Biometric Cryptosystems:

Fuzzy Vault Enhancement, ANN & Secure Sketch for Key Generation

Assoc. Prof. Dr. **DANG TRAN KHANH**

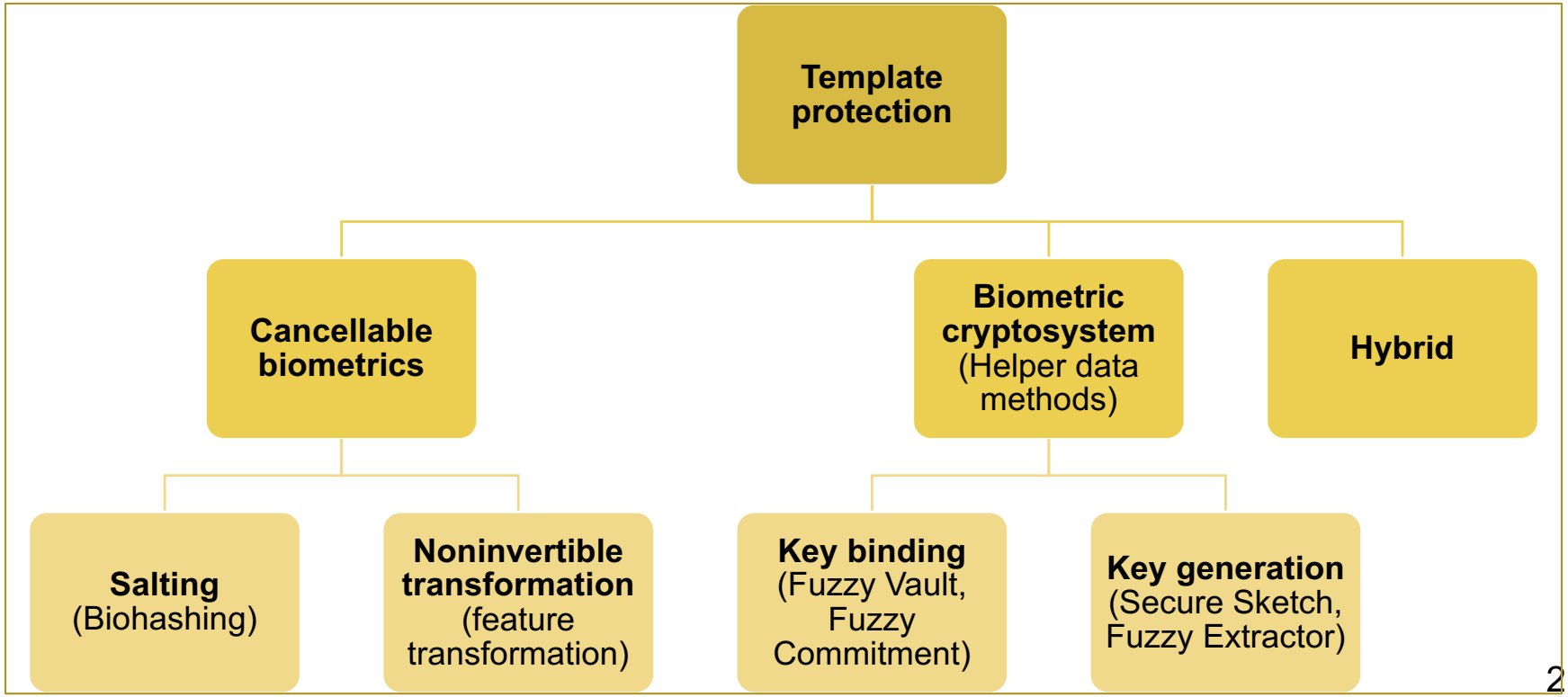
CSE/HCMUT, Vietnam

khanh@hcmut.edu.vn

Data SecuriTy Applied Research Lab

Contents

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



Contents

Outline

- An approach to enhance fuzzy vaults
- ANN and secure sketch for biometric key generation
- Reading:

DANG Tran Khanh, et al. (2016): *A Novel Chaff Points Generation Mechanism for Improving Fuzzy Vault Security*. IET Biometrics, United Kingdom, 5(2):147-153, ISSN 2047-4938, June 2016 (SCIE)

DANG Tran Khanh, et al. (2018): *A Hybrid Template Protection Approach using Secure Sketch and ANN for Strong Biometric Key Generation with Revocability Guarantee.* The International Arab Journal of Information Technology (IAJIT), 15(2):331-340, ISSN 1683-3198, 2018 (SCIE)

