Secret Sharing and Visual Cryptography
Outline

- Secret Sharing
- Visual Secret Sharing
- Constructions
- Moiré Cryptography
- Issues
Secret Sharing
Secret Sharing

- **Threshold Secret Sharing** (Shamir, Blakely 1979)

- Motivation – increase confidentiality and availability

- \((k,n)\) threshold scheme
  - Threshold \(k\)
  - Group Size \(n\)

- Confidentiality vs Availability
General Secret Sharing

- $S$ – Secret to be shared
- $\mathcal{P}$ – Set of participants
- Qualified Subsets of $\mathcal{P}$ can reconstruct $S$
- Access Structure
  - Family of qualified subsets $\mathcal{A} \subseteq 2^{\mathcal{P}}$
  - Generally monotone
    - Superset of a qualified subset is also qualified

$$A \in \mathcal{A}, A \subseteq A' \subseteq \mathcal{P} \Rightarrow A' \in \mathcal{A}$$
Information Theoretically

- **Perfect Secret Sharing** scheme for S
  - Qualified Subset G
    \[ G \in A, \ H(S|G) = 0 \]
  - Unqualified Subset B
    \[ B \notin A, \ H(S|B) = H(S) \]

- **Information Rate of a scheme**
  \[ \rho = \frac{\log_2|\text{Secret}|}{\max \log_2|\text{Share}|} \]
  \[ \rho \leq 1 \]

- Measure of efficiency of the scheme
Size of Shares

- **Perfect Scheme**
  - Size of share at least size of secret
  - Larger share size
    - More memory required
    - Lower efficiency

- **Ideal Scheme**
  - Share size = secret size
  - Information rate/efficiency is high
Shamir’s Threshold Scheme

- \((k,n)\) Threshold scheme
  - \(s \in F_q\) is the secret to be shared
  - \(x_1, x_2 \ldots x_n\) are distinct non-zero elements chosen from \(F_q\)
  - Chose coefficients \(f_1, \ldots f_{k-1}\) at random from \(F_q\)
  - Let \(y = f(x) = s + \sum_{j=1}^{k-1} f_j x^j\)
  - Share \(s_i = (x_i, y_i)\)
Lagrange’s Interpolation

- Need $k$ shares for reconstruction
- Figure shows $(2,n)$ scheme
- Scheme is perfect and ideal
  - 2 shares: secret is defined
  - < 2 shares: secret can be any point on y axis

$$s = \sum_{j=1}^{k} (\prod_{1 \leq t \leq k, t \neq j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}}) y_{i_j}$$
Blakely’s Secret Sharing

- Secret is point in $m$-dimensional space
- Share corresponds to a hyper plane
- Intersection of threshold planes gives the secret
- Less than threshold planes will not intersect to the secret
Blakely’s Secret Sharing

- 2 dimensional plane
- Each share is a Line
- Intersection of 2 shares gives the secret
Non-perfect secret sharing scheme

- Motivation

- Semi-qualified subsets
  - Partial Information about Secret
  - Size of shares < Size of secret

- $(d,k,n)$ ramp scheme [Blakely, Medows Crypto 84]
  - Qualified subset $A$, $|A| \geq k$
    - $H(S|A)=0$
  - Unqualified subset $U$, $|U| \leq k-d$
    - $H(S|U)=H(S)$
  - Semi Qualified subset $P$, $k-d<|P|<k$
    - $0<H(S|P)<H(S)$
Making Shamir’s scheme non-perfect

- Instead of one secret have a vector of secrets
- Each share is also a vector
- Each share reduces by the dimension of the secret space by 1
- Linear gain of information as you compromise more shares
Applications of Secret Sharing

- Secure and Efficient Metering [Naor and Pinkas, Eurocrypt 1998]

Diagram:
- Audit Agency
- Client Machines
- Proof of $k$ visits
- Reconstruct secret
- Shares
Applications of Secret Sharing

- Threshold Signature Sharing
  - Signing key with a single entity can be abused
  - Distribute the power to sign a document

- RSA Signatures
  - A Simplified Approach to Threshold and Proactive RSA [Rabin, CRYPTO 98]
    - Signing key shared at all times using additive method
Basic Method of Signature Sharing

- **Signing Key**: `d`
- **Shares of key**: `d = d1 + d2 + d3`
- **Partial Signature**: `M^{d1} mod n`, `M^{d2} mod n`, `M^{d3} mod n`
- **Final Signature**: `M^d mod n = \prod_{i=1}^{3} M^{d_i} mod n`
Visual Secret Sharing
Visual Secret Sharing

