Journal of Information Security and Applications 000 (2017) 1–4

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Realizing correlated equilibrium by secure computation

Lirong Qiu[a], Xin Sun[b,c,*], Xishun Zhao[d]

[a] Information Engineering School, Minzu University of China Beijing, China
[b] Institute of Logic and Cognition, Sun Yat-sen University Guangzhou, China
[c] Department of Foundations of Computer Science, Faculty of Philosophy, The John Paul II Catholic University of Lublin Lublin, Poland
[d] Institute of Logic and Cognition, Sun Yat-sen University Guangzhou, China

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Correlated equilibrium
Multi-party computation

ABSTRACT

In this paper we propose a cryptographic protocol to realize correlated equilibrium without a mediator. Our protocol realizes correlated equilibria of multi-agent games. It is collusion free, unconditional secure and much simpler than other existing protocols.

1. Introduction

The study of game theory and secure computation are both interested in the interactions of mutually untrusting agents. Game theory studies the behavior of rational agents that aim to maximize their utility [1]. Secure computation studies the design of protocols that allow agents to perform computations while keeping privacy of their inputs [2]. Game theory offers a variety of solution concepts to reason about the behavior of rational agents. The most famous one is Nash equilibrium. In two-agent games, a Nash equilibrium is a pair of two independent strategies, one for each agent, such that no agent can unilaterally benefit by deviating from its strategy. Correlated equilibrium, first discussed in Aumann [3], is a solution concept that is more general than Nash equilibrium. Correlated equilibrium allow agents to pick their actions in a correlated way and are in many cases preferable over Nash equilibrium, because they are able to guarantee higher utility for the agents. In order to be able to act in a correlated manner, the agents are assumed to have access to a mediator that provides them with private and correlated recommendations on the action to be taken. However, we are concerned with situations in which a trusted mediator is not available. In this case, secure computation suggests a solution: The agents can run a secure protocol that simulates the mediator while guaranteeing the correctness of correlated action distribution, and the privacy of the actions assigned to each agent.

This line of research is initialed by Dodis et al.[4] and followed by several researcher [5–8]. This paper also belongs to this line of research. In this paper, we propose a cryptographic protocol to realize correlated equilibrium without a mediator. The novelty of this paper is that the cryptographic protocol we propose is collusion free, unconditional secure and simpler than the existing protocol for the same purpose [4,5].

The remainder of this paper is organized as follows: In Section 2 we give a quick review of correlated equilibrium. In Section 3 we develop a protocol to realize correlated equilibrium. We discuss related work in Section 4 and finally we summarize and conclude this paper in Section 5.

2. Correlated equilibrium

A correlated equilibrium is a probability distribution over agents' strategy profiles, which can be understood as a randomized signal, such that each agent can choose his strategy according to the recommendation of the signal. If no agent would want to deviate from the recommended strategy, assuming the others don't deviate, the probability distribution is called a correlated equilibrium. Formally, given a normal-form game $(Agent, A_1, \ldots, A_n, u_1, \ldots, u_n)$, where $Agent = \{1, \ldots, n\}$ is the set of agents, A_i and u_i are respectively the strategy space and utility function for agent i, a correlated equilibrium is a probability distribution τ over $A = A_1 \times \ldots, \times A_n$ such that for every agent $i \in Agent$, for every pair of strategies $\alpha_i, \alpha_i' \in A_i$, we have $\sum_{\alpha_{-i} \in A_{-i}} \tau(\alpha_i, \alpha_{-i}) \times u_i(\alpha_i, \alpha_{-i}) \geq \sum_{\alpha_{-i} \in A_{-i}} \tau(\alpha_i, \alpha_{-i}) \times u_i(\alpha_i', \alpha_{-i})$, where $A_{-i} = A_1 \times \ldots \times A_{i-1} \times A_{i+1} \times \ldots \times A_n$.