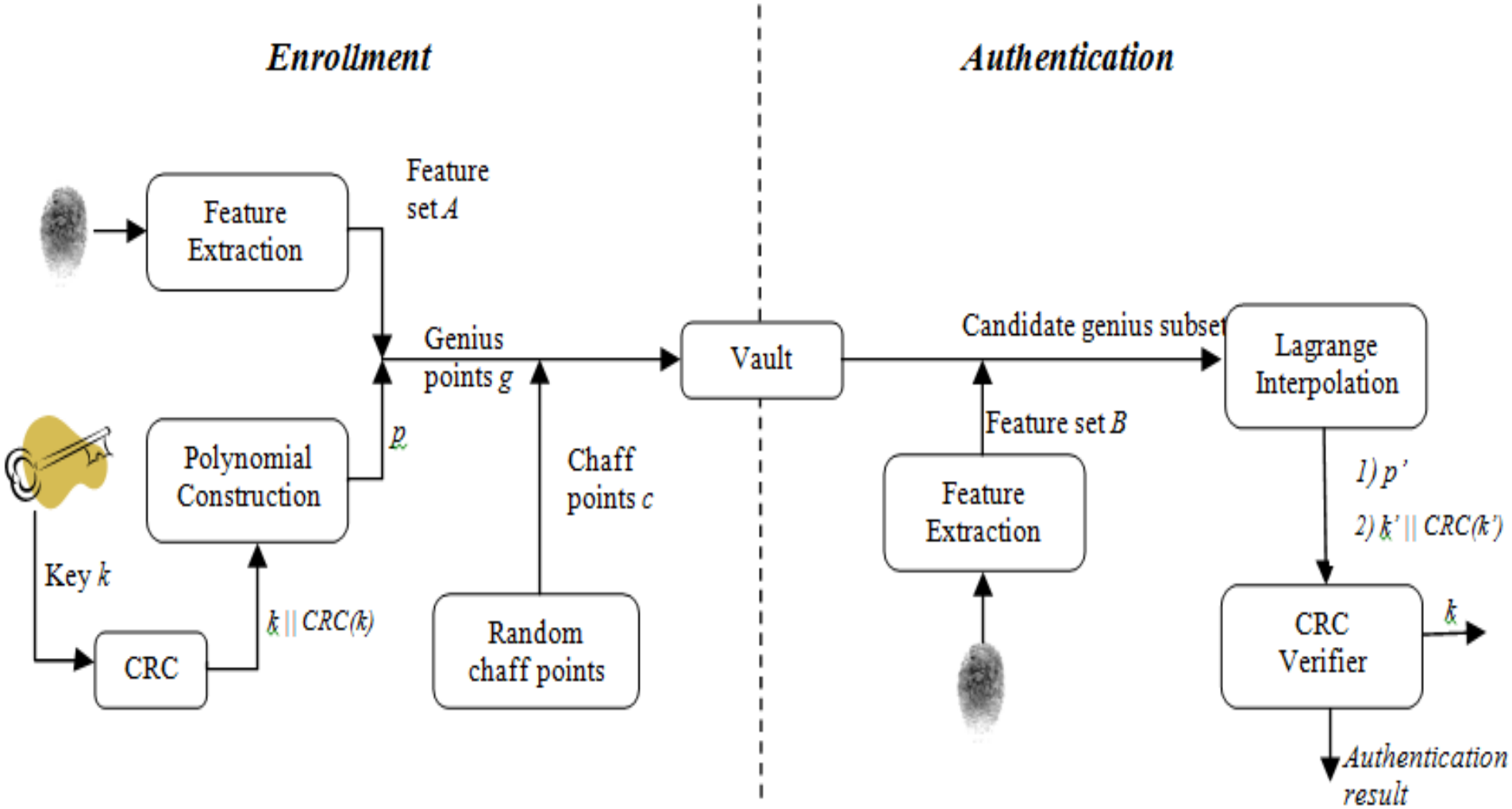
(optional)

Fuzzy vault enhancement

Discussion exercise: fuzzy vault security

Dealing with cross-matching & blended substitution attacks in traditional fuzzy vaults ?

Traditional Fuzzy Vault with CRC Error Correction



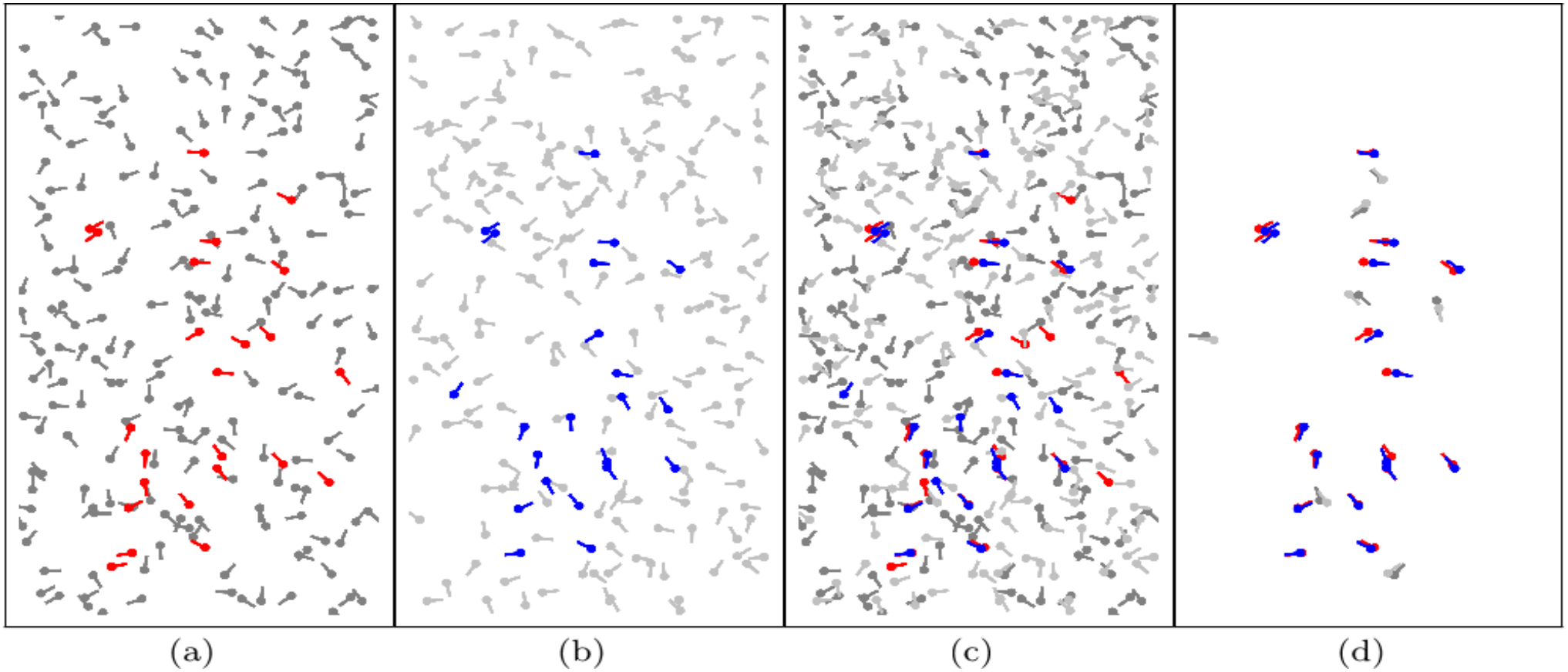
Traditional Fuzzy Vault with CRC Error Correction

- Alice places a secret κ in a fuzzy vault and locks it using a set A of elements
- To unlock the vault, and retrieve κ, Bob must present a set B that substantially overlaps with A
- Fuzzy vaults are order invariant, meaning A and B may be arranged in any order
- To protect κ, it is represented as a polynomial p, specifically encoded in the coefficients. A set of points R is constructed from A and p(A). Chaff points C are randomly generated and inserted into R
- The subset matching problem with some error correction codes (like Reed-Solomon) can be used

