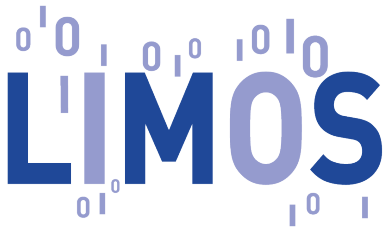
How (not) to Fuzzy Vault?

Axel DURBET

Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS, France
ANR-20-CE39-0005 (project PRIVABIO)

May 11, 2023



Biometric?

Biometric

Definition (CNIL)

"Biometrics groups all the computer techniques that make possible to automatically recognize a person based on his physical, biological or behavioral characteristics. Most of them have the particularity of being unique and permanent (DNA, fingerprints, etc.)."

Table of Contents

Biometric Protocol

Enrollement

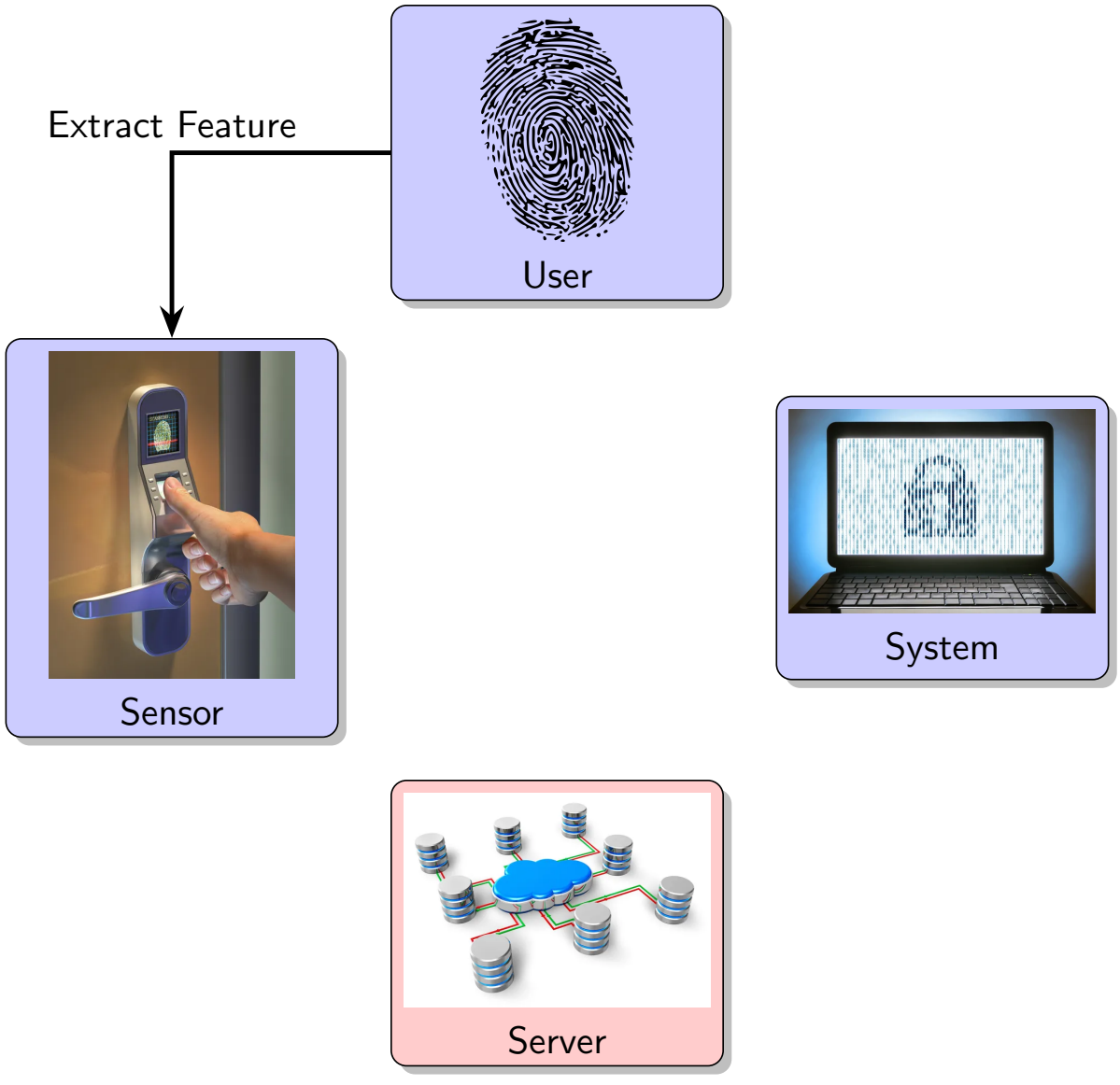
User

Sensor

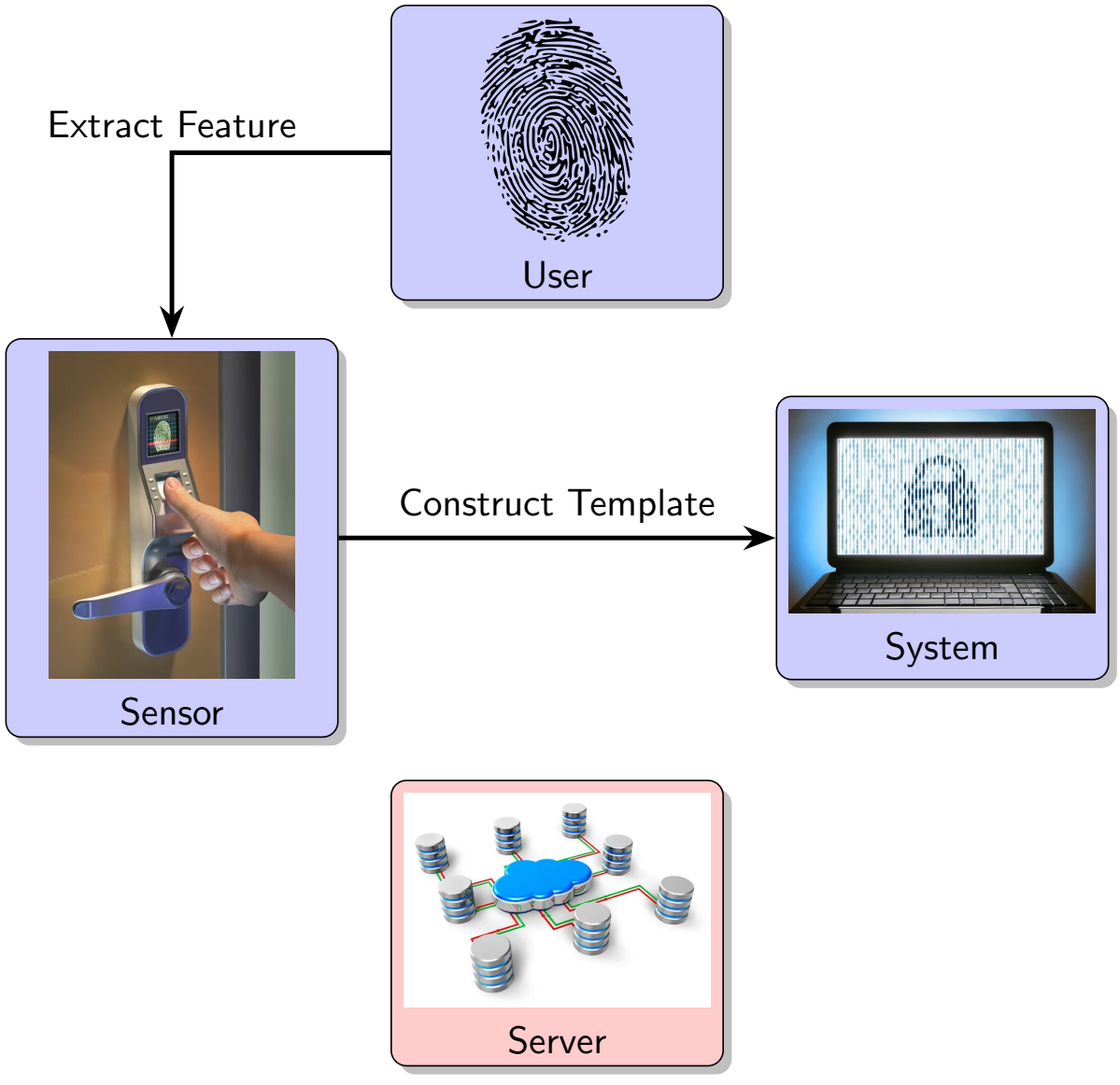
System

Server

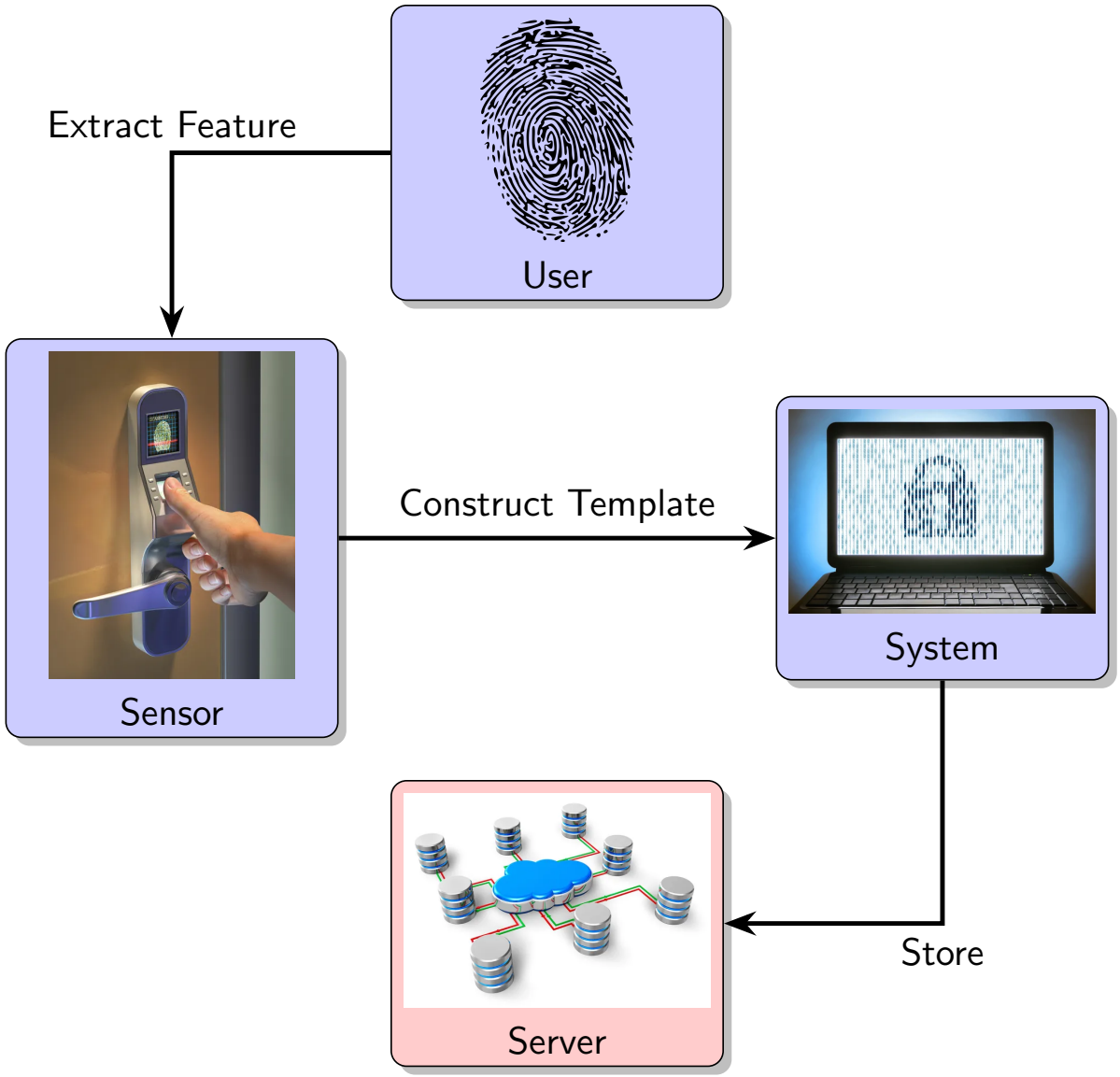
Enrollement



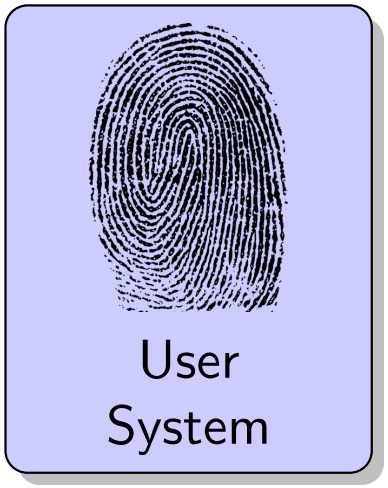
Enrollement



Enrollement



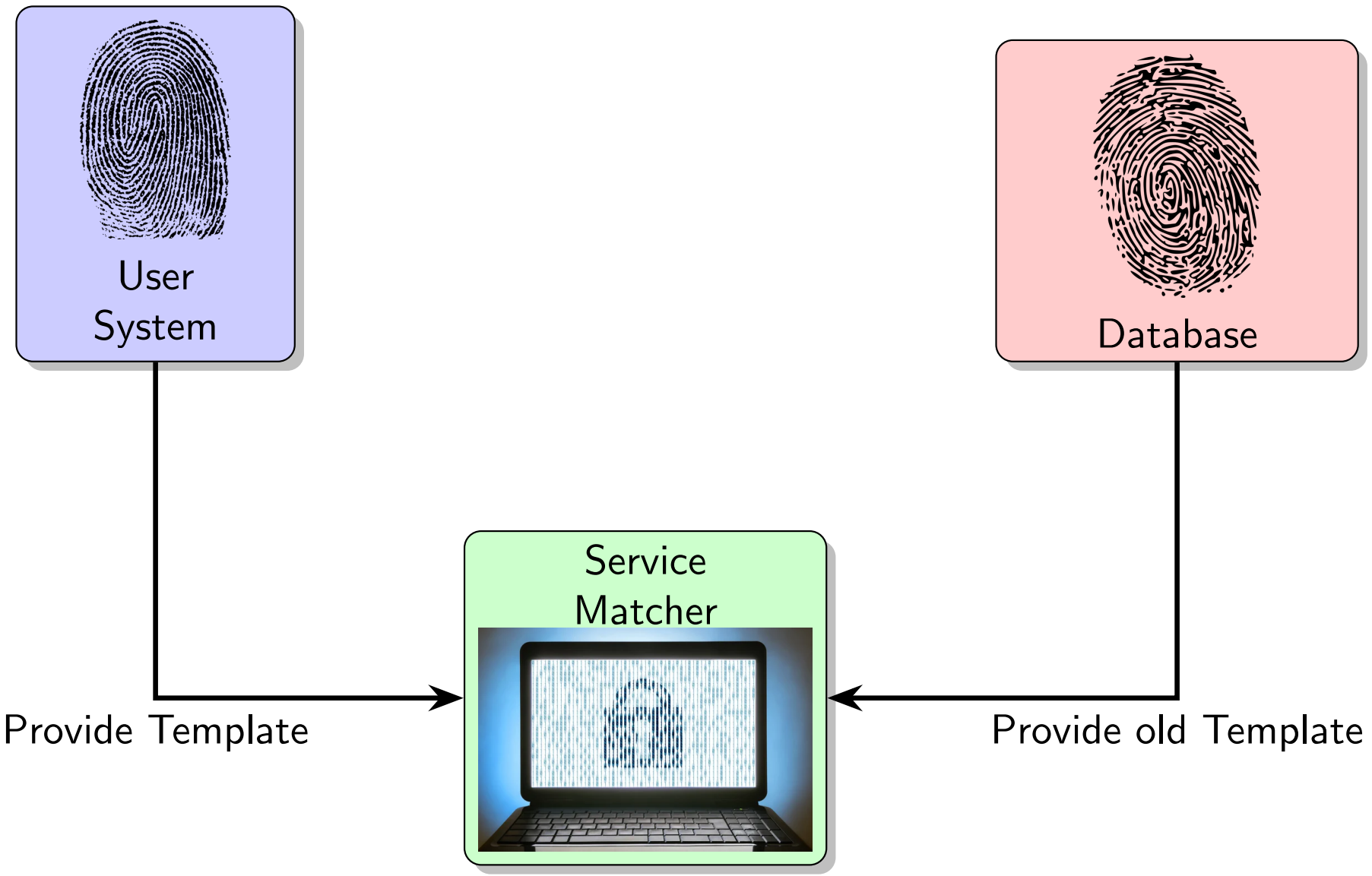
Login



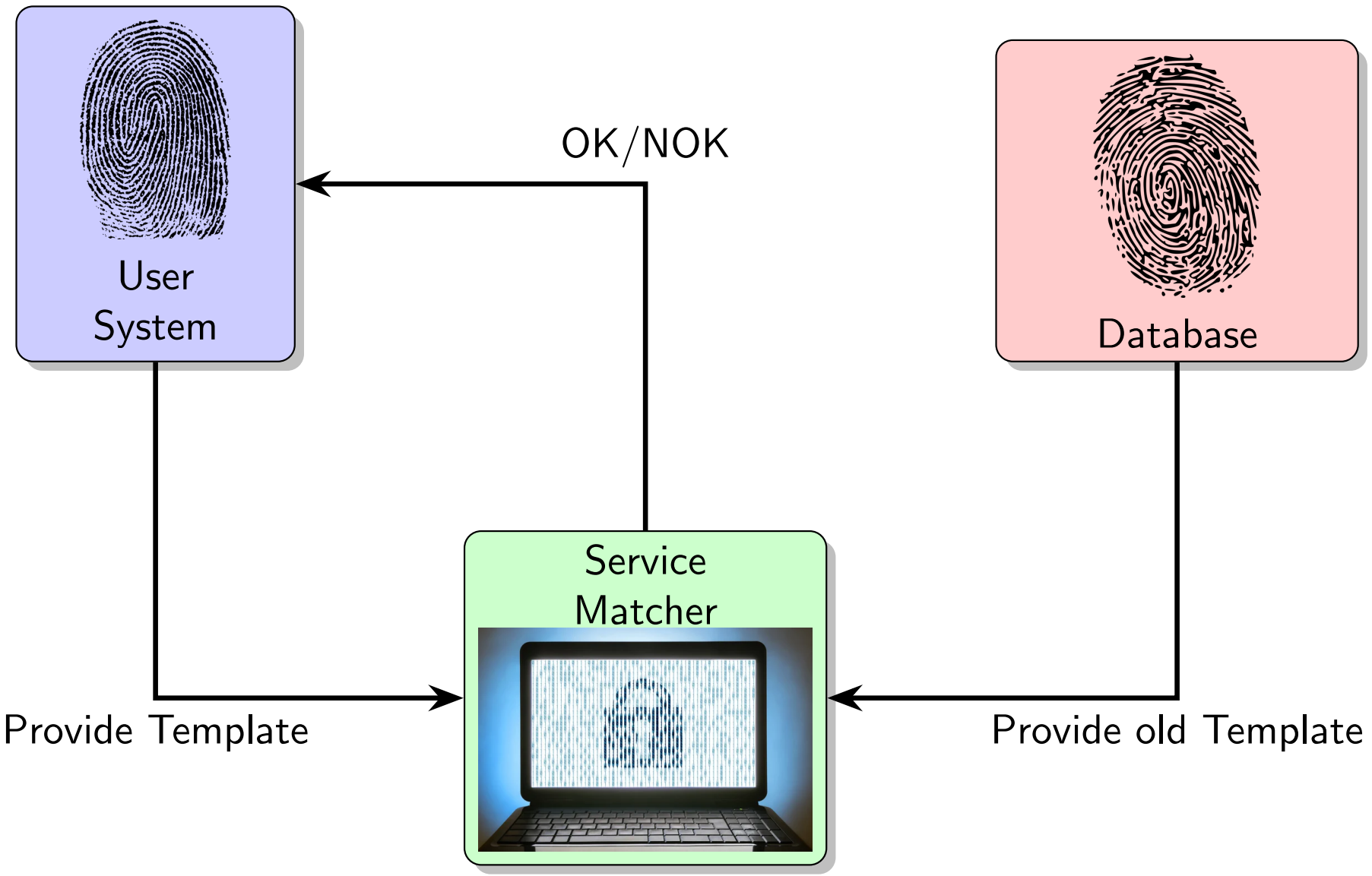
Login

Provide Template

Login


User
System
Database
Service
Matcher
Provide Template
Provide old Template

Login

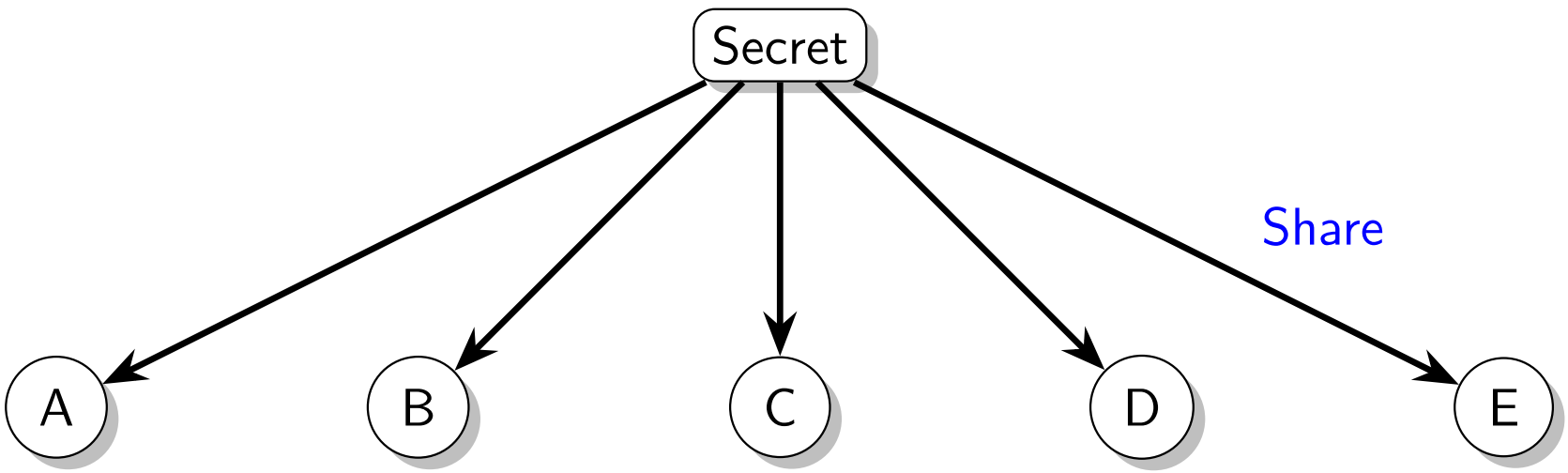

User
System
OK/NOK
Database
Service
Matcher
Provide Template
Provide old Template

