

Vers des systèmes de reconnaissance biométrique respectueux de la vie privée

PRIVABIO

anr ©
agence nationale
de la recherche

Appel : ANR AAPG 2020

Année : 2021 (fin du projet : 2025)

Instrument : JCJC

Contact : kevin.atighehchi@gmail.com

COORDINATEUR : Kevin Atighehchi

Résumé :

Avec le déploiement à grande échelle des technologies basées sur la biométrie, les bases de données et les dispositifs biométriques deviennent des cibles naturelles de cyber-attaques. Ce projet permettra de développer une meilleure compréhension de la sécurité de ces systèmes pour proposer des approches plus performantes et plus respectueuses de la vie privée.

CONTEXTE ET OBJECTIFS

L'objectif est de remédier aux problèmes de sécurité et de confidentialité liés à l'utilisation de la biométrie, en proposant des protocoles peu gourmands en ressources et offrant des garanties de sécurité adaptées à la sensibilité de ces données personnelles. PRIVABIO est divisé en 4 axes :

- Evaluer la sécurité des schémas de protection des modèles biométriques (BTP) et des protocoles biométriques
- Fournir des schémas BTP plus sûrs sans dégrader la précision de reconnaissance et sans compromettre leur utilisation sur des dispositifs aux ressources limitées
- Identifier les mécanismes cryptographiques présentant un intérêt pour les aspects liés à la protection de la vie privée
- Intégrer les mécanismes biométriques et cryptographiques dans des protocoles d'authentification multi-facteurs et dans des protocoles d'identification, en fournissant des garanties formelles de sécurité

MÉTHODOLOGIE ET RÉSULTATS

Outils et méthodes :

- Preuves ZK
- Calcul multiparties sécurisé
- Biométrie
- Réductions de sécurité
- Statistique et machine learning
- Prototypage Python

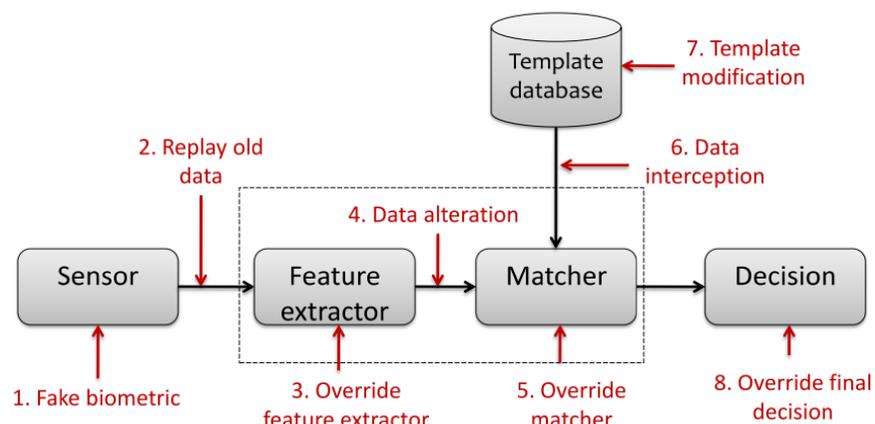
Retombées :

- Stimulation de la recherche :
 - Mise à disposition des implémentations
 - Soumission des schémas de reconnaissance biométrique aux programmes d'évaluation (ex. FVC-onGoing)
 - Publications
- Moins de résistance du public en matière de prise d'empreintes
- Diminution du coût d'une compromission de BD biométrique

MODALITÉS MORPHOLOGIQUES CONSIDÉRÉES



POINTS D'ATTAQUE D'UN SYSTÈME BIOMÉTRIQUE



CHRONOLOGIE DES WORKPACKAGES

