SpringerBriefs in Electrical and Computer Engineering

For further volumes:
http://www.springer.com/series/10059

Marco Baldi

QC-LDPC Code-Based Cryptography

Springer

Marco Baldi
DII
Università Politecnica delle Marche
Ancona
Italy

ISSN 2191-8112 ISSN 2191-8120 (electronic)
ISBN 978-3-319-02555-1 ISBN 978-3-319-02556-8 (eBook)
DOI 10.1007/978-3-319-02556-8
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014936435

© The Author(s) 2014
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To Eugenio,
my beloved son

Foreword

This monograph reports a series of pioneering works which aim at improving the theory and practice of code-based cryptography. These research works make intensive use of mathematics, because the structures, algorithms, and security arguments demand it. Also, equally important, they are about engineering, because the practicality of the proposed cryptosystems has been the author's concern at every step of the design. Before I tell what you should expect from this volume, let me tell you first a few words about the context.

Do We Need Code-Based Cryptography?

Most, if not all, applications of public-key cryptography today make use of number theory. Regardless of the reasons for this choice, diversity would be welcomed. The matter becomes vivid when one considers the threat posed by quantum computing. We do not know when a large enough quantum computer will appear, but number-theory-based cryptography would be vulnerable to it, unlike a few other techniques, including code-based cryptography. Besides, reaching the point where one is able to engineer an efficient and secure cryptosystem requires years, maybe decades, of research. So yes, we need to increase our understanding of code-based cryptography and we need to do it now.

A Short History of Code-Based Cryptography

Interactions between error correcting codes and cryptography are numerous and fascinating. One of such interactions relates with the design of asymmetric cryptographic primitives and has appeared in the early years of the modern cryptography era. Robert J. McEliece proposed in 1978 an encryption scheme based on the hardness of decoding. This happened a few months only after R. Rivest, A. Shamir, and L. Adleman proposed the famous RSA scheme, based on the hardness of factoring. The trapdoor of the McEliece scheme would be the underlying algebraic

structure of a code (in fact a binary Goppa code), whose generator matrix is revealed as public key—similarly, the public key of RSA is a composite integer whose factorization is kept private.

Later, many attempts were made, with little success, to improve the McEliece scheme by instantiating it with families of codes other than Goppa. In particular, Low Density Parity Check (LDPC) codes could have been of great interest because of their efficient encoding and decoding procedures and their lack of algebraic structure. Unfortunately, some pitfalls seemed difficult to avoid[1] and the idea was discarded at first. A second important line of work to improve the scheme has been the attempts at reducing the public key size. Using quasi-cyclic codes was first proposed by P. Gaborit[2] and allows a compact representation of the public key. The difficulty here arises from two layers of structure—one coming from the algebraic code (an alternant code, for instance a Goppa code) and the other from the quasi-cyclicity—which combine into a sharp cryptanalytic tool. We do not know precisely how deep this tool can cut and the question of whether or not we may use quasi-cyclic alternant codes for the McEliece scheme is not clearly settled today.

Why Does This Book Matter?

This book details how to design a secure public-key code-based encryption scheme based on quasi-cyclic LDPC codes. LDPC codes have been one of the main breakthroughs in the engineering of communication systems in the past decade; they enjoy efficient encoding and decoding procedures and considering their use in a McEliece-like scheme was natural. What makes these codes particular and so useful is a sparse parity check matrix and only that. Unfortunately, this sparsity is difficult to disguise and is thus the reason why LDPC codes were not recommended. The first achievement of this book is to propose a new disguise for the public key, which is now closer to pseudorandom,[3] while the legitimate user may still use the sparsity for decryption. The second achievement is the key size reduction. What the author tells us here is that, for LDPC codes, unlike many other code families, quasi-cyclicity does not seem to lower significantly the security.

And this is it, we now have a new candidate, a cryptosystem which is efficient and presumably secure, something we already had with Goppa-McEliece, but this time with short keys, increasing the usability of the scheme.

---

[1] C. Monico, J. Rosenthal, and A. Shokrollahi, *Using low density parity check codes in the McEliece cryptosystem*, at ISIT 2000 conference.

