CHICAGO JOURNAL OF THEORETICAL COMPUTER SCIENCE 2023, Article 01, pages 1–14
http://cjtcs.cs.uchicago.edu/

Discrete logarithm and Diffie-Hellman problems in identity black-box groups

Gábor Ivanyos* Antoine Joux† Miklos Santha‡

Received May 19, 2021; Revised January 5, 2023; Published June 15, 2023

Abstract: We investigate the computational complexity of the discrete logarithm, the computational Diffie-Hellman and the decisional Diffie-Hellman problems in some identity black-box groups $G_{p,t}$, where p is a prime number and t is a positive integer. These are defined as quotient groups of vector space $\mathbb{Z}_p^{t+1}$ by a hyperplane H given through an identity oracle. While in general black-box groups that have unique encoding of their elements these computational problems are classically all hard and quantumly all easy, we find that in the groups $G_{p,t}$ the situation is more contrasted. We prove that while there is a polynomial time probabilistic algorithm to solve the decisional Diffie-Hellman problem in $G_{p,1}$, the probabilistic query complexity of all the other problems is $\Omega(p)$, and their quantum query complexity is $\Omega(\sqrt{p})$. Our results therefore provide a new example of a group where the computational and the decisional Diffie-Hellman problems have widely different complexity.

1 Introduction

Black-box groups were introduced by Babai and Szemerédi [5] for studying the structure of finite matrix groups. In a black-box group, the group elements are encoded by binary strings of certain length, the

*Supported by the National Research Foundation, Singapore and A*STAR under its CQT Bridging Grant, and by the NRDI Office of Hungary within the framework of the Artificial Intelligence National Laboratory Program.

†Supported by the European Union as H2020 Programme under grant agreement number ERC-669891. The work was perfomed while the author was visiting CQT with support by the National Research Foundation, Singapore and A*STAR under its CQT Bridging Grant.

‡Supported by the National Research Foundation, Singapore and A*STAR under its CQT Bridging Grant and its Quantum Engineering Programme NRF2021-QEP2-02-P05.

Key words and phrases: Discrete logarithm, Diffie-Hellman problems, black-box groups, classical and quantum complexity

DOI: 10.4086/cjtcs.2023.001

group operations and their inverses are given by oracles. Similarly, identity testing, that is checking whether an element is equal to the identity element, is also done with a special identity oracle. These oracles are also called black-boxes, giving their names to the groups. Identity testing is required when several strings may encode the same group element. In this case we speak about non-unique encoding, in opposition to unique encoding when every group element is encoded by a unique string. Black-box groups with non-unique encoding are motivated by their ability to capture factor groups of subgroups of matrix groups by certain normal subgroups which admit efficient algorithms for membership testing. An important example for such a subgroup is the solvable radical, that is the largest solvable normal subgroup.

A black-box group problem that concerns some global properties of the group may have no inputs other than the oracles. In some other cases it might also have standard inputs (or inputs, for short), a finite set of group elements represented by their encodings. A black-box group algorithm is allowed to call the oracles for the group operations and for the identity test and it might also perform arbitrary bit operations. The query complexity of an algorithm is the number of oracle calls, while the running time or computational complexity is the number of oracle calls together with the number of other bit operations, when we are maximizing over both oracle and standard inputs. In the quantum setting, the oracles are given by unitary operators.

Many classical algorithms have been developed for computations with black-box groups [6, 4, 15], for example the identification of the composition factors, even the non-commutative ones. When the oracle operations can be simulated by efficient procedures, efficient black-box algorithms automatically produce efficient algorithms. Permutation groups, finite matrix groups over finite fields and over algebraic number fields fit in this context. There has been also considerable effort to design quantum algorithms in black-box groups. In the case of unique encoding efficient algorithms have been conceived for the decomposition of Abelian groups into a direct sum of cyclic groups of prime power order [9], for order computing and membership testing in solvable groups [24], and for solving the hidden subgroup problem in Abelian groups [18].

The discrete logarithm problem DLOG, and various Diffie-Hellman type problems are fundamental tasks in computational number theory. They are equally important in cryptography, since the security of many cryptographic systems is based on their computational difficulty. Let G be a cyclic group (denoted multiplicatively). Given two group elements g and h, where g is a generator, DLOG asks to compute an integer d such that $h = g^d$. Given three group elements g, g^a and g^b, where g is a generator, the computational Diffie-Hellman problem CDH is to compute g^{ab}. Given four group elements g, g^a, g^b and g^c, where g is a generator, the decisional Diffie-Hellman problem DDH is to decide whether $c = ab$ modulo the order of g.

The problems are enumerated in decreasing order of difficulty: DDH can not be harder than CDH and CDH is not harder than DLOG. While there are groups where even DLOG is easy (for example $\mathbb{Z}_m$, the additive group of integers modulo m), in general all three problems are thought to be computationally hard. We are not aware of any group where CDH is easy while DLOG is hard. In fact, Maurer and Wolf have proven in [17] that under a seemingly reasonable number-theoretic assumption, the two problems are equivalent in the case of unique-encoding groups. Based on this, Joux and Nguyen [14] have constructed a cryptographic group where DDH is easy to compute while CDH is as hard as DLOG. In generic black-box groups we have provable query lower bounds for these problems, even in the case of unique encoding. Shoup has proven [23] that in $\mathbb{Z}_p$, given as a black-box group with unique encoding, to solve DLOG and CDH require $\Omega(p^{1/2})$ group operations. Subsequently, Damgård, Hazay and Zottare [10] have established a lower bound of the same order for DDH. We remark that the Pohlig-Hellman [19] algorithm reduces DLOG in arbitrary cyclic groups to DLOG in its prime order subgroups. Furthermore, in prime order groups (with unique encodings), Shanks's baby-step giant-step algorithm solves the problem using $O(p^{1/2})$ group operations, thus matching the lower bound for black-box groups.

Though, as we said, all three problems are considered computationally intractable on a classical computer, there is a polynomial time quantum algorithm for DLOG due to Shor [22]. Since DLOG is an instance of the Abelian hidden subgroup problem, Mosca's result [18] implies that by a quantum computer it can also be solved efficiently in black-box groups with unique encoding.

