Biometric Privacy Protection with Untrusted Servers

Presenter: **Nguyễn Thị Ái Thảo**

Content

Introduction

Kerberos

Separated Server

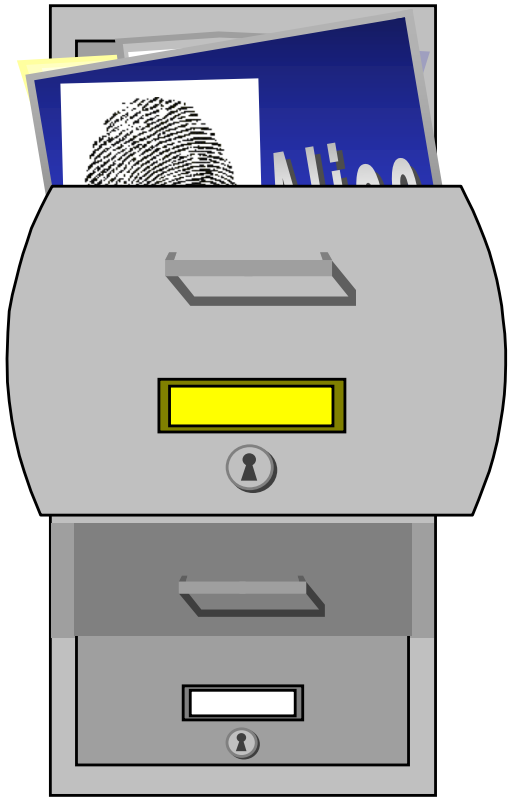
Secure Processor

Registration

Alice

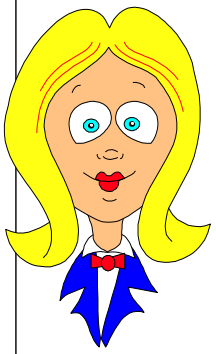
Template

Template is stored



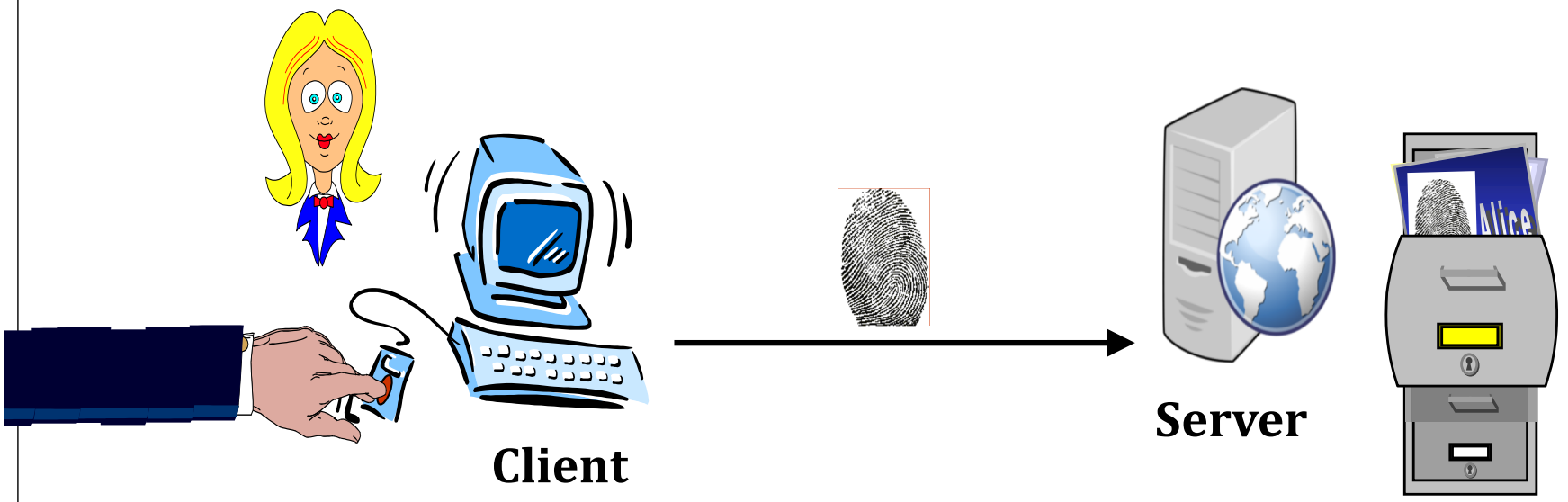
Authentication

Authentication

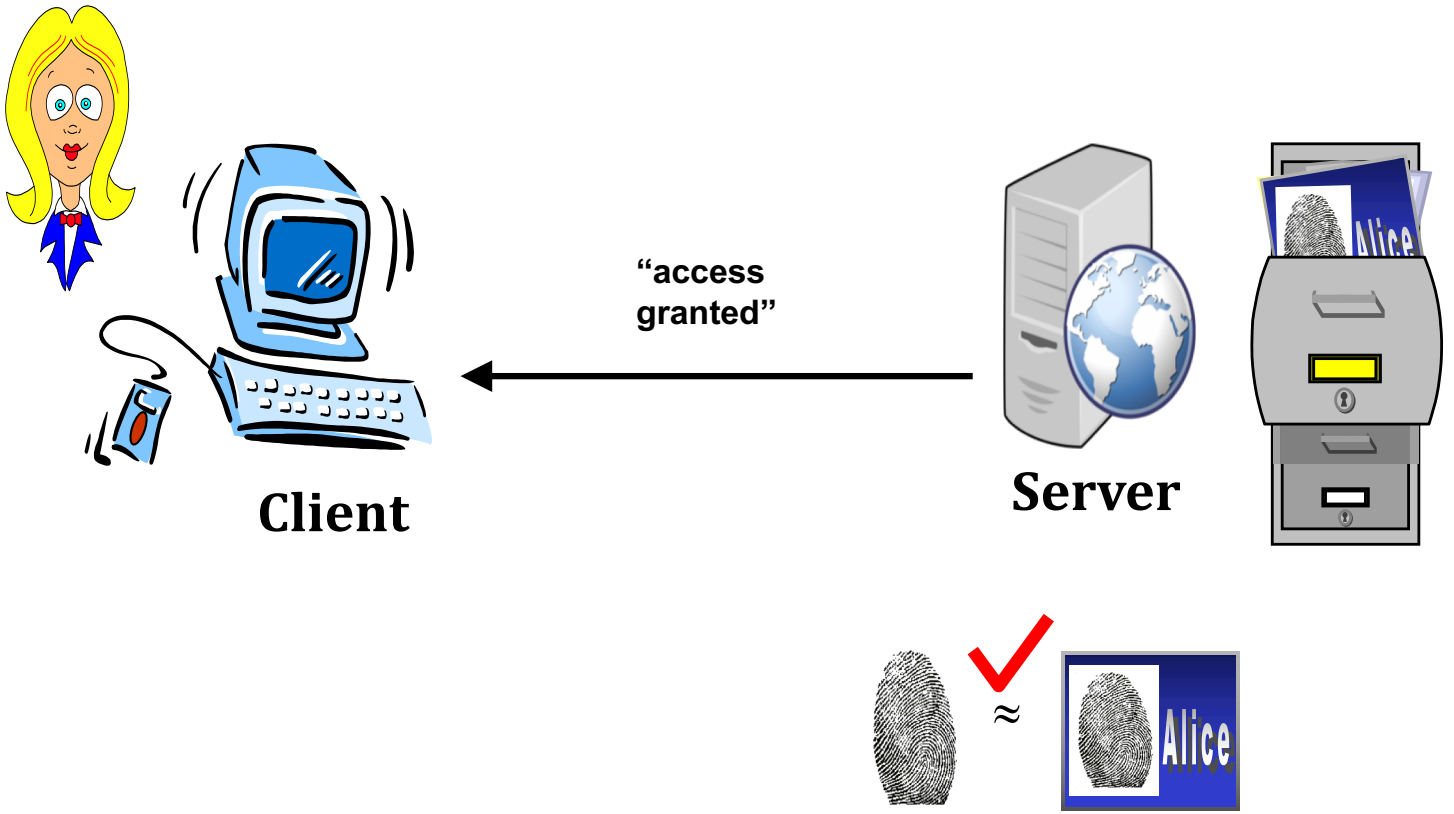


It's Alice!

