文章编号:1671-4598(2019)05-0260-05 DOI:10.16526/j.cnki.11—4762/tp.2019.05.057 中图分类号:TN06 文献标识码:A

基于 FPGA 数据采集的 USBKey 安全评估系统设计与实现

董 攀,白长虹
(北京中电华大电子设计有限责任公司 射频识别芯片检测技术北京市重点实验室,北京 100102)

摘要:USBKey 具有硬件加密功能,目前广泛应用在软件版权保护、网银支付、智能家居等重要场所,因此,对其安全性能的评估是十分重要的;基于 FPGA 数据采集的评估系统正是实现 USBkey 的安全性能评估的,同时在一定程度上弥补了现有的 USBKey 安全性能评估方法的缺点;该系统使用 USBHUB 连接 PC 机和 USBkey,同时采用 FPGA 采集并解析 USB 数据包,这不但能够精确地捕获 USBKey 在进行算法调用时产生的功耗波形图,还能实现启动攻击设备和功耗采集设备时间和 USB 进行安全运算的时间的精确匹配,从而实现高效率地评估 USBKey 的安全性能;该系统已在实验室进行了验证,结果表明该系统的评估效果好,成功率高。

关键词:USBKey;安全攻击;加密;解密;微控制器;可编程逻辑门阵列

Design and Implementation of a USBkey Equipment Security Evaluation System Based on Real—time Acquisition of FPGA

Dong Pan, Bai Changhong
(Beijing CEC Huada Electronic Design Co., Ltd., Beijing Key Laboratory of RFID Chip Test Technology, Beijing 100102, China)

Abstract: USBKey has hardware security encryption function and is widely used in important places such as software copyright, online banking payment and intelligent home system Therefore, the hardware security capability is an important evaluation index. The USBKey Equipment Security Evaluation System Based on Real—time Acquisition of FPGA is designed for evaluating the security capability, which also partly covers the shortages of currently existing methods. The system uses USBHUB to connect the PC and the USBKey and the FPGA to collect and analyze USB data packets, which can not only accurately capture the power waveforms that generated by the USBKey while running algorithms and also exactly matches the time interval between the time of turning on the attack equipment and the power —measurement equipments and the time of starting to run algorithms. Thus the system can evaluate the security capability of the USBKey efficiently. The system was verified in the laboratory, and the result show that the effect is good and the success rate is high.

Keywords: USBKey; security attack; encryption; decryption; MCU; FPGA

0 引言

USBKey 是一种基于硬件加密的安全设备,主要应用于防止软件盗版,近年来也逐渐应用于网银和安全支付等方面。由于 USBKey 内嵌多种硬件安全加密(Encryption)算法,如果用户需要使用软件或者网银支付,需要输入密码通过硬件加密认证方可正常使用或支付,这种方式极大的保护了软件版权和用户财产安全。随着人工智能理念的推广,USBKey 作为电子锁能够为家居安全提供有力保障,应用在家居安全方面的前景也非常广阔。

由于 USBKey 的广泛使用且涉及软件版权保护、文件资料加密传输[1-2]及网银交易[3]等重要场合,这让作为“安全保障”的 USBKey 的地位显得十分重要,因此 USBKey 的安全性能如何评估就更加重要了。

评估 USBKey 的安全性能,主要方法就是对其施加安全攻击(Security Attack)信号,同时使用设备采集其运算期间的功耗,通过分析 USBKey 的功耗规律来破解 USBKey 使用的加密(Encryption)算法、解密(Decryption)算法和密钥(KEY)[4]。在安全攻击的过程中最重要的一点就是告知攻击设备和功耗采集设备何时开始工作。由于 USBKey 使用 USB 接口,遵循 USB 标准规范和相关协议,其工作的特殊性导致其安全性能的评估存在一定的难度。

评估 USBKey 安全性能主要过程分为以下三步:

