Workshop on Selected Areas in Cryptography 2002 (15 – 16 august 2002, St. John's, Newfoundland, Canada)
H. Heys and K. Nyberg Eds. Springer-Verlag, LNCS ????, pages ???–???.

The Group Diffie-Hellman Problems

Emmanuel Bresson[1], Olivier Chevassut[2,3], and David Pointcheval[1]

[1] École normale supérieure, 75230 Paris Cedex 05, France
http://www.di.ens.fr/~ {bresson,pointche}, {Emmanuel.Bresson,David.Pointcheval}@ens.fr.
[2] Lawrence Berkeley National Laboratory, Berkeley, CA 94720, USA,
http://www.itg.lbl.gov/~chevassu, OChevassut@lbl.gov.
[3] Université Catholique de Louvain, 31348 Louvain-la-Neuve, Belgium.

Abstract. In this paper we study generalizations of the Diffie-Hellman problems recently used to construct cryptographic schemes for practical purposes. The *Group Computational* and the *Group Decisional Diffie-Hellman assumptions* not only enable one to construct efficient pseudo-random functions but also to naturally extend the Diffie-Hellman protocol to allow more than two parties to agree on a secret key. In this paper we provide results that add to our confidence in the GCDH problem. We reach this aim by showing exact relations among the GCDH, GDDH, CDH and DDH problems.

1 Introduction

The theoretical concepts of public-key cryptography go back to Diffie and Hellman in 1976 [10] whereas the first public-key cryptosystem appeared only two years later to Rivest, Shamir and Adleman [13]. In their seminal paper *New Directions in Cryptography*, Diffie and Hellman provided a method whereby two principals communicating over an insecure network can agree on a secret key: a key that a (computationally bounded) adversary cannot recover by only eavesdropping on the flows exchanged between the two principals.

Given a prime-order cyclic group $\mathbb{G}$ and a generator g, the Diffie-Hellman protocol works as follows. Two principals U_1, U_2 pick at random $x_1, x_2 \in [1, |\mathbb{G}|]$ and exchange the values g^{x_1}, g^{x_2} over the network. Principal U_1 (U_2 resp.) then computes the Diffie-Hellman secret $g^{x_1 x_2}$ upon receiving the flow from principal U_2 (U_1 resp.). The motivation for running this protocol is to use the Diffie-Hellman secret as input of key derivation function mapping elements of the cyclic group to the space of either a MAC and/or a symmetric cipher.

The security of Diffie-Hellman schemes has thus far been based on two intractability assumptions. Schemes analyzed in the random-oracle model [4] generally rely on the *Computational Diffie-Hellman assumption* (CDH-assumption) which states that given the two values g^{x_1}, g^{x_2} a computationally bounded adversary can not recover the Diffie-Hellman secret [2, 3]. Strong security for schemes analyzed in the standard model usually relies on a stronger assumption than the CDH one [3, 14], the so called *Decision Diffie-Hellman assumption* (DDH-assumption). It states that given g^{x_1}, g^{x_2} a computationally bounded adversary cannot distinguish the Diffie-Hellman secret from a random element in the group. This latter assumption is also useful to prove secururity of El-Gamal -based encryption schemes [11, 9].

With the advance of multicast communication the Diffie-Hellman method has been extended to allow more than two principals to agree on a secret key [16]. In the case of three parties, for example, each principal picks at random a value

$x_i \in [1, |\mathbb{G}|]$ and they exchange the set of values $g^{x_i}, g^{x_i x_j}$, for $1 \leq i < j \leq 3$, to compute the common group Diffie-Hellman secret $g^{x_1 x_2 x_3}$.

The security of group Diffie-Hellman schemes has thus far been based on generalizations of the Diffie-Hellman assumptions. Schemes analyzed in the random-oracle model [4] have been proved secure under the *Group Computational Diffie-Hellman assumption* (GCDH-assumption) which states that given the values $g^{\prod x_i}$, for *some* choice of proper subsets of $\{1, \ldots, n\}$, a computationally bounded adversary cannot recover the group Diffie-Hellman secret [6, 8]. This assumption has also found application in the context of pseudo-random functions [12]. Schemes for group Diffie-Hellman key exchange analyzed without the random-oracle model achieve strong security guarantees under the *Group Decision Diffie-Hellman assumption* (GDDH-assumption) which states that given the values $g^{\prod x_i}$ the adversary cannot distinguish the group Diffie-Hellman secret from a random element in the group [7].

Motivated by the increasing applications of the group Diffie-Hellman assumptions to cryptography we have studied their validity. Although we cannot prove the equivalence between the CDH and the GCDH in this paper, we are able to show that the GCDH can be considered to be a standard assumption. We reach this aim by relating the GCDH to both the CDH-assumption and the DDH-assumption. The GCDH was furthermore believed to be a weaker assumption than the GDDH but it was not proved until now. In this paper we prove this statement by comparing the quality of the reduction we obtain for the GCDH and the one we carry out to relate the GDDH to the DDH. The results we obtain in this paper add to our confidence in the GCDH-assumption.

This paper is organized as follows. In Section 2 we summarize the related work. In Section 3 we formally define the group Diffie-Hellman complexity assumptions. In Section 4 we show the relationship between the GDDH and the DDH. In Section 5 we carry out a similar treatment to relate the GCDH to both the CDH and DDH.

