

一种基于随机指令延迟的抗旁路攻击处理器结构

李 红^{1,2}, 贺章擎³, 徐元中³

(1 湖北工业大学 计算机科学与技术学院, 湖北 武汉 430068;

2 华中科技大学 计算机科学与技术学院, 湖北 武汉 430074;

3 湖北工业大学 太阳能高效利用湖北省协同创新中心, 湖北 武汉 430068)

摘 要: 提出了一种基于随机延迟的高效的抗旁路攻击处理器结构, 综合采用随机指令调度、随机指令注入和随机流水段延迟技术以抵抗旁路攻击. 基于 ARM7 处理器实现了该架构, 实现结果表明本处理器比原始 ARM7 处理器增加了约 20% 的硬件面积. 通过相关系数分析攻击(Correlation Power Analysis, CPA)实验证明, 采用本架构的处理器具备有极高的抗旁路攻击防护能力, 可以应用在 USBKEY、智能卡(Smart CARD)等高安全应用场合.

关键词: 旁路攻击; 随机延迟; 随机指令调度; ARM7

中图分类号: TP391

文献标识码: A

文章编号: 1000—7180(2016)05—0006—04

An Efficient Processor Architecture to Resist Side Channel Attacks

LI Hong^{1,2}, HE Zhang-qing³, XU Yuan-zhong³

(1 College of Computer Science and Technology, Hubei University of Technology,
Wuhan 430068, China; 2 School of Computer Science and Technology, Huazhong

University of Science and Technology, Wuhan 430074, China; 3 Hubei Collaborative

Innovation Center for High-efficiency Utilization of Solar Energy,

Hubei University of Technology, Wuhan 430068, China)

Abstract: In this article, based on random delay insertion, an effective processor architecture resistant to side-channel attacks was proposed. It used a combination of randomized scheduling, randomized instruction insertion and randomized pipeline-delay to resist side-channel attacks. On the base of ARM7 processor, we implemented this architecture and the implementation results showed that this processor has increased approximate 20% in hardware area than the original ARM7 processor. The CPA attack experiment results suggested that our new secure processor have high capacity to resist side-channel attacks and thus could be used in USBKEY, Smart CARD and other application scenarios which require extremely high security level.

Key words: side-channel attacks; random delay; randomized scheduling; ARM7

1 引言

旁路攻击是近年来出现的一种针对嵌入式加密系统的攻击手段^[1]. 它的出现, 使攻击者可以绕过传统的数学安全理论, 利用密码算法执行过程中泄露的旁路信息(执行时间、功耗、电磁辐射等)来直接破解密钥, 危及到了密码算法的理论基础. 研究人员利用旁路攻击技术先后破解了几乎所有曾被认为牢不

可破的加密算法, 在信息安全领域引起了巨大震动.

对此, 研究人员提出了各种防护机制来抵抗旁路攻击, 比较典型的包括随机掩码(Masking)^[2-3], 采用非确定性处理器(non-deterministic processing)^[4]、软件混淆(Shuffling)^[5], 以及功耗恒定逻辑单元与功耗平滑技术^[6-7]等. 但是以上防御技术往往会带来大量的防护开销, 同时防护效果也有限. 采用功耗恒定逻辑单元在一定程度上可以抵抗功耗攻

击,但与基于静态标准单元的实现相比,芯片面积和功耗大约增加一倍,但运算性能约下降为前者的一半.

随机时间延迟技术^[8-9]通过在密码算法中引入随机时间延迟,使得旁路攻击无法确定特定运算的执行时间点,从而增加统计分析的难度. 该技术容易实现,且可以应用在各种算法中,对故障攻击、时间攻击、差分功耗攻击和高阶差分功耗攻击等都具有有一定的防护作用. 已提出的随机延迟技术包括采用多时钟、插入空指令、插入随机指令等. 但是,单一的随机延迟方法被证明存在局限. 研究表明,针对 DPA(Differential Power Analysis)攻击,插入随机时间延迟后,虽然单一的偏置尖峰分散为若干不同位置上的小尖峰,显著降低 DPA 攻击的信噪比,但是如果攻击者能够估算时间延迟可能出现的范围,也就是确定时间延迟窗口,那么通过分析这个时间窗口内的总功耗,能够有效提高 DPA 攻击的信噪比,使得随机延迟技术失效^[10].

