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 [11] whereas the first public-key cryptosystem appeared only two years later to Rivest, Shamir and Adleman [14]. 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 first 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} and g^{x_2} a computationally bounded adversary cannot recover the Diffie-Hellman secret $g^{x_1 x_2}$ [2,3]. Strong security for schemes analyzed in the standard model usually relies on a stronger assumption than the CDH one [3,15], the so-called *Decisional Diffie-Hellman assumption*

(DDH-assumption). It states that given g^{x_1} and g^{x_2} a computationally bounded adversary cannot distinguish the Diffie-Hellman secret $g^{x_1 x_2}$ from a random element g^r in the group. This latter assumption is also useful to prove the security of ElGamal-based encryption schemes [12,10].

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 [17]. 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 [6,7,9]. This assumption has also found application in the context of pseudo-random functions [13]. Schemes for group Diffie-Hellman key exchange analyzed without the random-oracle model achieve strong security guarantees under the *Group Decisional 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 [8].

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 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 by Steiner et al. [17]. They exhibited an asymptotic reduction to show that the DDH-assumption implies the *Generalized* GDDH-assumption. In his PhD thesis [16], 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 *Generalized* GDDH instance is exponentially large. He also pointed out as a research direction to study these reductions when the GDDH instance is not *Generalized*.

In practice, it is fortunately possible to 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 [6,9], we used the special structure of basic trigon (see Figure 1). To prove secure protocols for dynamic group Diffie-Hellman key exchange [7,8], we used the special structure of extended basic trigon (see Figure 2).

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 our group DH key exchange schemes [6,7,8,9] use large groups of known prime order so that the proofs can benefit from the multiplicative random self-reducibility (see below). Therefore in this paper we focus on this latter case only.

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 group decisional Diffie-Hellman assumption (GDDH-assumption). For the remainder of the paper we fix a cyclic group $\mathbb{G} = \langle g \rangle$ of prime order q.

3.1 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:

$$\mathsf{GDH}_{\Gamma_n} = \{\mathcal{D}_{\Gamma_n}(x_1, \ldots, x_n) \,|\, x_1, \ldots, x_n \in_R \mathbb{Z}_q\},$$

where

$$\mathcal{D}_{\Gamma_n}(x_1, \ldots, x_n) = \left\{ \left(J, g^{\prod_{j \in J} x_j}\right) \Big| \, J \in \Gamma_n \right\}.$$

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

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

$j = 1$					$\{\}$
$j = 2$				$\{1\}$	$\{2\}$
$j = 3$			$\{1,2\}$	$\{1,3\}$	$\{2,3\}$
$j = 4$ $(= n-1)$		$\{1,2,3\}$	$\{1,2,4\}$	$\{1,3,4\}$	$\{2,3,4\}$
$j = 5$ $(= n)$	$\{1,2,3,4\}$	$\{1,2,3,5\}$	$\{1,2,4,5\}$	$\{1,3,4,5\}$	$\{2,3,4,5\}$

basic trigon

Fig. 1. Basic GDH-distribution (Example when $n = 5$ and $\Gamma_n = \mathcal{T}_5$)

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

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

				$\{\}$						
			$\{1\}$	$\{2\}$						
		$\{1,2\}$	$\{1,3\}$	$\{2,3\}$						
	$\{1,2,3\}$	$\{1,2,4\}$	$\{1,3,4\}$	$\{2,3,4\}$	$\{1,2,5\}$	$\{1,3,5\}$	$\{1,4,5\}$	$\{2,3,5\}$	$\{2,4,5\}$	$\{3,4,5\}$
$\{1,2,3,4\}$	$\{1,2,3,5\}$	$\{1,2,4,5\}$	$\{1,3,4,5\}$	$\{2,3,4,5\}$						

basic trigon — extension

Fig. 2. Extended GDH-distribution (Example when $n = 5$ and $\Gamma_n = \mathcal{E}_5$)

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

The γ function denotes the cardinality of any structure Γ:

- For $\mathcal{T}_n$, we have $\tau_n = \gamma(\mathcal{T}_n) = \sum_{i=1}^{n} i = n(n+1)/2$ since the i-th "line" of this structure has exactly i elements.
- And the cardinality of $\mathcal{E}_n$ is $\varepsilon_n = \gamma(\mathcal{E}_n) = \gamma(\mathcal{T}_n) + \binom{n-2}{n} - n + 1 = n^2 - n + 1$ 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 later is exponential in n, while the two others are quadratic.

