物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于时间相关单光子计数技术的密码芯片光辐射分析

王红胜 纪道刚 高艳磊 张阳 陈开颜 陈军广 吴令安 王永仲

Photonic emission analysis of cipher chips based on time-correlated single-photon counting

Wang Hong-Sheng Ji Dao-Gang Gao Yan-Lei Zhang Yang Chen Kai-Yan Chen Jun-Guang Wu Ling-An Wang Yong-Zhong

引用信息 Citation: Acta Physica Sinica, 64, 058901 (2015) DOI: 10.7498/aps.64.058901
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.058901
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I5

基于时间相关单光子计数技术的密码芯片光辐射分析*

王红胜[1)†] 纪道刚[1)] 高艳磊[2)3)] 张阳[1)] 陈开颜[1)] 陈军广[1)]
吴令安[2)] 王永仲[1)]

1) (军械工程学院, 信息工程系, 石家庄 050003)

2) (中国科学院物理研究所, 北京凝聚态物理国家实验室, 北京 100190)

3) (河北师范大学, 石家庄 050018)

(2014 年 8 月 6 日收到; 2014 年 9 月 23 日收到修改稿)

密码芯片运行时的光辐射可泄露其操作和数据的重要特征信息. 基于单光子探测技术, 设计并构建了针对 CMOS 半导体集成电路芯片光辐射信号的采集、传输、处理和分析的光电实验系统. 以 AT89C52 单片机作为实验对象, 采用时间相关单光子计数技术, 对不同工作电压下密码芯片的光辐射强度进行了对比, 分析了芯片指令级光辐射信息的操作依赖性和数据依赖性. 此外, 使用示波器对时间相关单光子计数技术在芯片光辐射分析上的可行性进行了验证. 实验结果表明, 采用时间相关单光子计数技术对密码芯片进行光辐射分析, 是一种直接有效的中低等代价光旁路分析攻击手段, 对密码芯片的安全构成了严重的现实威胁.

关键词: 密码芯片安全性分析, 旁路攻击, 时间相关单光子计数, 光辐射的操作/数据依赖性

PACS: 89.20.Ff, 85.60.–q, 07.05.Kf, 03.67.Dd **DOI:** 10.7498/aps.64.058901

1 引 言

密码算法的载体——密码芯片, 在运行时会泄露出特征信息, 特征信息来自功耗、电磁辐射、光辐射等, 这些可能泄露密码芯片敏感信息的通道称为旁路 (side channel). 通过俘获、分析密码芯片的旁路信息, 进而破解密码算法的相关秘密参量, 使得旁路攻击可以对密码芯片的安全性产生巨大的威胁 [1−4].

作为一种新型旁路攻击方法, 光辐射分析攻击于 2008 年首次提出; Ferrigno 和 Hlavác 利用集成电路晶体管状态转换时存在光子泄漏的原理, 使用皮秒成像电路分析系统 (PICA) 探测芯片光子辐射, 通过对这些辐射信息进行分析, 能够识别出芯片内部的秘密参量 [5].

光辐射分析攻击的区域选择性大大超过功耗等旁路攻击, 探测密码芯片时有较好的信噪比, 并能俘获由全部泄漏组成的信号 [6]. 由于文献 [5] 中使用的设备复杂且成本巨大, 当时光旁路不被视为一个现实的威胁. 随着日新月异的半导体技术为单光子探测技术的发展提供了强大的动力, 适合可见光、近红外等波段的硅基、铟镓砷、超导等单光子探测、处理技术得到了快速的发展 [7−11], 探索中低成本和高效的光辐射分析的攻击方法, 对于密码芯片的安全和防护具有十分重要的现实意义.

* 国家自然科学基金 (批准号: 51377170), 国家高技术研究发展计划 (批准号: 2011AA120102) 和河北省自然科学基金 (批准号: F2012506008) 资助的课题.

† 通信作者. E-mail: whswzx@aliyun.com

2 基本原理

2.1 密码芯片光辐射机理

当前, 绝大部分数字电路是基于CMOS工艺构建的, 使用互补晶体管作为基本元素. 标准CMOS反向器门电路由一对n-MOS和p-MOS晶体管组成, 当输出状态从高变为低时, n沟道晶体管发生光辐射; 当输出状态从低变为高时, p沟道晶体管发生光辐射. 由于电子比空穴的流动性好, n沟道晶体管的光辐射更多; 另外, 靠近漏极电场的区域辐射光子较多. CMOS逻辑的光辐射表明数据相关行为与功耗相似, 但不等于功耗; 光子生成速率与电源电压及晶体管开关频率成正比[12,13].

