·网络空间安全· 文章编号：1000-3428(2020)06-0115-07 文献标志码：A 中图分类号：TP391

基于 FPGA 的时钟同步功耗信息采集方法

宋 安[1a]，王 琴[1a]，谷大武[1a]，郭 筝[1a,1b]，刘军荣[1a,2]，张 驰[1a]

（1. 上海交通大学 a. 电子信息与电气工程学院；b. 网络空间安全学院，上海 201100；
2. 智巡密码（上海）检测技术有限公司，上海 201100）

摘 要： 传统的异步采集方法会影响采集到的功耗信息的信噪比，降低功耗分析的成功率。针对异步采集的问题，提出一种新的时钟同步功耗信息采集方法。该采集方法基于现场可编程门阵列（FPGA）的时钟同步采集平台，利用基于 FPGA 时钟同步设备向待采集设备和示波器发送同步的时钟信号，使采集过程中的待采集设备与示波器的工作状态同步。在此基础上运用电气解耦原理，隔离外部信号对待采集设备的影响，改善功耗信息的信躁比。通过相关功耗分析进行实验验证，结果表明，该方法采集效率最高提升 66.7%，明显提高功耗分析的成功率。

关键词： 旁路攻击；功耗分析；现场可编程门阵列；时钟同步采样；电气解耦

开放科学（资源服务）标志码（OSID）：

中文引用格式： 宋安，王琴，谷大武，等. 基于 FPGA 的时钟同步功耗信息采集方法[J]. 计算机工程，2020，46(6)：115-121.

英文引用格式： SONG An，WANG Qin，GU Dawu，et al. FPGA-based collection method for power information of clock synchronization[J]. Computer Engineering，2020，46(6)：115-121.

FPGA-based Collection Method for Power Information of Clock Synchronization

SONG An[1a]，WANG Qin[1a]，GU Dawu[1a]，GUO Zheng[1a,1b]，LIU Junrong[1a,2]，ZHANG Chi[1a]

（1a. School of Electronic Information and Electrical Engineering；
1b. School of Cyber Science and Engineering，Shanghai Jiao Tong University，Shanghai 201100，China；
2. ZhiXun Crypto Testing and Evaluation Technology Co.，Ltd.，Shanghai 201100，China）

【Abstract】 Traditional asynchronous acquisition method affects the signal-to-noise ratio of collected power information information，resulting in a decrease in the success rate of power information analysis. To address the problem of asynchronous acquisition，this paper proposes a new power information collection method for clock synchronization. Based on the clock synchronization collection platform of the Field Programmable Gate Array（FPGA），this method uses clock synchronization based devices to send a clock signal of synchronization to the to-be-collected device and the oscilloscope，so that the to-be-collected device is synchronized with the working state of the oscilloscope. The principle of electrical decoupling is used to isolate the influence of external signals on the to-be-collected device，and improves the signal-to-noise ratio of the power consumption information. Through Correlation Power Analysis（CPA），result shows that the proposed method improves the collection efficiency by up to 66.7%，greatly improving the success rate of power analysis.

【Key words】 Side Channel Attacks（SCA）；power analysis；Field Programmable Gate Array（FPGA）；clock synchronous sampling；electrical decoupling

DOI： 10.19678/j.issn.1000-3428.0054936

0 概述

旁路攻击（Side Channel Attacks，SCA）是一种通过利用芯片泄露的物理信息并对其进行统计分析以获得芯片内部敏感信息的攻击方法[1]。旁路攻击主要手段为功耗分析，是通过采集密码系统运行时的功耗信息，并利用统计学和信号处理的方法找出数据中与密码算法执行有关的信息，再结合电路的运

基金项目： 闵行区中小企业技术创新计划“基于区块链技术的金融业务平台”（2018MH110）。

作者简介： 宋 安（1995—），男，硕士研究生，主研方向为旁路攻击；王 琴，副教授；谷大武，教授；郭 筝，博士；刘军荣，博士研究生；张 驰，博士。

收稿日期： 2019-05-16 **修回日期：** 2019-07-03 **E-mail：** 2832577601@qq.com

行特征进行密钥破解[2]。功耗分析是旁路攻击研究的核心内容,而功耗采集则是功耗分析的基础[3]。

传统的采集方法是用示波器对待测芯片进行异步采集,即示波器的采集时钟与待测芯片的时钟完全独立[4],示波器的采集时钟一般使用内置的高频时钟,待测芯片的工作时钟来源于晶振,因此采集时钟和待测芯片工作时钟之间存在不稳定的相位差。由于待测芯片多数在时钟边沿执行密码运算,传统的异步采集方法很难完全采集到待测芯片的密码操作相关信息。为了得到充足的时钟边沿信息,传统的异步采集方法需要增大示波器的采样频率,但同时获得了大量冗余信息,增加了旁路分析的复杂度。此外,传统异步方法采集的功耗信息的触发时间是不对齐的,这极大地增加了旁路分析的时间成本。由文献[5]可知,异步采集的功耗信息使得功耗分析难以完成。

