ICSI-526/426
Cryptography

Shamir's Secret Sharing and Homomorphism

Pradeep Atrey
University at Albany – SUNY

Secret Sharing

- In cryptography, **secret sharing** refers to a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret.

- The secret can only be reconstructed when the shares are combined; individual shares are of no use on their own.

Threshold Secret Sharing

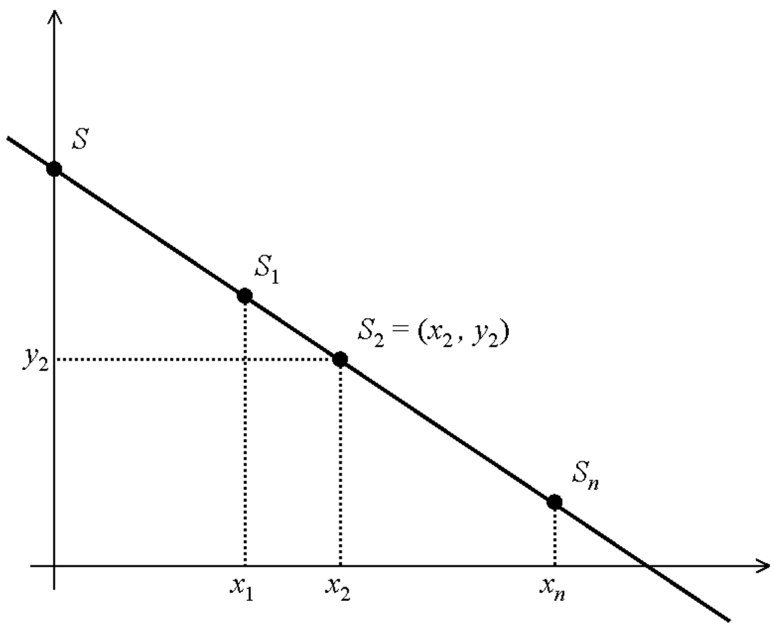
- Let k,n be positive integers, $k \le n$. A (k,n) **threshold scheme** allows to divide a confidential message into n shares and requires the knowledge of at least k out of n shares to reconstruct the original content.

- Shamir's secret sharing scheme was introduced in 1979.

His method is based on a well-known fact: a polynomial of degree k-1 is uniquely determined by any k points on it.

Degree-1 Polynomial

- Graphic-representation of a degree-1 polynomial and its shares.



