基于动态补偿的椭圆曲线密码低成本抗功耗攻击策略及硬件结构研究

李 伟*① 曾 涵① 陈 韬① 南龙梅②

①(解放军信息工程大学 郑州 450000)

②(复旦大学专用集成电路与系统国家重点实验室 上海 200433)

摘 要：椭圆曲线密码(ECC)芯片的抗功耗攻击能力往往以电路性能、面积或功耗为代价。该文分析了在椭圆曲线密码 点乘运算中密钥猜测正确与错误时的中间数据汉明距离概率分布差异性，提出一种基于动态汉明距离调控的功耗补偿方法，利用模拟退火算法离线寻找最优的映射矩阵，最终形成椭圆曲线密码硬件电路的等概率映射补偿模型，大大降低了中间数据与功耗的相关性。同时，以该模型为指导设计了低成本的同步功耗补偿电路，在CMOS 40 nm工艺下，防护后的ECC128电路面积增加22.8%。基于Sakura-G开发板开展了测试验证，防护电路的功耗仅增加18.8%，最小泄露轨迹数大于10^4，抗相关功耗分析能力提升了312倍。该策略在与随机化方法防护能力相当的情况下，不损失电路性能且硬件成本小，适用于高速或资源受限的ECC电路。

关键词：椭圆曲线密码；相关功耗分析；低成本；模拟退火算法

中图分类号：TN918.2; TP316.4 **文献标识码**：A **文章编号**：1009-5896(2021)09-2439-10

DOI: 10.11999/JEIT210581

Dynamic Compensation Based Low-cost Power-analysis Countermeasure for Elliptic Curve Cryptography and Its Hardware Structure

LI Wei① ZENG Han① CHEN Tao① NAN Longmei②

①(*PLA Information Engineering University*, *Zhengzhou* 450000, *China*)

②(*State Key Laboratory of ASIC and System*, *Fudan University*, *Shanghai* 200433, *China*)

Abstract: The power-analysis countermeasure for Elliptic Curve Cryptographic (ECC) chips endures large area, power consumption and performance degradation. In this paper, the difference in the probability distribution of the intermediate data Hamming distance is analyzed when the key guess is correct and incorrect in the point multiplication of ECC. A power compensation method based on dynamic Hamming distance control is proposed, which uses the simulated annealing algorithm offline to find the optimal mapping matrix. Finally, a mapping compensation model of equal probability on the elliptic curve cryptographic hardware is formed, which greatly reduces the correlation between intermediate data and power consumption. At the same time, a low-cost synchronous power compensation circuit is designed in the guidance of this model. Under the CMOS 40 nm process, the area of protected ECC128 is only increased by 22.8%. Experiments and tests are carried out on the Sakura-G board. The power overhead is 18.8%, and the number of minimum leakage traces is greater than 10^4, which is increased by 312 times. This countermeasure is the same as randomization with low cost and no impact on the throughput rate, which is suitable for high-speed or resource-constrained ECC circuits.

Key words: Elliptic Curve Cryptography (ECC); Correlation Power Analysis (CPA); Low cost; Simulated annealing algorithm

收稿日期：2021-06-16；改回日期：2021-08-16；网络出版：2021-08-27

*通信作者： 李伟 liwei12@fudan.edu.cn

基金项目：国家科技重大专项(2018ZX01027101-004)，基础加强计划基金(2019-JCJQ-JJ-123)

Foundation Items: The National Science and Technology Major Project (2018ZX01027101-004), The Foundation Strengthening Program (2019-JCJQ-JJ-123)

1 引言

在公钥密码体制中，由Koblitz和Miller提出的椭圆曲线密码(Elliptic Curve Cryptography, ECC)在安全性、处理速度、硬件实现代价等方面的优势，使其逐渐取代RSA密码算法成为下一代公钥密码标准，具有广泛的应用前景。同时，随着密码应用的不断发展，密码算法在各种硬件平台上具备不同的实现形式，密码算法运算时旁路信息电气特征往往会泄露密码运算中的秘密信息[1]，因此对于ECC芯片而言，除了传统密码分析安全性外，侧信道安全性同样至关重要。侧信道攻击一般分为时间攻击、能量攻击和电磁攻击等，其中能量攻击中的相关功耗分析(Correlation Power Analysis, CPA)通过中间数据与功耗之间的相关性差异来获取密钥信息，具有攻击成本小、成功率高的特点，是硬件电路安全防护的重点研究对象。

目前针对硬件电路的安全防护可分为电路级、行为级和系统级。电路级的防护策略包括安全倍速寄存器(Secure Double Rate Registers, SDRRs)[2]、感应调压器(Inductive Voltage Regulators, IVRs)[3]、低压降稳压器(Low-DropOut Regulator, LDO)[4]等，由于其涉及到元器件级或门级改进，对于ECC这类复杂电路来说难度高，同时其防护代价较大，如SDRR提供了功耗的随机化，但它的功耗和面积开销成倍增加，频率降低1倍。ECC电路的行为级防护策略发展较为成熟，在文献[5]中，Coron提出了椭圆曲线密码防御侧信道攻击的3个策略：随机化基点、随机化私钥、随机化射影坐标，此后大量研究人员在高速或小面积的ECC电路上进行了应用[6–8]，带来了额外的计算时间和较大的硬件资源开销，并会在电路中引入额外的随机源，成本较高。此外，可重构体系结构的调度也用于抗侧信道分析[9,10]，这些方法在芯片级的防护中有较好的效果，但其电路设计复杂、对灵活性要求高，存在吞吐量损失或较大的面积开销。而一般的功耗隐藏通过随机产生冗余功耗或平滑各时间点功耗进行，这样的策略存在着引入额外随机源或功耗代价过大的问题。

针对上述分析，本文通过深入研究ECC点乘的中间数据汉明距离的数据特点，提取出其概率分布特征；然后，将降低功耗中的密钥信息量问题转换成为减少猜测正确与错误密钥对应的中间数据汉明距离概率分布差异性问题，以概率分布函数差异为对象构建了等概率映射的功耗补偿模型，并通过模拟退火算法求得模型的最优矩阵解；最终，以该模型为指导，结合模运算基本电路结构，采用离线的方式进行配置矩阵计算，大大减少了硬件资源开销，完成了低成本的防护硬件电路设计。ECC运算复杂，不同ECC算法下的硬件设计方案不尽相同[6–8,11]，本文提出的功耗补偿策略依赖于统计提取的中间数据特征，可变化的模型参数与可替换的动态补偿电路设计支持不同硬件结构ECC电路。

本文结构安排如下：第2节对ECC运算及其泄露模型进行了分析；第3节基于中间数据的概率分布特征提出了等概率映射的功耗补偿模型与基于模拟退火的映射矩阵求解算法；在该模型的基础之上，第4节介绍了功耗补偿的硬件电路设计方案；第5节进行了实验验证及分析，第6节总结了全文工作。

