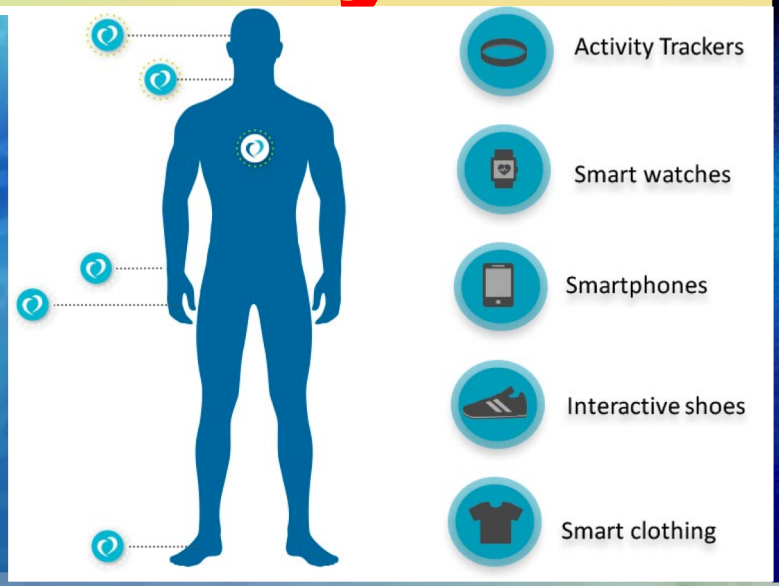



# Security of Biometric Systems





Assoc. Prof. Dr. **DANG TRAN KHANH**
CSE/HCMUT, Vietnam
khanh@hcmut.edu.vn

Data SecuriTy Applied Research Lab

# Outline

- Introduction
  - Security issues of biometric systems
- Biometric template protection
  - Cancellable biometrics
  - Biometric cryptosystems
  - Hybrid approaches
- Reading:
  - Chapter 7 [1]
  - [2, 3]

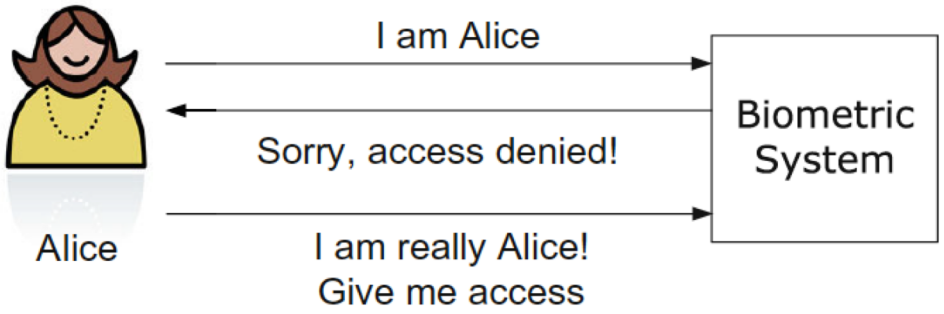
# Introduciton

- Obviously users prefer a biometric system that has the least probability of failure
- Non-repudiation ensures that an individual who accesses a certain resource cannot later deny using it
- The integrity  of a biometric system is determined by its ability to guarantee non-repudiable authentication
- Security threats in biometric systems can be classified into 4 major classes

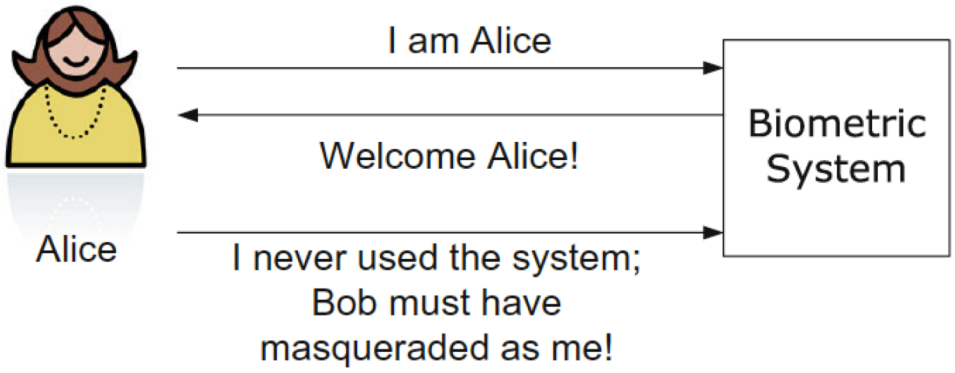
# Introduciton

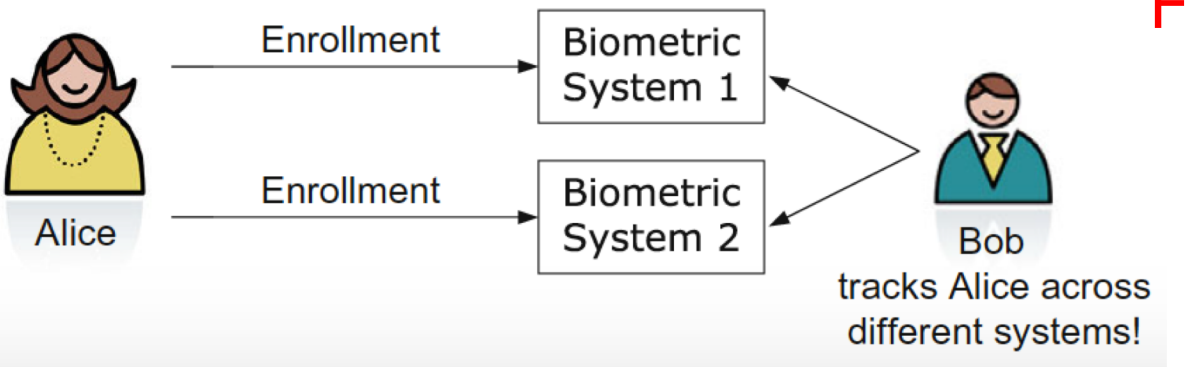
- Obviously users prefer a biometric system that has the least probability of failure
- Non-repudiation ensures that an individual who accesses a certain resource cannot later deny using it
- The integrity  of a biometric system is determined by its ability to guarantee non-repudiable authentication
- Security threats in biometric systems can be classified into 4 major classes

# Security issues of biometric systems





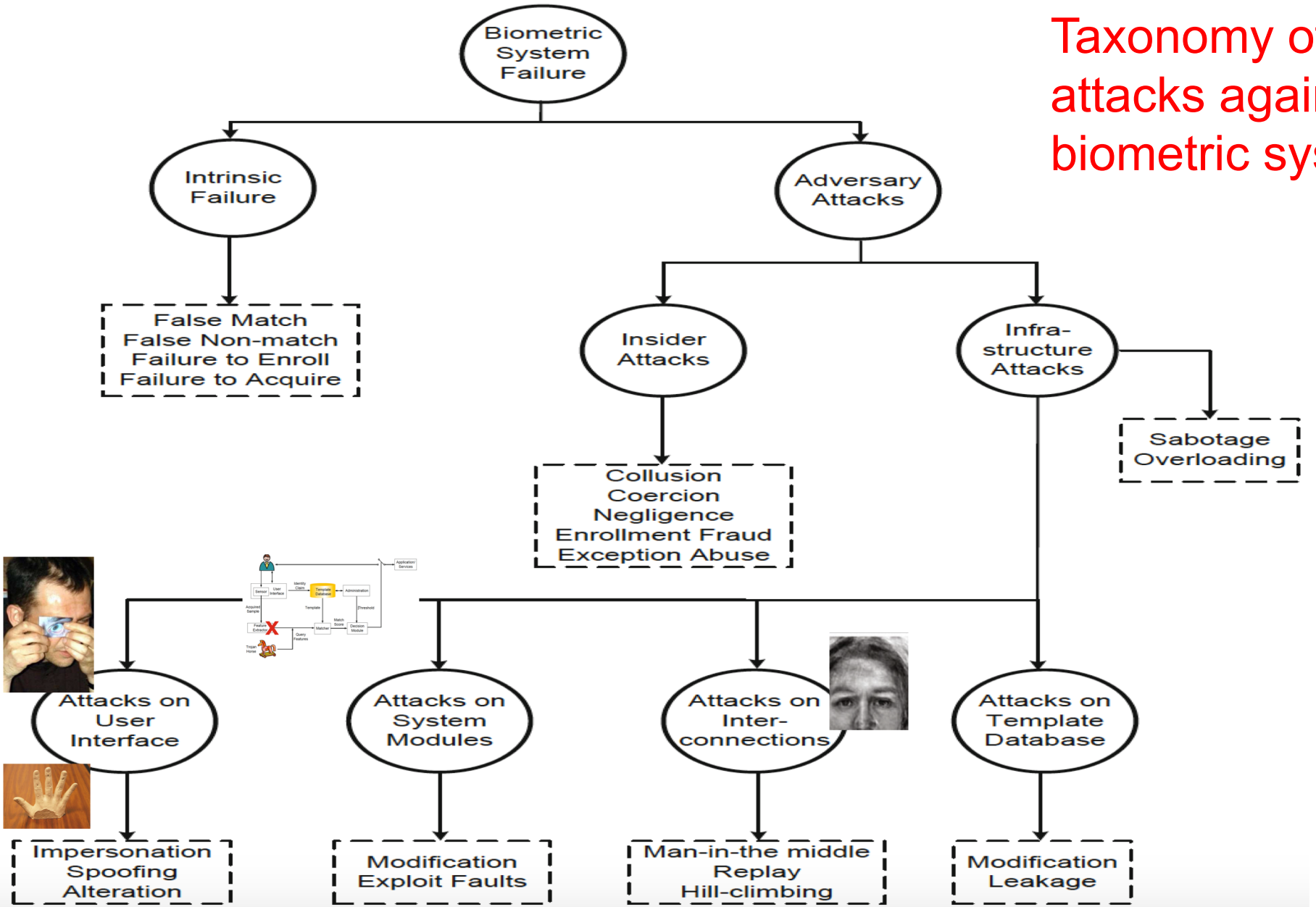



Four major classes of security threats in a biometric system: DoS, Intrusion, Repudiation, and Function creep

