

基于主成分分析的指令旁路模板分析方法

吴恒旭^{1,2}, 陈开颜¹, 邓高明¹, 张 鹏¹, 邹 程¹

(1 军械工程学院 计算机工程系, 河北 石家庄 050003; 2 成都军区 78086 部队, 四川 成都 610000)

摘 要: 提出一种微控制器指令逆向恢复方法. 根据微控制器内执行的指令与功耗、电磁等旁路信号之间的相关性, 为不同指令分别构建旁路模板, 将未知指令的旁路轨迹与模板进行匹配来恢复指令. 为解决旁路轨迹中样本点数量较大, 导致的模板构建与匹配效率较低的问题, 利用主成分分析 (PCA) 的方法从功耗轨迹中提取旁路信号主成分. 实验结果显示, 在约 400 个样本点中选取约 30 个分量的相同条件下, PCA 方法获得的匹配正确率比人工选取有效点方法提高近 50%.

关键词: 逆向工程; 指令恢复; 旁路模板分析; 主成分分析

中图分类号: TP39

文献标识码: A

文章编号: 1000-7180(2011)03-0144-05

Principal Component Analysis in Retrieve Instructions with Side Channel Template

WU Heng-xu^{1,2}, CHEN Kai-yan¹, DENG Gao-ming¹, ZHANG Peng¹, ZOU Cheng¹

(1 Department of Computer Engineering, Ordnance Engineering College, Chengdu 050003, China;

2 Chengdu Military Area Commands Unit 78086, Chengdu 610000, China)

Abstract: An method of instruction retrieve is proposed for microcontroller, which can takes the advantage of the relationship between instructions executed in microcontroller and the side channel leakages such as power consumption and electromagnetic emissions, builds side channel templates for instructions and matches the side channel trace from an unknown instruction to retrieve the operation. However, there are usually so many points in a side channel trace that the compute efficiency is very low. An interest component selection method with principle components analysis (PCA) is proposed to select interest components from side channel trace. With about 30 components selected from about 400 sample points, the correct matching ratio gained by PCA is about 50% higher than that by selecting points artificially.

Key words: reverse engineering; instruction retrieve; side channel template analysis; PCA

1 引言

近年来旁路攻击 (Side Channel Attacks, SCA) 方法^[1], 绕过对各种密码算法烦琐的数学分析, 通过对密码芯片泄漏的功耗^[2]、电磁等旁路信息的分析, 获取密码芯片的相关秘密信息, 模板分析^[3-4]更是旁路攻击研究的重点. 最近, 旁路模板的方法开始运用于逆向工程领域^[5]. 结合逆向工程的思想, 运用模板分析的方法对微控制器指令执行时的旁路泄漏信号建立模板, 逆向微控制器所运行的秘密算法, 可以获

取微控制器所运行的程序指令并分析其代码.

文中利用 CMOS 门电路的功耗旁路泄漏信号, 在分析功耗泄漏与指令相关性的基础上, 以 AT89C52 微控制器指令作为指令分析实例, 并将主成分分析方法应用于功耗轨迹的有效点选取, 大大的提高了指令判别成功率.

2 基于旁路模板的指令分析

2.1 微控制器指令旁路泄漏相关性

微控制器中寄存器的基本结构单元就是 CMOS

收稿日期: 2010-04-23; 修回日期: 2010-06-20

基金项目: 国家自然科学基金项目 (60940019); 军械工程学院原始创新基金 (YSCX0903)

反相器,根据微控制器芯片功耗泄漏机理(参见文献[6]),CMOS反相器的功耗与其发生翻转的概率有关.因此微控制器芯片在某个时刻总的功耗与该时刻发生翻转的反相器个数相关.微控制器指令的功耗泄漏特征与指令的操作及数据具有相关性.

