北京大学学报(自然科学版), 第 50 卷, 第 4 期, 2014 年 7 月
Acta Scientiarum Naturalium Universitatis Pekinensis, Vol. 50, No. 4 (July 2014)
doi: 10.13209/j.0479-8023.2014.097

基于 FPGA 平台的电路级抗差分功耗分析研究

黄颖　崔小欣†　魏为　张潇　廖凯　廖楠　于敦山

北京大学信息科学技术学院微电子学研究院, 北京 100871; †通信作者, E-mail: cuixx@pku.edu.cn

摘要　研究 DPA 攻击方法以及相应的电路级防护技术, 提出在 FPGA (现场可编程门阵列)上实现 WDDL 的设计方法以及适用于 FPGA 的对称布线技术, 随后在 FPGA 平台上实现一个 4 位加法器并进行功耗分析。实验结果表明, WDDL 电路的功耗波动比普通电路有较明显的下降。WDDL 结构以一定的芯片面积为代价, 可有效降低 FPGA 功耗与数据的相关性, 具有较好的抗 DPA (差分功耗分析)攻击性能。

关键词　差分功耗分析(DPA); WDDL; 对称布线; FPGA

中图分类号　TN47

Research on DPA Resistant Circuit for FPGA

HUANG Ying, CUI Xiaoxin†, WEI Wei, ZHANG Xiao, LIAO Kai, LIAO Nan, YU Dunshan

Institute of Microelectronics, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871;
† Corresponding author, E-mail: cuixx@pku.edu.cn

Abstract　The authors studied the DPA attack method and circuit level protection technology, and introduced a security circuit WDDL on FPGA and a new symmetrical routing technology. A 4-bit WDDL adder on FPGA (field programmable gate array) platform was implemented and the power consumption of the circuit was analyzed. The results show that power consumption of WDDL decreases obviously than that of the traditional circuit and WDDL circuit can reduce the correlation of power consumption and data effectively. WDDL is proved to have better anti DPA (differential power analysis) attack ability at the cost of chip size.

Key words　DPA; WDDL; symmetrical routing; FPGA

近年来, 互联网的高速发展彻底改变了人们的生活。电子邮件、网络购物、网上银行等, 成为人们日常生活中的重要部分, 同时信息安全问题也日益突出。因此, 人们运用密码学的方法来保护隐私数据。目前密码算法大致分为两类: 以 DES, AES 为代表的对称算法和以 RSA, ECC 为代表的非对称算法。通常加密算法需要高速地处理大量数据, 因此加密函数通常用专用硬件实现, 现场可编程门阵列(field programmable gate array, FPGA)因其低成本、高性能、可编程的特点被广泛应用于安全领域。

任何密码系统都必须面对如何防御攻击的问题。传统的攻击方法是一种数学手段, 通过大量计算来搜索密钥。强力攻击是一个典型的例子: 尝试所有可能的密钥, 直至找到正确密钥。但是这种方法的攻击难度会随着密钥长度的增加几何增加。差分功耗分析(differential power analysis, DPA)[1]是一种快速、低成本的密码芯片攻击技术, 可以有效获取密码芯片的关键数据和密钥, 对密码芯片构成严重的挑战。

DPA 的攻击思路是以电路功耗为基础, 利用功耗与数据的关系, 猜测得到正确密钥。因此, 进行 DPA 攻击的根本原因是由电路与逻辑的不对称引起的。本文利用 FPGA 的结构特点, 结合目前抗 DPA 攻击的技术以及对称布线技术, 研究 FPGA 平台抗 DPA 攻击的电路级防护技术——WDDL (wave dynamic differential logic)。

1　差分功耗分析

1.1　FPGA 芯片功耗分析

目前 FPGA 主要分为 3 类: 基于 SRAM 的查

收稿日期: 2013–04–05; 修回日期: 2014–02–18; 网络出版日期: 2014–07–13

找表结构、基于多路开关的反熔丝以及近几年兴起的基于 FLASH 的 FPGA。FLASH 结构尚未普及; 反熔丝结构价格昂贵, 多用于军工领域; 基于 SRAM 的 FPGA 因其低成本、高灵活性, 在民用领域应用非常广泛。以 Xilinx 公司 Virtex-2P 系列芯片为例, 该类芯片主要由可配置逻辑块(configurable logic block, CLB)、I/O 块、Block Ram、DCM 和可编程连线等组成。其中 CLB 是 FPGA 可编程的关键, 一个 CLB 包含两个 slices, 每个 slice 内有两个 4 输入 LUT (looking up table)、两个触发器以及多路器等相关逻辑。用 HDL 语言完成逻辑电路后, FPGA 开发软件会将它映射成 FPGA 的基本单元, 完成 CLB 配置以及布局布线, 最终下载至 FPGA 芯片。