2 ECC运算及泄露分析

2.1 ECC概述

椭圆曲线密码运算包含多个层次，分别为群运算层、曲线层和有限域层。群运算层主要包括点乘(Point Multiplication, PM)，是ECC中私钥参与计算的核心运算，通过其运算产生的功耗可以直接或间接推测出密钥信息；曲线层主要是点加(Point Add, PA)和倍点(Point Double, PD)运算，在不同坐标系下以不同的算法通过调用底层的模运算来实现；模运算(Modular Arithmetic, MA)位于有限域层，包括模加、模减、模乘、模逆等基本操作。

ECC点乘运算相对复杂，硬件电路实现中需要分级调用各层次的运算，计算过程中的各级数据变化如图1所示，点乘(PM)多次调用点加与倍点(PA&PD)运算，点加与倍点运算多次调用模运算(MA)，模运算需要多个时钟周期(Clock Period, CP)实现，在每一种运算的计算过程中，硬件电路中的寄存器数据在不断翻转变化。每一比特私钥$k_a, k_b, \cdots, k_z$在相应迭代轮的曲线层运算决定运算操作，因此在ECC硬件电路中存在中间数据与私钥的操作相关性与数据相关性。目前，存在着多种防护策略可较好地消除操作相关性，有效防止简单功耗分析，如Double-and-Always点乘算法、点加与倍点并行等，在此安全防护框架之下，本文针对数

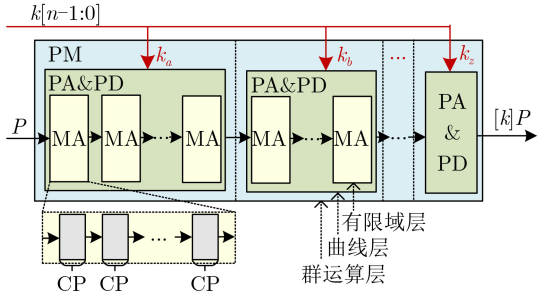


图 1 椭圆曲线密码各层次运算

据相关性进行研究。基点P作为输入，在每比特密钥的控制下进行不同的曲线层运算，最终得到点乘结果$[k]P$。每一次迭代输出的数据与密钥相关，这些与密钥相关的数据会在下一次迭代中进入曲线层、有限域层运算，在点乘运算每一个时钟周期的中间数据寄存器翻转都存在着不同程度的功耗泄露。

2.2 功耗泄露模型

依据汉明距离模型，功耗Power $\propto$ HW(state $\oplus$state$'$), state和state$'$为寄存器翻转的前后两个状态，则数据分析的对象应为模运算中的每个时钟周期寄存器的翻转情况，以及曲线层和群运算层的中间数据。对于模运算而言，首先，由于模加减运算相比于模乘除运算硬件电路规模小，电路中的功耗主要取决于模乘除；其次，模乘除运算的实现算法较多，主要包括基于加法器和基于乘法器的硬件实现方式，不同算法的中间数据特征不同；再者，有限域运算相对复杂，进行汉明距离与统计学计算的公式推导难度大。因此，采用统计方法，通过大量随机数据的计算，得到模乘、模逆计算数据的概率分布，对于不同参数、不同硬件结构的ECC电路，概率分布的特征不同。下面以基于加法器结构的模乘电路为例，进行数据的统计学特征分析，模乘算法如表1所示。

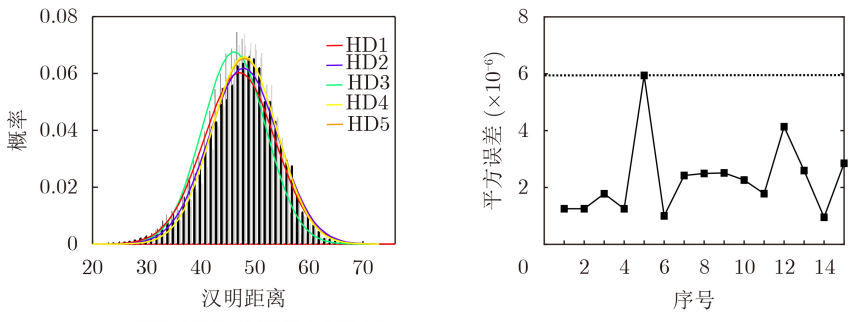
模乘电路主要由$2A \bmod P$，$4A \bmod P$，$V + b_0 \cdot U + b_1 \cdot A \bmod P$ 3个部分构成，m位的模乘由$\lceil m/2 \rceil$次迭代实现。取10000个随机变化的32 bit数据组A, B，对32位模乘运算的16轮迭代中间值汉明距离进行概率统计，图2(a)绘制出了任意5轮的离散概率分布，图中相同颜色的曲线代表由正态分布拟合的概率分布曲线，可以看出汉明距离基本满足正态分布的特性。取50个随机的模数P，重复上述统计，得到的16轮迭代中间值汉明距离的实际离散概率分布与近似正态分布的平均平方误差如图2(b)所示，误差小于6×10^{-6}，可由正态分布近似描述其统计学特性。

基于上述分析与统计样本，计算50组模数P下的16轮迭代中间值汉明距离的均值与标准差，前6轮迭代的均值与标准差如图3(a)所示，图中横坐标表示随机模数P的序号，曲线的颜色由深至浅表示迭代次数的增多，可以看出不同模数P下的汉明距离统计特征不同，但随着迭代次数的增多，均值与标准差均趋于一致。计算50组P下的1～15轮迭代的实际概率分布与后一轮迭代的平方误差的均值，如图3(b)所示，在第4次迭代后，相邻两轮迭代之间的误差小于10^{-6}。因此，通过4个概率分布即可较好地描述一个模运算内的所有中间数据概率分布特征。

对于不同硬件结构的ECC实现，其功耗泄露模型的差异性体现在模运算的实现方式。设计者依据自身设计中寄存器的翻转特征，通过统计的方式得到中间数据汉明距离的概率分布。一般来说，模乘算法可分为基于加法器实现和基于乘法器实现，前者即为上文所描述的情况，后者相比前者其迭代次数大大减少，可由全部迭代中间数据汉明距离的概率分布直接描述其统计特征。模除算法包括基于费马小定理或对求最大公约数算法的扩展。前者通过大量乘法运算迭代实现，硬件代价与运算时间长，一般不使用；后者通过加减法与移位实现，经统计分析，其中间数据统计特征与上文基于加法器的模乘算法相似，可通过同样的方式简化。

