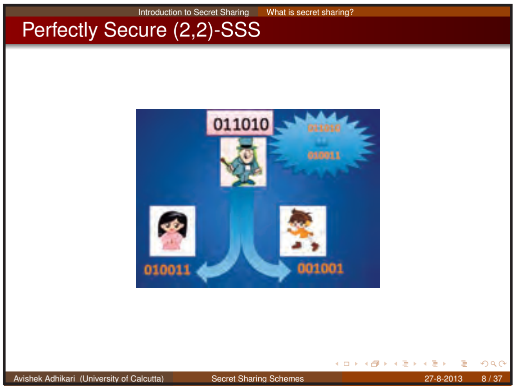
- The key is chosen by a special participant $\mathcal{D}$, called the *dealer*, and it is usually (for the classical SSS) assumed that $\mathcal{D} \notin \mathcal{P}$. The dealer gives partial information, called *share* or *shadow*, to each participant to share the secret key K.
- A secret sharing scheme is said to be *perfect* if the condition 2 of the above is strengthened as follows :
Any unauthorized group of shares cannot be used to gain any information about the secret key that is if an unauthorized subset of participants $\mathcal{B} \subset \mathcal{P}$ pool their shares, then they can determine nothing more than any outsider about the value of the secret K.



Introduction to Secret Sharing What is secret sharing?

Simple Way!

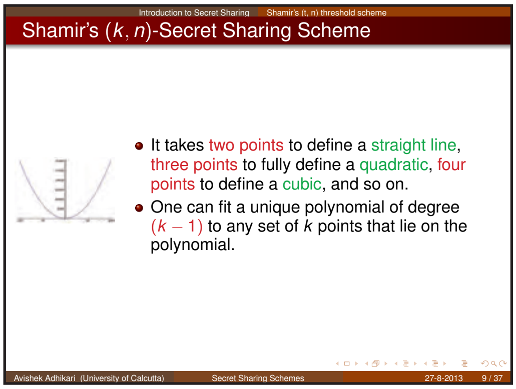
Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 7 / 37



Introduction to Secret Sharing What is secret sharing?

Perfectly Secure (2,2)-SSS

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 8 / 37

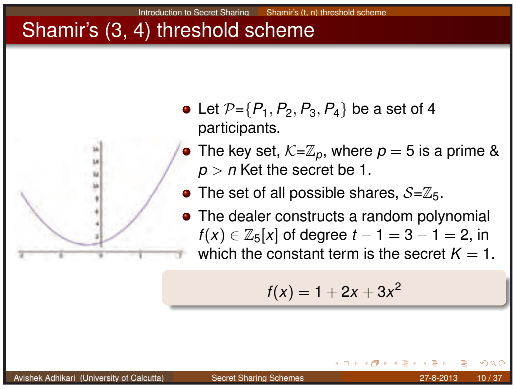


Introduction to Secret Sharing Shamir's (t, n) threshold scheme

Shamir's (k, n)-Secret Sharing Scheme

- It takes two points to define a straight line, three points to fully define a quadratic, four points to define a cubic, and so on.
- One can fit a unique polynomial of degree $(k-1)$ to any set of k points that lie on the polynomial.

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 9 / 37



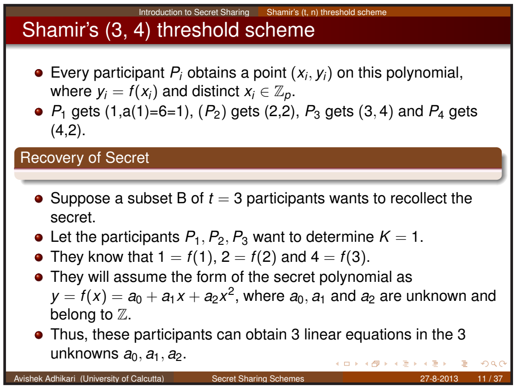
Introduction to Secret Sharing Shamir's (t, n) threshold scheme

Shamir's (3, 4) threshold scheme

- Let $\mathcal{P}$=$\{P_1, P_2, P_3, P_4\}$ be a set of 4 participants.
- The key set, $\mathcal{K}$=$\mathbb{Z}_p$, where $p=5$ is a prime & $p>n$ Ket the secret be 1.
- The set of all possible shares, $\mathcal{S}$=$\mathbb{Z}_5$.
- The dealer constructs a random polynomial $f(x) \in \mathbb{Z}_5[x]$ of degree $t-1=3-1=2$, in which the constant term is the secret $K=1$.

