Review of the book
"Cryptanalysis of RSA and its Variants"
by M. Jason Hinek
CRC Press, Taylor & Francis Group
ISBN: 978-1-4200-7512-2

Jannik Pewny

2009-12-20

1 What the book is about

As the title says, the book is about cryptanalysis of RSA and its variants.

The book starts with a chapter called *The RSA Cryptosystem*, which gives you an introduction to RSA. There are subchapters on its security based on integer factorization, semantic security and the efficiency of prime generation and modular exponentiation, which form the generation of an RSA instance and the computation of encryption and decryption resp. signing and verification. The homomorphic properties as well as the signature-scheme gets mentioned, each in an own sub-chapter.

Named *Some Notation, Mathematics and Techniques*, the next chapter explains, what the variables in the further text are supposed to mean, what integer factorization is, what continued fractions and lattices are and how you compute roots of linear equations (modular and over $\mathbb{Z}$) via Coppersmith's method (univariate) or multivariate.
In this chapter you can also find the declaration of strict separation between provable attacks (which are noted as Theorem, Lemma or Corollary) and heuristic attacks (which are simply noted as Attacks).

This closes the first part, called *Preliminaries*. The next part, called *Cryptanalysis of RSA*, starts with a chapter called *Some early Attacks*, in which the Common Modulus attack, the Håstad attacks (with sub-chapters on common and related plaintext attacks) and cyclic attacks are handled.

This is followed by the chapters *Small Public Exponent Attacks* (in which stereotyped and related message attacks and random padding attacks occur), *Small Private Exponent Attacks* (with Wiener's attack, as well in the original continued fraction style as in the lattice style, Boneh-Durfee's lattice attack and the Blömer-May-approach), *Partial Key Exposure Attacks* (Most-Significant-Bits of the key, Least-Significant-Bits of the Key, Partially known Primes and a variety of combinations of these three attacks, Factoring with a hint, Arbitrary Sized Exponents, Full-Sized Private Key, Full-Sized Public Key). The part ends with a chapter called *More Small Private Exponent Attacks*, which handles again the Common Modulus Attack (the first time it was shown, that any of the users sharing a modulus could easily factor it; this time it is shown for a single user, who has no interest in breaking his own scheme, it is also insecure to have multiple users of RSA-instances sharing a modulus) and a Common Private Exponent Attack.

By *Variants* of RSA the author means *CRT-RSA*, *Multi-Prime RSA*, *Multi-Power RSA*, *Common Prime RSA* and *Dual RSA*.
In the third part (called *Cryptanalysis of Variants of RSA*) each of these variants has its own chapter in which almost all attacks mentioned so far are reviewed in this new context.

Each chapter ends with a sub-chapter *Additional Notes*, in which the author gives side-notes on a certain topic, which would not really fit into the chapter itself, but give an interesting outlook.

A *List of figures* and a *List of tables* is given before the *Preface* and in the Appendix you can find *Observations on the distribution of the parameter* $g = gcd(p-1, q-1)$, *Geometrically progressive matrices* (which are important for the Boneh-Durfee attack) and an Algorithm to generate an instance of *Dual RSA*.

There is also a page on *Further reading*, where the author recommends some sources he thinks are interesting/worth knowing for the reader.

The *Bibliography*, holding 258 sources, and an *Index* are also to be found in the end of the book.

2 What the book is like

As you can see from the above given list of content, the book is as well structured as it gives a complete summary of the topic.

Though it is full of mathematics, it is relatively easy to read, since almost every step is explained and the same notation was used in the whole book. Reasonably, it is the same notation that is used in common literature, so that the reader should feel familiar with it. The content is not always that simple, so even though it is written quite good, it takes a while to read it completely.

The author gives a lot of references and lists sources, in a way, that makes you think of scientific papers. Nevertheless it is a textbook, so I cannot complain about an abbreviated style of writing or an mathematic over-shortening of statements.
It might be interesting to know that this book is based on the author's PhD thesis, therefore it is written seriously as well as scientific.

The separation between provable and heuristic attacks was followed through the whole book (apart from the chapter-names).

One negative thing is to be found in the Appendix, Part *C Some Algorithms*. It actually only holds one algorithm, as mentioned above. It should either be integrated into a fitting chapter, so that you could leave out this Appendix or it could be extended by further algorithms (e.g. by primality-test like Miller-Rabin).

3 Recommendation

I can honestly recommend this book. It is written straightforward and is therefore easy to read. Every step is explained and original sources are given, so if you want to look deeper into the background of a certain problem, you can easily do that.
Since the book is full of mathematics and readers tend to read across such things, you should have at least a rough idea of RSA and lattices.
But apart from that, the book seems to be excellent to give a substantiated overview over the current state of cryptanalysis of RSA. It might even go a little too far for students, which do not want to specialize on this topic.
You should keep in mind, that this book does not do a 101 on cryptology, which is why it is not the proper book for non-technicians, non-mathematicians or in general readers, which are completely unexperienced with cryptology.

The reviewer is a student of IT Security at the Ruhr University of Bochum (Horst Görtz Institute)