Spring 2021-2022

CDH 问题困难 + H 为 RO

DHIES 算法（简化版 DHIES 算法）是 IND-CPA 安全的

2022 年 6 月 13 日

证明：由攻破 DS' EUF-CMA 安全性的敌手 $\mathcal{A}$ 构造攻破 DS EUF-CMA 安全的敌手 $\mathcal{B}$。

1. 挑战者执行 Gen 算法, 生成公私钥对 (pk, sk), 并将公钥发送给敌手 $\mathcal{B}$, 敌手 $\mathcal{B}$ 将公钥发送给敌手 $\mathcal{A}$.

2. 敌手 $\mathcal{A}$ 多次向敌手 $\mathcal{B}$ 发送 M_i 进行 oracle 查询. 敌手 $\mathcal{B}$ 收到信息后, 向挑战者发送 $H(M_i)$ 并将结果 σ_i 发送给敌手 $\mathcal{A}$.

3. 敌手 $\mathcal{A}$ 以不可忽略的概率攻破 EUF 问题向敌手 $\mathcal{B}$ 发送 $(M^* \ \sigma^*)$. 敌手 $\mathcal{B}$ 将信息对 $(H(M^*), \sigma^*)$ 转发给挑战者, 此时敌手 $\mathcal{B}$ 以不可忽略的概率攻破 DS EUF-CMA.