3.2 Good Structure Families

For any indexed structure $\Gamma = \{\Gamma_n\}$, we consider an auxiliary structure $\hat{\Gamma} = \{\hat{\Gamma}_n\}$, where $\hat{\Gamma}_n$ is built from the set $\{0, 3, \ldots, n+1\}$ in the same way Γ_n is built from the set I_n through the map $1 \to 0$, $2 \to 3$, $\ldots$, $n \to n+1$.

Definition 1 (Good Structure Family). A family $\Gamma = \{\Gamma_n\}$ is **good** if for any integer n greater than 3 the following four conditions are satisfied:

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

where for any J, we denote by J_1, J_2 and J_{12} the sets $J \backslash \{1\}$, $J \backslash \{2\}$ and $J \backslash \{1, 2\}$ respectively.

In other words, this means that

$$\Gamma_n \subseteq \left\{ J_0 \cup \{1, 2\} \middle| J \in \hat{\Gamma}_{n-1}, 0 \in J \right\} \bigcup \left\{ J \cup \{2\}, J \cup \{1\}, J \middle| J \in \hat{\Gamma}_{n-1}, 0 \notin J \right\},$$

where for any J, we denote by J_0 the set $J \backslash \{0\}$.

Note 2. The basic trigon $\mathcal{T} = \{\mathcal{T}_n\}$ and extended trigon $\mathcal{E} = \{\mathcal{E}_n\}$ are *good structure families.*

3.3 Group Diffie-Hellman Assumptions

Definition 3 (The Group Computational Diffie-Hellman assumption). A (T, ε)-GCDH_{Γ_n}-attacker in $\mathbb{G}$ is a probabilistic Turing machine Δ running in time T such that

$$\mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_n}}(\Delta) = \Pr_{x_i}\left[\Delta(\mathcal{D}_{\Gamma_n}(x_1, \ldots, x_n)) = g^{x_1 \cdots x_n}\right] \geq \varepsilon.$$

The GCDH_{Γ_n}-problem is (T, ε)-**intractable** if there is no (T, ε)-GCDH_{Γ_n}-attacker in $\mathbb{G}$. The GCDH_{Γ}-assumption states this is the case for all polynomial T and non-negligible ε, for a family $\Gamma = \{\Gamma_n\}$.

Let us define two additional distributions from the GDH-distribution:

$$\begin{aligned} \mathsf{GDH}^{\star}_{\Gamma_n} &= \left\{ \mathcal{D}^{\star}_{\Gamma_n}(x_1, \ldots, x_n) \,|\, x_1, \ldots, x_n \in_R \mathbb{Z}_q \right\}, \\ \mathsf{GDH}^{\$}_{\Gamma_n} &= \left\{ \mathcal{D}^{\$}_{\Gamma_n}(x_1, \ldots, x_n, r) \,|\, x_1, \ldots, x_n, r \in_R \mathbb{Z}_q \right\}, \end{aligned}$$

where

$$\begin{aligned} \mathcal{D}^{\star}_{\Gamma_n}(x_1, \ldots, x_n) &= \mathcal{D}_{\Gamma_n}(x_1, \ldots, x_n) \cup \{(I_n, g^{x_1 \cdots x_n})\} \\ \mathcal{D}^{\$}_{\Gamma_n}(x_1, \ldots, x_n, r) &= \mathcal{D}_{\Gamma_n}(x_1, \ldots, x_n) \cup \{(I_n, g^{r})\} \end{aligned}$$

A GDDH_{Γ_n}-distinguisher in $\mathbb{G}$ is a probabilistic Turing machine trying to distinguish $\mathsf{GDH}^{\star}_{\Gamma_n}$ from $\mathsf{GDH}^{\$}_{\Gamma_n}$.

