TELECOM ParisTech

Institut Mines-Télécom

ANR

SECURE IC THE TRUSTED COMPUTING COMPANY

SAFRAN Morpho

Studying Leakages on an Embedded Biometric System Using Side Channel Analysis

M. Berthier, Y. Bocktaels, J. Bringer, H. Chabanne, T. Chouta, J-L. Danger, M. Favre, T. Graba

Outline

1- Technical background:

- Fingerprint standard representation.
- Generic biometric system & vulnerabilities.

Outline

1- Technical background:

- Fingerprint standard representation.
- Generic biometric system & vulnerabilities.

2- First Side Channel Analysis:

- Description of the targeted computation.
- SCA approach & results.

3- Second Side Channel Analysis:

- Description of the targeted computation.
- SCA approach & results.

Outline

1- Technical background:
- Fingerprint standard representation.
- Generic biometric system & vulnerabilities.

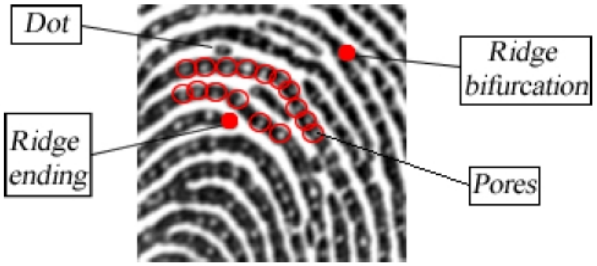
2- First Side Channel Analysis:
- Description of the targeted computation.
- SCA approach & results.

3- Second Side Channel Analysis:
- Description of the targeted computation.
- SCA approach & results.

4- Countermeasures.

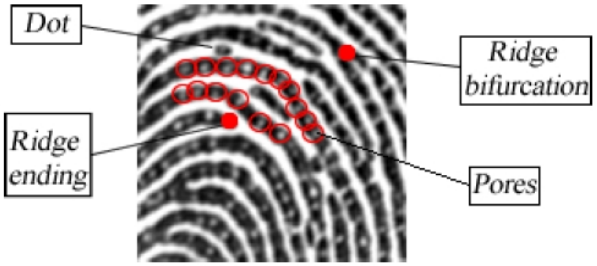
The INCITS 378 and the ISO 19794-2 standards

A fingerprint contains different types of ridge patterns and other kind of minutiae.



The INCITS 378 and the ISO 19794-2 standards

A fingerprint contains different types of ridge patterns and other kind of minutiae.



Compact version of the standard:

•Two types of minutiae are considered :

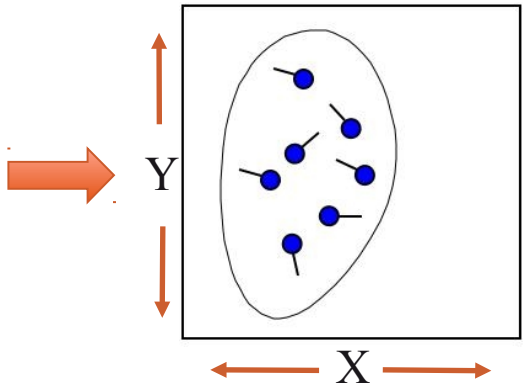
- *Ridge ending*
- *Ridge bifurcation*.

• Fingerprint can be considered as a set of points (x, y, θ, t)

• In this study type is not used

$$S = \{(x_0, y_0, \theta_0), \ldots, (x_n, y_n, \theta_n)\}$$

Fingerprint image

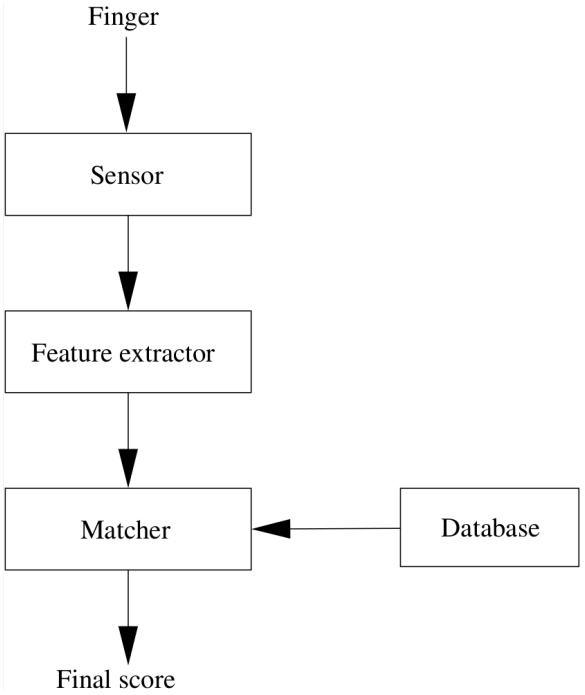


Standard representation

Generic Biometric System

– Four main modules:

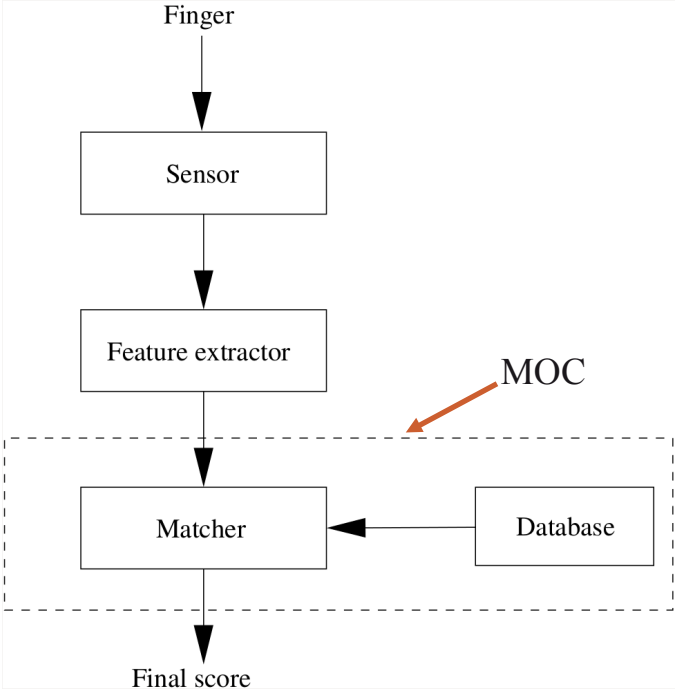
- The S**ensor** for finger image acquisition.
- The **Feature extractor** producing the minutiae set.
- The **Matcher** computing the similarity level.
- The **Database** storing the reference set(s).



Biometric authentication system with four main modules

MOC System

The Match On Card embeds the matcher and the reference set within embedded system.



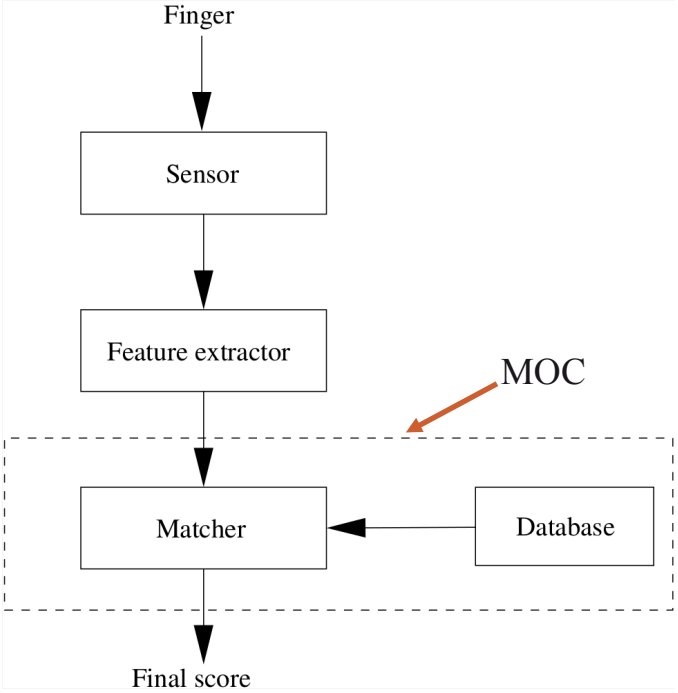
The Biometric Match-On-Smart-Card

MOC System

The Match On Card embeds the matcher and the reference set within embedded system.

