一种新型的抗 DPA 攻击可配置逻辑结构

乐大珩,张民选,李少青,孙 岩,谷晓忱
(国防科技大学并行与分布处理国防科技重点实验室,湖南长沙 410073)

摘 要: DPA(Differential Power Analysis)攻击的强度取决于芯片电路功耗与所处理的数据之间的相关性以及攻击者对算法电路实现细节的了解程度.本文结合动态差分逻辑和可配置逻辑的特点,提出了一种具有抗 DPA 攻击能力的双端输出可配置逻辑(DRCL:Dual-Rail Configurable Logic).该逻辑一方面具有与数据取值无关的信号翻转率和信号翻转时刻,因而能够实现很好的功耗恒定特性;另一方面去除了电路结构与电路功能之间的相关性,从而可以阻止攻击者通过版图逆向分析的方法窃取算法电路实现细节.实验结果表明,DRCL 比典型的抗 DPA 攻击逻辑 WDDL(Wave Dynamic Differential Logic)具有更好的功耗恒定性,因而具有更强的 DPA 攻击防护性能.

关键词: 安全芯片; 旁路攻击; 功耗分析攻击; 动态差分逻辑; 可配置逻辑
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2011) 02-0453-05

A Novel DPA-Resistance Configurable Logic

YUE Da-heng, ZHANG Min-xuan, LI Shao-qing, SUN Yan, GU Xiao-chen
(*Parallel and Distributed Processing Laboratory*, *National University of Defense Technology*, *Changsha*, *Hunan* 410073, *China*)

Abstract: The efficiency of Differential Power Analysis (DPA) depends on the correlation between power consumption and data value, as well as the attacker's understanding of circuit details. To counteract DPA attack, this paper presents a novel logic, Dual-Rail Configurable Logic (DRCL), which combines the characteristics of dynamic differential logic and configurable logic. The DRCL has constant power consumption which is independent of the data value. At the same time, the uniform structure of DRCL prevents attackers from revealing circuit details by layout reverse analysis. The experimental results show that the proposed logic DRCL has better power constant than the typical DPA resistant logic WDDL.

Key words: security chip; side channel attack; differential power analysis; dynamic differential logic; configurable logic

1 引言

传统的安全芯片设计通常以电路性能、功耗和面积等方面作为主要优化目标,如文献[1]提出一种可高速实现 DES、3DES 和 AES 算法的可重构体系结构,文献[2]提出一种面积优化的 S 盒组合逻辑电路设计方法.然而,自从以差分功耗分析(Differential Power Analysis,简称 DPA)技术[3]为代表的旁路攻击技术出现以后,作为密码算法执行载体的安全芯片本身的安全性也是设计者需要关注的重要问题.有研究指出在物理可观测条件下,旁路攻击可以在多项式时间内获取算法密钥[4],这对安全芯片造成了重大威胁.

分析 DPA 攻击技术的特点可知其实施效率除了受电路功耗与处理数据之间相关性的强弱程度影响外,还取决于攻击者对算法电路实现细节的了解程度.比如在掌握算法电路流水线结构的情况下,DPA 攻击者就可能通过更少的功耗样本窃取算法密钥[5].而且当攻击者对电路结构足够了解时,甚至能够攻击某些采用了防护技术的密码算法[6].而对于非公开的密码算法,攻击者也可以首先通过版图逆向分析技术窃取密码算法实现细节[7],为后续的 DPA 攻击提供支持.因此,针对安全芯片,尤其是采用非公开加密算法的安全芯片,需要从去除电路功耗相关性和隐藏芯片电路实现细节两个方面展开防护.由此,本文提出了一种具有动态差分逻辑特点的双端输出可配置逻辑结构(DRCL:Dual-Rail Configurable Logic).一方面通过逻辑单元的功耗恒定特性减小电路功耗与数据的相关性;另一方面利用可配置逻辑单元的结构特点阻止攻击者通过版图逆向分析窃取密码算法实现细节.实验结果表明,DRCL 逻辑解决了已有动态差分逻辑中逻辑门翻转时刻与输入信号取值的相关性问题,因而具有更好的抗 DPA 攻击性能.

