Cryptology ePrint Archive: Report 2013/198

On Evaluating Circuits with Inputs Encrypted by Different Fully Homomorphic Encryption Schemes

Zhizhou Li and Ten H. Lai

Abstract: We consider the problem of evaluating circuits whose inputs are encrypted with possibly different encryption schemes. Let $\mathcal{C}$ be any circuit with input $x_1, \dots, x_t \in \{0,1\}$, and let $\mathcal{E}_i$, $1 \le i \le t$, be (possibly) different fully homomorphic encryption schemes, whose encryption algorithms are $\Enc_i$. Suppose x_i is encrypted with $\mathcal{E}_i$ under a public key pk_i, say $c_i \leftarrow \Enc_i({pk_i}, x_i)$. Is there any algorithm $\Evaluate$ such that $\Evaluate(\mathcal{C}, \langle \mathcal{E}_1, pk_1, c_1\rangle, \dots, \langle \mathcal{E}_t, pk_t, c_t\rangle)$ returns a ciphertext c that, once decrypted, equals $\mathcal{C}(x_1, \dots, x_t)$? We propose a solution to this seemingly impossible problem with the number of different schemes and/or keys limited to a small value. Our result also provides a partial solution to the open problem of converting any FHE scheme to a multikey FHE scheme.

Category / Keywords: foundations / Fully Homomorphic Encryption, Multi-Scheme FHE, Trivial Encryptions, Ciphertext Trees, Multiparty Computations.

Publication Info: under review in a iacr conference.

Date: received 6 Apr 2013

Contact author: lizh at cse ohio-state edu, lai@cse ohio-state edu