密码学报
Journal of Cryptologic Research
ISSN 2095-7025,CN 10-1195/TN

《密码学报》网络首发论文

题目：旁路功耗分析中不同平台的差异化研究
作者：郭筝
收稿日期：2020-06-03
网络首发日期：2020-09-08
引用格式：郭筝．旁路功耗分析中不同平台的差异化研究．密码学报．
https://kns.cnki.net/kcms/detail/10.1195.TN.20200904.1725.019.html

旁路功耗分析中不同平台的差异化研究

郭 筝

智巡密码（上海）检测技术有限公司，上海，201601
通讯作者：郭筝 E-mail：guozheng@zxcsec.com

摘 要：旁路功耗分析已成为密码芯片渗透性测试的重要手段。为了在电路设计阶段验证防护措施的有效性，通常设计者会利用功耗仿真工具或 FPGA 来测量电路功耗，并进而进行旁路分析。在对一些通过安全认证的密码芯片进行试验后，发现用仿真功耗方法对这些芯片的原始电路代码进行分析，仍旧可以发现一些旁路泄露信息。甚至是对于一些采用掩码的防护措施，也可以通过一阶分析的方法攻击成功。并且不同实现方式下，不同功耗数据形式下，分析存在一定差异。本文通过理论和实验结合，以分组密码算法 DES 为例，深入分析了仿真功耗和实际功耗的差异，揭示已有防护措施仍旧存在旁路信息泄露的原因。本文的实验结果证实了功耗仿真和 FPGA 平台的有效性，改进建议有助于低价带防护方案的实现。

关键词：旁路功耗分析；密码芯片；仿真功耗；掩码防护

中图法分类号：TP309.7　　**文献标识码:** A

Research on the difference of different platform in side-channel power analysis

GUO Zheng

Zhixun Crypto Testing and Evaluation Technology Co, Ltd.，Shanghai，201601，P. R. China
Corresponding author: GUO Zheng, E-mail:guozheng@zxcsec.com

Abstract: Side channel power analysis has become an important method for penetration testing of cryptographic chips. In order to verify the effectiveness of the countermeasures during the periods of circuit design, it's common for designers to use simulation or FPGA to measure the power consumption of the circuit. On the basis, they perform side channel analysis. However, the paper performs simulation on the circuit which passed the security certification and find that there still exist some leakages. Even within the masking protection, attacks can be successfully performed through first-order analysis. Analysis depends on implementations and the form of power consumption. Through the combination of theory and experiment, this paper chooses the block cipher algorithm DES to deeply analyze the difference between simulation and physical, revealing what causes the side channel leakages under the theory security. The experimental results in this paper confirm the effectiveness of simulation and FPGA platform, and give the improvement against the leakages.

Key words: Power Analysis; Cryptographic Chip; Simulation Power; Masking

1 引言

旁路功耗分析是当前对密码芯片威胁最大的攻击方式之一，其原理是利用 CMOS 电路在翻转时产生的功耗和数据相关的特征，通过猜测算法的中间结果来恢复密钥。目前已有大量的分析方法被提出，其中应用最为广泛的就是差分功耗分析（DPA）和由其衍生的相关性功耗分析（CPA）。一些实验也证实，如果不添加防护措施，几乎所有的密码电路都易受此类攻击的影响。

为了抵御旁路功耗分析，一种常用的有效方法是掩码，其原理是使得算法运算过程中的中间结果随机化。事实上，在过去几年中，很多可选择的、针对 DES 等分组密码的掩码方案被提出。这些方法主要是考虑算法中非线性部分的掩码，该部分掩码通常需要花费较大的电路代价；相比之下，线性部分容易进行掩码的添加。目前的安全芯片设计中，几乎都会实现线性部分的掩码，非线性部分则是根据电路代价选择性添加。

基金项目：国家自然科学基金项目（U1636217）；上海市科委科研计划项目（19511103900）
收稿时间： 2020-06-03　　定稿时间：2020-06-24

