上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

学士学位论文

THESIS OF BACHELOR

论文题目：序列密码算法电路的新型物理攻防技术研究

学生姓名：于泽汉

学生学号：5142119010

专　　业：微电子科学与工程

指导教师：郭筝

学院(系)：电子信息与电气工程学院

上海交通大学
学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：_____

日　期：_____年 _____月 _____日

上海交通大学
学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权上海交通大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

本学位论文属于

保　密 □，在 _____ 年解密后适用本授权书。

不保密 □。

（请在以上方框内打 ✓）

学位论文作者签名：_____　　指导教师签名：_____

日　期：_____年 _____月 _____日　　日　期：_____年 _____月 _____日

序列密码算法电路的新型物理攻防技术研究

摘　要

密码设备的安全性一直备受研究人员关注，其中侧信道攻击技术扮演了十分重要的角色，而功耗分析攻击又是诸多侧信道攻击方法中极为强大的一种。因此，研究功耗分析技术，不但可以加深我们对密码设备安全性的理解，更能揭示出理论安全的密码算法在实际实现时可能会出现的众多问题，从而指导我们在生产实践中采取必要的防护措施。

在传统的旁路攻击中，分组密码是主要的研究对象，这方面的研究成果也较多。由于序列密码（也称为流密码）算法中的加密变换随时间变化，因此，相比分组密码，找到序列密码中密钥和设备功耗之间的对应关系相对困难，所以针对序列密码算法的功耗分析研究相对较少。

本文以祖冲之算法作为序列密码算法的典型，力图将传统的分组密码功耗分析方法应用于序列密码算法，并借此表明序列密码算法同样无法抵御功耗分析攻击，并试图提出一些可行的防护方案以提升祖冲之算法的安全性。

关键词：旁路攻击　差分功耗分析　祖冲之算法

A STUDY ON NEW PHYSICAL ATTACKS AND DEFENCES OF CIRCUITS RUNNING STREAM CIPHER ALGORITHM

ABSTRACT

Researchers have paid a lot of attentions to the security of cryptographic devices. Side-channel attacks have greate influences on it. Power analysis is one of the most powerful methods in side-channel attacks. Therefore, the studies on power analysis can not only deepen our understanding of the security of cryptographic devices, but can also reveal a number of potential problems when theoretically secure algorithms are used in real-world applications, which will provide much guidance on the defence of the security of cryptographic devices.

In traditional side-channel attacks, block cipher algorithms are the main objects of study and researchers have a lot of achievements on them. Compared to block cipher algorithms, it is harder for stream cipher algorithms to find the relations between the power of devices and the cipher key of the algorithm for because of the time-variant transformations during encryptions. This leads to less studies on the power analysis of stream cipher algorithms.

This paper studies the technologies used in traditional power analysis of block cipher algorithms, and applies them to stream cipher algorithms. We take the ZUC algorithm as a typical case. The results indicate that stream cipher algorithms are also vulnerable to power analysis attacks and we try to provide some practical protection methods to improve the security of the ZUC algorithm.

KEY WORDS: side-channel attack, differential power analysis, ZUC algorithm

目 录

第一章　现代密码学与旁路攻击

经过多年的学术研究和工业应用，密码学理论已经日趋系统和完善，各种密码算法广泛应用于各种工业设备，以保障系统和数据的安全。

目前，那些得到广泛使用的密码算法，通常都经过数学上的严格论证，并且经过了大量专家的研究和改进，因而在理论上基本是安全的。然而在现实生活中，这些算法都运行在具体的设备上，因此可能会暴露出各种各样的安全问题，研究者和攻击者可以藉由各种手段，获取密码设备中的秘密信息。

在诸多攻击密码算法和密码设备的手段中，旁路攻击是极为优秀和实用的一类。“旁路”的含义是利用实际密码设备泄露的信息，而不是利用密码算法本身的漏洞。根据时间、成本以及仪器的不同，旁路攻击又可以划分为很多种类，实际的方法也五花八门。在实际应用中，旁路攻击的效果远优于传统的密码学理论分析，因此得到了攻击者和研究人员的青睐。