针对以上问题,文献[4]通过弯曲的磁线对待测芯片的功耗进行采集,尝试获得精准的功耗信息。文献[5]通过电源注入的方法强制使内部振荡器的频率锁定于外部时钟的频率。文献[6]设计了包含锁相环(Phase Lock Loop,PLL)的放大滤波电路,尝试恢复出待测芯片内部的工作时钟。然而,以上研究存在着明显局限性:测评者需要熟悉待测芯片泄露功耗的电路,精确定位功耗泄露的采集位置,这是一项复杂且难度很高的工作[4];目前多数芯片使用稳定的晶振作为时钟源,无法与外部时钟锁定,且未进行后续的旁路采集和功耗分析验证,缺乏实验支撑[5];由于存在放大和滤波通路,恢复出的时钟会随着待测芯片原本的工作时钟的变化而产生不稳定的相位延时[6]。此外,文献[4,6]的方法需要在专用的采集平台(如 Chipwhisper 硬件[7])上实现,可供选择的测评参数有限,并不适用于实际的测评。

为改善以上问题,需要一种通用的采集方法和采集平台,既可大幅提升功耗分析的成功率,又能广泛地应用在实际的测评中。为此,本文提出一种基于 FPGA 的时钟同步功耗信息采集方法。

1 基于 FPGA 的时钟同步设备的硬件实现

现场可编程门阵列(Field Programmable Gate Array,FPGA)具有速度快、效率高、组成形式灵活以及内部时延小的特点,可以大幅提升系统对信号的响应和处理时间,并且能进行现场设计、编程等,在高速数据处理方面起到了关键作用[8]。因此,本文选用 FPGA 进行硬件实现,设计了基于 FPGA 的时钟同步设备,为数字示波器和待测设备提供状态同步、相位可调、频率可变、驱动能力强的时钟信号。基于 FPGA 的时钟同步设备具有以下优势:

1)FPGA 内部时钟资源非常丰富,可构建稳定的多时钟系统,内部产生的时钟信号可通过众多的时钟管脚引出。

2)FPGA 内置锁相环模块,内部时钟的频率和相位可调,测评者可根据需求自行调节,以满足各种功耗信息采集场景的需求。传统的采集方法中测评者难以控制待测设备和示波器的时钟频率和相位差。然而在基于 FPGA 的时钟同步采集系统下,测评者可方便配置待测设备和示波器的时钟频率和相位,来获得更高信噪比的功耗曲线,以达到最佳的采集效果。

3)FPGA 可拓展性强。待测设备和示波器对外部信号的驱动能力有一定要求,若外部信号电平过低或不稳定会造成驱动不足的问题。本文采用的 FPGA 开发板的 I/O 管脚电平为 3.3 V,且封装良好,满足待测设备和示波器对外部信号驱动能力的要求。

在本文的采集方法中,基于 FPGA 的时钟同步设备产生状态同步(即相位差稳定)的时钟 CLK1 和 CLK2,作为数字示波器的采集时钟,经过解耦电路后作为待测设备的工作时钟,然后进行后续的采集。

时钟同步设备的硬件实现如图 1 的虚线框所示。状态同步时钟产生的基本原理是:来自晶振的时钟经过锁相环电路产生多个输出时钟,全部存储到寄存器组中;多路电路选择寄存器组中的时钟后,经过缓冲电路、输出电路,由设备的 I/O 引出。

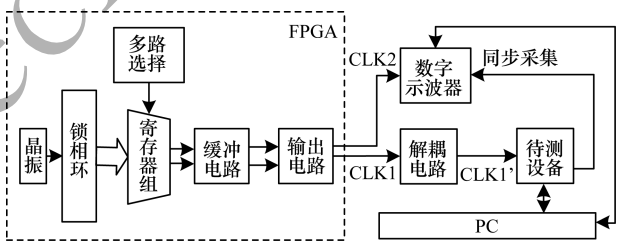

图 1 时钟同步采集系统

Fig. 1 Clock synchronization acquisition system

硬件的设计基于硬件描述语言 Verilog HDL,采用的 EDA 平台为 Xilinx 公司的 Vivado 套件[9],FPGA 开发板采用 Airtex-7 系列 FPGA 的 Basys3 开发板[10]。保证状态同步的时钟的正确产生是硬件设计的关键。硬件设计包含以下关键电路:

1)锁相环电路

若采用逻辑电路来产生时钟信号,时钟信号的相位将不稳定,且在实际的电路中会存在毛刺和抖动。然而,锁相环电路能很好地解决这一问题。锁相环电路不仅为 FPGA 提供灵活可变的时钟,还有