Remote authentication system



Remote authentication system

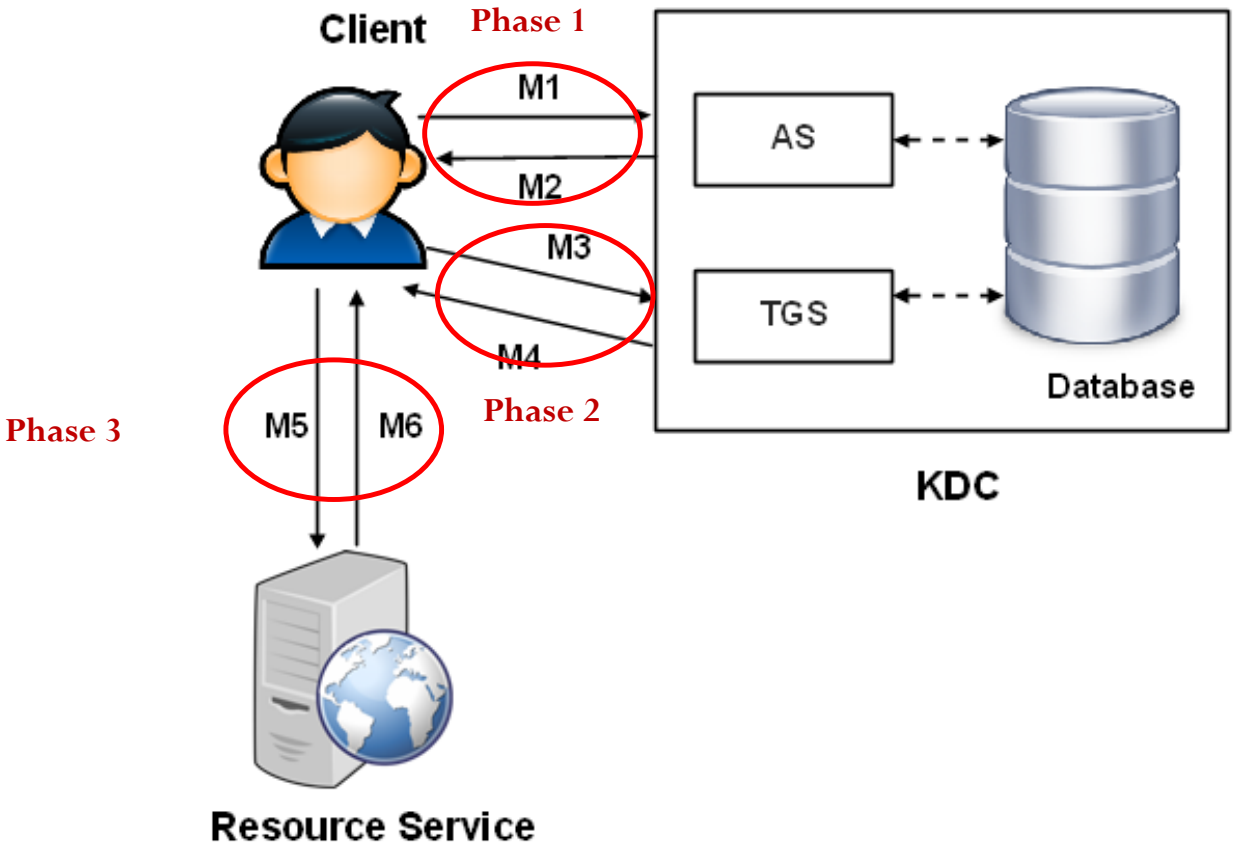


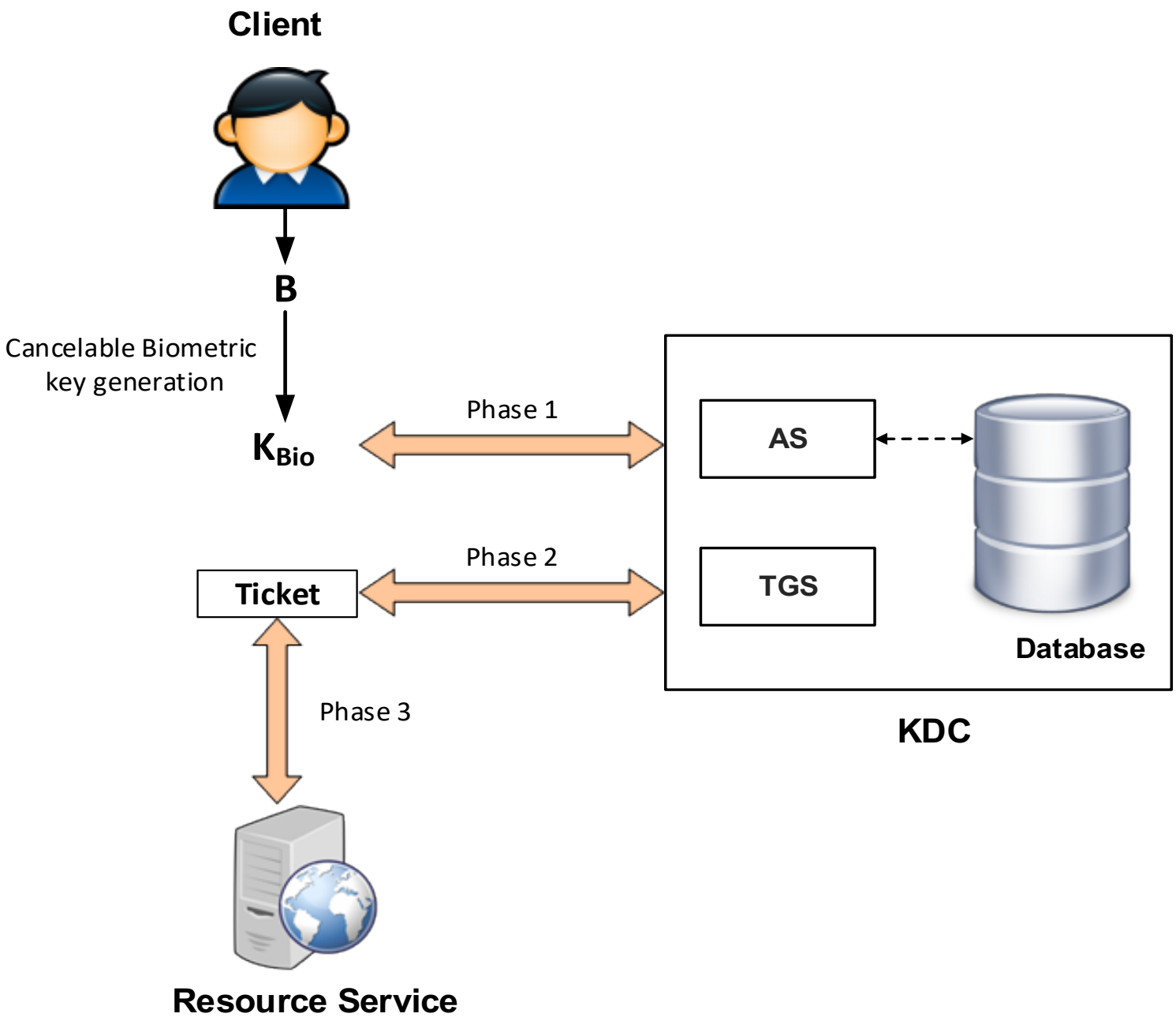
Problems

- Biometric template is compromised
- Privacy is violated
- …

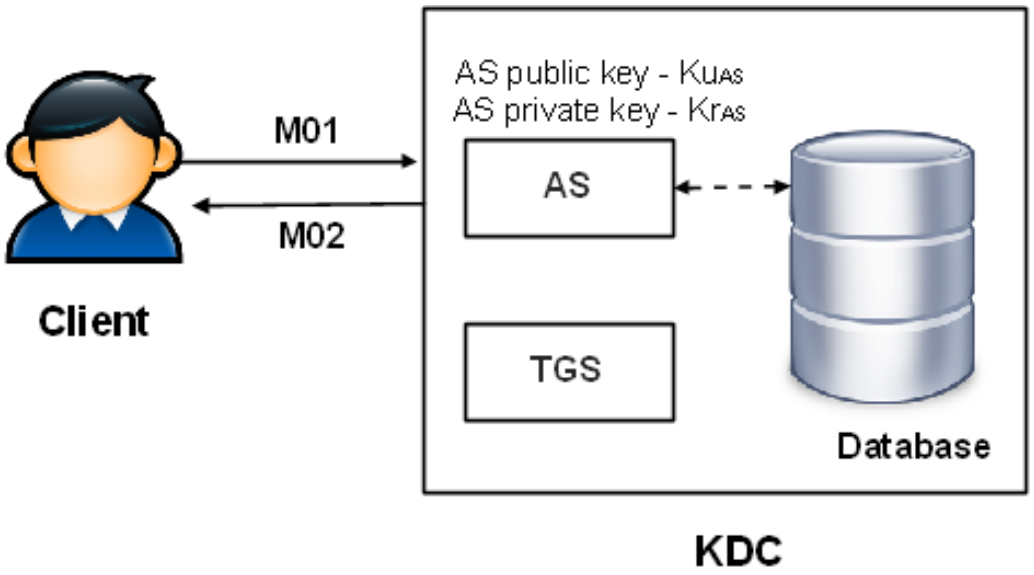
➔*everybody is allowed to know that you are registered to a particular service, but no one is able to know* ***when you use it*** *and* ***for which