收稿日期:2009-05-22;修回日期:2010-10-12
基金项目:国家自然科学基金(No.60970036);国家 863 高技术研究发展计划(No.2009AA01Z124)

2 基于动态差分逻辑的防护技术

动态差分逻辑是一种具有差分输入、输出引脚的动态逻辑,通过使单元功耗特征恒定的方式去除电路功耗与信号的相关性.在预充电阶段,电路中所有的差分信号都被充电(或是放电)到相同的电平.而在求值阶段,每对差分信号通过互补的电平表征信号逻辑值.这样,在每个时钟周期无论动态差分逻辑的输出是否有逻辑值变化,其差分输出端都有且仅有一次信号翻转,从而实现与信号取值无关的信号翻转率.在这种情况下,只要能保证单元正、负输出端具有对称的电容负载就可以实现与信号取值无关的恒定功耗特性.基于这一思想,研究者提出了多种动态差分逻辑的实现结构[8~14].

在已有的动态差分逻辑中,Kris Tiri 等人提出的 WDDL(Wave Dynamic Differential Logic)利用普通的标准单元构成,且引入了行波预充电思想[9].这样大大简化了 WDDL 电路的设计复杂性,使其成为最早实现原形芯片并经过 DPA 攻击验证的逻辑结构[11],图 1 显示了 WDDL 的基本原理.每个 WDDL 逻辑单元包含一对 AND-OR 逻辑门,根据德·摩根定律,两个逻辑门分别接收输入信号的正、负逻辑值,并产生相应的互补逻辑输出.以二输入 AND 逻辑单元为例,z 端输出 AND 逻辑值,即 $z = a \cdot b$.而 $\bar{z}$ 端输出 NAND 逻辑值,即 $\bar{z} = \bar{a} + \bar{b} = \overline{a \cdot b}$.WDDL 实现行波预充电的原理在于每个 WDDL 单元都是由 AND-OR 逻辑门构成,当这两种逻辑门的输入端信号都为"0"时,其输出信号也都为"0".这样,在前级单元进入预充电状态后,其互补的两个输出端同时输出"0"信号,这使得其扇出的后级单元也进入预充电状态.因此,只要在电路的初级输入端插入能产生全"0"信号的预充电逻辑,如图 1 中左图所示,就可以将预充电状态像行波一样在组合电路中传播.

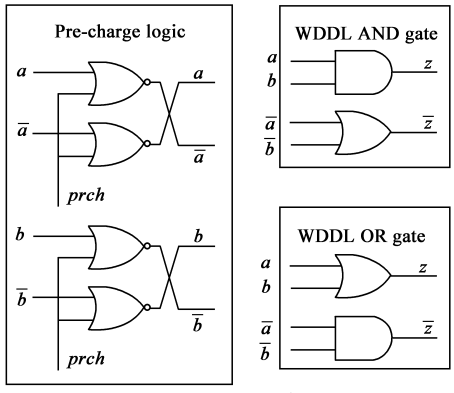

图1 WDDL逻辑

在 WDDL 以及其他类似的动态差分逻辑中,研究者大多忽略了单元翻转时刻与输入信号取值之间的相关性.表 1 列出了 WDDL 的 AND 逻辑单元在不同输入情况下的单元翻转时刻.从中可以看出,当两个输入端 a 和 b 的信号传输延迟 t_a、t_b 不相等时,单元的翻转时刻会因为输入逻辑值的不同而不同.Suzuki 在文献[15]中分析了输入信号到达时间差异对动态差分逻辑功耗恒定性的影响,指出逻辑门翻转时刻与数据取值的相关性同样可能造成安全芯片信息的泄漏.本文在 3.2 节中也通过对模型电路的 SPICE 模拟验证了这一结论.

