

Preface

If we knew what it was we were doing, it would not be called research, would it?

ALBERT EINSTEIN (1879–1955)
The 1921 Nobel Laureate in Physics

In research, if you know what you are doing, then you shouldn't be doing it.

RICHARD HAMMING (1915–1998)
The 1968 Turing Award Recipient

It is well known that the security of the most widely used public-key cryptosystems such as RSA (Rivest-Shamir-Adleman), DSA (digital signature algorithm), and ECC (elliptic curve cryptography) relies on the intractability of one of the following three number-theoretic problems, namely, the integer factorization problem (IFP), the discrete logarithm problem (DLP), and the elliptic curve discrete logarithm problem (ECDLP). Since no polynomial-time algorithms have been found so far for solving these three hard problems, the cryptosystems based on them are secure. There are, however, quantum algorithms, due to Shor and others, which can solve these three intractable problems in polynomial time, provided that a practical quantum computer can be constructed.

The monograph provides a quantum approach to solve all these three intractable number-theoretic problems and to attack the cryptosystems based on these three problems. The organization of the book is as follows. Chapter 1 provides an introduction to the basic concepts and ideas of quantum computation. Chapter 2 discusses Shor's quantum factoring algorithm and its application to the cryptanalysis of IFP-based, particularly RSA cryptosystems. Chapter 2 discusses Shor's quantum discrete logarithm algorithm and its application to the cryptanalysis of DLP-based cryptosystems.

Chapter 4 is devoted to the study of the extension of Shor's quantum algorithms for solving the ECDLP problems and the attacks on the ECDLP-based cryptosystems. Finally in Chapter 5, some quantum resistant public-key cryptosystems are studied, which can be used in the post-quantum age.

The monograph is a revised and extended version of the author's earlier version *Cryptanalytic Attacks on RSA*, with an emphasis on quantum attacks for public-key cryptography. It is self-contained and can be used as a basic reference for computer scientists, mathematicians, electrical engineers, and physicists, interested in quantum computation and quantum cryptography. It can also be used as a final year undergraduate or a 1st-year graduate text in the field.

Acknowledgments

The author would like to thank the three anonymous referees for their very helpful suggestions and comments. Special thanks must be given to Prof Michael Sipser and Prof Ronald Rivest at MIT, Prof Benedict Gross at Harvard, Susan Lagerstrom-Fife, Courtney Clark and Jennifer Maurer at Springer New York, for their encouragement, support, and help. The research was supported in part by the Royal Academy of Engineering, London, the Royal Society, London, Harvard University, Massachusetts Institute of Technology, and Wuhan University.

Finally, the author would specifically like to thank Prof Yanxiang He, Dean of Computer School of Wuhan University for his encouragement, support, and collaboration.

Cambridge, MA

S.Y. Yan



<http://www.springer.com/978-1-4419-7721-2>

Quantum Attacks on Public-Key Cryptosystems

Yan, S.Y.

2013, VIII, 207 p., Hardcover

ISBN: 978-1-4419-7721-2