Polynomials with Varying Degrees

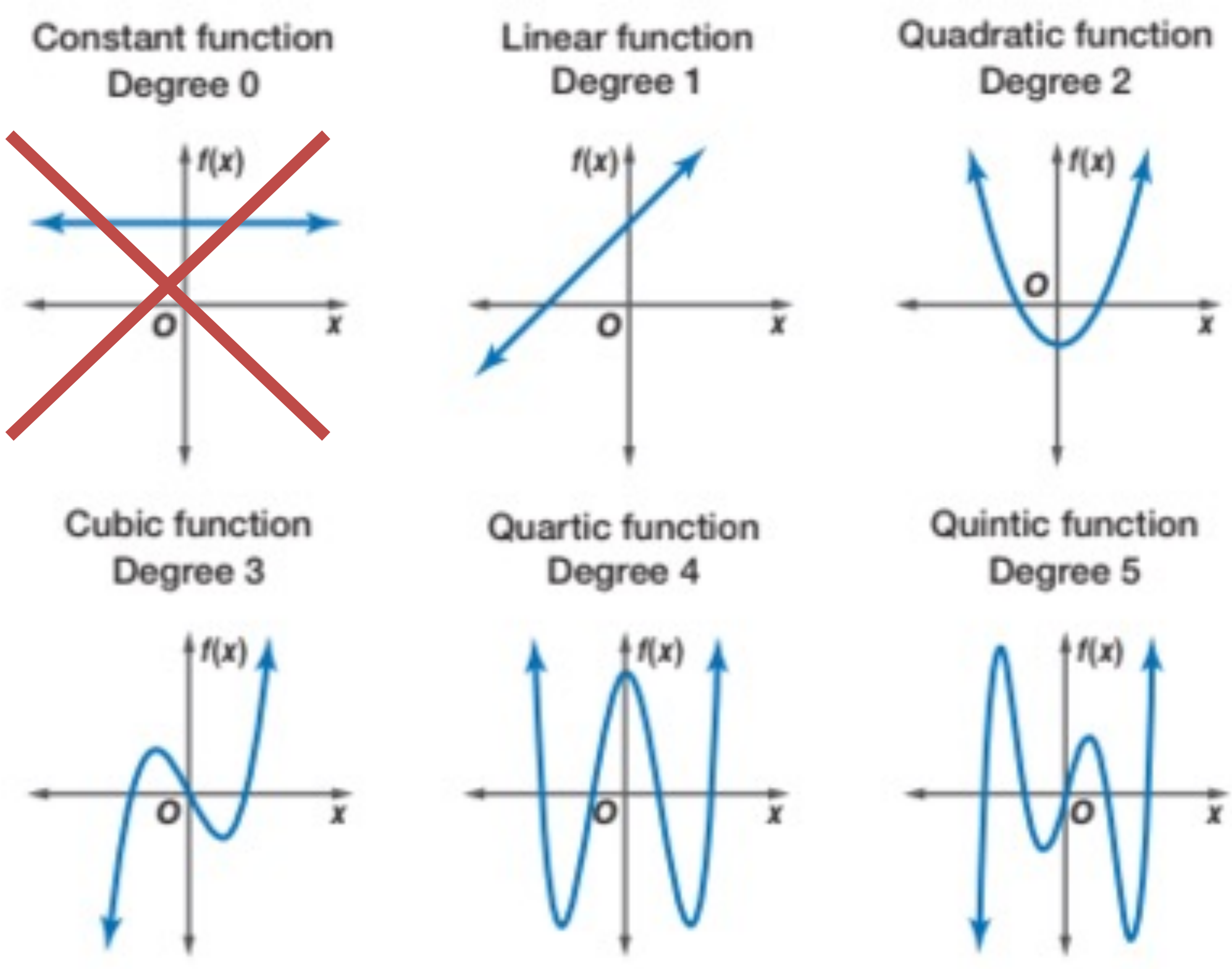
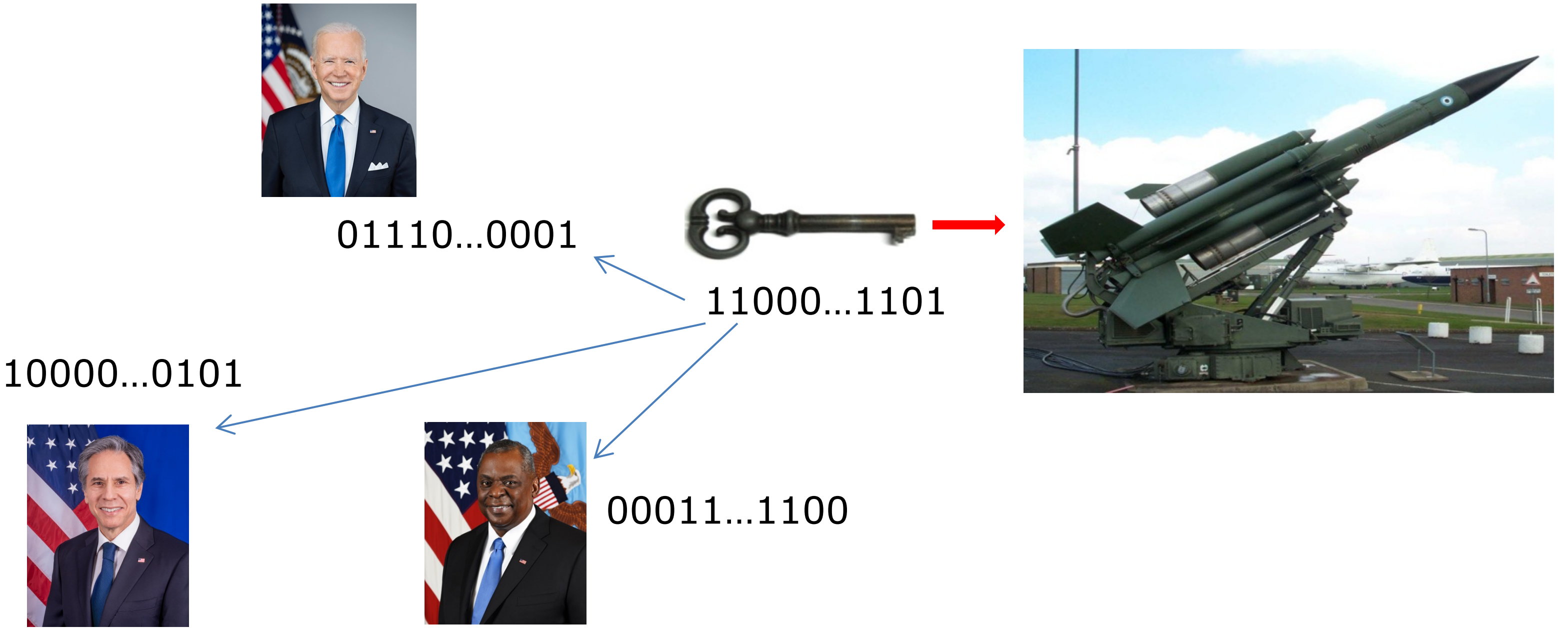


Image source: https://en.wikiversity.org/wiki/Algebra_II/Polynomial_Functions

Shamir's Secret Sharing



<u>Sharing a Secret</u>

$$F(x) = \left(S + \sum_{i=1}^{k-1} a_i x^i\right) \bmod q$$

Secret

Random Number

Shamir’s Secret Sharing

01110…0001

11000…1101

10000…0101

00011…1100

Trash

Shamir's Secret Sharing

01110…0001

10000…0101

00011…1100

Reconstructing a Secret

Lagrange Interpolation Formula

$(x_1, y_1), \ldots, (x_n, y_n)$ points with different x coordinates, then

$$F(x) = \sum_{i=1}^{n} y_i \prod_{i=j} \frac{(x - x_j)}{(x_i - x_j)} \quad mod\ q$$

