EE 720: An Introduction to Number Theory and Cryptography (Spring 2019)

Lecture 6 — January 21, 2019

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Discuss pseudorandom generators some more
- Construct a fixed-length private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.
- Prove the security of the above scheme assuming the existence of a pseudorandom generator.

2 Recap

- Recall the indistinguishability in the presence of an eavesdropper experiment
- Recall the definition of EAV-security
- Recall the definition of pseudorandom generators

3 Pseudorandom Generators

- Example of a *non-pseudorandom generator*: Define $G : \{0,1\}^n \to \{0,1\}^{n+1}$ as $G(s) = s \| \left(\oplus_{i=1}^n s_i\right)$.
- What happens if remove the restriction that D is polynomial time?
- **Exercise:** Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a pseudorandom generator with expansion factor $l(n) > n$. Assume that G is defined for all $n > 1$. Prove or disprove that the following functions are pseudorandom generators where $s \in \{0,1\}^n$, $n \geq 2$, and s_i is the ith bit of s.
  - $G_1(s) = G(s)\|0$.
  - $G_2(s) = G(s_1, s_2, \ldots, s_{|s|-1})\|s_{|s|}$.
  - $G_3(s) = G(s\|0)$.
- There is no known way to prove the unconditional existence of pseudorandom generators. We will see some constructions of stream ciphers which we hope are pseudorandom generators.

4 A Secure Fixed-Length Encryption Scheme

- Let G be a pseudorandom generator with expansion factor l. Define a private-key encryption scheme for messages of length l as follows:
  - `Gen`: On input 1^n, choose k uniformly from $\{0,1\}^n$.
  - `Enc`: Given $k \in \{0,1\}^n$ and message $m \in \{0,1\}^{l(n)}$, output the ciphertext
  $$c := G(k) \oplus m.$$
  - `Dec`: Given $k \in \{0,1\}^n$ and ciphertext $c \in \{0,1\}^{l(n)}$, output the message
  $$m := G(k) \oplus c.$$

Theorem. *If G is a pseudorandom generator, then the above construction is a fixed-length encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper, i.e. for any PPT adversary $\mathcal{A}$ there is a negligible function* **negl** *such that*

$$\Pr\left[\mathit{PrivK}^{eav}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathit{negl}(n).$$

Proof. Note that if a one-time pad is used instead of the pseudorandom generator $G(k)$, the system is EAV-secure. The key idea is that if a PPT adversary $\mathcal{A}$ can distinguish between the encryptions of m_0 and m_1, then it can distinguish between $G(k)$ and a uniformly random bitstring.

Distinguisher D: D is given a string $w \in \{0,1\}^{l(n)}$ (assume n can be determined from $l(n)$)

1. Run $\mathcal{A}(1^n)$ to obtain a pair of messages $m_0, m_1 \in \{0,1\}^{l(n)}$.
2. Choose a uniform bit $b \in \{0,1\}$. Set $c := w \oplus m_b$.
3. Give c to $\mathcal{A}$ and get b'. If $b = b'$ output 1 and output 0 otherwise.

If $\mathcal{A}$ succeeds, D decides that w is a pseudorandom string and if $\mathcal{A}$ fails D decides w is a random string.

Rest of proof done in class. $\square$

5 References and Additional Reading

- Sections 3.2,3.3 from Katz/Lindell