We are concerned here with identity black-box groups, a special class of black-box groups where only the identity test is given by an oracle. These groups are quotient groups of some explicitly given ambient group. An identity black box group G is specified by an ambient group G' and an identity oracle Id which tests membership in some (unknown) normal subgroup H of G'. In G the group operations are explicitly defined by the group operations in G', and therefore it is the quotient group G'/H.

Let p be a prime number. More specifically we will study the problems DLOG, CDH and DDH in identity black-box groups whose ambient group is $\mathbb{Z}_p^{t+1}$, for some positive integer t, and where the normal subgroup H, specified by the identity oracle, is isomorphic to $\mathbb{Z}_p^t$. We denote such an identity black box group by $G_{p,t}$. We fully characterize the complexity of the three problems in these groups. Our results are mainly query lower bounds: the probabilistic query complexity of all these problems, except DDH in level 1 groups, is $\Omega(p)$, and their quantum query complexity is $\Omega(\sqrt{p})$. These lower bounds are obviously tight since $\mathrm{DLOG}(G_{p,t})$ can be solved, for all $t \geq 1$, by exhaustive search and by Grover's algorithm in respective query complexity p and $O(\sqrt{p})$. We have also one, maybe surprising, algorithmic result: the computational complexity of $\mathrm{DDH}(G_{p,1})$ is polynomial. Our results can be summarized in the following theorems.

Theorem (Lower bounds)

1. For all $t \geq 1$, the randomized query complexity of $\mathrm{DLOG}(G_{p,t})$ and $\mathrm{CDH}(G_{p,1})$ is $\Omega(p)$.
2. For all $t \geq 1$, the quantum query complexity of $\mathrm{DLOG}(G_{p,t})$ and $\mathrm{CDH}(G_{p,1})$ is $\Omega(\sqrt{p})$.
3. For all $t \geq 2$, the randomized query complexity of $\mathrm{DDH}(G_{p,t})$ is $\Omega(p)$.
4. For all $t \geq 2$, the quantum query complexity of $\mathrm{DDH}(G_{p,t})$ is $\Omega(\sqrt{p})$.

Theorem (Upper bound) $\mathrm{DDH}(G_{p,1})$ can be solved in probabilistic polynomial time in $\log p$.

2 Preliminaries

Formally, a *black-box group* G is a 4-tuple $G = (C, \mathrm{Mult}, \mathrm{Inv}, \mathrm{Id})$ where C is the set of admissible codewords, $\mathrm{Mult} : C \times C \mapsto C$ is a binary operation, $\mathrm{Inv} : C \to C$ is a unary operation and $\mathrm{Id} : C \to \{0, 1\}$ is a unary Boolean function. The operations Mult, Inv and the function Id are given by *oracles*. We require that there exists a finite group $\widetilde{G}$ and a surjective map $\phi : C \to \widetilde{G}$ for which, for every $x, y \in C$, we have $\phi(\mathrm{Mult}(x,y)) = \phi(x)\phi(y)$, $\phi(\mathrm{Inv}(x)) = \phi(x)^{-1}$, and $\phi(x) = 1_{\widetilde{G}}$ if and only if $\mathrm{Id}(x) = 1$. We say that x is (more accurately, encodes) the identity element in G or that $x = 1$ if $\mathrm{Id}(x) = 1$. With the identity oracle we can test equality since $x = y$ in G exactly when $\mathrm{Id}(\mathrm{Mult}(x,\mathrm{Inv}(y))) = 1$. We say that a black-box group has *unique encoding* if ϕ is a bijection. For abelian groups we also use the additive notation in which case the binary operation of G is denoted by Add and its identity element is denoted by 0.

We are concerned here with a special class of black-box groups which are quotient groups of some explicitly given group. An *identity black-box group* is a couple $G = (G',\mathrm{Id})$ where G' is group and the *identity oracle* $\mathrm{Id} : G' \to \{0,1\}$ is the characteristic function of some (unknown) normal subgroup H of G'. We call G' the *ambient group* of G. In G the group operations Mult and Inv are defined by the group operations in the ambient group G' modulo H. As a consequence, G is the quotient group G'/H.

Let p be a prime number and let $t \geq 1$ be a positive integer. We denote by $\mathbb{Z}_p$ the additive group of integers modulo p, by $\mathbb{F}_p$ the finite field of size p, and by $\mathbb{Z}_p^t$ the t-dimensional vector space over $\mathbb{F}_p$. For $h,k \in \mathbb{Z}_p^t$, we denote their scalar product modulo p by $h \cdot k$.

We will work with identity black-box groups whose ambient group is $\mathbb{Z}_p^{t+1}$, and the subgroup H is isomorphic to $\mathbb{Z}_p^t$, that is a hyperplane of $\mathbb{Z}_p^{t+1}$. Regarding the problems we are concerned with, the only real restriction of this model is that our black-box group G has (known) prime order p. Indeed, let $G = (C,\mathrm{Mult},\mathrm{Inv},\mathrm{Id})$ be a cyclic black box group of order p. Let $g_1 = g$, $g_2 = g^a$, $g_3 = g^b$ and $g_4 = g^c$ be the input quadruple for DDH. We define maps $\psi_i : \{0,\ldots,p-1\} \to C$ as $\psi(x) = g_i^x$. Here g_i^x is computed by a fixed method based on repeated squaring and the binary expansion of x using $\mathrm{poly}(\log p)$ iterated applications of the oracle Mult. We also define an oracle Id' on $\{0,\ldots,p-1\}^4$ by $\mathrm{Id}'(x_1,x_2,x_3,x_4) = \mathrm{Id}(\phi_1(x_1),\phi_2(x_2),\phi_3(x_3),\phi_4(x_4))$. It is not difficult to see that this makes G an identity black box group with ambient group $\mathbb{Z}_p^4$ where the identity oracle Id' can be implemented using a $\mathrm{poly}(\log p)$ calls to Mult and a single call to Id. This recipe reduces the given instance of DDH to an instance of DDH in the new setting in an obvious way. Similarly, DLOG and CDH can be reduced to instances with ambient groups Z_p^2 and $\mathbb{Z}_p^3$, respectively.

