Biometric Matching in Encrypted Domain

Karthik Nandakumar

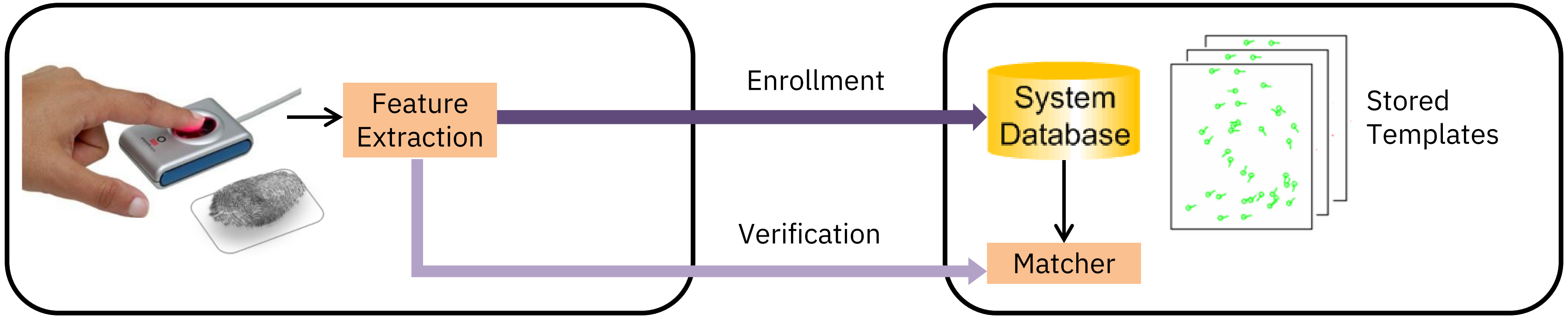
Associate Professor

CSE Department, Michigan State University, USA

CV Department, MBZUAI, Abu Dhabi, UAE

https://www.sprintai.org

How Biometric Systems Work?



- Templates consist of features extracted from biometric images/samples
- Usually stored in a database during enrollment – to be used later for verification
- A biometric template should be salient, invariant and compact

Examples of Biometric Templates

Fingerprint

Minutiae (Template)

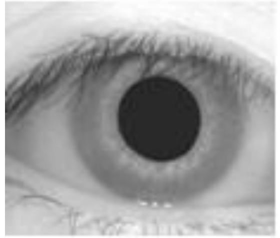
X	Y	θ
207	138	198
81	144	326
73	158	144
135	203	155
53	205	313
¦	¦	¦

Face

Face Embedding (Template)

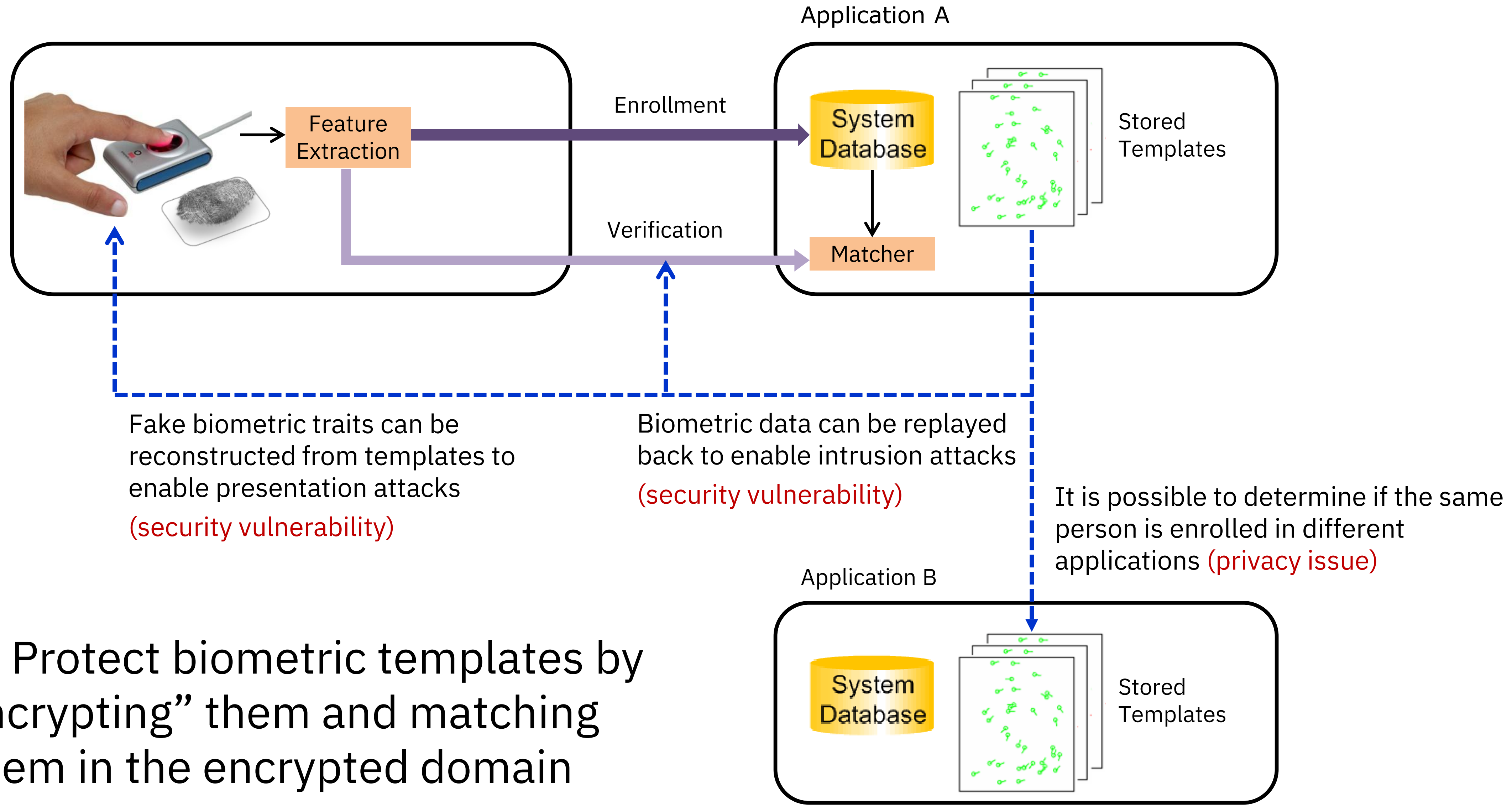
0.23
0.15
-0.01
0.09
-0.03
0.11
0.30
-0.04
0.02
0.10

Iris



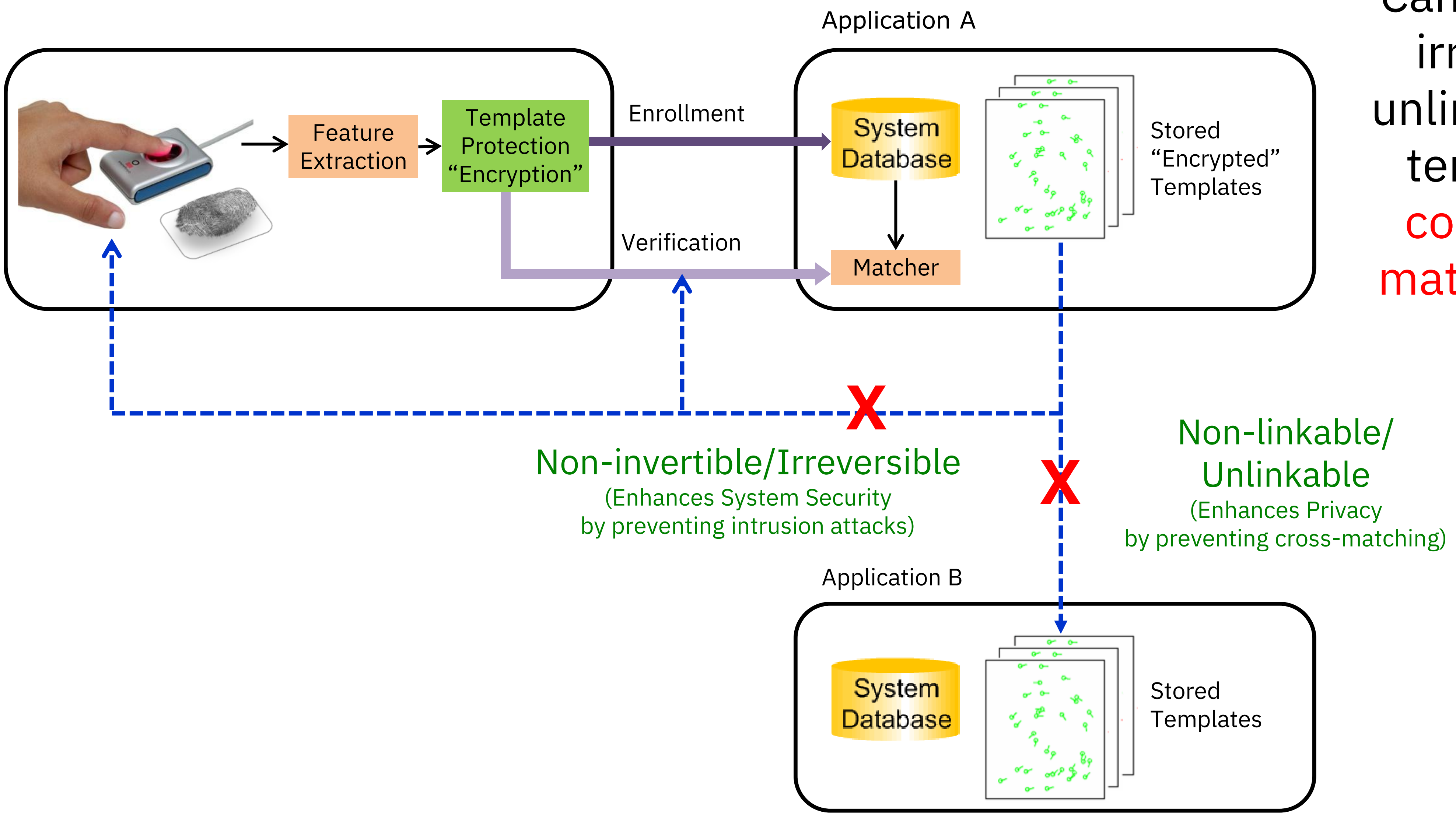
IrisCode (Template)

Potential Misuse of Biometric Templates



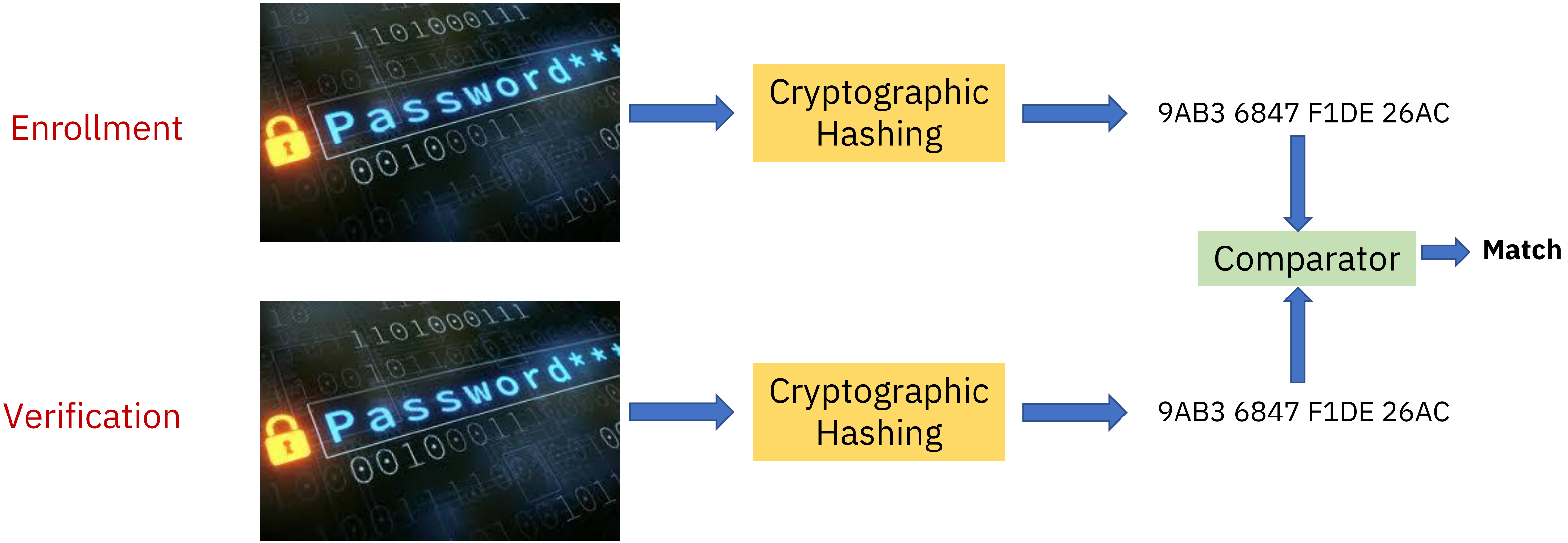
Goal: Protect biometric templates by "encrypting" them and matching them in the encrypted domain

Biometric Template Protection/Encryption



Can we generate an irreversible AND unlinkable biometric template without compromising on matching accuracy?

Password Protection With Cryptographic Hashing



- Passwords provided during enrollment & verification must be exactly identical
- Since two biometric samples from the same person are seldom identical, the above approach cannot be directly applied to secure biometric templates

Cryptographic vs. Biometric Hashing

Cryptographic Hash Functions

Following problems should be computationally infeasible

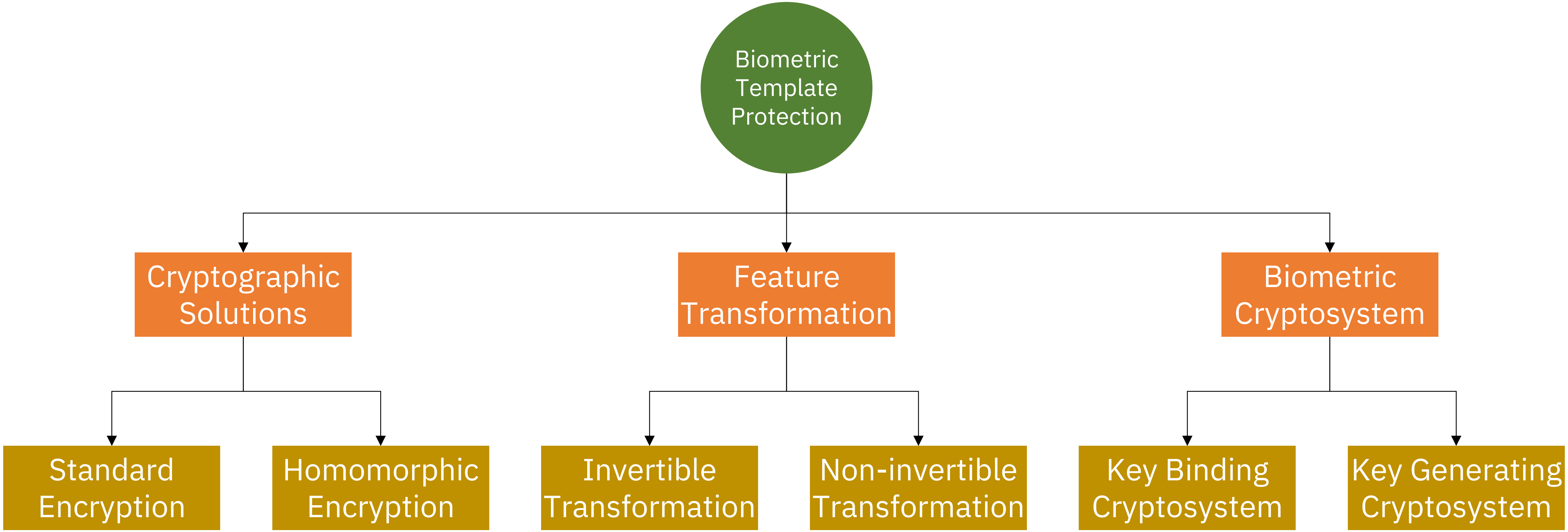
- Given $\boldsymbol{y}$, find x such that $h(\boldsymbol{x}) = \boldsymbol{y}$ (first pre-image resistance)
- Given $\boldsymbol{x}$, find $\boldsymbol{x}' \neq \boldsymbol{x}$ such that $h(\boldsymbol{x}) = h(\boldsymbol{x}')$ (second pre-image resistance)
- Find $(\boldsymbol{x}, \boldsymbol{x}')$ with $\boldsymbol{x}' \neq \boldsymbol{x}$, such that $h(\boldsymbol{x}) = h(\boldsymbol{x}')$ (collision resistance)

Robust Biometric Hash

- Given y, it should be computationally infeasible to find $\boldsymbol{x}$ such that $h(\boldsymbol{x}) = \boldsymbol{y}$ (first pre-image resistance)
- Given $\boldsymbol{x}$, any $\boldsymbol{x}' \neq \boldsymbol{x}$ with $d_1(\boldsymbol{x}, \boldsymbol{x}') \leq \varepsilon_1$, then $h(\boldsymbol{x}) = h(\boldsymbol{x}')$ (or $d_2(h(\boldsymbol{x}), h(\boldsymbol{x}')) \leq \varepsilon_2$)
- For any (x, x') with $d_1(\boldsymbol{x}, \boldsymbol{x}') \leq \varepsilon_1$, then $h(\boldsymbol{x}) = h(\boldsymbol{x}')$ (or $d_2(h(\boldsymbol{x}), h(\boldsymbol{x}')) \leq \varepsilon_2$)

Is a robust biometric hash with above properties practically feasible?