Definition 4 (The Group Decisional Diffie-Hellman assumption). A (T, ε)-GDDH_{Γ_n}-distinguisher in $\mathbb{G}$ is a probabilistic Turing machine Δ running in time T such that its advantage $\mathsf{Adv}_{\mathbb{G}}^{\mathsf{gddh}_{\Gamma_n}}(\Delta)$ defined by

$$\left| \Pr_{x_i}\left[\Delta(\mathcal{D}^{\star}_{\Gamma_n}(x_1, \ldots, x_n)) = 1\right] - \Pr_{x_i, r}\left[\Delta(\mathcal{D}^{\$}_{\Gamma_n}(x_1, \ldots, x_n, r)) = 1\right]\right|$$

is greater than ε.
The GDDH_{Γ_n}-problem is (T, ε)**-intractable** if there is no (T, ε)-GDDH_{Γ_n}-distinguisher in $\mathbb{G}$. The GDDH_{Γ}-assumption states this is the case for all polynomial T and non-negligible ε, for a family $\Gamma = \{\Gamma_n\}$.

3.4 The Random Self-Reducibility

The Diffie-Hellman problems have the nice property of random self-reducibility. Certainly the most common is the additive random self-reducibility, which works as follows. Given, for example, a GCDH-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 for the *Generalized* DH-distribution only and thus 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 GDH-problems in a prime order cyclic group. Given, for example, a GCDH-instance $\mathcal{D} = (g^a, g^b, g^{ab}, g^{ac})$ for any a, b, c it is easy to generate a random instance $\mathcal{D}' = (g^{a\alpha}, g^{b\beta}, g^{ab\alpha\beta}, g^{ac\alpha\gamma})$ where α, β and γ are random numbers in $\mathbb{Z}_q^*$. And given the solution K' to the instance $\mathcal{D}'$, we directly get the solution $K = {K'}^{\delta}$, where $\delta = (\alpha\beta\gamma)^{-1} \bmod q$, to the 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 (GDDH) problem, but for the good structure families only.

4.1 The Main Result

Theorem 5. *Let $\mathbb{G}$ be a cyclic multiplicative group of prime order q and $t_{\mathbb{G}}$ the time needed for an exponentiation in $\mathbb{G}$. For any integer n and any good structure* *family $\Gamma = \{\Gamma_n\}$ of cardinality $\gamma = \{\gamma_n\}$, we have:*

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

The proof of this theorem results, by induction, from the following two lemmas 6 and 7 which lead to

$$\mathsf{Adv}_{\mathbb{G}}^{\mathsf{gddh}_{\Gamma_n}}(t) \leq \mathsf{Adv}_{\mathbb{G}}^{\mathsf{gddh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}}) + 2\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}).$$

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 t' is less than $t + n^3 t_{\mathbb{G}}/3$;
- for the structure of extended trigon $\mathcal{E}_n$, the time t' is less than $t + 2n^3 t_{\mathbb{G}}/3$.

For proving this result, we need to alter Group Diffie-Hellman tuples, introducing some randomness. This leads to the *group random distributions* (the *group random adversaries* resp.) where some elements are independently random in the *group Diffie-Hellman distributions* (the *group Diffie-Hellman problems* resp.).

