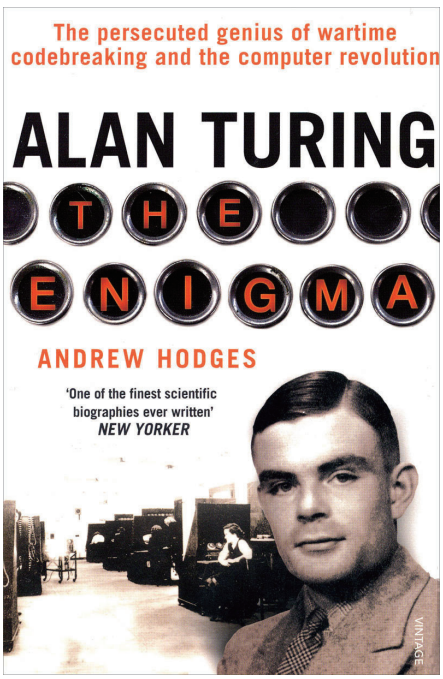
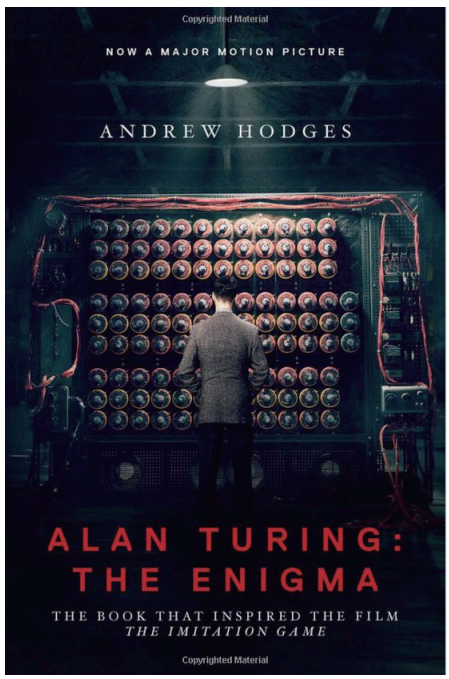
一位密码破译者的回忆与思考[1]

Peter Hilton / 文　蔡春彦 韩广国 许丽卿 / 译

1. 引言





普林斯顿出版社分别于 2012 年和 2014 年出版的 *Alan Turing*: *The Enigma*

关于二战期间布莱切利庄园（Bletchley Park，二战期间英国政府的密码破译基地）的工作，现在已经出版了很多书籍。其中，优秀的一本书是 Andrew Hodges 著的 *Alan Turing*: *The Enigma*。这是一本非常有教育意义的传记，讲述了一个对二战胜利和计算机的发明做出杰出贡献的天才。另外一本书是 Francis Harry Hinsley 和 Alan Stripp 著的 *Codebreakers*，该书编辑了一系列的小文章对布莱切利庄园里破译者使用的破译方法做了详细介绍。在这些系列文章中，最值得一提的是由 Irving Jake Good 写的题为 *Enigma and Fish* 的文章[2]。在文中，Irving Jake Good 作为解码团队[3]的核心成员，具体描述了德国人使用的密码机和我们所开发的解密机，用于破译德国密码机所加密的信息。这些内容直到最近才由政府解密得以让公众知晓，也正是由于像 Jack Good 这样有能力的人，对这些密码机和我们所用的方法进行了精确的描述。

[1] David Joyner, Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory, Springer, 1999.11, Pages1-8.

[2] Enigma，一般翻译为恩尼格玛密码，和 Fish 同为二战时德国使用的密码。

[3] 起初解密海军恩尼格玛密码，而后解密更为复杂的 Geheimschreiber 密码，即我们所称的 Fish 密码。

既然有如此多的优质信息资源可用，再写一篇技术文章似乎没有意义。但是，关于我们在布莱切利庄园的活动更私人感受的一面，可获得的此类信息资源并非如此丰富。因此，也许此文可以弥补这个空白。当然，我仅从自己的角度讲述。同 Jack Good 一样，我刚入职时从事海军恩尼格玛破译工作（1942 年），继而研究 Fish 密码直至欧战结束（1945 年 5 月）。但我曾有一段时间，也就是 1942 年底至 1943 年初，当我退出恩尼格玛解密团队后，我加入了致力于推断 Geheimschreiber 密码加密机运行模式的研究小组。我当时隶属于 Testery，不过仍和 Newmanry 联络[4]。Testery 的研究人员大多数使用手工方法破译，也就是说，他们自己不使用巨人机。但是，他们通常应用巨人机的输出来完成高效率的解密。当时，Newmanry 部门负责管理巨人机。

尽管这些回忆是非正式的和私人的，但我必须强调的是，我所隶属的团队致力于破译的是德国军队和外交上绝密级的密码。我相信那些破译初级密码的人不能感受到与我们同等的兴奋；我也确信，那些仅在信息解密后参与进来的人们跟我们的感受也完全不同。