Traditional Fuzzy Vault with CRC Error Correction

- By using a number of evaluation points greater than the degree of the polynomial, it will be possible to obtain the polynomial (and therefore the message) by interpolation even in the presence of missing or erroneous values
- If there are too many errors, there will not be a unique interpolating polynomial of the proper degree
- Further details:
  - ✓ https://wiki.cse.buffalo.edu/cse545/content/fuzzy-vault
  - ✓ https://en.wikipedia.org/wiki/Reed%E2%80%93Solomon_error_correction

Cross-matching Attack



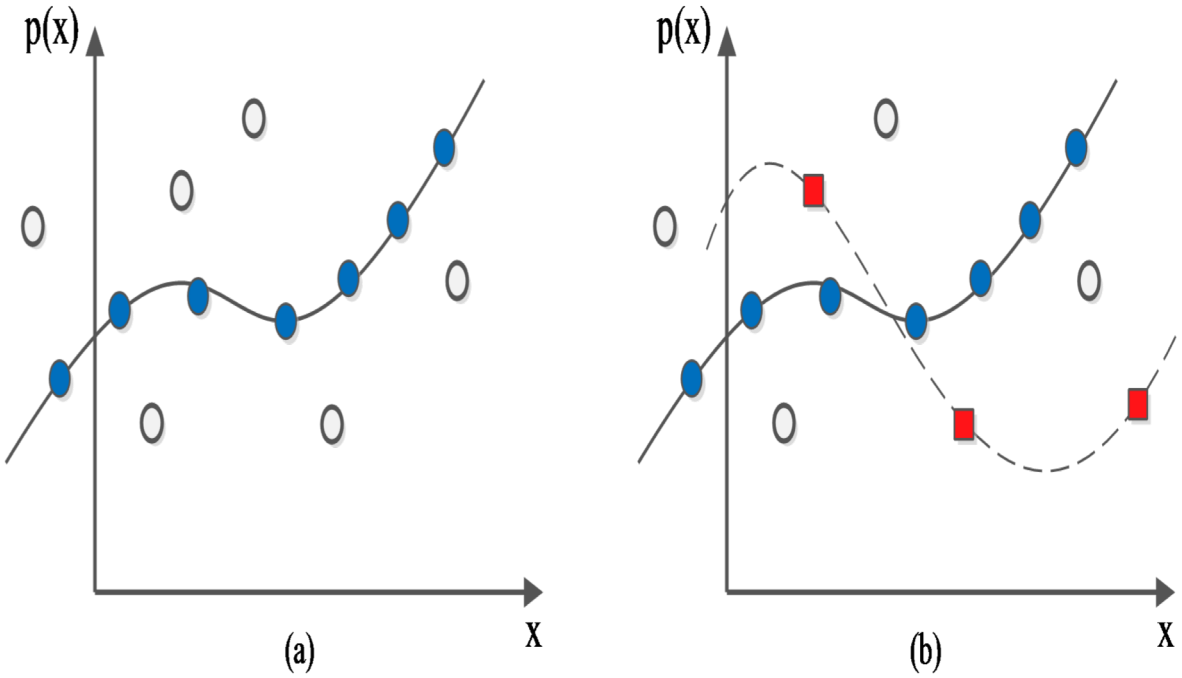
