On the Issues of Fuzzy Vault and Private Set Intersection Based Biometric Protocol

Axel DURBET and Kévin THIRY-ATIGHEHCHI

Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS France

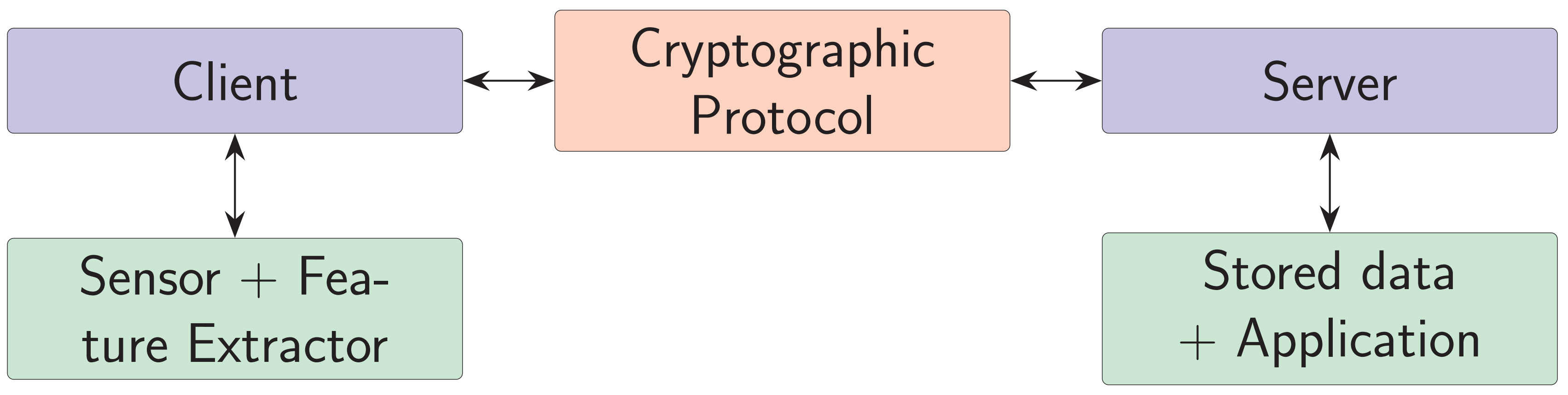
Objectives

1. Describe and popularize the construction of Fuzzy Vault for biometric usage.
2. Highlighting the open problems associated with this usage.
3. Propose solutions to patch those issues.