已有些研究提出了针对掩码的安全性分析，其中大多数研究者认为，即使加了掩码，但由于电路延迟产生的毛刺，仍旧使得电路运行过程中有真正的中间值泄露[1,2]，从而会使得分析成功。[3]中基于 SPICE 仿真证明了毛刺导致旁路信息泄露的现象。[4]中讨论了毛刺对于掩码电路的影响。[5]中则利用功耗仿真的方法对电路中组合逻辑部分进行了建模，并发现利用一阶分析方法亦可以侦测到掩码电路中的泄露信息，作者攻击了掩码后非线性逻辑的输出，某些比特的信息泄露较大，这说明电路实现方式会影响最终的攻击效果和结果。[6]中使用作者自己提出的仿真器对多款 AVR 微控制器进行了仿真攻击。另有一些分析人员致力于研究抗毛刺的掩码方案[7-9],这些研究通常紧密依附于上述对于电路仿真的研究。

同样是研究掩码的信息泄露，本文的立足角度不同。基于对一款通过安全认证的 DES 实际芯片和相应电路代码的功耗分析比较，指出两者之间在各类分析模型下的分析结果差异，并利用功耗仿真曲线可层次化计算模块消耗功耗的特点，对泄露进行定位和解释。

值得一提的是，本文的实验过程将结合功耗仿真和 FPGA 验证的方法进行。其中仿真功耗由于无噪声的缘故，所以可能泄露更多的信息，以至于一些研究者认为其与真实情况相差过大，不太具备参考价值。然而在本文看来，功耗仿真是在代码设计阶段发现旁路信息泄露的重要手段，有理由相信，如果电路代码的防护措施在仿真功耗分析下有效，则该防护对于实际芯片也同样有效。

本文余下的章节安排如下。第一部分将阐述分析对象的防护措施结构。第二部分将展示利用功耗仿真分析的结果。第三部分将展示通过 FPGA 实现的分析结果。第四部分是对泄露的分析。第五部分是一些防护建议。最后是总结，并将针对仿真功耗、FPGA 等不同实现的分析方法，给出一些未来可研究的方向。

2 DES 密码电路的防护结构

本文选择了一款已通过（国内）EAL 4+安全认证的密码芯片作为分析对象，该密码芯片中包含 DES 密码算法，采用了两种防护措施。第一种防护措施是仅对于线性部分的掩码方案，图 1 说明了 DES 线性掩码的运算结构。

在该防护方法中，线性部分都添加了掩码，且掩码共同参与计算，非线性部分的 S 盒则利用原值进行计算。每轮运算的掩码不同，在寄存器存取操作时，去掉旧掩码时先掩上新的掩码，且为了避免寄存器输入端的毛刺现象，轮运算寄存器置于新旧掩码操作之间。在算法计算过程中，轮运算寄存器始终保持两轮的掩码。

通常在攻击硬件实现的密码算法时，首先会考虑对轮寄存器的数据存储过程进行攻击，对于 DES 算法，可攻击第一轮计算结果覆盖明文的过程，采用的功耗模型是汉明距离模型，根据[10]，有时候汉明重量模型也会有效。根据上述描述的防护机制，算法计算过程中的真值仅出现在非线性运算部分，因此，该防护应该有效抵御针对轮寄存器的功耗分析。

