

Biometric Privacy and Information Protection

Christoph Busch and Marcel Grimmer

Department of Information Security and Communication Technology
Norwegian University of Science and Technology - Gjøvik

PriMa ITN workshop 2021-05-10



Structure of this session

Lecture (Christoph Busch)

<https://christoph-busch.de/files/Busch-Privacy-210510.pdf>

- Data privacy culture
- Privacy protection principles
- Non discriminatory biometric systems
- Additional information in biometric samples
- Data storage and attacks
- Biometric template protection

Practical (Marcel Grimmer)

<https://christoph-busch.de/files/210510-prima-practical-material.zip>

- Biometric template protection with Bloom filters

Assignment (Christoph Busch)

Data Privacy Culture and Legal Framework

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, China):
 - ! Biometric data is **owned** by the **organization** that processed the data



Source: Hoan Ton-That (Clearview 2021)

<https://weta.org/watch/shows/amanpour-and-company/clearview-ai-ceo-defends-facial-recognition-software-nuyagm>



Erik Carter

China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment

Even children are pressed into giving blood samples to build a sweeping genetic database that will add to Beijing's growing surveillance capabilities, raising questions about abuse and privacy.

Legal & Regulatory Framework for Biometrics

EU legal Framework

- **General Data Protection Regulation (GDPR)**
 - ! Regulation 2016/679
- Rules apply to **all companies** targeting EU consumers, regardless of whether they are established inside or outside the EU



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)

Legal & Regulatory Framework for Biometrics

What is the impact of Recital 51

- on video surveillance and face recognition ?
- Data privacy authorities position [Arnes2019]
 - ! *To qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a **measurement** of this characteristics.*
 - ! *The video footage of an individual **cannot** however in itself be **considered** as **biometric data** under Article 9, if it has not been specifically technically processed in order to contribute to the **identification** of an individual.*

Domain conflict between legal experts and technical experts

[Arnes2019] A. Arnes: "ID management and the use of Biometrics from a personal data protection perspective", NBF, (2019)

Data Protection Principles

EU - Data Protection Principles

Criteria for processing biometric data:

- Proper **processing basis** must exist
 - ! 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
 - ! 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

- **Accuracy** principle

- ! personal data shall be accurate and kept up to date

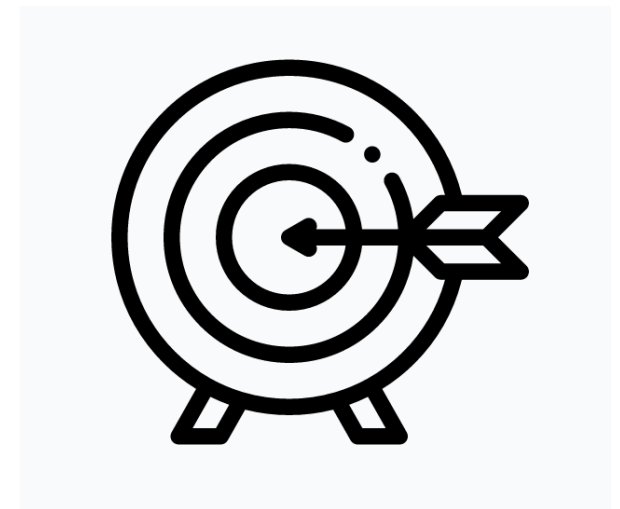


Image Source: <https://www.flaticon.com> (2020)

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

! 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*

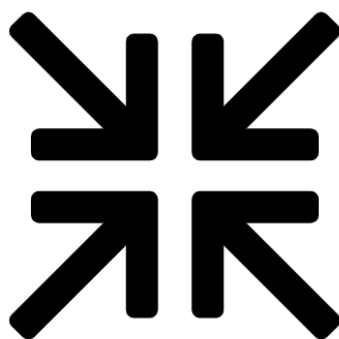


Image Source: <https://www.flaticon.com> (2020)

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



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**

- **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 alphanumeric 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

alphanumeric 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: _____

Non-discriminatory Biometric System

Operational Risk

Worn-down ridges on a fingertip may result in:

- **discriminatory** situation for the capture subject

Jan 2, 2004 Faded fingerprints cost former welder a job

ASSOCIATED PRESS

DECATUR — The years Chuck Strickler spent as a welder provided him with the experience he needed as a welding inspector at power plants across the nation.

But the welding also has left Strickler, 60, of Decatur, lacking a full set of intact fingerprints required under new, stepped-up security regulations at nuclear plants. Since the U.S. Department of Homeland Security issued the new rules in the wake of Sept. 11, the reams of documents Strickler has attesting to his identity no longer are sufficient.

"I first ran into a problem with it three or four years ago," Strickler said. "They said my fingerprints weren't valid. But at the time they accepted a picture ID as proof of identity."

Earlier this year, when he tried to get a job inspecting the D.C. Cook Nuclear Power Station near Bridgman, where he had worked before, his application was turned down because of the worn-down

ridges on his fingertips.

"I passed everything except for the fingerprints," Strickler said adding that the application process included a comprehensive psychological examination and criminal background check.

"The plant sent the fingerprints to the FBI, and they said it's outside the realm of the Homeland Security's guidelines (for what is needed). It was a little frustrating."

A person has about 100 identification marks on his or her fingerprints, and most adults have about 80 that can be used to identify them.

But because of his welding work, Strickler has only about 30 of the identification points.

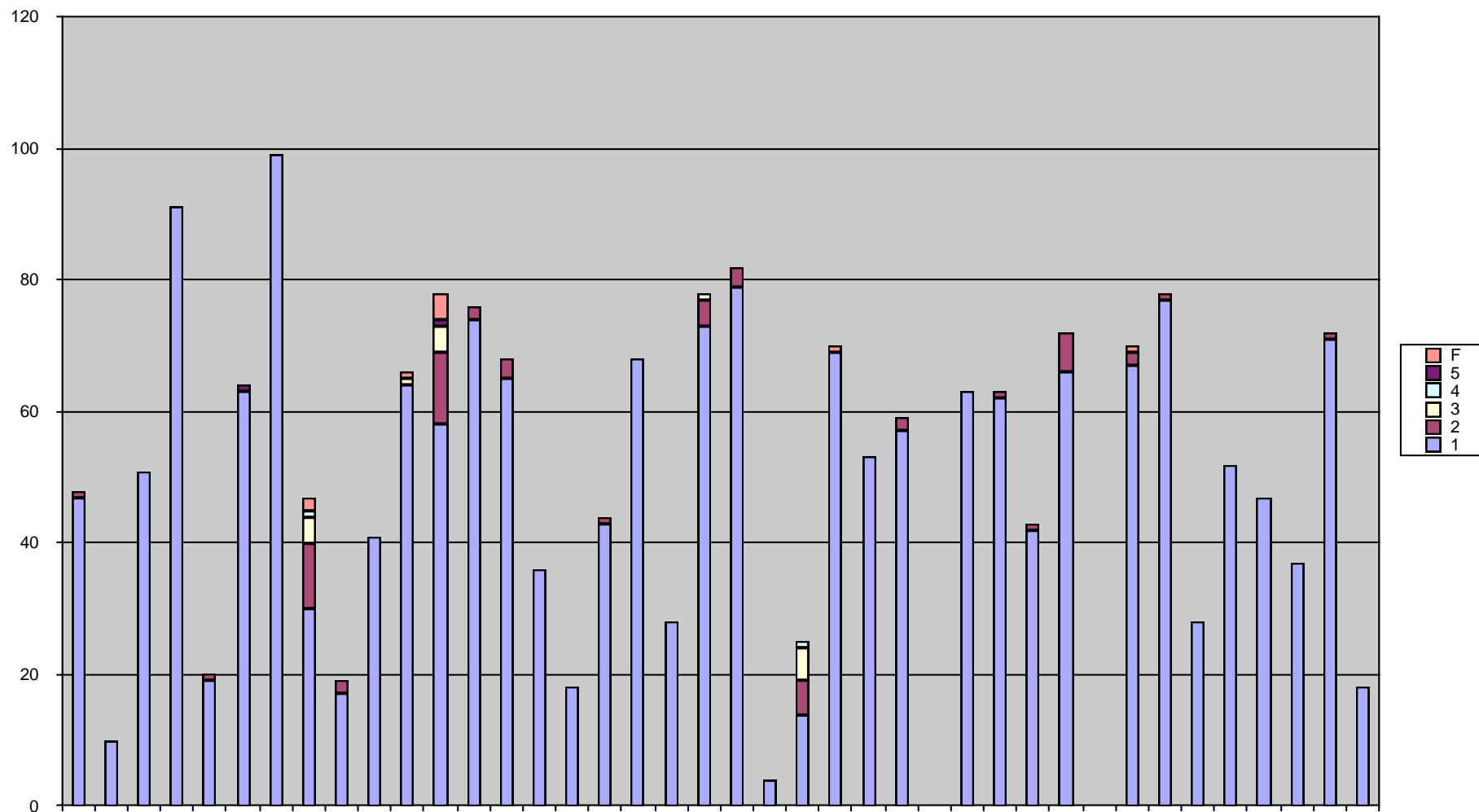
Strickler is free to work at non-nuclear plants. But he says he prefers to have the option of working for the nuclear facilities.

"This cuts my income in half," he said.



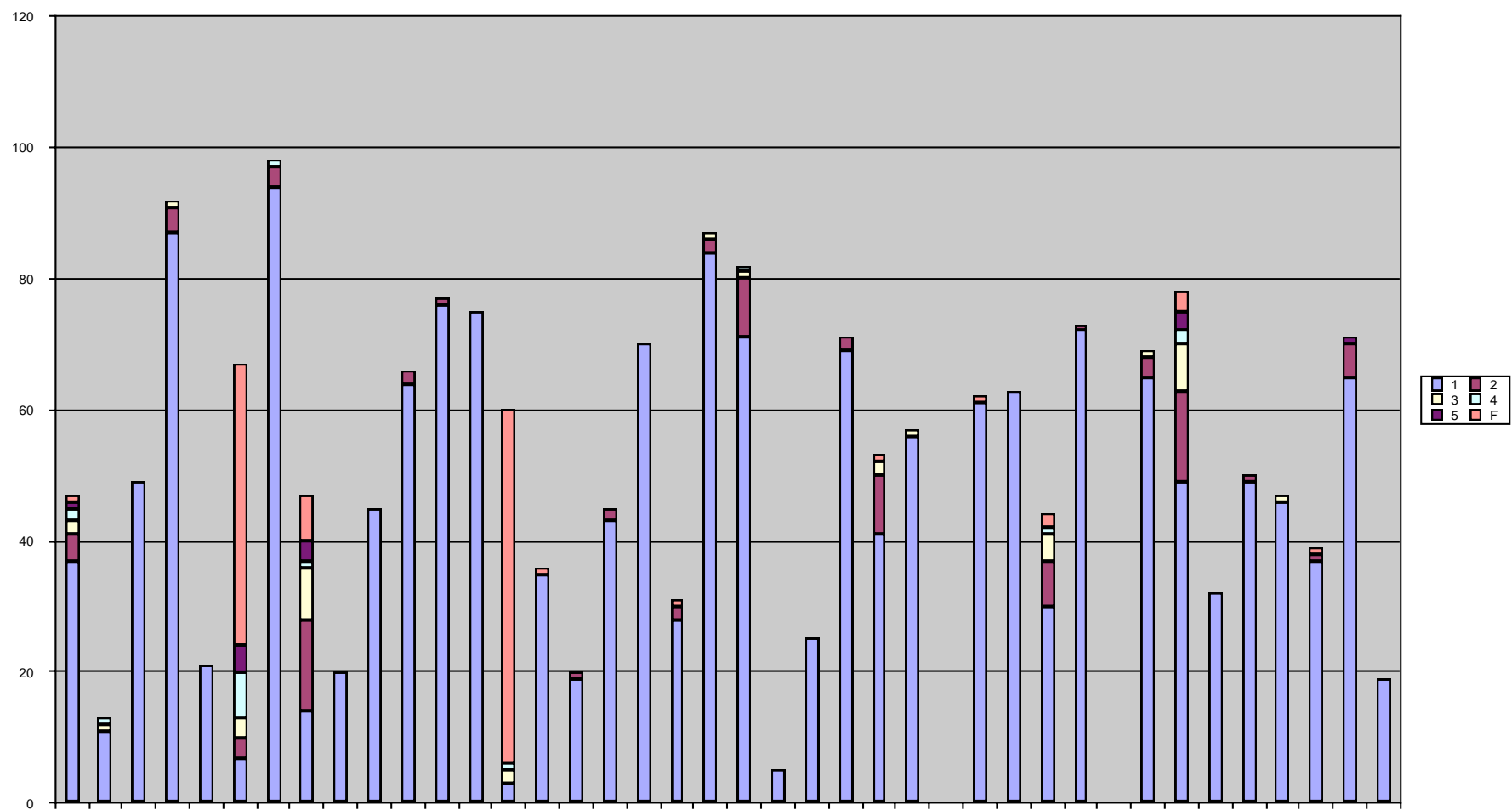
Strickler

Results BioIS (2)



[Zwie2000] A. Zwiesele, A. Munde, C. Busch, H. Daum: "Comparative Study of Biometric Identification Systems" In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, (2000)

Results BioIS (3)

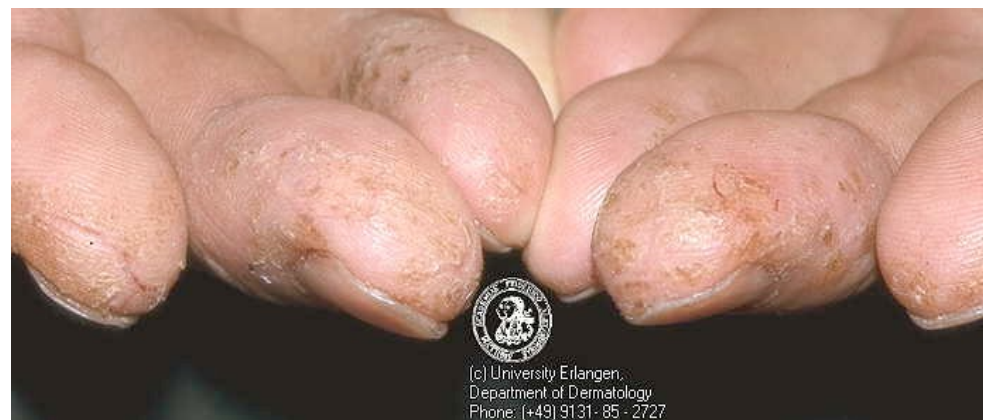


[Zwie2000] A. Zwiesele, A. Munde, C. Busch, H. Daum: "Comparative Study of Biometric Identification Systems" In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, (2000)

Demographic Effects

Failure to enrol

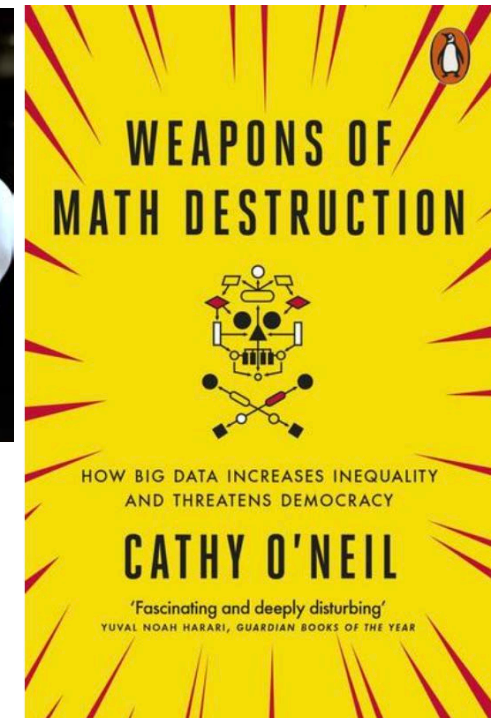
- Dermatologists estimate that up to 11% of the population suffers from **skin diseases**, which will directly impact fingerprint recognition
 - ! atopic eczema
 - ! atopic hand eczema
 - ! hyper ceratotic hand eczema
 - ! thrombangitis obliterans etc.
- Operational systems must provide non-discriminatory fallback procedures!



