Secure Evaluation of Hamming Distance

Superviser: David Pointcheval (contact: David.Pointcheval@ens.fr)
Computer Science Department – Ecole Normale Supérieure – 75005 Paris

General Context

For biometrics, a.k.a. biometric authentication, the server checks whether the biometric sample (from the sensor) and the biometric template (in the database) match or not. However, for privacy reasons, no biometric data should be sent over a network: the sensor could try to learn the template and the server could be a dishonest one. The matching procedure should thus be run between the two parties, so that the server learns the outcome, but nothing else, and the sensor nothing at all. One could also consider the three-party setting, where there is the client (with the sensor), the authentication server (with the biometric database) and the service provider, to which the client wants to connect, but only if the authentication server grants the authorization. In this case, the service provider should not learn anything else than the outcome of the matching, while the two other parties should know their own input only: the biometric sample for the sensor, and the biometric template for the authentication server.

According to the characteristic in use (fingerprint, palm print, iris, etc), the matching procedure essentially consists in measuring the Hamming distance between the two bit-strings that encode the biometric sample and template.

Goal of the Internship

Secure multi-party computation has been initially introduced in [Bea91], and secure evaluation of Hamming distance has been dealt in several papers [JP09, BCP12], but with various security models, and never in the three-party setting (see also [AFP05]).

The goal is thus to enhance the previous constructions in various directions: in a new setting (the three-party setting), with a better security (in the universal composability framework [Can01]) or with a better efficiency (see also [ABB+13]).

Expected Skills

We are looking for candidates with good skills in algorithmics and complexity theory. Provable security for cryptographic protocols (as one can get in courses 2.12.1 and 2.30 of the MPRI) will be the basis of this internship.

Internship

The internship will be within the Crypto Team (see http://www.di.ens.fr/CryptoTeam.html) at ENS, allowing interactions with all the members of the group, and the opportunity to participate to many seminars and reading groups.

This internship may also lead to a PhD thesis on privacy.
References