4.2 Group Random Distributions

Let us split in two parts instances $\mathcal{D}_{\Gamma_n}(x_1, \ldots, x_n)$:

$$\begin{aligned}
&= \left\{ \left(J, g^{\prod_{j \in J} x_j}\right) \middle| \, J \in \Gamma_n, \{1,2\} \not\subseteq J \right\} \cup \left\{ \left(J, g^{\prod_{j \in J} x_j}\right) \middle| \, J \in \Gamma_n, \{1,2\} \subseteq J \right\} \\
&= \left\{ \left(J, g^{\prod_{j \in J} x_j}\right) \middle| \, \{1,2\} \not\subseteq J \right\} \cup \left\{ \left(J, g^{x_1 x_2 \prod_{j \in J_{12}} x_j}\right) \middle| \, \{1,2\} \subseteq J \right\}.
\end{aligned}$$

We can now define an additional distribution:

$$\mathsf{GR}_{\Gamma_n} = \{\mathcal{V}_{\Gamma_n}(x_1, \ldots, x_n, \alpha) \,|\, x_1, \ldots, x_n, \alpha \in_R \mathbb{Z}_q\},$$

where

$$\begin{aligned}
\mathcal{V}_{\Gamma_n}(x_1, \ldots, x_n, \alpha) = &\left\{ \left(J, g^{\prod_{j \in J} x_j}\right) \middle| \, J \in \Gamma_n, \{1,2\} \not\subseteq J \right\} \\
&\bigcup \left\{ \left(J, g^{\alpha \prod_{j \in J_{12}} x_j}\right) \middle| \, J \in \Gamma_n, \{1,2\} \subseteq J \right\}.
\end{aligned}$$

Similarly to above, we define $\mathcal{V}^{\star}_{\Gamma_n}(x_1, \ldots, x_n, \alpha)$ and $\mathcal{V}^{\$}_{\Gamma_n}(x_1, \ldots, x_n, \alpha, r)$, the extensions of $\mathcal{V}_{\Gamma_n}(x_1, \ldots, x_n, \alpha)$ where one appends $\{(I_n, g^{\alpha x_3 \cdots x_n})\}$ and $\{(I_n, g^r)\}$ respectively. Then,

$$\begin{aligned}
\mathsf{GR}^{\star}_{\Gamma_n} &= \left\{\mathcal{V}^{\star}_{\Gamma_n}(x_1, \ldots, x_n, \alpha) \,|\, x_1, \ldots, x_n, \alpha \in_R \mathbb{Z}_q\right\}, \\
\mathsf{GR}^{\$}_{\Gamma_n} &= \left\{\mathcal{V}^{\$}_{\Gamma_n}(x_1, \ldots, x_n, \alpha, r) \,|\, x_1, \ldots, x_n, \alpha, r \in_R \mathbb{Z}_q\right\}.
\end{aligned}$$

We note that under the constraint $\alpha = x_1x_2$, for any $x_1, \dots, x_n, r \in_R \mathbb{Z}_q$, one has,

$$\mathcal{V}_{\Gamma_n}(x_1, \dots, x_n, \alpha) = \mathcal{D}_{\Gamma_n}(x_1, \dots, x_n)$$
$$\mathcal{V}^\star_{\Gamma_n}(x_1, \dots, x_n, \alpha) = \mathcal{D}^\star_{\Gamma_n}(x_1, \dots, x_n)$$
$$\mathcal{V}^\$_{\Gamma_n}(x_1, \dots, x_n, \alpha, r) = \mathcal{D}^\$_{\Gamma_n}(x_1, \dots, x_n, r)$$

and thus,

$$\mathsf{GR}_{\Gamma_n} \equiv \mathsf{GDH}_{\Gamma_n} \quad \mathsf{GR}^\star_{\Gamma_n} \equiv \mathsf{GDH}^\star_{\Gamma_n} \quad \mathsf{GR}^\$_{\Gamma_n} \equiv \mathsf{GDH}^\$_{\Gamma_n}.$$

4.3 Group Random Adversaries

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

$$\mathsf{Succ}^{\mathsf{gcr}_{\Gamma_n}}_{\mathbb{G}}(\Delta) = \Pr_{x_i, \alpha}\left[\Delta(\mathcal{V}_{\Gamma_n}(x_1, \dots, x_n, \alpha)) = g^{\alpha x_3 \cdots x_n}\right] \geq \varepsilon.$$