Demographic Effects

Algorithm bias in the media

- Movie **Coded Bias**
- Press information



Nov 4, 2020, 08:10am EST | 621 views

Biometrics Aren't Inherently Biased — We're Training Them Wrong



Stephen Ritter Forbes Councils Member
Forbes Technology Council

TECHTANK
Machines learn that Brussels writes the rules: The EU's new AI regulation
Mark MacCarthy and Kenneth Propp - Tuesday, May 4, 2021

TECHTANK

f t in e ...

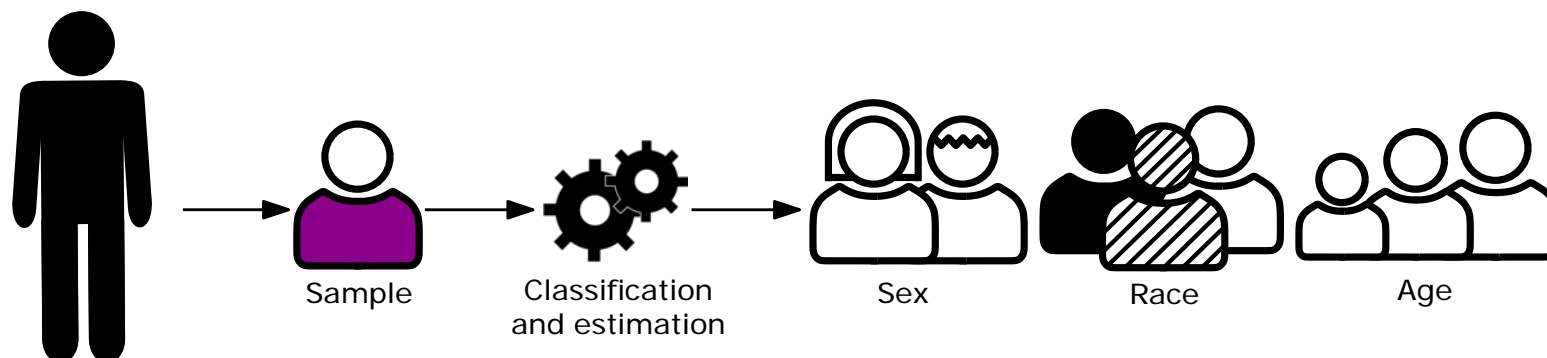
Editor's Note: This post originally appeared on the [Lawfare blog](#).

The European Union's [proposed](#) artificial intelligence (AI) regulation, released on April 21, is a direct challenge to Silicon Valley's common view that law should leave emerging technology alone. The proposal sets out a nuanced regulatory structure that bans some uses of AI, heavily regulates high-risk uses and lightly regulates less risky AI systems.

Demographic Effects

Current findings for facial biometric characteristics

- Studies showed **substantial impact** of gender and race on the accuracy.
 - ! In particular, lower accuracy for **dark-skinned females** observed




- NIST Face Recognition Vendor Test: Demographics Effects
 - ! 200 algorithms tested
 - ! found empirical evidence for the existence of a **wide range of accuracy** across demographic differences in the majority of the current face recognition algorithms that were evaluated

[Drozd2020] P. Drozdowski, C. Ratgeb, A. Dantcheva, N. Damer, C. Busch: "Demographic Bias in Biometrics: A Survey on an Emerging Challenge", in IEEE Transactions on Technology and Society (TTS), (2020)

Demographic Fairness

Learn more on fairness in biometric systems

- <https://eab.org/events/program/237>



The image is a promotional poster for an event. It features a large, diverse crowd of stylized human figures in various colors (red, blue, yellow, green, etc.) walking on a light blue background. In the top right corner, there is the logo for the European Association for Biometrics (EAB), which includes the text 'European Association for Biometrics', the acronym 'eab', and the tagline 'Human Identity in Europe', accompanied by a circular emblem of yellow stars. The main title 'DEMOGRAPHIC FAIRNESS IN BIOMETRIC SYSTEMS' is written in large, white, bold, sans-serif capital letters on the left side. In the bottom right corner, the text 'EAB VIRTUAL EVENTS SERIES' is followed by three dates: '09/03/2021', '15/03/2021', and '30/03/2021'.

Sensitive Data

Additional Information in Biometric Samples

Additional Information from Palm Images

Limited intellectual capabilities are correlated with a certain hand pattern

- Down syndrome (aka Trisomy 21) - **Simian crease**
“A simian crease is defined as fusion of the proximal and distal transverse palmar creases into **single transfers palmar crease**.” [Pur1972]

Normal
flexion crease



Simian
crease



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

Additional Information from Iris Images

Malign Melanom of the Iris

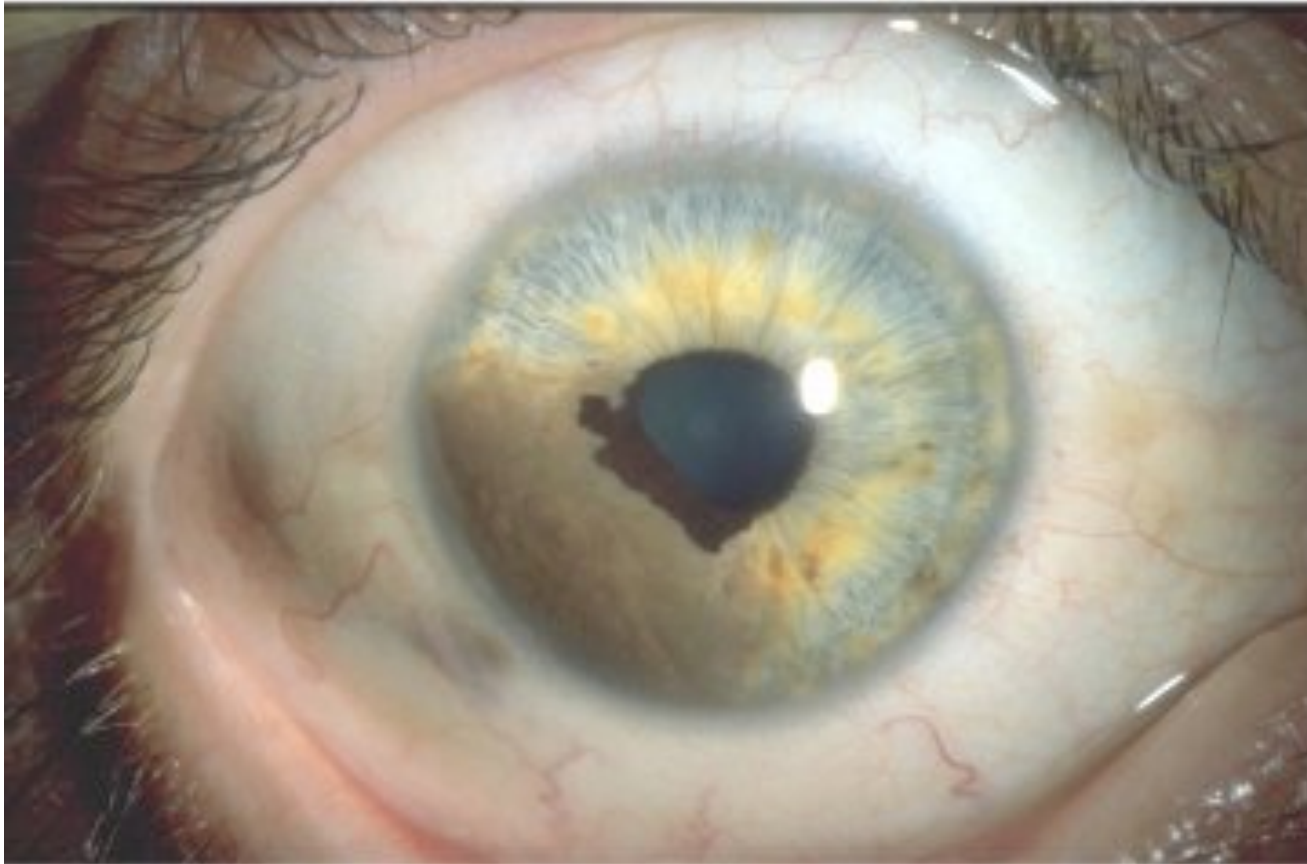


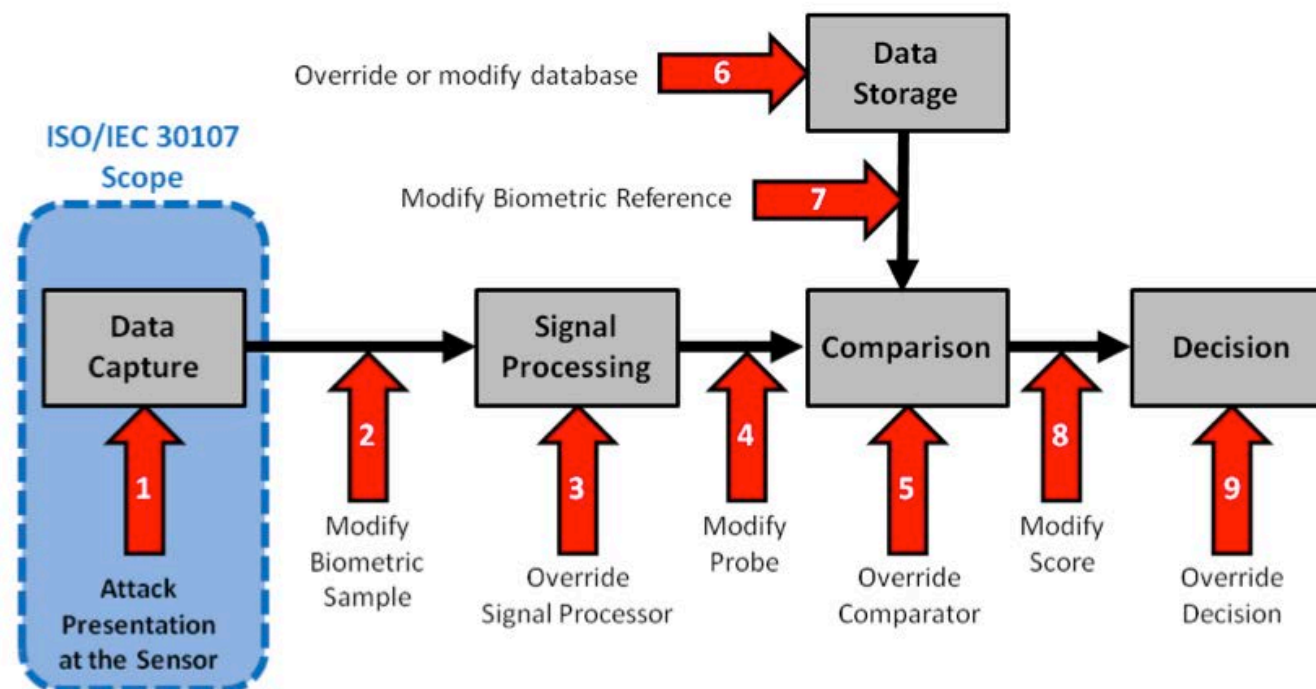
Image Source: Online Journal of Ophthalmology

Data Storage and Attacks

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>



Money International +

Markets Economy Companies Tech

🕒 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.

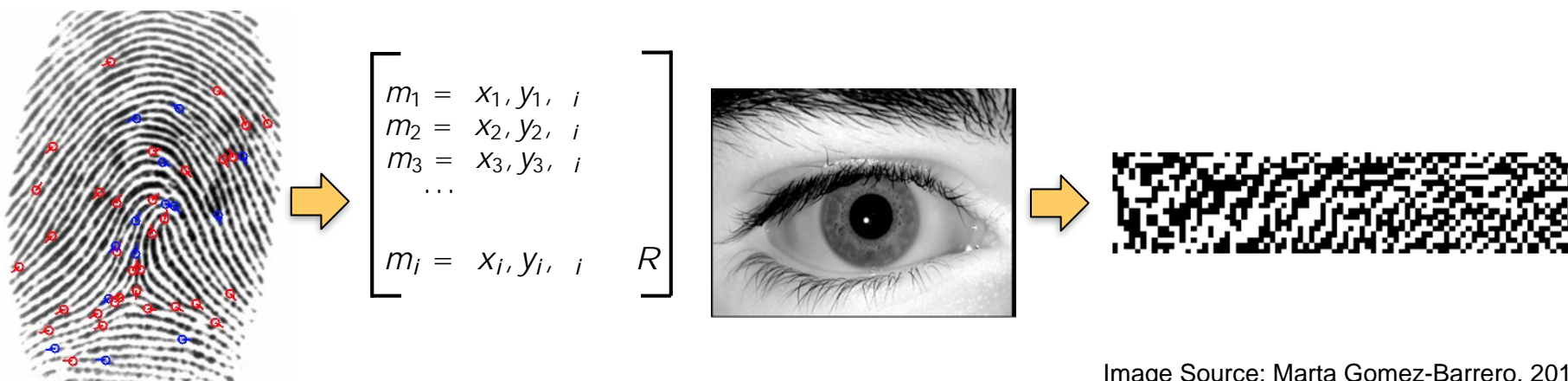
As an OPM spokesman told CNNMoney in July: "It's across federal agencies. It's everybody."

