A Cryptographic Solution to a Game Theoretic Problem

Yevgeniy Dodis
(MIT)

Shai Halevi
(IBM)

Tal Rabin
(IBM)

Two-Player Strategic Games

	S	P	R
S	0,0	1,-1	-1,1
P	-1,1	0,0	1,-1
R	1,-1	-1,1	0,0

Scissors, Paper, Rock

Game Theory Setting

- Simultaneous moves.
- Strategy can be probabilistic.
- Action spaces, utility functions are fixed and known.
- Each player rational and selfish:
  only cares to maximize his payoff.
- Which behaviors are reasonable???

Equilibrium

- "Self-enforcing" strategies.
- Each player is optimal given his information about the other player's strategy.
- No player has an incentive to deviate.
- Classical Equilibria: Nash and Correlated.

Notation and Terminology

Player 1	Player 2
Choose $a_1 \in A_1$	Choose $a_2 \in A_2$
Play (a_1, a_2)	
Get $u_1(a_1, a_2)$	Get $u_2(a_1, a_2)$

- a_i — action of player i.
- $u_i(a_1, a_2)$ — payoff of player i.
- s_i — strategy of player i.
- $s = (s_1, s_2)$ — strategy profile.

Nash Equilibrium

(s_1^*, s_2^*) is a Nash Equilibrium (NE) if

- s_1^* is a best response of player 1 to s_2^*:

  $u_1(s_1^*, s_2^*) \;\geq\; u_1(a_1, s_2^*)$, for any $a_1 \in A_1$

- Same for player 2.

- Deterministic $s_1^*, s_2^* \Rightarrow$ pure-strategy NE.

Notice:

- Strategies s_1^*, s_2^* are independent.

Theorem: Every game has a NE [Nash'50].

Examples

Game	Nash Eq.	Payoffs
$\begin{array}{c|c|c} & C & D \\ \hline C & 1,1 & -1,2 \\ \hline D & 2,-1 & 0,0 \end{array}$	$\cancel{(C,C)}$	$\cancel{[1,1]}$
	(D,D)	$[0,0]$
Prisoner's Dilemma		
$\begin{array}{c|c|c} & B & S \\ \hline B & 1,2 & 0,0 \\ \hline S & 0,0 & 2,1 \end{array}$	(B,B)	$[1,2]$
Battle of Sexes	(S,S)	$[2,1]$
	$(\frac{1}{3}B+\frac{2}{3}S, \frac{2}{3}B+\frac{1}{3}S)$	$[\frac{2}{3},\frac{2}{3}]$