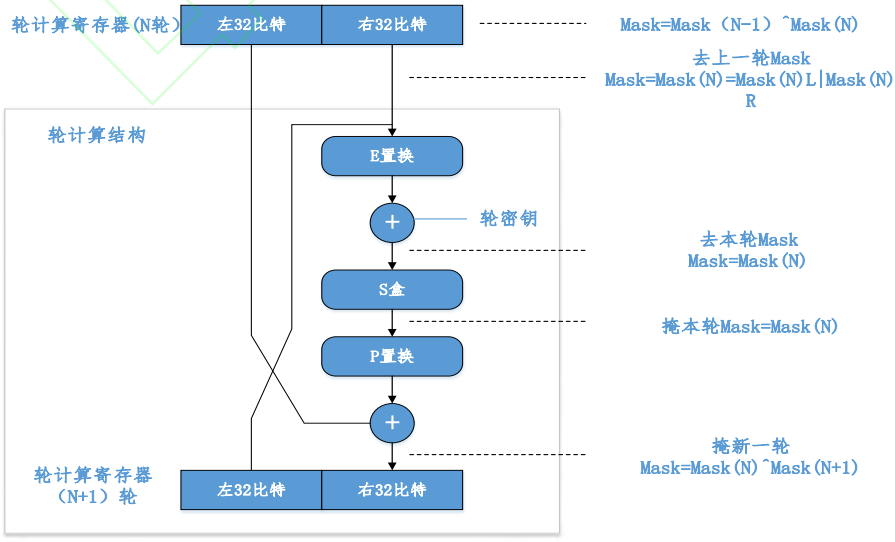

图 1　DES 线性掩码的运算结构

第二种防护是全掩码，在线性部分掩码基础上加上掩码的 S 盒，即对非线性部分也进行掩码。从理论上分析，后一种防护使得算法在计算过程中，不会出现真实的中间结果，因此应该能有效抵御任何对于线性逻辑和非线性逻辑的差分功耗分析。

事实上，如果线性部分的防护措施添加恰当，则能够基本抵御差分功耗分析。原因是非线性逻辑主要由组合逻辑组成，其翻转速度较快，虽然存在毛刺现象，但利用现有精度的示波器去发现此类毛刺并加以利用，其分析代价也会十分巨大。但在仿真实验中，由于模拟采样精度可以很高，所以会发现由于毛刺产生的泄露。在后续的实验中，会对上述两类防护分别进行分析。

3 基于功耗仿真的分析结果

3.1 实验过程

本文利用 EDA 工具对 DES 的 verilog 代码进行综合、布局布线。完成版图后，对网表进行带反标时序参数的仿真。利用功耗仿真工具 PTPX，可以得到不同明文输入下电路的功耗曲线，由此形成分析样本，在本实验中准备了 4000 条功耗曲线作为分析样本。同时，为了作对比实验，本文利用 FPGA（Sasebo GII）对同样的电路代码进行综合仿真，利用外部线性反馈移位寄存器每周期生成随机掩码。通过示波器进行功耗曲线采集，由此形成与电路代码对应的分析样本，在本实验中利用 FPGA 采集了 30 万条功耗曲线作为样本。

对于 DES 算法的攻击，通常利用非线性逻辑 S 盒操作，在无防护情况下，单个 S 盒可恢复 4 比特密钥数据。本文主要采取表 1 所示的攻击位置和攻击模型，采用的攻击方法主要是相关性功耗分析。

表 1 攻击位置和攻击模型

攻击选择	攻击位置	攻击模型
第一种	轮寄存器	汉明距离
第二种	轮寄存器	汉明重量
第三种	S 盒输出	汉明距离
第四种	S 盒输出	汉明重量

针对线性部分掩码防护，由于仅在 S 盒输出位置出现了真值，理论上可抵御第一种、第二种和第三种攻击，而在第四种攻击下有泄露。针对全掩码的防护方法，理论上可抵御所有攻击。

3.2针对线性部分掩码防护的分析

根据上述分析，线性部分的掩码将有效抵御针对轮寄存器的功耗分析，即无法攻击寄存器的存取操作，实际芯片的攻击也显示该防护方法有效。对于电路代码，采取了表 1 中攻击选择对其进行分析，下图显示了对单个 S 盒输出的攻击结果。

