CSL 759 – Cryptography and Network Security Jan 22, 2014

Lecture 8: Applications of hardcore bits and Introduction to PRG

Instructor: Shweta Agrawal *Scribe: Ujjwal Kumar Gupta*

1 Applications of Hardcore Bit

1.1 Using hardcore bit for coin tossing on the telephone

How can two parties A and B toss a fair random coin over the phone?

- **Solution-1**
  A tosses the coin and tell the result to B.

  Analysis - If only one of them actually tosses a coin, then person who tosses coin may tell lie.

- **Solution-2**
  Both players toss a coin and they take the XOR as the shared coin

  Analysis -(1) Even if B does not trust A to use a fair coin, he knows that as long as his bit is random, the XOR is also random.
  (2)Whoever reveals his result first has a disadvantage: the other person can adjust his answer to his favor.

- **Solution-3**
  Assume that A and B can not invert OWP then Scheme is as follows:
  1. Alice sends $g_f(x_A,r_A) = f(x_A), r_A$ to Bob.
  2. Bob sends $g_f(x_B,r_B) = f(x_B), r_B$ to Alice.

  3. A sends $x_A \langle\ x_A,r_A\ \rangle$
  4. B sends $x_B \langle\ x_B,r_B\ \rangle$

  5.A verifies x_B by computing $f(x_B)$ and use $x_B \oplus x_A$ as shared coin.
  6.B verifies x_A by computing $f(x_A)$ and use $x_B \oplus x_A$ as shared coin.

  Analysis -

1. B can verify that x_A is the same as in the first message by applying f_n, therefore A cannot change his result after learning B's result.Similarly, A can verify for x_B.Therefore we say A's first message as his commitment to $\langle\ x_A$,$r_A\ \rangle$.

2. B can not cheat because he can not get $\langle\ x_A$,$r_A\ \rangle$ from first message of A and hence can not change his result.Similarly A can not cheat.
   Hence Both parties (A and B) can toss a fair random coin over the phone

1.2 Using hardcore bit for one bit encryption

Bob(B) wants to send a bit b to Alice(A).Eve(E) tries to get b. Then scheme is as follows:
1. Alice has TDP f as her public key and its trapdoor information t as her secret key.
2. Bob selects a random $x \epsilon \{0,1\}^k$ and sends Alice cipher text $c = \langle f(x), h(x) \oplus b\rangle$.
3.Alice gets x from $f(x)$ using the trapdoor t;$h(x)$ is computed from x; b is obtained from $(h(x) \oplus b)$ using $h(x)$.

Analysis - (Security from E) - To learn anything about b, Eve must learn about $h(x)$.Here Eve only knows $f(x)$.Since, $h(x)$ is a hardcore and Eve cannot predict $h(x)$ given $f(x)$ better than flipping a coin,so b is completely secure.

2 Computational Indistinguishability

Definition 1 *Two ensembles x_k and $x_k^{'}$ are computationally indistinguishable if $\forall$ PPT distinguisher D,*

$$Pr_{x \leftarrow x_k}[D(x) \rightarrow 1] - Pr_{x \leftarrow x_{k'}}[D(x) \rightarrow 1] \leq negl(k)$$

Informally, if given two samples to any polynomial time distinguisher D, it does not change its behavior then these samples are called computationally indistinguishable.

3 Pseudorandom Generator (PRG)

A PRG stretches a short random input to a longer output such that output still looks same.

Definition 2 *A PRG is a deterministic polynomial computational function in $G : \{0,1\}^k \rightarrow \{0,1\}^{P(k)}$ such that*

1. *$P(k) > k$*

2. *$\forall$ PPT distinguisher D,*
   $Pr_{x \leftarrow \{0,1\}^{P(k)}}(G(x) \rightarrow 1) - Pr_{y \epsilon \{0,1\}^{P(k)}}(y \rightarrow 1) \leq negl(k)$

Theorem 1 *If f be a OWP with h be its hardcore bit then the function $G : \{0,1\}^k \rightarrow \{0,1\}^{P(k)}$ defined by $G(x) = f(x) \,||\, h(x)$ is a PRG.*

Proof. Proof By Contradiction Assume that $G(x)$ is not a PRG.
This means that $\exists$ a distinguisher C s.t.

$$Pr(C(U_{k+1}) \rightarrow 1) - Pr(C(G(x) \rightarrow 1))$$

is not negligible.
Here, U_{k+1} is Uniformly distributed string of k+1 bits.
Now we will use C to construct a PPT algorithm A that "breaks" hardcore bit h of f i.e. we will use a PPT algorithm A which computes $h(x)$ from $f(x)$ with non-negligible advantage $(\frac{1}{2} + \varepsilon)$
We construct algorithm $A(f(x) \rightarrow h(x))$ which on input $y = f(x)$,choose a random bit $b \xleftarrow{Rand.} \{0,1\}$ and run $C(y,b)$.If $(C(y,b) \rightarrow 1)$ (represent that C has identified that string is output of $G(x)$), then C outputs $h(x) = b$ else it outputs $h(x) = 1 - b$.

Clearly,$(y,b) \epsilon U_{k+1}$ because $f(x), b$ are both uniform with probability $\frac{1}{2}$.

Let $Pr(C(U_{k+1}) \rightarrow 1) = p$ then $Pr(C(G(k)) \rightarrow 1) \leq p - \varepsilon$
and

$$Pr(C(y,b) \rightarrow 1) = \frac{1}{2} * Pr(C(y,h(x)) \rightarrow 1) + \frac{1}{2} * Pr(C(y,\overline{h(x)}) \rightarrow 1) \tag{1}$$

where $\overline{h(x)}$ means $b \neq h(x)$
Thus with probability $\frac{1}{2}$ we choose $b = h(x)$ and output b with probability $< p - \varepsilon$
also with probability $\frac{1}{2}$ we choose $b = \overline{h(x)}$ and output b with probability $> 1 - (p - \varepsilon)$
i.e.

$$Pr(C(y,h(x)) \rightarrow 1) \leq p - \varepsilon \tag{2}$$

$$Pr(C(y,\overline{h(x)}) \rightarrow 1) > 1 - (p - \varepsilon) \tag{3}$$

Therefore, overall probability that A outputs $h(x)$ correctly

$$\begin{aligned} Pr(C(y,b) \rightarrow 1)) &> \frac{1}{2}(p - \varepsilon + (1 - (p - \varepsilon))) \\ &= \frac{1}{2} + \varepsilon \end{aligned} \tag{4}$$

Thus if C can break G then A can computes h(x) from f(x) with probability non-negligible $(\frac{1}{2} + \varepsilon)$. This is contradiction to the statement that h is hardcore bit of f. ■

In the next lecture we will look towards stretching of PRG outputs.