表 1　Radix-4交错模乘算法

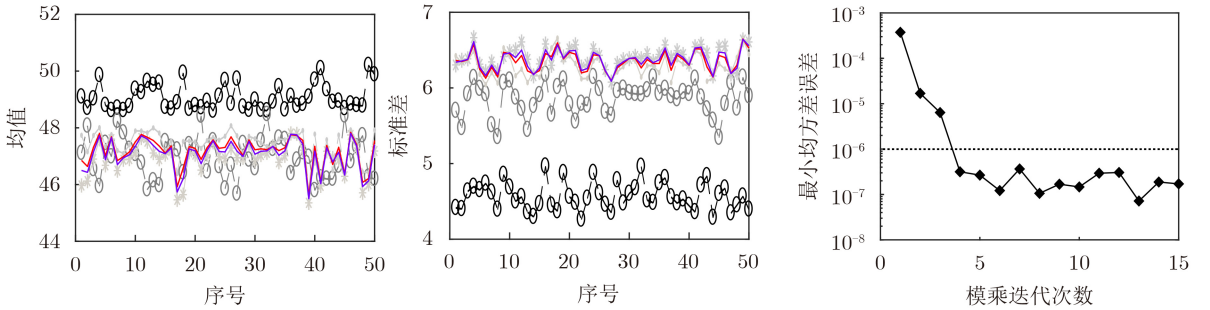
输入：A, B, P, 位宽m
输出：$V = A \cdot B \bmod P$
(1) $V = b_0 \cdot A$, $U = 2A \bmod P$, $A = 4A \bmod P$, $B = B/2$;
(2) For i from 0 to $\lceil m/2 \rceil - 1$
$V = (V + b_0 \cdot U + b_1 \cdot A) \bmod P$, $U = 2A \bmod P$,
$A = 4A \bmod P$, B=$B/4$;
(3) Return V



(a) 5组模运算单元汉明距离实际离散概率分布与其近似正态分布

(b) 16组近似正态分布的平均误差

图 2 正态分布对模运算的中间值汉明距离拟合程度



(a) 前6轮迭代中间数据汉明重量的均值与标准差

(b) 与前一次迭代汉明距离的平均误差

图 3 不同有限域P下的中间数据汉明距离的均值与标准

3 基于动态补偿的抗功耗攻击模型构建

3.1 等概率映射的功耗补偿模型

在一般的攻击与防护场景中，某一时刻的能量消耗由可利用的能量消耗I_{exp}、转换噪声$I_{\text{sw.noise}}$和电子噪声$I_{\text{el.noise}}$ 3个随机变量组成，三者相互独立[12]，如式(1)所示。对于攻击者而言，当密钥猜测错误时密钥仍未知，能量迹中包含与密钥相关的信息量，即$I_{\text{wrong}}=I_{\text{exp}}+I_{\text{sw.noise}}+I_{\text{el.noise}}$；当密钥猜测正确时密钥已知，能量迹中不再包含与密钥相关的信息量，即$I_{\text{right}}=I_{\text{sw.noise}}+I_{\text{el.noise}}$。从统计学的角度，密钥猜测正确与错误时的功耗概率分布存在差异性，主要体现在I_{exp}分量上，在上述2.2节中，ECC点乘在不同私钥下的中间数据汉明距离的概率分布很好地体现了这种差异性。功耗攻击与防护中，信噪比(Signal to Noise Ratio, SNR)用来描述功耗这一侧信道信息中包含的信息量，如式(2)所示。其中，$\text{Var}(X)$表示随机变量X的方差，I_{right}与I_{wrong}的方差差值ΔVar与SNR成正比，即可通过消除I_{right}与I_{wrong}的概率分布差异性降低信噪比，减少信息泄露

$$I_{\text{total}}=I_{\text{exp}}+I_{\text{sw.noise}}+I_{\text{el.noise}} \tag{1}$$

$$\begin{aligned}\text{SNR}&=\frac{\text{Var}(I_{\text{exp}})}{\text{Var}(I_{\text{sw.noise}}+I_{\text{el.noise}})}\\&=\frac{\text{Var}(I_{\text{exp}}+I_{\text{sw.noise}}+I_{\text{el.noise}})-\text{Var}(I_{\text{sw.noise}}+I_{\text{el.noise}})}{\text{Var}(I_{\text{sw.noise}}+I_{\text{el.noise}})}\\&=\frac{\text{Var}(I_{\text{wrong}})-\text{Var}(I_{\text{right}})}{\text{Var}(I_{\text{sw.noise}}+I_{\text{el.noise}})}\\&=\frac{\Delta\text{Var}}{\text{Var}(I_{\text{sw.noise}}+I_{\text{el.noise}})}\end{aligned} \tag{2}$$

基于功耗隐藏的思想，产生额外实时功耗来改变I_{right}与I_{wrong}的统计学特征[13,14]。基于汉明距离模型，将功耗抽象为中间数据的汉明距离(Hamming Distance, HD)，电路实际汉明距离与防护后的汉明距离之间满足某种一一对应关系，使得ΔVar尽可能小，将该对应关系描述为列向量形式$\boldsymbol{m}=(m_1,m_2,\cdots,m_n)^{\text{T}}$，其中$n$为汉明距离可能的取值个数，$m_i$表示当实际汉明距离为$i$时防护后的汉明距离为$m_i$，$m_i\in\{x\,|1\le x\le n,x\in Z\}$，未进行防护时$\boldsymbol{m}=(1,2,\cdots,n)^{\text{T}}$。用统计学中的平方差作为描述密钥猜测正确与错误的概率分布差异性的代价函数，则防护后的代价函数如式(3)所示。其中，f_{wrong}与f_{right}分别表示密钥猜测错误与正确时的离散概率分布函数，f_{wsubr}为二者的差值，即$f_{\text{wrong}}-f_{\text{right}}$，$\boldsymbol{f}(m)=(f(m_1),f(m_2),\cdots,f(m_n))^{\text{T}}$为一个列向量。由2.2节可知，模乘除运算的每一次迭代的中间数据可由num次迭代过程中的中间数据汉明距离的概率分布函数对代表模乘除数据的全部f_{wsubr}。点加与倍点运算一般通过调用8～30次模乘除实现，假设电路实现点加与倍点需要mmd个模乘除，则一共需要$\text{num}\cdot\text{mmd}$个$f_{\text{wsubr}}$来描述一次点乘迭代中所有时钟周期上的数据汉明距离统计差异性。

点乘迭代过程中，每一次迭代在相应的1 bit密钥的控制下进行，该轮迭代的中间数据与当前比特密钥以及在这之前参与计算的所有比特密钥相关。对于分组密码而言，攻击者通常不会采取比特攻击方式分析密钥，因为当攻击对象为某一位时，其他的所有密钥皆为转换噪声，此时的信噪比较低，攻击效果不理想；同时，攻击者也不会选择过多的位数进行攻击，因为采集的样本数随一次攻击的位数成指数上升，将导致样本量过大。但对于ECC而言，不存在比特攻击转换噪声大的问题，因为密钥逐比特参与运算，若逐比特攻击，在已知参与计算的所有比特的情况下攻击当前比特，能量迹对应的该轮迭代的功耗段将只于该比特密钥有关，其他密钥要么为已知，要么还未参与计算，不产生由密钥带来的转换噪声，且此时攻击者每次攻击1 bit密钥仅需猜测密钥为1或0两种情况，样本量大大降低。因此，针对ECC的攻击通常采用比特攻击的方式，在进行防护时对于任意一轮点乘迭代，在之前参与

