Tight Reductions among Strong Diffie-Hellman Assumptions

Victor K. Wei

Department of Information Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong
kwwei@ie.cuhk.edu.hk

Abstract. We derive some tight equivalence reductions between several Strong Diffie-Hellman (SDH) assumptions.

1 Results

Let $\hat{e} : G_1 \times G_2 \to G_T$ be a bilinear mapping. The *k-Strong Diffie-Hellman Problem (k-SDH)* is the problem of computing a pair $(g_1^{1/(\gamma+x)}, x)$ given $g_1 \in G_1$, and g_2, g_2^γ, $g_2^{\gamma^2}$, $\cdots$, $g_2^{\gamma^k} \in G_2$. The *k-Strong Diffie-Hellman Assumption* is that no PPT algorithm has a non-negligible probability of solving a random instance of the k-Strong Diffie Hellman Problem. For details, see [2, 3].

The k-SDH Assumption is closely related to the coalition-resistance of pairing-based signature schemes and group signature schemes [4, 6, 2, 3, 5]. Typically, k colluders cannot jointly forge an additional signature not traceable to them when the k-SDH Assumption holds. The following variants are also related to the coalition-resistance of pairing based signatures and group signatures:

- The *k-SDH' Problem* is the problem of computing a pair $(g_1^{1/(\gamma+x)}, x)$ given g_1, g_1^γ, $g_1^{\gamma^2}$, $\cdots$, $g_1^{\gamma^k} \in G_1$ and $g_2, g_2^\gamma \in G_2$.
- The *k-CAA Problem* is, given g_2, $g_2^\gamma \in G_2$, $v \in G_1$, and and pairs (A_i, e_i) with distinct and nonzero e_i's satisfying $A_i^{\gamma+e_i} = v$, $1 \le i \le k$, compute a pair (A_{k+1}, e_{k+1}) with $e_{k+1} \ne e_i$ for any i, $1 \le i \le k$, and satisfying $A_{k+1}^{\gamma+e_{k+1}} = v$.
- The *k-SDH'2 Problem* is, given $g_2, g_2^\gamma \in G_2$, $g_1^{\gamma^i}$ and $g_3^{\gamma^i}$ in G_1 for $0 \le i \le k$, compute a triple $((g_1 g_3^{\tilde{x}})^{1/(\gamma+\tilde{e})}, \tilde{x}, \tilde{e})$.
- The *k-CAA2 Problem* is, given g_2, $g_2^\gamma \in G_2$, u, $v \in G_1$, (A_i, e_i, x_i) satisfying $A_i^{\gamma+e_i} u^{x_i} = v$ for $1 \le i \le k$ and all e_i's are distinct and nonzero, compute another triple $(A_{k+1}, e_{k+1}, x_{k+1})$ satisfying $A_{k+1}^{\gamma+e_{k+1}} u^{x_{k+1}} = v$ and $e_{k+1} \ne n_i$ for any i, $1 \le i \le k$.

The *k-SDH' (resp. k-CAA, k-SDH'2, k-CAA2) Assumption* is that no PPT algorithm has a non-negligible probability of solving a random instance of the k-SDH' (resp. k-CAA, k-SDH', k-CAA2) Problem. The k-CAA Assumption is from Zhang, et al.[6], where CAA stands for *Collusion Attack Algorithm.* They showed the k-CAA Assumption holds if and only if their group signature scheme is k-coalition resistant. [2, 3] showed the k-CAA Assumption implies the k-SDH Assumption. However, no implicaiton in the opposite direction was given. The *full traceability* of the *exculpable* version of [3]'s group signature in their Section 7 can be easily shown equivalent to the k-CAA2 Assumption. [5] showed the k-CCA2 Assumption implies the k-SDH Assumption. Abdalla, et al.[1] defined a different, and only remotely related, assumption which they also called the strong Diffie-Hellman assumption.

Typically, there exists an efficiently computable homomorphism ψ such that $\psi(g_2) = g_1$. Then the k-SDH Assumption implies the k-SDH' Assumption. In Section 2, we prove the following Theorems:

Theorem 1. *The k-SDH' Assumption and the k-CAA Assumption are equivalent.*

Theorem 2. *Assume the discrete log value $\log_v(u)$ is known. Then the k-SDH' Assumption and the k-CAA2 Assumption implies each other.*

Theorem 3. *The k-SDH'2 Assumption implies the k-CAA2 Assumption.*

In proving results concerning SDH-based signatures (resp. group signatures), u is often the output of a hashing function. Then the value of $\log_v(u)$ is known to the *Simulator* under the random oracle model. More specifically, $u = Hash(something)$, and the *Simulator* can select α and backpatch $Hash(something) \leftrightarrow v^\alpha$. In such cases, Theorem 2 can be used to establish equivalence between coalition-resistant unforgeability of SDH-based signature (resp. group signature) schemes and the k-SDH' Assumption. On the other hand, Theorem 3 can be used to reduce the coalition-resistant unforgeability of some SDH-based signatures (resp. group signatures) to the k-SDH'2 Assumption without the random oracle model. It remains intereating to explore other equivalence reductions between these and other SDH-related assumptions, and their applications to pairing-based signatures and group signatures.

