PHILIPS

sense and simplicity

A quantitative analysis of indistinguishability for a continuous source biometric cryptosystem

I. Buhan-Dulman, J. Breebaart, Jorge Guajardo, K. Groet, E. Kelkboom, T. Akkermans

DPM workshop – *Saint Malo* - September 2009

PHILIPS

OVERVIEW

- Biometric authentication system;
- Authentication with protected templates
- QIM fuzzy embedder;
- Cross-matching scenario;
- Classification function used by the adversary;
- Quantitative measures for indistinguishability:
  - advantage of an adversary
  - cross-matching fingerprints from MCYT fingerprint database

- Conclusions

PHILIPS

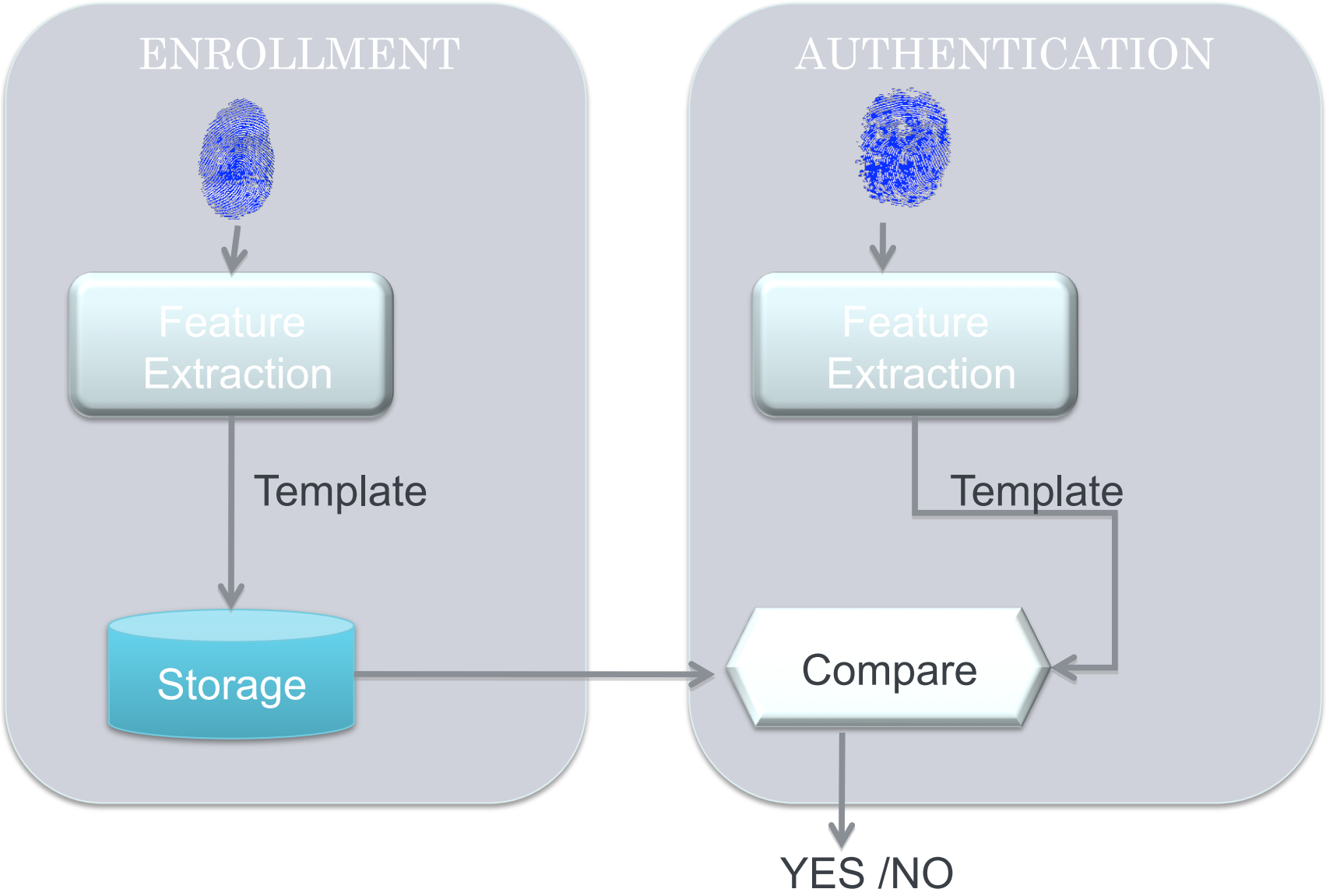
MOTIVATION

- Biometrics is CONVENIENT method for authentication
- LINKED to a person;

- APPLICATIONS:
  - Border control (passport, visa, ID, drivers license)
  - Crime prevention (social security fraud)
  - Ticketing applications
  - Payment systems
  - Access control
  - Forensics
  - Watch lists

PHILIPS

TRADITIONAL BIOMETRIC SYSTEM



PHILIPS

TEMPLATE PROTECTION

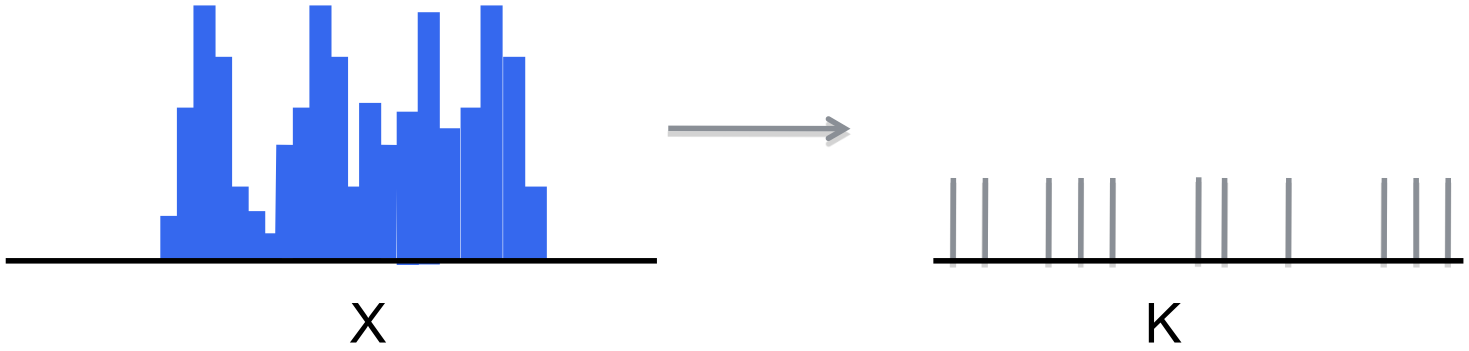
- WHY:
  1. Identity theft;
  2. Cross matching;
  3. Not renewable;
  4. Reveal medical information;
  5. Legislation;

- A TEMPLATE PROTECTION SYSTEM:
  1. Protects the stored reference information (the template)
  2. Performs authentication is protected domain
  3. A system that gives the state of the art performance;

