Privacy Enhancing Technology for Biometric Data

Christoph Busch / Marta Gomez-Barrero

Hochschule Darmstadt

12.07.2018

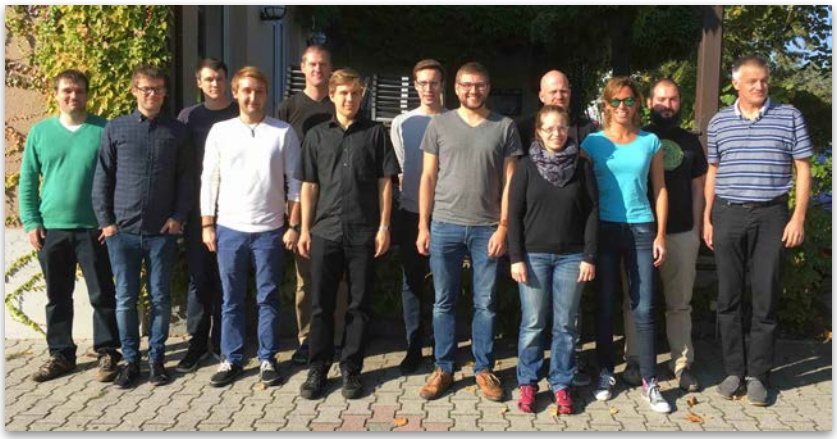
da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

CRISP
Center for Research
in Security and Privacy

Research Team

da/sec - Biometrics and Internet-Security Research Group

- Faculty-Members / PostDocs:
  - Harald Baier
  - Christoph Busch
  - Christian Rathgeb
  - Marta Gómez-Barrero
- PhD-Students:
  - Andreas Nautsch
  - Hareesh Mandalapu
  - Jannis Priesnitz
  - Jascha Kolberg
  - Lorenz Liebler
  - Nicolas Buchmann
  - Pawel Drozdowski
  - Thomas Göbel
  - Ulrich Scherhag
  - Jessica Steinberger

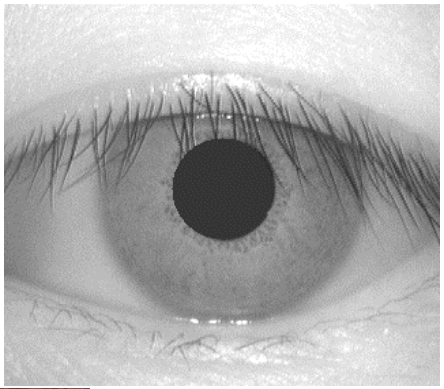


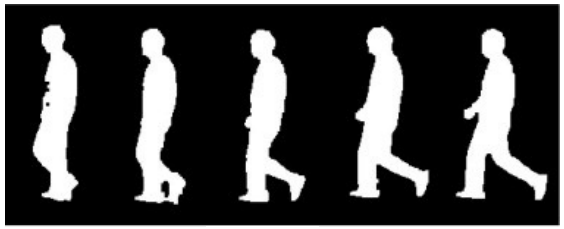
2017

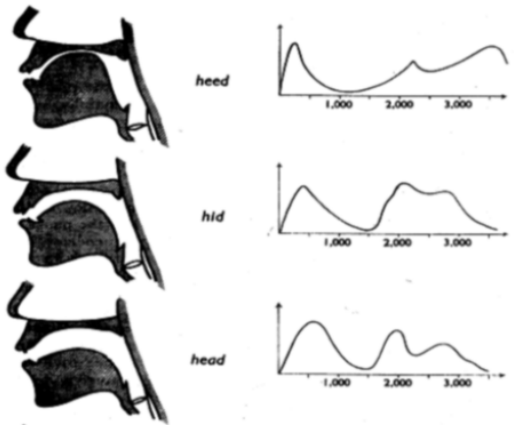
- Key-factors - since 2009:
  - 2 European funded projects,
    10 German funded projects
    5 research projects funded by the German BSI,
    2 industrial projects,
  - cooperated with > 30 research partners
  - more than 300 peer-reviewed publications

Research on Biometrics

- International Organization for Standardization defines:
  - **Biometrics**:
    "*automated recognition of individuals based on their behavioural and biological characteristics* "
  - Remark: behavioural has to do with the function of the body
    biological / anatomical has to do with the structure of the body







General Data Protection Regulation

European Data Protection Positions

What is Biometric data from a data protection perspective?

- Biometric data in whatever form (captured sample, template) is clearly personal data
- It may be sensitive data?

Sensitive Data

- Article 9 of GDPR listed the following special categories of data that demand specific additional attention.
  - racial or ethnic origin,
  - political opinions, religious or philosophical beliefs,
  - or trade union membership,
  - the processing of genetic data,
  - biometric data for the purpose of uniquely identifying a natural person,
  - data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Sensitive Data regarding Health in Biometric Samples

Health Information from Hand Patterns

Limited intellectual capabilities are correlated with a certain hand pattern

- Down syndrome (aka Trisomy 21) - Simian crease
  "*A simian crease is defined as fusion is defined as fusion of the proximal and distal transverse palmar creases into single transfers palmar crease.*" [Pur1972]
- Roseola - Sydney line
  "*A sydney line occurs where the proximal transverse crease extends beyond the midline axis of the fifth finger towards the ulnar border of the palm.*" [Pur1972]