purpose****, moreover* ***none*** *is able to* ***distinguish you*** *among the other clients*

Biometric-Kerberos based authentication




Client
B
Cancelable Biometric key generation
K_{Bio}
Phase 1
AS
Database
Phase 2
Ticket
TGS
Phase 3
KDC
Resource Service

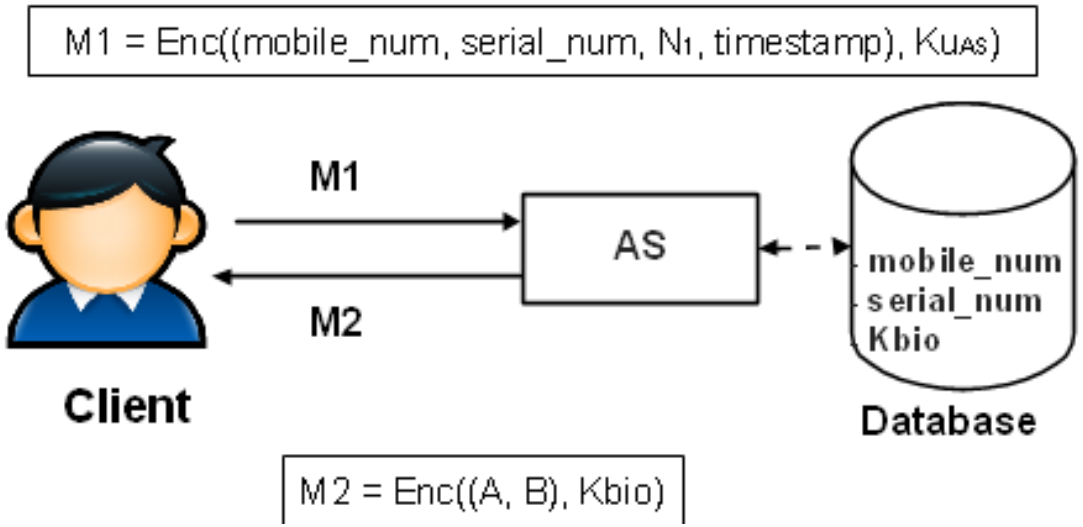
Enrollment stage



$$M_{01} = Enc((\ mobile\_num, serial\_num, K_{bio}, N_{01}, timestamp, is\_enroll),\ Ku_{As})$$