图1显示的是微控制器在执行指令“MOV A, R3”时,功耗轨迹上某个特定时刻的功耗值随赋值的操作数(R3)的汉明重量增大而减小.图2显示的是执行两个不同的单周期指令序列并采集对应的功耗轨迹,第一个序列为两个不同的操作(NOP和ADD A, R3),对应图2的虚线轨迹;第二个序列为两个相同的操作(NOP和NOP),对应图2的实线轨迹.将两条功耗轨迹作差得到差分轨迹(图2下方轨迹)可以看出,当指令相同时(左半部分)差分轨迹趋近于0,当指令不同时(右半部分)差分轨迹出现明显波动.对微控制器中不同的指令要用到不同的寄存器,因而会产生不同的功耗泄漏特征,这就为利

用功耗泄漏恢复指令代码提供了可能.

2.2 统计模板分析技术

在模板分析攻击中,攻击者通过被完全控制的设备,对所有可能的指令构建模板,然后用同样的方法在被攻击的设备运行时获取一组旁路信号,并将之与已构建好的模板相匹配.统计模板分析攻击由两个步骤组成:

(1) 指令模板构建阶段

为了将功耗曲线按不同的指令分类,需要预先为每个可能的指令都构建一个模板.该模板反映了和指令对应的功耗曲线的统计特性,也就是说模板反映了曲线上所有点的概率分布的特性.

由于指令执行的各状态期受到地址、累加器、数据等因素的影响,造成不同的指令可能表现出相似的功耗特征.假设芯片指令集有 r 条指令,每条指令由于地址、累加器、数据等因素而造成的影响因子数目为 c ,因此需要为所有可能的指令构建 $r \times c$ 个模