因此, 当CMOS门电路改变它的状态, 就会发生光辐射效应[14]. 由于热载流子获得的能量不同, 通过跃迁辐射出光子的光谱也不同, 辐射光谱范围从500到1200 nm以上, 最大辐射范围在900和1100 nm之间[15]. 辐射光子的数量(光子辐射概率)通过以下公式能够计算出来[16]:

$$N_{\mathrm{e}} = S_{\mathrm{e}} B \frac{L_{\mathrm{H}} I_{\mathrm{d}}}{q v_{\mathrm{s}}} T_{\mathrm{s}}, \tag{1}$$

其中, S_{e}是光谱辐射密度, B为辐射带宽, L_{H}是热载流子区域长度, I_{d}是漏电流, q是电子电荷, v_{s}是载体饱和速度, T_{s}是开关转换周期. 随着密码芯片工艺的不同, 每次晶体管翻转辐射的光子数从10^{-2}到10^{-4}不等[17].

2.2 单光子探测技术

由于密码芯片的光辐射特性, 密码芯片在执行不同的操作和处理不同的数据时, 不同区域的光辐射强度是不同的. 因此, 密码芯片工作时, 光信号的俘获和分析涉及单光子信号处理领域, 要求采集设备能够区分单光子, 且对特定的光谱范围内单光子探测具有较高灵敏度和较高的时间/空间分辨率. 由于光辐射波长在500到1200 nm以上, 覆盖了可见光和近红外两个波段, 因此, 对探测器的材料构成有特殊要求. 例如, 硅基(Si-based) CCD、光电倍增管或雪崩光二极管适合采集可见光部分(500—850 nm), 铟镓砷(InGaAs)雪崩光二极管适合采集近红外部分(850—1200 nm). 对于光辐射迹的分析和处理, 涉及光强的时间和空间分布, 这需要采用与探测器匹配的高速光子计数技术进行处理. 最后, 由于集成电路封装在硅衬底中, 为减少硅封装对光子的吸收, 提高光子探测效率, 需将芯片上面打磨以便露出集成电路或将背面减薄.

因此, 针对不同工艺尺寸和集成度的密码芯片, 开展更加高效和深入的密码芯片光辐射分析, 需要多种组合和更加复杂的解决方案.

与文献[5, 18, 19]中价格昂贵且复杂的光探测设备相比, 本文设计了中低等成本的密码芯片光辐射采集和处理系统, 使用硅基单光子雪崩光二极管(single-photon avalanche diode, SPAD)探测器[20]作为信号采集模块, 首次提出采用时间相关单光子计数技术[21,22]进行密码芯片光辐射信号处理. 经实验验证, 这是一种简单高效的可针对密码芯片特定区域进行相对精确分析的光辐射探测和处理系统.

2.3 时间相关单光子计数技术

时间相关单光子计数(time-correlated single-photon counting, TCSPC)基本原理是: 被测光源辐射的光强很低, 在一个信号采集周期内探测到一个光子的概率远远小于1, 即在一个信号周期内一般最多只有一个光子到达SPAD探测器, 而每个光子到达探测器的时间不同; 经过多次的高重复频率同步采样后, 可建立光子时间统计分布的直方图, 如图1所示.

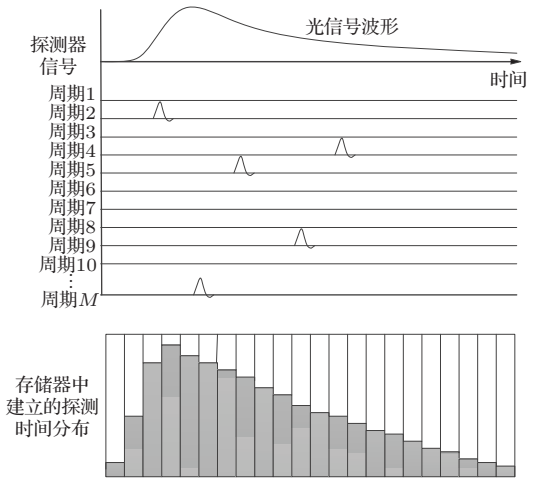

图1 TCSPC技术基本原理(摘自文献[22])

TCSPC技术具有单光子灵敏度, 根据时间通道的多少可以达到皮秒级的时间分辨率. 实验中, 单片机AT89C52的机器周期是1 μs, 指令周期主要集中在1—2 μs, 使用TCSPC技术对SPAD探测

器的输出进行统计处理, 能够满足密码芯片光辐射分析的采样需求, 这在后面的实验中得到了验证.