PHILIPS

FUZZY SKETCH

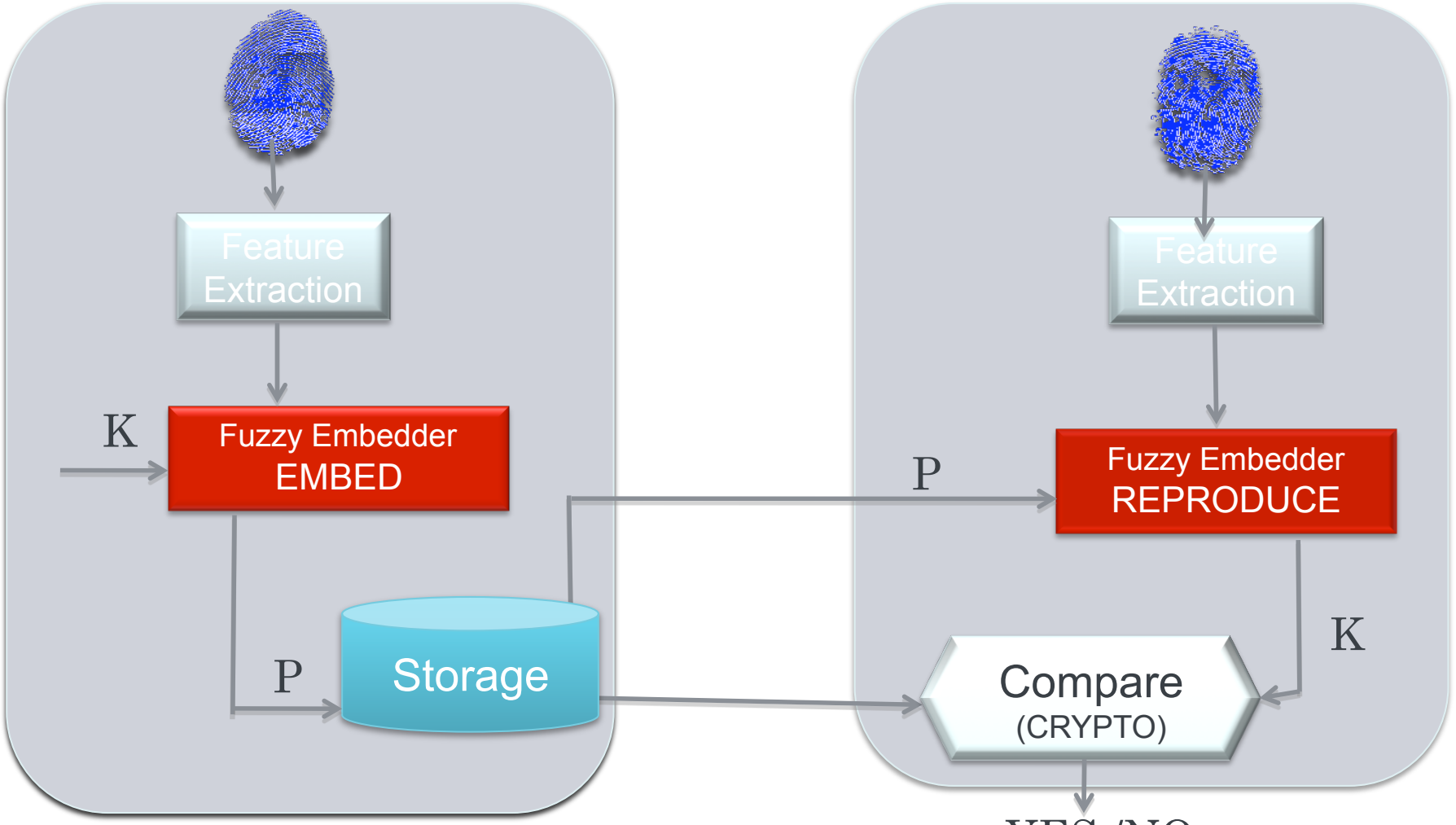
A theoretical TEMPLATE PROTECTION SYSTEM:



- Transforms noisy, non-uniform data into reproducible, uniform binary sequences;
- Their properties are well understood

