# Master Thesis

## PSI Meets Signal: Integrating a Malicious-Secure Private Contact Discovery Solution in an Open-Source Instant Messaging Service

TECHNISCHE UNIVERSITÄT DARMSTADT

The *Engineering Cryptographic Protocols Group* (ENCRYPTO) is offering a master thesis that will be supervised by Christian Weinert (christian.weinert@crisp-da.de) and Dr. Thomas Schneider.

### Motivation

The term *contact discovery* in the context of mobile instant messaging refers to the task of determining which contacts in a client's address book, identified by their phone numbers, are registered at the same messaging service. Because of privacy concerns, one might prefer to not simply share all contacts with the service provider in order to compute the intersection.

A naive solution to this *private set intersection* (PSI) problem is sending the phone numbers in hashed form. Unfortunately, this is inherently insecure as brute-force and dictionary attacks allow to easily recover such low entropy values. Also, there is no forward-secrecy in the sense that after the protocol execution the service provider can test new values later-on without the client's permission.

The developers of Signal, an open-source instant messenger for encrypted communication, considered employing encrypted bloom filters[1], but this approach turned out to be unfeasible due to the requirement of sending ∼40 MB to each client for a database of 10 million users.

Thus, the current situation seems anything but satisfying: widely-used messenger services take none or insufficient measures to protect their customers' privacy as the scientific community fails to provide practical solutions for private contact discovery.

### Goal

The overall goal of this thesis is to develop a practical PSI solution for private contact discovery and to integrate it in the Signal server as well as the corresponding Android application.

As a first step, to support our motivation, popular Android instant messengers should be analyzed with respect to their currently used contact discovery procedure. This survey is expected to be performed by analyzing code, protocol specifications, and network traffic, as well as by contacting the responsible developers.

A recent review of different PSI protocols operating on unequal set sizes in the mobile setting suggests that obliviously evaluating garbled AES circuits in order to compare encrypted values offers the best trade-off between communication and computational complexity. Whereas this review conducts a performance evaluation based on comparatively slow Java implementations, a goal of this thesis is to port ABY[2], a state-of-the-art framework for secure multi-party computation written in C/C++, to the ARM architecture and then integrate it into the Android application using the Android NDK and the server implementation using JNI.

Whenever deploying applications large-scale, it must be assumed that there are malicious clients trying to learn additional information from the server by deviating from the actual protocol. When using a garbled circuit based protocol, this can be mitigated by employing a malicious-secure instead of a semi-honest OT extension protocol. Therefore, an existing malicious-secure OT extension library, such as libOTe[3], should be combined with the ABY garbled circuit implementation.

Finally, while evaluating the performance, possibilities of reducing the necessary communication at the cost of minimal information leakage should be investigated, e.g. database partitioning/sharding and adjusting protocol parameters according to the client's set size. Completing several optional tasks, such as implementing circuit optimized PRFs instead of AES, exploiting parallelism, and using GMW instead of Yao's circuit evaluation protocol could further improve performance.

### Requirements

- Good programming skills in C/C++, at least basic programming skills in Android/Java
- At least basic knowledge of cryptography and statistics
- High motivation + ability to work independently
- Knowledge of the English language, Git, LaTeX, etc. goes without saying

1 https://whispersystems.org/blog/contact-discovery/
2 https://github.com/encryptogroup/ABY
3 https://github.com/osu-crypto/libOTe