

Quantum Computing, Cyber Security and Cryptography

Issues, Technologies, Algorithms, Programming and Strategies

This book examines the fundamentals of quantum computing and its applications in codebreaking and hacking, as well as strategies and technologies for defending systems against quantum attacks. It brings together leading experts from across academia and industry to provide a comprehensive overview of the impacts of quantum computing on cybersecurity and cryptography. As quantum computers become more powerful and practical in the coming years, they pose a serious threat to current encryption and cybersecurity methods which rely on computational difficulty. The book provides readers with a holistic understanding of the quantum computing landscape and its implications on information security. The chapters cover the foundational concepts of quantum mechanics and key quantum algorithms relevant to cryptography and cybersecurity. Detailed discussions on quantum cryptanalysis, post-quantum cryptography, quantum key distribution, and quantum random number generation equip readers with technical knowledge of quantum-safe cryptosystems. Practical topics such as quantum programming, software tools, and implementation of quantum-resistant solutions in different sectors like finance, healthcare, and the Internet of Things provide actionable insights for organizations. The book concludes with an analysis of collaborative strategies, policies and future research directions to foster innovation in quantum-safe cybersecurity. Overall, this book serves as an essential reference for security professionals, researchers, students, and technology leaders interested in preparing systems and data for the quantum computing era.

This book examines the fundamentals of quantum computing and its applications in codebreaking and hacking, as well as strategies and technologies for defending systems against quantum attacks. It brings together leading experts from across academia and industry to provide a comprehensive overview of the impacts of quantum computing on cybersecurity and cryptography. As quantum computers become more powerful and practical in the coming years, they pose a serious threat to current encryption and cybersecurity methods which rely on computational difficulty. The book provides readers with a holistic understanding of the quantum computing landscape and its implications on information security. The chapters cover the foundational concepts of quantum mechanics and key quantum algorithms relevant to cryptography and cybersecurity. Detailed discussions on quantum cryptanalysis, post-quantum cryptography, quantum key distribution, and quantum random number generation equip readers with technical knowledge of quantum-safe cryptosystems. Practical topics such as quantum programming, software tools, and implementation of quantum-resistant solutions in different sectors like finance, healthcare, and the Internet of Things provide actionable insights for organizations. The book concludes with an analysis of collaborative strategies, policies and future research directions to foster innovation in quantum-safe cybersecurity. Overall, this book serves as an essential reference for security professionals, researchers, students, and technology leaders interested in preparing systems and data for the quantum computing era.

 **fachmedien.de**
WISSEN. EINFACH. FINDEN.

160,49 €

149,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9789819649501

Medium: Buch

ISBN: 978-981-964950-1

Verlag: Springer

Erscheinungstermin: 21.07.2026

Sprache(n): Englisch

Auflage: Erscheinungsjahr 2026

Produktform: Kartoniert

Seiten: 504

Format (B x H): 155 x 235 mm

