# CryptoFace: End-to-End Encrypted Face Recognition

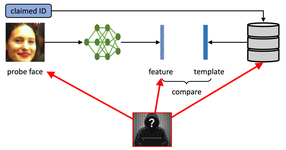
Wei Ao
Vishnu Boddeti

## Motivation: *face identity is at risk*

**Face recognition integrates into daily practical applications.**

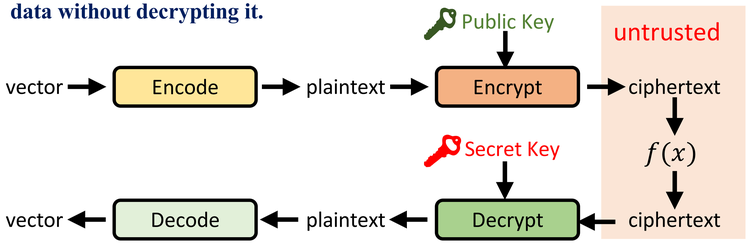
Mobile Financial Customs

**Face recognition systems are vulnerable to identity theft.**




## FHE: *computation over encrypted data*

**Fully homomorphic encryption (FHE) allows computation over encrypted data without decrypting it.**

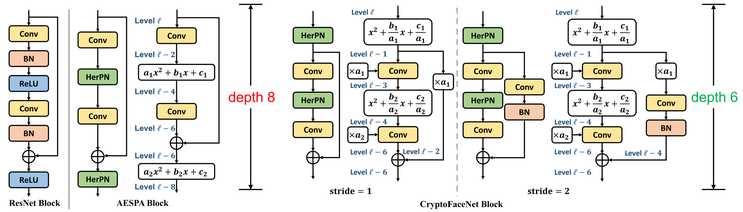



**FHE supports polynomials with the limited number of multiplications.**

$f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_d x^d$ ➡ depth $= \lceil \log_2(d+1) \rceil$ multiplications

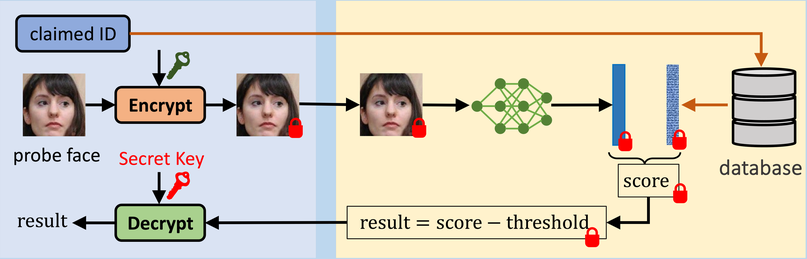
**FHE uses bootstrapping to refresh ciphertext to extend multiplication capacity.** ➡ **computationally expensive memory intensive**

## CryptoFaceNet: *depth-optimal* CNNs

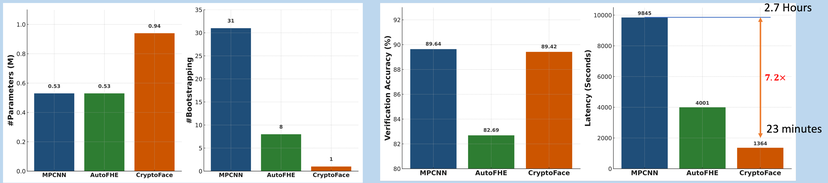



# We encrypt face images to provide **biometric** and **database security**

**CryptoFace is the first secure face recognition across all stages from feature extraction to storage and matching.**



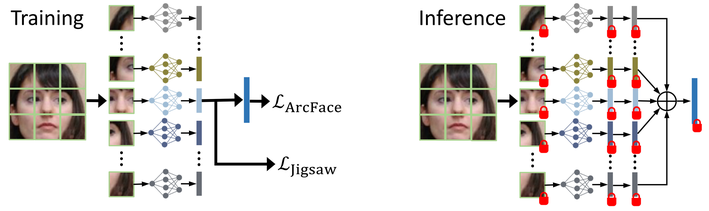

**CryptoFace reduces bootstrapping operations, speeds up inference and improves verification accuracy.**




**CryptoFace is scalable to high resolution and achieves near-resolution-independent latency.**

## CryptoFaceNet: *aggregation & parallelism*

**CryptoFaceNet is a mixture of patch CNNs with a small depth under FHE.**



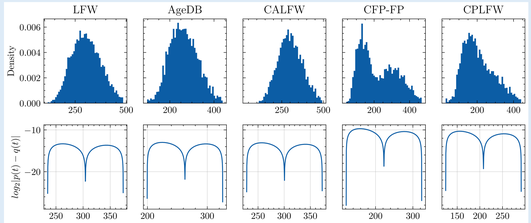

▷ Jigsaw auxiliary task helps to learn position information.

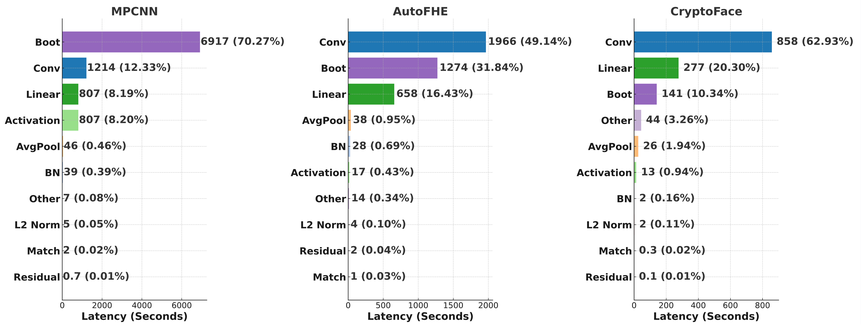
▷ Mixture of patch CNNs can be evaluated in parallel under FHE.

**Non-linear similarity measure is approximated by a distribution-aware polynomial.**

$$\cos(\theta) = \frac{xy}{\|x\|\|y\|}, \quad L2 = \left\| \frac{x}{\|x\|} - \frac{y}{\|y\|} \right\| \quad \Big\} \; q(t) = \frac{1}{\sqrt{t}}$$

$$p(t) = \beta_2 t^2 + \beta_1 t + \beta_0$$




## Benchmark under SEAL FHE

**CryptoFace reduces bootstrapping operations and convolutional layers to speed up face recognition inference under FHE.**