Cryptology ePrint Archive: Report 2011/069

Constant-Rounds, Linear Multi-party Computation for Exponentiation and Modulo Reduction with Perfect Security

Chao Ning and Qiuliang Xu

Abstract: Bit-decomposition is an important primitive in multi-party computation (MPC). Given a sharing of secret x, it allows the parties to compute the sharings of the bits of x in constant rounds. With the help of bit-decomposition, we will be able to construct constant-rounds protocols for various MPC problems, such as \emph{equality test}, \emph{comparison}, \emph{public modulo reduction} and \emph{private exponentiation}, which are four main applications of bit-decomposition. However, when considering perfect security, bit-decomposition does \emph{not} have a linear communication complexity. Thus any protocols involving bit-decomposition inherit this inefficiency, i.e. the communication complexity is non-linear. Constructing protocols for MPC problems without relying on bit-decomposition is a meaningful work because this may provide us with perfect secure protocols with linear communication complexity. It is already proved that \emph{equality test}, \emph{comparison} and \emph{public modulo reduction} can be solved without involving bit-decomposition and the communication complexity can be reduced to linear. However, it remains an open problem whether \emph{private exponentiation} could be done without relying on bit-decomposition. In this paper, maybe somewhat surprisingly, we show that it can. That is to say, we construct a \emph{constant-rounds, linear, perfect secure} protocol for private exponentiation \emph{without} relying on bit-decomposition though it seems essential to this problem. Compared with the previous solution for this problem (with perfect security), our protocol has a lower round complexity and a much lower communication complexity.

In a recent work, Ning and Xu proposed a generalization of bit-decomposition which can, given a sharing of secret x and an integer $m \ge 2$, compute the sharings (or bitwise sharings) of the base-m digits of x. They also proposed a linear protocol for public modulo reduction as a simplification of their generalization. In this paper, we show that their generalization can be further generalized. More importantly, as a simplification of our further generalization, we propose a public modulo reduction protocol which is more efficient than theirs. Specifically, the round complexity of our (modulo reduction) protocol is the same with theirs, but the communication complexity can be considerably lower.

Category / Keywords: Secure Computation / Multi-party Computation, Constant-Rounds, Linear, Exponentiation, Modulo Reduction, Bit-Decomposition.

Date: received 9 Feb 2011, last revised 23 Aug 2011

Contact author: ncnfl at mail sdu edu cn