计算的所有比特密钥已知的情况下，分析当前比特密钥。

假设防护针对比特攻击，用于描述计算过程中的概率分布差异性的f_{wsubr}函数个数为n，一般n=162～576，将导致代价函数累加项过多，使得统计的工作量以及代价函数寻优的复杂度增加。假设只对第1轮迭代进行防护，则使得攻击者在第1轮迭代对应的能量迹上对第1 bit密钥的攻击失败，此时攻击者可以通过对第2轮迭代对应的能量迹得到密钥的第1,2 bit，此时攻击者需要猜测4个密钥值；以此类推，若对前i轮迭代进行防护，攻击者可以通过对第(i+1)轮迭代对应的能量迹得到密钥的前(i+1) bit，此时攻击者需要猜测2^{i+1}个密钥值。当猜测密钥数量过大时，攻击者攻击的难度也将加大，从实践的角度来讲，当攻击成功所需的样本量过大时，可以认为攻击失败。设定当猜测密钥数大于100000时，攻击失败，则i≥16，即对前16轮迭代进行防护可以在实践上认为ECC点乘具备防护能力。与此同时，对前16轮的防护仅仅体现在代价函数的构建上，使得通过得到的矩阵映射能够有效减少前16轮数据的概率差异性，但是补偿电路产生额外功耗发生点乘的每一次迭代中，根据正态分布的特性，代价函数不包含这些迭代对应的$\|f_{\mathrm{wsubr}}(\boldsymbol{m})\|$项只是使得映射后的差异性减少程度变小，仍然具备防护能力，使得该策略为电路抗功耗攻击提供了第2层防护。因此，总体代价函数如式(4)所示，为$16\cdot\mathrm{num}\cdot\mathrm{mmd}$项$\|f_{\mathrm{wsubr}}(\boldsymbol{m})\|$的均值。

$$\mathrm{cost}=\|f_{\mathrm{wrong}}(\boldsymbol{m})-f_{\mathrm{rignt}}(\boldsymbol{m})\|=\|f_{\mathrm{wsubr}}(\boldsymbol{m})\| \tag{3}$$

$$\mathrm{cost}_{\mathrm{SUM}}(\boldsymbol{m})=\frac{1}{16\cdot\mathrm{num}\cdot\mathrm{mmd}}\cdot\sum_{j=1}^{16\cdot\mathrm{num}\cdot\mathrm{mmd}}\left\|f_{\mathrm{wsubr}(j)}(\boldsymbol{m})\right\| \tag{4}$$

此时，汉明距离的补偿关系为一一对应的，而点乘中间数据的概率分布差异性较小，该补偿方式的精度较低，为使得代价函数达到阈值，根据正态分布的特性可知最优解容易达到全补偿，即$\boldsymbol{m}=(n,\cdots,n)^{\mathrm{T}}$，导致补偿的功耗代价过大。因此，将模型改进为概率映射，电路实际汉明距离按照一定概率映射为2^h个值，将该映射关系描述为矩阵形式如式(5)，改进后的代价函数如式(6)所示，其中参数的含义如表2所示

$$\boldsymbol{M}=\begin{pmatrix} m_{11} & m_{12} & \cdots & m_{12^h} \\ m_{21} & m_{22} & \cdots & m_{22^h} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{n2^h} \end{pmatrix}_{n\times 2^h} \tag{5}$$

$$\mathrm{cost}_{\mathrm{SUM}}(\boldsymbol{M})=\frac{1}{16\cdot\mathrm{num}\cdot\mathrm{mmd}}\cdot\sum_{j=1}^{16\cdot\mathrm{num}\cdot\mathrm{mmd}}\left(\frac{1}{2^h}\sum_{i=1}^{2^h}\left\|f_{\mathrm{wsubr}(j)}(\boldsymbol{M}_i)\right\|\right) \tag{6}$$

寻找$\boldsymbol{M}$矩阵使得$\mathrm{cost}_{\mathrm{SUM}}(\boldsymbol{M})$足够小，对于同一参数下的椭圆曲线，对应的$f_{\mathrm{wsubr}}$函数相同，在ECC计算不更换参数的情况之下，可使用同一$\boldsymbol{M}$矩阵进行映射，以达到防护的效果。因此寻找$\boldsymbol{M}$矩阵的过程可以通过离线的方式进行，这样可以减少防护带来的额外面积开销。在更换参数时，防护者统计样本得到f_{wsubr}函数组，并通过离线计算的方式得到$\boldsymbol{M}$矩阵，将矩阵配置到硬件电路中产生相应的补偿功耗。

3.2　基于模拟退火的映射矩阵求解

求解最优转换矩阵属于离散最优化问题中的整数非线性规划问题，属于NP问题，目前没有普适的算法[15]，引入元启发式算法中的模拟退火算法来寻找全局最优解。模拟退火是一种基于概率的算法，在寻找最优解的过程之中引入随机数，但使用该算法求解最优$\boldsymbol{M}$矩阵是离线进行的，避免了电路开销与随机源的引入，算法如表3所示。

算法产生新的$\boldsymbol{M}$矩阵后，对比原$\boldsymbol{M}$矩阵与代价函数值。若代价函数变小，则说明新的$\boldsymbol{M}$矩阵使得正确与错误密钥下的概率分布差异减小，算法

表 2　参数列表

参数	含义
num	模乘除运算中间数据的概率分布函数之差的个数
$f_{\mathrm{wsubr}(j)}$	第j个密钥猜测错误与正确时的离散概率分布函数之差
mmd	ECC硬件实现时，在能量迹上显示出的模乘和模除数量之和
n	ECC硬件实现中，中间数据汉明距离的所有可能汉明距离的个数
h	衡量等概率映射时的概率参数，汉明距离以概率2^{-h}被映射为2^h个值
$\boldsymbol{M}$	为一个n行2^h的概率矩阵，矩阵中的第x行元素$(m_{x,1},m_{x,2},\cdots,m_{x,2^h})$表示将实际汉明距离$x$分别以相等的概率$2^{-h}$映射为$m_{x,1},m_{x,2},\cdots,m_{x,2^h}$
$\boldsymbol{M}_i$	矩阵的第i列向量

表 3 寻找最优$\boldsymbol{M}$矩阵的模拟退火算法

输入：代价函数cost_{SUM}，降温系数α，代价函数阈值threshold，矩阵维度n, h；
输出：映射矩阵$\boldsymbol{M}'$。

(1) 初始化$\boldsymbol{M}$矩阵元素$m_{i,j}=i$，温度Tmp；
(2) 计算代价函数$\text{cost}_{\text{old}}=\text{cost}_{\text{SUM}}(\boldsymbol{M})$；
(3) 生成随机向量$\boldsymbol{r}=(r_1,r_2,\cdots,r_n)_n$，其中$r_i=(i-1)+(n-i+1)\cdot\text{rand}_i$, rand_i为0～1之间的随机数；将矩阵的一列向量更新为$\boldsymbol{M}_i=\lceil\boldsymbol{r}\rceil=(\lceil r\rceil_1,\lceil r_2\rceil,\cdots,\lceil r_n\rceil)^{\text{T}}$；
(4) 重复步骤 3，直到矩阵的h个列向量全部被替换，生成新的$\boldsymbol{M}_{\text{new}}$；
(5) 计算新的代价函数cost_{new}，以及$\delta=\text{cost}_{\text{new}}-\text{cost}_{\text{old}}$；
(6) 生成一个0～1的随机数R，若$\delta<0$，则$\boldsymbol{M}=\boldsymbol{M}_{\text{new}}$, $\text{cost}_{\text{old}}=\text{cost}_{\text{new}}$；
否则，若$\exp(-\delta/\text{Tmp})>R$，则$\boldsymbol{M}=\boldsymbol{M}_{\text{new}}$, $\text{cost}_{\text{old}}=\text{cost}_{\text{new}}$，并进行降温，令$\text{Tmp}=\text{Tmp}\cdot\alpha$；
(7) 若$\text{cost}_{\text{old}}>$ threshold，则返回步骤 3；
(8) 令$\boldsymbol{M}$中的元素$m_{i,j}=m_{i,j}-i$，生成$\boldsymbol{M}'$矩阵并返回。