$$M_{02} = Enc((\ N_{01}, timestamp, is\_success),\ Kr_{As})$$

Authentication stage



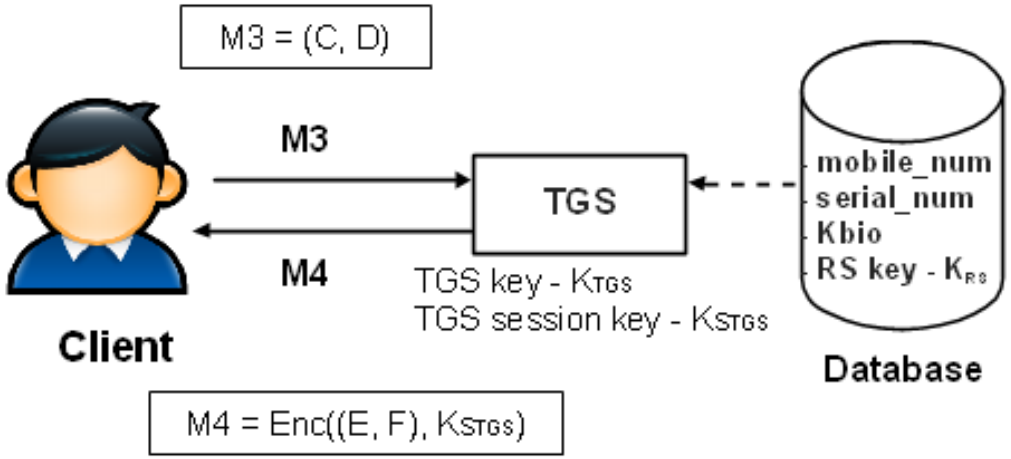
$$A = (timestamp, N_1, Ks_{TGS})$$

$$B = Enc((Ks_{TGS}, mobile\_num, serial\_num, N_1, timestamp), K_{TGS})$$

Authentication stage

$$C = Enc((\ mobile\_num, serial\_num, N_1, timestamp, RS\_ID), Ks_{TGS})$$

$$D = M_2.B$$



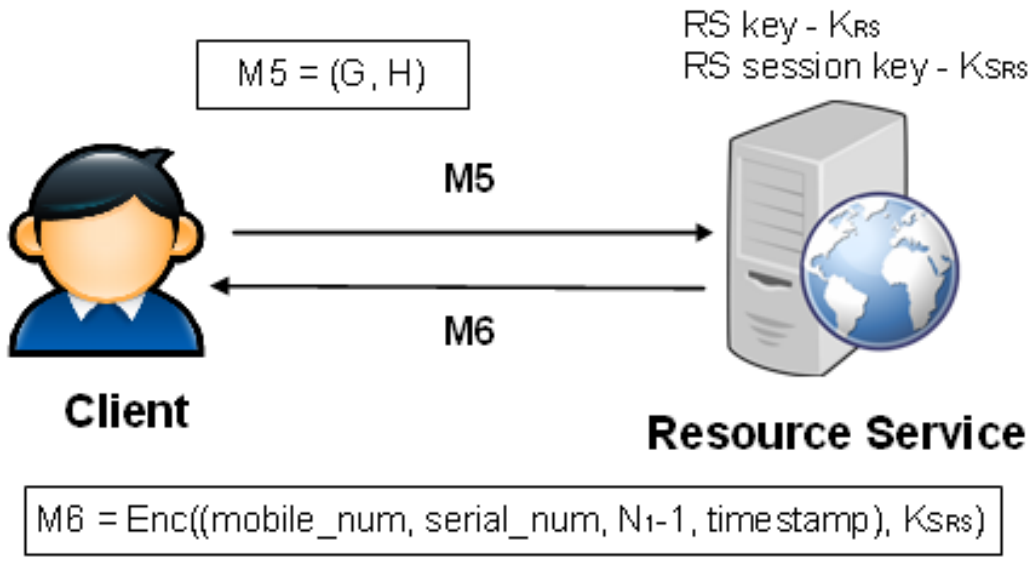
$$E = Ks_{RS}$$

$$F = Enc((\ Ks_{RS}, mobile\_num, serial\_num, N_1, timestamp, RS\_ID), K_{RS})$$