表 1 WDDL AND 逻辑门跳变时间

Input		Evaluation Phase				Pre-Charge Phase			
a	b	q	Timing	$\bar{q}$	Timing	q	Timing	$\bar{q}$	Timing
0	0	0	–	1	t_a	0	–	1	t_b
0	1	0	–	1	t_a	0	–	1	t_a
1	0	0	–	1	t_b	0	–	1	t_b
1	1	1	t_b	0	–	1	t_a	0	–

3 双端输出可配置逻辑

3.1 基本单元

可配置逻辑单元是广泛应用于 FPGA 芯片中的核心功能单元,其中基于 LUT 结构的可配置逻辑单元使用最为广泛,如图 2 所示.其基本原理是将逻辑单元需要实现的函数真值表存储于 LUT 的存储单元(RAM)中,在单元工作时根据输入的信号值选择对应的函数输出.因此逻辑单元所实现的功能仅由存储单元中存储的逻辑值决定,而与单元的电路结构无关.对于采用可配置逻辑单元实现的集成电路,即使攻击者通过侵入式攻击窃取到芯片的版图,也无法通过版图逆向分析技术窃取电路结构.因此,基于 LUT 结构的可配置逻辑单元具有良好的抗版图逆向分析特性.

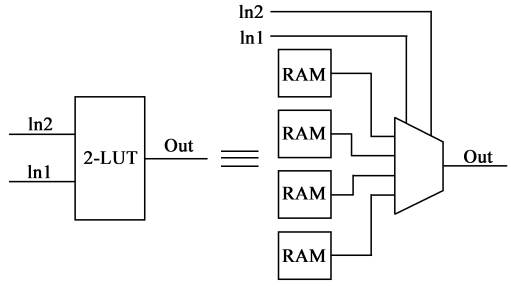

图2 二输入LUT结构

普通的可配置逻辑单元结构与 CMOS 逻辑一样采用静态单端输出的工作模式,这使其与 CMOS 逻辑一样容易泄露功耗信息[5].因此,本文提出 DRCL 逻辑结构,能够实现动态差分逻辑的功耗恒定特性.图 3 所示是二输入 DRCL 单元的电路结构,其具有两个特征:首先,每个 SRAM 单元的正、负输出信号同时经过由 NMOS 晶体管构成的多路选择器连接到单元的正、负输出端,实现求值阶段的差分输出;其次,由 PMOS 晶体管构成的预充电逻辑实现类似 WDDL 中的行波预充电操作.因此,单元的差分输出端就具有如公式(1)所示的函数功能,公式中的 $f(a,b)$ 代表单元所配置的逻辑功能.这样,在

每个时钟周期无论单元的逻辑值是否变化,其差分输出端都有且仅有一次信号翻转.而从图 3 中可见两个差分输出端具有完全对称的结构,因此,正、负输出端在发生信号翻转时消耗相同的功耗.由此可实现 DRCL 单元与信号逻辑值无关的恒定功耗特征.

$$q=\begin{cases}f(a,b), & \text{eval}\\ 0, & \text{prech}\end{cases}$$
$$\bar{q}=\begin{cases}f(a,b), & \text{eval}\\ 0, & \text{prech}\end{cases}\qquad(1)$$

