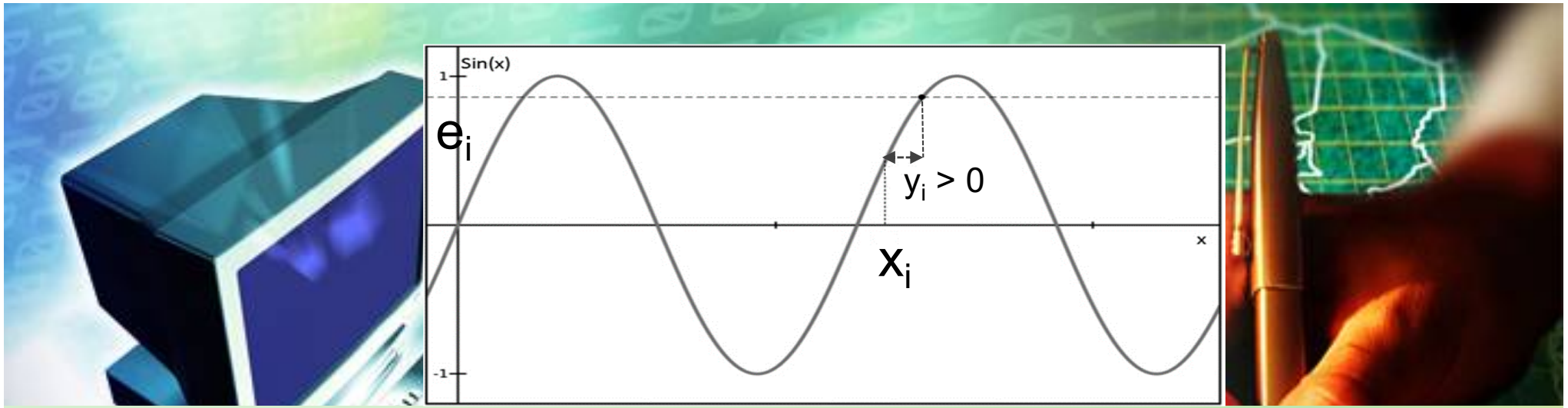


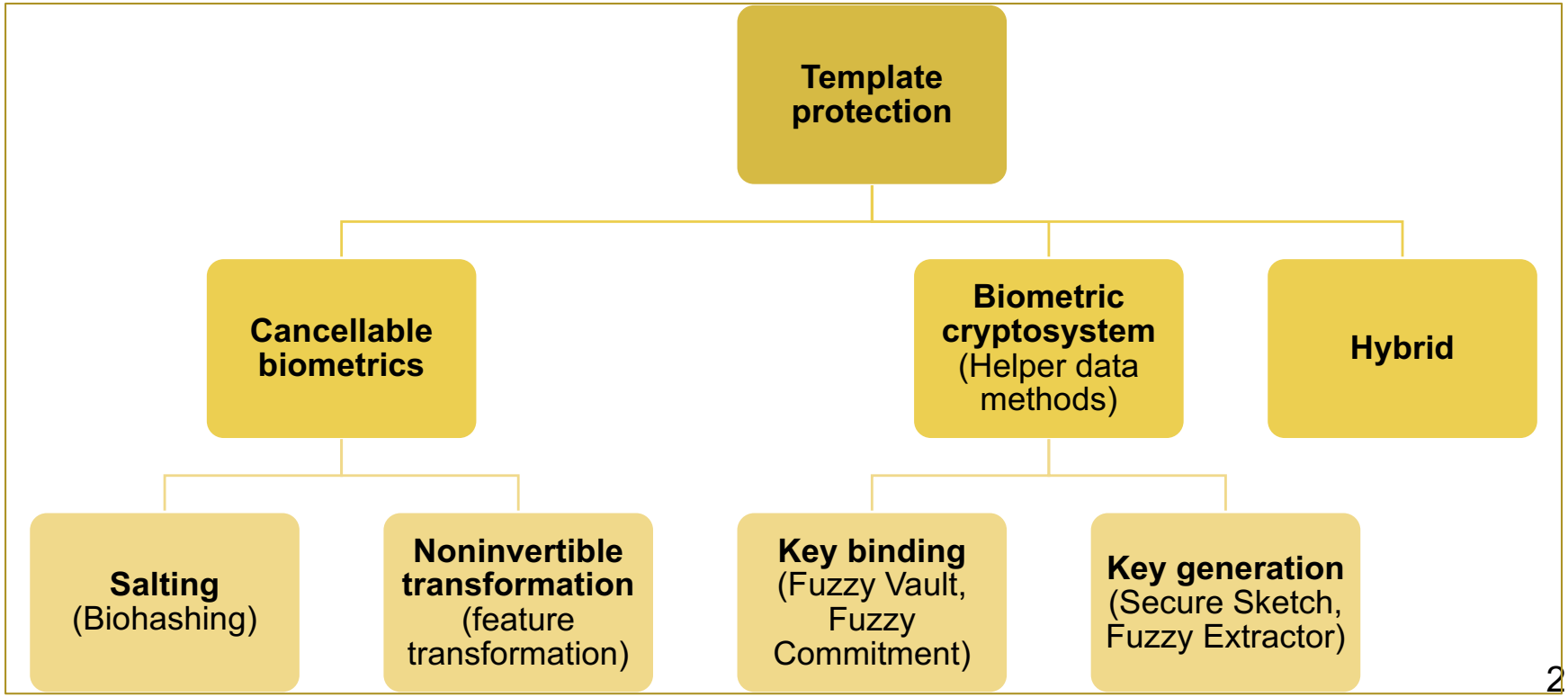
Cancelable Fuzzy Vault with Periodic Transformation for Biometric Template Protection

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

- Introduction
  - Fuzzy vault issues
  - A solution: transformation + fuzzy vault scheme
- Cancelable fuzzy vault with periodic transformation for biometric template protection
  - Cancellable biometrics: periodic transformation – SIN
  - Hybrid approaches: cancellable biometrics + fuzzy vault scheme
- Reading:

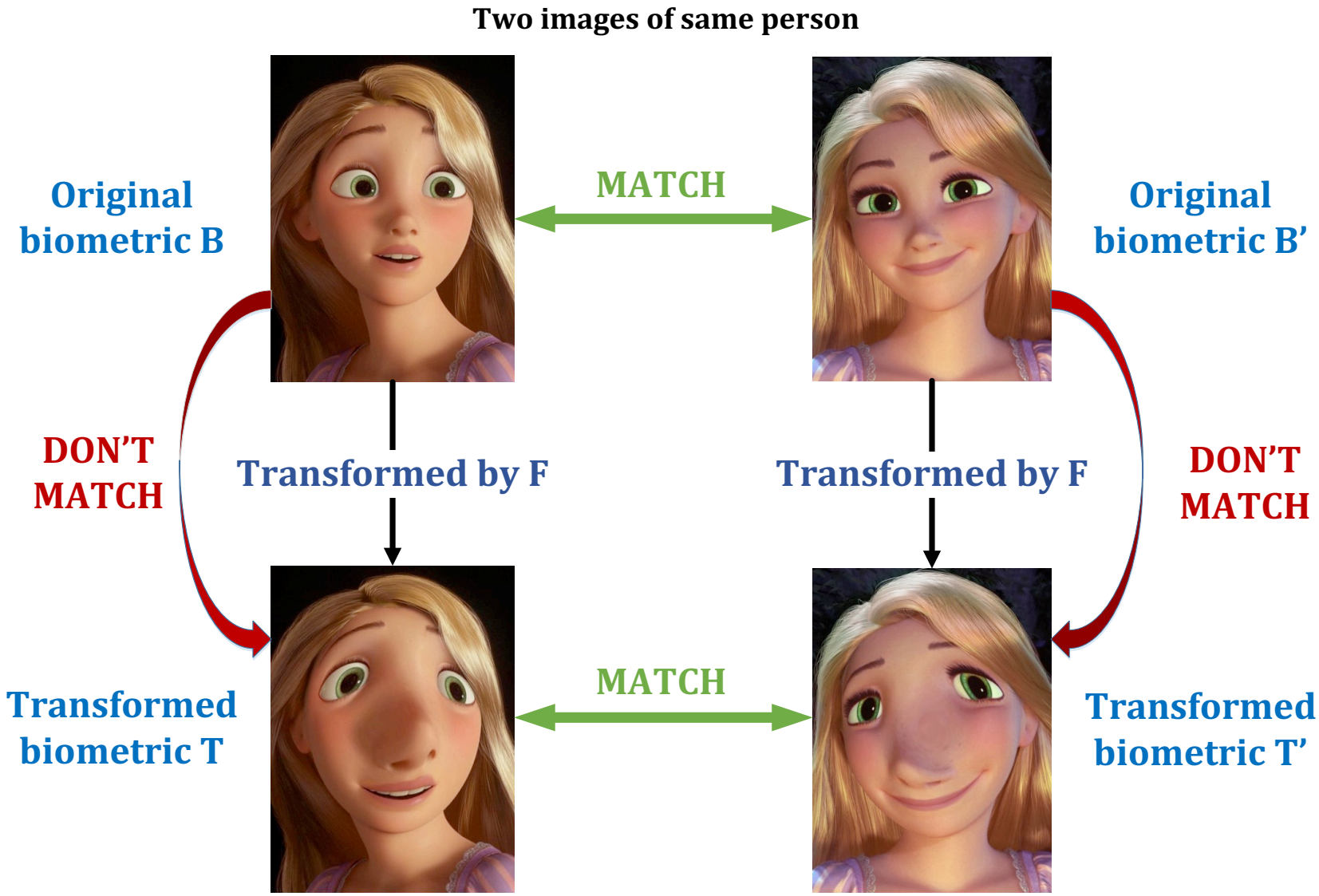
Dang, Tran Khanh, et al. (2016): Cancellable fuzzy vault with periodic transformation for biometric template protection. *IET Biometrics* 5(3): 229-235 (SCIE)

Introduction: fuzzy vault issues

- Correlation attack
  - Unstructured chaff points (random)
  - Correlate some vaults of the same person → genuine points
- Cross-matching across different databases
  - Structured chaff points
  - The same vault → The same person
- Blended substitution attack
  - Substitute a few points in the vault using his own biometric data
- **No diversity and no revocability**

→Apply **transformation** in **fuzzy vault scheme**

Non-invertible transforming (revised)



Non-invertible transforming (revised)

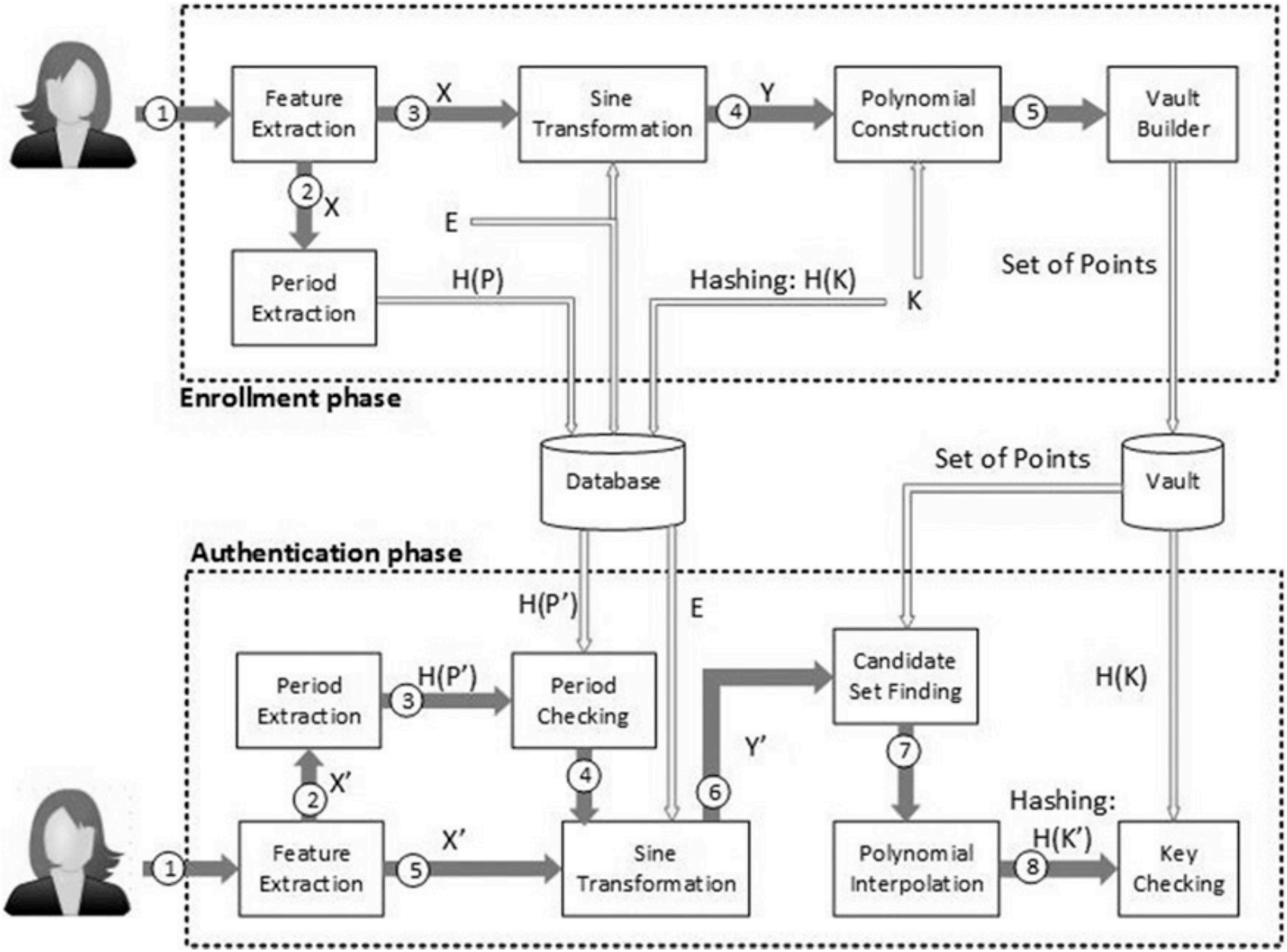
- The most challenge is that how to preserve the similarity of distances among transformed templates and among original templates
- It means that two transformed templates must be closed if the two original templates are closed
- This characteristic keeps the error rates of the transformed biometric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

Outline

- ~~Introduction~~
  - ~~Fuzzy vault issues~~
  - ~~A solution: transformation + fuzzy vault scheme~~
- Cancelable fuzzy vault with periodic transformation for biometric template protection
  - Cancellable biometrics: periodic transformation – SIN
  - Hybrid approaches: cancellable biometrics + fuzzy vault scheme
- Reading:

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

Proposed Architecture



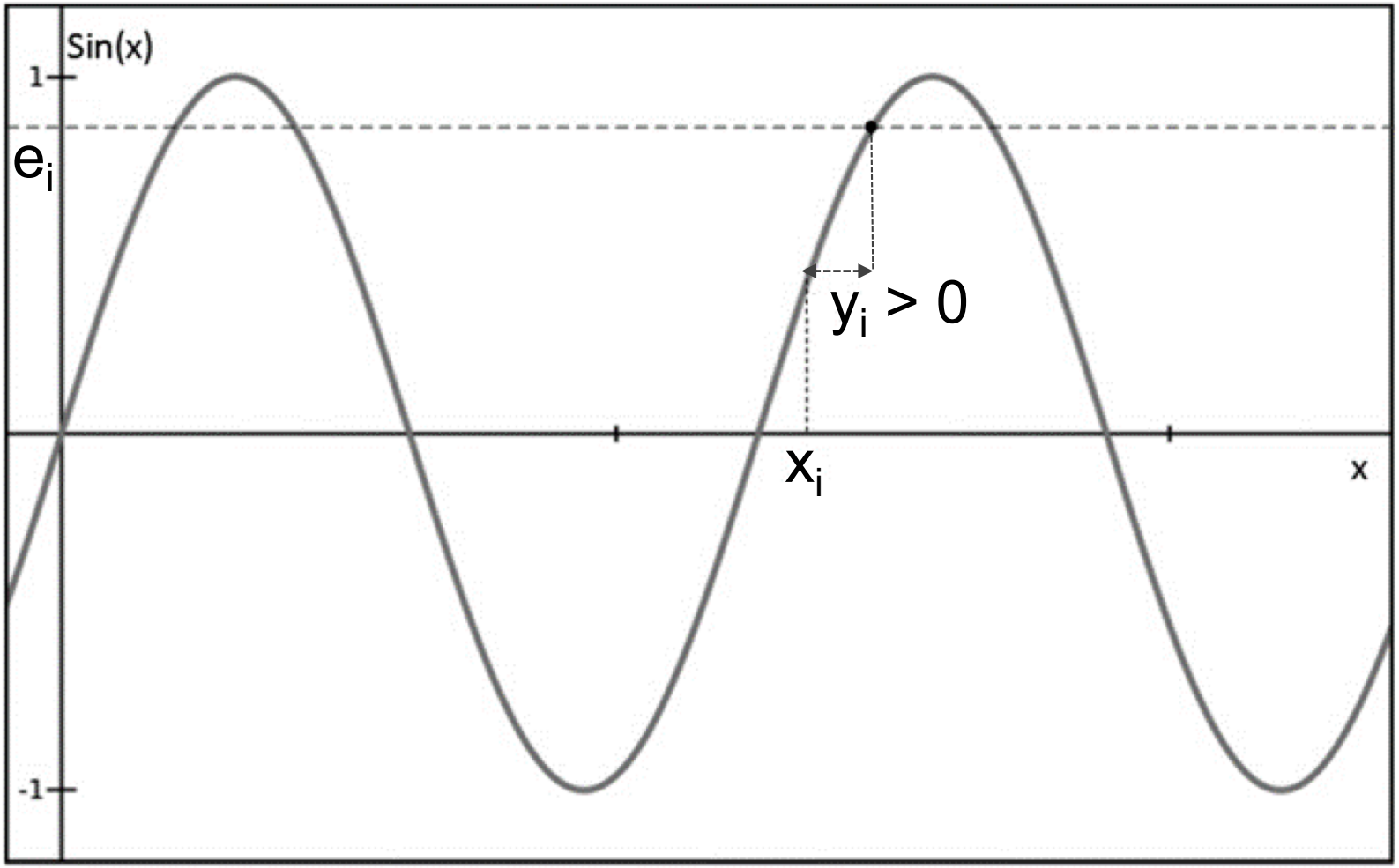
Periodic transformation

- $X = \{x_1, x_2, .., x_n\}$: a biometric feature vector extracted from the face image of a user.
- $Y = \{y_1, y_2, .., y_n\}$: a transformed vector after applied sine transformation on X
- $E = \{e_1, e_2, .., e_n\}$: a random vector, in which e_i is chosen randomly between [−1, 1].
- $P = p_1, p_2, \ldots, p_n$: a string of period numbers of elements in X.
- The transformation function:

$$\sin(x_i + y_i) = e_i$$

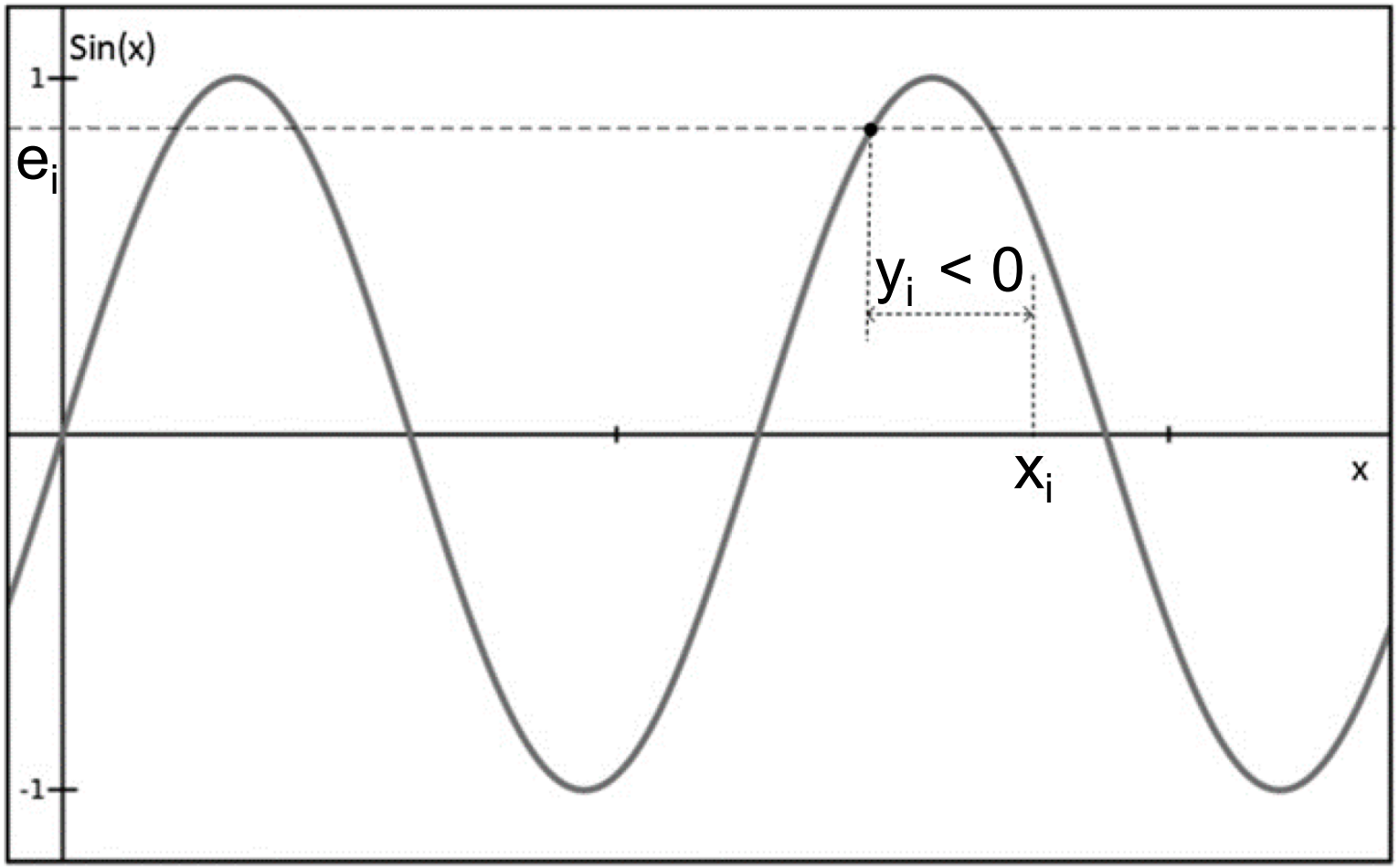
Sine Transformation

- Sine transformation with yi> 0



Sine Transformation

- Sine transformation with yi<0



Period extraction

- For each x_i in X, calculate p_i - the period number of xi.

$$p_i = x_i \div 2\pi$$

- Convert p_i to binary.