We also note that the above equivalence reductions are *tight*, meaning that one solution algorithm's time complexity (resp. success probability) is within a reasonable additive term of the solution algorithm of the other problem. Such tightness will be established by our proofs below.

2 Proofs

2.1 Proof Sketch of Theorem 1

(1) *Solving k-CAA Problem implies solving k-SDH' Problem.* Assume PPT algorithm $\mathcal{A}$ solves k-CAA. Given a k-SDH' problem instance, randomly generate distinct nonzero e_i, $1 \leq i \leq k$. Let $f(\gamma) = \prod_{i=1}^k(\gamma + e_i)$. Denote $f(\gamma) = \sum_{i=0}^k f_i\gamma^i$. Let $v = g_1^{f(\gamma)}$. For $1 \leq i \leq k$ let $f^{[j]} = f(\gamma)/(\gamma + e_j) = \sum_{i=0}^{k-1} f_i^{[j]}\gamma^i$. Then

$$A_j = v^{1/(\gamma+e_j)} = g_1^{f^{[j]}(\gamma)} = g_1^{\sum_{i=0}^{k-1} f_i^{[j]}\gamma^j} = \prod_{i=0}^{k-1}(g_1^{\gamma^j})^{f_i^{[j]}}$$

Note that for each j, $1 \leq j \leq k$, we have $A_j^{\gamma+e_j} = v$. Invoking $\mathcal{A}$ to solve this k-CAA Problem, we obtain (A_{k+1}, e_{k+1}) satisfying $A_{k+1}^{\gamma+e_{k+1}} = v$. Denote $B = v^{\hat{f}(\gamma)^{-1}}$ where $\hat{f}(\gamma) = f(\gamma)(\gamma + e_{k+1})$. Next, we describe how to compute B. Denote $\hat{f}(\gamma) = \sum_{i=0}^{k+1} \hat{f}_i\gamma^i$ and

$$\hat{f}^{[j]}(\gamma) = \hat{f}(\gamma)(\gamma + e_j)^{-1} = \prod_{1\leq i\leq k+1, i\neq j}(\gamma + e_i) = \sum_{i=1}^{k} \hat{f}_i^{[j]}\gamma^i$$

for $1 \leq j \leq k+1$. Denote $\tilde{e} = e_{k+1}$, we have

$$\begin{aligned} &B^{\gamma^{j+1}+\gamma_j\tilde{e}} = B^{(\gamma^j+\gamma^{j-1}\tilde{e})\gamma} = g_1^j, \text{ for } 0 \leq j \leq k \\ &B^{\hat{f}(\gamma)} = v \end{aligned}$$

The above system of $k+2$ equations can be solved for the $k+2$ unknowns B^{γ^ℓ}, $0 \leq \ell \leq k+1$, including B where $(B, \tilde{e})$ solves the k-SDH' Problem.

(2) *Solving k-SDH' Problem implies solving k-CAA Problem.* Assume $\mathcal{A}$ is a PPT solver of the k-SDH' Problem. Given $A_i^{\gamma+e_i}$, $1 \leq i \leq k$, let $f(\gamma) = \prod_{I=1}^k(\gamma + e_i)$. Let $g_1 = v^{1/f(\gamma)}$. Next, we describe how to compute g_1.

Denote $f(\gamma) = \sum_{i=0}^k f_i\gamma^i$ and $f^{[j]}(\gamma) = f(\gamma)/(\gamma + e_j) = \sum_{i=0}^{k-1} f_i^{[j]}\gamma^i$, for $1 \leq j \leq k$. We have $v = g_1^{f(\gamma)} = \prod_{i=0}^k(g_1^{\gamma^i})^{f_i}$ and

$$A_j = g_1^{f^{[j]}(\gamma)} = \prod_{i=0}^{k}(g_1^{\gamma^i})^{f_i^{[j]}} \tag{1}$$

Rearranging, we have

$$\prod_{i=0}^{k}(g_1^{\gamma^i})^{M_{i,j}} = A_j, \text{ for } 0 \leq j \leq k, \tag{2}$$

where the $(k+1)\times(k+1)$ matrix $\bar{\mathbf{M}}$ is

$$\bar{\mathbf{M}} = [M_{i,j}]_{0\le i,j\le k} = \begin{bmatrix} f_0 & f_1 & \cdots & f_k \\ 0 & f_1^{[1]} & \cdots & f_k^{[1]} \\ \vdots & & & \\ 0 & f_1^{[k]} & \cdots & f_k^{[k]} \end{bmatrix}$$