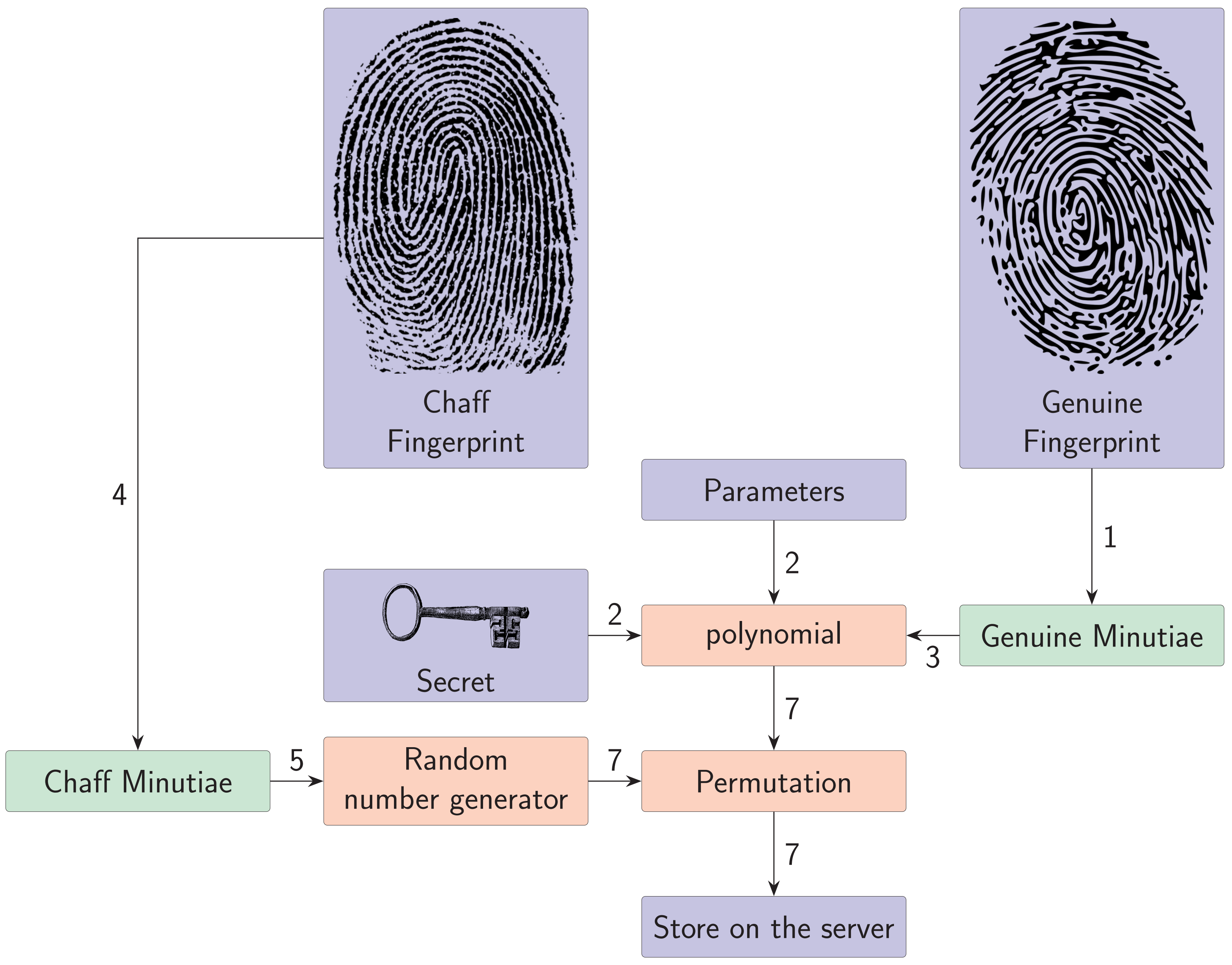
Introduction

- Wide use of biometric authentication (smartphones and laptops).
- More convenient and quicker.
- Biometric features cannot be lost or forgotten.
- Minutiae point are sensitive data and must remain secret.
- Biometric protocol must fulfil the ISO/IEC 30136 properties.