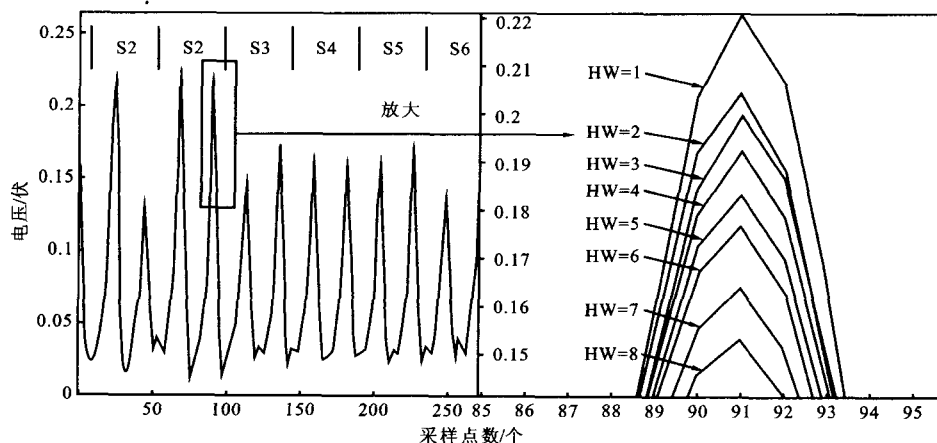


图1 指令功耗数据相关性

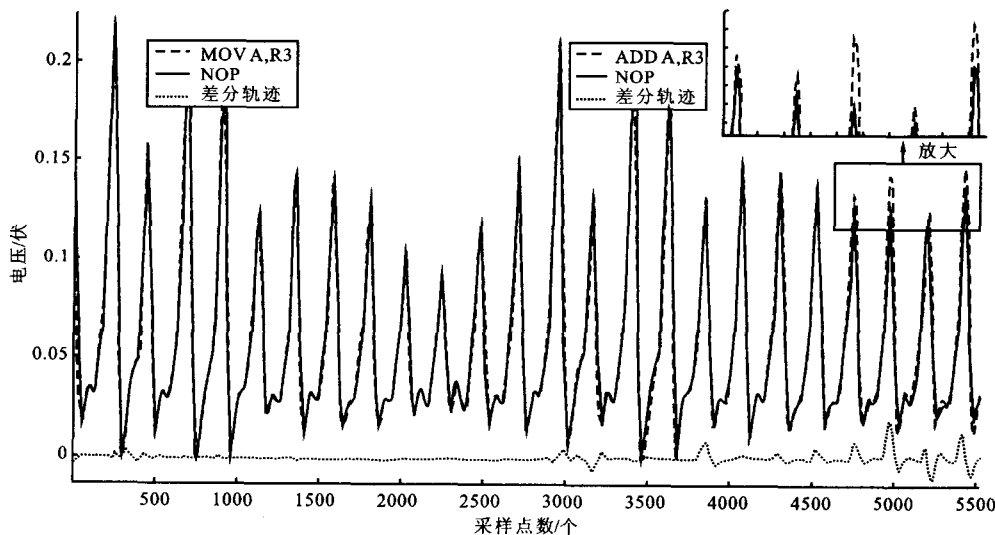


图2 指令功耗的操作相关性

板. 用每个指令对同一个影响因子运算 m 次, 并获取对应的 m 条功耗曲线, 每条曲线有 n 个采样点, 即 $t_{i1}, t_{i2}, \dots, t_{in} (1 \leq i \leq m)$. 这样, 功耗曲线样本组成了一个矩阵 $t_{m \times n}$, 对应的均值向量计算如下:

$$\bar{t} = \langle \bar{t}_1, \bar{t}_2, \dots, \bar{t}_n \rangle = \langle \frac{1}{m} \sum_{i=1}^m t_{i1}, \frac{1}{m} \sum_{i=1}^m t_{i2}, \dots, \frac{1}{m} \sum_{i=1}^m t_{in} \rangle \quad (1)$$

因为所有的曲线都是从同一个操作获取的, 存在的随机噪声用样本与样本均值作差的方法求得. 某个指令的训练样本曲线, 对应的噪声矩阵 $N_{m \times n}$ 为:

$$N_{m \times n} = \begin{bmatrix} t_{11} - \bar{t}_1 & t_{12} - \bar{t}_2 & \dots & t_{1n} - \bar{t}_n \\ t_{21} - \bar{t}_1 & t_{22} - \bar{t}_2 & \dots & t_{2n} - \bar{t}_n \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} - \bar{t}_1 & t_{m2} - \bar{t}_2 & \dots & t_{mn} - \bar{t}_n \end{bmatrix} \quad (2)$$

矩阵中的每一行组成了一条功耗样本曲线的噪声向量, 每一列是反映该时间点的噪声的一个随机变量.

用协方差来描述两个随机变量之间的线性相关性, 两个随机变量 N_i 和 N_j 之间的协方差通过下式计算:

$$\text{cov}(N_u, N_v) = \frac{1}{m-1} \sum_{k=1}^m (t_{ku} - \bar{t}_u)(t_{kv} - \bar{t}_v) \quad (3)$$

为了描述两个以上随机变量之间的协方差, 需要一个协方差矩阵. 噪声信号的协方差矩阵定义如下:

$$C_{n \times n} = \begin{bmatrix} \text{cov}(N_1, N_1) & \text{cov}(N_1, N_2) & \dots & \text{cov}(N_1, N_n) \\ \text{cov}(N_2, N_1) & \text{cov}(N_2, N_2) & \dots & \text{cov}(N_2, N_n) \\ \vdots & \vdots & \ddots & \vdots \\ \text{cov}(N_n, N_1) & \text{cov}(N_n, N_2) & \dots & \text{cov}(N_n, N_n) \end{bmatrix} \quad (4)$$

因此, 一个模板定义为一个 2 元组:

$$T = \langle \bar{t}, C \rangle$$

为了创建这样一个模板, 需要采集大量的功耗曲线样本. 显然, 曲线样本量越大模板就越精确.

(2) 指令模板匹配阶段

通过一个被完全控制的芯片完成了所有指令模板的构建后, 用被攻击的芯片对模板构建阶段中用到的指令进行运算, 并采集对应的芯片运行时的功耗曲线 t' , 与先前构建好的模板进行比较. t' 与模板 $\langle \bar{t}, C \rangle$ 匹配的概率可通过式(5)求得. 根据极大似

然法则, 概率最大的就是匹配得最好的模板, 其对应的指令就是最可能匹配正确的指令.

$$p(t', \langle \bar{t}, C \rangle) = \frac{1}{\sqrt{(2\pi)^m |C|}} \exp\left(-\frac{1}{2}(t' - \bar{t})^T C^{-1} (t' - \bar{t})\right) \quad (5)$$

2.3 AT89C52 芯片指令周期分析

文中以 AT89C52 微控制器芯片为例说明统计模板分析方法. AT89C52 芯片一个机器周期包含 6 个状态期(12 个振荡周期), 每个状态周期划分为 2 个节拍, 分别对应 2 个节拍时钟振荡期间.