Normal flexion crease

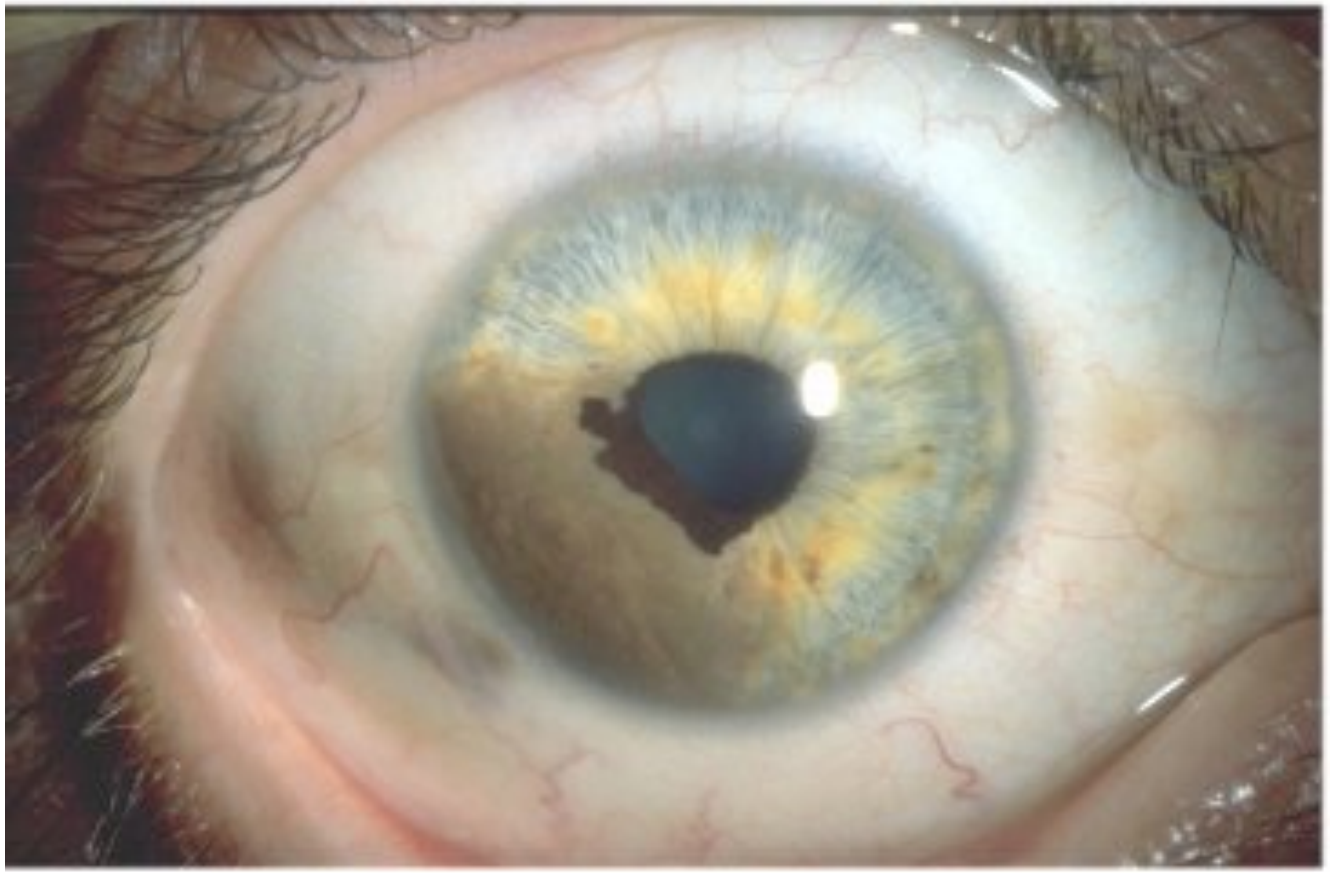
Simian crease

Sydney line

[Pur1972] S.G. Purvis-Smith: „The Sydney Line: A significant Sign in Downs Syndrome", Australian Paediatric Journal, 8:198-200, (1972)

Health Information from Iris Patterns

Malign melanom



Source: Online Journal of Ophthalmology

Issues with Data Storage

Secure Data Storage?

An incident: http://money.cnn.com/2015/09/23/technology/opm-fingerprint-hack

September 23, 2015: 12:34 PM ET

It's becoming painfully clear that the massive theft of federal personnel records is worse than previously thought.

On Wednesday, the Office of Personnel Management said hackers stole 5.6 million fingerprints it had on file. That's significantly higher than the agency's original estimate of 1.1 million fingerprints.

This is extremely sensitive information that poses an immediate danger to American spies and undercover law enforcement agents.

As an OPM spokesman told CNNMoney in July: "It's across federal agencies. It's everybody."

Hackers now have a gigantic database of American government employee fingerprints which can be used to positively identify the true identities of those employees.

Secure Data Storage?

An incident: http://money.cnn.com/2015/09/23/technology/opm-fingerprint-hack

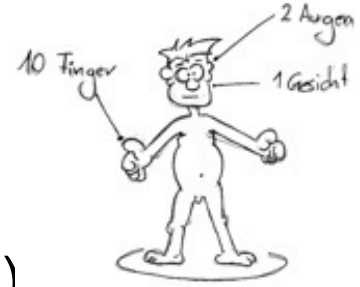
- The consequence: presentation attack instruments can be produced easily

Risks for Biometric References

Possible attacks on reference data

- Additional information
  - almost for each biometric characteristic

- Renewability: The biometric characteristic can not be revised
  - Only 10 finger, 2 eyes, 1 face, ...
  - Once compromised, compromised for ever
  - For PW-based system you would expect renewal frequently (e.g. every 3 month)



- Cross-Comparison: Identical template can establish unwanted links for one individual between several databases

Is encryption of biometric references a sufficient level of protection?

Template Protection

Encryption of the reference?

Conventional cryptography yields two main drawbacks

- Shift of problem: the encrypted template will be secure only as long as the decryption key is unknown to the attacker.
- Decryption at authentication: the template needs to be decrypted during every authentication attempt since comparison cannot be directly performed in the encrypted domain.

Template Protection

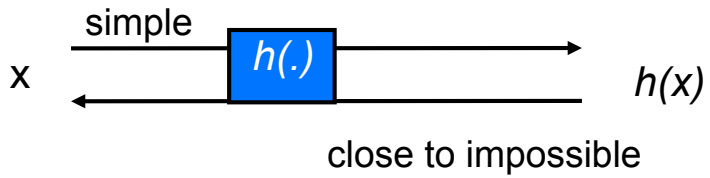
Hashing the reference?