从工艺上看, SRAM 结构的 FPGA 基本采用 CMOS 技术, 因此该类型的 FPGA 的功耗主要分为静态功耗和动态功耗两部分。静态功耗由泄露电流引起, 动态功耗是由于电路状态转换, 对负载进行充放电造成的。此外, 还会有部分短路功耗。

大量DPA 攻击实验证明, 集成电路功耗与数据操作是密切相关的, 但是FPGA芯片的功耗特点与ASIC等不完全相同。以 Virtex-2 系列芯片为例, 芯片中 CLB、RAM 等结构使用 2.5 V 电压, 而 I/O 块使用 3.3 V 电压。在该类芯片的总动态功耗中, 内连线占 60%, 时钟占 14%, 逻辑电路占 16%, I/O 占 10%[2]。与数据相关性从高到低依次为逻辑电路、内连线电路、I/O 块和时钟, 其中逻辑电路和内连线电路所占比例最大, 联系最紧密。

1.2　差分功耗分析

DPA 是一种极为有效的密码攻击技术, 其理论基础是加密过程中消耗的能量会随处理的数据不同而产生细微的变化, 根据这种变化可以确定所处理的数据是 1 或是 0, 通过大量数据的比对分析, 猜测出算法中的密钥。

DPA 攻击无须知道加密设备的任何详细信息, 只需获知设备执行的算法就足够。DPA 攻击通常包括以下 4 个步骤。

1) 选择算法的某个中间值。这个中间值必须是一个函数 $f(d, k)$, 其中 d 是已知的非常量数据, k 是密钥的一部分。

2) 测量能量消耗。攻击者进行大量不同数据的加密或解密, 记录数值 d_i 和相应的能量迹 t_i。

3) 猜测子密钥。根据猜测的子密钥与已知的 d_i 进行运算, 得到猜测的中间值后, 按照一定的模型将功耗迹进行分类。将分类后的功耗迹与平均功耗做差分运算, 若出现尖峰则猜测正确, 否则重复本步骤。

4) 按上述方法获得所有子密钥, 计算恢复加密系统的密钥。

2　电路防护技术

针对能量分析攻击, 主要有两类电路级抗攻击思路: 一类是掩码[3], 利用随机数 m 对加密过程的中间值进行变换, 使得电路功耗随机化, 但是目前研究表明, 仅靠掩码技术难以抵抗高阶 DPA 攻击[4]; 另一种是隐藏, 通过电路中逻辑元件结构来保证设备的能量消耗独立于设备处理的数据和执行的操作, 这类结构通常使用双轨预充电的技术来实现。由于 FPGA 基本单元的限制, 能够应用于 FPGA 的双轨预充电结构十分有限。WDDL[5]是目前最主要的一种 FPGA 平台抗 DPA 攻击的电路结构。WDDL 基本单元的实现如图 1 所示, 其特点如下。

1) 双轨电路。无论输入还是输出, 都用互补的两根线来表示, 例如输入信号 A 由 A 和 $\overline{A}$ 表示, 输出由 Z 和 $\overline{Z}$ 表示。这样电路内部的逻辑 1 和逻辑 0 就是对称的。

2) 预充电结构。WDDL 还引入预充电结构, 在起始阶段, 电路会产生一个预充电信号, 将所有的

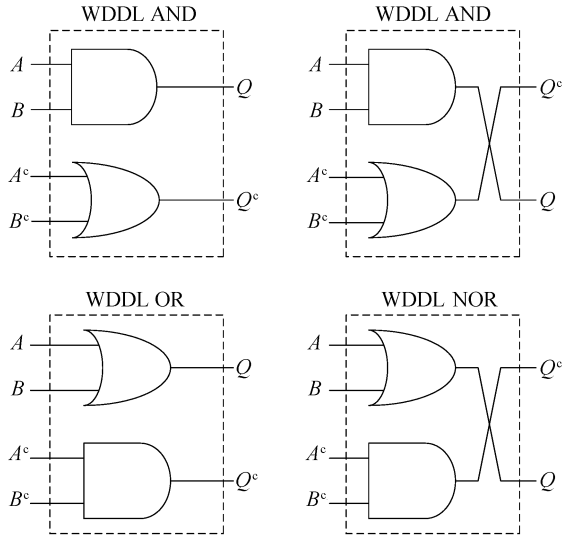


图 1　WDDL 基本单元[5]
Fig. 1　WDDL components[5]

