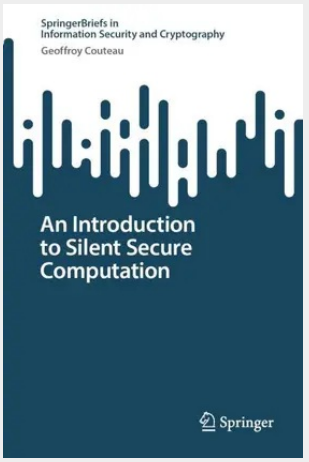
Couteau

An Introduction to Silent Secure Computation



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Secure computation allows any number of mutually distrustful parties to jointly run an arbitrary computation on their combined inputs without compromising their privacy. Secure computation offers a theoretical solution to a vast array of problems where one wishes to simultaneously maintain a fine-grained control over the users' privacy and have flexibility in how their data is used in a protocol. Over the past decade, secure computation has largely emerged from the depth of theoretical research to enter the realm of practically-usable technologies, and secure protocols are now routinely implemented and deployed. This is the result of a widespread and ongoing research effort from the cryptography community, which has produced a diverse ecosystem of protocols and paradigms optimized for a variety of concrete applications. This book covers one such recent paradigm, the area of silent secure computation, which strikes a careful balance between communication and computation overheads. This paradigm has recently emerged as a promising path towards fast secure computation in bandwidth-restricted settings, and has had a significant influence on the landscape of practical secure computation. The goal of the book is to provide an accessible introduction to silent secure computation. It is aimed at Ph.D. students and researchers in cryptography and has a strong focus on explaining the intuitions and giving the reader a sense of scale, in the hope of conveying insights about the practicality of silent secure computation in various contexts and to give a clear overview of some of the core challenges in the field.

Secure computation allows any number of mutually distrustful parties to jointly run an arbitrary computation on their combined inputs without compromising their privacy. Secure computation offers a theoretical solution to a vast array of problems where one wishes to simultaneously maintain a fine-grained control over the users' privacy and have flexibility in how their data is used in a protocol. Over the past decade, secure computation has largely emerged from the depth of theoretical research to enter the realm of practically-usable technologies, and secure protocols are now routinely implemented and deployed. This is the result of a widespread and ongoing research effort from the cryptography community, which has produced a diverse ecosystem of protocols and paradigms optimized for a variety of concrete applications. This book covers one such recent paradigm, the area of silent secure computation, which strikes a careful balance between communication and computation overheads. This paradigm has recently emerged as a promising path towards fast secure computation in bandwidth-restricted settings, and has had a significant influence on the landscape of practical secure computation. The goal of the book is to provide an accessible introduction to silent secure computation. It is aimed at Ph.D. students and researchers in cryptography and has a strong focus on explaining the intuitions and giving the reader a sense of scale, in the hope of conveying insights about the practicality of silent secure computation in various contexts and to give a clear overview of some of the core challenges in the field.

Artikelnummer: 9783032070883
Medium: Buch
ISBN: 978-3-032-07088-3
Verlag: Springer
Erscheinungstermin: 24.04.2026
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2026
Serie: SpringerBriefs in Information Security and Cryptography
Produktform: Kartoniert
Gewicht: 242 g
Seiten: 142
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)