南京邮电大学

硕士学位论文

基于纠错码的公钥密码体制研究

姓名：朱陆费

申请学位级别：硕士

专业：信息与通信工程

指导教师：张宗橙

20090301

摘 要

随着通信的迅速发展以及由此带来的信息失密问题，例如信息被非法截取和数据库资料被窃，保密通信是十分重要的。在通信系统中采取消息加密和纠错编码等措施，可以使得在开放信道中传输的消息具有抗信道干扰和防止消息被非法接收者或无关人员窃听的能力，从而能够安全、可靠地把消息传送给指定的接收者。由此可见，纠错编码和密码技术是实现保密通信的两个不同侧面的技术手段。在构造加密体制时，结合纠错码以保证加密信息，能够安全、可靠地传输，因此，纠错码与密码的结合是代数编码理论和密码学发展的必然产物。

基于保密通信、纠错码与密码三者之间的关系，本文深入研究了基于纠错码的公钥密码体制，例如：M 公钥密码体制、N 公钥密码体制与 M 公钥密码体制的推广，通过 MATLAB 数值计算，分析比较了这些体制的性能。

关键词：保密通信；纠错码；Goppa 码；公钥密码体制

Abstract

With the rapid development of communications, the combination of error-correcting codes and encryption system ensure that encrypted information have security, therefore, the combination is the inevitable outcome of the development of algebraic coding theory and cryptography.

In this thesis, based on the relationship between confidential communications, error-correcting code and encryption, the writer deeply analyzes M-public-key cryptosystem, N-public-key cryptosystem and other M-public-key cryptosystem. By computer calculation, the writer compares and analyzes the performance.

Keywords: security communication; error-correcting code; Goppa; public-key cryptosystem

南京邮电大学学位论文原创性声明

本人声明所呈交的学位论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得南京邮电大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

研究生签名：朱张贵 日期：2009.4.11

南京邮电大学学位论文使用授权声明

南京邮电大学、中国科学技术信息研究所、国家图书馆有权保留本人所送交学位论文的复印件和电子文档，可以采用影印、缩印或其它复制手段保存论文。本文电子文档的内容和纸质论文的内容相一致。除在保密期内的保密论文外，允许论文被查阅和借阅，可以公布（包括刊登）论文的全部或部分内容。论文的公布（包括刊登）授权南京邮电大学研究生部办理。

研究生签名：朱张贵 导师签名：张宗橙 日期：2009.4.11

第一章 绪 论

由于通信的迅速发展带来了信息失密问题，信息(如金融信息、军事情报等)被非法截取和数据库资料被窃的事例经常发生，信息失密势必会造成严重后果，因此，保密通信成为十分重要的问题。

保密通信是发送端对欲传输的消息采取加密措施后才在信道中传送，而接收端对所收到的加密消息进行解密使它恢复出原消息的一种通信方式。加密的目的是隐蔽消息内容，使窃听者和无关人员在收到加密消息后无法获得原消息，而指定的接收方则可用“密钥”方便地把收到的加密消息正确地变换成原消息。而为了保证消息传输可靠性，加密消息在进入信道开始传输之前，要进行一次纠错编码，以增强消息的抗干扰能力。

1．1 通信系统模型

所有通信或信息传输系统都可归结成如图 1.1 所示的数字通信系统模型。

信息传输或通信的目的，是要把收方不知道的信息及时、可靠、完整、安全而又经济地传送给指定的收方。图 1.1 中描述的整个系统的各个部分，就是为了完成上述目的。当然，由于具体要求与应用场合的不同，图中的某些组成部分可能没有，也有可能还要增加其它部分。

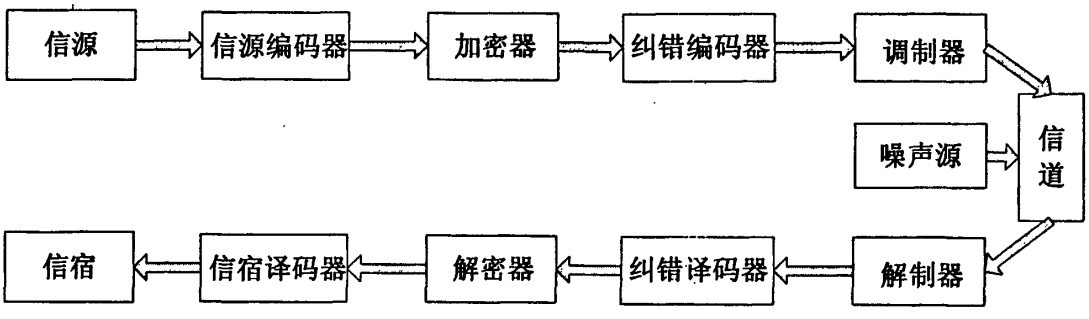

图 1.1 数字通信系统模型

图 1.1 中信源编码器是把信源(人、计算机或其它信息处理设备)发出的消息，如语音、图像、文字等转换成二进制形式的信息序列，也就是 0, 1 符号串，并且为了使传输更为经济有效，还要去除一些与被传信息无关的冗余度。

在信息传输或处理过程中，除了指定的接收者外，还有非指定的或非授权的用户，他们通过各种技术手段企图窃取机密信息。因此，为了保证被传送信息的安全和隐私，必须在信源编码器输出信息通过加密器时，用编码方法对信息进行隐藏。

由于传输信息的媒介如电波、电线等总是存在有各种人为或天然的噪声和干扰，因此，为了提高整个系统传输信息的可靠性，就需要对加密器输出的信息进行一次纠错编码，人为地增加一些冗余信息，使其具有自动检错或纠错功能。这种功能由图中的纠错编码器完成。

为了使信息能与传输媒介的特性相匹配，使传输更为有效和可靠，将纠错编码器输出的二进制(或多进制)数据送入调制器进行调制。从调制器输出的信号经传输媒介后到达收端。由于受传输媒介中的各种干扰的影响，到达收端的信号序列中可能已有错误。收端的解调器对收到的信号解调，变成二进制(或多进制)序列串，送入纠错译码器纠错后，进入解密器，解密器把输入的序列恢复成原本的信息，再通过信源译码器恢复成原始的消息送给信宿(人或计算机等)。

信道是传输信息的通道，又是传送物理信号的具体媒介。它可以是一对导线、一条同轴电缆、光导纤维或传输电磁波的空间等。一般信道都属于开放信道，无论是指定的接收者或窃听者都可同样方便地收到在开放信道中传输的消息。因此当信号通过这些媒介时，是很不安全的。不仅存在着各种天然和人为干扰使被传送信号产生错误以外，而且还存在着非指定或非授权用户通过各种方法(如搭线、电磁波接收、声音接收等)对所传输的信号进行侦听，这种攻击称为被动攻击。更有甚者，有些非法入侵者主动向系统攻击，采用删除、更改、增添、重放、伪造等手段，向系统注入信号或破坏被传的信号，以达到欺骗别人，有利于自己的目的，这种攻击称为主动攻击。因此如何保护系统中所传消息的真实性、完整性、可靠性，即如何实现保密通信，这是任何一个通信系统都面临和必须解决的问题。

1．2 纠错密码理论

在通信系统中采取消息加密和纠错编码等措施，可以使得在开放信道中传输的消息具有抗信道干扰和防止消息被非法接收者或无关人员窃听的能力，从而能够安全、可靠地把消息传送给指定的接收者。由此可见，纠错编码和密码技术是实现保密通信的两个不同侧面的技术手段，这也是 Shannon 在 40 年代同时研究编码理论和密码学的原因。

1948 年 Shannon 发表了著名文章“通信的数学理论”[1]，奠定了信息论的基础，其中包括信源编码和信道编码定理。

1949 年 Shannon 发表的“保密系统的信息理论”[2]为私钥密码系统建立了理论基础，从此密码学成为一门科学。

密码学是一门研究通信安全和保护信息资源的既古老而又年青的科学和技术。它包括两方面：密码编码学和密码分析学。密码编码学是对信息编码以隐蔽信息的一门学问；而密码分析学是研究分析破译密码的学问。这二者既相互对立又相互促进，共同推动密码学的发展。

纠错编码是提高通信质量或可靠性的一门年青的学科。自 1948 年 Shannon 提出信道编码定理至今，这门学科已取得了丰硕的成果。利用纠错编码的差错控制技术，已成为通信系统设计中一种重要、在某些场合甚至是必不可少的技术手段，纠错编译码器已成为现代通信系统中的重要组成部分。

当把纠错码与密码结合在一起设计，或用纠错码构造密码系统时，不可避免的要加上冗余度，而冗余度的增加，无疑减少了保密系统的安全性。另一方面，从密码系统的随机性来看，利用纠错码构造的密码体制不能做到使密码系统完全随机化，而只能做到局部随机化。本质上讲，纠错密码体制仅仅是一类局部随机化的密码体制。但是，如果这类纠错密码体制的最终安全乃是计算上安全的话，那么纠错与加密相结合的密码体制，或利用纠错码构造的密码系统乃是实际上安全的，因而也是可行的。

总之，为了设计一个实际可行的好的密码系统，正如 Shannon 在 1949 年的论文中指出的“好密码的设计问题，本质上是寻找针对某些其它条件的一种求解难题的问题”。

1．3 课题的主要内容

本文的第一章提出保密通信、纠错码与密码三者之间的关系。信息的传输、变换、压缩和存储等信息处理的有效性、可靠性和安全性已成为当今信息处理中的重要问题，而各种形式的编码和密码则是解决上述问题的基本理论和方法。在任何实际系统中，纠错码经常是和加密联系在一起的，因为在一个设计周到的密码体制中，哪怕是一丁点的改变也会完全破坏信息的完整性。

第二章简述了纠错码译码问题和 Goppa 码。指出一般线性码的译码问题是 NPC 问题，NPC 问题是最复杂的问题。因为，Goppa 码具有快速译码算法，所以，第一个基于

线性分组码的公钥密码体制就是由 Goppa 码构造的，由于 Goppa 码的特点，在构造某些公钥密码体制中，具有重要意义。

第三章深入研究了基于纠错码的公钥密码体制。首先，分析了 M 公钥密码体制和 N 公钥密码体制的性能以及两者的等价性。然后，针对 M 公钥密码体制在有扰信道中的缺点，进而介绍了 M_S 公钥密码体制，并对其性能进行分析。最后，为了改善 M 公钥密码体制的两大不足——公钥量大和速率低，又引入了各种变型后的 M 公钥密码体制。

接下来，第四章就是本文的核心章节，也是作者在本次课题中所做的主要工作。通过第三章的理论分析以后，在第四章中，作者将第三章中所介绍的公钥密码体制，通过计算机，进行 MATLAB 数值计算分析。根据对 M 公钥密码体制、N 公钥密码体制和 M_S 公钥密码体制进行解线性方程组攻击和 Lee-Brickell 攻击，作者得出了相应的工作因子曲线图。此外，作者还得出 M 公钥密码体制、N 公钥密码体制、M_S 公钥密码体制和变型后的公钥密码体制的速率曲线图。

最后，对于论文所涉及的公钥密码体制，本文作者对此进行性能比较分析，并且归纳作者所做的工作，得到了一些有价值的结果，提出了对未来的展望。

第二章 纠错码理论及其NPC问题

目前，几乎所有得到实际应用的纠错编码都是线性的。线性分组码是整个纠错编码中很重要的一类码，也是讨论各类码的基础。在此基础上，介绍了Goppa码，它在利用纠错码构造密码系统中起着关键作用。

2．1 纠错编码的概述

随着数字信息交换、处理和存储用的大规模、高速数据网的飞速发展，如何保证数据在有噪声信道中无误差地高速传输正变得越来越重要。正是社会的这一巨大需求促进了纠错编码理论以及其工程应用的迅速发展。各种纠错编码以其能自动地纠正或检测出数据传输过程中的误差这一鲜明的特点，深受广大科技工作者的青睐。

Shannon信道编码定理指出，在编码效率小于信道容量的条件下，通过编码可以使译码错误概率任意小，从而达到可靠通信。定理的证明采用了随机编码技术，给出的结果只说明存在一种编码方式，其误码率随着码长 n 的增长趋于任意小。但证明是非构造性的，它没有告诉我们如何构造实际上可实现的、具有上述性能的这类码的方法。Hamming提出的纠错编码就是为了试图去解决这一问题。它的目的是寻找在实际上易于实现且能达到有效而可靠通信的编译码方法。

所谓纠错编码，就是按一定规则给信息序列M增加一些多余的码元，使不具有规律性的信息序列M变换为具有某种规律性的数字序列 c，又称为码序列。也就是说，码序列中的信息序列M的诸码元与多余码元之间是相关的。在接收端，纠错译码器利用这种预知的编码来译码，根据相关性来检测和纠正传输过程中产生的差错就是纠错编码的基本思想。纠错编码的主要功能就是能自动地纠正或检测出数据传输过程中由于各种噪声干扰而造成的误差。目前能达到这种目的的纠错编码有许许多多。按照不同的方式可以将众多的纠错编码进行不同的分类。例如：

1、按照对信源序列处理方式的不同，可分为分组码与卷积码两大类。

分组码是把信息序列，以 k 个码分组，通过编码器将每组的 k 元信息按一定规律产生 r 个多余码元(称为校验元)，输出长为 $n=k+r$ 的一个码字。因此每一个码组的 r 个校验元仅与本组的信息元有关而与别组无关。分组码用[n，k]表示，n 表示码长，k 表示信息位数目，$R=k/n$ 称为分组码的码率。

卷积码是把信源输出的信息序列，以 k_0 个(k_0 通常很小)码元分段，通过编码器输出长为 $n_0(\geq k_0)$ 的一段码段。但是该码的 n_0-k_0 个检验元不仅与本段的信息元有关，而且也与其前 m 段的信息元有关，故卷积码用 $[n_0,k_0,m]$ 表示，称 $N_c=(m+1)n_0$ 为卷积码的编码约束长度。

2、按照校验元与信息元之间的关系可分为线性码与非线性码。

线性码的所有码字在并元和运算之下是封闭的，而非线性码则不封闭。或者换句话说，线性码实际上就是 n 维线性空间中的一个 k 维 $(k<n)$ 子空间。

3、按照纠正错误的类型可分为纠正随机(独立)错误的码、纠正突发错误的码、纠正同步错误的码和既能纠随机错误又能纠突发错误的码。

4、按照每个码元的取值来分，可分为二进制码和多进制码。

当然，同一种纠错码在不同分类之下是属于不同类别的，例如线性分组码，它就既是分组码又是线性码。

2．2 线性码的重量分布与等价类

$[n, k, d]$码的重量分布问题就是，二进制线性分组码的 2^k 个码字，除全 0 码字以外，没有重量小于 d 的码字，但重量等于 d，$d+1$，…，n 的码字各有多少个。这对研究码的纠错性能有极重要的意义。