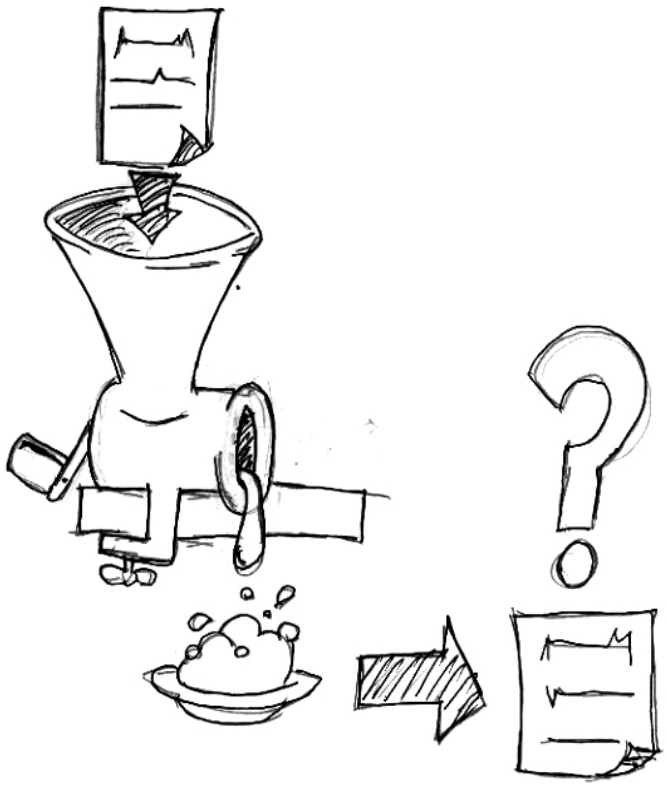
- Approach analog to UNIX Password authentication
- Public assessable file: /etc/passwd

```
id:<login_name>:hash(password)
```

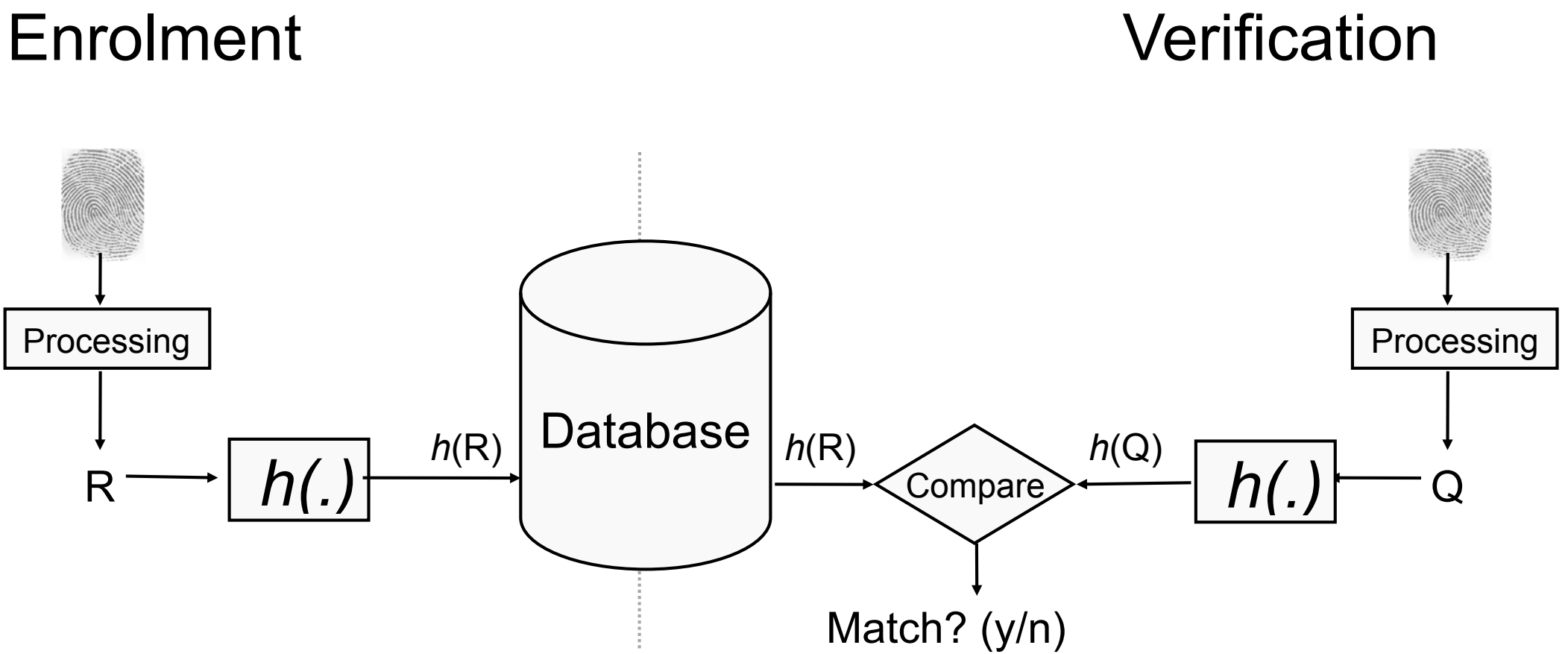
- Authentication:

```
hash(input) =?= hash(password)
```





Template Protection with Hash functions



h(.) = one-way hash function

Challenges

Difference between passwords and biometric samples

`h(01000101)` is not similar to `h(01010101)`

- Biometric measurements are influenced by noise
- Cryptographic one way functions are (by purpose) extremely sensitive to smallest changes in the input data

Classical hashing does not solve the problem either

Either we work with homomorphic encryption or we need a transformation

[Nau2018] Andreas Nautsch, S. Isadskiy, J. Kolberg, M. Gomez-Barrero, C. Busch, „Homomorphic Encryption for Speaker Recognition: Protection of Biometric Templates and Vendor Model Parameters“, in Proc. Odyssey, (June 2018).