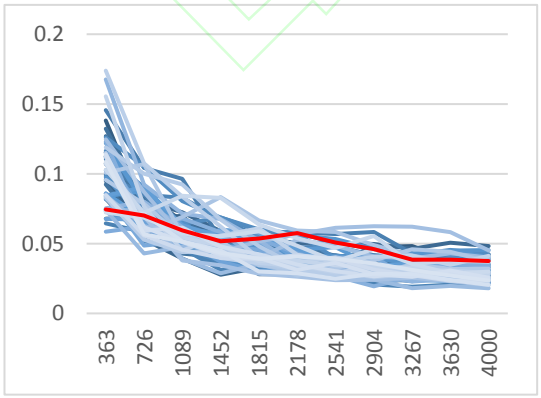

图 2.1 第一种攻击结果

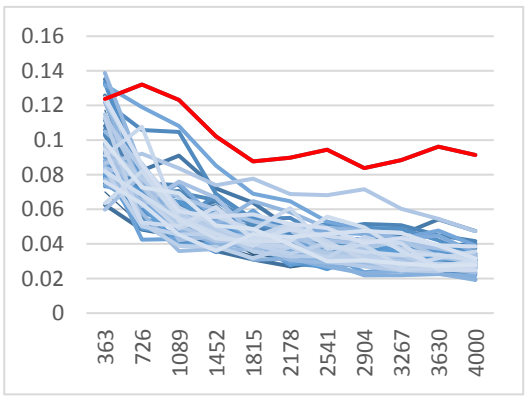

图 2.2 第二种攻击结果

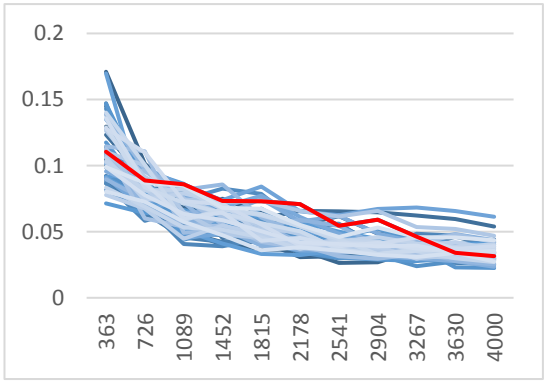

图 2.3 第三种攻击结果

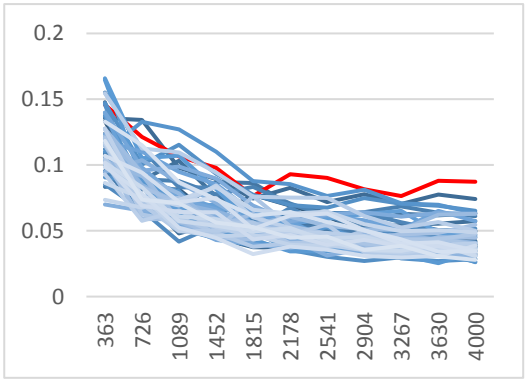

图 2.4 第四种攻击结果

上图中横坐标为曲线数量，纵坐标为相关性系数，红色实线显示的是正确密钥下对应的相关性系数。根据结果显示，除了 S 盒输出的汉明重量有泄漏之外，攻击轮寄存器的汉明重量也存在信息泄露。这说明在算法执行过程中，有真值泄露，根据分析结果所对应的功耗模型可初步判断与第一轮输出结果相关的计算部分产生了泄露，由于非线性部分未采取掩码措施，因此泄露可能出现在 S 盒的输出。

3.3 针对非线性部分掩码防护的分析

根据第二章的分析，同时使用非线性和线性部分的掩码，在整个算法过程中将不出现真值，因此无法通过旁路功耗分析攻击寄存器存取和 S 盒计算部分，即抵御所有的攻击方式。实验结果也表明无信息泄露。

