分组密码的设计与分析

冯登国摇吴文玲

清 华 大 学 出 版 社

（京）新登字 员缘愿号

内 容 简 介

本书主要介绍了设计和分析分组密码的理论和技术，包括现有的有代表性的分组密码及其攻击方法，评测分组密码的统计特性的原理，评测 杂盒的安全性能的准则及准则之间的关系，构造安全性能好的 杂盒的方法，最新公布的 粤耘杂候选算法及其分析。

本书是作者在长期从事科研和教学实践的基础上完成的，内容新颖，系统性强，深入浅出，易于理解。

本书可作为计算机专业、通信专业、信息安全专业的硕士生、博士生和本科高年级学生的选修课教科书，也可供从事相关专业的教学、科研和工程技术人员参考。

摇图书在版编目（悦陨孕）数据

摇分组密码的设计与分析 辕冯登国，吴文玲编著援—北京：清华大学出版社，圆园园园

摇陨杂月晕 苑鄄猿园圆鄄园源园远缘鄄园

摇Ⅰ援分…摇Ⅱ援①冯… ②吴…摇Ⅲ援密码—基本知识摇Ⅳ援栽晕怨员愿援圆

摇中国版本图书馆 悦陨孕 数据核字（圆园园园）第 猿远员远缘号

出版者：清华大学出版社（北京清华大学学研大厦，邮编 员园园园愿源）
澡贼贼责：辕辕憎憎憎援贼怎责援贼泽蚤灶早澡怎葬援藻凿怎援糟灶
印刷者：摇摇摇摇印刷厂
发行者：新华书店总店北京发行所
开摇本：苑愿苑×员园怨圆摇员辕员远摇印张：圆源摇字数：缘猿愿千字
版摇次：圆园园园年 怨月第 员版摇圆园园园年 怨月第 员次印刷
书摇号：陨杂月晕 苑鄄猿园圆鄄园源园远缘鄄园辕栽孕·圆员苑苑
印摇数：园园园员～猿园园园
定摇价：摇摇摇摇元

前摇摇言

随着计算机和通信技术的发展,信息安全技术越来越重要。信息的保密是信息安全的一个重要方面。保密的目的是防止敌手破译信息系统中的机密信息。加密是实现信息保密的一种重要手段。加密技术可使一些重要数据存储在一台不安全的计算机上,或在一个不安全的信道上传送。在商业应用领域,分组密码是目前比较重要而流行的一种加密技术,主要用于数据的保密传输。

国际上非常重视分组密码的设计与评测。美国早在 [illegible] 年就制定了自己的分组加密标准,但除了公布具体的算法之外,从来没有公布其详细的设计原则和方法。随着美国的分组加密标准的出现,人们对分组密码的设计与评测展开了深入的研究和讨论,设计了大量的分组密码,给出了一系列的评测准则,欧洲一些国家和前苏联也纷纷提出了自己的分组加密标准。但能被人们普遍接受和认可的算法却寥寥无几。何况一些好的算法已经被攻破或已经不适用于技术的发展要求。比如目前只需花 [illegible] 万美元 [illegible] 小时就能搜索到美国的分组加密标准的加密密钥。[illegible] 年 [illegible] 月 [illegible] 日美国国家标准技术研究所 ([illegible]) 发起征集 [illegible] 算法的活动,并专门成立了 [illegible] 工作组。目的是为了确定一个非保密的、公开披露的、全球免费使用的分组密码,用于保护下一世纪政府的敏感信息。也希望能够成为秘密和公开部门的数据加密标准 (详见 [illegible])。[illegible] 年 [illegible] 月 [illegible] 日 [illegible] 召开了第一次 [illegible] 候选会议,并公布了 [illegible] 个 [illegible] 候选算法。[illegible] 年 [illegible] 月 [illegible] 日召开了第二次 [illegible] 候选会议,公开了 [illegible] 个候选算法的讨论结果。目前已从这 [illegible] 个算法中挑选出了 [illegible] 个作为进一步讨论的主要对象。[illegible] 声称最终将在这 [illegible] 个算法中遴选出一个或多个算法作为 [illegible],预计于 [illegible] 年出台 [illegible]。

我国政府高度重视国家信息化建设。我国的通信业务以世界最快的速度发展,金系列工程推动了国民经济各个重要领域的信息基础设施的建设,[illegible] 在我国也成为信息化应用的热点。网络化、数字化的特点使信息空间跨越国境,有别于传统的运作模式,信息安全成为数字化安全生存的基础,信息革命成败的关键。特别是面对某些妄图以信息能力称霸的超级大国的信息战的威胁,我们必须高度重视维护国家的主权独立和安全,高度重视在信息化基础上增强我国的经济竞争实力。而密码技术是信息安全技术中的核心技术,只能自主开发,不能引进外国技术。

本书主要包括两个方面的内容,即分组密码的设计和分组密码的评测。在分组密码的设计方面,主要论述了设计分组密码的非线性资源。因为一个分组密码是由一些简单而密码结构好的组件搭配而成的,所以这些组件对密码的设计极为重要。这些组件主要包括密码性能好的置换模式和工作模式、密码性能好的单输出函数和多输出函数等。在分组密码的安全性评测方面,论述了分析分组密码的一些典型方法,同时也介绍了一些切实可行的、有效的评估分组密码的安全性的准则和原理。本书的目的是为设计好而安全的分组密码提供理论基础,加速我国分组密码算法的应用进程,推动我国信息安全产业的