那么关于那些日子的生动记忆是怎样的呢？让我从入伍开始说起吧。

2. 走向布莱切利庄园之路

众所周知，在 1941 年 10 月，布莱切利庄园包括 Alan Turing 在内的四位顶尖密码专家，曾写信给丘吉尔首相，提议授与布莱切利庄园对破译者选聘人员和必要设备供应的最高优先权。丘吉尔完全可以很官僚地回复这封信，经由白厅[5]按规程处理，但是他没有这么做。他认识到这个提议的良好判断力和紧迫性，于是，他命令参谋长“马上行动”。因此，就有了后来的一幕（虽然我当时并不知道这些）。1941 年 11 月，一个面试委员会来到牛津大学寻找“具备当代欧洲语言知识的数学家”。（然而，由于安全的原因，规定要求，不得告知候选人他们即将从事的工作的性质。让我印象最深刻的是，面试委员会成员自己也并不了解实情。）

当时的英国教育体制是基于过早专业化的原则。这实际上导致了不太可能有合适的人选。当然，除了偶然的例外[6]。

我的导师推荐我参加面试。尽管我不是数学家，而仅是一个数学系研究生。而且我只会一点基础的德语，因为我仅自学了一年[7]。

结果我是唯一候选人，并立刻在外交部得到了一个职位。然而，强制的条件是我必须 1942 年 1 月入伍。这给我当头一棒。由于我的年龄原因（我生于 1923 年），只有到 1942 年 8 月后，我才能应征入伍。但是，在牛津大学学生时代在皇家炮兵队军训的经历（所有大学生都得参加军训）使我坚信，如果被征召进入皇家炮兵队，我几乎肯定会很年轻时就死掉，那样的话就没意思了。因此，我马上决定，无论在布莱切利庄园从事何种秘密工作，那肯定都会比成为一个炮兵更有趣。尽管我惋惜错过了在牛津的两个学期的学习，但这个牺牲肯定是值得的。这是多么正确的决定！

于是，1942 年 1 月 12 日，我出现在了布莱切利庄园的大门口，并被人送到了小屋 8 号[8]。那天，我认识了许多人，但仍然没弄清楚工作的性质。我遇到的其中一人正是 Turing 本人。他问我是否会玩国际象棋和填字游戏，在得到我的肯定回答后，告诉了我一个他还没解决的象棋难题并邀请我帮他解决。很幸运我解决了。后来，我总是将在 Turing 悲剧短暂的生命[9]里与他建立的真挚友谊归因于这次幸运的初见。第二天，我被安排参与到海军恩尼格玛密码机的破译工作中，尤其是军官间高级机密信息。我获得了第一个命令，用小屋 8 号密码专家小组发明的精妙的方法破译这些密码，这达到了惊人的成功率和速度。我生命中独一无二的激动时刻开始啦！

[4] 这里 Testery 和 Newmanry 都是破译中心的部门名。

[5] 英国政府

[6] 来自德国和澳大利亚的犹太难民中有很多杰出的数学家，但他们被看作敌国公民而不受信任。

[7] 勿容置疑，德语是上述的“现代欧洲语言”。

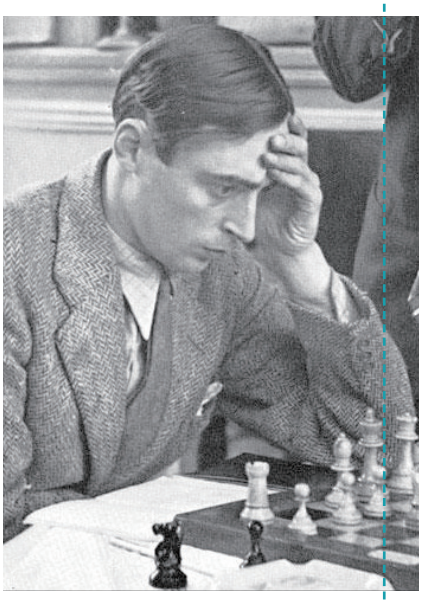
[8] Hut 8，布莱切利庄园的一个部门，专门对使用于海军的恩尼格玛密码机系统进行破译。

[9] 1954 年，在刚过完 42 周岁生日不久，Turing 自杀身亡。

3. 向我的同事致敬

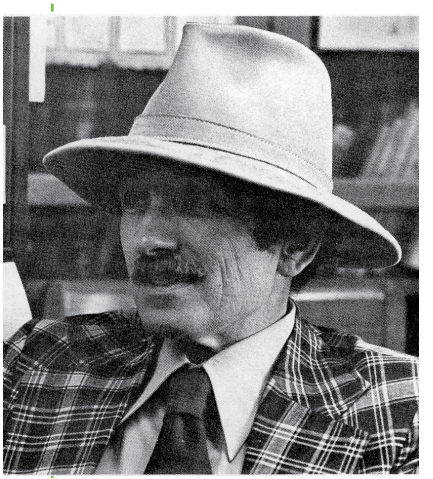
在布莱切利庄园，不言而喻，我的同事们都格外擅长他们的战时工作。他们都聪明、敏捷、有创造力，工作非常卖力且经常互相鼓励。二战后，几乎所有人都恢复或继续从事学术研究工作，尽管有些人选择了不同的领域[10]。