- Naor and Shamir [1994]

Bob faxes secret message

No computer needed but other printer constraints involved
Visual Secret Sharing

- Encode secret image $S$ in threshold shadow images (shares).
- Shares are represented on transparencies
- Secret is reconstructed visually
- $(k,n)$ visual threshold scheme
  - $k$ of the shares (transparencies) are superimposed reveal secret
  - $<k$ shares do not reveal any information
Constructing a Threshold Scheme

- Consider (2,2) regular threshold scheme
  - Secret $K = s_1 \text{xor} s_2$
  - $s_1, s_2$ take values (0,1)
    - $0 \text{xor} 0 = 0, 1 \text{xor} 1 = 0$
    - $0 \text{xor} 1 = 1, 1 \text{xor} 0 = 1$
  - Neither $s_1$ nor $s_2$ reveal any information about $K$
Constructing a Visual Threshold Scheme

- Associate black pixel with binary digit 1
- Associate white pixel with binary digit 0
  - 0 on 0 = 0 (good)
  - 0 on 1 = 1 (good)
  - 1 on 0 = 1 (good)
  - 1 on 1 = 1 (oops!)
- Visual system performs Boolean OR instead of XOR
Naor and Shamir Constructions

- **Basic Idea**
  - Replace a pixel with $m > 1$ subpixels in each share
  - Gray level of superimposed pixels decides the color (black or white)
- Less than threshold shares do not convey any information about a pixel in final image
Naor and Shamir Construction (2,2) Scheme

<table>
<thead>
<tr>
<th>pixel</th>
<th>share #1</th>
<th>share #2</th>
<th>superposition of the two shares</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$p = .5$</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$p = .5$</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$p = .5$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$p = .5$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$p = .5$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$p = .5$</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note the difference in gray levels of white and black pixels
Example

- (2,2) Threshold Scheme – Mona Lisa image
- This is like a one time pad scheme
- Original Picture

- Superimposed picture has 50% loss in contrast
Further Naor Shamir Constructions

- Will be considering
  - $(3,n)$
  - $(k,k)$
  - $(k,n)$

- Each has a different properties in terms of pixel expansion and contrast
Preliminary Notation

- $n \rightarrow$ Group Size
- $k \rightarrow$ Threshold
- $m \rightarrow$ Pixel Expansion
- $\alpha \rightarrow$ Relative Contrast
- $C_0 \rightarrow$ Collection of $n \times m$ boolean matrices for shares of White pixel
- $C_1 \rightarrow$ Collection of $n \times m$ boolean matrices for shares of Black pixel
- $V \rightarrow$ OR'ed $k$ rows
- $H(V) \rightarrow$ Hamming weight of $V$
- $d \rightarrow$ number in $[1,m]$
- $r \rightarrow$ Size of collections $C_0$ and $C_1$
Properties of \((k,n)\) scheme

- **Contrast**
  - For \(S\) in \(C_0\) (WHITE): \(H(V) \leq d - \alpha m\)
  - For \(S\) in \(C_1\) (BLACK): \(H(V) \geq d\)

- **Security**
  - The two collections of \(q \times m\) \((l \leq q < k\) matrices, formed by restricting \(n \times m\) matrices in \(C_0\) and \(C_1\) to any \(q\) rows, are indistinguishable

- **Their constructions are uniform**
  - There is a function \(f\) such that the for any matrix in \(C_0\) or \(C_1\) the hamming weight of OR’ed \(q\) rows is \(f(q)\)
Constructing a \((3,n)\), \(n \geq 3\) scheme

- \(m=2n-2\)
- \(\alpha=1/2n-2\)
- \(B\) is a \(n \times (n-2)\) matrix containing 1’s
- \(I\) is a \(n \times n\) identity matrix
- \(BI\) is a \(n \times (2n-2)\) concatenated matrix
- \(c(BI)\) is the complement of \(BI\)
- \(C_0\) contains matrices obtained by permuting columns of \(c(BI)\)
- \(C_1\) contains matrices obtained by permuting columns of \(BI\)
$m=4, \ \alpha = 1/4, \ (3,3)$ Scheme Example

\[
\begin{align*}
B & := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
I & := \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \\
BI & := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \\
c(BI) & := \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}
\end{align*}
\]

