基于亚稳态的 QDI 逻辑随机路径切换方法研究

欧庆于[1,2],张焕国[1],吴晓平[2],李凤华[3],罗 芳[2]
(1.武汉大学计算机学院,湖北武汉,430072;2.海军工程大学信息安全系,湖北武汉 430033;
3.中国科学院信息工程研究所,北京 100093)

摘 要: 基于 QDI 异步逻辑与四相双轨协议相结合时数据路径平衡的特性,能够实现双轨编码输入点的随机切换,从而达到各数据路径的平均功耗平衡,消除数据与功耗之间关联的目的.然而,现有的利用多路复用器实现数据路径随机切换的方法存在抗攻击弱点,削弱了系统的抗能量分析攻击能力.为此,我们提出了基于亚稳态的 QDI 随机路径切换方法:采用两级切换结构,利用亚稳态发生器和亚稳态滤波器,实现数据路径组和数据路径的随机切换.仿真结果表明,基于亚稳态的 QDI 随机路径切换方法具有良好的功耗平衡特性,能够很好的抵消由于寄生电容和负载电容差异造成的旁路信息泄露,从而极大地提高系统的安全性.

关键词: 能量分析攻击; QDI 逻辑; 亚稳态; 随机路径切换
中图分类号: TP309.1 **文献标识码:** A **文章编号:** 0372-2112 (2012)10-1996-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.10.016

The Research on QDI Random Path Swapping Based on the Metastability

OU Qing-yu[1,2], ZHANG Huan-guo[1], WU Xiao-ping[2], LI Feng-hua3, LUO Fang[2]
(1. *School of Computer Science, Wuhan University, Wuhan, Hubei* 430072, *China*;
2. *Depart. of Information Security, Naval University of Engineering, Wuhan, Hubei* 430033, *China*;
3. *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract: Based on the balance characteristic of the data-path when combining QDI asynchronous logic and the four-phase protocol with dual-rail encoding, the random swapping of the data-path rail can be implemented, so the balance of the average power for every data-path can be implemented, and the correlation between the data and the power can also be eliminated. But because of using the multiplexer for the random swapping, the current method will induce the system's ability of against power analysis attack to be weakened. So the method of QDI random data-path swapping, which is based on the metastability is put forward. By adopting the two-level swapping structure, the metastability generator and metastability filter, the random swapping between the data-path group and the data-path can be implemented. Simulation results show that, the method has the characteristic of preferable power balance, and the leakage of the side-channel information brought by the differences of the parasitic capacitor and the load capacitor, can also be counteracted.

Key words: power analysis attack; QDI logic; metastability; random path swapping

1 引言

自从 1996 年 Paul Kocher 首次发现密码芯片运算时泄漏的旁路信息能被用于密码分析[1],人们对旁路攻击技术倾注了极大的关注和热情,并提出了众多基于不同旁路泄露信息的攻击方法,如:时间攻击、功耗攻击、电磁攻击及故障攻击等.其中,能量分析攻击以其简单易行、适用范围广和行之有效等特点得到了广泛研究和使用,并由最初的简单能量分析[2]、差分能量分析[3]发展为地址差分能量分析[4]及相关性增强能量碰撞分析[5]等,从而对密码应用安全造成了严重威胁.

为了使密码芯片具备抵抗能量分析攻击的能力,大量的专用硬件逻辑结构被提出[6~10],并取得了一定的效果.其中,Fraidy Bouesse 等人提出的 QDI 随机路径切换方法[9]利用准延迟非敏感(Quasi-Delay-Insensitive, QDI)逻辑的数据路径对称和平衡[11,12]特性,在保证计

收稿日期:2011-06-08;修回日期:2011-12-13
基金项目:国家自然科学基金(No.91018008);教育部重点项目(No.209156);北京市自然科学基金(No.4102056)

算正确性和可靠性的前提下,能够实现运算逻辑的平均功耗平衡,克服了由于寄生电容及负载电容差异所造成的数据路径功耗差异,具备很好的抗能量分析攻击能力[13].然而,在现有的实现方法中,由于依赖多路复用器和随机数输入的数据路径随机切换机制仍然存在较明显的安全漏洞,其旁路信息泄露的隐患仍然没有被完全消除,使得抗能量分析攻击的能力被极大地削弱.

