ISO/IEC 30136 Performance Testing of Template Protection Schemes

Marta Gomez-Barrero

BioML lab, RI CODE, Universität der Bundeswehr München

Int. Face and Fingerprint Performance Conf., 2025-04-01

BioML

CODE RI Research Institute Cyber Defence Universität der Bundeswehr München

BioML: Biometrics & Machine Learning

- Since 2023 (before @UAM, h_da, HSAN)
- Research on (but not limited to!):
  - Different biometric modalities, and multi-biometrics
  - Biometric Template Protection and Attack Detection
  - Synthetic data
  - Explainability
- Chair BIOSIG
- Involved in EAB and ISO/IEC SC 37

- More details on:
  https://www.unibw.de/bioml-en
  https://www.marta-gomez-barrero.com
  marta.gomez-barrero@unibw.de

Introduction

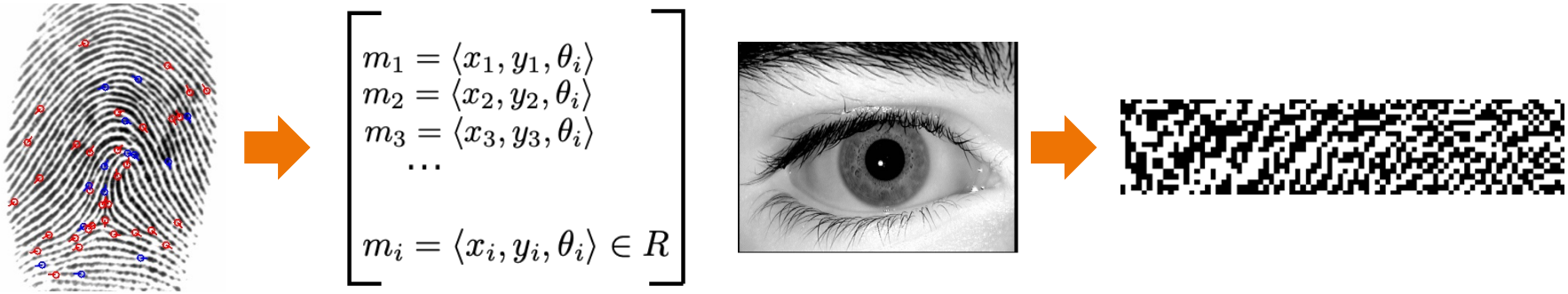
Biometrics & Privacy

- Biometric data is classified as **sensitive personal data** by the European Data Protection Regulation (GDPR)

- Different legislations across the globe, adding more protection:
  - Japan Act on the Protection of Personal Information (APPI) also includes extra-territorial protection since 2022
  - Australian Privacy Act is undergoing reforms
  - The California Consumer Privacy Act (CCPA), based on the GDPR, aims to empower consumers with new rights in order to protect their privacy
  - …

Inverse biometrics attacks

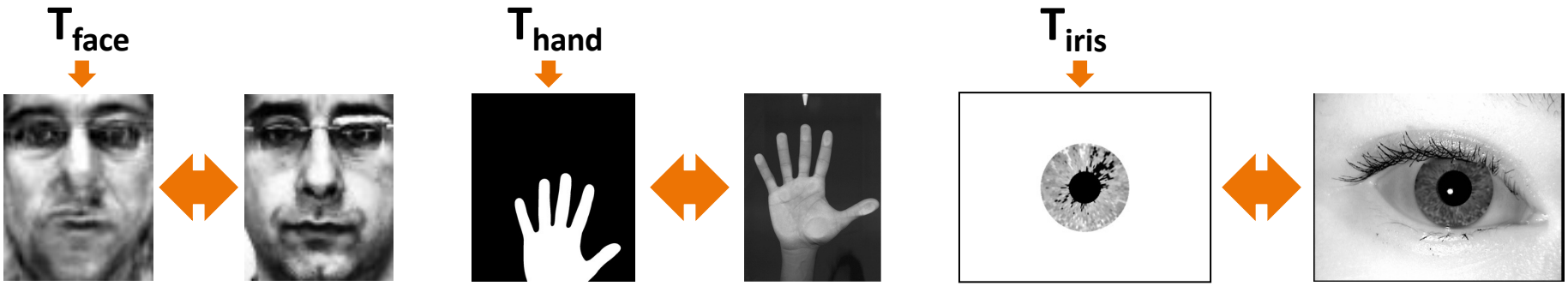
- It was a common belief that the stored templates revealed no information about the biometric characteristics:



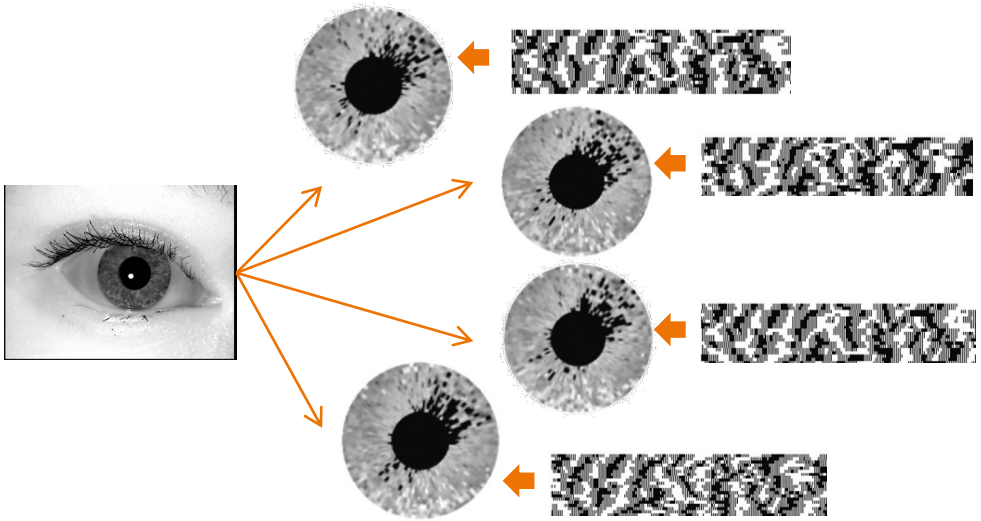
- However, biometric samples can be recovered from the stored unprotected templates

Inverse biometrics attacks: Hill-Climbing

- Based on the HC algorithms, we can reconstruct biometric samples:



[M. Gomez-Barrero *et al.*, *Int. Conf. on Biometrics*, 2012]
[M. Gomez-Barrero *et al.*, *Information Sciences*, 2014]
[J. Galbally, *et al.*, *Computer Vision & Image Understanding*, 2013]



Linkage attacks

- We can enroll with a single instance in different applications

T_{mail}

Santander CONSUMER BANK

T_{bank}

der Bundeswehr Universität München

T_{job}

$T_{facebook}$

$T_{linkedin}$

Same person??