Advantage:
Takes advantage from the tamper resistance of the Smart-card.

Challenges:
Limitation of available resources:
- Constrained memory footprint.
- Low speed CPU.



The Biometric Match-On-Smart-Card

Vulnerability Points of Biometric Systems

(1) Using false finger.

(2) Biasing the sensor.

(3) Forcing the extractor.

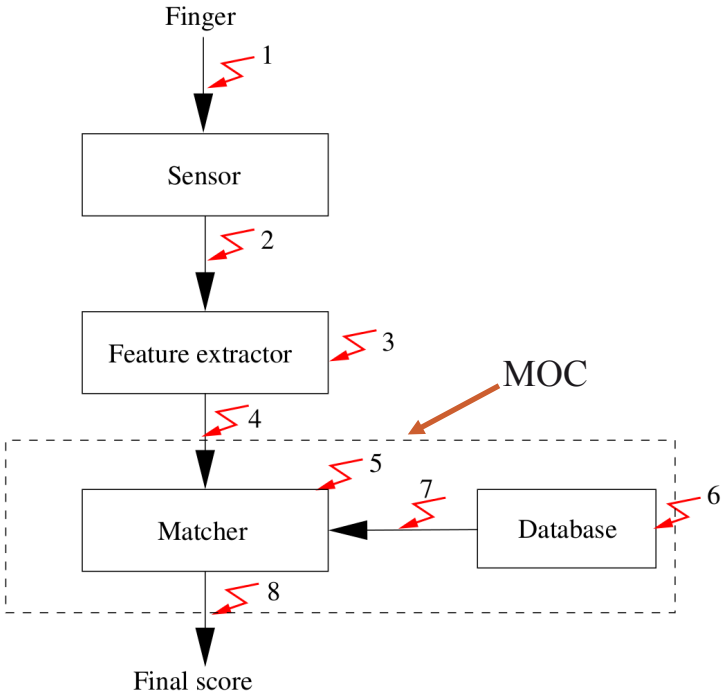
(4) **Intercepting and modifying the input vector.**

(5) Spying or forcing the comparator computation.

(6) Tampering with the reference set.

(7) Intercepting the reference set.

(8) Overriding the final decision.

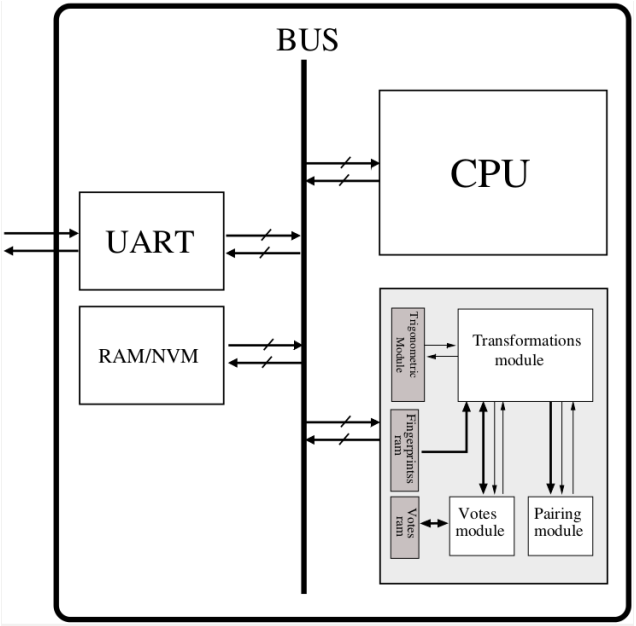


Vulnerabilities of generic biometric systems

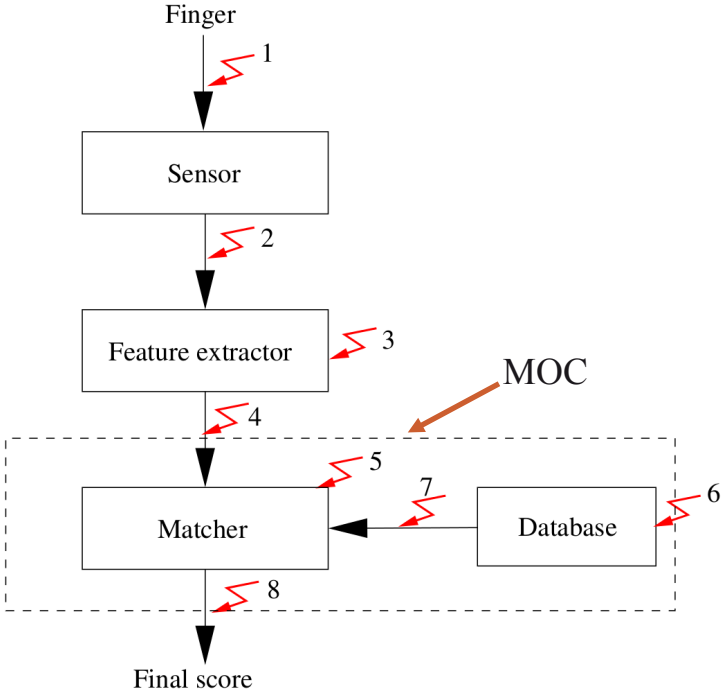
Vulnerabilities of MOC System

The Analysis is done on an FPGA prototype:

- System On Chip
- Independent biometric co-processor.



MOC prototype

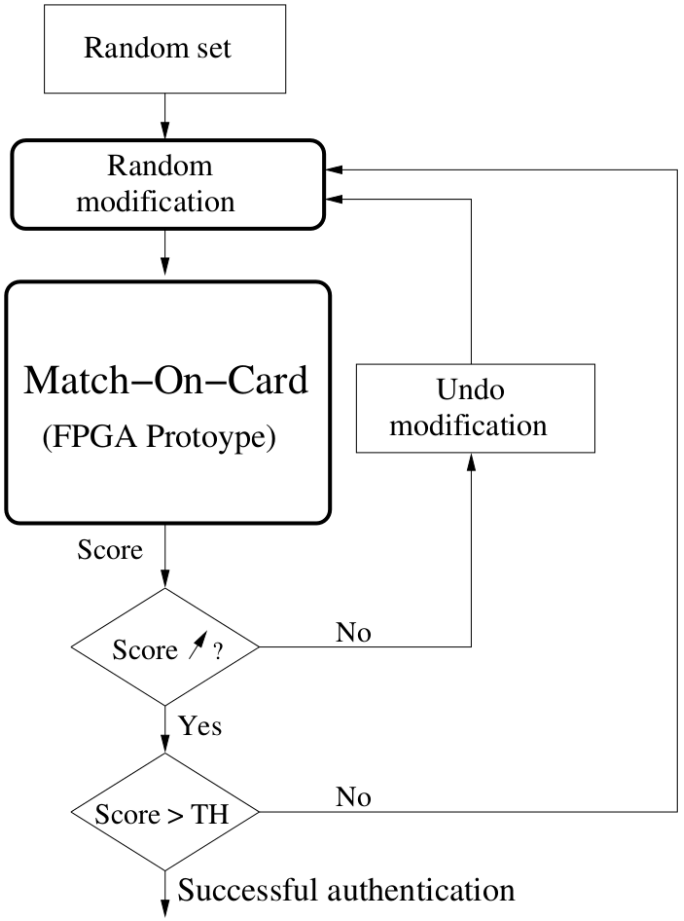


Vulnerabilities of generic biometric systems

The Hill Climbing Heuristic

The HC aims at optimizing the similarity score iteratively by applying random modifications.

