Cryptology ePrint Archive: Report 2011/613

Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE

Gilad Asharov and Abhishek Jain and Daniel Wichs

Abstract: Fully homomorphic encryption (FHE) provides a simple template for secure computation between two parties (Alice and Bob) where: (I) Alice encrypts her input under her key, (II) Bob homomorphically evaluates the desired function on Alice's ciphertext and his own input, and sends the encrypted output to Alice. Extending this approach to multiple parties raises the problem of which key to encrypt under; if all parties choose a key on their own, then homomorphic evaluation on ciphertexts under di erent keys will not be possible, and if a single party chooses the key for everyone then corrupting this party will break privacy for all.

In this work, we explore the option of using threshold fully homomorphic encryption (TFHE), allowing many parties to cooperatively generate a common public key whose secret key is shared/distributed among them. Moreover, the parties can cooperatively decrypt a ciphertext without learning anything but the plaintext. We show how to instantiate this approach e ciently using the recent FHE schemes of Brakerski et al. (FOCS '11, ITCS '12) based on the learning with errors (LWE) assumption. Our main tool is to exploit the property that such LWE-based encryption schemes are homomorphic over their keys. Using TFHE, we construct multiparty computation (MPC) protocols secure against fully malicious settings, tolerating any number of corruptions, and providing security in the universal composability framework.

Our schemes have several benefits fits over prior templates for MPC.

Interaction: We get protocols with only 3 rounds of interaction in the common random string model, or 2 rounds with a reusable public-key infrastructure, improving on prior known results.

Communication: The communication in our protocol is only proportional to the input and output size of the function being evaluated and independent of its circuit size.

Computation: The only computation that depends on the size of the circuit being computed is a homomorphic evaluation over public ciphertexts. This computation can be performed by a single party or can be outsourced to an external server.

Novel Approach: Prior approaches to MPC with a dishonest majority rely in part on some combination of the techniques of Yao (FOCS '86) and/or Goldreich, Micali and Wigderson (STOC '87). Our approach is fundamentally different and relies only on the homomorphic properties of LWE-based encryption.

Category / Keywords: public-key cryptography / fully homomorphic encryption, threshold encryption, secure multiparty computation,

Date: received 14 Nov 2011

Contact author: wichs at cs nyu edu