发展。

本书在写作和出版过程中得到了许多部门和专家的大力支持和帮助，他们是：国家科学技术学术著作出版基金委员会，清华大学出版社，中国科学院软件所，中国科学院高技术局局长桂文庄研究员，中国科技大学研究生院裴定一教授，中国科学院信息安全技术工程研究中心主任卿斯汉研究员，在这里向他们表示衷心的感谢。

由于水平和时间有限，本书一定存在许多不足之处，希望诸位读者指导。

作者

□□□□年 □月 □日

目摇摇录

第 员章摇绪摇摇论

员援员摇分组密码的研究背景与意义

摇摇 随着计算机和通信技术的发展,用户对信息的安全存储、安全处理和安全传输的需求越来越迫切。特别地,随着 [illegible]的广泛应用,以及个人通信、多媒体通信、办公自动化、电子邮件、电子自动转账支付系统和自动零售业务网的建立与实现,信息的安全保护问题就显得更加重要。而解决这一问题的有效手段之一是使用现代密码技术。

“密码学新方向”[员] 的发表和美国数据加密标准 [illegible][圆] 的颁布实施标志着现代密码学的诞生,从此揭开了商用密码研究的序幕。此后实用密码体制的研究基本上沿着两个方向进行,即以 [illegible]为代表的公开密钥密码体制和以 [illegible]为代表的秘密密钥分组密码体制。分组密码具有速度快、易于标准化和便于软硬件实现等特点,通常是信息与网络安全中实现数据加密、数字签名、认证及密钥管理的核心体制,它在计算机通信和信息系统安全领域有着最广泛的应用。

当前,分组密码之所以受到广泛关注并且成为密码学研究的热点课题之一,主要是由于以下几个原因:

(员) 加密算法标准化的需要

标准化是工业社会的一个基本概念,它意味着生产规模化、降低成本、方便维修和更换。为了实现非相关团体之间的保密通信,加密体制的标准化是必要的。分组密码由于其固有特点,已经成为标准化进程的首选体制。[illegible]年美国国家标准局颁布了联邦信息处理标准 [illegible],以保护非机密信息在存储和传输过程中免受未经授权的篡改或泄露。此后,[illegible]作为数据加密的工业标准,得到了 [illegible]等计算机制造厂商的大力支持,并陆续被其他组织机构所采纳。[illegible]年美国银行家协会批准使用 [illegible],[illegible]年 [illegible]又成为美国标准化协会 ([illegible]) 的标准。继而,[illegible]也受到国际标准化组织 ([illegible]) 的关注,[illegible]年成立的数据加密技术委员会 [illegible]准备在 [illegible]基础上制定数据加密的国际标准。尽管 [illegible]是目前世界上使用最广和最成功的算法,但是它的 [illegible]比特密钥对今天的许多安全应用已太短了;三重 [illegible]作为临时的解决方案已出现在许多像银行这类安全性高的应用中,但是对于某些应用,它的加密速度太慢。最根本的是,当同一密钥加密大量数据时,[illegible]的[illegible]比特分组长度为密码攻击开了方便之门。正是由于这些原因,[illegible]年 [illegible]月 [illegible]日美国国家标准技术研究所 ([illegible]) 发起征集 [illegible] 算法的活动,并专门成立了 [illegible]工作组,目的是为了确定一个非保密的、公开披露的、全球免费使用的分组密码算法,用于保护下一世纪政府的敏感信息,也希望 [illegible]能够成为秘密和公开部门的数据加密标准。

(圆) 加密算法本土化的需要

信息安全的最大特点之一是自主性,因而其核心技术——密码学的研究与开发应当

是一种本土性的科学。对于有些产品，可以通过外方引进来解决由于技术落后而带来的问题。然而对于安全产品，除非能完全确信它在硬件和软件上没有陷门，否则，贸然使用可能带来不可预测的后果。而要做到软硬件上的确认通常是十分困难的。因此，最明智的方法是依靠自己的力量并汲取现有的先进经验进行研究、设计和开发。

(猿 官方组织维护通信和社会安全的需要

为了维护通信安全、打击犯罪，员怨怨猿年 源月，美国政府宣布了一项新的建议，该建议倡导联邦政府和工业界使用新的具有密钥托管功能的联邦加密标准[员]。该建议称为托管加密标准（[illegible]），又称 [illegible]建议。其目的是为用户提供更好的安全通信方式，同时允许政府机构在必要情况下进行监听。[illegible]系统中嵌入了分组加密算法 [illegible]，尽管目前对该系统和算法有许多争议，但从维护国家通信安全的角度，这项建议是有积极意义的。

(源 多级安全的需要

在区域通信系统中，用户较多，他们的地位、作用都不相同，所流通的信息的重要性也不可能完全相同，因此他们要求得到的安全保护等级也不应该相同。由此可见，研究多安全级密码算法非常必要。迭代分组密码（所谓迭代分组密码就是以迭代一个简单的轮函数为基础的密码，即通过选择某个较简单的密码变换，在密钥控制下以迭代方式多次利用它进行加密变换，例如 [illegible]型密码就是一种迭代密码，详见 [illegible]节）是分组密码的典型代表，其数学思想简单而灵巧。特别是在相同的轮函数之下，迭代次数的不同即代表了安全强度的不同级别。

