



Transformation of biometric data for privacy

Paris – France

13th June 2019





RESEARCH LAB

Research in *Digital Science*

*computer security, biometrics, cryptography,
machine learning, electronics, image
processing, artificial intelligence, Web
science...*



E-PAYMENT & BIOMETRICS UNIT



Research activities in computer security

Members

2 full professors, 5 associate professors, 12 PhD students, 2 post-docs, 5 R&D engineers

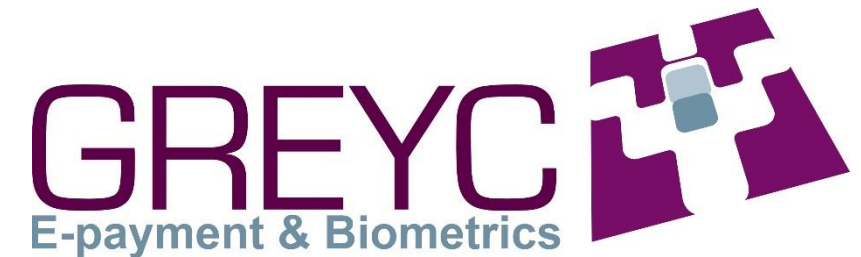
RESEARCH TOPICS

TRUST

Codes & applied cryptography
Architectures & applications with secure element
Random data & information security

BIOMETRICS

Definition of biometric systems
Evaluation of biometric systems
Protection of biometric data





PROTECTION OF BIOMETRIC DATA

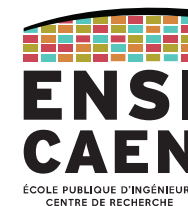
Motivations

State of the art

BioHashing

Evaluation

GREYCHashing



SECURITY

Why is it necessary ?

- ☐ Personal data
- ☐ Can be captured without any consent
- ☐ Difficult to revoke a biometric data
- ☐ Its classical encryption is not sufficient



ATTACKS

HOME » FEATURED ARTICLES » Hackers Have Stolen Almost Six Million US Government...

Hackers Have Stolen Almost Six Million US Government Fingerprints



GRAHAM CLULEY

SEP 24, 2015

IT SECURITY AND DATA PROTECTION



f 78 t 195 in 129 g+ + 33

The Office of Personnel Management (OPM) has revealed in a [statement](#) that when hackers breached its systems earlier this year they made away with approximately 5.6 million fingerprints – a significant increase from the 1.1 million previously reported.

As is now well known, in addition to fingerprint data being stolen the Social Security numbers, addresses, employment history, and financial records of some 21.5 million current and former US government employees was also stolen.

The good news is that they believe the opportunities for criminals to exploit the fingerprint data is currently limited.

But the bad news is that chances are that won't continue to be the case.



The Quint's investigation reveals glaring loopholes in the security setup of the Aa