定理 2.1 设 c 是 $[n, k, d]$ q 进制线性分组码，A_i 是重量为 i 的码字个数，则

$$A(z)\overset{\Delta}{=}\sum_{i=0}^{n}A_i z^i \tag{2.1}$$

定义为码 c 的重量分布算子，序列 $\{A_0,A_1,\cdots,A_n\}$ 称为 c 的重量分布。

码 c 的重量分布算子与它的对偶码 $c^{\perp}$ 的重量分布算子之间有一个重要的关系。

定理 2.2[5] 设 c 是 $GF(q)$ 上的 $[n, k]$码，它的重量分布算子为 $A(z)$，又设 $B(z)$ 是它的对偶码 $c^{\perp}$ 的重量分布算子，则

$$B(z)=q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right) \tag{2.2}$$

称该式为 MacWilliams 恒等式。可知由码的对偶码的重量分布可以很快得到码的重量分布，反之亦然。

交换码校验矩阵 H 的列或对 H 矩阵的行进行交换，都不会改变码的最小距离及码的重量分布。因此由 H 矩阵所产生的码 c，及由交换 H 矩阵的列所得到的 H'所产生的码 c'，若它们的距离特性或码的重量分布一样，则 c 和 c' 码是等价的，属于同一等价类。

定义 2.1[5] 两个[n，k]分组码 c 和 c' 码，若对 c 码的 n 个码元位置进行置换、以及加一个不变的 n 重后得到了码 c'，则 c 和 c' 码等价。即若有一个置换 π 和一个矢量(n 重)α，使

$$c' = \{\pi(u) + \alpha, u \in C\} \tag{2.3}$$

则 c 和 c' 码等价，属于一个等价类。

在线性码的情况下，上述定义说明等价码 c 和 c'，仅仅只是码元位置次序排列的不同，而码的重量分布并不会改变。

可知对线性码而言，找码的等价类归结于找一个满秩的 $k \times k$ 阶矩阵 S 和 n 阶置换阵 P，使

$$S^{-1}G_1 = G_2P \tag{2.4}$$

这里 G_1 是[n，k]码 c_1 的生成矩阵，G_2 是码 c_2 的生成矩阵，如果能找到 S^{-1} 和 P，则 c_1 和 c_2 码等价。

码的等价类，对于决定用何种纠错码构造密码体制有重大意义，若码的等价类很难找，且不同等价类非常多，则这类码就可用来构造某些密码体制，反之则不能或很困难。

2．3 线性分组码的译码

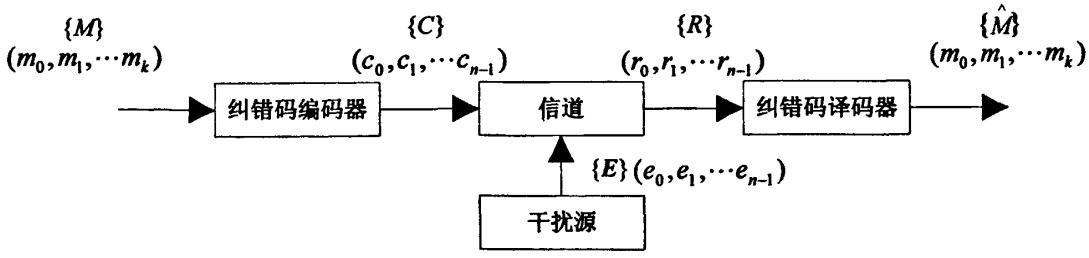

图 2.1 利用纠错码的数字通信模型

由图 2.1 可知，信道输出的 R 是一个二(或 q)进制序列，而译码器的输出是一个信息序列 M 的估值序列 $\hat{M}$ 。

译码器的基本任务就是根据一套译码规则，由接收序列 R 给出与发送的信息序列 M 最接近(最好是相同)的估值序列 $\hat{M}$ 。由于 M 与码字 C 之间存在一一对应关系，所以这等价于译码器根据 R 产生一个 C 的估值序列 $\hat{C}$ 。显然，当且仅当 $\hat{C}=C$ 时，$\hat{M}=M$，这时译码器正确译码。

如果译码器输出的 $\hat{C}\neq C$，则译码器产生了错误译码，之所以产生错误译码是由于：信道干扰很严重，超过了码本身的纠错能力；其次，由于译码设备的故障。当给定接收序列 R 时，译码器的条件译码错误概率定义为

$$P(E\mid R)=P(\hat{C}\neq C\mid R) \tag{2.5}$$

所以译码器的错误译码概率

$$P_E=\sum_R P(E\mid R)P(R) \tag{2.6}$$

$P(R)$是接收 R 的概率，与译码方法无关，所以译码错误概率最小的最佳译码规则是使

$$\begin{aligned}&\min P_E=\min_R P(E\mid R)=\min_R P(\hat{C}\neq C\mid R)\\&\min P(\hat{C}\neq C\mid R)\Rightarrow \max P(\hat{C}=C\mid R)\end{aligned} \tag{2.7}$$

因此，译码器对输入的 R，如果能在 2^k(或 q^k)码字中选择一个使 $P(\hat{C}_i=C\mid R)(i=1,2,\cdots,2^k)$ 最大的码字 C_i 作为 C 的估值序列 $\hat{C}$，则这种译码规则一定使译码器输出错误概率最小，称这种译码规则为最大后验概率译码。

由贝叶斯公式

$$P(C_i \mid R) = \frac{P(C_i)P(R \mid C_i)}{P(R)} \tag{2.8}$$

可知，若发端发送每个码字的概率 $P(\mathrm{Ci})$均相同，且由于 $P(\mathrm{R})$与译码方法无关，所以

$$\max_{i=1,2,\cdots,2^k} P(C_i \mid R) \Rightarrow \max_{i=1,2,\cdots,2^k} P(R \mid C_i) \tag{2.9}$$

对二进制对称信道(BSC)而言，

$$P(R \mid C_i) = \prod_{j=1}^{n} P(r_i \mid c_{ij}) \tag{2.10}$$

这里码字 $C_i=(c_{i1},c_{i2},\cdots,c_{in})$，$i=1,2,\cdots,2^k$。

一个译码器的译码规则若能在 2^k 个码字 C 中选择某一个 C_i 使式(2.9)成为最大，则这种译码规则称为最大似然译码(MLD)，$P(R \mid C)$称为似然函数，相应的译码器称为最大似然译码器。由于 $\log_b x$ 与 x 是单调关系，因此式(2.9)与式(2.10)可写成

$$\max_{i=1,2,\cdots,2^k} \log_b P(R \mid C_i) = \max_{i=1,2,\cdots,2^k} \sum_{j=1}^{n} \log_b p(r_i \mid c_{ij}) \tag{2.11}$$

称 $\log_b P(R \mid C)$为对数似然函数或似然函数。对于离散无记忆信道(DMC)，MLD 是使译码错误概率最小的一种最佳译码准则或方法，但此时要求发端发送每一码字的概率 $P(C_i)(i=1, 2,\ldots, 2^k)$均相等，否则 MLD 不是最佳的。在以后的讨论中，都认为 $P(C_i)$均近似相等。

2．4 纠错码理论中的 NPC 问题与复杂性系数

一个码能否实用的关键取决于它的译码方法是否简单、译码器的成本是否低廉、译码速度是否快以及译码错误概率是否小，总而言之，译码复杂性要小、性能要好。

另一方面，如果用纠错码构造公钥密码体制，则要求码不存在快速的译码算法，而只能采取穷搜索或其它译码复杂性极高的通用译码算法。因此在差错控制系统中应用纠错码以提高通信可靠性，与在密码中应用纠错码构造某些密码体制，这二者对纠错码的译码要求是截然相反的。有折中办法吗？回答是肯定的，这是因为一般线性码的译码问题是 NPC 问题。

2．4．1 纠错码理论中的 NPC 问题

如果一个问题可以找到一个能在多项式的时间里解决它的算法，那么这个问题就属于 P 问题。NP 问题不是非 P 类问题，NP 问题是指可以在多项式的时间里验证一个解的问题。

为了说明 NPC 问题，先引入一个概念——约化(Reducibility，也叫“归约“)。

如果能找到这样一个变化法则，对任意一个程序 A 的输入，都能按这个法则变换成程序 B 的输入，使两程序的输出相同，那么，问题 A 就可约化为问题 B。

当然，这里所说的“可约化”是指的可“多项式地”约化(Polynomial-time Reducible)，即变换输入的方法是能在多项式的时间里完成的。约化的过程只有用多项式的时间完成才有意义。

从约化的定义中，可知，一个问题约化为另一个问题，时间复杂度增加了，问题的应用范围也增大了。存在这样一个 NP 问题，所有的 NP 问题都可以约化成它。换句话说，只要解决了这个问题，那么所有的 NP 问题都解决了。这一类问题就是 NPC 问题。NPC 问题的出现使整个 NP 问题的研究得到了飞跃式的发展。

NPC 问题的定义非常简单，同时满足下面两个条件的问题就是 NPC 问题。首先，它得是一个 NP 问题；然后，所有的 NP 问题都可以约化到它。

既然所有的 NP 问题都能约化成 NPC 问题，那么只要任意一个 NPC 问题找到了一个多项式的算法，那么所有的 NP 问题都能用这个算法解决了，NP 也就等于 P 了。因此，“正是 NPC 问题的存在，使人们相信 P≠NP”。 NPC 问题目前没有多项式的有效算法，只能用指数级甚至阶乘级复杂度的搜索。

若已知一般的$[n,k,d]$二进制线性分组码的 H，t 及任一$(n-k)$维伴随式 s，求 n 维错误矢量 e，$w(e)\le t$，且 e 满足

$$e\cdot H^T = s \tag{2.12}$$

是 NPC 问题。

由 H 求 G 或 G 求 H，由 $G\cdot H^T = 0$ 可以用多项式时间求解，因此式(2.12)也可用生成矩阵 G 来描述。

因为由伴随 s 求错误图样 e 就是纠错码的译码问题，故一般线性码的译码问题是 NPC 问题，也是纠错码构造某些密码体制的理论基础。但是对某些有特殊代数结构的非一般

的$[n,k,d]$二进制线性分组码，如Goppa码，存在有快速译码算法。因此利用某些置换把Goppa码化成一般线性码，再用来构造某些公钥密码体制。

对一般线性码，还有以下NPC问题：

①是否存在有给定重量的码字；

②求汉明重量不是k的倍数的最小汉明重量码字，这里$k \geq 2$。$k=2$时，则求最小奇重量码字是NPC问题；

③若给定任意正整数w_1，w_2；$0<w_1<w_2$，求满足$w_1 \leq w(x) \leq w_2$的码字x；

④求最大汉明重量码字。

存在某些线性分组码，它们很可能不存在有效的译码算法。这里所指的有效译码算法，是指译码的计算复杂性和空间复杂性是多项式时间。

在用纠错码构造密码体制方面，如何利用其NPC问题，值得研究。

2．4．2 译码复杂性系数

译码的计算复杂性是指译码器收到n重R后，平均译出一个码字所需的时间和空间复杂性，也可定义为平均译出一个码元所需的计算复杂性。

定义2.2 令A是解决二进制$[n, k]$线性分组码类的一个给定译码问题的算法。A的译码复杂性$D_A[n,k]$是时间复杂性(工作因子)W_A和空间复杂性S_A的乘积：

$$D_A[n,k]=W_A S_A$$

则译码复杂性系数定义为

$$d_{CA}[n,k]=\lim_{n\to\infty}\frac{1}{n}\log_2 D_A[n,k] \tag{2.13}$$

若该极限存在的话。

由该定义可得

$$d_{CA}[n,k]=\lim_{n\to\infty}\frac{1}{n}\log_2 D_A[n,k]=\lim_{n\to\infty}\frac{1}{n}\log_2 W_A+\lim_{n\to\infty}\frac{1}{n}\log_2 S_A \tag{2.14}$$

如果仅只有A的空间复杂性是多项式限定的，则

$$d_{CA}[n,k]=\lim_{n\to\infty}\frac{1}{n}\log_2 W_A \tag{2.15}$$

2．5 Goppa 码

本世纪 70 年代初俄国学者 Goppa 系统地构造出了一类有理分式码：Goppa 码。Goppa 码的最主要优点是它的某些子类能达到 Shannon 信道编码定理所给出的性能，并且有快速译码算法。特别是它的不等价码类数目很大，因此在 1978 年 McEliece 用 Goppa 码构造了一类公钥密码体制，自此开始了用纠错码构造密码体制及各种认证码。因此无论在实际中还是在理论中，也无论是在差错控制系统还是在密码中，Goppa 码都具有重要意义。

定义 2.3[32] 设 $0<n\le q^m$（q 为素数或素数幂，$m>0$ 的整数），$L=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 是一个有序集合，$\alpha_i \in GF(q^m)$，且对任何 $i\neq j$ 恒有 $\alpha_i \neq \alpha_j$，$i、j \le n$。又设 $GF(q)$上的 n 维线性空间为 V_n，且矢量 $C=(c_1, c_2, \ldots, c_n)\in V_n$，则与 C 对应的 $GF(q^m)$上的 z 的有理分式表示是

$$R_c(z)=\sum_{i=1}^{n}\frac{c_i}{z-\alpha_i} \tag{2.16}$$

又设 $g(z)$是系数在 $GF(q^m)$上的 z 多项式，它的根不在 L 中，则以下 n 重矢量集合

$$\{C \mid R_C(z)\equiv 0 \ (\mathrm{mod}\ g(z)),\quad C\in V_n\} \tag{2.17}$$

或等价地说由 $g(z)$生成的多项式环中使 $R_C(z)\equiv 0(\mathrm{mod}\ g(z))$的多项式集合 $\{R_C(z)\}$，称为由 $g(z)$生成的 Goppa 码，称 $g(z)$是码的生成多项式或 Goppa 多项式。若 $g(z)$在 $GF(q^m)$上既约，则称为既约 Goppa 码。

由 Goppa 码的定义可知：

$$R_c(z)=\sum_{i=0}^{n-1}\frac{c_i}{(z-\alpha_i)}\equiv 0 \quad (\mathrm{mod}\ g(z)) \tag{2.18}$$

