SAMSUNG SDS

Foresee

Techtonic 2021

Partner

Disrupt

얼굴 인식용 Fuzzy Extractor 활용한 안전한 사용자 인증 기법

김진수

Contents

- Motivation

- Fuzzy Extractor

- Problem to be Solved

- Our Solution

- Performance Comparison

Motivations

ID/PW: What you know

Decryption Key: What you have

Biometrics: Who you are

Cloud environment may cause serious privacy concerns

- Celebrity's private image leakage
- ID/PW-based access control

Private cloud using data encryption/decryption

- Risk in cryptographic key management
- Server: Secret key protection
  Client: Device loss and hard to applicable to MDE

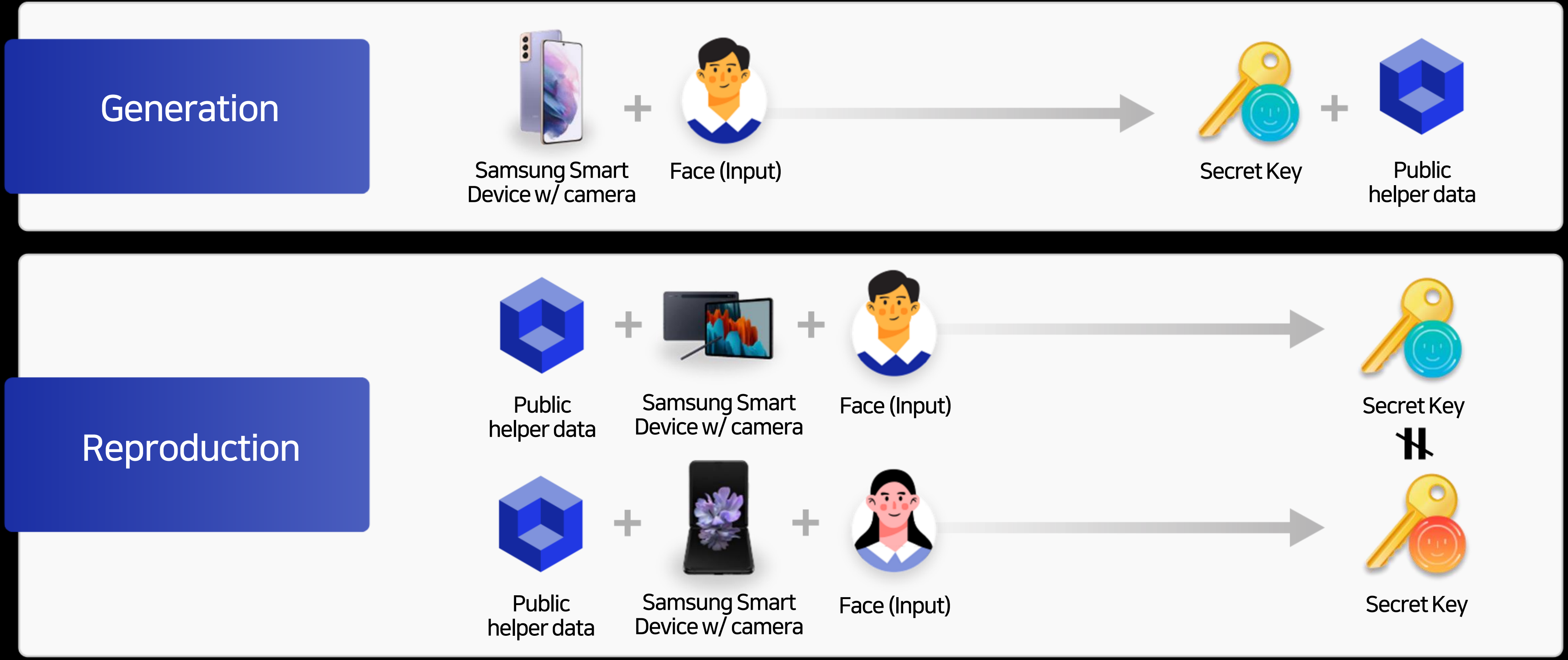
A new solution of data privacy protection in MDE environment

- Real-value based Error Correcting Code
- Fuzzy extractor for biometric-based data encryption

