SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND
INFORMATION TECHNOLOGY

CONTRIBUTIONS TO THE ANALYSIS OF THE QC-LDPC MCELIECE CRYPTOSYSTEM

2017 Mgr. Tomáš Fabšič

SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Registration number: FEI-104372-63826

CONTRIBUTIONS TO THE ANALYSIS OF THE QC-LDPC MCELIECE CRYPTOSYSTEM

DISSERTATION THESIS

Study Programme:	Applied Informatics
Field Number:	2511
Study Field:	9.2.9 Applied Informatics
Training Workplace:	Institute of Computer Science and Mathematics
Supervisor:	prof. RNDr. Otokar Grošek, PhD.
Consultant:	prof. RNDr. Peter Horák, DrSc.

Bratislava 2017 **Mgr. Tomáš Fabšič**

Slovak University of Technology in Bratislava
Institute of Computer Science and Mathematics

Faculty of Electrical Engineering and Information Technology
Academic year: 2016/2017
Reg. No.: FEI-104372-63826

STU FEI

DISSERTATION THESIS TOPIC

Student: **Mgr. Tomáš Fabšič**
Student's ID: 63826
Study programme: Applied Informatics
Study field: 9.2.9. Applied Informatics
Thesis supervisor: prof. RNDr. Otokar Grošek, PhD.
Consultant: prof. RNDr. Peter Horák, DrSc.
Workplace: Institute of Computer Science and Mathematics, FEI STU

Topic: **Contributions to the Analysis of the QC-LDPC McEliece Cryptosystem**

Language of thesis: English

Specification of Assignment:

In 1999, P. W. Shor demonstrated that prime factorization and discrete logarithms can be solved in polynomial time on a quantum computer. This means that building a sufficiently large quantum computer would render currently used public key cryptosystems insecure.

One of prominent candidates for quantum-resistant cryptography is the McEliece cryptosystem. The main disadvantage of the cryptosystem, however, is the large size of the public key.

A number of variants of the McEliece cryptosystem have been proposed with the intention to reduce the size of the public key. Among these proposals are variants which employ quasi-cyclic low-density parity-check (QC-LDPC) codes. The aim of the dissertation is to study these variants of the McEliece cryptosystem.

Objectives:

1. Contribute to the cryptanalysis of variants of the McEliece cryptosystem based on QC-LDPC codes.
2. Propose methods to generate invertible sparse circulant matrices suitable for use in variants of the McEliece cryptosystem based on QC-LDPC codes.

Selected bibliography:

1. Baldi, M., Bodrato, M., Chiaraluce, F.: A new analysis of the McEliece cryptosystem based on QC-LDPC codes. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) 6th International Conference on Security and Cryptography for Networks (SCN 2008). LNCS, vol. 5229, pp. 246-262. Springer, Berlin (2008)

Assignment procedure from: 27. 08. 2013

Date of thesis submission: 31. 08. 2017

Mgr. Tomáš Fabšič
Solver

prof. RNDr. Otokar Grošek, PhD.
Head of department

prof. RNDr. Gabriel Juhás, PhD.
Study programme supervisor

ABSTRACT

The present thesis focuses on the QC-LDPC McEliece cryptosystem and the QC-MDPC McEliece cryptosystem. Both cryptosystems are candidates for post-quantum cryptography, and compared to the original McEliece cryptosystem they have the advantage of smaller public keys.

The thesis is a compilation of three research papers. In the first paper, we presented a reaction attack on the QC-LDPC McEliece cryptosystem. Our attack was inspired by the previous work of Guo et al., who invented a reaction attack on the QC-MDPC McEliece cryptosystem. Their attack is based on the observation that when a bit-flipping decoding algorithm is used in QC-MDPC McEliece, then there exists a dependence between the secret matrix H and the failure probability of the bit-flipping algorithm. This dependence can be exploited to reveal the matrix H which constitutes the private key in the cryptosystem. It was conjectured that such dependence is present even when a soft-decision decoding algorithm is used instead of a bit-flipping algorithm. Our paper shows that a similar dependence between the secret matrix H and the failure probability of a decoding algorithm is also present in the QC-LDPC McEliece cryptosystem. Unlike in QC-MDPC McEliece, the secret key in QC-LDPC McEliece also contains matrices S and Q in addition to the matrix H. We observed that there also exists a dependence between the failure probability and the matrix Q. We showed that these dependencies leak enough information to allow an attacker to construct a sparse parity-check matrix for the public code. This parity-check matrix can then be used for decrypting ciphertexts. We tested the attack on an implementation of the QC-LDPC McEliece using a soft-decision decoding algorithm. Thus, we also confirmed that soft-decision decoding algorithms can be vulnerable to leaking information about the secret key.

