Fiscal Year 2015 Tokyo Institute of Technology ASPIRE League Research Grant

Selected Research Projects for Type 2 in FY2015

Principal Researcher	Name	**Keisuke Tanaka**
	Department and graduate school(institute) in Tokyo Tech	Department of Mathematical and Computing Science, Graduate School of Information Science and Engineering
	Position	Associate Professor
Co-researchers	HKUST	Mordecai Golin, Professor Department of Computer Science
	KAIST	—
	NTU	Ning Chen, Professor Department of Mathematical Sciences
	Tsinghua	—
Subject of the research project		A new protocol design method based on algorithmic game theory
Summary of the research project		Game theory is a mathematical framework for studying decision-making processes by multiple agents who pursue strategies rationally through interaction with other agents. Game theory started from 1940s, and it has been developed as a research field of Operations Research. In game theory, decision-making processes under various situations have been studied. At the beginning of 2000s, a new type of game theory has been initiated that studies the computational aspects of such decision-making processes. Such an area is now called algorithmic game theory. One of the important topics in algorithmic game theory is to study decision-making processes by regarding those agents participating in decision-making processes as distributed computing systems that make their own decisions based on network communications. Researchers have started using this framework for discussing information security. In this project, we

Summary of the research project	propose to push this idea further and use algorithmic game theory for designing efficient and secure protocols for general social agreements such as voting through the internet. We propose the following research topics as basic studies. [Specific Research Topics] We consider a model that is similar to the non-cooperative game model, which is the basic model that has been studied extensivelyin game theory. That is, we consider the situation in which each player makes his/her decision independently to maximize his/her benefit. Then we may assume that such a player will not pursue a strategy that (eventually) gives a loss to the player. We may use this assumption to design an efficient protocol. This point has been used in some protocols for secure communication. When designing a protocol for achieving some communication task in a secure way, it has been assumed that all adversaries have some computational limit. Now we may add some more assumptions from a game theoretic viewpoint. It is sometimes the case that such assumptions help us to design an efficient and natural protocol. We first show examples of information security protocols and then try to extend this approach to protocols for other purposes, such as voting, auctions, etc. We also investigate properties of computation and/or limits of computation executed under game theoretic assumptions. Co-researcher: Prof. Osamu Watanabe, Department of Mathematical and Computing Sciences, Information Science and Engineering, Tokyo Tech