Aadhaar's Dirty Secret Is Out, Anyone Can Be Added as a Data Admin

MEGHNAD BOSE | UPDATED: 04.01.18

INDIA 5 min read

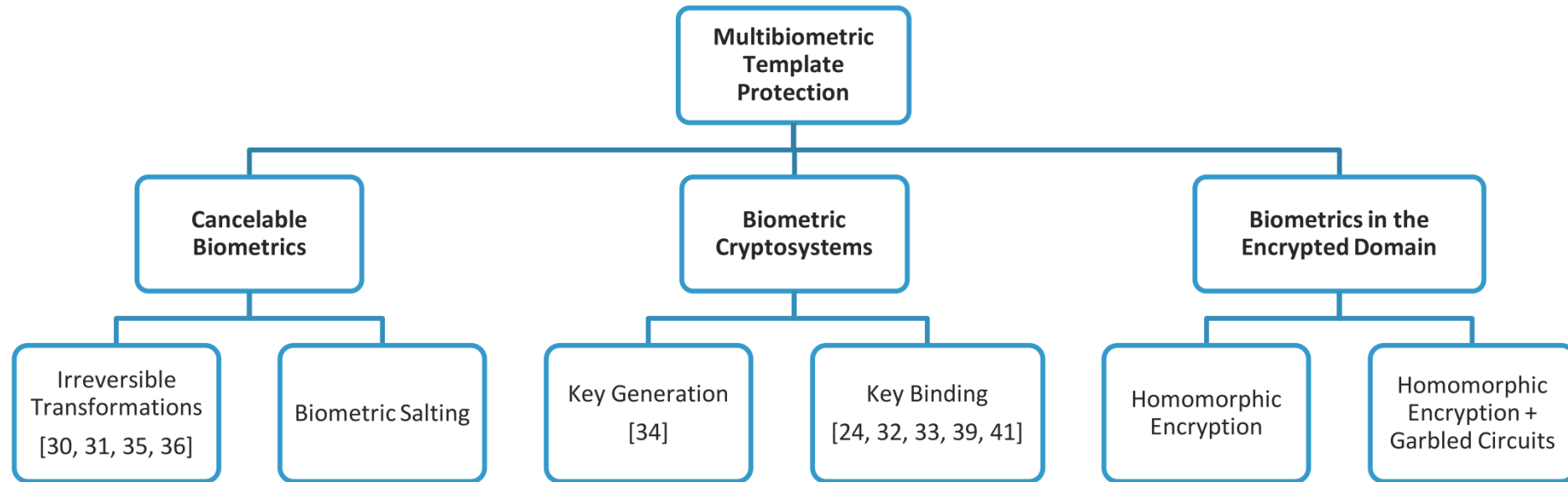
67.6k ENGAGEMENT



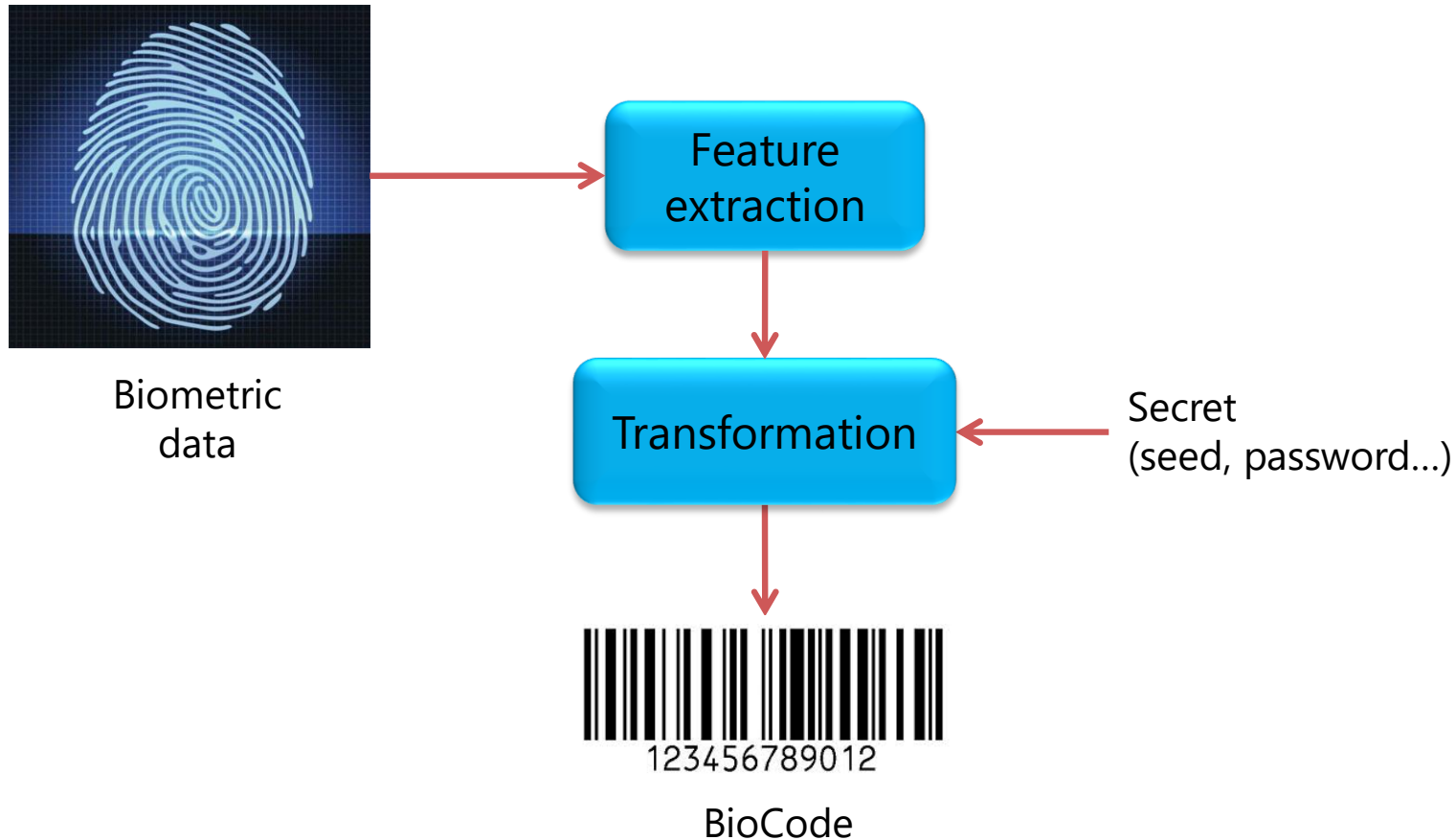
If you think your Aadhaar data is only in the hands of those authorised to access the official Aadhaar database, think again. Following up on an investigation by [The Tribune](#), **The Quint** found that completely random people like you and me, with no official credentials, can access and become admins of the official Aadhaar database (with names, mobile numbers, addresses of every Indian linked to the UIDAI scheme). But that's not even the worst part. Once you are an admin, you can make



Privacy Enabling Technologies schemes (algorithmic solutions) :



