# Tutorial 6

CSCI361 – Computer Security

Sionggo Japit
sjapit@uow.edu.au

# OBJECTIVE

## Secret Sharing

- Shamir Secret Sharing

# SECRET SHARING

- In situations where a large amount of data needs to be encrypted quickly or the users are computationally limited, symmetric cryptosystems still play an important role.
- However, a major problem symmetric cryptosystems face is how to agree a common secret key to enable communications to begin.
- This basic 'key exchange problem' becomes ever more severe as communication networks grow in size and more and more users wish to communicate securely.
- Many technique have been device to overcome this problem; one popular and elegant technique is Shamir Secret Sharing, proposed by Shamir in 1979.

# SECRET SHARING

- For example, a company wishes to allow only a certain group of employees to electronically sign documents. Each employee in this group is assigned with a secret share that the employee himself/herself knows.
- It is also decided that any three employee from the group are needed to sign a document.
- This requirement is known as threshold.
- To achieve this, Shamir threshold secret sharing scheme may be used.

# Threshold Scheme

- A (t, m) *threshold scheme* ($t \leq m$) is a method by which a trusted party computes secret *shares* $S_i$, $1 \leq i \leq m$ from an initial secret S, and securely distributes $S_i$ to user $P_i$ , such that the following is true:
  - Any t or more users who pool their shares may easily recover S, but any group knowing only $t - 1$ or fewer shares may not.
- A *perfect* threshold scheme is a threshold scheme in which knowing only $t - 1$ or fewer shares provide no advantage (no information about S whatsoever, in the information-theoretic sense) to an opponent over knowing no pieces.

# Shamir Secret Sharing

- Shamir's scheme is based on polynomial interpolation and relies on the fact that given $n$ points $(x_1, y_1),\ldots,(x_n, y_n)$ with the $x_i$ distinct, there is exactly one polynomial $y(x)$ of degree $n-1$ such that $y(x_i) = y_i$ for $1 \leq i \leq n$.

# SHAMIR SECRET SHARING

**Construction and distribution of secret share:**

1. A trusted party select a prime p > max(S, m), and constructs random polynomial *y(x)* of degree at most *(t-1)*; the constant of the polynomial is the secret or the key; i.e., $a_0=S$.

$$y(x) = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \bmod p$$

# SHAMIR SECRET SHARING

2. The trusted party computes $S_i = y(i) \bmod p$ shares and distributes each share to each participating members (users).

$$y(1) = a_0 + a_1(1) + a_2(1)^2 + \ldots + a_{t-1}(1)^{t-1} \bmod p$$

$$y(2) = a_0 + a_1(2) + a_2(2)^2 + \ldots + a_{t-1}(2)^{t-1} \bmod p$$

$$y(3) = a_0 + a_1(3) + a_2(3)^2 + \ldots + a_{t-1}(3)^{t-1} \bmod p$$

...

...

...

$$y(m) = a_0 + a_1(m) + a_2(m)^2 + \ldots + a_{t-1}(m)^{t-1} \bmod p$$

# SHAMIR SECRET SHARING

- The shares $S(1,y(1)), S(2,y(2)),\ldots,S(m,y(m))$ are then distributed to each participating members.

# SHAMIR SECRET SHARING

**Reconstructing the share (key):**

- Any t or more of the group members may be pooling their secret shares to recover the secret S.
- To recover the secret S, the group use Lagrange interpolation.

$$s(x) = \sum_{i=1}^{t} x_i y_i, \qquad where\ x_i = \prod_{1 \le j \le t, j \neq i} \frac{x - x_j}{x_i - x_j}$$

*or*

$$s(0) = \sum_{i=1}^{t} x_i y_i, \quad where\ x_i = \prod_{1 \le j \le t, j \neq i} \frac{-x_j}{x_i - x_j}$$

# SHAMIR SECRET SHARING

Example, To ensure integrity to its documents, an organization wants a minimum of 3 of its 5 selected members to sign a document. The key (secret) to sign the document is, let's say 13. (Note, the participating members do not know the secret, only a trusted body appointed by the organization knows.)

