Variations of Diffie-Hellman Problem

Feng Bao, Robert H. Deng, Huafei Zhu

Infocomm Security Department, Institute for Infocomm Research.
21 Heng Mui Keng Terrace, Singapore 119613.
email: {baofeng, deng, huafei}@i2r.a-star.edu.sg

Abstract. This paper studies various computational and decisional Diffie-Hellman problems by providing reductions among them in the high granularity setting. We show that all three variations of computational Diffie-Hellman problem: square Diffie-Hellman problem, inverse Diffie-Hellman problem and divisible Diffie-Hellman problem, are equivalent with optimal reduction. Also, we are considering variations of the decisional Diffie-Hellman problem in single sample and polynomial samples settings, and we are able to show that all variations are equivalent except for the argument DDH $\Leftarrow$ SDDH. We are not able to prove or disprove this statement, thus leave an interesting open problem.

Keywords: Diffie-Hellman problem, Square Diffie-Hellman problem, Inverse Diffie-Hellman problem, Divisible Diffie-Hellman problem

1 Introduction

The Diffie-Hellman problem [9] is a golden mine for cryptographic purposes and is more and more studied. This problem is closely related to the difficult of computing the discrete logarithm problem over a cyclic group[11]. There are several works to study classical and variable Diffie-Hellman problems([13], [14], [21], [18]) in the generic model. For the decisional Diffie-Hellman problem setting, there is alternative, yet equivalent notation, called matching Diffie-Hellman problem, have been studied by Handschuh, Tsiounis and Yung [10]. These variations are by now the security of many protocols relying on ([1], [2], [5], [6],[8]). Tatsuaki Okamoto and David Pointcheval[16] introduce a new notion called the Gap-Problems, which can be considered as a dual to the class of the decision problems. While Sadeghi and Steinerhere [19] rigourously consider a set of Diffie-Hellman related problems by identifying a parameter termed granularity, which describes the underlying probabilistic space in an assumption.

This paper studies various computational and decisional problems related to the Diffie-Hellman problems by providing reductions among them in the high granularity setting, i.e., we consider the variations of Diffie-Hellman problem defined over some cyclic group with explicit group structure. More precisely, we are interested in studying relationship among variations of Diffie-Hellman problem including computational and decisional cases in single and polynomial setting and try to obtain reductions that are efficient so that an advantage against one of these problems can be reached against the other one.

The basic tools for relating the complexities of various problems are polynomial reductions and transformations. We say that a problem A reduces in polynomial time to another problem B, denoted by $A \Leftarrow B$, if and only if there is an algorithm for A which uses a subroutine for B, and each call to the subroutine for B counts as a single step, and the algorithm for A runs in polynomial-time. The latter implies that the subroutine for B can be called at most a polynomially bounded number of times. The practical implication comes from the following proposition: If A polynomially reduces to B and there is a polynomial time algorithm for B, then there is a polynomial time algorithm for A also. Specially, for considering variation of Diffie-Hellman problem in polynomial time sampling case, we need to define the conception of efficient constructing algorithm to meet the requirement of the standard hybrid technique.

Our contributions: In this report, we are considering useful variations of Diffie-Hellman problem: square computational(and decisional) Diffie-Hellman problem, inverse computational(and decisional) Diffie-Hellman problem and divisible computational(and decisional) Diffie-Hellman problem. We are able to show that all variations of computational Diffie-Hellman problem are equivalent to the classic computational Diffie-Hellman problem if the order of a underlying cyclic group is a large prime. We remark that our reduction is efficient, that is an advantage against one of these problems can be reached against another one. Also, we are considering variations of the decisional Diffie-Hellman problem in single sample and polynomial samples settings, and we are able to show that all variations are equivalent except for the argument DDH $\Leftarrow$ SDDH. We are not able to prove or disprove this statement, thus leave an interesting open problem in this report.

2 Variations of Computational Diffie-Hellman Problem

Let p be a large prime number such that the discrete logarithm problem defined in Z_p^* is hard. Let $G \in Z_p^*$ be a cyclic group of prime order q and g is assumed to be a generator of G. Though out this paper, we assume that G is prime order, and security parameters p, q are defined as the fixed form $p{=}2q+1$ and $ord(g){=}q$. A remarkable computational problem has been defined on this kind of set by Diffie and Hellman [9]. More precisely, Diffie-Hellman assumption (CDH assumption) is referred to as the following statement:

Computational Diffie-Hellman problem (CDH): On input g, g^x, g^y, computing g^{xy}.