- Say permutation is \{2,3,4,1\}
- Shares
  - White Pixel
  - Black Pixel
Contrast for \((3,3)\) \(m=4\), \(\alpha=1/4\)

- **White**
  - Share 1
  - Share 2
  - Share 3
  - Superimposed

- **Black**
  - Share 1
  - Share 2
  - Share 3
  - Superimposed

Can also be seen by Hamming weight:

- **Black** \(H(V) = 4\)
  - \[
  \begin{pmatrix}
  1 & 1 & 0 & 0 \\
  1 & 0 & 1 & 0 \\
  1 & 0 & 0 & 1 \\
  \end{pmatrix}
  \]

- **White** \(H(V) = 3\)
  - \[
  \begin{pmatrix}
  0 & 0 & 1 & 1 \\
  0 & 1 & 0 & 1 \\
  0 & 1 & 1 & 0 \\
  \end{pmatrix}
  \]
Security for (3,3) Scheme

- Security
  - Superimposing < 3 shares does not reveal if secret pixel is white or black
  - Hamming weight of 2 superimposed shares is always 3

![Share1 White](image1)
![Share2 White](image2)
![Superimposed White](image3)

![Share1 Black](image4)
![Share2 Black](image5)
![Superimposed Black](image6)
Constructing 

\( \frac{1}{2^{k-1}} \), \( \alpha = \frac{1}{2^{k-1}} \)

Base Set \( W = \{e_1 \ldots e_k\} \)

Even cardinality subsets \( \pi_1 \ldots \pi_{2^{k-1}} \)

Odd cardinality subsets \( \sigma_1 \ldots \sigma_{2^{k-1}} \)

\( k \times 2^{k-1} \) matrix \( S^0, S^1 \)

\( S^0[i, j] = 1, \text{ if } e_i \in \pi_j \)

\( S^1[i, j] = 1 \text{ if } e_i \in \sigma_j \)
Example $m=8 \alpha=1/8, (4,4)$

- $W = \{1,2,3,4\}$
- Even cardinality subsets
  - $\{\emptyset,\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3,4\}\}$
- Odd cardinality subsets
  - $\{\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$
- Contrast
  - $H(V)$ for $S_0 = 7$
  - $H(V)$ for $S_1 = 8$
- Security
  - Restrict to $q<4$ rows (Say $q=3$)
  - The $3 \times 8$ collections of matrices will be indistinguishable

<table>
<thead>
<tr>
<th>$S_0$</th>
<th>$S_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>\begin{pmatrix} 0 &amp; 1 &amp; 1 &amp; 1 &amp; 0 &amp; 0 &amp; 0 &amp; 1 \ 0 &amp; 1 &amp; 0 &amp; 0 &amp; 1 &amp; 1 &amp; 0 &amp; 1 \ 0 &amp; 0 &amp; 1 &amp; 0 &amp; 1 &amp; 0 &amp; 1 &amp; 1 \ 0 &amp; 0 &amp; 0 &amp; 1 &amp; 0 &amp; 1 &amp; 1 &amp; 1 \end{pmatrix}</td>
<td>\begin{pmatrix} 1 &amp; 0 &amp; 0 &amp; 0 &amp; 1 &amp; 1 &amp; 1 &amp; 0 \ 0 &amp; 1 &amp; 0 &amp; 0 &amp; 1 &amp; 1 &amp; 0 &amp; 1 \ 0 &amp; 0 &amp; 1 &amp; 0 &amp; 1 &amp; 0 &amp; 1 &amp; 1 \ 0 &amp; 0 &amp; 0 &amp; 1 &amp; 0 &amp; 1 &amp; 1 &amp; 1 \end{pmatrix}</td>
</tr>
</tbody>
</table>
Moving to \((k,n)\) scheme

- **C** is \((k,k)\) scheme
  - Parameters \(m, r, \alpha\)
  - \(C_0 = T_1^0, T_2^0, \ldots T_r^0\)
  - \(C_1 = T_1^1, T_2^1, \ldots T_r^1\)

- **\(H\)** is collection of \(l\) functions
  \[
  \forall h \in H, h : \{1 \ldots n\} \rightarrow \{1 \ldots k\}
  \]

- **\(B\)** subset of \(\{1..n\}\) of size \(k\)

- \(\beta_q\) is probability that randomly chosen function \(h \in H\) yields \(q\) different values on \(B\), \(l \leq q \leq k\)
(k, n) scheme