输出预充电至(0, 0)。这样, 无论输入信号是什么, 即使输入信号没有改变, 输出也会有一根信号线从 0 翻转为 1, 电路完全平衡。预充电结构通常放置在系统的输入以及内部的触发器输出。预充时逻辑 0 会逐级传播至整个电路。

3) 无反相器。WDDL 通过逐级传播逻辑 0 来达到预充电的目的, 而反相器会打断预充电的过程。因此 WDDL 仅使用正逻辑单元, 反相器则依靠交换逻辑单元的互补输出实现。

3 FPGA 安全电路的设计实现

目前, WDDL 结构是基于数字标准单元的, 而 FPGA 是基于查找表逻辑的, 因此, 用 FPGA 实现仍有存在许多问题[6]。本文提出一种在 FPGA 上实现 WDDL 的方法。图 2 为 FPGA 实现 WDDL 的流程, 主要由 4 步组成。

1) 生成门级网表。

首先从高层次的设计开始, 将设计进行综合。综合时有两种选择, 一种是用 FPGA 设计工具, 另一种是 ASIC 的综合工具。我们注意到 FPGA 工具综合出来的网表是查找表(LUT)的结构, 采用 ASIC 工具进行综合得到的是门级网表。考虑到人们的思维习惯以及方便下一步的修改, 本文采用 Synopsys 公司的 ASIC 综合工具 Design Compiler 进行综合。

2) 生成双轨网表。

获得单端门级网表后, 需要对单端网表的连线和器件进行标注, 之后复制一份网表, 复制的网表也要进行标注, 以便区分原网表和复制之后的网表。随后进行修改, 生成 WDDL 基本单元。对于负逻辑, 注意交换原网表和复制网表的输出。

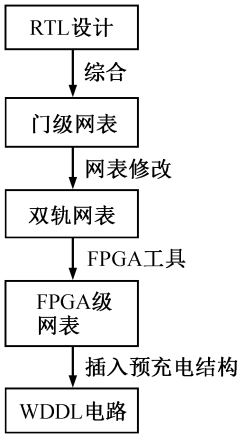


图 2 WDDL 设计流程

Fig. 2 WDDL implementation flow

若直接将双轨门级网表送入 FPGA 工具进行综合, 会发现综合后易生成多路器的结构。而多路器的选择信号会需要反相器, 这与 WDDL 的预充电要求不相符。所以需要把门级网表转成 LUT 级的网表, 将门级网表里的与门、或门用两输入 LUT 替换。LUT 级网表进入 FPGA 工具, 不会经过综合这一步, 所以能比较好地控制结果。虽然 LUT 级网表采用大量的两输入 LUT, 但是 FPGA 工具能针对这点进行优化, 合并部分 LUT 结构。

3) 生成 FPGA 级网表。

针对设计要求编写约束文件, 随后 FPGA 设计工具会将 LUT 级网表翻译、映射到 FPGA 的基本结构, 生成 FPGA 级的电路网表。

4) 插入预充电结构。

可以在生成门级网表的时候插入预充电结构, 但是更推荐在 FPGA 级网表插入预充电结构。因为在 FPGA 级插入预充电结构, 能充分利用每个 slice 内的资源, 减少 FPGA 资源的使用量。

在 FPGA 级插入预充电时, 有两种选择[7], 如图 3 所示。第一种方法是利用多路器实现, 将时钟信号作为选择信号, 输出预充电信号或者正常输出 LUT 的结果; 第二种是利用触发器, 将其配置成锁存器模式, 用时钟信号控制锁存器复位。

本文采用第二种方法, 以 Virtex-2P 系列芯片为例, 每个 slice 内有两个 LUT 和两个触发器, 但是仅有一个可供预充电的多路器。第一种结构需要引入 0 信号, 会消耗更多的布线资源。第二种锁存器结构能有效减少额外插入的预充电 slice。

完成以上步骤后进行布局布线, 即在 FPGA 上实现了 WDDL 结构。由于 FPGA 基本单元的约束, WDDL 电路的互补输出端的布线不对称, 负载不相等, 仍然易被 DPA 攻击。文献[8]介绍了一种对称布线技术 DWDDL, 其主要方法如图 4 所示。

