早期计算机密码学的历史及影响

The History and Influence of Arithmetical Machines and Early Cryptography

尹飞 /YIN Fei

（广西民族大学民族学与社会学学院，广西南宁，530006）
(College of Ethnology and Sociology, Guangxi University for Nationalities, Nanning, Guangxi, 530006)

摘　要：计算机的雏形多功能计算器由17世纪英国皇家学会会员塞缪尔·莫兰设计，其中加入了密码功能。早期密码学主要由约翰·威尔金斯探索。计算器及早期密码学的研究体现了数字化人文的思想，这是一种脑力工作结合手工工作的方式，也反映了人文学科和自然科学的异同。数字化人文思想力图打破人文学科与自然科学的疆界，数字化阅读与写作进入到公众视野，体现了多学科共融的认知态度。早期计算机密码学影响了人工造物文化的展现方式。

关键词：计算机密码学　数字化人文　人工造物文化　科学与人文

Abstract: The prototype of computers, the multifunctional arithmetical machine, was designed by Samuel Morland, while early cryptography was mainly explored by John Wilkins. The study of arithmetical machines and early cryptography embodies the idea of digital humanities, which is a way of combining mental work with manual work. It also reflects the similarities and differences between humanities and natural sciences. The idea of digital humanities attempts to break the boundaries between humanities and natural sciences, and digital reading and writing, which have stepped into the public view, reflect a cognitive attitude of multidisciplinary integration. Arithmetical machines and early cryptography influenced the way of representations of artificial culture.

Key Words: Arithmetical machines and cryptography; Digital humanities; Artificial culture; Science and humanities

中图分类号：N09　　**文献标识码：**A　　DOI:10.15994/j.1000–0763.2019.12.009

英国皇家学会会员塞缪尔·莫兰（S. Morland）在1666年前后设计了一系列的计算器，这些计算器可以计算购物价格，也可以破解一些简单的密码，是一种多功能计算器。皮普斯（S. Pepys）、罗伯特·胡克（R. Hooke）等都在传记里不厌其烦地描述这种机器的流行状况，计算器的外包装简直媲美现在的苹果手机。对于技术工作者而言，计算器的设计思想比它的实际用处更为伟大。

莫兰曾经在1666年的《密码使用方法》（*A New Method of Cryptography*）一书中提到设计这款计算器的初衷远不是方便消费者计算购物差价这么简单。使用他设计的计算器会具备加密和解密功能，也就是说莫兰设计的计算器更重视保护使用者的私人利益，尽管相关的条款在17世纪尾声才出现，却并不影响设计思想的独特性。这款计算器还具备多功能特点，一旦使用者输入资产项目，计算器马上提示可计算个人财富值，它将计算技术与现实可见的实物对应了起来，体现了脑力工作和体力劳动的对应。多功能计算器的数字化设计思路也开启了现代密码学的研究，早期密码学的探索得益于约翰·威尔金斯（J. Wilkins）。[1]

一、计算器密码与数字化人文

莫兰计算器的功能之一就是设置了密码，这需要数字化索引提供辅助功能。由于数字化索引提供了指向功能，使用者在写下记录或者进行加

收稿日期：2018年7月9日
作者简介：尹　飞（1981–）男，河北石家庄人，广西民族大学民族学与社会学学院讲师，研究方向为科技哲学、逻辑学。
Email: 1376291211@qq.com

密的同时，磁盘在快速运转。莫兰还给计算器设计了另外一款装置，非常类似于今天的电脑触笔，并不需要墨水就可以在计算器显示屏上留下印记，并用于完成提前制定好的程序。这种计算器以一种新颖的方式成为人们的“掌中宝”，可以用来方便地撰写文章、储存资料、检索字句以及做语句分析。[2] 与莫兰同时代的英国皇家学会会员威尔金斯是英国第一位研究密码技术的人，他也在挑战传统使用墨水和纸张进行写作的方式。威尔金斯认为古人保存文献和使用的加密技术都太过古老，例如有些珍贵文献记录在兽皮上，通过一些液体浸泡进行加密，这样的方式致使文献模糊，而且还原程度极低。这种加密与解密的游戏刺激威尔金斯开启了加密技术与图形联系起来的研究。就如同埃及人发明的象形文字，同时埃及人又是学者和工程师，他们使用的外部物品既具备图形要素，[3] 同时也是文献信息传达的内容，两者可以区分开来对待。17世纪英国的密码学专家主要就是莫兰和威尔金斯两人，他们都拓展了记录方式，拓宽了记录材料的范围，甚至发明了非物质的符号系统，他们转变了记录只是在平面上书写文字的观念。