为了克服现有技术的缺点与不足,本文提出了一种新的基于随机指令延迟的抗旁路攻击安全处理器架构,通过综合采用随机指令调度、随机指令注入和随机流水段延迟技术,能极大地提高处理器抗旁路攻击的能力,避免因旁路信息的泄露而导致密码算法被破解.

2 基于随机指令延迟的抗旁路攻击处理器架构

2.1 随机指令延迟技术抵抗旁路攻击的原理

本文以功耗攻击为例,来分析随机指令延迟技术抵抗旁路攻击的原理. 当前集成电路大都采用 CMOS 电路实现,而 CMOS 电路的功耗是与输入和输出的翻转状态直接相关的. 对于处理器来说,其执行某条指令的功耗曲线与操作数的值直接相关,因此攻击者就有可能通过功耗曲线推导出操作数的值从而分析出密钥. 例如,假设某个加密运算包含 7 条指令(用 I 表示),图 1(a)列出了处理器执行这 7 条指令的功耗曲线. 假设第 5 条指令(I5)的操作数与明文和部分密钥 k_i 相关,那么处理器在执行 I5 时刻的功耗也与明文和部分密钥 k_i 相关. 攻击者可以不断改变明文的值并执行多次运算,获取每个明文在 I5 时刻点对应的功耗,再通过统计分析从而破解未知密钥 k_i .

如果在指令执行过程中随机打乱指令的执行顺序,或者插入一些无效指令(用 R 表示),便会打乱

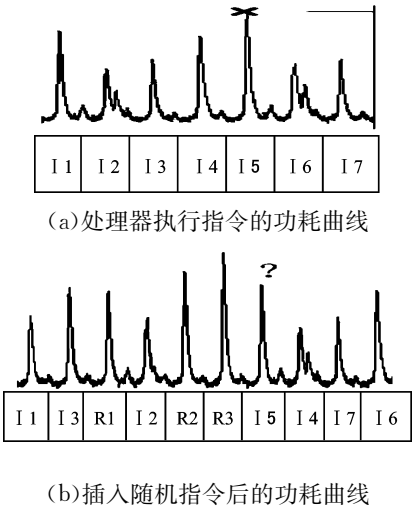


图 1 功耗曲线

正常指令的执行时序,使 I5 的执行时刻发生随机变化,如图 1(b)所示. 当攻击者不断改变明文进行加密运算时,攻击者难以精确获取 I5 时刻点的功耗进行统计分析,极大地增加了旁路攻击的难度,从而有效起到抗旁路攻击的作用.

2.2 处理器架构

本文所提出的抗旁路攻击处理器架构如图 2 所示. 该处理器架构包括指令随机调度模块、随机指令注入模块、随机流水段延迟模块、中央处理单元、随机数产生模块、指令存储器和数据存储器.

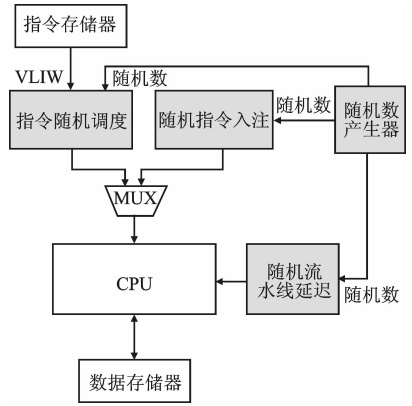


图 2 基于随机指令延迟的抗旁路攻击处理器架构

其中,指令随机调度模块能够随机调度多个可并行执行的指令并乱序发射;随机指令注入模块能在正常指令执行过程中产生一些随机实际指令并随机的发射到中央处理单元执行;随机流水段延迟模块能够对中央处理单元内部的流水段操作单元进行单周期内随机延时控制;片内随机数产生模块则产生真随机数供各个模块使用. 详细的内部结构原理图如图 3 所示.

综合后的面积为 36 185 等效门,而原始 ARM 核的面积为 30 081 等效门,硬件面积增加了 20.3%.

为了验证本处理器架构的防护效果,本文采用 Matlab 和 C 语言基于文献构建了 CPA 攻击模型,分别在原始 ARM 核上和采用了本技术之后的安全 ARM 核上执行未加保护的高级加密标准算法(Advanced Encryption Standard, AES),并进行了攻击实验.实验结果如表 1 所示.

