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. ψ 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 ψ 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 $(g_1, g_2, g_2^x, g_2^{x^2}, \ldots, g_2^{x^q}) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$, to compute a pair $(g_1^{1/(x+c)}, c) \in \mathbb{G}_1 \times \mathbb{Z}_p$.*

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 $(g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}, g_2, g_2^x) \in \mathbb{G}_1^{q+1} \times \mathbb{G}_2^2$, 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 ψ is the former no longer requires the existence of efficiently computable isomorphism ψ. We easily see that the Eurocrypt 2004 version problem is reducible to the Journal of Cryptology version problem as follows: for a given $(g_1, g_2, g_2^x, g_2^{x^2}, \ldots, g_2^{x^q})$, we compute $g_1^{x^i} = \psi(g_2^{x^i})$ for i $(1 \leq i \leq q)$ to obtain $(g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}, g_2, g_2^x)$, 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 generators $g_1 \in \mathbb{G}_1$, the* one-generator q-strong Diffie-Hellman Problem *is, given $(g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}) \in \mathbb{G}_1^{q+1}$, 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 $\mathbb{G}_1 = \mathbb{G}_2$ 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 $\mathbb{G}_1 = \mathbb{G}_2$, and then is reducible to the one-generator q-sDH problem.

$$\begin{aligned}\text{[the original } q\text{-}\mathsf{sDH} \text{ problem } (\mathbb{G}_1 = \mathbb{G}_2)] &\leq \text{[the JoC version problem } (\mathbb{G}_1 = \mathbb{G}_2)] \\ &\equiv \text{[the one-generator } q\text{-}\mathsf{sDH} \text{ problem]}\end{aligned}$$

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 $g_1 \in \mathbb{G}_1$, the* q-weak Diffie-Hellman Problem *is, given $(g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}) \in \mathbb{G}_1^{q+1}$, to compute an element $g_1^{1/x} \in \mathbb{G}_1$.*

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 $g_1 \in \mathbb{G}_1$, the* exponent q-strong Diffie-Hellman Problem *is, given $(g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}) \in \mathbb{G}_1^{q+1}$, to compute an element $g_1^{x^{q+1}} \in \mathbb{G}_1$.*

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.

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

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

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

We summarize the reductions that appears in the subsection:

$$\begin{aligned}\text{[the original } q\text{-}\mathsf{sDH} \text{ problemm } (\mathbb{G}_1 = \mathbb{G}_2)] &\leq \text{[the JoC version problem } (\mathbb{G}_1 = \mathbb{G}_2)] \\ &\equiv \text{[the one-generator } q\text{-}\mathsf{sDH} \text{ problem]} \\ &\leq \text{[the } q\text{-}\mathsf{wDH} \text{ problem]} \\ &\equiv \text{[the exponent } q\text{-}\mathsf{sDH} \text{ problem]}\end{aligned}$$

Acknowledgement

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

References

1. D. Boneh and X. Boyen, "Short Signatures Without Random Oracles," Proceedings of Eurocrypt 2004, Lecture Notes on Computer Science 3027, Springer-Verlag (2004), pp.56-73.
2. D. Boneh and X. Boyen, "Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups," *Journal of Cryptology* , Vol.21, No.2, (2008), pp.149-177.
3. D. Boneh, X. Boyen and H. Shacham, "Short Group Signatures," Proceedings of Crypto 2004, Lecture Notes on Computer Science 3152, Springer-Verlag (2004), pp.41-55.
4. J. H. Cheon, "Security Analysis of the Strong Diffie-Hellman Problem," Proceedings of Eurocrypt 2006, Lecture Notes on Computer Science 4004, Springer-Verlag (2006), pp.1-11.
5. S. Mitsunari, R. Sakai and M. Kasahara, "A New Traitor Tracing," IEICE Trans.Fundamentals, Vol.E85-A, no.2 (2002), pp.481-484.
6. J. Reardon, "The Strong Diffie Hellman Problem," *manuscript*, (2007).
7. F. Zhang, R. Safavi-naini and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," Proceedings of PKC 2004, Lecture Notes on Computer Science 2947, Springer-Verlag (2004), pp.277-290.

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

[**The one-generator q-sDH problem is reduced to the q-wDH problem.**] Assume that an instance of the q-sDH problem $(g, g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^q})$ is given. For any $c \in \mathbb{Z}_p$, we compute $(g, g^{\alpha+c}, g^{(\alpha+c)^2}, \ldots, g^{(\alpha+c)^q})$, input it to the q-wDH problem oracle and obtain $g^{1/(\alpha+c)}$. Thus we obtain an answer $(g^{1/(\alpha+c)}, c)$ 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 $(g, g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^q})$ is given. We let β denote α^{-1} and let $h = g^{\alpha^q}, h^{\beta} = g^{\alpha^q \beta} = g^{\alpha^{(q-1)}}, h^{\beta^2} = g^{\alpha^q \beta^2} = g^{\alpha^{(q-2)}}, \ldots, h^{\beta^q} = g^{\alpha^q \beta^q} = g$. We input $(h, h^{\beta}, h^{\beta^2}, \ldots, h^{\beta^q})$ to the q-wDH oracle and obtain $h^{1/\beta}$, which is $g^{\alpha^q \beta^{-1}} = g^{\alpha^{(q+1)}}$. Thus we obtain an answer $g^{\alpha^{(q+1)}}$ 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 $(g, g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^q})$ is given. We let β denote α^{-1} and let $h = g^{\alpha^q}$, $h^{\beta} = g^{\alpha^q \beta} = g^{\alpha^{(q-1)}}$, $h^{\beta^2} = g^{\alpha^q \beta^2} = g^{\alpha^{(q-2)}}, \ldots, h^{\beta^q} = g^{\alpha^q \beta^q} = g$. We input $(h, h^{\beta}, h^{\beta^2}, \ldots, h^{\beta^q})$ to the exponent q-sDH oracle and obtain $h^{\beta^{q+1}}$, which is equal to $g^{\alpha^q \beta^{q+1}} = g^{\alpha^q \alpha^{-(q+1)}} = g^{\alpha^{-1}}$. Thus we obtain an answer $g^{\alpha^{-1}}$ 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.