doi:10.3969/j.issn.1000-436x.2013.z1.010

基于 NCL 路径平衡的抗功耗分析方法

罗芳，欧庆于，吴晓平
（海军工程大学 信息安全系，湖北 武汉 430033）

摘 要：由于对路径结构平衡的本质以及设计方法缺乏系统的研究，导致其在实际应用中严重依赖设计者自身的经验，难以推广到各类自动化综合方法中。对实现路径平衡结构的形式化定义及充分条件进行了研究，并给出了证明，进而提出了一种基于改进二元决策图(BDD, binary decision diagram)的零协议逻辑(NCL, null convention logic)异步电路路径平衡扩展方法。该方法能够简便地扩展至各类自动化综合过程中，并能在不改变目标电路特性的前提下，有效实现 NCL 异步电路的路径平衡结构，抵消由于寄生电容和负载电容差异所造成的密码芯片旁路信息泄露。

关键词：功耗分析；路径平衡；二元决策图；零协议逻辑
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0076-08

Power analysis-resistant based on NCL path balance

LUO Fang, OU Qing-yu, WU Xiao-ping
(Department of Information Security, Naval University of Engineering, Wuhan 430033, China)

Abstract: Because of the insufficient research on the essence and the design technique of the path balance structure, the experience of the designer is severely relied on, so it can't be applied in kinds of automatization synthesis techniques. To solve this problem, the formal specification and the sufficient conditions of the implementation for the path balance structure were researched, and the proof was given. Based on the improvement of the binary decision diagram, a path balance extension technique of the null convention logic (NCL) asynchronous circuit was put forward, which could be applied in kinds of automatization synthesis techniques. By applying this technique, the path balance structure of the NCL asynchronous circuit could be implemented on the premise that the characteristics of the orientated circuit would be unchangeable, and the leakage of the side-channel information aroused by the differences of the parasitic capacitor and the load capacitor could also be resisted.

Key words: power analysis; path balance; binary decision diagram; null convention logic

1 引言

1996 年，Paul Kocher[1]发现密码芯片在运算时所泄漏的旁路信息能用于密码分析，此后，旁路攻击技术引起了人们的极大关注。其中，功耗分析以其简单易行、适用范围广以及行之有效等特点得到了广泛研究并日趋成熟。由最初的简单功耗分析[2]、差分功耗分析[3~5]发展为相关性增强功耗碰撞分析[6]、联合旁路攻击[7]等，对密码芯片的应用安全构成了严重威胁。

为使密码芯片具备抵抗功耗攻击的能力，大量的专用硬件逻辑结构被提出[8~10]，并取得了一定的效果，但遭受功耗分析的隐患仍未消除。其主要原因在于无法完全解决硬件实现过程中由于寄生电容及负载电容差异所造成的互补导线对功耗差异。

异步电路由于消除了时钟信号等时间参照信息，且具有对传输延迟非敏感以及低功耗等特点，使其在抗旁路攻击方面具有较大的优势。其中，基于路径平衡结构的随机路径切换方法通过对不同运算路径输入信号集的随机切换，实现了运算逻辑的功耗平衡，避

收稿日期：2013-06-29
基金项目：国家自然科学基金资助项目（61100042, 61202338）
Foundation Item: The National Natural Science Foundation of China (61100042, 61202338)

免了对互补输出对的电容及电阻进行平衡匹配，较好地消除了由于寄生电容与负载电容差异所造成的旁路信息泄露，因此，具有很强的抗功耗攻击能力[11]。然而，目前路径平衡结构的构造严重依赖于设计者自身的经验，使得在大规模复杂设计中缺少可操作性，难以推广到各类自动化综合方法中。

本文以 NCL[12]异步电路为基础，对其路径结构的平衡方法进行深入研究，提出了一种基于 BDD 的路径结构平衡方法，通过利用带权值有序二元决策图(WOBDD, weighted ordered binary decision diagram)对 NCL 异步电路布尔网络进行图形化，并实现了轨间平衡扩展及运算路径间平衡扩展，有效地克服了目前路径平衡方法无法扩展至各类自动化综合过程中的问题，为抗功耗分析密码电路的自动化设计提供了一种新的研究思路。

2　NCL 异步电路路径平衡结构

2.1　NCL 异步电路

根据异步电路对延迟进行建模方式的不同，异步电路可以分为多种模型。其中，延迟无关(DI, delay insensitive)异步电路模型假定每个门在其输出端有一个无限惯性延时单元，同时认为互连线的延时可以忽略。DI 异步电路具有低功耗、高性能、强顽健性、无时钟问题困扰的特点，在克服时钟偏移、低功耗设计、模块化设计等方面具有较大优势。但由于传统设计方法中，DI 异步电路只能由 Muller-C、反相器及缓冲器等有限电路单元构成[13]，从而限制了该类型异步电路的实际应用。

NCL 电路作为异步电路延迟非敏感模型的一种实现方式，在满足输入完全性及可见性的情况下，采用四相双轨编码，使用完成检测的方式进行延迟控制，可用于构建强顽健性的高速流水线系统，并可以完全由普通 EDA 工具综合，从而为 DI 异步电路提供了一种更加便利的实现方式。