4 基于 FPGA 的分析结果

同样的，对 FPGA 采集的功耗曲线也做了相应的分析，结果如下所示。

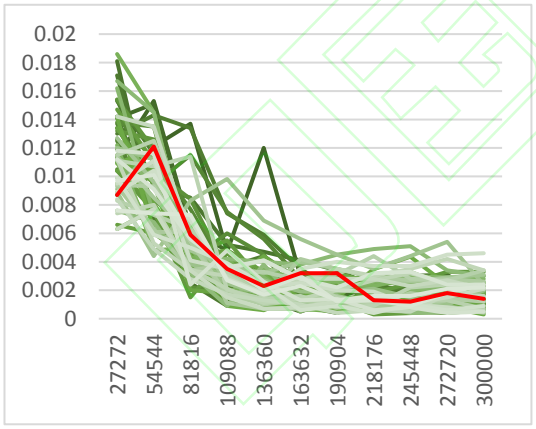

图 3.1 第一种攻击结果

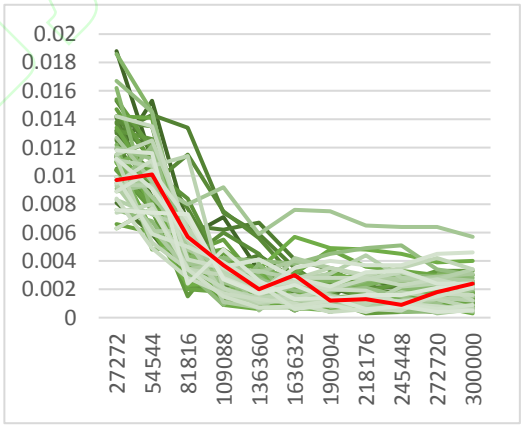

图 3.2 第二种攻击结果

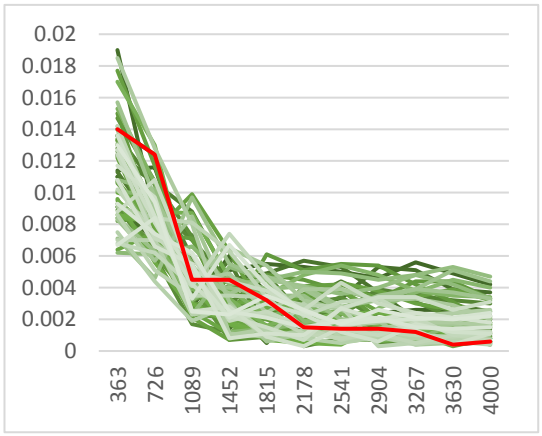

图 3.3 第三种攻击结果

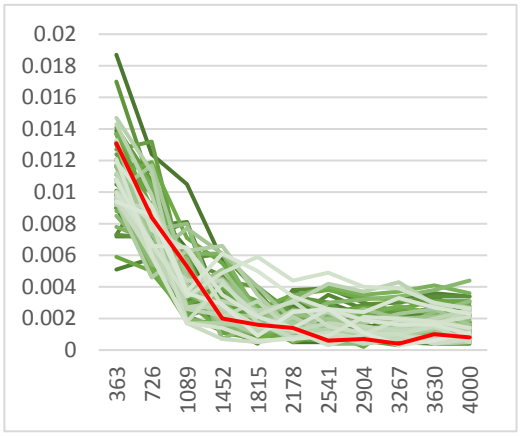

图 3.4 第四种攻击结果

综上试验结果，结合实际芯片通过测评的结果，表 2 列出了不同平台下，两种防护的实验结果。

表 2 不同平台下两种防护的实验结果

防护种类	仿真下防护效果	FPGA 下的防护效果	实际芯片
线性部分掩码	抵御第一种和第三种攻击，在第二种和第四种攻击下有泄漏	在四种攻击下未见明显泄露	在四种攻击下未见明显泄露
全掩码	抵御所有攻击	抵御所有攻击	抵御所有攻击

从上表中可以看出，不同实验平台下，不同的防护措施表现出不同的防护能力。同时，仿真平台下，第二种攻击出现了泄露，这与理论分析结果有所不同。在下章中尝试理论解释这些现象，同时本文也认为电路实现的差别对分析结果有影响。

5 泄露信息分析

泄露主要出现在线性部分的掩码防护中，功耗仿真工具 PTPX 可提取层次化模块的功耗，因此在编写电路代码时将算法中的 F 函数、E 置换和 S 盒等运算组件单独写成模块，便于对其功耗进行单独提取和分析。采用与发现旁路信息泄露同样的功耗模型，分别对 F 函数、E 置换和 S 盒进行了分析。结果发现几乎所有的泄露都出现在 S 盒模块中。

5.1 S盒本身输出的汉明重量的泄露

该泄露对应第四种攻击的结果。由于 S 盒输出是真值，虽然很快与掩码进行异或，但由于数据延迟的影响，会导致总线上出现数据真值。通过观察仿真曲线，发现 S 盒和输入信号和输出信号变化时存在大量毛刺。根据实验结果，可以确定泄露位置都在 S 盒计算的后半部分。此时 S 盒的真实结果陆续计算出来，并在数据线上进行输出。

