On the $q$-Strong Diffie-Hellman Problem

Naoki Tanaka and Taiichi Saito
Tokyo Denki University
{tanaka@crypt.,taiichi@c.dendai.ac.jp}

Abstract. This note is an exposition of reductions among the $q$-strong Diffie-Hellman problem and related problems\(^1\).

1 The $q$-Strong Diffie-Hellman Problem

We discuss reductions among the $q$-strong Diffie-Hellman ($q$-sDH) problem [1, 3] and related problems. We use the following notation:

1. $\mathbb{G}_1$ and $\mathbb{G}_2$ are two cyclic groups of prime order $p$.
2. $g_1$ is a generator of $\mathbb{G}_1$ and $g_2$ is a generator of $\mathbb{G}_2$.
3. $\psi$ is an isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, with $\psi(g_2) = g_1$.

1.1 The $q$-Strong Diffie-Hellman Problem over Two Groups

Boneh and Boyen defined the $q$-strong Diffie-Hellman ($q$-sDH) problem in the Eurocrypt 2004 paper [1] as follows:

Definition 1 ($q$-strong Diffie-Hellman Problem). Assume that $\psi$ is efficiently computable. For an randomly chosen element $x \in \mathbb{Z}_p$ and a random generator $g_2 \in \mathbb{G}_2$, the $q$-strong Diffie-Hellman Problem is, given $(g_1, g_2, g_2^x, \ldots, g_2^{x^q}) \in \mathbb{G}_1 \times \mathbb{G}_2^q$, to compute a pair $(g_1^{1/(x+c)}, c) \in \mathbb{G}_1 \times \mathbb{Z}_p$.

This $q$-sDH problem is defined based on two groups $\mathbb{G}_1$ and $\mathbb{G}_2$. We call this problem the Eurocrypt 2004 version $q$-sDH problem.

They defined a variant of the $q$-sDH problem in the Journal of Cryptology paper [2] as follows:

Definition 2 ($q$-strong Diffie-Hellman Problem (Journal of Cryptology version)). For an randomly chosen element $x \in \mathbb{Z}_p$ and random generators $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, the $q$-strong Diffie-Hellman Problem is, given $(g_1, g_1^x, \ldots, g_1^{x^q}, g_2, g_2^x) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$, to compute a pair $(g_1^{1/(x+c)}, c) \in \mathbb{G}_1 \times \mathbb{Z}_p$.

They said that this Journal of Cryptology version $q$-sDH problem is harder than the Eurocrypt 2004 version $q$-sDH problem, as $\psi$ is the former no longer requires the existence of efficiently computable isomorphism $\psi$. We easily see that the Eurocrypt 2004 version problem is reducible to the Journal of Cryptology version problem as follows: for a given $(g_1, g_2, g_2^x, \ldots, g_2^{x^q})$, we compute $g_i^t = \psi(g_2^i)$ for $i (1 \leq i \leq q)$ to obtain $(g_1, g_1^x, \ldots, g_1^{x^q}, g_2, g_2^x)$, input it to the oracle of the Journal of Cryptology version problem, and finally obtain $(g_1^{1/(x+c)}, c)$.

They [2] also said that when $\mathbb{G}_1 = \mathbb{G}_2$, the pair $(g_2, g_2^x)$ is redundant. Actually, in this case, the Journal of Cryptology version $q$-sDH problem is equivalent to the following problem:

Definition 3 (one-generator $q$-strong Diffie-Hellman Problem). For an randomly chosen element $x \in \mathbb{Z}_p$ and a random generator $g_1 \in \mathbb{G}_1$, the one-generator $q$-strong Diffie-Hellman Problem is, given $(g_1, g_1^x, \ldots, g_1^{x^q}) \in \mathbb{G}_1^{q+1}$, to compute a pair $(g_1^{1/(x+c)}, c) \in \mathbb{G}_1 \times \mathbb{Z}_p$.

We call this problem one-generator $q$-strong Diffie-Hellman (one-generator $q$-sDH) problem.

\(^1\)This note is based on the first author’s master thesis.
1.2 The $q$-Strong Diffie-Hellman Problem over Single Group

Here we assume that $G_1 = G_2$ and discuss reductions among the $q$-sDH problem over a single group and its variants. Recall that the one-generator $q$-sDH problem is also defined over a single group.

As in the previous section, the original $q$-sDH (the Eurocrypt 2004 version $q$-sDH) problem is also reducible to the Journal of Cryptology version $q$-sDH problem in the single group setting $G_1 = G_2$, and then is reducible to the one-generator $q$-sDH problem.