为了保证延迟不敏感特性，NCL 异步电路必须满足输入完全性及可见性。其中，输入完全性符合 Seitz[15]关于延迟无关信号所提出的“弱条件”，可通过构造完全析取范式得到满足；可见性能够通过等时分支的假设得到满足。

输入完全性。电路所有的输出信号只有在所有输入信息完成有效跳变（NULL 至 DATA 或 DATA 至 NULL）后才能进行相应的跳变。

可见性。在电路中不存在跨越门界限的孤儿路径传播，即电路中每一个门输出的跳变必将引起与之连接的输出信号的跳变。

2.2　NCL 异步电路路径平衡

为了实现 NCL 异步电路平均功耗平衡，并最终达到消除处理数据与功耗之间关联的目的，作者将 Fraidy Bouesse 等人[14]针对准延迟不敏感(QDI, quasi delay insensitive)电路提出的路径平衡概念扩展至 NCL 异步电路中。

定义 1　在 NCL 异步电路中，能够触发输出信号转换的最小输入信号集至输出信号的算子单元连接称为运算路径。

定义 2　在保证计算正确性的前提下，电路中每一条运算路径的输入信号集能够在所有运算路径输入端间进行等概率的交换，则称该电路具备路径平衡结构。

以如图 1 所示的 *xor* NCL 异步电路为例，对 NCL 异步电路路径平衡结构及其抗功耗分析攻击的机理进行说明。

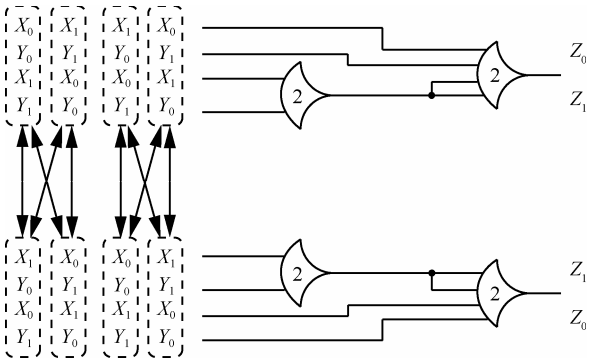


图 1　*xor* NCL 异步电路的路径平衡结构

根据定义 1 可知，在 *xor* NCL 异步电路中共存在 4 条运算路径。图中每一组虚线框内的输入信号代表互补输出信号 Z_0 或 Z_1 所对应的电路中运算路径输入信号集的一种组合情况，虚线框之间的箭头代表互补输出信号 Z_0 和 Z_1 所对应的电路间运算路径输入信号集的一种组合情况。通过对 4 条运算路径相对应的输入信号集$\{X_0, Y_0\}$、$\{X_1, Y_1\}$、$\{X_1, Y_0\}$、$\{X_0, Y_1\}$的输入位置在 8 种组合情况间以及与之对应的输出信号 Z_0 和 Z_1 进行随机切换，能够在保证计算结果正确的前提下，实现每个输入信号集等概率地出现在每条运算路径的输入端。

对以上电路进行 DPA 攻击时，其功耗均值偏差 T 为

$$T = P_{0\_\text{average}(xor)} - P_{1\_\text{average}(xor)} \tag{1}$$

由于运算路径相对应的输入信号集等概率地出现在 4 条运算路径的输入端。因此，无论输入数据如何变化，电路运行时产生的平均功耗恒定为 4 条运算路径功耗之和的平均，即

$$T = P_{0\_\text{average}(xor)} - P_{1\_\text{average}(xor)} = 0 \tag{2}$$

从而杜绝了功耗旁路信息的产生。

3 路径平衡的形式化及其充分条件

设双轨异步电路的网表分别为 (V_1, n_1, m_1, E_1) 和 (V_0, n_0, m_0, E_0)，V_1、V_2 为互补输出信号对应的电路中的单元集合；$E_1 \subseteq V_1 \times N \times V_1 \times N$、$E_0 \subseteq V_0 \times N \times V_0 \times N$ 为互补输出信号对应的电路单元连接集合；$n_1 : V_1 \to N$、$m_1 : V_1 \to N$ 和 $n_0 : V_0 \to N$、$m_0 : V_0 \to N$ 为记录互补输出信号对应的电路中单元与其他单元连接的输入及输出端数量的函数。

布尔网络。网表中每一个电路单元 v 均存在与之相对应的布尔函数 $f(v) : B^{n(v)} \to B^{m(v)}$，则称该网表为布尔网络，每个电路单元称为节点；满足 $n(v)=0$ 的节点 v 称为源输入节点；满足 $m(v)=0$ 的节点 v 称为源输出节点。

设 $\{s_j\}$ $(1 \leqslant j \leqslant m)$、$\{u_i\}$ $(1 \leqslant i \leqslant n)$ 分别为与双轨互补输出信号 1 和 0 对应电路的源输入信号集合，则对轨间输入信号交换和轨内输入信号交换进行如下定义。

轨间输入信号交换。在输入信号集 $\{s_j\}$ 和 $\{u_i\}$ 中，至少各存在一种排列顺序 P_s、P_u，使得与双轨互补输出信号 1 和 0 对应的布尔网络的输入信号集在该顺序下可互相进行交换，即

$$\begin{aligned} f_1^{V_1} &: B^{\{u_i\}P_u} \to B^{m(v)=0} = z_0 \\ f_0^{V_0} &: B^{\{s_j\}P_s} \to B^{m(v)=0} = z_1 \end{aligned} \tag{3}$$

