



Independent Performance Evaluation of Biometric Systems:

Minutiae Performance versus Pseudonymous Identifier Performance

Davrondzhon Gafurov (speaker), Bian Yang, Patrick Bours
and Christoph Busch

Gjøvik University College, NORWAY

davrondzhon.gafurov@hig.no

bian.yang@hig.no

patrick.bours@hig.no

christoph.busch@hig.no



FP7 Integrated Project TURBINE (TrUsted Revocable Biometric IdeNtitiEs)





Overview

- Biometric performance evaluation
- TURBINE project
- Performance metrics, data set and results
- Summary



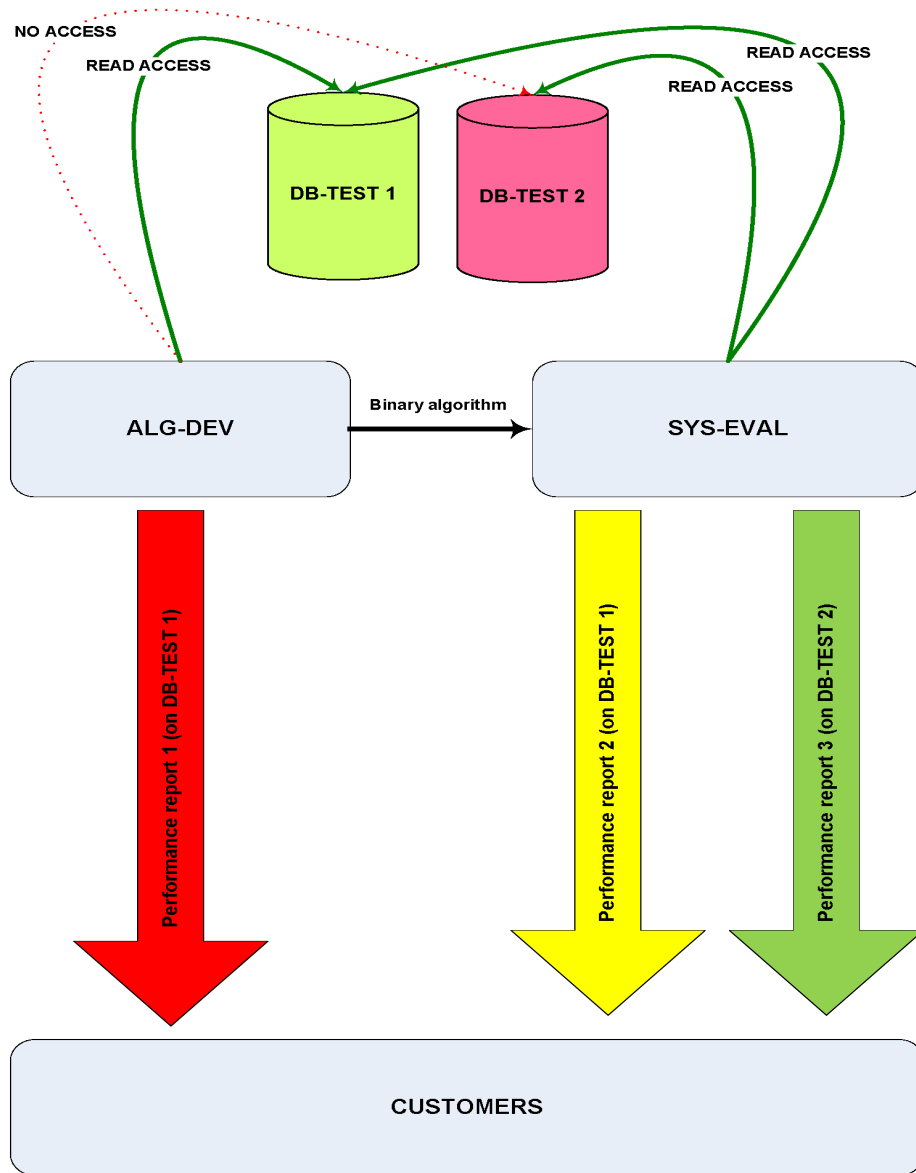
Biometric Performance Evaluation



- Test database
- Algorithm developer
- Performance evaluator
- Test report(s)



