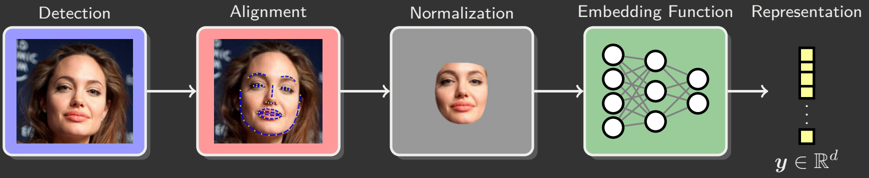
Secure Face Matching Using Fully Homomorphic Encryption

Vishnu Boddeti
Michigan State University

October 23rd, 2018

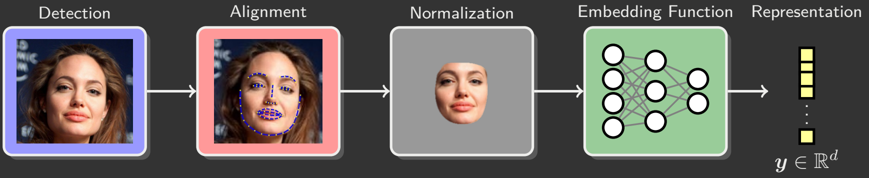
>>> Face Representation and Matching

* Face Representation:



Face Representation and Matching

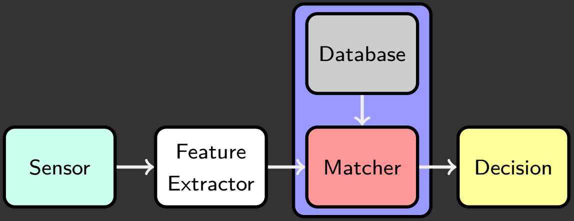
* Face Representation:



* Face Matching:

>>> Security Vulnerabilities

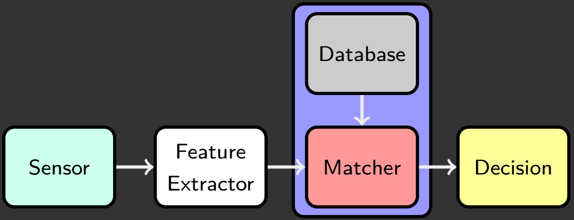
- Attacks on Biometric Systems:



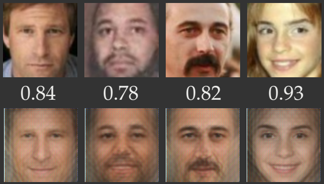
[1] Mai, Guangcan, Kai Cao, C. YUEN Pong, and Anil K. Jain. "On the Reconstruction of Face Images from Deep Face Templates." PAMI 2018

>>> Security Vulnerabilities

- Attacks on Biometric Systems:



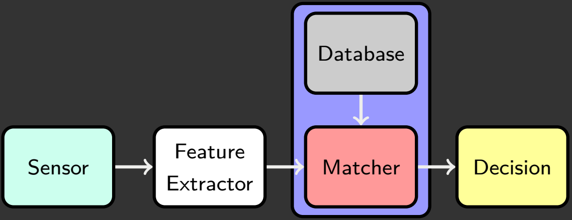
- Attacks on Templates:
  - Face reconstruction from template[1]



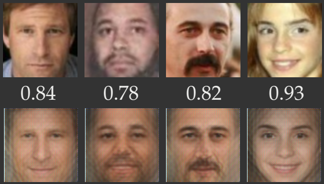
[1] Mai, Guangcan, Kai Cao, C. YUEN Pong, and Anil K. Jain. "On the Reconstruction of Face Images from Deep Face Templates." PAMI 2018

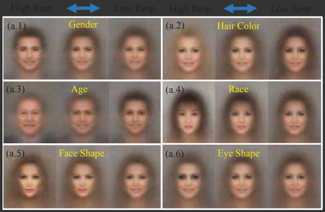
>>> Security Vulnerabilities

* Attacks on Biometric Systems:



