不务正业的在线期刊　　微信可检索到的期刊

卧村密码学报

Journal of WoCrypt

第 4 期

2019 年 3 月

作者:
刘巍然，段立，罗宁

谈（公钥）密码学入门材料*

刘巍然[1]，段立[2]，罗宁[3]

[1](知乎昵称：刘巍然-学酥，https://www.zhihu.com/people/liu-wei-ran-8-34)
[2](知乎昵称：玄星，https://www.zhihu.com/people/xuan-xing-29)
[3](知乎昵称：是不懂啊，https://www.zhihu.com/people/woods-84)
通讯作者：刘巍然, E-mail: footman_900217@126.com
通讯作者：段立, E-mail: liduan@mail.upb.de
通讯作者：罗宁, E-mail: nluo.sdu@gmail.com

摘 要：在刚开始进入一个领域时，入门材料的选择会对今后的学习与研究带来巨大的影响。好的入门材料深入浅出、引人入胜，不仅介绍了必要的知识和方法，还会引发读者学习的兴趣；反之，不适当的入门材料或者难度较大、或者过于抽象，会让读者产生挫败感。本文针对初入（公钥）密码领域的研究人员在阅读材料选择和甄别方面的先天不足问题，基于作者的学习经验，采用了分级、分类的方式，提纲挈领式地分析并推介一些入门素材以及学习心得，希望能引导初学者更高效地捕捉到密码学习的有效路径。本文的目标读者是初入公钥密码学领域的研究人员。此外，大部分基础材料适用于初入对称密码学、应用密码学、隐私保护基础领域的研究人员。

关键词：密码学；公开课；教材和书籍；入门论文；

---

* 开搞时间: 2019-03-02; 搞完时间: 2019-03-27;

1 引言

刚开始进入一个领域时，入门材料的选择非常重要。密码学是一个数学、计算机、电子信息的交叉学科。具有数学背景的同学往往无法理解计算复杂度、数据结构与算法等计算机学科的相关知识，在面对安全性证明、原型系统实现时会一筹莫展；具有计算机背景的同学可能会受困于群论、格等相对复杂的数学理论，在设计密码学方案时毫无办法；具有电子信息背景的同学虽具有两个学科的背景知识，但无论从深度还是从广度看，背景知识的掌握可能无法达到要求。如果没有掌握必要的基础知识，在阅读密码学论文，特别是三大密码学顶级会议（CRYPTO、EUROCRYPT、ASIACRYPT）和四大安全类会议（Security & Privacy、USENIX Security、CCS、NDSS）论文时或许会遇到困难，如难以理解约定俗成的符号表示，难以适应相关知识点的描述方式。在理解密码学概念时，背景知识的欠缺也可能导致理解出现偏差或错误，而这些最终会反应到所撰写的论文中。如果基本的定义描述出现偏差或错误，审稿人有理由相信论文中可能存在更严重的错误，对论文产生负面印象，甚至导致拒稿。

我们给出一个例子来说明这个问题。为了推广差分隐私（Differential Privacy）技术，差分隐私定义的提出者，微软研究院 Cynthia Dwork 研究员与美国宾夕法尼亚大学的助理教授 Aaron Roth 撰写了一本名为《The Algorithmic Foundations of Differential Privacy》的书籍[22]。此书给出的差分隐私定义如下：

定义 1（差分隐私） 给定一个定义在$\mathbb{N}^{|x|}$上的随机化算法$\mathcal{M}$，如果对于所有的$\mathcal{S} \subseteq \text{Range}(\mathcal{M})$，以及所有满足$\|x-y\|_1 \leq 1$的输入$x, y \in \mathbb{N}^{|x|}$：

$$Pr[\mathcal{M}(x) \in \mathcal{S}] \leq e^{\epsilon} \cdot Pr[\mathcal{M}(y) \in \mathcal{S}] + \delta$$

则称随机化算法$\mathcal{M}$满足(ϵ, δ)-差分隐私性。

这个定义看上去非常简单，但如果深入剖析就会发现其非常严谨：

算法$\mathcal{M}$定义为一个随机化算法，而不是定义为算法；$\mathcal{S}$的定义写为$\mathcal{S} \subseteq \text{Range}(\mathcal{M})$，而非写为$\mathcal{S} \in \text{Range}(\mathcal{M})$。如果缺乏相应的基础知识，则这些细微的差别会导致对定义产生错误的理解。

有位老师曾提到：想要学成下山独立写论文，至少需要花费一整年的时间（每天 10 个小时）[85]。既然已经决定要研究密码学领域，花费一整年的时间学习基础知识是必要的。然而，应该如何花费这一整年的时间高效地完成基础知识的学习？在知乎上，我们时常收到私信或回答邀请，询问是否可以推荐一些密码学入门材料。我们在本篇文章就尝试介绍相关入门材料，以供参考。

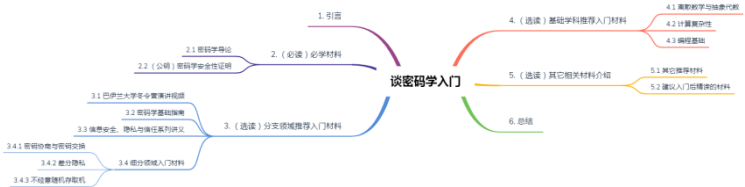

图 1：全文概览

由于作者水平有限，所能接触到的材料主要涉及公钥密码学和部分隐私保护技术，因此本文主要关注此方面的入门材料。某位研究对称加密侧信道攻击的博士研究生指出，如果主要研究方向为对称密码学的攻击领域，本文所介绍的大部分基础材料仍然适用，特此注明。

本文组织结构如下。第二章将介绍一些必学材料。无论未来将要研究（公钥）密码学的哪一个领域，都需要浏览这些必学材料，掌握必备的基础知识。第三章将介绍一些高质量的密码学分支领域入门材料，这些入门材料可以帮助我们快速了解核心思想，快速定位必读论文。第四章将介绍密码学关联学科的入门材料，如抽象代数、计算复杂性原理、数据结构与算法等。第五章将包含一些零散的意见和建议，如我们熟知领域的一些入门论文，部分难度较大、不适于入门的材料。第六章将对全文进行总结。图 1 为全文内容概览。

2 必学材料

当我们以在三大密码学会议或四大信息安全会议上发表论文为核心目标，从导师或者师兄师姐处得到密码学科研之路的第一篇学术论文，兴致勃勃地打印出论文并毫无阻碍地读完引言部分，信心满满地准备开始自己的科研之路时，我们可能会突然发现：从论文的预备知识部分就开始读不懂了。举个例子，为了帮助密码学研究者理解仿真证明技术，Yehuda Lindell 教授于 2018 年发布了一篇题目为《How To Simulate It – A Tutorial on the Simulation Proof Technique》的文章[53]。在相对轻松地阅读完引言后，我们在第二章，也就是预备知识和符号表示部分，遇到了这篇“指南”的第一个定义：计算不可区分性。下方的**定义 2** 为翻译结果，我们建议直接阅读原文的描述。

定义 2（计算不可区分性） 一个**概率总体**$X=\{X(a,n)\}_{a\in\{0,1\}^*;n\in\mathbb{N}}$是一个无穷随机变量序列，对应的索引为$a\in\{0,1\}^*$和$n\in\mathbb{N}$。在安全多方计算场景下，$a$表示参与方的输入，$n$表示安全参数。给定两个概率总体$X=\{X(a,n)\}_{a\in\{0,1\}^*;n\in\mathbb{N}}$和$Y=\{Y(a,n)\}_{a\in\{0,1\}^*;n\in\mathbb{N}}$，如果对于所有非均匀多项式时间算法$D$，存在一个可忽略函数$\mu(n)$，使得对于所有的$a\in\{0,1\}^*$和所有的$n\in\mathbb{N}$：

$$\left|Pr\left[D\left(X(a,n)\right)=1\right]-Pr\left[D\left(Y(a,n)\right)=1\right]\right|\leq\mu(n)$$

