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

Lecture 20 — April 4, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Discrete Logarithm Assumption
- Diffie-Hellman Assumptions
- Public-Key Encryption

2 Recap

- **Discrete Logarithms in Cyclic Groups**
  - **Definition:** If G is a cyclic group of order q with generator g, then for $h \in G$ the unique $x \in \mathbb{Z}_q$ which satisfies $g^x = h$ is called the discrete logarithm of h with respect to g.
  - The discrete logarithm problem is believed to be hard in cyclic groups of prime order. A subgroup of $\mathbb{Z}_p^*$ having prime order q is a good choice.
- **The Diffie-Hellman key-exchange protocol:**
  1. Alice runs a group generation algorithm to get (G, q, g) where G is a cyclic group of order q with generator g.
  2. Alice chooses a uniform $x \in \mathbb{Z}_q$ and computes $h_A = g^x$.
  3. Alice sends (G, q, g, h_A) to Bob.
  4. Bob chooses a uniform $y \in \mathbb{Z}_q$ and computes $h_B = g^y$. He sends h_B to Alice. He also computes $k_B = h_A^y$.
  5. Alice computes $k_A = h_B^x$.

  By construction, $k_A = k_B$.

3 Discrete-Logarithm Assumption

- For an integer N, let $\|N\|$ denote the length of the binary representation of N. Note that $\|N\| = \lfloor \log_2 N \rfloor + 1$.
- Let $\mathcal{G}$ denote a polynomial-time, group-generation algorithm. On input 1^n, $\mathcal{G}$ outputs a description of a group G, its order q (where $\|q\| = n$), and a generator $g \in G$. The running time of $\mathcal{G}$ is polynomial in n.
- **The discrete-logarithm experiment** $\texttt{DLog}_{\mathcal{A},\mathcal{G}}(n)$**:**

1. Run $\mathcal{G}(1^n)$ to obtain (G, q, g), where G is a cyclic group of order q (with $\|q\| = n$), and g is a generator of G.
2. Choose a uniform $h \in G$.
3. $\mathcal{A}$ is given G, q, g, h, and outputs $x \in \mathbb{Z}_q$.
4. The output of the experiment is defined to be 1 if $g^x = h$, and 0 otherwise.

- **Definition:** We say that **the discrete-logarithm problem is hard relative to** $\mathcal{G}$ if for all PPT algorithms $\mathcal{A}$ there exists a negligible function $\texttt{negl}$ such that $\Pr[\texttt{DLog}_{\mathcal{A},\mathcal{G}}(n) = 1] \leq \texttt{negl}(n)$.
- The discrete-logarithm assumption states that there exists a group-generation algorithm $\mathcal{G}$ for which the discrete-logarithm problem is hard.
- Groups $\mathbb{Z}_p^*$ where p is a prime are a class of cyclic groups where the discrete-logarithm problem is believed to be hard.
- **Theorem:** Let $p = rq + 1$ where p, q are primes. Then

$$G = \left\{h^r \bmod p \mid h \in \mathbb{Z}_p^*\right\}$$

  is a subgroup of $\mathbb{Z}_p^*$ of order q.
- Example: $p = 11$, $q = 5$
- Instance of a group-generation algorithm $\mathcal{G}$ with input being the security parameter 1^n
  1. Generate a uniform n-bit prime
  2. Generate an l-bit prime p such that q divides $p - 1$
  3. Choose a uniform $h \in \mathbb{Z}_p^*$ with $h \neq 1$
  4. Set $g = h^{(p-1)/q} \bmod p$
  5. Return p, q, g.

4 Diffie-Hellman Assumptions

- **The computational Diffie-Hellman experiment** $\texttt{CDH}_{\mathcal{A},\mathcal{G}}(n)$**:**
  1. Run $\mathcal{G}(1^n)$ to obtain (G, q, g), where G is a cyclic group of order q (with $\|q\| = n$), and g is a generator of G.
  2. Choose uniform $h_1, h_2 \in G$.
  3. $\mathcal{A}$ is given G, q, g, h_1, h_2, and outputs $h \in G$.
  4. The output of the experiment is defined to be 1 if $h = g^{x_1 x_2}$ where $h_1 = g^{x_1}$ and $h_2 = g^{x_2}$, and 0 otherwise.
- **Definition:** We say that **the computational Diffie-Hellman problem is hard relative to** $\mathcal{G}$ if for all PPT algorithms $\mathcal{A}$ there exists a negligible function $\texttt{negl}$ such that $\Pr[\texttt{CDH}_{\mathcal{A},\mathcal{G}}(n) = 1] \leq \texttt{negl}(n)$.