消除时钟抖动和抗时钟歪斜的作用。锁相环电路包括鉴相器、环路滤波器、压控振荡器、分频器等。首先鉴相器比较输入时钟和分频器的反馈时钟的相位和频率,产生比例信号。然后比例信号驱动环路滤波器,并把参考电压传输到压控振荡器,以此决定压控振荡器是否运行在更高或更低的频率[11]。

本文锁相环电路的实现调用了 Vivado 内置的 IP 核,在配置分频和倍频等参数后,得到多个频率的输出时钟。

2)多路选择电路

多路选择电路提供选择信号,用于控制产生不同频率和相位的时钟信号,保证了时钟信号的可调性。对于 Airtex-7 系列 FPGA,锁相环电路最多提供 6 个时钟输出,进入寄存器的多个时钟等待多路选择电路的控制信号,最后产生两个输出时钟。

多路选择电路的实现用到了累加器,每当外围电路的按键按下时,多路选择电路的选择信号就累加一次,将累加结果作为选择信号。

3)缓冲电路和输出电路

缓冲电路用于保证各电路之间时钟信号的正常驱动。输出电路的作用是将 FPGA 内部产生的时钟通过 I/O 引出。

缓冲电路调用了 Vivado 内置的 buffer 函数;输出电路调用了原语,在配置双倍数据速率输出(Output Double Data Rate,ODDR)电路参数后,实现了 FPGA 内部逻辑电平到输出模拟时钟的转换。

在完成基于 FPGA 时钟同步设备的硬件设计后,编译 Verilog 代码,并将编译后产生的比特流文件通过 JTAG 下载到 Airtex-7 FPGA 的 Basys3 中。用数字示波器对图 1 的 CLK1'(经过电气解耦后的 CLK1)、CLK2 信号进行检测,结果如图 2 所示。其中,C2 信道为采集参考时钟 CLK2,C3 信道为工作时钟 CLK1',其相位差稳定在 -1°~+1°范围内。

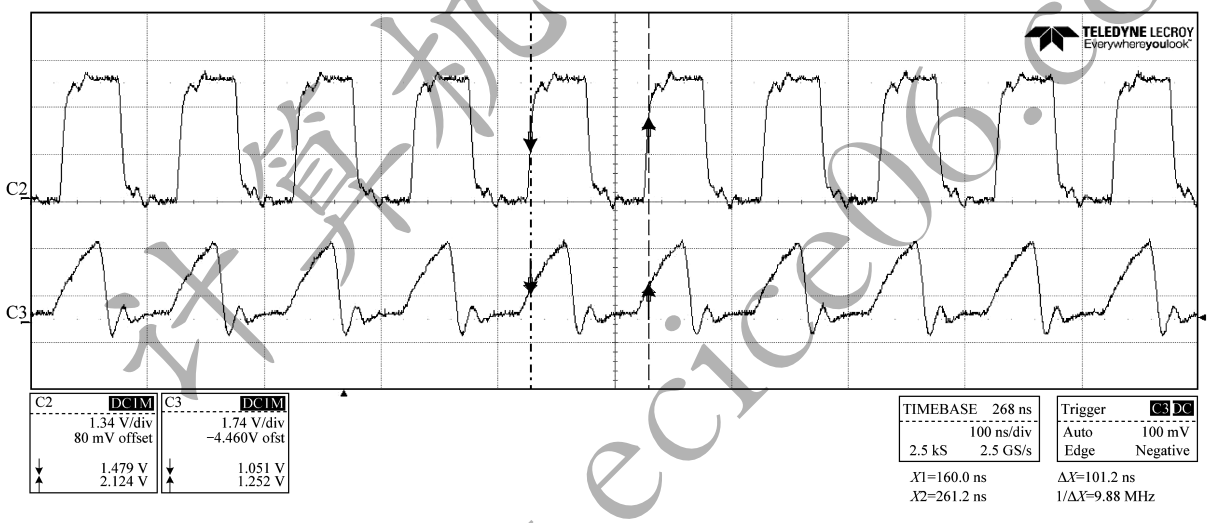

图 2　采样时钟与工作时钟

Fig. 2　Sampling clock and working clock

2　同步采集平台设计

本文选择专用安全 FPGA 芯片 SAKURA-G 作为待测设备。SAKURA-G 开发板用于硬件安全领域的研究和开发,如旁路攻击、故障注入攻击、物理不可克隆函数等[12]。

与传统采集方式相比,本文设计的同步采集方法主要在待测设备和示波器上体现差异。在传统方法异步采集时,待测设备的工作时钟来源于晶振,而在同步采集时,待测设备的工作时钟由基于 FPGA 的时钟同步设备提供并通过 SAKURA-G 上的 I/O 引脚引入。传统方法异步采集时,示波器一般使用内置的采集时钟,而在同步采集时,数字示波器的采集时钟由基于 FPGA 的时钟同步设备提供并通过示波器外部组件 WR6Zi-ExtRef-IN/OUT[13] 引入。该组件可以接受外部参考时钟,使内部采集时钟与外部参考时钟相位一致,且示波器内部采集时钟频率可任意调节,如图 3 所示。