Biometric Performance Test Reports



- ❖ **Least trustable** - Report 1 (on DB 1)
- ❖ **Medium trustable** - Report 2 (on DB 1)
- ❖ **Most trustable** - Report 3 (on DB 2)



TURBINE

- TURBINE – TrUsted Revocable Biometric IdeNtitiEs
- EU FP7 project, <http://www.turbine-project.eu>
- Two rounds of performance evaluation
- In this paper/presentation
 - **This is 1st round results (not final!)**
 - Performance report "Category 3"
 - Only "biometric performance/analysis" per se
 - Not "security performance/analysis"



Main Objectives and Principles

- Solutions: software-based, hardware-based, or both
- In general, it requires:

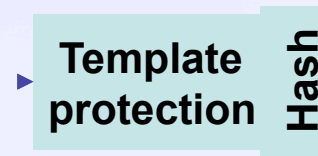
Fingerprint biometric characteristic



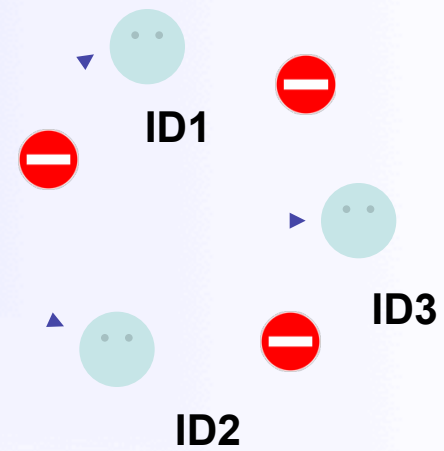
Multivendor interoperability



Generation of protected pseudo identifier



Multiple + revocable pseudo identifier based on same fingerprint



Identities are not invertible



Impact

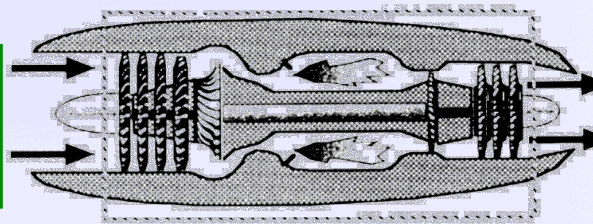


Name : SMITH
Date of birth: ...

Identity managed by issuance State,
including biometrics, certificates &
data protection mechanism



Mr SMITH +



ID1 + 101 011 101 011 110 0011 01
ID2 + 101 101 110 101 110 1010 10
ID3 + 110 011 011 101 101 0110 10



► TURBINE

IMPACT on "ID" verification

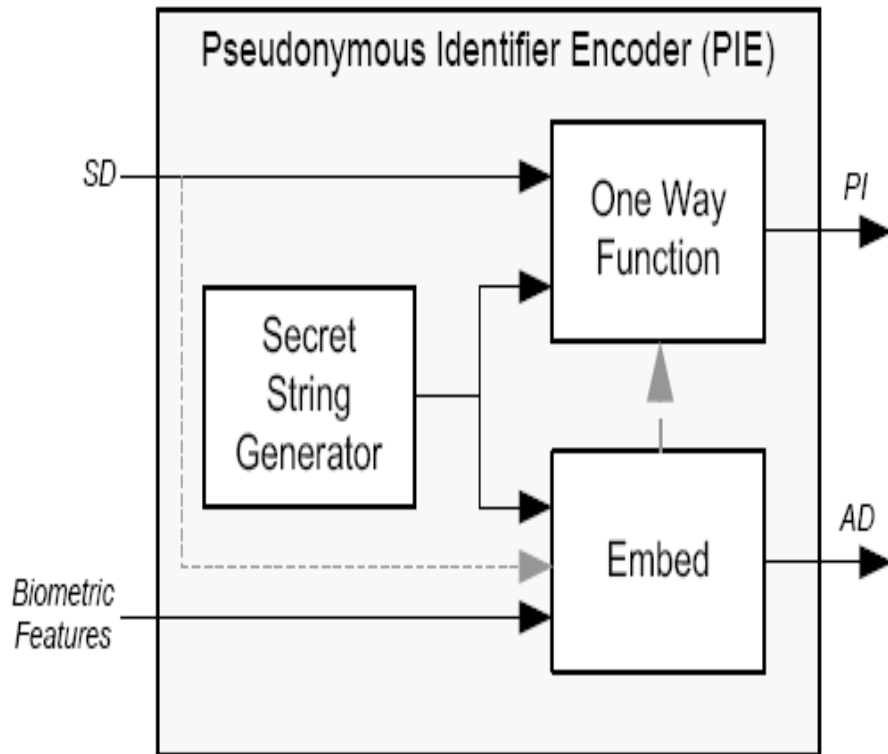
- Different identities (pseudo, voter, tax payer, ...) derivate from a trusted identity
 - Trust the token holder true his fingerprint
- Fingerprint is transformed & substituted instead of encrypted → privacy impact
- Revocation without impact on the original