Taxonomy of Biometric Encryption Approaches



Hybrid schemes employ more than one basic approach

Threat Models for Security Analysis (ISO-30136)

- Naïve Model
  No information, black box, no access to any biometric data

- Collision Model
  Adversary possesses a large amount of biometric data

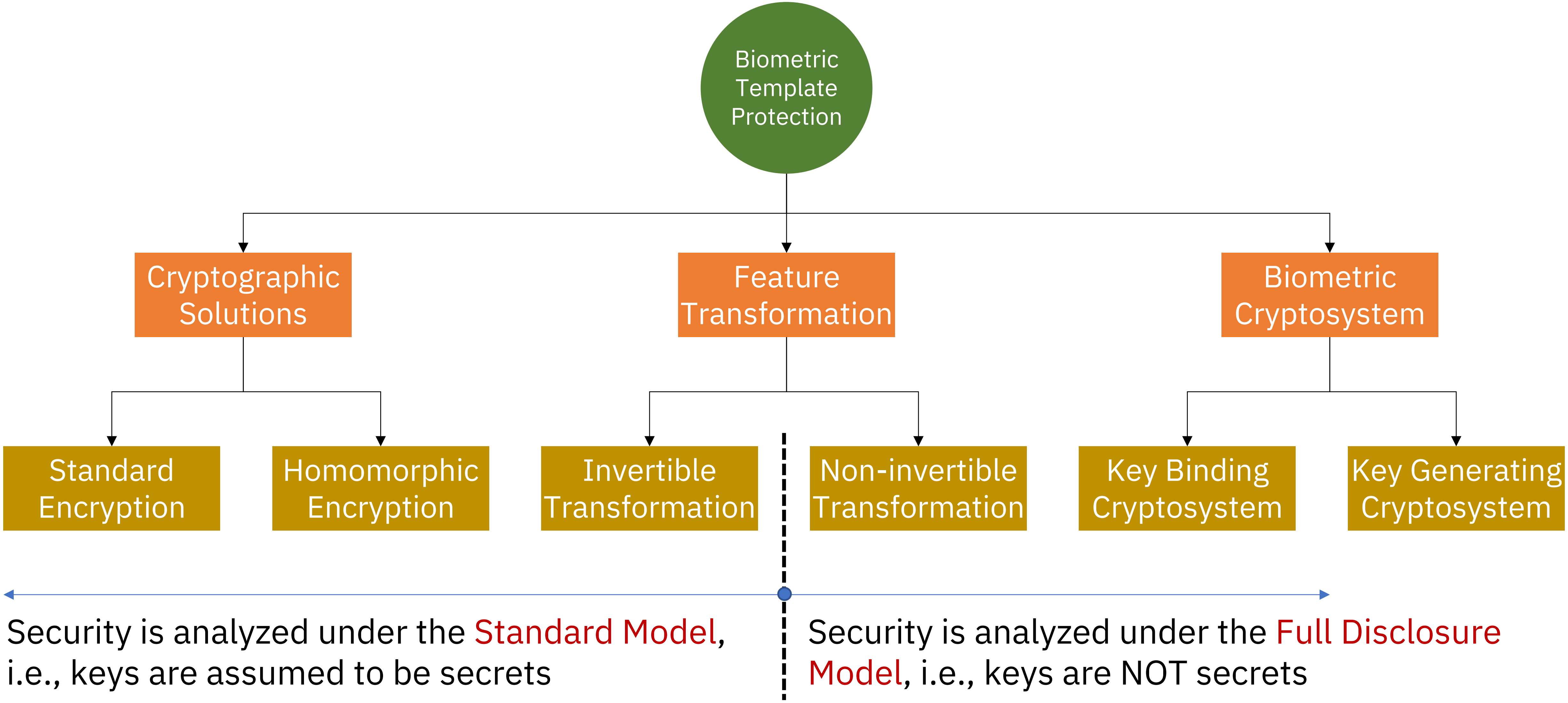
- General Models
  Full knowledge of the underlying template protection scheme

  - Standard Model
    - None of the secrets
    - Related to known ciphertext attack

  - Advanced Model
    - Augmented with the capability of the adversary to execute part of or all submodules that make use of the secrets
    - Related to chosen plaintext attack and chosen ciphertext attack

  - Full Disclosure Model
    - Augmented by disclosing the secrets to the adversary (e.g. malicious insider)

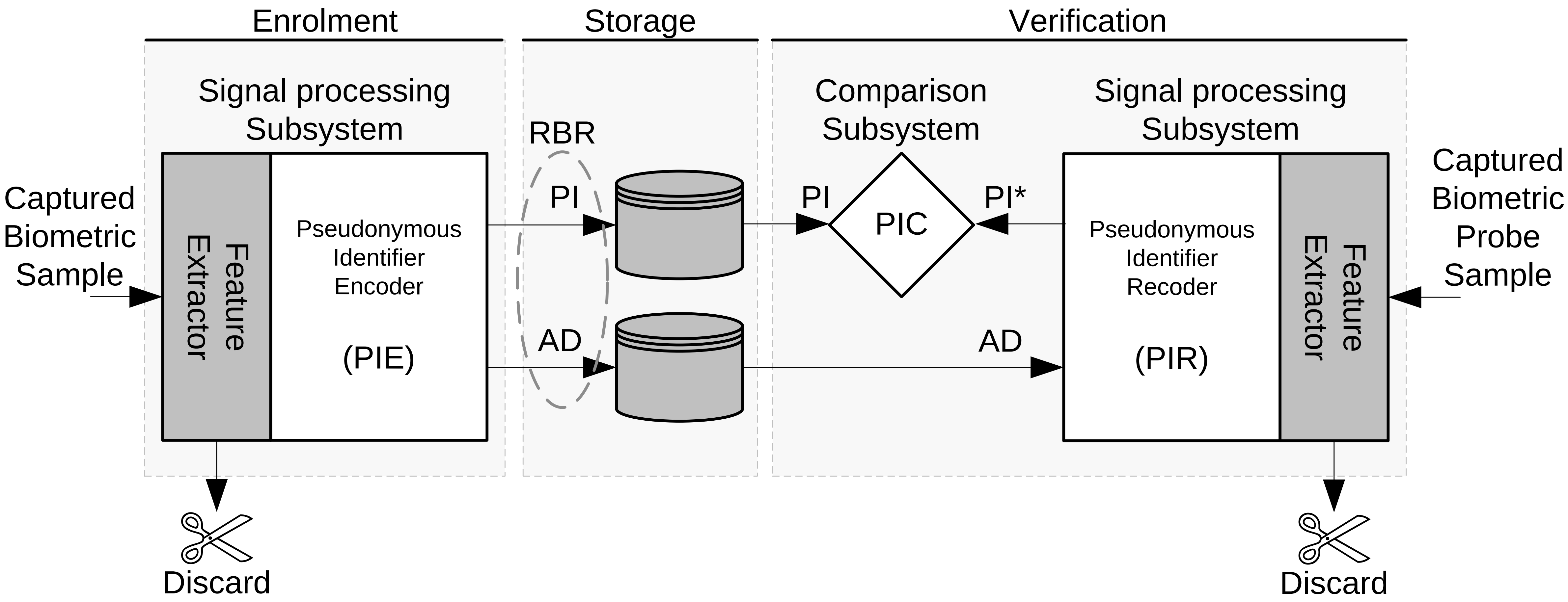
Taxonomy of Biometric Encryption Approaches



Security is analyzed under the Standard Model, i.e., keys are assumed to be secrets

Security is analyzed under the Full Disclosure Model, i.e., keys are NOT secrets

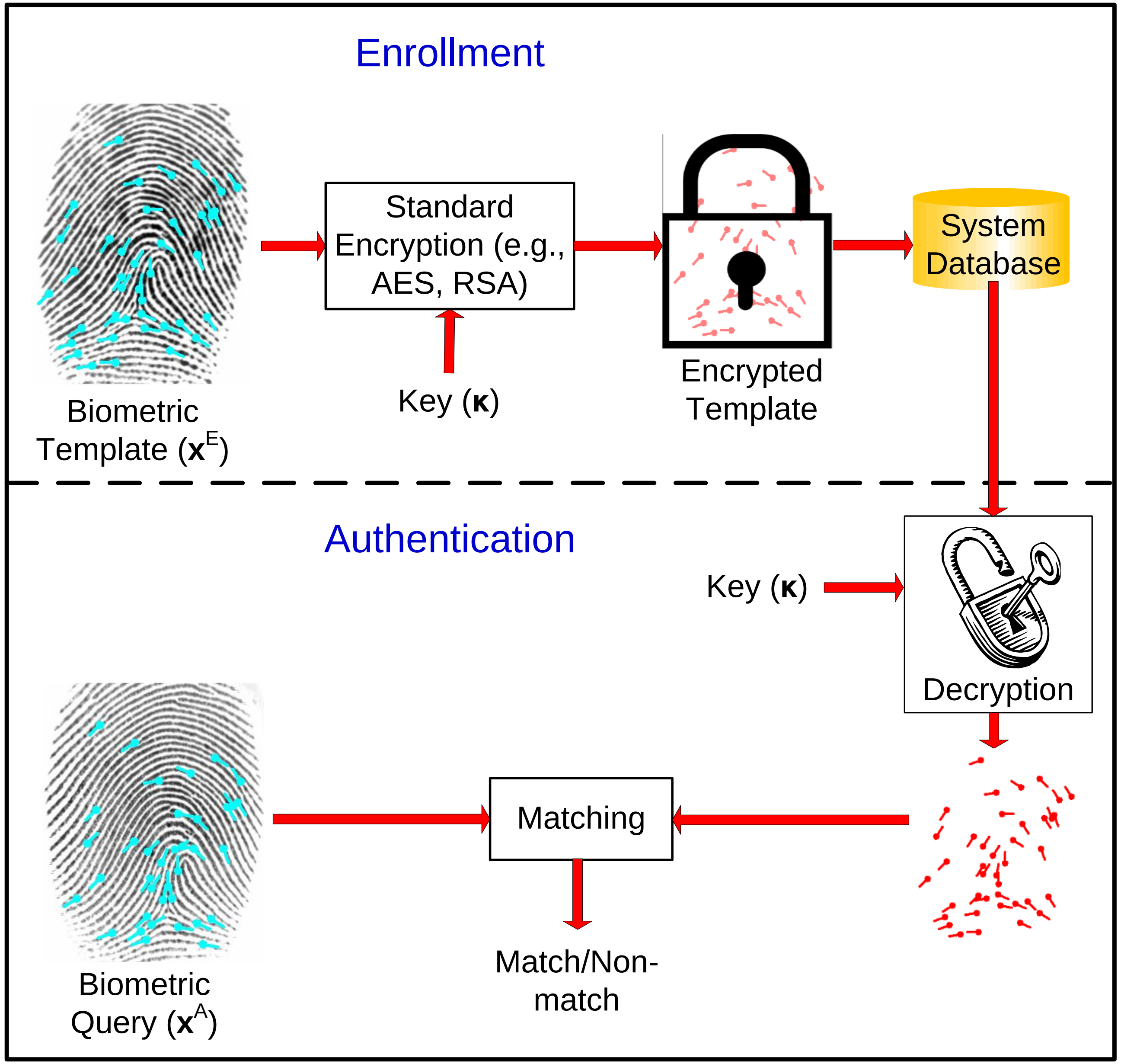
Standardized Biometric Encryption Framework



PI: Pseudonymous Identifier
AD: Auxiliary Data
PIC: Pseudonymous Identifier Comparator

ISO/IEC Standard 24745:
Biometric Information Protection

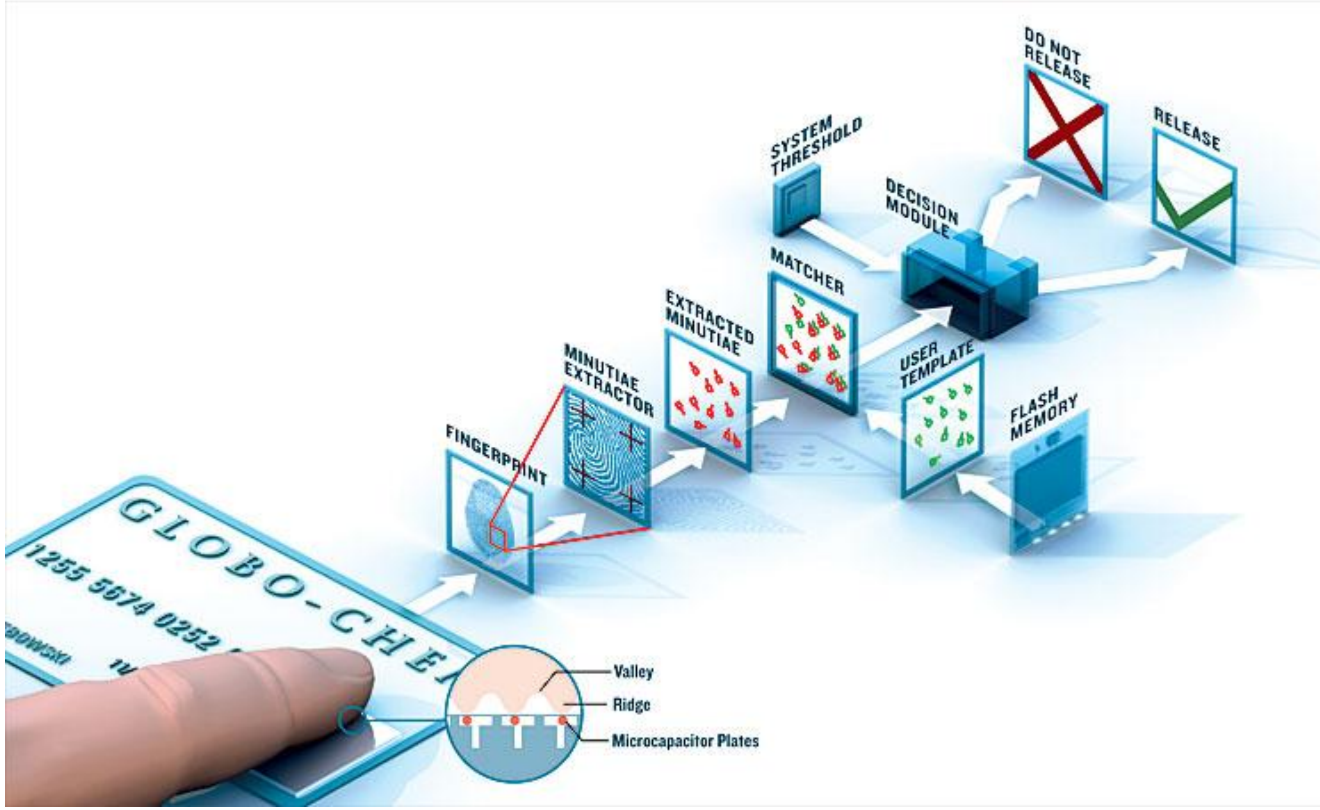
Standard Encryption Approach



- Key management problem: security of encryption/ decryption key
- Matcher needs original template; decrypted templates are vulnerable

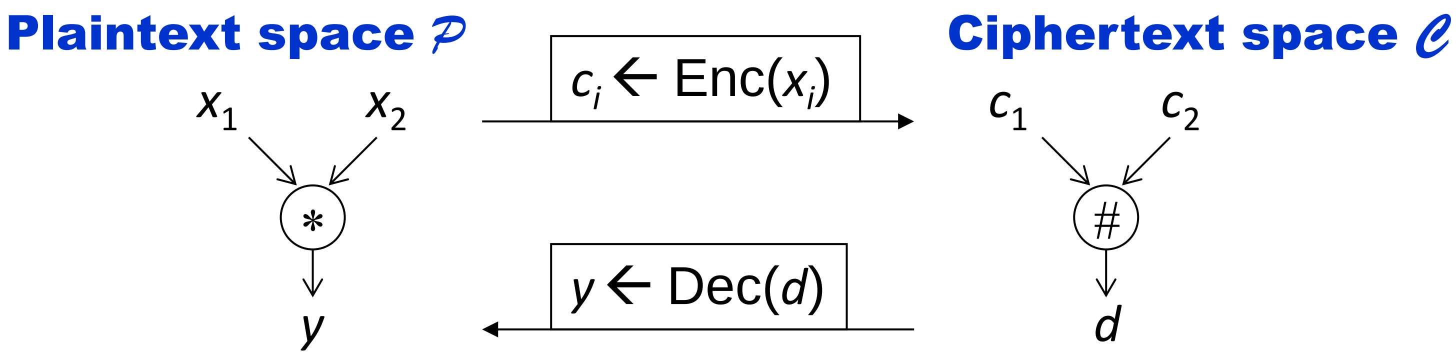
Biometric System on Card/Device

- Complete system (sensor, feature extractor, matcher, template) resides on card/device
- Template is stored within a secure enclave and is never transmitted or released outside