1)首先,在 USBKey 开始安全运算前,PC 告知设备准备产生攻击信号和采集功耗;

2)其次,PC 机根据 USBKey 所遵循的协议发送加密(Encryption)或解密(Decryption)指令开始进行安全运算;

3)最后,PC 通过功耗采集设备获取 USB 设备运算期

收稿日期:2018-11-27; **修回日期**:2018-12-19。

作者简介:董 攀(1986-),男,湖北襄阳人,硕士研究生,主要从事嵌入式验证技术方向的研究。

间的功耗。

目前传统的评估方法有以下三种：PC 机产生触发信号，外置 MCU 产生触发信号，非 USB 接口通讯产生触发信号。下面分别介绍以上三种方法工作的优缺点。

PC 机产生触发信号的原理框图如图 1 所示。

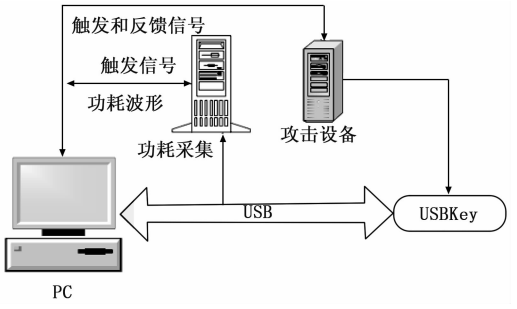

图 1　PC 机产生触发信号

PC 机具有丰富的软硬件资源，并且能够兼容各类 USB 协议和软件，外部设备的控制程序开发相对简单，因此该方法简单易实施。但是 USB 接口采用广播轮询方式信息传输，该方法 PC 机外部设备又比较多（如键盘、鼠标、示波器等）且大部分设备均采用 USB 接口，尤其部分攻击设备和功耗采集设备也会采用 USB 接口。这就导致该方法中 PC 机发送给 USBKey 的指令在物理层数据传输时，传输时间不确定（时早时慢），进而会出现攻击设备和功耗采集设备开始工作的时候，USBKey 尚未开始安全运算或者运算已结束的现象。因此，使用该方法会出现攻击迟滞或者攻击超前的情况，影响了安全评估的准确性和成功率。该方法已在射频识别芯片检测技术北京市重点实验室进行了验证，失败率达到了 85％以上。

采用外置 MCU 产生触发信号的原理框图如图 2 所示。

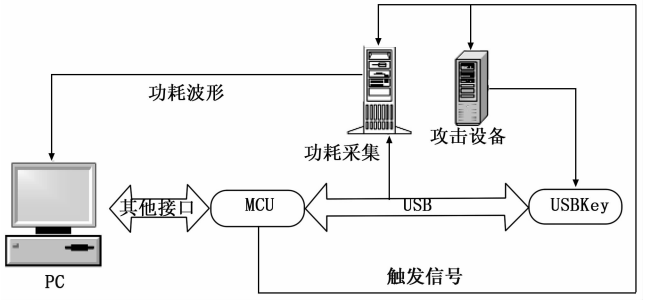

图 2　外置 MCU 产生触发信号

该方法主要是在 PC 机和 USBKey 之间外置一个具有 USBHOST 功能的 MCU 设备，该 MCU 对 PC 机是从设备，对 USBKey 是主设备。PC 机将 USBkey 加解密所需要的相关指令发送给 MCU 设备，通过 MCU 传递给 USBKey，MCU 可以在最后一条指令（即启动加解密运算）发送给 USBKey 之前产生触发信号，启动安全攻击和功耗采集，而后再发送加解密指令给 USBKey。由于 MCU 设备和 USBKey 之间没有其他设备，因此该方法的准确性比方法一要高。