# Security issues of biometric systems

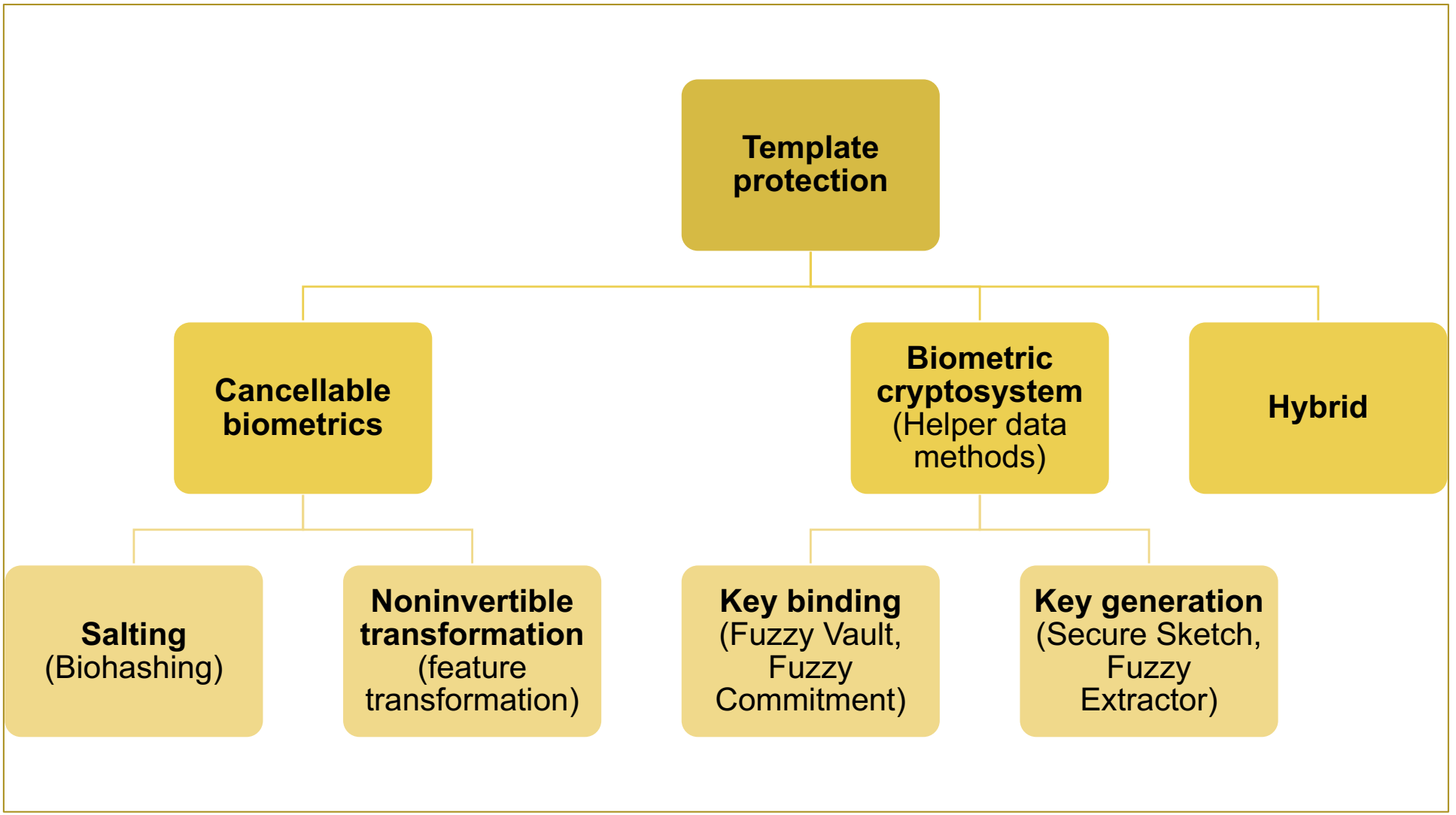
Taxonomy of attacks against a biometric system



# Outline

- ~~Introduction~~
  - ~~Security issues of biometric systems~~
- Biometric template protection
  - Cancellable biometrics
  - Biometric cryptosystems
  - Hybrid approaches
- Reading:
  - Chapter 7 [1]
  - [2, 3]

# Template protection

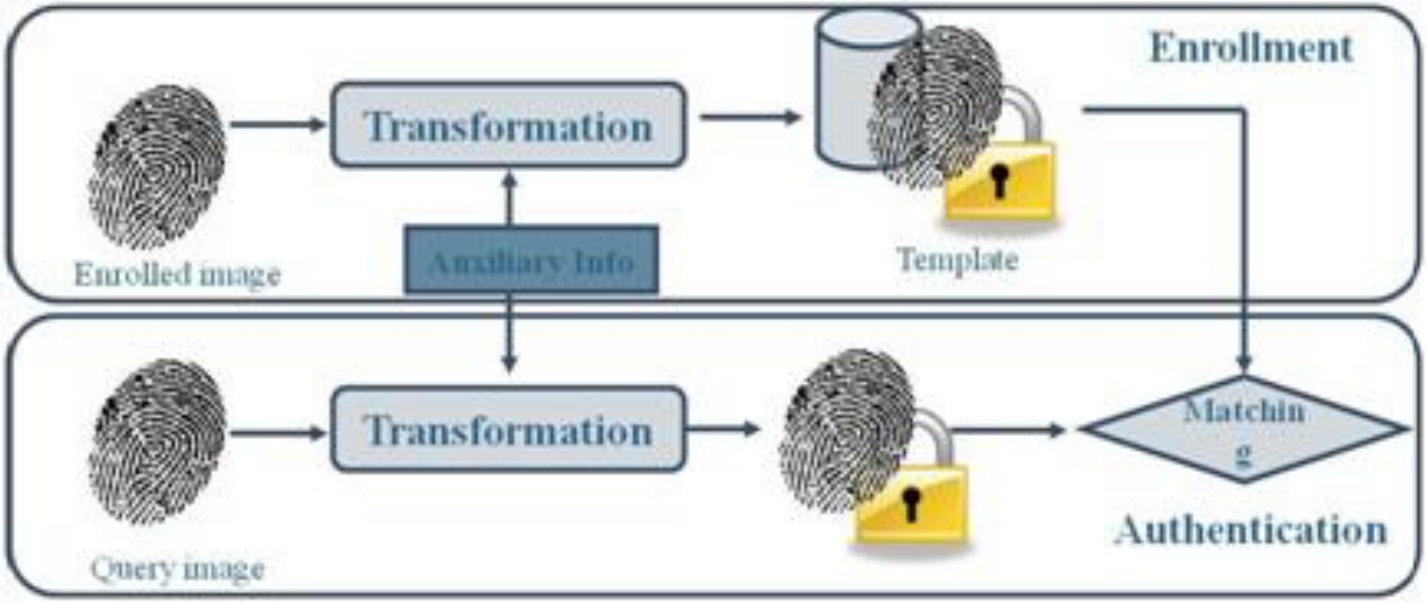


# Cancellable biometrics

- Biometric salting
- Non-invertible transforming

# Biometric salting

- Template protection approach in which the biometric features are transformed using a function defined by a user-specific key or password
- Transform is invertible, (secured) key is remembered and presented during the authentication



# Biometric salting: Advantages & Limitations

- Advantages:
  - Low false accept rate: due to the key
  - Biometric diversity : Multiple templates for the same biometric feature could be generated using different keys/passwords
  - Revoke and replace the compromised template