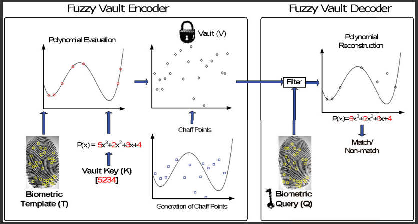
* Attacks on Templates:
  * Face reconstruction from template[1]
  * Privacy leakage through attribute prediction from template





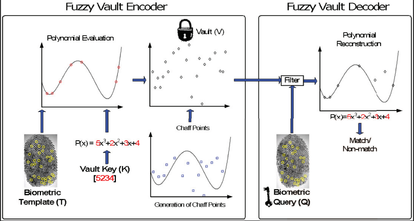
[1] Mai, Guangcan, Kai Cao, C. YUEN Pong, and Anil K. Jain. "On the Reconstruction of Face Images from Deep Face Templates." PAMI 2018

>>> Template Protection

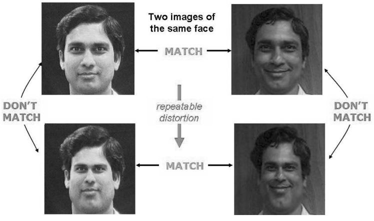


(a) Fuzzy Vault

>>> Template Protection

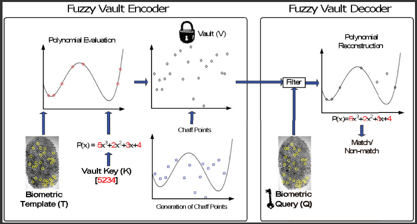


(a) Fuzzy Vault

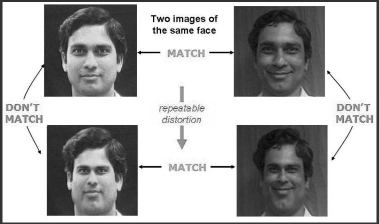


(b) Geometrical Transformations

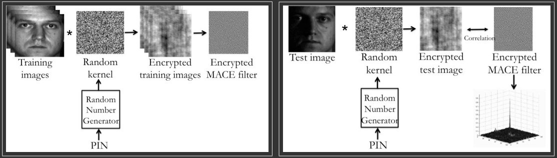
>>> Template Protection



(a) Fuzzy Vault

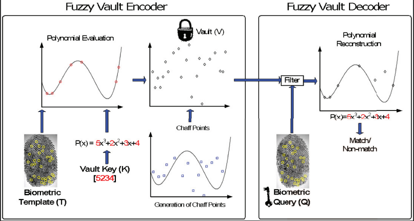


(b) Geometrical Transformations

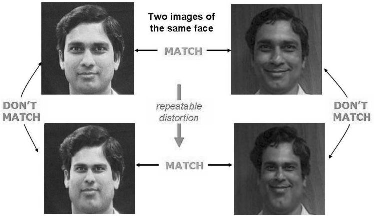


(c) Correlation with Random Masks

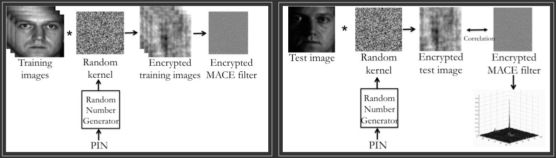
>>> Template Protection



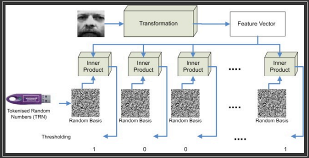
(a) Fuzzy Vault



(b) Geometrical Transformations

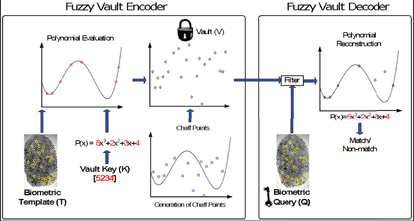


(c) Correlation with Random Masks

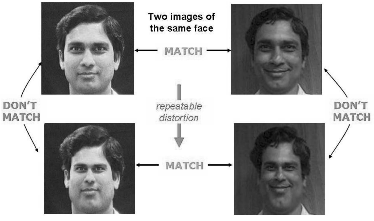


(d) Biohashing

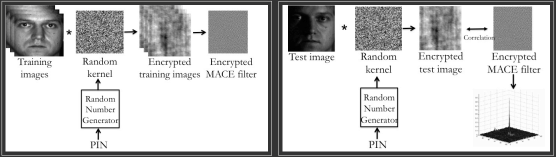
>>> Template Protection



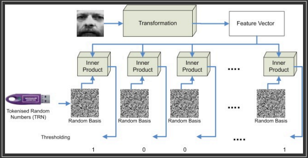
(a) Fuzzy Vault



(b) Geometrical Transformations



(c) Correlation with Random Masks



(d) Biohashing

* Drawback: Trade-Off matching performance for template security.

\>>> **Encryption: The Holy Grail?**

* Data encryption is an attractive option.

>>> Encryption: The Holy Grail?

* Data encryption is an attractive option.
    * protects user's privacy

\>>> **Encryption: The Holy Grail?**

* Data encryption is an attractive option.
    * protects user's privacy
    * enables free and open sharing

>>> Encryption: The Holy Grail?

* Data encryption is an attractive option.
    * protects user's privacy
    * enables free and open sharing
    * mitigate legal and ethical issues

>>> Encryption: The Holy Grail?

* Data encryption is an attractive option.
    * protects user's privacy
    * enables free and open sharing
    * mitigate legal and ethical issues
* Can we encrypt the biometric signatures?

>>> Encryption: The Holy Grail?

* Data encryption is an attractive option.
    * protects user's privacy
