Shamir's secret sharing

Computer & network security, a.y. 2014-15

Prof. Fabrizio d'Amore

sharing a secret

- assume a **secret** *S* is given
  - password, code, PIN, passphrase, any string…
- goal: sharing *s* with *n* subjects by consigning some data (fragment) to each of them
  - none of them knows *S*
  - they can reconstruct *s* (only) by "joining" the fragments they hold
- applications: boards of directors, nuclear weapons control, shutdown sequences, joint bank accounts, consensus etc.
  - all authorised members must agree
- can be *easily implemented* in an **information-theoretically secure** mode
  - cannot be broken even if adversary has infinite computing power

sharing *S* with *n* subjects

Assume:

S is given as a sequence of bits (unsigned integer)

$n \geq 2$

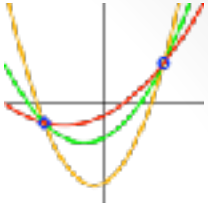
Algorithm (uses xor operation ^)

- randomly generate fragments (nonces) $s_1, \ldots, s_{n-1}$
- set $s_n = S \wedge s_1 \wedge s_2 \wedge \ldots \wedge s_{n-1}$

hence $S = s_1 \wedge s_2 \wedge \ldots \wedge s_n$

- S can be reconstructed by xoring the n fragments
- If attacker knows $n' < n$ fragments he cannot reconstruct S (not enough information)
- Knowing $n' < n$ fragments does not provide more information than knowing one fragment
- **Information-theoretically secure**

Shamir secret sharing (SSS)



Communications of the ACM 22 (11), 612:613 (1979)

threshold scheme

- given a secret S and a pair (k, n), with $1 < k \leq n$, find n data fragments $s_1, s_2, \ldots, s_n$ such that
  - given any $m \geq k$ fragments it is possible to reconstruct S
  - $m < k$ fragments are not sufficient for reconstructing S
  - reconstruction attempt from k-1 fragments is not easier than reconstruction attempt from 1 fragment
- requirement: information-theoretically secure

case $k = n$: easily solved by xoring nonces (see previous slide)

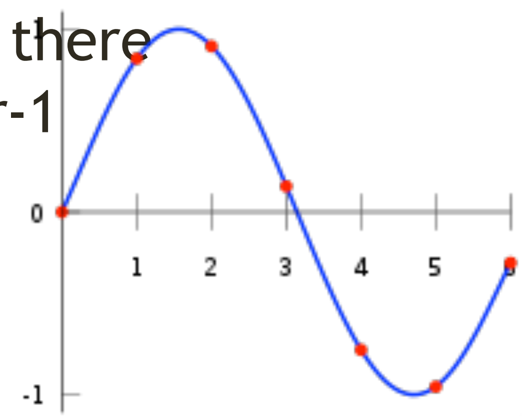
SSS: ingredients for general case

Ingredients

- mod arithmetic and finite fields
- polynomial interpolation

Polynomial interpolation is the *interpolation* of a given data set by a polynomial and is based on the following **unisolvence theorem**

Theorem. Given r > 1 points of $\mathbb{R}^2$ there exists a unique polynomial of degree r-1 going exactly through the r points