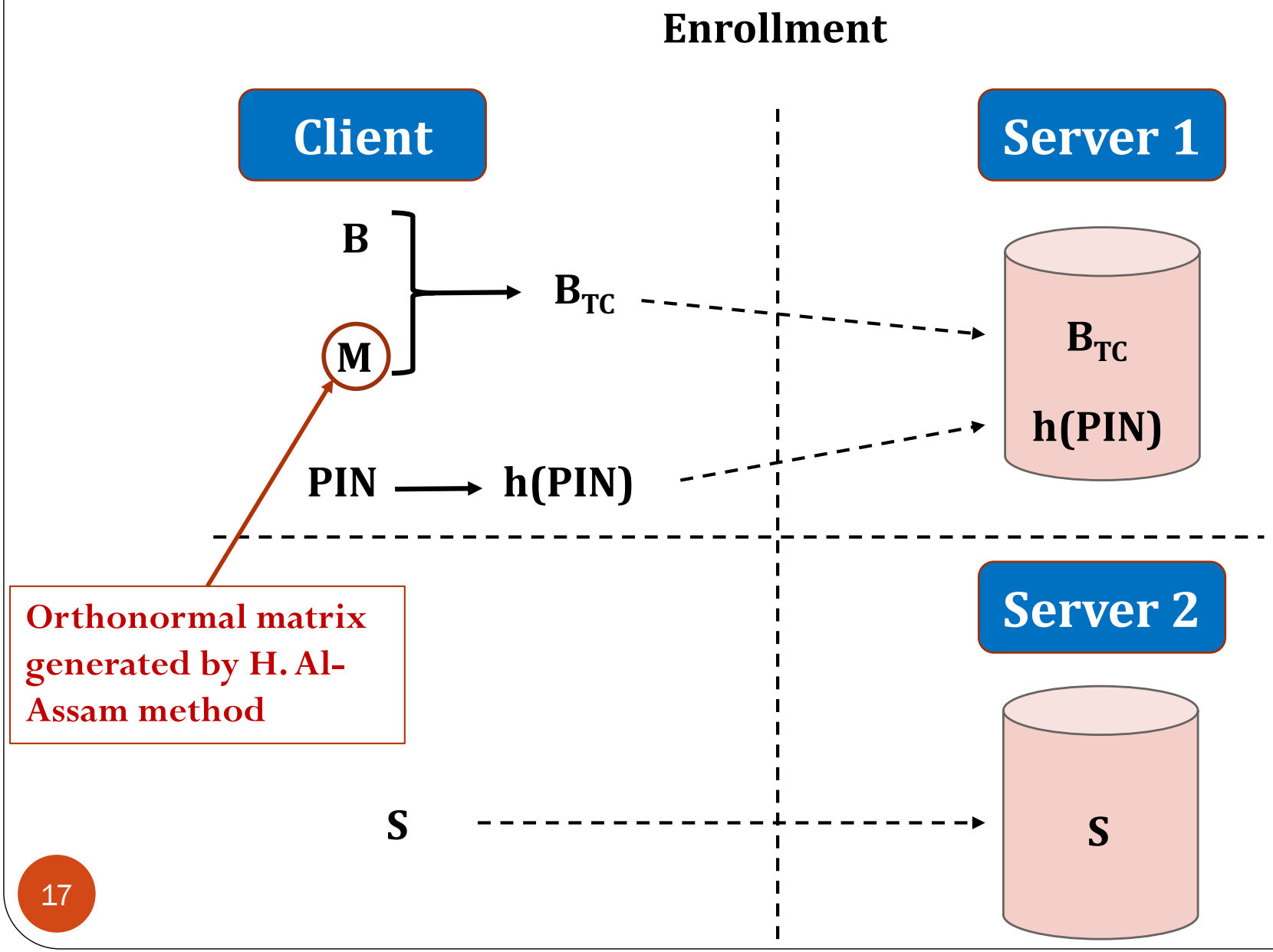
Authentication stage

$$G = Enc((mobile\_num, serial\_num, N_1, timestamp), Ks_{RS})$$

$$H = M_4.F$$



Separated servers approach



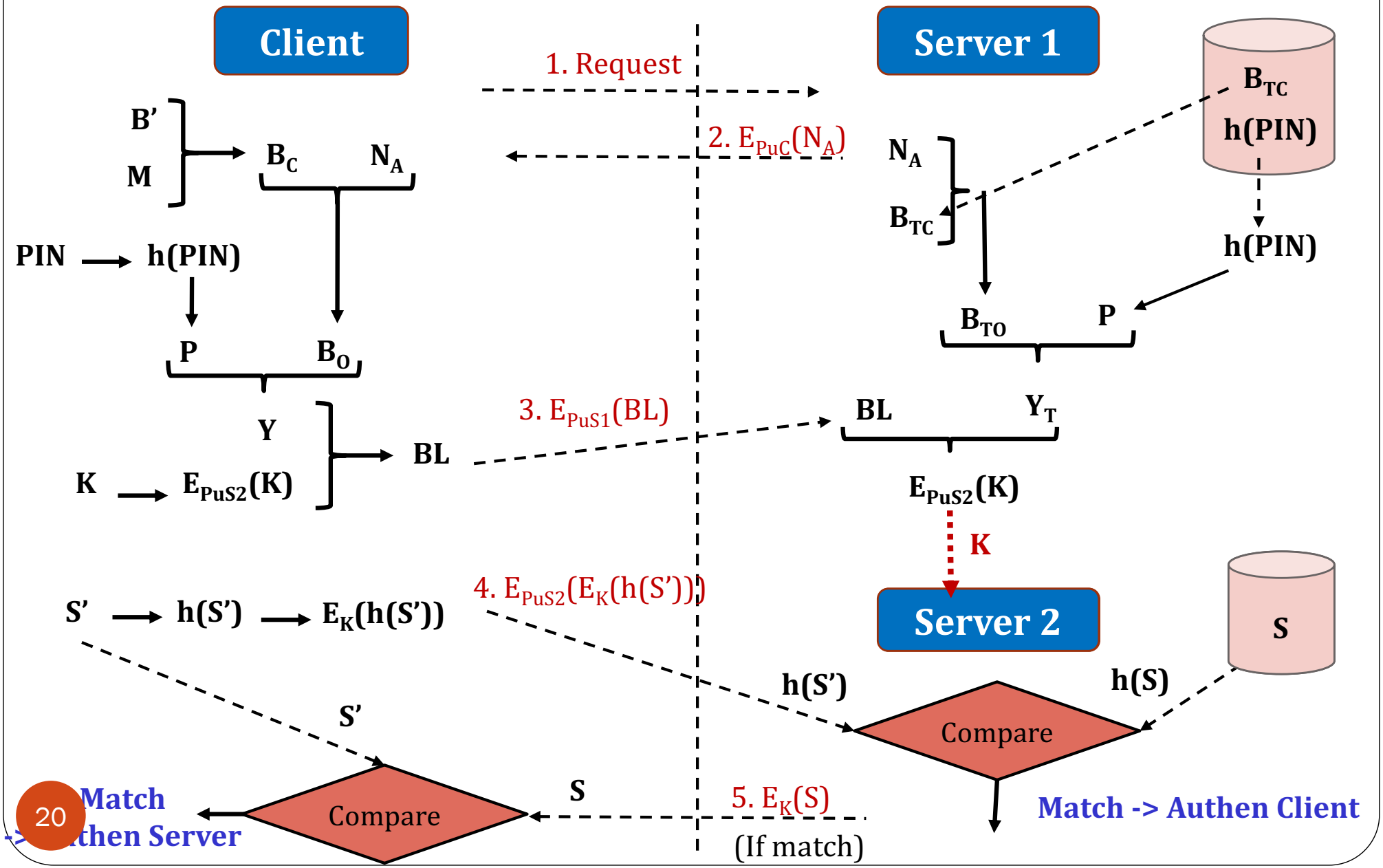
Orthonormal Random Project

- Traditional method: Gram-Schimidt
- New method: Orthonormal Random (by H. Al – Assam)

$$M = \begin{bmatrix} \cos\theta_1 & \sin\theta_1 & 0 & 0 & \dots & \dots & 0 \\ -\sin\theta_1 & \cos\theta_1 & 0 & 0 & \dots & \dots & 0 \\ 0 & 0 & \cos\theta_2 & \sin\theta_2 & \dots & \dots & 0 \\ 0 & 0 & -\sin\theta_2 & \cos\theta_2 & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cos\theta_n & \sin\theta_n \\ 0 & 0 & 0 & 0 & 0 & -\sin\theta_n & \cos\theta_n \end{bmatrix}$$

Al-Assam, H., H. Sellahewa, and S. Jassim. *A lightweight approach for biometric template protection*. in *Proceedings of SPIE*. 2009.

