Insert Your Awesome Title Here

coinstudent2048

August 22, 2021

1 Main 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 $f^{-1}(K, L)$ is "hard".

Theorem 1.1. *DL assumption is hard if and only if OTA assumption is hard.*

(This may be false though, see "Comment")

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, $y_1 A = y_2 B \Rightarrow y_1(1/y_2)A = B$.

□

2 Comment

I have doubt on the whole proof, because of the usage of two DL breaks and two OTA breaks. Upon briefly looking on the formal version of "easy" and "hard" (negligible function), I cannot connect my intuition to it yet.