6.875J/18.425J Cryptography and Cryptanalysis November 28, 2001

Lecture 22

Instructor: Anna Lysyanskaya *Scribed by: Ryan Wagner*

1 Outline

1. Discussion and ITMs.
2. Commitment Scheme
   a) Definition
   b) Constructions
   c) Applications

2 Discussion of Protocols

The purpose of a protocol is to realize some sort of functionality. For example, protocols can be used to realize the functionality of non-interactive applications such as encryption or signature generation. In this lecture we will examine how protocols can be used in the context of interactive applications, specifically for commitment schemes.

3 Coin Flipping

Suppose Anna and Adrian are planning a date (never mind any ethical issues this might raise about the lecturer/student relationship). Adrian is a cheap date and would prefer to eat Chinese food. Anna, on the other hand is a gourmand, and would like Adrian to spring for a dinner at the Blue Room.[1] They decide that the only fair way to choose a restaurant is to flip a coin. Unfortunately, they are on the phone and neither person trusts the other, so they need a way to simulate a coin flip in a fair manner.[2]

[1]See http://www.zagat.com/search/Details.asp?RID=894&NDPH=blue+room&VID=1&PID=1&LID=3 for a restaurant review

[2]See Blum, M., "Coin Flipping by Telephone," Proc. IEEE Spring COMPCON (1982), 133-137.

3.1 Try 1

Anna: Encrypts a 0 and a 1 and sends to Adrian in random order

Adrian: Chooses one of the ciphertexts

Anna: Decrypts both ciphertexts

There is a problem in this scheme. Encryption is not designed to handle this application. We need another building block.

3.2 Try 2–Commitment Scheme

Anna: Puts a 0 and a 1 into two envelopes and sends to Adrian in random order

Adrian: Chooses one of the envelopes

Anna: Opens both envelopes and examines the contents. If the envelopes do not open correctly, then refuses to go with Adrian.

We have two things to formalize about this protocol:

1. What is interaction and how do we model it?

   Answer: Interactive Turing Machines (ITMs)

2. What is a "secure envelope" (AKA a "commitment scheme")?

4 Interactive Turing Machines (ITMs)

4.1 Definition

To answer question 1 above, we begin with a standard Turing machine. To be interactive, we add two tapes in addition to the default tape: T_{send} and $T_{receive}$. T_{send} contains the data that Turing machine T sends to others, and $T_{receive}$ logs the data T receives from others. T operates in rounds. That is, in the "send" round, it writes output to its T_{send}, and in the "receive" round, it reads data from its $T_{receive}$.

Two ITMs, A and B, are communicating if A's T_{send} is B's $T_{receive}$ and vice versa.

4.2 Notation

If A and B are ITMs, then

$$a \leftarrow (A(x) \leftrightarrow B(y)) \rightarrow b \tag{1}$$

The notation "$(A(x) \leftrightarrow B(y))$" means that A and B are communicating. x and y are respectively A's and B's input on their normal, default tapes. a is A's output, b is B's output.

5 Definition of Commitment Schemes

A commitment scheme (secure envelope) consists of two stages–the *Commit Stage* and the *Reveal Stage*. In the *Commit Stage*, a secret is put into an envelope; in the *Reveal Stage*, the envelope is opened. Now that we have notation and terminology in place, we can work out the details of what criteria a commitment scheme must meet. We will do this in the context of an auction in which the parties do not know each others' bids. A good scheme consists of efficient algorithms for the Committer (A) and the Receiver (B) such that they have the following three properties:

Correctness If we put a 0 in, a 0 comes out. A bidder would want to have his bid correctly revealed. It would be really unfortunate to bid \$100 for a lamp, but have the bid revealed to be \$100,000! This is similar to the faithfulness requirement for encryption schemes.

$$\begin{aligned} &Pr[u \leftarrow A(1^k, b, \text{“Commit”}) \leftrightarrow B(1^k, \text{“Commit”}) \rightarrow v; \\ &\quad A(1^k, u, \text{“Reveal}) \leftrightarrow B(1^k, v, \text{“Reveal”}) \rightarrow b' : b = b'] = 1 \end{aligned}$$