Pros & Cons of Nash Equilibrium

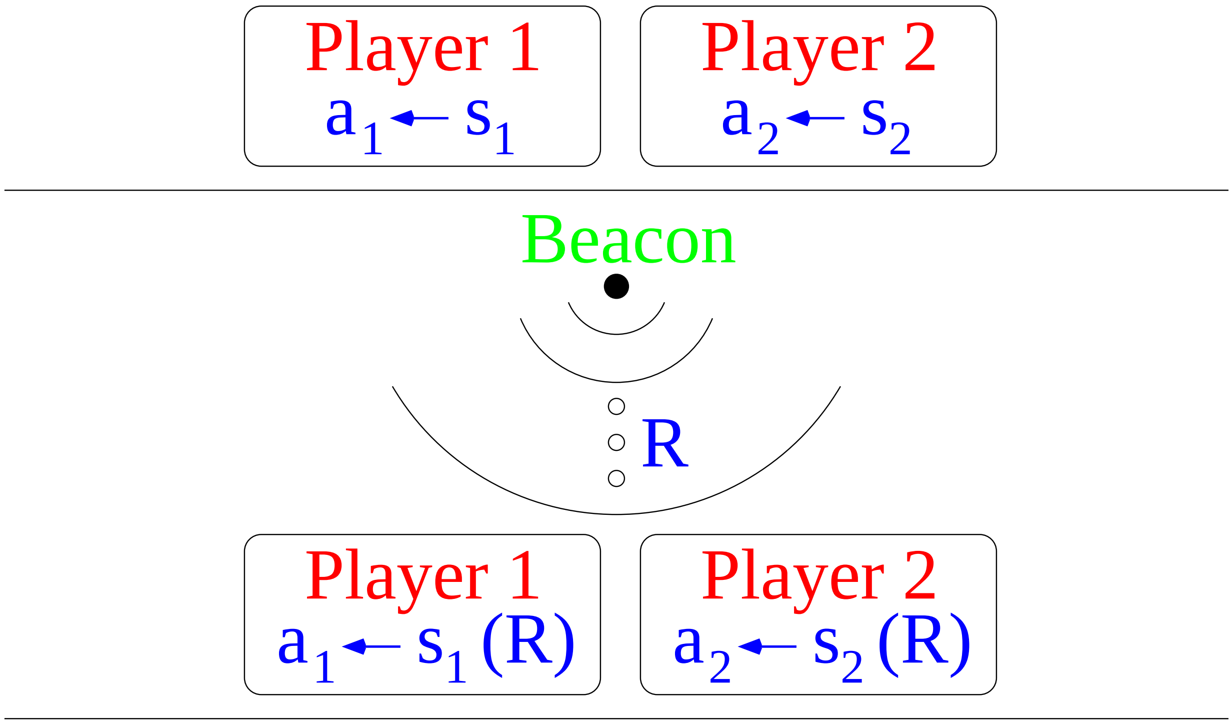
Main advantage:

- Independence of players' strategies.

Main Disadvantage:

- Often cannot achieve high payoffs.

