Lecture 14: Public-key Cryptography

- Let $(G, \circ)$ be a group
- We use g^i to represent the group element $\overbrace{g \circ \cdots \circ g}^{i\text{-times}}$, and g^0 is used to represent the identity element e of the group G
- $(G, \circ)$ is a cyclic group of order N generated by $g \in G$, if

$$G = \{g^0, g^1, \dots, g^{N-1}\}$$

- In our context, $N = 2^n$ and our algorithms should be polynomial in n
- Example: $(\mathbb{Z}_n, +)$ is generated by any $g \in \mathbb{Z}_n$ such that $\text{g.c.d.}(n, g) = 1$

Some Examples of Efficient Algorithms

Given $a \in \{0, \ldots, N-1\}$, compute g^a:

- Let $G_0 = g$
- For $i = 1$ to $(n-1)$: Do $G_i = G_{i-1} \circ G_{i-1}$
- Consider the binary decomposition of n. Suppose we have, $a = \sum_{k=0}^{(n-1)} a_k 2^k$, where $a_k \in \{0, 1\}$
- Output $\alpha = \prod_{k=0}^{(n-1)} (G_k)^{a_k}$

Proof of correctness: Prove that $G_k = g^{2^k}$ and $\alpha = g^a$. Note that this algorithm is polynomial in n (if computing $\circ$ is efficient in n)

Some Examples of Efficient Algorithms

Sampling a random element in G:

- Sample $a \xleftarrow{\$} \{0, \ldots, N-1\}$
- Output $\alpha = g^a$

Discrete Logarithm Assumption (DL)

- Intuition: For appropriate groups G and generator g, given $\alpha = g^a$, for $a \xleftarrow{\$} \{0, \dots, N-1\}$, it is computationally hard to recover a
- Formally, it is defined by the following game between honest challenger $\mathcal{H}$ and arbitrary efficient adversary $\mathcal{A}$:
  1. The honest challenger $\mathcal{H}$ samples, $a \xleftarrow{\$} \{0, \dots, N-1\}$ and computes $\alpha = g^a$, and sends (g, α) to the adversary $\mathcal{A}$
  2. The adversary $\mathcal{A}$ replies back with $\widetilde{a} \in \{0, \dots, N-1\}$
  3. The honest challenger outputs $z = 1$ if and only if $a = \widetilde{a}$
- Security requirement states that $\Pr[z = 1]$ is negligible for all efficient $\mathcal{A}$

A Simple Exercise

Assuming the Hardness of Discrete Logarithm Assumption for a cyclic group $(G, \circ)$ generated by g, prove that the following function is a one-way function:

$$f(g, a) = (g, g^a)$$

Decisional Diffie-Hellman Assumption (DDH)

- Intuition: The distribution (g, g^x, g^y, g^{xy}) is indistinguishable from the distribution (g, g^x, g^y, g^z), for uniformly random x, y, z in $\{0, \dots, N-1\}$
- Experiment is defined between a honest challenger $\mathcal{H}$ and arbitrary efficient adversary $\mathcal{A}$:
    - The honest challenger sample $b \xleftarrow{\$} \{0,1\}$ If $b = 0$, sample $x \xleftarrow{\$} \{0, \dots, N-1\}$ and $y \xleftarrow{\$} \{0, \dots, N-1\}$, and define $\alpha = g^x$, $\beta = g^y$ and $\gamma = g^{xy}$. If $b = 1$, sample $x \xleftarrow{\$} \{0, \dots, N-1\}$, $y \xleftarrow{\$} \{0, \dots, N-1\}$, and $z \xleftarrow{\$} \{0, \dots, N-1\}$, and define $\alpha = g^x$, $\beta = g^y$ and $\gamma = g^z$. Send $(g, \alpha, \beta, \gamma)$ to the adversary $\mathcal{A}$
    - The adversary replies back with $\widetilde{b}$
    - The honest challenger $\mathcal{H}$ outputs $z = 1$ if and only if $b = \widetilde{b}$
- The security assumption says that, for any efficient adversary $\mathcal{A}$, there exists a negligible function ν such that $\Pr[z = 1] \leqslant \frac{1}{2} + \nu$

DDH $\implies$ DL

- Let $\mathcal{A}^*$ be an adversary that can break DL assumption and $\Pr[z = 1] = \varepsilon \geqslant 1/n^c$
- Consider the following code of $\widetilde{\mathcal{A}}$ on input $(g, \alpha, \beta, \gamma)$:
  - Let $a' = \mathcal{A}^*(\alpha)$
  - If $g^{a'} \neq \alpha$, then output $\widetilde{b} \xleftarrow{\$} \{0, 1\}$
  - If $g^{a'} = \alpha$, then:
    - If $(\beta^{a'} = \gamma)$: Output $\widetilde{b} = 0$
    - If $(\beta^{a'} \neq \gamma)$: Output $\widetilde{b} = 1$
- The probability of successfully predicting b is $(1 - \varepsilon) \cdot \frac{1}{2} + \varepsilon \cdot \left(\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \left(1 - \frac{1}{N}\right)\right) = \frac{1}{2} + \left(\varepsilon/2 - \frac{1}{2N}\right)$

Computational Diffie-Hellman Assumption (CDH)

- Intuition: Given (g, g^x, g^y) is hard to compute g^{xy}
- Experiment is defined between honest challenger $\mathcal{H}$ and arbitrary efficient adversary $\mathcal{A}$:
  - The honest challenger samples $x \xleftarrow{\$} \{0, \ldots, N-1\}$ and $y \xleftarrow{\$} \{0, \ldots, N-1\}$ and sends $(g, \alpha = g^x, \beta = g^y)$ to $\mathcal{A}$
  - The adversary $\mathcal{A}$ replies back with $\widetilde{\gamma}$
  - The honest challenger $\mathcal{H}$ outputs $z = 1$ if and only if $g^{xy} = \widetilde{\gamma}$
- Security states that for any efficient adversary $\mathcal{A}$, we have $\Pr[z = 1] \leqslant \nu$, where ν is a negligible function

Reduction Exercises

- Show that CDH $\implies$ DL (Hint: Use an adversary that finds the logarithm to find the logarithm a' of α and then compute compute g^{xy} from β and a')
- Show that DDH $\implies$ CDH (Hint: Use an adversary that helps compute g^{xy} from (g, α, β) to check whether $\gamma = g^{xy}$ or not)