该方法虽然能够提高攻击准确性，但是存在以下缺点：

1）MCU 设备的资源有限，在 MCU 设备上开发支持各类 USB 协议驱动的工作量很大；

2）由于 USBKey 种类繁多，采用 MCU 设备存在一定的兼容性局限；

3）不同 USBKey 的加解密指令不一样导致 MCU 设备的底层驱动设计需要经常升级；

4）由于 MCU 中断程序的响应，触发信号的产生时间也会稍微不准确。

非 USB 接口通讯产生触发信号原理框图如图 3 所示。

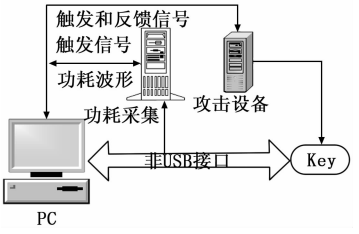

图 3　非 USB 接口通讯产生触发信号

该方法在 USBKey 使用的安全芯片上预留一个外置接口（UART、SPI、7816[5]、I^2C 等接口），PC 机通过该接口和 USBKey 通讯，这样既避免了方法一和方法二存在的准确性问题，又能继续在 PC 机上进行软件和驱动开发，大大节省软件开发的工作量。

该方法虽然简单方便且准备性高，但是存在以下不足：

1）实际应用场景使用 USB 通讯树并不是使用其他接口，因此该方法不贴近应用场景；

2）这种方法要求芯片在研发阶段除 USB 接口外预留一个接口，额外增加设计时间和验证成本；

3）不同厂家预留的接口不一致，针对各个接口都需要额外开发软件，因此，该方法的通用性不足。

综上所述，目前传统的三种评估方法存在以下问题：

1）无法达到精准的攻击时间；

2）通用性和易用性较差；

3）驱动开发和增加接口导致研发成本增高；

4）有效攻击效率降低，评估周期加长；

由此可见目前缺乏一种效率高、准确性高、通用、易行的 USBKey 安全评估系统。所以开发一种通用、精确并贴近应用场景的 USBKey 安全评估系统是十分必要的。

1　安全评估系统方案设计

1.1　USB 数据传输分析

根据上章节分析可知，USBKey 安全性能评估系统之所以存在精准性、易用性和贴近应用场景方面的问题，主要是因为攻击设备和功耗采集设备启动的时间（即触发信号产生时间）和 USB 启动安全运算的时间难以做到精确匹配，

解决了这个关键问题，也就解决了上述三种方法存在的问题。

解决这个问题的难度主要在于控制 USB 加解密指令到达 USBKey 的时间。要解决这个问题首先要分析 USB 物理层数据的传输方式和规律。根据 USB2.0 规范可知，USB 在物理层上传输数据是以数据包的形式传送，数据包主要有 SOF、SETUP、OUT、IN 等。数据包的传输方向如表 1 所示。

表 1 USB 主要数据包传输方向

数据包类型	阶段	传输方向
SOF	周期性发送	PC－＞设备
SETUP	枚举	PC－＞设备
OUT	数据通讯	PC－＞设备
IN	数据通讯	设备－＞PC

从数据包的传输方向可知：如果在 USB 数据线上解析到 OUT 包，可知这是一条由 PC 机传送至设备的信息；SETUP 虽然传输方向也是由 PC 机传送至设备，但是 SETUP 包仅在设备枚举阶段，设备枚举完成之后不会再产生 SETUP 包；SOF 包是周期性的数据包，很容易通过包头解码识别出来。

方法一出现攻击时间不确定的原因主要是 PC 机要面对多个 USB 设备，因此还需要分析 PC 机面对多个 USB 设备的传输方式和规律。根据 USB2.0 协议规范，USB2.0 通讯是广播通讯，即接在 USB 线上的所有设备都能接收到 PC 机发送过来的信息，如果该信息与接收设备无关，则该设备不予响应。另外，USBHUB 规范表明 HUB 可以独立与 USB 设备通讯，PC 机发送给 USB 设备的信息经过 USBHUB 时，USBHUB 可以将 PC 机广播过来的数据选择性的发送给 USBKey，即 USBHUB 可以屏蔽 PC 发送给非当前 USBKey 的信息。

