Privacy Protection

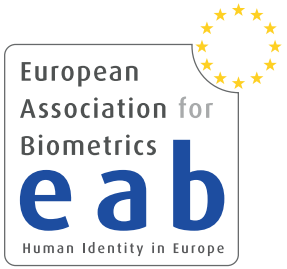
Christoph Busch

Hochschule Darmstadt / Norwegian University of Science and Technology

International Summer school for advanced studies on biometrics

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

ATHENE



NORWEGIAN BIOMETRICS LABORATORY

NTNU

Overview

Structure of this session

- Privacy protection culture
- Secure data storage - systems on card
- Attacks
- Biometric template protection

Privacy Protection Principles

What is the Perspective?

Data Privacy Culture differs

- European Countries:
  - Biometric data is owned by the data subjects,
    who determine the use and disclosure of their personal data
    (right of informational self-determination)
- non-European Countries (e.g. USA):
  - Biometric data is owned by the organization
    that processed the data

Legal & Regulatory Framework for Biometrics

Council of Europe

- Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981
  - Article 2 - Definitions:
    - *personal data means any information relating to an identified or identifiable individual ("data subject")*
    - *automatic processing includes the following operations if carried out in whole or in part by automated means: storage of data, ... retrieval or dissemination;*
    - *controller of the file means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, ... which operations should be applied to them.*

Legal & Regulatory Framework for Biometrics

EU legal Framework

- General Data Protection Regulation (GDPR)
  - Regulation 2016/679
    https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Reform aimed to make the rules clearer and more consistent by replacing the former patchwork of national laws with one, common EU-law.
- Rules apply to all companies targeting EU consumers, regardless of whether they are established inside or outside the EU
- Obligations of data controllers and processors are adjusted to the size of the business and/or the nature of the data being processed, in order to avoid burden for smaller companies.

Image Source: https://www.flaticon.com (2020)

Legal & Regulatory Framework for Biometrics

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.

Legal & Regulatory Framework for Biometrics

GDPR Recital 51

- *Personal data which are, …The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, …*

Image Source: https://www.tfeconnect.com (2020)

Image Source: https://www.verwaltung-der-zukunft.org/ (2020)

EU - Data Protection Principles

Criteria for processing biometric data:

- Proper legal basis for processing must exists
  - for example, data subject has unambiguously given consent
    OR
    compliance with legal obligation

Image Source: https://www.flaticon.com (2020)

- Fallback principle
  - Non-discriminatory systems
  - the data controller shall not condition the access to its services to the acceptance of the biometric processing
  - when used for authentication purpose, the data controller must offer an alternative solution (without biometrics)

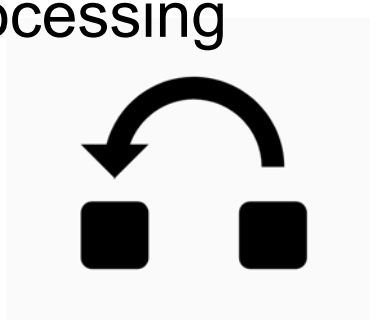


Image Source: https://thenounproject.com (2020)

EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Purpose binding / finality principle
  - personal data may be used only for the purpose they were originally collected for
  - personal data shall not further be processed in a manner that is incompatible with those purposes
- Accuracy principle
  - personal data shall be accurate and kept up to date
  - every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

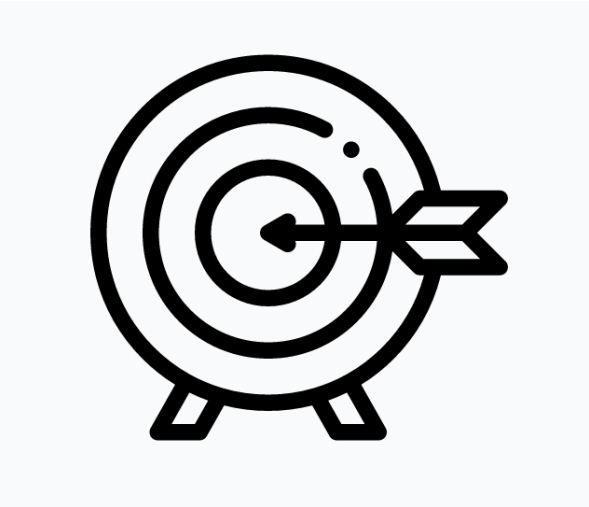


Image Source: https://www.flaticon.com (2020)

EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Proportionality in relation to interference
  - personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected
  - process is necessary to fulfill the purpose of the system

Image Source: https://www.flaticon.com (2020)

EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Data minimization principle
  - Storage limitation with automatic routines for deletion
  - Personal data to be deleted or anonymized as soon as possible:
    data must be kept ... for no longer than is necessary
    for the purposes for which the data were collected

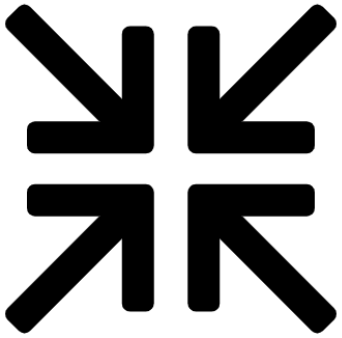


Image Source: https://www.flaticon.com (2020)

EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Transparency principle
  - It needs to be transparent for the data subject when and which data are collected and processed and for which purposes
  - data subjects should be informed, who is collecting their data
- Accountability principle
  - The controller is responsible for, and must be able to document, compliance with the regulations.

Image Source: https://www.flaticon.com (2020)

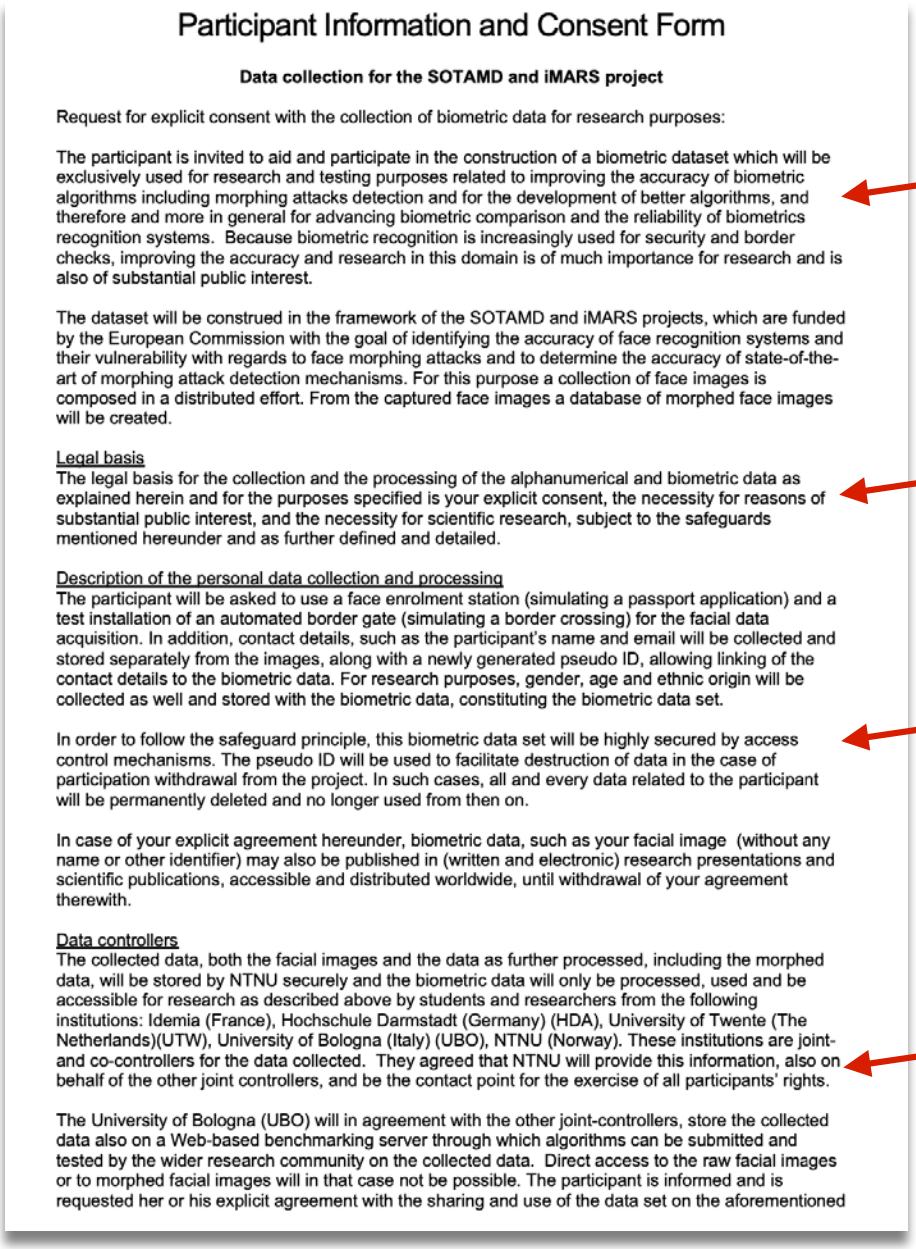
EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Protection of sensitive personal data
  - processing of sensitive data (e.g. concerning health) prohibited
- Integrity and confidentiality
  - Personal data shall be secured against unauthorized or illegal access and against accidental loss, destruction or damage.
- Safeguard principle
  - *controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access*

Image Source: https://www.flaticon.com (2020)

A Consent Form - Example



Participant Information and Consent Form

Data collection for the SOTAMD and iMARS project

Request for explicit consent with the collection of biometric data for research purposes:

The participant is invited to aid and participate in the construction of a biometric dataset which will be exclusively used for research and testing purposes related to improving the accuracy of biometric algorithms including morphing attacks detection and for the development of better algorithms, and therefore and more in general for advancing biometric comparison and the reliability of biometrics recognition systems. Because biometric recognition is increasingly used for security and border checks, improving the accuracy and research in this domain is of much importance for research and is also of substantial public interest.

The dataset will be construed in the framework of the SOTAMD and iMARS projects, which are funded by the European Commission with the goal of identifying the accuracy of face recognition systems and their vulnerability with regards to face morphing attacks and to determine the accuracy of state-of-the-art of morphing attack detection mechanisms. For this purpose a collection of face images is composed in a distributed effort. From the captured face images a database of morphed face images will be created.

Legal basis
The legal basis for the collection and the processing of the alphanumerical and biometric data as explained herein and for the purposes specified is your explicit consent, the necessity for reasons of substantial public interest, and the necessity for scientific research, subject to the safeguards mentioned hereunder and as further defined and detailed.

Description of the personal data collection and processing
The participant will be asked to use a face enrolment station (simulating a passport application) and a test installation of an automated border gate (simulating a border crossing) for the facial data acquisition. In addition, contact details, such as the participant's name and email will be collected and stored separately from the images, along with a newly generated pseudo ID, allowing linking of the contact details to the biometric data. For research purposes, gender, age and ethnic origin will be collected as well and stored with the biometric data, constituting the biometric data set.

In order to follow the safeguard principle, this biometric data set will be highly secured by access control mechanisms. The pseudo ID will be used to facilitate destruction of data in the case of participation withdrawal from the project. In such cases, all and every data related to the participant will be permanently deleted and no longer used from then on.

In case of your explicit agreement hereunder, biometric data, such as your facial image (without any name or other identifier) may also be published in (written and electronic) research presentations and scientific publications, accessible and distributed worldwide, until withdrawal of your agreement therewith.

Data controllers
The collected data, both the facial images and the data as further processed, including the morphed data, will be stored by NTNU securely and the biometric data will only be processed, used and be accessible for research as described above by students and researchers from the following institutions: Idemia (France), Hochschule Darmstadt (Germany) (HDA), University of Twente (The Netherlands)(UTW), University of Bologna (Italy) (UBO), NTNU (Norway). These institutions are joint- and co-controllers for the data collected. They agreed that NTNU will provide this information, also on behalf of the other joint controllers, and be the contact point for the exercise of all participants' rights.

The University of Bologna (UBO) will in agreement with the other joint-controllers, store the collected data also on a Web-based benchmarking server through which algorithms can be submitted and tested by the wider research community on the collected data. Direct access to the raw facial images or to morphed facial images will in that case not be possible. The participant is informed and is requested her or his explicit agreement with the sharing and use of the data set on the aforementioned

what is it about

the legal basis

purpose and safeguard

the data controller

A Consent Form - Example (cont.)