An algorithm that solves the computational Diffie-Hellman problem is a probabilistic polynomial time Turing machine, on input g, g^x, g^y, outputs g^{xy} with non-negligible probability. Computational Diffie-Hellman assumption means that there is no such a probabilistic polynomial time Turing machine. This assumption is believed to be true for many cyclic groups, such as the prime sub-group of the multiplicative group of finite fields.

2.1 Square computational Diffie-Hellman assumption

Let $G \in Z_p^*$ defined as above, we are interested in the square computational Diffie-Hellman problem, which has been studied at by a set of researchers already (see [3], [12],[13], [14] for more details). We remark that the reduction presented in this section emphasizes its efficient and optimal characteristic. Therefore our work is non-trivial indeed.

Square computational Diffie-Hellman problem (SCDH): On input g, g^x, computing g^{x^2}.

An algorithm that solves the square computational Diffie-Hellman problem is a probabilistic polynomial time Turing machine, on input g, g^x, outputs g^{x^2} with non-negligible probability. Square computational Diffie-Hellman assumption means that there is no such a probabilistic polynomial time Turing machine. Fortunately, we are able to argue that the SCDH assumption and CDH assumption are equivalent.

SCDH $\Leftarrow$ CDH

Proof: Given an oracle A_1, on input g,g^x, g^y, outputs g^{xy}, we want to show that there exists an algorithm A_2, on input g^x, outputs g^{x^2}. Given a random value $u := g^r$, we choose $t_1, t_2 \in Z_q$ at random, and compute $u_1 = u^{t_1} = g^{rt_1}$, and $u_2 = u^{t_2} = g^{rt_2}$. Therefore we are able to compute $v = A_1(u_1, u_2) = g^{r^2 t_1 t_2}$ with non-negligible probability. It follows that g^{r^2} can be computed from v, t_1, t_2 immediately with same advantage.

CDH $\Leftarrow$ SCDH

Proof: Given an oracle A_2, on input g, g^x, outputs g^{x^2}, we want to show that there exists an algorithm A_1, on input g, g^x, g^y, outputs g^{xy}. Now given g^x, we choose $s_1, s_2, t_1, t_2 \in Z_q$ at random and compute $v_1 := A_2(g^{xs_1}) = g^{(xs_1)^2}$, $v_2 := A_2((g^y)^{s_2}) = g^{(ys_2)^2}$. Finally, we compute $v_3 := A_2(g^{xs_1t_1+ys_2t_2}) = g^{(xs_1t_1+ys_2t_2)^2}$. Since s_1, s_2, t_1, t_2 are known already, it follows that g^{xy} can be computed from $v_1, v_2, v_3, s_1, s_2, t_1, t_2$ immediately with same advantage.

2.2 Inverse computational Diffie-Hellman assumption

We are also interested in such a computational variation of computational Diffie-Hellman problem, called inverse computational Diffie-Hellman assumption (InvCDH assumption) first studied at [17].

Inverse computational Diffie-Hellman problem (InvCDH): On input g, g^x, outputs $g^{x^{-1}}$.

An algorithm that solves the inverse computational Diffie-Hellman problem is a probabilistic polynomial time Turing machine, on input g, g^x, outputs $g^{x^{-1}}$ with non-negligible probability. Inverse computational Diffie-Hellman assumption means that there is no such a probabilistic polynomial time Turing machine. Fortunately, we are able to argue that the SCDH assumption and InvCDH assumption are also equivalent.

InvCDH $\Leftarrow$ SCDH

Proof: Given an oracle A_2, on input g, g^x, outputs g^{x^2}, we want to show that there exists an algorithm A_3, on input g^x, outputs $g^{x^{-1}}$. Given a random value

g^r, we set $h_1 \leftarrow g^r$ and $h_2 \leftarrow g$. Finally, we view (h_1, h_2) as an input to the oracle A_2 to obtain $A_2(h_1, h_2) = g^{r r^{-2}}$. It follows that $g^{r^{-1}}$ can be computed from A_2 immediately with same advantage.

SCDH $\Leftarrow$ InvCDH

Proof: Given an oracle A_3, on input g, g^x, outputs $g^{x^{-1}}$, we want to show that there exists an algorithm A_2, on input g, g^x, outputs g^{x^2}. Now given g, g^r, we set $h_1 \leftarrow g^r$ and $h_2 \leftarrow g$. Finally, we view (h_1, h_2) as an input to the oracle A_3 to obtain $A_3(h_1, h_2) = A_3(g^r, (g^r)^{r^{-1}})$. It follows that g^{r^2} can be computed from A_3 with the same advantage.