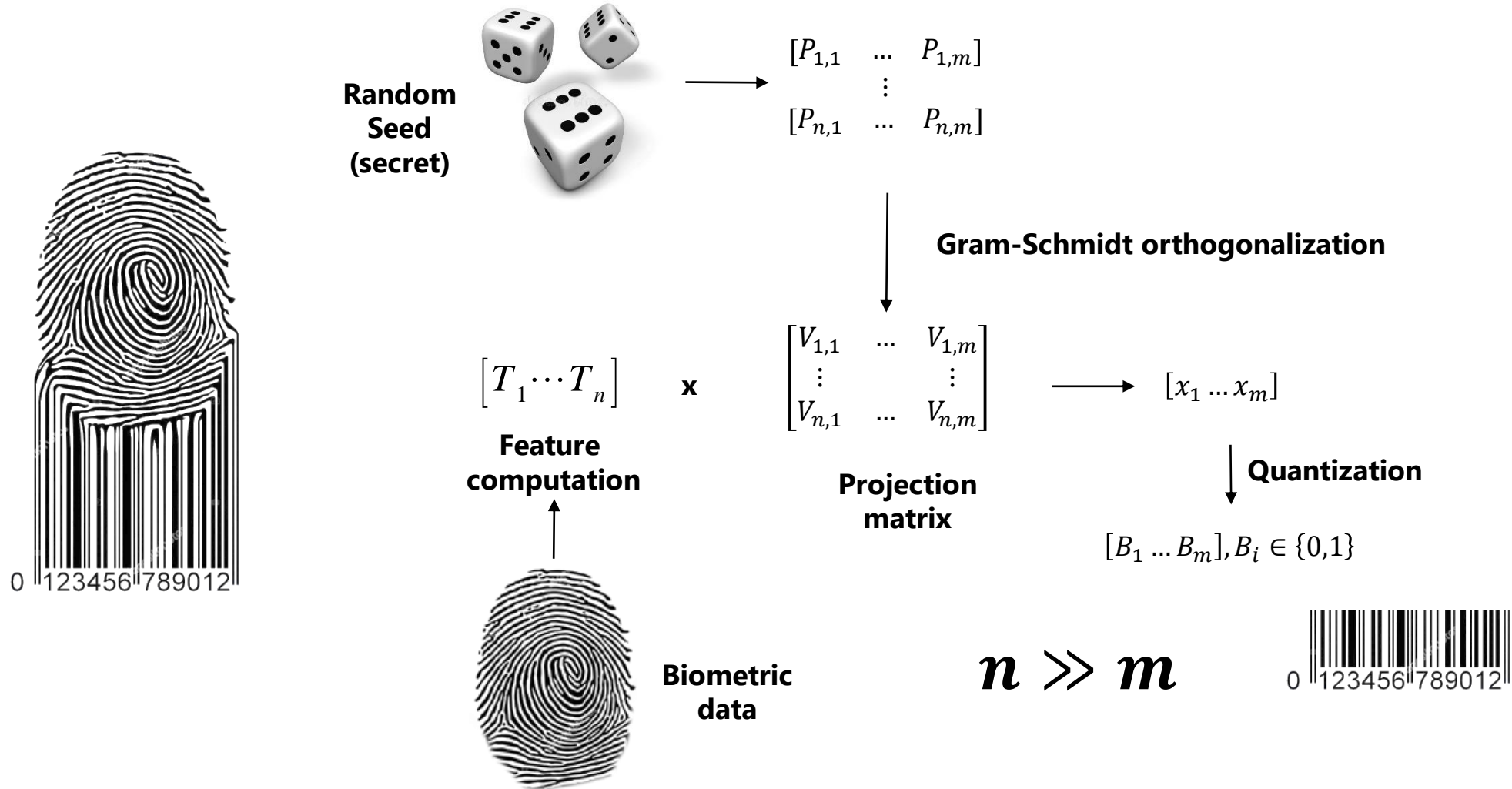
TRANSFORMATION BASED PROTECTION



Expected properties:

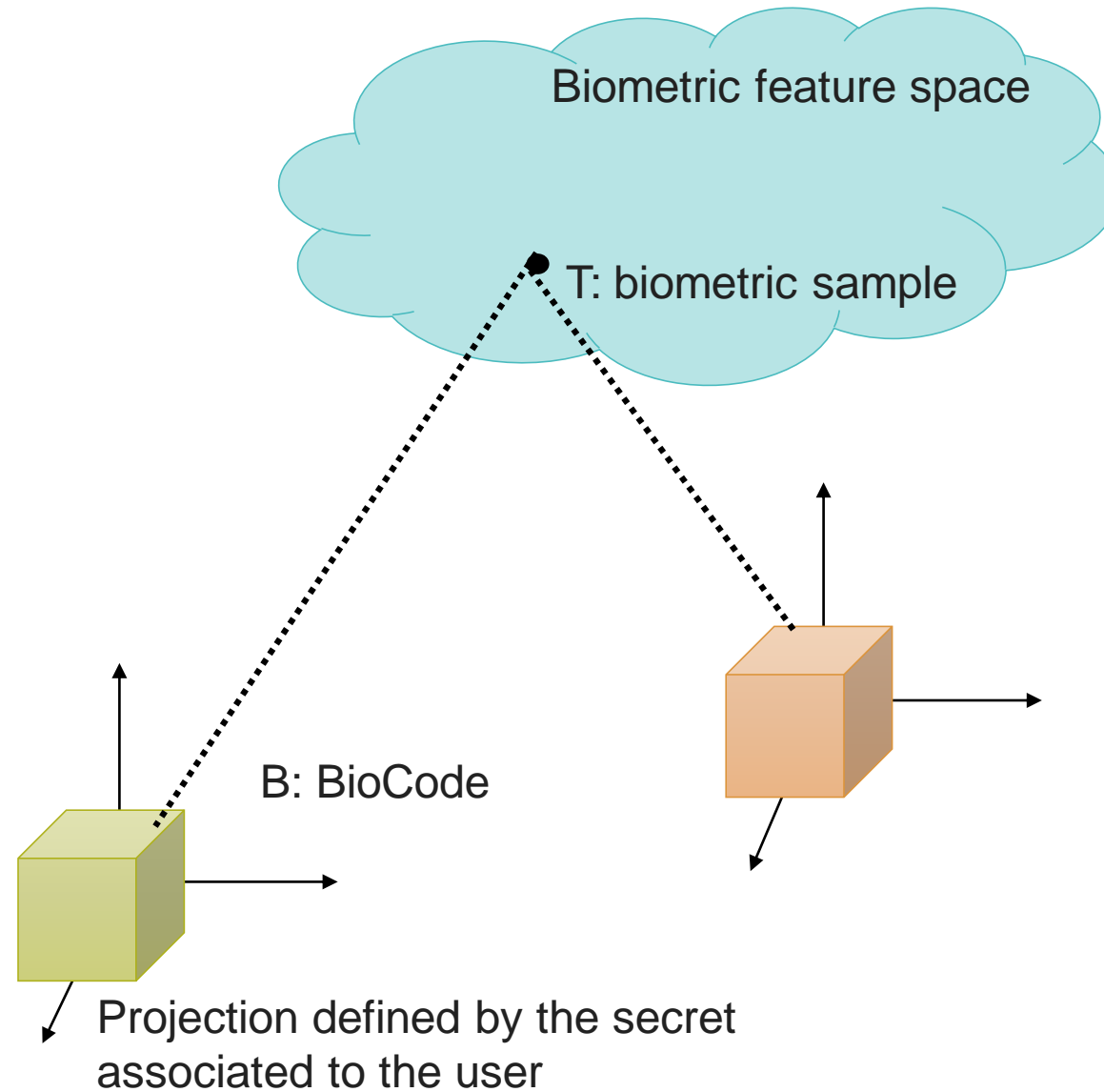
- **Verifiability:** it is possible to authenticate an user given a BioCode
- **Revocability:** it is possible to renew the BioCode in case of attack
- **Non invertibility or irreversability:** impossible to recover the raw biometric data given the BioCode and the Secret
- **Undistinguishability:** impossible to distinguish impostor BioCodes from legitimate ones with different Secrets
- **Unlikability:** no information leakage from different legitimate Biocodes