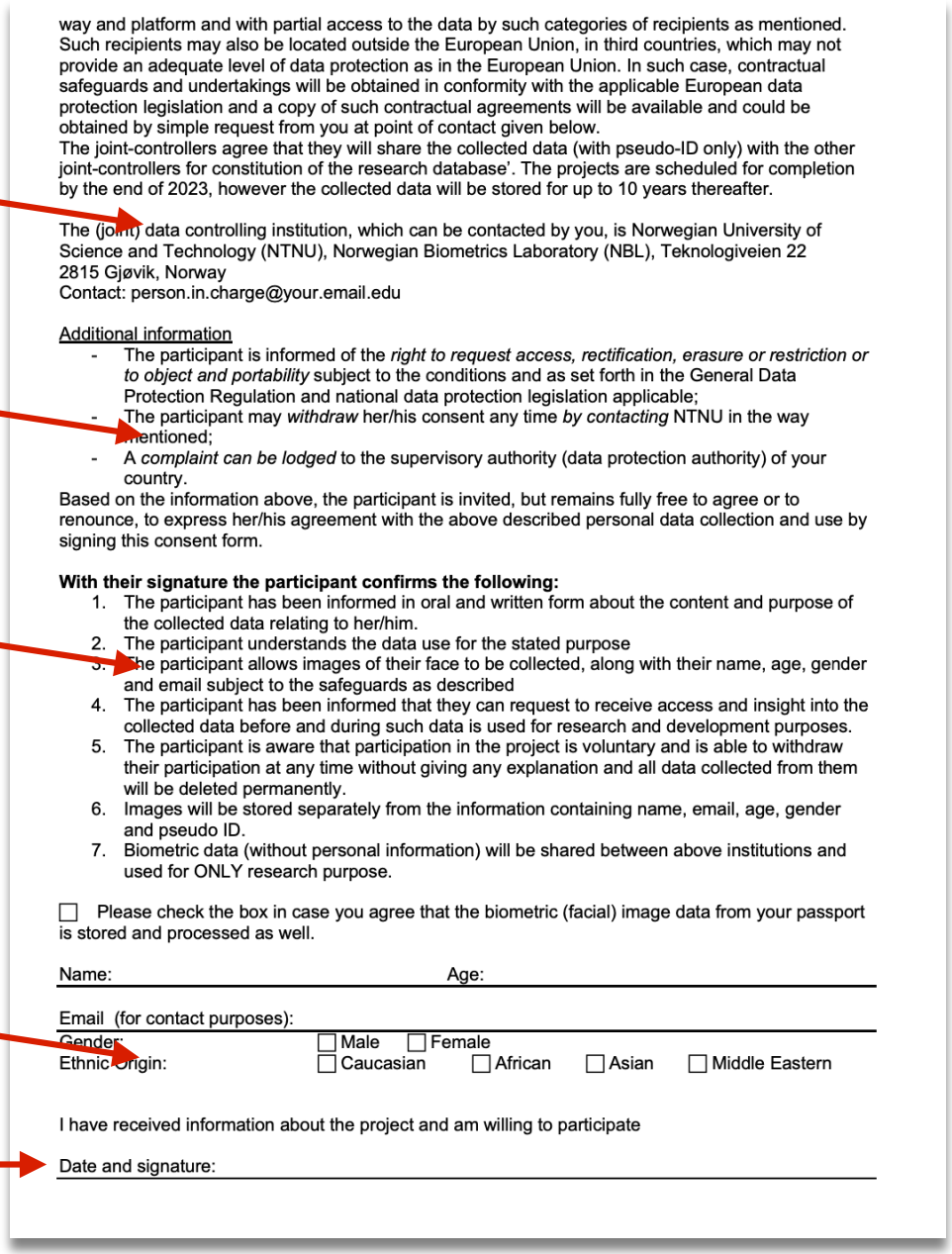
point of contact

right to withdraw

scope of agreement

alphanumerical data

signature



way and platform and with partial access to the data by such categories of recipients as mentioned. Such recipients may also be located outside the European Union, in third countries, which may not provide an adequate level of data protection as in the European Union. In such case, contractual safeguards and undertakings will be obtained in conformity with the applicable European data protection legislation and a copy of such contractual agreements will be available and could be obtained by simple request from you at point of contact given below.
The joint-controllers agree that they will share the collected data (with pseudo-ID only) with the other joint-controllers for constitution of the research database'. The projects are scheduled for completion by the end of 2023, however the collected data will be stored for up to 10 years thereafter.

The (joint) data controlling institution, which can be contacted by you, is Norwegian University of Science and Technology (NTNU), Norwegian Biometrics Laboratory (NBL), Teknologiveien 22
2815 Gjøvik, Norway
Contact: person.in.charge@your.email.edu

Additional information

- The participant is informed of the *right to request access, rectification, erasure or restriction or to object and portability* subject to the conditions and as set forth in the General Data Protection Regulation and national data protection legislation applicable;
- The participant may *withdraw* her/his consent any time *by contacting* NTNU in the way mentioned;
- A *complaint can be lodged* to the supervisory authority (data protection authority) of your country.

Based on the information above, the participant is invited, but remains fully free to agree or to renounce, to express her/his agreement with the above described personal data collection and use by signing this consent form.

With their signature the participant confirms the following:

1. The participant has been informed in oral and written form about the content and purpose of the collected data relating to her/him.
2. The participant understands the data use for the stated purpose
3. The participant allows images of their face to be collected, along with their name, age, gender and email subject to the safeguards as described
4. The participant has been informed that they can request to receive access and insight into the collected data before and during such data is used for research and development purposes.
5. The participant is aware that participation in the project is voluntary and is able to withdraw their participation at any time without giving any explanation and all data collected from them will be deleted permanently.
6. Images will be stored separately from the information containing name, email, age, gender and pseudo ID.
7. Biometric data (without personal information) will be shared between above institutions and used for ONLY research purpose.

☐ Please check the box in case you agree that the biometric (facial) image data from your passport is stored and processed as well.

Name: Age:

Email (for contact purposes):

Gender: ☐ Male ☐ Female
Ethnic Origin: ☐ Caucasian ☐ African ☐ Asian ☐ Middle Eastern

I have received information about the project and am willing to participate

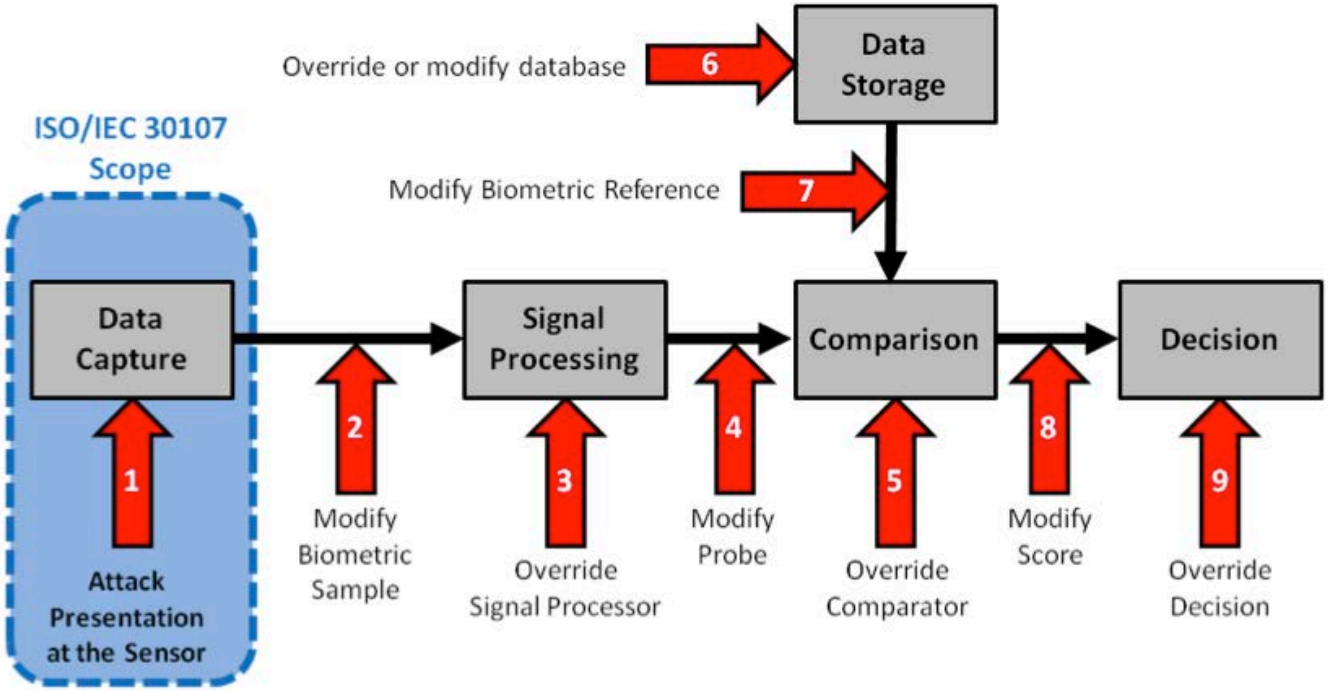
Date and signature:

Data Storage

Secure Data Storage

Two options to investigate

- Personal Card (RFID)
  - Store On Card
  - On Card Comparison
  - Sensor on Card
- Central databases



Source: ISO/IEC 30107-1:2016

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.

Sample Reconstruction

Inverse biometric attacks are underestimated risks

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

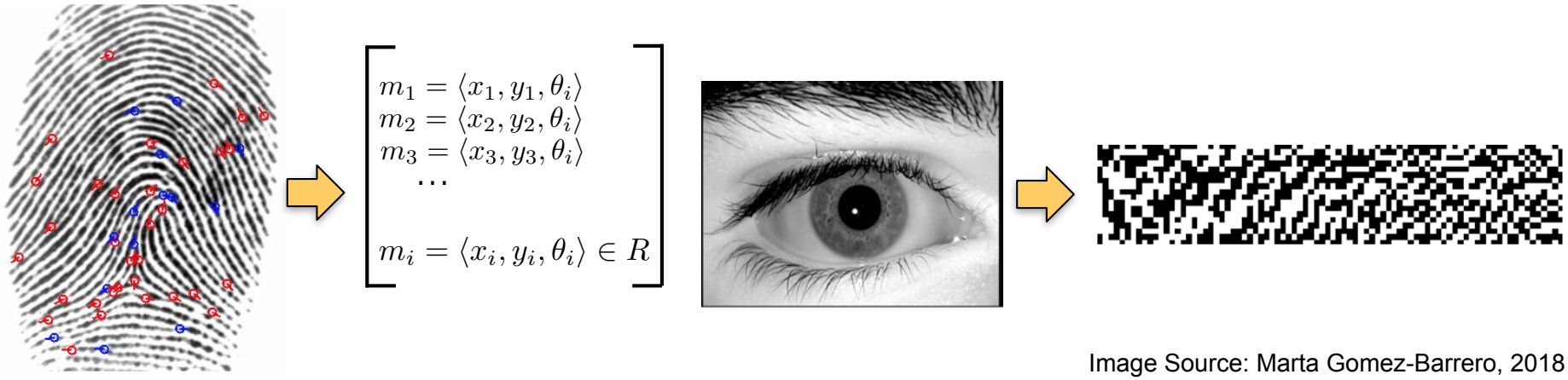


Image Source: Marta Gomez-Barrero, 2018

- Vendor's statement (some years back):
  "Our product is secure since it does store fingerprint minutiae and not fingerprint-image"
- However, biometric samples can be recovered from the stored unprotected templates

Sample Reconstruction

Inverse biometric attacks on minutia templates

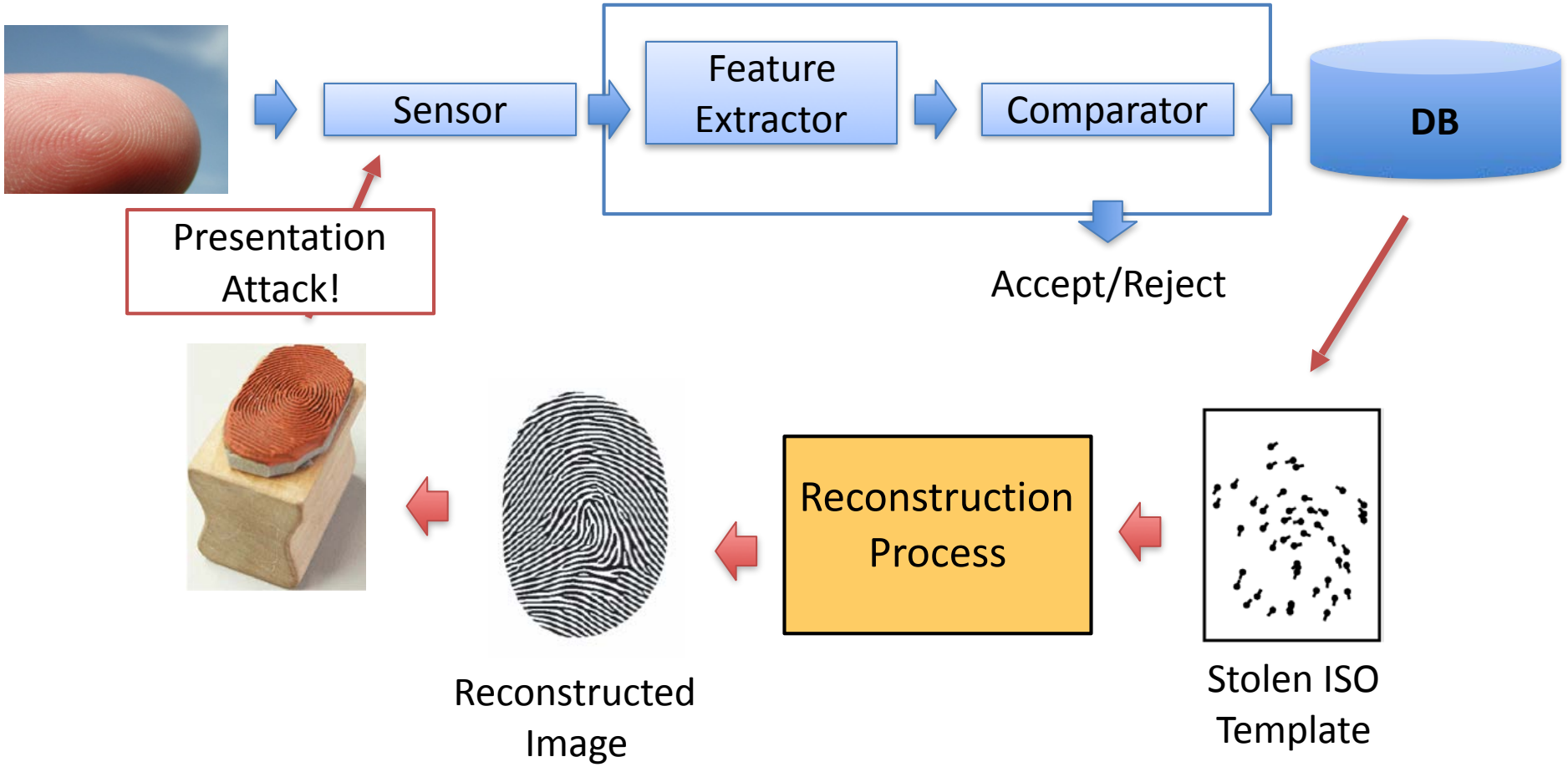


Image Source: Marta Gomez-Barrero, 2018

[Cappelli2007] R. Cappelli et al. „Fingerprint Image Reconstruction from Standard Templates“, in IEEE PAMI, (2007)

