

基于 WDDL 和行波流水技术的抗功耗攻击 高性能分组密码协处理器设计与实现

童元满 王志英 戴 葵 陆洪毅 石 伟

(国防科学技术大学计算机学院 长沙 410073)

摘 要 该文结合 WDDL 逻辑和行波流水技术,给出了分组密码协处理器的设计方法和设计流程.该设计流程实现简单,最大限度地利用了现有的成熟 EDA 工具.这种协处理器不仅能有效抗功耗攻击,而且具有运算性能高和功耗低的优势.文中以 DES 算法为例,给出了基于 WDDL 和行波流水技术的协处理器.实验结果表明,文中给出的分组密码协处理器设计方法以一定的芯片面积为代价获得了抗功耗攻击的能力,具有高运算性能和低功耗的优势.

关键词 功耗攻击;WDDL;行波流水;分组密码算法;协处理器;高性能;设计流程

中图法分类号 TP331

Designing Power Analysis Resistant and High Performance Block Cipher Coprocessor using WDDL and Wave-Pipelining

TONG Yuan-Man WANG Zhi-Ying DAI Kui LU Hong-Yi SHI Wei

(School of Computer, National University of Defense Technology, Changsha 410073)

Abstract Novel design method and design flow of block cipher is presented based on the WDDL (Wave Dynamic Differential Logic) and Wave-Pipelining techniques. This design flow utilized the current commercially available EDA tools to a large degree. The WDDL and wave-pipelining based coprocessor not only resists power analysis, but also achieves high performance and low power consumption in nature. According to the design flow, this paper implements a DES coprocessor. The simulation results show that the novel design method achieves high performance, low power consumption and power analysis resistant ability at the cost of chip area.

Keywords power analysis attack; WDDL; wave-pipelining; block cipher; coprocessor; high performance; design flow

1 引 言

分组密码算法是信息安全的核心技术,主要用以保证数据的机密性,因而分组密码协处理器也是

安全芯片中的关键模块.分组密码算法的安全性主要包括两方面内容,一是数学上的安全性;二是与实现相关的安全性.当前主流分组密码算法在数学上都具有高安全性,几乎无法破解.但是密码算法的实现可能存在一定的薄弱之处,成为破解的目标.旁路

收稿日期:2006-04-27;最终修改稿收到日期:2007-11-27.本课题得到国家自然科学基金(60706026)资助.童元满,男,1982年生,博士研究生,主要研究方向为抗旁路攻击的安全 SOC 芯片设计、密码算法 VLSI 实现. E-mail: yuanmantong@yahoo.com.cn. 王志英,男,1956年生,博士,教授,博士生导师,主要研究领域为高性能计算机体系结构、异步微处理器设计、计算机系统安全.戴 葵,男,1968年生,博士,副教授,主要研究方向为高性能微处理器设计、高可靠微处理器设计、信息安全.陆洪毅,男,1974年生,博士,副教授,主要研究方向为嵌入式系统、旁路攻击防护技术.石 伟,男,1982年生,博士研究生,主要研究方向为计算机系统结构、旁路攻击防护技术.

攻击方法就是一种利用密码算法实现时的薄弱之处来实施破解的攻击方法,比如时间攻击(Timing Analysis)、电磁辐射攻击(Electromagnetic Side-channel Analysis)以及功耗攻击(Power Analysis)等.由于密码算法执行时功耗与密钥之间存在一定相关性,功耗攻击通过采集大量功耗样本,利用数理统计方法来分析密钥的值^[1-2].功耗攻击方法具有简单有效的特点,给以智能卡为代表的安全芯片带来安全威胁.

为有效抗功耗攻击,在设计实现密码算法时可从不同角度采取防护技术,比如功耗恒定化和功耗随机化技术^[3].这些防护技术或者牺牲了运算性能^[3-4],比如在运算过程中插入了随机的延时和无效操作;或者造成功耗的大幅度增加,比如采用动态双轨逻辑以使得功耗恒定化^[5-6].本文主要在分组密码协处理器的抗功耗攻击能力和运算性能、面积以及功耗之间寻求一个较好的折衷解决方案.

文献[7-10]提出采用 WDDL(Wave Dynamic Differential Logic)逻辑来实现密码协处理器,其基本思想就是基于 WDDL 单元的功耗恒定特性来达到抗功耗攻击目的.本文在 WDDL 逻辑的基础上,结合行波流水(Wave Pipeline)技术^[11-12],给出了一种既能有效抗功耗攻击,又具有较高性能的分组密码算法的硬件实现技术.