BIOHASHING



Jin, Andrew Teoh Beng, David Ngo Chek Ling, and Alwyn Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." *Pattern recognition* 37.11 (2004): 2245-2255.

BIOHASHING



IRREVERSIBILITY ATTACKS

$$FAR_A(\epsilon_T) = P(D_T(f(b_z, K_z), A_z) \leq \epsilon_T)$$

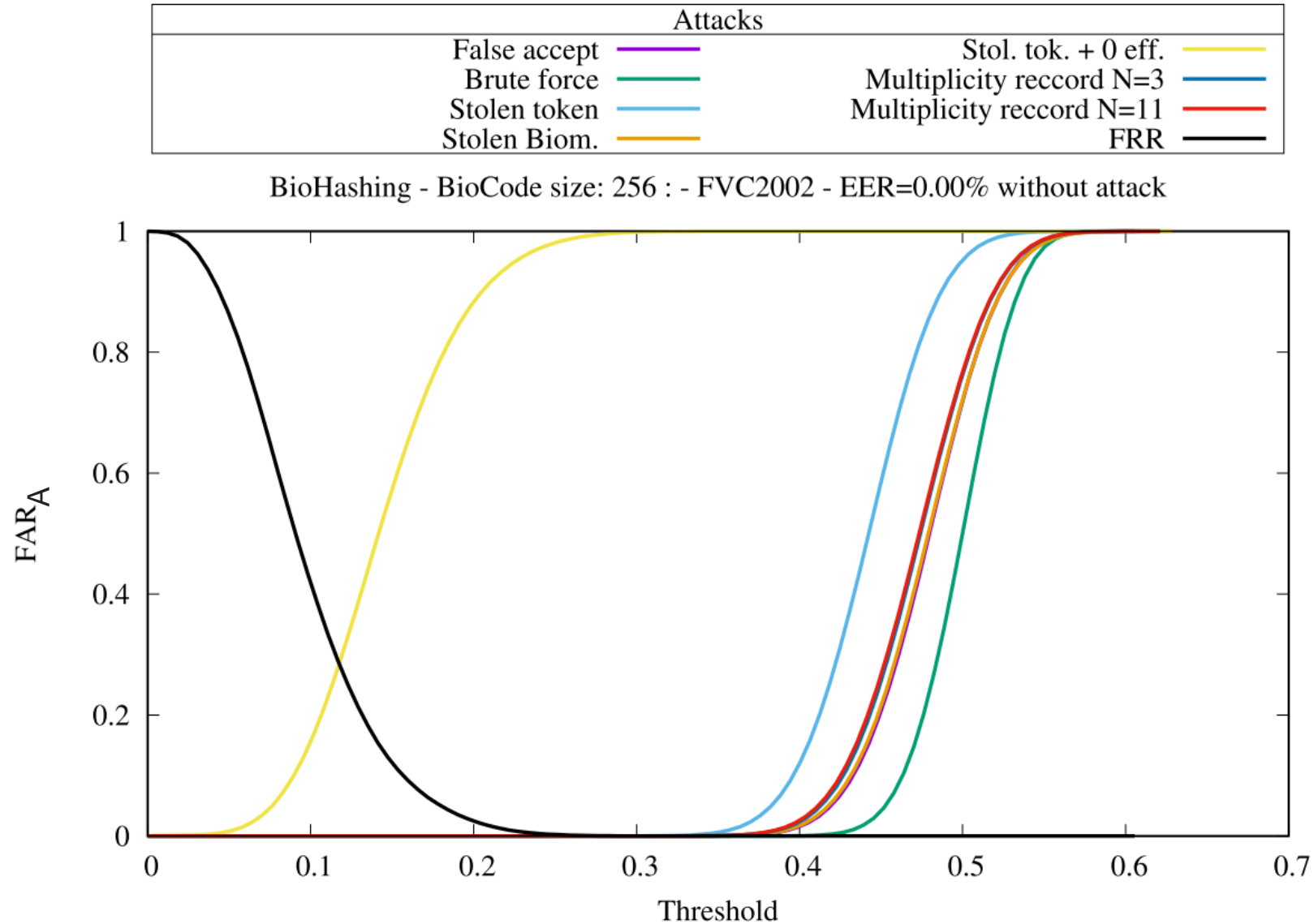
Where:

- $FAR_A(\epsilon_T)$: probability of a successful attack by the impostor for the threshold ϵ_T .
- A_z : generated biocode by the impostor with different methods,

