SECURE BIOMETRICS (ThuPmOR6)

Author(s) :

Marten Van Dijk (Philips Research, Netherlands)
Pim Tuyls (Philips Research, Netherlands)

Abstract :

In this paper, we extend the information theoretic secure constructions for biometrics to the computational setting. Based on semantically secure encryption, we introduce robust, fully private and secure biometric key distillation and verification. Our model incorporates an adversary with side information who has access to a database with reference information. Even though our schemes are based on a master key, no master key needs to be stored in biometric sensors. In our scheme it is possible to derive a polynomial number of keys from a single biometric and we show how to renew keys in a secure and private way without additional interaction with the user. Previous work considers unconditional secure key distillation which can at most reach partial (information theoretic) privacy and which can only lead to a small number of keys for each biometric.

Menu