为了解决以上问题,本文对现有 QDI 随机路径切换方法的抗能量分析攻击能力进行了形式化分析,并就晶体管亚稳态特性在 QDI 随机路径切换中的应用进行了研究,提出并实现了一种不依赖外部随机数输入的亚稳态 QDI 随机路径切换模型.仿真实验表明,该模型具有良好的功耗平衡特性,并能够较好的消除由于寄生电容及负载电容差异所造成的旁路信息泄露,具有很强的抗能量分析攻击能力.

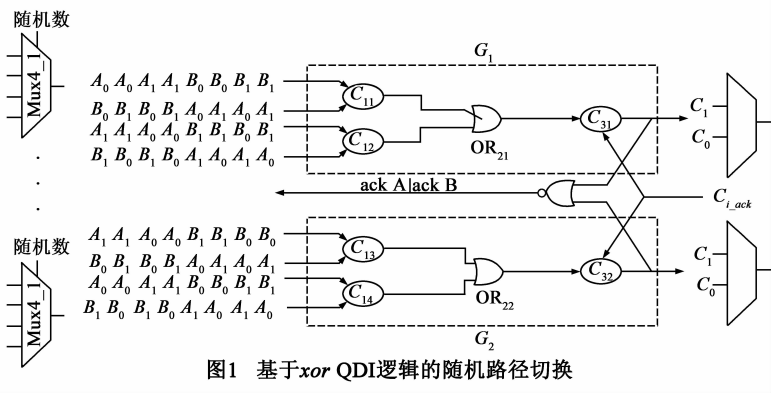


图1　基于*xor* QDI逻辑的随机路径切换

2　Fraidy Bouesse 随机路径切换方法分析

Fraidy Bouesse 等人提出的随机路径切换方法[9],其基本思想是利用 QDI 逻辑的数据路径平衡特性,对数据的双轨编码输入点位置进行随机切换,实现不同输入数据的平均功耗平衡,并最终达到消除处理数据与功耗之间的关联的目的.以 *xor* 逻辑为例,其 QDI 随机路径切换方法如图 1 所示.

在噪声源产生的随机数作用下,多路复用器对输入数据双轨编码组(A_0, B_0)、(A_1, B_1)、(A_0, B_1)、(A_1, B_0)的输入位置进行随机切换,使得在保证计算结果正确的前提下,每个双轨编码位的数据路径等概率的为 4 条数据路径中的任何一条.因此,对于不同的输入数据,*xor* 的平均功耗 $P_{xor\ average}$恒定为 4 条数据路径功耗之和的平均.此外,由于 Fraidy Bouesse 随机路径切换系统的功耗主要由前端多路复用器功耗、QDI 逻辑功耗和后端多路复用器功耗三部分组成,因此图 1 所示的 *xor* QDI 逻辑的系统功耗 P_{sum}为:

$$P_{sum} = P_{f\_mux} + P_{xor} + P_{b\_mux} \tag{1}$$

其中,P_{f_mux}表示前端多路复用器功耗、P_{xor}表示 *xor* QDI 逻辑功耗、P_{b_mux}表示后端多路复用器功耗.

当对图 1 所示的 *xor* QDI 逻辑进行基于均值检验的 DPA 攻击时,假设区分函数为 D,则系统瞬态功耗 P_{ij} 的离散集合可分为两个子集 $P_0 = \{P_{ij}\ D = 0\}$,$P_1 = \{P_{ij}\ D = 1\}$,分别对应 D 等于 0 和 D 等于 1 两种情况.然后计算两个子集的平均功耗 $P_{0_average}$和 $P_{1_average}$之间的偏差.由于系统的功耗由式(1)所示的三部分组成,因此其平均功耗同样由三部分组成:

$$P_{0\_average} = P_{0\_average(f\_mux)} + P_{0\_average(xor)} + P_{0\_average(b\_mux)} \tag{2}$$

$$P_{1\_average} = P_{1\_average(f\_mux)} + P_{1\_average(xor)} + P_{1\_average(b\_mux)} \tag{3}$$

功耗均值偏差 T 为

$$T = (P_{0\_average(f\_mux)} - P_{1\_average(f\_mux)}) + (P_{0\_average(xor)} - P_{1\_average(xor)}) + (P_{0\_average(b\_mux)} - P_{1\_average(b\_mux)}) \tag{4}$$

