Cryptology ePrint Archive: Report 2013/044

Efficient Computation Outsourcing for Inverting a Class of Homomorphic Functions

Fangguo Zhang and Xu Ma and Shengli Liu

Abstract: The rise of cloud computing and the proliferation of mobile devices make computation outsourcing popular. However, the servers are not fully trusted, and a critical problem is the verifiability and privacy of such computations. Although some computation outsoucing schemes provided a general method, the complicated cryptographic tools involved result in great inefficiency. The existing efficient computation outsourcing schemes however aim only at a specific computation task, lacking in generality. In this paper, we show how to construct a generic outsourcing computation scheme for inverting a class of homomorphic functions with computation disequilibrium. Extensive analysis shows that many cryptographic computations fall into this category. The formal security analysis proves that our scheme satisfies verifiability, input and output privacy in information-theoretic sense. Since the construction of our scheme tactfully takes advantage of the intrinsic property of the computation task being outsourced, no public key operations are used in the scheme, thus our solution clearly outperforms the existing schemes in terms of efficiency. In addition, we instantiate our generic construction with concrete examples, and the experimental result testifies the efficiency of our construction.

Category / Keywords: cryptographic protocols /

Date: received 28 Jan 2013

Contact author: isszhfg at mail sysu edu cn