Economic Mechanism Design and Cryptography

Game Theory & Cryptography seminar

Mika Kojo

mkojo@ssh.com

SSH Communication Security Corp

FEBRUARY 21, 2001

What is this all about?

This talk is based on the two papers;

(i) Hal R. Varian, Economic Machanism Design for Computerized Agents.

(ii) Moni Naor, Benny Pinkas, and Reuben Sumner, Privacy Preserving Auctions and Mechanism Design.

We concentrate on auctions, explain the revelation principle and then look how to use cryptography to implement auction in practice (in Naor et al. style).

Auction; notation

Let B denote the set of bidders, $a_0 \in A$ be the canonical auctioneer, and $o_0 \in O$ be the canonical object that is auctioned. Suppose there is a function; $v : B \times O \to \mathbb{R}$, written also as $v_b(o)$ for $b \in B, o \in O$. We write $v_b = v_b(o_0)$ for the canonical object. We write $\ell : B \times O \to \mathbb{R}$ for the actual bid function.

We will also define a function $u : B \times S \to \mathbb{R}$, where S is the set of states. u is called the utility function.

Example. $u_b(s) = v_b(s) - \ell_b(s)$, when $S = O$. Thus the utility is positive when $\ell_b(s) < v_b(s)$.

We usually assume that the object of the bidder $b \in B$ is to maximize the utility. Furthermore, the bidders are not allowed to collude.

English auction

The simplest of all auctions is the (open-cry) English auction. Now, we write $\ell : \mathbb{Z} \times B \times O \to \mathbb{R}$ for a time-parametrized bidding function, and $\ell_i(\cdot, \cdot) = \ell(i, \cdot, \cdot)$.

The auction proceeds as follows;

(i) The auction is set up and the start-up price is announced for the objects.

(ii) At time $i \in \mathbb{Z}$ all bidders send a bid $\ell_i(b, o)$ to the auctioneer.

(iii) Last bidder obtains the object.

Clearly the winner obtains the object for the second highest bid, at least very close to it.

Vickrey auction

Suppose we'd like an auction mechanism that doesn't require iteration. Vickrey's auction does this as follows;

(i) Auctioneer sets up the auction and announces the start-up prices $s(o)$, for all $o \in O$.

(ii) Bidders submit *sealed* bids $\ell_b(o)$ to the auctioneer.

(iii) Object $o \in O$ is given to $b \in B$ for which $\ell_b(o) > \ell_{b'}(o)$ for all $b' \in B$, by the second highest price $\ell_{b'}(o)$ with $\ell_{b'}(o) \geq \ell_{b''}(o)$, for all $b'' \in B$.

The difference to English auction is the fact that this is a *direct mechanism* opposed to a *indirect mechanism*. Namely, no iteration is needed but the result is obtained directly in one pass.

Further in Vickrey auction setting $\ell_b(o) = v_b(o)$ is the optimal strategy!

Nash equilibria in Vickrey auction

Suppose fixed bids $\ell_{(\cdot)}(o)$ for the object $o \in o$. Now, the bidder $b \in B$ would obtain the object for the smallest amount of payment required.

Now, if $\ell_b(o) < \ell_{b'}(o)$ then b wants to have $\ell_{b'}(o) < \ell_b(o) \leq v_b(o)$. However, b cannot affect (by definition) $\ell_{b'}(o)$ and we see that the payment is

$$\ell_{b'}(o),$$

for $b' \in B$ s.t. $\ell_{b'}(o) > \ell_{b''}(o)$ for all $b'' \in B, b'' \neq b$.

As b cannot affect the payment he will have to make anyway, it is as well to put $\ell_b(o) = v_b(o)$, for the maximal payoff.

Why not to maximize?

The game theoretical approach we used didn't take into account the effect of history.

For example, the auctioneer learns in the Vickrey auction the values $v_b(o)$. If the auctioneer sells object (or similar) o again it can just start with the start-up price $\max_{b \in B} v_b(o) - 1$.