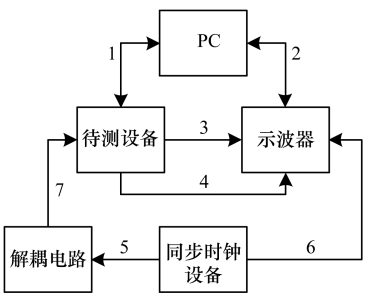

图 3　实验采集流程

Fig. 3　Experimental acquisition procedure

本文设计的同步采集步骤如下：

步骤 1 按照测评需求调节时钟频率的大小(由外围电路按键控制)，时钟同步设备产生 CLK1(序号 5)，经过解耦电路后的 CLK1'作为待测设备的工作时钟(序号 7)；时钟同步设备产生 CLK2，经过幅值调整后作为示波器的采集参考时钟(序号 6)。

步骤 2 PC 向待测设备发送明文(或密文)、随机数等指令，等待待测设备传回密文(序号 1)。

步骤 3 待测设备开始加密(或解密)，将触发信号传给示波器(序号 3)。

步骤 4 PC 向示波器发送采样率、触发延时、幅值分量等参数，等待示波器传回功耗曲线(序号 2)。

步骤 5 示波器对待测设备的功耗进行采集(序号 4)。

传统的异步采集方法包含序号 1～序号 4，最终采集到的功耗曲线信噪比较低。本文的同步采集在传统异步采集方法的基础上增加了序号 5～序号 7 部分，不仅实现了同步采集，还解决了噪声问题。按照设计的同步采集方法搭建采集平台，同步采集示意图如图 4 所示。

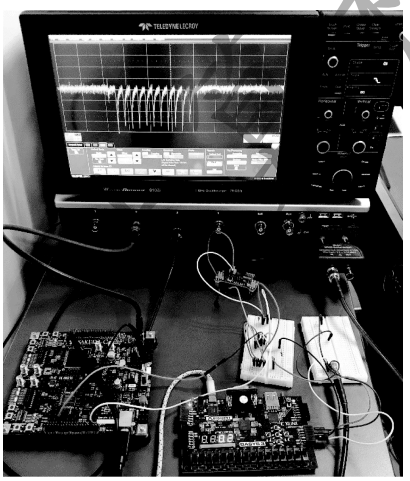

图 4 同步采集示意图

Fig. 4 Schematic diagram of synchronous acquisition

3 实验设计与分析

为验证本文提出的同步采集方法的效果，本文的实验设计主要基于相关功耗分析(Correlation Power Analysis，CPA)攻击。

3.1 CPA 攻击

CPA 是一种非建模类的功耗分析方法[14]。CPA 攻击由差分功率分析(Differential Power Analysis，DPA)[15]演变而来，在本文实验场景下，相比其他功耗分析方法，如 SPA[16]、TA[17]等，CPA 更加快速和有效。

本文以 AES 算法为例简要介绍 CPA 攻击过程。攻击者使 AES 密码设备运行 p 次加密运算，获得 p 条功耗曲线，记为 $\boldsymbol{T}=(t_1,t_2,\cdots,t_i,\cdots,t_p)$，$\boldsymbol{T}\in\mathbb{R}^{1\times p}$，并记录每条曲线对应的明文，记为 $\boldsymbol{D}=(d_1,d_2,\cdots,d_i,\cdots,d_p)$，$\boldsymbol{D}\in\mathbb{R}^{1\times p}$。假设的密钥为 $\boldsymbol{K}=(k_1,k_2,\cdots,k_j,\cdots,k_q)$，$\boldsymbol{K}\in\mathbb{R}^{1\times q}$，其中，$i\in[1,p]$，$j\in[1,q]$。

首先选择 AES 首轮 S 盒的输出 $\mathrm{Sbox}(d_i\oplus k_j)$ 作为中间值。d_i 与假设密钥 k_j 通过计算，得到假设的中间值矩阵 $\boldsymbol{V}=(v_{1,1},v_{1,2},\cdots,v_{i,j},\cdots,v_{p,q})$，$\boldsymbol{V}\in\mathbb{R}^{p\times q}$。然后将此假设的中间值通过功耗模型函数 $\boldsymbol{L}(\cdot)$ 映射为假设的功耗矩阵 $\boldsymbol{L}=(l_{1,1},l_{1,2},\cdots,l_{i,j},\cdots,l_{p,q})$，$\boldsymbol{L}\in\mathbb{R}^{p\times q}$。最后利用相关性函数 $\mathrm{Pr}(\cdot)$，将 $\boldsymbol{L}$ 与功耗曲线矩阵 $\boldsymbol{T}$ 进行相关性计算，相关性越大，假设的功耗和真实的功耗的匹配程度就越高。通过索引最大相关性的位置，即可找到与正确密钥最匹配的假设密钥 $\hat{k}$。CPA 攻击流程公式如下：

$$v_{i,j}=\mathrm{Sbox}(d_i\oplus k_j) \tag{1}$$

$$l_{i,j}=\boldsymbol{L}(v_{i,j}) \tag{2}$$

$$\hat{k}=\underset{k\in K}{\arg\max}\,|\mathrm{Pr}(\boldsymbol{L},\boldsymbol{T})| \tag{3}$$