[2] P. Gaborit, *Shorter keys for code based cryptography*, at WCC 2005 conference.

[3] i.e., *Computationally* indistinguishable from random.

This is just the beginning and this work will have some extensions. It already has. Anyone interested in the design of code-based cryptosystems will find here a thorough and far-reaching case study. It is always difficult to predict the future of a research domain, but it is likely that if some day code-based cryptography finds its way to applications, the present work will have a good place somewhere on that path.

Rocquencourt, February 27, 2014 Nicolas Sendrier

Preface

This book is the synopsis of an eight-year research work which began during my Ph.D. studies at the Università Politecnica delle Marche.

In the first 2000s, there was a huge research interest in the recently rediscovered class of low-density parity-check (LDPC) codes, with the aim to design new error correcting codes for many practical applications and for the revision and updating of several telecommunication standards.

At the beginning of 2006, I was entering my third year of Ph.D. study, and most of my research work up until that time had been in the design and performance assessment of several families of LDPC codes, with particular interest in codes like quasi-cyclic (QC) LDPC codes, having an intrinsic structure that facilitates their implementation.

Working with these codes, one realizes that their design has a huge number of degrees of freedom, and that random-based designs often result in very good codes. Furthermore, even when the constraint of some inner structure is imposed, as in the case of QC-LDPC codes, it is still possible to exploit some randomness to design very large families of codes with fixed parameters and equivalent performance.

Therefore, these codes seemed natural candidates for use in cryptography, and these observations motivated me to investigate the chance to use them in such a context. The most promising application appeared to be in the framework of the McEliece and Niederreiter cryptosystems, which had always suffered from the large size of their public keys. In fact, these cryptosystems use Goppa codes as secret codes, and the space needed to store their public matrices increases quadratically in code length.

By exploiting the sparse nature of LDPC matrices, such a limit could be overcome, at least in principle. A first study by Monico, Rosenthal, and Shokrollahi had already investigated such a chance, coming to the conclusion that the sparse nature of LDPC matrices could not be exploited to reduce the size of the public keys without endangering the security of those cryptosystems. However, such a first investigation did not consider QC-LDPC codes, which could achieve very compact representations of the public matrices even by renouncing to exploit their sparsity. In fact, the characteristic matrices of a QC code can be stored in a space that increases linearly in code length.

This was the starting point of this line of research for me and my colleagues, aimed at assessing the actual benefits and drawbacks coming from the use of QC-LDPC codes in the McEliece and Niederreiter cryptosystems.

As it often occurs in cryptography, a successful system is built on a number of identified and corrected vulnerabilities, which is the fundamental role of cryptanalysis. This was the case also for the first QC-LDPC code-based systems: though being able to counter all the classical attacks, the first instances we proposed revealed to be weak against new attacks, and some revisions were needed to restore security.

However, starting from 2008, some instances of QC-LDPC code-based systems have been developed which eliminate all known vulnerabilities, and are still considered secure up to now. More recently, by using a special class of LDPC codes named moderate-density parity-check (MDPC) codes, it has also been possible to devise the first security reduction to a hard problem for these systems.

The aim of this book is to provide the reader with the basics of QC-LDPC code-based public key cryptosystems, by describing their main components, the most dangerous attacks, and the relevant countermeasures. Some new variants arising from public key cryptosystems and concerning digital signatures and private key cryptosystems are also briefly addressed.

I would like to express my most sincere gratitude to my former supervisor, Prof. Franco Chiaraluce, for his bright guidance throughout my research career. Special thanks go to Prof. Giovanni Cancellieri for his insightful ideas on coding, to Marco Bianchi for his hard commitment to these research topics, and to all the people in the telecommunications group at the Università Politecnica delle Marche. Finally, I am eternally grateful to my parents and to my wife for their endless support and encouragement.

Ancona, February 2014 Marco Baldi

Acknowledgment

This work was supported in part by the Italian Ministry of Education, University and Research (MIUR) under the project “ESCAPADE” (Grant RBFR105NLC), within the “FIRB—Futuro in Ricerca 2010” funding program.

Contents