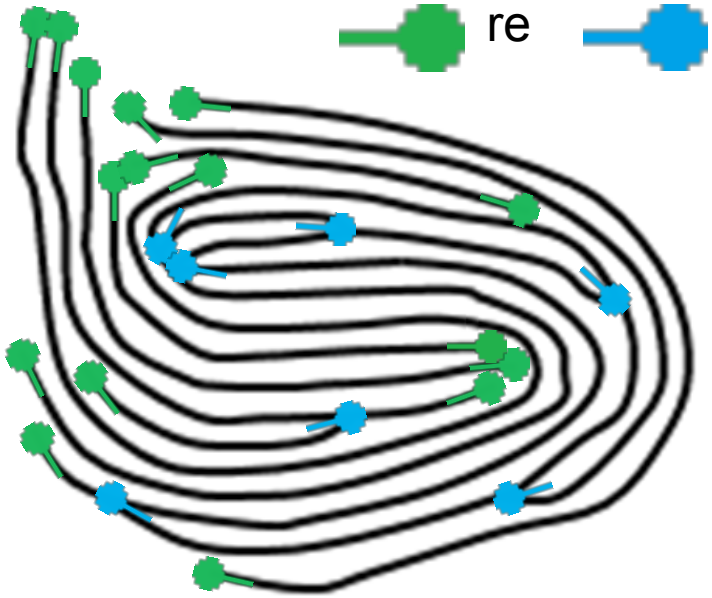
[Galbally2009] J. Galbally et al. „Template Reconstruction“, in Pattern Recognition Letters, (2009)

Sample Reconstruction

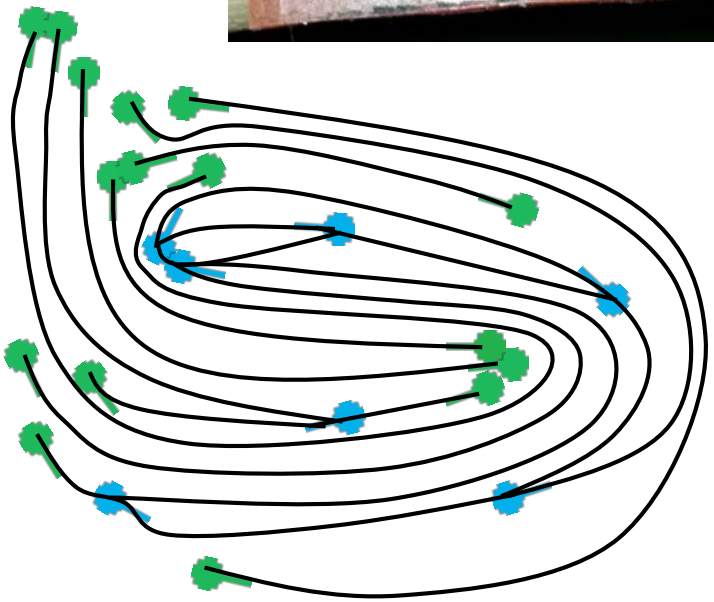
Processing the attack

We invert from fingerprint-minutia
to a sample that will grant access!

Sample reconstruction!



original sample



reconstructed sample

Sample Reconstruction

Approaches for face image reconstruction:

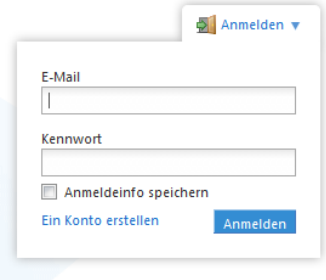
- Deep learning demonstrated the vulnerability of FR
- A neighbourly de-convolutional network can be used to reconstruct facial templates from FaceNet [Schroff2015]
- Over large open access databases, success rates over 73% and 95% are achieved [Mai2018]

[Schroff2015] Schroff et al. „FaceNet: A Unified Embedding for Face Recognition and Clustering“, in Proceedings CVPR, (2015)

[Mai2018] Mai et al. „On the Reconstruction of Face Images from Deep Face Templates“, in IEEE T-PAMI, (2018)

Biometric Template Protection

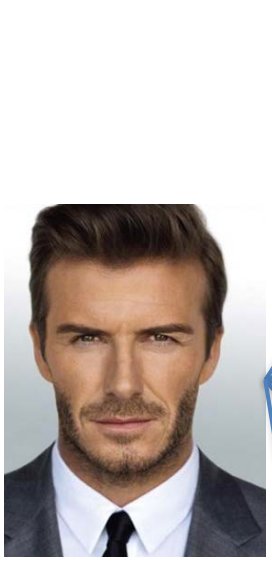
Benchmark of Authentication Methods

	Non-Invertibility from the reference	Revocability and Renewability	Strong link to the data subject
	✓ (?)	✓	✗
	✓	✓	✗
	✗	✗	✓

Further Risks for Biometric References

Cross-Comparison attacks

- We can enrol with a single biometric characteristic in different applications



T_{mail}

Santander CONSUMER BANK

T_{bank}

Employer

T_{job}

$T_{facebook}$

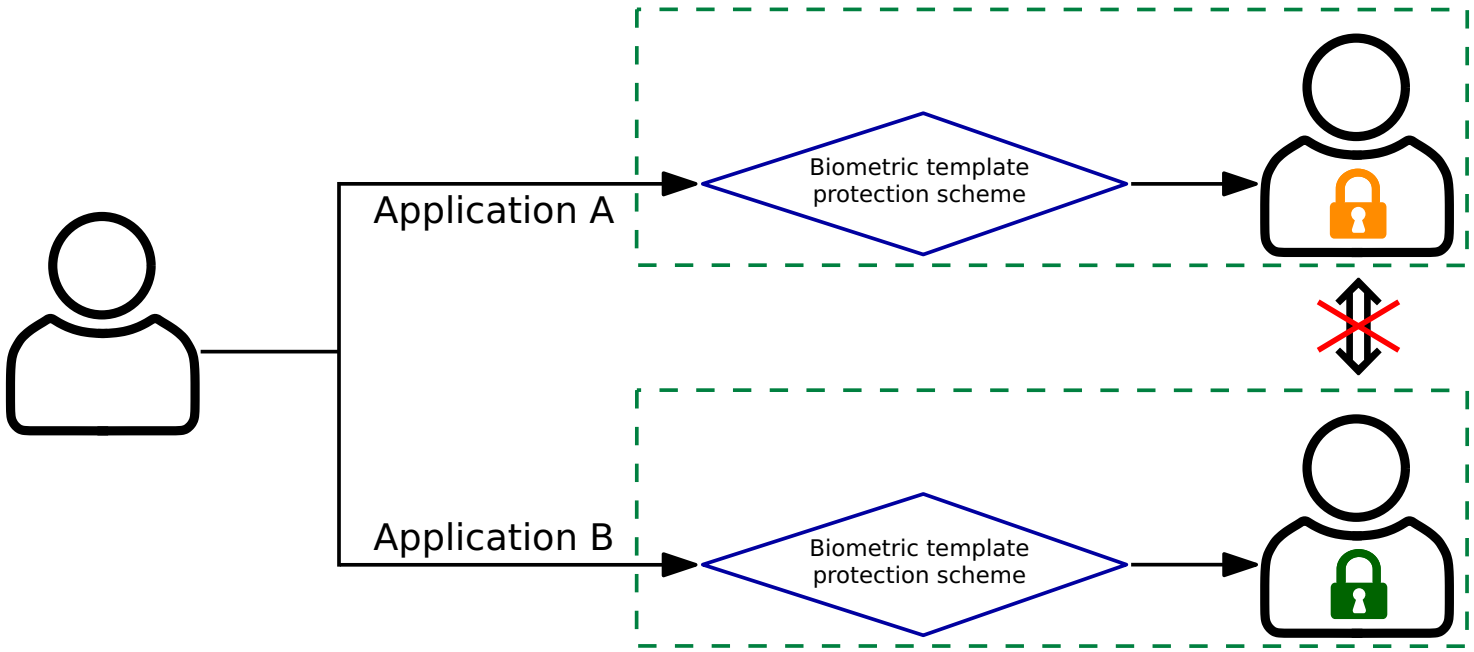
$T_{linkedin}$

Same subject??

Further Risks for Biometric References

Cross-Comparison attacks

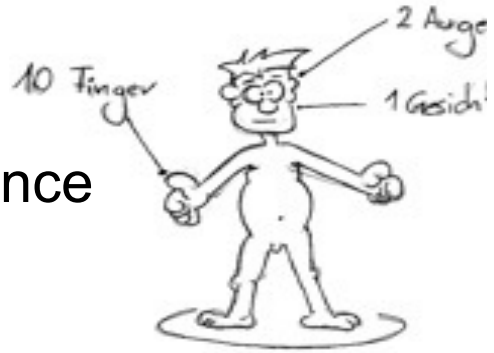
- Enrol with a single biometric characteristic in different applications
- Prevent the generation of profiles
  - Cross-correlating protected templates across different systems and databases must not be possible to avoid profiling



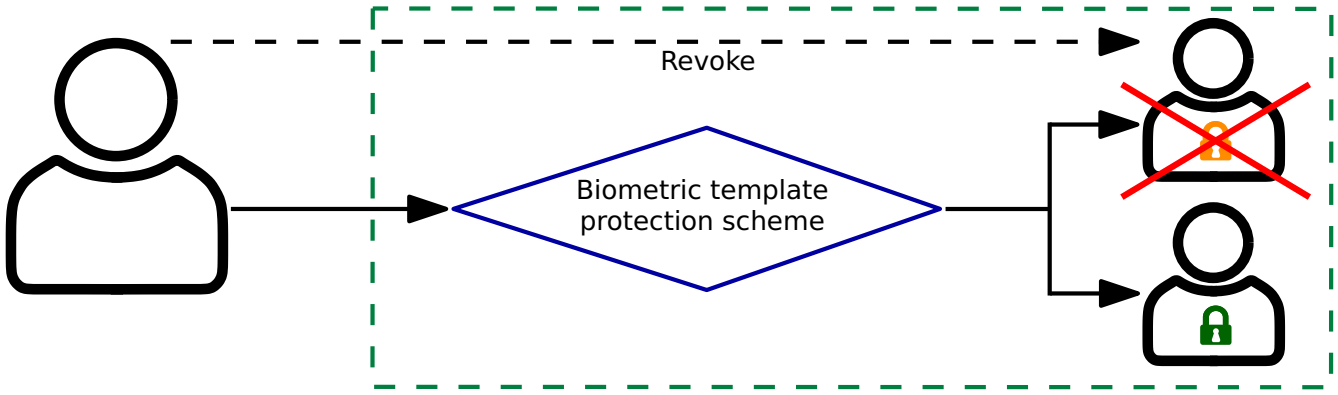
Further Risks for Biometric References

Leaking attacks against the reference data

- The biometric characteristic as such can not be revoked
  - Only 10 finger, 2 eyes, 1 face, ...
  - In case of being compromised, revoking and reissuing a new (different) protected biometric reference should be possible and straightforward.
  - For PW-based system you would expect renewal frequently (e.g. every 3 month)



We need renewability!



Further Risks for Biometric References

Summary: Possible attacks on reference data

- Cross-Comparison: Identical template can establish unwanted links for one individual between several databases
- Leaking references: The biometric characteristic can not be revoked
  - Only 10 finger, 2 eyes, 1 face, ...
  - we need to revoke and renew the biometric reference
- Disclosing additional information
  - almost for each biometric characteristic

Normal flexion crease

Simian crease

Is encryption of biometric references a sufficient level of template protection?

Template Protection

Encryption of the reference?

Conventional cryptography yields two main drawbacks

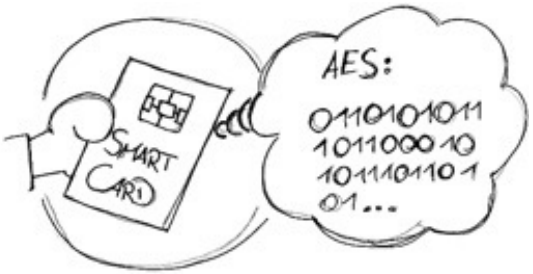
- Shift of problem: the encrypted template will be secure only as long as the decryption key is unknown to the attacker.
- Decryption at authentication: the template needs to be decrypted during every authentication attempt since comparison cannot be directly performed in the encrypted domain.
  - Adversary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

- Potential, but inconvenient 2 factor solution:
  - store the encrypted template and decryption key in a secure environment within a smart card or a secure chip.

Challenges

Classical crypto / encryption does not solve the problem

- Data needs to be decrypted prior to comparison



Template Protection

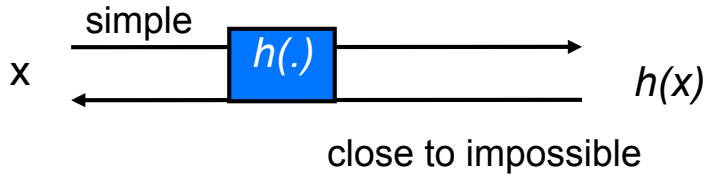
Hashing the reference?