本文在介绍 WDDL 和行波流水技术的基础上,分析这两种技术结合实现分组密码算法的可行性及优势,然后给出实现分组密码算法的设计方法和设计流程,并且分析基于 WDDL 和行波流水技术的分组密码协处理器的运算性能、面积、功耗以及安全性等.

2 WDDL 和行波流水技术原理

基于 WDDL 逻辑的电路具有如下特点^[7-10]:

- (1) 仅由二输入与门和或门(以下记为 AND2 和 OR2)实现所有的逻辑功能;
- (2) 根据德·摩根律,由 AND2 和 OR2 组成双轨逻辑单元,如图 1(a)和图 1(b)所示,双轨与门和或门分别记为 WAND2 和 WOR2;

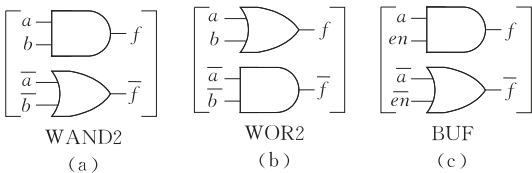


图 1 WDDL 逻辑单元

(3) 所有逻辑单元具有两种工作状态,预充和求值.与动态电路不同的是, WDDL 电路中无需全局预充信号(一般为时钟信号),而只需将 WDDL 电路的输入置为 0,则整个 WDDL 电路将逐级预充为 0,相当于预充控制信号逐级传递,如图 2 所示,经过一级与门(或门)延时之后, z_1, z_2 预充为 0,依此类推, z_3, O_2 依次预充为 0.

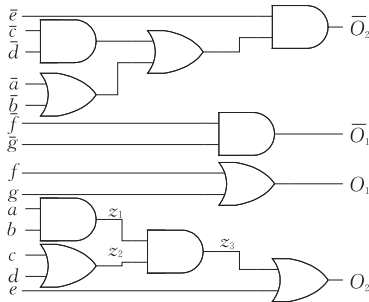


图 2 WDDL 电路实例

(4) 当 WDDL 单元双轨输出信号的等效负载电容相同, WDDL 单元具有功耗恒定特性.在负载平衡条件下,双轨与门 WAND2 的瞬态电流(Spice 模拟结果)如图 3 所示.在不同输入下, WAND2 消耗几乎相同的功耗.

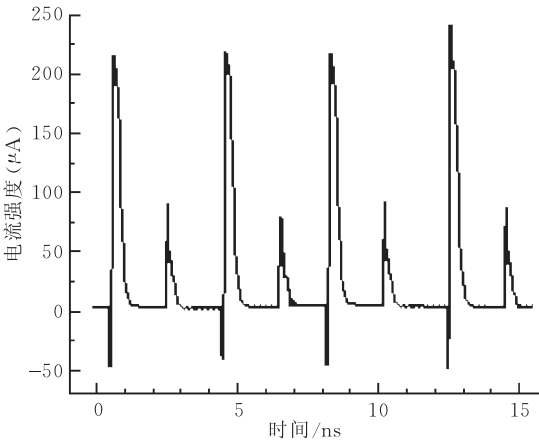


图 3 WDDL 单元的 Spice 模拟结果

行波流水是一种超高性能的集成电路设计技术^[11-12],其基本原理为:对于组合电路来说,当前数据处理完成之前,在保证不发生冲突的前提下输入下一组数据,这样同一组合电路中可能有多组数据被处理;每一组数据称为一个数据流(data wave).假设组合电路的关键路径延时为 t_c ,两组数据的输入间隔为 Δt ,则该组合电路可以看成为 $(t_c/\Delta t)$ 级的流水线,且相邻流水段之间无锁存,大大提高了电路的吞吐率.

虽然行波流水技术具有运算性能方面的优越性,但实现难度较大,目前并没有成熟的设计流程和

EDA 工具支持. 由于 WDDL 电路仅包括二输入的与门或或门两种逻辑单元, 二者延时基本相当, 如果采用行波流水技术来实现 WDDL 电路, 则可以大大降低设计难度. 另一方面, 分组密码算法具有良好的结构, 由若干次迭代组成并且各轮迭代的运算过程基本相似, 在 ECB 模式下, 单次加解密运算中不存在反馈结构, 且其硬件实现可由纯算术逻辑电路组成而不包括存储器, 因此其适合于采用行波流水技术实现. 由于行波流水电路中不包括时钟信号和寄存器, 并且由于 WDDL 电路的功耗恒定特性, 因此基于 WDDL 和行波流水技术的分组密码算法协处理器能够有效抗功耗攻击, 并且具有高运算性能和低功耗特性. 综上, 利用 WDDL 和行波流水技术实现分组密码算法不仅是完全可行的, 也具有运算性能和安全性方面的优势. 为简单起见, 下面将 WDDL 和行波流水技术的结合记为 WDP.