2.3 Divisible computation Diifie-Hellman assumption

Yet, there is another variation of CDH assumption, called divisible computation Diffie-Hellman assumption, which is interesting from point of views of both theoretical research and practice.

Divisible computation Diifie-Hellman problem (DCDH problem): On random input g,g^x, g^y, computing $g^{y/x}$. We refer this oracle to as divisional computation Diffie-Hellman problem.

An algorithm that solves the divisible computational Diffie-Hellman problem is a probabilistic polynomial time Turing machine, on input g, g^x, g^y, outputs $g^{x/y}$ with non-negligible probability. Divisible computation Diffie-Hellman assumption means that there is no such a probabilistic polynomial time Turing machine. As desired, we are able to show that divisible computational Diifie-Hellman assumption is equivalent to computational Diffie-Hellman assumption:

CDH $\Leftarrow$ DCDH

Proof: Suppose we are given an divisible computation Diffie-Hellman oracle denoted by A_4, on input g, g^x, g^y, outputs $g^{y/x}$. We want to show that there exists an algorithm A_1, on input g, g^x, g^y, outputs g^{xy}. Given g, g^x, g^y, we choose $s_1, s_2, t_1, t_2 \in Z_q$ at random, and compute $v_1 := A_4(g, (g^x)^{s_1}, g^{s_2}) = g^{x s_1 / s_2}$, $v_2 := A_4(g, g^{t_1}, (g^y)^{t_2} = g^{t_1/(y t_2)}$. Finally, we compute $v := A_3(v_1, v_2) = g^{(xy s_1 t_2)/(s_2 t_1)}$. Since s_1, s_2, t_1, t_2 are known already, it follows that g^{xy} can be computed from v, s_1, s_2, t_1, t_2 immediately with same advantage.

DCDH $\Leftarrow$ CDH

Proof: Suppose we are given an computational Diffie-Hellman oracle A_1, on input g, g^x, g^y, it outputs g^{xy}. We want to show that there exists an algorithm A_4, on input g, g^x, g^y, outputs $g^{y/x}$. Suppose we are given a triple g, g^x, g^y now. By assumption, we are given a computational Diffie-Hellman oracle A_1 , consequently, we are able to construct an InvCDH oracle A_3. Viewing g, g^y as input to A_3 to obtain $v := g^{y^{-1}}$. Finally, one views g, g^x, v as input to A_1 to obtain $g^{x/y}$.

We prove the fact that if the underlying group with prime order q, all variations of computational Diffie-Hellman problem are equivalent, i.e., CDH $\Leftrightarrow$ SCDH $\Leftrightarrow$ InvCDH $\Leftrightarrow$ DCDH.

3 Variations of decisional Diffie-Hellman problem

In this section, we study variations of decisional Dffie-Hellman problem. It has been known for years that the various DDH-based problems been published many times and commented under many angles. Recently reductions were known from the work of Sadeghi and Steiner [19] in the generic model, but the present paper provides reductions in the high granularity setting. Before formally study the relationship among the variation problems, we would like to provide a formal definitions of the related problems.

3.1 Formal definitions on variations of decisional Diffie-Hellman problem

Decisional Diffie-Hellman assumption-DDH: Let G be a large cyclic group of prime order q defined above. We consider the following two distributions:

- Given a Diffie-Hellman quadruple g, g^x, g^y and g^{xy}, where $x, y \in Z_q$, are random strings chosen uniformly at random;
- Given a random quadruple g, g^x, g^y and g^r, where $x, y, r \in Z_q$, are random strings chosen uniformly at random.

An algorithm that solves the Decisional Diffie-Hellman problem is a statistical test that can efficiently distinguish these two distributions. Decisional Diffie-Hellman assumption means that there is no such a polynomial statistical test. This assumption is believed to be true for many cyclic groups, such as the prime sub-group of the multiplicative group of finite fields.

Square decisional Diffie-Hellman assumption-SDDH: Let G be a large cyclic group of prime order q defined above. We consider the following two distributions:

- Given a square Diffie-Hellman triple g, g^x and g^{x^2}, where $x \in Z_q$, is a random string chosen uniformly at random;
- Given a random triple g, g^x and g^r, where $x, r \in Z_q$, are two random strings chosen uniformly at random.