The threshold is $(t,m) = (3,5)$.

# SHAMIR SECRET SHARING

Generating and distributing secret shares:

- Trusted party selects p = 17. (Note: *p > max(S, m); i.e., 17 > max(13, 5)*)
- Trusted party randomly chooses two coefficients, $a_1$=10 and $a_2$=2.
- The trusted party generates 5 shares using a polynomial of degree (t-1):

$$y(x) = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \bmod p$$

# SHAMIR SECRET SHARING

$x = 1$

$$y(1) = 13 + 10(1)^1 + 2(1)^2 \bmod 17$$

$$= 13 + 10 + 2 \bmod 17$$

$$= 25 \bmod 17$$

$$= 8$$

\ Share for participant 1 is $S_1(1, 8)$.

# SHAMIR SECRET SHARING

$x = 2$

$$y(2) = 13 + 10(2)^1 + 2(2)^2 \bmod 17$$

$$= 13 + 20 + 8 \bmod 17$$

$$= 41 \bmod 17$$

$$= 7$$

\ Share for participant 2 is $S_2(2, 7)$.

# SHAMIR SECRET SHARING

$x = 3$

$$y(3) = 13 + 10(3)^1 + 2(3)^2 \bmod 17$$

$$= 13 + 30 + 18 \bmod 17$$

$$= 61 \bmod 17$$

$$= 10$$

\ Share for participant 3 is $S_3(3,10)$.

# SHAMIR SECRET SHARING

$x = 4$

$$y(4) = 13 + 10(4)^1 + 2(4)^2 \bmod 17$$

$$= 13 + 40 + 32 \bmod 17$$

$$= 85 \bmod 17$$

$$= 0$$

\ Share for participant 4 is $S_4(4, 0)$.

# SHAMIR SECRET SHARING

$$x = 5$$

$$y(5) = 13 + 10(5)^1 + 2(5)^2 \bmod 17$$

$$= 13 + 50 + 50 \bmod 17$$

$$= 113 \bmod 17$$

$$= 11$$

\ Share for participant 5 is $S_5(5,11)$.

# SHAMIR SECRET SHARING

- The trusted party distributes the five shares to the respective five members.
- $S_1(1,8)$ to member 1
- $S_2(2,7)$ to member 2
- $S_3(3,10)$ to member 3
- $S_4(4,0)$ to member 4
- $S_5(5,11)$ to member 5.

# SHAMIR SECRET SHARING

Assuming members 1, 3, and 5 want to sign a document, the member each supplies their secrete share and the trusted party uses Lagrange interpolation to retrieve the secret (key).

# SHAMIR SECRET SHARING

$$Member\ 1 : S_1(1,8) \quad \Rightarrow x_1 = 1, y_1 = 8$$
$$Member\ 3 : S_3(3,10) \quad \Rightarrow x_3 = 3, y_3 = 10$$
$$Member\ 5 : S_5(5,11) \quad \Rightarrow x_5 = 5, y_5 = 11$$

$$l_1 = y_1 \times \prod_{j=3,5} \frac{x - x_j}{x_1 - x_j} \bmod p$$
$$= 8 \times \left[ \left( \frac{x - 3}{1 - 3} \right) \left( \frac{x - 5}{1 - 5} \right) \right] \bmod 17$$
$$= 8 \times \left[ \left( \frac{(x - 3)(x - 5)}{(-2)(-4)} \right) \right] \bmod 17$$
$$= 8 \times \left[ \frac{x^2 - 5x - 3x + 15}{8} \right] \bmod 17$$
$$= x^2 - 8x + 15 \bmod 17$$