由于无论输入数据如何变化,*xor* QDI 逻辑的平均功耗恒定为 4 条数据路径功耗之和的平均,也就意味着

$$P_{0\_average(xor)} = P_{1\_average(xor)} \tag{5}$$

$$T = (P_{0\_average(f\_mux)} - P_{1\_average(f\_mux)}) + (P_{0\_average(b\_mux)} - P_{1\_average(b\_mux)}) \tag{6}$$

又由于 *xor* QDI 逻辑的数据路径为随机切换,所以后端多路复用器实际上进行的是等概率路径切换,

$$P_{0\ average(b\_mux)} = P_{1\ average(b\_mux)} \tag{7}$$

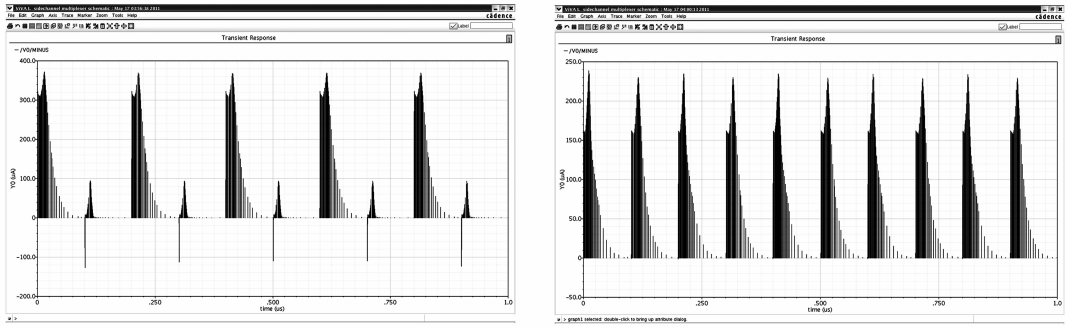
$$T = (P_{0\ average(f\_mux)} - P_{1\ average(f\_mux)}) \tag{8}$$

因此功耗均值偏差 T 实际上由前端多路复用器的平均功耗差异决定.

以静态 CMOS 结构的多路复用器为例,假设 A 为明文输入,B 为攻击者欲获取的秘密信息,并且 $B = 0$.攻击者分别输入明文 $A = 0$ 和 $A = 1$,由于多路复用器的选通信号为外部输入的随机数,多路复用器将等概率的选通 A_0 和 A_1 这两个通道.基于 Spectre6.1 的仿真环境,当 $A = 0$ 时功耗曲线如图 2(a)所示;当 $A = 1$ 时功耗曲线如图 2(b)所示.

由于多路复用器选通两个通道时选通晶体管的数据、类型的不同,以及寄生电容及负载电容的差异,当 $A = 0$ 时功耗曲线中出现了非常明显的尖峰电流,而当 $A = 1$ 时功耗曲线基本均匀.因此,攻击者可以非常容易的猜测出秘密信息 B.此外,由于多路复用器需要利用外部输入的随机数才能够实现随机切换,当攻击者截获、破坏或干扰外部随机数输入时,可达到绕过/屏蔽 QDI 逻辑的数据路径切换机制的目的,从而达到实施能

量分析攻击的目的.



(*a*) A=0,B=0, S_1=0时S_0选通通道A_0和A_1 (*b*) A=1、B=0、S_1=1时S_0选通通道A_0和A_1

图2 前端多路复用器选通时的功耗差异

3 基于亚稳态的 QDI 逻辑随机路径切换

3.1 基于亚稳态的 QDI 两级随机路径切换模型

通过分析图 1 所示的 *xor* QDI 逻辑可以发现,当进行随机路径切换时,对于任何一个双轨编码位 A_i 或 B_i, $P_{G1}=P_{G2}=1/2$, $P_{r1}=P_{r2}=P_{r3}=P_{r4}=1/4$. 其中, P_{G1}、P_{G1}表示某一双轨编码位处于路径组 G_1 或 G_2 的概率, P_{r1}、P_{r2}、P_{r3}、P_{r4}分别表示某一双轨编码位处于 4 条数据路径 $r1$、$r2$、$r3$ 和 $r4$ 的概率. 因此,输入数据的双轨编码组(A_0,B_0)、(A_1,B_1)、(A_0,B_1)、(A_1,B_0)总是在路径组 G_1 和 G_2 间等概率交换,而单个双轨编码位 A_i 或 B_i 则总是在每个路径组中的数据路径间等概率交换.