则称这两个概率总体**计算不可区分**，表示为$X\equiv Y$。

什么是随机变量序列的索引？怎么理解安全参数？什么是非均匀多项式时间算法？开始时我们或许认为可能是自己的英语功底不够，无法熟练地阅读专业英语材料。然而，即使是翻译成母语，这段话也我们来说可能也完全不知所云。理解这些定义需要一定的基础知识。在时间有限的条件下，我们可以查阅维基百科快速了解相关的定义内容。但是，如果想在以后的研究过程中走得更长、走得更稳，有必要深入理解这些定义的内涵。否则，总有一天我们会不得不回过头来重新补充那些当时我们没有认真探究的知识。

本章我们着重解决基础知识问题，推荐必学公开课和必学教材。公开课对基础知识的学习带来很大的帮助：（1）每节公开课的时长相对固定，这可以帮助我们合理安排时间，制定相应的学习计划；（2）可以将公开课看作教材的索引，帮助我们定位知识点，加深理解；（3）与阅读教材相比，观看公开课相对可能更有趣一些。优质的教材会帮助我们建立正确的密码学思维方式，了解约定俗成的符号定义和描述方法，为阅读论文扫清障碍。如果推荐的材料有对应的中文翻译版本，我们会进行注明。如果中文翻译材料为书籍，我们一并给出豆瓣读书的评分。如果感觉直接使用英文材料较为困难，可以先阅读对应的中文翻译版本。但我们想强调的是，早晚有一天我们需要阅读和撰写英文论文。因此，不如对自己狠一点，直接阅读英文教材。

2.1 密码学导论

说到密码学导论，必须要推荐 Dan Boneh 教授的公开课“Cryptography I”[10]。虽然目前只推出了第一部分，但这门课程已经包含密码学中常见概念的介绍，包括 Stream Cipher、Block Cipher、Message Integrity、Authenticated Encryption、Basic Key Exchange、以及 Public-Key Encryption。这门课程可以极大地提高我们的英语听力水平。Dan Boneh 教授的语速如机关枪一般，这可能也是我们一直没有翻译巴伊兰大学冬令营《密码学中的双线性群》讲座视频的原因[35]：讲座的听写难度太大了。这门课程另外一个有意思的地方是每一部分的编程作业。学生需要通过编程的方式解决实际中的密码学问题，加深相关知识点的理解。例如，需要应用 Padding Oracle Attack 破解用 Cipher Block Chaining（CBC）模式加密的密文；需要应用 Baby-Step-Giant-Step 法解决一个给定的离散对数问题；需要应用 Birthday Attack 得到一组前 50 比特哈希结果相同的消息。完成这些作业将帮助我们更好地理解相关的概念。

有关密码学导论的相关教材，我们必须要推荐 Jonathan Katz 教授

和 Yehuda Lindell 教授撰写的《Introduction to Modern Cryptography, 2nd Edition》[45]。这本书足够新，写得足够好、论述得足够深。最为重要的是，这本书通俗易懂地讲解了密码学的核心概念，以及安全性证明的核心思路。无论未来将从事哪方面密码学方向的研究，这本书都可以作为必读教材。如果想把里面的内容完全学懂学透，至少也需要 1 年至 2 年的时间。但我们认为，如果想在未来长期从事密码学的研究工作，这个时间的花费是必要的。遗憾的是，这本教材的第二版尚无中文版本。这本教材的第一版，即《现代密码学：原理与协议》（Introduction to Modern Cryptography: Principles and Protocols）[45]有对应的中文版本，由任伟老师翻译[47]，豆瓣读书尚无评分。

主讲“Cryptography I”公开课的 Dan Boneh 教授正在联合著名密码学家 Victor Shoup 教授撰写面向研究生的密码学教材《A Graduate Course in Applied Cryptography》[17]。这本教材与前面提到的《Introduction to Modern Cryptography, 2nd Edition》教材风格类似，但由于是面向研究生的教材，其难度相对会更大，安全性证明的描述更加全面。

2.2 （公钥）密码学安全性证明

研究公钥密码学相关领域，安全性证明是不可避免的门槛。正如 Yehuda Lindell 在文章《How To Simulate It – A Tutorial on the Simulation Proof Technique》的摘要中所描述：然而，构造仿真算法、应用仿真技术证明安全性，这不是一件简单的任务。绝大多数刚进入密码学领域的研究人员都认为这非常困难[53]。在此，我们推荐一些优秀的安全性证明阅读材料。希望这些材料可以帮助刚进入密码学领域的研究人员高效学习安全性证明的基本思想和基本方法。

实际上，通过密码学导论相关读物，我们已经或多或少地知晓了安全性证明的基本思路，也阅读到了一些密码学方案的安全性证明。但是，学习已有的证明是一方面，是否可以独立自主地撰写安全性证

明又是另一个难题。如果不知道如何为哪怕一个简单的方案撰写安全性证明，可以阅读 Victor Shoup 教授的论文《Sequences of Games: A Tool for Taming Complexity in Security Proofs》[75]。这篇论文不会让安全性证明变得简单，但是会讲解怎么更系统地整理证明思路，把细节一步步有调理的放在一串攻击者与仿真者的游戏里。读完里面关于 RSA 和 ElGamal 安全性证明的“改写”，会对原先的证明过程有全新认识。

如果仍然对安全性证明一筹莫展，可以考虑阅读 Fuchun Guo、Willy Susilo、Yi Mu 的著作《Introduction to Security Reduction》[32]。这本书最突出的特点是对几乎所有安全性证明写得非常好的方案进行了完整的讲解，如数字签名中随机预言模型下的 Boneh-Lynn-Shacham 方案[15]、标准模型下的 Boneh-Boyen 方案[13]；公钥加密方案中第一个选择密文安全的 Cramer-Shoup 方案[20]、第一个基于身份加密（Identity-Based Encryption，IBE）方案 Boneh-Franklin 方案[14]、标准模型下两个 IBE 方案 Waters 方案[83]和 Gentry 方案[26]。这几个方案所对应原始论文的安全性证明都写得非常清晰，建议精读。

特别要注意的是，很多论文都有会议版本和期刊版本。如果论文只有会议版本，作者一般也会将论文的扩展版本（或称完整版本）上传至国际密码学研究协会（International Association for Cryptologic Research，IACR）的网站上[1]。如果想精读一篇论文，建议寻找发表在 IACR 上的版本，此版本的内容可能会更加全面。

相对于加密方案或安全协议的安全性证明，我们更推荐先从数字签名方案的安全性证明入手。与加密方案和安全协议相比，数字签名方案的安全模型相对比较简单。数字签名方案的安全性一般依赖于计算性困难假设。与判定性困难假设相比，计算性困难假设更容易理解

[1] IACR 的官方网站是 www.iacr.org。此网站还会发布与密码学相关的众多资讯，强烈建议申请此网站的邮件订阅。

一些。建议阅读 Boneh-Lynn-Shacham 方案的会议版本[15]，因为会议版本是以逐个游戏迭代的模式撰写的，是一个学习此种证明方式的好论文，而期刊版本是以单个游戏的模式撰写的[16]。不可否认，期刊版本也是非常好的学习材料。强烈建议阅读 Boneh-Boyen 签名方案的期刊版本论文[13]。论文写得非常全面，作者几乎把所有能想到的点都写到了。从这篇论文可以领略顶级密码学家“走自己的路，让别人无路可走”的论文写作方法。

有关公钥加密方案的安全性证明，首先推荐 Cramer-Shoup 方案的论文[20]。相比于近些年来动辄数十页甚至上百页的论文来说，这篇论文的长度会短得多，阅读起来会显得轻松不少。这篇论文的安全性证明堪称范本，应用单个游戏的模式完成了安全性证明，描述非常清晰，很容易理解证明思路。有关逐个游戏迭代模式的安全性证明，推荐阅读 Lewko-Waters 方案论文[50]。这篇论文应用对偶证明方法，在合数阶双线性群下将 Boneh-Boyen-Goh 选择性安全（Selectively Secure）的层次基于身份加密（Hierarchical Identity-Based Encryption，HIBE）方案转换成了适应性安全（Adaptively Secure）的 HIBE 方案[12]。对偶证明方法需要以逐个游戏迭代模式完成证明，证明难度不大，但是符号特别多，可以尝试列举一下这篇论文一共使用了多少种不同的符号。

