Diffie-Hellman, Decision Diffie-Hellman, and Discrete Logarithms

Ueli Maurer Stefan Wolf [1]
Computer Science Department
ETH Zürich
CH-8092 Zürich, Switzerland
{maurer,wolf}@inf.ethz.ch

Abstract — **Let G be a cyclic group of order n. With respect to polynomial-time non-uniform generic reductions, the Diffie-Hellman problem and the discrete logarithm problem are equivalent in G if and only if n contains no multiple large prime factors. The Diffie-Hellman decision problem is equivalent to the Diffie-Hellman problem in G if and only if all prime factors of n are small.**

I. Computational Problems in Cyclic Groups

Let G be a finite cyclic group with generator g. The security of the well-known Diffie-Hellman (DH) protocol relies on the difficulty of the so-called *DH problem (DHP)*: Given two group elements g^x and g^y, compute g^{xy}. Of course this problem is at most as hard as the *discrete logarithm problem (DLP)*: Given g^x, compute x. Finally, the *DH decision problem (DHDP)* has been defined as follows: Given (g^x, g^y, g^z), decide whether $z \equiv xy \pmod{|G|}$. Challenging open problems in this context are whether the three problems are hard, and whether they are computationally equivalent. With respect to *generic* algorithms and reductions, the picture is quite complete.

II. Generic Complexity

The model of generic algorithms was introduced by Shoup [3]. Intuitively, a generic algorithm is a general-purpose algorithm that does not make use of any property of the representation of the group elements other than the fact that each group element has a unique representation. More precisely, a generic algorithm for the group $\mathbf{Z}_n$ takes as input a list $(\sigma(x_1), \ldots, \sigma(x_l))$, where the x_i are elements of $\mathbf{Z}_n$ and σ is a random encoding of the group elements, and is allowed to make calls to oracles for the group operation and inversion.

Shoup proved that the generic complexity of the DHP and of the DLP is $\Theta(\sqrt{p})$, where p is the largest prime factor of n, whereas the complexity of the DHDP is $\Omega(\sqrt{q})$ if q is the *smallest* prime factor of n. However, these results have no direct implications for any particular group G. On the other hand, a generic reduction of one problem to another proves their computational equivalence for *every* particular group G.

III. Generic Equivalence

Trivially, the DHDP in a group G can efficiently be reduced to the DHP in the same group, which can be further reduced to the DLP. This section deals with generic reduction algorithms in the inverse direction.

Both positive [2] and negative [1] results on the generic equivalence of the DHP and the DLP have been proved. The following completeness result depends on an unproven conjecture on the existence of smooth numbers in small intervals.

[1]Supported in part by the Swiss National Science Foundation (SNF), grant No. 20-42105.94.

Theorem 1 [2, 1]. There exists a polynomial-time generic reduction of the DL problem to the DH problem for groups G of order n if and only if all multiple prime factors of n are of size $(\log n)^{O(1)}$.

The following theorem on the other hand shows that the DHDP and the DHP are equivalent in a generic sense only in the trivial case where the group order is smooth. Intuitively, an oracle for the DHDP cannot help solving the DHP because for every possible input to the oracle which can be efficiently generated the answer is known in advance with overwhelming probability.

Theorem 2. Every generic reduction of the DHP to the DHDP for groups of order n has expected running time $\Omega(\sqrt{p})$, where p is the largest prime factor of n.

Proof Sketch. Given $\sigma(1)$, $\sigma(x)$, and $\sigma(y)$, the algorithm must output $\sigma(xy)$. Assume that the algorithm can interact with the oracles for the group operation and inversion and additionally with an oracle solving the DHDP. All the algorithm can do is compute $P_i(x,y)$ for *linear* expressions P_i and call the DHD oracle with inputs $(\sigma(P_i(x,y)), \sigma(P_j(x,y)), \sigma(P_k(x,y)))$. One can show that the answer of the oracle, for random x and y, is "no" but with probability $2/p$ (unless trivially "yes"). Finally, given that the algorithm always answers "no" during a particular execution, the success probability of the algorithm is roughly the same as for an algorithm which *cannot* make calls to the DHD oracle. $\square$

We conclude that DHP $\cong$ DLP holds exactly for groups whose orders are free of multiple large prime factors, whereas DHDP $\cong$ DHP is true for groups with smooth orders only.

Acknowledgements

Victor Shoup independently made a similar observation concerning the relationship between the DHP and the DHDP.

References

[1] U. Maurer and S. Wolf, "Lower bounds on generic algorithms in groups," *Advances in Cryptology – EUROCRYPT '98*, Lecture Notes in Computer Science, Springer-Verlag, 1998.

[2] U. Maurer and S. Wolf, "The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms," to appear in *SIAM Journal of Computing*, 1998.

[3] V. Shoup, "Lower bounds for discrete logarithms and related problems," *Advances in Cryptology – EUROCRYPT '97*, Lecture Notes in Computer Science, vol. 1233, pp. 256–266, Springer-Verlag, 1997.