Templates need to be protected, so that no one can find out on which applications we are enrolled

Protecting the subject's privacy

[ISO/IEC IS 24745 on Biometric Information Protection]

Female, white, 30s…

Irreversibility

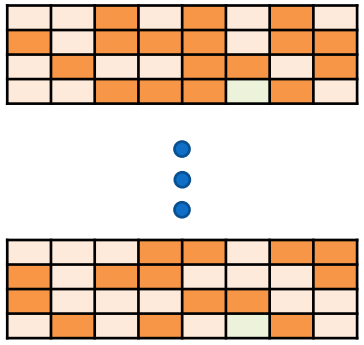
=?

Unlinkability

Renewability

K_1

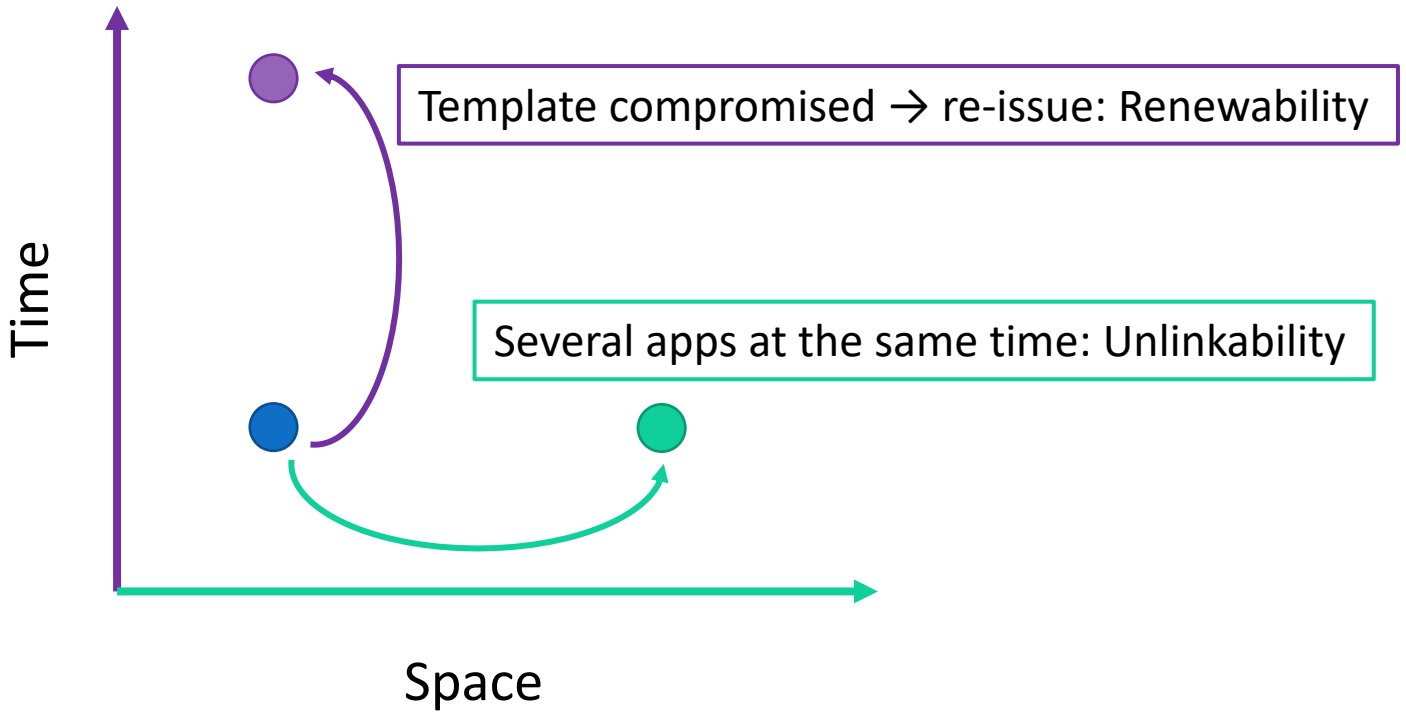
K_n



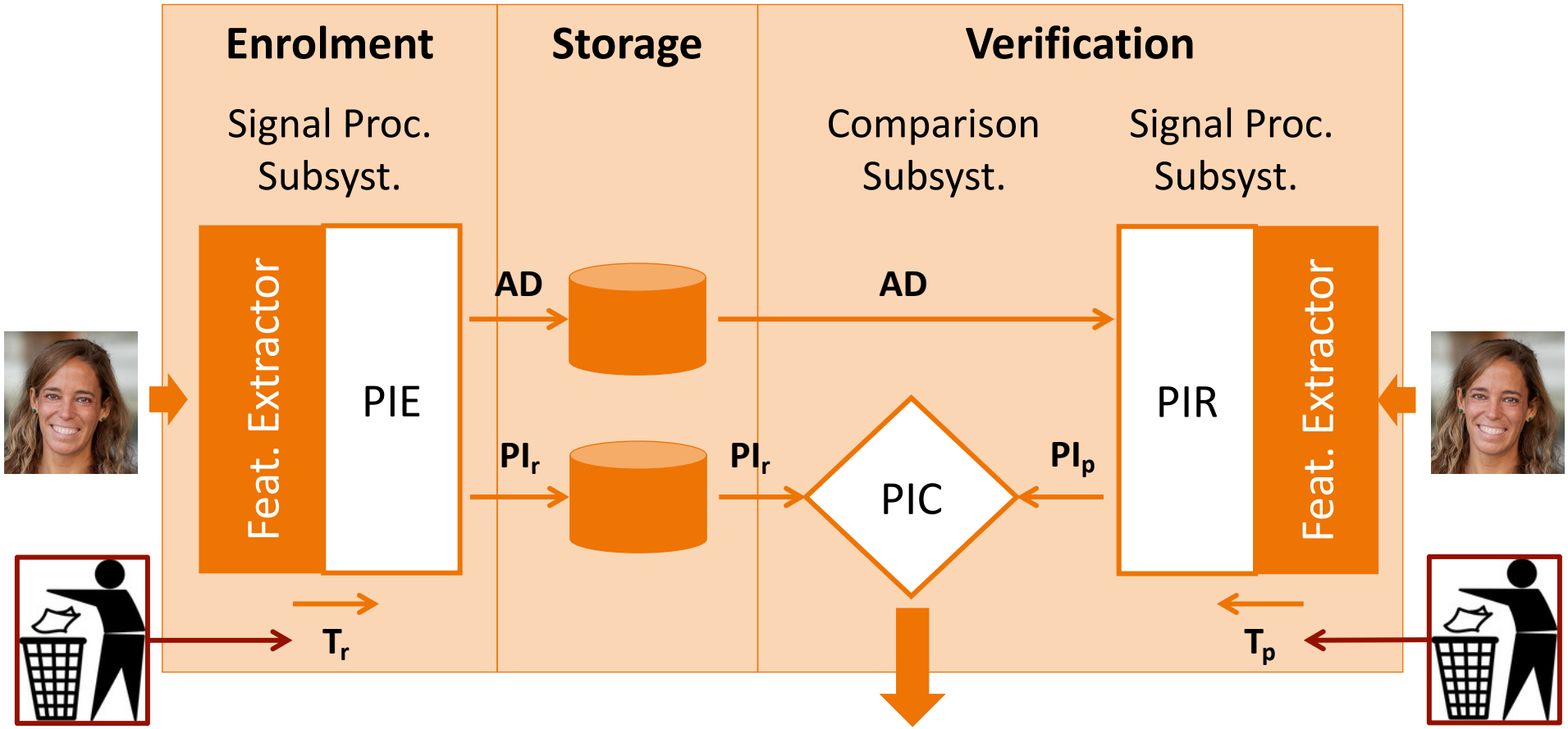
Accuracy, **template size** and **verification speed** must be preserved.