运算路径间输入信号交换。在输入信号集 $\{s_j\}$ 或 $\{u_i\}$ 中，设以布尔网络运算路径为单位获得输入信号集的有序分区 $\Sigma = \{\Sigma_1, \cdots, \Sigma_m\}$ 或 $\Pi = \{\Pi_1, \cdots, \Pi_l\}$，则无论顺序具体如何定义，总是能够使得下式成立。

$$\begin{aligned} f_1^{V_1} &: B^{\Sigma} \to B^{m(v)=0} = z_1 \\ f_0^{V_0} &: B^{\Pi} \to B^{m(v)=0} = z_0 \end{aligned} \tag{4}$$

定理 1（充分条件）当 $|\{s_j\}|=|\{u_i\}|$，且同时满足轨间、运算路径间的输入信号交换时，电路具有路径平衡的结构。

证明 设双轨互补输出信号 1 和 0 对应的输入信号集 $|\{s_j\}|=|\{u_i\}|$，且满足轨间、运算路径间的输入信号交换。则由于 $|\{s_j\}|=|\{u_i\}|$，电路具备了实现轨间输入信号交换的基础。又根据轨间输入信号交换及运算路径间输入信号交换的定义可知，当轨间及运算路径间的输入信号进行等概率交换时，每条运算路径的输入信号集等概率地出现在双轨电路每个运算路径的输入端，使得 $P_{0\_\text{average}} = P_{1\_\text{average}}$，满足路径平衡结构特性。

4 NCL 异步电路路径结构平衡扩展

目前已有的 NCL 电路综合方法[16~18]主要关注的是目标电路的延时无关特性的保持以及面积、吞吐率优化等问题，对于在自动化综合过程中路径结构平衡并没有提出相应的优化方法，使得设计者在完成目标电路综合后，需要依赖自身的经验进行手动优化。针对这一问题，本节对 NCL 异步电路的路径结构平衡方法进行了研究。

4.1 NCL 异步布尔网络图形化

NCL 异步电路由 NCL 基本算子构成，在 NCL 基本算子库中包含 25 个线性可分非蚀 NP 类布尔代表函数及 3 个非线性可分非蚀 NP 类布尔代表函数，能够涵盖所有的四输入及以下的布尔表达形式。NCL 异步电路的本质是阈值逻辑，由于阈值电路中的阈元是“与非”门的广义形式，意味着阈值逻辑是开关理论的统一理论。因此，基于 BDD 的分析及优化方法同样能够应用于 NCL 异步电路中。然而，由于在 NCL 电路中每个算子被赋予了一个阈值，每个输入端被赋予了相应的权值。在将 BDD 方法应用于 NCL 异步电路的路径平衡优化中，必须进行适当的修改。

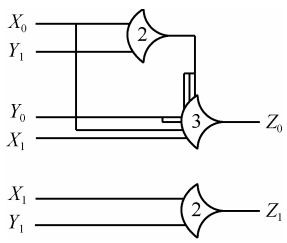
定义 3 在 NCL 异步布尔网络的基础上，利用 BDD 按以下原则对 NCL 异步电路的布尔网络进行图形化，获得相应的带权值 OBDD，简称为 WOBDD。

1) 以 NCL 异步电路布尔网络中的节点为对象，在忽略源输入、源输出的前提下按照节点之间的连接关系对节点连接进行抽象，得到节点抽象图。

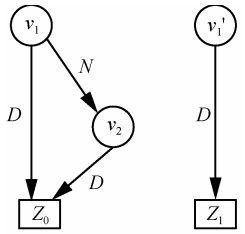
2) 对各个节点所对应的布尔函数进行约减的有序二元决策图(ROBDD, reduced ordered binary decision diagram)扩展。

3) 根据 NCL 异步电路中各节点的阈值及输入端权值设置，对 NCL 异步电路布尔网络有序二元决策图(OBDD, ordered binary decision diagram)中的节点进行权值标签扩展。

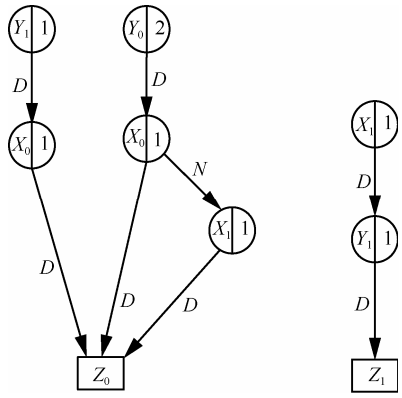
以图 2(a)所示的 *and* NCL 异步实现为例，该电路满足输入完全性及可见性。其所对应的节点抽象图如图 2(b)所示，WOBDD 如图 2(c)所示。



(a) *and* NCL 异步实现



(b) 节点抽象图



(c) WOBDD

图 2　*and* WOBDD 构造

其中，图 2(c)中边标签 *D* 表示 2NCL 中的 DATA 状态，边标签 *N* 表示 2NCL 中的 NULL 状态。路径(Y_0，2)→(X_0，1)→Z_0 和(Y_0，2)→(X_1，1)→Z_0 存在共用节点(Y_0，2)，称这样的路径为非独立路径。反之，路径(Y_1，1)→(X_0，1)→Z_0 由于不与其他路径存在共用节点，称为独立路径。

