The Decisional Diffie-Hellman assumption

(Entry for the Encyclopedia of Information Security)

Ran Canetti
IBM Research

December 17, 2002

The hardness of computing discrete logarithms in some large finite groups has been the basis for many cryptographic schemes and protocols in the past decades, starting from the seminal Diffie-Hellman key exchange protocol [8], and continuing with encryption and signatures schemes with a variety of security properties, as well as protocols for numerous other applications. Ideally, we would have liked to be able to prove unconditional statements regarding the computational hardness of computing discrete logarithms. However, since the current state of knowledge does not allow us to prove such claims, we formulate instead mathematical *assumptions* regarding the computational hardness of this set of problems, and prove properties of the protocols we develop based on these assumptions.

A first assumption that is closely related to the Diffie-Hellman key exchange is the Computational Diffie-Hellman assumption (see _Diffie-Hellman problem_ for more detail):

The Computational Diffie-Hellman (CDH) Problem: Given a group G, a generator g of G, and two elements $a = g^x, b = g^y \in G$, compute the value $c = g^{xy} \in G$.

The Computational Diffie-Hellman (CDH) Assumption: Any probabilistic polynomial time algorithm solves the CDH problem only with negligible probability.

Notes: (1). The probability is taken over the random choices of the algorithm. The probability is said to be negligible if it decreases faster than any inverse polynomial in the length of the input. (2.) As usual, the algorithm must run in time that is polynomial in the length of its input, namely in time that is polylogarithmic in the size of G. Also, a solution to the CDH problem is an algorithm that works for *all inputs.* Thus, the CDH assumption implies that there exists an infinite sequence of groups G for which no polytime algorithm can solve the CDH problem with probability that is not negligible. (Still, it is stressed that there exist infinite families of groups for which the CDH problem is in fact easy.) (3.) The assumption can be made with respect either to uniform-complexity or non-uniform complexity algorithms (i.e., circuit families.)

Indeed, the CDH assumption is very basic in cryptography. However, in many cases researchers were unable to prove the desired security properties of protocols based on the CDH assumption alone. (A quintessential example is the Diffie-Hellman key exchange protocol itself.) Furthermore, it appears that, at least in some groups, the CDH assumption captures only a mild flavor of the intractability of the Diffie-Hellman problem. Therefore the *Decisional* Diffie-Hellman assumption was formulated, as follows:

The Decisional Diffie-Hellman (DDH) Problem: Given a group G, a generator g of G, and three elements $a, b, c \in G$, decide whether there exist integers x, y such that $a = g^x$, $b = g^y$, and $c = g^{xy}$.

The Decisional Diffie-Hellman (DDH) Assumption (Version I): Any probabilistic polynomial time algorithm solves the CDH problem only with negligible probability.

The above formulation of the DDH assumption treats the problem as a worst-case computational problem (that is, an algorithm that solves the problem must work on *all* inputs. This formalization provides a useful comparison with the CDH problem. A much more useful alternative formulation of the DDH assumption only discusses the case where the inputs are taken from certain distributions. It is stated as follows:

The Decisional Diffie-Hellman (DDH) Assumption (Version II): The following two distributions are computationally indistinguishable:

- G, g, g^x, g^y, g^{xy}
- G, g, g^x, g^y, g^z

where g is a generator of group G and x, y, z are chosen at random from $\{1, ..., |G|\}$.

Note: More formally, the above two distributions are actually two distribution *ensembles,* namely two families of distributions where each distribution in a family is parameterized by the group G and the generator g. Recall that two distribution ensembles are computationally indistinguishable if, given a set of parameters (in our case, given G and g), no polytime algorithm can tell whether its input is drawn from the first ensemble or from the second. See more details in [10].

This version is useful since it asserts that, even when g^x and g^y are known, the value g^{xy} appears to be a "freshly chosen" random and independent number for any computationally bounded attacker. This holds in spite of the fact that the value g^{xy} is uniquely determined by g^x and g^y, thus its "entropy" (in the information-theoretic sense) is in fact zero. As shown in [14, 12], the two versions of the DDH assumption are equivalent. (Essentially, equivalence holds due to the *random self reducibility* property of the discrete logarithm problem.)

Clearly, the DDH assumption implies the CDH assumption. Furthermore, it appears to be considerably stronger. In fact, there are groups where DDH is clearly false, but CDH may still hold. Still, there exist groups where DDH is believed to hold, for instance multiplicative groups of large prime order. A quintessential example is the subgroup of size q of $\mathbf{Z}_p^*$ where $p = 2q + 1$ and p, q are primes. (In this case the larger prime p is called a _safe prime_, and the smaller prime q is called a _Sophie-Germain_ prime.)