2 Related Work

The *generalized* GDDH-assumption, defined in terms of the values $g^{\prod x_i}$ formed from *all* the proper subsets of $\{1, \ldots, n\}$, first appeared in the literature in the paper of Steiner et al. [16]. Steiner et al. exhibited an asymptotic reduction to show that the DDH-assumption implies the generalized GDDH-assumption. In his PhD thesis [15] Steiner later quantified this reduction and showed that relating the *generalized* GDDH problem to the DDH problem leads to very inefficient reductions, especially because a Genralized GDDH instance is exponentially large.

In practice, it is possible to fortunately improve on the quality of the reductions since only some of the proper subsets of indices are used in the key exchange protocol flows. These are special forms of the generalized GDDH or even the generalized GCDH. To prove secure protocols for static group Diffie-Hellman key exchange [6], we used the special form of basic trigon. To prove

secure protocols for dynamic group Diffie-Hellman [8, 7], we used the form of extended basic trigon.

The first attempts to relate the *generalized* GCDH to the CDH is due to Biham et al. [1]. Their results gave some confidence in the *generalized* GCDH in the multiplicative group $\mathbb{Z}_n^*$ (where n is composite) by relating it to factoring, but in group key exchange, schemes [8, 6, 7] use large group of known prime order so that the proofs can use the multiplicative random self-reduction. therefore, we focus on this case in the following.

3 Complexity Assumptions

This section presents the group Diffie-Hellman assumptions by first introducing the notion of group Diffie-Hellman distribution and using it to define the group computational Diffie-Hellman assumption (GCDH-Assumption) and the decisional Diffie-Hellman assumption (GDDH-Assumption). For the remainder of the paper we fix a prime-order cyclic group $\mathbb{G} = \langle g \rangle$.

Group Diffie-Hellman distribution. The group Diffie-Hellman distribution (GDH-Distribution) of size an integer n is the set of elements $g^{\prod_{j\in J} x_j}$ for some proper subsets $J \subsetneq I_n = \{1, .., n\}$. We formally write it using the set $\mathcal{P}(I_n)$ of all subsets of I_n and any subset Γ_n of $\mathcal{P}(I_n)\backslash\{I_n\}$, as follows:

$$\mathsf{GDH}_{\Gamma_n} = \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{J\in\Gamma_n} \mid x_1, \ldots, x_n \in_R \mathbb{Z}_q \right\}.$$

Since this distribution is a function of the parameters n and Γ_n it could be instantiated with any of the following special forms:

- If $n = 2$ and $\Gamma_2 = \{\{1\}, \{2\}\}$, the GDH-Distribution is the Diffie-Hellman distribution.

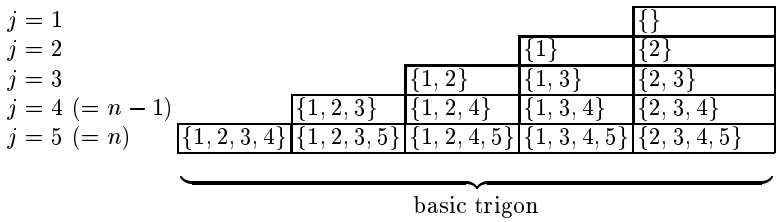

Fig. 1. Basic GDH-Distribution. GDH-Distribution when $n = 5$ and $\Gamma = \mathcal{T}_5$.

- If Γ_n has the following triangular structure $\mathcal{T}_n$, the GDH-Distribution is the basic trigon depicted in Figure 1:

$$\mathcal{T}_n = \bigcup_{1\le j\le n} \left\{ \{i \mid 1 \le i \le j, i \ne k\} \mid 1 \le k \le j \right\}$$

  This triangular structure is employed to properly deal with the security of a static group Diffie-Hellman key exchange protocol [8], in which the players send their flows in a fixed order.

– If Γ_n has the following structure $\mathcal{E}_n$, the GDH-Distribution is the extended trigon depicted in Figure 2:

$$\mathcal{E}_n = \bigcup_{1\leq j\leq n-2} \left\{ \{i \,|\, 1 \leq i \leq j, i \neq l\} \mid 1 \leq l \leq j \right\} \bigcup \left\{ \{i | 1 \leq i \leq n, i \neq k, l\} | 1 \leq k, l \leq n \right\}$$

This structure is used to properly deal with the security of a dynamic group Diffie-Hellman key exchange protocol [6, 7], in which *any* player should be able to send the last flow (thus, the last line of the extended trigon must contain *any* of the proper subsets of $n-2$ elements, see Figure 2)

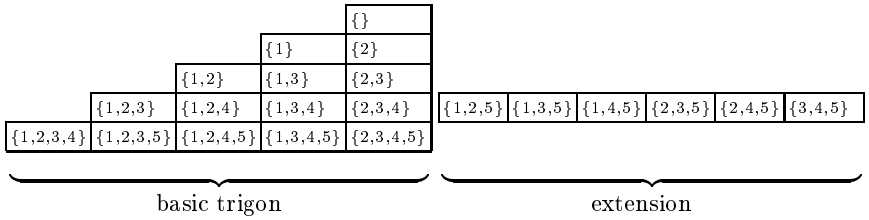

Fig. 2. Extended GDH-Distribution: GDH-Distribution when $n = 5$ and $\Gamma = \mathcal{E}_5$.