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



- 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

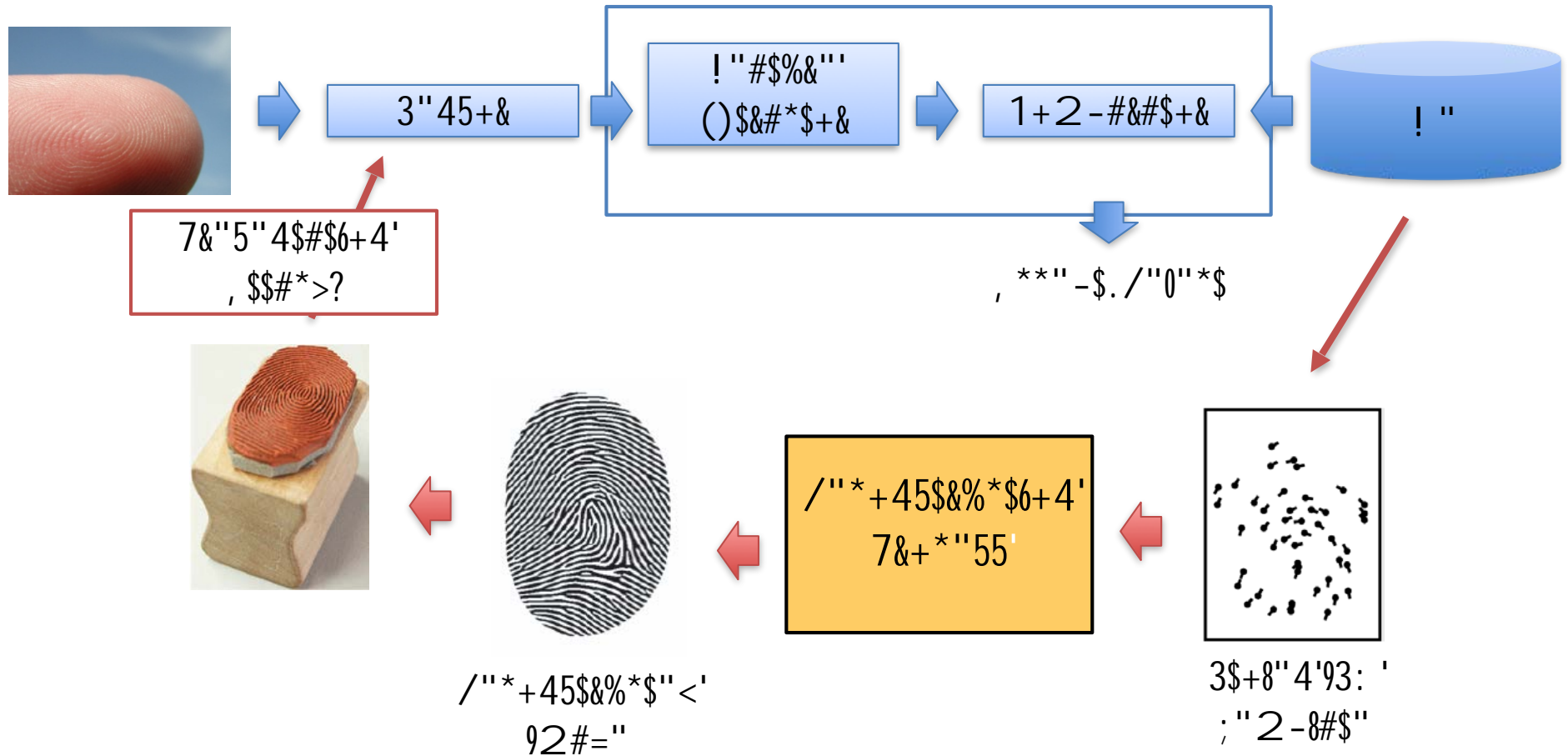


Image Source: Marta Gomez-Barrero, 2018

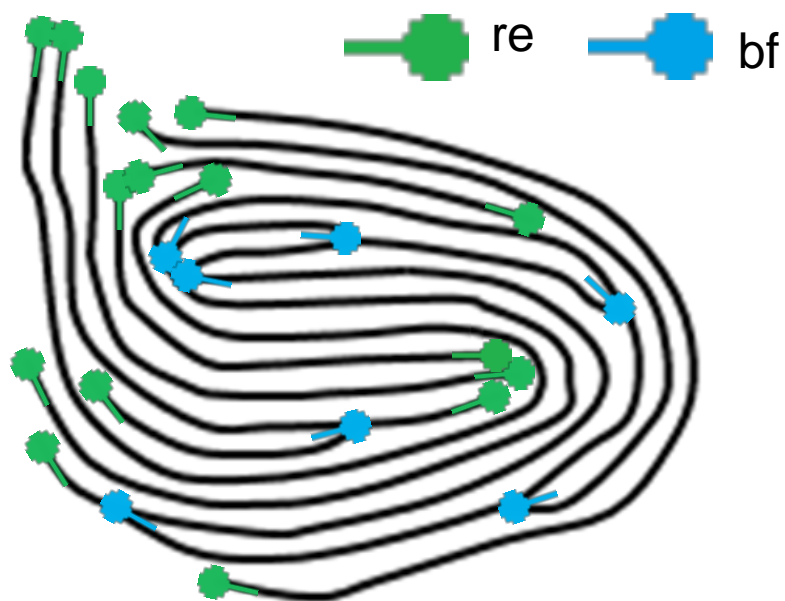
- [Cappelli2007] R. Cappelli et al. „Fingerprint Image Reconstruction from Standard Templates“, in IEEE PAMI, (2007)
- [Galbally2009] J. Galbally et al. „Template Reconstruction“, in Pattern Recognition Letters, (2009)

Sample Reconstruction

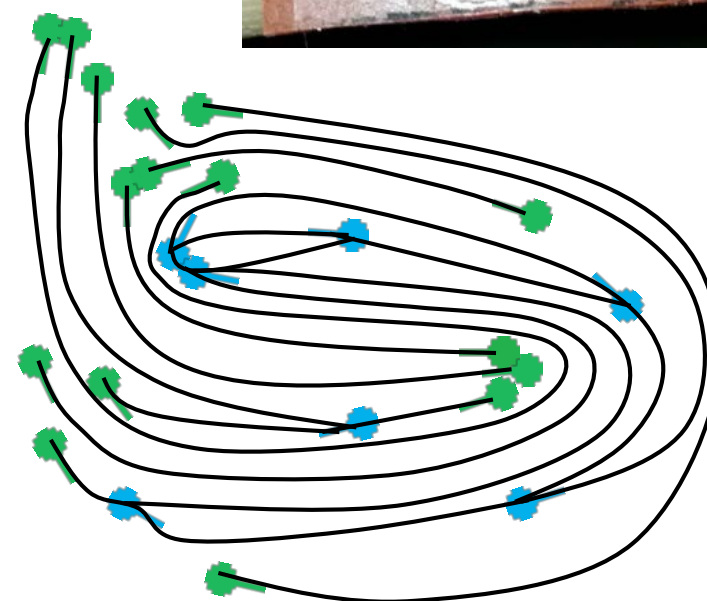
Processing the attack

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

Sample reconstruction!



original sample

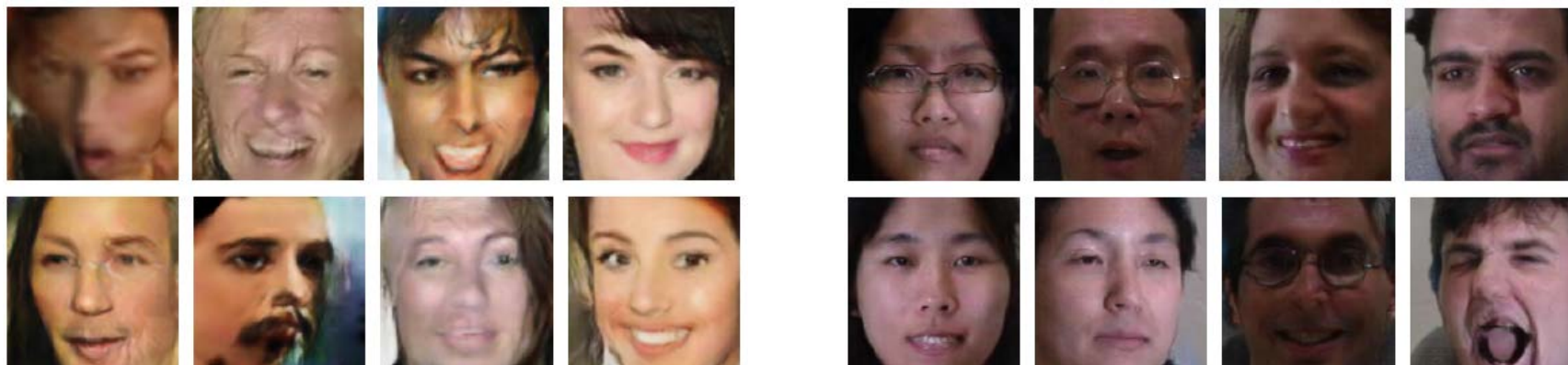


reconstructed sample

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]



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

Hill Climbing Attack

Assumption:

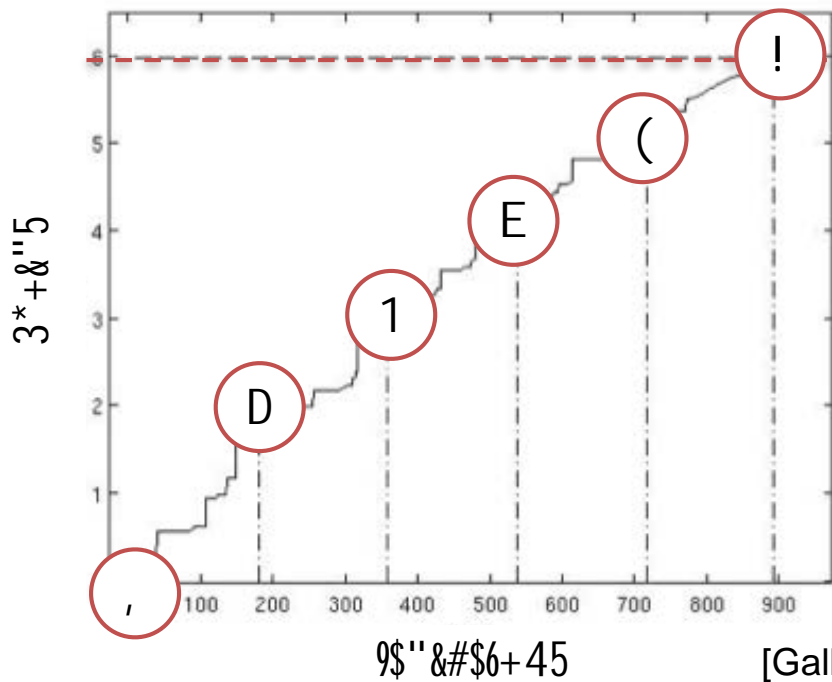
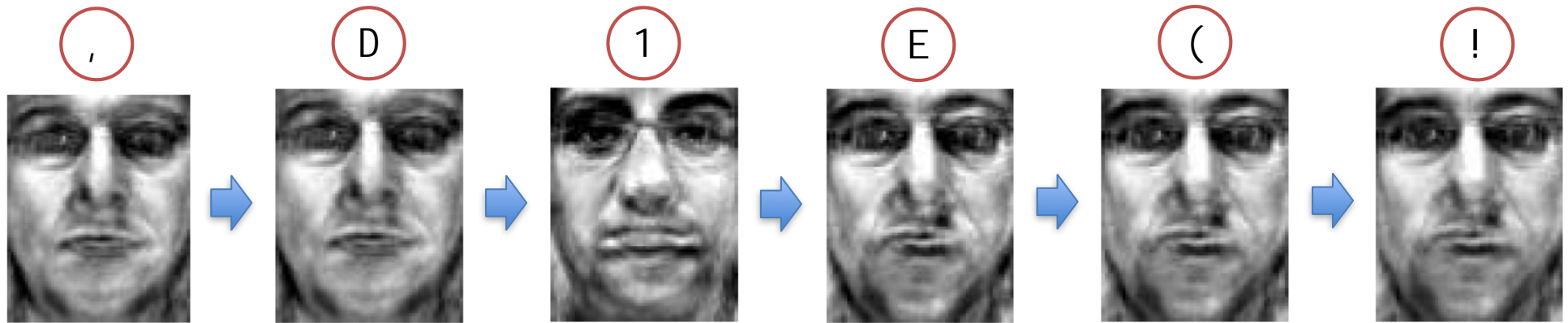
- The template is **not** accessible
 - ! Thus reconstruction of the sample is not possible - good!
- But we have a verification system that will create **comparison scores**

Attack vector

- Create a **synthetic sample** and compare the the derived **feature vector** with the reference template
- Use the Hill-Climbing approach, until the adapted synthetic sample (and the derived feature vector) is **sufficiently similar** to the attacked reference template
 - ! The process will take up to millions of iterations

Hill Climbing Attack

Example: Attack attack for face recognition



A\"&6B6*#\$6+4'
; C&\"5C+8<

; C\"#\$#\$*>'F#5'
5%*\"55B%8G'#4<'F\"'
+48H'4\"\"<\"<'#*\"55'
\$+'\$C\"5*+&\"5



;&=#\$@(4&+88\"<'
3#2-8\"

[Galbally2009] J. Galbally et al. „Hill-climbing attack“, in BiDS conference, (2009)

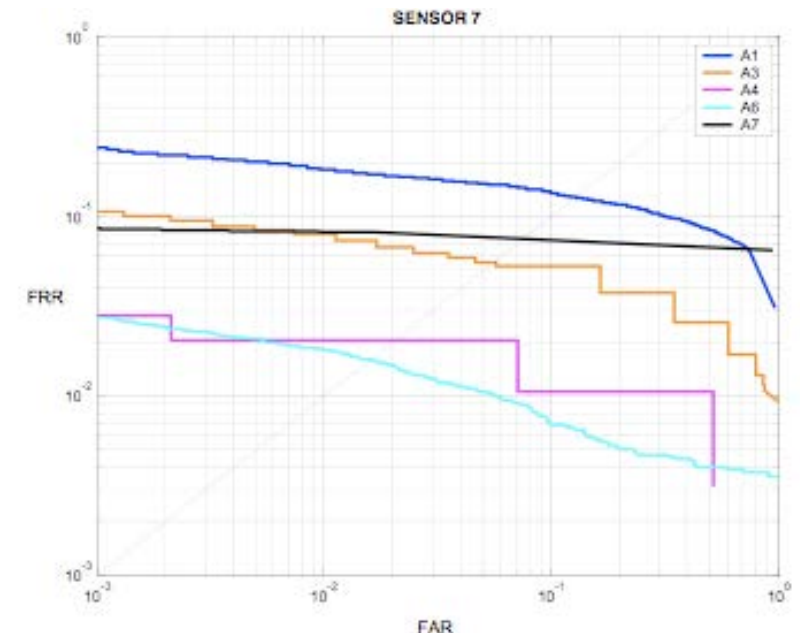
Hill Climbing Attack

Assessment

- Synthetic biometric samples can be constructed such that they are **fairly similar** to the biometric reference
- A complete and visually satisfying reconstruction is not necessary

Countermeasures against hill climbing attack

- **Quantization** of the comparison score
- Output the comparison score only if the score is above threshold and comparison is likely to be a mated comparison trial

