# ElGamal加密方案的IND-CPA安全性证明

- DDH问题：给定一大素数$p$阶群$\mathbb{G}$, $g, g^a, g^b \in \mathbb{G}$.
  令$\beta \in \{0,1\}$为一个随机比特。若$\beta = 1$,令$Z = g^{ab}$; 若$\beta = 0$, 令Z为群$\mathbb{G}$中的一个随机元素。那么DDH问题就是：给定$(g, g^a, g^b, Z)$, 输出$\beta$的猜测$\beta'$. 若$|\Pr[\beta' = \beta] - 1/2| \geq \epsilon$, 则我们就说一个算法具有优势$\epsilon$解决群$\mathbb{G}$中的DDH问题。
- 若不存在$t$时间的算法能够以优势$\epsilon$来解决群$\mathbb{G}$中的DDH问题，则称群$\mathbb{G}$的DDH问题是$(t, \epsilon)$ 困难的。

**Theorem**

若群$\mathbb{G}$上的*DDH*问题是困难的，则*ElGamal*方案是*IND-CPA*安全的。

# 双线性映射

- $G$和$G_T$是两个阶为素数$p$的乘法循环群，$g$是$G$的生成元。
- 如果映射$\mathrm{e}: G \times G \to G_T$具有以下性质，则该映射是双线性映射。
  - 双线性：对于所有$a, b \in Z_p$，$g, h \in G$，都有$\mathrm{e}(g^a, h^b) = \mathrm{e}(g, h)^{ab}$
  - 非退化性：$\mathrm{e}(g, h) \neq 1$，即如果$g$和$h$是$G$的生成元，则$\mathrm{e}(g, h)$是$G_T$的生成元
  - 可计算性：对于所有$g, h \in G$，存在计算$\mathrm{e}(g, h)$的有效算法
- 双线性映射具有性质：
  - 对于所有$u_1, u_2, h \in G$，都有$\mathrm{e}(u_1 \cdot u_2, h) = \mathrm{e}(u_1, h) \cdot \mathrm{e}(u_2, h)$

# 困难问题假设

- 计算Diffie-Hellman问题（Computational Diffie-Hellman，CDH）
  - 给定$(g, g^a, g^b)$，计算$g^{ab}$，其中$a, b \in Z_p^*$。
- 判定Diffie-Hellman问题（Decisional Diffie-Hellman，DDH）
  - 给定$(g, g^a, g^b, g^c)$，判断$g^c \stackrel{?}{=} g^{ab}$，其中$a, b, c \in Z_p^*$。
- 计算双线性Diffie-Hellman问题（Computational Bilinear Diffie-Hellman，CBDH）
  - 给定$(g, g^a, g^b, g^c)$，计算$e(g, g)^{abc}$，其中$a, b, c \in Z_p^*$。
- 判定双线性Diffie-Hellman问题（Decisional Bilinear Diffie-Hellman，DBDH）
  - 给定$(g, g^a, g^b, g^c, Z)$，判断$Z \stackrel{?}{=} e(g, g)^{abc}$，其中$a, b, c \in Z_p^*$, $Z \in G_T$ 。