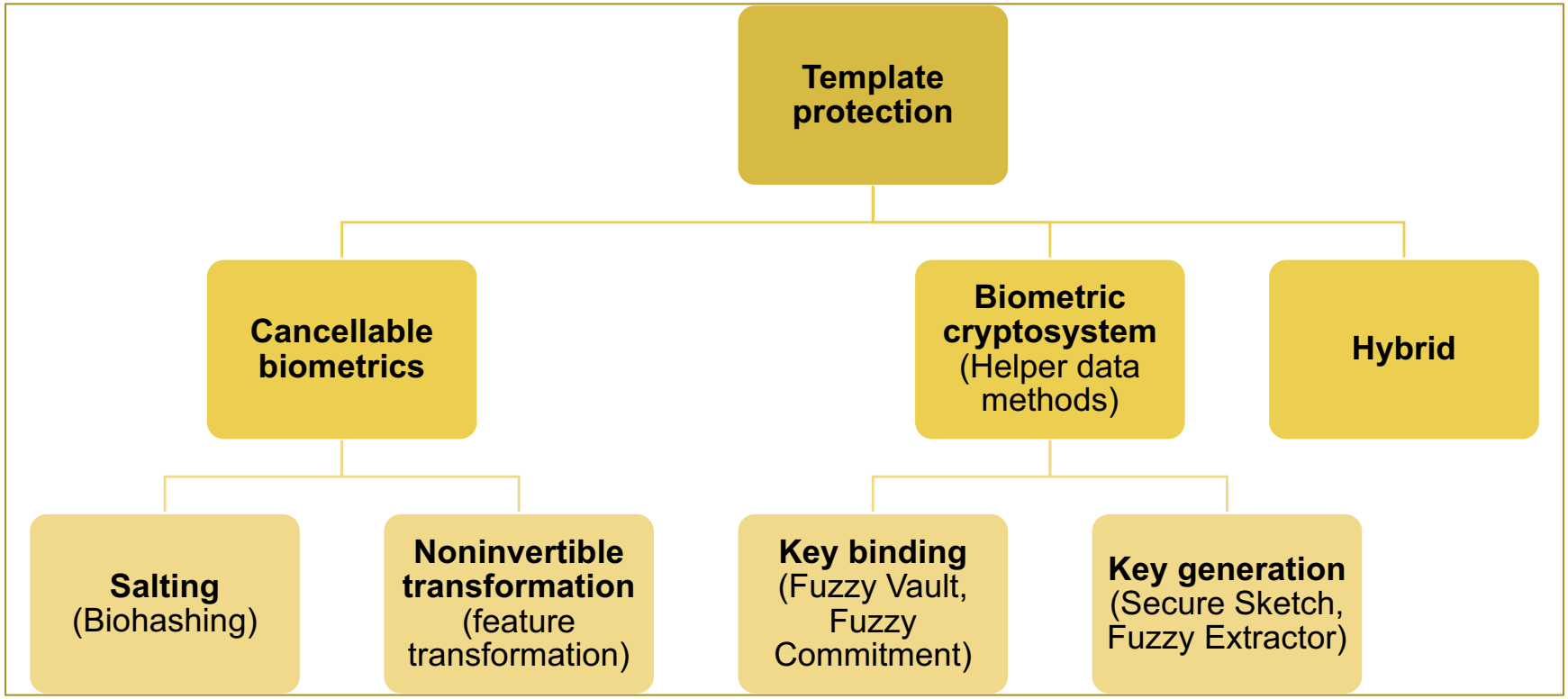
- Limitations:
  - If the user-specific key is compromised, the template is no longer secured due to invertible
  - Recognition performance usually decreases since matching takes place in the transformed domain

# Outline

- ~~Introduction~~
  - ~~Security issues of biometric systems~~
- Biometric template protection
  - Cancellable biometrics
  - Biometric cryptosystems
  - Hybrid approaches
- Reading:
  - Chapter 7 [1]
  - [2, 3]

# Non-invertible transforming

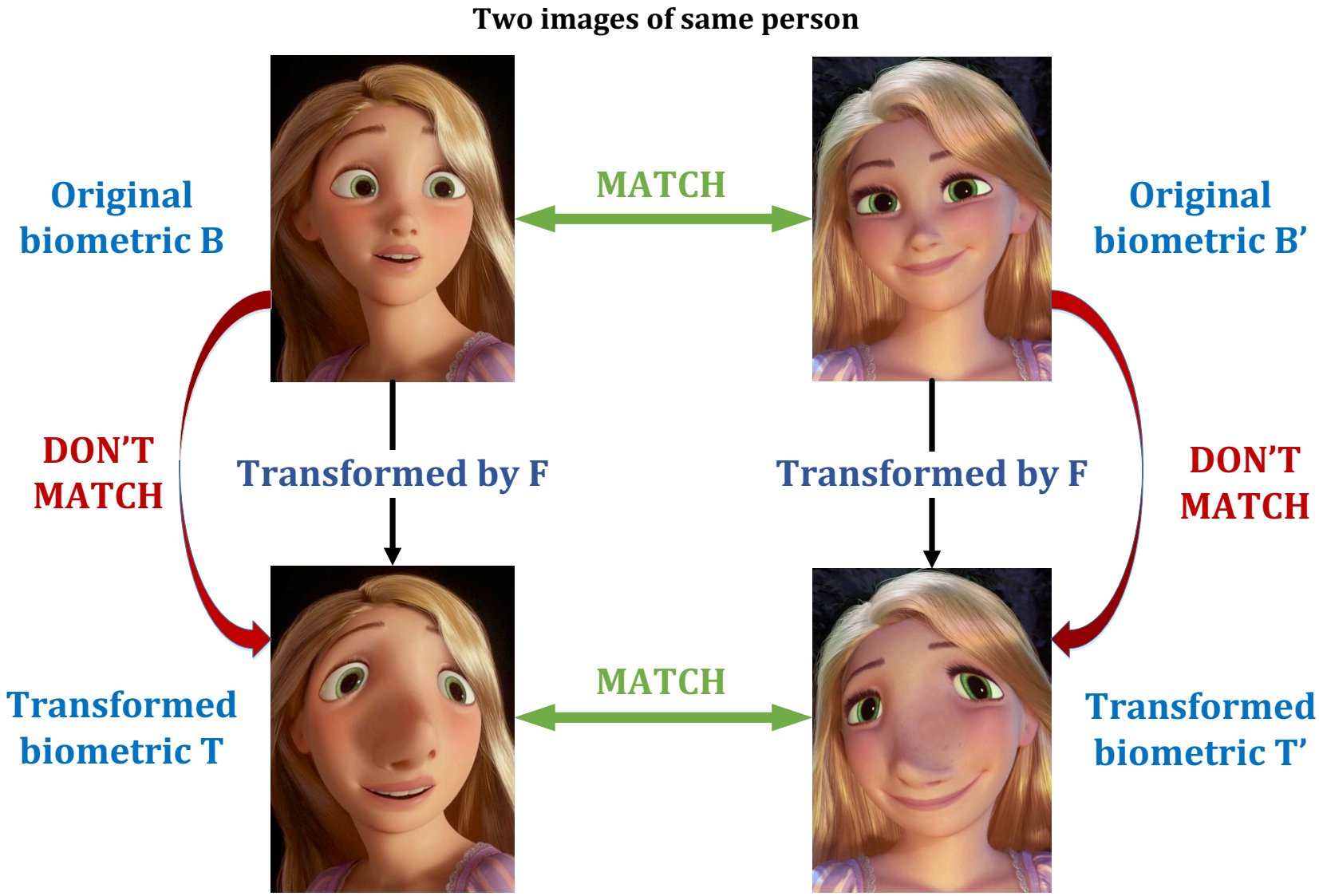
- Biometric salting
- Non-invertible transforming



# Non-invertible transforming (1)

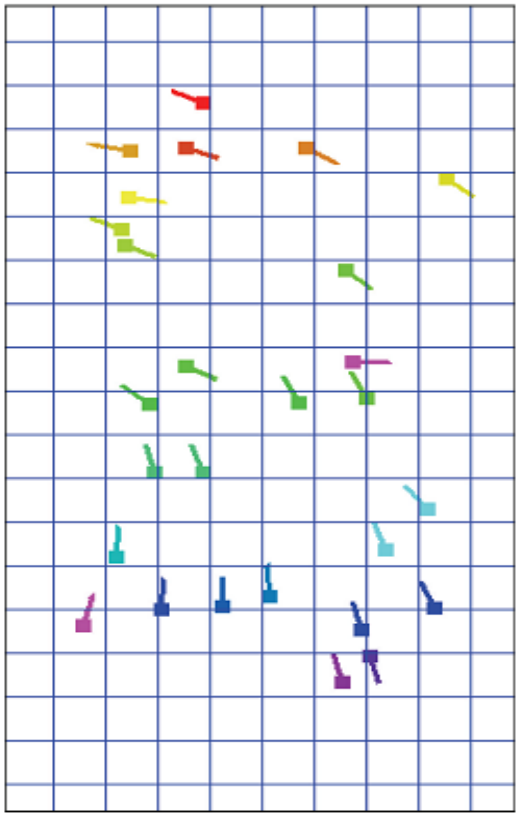
- The biometric features are transformed using a one-way function, that is **easy to compute** (in polynomial time) but **hard to invert**
- **Advantage:**
  - provides better security than the salting approach
  - can generate different templates for the same user by using different transformation function (parameters)
  - do not have to keep the transformed function secret
- **Disadvantage:**
  - loss of accuracy → balancing the discriminability and non-invertibility of the transformation function