4.2　NCL 异步电路轨间平衡扩展

定义 4　在布尔网络 Φ_1 和 Φ_2 之间，如果其源输入能够以某种排列顺序进行互换，并使得互换后的源输入能够根据与之相连的布尔网络产生与其对应的源输出，则称这 2 个布尔网络在结构上等价。

定义 5　当双轨互补输出对应布尔网络的WOBDD在不考虑节点标签及权值标签的情况下同构，且在不考虑顺序的情况下各同构子图的权值序列相等，则称这 2 个 WOBDD 同构。

推论 1　假设布尔网络 Φ_1 和 Φ_2 依据定义 3 所得到的 WOBDD 同构，则布尔网络 Φ_1 和 Φ_2 的源输入能够以某种排列顺序进行互换，即能够实现轨间输入信号交换。

推论 2　当 NCL 异步电路互补输出信号 1 和 0 对应电路的布尔网络在结构上等价时，NCL 异步电路能够实现轨间输入信号交换。

由于布尔网络的结构等价能够转化为 WOBDD 的图形同构，因此可利用图形同构探测算法对双轨互补输出信号 1 和 0 对应电路布尔网络间的结构等价特性进行探测。当双轨输出信号所对应的 WOBDD 不同构时，可基于以下描述的结构调整方法对 WOBDD 进行重构，实现双轨输入信号所对应的 WOBDD 同构。

WOBDD 结构调整分以下 2 种情况实施。

1) 当某个双轨输出信号对应的 WOBDD 在不考虑节点标签，且不考虑权值标签顺序的情况下，包含于与其互补的双轨输出信号对应的 WOBDD 中时，利用 Dummy 条件在被包含的 WOBDD 中进行扩展。

2) 当双轨输出信号对应的 WOBDD 不存在包含关系时，对 WOBDD 中的共用节点进行复制，将非独立路径进行分离，构成独立路径。

以 NCL 异步电路中使用的四相双轨编码协议为例。对于任意信号 *X*，在四相双轨编码协议中永远不会出现 X_0，X_1 同时为 1 的情况。因此，$X_0 \wedge X_1$ 被称为 Dummy 条件。

定理 2　通过对 WOBDD 中的共用节点进行复制、分离操作，必能使 NCL 异步电路双轨互补输入信号所对应的 WOBDD 间存在包含关系。

证明　由于NCL异步电路必须满足输入完全性和可见性，因此其最终的布尔表达形式必为完全析取范式的形式。由于 WOBDD 中每条从根节点至输出目标节点的路径代表一个完全析取项，故在 NCL 异步电路的 WOBDD 中每条从根节点至输出目标节点路径的节点数相等。因此，通过对共用节点进行复制、分离操作，在 WOBDD 完全由独立路径构成的极端情况下，必存在 WOBDD 间的包含关系。

基于 Dummy 条件进行 WOBDD 扩展的核心思想是，当双轨输出信号对应的 WOBDD 不同构，且存在包含关系时，利用 Dummy 条件构造无效路径

实现 WOBDD 的同构。基于 Dummy 条件扩展的具体步骤如下。

1) 当双轨输出信号对应 WOBDD 中非平衡区域的某个非独立路径，某条运算路径的非共用节点数量小于 2 时，则对该收敛节点进行复制、分离操作，使得该路径的非共用节点数不小于 2。

2) 在待扩展 WOBDD 中复制非平衡区域结构，并对复制结构的每条运算路径所包含的节点标签进行重置，使得每条运算路径至少包含一组 Dummy 条件。

以图 2(c)所示的 WOBDD 为例，输出信号 Z_1 对应的 WOBDD 与输出信号 Z_0 对应的 WOBDD 中的路径 $Y_1 \rightarrow X_0 \rightarrow Z_0$ 同构。因此，输出信号 Z_1 对应的 WOBDD 被输出信号 Z_0 对应的 WOBDD 包含，而输出信号 Z_0 对应的 WOBDD 中的非平衡区域由非独立路径 $Y_0 \rightarrow X_0 \rightarrow Z_0$，$Y_0 \rightarrow X_1 \rightarrow Z_0$ 构成，且每条运算路径的非共用节点数小于 2。根据 Dummy 扩展的步骤对其扩展后的 WOBDD 如图 3 所示。