Secret Sharing in a Nutshell

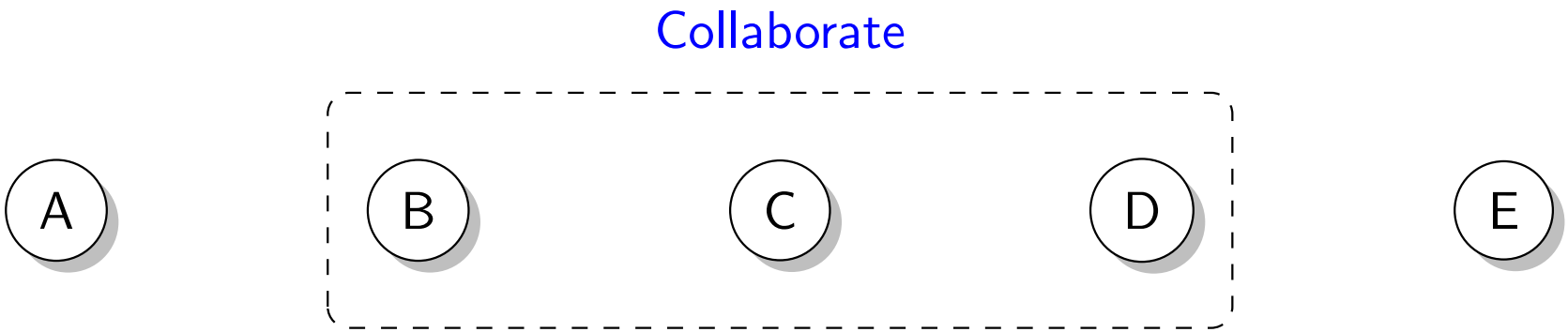
Secret Sharing in a Nutshell

Secret

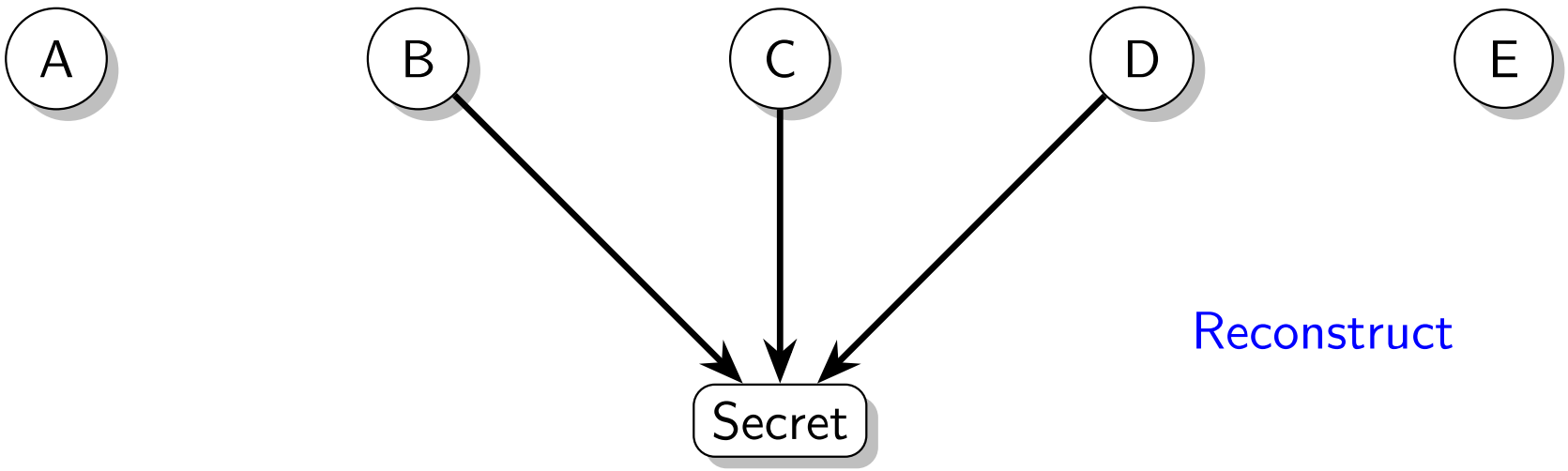
Secret Sharing in a Nutshell



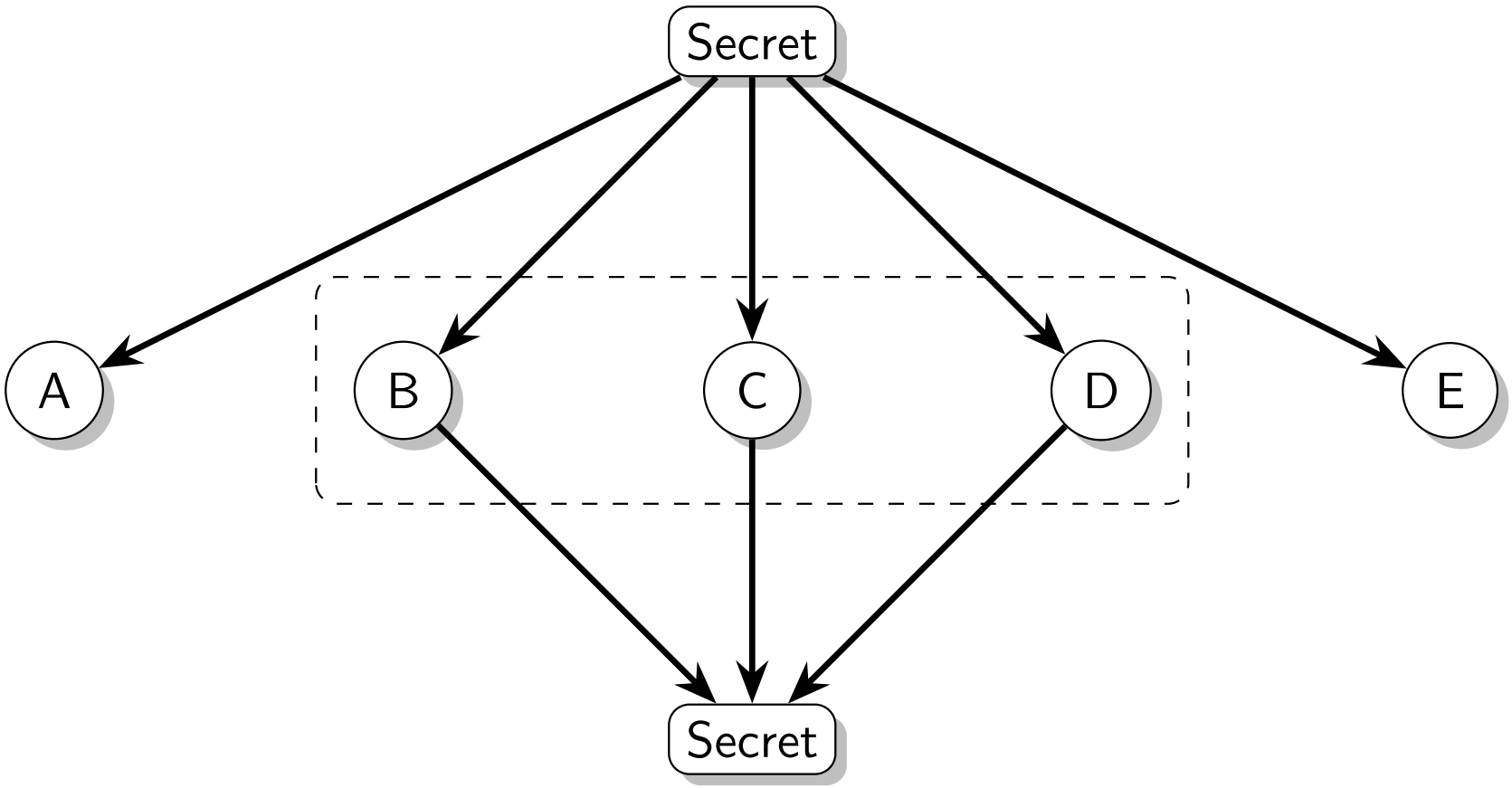
Secret Sharing in a Nutshell



Secret Sharing in a Nutshell

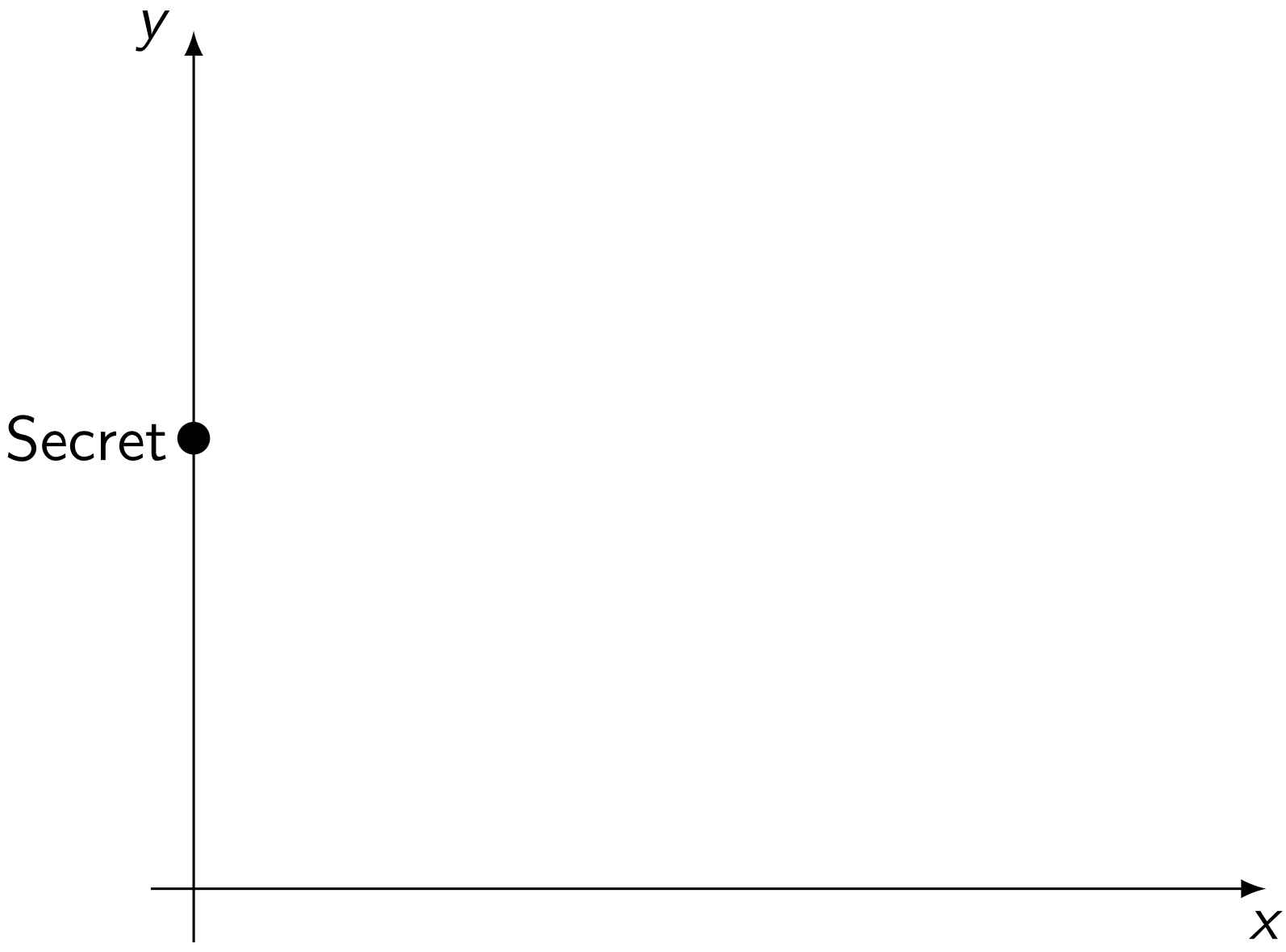


Secret Sharing in a Nutshell

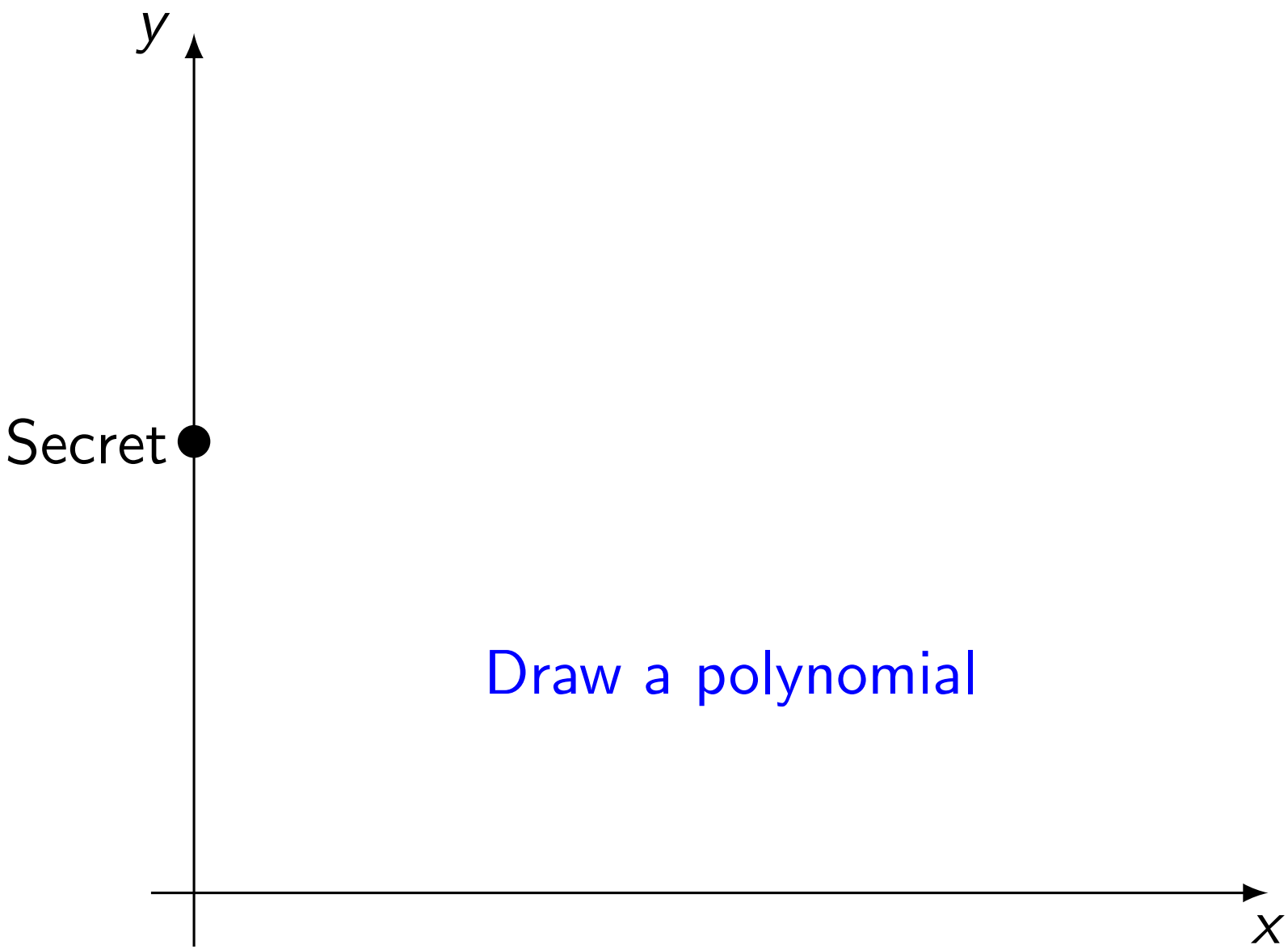


Overview