MDE: Multi-Device Environment

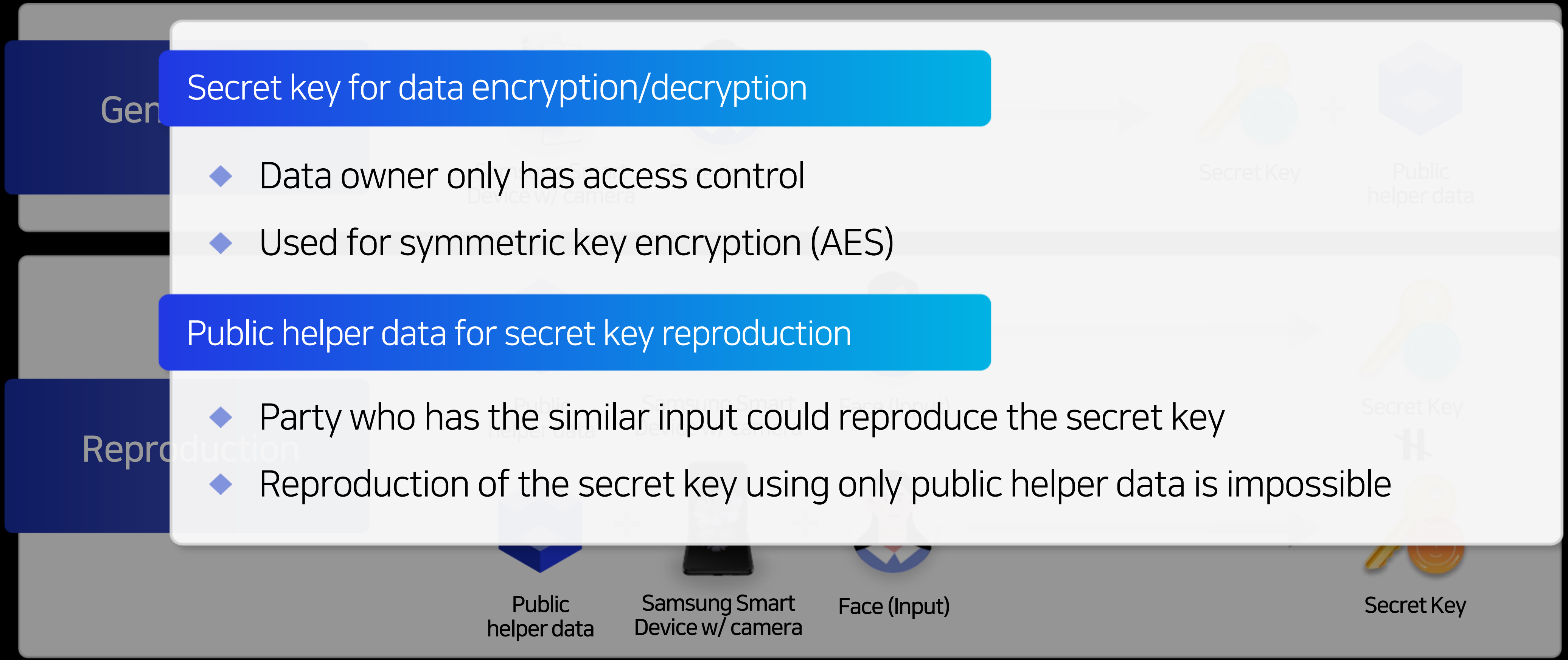
Fuzzy Extractor | Concept

- "FuzzyExtractor" outputs the same secret key even though inputs have certain noise
- "FuzzyExtractor" does not store inputs/secret key anywhere



Fuzzy Extractor | Concept

- "FuzzyExtractor" outputs the same secret key even though inputs have certain noise
- "FuzzyExtractor" does not store inputs/secret key anywhere



Secret key for data encryption/decryption

- Data owner only has access control
- Used for symmetric key encryption (AES)