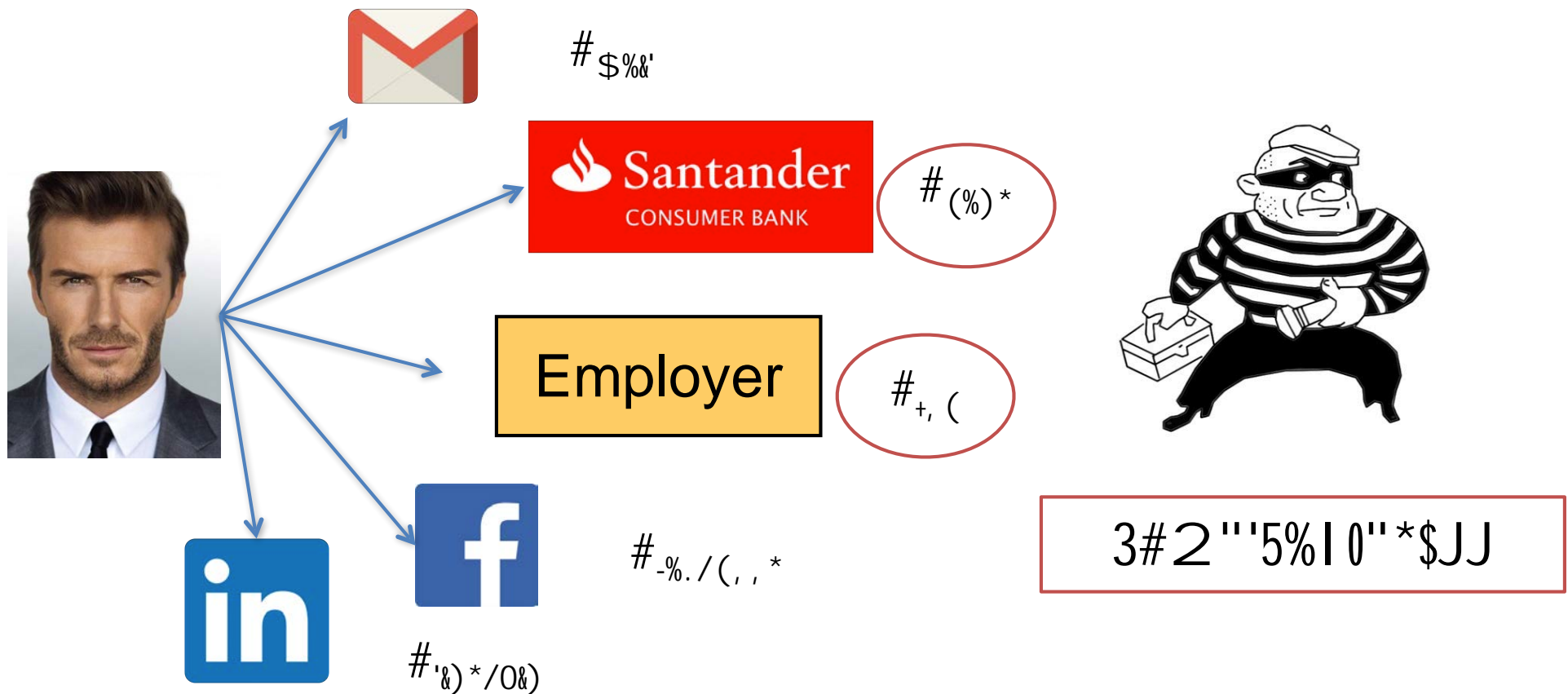


Biometric Template Protection

Further Risks for Biometric References

Cross-Comparison attacks

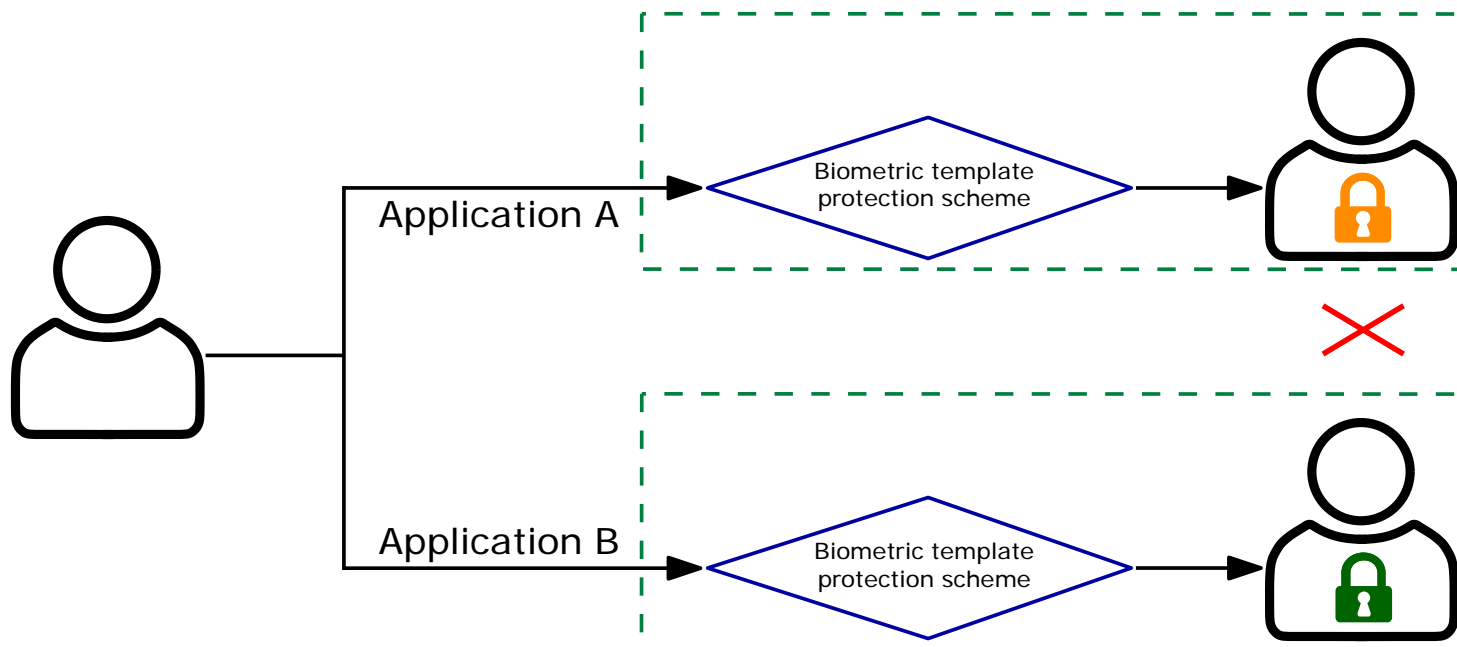
- We want to enrol with a single biometric characteristic in **different applications**



Further Risks for Biometric References

Cross-Comparison attacks

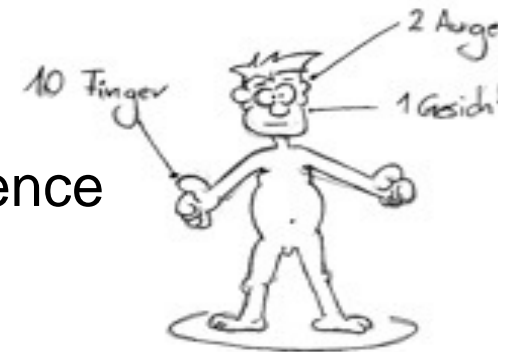
- Enrol with a single biometric characteristic in **different applications**
- Prevent the generation of **profiles**
 - ! **Cross-correlating** protected **templates across** different **systems** and databases must **not** be **possible** to avoid profiling



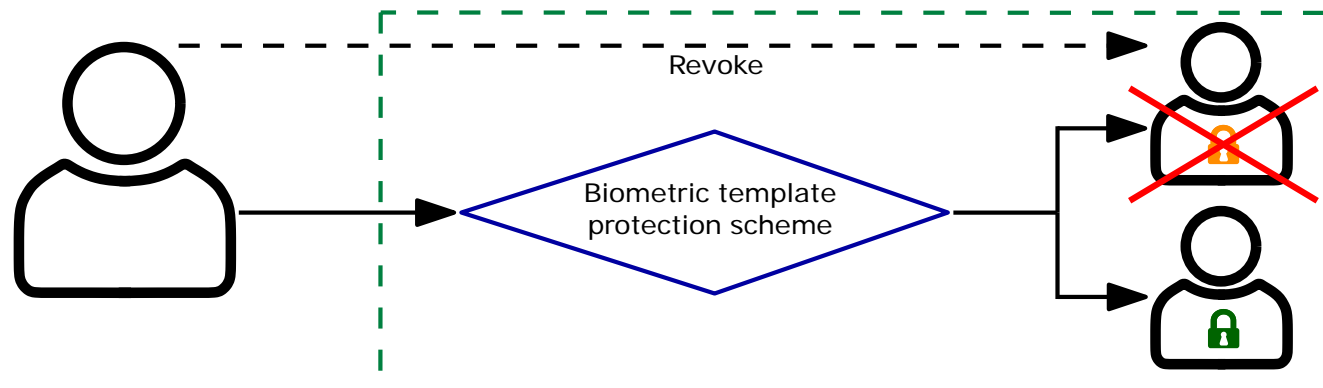
Further Risks for Biometric References

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 the biometric reference?

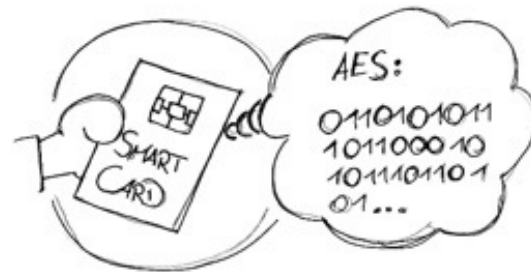
Conventional cryptography yields two main drawbacks

- **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!

Challenges

Classical crypto / encryption does **not** solve the problem

- Data needs to be decrypted prior to comparison



Template Protection

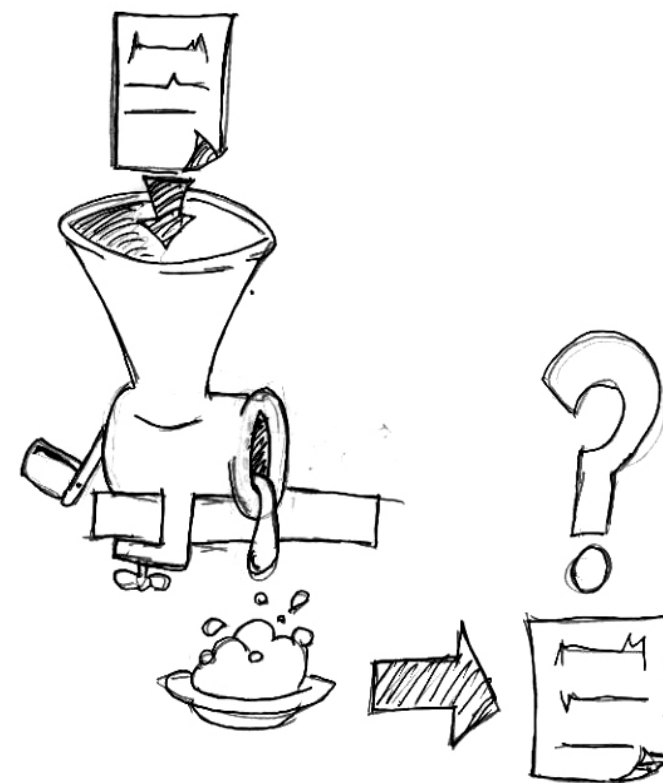
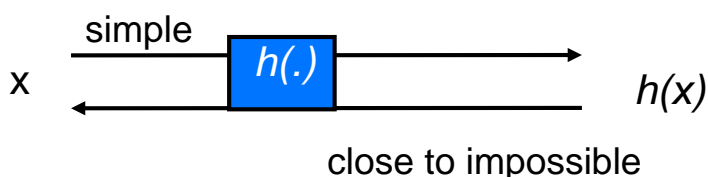
Hashing the reference?

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

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

- Authentication:

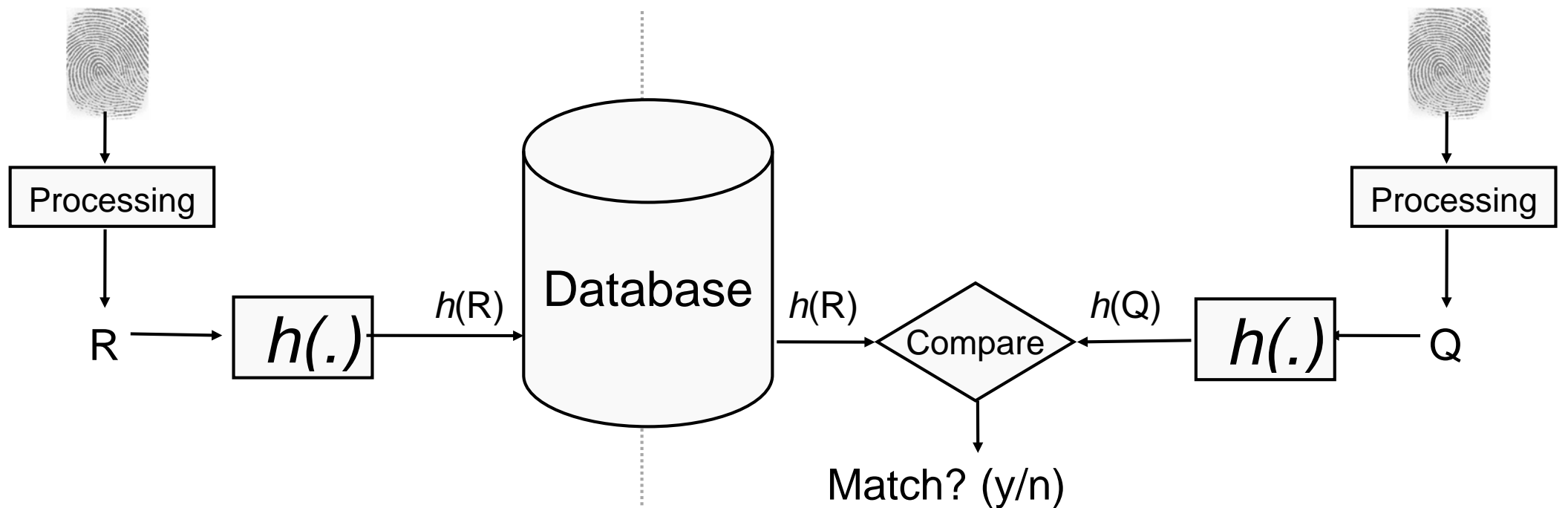
```
hash(input) == hash(password)
```



Template Protection with Hash functions

Enrolment

Verification



$h(\cdot)$ = 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

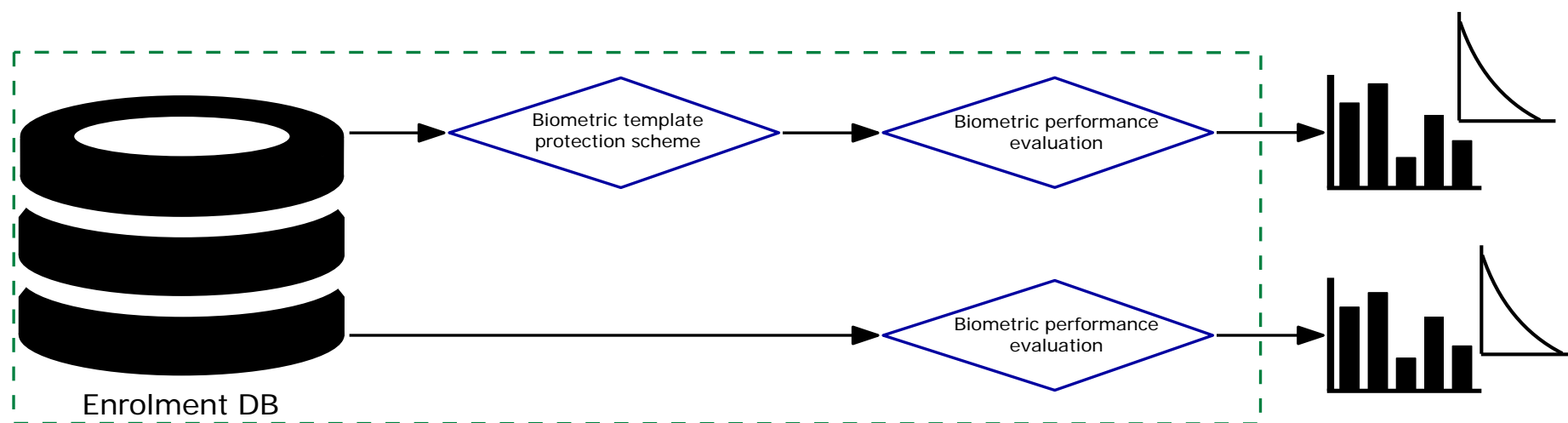
[Br2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: "A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008)