Biometric Template Protection

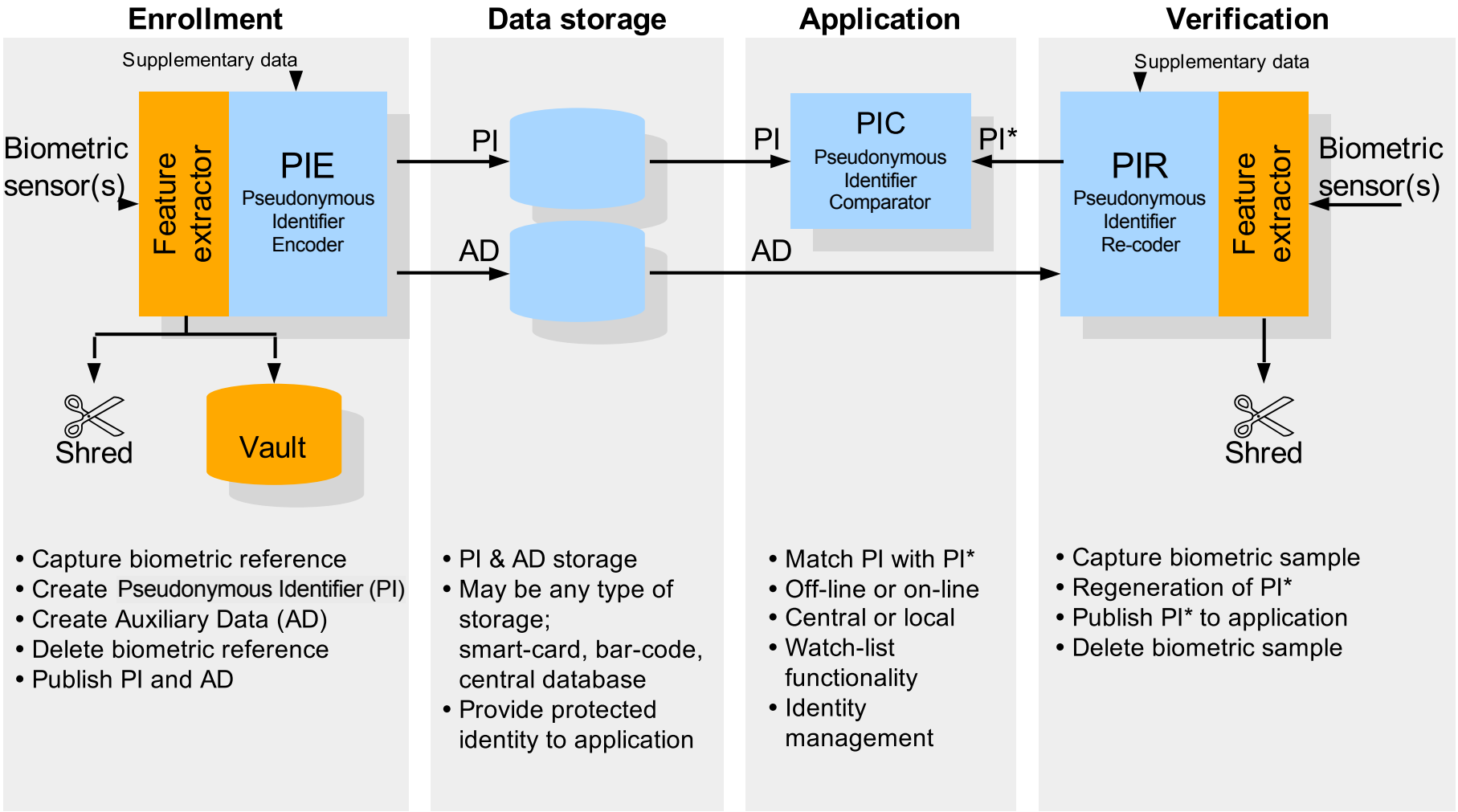
We do NOT store fingerprint, iris or face images

- we transform templates to pseudonymous identifiers (PI)
- we reach
  - Diversifiability / Unlinkability: Unique pseudonymous identifier can be created for each application to prevent database cross-comparison
  - Renewability: we can revoke and renew the reference data.
  - Non-invertibility: Original biometric sample can **not** be reconstructed
  - Secrecy: biometric references (PI) can be compared without decryption.

[Br2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: "A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008)
http://www.christoph-busch.de/files/Breebaart-BTPReferenceArchitecture-BIOSIG-2008.pdf