    * enables free and open sharing
    * mitigate legal and ethical issues
* Can we encrypt the biometric signatures?
* Can we perform biometric matching in the encryption domain?

>>> Encryption: The Holy Grail?

* Data encryption is an attractive option.
    * protects user's privacy
    * enables free and open sharing
    * mitigate legal and ethical issues
* Can we encrypt the biometric signatures?
* Can we perform biometric matching in the encryption domain?
* Can we maintain matching performance in the encrypted domain?

>>> Encryption: The Holy Grail?

* Data encryption is an attractive option.
    * protects user's privacy
    * enables free and open sharing
    * mitigate legal and ethical issues
* Can we encrypt the biometric signatures?
* Can we perform biometric matching in the encryption domain?
* Can we maintain matching performance in the encrypted domain?
* Encryption scheme needs to allow computations directly on the encrypted data.

>>> What is Homomorphic Encryption?

* Encryption that allows computations on ciphertext.

>>> What is Homomorphic Encryption?

* Encryption that allows computations on ciphertext.
* Partially Homomorphic Encryption: allows homomorphic additions or multiplications

>>> What is Homomorphic Encryption?

* Encryption that allows computations on ciphertext.
* Partially Homomorphic Encryption: allows homomorphic additions or multiplications
* Somewhat Homomorphic Encryption: allows limited number of homomorphic additions and multiplications

>>> What is Homomorphic Encryption?

* Encryption that allows computations on ciphertext.
* Partially Homomorphic Encryption: allows homomorphic additions or multiplications
* Somewhat Homomorphic Encryption: allows limited number of homomorphic additions and multiplications
* Fully Homomorphic Encryption: allows unlimited number of additions and multiplications

>>> What is Homomorphic Encryption?

* Encryption that allows computations on ciphertext.
* Partially Homomorphic Encryption: allows homomorphic additions or multiplications
* Somewhat Homomorphic Encryption: allows limited number of homomorphic additions and multiplications
* Fully Homomorphic Encryption: allows unlimited number of additions and multiplications

This Paper Explores:

>>> What is Homomorphic Encryption?

