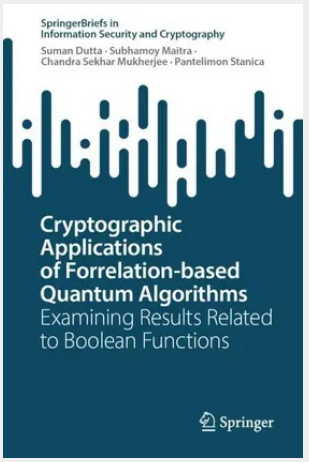
Dutta / Maitra / Mukherjee

# Cryptographic Applications of Forrelation-based Quantum Algorithms

Examining Results Related to Boolean Functions




**58,84 €**
54,99 € (zzgl. MwSt.)

*vorbestellbar, Erscheinungstermin ca. Dezember 2026*

This book provides a research-level treatment of quantum algorithms for analyzing Boolean functions through the framework of Forrelation. It develops a unified account of how Forrelation, nega-Forrelation, and generalized Forrelation can be used to study major Boolean-function spectra, including Walsh-Hadamard, nega-Hadamard, crosscorrelation, and autocorrelation spectra, along with related questions on bent, negabent, and their hidden-shift structures. The central aim is to connect modern quantum query complexity related techniques with spectral problems that are fundamental in cryptography, coding theory, and the combinatorial theory of Boolean functions. The book begins with the necessary background on Boolean functions and basics of quantum computing, making the later chapters substantially self-contained. It then develops three main contributions. First, it studies Forrelation as a tool for sampling and estimating Walsh-Hadamard, crosscorrelation, and autocorrelation spectra, including applications to resiliency testing and bounded-degree uncorrelatedness checking. Next, it introduces nega-Forrelation and uses it to design quantum algorithms for estimating nega-Hadamard, nega-crosscorrelation, and nega-autocorrelation spectra, while linking these methods to hidden-shift problems involving bent and negabent functions. Finally, it presents a generalized framework based on roots of unity, extending prior transform-based methods and introducing generalized Deutsch-Jozsa and generalized Forrelation algorithms. The topic is timely because Forrelation is one of the landmark problems establishing a separation between the probabilistic classical and bounded-error quantum models, and the spectral analysis of Boolean functions remains central to the design and evaluation of cryptographic primitives. By bringing these strands together, the book offers both new algorithmic perspectives and a coherent mathematical framework for spectral analysis in the quantum setting. The primary audience of this book comprises researchers, advanced graduate students, and specialists in cryptography, discrete mathematics, and quantum computation.

This book provides a research-level treatment of quantum algorithms for analyzing Boolean functions through the framework of Forrelation. It develops a unified account of how Forrelation, nega-Forrelation, and generalized Forrelation can be used to study major Boolean-function spectra, including Walsh-Hadamard, nega-Hadamard, crosscorrelation, and autocorrelation spectra, along with related questions on bent, negabent, and their hidden-shift structures. The central aim is to connect modern quantum query complexity related techniques with spectral problems that are fundamental in cryptography, coding theory, and the combinatorial theory of Boolean functions. The book begins with the necessary background on Boolean functions and basics of quantum computing, making the later chapters substantially self-contained. It then develops three main contributions. First, it studies Forrelation as a tool for sampling and estimating Walsh-Hadamard, crosscorrelation, and autocorrelation spectra, including applications to resiliency testing and bounded-degree uncorrelatedness checking. Next, it introduces nega-Forrelation and uses it to design quantum algorithms for estimating nega-Hadamard, nega-crosscorrelation, and nega-autocorrelation spectra, while linking these methods to hidden-shift problems involving bent and negabent functions. Finally, it presents a generalized framework based on roots of unity, extending prior transform-based methods and introducing generalized Deutsch-Jozsa and generalized Forrelation algorithms. The topic is timely because Forrelation is one of the landmark problems establishing a separation between the probabilistic classical and bounded-error quantum models, and the spectral analysis of Boolean functions remains central to the design and evaluation of cryptographic primitives. By bringing these strands together, the book offers both new algorithmic perspectives and a coherent mathematical framework for spectral analysis in the quantum setting. The primary audience of this book comprises

**Artikelnummer:** 9783032395900
**Medium:** Buch
**ISBN:** 978-3-032-39590-0
**Verlag:** Springer
**Erscheinungstermin:** 03.12.2026
**Sprache(n):** Englisch
**Auflage:** Erscheinungsjahr 2026
**Serie:** SpringerBriefs in Information Security and Cryptography
**Produktform:** Kartoniert
**Seiten:** 96
**Format (B x H):** 155 x 235 mm



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