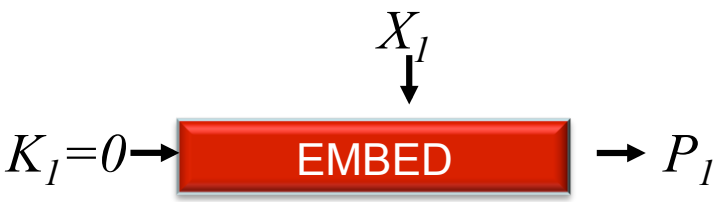
PHILIPS

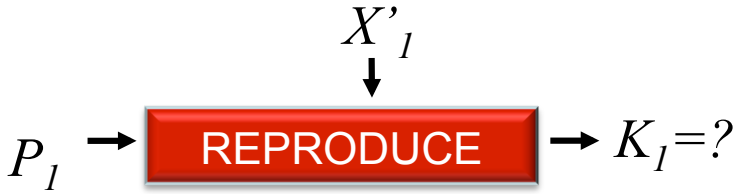
BIOMETRIC TEMPLATE PROTECTION SYSTEM

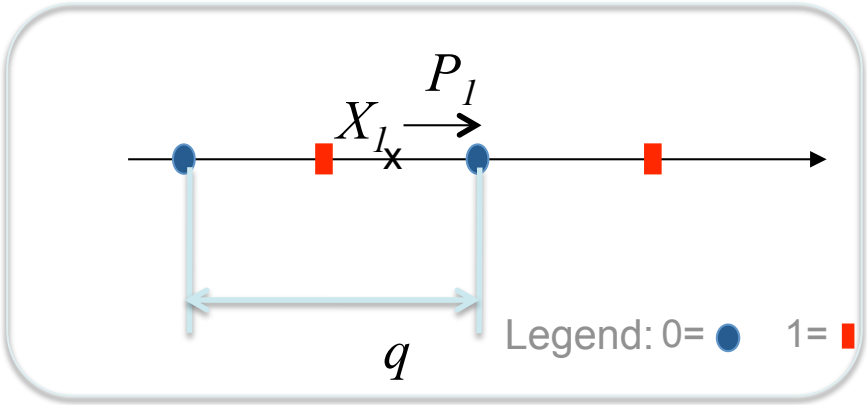


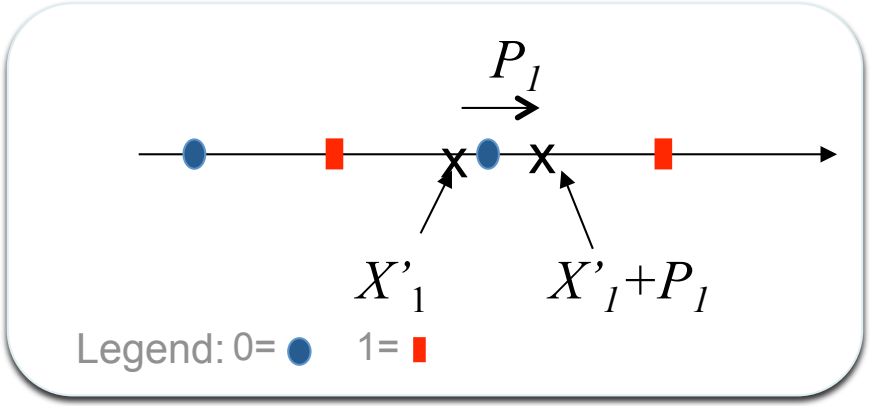
PHILIPS

QIM FUZZY EMBEDDER







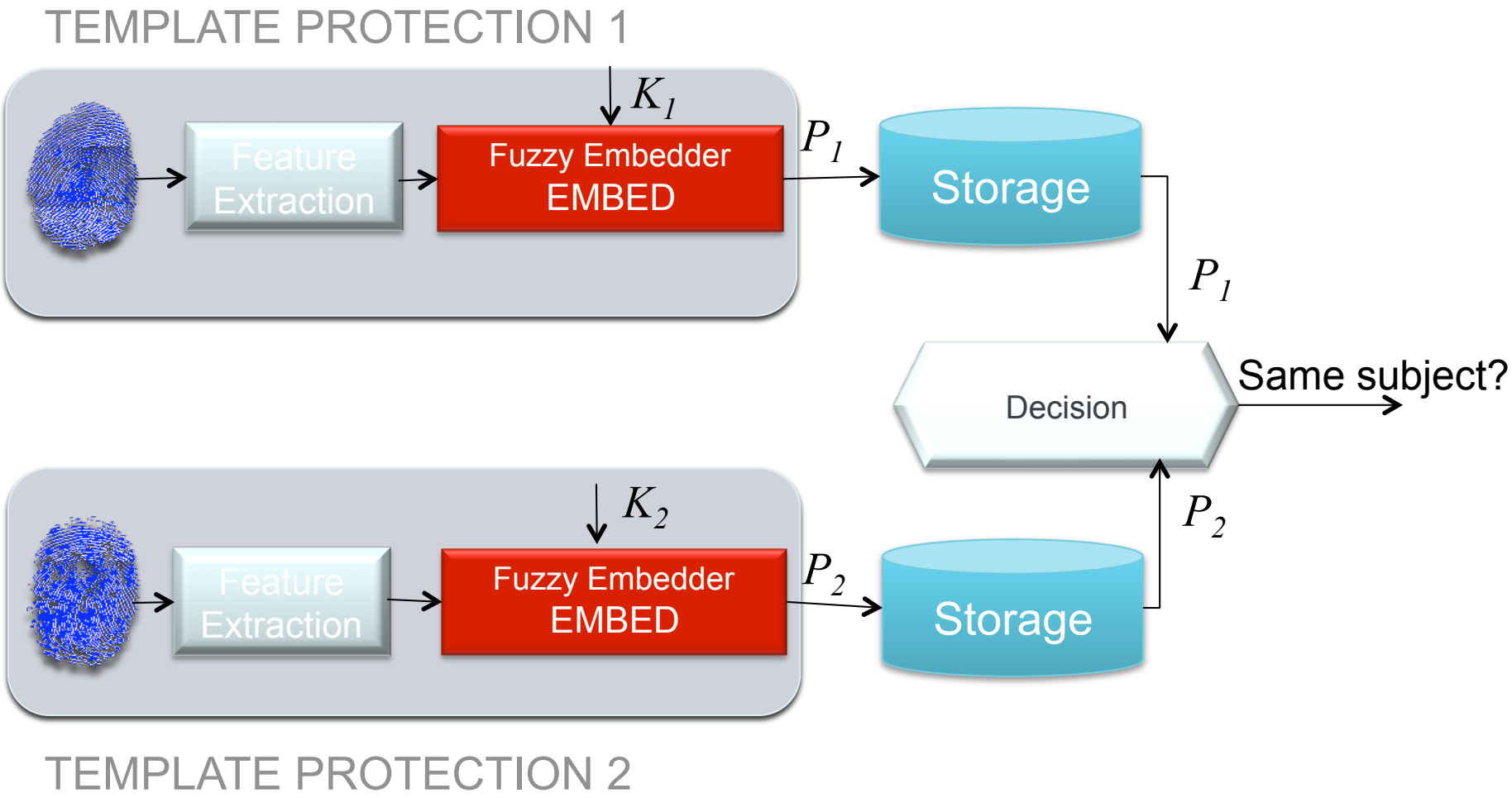


$$P_1 = Q_{K_1}(X_1) - X_1$$

$$K_1 = \arg\min\left(\left\lfloor \frac{2(X_1 + P_1)}{q} \right\rfloor \frac{q}{2} \right)$$

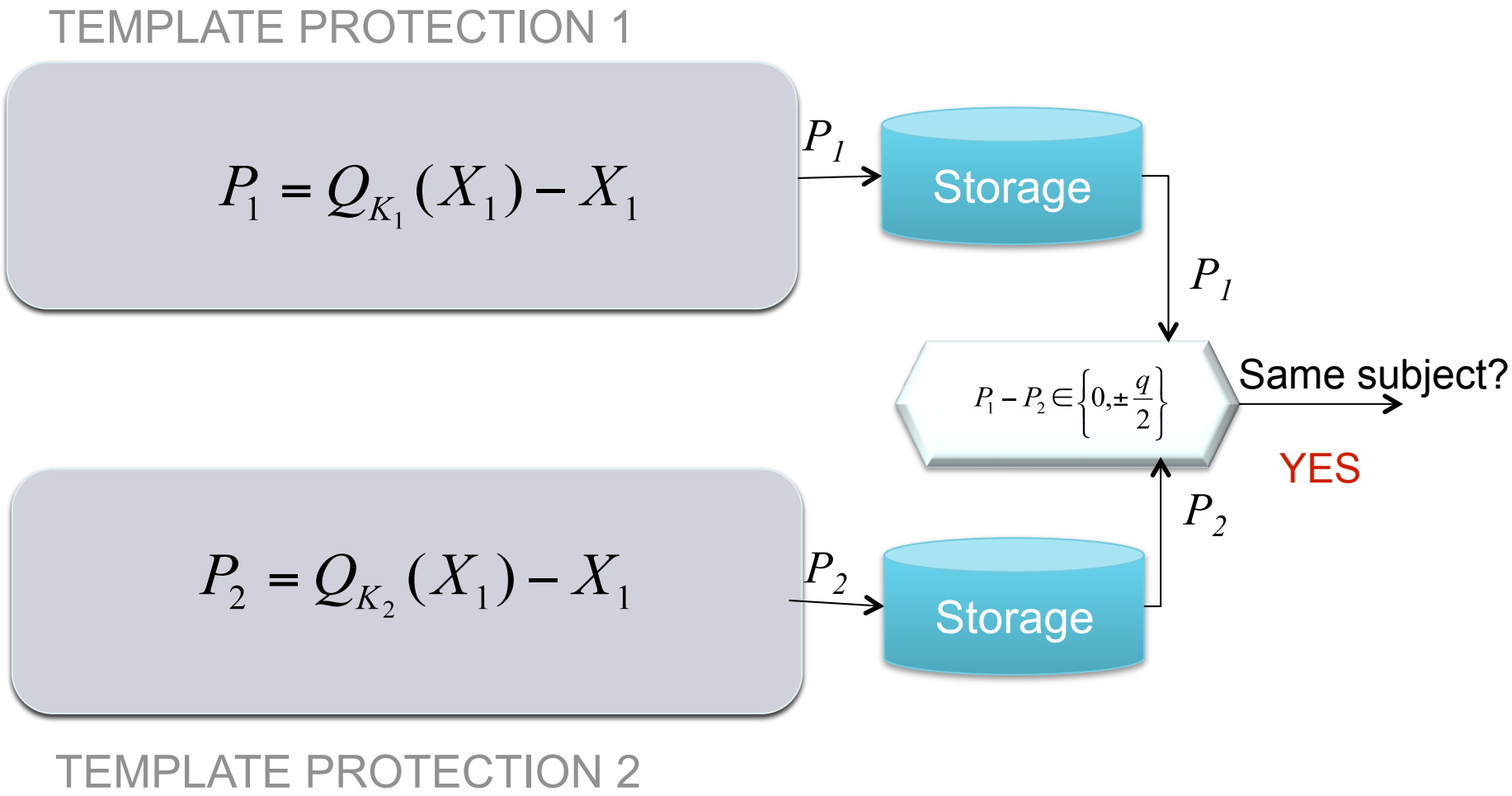
PHILIPS

TYPICAL SCENARIO- simple case (no noise)



