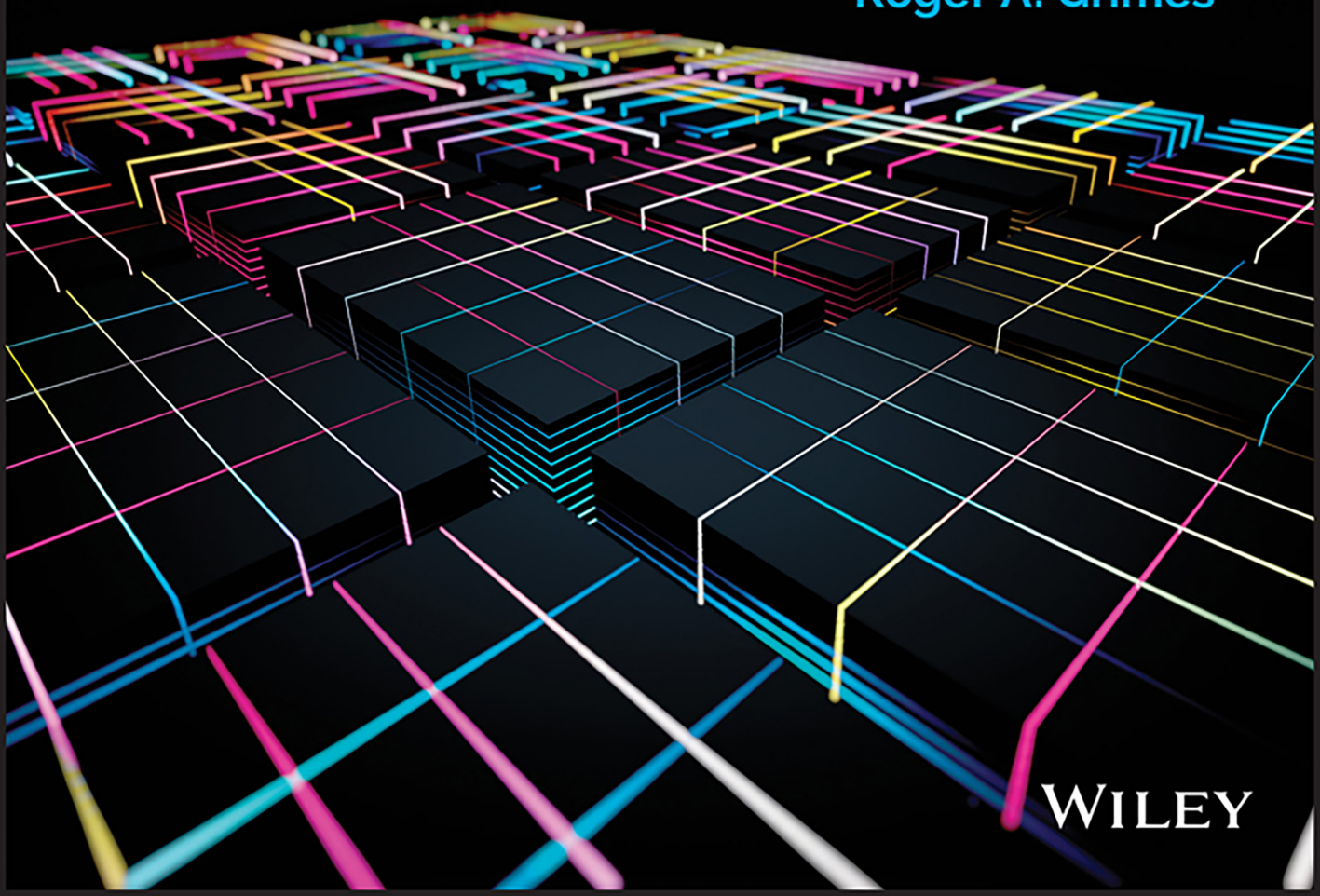


Cryptography Apocalypse

**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

Copyright © 2020 by John Wiley & Sons, Inc.