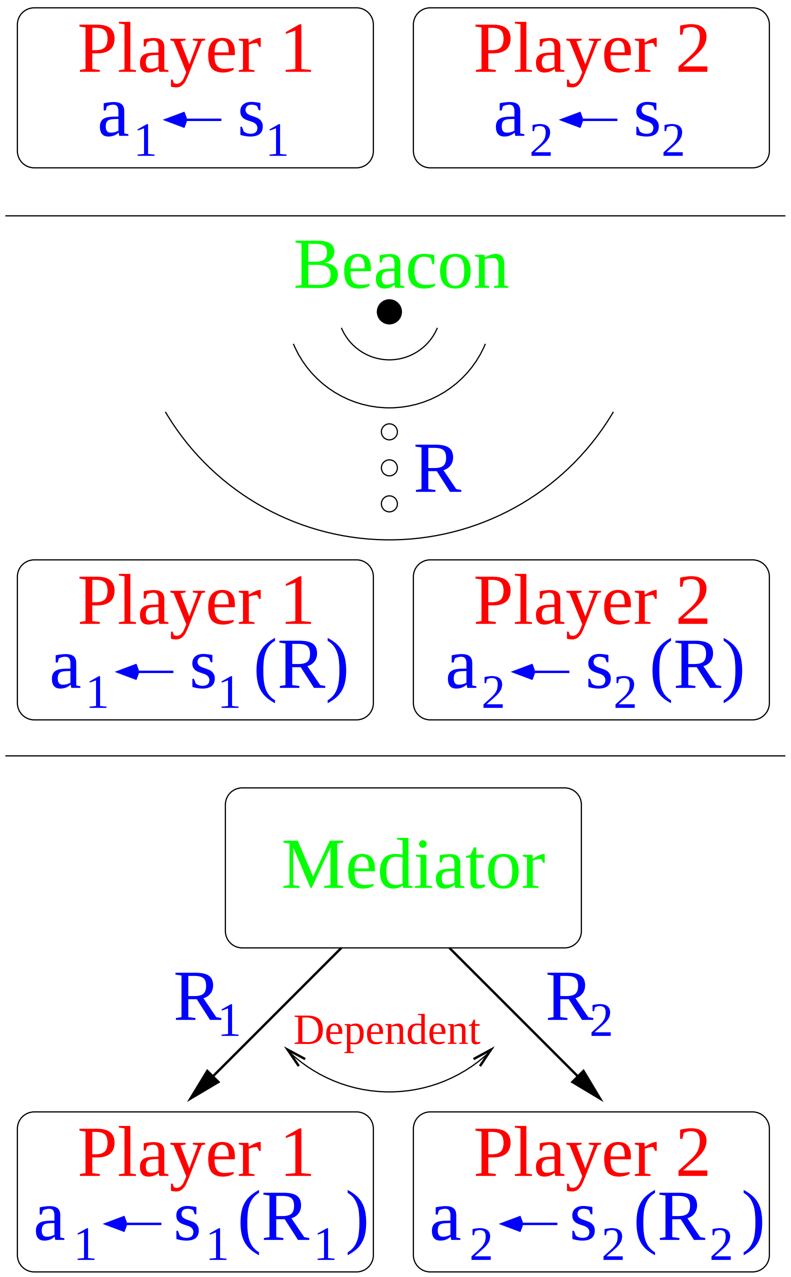
Nash Equilibrium with Public Coins



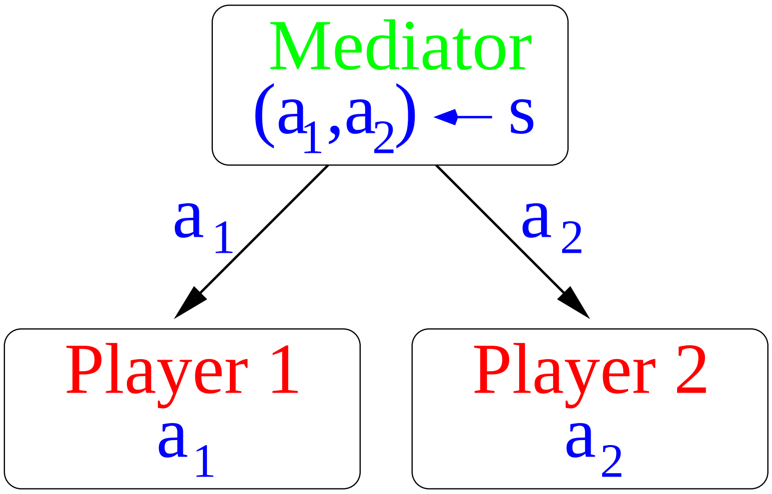
Battle of Sexes: $\frac{1}{2}(B, B) + \frac{1}{2}(S, S) \Rightarrow [\frac{3}{2}, \frac{3}{2}]$.

- $\forall\ R \Rightarrow (s_1(R), s_2(R))$ is a NE.
- No longer independent strategies.
- Rather, perfectly correlated.
- Can achieve any convex combination of NE.
- Can we do better?