- $m' = ml$, $\alpha' \geq \beta_k \alpha$, $r' = r^l$
- Each $S^b_t, 1 \leq t \leq r^l, b \in \{0, 1\}$
  - Indexed by $t = (t_1, \ldots, t_u \ldots t_l), 1 \leq t_i \leq r$
  - $S^b_t[i, (j, u)] = T^b_{tu}[h(i), j]$
  - $1 \leq i \leq n$
  - $1 \leq u \leq l$
  - $1 \leq j \leq m$
  - $1 \leq h(i) \leq k$
Contrast \( \geq \beta_k \alpha \)

- \( k \) rows is \( S_t^b \) mapped to \( q < k \) different values by \( h \)
- Hamming weight of OR of \( q \) rows is \( f(q) \)
- Difference \( \alpha m \) white and black pixels occurs when \( h \) is one to one and happens at \( \beta_k \)

**WHITE:**
\[
H(V) \leq l(\beta_k (d - \alpha m) + \sum_{q=1}^{k-1} \beta_q \cdot f(q))
\]

**BLACK:**
\[
H(V) \geq l(\beta_k d + \sum_{q=1}^{k-1} \beta_q \cdot f(q))
\]
Security

- You are using \((k,k)\) scheme to create \((k,n)\) scheme
- Security properties of the \((k,k)\) scheme implies the security of \((k,n)\) scheme
- Expected Hamming weight of OR of \(q\) rows, \(q<k\) is \(l \sum_{q=1}^{k-1} \beta_q f(q)\) irrespective of WHITE or BLACK pixel

- **Goal:**
  - Create a scheme such that qualified combinations of participants can reconstruct secret
  - Unqualified combinations of participants gain no information about the secret

- For a \((2,n)\) scheme access structure can be represented as Graph
  - Share \(s_i\) and \(s_j\) reveal secret image if \(ij\) is edge in Graph
Example (2,4) scheme

- Qualified Subsets \{\{1,2\},\{2,3\},\{3,4\}\}
- Forbidden Subsets \{\{1,3\},\{1,4\},\{2,4\}\}
- Matrices for the scheme
- Some Shares Darker

\[
S_0 = \begin{pmatrix}
1 & 0 & 0 \\
1 & 1 & 0 \\
1 & 1 & 0 \\
0 & 1 & 0
\end{pmatrix} \quad S_1 = \begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & 1 \\
1 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
\]
Example

- Original Image

- Is superset of qualified subset also qualified?
Problem with various schemes

- The shares in the schemes are random transparencies
- A person carrying around these shares is obviously suspicious
- Need to hide the share in innocent looking images
Related works with Natural Images

- M. Nakajima. Y. Yamaguchi.
  - *Extended Visual Cryptography for natural Images* [2002]

- Y. Desmedt and Van. Le.
  - *Moire Cryptography*. [CCS 2000]
Moiré Cryptography
Moiré effect

- Interference of two or more regular structures with different frequencies
- High frequency lattices combined produce a low frequency pattern
Moiré Cryptography
[Demedt, Van Le (2000)]

- Use steganography to create secret sharing schemes
- Shares are realistic images
- Utilize moiré patterns to create the images
Moiré Cryptography process

- Randomize Embedded Picture into pre-shares
- Hide the pre-shares in cover picture
- Note the cryptography lies in X
Moiré Effect …

- For 0 bit
  - Superimposed shares whose dots are oriented at same angle

- For 1 bit
  - Superimposed shares where dots are oriented with different angles

- Moire pattern forms the embedded picture and not gray level of shares as in visual cryptography

- Superimposing shares results
  - Two moire patterns with different textures
  - Since textures are visually different we see picture
Example

- FSU Moiré Example
- Robustness against misplacement or orientation
Comparison and Issues
Visual Schemes Seen So Far

- Perfect secrecy 😊
- No expensive computer operations 😊
- Size of shares large 😞
  - If secret contains $p$ pixels share contains $pm$ pixels
  - Cannot have ideal visual scheme
- Superimposed secret - loss in contrast 😞
- Tedious 😞
Honest Dealer Issue

- Honest dealer assumed
- Verifiable Secret Sharing schemes tolerate a faulty dealer
  - Security is computational
Verifiable Secret Sharing for Shamir’s scheme [Feldman87] (2,3) VSS scheme

