Security evaluation of a BMOS (Biometric Match On Smartcard)

Presented by Taoufik Chouta

Plan

I **–** Categories of biometric authentication system

II **–** What is a *BMOS* system ? And why ?

III **-** Fingerprint features levels

IV **–** A Verification algorithm (algorithmic adaptation)

V – A *CPA* approach

VI **-** Conclusion

Categories of biometric authentication system

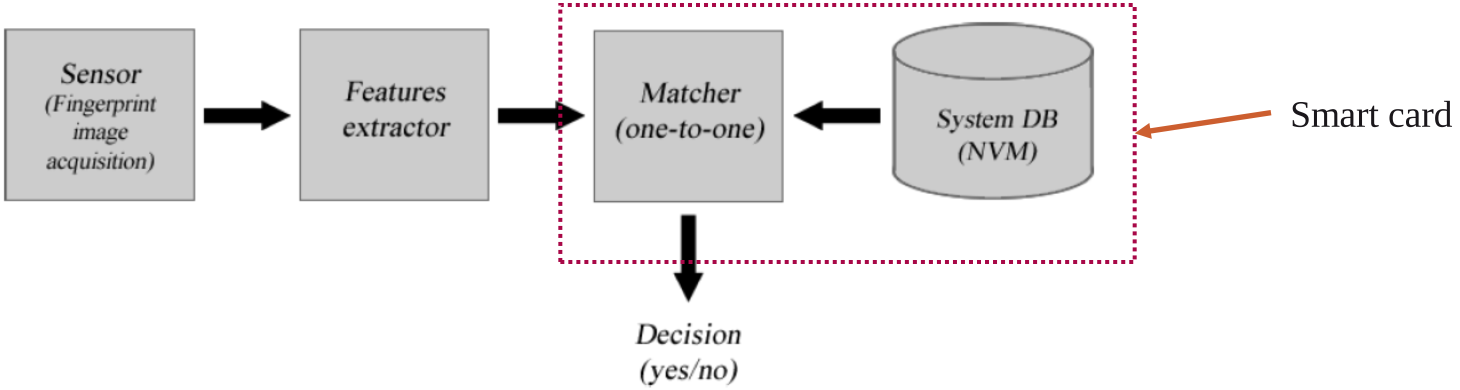
- *Identification:* identify biometric traits in a database => 1:n comparisons.
- *Verification:* confirming the identity of an individual =>1:1 comparison.

Examples of application domain

Advantages: Increasing security level by Substituting the PIN by a biometric trait

What is a BMOS system ? And why?

BMOS: Biometric Match On Smart card (matching only).



Biometric authentication system with four main modules

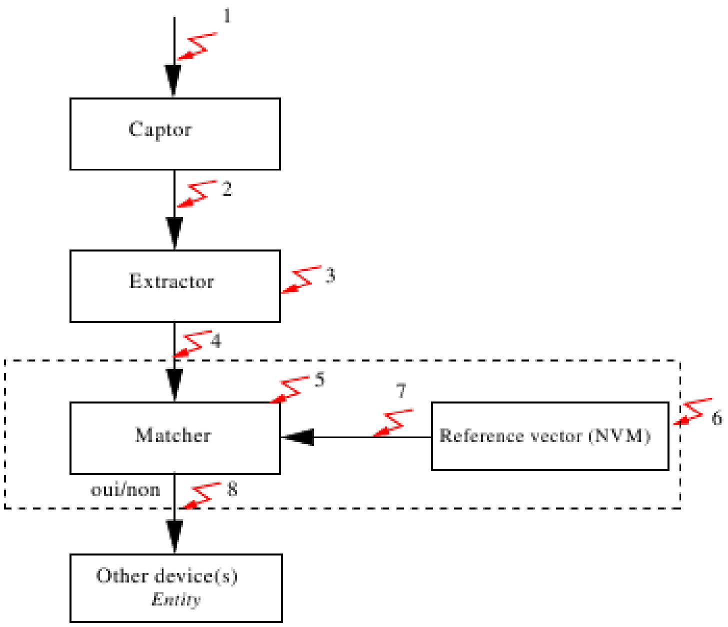
Advantage:
1-Verification inside the card, sensitive data kept secret.
2- Only decision is communicated (avoid direct Hill Climbing attacks [2])

Drawbacks:
Limitation of available resources
- Small RAM memory.
- Internal clock (24Mhz)
- Low calculation magnitude of the CPU