– If $\Gamma = \mathcal{P}(I)\backslash\{I_n\}$, the GDH-distribution is the generalized GDH-distribution since we have *all* the proper subsets of $\{1, \ldots, n\}$.

The cardinality of a structure Γ is denoted by γ_n. For $\mathcal{T}_n$, we have $\gamma_n(\mathcal{T}_n) = \sum_{i=1}^{n} i = n(n+1)/2$ since the i-th "line" of this structure has exactly i elements. And the cardinality of $\mathcal{E}_n$ is $\gamma_n(\mathcal{E}_n) = \gamma_n(\mathcal{T}_n) + \binom{n-2}{n} - n + 1 = n^2 - n + 1$ since the extension of the $n-1$-th line of this structure has exactly $\binom{n-2}{n} - (n-1)$ elements. It is also worthwhile to mention that the cardinality of the generalized one is $2^n - 2$.

The computational Diffie-Hellman assumption. A(T, ε)-GCDH$_\Gamma$-attacker in $\mathbb{G}$ is a probabilistic Turing machine Δ running in time T such that

$$\mathsf{Succ}^{\mathsf{gcdh}_\Gamma}_{\mathbb{G}}(\Delta) = \Pr_{x_i}\left[\Delta(\mathsf{GDH}_\Gamma(x_i)) = g^{x_1 \cdots x_n}\right] \geq \varepsilon$$

where $\mathsf{GDH}_\Gamma(x_i)$ means a tuple randomly drawn from the GDH_Γ distribution by using random elements x_i. We will (abusively) denote Δ operating on such a tuple by $\Delta(\mathsf{GDH}_\Gamma)$.

The GCDH$_\Gamma$-Problem is (T, ε)-**intractable** if there is no (T, ε)-GCDH$_\Gamma$-attacker in $\mathbb{G}$. The GCDH$_\Gamma$-assumption states this is the case for all polynomial T and non-negligible ε.

The decisional Diffie-Hellman assumption. Let us first define two additional distributions from the GDH-Distribution:

$$\mathsf{GDH}^{\star}_{\Gamma} = \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{J\in\Gamma}, (I_n, g^{x_1\cdots x_n}) \mid x_1, \ldots, x_n \in_R \mathbb{Z}_q \right\}$$

$$\mathsf{GDH}^{\$}_{\Gamma} = \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{J\in\Gamma}, (I_n, g^{r}) \mid x_1, \ldots, x_n, r \in_R \mathbb{Z}_q \right\}$$

A (T, ε)-GDDH$_\Gamma$-distinguisher in $\mathbb{G}$ is a probabilistic Turing machine Δ running in time T such that:

$$\mathsf{Adv}^{\mathsf{gddh}_\Gamma}_{\mathbb{G}}(\Delta) = \left| \Pr_{x_i}\left[\Delta\big(\mathsf{GDH}^{\star}_{\Gamma}\big) = 1\right] - \Pr_{x_i, r}\left[\Delta\big(\mathsf{GDH}^{\$}_{\Gamma}\big) = 1\right] \right| \geq \varepsilon$$

The GDDH$_\Gamma$-Problem is (T, ε)**-intractable** if there is no (T, ε)-GDDH$_\Gamma$-distinguisher in $\mathbb{G}$. The GDDH$_\Gamma$-assumption states this is the case for all polynomial T and non-negligible ε.

The Random Self-Reducibility. The Diffie-Hellman problems have the nice property of random self-reducibility [12]. Certainly the most common is the additive random self-reducibility, which works as follows. Given, for example, an instance $\mathcal{D} = (g^a, g^b, g^c, g^{ab}, g^{bc}, g^{ac})$ for any a, b, c it is possible to generate a random instance

$$\mathcal{D}' = (g^{(a+\alpha)}, g^{(b+\beta)}, g^{(c+\gamma)}, g^{(a+\alpha).(b+\beta)}, g^{(b+\beta).(c+\gamma)}, g^{(a+\alpha).(c+\gamma)})$$

where α, β and γ are random numbers in $\mathbb{Z}_q$, whose solution may help us to solve $\mathcal{D}$. Indeed, given the solution $z = g^{(a+\alpha).(b+\beta).(c+\gamma)}$ to the instance $\mathcal{D}'$ it is possible to recover the solution g^{abc} to the random instance $\mathcal{D}$ (i.e. $g^{abc} = z(g^{ab})^{-\gamma}(g^{ac})^{-\beta}(g^{bc})^{-\alpha}(g^a)^{-\beta\gamma}(g^b)^{-\alpha\gamma}(g^c)^{-\alpha\beta}g^{-\alpha\beta\gamma}$). However the cost of such a computation may be high; furthermore it is easily seen that such a reduction works only if $\mathcal{D}$ is the *generalized* DH-Distribution and that its cost increases exponentially with the size of $\mathcal{D}$.

On the other hand, the multiplicative random self-reducibility works for any form of the GDDH-Problem (but also GCDH)in a prime-order cyclic group. Given, for example, an instance $\mathcal{D} = (g^a, g^b, g^{ab}, g^{ac}, K)$ for any a, b, c it is easy to generate a random instance $\mathcal{D}' = (g^{a\alpha}, g^{b\beta}, g^{ab\alpha\beta}, g^{ac\alpha\gamma}, K^{\alpha\beta\gamma})$ where α, β and γ are random numbers in $\mathbb{Z}_q^*$. And given the solution "`True`" or "`False`" to the instance $\mathcal{D}'$, we directly get the solution to the random instance $\mathcal{D}$. Such a reduction is efficient and only requires a linear number of modular exponentiations.