Authentication



Separated servers approach

- The proposed protocol relying on
  - Fuzzy commitment
  - Orthonormal random transformation
- Mutual authentication
- Immune from some main attacks over insecure network.
- Reduce the possibility of inside attackers

Encrypted Computation

- Homomorphic cryptosystems
- Secure processor

Homomorphism

- If G and H are groups, a **homomorphism** from G to H is a function $f: G \longrightarrow H$ such that

$$\mathbf{f(g_1 + g_2) = f(g_1) +' f(g_2)}$$

For any elements $g_1, g_2 \in G$

*W*here + denotes the operation in G

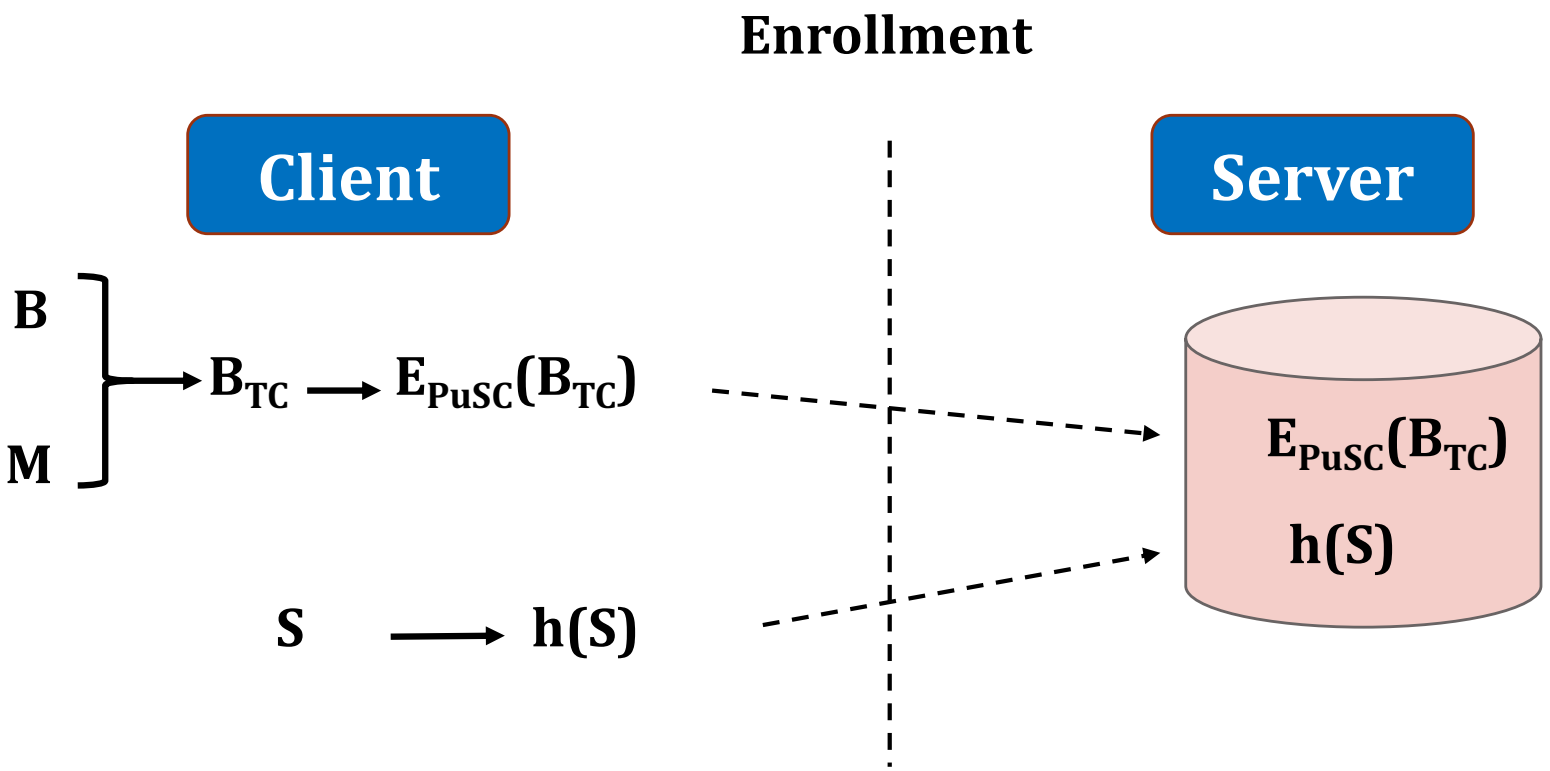
+' denotes the operation in H.

Example: f: matrix 2*2 ⟶ matrix 2*2

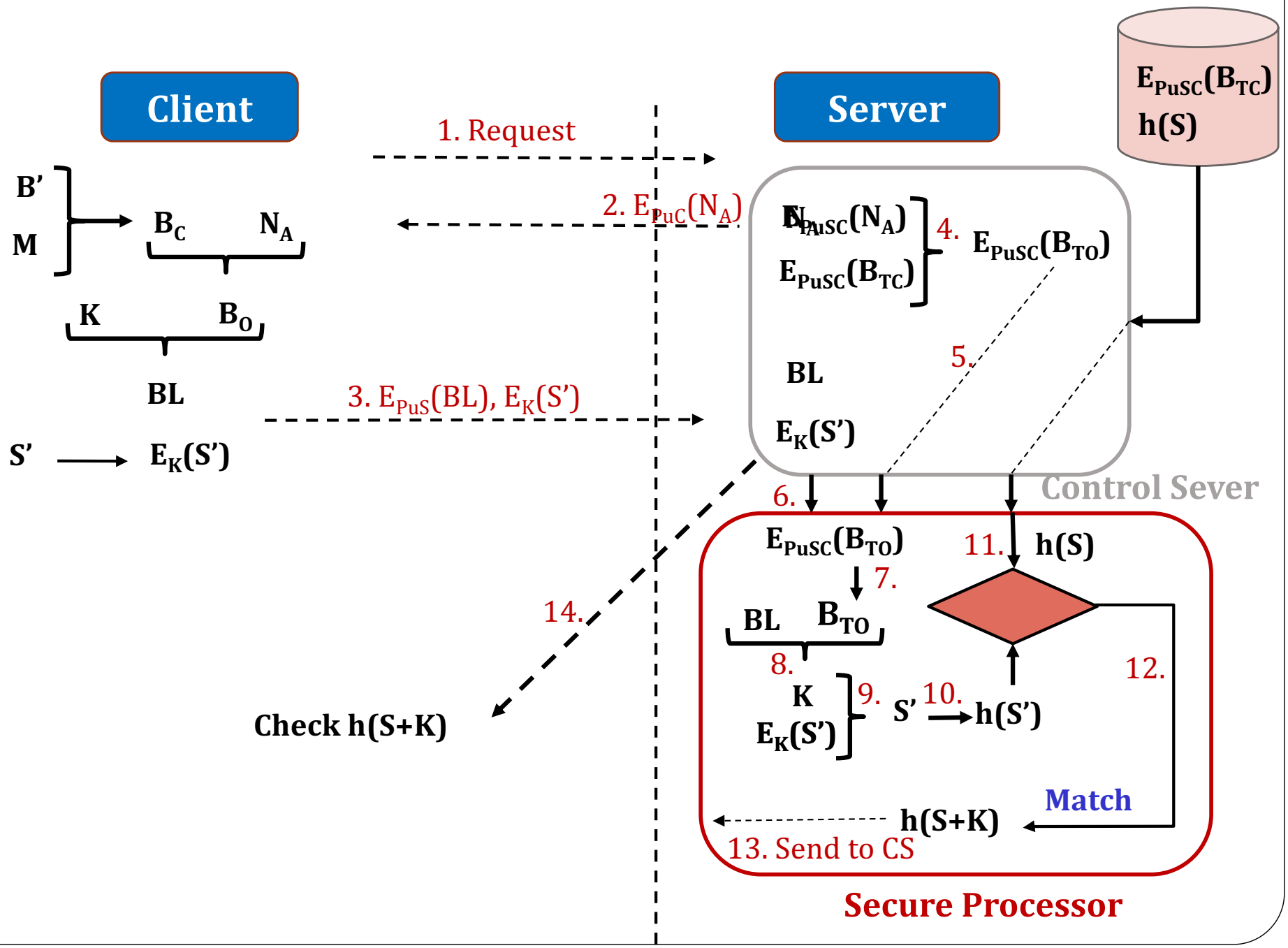
where r is real number, then f is a homomorphism group, since f preserves b 'addition' operation.