We will specify the identity oracle by a non-zero normal vector $n \in \mathbb{Z}_p^{t+1}$ of H. By permuting coordinates and multiplying by some non-zero constant, we can suppose without loss of generality that it is of the form $n = (1,n_1,\ldots,n_t)$. We call such a vector *t-suitable*. We define the function $\mathrm{Id}_n : \mathbb{Z}_p^{t+1} \to \{0,1\}$ by $\mathrm{Id}_n(h) = 1$ if $h \cdot n = 0$. Clearly Id_n is the characteristic function of the hyperplane $H_n = \{h \in \mathbb{Z}_p^{t+1} : h \cdot n = 0\}$. We define the identity black-box group $G_{p,t} = (\mathbb{Z}_p^{t+1},\mathrm{Id})$, where the identity oracle Id satisfies $\mathrm{Id} = \mathrm{Id}_n$, for some (unknown) t-suitable vector n. We call t the *level* of the group $G_{p,t}$. We emphasize again that the group operations of $G_{p,t}$ are performed as group operations in $\mathbb{Z}_p^{t+1}$. Therefore, for $h,k \in \mathbb{Z}_p^{t+1}$, the equality $h = k$ in $G_{p,t}$ means equality in $\mathbb{Z}_p^{t+1}$ modulo H_n, where H_n is identified by Id_n. To be short, we will refer to $G_{p,t}$ as the *hidden cyclic group* of level t. We remark that any lower bound for t-suitable n remain trivially valid for general normal vector n. Also, the first nonzero coordinate of n can be found using at most t queries (namely $\mathrm{Id}(1,0,0,\ldots,0)$, $\mathrm{Id}(0,1,0,\ldots,0)$, $\ldots$, $\mathrm{Id}(0,\ldots,0,1,0)$). Furthermore, scaling this coordinate to 1 does not affect the oracle Id_n. Therefore t-suitability of n affects any upper bound by at most t queries.

Proposition 2.1. *The groups $G_{p,t}$ and $\mathbb{Z}_p$ are isomorphic and the map $\phi : G_{p,t} \to \mathbb{Z}_p$ defined by $\phi(h) = h \cdot n \in \mathbb{Z}_p$ is a group isomorphism.*

Proof. The maps from $\mathbb{Z}_p^{t+1}$ to $G_{p,t}$ (respectively to $\mathbb{Z}_p$) mapping $h \in \mathbb{Z}_p^{t+1}$ to its class in the quotient $G_{p,t}$ (respectively to $h \cdot n$) are group homomorphisms with the same kernel H_n. □

We recall now the basic notions of query complexity for the specific case of Boolean functional oracle problems. Let m be a positive integer. A *functional oracle problem* is a function $A : S \to \{0,1\}^M$, where $S \subseteq \{0,1\}^m$ and $M \geq 1$ is a positive integer. If $M = 1$, then we call the functional oracle problem *Boolean*. The input $f \in S$ is given by an oracle, that is $f(x)$ can be accessed by the query x. The output on f is $A(f)$. Each query adds one to the complexity of an algorithm, but all other computations are free. The state of the computation is represented by three registers, the query register $1 \leq x \leq m$, the answer register $a \in \{0,1\}$, and the work register z. The computation takes place in the vector space spanned by all basis states $|x\rangle|a\rangle|z\rangle$. In the *quantum query* model introduced by Beals et al. [7] the state of the computation is a complex combination of all basis states which has unit length in the norm l_2. In the *randomized query* model it is a non-negative real combination of unit length in the norm l_1, and in the deterministic model it is always one of the basis states.

The query operation O_f maps the basis state $|x\rangle|a\rangle|z\rangle$ into the state $|x\rangle|(a + f(x)) \bmod 2\rangle|z\rangle$. Non-query operations do not depend on f. A *k-query algorithm* is a sequence of $(k+1)$ operations $(U_0, U_1, \ldots, U_k)$ where U_i is unitary in the quantum, and stochastic in the randomized model. Initially the state of the computation is set to some fixed value $|0\rangle|0\rangle|0\rangle$, and then the sequence of operations $U_0, O_f, U_1, O_f, \ldots, U_{k-1}, O_f, U_k$ is applied. A quantum or randomized algorithm *computes* A on input f if the observation of the last M bits of the work register yields $A(f)$ with probability at least $2/3$. Then $\mathrm{Q}(A)$ (respectively $\mathrm{R}(A)$) is the smallest k for which there exists a k-query quantum (respectively randomized) algorithm which computes A on every input f. We have $\mathrm{R}(A) \leq \mathrm{Q}(A) \leq m$.

We define now the problems we are concerned with, the *discrete logarithm* problem DLOG, the *computational Diffie-Hellman* problem CDH and the *decisional Diffie-Hellman* problem DDH in hidden cyclic groups $G_{p,t}$. As in the rest of the paper the additive notation will to be more convenient, in contrast to the informal definitions if the introduction, we use here the additive terminology. We say that a quadruple $(g,h,k,\ell) \in G_{p,t}^4$ is a DH-*quadruple* if g is a generator of $G_{p,t}$, $h = ag, k = bg$ and $\ell = cg$ for some integers a,b,c such that $c = ab$ modulo p.

DLOG$(G_{p,t})$
Oracle input: Id_n for some t-suitable vector n.
Input: A couple $(g,h) \in G_{p,t}^2$ such that g is a generator of $G_{p,t}$.
Output: A non-negative integer d such that $dg = h$.

CDH$(G_{p,t})$
Oracle input: Id_n for some t-suitable vector n.
Input: A triple $(g,h,k) \in G_{p,t}^3$ such that g is a generator of $G_{p,t}$.
Output: $\ell \in G_{p,t}$ such that (g,h,k,ℓ) is a DH-quadruple.

$\mathrm{DDH}(G_{p,t})$
Oracle input: Id_n for some t-suitable vector n.
Input: A quadruple $(g,h,k,\ell) \in G_{p,t}^4$ such that g is a generator of $G_{p,t}$.
Question: Is (g,h,k,ℓ) a DH-quadruple?

An algorithm for these problems has access to the input and oracle access to the oracle input, and every query is counted as one computational step. We say that it solves the problem *efficiently* if it works in time polynomial in $\log p$ and t. For any fixed input, the problems become functional oracle problems, where we consider only those identity oracles for which the input is legitimate. By their *query complexity* we mean, both in the quantum and in the randomized model, the maximum, over all inputs, of the respective query complexity of these functional oracle problems.