- Combine all period data pi to get a binary string.

  $P = p_1 \,||\, p_2 \,||\, \ldots \,||\, p_n$

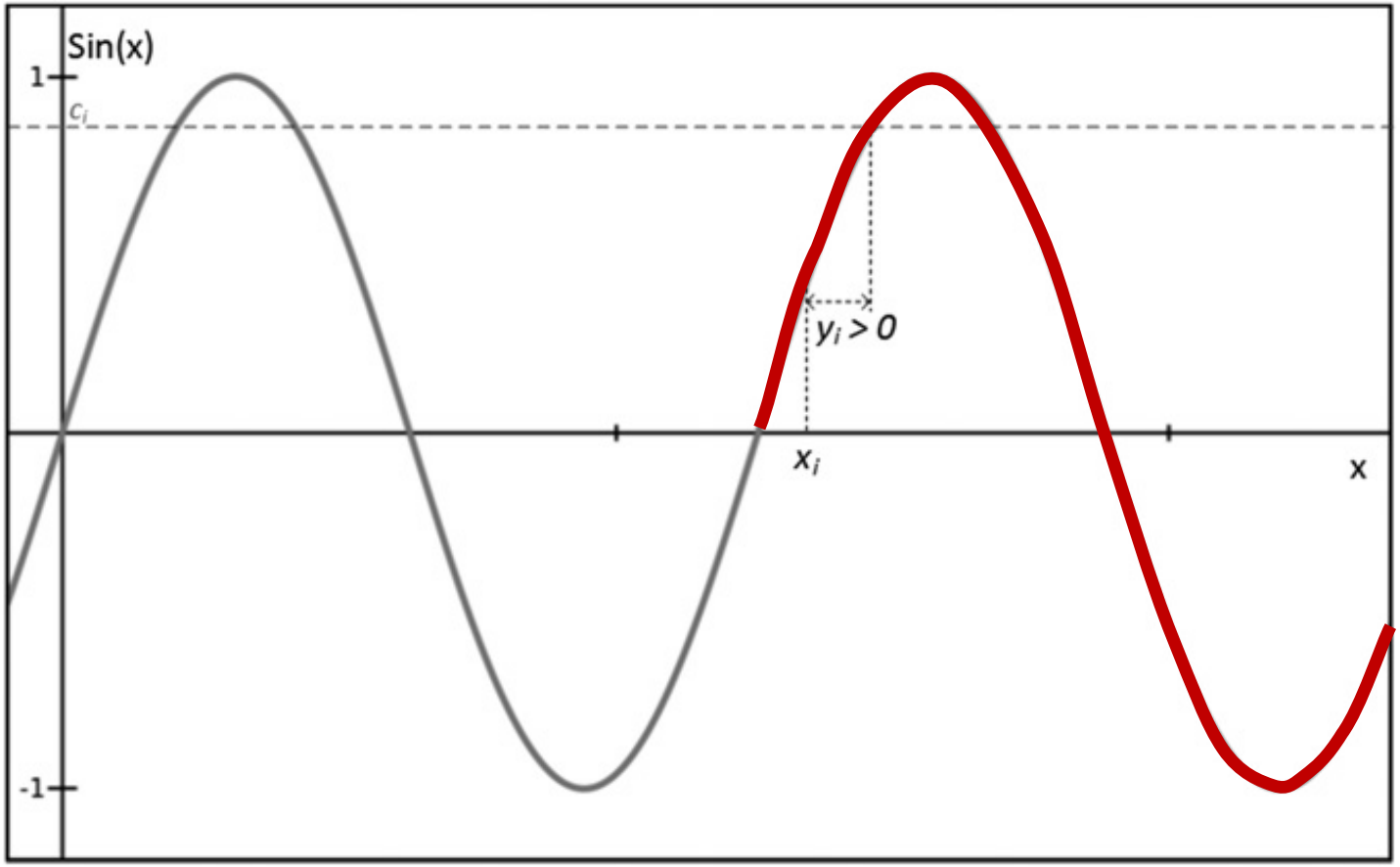
  HP = H(P)

  C: error-correction code for P

- HP || C: stored in the database.

