Non-negligible Functions and Reduction Proofs

coinstudent2048

November 19, 2021

Abstract

We present a lemma about non-negligible functions that is helpful in reduction proofs in cryptography. We also provide a reduction proof as a demonstration.

1 The Thing

Let $\mathbb{R}_{\geq 0}$ be the set of non-negative real numbers. Let us define the concept of *negligible function* first:

Definition 1.1. *A function $f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is* **negligible** *if for all 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 1.1 is from Katz & Lindell [4]. We now prove the following lemma:

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

Proof. The function f being not negligible 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 $f(n_f) \geq \frac{1}{p_f(n_f)} \implies f(n_f)^m \geq \frac{1}{p_f(n_f)^m}$. $\square$

Lemma 1.1 justifies the usage of finite number of "breaks" of one hardness assumption in reduction proofs. For a start, the probability of breaking the hardness assumption HA is a function of the security parameter λ. Just here we denote this as $\mathsf{Pr}[\mathsf{HA}(\lambda)]$. Hence, for $m > 1$, the probability for breaking HA m times, $\mathsf{Pr}[\wedge_{i=1}^{m}\mathsf{HA}_i(\lambda)] \geq \mathsf{Pr}[\mathsf{HA}(\lambda)]^m$. Now Lemma 1.1 says that if $\mathsf{Pr}[\mathsf{HA}(\lambda)]$ is non-negligible (or equivalently, for all negligible function $\mathsf{negl}(\lambda)$, $\mathsf{Pr}[\mathsf{HA}(\lambda)] \geq \mathsf{negl}(\lambda)$), then $\mathsf{Pr}[\mathsf{HA}(\lambda)]^m$ must also be non-negligible and hence $\mathsf{Pr}[\wedge_{i=1}^{m}\mathsf{HA}_i(\lambda)]$ is also non-negligible.

2 The Demo

Let $\mathbb{G}$ be a cyclic group where the Discrete Logarithm (DL) assumption holds, and $\mathbb{F}$ be its scalar field. We now present a hardness assumption used in Bulletproofs [1], Bulletproofs+ [3], and Halo [2]:

Definition 2.1 (Discrete Logarithm Relation Assumption)**.** *DL Relation assumption holds relative to* Setup *if for all $n \geq 2$ and* PPT *adversary $\mathcal{A}$, there exists a negligible function* $\mathsf{negl}(\lambda)$ *such that*

$$\mathsf{Pr}\left[\begin{array}{c|c} \exists i \in \{1, \ldots, n\} : x_i \neq 0 & (\mathbb{G}, \mathbb{F}) \leftarrow \mathsf{Setup}(1^\lambda); \\ \wedge \sum_{i=1}^{n} x_i G_i = 0 & \{G_i\}_{i=1}^{n} \xleftarrow{\$} \mathbb{G}^n; \\ & \{x_i\}_{i=1}^{n} \leftarrow \mathcal{A}(\mathbb{G}, \mathbb{F}, \{G_i\}_{i=1}^{n}) \end{array}\right] \leq \mathsf{negl}(\lambda).$$

Note that the $\sum_i x_i G_i$ operation is also called *multi-scalar multiplication.*

Theorem 2.1. *DL relation assumption holds if and only if DL assumption holds.*

Proof. The forward direction is trivial. For the backward direction, we prove by induction on n:

Base case ($n = 2$): Assume that $\mathcal{A}$ breaks DL relation: with non-negligible probability, for $G_1, G_2 \xleftarrow{\$} \mathbb{G}$, $\mathcal{A}$ outputs $x_1, x_2 \in \mathbb{F}$ such that $x_1G_1 + x_2G_2 = 0$. Then $G_1 = (-x_2/x_1)G_2$, breaks DL assumption.

Inductive case: Assume that the backward direction of Theorem 2.1 holds for case n. Then we prove the same for case $n + 1$. Assume that $\mathcal{A}$ breaks DL relation for case $n + 1$. By Lemma 1.1, $\mathcal{A}$ can break it *twice*: with non-negligible probability, for $\{G_i\}_{i=1}^{n+1} \xleftarrow{\$} \mathbb{G}^{n+1}$, $\mathcal{A}$ outputs $\{x_i\}_{i=1}^{n+1}$ *and* $\{x'_i\}_{i=1}^{n+1}$ such that both satisfy the multi-scalar multiplication with $\{G_i\}_{i=1}^{n+1}$ to zero. Now observe that

$$
\begin{aligned}
x'_1 \sum_{i=1}^{n+1} x_i G_i = x'_1 \cdot 0 = 0 \;\wedge\; x_1 \sum_{i=1}^{n+1} x'_i G_i = x_1 \cdot 0 = 0 \\
\implies \sum_{i=1}^{n+1} x'_1 x_i G_i - \sum_{i=1}^{n+1} x_1 x'_i G_i = 0 - 0 = 0 \\
\implies \sum_{n=1}^{n+1} (x'_1 x_i - x_1 x'_i) G_i = 0 \\
\implies \sum_{n=2}^{n+1} (x'_1 x_i - x_1 x'_i) G_i = 0
\end{aligned}
$$

with the last implication because $x'_1 x_1 - x_1 x'_1 = 0$. Now the last implication has only n addends, hence this breaks DL relation assumption for case n. From the above assumption of the backward direction of Theorem 2.1 holding for case n, this must also break DL assumption. $\square$

References

[1] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. Cryptology ePrint Archive, Report 2017/1066, 2017. `https://ia.cr/2017/1066`.

[2] Sean Bowe, Jack Grigg, and Daira Hopwood. Recursive proof composition without a trusted setup. Cryptology ePrint Archive, Report 2019/1021, 2019. `https://ia.cr/2019/1021`.

[3] Heewon Chung, Kyoohyung Han, Chanyang Ju, Myungsun Kim, and Jae Hong Seo. Bulletproofs+: Shorter proofs for privacy-enhanced distributed ledger. Cryptology ePrint Archive, Report 2020/735, 2020. `https://ia.cr/2020/735`.

[4] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography: Principles and Protocols*. Chapman and Hall/CRC, 2007.