从某种意义上讲，莫兰认为密码对于人类经验表达来说是一种必要前提条件，因此密码学的研究即便对于政治或者军事目的而言也是一种人文要求和精神追求。 在传统观点看来密码学是一种神秘的技术，甚至跟巫术、炼金术、占星术都能扯上关系。这些相关学科的研究在17世纪很长一段时间里得到了长足的发展，对密码学的研究起到了助推作用。除去神秘术的部分，密码学是依照传统的文科规则进行研究的。首先，威尔金斯认为密码与编码、加密与解密这样的技术是创造型的、艺术型的，同时也是叙述型的，是完全的文本编辑和阅读。并且密码学是按照字母排序进行表达的。其次，威尔金斯并没有把密码学和科学技术联系在一起，例如实验室和工程技术种种课程在当时还未被高等教育所接受。威尔金斯作为皇家协会的会员，有义务改变公众的观点，使科学和机械的严谨性被社会接受。这个任务由莫兰的多功能计算器来完成。

科学、技术、工程实践类似的学科需要学术权威认证其合法性，而人文学科已经被学术权威确立为知识追求的目标。17世纪的学者对于文学、历史、逻辑学、修辞学普遍持有认同态度。所以威尔金斯对于密码学的认同是存在于人文学科之内的，如果将密码学位列计算机科学研究领域一定会产生人们的诧异，因此密码学的知识合法性在当时确实是一个问题。威尔金斯并不认为人文学科是高尚的脑力工作，而技艺是普通的手工劳动。威尔金斯的观点是人文学科作为学术知识理应被认同，但是工程技术也应该被重点学习，因为它们创造了有形资产。但是威尔金斯也强烈认同学科传统，并对人文学科的合法性保持敬畏，他认为密码学作为学科必须根植于人文学科的土壤，他一生都在努力构造科学、人文、工程的学科统一，但是如何消弭学科分歧一直没有好的对策。今天的人文学者却要捍卫自己的领地，要对人文学科无用论进行反驳，因为人文学科只是产生非物质知识，并不针对现实实物。

威尔金斯致力于密码学的合法地位，其他的工程科学也纷纷效仿，当然这一切在今天看来早已尘埃落定。这些需要一个所有学科能够分享知识的大视野。这样的大视野要能够跨越国家以及各个课程的边界，也需要学者们持有研究目标能够融合的态度。密码学从理性视角而言，人们对于保密的要求逐步升级，这就需要不断融合一些理念、方法和信息传输媒介。威尔金斯提倡的英语作为世界语言可以沟通本土和异地，这是由他本人的知识结构导致的。这背后是英国当时在世界上的财富和知识地位决定的。这种打通各个学科边界的做法揭示了学科划分的一些模糊性。直至今日，各种跨学科研究的模糊性依然存在，从各种题材样式来看包括了信件、说明书、游戏、网文等等，甚至它们创造的模糊性与开发的新形式题材一样多。17世纪的密码学就精细地研究这些模糊性。实际上学科的边缘缺陷和观察缺陷在密码学中一直存在。威尔金斯和莫兰对于这种短期的文化现象非常好奇，它们可以增强概念的模糊性，并且从多视角来看，思考者是隐藏在研究目标之后的。这种现象的典型案例就是21世纪开发的Web2.0，一方面网络接口的要求是别人必须能够浏览网页，而另一方面计算机服务器又必须保护本台电脑的私人秘密，不该用户浏览的内容绝对不能泄密。这就在人文学术和全球共享之间存在了张力，这是一种跨越边界的联合。这就需要在高等教育里拓展一种更为宽泛的跨学科教

育，威尔金斯提倡的多重学科同时也要伴随公众的多重智能化。威尔金斯的学术著作提供了一种周密的教学计划，可以使学生和公众达到一种更为广泛的学习认识，在学习自然哲学的同时也要将技艺实践拓展至学术领域。这是一种流行性教学，将高等教育拓展至实用技巧，这对学科进一步细化是有帮助的，但是对于跨学科综合的效果却不是那么明显。