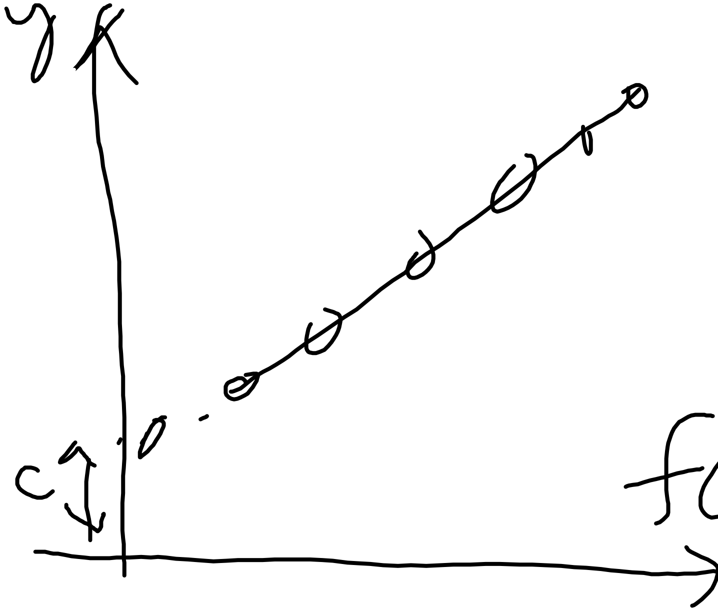
is only one polynomial of degree $n-1$ that passes through all

$$y = mx + c \mod p$$

$$y = c + mx$$

$$= a_0 + a_1 x$$

$$p = 11$$



$$f(x) = y = 10 + 3x \mod 11$$

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$$

(x_1, y_1)

(x_2, y_2)

$x = 1 \rightarrow$ $f(1) = 10 + 3.1 \mod 11$

$= 2$

$x = 3$ $f(3) = 10 + 3\,3 \mod 11$

$= 8$

$x = 11$ $f(11) = 10 + 3.11 \mod 11$

$\Rightarrow$ $= 10$

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

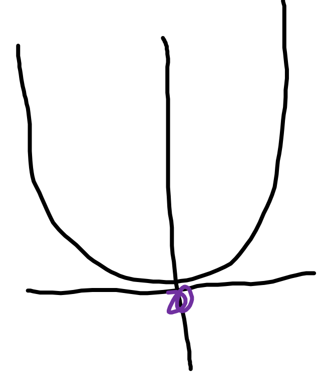
polynomial of deg $k-1$ mod p

we need <u>k points</u> to reconstruct the polynomial secret

$x = 0$ $\quad f(0)$

$$f(x) = a_0 + a_1 x + a_2 x^2 \bmod p$$

$$f(x) = \cancel{8} + 3x + 2x^2 \bmod 11$$



$$f(1) = 8 + 3 \cdot 1 + 2 x^2 \bmod 11 = 2$$

$$f(2) = 8 + 3 \cdot 2 + 2 \cdot 2^2 \bmod 11 = 0$$

$$f(5) = 8 + 3 \cdot 5 + 2 \cdot 5^2 \bmod 11 = 7$$

$$f(10) = 8 + 3 \cdot 10 + 2 \cdot 10^2 \bmod 11 = \cancel{6}\ 7$$

$p = 11$

$a_0 = 5 = \cancel{8}$

$a_1 = 3$

$a_2 = 2$

$(1, f(1)) = (1, 2) \rightarrow U1$

$(2, f(2)) = (2, 0) \rightarrow U2$

$(5, f(5)) = (5, 7) \rightarrow U3$

$(10, f(10)) = (10, \cancel{6}\ 7) \rightarrow U4$

238 m 11

~~$x_1, y_1 \quad x_2, y_2 \quad x_3, y_3 \quad x_4, y_4$~~

$(1, 2) \quad (2, 0) \quad (5, 7) \quad (10, 6)$

$x_1, y_1 \qquad x_2, y_2 \qquad x_3, y_3$

$$f(x) = \left[y_1 \times \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)} + y_2 \times \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)} + y_3 \times \frac{(x - x_2)(x - x_1)}{(x_3 - x_2)(x_3 - x_1)} \right] \bmod p$$

$y =$

$$= \left[2 \times \frac{(x-5)(x-10)}{(1-5)(1-10)} + 7 \times \frac{(x-1)(x-10)}{(5-1)(5-10)} + \cancel{6}\,7 \times \frac{(x-5)(x-1)}{(10-5)(10-1)} \right] \bmod 11$$

$$= 2 \times \frac{\cancel{x^2} - 15\cancel{x} + 50}{(-4)(-9)} + 7 \times \frac{\cancel{x^2} - 11\cancel{x} + 10}{(4)(-5)} + \cancel{6}\,7 \times \frac{\cancel{x^2} - 6\cancel{x} + 5}{(5)(9)} \bmod 11$$

$$f(0) = \frac{2\times 5015}{3618\,9} + \frac{7\times 10}{-20} + \frac{\cancel{8}\,7 \times 5}{45\,9\,3} \bmod 11$$

$$= \frac{25}{9} - \frac{7}{2} + \frac{\cancel{2}\,7}{9} \bmod 11$$

$$= \left(\underline{25\times 9^{-1} \bmod 11} - 7\times 2^{-1} \bmod 11 + \cancel{2}\,7 \times 9^{-1} \bmod 11\right)$$

$$= 25\times 5 \bmod 11 - 7\times 6 \bmod 11 + \cancel{2}\,7\times 5 \bmod 11 \bmod 11$$

$$= \left(4 - 9 + \cancel{8}\,35\right) \bmod 11$$

$$= \cancel{3 \bmod 11 = 3} \quad X$$

$$= 30 \bmod 11 = 8$$

$$S \begin{cases} \to s_1 \\ \to s_i \\ \vdots \\ \to s_n \end{cases} \Bigg\} \; k$$

