Cryptology ePrint Archive: Report 2012/733

Succinct Functional Encryption and Applications: Reusable Garbled Circuits and Beyond

Shafi Goldwasser and Yael Kalai and Raluca Ada Popa and Vinod Vaikuntanathan and Nickolai Zeldovich

Abstract: Functional encryption is a powerful primitive: given an encryption $\Enc(x)$ of a value x and a secret key $\sk_f$ corresponding to a circuit f, it enables efficient computation of $f(x)$ without revealing any additional information about x. Constructing functional encryption schemes with succinct ciphertexts that guarantee security for even a single secret key (for a general function f) is an important open problem with far reaching applications, which this paper addresses.

Our main result is a functional encryption scheme \textit{for any general function f of depth d, with succinct ciphertexts} whose size grows with the depth d rather than the size of the circuit for f. We prove the security of our construction based on the intractability of the learning with error (LWE) problem. More generally, we show how to construct a functional encryption scheme from \textit{any} public-index predicate encryption scheme and fully homomorphic encryption scheme.

Previously, the only known constructions of functional encryption were either for specific inner product predicates, or for a weak form of functional encryption where the ciphertext size grows with the size of the circuit for f.

We demonstrate the power of this result, by using it to construct a \textit{reusable circuit garbling scheme with input and circuit privacy}: an open problem that was studied extensively by the cryptographic community during the past 30 years since Yao's introduction of a one-time circuit garbling method in the mid 80's. Our scheme also leads to a new paradigm for general function obfuscation which we call token-based obfuscation. Furthermore, we show applications of our scheme to homomorphic encryption for Turing machines where the evaluation runs in input-specific time rather than worst case time, and to publicly verifiable and secret delegation.

Category / Keywords: functional encryption

Date: received 31 Dec 2012

Contact author: ralucap at mit edu