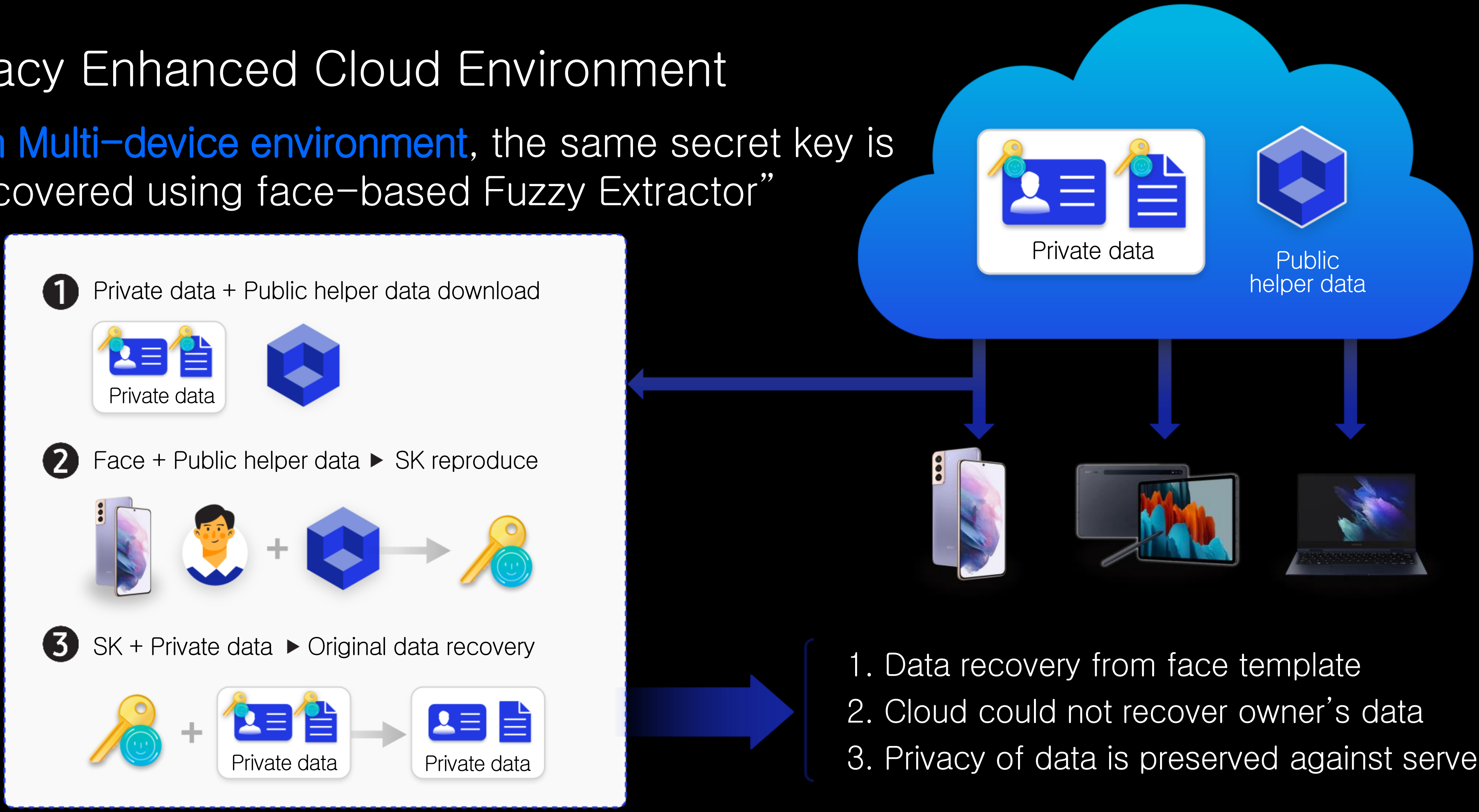
Public helper data for secret key reproduction

- Party who has the similar input could reproduce the secret key
- Reproduction of the secret key using only public helper data is impossible

Fuzzy Extractor | Application

Privacy Enhanced Cloud Environment

- “In Multi-device environment, the same secret key is recovered using face-based Fuzzy Extractor”