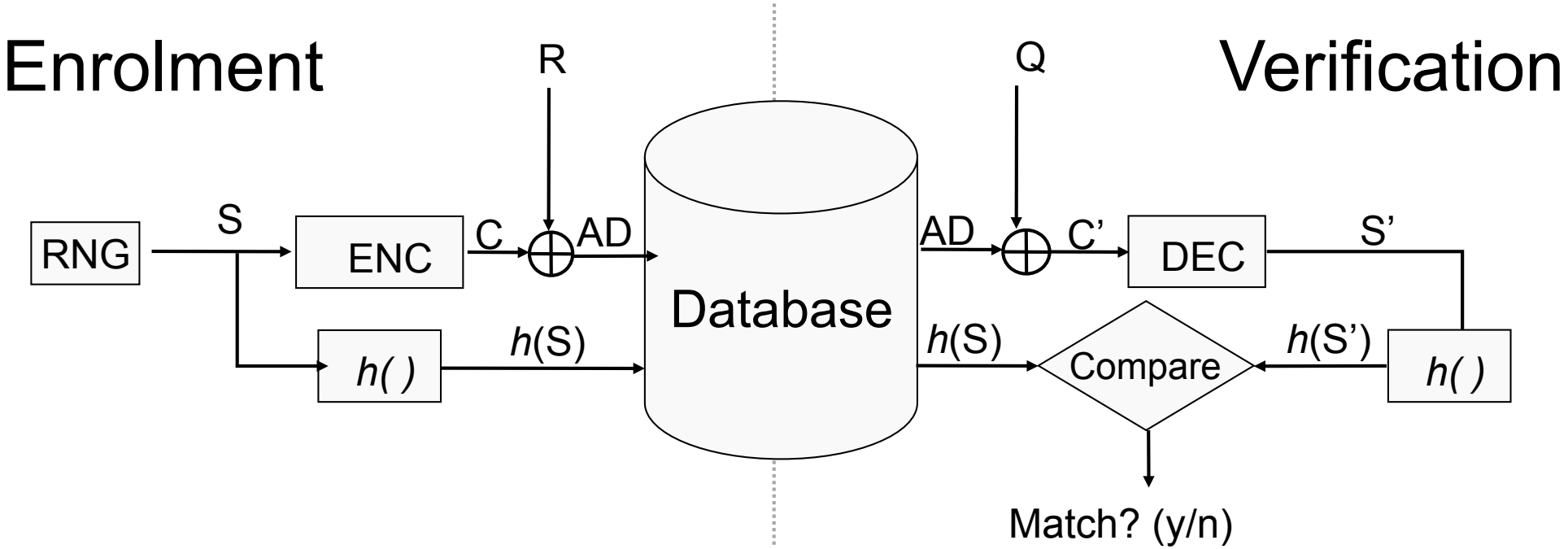
PI Framework in ISO/IEC 24745

- Standardized architecture
  for renewable biometric references



Biometric Cryptosystem

Fuzzy Commitment Scheme [Philips2006]

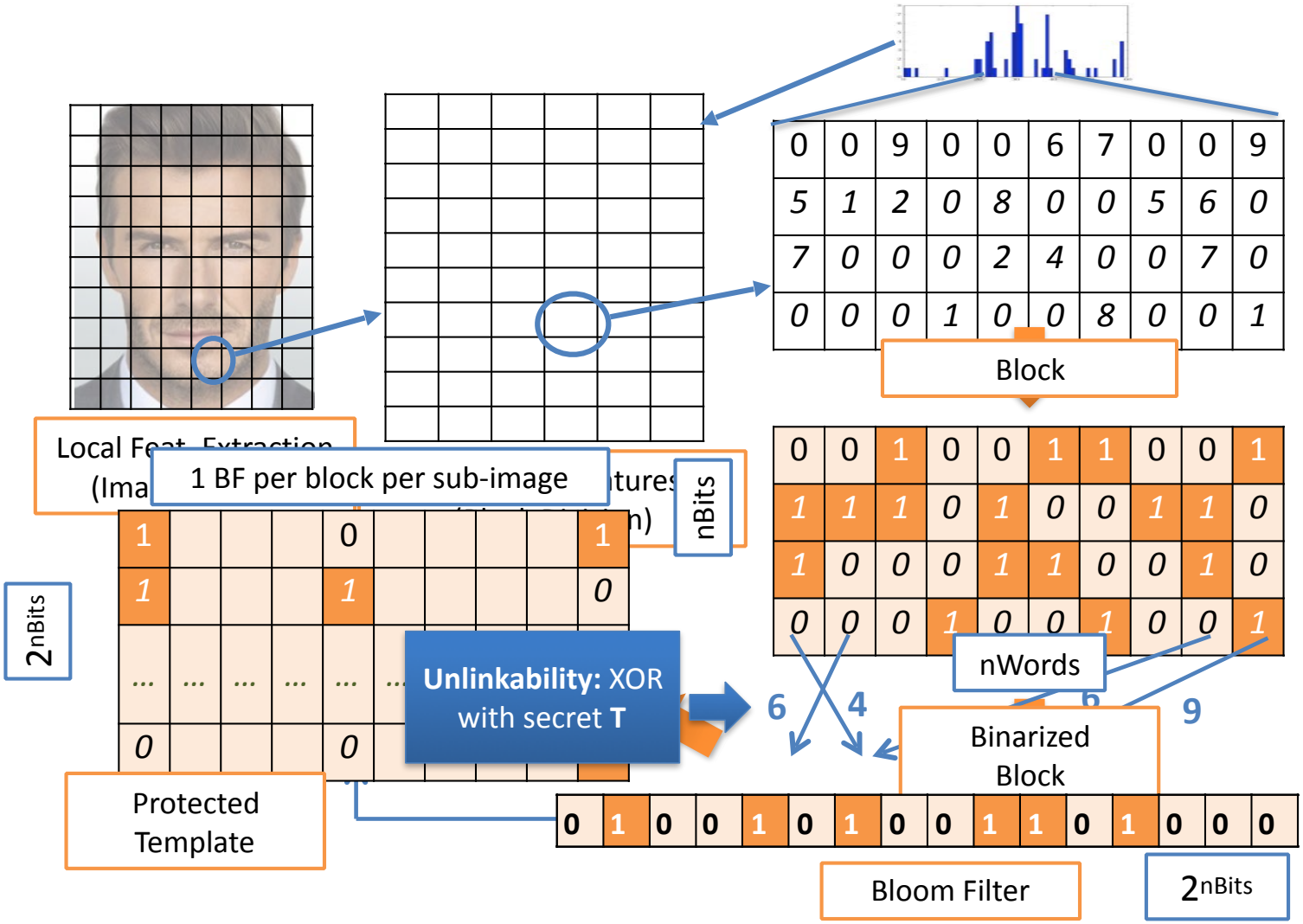


- R is the binary extract of feature vector F
- C is the codeword generated for random string S
- AD = C⊕R is the public helper data and { h(S), AD} are stored as reference
- C'=AD⊕Q is computed in the recognition process
  - Hamming Distance between C and C´ needs to be smaller than the error correction capabilities

