Computational Diffie–Hellman assumption

From Wikipedia, the free encyclopedia

The **computational Diffie–Hellman (CDH assumption)** is the assumption that a certain computational problem within a cyclic group is hard.

Consider a cyclic group *G* of order *q*. The CDH assumption states that, given

$$(g, g^a, g^b)$$

for a randomly-chosen generator *g* and random

$$a, b \in \{0, \ldots, q-1\},$$

it is computationally intractable to compute the value

$$g^{ab}.$$

The security of many cryptosystems is based on the CDH assumption, including notably the Diffie–Hellman key agreement scheme. Also, the confidentiality of ElGamal encryption is equivalent to the CDH assumption (though the semantic security of the scheme is based on the decisional Diffie–Hellman assumption).

The CDH assumption is related to the discrete logarithm assumption, which holds that computing the discrete logarithm of a value base a generator g is hard. If taking discrete logs in $\mathbb{G}$ were easy, then the CDH assumption would be false: given

$$(g, g^a, g^b),$$

one could efficiently compute g^{ab} in the following way:

- compute a by taking the discrete log of g^a to base g;
- compute g^{ab} by exponentiation: $g^{ab} = (g^b)^a$;

It is an open problem to determine whether the discrete log assumption is equivalent to CDH, though in certain special cases this can be shown to be the case.

The CDH assumption is also related to the decisional Diffie–Hellman assumption (DDH), which holds that it is hard to distinguish tuples of the form (g,g^a,g^b,g^{ab}) from random tuples. If computing g^{ab} from (g,g^a,g^b) were easy, then one could detect DDH tuples trivially. It is believed that CDH is a **weaker** assumption than DDH: there are groups for which detecting DDH tuples is easy, but solving CDH problems is believed to be hard.

See also

- Diffie–Hellman problem
- Diffie–Hellman key exchange

References

1. Variations of the Diffie–Hellman Problem (pdf file (http://www.i2r.a-star.edu.sg/icsd/publications /Baofeng_2003_Variations%20of%20Diffie%20Hellman%20problems.pdf))

2. Towards the Equivalence of Breaking the Diffie–Hellman Protocol and Computing Discrete Logarithms (pdf file (http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C94/271.PDF))

Retrieved from "http://en.wikipedia.org/wiki/Computational_Diffie%E2%80%93Hellman_assumption"
Categories: Asymmetric-key cryptosystems | Computational hardness assumptions

- This page was last modified on 31 January 2010 at 01:43.
-