The problems are enumerated in decreasing order of difficulty. The existence of an efficient algorithm for $\mathrm{DLOG}(G_{p,t})$ implies the existence of an efficient algorithm for $\mathrm{CDH}(G_{p,t})$, which in turn gives rise to an efficient algorithm for $\mathrm{DDH}(G_{p,t})$. For query complexity we have $\mathrm{Q}(\mathrm{DDH}(G_{p,t})) \leq \mathrm{Q}(\mathrm{CDH}(G_{p,t}))+1$ and $\mathrm{Q}(\mathrm{CDH}(G_{p,t})) \leq 2\mathrm{Q}(\mathrm{DLOG}(G_{p,t}))$, and the same inequalities hold for the randomized model. The problems are getting harder as the level of the hidden cyclic group increases, as the almost trivial reductions in the next Proposition show. To ease notation, for $h=(h_0,\ldots,h_t)$ in $\mathbb{Z}_p^{t+1}$, we denote by h' the element $(h_0,\ldots,h_t,0) \in \mathbb{Z}_p^{t+2}$.

Proposition 2.2. *For every $t \geq 1$, $\mathrm{DLOG}(G_{p,t})$ and $\mathrm{DDH}(G_{p,t})$ are polynomial time many-one reducible to respectively $\mathrm{DLOG}(G_{p,t+1})$ and $\mathrm{DDH}(G_{p,t+1})$; and $\mathrm{CDH}(G_{p,t})$ is commutable in polynomial time with a single query to $\mathrm{CDH}(G_{p,t+1})$.*

Proof. First observe that the identity oracle $\mathrm{Id}_{n'}$ in $G_{p,t+1}$ can be simulated by the identity oracle Id_n of $G_{p,t}$. Indeed, for an arbitrary element h^* in $G_{p,t+1}$, where $h^*=(h_0,h_1,\ldots,h_t,h_{t+1})$, set $h=(h_0,h_1,\ldots,h_t)$. Then $h^* \cdot n' = h \cdot n$. Let g be a generator of $G_{p,t}$ with identity oracle Id_n, that is $g \cdot n \neq 0$. Then $g'=(g,0)$ is a generator of $G_{p,t+1}$ with identity oracle $\mathrm{Id}_{n'}$, since $g' \cdot n' = g \cdot n$, and therefore $g' \cdot n' \neq 0$.

For arbitrary $g,h,k,\ell \in G_{p,t}$, and for every integer d, we have $dg=h$ if and only if $dg'=h'$. Similarly, (g,h,k,ℓ) is a DH-quadruple if and only if (g',h',k',ℓ') is a DH-quadruple. This gives the many-one reductions for DLOG and DDH. In the CDH reduction, on an instance (g,h,k), we call $\mathrm{CDH}(G_{p,t+1})$ on instance (g',h',k'). Suppose that it gives the answer $\ell^*=(\ell_0,\ell_1,\ldots,\ell_t,\ell_{t+1})$. We set $\ell=(\ell_0,\ell_1,\ldots,\ell_t)$, and observe that (g,h,k,ℓ) is a DH-quadruple because (g',h',k',ℓ^*) is a DH-quadruple and $\ell^* \cdot n' = \ell \cdot n$. □

3 The complexity in groups of level 1

In most parts of this section we restrict ourselves to the case $t=1$. To simplify notation, we set $n=(1,s)$ and we denote the identity oracle Id_n by Id_s and the line H_n of the plane $\mathbb{Z}_p^2$ by H_s. Also, we refer to s as the *secret*. As it turns out, solving $\mathrm{DLOG}(G_{p,1})$ or $\mathrm{CDH}(G_{p,1})$ is essentially as hard as finding the secret, therefore we formally define this problem as

$\mathrm{SECRET}(G_{p,1})$
Oracle input: Id_s for some $s \in \mathbb{Z}_p$.
Output: s.

What is the query complexity of finding s, that is how many calls to the identity oracle are needed for that task? To answer this question, we consider US, the well studied unstructured search problem. For this, let C be an arbitrary set, and let $s \in C$ be an arbitrary distinguished element. Then the *Grover oracle* $\Delta_s : C \to \{0,1\}$ is the Boolean function such that $\Delta_s(x) = 1$ if and only if $x = s$. The *unstructured search* problem over C is defined as

$\mathrm{US}(C)$
Oracle input: Δ_s for some $s \in C$.
Output: s.

Suppose that the size of C is N. It is easily seen that probabilistic query complexity of $\mathrm{US}(C)$ is linear in N. The quantum query complexity of the problem is also well studied. Grover [12] has determined that it can be solved with $O(\sqrt{N})$ queries, while Bennett et al. [8] have shown that $\Omega(\sqrt{N})$ queries are also necessary.

Fact 3.1. *For $|C| = N$, the randomized query complexity of $\mathrm{US}(C)$ is $\Theta(N)$ and its quantum query complexity is $\Theta(\sqrt{N})$.*

The relationship between US and the problem SECRET is given by the fact that the identity oracle Id_s and the Grover oracle Δ_s can simulate each other with a single query.

Proposition 3.2. *The identity oracle Id_s of $G_{p,s}$ and the Grover oracle Δ_s, defined over $\mathbb{Z}_p$, can simulate each other with at most one query.*

Proof. The simulation of the Grover oracle by the identity oracle is simple: for $x \in \mathbb{Z}_p$ just query Id_s on $(x, -1)$.