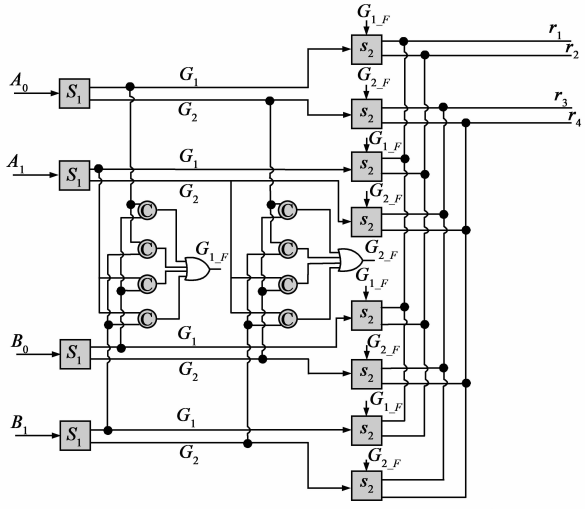


图3 基于亚稳态的QDI两级随机路径切换模型

基于 QDI 随机路径切换的这一特点,本文利用晶体管的亚稳态特性设计了 QDI 随机路径切换模型,以取代前端多路复用器. 在保证 QDI 逻辑数据路径随机切换的前提下,解决路径切换时的功耗差异和外部随机数输入易受攻击等问题. 以 *xor* QDI 逻辑为例,其随机路径切换模型如图 3 所示,主要由 1 级亚稳态路径切换单元 S_1、2 级亚稳态路径切换单元 S_2 和 Muller-C 单元三部分构成.

其中,1 级路径切换单元 S_1 用于对双轨编码位 A_i/B_i 进行数据路径组 G_1/G_2 的选择. 当某个编码位为 1 时,其对应的 S_1 单元被激活,实现对数据路径组 G_1/G_2 的随机选择. 然后,利用 S_2 单元实现路径组内数据路径的随机选择. 与 S_1 单元不同,当$\{A_0,A_1\}$和$\{B_0,B_1\}$中为 1 的编码位选择了同一个路径组时,意味着该路径组的两条数据路径均输入信号 1,此时通过图 3 中的 Muller-C 单元产生 G_{i_F}信号,并在 S_2 单元内直接将该路径组内的两条数据路径输入均置为高电平. 而当$\{A_0,A_1\}$和$\{B_0,B_1\}$中为 1 的编码位选择不同的路径组时,则通过亚稳态机制在各个路径组中随机选择数据路径.

此外,为了防止选择同一个路径组时,由于不同 S_1 单元之间的输出延迟造成的输出跳变,还需利用完成侦测逻辑(Completion detector)对为 1 的编码位的路径组选择情况进行侦测,只有当两个为 1 的编码位均完成了路径组选择时,S_2 单元的亚稳态滤波器才产生输出,图中将该部分电路省略.

3.2 亚稳态随机路径切换单元设计

在 QDI 两级随机路径切换模型中,1 级亚稳态路径切换单元 S_1 和 2 级亚稳态路径切换单元 S_2 均基于双路异步仲裁器[14]的思想进行设计.

1 级亚稳态路径切换单元 S_1 的结构如图 4 所示,由亚稳态产生器及亚稳态滤波器两部分组成,信号 $\overline{G}_1$、$\overline{G}_2$ 的初始值为 1,亚稳态产生器输入 A_i/B_i 为等时分支. 当双轨编码位输入 A_i 或 B_i 为 1 时,S_1 单元被激活,亚稳态产生器的信号 $\overline{G}_1$ 和 $\overline{G}_2$ 被下拉至低电平,同时信号 $\overline{G}_1$ 和 $\overline{G}_2$ 互相试图上拉对方至高电平,从而使得电路进入亚稳态. 此时,由于后端亚稳态滤波器的作用,路径组选择信号 G_0、G_1 的输出仍保持为初始值 0,表示 S_1 单元还没有完成路径组的选择. 经过一段时间后,由于晶体管热噪声及电路噪声等的作用,亚稳态产生器将信号 $\overline{G}_1$ 或 $\overline{G}_2$ 中的某一个信号上拉至高电平,另一个信号下拉至低电平,此时亚稳态滤波器输出最

终的路径组选择结果 G_1 和 G_2.在 S_1 单元的路径组选择过程中,由于亚稳态的退出是由晶体管热噪声和电路内部噪声等造成的,因此最终信号 $\overline{G}_1$、$\overline{G}_2$ 的上拉/下拉是一个完全随机的过程,这也就意味着 S_1 单元的路径组选择结果是随机的.

