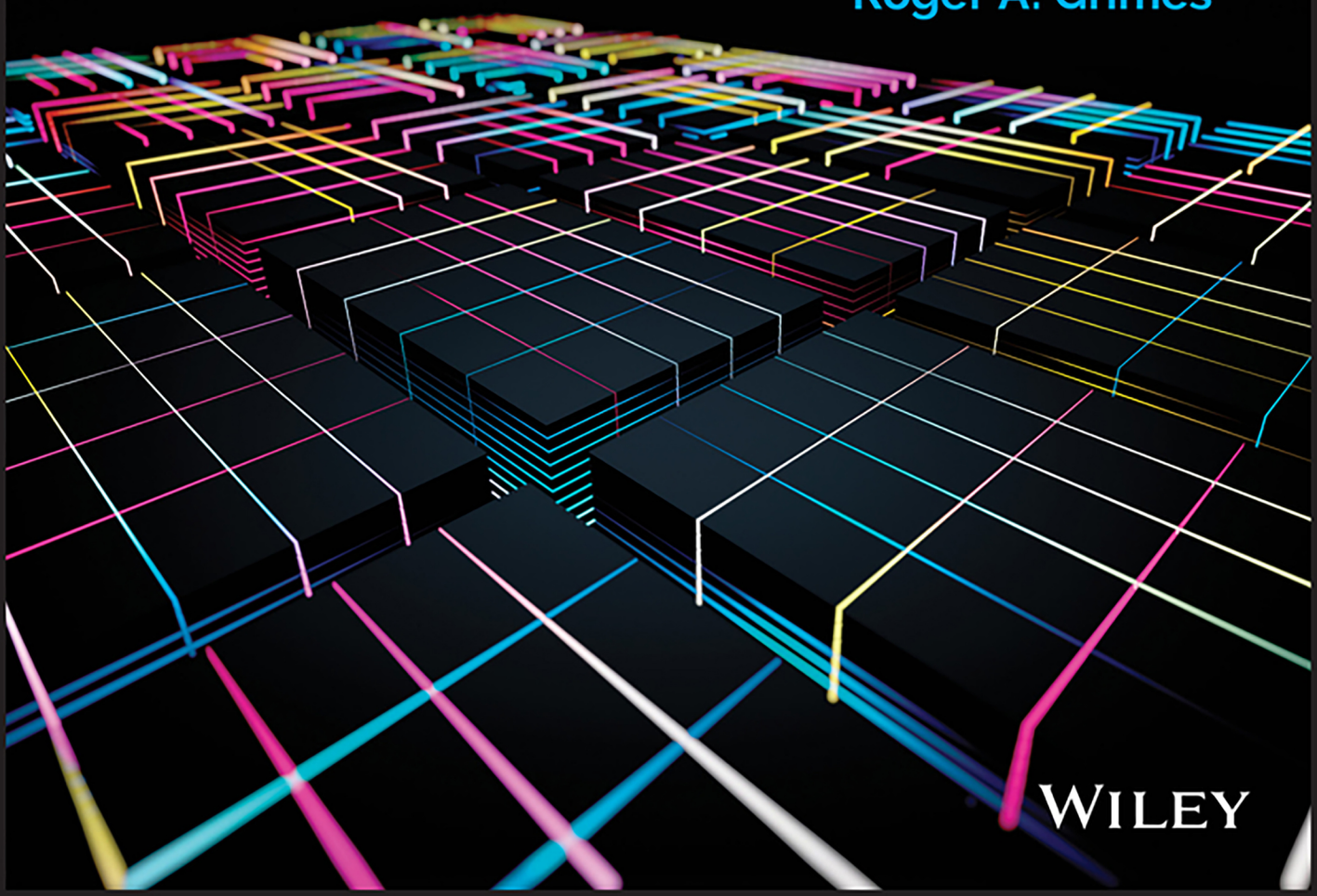
Cryptography Apocalypse

Preparing for the Day When Quantum Computing Breaks Today's Crypto

Roger A. Grimes



WILEY

Cryptography Apocalypse

Cryptography Apocalypse

Preparing for the Day When Quantum Computing Breaks Today's Crypto

Roger A. Grimes

WILEY

Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto

Published by
John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
www.wiley.com

Published simultaneously in Canada

ISBN: 978-1-119-61819-5
ISBN: 978-1-119-61821-8 (ebk)
ISBN: 978-1-119-61822-5 (ebk)

Manufactured in the United States of America

Library of Congress Control Number: 2019946679

I dedicate this book to my wife, Tricia. She is the woman behind the man in every sense of the saying.