An algorithm that solves the square decisional Diffie-Hellman problem (SDDH for short) is a statistical test that can efficiently distinguish these two distributions. Square decisional Diffie-Hellman assumption means that there is no such a polynomial statistical test.

Inverse decisional Diffie-Hellman assumption -InvDDH: Let G be a large cyclic group of prime order q defined above. We consider the following two distributions:

- Given a inverse Diffie-Hellman triple g, g^x and $g^{x^{-1}}$, where $x \in Z_q$, is a random string chosen uniformly at random.;
- Given a random triple g, g^x and g^r, where $x, r \in Z_q$, are random strings chosen uniformly at random.

An algorithm that solves the Inverse decisional Diffie-Hellman problem (InvDDH for short) is a statistical test that can efficiently distinguish these two distributions. Inverse decisional Diffie-Hellman assumption means that there is no such a polynomial statistical test.

Divisible decision Diffie-Hellman assumption-DDDH: Let G be a large cyclic group of prime order q defined above. We consider the following two distributions:

- Given a divisible Diffie-Hellman quadruple g, g^x, g^y and $g^{x/y}$, where $x, y \in Z_q$, are random strings chosen uniformly at random;
- Given a random quadruple g, g^x and g^y and g^r, where $x, y, r \in Z_q$, are random strings chosen uniformly at random.

An algorithm that solves the divisible decision Diffie-Hellman problem (DDDH for short) is a statistical test that can efficiently distinguish these two distributions. Divisive decision Diffie-Hellman assumption means that there is no such a polynomial statistical test.

3.2 Relations among variations of decisional Diffie-Hellman assumption

Analogous the arguments above, we consider relations among variations of decisional Diffie-Hellman assumption. We first prove the equivalence between InvDDH and SDDH assumptions.

InvDDH $\Leftarrow$ SDDH.

Proof: Given a distinguisher D_1 which is able to tell square Diffie-Hellman triple from a random triple with non-negligible probability, we want to show that there exists a polynomial distinguisher D_2 which is able to tell inverse Diffie-Hellman triple from a random triple with non-negligible advantage. Now we are given g, g^x and g^r, where r is either x^{-1} or a random string. Setting $h_1 \leftarrow (g^r)^s$, $h_2 \leftarrow g^s$ and $h_3 \leftarrow (g^x)^{s^2}$), where $s \in Z_q$ is a random string. We remark that if $r = x^{-1}$, then $h_1 = (g^{x^{-1}})^s$, and $h_2 = (g^{x^{-1}})^{sx}$, and $h_3 = (g^{x^{-1}})^{s^2x^2}$. If g^r is a random triple, then (h_1, h_2, h_3) is also a random triple. We then view (h_1, h_2, h_3) as input to the oracle D_1 to obtain correct value $b \in \{0, 1\}$ (b=0 if the answer of D_1 is SDDH triple, and 0 otherwise). Therefore, we have a polynomial distinguisher D_2 which is able to tell inverse Diffie-Hellman triple from a random triple with same non-negligible advantage.

SDDH $\Leftarrow$ InvDDH.

Proof: Given a distinguisher D_2, which is able to tell the inverse decisional Diffie-Hellman triple from a random triple with non-negligible advantage, we want to show that there exists a distinguisher D_1 that is able to tell the square decisional Diffie-Hellman triple from a random pair with non-negligible advantage. Given g, g^x, g^r, where either $r = x^2$ or $r \in Z_q$ a random string. Setting, $h_1 \leftarrow g^x$, $h_2 \leftarrow (g^r)^s$ and $h_3 \leftarrow g^{s^{-1}}$. We remark that if $r = x^2$, then $h_1 = g^x$, $h_2 = (g^x)^{xs}$ and $h_3 = (g^x)^{(xs)^{-1}}$. If r is a random string, then h_1, h_2 and h_3 are random triple. We view (h_1, h_2, h_3) as input to inverse decisional Diffie-Hellman distinguisher D_2 to obtain correct value $b \in \{0, 1\}$ (b=0 if the answer of D_2 is

InvDDH triple, and 0 otherwise). Therefore, we have a polynomial distinguisher D_2 which is able to tell square Diffie-Hellman triple from a random triple with same non-negligible advantage.

Based on the above arguments, we know the fact that SDDH $\Leftrightarrow$ InvDDH.

Then we consider the equivalence between DDDH and DDH.

DDDH $\Leftrightarrow$ DDH.