Intuitively, in a correlated equilibrium the expected utility of an agent following the randomized signal produced by the correlated equilibrium $(\sum_{\alpha_{-i} \in A_{-i}} \tau(\alpha_i, \alpha_{-i}) \times u_i(\alpha_i, \alpha_{-i}))$ is higher than his expected utility of deviating from the signal $(\sum_{\alpha_{-i} \in A_{-i}} \tau(\alpha_i, \alpha_{-i}) \times u_i(\alpha_i', \alpha_{-i}))$. An equivalent characterization of correlated equilib-

* Corresponding author.
E-mail address: xin_sun_logic@sina.com (X. Sun).

http://dx.doi.org/10.1016/j.jisa.2017.01.008
2214-2126/

		Bob	
		Continue	Swerve
Alice	Continue	0,0	5,1
	Swerve	1,5	4,4

Fig. 1. The game of chicken.

rium is

$$\sum_{\alpha_{-i}\in A_{-i}} \tau(\alpha_i, \alpha_{-i}) \times (u_i(\alpha_i, \alpha_{-i}) - u_i(\alpha_i', \alpha_{-i})) \geq 0.$$

The difference between $u_i(\alpha_i', \alpha_{-i})$ and $u_i(\alpha_i, \alpha_{-i})$ can be understood as a measure of the *regret* of agent i choosing α_i' instead of α_i, when other agents choose α_{-i}. When $(u_i(\alpha_i, \alpha_{-i}) - u_i(\alpha_i', \alpha_{-i}))$ is positive, agent i has no regret for choosing α_i compared to α_i', when other agents choose α_{-i}. Therefore this characterization of correlated equilibrium shows that there is no expected regret for each agent in a correlated equilibrium, which is why all agents are willing to follow the signal produced by a correlated equilibrium.

Example 1 (chicken game)**.** The chicken game is shown in Fig. 1. In this game, Alice and Bob drive their cars towards each other at high speed. The one who swerves first is a chicken and thus loses the game. But, if neither of them swerves then they both injured in a horrible crash. This game has two pure Nash equilibria: strategy profile (*C, S*) with expected utility vector (5, 1) and (*S, C*) with expected utility vector (1, 5). It has one mixed Nash equilibrium: the mixed strategy profile (1/2, 1/2), which each agent assign probability 1/2 to *S*, with expected utility vector (2.5, 2.5).

τ is a correlated equilibrium in this game if the following is satisfied:

- $\tau(C,C) \times 0 + \tau(C,S) \times 5 \geq \tau(C,C) \times 1 + \tau(C,S) \times 4$
- $\tau(S,C) \times 1 + \tau(S,S) \times 4 \geq \tau(S,C) \times 0 + \tau(S,S) \times 5$
- $\tau(C,C) \times 0 + \tau(S,C) \times 5 \geq \tau(C,C) \times 1 + \tau(S,C) \times 4$
- $\tau(C,S) \times 1 + \tau(S,S) \times 4 \geq \tau(C,S) \times 0 + \tau(S,S) \times 5$

Therefore $\tau_1(C,C) = 0.1, \tau_1(C,S) = 0.4, \tau_1(S,C) = 0.3, \tau_1(S,S) = 0.2$ is a correlated equilibrium with expected utility (3.1, 2.7). $\tau_2(C,S) = \tau_2(S,C) = \tau_2(S,S) = 1/3$ is another correlated equilibrium with expected utility (10/3, 10/3).

3. Realizing correlated equilibrium via cryptographic protocol

A probability distribution τ of strategy profiles of an $n-$agent game can be represented with arbitrary accuracy by a list of tuples $(a_1^1, \ldots, a_n^1), \ldots, (a_1^m, \ldots, a_n^m)$ with possible repetitions of strategy profiles such that the number of appearance of a strategy profile $\mathbf{a} = (a_1^i, \ldots, a_n^i)$ in the list equals to $\tau(\mathbf{a}) \times |A_1 \times \ldots \times A_n|$. To realize correlated equilibrium for such games, we need an efficient cryptographic protocol for the following problem: agents $\{1, \ldots, n\}$ know a list of tuples $(a_1^1, \ldots, a_n^1), \ldots, (a_1^m, \ldots, a_n^m)$, and they need to jointly choose a random index i, and have agent 1 learns only the value a_1^i and agent 2 learns only the value a_2^i and so on. This problem is called the*correlated element selection problem* in Dodis et al. [4]. In this section we describe our solution to this problem.

