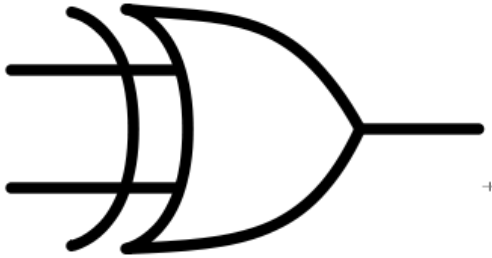
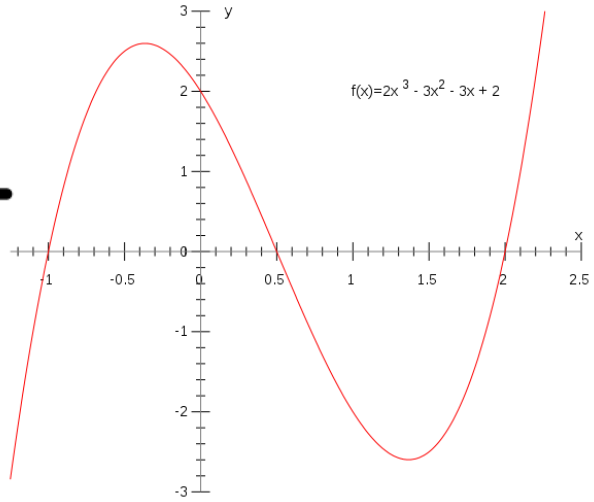
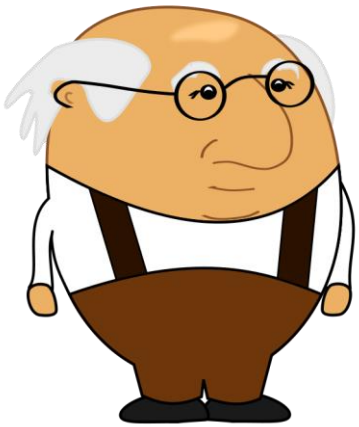
Sharing Secrets using *scissors*, ***XORs***, and *polynomials* ?