Note $f_i^{[j]} = \mathsf{S}_{k-1-i}(E\setminus\{e_j\})$ for all i and j, $1\le i\le k-1$, $1\le j\le k$, where $E=\{e_1,\cdots,e_k\}$ and $\mathsf{S}_a(\{x_1,\cdots,x_n\})$ is the a-th order symmetric function

$$\mathsf{S}_a(\{x_1,\cdots,x_n\}) = \sum_{1\le i_1<\cdots<i_a\le n} x_{i_1}\cdots x_{i_a}$$

Denote the $k\times k$ matrix $\mathbf{M}=[M_{i,j}]_{1\le i,j\le k}$. We prove the following Lemma later:

Lemma 4 $\det(\mathbf{M}) = \prod_{1\le i<j\le k}(e_i-e_j)$.

Therefore $\det(\bar{\mathbf{M}}) = (\prod_{\ell=1}^{k} e_\ell)(\prod_{1\le i,j\le k}(e_i-e_j)) \ne 0$, and Equation (2) can be solved to obtain $g_1^{\gamma^i}$, for all i, $0\le i\le k$. Invoking the k-SDH' solver $\mathcal{A}$ to obtain $g_1^{1/(\gamma+x)}$ and x.

Let $\bar{f}(\gamma)=\sum_{i=0}^{k-1}\bar{f}_i\gamma^i$ and $\bar{c}$ be such that $f(\gamma)/(\gamma+x)=\bar{f}(\gamma)+\bar{c}/(\gamma+x)$. Then compute

$$A_{k+1} = g_1^{f(\gamma)/(\gamma+x)} = g_1^{\bar{f}(\gamma)}(g_1^{1/(\gamma+x)})^{\bar{c}} = [\prod_{i=0}^{k-1}(g_1^{\gamma^i})^{\bar{f}_i}](g_1^{1/(\gamma+x)})^{\bar{c}}$$

and we solve k-CAA Problem with $(A_{k+1},\, x)$. $\square$

2.2 Proof Sketch of Lemma 4

Note $\mathbf{M}$ equals the following matrix:

$$\mathbf{M}(k,e_1,\cdots,e_k) = \begin{bmatrix} \mathsf{S}_{k-1}(E\setminus\{e_1\}) & \mathsf{S}_{k-2}(E\setminus\{e_1\}) & \cdots & \mathsf{S}_0(E\setminus\{e_1\}) \\ \mathsf{S}_{k-1}(E\setminus\{e_2\}) & \mathsf{S}_{k-2}(E\setminus\{e_2\}) & \cdots & \mathsf{S}_0(E\setminus\{e_2\}) \\ \vdots & & & \\ \mathsf{S}_{k-1}(E\setminus\{e_k\}) & \mathsf{S}_{k-2}(E\setminus\{e_k\}) & \cdots & \mathsf{S}_0(E\setminus\{e_k\}) \end{bmatrix}$$

By convention $\mathsf{S}_0=1$. We prove the the following statement:

$$\det(\mathbf{M}(k,e_1,\cdots,e_k)) = (\prod_{i=2}^{k}(e_1-e_i))\det(\mathbf{M}(k-1,e_2,\cdots,e_k)) \tag{3}$$

Then induction on k yields the Lemma.

Let matrix

$$\mathbf{U} = \begin{bmatrix} 1 & -1 & -1 & \cdots & -1 \\ & 1 & & & \\ & & \ddots & & 0 \\ 0 & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

Multiplying two matrices we obtain $\mathbf{M}(k,e_1,\cdots,e_k)\mathbf{U} =$

$$\begin{bmatrix} \mathsf{S}_{k-1}(E\setminus\{e_1\}) & \mathsf{S}_{k-2}(E\setminus\{e_1\}) & \cdots & \mathsf{S}_1(E\setminus\{e_1\}) & \mathsf{S}_0(E\setminus\{e_1\}) \\ (e_1-e_2)\mathsf{S}_{k-2}(E\setminus\{e_1,e_2\}) & (e_1-e_2)\mathsf{S}_{k-3}(E\setminus\{e_1,e_2\}) & \cdots & (e_1-e_2)\mathsf{S}_0(E\setminus\{e_1,e_2\}) & 0 \\ (e_1-e_3)\mathsf{S}_{k-2}(E\setminus\{e_1,e_3\}) & (e_1-e_3)\mathsf{S}_{k-3}(E\setminus\{e_1,e_3\}) & \cdots & (e_1-e_3)\mathsf{S}_0(E\setminus\{e_1,e_3\}) & 0 \\ \vdots & & & & \\ (e_1-e_k)\mathsf{S}_{k-2}(E\setminus\{e_1,e_k\}) & (e_1-e_k)\mathsf{S}_{k-3}(E\setminus\{e_1,e_k\}) & \cdots & (e_1-e_k)\mathsf{S}_0(E\setminus\{e_1,e_k\}) & 0 \end{bmatrix}$$