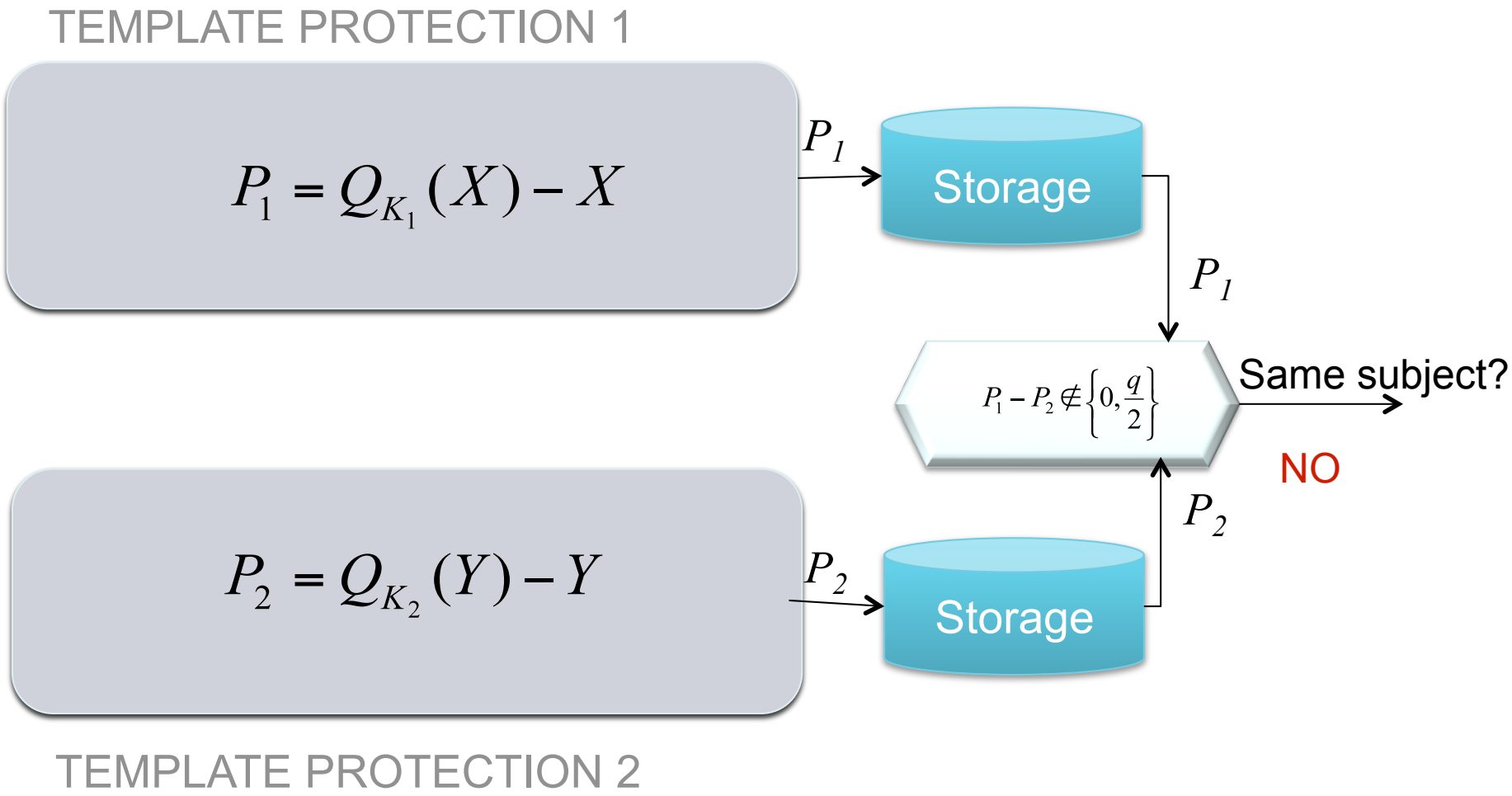
PHILIPS

CASE 1: same subject –no noise is present



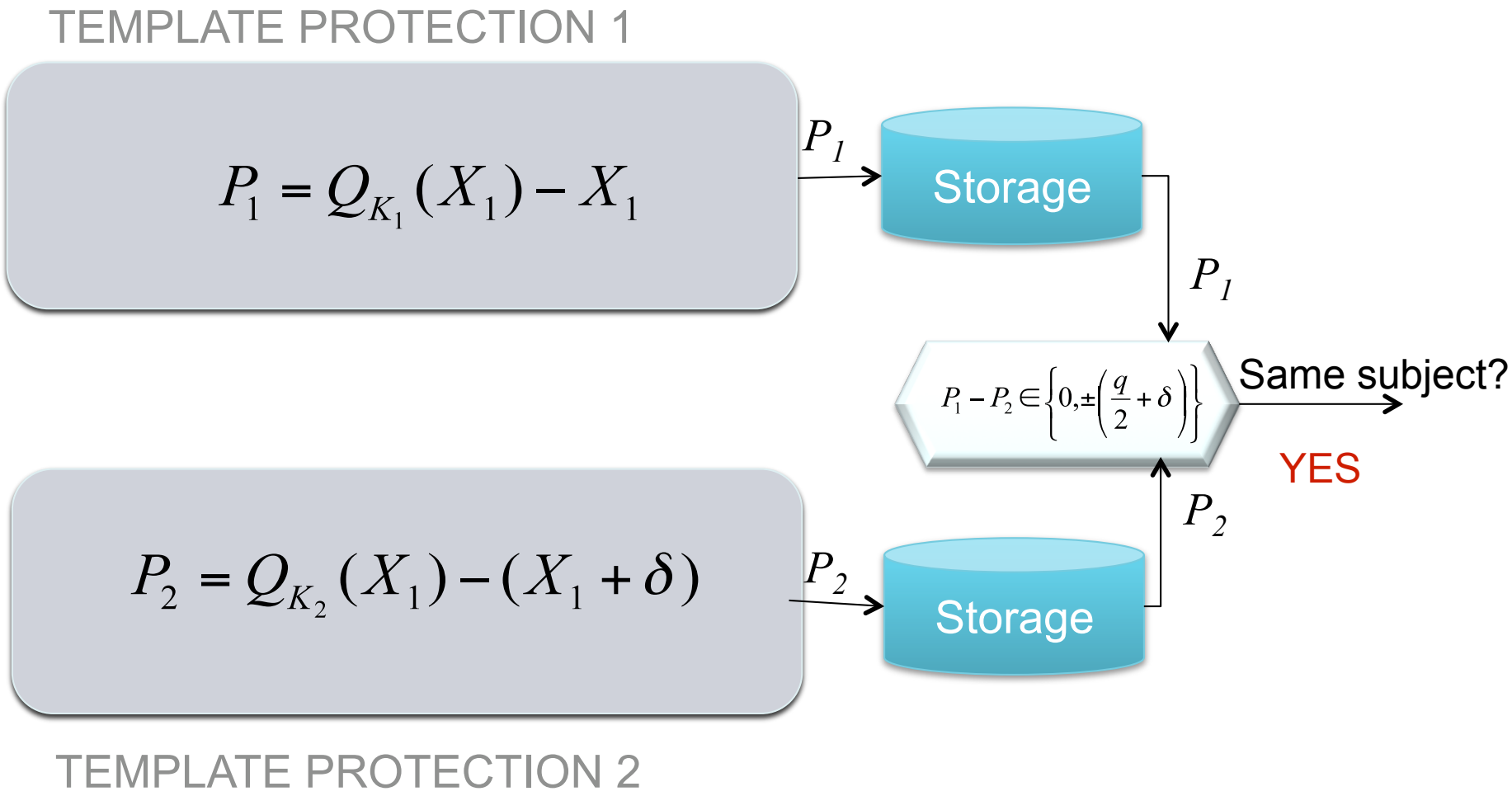
PHILIPS

CASE 2: different subjects



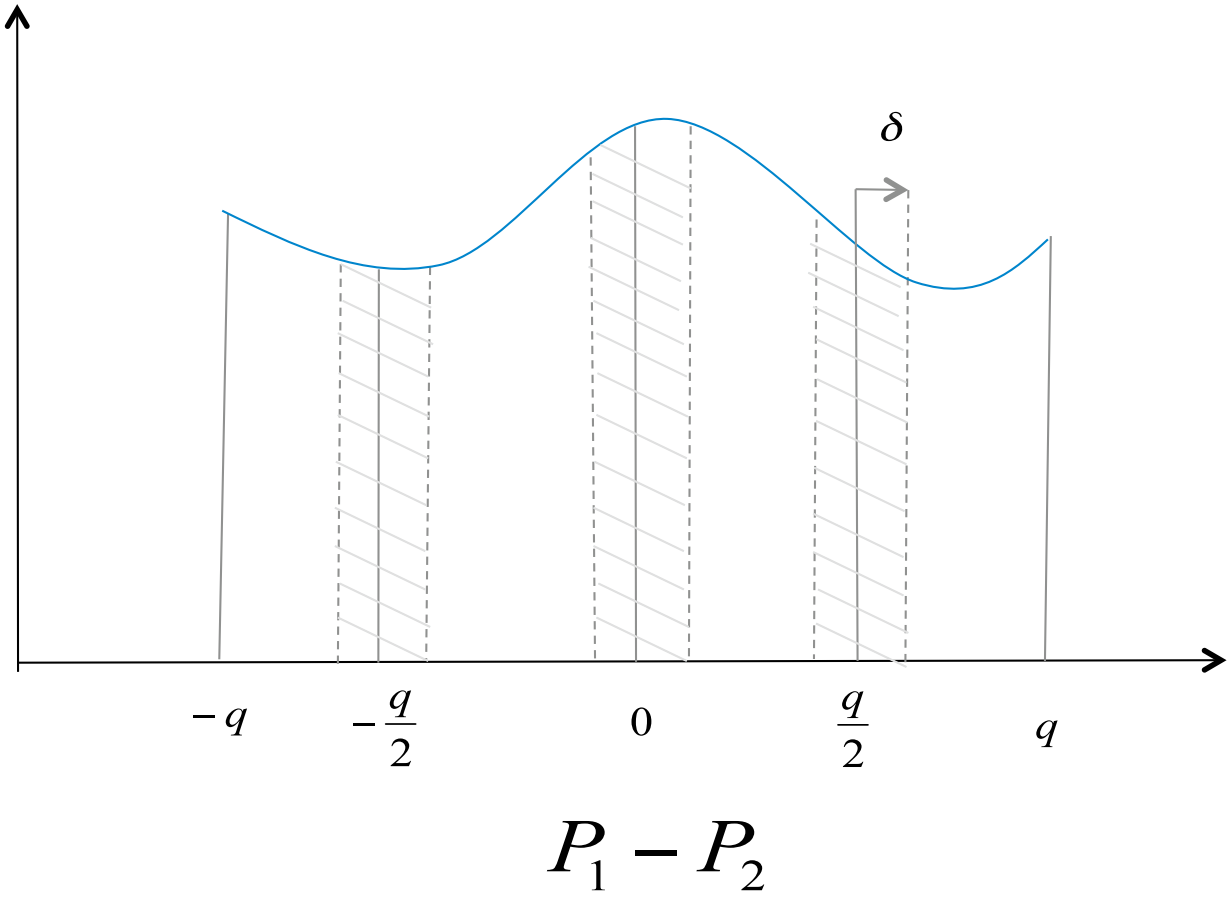
PHILIPS

CASE 1: same subject



DECISION FUNCTION –in the presence of noise