2.4 密码芯片光辐射依赖性

密码芯片光辐射分析攻击是通过采集、分析密码芯片在运行时的光子辐射轨迹特征获取密码算法的秘密参量. 这种攻击主要利用了两类光子辐射依赖性: 操作依赖性和数据依赖性, 即处于工作状态密码芯片的瞬时光子辐射依赖于密码芯片所执行的操作和所处理的数据.

与功耗、电磁等旁路攻击集中于全系统的信息泄漏相比, 光辐射分析攻击能够对探测器探测空间的范围进行比较灵活的选择, 这使得可以选择密码芯片的特定区域进行深入分析, 从而使得光辐射分析攻击更加高效. 对于指令级的光辐射分析来说, 密码芯片不同位置的光泄露所体现的指令的操作依赖性和数据依赖性是有差异的. 选择的探测区域大, 相关操作和数据的光辐射依赖性具有一定全局特征和可比性; 选择的探测区域小, 则便于更好地对所关心的操作和数据进行更为精确的分析. 一般而言, 由于对芯片位置敏感, 光辐射分析攻击需要对准位置, 这取决于攻击者所关心的指令和操作数. 因此, 在实验中, 我们主要围绕针对SRAM数据区的指令和操作数, 通过采集密码芯片SRAM相关区域的光辐射, 进行了部分相关指令的操作依赖性和数据依赖性的光辐射分析. 根据密码芯片选定区域的光辐射信息与操作、数据的依赖关系, 针对具体的密码算法进行光辐射分析攻击, 就可以进而获取密码算法的秘密参量. 例如, 通过简单光辐射分析、差分光辐射分析、相关性光辐射分析等分析方法对具体密码算法进行攻击.

3 实验设置

在对AT89C52密码芯片的光辐射分析实验中, 为了实际验证使用TCSPC技术的有效性和可行性, 我们设计了两套实验系统: 基于TCSPC技术的光电实验系统和使用示波器的光电实验系统.

3.1 待测芯片

使用AT89C52单片机作为待测密码芯片, 它具有8 k字节的Flash程序存储器和256字节的内部数据存储器SRAM. 实验中, AT89C52的工作时钟频率是12 MHz, 1个机器周期是1 μs; AT89C52执行的指令和操作的数据被定制; 外部计算机通过RS232接口与AT89C52通信, 控制单片机执行什么指令和操作哪些数据; 单片机通过RS232接口接收明文数据, 并可将加密后的密文数据返回给外部计算机; 观测分析的主要目标是SRAM存储器区域.

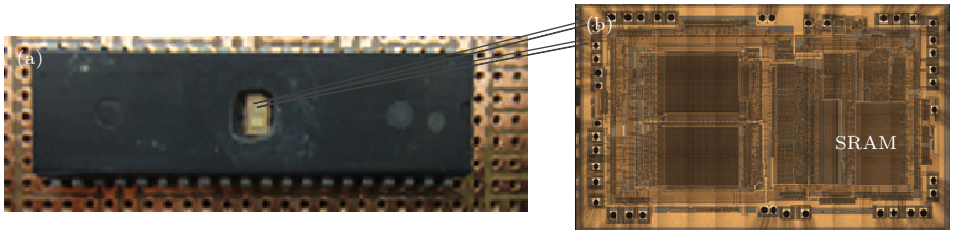

图2 (a) 解封后的AT89C52微控制器; (b) 放大后的AT89C52芯片

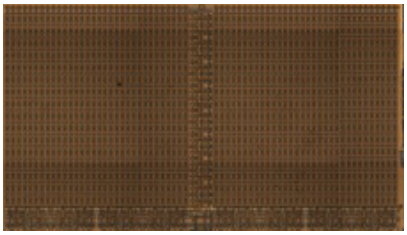

图3 放大后的SRAM区域

对AT89C52进行光辐射分析, 需要事先使用机械打磨和化学腐蚀相结合的方法对设备打开封装, 这样便于对芯片的光辐射情况进行探测. 如图2所示, 其中图2 (b)是解封后放大的AT89C52芯片, 图2 (b)右下角区域是SRAM存储器.