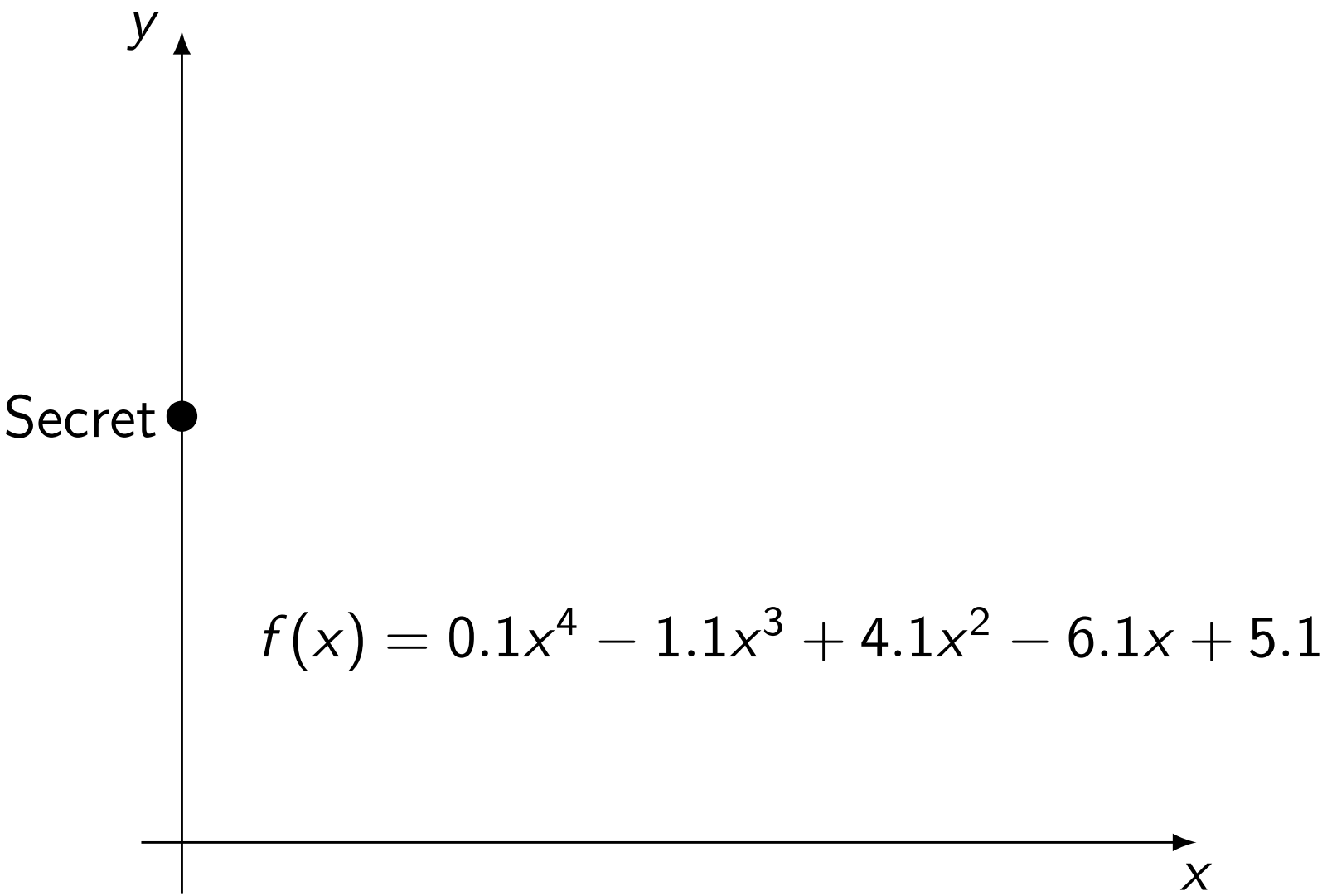
Shamir's Secret Sharing



Shamir's Secret Sharing

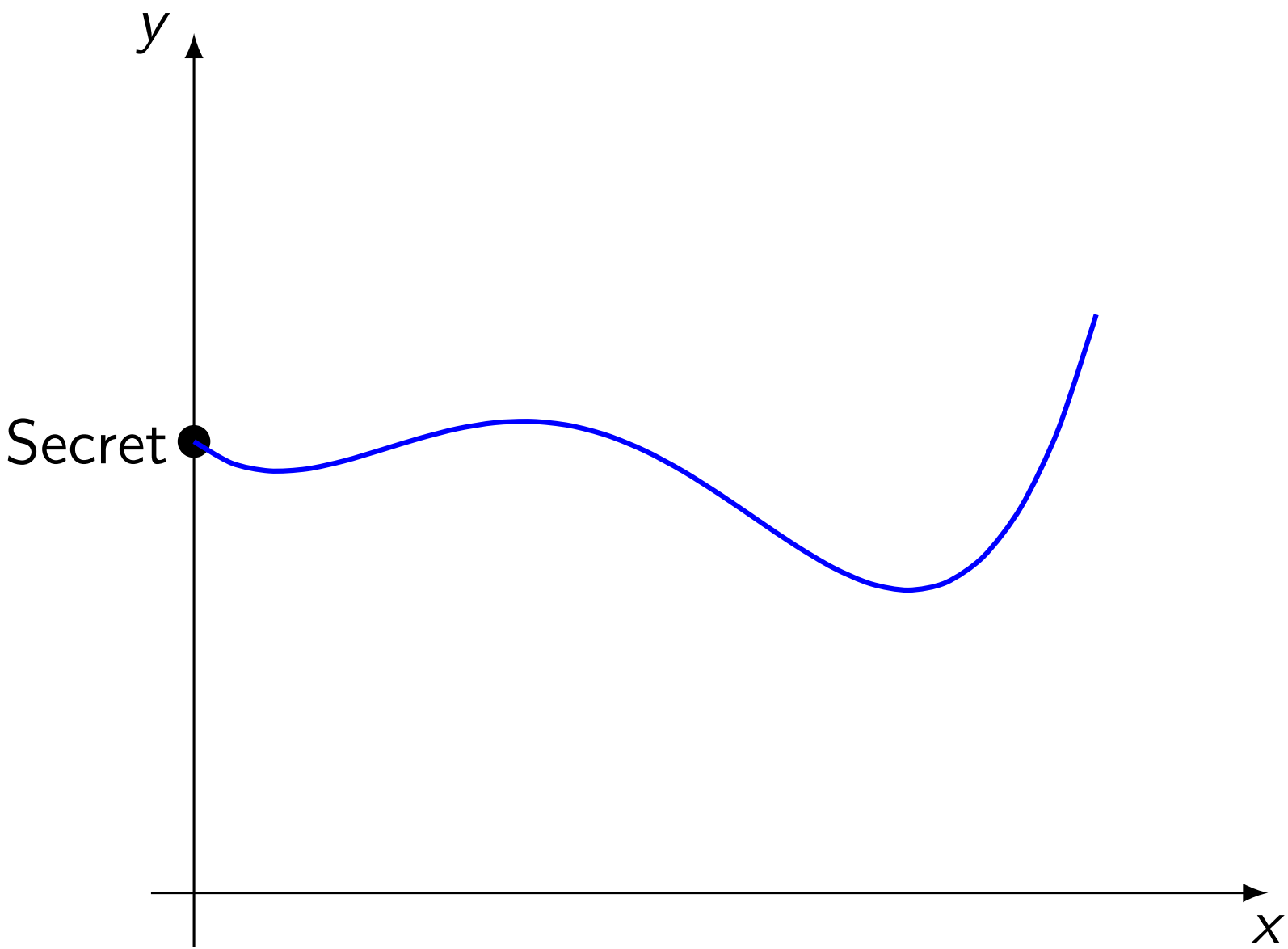


Shamir's Secret Sharing

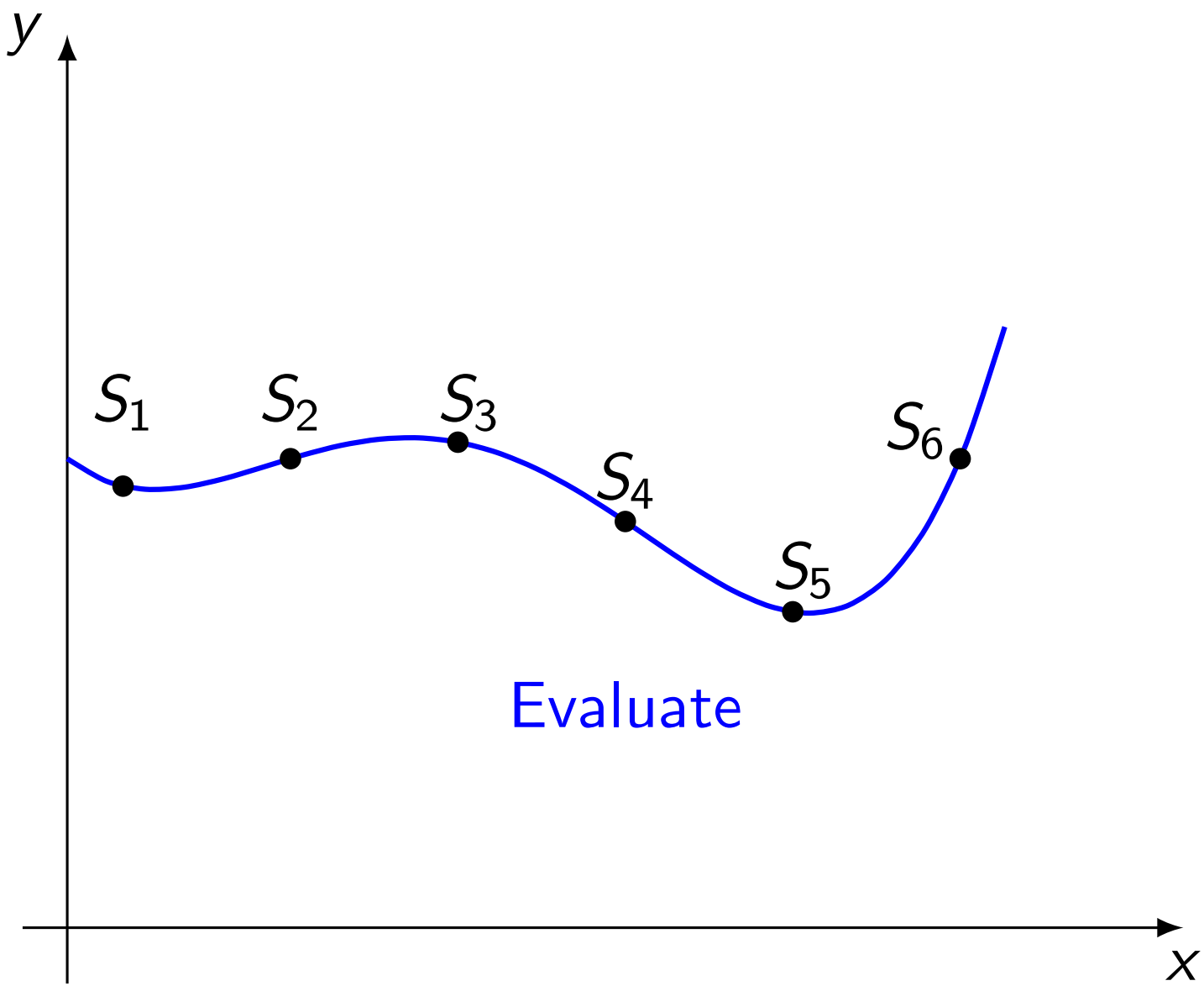


$$f(x) = 0.1x^4 - 1.1x^3 + 4.1x^2 - 6.1x + 5.1$$

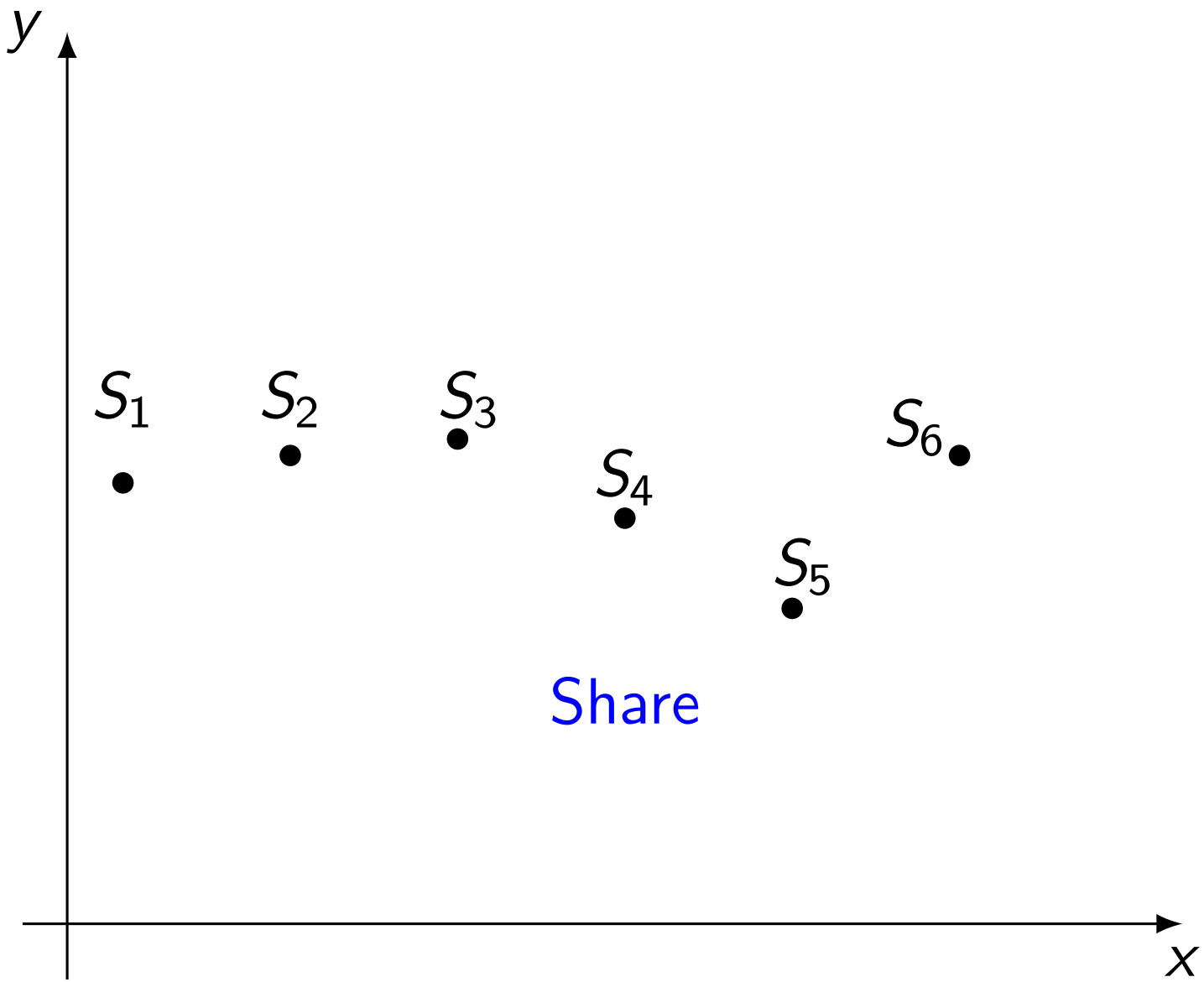
Shamir's Secret Sharing



Shamir's Secret Sharing



Shamir's Secret Sharing



Shamir's Secret Sharing: Recover by solving a system

The users know:

- Some values $(x, f(x))$
- $f(x) = \sum_{i=1}^{n} a_i X^i + Secret$

Solve system with n-unknowns and n-equations system:

$$\begin{cases} f(x_1) & = \sum_{i=1}^{n-1} a_i x_1^i + Secret \\ & \vdots \\ f(x_n) & = \sum_{i=1}^{n-1} a_i x_n^i + Secret \end{cases}$$

Shamir's Secret Sharing: Recover by solving a system

The users know:

- Some values $(x, f(x))$
- $f(x) = \sum_{i=1}^{n} a_i X^i + Secret$

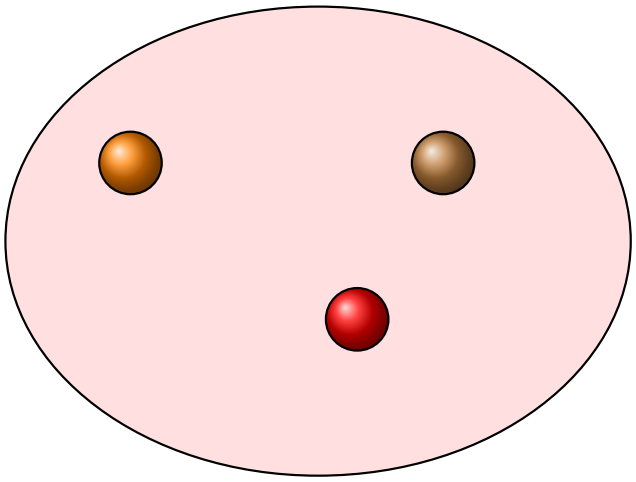
Solve system with n-unknowns and n-equations system:

$$\begin{cases} f(x_1) & = \sum_{i=1}^{n-1} a_i x_1^i + Secret \\ & \vdots \\ f(x_n) & = \sum_{i=1}^{n-1} a_i x_n^i + Secret \end{cases}$$