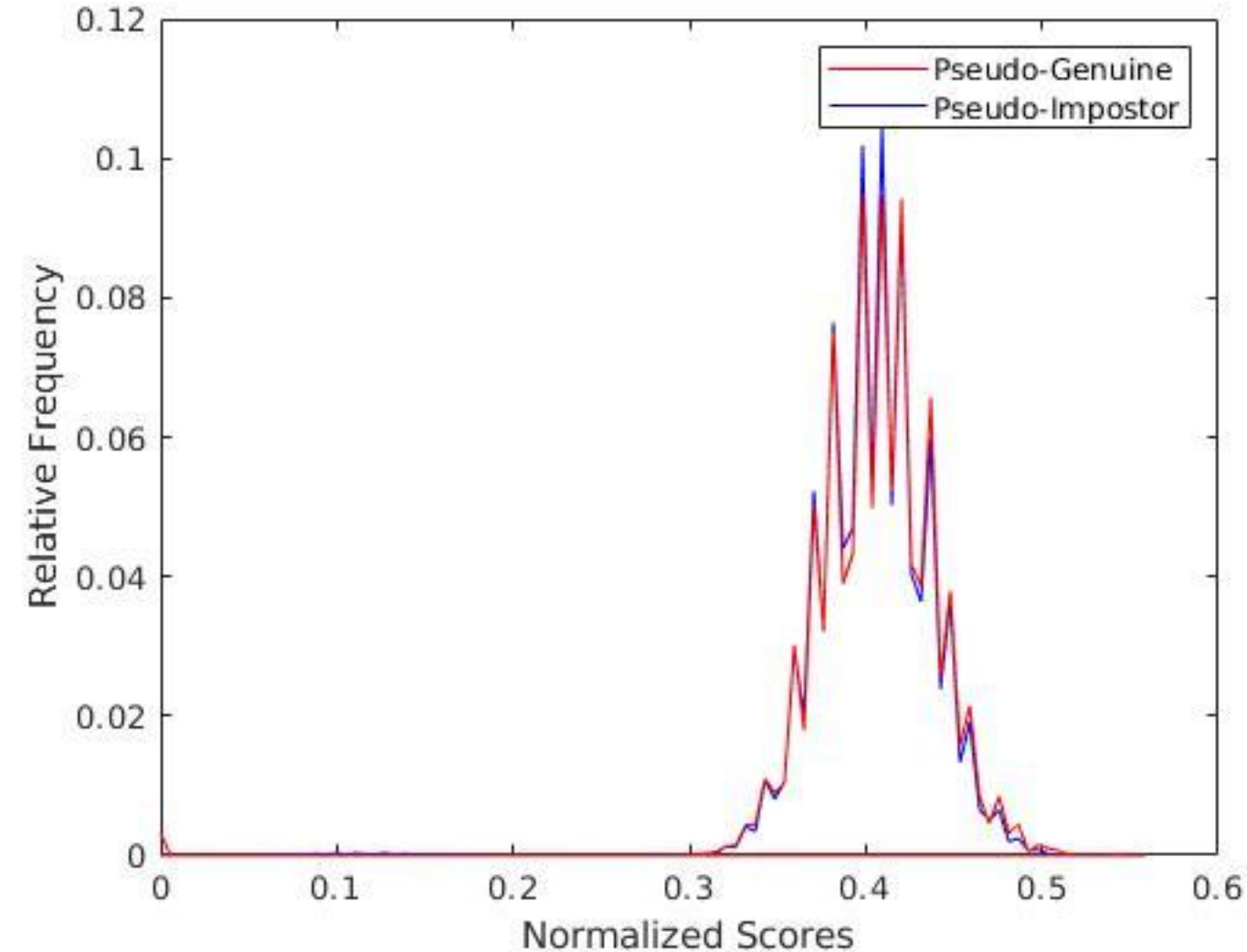
ATTACKS

- *Zero effort attack* |
An impostor provides one of its biometric sample to be authenticated as the user z : $A_z = f(b'_x, K_x)$,
- *Brute force attack*:
An impostor tries different random values of A : $A_z = A$,
- *Stolen token attack*:
An impostor has obtained the token K_z of the genuine user z and tries different random values of b to generate: $A_z = f(b, K_z)$,
- *Stolen biometric data attack*:
An impostor knows b'_z and tries different random numbers K to generate: $A_z = f(b'_z, K)$.
- *Worst case attack*:
An impostor user x provides its own biometric feature b'_x and has also obtained the token K_z of the genuine user z to generate: $A_z = f(b'_x, K_z)$

IRREVERSIBILITY ATTACKS



EVALUATION



Undistinguishability analysis:

Distribution of BioCodes

- Pseudo-impostor scores: matching scores between BioCodes generated from different biometric data of individual A with different keys.
- Pseudo-genuine scores: computed between BioCodes derived from different biometric data from impostors with the key of individual A.

