Handout 9: Chosen Ciphertext Security

Boaz Barak

Total of 100 points.
Exercises due November 29th, 2005 1:30pm.

Exercise 1 (Login protocol needs CCA - 50 points)**.** Consider the following login protocol mentioned in class:

- Client and server share secret PIN chosen at random from $\{0,1\}^\ell$.
- Client and server has public encryption key e of server.
- To login, client sends encryption of PIN with key e to server.
- If PIN is valid then server sends "START" message to client. Otherwise it aborts.

1. Give an example for a CPA-secure public key encryption such that if it is used in this protocol then the protocol is *not* secure: an active person-in-the-middle adversary can recover the PIN by intercepting $O(\ell)$ sessions.
2. Show that if the encryption scheme used is CCA secure and an adversary can interact with the client and server at most m times, then its probability of guessing the PIN is at most $O(\frac{m}{2^\ell})$.

Exercise 2 (Non malleability of CCA secure schemes - 50 points)**.** An attractive way to perform a bidding is the following: the seller publishes a public key e. Each buyer sends through the net the encryption $\mathsf{E}_e(x)$ of its bid, and then the seller will decrypt all of these and award the product to the highest bidder.

One aspect of security we need from $\mathsf{E}(\cdot)$ is that given an encryption $\mathsf{E}_e(x)$, it will be hard for someone not knowing x to come up with $\mathsf{E}_e(x+1)$ (otherwise bidder B could always take the bid of bidder A and make into a bid that is one dollar higher). You'll show that this property is also related to CCA security:

1. Show a CPA-secure public key encryption such that there is an algorithm that given e and a ciphertext $y = \mathsf{E}_e(x)$, converts y into a ciphertext y' that decrypts to $x+1$. (If it makes your life easier, you can make the algorithm work only if x is, say, a multiple of 100.)
2. Show that if E is CCA secure then there is no such algorithm. In particular show that if M is any polynomial time algorithm, and X is a set of possible numbers x, then

$$\Pr_{(e,d)\leftarrow\mathsf{G}(1^n)}[\mathsf{D}_d(M(e,\mathsf{E}_e(x))) = x+1] < \tfrac{1}{|X|} + n^{-\omega(1)}$$

Exercise 3 (0 points)**.** The proof for the CCA secure scheme given in class was a bit handwavy. Go over the notes and make sure you understand it. For double the points, go over the proof the OAEP+ scheme in Shoup's paper (see link on website) and make sure you understand it. For triple the points, do this for Boneh's scheme (see link on web site).