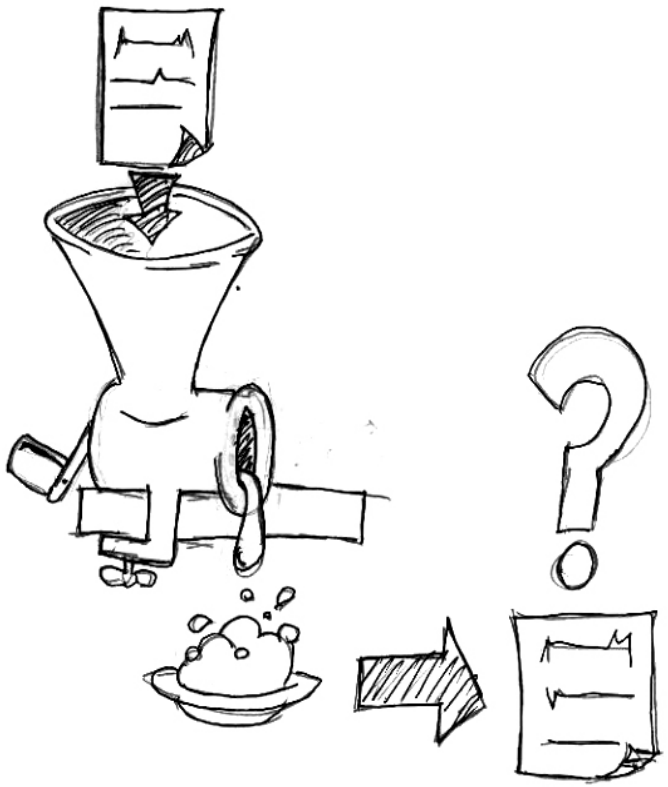
- Approach analog to UNIX Password authentication
- Public assessable file: /etc/passwd