3.2 无防护 AES 功耗曲线的 CPA 攻击

同步采集对异步采集的提升率计算公式可以表示为：

$$\delta=\frac{|C_s|-|C_a|}{|C_a|}\times 100\% \tag{4}$$

其中，C_s 表示异步功耗曲线的密钥相关性，C_a 表示同步功耗曲线的密钥相关性。

选择 10 000 条无防护的 AES 功耗曲线(待测芯片工作频率为 10 MHz)进行单字节功耗分析，分析平台为 Matlab[18]。图 5(a)给出示波器采样率为 25 MS/s时异步和同步采集的功耗曲线的密钥相关性示意图。灰色实线代表错误密钥的相关性，黑色虚线表示异步的正确密钥的相关性曲线，黑色实线表示同步的正确密钥的相关性曲线(图 5(b)、图 5(c)、图 5(d)的表示相同)。黑色虚线在时刻 45 附近出现了尖峰，最高相关性 -0.03 左右，但未与灰色实线区分开。黑色实线在时刻 45 附近产生了明显的尖峰，最高相关性提升至 -0.05，且泄露点数量增加。按照式(4)，同步采集的功耗分析的提升率 δ 为 66.7%。

图 5(b)给出示波器采样率为 100 MS/s 时异步和同步采集的功耗曲线的密钥相关性示意图。在时刻 255 附近，黑色虚线的最大相关性为 -0.10，而黑色实线的最大相关性提升到 -0.13，同步采集的提升率 δ 为 30%。

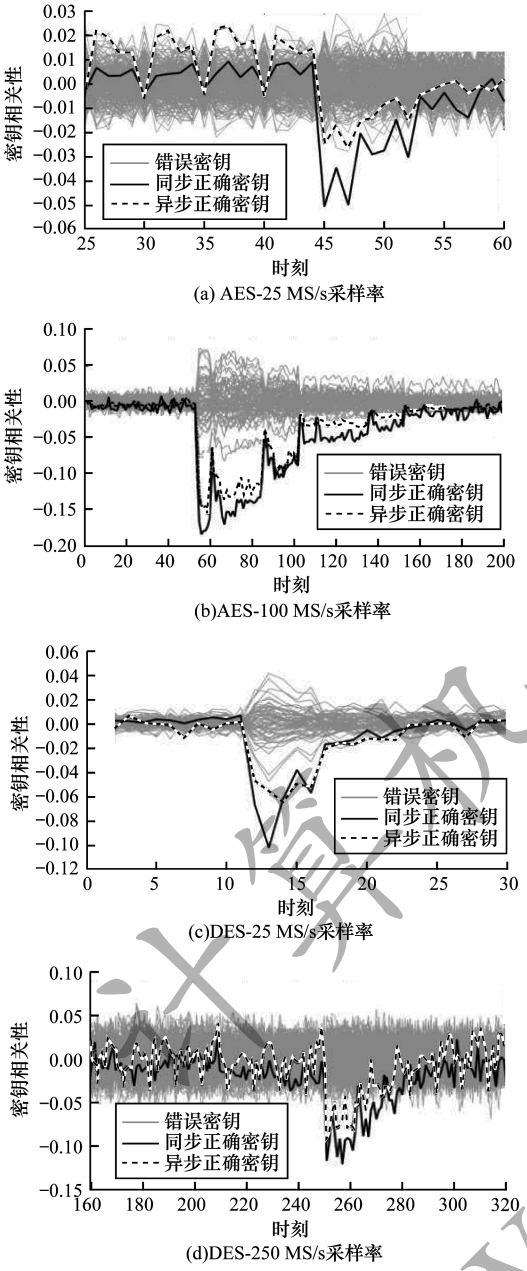

图 5　不同采样频率的 CPA 攻击结果

Fig. 5　CPA attack results at different sampling frequencies

3.3　带防护 DES 功耗曲线的 CPA 攻击

DES 的分析与 AES 类似,由于 DES 算法存在掩码防护,需要更多的功耗曲线。在此场景下,选择 150 000 条功耗曲线(待测芯片工作频率为 10 MHz)进行单字节功耗分析,分析平台为 Matlab。图 5(c)给出示波器采样率为 25 MS/s 时异步和同步采集的功耗曲线的密钥相关性示意图。黑色虚线的相关性最大值为 −0.075,黑色实线的相关性最大值达到 −0.10。按照最高相关性计算提升率,同步采集的功耗分析的提升率 δ 为 33.3% 。