1.1　现代密码学

由于目前应用在实际生活中的绝大多数密码学理论都属于现代密码学，因此我们讨论的重点也集中在现代密码学。

现代密码学和古典密码学的一个重要区别是：现代密码学构建在严格的数学论证和完备的系统架构之上。目前普遍使用的算法也都是现代密码算法，并且经过许多分析、攻击和改进，才渐渐保证其理论上的安全性。

信息安全是现代密码学的一个重要应用领域。衡量信息安全的指标包括：保密性、完整性、认证性、不可否认性以及可用性。要达成这些严格的指标，就需要同样严格的现代密码学体系支撑。这些安全指标有些是彼此掣肘的，因此在设计一个密码系统时，需要综合各方面的因素，才能达到预期的目的，保证系统的安全性。

现代密码学遵循一些基本的准则，比如柯克霍夫原则（Kerckhoffs’s principle）。该原则指出，系统的安全性不应依赖于具体实现的保密性。信息论的创始人香农（Shannon）也说：“敌人了解系统。”这些原则来源于历史上的经验和教训：几乎所有尝试隐藏算法和系统实现方式本身的做法，最后都失败了。

这些原则促进了通用算法的公开和评审，现实表明，公开的算法经过层层筛选和多次改进，具备更加优良的理论安全性和实际可用性。因此，当前应用广泛的许多密码算法都是公开透明的。我们在进行密码学分析和旁路攻击时，不需要在获取算法细节方面花费不必要的工夫（不过，相应地，这也意味着这些算法本身已经具有极高的安全性，想要分析和攻击它们是一件非常困难的事情）。

划分现代密码学有很多依据，其中一个就是密钥的特征，分为对称密码学和非对称密码学。对称密码学应用的一个典型是 AES 算法（Advanced Encryption Standard，高级加密标准），其特点是加密和解密使用相同的密钥。非对称密码学应用的代表是 RSA 算法（Rivest–Shamir–Adleman），其特点是加密和解密使用不同的密钥。

相比非对称密码学，旁路攻击在对称密码学方面的研究相对多一些。一方面可能是因为对称密码算法加解密采用同一密钥，破解密钥更有意义；另一方面是由于非对称密码算法常常要进行大数运算，速度比对称密码算法要慢很多，因而在对性能要求较高的工业密码设备中，非对称密码算法应用较少，也就造成了实际样本较少，并且研究动力不足。本文涉及的祖冲之算法，也是对称密码算法中的一种。

1.2 密码设备

数学家和密码学家们常常关注理论层面，试图从根本上提高密码算法的安全性，而工程师则更多地和现实打交道，将这些纸上的东西转化成真正能够工作的软硬件设备。也正是由于这种分工，熟悉密码学理论的数学家和密码学家们难以注意到现实设备在实现时可能存在的安全隐患，而整天从事软硬件设备开发和维护的工程师，也鲜有人能够通晓算法背后的原理，从而留下一些潜在的可以利用的漏洞和瑕疵。

上一小节我们简单提及了密码学的理论部分，因此这一小节我们将讲述一些和实际密码设备相关的知识。了解密码设备的软硬件构成，有助于我们掌握实际设备的特性，以及可能出现的信息泄露点，为我们的旁路攻击打下必要的基础。

密码算法的执行通常涉及到两部分，一部分是数据的保存，另一部分是数据的操作。相应地，密码设备也可以分为两种，一种是保存数据的存储设备，另一种是操作数据的处理设备。

密码设备一般拥有这几个部分：

- 专用硬件：比如执行特定密码算法的电路
- 通用硬件：比如控制算法流程的控制电路
- 存储硬件：用于存储数据和程序
- 接口：用于规定数据的输入和输出

密码设备通常由数字电路实现，不同部分既可以在同一块芯片上完成，也可以分到多个芯片上。我们这里以单芯片的密码设备为例。通常，单芯片数字电路可以通过两种方式实现，一种是 FPGA（Field Programmable Gate Array，现场可编程门阵列），另一种是 ASIC（Application-Specific Integrated Circuit，专用集成电路）。虽然用不同方式实现的密码设备在运行性能、工作场景以及成本上有所不同，但实现流程却基本相同。

