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

1. 首先挑战者生成 (PK, SK), 并发送 PK 给敌手 $\mathcal{B}$:

   (a) 敌手 $\mathcal{B}$ 多次向挑战者发起多次查询, 并获得挑战者返回的信息 (R_i, e_i, z_i);

   (b) 敌手 $\mathcal{B}$ 向挑战者发起一次挑战, 提交一个 R^*, 挑战者返回 e^*;

   (c) 敌手 $\mathcal{B}$ 可再次向挑战者发起多次查询, 并获得挑战者返回的信息 (R_i, e_i, z_i);

   (d) 敌手 $\mathcal{B}$ 向挑战者发送 z^*, 其挑战成功的概率为 $Pr[g^{z^*} = h^{e^*} \cdot R^*]$;

2. 敌手 $\mathcal{B}$ 在与敌手 $\mathcal{A}$ 进行通信:

   (a) 敌手 $\mathcal{B}$ 将公钥 PK 发送给敌手 $\mathcal{A}$;

   (b) 敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 发送若干 M_i 进行签名查询. 因为敌手 $\mathcal{B}$ 没有私钥信息, 无法进行正确的签名, 故从挑战者返回的信息 (R_i, e_i, z_i) 中随机选择 e_i, 规约为 $e_i = H(R_i, M_i)$ 并向敌手 $\mathcal{A}$ 返回签名信息 $\sigma_i = (R_i, z_i)$;

   (c) 敌手 $\mathcal{B}$ 向敌手 $\mathcal{A}$ 提供一个 RO;

   (d) 敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 发送若干 (R_i, M_i) 进行 RO 查询, 并存储对应返回值 $H(R_i, M_i)$;

   (e) 由假设, 敌手 $\mathcal{A}$ 可以攻破 EUF-CMA 问题, 则敌手 $\mathcal{A}$ 可向敌手 $\mathcal{B}$ 提交信息 $(M^*, \sigma^* = (R^*, z^*))$, 且满足关系 $e^* = H(R^*, M^*), g^{z^*} = h^{e^*} \cdot R^*$. 显然 (R^*, M^*) 必为敌手 $\mathcal{A}$ 查询过的信息, 则其有多项式概率成功. 若没有查询过, 则敌手 $\mathcal{A}$ 成功概率仅为 $1/p$, 是可忽略的;

3. 此时敌手 $\mathcal{B}$ 的挑战策略:

   (a) 记敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 发起 RO 查询的次数为 Q, 敌手 $\mathcal{B}$ 从中随机抽取, 则有 $1/Q$ 的概率满足 $(R_i, M_i) = (R^*, M^*)$, 此时有 $e^* = H(R^*, M^*) = H(R_i, M_i)$. 此时敌手 $\mathcal{B}$ 将敌手 $\mathcal{A}$ 提交的 R^*, z^* 和敌手 $\mathcal{A}$ 查询过的 e^* 发送给挑战者便可以不可忽略的概率攻破其安全性.