MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Separation between CDH and DDH). *Let $\mathbb{G}$ be a finite additive group of prime order q such that all elements $y \in \mathbb{G}$ can be expressed as multiples of $g \in \mathbb{G}$.*

- *Then the Computational Diffie-Hellman (CDH) problem is following. Given $x = a \cdot g$ and $y = b \cdot g$, find a group element $z = ab \cdot g$.*
- *Then the Decisional Diffie-Hellman (DDH) problem is the following. For any triple $x, y, z \in \mathbb{G}$, you must decide whether it is a Diffie-Hellman triple or not.*
- *The group $\mathbb{G}$ has a bilinear pairing $\langle \cdot, \cdot \rangle : \mathbb{G} \times \mathbb{G} :\rightarrow \mathbb{G}_*$ when following equalities hold*

$$\langle x_1 + x_2, y \rangle = \langle x_1, y \rangle \cdot \langle x_2, y \rangle$$
$$\langle x, y_1 + y_2 \rangle = \langle x, y_1 \rangle \cdot \langle x, y_2 \rangle$$

  and the pairing is efficiently computable and non-degenerate, i.e., $\langle g, g \rangle \neq 1$.

Prove that (t, ε)-CDH group with a bilinear pairing cannot be DDH group.

Solution.