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

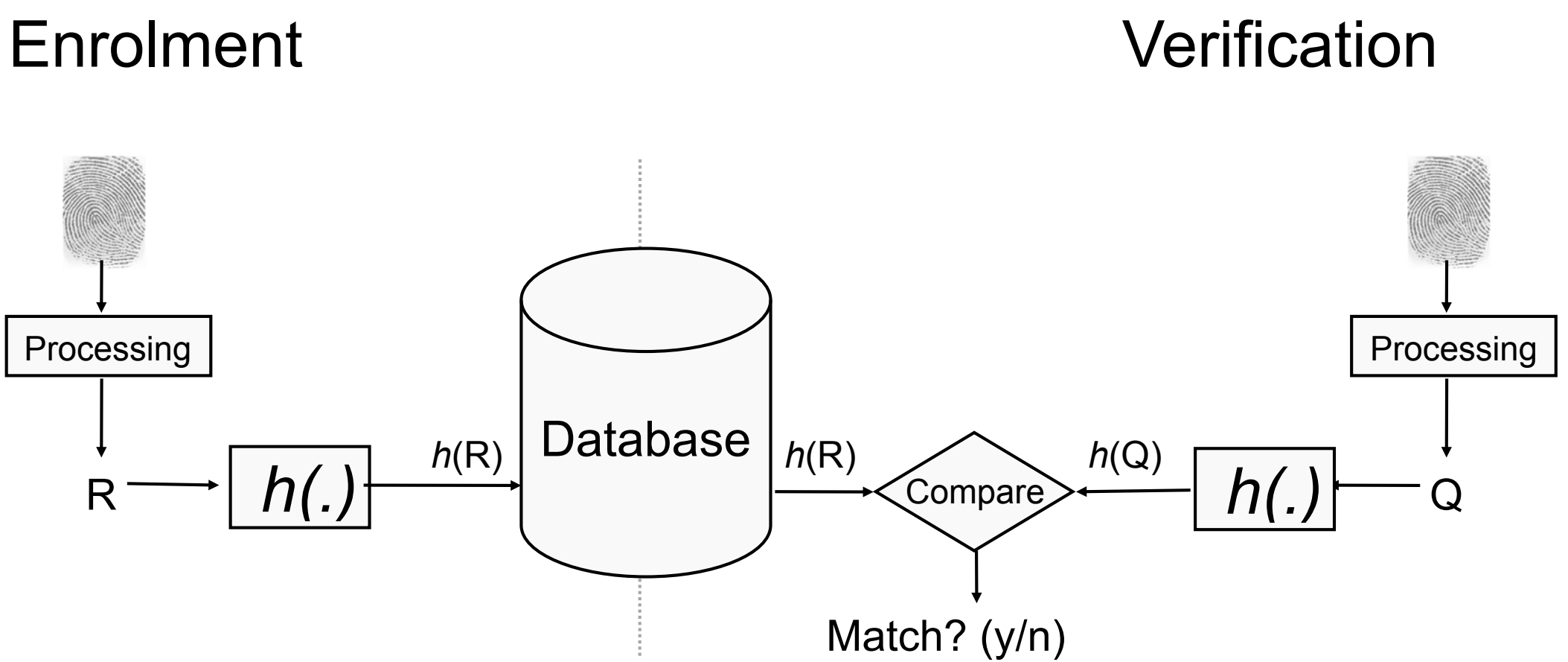
- Authentication:

```
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 crypto hashing does not solve the problem either

Biometric Template Protection

Preliminary conclusion

- We do NOT store fingerprint, iris or face images
- We do NOT store fingerprint, iris or face templates

But

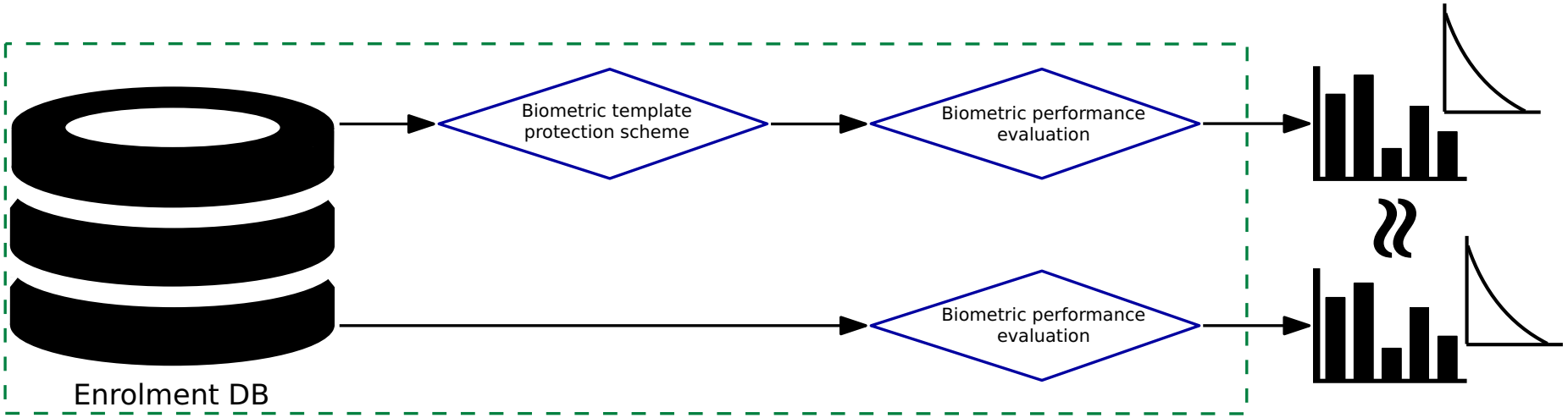
- we transform templates to pseudonymous identifiers (PI)
- we reach
  - Secrecy: biometric references (PI) can be compared without decryption.
  - Diversifiability / Unlinkability: Unique pseudonymous identifier can be created for each application to prevent database cross-comparison
  - Renewability: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

[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

Biometric Template Protection

Expectation

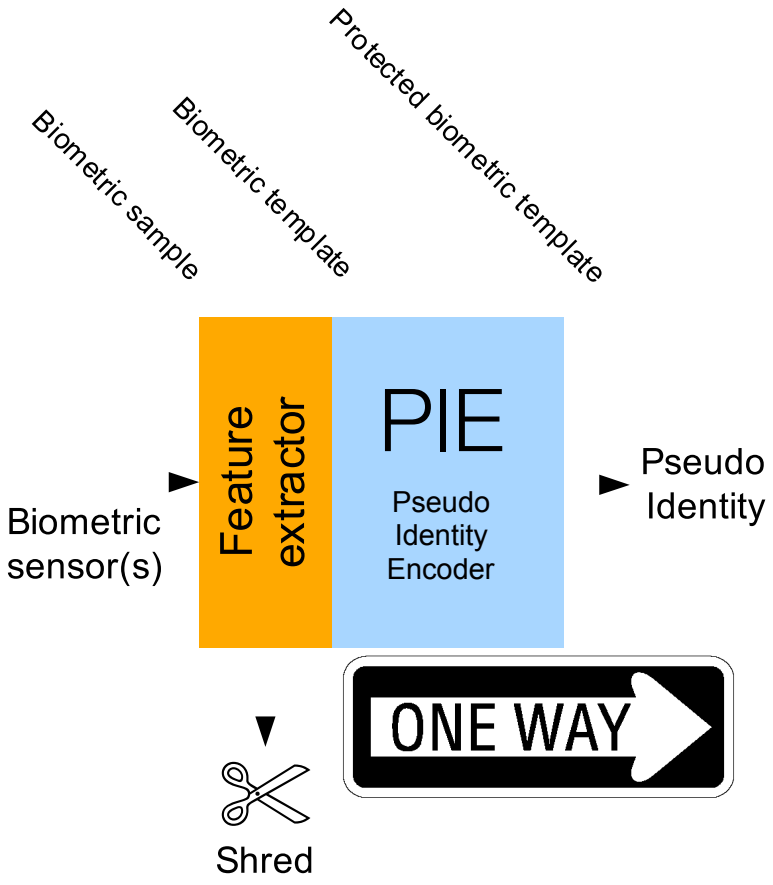
- The biometric performance of the protected system must not be (severely) impaired by the template protection scheme.



Pseudonymous Identifier Framework

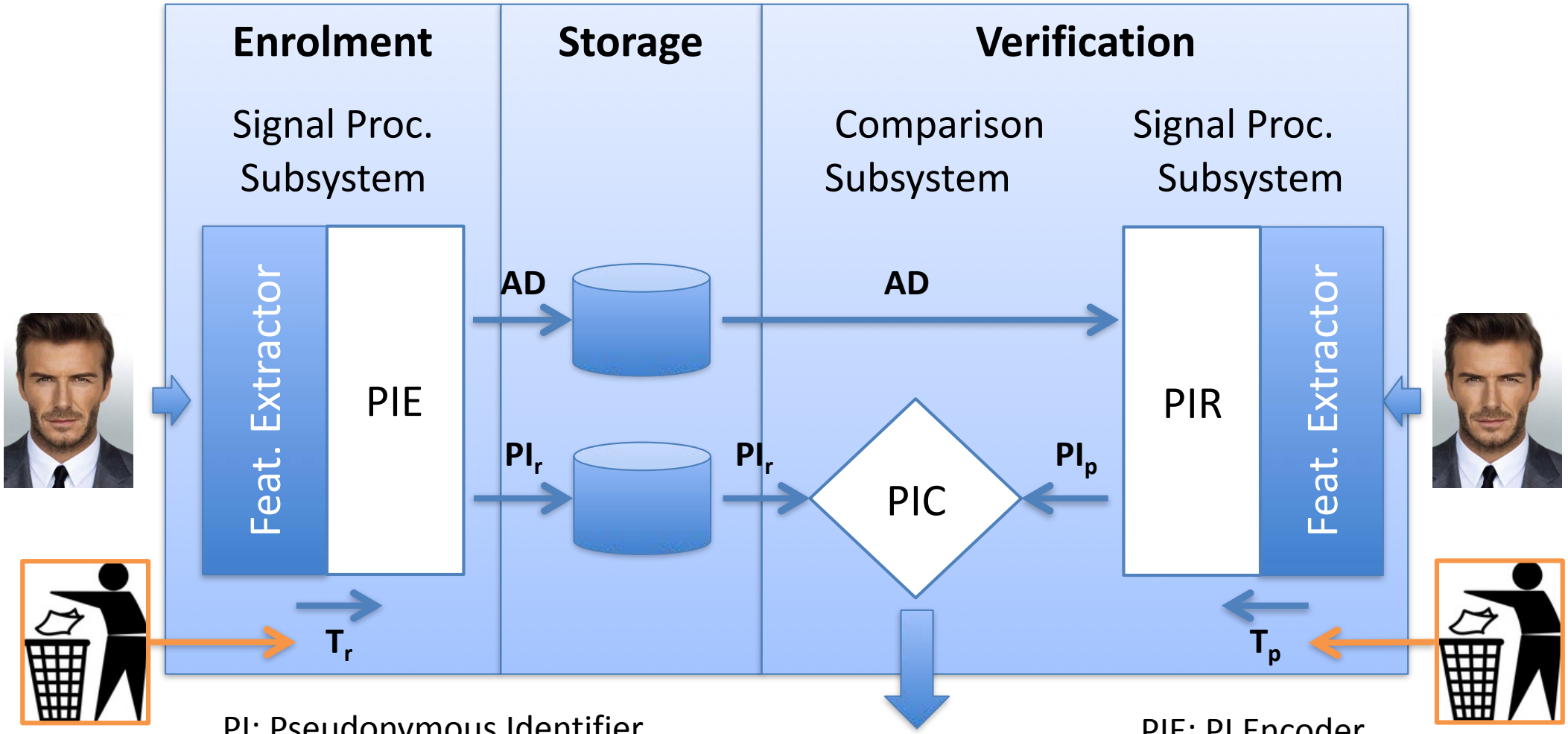
BTP Framework defined in ISO/IEC 24745

- Two-stage conversion of captured biometric samples to protected templates.
- Protected storage, transmission and comparison
  - Impossible to retrieve original biometric sample from protected template
  - A template represents identification data for a specific purpose or application *only*



Pseudonymous Identifier Framework

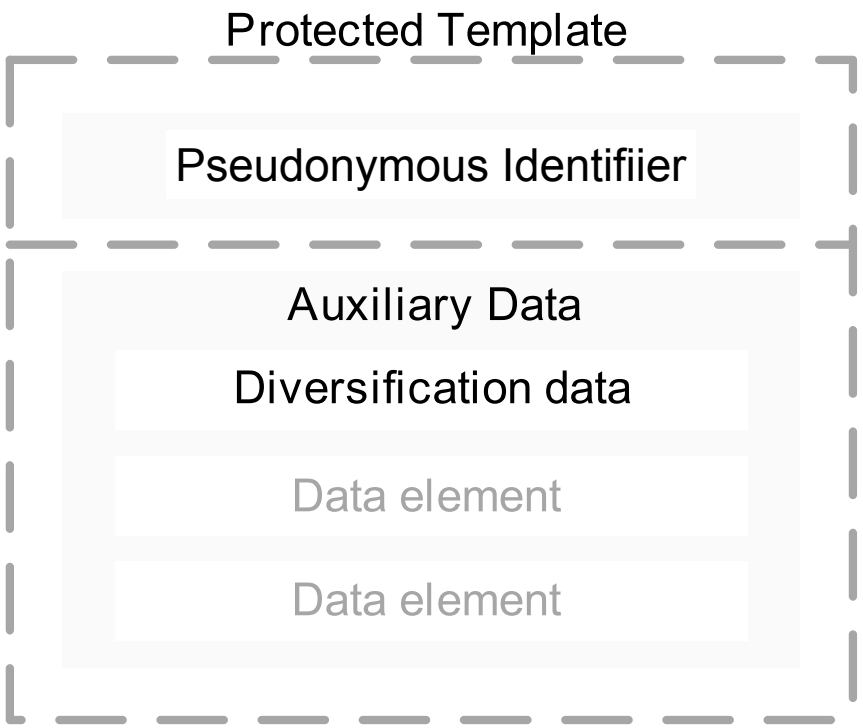
- Biometric Template Protection (BTP) architecture



Protected Template Structure

Resulting Protected Template

- Pseudonymous Identifier
- Auxiliary Data
  - Diversification Data
  - Other data elements



Survey of BTP Algorithms

BTP approaches: Cancelable biometrics

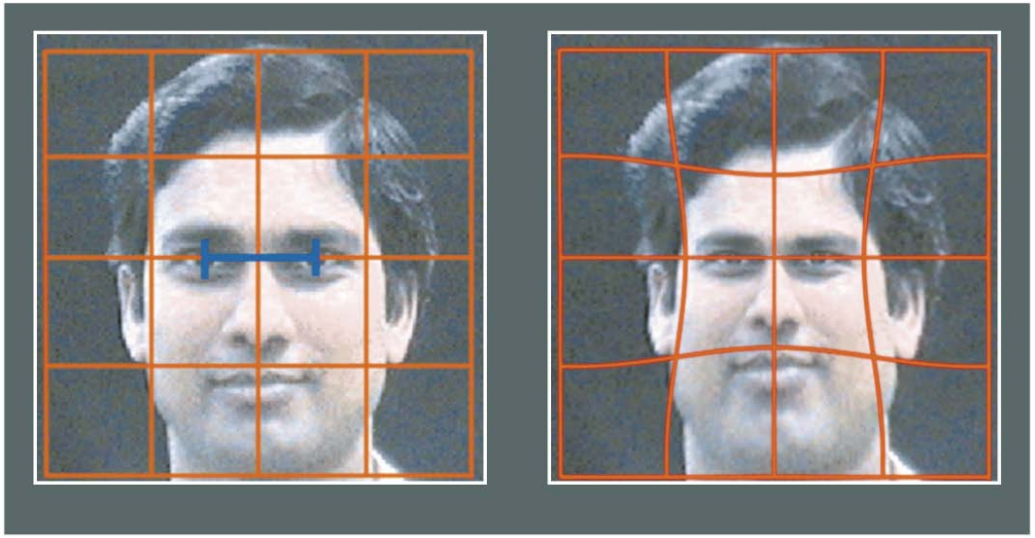
- Cancelable biometrics consist of intentional, repeatable distortions of biometric signals based on transformations which provide a comparison of biometric templates in the protected domain.
- Two types:
  - Non-reversible transformations of the biometric data or unprotected templates.
  - Biometric salting, in which Auxiliary Data (AD) is blended with biometric data to derive a distorted version of the biometric template.

Cancelable Biometrics

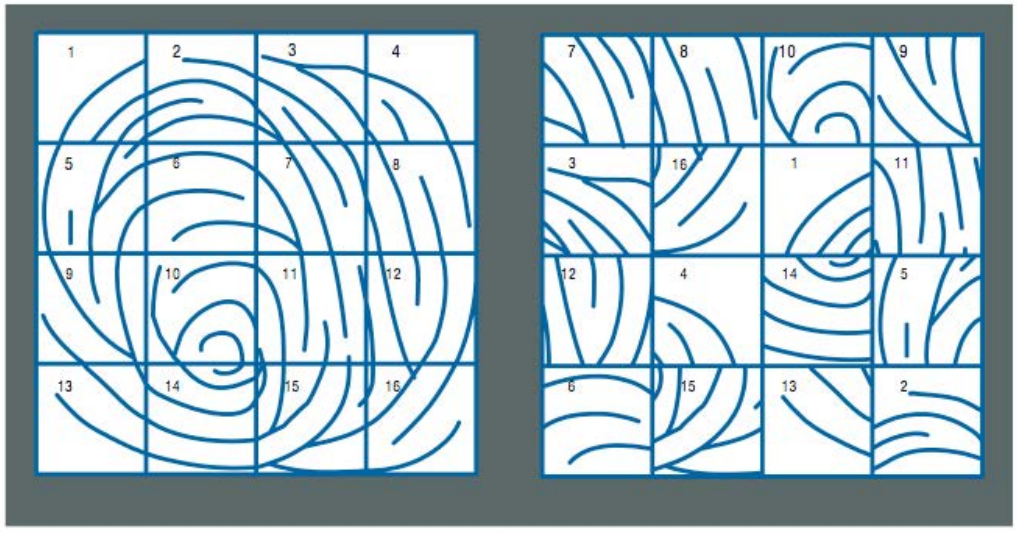
Transformation of a signal prior to feature extraction

- Grid morphing

  [Ratha2001]



Block permutation

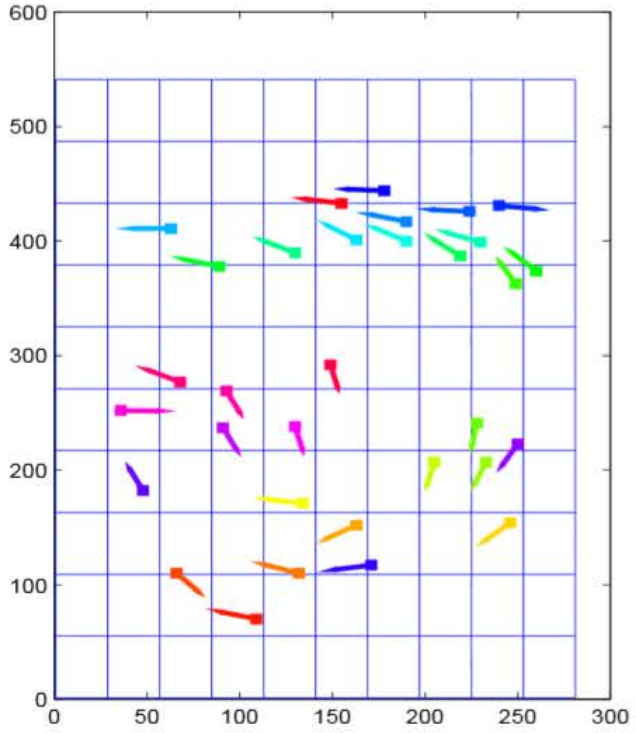


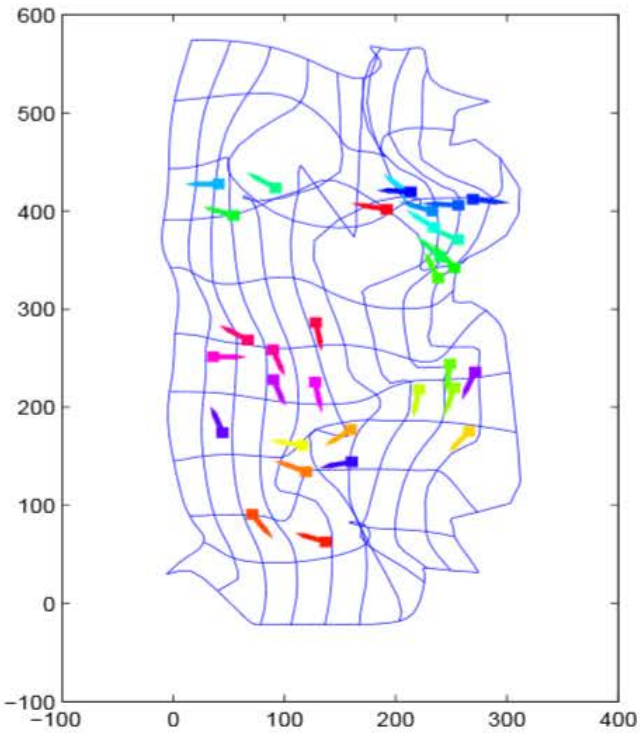
Cancelable Biometrics

Transformation of a signal prior to feature extraction

- Non-invertible transformation based algorithm: Cancelable biometrics [Ratha2007]

X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B





Non-invertibility introduced by “folding” operations

Survey of BTP Algorithms

BTP Approaches: Cryptobiometrics

- These methods combine cryptographic keys with transformed versions of the original biometric templates to obtain secure templates.
- In most cases, some public information, known as helper data or auxiliary data, is generated.
- Two types:
  - Key binding schemes, where AD are obtained combining the key with the biometric template. At verification time, applying an appropriate key retrieval algorithm to the probe biometric sample, the key is obtained from the AD.