$$P_1 - P_2 \in \left\{0, \pm\left(\frac{q}{2} + \delta\right)\right\}$$



PHILIPS

1. INDISTINGUISHABILITY GAME

CHALLENGER **ADVERSARY**

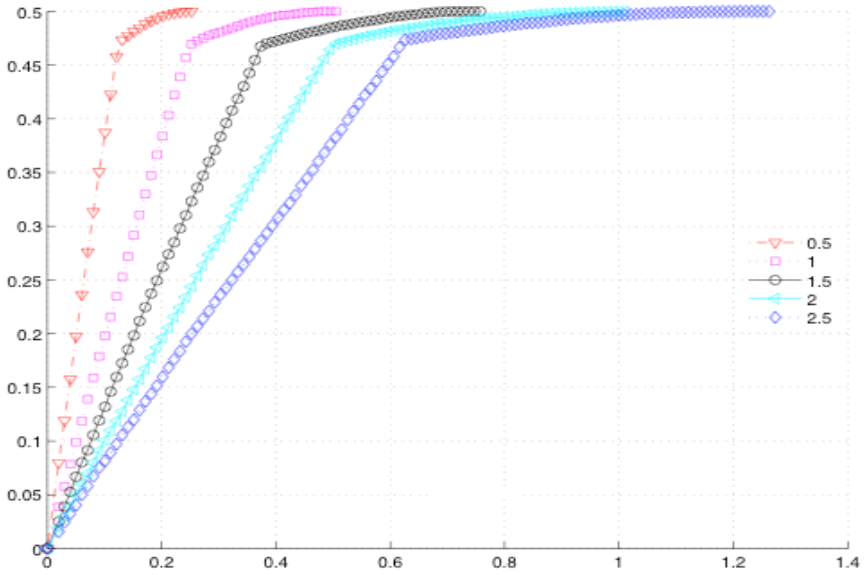
1. CHOSE: X, K
2. COMPUTE: $P = Embed(X, K)$
3. SEND → P
4. FLIP COIN $b \in \{0,1\}$
   IF $b = 0$ $P^* = Embed(X', K^*)$
   ELSE $P^* = Embed(Y, K^*)$
5. SEND → P*
6. OUTPUT b*