该式可写成

$$\left[\frac{1}{z-\alpha_0}\ \frac{1}{z-\alpha_1}\cdots\frac{1}{z-\alpha_{n-1}}\right]\begin{bmatrix}c_0\\ c_1\\ \vdots\\ c_{n-1}\end{bmatrix}=H_1C^T\equiv 0 \quad (\mathrm{mod}\ g(z)) \tag{2.19}$$

其中

$$H_1=\left[\frac{1}{z-\alpha_0}\ \frac{1}{z-\alpha_1}\cdots\frac{1}{z-\alpha_{n-1}}\right]$$

称为 Goppa 码的校验矩阵。我们可把 H_1 化成其它形式，为此把 H_1 矩阵中的每一个元素进行化简。

因为

$$\frac{g(z)}{z-\alpha_i} \equiv 0 \pmod{g(z)}$$

所以

$$\frac{-1}{z-\alpha_i} \equiv \frac{g(z)-g(\alpha_i)}{z-\alpha_i} g^{-1}(\alpha_i) \pmod{g(z)}$$

把 H_1 中的每个元素都用上式代入得

$$H_2 = \left[\frac{g(z)-g(\alpha_0)}{z-\alpha_0} g^{-1}(\alpha_0), \frac{g(z)-g(\alpha_1)}{z-\alpha_1} g^{-1}(\alpha_1), \cdots, \frac{g(z)-g(\alpha_{n-1})}{z-\alpha_{n-1}} g^{-1}(\alpha_{n-1}) \right] \quad (2.20)$$

若 $C(z)=c_{n-1}z^{n-1}+c_{n-2}z^{n-2}+\cdots+c_0$ 是由 $g(z)$生成的 Goppa 码的一个码字，则由 $H_2 \cdot C^T = 0$ 可知

$$\sum_{i=0}^{n-1} c_i \frac{g(z)-g(\alpha_i)}{z-\alpha_i} g^{-1}(\alpha_i) = 0$$

对式(2.20)进行化简后， 可把 H_2 矩阵写成以下形式：

$$H_2 = \begin{bmatrix} g_r & 0 & \cdots & 0 \\ g_{r-1} & g_r & \cdots & 0 \\ g_{r-2} & & g_r & 0 \\ \vdots & \vdots & & \vdots \\ g_1 & g_2 & \cdots & g_r \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & \cdots & \alpha_{n-1}^2 \\ \vdots & \vdots & & \vdots \\ \alpha_0^{r-1} & \alpha_1^{r-1} & \cdots & \alpha_{n-1}^{r-1} \end{bmatrix} \cdot \begin{bmatrix} g^{-1}(\alpha_0) & & & 0 \\ & g^{-1}(\alpha_1) & & \\ & & \ddots & \\ 0 & & & g^{-1}(\alpha_{n-1}) \end{bmatrix}$$
$$= A\alpha B \quad (2.21)$$

该式中的 A 矩阵最后可化为只有主对角线元素，而其它元素均为 0 的矩阵，因此它的存在与否不会影响码的纠错能力。 所以式(2.21)的 H_2 矩阵最后可化简为

$$H_3=\begin{bmatrix}1 & 1 & \cdots & 1\\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1}\\ \alpha_0^2 & \alpha_1^2 & \cdots & \alpha_{n-1}^2\\ \vdots & \vdots & & \vdots\\ \alpha_0^{r-1} & \alpha_1^{r-1} & \cdots & \alpha_{n-1}^{r-1}\end{bmatrix}\begin{bmatrix}g^{-1}(\alpha_0) & & & \\ & g^{-1}(\alpha_1) & & 0\\ & & \ddots & \\ 0 & & & g^{-1}(\alpha_{n-1})\end{bmatrix}=\alpha B$$

$$=\begin{bmatrix}g^{-1}(\alpha_0) & g^{-1}(\alpha_1) & \cdots & g^{-1}(\alpha_{n-1})\\ \alpha_0 g^{-1}(\alpha_0) & \alpha_1 g^{-1}(\alpha_1) & \cdots & \alpha_{n-1} g^{-1}(\alpha_{n-1})\\ \vdots & \vdots & & \vdots\\ \alpha_0^{r-1} g^{-1}(\alpha_0) & \alpha_0^{r-1} g^{-1}(\alpha_1) & \cdots & \alpha_{n-1}^{r-1} g^{-1}(\alpha_{n-1})\end{bmatrix}$$

(2.22)

显然在 α 矩阵中任意取出 r 列所组成的矩阵是一个范德蒙矩阵，其秩为 r。因此，只要 α_1，α_2，…，α_n 不相等且不为 0，则 α 矩阵的秩为 r，而 B 矩阵显然是一个满秩矩阵。由此可知，H_3 矩阵的秩为 r，即 H_3 矩阵中各行线性无关，且任意 r 列线性无关。满足 H_3 矩阵的 Goppa 码有最小距离为

$$d \geq r+1=\deg g(z)+1$$

定理 2.3[32] 由 r 次多项式 $g(z)$生成的 q 进制 Goppa 码，至多有 $\max(\deg g(z))$ 个校验位，有最小距离 $d \geq \deg g(z)+1$，其位置域 L 中的元素为 $\alpha_i \in GF(q^m)$，i=0，1，2，…，n-1。如果 $g(z)$的根不在 $GF(q^m)$中，则生成一个［q^m，$k \geq q^m-rm$，$d \geq r+1$］的既约 Goppa 码。

定理 2.4[32] 给定码率 $R>0$ 和任意小 $\varepsilon>0$，则码长 $n \to \infty$时，一定可以找到 $GF(q)$上的既约 Goppa 多项式 $g(z)$，由它生成的 Goppa 码满足以下关系：

$$\frac{d}{n}>\varphi^{-1}(1-R)-\varepsilon \tag{2.23}$$

其中

$$\varphi(x)=x\log_q(q-1)-x\log_q x-(1-x)\log_q(1-x)$$

第三章 基于纠错码的公钥密码体制

20 世纪 70 年代中期，W. Diffe 和 M. E. Hellman 发表了在密码学领域中具有里程碑意义的文章——《密码学的新方向》[4]，提出了新的密码思想，构造了许多不同的基于数学难题的公钥密码系统。1978 年 Berlekamp 等证明了一般线性分组码的译码问题是一个难解的数学问题[7]，从而为纠错码在密码中的应用打开了大门。同年，McEliece 利用 Goppa 码构造了第一个基于线性分组码的公钥密码体制[8]。

3．1 McEliece 公钥密码体制

McEliece 公钥密码体制，简称 M 公钥密码体制，是 McEliece 利用一般线性码的译码问题是一个 NPC 问题和 Goppa 码有快速译码算法的特点，最早提出的一个基于纠错码的公钥密码体制。该体制的公钥是随机产生的一个线性分组码的生成矩阵，公钥隐藏了线性分组码的快速译码算法，它是一种局部随机的密码体制。

3．1．1 M 公钥密码体制的加解密原理

设 G 是二元 $[n,k,d]$ Goppa 码的生成矩阵，这里 $n=2^m$，$d=2t+1$，$k=n-mt$。

设明文集合是 $GF(2)^k$，密文集合是 $GF(2)^n$。

密钥的产生

随机地选取有限域 $GF(2)$ 上的 $k\times k$ 阶可逆矩阵 S 和 $n\times n$ 阶置换矩阵 P，令 $G^{'}=SGP$，将 S，G，P 作为私钥，$G^{'}$ 作为公钥。

加密过程

对于任意一个明文 $m\in GF(2)^k$，将其加密成密文

$$c=mG^{'}+z \tag{3.1}$$

式中：z 是 $GF(2)^n$ 上重量为 t 随机向量。

解密过程

收方收到一个密文 c 以后，计算 $cP^{-1}=mSGPP^{-1}+zP^{-1}=mSG+z'$，因为 P 是置换矩阵，所以 $w(z)=w(z')=t$，然后利用 Goppa 的快速译码算法将其译码成 $m'=mS$，密文 c 对应的明文为 $m=m'S^{-1}$。

在 M 公钥密码体制中，一个明文对应可能的 C_n^t 个密文中的某一个。

3．1．2 M 公钥密码体制的安全性分析

M 公钥密码体制使用的是二元既约 Goppa 码，Goppa 码的数量随参数的增加而快速增加。对 M 公钥密码体制的攻击可以归结为下列问题：对于一个加密矩阵 G'，若存在一个 $k\times k$ 阶可逆矩阵 S，$n\times n$ 阶可逆矩阵 P，密码分析者知道其快速译码算法的码 c 的生成矩阵 G，且 $G'=SGP$。若这种情况发生，M 公钥密码体制就可被攻破，但这种情况发生的概率是很小的。下面给出 M 公钥密码体制的其它几种攻击方法：

1、已知码字的攻击[8,15]

密码分析者随机地选 n 比特密文中的 k 比特，k 比特没有错误的概率为 $p_k=\binom{n-t}{k}\Big/\binom{n}{k}$，与 $k\times n$ 阶矩阵 G' 相对应的 $k\times k$ 阶矩阵可逆的概率为 q_k，因此，任意取密文 c 的 k 比特，它既没有错误且对应的 $k\times k$ 阶子矩阵可逆的概率为 q_kp_k，求一个 $k\times k$ 阶可逆矩阵逆的时间复杂度为 $O(k^3)$，因此，这种攻击的工作因子为 $O(k^3/q_kp_k)$。这是 1978 年 McEliece 给出的一种攻击方法。

2、错误图样的攻击[14]

随机地选取 $k\times n$ 阶矩阵 G' 的 k 列 $j_1,j_2,\cdots,j_k$，且使其构成 $k\times k$ 阶可逆矩阵 G_k'，令 y_k，z_k 分别表示由 n 维矢量 y 和 z 的第 $j_1,j_2,\cdots,j_k$ 个分量构成的 k 维矢量，因此 $y_k+z_k=mG_k'$，$(y_k+z_k)(G_k')^{-1}G=mG$。取 k 比特码字 z_k'，z_k' 的汉明重量小于等于 $j(j\le c)$，若 $y+(y_k+z_k')(G_k')^{-1}G$ 的重量为 t，则 $z_k'=z_k$，因此明文 $m=(y_k+z_k')(G_k')^{-1}$，否则选另一个 k 维矢量 z_k'，重复上面的步骤。若重量小于等于 j 的 k 比特矢量被用完，但消息还未恢复出来，取 $k\times n$ 阶矩阵 G' 的另一个 $k\times k$ 阶子矩阵，重复上面的步骤，直到明文 m 被

发现为至。它是目前对M公钥密码体制攻击中最常用的方法。这是1988年Lee和Brickell给出的一种攻击方法，被称为Lee和Brickell攻击。随机选取密文的任意 k 比特，有 i 个错误的概率为 $P_i=\binom{t}{i}\binom{n-t}{k-i}\Big/\binom{n}{k}$。因此，任意选取密文的 k 比特，有小于等于 j 个错误的概率为 $\sum_{i=0}^{j}P_i$。重量小于等于 j 的 k 比特码字的个数为 $N_j=\sum_{i=0}^{j}\binom{k}{i}$ 令 $T_j=1/\sum_{i=0}^{j}P_i$。因此，Lee-Brick攻击的工作因子为 $O((\alpha k^3+\beta N_j k)T_j)$。

3、最小汉明重量的码字攻击[8]

设 $y=xG+z$ 是一个接收码字，这里 G 是 $[n,k,d]$ 线性码的生成矩阵，z 是重量为 t 的错误矢量，$(k+1)\times n$ 阶矩阵 G/z 是 $[n,k+1,t]$ 线性码的生成矩阵。因此，发现一个码的最小重量码字对应于发现错误矢量 z。若有算法能发现一个码的最小重量的码字，就可被用来攻击M公钥密码体制，但发现一个码的最小重量的码字是一个NPC问题，因此，通过这种方法攻击，也是很困难的。

4、消息重发攻击[22]

1997年，Berson提出两种对M公钥密码体制的攻击方法，即消息重发攻击和相关消息攻击。考查具有如下参数的M公钥密码体制，$n=1024$，$k=524$，$t=50$。假定消息 m 被加密两次，那么密码分析者知道 $c_1=mG'+e_1$，$c_2=mG'+e_2$，其中 $e_1\neq e_2$，称这种条件为消息重发条件。因此，$c_1+c_2=e_1+e_2$。注意到 e_1+e_2 的汉明重量最多为100，Berson通过分析得到，若满足消息重发条件，那么 e_1+e_2 的平均汉明重量为95.1，若消息不同，则 c_1+c_2 的平均汉明重量为512，通过分析 c_1+c_2 的重量，容易得到是否有消息重发条件发生。若 e_1+e_2 的汉明重量为94，这说 c_1 的其余930个位置中发生了三个错误，那么正确猜测这三个错误的概率为 $\binom{927}{524}\Big/\binom{930}{524}\approx 0.0828$，这意味着密码分析者大约通过12次猜测就能攻击成功。同理，若 e_1+e_2 的汉明重量为96，密码分析者大约通过5次猜测就能攻击成功。

5、相关消息攻击[22]

若两个消息m_1，m_2被加密，假定密码分析者知道m_1+m_2，那么密码分析者知道：$c_1=m_1G'+e_1$，$c_2=m_2G'+e_2$，这里$m_1\neq m_2$，$e_1\neq e_2$。因此，$c_1+c_2=m_1G'+e_1+m_2G'+e_2=(m_1+m_2)G'+e_1+e_2$。由于预先知道$m_1+m_2$，可计算$(m_1+m_2)G'$，因此，$c_1+c_2+(m_1+m_2)G'=e_1+e_2$，类似于消息重发攻击，仅需要次数比较少的猜测就能攻击成功。消息重发攻击可看成相关消息攻击的特例。

M 公钥密码体制加密、解密算法简单、而且安全性高。当然，M 公钥密码体制也存在一些弱点，其中最大的不足是需要存储的密钥量大、信息率比较低。

3．2 Niederreiter 公钥密码体制

Niederreiter 公钥密码体制，简称 N 公钥密码体制，是 Niederreiter 提出的一个基于纠错码的公钥密码体制[11]，该体制是一个背包型公钥密码体制。N 公钥密码体制的公钥为随机产生的线性分组码的校验矩阵，与 M 公钥密码体制不同的是 N 公钥密码体制隐藏了具有快速译码算法的线性分组码的校验矩阵。

3．2．1 N 公钥密码体制的加解密原理

设c是有限域$GF(q)$上线性$[n,k,2t+1]$Goppa 码，H是码 c 的$(n-k)\times n$阶校验矩阵，M是有限域$GF(q)$上的一个$(n-k)\times(n-k)$阶非奇异矩阵，P是有限域$GF(q)$上的一个$n\times n$阶置换矩阵。