About the Author

Roger A. Grimes has been fighting malicious computer hackers for more than three decades (since 1987). He's earned dozens of computer certifications (including CISSP, CISA, MCSE, CEH, and Security+), and he even passed the very tough Certified Public Accountant (CPA) exam, although it has nothing to do with computer security and he is the worst accountant ever. He's been paid as a professional penetration tester to break into companies and their websites for over 20 years, and it has never taken him more than three hours to do so. He has created and updated computer security classes, been an instructor, and taught thousands of students how to hack or defend. Roger is a frequent presenter at national computer security conferences. He's previously written or co-written 10 books on computer security and more than a thousand magazine articles. He's been the computer security columnist for *InfoWorld* and *CSO* magazines (`www.infoworld.com/blog/security-adviser/`) since August 2005, and he's been working as a full-time computer security consultant for more than two decades. Roger is frequently interviewed by magazines and television shows, and for the radio, including by *Newsweek* magazine and NPR's *All Things Considered*. Roger currently advises companies, large and small, around the world on how to stop malicious hackers and malware in the quickest and most efficient ways. He has been reading and studying quantum physics since 1983.

You can contact and read more from Roger at:

- Email: `roger@banneretcs.com`
- LinkedIn: `www.linkedin.com/in/rogeragrimes/`
- Twitter: `@rogeragrimes`
- CSOOnline: `www.csoonline.com/author/Roger-A.-Grimes/`

Acknowledgments

I would like to thank Wiley and Jim Mintel for greenlighting this book. I had been giving presentations on this topic for more than a year to enthusiastic crowds and didn't see the opportunity right in front of my face. Thanks to my employer, KnowBe4, Inc., and awesome CEO Stu Sjouwerman, Kathy Wattman, Kendra Irmie, and Mary Owens for letting me develop the original presentation and go around the county presenting it. Thanks to my core KnowBe4 quantum presentation support team: Amy Mitchell, Jessica Shelton, and Andy Reed.

I want to thank everyone whom I interviewed and sent emails back and forth with in my quest to better understand how quantum computers will impact our world, including cryptography. I don't think my head has ever hurt worse figuring out how to understand very complex concepts and trying to convey them in a more understandable way to lay audiences. This was further complicated by the fact that much of quantum physics and cryptography is defined in the world of advance mathematics. In a few areas I just gave up and just quoted what the experts wrote or said. Easily my favorite "give-up" quote appears in Chapter 6 when I'm trying to generally describe one of the quantum-resistant ciphers: "The NTRU Prime team describes their cipher as 'efficient implementation of high-security prime-degree large-Galois-group inert-modulus ideal-lattice-based cryptography' and which others describe as using 'irreducible, non-cyclotomic polynomials.'" I still can't stop laughing when I see that description because of everything I do not know involving it and all the advanced mathematics I would have to explain to basically say, "This is a really hard-to-solve math problem."

With that said, any factual errors made in this book are mine alone. I tried my best to make sure not a single mistake made it into the book. I pride myself on being factually correct above everything else. But in a book that covers so many advanced topics, I've bound to have made mistakes. There is going to be a quantum cryptographic expert somewhere mad at me for horribly messing up some key concept. Please know that I tried my best to be as accurate as possible, and that I'm only human. I apologize in advance for any mistakes.

I want to thank all the great teachers and writers who attempted to more simply explain quantum mechanics and computing to me and everyone else. In this book, I often repeated examples and allegories made by many others that I have read, listened, and watched over the last 20 years. I only understand these sometimes difficult subjects because of their prior work. I tried to give credit to any examples or explanations where I could remember or find the author. I apologize for any missed credit. I am simply humbled.

I want to thank all the submission teams who responded to my call for their help to correct and clarify my summaries of their NIST-submitted algorithms in Chapter 6. They tried their best to

get me see the facts of their cryptographic solution. Not all teams replied (or replied in time) to my queries. Here are the ones who did: Peter Schwabe with CRYSTAL-Kyber; Thomas Prest with FALCON; Douglas Stebila with FRODOKEM; Philippe Gaborit with HQC, Rollo, and RQC; Vadim Lyubashevsky with Dilithium; Xianhui Lu with LAC; Marco Baldi with LEDCrypt; Ward Beullens with LUOV; Joost Rijneveld with MQDSS & SPHINCS+; Simona Samardziska with MQDSS; Thomas Poeppelmann with NewHope; John Schanck with NTRU; Nina Bindel with qTESLA; Scott Fluhrer with SPHINCS+; and Mike Hamburg with ThreeBears. Thank you all.