Dr. Yan Huang

Mar. 2014

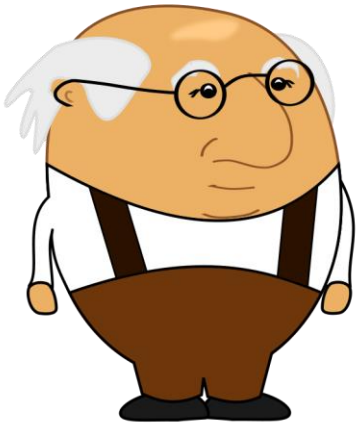


BANK OF CANADA

Secret password

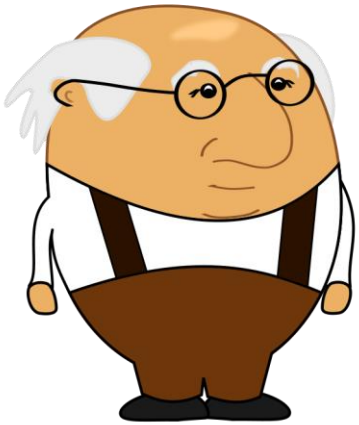
1010 0010 1100 0110

1st Try: Naïve Cutting



1010 0010 1100 0110

Secret Recover



1010 0010

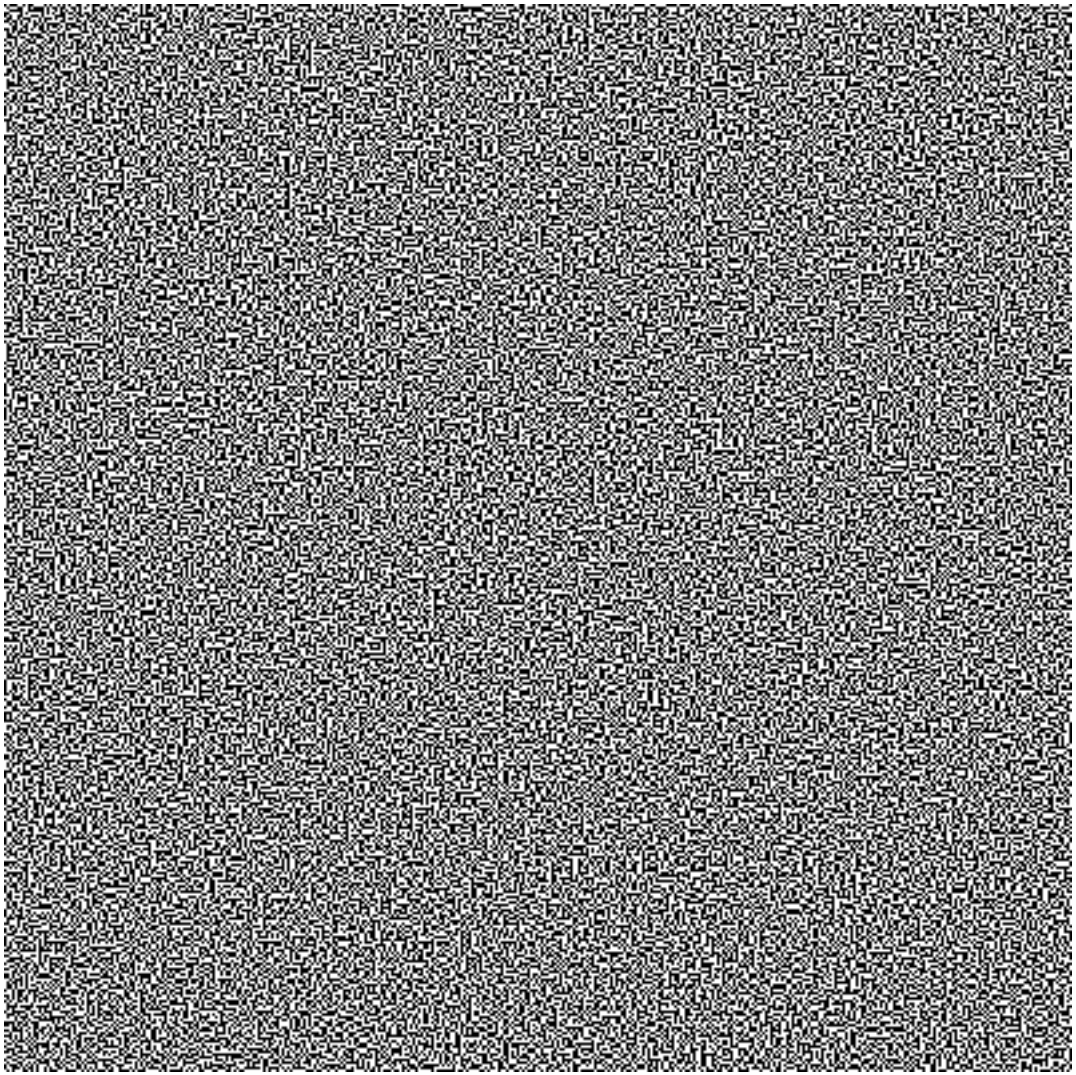
1100 0110

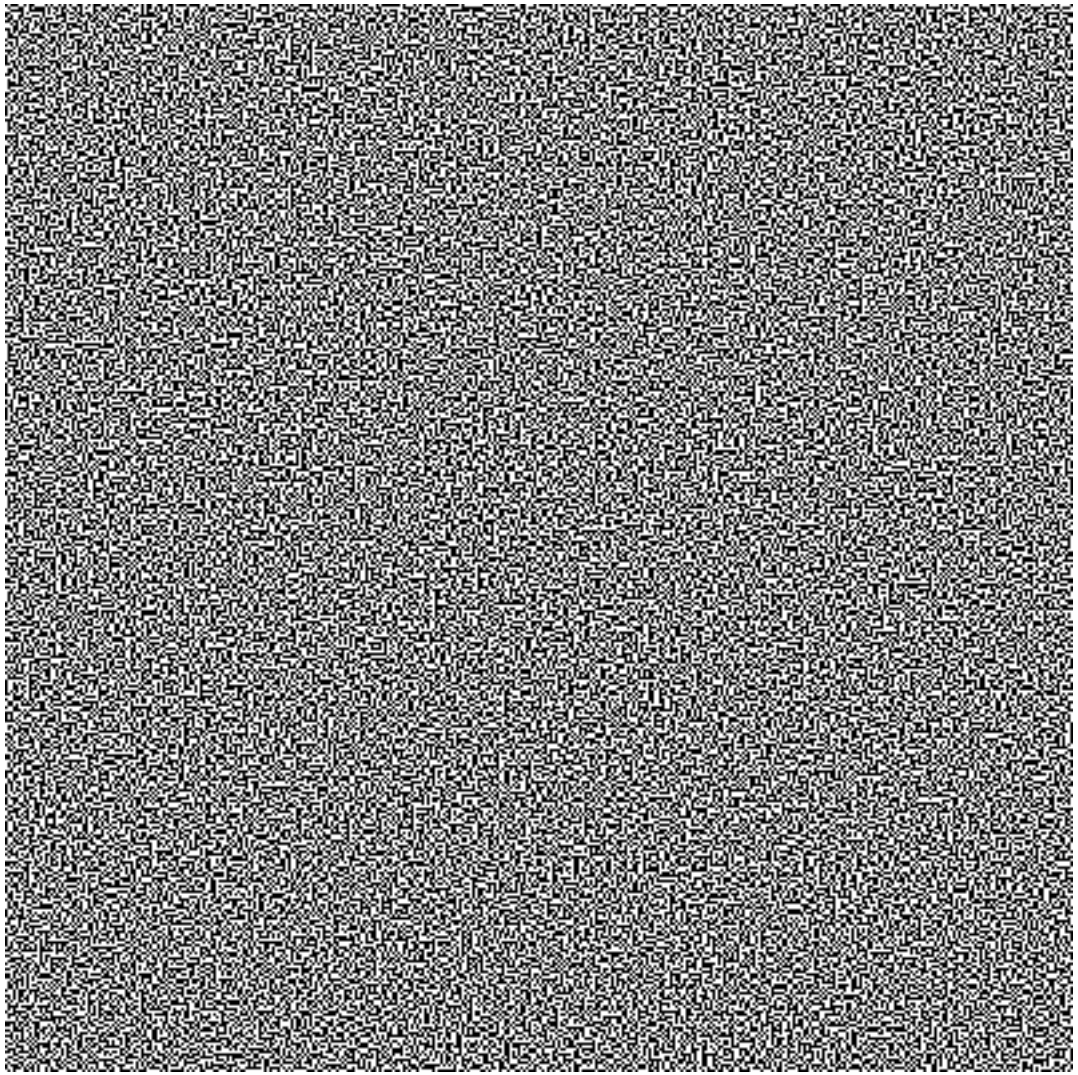
Problems

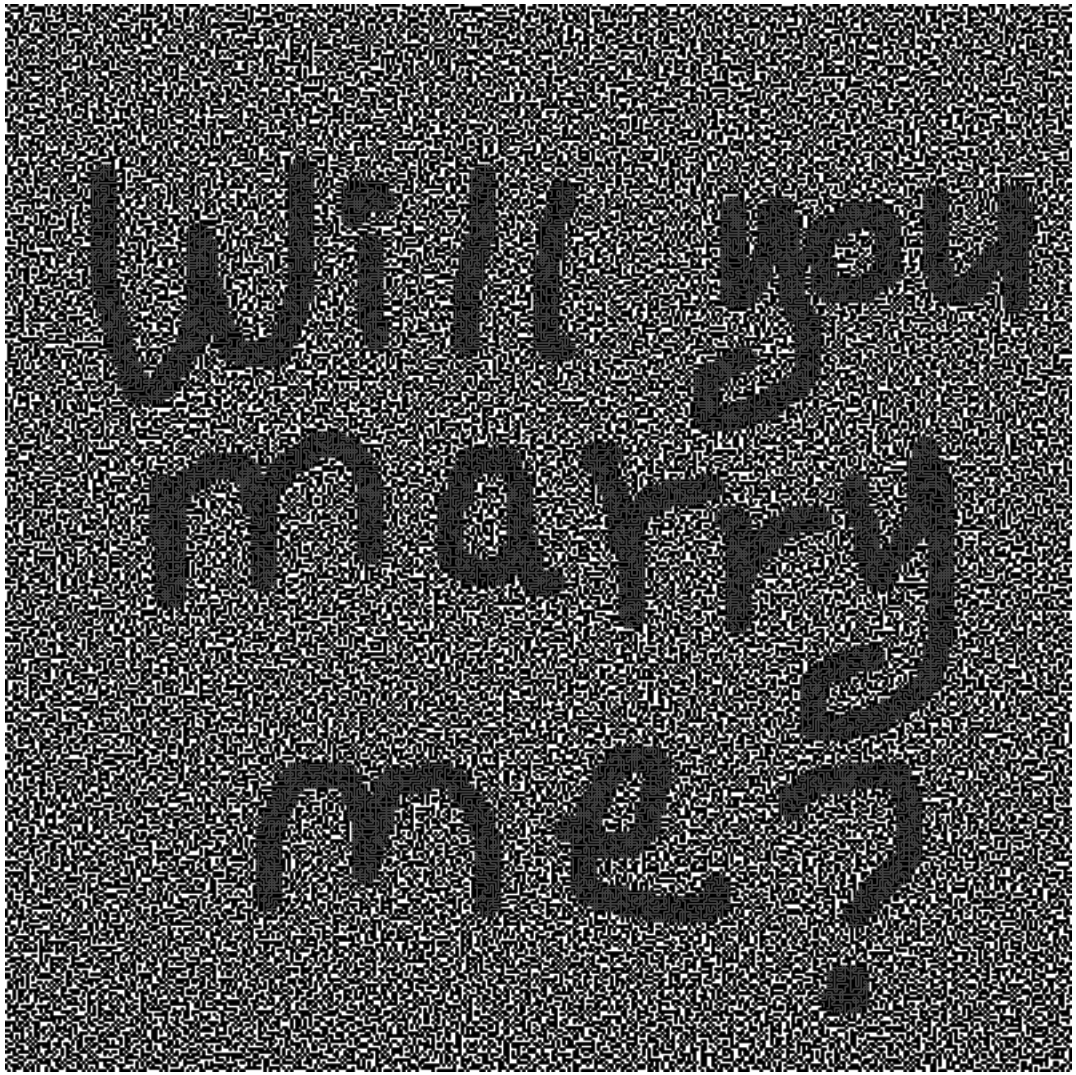
Some boxes/keys could be lost

- Bad guy learns part of the secret
- Good guy CAN'T recover the secret

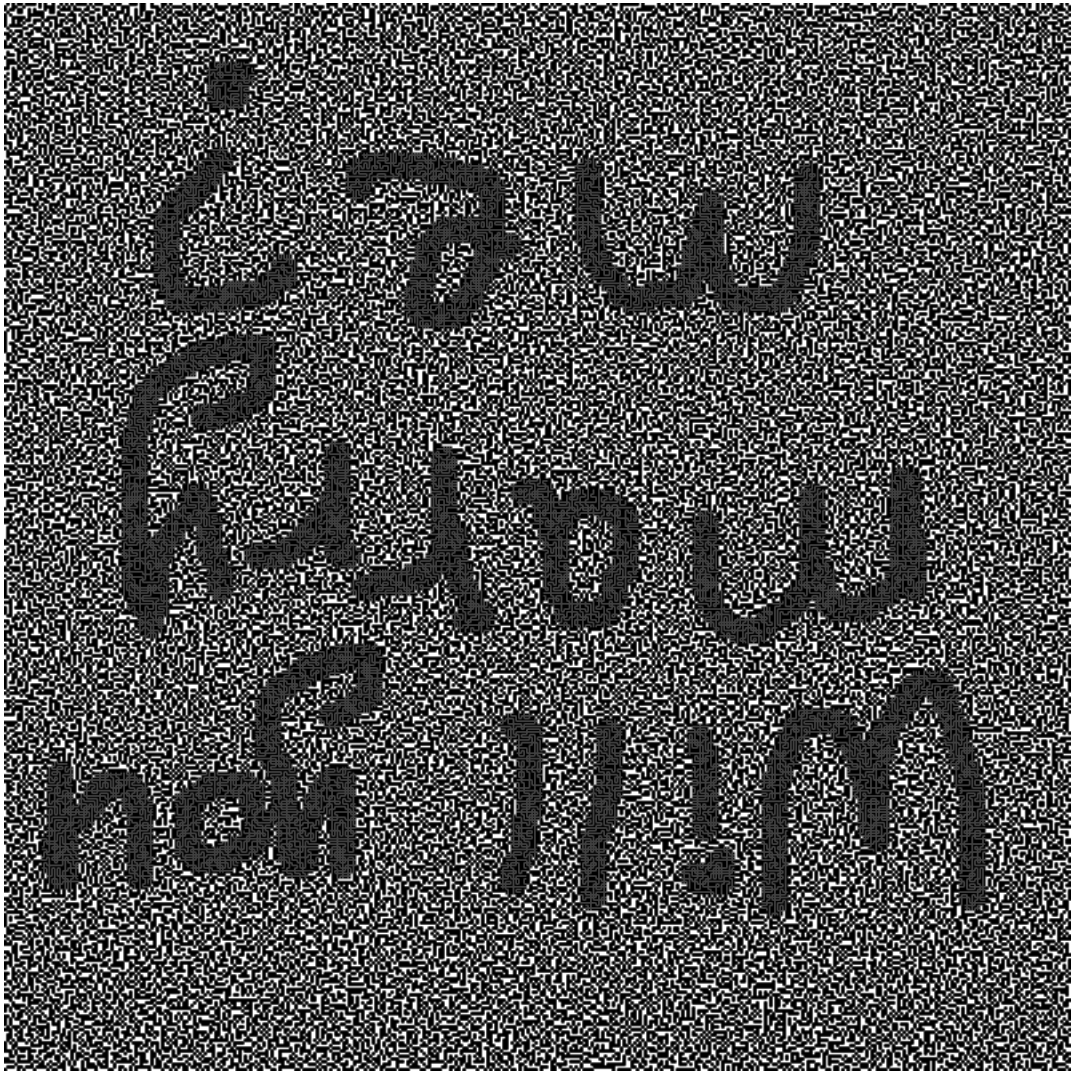
A True Story







Yes I will!


Proud
Parent

XOR ⊕

a	b	z = a ⊕ b
0	0	0
0	1	1
1	0	1
1	1	0

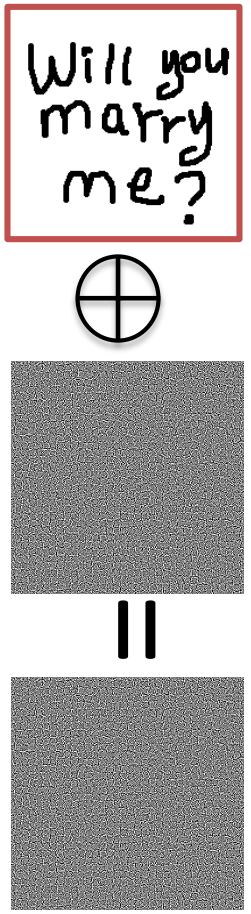
2nd Try: Divide using XOR

Secret: 1010 0010 1100 0010

⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕

Randomly generate 0110 1001 1001 1110

1100 1011 0101 1100



Recover the Secret

0110 1001 1001 1110

⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕

1100 1011 0101 1100