图 5(d)给出了 250 MS/s 异步和同步采集的相关性示意图。黑色虚曲线最大相关性为 −0.16,且在时刻 105 和时刻 120 时与灰色实线有所重叠。黑色实线最大相关性提升到 −0.19,在时刻 105 和时刻 120 仍与错误曲线有很好的区分度,信息泄露更为明显。同步采集的功耗分析的提升率 δ 为 18.75% 。

3.4　结果分析

3.2 节、3.3 节分别对 AES 和 DES 进行单个字节的 CPA 攻击,本节将给出所有字节的 CPA 攻击的综合结果。

以图 5(b)中时刻 250 处的泄露点进行 CPA 分析为例(以 5(a)、图 5(c)、图 5(d)为例也能得到类似的结论),结果如图 6 所示。其中,横坐标表示功耗曲线数量,纵坐标表示密钥相关性,每一条曲线代表每一种假设密钥的相关性。

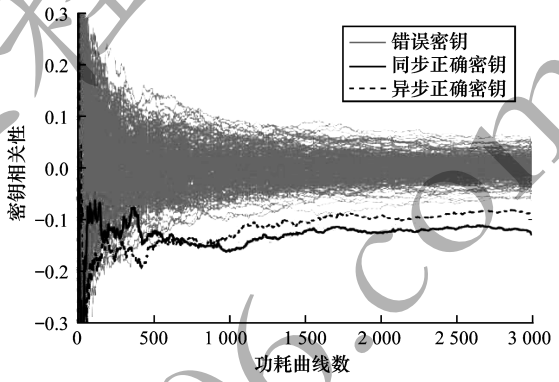

图 6　相关性与曲线数量的关系

Fig. 6　Relationship between correlation and number of curves

当功耗曲线数量较少时,虚线和实线都未能与灰色曲线区分;随着使用功耗曲线的数量增加,正确曲线的相关性与错误曲线区分增大。当功耗曲线数量达到 600 条时,正确密钥曲线开始与错误曲线区分,最终灰色曲线的相关性的收敛于 ±0.06,虚线的最高相关性为 −0.08,实线的最高相关性为 −0.12。

从图 6 还可以发现,虚线在曲线数量为 1 800 时与灰色曲线有重合部分,然而实线从 500 条开始就与错误曲线产生了良好的区分度。结果表明,本文采用的同步采集比异步采集更容易产生泄露,只需利用较少的功耗曲线即可攻击出正确密钥。

上文为单字节 CPA 分析,下面将剩余所有字节进行 CPA 攻击,统计攻击出所有正确密钥所需的曲线数如表 1、表 2 所示(考虑实验环境对功耗曲线的微小影响,表中曲线数为多次实验统计的近似结果)。其中,表 1 是未防护的 AES 算法的攻击结果,表 2 是带防护的 DES 算法的攻击结果。

表 1　未防护的 AES 的攻击结果

Table 1　Attack results of unprotected AES

采样率/(MS · s^{-1})	异步功耗曲线数	同步功耗曲线数	提升率/%
25	12 000	7 500	37.5
50	6 000	3 800	36.7
100	2 100	1 600	23.8
250	1 400	1 300	7.1

表 2 带防护的 DES 的攻击结果

Table 2 Attack results with guarded DES

采样率/(MS·s^{-1})	异步功耗曲线数	同步功耗曲线数	提升率/%
25	200 000	130 000	35.0
50	150 000	118 000	21.3
100	115 000	100 000	13.0
250	100 000	95 000	5.0

如表 1 所示,当示波器的采样率为 250 MS/s 时,同步采集的功耗分析提升率为 7.1% ,这是由于采样率远高于待测芯片工作时钟后,每条功耗曲线的泄漏点增多,异步采集的不良效应被稀释。然而,随着示波器采样率的降低,提升率迅速上升,在采样率为 25 MS/s 时产生了最佳的效果,同步采集相比异步采集减少了 37.5% 的功耗曲线数量。

表 2 与表 1 的结果类似。当示波器采样率为 250 MS/s 时,功耗曲线的 CPA 攻击提升率为5.0% 。随着示波器采样率的降低,提升率迅速上升,在采样率为 25 MS/s 时产生了最佳的效果,同步采样相比异步采样减少了 35.0% 的功耗曲线数量。