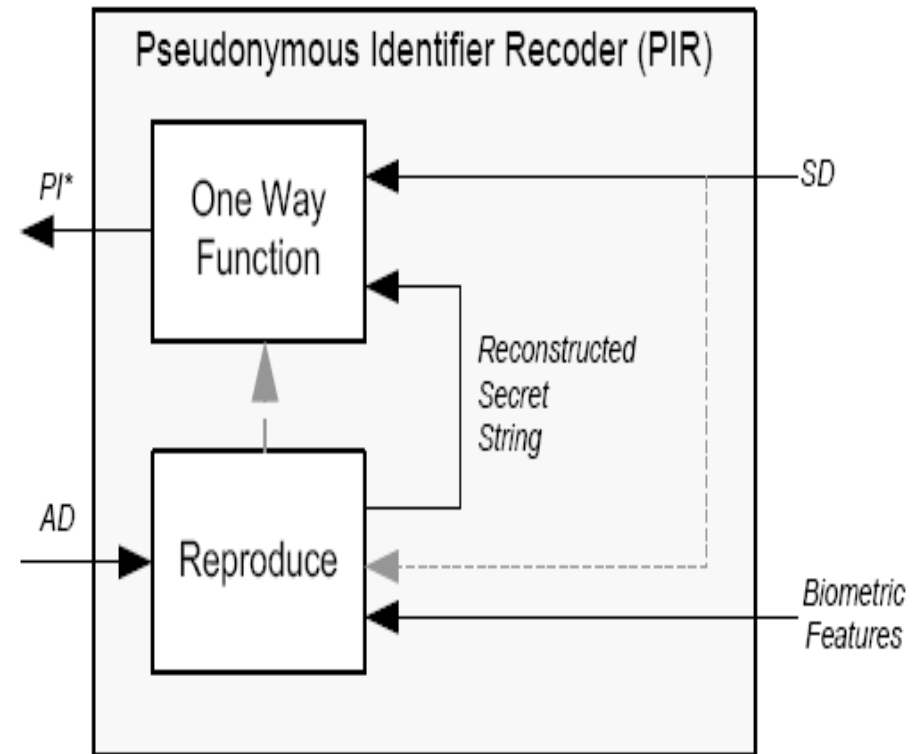
Pseudo Identifier Encoder in ISO 24745 (2nd CD)



Enrolment



Verification





TURBINE

- Algorithm developers
 - [Sagem Sécurité](#) (France)
 - [Precise Biometrics AB](#) (Sweden)
 - [Philips Research Europe](#) (The Netherlands)
 - [University of Twente](#) (The Netherlands)
- Biometric performance evaluator
 - [Gjøvik University College](#) (Norway)
- Security performance evaluator
 - [K.U.Leuven \(ICRI, COSIC\)](#) (Belgium)



Test database

- GUC100
 - 6 scanners,
 - 100 subjects, all 10 fingers
 - ~ 72000 images





Test database (II)

- Temperature variation (Norway 2008/09)
- 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



Performance metrics

- Algorithm performance
 - FMR vs. FNMR
- System performance
 - FAR vs. FRR
- Formulas
 - FAR = FMR*(1-FTA)
 - FRR = FNMR*(1-FTA) + FTA
 - **FTA = FTC + FTX*(1-FTC)**

$$FTX = \frac{\text{\#-of - not encoded - images}}{\text{total \# of - images submitted - to - encoder}}$$



