Lecture 15: Key-Agreement and Public-key Encryption
Assumptions

- Decisional Diffie-Hellman (DDH). Intuition: The distribution \((g, g^x, g^y, g^{xy})\) is indistinguishable from \((g, g^x, g^y, g^z)\)
- Computational Diffie-Hellman (CDH). Intuition: Given \((g, g^x, g^y)\) it is computationally hard to compute \(g^{xy}\)
- Discrete Log (DL). Intuition: Given \((g, g^x)\) it is computationally infeasible to calculate \(x\)
- We have shown that: \(DDH \implies CDH \implies DL\)
- DDH Assumption is a much stronger assumption than CDH Assumption
We will show the existence of a group where DDH is false but CDH is believed to hold true

- Let \((\mathbb{Z}_p^*, \cdot)\) be the multiplicative group \(\mod p\), where \(p\) is a prime
- Let \(g\) be a generator for \((\mathbb{Z}_p^*, \cdot)\)
- Note: For all \(a \in \mathbb{Z}_p^*\), we have \(a^{p-1} = 1 \mod p\)
- We say that \(x\) is a square if there exists \(y\) such that \(x = y^2 \mod p\)
- Note: \(a^{(p-1)/2} \mod p\) is 1 if and only if \(a\) is a square; otherwise it is \((p-1)\)
- If \(g^x\) or \(g^y\) is a square then \(g^{xy}\) is a square with probability 1
- If \(g^x\) or \(g^y\) is a square then \(g^z\) is a square with probability 1/2
- Think: Use the above observation to distinguish \((g, g^x, g^y, g^{xy})\) from \((g, g^x, g^y, g^z)\)
We give an example of a group where we believe DDH holds

- Let $n = 2p + 1$ such that $n$ and $p$ are primes
- Let $(\mathbb{QR}_n^*, \cdot)$ be the multiplicative subgroup of $(\mathbb{Z}_n^*, \cdot)$, where $\mathbb{QR}_n^*$ is the set of all squares

We believe that DDH holds in $(\mathbb{QR}_n^*, \cdot)$
Key-agreement Protocol

General Template

- Alice samples local randomness \( r_A \)
- Bob samples local randomness \( r_B \)
- Starting with Alice, the parties interactively generate the transcript \((\tau_1, \tau_2, \ldots, \tau_{2k-1}, \tau_{2k})\)
- Alice outputs a key \( k_A \) based on her view (Alice view is \( V_A = (r_A, \tau_2, \tau_4, \ldots, \tau_{2k}) \))
- Bob outputs a key \( k_B \) based on his view (Bob view is \( V_B = (r_B, \tau_1, \tau_3, \ldots, \tau_{2k-1}) \))

- **Correctness:** \( \Pr[K_A = K_B] \geq 0.99 \)
- **Security:** For all efficient eavesdropper Eve (her view \( V_E = (\tau_1, \tau_2, \ldots, \tau_{2k}) \)) we have

\[
(K_A, V_E) \approx^{(c)} (U, V_E)
\]
2-round Key-agreement Protocol

- Alice samples $x \leftarrow \{0, \ldots, |G| - 1\}$ and sends $\alpha = g^x$ to Bob
- Bob samples $y \leftarrow \{0, \ldots, |G| - 1\}$ and sends $\beta = g^y$ to Alice
- Alice outputs $k_A = \beta^x$ and Bob outputs $k_B = \alpha^y$
- Correctness probability is 1
- Eve view $V_E = (g^x, g^y)$ and $k_A = g^{xy}$ By DDH assumption we know that $(g^{xy}, g^x, g^y) \approx (c) (g^{z}, g^x, g^y)$. Hence, this is a secure key-agreement protocol
Intuition: Alice is the receiver and Bob is the sender. At the end of 2-rounds of key-agreement, we have a secret key $k_A = k_B$ shared between the parties. Use that as a one-time pad to encrypt the message.

- Let $pk = \alpha$ and $sk = x$
- Let $Enc(m) = (\beta, c = m \cdot k_B)$
- Let $Dec(m, sk) = c \cdot (k_A)^{-1}$

Proof of security.

Intuition: The distribution of the encryptions of $m$ is computationally indistinguishable from the distribution of the encryptions of $m'$.

Prove: $(g^x, g^y, m \cdot g^{xy}) \approx (g^x, g^y, m \cdot g^z) \equiv (g^x, g^y, m' \cdot g^z) \approx (g^x, g^y, m' \cdot g^{xy})$