Secrecy No matter what Bob does, he can't know what's in the envelope. This might cause him to consistently bid \$1 over Alice, rather than bidding the maximum price he is willing to pay for an item. Again, this is very similar to what we have seen before in encryption schemes.

$$\begin{aligned} &\forall \{C_k\} \in IPPTF\ \exists \nu(k) \text{ such that} \\ &\quad \Pr[b \leftrightarrow 0, 1; u \leftarrow A(1^k, b, \text{“Commit”} \leftrightarrow C_k(1^k, \text{“Commit”}) \rightarrow b' : \\ &\quad b' = b] \leq 1/2 + \nu(k) \end{aligned}$$

Note that $PPTF$ is now $IPPTF$, since the protocol is interactive.

Binding We cannot open the envelope different ways to have different outputs. This is new. In an encryption scheme, we do not care if it is possible to decrypt something multiple ways. In fact, that might be an advantage, since it would keep the adversary guessing what the input was. In a commitment scheme, however, we must be unambiguous. This could allow Alice to effectively change her bid after the auction closes.

$$\begin{aligned} &\forall \{C_k\} \in IPPTF\ \exists \nu(k) \text{ such that} \\ &\quad \Pr[u \leftarrow C_k(1^k) \leftrightarrow B(1^k, \text{“Commit”}) \rightarrow v : \\ &\quad C_k(u, 0) \leftrightarrow B(1^k, v, \text{“Reveal”}) \rightarrow b'_0; \\ &\quad C_k(u, 1) \leftrightarrow B(1^k, v, \text{“Reveal”}) \rightarrow b'_1 : b'_0 \neq b'_1] < \nu(k) \end{aligned}$$

This property is the one that sets commitment schemes apart from encryption and is why we must use a commitment scheme rather than encryption to effectively perform the coin flip over the telephone.

As an exercise, show that the above definition of binding is equivalent to the following one:

$\forall \{C_k\} \in IPPTF \; \exists \nu(k)$ such that

$\Pr[u \leftarrow C_k(1^k) \leftrightarrow B(1^k, \text{“Commit”}) \rightarrow v :$
$C_k(u, 0) \leftrightarrow B(1^k, v, \text{“Reveal”}) \rightarrow b'_0;$
$C_k(u, 1) \leftrightarrow B(1^k, v, \text{“Reveal”}) \rightarrow b'_1 : b'_0 = 0 and b'_1 = 1] < \nu(k)$

6 Constructions of Commitment Schemes

6.1 OWP-based

Let p be a OWP. If p is a OWP, then consider p': $p'(x \circ b) = p(x) \circ b$. Let B be a hard core bit for p.

Commit: On input $(1^k, b, \text{“Commit”})$, A chooses a random r such that $B(r) = b$ and sends $p(r) = v$.

Reveal: A sends r.

B outputs $B(r)$ and verifies that $v = p(r)$.

Since v is the result of the OWP, it is hard to reverse the permutation to recover r, which would allow Bob to calculate b easily. Alice cannot change her commitment to r, since she cannot guess a different r' such that $r' \neq r$ and $p(r) = p(r') = v$. The proofs that this is a commitment scheme should be clear.

6.2 PRG-based

Let G be a PRG. This is a weaker assumption than using a OWP, since $OWP \Rightarrow PRG$, but PRGs are not known to imply OWPs.

Commit: **Bob** chooses a $3k$ bit random R and sends R to Alice.

Alice chooses a k-bit seed s. If $b = 0$, she sends Bob $G(s)$. If $b = 1$, she sends Bob $G(s) \oplus R$.

Bob 's output v is Alice's message.

Reveal: **Alice** sends Bob s, b.

Bob verifies that $v = G(s) \oplus R$ if $b = 1$ or $v = G(s)$ if $b = 0$. If he cannot verify the commitment, he outputs “REJECT.”