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

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2019946679

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

*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 Poepplmann 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 Mafla 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

Introduction	xxi
I Quantum Computing Primer	1
1 Introduction to Quantum Mechanics.....	3
2 Introduction to Quantum Computers	31
3 How Can Quantum Computing Break Today's Cryptography?	59
4 When Will the Quantum Crypto Break Happen?	85
5 What Will a Post-Quantum World Look Like?	99
II Preparing for the Quantum Break	127
6 Quantum-Resistant Cryptography	129
7 Quantum Cryptography	167
8 Quantum Networking	189
9 Preparing Now	207
Appendix: Additional Quantum Resources	231
Index	239

Contents

Introduction	xxi
I Quantum Computing Primer	1
1 Introduction to Quantum Mechanics	3
What Is Quantum Mechanics?	3
Quantum Is Counterintuitive	4
Quantum Mechanics Is Real	5
The Basic Properties of Quantum Mechanics	8
Photons and Quantum Mechanics	8
Photoelectric Effect	9
Wave-Particle Duality	10
Probability Principle	14
Uncertainty Principle	17
Spin States and Charges	20
Quantum Tunneling	20
Superposition	21
Observer Effect	22
No-Cloning Theorem	24
Spooky Entanglement	24
Decoherence	25
Quantum Examples in Our World Today	27
For Additional Information	28
Summary	29
2 Introduction to Quantum Computers	31
How Are Quantum Computers Different?	31
Traditional Computers Use Bits	31

Quantum Computers Use Qubits	33
Quantum Computers Are Not Ready for Prime Time Yet	37
Quantum Will Reign Supreme Soon.	38
Quantum Computers Improve Qubits Using Error Correction	39
Types of Quantum Computers	44
Superconducting Quantum Computers	44
Quantum Annealing Computers	45
Universal Quantum Computers	47
Topological Quantum Computers	49
Microsoft Majorana Fermion Computers	50
Ion Trap Quantum Computers	51
Quantum Computers in the Cloud.	53
Non-U.S. Quantum Computers	53
Components of a Quantum Computer.	54
Quantum Software	55
Quantum Stack	55
Quantum National Guidance	56
National Policy Guidance.	56
Money Grants and Investments.	56
Other Quantum Information Science Besides Computers	57
For More Information	58
Summary	58
3 How Can Quantum Computing Break Today's Cryptography?	59
Cryptography Basics.	59
Encryption.	59
Integrity Hashing	72
Cryptographic Uses	73
How Quantum Computers Can Break Cryptography	74
Cutting Time	74
Quantum Algorithms.	76
What Quantum Can and Can't Break	79
Still Theoretical	82
Summary	83

4	When Will the Quantum Crypto Break Happen?	85
	It Was Always “10 Years from Now”	85
	Quantum Crypto Break Factors.	86
	Is Quantum Mechanics Real?	86
	Are Quantum Computers Real?	87
	Is Superposition Real?	87
	Is Peter Shor’s Algorithm Real?	88
	Do We Have Enough Stable Qubits?	88
	Quantum Resources and Competition	89
	Do We Have Steady Improvement?	89
	Expert Opinions.	90
	When the Quantum Cyber Break Will Happen	90
	Timing Scenarios	90
	When Should You Prepare?	93
	Breakout Scenarios	95
	Stays in the Realm of Nation-States for a Long Time	95
	Used by Biggest Companies.	97
	Mass Proliferation	97
	Most Likely Breakout Scenario	97
	Summary	98
5	What Will a Post-Quantum World Look Like?	99
	Broken Applications	99
	Weakened Hashes and Symmetric Ciphers.	100
	Broken Asymmetric Ciphers.	103
	Weakened and Broken Random Number Generators	103
	Weakened or Broken Dependent Applications	104
	Quantum Computing.	114
	Quantum Computers.	114
	Quantum Processors	115
	Quantum Clouds	115
	Quantum Cryptography Will Be Used.	116
	Quantum Perfect Privacy	116
	Quantum Networking Arrives.	117

