# 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
- $(G, \bullet)$ is a group if it satisfies the following conditions:
  - Closure: For all $a, b \in G$, we have $a \bullet b \in G$
  - Associativity: For all $a, b, c \in G$, we have $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
  - Identity: There exists an element $e$ such that for all $a \in G$, we have $e \bullet a = a$
  - Inverse: For every $a \in G$, there exists $b \in G$ such that $a \bullet b = e$
- Abelian Groups: $a \bullet b = b \bullet a$

# Cyclic Groups

- A group $(G, \cdot)$ is a cyclic group if it is generated by a single element
- That is: $G = \{1 = e = g^0, g^1, \ldots, g^{n-1}\}$, 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 $a \xleftarrow{\$} \{0, \ldots, p-1\}$, 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 $\mathcal{A}$, there exists a negligible function $\varepsilon$ such that

$$\Pr[a \xleftarrow{\$} \{0, \ldots, p-1\}, a' \leftarrow \mathcal{A}(G, p, g, g^a) : a = a'] \leqslant \varepsilon$$

# Schnorr Signature Scheme

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

- $(sk, pk) \xleftarrow{\$} \mathsf{keygen}(1^k)$: Choose $x \xleftarrow{\$} \mathbb{Z}_p$ and set $sk = x$. Set $pk = g^x$.
- $\sigma \xleftarrow{\$} \mathsf{sign}(sk, m)$: 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 $\sigma = (h, s)$.
- $\{0,1\} \leftarrow \mathsf{verify}(pk, m, \sigma)$: Parse $\sigma$ as $(h, s)$ and output 1 if $H(m, \frac{g^s}{pk^h}) = h$, else return 0.

# Schnorr Signature Scheme

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

- $(sk, pk) \xleftarrow{\$} \mathsf{keygen}(1^k)$: Choose $x \xleftarrow{\$} \mathbb{Z}_p$ and set $sk = x$. Set $pk = g^x$.
- $\sigma \xleftarrow{\$} \mathsf{sign}(sk, m)$: 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 $\sigma = (h, s)$.
- $\{0,1\} \leftarrow \mathsf{verify}(pk, m, \sigma)$: 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.*