3 基于 WDP 技术的分组密码协处理器结构

基于 WDP 技术的分组密码协处理器具有如图 4 所示的多层次互联网络结构, 包括逻辑输入层、逻辑运算层以及逻辑输出层, 每一层仅接受来自上一层次的输入. 图 4 中 (in, \bar{in}) 为双轨输入向量, (out, \bar{out}) 为双轨输出向量. 逻辑运算层包括三种逻辑单元: WAND2、WOR2 以及 BUF. 其中 BUF 为一延时单元, 其结构如图 1(c) 所示. 在预充阶段, 所有输入置为 0, 经过一级延时之后输出预充到 0; 在求值阶段, en 置为 1, 而 \bar{en} 保持为 0, 则 (f, \bar{f}) 分别稳定到 (a, \bar{a}) , 完成了对双轨信号 (a, \bar{a}) 的缓冲功能.

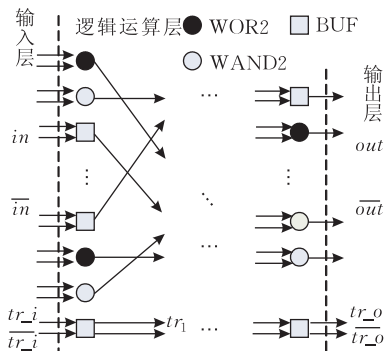


图 4 基于 WDP 技术的协处理器结构

(tr_i, \bar{tr}_i) 为双轨的运算触发控制信号, 当且仅当 tr_i 为 1 且所有数据输入有效时, WDP 协处理器作有效运算; 当 tr_i 为 0 时, 同时保证数据输入全为 0, WDP 协处理器不做有效运算, 进入预充状

态. tr_i 和 \bar{tr}_i 通过 BUF 单元逐级传递, 经过与逻辑运算层相同级数的缓冲之后输出到 tr_o 和 \bar{tr}_o . 当 tr_o 由 0 翻转到 1 时, 表明当前数据处理完毕, 输出向量 out 为有效结果. 对于第 i 级逻辑运算层上的 BUF 单元来说, 其双轨输入 (en, \bar{en}) 分别为第 $i-1$ 级的运算触发传递信号 $(tr_{i-1}, \bar{tr}_{i-1})$.

上述分组密码协处理器的运算模型可记为 $ENC(IN, L_1, \dots, L_n, OUT)$, 其中 IN, OUT 分别为输入和输出信号的集合; $L_i (1 \leq i \leq n)$ 为第 i 级逻辑运算层的所有信号集合. 该运算模型满足如下条件:

$$\forall o \in OUT, o = (x \wedge y), \text{ or } o = (x \vee y),$$

$$x, y \in L_n;$$

$$\forall z \in L_i, z = (x \wedge y), \text{ or } z = (x \vee y), i > 1,$$

$$x, y \in L_{i-1};$$

$$\forall z \in L_1, z = (x \wedge y), \text{ or } z = (x \vee y),$$

$$x, y \in IN.$$

在上述运算模型中, 逻辑运算层的各级延时大致相当, 并且所有逻辑单元的两个输入的到达时间几乎相同, 因此上述结构可以按照行波流水方式进行工作. 相邻两组数据的输入间隔 Δt 为各逻辑运算层中的最大延时, 也就是具有最大扇出的逻辑单元的门延时与互联线延时之和, 具体计算方式为

$$\Delta t = t_{\text{intrinsic}} + (K_{\text{load}} \times C_{\text{load}}) \quad (1)$$

式(1)中 $t_{\text{intrinsic}}$ 表示逻辑单元的负载为 0 时的延时, C_{load} 表示单元的负载电容, 而 K_{load} 表示逻辑单元的负载延时因子.

基于上述结构, 本文给出的分组密码协处理器的工作流程如图 5 所示, 预充过程与有效运算过程交替进行; 在同一时刻, 可能有多组数据被处理.

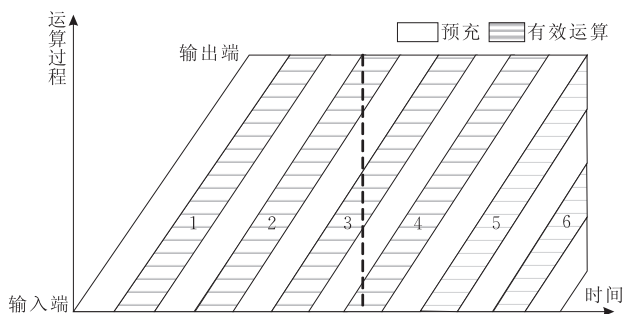


图 5 WDP 电路的工作流程

4 基于 WDP 技术的分组密码协处理器设计流程

分组密码算法具有十分规则的结构, 包含若干次迭代, 每轮迭代完成基本一致的运算并且具有良

好的模块化结构. 为降低设计复杂度, 本文按照自顶向下的方式划分子模块, 在得到各子模块的 WDP 网表之后, 再自底向上组合各子模块以得到整个分组密码算法协处理器的 WDP 网表. 例如, DES 算法的每轮迭代就可以划分密钥扩展、8 个 S 盒和置换等子模块.