通用密码学协议（General Cryptographic Protocol）是为实现任意函数的计算，通过安全地组合各种密码学原语而形成的安全计算协议。有关通用密码学协议的安全性证明学习，我们推荐 Yehuda Lindell 的文章《How To Simulate It – A Tutorial on the Simulation Proof Technique》[53]。这是目前为止唯一一个针对密码学协议，以教程（Tutorial）的形式分析仿真安全性证明方法的文章。全文从半诚实攻击者攻击下安全的不经意传输协议（Oblivious Transfer Secure against Semi-Honest Adversary）这一最基础的协议开始，到混合模型下的证明（Security in Hybrid Model），再到顺序组合定理（Sequential

Composition Theorem）和针对恶意攻击者攻击的转换方法，最后在结尾简要介绍了通用组合性（Universal Composition）的概念，每一步的讲解都极尽精准和详细。但需要注意的是，这篇文章的阅读可能需要花费较长的时间。静下心来慢慢读、多读几遍，每一次阅读都一定会有新的收获。

3 分支领域推荐入门材料

学习完必学材料后，我们可能就会切入到具体的研究方向中，开展自己的密码学研究了。然而，每一个密码学领域或多或少都有一定的差异，对应的经典论文也不尽相同。如何快速把握某一分支领域的核心思想和关键论文就成为了接下来的难题。接下来，我们介绍一些可以快速了解密码学分支领域的材料。

3.1 巴伊兰大学冬令营演讲视频

讲到密码学分支领域，不得不提巴伊兰大学的密码学冬令营（BIU Winter School on Cryptography）。这可能是密码学研究者们为全世界带来的最佳密码学分支领域科普材料。自 2011 年起，以色列巴伊兰大学每年冬天都会选择一个密码学主题，邀请这个主题下全世界最著名的密码学家来到巴伊兰大学带来精彩的讲座。巴伊兰应用密码学和网络安全研究中心（The BIU Research Center on Applied Cryptography and Cyber Security）在 YouTube 上传了全部讲座的视频录像。可以在对应的官方网站上找到所有视频的幻灯片。

安全多方计算领域的两位著名学者 Yehuda Lindell 和 Benny Pinkas 在巴伊兰大学任职。因此，2011 年第一届密码学冬令营毫无悬念地选择了“Secure Computation And Efficiency”作为主题，举办时间为 2011 年 01 月 30 日至 2011 年 02 月 01 日[33]。由于这是第一年组织冬令营，此系列视频录制的质量相对较低，讲解的内容较为分散。

第二届密码学冬令营于 2012 年 02 月 19 日至 2019 年 02 月 22 日

召开，主题为“Lattice-Based Cryptography”。[34]此次冬令营邀请到了 Oded Regev（提出了著名密码学假设 Learning With Error[65]）、Chris Peikert（提出了基于格的陷门构造方法[63]，2019 年提出了基于格的非交互式零知识证明构造方法[62]）、Vadim Lyubashevshy（提出了理想格和理想格上的 Learning With Error 困难问题[56]）、以及 Craig Gentry（第一个全同态加密方案的构造者[25]）。巴伊兰大学后续组织的冬令营主题和举办时间列举如下。

- “Bilinear Pairing in Cryptography”[35]，2013 年 02 月 04 日至 2013 年 02 月 07 日。
- “Symmetric Encryption in Theory and in Practice”[36]，2014 年 01 月 27 日至 2014 年 01 月 30 日。
- “Advances in Practical Multiparty Computation”[37]，2015 年 02 月 15 日至 2015 年 02 月 19 日。
- “Cryptography in the Cloud – Verifiable Computation and Special Encryption”[38]，2016 年 01 月 04 日至 2016 年 01 月 07 日。
- “Differential Privacy: From Theory to Practice”[39]，2017 年 02 月 12 日至 2017 年 02 月 16 日。
- “Secret Key Exchange”[42]，2018 年 01 月 11 日至 2018 年 01 月 15 日。
- “Zero Knowledge”[49]，2019 年 02 月 18 日至 2019 年 02 月 19 日。

巴伊兰大学的密码学冬令营的讲座主题已经涵盖了密码学领域几乎所有的分支。相关视频也成为了密码学入门的宝贵资料。在多方的共同努力下，我们目前已经完成了“Lattice-Based Cryptography”全部视频、“Differential Privacy: From Theory to Practice”除博弈论外其余所有视频的听写和翻译工作。在 i 春秋的赞助下，“Lattice-Based Cryptography”视频已经发布在 i 春秋课程库中的《世界上最顶级的密码学课程》中[87]。由于尚未找到合适的视频发行方，“Differential Privacy: From Theory to Practice”尚未发布。当前，我们在进行

“Advances in Practical Multiparty Computation”视频的听写和翻译工作，但由于视频较长、难度较大，进度并不乐观。我们衷心希望对此有兴趣的密码学研究人员可以加入我们，共同翻译这一系列课程。

3.2 密码学基础指南

Oded Goldreich 教授是密码学先驱科学家，为密码学理论做出了卓越的贡献。他也指导出了大批优秀的密码学研究人员。为了纪念这位密码学先驱，他的学生们联合起来，于 2017 年撰写了一本有关高级密码学理论和计算复杂性的研究生教材，教材名称为《Tutorials on the Foundations of Cryptography》[54]。

这本教材涵盖了当前密码学的几大分支领域：安全多方计算中的乱码电路、公钥密码学、伪随机函数、单向函数、同态加密、仿真证明技术、差分隐私，对应的章节名称分别为：《Garbled Circuits as Randomized Encodings of Functions: a Primer》、《The Complexity of Public-Key Cryptography》、《Pseudorandom Functions: Three Decades Later》、《The Many Entropies in One-Way Functions》、《Homomorphic Encryption》、《How to Simulate It: A Tutorial on the Simulation Proof Technique》、《The Complexity of Differential Privacy》。前面多次提到的《How to Simulate It: A Tutorial on the Simulation Proof Technique》[53]就是这本教材的其中一个章节。这本教材偏向于密码学理论，涵盖了各个领域的基本思想、定义、当前主要研究成果。既然偏向于理论，这本教材的缺点是学习曲线比较陡峭。即使是《How to Simulate It: A Tutorial on the Simulation Proof Technique》[53]，读起来也并不轻松。但是，能够完整理解这本教材的撰写内容，会对后续的研究起到可观的促进作用。因此，我们仍然推荐密码学理论研究人员阅读这本教材。

3.3 信息安全、隐私与信任系列讲义

既然有面向理论研究人员的教材，也就必然有面向应用研究人员的教材。我们推荐 Elisa Bertino 和 Ravi Sandhu 主编的系列丛书

《Synthesis Lectures on Information Security, Privacy, and Trust》。这套系列丛书的目的是围绕信息安全、隐私和信任这一主题，为每一个网络安全分支领域推出一本 50 至 100 页的书籍。截至 2019 年 03 月，此系列书籍已经涵盖了异常检测、智能电网安全、区块链与密码货币、差分隐私、隐私风险分析、安全外包计算、数据库隐私、社交网络安全、RFID 安全、隐私信息检索、操作系统安全等多个领域。

目前，我们正在尝试翻译 Ninghui Li、Min Lyu、Dong Su、Weining Yang 老师撰写的《Differential Privacy: From Theory to Practice》[51]。这本书站在工程师的角度介绍了差分隐私的基本定义、基本概念，以及可以在数据库应用系统中可以使用的差分隐私技术。书籍中所介绍的技术并非来自于诸如 STOC、FOCS、TCC 等偏向于计算机理论的会议论文，而是来自于 SIGMOD、VLDB、ICDE 等数据库领域会议论文。由此可见，此书轻理论、重应用，是一本很不错的差分隐私分支领域阅读材料。遗憾的是，由于篇幅原因，这本书没有介绍(ϵ, δ)-差分隐私、图数据集差分隐私、本地差分隐私等内容。作者在引言部分指出，本书的第二卷将涵盖这些方面。

3.4 细分领域入门材料

密码学领域可以进一步细分为更为分支的研究方向，每一个研究方向又包含其独有的核心入门材料。本节，我们列举一些我们所熟知领域的优秀入门材料，仅供参考。

3.4.1 密钥协商与密钥交换

对于非通用密码学协议，尤其是认证密钥协商（Authenticated Key Exchange），更常见的仍是和加密方案类似、使用基于游戏的证明（Game-Based Proof）方法。对于已经学习过密码学基础的同学，我们推荐 Mihir Bellare、David Pointcheval 和 Philip Rogaway 撰写的论文《Authenticated Key Exchange Secure against Dictionary Attacks》[8]和 Tibor Jager、Florian Kohlar、Sven Schäge、Jörg Schwenk 撰写的论文