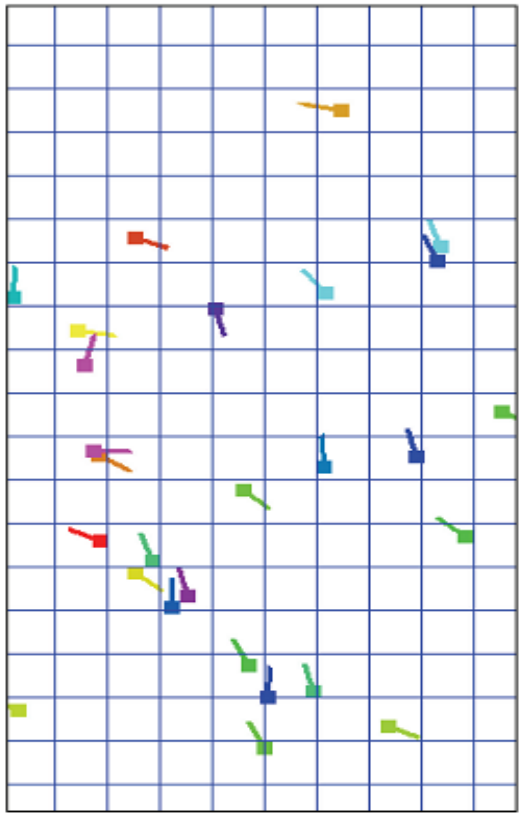
# Non-invertible transforming (2)



# Non-invertible transforming (3)

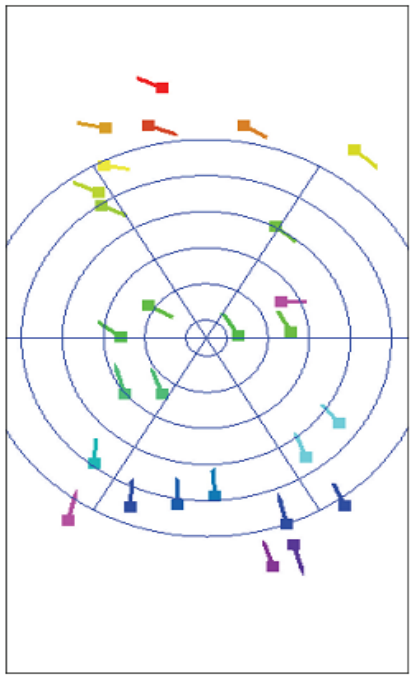
- Cancelable fingerprint templates: (Ratha et al. - Generating cancelable fingerprint templates, IEEE Transactions on Pattern Analysis and Machine Intelligence **29**(4) (2007)561-572)
  - Cartesian Transformation:

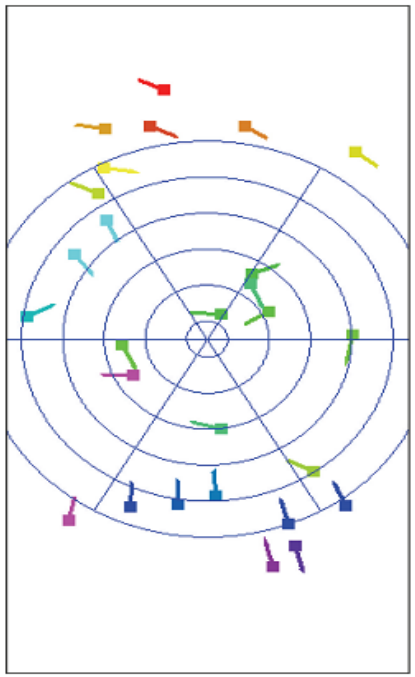




# Non-invertible transforming (4)

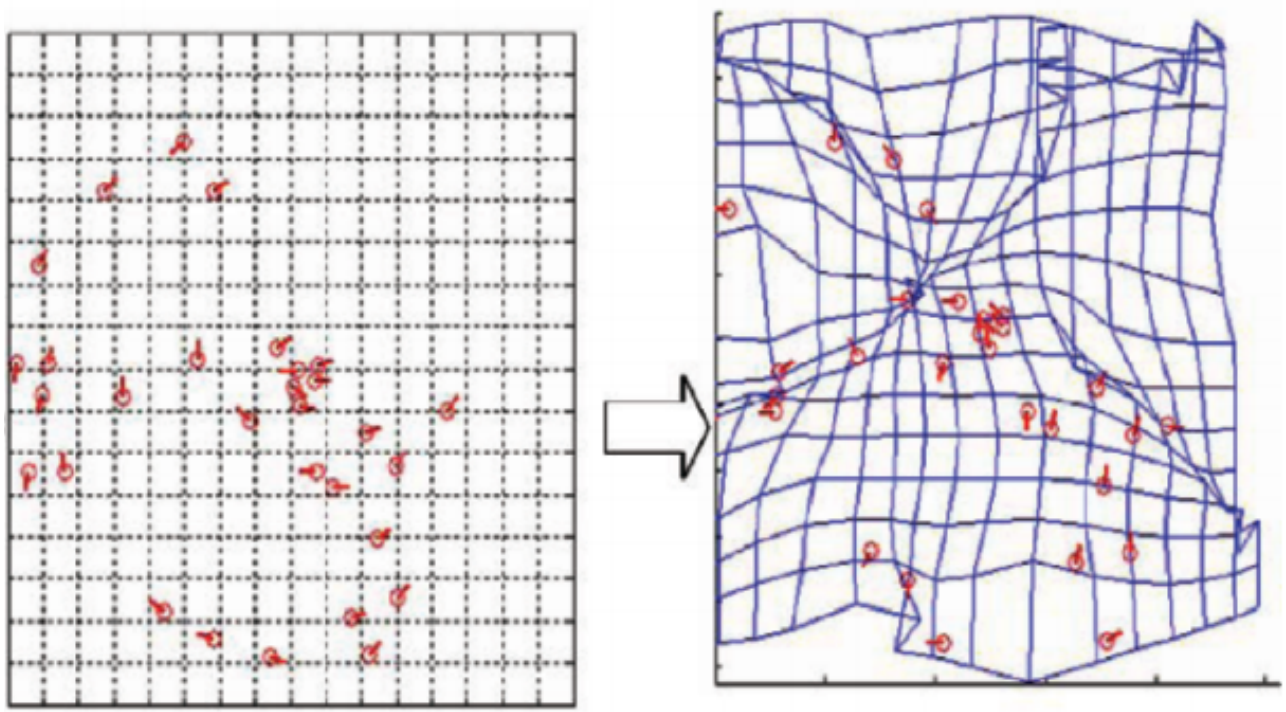
- Cancelable fingerprint templates: (Ratha et al. 2007)
  - Radial Transformation:





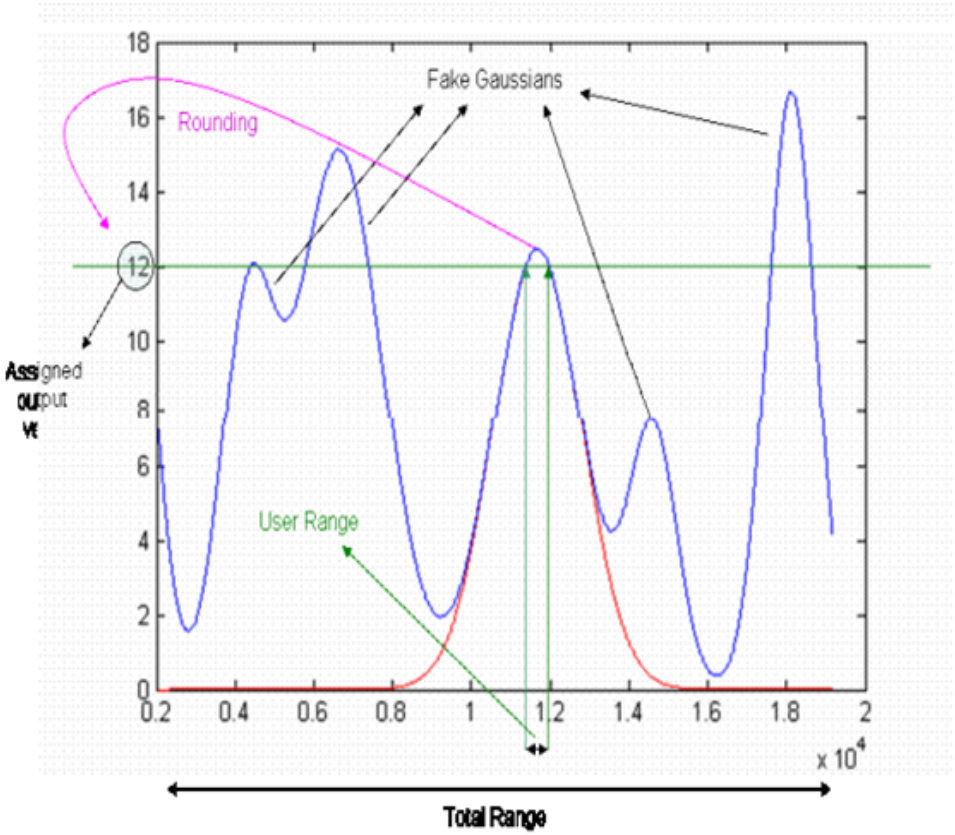
# Non-invertible transforming (5)