Thus in practice it would be beneficial to have mechanism that hides the bids from the auctioneer, except for the second highest bid and the identity of the winner.

This brings in cryptography.

Naor, Pinkas & Sumner mechanism

To obtain “ideal” security of the auction Naor, Pinkas & Sumner introduced the following mechanism;

(i) Auctioneer sets up the auction and announces the details of the auction. This includes the public key of the trusted third party (e.g. through a PKI).

(ii) Bidders engage into a (proxy) secure function evaluation with the auctioneer (and the trusted third party) to generated encrypted version of their bids.

(iii) Auctioneer evaluates the garbled function. He announces based on this output the winner and information to allow bidders to verify the computation.

Observe that this can be used also for other things than just auction.

Oblivious transfer & proxy oblivious transfer

Let a, b be the communicating parties. Let a have input (m_0, m_1) and let b have input $\sigma \in \{0, 1\}$. Then using *oblivious transfer* a can share m_σ to b, so that a will not learn σ and b will not learn $m_{1-\sigma}$.

Naor, Pinkas & Sumner introduce a *proxy oblivious transfer* that has parties a, b, c such that they have inputs (m_0, m_1), $\sigma \in \{0, 1\}$ and nothing, respectively. The proxy oblivious transfer makes sure that c obtains m_σ, but no information about σ nor $m_{1-\sigma}$. Similarily, a does not learn σ, and b does not learn m_0 nor m_1.

This proxy oblivious transfer is used in the auction mechanism with a, b, c being the trusted third party, the bidders, and the auctioneer, respectively.

Secure function evaluation; gate circuits

Let us consider following simple gate;

$$g : \{0,1\} \times \{0,1\} \to \{0,1\}.$$

Now, we want to garble this gate and still be able to compute with it.

Take i to denote a wire in the gate circuit. $b_i \in \{0,1\}$ be its value, and $\pi_i : \{0,1\} \to \{0,1\}, b_i \mapsto c_i$ be a randomly chosen permutation. Write $\langle W_i^{b_i}, c_i \rangle$ for the value of the garbled wire, where $W_i^{b_i} \in \{0,1\}^t$ with t being some security parameter, and $W_i^{b_i}$ are randomly selected.

Now, basic idea is to show that there exists a map

$$g^* : \langle \{0,1\}^t, \{0,1\} \rangle \times \langle \{0,1\}^t, \{0,1\} \rangle \to \langle \{0,1\}^t, \{0,1\} \rangle$$

that is the garbled version of the map g.

Garbled gates

The garbled gate g^* can be implemented by a use of a pseudo-random function $F : \{0,1\}^t \times \{0,1\} \to \{0,1\}^{t+1}$.
Assume the fan-in wires have values $\langle W_i^{b_i}, c_i \rangle$ and $\langle W_j^{b_j}, c_j \rangle$. Further the fan-out wire has value $\langle W_k^{b_k}, c_k \rangle$.

Thus we tabulate all the 4 possibilities as follows;

$$(c_i, c_j) : \langle W_k^{g(b_i,b_j)}, c_k \rangle \oplus F_{W_i^{b_i}}(c_j) \oplus F_{W_j^{b_j}}(c_i).$$

Clearly given the fan-ins we can compute the fan-out $\langle W_k^{b_k}, c_k \rangle$ using this table.

The security is based on the fact that F is pseudo-random function, and the values $W_i^{b_i}$ are random and unique.

Creating the circuit

In the Naor, Pinkas & Sumner mechanism the input to the generated gates is created using proxy oblivous transfer.

The trusted third party generates the auction circuit (by a specification submitted by the auctioneer) and then garbles it. After this the TTP, each bidder and the auctioneer engage into a proxy oblivious transfer.

Thus, TTP has a pair (m_0, m_1) and the bidder choose $\sigma \in \{0, 1\}$ s.t. auctioneer obtains m_σ and nothing else.

Hence the auctioneer obtains the input to the garbled circuit and can evaluate the circuit.