Our protocol is explained in Fig. 2. The function of the protocol is to realize the correlated equilibrium. That is, the protocol selects a strategy profile in accordance to the probability distribution of correlated equilibrium, meanwhile keep the privacy of the strategy assigned to each agent.

Assume a correlated equilibrium is given. Before the protocol starts, we first transform the correlated equilibrium into a list of strategy profiles. We further assume every agent has a private key. The encryption/decryption scheme we use is *exclusive or* $\oplus$. That is, given plain text $x_1 \ldots x_n$ and key $y_1 \ldots y_n$, the ciphertext $z_1 \ldots z_n$ is produced by letting $z_i = x_i \oplus y_i$. We choose this encryption scheme because it is commutative: for two keys $y_1 \ldots y_n$ and $y_1' \ldots y_n'$, $(x_i \oplus y_i) \oplus y_i' = (x_i \oplus y_i') \oplus y_i$.

At the beginning of the protocol, agent 1 randomly permutes the list, encrypts it element-wise and sends the resulting list to the agent 2. Then agent 2 selects a subset of n indexes. Agent 2 further deletes 1 index and encrypts the ciphertext of the strategy belongs him, for all remaining indexes. After the encryption agent 2 sends this list to agent 3. On receiving this list, agent 3 first randomly deletes a tuple, then encrypts the ciphertext of the strategy belongs to him for all remaining indexes. Then agent 3 sends the list to agent 4. For $i \in \{4, \ldots, n-1\}$, agent i behaves like agent 3. When agent n receives the list, there are two tuples remain. Agent n chooses one tuple by random then encrypts his strategy and send the tuple to agent 1. Agent 1 then decrypts all strategies in the tuple, keeps the strategy which belongs to himself, and sends the rest of the tuple to agent 2. Now for all other agents, they decrypt their strategies one by one.

It is easy to show that if all agents follow the protocol then their output is indeed a random pair $(d_1, \ldots, d_n)$ from the known list. Moreover, at the end of the protocol each agent has no information about other agent's output. Therefore this protocol realizes correlated equilibrium. Note that all agents are rational instead of malicious. They behave in order to maximize their utility. They will follow the protocol because the protocol will help them achieve a coorelated equilibrium. Note that our protocol is collusion free because even a group of agents collude, they cannot know the output of those agents who are not in their group.

The existing protocols [4,5] to realize correlated equilibrium are based on blindable encryption. Compared to those protocols, our protocol is much simpler because we use the simple exclusive or as our encryption scheme. Moreover, the security of blindable encryption relies on the computational complexity of problems like prime factorization. Our protocol provides unconditional security because we use one-time pad encryption with exclusive or.

4. Related work

Dodis et al. [4] raise the question whether there exists a mechanism that eliminates the need for the mediator to implement correlated equilibrium yet allows the agents to maintain the high payoffs offered by mediator-assisted strategies. They partially solve this problem by providing a cryptographic protocol to the two-agent correlated element selection problem. Hubácek et al. [7] classify necessary and sufficient cryptographic assumptions for implementing a mediator that allows to achieve a given utility profile of a correlated equilibrium. Wang et al. [8] explore the approach of replacing the trusted mediator with an unconditionally secure sampling protocol that jointly generates the agentsâ;; actions. They characterize the joint distributions that can be securely sampled by malicious agents via protocols using error-free communication.

5. Summary

In this paper we propose a cryptographic protocol to realize correlated equilibrium without a mediator. Our protocol is collusion free, unconditional secure and much simpler than other existing protocols. In the literature of quantum game theory, Huberman and Hogg [9] and La Mura [10] shows that in some games, if the recommendations the agents receive from the mediator are

Please cite this article as: L. Qiu et al., Realizing correlated equilibrium by secure computation, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.008