Full Correlation

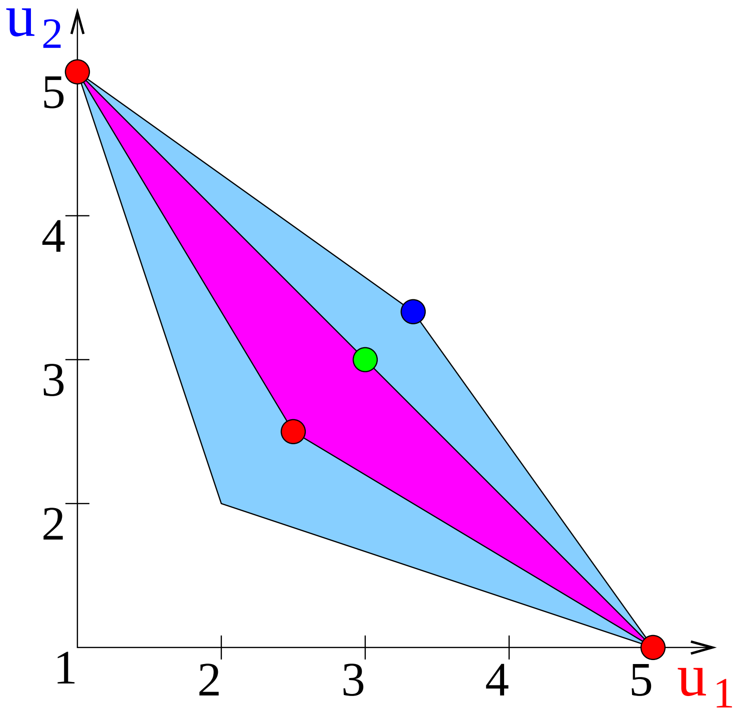


Correlated Equilibrium [Aumann'74]



- s — joint (not product!) distribution.
- a_i — "recommended action" for player i.
- CE: players always follow recommendation.
  - $s_2 \mid a_1$ — conditional advice of player 2 when player 1 got a_1.
  - a_1 is always best response to $s_2 \mid a_1$.
  - Same for player 2.

Game of "Chicken"



	C	D
C	4,4	1,5
D	5,1	0,0

"Chicken"

	C	D
C	1/4	1/4
D	1/4	1/4

Mixed Nash

	C	D
C	0	1/2
D	1/2	0

Public Coin

	C	D
C	1/3	1/3
D	1/3	0

Correlated

- Nash Equilibria: $[1, 5]$, $[5, 1]$, $[\frac{5}{2}, \frac{5}{2}]$.

- Public Coin NE: $[3, 3]$

- "Best" CE: $[3\frac{1}{3}, 3\frac{1}{3}]$

Nash vs. Correlated Equilibria

Nash Eq: strategies are independent.

√ Players can play Nash Eq. on their own.

Correlated Eq: strategies can be correlated.

√ Payoffs often outside (and better than) any convex combination of Nash Eq.

× Trusted third party (mediator) is needed to choose correlated strategies.

Problem:

- Achieve CE payoffs without mediator.

Related Work in Game Theory

- [NCH97]: "NE are superficial CE".
- [MSS95]: NE of local-interaction game $\Leftrightarrow$ CE of underlying game.
- [L96,LS97]: reduce role of mediator.
- [B92]: replace mediator for $n \geq 4$ players.
- [F88,90]: communication equilibrium, incomplete information for $n \geq 4$ players.
- Few recent papers [B98], [UV98a,98b,99].

Getting Rid of Mediator

<u>`Idea`</u>: Replace mediator by communication.

- Task of mediator: privately compute probabilistic function $s(\cdot, \cdot) \to (a_1, a_2)$.

- Unbounded players: not even a coin-flip.

- "Honest-but-curious": convex hull of NE [Barany].

- Computationally bounded: any function can be securely computed (in cryptographic sense) [GMW,Yao].

Implementation Idea

- To implement a given CE s of G:
  - Compute $(a_1, a_2) \leftarrow s$ using secure two-party protocol.
  - Play (a_1, a_2) in G.
- **Meta-Theorem:** Any CE of G can be implemented as a NE by computationally bounded players that can communicate before G starts.

Adding "Cheap Talk"

Player 1	Player 2
Pre-Play Communication	
Choose $a_1 \in A_1$	Choose $a_2 \in A_2$
Play (a_1, a_2)	
Get $u_1(a_1, a_2)$	Get $u_2(a_1, a_2)$

- Resulting $\tilde{G}$ = extended game of G.
- Strategy = probabilistic algorithm, telling a player what to do in each situation.
- NE of $\tilde{G}$ is defined same way as before.
- **Observation:**
  Every NE of $\tilde{G}$ corresponds to CE of G.
- **Goal:** "cryptographic" converse.

