Cryptology ePrint Archive: Report 2011/108

Practical Secure and Efficient Multiparty Linear Programming Based on Problem Transformation

Jannik Dreier and Florian Kerschbaum

Abstract: Cryptographic solutions to privacy-preserving multiparty linear programming are slow. This makes them unsuitable for many economically important applications, such as supply chain optimization, whose size exceeds their practically feasible input range. In this paper we present a privacy-preserving transformation that allows secure outsourcing of the linear program computation in an efficient manner. We evaluate security by quantifying the leakage about the input after the transformation and present implementation results. Using this transformation, we can mostly replace the costly cryptographic operations and securely solve problems several orders of magnitude larger.

Category / Keywords: cryptographic protocols / applications, cryptanalysis, distributed cryptography, information hiding, information theory, secret sharing, outsourcing, linear optimization, cloud computing

Date: received 4 Mar 2011

Contact author: jannik dreier at imag fr