Potential attacks on generic biometric system

Potential attacks:

1. Using false finger.
2. Biasing the captor + Hill Climbing.
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.

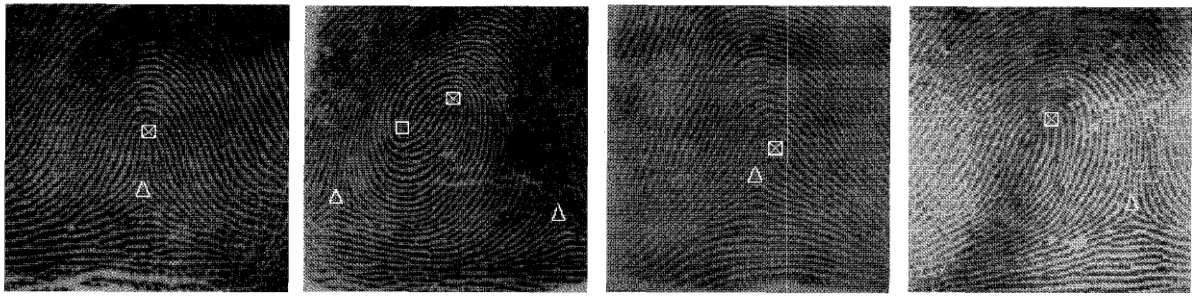


Potential attacks on biometric system

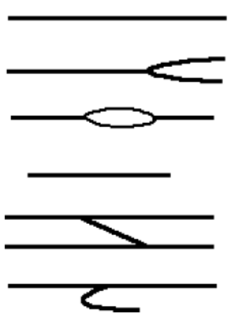
Attacks concerning smart card are surrounded: 4,5,6,7,8.

Fingerprint features levels (the secret data)

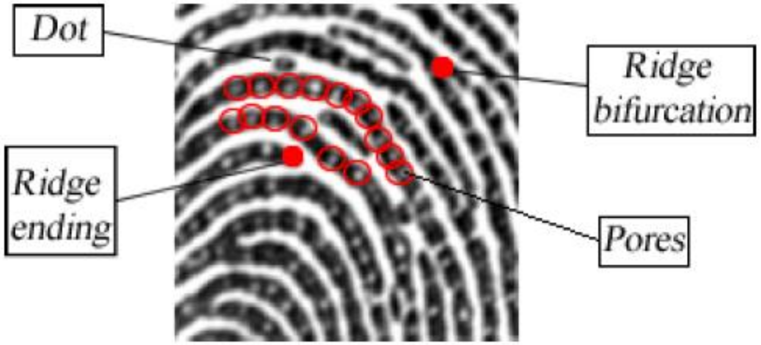
Level 1:
Core and delta positions.
(Global ridge shape)



Level 2: Minutiae (local ridge shape).

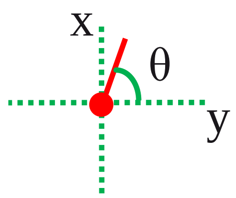


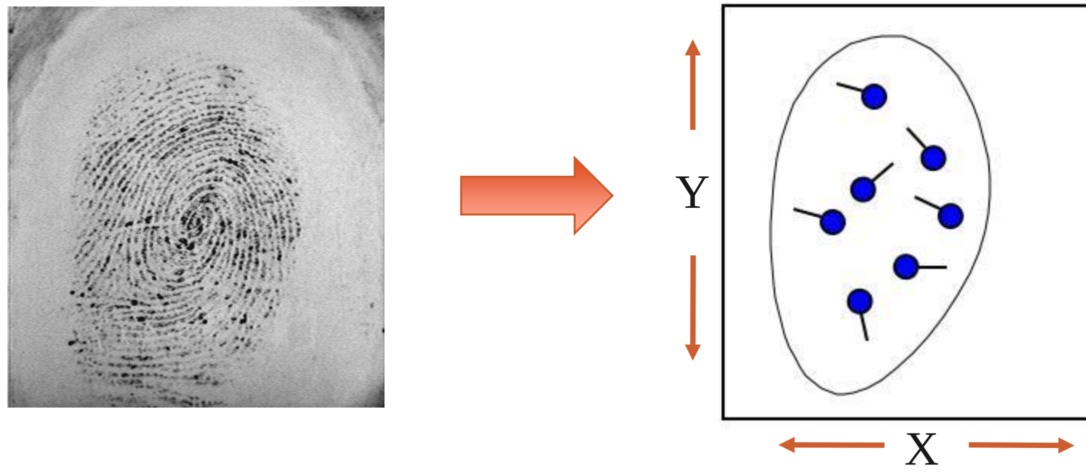
Level 3: High definition details: pores, dotes…



Fingerprint features levels (the secret data)

Compact version of the ISO standard 19794-2:
ridge ending & bifurcation minutiae (θ,x,y)





•Minutiae (θ,X,Y) coordinates are coded on (6,8,8) bits.
⇒256x256 image grid.
⇒64 possible orientations.