$$f(x) = 1 + 2x + 3x^2$$

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 10 / 37



Introduction to Secret Sharing Shamir's (t, n) threshold scheme

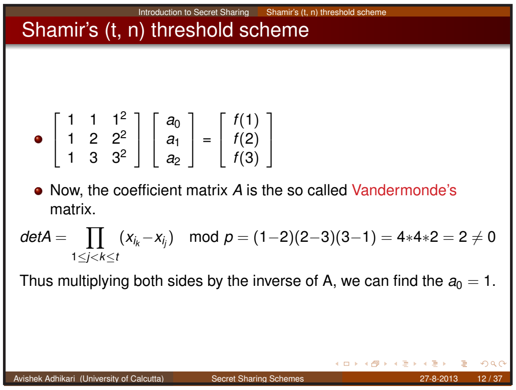
Shamir's (3, 4) threshold scheme

- Every participant P_i obtains a point (x_i, y_i) on this polynomial, where $y_i = f(x_i)$ and distinct $x_i \in \mathbb{Z}_p$.
- P_1 gets (1,a(1)=6=1), (P_2) gets (2,2), P_3 gets $(3,4)$ and P_4 gets (4,2).

Recovery of Secret

- Suppose a subset B of $t=3$ participants wants to recollect the secret.
- Let the participants P_1, P_2, P_3 want to determine $K=1$.
- They know that $1=f(1)$, $2=f(2)$ and $4=f(3)$.
- They will assume the form of the secret polynomial as $y=f(x)=a_0+a_1x+a_2x^2$, where a_0, a_1 and a_2 are unknown and belong to $\mathbb{Z}$.
- Thus, these participants can obtain 3 linear equations in the 3 unknowns a_0, a_1, a_2.

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 11 / 37



Introduction to Secret Sharing Shamir's (t, n) threshold scheme

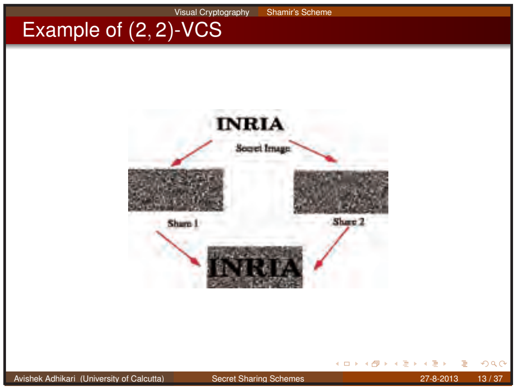
Shamir's (t, n) threshold scheme

- $\begin{bmatrix} 1 & 1 & 1^2 \\ 1 & 2 & 2^2 \\ 1 & 3 & 3^2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} f(1) \\ f(2) \\ f(3) \end{bmatrix}$
- Now, the coefficient matrix A is the so called Vandermonde's matrix.

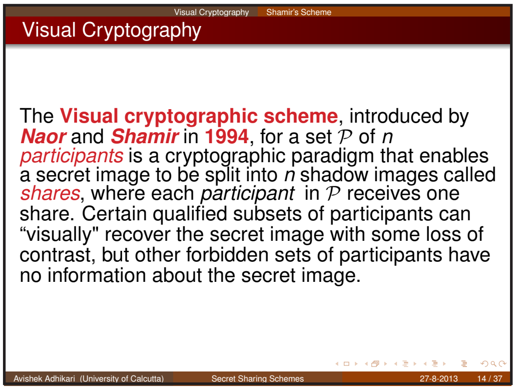
$$detA = \prod_{1 \le j < k \le t} (x_{i_k} - x_{i_j}) \mod p = (1-2)(2-3)(3-1) = 4*4*2 = 2 \neq 0$$

Thus multiplying both sides by the inverse of A, we can find the $a_0 = 1$.