In our second paper, we presented a simple power analysis attack on the QC-LDPC McEliece cryptosystem. Our attack was inspired by the previous work of Heyse et al., who demonstrated that a naive implementation of the decryption algorithm in the original McEliece cryptosystem allows an attacker to recover the secret matrix P by measuring the power consumption. We showed that a similar threat is present in the QC-LDPC variant of the McEliece cryptosystem. We considered a naive implementation of the decryption algorithm in the QC-LDPC McEliece cryptosystem employing a bit-flipping algorithm. We demonstrated that this implementation leaks information about positions of ones in the secret matrix Q. We argued that this leakage allows an attacker to completely recover the matrix Q. In addition, we noted that the quasi-cyclic nature of the matrix Q allows

to accelerate the attack significantly.

Although the attack from our first paper suggests that the QC-LDPC McEliece cryptosystem may not be suitable for the deployment in circumstances where a long-term use of keys is required, it may still be considered for situations where ephemeral keys are required, such as in key exchange protocols. In such situations, the cryptosystem is, however, still threatened by the squaring attack from Shooshtari et al.. To avoid this attack, the dimension of circulant blocks in the cryptosystem has to be odd. QC-LDPC McEliece requires generating matrices S and Q, which are invertible and are composed of blocks of circulant matrices of the dimension p. In addition, S is dense and Q is sparse with a prescribed low number of ones in a row. In their proposal of the QC-LDPC McEliece cryptosystem, its authors also proposed a method how to construct matrices satisfying these requirements for the case when p is a power of 2. In case p is not a power of 2, their method, however, does not necessarily produce an invertible matrix. In our third paper, we studied how to construct matrices S and Q when p is odd. We firstly studied how to construct invertible circulant binary matrices with a prescribed number of ones. In a previous work of von Maurich and Güneysu, this problem was solved by repeatedly generating random circulant matrices with the prescribed number of ones until an invertible matrix was obtained. We proposed alternative algorithms for generating invertible circulant matrices with a prescribed number of ones. Compared with the approach of von Maurich and Güneysu, our algorithms have the advantage that they generate matrices satisfying all the requirements on the first attempt. On the other hand, their disadvantage is that they generate matrices from a smaller pool. Subsequently, we proposed algorithms to construct matrices S and Q in the QC-LDPC McEliece cryptosystem. Our algorithms assume that the size of blocks in S and Q is odd.

Keywords: QC-LDPC McEliece cryptosystem, QC-MDPC McEliece cryptosystem, reaction attack, power analysis attack, invertible circulant matrices with a prescribed number of ones

SÚHRN (in Slovak)

Prezentovaná práca sa zaoberá QC-LDPC McEliece kryptosystémom a QC-MDPC McEliece kryptosystémom. Obidva kryptosystémy patria medzi kandidátov pre post-kvantovú kryptografiu. Oproti pôvodnému McElieceovmu kryptosystému majú tieto kryptosystémy výhodu v menšej veľkosti verejných kľúčov.

Dizertačná práca je súborom troch vedeckých článkov. V prvom článku prezentujeme reakčný útok na QC-LDPC McEliece kryptosystém. Náš útok bol inšpirovaný prácou autorov Guo, Johansson a Stankovski, ktorí zrealizovali reakčný útok na QC-MDPC McEliece kryptosystém. Ich útok je založený na pozorovaní, že ak sa v QC-MDPC McEliece kryptosystéme používa na dekódovanie algoritmus preklápania bitov (anglicky "bit-flipping algorithm"), potom vzniká závislosť medzi súkromným kľúčom H a pravdepodobnosťou chyby pri dekódovaní. Túto závislosť môže útočník využiť na získanie súkromného kľúča H. Guo, Johansson a Stankovski vyslovili vo svojej práci domnienku, že ich útok je možné realizovať aj v prípade, ak sa v QC-MDPC McEliece kryptosystéme namiesto algoritmu preklápania bitov používa dekódovací algoritmus s jemným rozhodovaním (anglicky "soft-decision decoding algorithm"). V našom článku sme ukázali, že podobná závislosť medzi maticou H a pravdepodobnosťou chyby pri dekódovaní existuje aj v QC-LDPC McEliece kryptosystéme. Na rozdiel od QC-MDPC McEliece kryptosystému, obsahuje súkromný kľúč v QC-LDPC McEliece kryptosystéme okrem matice H ešte aj matice S a Q. Ukázali sme tiež, že existuje aj závislosť medzi pravdepodobnosťou chyby pri dekódovaní a maticou Q. V článku sme vysvetlili, že útočník môže využiť tieto dve závislosti na skonštruovanie riedkej kontrolnej matice pre verejný kód používaný v QC-LDPC McEliece kryptosystéme. S pomocou tejto matice vie potom útočník dešifrovať zašifrované správy. Náš útok sme otestovali na verzii QC-LDPC McEliece kryptosystému, ktorá využívala dekódovací algoritmus s jemným rozhodovaním. Tým sme zároveň potvrdili domnienku, že útočník môže získať informácie o súkromnom kľúči aj v prípade, že kryptosystém používa dekódovací algoritmus s jemným rozhodovaním.