A (T, ε)-GDR_{Γ_n}-distinguisher in $\mathbb{G}$ is a probabilistic Turing machine Δ running in time T such that its advantage $\mathsf{Adv}^{\mathsf{gdr}_{\Gamma_n}}_{\mathbb{G}}(\Delta)$ defined by

$$\left| \Pr_{x_i, \alpha}\left[\Delta\big(\mathcal{V}^\star_{\Gamma_n}(x_1, \dots, x_n, \alpha)\big) = 1\right] - \Pr_{x_i, \alpha, r}\left[\Delta\big(\mathcal{V}^\$_{\Gamma_n}(x_1, \dots, x_n, \alpha, r)\big) = 1\right] \right|$$

is greater than ε.

4.4 Proof

Lemma 6. *For any integer n and any structure Γ_n, we have*

$$\mathsf{Adv}^{\mathsf{gddh}_{\Gamma_n}}_{\mathbb{G}}(t) \leq \mathsf{Adv}^{\mathsf{gdr}_{\Gamma_n}}_{\mathbb{G}}(t) + 2\mathsf{Adv}^{\mathsf{ddh}}_{\mathbb{G}}(t + \gamma_n t_{\mathbb{G}}).$$

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 maximal time t, in particular it always terminates, even if the input comes from neither $\mathsf{GDH}^\star_{\Gamma_n}$ nor from $\mathsf{GDH}^\$_{\Gamma_n}$. 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 $b = b'$.

Game $\mathbf{G_0}$. In this game, we are given a Diffie-Hellman triple $(A, B, C) = (g^{x_1}, g^{x_2}, g^{x_1x_2})$. Then we choose at random $(x_3, \dots, x_n)$ in $\mathbb{Z}^*_q$ and compute a tuple U_n which follows the distribution GDH_{Γ_n}, as follows

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

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: the computed tuple follows exactly the distribution $\mathsf{GDH}^{\star}_{\Gamma_n}$ (resp. $\mathsf{GDH}^{\$}_{\Gamma_n}$) if $b = 1$ (resp. $b = 0$). Thus by definition, if we feed the attacker $\mathcal{A}$ with this tuple, we have

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

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 attacker $\mathcal{A}$ follows the distribution $\mathsf{GR}^{\star}_{\Gamma_n}$ (resp. $\mathsf{GR}^{\$}_{\Gamma_n}$) if $b = 1$ (resp. $b = 0$). Then,

$$\Pr[S_1] = \frac{\mathsf{Adv}^{\mathsf{gdr}_{\Gamma_n}}_{\mathbb{G}}(\mathcal{A}) + 1}{2} \leq \frac{\mathsf{Adv}^{\mathsf{gdr}_{\Gamma_n}}_{\mathbb{G}}(t) + 1}{2}.$$

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

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

The lemma follows. □

Lemma 7. *For any good structure family $\Gamma = \{\Gamma_n\}$ and any integer n, we have*

$$\mathsf{Adv}^{\mathsf{gdr}_{\Gamma_n}}_{\mathbb{G}}(t) \leq \mathsf{Adv}^{\mathsf{gddh}_{\Gamma_{n-1}}}_{\mathbb{G}}(t + \gamma_n t_{\mathbb{G}}).$$

