SHANDONG UNIVERSITY

密码工程第七次实验报告

姓名: 谢子洋
学院: 网络空间安全学院 (研究院)
专业: 网络空间安全
学号:202100460116

2023 年 11 月 29 日

目录

1 作业一

1.1 A

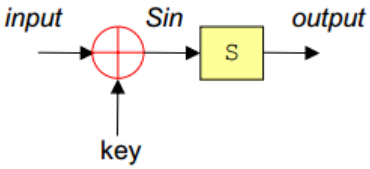
密码法哪一条款规定了关键基础设施需要使用密码技术进行保护?

第二十七条　法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。[1]

1.2 B

结合差分功耗分析的原理，完成下面密钥恢复。



input		Sin	Sbox		output	power
			in	out		
00		?	00	01	?	2
01	Key =?	?	01	10	?	0
10		?	10	11	?	1
11		?	11	00	?	1

图 1: 差分攻击

若以 S 盒的功耗与输入输出的汉明距离有关, 则可功耗应只存在两种情况, 与事实不符所以不成立.

因此本文以 S 盒输出的汉明重量作为衡量功耗的方式, 并进行如下推导. 排除矛盾的情

power	Sout	Sin	input	$key := input \oplus Sin$
2	11	10	00	10
0	00	11	01	10
1	10/01	01/00	10	11/10
1	01/10	00/01	11	11/10

表 1: 推导表

况, 密钥应 10.

2 作业二

2.1 Q1

下图为 AES 算法的功耗曲线，其中上图代表了 AES 整体运算，下图表示细节运算，请简述 ABCDEFGH 所代表的操作。

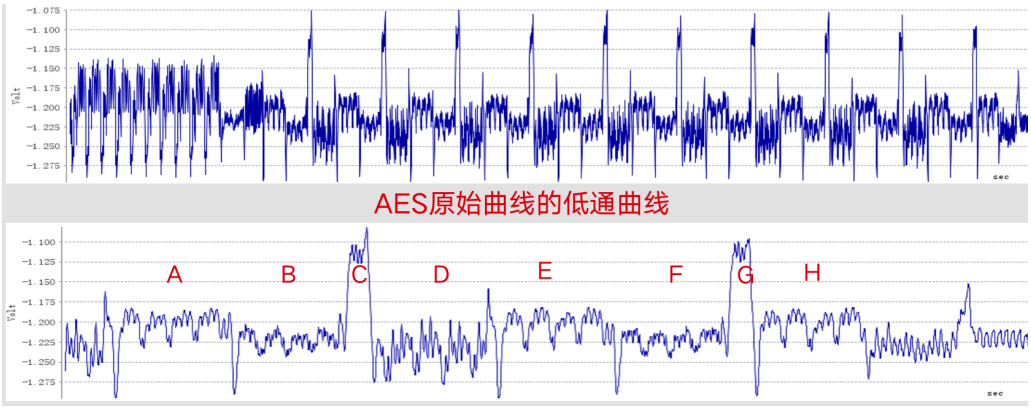


图 2: AES 功耗曲线

我们可观察到 D 在两次轮函数中只出现了一次, 因此我们可以判断 D 为 MixColumn, 且图中为最后两轮轮函数. 根据功耗曲线的最高峰部分为 C, 我们可以判断 C 为 SubBytes. 易证 AES 加密轮函数中 SubBytes 步骤和 ShiftRows 步骤可以调换顺序, 因此可猜测 B 为 ShiftRows 步骤. 所以 A 和 E 均为 AddRoundKey 步骤. 最后补全所有的对应步骤如下:

A:AddRoundKey

B:ShiftRows

C: SubBytes

D: MixColoum

E: AddRoundKey

F: ShiftRows

G: SubBytes

H: AddRoundKey

2.2 Q2

请概述密码应用的主要领域，包含数据要素应用中的典型场景.

(1) 物联网数据安全. 在物联网中，密码学可以提供设备之间的安全通信、认证和授权，以确保 IoT 设备及其数据的安全

(2) 网络通讯. 密码学被广泛应用于加密和认证，例如 TLS/SSL 协议用于加密网络数据传输.

(3) 电子支付. 在电子支付中, 使用密码学保证用户的隐私和身份认证.

(4) 保证大数据中个人隐私. 密码学中的安全多方计算, 隐私求交等方面保证在利用用户数据的同时不泄露个人隐私.

(5) 去中心化网络基础设施, 如区块链. 密码学技术被广泛应用于区块链中，例如比特币中的哈希函数和以太坊的智能合约等.

参考文献

[1] 人民日报. 中华人民共和国密码法 [EB/OL].(2019-10-28).[2023-10-20].https://www.oscca.gov.cn/sca/c100236/2019-10/28/content_1057345.shtml.