V druhom článku prezentujeme útok na QC-LDPC McEliece kryptosystém s využitím merania spotreby elektrickej energie kryptografického zariadenia. Náš útok bol inšpirovaný útokom autorov Heyse, Moradi a Paar na pôvodnú verziu McElieceovho kryptosystému. Heyse, Moradi a Paar ukázali, že v prípade jednoduchej implementácie dešifrovacieho algoritmu v pôvodnom McElieceovom kryptosystéme môže útočník pomocou merania spotreby elektrickej energie kryptografického zariadenia počas dešifrovania odhaliť maticu P, ktorá je súčasťou súkromného kľúča. V našom článku sme ukázali, že podobné nebezpečenstvo

existuje aj pri QC-LDPC McEliece kryptosystéme. Skúmali sme jednoduchú implementáciu dešifrovacieho algoritmu v QC-LDPC McEliece kryptosystéme, ktorá na dekódovanie využívala algoritmus preklápania bitov. Zistili sme, že pomocou merania spotreby elektrickej energie počas dešifrovania je možné získať informácie o pozíciách jednotiek v tajnej matici Q. Vysvetlili sme, že pomocou týchto informácií je možné maticu Q kompletne zrekonštruovať. Takisto sme vysvetlili, že kvázicyklická štruktúra matice Q umožňuje vykonať útok s menším počtom meraní.

Výsledok z prvého článku implikuje, že QC-LDPC McEliece kryptosystém momentálne nie je vhodný na použitie v podmienkach, v ktorých sa používa ten istý verejný kľúč po dlhšiu dobu. Tento výsledok ale nebráni použitiu QC-LDPC McEliece kryptosystému v situáciách, v ktorých sa vyžadujú iba jednorazové kľúče, ako napríklad v protokoloch na výmenu kľúča. V takom prípade môže ale QC-LDPC McEliece kryptosystém stále byť ohrozený útokom od autorov Shooshtari a spol.. Tomuto útoku sa dá predísť tak, že rozmer cyklických blokov p sa zvolí ako nepárne číslo. Ako súčasť súkromného kľúča v QC-LDPC McEliece kryptosystéme sa musia vygenerovať matice S a Q. Obidve tieto matice musia byť invertovateľné a zložené z cyklických blokov rozmeru $p \times p$. Okrem toho musí matica S byť hustá a matica Q naopak musí byť riedka s predpísaným počtom jednotiek. V návrhu QC-LDPC McEliece kryptosystému navrhli jeho autori spôsob ako generovať matice S a Q v prípade, že p je mocninou čísla 2. V prípade, že p nie je mocninou čísla 2, navrhovaný spôsob generovania negarantuje, že výsledné matice budú invertovateľné. V našom treťom článku sme sa zaoberali otázkou ako generovať matice S a Q v prípade, že p je nepárne. Najprv sme riešili otázku ako generovať invertovateľné cyklické matice s predpísaným počtom jednotiek. V článku od autorov von Maurich a Güneysu bolo generovanie takýchto matíc riešené tak, že sa generovali náhodné cyklické matice s predpísaným počtom jednotiek, až kým jedna z nich nebola invertovateľná. V našom článku sme navrhli alternatívne algoritmy na generovanie invertovateľných cyklických matíc s predpísaným počtom jednotiek. V porovnaní s algoritmom od autorov von Maurich a Güneysu majú naše algoritmy výhodu, že generujú matice spĺňajúce všetky požiadavky hneď na prvý pokus. Ich nevýhodou ale je, že generujú matice iba z obmedzenej množiny - nie je pomocou nich možné vygenerovať ľubovoľnú invertovateľnú cyklickú maticu s predpísaným počtom jednotiek. Následne sme v našom článku navrhli algoritmy na generovanie matíc S a Q v QC-LDPC McEliece kryptosystéme pre prípad, že rozmer cyklických blokov p je nepárny.