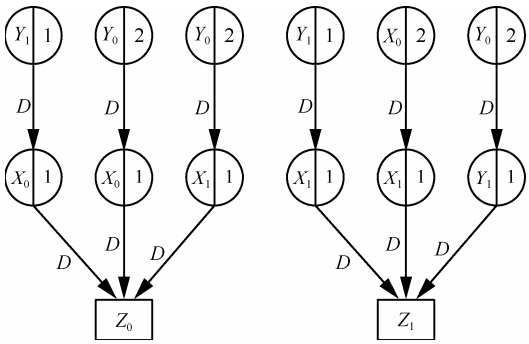


图 3 *and* WOBDD 轨间平衡扩展

4.3 NCL 异步电路运算路径平衡扩展

根据定理 1 可知，仅仅实现轨间输入信号交换并不足以构成路径平衡结构，还需要实现运算路径间输入信号的交换。

推论 3 当 WOBDD 中任意 2 条运算路径为独立路径，且所包含的节点权值标签同时满足式(5)及式(6)所示的条件时，该电路可进行运算路径间的输入信号交换。

$$w_1 + \cdots + w_k = w_1' + \cdots + w_k' \tag{5}$$

$$\forall w_i (1 \leqslant i \leqslant k),$$

$$\exists w_j' (1 \leqslant j \leqslant k) \rightarrow w_i = w_j' \tag{6}$$

证明 根据 OBDD 的特性可知，在 WOBDD 中，每条从根节点至输出目标节点的路径表示电路的一条运算路径。又根据 NCL 异步电路的输入完全性可知，WOBDD 中每一条从根节点至输出目标节点的路径所包含的节点数量相同。因此，当 WOBDD 中不存在非独立路径，且所有运算路径的节点权值标签满足式(5)和式(6)时，意味着任意 2 条运算路径能够以某种顺序进行互换，且不改变电路的特性，即可实现运算路径间的输入信号交换。

基于推论 3，NCL 异步电路运算路径平衡扩展对 WOBDD 中非独立路径的收敛节点进行复制、分离操作，使得最终 WOBDD 中所有的运算路径均为独立路径。然后，通过对各运算路径的节点阈值标签进行重置，使其满足式(5)和式(6)，最终达到运算路径间输入信号可交换的目的。以图 3 所示的 *and* 函数 WOBDD 轨间平衡扩展为例，其 NCL 异步电路运算路径平衡扩展的结果如图 4 所示。

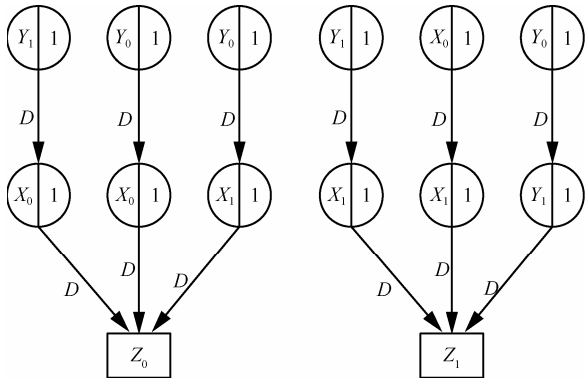


图 4 *and* WOBDD 运算路径平衡扩展

定理 3 NCL 异步电路总是能够通过 Dummy 扩展获得路径平衡结构。

证明 设双轨输出信号为 Z_0、Z_1，输入信号数量为 n，输入信号有效状态组合总数为 2^n。由于每个输入信号都可构造一个 Dummy 条件，去除一个全零状态组合后，输入信号的 Dummy 状态组合数为 2^{n-1}。又根据 NCL 异步电路的输入完全性及可见性，输出信号 Z_0 和 Z_1 至少存在一个有效的输入信号状态组合，且对于 Z_0 和 Z_1 不存在相同的有效输入信号状态组合。因此，极端情况下 Z_1 的有效输入信号状态组合数为 2^{n-1}，Z_0 的有效输入信号状态组合数为 1。由于 Dummy 状态组合数为 2^{n-1}，可通过 Dummy 扩展使得 Z_1 和 Z_0 的有效输入信号状态组合数相等。此外，由于 Dummy 条件为永远不会被触发的条件，且 $Dummy_1 \wedge Dummy_2 \wedge \cdots \wedge Dummy_k$ 仍为 Dummy 条件，Dummy 与有效输入信号状态组合 s 与操作时有 $s \vee Dummy_1 \triangleq s$。因此，可通过 Dummy 扩展实现轨间及运算路径间的平衡。

WOBDD 至 NCL 算子的映射可利用当前已有的异步阈值网络技术映射方法实现，从而保证目标电路的输入完全性及可见性。以图 4 所示的 WOBDD 为例，其技术映射后的结果如图 5 所示。

实际的平衡扩展过程要比本文中描述的情况复杂得多，很多具体细节需要考虑。本文抽取了其中的主要内容，简明介绍了路径平衡扩展的核心思想和基本方法。

5　实验结果与分析

基于 AMI 0.6 um CMOS 工艺，用 Spectre 分别对平衡扩展前及平衡扩展后的 *and* 异步电路进行瞬态仿真，以检验目标电路能量消耗与被处理数据之间的依赖程度。如图 6 所示，在非路径平衡结构电路中，当双轨信号$\{X_0, Y_1\}$有效时，电流尖峰值为 222.3 uA；当双轨信号$\{X_1, Y_0\}$有效时，电流尖峰值为 175.1 uA。由于输入信号与运算路径绑定，攻击者能够利用 SPA/DPA 方法，通过测量电流尖峰或分析平均功耗差异来获取参与运算的数据。