The studied verification algorithm

- The fingerprint verification problem can be presented as a point pattern matching.

Difficulties:

1- Sets are not sorted (depends on the extractor).
2- False minutiae (image quality).
3- Deformed minutiae (skin elasticity).
4- Sets with different cardinals (finger position).
5- No common landmark (core or delta)

Bad quality Images

Unlike cryptography there is no standard biometric verification algorithm !!

TELECOM ParisTech

The studied verification algorithm

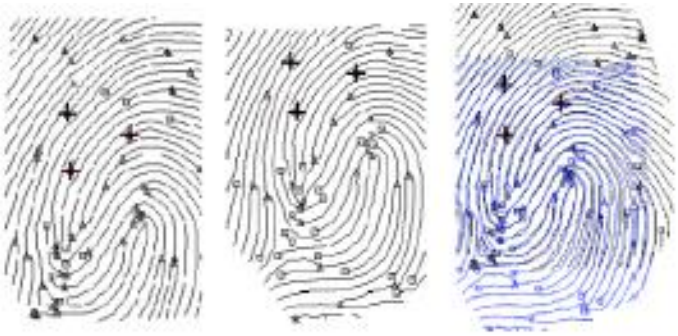
Two steps algorithm [3]:

1- Registration :
From two minutiae points sets, calculate best $\{\Delta\theta,\Delta x,\Delta y\}$ of affine transformation overlapping both sets (linear model).

$$T_{\Delta\theta,\Delta x,\Delta y} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix}$$

The affine transformation

2- Pairing:
a- Apply the found transformation.
b- Find nearest minutiae point in both sets and calculate a matching score.



Finger A Finger B Overlapped fingerprints

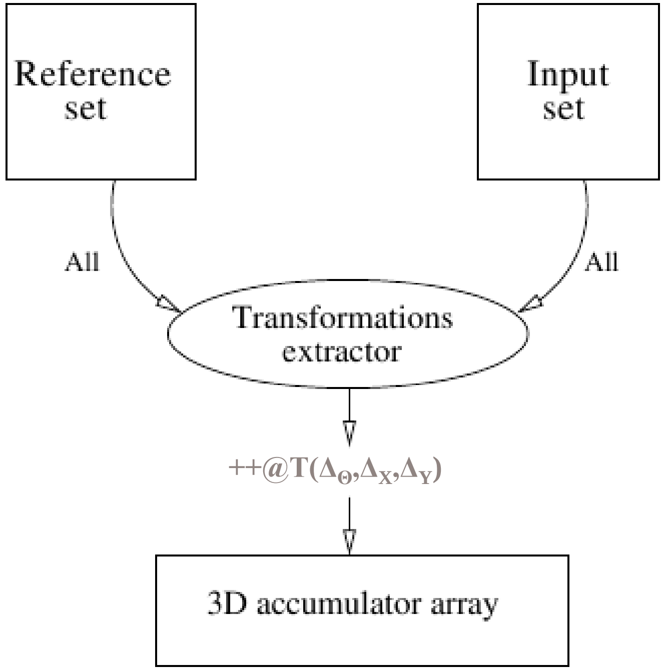
Constraints for smart card implementations:
- Verification in less than 0.5 second.
- Low performances deterioration.
- Limited resources.

The studied verification algorithm

Registration :

Transformation histogram construction:
1.Calculate Δ_{Θ}
2.Apply rotation on input minutiae.
3.Calculate Δ_X, Δ_Y
4.Increment @ $(\Delta_{\Theta}, \Delta_X, \Delta_Y)$.

- Statistically if the same parameters appears many times, they are likely to be the most appropriate ones for the analysis.