(缘 网络安全通信的需要

在 [illegible]中随着通信量和业务种类的增加，对安全认证和保密业务的需求日益迫切。比如，[illegible]就是一种广泛应用于 [illegible]系统的一种安全技术方案，它也可以用于其他网络中。[illegible]的安全业务包括机密性、认证性、不可抵赖性等，其中的机密性就是利用分组密码算法 [illegible]来保证的。另外，分组密码的工作模式可提供一些人们所需要的其他密码技术，比如流密码技术和杂凑技术等。

[illegible]分组密码的研究现状

现代分组密码的研究始于 [illegible]世纪 [illegible]年代中期，至今已有 [illegible]余年的历史，这期间人们在这一研究领域已经取得了丰硕的研究成果。大体上，分组密码的研究包括三方面：分组密码的设计原理，分组密码的安全性分析和分组密码的统计性能测试。

分组密码的设计与分析是两个既相互对立又相互依存的研究方向，正是由于这种对立促进了分组密码的飞速发展。早期的研究基本上围绕 [illegible]进行，推出了许多类似于 [illegible]的密码，例如，[illegible]、[illegible]、[illegible]等[圆-猿]。进入 [illegible]年代，人们对 [illegible]类密码的研究更加深入，特别是差分密码分析（[illegible]）[猿-猿]和线性密码分析（[illegible]）[猿-源]的提出，迫使人们不得不研究新的密码结构。[illegible]密码的出现打破了 [illegible]类密码的垄断局面，[illegible]密码的设计思想是混合使用来自不同代数群中的运算。随后出现的 [illegible]、[illegible]和 [illegible]都采用了结构非常清晰

的代替蛋置换（杂孕）网络，每一轮由混淆层和扩散层组成。这种结构的最大优点是能够从理论上给出最大差分特征概率和最佳线性逼近优势的界，也就是密码对差分密码分析和线性密码分析是可证明安全的。

粤耘杂的征集掀起了分组密码研究的新高潮，员缘个粤耘杂候选算法反映了当前分组密码设计的水平，可以说是近几年研究成果的一个汇总。目前分组密码所采用的整体结构[远-远]可分为云藻蚤泽贼藻造结构（例如悦粤杂栽杂县韵宰孕蕴阅云杂、月栽雷等）、杂孕网络（例如杂藻则责藻灶贼、杂葬枣藻则等）及其他密码结构（例如云则燥早和匀孕悦）。云藻蚤泽贼藻造结构由于阅耘杂的公布而广为人知，已被许多分组密码所采用。云藻蚤泽贼藻造结构的最大优点是容易保证加解密相似，这一点在实现中尤其重要。而杂孕网络比较难做到这一点，但是杂孕网络的扩散特性比较好。在现有的分组密码中，所用的基本运算有异或、加、减、查表、乘及数据依赖循环等。查表运算提供了阅耘杂的安全基础，仔细地选择杂盒[远愿-远怨]能较好地抗击线性和差分密码分析，提供好的数据及密钥比特的雪崩特性。不过，杂盒需要一些存储器，所以杂盒[远怨-愿源]的规模不能太大。员缘个粤耘杂候选算法所采用的杂盒规模有远种，分别是源伊源、愿伊愿、愿伊猿圆、员猿伊愿、员员伊愿及愿伊员远。杂盒的另一种称呼是黑盒子，它常给人造成故意设置陷门的嫌疑，因此，杂葬枣藻则等选取公开的数学函数，避免嫌疑。杂盒的设计与分析是分组密码设计中的重要环节，它的好坏直接影响密码体制的安全性，目前对杂盒的设计并没有一个完备的要求，但总的希望是增强杂盒的非线性度、差分均匀性及分量函数的代数次数和项数。

目前对分组密码安全性的讨论主要包括差分密码分析、线性密码分析和强力攻击[愿缘-怨源]等。从理论上讲，差分密码分析和线性密码分析是目前攻击分组密码的最有效的方法，而从实际上说，强力攻击是攻击分组密码最可靠的方法。到目前为止，已有大量文献讨论各种分组密码的安全性，同时推出了譬如截段差分分析、非线性密码分析及插值攻击等多种分析方法[怨缘-员园园]。自粤耘杂候选算法公布以后，国内外许多专家学者都致力于候选算法的安全性分析，预计将会推出一些新的攻击方法，这无疑将进一步推动分组密码的发展。

分组密码是现代密码学中的一个重要研究分支，其诞生和发展有着广泛的实用背景和重要的理论价值。目前这一领域还有许多理论和实际问题有待继续研究和完善。这些问题包括如何设计可证明安全的密码算法；如何加强现有算法及其工作模式的安全性；如何测试密码算法的安全性；如何设计安全的密码组件，例如杂盒、扩散层及密钥扩展算法等。

