Review of the book

"Post-Quantum Cryptography"

by Daniel J. Bernstein, Johannes Buchmann and Erik Dahmen (Editors)
Springer, 2010

ISBN: 978-3-642-10019-2

Edoardo Persichetti
University of Warsaw
June 2014

1 Summary of the review

In this review I present the book "Post-Quantum Cryptography". This volume gives a detailed, technical-level treatment of the post-quantum cryptography universe.

2 Summary of the book

When (if?) quantum computers of a big enough size will be available, most of the current public-key cryptography primitives based on number theory will be vulnerable. The "next generation" of cryptographic algorithms is commonly grouped into what is called Post-Quantum Cryptography. This is mainly divided in four areas: hash-based cryptography, code-based cryptography, lattice-based cryptography and multivariate cryptography. In this book, the editors put together the leading experts in the four areas to present the state of the art in each of the four incarnations of this exciting new research area.

3 Main Review

The main part of the book is, as expected, formed by four chapters, one for each of the areas mentioned above. In addition, the book features an introduction section and a preliminary chapter on Quantum Computing.

The introduction chapter, written by Bernstein, presents the contents of the book ahead, in a typical witty and provocative way. The author gives three examples, explained in layman's terms, of post-quantum primitives: the Lamport-Diffie one-time signature scheme, based on hash functions, the Niederreiter cryptosystem, based on linear codes, and the HFE signature scheme, based on multivariate equations. The chapter continues by illustrating the main challenges of post-quantum cryptography, namely improving the efficiency, strengthening the confidence in the area, and enlarging the usability of the primitives. The chapter is concluded with a brief comparison with Quantum cryptography, i.e. cryptography based on actual quantum algorithms.

The second chapter, written by Hallgren and Vollmer, is a natural continuation of the introduction, and focuses on how quantum algorithms actually work. After a brief section regarding state of the art quantum-secure algorithms, the authors proceed to explain the computational model and the quantum Fourier transform. The cornerstone of quantumly solvable problems, the Hidden Subgroup Problem (HSP) is presented in detail. The chapter is concluded with a presentation of search algorithms and a brief conclusions section.

The third chapter is the first dealing with actual post-quantum primitives. Buchmann, Dahmen and Szydlo describe hash-based signature schemes in rigorous detail. As a warm-up, the famous Lamport-Diffie one-time signature scheme (already hinted at in the introduction) is described, this time more accurately, along with a more efficient variant, the Winternitz scheme. The next step is presenting the Merkle's tree structure, that allows to transform every one-time signature scheme in a full-fledge signature scheme by using a binary tree and a cryptographic hash function. After explaining how to generate keys with a PRNG, the tree concept is expanded in Section 4, where a variety of techniques for the authentication path computation are illustrated. This is by far the largest and more detailed part of the chapter. In section 5, the authors present the "tree chaining" technique, designed to solve some problems intrinsic to the Merkle tree structure. At the same time, some new problems arise by using this technique: these are addressed by distributed signature generation, explained in Section 6. Finally, the chapter is concluded with a section dedicated to a careful security analysis.

The next area is that of code-based cryptography. In the chapter, written by Overbeck and Sendrier, this interesting area of cryptography is described extensively, even if not necessarily in a logical order. The first things to be described, in fact, are code-based cryptosystems (McEliece and Niederreiter), signature scheme (CFS), identification scheme (Stern's) and even a hash function. The "background" on coding theory problems (in particular syndrome decoding and its variants) is relegated to the following section. In the same section, the authors give a brief presentation of general decoding attacks. After this, back to code-based primitives, now with an eye to code families and structures. The section begins with a paragraph on code equivalence and the support-splitting algorithm, and includes a discussion on structural attacks against original McEliece and general pitfalls when choosing various code families.The next section is dedicated to practical aspects, mainly highlighting the pros (fast encryption and decryption) and cons (large public key) of code-based primitives, with an eye to higher security

level (semantic, CCA2). The chapter is concluded with an annex on coding theory, that perhaps should have been presented at the beginning, introducing the very basics of algebraic coding theory, GRS and Goppa codes, and Rank metric.

Regev and Micciancio are the authors of the chapter on lattice-based cryptography. Unlike the previous chapter, this is much better organized. It starts with a very informal, almost colloquial introduction, which is simple to understand. It then features a precise, compact preliminaries section, introducing all the notions that will be needed further. After that, it is time for discussing lattice problems, namely that of finding short vectors: this is done in Section 3. The first lattice-based object to be defined is hash functions, starting from Ajtai's original construction up to the recent SWIFFT proposal. Encryption schemes are described next, including GGH, NTRU and LWE-based constructions. The chapter continues with a section on signature schemes, and a short part dedicated to other primitives such as CCA-secure and identity-based encryption, oblivious transfer etc. To conclude, a few open questions are listed, regarding cryptanalysis, improving existing crypto systems and a comparison with number-theoretic cryptography. The chapter is always detailed yet easy to understand and not overly lengthy. Arguably the best chapter in the book.

The final chapter is written by Ding and Yang, and describes multivariate cryptography. Again, it begins by introducing the basics, starting with the bipolar and other constructions. The author then proceed to list a few examples of multivariate public-key cryptography. These include the famous Rainbow signature scheme, PMI+, the HFEv- scheme etc. All the basic constructions and variations are extensively described in Section 4, the largest by far, at a high technical level. Section 5 is dedicated to standard attacks such as linearization equations and differential and rank attacks. Finally, the chapter is concluded with a section on future goals and developments.

4 Style of the book

The book is highly technical and it is in fact more a collection of "survey" papers on the respective areas, rather than a textbook. There are no exercises, of course, and almost no proofs. Moreover the order in which the topics are presented is not always logical and introductory, and suggests a previous knowledge of the area. On the other hand, the first chapter is written in very simple language and successfully manages to introduce the reader to the topic.

5 Would you recommend the book?

This is a very important book for post-quantum cryptography. Due to its particular nature, though, it is not fully suitable to beginners, but rather more valuable for experts looking for references in the area, and a state of the art description of the subject.

The reviewer is Assistant Professor at University of Warsaw, Poland.