Digital Signatures

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

July 24, 2018

Group Theory Recap

Groups

Definition

A set G with a binary operation $\star$ defined on it is called a group if

- the operation $\star$ is associative,
- there exists an identity element $e \in G$ such that for any $a \in G$

$$a \star e = e \star a = a,$$

- for every $a \in G$, there exists an element $b \in G$ such that

$$a \star b = b \star a = e.$$

Example

- Modulo n addition on $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

Cyclic Groups

Definition

A finite group is a group with a finite number of elements. The order of a finite group G is its cardinality.

Definition

A cyclic group is a finite group G such that each element in G appears in the sequence

$$\{g, g \star g, g \star g \star g, \ldots\}$$

for some particular element $g \in G$, which is called a generator of G.

Example

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ is a cyclic group with a generator 1

$\mathbb{Z}_n$ and $\mathbb{Z}_n^*$

- For an integer $n \geq 1$, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$
  - Operation is addition modulo n
  - $\mathbb{Z}_n$ is cyclic with generator 1
- For an integer $n \geq 2$, $\mathbb{Z}_n^* = \{i \in \mathbb{Z}_n \setminus \{0\} \mid \gcd(i, n) = 1\}$
  - Operation is multiplication modulo n
  - $|\mathbb{Z}_n^*| = n - 1$ if n is a prime
  - $\mathbb{Z}_n^*$ is cyclic if n is a prime
- **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.
- Finding DLs is easy in $\mathbb{Z}_n$
- Finding DLs is hard in $\mathbb{Z}_n^*$

Cryptography based on the Discrete Logarithm Problem

Diffie-Hellman Protocol

- Alice and Bob wish to generate a shared secret key using a public channel
    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, $k_A = k_B$.
- An adversary capable of finding DLs in G can learn the key

El Gamal Encryption

- Suppose Bob wants to send Alice an encrypted message
- Alice publishes her public key $\langle G, q, g, h \rangle$
  - G is a cyclic group of order q with generator g
  - $h = g^x$ where $x \in \mathbb{Z}_q$ is Alice's secret key
- **Encryption:** For message $m \in G$, Bob chooses a uniform $y \in \mathbb{Z}_q$ and outputs ciphertext

$$\langle g^y, h^y \cdot m \rangle.$$

- **Decryption:** From ciphertext $\langle c_1, c_2 \rangle$, Alice recovers

$$\hat{m} := c_2 \cdot c_1^{-x}$$

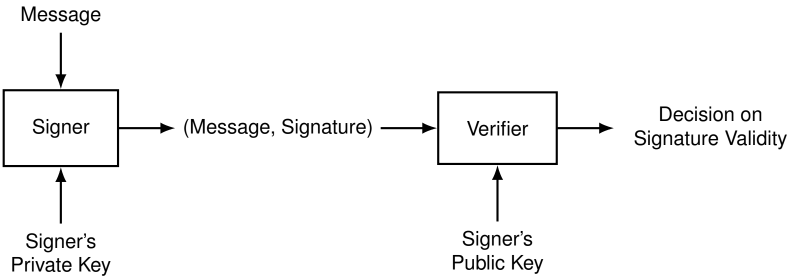
Schnorr Identification Scheme

- Let G be a cyclic group of order q with generator g
- Identity corresponds to knowledge of private key x where $h = g^x$
- A prover wants to prove that she knows x to a verifier without revealing it
  1. Prover picks $k \leftarrow \mathbb{Z}_q$ and sends initial message $I = g^k$
  2. Verifier sends a challenge $r \leftarrow \mathbb{Z}_q$
  3. Prover sends $s = rx + k \bmod q$
  4. Verifier checks $g^s \cdot h^{-r} \stackrel{?}{=} I$
- Passive eavesdropping does not reveal x
  - (I, r) is uniform on $G \times \mathbb{Z}_q$ and $s = \log_g(I \cdot y^r)$
  - Transcripts with same distribution can be simulated without knowing x
- If a cheating prover can generate two responses, he can implicity compute discrete logarithm

Digital Signatures

Digital Signatures

- Digital signatures prove that the signer knows private key
- Interactive protocols are not feasible in practice



References

- Section 10.3, 11.4, 12.5 of *Introduction to Modern Cryptography*, J. Katz, Y. Lindell, 2nd edition