表 1 攻击实验结果

执行平台	等效门	硬件开销	延时开销	所需样本数
ARM7	30 081	0	0	50
Secure-ARM7	36 185	20.3%	14.8%	>50 000

实验中,将电路综合后的门级网表经过 Model-Sim 软件电路仿真后得到攻击实验的 VCD 文件,进而用 Synopsys 公司 PrimePower 工具进行功耗仿真.通过随机改变明文执行 AES 加密运算从而获取对应的功耗样本,得到的功耗轨迹曲线可以认为是真实测量结果的无噪声近似.攻击时,选择 AES 算法首轮 S 盒输出的低 8 位作为中间值,采用汉明重量功耗模型进行功耗建模,然后分别对 256 个可能的子密钥所对应的汉明重量模型曲线与实际测得功耗曲线进行相关性分析,获取不同采样点的相关系数曲线.如果在某些特定采样点,某个猜测密钥对应的相关系数明显高于其他密钥对应的值,该密钥即为正确密钥.采用同样的攻击方式,可以获取其余的子密钥直至破解全部密钥.

图 4 列出了全部 256 猜测子密钥在中间值产生时刻点的相关系数随着样本量变化的曲线.其中图 4(a)是攻击原始 ARM 核上执行的 AES 算法的曲线,图 4(b)是攻击在本文所提出安全处理器上执行的 AES 的曲线.从中可以看出,对于在原始 ARM 核上执行的 AES 算法,样本数为 10 时,在特定攻击点的正确密钥对应的相关系数已经明显高于其他猜测密钥,50 条样本曲线足以破解 8 位子密钥(成功率接近 1),这证明旁路攻击技术具有极高的效率.而在采用随机指令注入技术之后,在平均时间开销约为 15% 的情况下,超过 5 万条样本量仍无法成功破解密钥(图 4b).证明本技术具有极高的防护效果.

4 结束语

本文提出了一种综合采用随机指令调度、随机指令注入和随机流水段延迟技术的安全处理器防护架构,并在 ARM7 实现了该架构.攻击实验结果表

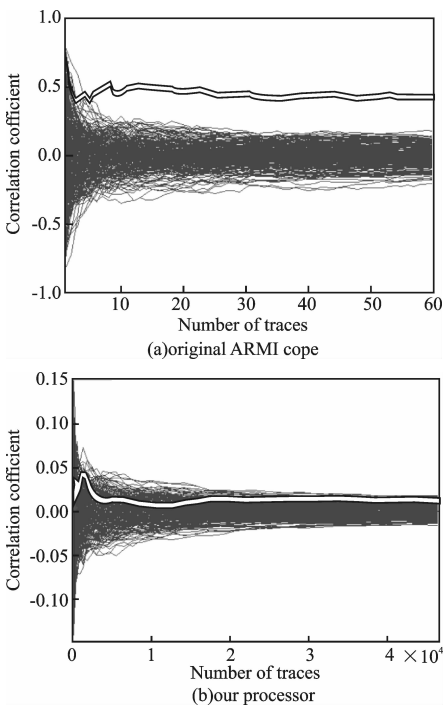


图 4 在原始处理器和安全处理器上分别对 AES 算法进行 CPA 攻击的结果对比

明,采用本架构的处理器具备有极高的抗旁路攻击防护能力,可以应用在 USBKEY、智能卡等高安全应用场合.另外需要指出的是,对于一些资源受限的应用,可以单独采用本文提出的任一种防护策略,以便在安全性和系统开销这两方面取得较好的平衡.

参考文献:

[1] Mangard S, Oswald E, Popp T, et al. Power analysis attacks;revealing the secrets of smart cards[M]. Berlin, Springer, 2007.

[2] Messerges T S, Dabbish E A. Examining smart-card security under the threat of power analysis attacks[J]. IEEE Trans. Comput,2002,51(5):541-552.

[3] Rivain M, Prouff E. Provably secure higher-order masking of AES[C]// CHES 2010, LNCS. American, Santa Barbara,2010,413-427.

[4] May D, Muller H L, Smart N P. Non-deterministic Processors[C]// Proc. 6th Australasian Conference on Information Security and Privacy. Australia, Sydney, 2010(219):115-129.

[5] Charvillan N V, Medwed M, Kerckhof S, et al. Shuffling against side-channel attacks a comprehensive study with cautionary note[C]// ASIACRYPT 2012, LNCS. Beijing,2012;740-757.