$$l_3 = y_3 \times \prod_{j=1,5} \frac{x - x_j}{x_3 - x_j} \bmod p$$
$$= 10 \times \left[ \left( \frac{x - 1}{3 - 1} \right) \left( \frac{x - 5}{3 - 5} \right) \right] \bmod 17$$
$$= 10 \times \left[ \left( \frac{(x - 1)(x - 5)}{(2)(-2)} \right) \right] \bmod 17$$
$$= 10 \times \left[ \frac{(x^2 - 5x - x + 5)}{-4} \right] \bmod 17$$
$$= 10 \times \left[ \frac{x^2 - 6x + 5}{-4} \right] \bmod 17$$
$$= \left[ \frac{10x^2 - 60x + 50}{-4} \right] \bmod 17$$
$$= \left[ \frac{10x^2 - 9x + 16}{-4} \right] \bmod 17$$
$$= -\frac{10}{4}x^2 + \frac{9}{4}x - 4 \bmod 17$$

# SHAMIR SECRET SHARING

$$l_5 = y_5 \times \prod_{j=1,3} \frac{x - x_j}{x_5 - x_j} \bmod p$$

$$= 11 \times \left[ \left( \frac{x - 1}{5 - 1} \right) \left( \frac{x - 3}{5 - 3} \right) \right] \bmod 17$$

$$= 11 \times \left[ \left( \frac{(x - 1)(x - 3)}{(4)(2)} \right) \right] \bmod 17$$

$$= 11 \times \left[ \frac{(x^2 - 3x - x + 3)}{8} \right] \bmod 17$$

$$= \left[ \frac{11x^2 - 44x + 33}{8} \right] \bmod 17$$

$$= \left[ \frac{11x^2 - 10x + 16}{8} \right] \bmod 17$$

$$= \frac{11}{8} x^2 - \frac{10}{8} x + 2 \bmod 17$$

# SHAMIR SECRET SHARING

$$y(x) = l1 + l3 + l5 \bmod 17$$

$$= (x^2 - 8x + 15) + (-\frac{10x^2}{4} + \frac{9}{4}x - 4) + (\frac{11}{8}x^2 - \frac{10}{8}x + 2)$$

$$= x^2 - 8x + 15 - \frac{10}{4}x^2 + \frac{9}{4}x - 4 + \frac{11}{8}x^2 - \frac{10}{8}x + 2$$

$$= (x^2 - \frac{10}{4}x^2 + \frac{11}{8}x^2) - (8x - \frac{9}{4}x + \frac{10}{8}x) + (15 - 4 + 2)$$

$$= \left(\frac{8x^2 - 20x^2 + 11x^2}{8}\right) - \left(\frac{64x - 18x + 10x}{8}\right) + 13$$

$$= \left(\frac{-1x^2}{8}\right) - \left(\frac{56x}{8}\right) + 13$$

$$= \left(\frac{16x^2}{8}\right) - \left(\frac{56x}{8}\right) + 13$$

$$= 2x^2 - 7x + 13$$

Thus y(0) = 13 = secret = key.

# SHAMIR SECRET SHARING

Alternatively,

$$y(0)=\frac{(y_1)(-x_3)(-x_5)}{(x_1-x_3)(x_1-x_5)}+\frac{(y_3)(-x_1)(-x_5)}{(x_3-x_1)(x_3-x_5)}+\frac{(y_5)(-x_1)(-x_3)}{(x_5-x_1)(x_5-x_3)} \bmod 17$$

$$=\frac{(8)(-3)(-5)}{(1-3)(1-5)}+\frac{(10)(-1)(-5)}{(3-1)(3-5)}+\frac{(11)(-1)(-3)}{(5-1)(5-3)} \bmod 17$$

$$=\frac{(8)(15)}{8}+\frac{(10)(5)}{-4}+\frac{(11)(3)}{8} \bmod 17$$

$$=15+\frac{50}{-4}+\frac{33}{8} \bmod 17$$

$$=15+\frac{16}{-4}+\frac{16}{8} \bmod 17$$

$$=15-4+2$$

$$=13$$

# SHAMIR SECRET SHARING

SUMMARY:

A trusted party (dealer) distributes shares of a secret S to n users.

