Proof by Reduction #1

coinstudent2048

August 22, 2021

1 The Thing

Let $\mathbb{G}$ be a cyclic group of prime order $l > 3$ and $\mathbb{F}$ be its scalar field.

Definition 1.1 (Discrete Logarithm (DL) Assumption)**.** *Let $G, H \in \mathbb{G}$. Then finding (the unique) $x \in \mathbb{F}$ such that $xG = H$ is "hard".*

Definition 1.2 ("One-time Address" (OTA) Assumption)**.** *Let $U, G \in \mathbb{G}$ whose DL relationship to each other is unknown. Let $f : \mathbb{F} \times \mathbb{F} \to \mathbb{G} \times \mathbb{G}$ be the following:*

$$(k_a, k_b) \mapsto (k_a U + k_b G, (1/k_a)G)$$

Then given $(K, L) \in \mathbb{G} \times \mathbb{G}$, finding (the unique) $f^{-1}(K, L)$ is "hard".

Definition 1.3. *A function $f : \mathbb{N} \to \mathbb{R}$ is* **negligible** *if for every polynomial $p(\cdot)$ there exists an $N \in \mathbb{N}$ such that for all integers $n > N$ it holds that $f(n) < \frac{1}{p(n)}$.*

Definition 1.3 is copied from Katz & Lindell. We first prove the following lemma:

Lemma 1.1. *If $f : \mathbb{N} \to \mathbb{R}$ is non-negligible, then $g(n) = f(n)^2$ is non-negligible.*

Proof. The non-negligibility of f means that there exists a polynomial $p(\cdot)$ such that for all $N \in \mathbb{N}$, there exists an $n > N$ such that $f(n) \geq \frac{1}{p(n)}$. Let $p_f(\cdot)$ be such polynomial and n_f be such $n > N$. Then setting $p_g(\cdot) = p_f(\cdot)^2$ and $n_g = n_f$ suffices for non-negligibility of $g(n)$ because $f(n_f) \geq \frac{1}{p_f(n)} \Rightarrow f(n_f)^2 \geq \left(\frac{1}{p_f(n)}\right)^2$. □

Theorem 1.2. *DL assumption is hard if and only if OTA assumption is hard.*

Proof. The proof consists of 2 parts:

- *DL is easy $\Rightarrow$ OTA is easy:* Applying the first DL break on $log_G(L)$ will give $1/k_a$, which will trivially give k_a. Then applying the second DL break on $log_G(K - k_a U)$ will give k_b.
- *OTA is easy $\Rightarrow$ DL is easy:* Let $A, B \in \mathbb{G}$ be the group elements to find DL for (without loss of generality, $x \in \mathbb{F}$ such that $xA = B$). Then perform the following procedure on A:
  1. Applying an OTA break on (U, A) will give $k_a, k_b \in \mathbb{F}$ such that $U = k_a U + k_b G$ and $A = (1/k_a)G$. Hence, $k_a A = G \Rightarrow U = k_a U + k_b(k_a A)$.
  2. Let $y_1 \in \mathbb{F}$ such that $U = y_1 A$. Now $U = k_a U + k_b k_a A$ becomes $y_1 A = k_a(y_1 A) + k_b k_a A \Rightarrow y_1 = k_a y_1 + k_b k_a \Rightarrow y_1 - k_a y_1 = k_b k_a$. Therefore,
  $$y_1 = k_b k_a (1/(1 - k_a)).$$

  Then perform the same procedure to B. Now we have $y_1, y_2 \in \mathbb{F}$ such that $U = y_1 A$ and $U = y_2 B$. Hence, $y_1 A = y_2 B \Rightarrow y_1(1/y_2)A = B$.

□

Remark. *Lemma 1.1 justifies the usage of two DL breaks and two OTA breaks.*