2级亚稳态路径切换单元 S_2 的结构如图5所示,同样由亚稳态产生器和亚稳态滤波器两部分组成,其与单元 S_1 的主要区别在于亚稳态滤波器的设计.当1级亚稳态路径切换单元 S_1 为{A_0,A_1}和{B_0,B_1}中为1的编码位选择了同一个路径组时,Muller-C单元产生 G_{i_F}信号,并在 S_2 的亚稳态滤波器中直接将该路径组对应的两条数据路径输入均置为高电平.

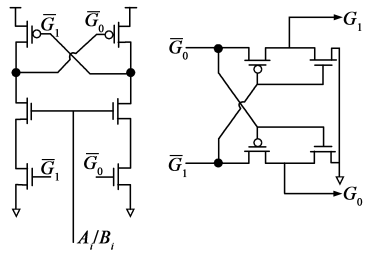


图4　单元S_1逻辑结构

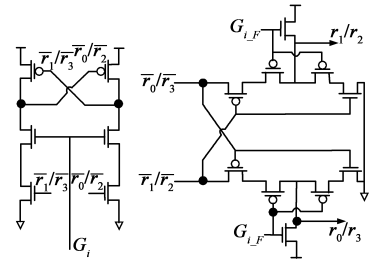
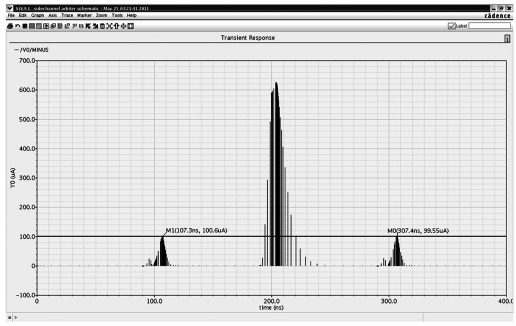


图5　单元S_2逻辑结构

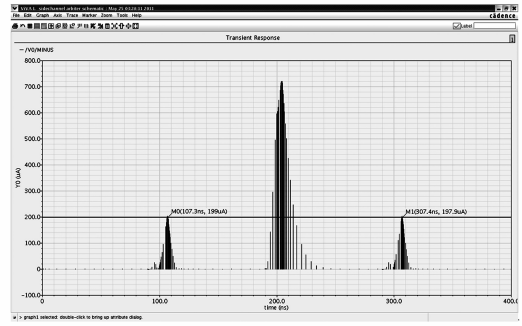
4　仿真实验及结果分析

4.1　实验场景设置

为了分析基于亚稳态的 QDI 两级随机路径切换模型的抗能量分析攻击能力,在忽略输入延迟差异及退出亚稳态延迟差异的前提下,分别针对不考虑寄生电容及负载电容差异和考虑寄生电容及负载电容差异的实验场景,在 Spectre6.1 环境下进行了仿真,结果如图6、图7所示.