If (score > Threshold)
→ Successful authentication.

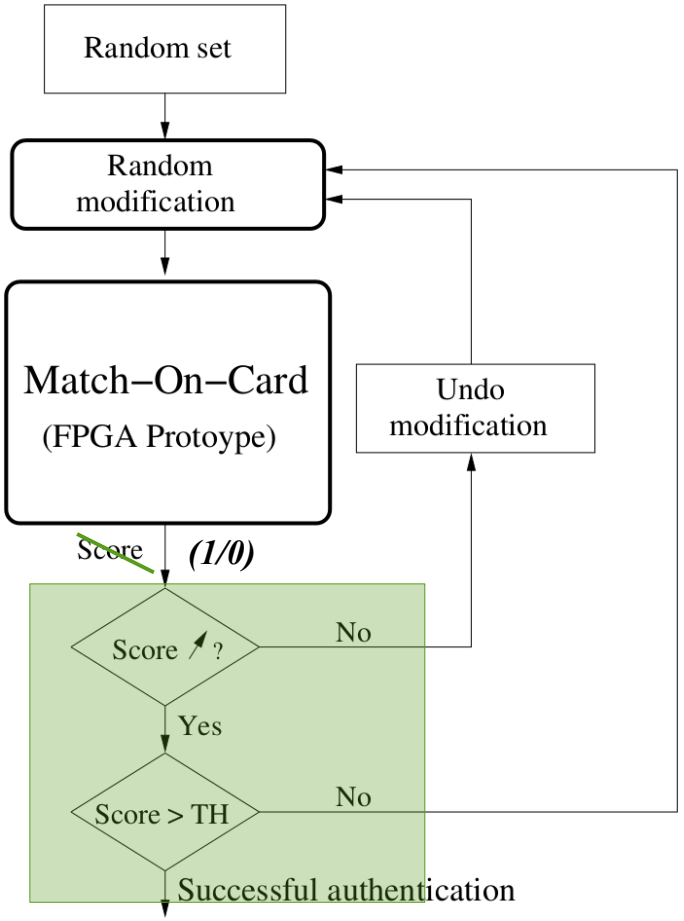


The Hill Climbing Heuristic

Basic countermeasure: output a binary decision only (accepted/rejected).

→ *The feedback is of **low** entropy.*

If (score > Threshold)
→ Successful authentication.

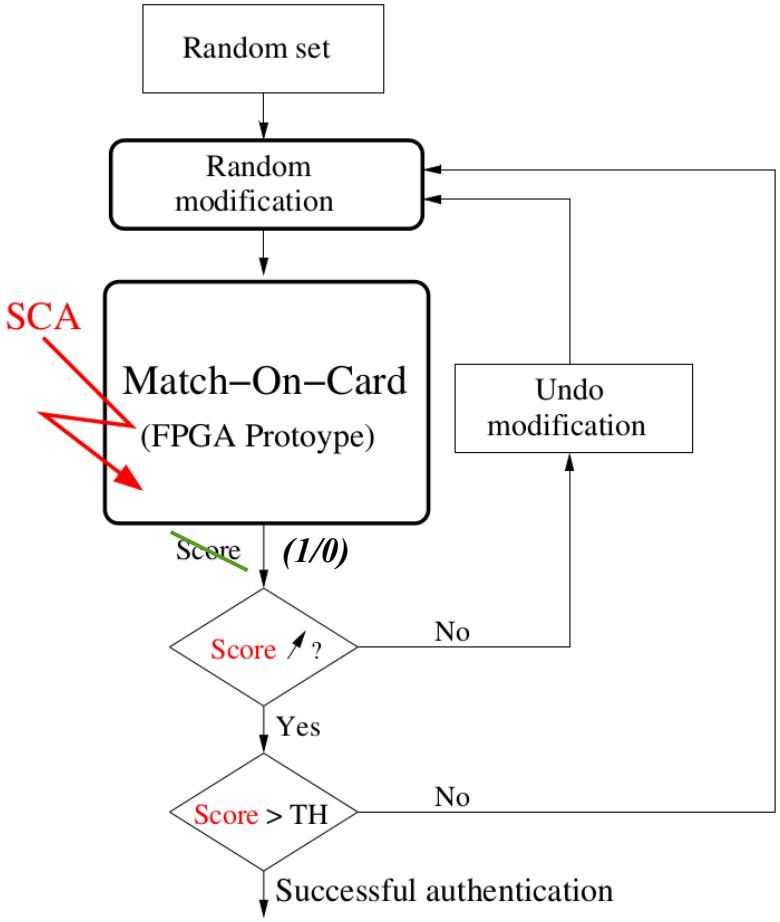


SCA on the similarity Score

By means of SCA, access to information about internal score.

→ *The feedback is of **high** entropy.*

If (score > Threshold)
→ Successful authentication



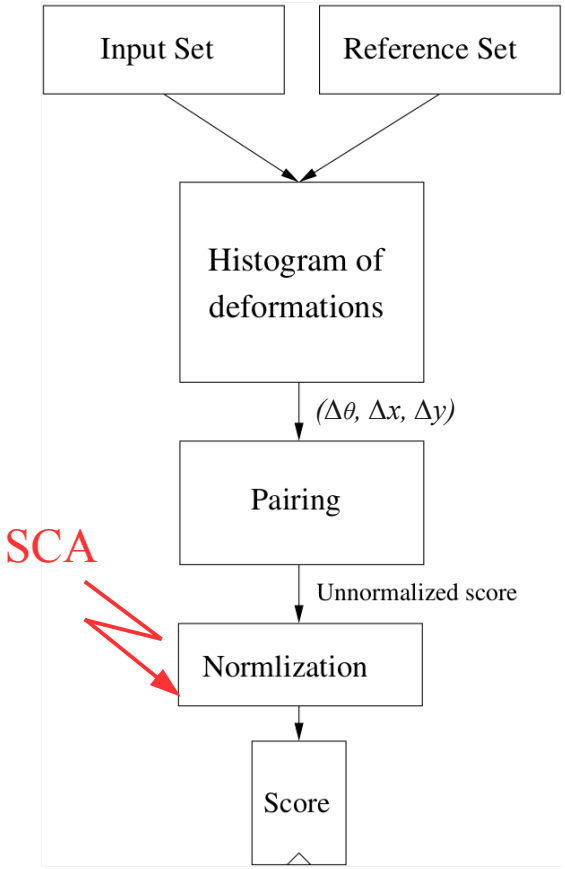
The Matching Algorithm

Can be seen as a three-step algorithm:

(1) Registration: Alignment.

(2) Pairing (1 to 1 comparison).

(3) Score normalization.