私钥 H，M，P

公钥 $H'=MHP$，t

明文 有限域$GF(q)$上重量为 t 的 n 维向量 y

加密算法 $z=yH^T$ (这里 z 是一个 $n-k$ 维向量)　　(3.2)

解密算法 由$z=y(MHP)^T$知：$z(M^T)^{-1}=y(P^T)H^T$，由码的快速译码算法得到yP^T，因此可以求出y。

3．2．2 N 公钥密码体制的安全性分析

显然，若能从公钥 H' 中恰好分解出密钥 H，M，P，则 N 公钥密码体制就被攻破。但这种攻击方法是一个 NPC 问题，在计算上是不可行的。除了上述攻击方法外，还能从解线性方程组的方法攻击 N 公钥密码体制，方法如下：

设某一给定的密文 z 对应的明文 $y=(y_1,y_2,\cdots y_n)$，令 $S_1=\{i:y_i=1,1\le i\le n\}$，$S_2=\{i:y_i=0,1\le i\le n\}$。设公钥为 $H'=[H_1',H_2',\cdots H_n']$，这里 H_i' 是 H' 中第 i 列，则：$z=yH'^T=\sum_{i=1}^{n}y_iH_i'^T=\sum_{i\in S_1}H_i'^T$。设密码分析者在 y 中任意选择 k 个分量，且这 k 个分量的位置集合为 S_3，然后在 y 中删除位置属于 S_3 的 k 个分量，则剩下 $n-k$ 个分量 $y_{i_1},y_{i_2},\cdots y_{i_{n-k}}$，并得到 $z^*=\sum_{j=1}^{n-k}y_{i_j}H_{i_j}'^T$。若 $S_3\subset S_2$，则 $z^*=z$，即 $z=(y_{i_1},y_{i_2},\cdots y_{i_{n-k}})\cdot[H_{i_1}',H_{i_2}',\cdots H_{i_{n-k}}']$。若矩阵 $[H_{i_1}',H_{i_2}',\cdots H_{i_{n-k}}']$ 可逆，则：$(y_{i_1},y_{i_2},\cdots y_{i_{n-k}})=z([H_{i_1}',H_{i_2}',\cdots H_{i_{n-k}}'])^{-1}$。从而密码分析者在已知 z 及 H' 后，通过解方程就可求得 $(y_{i_1},y_{i_2},\cdots y_{i_{n-k}})$，因为 y 中另外 k 个分量都为零，故从 $(y_{i_1},y_{i_2},\cdots y_{i_{n-k}})$ 中相应的位置中添加 k 个零，即可解得 y，解方程的工作因子至多为 $(n-k)^3$，而在 y 中任意选取 k 个位置，并使它们全部属于 S_2 的概率应为 $P=\binom{n-t}{k}\Big/\binom{n}{k}$，因此采用这种方法攻击 N 公钥密码体制的工作因子为 $(n-k)^3\binom{n}{k}\Big/\binom{n-t}{k}$。

3．3 M 公钥密码体制与 N 公钥密码体制

3．3．1 M 公钥密码体制和 N 公钥密码体制的关系

假定 M 公钥密码体制和 N 公钥密码体制采用的是相同的$[n,k,2t+1]$线性码 c，令码码 c 的生成矩阵是 G，校验矩阵是 H。同时假定 M 密码体制的另两个私钥为 $k\times k$ 阶可逆矩阵 S_1，和 $n\times n$ 阶置换矩阵 P，N 公钥密码体制另两个私钥为 $(n-k)\times(n-k)$ 阶可逆矩阵 S_2 和 $n\times n$ 阶置换矩阵 P。因此，M 公钥密码体制的公钥为 $G^{'}=S_1GP$，N 公钥密码体制的公钥为 $H^{'}=S_2HP$。

给定 M 公钥密码体制的公钥 $G^{'}$ 和加密方程 $c=mG^{'}+e$，给方程两端乘 $H^{'T}$ 得到 $z=cH^{'T}=mG^{'}H^{'T}+eH^{'T}=eH^{'T}$。给定 z 和 $H^{'}$，若 e 能够被发现，也就是说若 N 公钥密码体制被打破，则 M 公钥密码体制被打破，即密文 m 可以在多项式时间内被获得。因此，破译 M 公钥密码体制不会比破译 N 公钥密码体制难。

给定 N 公钥密码体制中的公钥 $H^{'}$ 和加密方程 $z=yH^{'T}$，则在多项式时间内可以求得一个 n 长码字 c，使得 $z=cH^{'T}$，因为 c 可以表示成为 $c=mG^{'}+y$，其中 m 是一个 k 维向量，因此，若 M 公钥密码体制被打破，即由 c 能解密得到 m，也就可得到 y，那么，N 公钥密码体制被打破。

因此，从这个角度看，M 公钥密码体制与 N 公钥密码体制是等价的[46]。

表 3.1 列出 M 公钥密码体制和 N 公钥密码体制的有关特点。

表 3.1 M 公钥密码体制和 N 公钥密码体制的特点

	M 公钥 [1024，524，101]二元码	N 公钥 [1024，524，101]二元码
公钥体积	67072byte	32750byte
每次加密传送的信息比特数	512	276
传输率	51.17%	56.81%
加密每信息比特需要的二元运算数	514	50
解密每信息比特需要的二元运算数	5140	7863

3．3．2 M 公钥密码体制和 N 公钥密码体制的参数优化和性能比较

由于 M 公钥密码体制和 N 公钥密码体制等价，因此对它们的分析可以互相转化。若两类公钥密码体制均选取的是$[n,k,t]$既约 Goppa 码，若用解线性方程组去分别攻击两类体制，设 W_1 是 M 公钥密码体制的工作因子，W_2 是 N 公钥密码体制的工作因子，则两类体制具有的安全性指标为 $\min\{W_1,W_2\}$。表 3.2 给出当 $n=1024$，$k=1024-10t$，$t\in[19,65]$时，两类体制的工作因子，公钥量及信息速率随 t 的变化情况。

表 3.2 工作因子、公钥量及信息速率随 t 的变化

t	19	29	37	41	51	65
$W_1(\log_2)$	76.4	82.9	84.1	83.7	80.2	70
$W_2(\log_2)$	70.0	78.8	81.6	82	80.2	72.4
M 公钥公钥量(千比特)	854	752	670	629	526	383
N 公钥公钥量(千比特)	195	297	379	420	522	666
M 公钥信息速率	0.81	0.76	0.64	0.60	0.50	0.37
N 公钥信息速率	0.7	0.67	0.61	0.59	0.57	0.53

当 $t=37$ 时，W_1 取最大值，$W_1\approx 2^{84.1}$，而 $W_2\approx 2^{81.6}$；当 $t=41$ 时，W_2 取最大值，$W_2\approx 2^{82}$，而 $W_1\approx 2^{83.7}$。由此可知，当 $t=41$ 时，两类体制具有最高的安全性，最高工作因子为 $W=\min\{W_1,W_2\}\approx 2^{82}$。

3．4 M 公钥密码体制的推广及性能分析

3．4．1 M_s 公钥密码体制及其性能分析

在分析 M 公钥密码体制的安全性时，都没有考虑有扰信道的情况，而是认为密文通过信道时没有干扰。但是在实际情况中，无论在点对点的通信中还是在计算机网通信和

卫星通信中，信道都是有扰的。密文在这些有扰信道中传输时，毫无例外地都要受到不同程度的干扰，从而引起收端不能正确解密。因此，在 M 公钥进行推广的基础上，王新梅提出了加密与纠错相结合的 M_s 公钥密码体制[42]。

设明文为 m，则对应的密文为

$$c_s = mG_s + e_s \tag{3.3}$$

式中 $G_s = SGP$ 与 M 公钥密码体制相同，$e_s \neq e$ 是一个长为 n 的二进制随机序列，且它的重量为

$$w(e_s) = t_s < t \tag{3.4}$$

显然，除了在加密运算中用 e_s 代替 M 公钥密码体制中的 e 外，其余的都与 M 公钥密码体制相同。当 $t_s = t$ 时，M_s 公钥密码体制就是 M 公钥密码体制。因此，M 公钥密码体制可以看成 M_s 公钥密码体制的特殊情况，M_s 公钥密码体制可以看成 M 公钥密码体制的推广。

M_s 公钥密码体制解密算法与 M 公钥密码体制基本相同。所不同的是，当密文在有扰信道中传输时，若信道产生的错误图样 e 的重量 $w(e_s) \le t - t_s$，M_s 公钥密码体制能保证解密后所得明文的正确性，而 M 公钥密码体制不具有这个性能。

3．4．2 修正的 M 公钥密码体制及其性能分析

Korzhik 和 Turkin 声称他们找到了一般线性码的快速译码算法，该算法可在多项式时间内纠正 $t \le \left[\frac{d-1}{2}\right]$ 个错。这一结论与一般线性码的最小距离译码是 NPC 问题并不矛盾。利用这一译码算法破译 M 公钥密码体制是十分有效的，称之为 KT 攻击。

通过对 M 公钥密码体制进行适当修正，可以在仍用汉明距离码的条件下，使修正后的体制也能有效地抗击 KT 攻击[50]。

设 G_g 是 $GF(2)$ 上具有快速译码算法的某 $[n,k,d]$ 线性码的生成矩阵，B 是 $GF(2)$ 上 $k \times n$ 阶矩阵，它的每一列至多有一个非零元素，且非零元素总数 $(2b)$ 小于 d，建立公钥

$$G^* = [SG_g + B]P = SG_gP + BP \tag{3.5}$$

保存密钥G_g，S，P和B，这里S与P的定义同M公钥密码体制，B的选择相当于在对应非零位上加$2b$个错。显然，当B为全零矩阵时，该体制就是M公钥密码体制。对应k比特明文m的n比特密文c为

$$c = mG^* + e = m(SG_gP + BP) + e \tag{3.6}$$

这里e是汉明重量$\le t-b$的n维随机向量。由于持有密钥的用户知道B中非零元素的位置，对于收到的密文c，可利用纠错纠删译码算法，至多二次译码就能得到真正明文。

由式(3.5)知道，当G_g是Goppa码的生成矩阵时，G^*不再是某个Goppa码(或与Goppa码等价的线性码)的生成矩阵，因此寻找等价Goppa码解密陷门的攻击方法对该方案是无效的。当$w(e) \le t-2b$时，式(3.6)所表示的密文相当于G_g生成的线性码的某个码字发生总数不大于t的错误，因此KT攻击可起作用。为抗击KT攻击，只需规定错误矢量e的重量满足$t-2b < w(e) \le t-b$。

3．4．3 变型的M公钥密码体制及其性能分析

为了抗击Berson攻击，将M公钥密码体制进行变型[26]：

变型1

加密　$c = (m + h(e))G' + e$　式中：e是重量为t的n比特随机向量；h是输入为n比特输出为k比特的单向Hash函数。

解密　由M公钥密码体制的解密算法可得$m + h(e)$，然后计算$m = (m + h(e)) + h(e)$

安全性　设m_1和m_2是两个消息，$m_1 = m_2$，则$c_1 + c_2 = (h(e_1) + h(e_2))G' + e_1 + e_2$。由于$h(e_1), h(e_2)$不知道，因此$(h(e_1) + h(e_2))G'$也是不知道的，密码分析者很难确定出错误位置，消息重发攻击不会成功。假定密码分析者知道$m_1 + m_2$的值，那么

$c_1 + c_2 = (m_1 + m_2 + h(e_1) + h(e_2))G' + e_1 + e_2$。虽然密码分析者知道$m_1 + m_2$的值，但$h(e_1), h(e_2)$不知道，因此$(m_1 + m_2 + h(e_1) + h(e_2))G'$也是不知道的，密码分析者很难确定错误位置，相关消息攻击也不能成功。

变型2

加密 $c=f(m,e)G'+e$ 式中：e 是重量为 t 的 n 比特随机向量；f 是一个单向函数，且满足给定 $f(m,e)$，确定 m，e 在计算上是不可行的。但在知道 $f(m,e)$，e 时，很容易计算 m。

解密 首先利用 M 公钥密码体制的解密算法求得 $f(m,e)$，e，然后利用 $f(m,e)$，e，求得 m。

安全性 设 $m_1=m_2$，则 $c_1+c_2=(f(m_1,e_1)+f(m_2,e_2))G'+e_1+e_2$。由于不知道 $f(m_1,e_1)$和$f(m_2,e_2)$，因此 $f(m_1,e_1)+f(m_2,e_2))G'$ 也是不知道的，密码分析者很难确定出错误位置，消息重发攻击不会成功。假定密码分析者知道 m_1+m_2 的值，那么 $c_1+c_2=(f(m_1,e_1)+f(m_2,e_2))G'+e_1+e_2$。虽然密码分析者知道 m_1+m_2 的值，但 $f(m_1,e_1)$和$f(m_2,e_2)$不知道，因此 $f(m_1,e_1)+f(m_2,e_2))G'$ 也是不知道的，密码分析者很难确定错误位置，相关消息攻击也不能成功。

3．4．4 改善 M 公钥密码体制弱点的变型

M公钥密码体制加密、解密算法简单、而且安全性高。当然，也存在一些弱点，其中最大的不足是需要存储的密钥量 $k\times n$ bit很大、信息速率 $R=k/n$ bit/s比较低。

1）增加M公钥的信息率

变型 I [12]

加密 设消息 $m=(m_a,m_b)$，密文 $c=m_aG'+e$，这里 $e=g(m_b)$，g是一个将 m_b 映射到重量为t的n比特错误向量的可逆映射。

解密 m_a 可以通过M公钥密码体制的解密算法得到，同时也就得到了 $g(m_b)$，那么 $m_b=g^{-1}g(m_b)$。

信息率 该方法的本质在于充分利用了e的作用，也即不仅用e实现体制的安全性，而且还让e携带消息，理由是发收双方都知道每次加密时所选用的e。因为可能的e共有 $\binom{n}{t}$，所

以每个e均可携带$\left[\log_2\binom{n}{t}\right]$比特的消息。这里[x]表示取不大于x的最大正整数。已有快速算法可用于完成$\left[\log_2\binom{n}{t}\right]$比特向量与$e$间的转换，这时体制总的速率：

$$R=(k+\left[\log_2\binom{n}{t}\right])/n \text{ bit/s。} \tag{3.7}$$

安全性 变型后的M公钥密码体制的思想与M公钥密码体制的思想基本相同，其主要差距是错误向量的随机性问题。变型后的M公钥密码体制的错误向量不是真正随机的，它由m_b确定，这是一种确定性加密。