对于一子模块来说, 按如下步骤得到该子模块的 WDP 网表:

(1) HDL 描述. 用 HDL 语言描述子模块的功能;

(2) 综合. 仅用反相器、二输入与门和或门等 3 种单元综合上述 HDL 代码, 得到子模块的静态单轨网表. 由于 (\sim, \vee, \wedge) 是布尔代数中的完备联结词集(对应于上述 3 类标准单元), 因此这个步骤在数学上是完备的. 由于没有引入特殊标准单元, 并且无额外约束, 该步骤可以使用目前成熟的综合工具, 如 Synopsys Design CompilerTM等.

(3) SR-WDDL. 将静态单轨网表转换为 WDDL 网表. 由于 WDDL 网表中所有信号都是双轨的, 因此无须反相器. 对于静态单轨网表中的与门(或门)实例来说, 根据德·摩根律增加一个互补的或门(与门)实例即可. 具体的转换规则如下所示, 其中 A 和 B 表示逻辑单元的输入端, Z 表示逻辑单元的输出端.

i. 对于任意的反相器实例 $\text{INV } U1(.A(X_1), .Z(Z_1))$ 而言, 将网表中信号 Z_1 的所有出现替换为 $\overline{X_1}$, 将信号 Z_1 的反相 $\overline{Z_1}$ 替换为 X_1 ;

ii. 对于任意的与门实例 $\text{AND2 } U2(.A(X_2), .B(Y_2), .Z(Z_2))$ 而言, 根据德·摩根律增加一个与 $U2$ 互补的或门实例 $\text{OR2 } N_U2(.A(\overline{X_2}), .B(\overline{Y_2}), .Z(\overline{Z_2}))$;

iii. 对于任意的或门实例 $\text{OR2 } U3(.A(X_3), .B(Y_3), .Z(Z_3))$ 而言, 根据德·摩根律增加一个与 $U3$ 互补的与门实例 $\text{AND2 } N_U3(.A(\overline{X_3}), .B(\overline{Y_3}), .Z(\overline{Z_3}))$.

(4) 路径平衡. 在 WDDL 网表中可能存在某些逻辑单元的输入到达时间不同, 也就是说从子模块的输入端到该逻辑单元所经过的逻辑处理级数不同. 如图 2 中 Z_3 与 e 的到达时间差别明显, 如果按照行波流水方式工作, 不仅造成时序分析的困难, 也不能有效提高运算性能. 本文通过插入 BUF 的方式得到如第 3 节所示的多层互联网络结构, 使得所有逻辑单元的两个输入端到达时间基本一致, 从而可

以易于按照行波流水的方式工作. 以下简要介绍路径平衡的具体过程.

WDDL 网表中的任意逻辑输出端 O 的逻辑表达式均可以用一棵二叉树来表示. 二叉树中每个结点表示 WDDL 网表中的信号, 其子结点要么为空, 要么为对应逻辑单元的两个输入信号; 二叉树的高度表示从输入端到输出端所经过的逻辑运算级数, 如图 2 所示. 电路中输出 O_2 对应的二叉树如图 6(a)所示, 该二叉树高度为 3. 对根结点 O_2 来说, 其二个子结点 z_3 和 e 的到达时间明显不同, 需要对输入信号 e 插入两级缓冲, 也就是在 WDDL 网表中增加两个相应的或门实例(如图 6(b)所示): $\text{OR2 } B_U1(.A(e), .B(tr_i), .Z(e_1))$ 和 $\text{OR2 } B_U2(.A(e_1), .B(tr_1, .Z(e_2)))$, 并将原网表中 e 的出现替换为 e_2 . 当然, 对于 $\overline{O_2}$ 而言, 需要插入互补的与门实例. 为简单起见, 下面用 $\text{InsertBuf}(x, h)$ 表示为输入信号 x 插入 h 级缓冲, 用 $\text{Height}(z)$ 表示二叉树中结点 z 的高度. 基于上述的二叉树表示方法, 对输出端 O 进行路径平衡的过程如算法 1 所示.

