封面

诚信声明书

摘要

Abstract

目录

1. 绪论
   1. 研究背景及意义

随着智能设备的普及，设备的安全问题也受到更多的关注。可信执行环境（TEE）是Global Platform提出的概念，通过软硬件方法在中央处理器中构建一个安全区域，保证其内部加载的程序和数据在机密性和完整性上得到保护。具体原理是，将系统的硬件和软件资源划分为两个执行环境——可信执行环境（TEE）和普通执行环境(REE)。两个环境是安全隔离且并存的运行环境，有各自独立的内部数据通路和计算所需存储空间。TEE给REE的操作系统提供安全服务，它具有其自身的执行空间，比普通执行环境的操作系统的安全级别更高。同时普通执行环境的应用程序无法访问TEE，即使在TEE内部，多个应用的运行也是相互独立的，不能无授权而互访。TEE提供了安全和成本的平衡，能够满足大多数应用的安全需求。与MPC和FL纯软件的解决方案相比，TEE不会对隐私区域内的算法逻辑语言有可计算型方面的限制，支持更多的算子及复杂计算，可实现联合统计、联合查询、联合建模及预测等多种计算，业务表达性更强。同时，TEE支持多层次、高复杂度的算法逻辑实现，运算效率高。

针对于可信执行环境（TEE）的攻击一直是学术界的研究热点，能量侧信道分析（SCA）是其中一种攻击方法，通过分析物理设备的能量消耗恢复运行时使用的敏感信息，这些泄露的信息依赖于所处理的数据和执行的操作，因此可以通过这些信息进行分析来恢复密码信息。侧信道攻击可以利用的信息广泛，其中包括功率消耗信息、电磁辐射信息、温度、声音、电压等物理信息，侧信道攻击利用设备泄露出的信息，结合已知的信息可以建立模型，推断出密钥信息，同时这类攻击方法不会在设备及系统中留下痕迹，如果系统级芯片未采取保护措施，则可能只需要很小的代价就可以实现破解并获得密钥，故侧信道分析攻击方式成为破解密码芯片的可能的一条“捷径”，越来越受到学术界和工业界的关注。

Trustzone是Arm公司提出的一种可信执行环境，在Android系统中被广泛使用，例如高通的qcomsee，三星的trustonic，google目前的trusty 以及ARM Linaro的op-tee都是Trustzone上运行的系统。实际上是一个ARMv8的处理器上可以运行两个独立的操作系统，一个是运行在普通执行环境上的Linux，另外一个就是运行在可信执行环境之上的小内核，它结构简单，代码少，攻击面小，从而安全性得到了提高。然而，Trustzone仅被宣传为软件安全解决方案，而不是硬件层面的保护，目前微处理器还没有对于侧信道攻击的保护方案。本课题需要采集密码实现在Arm TrustZone中的能量侧信道泄露信息，具体来说，需要比较当AES加密在普通执行环境和可信执行环境上执行的能量泄露模式，探索Trustzone环境下侧信道攻击的复杂性以及攻击结果。

* 1. 国内外研究现状

侧信道分析技术的缘起可追溯到二战期间，当时研究人员发现密文设备通过电磁发射会泄露明文，二战结束之后一些机构开始尝试通过不同侧信道的分析方式对密文设备进行检测，发现大部分设备都无法抵抗侧信道分析。目前侧信道分析方式主要包括计时分析、能量分析、电磁分析等。

从国内外发展现状来看，目前国际上侧信道分析技术已经较为成熟，荷兰Riscure公司的Inspector平台和FI平台、法国Secure-IC公司的Smart-SIC Analyzer平台、日本RCIS研究中心的SASEBO开发板，均为业内公认的侧信道分析工具，国际上已多次出现商用芯片被侧信道分析技术破解的实际案例。2016年CT-RSA上，以色列特拉维夫大学Tromer团队展示了如何利用电磁攻击获得隔壁房间计算机中的信息。2017年，NXP公司的Wagner等人破解了竞争对手生产的一款通过了国际CC EAL5+安全认证的智能卡中的3DES算法。2018年1月，Intel处理器被爆出MeltDown和Spectre漏洞，该漏洞使云服务器可能遭受来自千里之外的侧信道缓存分析。

相比之下，我国在侧信道攻防领域的研究积累较少，力量薄弱，还处于发展的初级阶段。目前在侧信道攻防方面的研究主要集中在差分故障攻击、经典能量攻击、缓存攻击等方向，由于缺少先进的侧信道分析与测评技术、以及安全高效的抗侧信道分析防护对策，国产芯片难以通过国际CC EAL5+认证或得到国际认可，以致在我国近几年银行卡从磁条卡向智能卡过渡的过程中，暂时被进口芯片占据了绝大部分市场。

* 1. 研究内容和组织框架

第二章

第三章

第四章

第五章 实验效果

第六章 总结

致谢

参考文献