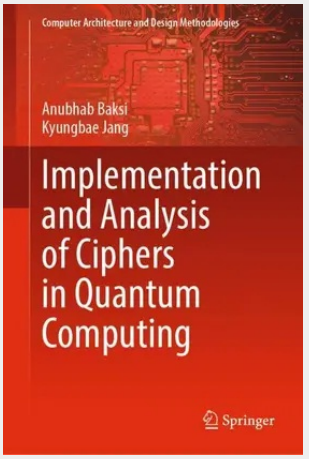
Baksi / Jang

Implementation and Analysis of Ciphers in Quantum Computing

This book deals with the upcoming threat that may be posed by quantum computers on modern-day security standards, particularly those involving symmetric key ciphers. Considering the progress in the field of quantum computing over the past few years, there is an ever-growing need to analyze the ciphers that are being employed in ensuring security. The symmetric key ciphers are generally considered safe against quantum computers, though one must consider the possible impact due to Grover's search algorithm (that reduces the security claim to the square root bound of what is expected against a classical computer). This book consolidates all the major research works in one place and presents it with adequate clarity, making the subject matter easy to understand for seasoned researchers and students alike. It covers the prerequisite information, new research works (including some of the state of the art), thought-provoking problems for further research, and all the relevant source codes. This book is interesting to engineers, researchers, and students who work/study in the field of cryptography.

This book deals with the upcoming threat that may be posed by quantum computers on modern-day security standards, particularly those involving symmetric key ciphers. Considering the progress in the field of quantum computing over the past few years, there is an ever-growing need to analyze the ciphers that are being employed in ensuring security. The symmetric key ciphers are generally considered safe against quantum computers, though one must consider the possible impact due to Grover's search algorithm (that reduces the security claim to the square root bound of what is expected against a classical computer). This book consolidates all the major research works in one place and presents it with adequate clarity, making the subject matter easy to understand for seasoned researchers and students alike. It covers the prerequisite information, new research works (including some of the state of the art), thought-provoking problems for further research, and all the relevant source codes. This book is interesting to engineers, researchers, and students who work/study in the field of cryptography.



149,79 €
139,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9789819700240
Medium: Buch
ISBN: 978-981-97-0024-0
Verlag: Springer
Erscheinungstermin: 18.04.2024
Sprache(n): Englisch
Auflage: 2024
Serie: Computer Architecture and Design Methodologies
Produktform: Gebunden
Gewicht: 455 g
Seiten: 151
Format (B x H): 160 x 241 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)