  - Key generation schemes, where both the AD and the key are generated directly from biometric data. Again, at verification time, a key is recovered from the probe sample using the AD.

Cryptobiometrics - Fuzzy Extractor

Error Correcting Codes (ECC)

- Compensate the intra-class variability
- Grid points represent ECC Code words

Enrolment

- A random codeword C is chosen
- R is the binary biometric reference template
- Helper data AD = C-R
- Store AD and h(S)=h(DEC(C))

Verification

- X is binary probe template
- X+AD=C'
- S'=DEC(C')
- h(S) == h(S') ?

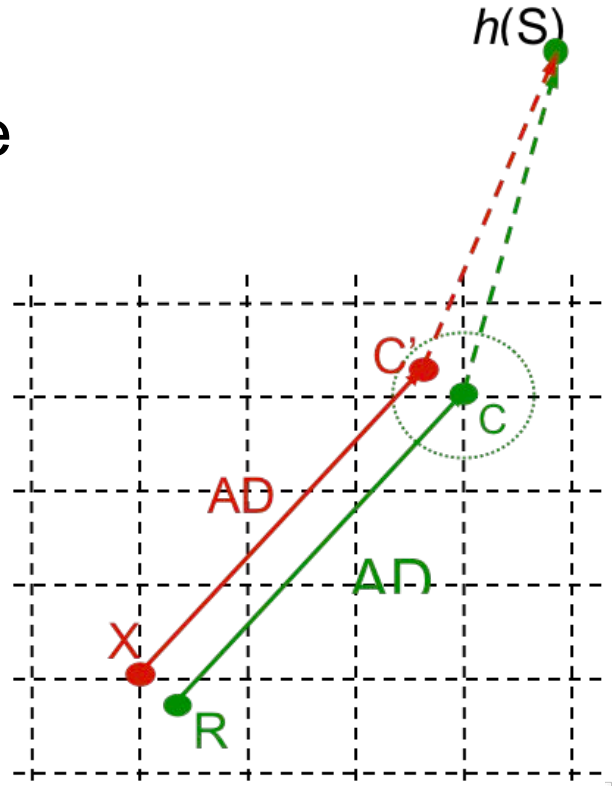
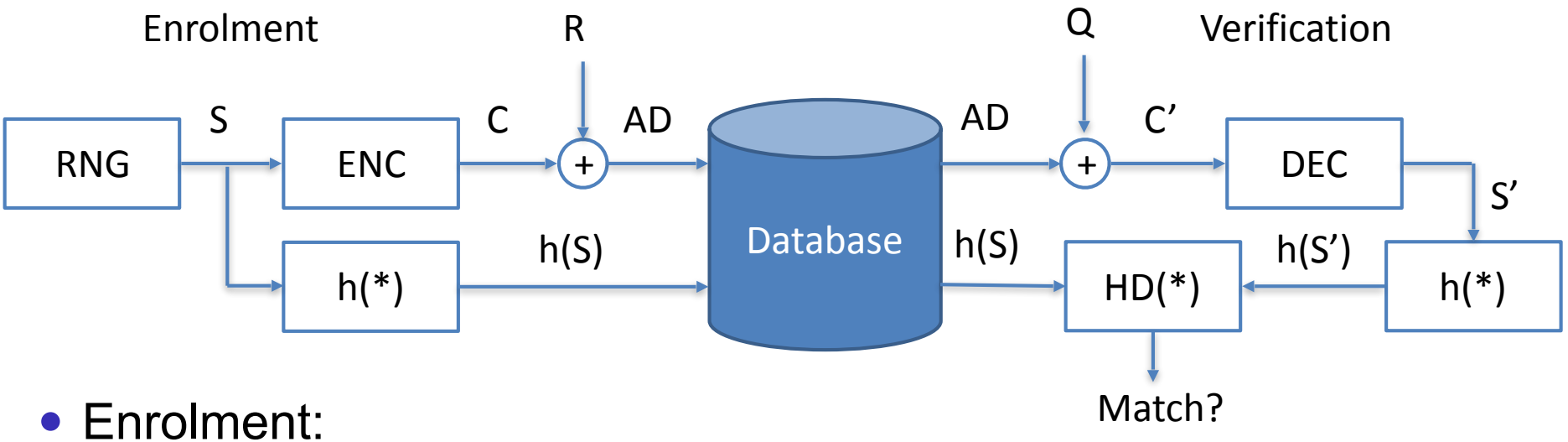


Image Source: Philips Research 2006

Cryptobiometrics - Fuzzy Commitment

- Hashed secret can ECC code words [Jules1999]



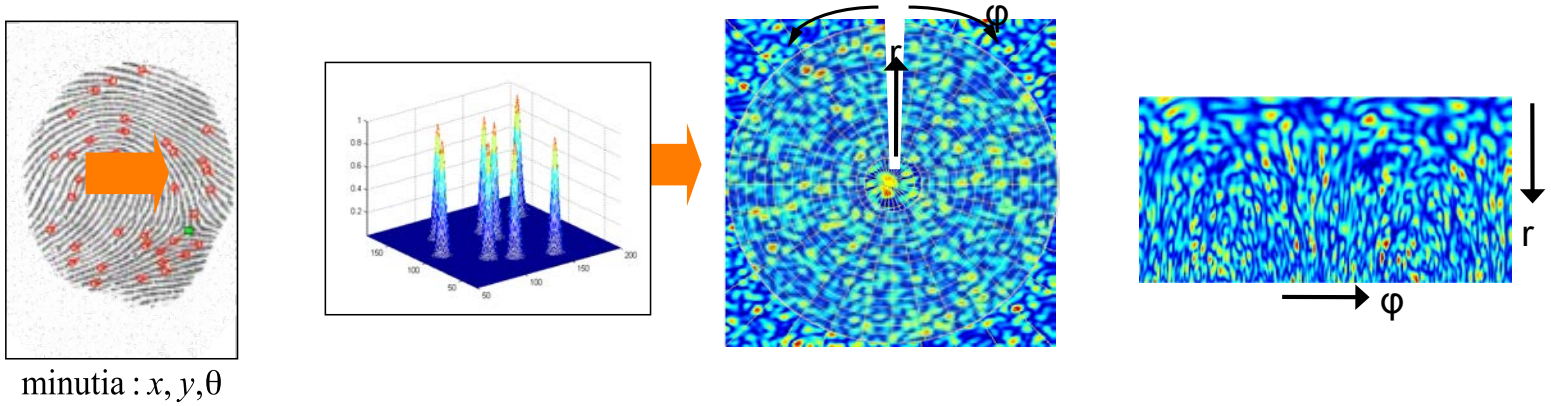
- Enrolment:
  - C is the codeword generated for the random string S
  - R is the binary extract of the reference vector
  - AD = C XOR R is the public AD
  - {h(S), AD} are stored as reference
- Verification:
  - C' = AD XOR Q (query vector)
  - HD(C, C') needs to be smaller than the error correction capabilities

[Juels1999] A. Jules and M. Wattenberg: „A Fuzzy Commitment Scheme“, in ACM CCS, (1999)

Fixed Length Minutiae Feature Vectors

Spectral Minutiae (SM) based Fuzzy Commitment

- Univ. of Twente [Xu2009]



minutia : x, y, θ

Complex valued functions
- Translation and rotation

2D Fourier transform
- Translation invariant

Polar sampling
- Fixed-length feature vector
- Rotation becomes translation

- Idea: convert minutiae to fixed length ordered representation (requirement helper data system)

[Xu2009] Haiyun Xu, et al. “Fingerprint Verification Using Spectral Minutiae Representations”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, (2009)

TURBINE Project - BTP Performance Testing

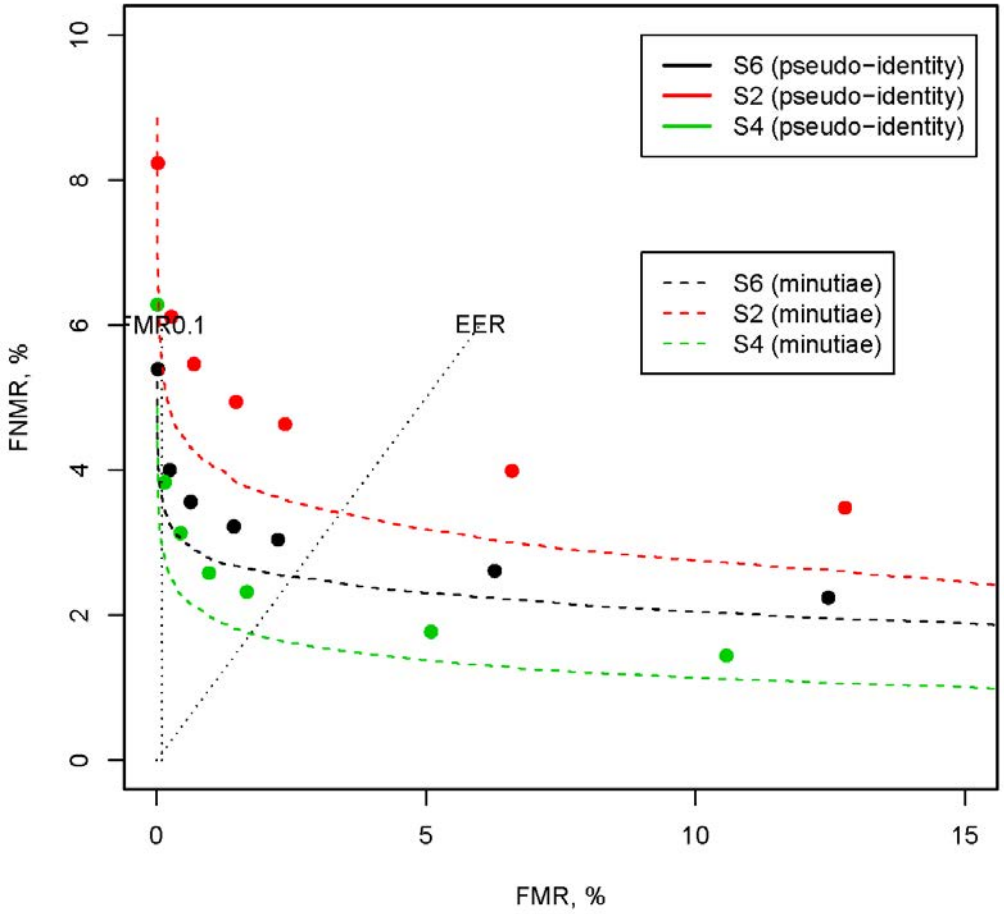
GUC100

- 6 scanners,100 subjects
- ~ 72000 images
- 12 sessions
  - on separate days
- Uncontrolled
  - No image quality control
- Controlled
  - Quality was controlled to some extend visually e.g. by wetting fingers if necessary
- Sequestered database -
  - No access granted to algorithm developers

TURBINE Project - BTP Performance

Performance results - Pseudonymous Identifier level

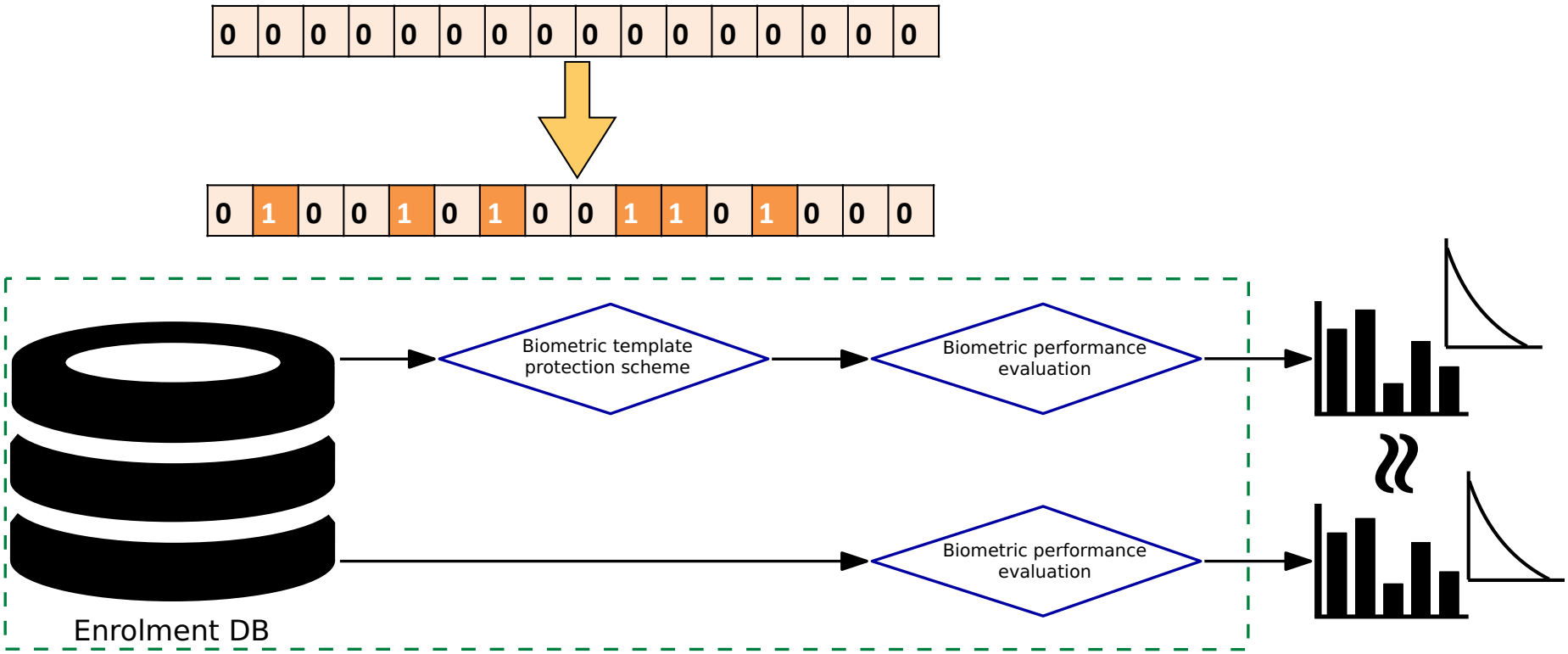
- One example of a PI algorithm.



Biometric Template Protection

Protection at the same accuracy level is possible

- Bloom filter-based pseudonymous identifiers



[Ra2014] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: „On the Application of Bloom Filters to Iris Biometrics“, in IET Journal on Biometrics 3(1), (2014)
http://www.christoph-busch.de/files/Rathgeb-BloomFilter-IET-2014.pdf

Biometric Template Protection

Bloom filters

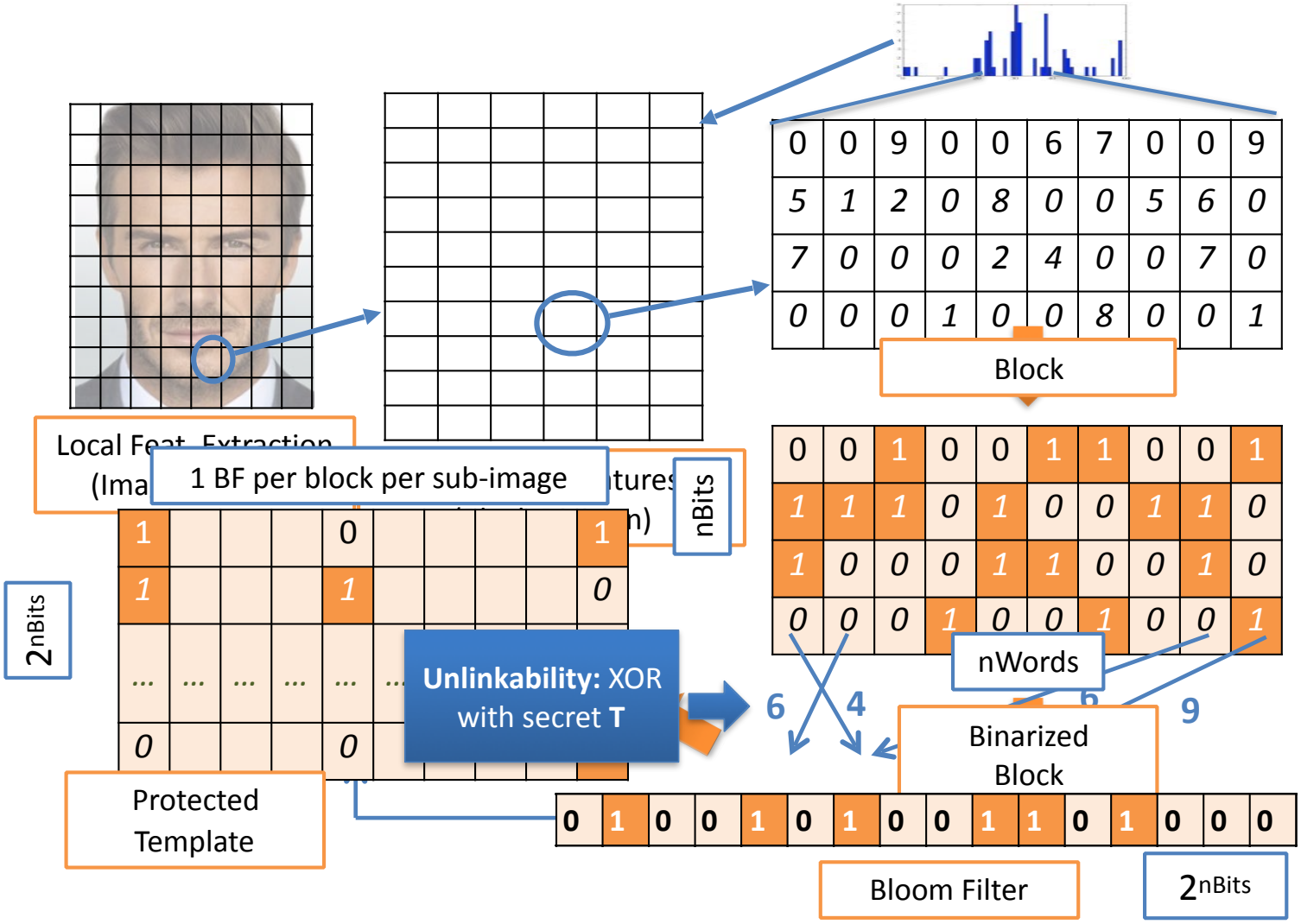
- A Bloom filter b is a space-efficient data structure representing a set S to support membership queries
- b is a simple bit array of length n (initially all bits are set to 0)
- To represent $S = \{x_1, x_2, \ldots, x_m\}$, k independent hash functions $h_1, h_2, \ldots, h_k$ with range [0,n−1] are utilized
- For each element $x \in S$, bits $h_i(x)$ of b are set to 1, for $1 \leq i \leq k$
- Indices can be set to 1 multiple times (but only the first change has an effect!)
- Let $|b|$ denote the amount of bits within a Bloom filter b, which are set to 1. Then the dissimilarity DS between two Bloom filters b_i and b_j is defined as

$$DS(b_i, b_j) = \frac{HD(b_i, b_j)}{|b_i \cup b_j|}$$

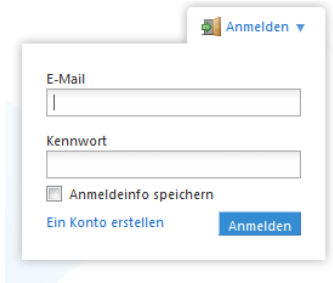
