|  |
| --- |
| 116965810473792200791017493533055 |
| **信息安全技术课程作业** |
|  |
| 姓名：xxxx  学号：xxxx  班级：xxxx  教师：xxxx |
|  |

|  |
| --- |
|  |

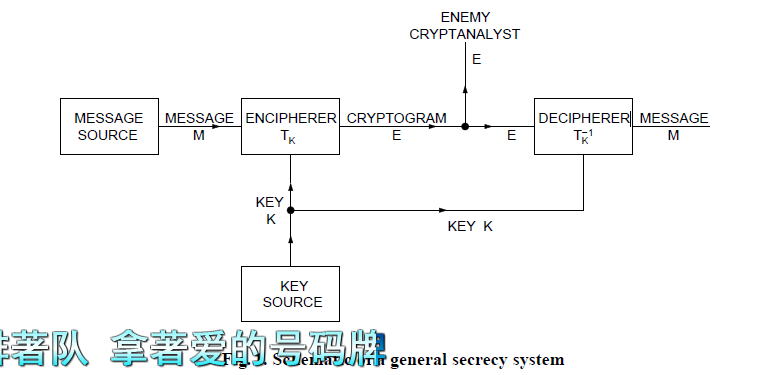
《保密系统的通信理论》读后感

1．学习这篇文章的收获。

这篇论文理解起来很不容易，我花费了很长的时间才把概论那一部分看完，由于缺乏必要的信息论方面的知识，有些名词的理解可能会有错误。这篇文章分三个部分分别介绍了保密系统的数学模型，理论保密的内容和实际保密的问题。至少我知道了密码理论和概率理论在保密系统中的大量应用。我也学会了一些概念比如什么是冗余度，什么事H（N），置换密码，唯一距离，条件信息量总平均值，“纯”的保密系统，“完美”的保密系统。

下面是我在这三个部分中所能理解的一些知识的总结。

密码术和保密系统的研究是通信理论一个很有趣味的应用.这篇论文在理论层面提出了保密系统的理论，试图补充处理标准文献中的密码方面的问题。这篇文章里面详细研究了许多典型密码编码和相应的破解方法。**我们将更加关注保密系统的一般数学结构和性质。**



这些处理方法限于某些情况。首先，**有三种一般型的保密系统：**（1）隐藏系统例如隐形墨水，把要传递的信息隐藏于一段与之毫无关系的文本中，或隐藏于假的起掩护作用的密码电文中等一系列手段使敌人发觉不到被隐藏了的信息的存在。（2）私密系统，例如在接收端用特殊设备将（隐藏）倒置的语言恢复。（3）名符其实的保密系统通过编码加密等方法使信息的含义隐形，虽然信息存在并没有被隐藏，而且敌人也可以使用任何设备中断并捕获传输的信号。我们只考虑第三种类型的系统——隐藏系统主要是心理学的问题而秘密系统主要是一个硬件技术上的问题。

其次，处理方法仅限于离散信息，信息被加密成一个由有限集中的离散字符组成的序列。这些字符可能是一种语言中的一些字母，一种语言中的一些文字，一个量化的声音或是视频信号的幅度等等。但是这里我们主要关注的是字母的情况。

这篇论文分为三部分.现在我们简要概括出主要结论。第一部分主要讨论了保密系统的基本数学结构。在通信理论中，我们通常情况下认为语言是一个按照某种可能的方法产生符号离散序列的随机过程。把和语言相关的一个参数D称为语言的冗余度。D在某种意义上反映了，一段文字在不丢失任何信息的情况下在长度上最多能够省略多少字符。比如说下面这个简单的例子，在英语单词中，u常常跟在q后面，u就可能被省略，原来的单词没有受到影响。由于英语这门语言有着特殊的统计结构如某个字母或单词的反复使用等，在英语中存在相当大可能的冗余。冗余在保密系统研究中扮演着非常重要的角色。

**保密系统**可以抽象为一个空间（可能的消息的集合）到另一个空间（可能的密文的集合）的函数集合。在这个函数集合中每一个特殊的映射对应于一把加密密钥。这个函数假设是可逆的以便于知道密钥后有进行解密的可能。

因此我们认为每一个密钥和每一个变换是靠先验概率相关连的，先验概率表示选择该密钥的可能性。类似地，我们认为每一个可能的消息也应该有一个与之相联系的先验概率，它是由整个随机过程决定的。选择这些密钥和消息的概率实际上是敌方密码破译者的破译上述消息和密钥的先验概率，可以体现出密码专家关于该情况的先验知识。

