EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 7 — January 31, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Define pseudorandom generators
- 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

Definition. *A* ***private-key encryption scheme*** *is a tuple of probabilistic polynomial-time algorithms (Gen, Enc, Dec) such that:*

1. *The key-generation algorithm takes 1^n as input and gives key k, i.e. $k \leftarrow \mathit{Gen}(1^n)$.*
2. *For $m \in \{0,1\}^*$, $c \leftarrow \mathit{Enc}_k(m)$.*
3. *For ciphertext c, $\mathit{Dec}_k(c) = m$ or error indicator $\perp$.*

It is required that for every n, c, k, we have $\mathit{Dec}_k\left(\mathit{Enc}_k\left(m\right)\right) = m$.

2.1 Indistinguishability in the presence of an eavesdropper

Consider the following experiment $\mathtt{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n)$:

1. The adversary $\mathcal{A}$ is given 1^n and outputs a pair of arbitrary messages $m_0, m_1 \in \mathcal{M}$ with $|m_0| = |m_1|$.
2. A key k is generated using $\mathtt{Gen}$, and a uniform bit $b \in \{0,1\}$ is chosen. Ciphertext $c \leftarrow \mathtt{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. This ciphertext c is called the *challenge ciphertext.*
3. $\mathcal{A}$ outputs a bit b'.
4. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. We write $\mathtt{PrivK}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n) = 1$ if the output of the experiment is 1 and in this case we say that $\mathcal{A}$ succeeds.

Definition. *A private-key encryption scheme $\Pi = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ has* ***indistinguishable encryptions in the presence of an eavesdropper****, or is* ***EAV-secure****, if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function negl such that, for all n,*

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

3 Pseudorandom Generators

- It is not known how to construct computationally secure encryption schemes without making any assumptions. We need to assume the existence of pseudorandom generators.
- A pseudorandom generator is an efficient (polynomial-time), deterministic algorithm for transforming a short, uniform bitstring called the *seed* into a longer, "uniform-looking" or "pseudorandom" output string.
- Pseudorandomness is a property of a *distribution* on strings.
- Some desirable properties of a pseudorandom generator:
  - Any bit of the output should be equal to 1 with probability close to $\frac{1}{2}$.
  - The parity of any subset of the output bits should be equal to 1 with probability close to $\frac{1}{2}$.
- A good pseudorandom generator should pass all efficient statistical tests, i.e. for any efficient statistical test or *distinguisher* D, the probability that D returns 1 given the output of the pseudorandom generator should be close to the probability that D returns 1 when given a uniform string of the same length.

Definition. *Let l be a polynomial and let G be a deterministic polynomial-time algorithm such that for any n and $s \in \{0,1\}^n$, the result $G(s)$ is a string of length $l(n)$. We say that G is a* ***pseudorandom generator*** *if the following conditions hold:*

1. ***Expansion:*** *For every n it holds that $l(n) > n$.*
2. ***Pseudorandomness:*** *For any PPT algorithm D, there is a negligible function* $\mathtt{negl}$ *such that*
$$\left|\Pr\left[D\left(G(s)\right)=1\right]-\Pr\left[D(r)=1\right]\right| \leq \mathtt{negl}(n),$$
where the first probability is taken over uniform choice of $s \in \{0,1\}^n$ and the randomness of D, and the second probability is taken over uniform choice of $r \in \{0,1\}^{l(n)}$ and the randomness of D.

We call l the ***expansion factor*** *of G.*

- 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?
- There is no known way to prove the unconditional existence of pseudorandom generators. We will 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 $\mathtt{negl}$ such that*

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

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