综上可知，在 PC 机和 USBKey 之间加入一个 USBHUB 便可以隔离 PC 机传送给其他 USB 设备的信息，这样经过 USBHUB 之后传输的信息仅仅只是发送给 USBKey 的信息；其次从 USB 数据线上解析数 OUT 数据包，即可知道当前这条信息是 PC 机发送给 USBKey 的加解密指令，此时便可以产生触发信号告知攻击设备开始攻击和采集功耗，实现启动攻击设备和功耗采集设备时间和 USB 进行安全运算的时间的精确匹配。

1.2 安全评估系统原理设计

根据 1.1 小节分析搭建如图 4 所示的安全评估系统。该系统的工作原理如下：使用 HUB 隔离待检测 USBKey 与其他 USB 设备；在 PC 机向待检测 USBKey 发送加解密指令之前先启动可编程逻辑门阵列（FPGA）抓取 USBKey 上的数据，再发送加解密指令；FPGA 在启动之后检测到 OUT 包便产生触发信号告知攻击设备如和功耗采集设备，否则继续解析数据包直至停止抓取[6-8]。

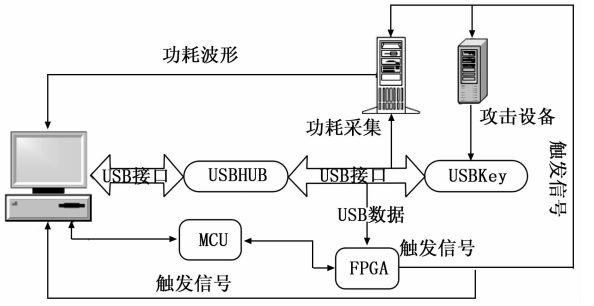

图 4 安全评估系统原理框图

由于 USB 数据传输速度固定且数据长度可知，FPGA 内部可设置 ns 级别的延时，这样可以产生精确的触发信号，从而保证 USBKey 加解密时间和攻击时间、功耗采集时间一致。

使用 FPGA 采集并解析 USB 数据去产生触发信号的方法，无需关注 USB 使用的协议，无需 PC 机开发额外的软件，也无需关注 USBKey 所使用的指令，易用性和通用性强。另外，该方法不破坏原有 USBKey 的工作场景，保持了与实际应用场景的一致性。

2 安全评估系统硬件设计

在图 4 原理框图的基础上完善 USBKey 的电源控制部分，在 FPGA 内部实现 USB 数据采集和解析功能，连接 USBHUB、攻击设备和功耗采集设备。最后所搭建的 USBKey 安全评估系统功能框图如图 5 所示。

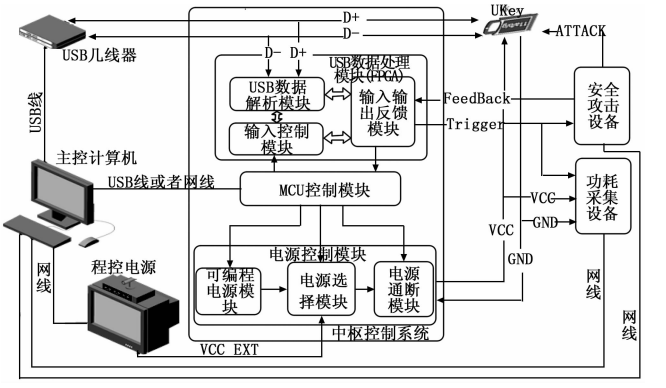

图 5 USBKey 安全评估系统硬件功能框图

安全评估系统模块主要包括：中枢控制系统、主控计算机、程控电源、USBHUB、MCU、安全攻击设备、功耗采集设备、USBKey，各个模块及设备的功能如下：

中枢控制系统：控制 USBKey 电源（MCU）、采集 USBKey 的物理数据信号（FPGA）和产生攻击触发信号。其中何时开始采集 USB 数据，解析 USB 数据包之后，何时产生触发信号是该方法需要实现且最重要的部分，也是实现该方法的难点。

