CSL7480 Cryptography **16 Jan 2023**

Lecture 6: Cryptography

Lecturer: Somitra Sanadhya *Scribe: Harshita Kalani (B20CS019)*

6.1 Recap

6.1.1 PRG (Pseudorandom generator)

Let $l()$ be a polynomial and let G be a deterministic polynomial-time algorithm such that for any input $s\epsilon\{0,1\}^n$ algorithm G outputs a string of length $l(n)$.

We say that G is a pseudorandom generator if the following two conditions hold:

- 1. (Expansion:) For every n it holds that $l(n) > n$.
- 2. (Pseudorandomness:) For all probabilistic polynomial-time distinguishers D, there exists a negligible function negl such that:
$$|Pr[D(r) = 1] - Pr[D(G(s)) = 1]| < negl(n)$$
where r is chosen uniformly at random from $\{0,1\}^{l(n)}$, the seed s is chosen uniformly at random from $\{0,1\}^n$, and the probabilities are taken over the random coins used by D and the choice of r and s.

6.1.2 Some facts:

- We do not know how to unequivocally prove the existence of pseudorandom generators.
- Nevertheless, we still believe in them.
- We base this belief in part upon the fact that they exist if one-way functions do.

6.1.3 Condition for pseudo randomness

- Probability of Randomess - pseudo randomness $< \epsilon(n)$

$$|Pr[r \leftarrow \{0,1\}^{l(n)}] - Pr[s \leftarrow \{0,1\}^n]| < \epsilon(n)$$

6.1.4 Significance of negligible functions in Cryptography

if an attack succeeds in violating a security condition only with negligible probability, and the attack is repeated a polynomial number of times, the success probability of the overall attack still remains negligible.

6.2 Eavesdropping Security

Let π be the encryption scheme/cipher where,

$$\pi = (KeyGen, Enc, Dec)$$

- We construct a fixed-length encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.
- This scheme is very similar to the one-time pad, except a pseudorandom string is used as the "pad" rather than a random string.

6.2.1 The 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 $k\epsilon\{0,1\}^n$ uniformly at random and output it as the key.
- Enc: On input a key $k\epsilon\{0,1\}^n$ and a message $m\epsilon\{0,1\}^{l(n)}$, output the ciphertext $c := G(k) \oplus m$
- Dec: On input a key $k\epsilon\{0,1\}^n$ and a ciphertext $c\epsilon\{0,1\}^{l(n)}$, output the plaintext message $m := G(k)\oplus c$

6.2.2 Adversary and the Challenger

The experiment is defined for any private-key encryption scheme $\pi = (Gen, Enc, Dec)$, any adversary A, and any value n for the security parameter:

- The adversary A is given 1^n, and outputs a pair of message $m_0, m_1\epsilon M$ of the same length.
- A key k is generated by running $Gen(1^n)$, and a random bit $b \leftarrow 0, 1$ is chosen. A challenge ciphertext $c \leftarrow Enc_k(m_b)$ is computed and given to A.
- A outputs a bit b'.
- The output of the experiment is defined to be 1 if b' = b, and 0 otherwise. If the output is 1 we say that A succeeded.

Theorem:

Let G be a pseudorandom generator, then the encryption scheme defined above is a fixed-length private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper.

Proof:

Adversarial indistinguishability: An encryption scheme $\pi = (Gen, Enc, Dec)$ had indistinguishable encryption in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries A there exisits a negligible function negl such that

$Pr[Priv_{Keav}\pi(n) = 1] \leq \frac{1}{2} + negl(n)$

Let π denote the encryption scheme.
We show that if there exists a probabilistic polynomial-time adversary A for which the adversarial indistinguishability does not hold, then we can construct a probabilistic polynomial-time algorithm that distinguishes the output G from a truly random one.
Let A be a probabilistic polynomial-time adversary. We use A to construct the following distinguisher D for the pseudorandom generator G.

Distinguisher D: D is given as input $w\epsilon\{0,1\}^{l(n)}$

- Run $A(1^n)$ to obtain a pair of messages $m_0, m_1\epsilon\{0,1\}^{l(n)}$
- Choose a random bit $b \leftarrow \{0,1\}$. Set $c := wm_b$.
- Give c to A and obtain output b'. Output 1 if $b' = b$, and output 0 otherwise.

6.2.3 Limitations of current security definition

- Assumes adversary observes just one ciphertext.
- What if adversary observes two ciphertexts?

$c_1 = Enc_s(m_1) = G(s) \oplus m_1$

$c_2 = Enc_s(m_2) = G(s) \oplus m_2$

6.3 Multiple message Eavesdropping Security

- We have assumed that the adversary receives only a single ciphertext
- In reality, communicating parties send multiple ciphertexts and an eavesdropper will see many of these.
- Some form of security upgrade is required.

6.3.1 The multiple message eavesdropping experiment

The experiment is defined for any private-key encryption scheme $\pi = (Gen, Enc, Dec)$, an adversary A, and a security parameter n:

- The adversary A is given 1^n, and outputs a pairs of vectors of messages $M_0 = (m_{0,1}, ..., m_{0,t})$ and $M_1 = (m_{1,1}, ..., m_{1,t})$ with
$$|m_{0,i}| = |m_{1,i}|$$
for all i.
- A key k is generated by running $Gen(1^n)$, and a random bit $b \leftarrow \{0,1\}$ is chosen. For all i, the ciphertext $c_i Enc_k(m_b, i)$ is computed and the vector of ciphertexts $C = (c_1, ..., c_t)$ given to A.
- A outputs a bit b'.
- The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

6.3.2 Multiple vs Single Encryptions

If Π has indistinguishable multiple encryptions in the presence of an eavesdropper then Π also has indistinguishable encryptions in the presence of an eavesdropper.

Question: Are the definitions equivalent?
Answer: No, indistinguishable multiple encryptions is a strictly stronger security notion.

Example:

$$Enc_s(m) = G(s) \oplus m$$
$$Dec_s(m) = G(s) \oplus c$$

References

- cs.wellesley.edu
- cs.purdue.edu
- Wikipedia for negligible functions