3.5 信噪比

在早期实验时发现采集过程中出现明显的噪声,这是由于待测芯片使用了外部时钟。较差的信噪比将影响功耗分析的成功率。下文讨论耦合噪声对功耗曲线的影响。

每条功耗曲线l_k都由 n 个功耗点组成,公式表达如下:

$$l_k = \{l_k(t) \in \mathbb{R} \mid t \in [1;n]\} \tag{5}$$

其中,$l_k(t)$为示波器在第 t 时刻采集的功耗点的值,它的大小由待测芯片中的密码算法产生的中间值 $\delta(t)$和噪声 ε 决定,即:

$$l_k(t) = \delta(t) + \varepsilon \tag{6}$$

其中,$\delta(t)$为 S 盒的输出产生的功耗,与明文和密钥 k 相关,ε 的大小独立于 $\delta(t)$,与外部设备的时钟频率相关(暂不考虑待测芯片内部的其他噪声)。在给定的场景中,功耗曲线l_k第 t 个点的信噪比的计算公式如下[19]:

$$\mathrm{SNR}(t) = \frac{\mathrm{Var}(\delta(t))}{\mathrm{Var}(\varepsilon)} \tag{7}$$

其中,Var(·)表示方差,Var($\delta(t)$)量化了可利用的信号造成的功耗点的变化大小,Var(ε)量化了由噪声导致的该点的变化。

为提升功耗曲线的信噪比,有以下两种减少 ε 的方法:1)为外部时钟设备提供高质量的稳压电源,把电源噪声的影响降至最低,但此方法对信噪比的改善不明显;2)对时钟信号进行电气解耦处理,屏蔽其对待测芯片的影响。

考虑成本和性能,本文使用高速光耦 6N137 作为信号隔离器[20]。光耦的输入端连接发光二极管,电信号驱动半导体发光器件发光,而接收端的光敏管将接收到的光信号转换为电信号输出。6N137 具备比普通光耦更快的速度和更强的驱动能力。将光耦元件应用在时钟同步设备输出端(如图 1 所示解耦电路的输入端),其电路如图 7 所示。其中,CLK1 代表输入端,CLK1' 代表输出端。调整电阻和电容的大小至最佳性能后,完成功耗曲线的采集。

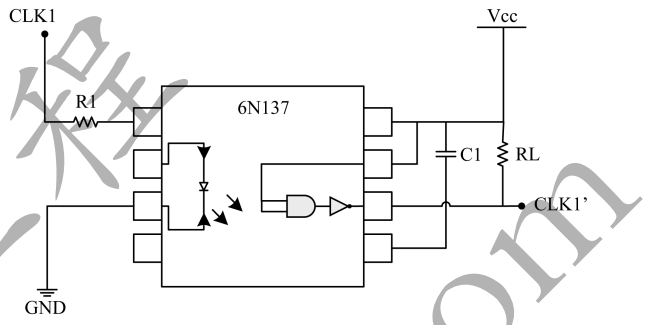

图 7 解耦电路示意图

Fig. 7 Schematic diagram of decoupling circuit

选择功耗曲线中包含密钥信息量最大的点,根据式(7),计算功耗曲线解耦前后的信噪比,结果如表 3 所示。

表 3 功耗点信噪比对比

Table 3 Comparison of signal-to-noise ratio of power consumption points

采样率/(MS·s^{-1})	解耦前信噪比/dB	解耦后信噪比/dB
25	0.055	0.065
100	0.039	0.062
250	0.054	0.077

由于待测设备的算法是硬件实现,且芯片内部存在其他电子噪声,导致信噪比相对较低。经过解耦处理后的功耗曲线,信噪比得到明显改善。

4 性能比较

表 4 列出了目前相关研究的关键指标。待测芯片执行的算法包括软件实现(SW)和硬件实现(HW)的 AES 和 DES 算法等,本文进行了硬件 AES 算法和硬件 DES 算法的功耗分析实验,证明了本文方法的提升效果。

表 4 相关方法性能对比

Table 4 Comparison of related method performance

方法	算法	工作频率/MHz	采样率/(MS·s^{-1})	预处理	提升率/%
文献[4]方法	HW-AES	24	96	无	28.0
文献[6]方法	SW-AES	3.95~13.0	31.2	有	33.0
本文方法	HW-AES HW-DES	0 ~ 10	25	无	66.7

工作频率是待测芯片执行密码算法时的工作时钟频率。本文的同步采集方法对待测芯片的工作频率最高为 10 MHz(受限于 6N137 光耦器件的最高信号转换频率,性能更优的光耦器件会提升此参数)。

采样频率是采集设备的时钟频率。文献[4]采集设备的采样频率为 96 MS/s 时达到了最优;文献[6]采集设备的采样频率为 31.2 MS/s 时达到了最优;本文在示波器采样频率为 25 MS/s 时达到最优。因此,本文对采集设备的采样频率要求最低,降低了对采集设备的成本要求。

预处理包括功耗曲线的再对齐、调整等优化操作。本文无需对功耗曲线进行处理,减少了分析的复杂度。

提升率利用了 CPA 攻击的结果,此列数据是各自采集环境下的计算结果(文献[4,6]未具体给出提升率,但可结合原文图表近似计算得到提升率)。本文方法的提升率最高达到 66.7% 。

