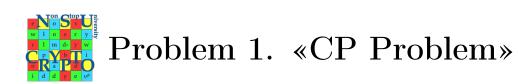
International Olympiad in Cryptography NSUCRYPTO'2022 Second round October 17-24 General, Teams



Let  $\mathbb{G} = \langle g \rangle$  be a group of prime order q,  $\kappa$  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  $\ell$ -OMDL problem. Both of them are believed to be difficult.

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

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

Consider another one problem that is close to the s-DLOG and  $\ell$ -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:	$g^{x_1}, g^{x_2}, \dots, g^{x_{t+1}}.$
<u>Access to oracles</u> :	at most k queries to $O_1$ that on input $(i, z) \in \{1, \ldots, t +$
	1} × $\mathbb{G}$ 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 $\alpha_1 x_1 + \ldots + \alpha_{t+1} x_{t+1}$ .
<u>The task</u> :	to find $x_1, x_2,, x_{t+1}$ .

It is easy to see that if there exists a polynomial (by  $\kappa$ ) 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  $\ell$ -OMDL problems, where  $k, t, s, \ell$  are upper bounded by polynomial of  $\kappa$ .



nsucrypto@nsu.ru