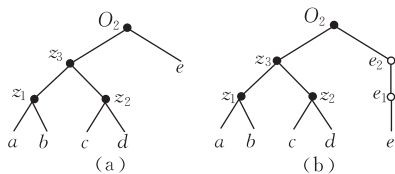


图 6 路径平衡的基本方法

算法 1. 输出信号 O 的路径平衡过程.

```

BalanceBranch(O)
{
    if (IN1(O) ∈ IN) //IN1(O)表示 O 的一个输入端,
        IN 为初始输入信号的集合
    {
        InsertBuf(IN1(O), Height(O)-1);
        if (IN2(O) ∈ IN) //IN2(O)表示 O 的另一输入端
        { InsertBuf(IN2(O), Height(O)-1); return; }
        else
            BalanceBranch(IN2(O)); //递归调用
    }
    else
    {
        BalanceBranch(IN1(O)); //递归调用
        if (IN2(O) ∈ IN)
        { InsertBuf(IN2(O), Height(O)-1); return; }
        else
            BalanceBranch(IN2(O)); //递归调用
    }
}

```

另外,子模块中不同输出端对应的二叉树高度可能不同,也就是从输入端到输出端的所经过的逻辑处理级数不同.为保证所有输出端的路径延时基本一致,需要为具有较小逻辑处理级数的输出端增加缓冲.在如图 2 所示的电路中,需要为输出端 O_1 增加两级缓冲,具体过程不再赘述.为简单起见,下面以 $AppendBuf(O, l)$ 表示为输出端 O 增加 l 级缓冲.

综上所述,子模块的路径平衡过程如算法 2 所示.

算法 2. 子模块的路径平衡过程.

```
BalanceModule(OUT) //OUT={O1, O2, ..., On}
{
    H=max(Height(Oi)), 1≤i≤n;
    for each Oi(1≤i≤n) in OUT
    {
        BalanceBranch(Oi);
        AppendBuf(Oi, H-Height(Oi));
    }
}
```

以上介绍了怎样得到一个子模块的 WDP 网表,下面介绍怎样将两个子模块组合成更大的模块.如果两个子模块 M_1 和 M_2 是串联的,则直接互联即可.如果 M_1 和 M_2 是并联的,设二者的逻辑处理级数分别为 L_1 和 L_2 ,且 $L_1 \geq L_2$,则为子模块 M_2 的所有输出端增加 $(L_1 - L_2)$ 级缓冲.基于上述方法,可以递增地将若干个子模块组合成宏模块.

设某分组密码算法的迭代轮数为 R ,则该分组密码算法的设计流程如下:

1. for i from 1 to R step by 1
 - 1.1. 将第 i 轮迭代划分成逻辑上独立的若干子模块,按照上述子模块的设计流程得到各子模块的 WDP 网表;
 - 1.2. 按子模块的组合方法组合步 1.1 中各子模块网表以得到第 i 轮变换逻辑的 WDP 网表;
 2. 将各轮变换逻辑的网表依次串联,得到分组密码协处理器的完整 WDP 网表;
 3. 布局布线(Place and Route):布局布线关键在于保证 WDDL 单元的双轨输出具有相同的负载,这样即可获得与输入无关的恒定功耗特性.随着工艺尺寸的减小,互连线的电容逐渐成为负载电容的最主要部分.假定双轨信号走线相同,则双轨信号的互联电容相同. Tiri 提出了一个在当前成熟 EDA 工具基础上的双轨布局布线方法^[8],能够达到均衡互连线负载电容的效果,该方法可以应用于本文的设计中.
 4. 对后端设计流程得到的协处理器版图进行 DRC 和 LVS 验证;
 5. 时序分析:确定协处理器以行波流水方式工作时相邻两次输入的最小间隔 Δt . 根据式(1),该步骤相当于找出

具有最大延时的逻辑单元.

上述设计流程最大限度地利用了现有的成熟 EDA 工具,无须定制标准单元,并且对后端设计没有特殊要求,无长互联线,布局布线简单.

5 性能以及安全性分析

设分组密码算法协处理器两组输入的时间间隔为 Δt ,并且协处理器的逻辑处理级数为 N .按照第 3 节所述的运算流程,预充与正常数据处理交替进行,因此完成一次数据加(解)密处理所需要的时间为 $(N+1)\Delta t$.当协处理器满负荷工作时,协处理器的最大吞吐率 TP_{\max} 为

$$TP_{\max} = \frac{1}{2\Delta t} \quad (2)$$

协处理器执行 m 组数据加(解)密操作的实际吞吐率 TP 为

$$TP = \frac{m}{(N+1)\Delta t + 2(m-1)\Delta t} = \frac{TP_{\max}}{1 + (N-1)/2m} \quad (3)$$

由式(3)可知,当 $m \gg N$ 时,协处理器的实际吞吐率接近于最大吞吐率,协处理器的性能得到充分发挥.