$$Adv_{IND} = \left| \Pr[b^* = b] - \frac{1}{2} \right|$$

PHILIPS

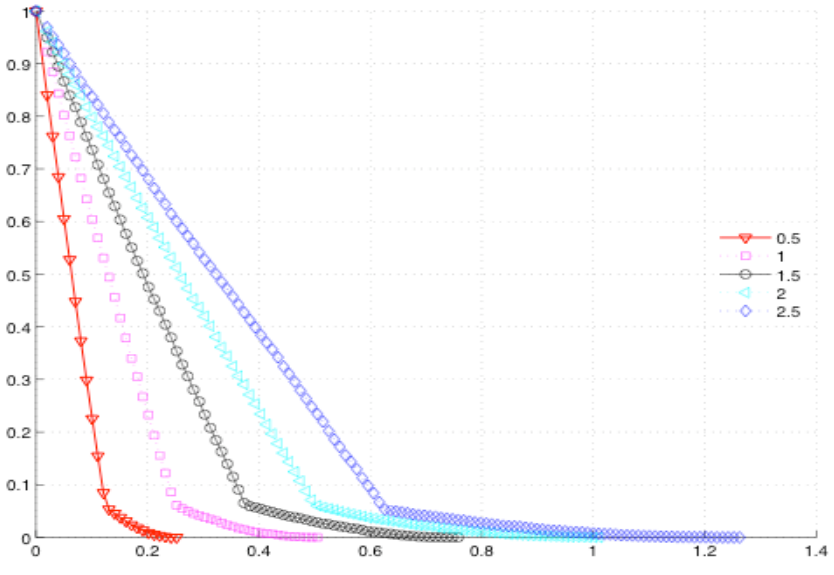
ADVANTAGE OF AN ADVERSARY

$$1 - \Pr[b^* = b]$$



$$0 < \delta < \frac{q}{4}$$

$$Adv_{IND}$$



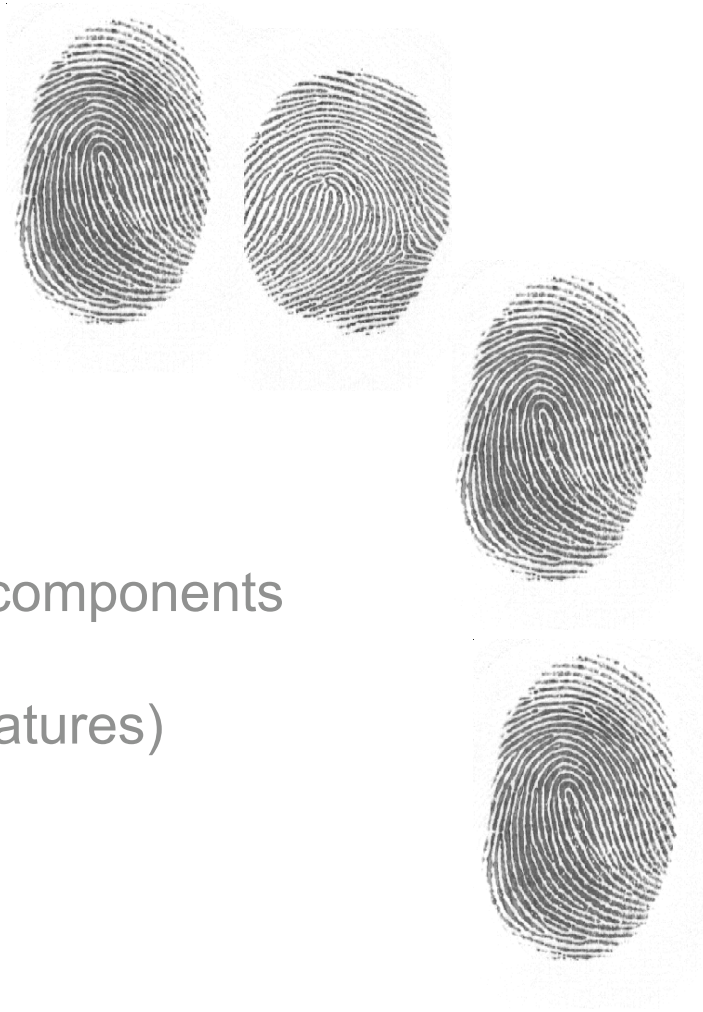
$$0 < \delta < \frac{q}{4}$$

PHILIPS

MCYT database

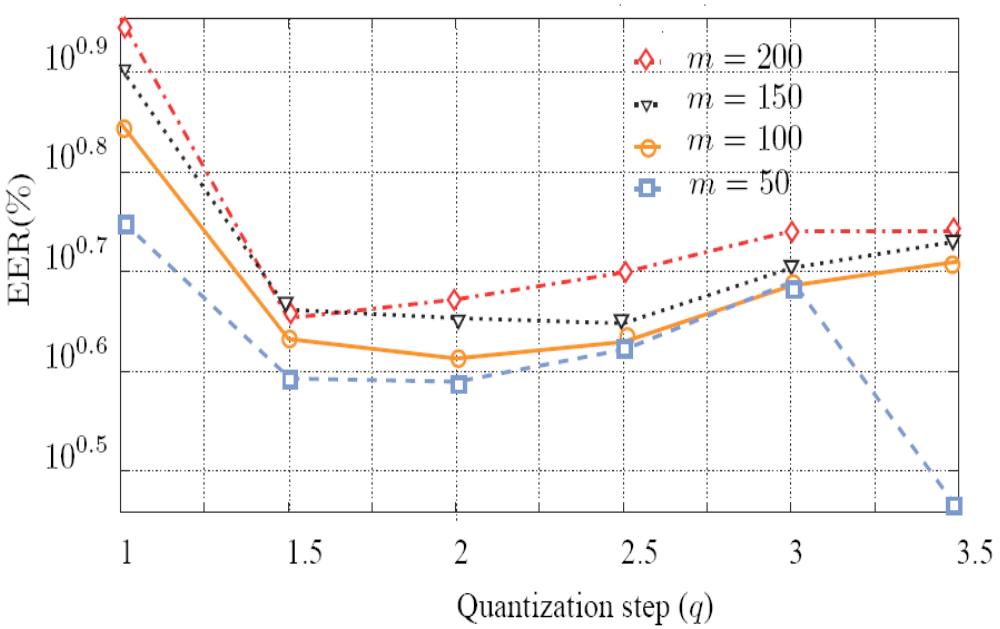
CHARACTERISTICS

- 323 persons
- 12 fingerprints per person (1 finger)
- processing of fingerprint:
  - -squared directional fields
  - -Gabor response of fingerprint => 1536 components
- PCA and LDA reduction =(200, 150, 100, 50 features)
- 80% used for training



PHILIPS

RELIABILITY QIM (4:1)