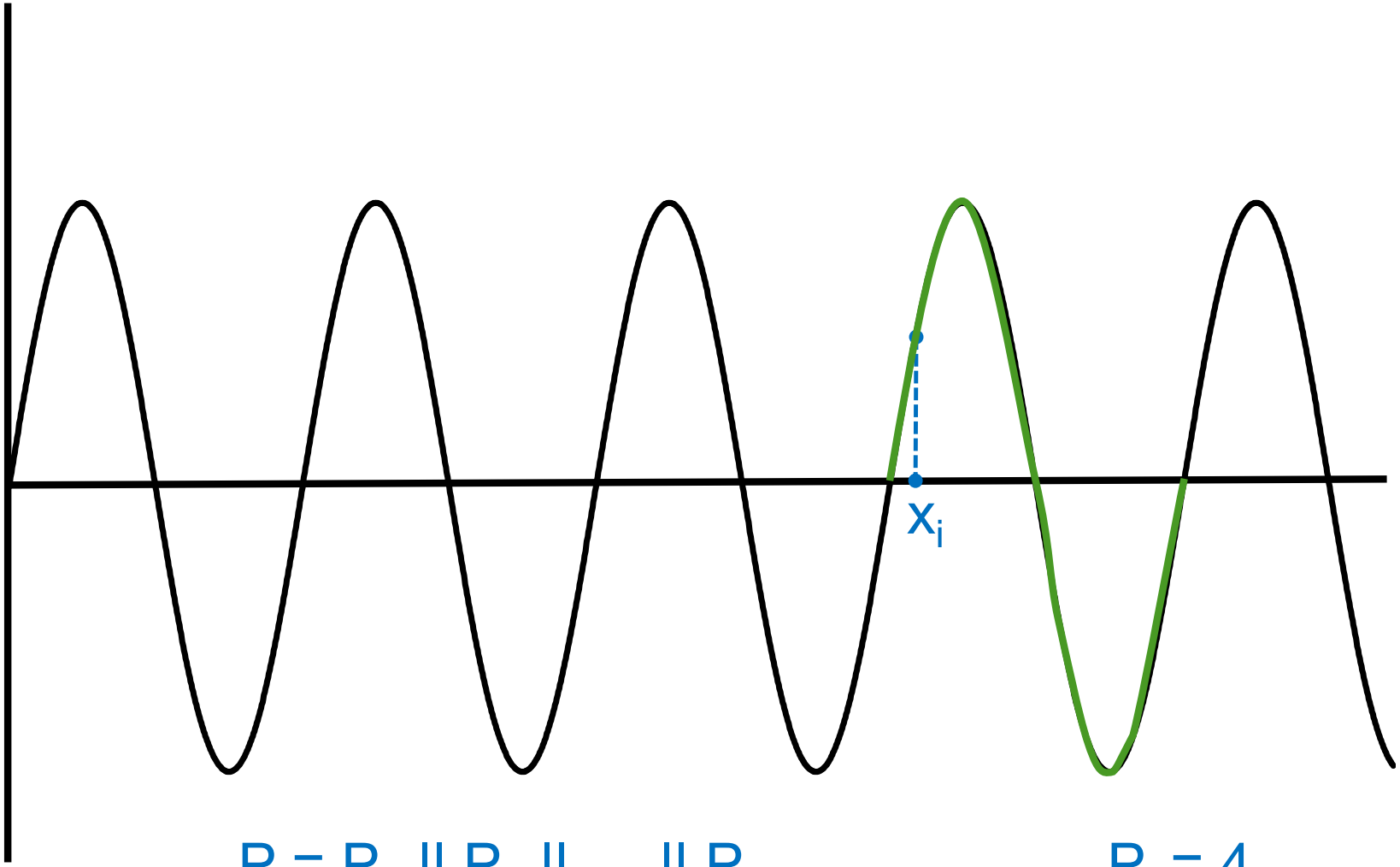
Period extraction

- $P_i = 1$



Enrollment: Period extraction

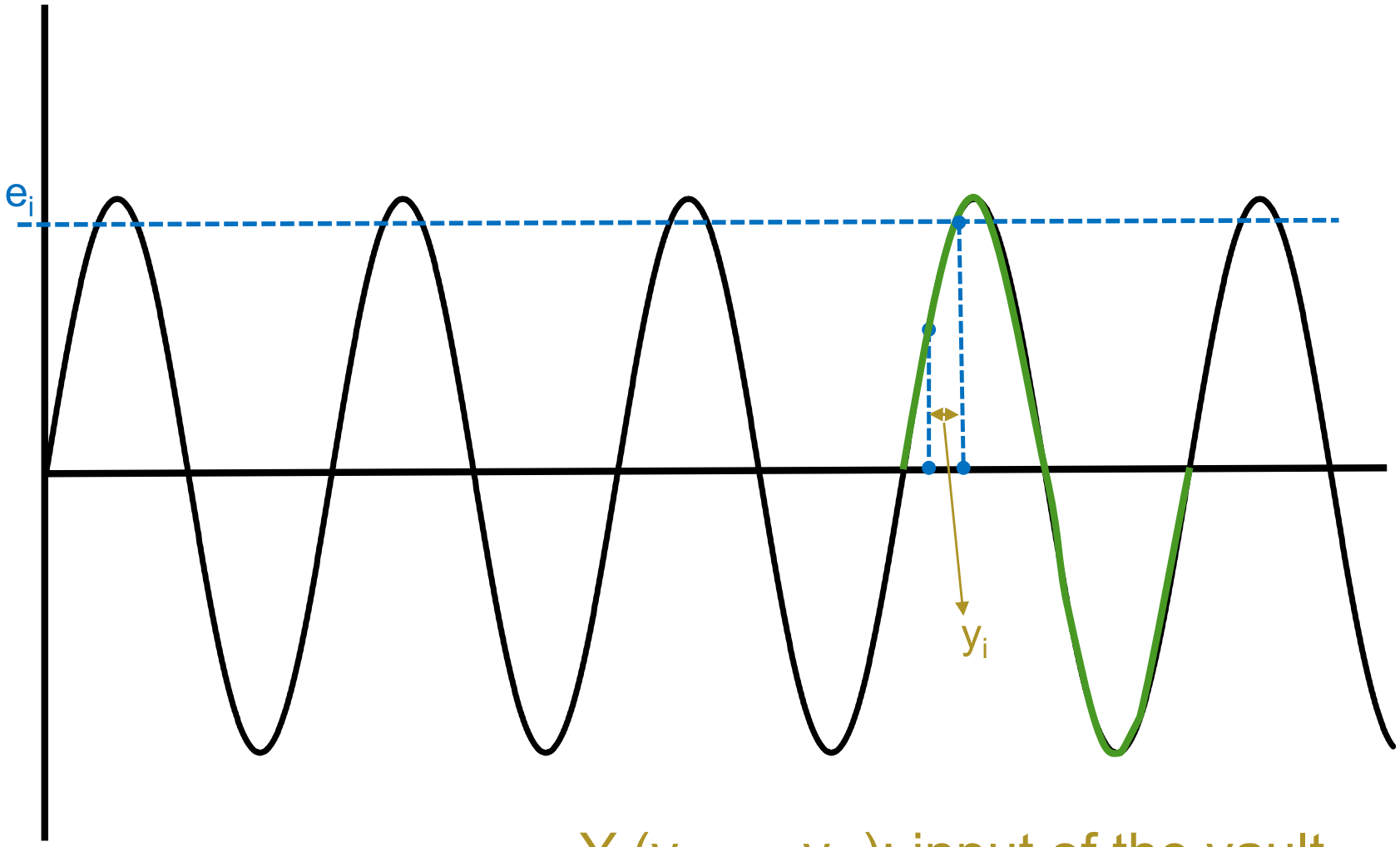
$X = \{x_1, x_2, .., x_n\}$: vector extracted from the enrolled face image



