A Cryptographic Solution to a Game Theoretic Problem

Yevgeniy Dodis, Shai Halevi, Tal Rabin, [DHR00] CRYPTO'00

Aditya Damodhar D

Indian Institute of Science

December 8, 2023

Part I: Motivations and Problem Statement

Part I

Motivations and Problem Statement

Motivation

- Two player games consists of two players with a set of moves and a payoff for each player which depends on the moves chosen by both the players.
- Strategy is a (randomized) function for choosing a move.
- Players are selfish and rational.
- Equilibrium achieved when strategies are self-enforcing (Nash Equilibrium).
- Payoff increased in the presence of a trusted third party (Correlated Equilibrium).
- **Can we get the higher payoff even after removing TTP?**

Problem Statement

Can a two player game achieve Correlated Equilibria with only two players involved?

Part II: Background

Part II

Background

Notation

We discuss in terms of finite strategy two-player games:
$i \in \{0, 1\}$

- Players: P_i
- Set of Actions: A_i
- Payoff Function: $U : A_0 x A_1 \rightarrow R$
- Payoff of Player i: $u_i(a_0, a_1)$
- Strategy of player i: s_i
- Conditional Distribution: $s(\cdot|a_i)$
- Utility in a conditional distribution: $u_0(a_0, s_1^*|a_0^*), u_1(s_0^*, a_1|a_1^*)$

Definition: Nash Equilibrium

Definition 1 *A* Nash equilibrium *of a game G is an independent strategy profile (s_1^*, s_2^*), such that for any $a_1 \in A_1$, $a_2 \in A_2$, we have $u_1(s_1^*, s_2^*) \geq u_1(a_1, s_2^*)$ and $u_2(s_1^*, s_2^*) \geq u_2(s_1^*, a_2)$.*

In other words, given that player 2 follows s_2^*, s_1^* is an optimal response of player 1 and vice versa.

DEFINITION: CORRELATED EQUILIBRIUM

Definition 2 *A* Correlated equilibrium *is a strategy profile* $s^* = s^*(A_1 \times A_2) = (s_1^*, s_2^*)$*, such that for any* (a_1^*, a_2^*) *in the support of* s^**, and any* $a_1 \in A_1$ *and* $a_2 \in A_2$*, we have* $u_1(a_1^*, s_2^* \mid a_1^*) \geq u_1(a_1, s_2^* \mid a_1^*)$ *and* $u_2(s_1^*, a_2^* \mid a_2^*) \geq u_2(s_1^*, a_2 \mid a_2^*)$.

Given Nash (resp. Correlated) equilibrium (s_1^*, s_2^*), we say that (s_1^*, s_2^*) achieves *Nash (resp. Correlated) equilibrium payoffs* $[u_1(s_1^*, s_2^*), u_2(s_1^*, s_2^*)]$.

PART III: THE SOLUTION

Part III

SOLUTION

Getting Rid of the Mediator

- Extended Games = Regular Game + two party protocol.
- Consider two party protocol to be the mediator.

Getting Rid of the Mediator

Deviation Consideration

- Deviation: Any party which deviates is forced to get its minimum possible payoff while the other party maximises its own payoff. THis is called the *minmax level*

Lemma 1: Let $[v_0, v_1]$ be the payoffs achieved by Correlated equilibrium s^*. Then, $v_i > \underline{v_i}$.

Getting Rid of the Mediator
Lemma 1 Proof

Proof: Consider player 1. Let s_2^* be the marginal strategy of player 2 in the Correlated equilibrium s^*, and let s_1' be the best (independent) response of player 1 to s_2^*. (The strategy s_1' can be thought of as what player 1 should do if it knows that player 2 plays according to s_2^*, but it did not get any "recommendation" from the mediator.)
Since s^* is a Correlated equilibrium, it follows that $v_1 \geq u_1(s_1'; s_2^*)$, since a particular deviation of player 1 from the correlated equilibrium is to "ignore" its recommendation and always play s_1', and we know that no such deviation can increase the payoff of player 1. Also, recall that s_1' is the best (independent) strategy in response to s_2^*, so we have $u_1(s_1'; s_2^*) = max_{s_1} u_1(s_1; s_2^*)$. Hence we get
$v_1 \geq u_1(s_1'; s_2^*) = max_{s_1} u_1(s_1; s_2^*) \geq min_{s_2} max_{s_1} u_1(s_1; s_2) = \underline{v_1}$

Getting Rid of the Mediator

Theorem

Theorem 1 *If secure two-party protocols exist for non-trivial functions, then for any Correlated equilibrium s of the original game G, there exists an extended game G' with a computational Nash equilibrium σ, such that the payoffs for both players are the same in σ and s.*

Getting Rid of the Mediator

Proof Sketch

- Extended protocol G' is protocol G with a protocol P to compute s.
- Computational Nash equilibrium consists of both players following their steps in P, then executing the moves they get from this protocol.
- This achieves the same payoffs as the correlated equilibrium for G. For it to be a computational Nash Equilibrium, Any deviation in the protocol will result in lower payoffs for the deviating party.
- When a player is caught deviating, the minmax level is enforced.
- When a player deviatesd without getting caught, we assume the probaility of that happening is $\mu(k)$, and the payoff achieved is $\overline{v_i}$, then the expected payoff in a protocol which involves cheating is given as follows:
  $\mu(k)\overline{v_i} + (1-\mu(k))\underline{v_i} = v_i + \mu(k)(\overline{v_i} - v_i) - (1-\mu(k))(v_i - \underline{v_i}) \leq v_i + \mu(k)(\overline{v_i} - v_i)$
- Inequality continues from Lemma 1, and as $\overline{v_i} - v_i$ is constant, the advantage in deviation is negligible.