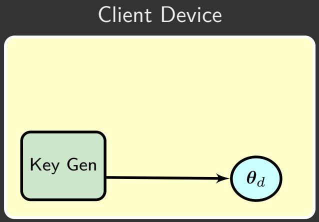
* Encryption that allows computations on ciphertext.
* Partially Homomorphic Encryption: allows homomorphic additions or multiplications
* Somewhat Homomorphic Encryption: allows limited number of homomorphic additions and multiplications
* Fully Homomorphic Encryption: allows unlimited number of additions and multiplications

This Paper Explores:

* feasibility of fully homomorphic encryption for secure face matching.
* efficiency of fully homomorphic encryption for secure face matching.

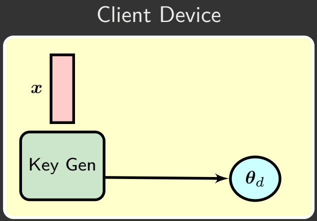
>>> Enrollment Protocol

- Client device:
  - generates cryptographic keys



>>> Enrollment Protocol

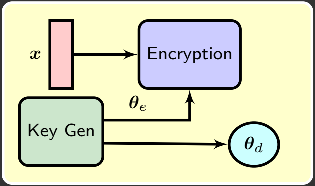
* Client device:
  * generates cryptographic keys
  * captures biometric signature + extracts feature



>>> Enrollment Protocol

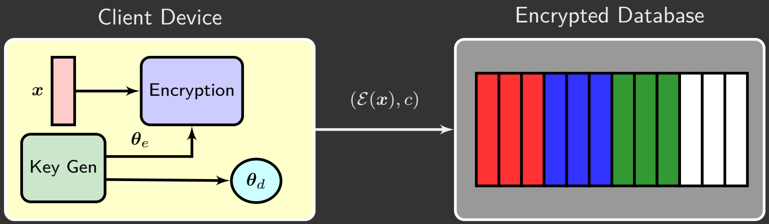
- Client device:
  - generates cryptographic keys
  - captures biometric signature + extracts feature
  - encrypts feature

Client Device



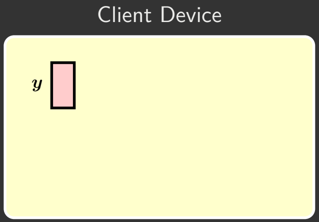
>>> Enrollment Protocol

* Client device:
  * generates cryptographic keys
  * captures biometric signature + extracts feature
  * encrypts feature
  * transmits encrypted feature + identity label to remote database



>>> Authentication Protocol

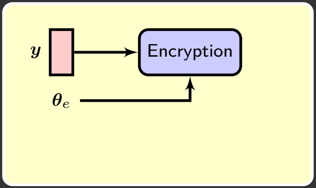
* Client device:
    * captures biometric signature + extracts feature



>>> Authentication Protocol

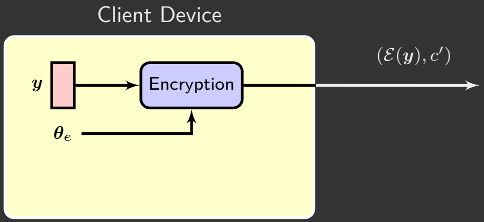
* Client device:
  * captures biometric signature + extracts feature
  * encrypts feature

Client Device



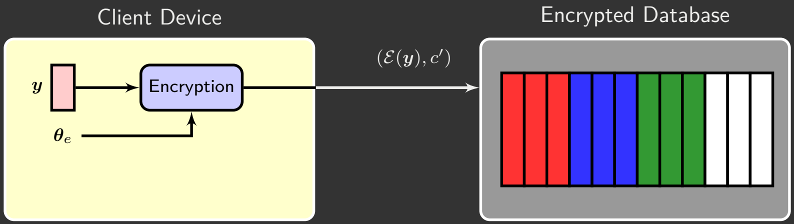
>>> Authentication Protocol

* Client device:
    * captures biometric signature + extracts feature
    * encrypts feature
    * transmits encrypted feature + claimed identity label to remote database