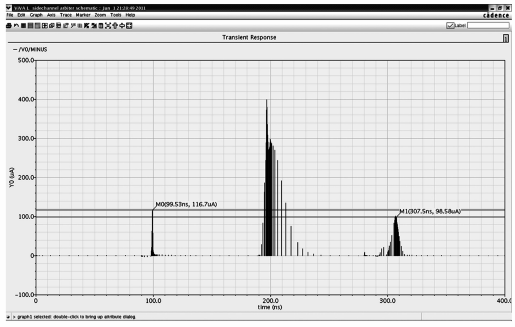


(*a*) *A*、*B*中为1的编码位选择了不同的路径组

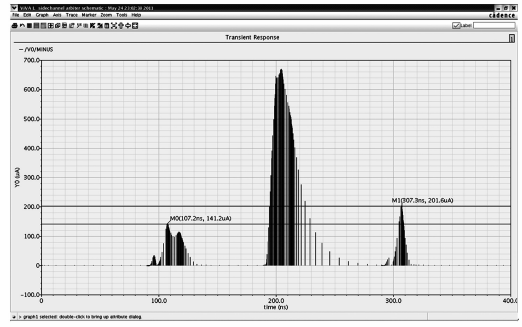


(*b*) *A*、*B*中为1的编码位选择了不同的路径组

图6　不考虑寄生电容及负载电容差异的实验场景



(*a*) *A*、*B*中为1的编码位选择了不同的路径组



(*b*) *A*、*B*中为1的编码位选择了不同的路径组

图7　考虑寄生电容及负载电容差异的实验场景

4.2　安全性分析与评价

通过仿真实验可以发现,在不考虑寄生电容及负载电容差异的情况下,{A_0,A_1}和{B_0,B_1}中为1的编码位选择不同或相同的路径组时,所产生的功耗曲线与选择的具体路径组无关.但由于选择相同的路径组时将触发 Muller-C 单元及完成侦测逻辑,因此选择相同的路径组时的尖峰电流值要明显的大于选择不同的路径组时的尖峰电流值,如图6所示.假设不考虑寄生电容及负载电容差异的情况下选择相同路径组时的功耗为 P_{sam},选择不同路径组时的功耗为 P_{dif},并且 $P_{sam} > P_{dif}$,则攻击者能够通过功耗分析判断出,当前随机路径切换模块是否选择的是相同的路径组.然而,由于路径组的选择是随机的,概率均为1/2,因此攻击者不能够从 P_{sam}与 P_{dif}的功耗差异中获取任何有用信息.

在考虑寄生电容及负载电容差异的情况下,随着差异的增大不同路径组的选择将产生较为明显的功耗

差异,如图 7 所示.以图 7(a)为例,A_0 选择路径组 G_1 时的尖峰电流值为 116.7uA,大于 B_1 选择路径组 G_2 时的尖峰电流值 98.58uA.然而,在实际情况中,由于亚稳态退出的时间延迟是随机的,也就意味着两个为 1 的编码位完成路径选择的时机是任意的,使得各个 S_1 单元和 S_2 单元的功耗以随机的方式分布在功耗曲线上.

此外,随机路径切换模块在设计时并没有进行任何延迟假设,这就意味着两个为 1 的编码位开始路径选择的时机是任意的,加之每个为 1 的编码位能够随机的在两个路径组间进行选择,使得 A、B 间任何一个编码位的组合均存在多种功耗情况.例如对于编码位 A_1 与 B_0 的组合,设 A_1 选择路径组 G_1、G_2 的功耗分别为 P_{A1_G1}和 P_{A1_G2},B_0 选择路径组 G_1、G_2 的功耗分别为 P_{B0_G1}和 P_{B0_G2},则编码位 A_1 与 B_0 的组合根据其到达随机路径选择模块的时机和最终所选择的路径组,存在 12 种功耗情景.因此,由于亚稳态退出的时间延迟的随机性以及编码位组合所产生的功耗情景复杂性,功耗均值偏差 T 被极大的削弱[15],使其很难和电路噪声相区分,并且攻击者也难以寻找到一种有效的方法将不同明文输入所产生的功耗曲线利用区分函数进行分类,从而使得实施能量分析攻击非常困难.

综上所述,基于亚稳态的随机路径切换模块在实现数据路径随机切换的前提下,提供了很强的抗能量分析攻击能力,而在实际实现中如果通过布局布线过程的处理降低寄生电容和负载电容差异,将进一步提升其安全性.

5 结论

围绕 QDI 逻辑抗能量分析攻击问题,本文提出并实现了一种基于晶体管亚稳态特性的 QDI 两级随机路径切换模型.该随机路径切换模型在实现数据路径随机切换时不需要外部的随机数输入,降低了设计的成本和复杂度.此外,该随机路径切换模型具有良好的功耗平衡特性和很强的抗功耗攻击分析能力,对于实现具备高等级抗能量分析攻击能力的密码电路具有重要意义.

参考文献

[1] P Kocher. Timeing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[A]. Advances in Cryptology′96 [C]. LNCS 1109, California: Springer-Verlag, 1996. 104 – 113.

[2] T S Messerges, E A Dabbish, R H Sloan. Investigations of power analysis attacks on smartcards [A]. Proc USENIX Workshop Smartcard Technology[C]. Chicago USA, 1999. 151 – 161.