不管是 FPGA 还是 ASIC，其本质都是数字电路。数字电路的基本组成部分是各种逻辑元件。通常有两种逻辑元件，一种是组合元件，实现基本的逻辑功能，比如与、或、非，另一种是时序元件，比如触发器、锁存器以及寄存器。时序元件和组合元件最大的不同是，时序元件的输出不仅取决于当前的输入，还和元件当前的状态有关。

目前，在实现逻辑元件的工艺中，以 CMOS（Complementary Metal Oxide Semiconductor，互补金属氧化物半导体）最为常见。

1.3 旁路攻击

传统的密码学分析试图挖掘算法本身存在的问题，抑或是寻找某些数学前提和密码学假设的漏洞，从而在根本上攻破某一密码学算法或系统。一旦从理论上揭露了某种密码学算法或系统的潜在

问题，那么暴露出来的问题就是致命的，使用这些算法或系统的设备要么被废弃，要么经受升级和改进，否则就不能消除安全隐患。

然而，正如上文提到的，由于现代密码学主张密码算法设计的公开化和透明化，因此，大多数现在广泛使用的密码算法和系统都经过了严格的论证、长期的研究和持续的改进。一方面，对于使用这些算法和系统的设备来说，安全性得到了极大的提升；另一方面，对于相关领域的研究人员和攻击者来说，使用传统方法破解算法或者是提取算法中的重要信息，变得日益困难。

虽然现代密码学的严格化和公开化的初衷正在于更好地保障信息安全，但是这对攻击者和研究人员无疑也是巨大的挑战：攻击者需要开发更强大的武器和工具，花费更多的时间和成本，才能达成目的；而研究人员也需要付出更多的精力和汗水，学习更多的数学知识，和更多的符号和数字打交道，才能做出点像样的成果，发几篇可能有用的论文。

而旁路分析的出现，则提供了另一种截然不同的思路，并且打开了一扇通往新世界的大门。旁路分析的思路和方法五花八门，各有千秋，狭义上的旁路攻击通常指被动型非侵入式攻击，也就是说，这类攻击只是对密码设备的各种攻击方法的一小部分。但是广义上的旁路攻击则包含各种非传统意义上的密码分析手段。

以攻击密码设备时使用的接口作为分类依据，一般将攻击的方式划分为三种：侵入式攻击，半侵入式攻击非和侵入式攻击。

下面对这三类攻击作一些简单的介绍和说明：

- 侵入式攻击（Invasive Attacks）：能够进行侵入式攻击的人通常能够对密码设备拥有较长时间的物理接触权限，因而可以对设备进行非常仔细的拆卸和分解，能够获得设备详尽的信息和状况。不过，要完成侵入式攻击，付出的代价也相对高，比如需要探测台和激光切片器这样昂贵的仪器和技术。
- 半侵入式攻击（Semi-Invasive Attacks）：半侵入式攻击一般也要对密码设备进行一定程度的拆卸和分解，但是通常不会破坏芯片的钝化膜，不直接接触芯片的表面。半侵入式攻击相比侵入式攻击，在仪器上花费的成本要低一些，但如何选择正确的部位以从设备中读取泄露的信息依旧要耗费大量的时间。比如常见的故障攻击，就属于半侵入式攻击的范畴。
- 非侵入式攻击（Non-Invasive Attacks）：相比上面两种攻击，非侵入式攻击成本是最低的，并且在攻击完成后，不会有明显的痕迹。狭义上的旁路攻击，就属于非侵入式攻击，只利用设备合法的接口以及泄露的侧信道信息，就能通过数学手段提取出设备中的敏感内容。正因为非侵入式攻击所需的设备以及花费的代价很低，因此比前两种攻击应用更加广泛，威胁也更大。

从具体的实施手段上讲，常见的旁路攻击有这些方式：

- 时序攻击（Timing Attack）：设备中的程序在运行时，不同的指令和操作耗时并不是相等的。如果这些指令和操作中包含秘密参数，那么执行时间上的差异就有可能将这些信息泄露出去。如果对设备或算法的具体实现非常了解，甚至可以结合统计学的方法将秘密参数完全恢复出来。
- 功耗分析攻击（Power Analysis Attack）：功耗分析攻击通常应用于硬件设备。在执行不同的指令或者处理不同的数据时，设备散发的功耗也是存在差异的。功耗分析通常也分为简单功耗