DWDDL 利用已有的 WDDL 电路, 生成一个互补的 WDDL 电路。编写脚本将原电路的布局布线信息完整地复制平移, 生成一个互补的 WDDL 电路, 在互补 WDDL 内, 每个 LUT 的内容与原 WDDL 互补, 每个 LUT 的输入也与原 WDDL 互补, 这样每对互补输出的连线长度一致, 负载相等。电路在每个时钟周期内功耗相等, 有较好的抗 DPA 攻击能力。

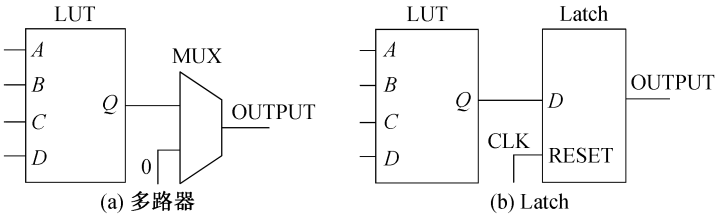
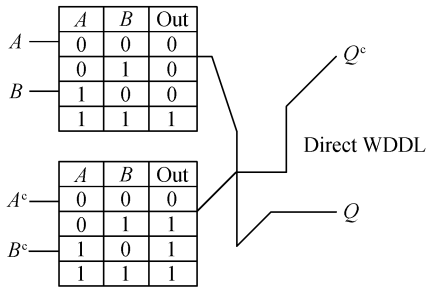


图 3 预充电结构[7]
Fig. 3　Pre-charge logic[7]



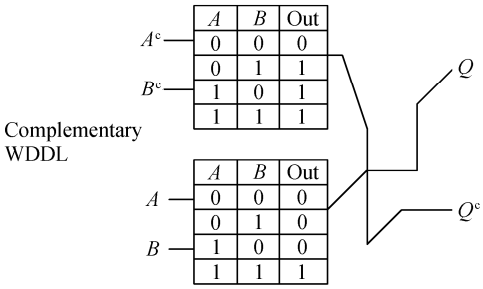


图 4　基于 WDDL 的对称布线方法
Fig. 4　WDDL symmetrical routing technology

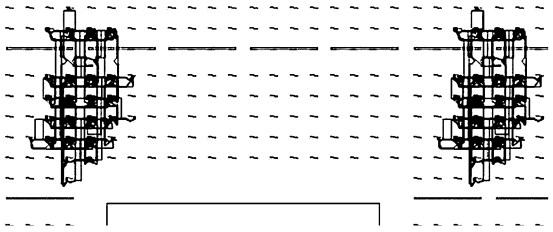


图 5　DWDDL 4-bit 加法器
Fig. 5　4-bit DWDDL adder

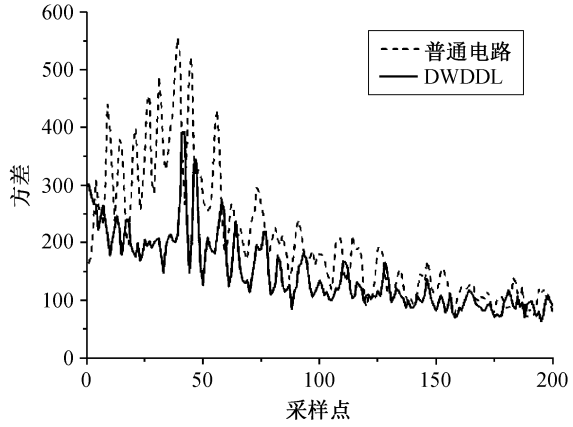


图 6　功耗方差曲线
Fig. 6　Power variance measurement

本文根据上述 DWDDL 电路设计流程, 实现一个 4 位加法器, 其 FPGA 电路如图 5 所示。随后利用 FPGA 平台对它进行功耗分析和测量, 输入 100 组随机数, 测量每组的功耗情况, 并计算功耗方差。另设一个未采用抗 DPA 结构的电路进行对比, 结果如图 6 所示, 可见采用 DWDDL 技术能有效地降低功耗与数据之间的相关性, 有较好的抗 DPA 能力。