Proof: Given $(g, g^x, g^y, g^{x/y})$, one simply submits $(g, g^y, g^{x/y}, g^x)$ to DDH to decide the divisible format of the quadruple;

DDH $\Leftrightarrow$ DDDH

Conversely, given (g, g^x, g^y, g^{xy}), one queries DDDH with (g, g^{xy}, g^y, g^x) and return DDDH's answer (plus, queries can be easily randomized if needed).

Therefore, we know the fact that DDDH $\Leftrightarrow$ DDH.

Finally, we consider the problem whether DDH $\Leftrightarrow$ SDDH or not. Firstly, we show the fact below:

SDDH $\Leftarrow$ DDH.

Proof: Given a distinguisher D, which is able to tell the standard decisional Diffie-Hellman triple from the random triple with non-negligible advantage, we want to show that there exists a distinguisher D_1 that is able to tell the square decisional Diffie-Hellman triple from a random triple with non-negligible advantage. Suppose we are given a triple (g, g^x, g^z), where g^z is either of the form g^y or g^{x^2}, we then choose two strings s, t at random, and compute $u \leftarrow (g^x)^s$,$v \leftarrow (g^x)^t$, $w \leftarrow (g^z)^{st}$. We remark that if (g, g^x, g^z) is square Diffie-Hellman triple then (g, u, v, w) is a Diffie-Hellman quadruple and if (g, g^x, g^z) is random triple then (g, u, v, w) is a random quadruple. Finally, we view the quadruple (g, u, v, w) as an input to the distinguisher D to obtain correct value $b \in \{0, 1\}$ (b=0 if the answer of D is DDH quadruple, and 0 otherwise). Therefore if D_1 is able to distinguish a Diffie-Hellman quadruple or random quadruple with non-negligible advantage then there is a square Difie-Hellman distinguisher D_1 that is able to tell the square decisional Diffie-Hellman triple from a random triple with same non-negligible advantage.

Unfortunately, we are not able to show that DDH $\Leftarrow$ SDDH. This leaves an interesting research problem. Recall that the computational Diffie-Hellman problem (CDH assumption) equivalents the square computational Diffie-Hellman problem (SCDH assumption), we believe this conjecture true if the underlying group $G \in Z_p^*$, e.g., $|G| = q$ and $p = 2q + 1$.

Conjecture: Under the assumption of group structure of G, DDH is equivalent to SDDH.

3.3 Polynomial samples setting

We are interested in generalized variations of Diffie-Hellman problem. These assumptions play central role for the construction of dynamic group protocols([1], [3], [6], [7], [19], [20]). In this section, we are considering variations of the decisional Diffie-Hellman problem in polynomial samples setting. We study those generalized variations of Diffie-Hellman problem by first provided some related notions, then we present optimal reductions from one to another.

Generalized Decisional Diffie-Hellman assumption: for any k, the following distributions are indistinguishable:

- The distribution R^{2k} of any random tuple $(g_1, \cdots, g_k, u_1, \cdots, u_k) \in G^{2k}$, where $g_1, \cdots, g_k$, and $u_1, \cdots, u_k$ are uniformly distributed in G^{2k};
- The distribution D^{2k} of tuples $(g_1, \cdots, g_k, u_1, \cdots, u_k) \in G^{2k}$, where $g_1, \cdots, g_k$ are uniformly distributed in G^k, and $u_1 = g_1^r, \cdots, u_k = g_k^r$ for random $r \in Z_q$ chosen at random.

An algorithm that solves the generalized decisional Diffie-Hellman problem is a statistical test that can efficiently distinguish these two distributions. Generalized decisional Diffie-Hellman assumption means that there is no such a polynomial statistical test.

Similarly, one can extend the variation of decisional Diffie-Hellman problem to the general case of other types.

Generalized square decisional Diffie-Hellman assumption (GSDDH): Let G be a large cyclic group of prime order q defined above. We consider the following two distributions:

- The distribution R^{3k} of any random tuple $(g_1, \cdots, g_k, {g_1}^{x_1}, \cdots, {g_k}^{x_k}, u_1, \cdots, u_k) \in G^{3k}$, where $g_1, \cdots, g_k$, $x_1, \cdots, x_k$ and $u_1, \cdots, u_k$ are uniformly distributed in G^{3k};
- The distribution D^{3k} of tuples $(g_1, \cdots, g_k, {g_1}^{x_1}, \cdots, {g_k}^{x_k}, u_1, \cdots, u_k) \in G^{3k}$, where $g_1, \cdots, g_k$, ${g_1}^{x_1}, \cdots, {g_k}^{x_k}$ are uniformly distributed in G^k while $u_1 = {g_1}^{{x_1}^2}, \cdots, u_k = {g_k}^{{x_k}^2}$ for each x_i uniformly distributed in Z_q.

