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

http://www.springer.com/978-3-319-02555-1

QC-LDPC Code-Based Cryptography

Baldi, M.

2014, XVI, 120 p. 15 illus., Softcover
ISBN: 978-3-319-02555-1