# Enhancement of Hill Climbing Attacks on Biometric Embedded System Using SCA

*Taoufik Chouta, Jean-Luc Danger, Tarik Graba*

**Abstract**

Although being widely used on heavy servers to secure access to restricted buildings/areas, biometrics authentication is considered nowadays as an emerging technology in the field of embedded systems. This means that these devices will come into reach of untrusted users, which may decrease the integrity and confidentiality over personal biometric traits.

While most of the Side Channel Attacks in the literature are focused on cryptographic implementations, there is no side channel attack targeting biometric matchers that has been published yet.

In this paper we present some side channels analysis that enhance the potential of the *Hill Climbing* [1] heuristic attack on biometric systems. Based on a comparison score, this heuristic aims to find the shortest path to synthesize an approximate duplication of the secret template within the embedded system. In our study, the fingerprints were chosen as biometric traits. Each fingerprint template is composed of a set of 3 dimensional points called minutiae. A minutiae point is an oriented $2D$ point $(x, y, \theta)$.

Thus, the attack based on the *Hill Climbing* takes as a start point, the most similar fingerprint to the secret, over a randomly composed database. This ensures to shorten the amount of modifications needed to be processed to reach a satisfying similarity level. Authors of [1] assumed that the secret fingerprint is hard to synthesize when heuristic requires above $5000$ iterations, which makes the attack unsuccessful. Therefore, we propose side channel based methods to shorten the synthesize path leading to a success rate increase.

Our main approach aims to synthesize a better starting point for each attacked fingerprint. From a statistical point of view, having any kind of information on that fingerprint decreases the synthesize possibilities, which can be very large (e.g., $2^2200$, or more).

An non exhaustive list of side channel information that can be used to optimize the heuristic attack is listed below:

1. Size of the secret minutiae set.
2. Partial coordinates of a subset (or the whole set).
3. Paired points between the secret and the synthesize sets.

Regarding the first point, the similarity of two sets of points is based on the percentage of overlapped points over both sets. Additional or missing points in the synthesized set decreases the percentage of similarity. As sizes of secret sets may vary, the exaction of this information using side channel analysis allows to optimize the heuristic search for each attacked fingerprint.

Concerning the second point, the construction of the secret set can be shared between a side channel analysis, which aims to extract partial coordinates using consumption traces, and the Hill Climbing heuristic that modifies the synthesized set based on the similarity score.

The last point enhances drastically the performance of the heuristic, as modifications are avoided on paired points between the secret and the synthesize sets, all modifications take place only on non-overlapped points which makes the heuristic efficient.

Hence, we designed a biometric coprocessor to acquire consumption traces, and extract useful information using side channel information like SPA, timing evaluation. As the duration of the paring phase is correlated to the compared sets, timing attacks allow us to successfully extract the size of the secret minutiae set. When simple power analysis permits to localize missing point subsets of the secret fingerprint. A low consumption was distinguished in case of memory requests to those missing sets. This allows to retrieve coordinates of minutiae points on the orientation dimension. We are still working on the pattern identification distinguishing consumption of paired and non-paired minutia points. For that goal we are investigating tools like pattern recognition, differential power attacks, correlation power attacks, *etc*.

**Keywords:** Side channel attacks, Fingerprint, MOC, Smart Card, Biometric verification.

## References

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