分析和差分功耗分析。在各种各样的旁路攻击方式中，功耗分析攻击是研究最为成熟的，其方法最为系统，对应的方案也最多，是当前旁路攻击研究领域中的热门方向。

- 电磁攻击（Electro Magnetic Attack）：除了功耗之外，设备在运行时还会发出电磁辐射。同样地，设备的指令和数据也会影响电磁辐射的特征。和功耗分析攻击类似，电磁攻击也分为简单电磁攻击和差分电磁攻击。军方很久之前就已经注意到了这种攻击，比如美国国家安全局。虽然功耗分析攻击和电磁攻击使用的方法和思路非常类似，但电磁攻击有时候比功耗分析更加强大，采用了功耗分析防护方案的设备有时候也不能抵挡电磁攻击。
- 可见光攻击（Visible Light Attack）：攻击者们还注意到了设备的光学信息。比如有研究表明，阴极射线显像管（CRT）产生的光在投射到墙壁上，并且经过漫反射后，依旧可能泄露设备的相关信息。相同的技术也可以应用到发光二极管（LED）上。可见光攻击的一大优点就是不需要物理接触设备，这是大部分其他攻击方式都不具备的。
- 声学攻击（Acoustic Attack）：处理器在执行操作时也会泄露声学信息，通过分析声学信息的差异，也有可能获取相关的秘密信息。但这一领域尚处在早期阶段，还没有呈现出成熟的技术。
- 故障攻击（Fault Attack）：大部分算法和程序都假定设备能够正常工作，很多防护方案也是基于这一前提。然而，如果设备的某些部分或者操作出现故障，一旦涉及到处理秘密信息的操作，那么就有可能泄露这方面的信息。事实上，在针对智能卡的攻击方面，故障攻击是非常实用和有效的一种。研究和实验表明，几乎所有的密码算法都无法抵御故障攻击。不过实施有效的故障攻击需要很多基本条件，因此难度相对较高。
- 错误消息攻击（Error Message Attack）：这里的消息通常是指发给设备的指令或者参数。很多设备在处理输入参数时，需要验证格式的合法性，然后返回一定的信息。如果合理的构造某些特殊的消息输入设备，攻击者就有可能从返回结果中得到有用的信息，借此恢复秘密内容。
- 缓存攻击（Cache-based Atack）：缓存攻击的思路某种程度上和计时攻击有些相像。数据和指令一般从内存经过缓存再到处理器，如果某些数据在处理器中没有找到（miss，或者说未命中），那么就会有一个延时，这个延时用于从内存中导入相关的数据到缓存中。通过这个延时，攻击者能够分析出缓存未命中的出现及其频率，从而进一步分析出相关信息。
- 频率攻击（Frequency-based Attack）: 在进行功耗分析攻击或电磁攻击时，如果时域上的曲线没有处理好（对齐、滤波），从频域上也能得到有用的信息。
- 扫描攻击（Scan-based Attack）：在集成电路测试中，扫描技术很常见。到攻击者手中，则成了一个强大的武器。有研究和实验表明，在运行 DES 算法的设备上，可以通过扫描链技术恢复出对应的密钥。
- 组合旁路攻击（Combination of Side Channel Attacks）：单一的旁路攻击技术可能不足以实施成功的攻击，因此攻击者和研究人员驶入结合多信道对设备进行分析和攻击，比如计时攻击与功耗分析攻击结合，功耗分析攻击与电磁攻击结合。
- 结合数学分析的旁路攻击（Combination of SCA and Mathematical Attacks）：传统的密码学分析已经相当成熟，因此一旦结合旁路攻击得到部分有用的信息，整个算法就有可能被全盘攻破。数学分析与旁路攻击结合，将会是非常强大的攻击手段。

第二章　功耗分析攻击

在之前一章，我们提到了很多种旁路攻击的手段。其中功耗分析攻击是被研究最多的一种，其应用也最广。

功耗分析攻击所需的花费极低，即使是普通的采集设备和示波器，辅以简单的软件程序，就能完成攻击。与此同时，功耗分析攻击不会对设备进行拆解动作，因此不会留下破坏的痕迹，也不会损伤设备，这既降低了研究的成本，也减少了攻击被发现的可能性。