❶ Private data + Public helper data download

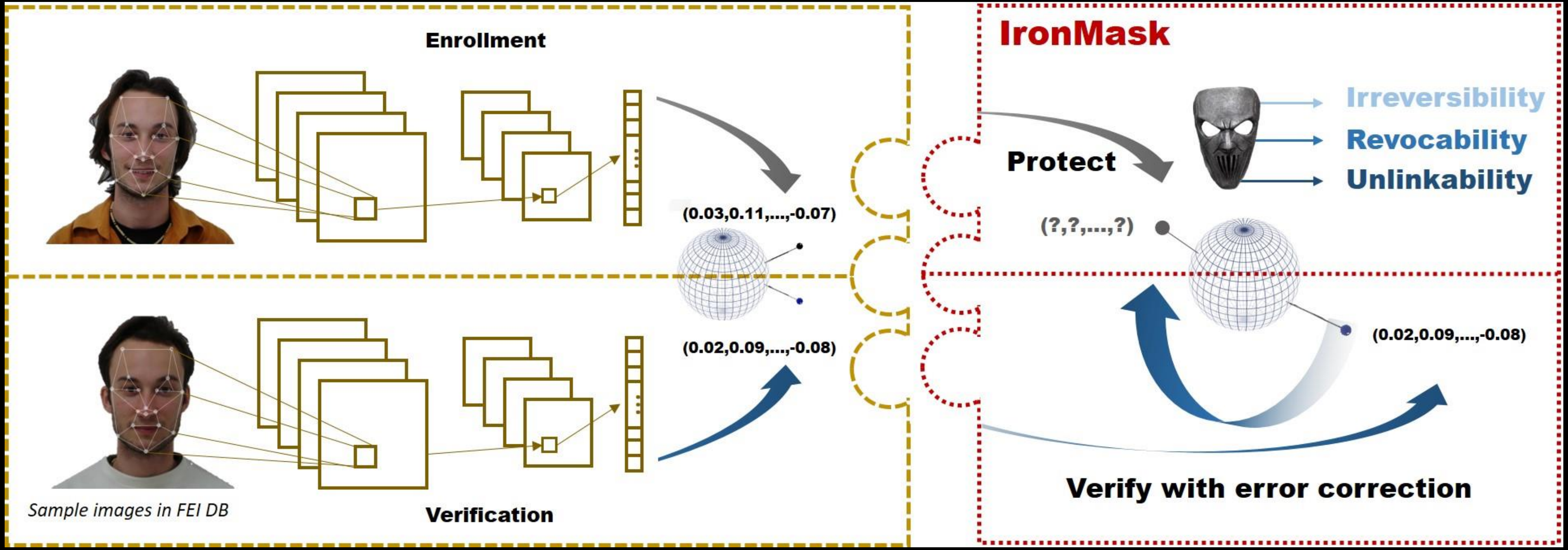
❷ Face + Public helper data ▶ SK reproduce

❸ SK + Private data ▶ Original data recovery

1. Data recovery from face template
2. Cloud could not recover owner’s data
3. Privacy of data is preserved against server hacking

Problem to be Solved | Face Authentication

Deep Learning based Face Authentication



Problem to be Solved | Face Authentication

Security Requirements

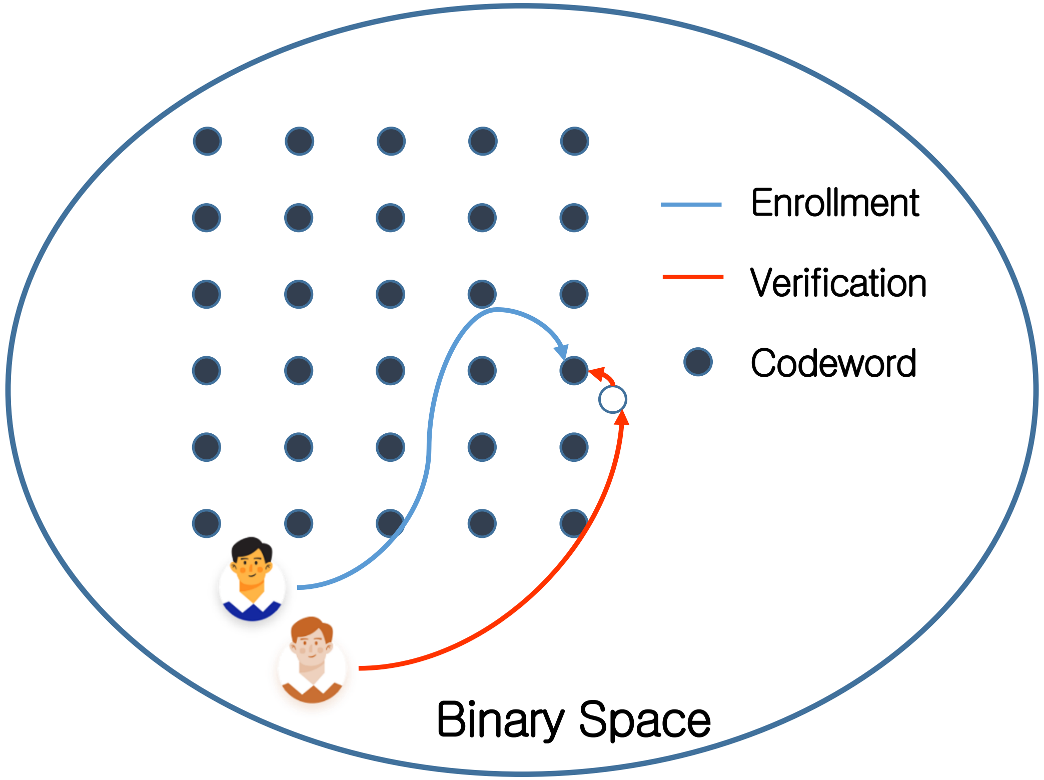
- Irreversibility: It is computationally infeasible to recover original biometric data from the protected template.
- Revocability: It is possible to issue new protected templates to replace the compromised one.
- Unlinkability: It is computationally infeasible to retrieve any information from protected templates generated in two different applications.

