Preface

This book is about relations between three different areas of mathematics and theoretical computer science: combinatorial group theory, cryptography, and complexity theory. We explore how non-commutative (infinite) groups, which are typically studied in combinatorial group theory, can be used in *public key cryptography*. We also show that there is a remarkable feedback from cryptography to combinatorial group theory because some of the problems motivated by cryptography appear to be new to group theory, and they open many interesting research avenues within group theory. Then, we employ complexity theory, notably *generic case complexity* of algorithms, for cryptanalysis of various cryptographic protocols based on infinite groups. We also use the ideas and machinery from the theory of generic case complexity to study *asymptotically dominant properties* of some infinite groups that have been used in public key cryptography so far. It turns out that for a relevant cryptographic scheme to be secure, it is essential that keys are selected from a "very small" (relative to the whole group, say) subset rather than from the whole group. Detecting these subsets ("black holes") for a particular cryptographic scheme is usually a very challenging problem, but it holds the key to creating secure cryptographic primitives based on infinite non-commutative groups.

The book is based on lecture notes for the Advanced Course on Group-Based Cryptography held at the CRM, Barcelona in May 2007. It is a great pleasure for us to thank Manuel Castellet, the Honorary Director of the CRM, for supporting the idea of this Advanced Course. We are also grateful to the current CRM Director, Joaquim Bruna, and to the friendly CRM staff, especially Mrs. N. Portet and Mrs. N. Hernández, for their help in running the Advanced Course and in preparing the lecture notes.

It is also a pleasure for us to thank our colleagues who have directly or indirectly contributed to this book. Our special thanks go to E. Ventura who was the coordinator of the Advanced Course on Group-Based Cryptography at the CRM. We would also like to thank M. Anshel, M. Elder, B. Fine, R. Gilman, D. Grigoriev, Yu. Gurevich, Y. Kurt, A. D. Miasnikov, D. Osin, S. Radomirovic, G. Rosenberger, T. Riley, V. Roman'kov, A. Rybalov, R. Steinwandt, B. Tsaban, G. Zapata for numerous helpful comments and insightful discussions.

We are also grateful to our home institutions, McGill University, the City

College of New York, and Stevens Institute of Technology for a stimulating research environment. A. G. Myasnikov and V. Shpilrain acknowledge support by the NSF grant DMS-0405105 during their work on this book. A. G. Myasnikov was also supported by an NSERC grant, and V. Shpilrain was also supported by an NSA grant.

Alexei Myasnikov
Vladimir Shpilrain
Alexander Ushakov

Montreal,
New York

Introduction

The object of this book is twofold. First, we explore how non-commutative groups which are typically studied in combinatorial group theory can be used in *public key cryptography*. Second, we show that there is a remarkable feedback from cryptography to combinatorial group theory because some of the problems motivated by cryptography appear to be new to group theory, and they open many interesting research avenues within group theory.

We reiterate that our focus in this book is on public key (or asymmetric) cryptography. Standard (or symmetric) cryptography generally uses a single key which allows both for the encryption and decryption of messages. This form of cryptography is usually referred to as symmetric key cryptography because the same algorithm or procedure or key is used not only to encode a message but also to decode that message. The key being used then is necessarily private and known only to the two parties involved in communication. This method for transmission of messages was basically the only way until 1976 when W. Diffie and M. Hellman introduced an ingenious new way of transmitting information, which has led to what is now known as public key cryptography. The basic idea is quite simple. It involves the use of a so-called one-way function f to encrypt messages. Very informally, a one-way function f is a function such that it is easy to compute the value of $f(x)$ for each argument x in the domain of f, but it is very hard to compute the value of $f^{-1}(y)$ for "most" y in the range of f. The most celebrated one-way function, due to Rivest, Shamir and Adleman, gives rise to the protocol called RSA, which is the most common public key cryptosystem in use today. It is employed for instance in the browsers Netscape and Internet Explorer. Thus it plays a critical and increasingly important role in all manner of secure electronic communication and transactions that use the Internet. It depends in its efficacy, as do many other cryptosystems, on the complexity of finite abelian (or commutative) groups. Such algebraic structures are very special examples of *finitely generated groups*. Finitely generated groups have been intensively studied for over 150 years and they exhibit extraordinary complexity. Although the security of the Internet does not appear to be threatened at this time because of the weaknesses of the existing protocols such as RSA, it seems prudent to explore possible enhancements and replacements of such protocols which depend on finite abelian groups. This is the basic objective of this book.