Unlinkability vs. Renewability

- Diversification in space and time



BTP architecture

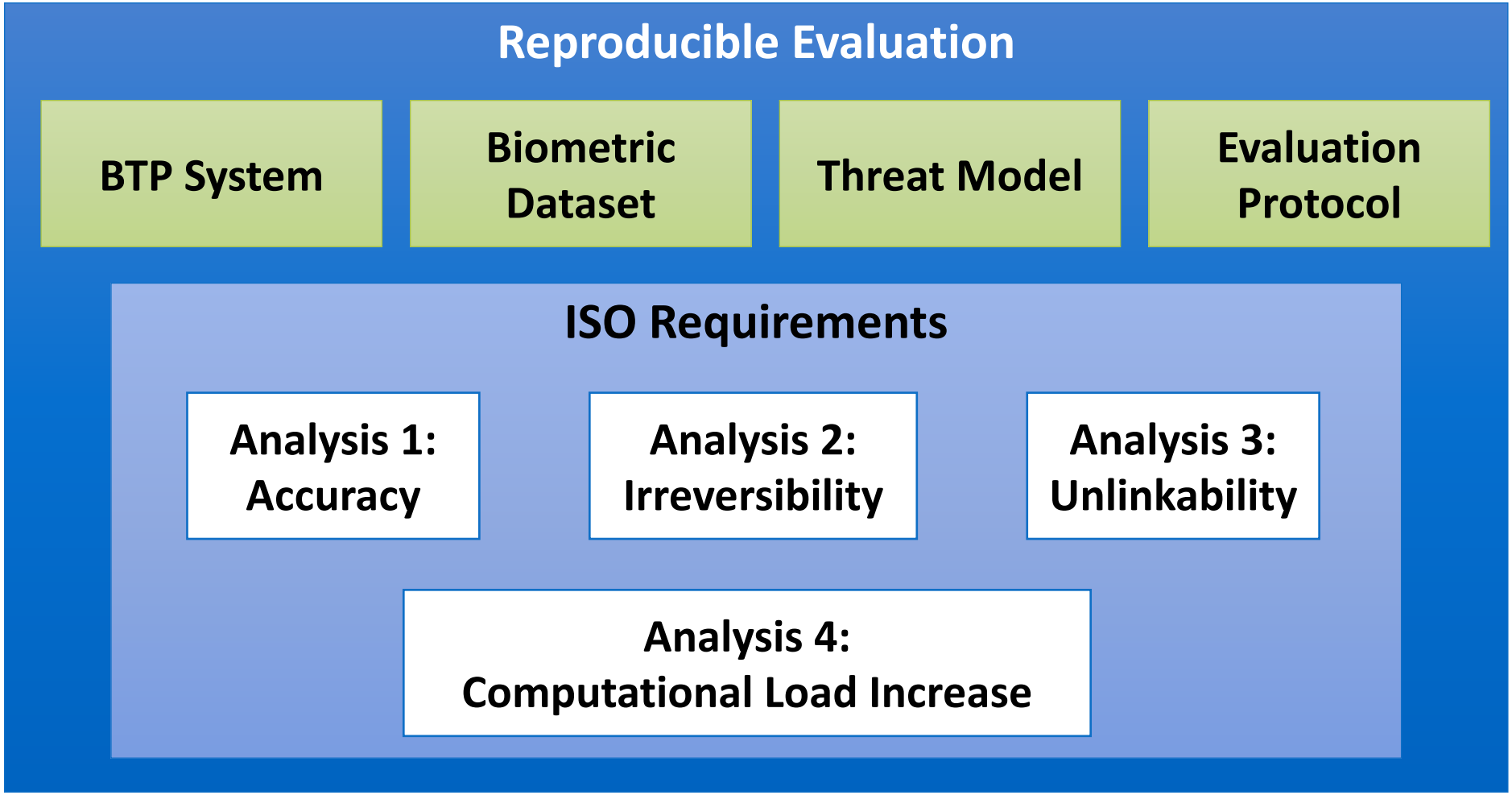


PI: Pseudonymous Identifier
AD: Auxiliary Data

PIE: PI Encoder
PIR: PI Recorder
PIC: PI Comparator

Security and Privacy Evaluation

BTP Evaluation: How to?



Threat models

- We need to describe the attacker's capabilities and skills:
  - **Naive model**:
    - No knowledge about the system, no access to large DBs
    - Access to RBRs + black-box system
  - **Collision model**:
    - Access to large DBs
    - Access to a BTP system that generates similar PIs to the system under attack
  - **General model**:
    - Full knowledge about the system, statistical properties of the enrolled data, access to protected data
    - **Standard model**: secret key remains secure
    - **Advanced model**: chosen-plaintext and chosen-ciphertext attack
    - **Full disclosure model**: secret key compromised

Accuracy degradation

- Most BTP schemes transform either the sample (e.g. surface folding) or the template (e.g., fuzzy vault)
- That leads to the addition of noise or information loss, which in turn leads to a decrease in accuracy
- We need to assess such performance loss in accordance with the ISO/IEC 19795:
  - Compute FMR and FNMR for the baseline system AND the BTP scheme
  - Following a common experimental protocol
  - Compare in terms of DET plots
    - The Equal Error Rate (EER), where FMR = FNMR, is not enough!!

