Analysis: Dual-Target Discrete Logarithm Assumption

koe `ukoe@protonmail.com`

May 4, 2021

Arcturus [1] depends on a novel hardness assumption called the 'dual-target discrete logarithm problem' (defined in the same paper). I demonstrate a break in that assumption.

Let the dual-target discrete logarithm challenger/adversary game play out as follows.

1. Challenger: define G and H
2. Adversary: randomly generate scalars g_i and h_i for $i = 0, ..., n-1$. Define $G_i = g_i G$ and $H_i = h_i H$.
3. Challenger: define μ^i for $i = 0, ..., n-1$.
4. Adversary: randomly generate scalars x_i for $i = 2, ..., n-1$. Define scalars x_0 and x_1 with the following procedure.

Note: Adversary wants all of the following to be true. Challenger wants at least one to be false.

- $\sum \mu^i (G_i - x_i G) = I$
- $\sum \mu^i (H - x_i H_i) = I$
- There exists an $0 \leq i < n$ such that either $x_i G \neq G_i$ or $x_i H_i \neq H$.

We can restate the first two conditions like this:

$$I = \sum_{i=0}^{n-1} \mu^i * (g_i - x_i) * G \tag{1}$$

$$I = \sum_{i=0}^{n-1} \mu^i * (1 - x_i * h_i) * H \tag{2}$$

Define the following variables (all terms are known constants):

$$\lambda_g = \mu^0 g_0 + \mu^1 g_1 + \sum_{i=2}^{n-1} \mu^i * (g_i - x_i) \tag{3}$$

$$\lambda_h = \mu^0 + \mu^1 + \sum_{i=2}^{n-1} \mu^i * (1 - x_i * h_i) \tag{4}$$

If the following scalar equalities hold, then the previous elliptic curve equalities will also hold:

$$0 = \lambda_g - \mu^0 x_0 - \mu^1 x_1 \tag{5}$$

$$0 = \lambda_h - \mu^0 x_0 h_0 - \mu^1 x_1 h_1 \tag{6}$$

There are two equations and two unknowns (x_0 and x_1). Solve and get:

$$x_1 = \quad (\lambda_h - h_0 \lambda_g)/[\mu^1 (h_1 - h_0)] \tag{7}$$

$$x_0 = -(\lambda_h - h_1 \lambda_g)/[\mu^0 (h_1 - h_0)] \tag{8}$$

Since g_i, h_i, and x_i (for $i \neq 0, 1$) are random, there is no reason to expect the third game condition to fail every time (only if you are unlucky).

Bibliography

[1] Sarang Noether. Arcturus: efficient proofs for confidential transactions. Cryptology ePrint Archive, Report 2020/312, 2020. https://eprint.iacr.org/2020/312.