Efficient Server-Aided Secure Two-Party Function Evaluation with Applications to Genomic Computation

Marina Blanton, Fattaneh Bayatbabolghani

Department of Computer Science and Engineering, University of Notre Dame

Motivation

- ❑ Genomic data is used in medical domain and other applications (e.g., ancestry, paternity, genomic compatibility testing).
- ❑ Genomic data is highly sensitive; it discloses information about data owner, as well as owner's relatives.

Goals

- ❑ To develop secure computation techniques for malicious and semi-honest users based on garbled circuit evaluation.
- ❑ To decrease computational overhead of two parties by adding a server with sufficient computational power.

Preliminaries of Genomic Testing

- ❑ Genomes represent complete hereditary information of an individual. Information extracted from one's genome is often represented as SNPs and STRs.
- ❑ Three common genomic tests:
  - ✓ **Ancestry**: We compare two SNP sequences belonging to two individuals to determine the number of SNPs they have in common.
  - ✓ **Paternity with a Single Parent**: There are two STR profiles $S = \langle \{x_{1,i}, x_{2,i}\} \rangle$ and $S' = \langle \{x'_{1,i}, x'_{2,i}\} \rangle$ and the test computes: $\wedge_{i=1}^{N} [\{x_{1,i}, x_{2,i}\} \cap \{x'_{1,i}, x'_{2,i}\}] = True$
  - ✓ **Genetic Compatibility**: We compare marked SNPs of parents to evaluate the possibility of their children inheriting at least one recessive genetic disease.

Garbled Circuits

- ❑ Garbled circuits allows two parties P_1 and P_2 to securely evaluate a Boolean circuit of their choice.

Desired function should be converted to a Boolean circuit and then:

- ➢ One party acts as a circuit generator and creates a garbled representation of the circuit by associating both values of each binary wire with random labels.
- ➢ Another party acts as a circuit evaluator and evaluates the circuit in its garbled representation without knowing the meaning of the labels.

The output labels can be mapped to their meaning and revealed to either or both parties.

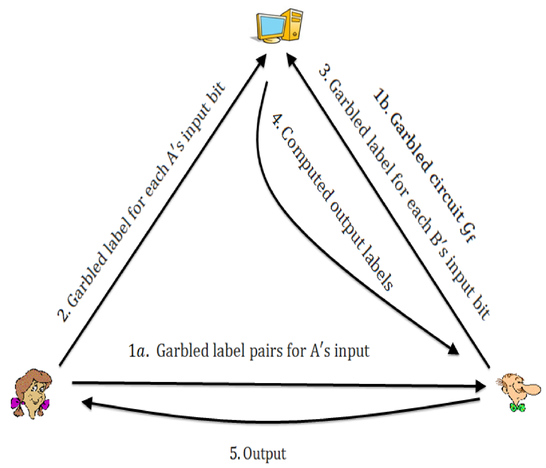
- ❑ In 1-out-of 2 oblivious transfer, sender has x_0 and x_1, and receiver obtains only x_b without revealing any information about b for sender.

Designed Protocols

1. The proposed solution for semi-honest parties and malicious server:

Both parties jointly create a garbled representation of the circuits. Then, they send the appropriate label for their input bits to the server for evaluation. Security is maintained because garbled circuit evaluation techniques are secure in presence of a malicious evaluator. At the end, the server returns the output to the parties. The parties can determine the result by mapping the output to its actual meaning.

Designed Protocols

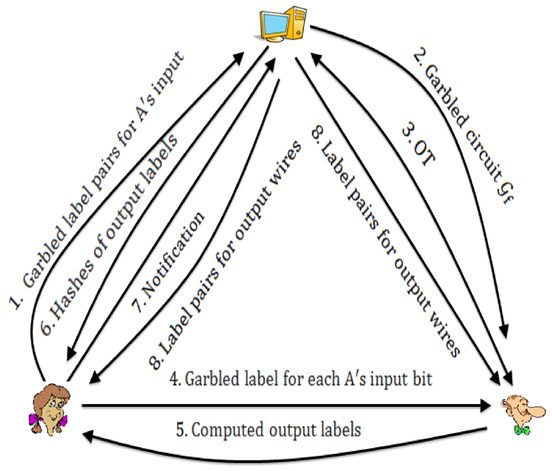


2. The protocol for semi-honest server and malicious parties:

Alice and the server jointly create a garbled representation of the circuits. Alice sends Bob her input bits and Bob is engaged by the server in oblivious transfers to find his input bits. Then Bob acts as the evaluator of garbled circuits. For completion of garbled circuit evaluation, Bob sends the computed labels to Alice. With the help of the server, Alice verifies the output labels without recognizing their meanings; Once the output labels are verified, Alice notifies the server which sends the label pairs to Alice and Bob. Both parties can therefore, interpret and learn the result.

According to this solution fairness is achieved because both parties or neither of them can learn the output.

Designed Protocols



Applications

- ❑ **Ancestry**: This test would often be invoked when two parties already know to be related or have reasons to believe to be related. Thus, they are unlikely to try to cheat each other. For that reason, we use the solution with semi-honest parties to perform this test.
- ❑ **Paternity**: We assessed that the security setting with malicious users is the most suitable for running paternity tests. That is, the participants may be inclined to tamper with the computation to influence the result.
- ❑ **Genetic Compatibility**: We added input certification to the security setting with malicious users because one party may modify the input to learn other party's genetic information.

Conclusion

- ❑ We developed general secure solutions in our server-aided framework with several applications in genomic testing, and other domains.
- ❑ Running time of all of our experiments indicate execution efficiency of the protocols.

"This work was supported by grants CNS-1223699 from the National Science Foundation"