For the reverse direction, let $h = (h_0, h_1)$ be an input to the identity oracle. Then h encodes the identity element, that is $\mathrm{Id}_s(h) = 1$, if and only if $-h_0 = sh_1$. When h_1 is invertible in $\mathbb{Z}_p$ we can check by the Grover oracle if $-h_0 h_1^{-1} = s$. For $h_1 = 0$ the only possible value for h_0 to put h into H_s is 0. Therefore we have

$$\mathrm{Id}(h) = \begin{cases} 1 & \text{if } h = (0,0) \\ 0 & \text{if } h_1 = 0 \text{ and } h_0 \neq 0 \\ \Delta_s(-h_0 h_1^{-1}) & \text{otherwise.} \end{cases}$$

□

Corollary 3.3. *The randomized query complexity of $\mathrm{SECRET}(G_{p,1})$ is $\Theta(p)$ and its quantum query complexity is $\Theta(\sqrt{p})$.*

We will now consider the reductions of $\mathrm{SECRET}(G_{p,1})$ to $\mathrm{DLOG}(G_{p,1})$ and $\mathrm{CDH}(G_{p,1})$. The case of $\mathrm{DLOG}(G_{p,1})$ in fact follows from the case of $\mathrm{CDH}(G_{p,1})$, but it is so simple that it is worth to describe it explicitly.

Lemma 3.4. *The secret s in $G_{p,1}$ can be found with a single oracle call to* $\mathrm{DLOG}(G_{p,1})$

Proof. First observe that $(1,0)$ is a generator of $G_{p,1}$, for every s. The algorithm calls $\mathrm{DLOG}(G_{p,1})$ on input $(g,h) = ((1,0),(0,1))$. Since $\phi(g) = 1$ and $\phi(h) = s$ where ϕ is as in Proposition 2.1, the oracle's answer is the secret s itself. □

We remark that with overwhelming probability we could have given also a random couple $(g,h) \in G_{p,1}^2$ to the oracle, where g is a generator. Indeed, let's suppose that d is the discrete logarithm. Then $h - dg \in H_s$, and therefore $s = -(h_0 - dg_0)(h_1 - dg_1)^{-1}$, where the operations are done in $\mathbb{Z}_p$, under the condition that $h_1 - dg_1 \neq 0$, which happens with probability $(p-1)/p$.

The reduction of $\mathrm{SECRET}(G_{p,1})$ to $\mathrm{CDH}(G_{p,1})$ requires more work. The main idea of the reduction is to extend $G_{p,t}$ to a field and use the multiplication for the characterization of DH-quadruples. Indeed, since $\mathbb{Z}_p$ is the additive group of the field $\mathbb{F}_p$, we can use the isomorphism ϕ of Proposition 2.1 between $G_{p,t}$ and $\mathbb{Z}_p$ to define appropriate multiplication and multiplicative inverse operations. This extends $G_{p,t}$ to a field isomorphic to $\mathbb{F}_p$ which we denote by $F_{p,t}$. This process is completely standard but we describe it for completeness. The definitions of these two operations are:

$$hk = \phi^{-1}(\phi(h)\phi(k)),$$
$$h^{-1} = \phi^{-1}(\phi(h)^{-1}).$$

With these operations the map ϕ becomes a field isomorphism between $F_{p,t}$ and $\mathbb{F}_p$.

Proposition 3.5. *The map ϕ of Proposition 2.1 is an isomorphism between $F_{p,t}$ and $\mathbb{F}_p$.*

Proof. By definition $\phi(hk) = \phi(h)\phi(k)$ and $\phi(h^{-1}) = \phi(h)^{-1}$. □

The field structure of $F_{p,t}$ yields a very useful characterization of DH-quadruples.

Proposition 3.6. *Let g be a generator of $G_{p,t}$. In $F_{p,t}$ the quadruple (g,h,k,ℓ) is a* DH*-quadruple if and only if*

$$g\ell - hk = 0.$$

Proof. Let $h = ag, k = bg$ and $\ell = cg$ for some integers a,b,c. Using the field structure of $F_{p,t}$, it is true that $g\ell - hk = 0$ if and only if $(c-ab)g^2 = 0$. Since $F_{p,t}$ is isomorphic to $\mathbb{F}_p$, an element g is a generator of the additive group $\mathbb{Z}_p$ exactly when $g \neq 0$, and therefore when g^2 is a generator. Therefore $(c-ab)g^2 = 0$ if an only if $c = ab$. □

We define the application $\chi : \mathbb{Z}_p^{t+1} \to \mathbb{F}_p[x_1,\ldots,x_t]$, from $\mathbb{Z}_p^{t+1}$ to the ring of t-variate polynomials over $\mathbb{F}_p$, where the image $\chi(h)$ of $h = (h_0,h_1,\ldots,h_t) \in \mathbb{Z}_p^{t+1}$ is the polynomial $p_h(x_1,\ldots,x_t) = h_0 + \sum_{i=1}^t h_i x_i$. Observe that $p_h(n_1,\ldots n_t) = h \cdot n$, therefore the isomorphism ϕ between $G_{p,t}$ with identity oracle Id_n and $\mathbb{Z}_p$ can also be expressed as $\phi(h) = p_h(n_1,\ldots n_t)$.

Proposition 3.7. *Let g be a generator of $G_{p,1}$ and let h,k,ℓ be arbitrary elements. Then (g,h,k,ℓ) is a DH-quadruple if and only if s is a root of the polynomial $p_g(x)p_\ell(x) - p_h(x)p_k(x)$.*

Proof. By Proposition 3.6 we know that (g,h,k,ℓ) is a DH-quadruple if and only if $g\ell - hk = 0$, that is when $p_{g\ell-hk}(s) = 0$. Now Proposition 3.5 implies that this happens exactly when $p_g(s)p_\ell(s) - p_h(s)p_k(s) = 0$.

□

Lemma 3.8. *There is a probabilistic polynomial time algorithm which, given oracle access to* $\mathrm{CDH}(G_{p,1})$*, solves* $\mathrm{SECRET}(G_{p,1})$*. The algorithm asks a single query to* $\mathrm{CDH}(G_{p,1})$*. If we are also given a quadratic non-residue in* $\mathbb{Z}_p$*, the algorithm can be made deterministic.*

Proof. The algorithm sets $g = (1,0), h = (0,1), k = (1,1)$ and presents it to the oracle. Let the oracle's answer be $\ell = (\ell_0, \ell_1)$. Since (g,h,k,ℓ) is a DH-quadruple, by Proposition 3.7 we have that s is the root of the second degree equation

$$x^2 + (1-\ell_1)x + \ell_0 = 0.$$

Assuming that a quadratic non-residue in $\mathbb{Z}_p$ is available then the (not necessarily distinct) roots x_1, x_2 can be computed in deterministic polynomial time using the Shanks-Tonelli algorithm [21]. Without this assumption, a quadratic non-residue can always be computed in probabilistic polynomial time because for $p > 2$ the quadratic residues form a subgroup of index two of the multiplicative group of $\mathbb{F}_p$ and hence $p > 2$ half of the nonzero elements in $\mathbb{Z}_p$ are not squares. Finally, we make at most two calls to Id_s on $(x_1, -1)$ and on $(x_2, -1)$. The positive answer tells us which one of the roots is the secret s. □