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 12 / 37

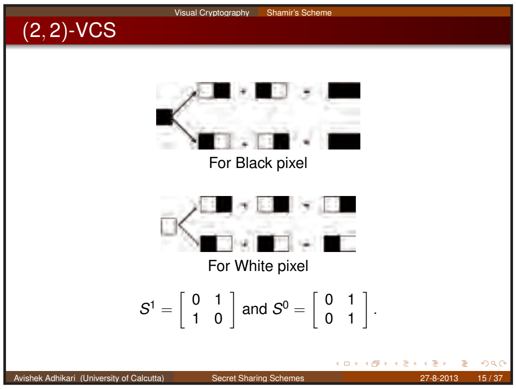


Example of $(2, 2)$-VCS



Visual Cryptography

The **Visual cryptographic scheme**, introduced by ***Naor*** and ***Shamir*** in **1994**, for a set $\mathcal{P}$ 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 $\mathcal{P}$ 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.

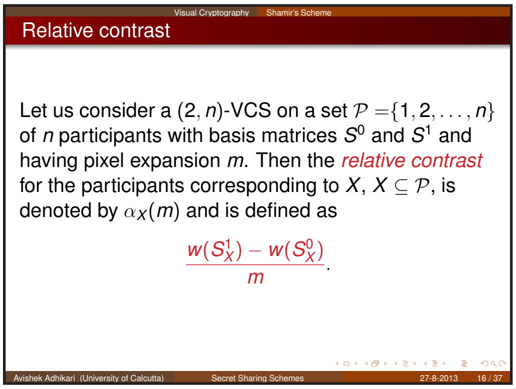


$(2, 2)$-VCS

For Black pixel

For White pixel

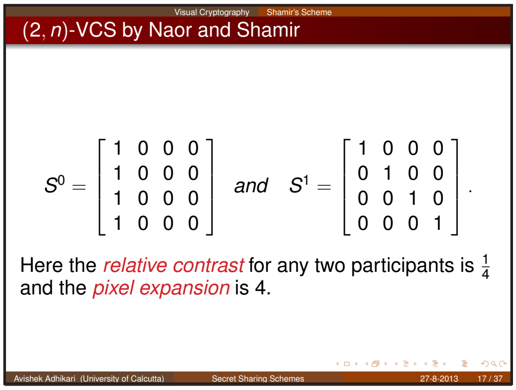
$$S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$



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

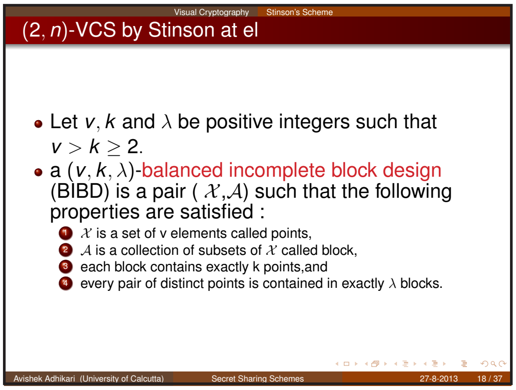
$$\frac{w(S^1_X) - w(S^0_X)}{m}.$$



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

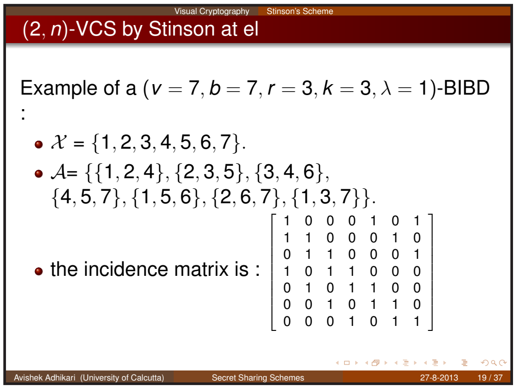
$$S^0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \textit{and} \quad S^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

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



$(2, n)$-VCS by Stinson at el

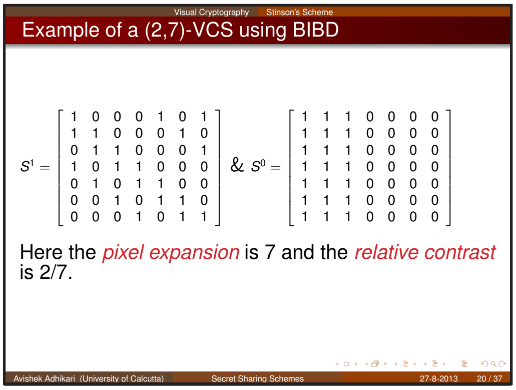
- Let v, k and λ be positive integers such that $v > k \geq 2$.
- a (v, k, λ)-balanced incomplete block design (BIBD) is a pair $(\mathcal{X}, \mathcal{A})$ such that the following properties are satisfied :
  1. $\mathcal{X}$ is a set of v elements called points,
  2. $\mathcal{A}$ is a collection of subsets of $\mathcal{X}$ called block,
  3. each block contains exactly k points,and
  4. every pair of distinct points is contained in exactly λ blocks.