(k,n)-SSS

(k,n)-Threshold scheme

$k \le n$

deg $k-1 \to k$ points to recon

Security $\to$ info theoretic

$k=3$

1 $\to$ share $\to$ No

2 $\to$ share $\to$ No   0

3 $\to$ share $\to$ Yes   1

Perfectly secure

$f(x) = a_0 + a_1 x \bmod p$

$f(5) = 9 + 2x \bmod p = 8$ $\quad p = 11$

$2 \times 5 \quad 11$

$(5, 8) \longrightarrow$ attacker $\quad p = 11$

$8 = a_0 + a_1 \times 5 \bmod 11 \qquad a_0 = ?, a_1$

a_0	a_1
0 ✓	$\cancel{0}$ 6
1 ✓	8
2 ✓	10
3 ✓	1
4 ✓	—
5	—
⋮	⋮
10	—

11

$0 \le a_0, a_1 < 11$

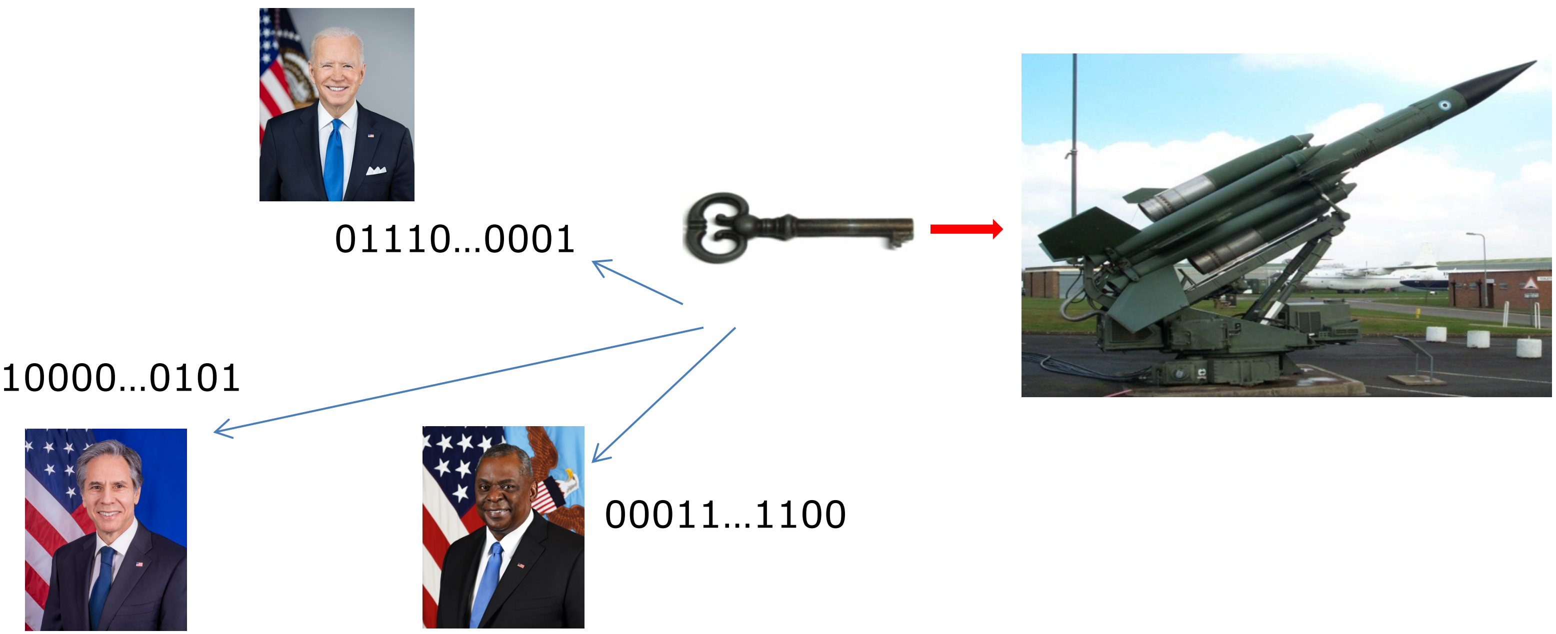
$8 = 1 + a_1 \times 5 \bmod 11$

$7 \times 5^{-1} \bmod 11 = a_1$

$$\text{Prob}(a_0=0) = \text{Prob}(a_0=1) = \text{Prob}(a_0=2)$$

$$= \cdots = \text{Prob}(a_0=10) = \frac{1}{11} = \frac{1}{p}$$

Shamir’s Secret Sharing



Homomorphic property: E(A) o E(B) = E(A o B)

o: +, - *, /, |

Ramp Secret Sharing

- (l, k, n) Ramp Secret Sharing (or Multi Secret Sharing)

<u>Sharing a Secret</u>

$$F(x) = \left(\sum_{i=0}^{l-1} s_i x^i + \sum_{i=l}^{k-1} a_i x^i\right) \bmod q$$

i^{th} Secret

Secret Sharing without mod q

- (l, k, n) Ramp Secret Sharing (or Multi Secret Sharing)

<u>Sharing a Secret</u>

$$F(x) = \left(\sum_{i=0}^{l-1} \underbrace{s_i}_{i^{th}\text{ Secret}} x^i + \sum_{i=l}^{k-1} a_i x^i\right)$$

