CS276 Cryptography **Spring 2004**

Lecture 19a: 2004.04.05

Lecturer: David Wagner *Scribe: Colin Dewey*

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

19.1 Bit commitment

Suppose that Alice is at a horse race and wants to place a bet on her favorite horse. She could just tell the bookie, Bob, what horse she is betting on and give him her money, but what if Bob is dishonest? If Bob knows Alice's bet, he could fix the race so that he makes the most money. A simple solution would be for Alice to place her bet in a sealed envelope (the *commitment* protocol) and only open the envelope in front of Bob after the race is over (the *opening* protocol). This scheme has two properties: it is both *concealing* and *binding*. It is *concealing* because Bob does not learn anything about Alice's bet from the sealed envelope and it is *binding* because when the envelope is opened in front of both Alice and Bob, Bob is certain that what is inside the envelope is Alice's original bet (Alice is unable to change her bet after submitting the sealed envelope).

How could we do this electronically? In the simplest case, Alice wants to commit to a (bit) value $x \in \{0, 1\}$. A common scheme for bit commitment is shown in Figure 19.1. In the *commitment* phase, Alice decides on a value for $x \in \{0, 1\}$ and sends to Bob the value $C(x, r)$, where C is a function with certain properties and $r \leftarrow \{0, 1\}^n$. Then in the *opening* phase, Alice sends to Bob the values of both x and r and Bob confirms that these values are consistent with the value he received in the *commitment* phase.

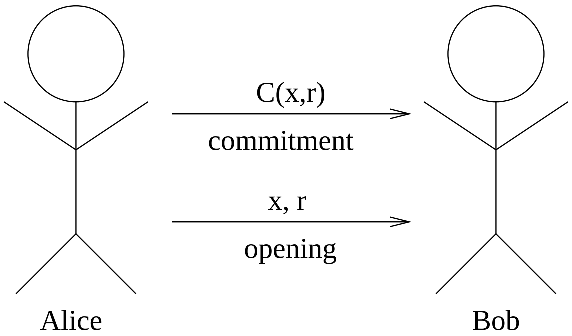

Figure 19.1: A common scheme for bit commitment

For this scheme to be *concealing*, we must have that

$$\forall x_0, x_1 \in \{0, 1\},\ C(x_0, r) \sim C(x_1, r)$$

And for this scheme to be *binding*, we must have that

$$\nexists x, r, x', r' \text{ s.t. } C(x, r) = C(x', r') \text{ and } x \neq x'$$

What function C can we use that has these properties? We will now show that a one-way permutation (OWP) can give us these properties.

19.1.1 OWP $\rightarrow$ Bit commitment

Let $f : \{0,1\}^n \rightarrow \{0,1\}^n$ be a OWP with a hardcore predicate $h : \{0,1\}^n \rightarrow \{0,1\}$. Goldreich-Levin tells us that if there exists a OWP, then a OWP with such a hardcore predicate also exists. Now we define our concealing function as

$$C(x, r) = (f(r), h(r) \oplus x), \text{ where } r \leftarrow \{0,1\}^n$$

From the definition of a hardcore predicate, one can not guess $h(r)$ given $f(r)$ with probability greater than $\frac{1}{2} + \epsilon$. Therefore, it is easy to see that

$$(f(r), h(r)) \sim (f(r), h(r) \oplus 1)$$

and thus C is concealing. Since f is a OWP, there is only one value for r which gives $f(r)$. Thus, C is also binding.

19.1.2 PRG $\rightarrow$ Bit commitment

We just showed that one can achieve bit commitment if there exists a OWP. We can use a weaker assumption, that of the existence of a PRG, to achieve bit commitment. Let $G : \{0,1\}^n \rightarrow \{0,1\}^{3n}$ be a PRG. In a previous lecture we showed that if there exists a PRG $G' : \{0,1\}^n \rightarrow \{0,1\}^n$, then there also exists a PRG G. We will use G in a bit commitment scheme shown in Figure 19.2.

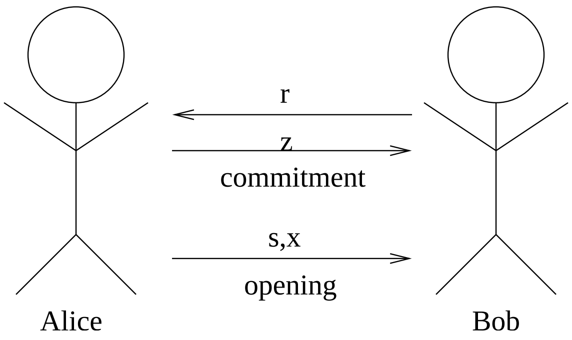

Figure 19.2: Bit commitment with a PRG

For the commitment protocol, Bob first sends Alice a random value $r \leftarrow \{0,1\}^{3n}$. Alice then generates a value $s \in \{0,1\}^n$ and sends a value z, defined as

$$z = \begin{cases} G(s) & \text{if } x = 0 \\ G(s) \oplus r & \text{if } x = 1 \end{cases}$$

For the opening protocol, Alice sends Bob the values of x and s.

