Problem 1. «CP Problem»

Let $\mathbb{G} = \langle g \rangle$ be a group of prime order q, κ is the bit length of q. Let us consider two known modifications of the discrete logarithm problem over $\mathbb{G}$, namely, s-DLOG problem and ℓ-OMDL problem. Both of them are believed to be difficult.

s-DLOG problem (with parameter $s \in \mathbb{N}$)

- Unknown values: x is chosen uniformly at random from $\mathbb{Z}_q^*$.
- Known values: $g^x, g^{x^2}, \ldots, g^{x^s}$.
- Access to oracles: no.
- The task: to find x.

ℓ-OMDL (One-More Discrete Log) problem (with parameter $\ell \in \mathbb{N}$)

- Unknown values: $x_1, x_2, \ldots, x_{\ell+1}$ are chosen uniformly at random from $\mathbb{Z}_q^*$.
- Known values: $g^{x_1}, g^{x_2}, \ldots, g^{x_{\ell+1}}$.
- Access to oracles: at most ℓ queries to O_1 that on input $y \in \mathbb{G}$ returns x such that $g^x = y$.
- The task: to find $x_1, x_2, \ldots, x_{\ell+1}$.

Consider another one problem that is close to the s-DLOG and ℓ-OMDL problems:

(k,t)-CP (Chaum—Pedersen) problem (with parameters $k, t \in \mathbb{N}$)

- Unknown values: $x_1, x_2, \ldots, x_{t+1}$ are chosen uniformly at random from $\mathbb{Z}_q^*$.
- Known values: $g^{x_1}, g^{x_2}, \ldots, g^{x_{t+1}}$.
- Access to oracles: at most k queries to O_1 that on input $(i, z) \in \{1, \ldots, t+1\} \times \mathbb{G}$ returns z^{x_i}, and at most t queries to O_2 that on input $(\alpha_1, \ldots, \alpha_{t+1}) \in \mathbb{Z}_q^{t+1}$ returns $\alpha_1 x_1 + \ldots + \alpha_{t+1} x_{t+1}$.
- The task: to find $x_1, x_2, \ldots, x_{t+1}$.

It is easy to see that if there exists a polynomial (by κ) algorithm that solves the s-DLOG problem, then there exists a polynomial algorithm that solves the $(s-1,t)$-CP problem for any $t \in \mathbb{N}$.

Problem for a special prize! Prove or disprove the following conjecture: if there exists a polynomial algorithm that solves (k,t)-CP problem, then there exists a polynomial algorithm that solves at least one of the s-DLOG and ℓ-OMDL problems, where k, t, s, ℓ are upper bounded by polynomial of κ.