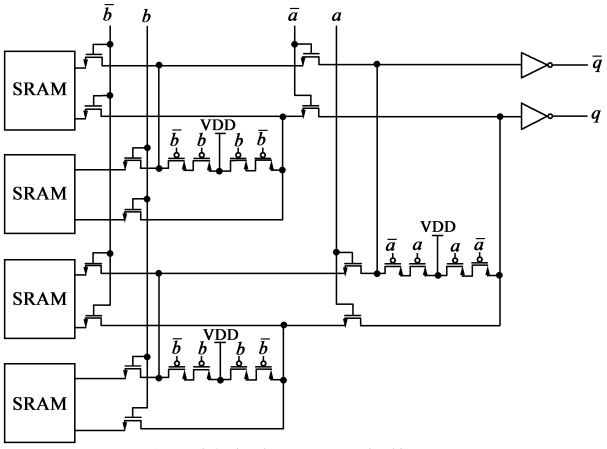

图3　功耗恒定可配置逻辑单元

与 WDDL 中利用 AND-OR 逻辑门的功能特性实现行波预充电行为的方式不同,DRCL 的预充电操作是由专门的预充电逻辑实现.在预充电阶段,由前级输入的预充电“0”信号将单元中的 PMOS 管打开,从而将多路选择器中所有的内部节点都充电到 VDD,并经过反相器输出预充电“0”信号使后级的逻辑单元也进入预充电状态.这样,不论 DRCL 单元被配置为何种逻辑功能都可以保证预充电状态在组合逻辑中正常传递.同时,由于多路选择器的所有内部节点都会被预充电到 VDD,这就避免了单元毛刺信号的产生,从而消除了由毛刺信号引起的功耗信息泄露.

3.2　功耗恒定性分析

相对于 WDDL 等其他的动态差分逻辑,DRCL 的优点在于消除了单元翻转时刻与输入信号取值的相关性.这是因为 DRCL 单元中的多路选择器只会等到最晚的输入信号到达后才将输出函数值传递到单元输出端.为了验证第二节中功耗分析的正确性,我们通过 SPICE 模拟对 DRCL 和 WDDL 的功耗恒定性进行了分析比较.所采用的模型电路是 8 个两输入的 AND 逻辑电路,并且通过在电路输入端添加延迟逻辑使 t_a 小于 t_b,如图 4 所示.

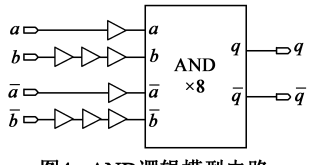

图4　AND逻辑模型电路

图 5 显示了两种 AND 逻辑电路在 b 信号为随机信号下,a 信号分别取值“0”和“1”时的平均工作电流,电流曲线的前半段是预充电阶段而后半段是求值阶段.从图中可以明显看出,由于 a 信号取值的不同,WDDL 的电流曲线在求值阶段的相位和峰值都存在明显差异.而对于 DRCL,由于 AND 逻辑单元的输出信号翻转时刻不随输入信号的取值而变化,因此在图中两条电流曲线几乎完全一致.

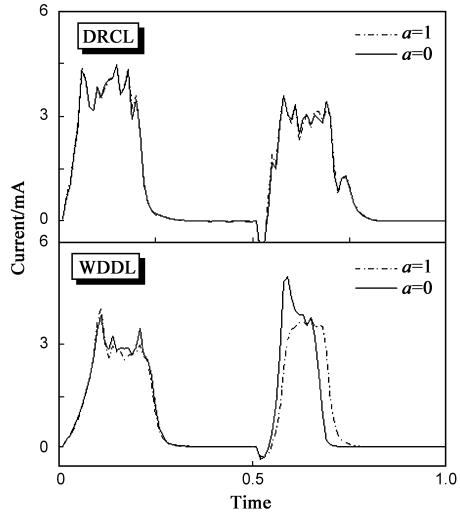

图5　AND逻辑电流曲线

图 6 显示了当 a 信号分别为“0”和“1”时电路的差分电流,从中可以看出 WDDL 差分电流的峰值达到了 2.89mA 而 DRCL 逻辑只有 0.33mA.由此可见,本文提出的 DRCL 逻辑单元具有非常优异的功耗恒定特性.