《On the Security of TLS-DHE in the Standard Model》[43]。推荐的首要原因是这两篇论文具有极高的易读性，所需要的前置知识只有判定性 Diffie-Hellman 假设（Decisional Diffie-Hellman Assumption）、哈希函数、伪随机函数（Pseudo-Random Function）和数字签名的安全概念。前者仔细剖析了如何通过定义参与方（Parties）、通信进程（Process | Session）、攻击者的能力（Queries）来定义一个密钥交换协议的执行环境（Exexution Environment），以及如何才算一个有效的攻击（Freshness、Forward Secrecy、Key Indistinguishability）。论文中提到的基于口令的密钥交换是以低熵值种子作为基础，通过互动逐步提升整体安全性的最佳例子之一。后者针对 TLS 1.2 这个应用最广泛的安全通信协议，扩展了前者的模型，定义了认证信道（Authenticated Channel）的概念。论文的完整版给出了极其详尽的安全性证明。

3.4.2 差分隐私

差分隐私属于隐私保护研究领域，但由于此技术具有严密的数学逻辑，可以通过形式化安全证明论述方案的隐私保护程度，因此差分隐私已经逐渐成为密码学领域中的一个独立的分支。

差分隐私最大的特点是入门门槛较高，此技术既包含了与公钥密码学类似的安全性证明技术，又包含了数理统计方面的内容。如果想入门差分隐私技术，建议直接阅读 Kunal Talwar 和 Frank McSherry 撰写的论文《Mechanism Design via Differential Privacy》[57]。这篇论文提出了差分隐私中最重要的机制之一，指数机制（Exponential Mechanism）。几乎所有ϵ-差分隐私机制都可以看成指数机制的特例，因此理解指数机制也意味着基本可以理解差分隐私的核心思想。本篇论文虽然发表在计算机领域顶级会议 FOCS 上，但论文的描述相对容易理解，但又不失严格，是一篇优秀的入门论文。如果仍然不能很好地理解差分隐私的概念，可以尝试阅读 Ninghui Li、Wahbeh H. Qardaji、Dong Su 等人的论文《Membership Privacy: A Unifying Framework for Privacy Definitions》[52]。此篇论文提出了成员隐私（Membership

Privacy）的定义。相比差分隐私，成员隐私应用先验概率和后验概率之间的关系描述隐私保护程度。这篇论文可以帮助我们从更广义的层面理解差分隐私。

差分隐私的一个重要定理是组合性定理（Composition Theorem）。组合性定理在隐私保护技术和数理统计之间建立了数学意义上的关联。建议直接阅读 Peter Kairouz、Oh Sewoong、Pramod Viswanath 撰写的论文《The Composition Theorem for Differential Privacy》[44]。这篇论文详细论述了差分隐私和假设检验之间的关系。阅读此篇论文不仅可以更深入的理解差分隐私，也可以理解差分隐私的另一个重要定义，(ϵ, δ)-差分隐私的概念，为研究差分隐私机器学习做好准备。

本地差分隐私（Local Differential Privacy）是差分隐私的另一大研究分支，主要关注于数据采集过程中的隐私保护技术。目前苹果和谷歌公司所使用的差分隐私技术就属于本地差分隐私的范畴。如果想系统地学习本地差分隐私技术，特别是理解苹果和谷歌公司所使用的本地差分隐私技术，可以阅读 Tianhao Wang、Jeremiah Blocki、Ninghui Li 等人的论文《Locally Differentially Private Protocols for Frequency Estimation》[82]。这篇论文详细讨论了应用本地差分隐私技术实现隐私保护频率估计的方法，并给出了不同场景下的最优解。

3.4.3 不经意随机存取机

加密方案通过加密信息的内容，也就是加密明文来实现信息保护；差分隐私则通过在计算的结果中加入噪音来实现个体信息保护；而不经意随机存取机（Oblivious Random Access Machine，ORAM）则是通过隐藏访问路径来实现信息保护。

对想了解 ORAM 的同学来说，建议从 Oded Goldreich 和 Rafail Ostrovsky 的论文《Software Protection and Simulation on Oblivious RAMs》[28]开始。这篇论文首次提出了 ORAM 的概念，虽然篇幅稍长，但无论是 RAM 模型（RAM Model）或者是不经意性（Obliviousness），论文中都给出了非常详细的定义和解释，即使是没

有相关基础的同学也可以直接上手。这篇论文用了较大的篇幅证明 ORAM 和软件保护（Software Protection）的等价关系，可以看情况决定是否直接跳过这一部分的内容。此外，这篇论文还给出了 ORAM 运行代价（Overhead）的下界及其证明，刚入门的同学了解结论即可。

单服务器（Single-Server）ORAM 的构造方案主要分为两大类：分级式的 ORAM（Hierarchical ORAM）方案和树状 ORAM（Tree Based ORAM）。《Software protection and simulation on oblivious RAMs》[28]中提出了分级式的 ORAM。很多后续方案也是在此基础上进行优化的。对于想要了解 ORAM 的同学来说，Emil Stefanov、Marten van Dijk、Elaine Shi 等人的《Path ORAM: An Extremely Simple Oblivious RAM Protocol》[81]是另外一篇必读的论文。Path ORAM 作为树状 ORAM 的一种，构造非常简单和经典，建议已有密码学基础的同学精读。

ORAM 的一个重要的应用是 RAM 模型下的安全多方计算。对这方面感兴趣的同学，建议在掌握了安全多方计算和 ORAM 的基础知识后，阅读 Samee Zahur、Xiao Wang、Mariana Raykova 等人的论文《Revisiting Square Root ORAM and Low Leakage Secure Boolean Queries》[84]。没有相关基础的同学，也可以先看一下 Mariana Raykova 在“The Alan Turing Institute”做的报告“Secure Computation with RAMs: Revisiting Square Root ORAM and Low Leakage Secure Boolean Queries”[64]，里面提到了一些生动的例子，可以帮助理解相关概念。

4 基础学科推荐入门材料

密码学是一门数学、计算机、通信领域的交叉学科。研究密码学，不可避免地要掌握这三个关联学科的基础知识。例如，密码学方案的构造离不开离散数学与抽象代数的应用；方案的安全性分析和计算复杂度分析要用到计算复杂度相关的知识；方案的实现需要一定的编程基础，如果仿真实现涉及到物联网、移动设备等特定的平台，则还需要一定的通信知识。

本章，我们尝试推荐一些基础学科的入门材料，主要为优质的公开课和教材。我们聚焦于离散数学与抽象代数、计算复杂性、编程基础这三门基础学科。它们是几乎所有密码学研究人员都需要了解和学习的领域。特定的密码学分支领域可能需要特定的入门知识。例如，隐私保护机器学习需要一定的机器学习基础知识；安全多方计算和同态加密需要一定的电路基础知识。由于能力有限，我们无法涵盖或逐一考察各个分支领域的入门材料。我们呼吁相关密码学研究人员可以分享出优质的入门材料。

4.1 离散数学与抽象代数

密码学的学习与研究离不开离散数学与抽象代数的知识。离散数学是抽象代数的基础，一般数学和计算机学院都会开设离散数学这门课程，但电子信息学院可能不会开设。进一步，可能只有数学学院会开设抽象代数课程，计算机学院和电子信息学院一般会开设编码理论。

如果需要学习离散数学，我们推荐阅读 AT&T 实验室 Kenneth H. Rosen 撰写的教材《Discrete Mathematics and Its Applications, Seventh Edition》[69]。这本教材已经由徐六通、杨娟、吴斌老师翻译并出版，教材名称为《离散数学及其应用，原书第 7 版》[70]。这是一本高中生都可以看懂的离散数学教材，里面包含了详尽的讲解、丰富的实例、大量的习题。屈婉玲、耿素云、张立昂老师所著的《离散数学（第 2 版）》也是相当优秀的教材[89]。教材的第 3 部分讲解了代数结构，第 6 部分讲解了初等数论，这两部分内容将对后续密码学数学基础的学习带来很大的帮助。在哔哩哔哩网站上可以找到屈婉玲老师讲解的“代数结构与组合数学”公开课视频[88]，相关评价非常正面。