The algorithm flowchart

The Score Normalization

- The score normalization is ***common*** to many biometric algorithms.
- It considers the size of the compared fingerprints.
- In our case:

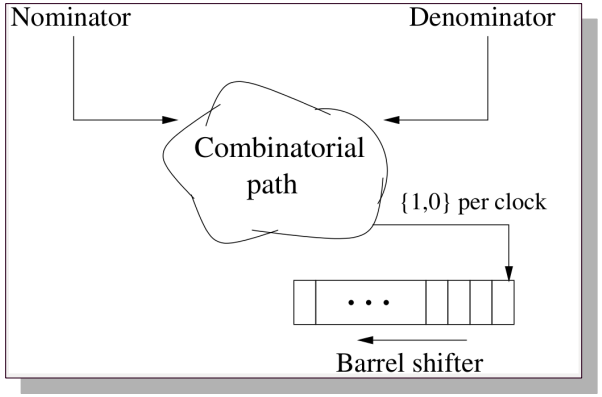
$$Score = \frac{\sum_{i=0}^{size_{in}} pair[i]}{\mathrm{Max}(size_{in}, size_{ref})}$$

The Score Normalization

- The score normalization is ***common*** to many biometric algorithms.
- It considers the size of the compared fingerprints.
- In our case:

$$Score = \frac{\sum_{i=0}^{size_{in}} pair[i]}{\mathrm{Max}(size_{in}, size_{ref})}$$

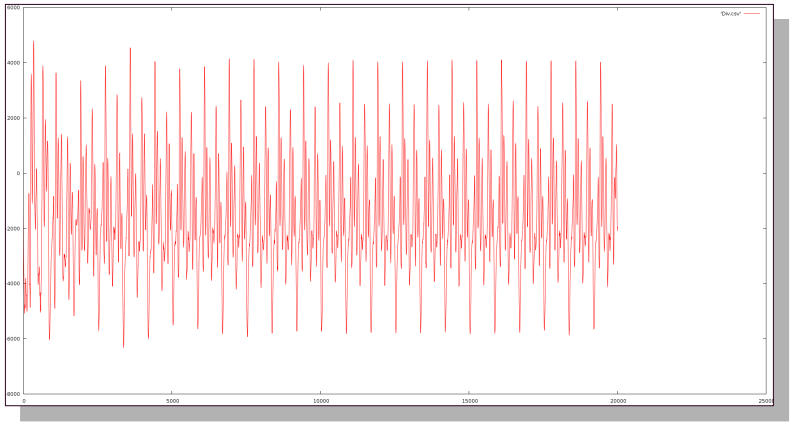
- Hardware Implementation:



Sequential division

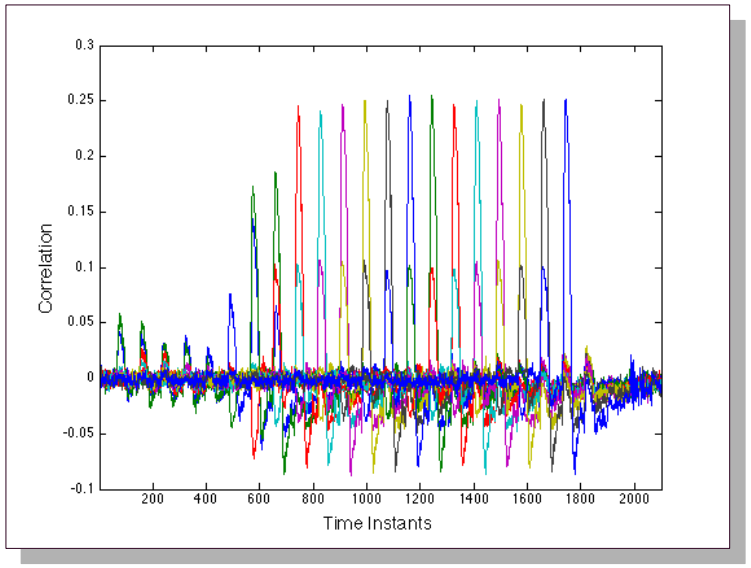
Template analysis

Retrieval of the score is done bit per bit by means of template analysis.



Profiling phase:

- The *Correlation(Val_bit, L)* allows the localization of each bit leakage moment.



Localization of leakage moments

Template analysis (results)

Profiling phase: Profiling of each bit of the score.

$$\mathcal{T}_{\mathcal{S}_i} = \{\mu_{\mathcal{S}_i}, Cov_{\mathcal{S}_i}\}$$

Analysis phase: Computation of the *Likelihood* coefficient.

$$p(\mathcal{L}_j|\mu_{S_i}, Cov_{S_i}) = \frac{1}{\sqrt{(2\pi)^N |Cov|}} \times e^{-\frac{1}{2}(\mathcal{L}_j - \mu_{\mathcal{S}_i})^T Cov^{-1}(\mathcal{L}_j - \mu_{\mathcal{S}_i})}.$$

Template analysis (results)

Profiling phase: Profiling of each bit of the score.

$$\mathcal{T}_{\mathcal{S}_i} = \{\mu_{\mathcal{S}_i}, Cov_{\mathcal{S}_i}\}$$

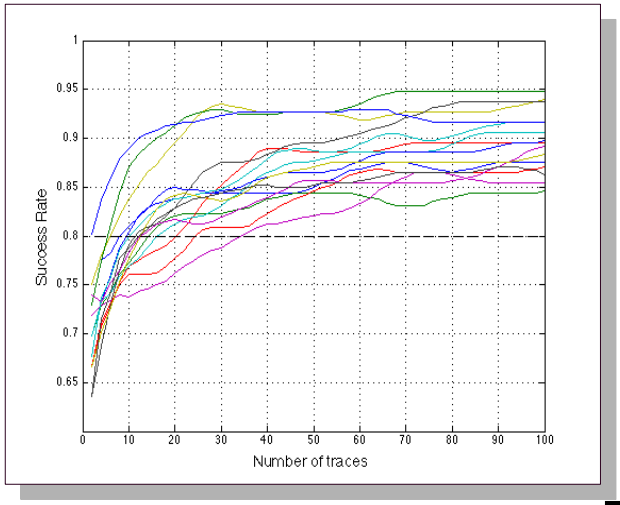
Analysis phase: Computation of the *Likelihood* coefficient.

$$p(\mathcal{L}_j|\mu_{S_i}, Cov_{S_i}) = \frac{1}{\sqrt{(2\pi)^N |Cov|}} \times e^{-\frac{1}{2}(\mathcal{L}_j - \mu_{\mathcal{S}_i})^T Cov^{-1}(\mathcal{L}_j - \mu_{\mathcal{S}_i})}.$$

PCA: During both phases
the principal component is used.

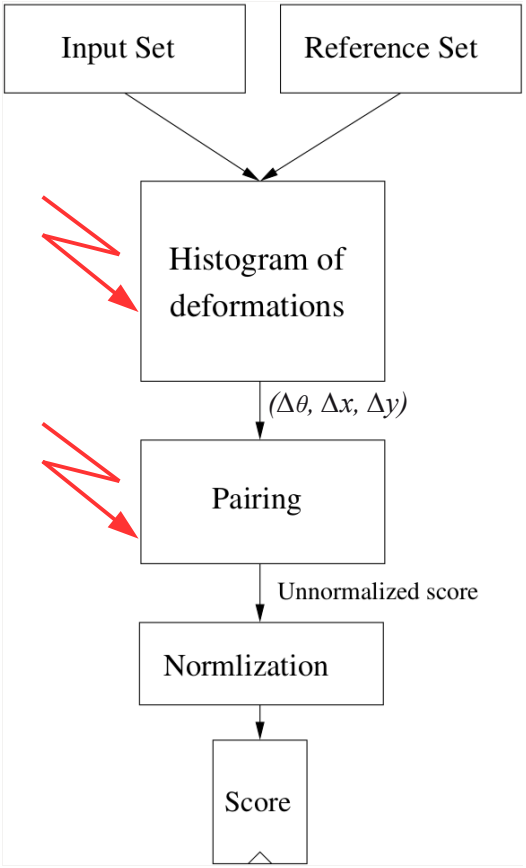
Results:

- Number of required traces differ for each bit.
- 34 traces are required per score extraction.