$(1, 1494)$ $(2, 1942)$ $(3, x)$

$$f(x) = a_0 + a_1 x + a_2 x^2$$

$$1494 = a_0 + a_1 \cdot 1 + a_2 1^2 \quad \text{— } 1$$

$$1942 = a_0 + a_1 \cdot 2 + a_2 2^2 \quad \text{— } 2$$

$$2 - 1 \Rightarrow \quad 448 = a_1 + 3a_2 \qquad a_1 = 31 \qquad a_2 = \; =$$

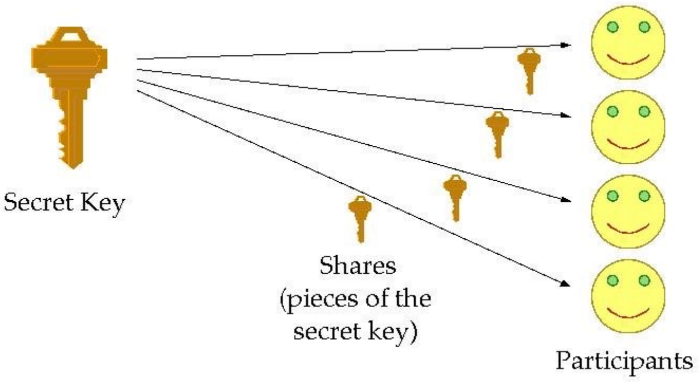
$$= a_1 \; 400 + 3 \cdot 16$$

$$331 = 3a_2 \qquad 448 = 418 + 3 \times 10$$

$$/3$$

Applications of Secret Sharing 1

- **Key Escrow / Key Backup**
  - Divide the secret key into pieces and distribute the pieces to different persons so that certain subsets of the persons can get together to recover the key.



  - Key escrow may also be (mis)used for law enforcement:
  - E.g., in 1991 the U.S. government tried to enforce a new standard for communication encryption: the government would have half of the encryption key and another authority would have the other half. In order to reconstruct the secret a court order would be needed. This standard was eventually broken.

Applications of Secret Sharing 2

- **Secure Storage**
  - divide data into several data-segments, so in order to reconstruct the whole data, several segments are required.
  - For example, the data is a file named X and its data segments are X1, X2, X3, so their XOR would reconstruct X.
  - Of course, this method achieves perfect security, however, we need all the three segments in order to reconstruct the file.
  - Secret sharing is a better option.

Applications of Secret Sharing 3

- **Collective Control**
  - A joint calculation of Key manipulation functions.
  - A major drawback of Public Key Cryptography is the dominance of a certain authority, therefore we wish to allow several authorities to participate in the creation of keys, distributing them, signing them etc.

- **Cryptographic Primitives**
  - A joint calculation of many cryptographic primitives, such as electronic voting, agreement protocols, SMPC (Secure Multi Party Computation), etc.

Applications of Secret Sharing 4

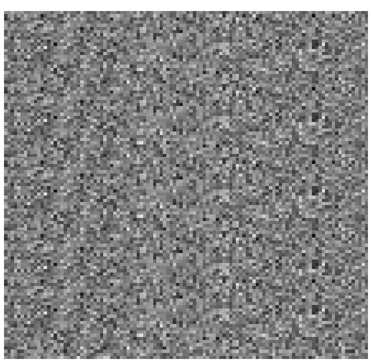
- **Secret Image Sharing**

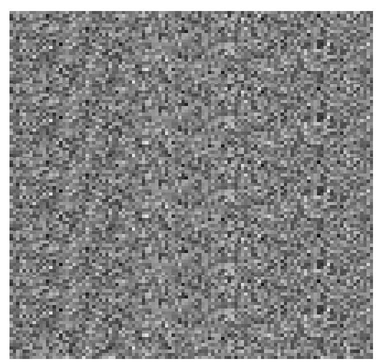
$$f(x) := \sum_{j=1}^{k} y_j l_j(x) \ mod\ P$$