漂移布线的线长结果显示,时钟抽象拓扑树结构的改变减小了总的连线长度。

4 结束语

本文提出了一种对三维抽象拓扑时钟树结构优化的 LMOR 算法,通过调整特定子树根节点的位置得到一棵结构更优的拓扑树。实验结果表明 LMOR 优化算法能够将总的连线长度和时钟延迟分别最多减小 4.56% 和 14.67%,而时钟树的零漂移性质并没有改变。

参考文献:

- [1] Pan X, Xie J, Wang Q, et al. Noise aware clock tree synthesis for 3D ICs[C]// Solid-State and Integrated Circuit Technology (ICSICT), 2014 12th IEEE International Conference on. China, Guilin, IEEE, 2014; 1-3.
- [2] Minz J, Zhao X, Lim S K. Buffered clock tree synthesis for 3D ICs under thermal variations[C]//Proceedings of the 2008 Asia and South Pacific Design Automation Conference. Soul, IEEE Computer Society Press, 2008; 504-509.
- [3] Kim T Y, Kim T. Clock tree embedding for 3D ICs [C]// Design Automation Conference (ASP-DAC), 2010 15th Asia and South Pacific. Taiwan, Taipei, IEEE, 2010; 486-491.
- [4] Zhao X, Lim S K. Power and slew-aware clock network design for through-silicon-via (TSV) based 3D ICs[C]//Proceedings of the 2010 Asia and South Pacific Design Automation Conference. Macao, IEEE

Press, 2010; 175-180.

- [5] Kim T Y, Kim T. Clock tree synthesis for TSV-based 3D IC designs [J]. ACM Transactions on Design Automation of Electronic Systems (TODAES), 2011, 16 (4): 11-21.
- [6] Zhao X, Minz J, Lim S K. Low-power and reliable clock network design for through-silicon via (TSV) based 3D ICs [J]. Components, Packaging and Manufacturing Technology, 2011, 1(2): 247-259.
- [7] Jackson M A B, Srinivasan A, Kuh E S. Clock routing for high-performance ICs[C]//Design Automation Conference, 1990. Proceedings. 27th ACM/IEEE. USA, California, IEEE, 1990; 573-579.
- [8] Edahiro M. A clustering-based optimization algorithm in zero-skew routings[C]//Proceedings of the 30th international Design Automation Conference. New York, ACM, 1993; 612-616.

作者简介:

钱 晨 男,(1990-),硕士.研究方向为大规模集成电路设计. E-mail:qianchenorange@gmail.com.

王 琴 女,(1975-),博士,副教授.研究方向为大规模集成电路设计、片上处理器体系结构、先进集成电路设计方法。

谢 憬 男,(1981-),助理研究员.研究方向为大规模集成电路设计、片上处理器体系结构、先进集成电路设计方法。

毛志刚 男,(1962-),博士,教授,博士生导师.研究方向为大规模集成电路设计、可重构体系结构设计、集成电路与元器件可靠性等。

(上接第 9 页)

- [6] Ratanpal G B, Williams R D, Blalock T N. An on-chip signal suppression countermeasure to power analysis attacks[J]. IEEE Trans. Depend. Secure Comput, 2004,1(3):179-189.
- [7] Tiri K, Hwang D, Hodjat A, et al. A side-channel leakage free coprocessor IC in 0.18 μ m cmos for embedded AES-based cryptographic and biometric processing [C] // Proc. IEEE/ACM Design Automa. Conf. New York, 2005;222-227.
- [8] Coron J S, Kizhvato I. An efficient method for random delay generation in embedded software[C]// CHES 2009, LNCS. Switzerland, Lausanne, 2009;156-170.
- [9] 贺章擎,敖天勇,刘恺,等. 基于随机指令注入的抗旁

路攻击硬件防护技术[J]. 华中科技大学学报(自然科学版),2014,42(5):128-132.

- [10] Clavier C, Coron J S, Dabbous N. Differential power analysis in the presence of hardware countermeasures [C] // Cryptographic Hardware and Embedded Systems-CHES2000. Berlin, Heidelberg, Springer, 2000.

作者简介:

李 红 女,(1981-),博士研究生,讲师.研究方向为计算机系统结构. E-mail:lilyhong420@126.com.

贺章擎 男,(1980-),博士,副教授.研究方向为信息安全与集成电路设计。

徐元中 男,(1974-),副教授.研究方向为嵌入式系统设计。