与离散数学相比，抽象代数的学习就没有那么轻松了。我们推荐哈佛大学 Benedict Gross 教授的公开课“Abstract Algebra”[31]。Benedict Gross 教授的讲解激情四射，引人入胜，唯一的遗憾就是他的课堂笔记实在有一些凌乱。可以在网络上找到这门课程的笔记，这可能会对

学习有所帮助[1]。

我们推荐的抽象代数教材为麻省理工学院 Michael Artin 撰写的《Algebra, Second Edition》[3]。这也是 Benedict Gross 教授的公开课所使用的教材。这本教材已经由姚海楼、平艳茹老师翻译并出版，教材名称为《代数（原书第 2 版）》[4]。由于补充抽象代数的时间节点不太相同，我们对于这本教材的评价有一些初入。总体来说，学习这本教材需要一定的离散数学或抽象代数背景知识，不是特别适合零基础入门。换句话说，这本教材所讲解的内容已经大大超出密码学研究所需的知识。如果需要一本离散数学和抽象代数的中间教材，可以阅读 Joseph Silverman 撰写的《Friendly Introduction to Number Theory (4th Edition)》[77]。从书名就可以看出这本教材相比于《Algebra, Second Edition》会更适合入门一些。这本教材的中文版本《数论概论，第四版》由孙志伟、吴克俭、卢青林、曹惠琴老师翻译[78]，豆瓣读书评分为 9.2。这本书涵盖了初等数论直接用于密码学的所有部分，包含素数理论、费马小定理、二次剩余、椭圆曲线，可读性非常好。

4.2 计算复杂性

无论是方案的计算复杂性分析，还是密码学的安全理论，都需要用到计算复杂性的知识。理解计算复杂性的相关概念将对密码学的理解带来很大的帮助。

我们寻找了计算复杂性的相关公开课。经过对比，我们推荐来自卡耐基梅隆大学的 Ryan O'Donnel 教授的计算复杂性课程。Ryan O'Donnel 教授分别为本科生开设了课程“Undergraduate Complexity Theory”[59]，为研究生开设了课程“Graduate Computational Complexity Theory”[58]。这两门课程最大的区别是：本科生课程不讲解概率多

[1] 在此课程的官方网站上无法找到课程笔记，需要访问归档网页 http://wayback.archive-it.org/3671/20150528171650/https://www.extension.harvard.edu/open-learning-initiative/abstract-algebra 下载。

项式时间算法。由于密码学领域经常涉及这一概念，因此我们推荐直接学习研究生课程。当然，如果感觉难度比较大，也可以先学习本科生课程。可以在 YouTube 上找到课程的相关视频。在 YouTube 上还可以找到 Ryan O'Donnel 教授讲解的“Quantum Computation and Information”课程、以及“Analysis of Boolean Function”课程，如果需要也可以听一听。

我们推荐 Ryan O'Donnel 教授这两门公开课所使用的教材，分别是 Michael Sipser 撰写的《Introduction to the Theory of Computation，3rd Edition》[79] 以及 Sanjeev Arora 和 Boaz Barak 撰写的《Computational Complexity: A Modern Approach》[1]。前一本教材的中文版本由段磊、唐常杰等老师翻译[80]，豆瓣读书评分为 9.4。后一本教材的中文版本由骆吉州老师翻译[2]，豆瓣读书尚无评分。我们认为，《Computational Complexity: A Modern Approach》虽然足够优秀，但不太适合计算复杂性理论的初学者，其更像是一本专门为计算机复杂性理论研究人员撰写的专业教材。相比来说，《Introduction to the Theory of Computation，3rd Edition》更适合入门。可以配合北京大学刘田老师的视频课程“理论计算机科学基础”学习这本教材。在哔哩哔哩上可以观看相应的课程视频[86]。

4.3 编程基础

现在密码学领域越来越重视方案的具体实现，在论文中包含原型系统的实现并给出方案在实际环境下的执行情况，会为论文增光添彩。Ben Lynn 在斯坦福大学攻读博士学位时的研究方向就是双线性群映射的实现。他撰写的双线性映射密码学函数库 PBC Library 代码简洁、文档详尽、是密码学函数库的经典实现范例之一[55]。目前在 Visa 研究院担任科学家的 Peter Rindal 聚焦于密码学和安全计算方案的实现。他的 libOTe[66]和 libPSI[67]密码学函数库已被广泛应用。但我们想强调的是，如果是简单地研究方案在通用平台上的性能，密码学方案的

实现并不需要过于高深的编程能力。例如，如果阅读 John Bethencourt、Amit Sahai、Brent Waters 撰写的 cpabe toolkit 函数库，你会发现其代码的质量并没有想象得那么高。只要可以通过编程实现自己的方案就足够了。当然，密码学方案最佳编程实践也是密码学的一个分支研究领域，FSE 和 CHES 这两个会议专门收录针对各种方案最佳编程实践的论文。

有关编程的学习，可以在知乎平台搜索到大量的意见和建议。从编程语言的入门角度，如果完全没有任何编程基础，我们推荐阅读“Head First”系列教材。这本教材使用大量的图画完成知识的讲解，使得知识的学习就像阅读漫画一般轻松。仅从编程语言角度，这一系列教材的中文版本已经推出了：

- 《Head First Java》（豆瓣读书评分 8.7）[76]；
- 《Head First Python》（豆瓣读书评分 7.9）[5]；
- 《Head First HTML 与 CSS》（豆瓣读书评分 9.3）[68]；
- 《Head First Servlets & JSP》（豆瓣读书评分 8.8）[6]；
- 《Head First PHP & MySQL》（豆瓣读书评分 8.5）[7]；
- 《Head First C》（豆瓣读书评分 9.3）[30]；
- 《Head First HTML5 Programming》（豆瓣读书评分 8.5）[24]。

通过阅读“Head First”系列教材，可以在很短的时间内掌握编程语言的基本知识，达到快速上手的目的。

学习了编程语言的基本知识后，可能还需要掌握一定的数据结构与算法知识。我们只推荐一本教材，即 Robert Sedgewick 和 Kevin Wayne 撰写的《Algorithms, 4th Edition》[73]，中文版本由谢路云老师翻译[74]，豆瓣读书评分为 9.3。这本书既讲解了 Java 编程语言的基础知识，又讲解了数据结构，同时深入浅出地讲解了计算机科学中的 50 个经典算法，包含了 Java 语言的完整实现。同时，两位作者还在 Coursera 上面开设了对应的公开课“Algorithms, Part I”和“Algorithms, Part II”。课程讲解非常清晰，编程题目还可以帮助纠正代码中存在的

负面习惯。需要提醒的是，公开课中并不会介绍 Java 语言本身，因此在参加公开课前，最好阅读《Algorithms, 4th Edition》的第一章，快速学习 Java 编程语言。

5 其它相关材料介绍

5.1 其它推荐材料

前面的章节中，我们推荐了与密码学相关的公开课与教材。本节，我们列举其它一些或者有趣、或者对相应密码学领域有帮助的材料。

- 《An Introduction to Mathematical Cryptography》，Jeffery Hoffstein、Jill Pipher、Joseph Silverman 著[41]。第三位作者是前面章节提到的《数论概论，第四版》的作者。这本书用很容易理解的语言和实例讲解了各种用于解决因数分解和离散对数的算法。其中一部分算法可能在《现代密码学（第二版）》中看到过，但这本书里解释得更具体、更生动。这本书另外的一个亮点是，提供了格加密算法的清晰讲解和具体实例。
- 《Understanding Cryptography: A Textbook for Students and Practitioners》，Chirstof Paar、Jan Pelzl 等著[61]。这是一本什么都讲，什么都没讲完的“系统性书籍”。这本书的优点是对于私钥加密部分的理论和实现讲得非常具体，把 DES、AES、SHA-1 都从里到外“拆开”看了。如果研究方向是分组密码、哈希函数、伪随机函数，或者是侧信道攻击（Side-Channel Attack），这本书将会成为入门必读书。对应的进阶书籍是 Lars R. Knudesen 和 Matthew Robshaw 的《The Block Cipher Companion》[48]。
- “A Few Thoughts on Cryptographic Engineering”，Matthew Green[29]。著名密码学家 Matthew Green 的博客。他在博客中经常更新有关密码学的相关文章，尤其是当顶级会议出现了有趣的论文后，他会把一些想法放在博客中与读者们分享。如果教材、

