ELEC 599 Project Abstract and Timeline

Student: Mohammad Sadegh Riazi
Advisor: Prof. Farinaz Koushanfar
Date: January 16, 2015

Privacy-Preserving Matching

Abstract: In several scenarios, there is a need to match a query against a dataset, where the query/dataset belongs to different parties and each of them requires keeping their own data private. The importance of this requirement arises in many various areas, e.g., medical history and criminal data. A frequent application of privacy-preserving scenario is matching. For example, Alice wants to find if she has a genetic disorder by matching her genome information with Bob's genetic disorder bank. But she doesn't want to reveal her private information and so does Bob.

This project aims to address the privacy-preserving matching using Yao's Garbled Circuit (GC) protocol. GC protocol has shown to be the most efficient secure two party computation approach. This protocol allows two parties to evaluate a function which is described as a Boolean circuit on their private data. This project objective is to study the applicability of GC-based privacy preserving protocols on real benchmarks and optimize its performance for real application on embedded or reconfigurable devices.

Keywords: Privacy-preserving computing, garbled circuits, secure multiparty computation, Yao's protocol.

Timeline:

Time	Task
Week 1&2 January 16-31	Literature review
Week 3&4 February 1-15	Implementation of Garbled Circuits
Week 5&6 February 16-28	Formulating the matching in the GC framework
Week 7&8 March 1-15	Logic level description of the matching problem
Week 9&10 March 16-31	Optimization of the secure communication via Oblivious Transfer
Week 11&12 April 1-15	End-to-end implementation
Week 13 April 16-24	Evaluation and report
Week 14 April 24-30	Final presentation