Secret: 1010 0010 1100 0010

Generalize to 3 shares

Randomly generate

1010 0010 1100 0010

⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕

0110 1001 1001 1110

⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕

0000 0111 0101 1000

1100 1100 0000 0100

Generalize to 3 shares

0110 1001 1001 1110

⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕

0000 0111 0101 1000

⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕ ⊕⊕⊕⊕

1100 1100 0000 0100

Secret: 1010 0010 1100 0010

Problems

Some boxes/keys could be lost

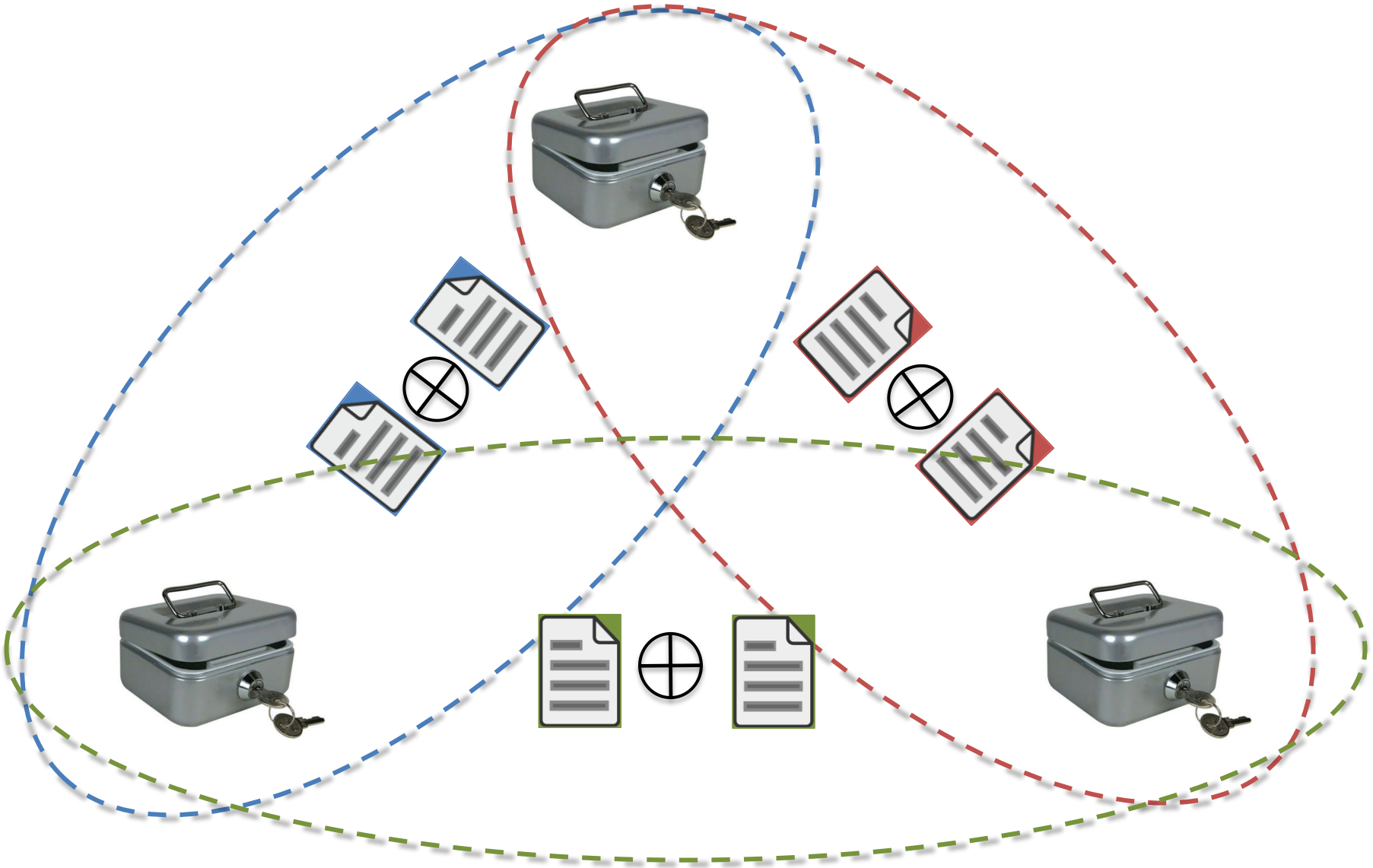
- Bad guy learns part of the secret
- Good guy CAN'T recover the secret

Problems

Preferably:

- A total of 3 shares
- Able to recover from any 2 shares
- Any 1 share reveals nothing

To Share



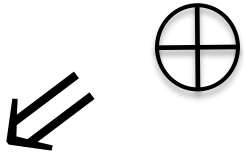
To Recover

1010 0010 1100 0010

⇑

⊕

To Recover



1010 0010 1100 0010

Problem

Every box needs to store 2 shares.