(a): First fuzzy vault

(b): Second fuzzy vault

(c): Matching two vaults

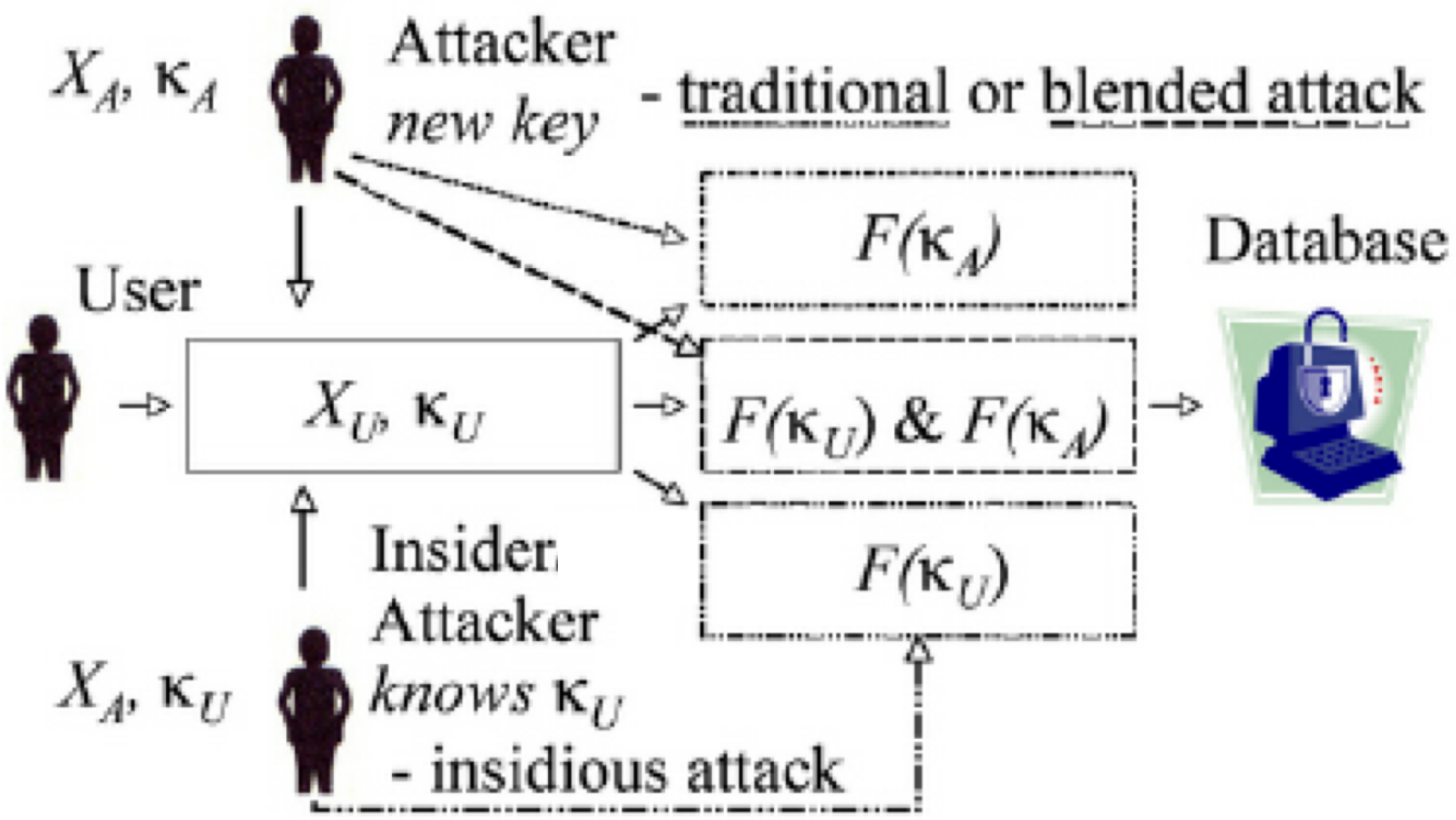
(d): Matching genuine points

Blended-substitution Attack



- Vault contains *g* genuine points, c chaff points
- *n*-degree polynomial
- At least (*n*+1) genuine points need to be verified to authenticate
- Imposter randomly remove (*n*+1) points of Vault and substitute his (*n*+1) genuine points
- The system accept both genuine and imposter user without any notifications

Blended-substitution Attack

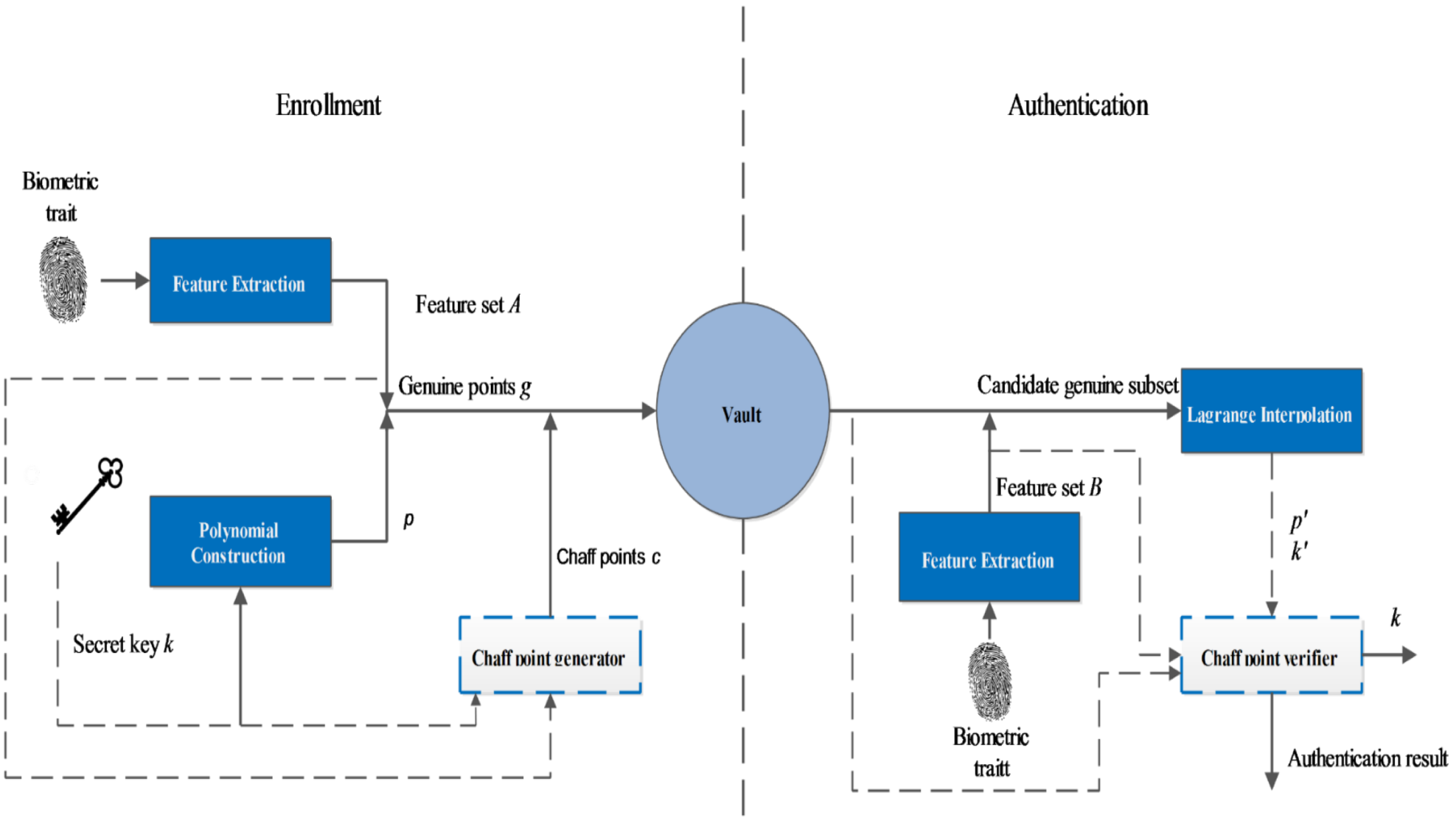


Different contexts !