Similarly to the DLOG case, we could have presented with overwhelming probability also a random triple $(g,h,k) \in G_{p,s}^3$ to $\mathrm{CDH}(G_{p,1})$, where g is a generator. Indeed, if the oracle answer is $\ell = (\ell_0, \ell_1)$ then s is a root of the (at most second degree) equation

$$(g_0 + g_1 x)(\ell_0 + \ell_1 x) = (h_0 + h_1 x)(k_0 + k_1 x).$$

If the equation is of degree 2 then we can proceed as in the proof of Lemma 3.8. This happens exactly when $h_1 k_1 \neq g_1 \ell_1$. But for every possible fixed value a for $g_1 \ell_1$, the probability, over random h_1 and k_1, that $h_1 k_1 = a$ is at most $2/p$, the worst case being $a = 0$. Therefore a random triple (g,h,k) would be suitable for the proof with probability at least $(p-2)/p$.

Theorem 3.9. *The following lower bounds hold for the query complexity of* DLOG *and* CDH*:*

(1) *The classical query complexity of both* $\mathrm{DLOG}(G_{p,s})$ *and* $\mathrm{CDH}(G_{p,s})$ *is* $\Omega(p)$*.*

(2) *The quantum query complexity of both* $\mathrm{DLOG}(G_{p,s})$ *and* $\mathrm{CDH}(G_{p,s})$ *is* $\Omega(\sqrt{p})$*.*

Proof. Let us suppose that with m queries to the identity oracle Id_s, one can solve $\mathrm{DLOG}(G_{p,1})$ or $\mathrm{CDH}(G_{p,1})$. Respectively Lemma 3.4 and Lemma 3.8 imply that $\mathrm{SECRET}(G_{p,1})$ can be solved with m queries. The result then follows from the lower bounds of Corollary 3.3. □

Theorem 3.10. *The* $\mathrm{DDH}(G_{p,1})$ *problem can be solved in probabilistic polynomial time. If we are given a quadratic non-residue in* $\mathbb{Z}_p$ *the algorithm can be made deterministic.*

Proof. Let (g,h,k,ℓ) be an input to $\mathrm{DDH}(G_{p,1})$ where g is a generator of $G_{p,1}$. By Proposition 3.7 it is a DH-quadruple if and only if s is a root of the polynomial $p_g(x)p_\ell(x) - p_h(x)p_k(x)$, and that is what the algorithm checks. When the polynomial is constant, then the answer is yes if the constant is zero, and otherwise it is no. When the polynomial is non constant, the algorithm essentially proceeds as the one in Lemma 3.8. It solves the (at most second degree) equation and then checks with the identity oracle if one root is equal to s. □

4 The complexity of DDH in groups of level 2

There are several powerful means to prove quantum query lower bounds, most notably the adversary and the polynomial method [7]. The quantum adversary method initiated by Ambainis [2] has been extended in several ways. The most powerful of those, the method using negative weights [13], turned out to be an exact characterization of the quantum query complexity [16]. We use here a special case of the positive weighted adversary method [1, 3, 25] that also gives probabilistic lower bounds [1].

Fact 4.1. *Let $A : S \to \{0,1\}$ be a Boolean functional oracle problem, where $S \subseteq \{0,1\}^m$. For any $S \times S$ matrix M, set*

$$\sigma(M,f) = \sum_{g \in S} M[f,g].$$

Let Γ be an arbitrary $S \times S$ nonnegative symmetric matrix that satisfies $\Gamma[f,g] = 0$ whenever $A(f) = A(g)$. For $1 \le x \le m$, let Γ_x be the matrix

$$\Gamma_x[f,g] = \begin{cases} 0 & \text{if } f(x) = g(x), \\ \Gamma[f,g] & \text{otherwise.} \end{cases}$$

Then

$$\mathrm{Q}(A) = \Omega\left(\min_{\Gamma[f,g]\neq 0, f(x)\neq g(x)} \sqrt{\frac{\sigma(\Gamma,f)\sigma(\Gamma,g)}{\sigma(\Gamma_x,f)\sigma(\Gamma_x,g)}} \right),$$

$$\mathrm{R}(A) = \Omega\left(\min_{\Gamma[f,g]\neq 0, f(x)\neq g(x)} \max\left\{ \frac{\sigma(\Gamma,f)}{\sigma(\Gamma_x,f)}, \frac{\sigma(\Gamma,g)}{\sigma(\Gamma_x,g)} \right\} \right).$$

Theorem 4.2. *The following lower bounds hold for the query complexity of* DDH *in level* 2 *hidden cyclic groups:*

$$\mathrm{Q}(\mathrm{DDH}(G_{p,2})) = \Omega(\sqrt{p}) \text{ and } \mathrm{R}(\mathrm{DDH}(G_{p,2})) = \Omega(p).$$

Proof. Let $i = ((1,0,0),(0,1,0),(0,0,1),(0,1,1))$. Observe that the element $(1,0,0)$ is a generator of $G_{p,2}$, for any 2-suitable vector $n = (1,n_1,n_2)$. By Proposition 3.6, we know that i is a DH-quadruple if and only if $n_1 + n_2 = n_1 n_2$. We say that n is *positive* if this equality holds, otherwise we say that it is *negative*. Let $m = p^3$ and let $S = \{\mathrm{Id}_n : n \in \mathbb{Z}_p^2\}$. We will apply Fact 4.1 to the Boolean functional oracle problem DDH defined in $G_{p,2}$ on input i with the oracle input being the identity oracle $\mathrm{Id}_n : \mathbb{Z}_p^3 \to \{0,1\}$.

