Cryptology ePrint Archive: Report 2011/454

Threshold Fully Homomorphic Encryption and Secure Computation

Steven Myers and Mona Sergi and abhi shelat

Abstract: Cramer, Damg\r{a}rd, and Nielsen~\cite{CDN01} show how to construct an efficient secure multi-party computation scheme using a threshold homomorphic encryption scheme that has four properties i) a honest-verifier zero-knowledge proof of knowledge of encrypted values, ii) proving multiplications correct iii) threshold decryption and iv) trusted shared key setup. Naor and Nissim~\cite{NN01a} show how to construct secure multi-party protocols for a function f whose communication is proportional to the communication required to evaluate f without security, albeit at the cost of computation that might be exponential in the description of f.

Gentry~\cite{Gen09a} shows how to combine both ideas with fully homomorphic encryption in order to construct secure multi-party protocol that allows evaluation of a function f using communication that is {\bf independent of the circuit description of f} and computation that is polynomial in $|f|$. This paper addresses the major drawback's of Gentry's approach: we eliminate the use of non-black box methods that are inherent in Naor and Nissim's compiler.

To do this we show how to modify the fully homomorphic encryption construction of van Dijk et al.~\cite{vDGHV10} to be threshold fully homomorphic encryption schemes. We directly construct (information theoretically) secure protocols for sharing the secret key for our threshold scheme (thereby removing the setup assumptions) and for jointly decrypting a bit. All of these constructions are constant round and we thoroughly analyze their complexity; they address requirements (iii) and (iv). The fact that the encryption scheme is fully homomorphic addresses requirement (ii).

To address the need for an honest-verifier zero-knowledge proof of knowledge of encrypted values, we instead argue that a weaker solution suffices. We provide a 2-round blackbox protocol that allows us to prove knowledge of encrypted bits. Our protocol is not zero-knowledge, but it provably does not release any information about the bit being discussed, and this is sufficient to prove the correctness of a simulation in a method similar to Cramer et al.

Altogether, \emph{we construct the first black-box secure multi-party computation protocol that allows evaluation of a function f using communication that is independent of the circuit description of f}.

Category / Keywords: Fully Homomorphic Encryption, Threshold Encryption, Secure Multi-Party Communication, Communication and Round Complexity, Proof Of Knowledge

Date: received 18 Aug 2011, last revised 21 Aug 2011

Contact author: ms4bf at virginia edu