以上讨论了基于 WDP 技术的分组密码协处理器的运算性能,下面简要分析协处理器的抗功耗攻击能力.

根据 WDP 电路的描述,可以得到如下结论.

引理 1. WDP 电路中任意双轨信号 z 和 \bar{z} 的扇出相同.

根据 WDDL 电路的描述,上述引理显然成立.根据上述结论以及负载平衡的布局布线过程,可知任意双轨信号 z 和 \bar{z} 的负载基本一致.基于 WDDL 逻辑单元的功耗恒定特性,记任意 WDDL 逻辑单元 U_i 在时刻 t 的功耗 $E_i(t)$ 为

$$E_i(t) = P_i(t) + \epsilon_i \quad (4)$$

上式中 $P_i(t)$ 为与单元 U_i 和时刻 t 相关的恒定值,而 ϵ_i 为噪声.噪声 ϵ_i 来源于多个方面,如热噪声等,并设 ϵ_i 服从参数为 $(0, \sigma^2)$ 的正态分布.

引理 2. 基于 WDP 技术的分组密码协处理器可以抗 DPA 攻击.

证明. 设 DPA 攻击的区分函数为 $z_j = D(k, C_j)$,其中 k 为攻击者猜测的密钥的一部分, C_j 为第 j 组样本对应的密文;攻击者根据 z_j 的值将功耗样本分为两个子集 S_1 和 S_0 .假设 z_j 产生于时刻 t ,则样本子集 S_1 和 S_0 在时刻 t 的功耗均值之差为 $\Delta E(t)$ ^[2]:

$$\Delta E(t) = \left(\sum_{j=1}^m z_j P(j, t) / \sum_{j=1}^m z_j \right) - \left(\sum_{j=1}^m (1 - z_j) P(j, t) / \sum_{j=1}^m (1 - z_j) \right) \quad (5)$$

上式中 m 为样本数, $P(j, t)$ 表示第 j 组功耗样本在时刻 t 的值, 其表达式为

$$P(j, t) = \sum_{i=1}^M E_i(t) = \sum_{i=1}^M [P_i(t) + \epsilon_i] \quad (6)$$

上式中 M 表示协处理器中 WDDL 逻辑单元的个数。
将式(6)代入式(5)可知 $\Delta E(t)$ 的均值为 0, 这表明不管 k 的猜测是否正确, 均不能观察到功耗均值偏差 $\Delta E(t)$ 的峰值, 因此 DPA 攻击无法实施。

证毕。

推论 1. 基于 WDP 技术的分组密码协处理器可以抗高阶功耗攻击。

在引理 2 的证明过程中, 式(6)表明了协处理器的功耗与其输入的无关性。因此攻击者无法选择可行的区分函数以实施高阶功耗攻击。

另外, 本文给出的基于 WDP 技术的分组密码协处理器还具有低功耗的特点, 这主要由于协处理器中无全局时钟信号、无寄存器和长互连线, 因此避免了因时钟、寄存器和长互连线引起的功耗。另外, 当且仅当向协处理器输入有效数据并且运算触发控制信号 tr_i 为高电平时, 协处理器才执行有效运算; 不执行有效运算时输入全部保持为 0, 电路处于稳定状态, 不消耗任何功耗。

6 实验结果

本文根据上述 WDP 分组密码协处理器的设计流程, 设计实现了 DES 算法协处理器。该协处理器的一些具体性能指标如表 1 所示。本文之所以选取 DES 算法对文中提出的设计技术进行验证, 是因为 DES 算法最为简单, 其硬件实现方式比较直观。但是文中提出的设计技术对于其它分组密码算法也是

同样适用的, 比如当前应用非常广泛的 AES 算法。但对于 AES 算法而言, 其中唯一的非线性变换即 S 盒不能采用查表(访问 ROM)方式实现, 而必须采用算术逻辑运算电路实现; 如文献[13]采用 WDDL 逻辑实现了 AES 协处理器。

本文实现的基于 WDP 技术的 DES 算法协处理器的版图如图 7 所示。根据协处理器的版图, 提取带寄生参数的 Spice 网表, 在 Synopsys PowerMill™ 中模拟得到的动态功耗曲线如图 8 所示。可以看出, 即使输入不同, 协处理器消耗的功耗几乎一致。