Consider the lower left $(k-1)\times(k-1)$ matrix. Its i-th row is exactly the i-th row of $\mathbf{M}(k-1,E\setminus\{e_1\})$ multiplied by e_1-e_i, . This proves Equation (3) and thus the Lemma. $\square$

2.3 Proof Sketch of Theorem 2

Assume $\log_v(u) = \alpha$. The proof is similar to that of Theorem 1. We describe mainly the difference below. Given a PPT algorithm $\mathcal{A}$ which solves k-CAA2, and a k-SDH' Problem instance, randomly generate distinct nonzero e_i and x_i, $1 \le i \le k$. Let $f(\gamma)$, $f^{[i]}(\gamma)$ be as defined in the proof of Theorem 1. Then

$$A_j = v^{(1-x_i\alpha)/(\gamma+e_i)} = g_1^{(1-x_i\alpha)f^{[i]}(\gamma)}$$

Invoking $\mathcal{A}$ to obtain $(A_{k+1}, e_{k+1}, x_{k+1})$ satisfying $A_{k+1}^{\gamma+e_{k+1}} u^{x_{k+1}} = v$. The rest is similar to the proof of Theorem 1.

Given a PPT algorithm $\mathcal{A}$ which solves the k-SDH' Problem and a k-CCA2 Problem instance, we have $A_i^{\gamma+e_i} = v^{1-x_i\alpha}$. Let $g_1 = v^{1/f(\gamma)}$, then Equation (1) becomes

$$A_j = g_1^{(1-x_i\alpha)f^{[j]}(\gamma)}, 1 \le j \le k.$$

The non-singularity of the matrix $\bar{\mathbf{M}}$ ensures that a k-SDH' Problem instance can be computed from the A_j's. Invoke $\mathcal{A}$ to solve this problem instance, and then convert its answer to an answer for the k-CAA2 Problem is straightforward. □

2.4 Proof Sketch of Theorem 3

Assume $\mathcal{A}$ solves the k-CAA2 Problem. Given a k-SDH'2 Problem instance, randomly choose nonzero distinct e_i and x_i, $1 \le i \le k$, and let $f(\gamma)$, $f^{[i]}(\gamma)$, and v be as defined in the Proof Sketch of Theorem 1. Furthermore, let $u = g_3^{f(\gamma)}$. Then let $A_i = g_1^{f(\gamma)/(\gamma+e_i)} g_3^{-x_i f(\gamma)/\gamma+e_i)}$, and we have $A_i^{\gamma+e_i} u^{x_i} = v$ for each i, $1 \le i \le k$. Invoking $\mathcal{A}$ to obtain $(\tilde{A}, \tilde{e}, \tilde{x})$ satisfying $\tilde{A}^{\gamma+\tilde{e}} u^{\tilde{x}} = v$. Then $(B, \tilde{e}, -\tilde{x})$ solves the k-SDH'2 Problem where $B = [\tilde{A}(g_1 g_3^{-\tilde{x}})^{\bar{f}(\gamma)}]^{\bar{c}^{-1}}$, $f(\gamma)/(\gamma+\tilde{e}) = \bar{f}(\gamma) + \bar{c}/(\gamma+\tilde{e})$, $\bar{d}$ is a constant. □

Acknowledgements to Professor Zhang, Fangguo, for helpful discussions.

References

1. M. Abdalla, M. Bellare, and P. Rogaway. DHIES: an encryption scheme based on the Diffie-Hellman problem. In *CT-RSA 2001*, volume 2045 of *LNCS*. Springer-Verlag, 2001.
2. D. Boneh and X. Boyen. Short signatures without random oracles. In *Eurocrypt 2004*, volume 3027 of *LNCS*, pages 56–73. Springer–Verglag, 2004.
3. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *CRYPYTO 2004*, volume 3152 of *LNCS*. Springer–Verglag, 2004.
4. S. Mitsunari, R. Sakai, and M. Kasahara. A new traitor tracing. *IEICE Trans.*, E85-A(2):481–484, 2002.
5. Victor K. Wei. Tracing-by-linking group signatures. Cryptology ePrint Archive, Report 2004/370, 2004. http://eprint.iacr.org/.
6. F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In *PKC 2004*, 2004.