在 AT89C52 芯片指令系统中, 根据各种操作的繁简程度其指令可由单字节、双字节和三字节组成; 从执行指令的时间上来看可以分为单周期、双周期和四周期, 只有乘除法指令占四周期. 图 3 显示的是单周期指令的取指和执行时序. 由图可知在每个机器周期内, 地址锁存控制 ALE 两次有效, 第一次出现在 S1P2 和 S2P1 期间, 第二次出现在 S4P2 和 S5P1 期间.

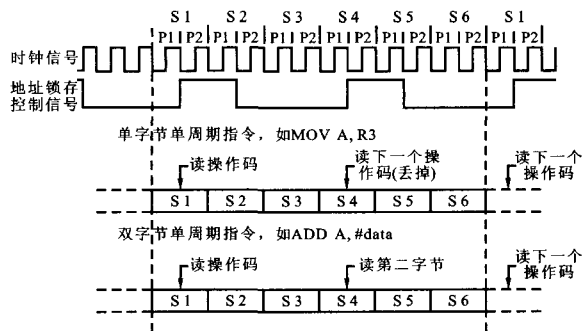


图 3 典型单周期指令执行时序

2.4 统计模板分析实验

由于指令在执行过程中不仅受到操作特性的影响, 还受到许多诸如地址、累加器、寄存器等因素的影响. 诸多因素的叠加使得同一指令在不同条件下各状态期呈现出不同的功耗轨迹, 若要为每个指令在所有条件下的功耗轨迹都构建一个模板, 会造成指令模板库过于庞大, 指令模板匹配的正确率低、工作量大.

在实际分析过程中, 由于一条功耗曲线中样本点可能较多(n 可达到 10^3 到 10^6), 可以从中选取部分和指令操作相关的有效点(interesting points)组成功耗信号样本. 选取指令机器周期 S1, S2 状态期功耗轨迹波谷的部分点作为有效点建立模板, 可以分辨单周期与双周期(见图 4(a), 双周期指令第二机器周期 S1, S2 状态期功耗轨迹波谷部分有明显尖峰); 选取指令机器周期 S4 状态期功耗轨迹波

峰的部分点作为有效点建立模板,可以作为单周期单字节指令与双字节指令区分依据(见图 4(b),单字节指令在机器周期 S4 状态期不做读操作,表现在功耗轨迹上明显比双字节指令低);单周期单字节指令周期中只有 S3 状态期受到指令本身的影响表现不同,可以选取其功耗轨迹上 S3 状态期波峰的部分点作为有效点.

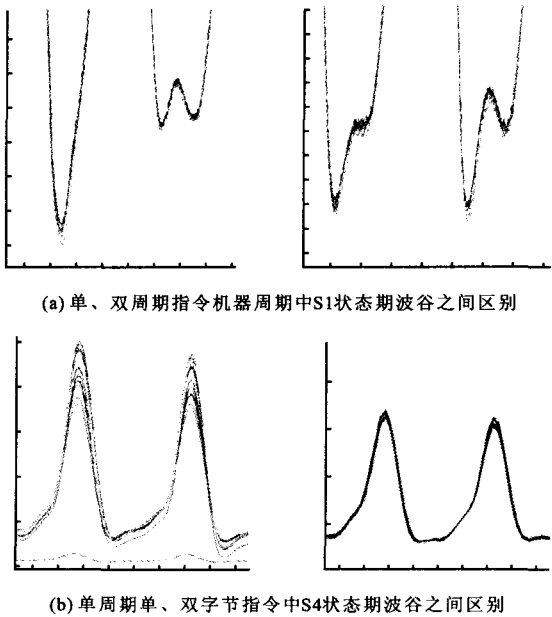


图 4 指令功耗轨迹上部分典型特征

选取 37 条单周期单字节指令功耗轨迹进行指令模板分析.按照本节所述方法选取 S3 状态期 441 个点中 30 个点建立模板,根据模板创建及匹配方法各进行 100 次匹配,实验结果如表 1 所示.