$(2,n)$-VCS by Stinson at el

Example of a $(v=7, b=7, r=3, k=3, \lambda=1)$-BIBD :

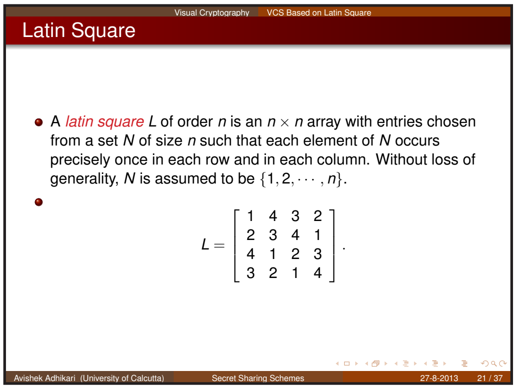
- $\mathcal{X} = \{1,2,3,4,5,6,7\}$.
- $\mathcal{A} = \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{1,5,6\},\{2,6,7\},\{1,3,7\}\}$.
- the incidence matrix is : $\begin{bmatrix} 1&0&0&0&1&0&1\\ 1&1&0&0&0&1&0\\ 0&1&1&0&0&0&1\\ 1&0&1&1&0&0&0\\ 0&1&0&1&1&0&0\\ 0&0&1&0&1&1&0\\ 0&0&0&1&0&1&1 \end{bmatrix}$



Example of a (2,7)-VCS using BIBD

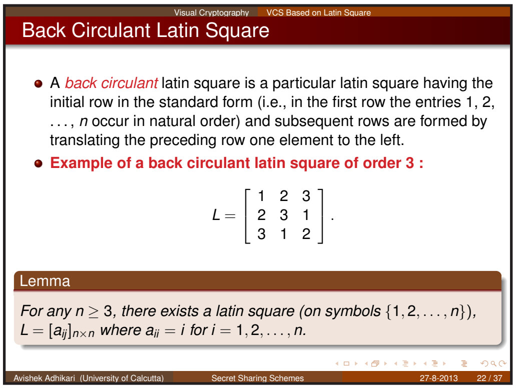
$$S^1 = \begin{bmatrix} 1&0&0&0&1&0&1\\ 1&1&0&0&0&1&0\\ 0&1&1&0&0&0&1\\ 1&0&1&1&0&0&0\\ 0&1&0&1&1&0&0\\ 0&0&1&0&1&1&0\\ 0&0&0&1&0&1&1 \end{bmatrix} \;\&\; S^0 = \begin{bmatrix} 1&1&1&0&0&0&0\\ 1&1&1&0&0&0&0\\ 1&1&1&0&0&0&0\\ 1&1&1&0&0&0&0\\ 1&1&1&0&0&0&0\\ 1&1&1&0&0&0&0\\ 1&1&1&0&0&0&0 \end{bmatrix}$$

Here the *pixel expansion* is 7 and the *relative contrast* is 2/7.



Latin Square

- A *latin square* L of order n is an $n \times n$ array with entries chosen from a set N of size n such that each element of N occurs precisely once in each row and in each column. Without loss of generality, N is assumed to be $\{1,2,\cdots,n\}$.
- $$L = \begin{bmatrix} 1&4&3&2\\ 2&3&4&1\\ 4&1&2&3\\ 3&2&1&4 \end{bmatrix}.$$



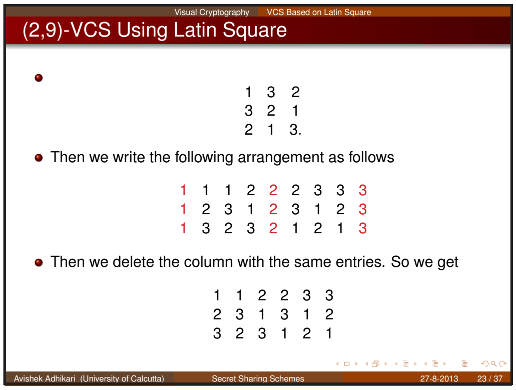
Back Circulant Latin Square

- A *back circulant* latin square is a particular latin square having the initial row in the standard form (i.e., in the first row the entries 1, 2, . . . , n occur in natural order) and subsequent rows are formed by translating the preceding row one element to the left.
- **Example of a back circulant latin square of order 3 :**

$$L = \begin{bmatrix} 1&2&3\\ 2&3&1\\ 3&1&2 \end{bmatrix}.$$

Lemma

For any $n \geq 3$, there exists a latin square (on symbols $\{1,2,\ldots,n\}$), $L = [a_{ij}]_{n\times n}$ where $a_{ii} = i$ for $i = 1,2,\ldots,n$.