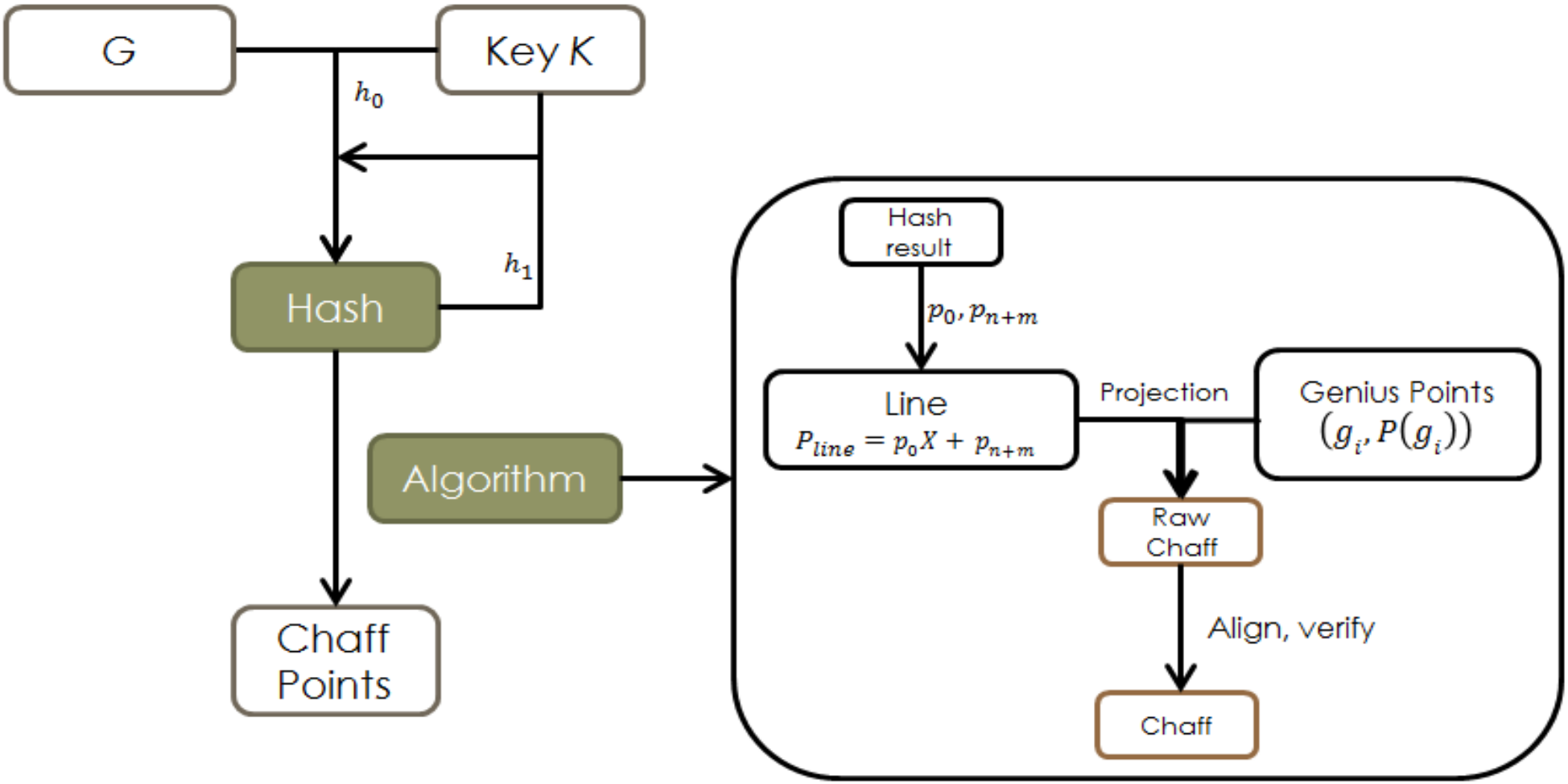
A novel chaff points generation mechanism for improving fuzzy vault security

DANG Tran Khanh, et al. (2016): *A Novel Chaff Points Generation Mechanism for Improving Fuzzy Vault Security*. IET Biometrics, United Kingdom, 5(2):147-153, ISSN 2047-4938, June 2016 (SCIE)