人文学科、工程技术甚至早期的计算科学都通过学科之间的直接联系或者间接联系融合在了一起，计算器服务于修辞学的目的也得到了知识分子和技术工作者的支持。这样的目的自17世纪至今300年的历史长河中并未消失，只是在有些历史阶段不太明显，有时甚至是隐藏的。密码学的人文学科背景真正消失并隶属于自然科学领域是在第一次世界大战时期，有了战争就有了密码。[4]

在这个时期，人们可以清晰看到密码学的认知除去了它的人文学科背景，并且表明了自然科学属性的原因和方式。人文学科是普遍的，它使人们的语言知识有价值地使用在文本分析，无论这样的语言知识来自于古希腊还是现代。但是在美国情报处，无论是对问题的争论还是收集证据的方法，这样的知识却丝毫没有用武之地。美国情报处及解密文件揭示了密码工作受17世纪密码使用手册的影响，甚至还有一些受到当时多功能计算器的启发。随着这些解密文件公布于众，人们才意识到密码学的重要性，正如马尔伯勒·丘吉尔（M. Churchill）写道“或许有一天，全世界民族以前认为的和谐相处将会发生改变，出于公众安全的考虑，各国应该都留有各自的密码。如果不是这些解密文件公布于众，我们甚至还不知道人文传统的密码学已经改头换面。”[5]在一战时期，更多早期的数字化研究思路特别是语言频率分析不仅作为20世纪的密码学基础，同样也是21世纪计算机语言的基础。因为当时密码系统的影响力已经波及到了人们今天熟知的计算机发明者们。

密码学与智能工作之间的联系是相当宽泛的，人文学科的影响依然存在于人们心中，但是今天对于人文学科的讨论却不是17世纪威尔金斯所希望的那样。科恩（D. Cohen）2006年标志性的文章《智能分析与人文学科》（*Intelligence Analysts and Humanities Sholars*）也表述了相同的观点。科恩描述了语句分析大会的盛况，参与发言的都是一些数字人文学者和计算机科学家。与会者发问如果数字人文与语句智能分析就是一回事的话，那么不同学科的两类人将会得到同一种答案。科恩随后在自己的博客中回复了这一问题，阐释了人文学科和计算机科学两者之间的张力，两种学科都试图努力进行真正的智能研究，并且通过各自的方式弥补自17世纪以来脑力工作和手工工作之间的鸿沟。[6]科恩这种跨学科关系的表述似乎在暗示这种智能工作的方法是对人文学科的轻视。他认为智能分析和传统人文学术之间确实存在差异，只要看到底哪种学科在扫描分析数据并整理电子信息材料，就能看出差异所在。只从方法论来看，两者似乎是趋同的，但是看到研究内容，人们就会明白两者确实不一样。科恩的主要观点是智能分析虽然需要理论，但是数字人文学者更应该开发他们自己的数字工具进行研究，而不仅仅是采用计算机学科领域的工具，无论两者的研究目的多么相像。仅开发工具还是不够的，还需要重新修订智能分析的假设，以及研究两个学科的科学史。除此之外，人文学者还要进一步精细化自己的理论，为计算机科学研究提供新的思路。密码学的发展史已经表明20世纪的计算机科学可以从中吸取充分的经验和教训，而这部分的工作是由人文学者完成的。

二、密码学及数字化阅读

瑞安·海瑟（R. Heuser）描述了人文学者开发工具表述数字化内容的困难，主要问题在按步骤将人文研究成果进行可视化处理成人工造物。[7]人们一定要问数字化的可视产品如何能保证经过加密后被阅读？难道一定要密码盘进行辅助吗？莫兰在1666年提供了一个早期答案，他提供了一种可修正密码盘的模式。当前多功能移动硬盘可以被用户轻松读取和改写，实际上这种模式早在莫兰的计算器使用手册中就有说明。这种模式可以允许阅读者并不需要在物理层面接触硬件就可进行磁盘的修改和阅读。莫兰改进了字母表排序的编码规则，并且使数据加密具备双形体形式，一种为书写加密，而另外一种为解码。使用者可以通过手动操作进行内容、页眉、副文本的编辑。莫兰和威尔金斯的专著实际上要求人文学者通过

他们的双手做比纸笔书写更多的事情。数字化的形式必须得到物理操作的检验，同时还要思考说明书和技术是如何建构的。这等于同时刺激了脑力工作和手工工作，从某种意义上讲促使了文本工作者使其工作数字化。