论文读累了，可以读一读他的博客，很有意思。我们比较推荐的几篇博客：（1）“Hash-based Signatures: An Illustrated Primer”。图文并茂地解释了基于哈希签名的原理和优点。（2）“Zero Knowledge Prrofs: An Illustrated Primer”。这篇文章分为两个部分，形象解释了交互式零知识证明的原理和安全性证明方法。

5.2 建议入门后精读的材料

有些材料写得浅显易懂、引人入胜，而有些材料主要面向专业研究人员，内容相对晦涩难懂。下面是一些我们建议入门后精读的学习材料。下列材料入选的标准仅仅是“阅读难度远超标题的字面意思”。请注意，这些材料非常优秀且通常无法替代，但需要读者具备一定的背景知识，或对此领域具有较深的理解后才能更好地阅读。

- 《Foundations of Cryptography》，Oded Goldreich 著[27]。这本书是 Oded Goldreich 撰写的重量级著作，分为两卷，第一卷讲解基础工具，第二卷讲解基础应用。这本书适合资深科研人员，概念密度很大，表述略显精简，需要一句一句精读。这本书是入门时学习的必备辅助材料，尤其研究安全多方计算，这本书是不可或缺的。举例来说，在完成某项翻译工作时，我们对安全多方计算协议中的两类攻击者：半诚实/被动/诚实但好奇（Semi-Honest / Passive / Honest-but-Curious）攻击者、恶意/主动（Active / Malicious）攻击者进行了讨论。最初我们认为这些名词并不等价。后续我们发现，《Foundations of Cryptography》第二册的第 603 页指出，半诚实/被动/诚实但好奇表达的是相同的意思，而恶意/主动表达的是相同的意思。磨刀不误砍柴功，所有想避开的困难问题，最后都需要回过头来返工。因此，如果想脚踏实地的夯实基础，我们强烈建议学习《Foundations of Cryptography》这本书，解决遇到的所有问题。
- 《The Algorithmic Foundations of Differential Privacy》，Cynthia

Dwork、Aaron Roth 著[22]。虽然是差分隐私提出者 Cynthia Dwork 研究员本人亲自撰写的书籍，书籍的描述非常严谨、准确，但这本书的阅读难度非常大。建议直接阅读相应技术的论文，当在相关公式、引理、定理等的推导过程中遇到困难时，再尝试从这本书找到答案。

- 《Universally Composable Security: A New Paradigm for Cryptographic Protocols》，Ran Canetti 著[19][21]。只要研究密码学协议，就一定听说过广义可组合性（Universal Composition）。由于 UC 安全证明里涵盖环境（Environment）、参与方（Parties）、理想功能模块（Ideal Functionality，记为$\mathcal{F}$）、仿真者（Simulator）和攻击者（Adversary）这 5 类实体，并使用了：（1）多带互动图灵机作为基本计算模型；（2）带有三个限定量词（Quantifier）的两个序列来定义安全性；（3）多重标识（sid、ssid、qid）来标记一个会话（session），导致协议安全定义和安全模型的使用都过于复杂。UC 论文发表在 2001 年的计算机领域顶级会议 FOCS 上，而作者 Ran Canetti 即使在 2018 年 12 月仍然在修改这篇论文的完整版，也从侧面反映出这个模型的复杂程度。著名密码学家 Matthew Green 于 2018 年 12 月 13 日在推特上写到[1]：“如果我必须在‘可组合安全’和‘把自己的脸拍在木头板上’这两者间选择一个，而前者要求我理解 sid、ssid 和函数$\mathcal{F}_{schmoo}$，我会选择后者。”

6 总结

本文总结了经典的（公钥）密码学入门材料，初入密码学领域的研究人员可以参考给出的材料高效地学习密码学以及相关领域的知识，更快地度过入门阶段，投入到密码学的实际研究中。

[1] https://twitter.com/matthew_d_green/status/1073319905741733888

7 后记与致谢

感谢卧村密码学报的编委会对本篇文章的大力支持。感谢 Yu Chen 老师为本篇文章提供支持和帮助。感谢知乎数学领域优秀回答者王希对文章中出现的数学词汇提供了翻译建议。

感谢编委会的匿名审稿专家们为本篇文章提出中肯而细致建议，并进一步推荐了高质量的教材与书籍，使这篇文章变得更加优秀。由于我们无法短时间内精读这些教材与书籍，因此无法针对它们给出恰当、准确的推荐意见。我们将这些推荐材料列举在此。

某位研究通用密码学协议的老师推荐阅读 Carmit Hazay 和 Yehuda Lindell 的书籍《Efficient Secure Two-Party Protocols》[40]。这本书虽然只讲解两方安全计算，但是内容中涵盖了多方安全计算协议的正明思想。换句话说，这本书以两方安全计算为例讲解多方安全计算协议。我们找到了 Maria C. Onete 在 2013 年为这本书撰写的评语[60]。评语中的章节“你是否会推荐这本书？”（Would you recommend this book?）中写到：“如果你对可证明安全和安全多方计算感兴趣，尤其如果你是一个刚开始接触密码学领域的学生，我强烈推荐你阅读这本书。这本书不仅介绍了相关主题的内容，更是尝试教授一种新的方法来学习和分析密码学方案，即通过形式化描述对方案进行论述，但又不局限于形式化描述中。自顶向下的论述方法使学习曲线变得平滑。前述章节所用的术语会被频繁提及，保证读者顺利掌握相关概念。然而，如果你只对最新的协议和两方计算协议的应用感兴趣，这本书就不适合你了。这本书的目的并不是总结已有的协议，而是一个为困惑于可证明安全技术的读者所撰写的教学材料。”

反之，如果只对最新的协议和安全多方计算应用感兴趣，推荐阅读 David Evans、Vladimir Kolesnikov、Mike Rosulek 撰写的书籍《A Pragmatic Introduction to Secure Multi-Party Computation》[23]。这本书于 2018 年 10 月出版，其目的就是介绍目前最新的安全多方计算协议

和应用场景。这本书并不包含任何安全性证明，只有简单的安全性描述。目前我们正在翻译这本书籍。不久的将来，这本书籍的中文版本就会与读者见面。

某位从事密钥协商和密钥交换领域的老师推荐了 Colin Boyd 和 Anish Mathuria 的书籍《Protocols for Authentication and Key Establishment》[18]。从亚马逊官方网站用户“Plunkett”的评价看，希望学习或研究此领域的人员需要阅读此书籍。然而，这本书是 2013 年出版的，因此这本书无法覆盖最新的研究成果，可以作为参考资料阅读和学习。

参考文献

[1] Arora, S., Barak, B. Computational Complexity: A Modern Approach[M]. Cambridge University Press, 2009.

[2] Arora, S.等著, 骆吉州译. 计算复杂性：现代方法[M]. 机械工业出版社, 2016.

[3] Artin, M. Algebra (2nd edition)[M]. Pearson, 2010.

[4] Artin, M.著, 姚海楼等译. 代数（原书第 2 版）[M]. 机械工业出版社, 2015.

[5] Barry, P.著, 林琪等译. Head First Python（中文版）[M]. 中国电力出版社, 2012.

[6] Basham, B.等著, 苏钰函等译. Head First Servlets & JSP（中文版）[M]. 中国电力出版社, 2006.

[7] Beighley, L.等著, 苏金国等译. Head First PHP & MySQL（中文版）. 中国电力出版社, 2010.

[8] Bellare, M., Pointcheval, D., Rogaway, P. Authenticated Key Exchange Secure against Dictionary Attacks[C]. EUROCRYPT 2000, Springer, 139-155.

[9] Bethencourt, J., Sahai, A., Waters, B. Ciphertext-Policy Attribute-Based Encryption[EB/OL]. Advanced Crypto Software Collection, 2011. http://acsc.cs.utexas.edu/cpabe/. Access Date: 2019-03-21.