For simplicity we will refer to this Boolean functional oracle problem just by $\mathrm{DDH}(n)$. We define the symmetric $p^2 \times p^2$ Boolean adversary matrix Γ as follows:

$$\Gamma[n,n'] = \begin{cases} 1 & \text{if } \mathrm{DDH}(n) \neq \mathrm{DDH}(n'), \\ 0 & \text{otherwise,} \end{cases}$$

where again $\Gamma[n,n']$ is a shorthand notation for $\Gamma[\mathrm{Id}_n, \mathrm{Id}_{n'}]$.

We first determine $\sigma(\Gamma,n)$. If $n_1 = 1$ then there is no n_2 such that $n_1+n_2 = n_1 n_2$. Otherwise, for every fixed $n_1 \neq 1$, there is a unique n_2 that makes this equality hold, in particular $n_2 = n_1(n_1-1)^{-1}$. Therefore the number of positive n is $p-1$ and the number of negative n is p^2-p+1. Thus we have the following values for $\sigma(\Gamma,n)$:

$$\sigma(\Gamma,n) = \begin{cases} p^2-p+1 & \text{if } n \text{ is positive,} \\ p-1 & \text{otherwise.} \end{cases}$$

Let us recall, that by definition, for every $h \in G_{p,2}$,

$$\Gamma_h[n,n'] = \begin{cases} 1 & \text{if } \mathrm{DDH}(n) \neq \mathrm{DDH}(n') \text{ and } \mathrm{Id}_n(h) \neq \mathrm{Id}_{n'}(h), \\ 0 & \text{otherwise.} \end{cases} \tag{4.1}$$

We fix now n and n' such that $\mathrm{DDH}(n) \neq \mathrm{DDH}(n')$, we will suppose without loss of generality that n is positive and n' is negative. We also fix $h = (h_0,h_1,h_2)$ in $\mathbb{Z}_p^3$ such that $\mathrm{Id}_n(h) \neq \mathrm{Id}_{n'}(h)$. This implies that $(h_1,h_2) \neq (0,0)$. We want to lower bound $\sigma(\Gamma,n)/\sigma(\Gamma_h,n)$ and $\sigma(\Gamma,n')/\sigma(\Gamma_h,n')$. Obviously both fractions are at least 1. We distinguish two cases according to whether $\mathrm{Id}_n(h) = 0$ or $\mathrm{Id}_{n'}(h) = 0$.

Case 1: $\mathrm{Id}_{n'}(h) = 0$. Then

$$\sigma(\Gamma_h,n') = \left| \left\{ (m_1,m_2) \in \mathbb{Z}_p^2 : \begin{array}{l} m_1+m_2 = m_1 m_2 \text{ and} \\ h_0 + h_1 m_1 + h_2 m_2 = 0 \end{array} \right\} \right|.$$

We claim that the carnality at the right hand side is at most 2. We know already that $m_1 \neq 1$ and $m_2 = m_1(m_1-1)^{-1}$. Therefore m_1 satisfies the second degree equation

$$h_1 x^2 + (h_0 - h_1 + h_2)x - h_0 = 0.$$

The number of roots of this equation is at most 2, unless the polynomial is 0. But this can not be the case, because then $h_1 = h_2 = 0$, a contradiction. Therefore, taking into account (4.1), we have

$$\frac{\sigma(\Gamma,n')}{\sigma(\Gamma_h,n')} = \Omega\left(\frac{p}{1}\right) = \Omega(p). \tag{4.2}$$

Case 2: $\mathrm{Id}_n(h) = 0$. Then

$$\sigma(\Gamma_h,n) \leq |\{(m_1,m_2) \in \mathbb{Z}_p^2 : h_0 + h_1 m_1 + h_2 m_2 = 0\}|.$$

Since $(h_1,h_2) \neq (0,0)$, the number of roots of this linear equation with two variables is p. Therefore, again taking into account (4.1), we have

$$\frac{\sigma(\Gamma,n)}{\sigma(\Gamma_h,n)} = \Omega\left(\frac{p^2}{p}\right) = \Omega(p). \tag{4.3}$$

The statements of the theorem immediately follow from equations (4.2) and (4.3). □

Similarly to the remarks after Lemmas 3.4 and 3.8, we could have used in the proof instead of i a random input (g,h,k,ℓ), with high probability of success. Indeed, if we can show that the number of solutions of the system of equations

$$\begin{cases} (g_0+g_1x+g_2y)(\ell_0+\ell_1x+\ell_2y) & \\ \quad -(h_0+h_1x+h_2y)(k_0+k_1x+k_2y) & =0 \\ 1+u_1x+u_2y & =0 \end{cases}$$

is at most 2 for every $u=(1,u_1,u_2)$ in $\mathbb{Z}_p^3$, with $(u_1,u_2)\neq(0,0)$, then the same proof works. To see what we claim we observe first that $g_2\ell_2-h_2k_2$ is nonzero with probability at least $(p-1)/p$. If this happens then we are done with every u of the form $u=(1,u_1,0)$. Indeed, in that case $u_1\neq 0$ and the second equation implies $x=-1/u_1$ and by substituting this in the first equation we obtain an equation in y with a proper quadratic term. To deal with those u for which $u_2\neq 0$ we set $\alpha=1/u_2$ and $\beta=u_1/u_2$. By the second equation we have $y=-\beta x-\alpha$ and substituting this in the first equation the polynomial becomes

$$P_0+P_1x+P_2x^2,$$

with

$$P_0=A+B\alpha+C\alpha^2,\ \ P_1=D+E\alpha+B\beta+2C\alpha\beta\ \text{ and }\ P_2=(F+E\beta+C\beta^2),$$

where $A=g_0\ell_0-h_0k_0$, $B=h_0k_2+h_2k_0-g_0\ell_2-g_2\ell_0$, $C=g_2\ell_2-h_2k_2)$, $D=g_0\ell_1+g_1\ell_0-h_0k_1-h_1k_0$, $E=h_1k_2+h_2k_1-g_1\ell_2-g_2\ell_1$ and $F=g_1\ell_1+h_1k_1$. Using Macaulay2 [11], one can show that the ideal of $\mathbb{F}_p[g_0,\ldots,\ell_2,\alpha,\beta]$ generated by P_0,P_1 and P_2 contains a nonzero polynomial f of degree six from $\mathbb{F}_p[g_0,\ldots,\ell_2]$. By the Schwartz-Zippel lemma [20, 26], f takes a nonzero value with probability at least $1-6/p$. If that happens then there exist no α,β making the three coefficients P_0,P_1 and P_2 simultaneously zero. The overall probability of choosing a good g,h,k,ℓ is therefore at least 1-7/p.