$P = P_1 \,||\, P_2 \,||\, \ldots \,||\, P_n$

$P_i = 4$

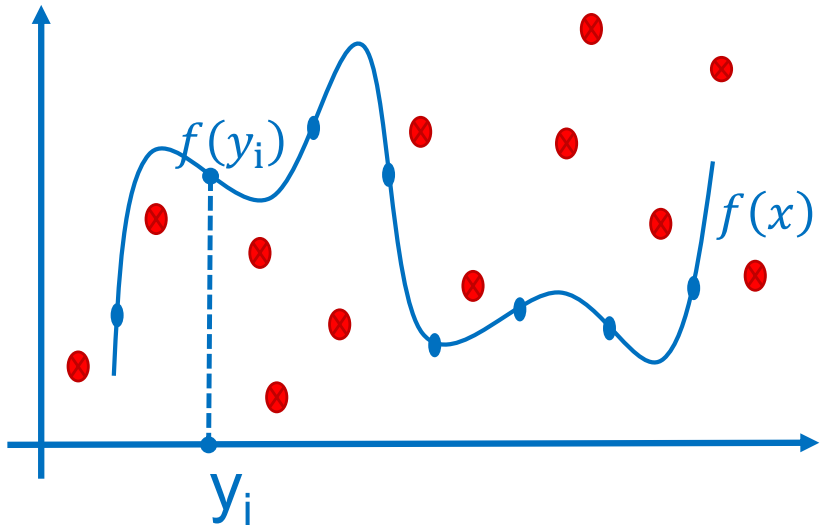
Enrollment: Sine Transformation



Y (y_1,…, y_n): input of the vault

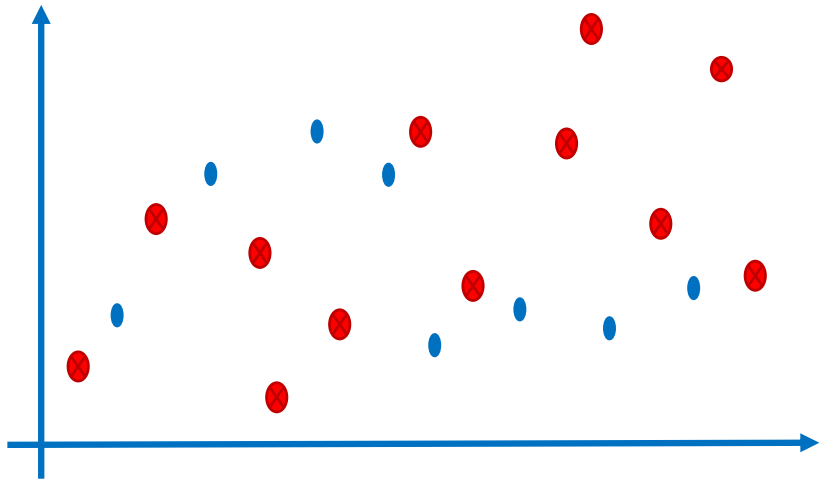
Enrollment: Construct fuzzy vault

- $f(x) = c_9x^9 + c_8x^8 + \cdots + c_1x + c_0$
- K = $c_9 \parallel c_8 \parallel \ldots \parallel c_0$
- $(y_1, f(y_1))$; $(y_2, f(y_2))$; … ; $(y_n, f(y_n))$: genius points



Enrollment: Construct fuzzy vault

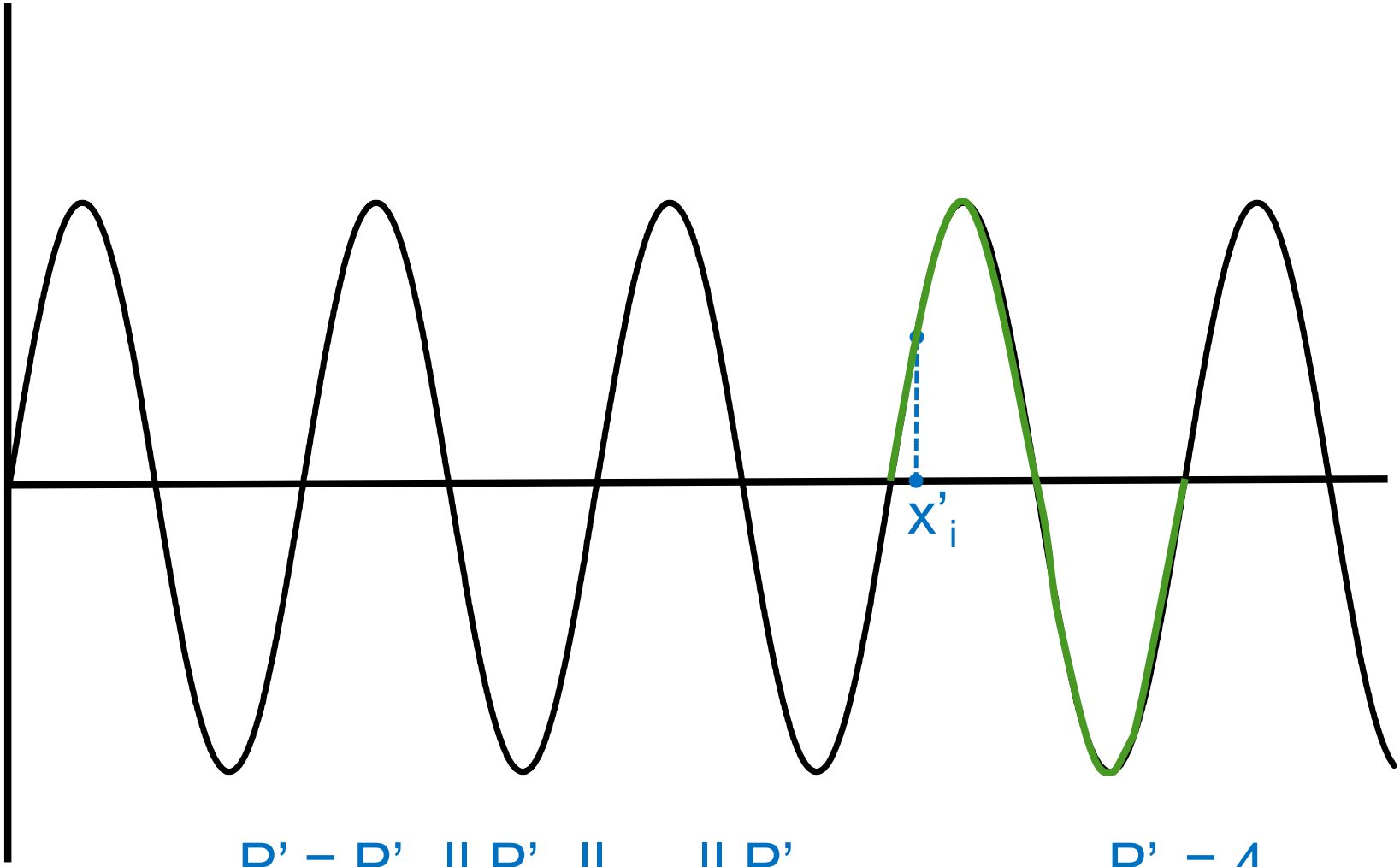
- $f(x) = c_9x^9 + c_8x^8 + \cdots + c_1x + c_0$
- K = $c_9 \parallel c_8 \parallel \ldots \parallel c_0$
- $(y_1, f(y_1))$; $(y_2, f(y_2))$; … ; $(y_n, f(y_n))$: genius points



Vault

Authentication: Period extraction

$X' = \{x'_1, x'_2, .., x'_n\}$: vector extracted from the authenticated face image