[10] Boneh, D. Cryptography I[EB/OL]. Coursera, 2012. https://www.coursera.org/learn/crypto. Access Date: 2019-03-03.

[11] Boneh, D. Cryptography II[EB/OL]. Coursera, 2012. https://www.coursera.org/learn/crypto2. Access Date: 2019-03-03.

[12] Boneh, D., Boyen, X, Goh, E. J. Hierarchical Identity Based Encryption with Constant Size Ciphertext[C]. EUROCRYPT 2005, 440-456.

[13] Boneh, D., Boyen, X. Short Signatures without Random Oracles and the SDH Assumption in Bilinear Groups[J]. Journal of Cryptology, 2008, 21(2): 149-177.

[14] Boneh, D., Franklin, M. Identity-Based Encryption from the Weil Pairing[C]. CRYPTO 2001, Springer, 213-229.

[15] Boneh, D., Lynn, B., Shacham, H. Short Signatures from the Weil Pairing[C]. ASIACRYPT 2001, Springer, 514–532.

[16] Boneh, D., Lynn, B., Shacham, H. Short Signatures from the Weil Pairing[J]. Journal of cryptology, 2004, 17(4): 297-319.

[17] Boneh, D., Shoup, V. A Graduate Crouse in Applied Cryptography[M]. Manuscript, 2017, https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_4.pdf.

[18] Boyd, C., Mathuria, A. Protocols for Authentication and Key Establishment[M]. Springer Science & Business Media, 2013.

[19] Canetti, R. Universally Composable Security: A New Paradigm for Cryptographic Protocols[C]. FOCS 2001, IEEE Computer Society, 136.

[20] Cramer, R., Shoup, V. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack[C], CRYPTO 1998, Springer, 13-25.

[21] Canetti, R. Universally Composable Security: A New Paradigm for Cryptographic Protocols[J]. IACR Cryptology ePrint Archive, 2000, 2000:067.

[22] Dwork, C., Roth, A. The Algorithmic Foundations of Differential Privacy[J]. Foundations and Trends in Theoretical Computer Science, 2014, 9(3–4): 211-407.

[23] Evans, D., Kolesnikov, V., Rosulek, M. A Pragmatic Introduction to Secure Multi-Party Computation[J]. Foundations and Trends in Privacy and Security, 2018, 2(2-3): 70-246.

[24] Freeman, E.等著，林琪等译. Head First HTML 5 Programming（中文版）. 中国电力出版社, 2012.

[25] Gentry, C. Fully Homomorphic Encryption Using Ideal Lattices[C]. STOC 2009, ACM, 9: 169-178.

[26] Gentry, C. Practical Identity-Based Encryption without Random Oracles[C]. EUROCRYPT 2006, Springer, 445-464.

[27] Goldreich, O. Foundations of Cryptography[M]. Cambridge University Press, 2009.

[28] Goldreich, O., Ostrovsky, R. Software Protection and Simulation on Oblivious RAMs[J]. Journal of the ACM, 1996, 34(3): 431-473.

[29] Green, M. A Few Thoughts on Cryptographic Engineering[EB/OL]. CryptographyEngineering, 2019. https://blog.cryptographyengineering.com/. Access Date: 2019-03-21.

[30] Griffiths, D.等著，程亦超译. 嗨翻 C 语言[M]. 人民邮电出版社, 2013.

[31] Gross, B. Abstract Algebra Open Learning Course[EB/OL]. Harvard University, 2014, https://www.extension.harvard.edu/open-learning-initiative/abstract-algebra. Access Date: 2019-03-03.

[32] Guo, F., Susilo, W., Mu, Y. Introduction to Security Reduction[M]. Springer, 2018.

[33] Hamer, G. The 1st BIU Winter School: Secure Computation and Efficiency[EB/OL]. Bar-Ilan University, 2016. https://cyber.biu.ac.il/event/the-1st-biu-winter-school. Access Date: 2019-03-02.

[34] Hamer, G. The 2nd BIU Winter School: Lattice-Based Cryptography and Applications[EB/OL]. Bar-Ilan University, 2016. https://cyber.biu.ac.il/event/the-2nd-biu-winter-school. Access Date: 2019-03-02.

[35] Hamer, G. The 3rd BIU Winter School: Bilinear Pairings in Cryptography[EB/OL]. Bar-Ilan University, 2016. https://cyber.biu.ac.il/event/the-3rd-biu-winter-school. Access Date: 2019-03-02.

[36] Hamer, G. The 4th BIU Winter School: Symmetric Encryption in Theory and in Practice[EB/OL]. Bar-Ilan University, 2016. https://cyber.biu.ac.il/event/the-4th-biu-winter-school. Access Date: 2019-03-02.

[37] Hamer, G. The 5th BIU Winter School: Advances in Practical Multiparty Computation[EB/OL]. Bar-Ilan University, 2016. https://cyber.biu.ac.il/event/the-5th-biu-winter-school. Access Date: 2019-03-02.

[38] Hamer, G. The 6th BIU Winter School: Cryptography in the Cloud – Verifiable Computation and Special Encryption[EB/OL]. Bar-Ilan University, 2016. https://cyber.biu.ac.il/event/the-6th-biu-winter-school. Access Date: 2019-03-02.

[39] Hamer, G. The 7th BIU Winter School on Cryptography: Differential Privacy: from Theory to Practice[EB/OL]. Bar-Ilan University, 2016. https://cyber.biu.ac.il/event/the-7th-biu-winter-school. Access Date: 2019-03-02.

[40] Hazay, C., Lindell, Y. Efficient Secure Two-Party Protocols[M]. Springer, 2010.

[41] Hoffstrein, J., Pipher, J., Silverman, J. An Introduction to Mathematical Cryptography, 2nd Edition[M]. Springer, 2014.

[42] Homburger, Y. The 8th BIU Winter School on Cryptography: Secure Key Exchange[EB/OL]. Bar-Ilan University, 2017. https://cyber.biu.ac.il/event/8th-biu-winter-school. Access Date: 2019-03-02.

[43] Jager, T., Kohlar, F., Schäge, S., Schwenk, J. On the Security of TLS-DHE in the Standard Model. CRYPTO 2012, Springer, 273-293.

[44] Kairouz, P., Oh, S., Viswanath, P. The Composition Theorem for Differential Privacy[J]. IEEE Transactions on Information Theory, 2017, 63(6): 4037-4049.

[45] Katz, J., Lindell, Y. Introduction to Modern Cryptography, 2nd Edition[M]. CRC Press, 2014.

[46] Katz, J., Lindell, Y. Introduction to Modern Cryptography: Principles and Protocols[M]. CRC Press, 2007.

[47] Katz, J.等著，任伟译. 现代密码学：原理与协议. 国防工业出版社, 2012.

[48] Knudsen, L. R., Robshaw, M. The Block Cipher Companion[M]. Springer, 2011.

[49] Krolzig, N. The 9th BIU Winter School on Cryptography: Zero Knowledge[EB/OL]. Bar-Ilan University, 2018. https://cyber.biu.ac.il/event/the-9th-biu-winter-school-on-cryptography. Access Date: 2019-03-02.

[50] Lewko, A., Waters, B. New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts[C]. CRYPTO 2010, Springer, 455-479.

[51] Li, N., Lyn, M., Su, D., Yang, W. Differential Privacy: from Theory to Practice[M]. Synthesis Lectures on Information Security, Privacy& Trust, 8(4): 1-138.

[52] Li, N., Qardaji, W., Su, D., et al. Membership Privacy: A Unifying Framework for Privacy Definitions[C]. CCS 2013 ACM, 889-900.

[53] Lindell, Y. How to Simulate It – A Tutorial on the Simulation Proof Technique[M]. Tutorials on the Foundations of Cryptography. Springer, Cham, 2017: 277-346.

[54] Lindell, Y. Tutorials on the Foundations of Cryptography: Dedicated to Oded Goldreich[M]. Springer, 2017.

[55] Lynn, B. PBC Library: The Pairing-Based Cryptography Library[EB/OL]. Standford University, 2013. https://crypto.stanford.edu/pbc. Access Date: 2019-03-21.

[56] Lyubashevsky, V., Peikert, C., Regev, O. On Ideal Lattices and Learning With Errors over Rings[J]. Journal of the ACM (JACM), 2013, 60(6): 43.