WHERE

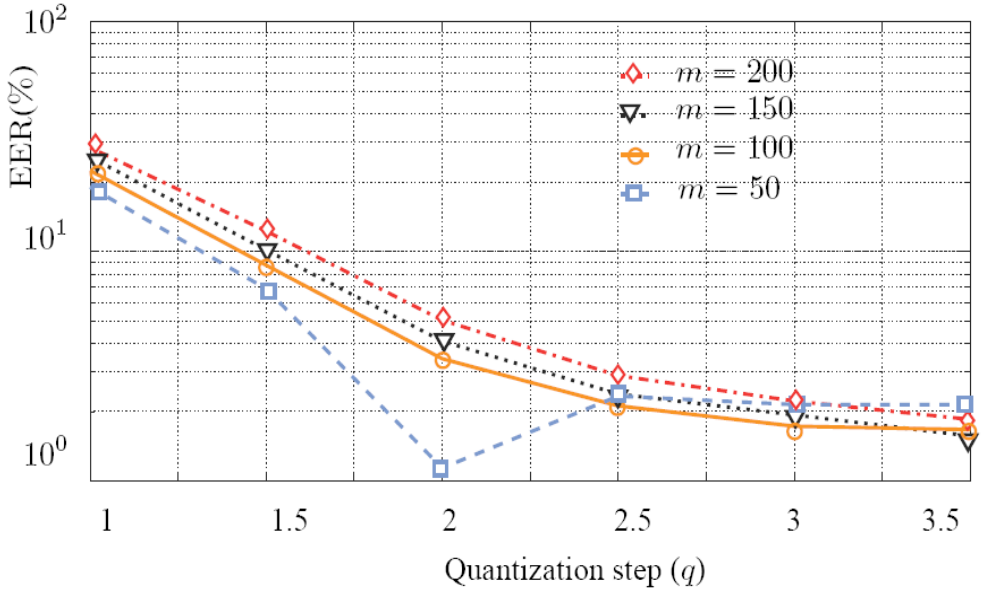
(1) $x = (x_1, x_2, \ldots x_m)$

(2) $d(x, x') < \frac{q}{2}$

	m=200	m=150	m=100	m=50
q=1	9.0	8.03	7.05	5.63
q=1.5	4.5	4.59	4.29	3.91
q=2	4.71	4.50	4.10	3.89
q=2.5	5.01	4.45	4.26	4.19
q=3	5.50	5.05	4.85	4.89
q=3.5	5.50	5.38	5.13	2.73

PHILIPS

CORRELATION QIM (4:4)



WHERE

(1) $x = (x_1, x_2, \ldots x_m)$

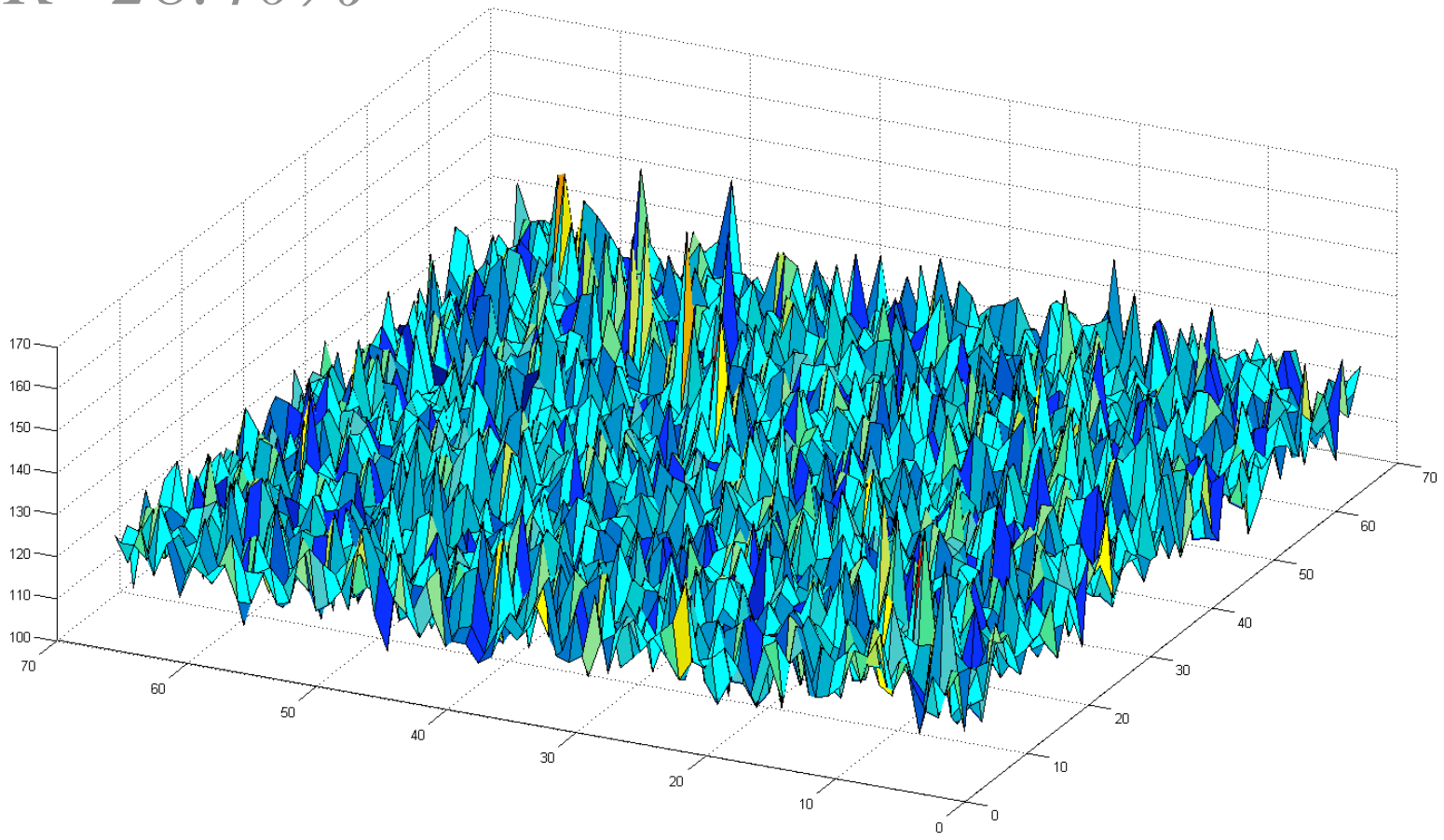
(2) $d(x, x') < \frac{q}{2}$

	m=200	m=150	m=100	m=50
q=1	28.40	25.81	22.56	19.11
q=1.5	12.30	10.17	8.74	6.90
q=2	5.03	4.08	3.42	1.15
q=2.5	2.89	2.40	2.14	2.35
q=3	2.24	1.95	1.74	2.16
q=3.5	1.86	1.58	1.68	2.16

PHILIPS

CORRELATION QIM (*q=1, M=200*)