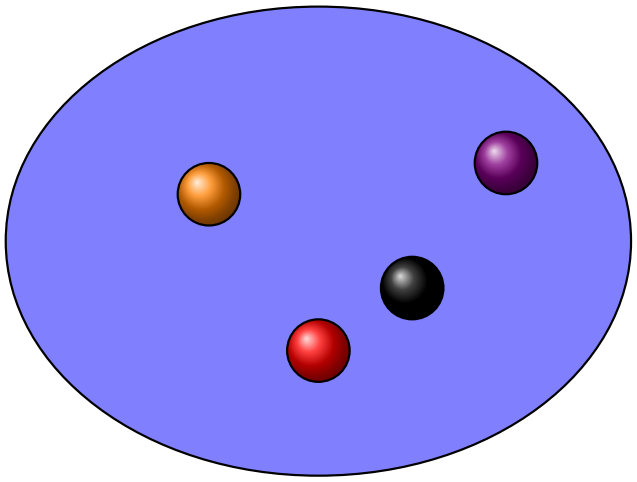
Set Intersection in a Nutshell

Set Intersection in a Nutshell

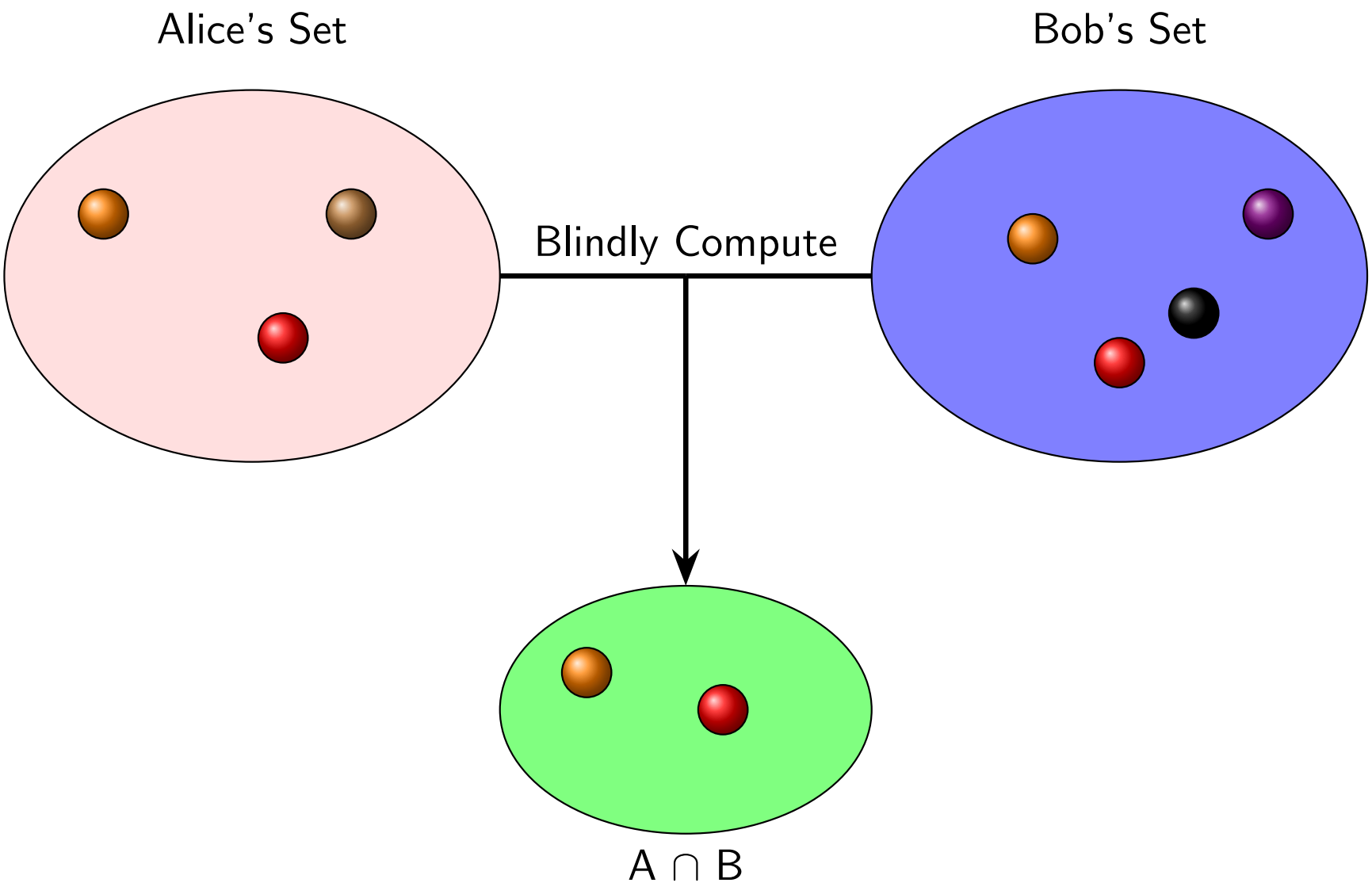
Alice's Set



Bob's Set



Set Intersection in a Nutshell



Fuzzy Vault For Beginners

FV_{Gen}


Chaff Fingerprint

Parameters


Genuine Fingerprint


Secret

polynomial

Genuine Minutiae

Chaff Minutiae

Random number generator

Permutation

Store on the server

FV_{Gen}


Chaff Fingerprint

Parameters


Genuine Fingerprint

1


Secret

polynomial

Genuine Minutiae

Chaff Minutiae

Random number generator

Permutation

Store on the server

FV_{Gen}


Chaff Fingerprint

Parameters

2


Genuine Fingerprint

1


Secret

2

polynomial

Genuine Minutiae

Chaff Minutiae

Random number generator

Permutation

Store on the server

FV_{Gen}


Chaff Fingerprint

Parameters


Genuine Fingerprint

2

1


Secret

2

polynomial

3

Genuine Minutiae

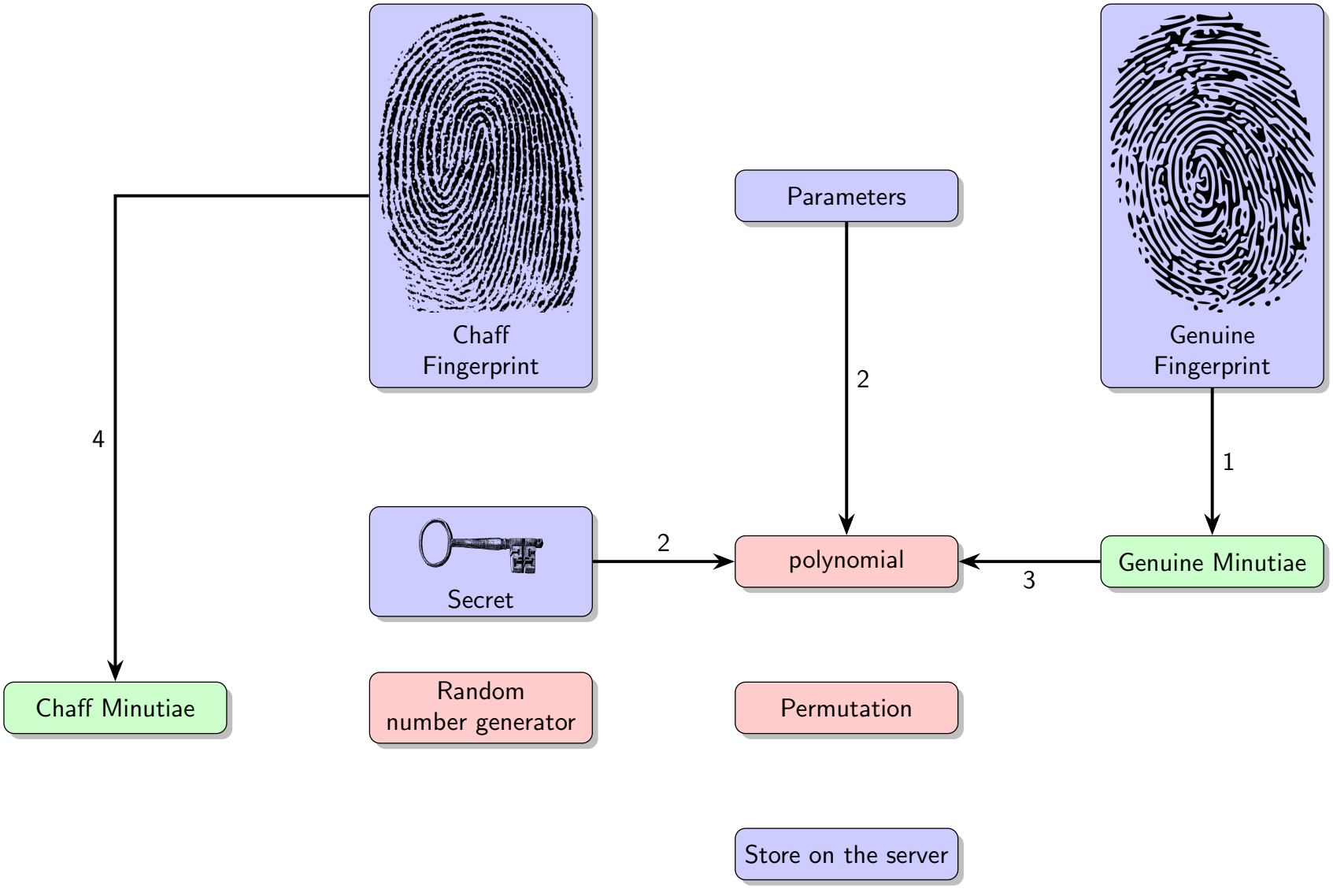
Chaff Minutiae

Random number generator

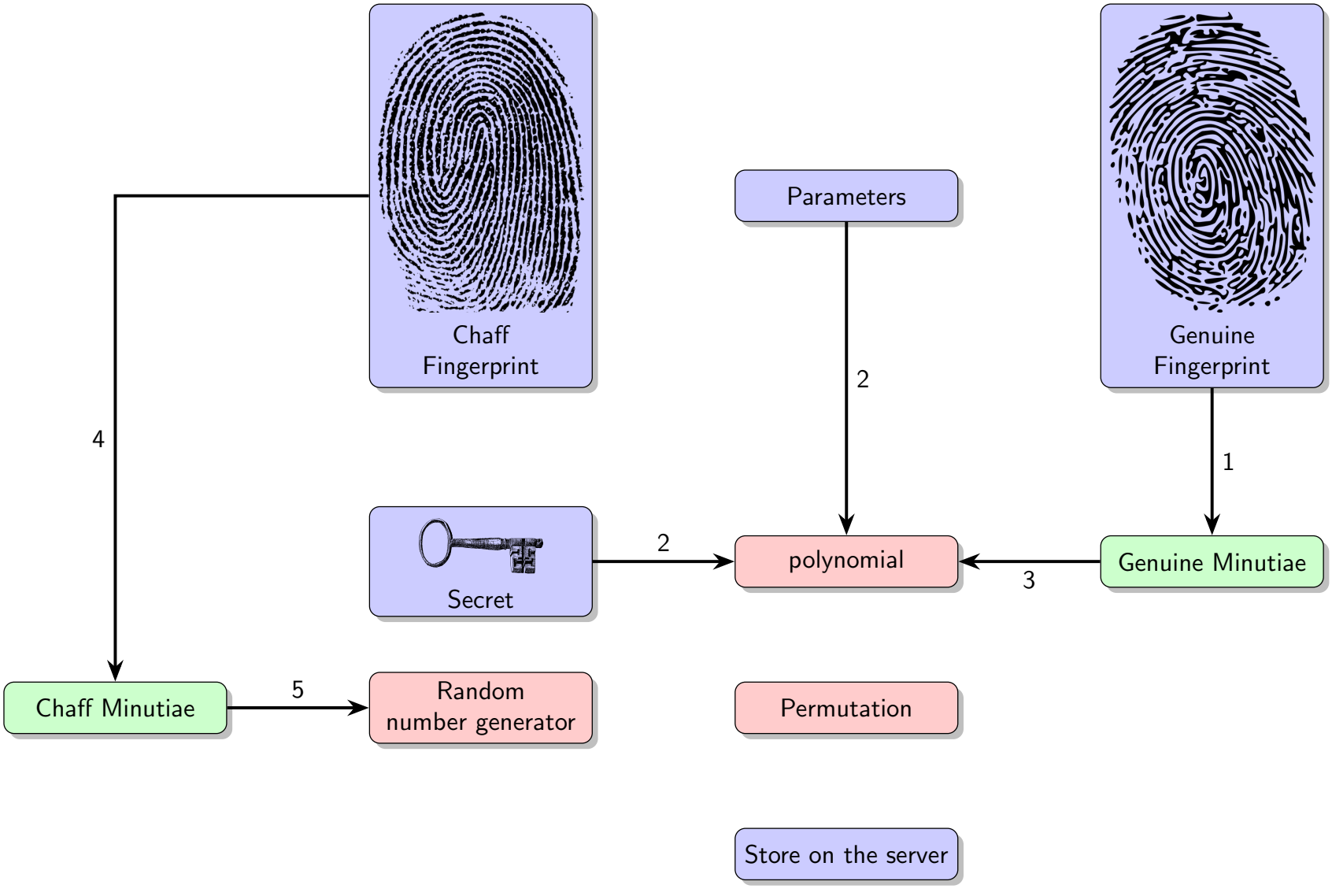
Permutation

Store on the server

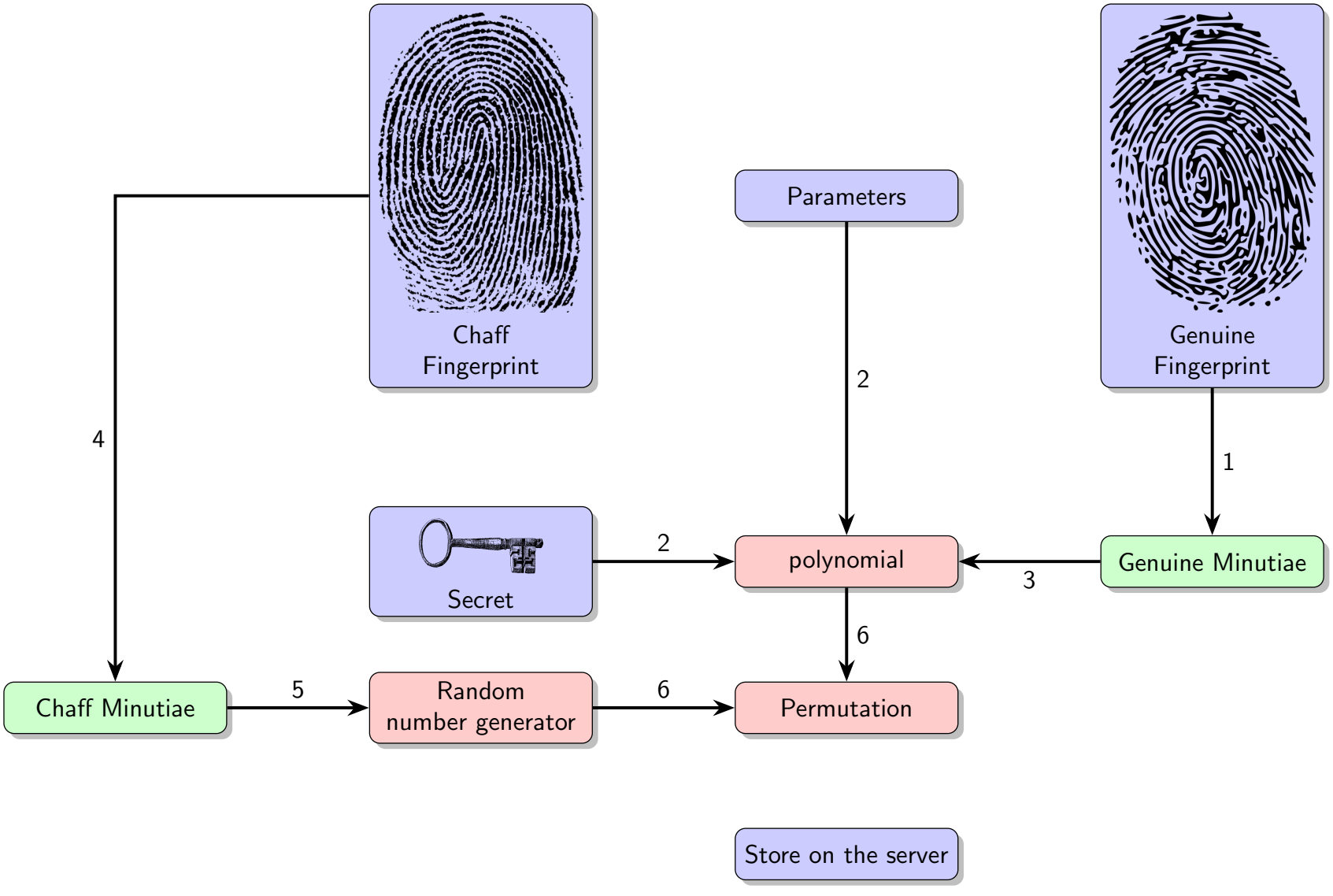
FV_{Gen}


Chaff Fingerprint
Parameters
Genuine Fingerprint
4
2
1
Secret
2
polynomial
3
Genuine Minutiae
Chaff Minutiae
Random number generator
Permutation
Store on the server

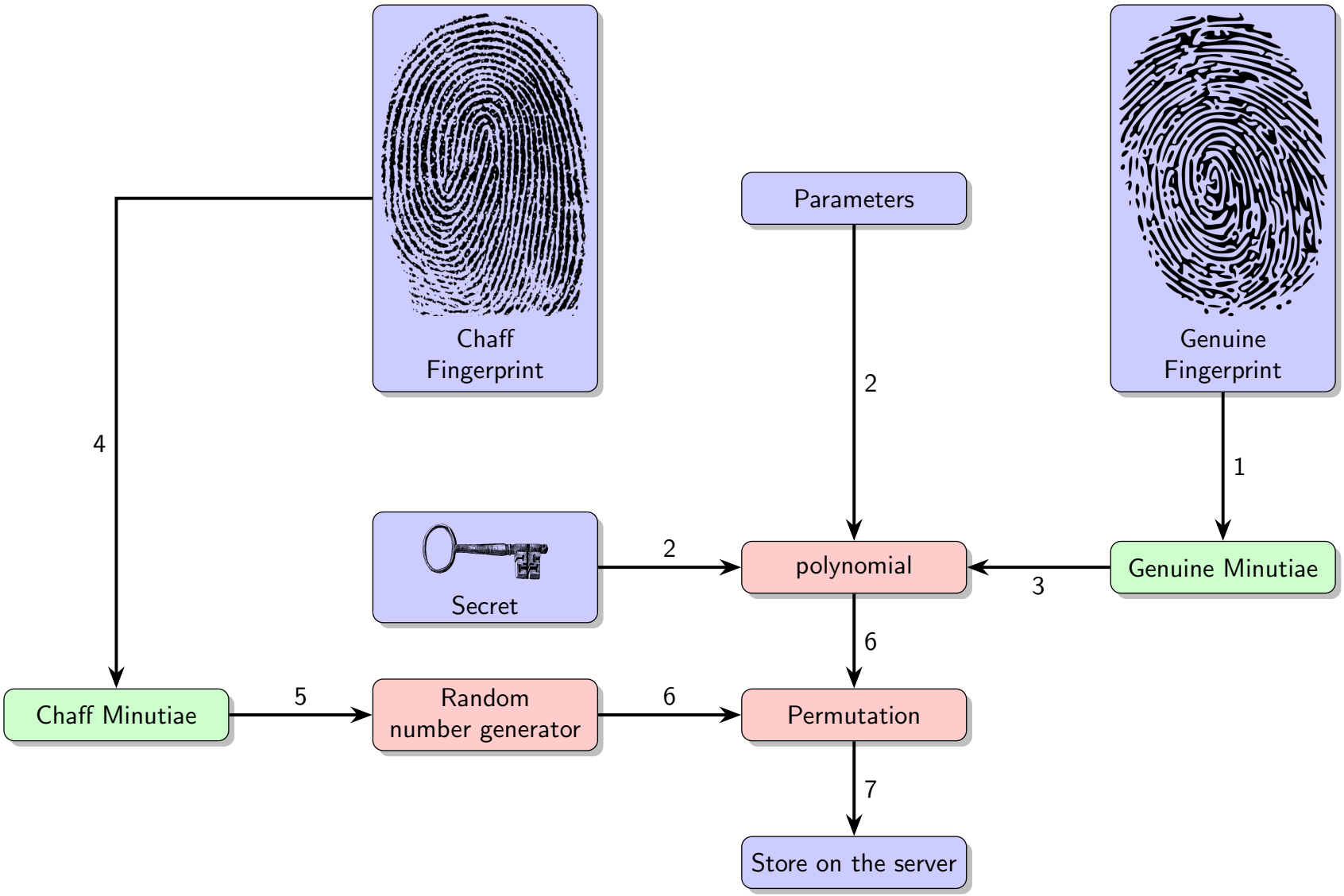
FV_{Gen}


Chaff Fingerprint
Parameters
Genuine Fingerprint
4
2
1
Secret
2
polynomial
3
Genuine Minutiae
Chaff Minutiae
5
Random number generator
Permutation
Store on the server

FV_{Gen}


Chaff Fingerprint
Parameters
Genuine Fingerprint
4
2
1
Secret
2
polynomial
3
Genuine Minutiae
6
Chaff Minutiae
5
Random number generator
6
Permutation
Store on the server

FV_{Gen}


Chaff Fingerprint
Parameters
Genuine Fingerprint
4
2
1
Secret
2
polynomial
3
Genuine Minutiae
6
Chaff Minutiae
5
Random number generator
6
Permutation
7
Store on the server

