Cryptology ePrint Archive: Report 2011/663

Cloud-Assisted Multiparty Computation from Fully Homomorphic Encryption

Adriana Lopez-Alt and Eran Tromer and Vinod Vaikuntanathan

Abstract: We construct protocols for secure multiparty computation with the help of a computationally powerful party, namely the "cloud". Our protocols are simultaneously efficient in a number of metrics:

* Rounds: our protocols run in 4 rounds in the semi-honest setting, and 5 rounds in the malicious setting.

* Communication: the number of bits exchanged in an execution of the protocol is independent of the complexity of function f being computed, and depends only on the length of the inputs and outputs.

* Computation: the computational complexity of all parties is independent of the complexity of the function f, whereas that of the cloud is linear in the size of the circuit computing f.

In the semi-honest case, our protocol relies on the ``ring learning with errors'' (RLWE) assumption, whereas in the malicious case, security is shown under the Ring LWE assumption as well as the existence of simulation-extractable NIZK proof systems and succinct non-interactive arguments. In the malicious setting, we also relax the communication and computation requirements above, and only require that they be ``small'' -- polylogarithmic in the computation size and linear in the size of the joint size of the inputs.

Our constructions leverage the key homomorphic property of the recent fully homomorphic encryption scheme of Brakerski and Vaikuntanathan (CRYPTO 2011, FOCS 2011). Namely, these schemes allow combining encryptions of messages under different keys to produce an encryption (of the sum of the messages) under the sum of the keys. We also design an efficient, non-interactive threshold decryption protocol for these fully homomorphic encryption schemes.

Category / Keywords:

Date: received 7 Dec 2011

Contact author: lopez at cs nyu edu