Problem

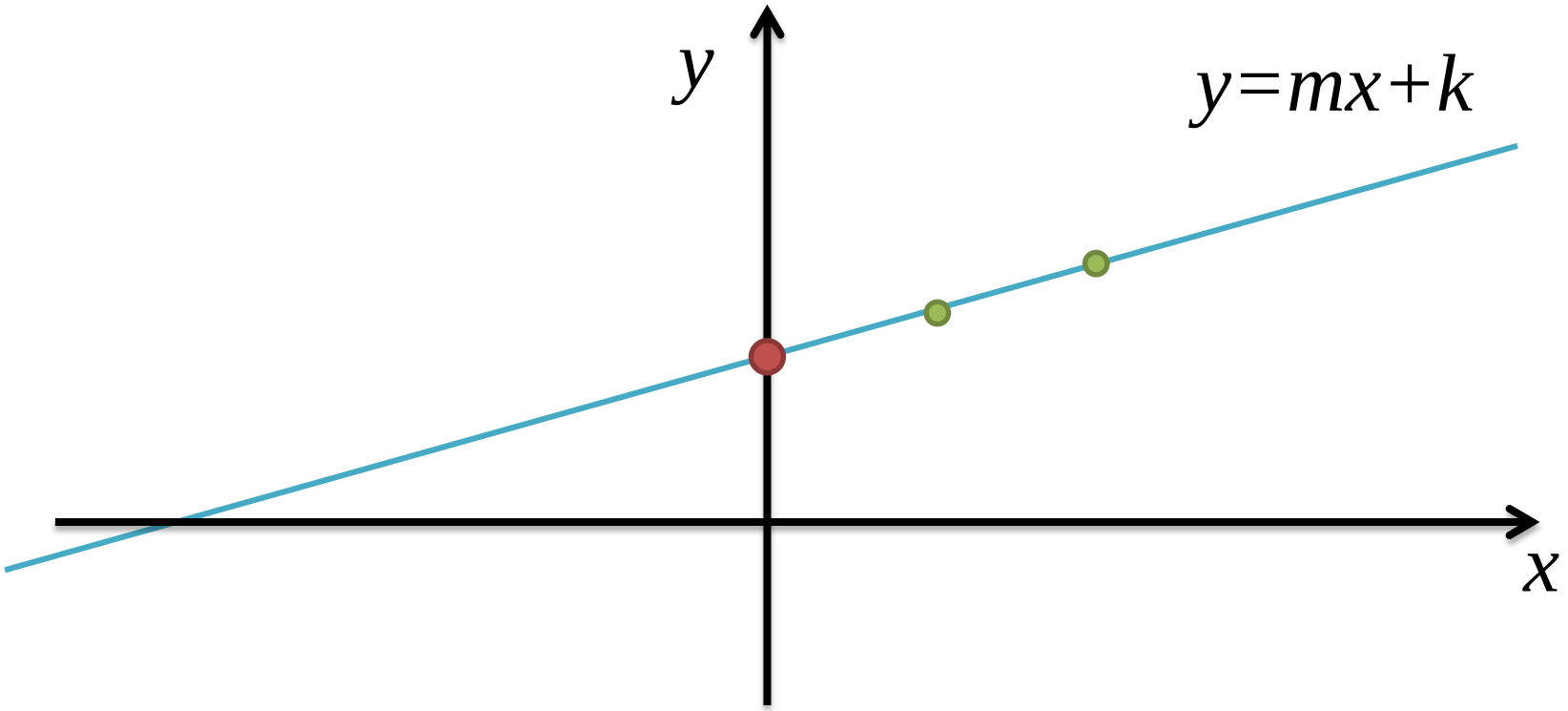
If we want n boxes and being able to recover from any t of them, every box needs to store about n^{t-1} shares.

Too many Shares!

3rd Try
Using Straight Lines

Generate Shares

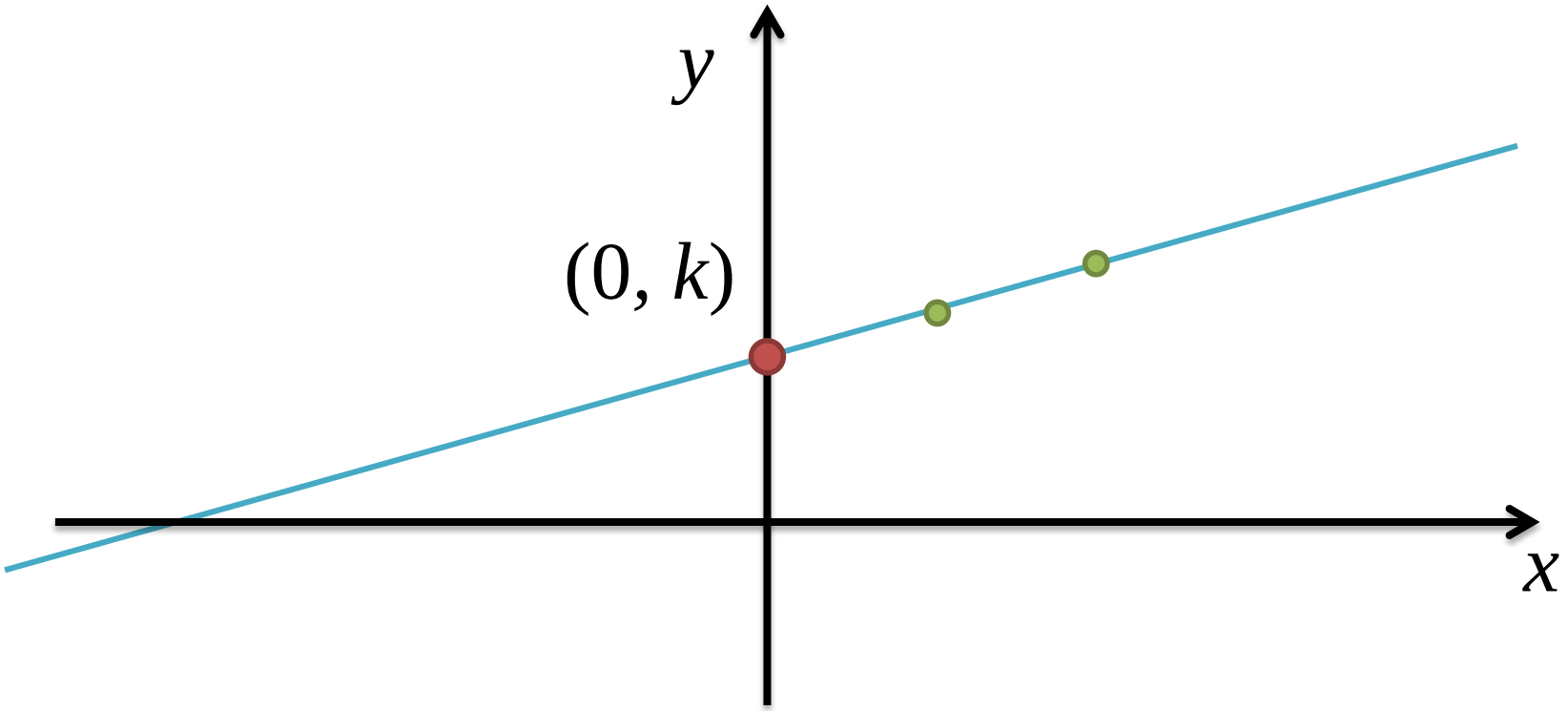
1. Mark the ***secret*** as a point on the y-axis.
2. Generate a ***random line*** crossing the secret point (0, k).
3. Pick the point $(1, \quad m+k)$ --- the 1st ***share***.
4. Pick the point $(2, 2m+k)$ --- the 2nd ***share***.



