Vorwort zur 8. Auflage

Uns haben zwei Entwicklungen dazu bewogen, eine weitere Auflage des Buches heraus zu bringen.

Zum einen haben Popularität und Bedeutung der Kryptographie seit den Mitte 2013 bekannt gewordenen Enthüllungen über grenzenloses Ausspähen spürbar zugenommen. Dabei genügt es natürlich nicht, vielfältige kryptografisch basierte Sicherheitslösungen zur Verfügung zu haben, diese müssen auch in konkreten Anwendungen implementiert und schließlich auch genutzt werden.

Zum anderen wird das Buch der durchweg positiven Resonanz zufolge zunehmend als Lehrbuch der Kryptographie herangezogen, nicht nur in Hochschulen, sondern auch in entsprechenden Vertiefungsfächern von Gymnasien. Dementsprechend haben wir den Stoff an einigen Stellen auf den neuesten Stand gebracht (Quantenkryptographie) und wichtige neue Themengebiete mit aufgenommen.

Kryptographie basierend auf elliptischen Kurven ist längst schon in der Praxis angekommen, sie wird in der Diffie-Hellman-Schlüsselvereinbarung und in digitalen Signaturverfahren eingesetzt. In Abschn. 8.1 werden sie kurz vorgestellt. Aus der Theorie der elliptischen Kurven heraus wurde in den letzten Jahren das Gebiet der Pairings basierten Kryptosysteme erschlossen: Pairings oder Bilineare Abbildungen ermöglichen es, viele Probleme der Kryptographie auf überraschend einfache Weise zu lösen, angefangen bei kurzen Signaturen über identitätsbasierte Kryptographie bis hin zu komplexen Beweissystemen.

Gießen, Bochum, Berlin, Juli 2015

Albrecht Beutelspacher
Jörg Schwenk
Klaus-Dieter Wolfenstetter

http://www.springer.com/978-3-8348-1927-7

Moderne Verfahren der Kryptographie
Von RSA zu Zero-Knowledge
Beutelspacher, A.; Schwenk, J.; Wolfenstetter, K.-D.
2015, XV, 186 S. 86 Abb., Softcover
ISBN: 978-3-8348-1927-7