Biometrics and Cryptography: *New Techniques for Protection of Identities*

Context Biometric recognition enables an individual

-to be authenticated without the need to hold or remember anything

-or to be identified among a set of many individuals.

However, biometrics raises privacy issues (confidentiality of the data and the privacy of the associated individuals); moreover, comparison of biometric data is not limited to a simple equality test due to the inherent noise of a biometric capture and classical cryptographic solutions are not sufficient.

Aims New privacy enhancing technologies for biometrics, to ensure confidentiality of data and privacy of human users.

Main Playground Research in Security and Cryptography Team (leaded by Hervé Chabanne), involved in and technical leader of several collaborative research projects

- BACH (Biometric Authentication with Cryptographic Handling), 2006-2009, French ANR Project

-TURBINE (TrUsted Revocable Biometric IdeNtitiEs), 2008-2011, FP7 Integrated Project

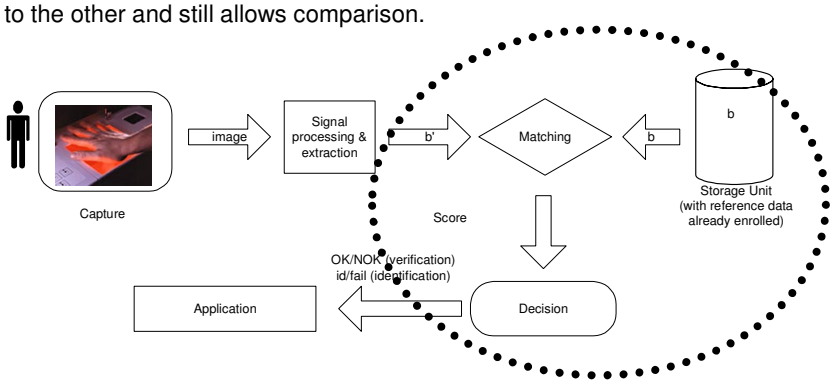
Main Works

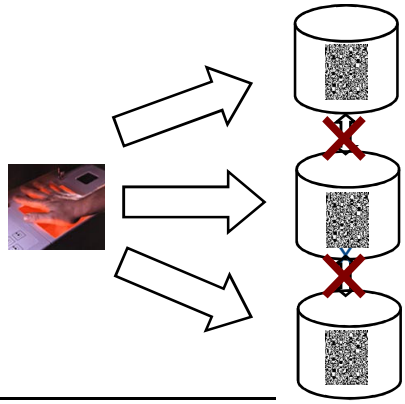
-Quantization/binarization of biometrics

-Definition of security/privacy models

-Integration into newly designed cryptographic protocols

What we want Increasing security/privacy during the treatments and storing biometric templates in a way: which is easy to renew; which does not leak information on the underlying biometric data/identity; but, which deals with variability that arises from one capture to the other and still allows comparison.

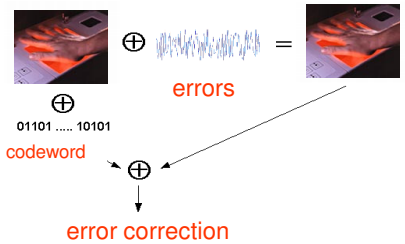




Example 1 Remote storage for an authentication scheme achieving both confidentiality of the biometric data and privacy of the users. *See « An Authentication Protocol with Encrypted Biometric Data », Bringer, Chabanne, AFRICACRYPT 2008, Best Paper Award.* Made possible thanks to the combination of secure sketches, of a Private Information Retrieval protocol due to Lipmaa and of the Goldwasser-Micali and Paillier cryptosystems.

Tools

Secure Sketches after binarization of biometrics

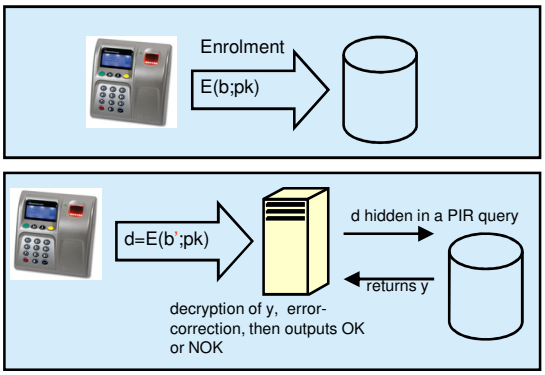


Homomorphic encryption

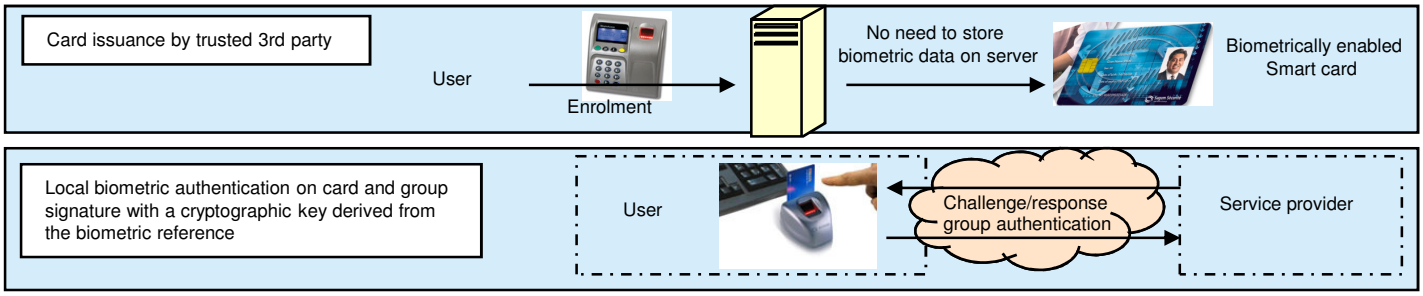
Dec(**Enc**(X;pk)×**Enc**(X';pk);sk) = X⊕X'

Private Information Retrieval (PIR)

Capability to query a block into a database without letting the database learn which block is returned.



Example 2 Securing a remote authentication using biometrics while preserving the user's anonymity?
See « An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication » Bringer, Chabanne, Pointcheval, Zimmer, IWSEC 2008. Biometric enabled token combined with group signature: biometric data does not leave the card; no identity information is sent; proven authorized access from the user; no mean to track user.



Collaboration Presentation partially illustrated thanks to joint works with Hervé Chabanne, Gérard Cohen, Malika Izabachène, Bruno Kindarji, David Pointcheval, Qiang Tang, Gilles Zémor, Sébastien Zimmer.

Contact Julien Bringer, Sagem Sécurité – julien.bringer@sagem.com

Sagem Sécurité