Generate Shares

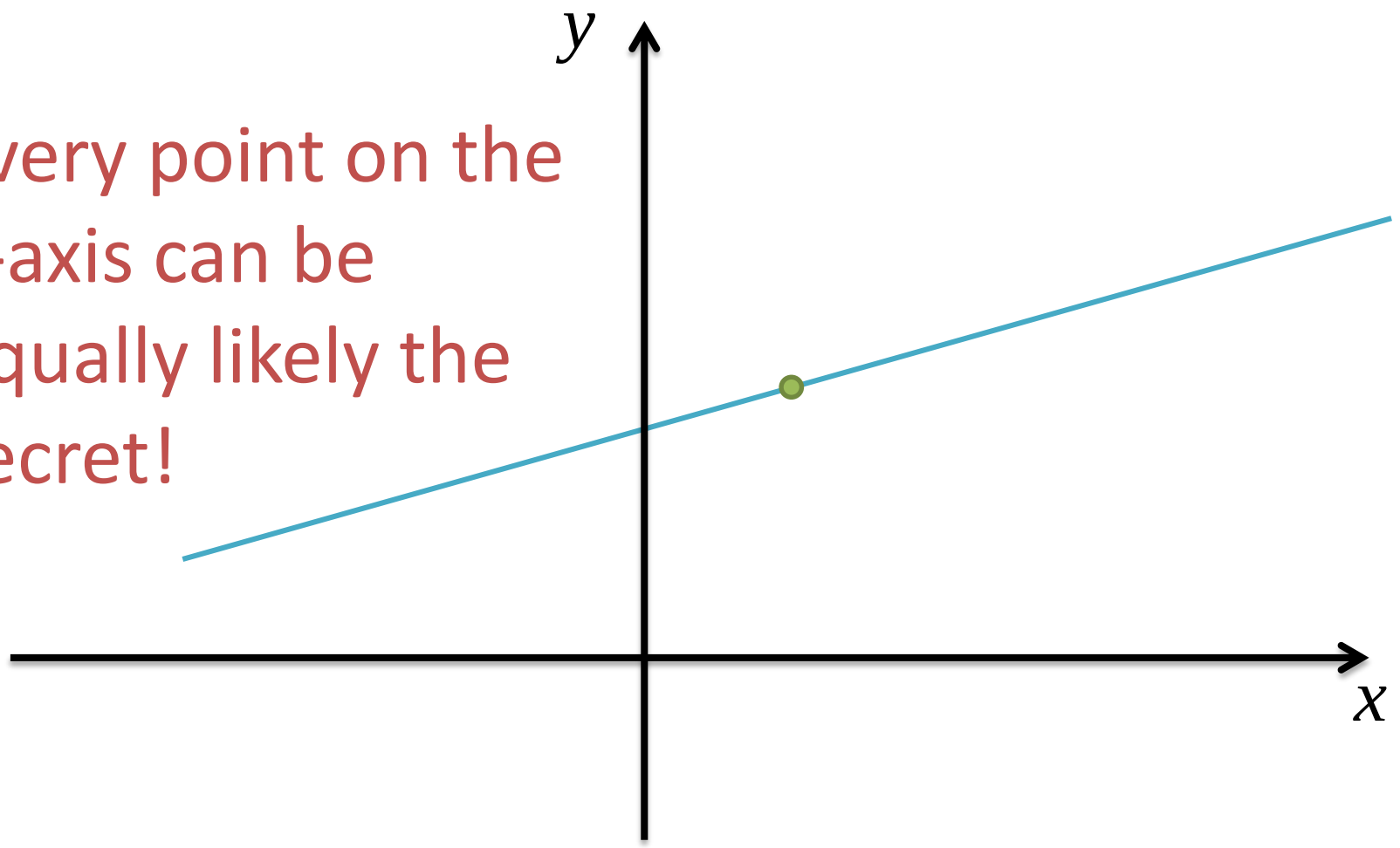
Recover the Secret

1. Two shares uniquely define ***a line***.
2. Intersection of ***this line*** and y-axis is the ***secret***.



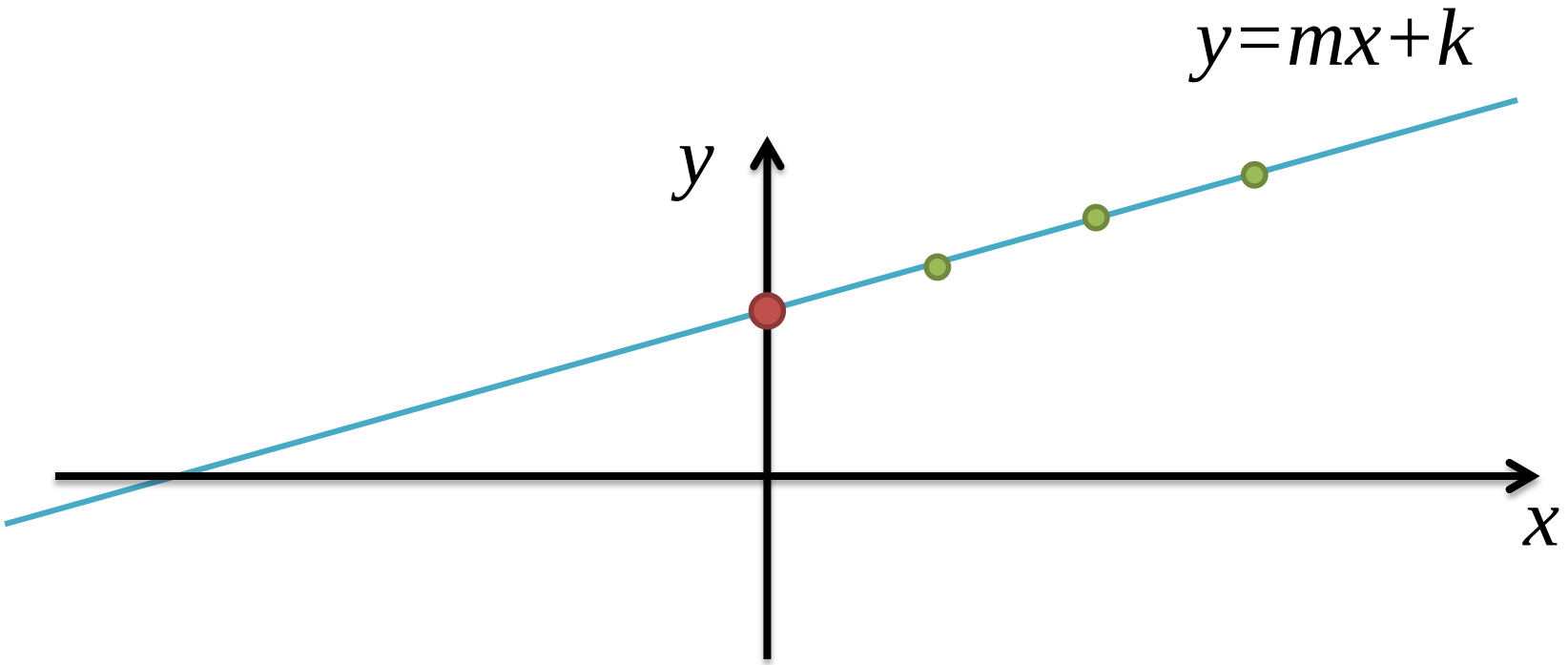
Recover from a Single Share?

Every point on the y-axis can be equally likely the secret!



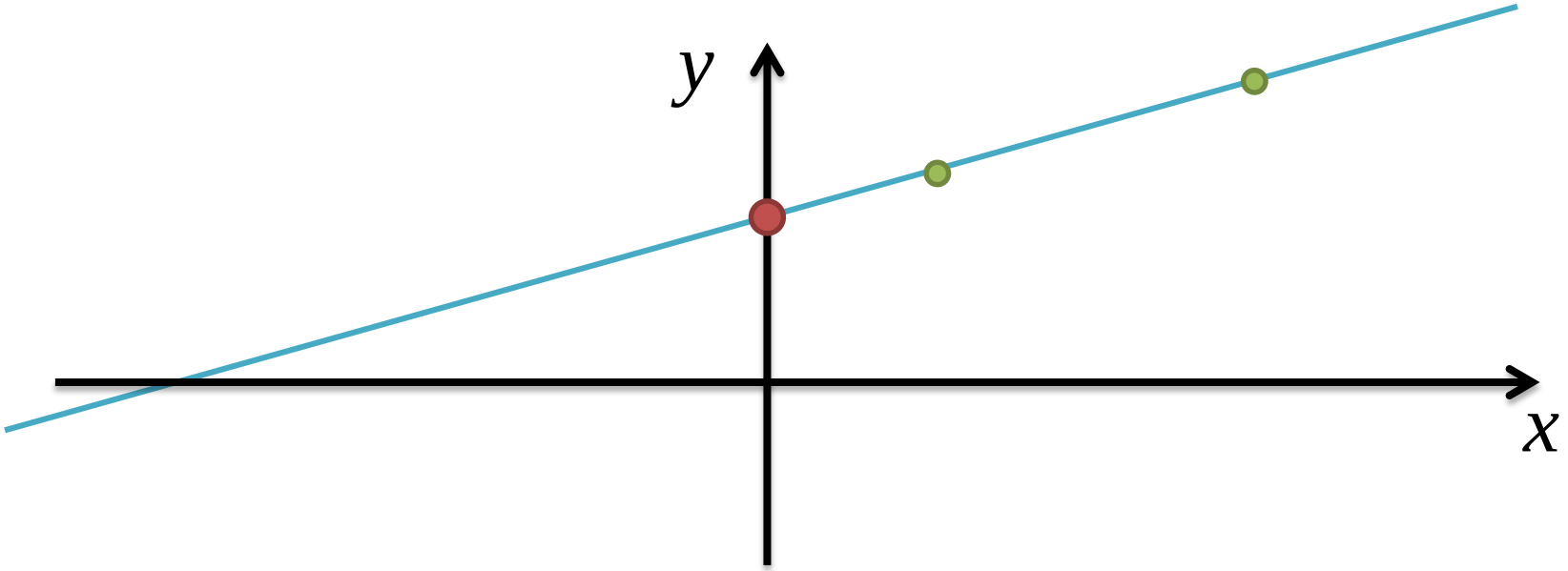
Generate 3 Shares

1. Mark the ***secret*** as a point on the y-axis.
2. Generate a ***random line*** crossing the secret point (0, k).
3. Pick the point $(1, \quad m+k)$ --- the 1st ***share***.
4. Pick the point $(2, 2m+k)$ --- the 2nd ***share***.
5. Pick the point $(3, 3m+k)$ --- the 3rd ***share***.

