假设结论错误：BLS 签名算法 (Type III) 不是 EUF-CMA 安全的, 即存在一个敌手 $\mathcal{A}$, 在 CMA 安全模型中, 能够以不可忽略的概率攻破 EUF 问题.

证明前提错误：Type III 配对群上的 co-CDH 问题是困难的 + H 为 RO, 即存在一个敌手 $\mathcal{B}$, 以不可忽略的概率能够攻破 DL 问题.

通过攻破 EUF-CMA 问题的敌手 $\mathcal{A}$ 来构造攻破 co-CDH 问题的敌手 $\mathcal{B}$:

1. 首先挑战者生成 $PG = (G_1, G_2, G_T, p, g_1, g_2, g_T, e)$ 为 Type III 配对群;
2. 挑战者均匀随机选取 $x, y \leftarrow \mathbb{Z}_p$, 发送信息 $(PG, g_1^x, g_1^y, g_2^y)$ 给敌手 $\mathcal{B}$;
3. 若敌手 $\mathcal{B}$ 向挑战者发送 $g_1^{x \cdot y}$, 则挑战成功;
4. 敌手 $\mathcal{B}$ 将信息 $(PG, h = g_2^y)$ 作为公钥 PK 发送给敌手 $\mathcal{A}$;
5. 敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 发送若干 M_i 进行查询, 敌手 $\mathcal{B}$ 返回信息 $\sigma_i = Sign(SK, M_i)$. 因为敌手 $\mathcal{B}$ 没有私钥信息, 此时敌手 $\mathcal{B}$ 的策略为：随机均匀选取 $m_i \leftarrow \mathbb{Z}_p$, 令 $H(M_i) = g_1^{m_i}$, 再计算 $\sigma_i = H(M)^y = g_1^{ym_i} = h^{m_i}$ 发送给敌手 $\mathcal{A}$;
6. 敌手 $\mathcal{B}$ 向敌手 $\mathcal{A}$ 提供一个 RO 查询;
7. 敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 发送若干 M_i 进行哈希 RO 查询, 并存储对应的返回值 $H(M_i)$;
8. 敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 发起一次挑战, 发送信息对 (M^*, σ^*);
9. 由假设, 敌手 $\mathcal{A}$ 可以攻破 BLS 签名算法 (Type III) EUF-CMA 问题, 则敌手 $\mathcal{A}$ 可向敌手 $\mathcal{B}$ 提交的信息有不可忽略的概率满足关系：$e(H(M^*), h) = e(\sigma^*, g_2)$;
10. 此时敌手 $\mathcal{B}$ 的挑战策略;
11. 在敌手 $\mathcal{A}$ 发起 RO 查询时, 敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 发送信息 M_j 后, 向敌手 $\mathcal{B}$ 随机选择一次返回 g_1^x;
12. 此时敌手 $\mathcal{A}$ 有不可忽略的概率选中 M_j, 并解决问题, 那么此时 $\mathcal{B}$ 就得到了 $\sigma^* = g_1^{xy}$;
13. 敌手 $\mathcal{B}$ 向挑战者发送结果, 挑战成功.