Cryptology ePrint Archive: Report 2013/085

Between a Rock and a Hard Place: Interpolating Between MPC and FHE

Ashish Choudhury and Jake Loftus and Emmanuela Orsini and Arpita Patra and Nigel P. Smart

Abstract: We present a computationally secure MPC protocol for threshold adversaries which is parametrized by a value L. When L=2 we obtain a classical form of MPC protocol in which interaction is required for multiplications, as L increases interaction is reduced in that one requires interaction only after computing a higher degree function. When L approaches infinity one obtains the FHE based protocol of Gentry, which requires no interaction. Thus one can trade communication for computation in a simple way.

Our protocol is based on an interactive protocol for ``bootstrapping" a somewhat homomorphic encryption scheme. The key contribution is that our presented protocol is highly communication efficient enabling us to obtain reduced communication when compared to traditional MPC protocols for relatively small values of L.

Category / Keywords: public-key cryptography /

Date: received 19 Feb 2013

Contact author: Ashish Choudhary at bristol ac uk,Emmanuela Orsini@bristol ac uk,Arpita Patra@bristol ac uk,loftus@cs bris ac uk,nigel@cs bris ac uk