Decisional Diffie–Hellman assumption

From Wikipedia, the free encyclopedia

The **decisional Diffie–Hellman (DDH) assumption** is a computational hardness assumption about a certain problem involving discrete logarithms in cyclic groups. It is used as the basis to prove the security of many cryptographic protocols, most notably the ElGamal and Cramer–Shoup cryptosystems.

Contents

Definition

Consider a (multiplicative) cyclic group G of order q, and with generator g. The DDH assumption states that, given g^a and g^b for randomly-chosen $a, b \in \mathbb{Z}_q$, the value g^{ab} "looks like" a random element in G.

This intuitive notion is formally stated by saying that the following two probability distributions are computationally indistinguishable (in the security parameter q):

- (g^a,g^b,g^{ab}), where a and b are randomly and independently chosen from $\mathbb{Z}_q$.
- (g^a,g^b,g^c), where a,b,c are randomly and independently chosen from $\mathbb{Z}_q$.

Triples of the first kind are often called **DDH triples** or **DDH tuples**.

Relation to other assumptions

The DDH assumption is related to the discrete log assumption. If it were possible to efficiently compute discrete logs in G, then the DDH assumption would not hold in G. Given (g^a,g^b,z), one could efficiently decide whether $z = g^{ab}$ by first taking the discrete log a of g^a, and then comparing z with $(g^b)^a$.

For this reason, DDH is considered a **stronger** assumption than discrete log, in the following sense: there are groups for which detecting DDH tuples is easy, but computing discrete logs is believed to be hard. Thus, requiring that the DDH assumption holds in a group is a more restricting requirement.

The DDH assumption is also related to the computational Diffie–Hellman assumption (CDH). If it were possible to efficiently compute g^{ab} from (g^a,g^b), then one could easily distinguish the two probability distributions above. Similar to above, DDH is considered a stronger assumption than CDH.

Other properties

The problem of detecting DDH tuples is random self-reducible, meaning, roughly, that if it is hard for even a

small fraction of inputs, it is hard for almost all inputs; if it is easy for even a small fraction of inputs, it is easy for almost all inputs.

Groups for which DDH is assumed to hold

When using a cryptographic protocol whose security depends on the DDH assumption, it is important that the protocol is implemented using groups where DDH is believed to hold:

- The subgroup of kth residues modulo a prime p, where $(p-1)/k$ is also a large prime (also called a Schnorr group). For the case of $k=2$, this corresponds to the group of quadratic residues modulo a safe prime.
- The cyclic group of order $(p-1)(q-1)$, where p and q are safe primes.
- A prime-order elliptic curve E over the field $GF(p)$, where p is prime, provided E has large embedding degree.
- A Jacobian of a hyper-elliptic curve over the field $GF(p)$ with a prime number of reduced divisors, where p is prime, provided the Jacobian has large embedding degree.

Importantly, the DDH assumption **does not hold** in the multiplicative group $\mathbb{Z}_p^*$, where p is prime. This is because given g^a and g^b, one can efficiently compute the Legendre symbol of g^{ab}, giving a successful method to distinguish g^{ab} from a random group element.

The DDH assumption does not hold on elliptic curves over $GF(p)$ with small embedding degree (say, less than $\log^2(p)$), a class which includes supersingular elliptic curves. This is because the Weil pairing or Tate pairing can be used to solve the problem directly as follows: given P,aP,bP,cP on such a curve, one can compute $e(P,cP)$ and $e(aP,bP)$. By the bilinearity of the pairings, the two expressions are equal if and only if $ab=c$ modulo the order of P. If the embedding degree is large (say around the size of p then the DDH assumption will still hold because the pairing cannot be computed. Even if the embedding degree is small, there are some subgroups of the curve in which the DDH assumption is believed to hold.

See also

- Diffie–Hellman problem
- Diffie–Hellman key exchange
- Computational hardness assumptions
- XDH assumption
- Decisional Linear assumption

References

- Dan Boneh, The Decision Diffie–Hellman Problem, ANTS 1998, pp. 48–63 [1] (http://crypto.stanford.edu/~dabo/abstracts/DDH.html) .