Part IV: The 2PC, Cryptographically

Part IV

The 2PC, Cryptographically

The Problem and the Primitive

We consider the Correlated Element Selection Problem and a2PC solution for it using Blindable Encryption.

The Problem and the Primitive

Correlated Element Selection Problem

- Players: A, B
- List of Pairs: $\{(a_1, b_1), \ldots, (a_n, b_n)\}$
- Result: $A \leftarrow a_i, B \leftarrow b_i$

Notation:

- $[n]$ is the set $\{1, 2, \ldots, n\}$
- $A(x)$ output distribution on of randomized algorithm A on x.
- $A(x; r)$ output value of randomized algorithm A on x.
- Algorithms of blindable encryption scheme: *Gen*, *Enc*, *Dec*, *Blind* and *Combine*.
- *Gen*, *Enc* and *Dec* are typical functions from an Encryption Scheme.
- **Blind** function is given as follows:
  There exists a Blindable encryption scheme $\mathcal{E}$ and for every message m and ciphertext $c \in Enc_{pk}(m)$, for any message m' (called blinding factor), $Blind_{pk}(c, m')$ produces a random encryption of $m + m'$.
  $Enc_{pk}(m + m') \equiv Blind_{pk}(c, m')$
- **Combine** function is given is as follows:
  There exists a Blindable encryption scheme $\mathcal{E}$ and for every message m and ciphertext $c \in Enc_{pk}(m)$. For successive blindings using random coins r_1, r_2, then for any blinding factors m_1, m_2
  $Blind_{pk}(Blind_{pk}(c, m_1; r_1), m_2; r_2) = Blind_{pk}(c, m_1 + m_2; Combine_{pk}(r_1, r_2))$

The Problem and the Primitive

Honest Players:

Common inputs: List of pairs $\{(a_i, b_i)\}_{i=1}^n$, public key pk.
Preparer knows: secret key sk.

P : **1. Permute and Encrypt.**
Pick a random permutation π over $[n]$.
Let $(c_i, d_i) = (Enc_{pk}(a_{\pi(i)}),\ Enc_{pk}(b_{\pi(i)}))$, for all $i \in [n]$.
Send the list $\{(c_i, d_i)\}_{i=1}^n$ to C.

C : **2. Choose and Blind.**
Pick a random index $\ell \in [n]$, and a random blinding factor β.
Let $(e, f) = (Blind_{pk}(c_\ell, 0),\ Blind_{pk}(d_\ell, \beta))$.
Send (e, f) to P.

P : **3. Decrypt and Output.**
Set $a = Dec_{sk}(e)$, $\tilde{b} = Dec_{sk}(f)$. Output a.
Send $\tilde{b}$ to C.

C : **4. Unblind and Output.**
Set $b = \tilde{b} - \beta$. Output b.

The Problem and the Primitive

Dishonest Players:

Common inputs: List of pairs $\{(a_i, b_i)\}_{i=1}^n$, public key pk.
Preparer knows: secret key sk.

P : **1. Permute and Encrypt.**
Pick a random permutation π over $[n]$, and random strings $\{(r_i, s_i)\}_{i=1}^n$.
Let $(c_i, d_i) = (Enc_{pk}(a_{\pi(i)}; r_{\pi(i)}),\ Enc_{pk}(b_{\pi(i)}; s_{\pi(i)}))$, for all $i \in [n]$.
Send $\{(c_i, d_i)\}_{i=1}^n$ to C.

Sub-protocol Π_1: P proves in zero-knowledge that it knows the randomness $\{(r_i, s_i)\}_{i=1}^n$ and permutation π that were used to obtain the list $\{(c_i, d_i)\}_{i=1}^n$.

C : **2. Choose and Blind.**
Pick a random index $\ell \in [n]$.
Send to P the ciphertext $e = Blind_{pk}(c_\ell, 0)$.

Sub-protocol Π_2: C proves in a witness-hiding manner that it knows the randomness and index ℓ that were used to obtain e.

P : **3. Decrypt and Output.**
Set $a = Dec_{sk}(e)$. Output a.
Send to C the list of pairs $\{(b_{\pi(i)}, s_{\pi(i)})\}_{i=1}^n$ (in this order).

C : **4. Verify and Output.**
Denote by (b, s) the ℓ'th entry in this lists (i.e., $(b, s) = (b_{\pi(\ell)}, s_{\pi(\ell)})$).
If $d_\ell = Enc_{pk}(b; s)$ then output b.

References

[DHR00] Yevgeniy Dodis, Shai Halevi, and Tal Rabin. **"A Cryptographic Solution to a Game Theoretic Problem".** In: *Advances in Cryptology — CRYPTO 2000*. Ed. by Mihir Bellare. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 112–130. ISBN: 978-3-540-44598-2.