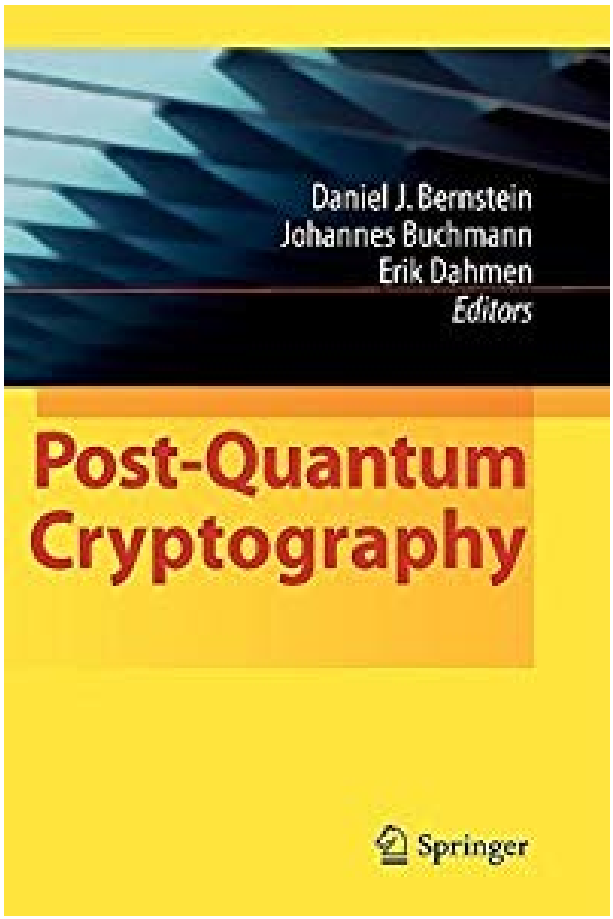
Post-Quantum Cryptography



ISBN13:	9783540887010
Genre:	Uncategorized
Published:	November 19th 2008 by Springer
Pages:	246
Language	English
ISBN10:	3540887016
Author:	Daniel J. Bernstein
Goodreads Rating:	2.75

Quantum computers will break today's most popular public-key cryptographic systems, including RSA, DSA, and ECDSA. This book introduces the reader to the next generation of cryptographic algorithms, the systems that resist quantum-computer attacks: in particular, post-quantum public-key encryption systems and post-quantum public-key signature systems. Leading experts have joined forces for the first time to explain the state of the art in quantum computing, hash-based cryptography, code-based cryptography, lattice-based cryptography, and multivariate cryptography. Mathematical foundations and implementation issues are included. This book is an essential resource for students and researchers who want to contribute to the field of post-quantum cryptography.