Vorwort von Prof. Paar

Abb. 1: Prof. Dr. Christof Paar
Direktor am Max-Planck-Institut für Sicherheit und Privatsphäre

Das vorliegende Buch zeichnet sich durch eine durchdachte Zusammenstellung hoch relevanter Themen in der Kryptografie aus, die einen einfachen Zugang zu diesem extrem spannenden Fachgebiet ermöglicht. Der Autor, Prof. Bernhard Esslinger, kann auf jahrzehntelange Erfahrung sowohl im akademischen Umfeld als auch in der Industrie zurückblicken, was sich in der geschickten Themenmischung aus Theorie und Praxis widerspiegelt.

In dem Buch ist der seltene Brückenschlag zwischen historischen Chiffren, die für das Verstehen der modernen Kryptografie sehr hilfreich sind, und moderner praxisrelevanter Kryptografie hervorragend gelungen. Im Bereich der asymmetrischen (oder auch: public-key) Kryptografie wird nicht nur das ganze Spektrum der heutzutage eingesetzten Algorithmen eingeführt, sondern es werden auch die nächste Generation von Verfahren behandelt, die sogenannte post-quantum Kryptografie. En passant gelingt es Prof. Esslinger, auch wichtige mathematische Konzepte aus dem Bereich der Zahlentheorie elegant einzuführen.

Durch die gelungene Kombination von Themen richtet sich das Werk an ein breites Publikum, nicht nur an naturwissenschaftlich Vorgebildete. Besonders hervorzuheben ist die Möglichkeit, die vorgestellten Verfahren direkt anhand der in den Fußnoten angegebenen Links zu Open-Source-Programmen wie CrypTool, OpenSSL oder SageMath auszuprobieren. Dies wird durch zahlreiche Screenshots unterstützt, die das Interesse wecken und den Einstieg erleichtern.

Ich freue mich, dass die immer noch recht beschränkte Auswahl an echten Lehrbüchern im Bereich der Kryptografie mit diesem Werk deutlich erweitert und bereichert wird!

Bochum, Oktober 2024 Christof Paar