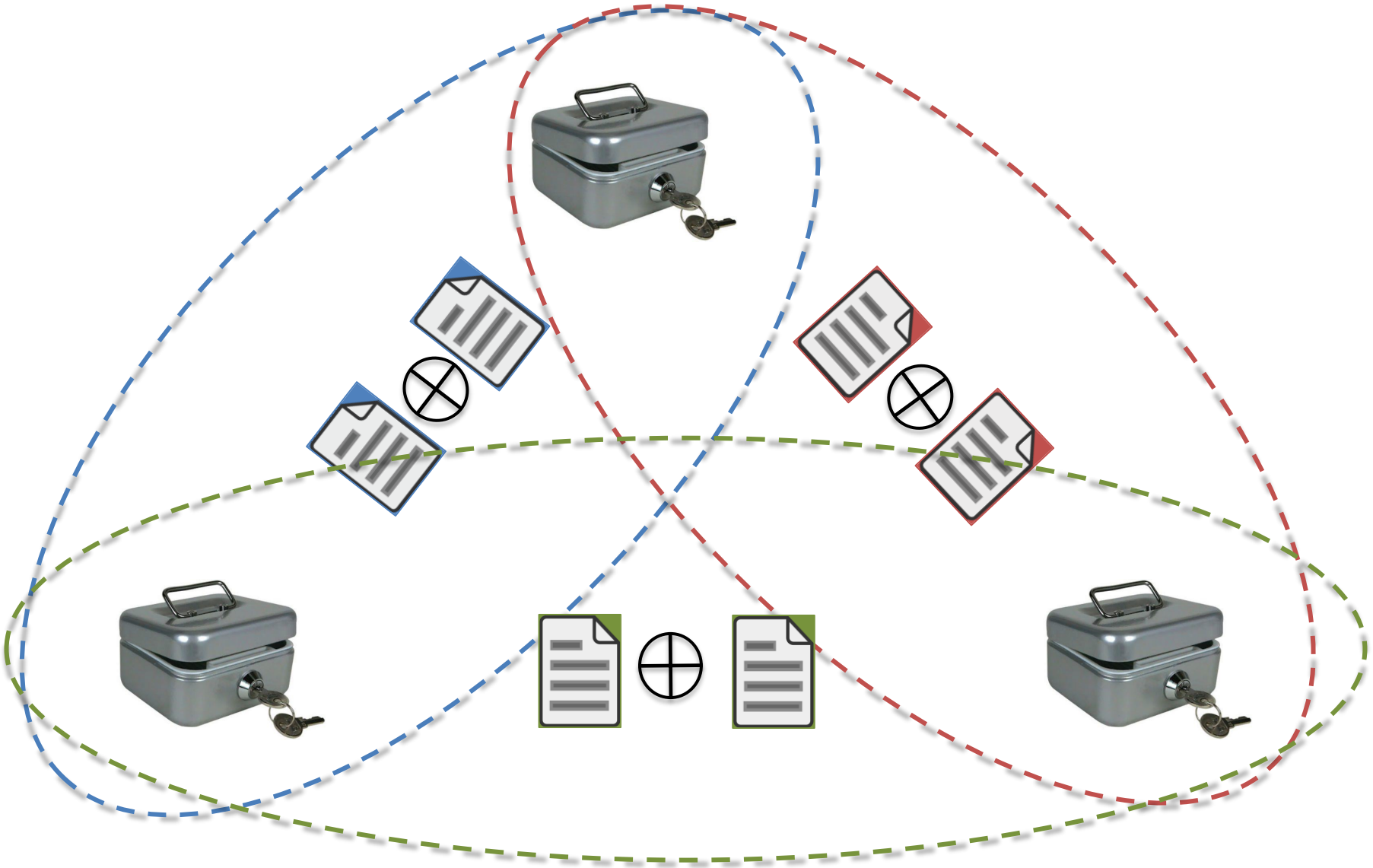


Recover the Secret

1. Any two points (shares) define ***a line***.
2. The intersection of ***the line*** and y-axis is the secret.

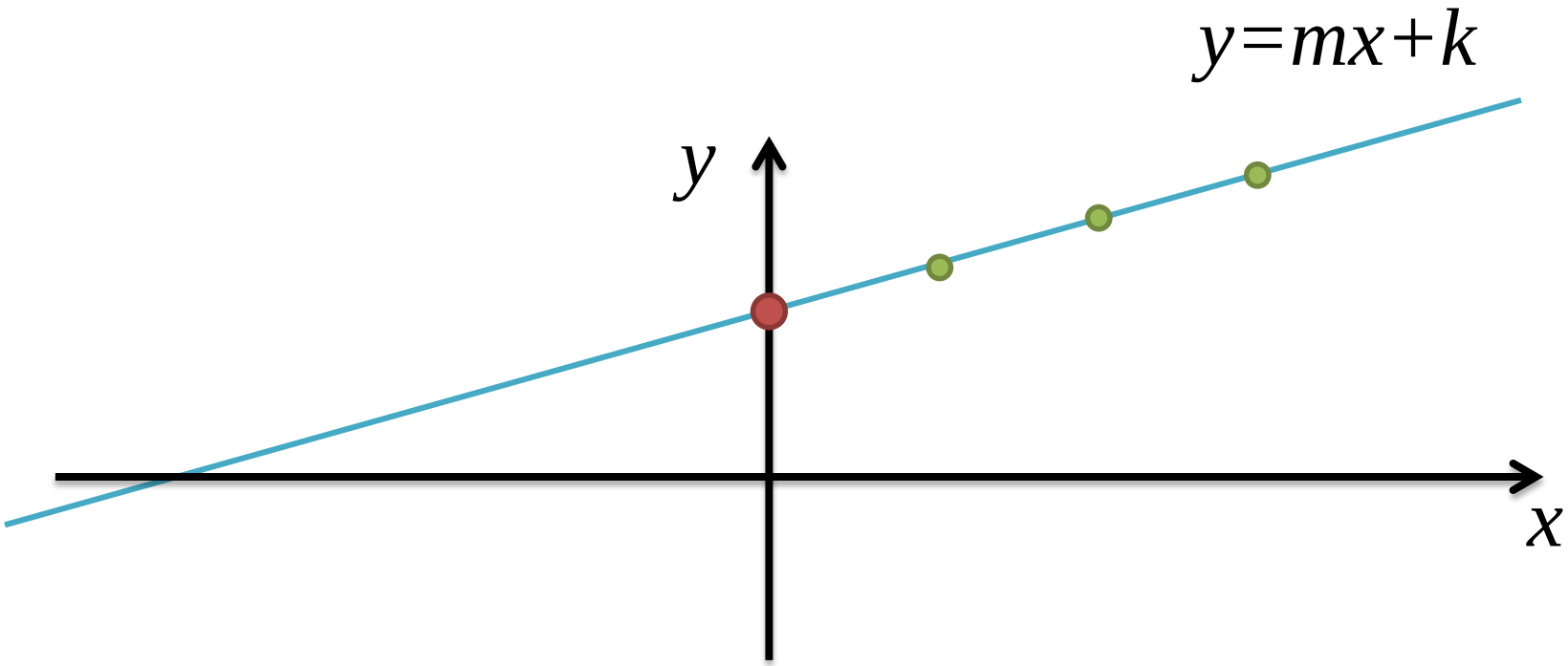


To Share



3 Shares in total, recoverable from 2

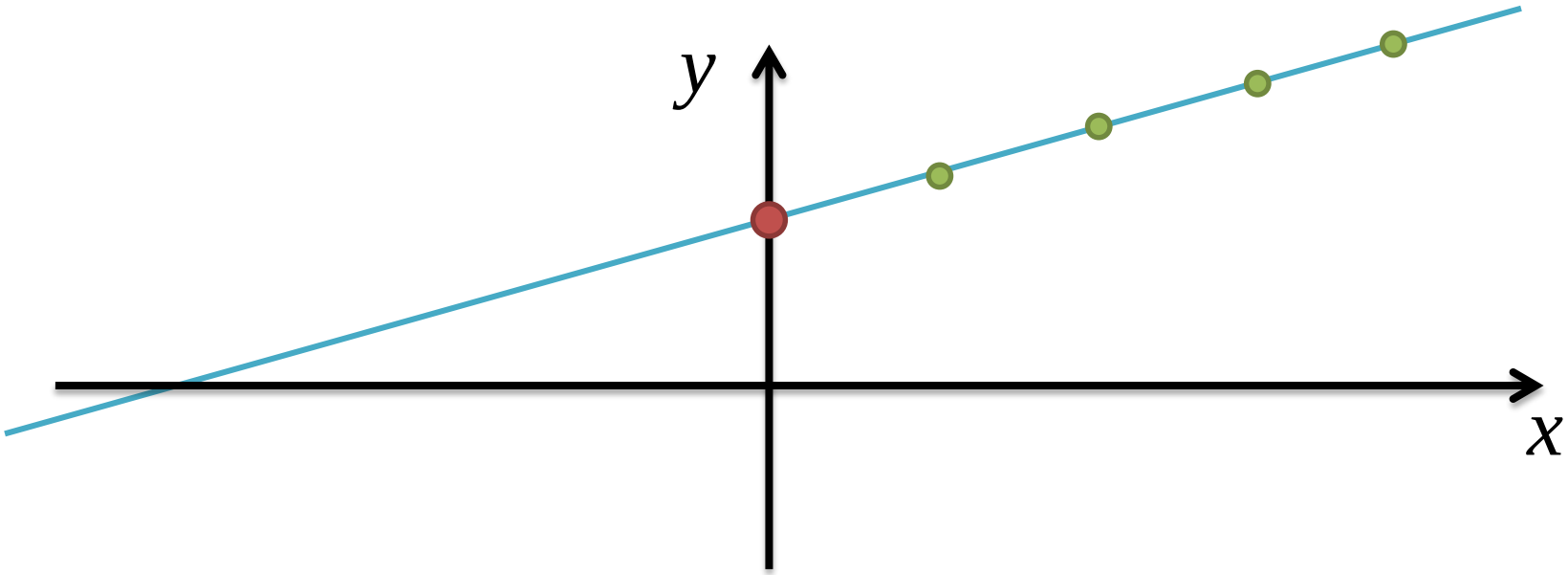
1. Mark the ***secret*** as a point on the y-axis.
2. Generate a ***random line*** crossing the secret point (0, k).
3. Pick the point $(1, \quad m+k)$ --- the 1st ***share***.
4. Pick the point $(2, 2m+k)$ --- the 2nd ***share***.