Success rate

Enhancement of the Hill Climbing



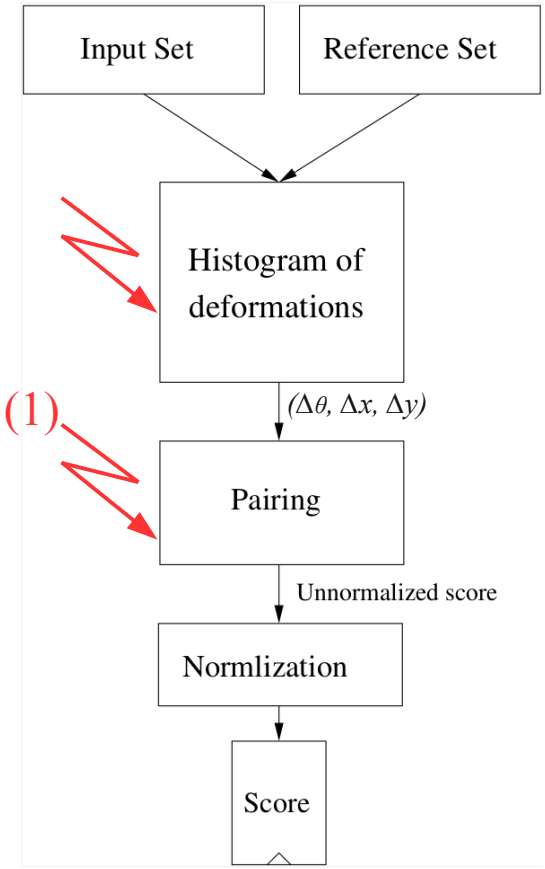
The matching algorithm

Enhancement of the Hill Climbing

Enhancement of the HC consists in:

(1)Retrieval of the reference set size

→ Optimal score normalization.



The matching algorithm

Enhancement of the Hill Climbing

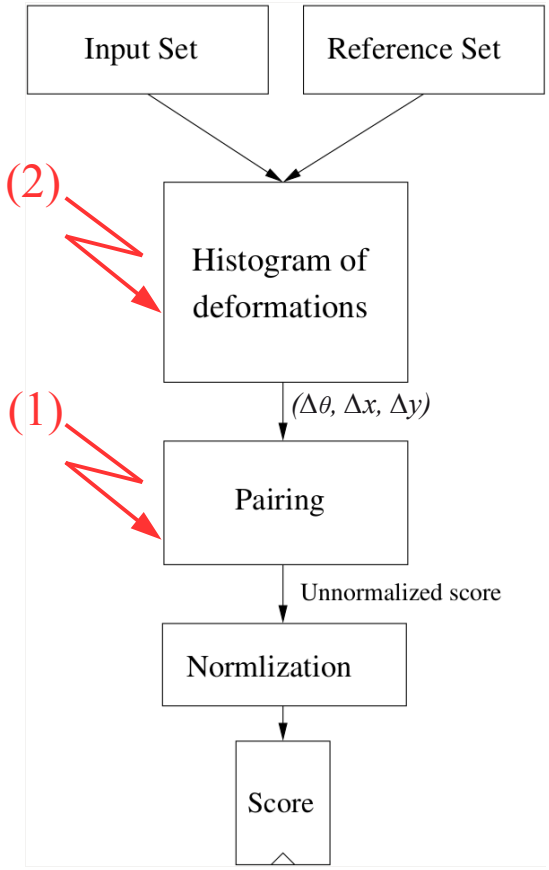
Enhancement of the HC consists in:

(1)Retrieval of the reference set size

→ Optimal score normalization.

(2)Retrieval of partial coordinates.

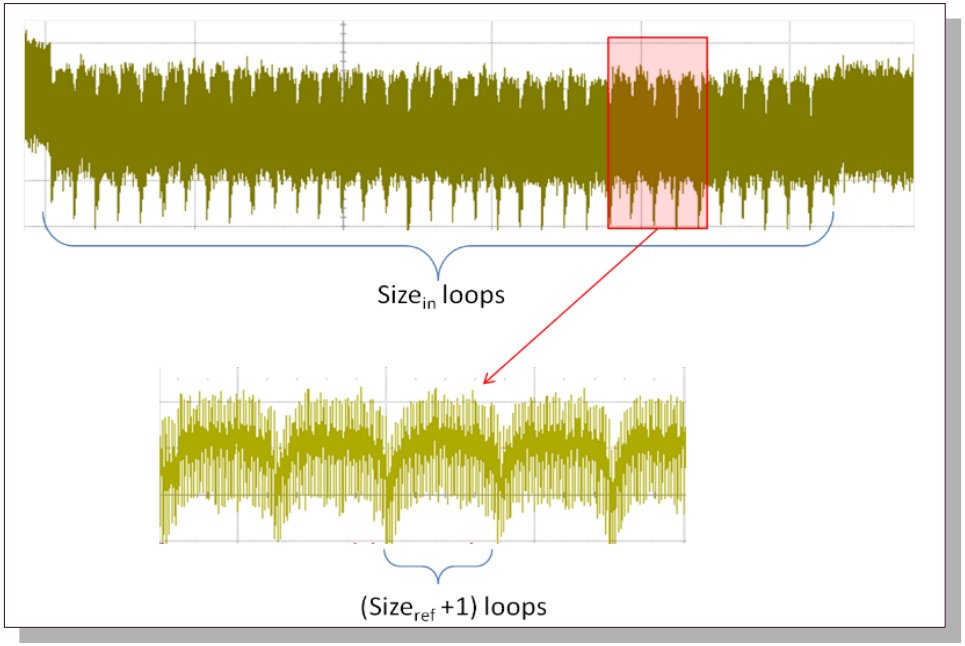
→ Reduction of the synthesis coordinates set.



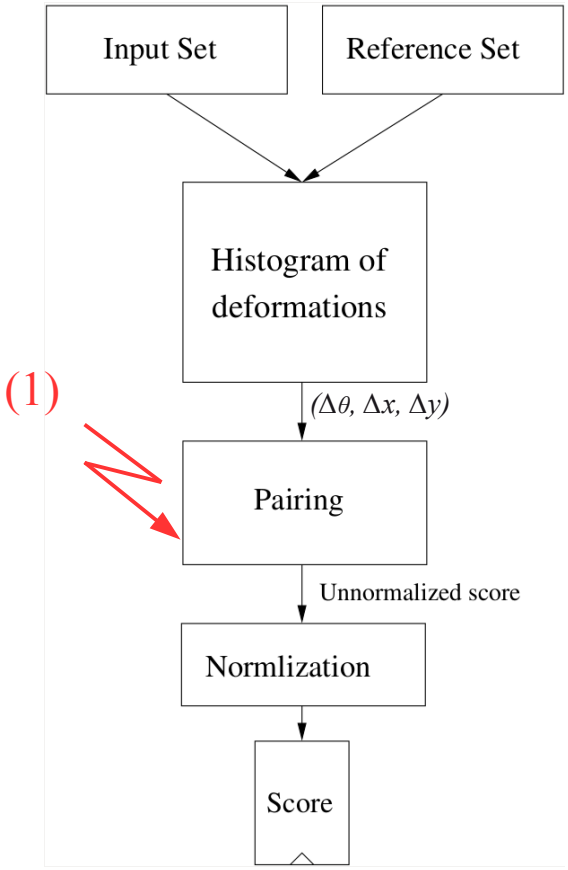
The matching algorithm

SPA on the Pairing phase

The pairing: ***Exhaustive*** one to one comparison between minutiae of the compared fingerprints.