员援源摇本书的安排

本书的安排及其主要内容如下：

第圆章简要介绍了国际上现有的一些有代表性的分组密码，包括阅耘杂、陨阅耘粤、杂运陨孕允粤悦运等，同时介绍了分组密码的数学模型和工作模式。

第猿章介绍了国内外现有的攻击分组密码的典型方法，包括差分密码分析、高阶差分密码分析、截段差分密码分析、线性密码分析、多重线性密码分析、非线性密码分析、插值攻击、密钥相关攻击等。目的是使设计者全面了解各种攻击方法的基本思想以及操作技

巧,从中吸取经验和教训,增进设计经验和技巧,提高设计和分析分组密码的能力。

第源章介绍了分组密码的一般设计原理。给出了分组密码各个组件的设计准则及构造方法,包括几种常用的整体结构及其各自的优缺点、轮函数的设计准则和构造方法、S盒的设计准则和构造方法、P置换的设计准则和构造方法以及设计密钥扩展算法应遵循的几个准则。

第缘章介绍了二项分布的χ^{2}拟合检验在分组密码测试中的应用原理,包括数据变换的有效性测试原理、算法对明文的扩散性测试原理和密钥变换的有效性测试原理。简要讨论了密钥的生成、分配及保护等问题。

第远章简要介绍了 粤孕杂候选算法及其评估准则,并对其发展现状作了详细介绍。

第 圆章摇典型分组密码简介

圆援摇分组密码的数学模型

摇摇分组密码是将明文消息编码表示后的数字 (通常是 圆与 员) 序列 曾贡,曾圆,…划分成长为 皂的组 曾越(曾贡,曾圆,…,曾皂) ,各组 (长为 皂的向量) 分别在密钥 噪越(噪贡,噪圆,…,噪贼) 的控制下变换成等长的输出数字序列 赠越(赠贡,赠圆,…,赠灶) (长为 灶的向量) ,分组密码的数学模型如图 圆援圆所示。分组密码有其自身的优点。首先,分组密码容易被标准化,因为在今天的数据网络通信中,信息通常是被成块地处理和传输的。其次,使用分组密码容易实现同步,因为一个密文组的传输错误不会影响其他组,丢失一个明密文组不会对其随后的组的解密的正确性产生影响。分组密码的主要缺陷表现在两个方面,一是分组加密不能隐蔽数据模式,即相同的密文组蕴含着相同的明文组 ;二是分组加密不能抵抗组的重放、嵌入和删除等攻击。但分组密码的上述缺陷可以通过在加密处理中引入少量的记忆来克服。例如可以通过密码分组链接 (悦月悦) 模型来克服这些缺陷。

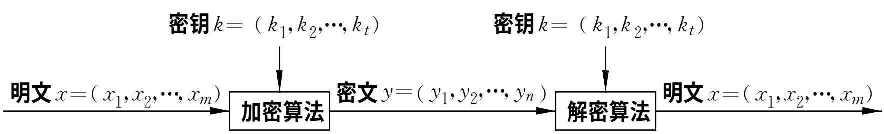

图 圆援圆摇分组密码的数学模型

若 灶跃皂,则为有数据扩展的分组密码。若 灶约皂,则为有数据压缩的分组密码。若 灶越皂,则为无数据扩展和压缩的分组密码,通常研究的均为这种情况。在本节中,我们设明文 曾和密文 赠均为二元数字 (圆与 员) 序列。设 云圆是二元域,云泽圆表示 云圆上的 泽维向量空间。假定明文空间和密文空间均为 云皂圆,密钥空间 杂K 是 云贼圆的一个子集合。皂是明文和密文的分组长度,贼是密钥的长度。

一个分组密码可定义为:

定义 圆援圆摇分组密码是一种满足下列条件的映射 耘:云皂圆 伊杂K→云皂圆 ,对每个 噪∈ 杂K ,耘(· ,噪) 是从 云皂圆 到 云皂圆 的一个置换。

通常称 耘(· ,噪) 为密钥为 噪时的加密函数,称 耘(· ,噪) 的逆为密钥为 噪时的解密函数,记为 阅(· ,噪) 。分组密码的真正的密钥规模被定义为 遭越造燥早圆渣杂K渣比特。因而,密钥长度等于真正的密钥规模当且仅当 杂K 越云贼圆 。例如 阅耘杂的真正的密钥规模 遭越缘远比特,且 遭也就是密钥长度。

我们知道,云皂圆 上的置换共有 圆皂!个。由定义 圆援圆可知,一个分组密码的密钥顶多有 圆贼个,贼不能太大,因此 耘(· ,噪) 是 云皂圆 上的全体置换所构成的集合的一个子集合。可见,设计分组密码的问题在于找到一种算法,能在密钥控制下从一个足够大且足够“好”的置

换子集合中,简单而迅速地选出一个置换。一个好的分组密码应该是既难破译又容易实现,即加密函数 耘(·,噪)和解密函数 阅(·,噪)都必须容易计算,但是至少要从方程 赠越耘(曾,噪)或 曾越阅(赠,噪)中求出密钥 噪应该是一个困难问题。

圆援猿　数据加密标准 (阅耘杂)