实验中主要利用SPAD对芯片内部SRAM区域内寄存器进行探测, 图3为放大后的SRAM区域.

3.2 基于TCSPC技术的光电实验系统

实验系统如图4所示. 选用的硅基SPAD探测器为Excelitas SPCM-AQRH-15-FC, 能够俘获400

到1060 nm波长的光子, 对可见光部分有较高的采集效率, 并能采集部分近红外光子, 其探测端通过光纤和非球面透镜对准密码芯片的待测区域. 使用Becker& Hickl SPC-130型的TCSPC数据采集与处理卡, 接收SPAD的输出信号, 根据时间记录在4096个道值上. 计算机1通过串口给AT89C52发送不同的消息, 控制密码芯片执行相关待测程序和处理相关数据. 计算机2内安装有SPC-130采集卡, 存储数据和进行基于TCSPC技术的光信号处理及分析.

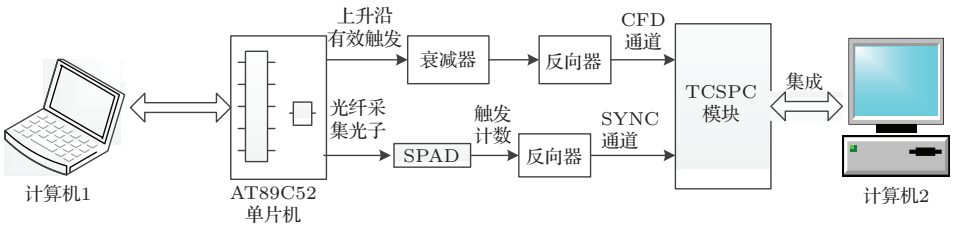

图4 基于TCSPC技术的光信号采集和处理系统

3.3 使用示波器的光电实验系统

实验系统如图5所示. 使用示波器作为光信号的核心处理模块. 选用同样的SPAD探测AT89C52密码芯片的光辐射信号, 其输出端连接到示波器CH1通道. 计算机通过串口给密码芯片发送不同的消息, 控制其执行相关待测程序和处理相关数据. 将AT89C52的触发输出连接到示波器CH2通道, 为示波器的信号采集提供同步信号, 采集的数据通过Labview存储到计算机中, 再进行信号处理及分析.

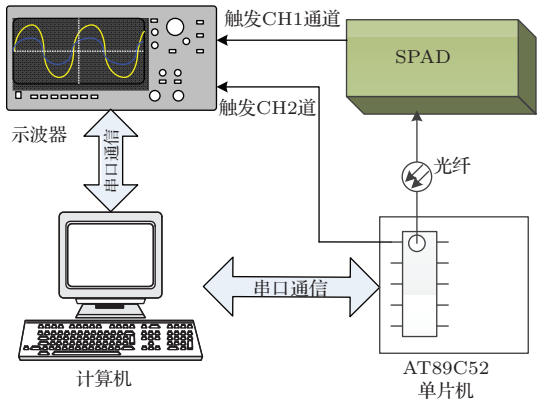

图5 使用示波器的光信号采集和处理系统

3.4 实验程序

主要针对AT89C52执行的MOV指令进行分析, 根据不同实验需求, 对MOV指令程序添加部分比较代码和辅助代码, 相关指令描述如图6所示. 计算机通过RS232接口与AT89C52通信, 控制单片机执行什么指令和操作哪些数据. 例如, 为实现测试过程中动态改变某一变量(如R7寄存器)的值, 计算机通过发送不同数据到密码芯片的#LOW单元, 控制被操作数据的改变. 程序前两指令是取出计算机发送的数据到累加器A中. 程序中异或指令(XRL)和转移指令(SJMP)各需要两个机器周期执行, 其余指令各需要一个机器周期执行, 测试程序周期共计10 μs.

```
1058:          ?C0032
1059:          MOV     R0,#LOW
1060:          MOV     A,@R0
1061:          XRL     P1,#08H
1062:          MOV     R7,A
1063:          XRL     P1,#08H
1064:          MOV     R7,#0x00
1065:          SJMP    C0032
```

图6 相关程序汇编代码

4 密码芯片光辐射分析

4.1 芯片电压对光辐射影响

实验中, 通过让微控制器芯片执行相同指令、处理相同数据并采集相同时间间隔的光辐射信号, 改变微控制器工作电压, 发现微控制器光辐射数量差异很大. 在使芯片正常工作的前提下, 电压越高, 光辐射强度越高. 对AT89C52在不同工作电压下进行的一组实验(采集5 min)表明, 光辐射与工作电压是近似指数关系而不是线性的, 如图7所示. 因此, 在后面的相关实验中, 为提高光辐射采集效率, 我们选择了较高的工作电压(6.5 V).