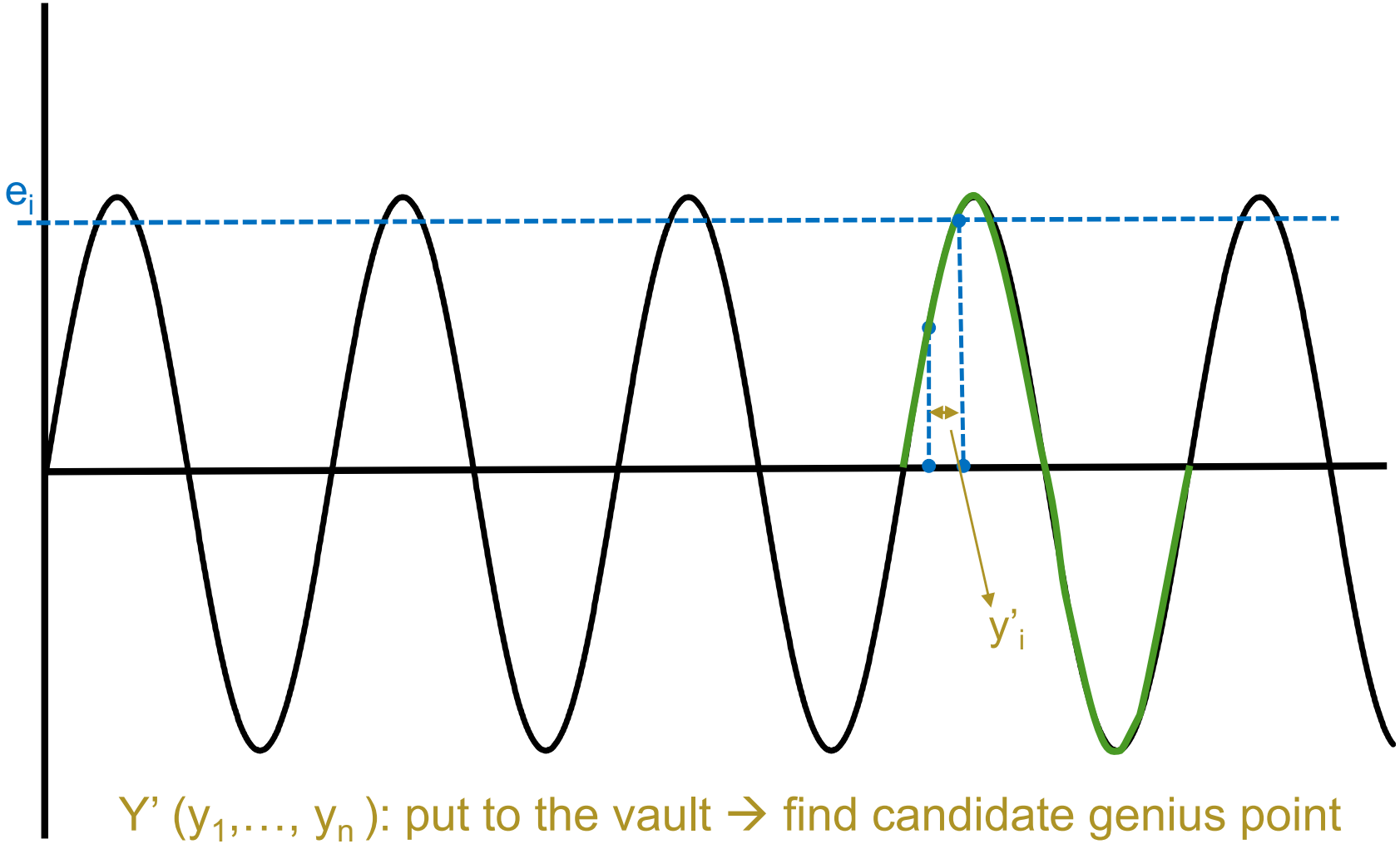


$P' = P'_1 \,||\, P'_2 \,||\, \ldots \,||\, P'_n$

$P'_i = 4$

Authentication: Sine transformation

$X' = \{x'_1, x'_2, .., x'_n\}$: vector extracted from the authenticated face image



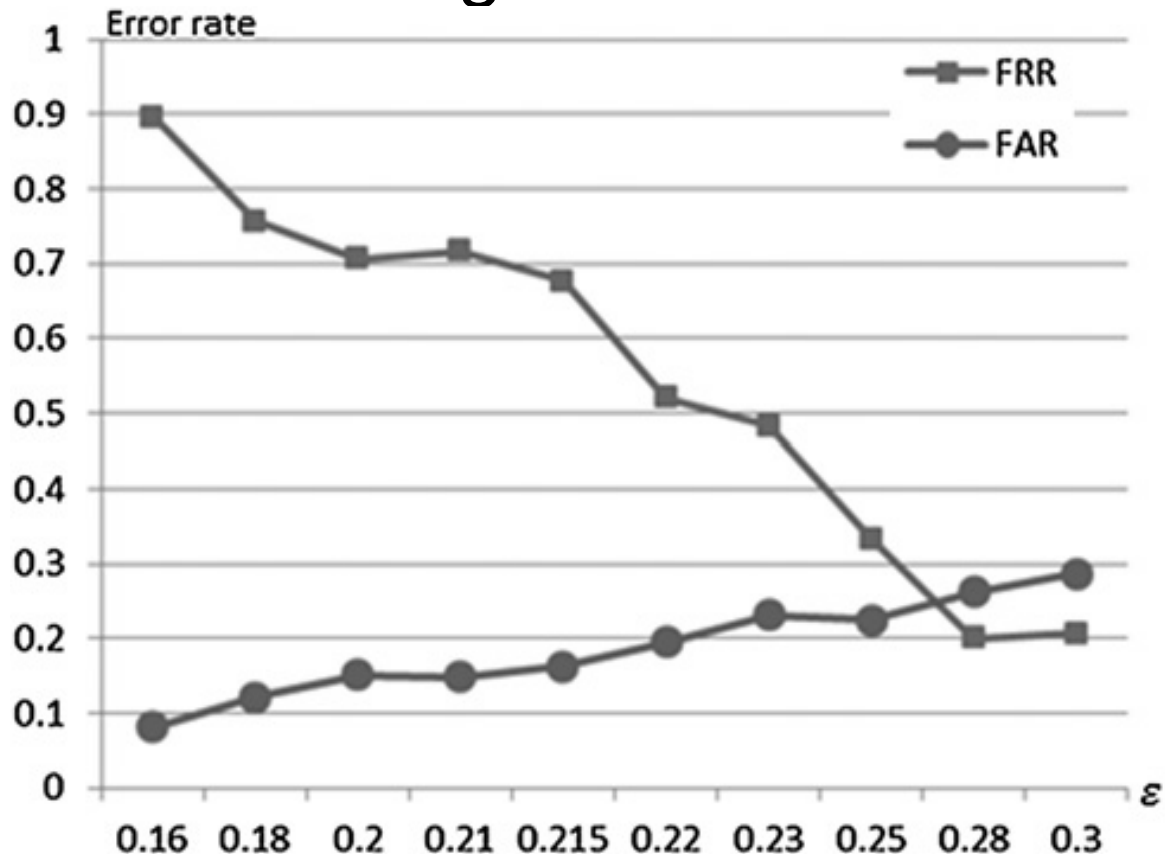
$Y' (y_1,\ldots, y_n)$: put to the vault → find candidate genius point → Recover the secret key

Evaluation

- The proposed scheme is tested with the Face94 database
  - In the training procedure, we used 100 images of 50 people, i.e. 2 images per person, to construct 40 eigenfaces. Then, we carried out the test with 152 people, including 50 people participated in the training process and 102 new people. Each person has 5 images in which 1 is used to create the vault and 4 are used to unlock the vault
- We measure the FAR (false accept rate), FRR (false reject rate) to this scheme