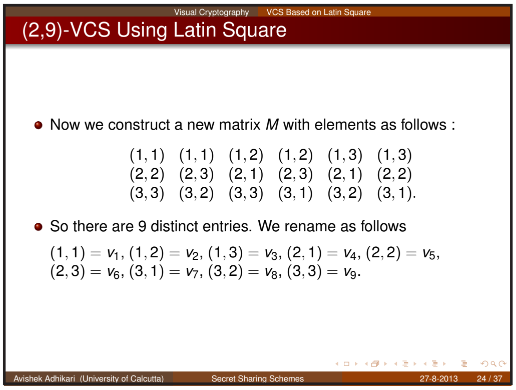
(2,9)-VCS Using Latin Square

- $$\begin{array}{ccc} 1&3&2\\ 3&2&1\\ 2&1&3. \end{array}$$
- Then we write the following arrangement as follows

$$\begin{array}{ccccccccc} 1&1&1&2&2&2&3&3&3\\ 1&2&3&1&2&3&1&2&3\\ 1&3&2&3&2&1&2&1&3 \end{array}$$

- Then we delete the column with the same entries. So we get

$$\begin{array}{cccccc} 1&1&2&2&3&3\\ 2&3&1&3&1&2\\ 3&2&3&1&2&1 \end{array}$$



(2,9)-VCS Using Latin Square

- Now we construct a new matrix M with elements as follows :

$$\begin{array}{cccccc} (1,1)&(1,1)&(1,2)&(1,2)&(1,3)&(1,3)\\ (2,2)&(2,3)&(2,1)&(2,3)&(2,1)&(2,2)\\ (3,3)&(3,2)&(3,3)&(3,1)&(3,2)&(3,1). \end{array}$$

- So there are 9 distinct entries. We rename as follows

$(1,1) = v_1$, $(1,2) = v_2$, $(1,3) = v_3$, $(2,1) = v_4$, $(2,2) = v_5$, $(2,3) = v_6$, $(3,1) = v_7$, $(3,2) = v_8$, $(3,3) = v_9$.

(2,9)-VCS Using Latin Square

- Thus the matrix becomes

$$\begin{array}{cccccc} v_1 & v_1 & v_2 & v_2 & v_3 & v_3 \\ v_5 & v_6 & v_4 & v_6 & v_4 & v_5 \\ v_9 & v_8 & v_9 & v_7 & v_8 & v_7. \end{array}$$

- $S^1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}, S^0 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$
- The pixel expansion is 6 and the relative contrast is either $\frac{2}{6}$ or $\frac{1}{6}$.

Association Scheme with 2 Classes

Given v symbols $1, 2, \ldots, v$, a relation satisfying the following conditions is said to an **association scheme with** 2 **classes** :

1. Any two symbols are either 1st or 2nd associates, the relation being symmetrical; that is, if the symbol α is the ith associate of the β, then β is the ith associate of α.
2. Each symbol α has n_i ith associates, the number n_i being independent of α.
3. If any two symbols α and β are ith associates, then the number of symbols that are jth associates of α, and kth associates of β, is independent of the pair α and β.

PBIBD

If we have an association scheme with 2 classes and given parameters, we get a **PBIBD** with 2 associate classes if the v symbols are arranged into b sets of size k ($k < v$) such that every symbol occurs at most once in a set, every symbol occurs in exactly r sets and if two symbols α and β are ith associates, then they occur together in λ_i sets, the number λ_i being independent of the particular pair of ith associates α and β, $i = 1, 2$.
The **notation** $(v, b, r, k, \lambda_1, \lambda_2)$-PBIBD will be used to denote a PBIBD. Let $N = (n_{ij})$ denote the **incidence matrix** of a $(v, b, r, k, \lambda_1, \lambda_2)$-PBIBD.