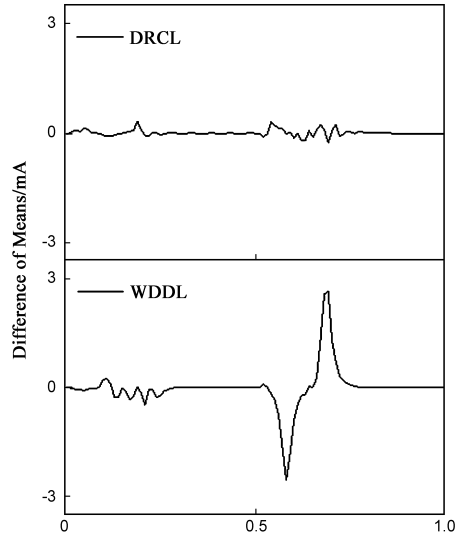

图6　AND逻辑差分电流

4　模拟 DPA 攻击结果

为了验证 DRCL 单元在实际电路中的抗 DPA 攻击能力,我们采用 DRCL、WDDL 和普通 CMOS 标准单元分

别设计实现了如图 7 所示的模型电路并进行了模拟 DPA 攻击. 在实际的 AES 算法电路中,最后一轮变换操作由 16 个上述电路并行执行,因此 DPA 攻击者可以针对每 8 位密钥分别进行猜测攻击. 由此可见,利用此模型电路进行抗 DPA 攻击能力分析具有实际意义. 而将算法电路作此简化是为了能够实现晶体管级的 SPICE 模拟,以得到精确的电路功耗. 此外,模型电路还省略了 AES 算法中的 ShiftRow 操作,因为在硬件中 ShiftRow 操作是通过交换信号线连接顺序实现的,对 DPA 攻击结果不会产生影响. 模型电路采用 0.18μm 工艺实现,其中普通标准单元版本是通过 Design Compiler 工具自动综合实现,而 WDDL 版本和 DRCL 版本采用全定制方式设计实现. 为了评估信号传输延时差异对电路抗 DPA 攻击性能的影响,两个全定制设计的模型电路中都具有与图 4 相似的电路结构.

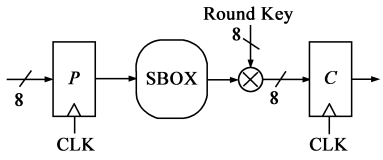

图7 DPA攻击模型电路

我们采用了与文献[16]中相同的方法对三个模型电路进行抗 DPA 攻击性能分析. 其中,加密操作使用 84 作为轮密钥,所选择的分析目标函数为输入数据的第 3 位. 模拟采用的时钟频率为 125MHz,每个时钟周期采样 400 个瞬态电流数据. 图 8 所示为加密操作样本数为 2000 时的 DPA 攻击结果,横坐标为穷举猜测的 256 个密钥值. 对于普通逻辑实现的模型电路,在正确的密钥猜测值(84)处,差分电流表现出了明显的尖峰. 采用 WDDL 逻辑实现的模型电路也表现出了与正确密钥对应的差分电流尖峰,这是因为电路中存在信号翻转时刻与输入信号取值相关的逻辑结构. 而采用 DRCL 逻辑实现的模型电路在 2000 个加密操作后差分电流没有表现出明显的尖峰.