The idea of using the complexity of infinite nonabelian groups in cryptography goes back to Magyarik and Wagner [97] who in 1985 devised a public-key protocol based on the unsolvability of the word problem for finitely presented groups (or so they thought). Their protocol now looks somewhat naive, but it was pioneering. More recently, there has been an increased interest in applications of nonabelian group theory to cryptography (see for example [1, 84, 129]). Most suggested protocols are based on *search problems* which are variants of more traditional *decision problems* of combinatorial group theory. Protocols based on search problems fit in with the general paradigm of a public-key protocol based on a one-way function. We therefore dub the relevant area of cryptography *canonical cryptography* and explore it in Chapter 4 of our book.

On the other hand, employing decision problems in public key cryptography allows one to depart from the canonical paradigm and construct cryptographic protocols with new properties, impossible in the canonical model. In particular, such protocols can be secure against some "brute force" attacks by a computationally unbounded adversary. There is a price to pay for that, but the price is reasonable: a legitimate receiver decrypts correctly with probability that can be made arbitrarily close to 1, but not equal to 1. We discuss this and some other new ideas in Chapter 11.

There were also attempts, so far rather isolated, to provide a rigorous mathematical justification of security for protocols based on infinite groups, as an alternative to the security model known as *semantic security* [50], which is widely accepted in the "finite case". It turns out, not surprisingly, that to introduce such a model one would need to define a suitable probability measure on a given infinite group. This delicate problem has been addressed in [17, 16, 89] for some classes of groups, but this is just the beginning of the work required to build a solid mathematical foundation for assessing security of cryptosystems based on infinite groups. Another, related, area of research studies *generic* behavior of infinite groups with respect to various properties (see [75] and its references). It is becoming clear now that, as far as security of a cryptographic protocol is concerned, the appropriate measure of computational hardness of a group-theoretic problem in the core of such a cryptographic protocol should take into account the "generic" case of the problem, as opposed to the worst case or average case traditionally studied in mathematics and theoretical computer science. Generic case performance of various algorithms on groups has been studied in [75, 77], [78], and many other papers. It is the focus of Part III of this book.

We have to make a disclaimer though that we do *not* address here security properties (e.g., semantic security) that are typically considered in "traditional" cryptography. They are extensively treated in cryptographic literature; here we single out a forthcoming monograph [51] because it also studies how group theory may be used in cryptography, but the focus there is quite different from ours; in particular, the authors of [51] do not consider infinite groups, but they do study "traditional" security properties thoroughly.

In the concluding Part IV of our book, we use the ideas and machinery from Part III to study *asymptotically dominant properties* of some infinite groups that have been used in public key cryptography so far. Informally, the point is that "most" elements, or tuples of elements, or subgroups, or whatever, of a given group have some "smooth" properties which makes them unfit for being used (as private or public keys, say) in a cryptographic scheme. Therefore, for a relevant cryptographic scheme to be secure, it is essential that keys are actually selected from a "very small" (relative to the whole group, say) subset rather than from the whole group. Detecting these subsets ("black holes") for a particular cryptographic scheme is usually a very challenging problem, but it holds the key to creating secure cryptographic primitives based on infinite nonabelian groups.

http://www.springer.com/978-3-7643-8826-3

Group-based Cryptography
Myasnikov, A.; Shpilrain, V.; Ushakov, A.
2008, XV, 183 p., Softcover
ISBN: 978-3-7643-8826-3
A product of Birkhäuser Basel