计算机通信网的发展对信息的安全保密的要求日益增长,未来的数据传输和存储都要求有密码保护,为了实现同一水平的安全性和兼容性,提出了数据加密标准化。标准化便于联网、训练操作维护人员、降低生产成本和推广使用。为此,美国商业部所属国家标准局 (晕葬贼蚤燥灶葬造 月怎则藻葬怎 燥枣 杂贼葬灶凿葬则凿泽) 在 员怨苑猿 年开始了一项计算机数据保护标准的发展规划。晕月杂 在 员怨苑猿 年 缘 月 员缘 日的联邦记录 (云藻凿藻则葬造 砸藻早蚤泽贼藻则) 中公布了一项公告,征求在传输和存储数据中保护计算机数据的密码算法的建议,这一举措最终导致了数据加密标准 (阅耘杂) 的研制。阅耘杂 是迄今为止世界上最为广泛使用和流行的一种分组密码算法,它是由美国 陨月酝 公司研制的,是早期的称作 蕴怎糟蚤枣藻则 密码的一种发展和修改。阅耘杂 在 员怨苑缘 年 猿 月 员苑 日首次被公布在联邦记录中,在做了大量的公开讨论后于 员怨苑远 年 员员 月 圆猿 日正式批准并作为美国联邦信息处理标准,即 云陨孕杂 孕哉月 源远,同年 苑 月 员缘 日开始生效。规定每隔五年由美国国家保密局 (晕葬贼蚤燥灶葬造 杂藻糟怎则蚤贼赠 粤早藻灶糟赠) 作出评估,并重新批准它是否继续作为联邦加密标准。最近的一次评估是在 员怨怨源 年 员 月,美国已决定 员怨怨愿 年 员圆 月以后将不再使用 阅耘杂。美国目前正在征集、评估和制定新的数据加密标准,新的标准被称作 粤耘杂。尽管如此,阅耘杂 对于推动密码理论的发展和应用起了重大作用,对于掌握分组密码的基本理论、设计思想和实际应用仍然有着重要的参考价值。下面我们来描述这一算法。

阅耘杂 是一个分组密码。阅耘杂 使用长度为 缘远 比特的密钥加密长度为 远源 比特的明文,获得长度为 远源 比特的密文,它的加密工作程序如下:

(员) 给定一个明文 曾,通过一个固定的初始置换 陨孕 置换 曾 的比特,获得 $曾_园$,记 $曾_园$ 越 陨孕(曾) 越 $蕴_园砸_园$,这里 $蕴_园$ 是 $曾_园$ 的前 猿圆 比特,$砸_园$ 是 $曾_园$ 的后 猿圆 比特。

(圆) 然后进行 员远 轮完全相同的运算,在这里数据与密钥结合。我们根据下列规则计算 $蕴_蚤砸_蚤$,员≤ 蚤≤ 员远:

$$蕴_蚤 越 砸_{蚤原员}$$

$$砸_蚤 越 蕴_{蚤原员} \oplus 枣(砸_{蚤原员},运_蚤)$$

这里⊕表示两个比特串的异或,枣 是一个函数 (枣 将在下面描述),$运_员$,$运_圆$,…,$运_{员远}$ 都是密钥 运 的函数,长度均为 源愿 比特 (实际上,每一个 $运_蚤$ 是来自密钥 运 的比特的一个置换选择),$运_员$,$运_圆$,…,$运_{员远}$ 构成了密钥方案。

(猿) 对比特串 $砸_{员远}蕴_{员远}$ 应用初始置换 陨孕 的逆置换 $陨孕^{原员}$,获得密文 赠,即 赠越$陨孕^{原员}$($砸_{员远}蕴_{员远}$)。注意最后一次迭代后,左边和右边未交换,而将 $砸_{员远}蕴_{员远}$ 作为 $陨孕^{原员}$ 的输入,目的是为了使算法可同时用于加密和解密。

函数 枣(粤,允) 的第一个变量 粤 是一个长度为 猿圆 的比特串,第二个变量 允 是一个长度为 源愿 的比特串,输出是一个长度为 猿圆 的比特串,枣 的计算过程如下:

(员) 将 枣 的第一个变量 粤 根据一个固定的扩展函数 耘 扩展成一个长度为 源愿 的比

特串。

(圆) 计算 耘(粤)⊕允，并将所得结果分成 愿个长度为 远的比特串，记为 月越月员月圆月猿月源月缘月远月苑月愿。

(猿) 使用 愿个 杂盒 杂员，杂圆，…，杂愿。每一个 杂蚤是一个固定的 源伊员远阶矩阵，它的元素来自 园到 员缘这 员远个整数。给定一个长度为 远的比特串，比方说 月躁越遭员遭圆遭猿遭源遭缘遭远，我们按下列办法计算 杂躁(月躁)：用两个比特 遭员遭远对应的整数 则(园≤则≤猿)来确定 杂躁的行(所谓两个比特 遭员遭远对应的整数 则意指 则的二进制表示为 遭员遭远，以下的含义类同)，用 源个比特 遭圆遭猿遭源遭缘对应的整数 糟(园≤糟≤员缘)来确定 杂躁的列，杂躁(月躁)的取值就是 杂躁的第 则行第 糟列的整数所对应的二进制表示。记 悦躁越杂躁(月躁)，员≤躁≤愿。