$$f(r+s) = f\begin{bmatrix} r+s & 0 \\ 0 & r+s \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} + \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} = f(r) + f(s)$$

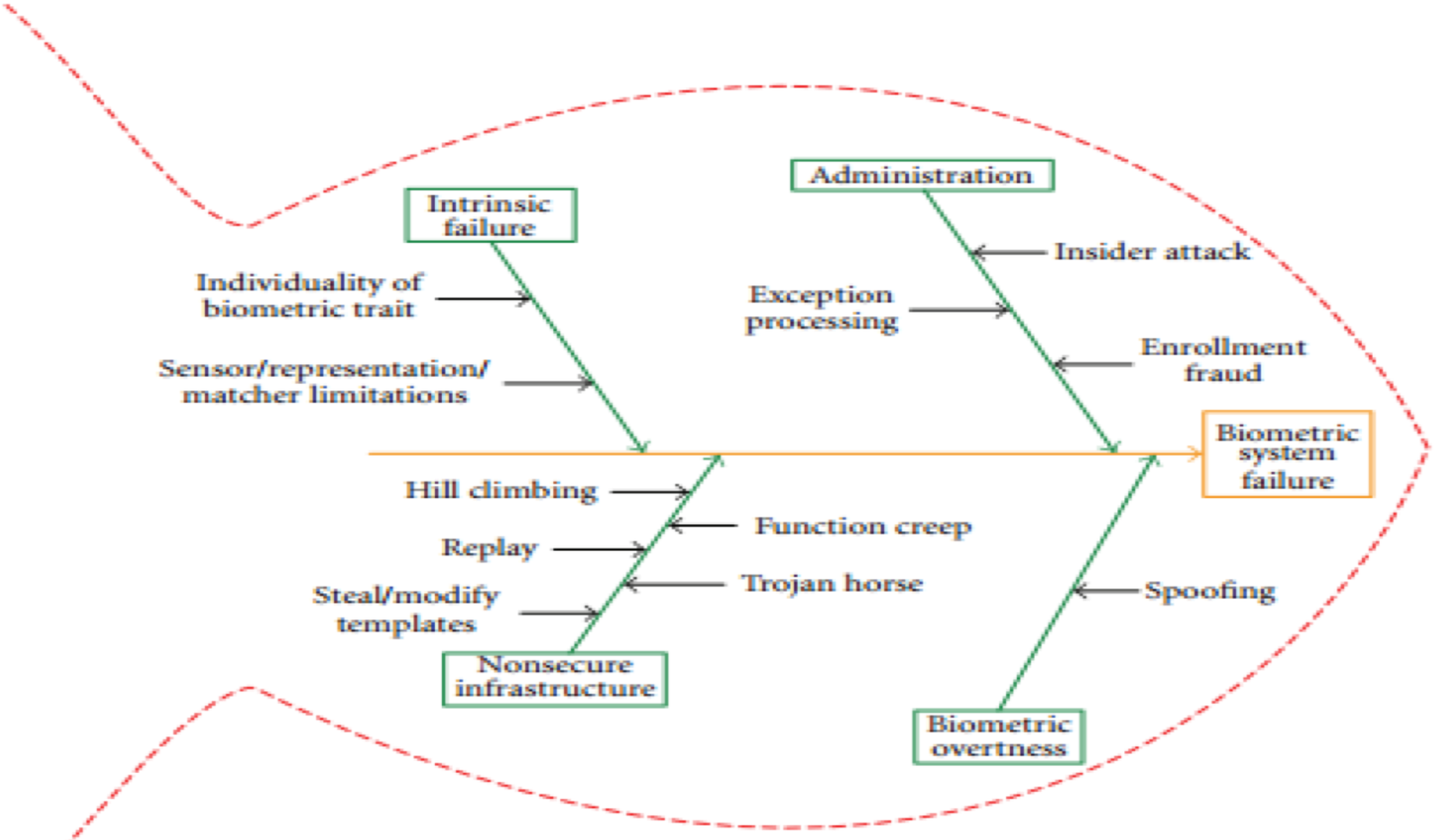
Secure Processor approach



Authentication



Biometric system failures

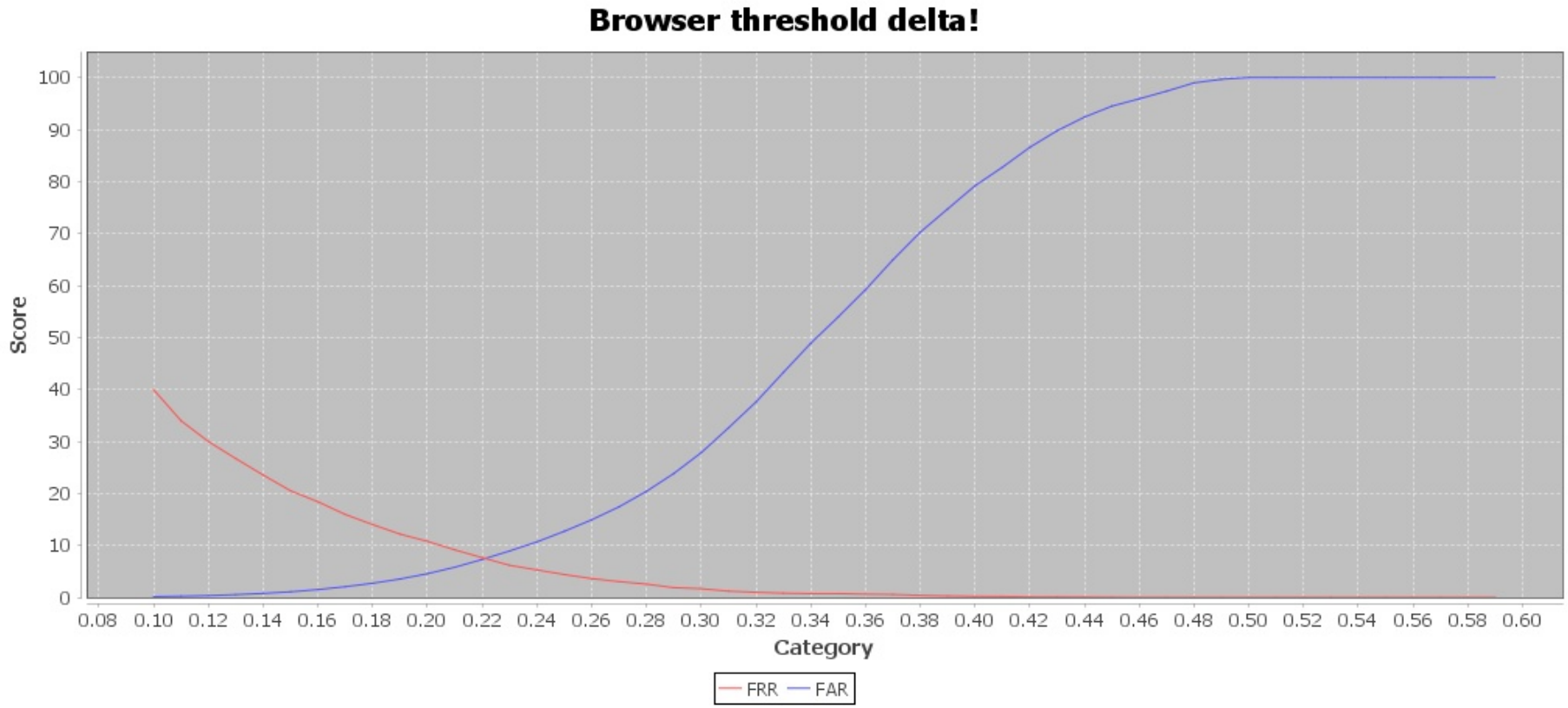


Biometric system failures

- **Adversary attacks:** an adversary intentionally attack to the biometric system.
- Three main classes:
  - Administration attack: due to improper administration of the biometric system (insider attack)