设$m_1=(m_{1a},m_{1b})$，$m_2=(m_{2a},m_{2b})$是两个要加密的消息，变型后的M公钥将消息分成两部分，因此它暴露出如表3.3所示的可能的弱点。

表3.3 变型Ⅰ可能的弱点

	预先知道的信息	信息泄漏
1	m_{1a}或m_{2a}	m_{1b}或m_{2b}
2	m_{1b}或m_{2b}	m_{1a}或m_{2a}
3	$m_{1a}=m_{2a}$，$m_{1b}=m_{2b}$	无
4	$m_{1a}=m_{2a}$，$m_{1b}\neq m_{2b}$	m_{1a}，m_{1b}，m_{2a}，m_{2b}
5	$m_{1a}\neq m_{2a}$，$m_{1b}=m_{2b}$	$m_{1a}+m_{2a}$
6	$m_{1a}+m_{2a}$，$m_{1b}=m_{2b}$	无
7	$m_{1a}+m_{2a}$，$m_{1b}\neq m_{2b}$	m_{1a}，m_{1b}，m_{2a}，m_{2b}

从这里可以看出，变型后的方案还存在很多弱点，为了克服这些弱点，提高信息速率，给出了M公钥的另一种变型。

变型Ⅱ[26]

加密 设消息$m=(m_a,m_b)$，密文$c=(m_a+h(e))G'+e$，这里$e=g(r\|m_b)$，r是q比特随机向量，g是一个将m_b映射到重量为t的n比特错误向量的可逆映射，h是一个将e映射成k比特向量的单向Hash函数。

解密 首先通过M公钥密码体制的解密算法，可得到$m_a^{'}=m_a+h(e)$和错误向量e，其次接收方计算$r\|m_b=g^{-1}(e)$，去掉前q比特，可得到m_b，最后计算$m_a^{'}=m_a+h(e)$。

信息率 与变型I所不同的是，由于增加了q比特随机向量，因此，一个消息的传送由原先的n比特增加至了$n+q$比特，信息速率$R=(k+\left[\log_2\binom{n}{t}\right])/(n+q)$ bit/s。

安全性 设$m_1=(m_{1a},m_{1b})$，$m_2=(m_{2a},m_{2b})$是两个要加密的消息，变型后的M公钥将消息分成两部分，因此它暴露出如表3.4和表3.5所示的可能的弱点。

表3.4 q=0时，变型II可能的弱点

	预先知道的信息	信息泄漏
1	m_{1a}或m_{2a}	无
2	m_{1b}或m_{2b}	m_{1a}或m_{2a}
3	$m_{1a}=m_{2a}$，$m_{1b}=m_{2b}$	无
4	$m_{1a}=m_{2a}$，$m_{1b}\neq m_{2b}$	无
5	$m_{1a}\neq m_{2a}$，$m_{1b}=m_{2b}$	$m_{1a}+m_{2a}$
6	$m_{1a}+m_{2a}$，$m_{1b}=m_{2b}$	无
7	$m_{1a}+m_{2a}$，$m_{1b}\neq m_{2b}$	无

表 3.5 q=64 时，变型Ⅱ可能的弱点

	预先知道的信息	信息泄漏
1	m_{1a} 或 m_{2a}	无
2	m_{1b} 或 m_{2b}	无
3	$m_{1a}=m_{2a}$， $m_{1b}=m_{2b}$	无
4	$m_{1a}=m_{2a}$， $m_{1b}\neq m_{2b}$	无
5	$m_{1a}\neq m_{2a}$， $m_{1b}=m_{2b}$	无
6	$m_{1a}+m_{2a}$， $m_{1b}=m_{2b}$	无
7	$m_{1a}+m_{2a}$， $m_{1b}\neq m_{2b}$	无

2）降低M公钥密码体制公钥量

对 M 公钥密码体制，目前主要的一个任务就是降低它的公开密钥量，这是 M 公钥密码体制趋于实用化的一个十分值得研究的问题。

M 公钥密码体制的公开密钥量为 $k\times n$ 比特，目前有一种方法[15]能使公钥量降低至 $k\times(n-k)$ 比特。将公钥 G' 变型，密文 $c=mG'+z=mS^*\left[I_k \quad A\right]+z=\underline{w}\left[I_k \quad A\right]+z$。式中，$A$ 是一个 $k\times(n-k)$ 阶矩阵，S^* 是一个新的非奇异矩阵。解密明文 $m=\underline{w}S^{*-1}$。$n=1024$，$t=37$ 时，M 公钥密码体制的密钥量为 $670kbits$，通过该方法密钥量降低为 $379kbits$。

第四章 MATLAB 性能分析

4．1 MATLAB 介绍

MATLAB 是 MathWorks 美国公司开发的新一代科学计算软件；MATLAB 是英文 MATrix LABoratory(矩阵实验室)的缩写；MATLAB 是一个专门为科学计算而设计的可视化计算器。利用这个计算器中的简单命令，能快速完成其他高级语言只有通过复杂编程才能实现的数值计算和图形显示。

MATLAB 是一种既可交互使用又能解释执行的计算机语言。所谓交互使用，是指用户输入一条语句后立即就能得到该语句的计算结果，而无需像 C 语言那样首先编写源程序，然后对之进行编译、连接，才能最终形成可执行文件。

MATLAB 语言可以用直观的数学表达式来描述问题，从而避开繁琐的底层编程，并把有限的时间和精力更多地花在要解决的问题上，因此可大大提高工作效率。MATLAB 的编程语法与交互使用是一致的，因此交互使用时输入的代码能够很方便地转化为可重用的函数或过程。

MATLAB 是解决工程技术问题的计算平台。利用它能够轻松完成复杂的数值计算、数据分析、符号计算和数据可视化等任务。

随着自身的不断发展，功能越来越强大，应用也越来越广泛。与其他高级语言(例如 C)相比，MATLAB 语言具有以下 6 个显著特点。

(1) MATLAB 的基本数据类型是双精度的、无须定义的、下标从 1 开始的复数矩阵。

(2) MATLAB 有命令行操作(像一个高级计算器)和编程执行两种使用方法，分别适用于简单的草稿式计算和复杂的应用开发。

(3) 绝大多数 MATLAB 函数的输入输出参数个数都是可变的，调用函数时输入输出参数的个数不同，函数完成的功能会有一定的差异。

(4) MATLAB 操作界面友好，编程语言简练，算法高效准确，图形显示和数据可视化功能强大。

(5) MATLAB 的帮助系统非常完善。

(6) MATLAB 采用开放性结构设计。

4．2 M 公钥密码体制的性能数值计算分析

根据 3.1.2 节中所提及的 McEliece 的攻击方法，也称解线性方程组攻击方法，Adams and Meijer 通过大量的研究，设 $q_k=1$，即 $k\times k$ 阶子矩阵可逆的概率为 1，$p_k=\binom{n-t}{k}\Big/\binom{n}{k}$，$n=1024$，给出了最大工作因子 $W=k^3/p_k=k^3\cdot\binom{n}{k}\Big/\binom{n-t}{k}$ 时，t 的值，即 t=37。此时 M 公钥密码体制有最高的安全性，$W\approx 2^{84.1}$。即使在 t=50 时，仍有很高的安全性，$W\approx 2^{80.7}$。

图 4.1 给出了当 $n=1024$ 时，工作因子 W 与 t 的 MATLAB 曲线图。

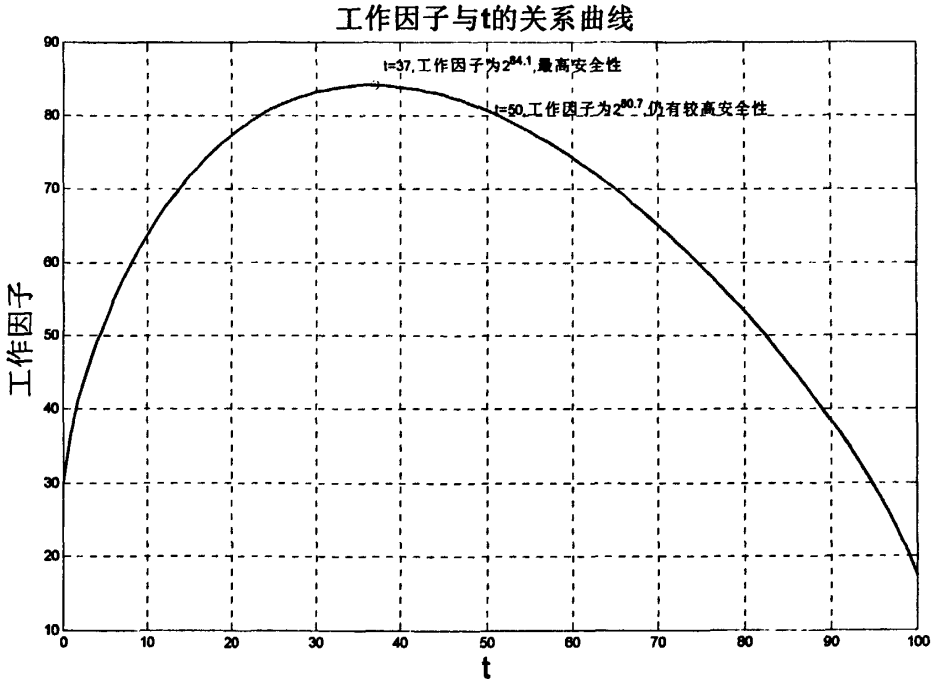

图 4.1 W~t 关系曲线($n=1024$)

图 4.2 给出了，当 $n=1024$，t=37 时，W 与 $w(z)$ 间的 MATLAB 曲线图。这时，$w(z)\le t$，$W=k^3\cdot\binom{n}{k}\Big/\binom{n-w(z)}{k}$。

由计算结果表明，当 $w(z)\in[22,28]$，$W>2^{60}$，当 $w(z)\in[28,37]$，$W>2^{70}$。

综合图 4.1 和图 4.2 的结果可知，当随机向量 z 的汉明重量 $w(z)\in[28,37]$ 时，M 公钥密码体制已有足够的安全性。当 $w(z)=37$ 时，体制达到最高安全性，即 $W\approx 2^{84.1}$。这也表明，M 公钥密码体制中的 z 的汉明重量 $w(z)$ 可以取小于 t(即码的纠错能力)，这就是 M_S 公钥密码体制，使之具有纠错能力的理论保证。

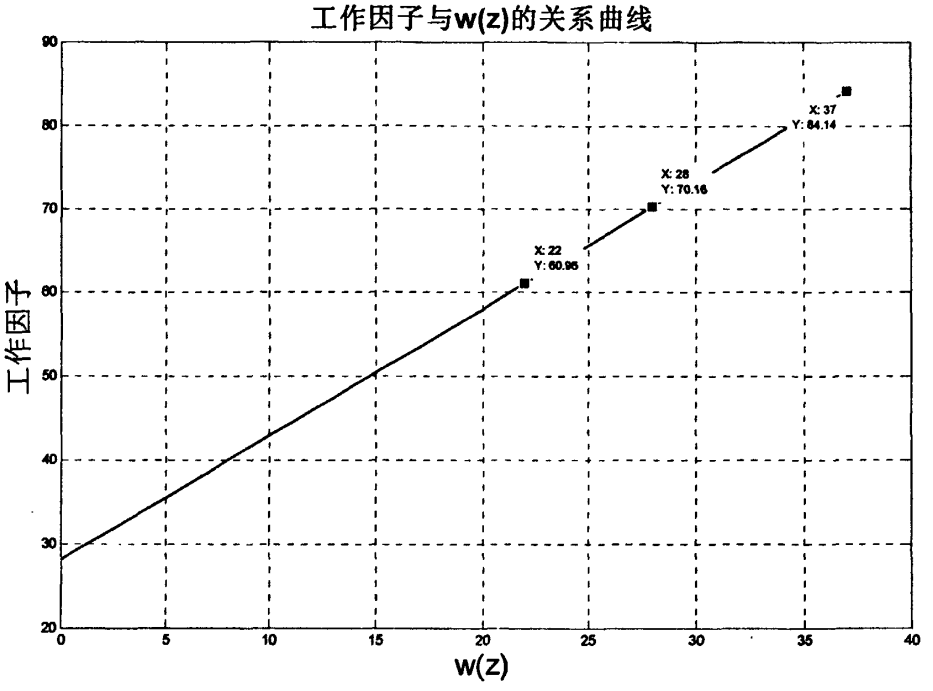

图 4.2 W~W(z)关系曲线(n=1024,t=37)

目前最有效最常用的攻击方法是 Lee-Brickell 攻击，3.1.2 节中列出了该攻击的工作因子 $W_j=(\alpha k^3+\beta N_j k)T_j$，式中：$P_i=\binom{t}{i}\binom{n-t}{k-i}\Big/\binom{n}{k}$，$T_j=1/\sum_{i=0}^{j}P_i$，$N_j=\sum_{i=0}^{j}\binom{k}{i}$。注意到，$W_0$ 就是 Adams and Meijer 所提出的 McEliece 攻击工作因子。对于任一合理变量 α 和 β，随着 j 的增加，W_j 先减小，而后增加。由于 $\alpha=\beta$，我们能够求得使 W_j 最小时，j 的最佳值为 2。由于 $\alpha=\beta=1$，Lee-Brickell 攻击的最小工作因子 W_2 比 W_0 下降 2^{11}。因此，当 $n=1024$，t=38 时，W_2 最大，$W_2\approx 2^{73.4}$，M 公钥密码体制具有最高的安全性。