使原$\boldsymbol{M}$矩阵更新；代价函数变大，说明新的$\boldsymbol{M}$矩阵概率分布差异增大，此时按照Metropolis准则，以概率$\exp(-\delta/\text{Tmp})$更新$\boldsymbol{M}$矩阵。最终，当代价函数小于阈值时，结束迭代得到最优的$\boldsymbol{M}$矩阵。由于矩阵中各元素的含义为补偿后新的汉明距离，而电路需要产生的功耗值与补偿后增加的汉明距离值直接相关，因此为适合硬件设计，在最后一个步骤将$\boldsymbol{M}$矩阵的每一个值减去其初始值，得到表征增加汉明距离关系的映射矩阵$\boldsymbol{M}'$。

在步骤(3)中，采用扰动的方式产生新的$\boldsymbol{M}$矩阵，由于采用补偿的方式进行防护时，电路中的功耗只可以增大不能够减少，因此对于矩阵中的元素$m_{i,j}$，其取值范围为i～n的整数，对于最后一行元素其值不可变，固定为n。在每一次产生新的矩阵时，随机产生$n\cdot h$个0～1的小数rand，使得$m_{i,j}=\lceil(i-1)+(n-i+1)\cdot\text{rand}\rceil$，等概率取$i$～$n$的整数。

3.3 等概率划分参数h的代价分析

上述基于概率的补偿映射模型在应用时代价函数中的参数h对防护的效果与代价影响显著，h越大使得每一个汉明距离对应的概率值被等分得越细，汉明距离映射的精度越大，在寻找最优$\boldsymbol{M}$矩阵的过程中达到近似全补偿的可能性越小；同时h的增大导致实际汉明距离到补偿汉明距离的映射次数增多、防护电路的硬件电路面积增大，也使得模拟退火算法的解空间增多，算法收敛时间增大。因此，需要针对具体的应用场景合理选择。

对于位宽为128 bit的ECC点乘，n=384，统计点乘计算的前16轮中间数据，得到相应代价函数，设定初始温度为3000。由正态分布的特点，随机变量大于$(\mu-z_{0.0001}\cdot\sigma)$的概率小于0.01%，相应的对于电路中间数据而言，其汉明距离大于354的概率极小，为避免不必要的功耗代价，可使得算法2中的$\boldsymbol{M}$矩阵元素的最大值不超过354(大于354的元素在算法迭代过程中不变)，将减少解空间大小，降低收敛时间。对参数h=1～5进行多次计算，其平均收敛时间与补偿后的汉明距离如图4所示。随增大收敛时间增加、补偿后的HD减少，但当h大于2后补偿后的HD减少不到1%，收敛时间却以指数形式增长。因此，在该应用场景下选择h为2。

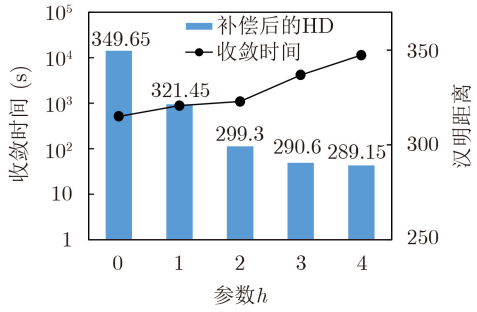


图 4 不同参数h下，针对ECC128的模拟退火算法收敛时间与补偿后的平均汉明距离

4 ECC的动态补偿电路设计

4.1 定量汉明距离输入转换电路

依据上述动态补偿模型，需要由汉明距离映射关系产生相应的实时冗余功耗，ECC电路功耗主要来源于模运算电路。冗余功耗产生电路工作时，在每个时钟周期内，依据电路当前汉明距离以及计算得到的最优$\boldsymbol{M}$矩阵产生定量的冗余功耗，通过输入来进行定量功耗产生的控制。ECC中的基本运算为模运算，由于其运算复杂，为减少电路规模，一般可通过寄存与复用在多周期实现，尤其对于模乘、模除运算。因此，电路在一个时钟周期内的功耗特征取决于设计者采用的算法将模运算分解为一个时钟周期内的何种基本运算。除此之外，对于可支持两种有限域的ECC电路，在二元域的计算由异或门实现，而在素数域一般为较复杂的加法器和乘法器，电路规模远大于前者，决定了功耗的主要特征。

补偿功耗产生电路为设计者在实现模运算使用

的基本运算op，一般为加法、乘法等。该运算在一个时钟周期内完成，为主要功耗产生来源，输入与汉明距离的关系如式(7)，其中HW(X)表示X的汉明重量，input1为基本运算op的可变输入，input2为不变输入，如模数P或$f(x)$等。式(7)中对input1所有可能取值情况的集合到HD所有可能取值的集合可能既非单射或非满射，当由HD求解input1时可能不存在反函数，因此需要对op运算进行分析，进而得到汉明距离与输入的表达式。由于篇幅有限，以op为加法为例进行分析说明，其余情况不再赘述

$$\mathrm{HD}=\mathrm{HW}(\mathrm{input1}\oplus\mathrm{op}(\mathrm{input1},\mathrm{input2})) \tag{7}$$

在模运算中，加法器用于计算数据加/减模数，其input1为A, input2为P，加法器第i位计算进位与结果表达式为$c_i=a_i\cdot p_i+c_{i-1}(a_i\oplus p_i)$，$s_i=a_i\oplus p_i\oplus c_{i-1}$，其中$a_i,p_i,c_i,s_i$依次为输入$A$，$P$，进位$C$和结果$S$的第$i$位。电路寄存器汉明距离则为输入与输出的异或值，对于第i位异或值$x_i=s_i\oplus a_i=p_i\oplus c_{i-1}$。由进位表达式可知，当$p_i$=0时，$c_i$=a$_i\cdot c_{i-1}$；当$p_i$= 1时，$c_i$=a$_i$+$c_{i-1}$，真值表如表4所示。其中当$p_i,c_i,c_{i-1}$分别为000和111对应的$a_i$的值任意，此时，无论$a_i$值为何，$c_i$的结果一定。为简化运算，令a$_i$=0。此外，该真值表不包含$p_i,c_i,c_{i-1}$为010和101两种情况，将这两种取值表示为表达式形式如式(8)。当x_i= 0且$x_{i+1}\oplus p_{i+1}\oplus p_i$=1时，state=1，即满足上述条件时，在当前$P$取值的情况下，$x_i$不可为0。$x_i$是输入与输出的异或值，为防护时设定的补偿汉明距离的1个比特，需要额外补偿e个汉明距离时，置x_i= $1, i\le e$，置x_i= $0, i>e$。因此为避免上述state为1，当$x_i=0$时，使得$p_i=0$，又由于x_i= 0时，x_{i+1}也一定为0，即P=$P\cdot X$。基于上述分析对真值表输出a_i修改为a_i'，得到a_i的表达式如式(9)。由补偿汉明距离值到加法器输出A的转换电路(Switching Circuit, SC)如图5所示，由于$c_0=0$, P为素数则$p_1=1$，则$x_1=c_0\oplus p_1=1$,$a_1=c_1$。