Example of a PBIBD

Let us consider a $(v = 6, b = 4, r = 2, k = 3, \lambda_1 = 0, \lambda_2 = 1)$-PBIBD. Here $\mathcal{X} = \{1, 2, 3, 4, 5, 6\}$ and $\mathcal{A} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{2, 4, 6\}, \{3, 5, 6\}\}$ The insidence matrix of this PBIBD is given as follows :

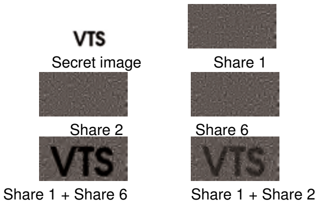
$$N = S^1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

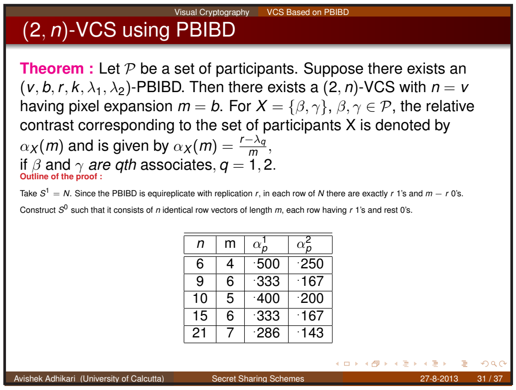
Example of a $(2, 6)$-VCS

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

Clearly, *pixel expansion* is 4 ($m = 4$) and the *relative contrast* is either $\frac{1}{2}$ or $\frac{1}{4}$.

$(2, 6)$-VCS using PBIBD





Visual Cryptography VCS Based on PBIBD

(2, n)-VCS using PBIBD

Theorem : Let $\mathcal{P}$ be a set of participants. Suppose there exists an $(v, b, r, k, \lambda_1, \lambda_2)$-PBIBD. Then there exists a $(2, n)$-VCS with $n = v$ having pixel expansion $m = b$. For $X = \{\beta, \gamma\}$, $\beta, \gamma \in \mathcal{P}$, the relative contrast corresponding to the set of participants X is denoted by $\alpha_X(m)$ and is given by $\alpha_X(m) = \frac{r-\lambda_q}{m}$,
if β and γ *are qth* associates, $q = 1, 2$.

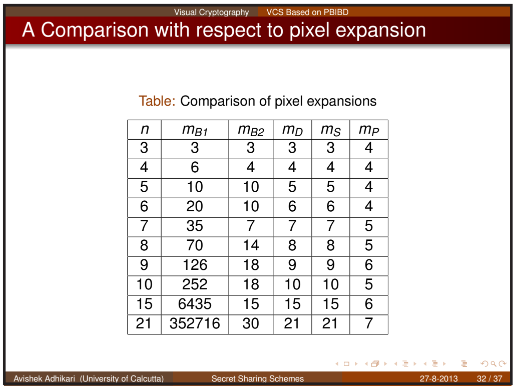
Outline of the proof :

Take $S^1 = N$. Since the PBIBD is equireplicate with replication r, in each row of N there are exactly r 1's and $m - r$ 0's.

Construct S^0 such that it consists of n identical row vectors of length m, each row having r 1's and rest 0's.

n	m	α_p^1	α_p^2
6	4	·500	·250
9	6	·333	·167
10	5	·400	·200
15	6	·333	·167
21	7	·286	·143

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 31 / 37



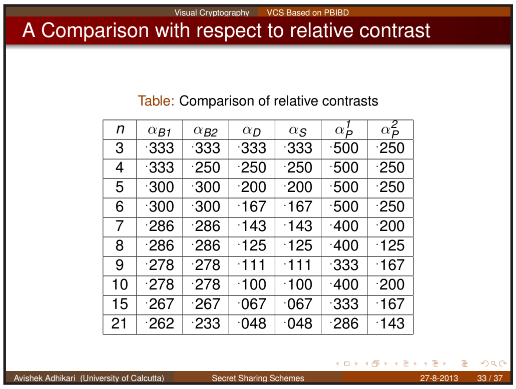
Visual Cryptography VCS Based on PBIBD

A Comparison with respect to pixel expansion

Table: Comparison of pixel expansions

n	m_{B1}	m_{B2}	m_D	m_S	m_P
3	3	3	3	3	4
4	6	4	4	4	4
5	10	10	5	5	4
6	20	10	6	6	4
7	35	7	7	7	5
8	70	14	8	8	5
9	126	18	9	9	6
10	252	18	10	10	5
15	6435	15	15	15	6
21	352716	30	21	21	7