<http://www.christoph-busch.de/files/Breebaart-BTPReferenceArchitecture-BIOSIG-2008.pdf>

Biometric Template Protection

Expectation

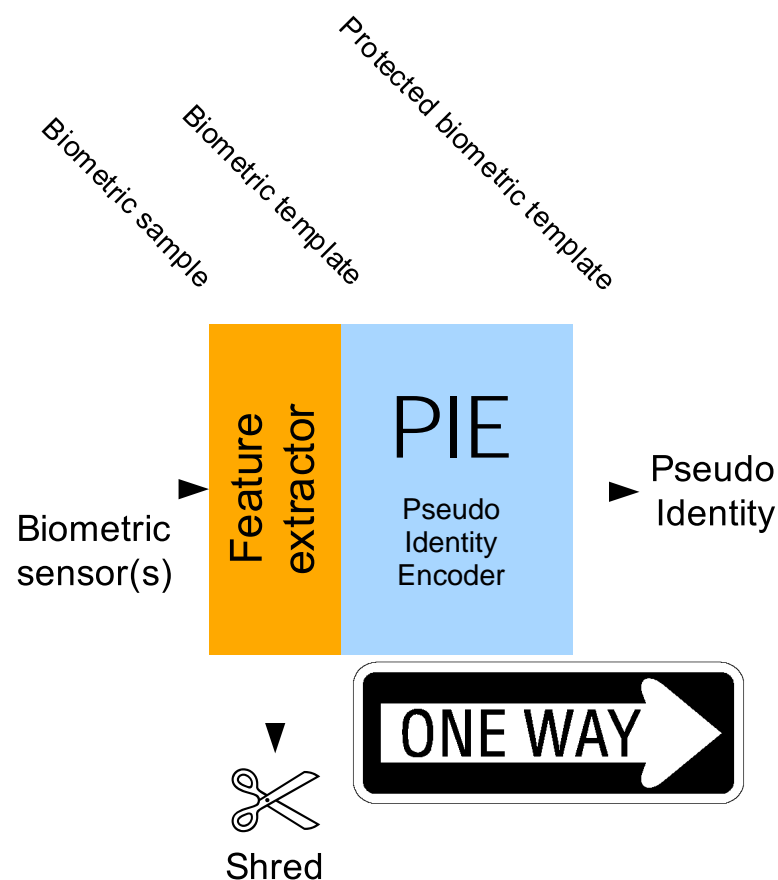
- The biometric performance of the protected system must not be (severely) impaired by the template protection scheme.



Pseudonymous Identifier Framework

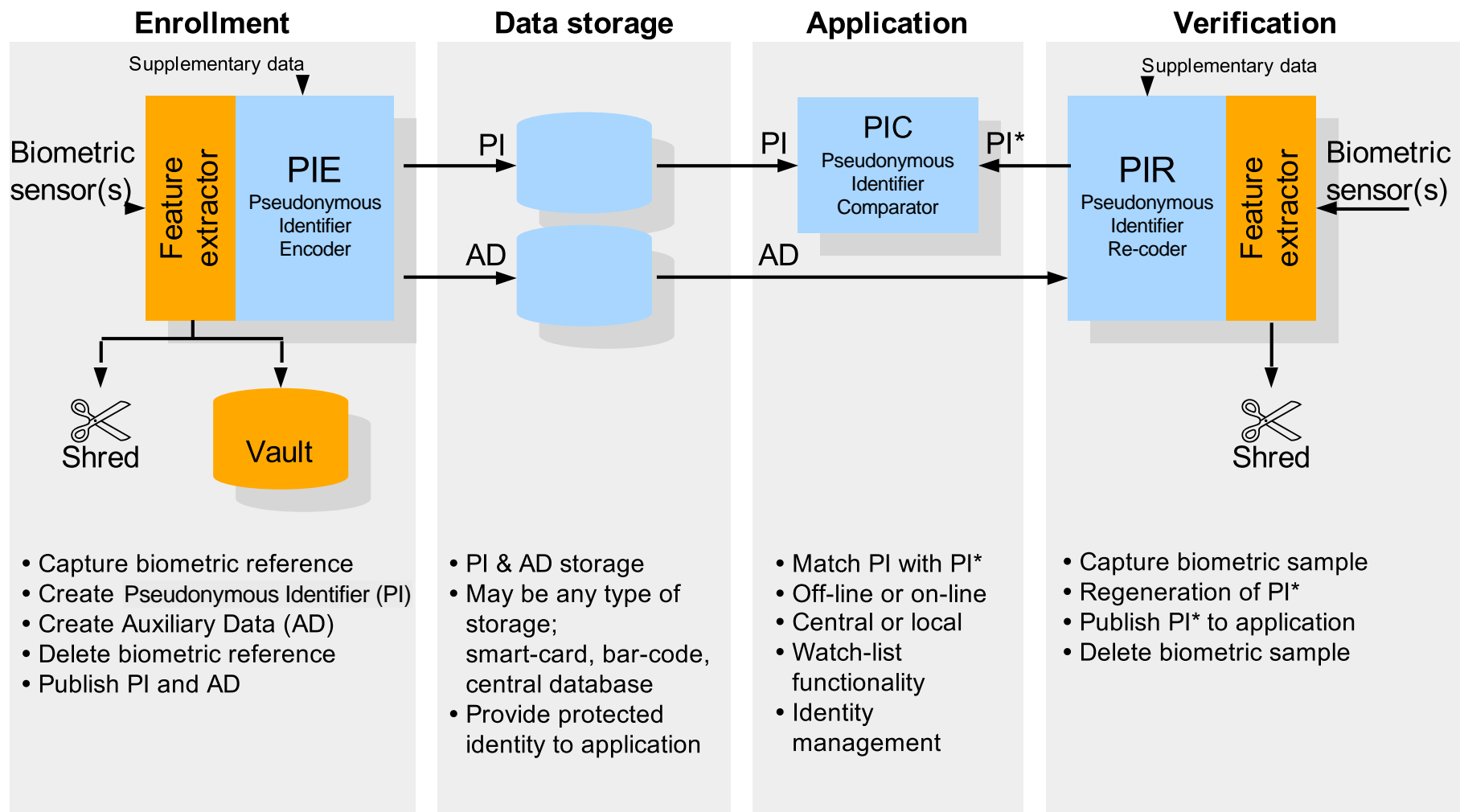
BTP Framework defined in ISO/IEC 24745

- 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**



PI Framework in ISO/IEC 24745

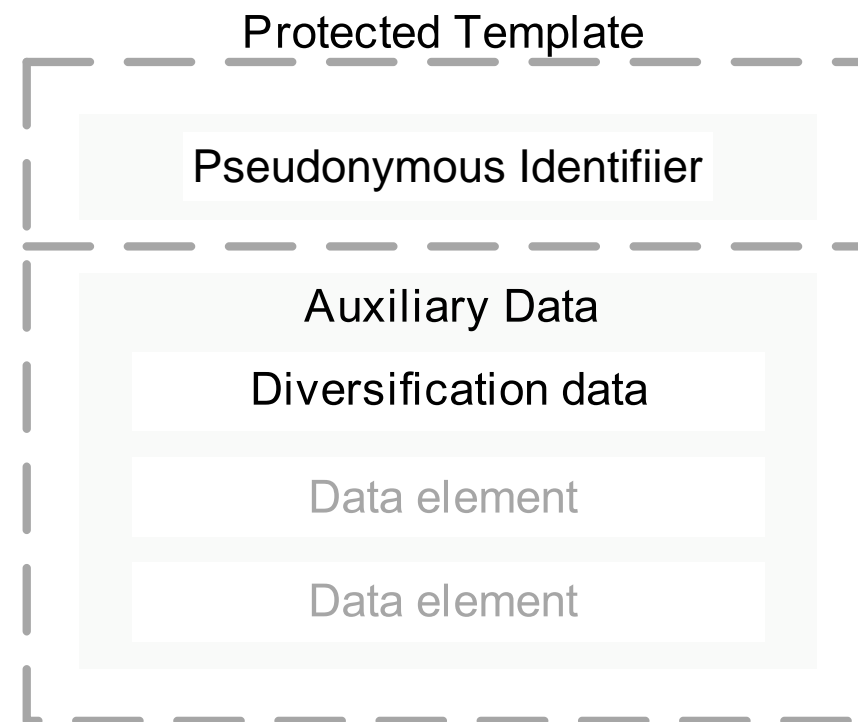
- Standardized architecture for renewable biometric **references**



Protected Template Structure

Resulting **Protected** Template

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



Survey of BTP Algorithms

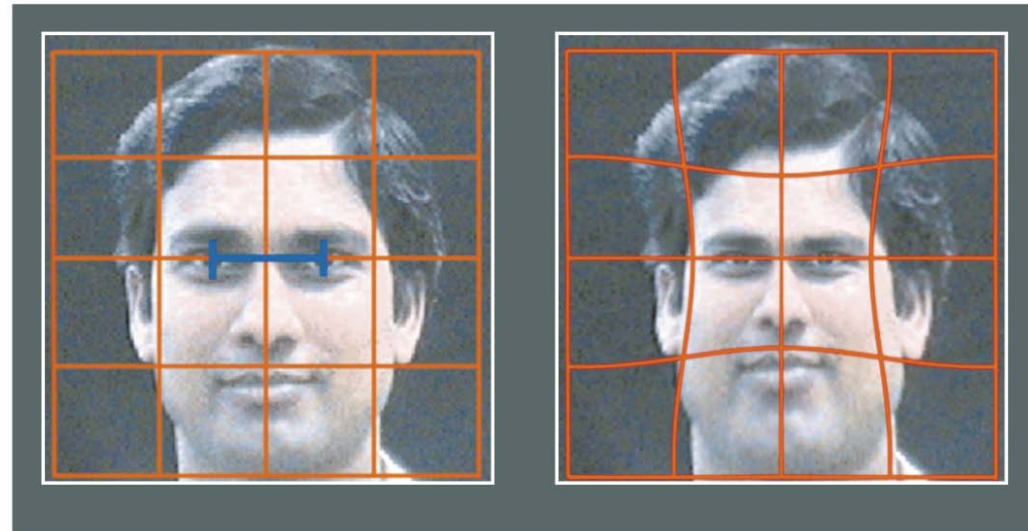
BTP approaches: **Cancelable biometrics**

- 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.

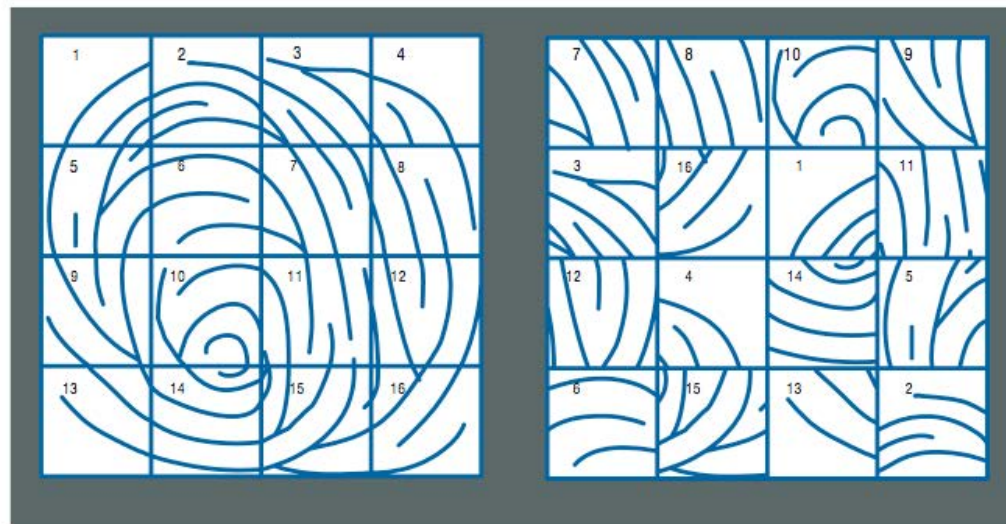
Cancelable Biometrics

Transformation of a signal prior to feature extraction

- Grid morphing
[Ratha2001]



Block permutation



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.