Bob does not know if his v is $G(s)$ or $G(s) \oplus R$. The only way for him to find out would be to break G and hope that either $G^{-1}(v)$ or $G^{-1}(v \oplus R)$ does not have a corresponding seed s. If one does and the other does not, then he knows the value of b. However, G would not be a PRG any more.

6.2.1 Proof of Correctness

This should be straightforward.

6.2.2 Proof of Secrecy

Suppose the above construction does not meet the secrecy property. Then, we will try to break the PRG. We do this by using a reduction. In the reduction, the adversary is on Bob's side. The input is the string r. Bob sends R. We pick a random b. If $b = 0$, we send r; if $b = 1$, we send $r \oplus R$.

Claim 1: If r is pseudorandom, then adversarial Bob's success in guessing b is $1/2+\varepsilon(k)$.

Claim 2: If r is random, then his success is equal to $1/2$. By an argument we have seen before in various contexts, we know that our reduction should, if Bob guesses correctly, output "pseudorandom;" if he guesses incorrectly, it should output "random." We will be correct with probability $1/2 + \varepsilon(k)/2$ because

$$Pr[\text{correct}] = Pr[\text{correct}|r \text{ random}] \cdot \frac{1}{2} + Pr[\text{correct } |r \text{ pseudorandom}] \cdot \frac{1}{2} \tag{2}$$

$$= \frac{1}{2} \cdot \frac{1}{2} + (\frac{1}{2} + \varepsilon(k)) \cdot \frac{1}{2} = \frac{1}{2} + \frac{\varepsilon(k)}{2} \tag{3}$$

6.2.3 Proof of Binding

Suppose we have a bad R such that there exists an s_1 and s_2 such that $G(s_1) = R \oplus G(s_2)$. How many Rs like that are there? For any pair (s_1, s_2), there is a unique R that satisfies these properties. This R is $R_{s_1 s_2} = G(s_1) \oplus G(s_2)$. There are 2^k choices for each s_1 and s_2, so there are

$$\binom{2^k}{2} + 2^k \leq 2^{2k} \tag{4}$$

bad Rs, but we (Bob) chose a *random* R, of which there are 2^{3k}, so

$$Pr[R \text{ bad}] = \frac{2^{2k}}{2^{3k}} = 2^{-k} \tag{5}$$

due to Naor.[3]

7 Application for Coin Flipping

Let us look at the plausibility of different ways of cheating using our coin flipping protocol:

- The probability of any value is $\leq 1/2 + negl$.
- If Anna is playing by the rules and Adrian tries to pick the 0 envelope with probability $\geq 1/2 + \varepsilon(k)$, then he breaks the secrecy property of the commitment scheme.
- If Adrian is playing by the rules and Anna cheats, she breaks the binding property of the commitment scheme.

[3] See Naor, "Bit Commitment Using Pseudo-Randomness," Journal of Cryptology 4(2) 151-158, 1991.

Question: Can it be possible that $Pr[0] > Pr[1]$ by a lot?

Adrian cheats: He can try to cheat by being silent. However, Anna simply does not go to dinner with Adrian, so this decreases the probability of both values.

Anna cheats: If the *Reveal* stage results in the Blue Room, she goes to dinner with Adrian. If it results in Chinese food, she stands him up.

As a challenge, reduce the unfairness to $1/poly$. *Hint: Do by rounds and pick the majority.*

8 Other Applications

1. As a building block for Zero Knowledge proofs (see next lecture). ZK Proofs are a way to convince someone of the truth of something without explaining why. Examples uses include graph coloring and signatures.

2. Secure two party computations. Anna and Moses have decided it would be nice to bring doughnuts and juice to 6.875 lectures for the rest of the term. They agree that the cost should be paid by the wealthier of the two, but they do not want to tell each other how much money they are worth. They can determine who has more money without giving away their net worths.

3. Secure multi-party computations. Similar to above, but with more players.