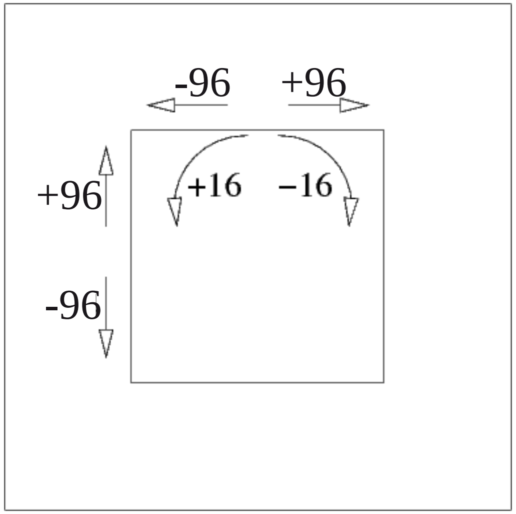
Histogram construction

The studied verification algorithm

Histogram memory requirement:

[-96, 96[^{2} * [-16, 16[for translations and rotation respectively.

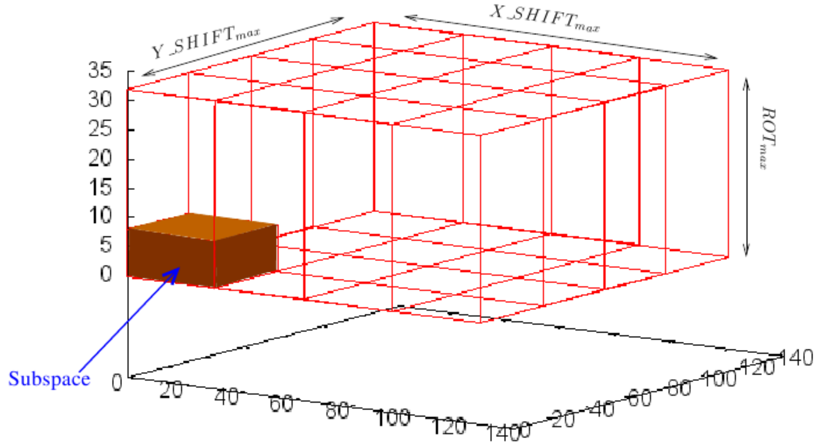
⇒Accumulator size 1.18MB! *(…On smart card??!)*
⇒How to reduce the required memory?
⇒What is the impact on the algorithm performances?



Rotation, translation inside an image grid

The algorithm adaptation

Transformation Subspaces:



Transformation space fragmentation

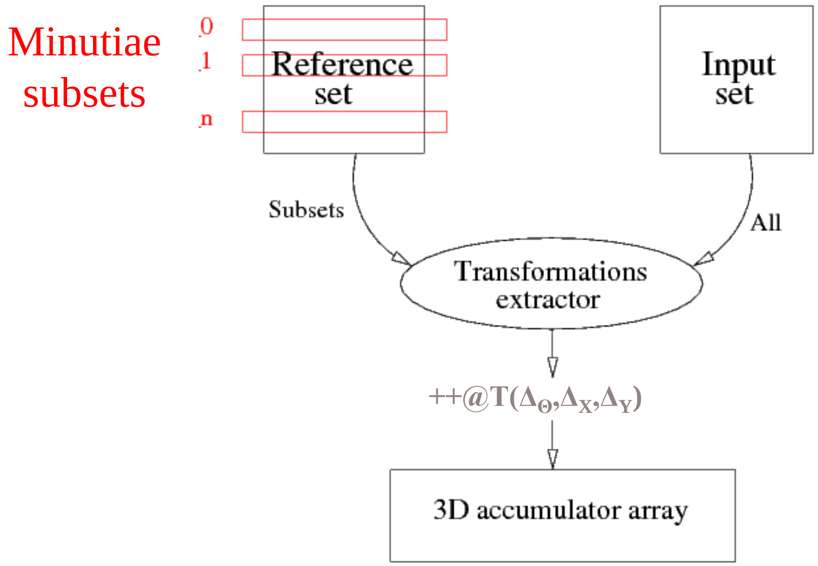
- Fragmentation of the transformation histogram space to many subspaces.
- A registration is done for each subspace.

⇒Required memory is relative to subspace dimension.
⇒Whole transformation space is parsed (no performance loss).
⇒Registration is repeated many times.

The algorithm adaptation

Transformation Subspaces:

Optimization n°1: Targeting a subset of minutiae involved in each subspace registration.