Homomorphic Encryption Approach

- Homomorphic Encryption (HE) provides the ability to perform an algebraic operation on plaintext by performing a (possibly different) algebraic operation on ciphertext



- "Raw RSA" is an example of multiplicative homomorphism

Enc: $c \leftarrow x^e \bmod N$, Dec: $x \leftarrow c^d \bmod N$

$c_1 c_2 = x_1^e \, x_2^e = (x_1 x_2)^e \bmod N$

Fully Homomorphic Encryption

Four procedures: KeyGen, Enc, Dec, Eval

- (sk,pk) ← KeyGen(λ)
  - Generate random public/secret key-pair
- c ← Enc(pk, m)
  - Encrypt a message with the public key
- m ← Dec(sk, c)
  - Decrypt a ciphertext with the secret key
- c ← Eval(pk, f, $c_1,\ldots,c_t$)
  - c_i is the encryption of input m_i
  - f is function to be evaluated
  - c is the encryption of the output $f(m_1,\ldots,m_t)$

FHE scheme should work for *any* well-defined function f (currently only low-degree polynomials are feasible) and be computationally "efficient"

Simple Construction of a FHE

- Shared secret key: odd number p
- To encrypt a bit m in $\{0,1\}$:
  - Choose at random small r, large q
  - Output $c = \boxed{m + 2r} + pq$
    - Ciphertext is close to a multiple of p
    - m = LSB of distance to nearest multiple of p
- To decrypt c:
  - Output $m = (c \bmod p) \bmod 2$
- Public key is many "encryptions of 0"
  - $x_i = q_i p + 2r_i$
- $Enc_{pk}(m) = \text{subset-sum}(x_i\text{'s}) + m$
- $Dec_{sk}(c) = (c \bmod p) \bmod 2$

The "noise" should be much smaller than p

❖ Semantic security is based on the approximate GCD problem
- Given many $x_i = s_i + q_i p$, output p
- Best known attacks (lattices) require 2^λ time

Homomorphic Properties of FHE

- Suppose $c_1=m_1+2r_1+q_1p$, $c_2=m_2+2r_2+q_2p$

Noise: Distance to nearest multiple of p

- $c_1 + c_2 = (m_1+m_2) + 2(r_1+r_2) + (q_1+q_2)p$
  - If $(m_1+m_2)+2(r_1+r_2)$ still much smaller than p
  - $c_1+c_2 \bmod p = (m_1+m_2) + 2(r_1+r_2)$
  - $(c_1+c_2 \bmod p) \bmod 2 = m_1+m_2 \bmod 2$

Noise: Distance to nearest multiple of p

- $c_1 \times c_2 = (m_1+2r_1)(m_2+2r_2) + (c_1q_2+q_1c_2-q_1q_2)p$
  - If $(m_1+2r_1)(m_2+2r_2)$ still much smaller than p
  - $c_1 x c_2 \bmod p = (m_1+2r_1)(m_2+2r_2)$
  - $(c_1 x c_2 \bmod p) \bmod 2 = m_1 x m_2 \bmod 2$

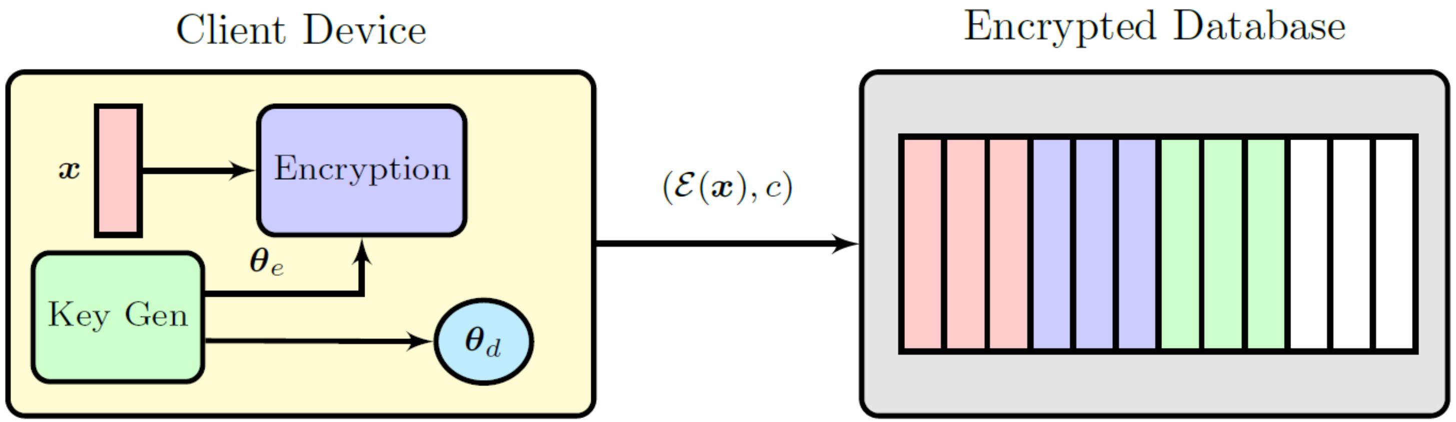
❖ Every operation increases the noise level of the ciphertext

❖ If the noise exceeds p/4, decryption may fail

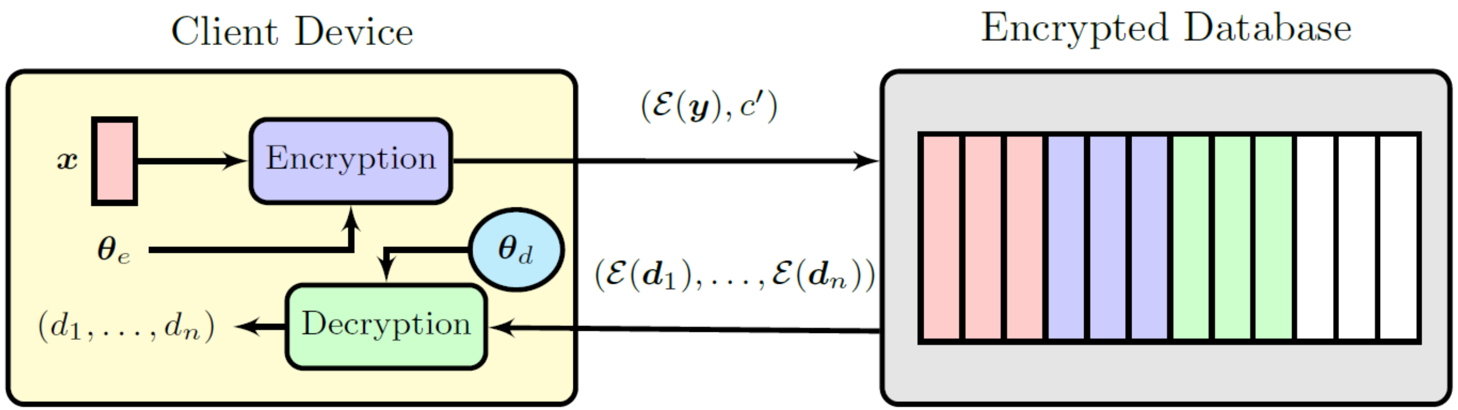
❖ This limits the "depth" of the operations

Verification Protocol based on HE

Enrollment



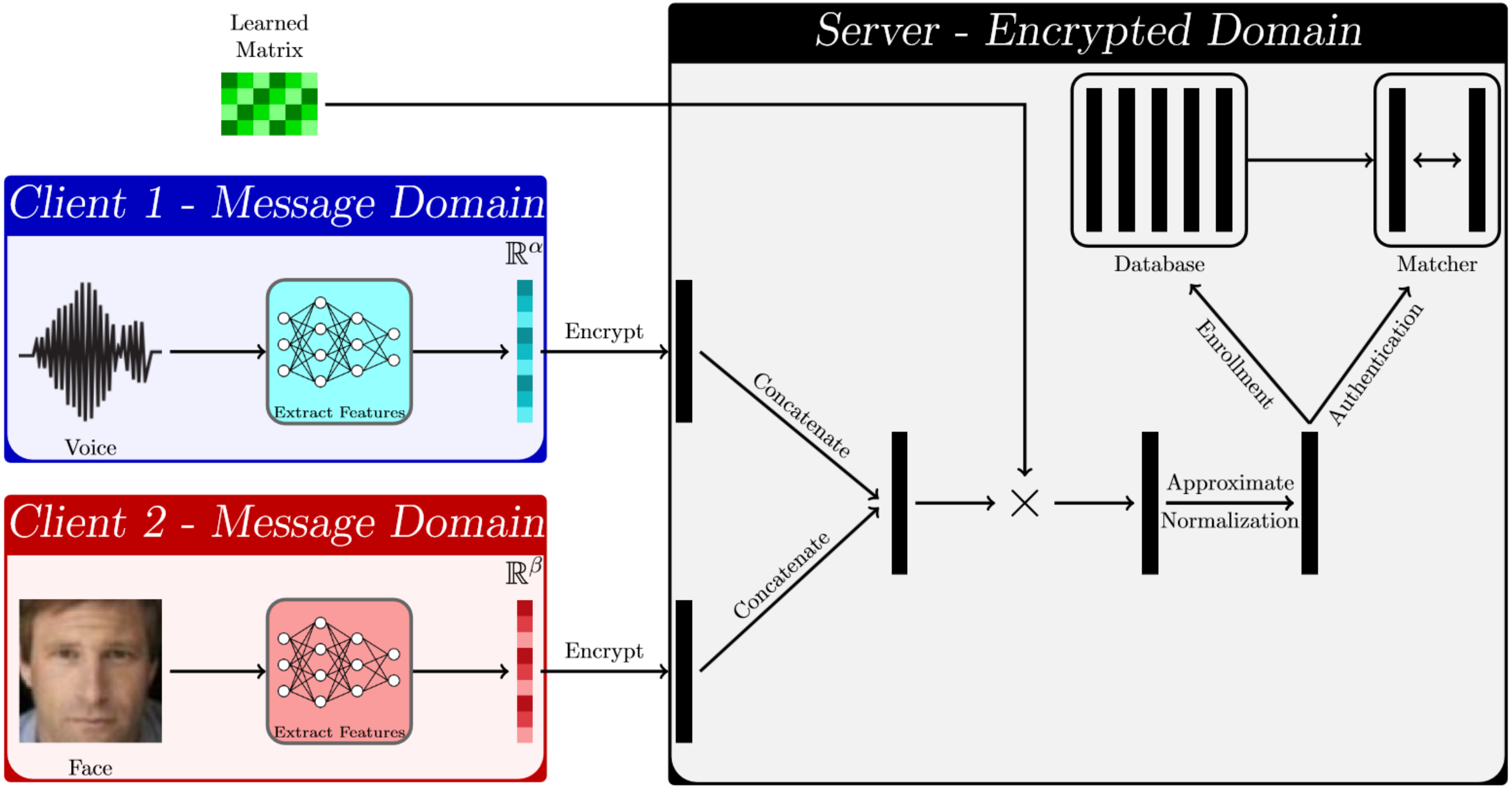
Verification



V. Bodetti, “Secure Face Matching Using Fully Homomorphic Encryption”, BTAS 2019

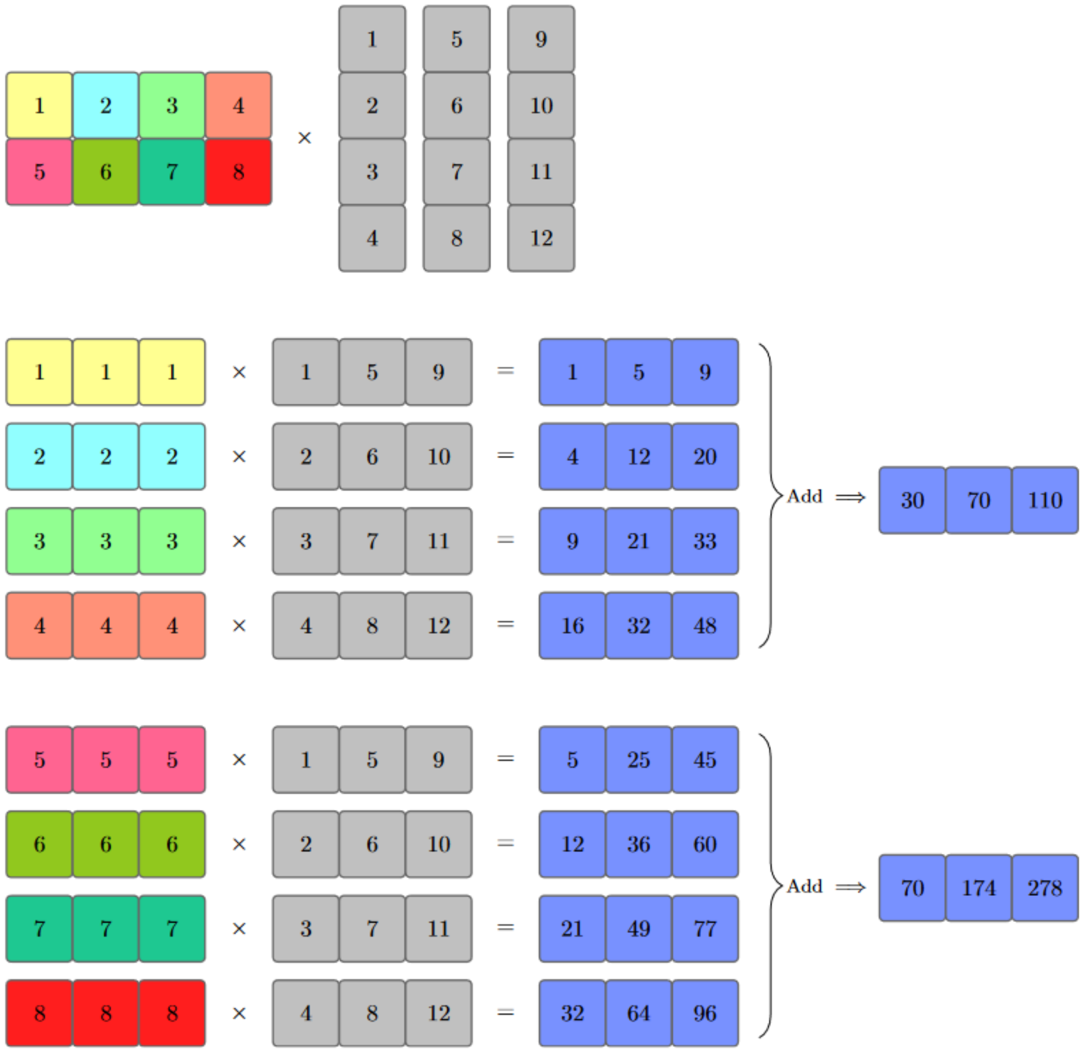
While match scores can be computed in the encrypted domain, the result still needs to be decrypted using the decryption key

Feature Fusion in Encrypted Domain



Sperling et al., “HEFT: Homomorphically Encrypted Fusion of Biometric Templates”, IJCB 2022