An algorithm that solves the generalized square decisional Diffie-Hellman problem is a statistical test that can efficiently distinguish these two distributions. Square decisional Diffie-Hellman assumption means that there is no such a polynomial statistical test.

Generalized inverse decisional Diffie-Hellman assumption (GInvDDH): Let G be a large cyclic group of prime order q defined above. We consider the following two distributions:

- The distribution R^{3k} of any random tuple $(g_1, \cdots, g_k, {g_1}^{x_1}, \cdots, {g_k}^{x_k}, u_1, \cdots, u_k) \in G^{3k}$, where $g_1, \cdots, g_k$, $x_1, \cdots, x_k$ and $u_1, \cdots, u_k$ are uniformly distributed in G^{3k};
- The distribution D^{3k} of tuples $(g_1, \cdots, g_k, {g_1}^{x_1}, \cdots, {g_k}^{x_k}, u_1, \cdots, u_k) \in G^{3k}$, where $g_1, \cdots, g_k$, ${g_1}^{x_1}, \cdots, {g_k}^{x_k}$ are uniformly distributed in G^k while $u_1 = {g_1}^{{x_1}^{-1}}, \cdots, u_k = {g_k}^{{x_k}^{-1}}$ for each x_i uniformly distributed in Z_q.

An algorithm that solves the generalized inverse decisional Diffie-Hellman problem (GInvDDH for short) is a statistical test that can efficiently distinguish these two distributions. Generalized inverse decisional Diffie-Hellman assumption means that there is no such a polynomial statistical test.

Now we are able to show that the generalized decisional Diffie-Hellman assumption is true even in the polynomial sampling setting. The argument is by mathematics induction.

6-DDH $\Leftarrow$ 4-DDH.

Proof: Let us consider a machine M that can get a non-negligible advantage ϵ between D^4 and R^4. We define a 6-DDH distinguisher M', which runs as follows: Given any six-tuple $(g_1, g_2, g_3, u_1, u_2, u_3)$, which comes from either R^6 or D^6, M' runs M on the quadruple $(g_1g_2, g_3, u_1u_2, u_3)$ and simply forwards the answer. As explained by the equations presented below, that if $(g_1, g_2, g_3, u_1, u_2, u_3)$ follows the distribution D^6, then $(g_1g_2, g_3, u_1u_2, u_3)$ follows the distribution D^4. It is also the same between R^6 and R^4. As a consequence, our new machine gets the same advantage ϵ in distinguishing D^6 and R^6 with the help of M in distinguishing D^4 and R^4, performing just one more multiplication in G, where G is assumed to be a cyclic group of order q, and g is assumed to be a generator of this group. We denote the output of M(respectively M')as follows: If the input comes from D^4(D^6 respectively), it outputs 1 and 0 if the input tuple comes from R^4(R^6 respectively).

$$\begin{aligned}
&Pr[M(g_1g_2, g_3, u_1u_2, u_3) = 1 | (g_1, g_2, g_3, u_1, u_2, u_3) \in R^6] \\
&= Pr[M(g^{x_1+x_2}, g^{x_3}, g^{x_4+x_5}, g^{x_6}) = 1 | x_1, x_2, x_3, x_4, x_5, x_6 \in Z_q] \\
&= Pr[M(g^x, g^y, g^z, g^r) = 1 | x, y, z, r \in Z_q] \\
&= Pr[M(g_1, g_2, u_1, u_2) = 1 | (g_1, g_2, u_1, u_2) \in R^4]
\end{aligned}$$

And

$$\begin{aligned}
&Pr[M(g_1g_2, g_3, u_1u_2, u_3) = 1 | (g_1, g_2, g_3, u_1, u_2, u_3) \in D^6] \\
&= Pr[M(g^{x_1+x_2}, g^{x_3}, g^{r(x_1+x_2)}, g^{rx_3}) = 1 | x_1, x_2, x_3, r \in Z_q] \\
&= Pr[M(g^x, g^y, g^{rx}, g^{ry}) = 1 | x, y, r \in Z_q] \\
&= Pr[M(g_1, g_2, u_1, u_2) = 1 | (g_1, g_2, u_1, u_2) \in D^4]
\end{aligned}$$