FV_{Open}

Minutiae

Private Set
Intersection

Server

System
Solve

FV_{Open}

1

Minutiae

Private Set
Intersection

Server

System
Solve

Secret

FV_{Open}

1

Minutiae

2

Private Set
Intersection

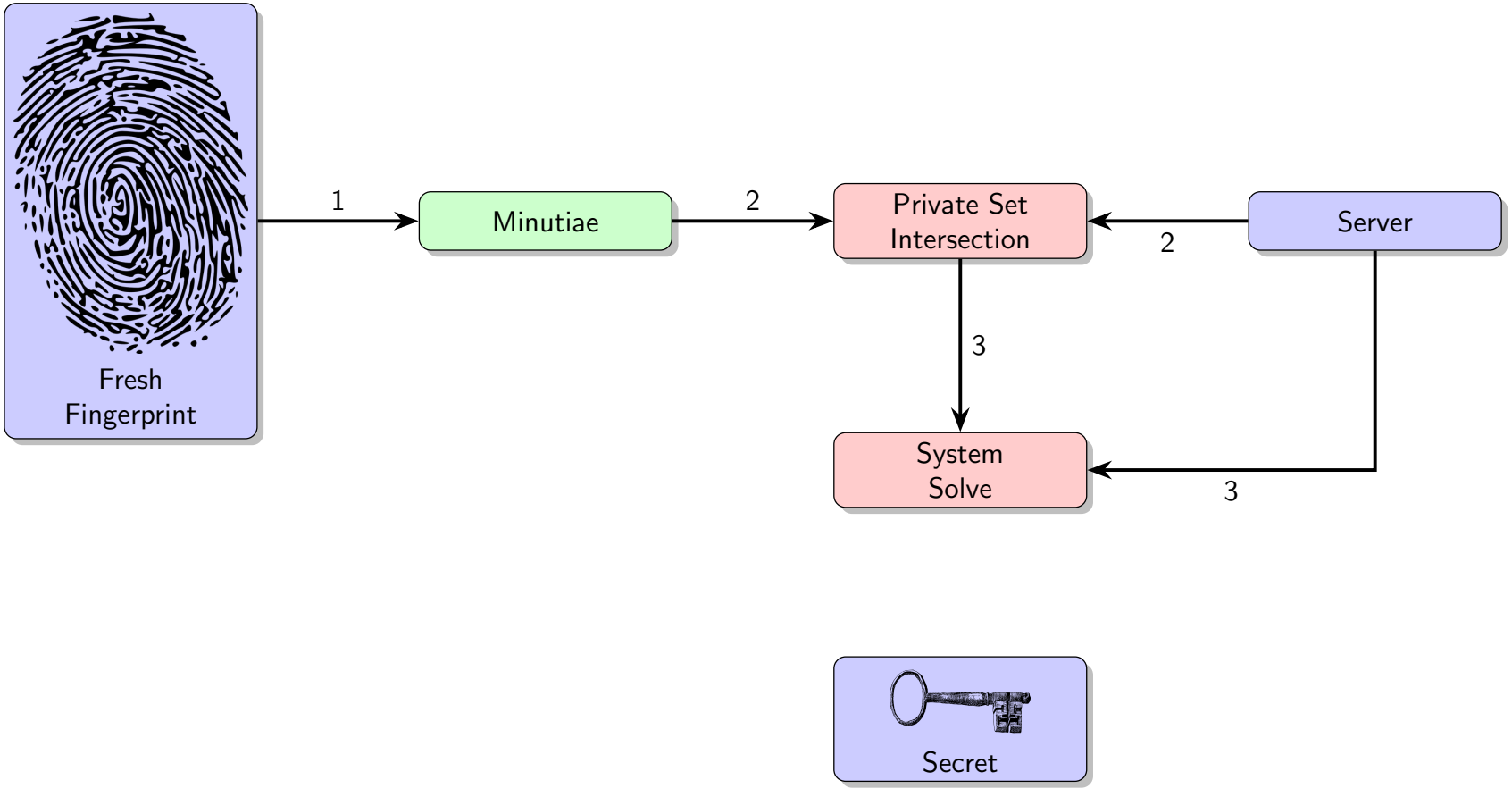
2

Server

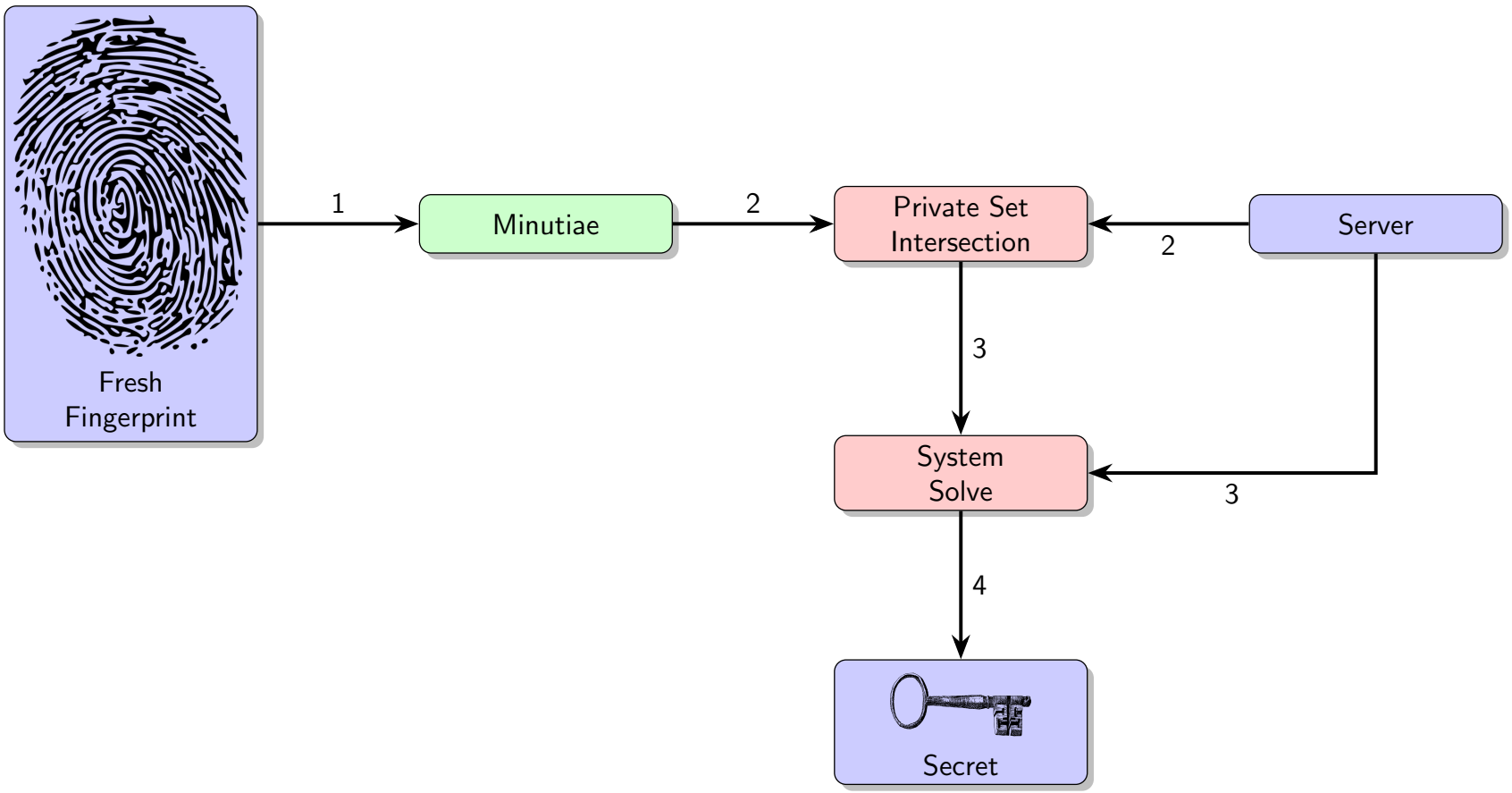
System
Solve

Secret

FV_{Open}

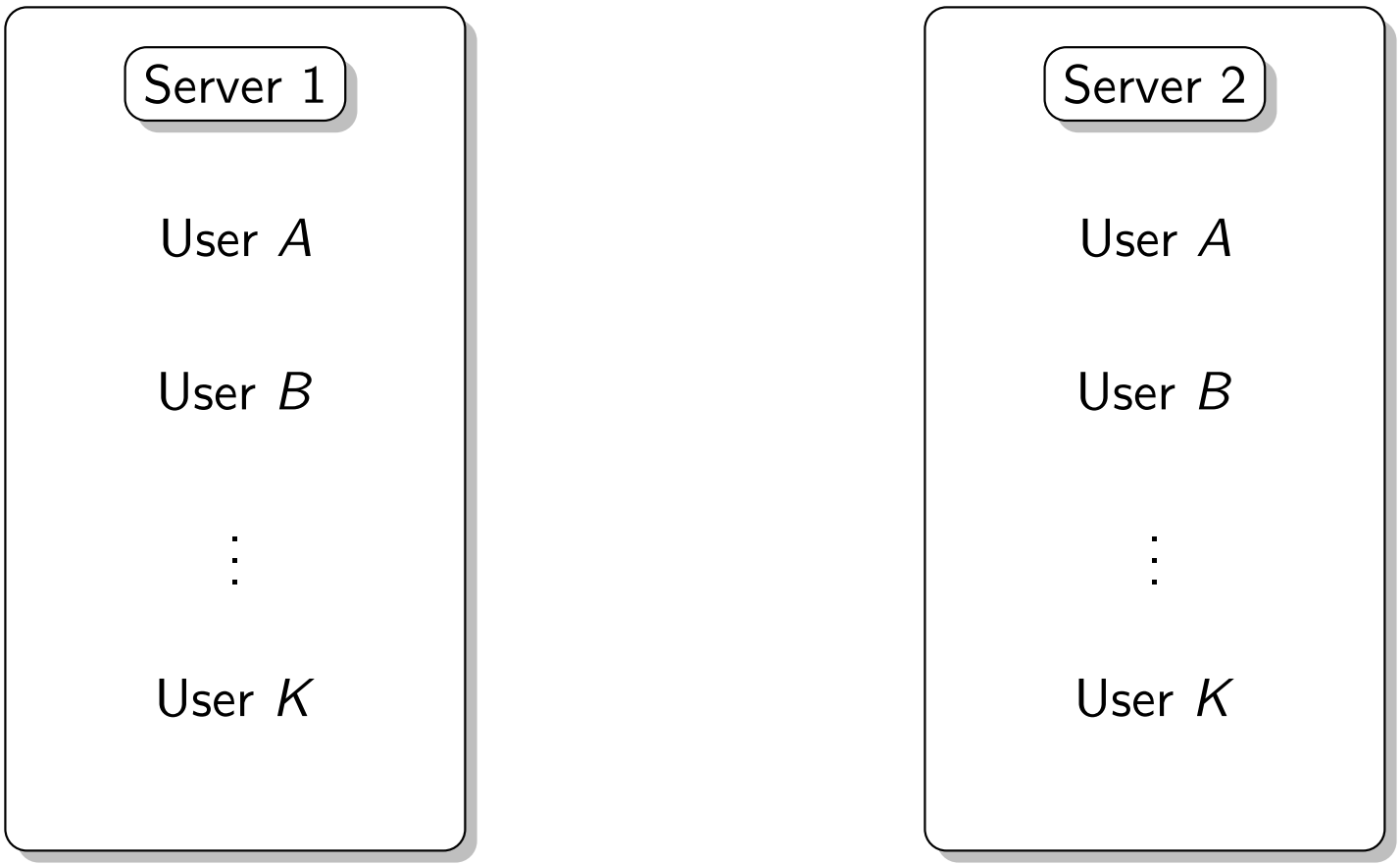

Fresh
Fingerprint
1
Minutiae
2
Private Set
Intersection
2
Server
3
System
Solve
3
Secret

FV_{Open}


Fresh
Fingerprint
1
Minutiae
2
Private Set
Intersection
2
Server
3
System
Solve
3
4
Secret