主控计算机（PC）：控制程控电源向 USBKey 提供所需

的工作电压并实时读取 USBKey 的工作电流；通过向 MCU 发送命令控制 FPGA 的数据采集的启动和关闭。

程控电源：受 PC 机控制，给 USBKey 提供不同的工作电源电压，并测量 USBKey 的工作电流。

USBHUB：将 PC 发送给其他 USB 设备的信息隔离，保证 FPGA 采集到的 USB 数据仅为 USBKey 的数据；

MCU：主要接收主控计算机的命令，启动和关闭 FPGA 数据采集，同时控制 USBKey 的电源选择。

安全攻击设备：产生安全攻击信号。

功耗采集设备：采集 USBKey 在加解密运算期间的功耗。

USBKey：过 USBHUB 连接主控计算机，用于接收主控计算机的指令进行加解密运算。

3　系统软件流程设计

3.1　安全评估工作流程

根据图 5 所设计的安全评估系统功能框图，对 USBKey 进行安全功能评估，具体工作流程如下：

1）中枢控制系统复位：首先给中枢控制系统通电，使其上电复位进入工作状态，连接主控计算机，通过控制命令将 USBUkey 设备断电。

2）USBKey 电源选择：主控计算机向 MCU 发送命令控制继电器选择 USBKey 工作电源，程控电源供电或者可编程电源模块供电。

3）初始检测：给 USBKey 上电，发送命令检测 USBKey 是否正常工作，如果 USBKey 不正常工作，更换 USBkey；

4）启动检测：给 USBKey 发送指令更新密钥，初始化加解密数据；

5）启动 FPGA 数据处理模块：PC 发送命令告知 MCU 启动 FPGA 采集并解析 USB 数据包；

6）发送加解密指令：PC 机向 USBKey 发送加解密指令；

7）判断是否 FPGA 解析数据包超时，若超时 PC 机记录超时信息并跳至步骤 4），否则跳至步骤 8）FPGA 继续检解析 USB 数据包；

8）FPGA 解析数据包是否有 OUT 包产生，没有跳至步骤 7），有则跳至步骤 9）；

9）产生触发信号，如果 FPGA 成功解析到 OUT 包，根据后续数据包长度延迟一定时间再产生触发信号并跳至步骤（10）；

10）攻击设备和功耗采集设备接收到触发信号后同时产生攻击信号和功耗采集，并判断是否攻击成功，若攻击成功则 PC 机保存攻击记录及功耗采集记录，反馈并跳至步骤 11），若失败则 PC 保存失败记录，并跳至步骤 4）；