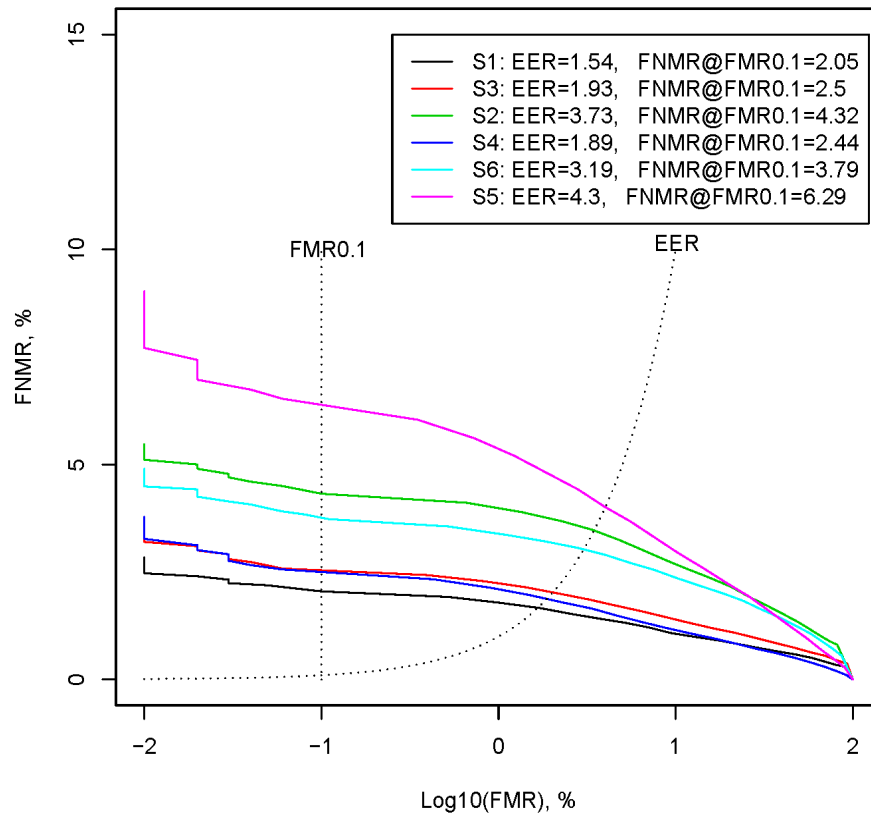
Performance metrics (II)

- Minutiae level (classical)
 - Without considering image quality
 - With image quality (NFIQ > 3 count in FTC)
- Pseudonymous Identifier (PI) level
 - Large throughput
 - Less points in DET curves
- DET curves
 - Scanner and software suppliers are anonymous