Proof. We consider a GDR_{Γ_n}-distinguisher $\mathcal{A}$ running in time t and we use it to built a $\mathsf{GDDH}_{\Gamma_{n-1}}$-distinguisher. To reach that goal, we receive as input a tuple drawn from either $\mathsf{GDH}^{\star}_{\Gamma_{n-1}}$ or $\mathsf{GDH}^{\$}_{\Gamma_{n-1}}$. We 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 of this input tuple:

$$\begin{aligned} \mathsf{U}_{n-1} &= \left\{ \left(J, g^{\prod_{j \in J} x_j} \right) \middle| \, J \in \Gamma_{n-1} \right\} = \mathcal{D}_{\Gamma_{n-1}}(x_1, \ldots, x_{n-1}) \in \mathsf{GDH}_{\Gamma_{n-1}} \\ u_{n-1} &= g^{x_1 \cdots x_{n-1}} \text{ if } b = 1, \text{ or } g^r \text{ if } b = 0. \end{aligned}$$

We split the tuple U_{n-1} in two blocks, depending whether $1 \in J$:

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

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 then follows that the elements of U_{n-1} are indexed by the elements of $\hat{\Gamma}_{n-1}$ rather than Γ_{n-1}:

$$\left\{ \left(J, g^{X_0 \prod_{j \in J_0} X_j} \right) \middle| J \in \hat{\Gamma}_{n-1}, 0 \in J \right\} \cup \left\{ \left(J, g^{\prod_{j \in J} X_j} \right) \middle| J \in \hat{\Gamma}_{n-1}, 0 \notin J \right\}.$$

Now we pick at random two values X_1, X_2 in $\mathbb{Z}_q^*$ and use them to construct the following tuple, in which the last block in the above equation is split in the last three blocks of W_{n-1}:

$$\begin{aligned}\mathsf{W}_{n-1} = &\left\{ \left(J, g^{X_0 \prod_{j\in J_0} X_j}\right) \middle| J \in \hat{\Gamma}_{n-1}, 0 \in J \right\}\\ &\bigcup \left\{ \left(J, g^{X_2 \prod_{j\in J} X_j}\right) \middle| J \in \hat{\Gamma}_{n-1}, 0 \notin J \right\}\\ &\bigcup \left\{ \left(J, g^{X_1 \prod_{j\in J} X_j}\right) \middle| J \in \hat{\Gamma}_{n-1}, 0 \notin J \right\}\\ &\bigcup \left\{ \left(J, g^{\prod_{j\in J} X_j}\right) \middle| J \in \hat{\Gamma}_{n-1}, 0 \notin J \right\}.\end{aligned}$$

Remember that Γ is a "good" structure family:

$$\Gamma_n \subseteq \left\{ J_0 \cup \{1,2\} \middle| J \in \hat{\Gamma}_{n-1}, 0 \in J \right\} \bigcup \left\{ J \cup \{2\}, J \cup \{1\}, J \middle| J \in \hat{\Gamma}_{n-1}, 0 \notin J \right\}.$$

Then one can build the following tuple V_n which is also included in W_{n-1}:

$$\begin{aligned}\mathsf{V}_n = &\left\{ \left(J, g^{X_0 \prod_{j\in J_{12}} X_j}\right) \middle| J \in \Gamma_n, \{1,2\} \subseteq J \right\}\\ &\bigcup \left\{ \left(J, g^{\prod_{j\in J} X_j}\right) \middle| J \in \Gamma_n, \{1,2\} \nsubseteq J \right\}.\end{aligned}$$

We note that

$$\mathsf{V}_n = \mathcal{V}_{\Gamma_n}(X_1, \ldots, X_n, X_0) \in \mathsf{GR}_{\Gamma_n}.$$

Then V_n is appended (I_n, u_{n-1}) and given to $\mathcal{A}$. The latter returns a bit b' that we relay back as an answer to the original $\mathsf{GDDH}_{\Gamma_{n-1}}$ 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

$$\mathsf{Adv}_{\mathbb{G}}^{\mathsf{gddh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}}) \geq \mathsf{Adv}_{\mathbb{G}}^{\mathsf{gdr}_{\Gamma_n}}(t).$$

□

Putting all together, we obtain:

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

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 8. *Let $\mathbb{G}$ be a cyclic multiplicative group of prime order q and $t_{\mathbb{G}}$ the time needed for an exponentiation in $\mathbb{G}$. Then for any integer n and any good structure family $\Gamma = \{\Gamma_n\}$ of cardinality $\gamma = \{\gamma_n\}$ we have:*