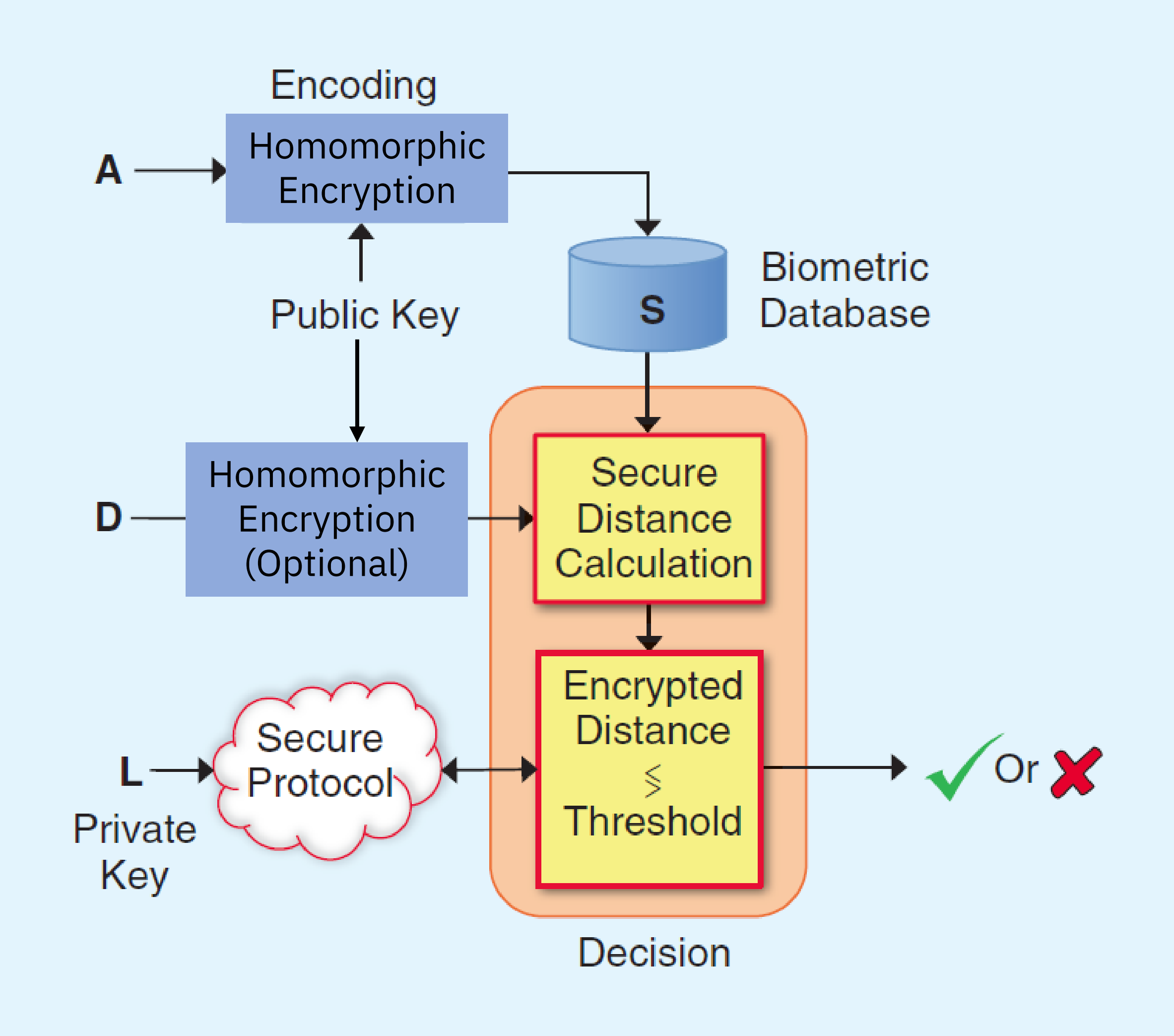
SIMD Operations in Encrypted Domain



A well-designed **ciphertext packing** strategy enables efficient computations in the encrypted domain by leveraging Single Instruction Multiple Data (SIMD) operations

Sperling et al., “HEFT: Homomorphically Encrypted Fusion of Biometric Templates”, IJCB 2022

Secure Multiparty Computation

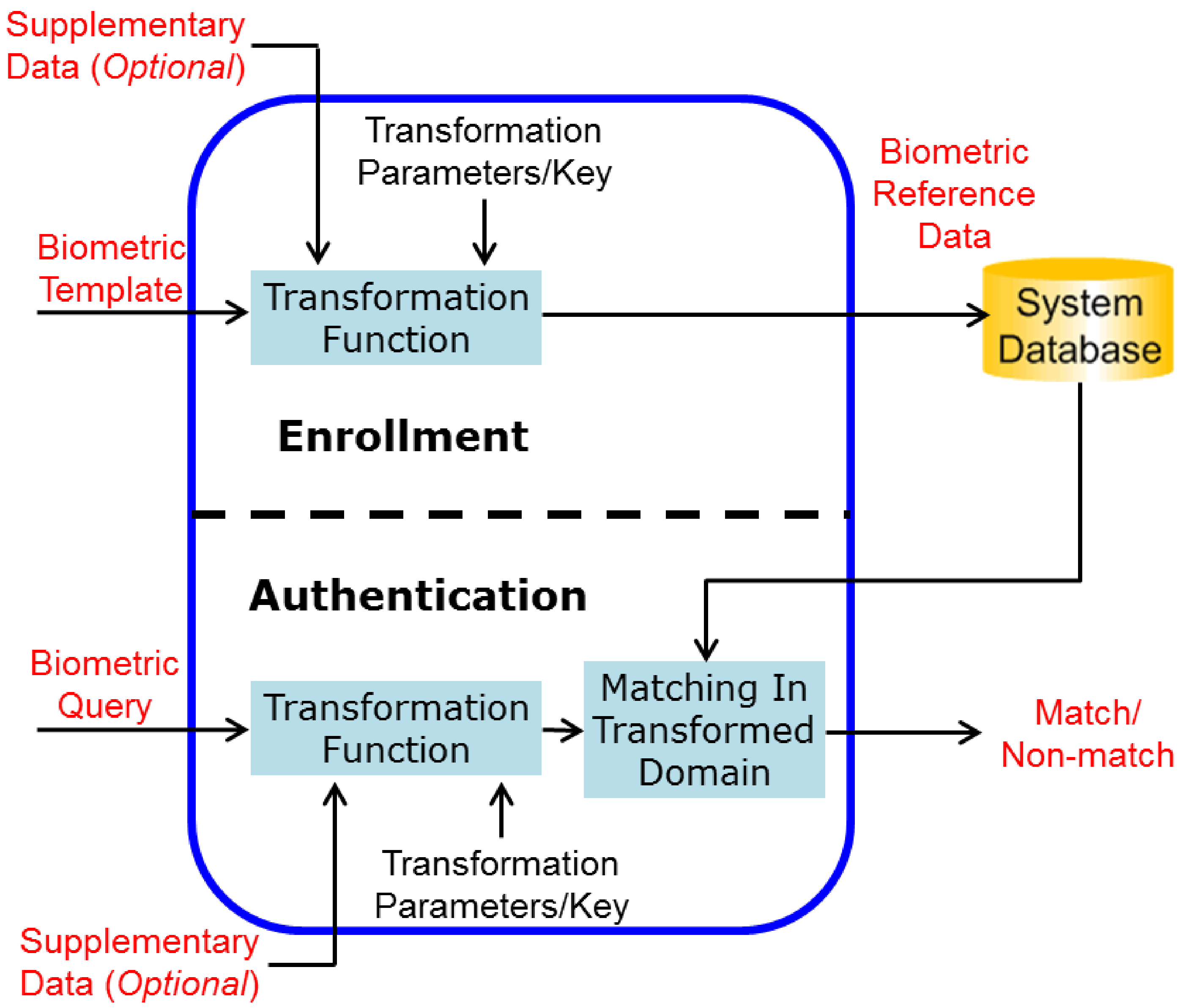


- Rane et al., "Secure Biometrics: Concepts, authentication architectures, and challenges", IEEE Signal Processing Magazine, Sept 2013
- Bringer et al., "Privacy-Preserving Biometric Identification Using Secure Multiparty Computation: An Overview and Recent Trends", IEEE Signal Processing Magazine, 30(2): 42-52, 2013

Challenges in HE Approach

- Exponential increase in
  - Template size
  - Computational complexity
  - Communication overhead
- How to handle real numbers?
- Efficient and secure protocols are required for matching in the encrypted domain – especially if the parties are malicious

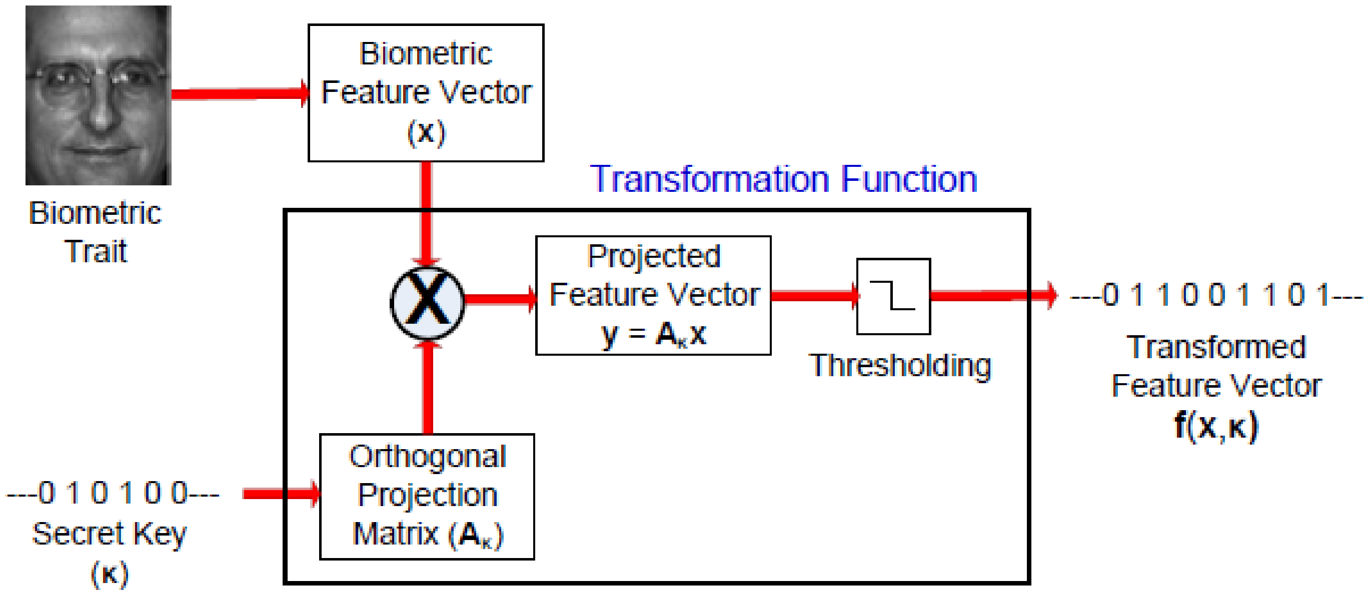
Feature Transformation Approach



- Template is revoked by changing transformation parameters/key

- Matching in transformed domain; if transformation is non-invertible, security of key is not critical

Invertible Transformation: BioHashing



Teoh et al., "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs," *IEEE TPAMI*, 28(12), pp.1892,1901, Dec 2006

An effective technique for features represented as fixed-length vectors; significant “improvement” in matching performance due to increased uniformity of feature distribution

How difficult is its inversion?

(Ir)reversibility of BioHashing

- Original features are obtained as solution of the following problem for

$$\arg\min \|x - a\|_2 ,$$

$$\sum_{j=1}^{n} M_{ij} x_j < \delta_i , if \quad b_i = 0$$

$$\sum_{j=1}^{n} M_{ij} x_j \geq \delta_i , if \quad b_i = 1$$

where a is the biometric feature from a database, M is the transformation matrix, b is the transformed feature and δ_i is the threshold for the *i*-th feature

- Weighted combination of multiple solutions is used as the final estimate of *x*

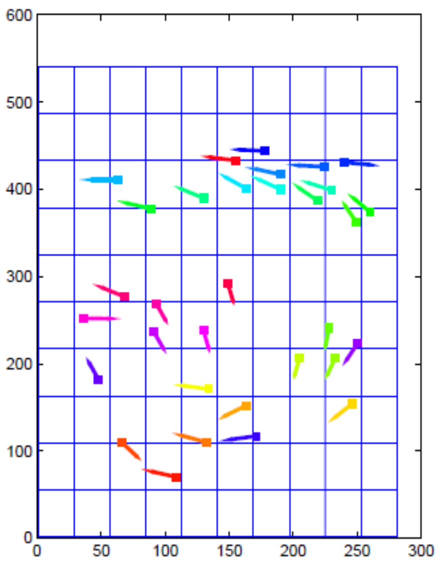
Original Face

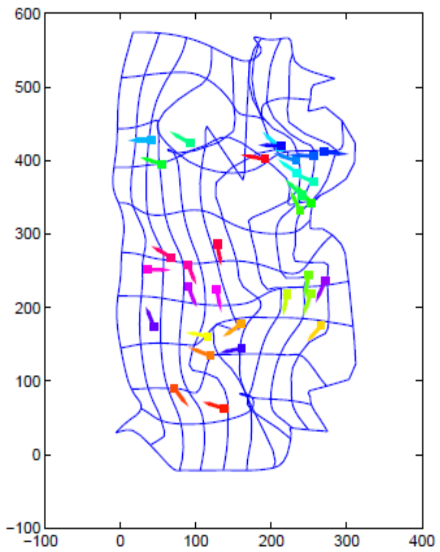
Recovered Face

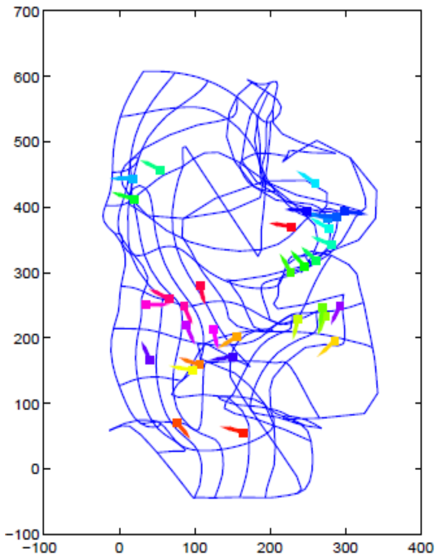
A. Nagar, K. Nandakumar & A. K. Jain, "Biometric Template Transformation: A Security Analysis", *Proc. SPIE Electronic Imaging, Media Forensics and Security XII*, Jan 2010

Non-Invertible Transformation

Many-to-one transforms that are locally smooth and globally non-smooth


Original minutiae

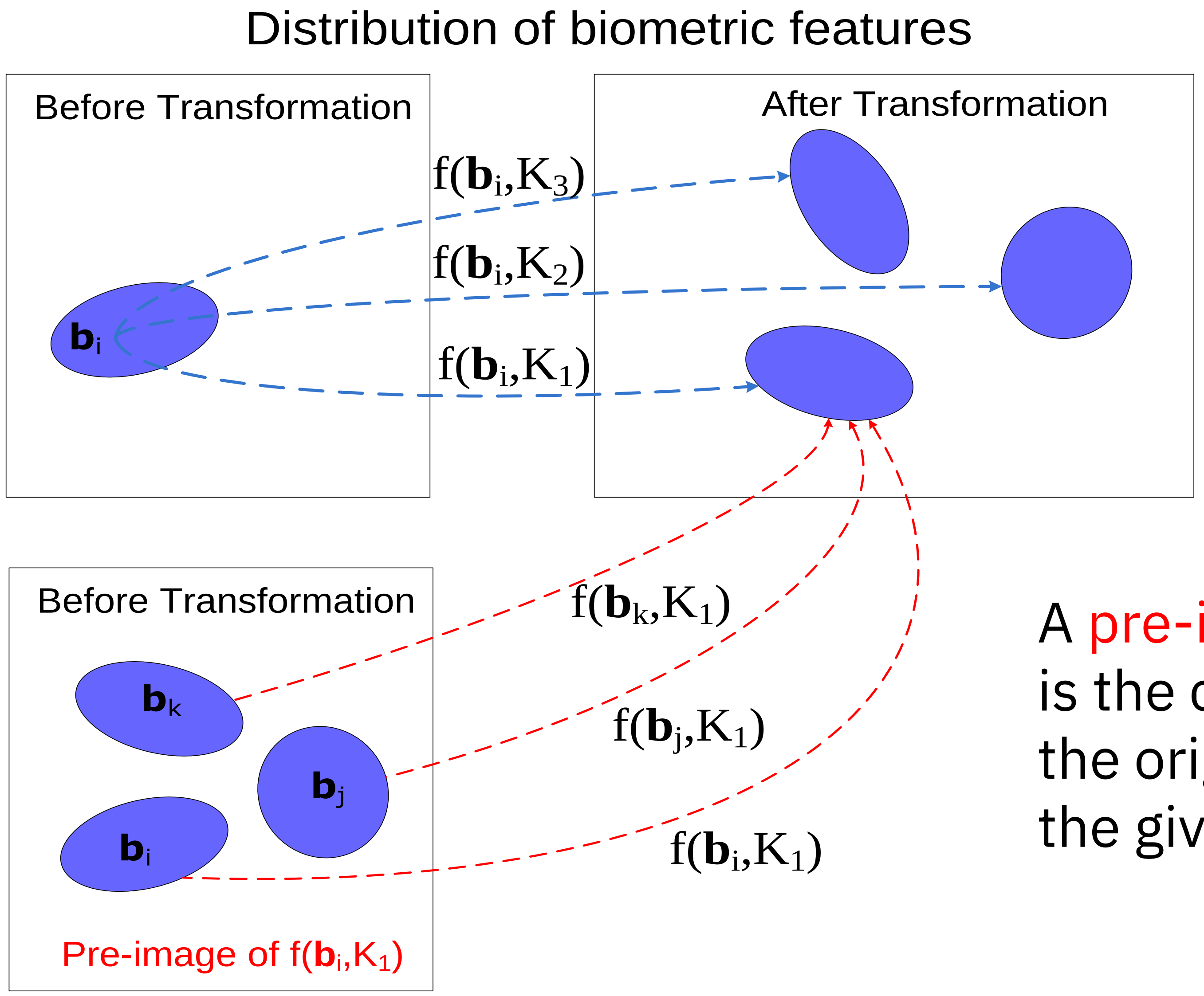

Transformed minutiae using Trans-1 (γ=30)