DEMO



Greyc Biocode

Database

Users

Username
christophe

Username

Secret


Fingerprint Capture



Secret

Biocode

FDF5BED618513EFA3B9E64D7C9446E8C

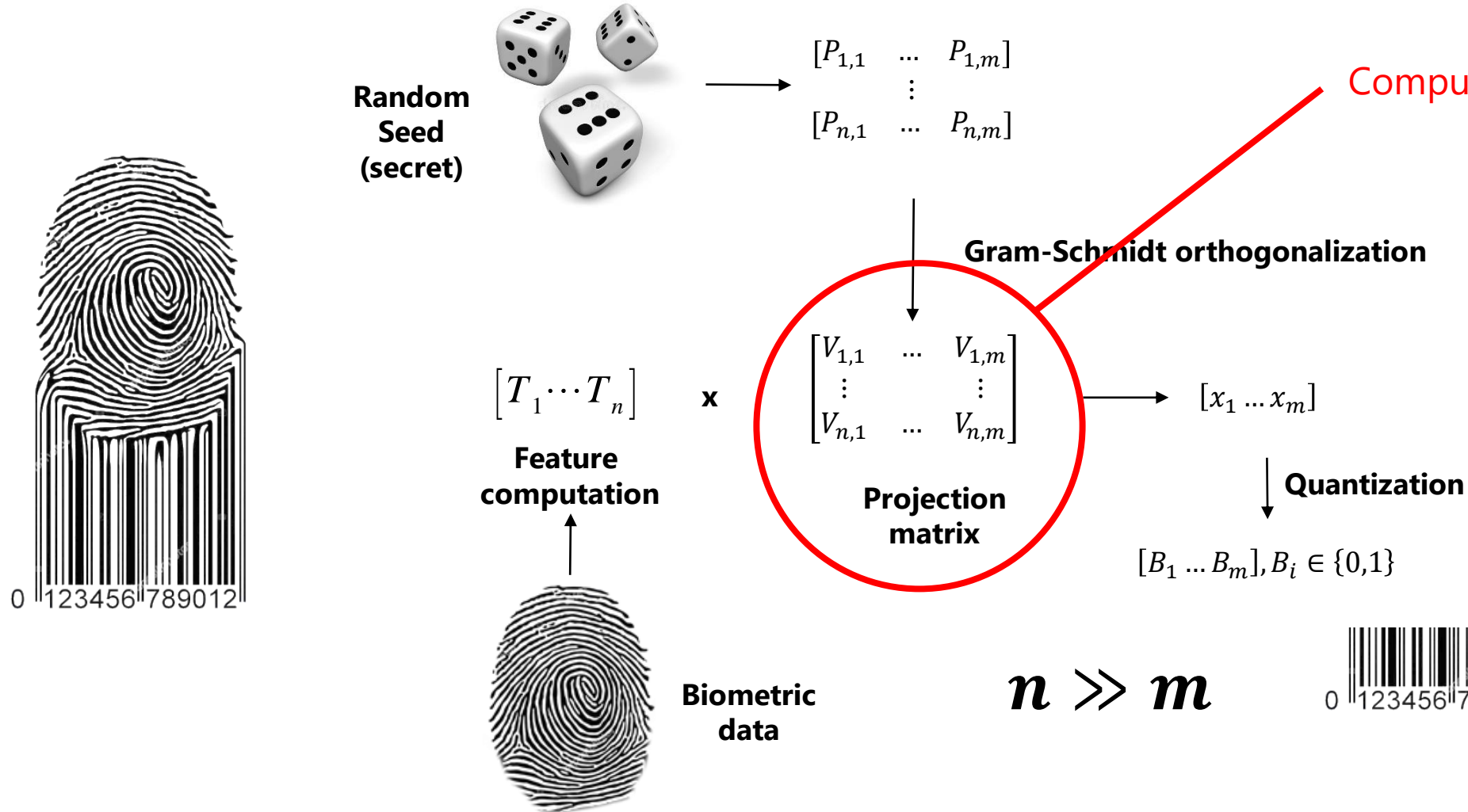


97,50 %

FDF59ED658513EFA3B9E64D7C9C46E8C

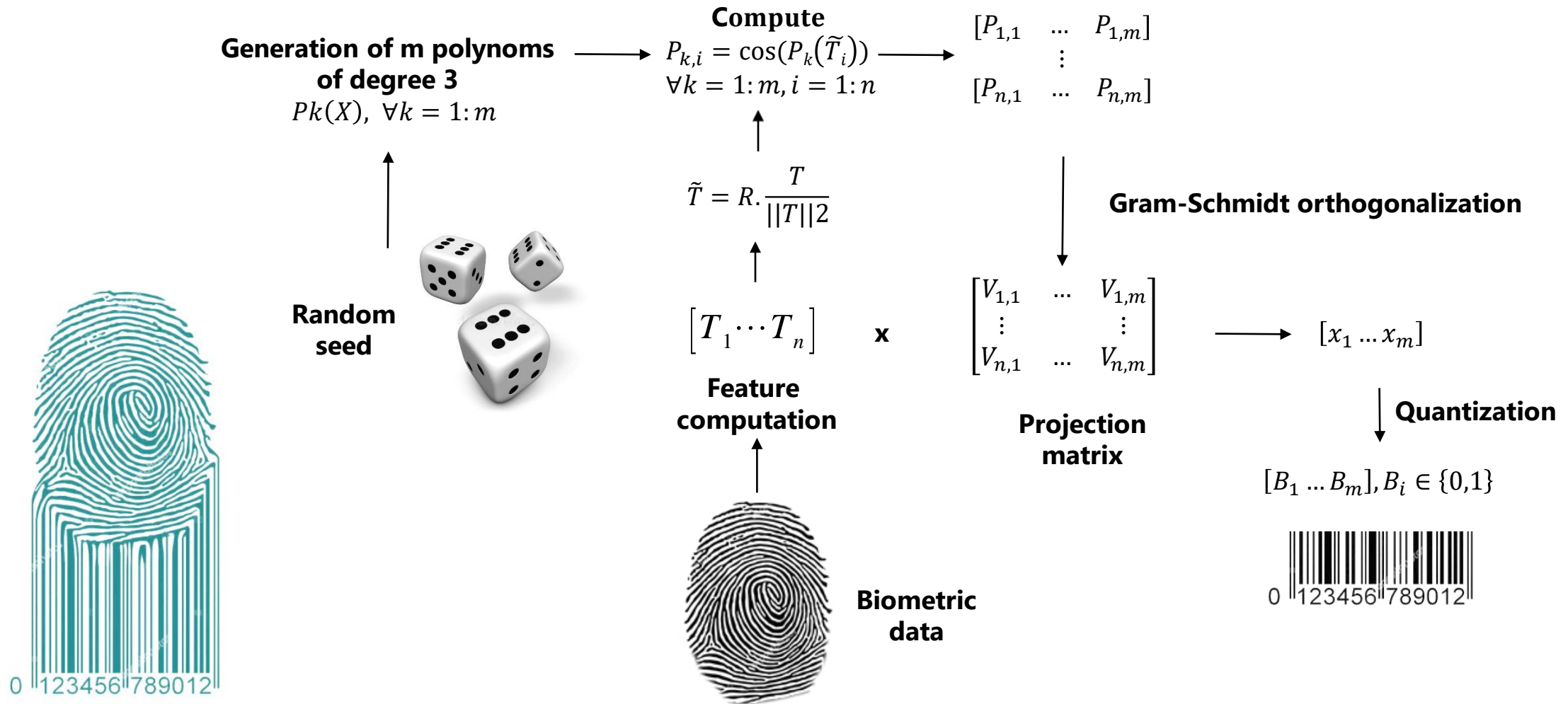
GREYC 

BIOHASHING