Kľúčové slová: QC-LDPC McEliece kryptosystém, QC-MDPC McEliece kryptosystém, reakčný útok, útok s využitím merania spotreby elektrickej energie kryptografického

zariadenia, invertovateľné cyklické matice s predpísaným počtom jednotiek

Declaration

I hereby declare that I am the sole author of this thesis, with the exception of the included copies of three research papers. These research papers are herein presented with the full list of authors. Further, I confirm that in writing this thesis I used only the referenced sources.

Bratislava, 16.8.2017

.....

Tomáš Fabšič

Acknowledgments

I would like to thank professor Otokar Grošek, professor Peter Horák and associate professor Pavol Zajac for their advice and support and for many insightful discussions. Furthermore, I would like to thank my coauthors for very enjoyable and productive collaborations. In addition, I thank every member of the Institute of Computer Science and Mathematics at FEI STU for creating a very pleasant working environment. Finally, I would like to express my deep gratitude to my parents for their continual support.

Contents

Resumé (in Slovak)

Ciele dizertačnej práce

V roku 1999 dokázal P. W. Shor [17], že s využitím kvantového počítača je možné riešiť problémy prvočíselnej faktorizácie a diskrétneho logaritmu v polynomiálnom čase. Dôsledkom tohto zistenia je, že v prípade, že technologický pokrok umožní postavenie dostatočne výkonného kvantového počítača, nebudú v súčasnosti používané asymetrické kryptosystémy môcť byť považované za bezpečné. Mnoho vedcov sa v súčasnosti domnieva, že postavenie výkonného kvantového počítača je už iba otázkou času a niektorí odborníci dokonca predpovedajú, že do 20 rokov budú existovať kvantové počítače s výkonom dostatočným na prelomenie akejkoľvek momentálne používanej asymetrickej šifry [14]. V roku 2016 zverejnil americký národný inštitút štandardov a technológie (National Institute of Standards and Technology, NIST) správu, v ktorej upozorňuje na hrozbu kvantových počítačov a vyzýva na štandardizáciu nových asymetrických kryptosystémov odolných voči útokom kvantovými počítačmi [4].

Z týchto dôvodov sa významná časť súčasného výskumu v kryptografii sústredí na návrh nových asymetrických kryptosystémov odolných voči útokom kvantovými počítačmi. Takéto kryptosystémy musia byť založené na matematických problémoch, ktoré nie je možné efektívne riešiť ani pomocou kvantového počítača. Jedným z takýchto problémov je problém dekódovania náhodného lineárneho kódu. Je známe, že tento problém je NP-úplný [3] a v súčasnosti neexistujú efektívne algoritmy na riešenie NP-úplných problémov ani s využitím kvantového počítača.

Prvý asymetrický kryptosystém založený na probléme dekódovania náhodného lineárneho kódu bol zverejnený už v roku 1978. Jeho autorom bol R. J. McEliece [11] a dnes ho označujeme ako McElieceov kryptosystém. McElieceov kryptosystém nebol do dnešného dňa prelomený, ale jeho nevýhodou sú veľké verejné kľúče. Z tohto dôvodu bol v minulosti McElieceov kryptosystém v praxi používaný iba minimálne. V posledných rokoch ale kvôli hrozbe kvantových počítačov záujem o McElieceov kryptosystém výrazne narástol a v súčasnosti je tento kryptosystém predmetom veľmi aktívneho akademického výskumu.

V odbornej literatúre bolo navrhnutých viacero variantov McElieceovho kryptosystému s cieľom znížiť veľkosť verejných kľúčov. Medzi takéto návrhy patrí aj variant McElieceovho kryptosystému využívajúci kvázicyklické kódy s riedkou kontrolnou maticou. Tieto kódy sa označujú ako QC-LDPC kódy (skratka QC-LDPC pochádza z anglick-

ého "quasi-cyclic low-density parity-check codes"). Prvý variant McElieceovho kryptosystému s QC-LDPC kódmi bol publikovaný autormi Baldi a Chiaraluce v práci [1]. V práci [15] bolo ale ukázané, že na tento kryptosystém je možné vykonať útok, pomocou ktorého sa dá zistiť súkromný kľúč. Následne v práci [2] prezentovali Baldi, Bodrato a Chiaraluce mierne pozmenený variant ich kryptosystému z [1], ktorý je odolný voči útoku z [15]. Tento pozmenený variant je v súčasnosti známy ako QC-LDPC McEliece kryptosystém. V roku 2013 bol publikovaný návrh príbuzného kryptosystému - QC-MDPC McEliece kryptosystému [12]. Od QC-LDPC McEliece kryptosystému sa QC-MDPC McEliece líši najmä tým, že využíva kvázicyklické kódy s hustejšou kontrolnou maticou (to znamená, že kontrolná matica obsahuje väčší podiel jednotiek ako v prípade QC-LDPC kódov). Skratka QC-MDPC pochádza z anglického "quasi-cyclic moderate-density parity-check codes".