4-DDH $\Leftarrow$ 6-DDH

Let us consider a machine M that can get a non-negligible advantage ϵ between D^6 and R^6. We define a 4-DDH distinguisher M', which runs as follows: on a given quadruple (g_1, g_2, u_1, u_2), M' runs M on the six-tuple $(g_1, g_2, g_1^s g_2^t, u_1, u_2, u_1^s u_2^t)$, for randomly chosen s and t in Z_q, and simply forwards the answer. Once again, the advantage of our new distinguisher M' is exactly the same as the advantage of M, with very few more computations: we assume again g to be a generator of G, and we insist on the fact that Z_q is a field.

$$\begin{aligned}
&Pr[M'(g_1, g_2, u_1, u_2) = 1 | (g_1, g_2, u_1, u_2) \in D^4] \\
&= Pr[M(g^{x_1}, g^{x_2}, g^{sx_1+tx_2}, g^{rx_1}, g^{rx_2}, g^{srx_1+trx_2}) = 1 | x_1, x_2, r, s, t \in Z_q] \\
&= Pr[M(g^{x_1}, g^{x_2}, g^{x_3}, g^{rx_1}, g^{rx_2}, g^{rx_3}) = 1 | x_1, x_2, x_3, r \in Z_q] \\
&= Pr[M(g_1, g_2, g_3, u_1, u_2, u_3) = 1 | (g_1, g_2, g_3, u_1, u_2, u_3) \in D^6]
\end{aligned}$$

And

$$Pr[M'(g_1, g_2, u_1, u_2) = 1 | (g_1, g_2, u_1, u_2) \in R^4]$$
$$= Pr[M(g^{x_1}, g^{x_2}, g^{sx_1+tx_2}, g^{y_1}, g^{y_2}, g^{sy_1+ty_2}) = 1 | x_1, x_2, s, t, y_1, y_2 \in Z_q]$$
$$= Pr[M(g^{x_1}, g^{x_2}, g^{x_3}, g^{y_1}, g^{y_2}, g^{y_3}) = 1 | (x_1, x_2, x_3, y_1, y_2, y_3) \in {Z_q}^6]$$
$$= Pr[M(g_1, g_2, g_3, u_1, u_2, u_3) = 1 | (g_1, g_2, g_3, u_1, u_2, u_3) \in R^6]$$

Based on the above argument, we obtain the useful result: the Decisional Diffie-Hellman Problems, 4-DDH and 6-DDH, are equivalent.

We known that the obtained reductions are optimal since an advantage against one of these problems can be reached against the other one. Therefore, under the sole classical Decisional Diffie-Hellman assumption, for any k, the generalized decisional Diffie-Hellman assumption is indistinguishable.

With the same technique above, the generalized square decisional Diffie-Hellman assumption and the generalized inverse decisional Diffie-Hellman assumption can be easily proved. We also remark that the standard hybrid technique provides alternative approach to prove the Decisional Diffie-Hellman problem in the polynomial sampling setting.

4 Conclusions

We have studied the relationship among variations of Diffie-Hellman problem including the computational and decisional cases with efficient reductions. We show that all four variations of computational Diffie-Hellman problem are equivalent if the order of a underlying cyclic group is large prime. Also, we are considering variations of the decisional Diffie-Hellman problem in single sample and polynomial samples setting. We are able to show that all variations are equivalent except for the argument DDH $\Leftarrow$ SDDH, and thus leave an interesting open problem.

References

1. Eli Biham, Dan Boneh, and Omer Reingold. Breaking generalized Diffie Hellman modulo a composite is no easier than factoring. Information Processing Letters, 70:83–87, 1999.
2. Bresson, Chevassut and Pointcheval, The Group Diffie-Hellman Problems, SAC'02.
3. Mike Burmester, Yvo Desmedt, and Jennifer Seberry. Equitable key escrow with limited time span (or, how to enforce time expiration cryptographically). In K. Ohta and D. Pei, editors, Advances in Cryptology – ASIACRYPT '98, number 1514 in Lecture Notes in Computer Science, pages 380–391. Springer Verlag, Berlin Germany, 1998.
4. D.Beaver: Foundations of Secure Interactive Computing. CRYPTO 1991: 377-391.