Transformed minutiae using Trans-2 (γ=60)

Ratha et al., "Generating Cancelable Fingerprint Templates," *IEEE TPAMI*, 29(4), pp.561,572, April 2007

- Requires core-point based alignment
- Trade-off between irreversibility & accuracy
- Lack of theoretical analysis of irreversibility

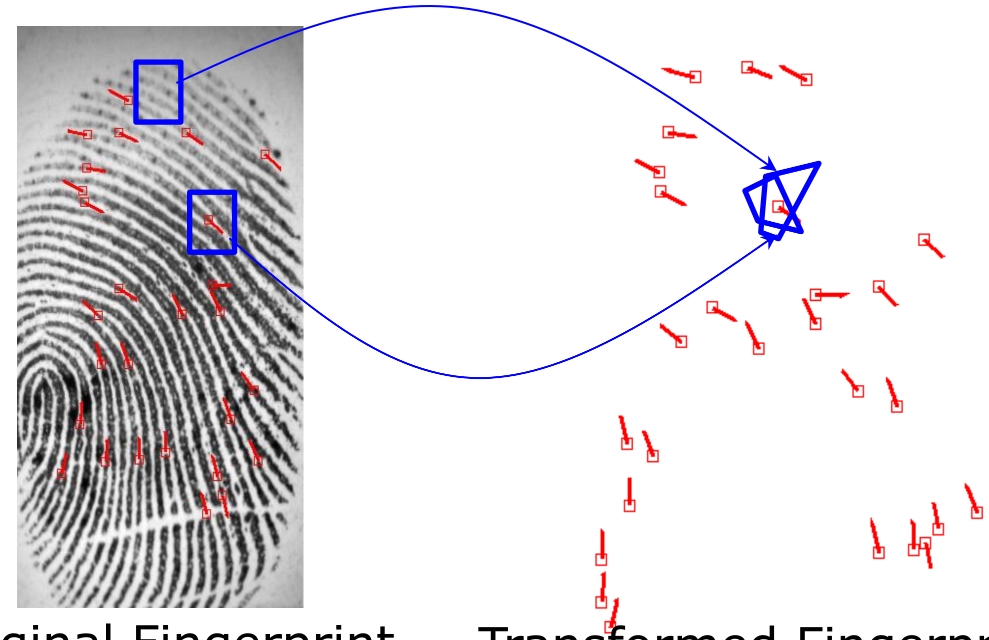
(Ir)reversibility of Feature Transformation



A pre-image of a transformed template is the collection of all the templates in the original domain that can generate the given transformed template

Example of Reversing a Non-Invertible Template

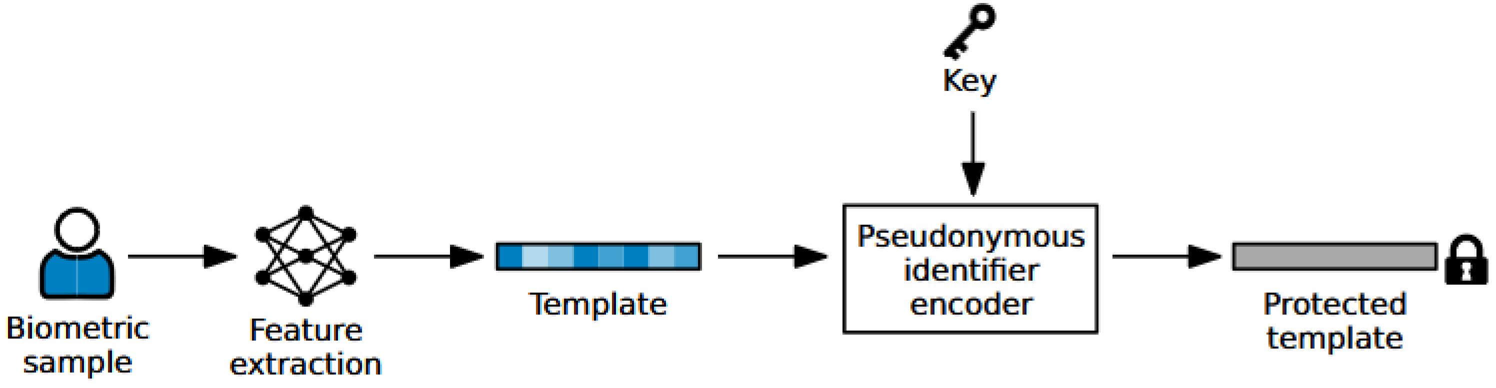
- Transformed squares encasing a minutia correspond to its pre-image
- Most likely pre-image element is taken as inverse
  - More pre-images considered in order of likelihood to improve feature recovery



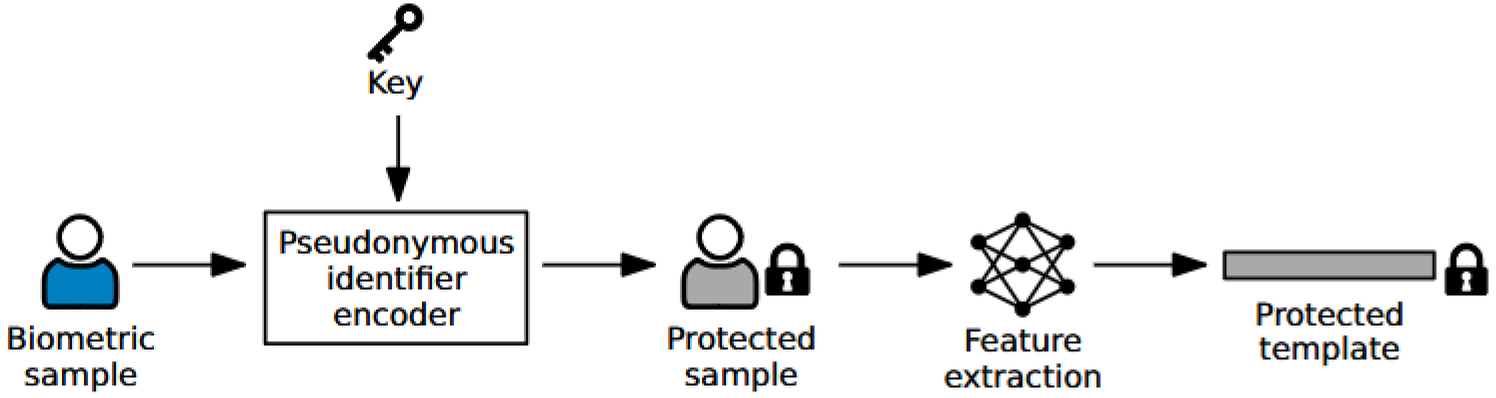
Original Fingerprint Transformed Fingerprint

A. Nagar and A. K. Jain, "On the Security of Non-Invertible Fingerprint Template Transforms", *IEEE WIFS*, Dec. 2009

Template Protection via Input Transformation



Feature Transformation



Input Transformation

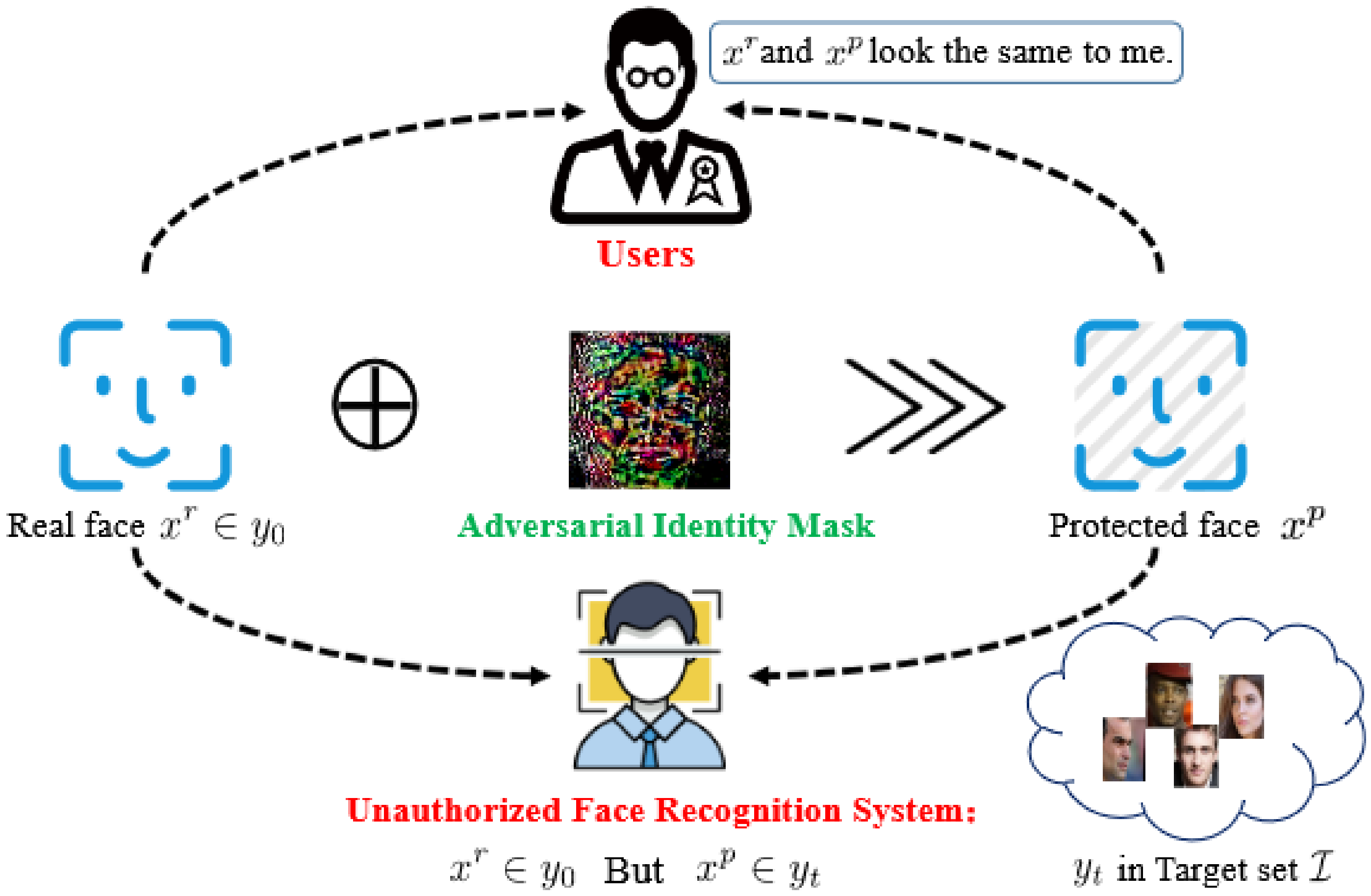
Rathgeb et al., “Deep Learning in the Field of Biometric Template Protection: An Overview”, https://arxiv.org/pdf/2303.02715

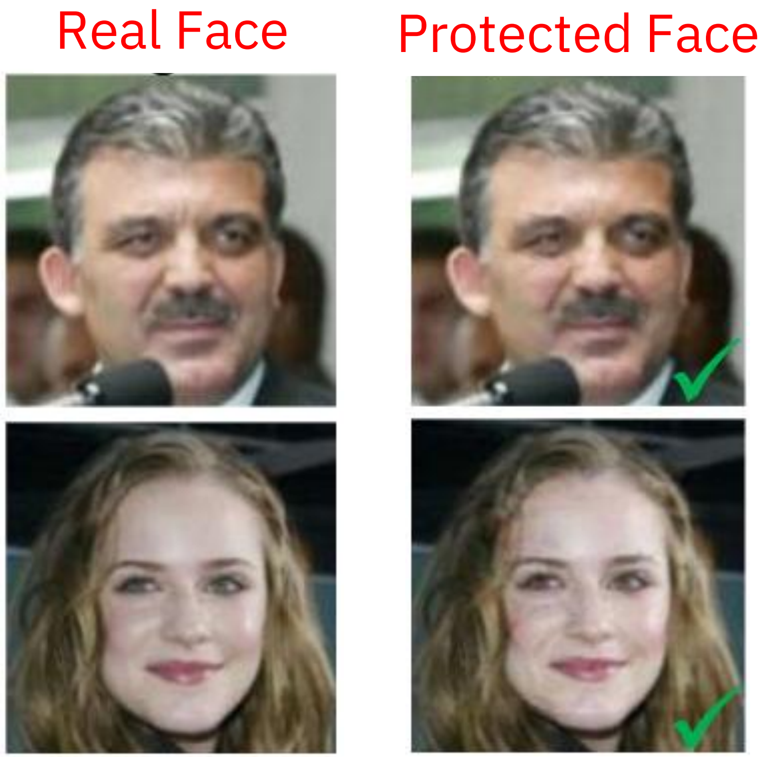
Protecting Facial Privacy via Adversarial Attacks

- Face recognition algorithms can be misused for unauthorized tracking of individuals based on images posted on social media, which constitutes a serious threat to privacy in the digital world
- Can face images be adversarially modified to protect facial privacy?

Noise-based Patch-based Adv-glasses Adv-hat Patch-based

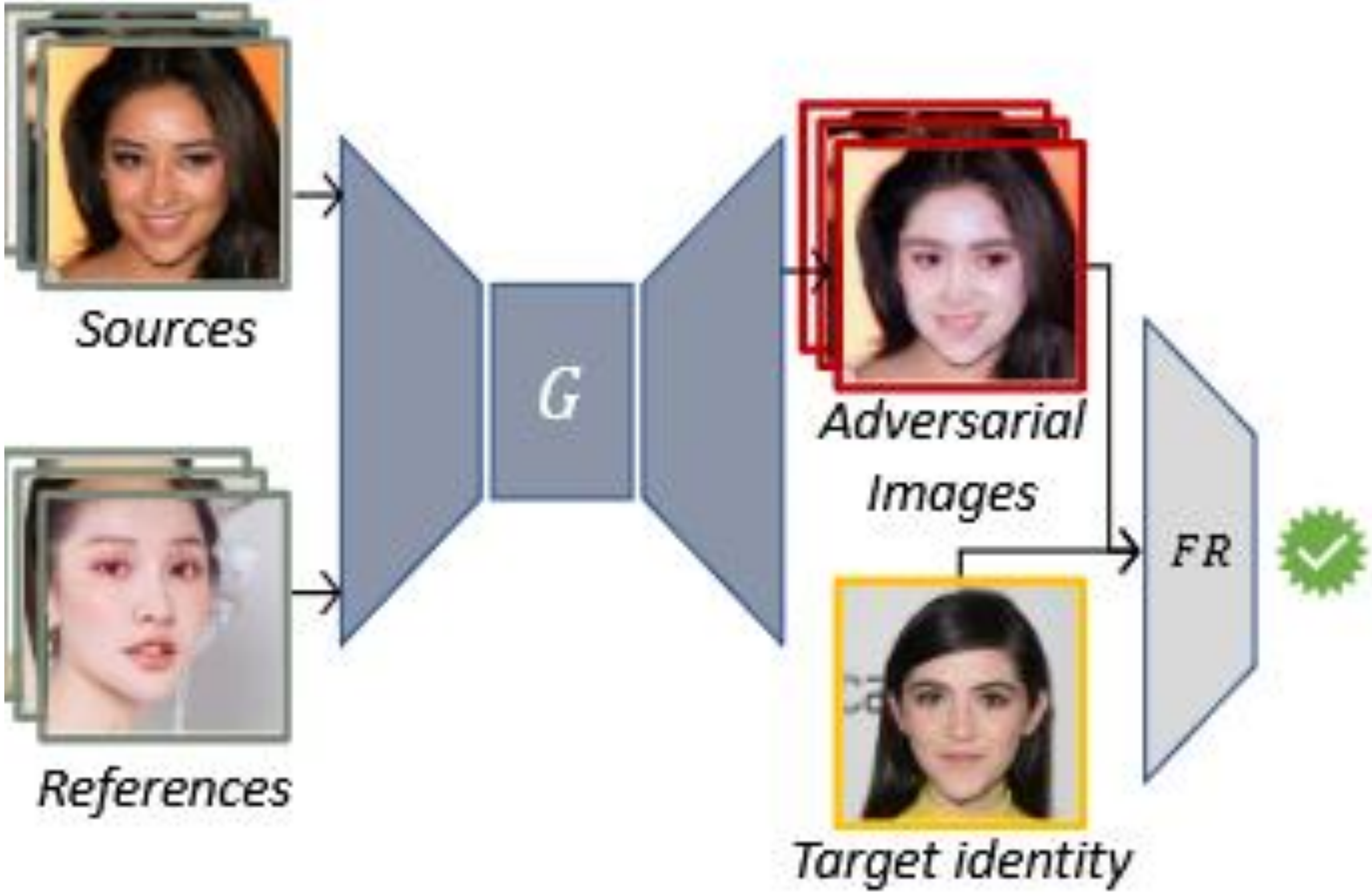
Input Transformation for Face Privacy Protection