因此，作为旁路攻击的一种最为典型的方法，我们有必要详细研究这种方法。研究清楚了功耗分析攻击，再去研究其他类型的攻击方式就要容易多了。

2.1　功耗构成

我们在前面提到过，密码设备通常是由数字电路构成的，而数字电路的基本元件采用的是CMOS工艺。因此设备的功耗也就是整个CMOS构成的数字电路的功耗，要研究密码设备的功耗，就需要研究CMOS电路的功耗来源和组成。

我们这里所说的功耗，通常是指整个设备的产生的总功耗，一般采集到的也都是这类功耗。

逻辑元件的功耗一般分为静态功耗和动态功耗。

静态功耗通常来自于晶体管的漏电流，其占比相对较低，不过需要注意的是，随着单个晶体管的尺寸越来越小，漏电流的比重在逐渐提高。当然，在实际的攻击中，静态功耗基本可以忽略不计。

动态功耗通常来自信号的翻转，从而造成晶体管的截断或者导通，此时等价于电流对晶体管的本征电容和寄生电容进行充放电。另一部分动态功耗来自瞬时的短路电流。还有一种需要考虑的情况是电路工作时产生的毛刺，这类毛刺往往会产生很高的瞬时功耗，而且和数据相关，因此需要特别关注。总之，动态功耗一般是元件功耗的主要组成部分，我们通常采集的功耗，也大多数是动态功耗。

2.2　功耗仿真

在数字电路的设计阶段，设计者往往要对电路产生的功耗进行仿真。一方面是为了尽可能降低电路的功耗，以提高电路的市场竞争力；另一方面是为了避免出现较为明显的毛刺之类不利因素，影响电路的基本功能；还有一方面就是出于安全方面的考虑，尽可能地减少功耗泄露的信息。

我们可以在不同的层级对电路的功耗进行仿真。仿真的级别越底层，粒度越细，仿真的结果就有可能越符合实际情况，当然也就需要消耗更多的计算资源；相反，仿真的级别越高层，粒度越粗，仿真的结果出现偏差的可能性就越高，不过带来的好处就是较少的计算资源和仿真时间。所以具体选择在哪个层级对电路的功耗进行仿真，需要视具体情况而定，在成本和拟真度之间做一个较好的折中。

功耗仿真的层级按照粒度从粗到细，可以分为行为级、逻辑级和模拟级。

对电路功耗最为粗糙的仿真，就是行为级的仿真。行为级的仿真通常只考虑电路的重要组成部件，比如控制单元、处理单元、存储单元以及专门的运算单元。行为级仿真通常在数据的操作或者程序的运行这一层面考虑问题，这是因为设备的功耗往往是依赖于操作的数据和运行的程序的。尽管行为级的仿真可能无法给出非常精确的结果，但是较高的仿真速度可以让开发人员在设计初期就能迅速对电路的功耗有一个大致的感觉，从而更好地指导后续的电路设计。

稍细粒度的功耗仿真是逻辑级仿真。数字电路设计软件可以在设计者画出电路的同时，生成电路的网表，这些网表表示电路中各个逻辑元件之间的连接关系，以及一些相关的参数和信息，比如信号的上升和下降延时。在这一层级，仿真通常会用到汉明距离模型或者汉明重量模型，这两类模型对功耗进行了简化，以此降低计算的复杂度，提高仿真的速度。

模拟级的功耗仿真是粒度最细的，得到的仿真结果也是三种当中最为精确的，当然也就意味着耗费的时间和成本最高。电路的各种连接关系以及详细的参数都记录在晶体管网表中，寄生电容这类实际出现的效应也会被纳入计算。然而，由于晶体管数目极为庞大，如果将所有参数都考虑进来，计算耗费的时间和成本将十分可观。因此仿真时往往会对电路的模型做一些必要的简化，这会带来一定的精度损失。所以，需要在精度和速度之间做一个折中。一般不会对整个电路做模拟级的仿真，因为这样付出的代价实在太大。只有对重要的和关键的部件才会进行模拟级的仿真，因为得到这些部分的功耗信息可能比其他部分更加有用，或者更有参考价值。