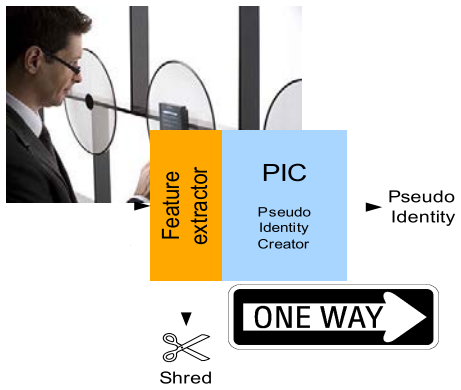
Bloom Filter Biometric Template Protection

Protection at the same accuracy level is possible

- Generating bloom filter-based pseudonymous identifiers



Revised Benchmark of Authentication

	Non-Invertibility from the reference	Revocability and Renewability	Strong link to the data subject
	(?)		
			
			

BTP Approaches

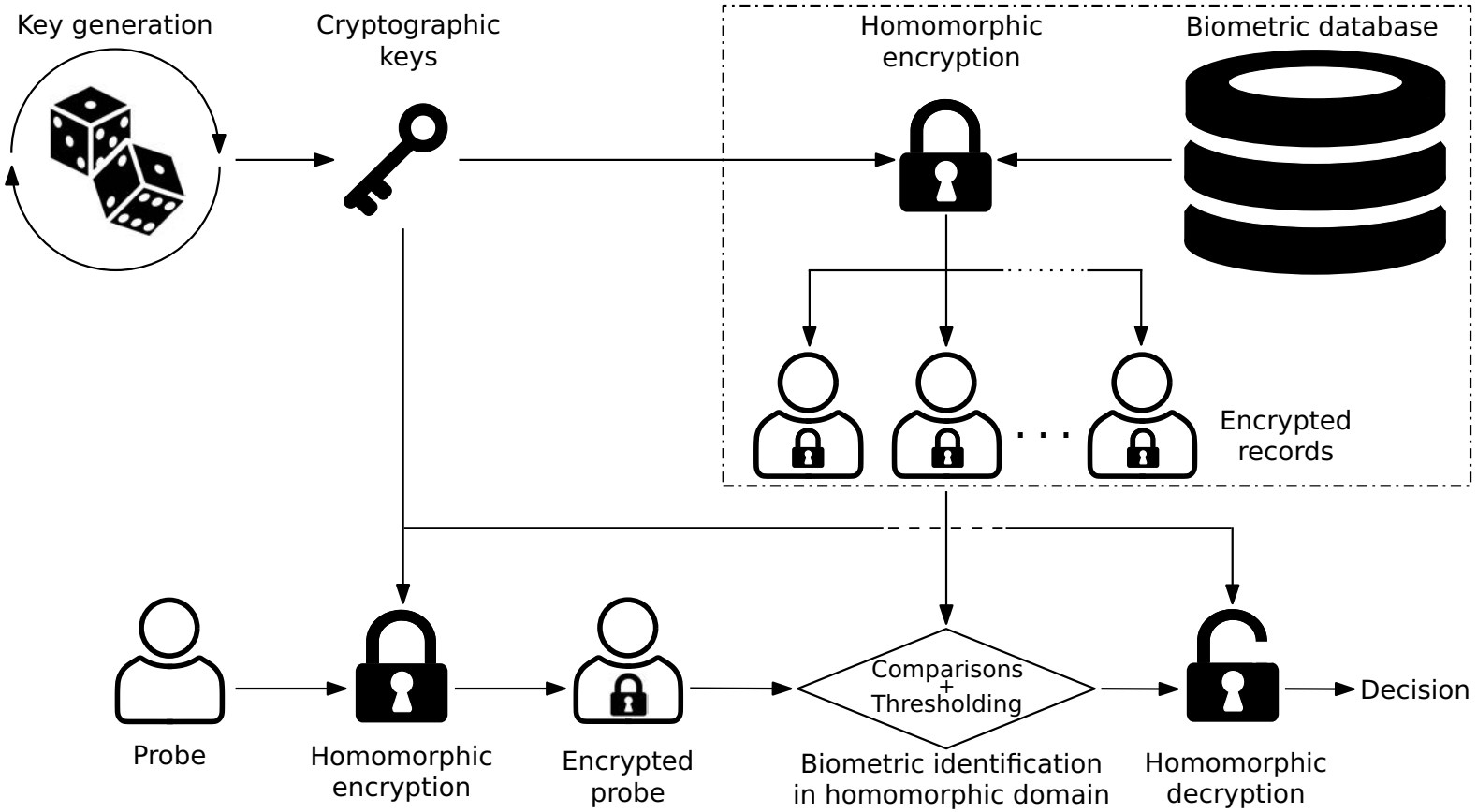
Biometrics in the Encrypted Domain

- Homomorphic Encryption (HE) schemes allow for computations to be performed on ciphertexts,
  - with no additional AD,
  - and which generate encrypted results
  - which decrypt to plaintexts
  - that match the result of the operations carried out on the original plaintext
- This solves the issue of decryption before authentication...

BTP Approaches

Biometrics in the Encrypted Domain

- Homomorphic Encryption (HE) schemes allow for computations to be performed on ciphertexts



BTP Approaches

Biometrics in the Encrypted Domain

- Partially Homomorphic Encryption (PHE) schemes
  - are defined as allowing only a single operation type an unlimited number of times.
  - PHE schemes have been around for over 30 years supporting only either addition or multiplication.
- Somewhat Homomorphic Encryption(SHE) schemes
  - allow multiple operation types, but only a limited number of times.
- Fully Homomorphic Encryption (FHE) schemes
  - support an unlimited number of operations.

BTP Approaches

Homomorphic Encryption

- Assymmetric Cryptosystem (pk/sk)
- Post-quantum secure (lattice-based)
- Homomorphic Properties:

$$\mathsf{Enc}_{pk}(A) + \mathsf{Enc}_{pk}(B) = \mathsf{Enc}_{pk}(A + B)$$

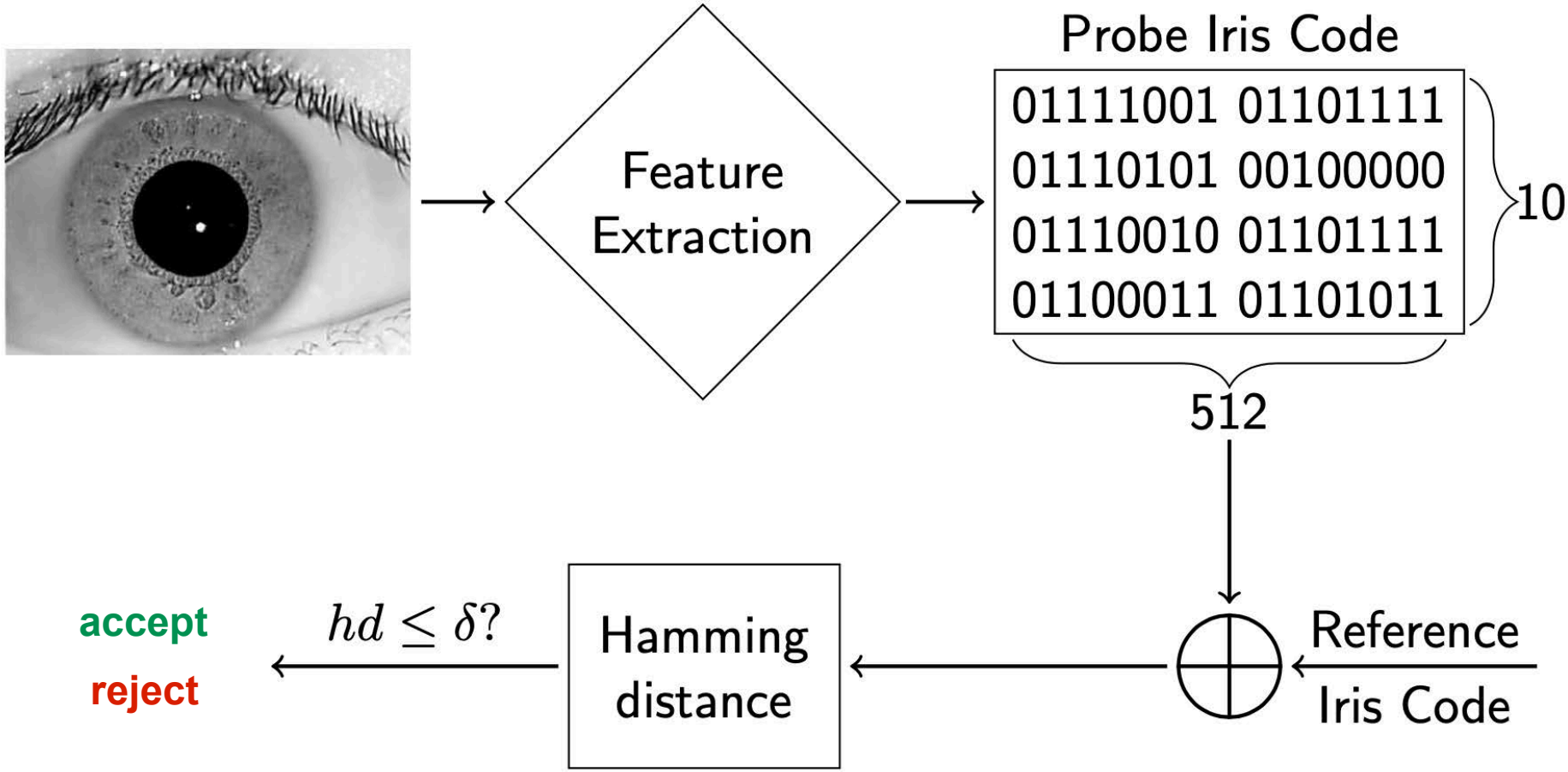
$$\mathsf{Enc}_{pk}(A) \cdot \mathsf{Enc}_{pk}(B) = \mathsf{Enc}_{pk}(A \cdot B)$$

[Kolb2019] J. Kolberg, et al.: "Template Protection based on Homomorphic Encryption: Computational Efficient Application to Iris-Biometric Verification and Identification ", in Proceedings of IEEE WIFS, Delft, NL, (2019)
[Dro2019] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, C. Busch: "On the Application of Homomorphic Encryption to Face Identification", in Proceedings of the IEEE 18th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 18-20, (2019)

BTP Approaches

Homomorphic Encryption

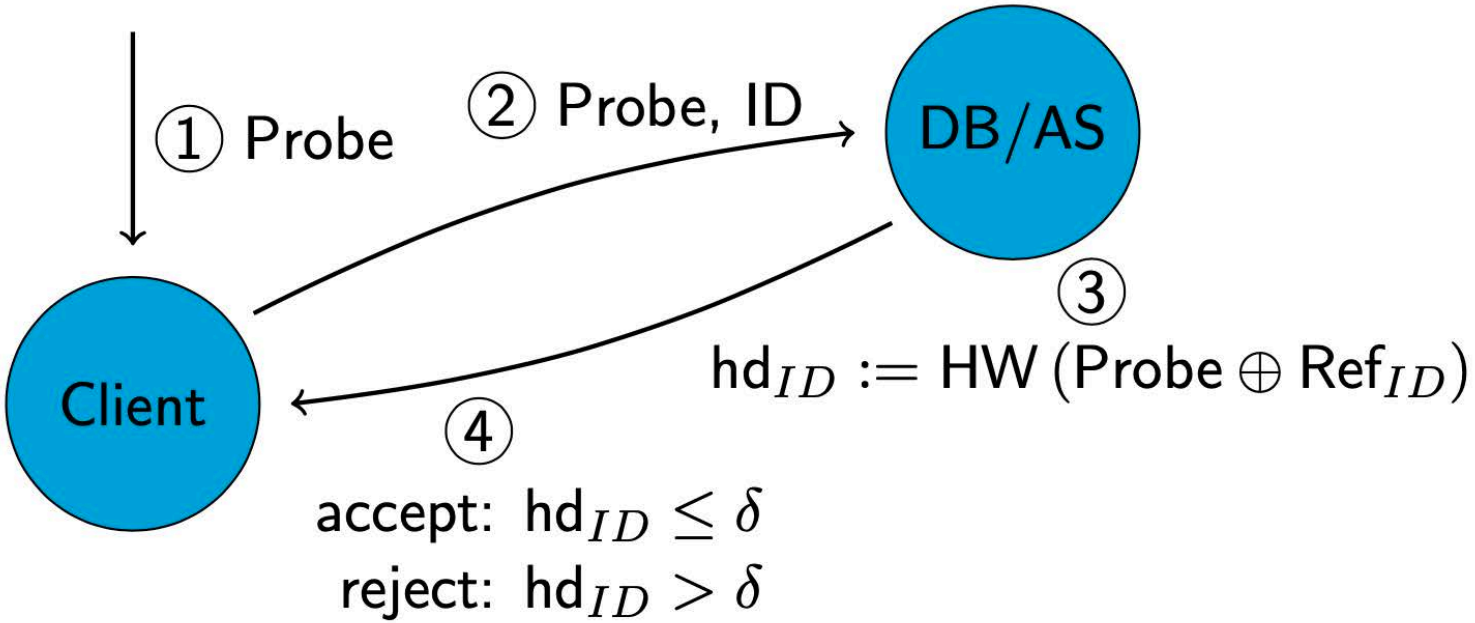
- Example: Iris Recognition
  - unprotected system



BTP Approaches

Homomorphic Encryption

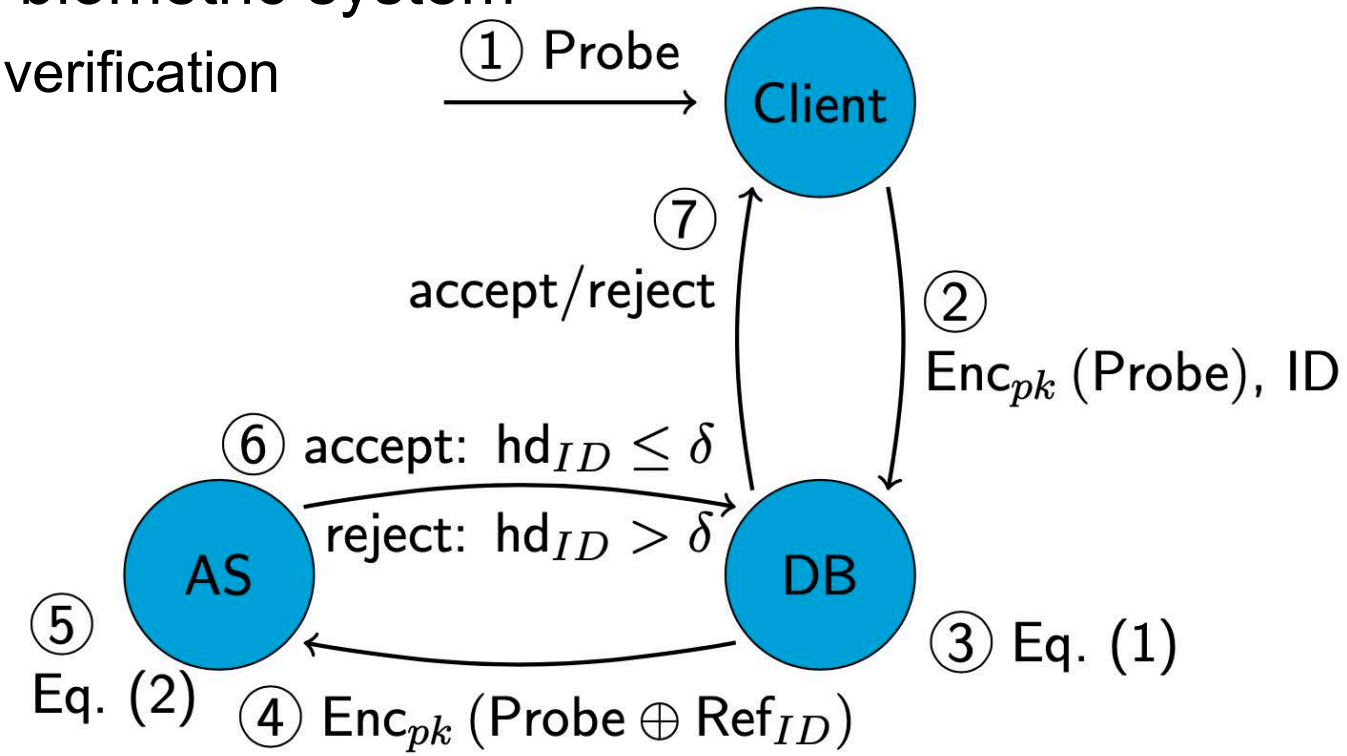
- Example: Iris Recognition
  - unprotected verification



BTP Approaches

Biometrics in the Encrypted Domain

- A protected biometric system
  - NTRU HE verification



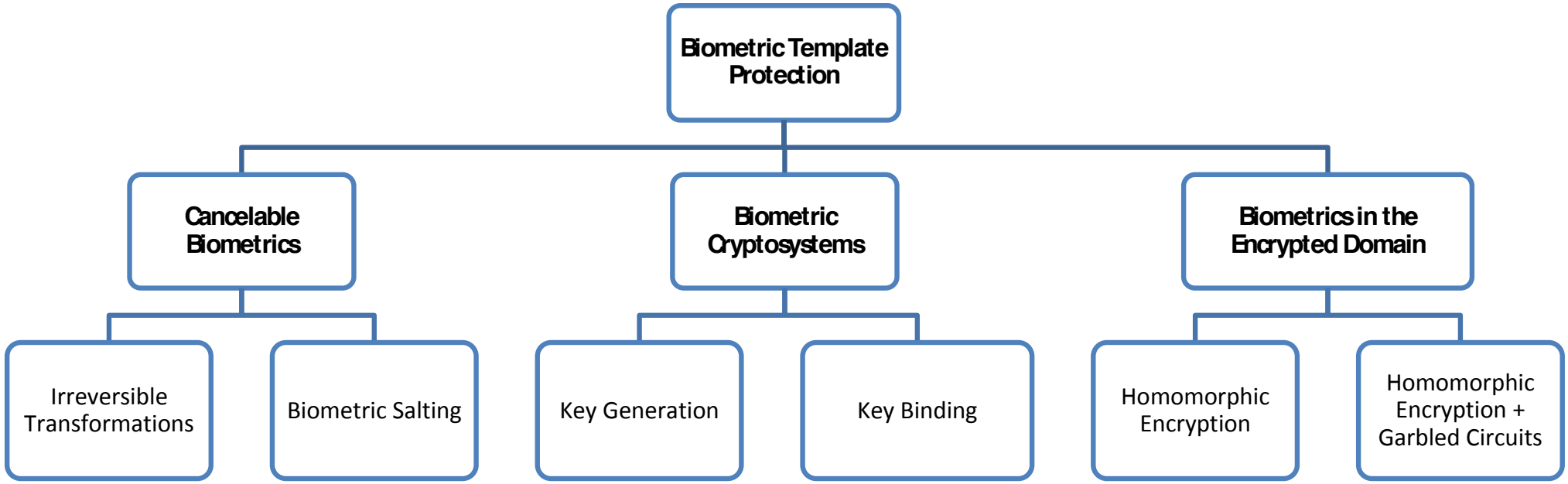
$$\text{Enc}_{pk}(\text{Probe} \oplus \text{Ref}_{ID}) := \text{Enc}_{pk}(\text{Probe}) \oplus \text{Enc}_{pk}(\text{Ref}_{ID}) \quad (1)$$

$$\text{hd}_{ID} := \text{HW}(\text{Dec}_{sk}(\text{Enc}_{pk}(\text{Probe} \oplus \text{Ref}_{ID}))) \quad (2)$$

[NTRU1998] J. Hoffstein, J. Pipher, J. Silverman: NTRU: A Ring-Based Public Key Cryptosystem, in Int. Algorithmic Number Theory Symposium. Springer, (1998)

Overview

BTP approaches: summary



Geometric trans.
Feature mixing
BioTokens
Bloom Filters

Correlation
Random projection
Visual crypto

Quantization

Fuzzy vault
Fuzzy commitment
BioHashing

Summary

Biometric Template Protection

- Biometric data is sensitive data, which needs to be protected, providing irreversibility, unlinkability, renewability and accuracy preservation.
