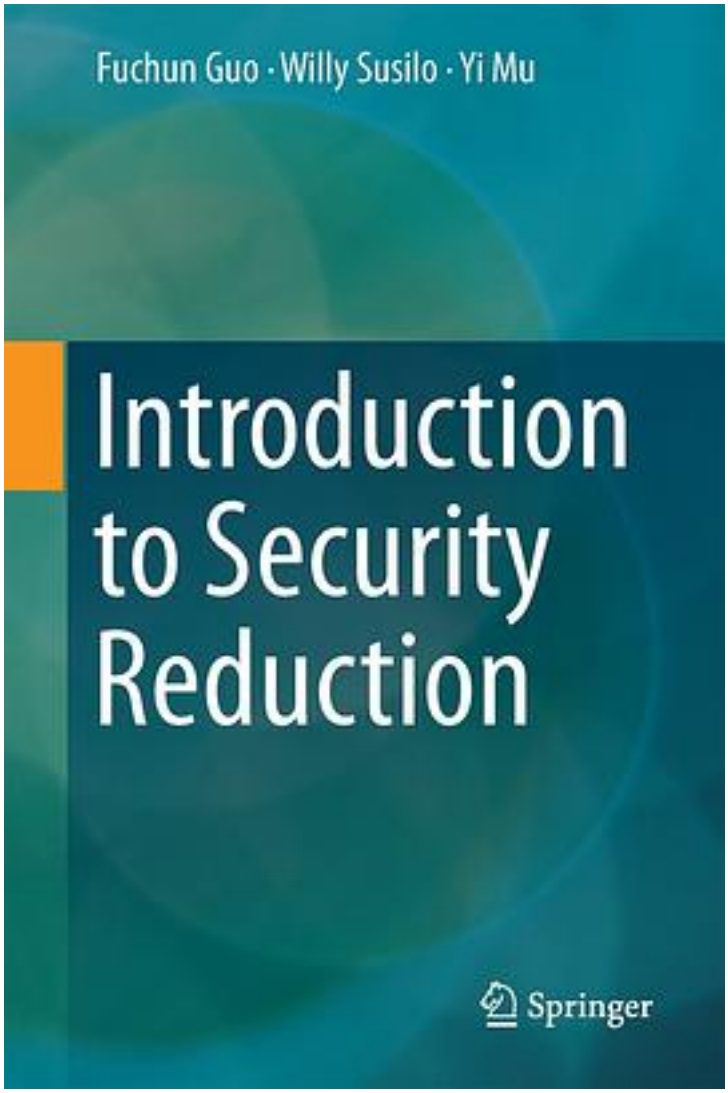
Introduction to Security Reduction



Introduction to Security Reduction_下载链接1_

著者:Fuchun Guo

出版者:Springer International Publishing

出版时间:2018-7

装帧:精装

isbn:9783319930480

网络空间安全—>密码学—>公钥密码—>安全证明方法—>安全归约

安全归约是公钥密码方案特别是签名方案和加密方案的安全证明方法。每提出一个方案需要给出一个对应的安全归约证明，否则安全性缺乏说服性。然而，安全归约对于初学者来说有点复杂和困难。通过简单地模仿他人证明事后被发现大多数的证明都是有问题的。安全归约证明有着多样性。方案不同对应的归约原理和方法也不尽相同。要学习安全归约不能针对具体方案的证明方法进行学习，否则难以掌握安全归约的本质。

本书只干一件事：解释清楚正确的安全归约应该怎么给予证明。

本书的构成主要分为三大块：

1.数学基础之群知识。解释安全归约需要用些例子。本书的例子均基于群知识。

2.安全归约基础。这部分的介绍是本书重点之重点。详细内容包括以下几点

・什么是安全归约。

・安全归约的基本原理。

・安全归约涉及的基本概念。

・安全归约的难点与重点。

・正确安全归约的原理，方法和技术。

・随机预言模型对应证明的原理和方法。

・签名的安全归约框架。

・加密的安全归约框架。

3.安全归约实例与训练。这部分的介绍是为了帮助读者巩固第二部分知识。

本书从2013年下半年开始撰写直到2018年上半年才完成并出版。
本书的作者也是一边写，一边学习，一边摸索。由于没有类似的教材可以借鉴，撰写过程非常辛苦，一步步最终完成。

【本书优点】

・如果论文里的安全归约证明方法看不懂，这本书将提供很大的帮助。

・截止2019年10月6日，这本书提供的内容和帮助无法被其它论文和书籍所取代。

【本书缺点】

・第二部分(安全归约基础)看起来很吃力。前半部分对很多概念进行解释但又不说明在哪用，所以看起来很枯燥和沉闷；后半部分将把之前介绍的概念融在一起。

・第二部分(安全归约基础)的知识点逻辑顺序有点乱。作者如此安排的理由是为了解释一个概念的时候尽量避免涉及到新概念。

・很多地方的文字表达不够清楚，太简单，缺乏足够多的解释。有些概念的解释之后没有跟随一个具体的例子，有点不知所云。

【本书建议】

・没有任何公钥密码基础的初学者几乎很难看懂此书。建议先做一些基础训练。训练可以参考《公钥密码方案构造及安全证明的知识要点和方法论》 密码学报. 2019, 6 (1): 1-17 这篇论文。

・这本书有些对应的学习心得。详情请微信搜索《卧村密码学报》这个假期刊。

・此书太贵，不建议购买英文原版，除非贼有钱。

作者介绍:

目录:

Introduction to Security Reduction_下载链接1_

标签

Cryptography

评论

密码学安全归约证明学习的不二选择

正在澳洲师从作者本人，学习公钥密码。
幸亏碰到这本书，帮我打开了公钥的门，这是我最大的幸运。虽然公钥密码学的书很多，但这本书应该是最能走捷径的一本书，直奔要害，干货十足。技术点和注意点被作者总结在一起，这是任何一本书不能比的。这本书要读懂，一定要有点基础，看懂CCA，这才算真懂了

Introduction to Security Reduction_下载链接1_

书评

《Introduction to Security Reduction》这本书将我正式带入密码学科研的大门，在之后的研究中，终于能感受到“科研有迹可循”，“一切皆有章法”。这本书可以说是将公钥密码学中密码方案安全归约证明的规则从头到尾梳理剖析了一遍，放在了读者面前。我个人认为这本书对于公钥...

这本书适合谁？ —L0：针对密码学初学者，很抱歉这本书真的不适合你。推荐先读《INTRODUCTION TO MODERN CRYPTOGRAPHY》。
—L1：针对有一定密码学基础的学者，很荣幸的告诉你这本书非常适合你，希望你能从这本书中学习安全规约的的思想、方法以及技术路线。配合本书后面几章...

Introduction to Security Reduction_下载链接1_