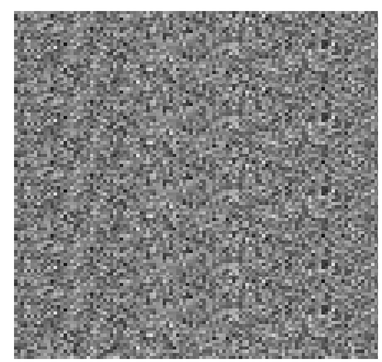
P is a prime number

Secret image

Gray Lena image



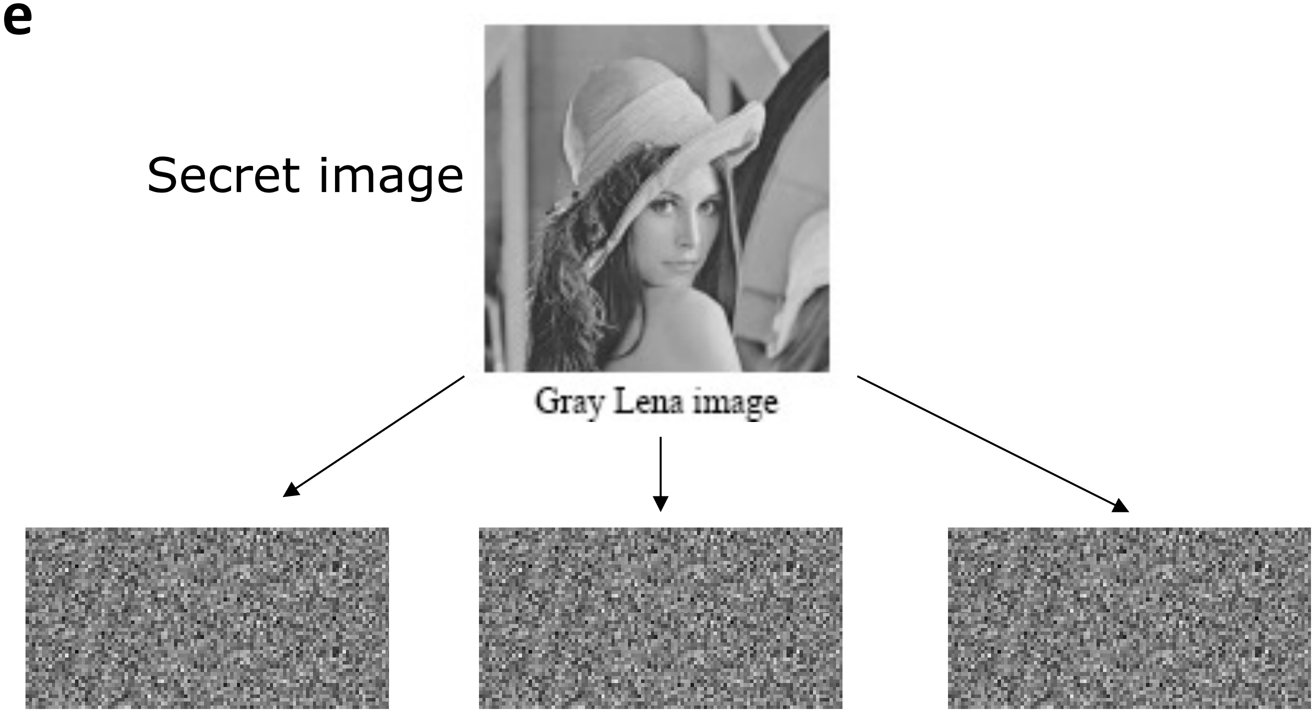




Share images

Applications of Secret Sharing 5

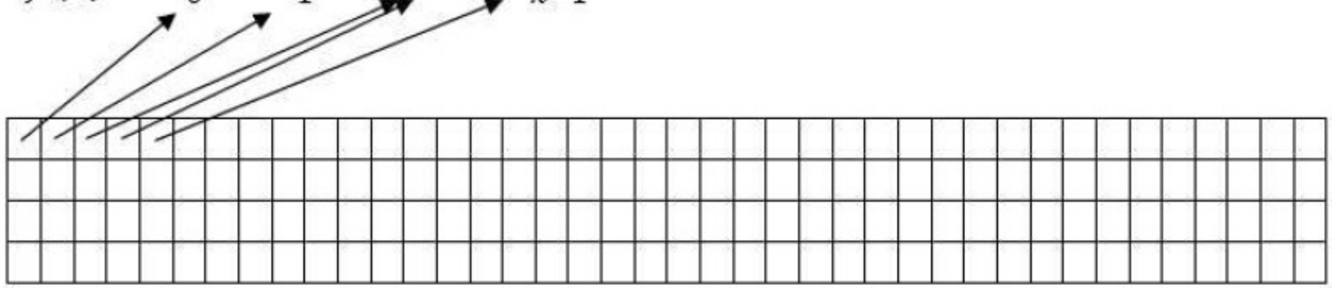
- **Secret Image Sharing (With reduced share sizes) – in ideal case**