4 The Group Decisional Diffie-Hellman Problem

In this section we provide a reduction of the Decisional Diffie-Hellman (DDH) problem to the group Decisional Diffie-Hellman problem.

Good structure family. For any indexed structure Γ_n, we consider an auxiliary structure $\hat{\Gamma}_n$ built from the set $\{0, 3, \ldots, n+1\}$ in the same way Γ_n is built from the set I_n. We see a structure family Γ as a good structure if for any integer n greater than 3 the following four conditions are satisfied (the basic trigon and extended trigon are good structure families):

1. $\forall J \in \Gamma_n, \{1, 2\} \subseteq J \Rightarrow J_{12} \cup \{0\} \in \hat{\Gamma}_{n-1}$
2. $\forall J \in \Gamma_n, 1 \notin J, 2 \in J \Rightarrow J_2 \in \hat{\Gamma}_{n-1}$
3. $\forall J \in \Gamma_n, 1 \in J, 2 \notin J \Rightarrow J_1 \in \hat{\Gamma}_{n-1}$

4. $\forall J \in \Gamma_n, 1 \notin J, 2 \notin J \Rightarrow J \in \hat{\Gamma}_{n-1}$

We then slightly change the notation when we will refer to the distribution $\mathsf{GDH}^{\star}_{\Gamma_n}$ ($\mathsf{GDH}^{\$}_{\Gamma_n}$ resp) to be $\mathcal{U}^{\star}_n$ ($\mathcal{U}^{\$}_n$ resp) wherein the tuple is appended $g^{x_1 \cdots x_n}$ (g^r resp) as follows:

$$\begin{aligned}\mathcal{U}_n &= \mathsf{GDH}_{\Gamma_n} \\ &= \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{\substack{J\in\Gamma_n \\ \{1,2\}\not\subseteq J}}, \left(J, g^{\prod_{j\in J} x_j}\right)_{\substack{J\in\Gamma_n \\ \{1,2\}\subseteq J}} \;\middle|\; x_1, \ldots, x_n \in_R \mathbb{Z}_q \right\}\end{aligned}$$

We also in a similar way define the two additional distributions $\mathcal{V}^{\star}_n$ and $\mathcal{V}^{\$}_n$, wherein the tuple in $\mathcal{V}_n$ is appended $g^{\alpha x_3 \cdots x_n}$ and g^r, respectively:

$$\mathcal{V}_n = \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{\substack{J\in\Gamma_n \\ \{1,2\}\not\subseteq J}}, \left(J, g^{\alpha \prod_{j\in J_{12}} x_j}\right)_{\substack{J\in\Gamma_n \\ \{1,2\}\subseteq J}} \;\middle|\; x_1, \ldots, x_n, \alpha \in_R \mathbb{Z}_q \right\}$$

where for each J, J_{12} denotes $J\backslash\{1,2\}$. We note that under the constraint $\alpha = x_1 x_2$, one has $\mathcal{V}_n = \mathcal{U}_n$.

A (T,ε)-$\mathcal{V}_n$-attacker in $\mathbb{G}$ is a probabilistic Turing machine Δ running in time T such that

$$\mathsf{Succ}^{\mathcal{V}_n}_{\mathbb{G}}(\Delta) = \Pr_{x_i,\alpha}\left[\Delta(\mathcal{V}_n) = g^{x_1\cdots x_n}\right] \geq \varepsilon$$

A (T,ε)-$\mathcal{V}_n$-distinguisher in $\mathbb{G}$ is a probabilistic Turing machine Δ running in time T such that:

$$\mathsf{Adv}^{\mathcal{V}_n}_{\mathbb{G}}(\Delta) = \left| \Pr_{x_i,\alpha}\left[\Delta\big(\mathcal{V}^{\star}_n\big) = 1\right] - \Pr_{x_i,\alpha,r}\left[\Delta\big(\mathcal{V}^{\$}_n\big) = 1\right] \right| \geq \varepsilon$$

We emphasize that while a $\mathcal{V}_n$-attacker must compute the value $A = g^{x_1\cdots x_n}$, a $\mathcal{V}_n$-distinguisher must distinguish the value $B = g^{\alpha x_3 \cdots x_n}$ from a random value in $\mathbb{G}$.

Theorem 1. *Let $\mathbb{G}$ be a cyclic multiplicative group of prime order q, $t_{\mathbb{G}}$ the time needed for an exponentiation in $\mathbb{G}$. Let Γ be a good structure family. Then for any integer $n > 1$, we have:*

$$\mathsf{Adv}^{\mathsf{gddh}_{\Gamma_n}}_{\mathbb{G}}(t) \leq (2n-3)\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(t') \;\; \textit{where } t' \leq t + t_{\mathbb{G}} \sum_{i=3}^{n} \gamma_i$$

where γ_i is the size of Γ_i, for any i.