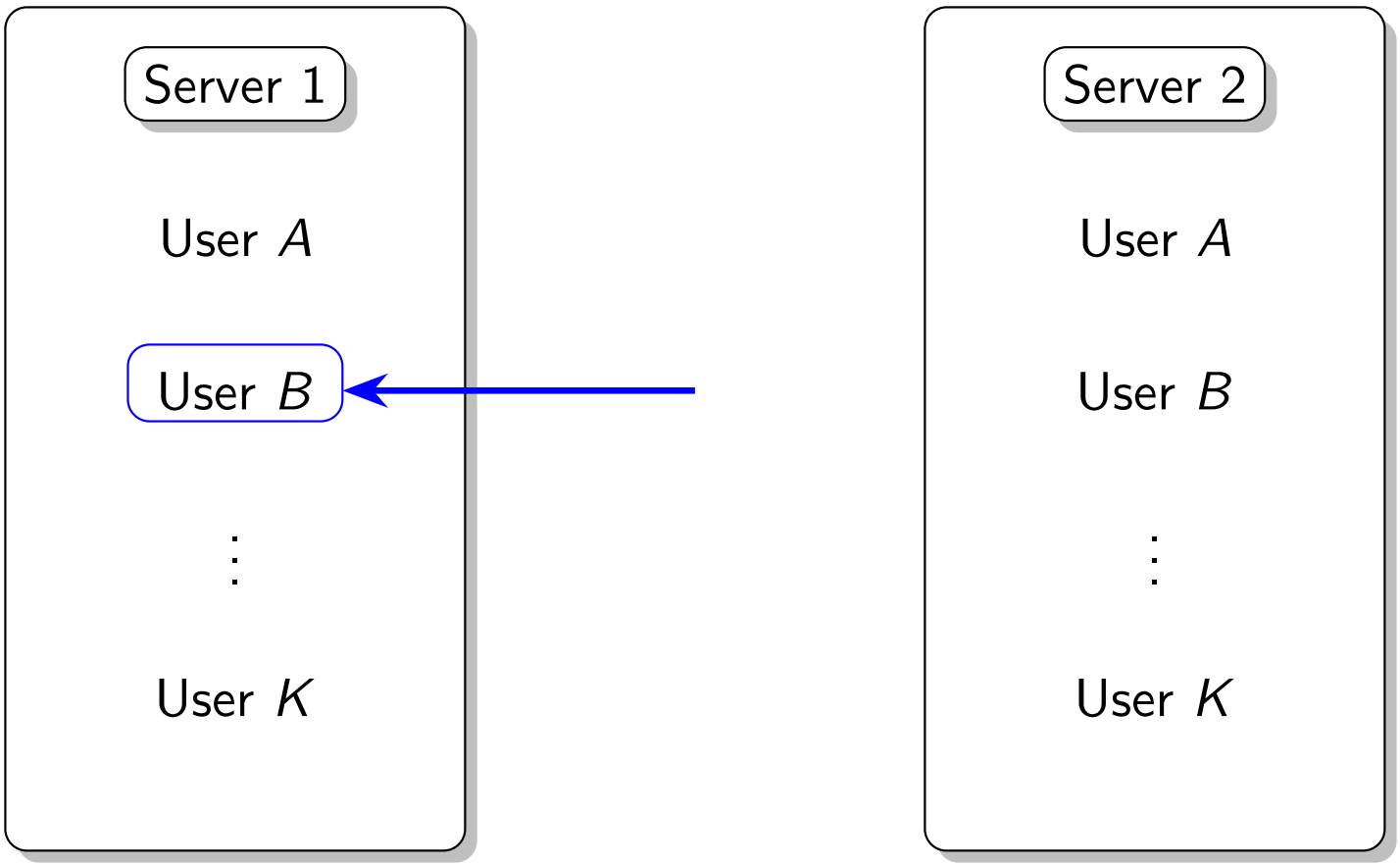
Intersection Attack

Intersection Attack



Pick a target

Intersection Attack

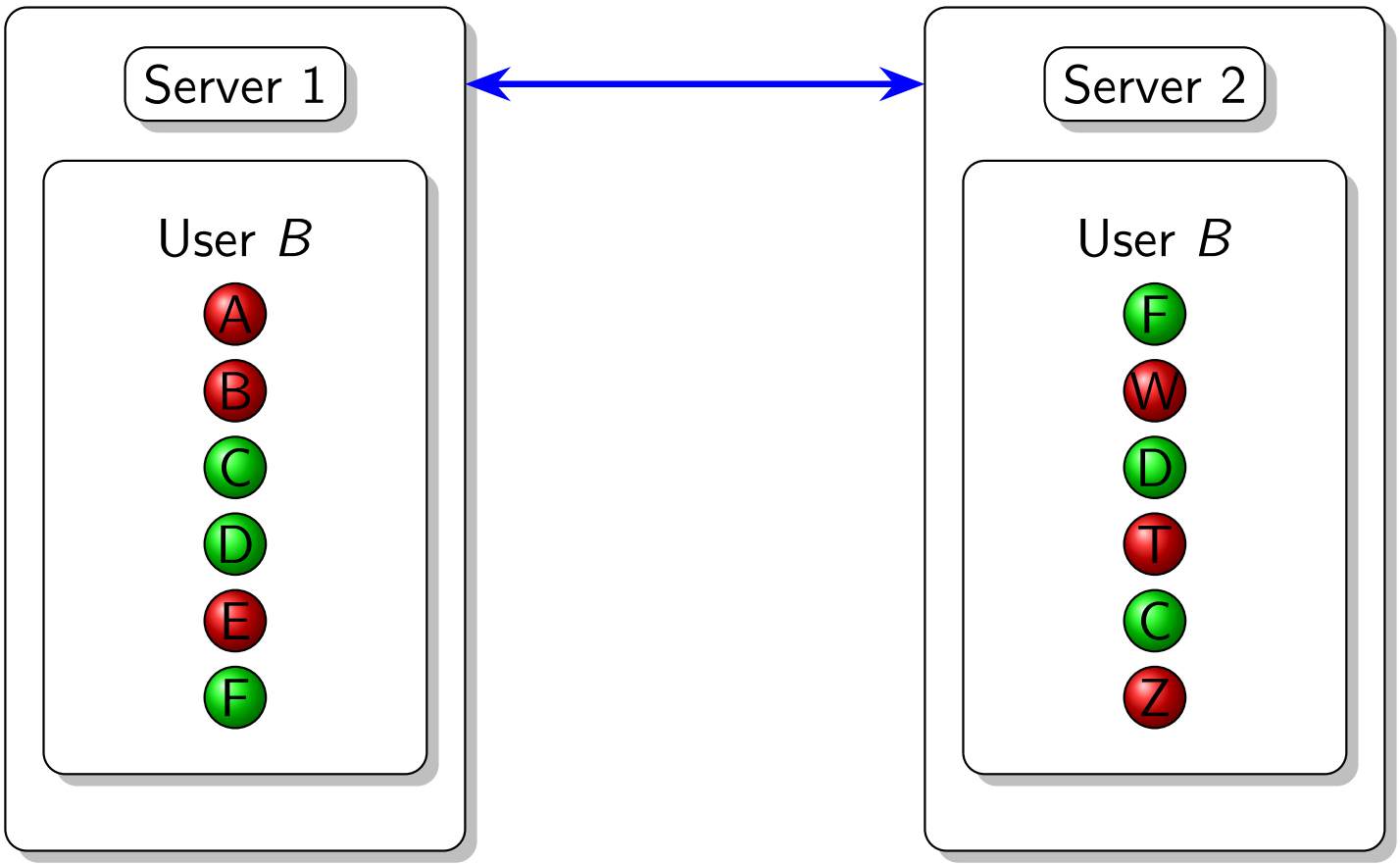


Pick a target

Intersection Attack

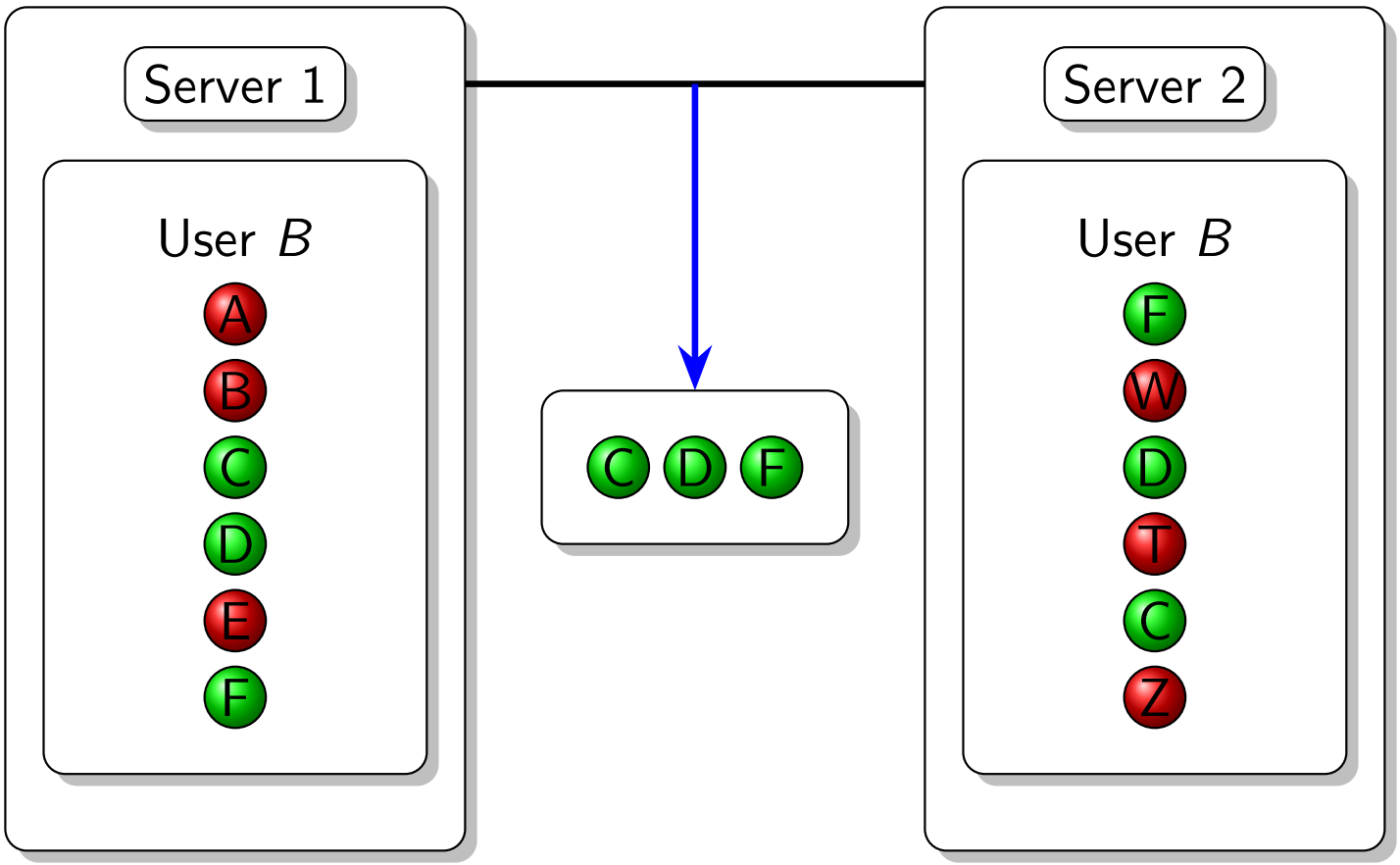
Content of the user B

Intersection Attack



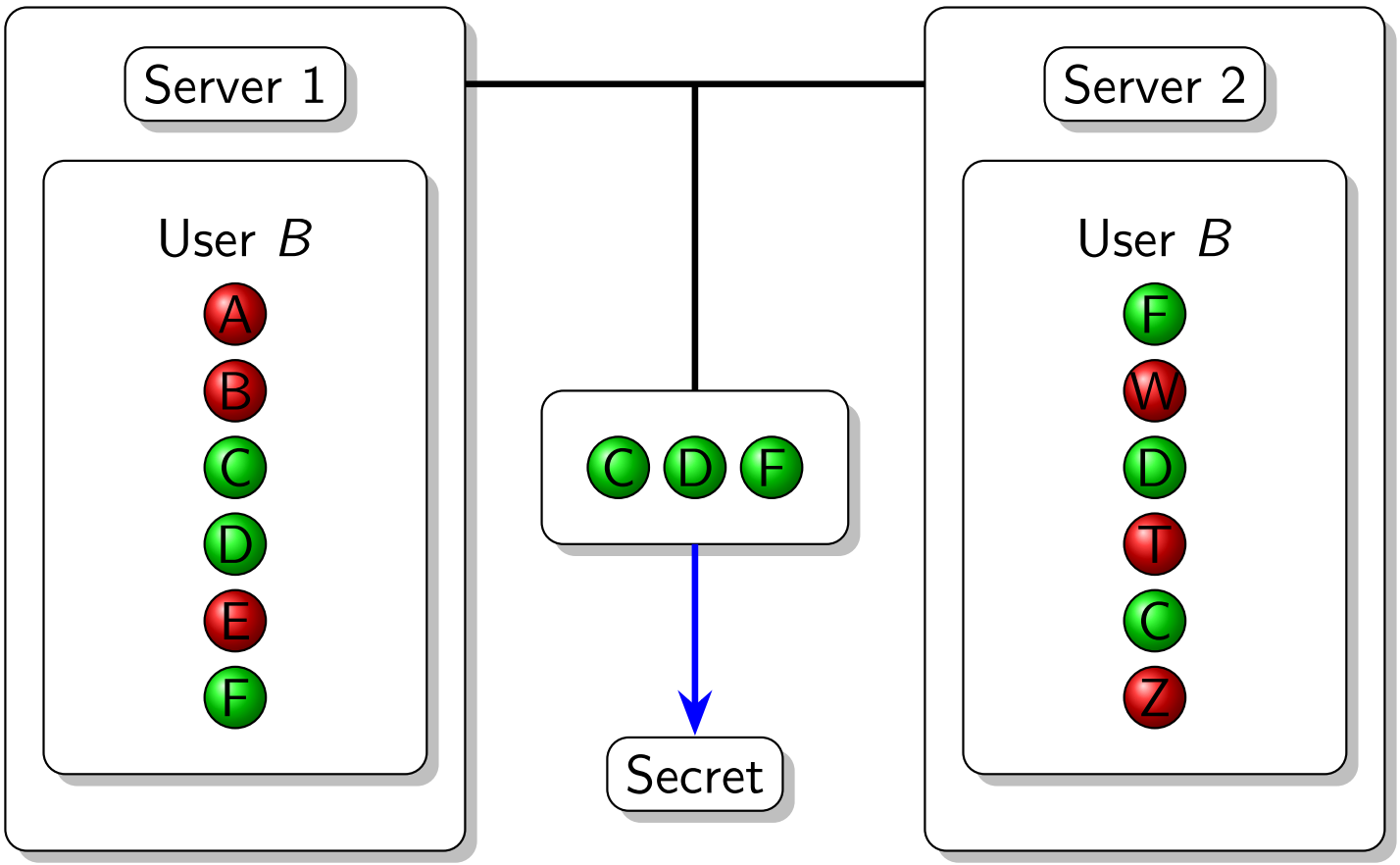
Collaboration

Intersection Attack



Gets the real points

Intersection Attack



Retrieve the secret

Conclusion

Question time