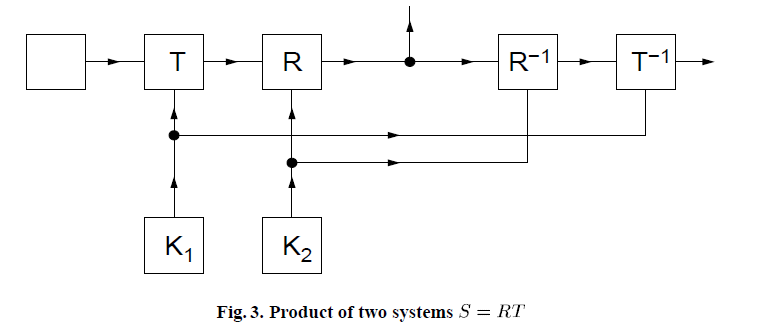
使用保密系统的时候，我们首先选择一个密钥然后把它送到接收端。密钥的选择决定了使用变换函数集中哪个函数来构建这个系统。然后选择相应的消息通过选择好的函数变换进行加密产生密文。密文通过一个通道穿送到接收端，在这个过程中可能敌方中途捕获。在接收端通过相反的函数变换（反函数）对密文进行解密来恢复原始消息。

如果敌方中途捕获，他能通过密文计算出产生密文的各种消息和密钥的先验概率。这个后验概率的集合构成了他关于上述密钥和消息的认识。因此，这个认识是由这些概率问题所决定的。关于后验概率的计算是密码破译者要解决的一般问题。

我们用下面这个例子来解释上述概念。在一个使用简单的替换密码加密过程中，我们可以随机选择26！个替换方式来替换26个不同的字母。这些方式是等概率出现的，所以每一个方式选取的先验概率应该是1/26!。如果把上述理论应用到标准英语中，同时假设密码破译者不知道消息源除了能够产生英文文档外的其他信息，那么由N个字母组成的消息的先验概率就是他们在标准英语文本中的相对频率。

如果敌方在保密系统中捕获N个字母的密文，它的先验概率是会发生变化的。如果N足够的大（比如说50个字节）那么通常会有一个可能的消息的后验概率接近1，同时其它所有消息的总的概率接近于0。这时就有一个特殊的方法来处理这个密文。如果N小一些（比如说N=15）将会有使用许多消息和密文的可能性。这种情况下将会有多种解可能的原消息。

我们用这种方式考虑一个保密系统，把它看成是一个集合中元素到另一个集合中元素的变换的集合，有两个基本运算的组合可以从某两个系统中产生第三个系统。第一种组合运算叫做乘积运算，它是把消息通过保密系统R进行加密，然后通过保密系统S对上面的加密结果再次进行加密得到密文，R、S系统的密钥的选取是相互独立的。这个总的运算组成立一个新的保密系统，它包含了R、S系统所有变换的乘积，这些乘积变换的概率是R、S系统中对应变换概率的乘积。

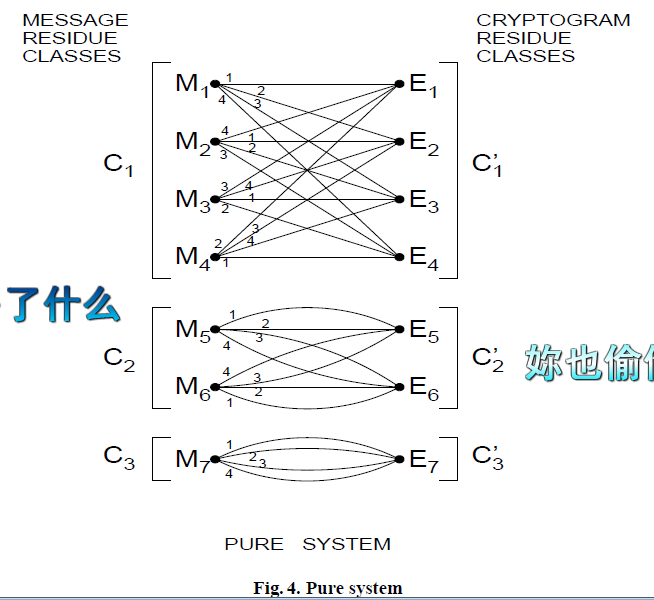


第二种综合运算是加权平均运算： 

它相当于用概率p、q表示对选择R系统还是S系统做一个初步的选择。此时R、S应当是确定的。

我们证实，一个通过上面两种综合运算组成的保密系统构成了一个“线性结合代数”和单位元，代数簇，这些数学理论已经被数学家们广泛讨论过。

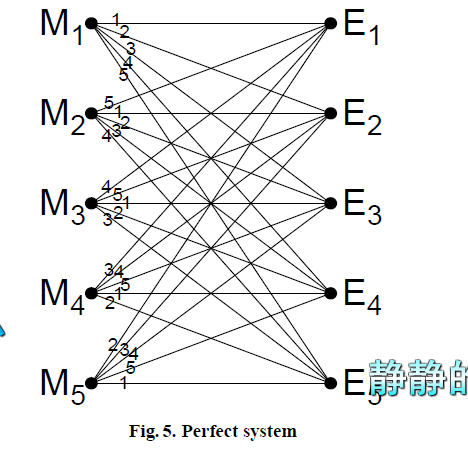
在众多保密系统中有一种保密系统特性很丰富。这种保密系统我们成为一个“纯”系统。一个系统是“纯”的当它的所有的密钥是相当的并且还要保证它的任意三个变换Ti,Tj,Tk的乘积同样在这个变换集中。也就是说，加密，解密和任意三个密钥组合完成的加密必须和某个密钥完成的加密是相当的。