The proof of this theorem results from the combinaison of the following two lemmas however before to prove it let's plug in some numerical values for the time of computation: for the structure of basic trigon $\mathcal{T}_n$ the time is $t' \leq t + (n-2)(n+3)(n+4)t_{\mathbb{G}}/6 \leq t + n^3 t_{\mathbb{G}}/3$; for the structure of extended trigon $\mathcal{E}_n$ the time is $t' \leq t + n(n-2)(n+5)t_{\mathbb{G}}/3 \leq t + 2n^3 t_{\mathbb{G}}/3$.

Lemma 2. *For any integer n and any structure Γ_n, we have*

$$\left|\mathsf{Adv}^{\mathsf{gddh}_{\Gamma_n}}_{\mathbb{G}}(t) - \mathsf{Adv}^{\mathcal{V}_n}_{\mathbb{G}}(t)\right| \leq 2\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(t + \gamma_n t_{\mathbb{G}}) \tag{1}$$

Proof. We consider an adversary $\mathcal{A}$ against the GDDH_{Γ_n} problem. Such an adversary, on input a distribution depending on a bit b, replies with a bit b' which is a guess for b. We assume that $\mathcal{A}$ runs in polynomial time t, in particular it always terminates, even if the input comes neither from $\mathcal{U}^\star_n$ nor from $\mathcal{U}^\$_n$. Then we define the following two games: $\mathbf{G}_0$, $\mathbf{G}_1$ and consider the event S_i in game $\mathbf{G}_i$ as $b = b'$. Also we denote $\mathsf{Adv}^{\mathbf{G}_i}(\mathcal{A}) = 2\Pr[S_i] - 1$.

Game $\mathbf{G_0}$. In this game, we are given a Diffie-Hellman triple $(A, B, C) = (g^{x_1}, g^{x_2}, g^{x_1 x_2})$. Then we choose at random $(x_3, \ldots, x_n)$ in $\mathbb{Z}^*_q$ and compute a tuple U_n which follows the distribution $\mathcal{U}_n$, as follows

$$\mathsf{U}_n = \left\{ \left(J, g^{\Pi_{j\in J}\, x_j}\right)_{J\in\Gamma_n, 1\notin J, 2\notin J}, \left(J, A^{\Pi_{j\in J_1}\, x_j}\right)_{J\in\Gamma_n, 1\in J, 2\notin J}, \right.$$
$$\left. \left(J, B^{\Pi_{j\in J_2}\, x_j}\right)_{J\in\Gamma_n, 1\notin J, 2\in J}, \left(J, C^{\Pi_{j\in J_{12}}\, x_j}\right)_{J\in\Gamma_n, \{1,2\}\subseteq J} \right\}$$

where for any J, we denote by J_1, J_2, J_{12} the sets $J\backslash\{1\}, J\backslash\{2\}, J\backslash\{1,2\}$ respectively. It is easy to see that the computed tuple follows exactly the distribution $\mathcal{U}_n = \mathsf{GDH}_{\Gamma_n}$. Then if $b = 1$, one appends to U_n the value $C^{x_3\cdots x_n}$; and if $b = 0$, one appends to U_n a value g^r, where r is a random exponent.

It is easy to see that the computed tuple follows exactly the same distribution, that is $\mathcal{U}^\star_n$ (resp. $\mathcal{U}^\$_n$) if $b = 1$ (resp. $b = 0$). Thus by definition, we have

$$\Pr[S_0] = \frac{\mathsf{Adv}^{\mathsf{gddh}_{\Gamma_n}}_{\mathbb{G}}(\mathcal{A}) + 1}{2} \leq \frac{\mathsf{Adv}^{\mathsf{gddh}_{\Gamma_n}}_{\mathbb{G}}(t) + 1}{2}$$

Game $\mathbf{G_1}$. Game $\mathbf{G}_1$ is the same as game $\mathbf{G}_0$ except that we are given a tuple $(A, B, C) = (g^{x_1}, g^{x_2}, g^\alpha)$, where α is a random exponent. It is easy to see that the tuple given to the adversary is perfectly indistinguishable from a tuple drawn from $\mathcal{V}^\star_n$ (resp. $\mathcal{V}^\$_n$) if $b = 1$ (resp. $b = 0$). Then it follows that

$$\Pr[S_1] \leq \left(\mathsf{Adv}^{\mathcal{V}_n}_{\mathbb{G}}(t) + 1\right)/2$$

Also, the only difference in the probability distributions in the two games is upper-bounded by:

$$\left|\Pr[S_1] - \Pr[S_0]\right| \leq \mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(t + \gamma_n t_{\mathbb{G}}) \tag{2}$$

□

Lemma 3. *For any integer n, we have*

$$\mathsf{Adv}^{\mathcal{V}_n}_{\mathbb{G}}(t) \leq \mathsf{Adv}^{\mathsf{gddh}_{\Gamma_{n-1}}}_{\mathbb{G}}(t + \gamma_n t_{\mathbb{G}}) \tag{3}$$

Proof. We consider a $\mathcal{V}_n$-distinguisher $\mathcal{A}$ running in time t and we use it to built a $\mathcal{U}_{n-1}$-distinguisher. To that goal, we receive as input a tuple drawn from either $\mathcal{U}^{\star}_{n-1}$ or $\mathcal{U}^{\$}_{n-1}$; We will use $\mathcal{A}$ to guess the underlying bit b. In the given tuple, we denote by (I_{n-1}, u_{n-1}) the last value and by U_{n-1} the first values:

$$\mathsf{U}_{n-1} = \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{J\in\Gamma_{n-1}} \right\}$$

