

实验 4: 区块链和共识协议

Lecturer: 钱宸 (Chen Qian)

免责声明: 该实验材料仅用于山东大学网络空间安全学院课程教学, 尚未经过通常用于正式出版物的审查。仅在获得讲师的许可的情况下, 可以在课堂外部分发。

4.1 实验说明

本次实验较短, 需要大家独立完成。截止日期为 1 月 8 日 23 点 59 分。

本次实验中所需要编写的协议中所用的签名算法可使用 RSA-FDH。哈希函数可以调用 python 的内置哈希函数。

4.2 Dolev-Strong 与区块链

问题 1: 在上一次实验中, 我们构造了 Dolev-Strong 共识协议。我们首先将上次的 Dolev-Strong 协议进行更改, 完成可以对多比特信息产生共识的 Dolev-Strong 协议。

在课堂中, 我们基于共识协议构造了最简单的区块链系统。

问题 2: 基于 Dolev-Strong 共识协议实现区块链系统。

4.3 Streamlet 区块链

问题 3: 基于 Streamlet, 实现简单的区块链系统。

我们在课堂上学到, 对于 streamlet 区块链而言, 如果只有小于 $\frac{n}{3}$ 个攻击者则该协议是安全的。

问题 4: 假设目前攻击者可以控制 $\frac{2n}{3}$ 个用户, 说明攻击者如何可以攻击协议。并编程实现该攻击。