1. Record Nr. UNINA9911015968003321

Autore	Goyal S. B
Titolo	Quantum Computing, Cyber Security and Cryptography : Issues, Technologies, Algorithms, Programming and Strategies / / edited by S. B. Goyal, Vidyapati Kumar, Sardar M. N. Islam, Deepika Ghai
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2025
ISBN	981-9649-48-X
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (601 pages)
Altri autori (Persone)	KumarVidyapati IslamSardar M. N GhaiDeepika
Disciplina	006.3843 530.12
Soggetti	Quantum computers Quantum communication Data protection Artificial intelligence Artificial intelligence - Data processing Quantum Computing Quantum Communications and Cryptography Data and Information Security Artificial Intelligence Data Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction to Quantum Computing -- 2. Quantum Computing Technologies -- 3. Quantum Algorithms -- 4. Quantum Programming Languages and Tools -- 5. Quantum Computing and Cyber Security -- 6. Quantum Cryptography Technologies -- 7. Quantum Computing and National Security -- 8. Quantum Computing and Financial Sector -- 9. Quantum Computing and Data Privacy -- 10. Quantum Computing and the Internet of Things (IoT) -- 11. Quantum Cybersecurity Strategies -- 12. Future Prospects of Quantum Computing and Cyber Security -- Appendix A: Glossary of Quantum Computing and Cryptography Terms

-- Appendix B: Selected Quantum Computing Resources -- Appendix C: List of Quantum Computing and Cyber Security Companies.

Sommario/riassunto

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.