Yang et al., "Towards Face Encryption by Generating Adversarial Identity Masks", ICCV 2021

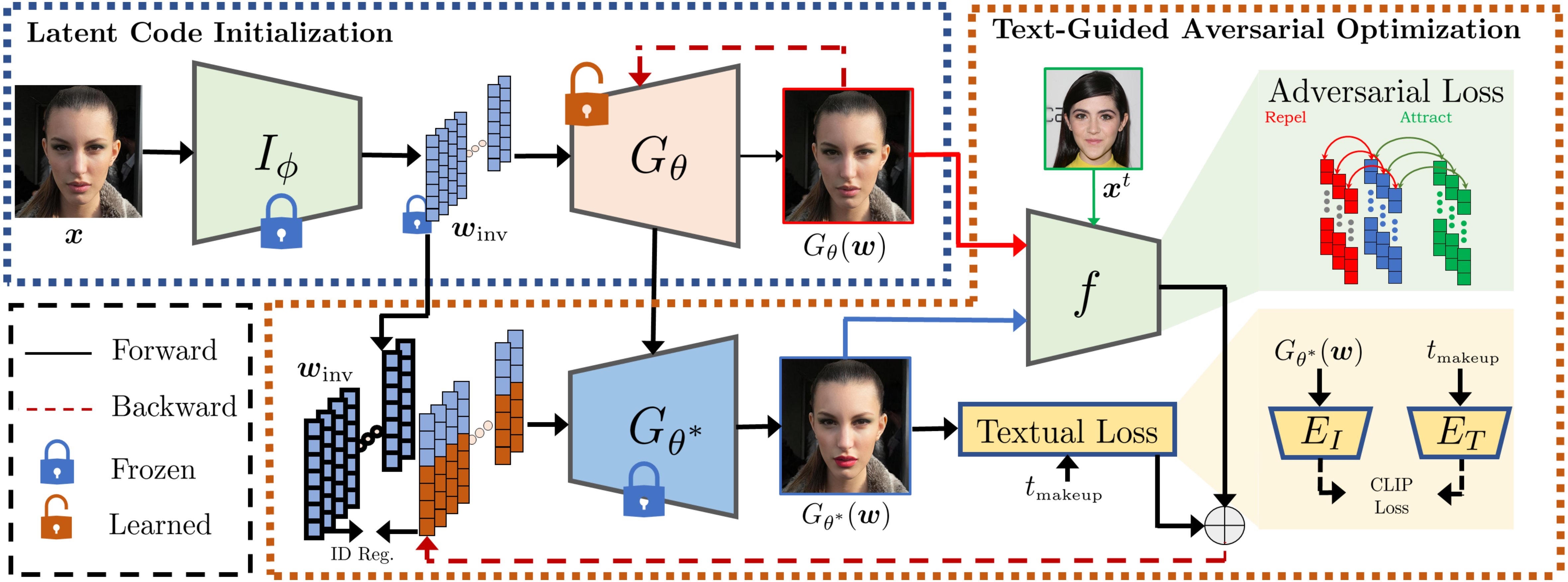
Makeup Transfer for Face Privacy Protection



Hu et al., “Protecting Facial Privacy: Generating Adversarial Identity Masks via Style-robust Makeup Transfer”, CVPR 2022

Protecting Facial Privacy via Adversarial Attacks

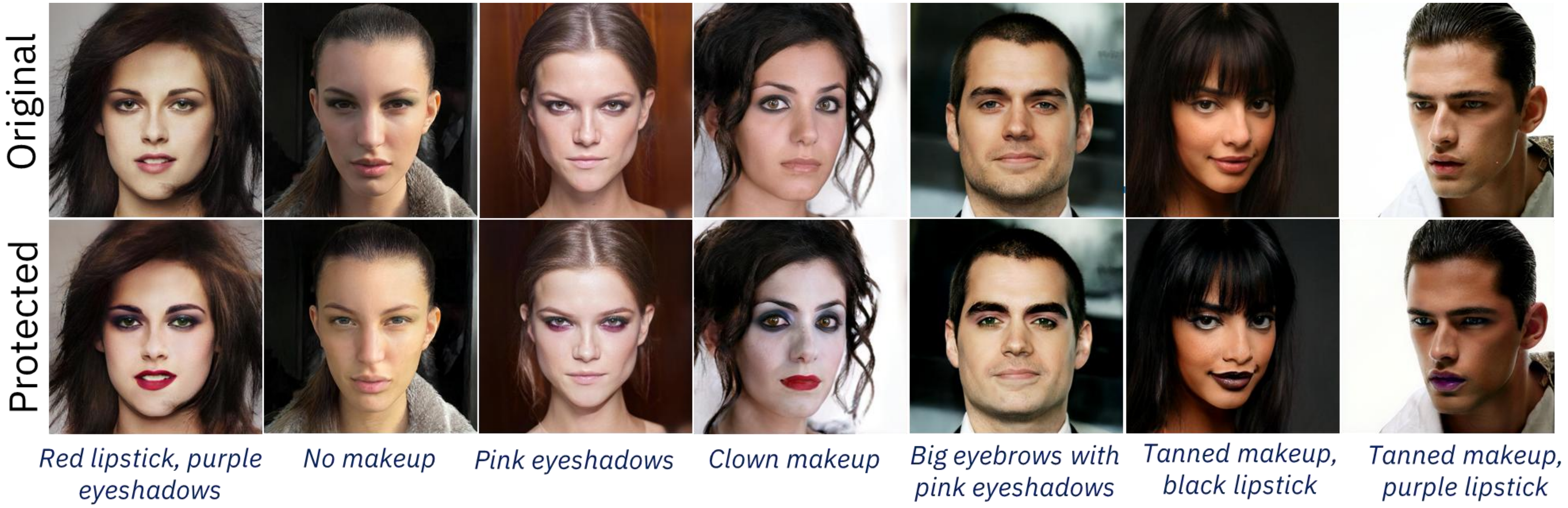
A two-step approach to find adversarial latent codes within the low-dimensional manifold of a pretrained generative model



Shamshad, Naseer, and Nandakumar, "CLIP2Protect: Protecting Facial Privacy using Text-Guided Makeup via Adversarial Latent Search", *CVPR 2023*

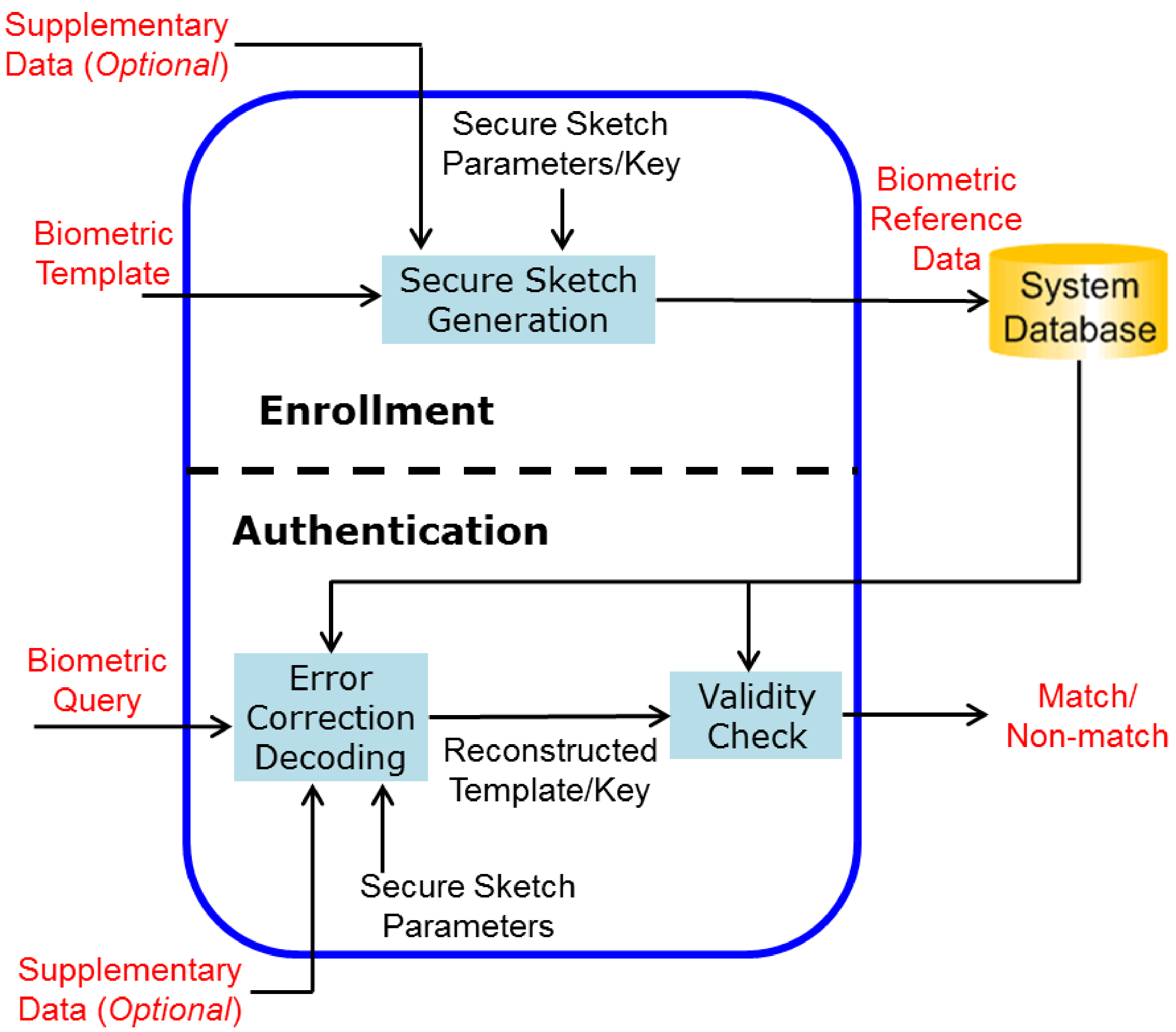
Protecting Facial Privacy via Adversarial Attacks

User-defined makeup prompts can effectively hide attack information in the desired makeup style



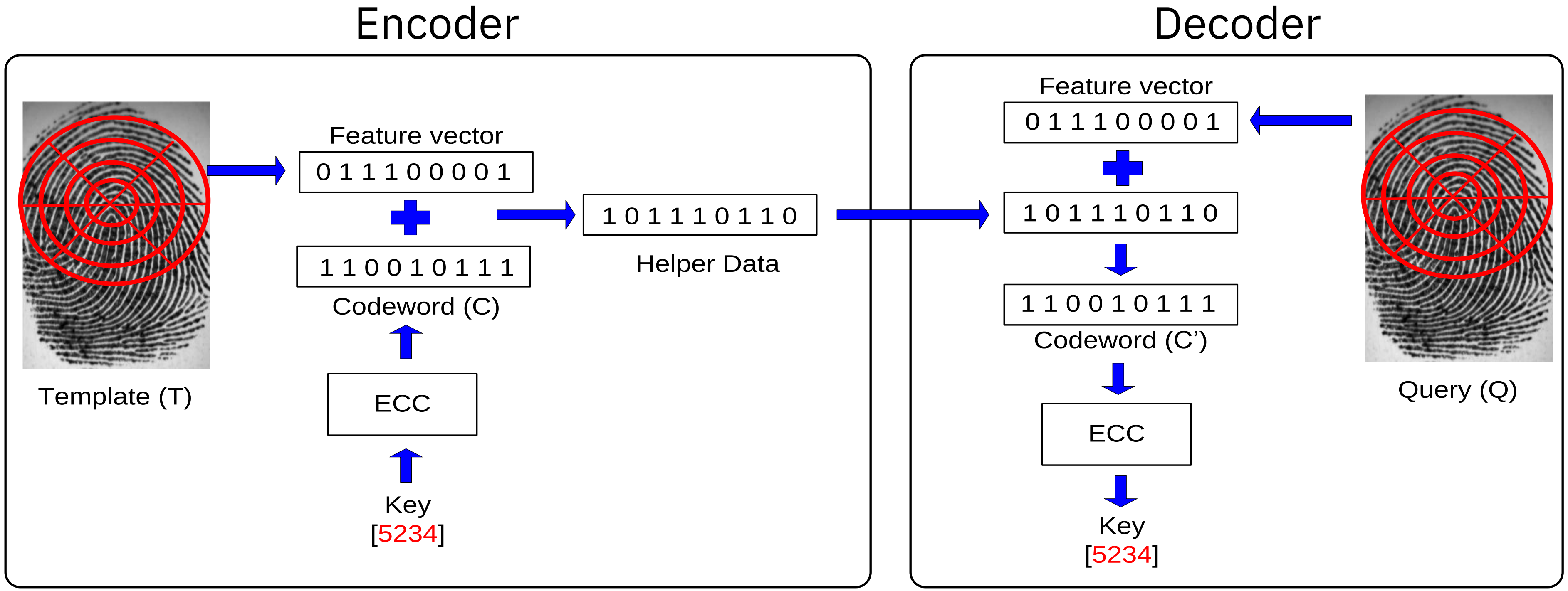
Shamshad, Naseer, and Nandakumar, "CLIP2Protect: Protecting Facial Privacy using Text-Guided Makeup via Adversarial Latent Search", *CVPR 2023*

Biometric Cryptosystems



Biometric cryptosystems enhance security and user privacy by binding biometric template & cryptographic key as one entity

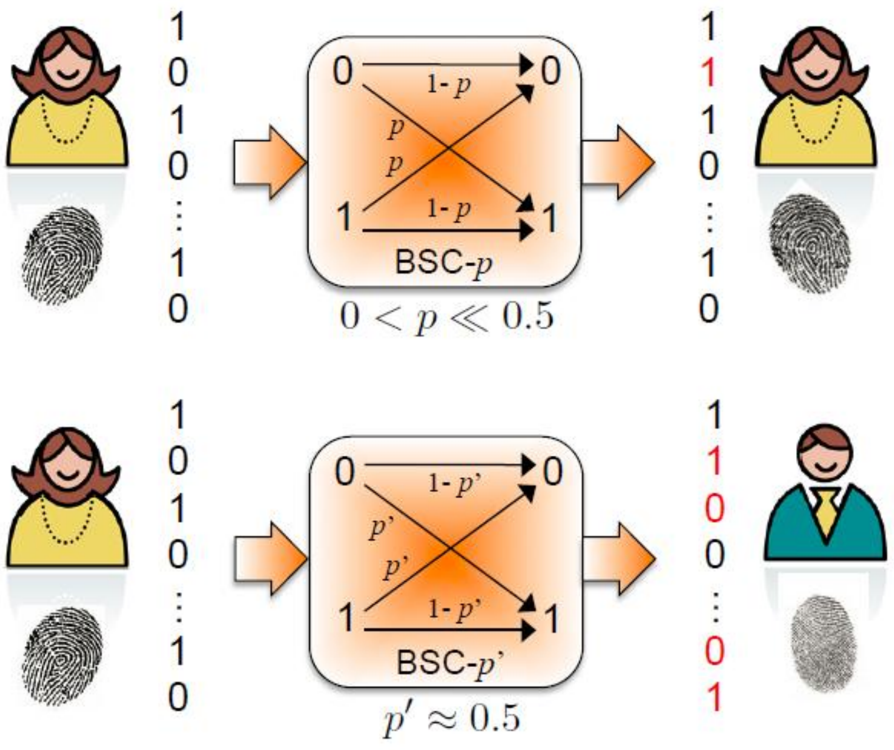
Fuzzy Commitment



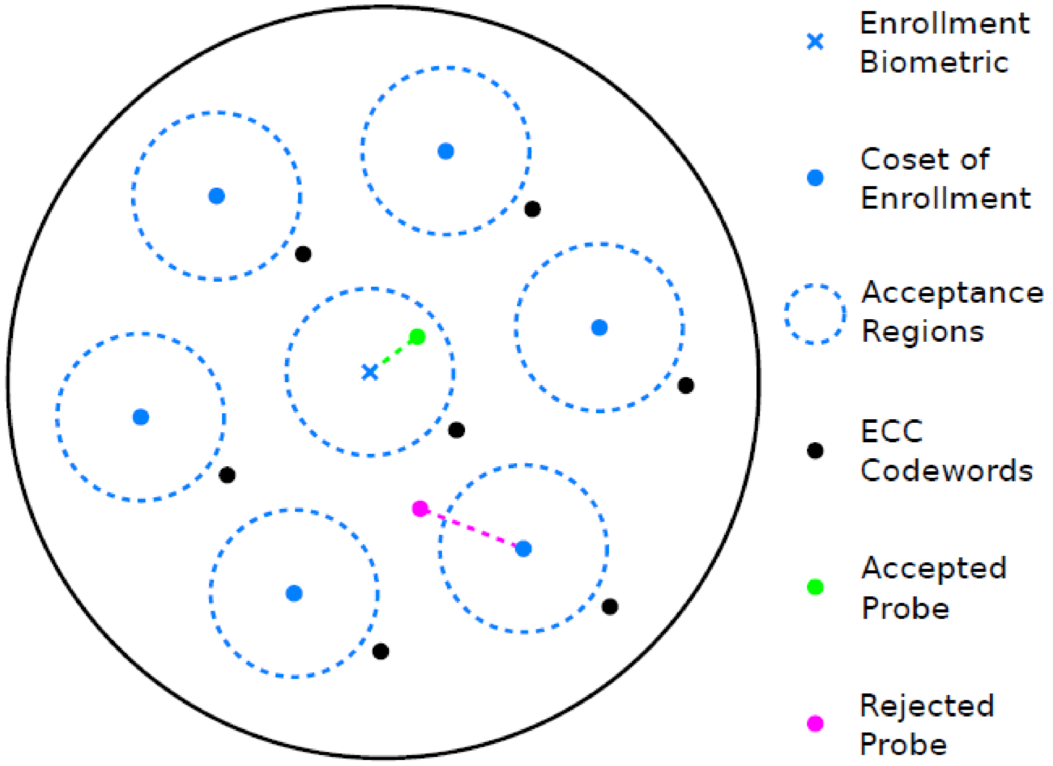
Juels and Wattenberg, "A fuzzy commitment scheme," in Proc. 6th ACM Conf. Computer & Communications Security, 1999