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 $h(S) = h(\text{DEC}(C))$

Verification

- X is binary probe template
- $X + AD = C'$
- $S' = \text{DEC}(C')$
- $h(S) == h(S') ?$

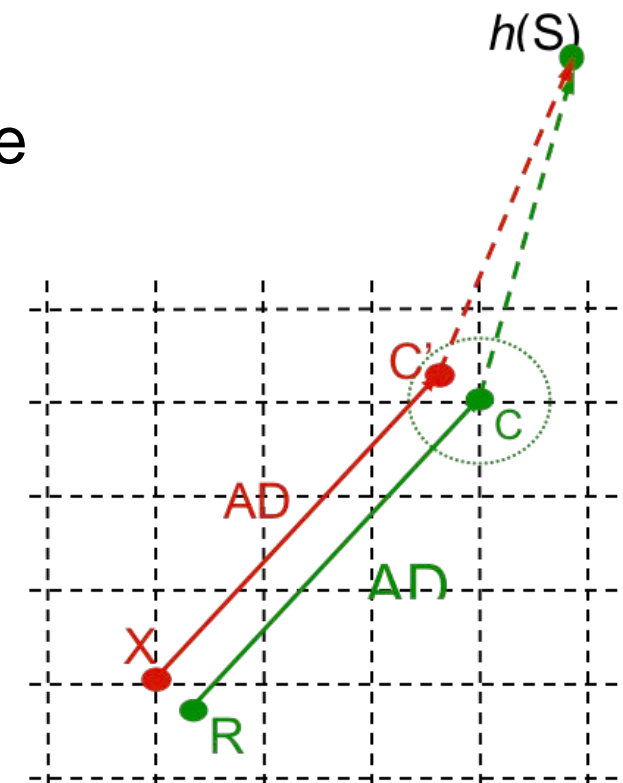
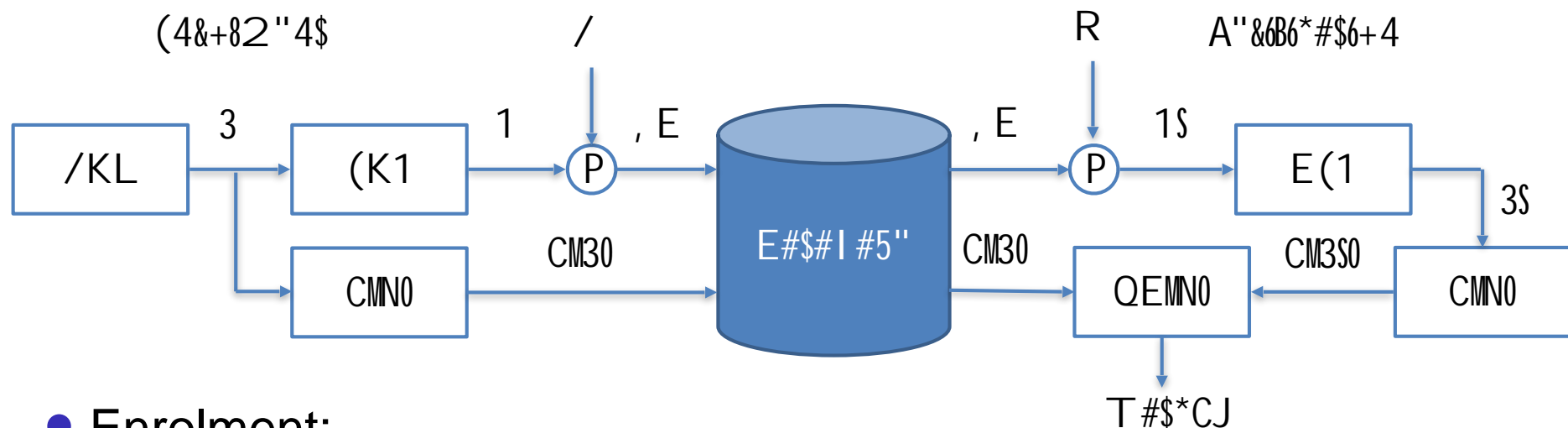


Image Source: Philips Research 2006

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
- ! $AD = C \text{ XOR } R$ is the public AD
- ! $\{h(S), AD\}$ are stored as reference

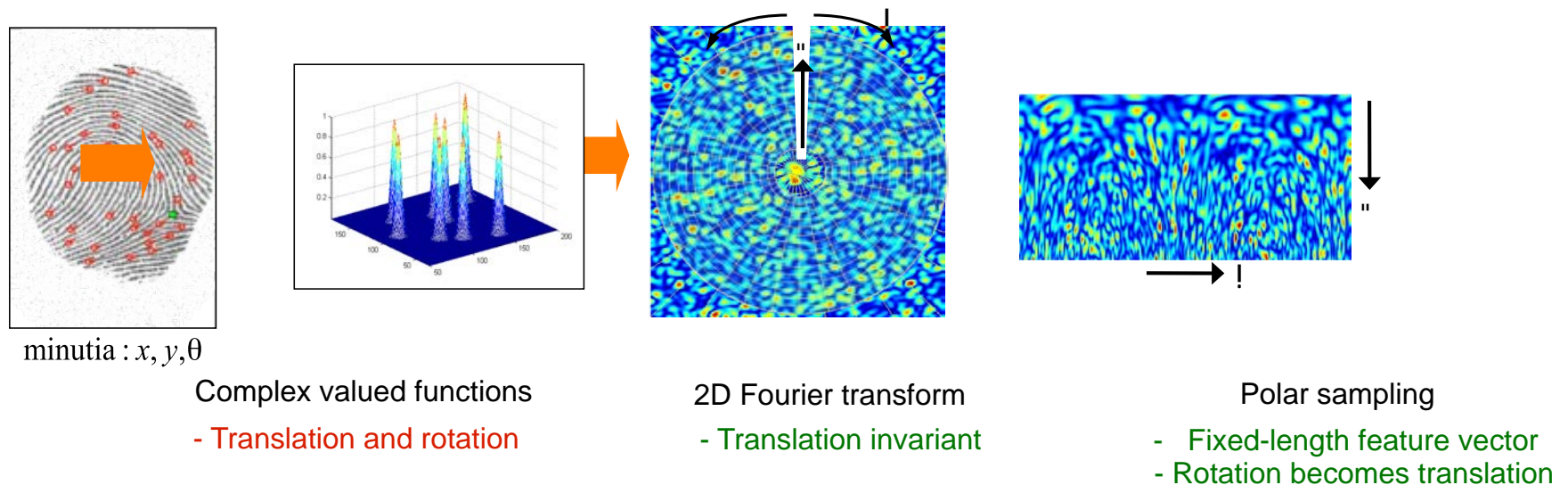
- Verification:

- ! $C' = AD \text{ XOR } Q$ (query vector)
- ! $HD(C, C')$ needs to be smaller than the error correction capabilities

Fixed Length Minutiae Feature Vectors

Spectral Minutiae (SM) based Fuzzy Commitment

- Univ. of Twente [Xu2009]



- 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

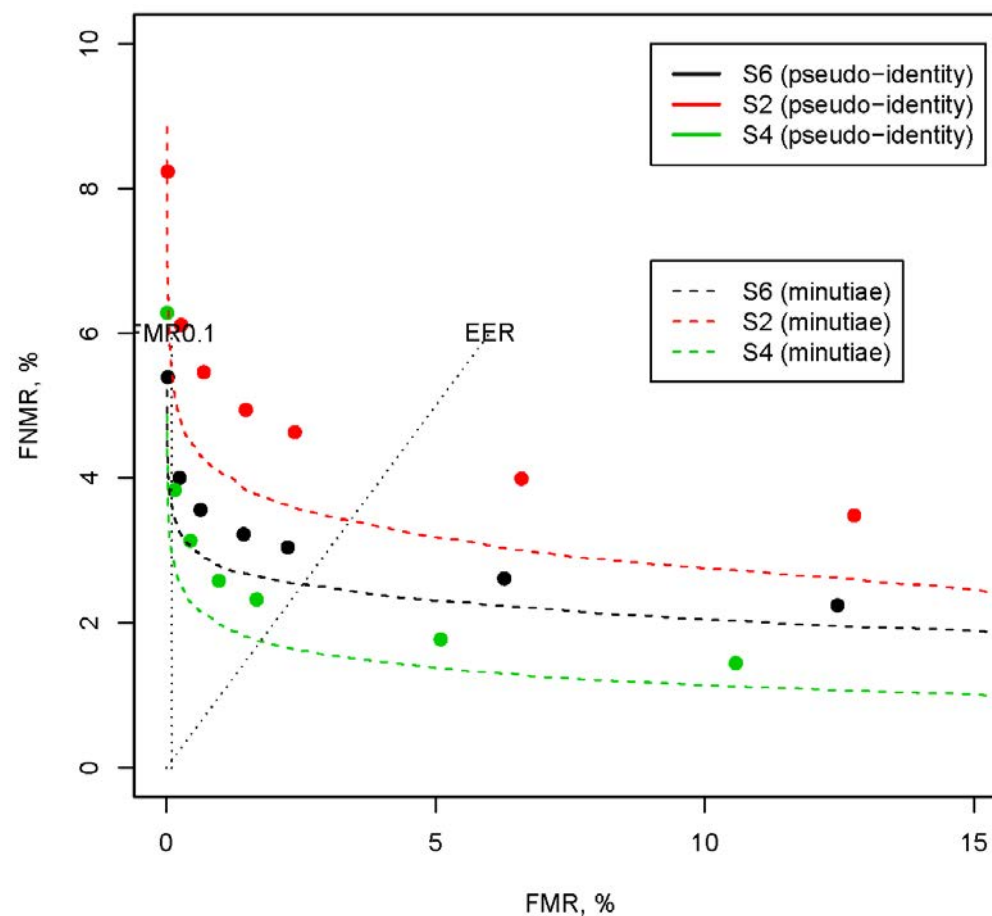
- 6 scanners, 100 subjects
- ~ 72000 images
- 12 sessions
 - ! on separate days
- Uncontrolled
 - ! No image quality control
- Controlled
 - ! Quality was controlled to some extent visually e.g. by wetting fingers if necessary
- Sequestered database -
 - ! No access granted to algorithm developers



TURBINE Project - BTP Performance Testing

Performance results - Pseudonymous Identifier level

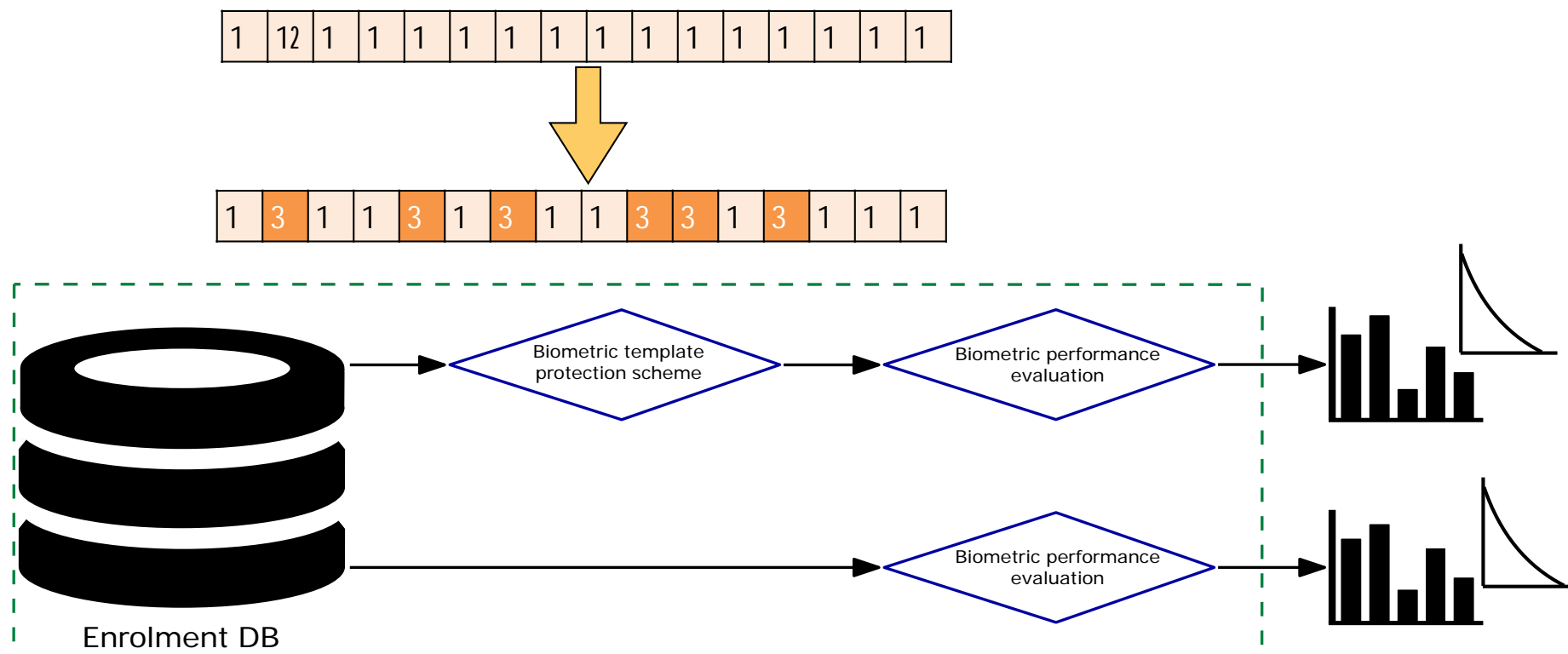
- One example of a PI algorithm.



Biometric Template Protection

Protection at the **same accuracy level** is possible

- Bloom filter-based **pseudonymous identifiers**



[Ra2014] C. Rathgeb, F. Breiting, 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

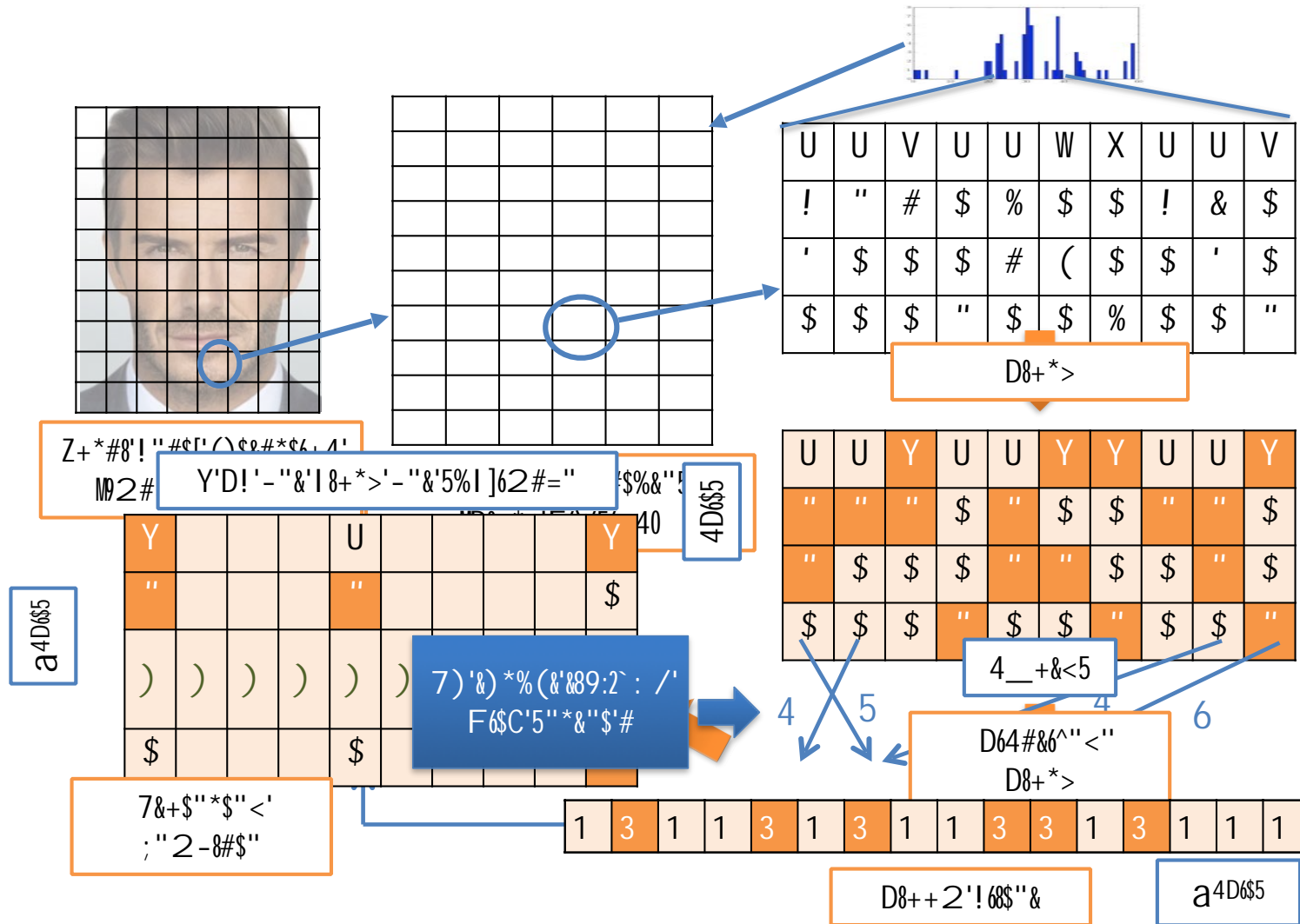
- A Bloom filter b is a space-efficient data structure representing a set S to support membership queries
- b is a **simple bit array** of length n (initially all bits are set to 0)
- To represent $S = \{x_1, x_2, \dots, x_m\}$, k independent hash functions h_1, h_2, \dots, h_k with range $[0, n-1]$ 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**