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 32 / 37



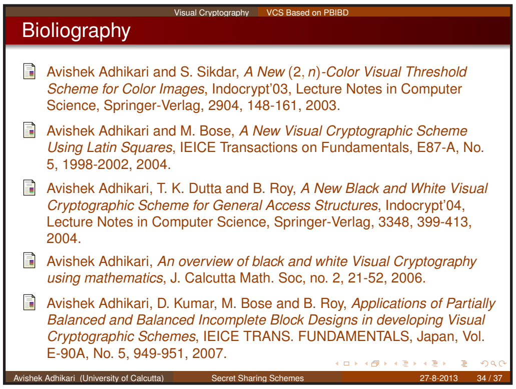
Visual Cryptography VCS Based on PBIBD

A Comparison with respect to relative contrast

Table: Comparison of relative contrasts

n	α_{B1}	α_{B2}	α_D	α_S	α_P^1	α_P^2
3	·333	·333	·333	·333	·500	·250
4	·333	·250	·250	·250	·500	·250
5	·300	·300	·200	·200	·500	·250
6	·300	·300	·167	·167	·500	·250
7	·286	·286	·143	·143	·400	·200
8	·286	·286	·125	·125	·400	·125
9	·278	·278	·111	·111	·333	·167
10	·278	·278	·100	·100	·400	·200
15	·267	·267	·067	·067	·333	·167
21	·262	·233	·048	·048	·286	·143

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 33 / 37

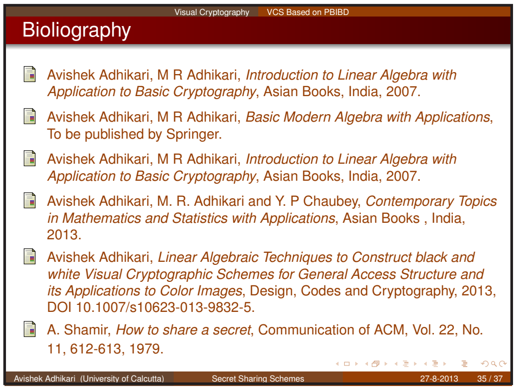


Visual Cryptography VCS Based on PBIBD

Bioliography

- 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 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*, Indocrypt'04, Lecture Notes in Computer Science, Springer-Verlag, 3348, 399-413, 2004.
- Avishek Adhikari, *An overview of black and white Visual Cryptography using mathematics*, J. Calcutta Math. Soc, no. 2, 21-52, 2006.
- Avishek Adhikari, D. Kumar, M. Bose and B. Roy, *Applications of Partially Balanced and Balanced Incomplete Block Designs in developing Visual Cryptographic Schemes*, IEICE TRANS. FUNDAMENTALS, Japan, Vol. E-90A, No. 5, 949-951, 2007.

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 34 / 37

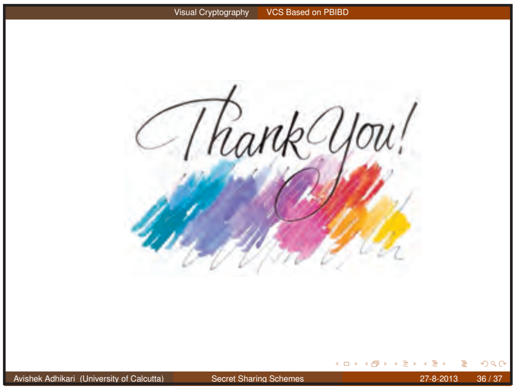


Visual Cryptography VCS Based on PBIBD

Bioliography

- 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.
- Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.
- Avishek Adhikari, M. R. Adhikari and Y. P Chaubey, *Contemporary Topics in Mathematics and Statistics with Applications*, Asian Books , India, 2013.
- 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.
- A. Shamir, *How to share a secret*, Communication of ACM, Vol. 22, No. 11, 612-613, 1979.

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 35 / 37



Visual Cryptography VCS Based on PBIBD

Avishek Adhikari (University of Calcutta) Secret Sharing Schemes 27-8-2013 36 / 37

Questions

Questions???