- Variability in binary biometric features is translated to variability in codeword of an error correction scheme, which is indexed by a key
- Corrupted codeword can be corrected to recover the embedded key
- Lack of *perfect* code for desired code length

Basic Concept of Fuzzy Commitment



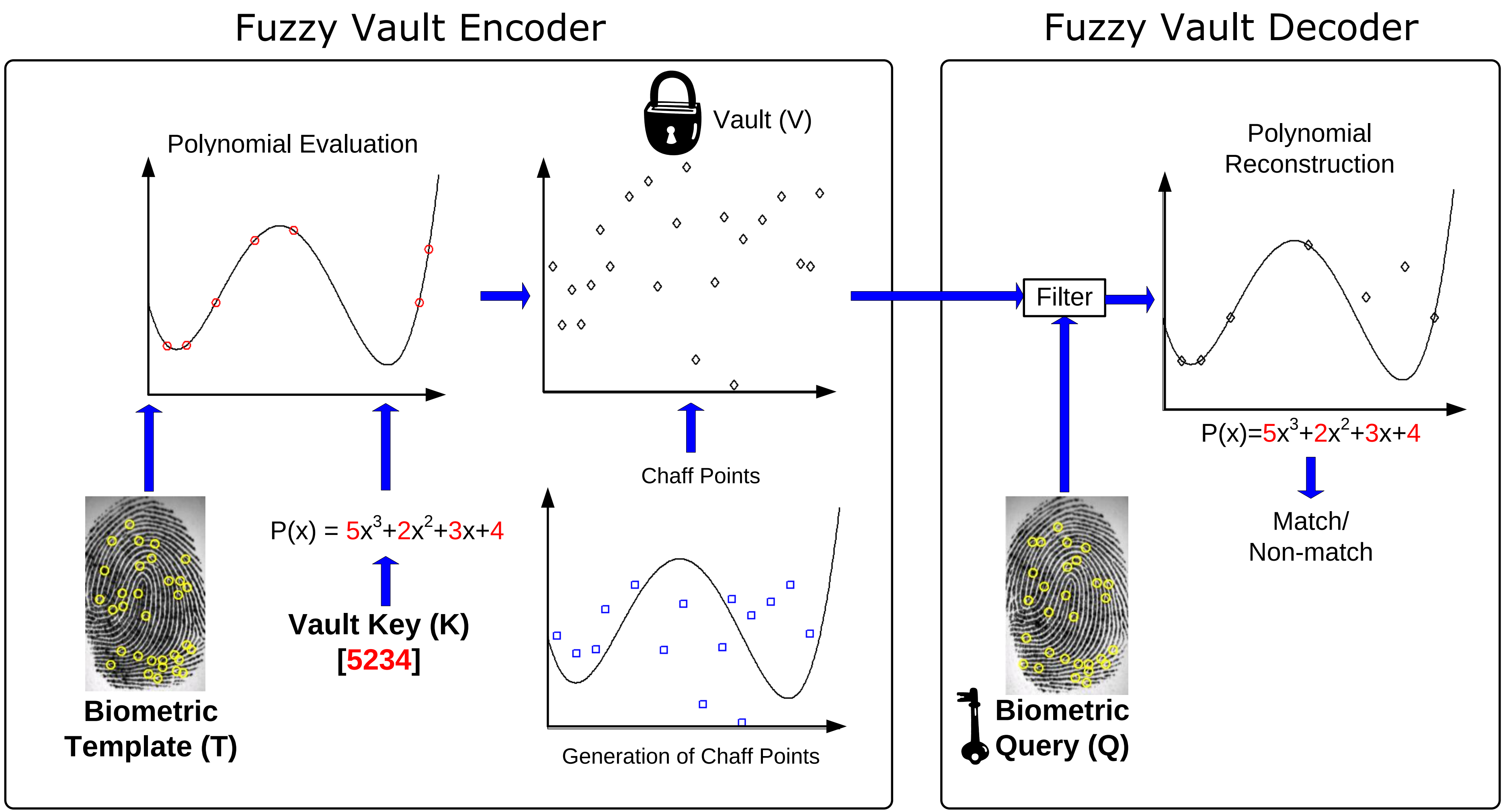
Variability in binary biometric feature vectors can be related to errors introduced by a binary symmetric channel



Pictorial representation of ECC-based biometric cryptosystem

Rane et al., "Secure Biometrics: Concepts, authentication architectures, and challenges", IEEE Signal Processing Magazine, Sept 2013

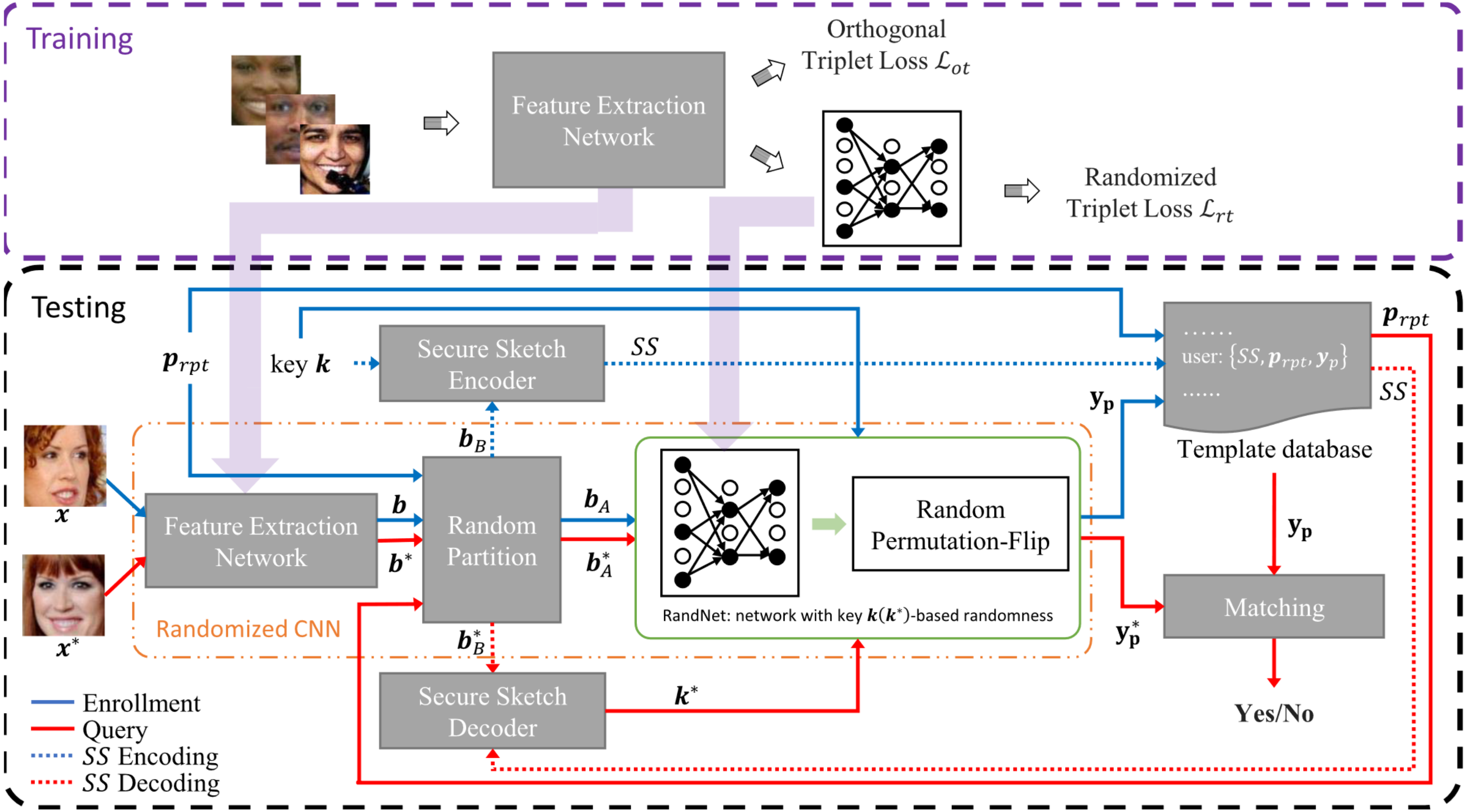
Fuzzy Vault



- Decoder identifies genuine points in mixture of genuine & chaff points
- How to generate chaff points that are indistinguishable from genuine points?

Nandakumar, Jain and Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance", *IEEE T-IFS*, 2007

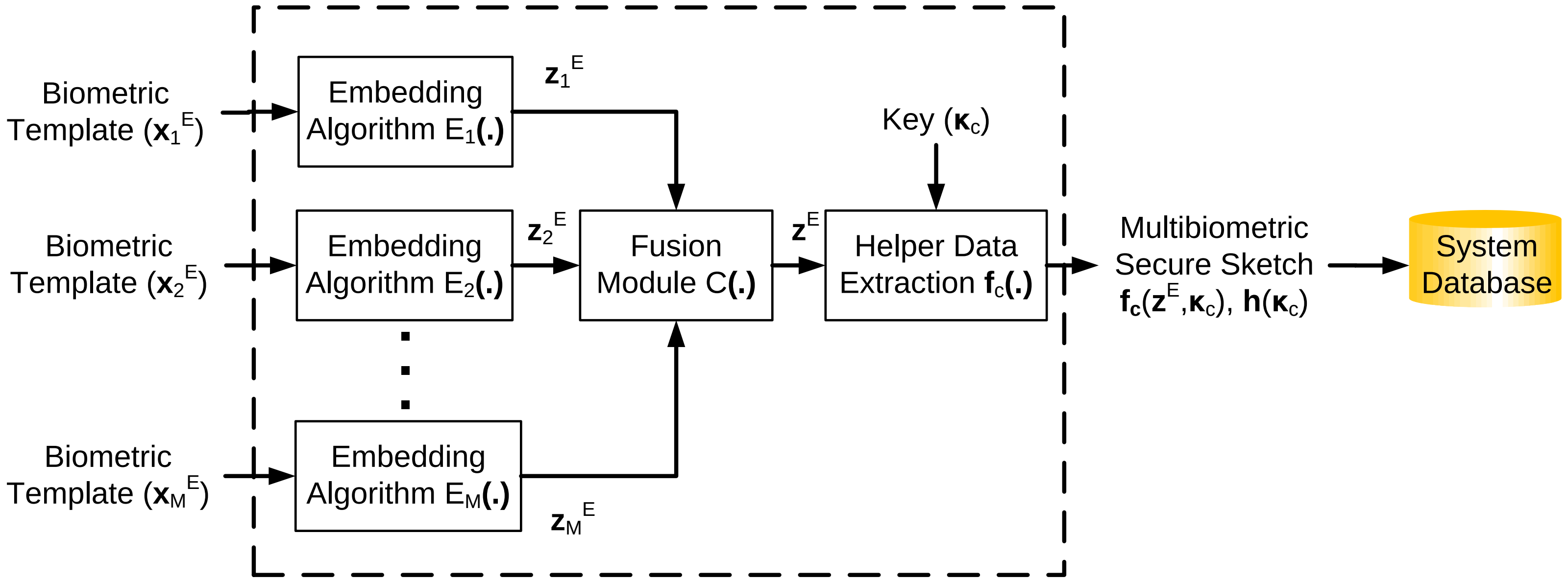
Hybrid Secure Face Template



Mai et al., “SecureFace: Face Template Protection”, *IEEE T-IFS*, 16, pp. 262-277, 2021

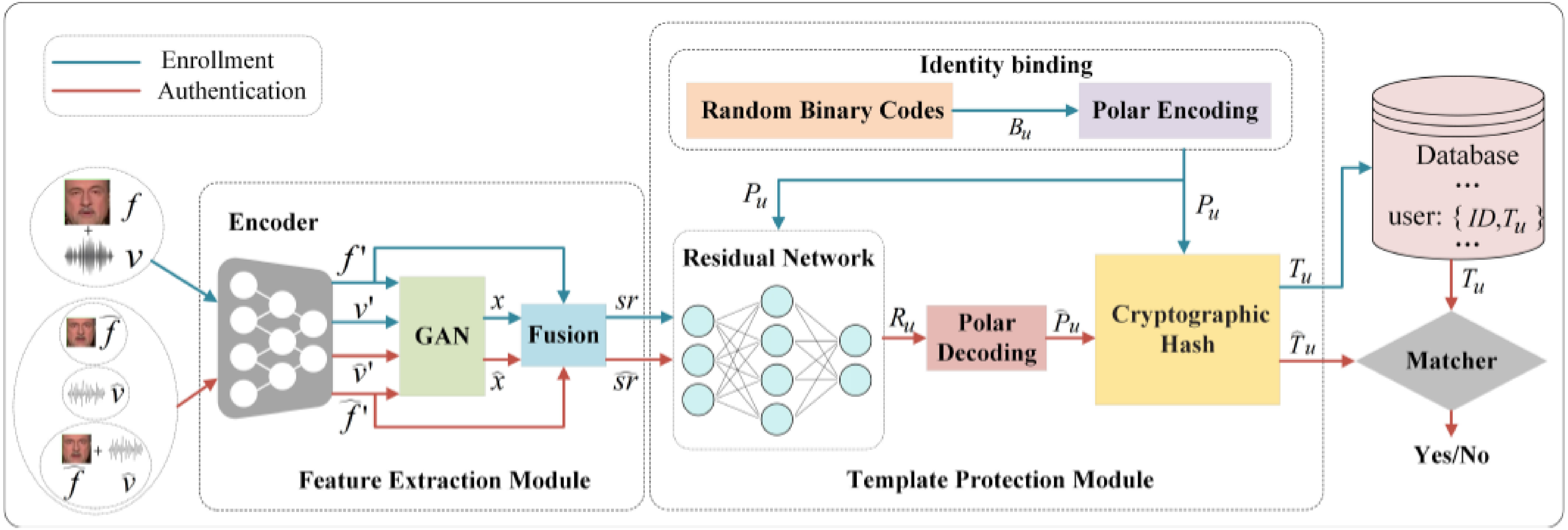
Multibiometric Cryptosystems

- Multibiometrics provides high matching accuracy and high universality
- Match score level fusion is most effective; but cryptosystems do not output scores
- Feature fusion leads to significant improvement versus cascade cryptosystems
- Major challenges
  - Heterogeneous biometric data
  - Feature adaptation for biometric cryptosystems