表 1 有效点简单选取匹配实验结果

指令	识 别								正 确 率
	I ₁	I ₂	I ₃	I ₄	...	I ₃₅	I ₃₆	I ₃₇	
I ₁	16	2	2	2	...	14	1	1	16%
I ₂	0	22	2	2	...	22	1	1	22%
I ₃	1	0	32	2	...	12	0	0	32%
I ₄	1	4	5	22	...	7	2	2	22%
...	...	...	...	...	...	...	...	...	...
I ₃₅	0	0	0	0	...	76	0	1	76%
I ₃₆	2	1	1	2	...	13	8	2	8%
I ₃₇	2	2	1	2	...	28	0	13	13%

3 主成分分析

从实验匹配结果可以看出,由于选取的有效点更接近第 35 条指令的特征,使得其他指令被识别成第 35 条指令几率较高.主成分分析^[7]为有效点选取

提供了一个科学的方法,能够在不丢失主要信息的前提下把数据维数降到最低.

3.1 主成分分析原理

主成分分析是一种常用的线性映射方法,即用它构造的每个新特征都是原有特征的线性函数.设 $X_1, X_2, \dots, X_p$ 为某实际问题所涉及的 p 个随机变量.记 $X = (X_1, X_2, \dots, X_p)^T$,其协方差矩阵为

$$\Sigma \triangleq (\delta_{ij})_{p \times p} \triangleq E[X - E(X)][X - E(X)]^T \tag{6}$$

它是一个 p 阶半正定矩阵.设 $l_i = (l_{i1}, l_{i2}, \dots, l_{ip})^T (i = 1, 2, \dots, p)$ 为 p 个常数向量,考虑如下线性组合

$$\begin{cases} Y_1 \triangleq l_1^T X = l_{11}X_1 + l_{21}X_2 + \dots + l_{p1}X_p \\ Y_2 \triangleq l_2^T X = l_{12}X_1 + l_{22}X_2 + \dots + l_{p2}X_p \\ \dots \\ Y_p \triangleq l_p^T X = l_{1p}X_1 + l_{2p}X_2 + \dots + l_{pp}X_p \end{cases} \tag{7}$$

则有

$$\begin{aligned} \text{Var}(Y_i) &= \text{Var}(l_i^T X) = l_i^T \Sigma l_i \\ i &= 1, 2, \dots, p \end{aligned} \tag{8}$$

$$\begin{aligned} \text{Cov}(Y_i, Y_j) &= \text{Cov}(l_i^T X, l_j^T X) = l_i^T \Sigma l_j \\ i &\neq j, i, j = 1, 2, \dots, p \end{aligned} \tag{9}$$

如果用 Y_1 代替原来 p 个变量 $X_1, X_2, \dots, X_p$,那么 Y_1 应尽可能反映原 p 个变量的信息.这里,“信息”用 Y_1 的方差来度量.由式(8)可知,必须对 l_i 加以限制,否则 $\text{Var}(Y_1)$ 无界,最方便的限制是要求所有 l_i 具有单位长度,即: $l_i^T l_i = 1$.在约束条件 $l_i^T l_i = 1$ 之下,求 l_1 使 $\text{Var}(Y_1)$ 达到最大,由此 l_1 所确定的随机变量 $Y_1 = l_1^T X$ 称为 $X_1, X_2, \dots, X_p$ 的第一主成分.

一般的,在约束条件 $l_i^T l_i = 1$ 及 $\text{Cov}(Y_i, Y_k) = l_i^T \Sigma l_k = 0$ 之下,求 l_i ,使 $\text{Var}(Y_i)$ 达到最大,由此 l_i 所确定的 $Y_i = l_i^T X$ 称为 $X_1, X_2, \dots, X_p$ 的第 i 个主成分.

3.2 基于主成分分析的有效点选取

同样选取 2.4 节所使用的 S3 状态期中 441 个点作主成分分析,计算后得出相关系数矩阵的特征值(Eigenvalue)、上下特征值之差(Difference)、各主成分的方差贡献率(Proportion)以及累积贡献率(Cumulative):

从表 2 可以看出,前 27 个主成分已经具有足够多的方差贡献率(两者累积方差贡献率为 97.7%),可以很好的概括这组数据.即原 441 个点可以用 $X = (\text{Prin1}, \text{Prin2}, \dots, \text{Prin27})$ 来表征,有效地降低了

数据维数.