I'd like to give special thanks to University of Texas Austin quantum professor Scott Aaronson; physical science writer Philip Bell; Ken Mafli of Townsend Security; and Daniel Burgarth. Last, a big thanks to the following Wiley folks who put up with my constant complete rewrites: Kim Wimpsett, Pete Gaughan, and Athiyappan Lalitkumar. They finally had to stop me from adding things and tell me to let them print it.

NOTE I often intentionally or unintentionally used the word *cipher* to describe any cryptographic algorithm. Technically, *cipher* refers only to encryption algorithms, and digital signature algorithms are *schemes*. I sometimes used the word *cipher* to refer to either to make writing about cryptography over nine chapters easier. Please forgive any technical misuse.

Contents

Contents

Introduction

In the late 1990s the world was consumed by a coming computer problem known as Y2K, which stood for the Year 2000. The difficulty was that most of the world's devices, computers, and programs to that point in time recorded dates using only the last two digits of the year. From a programmatic level, they couldn't tell the difference between 1850, 1950, and 2050.

When 1999 turned into 2000, many of those computers and programs would not have been able to correctly process any calculation involving two-digit dates in the new century. There had been many known failures by programs and devices that were already using dates in the future (such as scheduling and warranty programs). Symptoms of failed devices and programs ranged from visible errors to errors that happened but were not readily visible (which can be extremely dangerous) to complete device and program shutdowns.

The problem was that although we knew that a sizable percentage of devices and programs were impacted, no one knew which untested things were fine and didn't need to be updated and which had to be updated or replaced before January 1, 2000. There was a two- to three-year rush to find out what was broken and what was fine. As with many slow-moving potential catastrophes, most of the world did little to nothing to prepare until the last few months. The last-minute global rush created a bit of a worldwide panic about what would happen as clocks moved into the new century. There was even a fantastically bad 1999 disaster movie (`www.imdb.com/title/tt0215370`) that had planes dropping out of the sky along with other worldwide cataclysmic mayhem.

In the end, when Y2K rolled around, it was a bit of a dud if you wanted real life to be like the movies. There were issues, but for the most part the world continued as usual. There were devices and programs that failed to handle the newer dates appropriately, but most major systems worked correctly. There were no falling planes, fires, or burst dams. For many people who were expecting disaster outcomes, it was a bit of a letdown—so much so that, over time the term Y2K evolved to become a unofficial synonym for overly hyped events involving premature panic with little resulting damage.

What most people today don't realize is that Y2K was anticlimactic precisely because we had years of preparation and warning. Most major systems were checked for Y2K issues and replaced or updated as needed. Had the world not become aware of it and not done anything, Y2K would have certainly been far, far worse (albeit, I'm still not sure planes would be falling out of the sky). Y2K wasn't a premature panic dud. It was the foreseeable outcome from years of preparation, demonstrating the success of what humanity can do when faced with a looming digital problem.

The Coming Quantum Day of Reckoning

Most of the world doesn't know it yet, but we are in another even more momentous, looming Y2K moment, except this one is likely already causing serious problems and damage. Worse, we can't stop all the damage even if we begin preparing now. There are organizations sustaining harm today that will not be able to program their way out. Nation-states and corporate adversaries are likely already taking advantage of the problem.

Quantum computers will likely soon break traditional public key cryptography, including the ciphers protecting most of the world's digital secrets. These soon-to-be-broken protocols and components include HTTPS, TLS, SSH, PKI, digital certificates, RSA, DH, ECC, most Wi-Fi networks, most VPNs, smartcards, HSMs, most cryptocurrencies, and most multifactor authentication devices that rely on public key crypto. If the list just included HTTPS and TLS, it would cover most of the Internet. On the day that quantum computing breaks traditional public crypto, every captured secret protected by those protocols and mechanisms will be readable.

Even more important, anyone capturing and storing those (currently protected) secrets will be able to go back after the quantum crypto break and reveal them. How many secrets do you have or does your organization have that you want revealed to anyone within a few years? That's the new Y2K problem we are dealing with today.

There are many workable solutions you can implement today, although some are beyond the average company's means or, if implemented prematurely, can cause significant performance and operational disruption. Preparing for the coming quantum break requires education, critical choices, and planning. Individuals and organizations who clearly understand what is ahead can take the right steps now to be as prepared as possible. They can stop the unwarranted eavesdropping today and start to move their managed assets to a more quantum-resistant environment. This book has that knowledge and gives you the plan to help minimize your organization's risk from the coming quantum crypto break. If enough organizations prepare now, we can make the quantum break as inconsequential as the Y2K problem.

