Schnorr Signature Scheme

CS 601.641/441 Blockchains and Cryptocurrencies

Spring 2018
Groups

- A group $G$ is defined by a set of elements and an operation which maps two elements in the set to a third element.
- $(G, \cdot)$ is a group if it satisfies the following conditions:
  - Closure: For all $a, b \in G$, we have $a \cdot b \in G$
  - Associativity: For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - Identity: There exists an element $e$ such that for all $a \in G$, we have $e \cdot a = a$
  - Inverse: For every $a \in G$, there exists $b \in G$ such that $a \cdot b = e$
- Abelian Groups: $a \cdot b = b \cdot a$
A group \((G, \cdot)\) is a cyclic group if it is generated by a single element. That is: 
\[ G = \{1 = e = g^0, g^1, \ldots, g^{n-1}\}, \text{ where } |G| = n \]
Written as: \(G = \langle g \rangle\)
Order of \(G\): \(n\)
Discrete Logarithm Problem

- Let \((G, \cdot)\) be a cyclic group of order \(p\) with generator \(g\), where \(p\) is an \(n\)-bit prime number.
- Given \((g, b = g^a)\), where \(a \leftarrow \{0, \ldots, p - 1\}\), it is hard to predict \(a\).
Discrete Logarithm Problem: Definition

Definition (Discrete Logarithm Problem)
Let $(G, \cdot)$ be a cyclic group of prime order $p$ with generator $g$, then for every non-uniform PPT adversary $A$, there exists a negligible function $\varepsilon$ such that

$$\Pr[a \leftarrow \{0, \ldots, p-1\}, a' \leftarrow A(G, p, g, g^a) : a = a'] \leq \varepsilon$$
Schnorr Signature Scheme

Let $G$ be a cyclic group with prime order $p$

- $(sk, pk) \leftarrow \text{keygen}(1^k)$: Choose $x \leftarrow \mathbb{Z}_p$ and set $sk = x$. Set $pk = g^x$.

- $\sigma \leftarrow \text{sign}(sk, m)$: Choose $t \leftarrow \mathbb{Z}_p$ and compute $r = g^t$. Set $h = H(m, r)$ where $H$ is a hash function and $m \in \{0, 1\}^*$ is the input message. Compute $s = t + h \cdot x$ and set $\sigma = (h, s)$.

- $\{0, 1\} \leftarrow \text{verify}(pk, m, \sigma)$: Parse $\sigma$ as $(h, s)$ and output 1 if $H(m, \frac{g^s}{pk^h}) = h$, else return 0.
Let $G$ be a cyclic group with prime order $p$

- $(sk, pk) \xleftarrow{\$} \text{keygen}(1^k)$: Choose $x \xleftarrow{\$} \mathbb{Z}_p$ and set $sk = x$. Set $pk = g^x$.

- $\sigma \xleftarrow{\$} \text{sign}(sk, m)$: Choose $t \xleftarrow{\$} \mathbb{Z}_p$ and compute $r = g^t$. Set $h = H(m, r)$ where $H$ is a hash function and $m \in \{0, 1\}^*$ is the input message. Compute $s = t + h \cdot x$ and set $\sigma = (h, s)$.

- $\{0, 1\} \xleftarrow{\$} \text{verify}(pk, m, \sigma)$: Parse $\sigma$ as $(h, s)$ and output 1 if $H(m, \frac{g^s}{pk^h}) = h$, else return 0.

**Theorem (Pointcheval-Stern’96)**

Assuming the hardness of the discrete logarithm problem, Schnorr signature scheme is UF-CMA secure in the random oracle model.