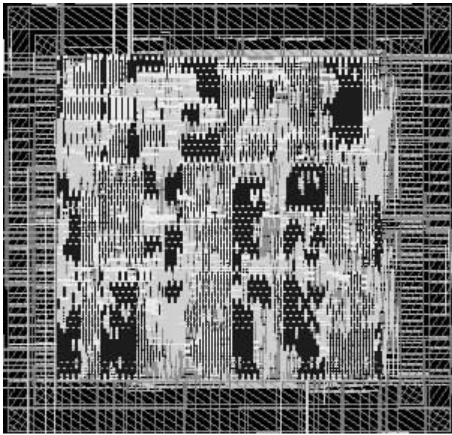


图 7 基于 WDP 技术的 DES 协处理器版图

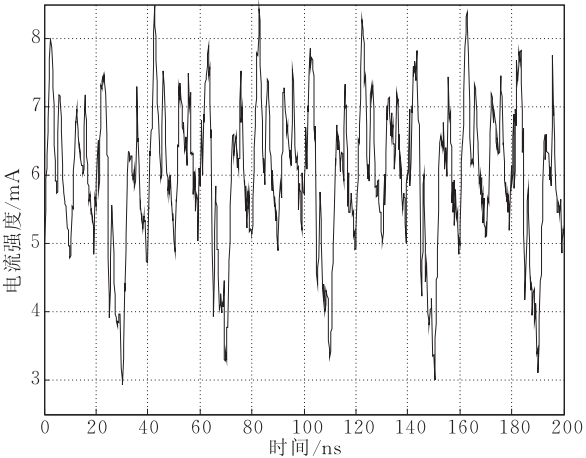


图 8 DES 协处理器的动态电流曲线

表 1 基于 WDP 技术的 DES 协处理器性能指标

类别	逻辑处理级数	门数	$\Delta t/\text{ns}$	单次加密运算延时(ns)
具体指标	192	76K	0.3	58
说明	DES 算法包括 16 轮变换	二输入与门和或门的总数	0.18 μm 工艺条件下的分析结果	逻辑处理级数与输入间隔的乘积

以上给出了基于 WDP 技术的 DES 协处理器的性能指标, 下面将其与其它典型的 DES 实现做简单比较, 包括未采取任何防护技术的实现和基于随机掩码技术的 DES 实现^[14]。所谓随机掩码技术就

是在执行密码运算之前, 令明(密)文与随机向量按位异或, 在运算结束之后再恢复出正确的结果; 这样使得中间结果与密钥无关, 从而达到抗 DPA 攻击的目的^[14]。为便于比较, 本文假定上述两种实现都

采用静态单轨标准单元实现,每轮迭代作为流水线的一段,并且采用同步方式工作.具体的比较如表 2 所示.

表 2 不同实现的比较

	门数	单次加密 运算延时/ns	最大 吞吐率/(ns ⁻¹)	可实施的 攻击
常规实现	37K	64	0.25	DPA
随机掩码 ^[14]	72K	>64	0.25	二阶功耗攻击 ^[15]
WDP	76K	58	3.3	/

从表 2 可以看出,本文提出的 WDP 技术与随机掩码技术所需的硬件开销基本相当,即约为常规实现的 2 倍;文献[15]指出文献[14]中随机掩码技术无法抗二阶功耗攻击.基于 WDP 技术的 DES 协处理器以一定的芯片面积为代价,具有运算性能和安全性等方面的优势.

7 结束语

本文给出了基于 WDP 技术的分组密码协处理器设计方法和设计流程.基于 WDP 技术的 DES 协处理器性能评测结果表明本文给出的设计方法以一定的芯片面积为代价,获得了抗功耗攻击能力,具有高运算性能和低功耗的优势.

由于 WDP 协处理器中无全局同步时钟,属于自定时(self-timed)电路.本文在下一步的工作中将探讨 WDP 协处理器在典型的全局同步安全 SOC 中的集成方法.

参 考 文 献

[1] Kocher P, Jaffe J, Jun B. Differential power analysis//Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara, California, USA, 1999: 388-397

[2] Messerges T, Dabbish E A, Sloan R H. Examining smart-card security under the threat of Power analysis attacks. IEEE Transactions on Computers, 2002, 51(5): 541-552

[3] Mangard S. Securing implementations of block ciphers against side-channel attacks[Ph. D. dissertation]. Graz University of Technology, Graz, Austria, 2004

[4] Tong Yuan-Man, Wang Zhi-Ying, Dai Kui, Lu Hong-Yi. Power analysis resistant method for scalar multiplication based on randomized mixed coordinates. Journal of Chinese Computer Systems, 2007, 28(1): 159-165(in Chinese)

(童元满,王志英,戴葵,陆洪毅.一种基于随机混合坐标表示

的防功耗分析标量乘法实现方法.小型微型计算机系统, 2007, 28(1): 159-165)

