Diffie–Hellman problem

The **Diffie–Hellman problem (DHP)** is a mathematical problem first proposed by Whitfield Diffie and Martin Hellman in the context of cryptography. The motivation for this problem is that many security systems use one-way functions: mathematical operations that are fast to compute, but hard to reverse. For example, they enable encrypting a message, but reversing the encryption is difficult. If solving the DHP were easy, these systems would be easily broken.

Contents

Problem description

The Diffie–Hellman problem is stated informally as follows:

> Given an element g and the values of g^x and g^y, what is the value of g^{xy}?

Formally, g is a generator of some group (typically the multiplicative group of a finite field or an elliptic curve group) and x and y are randomly chosen integers.

For example, in the Diffie–Hellman key exchange, an eavesdropper observes g^x and g^y exchanged as part of the protocol, and the two parties both compute the shared key g^{xy}. A fast means of solving the DHP would allow an eavesdropper to violate the privacy of the Diffie–Hellman key exchange and many of its variants, including ElGamal encryption.

Computational complexity

In cryptography, for certain groups, it is *assumed* that the DHP is hard, and this is often called the **Diffie–Hellman assumption**. The problem has survived scrutiny for a few decades and no "easy" solution has yet been publicized.

As of 2006, the most efficient means known to solve the DHP is to solve the discrete logarithm problem (DLP), which is to find x given g and g^x. In fact, significant progress (by den Boer, Maurer, Wolf, Boneh and Lipton) has been made towards showing that over many groups the DHP is almost as hard as the DLP. There is no proof to date that either the DHP or the DLP is a hard problem, except in generic groups (by Nechaev and Shoup).

Other variants

Many variants of the Diffie–Hellman problem have been considered. The most significant variant is the decisional Diffie–Hellman problem (DDHP), which is to distinguish g^{xy} from a random group element, given g, g^x, and g^y. Sometimes the DHP is called the computational Diffie–Hellman problem (CDHP) to more clearly distinguish it from the DDHP. Recently groups with pairings have become popular, and in these groups the DDHP is easy, yet the DHP is still assumed to be hard. For less significant variants of the DHP see the references.

References

- B. den Boer, *Diffie–Hellman is as strong as discrete log for certain primes* in Advances in Cryptology – CRYPTO 88, Lecture Notes in Computer Science 403, Springer, p. 530, 1988.
- U. M. Maurer and S. Wolf, *Diffie–Hellman oracle* in Advances in Cryptology – CRYPTO 96, (N. Koblitz, ed.), Lecture Notes in Computer Science 1070, Springer, pp. 268–282, 1996.
- Maurer, Ueli M.; Wolf, Stefan (2000). "The Diffie–Hellman Protocol". *Designs, Codes and Cryptography*. **19** (2/3): 147–171. doi:10.1023/A:1008302122286 (https://doi.org/10.1023%2FA%3A1008302122286).
- D. Boneh and R. J. Lipton, *Algorithms for black-box fields and their application to cryptotography* in Advances in Cryptology – CRYPTO 96, (N. Koblitz, ed.), Lecture Notes in Computer Science 1070, Springer, pp. 283–297, 1996.
- A. Muzereau, N. P. Smart and F. Vercauteran, *The equivalence between the DHP and DLP for ellipti curves used in practical applications*, LMS J. Comput. Math., **7**, pp. 50–72, 2004. See [www.lms.ac.uk].
- D. R. L. Brown and R. P. Gallant, *The Static Diffie–Hellman Problem* (http://eprint.iacr.org/2004/306), IACR ePrint 2004/306.
- V. I. Nechaev, *Complexity of a determinate algorithm for the discrete logarithm*, Mathematical Notes, **55** (2), pp. 165–172, 1994.
- V. Shoup, *Lower bounds for discrete logarithms and related problems* in Advances in Cryptology – EUROCRYPT 97, (W. Fumy, ed.), Lecture Notes in Computer Science 1233, Springer, pp. 256–266, 1997.
- Bao, Feng; Deng, Robert H.; Zhu, Huafei (2003). "Variations of Diffie-Hellman Problem". *ICICS 2003: Information and Communications Security*. Lecture Notes in Computer Science. **2836**. Springer. pp. 301–312. CiteSeerX 10.1.1.104.3007 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.104.3007). doi:10.1007/978-3-540-39927-8_28 (https://doi.org/10.1007%2F978-3-540-39927-8_28). ISBN 978-3-540-20150-2.
- Boneh, Dan (1998). "The Decision Diffie-Hellman problem". *ANTS 1998: Algorithmic Number Theory*. Lecture Notes in Computer Science. **1423**. Springer. pp. 48–63. CiteSeerX 10.1.1.461.9971 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.461.9971). doi:10.1007/bfb0054851 (https://doi.org/10.1007%2Fbfb0054851). ISBN 978-3-540-64657-0.
- Bresson, Emmanuel; Chevassut, Olivier; Pointcheval, David (2003). "The Group Diffie-Hellman Problems" (https://www.di.ens.fr/~bresson/papers/BreChePoi02b.pdf) (PDF). *SAC 2002: Selected Areas in Cryptography*. Lecture Notes in Computer Science. **2595**. Springer. pp. 325–338. doi:10.1007/3-540-36492-7_21 (https://doi.org/10.1007%2F3-540-36492-7_21). ISBN 978-3-540-00622-0.
- Biham, Eli; Boneh, Dan; Reingold, Omer (1999). "Breaking generalized Diffie–Hellman modulo a composite is no easier than factoring". *Information Processing Letters*. **70** (2): 83–87. CiteSeerX 10.1.1.39.110 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.39.110). doi:10.1016/S0020-0190(99)00047-2 (https://doi.org/10.1016%2FS0020-0190%2899%2900047-2).
- Steiner, Michael; Tsudik, Gene; Waidner, Michael (1996). "Diffie-Hellman key distribution extended to group communication" (https://archive.org/details/3rdacmconference00asso). *Proceedings of the 3rd ACM conference on Computer and communications security - CCS '96* (https://archive.org/details/3rdacmconference00asso/page/31). ACM. pp. 31–37 (https://archive.org/details/3rdacmconference00asso/page/31). CiteSeerX 10.1.1.35.9717 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.35.9717). doi:10.1145/238168.238182 (https://doi.org/10.1145%2F238168.238182). ISBN 978-0897918299.

- Diffie, W.; Hellman, M. (1976). "New directions in cryptography". *IEEE Transactions on Information Theory*. **22** (6): 644–654. CiteSeerX 10.1.1.37.9720 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.9720). doi:10.1109/tit.1976.1055638 (https://doi.org/10.1109%2Ftit.1976.1055638).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Diffie–Hellman_problem&oldid=931197857"

This page was last edited on 17 December 2019, at 15:39 (UTC).