Share images

Thien and Lin’s Method

$$f(x) = d_0 + d_1 x + \ldots + d_{k-1} x^{k-1}$$



(a) Gray Lena image

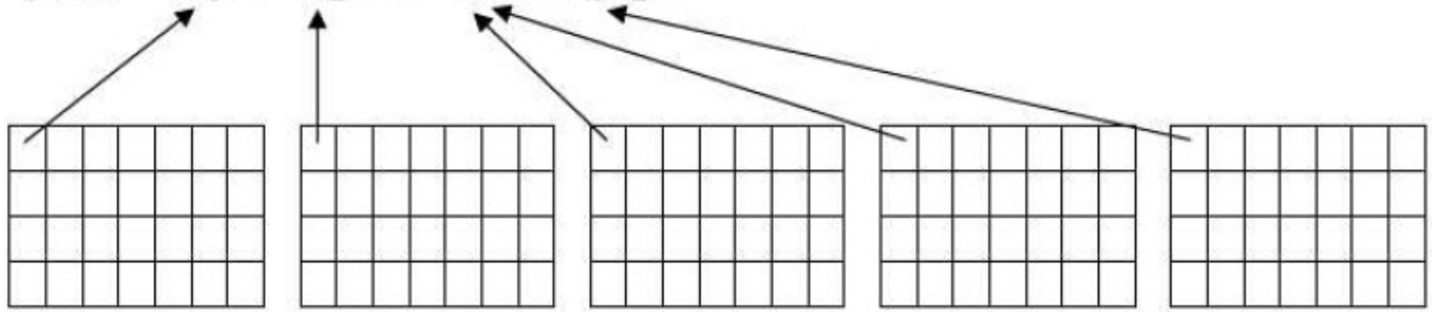
(b) Non-permuted share

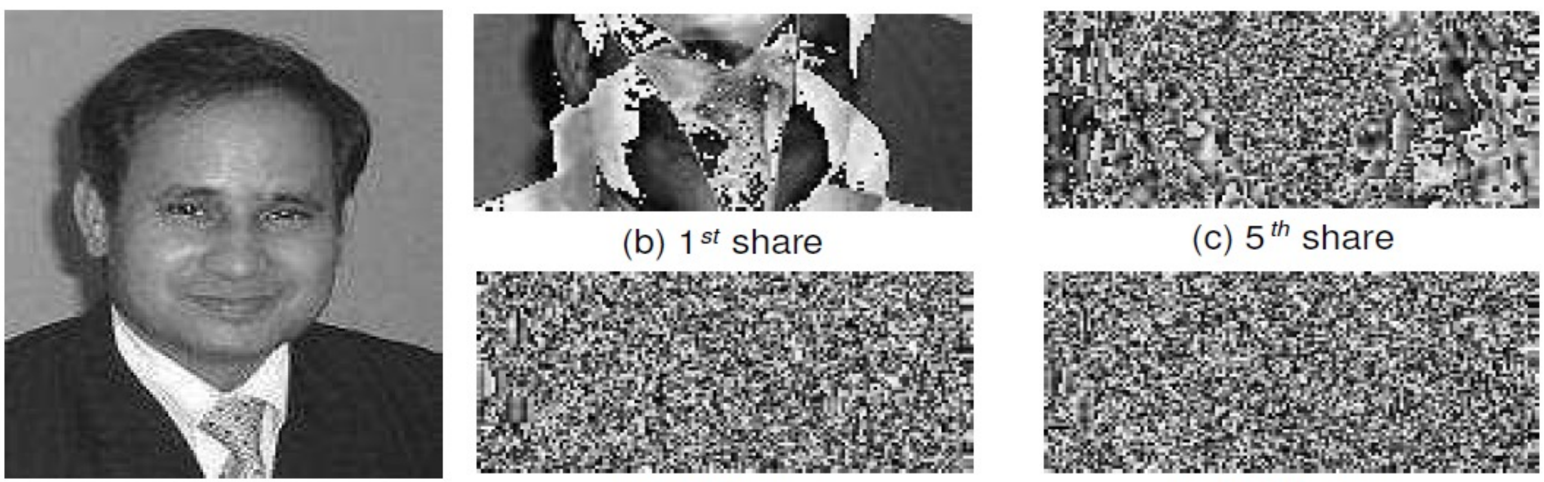
(c) Permuted share

C.-C. Thien and J.-C. Lin, “Secret image sharing,” *Computers & Graphics*, vol. 26, no. 5, pp. 765 – 770, 2002.