Problem to be Solved | Error Correction Code

Binary Error Correction Code

Binary Error Correction Code

- Controlling error in binary data over unreliable or noisy comm. channel
- Reed-Solomon Code, Hamming Code etc.



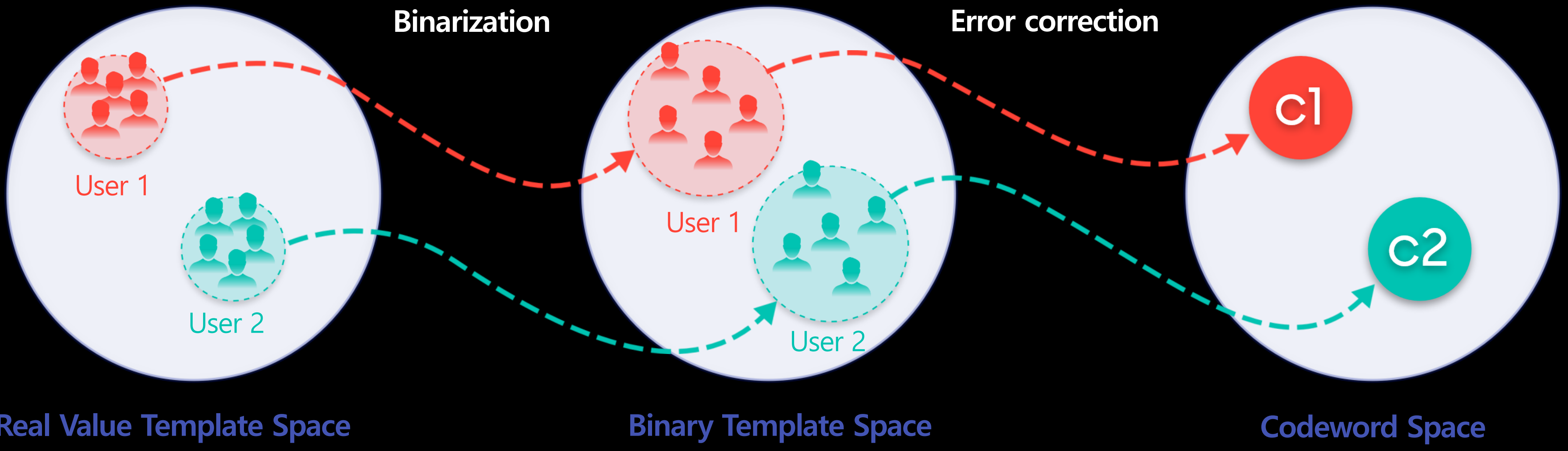
Problem to be Solved | Previous Approach

How to control noisy in face template?

- Applying an error correction code approach
- Binarizing face templates of real value vector

Error correction code approach

- Controlling error in binary data over unreliable or noisy comm. channel
- Reed-Solomon, BCH, Hamming codes etc.