图 4.3 给出了当 $n=1024$ 时，工作因子 W 与 t 的 MATLAB 曲线图。

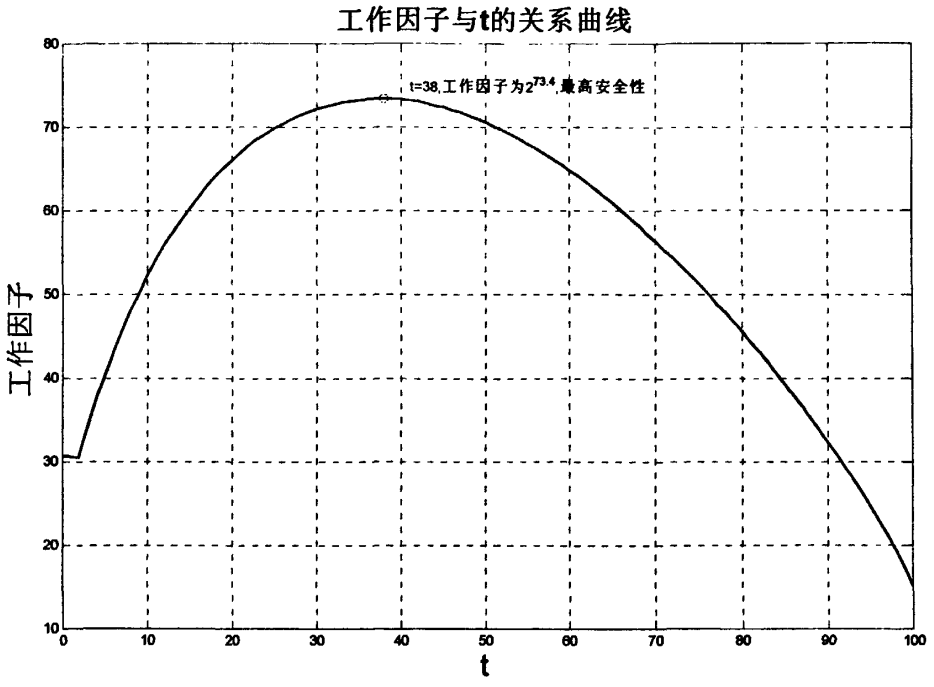

图 4.3 W~t 关系曲线($n=1024$)

由图 4.1 可知，对于 McEliece 所提出的的解线性方程组攻击方法，当$t\in[9,74]$，$W>2^{60}$，而当$t\in[14,65]$时，$W>2^{70}$。若考虑 Lee-Brickell 的攻击算法，该算法能使解线性方程组攻击方法工作因子下降2^{11}，即使如此，则当$t\in[14,65]$，M 公钥密码体制的工作因子大于2^{60}，可以认为 M 公钥密码体制已有足够的安全性。

4．3 M 公钥密码体制与 N 公钥密码体制性能比较数值计算分析

由 3.3 节，我们已经得出 M 公钥密码体制与 N 公钥密码体制两者之间的关系，在此，利用计算机 MATLAB 软件，得出两者性能曲线，使我们能够对它们有更加直观的认识。

首先，用解线性方程组攻击这两类体制，对于它们的安全性进行模拟数值计算分析。图 4.4 和图 4.5 分别是，M 公钥密码体制的工作因子曲线和 N 公钥密码体制的工作因子曲线。

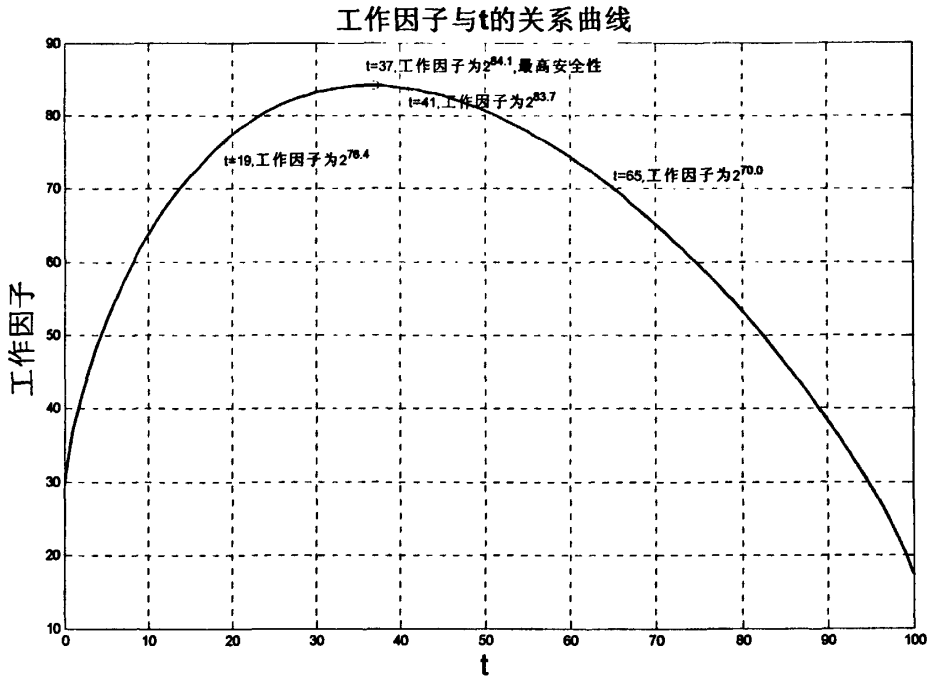

图 4.4 M 公钥密码体制工作因子与 t 的关系曲线(解线性方程组攻击)

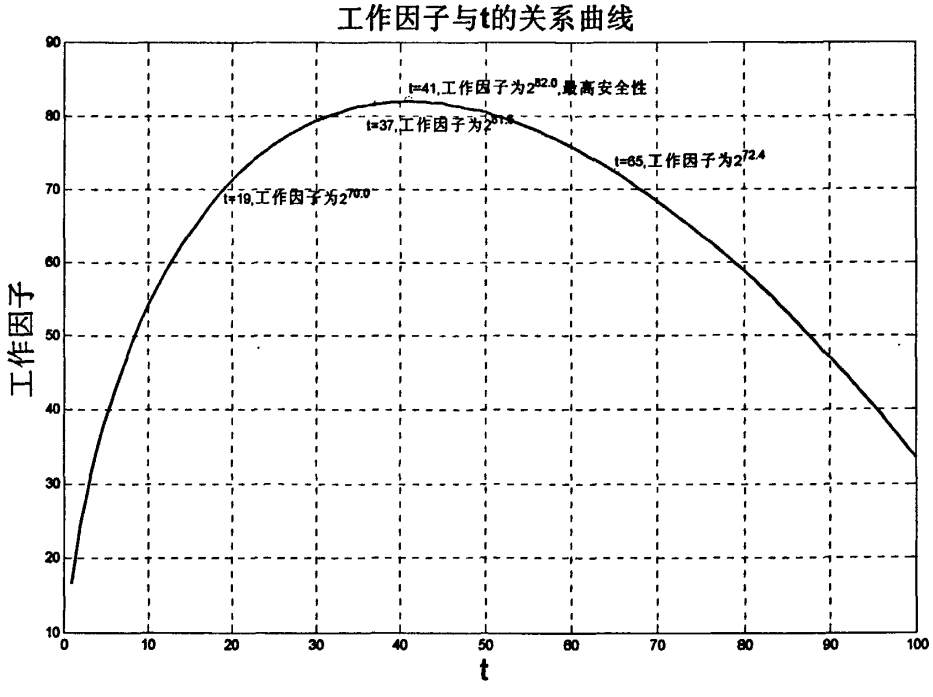

图 4.5 N 公钥密码体制工作因子与 t 的关系曲线(解线性方程组攻击)

通过图 4.4 和图 4.5，我们可以知道，当$t=37$时，W_1取最大值，$W_1\approx 2^{84.1}$，而$W_2\approx 2^{81.6}$；当$t=41$时，W_2取最大值，$W_2\approx 2^{82}$，而$W_1\approx 2^{83.7}$。由此可知，当$t=41$时，两类体制具有最高的安全性，最高工作因子为$W=\min\{W_1,W_2\}\approx 2^{82}$。

当$t\in[19,65]$时，W_1与W_2均大于2^{70}。若考虑对体制的 Lee-Brickell 攻击算法，则建议在实际应用中两类密码体制的$t\in[19,65]$，此时，即使在 Lee-Brickell 攻击算法下，体制也有很高的安全性。

图 4.6 给出了当$n=1024$，t=41 时，N 密码公钥体制 W 与 $w(y)$ 间的 MATLAB 曲线图。这时，$w(y)\le t$，$W=(n-k)^3\cdot\binom{n}{k}\Big/\binom{n-w(y)}{k}$。

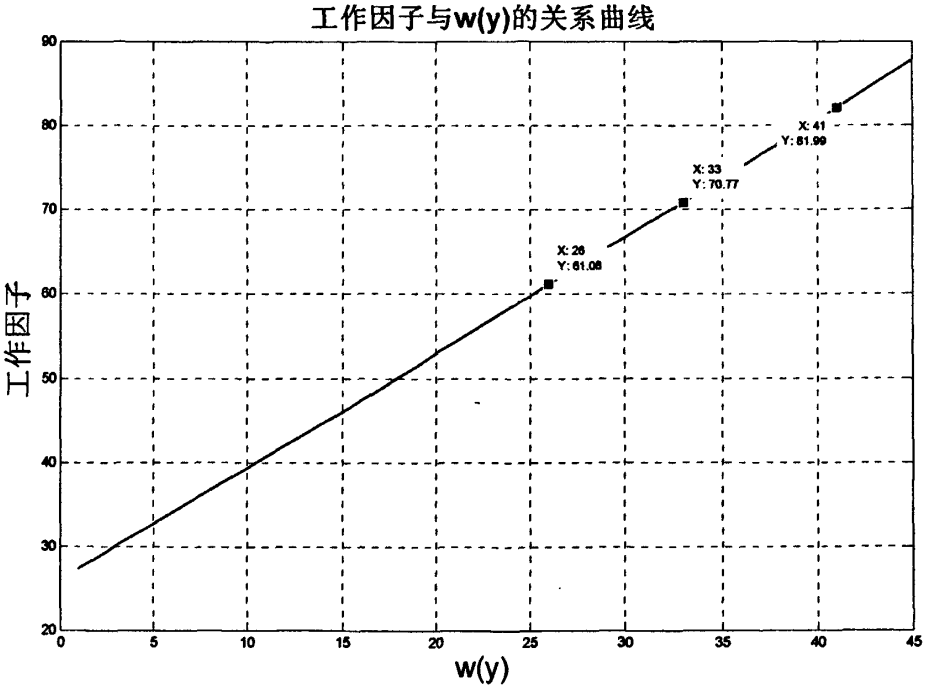

图 4.6 W~$W(y)$关系曲线(n=1024,t=41)

数值计算结果表明，当$w(y)\in[26,41]$时，$W>2^{60}$。而当$w(y)\in[33,41]$时，$W>2^{70}$。说明N密码公钥体制有足够的安全性。

由于目前最有效最常用的攻击方法是Lee-Brickell攻击，因此，对Lee-Brickell攻击两类体制的安全性也进行数值计算分析。由上一节分析可知Lee-Brickell攻击M公钥密码体制的

工作因子为$W_j=(\alpha k^3+\beta N_j k)T_j$。式中：$\alpha=\beta=1$，$P_i=\binom{t}{i}\binom{n-t}{k-i}\Big/\binom{n}{k}$，$T_j=1/\sum_{i=0}^{j}P_i$，$N_j=\sum_{i=0}^{j}\binom{k}{i}$。由此，同理可得出，Lee-Brickell攻击N公钥密码体制的工作因子为$W_j=(\alpha(n-k)^3+\beta N_j(n-k))T_j$。式中：$\alpha=\beta=1$，$P_i=\binom{t}{i}\binom{n-t}{k-i}\Big/\binom{n}{k}$，$T_j=1/\sum_{i=0}^{j}P_i$，$N_j=\sum_{i=0}^{j}\binom{k}{i}$。为使$W_j$最小，$j$的最佳值为2。

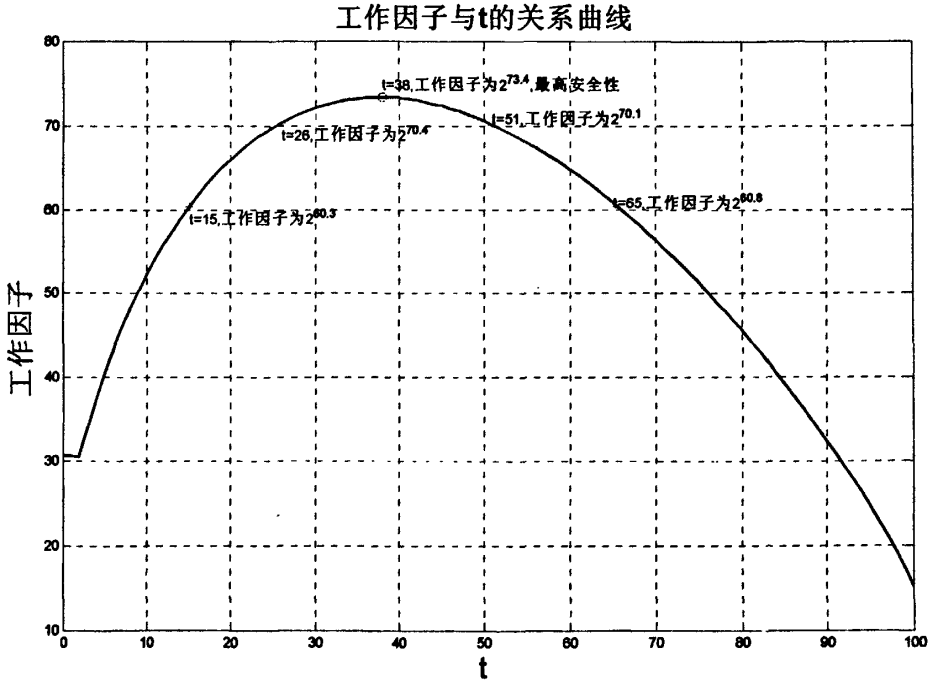

图4.7 M公钥密码体制工作因子与t的关系曲线(Lee-Brickell攻击)

