Introduction to Quantum Cryptography

This book offers an accessible and engaging introduction to quantum cryptography, assuming no prior knowledge in quantum computing. Essential background theory and mathematical techniques are introduced and applied to the analysis and design of quantum cryptographic protocols. The title explores several important applications such as quantum key distribution, quantum money, and delegated quantum computation, while also serving as a self-contained introduction to the field of quantum computing. With frequent illustrations and simple examples relevant to quantum cryptography, this title focuses on building intuition and challenges readers to understand the basis of cryptographic security. Worked examples and mid-chapter exercises allow readers to extend their understanding, and in-text quizzes, end-of-chapter homework problems, and recommended further reading reinforce and broaden understanding. Online resources available to instructors include interactive computational problems in Julia, videos, lecture slides, and a fully worked solutions manual.

THOMAS VIDICK is Professor in the Department of Computer Science and Applied Mathematics at the Weizmann Institute of Science in Israel. He received his PhD from UC Berkeley in 2011, followed by two years of postdoctoral research at the Massachusetts Institute of Technology, where he worked on quantum complexity and cryptography. He joined the Computer Science Faculty at the California Institute of Technology in 2014, and became Professor in 2018. In 2022 he took leave from CalTech to start his current position at the Weizmann Institute. Professor Vidick is best known for his research on device independence, including the first security proof of device-independent quantum key distribution. In 2019 he received a Presidential Early Career Award, and in 2021 was named a Simons Investigator at CalTech. In 2023 he received the Michael and Sheila Held prize from the National Academy of Sciences for his work in quantum cryptography and quantum complexity.

STEPHANIE WEHNER is Antoni van Leeuwenhoek Professor at Delft University of Technology, QuTech, and Director of the Quantum Internet Alliance. A member of the Royal Netherlands Academy of Arts and Sciences, she is also a co-founder of QCRYPT, the largest international conference in quantum cryptography. In a former life, she worked as a professional hacker. Her research is focused on manipulating the laws of quantum mechanics to construct better information networks and computer systems. Together with the Quantum Internet Alliance she is working on realizing a large-scale quantum computer network.

"If you are intrigued by the prospects of quantum cryptography but not yet familiar with the formalism behind it, then this book is the perfect starting point for you. It playfully introduces the most important concepts in modern quantum cryptography and at the same time gently but purposefully helps you discover the mathematical framework required to make formal statements."
Marco Tomamichel, National University of Singapore

"Vidick and Wehner cover quantum cryptography in its full beauty and depth. Packed with enlightening examples and comprehensive exercises, this book will likely become an indispensable companion next time I hold lectures on the subject."
Renato Renner, ETH Zurich

"Thomas Vidick and Stephanie Wehner take readers on an insightful exploration of the full landscape of quantum cryptography, skillfully weaving together theory and applications and providing pedagogical quizzes and exercises. The mathematical formalism is rigorous yet approachable, making this book an excellent introduction to this captivating area."
Anne Broadbent, University of Ottawa

"I recommend exploring the intriguing world of quantum cryptography with this definitive guide. Stephanie and Thomas, with expert precision, clarify the conceptual and mathematical complexities of quantum mechanics and secure communication, bringing clarity where confusion often reigns. It is an essential resource for anyone involved in quantum information science, from rookies to veterans."
Artur Ekert, University of Oxford and National University of Singapore

Introduction to **Quantum Cryptography**

Thomas Vidick
California Institute of Technology, USA
Weizmann Institute of Science, Israel

Stephanie Wehner
Delft University of Technology, The Netherlands

CAMBRIDGE UNIVERSITY PRESS

Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/highereducation/isbn/9781316515655
DOI: 10.1017/9781009026208

First published 2024

Printed in the United Kingdom by CPI Group Ltd, Croydon CR0 4YY

A catalogue record for this publication is available from the British Library

A Cataloging-in-Publication data record for this book is available from the Library of Congress

ISBN 978-1-316-51565-5 Hardback

Additional resources for this publication at www.cambridge.org/vidick-wehner

Contents

Preface

Welcome! We are excited to introduce you to one of our favorite topics: quantum cryptography. With this book, we would like to provide you with all the basics needed to understand and analyze fundamental quantum cryptographic protocols, and even motivate you to design your own. Most of all, we hope you have fun exploring the adventures – and occasional mishaps – of our chief protagonists, Alice and Bob, as they attempt to use quantum communication to solve cryptographic challenges.

This book is meant to provide a textbook introduction to the theory of quantum cryptography, presented in an engaging yet largely mathematically precise manner. Our writing is voluntarily playful and places a high emphasis on developing intuition, a style we find to be appropriate to the discussion of cryptographic tasks; we will frequently invite you to devise cryptographic schemes and break them. However, the formalism is introduced in mathematical detail, and proofs are included when they are useful to build understanding. Whenever we do provide a proof, we give one that requires minimal background knowledge and fosters physical intuition, rather than providing the most sharp statements obtained using advanced quantum information tools. End of chapter notes provide references to the literature, where more information can be found. We emphasize that the book is meant as an engaging introduction, not as a reference manual.

