Proofs by Reduction #1

coinstudent2048

October 12, 2021

1 Mathematics

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and let $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$. Let λ be the security parameter. Let Setup be the setup algorithm: $(\mathbb{G}, \mathbb{F}) \leftarrow \mathsf{Setup}(1^\lambda)$, where $\mathbb{G}$ is a cyclic group of prime order and $\mathbb{F}$ is its scalar field. Let $Z \in \mathbb{G}$ be the identity element.

The notation $\xleftarrow{\$}$ will be used to denote for a uniformly randomly chosen element, and $(1/x)$ for the modular inverse of $x \in \mathbb{F}$. Lastly, we use additive notation for group operations.

Definition 1.1. *A function $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is* **negligible** *if for all positive 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. *An equivalent formulation of negligibility for $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is if for all $c \in \mathbb{N}$ there exists an $N \in \mathbb{N}$ such that for all integers $n > N$ it holds that $f(n) < n^{-c}$.*

Definitions 1.1 and 1.2 is copied from Katz & Lindell. We first prove the following lemma:

Lemma 1.1. *If $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is non-negligible, then $g(n) = f(n)^m$ for any $m \in \mathbb{N}$ and $m > 1$ is non-negligible.*

Proof. We use the first definition. Non-negligibility of f means that there exists a positive 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 $f(n_f) \geq \frac{1}{p_f(n_f)} \implies f(n_f)^m \geq \left(\frac{1}{p_f(n_f)}\right)^m$. □

Lemma 1.1 justifies the usage of finite number of breaks of one hardness assumption in proofs by reduction.

I'll credit the proof idea of the following lemma to Atomfried (`@atomfried:matrix.org`).

Lemma 1.2. *If there exists an $n' > N$ that makes both $f_1 : \mathbb{N} \to \mathbb{R}_{\geq 0}$ and $f_2 : \mathbb{N} \to \mathbb{R}_{\geq 0}$ non-negligible, then $g(n) = f_1(n) f_2(n)$ is non-negligible.*

Proof. We use the second definition. Non-negligibility of f means that there exists a $c \in \mathbb{N}$ such that for all $N \in \mathbb{N}$, there exists an $n > N$ such that $f(n) \geq n^{-c}$. Let c_1, c_2 be such $c \in \mathbb{N}$ for f_1 and f_2 respectively, and let n' be, as being said in the lemma statement, such $n > N$ for both f_1 and f_2. Then setting $c_g = c_1 + c_2$ and $n_g = n'$ suffices for non-negligibility of g because $f_1(n') \geq (n')^{-c_1} \wedge f_2(n') \geq (n')^{-c_2} \implies f_1(n') f_2(n') \geq (n')^{-c_1} (n')^{-c_2} = (n')^{-(c_1 + c_2)}$. □

Lemma 1.2 can be used to further generalize Lemma 1.1 to products of functions $g(n) = \prod_{i=1}^{m} f_i(n)$ through induction, *as long as* there exists an $n' > N$ that makes all f_i non-negligible.

Definition 1.3 (Discrete Logarithm (DL) Assumption)**.** *DL assumption holds relative to* Setup *if for all* PPT *adversary $\mathcal{A}$, there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that*

$$\mathsf{Pr}\left[\, H = xG \;\middle|\; \begin{array}{c} (\mathbb{G}, \mathbb{F}) \leftarrow \mathsf{Setup}(1^\lambda); G, H \xleftarrow{\$} \mathbb{G}; \\ x \in \mathbb{F} \leftarrow \mathcal{A}(\mathbb{G}, \mathbb{F}, G, H) \end{array} \right] \leq \mathsf{negl}(\lambda).$$

Definition 1.4 ("Linking Tag" (LT) Assumption)**.** *LT assumption holds relative to* Setup *if for all* PPT *adversary* $\mathcal{A}$*, there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that*

$$\mathsf{Pr}\left[\begin{array}{c} C_1 = t_k G + k_a X + k_b U \\ \wedge\ C_2 = (k_b/k_a)U \end{array} \middle| \begin{array}{c} (\mathbb{G}, \mathbb{F}) \leftarrow \mathsf{Setup}(1^\lambda); G, X, U, C_1, C_2 \xleftarrow{\$} \mathbb{G}; \\ t_k, k_a, k_b \in \mathbb{F} \leftarrow \mathcal{A}(\mathbb{G}, \mathbb{F}, G, X, U, C_1, C_2) \end{array}\right] \leq \mathsf{negl}(\lambda).$$

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

Proof. The proof consists of 2 parts:

- *DL is broken* $\implies$ *LT is broken:* Assume that $\mathcal{A}$ can break DL with non-negligible probability. Applying the first DL break on C_2 base U will give k_b/k_a. $\mathcal{A}$ sets a random k_a and computes $k_b = k_a(k_b/k_a)$. Then applying the second DL break on $C_1 - k_a X - k_b U$ base G will give t_k.

- *LT is broken* $\implies$ *DL is broken:* Assume that $\mathcal{A}$ can break LT with non-negligible probability. 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 $B = xA$). Then perform this procedure for A: applying an LT break on $(C_1, C_2) = (G, A)$ will give $t_k, k_a, k_b \in \mathbb{F}$ such that $G = t_k G + k_a X + k_b U$ and $A = (k_b/k_a)U$. Note that both k_a and k_b will never be 0 because if one of them is, then $A \neq (k_b/k_a)U$, a contradiction.

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

This completes the proof. □