[57] McSherry, F., Talwar, K. Mechanism Design via Differential Privacy[C]. FOCS 2007, IEEE, 94-103.

[58] O'Donnell, R. Graduate Computational Complexity Theory[EB/OL]. Carnegie Mellon University, 2017. http://www.cs.cmu.edu/~odonnell/complexity17. Access Date: 2019-03-03.

[59] O'Donnell, R. Undergraduate Complexity Theory[EB/OL]. Carnegie Mellon University, 2017. http://www.cs.cmu.edu/~odonnell/15455-s17. Access Date: 2019-03-03.

[60] Onete, M. C. Review of the Book "Efficient Secure Two-Party Protocols" by Carmit Hazay, Yehuda Lindell, Springer, 2010[EB/OL]. IACR ePrint Archive, 2013. https://www.iacr.org/books/2013_sp_HazayLindell_Two-Party.pdf. Access Date: 2019-03-27.

[61] Paar, C., Pelzl, J. Understanding Cryptography: A Textbook for Students and Practitioners[M]. Springer, 2010.

[62] Peikert, C., Shiehian, S. Noninteractive Zero Knowledge for NP from (Plain) Learning With Errors[J]. IACR Cryptology ePrint Archive, 2019, 2019:158.

[63] Peikert, C., Waters, B. Lossy Trapdoor Functions and Their Applications[J]. SIAM Journal on Computing, 2011, 40(6): 1803-1844.

[64] Raykova, M. Secure Computation with RAMs: Revisiting Square Root ORAM and Low Leakage Secure Boolean Queries[EB/OL]. YouTube, 2017. https://www.youtube.com/watch?v=8EmFRbZAElM. Access Date: 2019-03-23.

[65] Regev, O. On Lattices, Learning With Errors, Random Linear Codes, and Cryptography[J]. Journal of the ACM (JACM), 2009, 56(6): 34.

[66] Rindal, P. LibOTe: A Fast, Portable, and Easy to Use Oblivious Transfer Library[EB/OL]. GitHub, 2019. https://github.com/osu-crypto/libOTe. Access Date: 2019-03-21.

[67] Rindal, P. LibPSI: A Repository for Private Set Intersection[EB/OL]. GitHub, 2019. https://github.com/osu-crypto/libPSI. Access Date: 2019-03-21.

[68] Robson, E.等著，徐阳等译. Head First HTML 与 CSS（第 2 版）. 中国电力出版社, 2013.

[69] Rosen, K. H. Discrete Mathematics and Its Applications[M]. McGraw-Hill Education, 2011.

[70] Rosen, K. H.著，徐六通等译. 离散数学及其应用（原书第 7 版）[M]. 机械工业出版社, 2015.

[71] Sedgewick, R., Wayne, K. Algorithm, Part I[EB/OL]. Coursera, 2013. https://www.coursera.org/learn/algorithms-part1. Access Date: 2019-03-21.

[72] Sedgewick, R., Wayne, K. Algorithm, Part II[EB/OL]. Coursera, 2013. https://www.coursera.org/learn/algorithms-part2. Access Date: 2019-03-21.

[73] Sedgewick, R., Wayne, K. Algorithms (4th Edition)[M]. Addison-Wesley Professional, 2011.

[74] Sedgewick, R.等著，谢路云译. 算法（第四版）[M]. 人民邮电出版社, 2012.

[75] Shoup, V. Sequences of Games: A Tool for Taming Complexity in Security Proofs[J]. IACR Cryptology ePrint Archive, 2004, 2004: 332.

[76] Sierra, K.等著，杨尊一译. Head first Java（第二版 • 中文版）[M]. 中国电力出版社, 2007.

[77] Silverman, J. Friendly Introduction to Number Theory (4th Edition)[M]. Pearson, 2014.

[78] Silverman, J.著，孙志伟等译. 数论概论（原书第 4 版）[M]. 机械工业出版社, 2016.

[79] Sipser, M. Introduction to the Theory of Computation, 3rd Edition[M]. Cengage Learning, 2012.

[80] Siper, M.著，唐常杰等译. 计算理论导引（原书第三版）[M]. 机械工业出版社, 2015.

[81] Stefanov, E., van Dijk, M., Shi, E., et al. Path ORAM: An Extremely Simple Oblivious RAM Protocol[C]. CCS 2013, ACM, 299-310.

[82] Wang, T., Blocki, J., Li, N., et al. Locally Differentially Private Protocols for Frequency Estimation[C]. USENIX Security 2017, USENIX, 729-745.

[83] Waters, B. Efficient Identity-Based Encryption without Random Oracles[C]. EUROCRYPT 2005, Springer, 114-127.

[84] Zahur, S., Wang, X., Raykova, M., et al. Revisiting Square-Root ORAM: Efficient Random Access in Multi-Party Computation[C]. S & P 2016, IEEE, 218-234.

[85] 郭福春. 致我公钥密码研究生的一封信[J]. 卧村密码学报, 第 1 期, 2019.

[86] 刘田. 理论计算机科学基础[EB/OL]. 哔哩哔哩, 2017. https://www.bilibili.com/video/av17253679/. Access Date: 2019-12-14.

[87] 刘巍然，Scalers 听力狂练小组. 世界上最顶级的密码学课程[EB/OL]. i 春秋, 2015. https://www.ichunqiu.com/course/50433. Access Date: 2019-03-03.

[88] 屈婉玲. 代数结构与组合数学[EB/OL]. 哔哩哔哩, 2017. https://www.bilibili.com/video/av9536834. Access Date: 2019-03-25.

[89] 屈婉玲，耿素云，张立昂. 离散数学（第 2 版）[M]. 高等教育出版社, 2015.

附录 A：推荐公开课汇总

公开课名称	开设高校	难度
Cryptography I	斯坦福大学	★
Cryptography	马里兰大学	★
BIU Winter School on Cryptography	巴伊兰大学	★★
代数结构与组合数学	北京大学	★★
Abstract Algebra	哈佛大学	★★★
Undergraduate Complexity Theory	卡耐基梅隆大学	★★★
Graduate Computational Complexity Theory	卡耐基梅隆大学	★★★★
理论计算机科学基础	北京大学	★★
Alrogithm, Part I	普林斯顿大学	★★
Alrogithm, Part II	普林斯顿大学	★★

附录 B：推荐教材与书籍汇总

教材与书籍名称	作者	难度	说明
Introduction to Modern Cryptography, 2nd Edition	J. Katz Y. Lindell	★★★	必读材料 本科及以上
A Graduate Course in Applied Cryptography	D. Boneh V. Shoup	★★★	进阶材料 硕士及以上
Introduction to Security Reduction	F. Guo W. Susilo Y. Mu	★★★	安全性证明 硕士及以上
Tutorials on the Foundations of Cryptography	Y. Lindell 等	★★★	分支领域高阶 博士
Synthesis Lectures on Information Security, Privacy, and Trust	E. Bertino R. Sandhu	★★	分支领域入门 本科及以上
Discrete Mathematics and Its Applications, Seventh Edition	K. Rosen	★	离散数学入门 高中及以上
离散数学（第 2 版）	屈婉玲 耿素云 张立昂	★★	离散数学参考 本科及以上
Algebra, Second Edition	M. Artin	★★★★	抽象代数高阶 博士
Friendly Introduction to Number Theory (4th Edition)	J. Silverman	★★	数论入门 本科及以上
Introduction to the Theory of Computation，3rd Edition	M. Sipser	★★★	计算理论入门 本科及以上

Computational Complexity: A Modern Approach	S. Arora B. Barak	★★★★★	计算理论高阶 博士
Head First 系列	K. Sierra 等	★	编程入门 高中及以上
Algorithms, 4th Edition	R. Sedgewick K. Wayne	★★	算法入门 本科及以上
An Introduction to Mathematical Cryptography	J. Hoffstein J. Pipher J. Silverman	★★★	偏向理论 硕士及以上
Understanding Cryptography: A Textbook for Students and Practitioners	C. Paar J. Pelzl	★★	广而不深 本科及以上
Foundations of Cryptography	O. Goldreich	★★★★	密码学高阶 博士
The Algorithmic Foundations of Differential Privacy	C. Dwork A. Roth	★★★★	差分隐私高阶 博士