Theorem also holds for polynomials defined over Galois fields

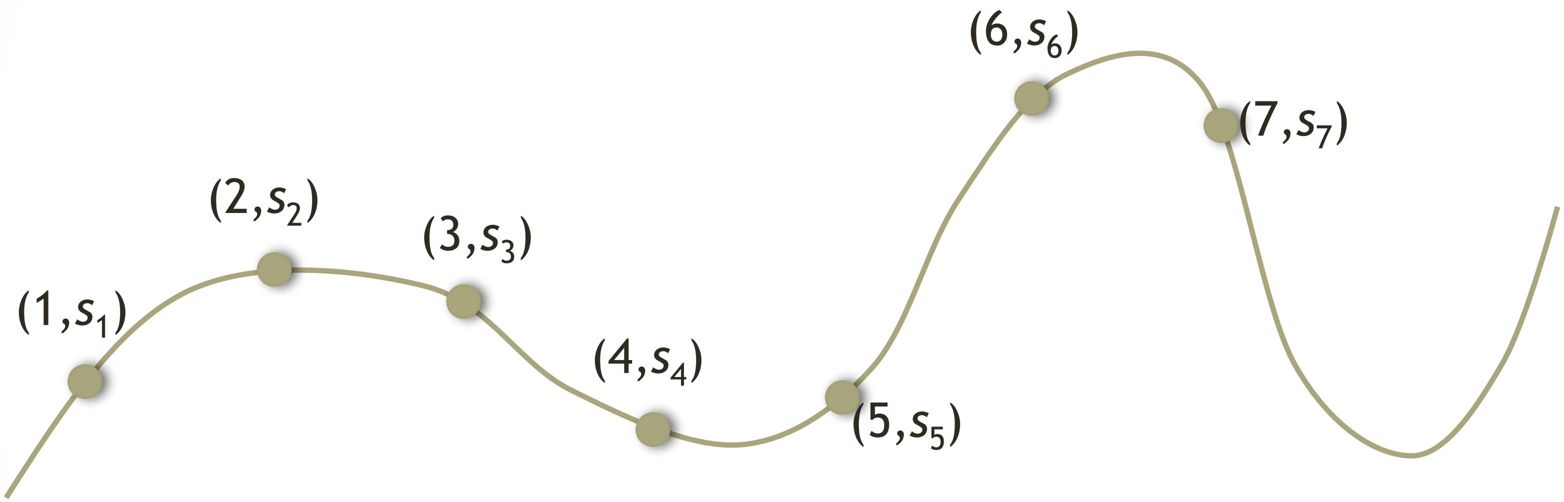
SSS: generation of fragments

- let p be a **prime** ($p > S$, $p > n$)
- randomly choose k-1 integers in $[0, p)$: $a_1, a_2, \ldots, a_{k-1}$; let be $a_0 = S$
- consider polynomial
  $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1 x + a_0 \pmod{p}$
- **let be s_i = P(i)**, for $i = 1, 2, \ldots, n$

by construction it holds P(0) = S

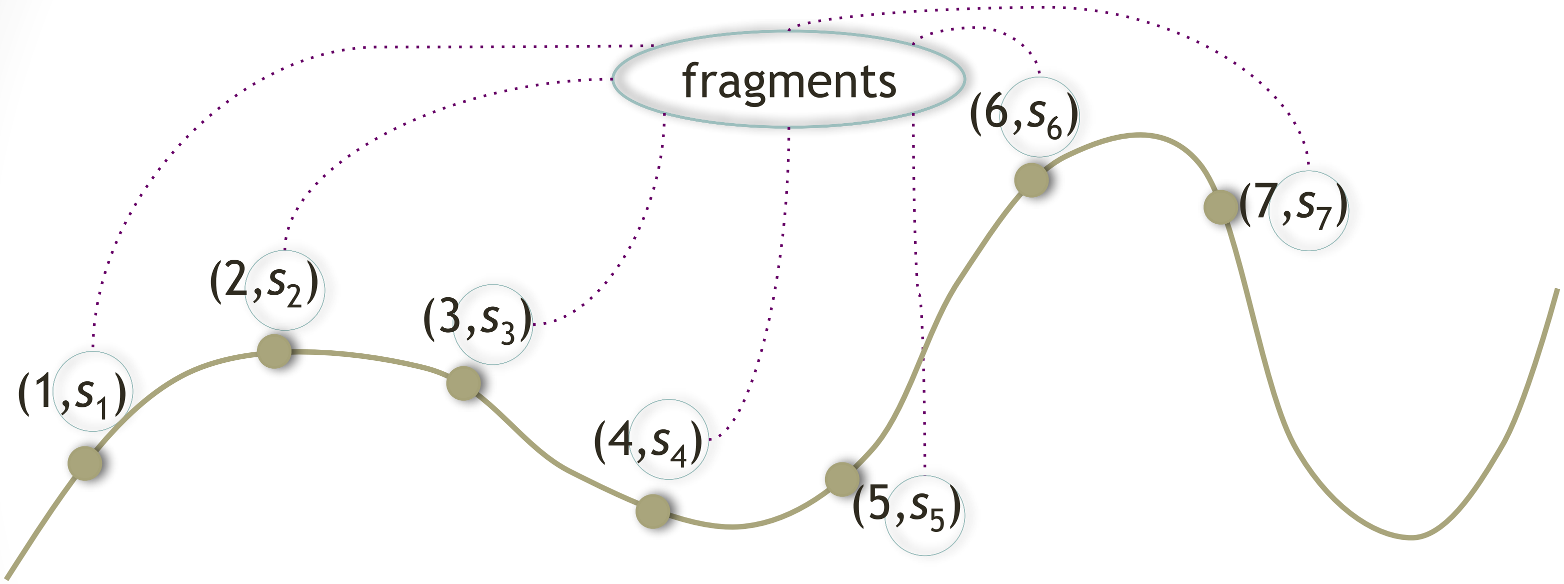
After discarding P(x) and S, only the n points (i, s_i) are known