挑出任何同事特别颂扬或恭维，都是不合适的。我认为从他们所表现的各方面的特征（无论是共同的还是个性的），以及他们的数学天赋，我都限定在这七人之中吧。为了避免有意地偏袒，我将按字母顺序提及。这些人都对我影响深远，且其中的大部分人在战后也继续影响着我。



Hugh Alexander（1909-1974），他是英国的国际象棋冠军。一个非常丰富多彩的人，拥有迷人的个性和惊人的智慧。在小屋 8 号的早期工作中，他和 Shaun Wylie 在海军恩尼格玛密码和破译问题上教给了我许多知识。他当时主管我们部门，除了我刚才提及的这些特质和他的幽默感，那时最打动我的，就是他完全不拘礼节和大公无私。在同事们中，我认为这些是他最显著的特征。遗憾的是，在我离开小屋 8 号后就很少见到他了。

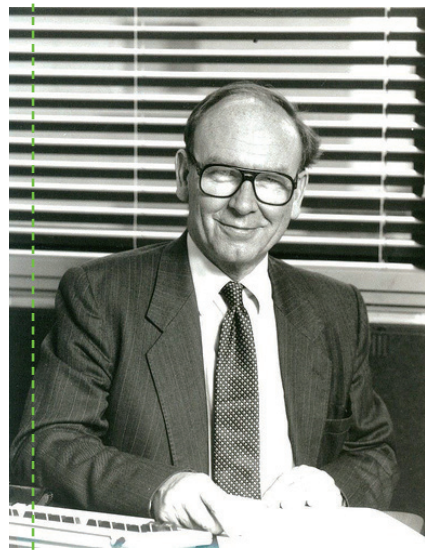
Jack Good（1916-2009）[11] 是我们中最接近于应用数学家的学者（我后面还将提到这一点）。实际上，他是概率学家，但他无论过去或者现在都是一个数学全才。在小屋 8 号和 Newmanry 工作时，无论是在解密还是在想法上，他都是非常高效和多产的。他拥有惊人的完全准确的记忆力，这使得他成为关于那段历史事件的最可信最综合的权威。他所拥有的很久以前的那些英雄们的特质——非常独特的幽默感和谦逊，滋养了我们的友谊，并持续到了今天。



[10] 一位是 Roy Jenkins, 后当选国会议员，曾任工党政府的内政大臣、牛津大学校长。另一位是 Peter Benenson，他倡导成立了国际特赦组织。

[11] Jack Good，弗吉尼亚理工学院荣休杰出大学教授（Emeritus University Distinguished Professor）。

Donald Michie（1923-2007）[12]，他是官方招聘来的人中一个很有天赋的典型例子。他以一个典型的学者的身份来到 Testery(尽管他也和 Newmanry 有非常密切的联系)，但是他对我们的工作表现出了非凡的适应性。尽管他对数学知之甚少，但是他具有良好的数学思维能力。他曾经是，而且仍然是真正才华横溢的人。他成为 Turing，Jack Good，我，以及其他许多人非常亲密的朋友。他开朗的性格，他的求知欲，连同他迅速处理问题的非凡能力，使他成为难能可贵的同事。当他从典型的学者转变成理论计算机科学大师时，他的政治立场同时由右倾转变为左倾。这或许不是巧合（对他而言是非常理性的转变）。



Max Newman（1897-1984），在他来到布莱切利庄园领导一个部门，负责 Fish 密码的解密机器方面的工作时，就已经是一个著名的拓扑学家了。到 1943 年为止，Fish 密码显然是德国军队使用的最重要的高级密码。他这个角色在解密工作中起到了很大作用。二战后，他和复员回到曼彻斯特大学的 Turing 建立了工作关系。在 Ferranti[13]，他们连同大学的电器工程师以及其他人，设计并建造了一台计算机 [14]。1948 年 Turing 和我都加入了他的部门——不过以不同的资历水平。

Max 在数学和行政管理上都有很好的想法，但首先让我记住他是因为他是一个协调者。无论是在 Newmanry 还是曼彻斯特大学数学系，他营造的工作环境使同事们发挥出最好的工作状态。他绝不会仅仅因为所谓的官僚主义理由而给我们施加杂务。在工作过的这两个地方，他的理解和领导都使我受益匪浅。关于 Newman 的更多评论可以参见 *Codebreakers*。

[12] Donald Michie，二战后曾出任爱丁堡大学机器智能与感知研究中心主任，并于 1983 年与他人合作发起创立了图灵研究所。

[13] 一家英国的电气工程与设备公司。

[14] 在 1945 年，Max 离开布莱切利庄园后，被聘任为曼彻斯特大学纯粹数学专业的 Fielden 讲座教授。