Secure Computation of Fingerprint Alignment and Matching
Fattaneh Bayatbabolghani, Marina Blanton
Department of Computer Science and Engineering, University of Notre Dame

Motivation
- Fingerprint images are one of the most accurate type of biometry used in biometric verification and identification.
- Fingerprint images are highly sensitive due to their ability to uniquely identify the data owner.

Goals
- To build secure protocols for fingerprint alignment (first time) and matching based on the most precise or efficient algorithms in the biometric literature.
- To develop secure computation techniques based on garbled circuit evaluation and linear secret sharing.

Building Security Solutions
- Standard Building Blocks such as addition/subtraction, multiplication, comparison, and compaction.
- More complicated building blocks such as division, square root (new for secure two-party computation), sine (totally new), and cosine (totally new).

Fingerprint Recognition
- Fingerprint matching based on minutiae alignment: Consider all possible alignments between two fingerprint images S and T and select the alignment that maximizes the matching score.
  \[ \text{Matching score} = \frac{\#\text{matched minutiae points}}{\#\text{minutiae points}_S \times \#\text{minutiae points}_T} \]
- Fingerprint matching based on trimmed iterative closest point algorithm: Align two sets of 3-D points of helper data S and T based on trimmed iterative closest point (TICP) to find matching score.
- Fingerprint matching based on spectral minutiae representation: Modify the representation of minutiae points by using Fourier transform and then reduce feature size to make recognition process faster without losing precision. At the end, consider different alignment and compute similarity score.

Extracted Features
- Minutia point
- Core Point
- Helper data

This work was supported by grant CNS-1223699 from the National Science Foundation.