SSS: the interpolating polynomial



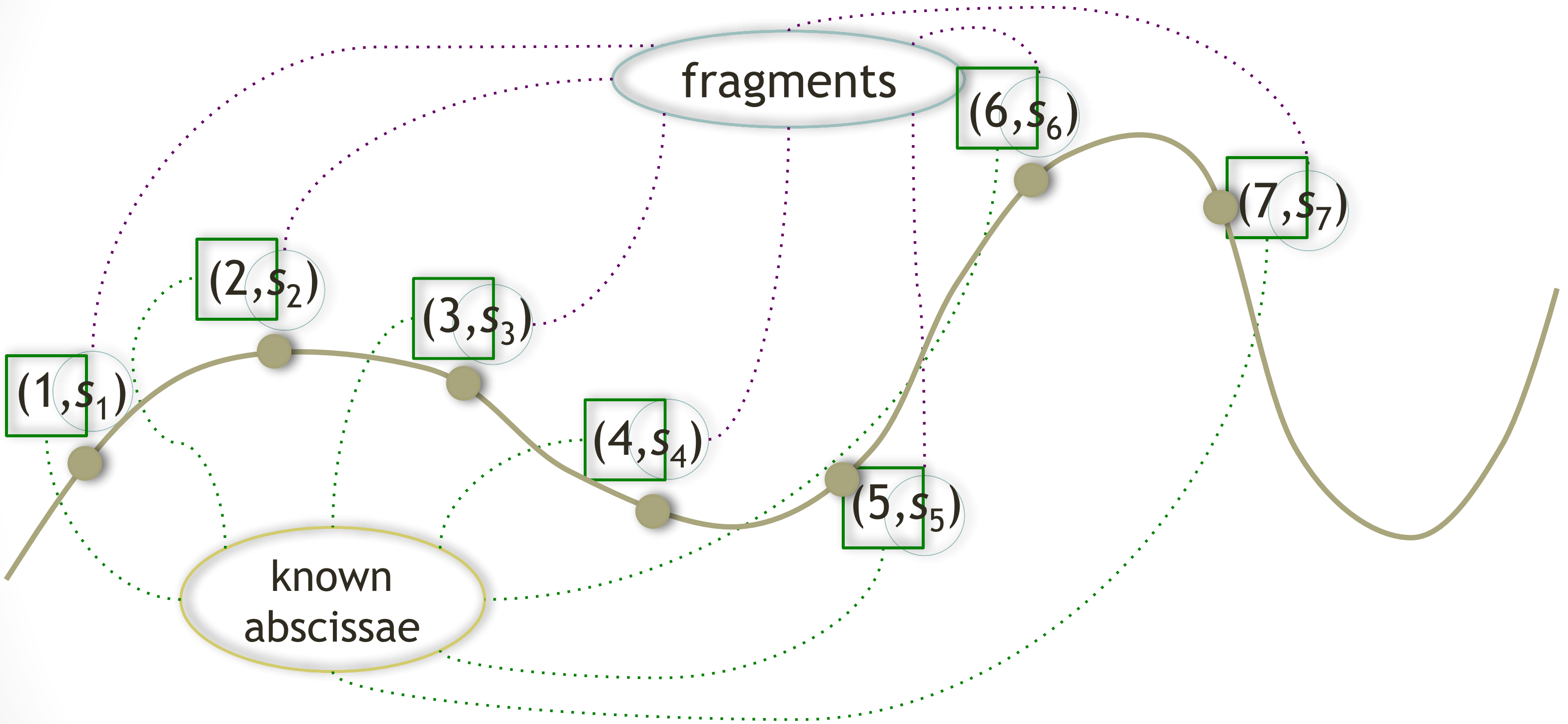
for simplicity, a polynomial on the real plane is showed