Fuzzy Vault Enhancement



Chaff points generation

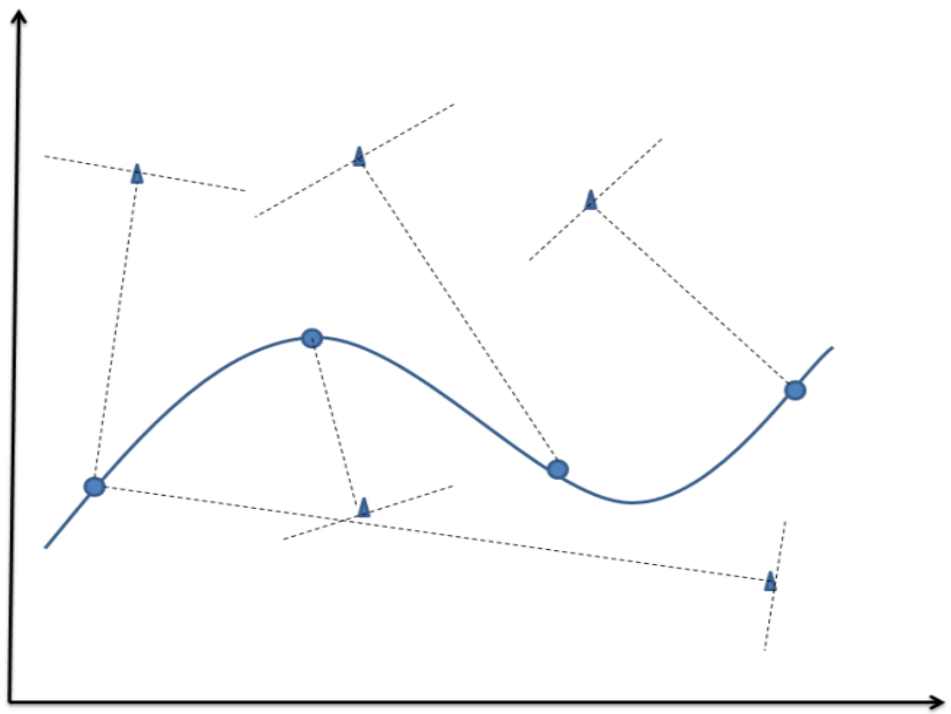


Chaff points generation

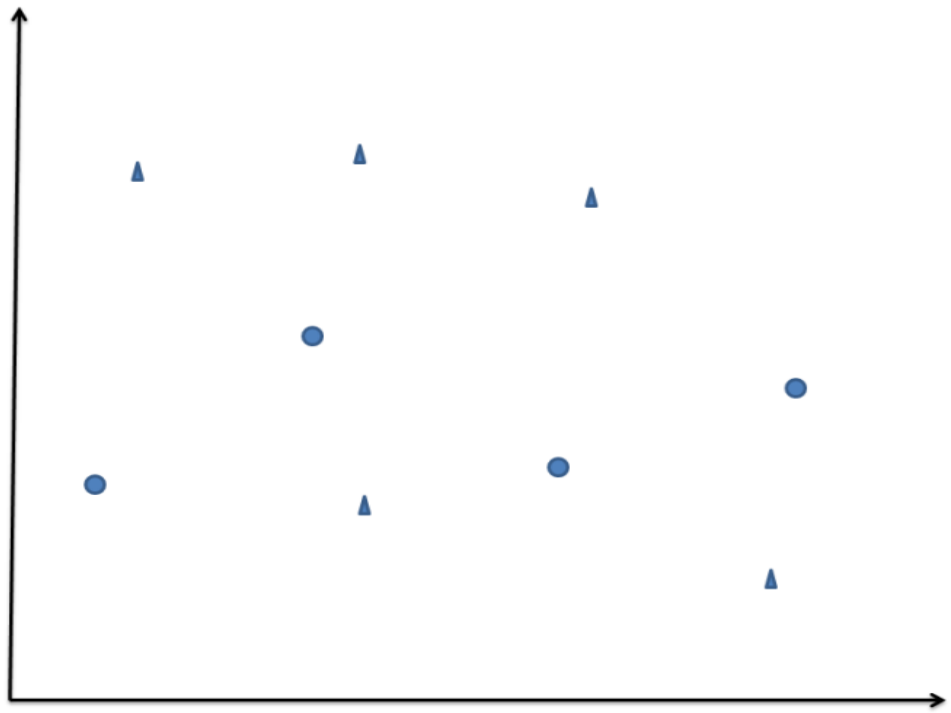
- **Step 1**: Sorting genuine set $G = \{(g_i, P(g_i)) \mid g_i \in g\}$ by g_i in ascending order
- **Step 2**: The original input h_0 is created by combining both g and secret key k

  $h_0 = (g_0, g_1, \ldots, g_{m-1}, k_0, k_1, \ldots, k_{n-1}) \in F_q^{n+m}$
- **Step 3**: A hashing function $f: F_q^{n+m} \rightarrow F_q^{n+m}$ is applied on h_0 to form a new hashed input: $h_1 = (p_0, p_1, \ldots, p_{n+m-1}) \in F_q^{n+m}$
- **Step 4**: Using p_0 and p_{n+m-1} to form a new line:
  - $P_{line} = p_0 X + p_{n+m-1}$
- **Step 5:** An element from genuine set $G = \{(g_i, P(g_i)) \mid g_i \in g\}$ is chosen and projected directly onto P_{line} to generate a chaff point $(c_i, P'_i) \in F_q^2$

Chaff points generation visualization



a)



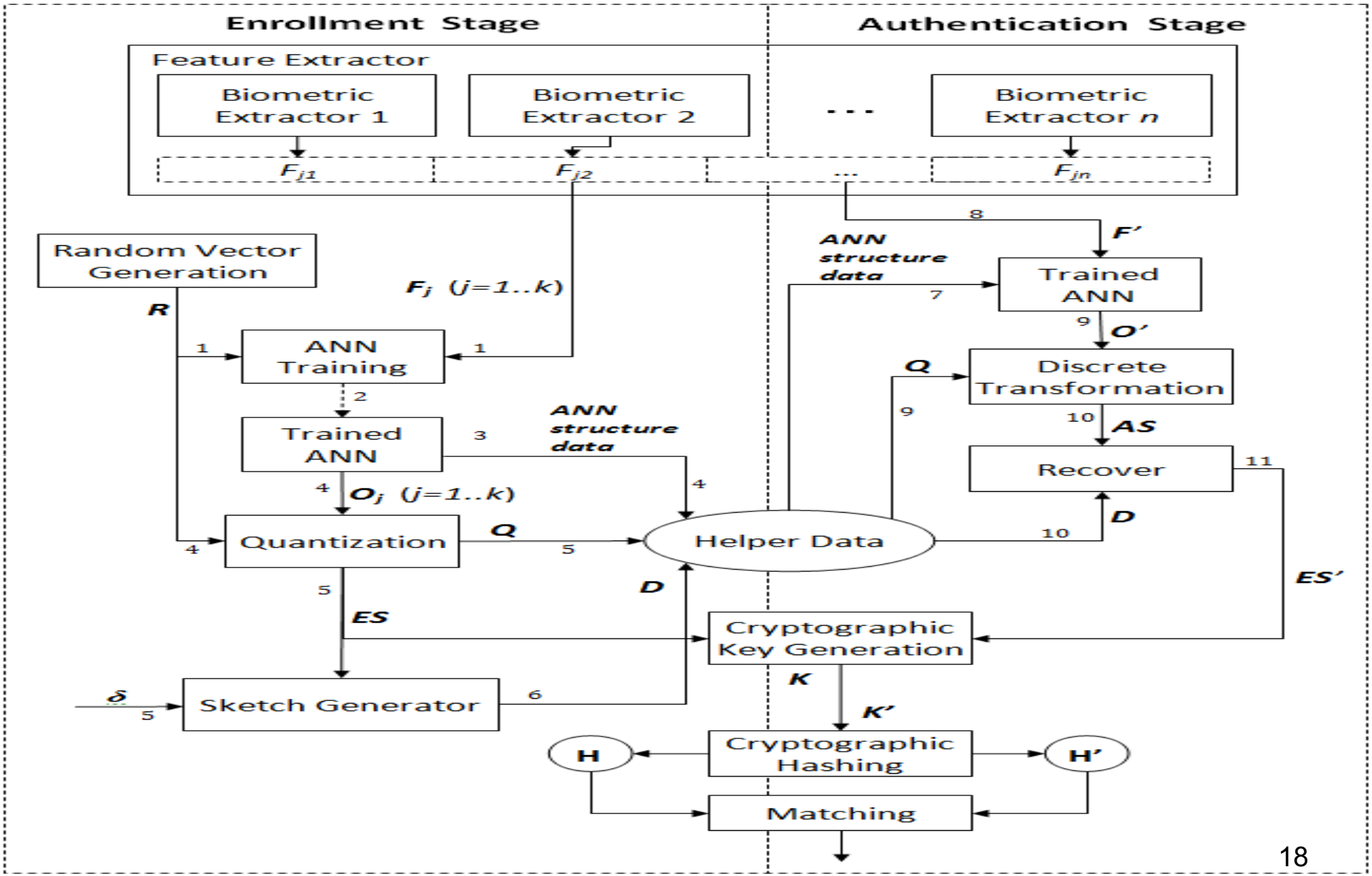
b)