Evaluation

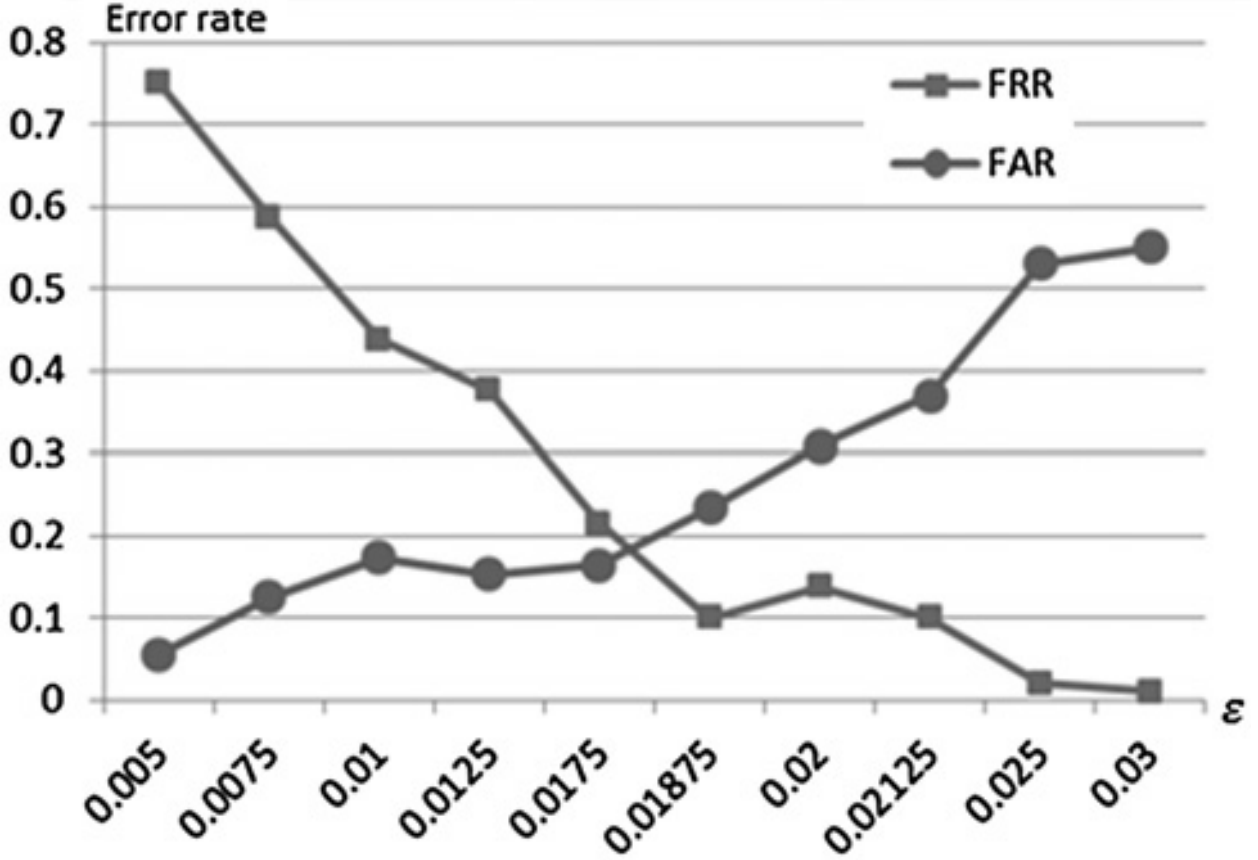
- FAR and FRR of original scheme:



The vertical axis is the error rate which is range [0, 1], and the horizontal axis is the minimum distance among points in the vault

Evaluation

- FAR and FRR of of the proposed scheme



Otherwise, using the new schema, we can get the better error rates FRR ≃ FAR < 0.2 at ε = 0.01875 with the capability of correcting up to four period errors

Conclusion

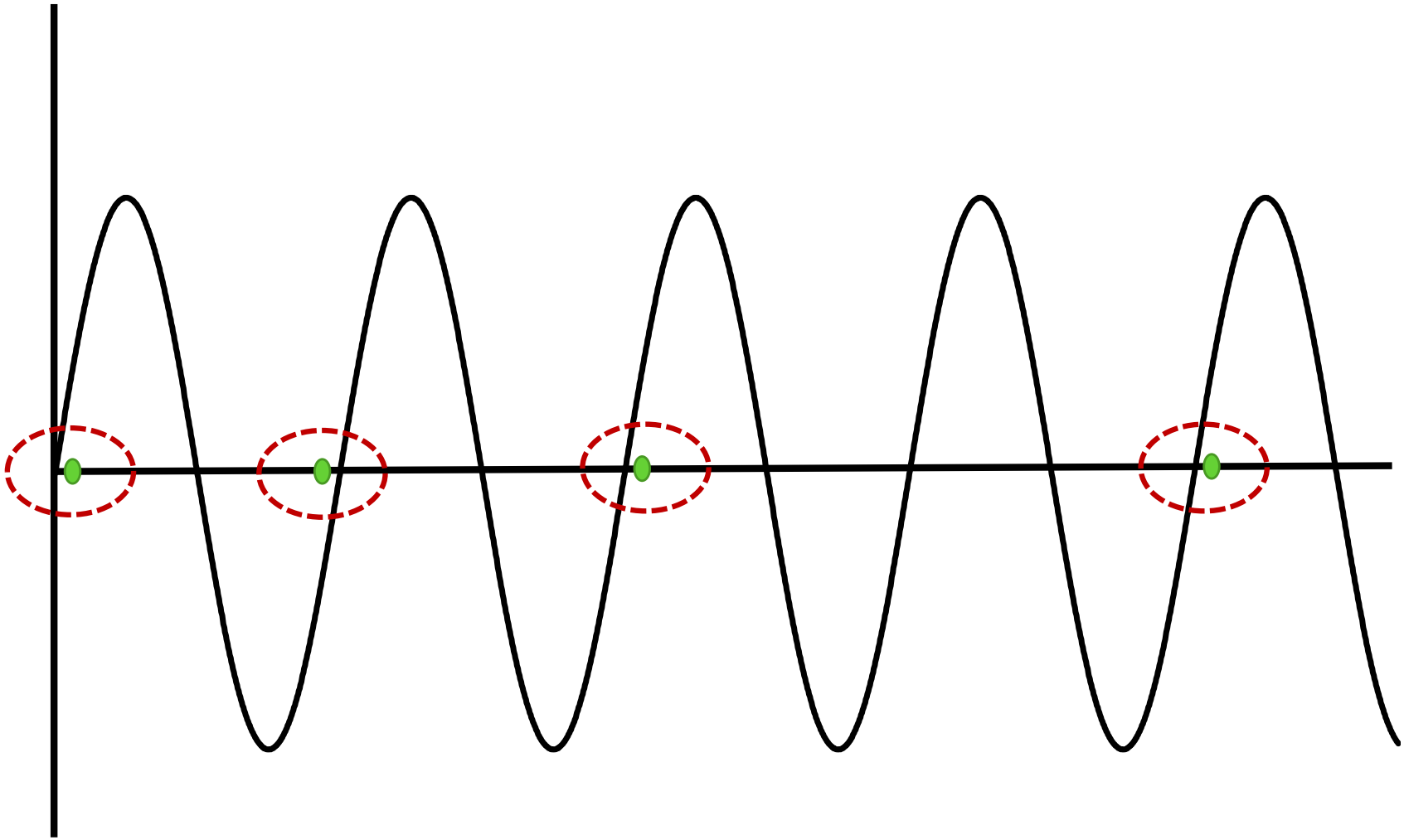
- Strengthen the fuzzy vault with the revocability property.
- The results of the evaluation confirm the effective and the practical properties of our scheme to protect biometric template.
- Future works:
  - reducing the error rates (FAR, FRR)
  - finding a proper way to add chaff points to the vault

Discussion

- Is there any exceptional biometric feature cannot be applied for this scheme? Propose solution to deal with that one?

- What are the advantages and disadvantages of the transformation function (sine transformation)?

Drawback



Discussion

1. Apply another periodic function
2. What are the advantages and disadvantages of the transformation function (sine transformation)?
   - ✓ Simple, O(M(n) log n), *n* refers to the number of digits of precision at which the function is to be evaluated. Due to the variety of multiplication algorithms, *M*(*n*) below stands in for the complexity of the chosen multiplication algorithm https://en.wikipedia.org/wiki/Computational_complexity_of_mathematical_operations
   - ✓ Weakness: do not keep the similarity of original features
   - ✓ Brute-force attack possibility?

Outline

- ~~Introduction~~
  - ~~Fuzzy vault issues~~
  - ~~A solution: transformation + fuzzy vault scheme~~
- ~~Cancelable fuzzy vault with periodic transformation for biometric template protection~~
  - ~~Cancellable biometrics: periodic transformation – SIN~~
  - ~~Hybrid approaches: cancellable biometrics + fuzzy vault scheme~~
- Reading:

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

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