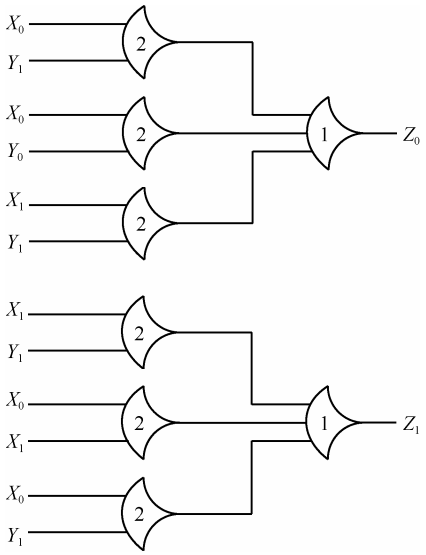


图 5　*and* WOBDD 技术映射结果

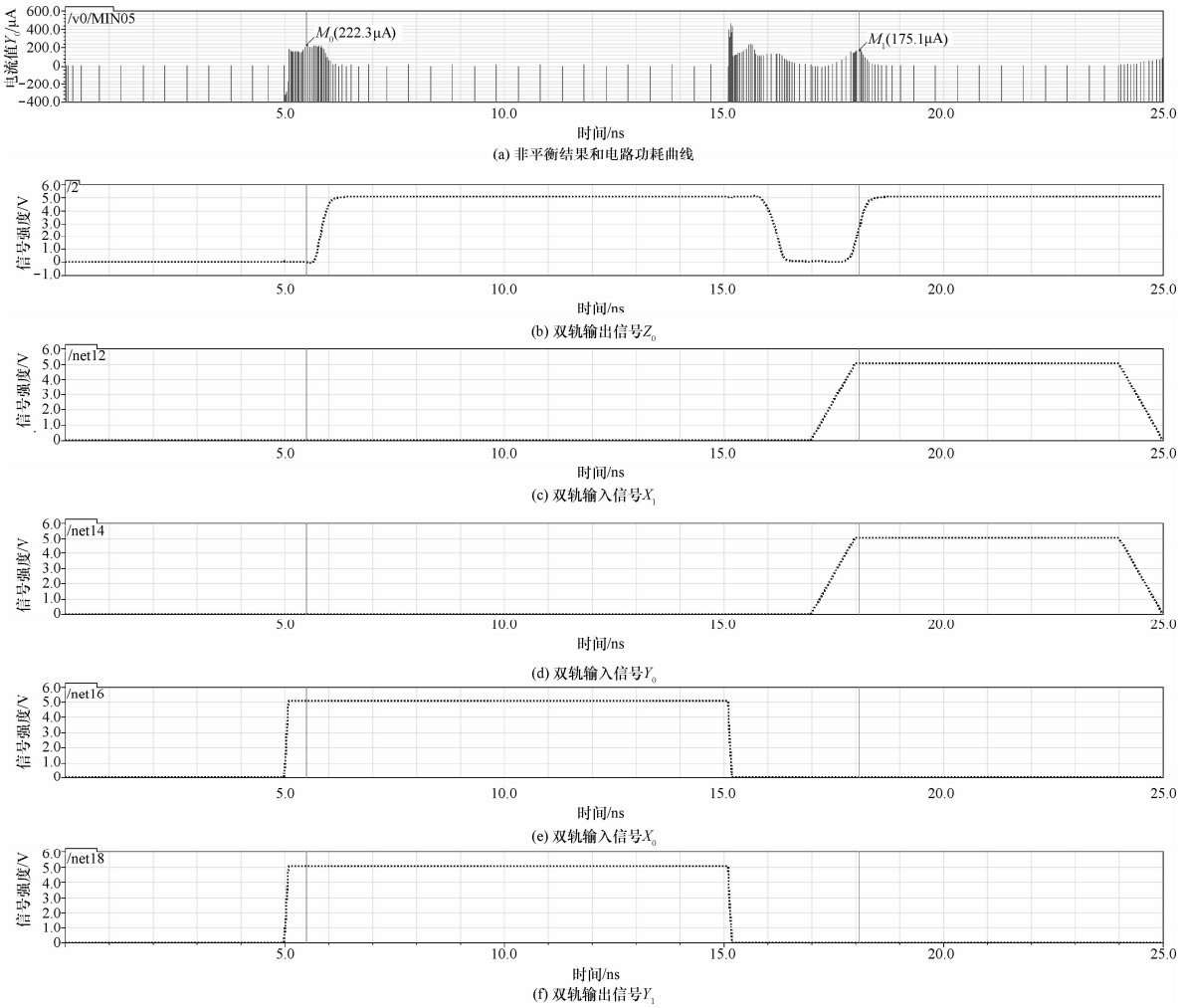