- Genuine points
- Chaff points

ANN and Secure Sketch for Biometric Key Generation

DANG Tran Khanh, et al. (2018): *A Hybrid Template Protection Approach using Secure Sketch and ANN for Strong Biometric Key Generation with Revocability Guarantee.* The International Arab Journal of Information Technology (IAJIT), 15(2):331-340, ISSN 1683-3198, 2018 (SCIE)

Proposed Scheme



Proposed Scheme

- Feature extraction vectors

  $F_j = F_{j1} \,||\, F_{j2} \,||\, \ldots \,||\, F_{jl} \in \mathbb{R}^m \;\; (1 \le j \le k), (l \ge 1)$

- Random Vector Generation: Generates the output for training the ANN

  $R = (r_1, r_2, \ldots, r_n) \in [0, 1]^n$ is randomly generated

- *k* instances of feature vectors are trained for the ANN

- *ANN:* Multilayer Feed-Forward Back-Propagation with one hidden layer containing $\sqrt{m * n}$ nodes

Proposed Scheme

- Quantization: extract the stability of output from ANN and generate biometric key ES

  trainedANN(F_j) = O_j = (O_{j1}, O_{j2}, …,O_{jn}), (j=1..k)

  $Q = (q_1, q_2, \ldots, q_n)$ is the quantization vector

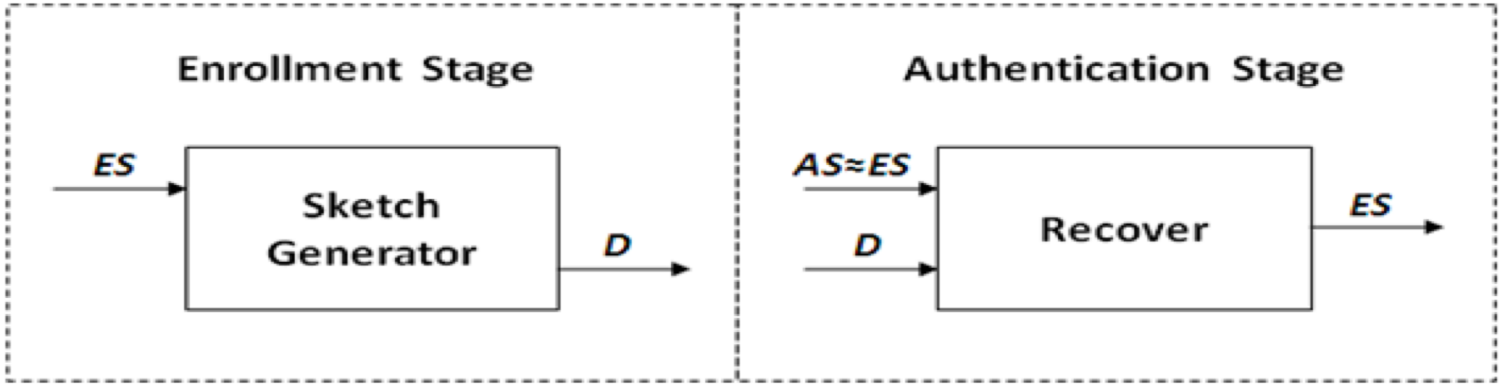
  $$q_i = \langle Max\ q \mid \lfloor 10^q * O_{ji} \rfloor = \lfloor 10^q * O_{li} \rfloor, \forall j, l \in [1, k], j \neq l \rangle$$

  $$ES_i = \mathrm{Round}(r_i * 10^{q_i}) \qquad (i=1..n) \qquad (2)$$

- The cryptography key *K* could be generated from *ES*
- The hash version of *K* is stored for authentication purposes

Proposed Scheme

- Sketch Generator



Generate Helper Data: $D = (d_1, d_2, \ldots, d_n)$

$$d_i = \mathrm{SG}(ES_i, \delta) = ES_i - \mathrm{Map}(ES_i, \delta) \qquad (i=1..n)$$

Map(x, δ) = ⟨c | c - $\delta \le x \le c + \delta$, $x \in$ N, $\delta \in$ N, $c \in$ δ-codebook⟩

δ-codebook = $\langle \{c \mid c \bmod \theta = 0, c \in \mathbb{N}\} \rangle$ $\theta = 2 * \delta + 1$

δ: error tolerance capacity

Proposed Scheme

- Recovery

  trainedANN(F') = O' = (O'_1, O'_2, …,O'_n)

  Vector O' is quantized to create AS = (AS_1, AS_2, …, AS_n) as followed: (Q was stored in the authentication step)

  - ✓ $AS_i = \text{Round}(O'_i * 10^{q_i})$
  - ✓ Q = $(q_1, q_2, \dots, q_n)$

  Biometric key ES' = (ES'_1, ES'_2, …, ES'_n) is recovered from AS and D (Helper Data D was stored in the database)

  - ✓ $ES'_i = \text{Map}(AS_i - d_i, \delta) + d_i$ (4)
  - ✓ D = $(d_1, d_2, \dots, d_n)$

Proposed Scheme

- Main features of proposed scheme

Key Diversity and Revocability

- ✓ Once the biometric key ES is compromised, another key is easily generated by re-applying the scheme with a new random vector

Template Protection ability

- ✓ The transformation from biometric template to biometric key is non-invertible

Experiments

- The experiments are evaluated on face and voice biometric

  Face: 51 input nodes, 40 output nodes

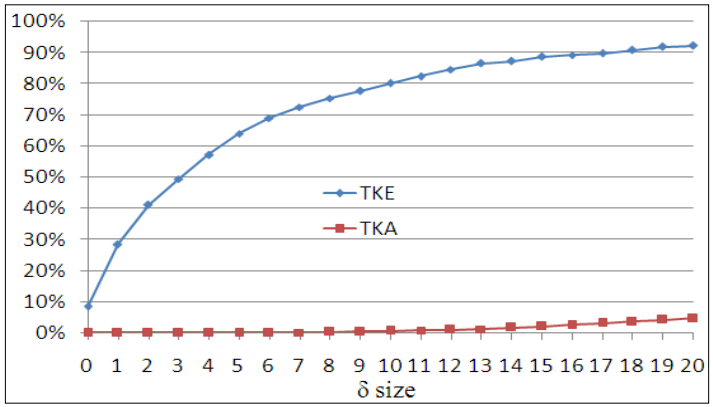
  - 105 face images are captured from Samsung Duos model GT-S7562
  - 306 face images of 153 persons from face94 dataset.

