Cryptology ePrint Archive: Report 2011/370

Socio-Rational Secret Sharing as a New Direction in Rational Cryptography

Mehrdad Nojoumian

Abstract: Rational secret sharing was proposed by Halpern and Teague in STOC'04. The authors show that, in a setting with rational players, secret sharing and multiparty computation are only possible if the actual secret reconstruction round remains unknown to the players. All the subsequent works use a similar approach with different assumptions. We change the direction by bridging cryptography, game theory, and reputation systems. We consider a ``social model" for repeated rational secret sharing which has elegant properties. We propose a novel scheme, named "socio-rational secret sharing", in which the players are invited to each game based on their reputations in the community. Indeed, they run secret sharing protocols while founding and sustaining a public trust network. As a result, new concepts such as a "rational foresighted player", "social game", and "social Nash equilibrium" are introduced. To motivate our approach, consider a repeated secret sharing game such as "secure auctions", where the auctioneers receive several sealed-bids from the bidders in order to define the auction outcome without revealing the losing bids. If we assume each party has a reputation value, we can then penalize (or reward) the players who are selfish (or unselfish) from game to game. We show that this social reinforcement rationally stimulates the players to be cooperative.

Category / Keywords: Cryptography, Game Theory, Reputation Systems.

Date: received 6 Jul 2011, last revised 21 Feb 2012

Contact author: mnojoumi at cs uwaterloo ca

Available formats: PDF | BibTeX Citation

Version: 20120221:153850 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]