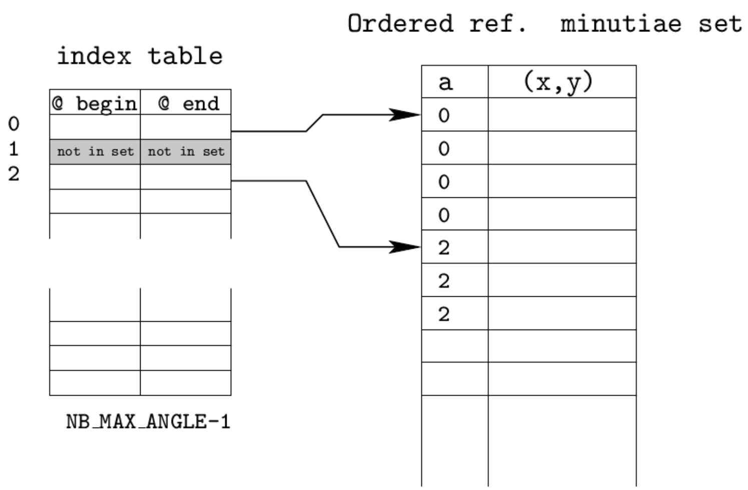
⇒ For each minutiae in the input set, find reference minutiaes with high probability to lead to a transformation accepted by the actual processed subspace.

The algorithm adaptation

Transformation Subspaces:

Optimization n°1: The Set_Access Table

- Sort reference minutiae in an increasing angle order.
- Use set_access table pointing to the first and last minutiaes with a particular orientation angle.
- Sorting reference minutiae is done once and off-line.



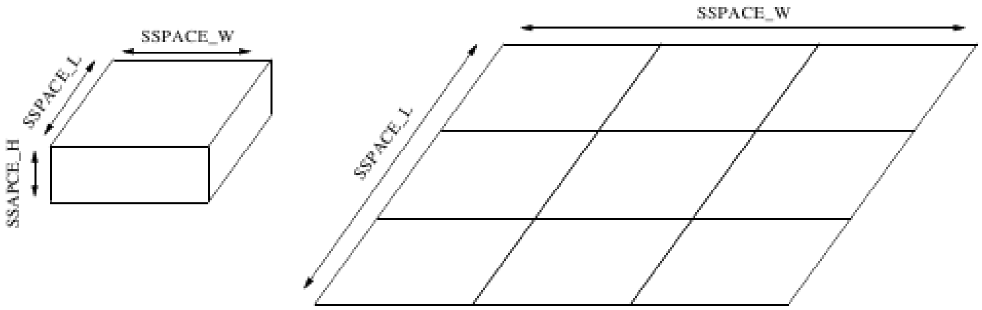
Set_Access table

The algorithm adaptation

Transformation Subspaces:

Optimization n°2: Subspace dimension strategy

- Increasing **translation** dimensions will decrease rejected transformations.
- Decreasing **rotation** dimension will not affect transformation acceptance by actual subspace.
- Same memory can represent many subspace dimensions