Irreversibility & Unlinkability

- Theoretical evaluation:
  - "Proving a computational or an information-theoretic property limiting the success probability or the advantage of any computationally-bounded adversary"
  - Example for unlinkability: *indistinguishability game describes the advantage of an attacker with respect to a perfect indistinguishable system*

- Empirical evaluation:
  - "The experimenter shall specify an empirical method of demonstrating irreversibility / unlinkability, for example, empirically estimating the success probability or the advantage over a random guess for some specific adversary in an attack scenario"

[ISO/IEC IS 30136 on Performance Testing of BTP Schemes]

Irreversibility analysis

- How can we analyse irreversibility? Following cryptographic paradigms?

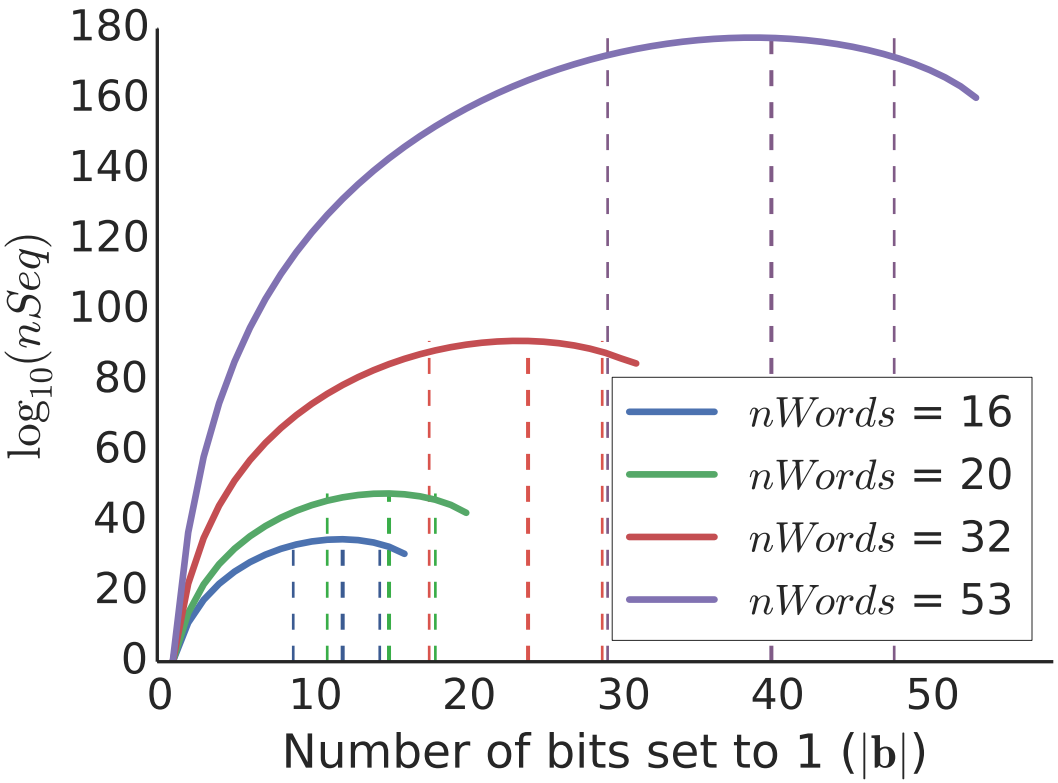
- Careful! Some assumptions are not valid:
  - Uniformity of data – neighbouring bits are correlated!!
  - In fact, some biometric templates (e.g., finger vein or fingerprint minutiae spectral representation) are compared in terms of their cross correlation!
  - There are also symmetries

- Therefore, we need to model such correlations and take them into account in the computations
  - No general method proposed so far

Irreversibility analysis

- $nSeq$: number of original sequences leading to a single template.
- For a full disclosure model, the probability of a reconstruction is

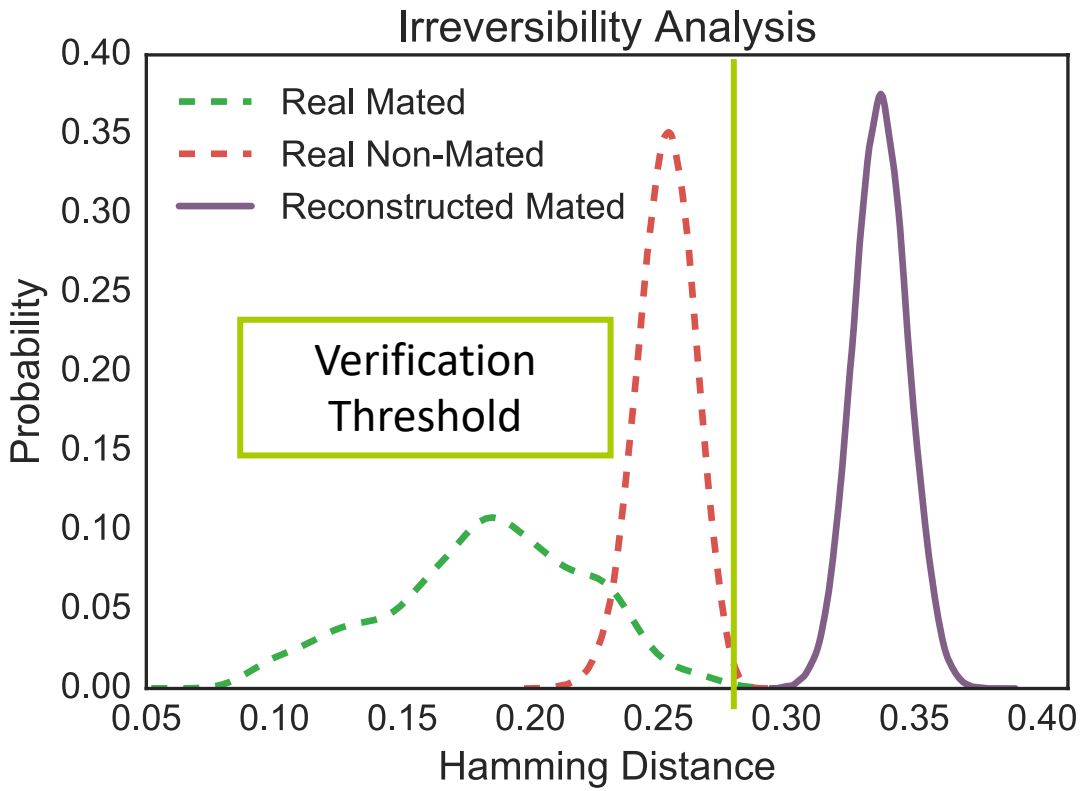
$$\mathbf{2^{-40,960}}$$



[Gomez-Barrero *et al.*, *Information Sciences* 2016]

Irreversibility analysis

- Are the reconstructed unprotected templates similar to the original ones?