Quantum Applications	117
Better Chemicals and Medicines	118
Better Batteries	118
True Artificial Intelligence.	119
Supply Chain Management	120
Quantum Finance	120
Improved Risk Management	120
Quantum Marketing	120
Better Weather Prediction	121
Quantum Money	121
Quantum Simulation	122
More Precise Military and Weapons	122
Quantum Teleportation	122
Summary	126
II Preparing for the Quantum Break	127
6 Quantum-Resistant Cryptography	129
NIST Post-Quantum Contest.	129
NIST Security Strength Classifications	132
PKE vs. KEM.	133
Formal Indistinguishability Assurances	134
Key and Ciphertext Sizes	135
Types of Post-Quantum Algorithms	136
Code-Based Cryptography.	136
Hash-Based Cryptography	137
Lattice-Based Cryptography.	138
Multivariate Cryptography.	140
Supersingular Elliptic Curve Isogeny Cryptography	140
Zero-Knowledge Proof.	141
Symmetric Key Quantum Resistance	142
Quantum-Resistant Asymmetric Encryption Ciphers.	143
BIKE.	145
Classic McEliece	145

CRYSTALS-Kyber	146
FrodoKEM	146
HQC	147
LAC	148
LEDACrypt	148
NewHope	149
NTRU	149
NTRU Prime	150
NTS-KEM	150
ROLLO	151
Round5	151
RQC	151
SABER	152
SIKE	152
ThreeBears	153
General Observations on PKE and KEM Key and Ciphertext Sizes	155
Quantum-Resistant Digital Signatures	156
CRYSTALS-Dilithium	156
FALCON	157
GeMSS	158
LUOV	158
MQDSS	159
Picnic	159
qTESLA	160
Rainbow	160
SPHINCS+	161
General Observations on Signature Key and Sizes	162
Caution Advised	164
A Lack of Standards	164
Performance Concerns	165
Lack of Verified Protection	165
For Additional Information	166
Summary	166

7	Quantum Cryptography	167
	Quantum RNGs	168
	Random Is Not Always Random	168
	Why Is True Randomness So Important?	170
	Quantum-Based RNGs	172
	Quantum Hashes and Signatures	177
	Quantum Hashes	177
	Quantum Digital Signatures	178
	Quantum Encryption Ciphers	180
	Quantum Key Distribution	181
	Summary	188
8	Quantum Networking	189
	Quantum Network Components	189
	Transmission Media	189
	Distance vs. Speed	191
	Point-to-Point	192
	Trusted Repeaters	193
	True Quantum Repeaters	194
	Quantum Network Protocols	196
	Quantum Network Applications	199
	More Secure Networks	199
	Quantum Computing Cloud	200
	Better Time Syncing	200
	Prevent Jamming	201
	Quantum Internet	202
	Other Quantum Networks	203
	For More Information	204
	Summary	204
9	Preparing Now	207
	Four Major Post-Quantum Mitigation Phases	207
	Stage 1: Strengthen Current Solutions	207
	Stage 2: Move to Quantum-Resistant Solutions	211
	Stage 3: Implement Quantum-Hybrid Solutions	213

Stage 4: Implement Fully Quantum Solutions	214
The Six Major Post-Quantum Mitigation Project Steps	214
Step 1: Educate	215
Step 2: Create a Plan	220
Step 3: Collect Data	225
Step 4: Analyze	226
Step 5: Take Action/Remediate.	228
Step 6: Review and Improve.	230
Summary	230
Appendix: Additional Quantum Resources	231
Index	239

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 an 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

Chapter 1: What is Quantum?

Chapter 2: Quantum Computers

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

Chapter 4: When Will the Quantum Crypto Break Happen?

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