  - Non-secure infrastructure: hardware, software, and the communication channels
  - Biometric overtness: not distinguish between a live biometric presentation and an artificial spoof

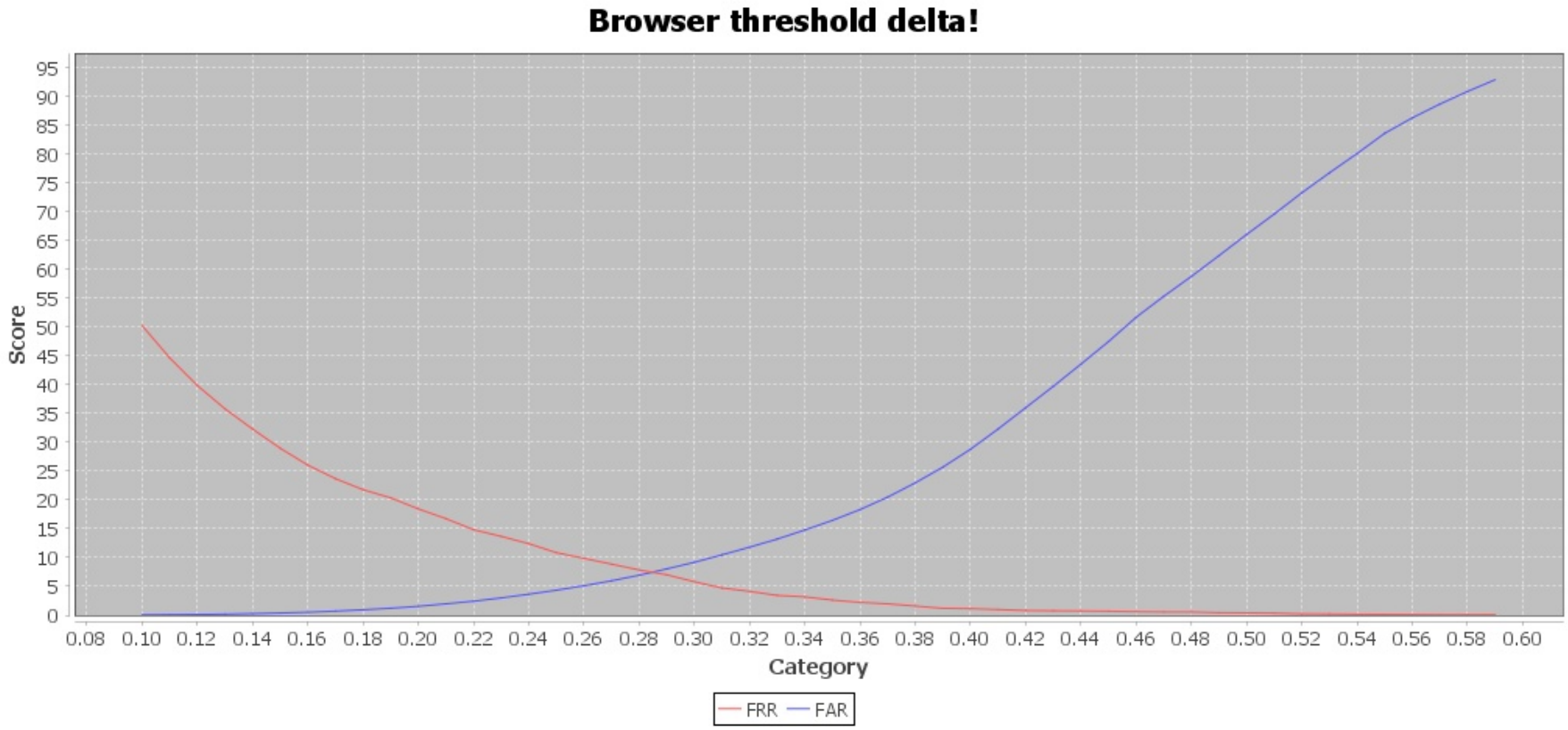
Experimental Resutls

- *Authentication with original feature vectors*



Experimental Resutls

- *Authentication with transformed feature vectors by orthonormal matrix*



Experimental Resutls

- Authentication with secure feature vectors by orthonormal matrix and fuzzy commitment.