Alharthi and Atrey's Method

$$f(x) = d_0 + d_1 x + \dots + d_{k-1} x^{k-1}$$





(a) Secret image

(b) 1^{st} share

(c) 5^{th} share

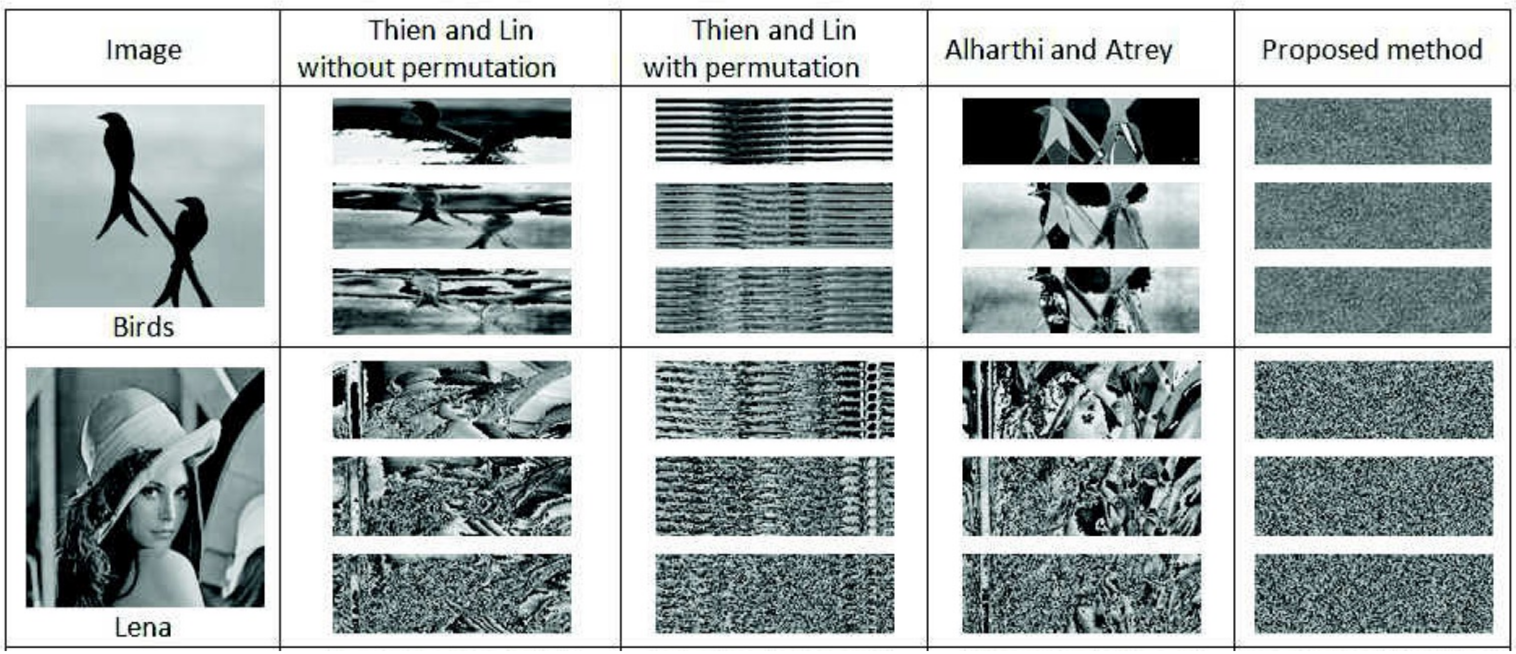
(d) 10^{th} share

(e) 20^{th} share

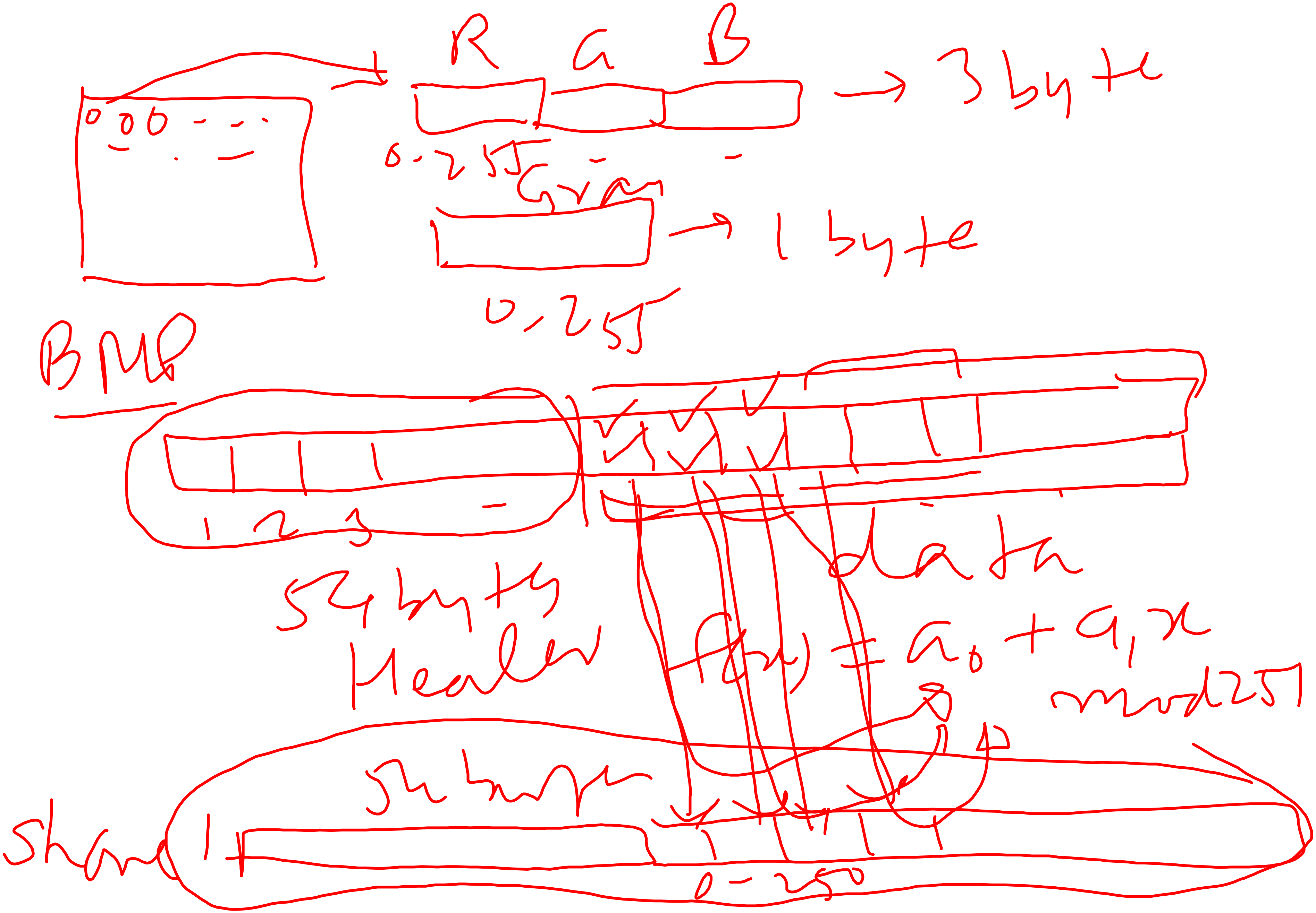
S. Alharthi and P. K. Atrey. An improved scheme for secret image sharing. *IEEE ICME Workshop on Content Protection and Forensics (CPAF)*, pp 1661-1665, July 2010, Singapore.

Alharthi and Atrey’s Improved Method

$$x = ((x + y) mod p) + 1$$
$$\text{where } 1 \leq y < p, 1 \leq x \leq p.$$



S. Alharthi and P. K. Atrey. [Further improvements on secret image sharing scheme](). ACM Multimedia 2010 Workshop on Multimedia in Forensics, Security and Intelligence ([MiFor'2010]()), October 2010, Firenze, Italy.


R G B
3 byte
0 , 255
Gray
1 byte
0 , 255
BMP
1 2 3
54 bytes
Header
data
f(x) = a0 + a1x
mod 251
54 bytes
Share 1
0 - 250

Summary

- Secret Sharing
- Threshold Secret Sharing
- Shamir's Secret Sharing Scheme
  - Applied to Images
- There are many other variants of secret sharing
  - Progressive Secret Sharing
  - Verifiable Secret Sharing