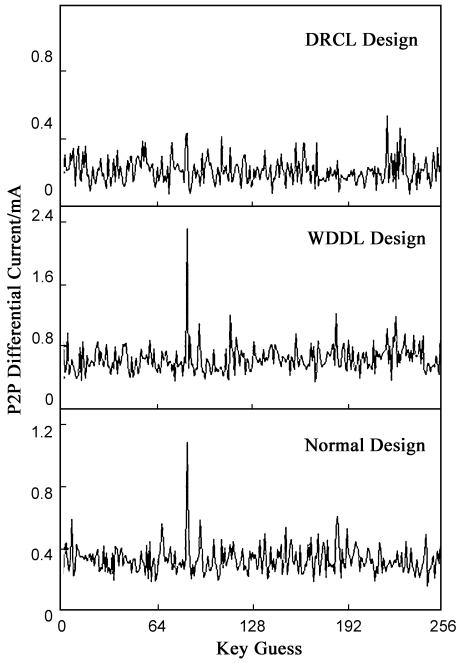

图8 DPA攻击结果

我们采用成功实施 DPA 攻击所需的功耗采样数量(MTD: Measurements to Disclosure)[17]来评估电路的抗 DPA 攻击能力. 图 9 显示了随着加密操作次数的增加,各种密钥猜测值所对应的差分电流峰-峰值的变化情况,其中黑色曲线对应正确密钥猜测值的分析结果而其他曲线对应错误的密钥猜测值. 从图中可以看出,不论是普通标准单元实现的电路还是 WDDL 实现的电路,当 DPA 样本数大于 400 以后正确密钥的差分电流峰-峰值都明显区别于错误密钥. 也即是说在模拟的 DPA 攻击中,攻击者只需要对电路实施 400 次加密操作就可以攻击成功. 而对于采用 DRCL 逻辑实现的模型电路,在 2000 个 DPA 样本下攻击者仍然无法破解出算法密钥. 由此可见,WDDL 仍然存在被 DPA 攻击的威胁,而 DRCL 由于在保证信号翻转率恒定的同时还去除了单元翻转时刻与输入取值的相关性,因而具有更强的 DPA 防护能力.

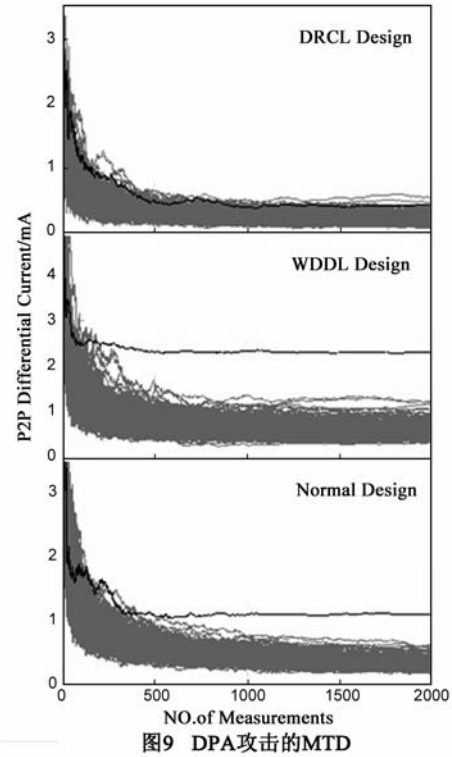

图9 DPA攻击的MTD

5 结论

本文提出了一种具有功耗恒定特性的双端输出可配置逻辑单元(DRCL). 相对于典型的抗 DPA 攻击逻辑 WDDL,DRCL 逻辑的优点在于其逻辑单元的信号翻转

时刻与输入信号取值无关,从而能够解决 WDDL 逻辑中存在的 DPA 攻击隐患.模拟结果表明,DRCL 实现的密码算法电路能够有效地防护 DPA 攻击.DRCL 逻辑的另一个优点是通过可配置逻辑单元的结构均一性阻止攻击者通过版图逆向分析的方式窃取密码算法的实现细节,对于安全芯片的 DPA 防护具有积极意义.由于采用了可配置逻辑结构,DRCL 单元相比于其他逻辑占据了更大的面积.为了尽量降低面积开销,在设计安全芯片时 DRCL 可仅用于实现密码算法中的关键模块.

参考文献:

[1] 高娜娜,李占才,王沁.一种可重构体系结构用于高速实现 DES、3DES 和 AES[J].电子学报,2006,34(8):1386 – 1390.
Gao Na-na, Li Zhan-cai, Wang Qin. A reconfigurable architecture for high-speed implementations of DES, 3DES and AES [J]. Acta Electronica Sinica, 2006, 34(8): 1386 – 1390. (in Chinese)

[2] 王沁,梁静,齐悦.一种有效缩减 AES 算法 S 盒面积的组合逻辑优化设计[J].电子学报,2010,38(4):939 – 942.
Wang Qin, Liang Jing, Qi Yue. The area optimized implementation of S-box in AES algorithm[J]. Acta Electronica Sinica, 2010,38(4):939 – 942. (in Chinese)

[3] P. Kocher, J. Jaffe, B. Jun. Differential power analysis[A]. Advances in Cryptology-CRYPTO'99: 19th Annual International Cryptology Conference [C]. Santa Barbara, CA, USA: Springer-Verlag, 1999. 388 – 397.