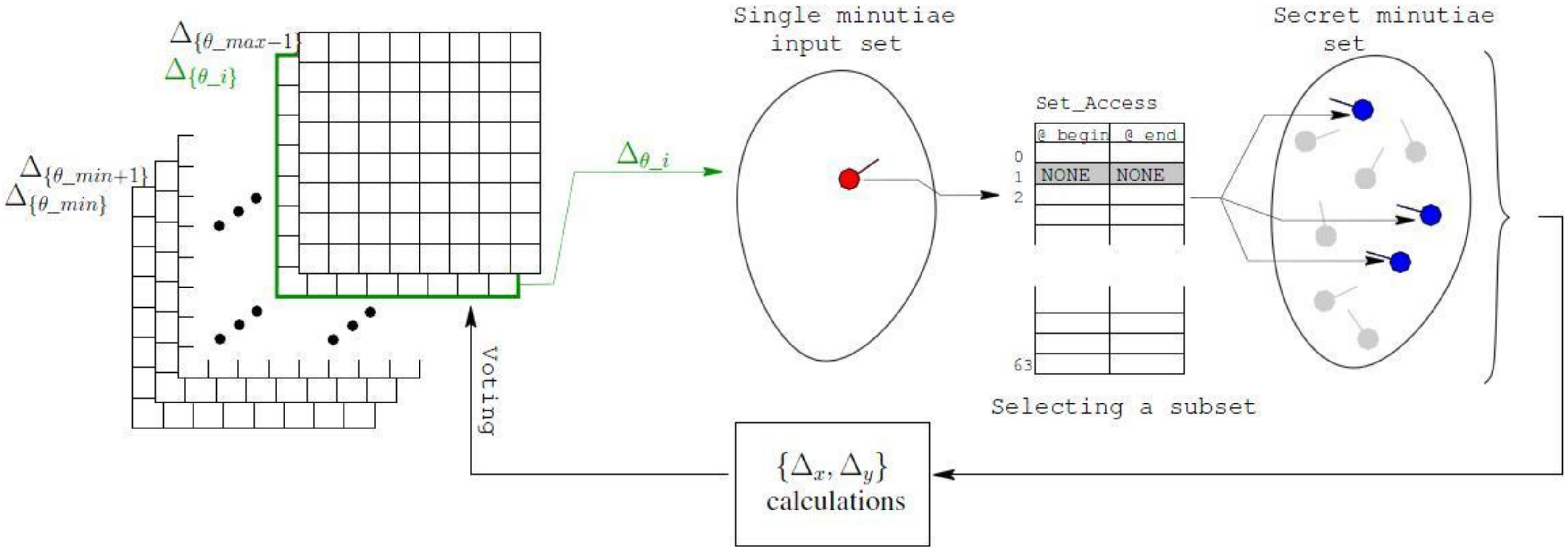


Same memory space representing two subspace dimensions

⇒ Less transformations are rejected due to Δx,Δy out of the subspace borders

The algorithm adaptation

Histogram subspace computation:



Histogram subspaces construction using a memory mapping array

A CPA approach

CPA attack on the first subspace:

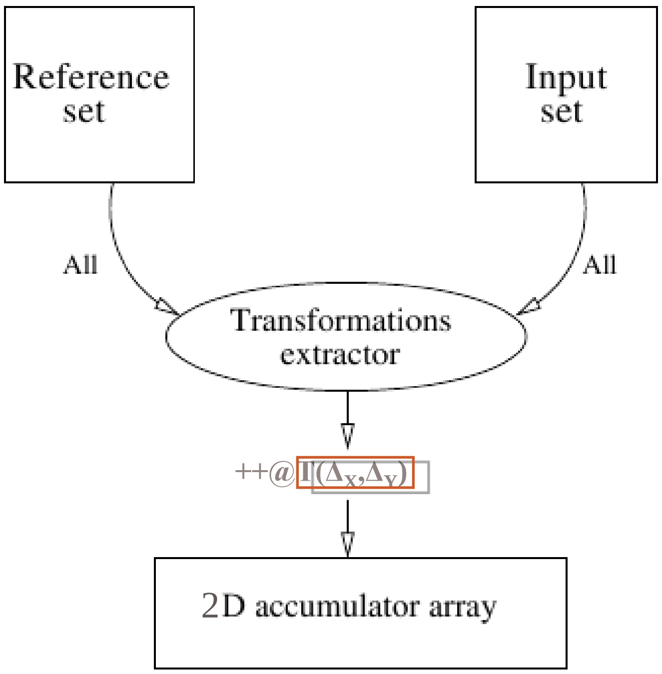
- By analogy to a ciphering algorithm
  The key is : a secret minutiae coordinates.
  The message is: input minutiae coordinates.
  Attacked registers: Δx and Δy registers.

⇒ The algorithm adaptation allows to target specific minRef.**θ.** Thus we assume θ *is known*.

⇒ Computing the leakage hypothesis

⇒ Hypothesys are done on (X,Y) = (2^{16}).

Remark: with a straightforward implementation hypothesis space will be composed from (2^{22}) minutia.