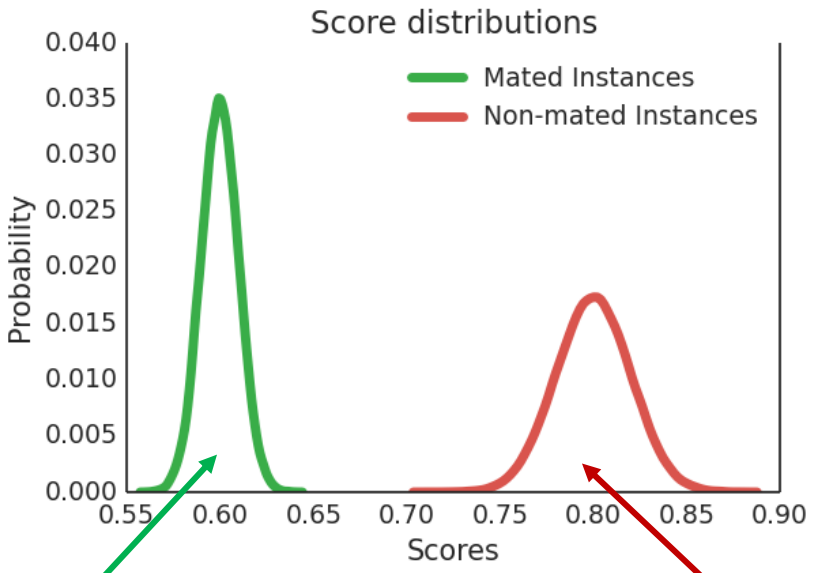
Irreversible: HD bigger than impostor comparisons

[Bringer *et al.*, *ICB* 2015]

Linkage Attacks: How to?

T_{job} T_{bank}

$s = LF(T_{job}, T_{bank})$



s here ➔ success!! ☺

s here ➔ try again!! ☹

s can be the dissimilarity score of the system or any other dissimilarity score, such as values extracted from partial decoding in fuzzy schemes

Unlinkability Analysis

- Plot *Mated* and *Non-mated instances* distributions, for templates protected with different keys, and analyse them
- Two measures:
  - Local measure $D_{\leftrightarrow}(s)$ ➔ for which scores is the system vulnerable?
  - Global measure $D_{\leftrightarrow}^{sys}$ ➔ how can we compare two systems globally?
- Both bounded in [0,1], and defined for all dissimilarity scores
- General measures, valid for all BTP schemes
- Available at: https://github.com/dasec/unlinkability-metric
- Included in the ongoing revision of ISO/IEC 30136

[Gomez-Barrero *et al.*, *IEEE T-IFS*, 2018]

Unlinkability Analysis

- We need to simulate the enrolment of the subjects in different applications, and then apply the linkage function to those protected templates

- We need access to:
  - Biometric database (DB)
  - BTP scheme to be evaluated (BTP)

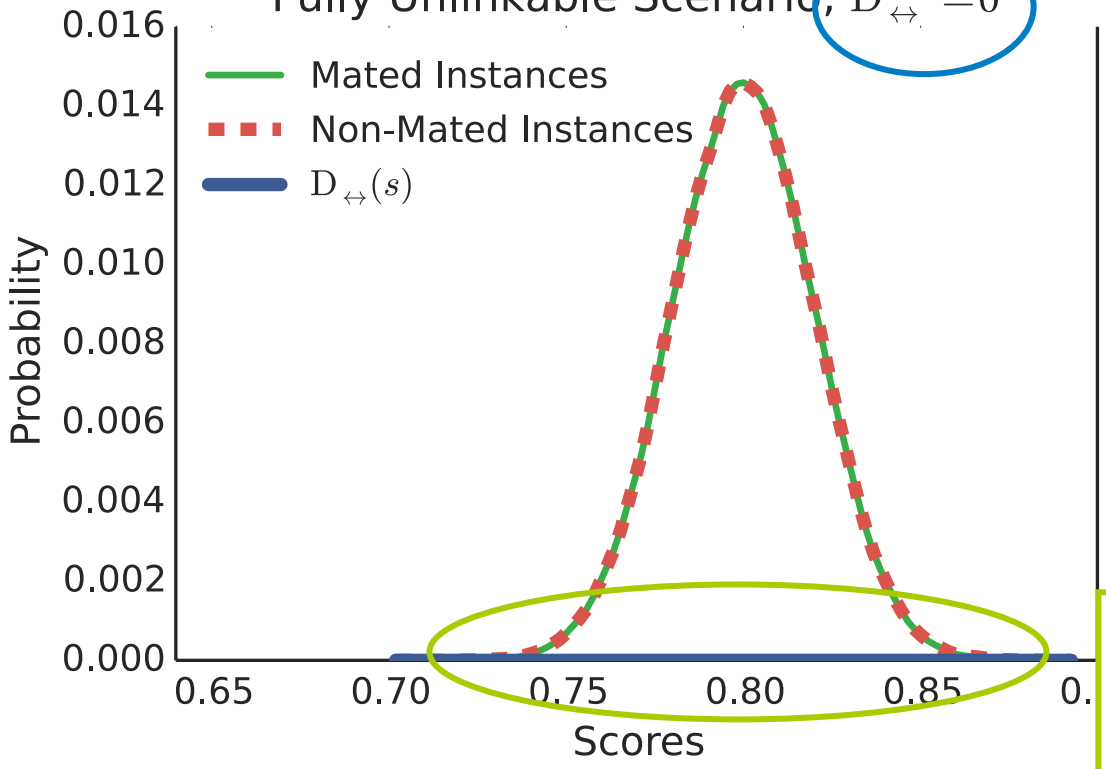
- Define a Linkage Function (LF)
  - Robustness to one LF does not imply robustness to all possible LFs!