[4] 陈开颜,张鹏,邓高明,赵强.物理可观测下 DES 的安全性研究[J].电子学报,2009,37(11):2389 – 2396.
Chen Kai-yan, Zhang Peng, Deng Gao-ming, Zhao Qiang. Research on the DES physical observable security[J]. Acta Electronica Sinica, 2009, 37(11): 2389 – 2396. (in Chinese)

[5] F-X Standaert, S B Ors, B Preneel Power analysis of an FPGA implementation of Rijindael: Is pipelining a DPA countermeasure? [A]. Cryptographic Hardware Embedded System-CHES 2004[C]. Boston: Springer-Verlag, 2004. 30 – 44.

[6] S Mangard, N Pramstaller, E Oswald. Successfully attacking masked AES hardware implementations [A]. Cryptographic Hardware Embedded System-CHES 2005[C]. Edinburgh, UK: Springer-Verlag, 2005. 157 – 171.

[7] O Kommerling, M G Kuhn. Design principles for tamper-resistant smartcard processor [A]. The USENIX Workshop on Smartcard Technology-Smartcard 1999[C]. Chicago: USENIX Association, 1999. 9 – 20.

[8] K Tiri, M Akmal, I Verbauwhede. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards[A]. European Solid-State Circuit Conference-ESSCIRC 2002[C]. Firenze, Italy: University of Bologna, 2002. 403 – 406.

[9] K Tiri, I Verbauwhede. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation[A]. Design, Automation, and Test in Europe Conference-DATE 2004 [C]. Paris, France: IEEE Computer Society, 2004. 246 – 251.

[10] K Tiri, I Verbauwhede. Place and route for secure standard cell design[A]. 6th International Conference on Smart Card Research and Advanced Applications-CARDIS 2004 [C]. Toulouse, France: Springer-Verlag, 2004. 143 – 158.

[11] K Tiri, D Hwang, A Hodjat, B-CLai, S Yang, P Schaumont, I. Verbauwhede. Prototype IC with WDDL and differential routing DPA resistance assessment[A]. Cryptographic Hardware Embedded System-CHES 2005[C]. Edinburgh, UK: Springer-Verlag, 2005. 354 – 365.

[12] F Mace, F-X Standaert, I Hassoune, J-D Legat, J-J Quisquater. A dynamic current mode logic to counteract power analysis attacks[A]. 19th International Conference on Design of Circuits and Integrated Systems-DCIS 2004[C]. Bordeaux, France, 2004. 186 – 191.

[13] T Popp, S Mangard. Masked dual-rail pre-charge logic: DPA-resistance without routing constraints[A] Cryptographic Hardware Embedded System-CHES 2005 [C]. Edinburgh, UK: Springer-Verlag, 2005. 172 – 186.

[14] M Bucci, L Giancane, R Luzzi, A Trifiletti. Three-phase dual-rail pre-charge logic[A] Cryptographic Hardware Embedded System-CHES 2006[C]. Yokohama, Japan: Springer-Verlag, 2006. 232 – 241.

[15] D Suzuki, M Saeki. Security evaluation of DPA countermeasures using dual-rail pre-charge logic style[A]. Cryptographic Hardware Embedded System-CHES 2006 [C]. Yokohama, Japan: Springer-Verlag, 2006. 255 – 269.

[16] K Tiri, I Verbauwhede. A VLSI design flow for secure side-channel attack resistant ICs[A]. Design, Automation, and Test in Europe Conference-DATE 2005[C]. Munich, Germany: IEEE Computer Society, 2005. 58 – 63.

[17] K Tiri, I Verbauwhede. Simulation models for side-channel information leaks [A]. Design Automation Conference-DAC 2005[C]. San Diego, CA, USA: ACM 2005. 228 – 233.

作者简介:

乐大珩　男,1980 年生于四川乐山,国防科学技术大学计算机学院博士研究生,主要研究方向为微电子与 VLSI 设计、抗旁路攻击的密码算法集成电路设计实现.
E – mail: yuedaheng@nudt.edu.cn