4　改进思路

上述电路仍存在一些缺点: 一是由于预充电的原因, 组合逻辑部分的输出会有半个周期处于预充电状态, 半个周期正常输出, 当组合电路的输出接到 FPGA 的 I/O 时, 会严重影响 FPGA 与外围电路的通信; 二是 FPGA 工具在优化、合并两输入 LUT 时, 会生成带非结构的 LUT, 例如 $D=\mathrm{A1}\times(\overline{\mathrm{A2}}+\mathrm{A3})$。若求值时 3 个信号到达时间不一致, 电路可能会产生竞争。例如 A3 保持为 0, A1 从 0→1, $\overline{\mathrm{A2}}$ 在 A1 之后 0→1, LUT 的输出会多出一个小尖峰, 电路有额外的翻转, 产生额外的功耗, 存在信息泄露。

针对第一个问题, 我们利用 FPGA 的特点, 配置 I/O 内部的触发器对输出进行采样。经过处理, 输出信号比未改进的电路落后一个周期。针对第二个问题, 可以利用图 7 的结构解决。首先我们用脚本寻找所有带非结构的 LUT, 找到相应的 pin 脚, 修改成为不带非的结构 $(\overline{\mathrm{A2}}\rightarrow X)$, 同时原输入信号经过反向, 通过触发器输出到 LUT。信号的反向

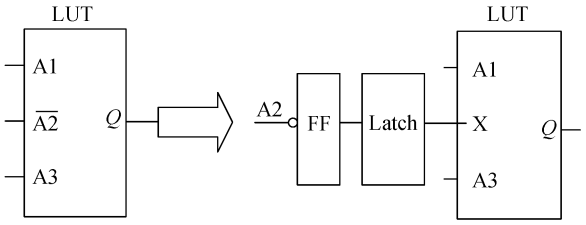


图 7 消除冒险的电路结构
Fig. 7 Hazards free logic

通过修改 slice 内部的配置即可实现。经过上述调整, LUT 的表达式为 D=A1×(X+A3), 不含带非的项, 表达式里的各项都只能单调地变化(0→1 或 0→0), 消除了冒险。

此结构依然存在其他问题: 由于插入了触发器, LUT 的输出会比之前慢一个周期, 因此需要对周围的电路也进行插入触发器的调整; 其次是多使用了一个触发器和一个锁存器, 资源开销变大。对于复杂设计来说, 这种触发器的插入使得时序设计的调整变得十分困难, 硬件开销也难以承受, 所以本文仅提出这个思路, 并未用于实际电路的实现。

5 结论

本文实现了一种 FPGA 安全电路 DWDDL并提出相应的改进, 这种安全电路采用双轨预充电技术与对称布线技术。与传统的WDDL 相比, 每个单元的输出负载基本相等, 在每个时钟周期内功耗更加恒定, 抗DPA 攻击的能力更优秀。但是抗 DPA 攻击能力的提高是以更大的资源消耗和更低的电路速度为代价, 所以在实际应用中, 应有一定的取舍。

参考文献

[1] Kocher P, Jaffe J, Jun B. Differential power analysis // Advances in Cryptology — CRYPTO'99. Berlin: Springer, 1999: 388–397

[2] Shang L, Kaviani A S, Bathala K. Dynamic powerconsumption in Virtex™-II FPGA family // Proceedings of the 2002 ACM/SIGDA Tenth International Symposium on Field-Programmable Gate Arrays. Princeton: ACM, 2002: 157–164

[3] Coron J, Goubin L. On boolean and arithmetic masking against differential power analysis // Cryptographic Hardware and Embedded Systems — CHES 2000. Berlin: Springer, 2000: 231–237

[4] Maghrebi H, Danger J L, Flament F, et al. Evaluation of countermeasure implementations based on boolean masking to thwart side-channel attacks // Signals, Circuits and Systems (SCS), 2009 3rd International Conference on. Piscataway: IEEE, 2009: 1–6

[5] Tiri K, Verbauwhede I. A digital design flow for secure integrated circuits. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, 2006, 25(7): 1197–1208

[6] Tiri K, Verbauwhede I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. IEEE Computer Society, 2004, 1: 246–251

[7] Yu P, Schaumont P. Secure FPGA circuits using controlled placement and routing // Hardware/ Software Codesign and System Synthesis (CODES+ ISSS), 2007 5th IEEE/ACM/IFIP International Conference on. Salzburg: IEEE, 2007: 45–50

[8] Yu P. Implementation of DPA-resistant circuit for FPGA[D]. Blacksburg: Virginia Polytechnic Institute and State University, 2007