Security aspects

Naor, Pinkas & Sumner state following security issues;

(i) Non-malleability of the encryption scheme. The scheme used to encrypt the bids (in the proxy oblivious transfer) should not allow meaningful malicious modification.

(ii) Replay attacks against bids, and freshness of the garbled circuit.

(iii) Verification of the output. The trusted third party can supply verification information, and the auctioneer needs to publish this.

(iv) Corrupted “trusted” third party.

(v) Denial of service by bidders.

Revalation principle

The mechanism introduced did not require anything particular about the auction mechanism, except that it should be a *direct sealed-bid* auction.

What is remarkable is that following holds; for any *indirect mechanism* there exists an equivalent *direct mechanism*. This is called the *revelation principle*.

Here we are interested in the situation where the dominant strategy is to tell the truth. Like in the Vickrey auction we could as well set $\ell_b(o) = v_b(o)$.

Generalized Vickrey auction I

Before we can look at the revelation principle closer it is worthwhile to look at the generalized Vickrey auction.

Let S denote the set of states, that indicate the distribution of goods between the bidders $b \in B$. That is, given $s \in S$ we can take $s(b)$ indicate the goods in the possession of b when in the state s.

We take some $s_0 \in S$ as the start state, and each bidder $b \in B$ tries to maximize $u(s_1)$, for some terminating state $s_1 \in S$.

A state transition $S \to S$ may be appropriately constrainted. For example, we may require that total number of goods is invariant through state transition.

Generalized Vickrey auction II

The auction is run as follows;

(i) Each bidder $b \in B$ submits a function $r_b : S \to \mathbb{R}$ to the center. (It is the "utility" function of the bidder b.)

(ii) The center uses some state transition $\alpha : S \to S$, that maximizes $\sum_{b \in B} r_b(\alpha(s_0))$.

(iii) The center also calculates transition $\beta_b : S \to S$ that maximizes $\sum_{b' \in B, b \neq b'} r_{b'}(\alpha(s_0))$.

(iv) The payoff for the bidder $b \in B$ is $\sum_{b' \in B, b' \neq b} r_{b'}(\alpha(s_0)) - r_{b'}(\beta_b(s_0))$.

Generalized Vickrey auction III

To maximize

$$u_b(\alpha(s_0)) + \sum_{b' \in B, b' \neq b} (r_{b'}(\alpha(s_0)) - r_{b'}(\beta_b(s_0))),$$

the bidder $b \in B$, would like to optimize her "utility" function r_b. Assume b submits her true utility function u and obtains

$$u_b(\alpha(s_0)) + \sum_{b' \in B, b' \neq b} (r_{b'}(\alpha'(s_0)) - r_{b'}(\beta_b(s_0))).$$

Now b wishes to maximize

$$\sum_{b' \in B, b' \neq b} (r_{b'}(\alpha(s_0)) - r_{b'}(\alpha'(s_0))).$$

However, player b can only affect this indirectly through α and α'. But those are maximized by the center and thus α' must dominate.

Revelation principle

Let us follow R. Varian to “prove” revelation principle.

Let u_b^t be the utility function with “type” t. Let $r = (r_1, \dots, r_n)$ be a set of reported utility “types” to the center. Further $x(r)$ implements the mechanism.

Truthtelling dominates iff

$$u_b^t(x(r_1, \dots, t_b, \dots, r_n)) \geq u_b^t(x(r_1, \dots, r_b, \dots, r_n)),$$

for all r_i.

The point is that for any other mechanism y such a relation can only exists if t_b depends directly on the type of the utility function. Hence as there is no real incentive in designing mechanisms that do not reveal the true type of the utility function.

This implies that we can happily restrict to *direct mechanisms*.

Interplay of game theory and cryptography

The interplay of cryptography and game theory seems to work here as follows;

(i) First you have a game theoretical problem (like auctions);

(ii) Then you generalize (and throw out game theory), and solve it in cryptographical context.