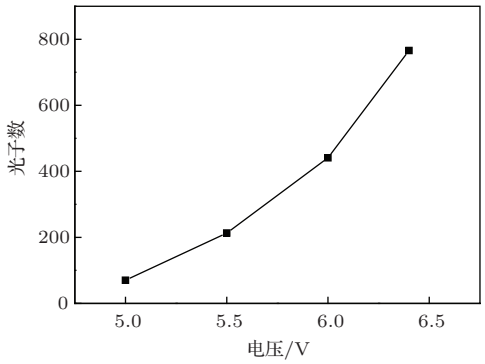

图 7 光辐射与芯片工作电压的关系

4.2 操作依赖性分析

微控制器执行如图 6 所示的实验程序, 先使用图 4 所示的 TCSPC 系统进行光辐射信号采集. 实验过程中, 通过计算机控制密码芯片执行相关指令, 密码芯片为 TCSPC 处理模块提供触发信号, 同时, 它所发出的光辐射由 SPAD 采集. 因单光子探测器 SPCM-AQRH-15-FC 输出信号为标准 TTL 形, 而 TCSPC 采集卡 SPC-130 需要负脉冲输入, 便使用了反向器. 光子按照到达单光子探测器的时间, 分布在 4096 个通道上. 采集 10 min, 将采集数据按照图 6 所示指令顺序处理, 结果如图 8 所示. 发现不同指令执行周期中辐射的光子数是不相同的, 说明密码芯片光辐射与指令操作有关.

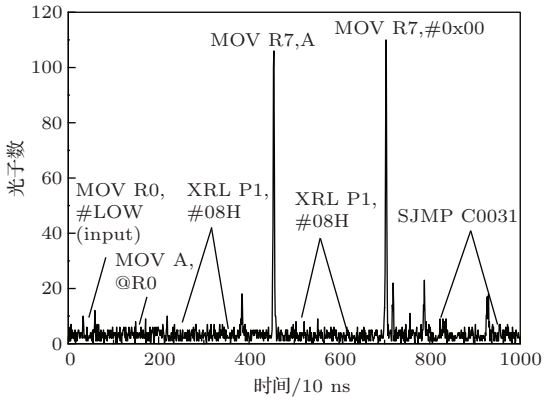

图 8 微控制器不同指令周期内的光辐射时间分布

4.3 数据依赖性分析

在某一时间间隔内, 密码芯片光辐射情况不但依赖于指令, 同时也依赖于被处理的数据. 为获知密码芯片执行相同指令处理不同数据的光辐射特征, 单光子探测器通过光纤对准微控制器 SRAM 区域 R7 寄存器, 针对 AT89C52 微控制器 R7 寄存器进行探测, 使用的指令是 MOV R7, A. 实验过程中参考了汉明距离模型 [23], 每次改变 R7 寄存器值前将 R7 设置 00(16 进制, 下同), 确保每次变换是从 00 翻转到某个数值的, 而后分别将 R7 值改变为 00, 01, 03, 07, 0F, 1F, 3F, 7F, FF, 对应寄存器 R7 依次翻转 0—8 位 (二进制). 对指令 MOV R7, A 光辐射采集的数据分析如图 9 所示, 采集时间是 10 min. 实验结果表明, 寄存器翻转位数越多, 辐射光子数越多, 数据的变化 (二进制数各位的变化) 与光辐射存在相关性.