SSS: the interpolating polynomial



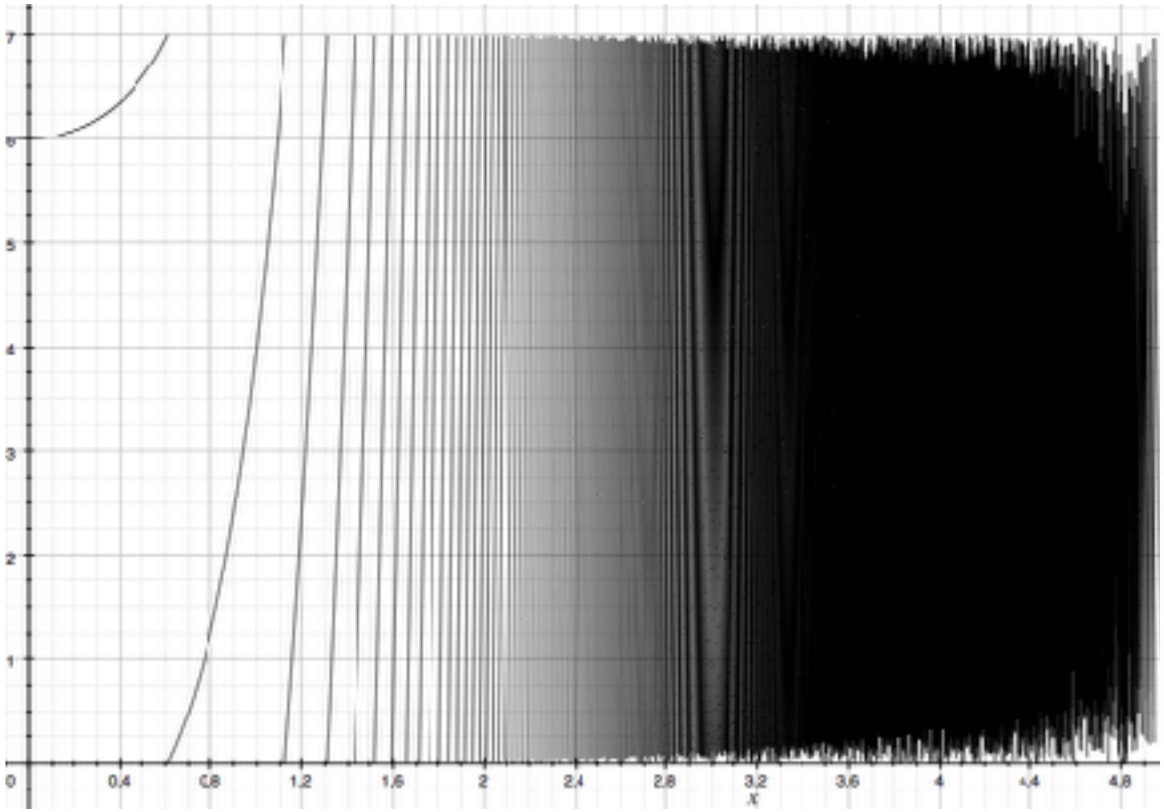
for simplicity, a polynomial on the real plane is showed

SSS: the interpolating polynomial



for simplicity, a polynomial on the real plane is showed

$$y = \left(3x^5 + 2x^2 + 6\right) \bmod 7$$



SSS: reconstructing S

- Given k fragments s_{i_1}, s_{i_2}, …, s_{i_k} find the degree k-1 polynomial going through (i_1, s_{i_1}), (i_2, s_{i_2}), …, (i_k, s_{i_k})
- Use for instance the Lagrange formula (polynomial denoted by L)

Given a set of $k+1$ data points

$$(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)$$

where no two x_j are the same, the interpolation polynomial in the Lagrange form is a linear combination

$$L(x) := \sum_{j=0}^{k} y_j \ell_j(x)$$

(Wikipedia)

of Lagrange basis polynomials

$$\ell_j(x) := \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m} = \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)},$$