- Cancelable fingerprint templates: (Ratha et al. 2007)
  - Surface Folding Transformation



# Non-invertible transforming (6)

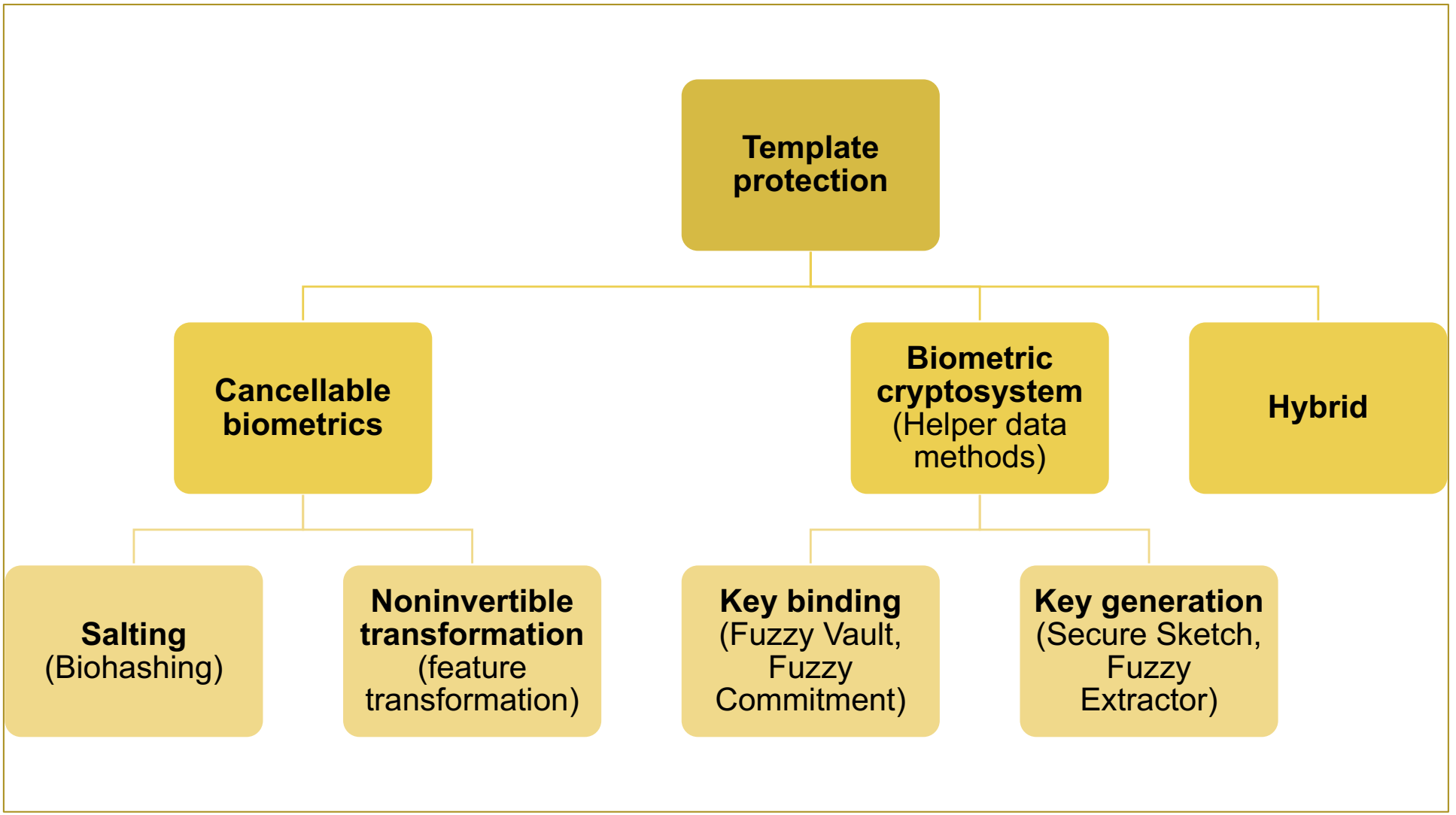
- Robust hashing: (Scutu et al. Memon- A secure biometric authentication scheme based on robust hashing, Proceedings of the 7th workshop on Multimedia and Security, ACM,2005, pp. 111-116.)



# Non-invertible transforming (7)

- The most challenge is that how to preserve the similarity of distances among transformed templates and among original templates
  - 2 transformed templates must be closed if the two original templates are closed
  - The error rate of the transformed biometric systems is similar to the generic biometric systems, but the transformed biometric systems protect the templates from being compromised

# Template protection

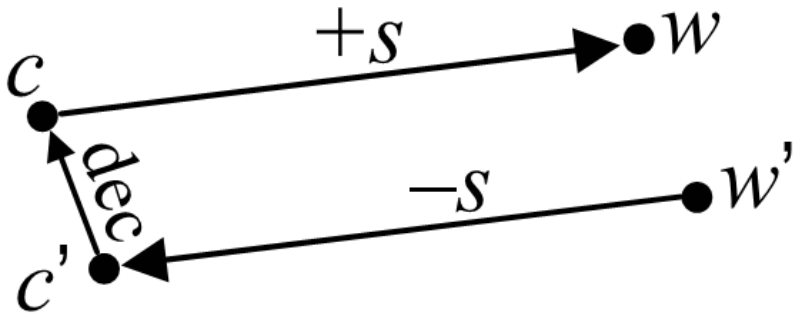


# Biometric cryptosystem and hybrid approach

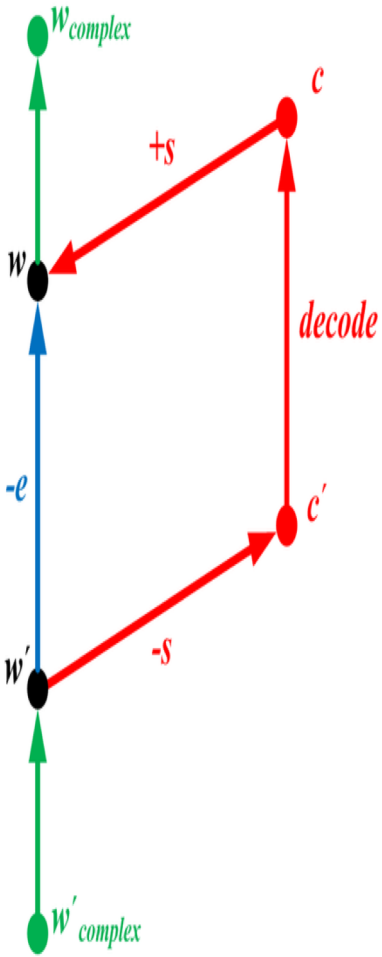
- Key-Binding cryptosystem
  - Fuzzy commitment scheme
  - Fuzzy vault scheme
- Key-Generation cryptosystem
  - Secure Sketch and Fuzzy extractor
- Hybrid approaches

# Code-offset construction

- Sketch:
  - Given $w \in M$
  - Select a random $c \in C$
  - Output: $s = \mathrm{SS}(w) = w - c$
- Recover:
  - Given $w' \in M$
  - $c' = w' - s$
  - Decode $c'$ to get $c$
  - Output: $w = c + s$