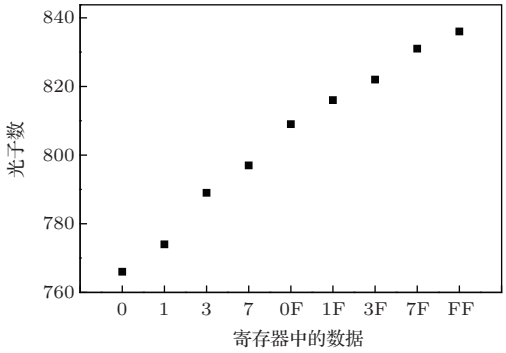

图 9 芯片光辐射与寄存器中数据变化的依赖性关系

4.4 对使用 TCSPC 技术可行性的实验验证

为验证基于 TCSPC 技术的实验系统记录的光辐射轨迹的有效性和使用该系统的可行性, 即是否

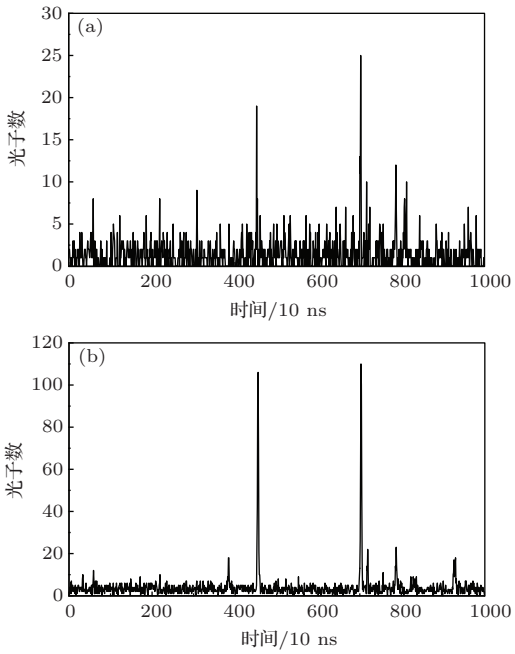

图 10 两个实验系统光辐射轨迹处理结果对比 (a) 示波器处理结果; (b) TCSPC 技术处理结果

准确可靠地反映了密码芯片的实际光辐射情况, 我们使用示波器进行了相同的实验(实验系统如图5所示). 密码芯片执行图6所示指令, 分别使用图5、图4实验系统进行光辐射信号采集处理. 光辐射轨迹如图10所示, 图10(a)是使用示波器进行光信号处理的结果, 其采集时间约2个小时; 图10(b)是使用TCSPC技术采集10 min的处理结果. 通过分析可以发现, 使用TCSPC技术与使用示波器的处理结果的光辐射轨迹特征一致, 但使用TCSPC技术的分析效率要远远高于使用示波器.

5 结 论

对AT89C52单片机进行操作依赖性和数据依赖性分析的光辐射实验结果表明, 作为一种直接有效的中低等代价旁路攻击手段, 采用TCSPC技术对密码芯片进行光辐射分析, 可以得到光辐射信号与密码芯片内相关信息的直接或间接依赖性联系, 进而对密码芯片的安全构成了严重的现实威胁, 同时, 以上研究为进一步深入开展针对AES, RSA等密码芯片的简单光辐射和差分光辐射等分析打下了良好的技术基础.

参考文献

[1] Boer B, Lemke K, Wicke G 2002 *Cryptographic Hardware and Embedded Systems-CHES 2002 4th International Workshop Redwood Shores*, CA, USA, August 13–15, 2002 p228

[2] Agrawal D, Archambeault B, Rao J R, Rohatgi P 2002 *Cryptographic Hardware and Embedded Systems-CHES 2002 4th International Workshop Redwood Shores*, CA, USA, August 13–15, 2002 p29

[3] Skorobogatov S, Anderson R 2002 *Cryptographic Hardware and Embedded Systems-CHES 2002 4th International Workshop Redwood Shores*, CA, USA, August 13–15, 2002 p2

[4] Skorobogatov S 2005 *Ph.D. Dissertation* (London: University of Cambridge)

[5] Ferrigno J, Hlavá M 2008 *IET Infor. Secur.* **2** 94

[6] Kramer J, Nedospasov D, Schlosser A, Seifert J 2013 *Constructive Side-Channel Analysis and Secure Design* (Berlin: Springer-Verlag) p1

[7] Sun Z B, Ma H Q, Lei M, Yang H D, Wu L A, Zhai G J, Feng J 2007 *Acta Phys. Sin.* **56** 5790 (in Chinese) [孙志斌, 马海强, 雷鸣, 杨捍东, 吴令安, 翟光杰, 冯稷 2007 物理学报 **56** 5790]