Biometric Template Protection

Protection at the same accuracy level is possible

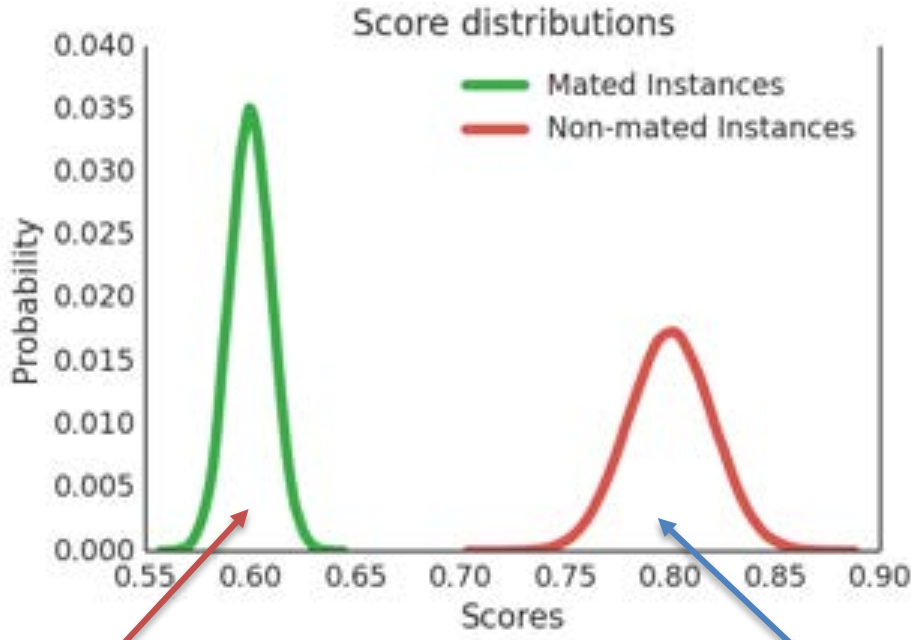
- Generating bloom filter-based pseudonymous identifiers



Linkage Attacks: how to?

T_{job} T_{bank}

$s = LS\ (T_{job}, T_{bank})$



s here ➔ success!! ☺

s here ➔ try again!! ☹

Measuring Linkability

Two measures:

- Local measure $D_{\leftrightarrow}(s)$ -> for which scores is the system vulnerable?
- Global measure $\mathrm{D}_{\leftrightarrow}^{sys}$ -> how can we benchmark two systems globally?

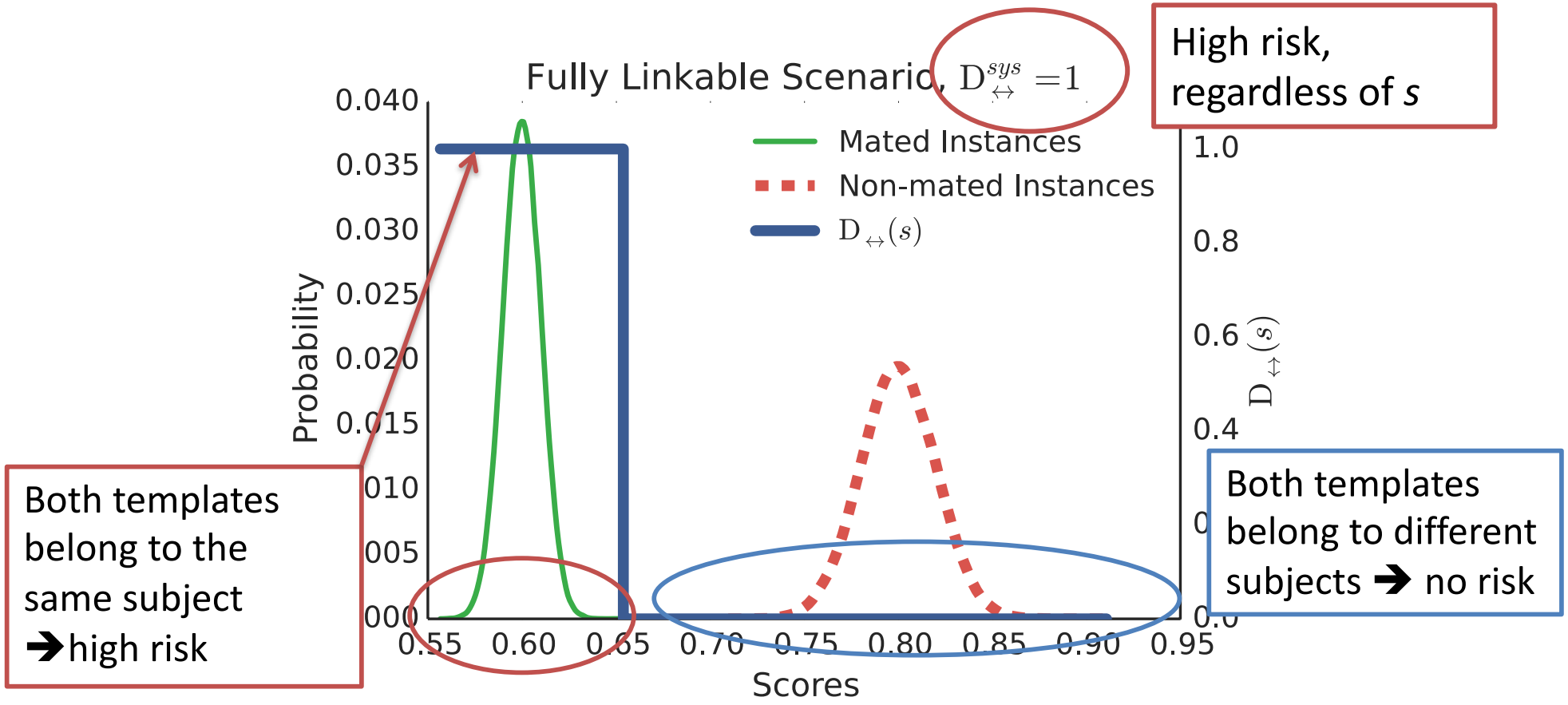
Both measures bounded in [0, 1] and defined for all possible linkage scores