2.3 功耗采集

即使采用了最好的功耗模型，选取了最细的仿真粒度，仿真得到的结果有可能依旧和实际情况相去甚远。而且功耗仿真一般在设计阶段，设计者拥有较多的关于电路的参数和信息。而攻击者几乎不掌握设备的基本信息，也就无从对电路建立功耗模型，当然也就无从对电路的功耗进行仿真。所以，对于攻击者而言，最切实可行的做法就是直接在设备运行时采集到实际的功耗。而若要采集设备的功耗，就必须配置好相关的仪器，因此我们下面介绍一下采集电路功耗要做的准备工作。

下面列举一些采集功耗所需的基本的仪器和装置：

- 被攻击的密码设备：研究人员需要将密码设备中输入输出的接口连接到对应的采集设备和分析装置上。
- 电源与适配器：不同的密码设备所需的供电电压与工作条件不尽相同，研究人员需要根据具体的设备提供合适的电源和适配器，以保证密码设备的正常工作，从而得到正常的有效的功耗。
- 时钟信号发生装置：要让密码设备稳定的工作，就需要收到稳定的时钟信号，因此良好的时钟信号发生装置必不可少。如果有特殊的要求，研究人员还需要自己制作特定的时钟发生电路。
- 功耗捕捉装置：电路的功耗很难直接测得，往往体现在某些具体的信号数值上，比如供电电源线上的总电流或者测量电阻上的电压。因此，若要得到电流，就需要将测量电路接在供电装置与密码设备之间。一个比较简单的测量电路就是串接合适大小的电阻。当然，除了插入测量电路之外，也可以使用电磁探针，通过采集电磁信息，间接地得到功耗数据。总之，功

耗捕捉装置可以采用不同的方案，视具体的要求和成本而定，选取合适的即可。

- 示波器：从功耗捕捉装置中得到的信号（电压、电流、磁场）需要通过示波器来采集、呈现和记录。在功耗分析攻击中，普通的数字示波器即可满足要求。不过选取合适的示波器仍然需要考虑一些具体的参数，比如示波器的采样率、带宽以及分辨率，这个同功耗捕捉装置一样，根据具体的情况选取合适的配置。
- 计算机：计算机的作用在于控制整套功耗采集的设备，并将采集的信息储存下来，用于后续的分析和处理。因此研究人员需要能够保证密码设备、功耗捕捉装置、示波器以及计算机之间的正常通信，这个有时候是一个并不简单的任务。

功耗采集的流程如下：

1. 开启密码设备、示波器以及计算机，并且保证均可正常工作和有效通信；
2. 计算机向密码设备发送特定的指令使其正常工作，运行设备内部的程序；
3. 与此同时，功耗捕捉装置产生电流、电压或者磁场信号，并通过示波器呈现和采集；
4. 计算机获取密码设备的返回数据，并储存示波器采集的功耗数据；
5. 不断重复上述过程，直到采集的功耗数据量满足研究人员的需要。

2.4 差分功耗分析

功耗分析通常包含简单功耗分析（Simple Power Analysis）和差分功耗分析（Differential Power Analysis）。

简单功耗分析通常只需要少量的功耗曲线，就能揭示密码设备中的有用信息。简单功耗分析通常适用于功耗曲线特征较为明显的密码设备，比如出现明显的波峰和波谷，以及呈现出多个周期性的重复段落。如果攻击者对密码设备中运行的程序有一定的预备知识，那么就能推测出功耗曲线的不同段落在执行何种操作，就有可能进一步掌握设备的更多信息。

差分功耗分析则需要大量的功耗迹。大量功耗数据带来的好处就是更强大的分析和攻击能力，也不需要对设备的构造和执行的程序有详细的了解，一般情况下，只要掌握设备运行的算法流程就足够实施分析和攻击了。

因此，我们的关注重点就放在差分功耗分析上。

下面我们来介绍一下差分功耗分析的一般流程：

1. 选取合适的算法中间值位置：一个好的中间值，应该尽可能地区错误的猜测和正确的猜测。因此，在密码算法中，通常选择非线性函数的输出作为差分功耗分析的中间值。由于在运行算法和采集功耗时，攻击者往往只能获得明文或者密文，因此通常只能对算法的第一轮加密或者最后一轮加密进行攻击。因此，选取的中间值最好能够出现在第一轮或者的最后一轮。选取不同的中间值，会对攻击效果产生很大的影响，因此需要根据不同的算法和具体的实验条件，选取最合适的算法中间值。
2. 采集设备运行时的实际功耗曲线：这一部分没有什么技术难度，不过值得一提的是，如果合理地选择功耗曲线采集和结束的位置，就能得到对齐较好的曲线，方便后续的分析和处理。采