5. Dan Boneh. The Decision Diffie- Hellman problem. In Third Algorithmic Number Theory Symposium, number 1423 in Lecture Notes in Computer Science, pages 48-63. Springer Verlag, Berlin Germany, 1998.
6. Christian Cachin, Klaus Kursawe, and Victor Shoup. Random oracles in Constantinople: Practical asynchronous Byzantine agreement using cryptography. In Proceedings of the 19th Annual ACM Symposium on Principles of Distributed Computing, Portland, Oregon, July 2000. ACM. Full version appeared as Cryptology ePrint Archive Report 2000/034 (2000/7/7).
7. Jan Camenisch, Ueli Maurer, and Markus Stadler. Digital payment systems with passive anonymity evoking trustees. In E. Bertino, H. Kurth, G. Martella, and E. Montolivo, editors, Proceedings of the Fourth European Symposium on Research in Computer Security (ESORICS), number 1146 in Lecture Notes in Computer Science, pages 33-43, Rome, Italy, September 1996. Springer Verlag, Berlin Germany.
8. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, Advances in Cryptology-CRYPTO'98, number 1462 in Lecture Notes in Computer Science, pages 13-25. International Association for Cryptologic Research, Springer Verlag, Berlin Germany, 1998.
9. Whitfield Diffie and Martin Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT No.2(6):644–654, November 1976.
10. Helena Handschuh, Yiannis Tsiounis, and Moti Yung. Decision oracles are equivalent to matching oracles. In International Workshop on Practice and Theory in Public Key Cryptography '99 (PKC '99), number 1560 in Lecture Notes in Computer Science, Kamakura, Japan, March 1999. Springer Verlag, Berlin Germany.
11. Kevin S. McCurley. The discrete logarithm problem. In Carl Pomerance, editor, Cryptology and Computational Number Theory, volume 42 of Proceedings of Symposia in Applied Mathematics, pages 49-74, Providence, 1990. American Mathematical Society.
12. Ueli M. Maurer and Stefan Wolf. Diffie-Hellman oracles. Neal Koblitz, editor. Advances in Cryptology-CRYPTO '96, number 1109 in Lecture Notes in Computer Science, pages 268–282. International Association for Cryptologic Research, Springer Verlag, Berlin Germany, 1996.
13. Ueli M. Maurer and Stefan Wolf. Lower bounds on generic algorithms in groups. In Kaisa Nyberg, editor, Advances in Cryptology-EUROCRYPT '98, number 1403 in Lecture Notes in Computer Science, pages 72–84. International Association for Cryptologic Research, Springer Verlag, Berlin Germany, 1998.
14. Ueli M. Maurer and Stefan Wolf. Diffie-Hellman, Decision Diffie-Hellman, and discrete logarithms. In IEEE Symposium on Information Theory, page 327, Cambridge, USA, August 1998.
15. Moni Naor and Omer Reingold. Number theoretic constructions of efficient pseudo-random functions. In 38th Symposium on Foundations of Computer Science (FOCS), pages 458-467. IEEE Computer Society Press, 1997.
16. Tatsuaki Okamoto and David Pointcheval, The Gap-Problems: a New Class of Problems for the Security of Cryptographic Schemes. Proceedings of the 2001 International Workshop on Practice and Theory in Public Key Cryptography (PKC'2001)(13-15 February 2001, Cheju Island, South Korea) K. Kim Ed., Pages 104-118, LNCS 1992, Springer-Verlag, 2001.

17. Birgit Pfitzmann and Ahmadeza Sadeghi. Anonymous fingerprinting with direct non-repudiation. T. Okamoto, editor. Advances in Cryptology – ASIACRYPT '2000, number 1976 in Lecture Notes in Computer Science, Kyoto, Japan, 2000, pages 401–414. International Association for Cryptologic Research, Springer Verlag, Berlin Germany.
18. Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, Advances in Cryptology-EUROCRYPT'97, number 1233 in Lecture Notes in Computer Science, pages 256–266. International Association for Cryptologic Research, Springer Verlag, Berlin Germany, 1997.
19. Ahmad-Reza Sadeghi, Michael Steiner: Assumptions Related to Discrete Logarithms: Why Subtleties Make a Real Difference; Eurocrypt 2001, LNCS 2045, Springer-Verlag, May 2001, 243-260.
20. Michael Steiner, Gene Tsudik, and Michael Waidner. Key agreement in dynamic peer groups. IEEE Transactions on Parallel and Distributed Systems, 11(8):769-780, August 2000.
21. Stefan Wolf. Information theoretically and Computationally Secure Key Agreement in Cryptography. PhD thesis, ETH Zurich, 1999.