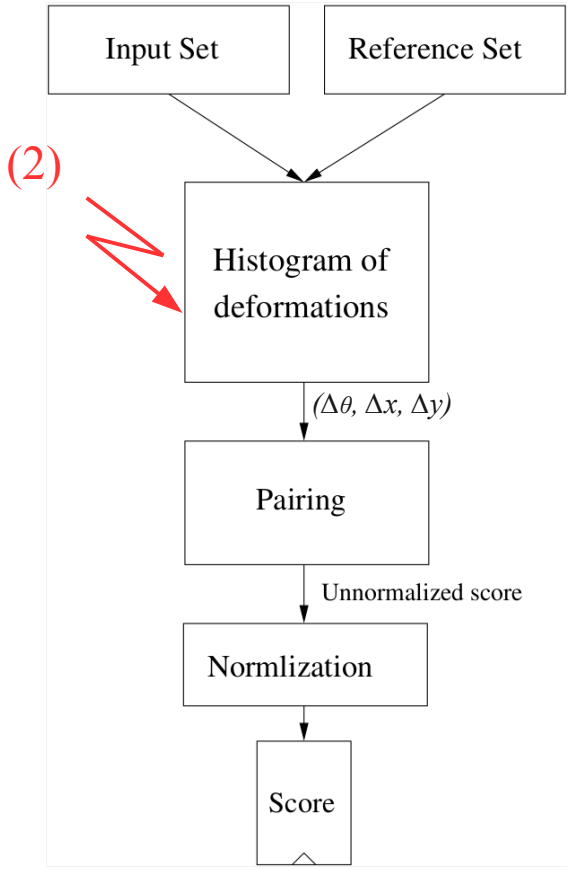
The pairing phase duration is correlated to the reference set size



The matching algorithm

Enhancement of the Hill Climbing

The registration:

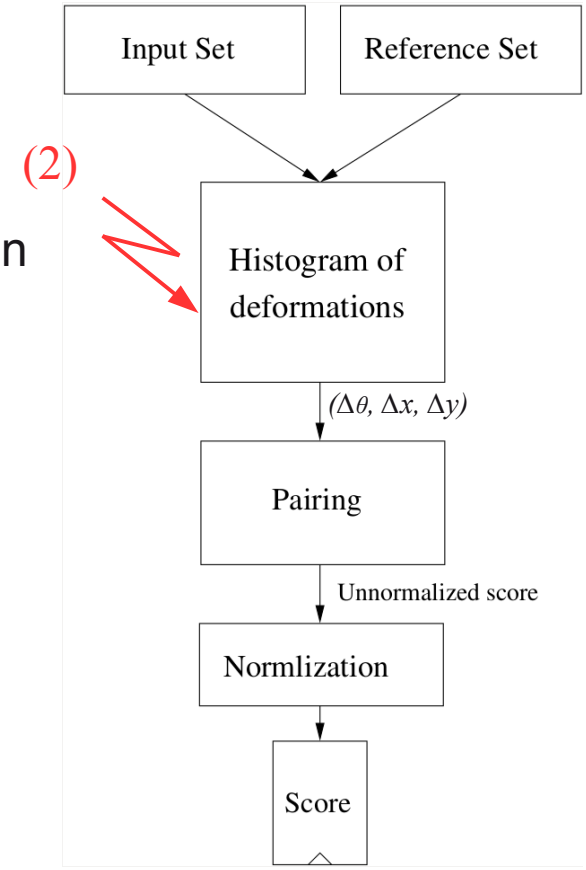


The algorithm flowchart

Enhancement of the Hill Climbing

The registration:

- Construction of a histogram of differences between each possible *(Ref, input)* minutiae pair.



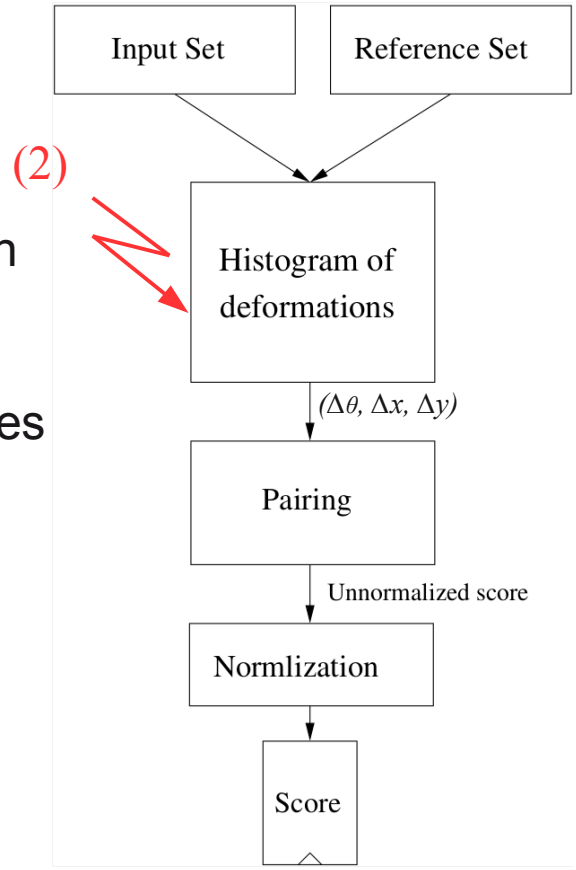
The algorithm flowchart

Enhancement of the Hill Climbing

The registration:

- Construction of a histogram of differences between each possible *(Ref, input)* minutiae pair.
- A straightforward implementation requires resources beyond what is available in actual smart-cards.

→ ***Hardware adaptation.***

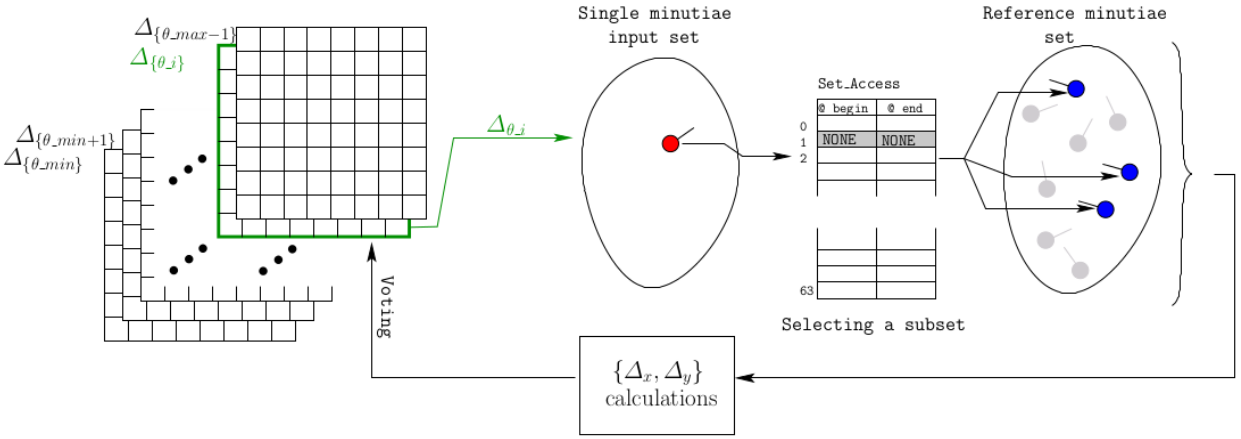


The algorithm flowchart

Enhancement of the Hill Climbing

Algorithmic adaptation:

(1) Iterative and partial constructions of the histogram *(<u>Δ_θ is processed in an incremental sequence</u>)*



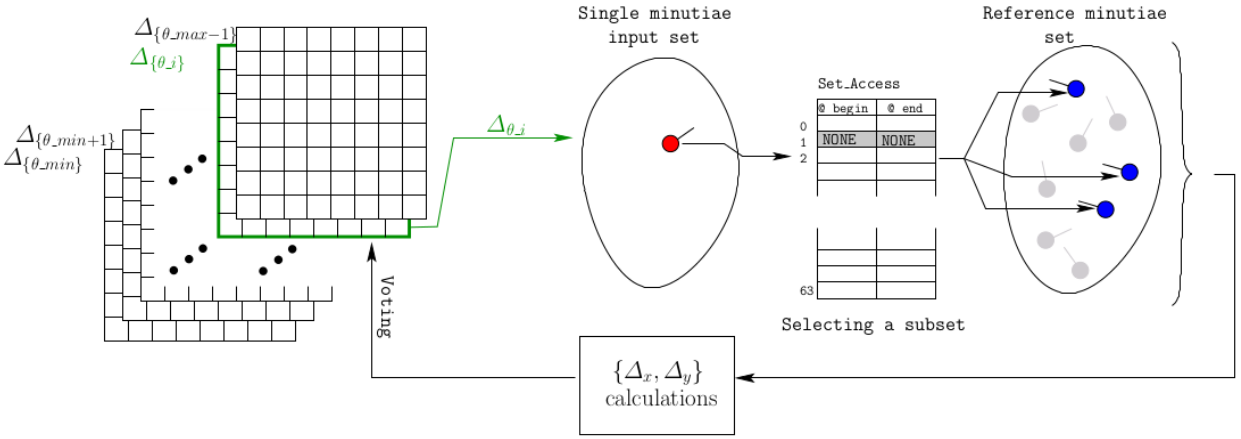
The algorithm adaptation

Enhancement of the Hill Climbing

Algorithmic adaptation:

(1) Iterative and partial constructions of the histogram *(<u>Δ_θ is processed in an incremental sequence</u>)*

(2) Usage of a *<u>fingerprint map</u>* to speedup the minutia search.