- Compute score distributions of LF using DB and BTP

Computing Score Distributions

- Simulate K different applications
  - Choose a reasonably big K - e.g., $K = 10$
- Enrol the data subjects into all K applications: for sample j of subject i, we have K templates: $T_1^{i,j}, T_2^{i,j}, \dots, T_k^{i,j} \dots, T_K^{i,j}$
  - For subject i, having J samples, we have a total of $J \times K$ templates: $T_1^{i,1}, T_1^{i,2}, \dots T_1^{i,J}, T_2^{i,1}, \dots, T_2^{i,J}, \dots, T_K^{i,J}$
- Design your protocol for mated and non-mated trials
- Compute mated and non-mated linkage scores by comparing:
  - Mated scores: samples of the **same** subject, enrolled in **different** applications: $s = LF\left(T_{\mathbf{1}}^{\mathbf{1},1}, T_{\mathbf{2}}^{\mathbf{1},2}\right)$
  - Non-Mated scores: samples of the **different** subjects, enrolled in **different** applications: $s = LF\left(T_{\mathbf{1}}^{\mathbf{1},1}, T_{\mathbf{2}}^{\mathbf{2},2}\right)$

Full Unlinkability



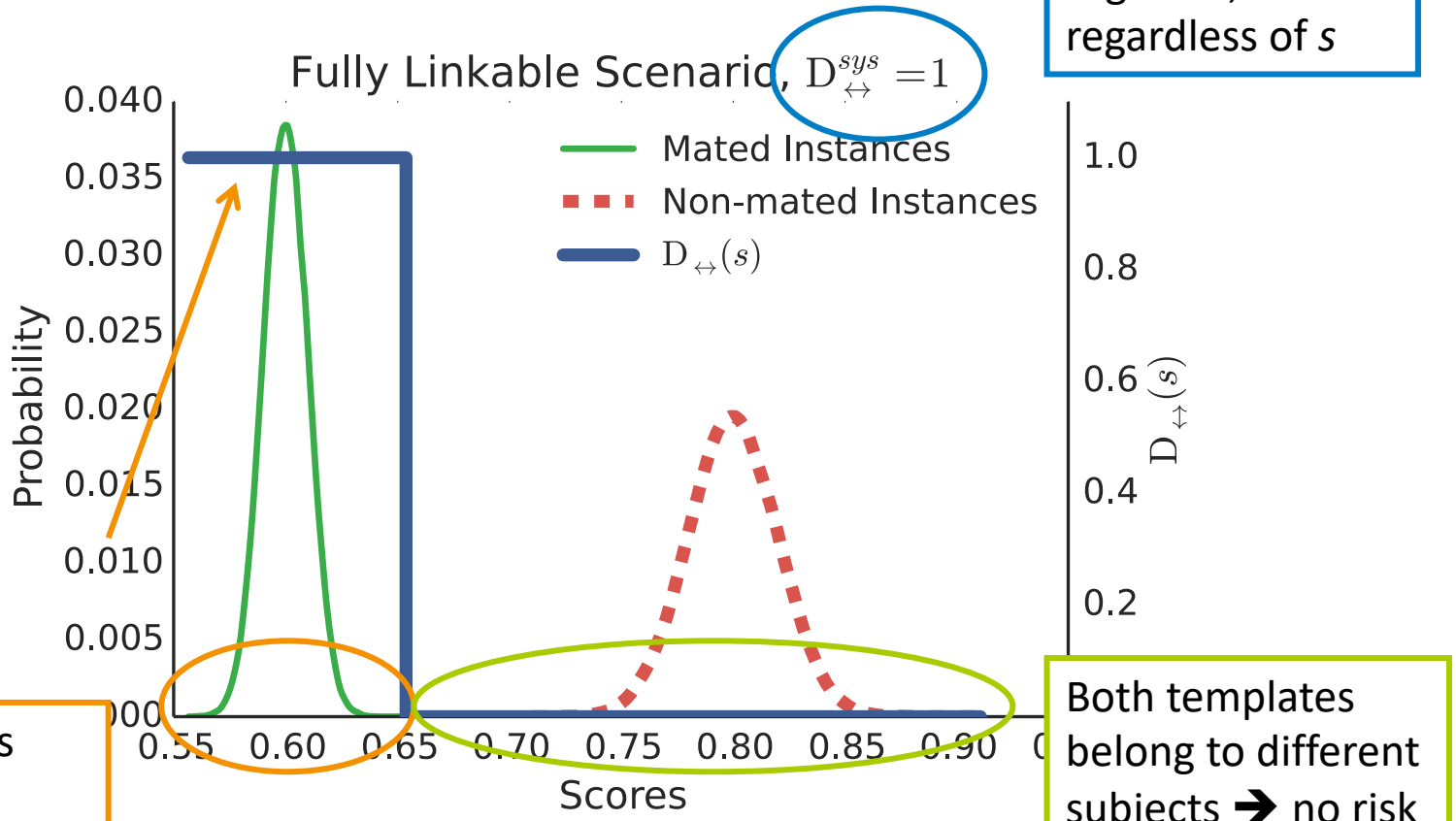
No risk, regardless of *s*

Cannot ensure both templates belong to the same subject ➔ no risk

[Gomez-Barrero *et al.*, *IEEE T-IFS*, 2018]