$$\begin{aligned}\mathrm{state}=&c_i\cdot\bar{c}_{i-1}\cdot\bar{p}_i+\bar{c}_i\cdot c_{i-1}\cdot p_i\\=&c_i\cdot(x_i\cdot p_i+\bar{x}_i\cdot\bar{p}_i)\cdot\bar{p}_i+\bar{c}_i\cdot(x_i\cdot\bar{p}_i+\bar{x}_i\cdot p_i)\cdot p_i\\=&\bar{x}_i\cdot(c_i\oplus p_i)\\=&\bar{x}_i\cdot(x_{i+1}\oplus p_{i+1}\oplus p_i)\end{aligned} \tag{8}$$

$$\begin{aligned}\mathrm{a}_i&=c_i\cdot c_{i-1}\cdot\bar{p}_i+c_i\cdot\bar{c}_{i-1}\cdot p_i=c_i\cdot(p_i\oplus c_{i-1})\\&=c_i\cdot x_i\end{aligned} \tag{9}$$

表 4　由c_i输出值推导出的a_i真值表

p_i	c_i	c_{i-1}	a_i	a_i'
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	1	1	1	1
0	1	0	–	X
1	0	0	0	0
1	1	0	1	1
1	1	1	0	0
0	1	1	1	0
1	0	1	–	X

4.2　低成本补偿电路设计

补偿电路依据算法得到的$\boldsymbol{M'}$矩阵，将主电路中的每一个时钟周期模运算结果存储寄存器数据汉明距离映射新的汉明距离，并产生相应的补偿功耗，电路结构如图6(a)所示，图中相应的位宽以128位ECC为例。计算参与模运算的寄存器输入与输出的汉明距离，当电路中的参数更换时，进行离线计算得到最优的$\boldsymbol{M'}$矩阵，将其配置在存储电路中。电路工作时，以主电路的相关寄存器的汉明距离作为数选信号，由数选器完成映射，得到2^h个列向量对应的需要增加的汉明距离。依据功耗补偿模型，电路以相等的概率选择这2^h个值产生补偿功耗，在电路增加一个h位的计数器，该计数器在每个时钟周期上升沿进行加1操作，即等概率地产生0～(2^h–1)的数据，以计数器的输出为数选信号得到每个时钟周期相应的汉明距离。

假设设计者在实现模运算使用的基本运算op对应的电路为OP电路，一般为加法器、乘法器等。OP电路与SC电路共同组成了冗余功耗产生电路。将该汉明距离扩展为相应的异或结果作为SC电路的输入，即汉明距离为e时，SC电路的输入为x，x的低e位为1，其余位为0。SC电路的输出与模数P进入OP电路产生补偿功耗。实验数据表明，相同汉明距离下，基于表1中算法加法器结构的模运算单元功耗是一个加法器OP电路的功耗2.34倍，因

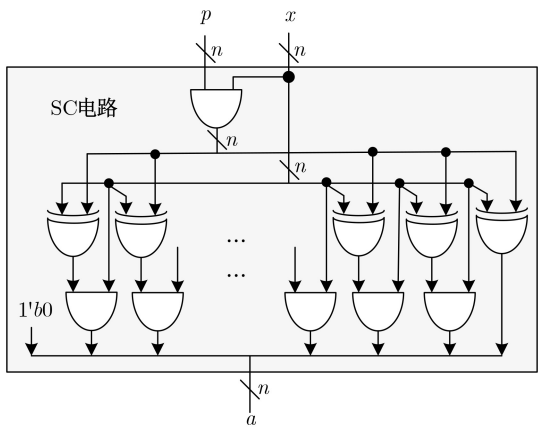
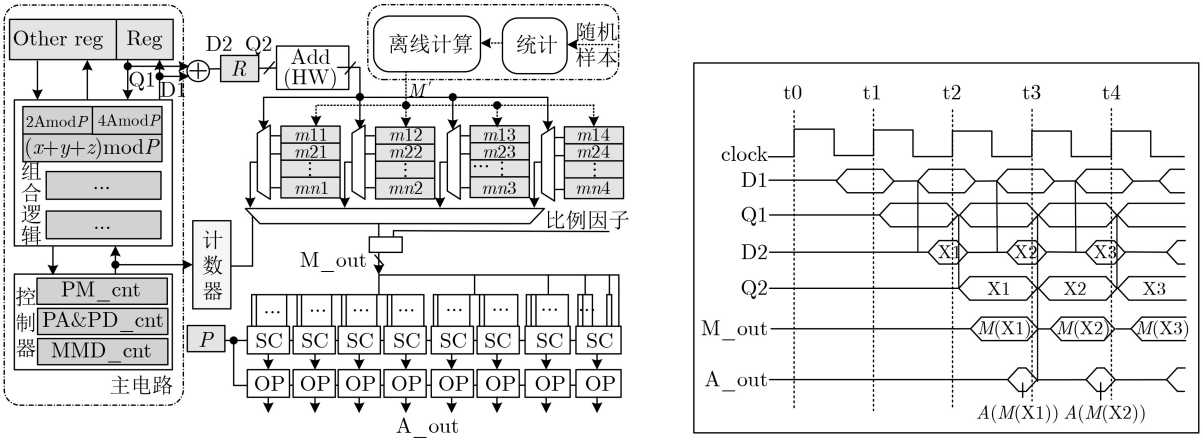


图 5 转换电路结构图



(a) 补偿电路结构图 (b) 补偿功耗时的相关中间数据时序图

图 6 补偿电路的硬件实现与时序逻辑

此在汉明距离扩展之前应将汉明距离乘以相应的比例因子。对于补偿矩阵$\boldsymbol{M}$的行数为n的ECC电路，其位宽为$n/3$，由于比例因子的存在，其补偿的最高汉明距离为$7.02\times(n/3)$，因此该ECC电路防护时的OP电路由8组$n/3$ bit加法器构成。