由于仿真精度较高，可达到皮秒级别，所以几乎可以发现每个 S 盒的真值泄露。在实验中该泄露出现的位置是在明文输入之后，即 S 盒已计算出实际结果，但还未更新寄存器。在 FPGA 和实际芯片中，由于采样精度受到限制，并且有外部器件产生的噪声，所以只能认为有可能发生泄露，但实际测量很困难。

5.2 轮计算结果的汉明重量的泄露

该泄露对应第二种攻击的结果。同样地，对各个运算组件分别进行了功耗分析，发现在轮计算之后有信息泄露。由于该处的数值与真值和随机掩码数据相关，于是直接计算了随机掩码后的轮运算数据和实际结果的相关性。仿真功耗实验中的随机掩码数据来自于软件随机函数生成，实验结果显示相关性较大，说明随机数样本的随机性较弱。FPGA 实验中的随机掩码数据来自于线性移位寄存器，实验结果显示相关性较小，说明该随机数样本的随机性符合防护要求。

6 防护措施的改进

虽然实际芯片和 FPGA 未发现明显泄露，但仿真功耗的实验说明了泄露隐患的存在。对于这些隐患，本文提出以下改进建议。

6.1 线性操作部分需注意电路实现方式

电路实现对于功耗信息的泄露有较大影响。根据图 1 的防护措施，对于非线性部分的掩码在进入 S 盒之前需要退去掩码。因此会出现带掩码的数据、子密钥和去掩码数据几乎同时进行异或操作的时候。

正常的异或顺序是带掩码的数据和子密钥先异或，其结果再和掩码数据异或。但由于电路延迟的缘故，可能三个数据到来的时间会有差异。如果子密钥在最后到达，就会造成 S 的输入和任何掩码无关，也就是说线性部分的掩码作用在轮计算结果到 S 盒之前完全消失。

下图显示了当三个值几乎同时异或时，利用第一种攻击方法的分析结果。分别用仿真和 FPGA 进行了实验。

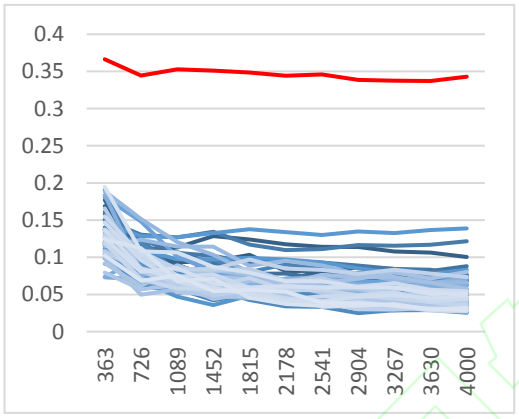

图 4.1 仿真曲线下的第一种结果

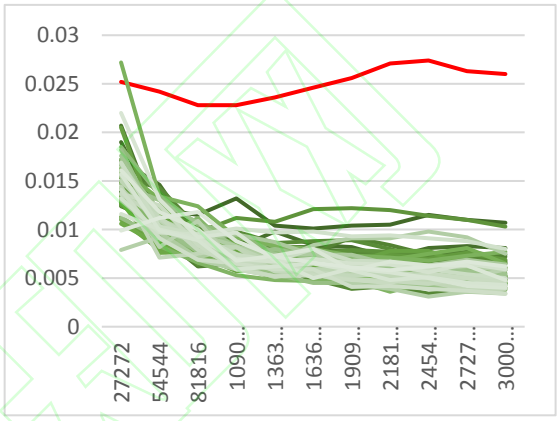

图 4.2 FPGA 下的第一种攻击结果

可以通过适当加入延迟单元，使得两个异或操作分开，则上述的攻击模型对曲线无效，同时可有效应对第四种攻击。这样一来，该防护方案的实现方式可抵御所有的一阶攻击。由于该方案在每次运算采用了不同的掩码，因此也可有效抵御高阶攻击。