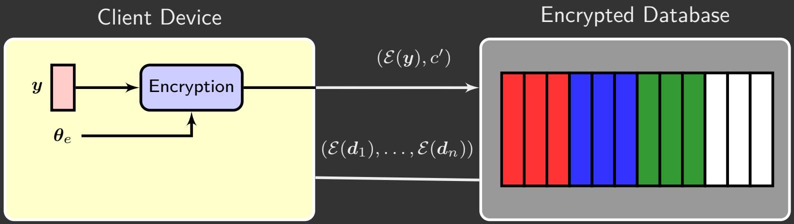
>>> Authentication Protocol

* Client device:
  * captures biometric signature + extracts feature
  * encrypts feature
  * transmits encrypted feature + claimed identity label to remote database
* Remote Database:
  * homomorphic inner product between encrypted probe and gallery



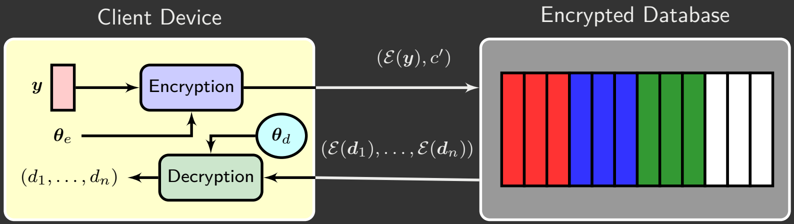
>>> Authentication Protocol

* Client device:
  * captures biometric signature + extracts feature
  * encrypts feature
  * transmits encrypted feature + claimed identity label to remote database
* Remote Database:
  * homomorphic inner product between encrypted probe and gallery
  * transmits encrypted scores to client



>>> Authentication Protocol

* Client device:
  * captures biometric signature + extracts feature
  * encrypts feature
  * transmits encrypted feature + claimed identity label to remote database
* Remote Database:
  * homomorphic inner product between encrypted probe and gallery
  * transmits encrypted scores to client
* Client device:
  * decrypts received scores and makes decision



>>> Homomorphic Inner Products

* Feature Matching:

$$\begin{aligned} \text{Euclidean Distance: } d(\boldsymbol{x}, \boldsymbol{y}) &= \|\boldsymbol{x} - \boldsymbol{y}\|_2^2 = \boldsymbol{x}^T\boldsymbol{x} + \boldsymbol{y}^T\boldsymbol{y} - 2\boldsymbol{x}^T\boldsymbol{y} \\ \text{Cosine Similarity: } s(\boldsymbol{x}, \boldsymbol{y}) &= \frac{\boldsymbol{x}^T\boldsymbol{y}}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} \end{aligned}$$

>>> Homomorphic Inner Products

* Feature Matching:

$$\begin{aligned} \text{Euclidean Distance: } d(\boldsymbol{x}, \boldsymbol{y}) &= \|\boldsymbol{x} - \boldsymbol{y}\|_2^2 = \boldsymbol{x}^T\boldsymbol{x} + \boldsymbol{y}^T\boldsymbol{y} - 2\boldsymbol{x}^T\boldsymbol{y} \\ \text{Cosine Similarity: } s(\boldsymbol{x}, \boldsymbol{y}) &= \frac{\boldsymbol{x}^T\boldsymbol{y}}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} \end{aligned}$$

* Inner Product:

$$\boldsymbol{x}^T\boldsymbol{y} = \sum_{i=1}^{d} x_i y_i$$

>>> Homomorphic Inner Products

* Feature Matching:

$$\begin{aligned}\text{Euclidean Distance: } d(\boldsymbol{x},\boldsymbol{y}) &= \|\boldsymbol{x}-\boldsymbol{y}\|_2^2 = \boldsymbol{x}^T\boldsymbol{x} + \boldsymbol{y}^T\boldsymbol{y} - 2\boldsymbol{x}^T\boldsymbol{y} \\ \text{Cosine Similarity: } s(\boldsymbol{x},\boldsymbol{y}) &= \frac{\boldsymbol{x}^T\boldsymbol{y}}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|}\end{aligned}$$

