Preface to the Third, Extended Edition

The third edition is a substantive extension. This is reflected in a considerable increase in pages. A number of new topics have been included. They supplement and extend the material covered in the previous editions. The major extensions and enhancements follow:

- We added a description of the new SHA-3 algorithm for cryptographic hash functions, Keccak, and the underlying sponge construction (Section 2.2.2).
- As a further important example of homomorphic encryption algorithms, Paillier encryption is introduced in Section 3.6.2.
- ElGamal encryption in a prime-order subgroup of a finite field is studied in detail in Section 3.4.4.
- An introduction to elliptic curve cryptosystems including Diffie–Hellman key exchange, ElGamal encryption and the elliptic curve digital signature standard ECDSA is given in Section 3.7.
- The basics of plane curves and elliptic curves that are necessary to understand elliptic curve cryptography are explained in Appendix A.11.
- Additional concepts of interactive proof systems, such as the special honest-verifier zero-knowledge property and the OR-combination of Σ-proofs, are addressed in Section 4.5.
- The exposition of cryptographic protocols for electronic elections and Internet voting has been substantially extended (Sections 4.6 and 4.7).
- Decryption and re-encryption mix nets and shuffles as the basic tools to anonymize communication are discussed in Section 4.6. A complete zero-knowledge proof for the correctness of a re-encryption shuffle is given. Such proofs are indispensable in critical applications of mix nets, such as electronic voting systems. The correct operations of the mix net must be publicly verifiable, without compromising the confidentiality of individual votes.
- Receipt-free and coercion-resistant elections are studied in Section 4.7. Various techniques that are useful in the design of cryptographic protocols are explained here, such as designated-verifier proofs, diverted proofs, untappable channels and plaintext equivalence tests.
- Unconditionally secure cryptographic schemes are not based on the practical infeasibility of a computational task. Their security is proven by using

methods from information theory. Unconditionally secure schemes are now addressed in an extra chapter, Chapter 10.

- Unconditional security is not achievable without an unconditionally secure authentication of the communication partners. Suitable message authentication codes are constructed from almost universal classes of hash functions in Section 10.3.
- Privacy amplification is one of the essential techniques to derive an unconditionally secure shared secret key from information that is publicly exchanged. We give a proof of the Privacy Amplification Theorem and explain the basic properties of Rényi entropy.
- In Section 10.5, we present an introduction to quantum cryptography. We describe, in detail, the famous BB84 protocol of Bennett and Brassard for quantum key distribution and prove its security, assuming intercept-and-resend attacks.

The description of cryptographic hash functions has been moved to Chapter 2, which is now headlined "Symmetric-Key Cryptography". Moreover, errors and inaccuracies have been corrected, and in some places, the exposition has been clarified.

Some exercises have been added. Answers to all exercises are provided on the webpage www.in.th-nuernberg.de/DelfsKnebl/Cryptography.

We thank our readers and our students for their comments and hints. Again, we are greatly indebted to our colleague Patricia Shiroma-Brockmann for proof-reading the English copy of the new and revised chapters. Finally, we would like to thank Ronan Nugent at Springer for his support.

Nürnberg, July 2015 Hans Delfs, Helmut Knebl