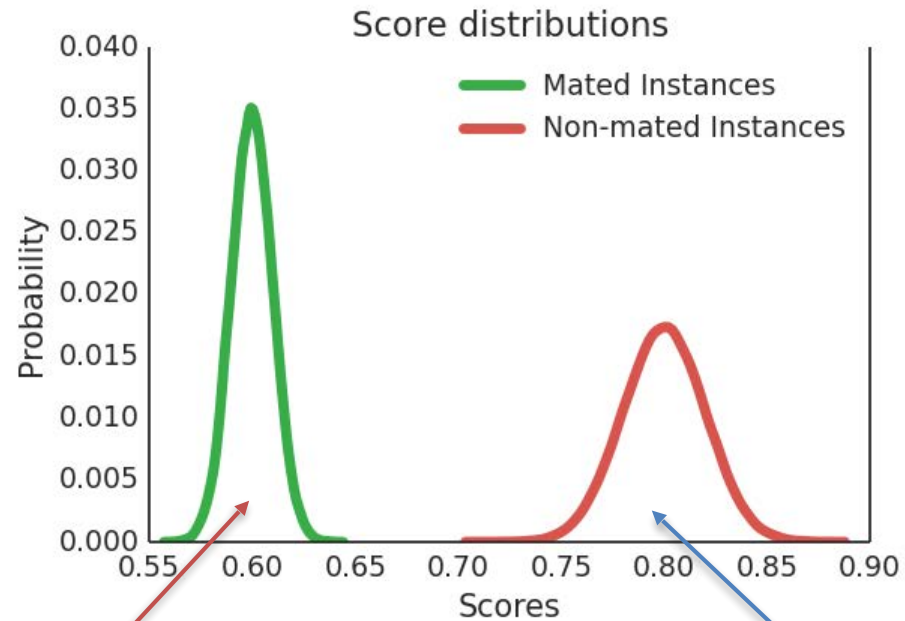


BTP Unlinkability Evaluation

Cross-Comparison Attacks: How to?



#+, (# (%)*
 ↓
 *'b'+, -M#+, (G2# (%)*0



'C"&""! '5%"55??' "

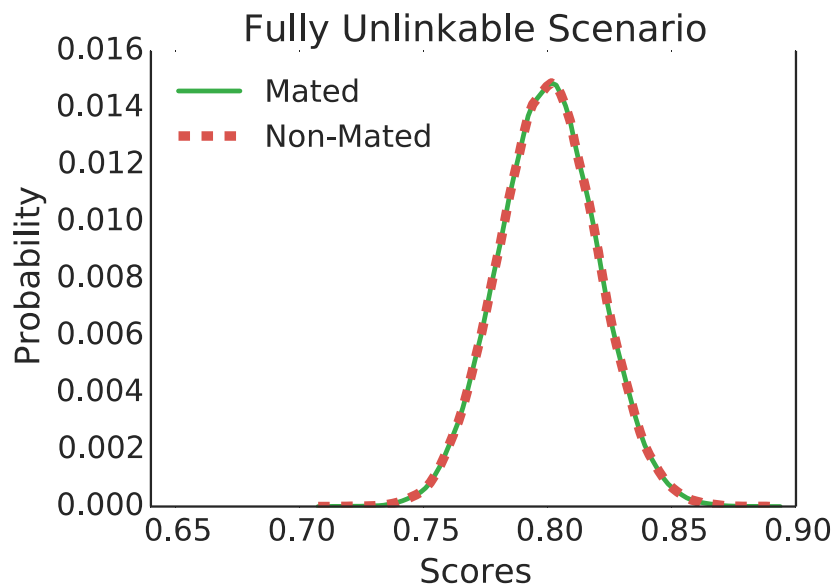
*'C"&""! '\$&H'#=#64??' !

'65'\$C"'<6556268#&6\$H'5 +&"" +B'\$C"'5H5\$" 2'

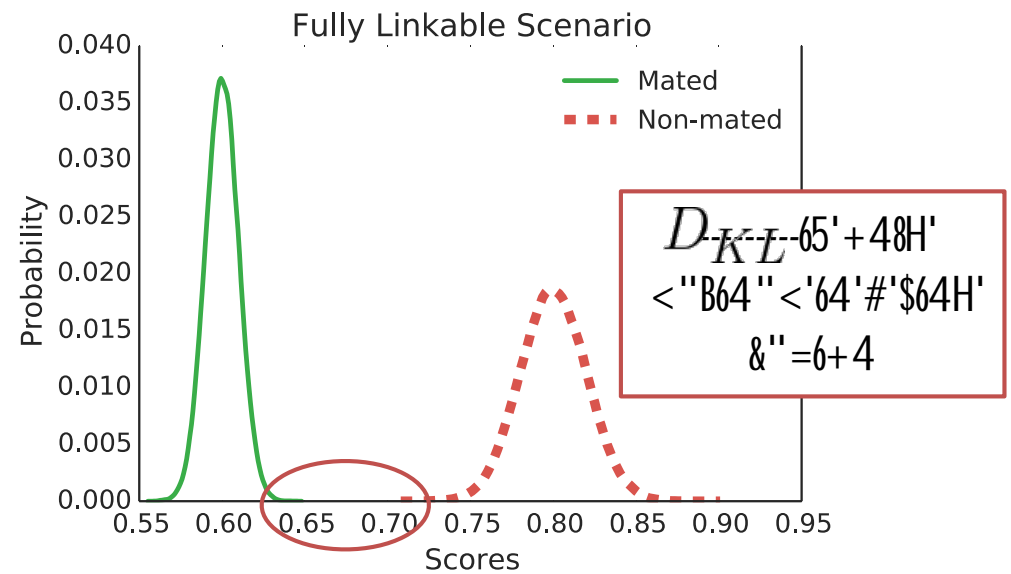
BTP Unlinkability Evaluation

Cross-Comparison Attacks - Unlinkability Analysis

- Plot **Mated** and **Non-mated** comparison score distributions, for templates protected with different keys.
- How to analyse those distributions?
 - Kullback-Leibler (D_{KL}) divergence?



$$D_{KL} \ll b'U[U$$



$$D_{KL} \approx 65' + 48H'$$

$$< "B64 " < '64' \# '$64H'$$

$$\&" = 6 + 4$$

$$D_{KL} \ll b'U[UUUc$$

$$D_{KL} \approx 65'4 + \$'I + \%4 < " < @'D_{KL} \in [0, \infty)' 滯' < 6BB6 * \%8\$' \$ + '* + 2 - \# \& "" 5H5\$" 25$$

BTP Unlinkability Evaluation

Cross-Comparison Attacks - Unlinkability Analysis

New Approach

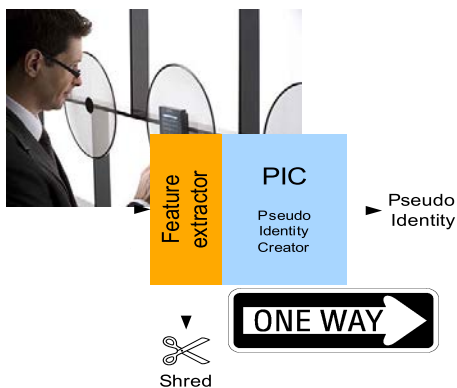
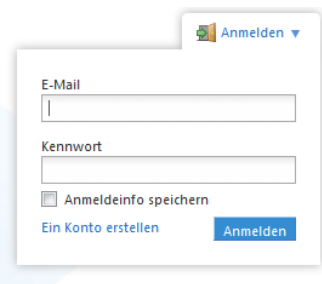
- Two measures:
 - Local measure $D_{\leftrightarrow}(s)$! for which scores is the system vulnerable?
 - Global measure $D_{\leftrightarrow}^{sys}$! how can we compare two systems globally?
- Both bounded in $[0,1]$, and defined for all dissimilarity scores.
- General measures, valid for all BTP schemes

Revised Benchmark of Authentication

Non-Invertibility !
from the reference

Revocability and !
Renewability

Strong link to the
data subject



Homomorphic Encryption

BTP Approaches

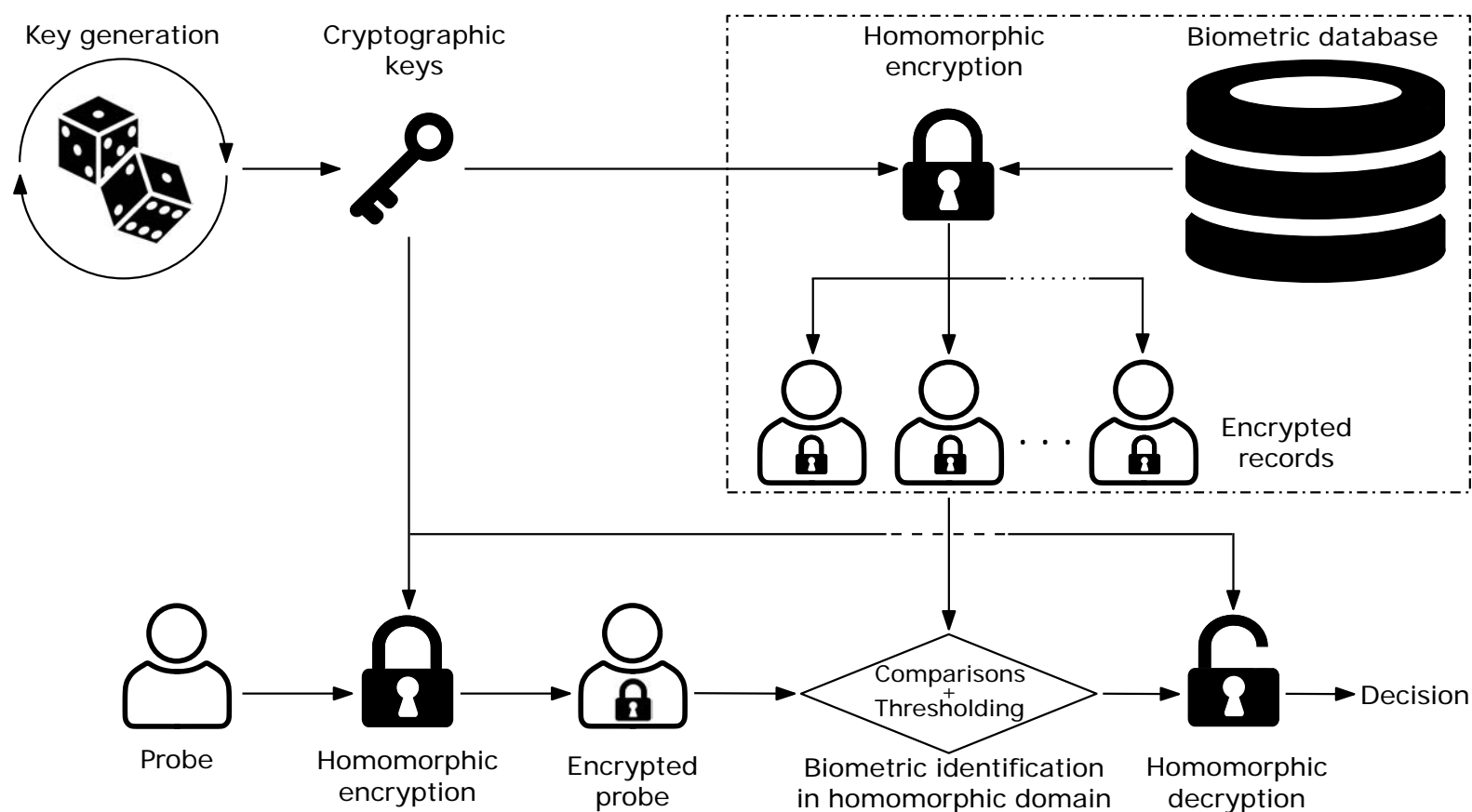
Biometrics in the Encrypted Domain

- **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

Homomorphic Encryption

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

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

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

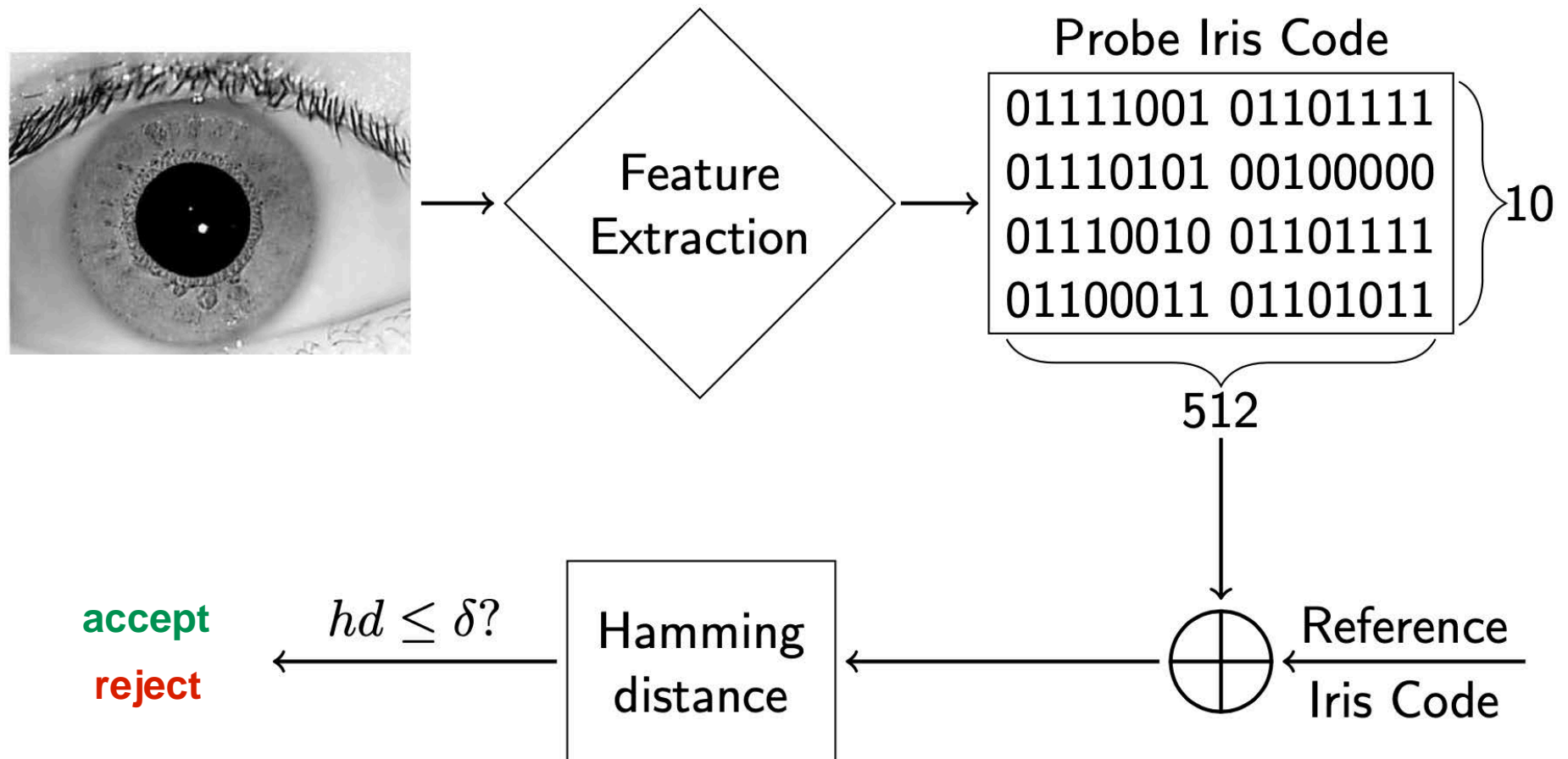
[Kolb2019] J. Kolberg, et al.: "Template Protection based on Homomorphic Encryption: Computational Efficient Application to Iris-Biometric Verification and Identification", in Proceedings of IEEE WIFS, Delft, NL, (2019)