* Inner Product:

$$\boldsymbol{x}^T\boldsymbol{y} = \sum_{i=1}^{d} x_i y_i$$

* Homomorphic Inner Product:

$$s(\boldsymbol{x},\boldsymbol{y}) = \mathcal{D}\left(\sum_{i=1}^{d} \mathcal{E}(x_i,\boldsymbol{\theta}_e)\mathcal{E}(y_i,\boldsymbol{\theta}_e), \boldsymbol{\theta}_d\right)$$

>>> Batching: Amortized Homomorphic Inner Product

* Inner Product: d homomorphic multiplications + $d-1$ homomorphic additions

>>> Batching: Amortized Homomorphic Inner Product

* Inner Product: d homomorphic multiplications $+\ d-1$ homomorphic additions
* Complexity: homomorphic multiplication $>>>$ homomorphic addition

>>> Batching: Amortized Homomorphic Inner Product

* Inner Product: d homomorphic multiplications $+$ $d - 1$ homomorphic additions
* Complexity: homomorphic multiplication $>>>$ homomorphic addition
* Batching Inner Product: 1 homomorphic multiplications $+$ $log_2(d)$ homomorphic additions

>>> Batching: Amortized Homomorphic Inner Product

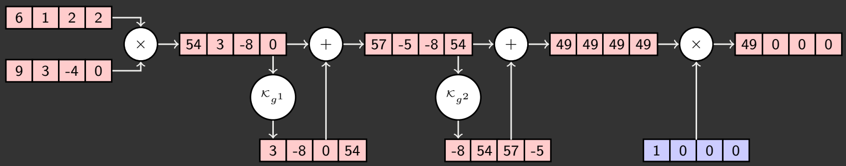
* Inner Product: d homomorphic multiplications $+\ d - 1$ homomorphic additions
* Complexity: homomorphic multiplication $>>>$ homomorphic addition
* Batching Inner Product: 1 homomorphic multiplications $+\ log_2(d)$ homomorphic additions
* Template Size: batching size $<<<$ no batching size

>>> Batching: Amortized Homomorphic Inner Product

* Inner Product: d homomorphic multiplications $+ d - 1$ homomorphic additions
* Complexity: homomorphic multiplication $>>>$ homomorphic addition
* Batching Inner Product: 1 homomorphic multiplications $+ log_2(d)$ homomorphic additions
* Template Size: batching size $<<<$ no batching size
* Key Idea: amortized inner product

>>> Batching: Amortized Homomorphic Inner Product

* Inner Product: d homomorphic multiplications + $d-1$ homomorphic additions
* Complexity: homomorphic multiplication $>>>$ homomorphic addition
* Batching Inner Product: 1 homomorphic multiplications + $log_2(d)$ homomorphic additions
* Template Size: batching size $<<<$ no batching size
* Key Idea: amortized inner product
  * Encode entire vector at once + repetitive circular shift and addition



>>> Experimental Setup

* **Datasets:** LFW, IJB-A, IJB-B and CASIA

* **Models:** FaceNet (128-D) and SphereFace (512-D)

* **Evaluation:** True Accept Rate 0.01%, 0.1% and 1% FAR

* **Options:** different quantization, security levels, dimensionality of features

>>> Computational Complexity

* Pairwise Matching Time
  * Homomorphic Encryption
  * Homomorphic Matching
  * Homomorphic Decryption
* Template Size
  * Database storage size
  * Communicating encrypted templates

>>> Computational Complexity

* Pairwise Matching Time
  * Homomorphic Encryption
  * Homomorphic Matching
  * Homomorphic Decryption
* Template Size
  * Database storage size
  * Communicating encrypted templates

