**作业汇报**

一、成员

**姓名：高瑞凯 账户：GaoRuikai123**

二、项目简介

1.crypto analysis。在由您的姓名和学生ID组成的消息下查找哈希值为“sdu \_cst \_20220610”的键。例如，“San Zhan 202000460001”。

2.bitcoin。在比特币测试网上发送一个tx，并将tx数据解析到每一位，报告此推断技术在以太坊ECDSA中的应用

3.SM2。实现SM2解密和PGP方案

4.SM4。对SM4进行软件优化。

5.SM3。实现生日攻击、对SHA256进行长度扩展攻击、优化SM3

完成人：高瑞凯

三、项目清单

**完成的项目：**

1.在比特币测试网上发送一个tx，并将tx数据解析到每一位，最好自己编写脚本

2.报告此推断技术在以太坊ECDSA中的应用

3.实现SM2解密

4.使用SM2实施PGP方案

5.优化SM4

6.实施简化SM3的生日攻击方法

7.SHA256等实施长度扩展攻击。

8.尽最大努力优化SM3实施（软件）

**未完成项目：**

1.在一些k下找到一条64字节的消息，证明它们的哈希值是对称的。

2.伪造签名假装你是佐藤

3.使用概念验证代码验证上述pit FAL

4.实现RFC6979解密

5.通过真实的网络通信实现sm22P标志

6.使用真实网络通信实现sm22P解密

7.实施简化SM3的Rho方法

8.对SM3实施长度扩展攻击。

9.尝试实现这个-泛化哈希链

**问题项目：**

1.在由您的姓名和学生ID组成的消息下查找哈希值为“sdu \_cst \_20220610”的键。例如，“San Zhan 202000460001”。

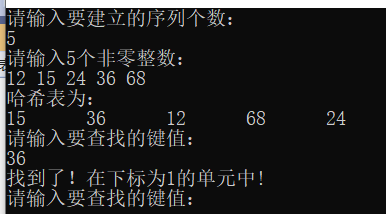
问题;消息只有学生ID

2.遵循RFC6962的Impl Merkle树。

问题：只建立了简单的Merkle树。

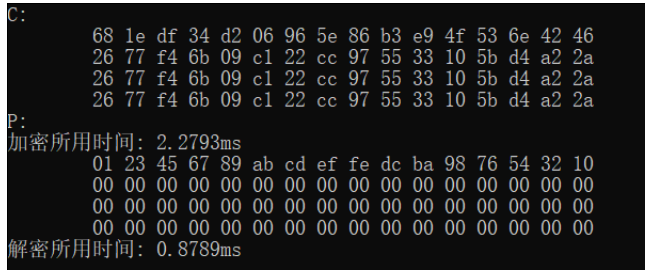
四、实验结果

**1.在由您的姓名和学生ID组成的消息下查找哈希值为“sdu \_cst \_20220610”的键。例如，“San Zhan 202000460001”。**

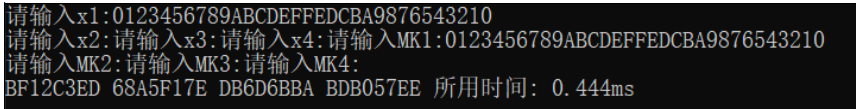


**2.优化SM4**

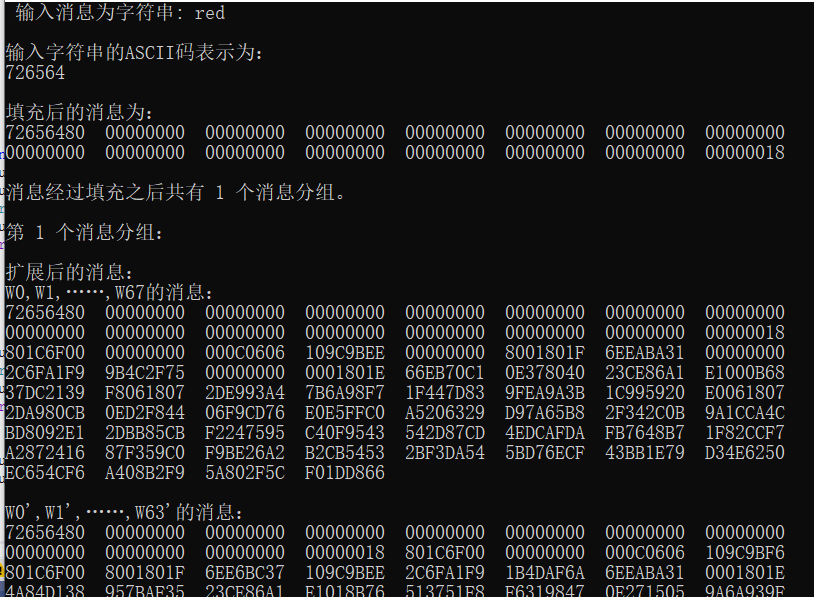
SIMD指令集

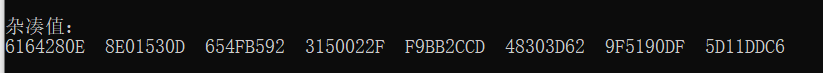
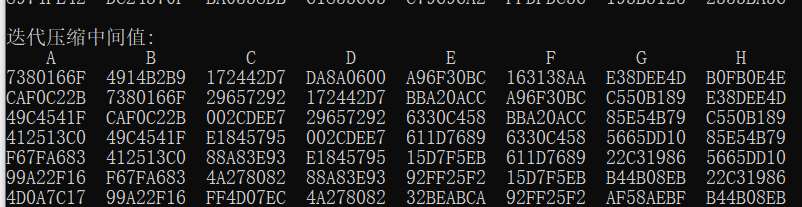


**流水线：**

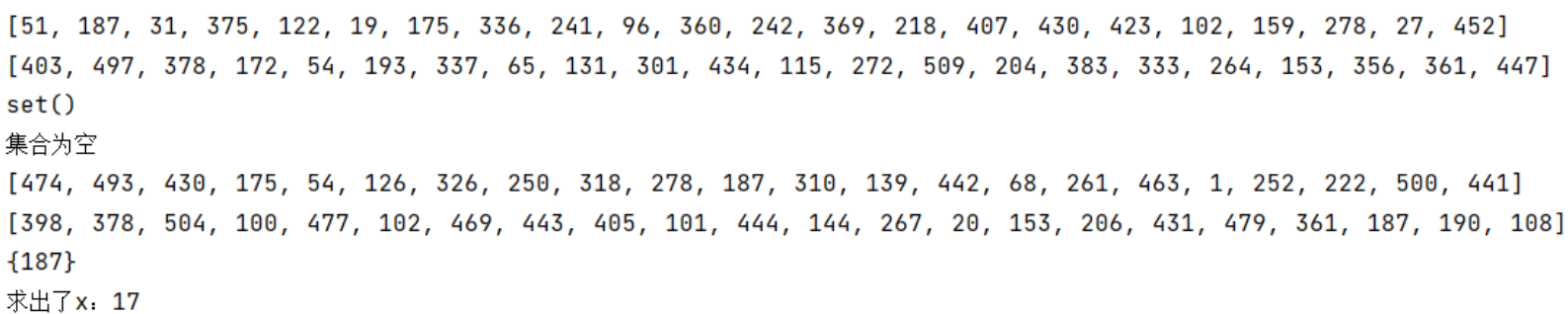
****

**3.优化SM3**





**4.生日攻击**



**5.merkle树**