11）USBKey 断电，判断是否结束攻击，若结束则跳至步骤（12），否则上电并跳至步骤 4）；

12）结束实验，分析功耗波形做性能评估。

3.2　软件工作流程图

系统工作流程如图 6 所示，该流程图详细表述了该安全评估系统在 USBKey 工作过程中的整个软件工作流程。

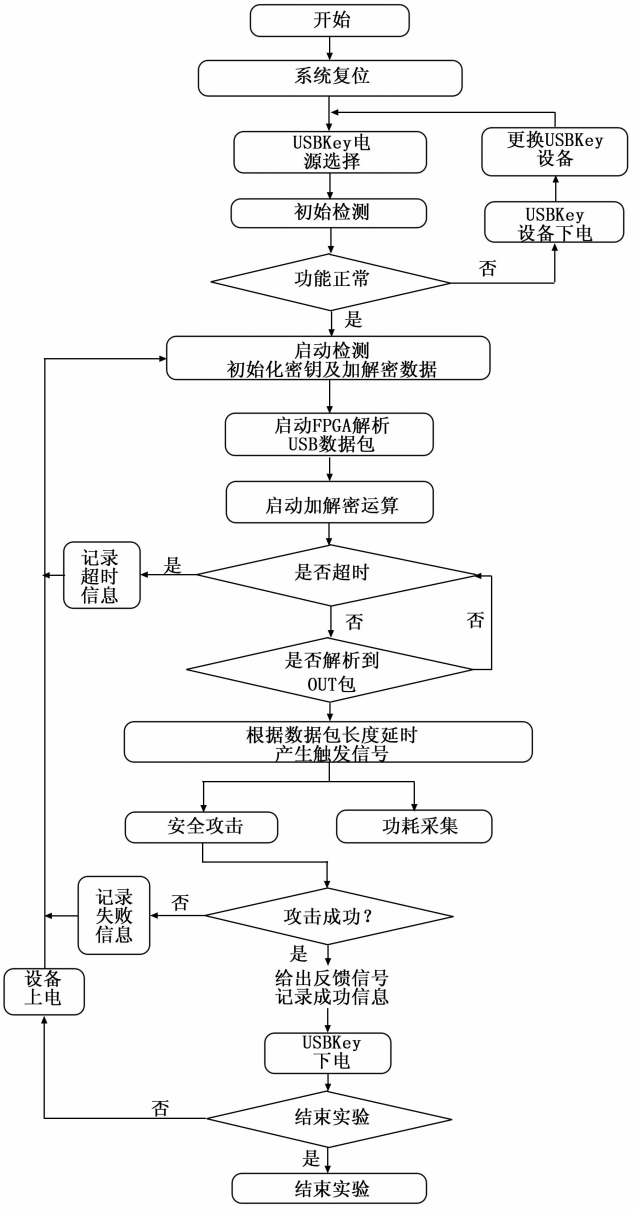

图 6　安全评估系统工作流程

4　实验结果与分析

4.1　实验结对比

选用 XlinxFPGA 和 STM32 的 MCU 实现中枢控制系统功能，在 FPGA 上完成 USB 数据包采集和解析功能，在 MCU 上完成 FPGA 控制部分功能。实现中枢控制系统后根据图 5 所示搭建安全评估系统，该系统已在射频识别芯片检测技术北京市重点实验室进行了系统级验证并取得了良

好的效果，实验成功率 90％以上，相比较于方法一（成功率＜15％）成功率很高。图 7 和图 8 为实验过程中捕获到的算法功耗波形图。

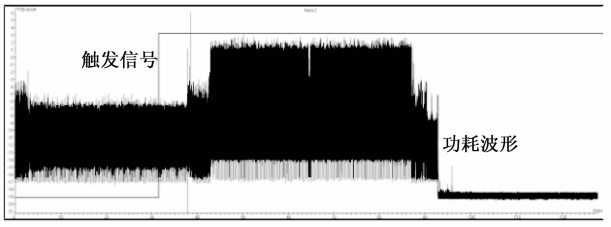

图 7 实验室捕获的 RSA 算法功耗图

图 7 为使用本方法在 USBKey 进行 RSA 运算过程中抓取的功耗波形图，其中触发信号为 FPGA 采集到 USBKey 加解密指令之后解析和产生，波形密集且变化剧烈部分为芯片运行 RSA 算法时的功耗[9-10]。