5. Pick the point $(3, 3m+k)$ --- the 3rd ***share***.



Generate Many Shares

1. Mark the ***secret*** as a point on the y-axis.
2. Generate a ***random line*** crossing the secret point (0, k).
3. Pick the point $(1, \quad m+k)$ --- the 1st ***share***.
4. Pick the point $(2, 2m+k)$ --- the 2nd ***share***.
5. Pick the point $(3, 3m+k)$ --- the 3rd ***share***.
6. Pick the point $(4, 4m+k)$ --- the 4th ***share***.
7. …

$$y=mx+k$$

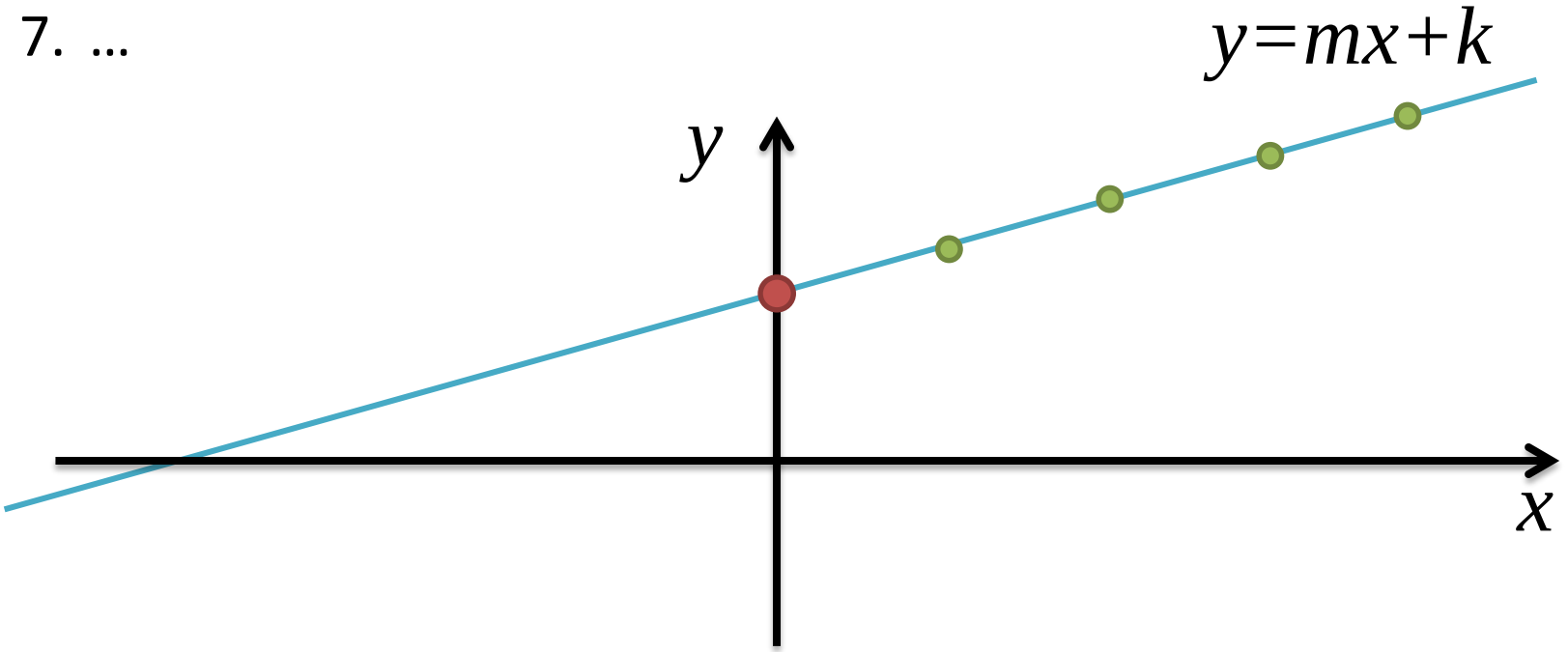


Make it *secure* even if **2** shares are stolen?

Require ***3 shares*** to recover.