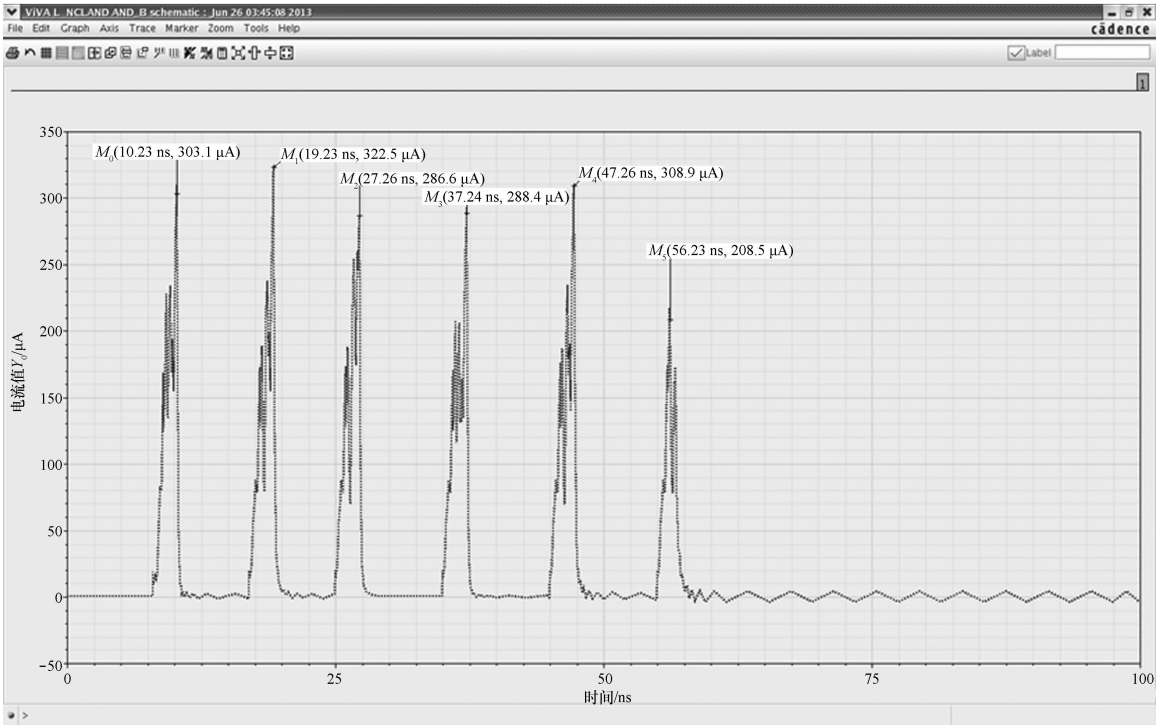
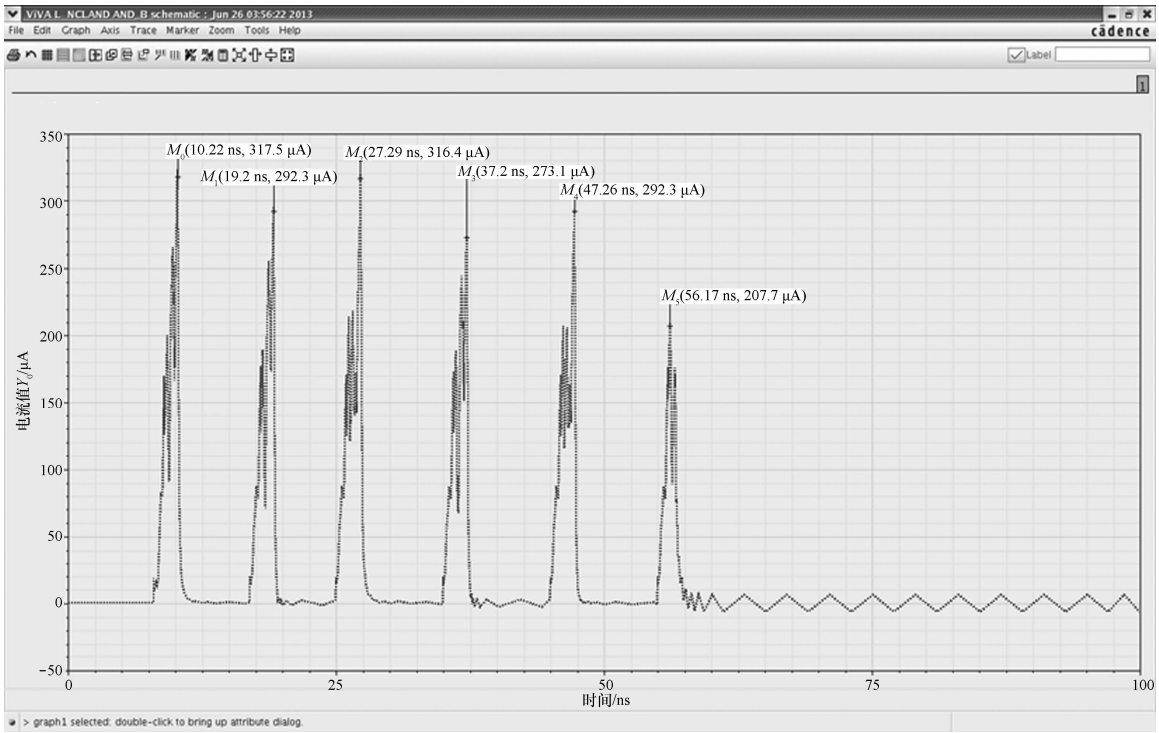