[5] Tong Yuan-Man, Wang Zhi-Ying, Dai Kui, Shi Wei, Lu Hong-Yi. Semi-custom design flow: Protecting security IC's against power analysis based on dynamic dual-rail logic. Journal of Chinese Computer Systems, 2007, 28(5): 935-939(in Chinese)

(童元满,王志英,戴葵,石伟,陆洪毅.基于动态双轨逻辑的抗功耗攻击安全芯片半定制设计流程.小型微型计算机系统, 2007, 28(5): 935-939)

[6] Schneider H. Analysis of the resistance of different logic styles against SPA & DPA attacks[M. S. dissertation]. Graz University of Technology, Graz, Austria, 2003

[7] Tiri K, Verbauwhede I. Securing encryption algorithms against DPA at the logic level: Next generation smart card technology//Cryptographic Hardware and Embedded Systems. Cologne, Germany, 2003: 125-136

[8] Tiri K, Verbauwhede I. Place and route for secure standard cell design//Proceedings of the 6th International Conference on Smart Card Research and Advanced Applications. Toulouse, France, 2004: 143-158

[9] Tiri K, Verbauwhede I. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation//Proceedings of the Design, Automation and Test in Europe Conference. Paris, France, 2004: 246-251

[10] Tiri K, Verbauwhede I. A VLSI design flow for secure side-channel attack resistant ICs//Proceedings of the Design, Automation and Test in Europe Conference. Munich, Germany, 2005: 58-63

[11] Wong D C, Micheli G De, Flynn M J. Designing high-performance digital circuits using wave pipelining: algorithms and practical experiences. IEEE Transactions on CAD of IC and Systems, 1993, 12(1): 25-46

[12] Burleson W P, Ciesielski M, Klass F, Liu W. Wave-pipelining: A tutorial and research survey. IEEE Transactions on VLSI Systems, 1998, 6(3): 464-474

[13] Tiri K, Hwang D, Hodjat A, Lai B, Yang S, Schaumont P, Verbauwhede I. AES-based cryptographic and biometric security coprocessor IC in 0.18-μm CMOS resistant to side-channel power analysis attacks//Proceedings of the Symposium on VLSI Technology and Circuits. Hualien, Taiwan, 2005: 216-219

[14] Akkar M L, Giraud C. An implementation of DES and AES, secure against some attacks//Proceedings of the Cryptographic Hardware and Embedded Systems. Paris, France, 2001: 309-318

[15] Akkar M L, Goubin L. A generic protection against high-order differential power analysis//Proceedings of the Fast Software Encryption. Lund, Sweden, 2003: 192-205



TONG Yuan-Man, born in 1982, Ph. D. candidate. His research interests include cryptographic hardware design, methodology of secure SOC's, side-channel attacks resistant implementing techniques.

WANG Zhi-Ying, born in 1956, Ph. D. , professor. His research interests include high performance architecture, asynchronous microprocessor, and information security.

Background

Power analysis attack is firstly proposed by P. Kocher in 1999. It is a very powerful attack to break the stored secret key in secure chip such as smart card. And it can be used to break almost all kinds of implementations of cryptographic algorithms without appropriate countermeasures. The countermeasures to prevent power analysis attack are divided into two groups. The one is to randomize the power consumption, and the other one is to make the power consumption constant, i. e. independent of the secret key. To achieve constant power consumption, several novel logic styles are proposed. These logic styles include SABL (sense amplifier based logic), WDDL (wave dynamic and differential logic), and MDPL (masked dual-rail and pre-charge logic) etc. And these novel logic styles have been used to implement different block cipher coprocessors. However, the hardware complexity, power consumption are greatly increased, and the per-

DAI Kui, born in 1968, Ph. D. , associate professor. His research interests include high performance microprocessor, computer architecture, and information security.

LU Hong-Yi, born in 1974, Ph. D. , associate professor. His research interests include embedded system and side-channel attacks resistant implementing techniques.

SHI Wei, born in 1982, Ph. D. candidate. His research interests include computer architecture and side-channel attacks resistant implementing techniques.

formance is decreased.

The authors have studied the SABL and implemented a standard cell library of SABL, and also proposed a semi-custom design flow of the hybrid implementation based on the static standard cell and SABL. The research of this paper belongs to the project (No. 60706026) funded by the Natural Science Foundation of China (NSFC). The main goal of this project is to research semi-custom design flow of power analysis resistant cryptographic devices, to research efficient countermeasures, design and implementation of secure SoCs (system on chip). In this paper, the WDDL and wave-pipelining are combined to implement power analysis resistant and high performance block cipher coprocessors. And the methodology to implement cryptographic coprocessors is presented and the experiment result of a practical DES coprocessor is shown.