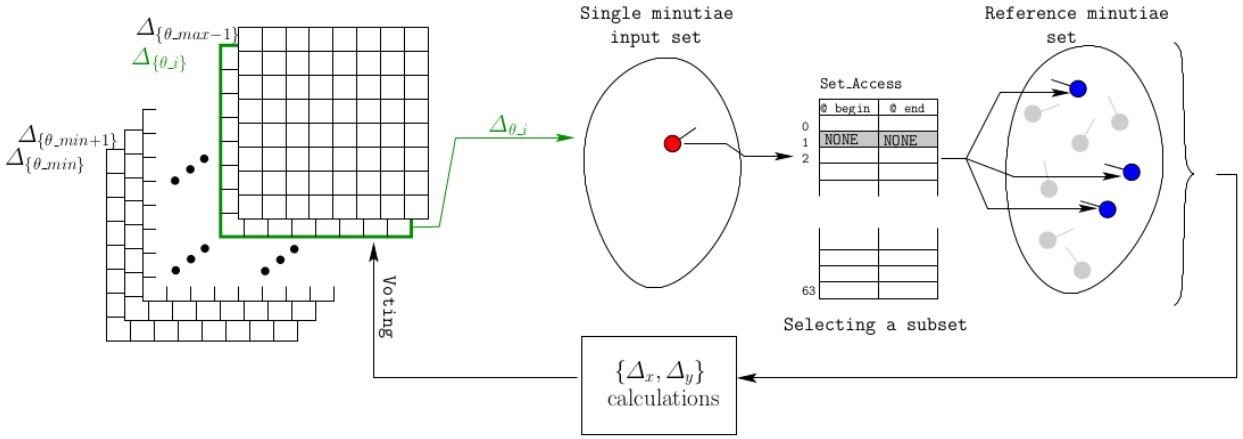
The algorithm adaptation

Enhancement of the Hill Climbing

Algorithmic adaptation:

(1) Iterative and partial constructions of the histogram *(<u>Δ_θ is processed in an incremental sequence)</u>*
(2) Usage of a *<u>fingerprint map</u>* to speedup the minutia search.

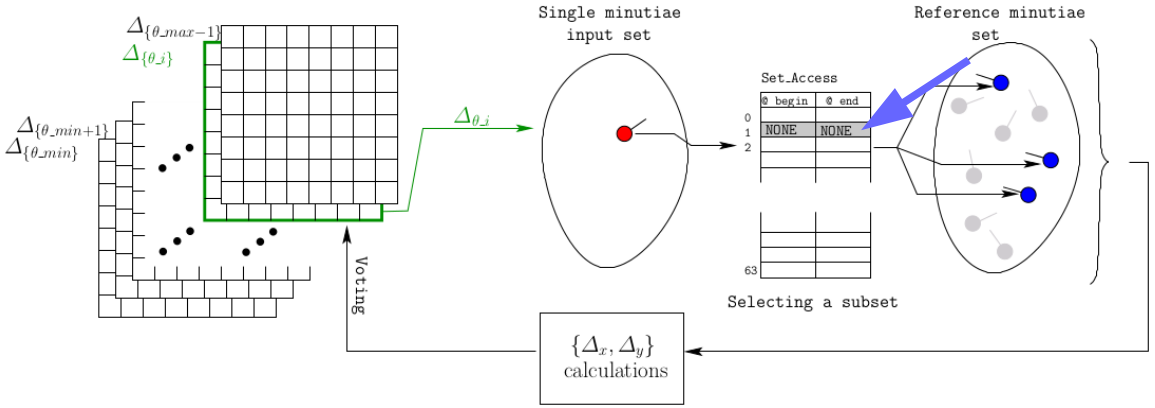
→The order in which the reference set is read in depends on (1) and (2).



The algorithm adaptation

SPA on the registration

Due to missing angles, distinguishable patterns in the power consumption are observed.



First observation:

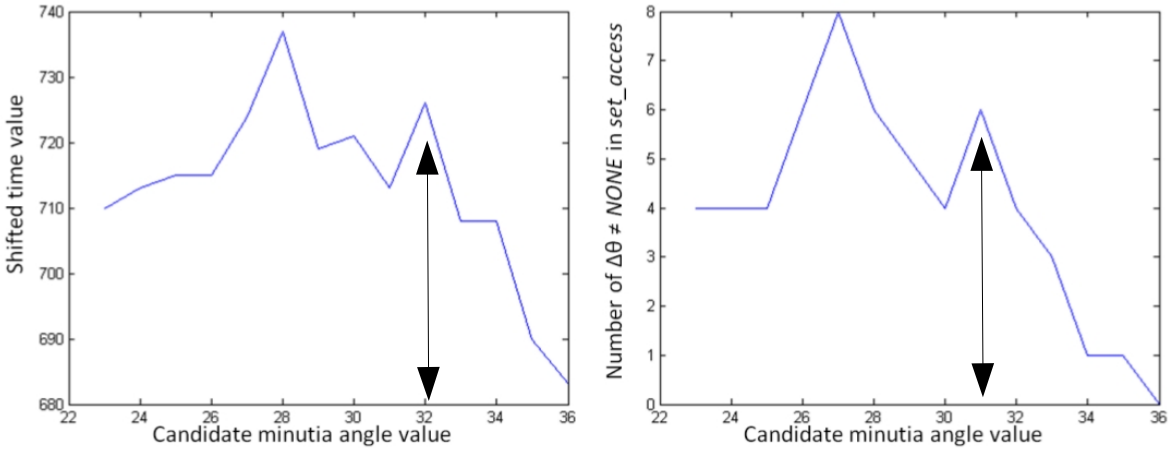
•Rotation of the input minutiae impacts the position of the consumption pattern.

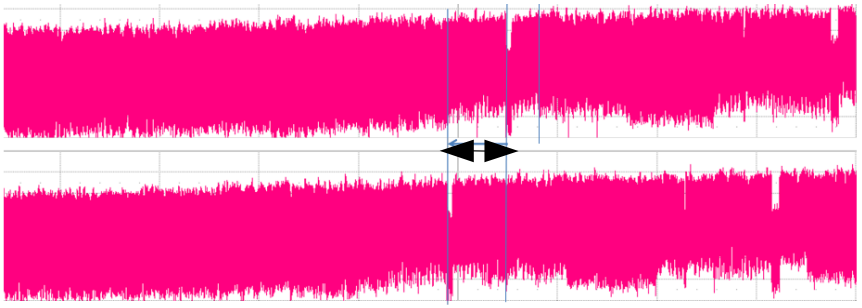
Pattern positions in the leakage traces

SPA on the registration

Second observation:

The duration of the shifts is correlated to the number of minutiae per angle for a particular angle.

