Cryptology ePrint Archive: Report 2013/094

On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption

Adriana Lopez-Alt and Eran Tromer and Vinod Vaikuntanathan

Abstract: We propose a new notion of secure multiparty computation aided by a computationally-powerful but untrusted "cloud" server. In this notion that we call on-the-fly multiparty computation (MPC), the cloud can non-interactively perform arbitrary, dynamically chosen computations on data belonging to arbitrary sets of users chosen on-the-fly. All user's input data and intermediate results are protected from snooping by the cloud as well as other users. This extends the standard notion of fully homomorphic encryption (FHE), where users can only enlist the cloud's help in evaluating functions on their own encrypted data.

In on-the-fly MPC, each user is involved only when initially uploading his (encrypted) data to the cloud, and in a final output decryption phase when outputs are revealed; the complexity of both is independent of the function being computed and the total number of users in the system. When users upload their data, they need not decide in advance which function will be computed, nor who they will compute with; they need only retroactively approve the eventually-chosen functions and on whose data the functions were evaluated.

This notion is qualitatively the best possible in minimizing interaction, since the users' interaction in the decryption stage is inevitable: we show that removing it would imply generic program obfuscation and is thus impossible.

Our contributions are two-fold:

1. We show how on-the-fly MPC can be achieved using a new type of encryption scheme that we call multikey FHE, which is capable of operating on inputs encrypted under multiple, unrelated keys. A ciphertext resulting from a multikey evaluation can be jointly decrypted using the secret keys of all the users involved in the computation.

2. We construct a multikey FHE scheme based on NTRU, a very efficient public-key encryption scheme proposed in the 1990s. It was previously not known how to make NTRU fully homomorphic even for a single party. We view the construction of (multikey) FHE from NTRU encryption as a main contribution of independent interest. Although the transformation to a fully homomorphic system deteriorates the efficiency of NTRU somewhat, we believe that this system is a leading candidate for a practical FHE scheme.

Category / Keywords:

Publication Info: An extended abstract of this work appeared in the proceedings of Symposium on Theory of Computing - STOC 2012. This is the full version.

Date: received 20 Feb 2013, last revised 21 Feb 2013

Contact author: lopez at cs nyu edu