Note: To see an example of a family of groups where DDH does not hold but CDH may still hold, consider a group G where it is easy to check whether an element is a quadratic residue. (E.g., let $G = \mathbf{Z}_p^*$ where p is prime and $|\mathbf{Z}_p^*| = p - 1$ is even.) Here, the CDH assumption may hold, yet DDH is false: If the input is drawn from G, g, g^x, g^y, g^{xy} then it is never the case that the last element is a quadratic non-residue but the preceding two elements are quadratic residues. In contrast, if the input is taken from G, g, g^x, g^y, g^z then the above event happens with significant probability. Other examples of such groups also exist. Here let us mention in particular the case of bilinear and multilinear pairings in Elliptic-Curve groups, which have been recently shown to be useful in cryptography. See e.g. [3].

Some applications of DDH. The DDH assumption proves to be very useful in cryptographic analysis of protocols. It is immediate to show based on DDH that the Diffie-Hellman key exchange results in a "semantically secure" key, i.e. a key that is indistinguishable from random. (It is not known how to prove this statement based on CDH alone.) Similarly, it implies the semantic security of _ElGamal_ encryption. In addition, it is used in proving security of efficient pseudorandom functions [12], chosen-ciphertext-secure encryption [6], commitment and zero-knowledge [13, 7], and many more.

Variants of DDH. The DDH assumption is only one of many assumptions that can be made on the intractability of the discrete logarithm problem. Several variants have been considered in the literature, some of which are *stronger* (allowing to prove stronger security properties of protocols), and some are *weaker* (and are believed to hold even in cases where DDH does not). Of the stronger ones, let us mention variants that allow the exponents x, y to be chosen from distributions other than uniform (or even in a semi-adversarial way) [5]. Other stronger variants are formalized in [3, 11, 9]. Of the weaker ones, we mention variants that give the distinguisher access only to a *hashed* version of the last element (either g^{xy} or g^z), e.g., [1].

Bibliographic note. The DDH assumption is implicit in many early works based on the Diffie-Hellman problem (starting with [8]). To the best of our knowledge, it was first formalized by Brands in [4] (in the context of undeniable signatures). It was further studied in [14, 12] and is widely used since. For further reading, see Boneh's survey [2].

References

[1] M. Abdalla, M. Bellare and P. Rogaway. DHIES: An Encryption Scheme Based on the Diffie-Hellman Problem. In *Topics in Cryptology – CT-RSA 2001*, LNCS No.2020, pp.143-158.

[2] Dan Boneh. The decision Diffie-Hellman problem. In Proceedings of the Third Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, Vol. 1423, Springer-Verlag, pp. 48–63, 1998.

[3] Dan Boneh and Alice Silverberg. Applications of Multilinear Forms to Cryptography. Proceedings of the Conferences in memory of Ruth Michler, Contemporary Mathematics, American Mathematical Society. Cryptology ePrint Archive, Report 2002/080, http://eprint.iacr.org/, 2002.

[4] S. Brands. An efficient off-line electronic cash system based on the representation problem. CWI TR CS-R9323, 1993.

[5] R. Canetti "Toward Realizing Random Oracles: Hash Functions that Hide All Partial Information" in *Advances in Cryptology - CRYPTO97,* Lecture Notes in Computer Science 1294, Springer-Verlag, 1997, pp. 455-469.

[6] R. Cramer and V. Shoup, "A paractical public-key cryptosystem provably secure against adaptive chosen ciphertext attack", *CRYPTO '98*, 1998.

[7] I. Damgård. Efficient Concurrent Zero-Knowledge in the Auxiliary String Model. Eurocrypt 2000.

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Info. Theory* IT-22, November 1976, pp. 644–654.

[9] Yevgeniy Dodis, Efficient Construction of (Distributed) Verifiable Random Functions, Cryptology ePrint Archive, Report 2002/133, http://eprint.iacr.org/, 2002.

[10] O. Goldreich. *Foundations of Cryptography: Volume 1 – Basic Tools.* Cambridge University Press, 2001.

[11] Anna Lysyanskaya. Unique signatures and verifiable random functions from the DH-DDH separation. In CRYPTO 2002.

[12] Moni Naor and Omer Reingold, Number-Theoretic constructions of efficient pseudo-random functions, Extended abstract in: Proc. 38th IEEE Symp. on Foundations of Computer Science, 1997, pp. 458-467

[13] T. P. Pedersen. Distributed provers with applications to undeniable signatures. *EUROCRYPT'91*, 1991.

[14] M. Stadler. Publicly Verifiable Secret sharing. In *Eurocrypt '96*, pages 190–199, 1996. LNCS No. 1070.