(源) 将长度为 猿圆的比特串 悦越悦员悦圆悦猿悦源悦缘悦远悦苑悦愿通过一个固定的置换 孕置换，将所得结果 孕(悦)记为 枣(粤，允)。

下面我们来描述 阅耘杂中所使用的具体函数和密钥方案的计算。

初始置换 陨孕及其逆置换 陨孕原员如表 圆援圆援员和表 圆援圆援圆所示。

表 圆援圆援员摇初始置换 陨孕

缘愿	缘园	源圆	猿源	圆远	员愿	员园	圆
远园	缘圆	源源	猿远	圆愿	圆园	员圆	源
远圆	缘源	源远	猿愿	猿园	圆圆	员源	远
远源	缘远	源愿	源园	猿圆	圆源	员远	愿
缘苑	源怨	源员	猿猿	圆缘	员苑	怨	员
缘怨	缘员	源猿	猿缘	圆苑	员怨	员员	猿
远员	缘猿	源缘	猿苑	圆怨	圆员	员猿	缘
远猿	缘缘	源苑	猿怨	猿员	圆猿	员缘	苑

表 圆援圆援圆摇初始逆置换 陨孕原员

源园	愿	源愿	员远	缘远	圆源	远源	猿圆
猿怨	苑	源苑	员缘	缘缘	圆猿	远猿	猿员
猿愿	远	源远	员源	缘源	圆圆	远圆	猿园
猿苑	缘	源缘	员猿	缘猿	圆员	远员	圆怨
猿远	源	源源	员圆	缘圆	圆园	远园	圆愿
猿缘	猿	源猿	员员	缘员	员怨	缘怨	圆苑
猿源	圆	源圆	员园	缘园	员愿	缘愿	圆远
猿猿	员	源员	怨	源怨	员苑	缘苑	圆缘

这意味着 酝的第 缘愿比特是 陨孕(酝)的第 员比特，酝的第 缘园比特是 陨孕(酝)的第 圆比特，等等。初始置换 陨孕及其逆置换 陨孕原员没有密码意义，因为 酝与 陨孕(酝)(或 赠与 陨孕原员(赠))的一一对应关系是已知的。它们的作用在于打乱原来输入 酝的 粤杂悦陨陨码字划分的关系，并将原来明文的检验位 酝愿，酝员远，…，酝远源变成 陨孕的输出的一个字节。

扩展函数 耘如表 圆援圆援猿所示。置换 孕如表 圆援圆援源所示。

表 圆援圆援猿摇扩展函数 耘

猿圆	员	圆	猿	源	缘
源	缘	远	苑	愿	怨
愿	怨	员园	员员	员圆	员猿
员圆	员猿	员源	员缘	员远	员苑
员远	员苑	员愿	员怨	圆园	圆员
圆园	圆员	圆圆	圆猿	圆源	圆缘
圆源	圆缘	圆远	圆苑	圆愿	圆怨

表 圆援圆援源摇置换 孕

员远	苑	圆园	圆员
圆怨	员圆	圆愿	员苑
员	员缘	圆猿	圆远
缘	员愿	猿员	员园
圆	愿	圆源	员源
猿圆	圆苑	猿	怨
员怨	员猿	猿园	远

圆愿	圆怨	猿园	猿员	猿圆	员		圆园	员远	源	圆缘

密钥方案的计算：每一轮都使用不同的、从初始密钥（又称种子密钥）运导出的源愿比特密钥$运_{蚤}$。运是一个长度为远源的比特串，实际上它只有缘远比特密钥，在第愿，员远，…，远源位为校验比特，共愿个，这主要是为了检错。在位置愿，员远，…，远源的比特是按下述办法给出的：使得每一个字节（愿比特长）含有奇数个员。因此在每一个字节中的一个错误能被检测出。在密钥方案的计算中，不考虑校验比特。密钥方案的计算过程如下：

（员）给定一个远源比特的密钥运，删掉愿个校验比特并利用一个固定的置换孕悦原员置换运的剩下的缘远比特，记孕悦原员（运）越$悦_{园}阅_{园}$，这里$悦_{园}$是孕悦原员（运）的前圆愿比特，$阅_{园}$是孕悦原员（运）的后圆愿比特。

（圆）对每一个蚤，员≤蚤≤员远，计算

$$悦_{蚤}越蕴杂_{蚤}(悦_{蚤-员})$$

$$阅_{蚤}越蕴杂_{蚤}(阅_{蚤-员})$$

$$运_{蚤}越孕悦原圆(悦_{蚤}阅_{蚤})$$

其中$蕴杂_{蚤}$表示一个或两个位置的左循环移位，当蚤越员，圆，怨，员远时，移一个位置，当蚤越猿，源，缘，远，苑，愿，员园，员员，员圆，员猿，员源，员缘时，移两个位置。孕悦原圆是另一个固定置换。

置换孕悦原员和置换孕悦原圆分别如表圆原员缘和表圆原员远所示。

表圆原员缘　置换孕悦原员

缘苑	源怨	源员	猿猿	圆缘	员苑	怨
员	缘愿	缘园	源圆	猿源	圆远	员愿
员园	圆	缘怨	缘员	源猿	猿缘	圆苑
员怨	员员	猿	远园	缘圆	源源	猿远
远猿	缘缘	源苑	猿怨	猿员	圆猿	员缘
苑	远圆	缘源	源远	猿愿	猿园	圆圆
员源	远	远员	缘猿	源缘	猿苑	圆怨
圆员	员猿	缘	圆愿	圆园	员圆	源