We review other two variants of $q$-sDH problem defined over a single group, $q$-weak Diffie-Hellman problem and exponent $q$-strong Diffie-Hellman Problem. Mitsunari et al. [5] defined the $q$-weak Diffie-Hellman (q-wDH) problem as follows:

**Definition 4 (q-weak Diffie-Hellman Problem).** For an randomly chosen element $x \in \mathbb{Z}_p$ and a random generators $g_1 \in G_1$, the $q$-weak Diffie-Hellman Problem is, given $(g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}) \in G_1^{q+1}$, to compute an element $g_1^{1/x} \in G_1$.

Zhang et al. [7] defined the following variant problem:

**Definition 5 (exponent $q$-strong Diffie-Hellman Problem).** For an randomly chosen element $x \in \mathbb{Z}_p$ and a random generators $g_1 \in G_1$, the exponent $q$-strong Diffie-Hellman Problem is, given $(g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}) \in G_1^{q+1}$, to compute an element $g_1^{x^{q+1}} \in G_1$.

This problem is deeply investigated by Cheon [4]. Zhang et al. [7] showed that the $q$-wDH problem is equivalent to the exponent $q$-sDH problem.

$$[\text{the q-wDH problem}] \equiv [\text{the exponent q-sDH problem}]$$

Reardon [6] showed that the one-generator $q$-sDH problem is reducible to the $q$-wDH problem.

$$[\text{the one-generator q-sDH problem}] \leq [\text{the q-wDH problem}]$$

We summarize the reductions that appears in the subsection:

$$[\text{the original q-sDH problem (G}_1 = G_2)] \leq [\text{the JoC version problem (G}_1 = G_2)] \equiv [\text{the one-generator q-sDH problem}] \leq [\text{the q-wDH problem}] \equiv [\text{the exponent q-sDH problem}]$$

**Acknowledgement**

The second author would like to thank Atsushi Fujioka, Berkant Ustaoğlu and Mehdi Tibouchi, for their helpful suggestions and useful information.
References


A Reductions.

We review the reductions among the following problems and prove them based on the first author’s master thesis.

- The one-generator $q$-sDH problem is to compute $(g^{1/(a+c)}, c)$ for given $(g, g^a, g^{a^2}, \ldots, g^{a^q})$.
- The exponent $q$-sDH problem is to compute $g^{a^{q+1}}$ for given $(g, g^a, g^{a^2}, \ldots, g^{a^q})$.
- The $q$-wDH problem is to compute $g^{1/c}$ for given $(g, g^a, g^{a^2}, \ldots, g^{a^q})$.

[The one-generator $q$-sDH problem is reduced to the $q$-wDH problem.] Assume that an instance of the $q$-sDH problem $(g, g^a, g^{a^2}, \ldots, g^{a^q})$ is given. For any $c \in \mathbb{Z}_p$, we compute $(g, g^{a+c}, g^{(a+c)^2}, \ldots, g^{(a+c)^q})$, input it to the $q$-wDH problem and obtain $g^{1/(a+c)}$. Thus we obtain an answer $(g^{1/(a+c)}, c)$ for the one-generator $q$-sDH problem.

We see that the exponent $q$-sDH problem is equivalent to the $q$-wDH problem.

[The exponent $q$-sDH problem is reduced to the $q$-wDH problem.] Assume that an instance of the exponent $q$-sDH problem $(g, g^a, g^{a^2}, \ldots, g^{a^q})$ is given. We let $\beta$ denote $\alpha^{-1}$ and let $h = g^{a^q}, h^\beta = g^{a^q\beta} = g^{a^{q-1}}, h^{\beta^2} = g^{a^q\beta^2} = g^{a^{q-2}}, \ldots, h^{\beta^q} = g^{a^q\beta^q} = g$. We input $(h, h^\beta, h^{\beta^2}, \ldots, h^{\beta^q})$ to the $q$-wDH oracle and obtain $h^{1/\beta}$, which is $g^{a\beta^{-1}} = g^{a^{q+1}}$. Thus we obtain an answer $g^{a^{q+1}}$ for the exponent $q$-sDH problem.

[The $q$-wDH problem is reduced to the exponent $q$-sDH problem.] Assume that an instance of the $q$-wDH problem $(g, g^a, g^{a^2}, \ldots, g^{a^q})$ is given. We let $\beta$ denote $\alpha^{-1}$ and let $h = g^{a^q}, h^\beta = g^{a^q\beta} = g^{a^{q-1}}, h^{\beta^2} = g^{a^q\beta^2} = g^{a^{q-2}}, \ldots, h^{\beta^q} = g^{a^q\beta^q} = g$. We input $(h, h^\beta, h^{\beta^2}, \ldots, h^{\beta^q})$ to the exponent $q$-sDH oracle and obtain $h^{\beta^{-1}}$, which is equal to $g^{a^{q+1}} = g^{a^{q-1}}$. Thus we obtain an answer $g^{a^{-1}}$ for the $q$-wDH problem.

Consequently, we have

the one-generator $q$-sDH problem $\leq$ the $q$-wDH problem $\equiv$ the exponent $q$-sDH problem.