We intend the book primarily for undergraduate students, as well as graduate students with a strong background in mathematics, physics, or computer science, but not necessarily any prior knowledge of quantum computing or cryptography. We do assume, however, that students have taken undergraduate courses on linear algebra and statistics before embarking on reading this book. The book can be used to teach a one-semester course on quantum cryptography (see examples below), or be used for self-study.

For the purpose of this book, quantum cryptography can be defined as the study of those cryptographic tasks that can be implemented using quantum hardware, i.e. devices capable of manipulating quantum information. The most prominent such task, quantum key distribution, acts as a focal point throughout the book. Other tasks, such as quantum commitments, quantum money, and others, are discussed. The reader should be warned that this is not a book about post-quantum cryptography, and neither quantum algorithms nor classical cryptographic schemes that are resistant to them are meant to be discussed in any detail.

Organization

The book is organized in a progressive manner, starting from the basic formalism of quantum communication, building intuition about properties such as no-cloning and uncertainty principles, and applying these properties to the design and analysis

of quantum cryptosystems. In more detail, the book is composed of 12 chapters, plus an introductory chapter, not counting this preface:

Chapter 1 forms a first introduction to quantum information, assuming a background in linear algebra and probability. It is not meant to replace a thorough introduction to quantum information, for which many good textbooks exist, but aims to provide sufficient knowledge to follow the rest of this book. In this chapter we give a first application of quantum information by studying a quantum random number generator. A reader already familiar with quantum information may skip this chapter, and it may be omitted in a course series where students have already taken an introduction to quantum information.

Chapter 2 introduces several quantum tools that are often not discussed in introductory courses in quantum information but are crucial for cryptography, such as density matrices and the partial trace. This chapter also introduces the notion of secure communication and contains a first quantum protocol, namely the quantum one-time pad. Chapter 2 assumes students are familiar with the material covered in Chapter 1.

Chapter 3 introduces one of the very first ideas in the development of quantum cryptography, quantum money. This chapter assumes the students are familiar with the material covered in Chapters 1 and 2.

Chapter 4 introduces the concept of quantum entanglement, as well as fundamental notions such as Bell nonlocality and the monogamy of entanglement. These notions play an important role in understanding quantum key distribution in later chapters. Chapter 4 assumes the students are familiar with the material covered in Chapters 1 and 2.

Chapter 5 discusses how to quantify information in quantum cryptography, providing a cornerstone for security definitions. It also introduces a tripartite uncertainty game that will play an important role in our security analysis of quantum key distribution. This chapter assumes the students are familiar with the material covered in Chapters 1, 2, and 4.

Chapter 6 introduces the concept of privacy amplification and its realization using randomness extractors. This chapter assumes familiarity with the material covered in Chapters 1 and 2.

Chapter 7 formally introduces the task of key distribution, and gives examples of key distribution protocols in simplified settings. This chapter assumes the students are familiar with the material covered in Chapters 1, 2, 5, and 6.

Chapter 8 introduces the BB'84 protocol and provides a sketch of its security analysis, using the purified protocol and uncertainty relations. Chapter 8 assumes the reader is familiar with the material covered in Chapters 1, 2, 4, 5, 6, and 7.

Chapter 9 discusses device-independent quantum key distribution. A partial security analysis, assuming independent rounds, is made using the notion of a guessing game. This chapter assumes the students know the material presented in Chapters 1, 2, 4, 5, 6, 7, and 8.

Chapter 10 examines the use of quantum communication for two-party cryptographic tasks such as coin flipping, bit commitment, and oblivious transfer. Chapter 10 assumes familiarity with Chapters 1, 2, 4, and 5.

Chapter 11 introduces the use of physical assumptions in combination with quantum communication to solve cryptographic challenges such as bit commitment and oblivious transfer. This chapter assumes the students have studied Chapters 1, 2, 5, 6, and10.

Chapter 12 discusses security notions for quantum encryption. It assumes familiarity with the material covered in Chapters 1 and 2.

Chapter 13 introduces the problem of delegating quantum computations to a quantum server in the cloud. This chapter assumes familiarity with the material covered in Chapters 1, 2, and 5.

Suggestions for Teaching

This book can be used to teach a variety of classes for undergraduate and graduate students. The following are suggestions organized by duration of the course and background of the students. We provide approximate time estimates based on our experience in teaching the material. More, or significantly less, time could be appropriate depending on the level and prior knowledge of the students, as well as the level of detail with which one wishes to cover the material.

