Commitment Schemes

Cryptography and Protocols
Andrei Bulatov

Commitment

- Making a bet
- Flipping a coin by phone

- **Definition**

A commitment scheme Com is an unkeyed family of functions $\{f_n\}$ that take two inputs: a plaintext P and randomness r

Choose a plaintext and randomness, and publish $Com(P, r)$. To verify the commitment publish r.

Properties of Commitment Schemes

- Secrecy / Indistinguishability

  For every $P, P' \in \{0,1\}^m$ distribution $Com(P, U_n)$ is computationally indistinguishable from $Com(P', U_n)$

  (There is no way to learn anything about P)

- Binding

  For any C there is at most one P such that $Com(P, r) = C$ for some $r \in \{0,1\}^n$

  (It is not possible to come up with P, P' and r, r' such that $Com(P, r) = Com(P', r')$

- Why not encryption?

  Encryption doesn't bind.

Applications

- Making a bet

  Straightforward.

- Flipping a coin by phone
  - Alice makes a commitment and sends it to Bob
  - Bob flips a coin and sends result to Alice
  - Alice sends her randomness, thus, opening the commitment
  - Bob verifies

One-Way Permutation

- **Definition**

A set of permutations $\{f_n\}$, $f_n\colon \{0,1\}^n \to \{0,1\}^n$
is called a one-way permutation if

(a) each f_n is a permutation,

(b) f_n is computable in polynomial time in n,

(c) there is a superpolynomial pair (T, ε) such that for any Eve of time complexity at most T

$$\Pr\big[Eve\big(f_n(X)\big) = X\big] < \varepsilon$$

- Difference with PRP: A OWP is unkeyed, so there is no help to compute f^{-1}

Candidate OWP

- Multiplication

  f_n computes the product of two integers of length n/2 each

  If the Factoring Assumption holds it is a OWP

- Block ciphers. Say, $f(X) = AES_X(0^{128})$

- **Theorem**

  If a secure SES exists then an OWP exists.

- Indeed, just set $f(X) = E_X(0^n)$

  As the scheme is secure it is not possible to learn the key

Hard-Core Bits

- Let f be a OWP, that is given $y = f(x)$ it is hard to compute x. Does it mean that it is hard to compute the first bit of x?

  NO!

  For example, $f(x_1 x_2) = x_1 g(x_2)$

- **Definition**

  Let $f = \{f_n\}$ be a OWP. Let $h: \{0,1\}^* \to \{0,1\}$ be a polynomial time computable function. We say that h is a hard-core bit for f if there is a superpolynomial pair (T, ε) such that for any Eve of time complexity at most T

$$\Pr\big[Eve\big(f(x)\big) = h(x)\big] < \frac{1}{2} + \varepsilon$$

Hard-Core Bits (cntd)

- **Theorem**

  Every OWP has a hard-core bit,

- Multiplication: Parity of all bits

- Block ciphers: Any bit (hopefully)

Applications

- Commitment Schemes.

  We commit only one bit.

  Let f be a OWP and h its hard-core bit

  To commit a bit b, choose a string $r \in \{0,1\}^n$ uniformly at random and let

$$Com(b,r) = (f(r), h(r) \oplus b)$$

- Pseudo random generator

  Let f and h be OWP and its hard-core bit.

  Then the following function $G: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ is a PRG

$$G(x) = f(x) \parallel h(x)$$