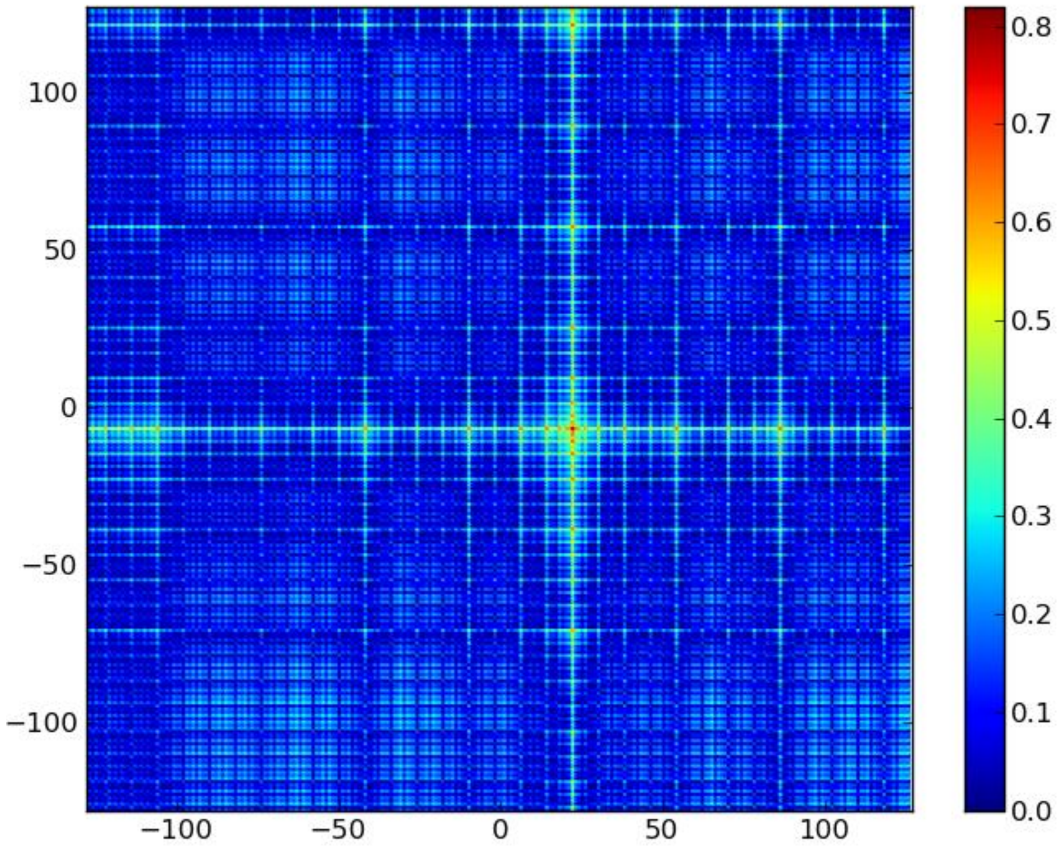
Histogram construction

A CPA approach (Simulated attack)

Example of simulated results :

- $Min_{secret} = (21, 22, -7)$
- Nbr traces = 1000
- SNR = 2.5
- Remark: high correlation on :
  $Min_{hyp} = (21, 22, y)$ and
  $Min_{hyp} = (21, x, -7)$

  => The rotation during the first registration round is near to zero.