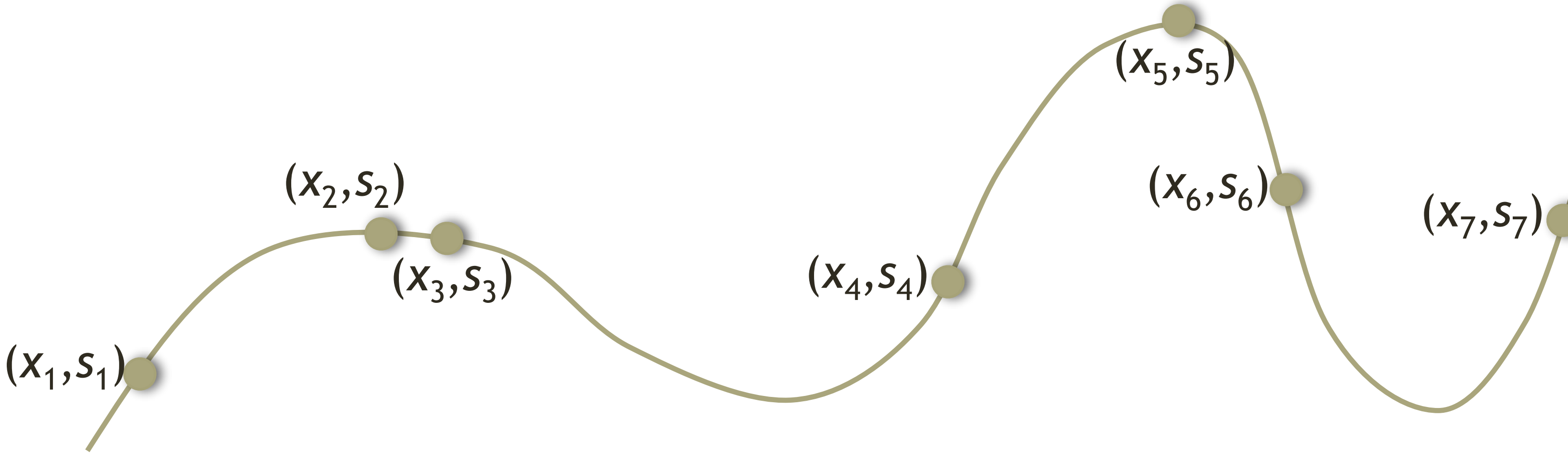
- **Then $S = L(0)$**

properties of SSS

- size of fragments and of secret are upper bounded by size of *p*
  ($|s_i|$, $|S| < |p|$)
- if *k* is kept fixed fragments can be dynamically added/ deleted without affecting the other fragments
- it is straightforward to generate a new set of fragments: randomly build a new polynomial
- we can assign higher weights to members by giving them more than one fragment

