

(Visual) Secret Sharing

Alexander Klink

klink@mathematik.tu-darmstadt.de

27. May 2003

What is secret ...
Why secret ...
“Hardware” ...
Mathematical ...
Visual secret ...
References



(Visual) Secret Sharing

What is secret sharing?
Why secret sharing?
“Hardware” secret sharing
Mathematical secret sharing
Visual secret sharing
References

What is secret ...
Why secret ...
“Hardware” ...
Mathematical ...
Visual secret ...
References



What is secret sharing?

What is secret ...

Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References

Definition (secret sharing scheme):

Let's assume we have some secret data S .

A (n, k) *threshold secret sharing scheme* achieves the following:

- The secret is split into n parts S_n which are distributed to the participants of the scheme
- Knowing at least k secret shares, one can easily recover the secret
- The knowledge of $k - 1$ or less secret shares does not reveal the secret



Definition (perfect secret sharing):

We call a secret sharing scheme *perfect*, if it satisfies the following additional property:

- Knowing $k - 1$ or less secret shares does not give *any* information on the secret S .

This actually means that all possible values for the secret are equally likely if you know only $k - 1$ shares.

[What is secret ...](#)

[Why secret ...](#)

[“Hardware” ...](#)

[Mathematical ...](#)

[Visual secret ...](#)

[References](#)



Why secret sharing?

So why would one want to do secret sharing?
Some possible applications are:

- key escrow in public key cryptosystems
- revocable anonymity in electronic money
- authorization for critical operations, i.e. missile launches, etc.

[What is secret ...](#)

[Why secret ...](#)

[“Hardware” ...](#)

[Mathematical ...](#)

[Visual secret ...](#)

[References](#)



“Hardware” secret sharing

- can be implemented using locks
- too complex to be usable
- $(11, 6)$ sharing needs 462 locks and 252 keys per person

[What is secret ...](#)

[Why secret ...](#)

[“Hardware” ...](#)

[Mathematical ...](#)

[Visual secret ...](#)

[References](#)



Mathematical secret sharing

Sharing a bit among two persons Using Polynomials (Shamir 79)

Secret sharing schemes were independently invented by both Adi Shamir and George Blakley in 1979.

What is secret ...

Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References



Sharing a bit among two persons

- XOR the secret S with a random bit R .
- $S_1 = S \oplus R$
- $S_2 = R$
- $S = S_1 \oplus S_2$, as
- $R \oplus R = 0 \in \mathbb{Z}_2$
- can also be used to share bitstrings
- perfect secret sharing scheme

What is secret ...

Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References



Using Polynomials (Shamir 79)

What is secret ...

Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References

(n, k) threshold secret sharing using polynomials:

- Take a random polynomial $p \in \mathbf{Z}_q[x]$ of degree $k - 1$ with $p(0) = S$.
(q prime $> n$)
- Distribute $S_i = (i, p(i) \bmod q)$, $i = 1, \dots, n$ to the participants.
- k participants can interpolate p and thus easily compute $S = p(0)$.



Remark: This secret sharing scheme is perfect. The value of $p(0)$ is equally likely – there are the same number of polynomials which pass through $k - 1$ points and $(0, y)$ for each $y \in \mathbf{Z}_q$

Drawback: open to cheating

- Problem: evil Mallory does not tell his real point, but invents one. So only he gets to know all points and can reconstruct the secret.
- Solution: (publicly) verifiable secret sharing schemes

[What is secret ...](#)

[Why secret ...](#)

[“Hardware” ...](#)

[Mathematical ...](#)

[Visual secret ...](#)

[References](#)



Visual secret sharing

Definition

2 out of 2

Naor/Shamir scheme

2 out of n

n out of n

k out of n

Advanced techniques

What is secret ...

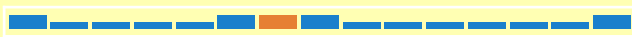
Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References



Definition

- uses mathematical secret sharing but implements in hardware:
- printed on transparencies
- + once created, it requires no technology
- – resolution and contrast is lost

[What is secret ...](#)

[Why secret ...](#)

[“Hardware” ...](#)

[Mathematical ...](#)

[Visual secret ...](#)

[References](#)



- Problem: XOR is impossible using transparencies (black on black stays black)
- Solution: split pixel into two halves
- actually a graphical “one time pad”

[What is secret ...](#)

[Why secret ...](#)

[“Hardware” ...](#)

[Mathematical ...](#)

[Visual secret ...](#)

[References](#)



What is secret ...