Who This Book Is For

This book is primarily aimed at anyone who is in charge of managing their organization's computer security and, in particular, computer cryptography. These are the people who will likely be in charge and leading the way for their post-quantum migration project. It is also for managers and other leaders who understand the importance of good cryptography and its impact on their organization. Last, anyone with a passing interest in quantum mechanics, quantum computers, and quantum cryptography will find many new facts to make this book a worthwhile read.

What Is Covered in This Book?

Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto contains nine chapters separated into two parts.

Part I, "Quantum Computing Primer," is a basic primer on quantum mechanics, computing, and how it can break today's cryptographic protection.

Chapter 1, "Introduction to Quantum Mechanics"

If you didn't understand quantum mechanics the first time you read about it, don't worry—quantum mechanics has vexed the most brilliant minds our planet has ever had for over a century. We mere mortals can be forgiven for not immediately grasping the central concepts. Chapter 1 explains the properties most important to our understanding of how it impacts our digital world. If I do my job right, you'll understand it better than 99 percent of everyone else in the computer world.

Chapter 2, "Introduction to Quantum Computers"

Quantum computers use quantum properties to provide capabilities, logic, and arithmetic outcomes that are simply not possible with traditional binary computers. Chapter 2 covers the different types of quantum computers, the various quantum properties they support, and where they are likely headed in the next decade as we become surrounded by them.

Chapter 3, "How Can Quantum Computing Break Today's Cryptography?"

The most common question asked when a person is told that quantum computers will likely break traditional public key cryptography is how. Chapter 3 tells why traditional binary computers can't easily break most public key crypto and how quantum computers likely will. It covers what quantum computers are likely to break and what is resistant to quantum computing power.

Chapter 4, "When Will the Quantum Crypto Break Happen?"

After explaining how quantum computers will likely break traditional public key crypto, the second most often asked question is when it will happen. Although no one (publicly) knows, it is likely to be sooner than later. Chapter 4 discusses the different possible timings and their possibilities.

Chapter 5, "What Will a Post-Quantum World Look Like?"

Like the invention of the Internet, there will be a world before and a world after quantum supremacy. Quantum will solve problems that have plagued us for centuries and will give us new problems that will vex us in the future. Chapter 5 will describe that post-quantum world and how it will impact you.

Part II, "Preparing for the Quantum Break," will help you and your organization most efficiently prepare for the coming quantum supremacy.

Chapter 6, "Quantum-Resistant Cryptography"

Chapter 6 covers over two dozen quantum-resistant ciphers and schemes, which the National Institute of Standards and Technology (NIST) is considering in the second round of its post-quantum

contest. Two or more of these quantum-resistant algorithms will become the next U.S. national cryptography standards. Read about the competitors and their strengths and weaknesses.

Chapter 7, "Quantum Cryptography"
Chapter 6 covered traditional binary quantum-resistant cryptography, which does not use quantum properties to provide protection. Chapter 7 covers ciphers and schemes, which do use quantum properties to provide their cryptographic strength. In the long run, you will likely be using quantum-based cryptography and not just quantum-resistant cryptography. Come learn what that looks like.

Chapter 8, "Quantum Networking"
Chapter 8 covers quantum-based networking devices, such as quantum repeaters, and the applications that are seeking quantum network protection. It covers the current state of quantum networking and where it will likely be over the near-term and long-term futures. One day the entire Internet will likely be quantum-based. Read about those networking parts and components and how we will get there.

Chapter 9, "Preparing Now"
Chapter 9 is a perfect reason to buy this book. It tells any organization how they can start preparing today for the coming quantum cryptographic break. It tells you what you can do today to protect your most critical long-term secrets, what cryptographic key sizes you need to increase, and what has to be replaced and when. The summarized plan has been used in previous global cryptographic updates and can be used to ward off a cryptographic apocalypse.

The appendix lists dozens of links to quantum information resources, including books, videos, blogs, white papers, and websites.

If I've done my job correctly, by the end of this book you will comprehend quantum physics better than ever before, understand how it will break today's traditional public key cryptography, and be able to appropriately prepare and better protect your critical digital secrets.

How to Contact Wiley or the Author

Wiley strives to keep you supplied with the latest tools and information you need for your work. Please check the website at `www.wiley.com/go/cryptographyapocalypse`, where I'll post additional content and updates that supplement this book should the need arise.

If you have any questions, suggestions, or corrections, feel free to email me at `roger@banneretcs.com`.

Quantum Computing Primer