与此同时，补偿电路应保证产生冗余功耗与主电路寄存器的翻转在一个时钟周期内同时发生，为满足时序特性，在主电路参与模运算的寄存器输入与输出异或电路之后插入一级寄存器R。插入寄存器后的时序如图6(b)所示，D1, Q1为主电路参与模运算的寄存器输入与输出，D2, Q2为插入寄存器的输入与输出，M_out为$\boldsymbol{M'}$矩阵映射后的输入，A_out为加法器输入。可以看出，Q1的翻转和加法器的计算同时发生在t2到t3时刻之间，满足时序要求。补偿电路仅在主电路的关键路径上增加了一级异或门的延时，与关键路径相比其增加的延时较小，可忽略不计，对主电路的ECC计算速度保持不变，电路性能不受影响。

5 实验验证及分析

在CMOS 40nm工艺下进行逻辑综合，防护前后的电路面积分别为0.281 mm^{2}和0.345 mm^2，面积增加22.8%，关键路径延时保持3.21 ns不变。补偿电路不影响关键路径与点乘的计算，对ECC的计算性能不产生任何影响。

实验以Sakura-G开发板为平台，电路在其主FPGA(Xilinx Spartan-6)实现，如图7所示。分别

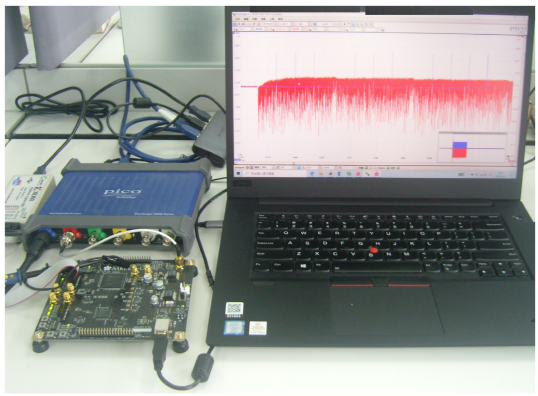


图 7 基于Sakura-G开发板的安全测试平台

以主电路和带防护ECC电路为对象进行CPA分析，其中主电路实现128位ECC点乘。带防护的ECC电路使用4285个FF，19687个LUT单元，功耗为0.12W，与主ECC电路相比，增加了19.9%FF，24.2%LUT单元以及18.8%功耗，如表5所示。

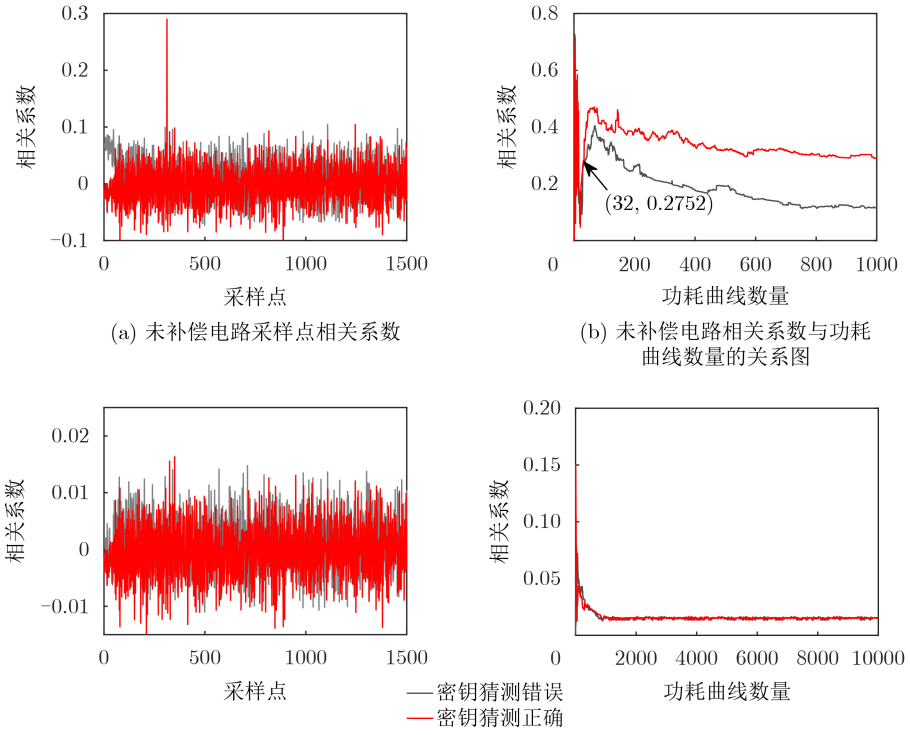
安全防护测试在PC端进行明文与密钥的输入以及点乘输出的验证，使用PicoScope 3403D示波器进行功耗波形采集，示波器探头与开发板电源之间连接1 Ω电阻，以该电阻上的压降等效为开发板功耗。对密钥的第2位进行CPA攻击，通过输入1000个基点采集功耗曲线，每个功耗曲线包含1500个采样点。未防护时，采样功耗曲线为1000条的情况之下，正确密钥在相应的采样点处的相关系数远大于其他点，而猜测错误密钥未出现这样的相关系数极大点，如图8(a)所示。此时，最小泄露轨迹数

表 5 防护前后代价与性能对比

	综合面积(mm^2/kGates)	关键路径延时(ns)	FPGA LUTs/FFs	FPGA 功耗(W)
防护前	0.281/293.4	3.21	15851/3574	0.101
防护后	0.345/360.3	3.21	19687/4285	0.120
增加的百分比	+22.8%	0	+24.2%/+19.9%	+18.8%

(Minimum Trace of Data, MTD)为32，如图8(b)所示。防护后，相同采样曲线条数的情况之下，相关系数曲线未见明显较大值点，如图8(c)所示。进一步增大采样曲线条数，观察相关系数，从图8(d)可以看出，防护后的MTD大于10^4，与防护前相比，抗CPA攻击能力提升大于312倍。

目前，ECC电路的防护主要依赖于随机化方法，表6展示了该策略分别与其他防护方法的对比结果，其中括号内为防护后的数据，与ECC电路的硬件实现方式有关，因此将防护后的数据占未防护时的百分比作为对比对象将更加准确。文献[6]中的基点随机化点乘算法需要存储额外的点坐标，并在每次计算前进行随机基点的点乘，导致其运算时间增加为原来的1倍左右，而文本提出的功耗补偿策略不对电路频率与ECC电路的迭代时间产生任何影响，虽然其防护能力提升了333倍，略优于本策略的防护效果，但其在性能上不具有优势。文献[7]和文献[16]分别使用中间点随机化技术和标量点乘随机化方法，前者在点乘算法的每次迭代中增加了一次点加计算；后者使得k的位宽变大，增加了迭代次数，安全防护使得二者的点乘时间增加约50%；此外，本文与之相比增加了22.8%的面积，但是在防护效果上，本文要明显优于二者。文献[17]使得射影坐标随机化，增加了额外的计算量，与未使用该方法相比计算时间增加了62%；且在功耗代价上，该文的防护方法使得功耗增加50%，而本文仅增加18.8%。总的来说，与随机化的防护方法相比，本文提出的防护策略虽然产生了一定的面积代价，但对电路的运算性能不产生任何影响，且具有良好的防护能力与更小的功耗代价。