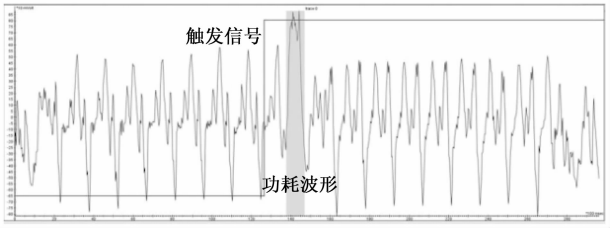

图 8 实验室捕获的 DES 算法功耗图

图 8 为使用本方法在 USBKey 进行 DES 运算过程中抓取的功耗波形图，其中阴影部分功耗波形为芯片运行 DES 算法时的功耗[11-12]。

实验结果表明测试人员可以通过触发信号后的功耗波形图分析出 USBKey 当前使用的安全算法、密钥等相关信息，通过这些信息确可以判断 USBKey 产品的安全性。

该方法与传统的三种方法的效果对比如表 2 所示。

表 2 方法效果对比

方法	易用性	通用性	精确性	应用性
方法一	优	良	差	优
方法二	良	差	良	优
方法三	良	差	良	差
本方法	优	优	优	优

综上所述，本文设计的评估系统与现有技术相比有以下优点：

1）易用性：无需关注 USB 协议，PC 端无需开发额外软件。

2）通用性：无需关注不同 USBKey 的加解密指令，解析出 OUT 数据包即可产生触发信号。

3）精确性：能够在芯片启动安全运算之前控制触发信号的产生时间，精度达到 ns 级别。

4）应用性：贴近 USBKey 实际应用场景。

4.2 实验结果分析

该系统在实验室验证效果良好，成功率达到 90％以上，但是仍未达到 100％，主要原因是 USB 数据采集和解析部分代码尚存在不完善的地方，未能够 100％正确解析出数据包，在后续的研发工作中还需要优化该部分代码。

5 结束语

本文利用 FPGA 采集 USB 数据的方法设计并实现了一套基于 FPGA 数据采集的 USBkey 设备安全评估系统，可以在 USBKey 进行交易时产生精确的攻击和功耗采集，从而评估该 USBKey 的安全性能。该系统能够精确控制产生攻击 USBKey 信号的间，并支持 USB 各类协议，无需开发相关软件，大大弥补了现有方法存在的不足，提高了 USBkey 安全评估的准确性和工作效率。该系统经过后续完善后，成功率能够达到 100％，应用前景将非常广阔。

参考文献：

[1] 喻 潇，田 里，刘 喆，等. 基于 USBKEY 的网络存储用户数据保护的研究与实现 [J]. 2018，4 (6)：63－64.

[2] 郭利芳，赵 凡，李小兵，等. 一种 USBKey 的文件加密软件方案的设计 [J]. 2013 (2)：27－28.

[3] 余 慧. 基于 BSK 即杖术实现电子钱包的安全应用解决方案 [J]. 湖北教育学院学报，2007 (2)：71.

[4] 刘玉兵，许 森，单勇龙. USBKey 设备功耗采集方法研究 [J]. 2016，20 (1)：67－68.

[5] 乌力吉，李贺鑫，任燕婷等. 智能卡功耗分析平台设计与实现 [J]. 2012，52 (10)：1409－1414.

[6] 彭家伟. 基于 FPGA 的 USB 数据采集系统设计 [J]. 2014 (5)：75－77.

[7] 陈柯勋，王振田，王 飞. 基于 FPGA 和 USB2. 0 的数据采集系统 [J]. 2017，4 (5)：12－14.

[8] 吴晓陆. 基于 FPGA 的 USB 通信系统的设计 [D]. 辽宁：大连交通大学，2009.

[9] 范黎恒，向凯全，赵 强，等. 针对 RSA 的简单功耗分析攻击实验 [J]. 2009，25：12－2.

[10] Kocher P. Timing attacks on implementations of Diffie －HellAmann，RSA，DSS，and other systems [A]. CRYPTO’96 [C]. 1996，LNCS 1109.

[11] 曹 凯，陆海宁，邓 峰，等. 一种抗二阶功耗分析的 DES 算法实现方案 [J]. 2015 (12)：38－41.

[12] Paul Kocher，Joshua Jaffe，Benjamin Jun. Differential Power Analysis [A]. Proceedings of Advances in Cryptology －CRYPTO’99 [C]. 1999：388－397.