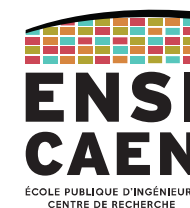
Jin, Andrew Teoh Beng, David Ngo Chek Ling, and Alwyn Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." *Pattern recognition* 37.11 (2004): 2245-2255.

GREYHASHING

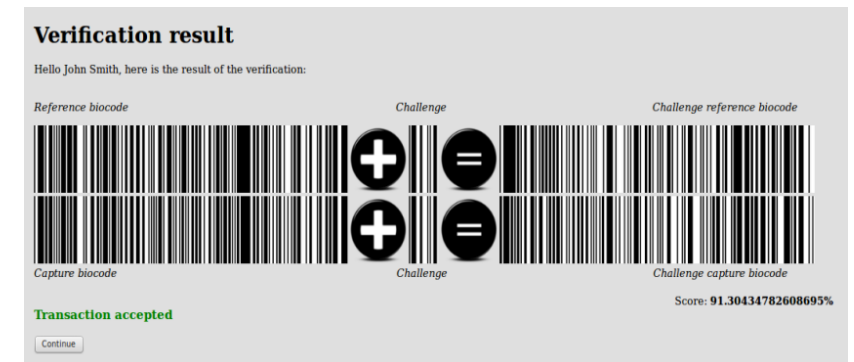
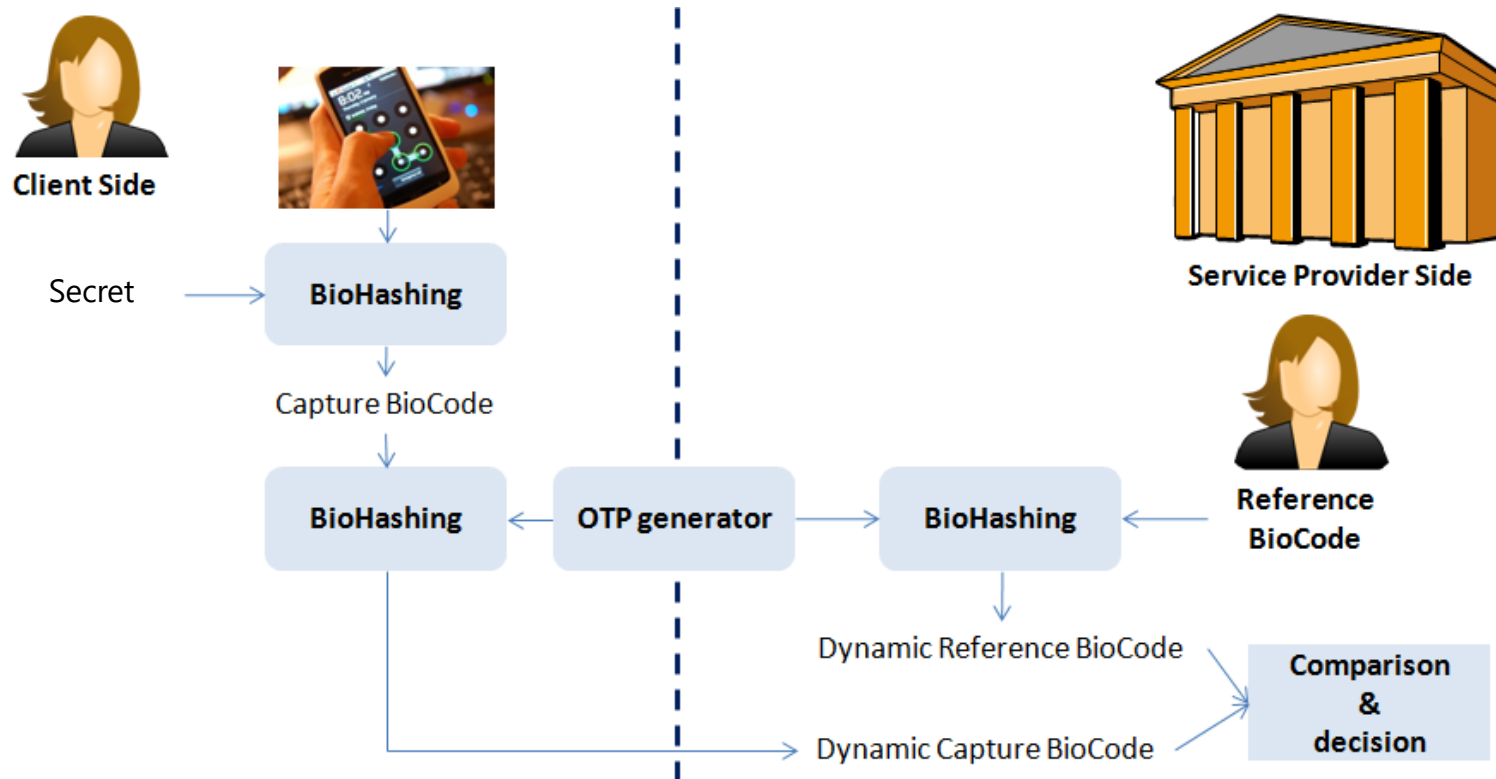