We split this tuple into two blocks, depending on whether $1 \in J$ or not:

$$\mathsf{U}_{n-1} = \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{J\in\Gamma_{n-1},1\notin J}, \left(J, g^{\prod_{j\in J} x_j}\right)_{J\in\Gamma_{n-1},1\in J} \right\}$$

or, equivalently, by denoting $J_1 = J\backslash\{1\}$ for any J:

$$\mathsf{U}_{n-1} = \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{J\in\Gamma_{n-1},1\notin J}, \left(J, g^{x_1 \prod_{j\in J_1} x_j}\right)_{J\in\Gamma_{n-1},1\in J} \right\}$$

Now we write this tuple by renaming the variables $x_1, \ldots, x_{n-1}$ to be respectively $X_0, X_3, \ldots, X_n$. It follows that the elements of U_{n-1} are now indexed by the elements of $\hat{\Gamma}_{n-1}$ rather than Γ_{n-1}.

$$\mathsf{U}_{n-1} = \left\{ \left(J, g^{\prod_{j\in J} X_j}\right)_{J\in\hat{\Gamma}_{n-1},0\notin J}, \left(J, g^{X_0 \prod_{j\in J_0} X_j}\right)_{J\in\hat{\Gamma}_{n-1},0\in J} \right\}$$

Now we rewrite U_{n-1} using the elements of Γ_n as indices to obtain a new tuple W_n. We can derive the first block of W_n from the first block of U_{n-1} since for any $J \in \Gamma_n$ such that $1 \notin J$ and $2 \notin J$, we have $J \in \hat{\Gamma}_{n-1}$ because Γ is a "good" structure family. This lead us to the following tuple:

$$\mathsf{W}_n = \left\{ \left(J, g^{\prod_{j\in J} X_j}\right)_{J\in\Gamma_n,1\notin J,2\notin J}, \left(J_1, g^{\prod_{j\in J_1} X_j}\right)_{J\in\Gamma_n,1\in J,2\notin J}, \right.$$
$$\left. \left(J_2, g^{\prod_{j\in J_2} X_j}\right)_{J\in\Gamma_n,1\notin J,2\in J}, \left(J, g^{X_0 \prod_{j\in J_{12}} X_j}\right)_{J\in\Gamma_n,\{1,2\}\subseteq J} \right\}$$

Now we pick at random two values X_1, X_2 in $\mathbb{Z}_q^*$ and use them to construct the following tuple V_n:

$$\left\{ \left(J, g^{\prod_{j\in J} X_j}\right)_{J\in\Gamma_n,1\notin J,2\notin J}, \left(J, g^{X_1 \prod_{j\in J_1} X_j}\right)_{J\in\Gamma_n,1\in J,2\notin J}, \right.$$
$$\left. \left(J, g^{X_2 \prod_{j\in J_2} X_j}\right)_{J\in\Gamma_n,1\notin J,2\in J}, \left(J, g^{X_0 \prod_{j\in J_{12}} X_j}\right)_{J\in\Gamma_n,\{1,2\}\subseteq J} \right\}$$

The first three blocks collude into one block as follows:

$$\mathsf{V}_n = \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{J\in\Gamma_n,\{1,2\}\nsubseteq J}, \left(J, g^{X_0 \prod_{j\in J_{12}} x_j}\right)_{J\in\Gamma_n,\{1,2\}\subseteq J} \right\}$$

We note that V_n perfectly follows the distribution $\mathcal{V}_n$.

Then V_n is appended (I_n, u_{n-1}) (where $I_n = \{1, \ldots, n\}$) and given to $\mathcal{A}$. The latter returns a bit b' that we relay back as an answer to the $\mathbf{G\text{-}DDH}_{\Gamma_{n-1}}$ problem. The computation time needed to properly generate V_n from the input U_{n-1} is at most $\gamma_n t_{\mathbb{G}}$.

Thus, we have

$$\mathsf{Adv}_{\mathbb{G}}^{\mathsf{gddh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}}) \geq \mathsf{Adv}_{\mathbb{G}}^{\mathcal{V}_n}(t) \tag{4}$$

□

Putting all together we obtain:

$$\begin{aligned}
\mathsf{Adv}_{\mathbb{G}}^{\mathsf{gddh}_{\Gamma_n}}(t) &\leq \mathsf{Adv}_{\mathbb{G}}^{\mathcal{V}_n}(t) + 2\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}) \\
&\leq \mathsf{Adv}_{\mathbb{G}}^{\mathsf{gddh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}}) + 2\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}) \\
&\leq \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}\left(t + \sum_{i=3}^{n} \gamma_i t_{\mathbb{G}}\right) + 2\sum_{i=3}^{n} \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}\left(t + \sum_{j=i}^{n} \gamma_j t_{\mathbb{G}}\right) \\
&\leq (2n-3)\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t') \text{ where } t' \leq t + t_{\mathbb{G}} \sum_{i=3}^{n} \gamma_i
\end{aligned}$$

5 The Group Computational Diffie-Hellman Problem

In this section we show the GCDH is a standard assumption by relating it to both the CDH and the DDH.