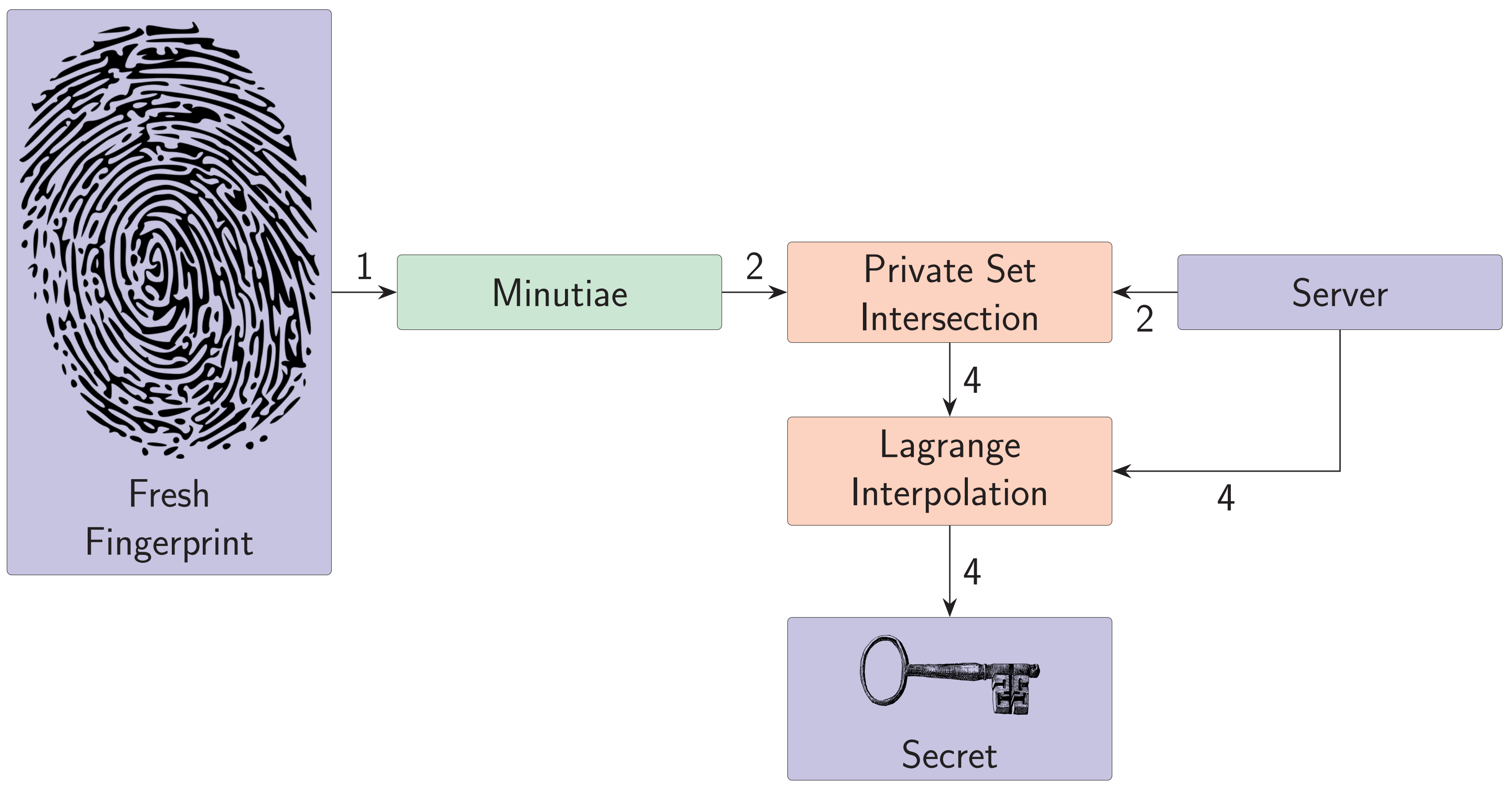
Online Biometric System Representation



FV_{Gen}: Fuzzy Vault Generation Illustrated



FV_{Open}: Fuzzy Vault Secret Recovery Illustrated



Shamir's Secret Sharing

Let $s \in \mathbb{F}_q$ be the secret, q a prime number, $n \ll q$ the number of participants and $k \leq n$ the minimum number of shares needed to find s. Then, the secret sharing proceeds as follows:

1. A polynomial $f \in \mathbb{F}_q[x]$ of degree $k - 1$ is drawn at random such that $f(0) = s$.
2. We draw n points p_i pairwise distinct and different from 0.
3. The i-th participant receives his share of the secret $D_i = (p_i, f(p_i))$.

For the reconstruction of the secret, we proceed as follows:

1. k users pool their contributions D_i.
2. With the D_i, they compute $f(x)$ using Lagrange interpolation.
3. They find the secret $s = f(0)$.

Fuzzy Vault Mathematical Construction

- FV_{Gen}:
  1. Read the biometric data and extract the informations $BT = (b_1, \dots, b_m)$ such that $\forall (i, j); i \neq j, dist(b_i, b_j) > w$.
  2. Choose a random secret k and draw a polynomial $f \in \mathbb{F}_q$ of degree $d - 1$ such that $f(0) = k$.
  3. Evaluate the b_i with f as in Shamir's Secret Sharing.
  4. Draw randomly $CP = (r_1, \dots, r_n)$ the chaff points such that $\forall (i, j), dist(b_i, r_j) > w$ and such that the r_i are indistinguishable from b_i.
  5. Evaluate the r_i with a random function f'.
  6. Let the data $D = ((b_1, f(b_1)), \dots, (b_m, f(b_m)), (r_1, f'(r_1)), \dots, (r_n, f(r_n)))$.
  7. Choose P a random permutation and set the helping data $HD = P(D)||H(k)$.
- FV_{OPEN}:
  1. Read the fresh biometric data $BT' = (b'_1, \dots, b'_m)$ and get the helping value HD.
  2. For each index j such that $dist(\overline{b}_i, b'_j) \leq w$, get $(\overline{b}_i, f(\overline{b}_i))$ with $\overline{b}_i = r_i$ or b_i.
  3. If BT and BT' are close enough, at least d couples are corrects.
  4. For each subset of d couples, perform the Lagrange interpolation as in SSS to get $f(x)$ and verify it by testing $H(f(0)) = H(k)$.

Related issue

1. Extract enough well distinct minutiae.
2. Generation of chaff points indistinguishable from real minutia.
3. Linkability of templates on several services if the servers are collaborating.
4. Handling several distance metrics for different biometric modalities.
5. Multiple interpolations make the protocol impractical for large vectors or large threshold.
6. Good preservation of the recognition accuracy.
7. Intersection attack by collaborating servers.

Idea to patch the issue

- For 2: Use a Generative Adversarial Network (GAN).
- For 3 and 7: Introduce variability on the minutia with a salted hash function.
- For 4: Use an error correcting code (LWE).

Acknowledgments

- The authors acknowledges the support of the French Agence Nationale de la Recherche (ANR), under grant ANR-20-CE39-0005 (project PRIVABIO).

Contact Information

- Web: PRIVABIO Project on: https://privabio.limos.fr/
- Email: axel.durbet@uca.fr or kevin.atighehchi@uca.fr