西安电子科技大学 计算机科学与技术 学院

本科生毕业论文（设计）开题报告

（2022届）

学生姓名 何开颜

专 业 计算机科学与技术

学 号 18030100178

指导教师 杨利英

2022年2月21日

（本表一式三份，学生、指导教师、学院各一份）

|  |
| --- |
| 一、论文名称及项目来源  针对 Arm Trustzone 环境的能量侧信道分析  课题组自行出题 |
| 二、研究目的和意义  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。攻击者可以通过测量设备进行加密操作时所释放出的能量信号如电磁信号，对加密密钥进行破解。为了保护敏感数据，防止重要数据泄露，新的安全技术如Arm TrustZone已经被开发出，但TrustZone仅被ARM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（Rich Execution Environment）和可信执行环境（Trusted Execution Environment）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。在实验中主要使用电磁（EM）侧信道泄漏分析，基于EM的侧信道分析的非接触性和空间灵活性意味着它是一种侵入性较低的采集手段，允许针对SoC上的特定区域（或组件）。 |
| 三、国内外研究现状和发展趋势  长期以来，侧信道攻击（SCA）的目标设备大多是智能卡、微控制器等，它们是带有关键信息的嵌入式设备，处理信息的速度相对较慢（低于10MHz），同时具有相对简单的架构，如简单的缓存架构。这些特点都使得侧信道攻击更加容易。因此，智能卡行业开发了一定的措施来防止诸如此类的物理攻击。  然而，在现代，越来越多的应用程序在智能手机上执行，其中使用的芯片是以高速运行（1GHz以上，比智能卡快100倍以上）的处理器，具有复杂的架构（多级缓存，深度管道）。因此，对这些芯片进行侧信道攻击是非常复杂的，因为测量设备必须能够在高频信号中获得准确的信号数据。由于缓存的存在，信号的抖动也使得同步化更加困难。然而，也有学者已经对智能手机进行成功的侧信道攻击。在[1]中，作者在安卓手机上开发了一种电磁分析技术(EMA)，以安卓BouncyCastle库中的AES实现的密钥为目标，展示了250条曲线的密钥恢复。  在[2,3]中，作者描述了如何在现代的高速系统中进行EMA。他们都运行在1GHz的Beaglebone Black板上。在实验中，他们必须过滤掉那些由于中断和其他操作系统的操作而不能正确同步的曲线。由此可以看出，对曲线的同步化和过滤是非常重要的。在[2]中，作者攻击了他们自己优化的AES，并得到了有效的攻击结果。在[3]中，Longo等人比较了ARM内核与NEON协处理器上的AES的泄漏情况,攻击了一个运行在JAVA ME下的SoC，利用EMA攻击了一个运行在Debian下的SoC，以提取AES密钥。  一部份学者在ARM TrustZone和TEE进行攻击，其中主要是软件攻击。在[5]中，Rosenberg利用QSEE（Qualcomm TEE）的一个安全漏洞，解锁了摩托罗拉智能手机的引导程序。在[6]中，Laginimaineb重定向了QSEE中的一些函数，使其能够在TEE内执行任意代码。也有学者对基于TEE的系统进行了物理攻击。在[7]中，Tang等人进行了一次故障攻击，以修改时钟和电压调节器的行为，违反时序约束，得以提取安卓和TEE上的AES密匙。在[8]中，Zhang等人在TEE上的软件AES加密时，通过探测缓存提取信息。在[9]中，Kevin等人在裸机上完成了EMA，以此来提取TEE中的密匙。  在智能手机上进行的第二类EMA的目标是公钥密码学（RSA [10,11] 或ECC [12]），这些攻击具有相同的泄漏原理，因为公钥密码学处理的都是大数字(RSA为3072位，ECC为256位)。在软件中处理这些大数字需要将它们分割成字，其大小由芯片结构决定（大多数架构为32位或64位）。例如，两个大数字的乘法需要在构成操作数的字上循环，由于循环是重复的迭代过程，具体的操作顺序可以通过分析频域特征获得泄漏特征，而频域中的泄漏与时钟频率相比，发生在一个相对较低的频率上。因此，攻击者可以通过与平方运算（RSA）或点加法与点加倍法（ECC）比较，识别大数乘法的泄露特征。  [1] Aboulkassimi, D., Agoyan, M., Freund, L., Fournier, J., Robisson, B., & Tria, A. (2011, November). ElectroMagnetic analysis (EMA) of software AES on Java mobile phones. In *2011 IEEE International Workshop on Information Forensics and Security* (pp. 1-6). IEEE.  [2] Balasch, J., Gierlichs, B., Reparaz, O., & Verbauwhede, I. (2015, September). DPA, bitslicing and masking at 1 GHz. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 599-619). Springer, Berlin, Heidelberg.  [3] Longo, J., Mulder, E. D., Page, D., & Tunstall, M. (2015, September). SoC it to EM: electromagnetic side-channel attacks on a complex system-on-chip. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 620-640). Springer, Berlin, Heidelberg.  [4] Rosenberg, D. (2013). Unlocking the motorola bootloader. *Azimuth Security Blog*.  [5] Laginimaineb, “Exploring qualcomm’s trustzone,” Bits, Please!, 2015.  [6] [Adrian Tang](https://dblp.uni-trier.de/pid/68/5424.html), [Simha Sethumadhavan](https://dblp.uni-trier.de/pid/46/652.html), [Salvatore J. Stolfo](https://dblp.uni-trier.de/pid/s/SalvatoreJStolfo.html): CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management. [USENIX Security Symposium 2017](https://dblp.uni-trier.de/db/conf/uss/uss2017.html#TangSS17): 1057-1074  [7] N. Zhang et al., “Truspy: Cache side-channel information leakage from the secure world on arm devices.,” 2016.  [8] Bukasa, S.K., Lashermes, R., Bouder, H.L., Lanet, J., & Legay, A. (2017). How TrustZone Could Be Bypassed: Side-Channel Attacks on a Modern System-on-Chip. *WISTP*.  [9] Genkin, D., Pachmanov, L., Pipman, I., & Tromer, E. (2015, September). Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation. In *International workshop on cryptographic hardware and embedded systems* (pp. 207-228). Springer, Berlin, Heidelberg.  [10] Uno, H., Endo, S., Hayashi, Y.I., Homma, N., Aoki, T.: Chosen-message electromagnetic analysis against cryptographic software on embedded OS. In: 2014 International Symposium on Electromagnetic Compatibility, Tokyo, pp. 314–317, May 2014  [11] Genkin, D., Pachmanov, L., Pipman, I., Tromer, E., Yarom, Y.: ECDSA key extraction from mobile devices via nonintrusive physical side channels. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS 2016, pp. 1626–1638. ACM, New York (2016) |
| 四、主要研究内容、要解决的问题及本文的初步方案  研究内容：本课题拟在Raspberry Pi 3B上配置TEE环境，在普通环境以及TEE环境中分别进行AES加密算法的实现，使用电磁探头采集在TEE中实现加密过程中的电磁曲线，并与普通环境中的密码实现过程进行比较，探索trustzone环境下的能量泄露模式。对电磁曲线利用相关能量分析（CPA）方法，对算法的密钥进行攻击恢复。本课题最终将比较两种不同环境下密码实现过程中，能量侧信道攻击的结果，探究trustzone环境对敏感数据在侧信道攻击中的保护作用。  待解决问题：完成Raspberry Pi 3B的系统及TEE环境配置，完成普通环境及TEE环境中进行AES密码算法的实现，利用电磁探头对加密过程进行电磁曲线采集与有效的处理，利用CPA对曲线进行密钥恢复。  初步方案：首先完成对Raspberry Pi 3B的系统及环境配置，使得AES算法能够在普通环境下和TEE环境下得到实现。其次使用电磁探头，对两种环境中算法实现时的电磁曲线进行采集，并对曲线进行数据处理。利用CPA对曲线进行处理，判断trustzone环境下密钥是否能通过侧信道攻击获取，以此探究trustzone环境对敏感数据在侧信道攻击中的保护作用。 |
| 五、工作的主要阶段、进度和完成时间  2021.12.1-2021.12.31：查阅文献，搜集资料，调研可信执行环境和侧信道分析的研究现状，对于课题相关理论知识进行学习。  2022.1.1-2022.1.31：学习CPA的代码框架，对现有数据集进行模拟攻击  2022.2.1-2022.2.28：配置Raspberry Pi 3B的系统及环境  2022.3.1-2022.3.31：采集普通环境与TEE环境中AES算法实现时的电磁曲线并进行数据的初步处理  2022.4.1-2022.4.30：对曲线进行CPA分析，探究是否能恢复密钥  2022.5.1-2022.5.31：实验数据整理，论文书写，准备论文答辩。 |
| 六、已进行的前期准备工作  查阅相关文献和材料调研了目前可信执行环境和侧信道分析的研究现状，对于该课题的研究及系统的构建有了初步的想法与方案，对于系统中所需用到的Raspberry Pi等软硬件也进行了一定的接触，对于该课题所需涉及到的理论基础知识也进行了学习。  七、指导教师意见  本课题具有一定的研究意义及应用场景，并且可以同时锻炼学生软硬件结合使用的能力，所以同意开题。  签名  2021年 12 月22日 |
| 1. 学院审核意见   签名  年 月 日 |