Problem to be Solved | Previous Approach

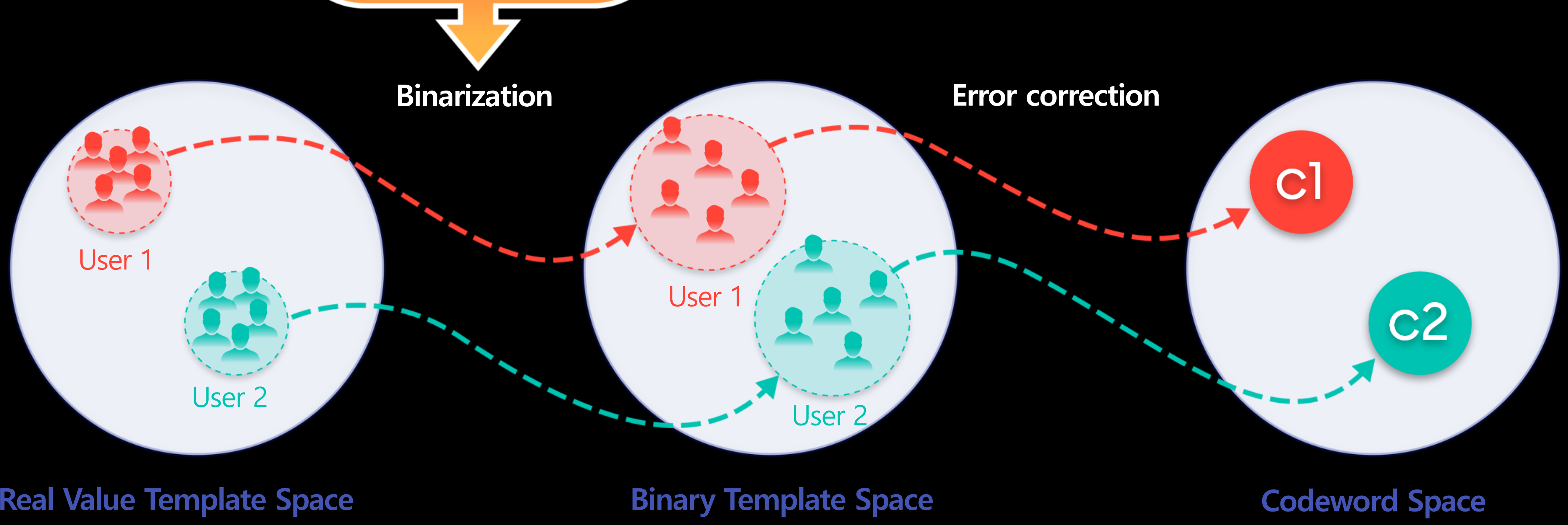
How to control noisy in face template?

- Applying an error corre
- Binarizing face templat

Accuracy Degradation

Error correction code approach

- Controlling error in binary data over unreliable or noisy comm. channel
- Reed-Solomon, BCH, Hamming codes etc.



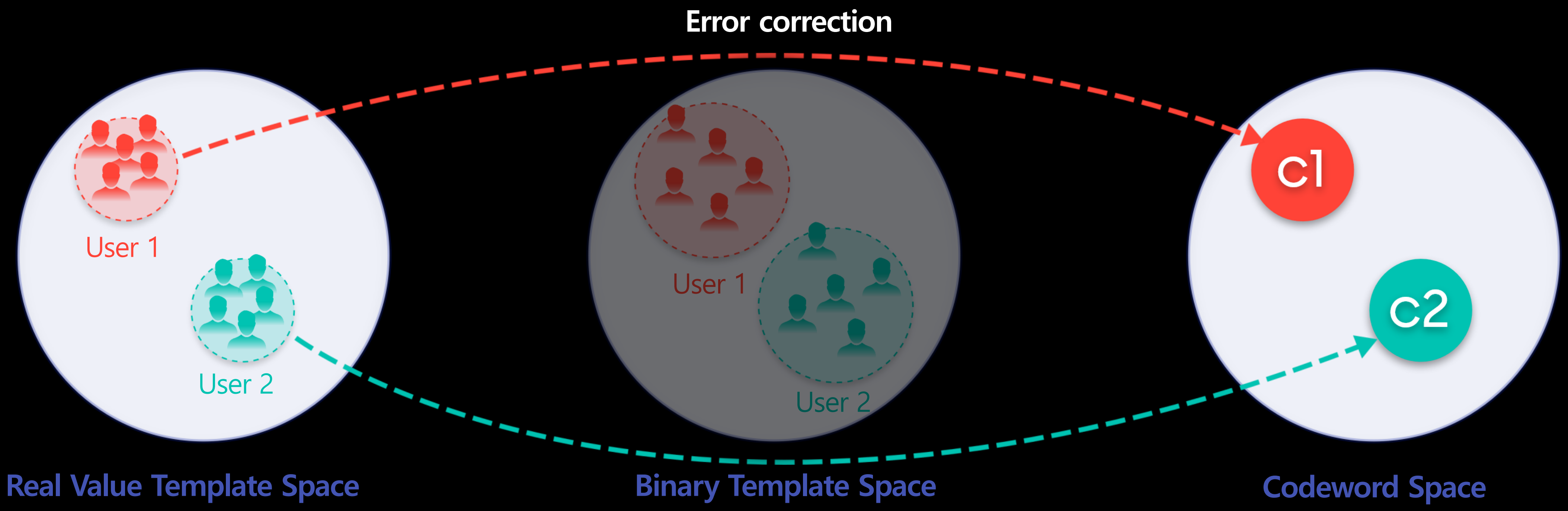
Problem to be Solved | Previous Approach

