Cryptology ePrint Archive: Report 2011/662

Deploying secure multi-party computation for financial data analysis

Dan Bogdanov and Riivo Talviste and Jan Willemson

Abstract: In this paper we describe a secure system for jointly collecting and analyzing financial data for a consortium of ICT companies. To guarantee each participant's privacy, we use secret sharing and secure multi-party computation (MPC) techniques. While MPC has been used to solve real-life problems beforehand, this is the first time where the actual MPC computation was done over the internet with computing nodes spread geographically apart. We describe the system architecture, security considerations and implementation details. We also present the user feedback analysis revealing that secure multi-party computation techniques give sufficient assurance for data donors to submit their sensitive information, and act as a critical enabling feature for privacy-preserving data mining.

Category / Keywords: applications / financial data analysis, privacy-preserving data mining, secure multi-party computation

Publication Info: This is an extended version of the paper presented at Financial Cryptography and Data Security 2012.

Date: received 7 Dec 2011, last revised 16 Dec 2011

Contact author: riivo talviste at cyber ee

Available formats: PDF | BibTeX Citation

Note: Edit: added reference to the work of J. Feigenbaum et al.

Version: 20111216:094601 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]