$g^s, g^{f_1}$

Dealers

Participants

$S_1$

$S_2$

$S_3$

$g$ is the generator of a group

$y = f(x) = s + \sum_{j=1}^{k-1} f_j x^j$

$s_i = (x_i, y_i)$

$gy_i = g^s (g^{f_1}) x_i$

Can visual VSS schemes be created?
Dynamic Groups

- Old share holder leaves
- New share holder joins
- Threshold changes
- Need to refresh the sharing \((k,n)\) to \((k’,n’)\)
- Is there any way to do that visually without requiring an online dealer?
Related Works

- Proactive Secret Sharing and public key cryptosystems [Jarecki, 1995]
- Verifiable Secret Redistribution for threshold sharing schemes [Wong et. al. 2002]
- Asynchronous verifiable secret sharing and proactive cryptosystems [Cachin et. al CCS 2002]
Questions?
Visual Cryptography: Hadamard BIBDs

- Constructions for optimal contrast and minimal pixel expansion [Blundo et. al. ’98]
- $(v,p,\lambda)$- Balanced Incomplete Block Design (BIBD)
  - Pair $(X,A)$
  - $X$ is set of $v$ elements called points
  - $A$ is collection of subsets of $X$ called blocks
  - Each block has $p$ points
  - Every pair of distinct points is contained in $\lambda$ blocks
Hadamard Matrices

- $n \times n$ matrix $H$
- Every entry is $\pm 1$ and $HH^T = nI_n$
- Example Hadamard Matrix of order 4

\[
\begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix}
\]
Hadamard and BIBD equivalence

- \((4t-1, 2t-1, t-1)\)–BIBD exists if and only if Hadamard matrix of order \(4t\) exists

- Blundo \textit{et. al.} show
  - if \(n \equiv 3 \mod 4\), there exists a \((2, n)\) visual scheme with optimal \(\alpha\) and optimal \(m\) if and only if Hadamard matrix of order \(n+1\) exists
Construction \((2,n) \ (n \equiv 3 \mod 4)\)

- **Blocks**
  - \(A_0 = \{i^2 \mod n: 1 \leq i \leq (n-1)/2\}\)
  - \(A_i = A_0 + i \mod n, \ 1 \leq i \leq n-1\)

- **Points** \(Z_n\)

- **Point Block Incidence matrix** \(M\)
  - Rows indexed by points and columns indexed by Blocks
  - \(M[i,j] = 1 \text{ if } i \in A_j\)

- \(M\) is the basis matrix \(S^l\)
Construction \((2,11)\)

- \(m=11, \alpha = 3/11\)
- Basis matrix \(S^1\)
- Basis matrix \(S^0\)
  - Each row is \((1111000000)\)
- Contrast
  - Black \(H(V) = 8\)
  - White \(H(V) = 5\)
- Security
  - \(1\times11\) matrix collections are indistinguishable

\[
S^1 = \begin{pmatrix}
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & & \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}
\]
\[ m = 2^k, \alpha = 1/2^k \ (k,k) \text{ scheme} \]

- Two lists of vectors each of length \( k \) over \( \text{GF}[2] \)
  - \( J_1^0 \ldots J_k^0 \)
    - \( k-1 \) linearly independent, \( k \) are not independent
    - \( J_i^0 = 0^{i-1}10^{k-i}, 1 \leq i \leq k, J_k^0 = 1^{k-1}0 \)
  - \( J_1^1 \ldots J_k^1 \)
    - Linearly independent

- \( S^t[i, x] \equiv < J_i^t, x >, t \in \{0, 1\} \)
  - Indexing the columns of \( S \) with a vector \( x \) of length \( k \) over \( \text{GF}[2] \)
Example \( m=8, \alpha =1/8, (3,3) \) scheme

- \( J_1^0 = [1 \ 0 \ 0], J_2^0 = [0 \ 1 \ 0], J_3^0 = [1 \ 1 \ 0] \)
- \( J_1^1 = [1 \ 0 \ 0], J_2^1 = [0 \ 1 \ 0], J_3^1 = [0 \ 0 \ 1] \)
- \( x = [0 \ 0 \ 0], \ldots [1 \ 1 \ 1] \)
- \( S^0 \left( \begin{array}{ccccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ \end{array} \right) [1 \ 0 \ 0] \left( \begin{array}{c} 0 \\ 1 \\ 1 \\ \end{array} \right) = 0 \)