Full Linkability

High risk, regardless of *s*



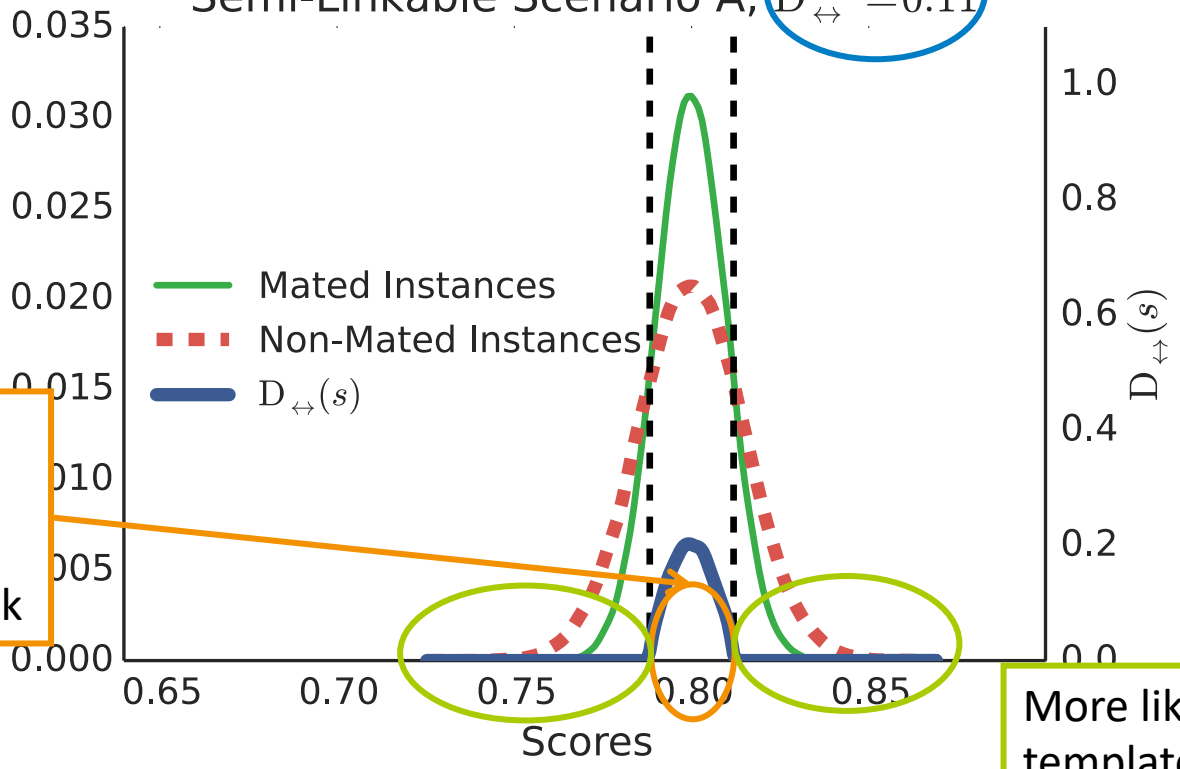
Both templates belong to the same subject ➔high risk

Both templates belong to different subjects ➔ no risk

[Gomez-Barrero *et al.*, *IEEE T-IFS*, 2018]

Semi-Linkable Scenario A

High risk only for some *s*



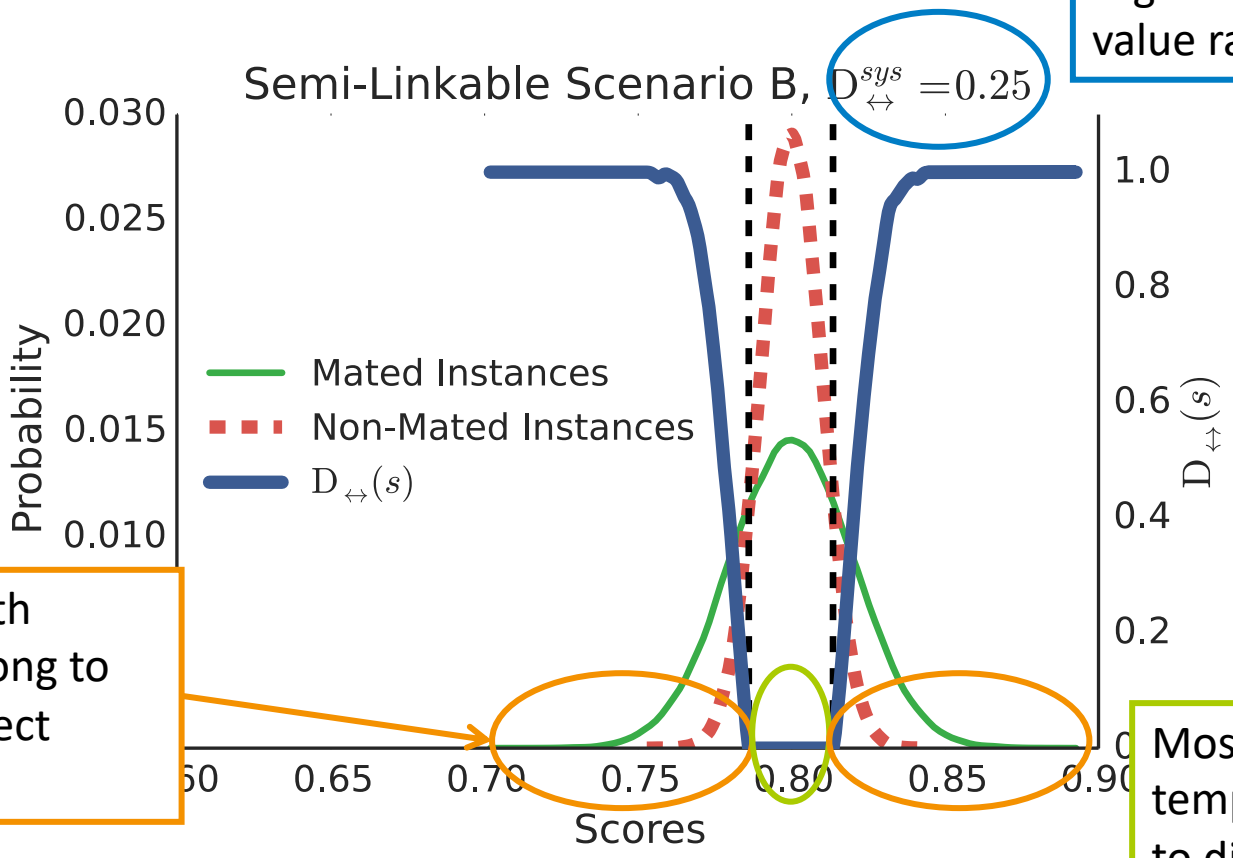
More likely both templates belong to the same subject ➔high risk

More likely both templates belong to different subjects ➔ no risk

[Gomez-Barrero *et al.*, *IEEE T-IFS*, 2018]

Semi-Linkable Scenario B

High risk, for larger value range *s*



Most likely both templates belong to the same subject ➔high risk

Most likely both templates belong to different subjects ➔ no risk

[Gomez-Barrero *et al.*, *IEEE T-IFS*, 2018]

Unlinkability Metrics

- We are interested in evaluating: $D_{\leftrightarrow}(s) = p(H_m|s) - p(H_{nm}|s)$
- Doing some math tricks, we get:

$$\mathrm{D}_{\leftrightarrow}(s) = \begin{cases} 0 & \text{if } LR(s) \cdot \omega \leq 1 \\ 2\frac{LR(s)\cdot\omega}{1+LR(s)\cdot\omega} - 1 & \text{if } LR(s) \cdot \omega > 1 \end{cases}$$