[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

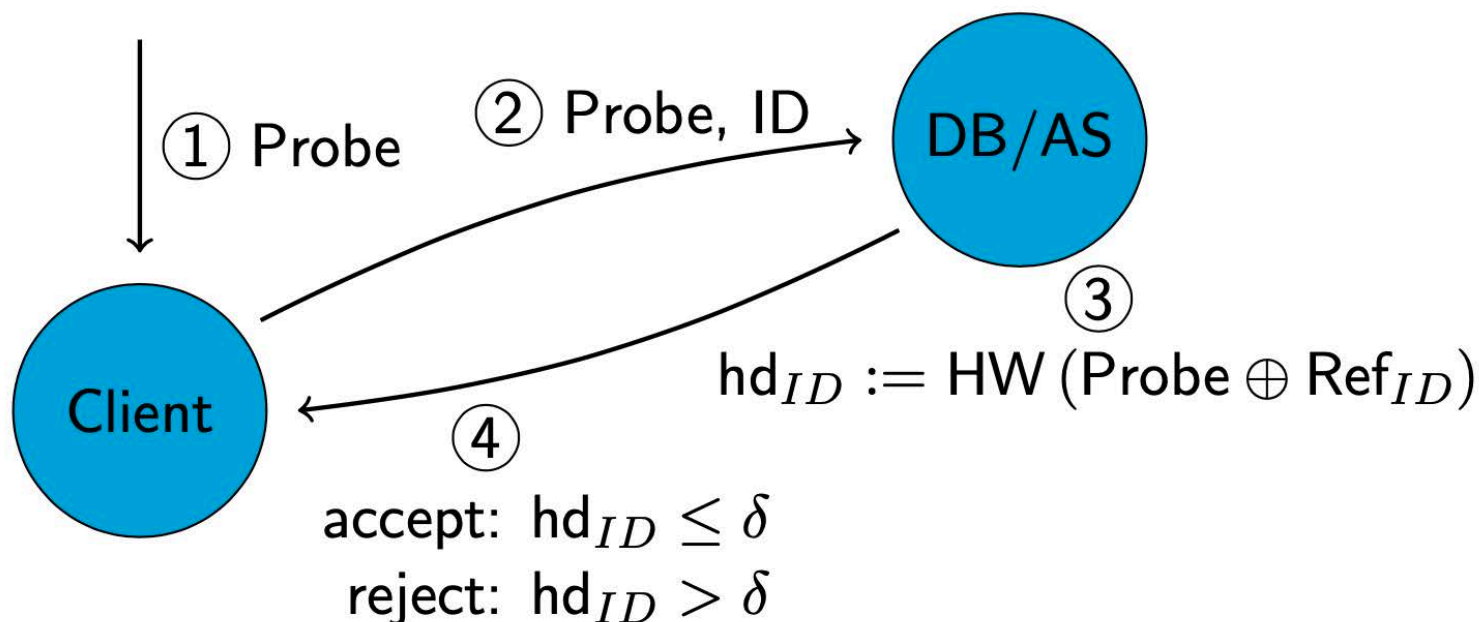


BTP Approaches

Homomorphic Encryption

- Example: Iris Recognition

! unprotected verification



BTP Approaches

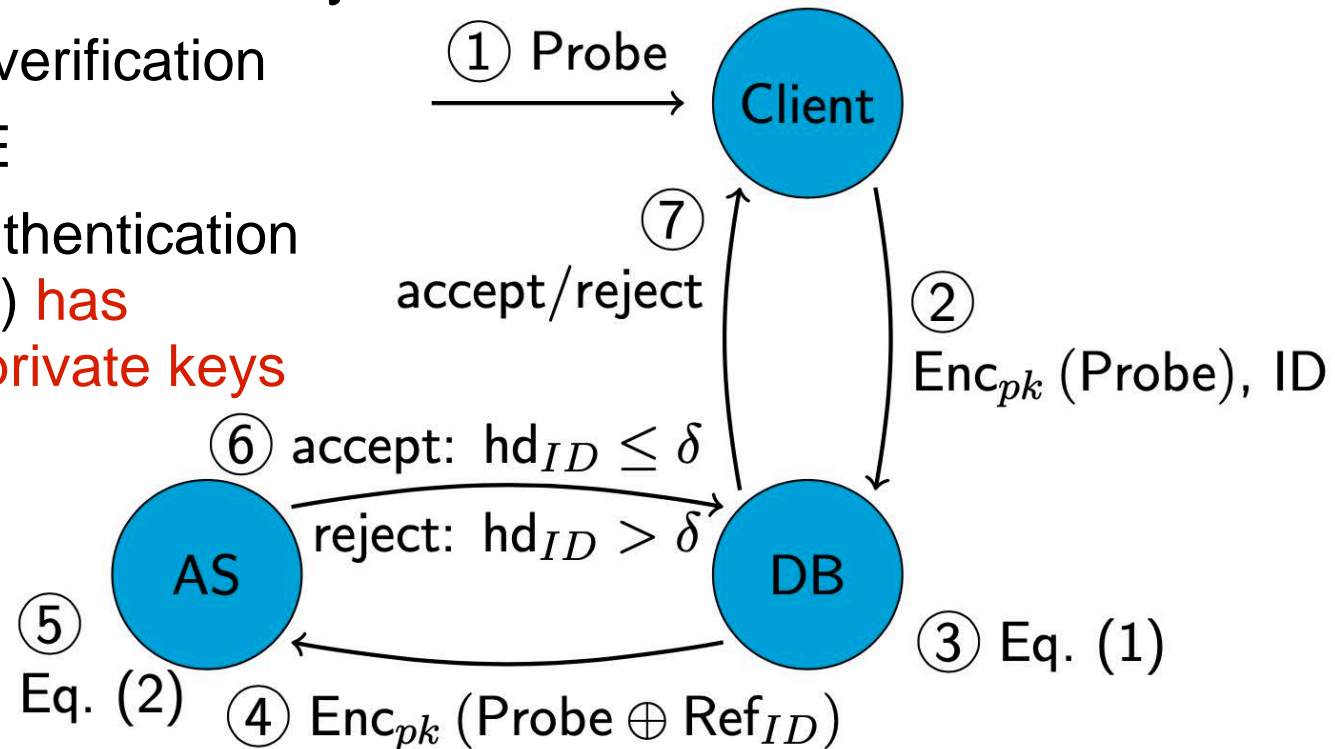
Biometrics in the Encrypted Domain

- A **protected** biometric system

! **NTRU** HE verification

! additive HE

! **only** the Authentication Server (**AS**) has access to **private keys**



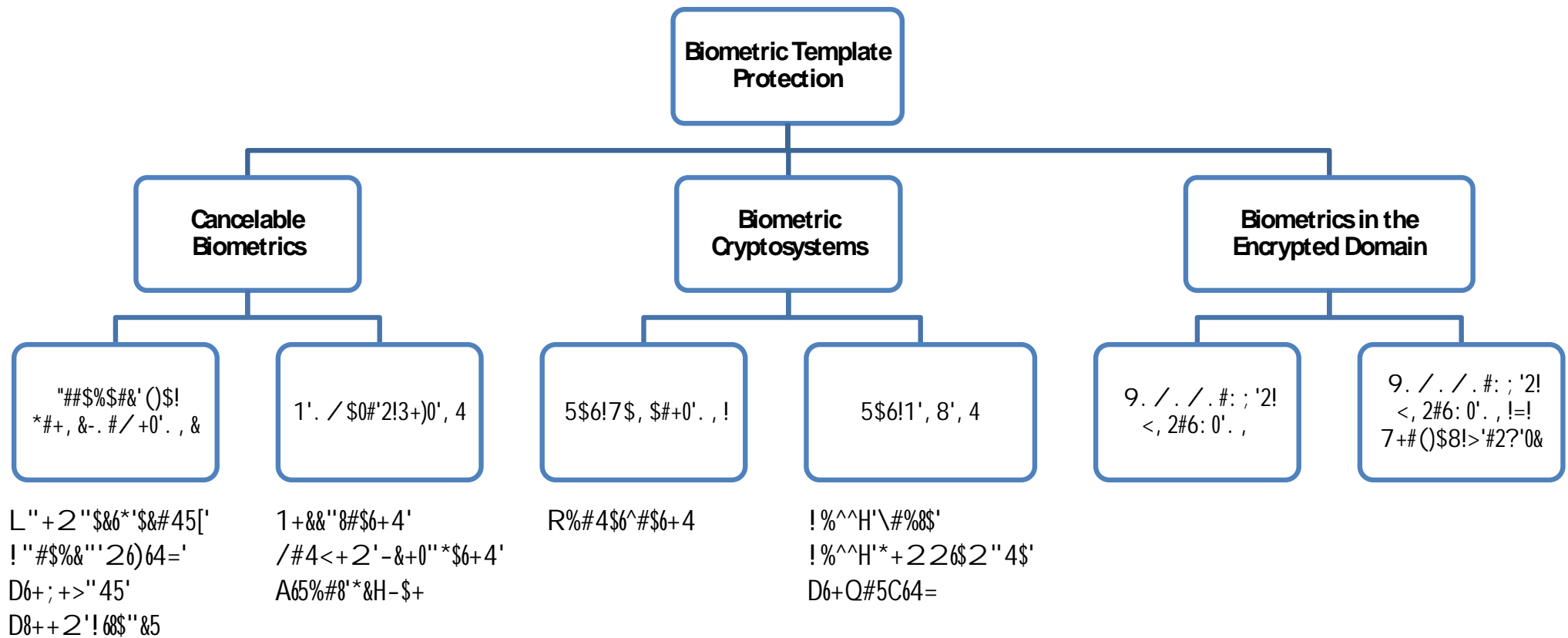
$$Enc_{pk}(\text{Probe} \oplus \text{Ref}_{ID}) := Enc_{pk}(\text{Probe}) \oplus Enc_{pk}(\text{Ref}_{ID}) \quad (1)$$

$$hd_{ID} := HW(Dec_{sk}(Enc_{pk}(\text{Probe} \oplus \text{Ref}_{ID}))) \quad (2)$$

!

Overview

BTP approaches: 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.
- BTP schemes based on Bloom filters or Homomorphic Encryption comply with ISO/IEC IS 24745.
- We need to follow a standardised methodology for a standardised security and privacy evaluation of BTP schemes.

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
- Cross-comparision-resistant RBRs **prevent** from **tracking** without consent in case biometric databases are compromised

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. Breitingner, 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)

References

Web

- General Data Protection Regulation (GDPR)
<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
- European Convention on Human Rights (ECHR)
http://www.echr.coe.int/Documents/Convention_ENG.pdf
- European Convention 108
<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>
- Ann Cavoukian: „Privacy by Design“;
<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>

Complementary reading

- M. Meints et al.: „Biometric Systems and Data Protection Legislation in Germany“, 2008
- ISO/IEC 24714-1: „Guide to the accessibility, privacy and health and safety issues in the deployment of biometric systems for commercial application”

Practical

Practical

During the coffee break

- Start Matlab R2020b (Windows) "local" on your computer.
- In addition the following Add-Ons must be installed (in Matlab under: Home -> Add-Ons -> Get Add-Ons):
 - ! DSP System Toolbox
 - ! Communications Toolbox
 - ! Signal Processing Toolbox
- Download the task framework
<https://christoph-busch.de/files/210510-prima-practical-material.zip>

Post-lecture Assignment

Post-lecture Assignment

You should write a **five** to eight **page** paper

- prior to **June 09** on one of the three topics
- 1.) The rationale behind GDPR Recital 51
 - ! Why is a latent face embedding derived from a facial image sensitive data, but the video footage with the facial image itself is not sensitive?
- 2.) Survey on bloom filter and homomorphic encryption
 - ! Which method is more promising to satisfy the requirements set forth in ISO/IEC 24745?
- 3.) Reaching fairness in biometric systems
 - ! What are the measures for fairness and why are they relevant ?

Use the BIOSIG 2021 paper template:

- Word: https://biosig.de/fileadmin/TG/BIOSIG/BIOSIG2021/LNI-Word-Template_en_final.doc
- LaTeX: https://biosig.de/fileadmin/TG/BIOSIG/BIOSIG2021/LNI-LaTeX-Template_en_final.zip

More Information

European Association for Biometrics (EAB)

- The EAB is a **non-profit**, nonpartisan **association**
<https://eab.org/>
- **EAB** supports all sections of the ID community across Europe, including **governments**, NGO's, **industry**, associations and special interest groups and **academia**.
- Our role is to promote the **responsible use** and adoption of modern **digital identity systems** that enhance people's lives and drive economic growth.
- **Free membership** for PhD students!
https://eab.org/membership/types_of_membership.html



More Information



European Association for Biometrics (EAB)

- Our **initiatives** are designed to foster **networking**

- ! Annual conference: EAB-RPC

<https://eab.org/events/program/195>

- ! Biometric Training Event

<https://eab.org/events/program/208>

- ! Workshops on relevant topics (e.g. Presentation Attack Detection, Morphing Attack Detection, Sample Quality, Bias in Biometric Systems)

<https://eab.org/events/>

- ! Online Seminar every second week

<https://eab.org/events/program/227>

- ! Recorded keynote talks

<https://eab.org/events/lectures.html>

- ! Monthly newsletter

<https://eab.org/news/newsletter.html>

- ! Annual academic graduation report

<https://eab.org/upload/documents/1799/EAB-research-report-2019.pdf>

Research opportunities

- Darmstadt (Germany) <https://dasec.h-da.de/>
- Gjøvik (Norway) <https://www.ntnu.edu/nbl>
- Internships for Msc and PhD students with possibility of a grant
- Collaboration with governmental and industrial partners



Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: christoph.busch@ntnu.no
Phone: +47-611-35-194