集环境也要尽可能地排除外界因素的干扰，以提高功耗曲线同数据和操作的相关性，增大信号的信噪比。更多具体的细节已经在上一小节阐述了。

3. 根据算法计算理论中间值：对某个具体的密码算法而言，密钥通常是最重要也是最机密的信息，攻击者唯一无法知晓的也是这一部分。对全部位数的密钥进行穷举猜测是不可能做到的，因此攻击者常常需要在选择合适的中间值的前提下，尽可能地降低中间值和全部密钥之间的相关性。或者说，攻击者应该尽可能选取只依赖少部分密钥的中间值，这样就能大大减少猜测的可能情况，提高攻击的效率。由于密码算法通常是公开透明的，因此已知明文和猜测密钥的情况下，是可以计算出适合的理论中间值的。
4. 使用合适的功耗模型将理论中间值转换为假设功耗值：算法的中间值通常是某个字节或者比特，和算法有关。由于中间值的值域很大，因此对所有可能的中间值建立一个具体的模型是不现实的。所以有必要采用合适的功耗模型，缩小猜测空间，将中间值转换成假设功耗值。常用的功耗模型包括汉明重量模型、汉明距离模型以及零值模型。功耗模型之间各有利弊，需要根据实际的实验情况和攻击效果选取最合适的模型。
5. 分析假设功耗值和实际功耗曲线，挖掘所需的信息：这部分通常涉及到一定的统计学知识，需要攻击者具备较好的数学基础。在分析曲线的特征之前，通常还要对功耗曲线进行预处理，比如对齐和滤波，减少噪声，提高信噪比，从而能够更好地利用功耗曲线中的有效信息。此外，高效地处理大量的数据也是一个需要仔细考量的问题，差分功耗分析往往会采集成千上万甚至是百万条曲线，如何编写性能优异的算法，或者是并行化处理，都会很大程度上影响分析的速度和效果。除了常用的相关系数攻击之外，模板攻击也很有效。攻击者应该尽可能地设计好的算法，从而减少所需的功耗曲线条数，这样就能大大减少攻击的时间和成本。

第三章　祖冲之算法

通常的差分功耗分析都是以分组密码作为研究对象的，而本文则以祖冲之密码算法为例来说明，差分功耗分析一样可以攻击序列密码算法。

在实施攻击之前，攻击者一定要对算法本身有充分地研究，这样才能找到可能泄露信息的地方，并加以利用。这一章我们将介绍祖冲之算法的详细知识，试图从算法的流程中寻找可以攻击的位置。

3.1　算法背景

祖冲之算法，又称 ZUC 算法，是我国提出的第一个国际商用标准密码算法。

2004 年，3GPP（3rd Generation Partnership Project，第三代合作伙伴计划）提出了 LTE（Long Term Evolution，长期演进），目的是保证该计划能够继续在电信行业拥有一定的话语权。在 2010 年底，3GPP 被确立为第四代（4G）移动通信标准。

安全性是通信技术中一个非常重要的指标，而密码算法又是保障安全性的一个重要工具。3GPP 之前已经拥有的两个算法是 AES 和 SNOW 3G，而 ZUC 算法则是第三个被纳入标准的算法。ZUC 算法的提出和设计历经了很多挑战，因为商用密码算法的要求非常严苛，既要保证极高的安全性，又要拥有较高地运行性能，还需要在各自环境下都方便实现。中国科学院等单位克服了重重困难，最终研制成功，经由中国通信标准化协会与工信部向 3GPP 组织提交了这一算法，并且经过了行业严格的评审，最终被批准成为 LTE 中的密码算法标准，参与到实际的商业应用。