- Where $\omega = p(H_m)/p(H_{nm})$

- And we can define a global metric as:

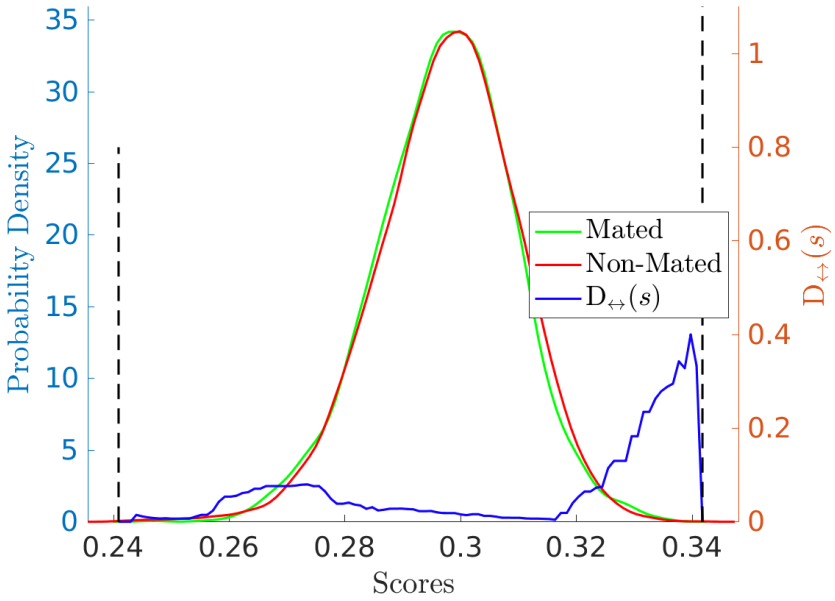
$$\mathrm{D}_{\leftrightarrow}^{sys} = \int_{s_{min}}^{s_{max}} p(s|H_m) \cdot \mathrm{D}_{\leftrightarrow}(s)\,\mathrm{d}s$$

[Gomez-Barrero *et al.*, *IEEE T-IFS*, 2018]

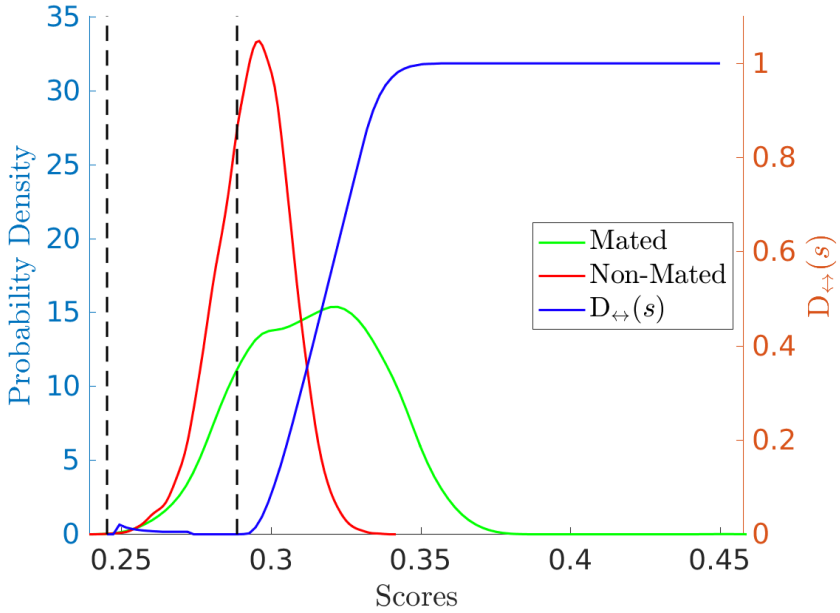
Choosing „proper“ keys

- Assumption: Key selection is done *properly*
  - What means properly?
  - Improper: leading to template collisions – can be spotted using $D_{\leftrightarrow}^{sys}$

Proper Keys, $D_{\leftrightarrow}^{sys} = 0.02$



Improper Keys, $D_{\leftrightarrow}^{sys} = 0.45$



[S. Kirchgasser & A. Uhl, Proc. BIOSIG 2022]

Summary

Main BTP Requirements

- Do the stored templates reveal any information about the original biometric samples? — IRREVERSIBILITY
- Are my enrolled templates in different recognition systems somehow related to each other? — UNLINKABILITY
- What if someone steals a template extracted from my face? Has it been permanently compromised? — RENEWABILITY

[ISO/IEC IS 24745 on Biometric Information Protection]

[ISO/IEC IS 30136 on Performance Testing of BTP Schemes]

References

- M. Gomez-Barrero, J. Galbally. “Reversing the irreversible: A survey on inverse biometrics” Computers & Security, vol. 19, pp. 101700, 2020
- M. Gomez-Barrero, J. Galbally, C. Rathgeb, C. Busch, “General Framework to Evaluate Unlinkability in Biometric Template Protection Systems”, *IEEE Trans. on Information Forensics and Security*, vol. 3, no. 6, pp. 1406-1420, 2018
- M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, J. Fierrez, “Unlinkable and irreversible biometric template protection based on Bloom filters”, *Information Sciences*, vol. 370-371, pp. 18-32, 2016
- M. Gomez-Barrero, C. Rathgeb, G. Li, R. Raghavendra, J. Galbally, C. Busch, “Multi-Biometric Template Protection Based on Bloom Filters”, *Information Fusion*, vol. 42, pp. 37-50, 2018
- S. Kirchgasser, A. Uhl, “Template Protection: On the need to adapt the current Unlinkability Evaluation Protocol”, Proc. BIOSIG, 2022
- ISO/IEC 24745 on Biometric information protection
- ISO/IEC 30136 on Performance testing of biometric template protection schemes - **IN REVISION!!!**
- S. Rane, “Standardization of biometric template protection”, *IEEE MultiMedia*, vol. 21, no. 4, pp. 94-99, 2014
- **Handbook of Biometric Template Protection, Springer, eds. V. Krivokuca Hahn, M. Gomez-Barrero, A. Ross, S. Marcel, 2025 (soon)**
  - **EAB Workshop on BTP on October 29 and 30, 2025**

Research Institute
Cyber Defence
Universität der Bundeswehr München

BioML

BioML Lab

Marta Gomez-Barrero

marta.gomez-barrero@unibw.de

https://www.marta-gomez-barrero.com/
https://www.unibw.de/bioml-en