To show that this scheme has the concealing property, we use a hybrid argument. When $x = 0$, Alice sends $G(s)$ and when $x = 1$, Alice sends $G(s) \oplus r$. Since G is a PRG, $G(s) \sim u$, where u is the uniform distribution.

Therefore,

$$\forall r,\ G(s)\ \sim\ u\ \equiv\ u \oplus r\ \sim\ G(s) \oplus r$$

And by the triangle inequality,

$$\forall r,\ G(s) \sim G(s) \oplus r$$

Which shows that this scheme has the concealing property. How about the binding property? Alice can actually cheat if, after having received r from Bob, she can find a pair of values s, s' such that $G(s) = G(s') \oplus r$. By the union bound, the probability of such a pair of values existing is

$$\begin{aligned}
\Pr_{r \leftarrow \{0,1\}^{3n}} [\exists s, s' \text{ s.t. } G(s) = G(s') \oplus r] &\leq \sum_{s,s' \in \{0,1\}^n} \Pr_{r \leftarrow \{0,1\}^{3n}} [G(s) \oplus G(s') = r] \\
&= \sum_{s,s' \in \{0,1\}^n} 2^{-3n} \\
&= 2^{2n} \cdot 2^{-3n} \\
&= 2^{-n}
\end{aligned}$$

Therefore, we can make this probability as small as we like by choosing the length n. We will say that this is good enough for the binding property.

19.1.3 More implications

Since PRG $\rightarrow$ bit commitment and OWF $\leftrightarrow$ PRG, it must be that OWF $\rightarrow$ bit commitment. It can also be shown that bit commitment $\rightarrow$ OWF, which means that bit commitment is equivalent to OWF. Figure 19.3 shows the implications that we have discussed thus far.

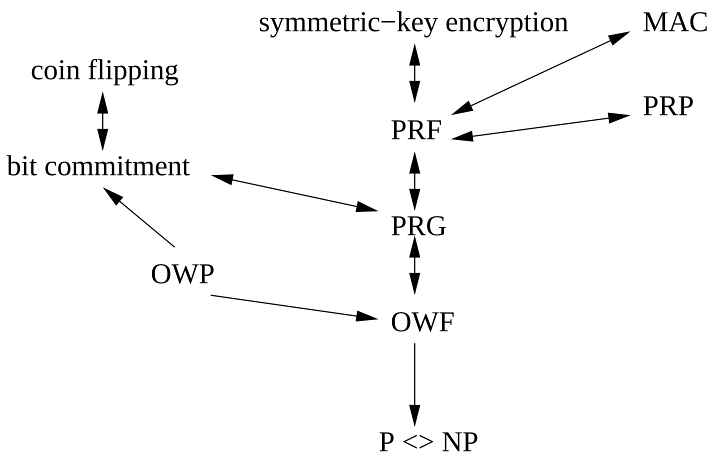

Figure 19.3: Cryptographic implications

19.2 Coin Flipping

Suppose now that Alice and Bob are on the phone and would like to flip a coin fairly to make some decision. It turns out that we can use a modified bit commitment scheme to implement coin flipping. FIgure 19.4 shows a coin flipping scheme where $x, x' \in \{0,1\}$ and $C(x,r)$ is a function like that in section 19.1.1.

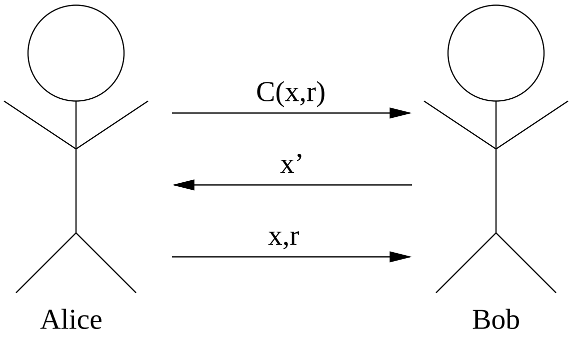

Figure 19.4: A coin flipping scheme

The outcome of the coin toss is $x \oplus x'$. This is secure because Bob learns nothing about x from $C(x, r)$ and therefore can do no better than to pick a x' at random. By using a bit commitment protocol, we assure that Alice can not change x after receiving x' from Bob.