表 2 主成分分析结果

	Eigenvalue	Difference	Proportion	Cumulative
1	210.747283	116.373990	0.4779	0.4779
2	94.373293	38.826544	0.2140	0.6919
3	55.546749	41.253150	0.1260	0.8178
4	14.293599	9.990312	0.0324	0.8503
	...			
27	1.478550	0.083004	0.0034	0.9770
	...			

使用主成分分析所得的 27 个点作为建立指令模板的有效点,重新指令模板分析实验,实验结果如表 3 所示.

表 3 主成分分析有效点选取匹配实验结果

指令	识别									正确率
	I ₁	I ₂	I ₃	I ₄	...	I ₃₅	I ₃₆	I ₃₇		
I ₁	63	1	1	0	...	4	2	1	63%	
I ₂	1	68	1	2	...	3	0	2	68%	
I ₃	1	0	78	1	...	3	0	0	78%	
I ₄	1	1	1	78	...	1	1	1	78%	
...	...	...	...	...	...	...	...	...	...	
I ₃₅	0	2	1	1	...	89	1	0	89%	
I ₃₆	1	0	0	0	...	5	62	2	62%	
I ₃₇	1	1	1	0	...	0	1	66	66%	

通过实验对比可以看出,使用主成分分析进行有效点选取可以大大提高指令模板识别率.

4 结束语

结合逆向工程思想和模板攻击原理,利用芯片功耗泄漏信号为芯片指令以及程序执行路径构建模板,将目标芯片上获取的旁路信号与模板进行匹配以推断芯片中执行的指令代码.通过对 AT89C52

单片机上运行单周期指令的指令模板分析试验,证明了旁路模板指令分析的可行性与有效性.并通过主成分分析提取有效点,极大提高模板匹配的效率.

参考文献:

[1] Paul Kocher. Timing attacks on implementations of dif-fie-hellman, RSA, DSS, and other systems[C]// Neal Koblitz. Advances in Cryptology, Proceedings Crypto '96, LCNS. New York: ACM, 1996:104-113.

[2] 张鹏,邓高明,邹程,等. 差分功率分析攻击中的信号处理与分析[J]. 微电子学与计算机,2009, 26(11): 1-4.

[3] Chari S, Rao J R, Rohatgi P. Template attacks[C]// Proceeding of the Workshop on Cryptographic Hardware and Embedded Systems (CHES'03). Cologne, Germa-ny: Computer Science, 2003:13-28.

[4] 邓高明,张鹏,赵强,等. 针对密码芯片的电磁模板分析攻击[J]. 微电子学与计算机,2010, 27(1): 1-4.

[5] Dennis Vermoen. Reverse engineering of Java Card ap-plets using power analysis [D]. Netherlands: TU Delft, 2007.

[6] Sung-Mo Kang, Yusuf Leblebici. CMOS 数字集成电路一分析与设计[M]. 王志功, 窦建华, 译. 北京:电子工业出版社,2005: 97-98.

[7] 梅长林,周家良. 实用统计方法[M]. 北京:科学出版社,2006:53-65.

作者简介:

吴恒旭 男,(1983-),硕士研究生.研究方向为信息安全.

陈开颜 女,(1970-),博士,硕士生导师.研究方向为信息安全.

邓高明 男,(1983-),博士研究生.研究方向为电磁信息检测与主动防护技术.

张 鹏 男,(1976-),博士研究生.研究方向为电磁信息检测与主动防护技术.

邹 程 男,(1982-),博士研究生.研究方向为电磁信息检测与主动防护技术.

(上接第 143 页)

[5] Ceze L., Tuck J., Cascaval C., et al. Bulk disambiguation of speculative threads in multiprocessors [C]// Proceedings of the 33st Annual International Symposium on Computer Ar-chitecture(ISCA'06). Boston: ACM, 2006.

作者简介:

时 磊 男,(1983-),博士研究生.研究方向为 VLSI 信号处理.