Theorem 4. *Let $\mathbb{G}$ be a cyclic multiplicative group of prime order q, $t_{\mathbb{G}}$ the time needed for an exponentiation in $\mathbb{G}$. Then for any integer n and any structure Γ of cardinality γ_n we have:*

$$\mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma}}(t) \leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{cdh}}(t') + (n-2)\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t') \text{ where } t' \leq t + \sum_{i=3}^{n} \gamma_i t_{\mathbb{G}}$$

Proof. We consider an adversary $\mathcal{A}$ against the $\mathbf{G\text{-}CDH}_{\Gamma_n}$ problem. Such an adversary, on input a tuple drawn from the GDH_{Γ} distribution, replies with a single value which is a guess for the corresponding secret. We assume that $\mathcal{A}$ runs in polynomial time t, in particular it always terminates, even if the input does not come from GDH_{Γ}.

We then define the two games $\mathbf{G}_0$, $\mathbf{G}_1$. In each game, we are given a triple (A, B, C) and $n-2$ random elements $(x_3, \ldots, x_n)$ in $\mathbb{Z}_q^*$ and we denote by S_i the event that the adversary $\mathcal{A}$ outputs $C^{x_3 \cdots x_n}$.

Game $\mathbf{G_0}$. In this game, we are given a Diffie-Hellman triple $(A, B, C) = (g^{x_1}, g^{x_2}, g^{x_1 x_2})$. Then using $(x_3, \ldots, x_n)$ we can compute:

$$\mathsf{U}_n = \left\{ \left(J, g^{\prod_{j\in J} x_j}\right)_{J\in\Gamma_n, 1\notin J, 2\notin J}, \left(J, A^{\prod_{j\in J_1} x_j}\right)_{J\in\Gamma_n, 1\in J, 2\notin J}, \right.$$
$$\left. \left(J, B^{\prod_{j\in J_2} x_j}\right)_{J\in\Gamma_n, 1\notin J, 2\in J}, \left(J, C^{\prod_{j\in J_{12}} x_j}\right)_{J\in\Gamma_n, \{1,2\}\subseteq J} \right\}$$

where for any J, we denote by J_1, J_2, J_{12} the sets $J\backslash\{1\}, J\backslash\{2\}, J\backslash\{1,2\}$ respectively. It is easy to see that the computed tuple follows exactly the distribution $\mathcal{U}_n = \mathsf{GDH}_{\Gamma_n}$. Then the tuple U_n is provided to the adversary. By definition, since $C^{x_3\cdots x_n} = g^{x_1\cdots x_n}$, we have $\Pr[S_0] = \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_n}}(\mathcal{A}) \leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_n}}(t)$.

Game $\mathbf{G_1}$. Game $\mathbf{G}_1$ is the same as game $\mathbf{G}_0$ except that we are given a tuple $(A, B, C) = (g^{x_1}, g^{x_2}, g^{\alpha})$, where α is a random. We then perform the same operations as in game $\mathbf{G}_0$ to obtain a tuple following the distribution $\mathcal{V}_n$. The computed tuple is provided to the adversary. By definition, we have $\Pr[S_1] \leq \mathsf{Succ}_{\mathbb{G}}^{\mathcal{V}_n}(t)$.

In both games the computation time needed for generating the tuple from the input a triple (A, B, C) is at most $(\gamma_n - 1)t_{\mathbb{G}}$ where $t_{\mathbb{G}}$ is the time required for an exponentiation in $\mathbb{G}$. Another exponentiation is needed to compute $C^{x_3\cdots x_n}$. Clearly the computational distance between the games is upper-bounded by $\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}})$:

$$\left|\Pr[S_0] - \Pr[S_1]\right| \leq \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}})$$

Game $\mathbf{G_2}$. Game $\mathbf{G}_2$ is the same as game $\mathbf{G}_1$ except that we choose x_1 and x_2 by ourselves. Therefore $(A, B, C) = (g^{x_1}, g^{x_2}, g^{\alpha})$ where x_1 and $x - 2$ are known, but α is not. The remaining of this game is distributed exactly as in the previous one, so $\Pr[S_2] = \Pr[S_1]$.

Game $\mathbf{G_3}$. Game $\mathbf{G}_3$ is the same as game $\mathbf{G}_2$ except that we do not know the elements $(x_3, \ldots, x_n)$. Instead, we are given an instance U_{n-1} of the $\mathbf{G\text{-}CDH}_{\Gamma_{n-1}}$ problem, built from the (unknown) exponents $(\alpha, x_3, \ldots, x_n)$, where α is the same than the underlying (hidden) exponent in C. By operating as in the previous section, we can complete the given tuple by using x_1 and x_2 (which are known) to obtain a tuple V_n following the distribution $\mathcal{V}_n$.

The variables are distributed exactly as in the previous game, so we have $\Pr[S_3] = \Pr[S_2]$. Note however, that we are not long able to decide whether the adversary outputs $C^{x_3\cdots x_n}$ or not, since we do not know $x_3, \ldots, x_n$. But this is not a problem because the two games are identically distributed.

Anyway, since $C^{x_3\cdots x_n} = g^{\alpha x + 3\cdots x_n}$ is the Diffie-Hellman secret associated to the given $\mathbf{G\text{-}CDH}_{\Gamma_{n-1}}$ instance, the adversary outputs $C^{x_3\cdots x_n}$ with probability at most $\mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}})$.