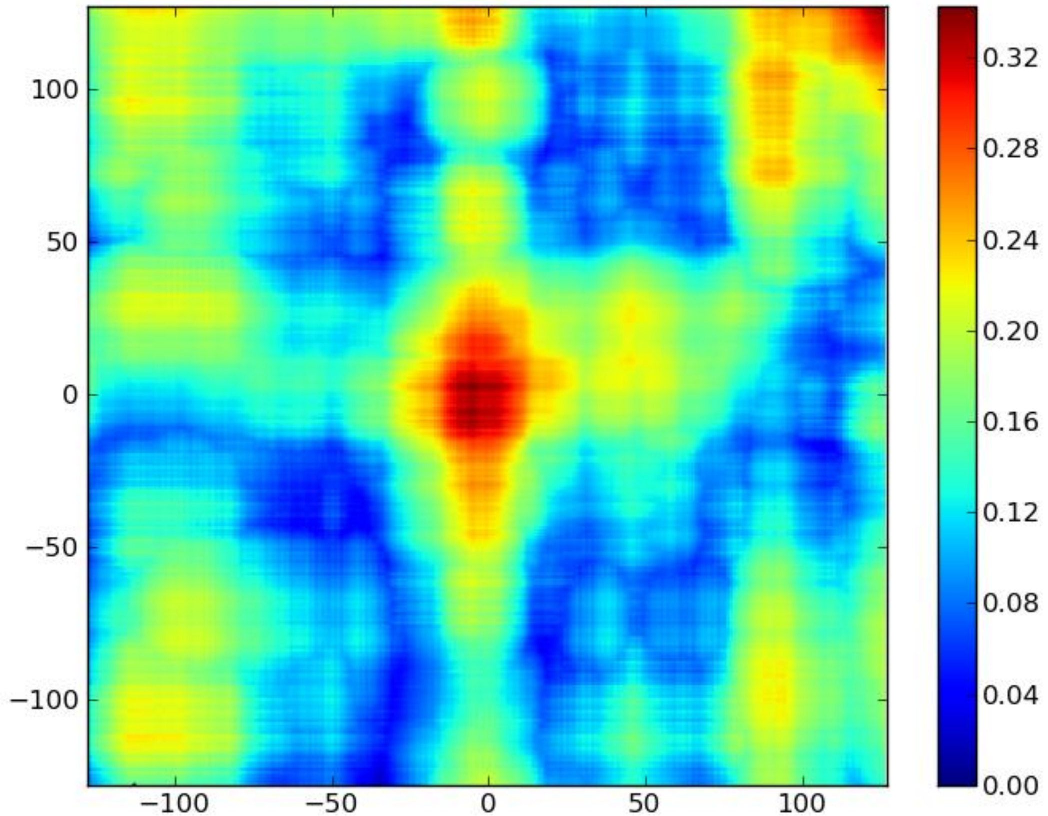
Simulated CPA coefficient

TELECOM ParisTech

A CPA approach (Real attack)

<u>Results of real attack :</u>

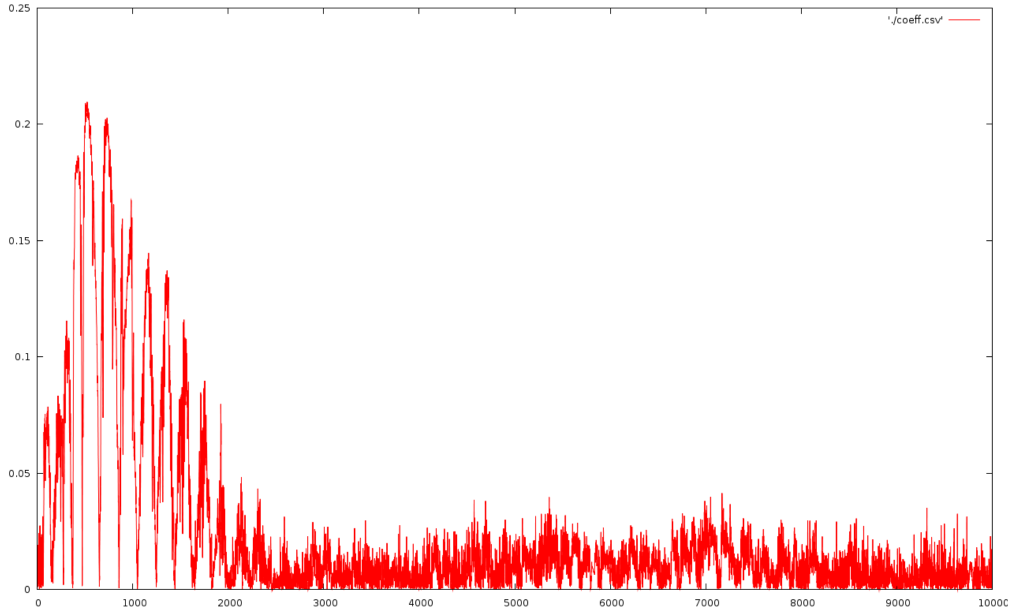
- Min_{True} = (21, 22, -7)
- Nbr traces = 30K
- Remark: high correlation on false hypothesis (0.34)



Results of real CPA

A CPA approach (Real attack)

Results of real attack :



Real CPA coefficients

- What gives multiple correlation spikes …?

=> Data loading ?

=> Attacked registers are used at next processing entities?

TELECOM ParisTech

Conclusion & Perspectives

- **Conclusion:**
  - Algorithm adaptation of a BMOS algorithm to limited resources systems.
  - Potential side channel attack on the registration phase.

- **Perspectives:** evaluating the efficiency of the following countermeasures:
  - Randomizing subspaces sequence.
  - Masking by using false minutiae.
  - Transforming the input vector before computation.
  - Randomizing the input set as well.

Questions ?

Thank you for your attention

References

[1] “Spotlight on Biometrics[online],” http://www.unisyssecurityindex.com.

[2] Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification, oct. 2006.

[3] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, “A real-time matching system for large fingerprint databases,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 18, no. 8, pp. 799–813, 1996.

Annex: Biometric traits

Biometric technologies evaluation [1]

Effort: the end user required effort.

Intrusiveness: end user acceptance of the biometrical technology.

Cost: technology cost, (reader, scanner…).

Accuracy: discrimination level the biometric trait.