Tik-110.505

Methods of Cryptography:
”Interplay between Cryptography and Game Theory”

Helger Lipmaa
Helsinki University of Technology
helger@tml.hut.fi

February 7, 2001

Today's literature

- [OR94] Martin J. Osborne, Ariel Rubinstein, 'A Course in Game Theory", The MIT Press, 1994.

- [DHR00] Yevgeniy Dodis, Shai Halevi and Tal Rabin, "A Cryptographic Solution to a Game Theoretic Problem" , CRYPTO 2000.

- [NPS99] Moni Naor, Benny Pinkas, Reuben Sumner, "Privacy Preserving Auctions and Mechanism Design", ACM Conf. on E-Commerce, 1999.

`http://www.tml.hut.fi/~helger/teaching/crypto-gametheory/`

Comparison of Areas

	Game theory	Cryptography
Environment	Multi-player	
Player motivation	Selfish	Honest, Honest-but-curious, malicious
Player abilities	(Unbounded) rational (Bounded) rational Mostly symmetric	Information-theoretic Computational Symmetric/Asymmetric
Protocols	Simultaneous, move-by-move	Sequential
Semantics	Steady state/deductive	? Kerckhoffs principle

I guess we are able to draw a better table in the last lecture!

Game theory, more precisely, I

- Game theory models the actions of decision-makers.

- Players either know the complete situation (*deductive* semantics), or have guessed it from their long experience (*steady state* semantics).

Game theory, more precisely, II

- Players act *selfishly* and *rationally*, by taking into account the possible actions of other players.
  - ⋆ Selfish: the sole goal is to maximize your own payoff!
  - ⋆ You really don't care how it makes the others feel, as long as you do well yourself. You may actually help the others if it suits you.

    Example: Microsoft...
- After making decisions, players act simultaneously.

Cryptography, more precisely

- Cryptography models *any* interaction of people.
- We assume that players know the environment they are working in, except some short secrets (Kerckhoffs principle).
- The goals vary from the selfish behavior of game theory to the extreme sado-masochism (let us hurt others, even if it hurts us.)
- The players act sequentially.
  - ⋆ Malicious players have incentive to break simultaneousity!

Cryptography = a superset of game theory?

and thus. . .

Why cryptography could help game theory?

but before. . .

Game Theory: Strategies

- Let N be the set of players; A_i be the action of i's player; $(A_i) = (A_i)_{i \in N}$ — the tuple of actions; A_{-i} — the tuple of actions of everybody else but i.
- Alice knows what is her payoff in a game in the case of every (A_j).
- Only in trivial games her payoff does not depend on $A_{-\mathsf{Alice}}$, or the payoff of others would not depend on A_{Alice}.
- Deterministic action is not always rational!

Strategies, II

- Strategy s_i of i's player is usually a probability distribution over the set of her possible actions A_i, $s_i(A_i)$.
- $s(\prod A_i) = s(A_1 \times \cdots \times A_{|N|})$ is a probability distribution over A^N.
- Sometimes, the distribution $s(\prod A_i)$ could be seen as the direct product of distributions $s_i(A_i)$, $s(\prod A_i) = \prod s_i(A_i)$.
  - ⋆ We say then that players' strategies are independent.
- . . . but not always.

Equilibria

- Many games have *equilibria*:
  - ⋆ A tuple of strategies, where assuming other people are following their strategies, no participant has incentive to change strategy.
  - ⋆ Summa summarum, nobody is going to change.
  - ⋆ Some kind of black hole: you never come back!
- Not all equilibria have equally good payoffs.

Nash Equilibria

Nash equilibria: Equilibria in the case where strategies are independent.

"Chicken" game:

Alice\Bob	Chicken	Dare
Chicken	(4,4)	(1,5)
Dare	(5,1)	(0,0)

There are three Nash equilibria (check it!):

- s^1 =(Chicken,Dare) — payoff $(1, 5)$, s^2 =(Dare,Chicken) — payoff $(5, 1)$, $s^3 = \frac{1}{2}$(Chicken,Dare)+$\frac{1}{2}$(Dare,Chicken) — payoff $(2.5, 2.5)$.

The best "fair" equilibrium in the convex hull of the Nash equilibria is $\frac{1}{2}s^1 + \frac{1}{2}s^2$ with payoff $(3, 3)$.