Putting all these together gives us

$$\begin{aligned}\Pr[S_0] &= \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_n}}(\mathcal{A}) \\ &\leq \Pr[S_1] + \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}) \\ &\leq \Pr[S_3] + \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}) \\ &\leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}}) + \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}})\end{aligned}$$

Then it follows:

$$\begin{aligned}\mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_n}}(\mathcal{A}) &\leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}}) + \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}) \\ &\leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_{n-2}}}(t + (\gamma_n + \gamma_{n-1}) t_{\mathbb{G}}) + \\ &\qquad \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + (\gamma_n + \gamma_{n-1}) t_{\mathbb{G}}) + \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}) \\ &\leq \ldots \\ &\leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{cdh}}\left(t + \sum_{i=3}^{n} \gamma_i t_{\mathbb{G}}\right) + \sum_{i=3}^{n} \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}\left(t + \sum_{j=i}^{n} \gamma_j t_{\mathbb{G}}\right) \\ &\leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{cdh}}(t') + (n-2)\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t') \text{ where } t' \leq t + \sum_{i=3}^{n} \gamma_i t_{\mathbb{G}}\end{aligned}$$

□

6 Conclusion

In this paper, we have shown that breaking the Group Computational Diffie-Hellman problem is at least as hard as breaking either the Computational or Decisional (two-party) Diffie-Hellman problems. This result is particularly relevant in practice since when engineers and programmers choose a protocol for authenticated group Diffie-Hellman key exchange [8, 6, 7] they are ensured that the intractability assumptions underlying the security of this protocol have been deeply studied, and thus, well accepted by the cryptographic community. Furthermore providing implementers with an exact measurement of this relations gives them the ability to compare the security guarantees achieved by the protocol in terms of tightness of the reduction. An open problem is to still show whether (when not considered modulo a composite) breaking the GCDH problem is as hard as breaking the CDH problem.

7 Acknowledgments

The second author was supported by the Director, Office of Science, Office of Advanced Scientific Computing Research, Mathematical Information and Computing Sciences Division, of the U.S. Department of Energy under Contract No. DE-AC03-76SF00098. This document is report LBNL-50775. Disclaimer available at http://www-library.lbl.gov/disclaimer .

References

1. E. Biham, D. Boneh, and O. Reingold. Breaking generalized Diffie-Hellman modulo a composite is no easier than factoring. In *Information Processing Letters (IPL)*, volume 70(2), pages 83–87. Elsevier Science, April 1999.
2. S. Blake-Wilson, D. Johnson, and A. Menezes. Key agreement protocols and their security analysis. In M. Darnell, editor, *Proc. of 6^{th} IMA International Conference on Crypotography and Coding*, volume 1355 of *LNCS*, pages 30–45. Springer-Verlag, 1997.
3. S. Blake-Wilson and A. Menezes. Authenticated Diffie-Hellman key agreement protocols. In H. Meijer and S. Tavares, editors, *Proc. of Selected Areas in Cryptography SAC '98*, volume 1556 of *LNCS*, pages 339–361. Springer-Verlag, August 1998.
4. Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In *Proc. of ACM CCS '93*, pages 62–73. ACM Press, November 1993.
5. D. Boneh. The decision Diffie-Hellman problem. In J. P. Buhler, editor, Proc. of the *3^{rd} ANTS Symposium*, volume 1423 of *LNCS*, pages 48–63, Portland, OR, USA, June 1998. Springer-Verlag.
6. E. Bresson, O. Chevassut, and D. Pointcheval. Provably authenticated group Diffie-Hellman key exchange – the dynamic case. In C. Boyd, editor, *Proc. of Asiacrypt '01*, volume 2248 of *LNCS*, pages 290–309. Springer-Verlag, December 2001.
7. E. Bresson, O. Chevassut, and D. Pointcheval. Dynamic group Diffie-Hellman key exchange under standard assumptions. In L. R. Knudsen, editor, *Proc. of Eurocrypt '02*, volume 2332 of *LNCS*, pages 321–336. Springer-Verlag, May 2002.
8. E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater. Provably authenticated group Diffie-Hellman key exchange. In P. Samarati, editor, *Proc. of ACM CCS '01*, pages 255–264. ACM Press, November 2001.
9. R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In H. Krawczyk, editor, *Proc. of Crypto '98*, volume 1462 of *LNCS*, pages 13–25. Springer-Verlag, August 1998.
10. W. Diffie and M. E. Hellman. New directions in cryptography. *Transactions on Information Theory*, IT-22(6):644–654, November 1976.
11. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proc. of Crypto '84*, LNCS 196, pp. 10–18.
12. M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. In *Proc. of FOCS '97*, pages 458–467. IEEE Computer Society Press, October 1997.
13. R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.
14. V. Shoup. On formal models for secure key exchange. Technical Report RZ 3120, IBM Zrich Research Lab, November 1999.
15. M. Steiner, B. Pfitzmann, and M. Waidner. A formal model for multi-party group key agreement. PhD Thesis RZ 3383, IBM Research, April 2002.
16. M. Steiner, G. Tsudik, and M. Waidner. Diffie-Hellman key distribution extended to group communication. In *Proc. of ACM CCS '96*, pages 31–37. ACM Press, March 1996.