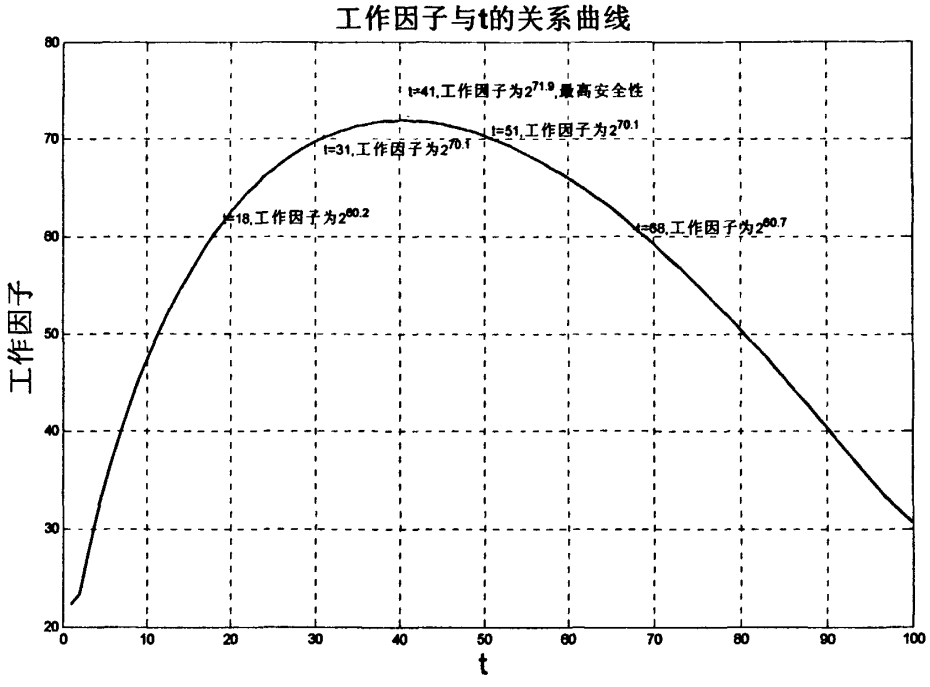

图4.8 N公钥密码体制工作因子与t的关系曲线(Lee-Brickell攻击)

综合图4.7和图4.8，建议两类公钥密码体制的t取值[18,65]，这时，即使在Lee-Brickell攻击下，两类公钥密码体制仍有2^{60}以上的安全性。

4．4 M公钥密码体制与M_S公钥密码体制性能比较数值计算分析

M公钥密码体制可以看成M_S公钥密码体制的特殊情况，M_S公钥密码体制可以看成是M公钥密码体制的推广。当$t_s = t$时，M_S公钥密码体制就是M公钥密码体制。

采用解线性方程组攻击法来比较分析这两类体制的性能。计算机数值计算结果如下图4.9如示。

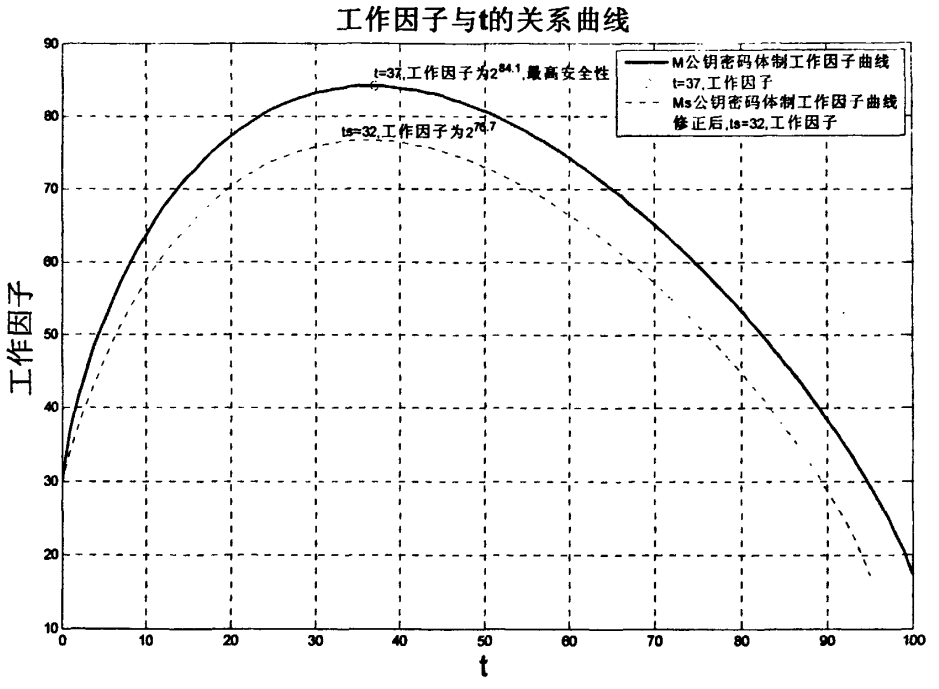

图4.9 M体制和M_S体制工作因子与t的关系曲线(解线性方程组攻击)

若以n=1024，k=644，t=37的M公钥密码体制为例来进行分析，假设信道产生错误图样的重量$w(e)\le 5$，则取$t_s=32$时构造M_S公钥密码体制。由图4.9中，可以看出，此时，攻击M_S公钥密码体制的工作因子有所下降，即为$2^{76.7}>2^{60}$，所以，验证了M_S公钥密码体制同样具有足够的安全性。

同样，对两类体制均采用Lee-Brickell攻击，运用MATLAB数值计算，得到攻击这两类体制的工作因子曲线图，见图4.10。

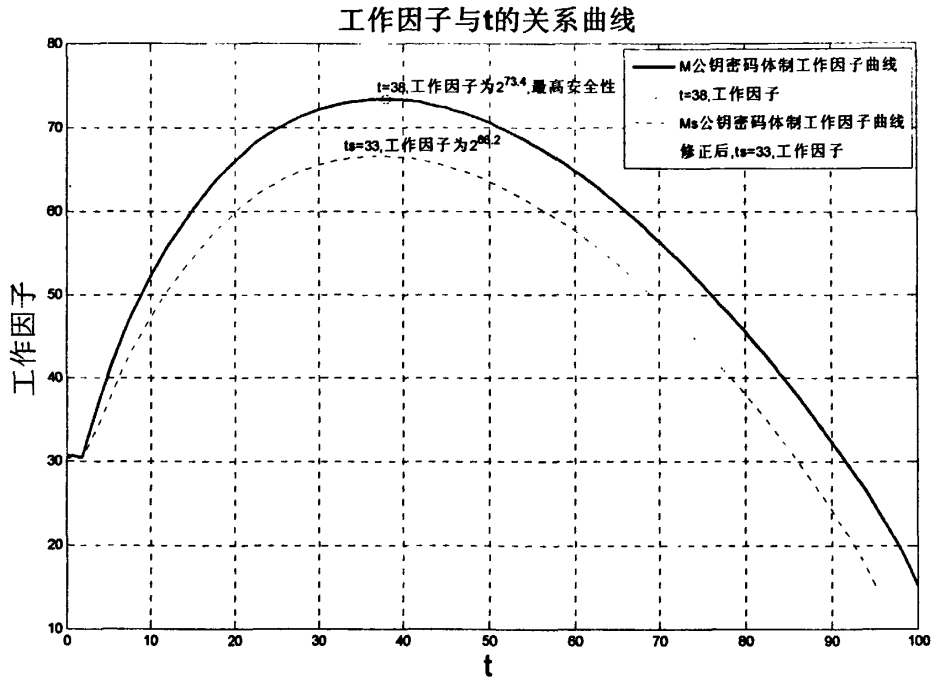

图4.10 M体制和M_S体制工作因子与t的关系曲线(Lee-Brickell攻击)

若以n=1024，k=644，t=38的M公钥密码体制为例来进行分析，假设信道产生错误图样的重量$w(e)\le 5$，则取$t_s=33$时构造M_S公钥密码体制。由图4.10中，可以看出，此时，攻击M_S公钥密码体制的工作因子有所下降，即为$2^{66.2}$，但即便如此，工作因子仍是$>2^{60}$，所以，M_S公钥密码体制仍有足够的安全性。

4．5 信息速率数值计算分析

M公钥密码体制的信息速率$R=k/n$ bit/s，就等于Goppa码的码率。

t	19	29	37	41	50	65
M 公钥信息速率	0.81	0.76	0.64	0.60	0.50	0.37

其实，M公钥密码体制的信息速率还可进一步提高。在3.3.4节中，给出了提高M公钥密码体制信息率的好方法。这时，变型后的M公钥密码体制信息速率：$R=\left(k+\left\lfloor \log_2\binom{n}{t}\right\rfloor\right)/n$ bit/s。图4.11给出了MATLAB曲线图。

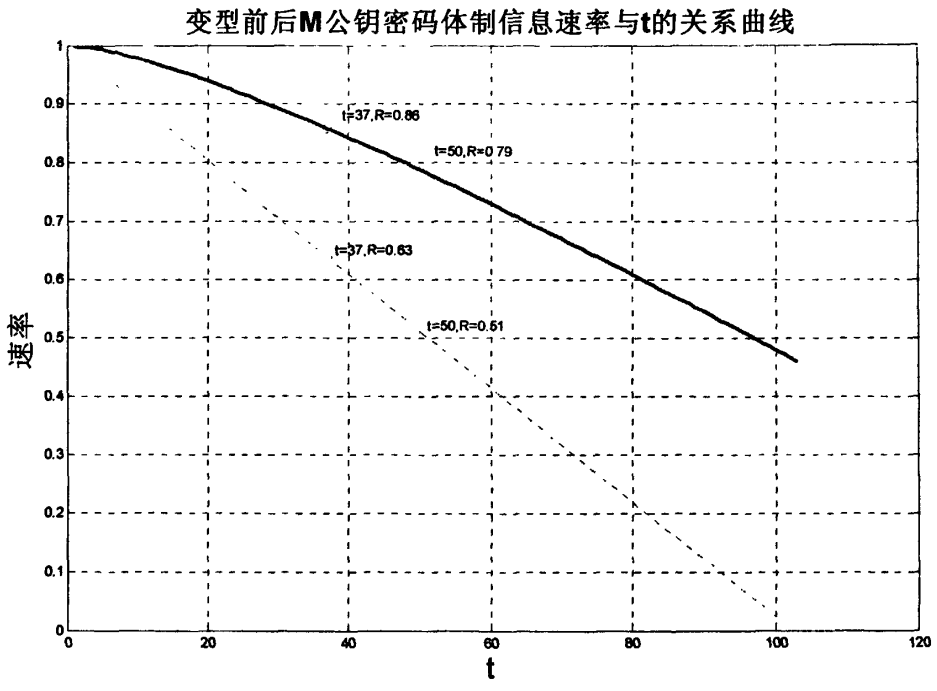

图4.11 变型前后M公钥密码体制信息速率与t的关系曲线

图4.11上，虚线代表了变型前M公钥密码体制的信息速率，实线代表了变型后M公钥密码体制的信息速率。由图4.11可知，通过变型，$t=37$时，信息速率由0.63提高到了0.86。$t=50$时，信息速率由0.51提高到了0.79。

由于变型后的方案的安全性存在弱点，为了克服这些弱点，提高M公钥密码体制的信息速率，在3.3.4节中，又给出了另一种变型方案。该方案使得变型后的M公钥密码信息速率 $R=(k+\left\lfloor \log_2 \binom{n}{t} \right\rfloor)\Big/(n+q)$ bit/s。

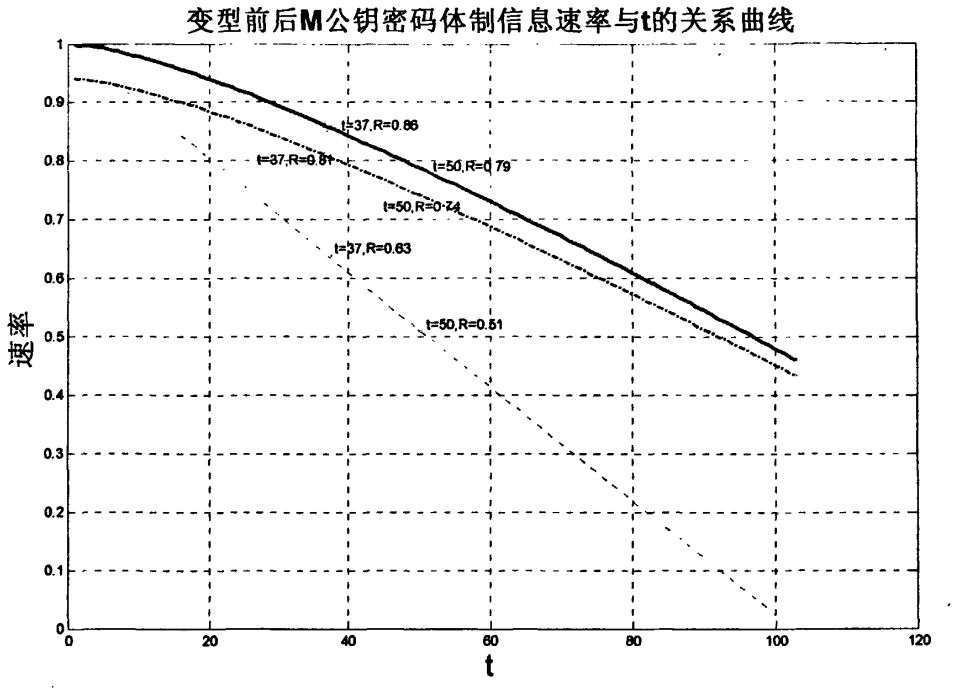

图4.12 变型前后M公钥密码体制信息速率与t的关系曲线($q=0, q=64$)

图4.12中，虚线代表变型前M公钥密码体制的信息速率。实线代表在$q=0$的情况下，变型后M公钥密码体制的信息速率。点划线代表在$q=64$的情况下，变型后M公钥密码体制的信息速率。由图4.12可知，在$q=0$时，通过变型，$t=37$时，信息速率由0.63提高到了0.86，$t=50$时，信息速率由0.51提高到了0.79。在$q=64$时，通过变型，$t=37$时，信息速率由0.63提高到了0.81，$t=50$时，信息速率由0.51提高到了0.74。

与M公钥密码体制相比，N公钥密码体制的信息速率要低一些，该体制的信息速率$R=\left[\log_2\binom{n}{t}\right]\Big/(n-k)$ bit/s。图4.13 给出了N公钥密码体制信息速率与t的关系曲线。