21世纪的数字化研究是人类手掌如何掌控数字化产品，如何读取数字化产品，这与17世纪的密码学影响是相关的。有人可能会争论，线上资源的盛行抑制了数字化的研究，人们将精力投诸于加密文本受到了限制。但是现代计算机科学早期的研究还是专注于指尖可触碰的范围，通过GIS技术分析程序频率、对软件加密和解密、3D成像技术等等。这些成果非常适应早期的密码学分析，通常对人文学术意义不大，并且开发费用昂贵。软件的加密和解密也不像人文学者认为的那样。软件解密的明码本一旦生成，软件的工作也就告一段落。政府和企业解密软件的设计并非依靠人文学者，杰罗姆·麦克甘（J. McGann）2011年写道“常规传统学术人文学部的成员并不是当前计算机科学的参与者。这些智能工具的发展已经引领和规范我们当前的研究框架。”[8]这样的观点也出现在科恩的博客中，谷歌全书的理论设计没有人文学者的加入，更不用说计算机辅助设备的研发。学者们通常会抱怨早期英文图书在线（EEBO）和十八世纪文献在线收藏（ECCO）两个项目的发展过程中没有人文学者加入其中，所以今天人们希望字符标识要更加准确，以方便学者们各自的研究。尽管使用者不能详细研究技术细节，但是密码学的使用手册和加密文本对于PDF非常有效。使用者依据文本数字化编码标准TEI进行编码的时候，就已经使用了另外一套系统，多余的技术环节已经被忽略了。

但是这里要指出，数字化手段的思想分析是先于这些技术工程的，TEI是典型的跨学科模式，如果TEI的发展符合考古学家、艺术史家和科学史家的内心意愿，那么这个模式需要人文学者输入信息，并且要参考当代早期的密码学发展。文本导向的人文计算机科学认为概念模式和本体论较为容易与数据库联系在一起，容易程度超过了文本研究。TEI的使用应该结合CIDOC-CRM模式，这是由国际博物馆协会制作的标准。这种标准的强大之处在于允许程序语言通过历史事件识别人工造物，也可以进行进一步的表述分析。2013年出品了TEI P5版本，更利于人文学者的简单学习。TEI P5版本体裁灵活，是当前存储和检索的趋势，数字化工程不再以统计数据为目标。除去数据分析支持之外，现代密码学的线上资源必须能保证人工造物的三维成像，并且要允许使用者通过人类手掌以各种方式进行操作。传统的写作工具就是鼠标、键盘、绘画板等等，使用者通过触碰能够显现成像的设备。3D打印目前是比较经济且能够实现的技术，可以使密码学的文化再次展示人工造物。

早期的密码学家莫兰和威尔金斯必须面对文理学科分类的困难，因为所有的知识只能凭借平板介质打印出来。威尔金斯依靠凸版印刷和副文本显示内容，莫兰则需要彩色图表阐释他的知识。莫兰对于黄绿墨水的使用达到了极致，彩色显示的特点是掌上设备的重要特征。但是在EEBO项目中，PDF图文副本并不能捕捉色彩和三维成像。如果是静电成像，即便图像本身是彩色的，也不允许用户依照莫兰手册的规则去获取三维成像实体。人工造物在历史长河里是碎片化的，而科学是经验积累性质的，所以追本溯源人工造物的源头并不是一个非常恰当的方法。像Sketch Up这样的设计软件允许设计者在特定时间和地点之内掌控三维影像，并且支持加密和解密数字页码，就像密码学那样可以存储。操作环境类似于软件的第二生命，并不需要多大成本就可以接入人文学术系统进行3D打印。哲学的辩证思维对于早期密码学的研究设置了前提假设。2007年，马修·德里斯科尔（M. Driscoll）在数字人文夏令营发言，指出新哲学的导向是将物理实体进行文本研究，这需要对人工造物文本语言进行研究。他将这种哲学称为“反事实哲学”或者是“思辨哲学”。这样结合的研究需要数据和元数据。德里斯科尔需要物理实体综合性表述，当文本需要提供解释时，使用者就要追本溯源，但麻烦是密码学并不支持二进制的表述。人工造物完全依照编辑解释，那么阅读进程需要多维度测试吗？数字信息还不十分确定能否从人文学科的语料库和密码学历史中提取出来，因为从现代科技的角度看人文学科已经失去了传统学术地位的优势。