# Fuzzy Commitment Scheme




**Client**

- Biometric **B**

**Server**

Registration

- Code word **c**
- Computer $\delta = B \oplus c$
- Store $(\delta, Hash(c))$

Authentication

- Biometric **B'**

- Compute

$$c' = B' \oplus \delta$$

$$Hash(Decode(c'))$$

- If $Hash(c)=Hash(Decode(c'))$

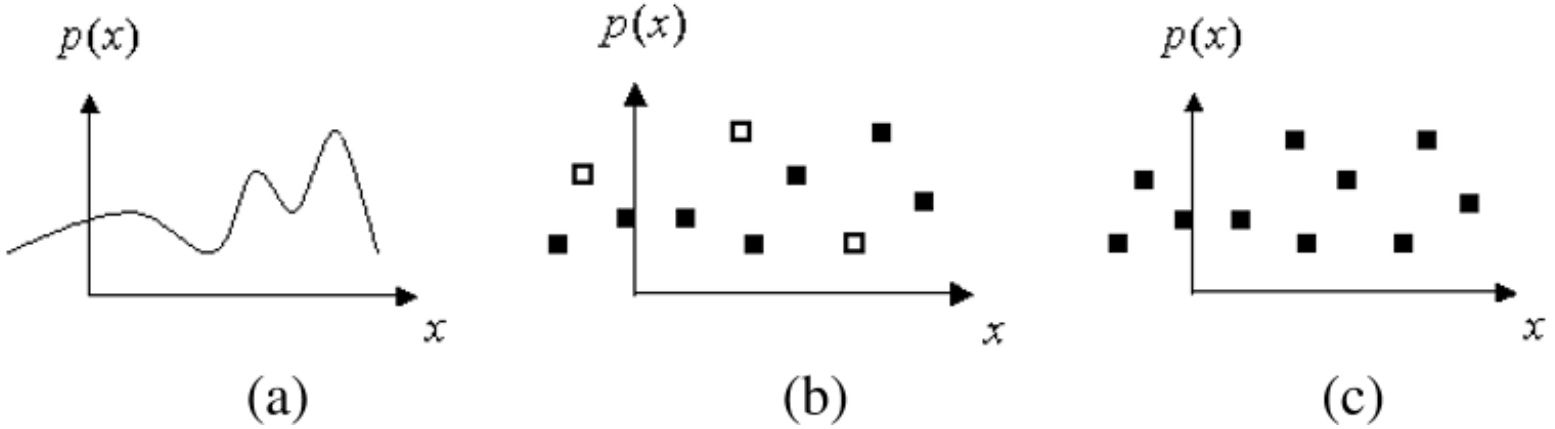
→ Authenticated

# Part 4: Biometric cryptosystem and hybrid approach

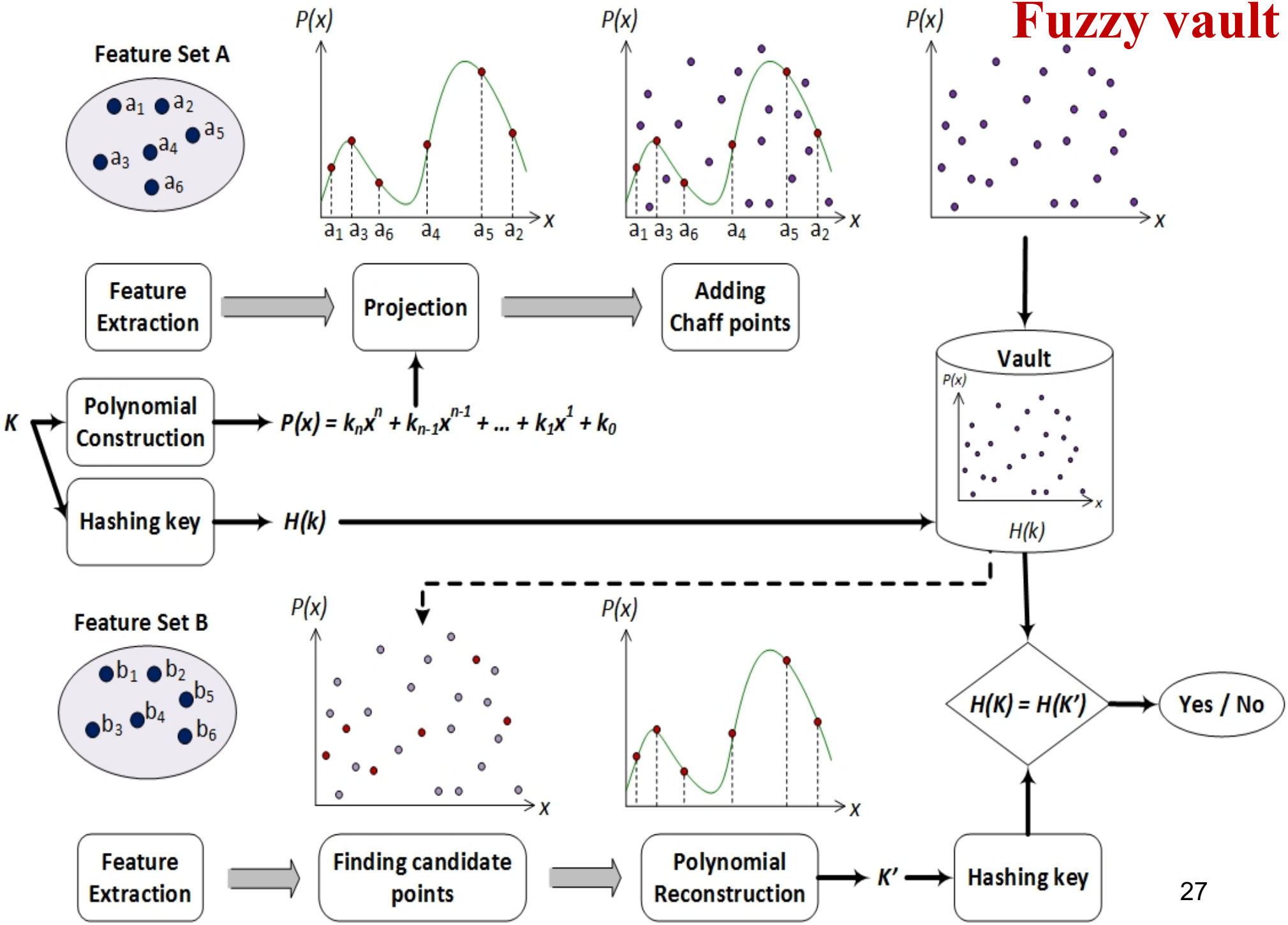
- Key-Binding cryptosystem
  - Fuzzy commitment scheme
  - Fuzzy vault scheme
- Key-Generation cryptosystem
  - Secure Sketch and Fuzzy extractor
- Hybrid approaches

# Fuzzy vault

- Fuzzy vault is one of the most popular biometrics template protection schemas
- The idea is that Alice places a secret k in a fuzzy vault and locks it using a set A of elements from some public universe U
- To unlock the vault and retrieve k, Bob must present a set B similar to A, i.e. B and A overlap substantially



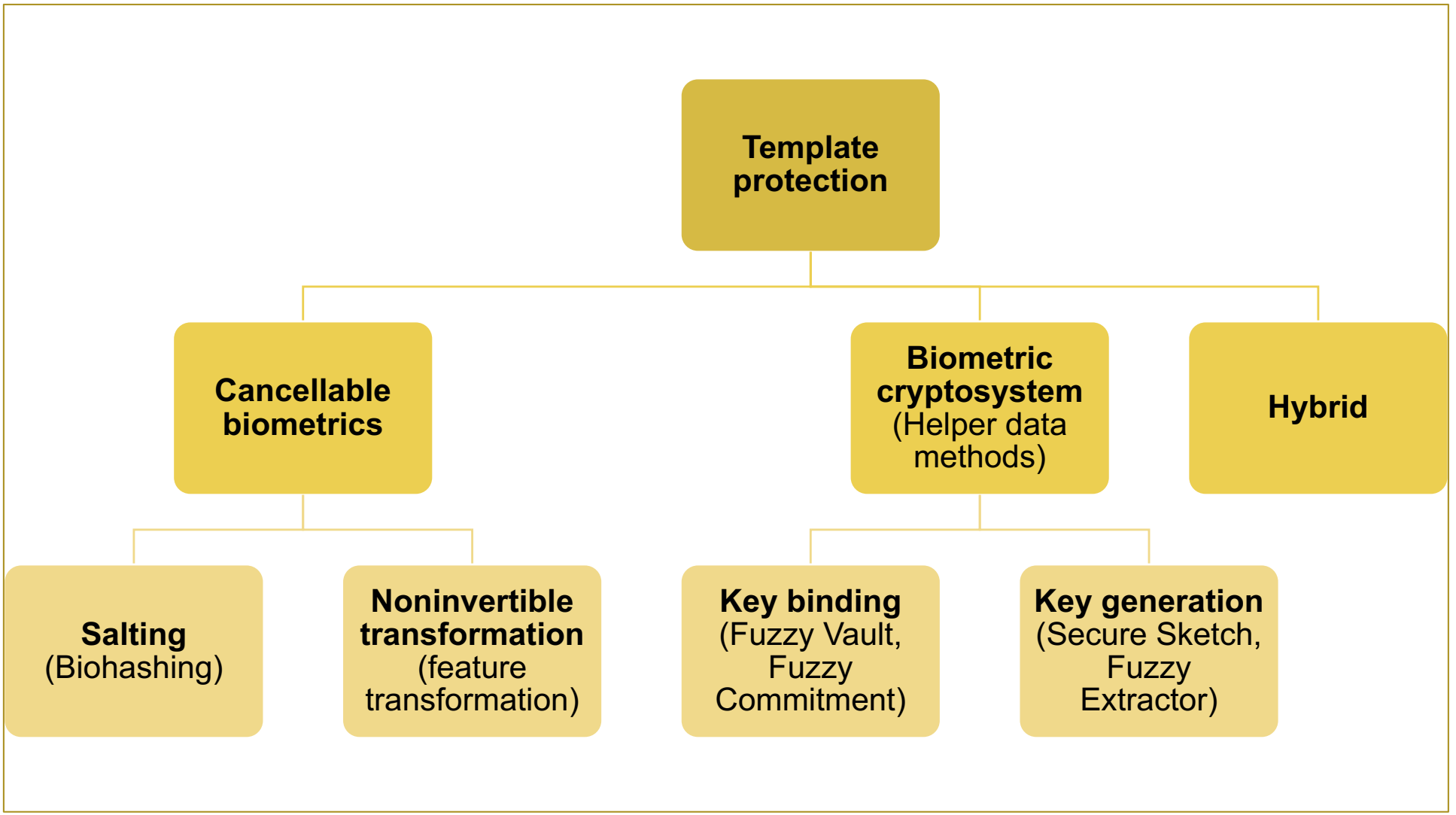
# Fuzzy vault


Feature Set A
a1 a2 a5 a4 a3 a6
P(x)
a1 a3 a6 a4 a5 a2
x
Feature Extraction
Projection
Adding Chaff points
K
Polynomial Construction
P(x) = knx^n + kn-1x^n-1 + ... + k1x^1 + k0
Hashing key
H(k)
Vault
Feature Set B
b1 b2 b5 b4 b3 b6
Finding candidate points
Polynomial Reconstruction
K'
H(K) = H(K')
Yes / No