[8] Wang Y J, Ding T, Ma H Q, Jiao R Z 2014 *Chin. Phys. B* **23** 060308

[9] LIANG Y, ZENG H P 2014 *Sci. China Phys. Mech. Astron.* **57** 1218

[10] Liu Y, Wu Q L, Han Z F, Dai Y M, Guo G C 2010 *Chin. Phys. B* **19** 080308

[11] Zhang L B, Kang L, Chen J, Zhao Q Y, Jia T, Xu W W, Cao C H, Jin B B, Wu P H 2011 *Acta Phys. Sin.* **60** 038501 (in Chinese) [张蜡宝, 康琳, 陈健, 赵清源, 郑涛, 许伟伟, 曹春海, 金飚兵, 吴培亨 2011 物理学报 **60** 038501]

[12] Stellari F, Zappa F, Cova S, Vendrame L 1999 *IEDM Technical Digest–International Electronic Devices Meeting Washington*, USA 1999 p487

[13] Schlosser A, Nedospasov D, Kramer J, Orlic S, Seifert J–P 2013 *J. Cryptogr. Eng.* **3** 3

[14] Deboy G, Kölzer J 1993 *Semicond. Sci. Technol.* **9** 1017

[15] Villa S, Lacaita A L, Pacelli A 1995 *Phys. Rev. B* **52** 10993

[16] Stellari F, Zappa F, Ghioni M, Cova S 1999 *Solid-State Device Research Conference Leuvem*, Belgium, September 13–15, 1999 p172

[17] Skorobogatov S 2009 *6th Workshop on Fault Diagnosis and Tolerance in Cryptography* (FDTC 2009) Lausanne, Switzerland September 2009 p111

[18] Tsang J C, Kash J A, Vallett D P 2000 *IBM J. Res. Develop.* **44** 583

[19] Kash J, Tsang J 1997 *Elect. Dev. Lett.* **18** 330

[20] Excelitas Technologies http://www.excelitas.com [2012-01-24]

[21] Becker W 2005 *Advanced Time-Correlated Single Photon Counting Techniques* (Berlin: Springer-Verlag) pp19–23

[22] Becker W 2012 *The bh TCSPC Handbook 5th Edition* (Berlin: Becker & Hickl GmbH) pp51–57

[23] Mangard S, Oswald E, Popp T 2010 *Power Analysis Attacks: Revealing the Secret of Smart Cards* (New York: Springer Science+Business Media, LLC) pp38–43

Photonic emission analysis of cipher chips based on time-correlated single-photon counting*

Wang Hong-Sheng[1)†] Ji Dao-Gang[1)] Gao Yan-Lei[2)3)] Zhang Yang[1)] Chen Kai-Yan[1)]
Chen Jun-Guang[1)] Wu Ling-An[2)] Wang Yong-Zhong[1)]

1) (*Department of Information Engineering, Ordnance Engineering College, Shijiazhuang 050003, China*)

2) (*Laboratory of Optical Physics, Beijing National Laboratory for Condensed Matter Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China*)

3) (*Hebei Normal University, Shijiazhuang 050018, China*)

(Received 6 August 2014; revised manuscript received 23 September 2014)

Abstract

When in operation, cipher chips emit photons which can reveal important information about their operation and data. An experimental system based on single-photon counting for the detection, transmission, processing and analysis of photonic emission from CMOS semiconductor integrated circuits has been designed and constructed. Using time-correlated single-photon counting (TCSPC) technology, we have analyzed the photon emission of cipher chip AT89C52, and measured the relationship between its emission intensity and voltage. We have also analyzed in detail the relationship between the photonic emission and the operations and data processed in the chip at the instruction level. Furthermore, we have confirmed the feasibility of our TCSPC technique using an oscilloscope. Our experimental results show that cipher chip photonic emission analysis based on TCSPC technology is a relatively low cost but effective method for optical side-channel attacks, and that it poses a serious practical threat to cipher chip security.

Keywords: cipher chip security analysis, side-channel attack, time-correlated single-photon counting, operation/data dependency of photonic emission

PACS: 89.20.Ff, 85.60.–q, 07.05.Kf, 03.67.Dd **DOI:** 10.7498/aps.64.058901

* Project supported by the National Natural Science Foundation of China (Grant No. 51377170), the National High Technology Research and Development Program of China (Grant No. 2011AA120102), and the Natural Science Foundation of Hebei province, China (Grant No. F2012506008).

† Corresponding author. E-mail: whswzx@aliyun.com