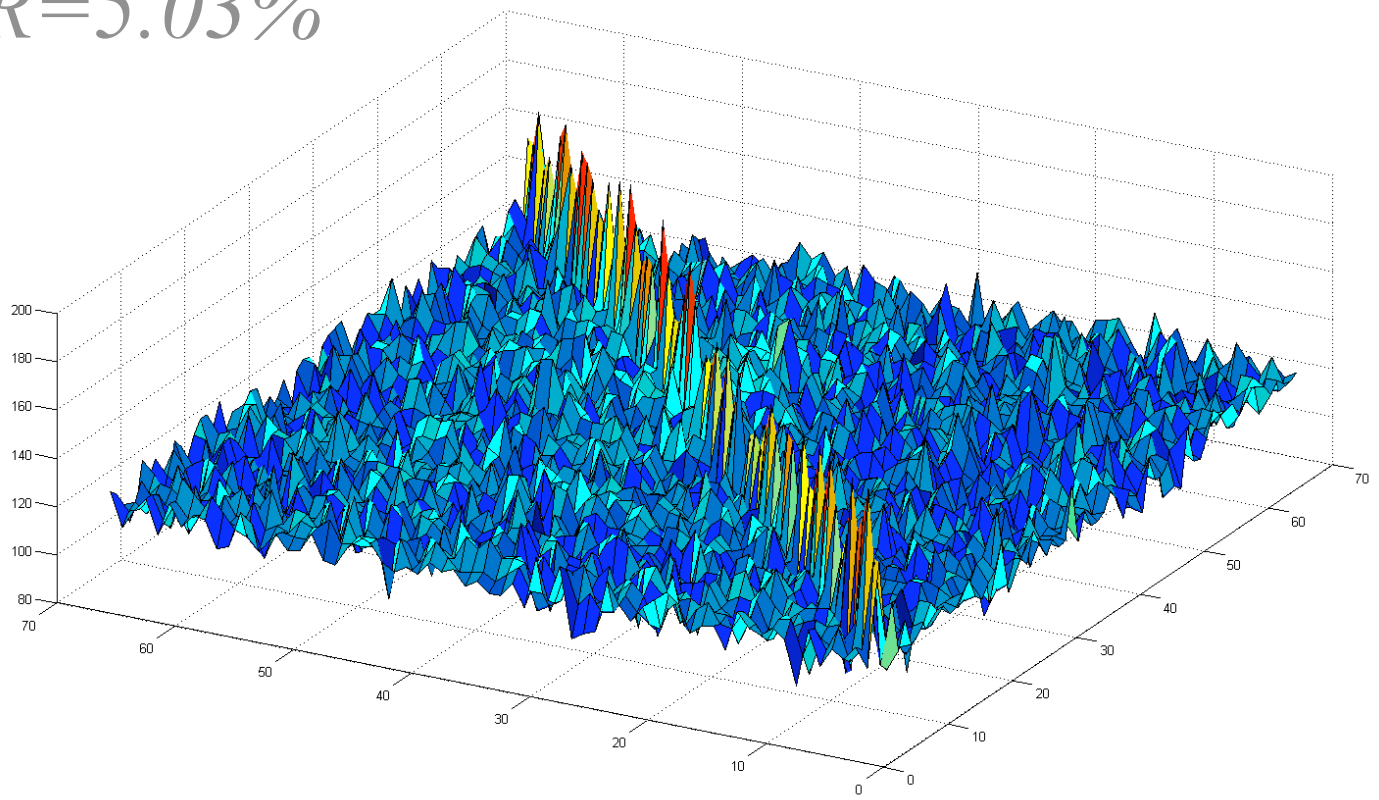
EER=28.40%



PHILIPS

CORRELATION QIM (*q=2, m=200*)

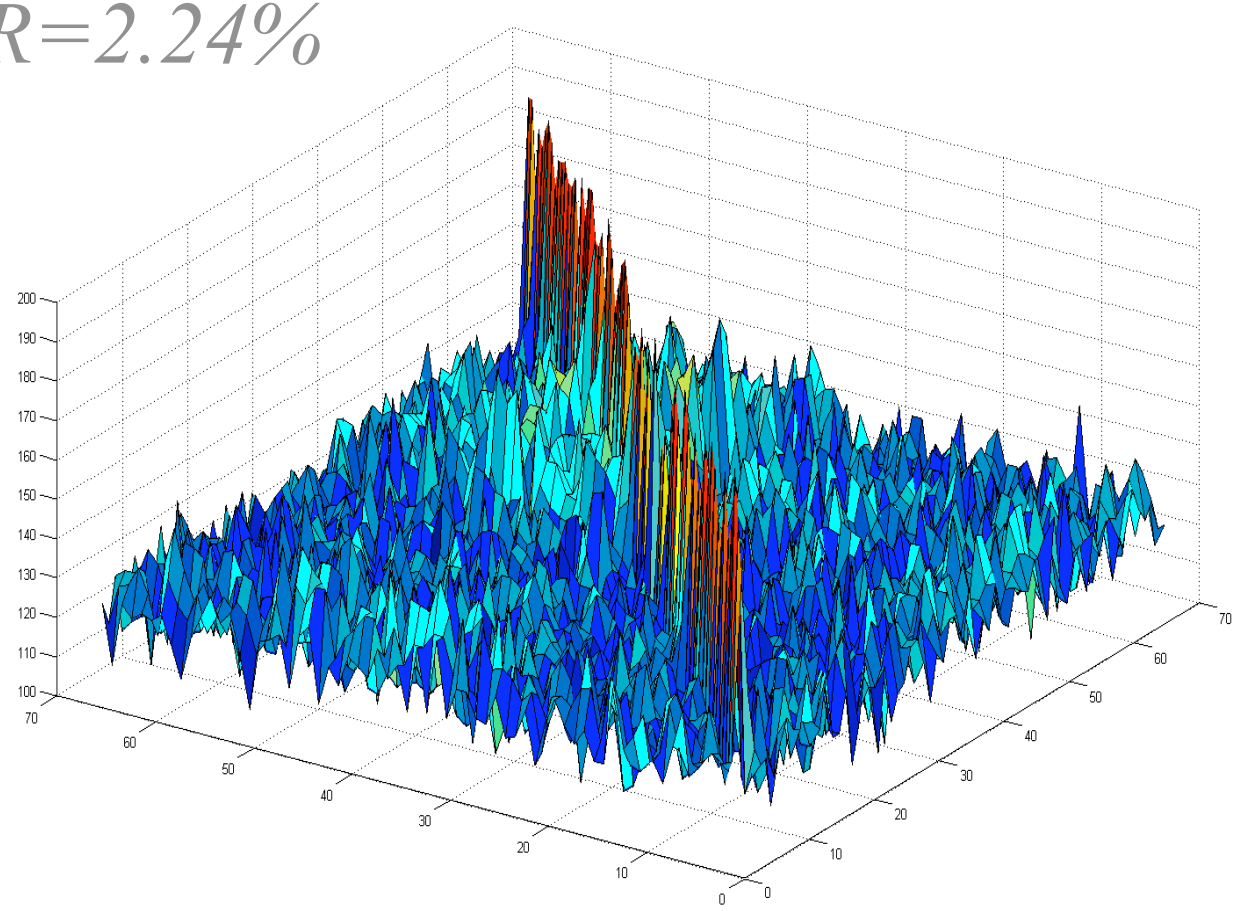
EER=5.03%



PHILIPS

CORRELATION QIM (*q=1, m=200*)

EER=2.24%



PHILIPS

CONCLUSIONS

- We show that it is possible to correlate protected biometric information;
- Give two measures for indistinguishability;
- The first measures *how far from ideal* the biometric cryptosystem is;
- The second measures *how much we gain* in privacy when protecting the biometric templates;


PHILIPS