General measure, valid for all BTP schemes

[Gomez-Barrero18a] 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, June 2018

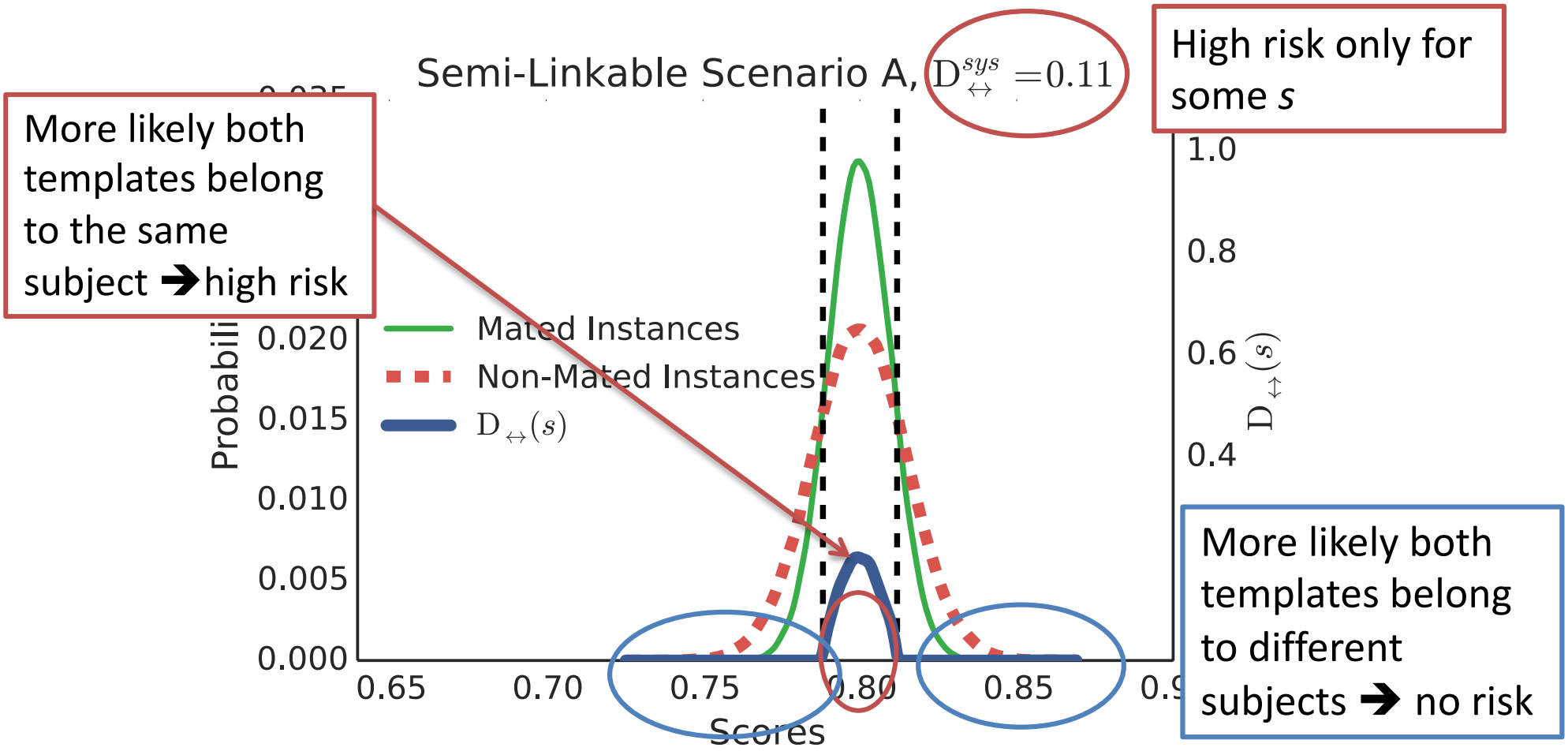
Measuring Linkability

Full Linkability



Measuring Linkability

Semi-Linkable Scenario



Measuring Linkability

The local measure evaluates:

$$D_{\leftrightarrow}(s) = p(H_m|s) - p(H_{nm}|s)$$

in terms of likelihood rates:

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

The global measure is defined as:

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

https://github.com/dasec/unlinkability-metric

Conclusion

Benefits and Applications

- Pseudonymous biometric databases which only consist of renewable biometric references (RBRs)
- Biometric-dependent key/PIN release,
  which could improve user convenience in eBanking
- Improvement of the public confidence and acceptance
  of biometrics, since most concerns against the common use of biometrics arise from the storage/misuse of biometric data
- Crossmatching-resistant RBRs prevent form tracking without consent in case biometric databases are compromised