- The computational Diffie-Hellman assumption states that there exists a group-generation algorithm $\mathcal{G}$ for which the CDH problem is hard.
- If the DH is easy for some group, then the CDH is easy in the group. But it is not known if hardness of the DH problem implies the hardness of the CDH problem.
- For $h_1, h_2 \in G$, let $\mathtt{DH}_g(h_1, h_2) = g^{\log_g h_1 \cdot \log_g h_2}$.
- In the *decisional Diffie-Hellman experiment*, an adversary $\mathcal{A}$ is either given a uniform $h \in G$ or $DH_g(h_1, h_2)$ where h_1, h_2 are chosen uniformly from G. The adversary has to distinguish between the two inputs. It outputs 0 or 1 depending on which input it thinks it has been given.
- **Definition:** We say that **the decisional Diffie-Hellman problem is hard relative to** $\mathcal{G}$ if for all PPT algorithms $\mathcal{A}$ there exists a negligible function $\mathtt{negl}$ such that

$$|\Pr[\mathcal{A}(G, q, g, g^x, g^y, g^z) = 1] - \Pr[\mathcal{A}(G, q, g, g^x, g^y, g^{xy}) = 1]| \leq \mathtt{negl}(n),$$

  where the probabilities are taken over the experiment in which $\mathcal{G}(1^n)$ outputs (G, q, g), and then uniform $x, y, z \in \mathbb{Z}_q$ are chosen.
- The decisional Diffie-Hellman assumption states that there exists a group-generation algorithm $\mathcal{G}$ for which the DDH problem is hard.

5 Proof of Security of the Diffie-Hellman Protocol

- **The key-exchange experiment** $\mathtt{KE}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n)$:
  1. Two parties holding 1^n execute protocol Π. This results in a transcript $\mathtt{trans}$ and a key k output by both of the parties.
  2. A uniform bit $b \in \{0, 1\}$ is chosen. If $b = 0$ set $\hat{k} := k$, and if $b = 1$ then choose $\hat{k}$ uniformly from $\{0, 1\}^n$.
  3. Adversary $\mathcal{A}$ is given $\mathtt{trans}$ and $\hat{k}$, and outputs a bit b'.
  4. The adversary succeeds if $b' = b$ and the output of the experiment is 1. Otherwise, the output is 0.
- **Definition:** A key-exchange protocol Π is **secure in the presence of an eavesdropper** if for all PPT adversaries $\mathcal{A}$ there is a negligible function $\mathtt{negl}$ such that

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

- **The Diffie-Hellman key-exchange protocol:**

  Both Alice and Bob have common input 1^n
  1. Alice runs group-generation algorithm $\mathcal{G}(1^n)$ to get (G, q, g) where G is a cyclic group of order q with generator g.
  2. Alice chooses a uniform $x \in \mathbb{Z}_q$ and computes $h_A = g^x$.

3. Alice sends (G, q, g, h_A) to Bob.
4. Bob chooses a uniform $y \in \mathbb{Z}_q$ and computes $h_B = g^y$. He sends h_B to Alice. He also computes $k_B = h_A^y$.
5. Alice computes $k_A = h_B^x$.

- **Theorem:** If the decisional Diffie-Hellman problem is hard relative to $\mathcal{G}$, then the Diffie-Hellman key-exchange protocol Π is secure in the presence of an eavesdropper.

6 Public-Key Encryption

Definition. *A **public-key encryption scheme** is a triple of probabilistic polynomial-time algorithms ($\mathtt{Gen}$, $\mathtt{Enc}$, $\mathtt{Dec}$) such that:*

1. *The key-generation algorithm takes 1^n as input and outputs a pair of keys (pk, sk). The first key is called the **public key** and the second key is called the **secret key** or **private key**.*
2. *The encryption algorithm $\mathtt{Enc}$ generates the ciphertext $c \leftarrow \mathtt{Enc}_{pk}(m)$*
3. *For ciphertext c, the decryption algorithm uses the private key sk to output a message $m = \mathtt{Dec}_{sk}(c)$ or error indicator $\perp$.*

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

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

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

Proposition. *If a public-key encryption scheme has indistinguishable encryptions in the presence of an eavesdropper, it is CPA-secure.*

7 References and Additional Reading

- Sections 8.3.2, 8.3.3 from Katz/Lindell
- Sections 10.1,10.2,10.3 from Katz/Lindell
- Sections 11.1,11.2.1 from Katz/Lindell