- RESULT: any group of t users which pool their shares can recover S.
  1. *Setup*. The trusted party T begins with a secret integer $S \geq 0$ it wishes to distribute among n users.
     a) T chooses a prime $p > \max(S, n)$, and defines $a_0 = S$.

# SHAMIR SECRET SHARING

a) T selects t−1 random, independent coefficients a1, . . . , $a_{t-1}$, $0 \le a_j \le p-1$,defining the random polynomial over *Zp*, $y(x) = \sum_{j=0}^{t-1} a_j x^j$.

b) T computes $S_i$ =y(i) mod p, where 1≤i≤n(or for any *n* distinct point $s_i$, $1 \le i \le p-1$), and securely transfers the share $S_i$ to user $P_i$, along with public index i.

# SHAMIR SECRET SHARING

2. *Pooling of shares*. Any group of $t$ or more users pool their shares. Their shares provide $t$ distinct points $(x, y) = (i, S_i)$ allowing computation of the coefficients $a_j$, $1 \leq j \leq t - 1$ of $y(x)$ by Lagrange interpolation. The secret is recovered by noting $y(x) = a_0 = S$.

# SHAMIR SECRET SHARING

- The coefficients of an unknown polynomial $y(x)$ of degree less than $t$, defined by points $(x_i, y_i)$, $1 \le i \le t$, are given by the Lagrange interpolation formula:

$$y(x) = \sum_{i=1}^{t} y_i \prod_{1 \le j \le t, j \ne i} \frac{x - x_j}{x_i - x_j}$$

Since $y(x) = a_0 = S$, the shared secret may be expressed as:

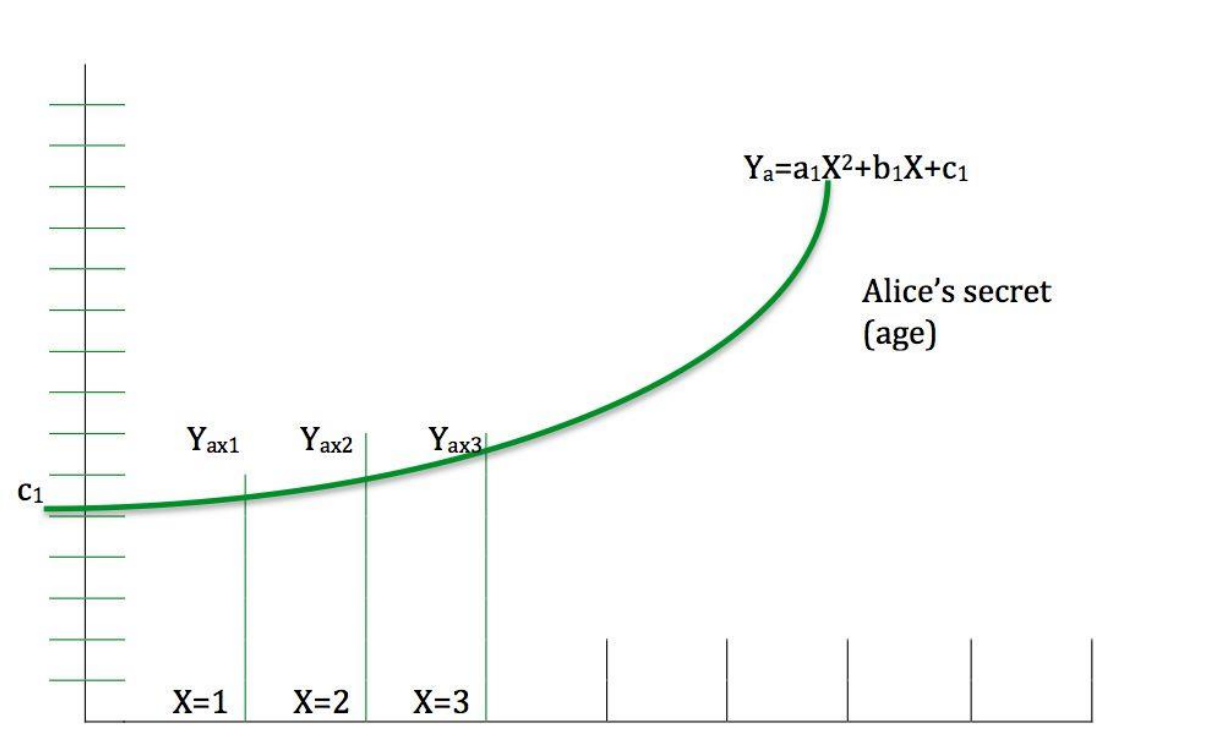
$$s = \sum_{i=1}^{t} x_i y_i, \qquad where\ x_i = \prod_{1 \le j \le t, j \ne i} \frac{x - x_j}{x_i - x_j}$$

