# Private Fingerprint Matching

**Siamak F Shahandashti**
Reihaneh Safavi-Naini
Philip Ogunbona

Uni of Wollongong & Uni of Calgary

ACISP 2012

- Usage of **biometrics** (esp. **fingerprints**) for authentication increasing rapidly

- Usage of **biometrics** (esp. **fingerprints**) for authentication increasing rapidly
- System heart: **fingerprint matching algorithm**

# Fingerprint Matching: from Algorithm to Private Protocol

- Usage of **biometrics** (esp. **fingerprints**) for authentication increasing rapidly
- System heart: **fingerprint matching algorithm**
- Often 2 fingerprints held by 2 separate entities not willing to share unnecessary information

# Fingerprint Matching: from Algorithm to Private Protocol

- Usage of **biometrics** (esp. **fingerprints**) for authentication increasing rapidly
- System heart: **fingerprint matching algorithm**
- Often 2 fingerprints held by 2 separate entities not willing to share unnecessary information
- Hence, a need for protocols that enable 2 parties decide if their fingerprints match without revealing any further info

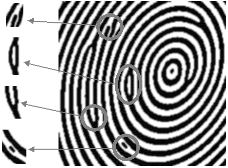
# Fingerprint Matching: from Algorithm to Private Protocol

- Usage of **biometrics** (esp. **fingerprints**) for authentication increasing rapidly
- System heart: **fingerprint matching algorithm**
- Often 2 fingerprints held by 2 separate entities not willing to share unnecessary information
- Hence, a need for protocols that enable 2 parties decide if their fingerprints match without revealing any further info
- Let's call it a **private fingerprint matching protocol**

The most widely-used method for fingerprint matching [HFR]:

- extraction of features called **minutiae**,
- comparing them based on their **types**, **locations**, and **orientations**, and
- deciding based on the number of matching pairs of minutiae

$$F = \{p_1, \ldots, p_n\}$$
$$p_i = (t_i, x_i, y_i, \theta_i)$$



[Keogh'01]

# Previous Works vs. Ours

Shortcomings of previous works:

- **Over-simplification**
  - Private Hamming distance calculation
- **Under-performance**
  - Private matching as images, e.g. FingerCode
- **Genericness**
  - Private matching based on generic multiparty computation

# Previous Works vs. Ours

Shortcomings of previous works:

- **Over-simplification**
  - Private Hamming distance calculation
- **Under-performance**
  - Private matching as images, e.g. FingerCode
- **Genericness**
  - Private matching based on generic multiparty computation

Our proposal:

- **concrete** private protocol for **full minutiae matching** method

# Previous Works vs. Ours

Shortcomings of previous works:

- **Over-simplification**
  - Private Hamming distance calculation
- **Under-performance**
  - Private matching as images, e.g. FingerCode
- **Genericness**
  - Private matching based on generic multiparty computation

Our proposal:

- **concrete** private protocol for **full minutiae matching** method using homomorphic encryption

$$\mathsf{E}(a+b) = \mathsf{E}(a) \oplus \mathsf{E}(b)$$

# Main Idea

Homomorphic encryption enables the computation of $\mathrm{E}\left(P(x)\right)$ from $\mathrm{E}(x)$ through interaction with the holder of the decryption key:

- Calculate $\mathrm{E}\left(rx\right)$ and send
- Decrypt, calculate $\left\{(rx)^i\right\}$, encrypt again to $\mathrm{E}\left((rx)^i\right)$ and send
- Calculate $\mathrm{E}\left(P(x)\right)$ using $\mathrm{E}\left((rx)^i\right)$

Define the following polynomials via Lagrange interpolation:

- $Q_i(t_j)$ equals 0 if $t_j = t_i$ and 1 otherwise
- $Q_{\mathrm{E}}(d_{ij}^2)$ equals 0 if $d_{ij}$ is less than the threshold and 1 otherwise
- $Q_{\mathrm{a}}(\gamma_{ij})$ equals 0 if $\gamma_{ij}$ is less than the threshold and 1 otherwise

A party receiving an encrypted version of the minutiae of the other party

# The Protocol Flow

Define the following polynomials via Lagrange interpolation:

- $Q_i(t_j)$ equals 0 if $t_j = t_i$ and 1 otherwise
- $Q_{\mathrm{E}}(d_{ij}^2)$ equals 0 if $d_{ij}$ is less than the threshold and 1 otherwise
- $Q_{\mathrm{a}}(\gamma_{ij})$ equals 0 if $\gamma_{ij}$ is less than the threshold and 1 otherwise

A party receiving an encrypted version of the minutiae of the other party can compute the encrypted versions of the above polynomials

# The Protocol Flow

Define the following polynomials via Lagrange interpolation:

- $Q_i(t_j)$ equals 0 if $t_j = t_i$ and 1 otherwise
- $Q_{\mathrm{E}}(d_{ij}^2)$ equals 0 if $d_{ij}$ is less than the threshold and 1 otherwise
- $Q_{\mathrm{a}}(\gamma_{ij})$ equals 0 if $\gamma_{ij}$ is less than the threshold and 1 otherwise

A party receiving an encrypted version of the minutiae of the other party can compute the encrypted versions of the above polynomials and sum them up to compute an encryption of

$$z_{ij} = Q_i(t_j) + Q_{\mathrm{E}}(d_{ij}^2) + Q_{\mathrm{a}}(\gamma_{ij})$$

# The Protocol Flow (cont'd)

Similarly, define the following polynomials via Lagrange interpolation:

- $R(z_{ij})$ equals 1 if $z_{ij} = 0$ and 0 otherwise

Then an encryption of $R(z_{ij})$ can be calculated which is 1 if $p_i$ and $p_j$ match.

# The Protocol Flow (cont'd)

Similarly, define the following polynomials via Lagrange interpolation:

- $R(z_{ij})$ equals 1 if $z_{ij} = 0$ and 0 otherwise

Then an encryption of $R(z_{ij})$ can be calculated which is 1 if $p_i$ and $p_j$ match.

Then an encryption of the count of minutiae matchings can be calculated and thresholded similarly and we are done!

# Security and Practicality

Full privacy against honest-but-curious adversaries proven

# Security and Practicality

Full privacy against honest-but-curious adversaries proven
Full privacy against malicious adversaries achievable via standard techniques

# Security and Practicality

Full privacy against honest-but-curious adversaries proven
Full privacy against malicious adversaries achievable via standard techniques

Typical fingerprints can be compared at the expense of around a hundred encryptions.

# Security and Practicality

Full privacy against honest-but-curious adversaries proven
Full privacy against malicious adversaries achievable via standard techniques

Typical fingerprints can be compared at the expense of around a hundred encryptions.

Full paper: `eprint.iacr.org/2012/219`