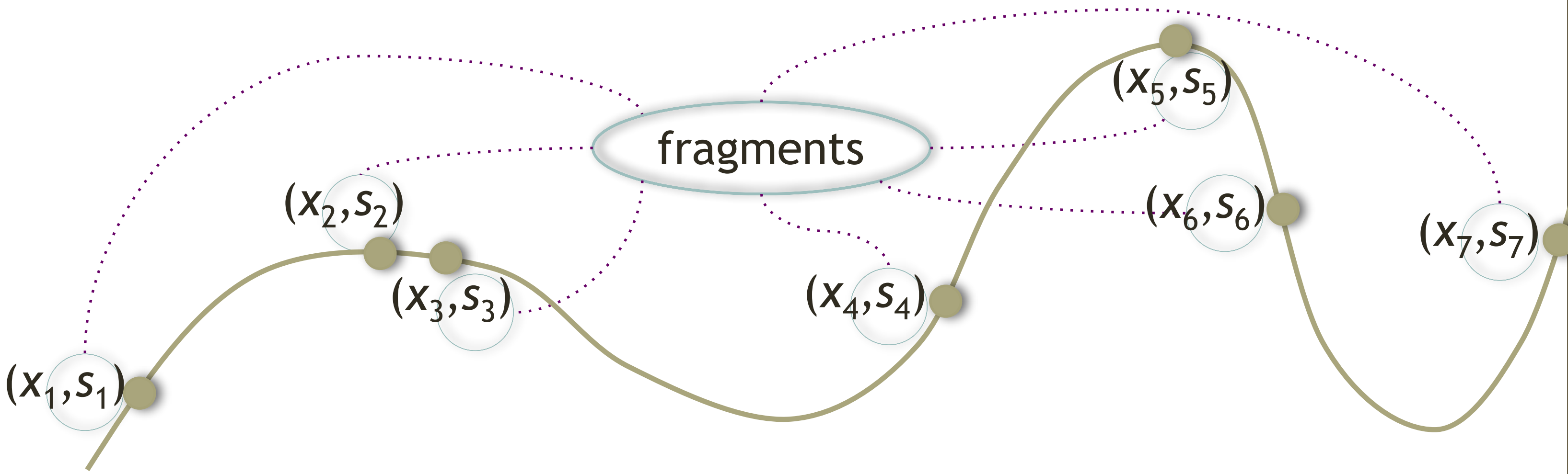
introducing a third party

- use unknown abscissae, given to a **trusted third party**, for additional services



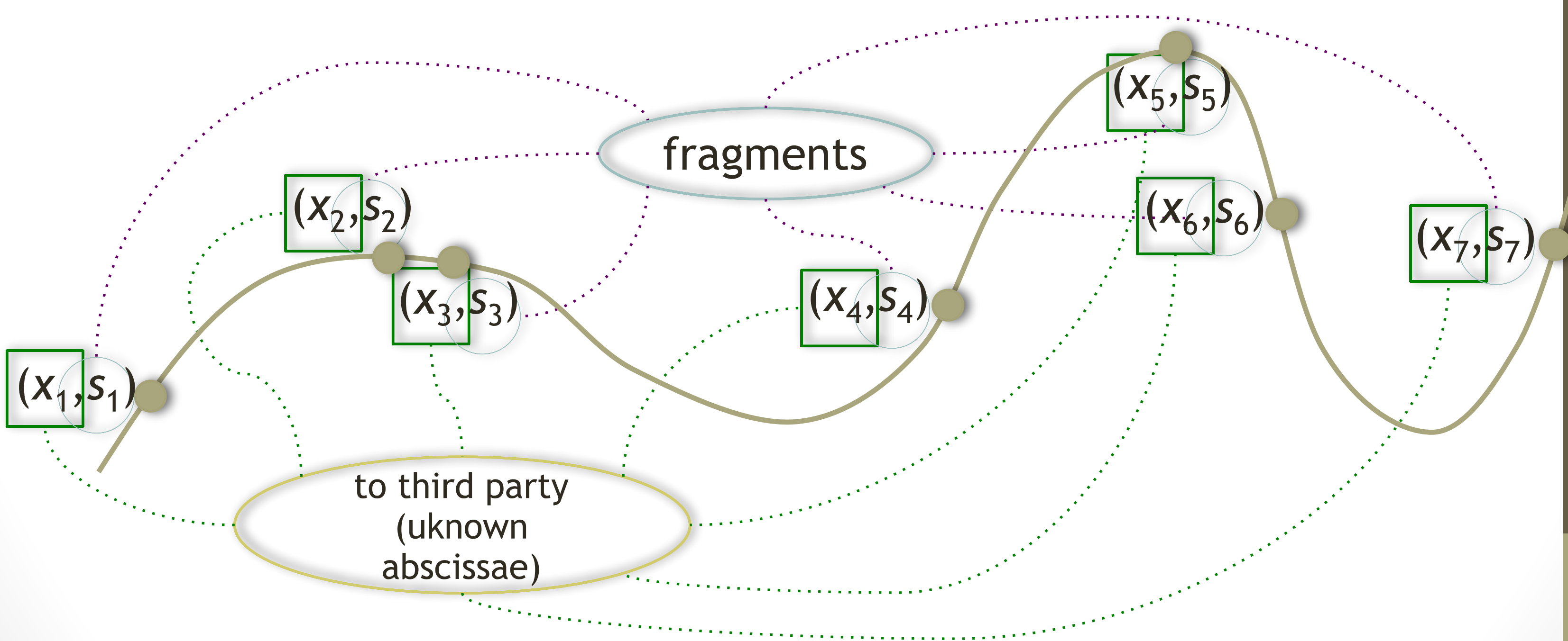
introducing a third party

- use unknown abscissae, given to a **trusted third party**, for additional services



introducing a third party

- use unknown abscissae, given to a **trusted third party**, for additional services



third party: extra services

- gives evidence of reconstruction and identifies the contributors
  - crystal safe-box metaphor
- can recognise possible cheaters (if stores hashes of fragments)
- maintains at least same security as traditional approach
  - if compromised does not reveal the secret