# SHAMIR SECRET SHARING

- Thus each group member may compute S as a linear combination of $t$ shares $y_i$, since the $x_i$ are non-secret constants (which for a fixed group of $t$ users may be pre-computed).

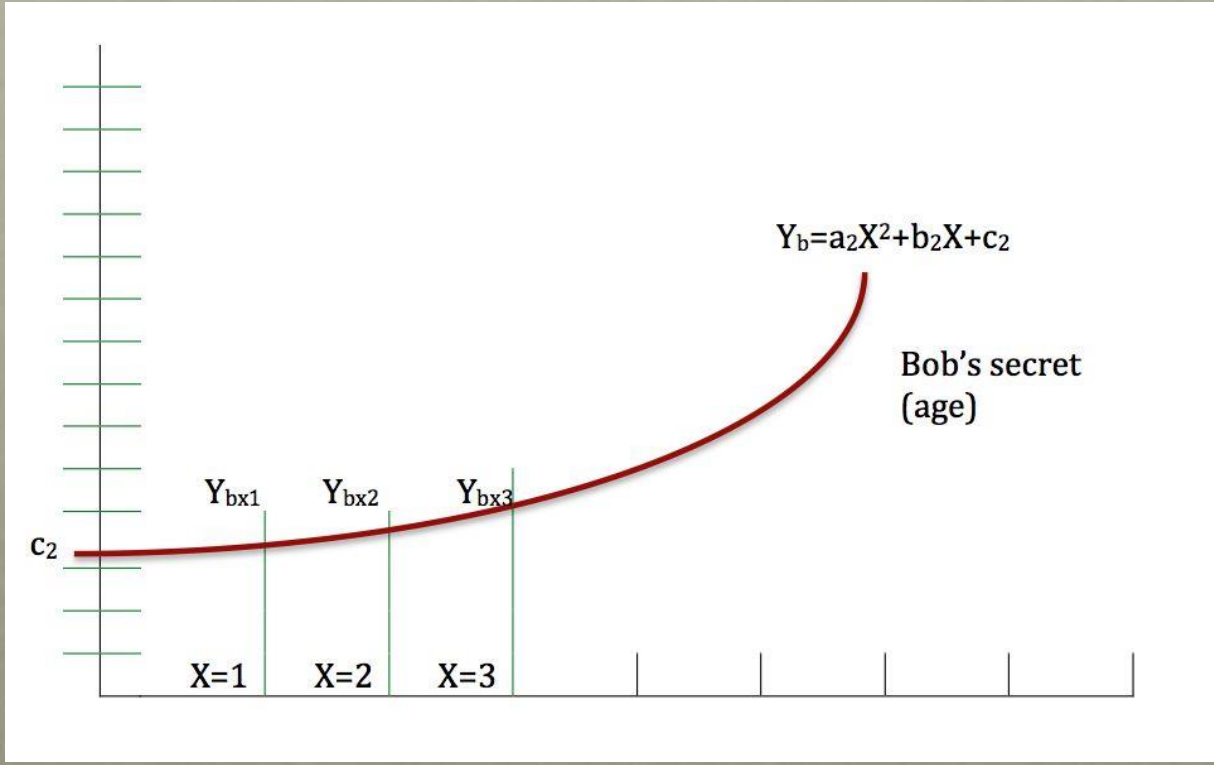
# ASSIGNMENT RELATED

- This may be one approach to tackle the problem.
- Considering the following function as Alice's age:



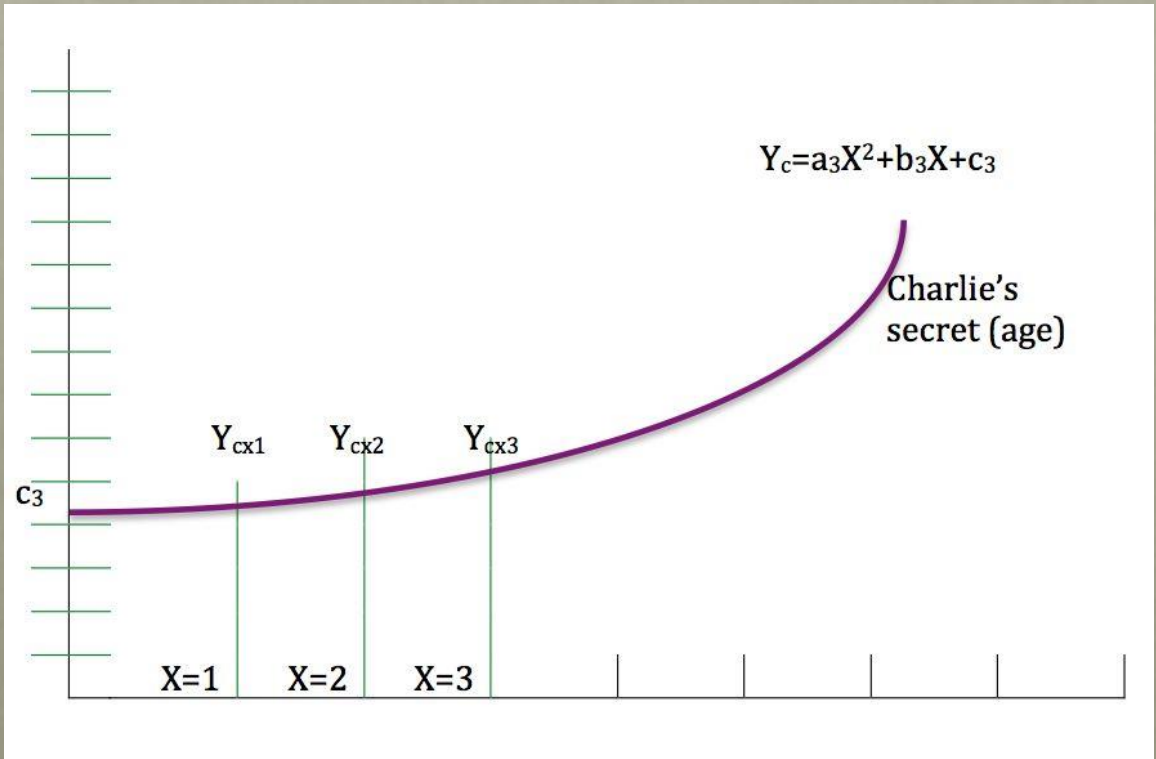
# ASSIGNMENT RELATED

- … and the following function as Bob's age:



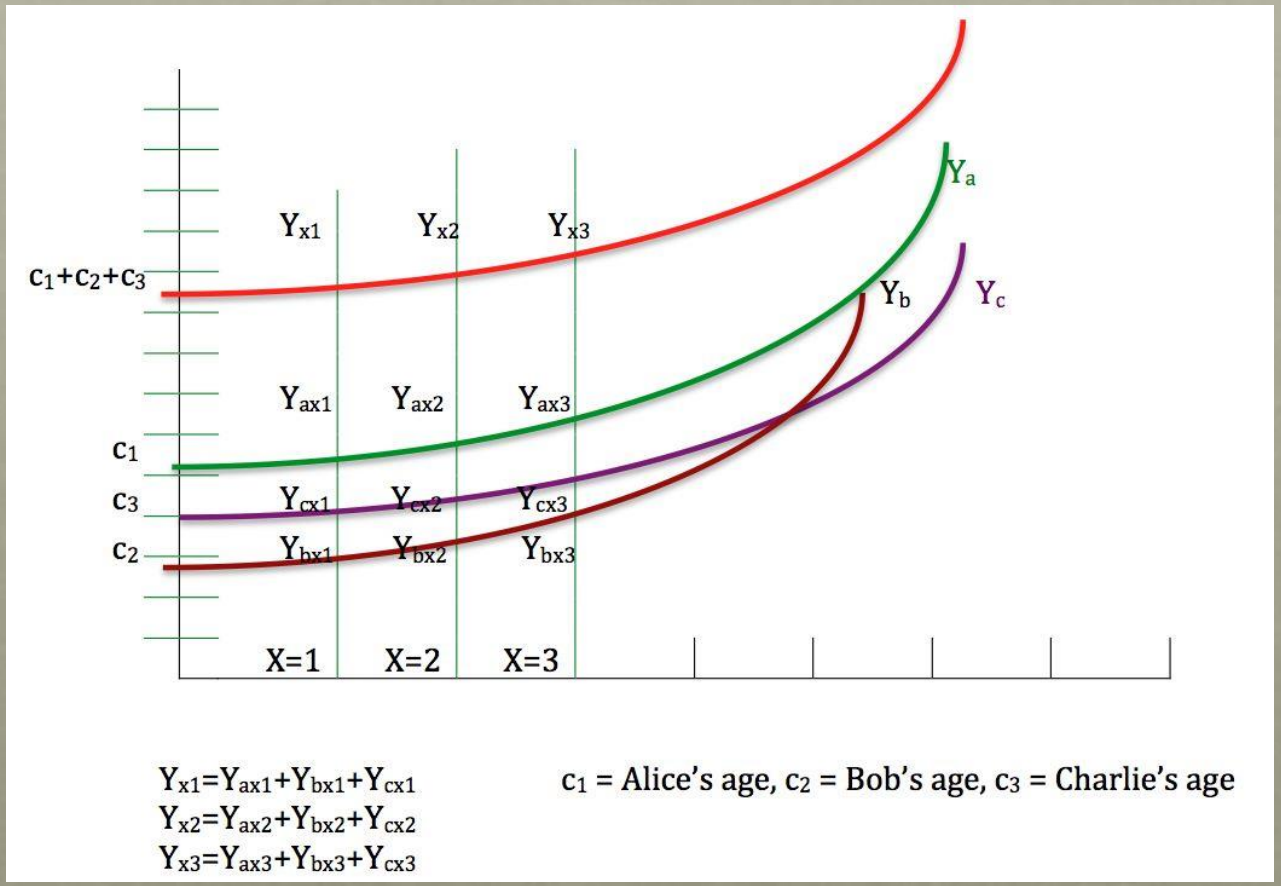
# ASSIGNMENT RELATED

- … and the following function as Charlie's age:



# ASSIGNMENT RELATED

- … and the following function is the addition of the three person's age:




From this function (Y), you can find c1+c2+c3 (the total age of the three person) through $Y_{x1}$, $Y_{x2}$, and $Y_{x3}$. $Y_{x1}$, $Y_{x2}$, and $Y_{x3}$ are the secret share of Alice, Bob, and Charlie respectively. Think of how to get $Y_{x1}$, $Y_{x2}$, and $Y_{x3}$. If you can calculate $Y_{x1}$, $Y_{x2}$, and $Y_{x3}$ effectively, you may be able to solve the problem using Largrange interpolation to get c1+c2+c3.