Computational Nash Equilibrium

- Introduce external security parameter k.
- All parameters of G are "constants".
- (σ_1^*, σ_2^*) is Computational NE of $\tilde{G}$ if:

(a) both σ_1^*, σ_2^* are PPT computable; and

(b) for any other PPT strategies σ_1, σ_2,

$$\begin{aligned} u_1(\sigma_1, \sigma_2^*) &\leq u_1(\sigma_1^*, \sigma_2^*) + negl(k) \\ u_2(\sigma_1^*, \sigma_2) &\leq u_2(\sigma_1^*, \sigma_2^*) + negl(k) \end{aligned}$$

Our Result

Theorem: Any CE s^* of G can be implemented as Computational NE of $\tilde{G}$.

Proof Idea: Here is strategy σ_i^*:

- Participate in secure protocol P for s^* in the pre-play communication stage.

- Play the output a_i in G.

Are we done?

What if opponent misbehaves in P?

- Cryptography: get "caught" w.h.p.

- Game Theory: still have to play G and get payoffs...

Minimax Punishment

- Minimax level of player 2 — lowest payoff player 1 can force upon player 2:

$$\underline{v_2} = \min_{s_1} \max_{s_2} \; u_2(s_1, s_2)$$

- Similarly for player 1.

Lemma: If $[v_1, v_2]$ – payoffs of CE s^*, then

$$v_i \geq \underline{v_i}$$

- If opponent misbehaves $\Rightarrow$ punish to his minimax level.

- Negligible incentive to deviate.

$\blacksquare$

Why Punish the Deviator?

- Punishing may be costly for the punisher.

- NE only requires optimal response when the other player follows his strategy.

- OK to lose when punishing: the cheater was not supposed to cheat!

- Inherent weakness of NE in extensive-form games.

- Subgame Perfect Equilibrium (SPE) solves this problem: always optimal to follow the strategy no matter what the opponent does.

Theorem: Any Nash-Compatible CE of G can be implemented as Computational SPE of $\tilde{G}$.

Cryptographic Protocols vs. Games

Issue	Cryptography	Game Theory
Incentive	None	Payoff
Players	Totally Honest or Malicious	Always Rational
Punishing Cheaters	Outside Model	Central Part
Solution Concept	Secure Protocol	Equilibrium
Early Stopping	Problem	Not an Issue

Doing It Efficiently

- Generic two-party computation is expensive and non-intuitive.

- In many games distribution s is describable by a short list of pairs $\{(\text{move-1},\ \text{move-2})\}$.

- Game of “Chicken” : $\{(C, C), (C, D), (D, C)\}$.

Correlated Element Selection

Participants: Alice and Bob.

Instance: Fixed list of pairs:

$$(a_1, b_1), \ldots, (a_n, b_n), \qquad a_i \in A,\ \ b_i \in B$$

Goal: Pick random $i \in [n]$ such that

- Alice only learns a_i.
- Bob only learns b_i.

Properties of our Solution

- Efficient and intuitive.
- Constant round, exponential error.
- Uses only simple zero-knowledge proofs (similar to, e.g., [Abe'98]).
- Works with any semantically secure encryption which is blindable:
  - Given $c = E(x)$ (x unknown) and y, can generate random $c' = E(x + y)$.
    Denote $c' = Blind(c, y)$.
  - Examples: El-Gamal, Goldwasser/Micali, Benaloh.

Honest-but-Curious Protocol

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

A : **Permute and Encrypt**.
Pick random permutation $\pi \in S_n$.
Let $(c_i, d_i) = (E(a_{\pi(i)}),\ E(b_{\pi(i)}))$.
Send list $\{(c_i, d_i)\}_{i=1}^n$ to B.

B : **Choose and Blind**.
Pick random $\ell \in [n]$ and "blinding" β.
Let $(e, f) = (Blind(c_\ell, 0), Blind(d_\ell, \beta))$.
Send (e, f) to A.

A : **Decrypt and Output**.
Set $a = D(e)$, $\tilde{b} = D(f)$. Output a.
Send $\tilde{b}$ to B.

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

Summary

- Show how cryptographic protocols can be used to solve a game theoretic problem.

- Gave efficient protocol for Correlated Element Selection problem.

- Show usefulness of blindable encryption.