A First Introduction to Quantum Information and Cryptography

This course is aimed at undergraduate students as an introduction to quantum information with some applications to quantum cryptography. The course would cover Chapters 1, 2, 3, and possibly 4, introducing quantum applications such as the quantum random number generator, the quantum one-time pad, and quantum money, in roughly nine interactive lectures of two hours each. If more time is available, parts of Chapters 5, 7, and 8 could be used to introduce quantum key distribution, omitting many of the formal details and proofs.

Introduction to Quantum Information and Quantum Key Distribution

Such a course is aimed at advanced undergraduate students with no prior knowledge of quantum information. The course introduces the students to the basic notions of quantum information, and works its way up to quantum key distribution and its security analysis. This could cover Chapters 1, 2, 4, 5, 7, and 8, assuming roughly 12 interactive lectures of two hours each. Depending on the level of the students, one might add device-independent quantum key distribution in Chapter 9.

Quantum Key Distribution

This course is aimed at advanced undergraduate students who are already familiar with quantum information through, for example, a class focusing mainly on quantum computing. Such a class would typically cover the materials covered in Chapter 1, but often not more advanced notions such as density matrices or the partial trace

introduced in Chapter 2. The course could cover Chapters 2, 4, 5, 7, 8, and 9, assuming roughly 10 interactive lectures of two hours each. Depending on the level or interest of the students, one might add any of the further topics in this book from Chapters 3, 10, 11, or 13.

Quantum Cryptography beyond Quantum Key Distribution
This course is aimed at advanced undergraduate or graduate students who are already familiar with quantum information and who have at least a passing familiarity with quantum key distribution (QKD). Its focus would be on quantum cryptography beyond QKD. The course could cover Chapters 2, 4, and 5 as necessary, and continue with quantum protocols beyond QKD using Chapters 3, 11, 12, and 13.

Quantum Cryptography
A course for graduate students could cover the entirety of this book in a linear fashion, going faster over the first two chapters. Depending on the students, these could also be assigned as preparatory reading, with the students using the quiz questions to test their understanding. The course could proceed more slowly over the technically more advanced sections, such as the end of Chapters 6 and 9 and Chapter 13.

Resources

When the web icon shown here appears on the page, a supporting resource can be found on the website. Several resources accompany this book, and are available at `www.cambridge.org/vidick-wehner`. These include:

Julia sheets: Online interactive exercise sheets in the Julia language to enable you to explore and play with the material presented here.
Videos: Videos from our online MOOC that match the relevant portions of the text.
End of chapter notes: References to the literature mentioned in a chapter.
Quizzes: Throughout the book you are encouraged to test yourself using short quizzes. The answers to the quizzes may be found at the end of each chapter.
Exercises: Several longer exercises are provided throughout the text to challenge yourself. Additional homework problems may be found at the end of each chapter.
Solution manual: A solution manual for the problems given at the end of each chapter.
Slide materials: Materials are available that may be used for slides for a course using this book.

We also recommend two additional resources to explore some of the materials in this book, and expand your knowledge further. The Quantum Protocol Zoo (`https://wiki.veriqloud.fr/index.php?title=Main_Page`) provides an overview of many cryptographic protocols not included in this book. The Quantum Network Explorer (`http://quantum-network.com`) lets you program quantum cryptographic protocols, and also provides a graphical interface to help you understand the effects of hardware imperfections on some of the protocols we discuss in this book.

Origins and Acknowledgments

This book grew over the years out of our offline and online classes, chiefly our MOOC QuCryptoX "Quantum cryptography" initially offered on edX in Fall 2017. Lecture notes created for the MOOC were refined over multiple years of teaching the course in a hybrid format in Delft and in Caltech, and formed the basis for this now expanded book.

Since this book evolved from our lecture notes, a great many people have made contributions to the book over the years. Generations of teaching assistants for both offline and online classes have made diverse contributions to developing these notes, exercises, figures, and corrections. In roughly chronological order they are, from TU Delft, Nelly Ng, Jed Kaniewski, Corsin Pfister, Willem Hekman, Jeremy Ribeiro, Kenneth Goodenough, Filip Rozpçdek, Jonas Helsen, Victoria Lipinska, Guus Avis, Francisco Horta Ferreira da Silva, Alvaro G. Iñesta, Scarlett Gauthier, Ravisankar Ashok Kumar Vattekkat, and Hana Jirovska. We also thank guest lecturer David Elkouss for his contributions to explaining information reconciliation. From Caltech, they are Chinmay Nirkhe, Jalex Stark, Andrea Colandangelo, and Tina Zhang. Last but not least, we would like to thank all the students who have taken our classes over the years and provided useful feedback that helped us to improve this book.

Chapter title images are from Hanson Lab, QuTech, Delft University of Technology.