How to control noisy in face template?

- Applying an error correction code approach
- Binarizing face templates of real value vector

Error correction code approach

- Controlling error in binary data over unreliable or noisy comm. channel
- Reed-Solomon, BCH, Hamming codes etc.



Our Solution | A New Error Correcting Code

Goal

- Design a ECC for hypersphere S^n with the cosine similarity metric

Requirement

- Exponentially many codewords
- Spread the distance between all codewords above a certain level
- Efficient decoding method (finding closest codeword)

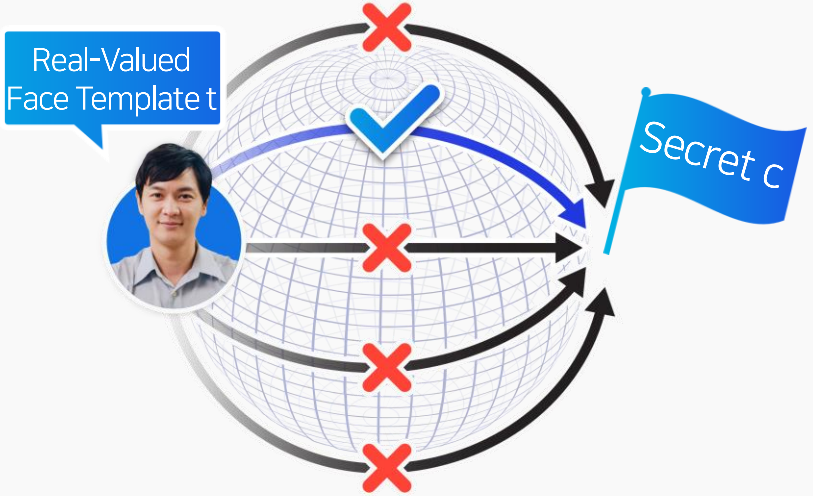
Strategy

- Specific codeword generation

e.g., $\mathcal{C}_1$ over $S^4 = \{(\pm1,0,0,0), (0,\pm1,0,0), (0,0,\pm1,0), (0,0,0,\pm1)\}$

$\mathcal{C}_2$ over $S^4 = \{(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0), (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}, 0), \cdots, (0, 0, -\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})\}$

- Hidden rotation matrix generation



Performance Comparison

Experimental results

- Face recognition: ArcFace (State-of-the-Art)
- Results: Smaller degradation compared to previous works

Dataset	Algorithm	Enrollment Type	Output Type	TAR@FAR
CMU Multi-PIE	[TVN19]	Zero-shot	Binary 255	81.40@1e-2
			Binary 1023	81.20@1e-2
	Ours	Zero-shot	Real 512	98.95@0
		Zero-shot & Center	Real 512	99.96@1.3e-3
FEI	[JCJ19]	One-shot	Binary 256	99.73@0
			Binary 1024	99.85@0
		Multi-Shot	Binary 256	99.84@0
			Binary 1024	99.98@0
	Ours	Zero-shot	Real 512	99.27@0
		Zero-shot & Center	Real 512	99.96@3e-4
Color-Feret	[JCJ19]	One-shot	Binary 256	98.31@0
			Binary 1024	99.13@0
		Multi-Shot	Binary 256	98.69@0
			Binary 1024	99.24@0
	Ours	Zero-shot	Real 512	98.06@0
		Zero-shot & Center	Real 512	99.46@0

[JCJ19] Securing Face Templates using Deep Convolutional Neural Network and Random Projection
[TVN19] Zero-Shot Deep Hashing and Neural Network Based Error Correction for Face Template Protection

Thank you