Generate Many Shares

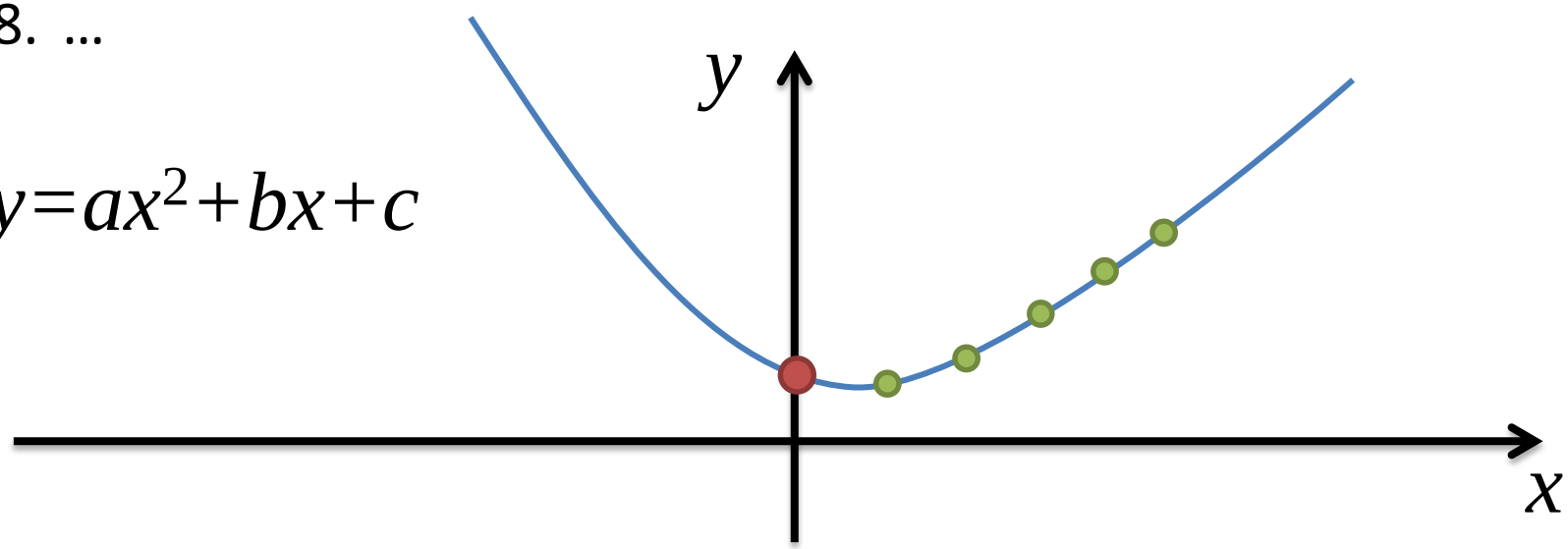
1. Mark the ***secret*** as a point on the y-axis.
2. Generate a ***random line*** crossing the secret point (0, k).
3. Pick the point $(1, \quad m+k)$ --- the 1st ***share***.
4. Pick the point $(2, 2m+k)$ --- the 2nd ***share***.
5. Pick the point $(3, 3m+k)$ --- the 3rd ***share***.
6. Pick the point $(4, 4m+k)$ --- the 4th ***share***.
7. …



Generate the Shares

1. Mark the ***secret*** as a point on the y-axis.
2. Generate a ***random quadratic curve*** crossing the secret point.
3. Pick the point $(1, f(1))$ --- the 1st ***share***.
4. Pick the point $(2, f(2))$ --- the 2nd ***share***.
5. Pick the point $(3, f(3))$ --- the 3rd ***share***.
6. Pick the point $(4, f(4))$ --- the 4th ***share***.
7. Pick the point $(5, f(5))$ --- the 5th ***share***.
8. …

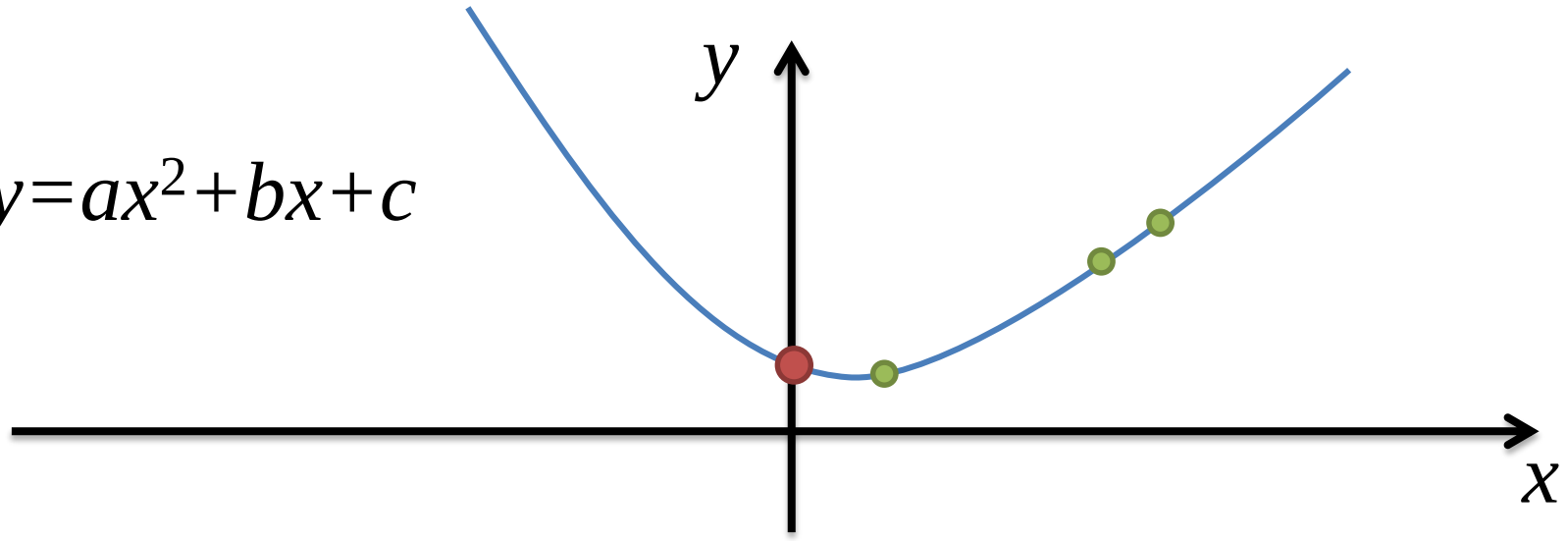
$$y = ax^2 + bx + c$$



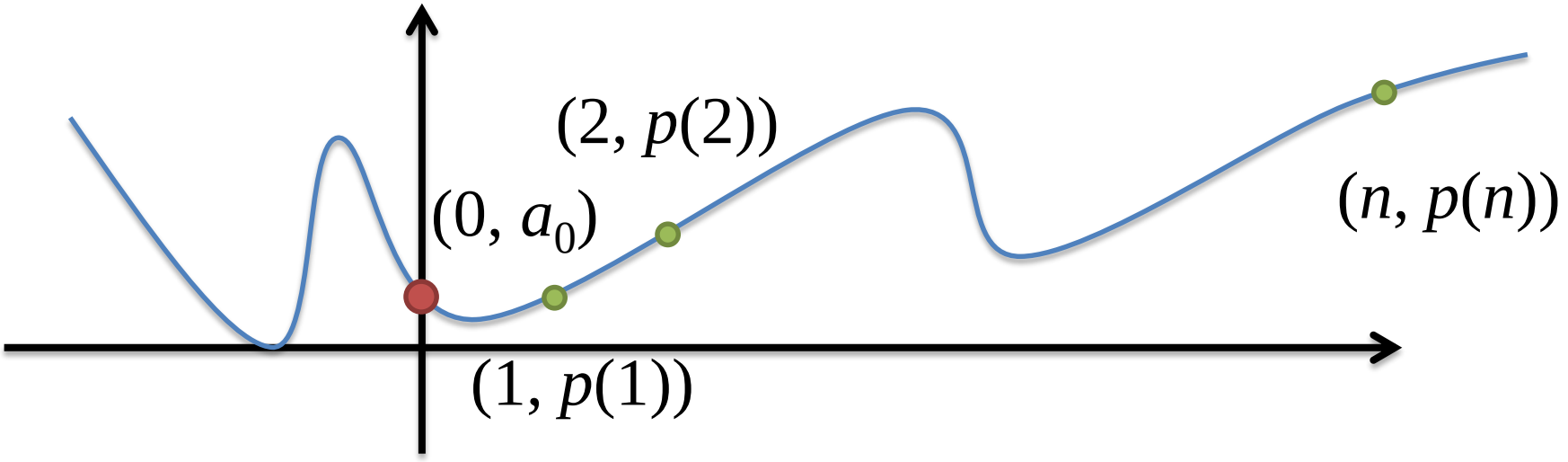
Recover the Secret

1. Any 3 points (shares) uniquely define a ***quadratic*** curve.
2. The intersection of ***the curve*** and y-axis represents the secret.

$$y = ax^2 + bx + c$$



General (n, t) Secret Sharing



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

– The secret: $p(0) = a_0$

In Practice, a_i should come from a Finite Field.

Recover the Secret

- Use any t points to find $p(x)$
  - Solve the t unknown coefficients, a_i , with t equations
  - **Security**: with t-1 shares (i.e, t-1 equations) the linear equation system with t unknowns has infinitely many equally likely solutions

Review

- Scissors don’t hide your secret
- XOR
  - Can be done *visually*
- Polynomial
  - Adjustable utility/security