早期的密码学需要重新设计，需要在更广的范围内讨论学科、方法论和媒体。使用TEI P5进行重新编码，重新植入数字化的进程得到了考古

学和艺术史的支持，提供了三维操作界面，支持各类手写工具，并且它可以依照人造数字产品密码规律展示，并不仅是简单的物体造像。这种方法顾虑在文本的组建和阅读阶段进行解码，分析的文本包括了文学、语言、考古、文化，甚至数学层面。数字化重新设计必须支持频率分析，也包括一些硬件设备，如相关器、显示设备、内置翻译器等等。这样的工程是开放式的，社交网络、众包、专家及初学者解读都包含在其中。除了这些交流形式，人造密码的网络形式还提供类似DM工程式的动态文本注释。现代密码学的数字化引导人文学者以自己的方式阅读加密文本，包括以历史、文化甚至是模糊性的方式阅读。

三、数字人文的非传统写作方式

20世纪末的人文学者对于不熟悉科技的内在结构并不会感到羞耻。这个后遗症恐怕要归结于17世纪密码学先驱莫兰和威尔金斯缺乏全球化知识分享的精神。1685年，约翰·福尔康纳（J. Falconer）在《密码学》（*Cryptography*）前言中指出，密码技术揭示了解码并非是依靠证据密钥进行的，在当时的时间阶段学科划分不清，密码工作者停止了学科多元化的思考，并且将这一技术独自归纳在计算领域。福尔康纳认识到了威尔金斯的短板，但是对于印刷技术的进步并未留意，他只使用简单的罗马字母和斜线字体进行密码表述，对威尔金斯的凸版印刷和塑形技术忽略不见。所以导致了威尔金斯的著作只保留单一形式，缺乏了多态塑形的可能。因此他自己在编码的时候插入物理实体的办法是失败的。

科学史家约翰·亨利（J. Henry）曾说系统碎片化在17世纪看来是神秘的，[9] 而密码学就是这样神秘的学科，它吸收了自然科学的知识，并且在方法和实践上处于各个学科的边缘。在20世纪和21世纪之交的时候，传统认知学科划分的导向受到了指责，各个学科开始专门化，很难相信一个人文学者可以从事外科手术、计算机编码、数据检索等等类似的工作。人文艺术在这些领域完全被废止了，只保留了一些历史遗迹。霍伊泽尔（R. Heuser）的问题直击人们的心灵“数字人文难道只是现代科学在人文领域的殖民地吗？”[10]

如果参看密码学的发展历史就可以得出答案，不是这样的。密码学对于自然科学保持了专注，但是方法论和学术传统依然来自于人文学科。解码技术取得突破性进展就可以为此提供证据。2012年布朗大学的研究团队根据前任图书馆长爱德华·威德默（E. Widmer）的指导下解密了罗杰·威廉斯（R. Williams）的速记法，这份文本是记录罗德岛17世纪历史的关键文本。在计算机频率分析领域，计算机科学专业的学生梅森·布朗（M. Brown）研究了17世纪速记法，并且使用了计算机相似系统。南加州大学的凯文·奈特（K. Knight）研究了18世纪德国社会的加密文档，他像梅森·布朗一样使用了计算机频率分析系统分析符号和句式，但是18世纪的语句却不能通过计算机进行测试。字母特征无法使用计算机系统识别，文本中的信息使用几何符号进行加密。它们只是形似于现在的德国字母，但意义完全不同。凯文·奈特只能借助于手写形式与文本手册阅读的方式来描述这些加密符号的特征，手写的方式配合脑力工作取得了突破性进展。这为研究密码史和相关科学史提供了新的思路，当符号不能数字化表述的时候，计算机系统将失去效力。这就给人们带来了启示，人工造物的加密工作必须以多维度形式编码，这里有机器工作发挥效应也有手工编码参与其中，所以计算机必须开发新的软件编辑语言。这些案例不仅强调了手工工作数字化，也强调了人文学科对于密码学的支持。