Related Publications 2016-18

- M. Gomez-Barrero, C. Rathgeb, G. Li, R. Raghavendra, J. Galbally, C. Busch, „Multi-Biometric Template Protection Based on Bloom Filters“, in *Information Fusion*, Vol. 42, pp. 37-50, July 2018
- M. Gomez-Barrero, J. Galbally, C. Rathgeb, C. Busch, „General Framework to Evaluate Unlinkability in Biometric Template Protection Systems“, in *IEEE Trans. on Information Forensics and Security*, vol. 3, no. 6, pp. 1406-1420, June 2018
- M. Gomez-Barrero, J. Galbally, A. Morales, J. Fierrez, „Privacy-Preserving Comparison of Variable-Length Data with Application to Biometric Template Protection“, in *IEEE Access*, Vol. 5 (1), pp. 8606-8619, December 2017
- M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, J. Fierrez, „Multi-Biometric Template Protection Based on Homomorphic Encryption“, in *Pattern Recognition*, Vol. 67, pp. 149-163, July 2017
- M. Gomez-Barrero, C. Rathgeb, C. Busch, „Standardisierung von Biometric Template Protection: Aktueller Status und Bewertung der Verknüpfbarkeit“, in *Datenschutz und Datensicherheit* (DuD), Vol. 41, no. 7, pp. 422-426, July 2017.
- Y.L. Lai, Z. Jin, A. Teoh, B. Goi, W. Yap, T. Chai, C. Rathgeb, „Cancellable iris template generation based on Indexing-First-One hashing“, In Pattern Recognition, vol. 64, pp. 105-117, 2017.
- E. Martiri, M. Gomez-Barrero, B. Yang, C. Busch, „Biometric Template Protection Based on Bloom Filters and Honey Templates“, in *IET Biometrics*, Vol. 6 (1), pp. 19-26, January 2017.
- M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, J. Fierrez, „Unlinkable and irreversible biometric template protection based on Bloom filters“, in *Information Sciences*, Vol. 370-371, pp. 18-32, November 2016.
- J. Bringer, C. Morel, C. Rathgeb, „Security analysis and improvement of some biometric protected templates based on Bloom filters“, In Image and Vision Computing, 2016.
- C. Rathgeb, B. Tams, J. Wagner, C. Busch, „Unlinkable Improved Multi-Biometric Iris Fuzzy Vault“, In EURASIP Journal on Information Security, 2016.

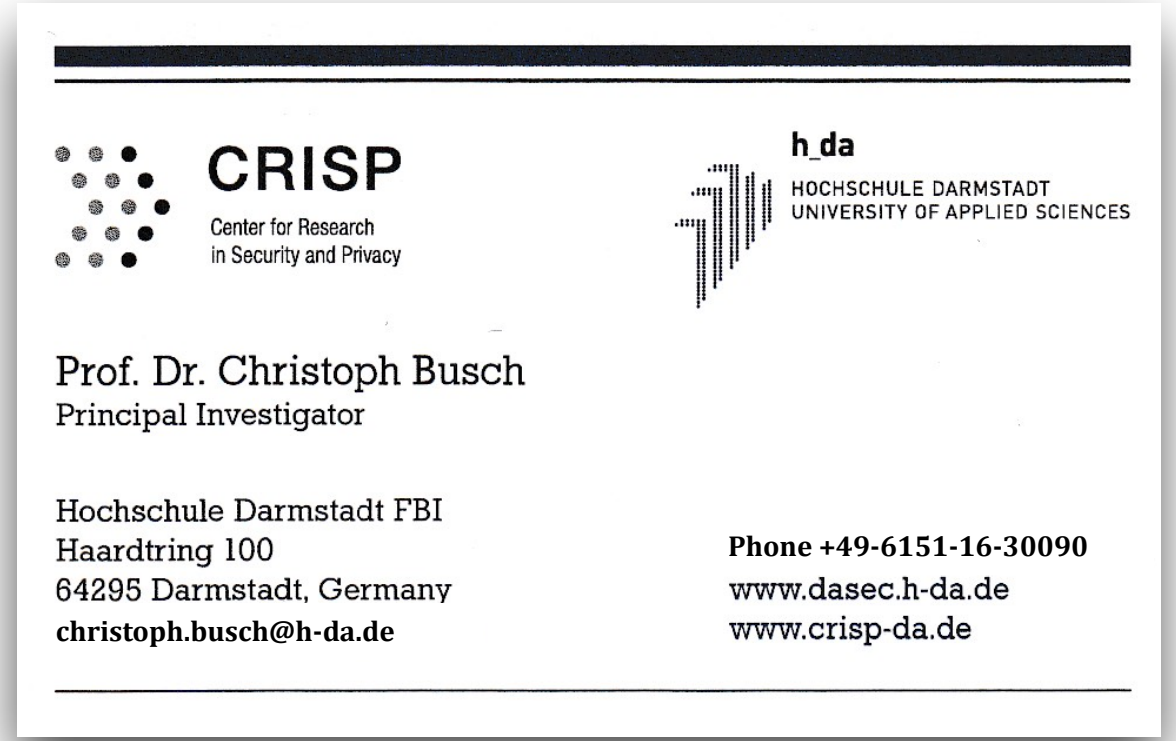
- A. Nautsch, S. Isadskiy, J. Kolberg, M. Gomez-Barrero, C. Busch, „Homomorphic Encryption for Speaker Recognition: Protection of Biometric Templates and Vendor Model Parameters“, in Proc. Odyssey, France, June 2018.
- M. Gomez-Barrero, C. Rathgeb, K. Raja, R. Raghavendra, C. Busch, „Biometric Symmetry: Implications on Template Protection“, in *Proc. European Signal Processing Conference* (EUSIPCO), Greece, August 2017
- P. Drozdowski, C. Rathgeb, C. Busch, „Bloom Filter-based Search Structures for Indexing and Retrieving Iris-Codes“, in IET Biometrics, 2017.
- P. Drozdowski, C. Rathgeb, C. Busch, „Multi-Iris Indexing and Retrieval: Fusion Strategies for Bloom Filter-based Search Structures“, in Proc. Int. Joint Conf. on Biometrics (IJCB), Denver, USA, October 2017

- C. Rathgeb, J. Wagner, Christoph Busch, „Iris Biometric Template Protection“, In Iris and Periocular Biometric Recognition, IET, 2017.

More Information

da/sec website:
https://dasec.h-da.de

Contact


CRISP
Center for Research
in Security and Privacy
h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
Prof. Dr. Christoph Busch
Principal Investigator
Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@h-da.de
Phone +49-6151-16-30090
www.dasec.h-da.de
www.crisp-da.de