References

[1] SCOTT AARONSON: Lower bounds for local search by quantum arguments. *SIAM J. Comput.*, 35(4):804–824, 2006. 10

[2] ANDRIS AMBAINIS: Quantum lower bounds by quantum arguments. *J. Comput. Syst. Sci.*, 64(4):750–767, 2002. 10

[3] ANDRIS AMBAINIS: Polynomial degree vs. quantum query complexity. *J. Comput. Syst. Sci.*, 72(2):220–238, 2006. 10

[4] LÁSZLÓ BABAI AND ROBERT BEALS: A polynomial-time theory of black-box groups i. In *Groups St. Andrews 1997 in Bath, I*, volume 260, pp. 30–64. Cambridge Univ. Press, 1999. 2

[5] LÁSZLÓ BABAI AND ENDRE SZEMERÉDI: On the complexity of matrix group problems i. In *FOCS*, pp. 229–240. IEEE Computer Society, 1984. 1

[6] ROBERT BEALS AND LÁSZLÓ BABAI: Las vegas algorithms for matrix groups. In *FOCS*, pp. 427–436. IEEE Computer Society, 1993. 2

[7] ROBERT BEALS, HARRY BUHRMAN, RICHARD CLEVE, MICHELE MOSCA, AND RONALD DE WOLF: Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001. 5, 10

[8] CHARLES H. BENNETT, ETHAN BERNSTEIN, GILLES BRASSARD, AND UMESH VAZIRANI: Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997. 7

[9] KEVIN K. H. CHEUNG AND MICHELE MOSCA: Decomposing finite abelian groups. *Quantum Inf. Comput.*, 1(3):26–32, 2001. 2

[10] IVAN DAMGÅRD, CARMIT HAZAY, AND ANGELA ZOTTAREL: Short paper on the generic hardness of ddh-ii. Manuscript, `http://cs.au.dk/~angela/Hardness.pdf`, 2014. 3

[11] DANIEL R. GRAYSON AND MICHAEL E. STILLMAN: Macaulay2, a software system for research in algebraic geometry. Available at `http://www.math.uiuc.edu/Macaulay2/`. 12

[12] LOV K. GROVER: Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, 1997. preliminary version in STOC 1996. 7

[13] PETER HØYER, TROY LEE, AND ROBERT SPALEK: Negative weights make adversaries stronger. In DAVID S. JOHNSON AND URIEL FEIGE, editors, *STOC*, pp. 526–535. ACM, 2007. 10

[14] ANTOINE JOUX AND KIM NGUYEN: Separating decision diffie-hellman from computational diffie-hellman in cryptographic groups. *J. Cryptol.*, 16(4):239–247, 2003. 2

[15] WILLIAM M. KANTOR AND ÁKOS SERESS: *Black box classical groups,*. Volume 208 of *Memoirs of the AMS, Vol. 208*. American Mathematical Society, 2001. 2

[16] TROY LEE, RAJAT MITTAL, BEN W. REICHARDT, ROBERT SPALEK, AND MARIO SZEGEDY: Quantum query complexity of state conversion. In RAFAIL OSTROVSKY, editor, *FOCS*, pp. 344–353. IEEE Computer Society, 2011. 10

[17] UELI M. MAURER AND STEFAN WOLF: The relationship between breaking the diffie-hellman protocol and computing discrete logarithms. *SIAM J. Comput.*, 28(5):1689–1721, 1999. 2

[18] MICHELE MOSCA: *Computations for Algebras and Group Representations*. Ph. D. thesis, University of Oxford, 1999. 2, 3

[19] STEPHEN C. POHLIG AND MARTIN E. HELLMAN: An improved algorithm for computing logarithms over gf(p) and its cryptographic significance (corresp.). *IEEE Trans. Inf. Theory*, 24(1):106–110, 1978. 3

[20] JACOB T. SCHWARTZ: Probabilistic algorithms for verification of polynomial identities (invited). In EDWARD W. NG, editor, *EUROSAM*, volume 72 of *Lecture Notes in Computer Science*, pp. 200–215. Springer, 1979. 12

[21] DANIEL SHANKS: Five number-theoretic algorithms. In *Proceedings of the second Manitoba conference on numerical mathematics*, pp. 51–70, 1972. 9

[22] PETER W. SHOR: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. 3

[23] VICTOR SHOUP: Lower bounds for discrete logarithms and related problems. In WALTER FUMY, editor, *EUROCRYPT*, volume 1233 of *Lecture Notes in Computer Science*, pp. 256–266. Springer, 1997. 3

[24] JOHN WATROUS: Quantum algorithms for solvable groups. In JEFFREY SCOTT VITTER, PAUL G. SPIRAKIS, AND MIHALIS YANNAKAKIS, editors, *STOC*, pp. 60–67. ACM, 2001. 2

[25] SHENGYU ZHANG: On the power of ambainis's lower bounds. In JOSEP DÍAZ, JUHANI KARHUMÄKI, ARTO LEPISTÖ, AND DONALD SANNELLA, editors, *ICALP*, volume 3142 of *Lecture Notes in Computer Science*, pp. 1238–1250. Springer, 2004. 10

[26] RICHARD ZIPPEL: Probabilistic algorithms for sparse polynomials. In EDWARD W. NG, editor, *EUROSAM*, volume 72 of *Lecture Notes in Computer Science*, pp. 216–226. Springer, 1979. 12

AUTHORS

Gábor Ivanyos
research advisor
Institute for Computer Science and Control, Eötvös Loránd Reseach Network, Budapest, Hungary
Gabor.Ivanyos@sztaki.hu
www.sztaki.hu/~ivanyos

Antoine Joux
tenured faculty
CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
antoine.joux@m4x.org
https://cispa.de/en/people/c01anjo

Miklos Santha
professor
Centre for Quantum Technologies and MajuLab, National University of Singapore, Singapore
miklos.santha@gmail.com
https://www.quantumlah.org/people/profile/miklos