可以证明当我们采用一个“纯”的密码加密时，所有的密钥是等价的。他们产生相同的后验概率集。而且，当某个密文被拦截后，我们会发现有许多消息可能产生这段密文。（我们称其为剩余类），这些消息（剩余类）的后验概率与先验概率是成比例的。敌方拦截的所有信息只是剩余类的一个特殊情况罢了。许多常见的密码是”纯”保密系统。包括替代密码（随机密钥）。在这种情况下，剩余类组成了按这种方式产生这段密文的所有可能的消息。

如果存在一个变换A和它的逆变换满足R=AS，那么R和S是相似的。如果R和S是相似的，R和S产生的密文具有相同的后验概率。这两个系统在密码分析上是相同的。

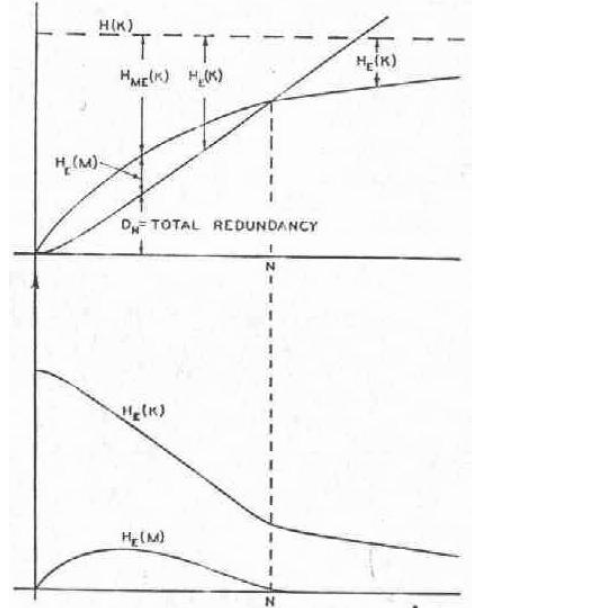
**这篇论文的第二部分**主要解决“理论保密”的问题。当敌方有无限的时间和体力对拦截到的密文进行分析的时候这个系统对密码分析的安全性有多大。这个问题和以噪声形式进行的通信是紧密相关的，与通信问题有关的信息熵和条件信息量的总平均值的概念在密码学的这些方面取得了直接的应用。



“完美保密”的条件：找到一个系统，当他产生的密文被敌方拦截后，这段密文所能表示的各种消息的后验概率代表和拦截前它所能表示的各种消息的先验概率的是相同的。可以证明，完全保密是可以实现的但是需要条件：要传递的消息的是有限长的，可能的密钥也需要有同样地长度。如果消息被认为是以某一速率“R“连续生成的，相应的密钥必须也是以相同的速率产生。

如果一个保密系统用一个有限长的密钥进行加密，产生的长度为N的密文被敌方拦截了，对于敌方来说可能获得这段密文所代表的某个消息的集合。当N增加的时候，这个消息的集合会越来越小直至最后只有一个答案。这个消息的概率变为一，其他可能的消息的概率变成零。H（N）——条件信息量总平均值从统计学的角度，描述了N个字母长度的密文和相应的被破译的消息的相近程度，也就是，敌方获得原始信息的不确定程度。条件信息量总平均值的特性可以推断出来。例如，密钥的的条件信息量总平均值不会随N的增加而增大。条件信息量总品均值是“理论保密”的一个指数，它表示敌方需

要花多长时间来分析密文。



随机密码的函数H(N)函数是确定的。这个函数稍加改动就可以应用与许多实际应用中。它提供了一种计算被拦截的密文和破译相应的保密系统的近似程度的方法。从刚才的分析中我们可以得到：采用通用的语言和普通的密码手段，这个唯一距离近似等于“H（K）/D”。H（K）是可能的密钥数的对数。D是语言的冗余度，表示这么语言施加的统计约束。对于简单的置换密码，，英语的D=0.7。因此唯一性距离大约是30个字。

用一个有限长的密钥使用某种语言构建一个保密系统使条件信息量总平均值在N无穷大的情况下不趋近于零是可以实现的。这种情况下，无论多少东西被敌方拦截到，敌方仍然不能获取这个唯一解但是可以获得许多可供选择的答案，每个答案都有一定的可能性。这样的系统我们称为理想系统。使用任何语言都可以做成类似的系统，当H（N）趋于0的时候使它倒退到任意大的数N。然而，这样的系统有一些缺点，例如密文传输比较复杂，对错误很敏感。

**论文的第三部分主要讨论了“实际保密”的问题**。当N个字符被拦截后，两个用大小密钥加密的系统可能都被攻破，但攻破系统所需要的人力物力会差别很大。我们将对保密系统的基本缺陷进行分析。这样我们就可以构建一个需要很大的人力物力才能攻破的系统。最终，我们会讨论一下各色保密系统之间的兼容性问题。