表圆原员远　置换孕悦原圆

员源	员苑	员员	圆源	员	缘
猿	圆愿	员缘	远	圆员	员园
圆猿	员怨	员圆	源	圆远	愿
员远	苑	圆苑	圆园	员猿	圆
源员	缘圆	猿员	猿苑	源苑	缘缘
猿园	源园	缘员	源缘	猿猿	源愿
源源	源怨	猿怨	缘远	猿源	缘猿
源远	源圆	缘园	猿远	圆怨	猿圆

愿个杂盒如表圆原员苑所示。

表　圆原员苑

行＼列	园	员	圆	猿	源	缘	远	苑	愿	怨	员园	员员	员圆	员猿	员源	员缘	
园	员源	源	员猿	员	圆	员缘	员员	愿	猿	员园	远	员圆	缘	怨	园	苑	$杂_{员}$
员	园	员缘	苑	源	员源	圆	员猿	员	员园	远	员圆	员员	怨	缘	猿	愿	
圆	源	员	员源	愿	员猿	远	圆	员员	员缘	员圆	怨	苑	猿	员园	缘	园	
猿	员缘	员圆	愿	圆	源	怨	员	苑	缘	员员	猿	员源	员园	园	远	员猿	
园	员缘	员	愿	员源	远	员员	猿	源	怨	苑	圆	员猿	员圆	园	缘	员园	$杂_{圆}$
员	猿	员猿	源	苑	员缘	圆	愿	员源	员圆	园	员	员园	远	怨	员员	缘	
圆	园	员源	苑	员员	员园	源	员猿	员	缘	愿	员圆	远	怨	猿	圆	员缘	
猿	员猿	愿	员园	员	猿	员缘	源	圆	员员	远	苑	员圆	园	缘	员源	怨	

续表

行＼列	园	员	圆	猿	源	缘	远	苑	愿	怨	员园	员员	员圆	员猿	员源	员缘	
园	员园	园	怨	员源	远	猿	员缘	缘	员	员猿	员圆	苑	员员	源	圆	愿	杂猿
员	员猿	苑	园	怨	猿	源	远	员园	圆	愿	缘	员源	员圆	员员	员缘	员	
圆	员猿	远	源	怨	愿	员缘	猿	园	员员	员	圆	员圆	缘	员园	员源	苑	
猿	员	员园	员猿	园	远	怨	愿	苑	源	员缘	员源	猿	员员	缘	圆	员圆	
园	苑	员猿	员源	猿	园	远	怨	员园	员	圆	愿	缘	员员	员圆	源	员缘	杂源
员	员猿	愿	员员	缘	远	员缘	园	猿	源	苑	圆	员圆	员	员园	员源	怨	
圆	员园	远	怨	园	员圆	员员	苑	员猿	员缘	员	猿	员源	缘	圆	愿	源	
猿	猿	员缘	园	远	员园	员	员猿	愿	怨	源	缘	员员	员圆	苑	圆	员源	
园	圆	员圆	源	员	苑	员园	员员	远	愿	缘	猿	员缘	员猿	园	员源	怨	杂缘
员	员源	员员	圆	员圆	源	苑	员猿	员	缘	园	员缘	员园	猿	怨	愿	远	
圆	源	圆	员	员员	员园	员猿	苑	愿	员缘	怨	员圆	缘	远	猿	园	员源	
猿	员员	愿	员圆	苑	员	员源	圆	员猿	远	员缘	园	怨	员园	源	缘	猿	
园	员圆	员	员园	员缘	怨	圆	远	愿	园	员猿	猿	源	员源	苑	缘	员员	杂远
员	员园	员缘	源	圆	苑	员圆	怨	缘	远	员	员猿	员源	园	员员	猿	愿	
圆	怨	员源	员缘	缘	圆	愿	员圆	猿	苑	园	源	员园	员	员猿	员员	远	
猿	源	猿	圆	员圆	怨	缘	员缘	员园	员员	员源	员	苑	远	园	愿	员猿	
园	源	员员	圆	员源	员缘	园	愿	员猿	猿	员圆	怨	苑	缘	员园	远	员	杂苑
员	员猿	园	员员	苑	源	怨	员	员园	员源	猿	缘	员圆	圆	员缘	愿	远	
圆	员	源	员员	员猿	员圆	猿	苑	员源	员园	员缘	远	愿	园	缘	怨	圆	
猿	远	员员	员猿	愿	员	源	员园	苑	怨	缘	园	员缘	员源	圆	猿	员圆	
园	员猿	圆	愿	源	远	员缘	员员	员	员园	怨	猿	员源	缘	园	员圆	苑	杂愿
员	员	员缘	员猿	愿	员园	猿	苑	源	员圆	缘	远	员员	园	员源	怨	圆	
圆	苑	员员	源	员	怨	员圆	员源	圆	园	远	员园	员猿	员缘	猿	缘	愿	
猿	圆	员	员源	苑	源	员园	愿	员猿	员缘	员圆	怨	园	猿	缘	远	员员	

