On the q-Strong Diffie-Hellman Problem

Naoki Tanaka[1] and Taiichi Saito[1]

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, and is based on the first author's master thesis.

We discuss reductions among the q-strong Diffie-Hellman (q-SDH) problem [1, 2] and related problems. Cheon [3] defined a variant of the q-SDH problem (Cheon's q-SDH problem) and investigated difficulty of it. Mitsunari et al. [4] used another variant, q-weak Diffie-Hellman (q-WDH) problem, to construct a secure traitor tracing scheme.

- The q-SDH problem is to compute $(g^{1/(\alpha+c)}, c)$ for given $(g, g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^q})$.
- Cheon's q-SDH problem is to compute g^{α^q} 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 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 q-SDH problem.

We see that Cheon's q-SDH problem is equivalent to the q-WDH problem.
[**Cheon's q-SDH problem is reduced to the q-WDH problem.**] Assume that an instance of Cheon's 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 Cheon's q-SDH problem.

[**The q-WDH problem is reduced to Cheon's 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 Cheon's 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

$$\text{the } q\text{-SDH problem} \leq \text{the } q\text{-WDH problem} \equiv \text{Cheon's } q\text{-SDH problem.}$$

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, X.Boyen and H.Shacham, "Short Group Signatures," Proceedings of Crypto 2004, Lecture Notes on Computer Science 3152, Springer-Verlag (2004), pp.41-55.

3. 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.
4. S.Mitsunari, R.Sakai and M.Kasahara, “A New Traitor Tracing,” IEICE Trans.Fundamentals, Vol.E85-A, no.2 (2002), pp.481-484.