图 6　非路径平衡结构 *and* 电路瞬态仿真结果

在路径平衡结构 *and* NCL 异步电路中，分别对双轨信号{X_0, Y_1}、{X_1, Y_1}有效时的功耗情况进行仿真，分别如图 7(a)、图 7(b)所示。由于在路径平衡结构 *and* NCL 异步电路中，输入信号没有与运算路径绑定，攻击者只能通过分析平均功耗的方法试图获取参与运算的数据。通过对图 7(a)和图 7(b)中的电流曲线积分，乘以 *VDD* 再除以时间间隔可以发现，2 个场景中的平均功耗均为 0.25 uWatts。



(a) {X_0, Y_1}有效时的功耗曲线



（b）{X_1, Y_1}有效时的功耗曲线

图 7　路径平衡结构 *and* NCL 异步电路功耗仿真

因此，在路径平衡结构 *and* NCL 异步电路运行的过程中，通过分析平均功耗，攻击者不能获取到任何功耗旁路信息。从而能够有效地抵御 DPA 攻击，防止功耗旁路信息的泄露。

6　结束语

围绕基于 NCL 异步电路的抗功耗分析问题，本文给出了实现 NCL 异步电路路径平衡结构的充分条件，并提出了一种基于 BDD 的路径结构平衡扩展方法。该方法能够在不改变目标电路特性的前提下有效地实现 NCL 异步电路的路径平衡结构，抵消由于寄生电容和负载电容差异所造成的旁路信息泄露，达到提高系统安全性的目的。此外，该方法还能扩展至各类自动化综合过程中，对于实现各类具备高等级抗功耗分析能力的密码芯片自动化设计具有重要意义。

参考文献：

[1] KOCHER P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[A]. Advances in Cryptology'96[C]. Berlin, Germany, 1996. 104-113.

[2] MESSERGES T S, DABBISH E A, SLOAN R H. Investigations of power analysis attacks on smartcards[A]. Proc USENIX Workshop Smartcard Technology[C]. Chicago, USA, 1999. 151-161.

[3] KOCHER P, JAFFE J, JUN B. Differential power analysis[A]. Advances in Cryptology'99[C]. Singapore, 1999. 388-397.

[4] FISCHER W, GAMMEL B M, KNIFFLER O, *et al*. Differential power analysis of stream ciphers[A]. CT-RSA 2007[C]. San Francisco, USA, 2007. 257-270.

[5] MCEVOY R, TUNSTALL M, MURPHY C C, *et al*. Differential power analysis of HMAC based on SHA-2, and countermeasures[A]. LNCS 4867:WISA 2007[C]. Beijng, China, 2007. 317-332.

[6] CLAVIER C, FEIX B, GAGNEROT G, *et al*. Improved collision-correlation power analysis on first order protected AES[A]. LNCS 6917: CHES 2011[C]. Nara, Japan, 2011. 49-62.

[7] ROCHE T, LOMN_E V, KHALFALLAH K. Combined fault and side-channel attack on protected implementations of AES[A]. The 10th IFIP WG 8.8/11.2 International Conference(CARDIS 2011)[C]. Leuven, Belgium, 2011. 65-83.

[8] TIRI K, VERBAUWHEDE I. 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.

[9] MARZOUQI H, SALAH K, AL-QUTAYRI M, *et al*. A unified countermeasure against side channel attacks on cryptographic RFID[A]. The 6th International Conference for Internet Technology and Secured Transactions(ICITST 2011)[C]. Abu Dhabi, 2011.13-18.

[10] BILGIN B, NIKOVA S, NIKOV V, *et al*. Threshold implementations of all 3×3 and 4×4 S-Boxes[A]. LNCS 7428: CHES 2012[C]. Leuven, Belgium, 2012. 76-91.

[11] JAFFE J, KOCHER P, JUN B. Balanced cryptographic computational method and apparatus for leak minimization in smartcards and others Cryptosystems[EB/OL]. http://patentscope.wipo.int.

[12] FANT K M, BRANDT S A. Null convention logic: a complete and consistent logic for asynchronous digital circuits synthesis[A]. Proc of International Conference on Application Specific Systems, Architectures and Processors[C]. Chicago, USA, 1996. 261-273.

[13] MARTIN A J. The limitations to delay-insensitivity in asynchronous circuits[A]. Proceedings of the Sixth MIT Conference[C]. 1990. 263-278.

[14] BOUESSE G F, SICARD G, RENAUDIN M. Path swapping method to improve DPA resistance of quasi delay insensitive asynchronous circuits[A]. LNCS 4249:CHES 2006[C]. Yokohama, Japan, 2006. 384-398.

[15] SEITZ C L. System Timing, in Introduction to VLSI Systems[M]. Addison-Wesley, 1980. 218-262.

[16] 管旭光, 周端，杨银堂. 一种零协议逻辑全异步流水线电路的优化设计研究[J]. 半导体学报, 2009, 30(7):75010-75016.
GUAN X G, ZHOU D, YANG Y T. Optimization design of a full asynchronous pipeline circuit based on null convention logic[J]. Journal of Semiconductors, 2009, 30(7):75010-75016.

[17] KAPOOR H K, ASTHANA A, KRILAVICIUS T, *et al*. Towards a language based synthesis of NCL circuits[A]. Proceedings of the International Multi Conference of Engineers and Computer Scientists (IMECS)[C]. Hong Kong, China, 2010.1033-1038.

[18] GOWDA T, VRUDHULA S, KULKARNI N, *et al*. Identification of threshold functions and synthesis of threshold networks[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2011, 30(5):665-673.

作者简介：

罗芳（1983-），女，江西吉安人，海军工程大学讲师，主要研究方向为密码分析、旁路攻击防御。

欧庆于（1978-），男，江西萍乡人，海军工程大学副教授，主要研究方向为密码芯片设计与安全防护。

吴晓平（1961-），男，山西新绛人，海军工程大学教授、博士生导师，主要研究方向为复杂系统分析。