Proofs by Reduction #1

coinstudent2048

September 17, 2021

1 The Thing

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

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. *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 1.2 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 $g(n) = f(n)^m$ for any $m \in \mathbb{N}$ and $m > 1$ 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 $p_g(\cdot) = p_f(\cdot)^m$ and $n_g = n_f$ suffices for non-negligibility of g because $f(n_f) \geq \frac{1}{p_f(n_f)} \Rightarrow f(n_f)^m \geq \left(\frac{1}{p_f(n_f)}\right)^m$. $\square$

Lemma 1.1 justifies the usage of finite number of breaks in proof by reduction.

Definition 1.3 ("One-time Address" (OTA) Assumption)**.** *Let $U, G \in \mathbb{G}$ whose DL relationship to each other is unknown. Let $f : \mathbb{F} \setminus \{0\} \times \mathbb{F} \to \mathbb{G} \times \mathbb{G}$ 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".

Theorem 1.2. *OTA assumption holds if and only if DL assumption holds.*

Proof. The proof consists of 2 parts:

- *DL is easy $\Rightarrow$ OTA is easy:* Applying the first DL break on L base G will give $1/k_a$, which will trivially give k_a. Then applying the second DL break on $K - k_a U$ base G will give k_b.
- *OTA is easy $\Rightarrow$ DL is easy:* Let $A, B \in \mathbb{G}$ (both not equal to Z) 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 on B (hence another OTA break). Now we have $y_1, y_2 \in \mathbb{F}$ such that $U = y_1 A$ and $U = y_2 B$. Hence, $y_1 A = y_2 B \Rightarrow y_1(1/y_2)A = B$.

This completes the proof. $\square$

Definition 1.4 (DL "Vector" Assumption)**.** *Let $G_1, \ldots, G_n \in \mathbb{G}$ (with $n > 1$) whose DL relationship to each other is unknown. Also let $H \in \mathbb{G}$. Then finding $z_1, \ldots, z_n \in \mathbb{F}$ such that $\exists z_i(z_i \neq 0)$ and $\sum_{i=1}^{n} z_i G_i = H$ is "hard".*

Theorem 1.3. *DL Vector assumption holds if and only if DL assumption holds.*

Proof. The proof consists of 2 parts:

- *DL is easy $\Rightarrow$ DL Vector is easy:* Set random scalars on $z_2, \ldots, z_n$ so that at least one of them is not zero. Then applying DL break on $H - \sum_{i=2}^{n} z_i G_i$ base G_1 will give z_1.
- *DL Vector is easy $\Rightarrow$ DL is easy:* Set $n = 2$. Let $A, B \in \mathbb{G}$ (both not equal to Z) be the group elements to find DL for (without loss of generality, $x \in \mathbb{F}$ such that $xA = B$). Then applying a DL Vector break on $G_1 = A, G_2 = B, H = Z$ will give z_1, z_2 such that $z_1 A + z_2 B = Z$. Now we have $z_1 A + z_2(xA) = Z \Rightarrow z_1 + z_2 x = 0 \Rightarrow x = (-z_1)(1/z_2)$.

  Note that both z_1 and z_2 will never be zero, because if one of them is, then the other should also be zero, contradicting the requirement $\exists z_i(z_i \neq 0)$.

This completes the proof. $\square$