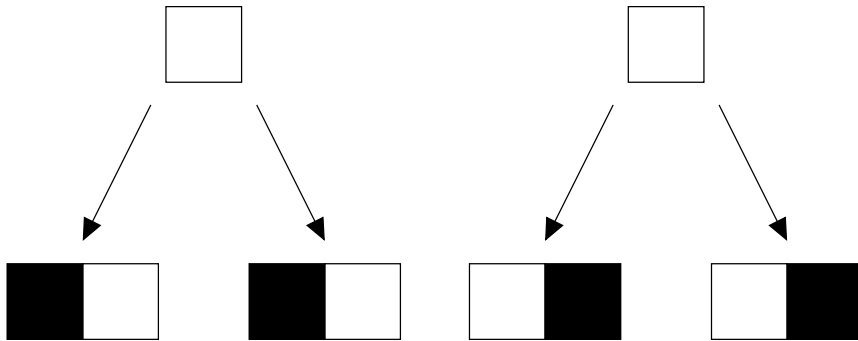
Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References



Sharing a white pixel



What is secret ...

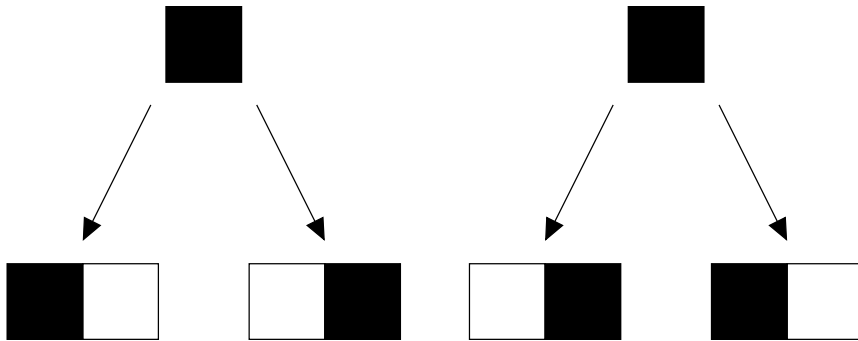
Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References



Sharing a black pixel



Naor/Shamir scheme

- invented in 1994
- n : number of shares
- k : threshold to be able to see the secret
- m : number of subpixels
- C_0, C_1 : collection of $n \times m$ Boolean matrices
- (C_0/C_1) : white/black pixel shares

What is secret ...

Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References



- **Example:** (2,2) scheme (as seen before):

- $C_0 = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$

- $C_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$

- deleting one row from entries: $C_0 = C_1$

2 out of n

- $S_0 = \left\{ \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ & & \vdots & & \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} \right\}$

- $S_1 = \left\{ \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ & & \vdots & & \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \right\}$

- $C_0 =$ all column permutations of S_0

- $C_1 =$ all column permutations of S_1

[What is secret ...](#)

[Why secret ...](#)

[“Hardware” ...](#)

[Mathematical ...](#)

[Visual secret ...](#)

[References](#)



Definition (Hamming weight): The hamming weight $h(v)$ of a vector $v \in \mathbf{Z}_2^n$ is the number of ones in the vector.

- all vectors with even hamming weight:
columns of $S_0 \in M(\mathbf{Z}_2, n \times 2^{n-1})$
- all vectors with odd hamming weight:
columns of $S_1 \in M(\mathbf{Z}_2, n \times 2^{n-1})$
- C_0, C_1 : again all column permutations of S_0, S_1 .



What is secret ...

Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References

Example ($n = 3$):

- $S_0 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$

- $S_1 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$



What is secret ...

Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References

Security:

- take $k - 1$ rows from S_0 or S_1

- the columns are exactly $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ to $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$

- i.e. subpixel shares are the same



k out of n

- uses hash functions

$$h : \{1, \dots, n\} \rightarrow \{1, \dots, k\}$$

- complex construction

[What is secret ...](#)

[Why secret ...](#)

[“Hardware” ...](#)

[Mathematical ...](#)

[Visual secret ...](#)

[References](#)



Advanced techniques

- contrast enhancement techniques
- greyscale/color (already made to work)
- steganography

[What is secret ...](#)

[Why secret ...](#)

[“Hardware” ...](#)

[Mathematical ...](#)

[Visual secret ...](#)

[References](#)



References

- *How to share a secret*, Adi Shamir, <http://szabo.best.vwh.net/secret.html>
- *Visual Cryptography*, Moni Naor & Adi Shamir, <ftp://ftp.wisdom.weizmann.ac.il:/pub/CSreports/reps94/94-14.ps.Z>

What is secret ...

Why secret ...

“Hardware” ...

Mathematical ...

Visual secret ...

References