对于密码学这种特殊的写入形式，设密与解密就成为了对应的写作与阅读方式。我国学者较早注意到了这种特殊方式，并注重研究其在计算机以及网络技术层面的应用，这其中军事领域研究较多。秦嘉海1979年较早地介绍了现代密码学专家惠特菲尔德·迪菲（W. Diffie）的成果。[11] 随着社会信息化的进步，密码学也由军事领域逐步扩大至民用领域，特别是2006年以后，依据赵仁玲的密码学文献分析，呈现了跨学科研究的趋势。[12] 对于密码学人文方向的研究我国以人物传记为主，介绍较多的是肖国镇与王小云两位专家。难能可贵的是曾恳诚较早进行了密码学的科普介绍，[13] 鲍振东进行了密码学史的划分，分为密码学起源、发展、现代、新方向四个时期。[14] 目前，计算机密码学在分组密码、序列密码、公钥密码、混沌密码等方面研究都有新进展，但是人文学科方面的渗透研究还比较缺乏。

四、评价及展望

通过本文梳理计算机密码学的早期发展历史，可以反映英国学者乃至学术界对于人文学科和自然科学的认知态度，脑力工作和手工工作结合是其生产方式，多学科融合是发展的方向。这对于人们进一步发展密码学以及认知科学的整体态度有启发作用，人工造物文化的展现方式也体现这一积极意义。

密码学未来的发展要遵循17世纪打破学科划分的状态，以多维度的形式保持机械工作和手工技巧以及人脑智能的结合运作。麦克甘曾强调在创造实用的未来过程中，人类文化的记录是综合性、稳定性、可获取性的。这等于是在重述17世纪传统学术的固有观点。威尔金斯和皇家学会仔细考虑了学术信息如何传播，如何被大众分享的问题。从某种角度来说，数字人文是寻找一种全世界通用语言的集合，设定了一种标准跨越学术疆界并且适应创造密码者的初衷，但是这并不同于威尔金斯及其他皇家协会成员的世界语言目标。威尔金斯对使用人文艺术并不质疑，并且他对于历史、哲学、修辞学十分欣赏，认为自然科学和技术可以成为其有益补充。尽管这样的举措在今天试图拯救人文学科是徒劳的，但是他是当之无愧为高等教育学科划分辩护的人。他在牛津大学创造的国际交流部是成功的，并且防止了偏激的宗教改革。现代早期的数字人文就是从他和他的密码学研究中汲取的营养。他的那些速记式加密、密码手册和信息使用系统以及将这些嵌入至计算模型的研究都颠覆了传统的存储和检索领域。当今时代这样的融合多学科项目还在持续得到关注，密码学的发展也刺激了科学家、人文学者以及数学家们的多维度思考，关于密码学形而上学的研究反映了人们理解人工造物文化的方式。

［参 考 文 献］

[1]Aarsleff, H. *John Wilkins and 17th-Century Linguistics*[M]. Amsterdam: John Benjamins, 1992, 3–44.

[2]Bono, J. *The Word of God and the Languages of Man: Interpreting Nature in Early Modern Science and Medicine*[M]. Madison: University of Wisconsin Press, 1995, 19–59.

[3]邓勇进. 古典密码学[J]. 硅谷, 2011,(7): 14.

[4]张红、周尚波. 混沌理论在密码学中的应用[J]. 重庆大学学报, 2004,(4): 39–43.

[5]Winston, C. *Marlborough His Life And Times*[M]. Chicago: University of Chicago Press, 2002.

[6]Cohen, D. 'Intelligence Analysts and Humanities Scholars'[EB/OL]. http://hdl.handle.net/1920/6051/.2006–11–13.

[7]Heuser, R. 'Learning to Read Data: Bringing Out the Humanistic in the Digital Humanities'[J]. *An Interdisciplinary Journal of Social, Political, and Cultural Studies*, 2011, 54(1): 79–86.

[8]McGann, J. 'On Creating a Usable Future'[J]. *Profession*, 2011, (1): 82–95.

[9]Henry, J. 'The Fragmentation of Renaissance Occultism and the Decline of Magic'[J]. *History of Science*, 2008, 46(1): 1–48.

[10]Knight, K. 'The Secrets of the Copiale Cipher'[J]. *Journal for Research into Freemasonry and Fraternalism*, 2012, (2): 14–24.

[11]秦嘉海. 密码学介绍: 保密和验证[J]. 通信保密, 1979,(6): 1–46.

[12]赵仁玲. 对密码学文献的定量分析[J]. 情报科学, 2006,(11): 1738–1742.

[13]曾恳诚. 密码学[J]. 科学学与科学技术管理, 1988,(6): 40–41.

[14]鲍振东. 密码技术的回顾和展望[J]. 自然杂志, 1988,(1): 9–15.

［责任编辑　王大明　柯遵科］