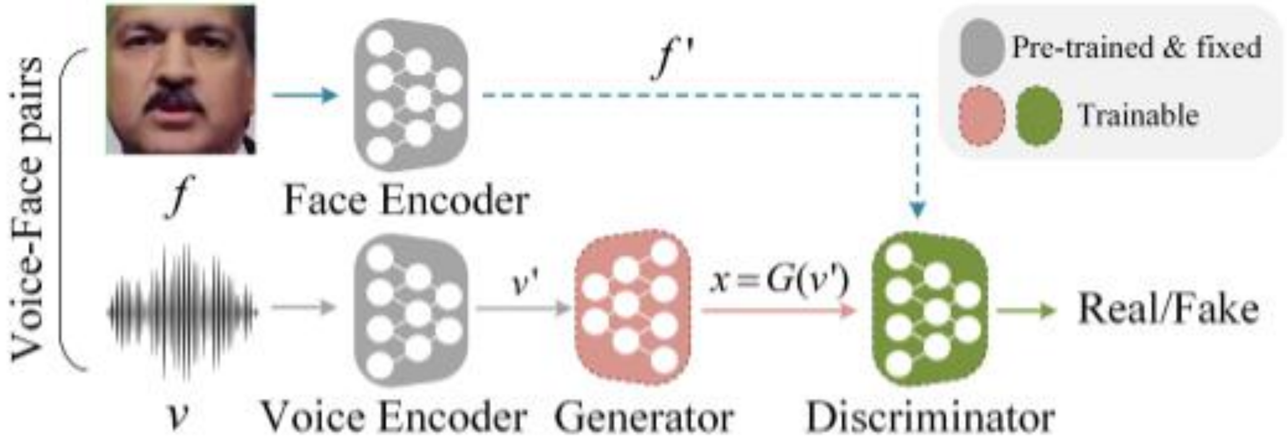
A. Nagar, K. Nandakumar and A. K. Jain, “Multibiometric Cryptosystems based on Feature Level Fusion”, *IEEE T-IFS,* 2012

Multibiometric Fusion in the Input Domain



Jiang et al., "Cross-Modal Learning Based Flexible Bimodal Biometric Authentication With Template Protection", *IEEE T-IFS,* 2024

Multibiometric Fusion in the Input Domain



Original Face Images

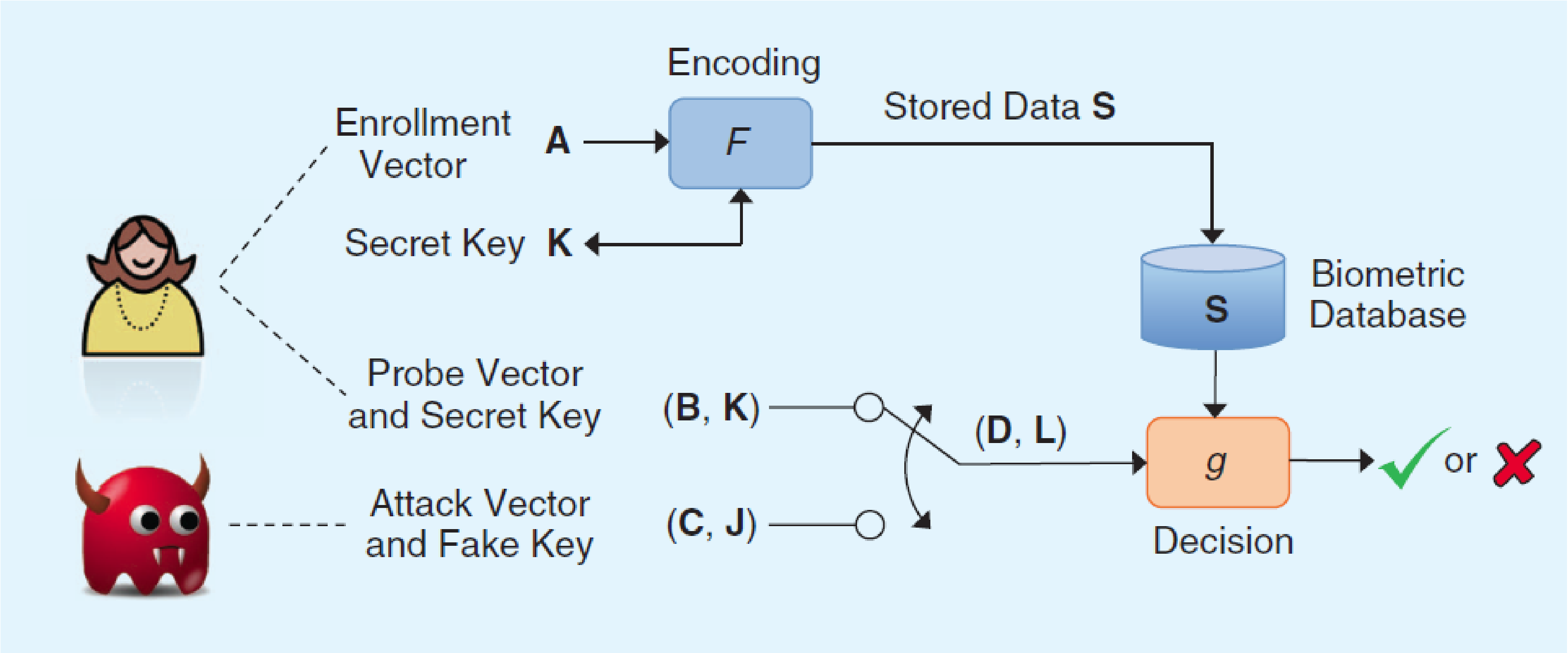
Synthetic Face Images generated from Voice

Key Points for Alignment

Fusion of Original & Synthetic Face Images

Jiang et al., "Cross-Modal Learning Based Flexible Bimodal Biometric Authentication With Template Protection", *IEEE T-IFS,* 2024

Metrics for Template Security Evaluation



Rane et al., “Secure Biometrics: Concepts, authentication architectures, and challenges”, IEEE Signal Processing Magazine, Sept 2013

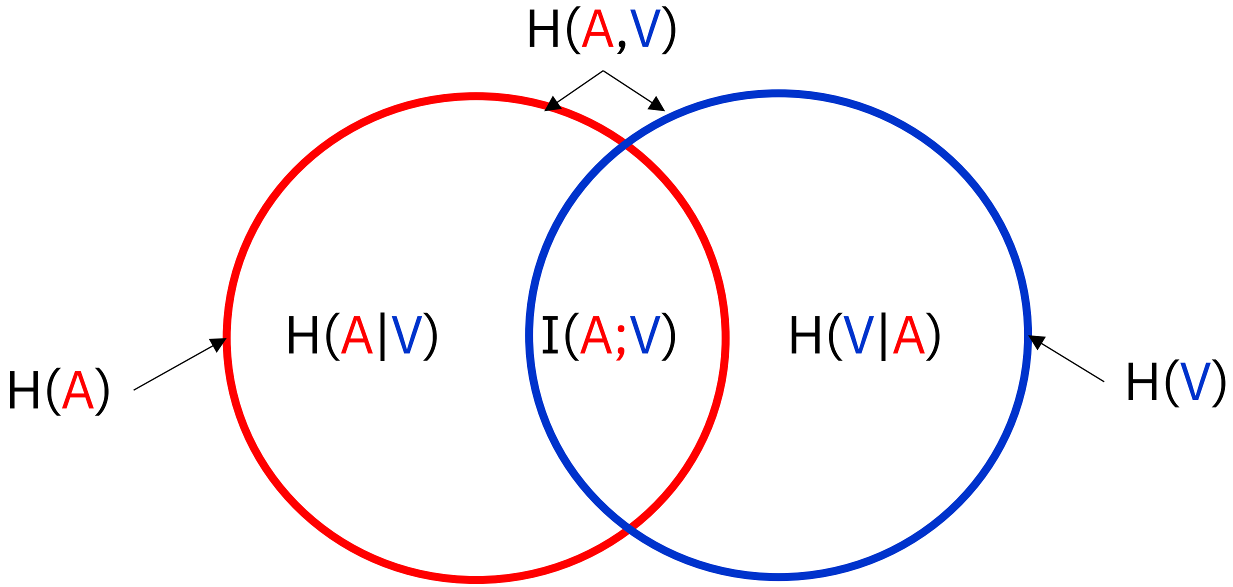
False Non-match Rate (FNMR) = P(g = Non-match | D = B, L = K)

False Match Rate (FMR) = P(g = Match | D = C, L = J)

Successful Attack Rate (SAR) = P(g = Match | D = C, L = K, side info)

Privacy Leakage = Mutual Information (A; V = (S, K))

Information-Theoretic Framework for Irreversibility



A: Enrollment Biometric Vector (Template)
V: Stored Data (includes AD, PI, SD)

- Privacy Leakage (Entropy Loss) = I(A; V)
- Suitable only for comparing two BTP schemes acting on same A

Measuring Irreversibility

- How difficult it is to recover the original template from the stored data?
- Typically expressed in bits & measured based on
  - Avg. no. of trials needed to recover the template
  - Entropy of original template given the stored data ($H(A|V)$)
- Estimate of security requires a model of the biometric feature distributions
- FRR, FAR, and SAR are reported separately

Irreversibility of Biometric Cryptosystems

- Fuzzy vault[1]

$$H(A|V) = \log_2\left(\frac{C(r,n+1)}{C(t,n+1)}\right)$$

r: total no. of points in the vault
t: no. of genuine points
n: degree of polynomial used

Assumption: Both genuine and chaff points are uniformly distributed

- Fuzzy commitment[2]

$$H(A|V) = \log_2\left(\frac{2^I}{C(I,\rho I)}\right)$$

I: Entropy of binary template
ρ: Fraction of errors corrected

Assumption: Reliable estimate of entropy (no. of i.i.d bits) is available

How to modify features to satisfy these assumptions?

[1] Nandakumar, Jain and Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance", *IEEE T-IFS*, 2007

[2] Hao, Anderson, and Daugman, "Combining Crypto with Biometrics Effectively," *IEEE Trans. Computers*, 2006

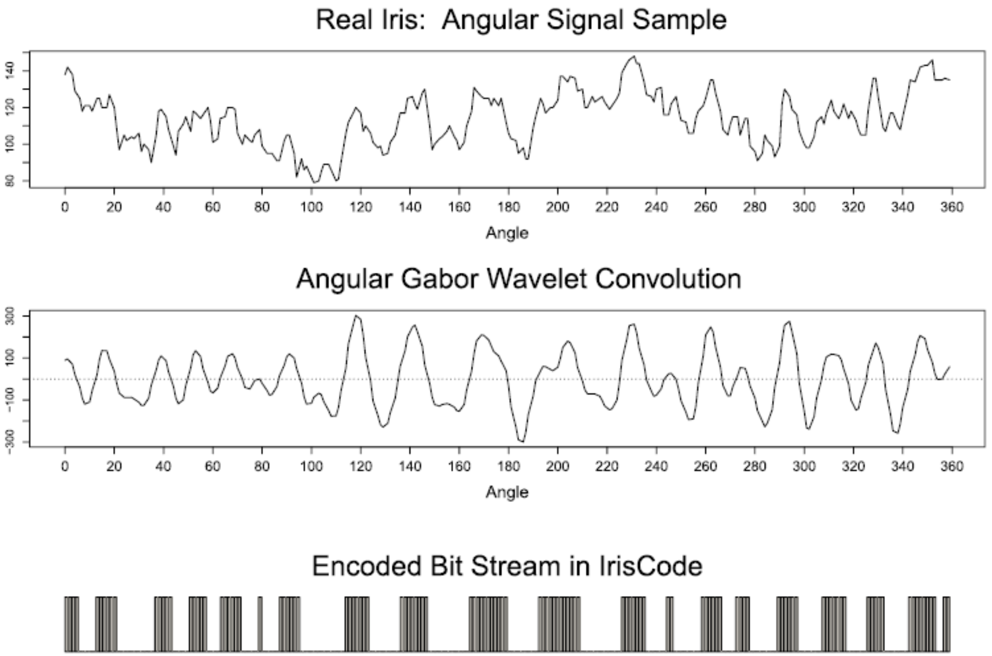
Gap Between Theory & Practice of Biometric Encryption

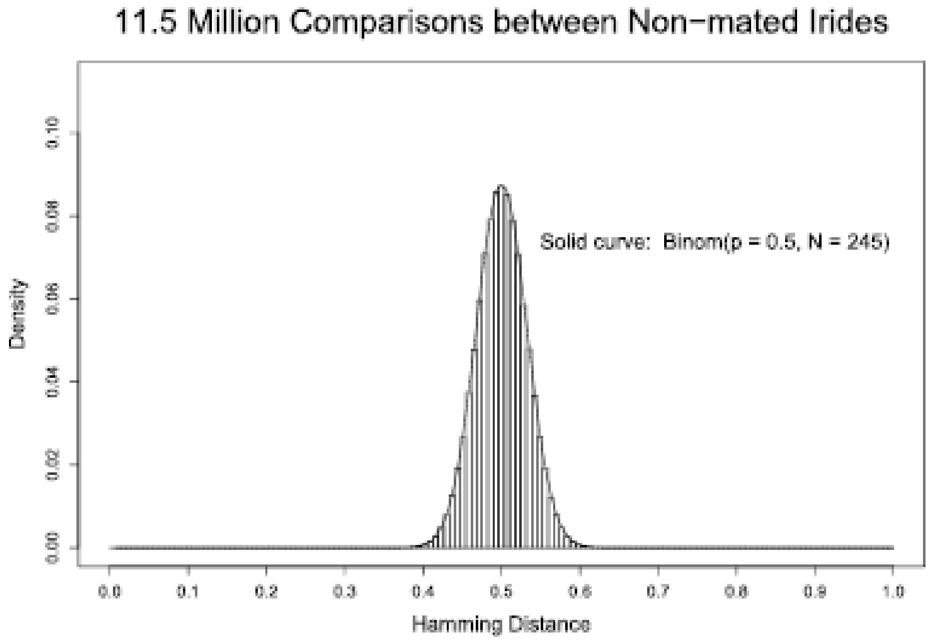
- 7 algorithms in FVC-onGoing have equal error rate (EER) less than 0.2% without BTP; best BTP algorithm has EER of 1.54% on same data
- AES system with a 128-bit key or a RSA cryptosystem with a 3072-bit key can provide a security strength of approximately 128 bits. No consensus on metrics to measure the irreversibility of a BTP scheme
- Still no consensus on how to define & measure the unlinkability of a BTP scheme

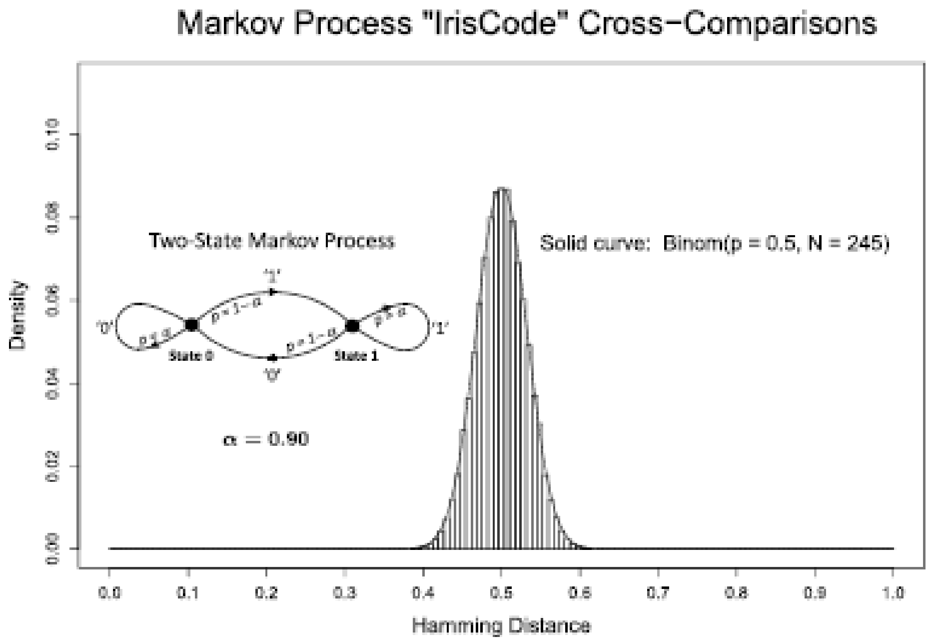
Akerlof's 'market for lemons' explains why so many information security products are poor: buyers are unwilling to pay a premium for quality they cannot measure.

- Anderson and Moore, 2009

Biometric Entropy Estimation







- A 2048-bit IrisCode may have only 245 degrees of freedom
- Entropy of IrisCode is only 0.469 bits per encoded bit

J. Daugman, "Information Theory and the IrisCode," *IEEE T-IFS*, 2016

Measuring Unlinkability

- Possible definition of unlinkability
  - Given two instances of stored data V_1 and V_2 generated from the same biometric trait of the same person, what is the probability of determining that they are linked?
- Often, unlinkability is possible only under the assumption that the second factor (supplementary data) is not compromised

$$V_1 = X + C_1, \;\; V_2 = X' + C_2$$

$$(V_1 + V_2) = (X + X') + (C_1 + C_2) = \Delta + C_3$$

If Hamming weight of Δ is small, one can decode successfully

- What are the reasonable assumptions for analyzing unlinkability?

Summary

- Biometric matching in the encrypted domain is an important issue because compromised templates cannot be revoked/reissued
- A biometric encryption scheme with provable security & acceptable performance has remained elusive
- Challenge is to design transforms/cryptosystems that
  - generate unlinkable templates
  - provide good trade-off between accuracy & security
- Future lies in leveraging advancements in deep learning and generative models to develop new schemes that work at the input/signal level