Table: Matching Time and Template Memory

Security in bits (λ)	Dim (d)	No FHE Time (μs)	No FHE Mem (KB)	No Batching Time (ms) Enc	No Batching Time (ms) Score	No Batching Time (ms) Dec	No Batching Time (ms) Total	No Batching Mem (MB)	Batching Time (ms) Enc	Batching Time (ms) Score	Batching Time (ms) Dec	Batching Time (ms) Total	Batching Mem (KB)
	64	0.44	2.0										
	128	0.89	4.0										
	512	3.48	16.0										
	1024	7.49	32.0										

>>> Computational Complexity

* Pairwise Matching Time
  * Homomorphic Encryption
  * Homomorphic Matching
  * Homomorphic Decryption
* Template Size
  * Database storage size
  * Communicating encrypted templates

Table: Matching Time and Template Memory

Security in bits (λ)	Dim (d)	No FHE Time (μs)	No FHE Mem (KB)	No Batching Time (ms) Enc	Score	Dec	Total	No Batching Mem (MB)	Batching Time (ms) Enc	Score	Dec	Total	Batching Mem (KB)
	64	0.44	2.0	4.40	5.25	0.01	9.66	0.25					
	128	0.89	4.0	17.57	21.05	0.02	38.64	1.0					
128	512	3.48	16.0	280.19	343.81	0.08	624.07	16.5					
	1024	7.49	32.0	2214.88	2924.75	0.33	5139.97	131.0					

>>> Computational Complexity

* Pairwise Matching Time
    * Homomorphic Encryption
    * Homomorphic Matching
    * Homomorphic Decryption
* Template Size
    * Database storage size
    * Communicating encrypted templates

Table: Matching Time and Template Memory

Security in bits (λ)	Dim (d)	No FHE Time (μs)	No FHE Mem (KB)	No Batching Time (ms) Enc	Score	Dec	Total	No Batching Mem (MB)	Batching Time (ms) Enc	Score	Dec	Total	Batching Mem (KB)
	64	0.44	2.0	4.40	5.25	0.01	9.66	0.25	0.07	0.17	0.01	0.25	2.0
	128	0.89	4.0	17.57	21.05	0.02	38.64	1.0	0.14	0.38	0.02	0.59	4.0
128	512	3.48	16.0	280.19	343.81	0.08	624.07	16.5	0.58	1.80	0.07	2.45	16.0
	1024	7.49	32.0	2214.88	2924.75	0.33	5139.97	131.0	2.27	8.36	0.30	11.42	32.0

>>> Homomorphic Matching Performance

* Face verification: different quantization levels

Table: Face Recognition Accuracy (TAR @ FAR in %)

Dataset	Method	128-D FaceNet			512-D SphereFace		
		0.01%	0.1%	1%	0.01%	0.1%	1%
IJB-B	No FHE	25.77	48.31	74.47	7.86	31.27	69.83
	FHE (2.5×10^{-3})	25.78	48.28	74.46	7.86	31.27	69.82
	FHE (1.0×10^{-2})	25.71	48.31	74.44	7.80	31.29	69.75
	FHE (1.0×10^{-1})	23.75	46.08	72.87	7.49	30.92	67.45

>>> Take Home Message

* Facial template security is of growing importance.

>>> Take Home Message

* Facial template security is of growing importance.

* Fully homomorphic face matching in encrypted domain is feasible and practical.

>>> Take Home Message

* Facial template security is of growing importance.
* Fully homomorphic face matching in encrypted domain is feasible and practical.
* What next?

>>> Take Home Message

* Facial template security is of growing importance.

* Fully homomorphic face matching in encrypted domain is feasible and practical.

* What next?
    * Limitation: score thresholding is performed after decryption
    * Consequence: hill climbing attack is still possible from decrypted score

>>> Take Home Message

* Facial template security is of growing importance.

* Fully homomorphic face matching in encrypted domain is feasible and practical.

* What next?
    * Limitation: score thresholding is performed after decryption
    * Consequence: hill climbing attack is still possible from decrypted score
    * Limitation: encryption and decryption key are on client device
    * Consequence: key management on client device is the weakest link