Correlated Equilibria

- One could get better equilibria by having *correlated strategies* where $s(\prod A_i)$ is not necessarily a direct product.

- Implemented classically by using a *trusted third party*, who recommends some actions A_i to players.

Correlated Equilibria, II

- After recommendation A_{Alice}, Alice knows conditional distributions $s_{\mathsf{Alice}}(\cdot|A_{\mathsf{Alice}})$ over the actions of the other player, but nothing more.

- Since we have an equilibria and a *trusted* third party, Alice should have no incentive to deviate from the recommendation: she would not gain anything from that.

- May sound impossible, but this simple scheme really helps to get better payoffs. How then?

A nice correlated equilibrium

The next correlated equilibrium gives fair payoff $(3.5, 3.5)$:

Alice\Bob	Chicken	Dare
Chicken	$\frac{1}{3}$	$\frac{1}{3}$
Dare	$\frac{1}{3}$	0

Proof: If Alice is recommended to be chicken, her expected payoff is $\frac{1}{2} \cdot 4 + \frac{1}{2} \cdot 1 = \frac{5}{2}$. If she deviates (plays "dare"), her new payoff is $\frac{1}{2} \cdot 5 + \frac{1}{2} \cdot 0 = \frac{5}{2}$, exactly the same. Hence, she does not have motivation for deviating!
If Alice is recommended to dare, her expected payoff by daring is 5 (since (Dare,Dare) is never played); if she deviates, she gets payoff 4.

Hence, Alice (and equally Bob) is motivated to follow the advice.

And now, ladies and gentlemen, cryptography...

- A standard question in cryptography: can we eliminate the TTP?
- A standard answer: we can, by using general multi-player computation.
- A good answer: we can do it efficiently, by employing customized zero-knowledge and witness-hiding techniques. See [DHR00].
- Payoff: we have to assume both players are computationally bounded and can communicate before the actual game.

But what does cryptography gain?

[DHR00] uses the standard *minmax* methodology of game theory:

- The game has to go on, even if one player does not finish the initial zero-knowledge protocol.

- In cryptography, various methods are used to guarantee the *atomicity*. (Asokan can talk about that!)

But what does cryptography gain?

- Here, atomicity does not matter. A honest player can apply the method of sado-masochism, by choosing a strategy that gives the least payoff to the deviator when the deviator chooses his best strategy.

- It can hurt the honest player, but on the other hand, makes everybody reluctant to hurt the atomicity.

- Selfishness rules!!! (Selfish. . . malicious)

See [DHR00] for more. Moreover, game theory is a much older *science* than cryptography, and could hence be used to borrow more mature view of world.

Another Interplay: Auctions

Example 18.1 from [OR94]. An object is assigned to one player $i \in N$ in exchange for a payment. Player i's valuation of the object is v_i, s.t. $v_1 > v_2 > \ldots v_{|N|} > 0$. The mechanism used to assign the object is a (sealed bid) auction: the players simultaneously submit bids (non-negative numbers), and the object is given to the player with the lowest index among those who submit the highest bid, in exchange for a payment.

In a *first price* auction the payment that the winner makes is the price that he bids.

Exercise 18.2 Formulate a first price auction as a strategic game and analyze its Nash equilibria. Show that in all equilibria player 1 obtains the object.

Auctions, second-price

In a second price auction the winner obtains the object for the second-highest submitted bid.

Exercise 18.3 Show that in a second price auction the tuple of bids (v_i) form a *weakly dominant action*: Player i's payoff when he bids v_i is at least as high as his payoff when he submits any other bid, regardless of the actions of the other players. Show that nevertheless there are equilibria in which the winner is not player 1.

Revelation principle

- There is a general *Revelation Principle* that actually for *any* mechanism there is a direct, incentive-compatible mechanism with the same result.

- There are (more) efficient cryptographic protocols for first-price auctions and (less) efficient cryptographic protocols for second-price auctions.

- Is there a transform that takes a FP auction protocol and converts it into an as-secure SP auction?

Open problems?

A general research question: Give an efficient transformation that, given a secure cryptographic protocol for (some type of) game, transforms this protocol to a secure *efficient* cryptographic protocol for an incentive-compatible game, by using the revelation principle?

Compare: given a circuit for "any" function f, it is possible to transform it to another circuit for the same function f, s.t. every player obtains only some inputs to the circuit, and as a result of the circuit execution gains no more knowledge than the value of f on given inputs!