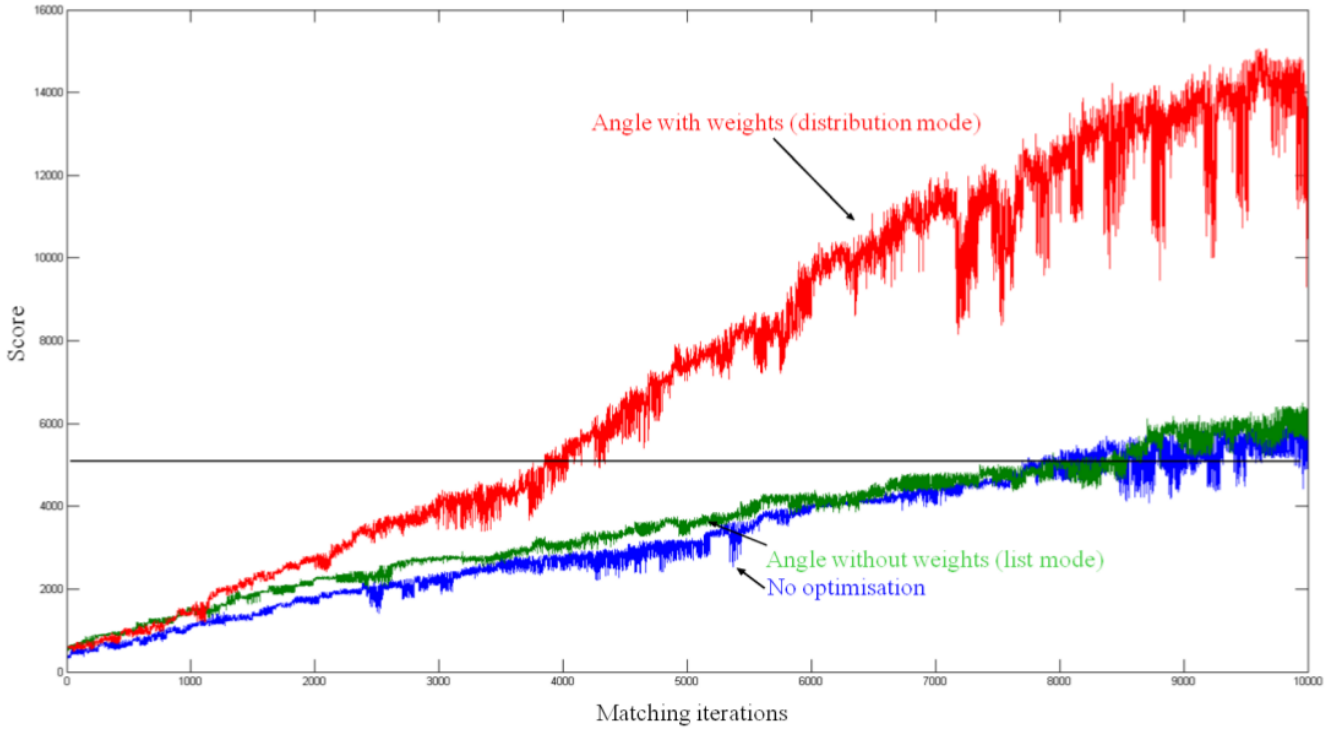




Enhancement of the Hill Climbing

Number of iterations is reduced by nearly half.

- *For the following example, 4000 iterations are required.*



Reduction of the number of iterations required for HC

The Countermeasures (1): The Score

Straightforward normalization :

In order to produce a binary answer:
(1) The score is computed.
(2) Compared to a fixed threshold.

$$Score = \frac{\sum_{i=0}^{size_{in}} pair[i]}{\mathrm{Max}(size_{in}, size_{ref})}$$

The Countermeasures (1): The Score

Straightforward normalization :

In order to produce a binary answer:
(1) The score is computed.
(2) Compared to a fixed threshold.

$$Score = \frac{\sum_{i=0}^{size_{in}} pair[i]}{\mathrm{Max}(size_{in}, size_{ref})}$$

Dynamic threshold :
The score is not normalized!
The threshold is dynamically adjusted.

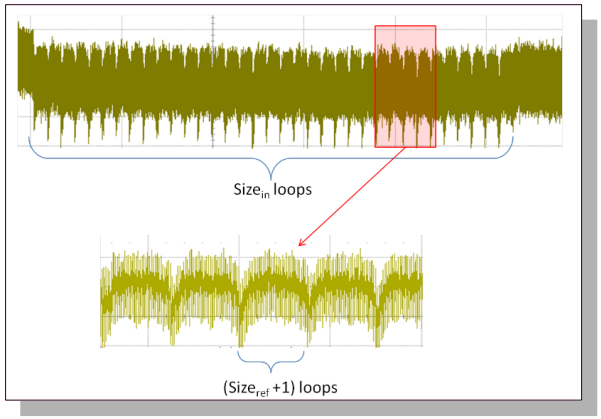
$$AccuScore = \sum_{i=0}^{size_{in}} pair[i]$$
$$DyScore_{Th} = Score_{Th} \times \mathrm{Max}(size_{in}, size_{ref})$$
if $DyScore_{Th} \leqslant AccuScore$ **then**
  Answer $= 1$
else
  Answer $= 0$
end

The Countermeasures (2): HC Enhancements

Masking the pairing duration:

- Random padding during the pairing phase.

- Constant duration of the pairing.

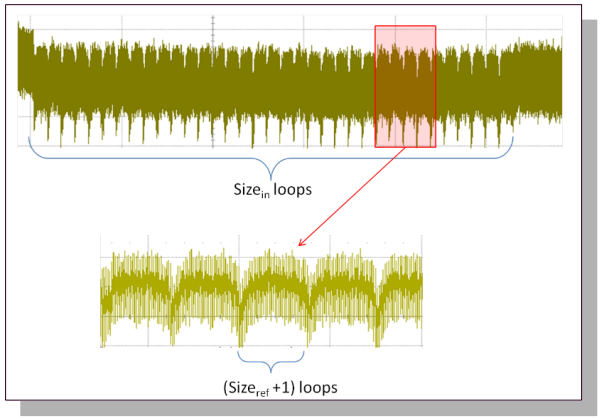


The pairing phase duration can be randomly padded.

The Countermeasures (2): HC Enhancements

Masking the pairing duration:

- Random padding during the pairing phase.
- Constant duration of the pairing.



The pairing phase duration can be randomly padded.

Masking the angle sequence:

Construction of histogram can be done in any random order.

```
for rot_a=0 to NB_MAX_ANGLE-1 do
    use(rot_a) ...
end
```

Sequence order of the angle process

```
mask = generate_random_number()
for rot_a=0 to NB_MAX_ANGLE-1 do
    m_rot_a = rot_a ⊕ mask
    use(m_rot_a) ...
end
```

Random order of the angle process

The BMOS project

The presented work is funded by the ANR project BMOS

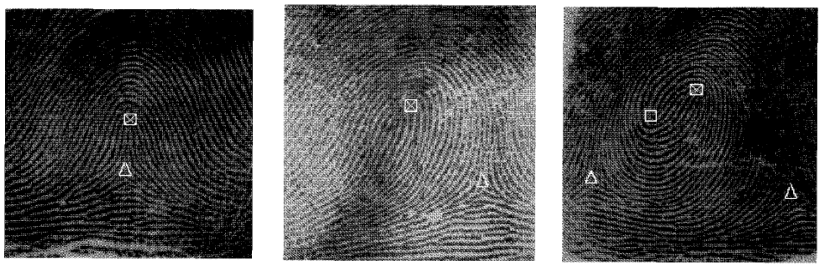
Questions ?

Thank you for your attention

How to identify a fingerprint?

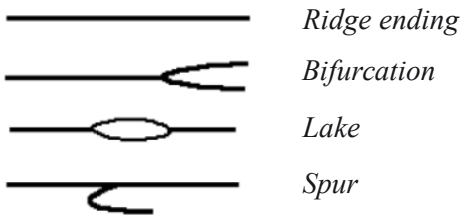
Different ridges shapes with *3 resolution levels*.

Level 1: Global ridges shape forming Core and delta.



. . .

Level 2: local ridge shapes i.e. Minutiae



Level 3: High definition details, pores, dotes…