6.2 非线性操作部分采用隐藏的防护方法

根据上述分析，掩码中的泄露主要来自于非线性逻辑。非线性逻辑的掩码需要较高的电路面积代价，因此可以考虑采用隐藏和掩码结合的方式，以时间代价换取面积的减少。目前旁路攻击的模型主要是针对非线性逻辑的，可以通过功耗仿真的方法定位泄露细节，采取相应的防护措施，从而消除非线性逻辑的安全隐患。

7 总结与展望

本文对一类已通过安全认证的密码芯片的电路代码进行了仿真和 FPGA 实验，以期验证芯片在设计阶段抵御旁路功耗分析的能力，并尝试说明不同实现方式下，功耗曲线和分析结果的差异。通过一些对比实验，可做出以下总结：

（1）对于已加入掩码防护的电路可能存在旁路信息泄露隐患，利用仿真功耗精度高的特点可有效发现 。

（2）不同阶段、不同形式的功耗数据，在同样的分析方法下表现出一定的差异。功耗仿真和 FPGA 的分析对于实际电路都有参考价值。在同样的泄露分析模型，一般而言如果仿真功耗未发现泄露，则实际电路也能抵御相应攻击。

（3）电路实现对于分析结果有较大影响。处理好线性部分的掩码，可有效实现低代价的防护方案。

当然有些问题还未彻底解决。譬如虽然发现仿真曲线和实际曲线在分析方面的差异，但造成这些差异

的原因无法准确解释。本文猜测信息的泄露来自于电路毛刺，在仿真功耗中，无噪声且精度较高，因此信噪比很高。而在实际电路中，受采样频率的影响，可能无法精确采集到此类毛刺，且由于噪声的叠加，使得信噪比较低。此外，不同结构分组密码算法的防护实现方式也值得进一步研究。

旁路功耗分析技术在不断发展，该技术体现了微电子、计算机和密码等领域的融合。对于分析方法实施的研究，可揭示新的可能存在的安全隐患，有助于降低防护方案的成本。

References

[1] Mangard S, Pramstaller N, Oswald E. Successfully attacking masked AES hardware implementations[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2005: 157-171.

[2] Bozzato C, Focardi R, Palmarini F. Shaping the Glitch: Optimizing Voltage Fault Injection Attacks[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019: 199-224.

[3] Stefan Mangard, Thomas Popp, and Berndt M. Gammel. Side-Channel Leakage of Masked CMOS Gates. In Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings, volume 3376 of Lecture Notes in Computer Science, pages 351–365. Springer, 2005.

[4] Daisuke Suzuki, Minoru Saeki, and Tetsuya Ichikawa. Random Switching Logic: A Countermeasure against DPA based on Transition Probability. Cryptology ePrint Archive (http://eprint.iacr.org/), Report 2004/346, 2004.

[5] Mangard S, Pramstaller N, Oswald E. "Successfully attacking masked AES hardware implementations", CHES 2005, Springer Berlin Heidelberg, Germany, pp. 157-171, 2005.

[6] Veshchikov N, Guilley S. Use of simulators for side-channel analysis[C]//2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2017: 104-112.

[7] Roche T, Prouff E. Higher-order glitch free implementation of the aes using secure multi-party computation protocols[J]. Journal of Cryptographic Engineering, 2012, 2(2): 111-127.

[8] Moradi A, Mischke O. Glitch-free implementation of masking in modern FPGAs[C]//2012 IEEE International Symposium on Hardware-Oriented Security and Trust. IEEE, 2012: 89-95.

[9] Moos T, Moradi A, Schneider T, et al. Glitch-Resistant Masking Revisited[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019: 256-292.

[10] M.Stefan, E.Oswald, T.Popp, "Power analysis attacks: Revealing the secrets of smart cards." Vol. 31, Spring. 2007.

作者信息

郭筝（1980–），上海人，博士。

主要研究领域为侧信道攻击、芯片安全攻防技术、密码产品和系统测评技术。

E-mail：guozheng@zxcsec.com