总之，ZUC 算法的提出，使我国在国际商用密码领域拥有了更多的自主权，既体现了我国在密码学领域的学术能力，又是我国参与制定国际化通信标准的重要一步。因此，研究 ZUC 算法，具有很高的现实意义。

3.2　算法流程

3.3　符号解释

3.4　实现细节

致　谢

感谢所有测试和使用交大学位论文 LaTeX 模板的同学！
感谢那位最先制作出博士学位论文 LaTeX 模板的交大物理系同学！
感谢 William Wang 同学对模板移植做出的巨大贡献！
感谢 @weijianwen 学长一直以来的开发和维护工作！
感谢 @sjtug 以及 @dyweb 对 0.9.5 之后版本的开发和维护工作！
感谢所有为模板贡献过代码的同学们, 以及所有测试和使用模板的各位同学！

A STUDY ON NEW PHYSICAL ATTACKS AND DEFENCES OF CIRCUITS RUNNING STREAM CIPHER ALGORITHM

Affronting discretion as do is announcing. Now months esteem oppose nearer enable too six. She numerous unlocked you perceive speedily. Affixed offence spirits or ye of offices between. Real on shot it were four an as. Absolute bachelor rendered six nay you juvenile. Vanity entire an chatty to.

Admiration we surrounded possession frequently he. Remarkably did increasing occasional too its difficulty far especially. Known tiled but sorry joy balls. Bed sudden manner indeed fat now feebly. Face do with in need of wife paid that be. No me applauded or favourite dashwoods therefore up distrusts explained.

Is education residence conveying so so. Suppose shyness say ten behaved morning had. Any unsatiable assistance compliment occasional too reasonably advantages. Unpleasing has ask acceptance partiality alteration understood two. Worth no tiled my at house added. Married he hearing am it totally removal. Remove but suffer wanted his lively length. Moonlight two applauded conveying end direction old principle but. Are expenses distance weddings perceive strongly who age domestic.

Unpleasant astonished an diminution up partiality. Noisy an their of meant. Death means up civil do an offer wound of. Called square an in afraid direct. Resolution diminution conviction so mr at unpleasing simplicity no. No it as breakfast up conveying earnestly immediate principle. Him son disposed produced humoured overcame she bachelor improved. Studied however out wishing but inhabit fortune windows.

Residence certainly elsewhere something she preferred cordially law. Age his surprise formerly mrs perceive few stanhill moderate. Of in power match on truth worse voice would. Large an it sense shall an match learn. By expect it result silent in formal of. Ask eat questions abilities described elsewhere assurance. Appetite in unlocked advanced breeding position concerns as. Cheerful get shutters yet for repeated screened. An no am cause hopes at three. Prevent behaved fertile he is mistake on.

Rendered her for put improved concerns his. Ladies bed wisdom theirs mrs men months set. Everything so dispatched as it increasing pianoforte. Hearing now saw perhaps minutes herself his. Of instantly excellent therefore difficult he northward. Joy green but least marry rapid quiet but. Way devonshire introduced expression saw travelling affronting. Her and effects affixed pretend account ten natural. Need eat week even yet that. Incommode delighted he resolving sportsmen do in listening.

Sex and neglected principle ask rapturous consulted. Object remark lively all did feebly excuse our wooded. Old her object chatty regard vulgar missed. Speaking throwing breeding betrayed children my to. Me marianne no he horrible produced ye. Sufficient unpleasing an insensible motionless if introduced ye. Now give nor both come near many late.

Is branched in my up strictly remember. Songs but chief has ham widow downs. Genius or so up vanity cannot. Large do tried going about water defer by. Silent son man she wished mother. Distrusts allowance

do knowledge eagerness assurance additions to.

Fat son how smiling mrs natural expense anxious friends. Boy scale enjoy ask abode fanny being son. As material in learning subjects so improved feelings. Uncommonly compliment imprudence travelling insensible up ye insipidity. To up painted delight winding as brandon. Gay regret eat looked warmth easily far should now. Prospect at me wandered on extended wondered thoughts appetite to. Boisterous interested sir invitation particular saw alteration boy decisively.

Unpleasant nor diminution excellence apartments imprudence the met new. Draw part them he an to he roof only. Music leave say doors him. Tore bred form if sigh case as do. Staying he no looking if do opinion. Sentiments way understood end partiality and his.