# How to generate chaff points?

- Most popular approach: generate chaff points randomly!
- Constraints:
  - Number of chaff points
  - Minimum distance among points in Vault
  - Chaff points must not be on the P(x) graph
  - Distribution of chaff points must be around genuine points

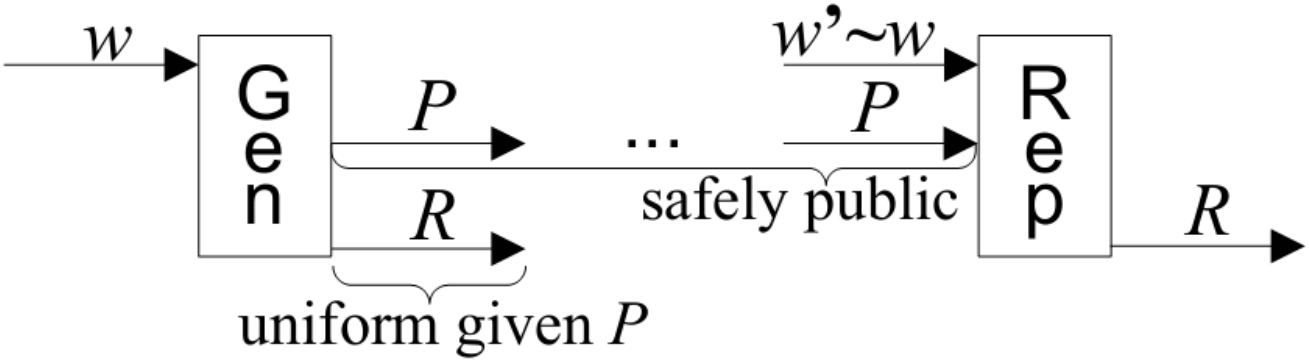
# Template protection



# Secure Sketch & Fuzzy Extractor

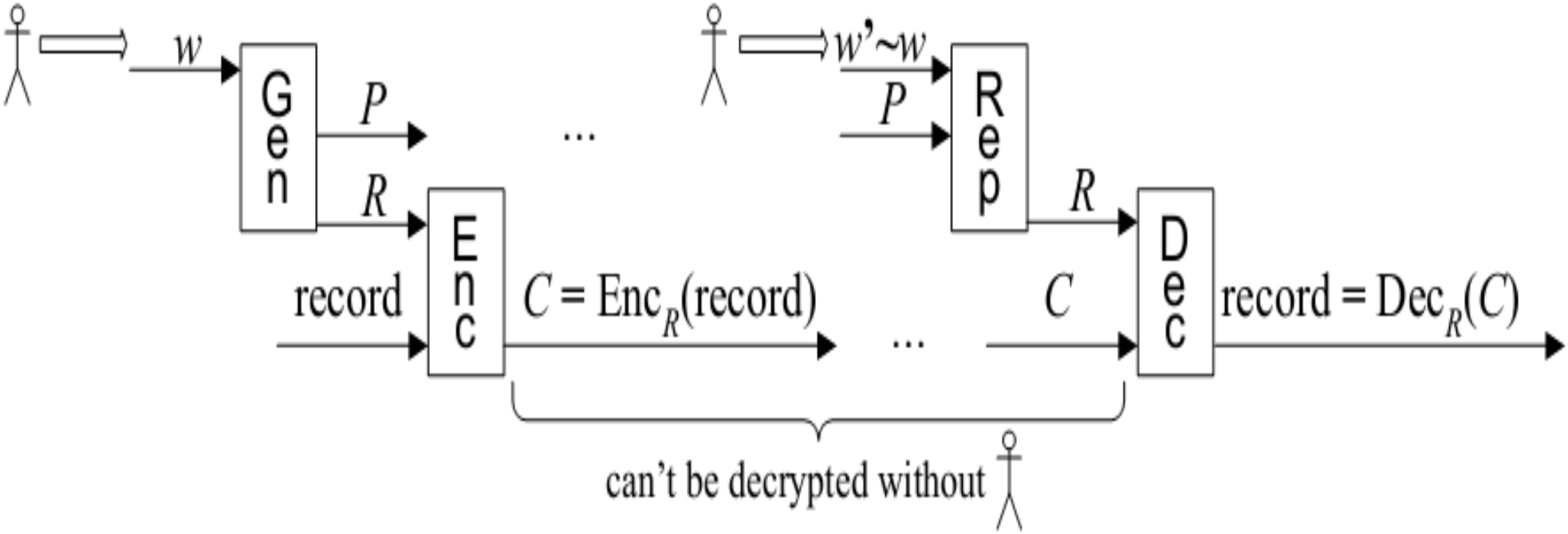
- Secure sketch


- Fuzzy Extractor



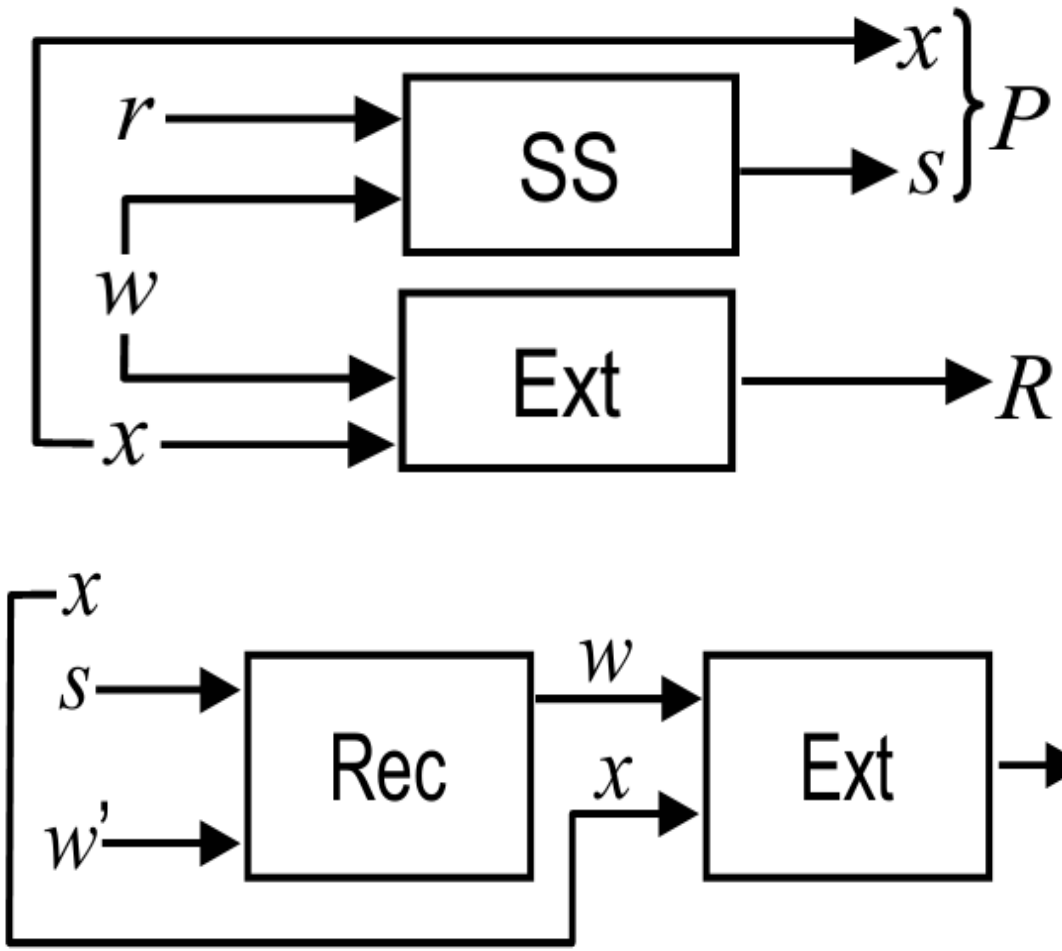
# Fuzzy Extractor

- Cryptographic application



# Fuzzy Extractor from Secure Sketch

❖ Secure Sketch ⇨ Fuzzy Extractor

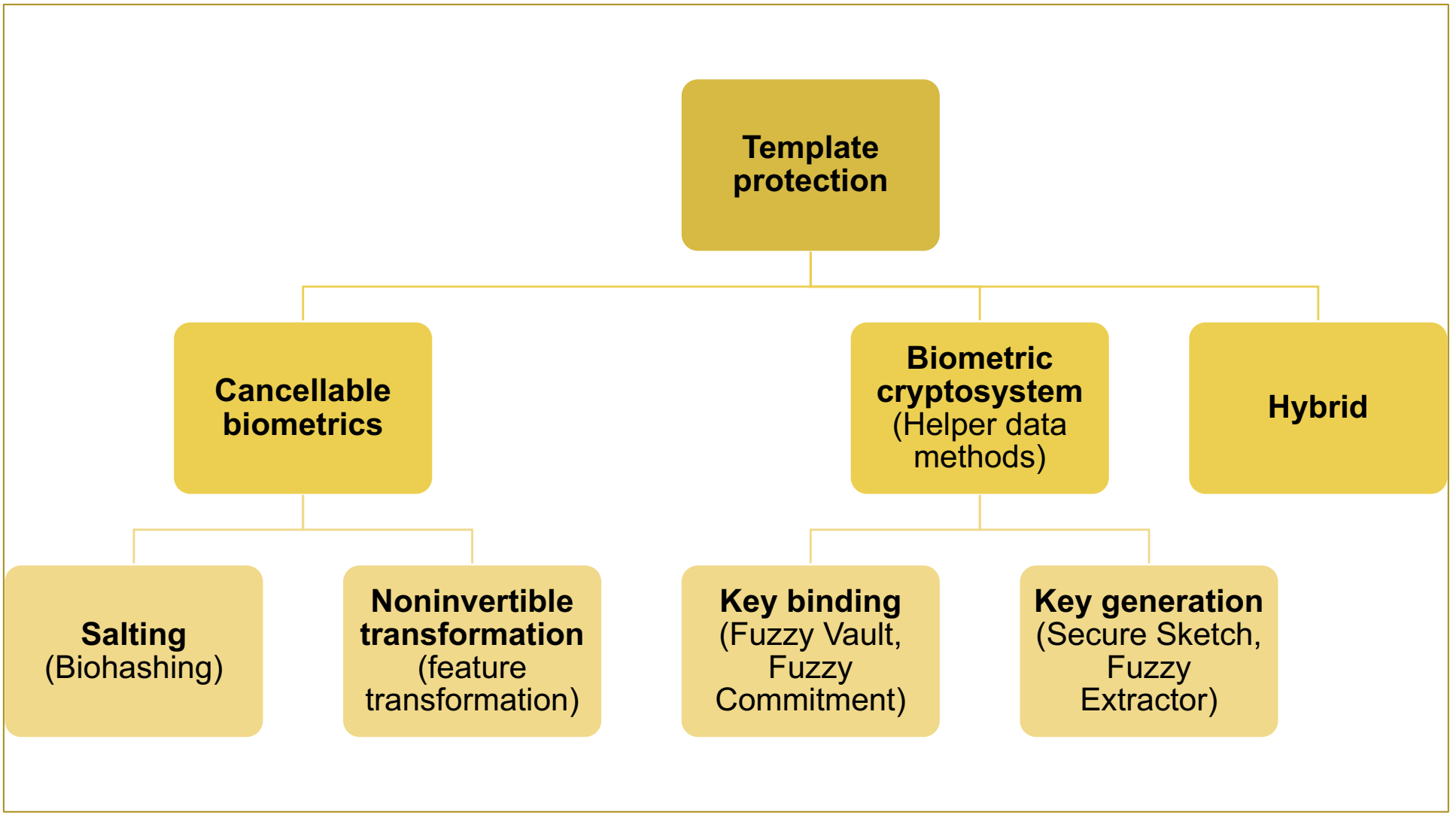



- To preserve high entropy, SS is employed to construct fuzzy extractor. The SS is applied to w to get the sketch s
- Along with this procedure, a randomness x and biometrics w are used as input of the strong extractor Ext to obtain the key R
- The pair (s, x) is stored as the helper data P
- To reproduce R from w' (close to w), first retrieve P = (s, x), then use Rec( s, w') to recover w, and lastly Ext(w, x) to have R

# Outline

- ~~Introduction~~
  - ~~Security issues of biometric systems~~
- ~~Biometric template protection~~