  Voice: 39 input nodes, 25 output nodes

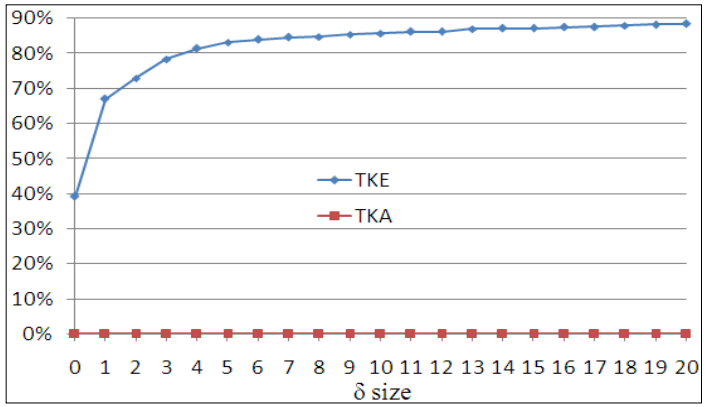
  - 105 audio files are recorded from Samsung Duos model GT-S7562
  - The AN4 dataset is collected from 84 persons. 13 audio files per each person

  Face + Voice: 90 input nodes, 65 output nodes

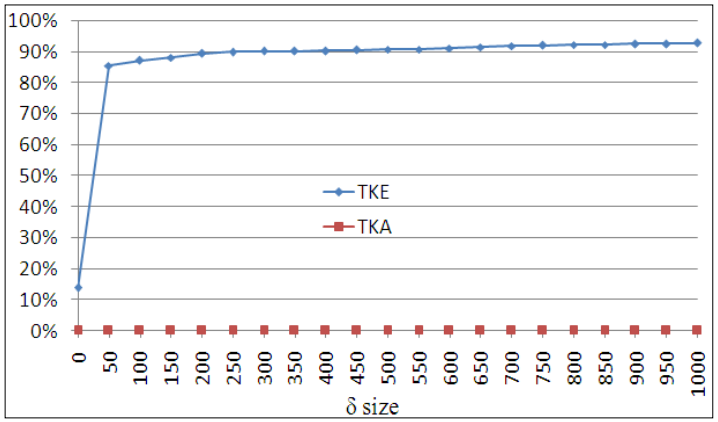
Experiment



a) Face biometric

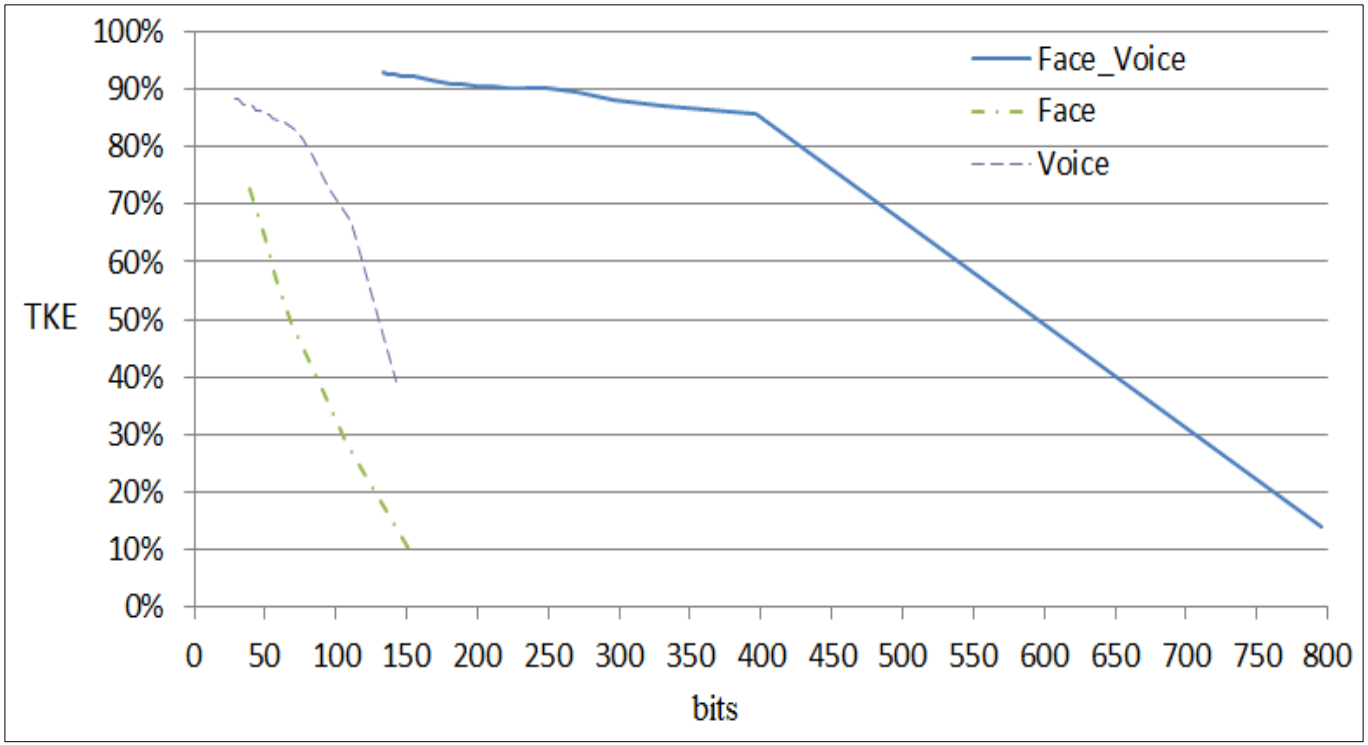


b) Voice biometric



c) Face and Voice biometric

Experiments



d) Balance between recognition performance and Average Remaining Entropy

Main features of proposed scheme

- Important features of biometric cryptosystem are guaranteed
  - Revocability and Diversity
  - Template protection
- Maintain good recognition performance comparing with original features
- Achieve high balance between recognition performance and security (evaluated by average remain entropy)

Summary

- An approach to enhance fuzzy vaults
- ANN and secure sketch for biometric key generation

Q&A

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

khanh@hcmut.edu.vn

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