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

As for the previous theorem, the result comes, by induction, from both

$$\begin{aligned} \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_n}}(t) &\leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcr}_{\Gamma_n}}(t) \\ \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcr}_{\Gamma_n}}(t) &\leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}}) + \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}). \end{aligned}$$

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

We then define a sequence of games $\mathbf{G}_0$, $\mathbf{G}_1$, ... In each game, given a triple (A, B, C) and $n-2$ random elements $(x_3, \ldots, x_n)$ in $\mathbb{Z}_q^*$ (which are not necessarily known), we consider S_i as 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 by randomly choosing $(x_3, \ldots, x_n)$ we can compute:

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

It is easy to see that $\mathsf{U}_n = \mathcal{D}_{\Gamma_n}(x_1, \ldots, x_n)$, and thus follows exactly the distribution GDH_{Γ_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

$$\Pr[S_0] = \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_n}}(\mathcal{A}).$$

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 element in $\mathbb{Z}_q^*$. We then perform the same operations as in game $\mathbf{G}_0$ to obtain a tuple which follows the distribution GR_{Γ_n}: $\mathsf{U}_n = \mathcal{V}_{\Gamma_n}(x_1, \ldots, x_n, \alpha)$. This tuple is provided to the adversary, which computes $g^{\alpha x_3 \cdots x_n}$. By definition, we have:

$$\Pr[S_1] = \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcr}_{\Gamma_n}}(\mathcal{A}) \leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcr}_{\Gamma_n}}(t).$$

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 $\mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}})$, then:

$$\mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_n}}(\mathcal{A}) \leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcr}_{\Gamma_n}}(t) + \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}).$$

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 $\mathsf{GCDH}_{\Gamma_{n-1}}$ 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, granted the property of good structure family, 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 GR_{Γ_n}.

The variables are distributed exactly as in the previous game, so we have $\Pr[S_3] = \Pr[S_2]$. Note that since we do not know $x_3, \ldots, x_n$, we are no longer able to decide whether the value the adversary outputs is $C^{x_3 \cdots x_n}$. But it is not a problem since the two games are *perfectly* identical.

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

$$\Pr[S_3] \leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}}).$$

Putting all these together gives us

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

Since it is true for any adversary running within time t,

$$\mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_n}}(t) \leq \mathsf{Succ}_{\mathbb{G}}^{\mathsf{gcdh}_{\Gamma_{n-1}}}(t + \gamma_n t_{\mathbb{G}}) + \mathsf{Adv}_{\mathbb{G}}^{\mathsf{ddh}}(t + \gamma_n t_{\mathbb{G}}).$$

By induction, it follows:

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

□

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 [6,7,8,9] 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 these 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 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, 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.
7. 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. Full Version available at `http://www.di.ens.fr/users/pointche`.
8. 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. Full Version available at `http://www.di.ens.fr/users/pointche`.
9. E. Bresson, O. Chevassut, and D. Pointcheval. Group diffie-hellman key exchange secure against dictionary attacks. In Y. Zheng, editor, *Proc. of Asiacrypt '2002*. Springer, December 2002. Full Version available at `http://www.di.ens.fr/users/pointche`.
10. 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.
11. W. Diffie and M. E. Hellman. New directions in cryptography. *Transactions on Information Theory*, IT-22(6):644–654, November 1976.
12. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proc. of Crypto '84*, LNCS 196, pp. 10–18.
13. 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.
14. 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.
15. V. Shoup. On formal models for secure key exchange. Technical Report RZ 3120, IBM Zürich Research Lab, November 1999.
16. M. Steiner. Secure Group Key Agreement. PhD Thesis, Naturwissenschaftlich-Technische Fakultät der Universität des Saarlandes, Saarbrücken, March 2002.
17. 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.