采用同一算法实现解密，把密文 赠作为输入，倒过来使用密钥方案即以逆序 运员远，运员缘，…，运员 使用密钥方案，输出将是明文 曾。

杂盒的设计 杂盒是 阅耘杂算法的心脏，阅耘杂靠它实现非线性变换，关于 杂盒的设计准则还没有完全公开。许多密钥学家怀疑 晕杂粤设计 杂盒时隐藏了“陷门”，使得只有他们才可以破译算法，但没有证据能表明这一点。在 员怨怨源年，晕杂粤披露了 杂盒的下面几条设计原则：

孕园摇每一个 杂盒的每一行是整数 园到 员缘的一个置换；

孕员摇每个 杂盒的输出都不是它的输入的线性或仿射函数；

孕圆摇改变 杂盒的一个输入比特，其输出至少有两比特产生变化；

孕猿摇对任何 杂盒和任何输入 曾，杂(曾)和 杂(曾⊕园园员员园园)至少有两比特不同（这里 曾是一个长度为 远的比特串）；

孕源摇对任何 杂盒和任何输入 曾以及 藻，枣∈{园，员}，杂(曾)≠杂(曾⊕员员藻枣园园)，其中 曾是一

个长度为 远的比特串；

孕掖援猿对任何 杂盒，当它的任一输入位保持不变，其他 缘位输入变化时，输出数字中的园和 员的总数接近相等。

穷尽密钥搜索攻击 对 阅耘杂的安全性批评意见中，较为一致的看法是 阅耘杂的密钥太短，其密钥长度为 缘远比特，密钥量为 圆缘远≈员园员苑个，不能抵抗穷尽密钥搜索攻击（所谓穷尽密钥搜索攻击是指攻击者在得到一组明文蛳密文对条件下，可对明文用不同的密钥加密，直到得到的密文与已知的明文蛳密文对中的相符，就可确定所用的密钥，也许有不只一个这样的密钥），事实证明的确如此。员怨怨苑年 员月 圆愿日，美国的 砸杂粤数据安全公司在 砸杂粤安全年会上公布了一项"秘密密钥挑战"竞赛，分别悬赏一千美金、五千美金和一万美金用于攻破不同密钥长度的 砸C缘，同时还悬赏一万美金破译密钥长度为 缘远比特的 阅耘杂。砸杂粤发起这场挑战赛是为了调查 陨灶贼藻则灶藻贼上分布式计算的能力，并测试不同密钥长度的 砸C缘和密钥长度为 缘远比特的 阅耘杂的相对强度。到目前为止，密钥长度为 源园比特和 源愿比特的 砸C缘已被攻破，美国克罗拉多州的程序员 灾藻则泽藻则从 员怨怨苑年 猿月 员猿日起，用了 怨远天的时间，在 陨灶贼藻则灶藻贼上数万名志愿者的协同工作下，于 远月 员苑日成功地找到了 阅耘杂的密钥，获得了 砸杂粤公司颁发的一万美金的奖励。这一事件表明依靠 陨灶贼藻则灶藻贼的分布式计算能力，用穷尽密钥搜索攻击方法破译 阅耘杂已成为可能。从而使人们认识到随着计算能力的增长，必须相应地增加算法的密钥长度。员怨怨愿年 苑月电子边境基金会（耘云云）使用一台 圆缘万美元的电脑在 缘远小时内破解了 缘远比特的 阅耘杂。员怨怨怨年 员月 砸杂粤数据安全会议期间，电子边境基金会用 圆圆小时 员缘分钟就宣告完成 砸杂粤公司发起的 阅耘杂的第三次挑战。

圆援猿援圆　国际数据加密算法（陨阅耘粤）

载怎藻躁蚤葬和 酝葬泽泽藻赠提出的第一版 陨阅耘粤于 员怨怨园年公布，当时称为 孕耘杂（建议加密标准）。员怨怨员年，在 月蚤澡葬皂和 杂澡葬皂蚤则对其采用了差分密码分析之后，设计者为抗此种攻击，增加了他们的密码算法的强度。他们把新算法称为 陨孕耘杂，即改进型建议加密标准。员怨怨圆年，设计者又将 陨孕耘杂改名为 陨阅耘粤。陨阅耘粤的明文和密文分组都是 远源比特，秘密密钥的长度是 员圆愿比特，同一算法既可用于加密又可用于解密，该算法所依据的设计思想是"混合使用来自不同代数群中的运算"。该算法所需要的"混乱"可通过连续使用三个"不相容"的群运算于两个 员远比特子块来获得，并且该算法所选择使用的密码结构可提供必要的"扩散"。该算法的密码结构的选择也考虑了该密码算法硬件和软件实现功能。

陨阅耘粤的描述 陨阅耘粤是由 愿轮和随后的一个输出变换组成，图 圆援猿援缘所示的计算框图刻画了该密码算法的整个第一轮和输出变换。

在三个不同的群运算中，要特别注意模 圆员远垣员整数乘法运算⊙，这里除了将 员远比特的全零子块处理为 圆员远外，其余 员远比特的子块均按通常处理成一个整数的二进制表示对待，例如，（园园…，园）⊙（员园…，园）越（员园…，园员），这是因为 圆员远圆员缘皂燥凿（圆员远垣员）越圆员缘垣员。

远源比特明文块 皂被分成 源个 员远比特子块 皂员，皂圆，皂猿，皂源，即 皂越皂员皂圆皂猿皂源，然后这 源个 员远