5　结束语

本文提出一种基于 FPGA 的时钟同步功耗信息采集方法。运用该方法设计同步采集平台,实现了同步功耗信息的采集。通过相关功耗分析进行实验验证,结果表明,与 AES 和 DES 算法相比,本文同步采集方法功耗分析的成功率有较大提升。本文利用光电解耦原理改善了采集过程中的噪声问题,使信噪比得到一定提升,为解决功耗信息采集过程中的噪声问题提供了新思路。本文时钟同步设备和耦合电路是分离的,下一步通过将其合理整合并制板,以进一步提升采集的信噪比。

参考文献

[1] TAN Ruineng, LU Yuanyuan, TIAN Jiaoling. SM4 multi-path multiplicative masking method against side-channel attack[J]. Computer Engineering, 2014, 40(5): 103-108. (in Chinese)
谭锐能,卢元元,田椒陵. 抗侧信道攻击的 SM4 多路径乘法掩码方法[J]. 计算机工程,2014,40(5):103-108.

[2] ZHANG Tao. Research on key technologies of bypass attacks for cryptographic chips[D]. Chengdu: University of Electronic Science and Technology of China, 2008. (in Chinese)
张涛. 面向密码芯片的旁路攻击关键技术研究[D]. 成都:电子科技大学,2008.

[3] LIU Yubing, XU Sen, SHAN Yonglong. Research on equipment power consumption acquisition method for USBKey[J]. Computer Engineering, 2016, 42(1): 66-70, 76. (in Chinese)
刘玉兵,许森,单勇龙. USBKey 设备功耗采集方法研究[J]. 计算机工程,2016,42(1):66-70,76.

[4] O'FLYNN C, CHEN Z. A case study of side-channel analysis using decoupling capacitor power measurement with the OpenADC[C]//Proceedings of International Symposium on Foundations and Practice of Security. Berlin, Germany: Springer, 2012: 341-356.

[5] SKOROBOGATOV S. Synchronization method for SCA and fault attacks[J]. Journal of Cryptographic Engineering, 2011, 1(1): 71-77.

[6] O'FLYNN C, CHEN Z. Synchronous sampling and clock recovery of internal oscillators for side channel analysis and fault injection[J]. Journal of Cryptographic Engineering, 2015, 5(1): 53-69.

[7] O'FLYNN C, CHEN Z. Chipwhisperer: an open-source platform for hardware embedded security research[C]//Proceedings of International Workshop on Constructive Side-Channel Analysis and Secure Design. Berlin, Germany: Springer, 2014: 243-260.

[8] DEVLIN M, SHAND D. Scaling FPGA systems for software radio[C]//Proceedings of IEEE Conference on DSP Enabled Radios. Washington D. C., USA: IEEE Press, 2003: 1-7.

[9] Xilinx. Vivadodesign suite [EB/OL]. [2019-04-01]. https://www.xilinx.com/products/design-tools/vivado.html.

[10] Digilent, Inc. Basys 3 FPGAboard reference manual[EB/OL]. [2019-04-01]. https://reference.digilentinc.com/_media/reference/programmable-logic/basys-3/basys3_rm.pdf.

[11] Xilinx. 7 Series FPGAs clocking resources user guide [EB/OL]. [2019-04-01]. https://www.xilinx.com/support/documentation/user_guides/ug472_7Series_Clocking.pdf.

[12] TROCHE Co., Ltd. SAKURA-G board[EB/OL]. [2019-04-01]. http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G.html.

[13] Teledyne LeCroy. WR6Zi-ExtRef-IN/OUT accessory [EB/OL]. [2019-04-01]. http://cdn.teledynelecroy.com/files/manuals/wr6zi_extref_in_out_instructions.pdf.

[14] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[C]//Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2004: 16-29.

[15] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]//Proceedings of Annual International Cryptology Conference. Berlin, Germany: Springer, 1999: 388-397.

[16] MANGARD S. A simple power-analysis attack on implementations of the AES key expansion[C]//Proceedings of International Conference on Information Security and Cryptology. Berlin, Germany: Springer, 2002: 343-358.

[17] ARCHAMBEAU C, PEETERS E, STANDAERT F X, et al. Template attacks in principal subspaces[C]//Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer, 2006: 1-14.

[18] The MathWorks, Inc. Matlab[EB/OL]. [2019-04-01]. https://ww2.mathworks.cn/products/matlab.html.

[19] MANGARD S. OSWALD E, POPP T. Power analysis attacks: revealing the secrets of smart cards[M]. Berlin, Germany: Springer, 2007.

[20] Vishay, Inc. High speed optocoupler[EB/OL]. [2019-04-01]. https://www.vishay.com/docs/84732/6n137.pdf.

编辑　索书志