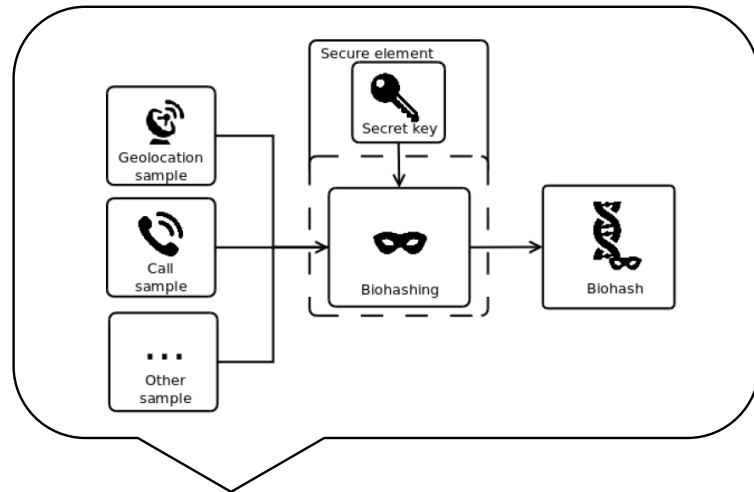
APPLICATIONS



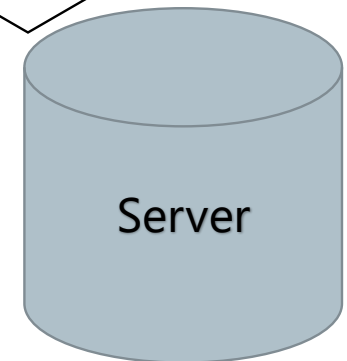
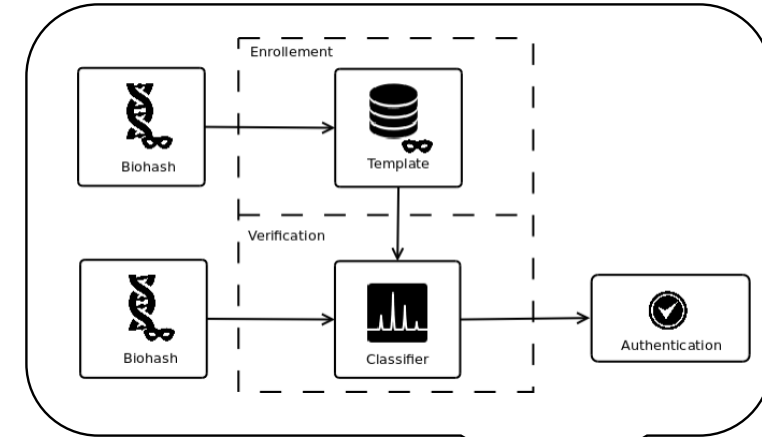
DYNAMIC AUTHENTICATION



TRANSPARENT AUTHENTICATION





Continuous transmission




Hatin, Julien, et al. "Privacy Preserving Transparent Mobile Authentication." *International Conference on Information Systems Security and Privacy (ICISSP)*. 2017.

PERSONAL CODE




xCRP Démonstration Titi  



1. Compute your *Personal Identity Code Respecting Privacy*

Type an Identifier 


Titi


Type some text 

Ce texte doit être suffisamment long pour montrer que cela fonctionne correctement.



 

2. See your *Personal Identity Code Respecting Privacy*



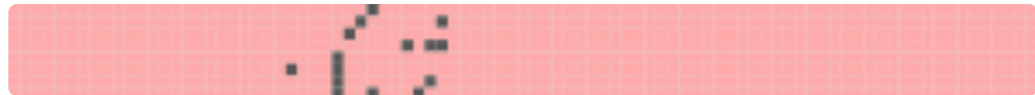
Copy PICRP to clipboard: 



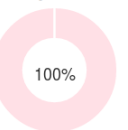
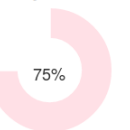
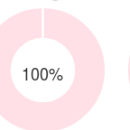
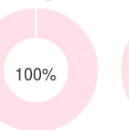
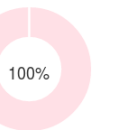
3. Enter another *Personal Identity Code Respecting Privacy*

'KaBPraZz/b6vLls3pDpryTLJ1Eh031zJJrrKAPn+XTawM3ldxE2iDOAtJ4RthYmznFS0VWL4P8='  

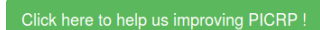
4. Compare your *Personal Identity Code Respecting Privacy*

Differences (in black)






Score	browser	keystrk.1	keystrk.2	config.1	config.2	ip
 96%	 100%	 100%	 75%	 100%	 100%	 100%

5. Help us improving the *Personal Identity Code Respecting Privacy*



This work as been presented at the CORESA2017 and ICISSP2018 conferences, and is part of Denis Migdal's PhD thesis, co-founded by the Normandy region and the GREYC laboratory. As computations are performed locally, no information are sent to our servers. A random key is generated, and stored, on your browser, however, this key is not sent to our servers, and cannot be accessed by other websites.

Developped by  Founded by  

Migdal, Denis, Christophe Rosenberger. "Towards a Personal Identity Code Respecting Privacy." *International Conference on Information Systems Security and Privacy (ICISSP)*. 2018.

THANKS

Christophe ROSENBERGER

christophe.rosenberger@ensicaen.fr



Laboratoire GREYC – UMR CNRS 6072