[3] P Kocher, J Jaffe, B Jun. Differential power analysis[A]. Advances in Cryptology′99[C], LNCS 1666, Singapore, 1999. 388 – 397.

[4] K Itoh, T Izu, M Takenaka. Address-bit differential power analysis of cryptographic schemes OK-ECDH and OK-ECDSA [A]. CHES 2002 [C]. LNCS 2523, San Francisco Bay: Springer-Verlag, 2002. 129 – 143.

[5] A Moradi, O Mischke, T Eisenbarth. Correlation-Enhanced Power Analysis Collision Attack[A]. CHES 2010[C]. LNCS 625, Santa Barbara, California: Springer-Verlag, 2010. 125 – 139.

[6] K Tiri, I Verbauwhede. A Digital Design Flow for Secure Integrated Circuits[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2006, 25(7): 1197 – 1208.

[7] K Tiri, D Hwang, A Hodjat, B C Lai, S Yang, P Schaumont, I Verbauwhede. Prototype IC with WDDL and Differential Routing-DPA Resistance Asssessment[A]. CHES 2005[C]. LNCS 3659, Edinburgh: Springer-Verlag, 2005. 354 – 365.

[8] M Bucci, L Giancane, R Luzzi, A Trifiletti. Three-Phase Dual-Rail Pre-charge Logic [A]. CHES 2006 [C]. LNCS 4249, Yokohama Japan: Springer-Verlag, 2006. 234 – 241.

[9] G F Bouesse, G Sicard, M Renaudin. Path Swapping Method to Improve DPA Resistance of Quasi Delay Insensitive Asynchronous Circuits[A]. CHES 2006[C]. LNCS 4249, Yokohama Japan: Springer-Verlag, 2006. 384 – 398.

[10] 乐大珩,张民选,李少青,孙岩,谷晓忱.一种新型的抗 DPA 攻击可配置逻辑结构[J].电子学报,2011,39(02):453 – 457.
YUE Da-heng, ZHANG Min-xuan, LI Shao-qing, SUN Yan, GU Xiao-chen. A Novel DPA-Resisance Configurable Logic [J]. Acta Electronica Sinica, 2011, 39(02): 453 – 457. (in Chinese)

[11] S Moore, R Anderson, P Cunningham, R Mullins, G Taylor. Improving Smart Card Security using Self-timed Circuits[A]. Eighth International Symposium on Asynchronous Circuits and systems(ASYNC 2002)[C]. Manchester, 2002. 8 – 11.

[12] G F Bouesse, M Renaudin, S Dumont, F Germain. DPA on Quasi Delay Insensitive Asynchronous Circuits: Formalization and Improvement [A]. DATE′05 [C]. Munich Germany, 2005. 126 – 134.

[13] J Jaffe, P Kocher, B Jun. Balanced Cryptographic computational mehtod and apparatus for leak minimization in smartcards and others Cryptosystems [DB/OL]. EP1088295/WO9967766.

[14] C L Seitz. System timing[A], in Introduntion to VLSI System [C], C A. Mead and L A. Conway, eds. Addison-Wesley, 1980. 360 – 420.

[15] G F Bouesse, M Renaudin, G Sicard. Improving DPA resis-

tance of Quasi Delay Insensitive Circuits using randomly time-shifted Aknowledgement Signals[A]. Communication to VLSISOC'05[C], Perth Australia: Springer-Verlag, 2005. 187 – 198.

作者简介

欧庆于　男,1978 年生于江西靖安,现为武汉大学计算机学院博士生,海军工程大学信息安全系讲师,主要研究领域为异步电路设计、旁路攻击防御.
E-mail: ouqingyv@sina.com

张焕国　男,1945 年生于河北,武汉大学计算机学院教授、博士生导师,主要研究领域为密码学与信息安全理论与技术.
E-mail: liss@whu.edu.cn

吴晓平　男,1961 年 5 月生于山西新绛.海军工程大学信息安全系主任、教授、博士生导师.主要研究领域为信息安全、系统决策.
E-mail: wxp8@souhu.com.cn

李凤华　男,1966 年 3 月出生于湖北省浠水县,中国科学院信息工程研究所研究员、博士、博士生导师,主要研究领域为网络安全与可信计算.
E-mail: lfh@besti.edu.cn

罗　芳　女,1983 年 2 月出生于江西吉安,海军工程大学信息安全系讲师,主要研究领域为流密码、密码安全性分析.