  - ~~Cancellable biometrics~~
  - ~~Biometric cryptosystems~~
  - Hybrid approaches
- Reading:
  - Chapter 7 [1]
  - [2, 3]

# Template protection



# Hybrid Approach

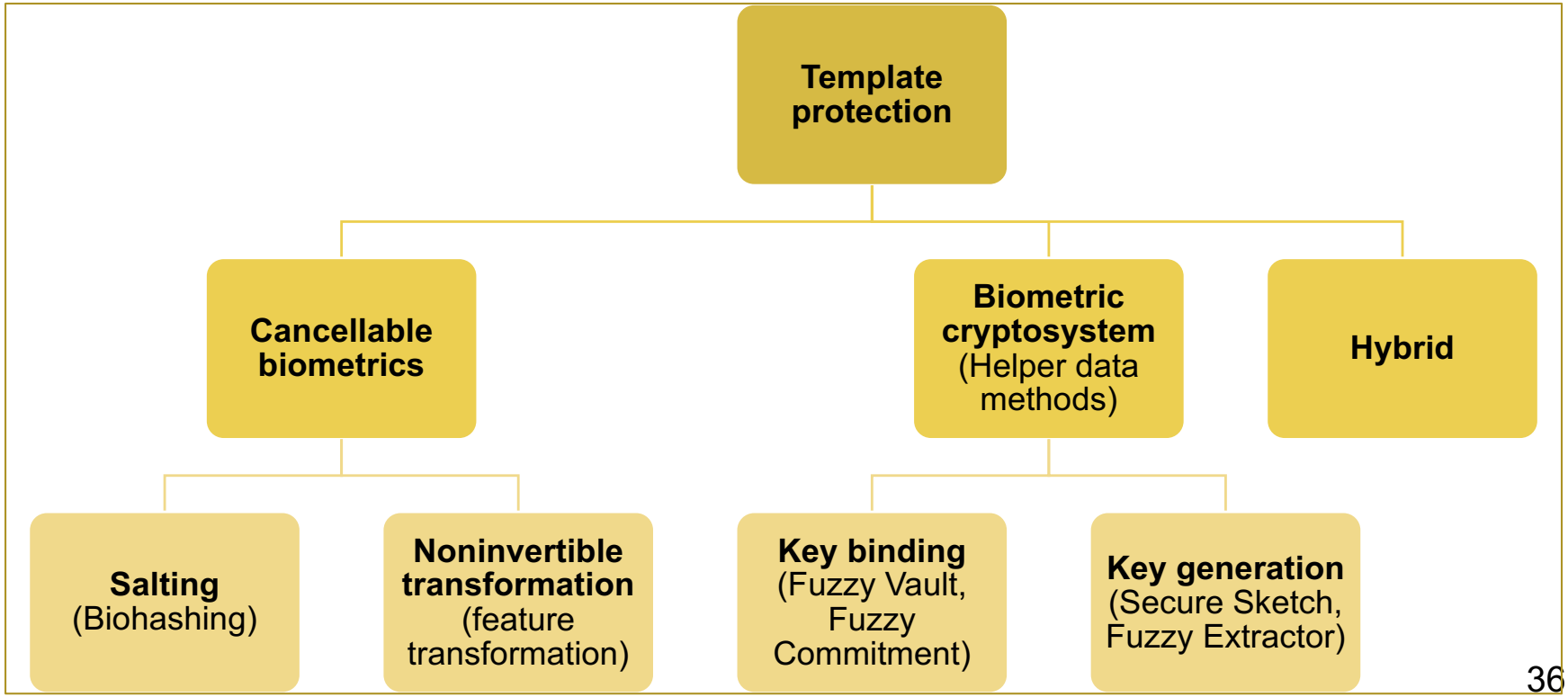
- Combine two or more approaches to a single protection scheme:
  - Improve accuracy or security
  - Increase complexity of computing and impl. cost
- Hybrid fingerprint-based biometric cryptosystems: fuzzy vault + fuzzy commitment scheme
- Cancelable fuzzy vault with periodic transformation for biometric template protection security

Nagar Abhishek, Karthik Nandakumar, and Anil K. Jain (2010): A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recognition Letters* 31(8):733-741

**Dang, Tran Khanh, et al. (2016):** Cancellable fuzzy vault with periodic transformation for biometric template protection. *IET Biometrics* 5(3): 229-235

# Contents

1. Biometrics: A Quick Introduction
2. Biometric System Architecture



# Contents

# Summary

- Security issues of biometric systems
- Biometric template protection
  - Cancellable biometrics
  - Biometric cryptosystems
  - Hybrid approaches

# Q&A

www.cse.hcmut.edu.vn/~khanh


khanh@hcmut.edu.vn

https://www.facebook.com/dang.ssolutions