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

Lecture 22 — April 8, 2019

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Public-Key Encryption Definition
- El Gamal Encryption
- Hash functions

2 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,*

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

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

Theorem. *No deterministic public-key encryption scheme is CPA-secure.*

3 El Gamal Encryption

Define a public-key encryption scheme as follows:

- `Gen`: On input 1^n run $\mathcal{G}(1^n)$ to obtain (G, q, g). Then choose a uniform $x \in \mathbb{Z}_q$ and compute $h = g^x$. The public key is $\langle G, q, g, h \rangle$ and the private key is $\langle G, q, g, x \rangle$. The message space is G.
- `Enc`: On input a public key $pk = \langle G, q, g, h \rangle$ and message $m \in G$, choose a uniform $y \in \mathbb{Z}_q$ and output the ciphertext $\langle g^y, h^y \cdot m \rangle$.
- `Dec`: On input a private key $sk = \langle G, q, g, x \rangle$ and ciphertext $\langle c_1, c_2 \rangle$, output $\hat{m} = c_2 / c_1^x$.

Theorem. *If the DDH problem is hard relative to $\mathcal{G}$, then the El Gamal encryption scheme is CPA-secure.*

4 Hash Functions

Will be covered using slides

5 References and Additional Reading

- Sections 11.1, 11.2.1, 11.4.1 from Katz/Lindell