- Unprotected templates can be reconstructed using inverse biometrics methods, where only access to similarity scores is required.
- Current BTP schemes can be classified as cancelable biometrics, cryptobiometric systems, or biometrics in the encrypted domain.
- We need to follow a standardised methodology for a standardised security and privacy evaluation of BTP schemes.
  - BTP schemes based on Bloom filters or Homomorphic Encryption comply with ISO/IEC IS 24745.

Conclusion

Benefits and Applications

- Pseudonymous biometric databases which only consist of renewable biometric references (RBRs)
- 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 from tracking without consent in case biometric databases are compromised

References

Publications

- N.K. Ratha, J.H. Cornell, R.M. Bolle: „Enhancing security and privacy in biometrics-based authentication systems“, (2001)
- M. Veen, T. Kevenaar, G.J. Schrijen, T.H. Akkermans. F. Zuo "Face Biometrics with Renewable Templates", SPIE Conference Multimedia and Security, (2006)
- C. Rathgeb, A. Uhl: „A survey on biometric cryptosystems and cancelable biometrics“, Springer, (2011)
- C. Rathgeb, F. Breitinger, C. Busch, H. Baier: "On the Application of Bloom Filters to Iris Biometrics", in IET Journal on Biometrics 3(1), (2014)
- M. Gomez-Barrero, C.Rathgeb, J. Galbally, J. Fierrez, C. Busch: „Protected Facial Biometric Templates Based on Local Gabor Patterns and Adaptive Bloom Filters“, in Proceedings ICPR, Stockholm, Sweden, (2014)
- G. Li, B. Yang, C. Rathgeb, C. Busch: "Towards Generating Protected Fingerprint Templates based on Bloom Filters", in Proceedings IWBF, Gjøvik, Norway, (2015)
- M. Gomez-Barrero, et al: "Unlinkable and Irreversible Biometric Template Protection Based on Bloom Filters“, in Journal Information Sciences, (2016)
- M. Gomez-Barrero, J. Galbally, C. Rathgeb, C. Busch: "General Framework to Evaluate Unlinkability in Biometric Template Protection Systems“, in IEEE Transactions on Information Forensics and Security (TIFS), (2018)

References

Standard

- ISO/IEC JTC 1/SC 27 IT Security techniques: ISO/IEC 24745:2011, Security techniques – Biometric information protection, (2011)

Publications HE

- J. Kolberg, et al.: "Template Protection based on Homomorphic Encryption: Computational Efficient Application to Iris-Biometric Verification and Identification ", in Proceedings of IEEE WIFS, Delft, NL, (2019)
- P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, C. Busch: "On the Application of Homomorphic Encryption to Face Identification", in Proceedings of the IEEE 18th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 18-20, (2019)
- M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, J. Fierrez: Multi-Biometric Template Protection Based on Homomorphic Encryption. Pattern Recognition, (2017)

Two Recommendations

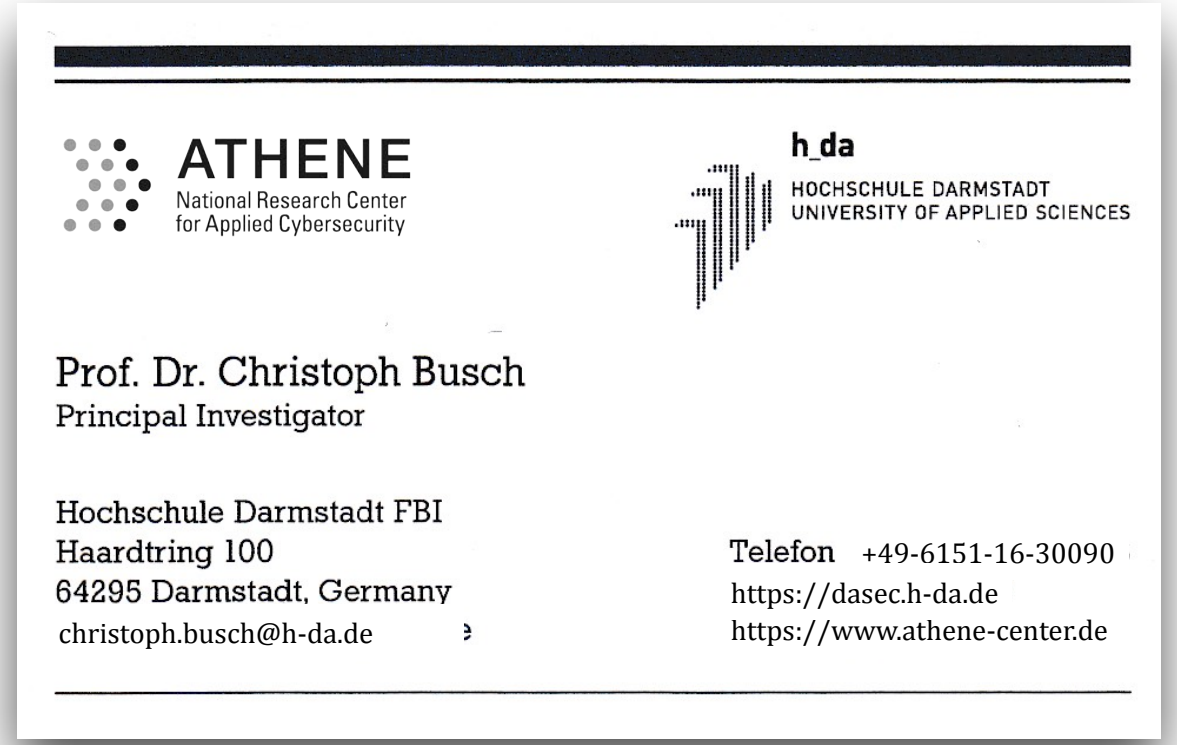
Join the European Association for Biometrics (EAB)

- Membership for students (Bachelor, Master, PhD) is free of charge!
  https://eab.org/membership/types_of_membership.html

Join the EAB webinar on Biometric Template Protection

- on June 15th at 12.30h
- register at:
  https://eab.org/events/program/214

Contact


ATHENE
National Research Center
for Applied Cybersecurity
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
Telefon +49-6151-16-30090
https://dasec.h-da.de
https://www.athene-center.de