(a) 未补偿电路采样点相关系数　(b) 未补偿电路相关系数与功耗曲线数量的关系图

(c) 补偿后电路采样点相关系数　(d) 补偿后电路相关系数与功耗曲线数量的关系图

图 8 CPA攻击相关系数与最小泄露轨迹数

表 6　防护能力与电路代价对比分析

	VLSI'14 [6]	TIE'16[7]	TDSC'18[16]	TCAS-I'21[17]	本文
原理	基点随机化	中间点随机化	标量k随机化	射影坐标随机化	功耗补偿
域-位宽(bit)	素域-160	素域-163	素域-128	素域-256	素域-128
运算性能代价	+100.6%	+53.8%	+50%	+62%	+0
(点乘时间@频率/ms@MHz)	(0.34@194)	(0.6@316)	(82.5@8)	(0.089@222)	(0.37@312)
面积代价(面积/kGates)	+0(98)	+0(189)	+0(--)	+0(194.7)	+22.8%(360.3)
功耗代价(功率/mW)	--(34.4)	--(34.3)	--(--)	+50%(73.5)	+18.8%(120.0)
最小泄露轨迹数MTD	$> 10^5$	$> 2 \times 10^4$	$> 5 \times 10^3$	--	$> 10^4$
防护能力提升倍数	> 333	> 250	>119	--	> 312

6 结束语

本文针对ECC硬件电路中由数据相关性带来的侧信息泄露问题，提出了一种基于模拟退火算法的功耗隐藏策略，通过建立映射模型动态补偿功耗。依据该模型设计的防护电路在一定面积与功耗代价下具备与目前普遍使用的随机化方法相当的安全防护能力，且不会带来电路运算性能的损失。该模型理论上可支持不同硬件结构的ECC电路，但防护电路不尽相同，更加普适的防护电路设计是未来研究的重点。

参 考 文 献

[1] 陈华, 习伟, 范丽敏, 等. 密码产品的侧信道分析与评估[J]. 电子与信息学报, 2020, 42(8): 1836–1845. doi: 10.11999/JEIT190853.
CHEN Hua, XI Wei, FAN Limin, *et al*. Side channel analysis and evaluation on cryptographic products[J]. *Journal of Electronics & Information Technology*, 2020, 42(8): 1836–1845. doi: 10.11999/JEIT190853.

[2] BELLIZIA D, BONGIOVANNI S, MONSURRÒ P, *et al*. Secure double rate registers as an RTL countermeasure against power analysis attacks[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2018, 26(7): 1368–1376. doi: 10.1109/TVLSI.2018.2816914.

[3] KAR M, SINGH A, MATHEW S, *et al*. 8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator[C]. 2017 IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, USA, 2017: 142–143.

[4] SINGH A, KAR M, MATHEW S, *et al*. 25.3 A 128b AES engine with higher resistance to power and electromagnetic side-channel attacks enabled by a security-aware integrated all-digital low-dropout regulator[C]. 2019 IEEE International Solid- State Circuits Conference - (ISSCC), San Francisco, USA, 2019: 404–406.

[5] CORON J S. Resistance against differential power analysis for elliptic curve cryptosystems[C]. The First International Workshop, CHES'99, Worcester, USA, 1999: 292–302.

[6] LEE J W, CHUNG S C, CHANG H C, *et al*. Efficient power-analysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2014, 22(1): 49–61. doi: 10.1109/TVLSI.2013.2237930.

[7] LIU Zilong, LIU Dongsheng, and ZOU Xuecheng. An efficient and flexible hardware implementation of the dual-field elliptic curve cryptographic processor[J]. *IEEE Transactions on Industrial Electronics*, 2017, 64(3): 2353–2362. doi: 10.1109/TIE.2016.2625241.

[8] YEH L Y, CHEN P J, PAI Chenchun, *et al*. An energy-efficient dual-field elliptic curve cryptography processor for internet of things applications[J]. *IEEE Transactions on Circuits and Systems II*: *Express Briefs*, 2020, 67(9): 1614–1618. doi: 10.1109/TCSII.2020.3012448.

[9] GOGNIAT G, WOLF T, BURLESON W, *et al*. Reconfigurable hardware for high-security/high-performance embedded systems: The SAFES perspective[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2008, 16(2): 144–155. doi: 10.1109/TVLSI.2007.912030.

[10] YANG Jianwei, HAN Jun, DAI Fan, *et al*. A power analysis attack resistant multicore platform with effective randomization techniques[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2020, 28(6): 1423–1434. doi: 10.1109/TVLSI.2020.2971636.

[11] 戴紫彬, 易肃汶, 李伟, 等. 椭圆曲线密码处理器的高效并行处理架构研究与设计[J]. 电子与信息学报, 2017, 39(10): 2487–2494.
DAI Zibin, YI Suwen, LI Wei, *et al*. Research and design of efficient parallel processing architecture for elliptic curve cryptographic processor[J]. *Journal of Electronics & Information Technology*, 2017, 39(10): 2487–2494.

[12] MANGARD S, OSWALD E, POPP T, 冯登国, 周永彬, 刘继业, 等译. 能量分析攻击[M]. 北京: 科学出版社, 2010: 56–63.
MANGARD S, OSWALD E, POPP T, FENG Dengguo, ZHOU Yongbin, LIU Jiye, *et al*. translation. Power Analysis Attacks: Revealing the Secrets of Smart Cards[M]. Beijing: Science Press, 2010: 56–63.

[13] SHAN Weiwei, ZHANG Shuai, XU Jiaming, *et al*. Machine learning assisted side-channel-attack countermeasure and its application on a 28-nm AES circuit[J]. *IEEE Journal of Solid-State Circuits*, 2020, 55(3): 794–804. doi: 10.1109/JSSC.2019.2953855.

[14] SHAN Weiwei, ZHANG Shuai, and HE Yukun. Machine learning based side-channel-attack countermeasure with hamming-distance redistribution and its application on advanced encryption standard[J]. *Electronics Letters*, 2017, 53(14): 926–928. doi: 10.1049/el.2017.1460.

[15] 刘振宏, 马绍汉. 离散最优化算法[M]. 北京: 科学出版社, 2012: 36–38.
LIU Zhenhong and MA Shaohan. Discrete Optimization Algorithms[M]. Beijing: Science Press, 2012: 36–38.

[16] LIU Zhe, LONGA P, PEREIRA G C C F, *et al*. on embedded devices with strong countermeasures against side-channel attacks[J]. *IEEE Transactions on Dependable and Secure Computing*, 2020, 17(3): 536–549.

[17] CHOI P, LEE M K, and KIM D K. ECC coprocessor over a NIST prime field using fast partial Montgomery reduction[J]. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, 2021, 68(3): 1206–1216. doi: 10.1109/TCSI.2020.3039753.

李 伟：男，1983年生，副教授，博士生导师，研究方向为密码处理器设计，ASIC专用芯片设计.

曾 涵：女，1998年生，硕士生，研究方向为安全SoC与专用指令处理器设计.

陈 韬：男，1979年生，副教授，硕士生导师，研究方向为安全专用芯片设计.

南龙梅：女，1981年生，博士生，研究方向为大规模集成电路设计、专用集成电路设计.

责任编辑：余 蓉