PRIVABIO : Vers des systèmes de reconnaissance biométrique respectueux de la vie privée

Paul-Marie Grollemund[2], Pascal Lafourcade[1], and Kevin Thiry-Atighehchi[1]

[1]Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS, France
[2]Université Clermont-Auvergne, CNRS, LMBP, France

***Résumé*—Le projet PRIVABIO[1] est financé par l'ANR grâce à l'instrument JCJC (Jeunes Chercheuses et Jeunes Chercheurs). L'objectif du projet est de développer par une recherche scientifique amont[2] une meilleure compréhension de la sécurité des systèmes biométriques afin de proposer des approches plus performantes et plus respectueuses de la vie privée. Ce projet a débuté en 2021 et se termine en 2025. Dans cette presentation pour la conférence RESSI, nous décrivons la problématique, l'organisation du projet et les pistes exploratoires.**

I. Introduction

Avec un usage répandu de la biométrie, les bases de données et les dispositifs biométriques deviennent des cibles naturelles de cyber-attaques. L'objectif du projet est de remédier aux problèmes de sécurité et de confidentialité liés à l'utilisation de la biométrie. Pour cela, nous envisagons de proposer des protocoles peu gourmands en ressources Tet offrant des garanties de sécurité adaptées à la sensibilité de ces données personnelles. PRIVABIO est divisé en 4 axes :

- **(WP1)** Evaluer la sécurité des schémas de protection des modèles biométriques (BTP) et des protocoles biométriques, incluant les standards (FIDO [1], BOPS [2]). La figure 1 présente les possibles points d'attaque d'un système biométrique générique (Modèle de Ratha [3]).
- **(WP2*a*)** Fournir des schémas BTP plus sûrs sans dégrader la précision de reconnaissance et sans compromettre leur utilisation sur des dispositifs aux ressources limitées.
- **(WP2*b*)** Identifier les mécanismes cryptographiques présentant un intérêt pour les aspects liés à la protection de la vie privée.
- **(WP3)** 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.

La figure 2 présente la chronologie des workpackages.

II. Méthodologie et retombées

Les outils et méthodes mobilisées dans ce projet comprennent le calcul multiparties sécurisé, les preuves à divulgation nulle de connaissance, la biométrie, les statistiques, le machine learning, les méthodes formelles de preuve de sécurité, et le langage de programmation Python pour les expérimentations.

1. Numéro de projet : ANR-20-CE39-0005 https://privabio.limos.fr
2. Niveaux de TRL 1 à 3

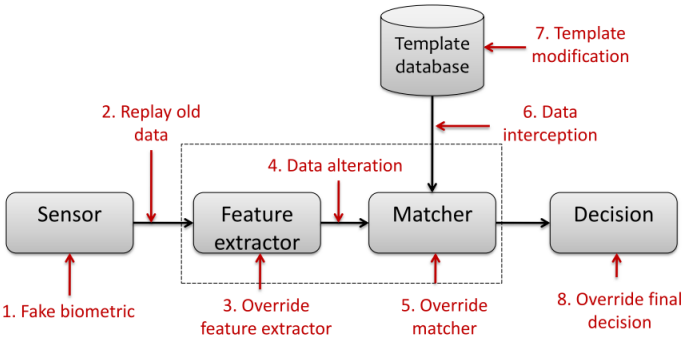

Figure 1. Possibles points d'attaque d'un système biométrique.

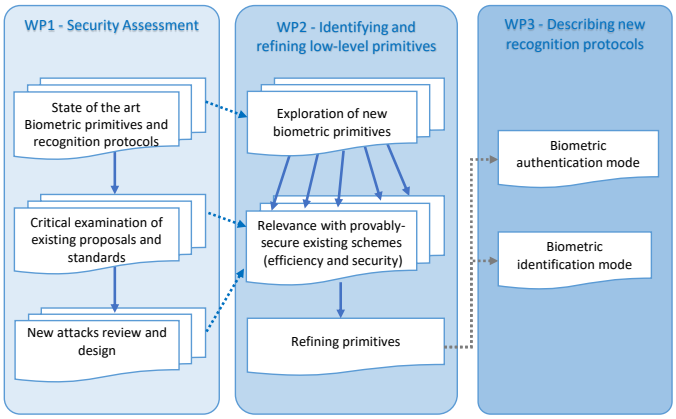

Figure 2. Liens entre les tâches.

Le respect de la vie privée est un droit fondamental mis en œuvre par le biais du RGPD. Ce projet contribuera à la fois à la sécurité des solutions biométriques et à l'application technique de ce droit fondamental. Les retombées attendues sont multiples : une étude des propriétés de sécurité attendues, la conception de protocoles d'authentification et d'identification vérifiant ces propriétés, la mise à disposition de la communauté scientifique de nos résultats et logiciels, la soumission des schémas de reconnaissance biométrique aux programmes d'évaluation (ex. FVC-onGoing), et enfin le développement d'un réseau de partenaires pour de futurs projets.

Références

[1] FIDO Alliance. [Online]. Available : https://fidoalliance.org/overview/
[2] "IEEE Standard for Biometric Open Protocol - Redline," *IEEE Std 2410-2019 (Revision of IEEE Std 2410-2017) - Redline*, pp. 1–134, 2019.
[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *AVBPA*, 2001.