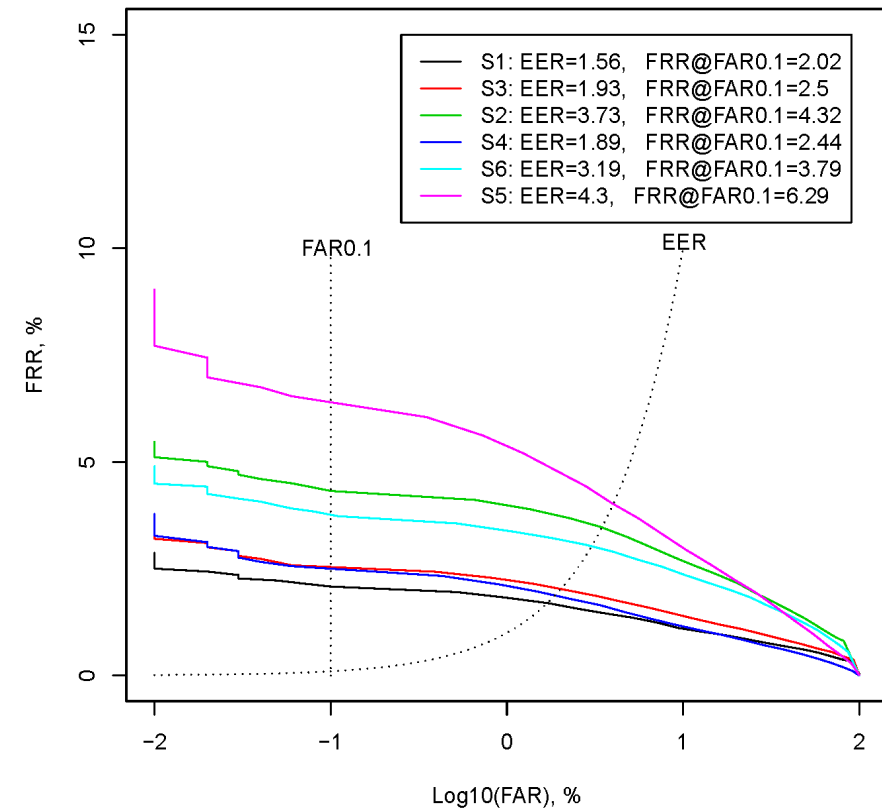


Minutiae level: Neurotechnology without considering image quality

Algorithm performance



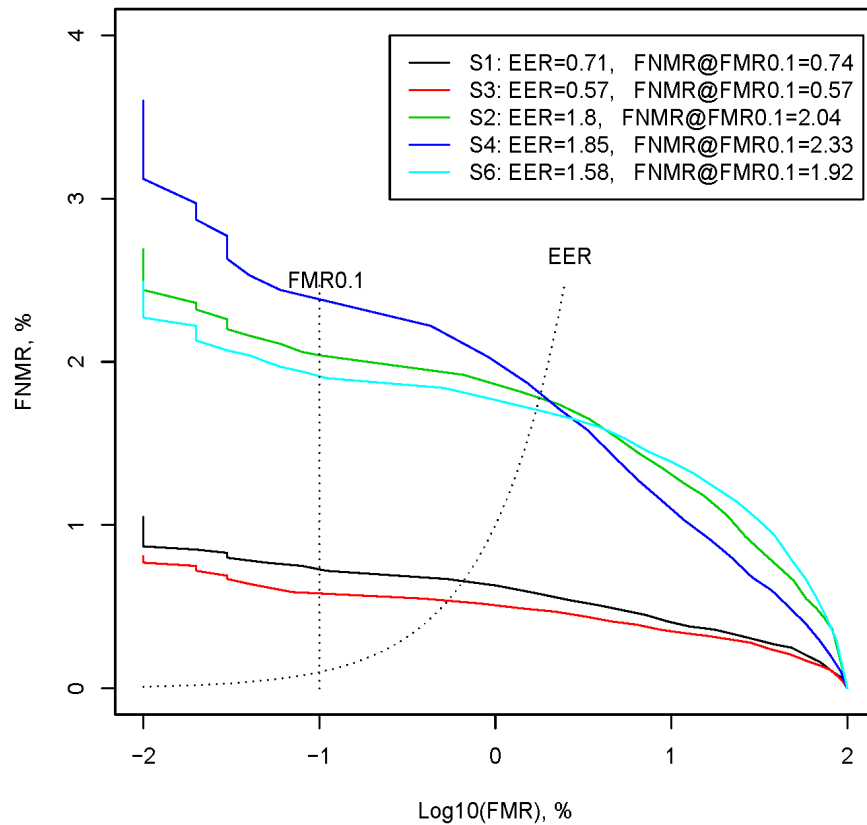
System performance



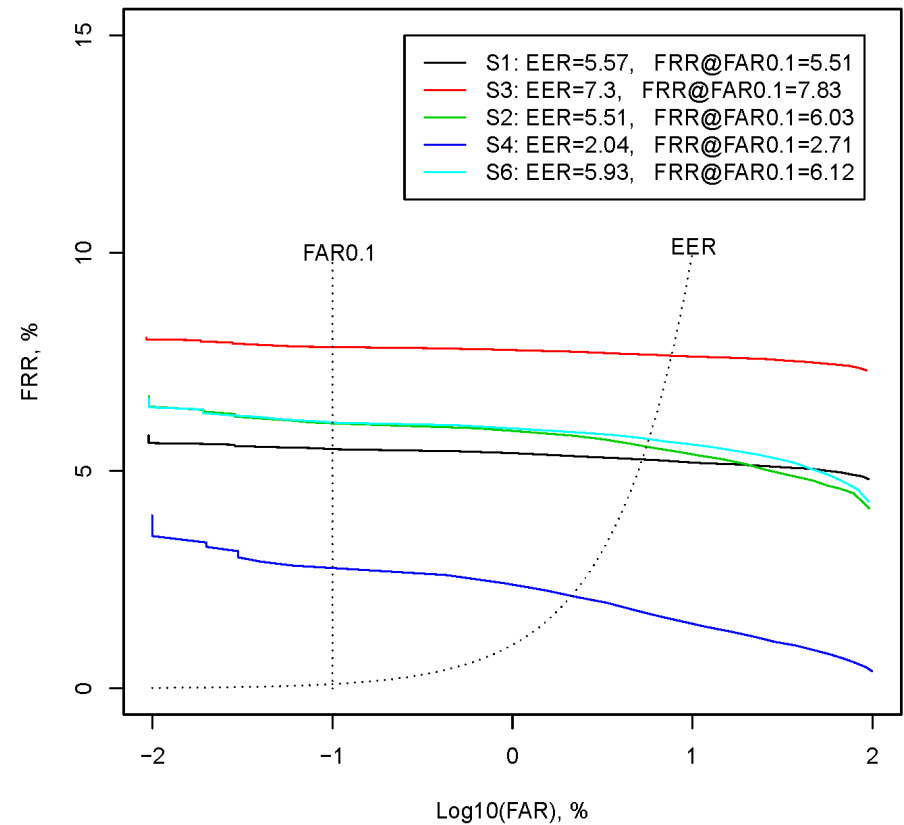


Minutiae level: Neurotechnology with considering image quality

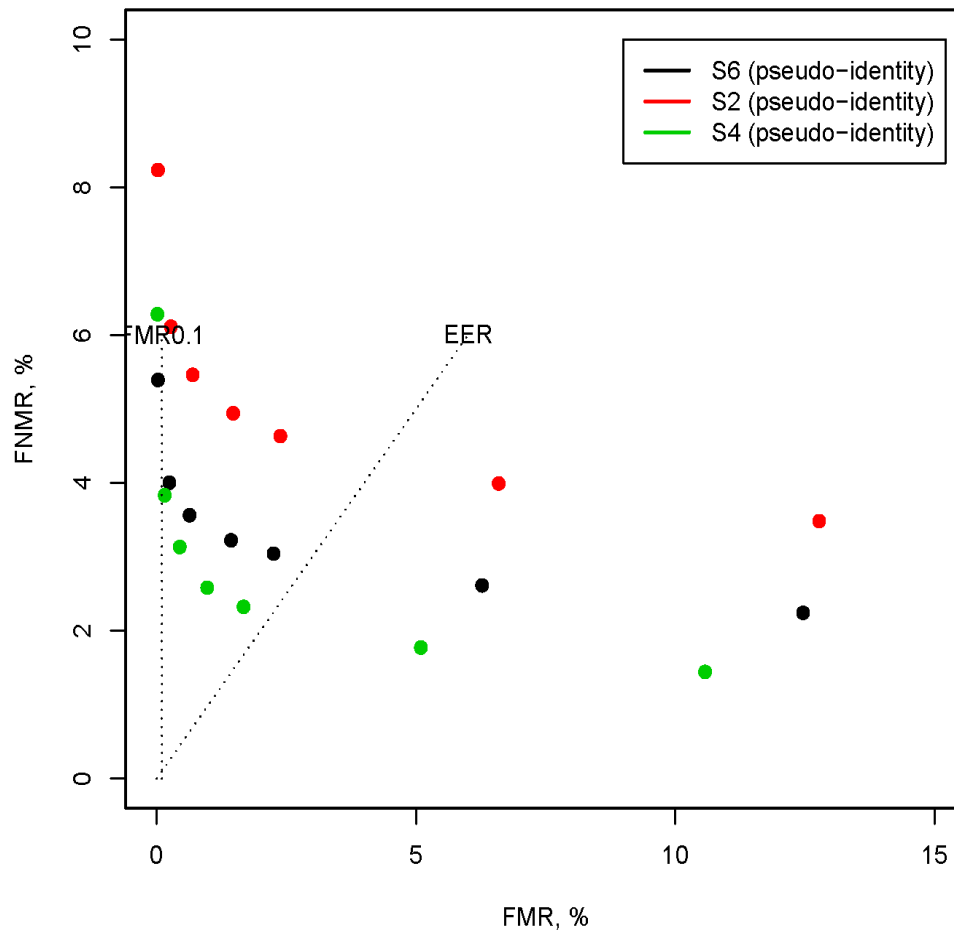
Algorithm performance



System performance

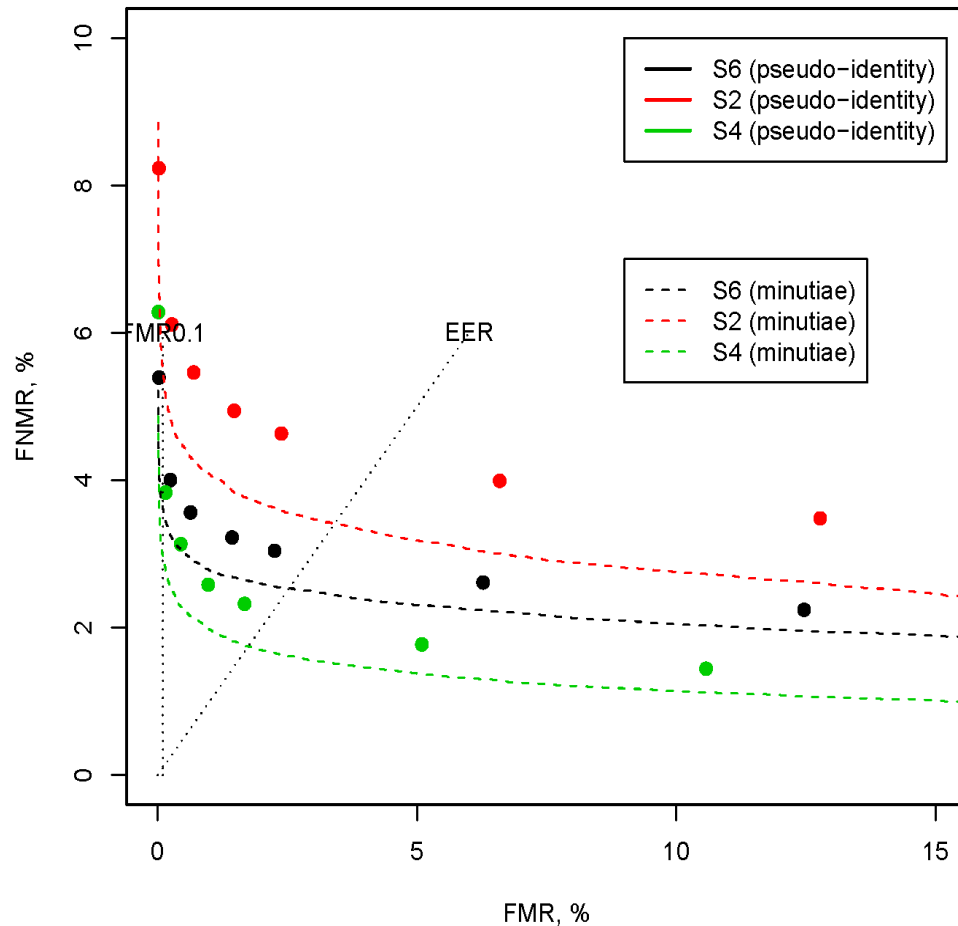


PI level: Supplier A



- One example of a PI algorithm.
- Only a biometric performance (no assessment on the security).
- Disclaimer: other algorithms have also been tested in the benchmark, and the security analysis is still ongoing (results subject to the research by Koen Simoens)

PI vs. Minutiae level: Supplier A



- One example of a PI algorithm.
- Only a biometric performance (no assessment on the security).
- Disclaimer: other algorithms have also been tested in the benchmark, and the security analysis is still ongoing (results subject to the research by Koen Simoens)



Summary and future work

- Desirably "Developers" and "Evaluators" to be independent entities
- PI level verification aims to provide more gain with respect to privacy, although there might be some degradation of performance
- Security analysis must also be taken into account
- 2nd round of tests in TURBINE in second half of year 2010, and the results in year 2011





Acknowledgment

This work is supported by funding under the Seventh Research Framework Programme of the European Union, Project TURBINE (ICT-2007-216339). This document has been created in the context of the TURBINE project. All information is provided *as is* and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The European Commission has no liability in respect of this document, which is merely representing the authors' view.