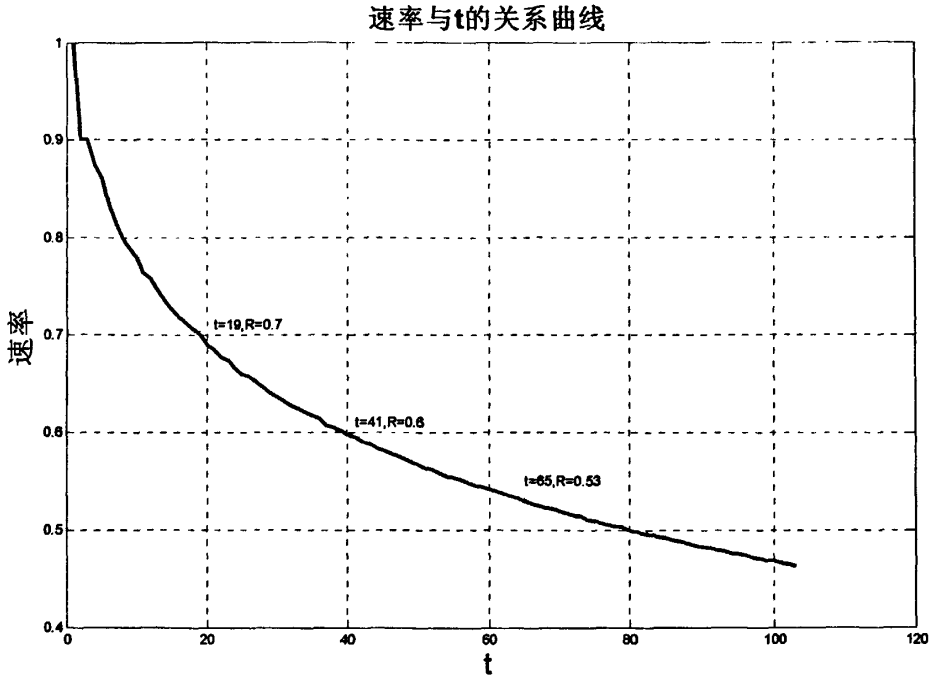

图4.13 N公钥密码体制信息速率与t的关系曲线

由图可知，R随t的增大而减小。$t \in [19,65]$时，$R \in [0.7,0.53]$。$t=41$时，$R \approx 0.6$。

第五章 总结与展望

自从开创了现代密码学，密码学的研究便进入了一个崭新的飞速发展时期。纠错码与密码的结合是代数编码和密码学发展的必然产物。纠错码的成熟理论和技术成功地解决了密码学中的许多问题，同时，这些问题的解决又进一步促进了代数编码理论和技术的发展。

由于公钥密码体制与纠错码的特殊关系，本文作者针对基于纠错码的公钥密码体制的性能做出了深入分析，并且进行了数值分析，最后得到了重要结果。

对于M公钥密码体制，作者用第三章所介绍的解线性方程组攻击方法和Lee-Brickell的攻击方法，通过第四章的计算机数值计算分析，从模拟曲线图中，可以看出，当$t\in[14,65]$，M公钥密码体制的工作因子仍大于2^{60}。因此，在实际应用中，只要取$t\in[14,65]$，此时，M公钥密码体制就有足够的安全性。

综合分析M公钥密码体制与N公钥密码体制后，作者建议两类公钥密码体制的t取值$[18,65]$。因为，当$t\in[18,65]$，即使在解线性方程组攻击和Lee-Brickell攻击下，两类公钥密码体制仍保持工作因子在2^{60}以上，足够保证这两类公钥密码体制的安全性。

通过作者对M公钥密码体制的工作因子与码的纠错能力之间的关系分析，可知，在M公钥密码体制中，若$w(z)\le t$，则体制有足够高的安全性。因此，当$w(z)<t$时，M_S公钥密码体制不仅是安全的，而且还至少具有$t-w(z)$的纠错能力。同样，对M_S公钥密码体制进行解线性方程组攻击和Lee-Brickell攻击，从第四章的计算机数值计算分析结果中，可以看出，虽然M_S公钥密码体制的工作因子，与M公钥密码体制相比，有所下降，但是仍具有安全性，可以用于保密通信中。所以说，在有扰信道上，具有加密纠错功能的M_S公钥密码体制比仅有加密功能的M公钥密码体制更适合实际的需要。M_S公钥密码体制充分发挥了z的双重作用，而M公钥密码体制仅发挥了z的保密价值。

在第四章中，对于各类基于纠错码的公钥密码体制的工作因子数值计算分析，可见，随着码的纠检错能力增强，公钥密码体制的安全性随之提高，但是当公钥密码体制达到最高安全性的时候，再随着码的纠检能力增强，公钥密码体制安全性反而降低。由此，作者可知，冗余信息过少或过多，都会降低该通信系统的保密性，因此，作者建议，在实际应用中，码的纠检错能力应取适合的范围，才能使通信系统达到足够的安全性。

M 公钥密码体制的一个不足是信息速率低，第三章中介绍了几种经过变型的 M 公钥密码体制，尤其对于变型 II，它既克服了变型 I 的不足，也提高了信息速率。经过对该变型的分析，作者得知它的信息速率 $R=(k+\left\lfloor \log_2 \binom{n}{t} \right\rfloor)/(n+q)$ bit/s。通过第四章的数值计算分析，作者得出 M 公钥密码体制、变型 I 与变型 II 的信息速率比较曲线图，从图中可以直观验证出第三章中的理论分析。

在 N 公钥密码体制中，公钥量随 t 增加而增加，但信息速率则随 t 的增加而降低，因此，在 N 公钥密码体制中应选用小的 t。但在 M 公钥密码体制中，公钥量及信息速率均随 t 的增加而降低，因而，作者知道，在公钥密码体制中，对于 t 的选择，存在一个公钥量与信息速率间的折衷问题。另外，当 t 较小时，N 公钥密码体制的公钥量要比 M 公钥密码体制少，相比之下，N 公钥密码体制的信息速率比 M 公钥密码体制的低一些。如当 t=19 时，N 公钥密码体制的公钥量约是 M 公钥密码体制的 22.8%，相比之下，N 公钥体制的信息速率约是 M 公钥体制信息速率的 86.4%。然而，当 t 较大时，结论相反，M 公钥密码体制的公钥量反而要比 N 公钥密码体制少，相比之下，M 公钥密码体制的信息速率比 N 公钥密码体制的低一些。如当 t=65 时，M 公钥密码体制的公钥量约是 N 公钥密码体制的 57.5%，相比之下，M 公钥体制的信息速率约是 N 公钥体制信息速率的 69.8%。作者通过上述比较，由此可见，虽然 M 公钥密码体制与 N 公钥密码体制是等价的，但是两类公钥密码体制各自都具有优缺点。作者认为，在实际应用中，可以根据各自的特点，挑选出适合实际应用系统的公钥密码体制。

此外，作者通过观察第四章的信息速率曲线图，可以看出，无论是 M 公钥密码体制、N 公钥密码体制还是变型后的 M 公钥密码体制，随着码检错能力的增强，信息速率反而下降。作者得出结论：提高可靠性和提高有效性发生矛盾。从这一结论可以看出，在构造一个保密通信系统时，需要统筹兼顾。

这些结果对设计和构造基于纠错码的密码体制和方案都有指导价值。从传输数据的可靠性与安全性的整体出发，如何利用纠错码的特点构造出性能更好的加密与纠错相结合的体制，是非常值得研究的。

参考文献

[1] Shannon C. E., A Mathematical Theory of Communication, Bell System Technical Journal, 1948, 27:379~423,625~656.

[2] Shannon C. E., Communication Theory of Secrecy System, Bell System Technical Journal, 1949, 28:656~715.

[3] Berlekamp E. R., Goppa codes, IEEE Trans. Inform. Theory, 1973, vol.IT-19, p590~592.

[4] Diffie W., Hellman M. E., New Directions in Cryptography, IEEE Trans. Inform. Theory, 1976,22 :644~654.

[5] F. J. MacWilliams and N .J .A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.

[6] Rivest, Shamir R. A., and Adleman L., A Method of Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM, 1978, 21:120~126.

[7] Berlekamp E. R., McEliece R. J., and Van Tiborg H. C. A., On The Inherent Intractability of Certain coding Problems, IEEE Trans. Inform. Theory, 1978, 24 :384~386.

[8] McEliece R. J., A Public-key Cryptosystem Based On Algebraic Coding Theory, In: DSN Progress Rep 42~44, Jet Propulsion Lab., 1978, 114~116.

[9] Lu S. C., Lee L. N., and Fang R. J. F., An integrated system for secure and reliable communications over noisy channels, COMSAT Technical Review, 1979, p49~60..

[10] Jordan J P., A variant of a public-key cryptosystem based on Goppa codes, Sigact news, 1983, 15:61~66.

[11] Niederreiter H. K., Knapsack-type cryptosystems and algebraic coding theory, problems of Control and Inform. Theory, 1986, 15:159-166.

[12] Park C. S., Improving code rate of McEliece's public-key cryptosystem, IEEE Electronics Letters, 1989, 25:1466~1467.

[13] Adams.C,Meijer H.Security-related comments regarding McEliece's public-key cryptosystem, Lecture Notes in Computer Science, Advances in Cryptogy-Crypto'87,1988, p221~228.

[14] Lee P. J. and Brickell E. F., An observation on the security of McEliece's public-key cryptosystem, Advances in Cryptology-Eurocrypto'88, 1989, p275~280.

[15] van Tilburg J., On the McEliece public-key cryptosystem, Advances in Cryptology-Crypto'88, Proceedings, Springer-Verlag, 1990, p119~131.

[16] Lin M. C., Chang T. C., and Fu H.L., Information rate of McEliece's public-key cryptosystem, IEEE Electronics Letters, 1990, 26:16~18.

[17] Korzhik V. I., Turikin A. I., Cryptanalysis of McEliece's public-key cryptosystem, Advanecs in Cryptology Proceedings of Euro-crypt'91, Lecture notes in computer science, vol 330, Springer-verlag,1991,68~70.

[18] Gibson J. K., Equivalent Goppa codes and trapdoors to McEliece's public-key cryptosystem, Advance in Cryptology-Eurocrypto'91, 1992, p517~521.

[19] Goodman R.M., McEliece R.J., Sayano M ., Phased Burst Error-Correcting Array Codes, IEEE Trans. on Inform. Theory, 1993(39):684-693.

[20] Chabaud F., On the security of some cryptosystems based on error-correcting codes, Proc Eurocrypt'94,LNCS 950,1994,131~139.

[21] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, New York: John Wiley&Sons, 1996.

[22] Berson T. A., Failure of the McEliece public-key cryptosystem under message-resend and related-message attack, Advance in Cryptology-Crypto'97, 1997, p213~220.

[23] V. Pless, Introduction to the Theory of Error-Correcting Codes, Third Edition,. New York: Wiley, 1998.

[24] Fox B., Lamacchia B., Certificate Revocation: Mechanics and Meaning, Proc Financial Cryptography FC'98, 1998, 158-164.

[25] Kocher P., On Certificate Revocation and Validation, Proc Financial Cryptography FC'98, 1998, 172-177.

[26] Sun H. M., Improving the security of the McEliece public-key cryptosystem, Asiacrpty'98, 1998, p200~213.

[27] Engelbert D., Overbeck R., Schmidt A., A summary of McEliece-type cryptosystems and their security, Journal of Mathematical Cryptology, 2007, p151~199.

[28] Ryan J., Excluding some weak keys in the McEliece cryptosystem, IEEE Africon Conference, 2007, 44:16~20.

[29] Nojima R., Imai H., Kobara K., Morozov K., Semantic security for the McEliece cryptosystem without random oracles, 2008, p289~305.

[30] Bernstein D.J, Lang T., and Peters C., Attacking and defending the McEliece cryptosystem, Lecture Notes in Computer Science, Advance in PQCrypto'2008, 2008, p31~46.

[31]周炯梁，信息论基础，北京：人民邮电出版社，1983.

[32]王新梅，肖国镇，纠错码——原理与方法，西安：西安电子科技大学出版社，1991.

[33]Arto Salomaa 著，公钥密码学，丁存生，单炜娟译，北京：国防工业出版社，1998.

[34]杨义先，林须端，编码密码学，北京：人民邮电出版社，1992.

[35]肖国镇，卿斯汉，编码理论，北京：国防工业出版社，1993.

[36] Adams C., Lloyd S.著，公开密钥基础设施一概念、标准和实施，冯登国等译，北京：人民邮电出版社，2001.

[37]王新梅，马文平，武传坤，纠错密码理论，北京：人民邮电出版社，2001.

[38] Wade Trappe, Lawrence C. Washington 著，密码学概论，邹红霞，许鹏文，李勇奇译，北京：人民邮电出版社，2004.

[39]张宗橙，纠错编码原理和应用，北京：电子工业出版社，2005.

[40] Ranjan Bose 著，信息论、编码与密码学，武传坤译，北京：机械工业出版社，2005.

[41]王新梅，既约 Goppa 码的纠突发能力，西安电子科学大学学报，1981，No.1，p62~68.

[42]王新梅，M 公钥的推广及通过有扰信道时的性能分析，电子学报，1986，No.4，p83~90.

[43]王新梅，MC 分组加密纠错体制，通信学报，1986，No.5，p1~6.

[44]王新梅，纠错码中的几个重要问题及其最近进展，通信学报，1988，No.4，p58~71.

[45]李元兴，纠错码在现代密码学中的应用，通信学报，1991，No.4，p102~106.

[46]李元兴，N公钥与M公钥密码的安全性等价，自然杂志，1991，No.6，p471~472.

[47]王育民，张海林，张侃， M公钥的性能分析及参数优化问题，电子学报，1992，No.4，p32~36.

[48]李元兴，用 BCH 等线性分组码构造 McEliece 纠错码公钥密码体制，电子科学学刊，1993，No.2，p208~211.

[49]李元兴，王新梅，关于 Niederreiter 代数码公钥密码体制的安全性及参数优化，电子学报，1993，No.7，p32~36.

[50]王新梅，李元兴，武传坤，McEliece 公钥体制的修正，电子学报，1994，No.4，p90~92.

[51]杜伟章，基于最大秩距离码的 Niederreiter 公钥密码系统，计算机工程与科学，2000，No.4，p4~5.

[52]梅挺，代群，基于 Niederreiter 纠错码的公钥密码体制的研究，通信技术，2007，No.6，p36~39.

[53]梅挺，代群，张明，基于 McEliece 纠错码的公钥密码体制的研究，通信技术，2007，No.9，p61~63.

致 谢

在本论文结束之际，回想起这二年半来的学习生活，不禁心怀感激之情！我的每一点进步都与许多人的关怀和帮助是分不开的。

首先要深深感谢我的导师张宗橙教授。张宗橙教授在我攻读硕士学位期间给我提供了充分的发展空间和良好的研究氛围，掌握相关研究领域最新的研究动向。二年半来张老师始终给予我悉自的指导，他勤奋钻研的科学态度对我一直耳濡目染，也将是我以后在科研和生活中学习的榜样。

同时，我由衷地感谢教研室同门对我论文的直接指导和帮助。他们在我论文工作期间，给我的帮助很大。

最后，我要特别感谢我的父母和家人。感谢他们对我学业的一贯支持，使我得以顺利完成硕士学位论文。

在读期间发表的论文

朱陆费，CG 网基站共站址杂散干扰的分析研究，《消费导刊》，2008 年 6 月。