Prezentovaná dizertačná práca sa zameriava práve na QC-LDPC McEliece kryptosystém a QC-MDPC McEliece kryptosystém. Práca si kladie nasledovné ciele:

1. *Cieľ 1:* Prispieť ku kryptoanalýze variantov McElieceovho kryptosystému založených na QC-LDPC kódoch.

2. *Cieľ 2:* Navrhnúť metódy na generovanie invertovateľných riedkych cyklických matíc vhodných na využitie vo variantoch McElieceovho kryptosystému založených na QC-LDPC kódoch.

Dosiahnuté výsledky

Prezentovaná dizertačná práca je súborom troch vedeckých článkov [5, 6, 7]. V článku [5] prezentujeme reakčný útok na QC-LDPC McEliece kryptosystém. V článku [6] prezentujeme útok na QC-LDPC McEliece kryptosystém s využitím merania spotreby elektrickej energie kryptografického zariadenia. V článku [7] navrhujeme metódy na generovanie invertovateľných riedkych cyklických matíc s predpísaným počtom jednotiek v riadku. Taktiež vysvetľujeme, ako je možné nami navrhnuté metódy použiť v QC-LDPC McEliece kryptosystéme pri generovaní súkromného kľúča.

Reakčný útok na QC-LDPC McEliece kryptosystém

V článku [5] sme prezentovali reakčný útok na QC-LDPC McEliece kryptosystém. Náš útok bol inšpirovaný prácou autorov Guo, Johansson a Stankovski [8], ktorí zrealizovali reakčný útok na QC-MDPC McEliece kryptosystém. Ich útok je založený na pozorovaní, že ak sa v QC-MDPC McEliece kryptosystéme používa na dekódovanie algoritmus preklápania bitov (anglicky "bit-flipping algorithm"), potom vzniká závislosť medzi

súkromným kľúčom H a pravdepodobnosťou chyby pri dekódovaní. Túto závislosť môže útočník využiť na získanie súkromného kľúča H.

Namiesto algoritmu preklápania bitov je v QC-LDPC McEliece kryptosystéme a v QC-MDPC McEliece kryptosystém možné použiť dekódovací algoritmus s jemným rozhodovaním (anglicky "soft-decision decoding algorithm"). Guo, Johansson a Stankovski vyslovili vo svojej práci domnienku, že ich útok je možné realizovať aj v prípade, ak sa v QC-MDPC McEliece kryptosystéme namiesto algoritmu preklápania bitov používa dekódovací algoritmus s jemným rozhodovaním.

V našom článku sme ukázali, že podobná závislosť medzi maticou H a pravdepodobnosťou chyby pri dekódovaní existuje aj v QC-LDPC McEliece kryptosystéme. Na rozdiel od QC-MDPC McEliece kryptosystému, obsahuje súkromný kľúč v QC-LDPC McEliece kryptosystéme okrem matice H ešte aj matice S a Q. Ukázali sme tiež, že existuje aj závislosť medzi pravdepodobnosťou chyby pri dekódovaní a maticou Q. V článku sme vysvetlili, že útočník môže využiť tieto dve závislosti na skonštruovanie riedkej kontrolnej matice pre verejný kód používaný v QC-LDPC McEliece kryptosystéme. S pomocou tejto matice vie potom útočník dešifrovať zašifrované správy.

Na vykonanie útoku musí útočník (Alica) poslať obeti (Bob) veľké množstvo správ zašifrovaných Bobovým verejným kľúčom. Pri útoku predpokladáme, že o každej odoslanej správe sa Alica dozvie, či bola úspešne dešifrovaná alebo nie (komunikačný protokol môže byť napríklad nastavený tak, že v prípade, že sa Bobovi nepodarí správu dešifrovať, odošle Bob Alici požiadavku na opätovné zaslanie správy). To umožní Alici odhadnúť pravdepodobnosť chyby pri dekódovaní.

Je známe, že pôvodný McElieceov kryptosystém nie je bezpečný v prípade, že je použitý vo svojom základnom tvare. Pre dosiahnutie bezpečnosti je nutné používať McElieceov kryptosystém spolu s takzvanou CCA2 konverziou. Rovnako to platí aj pre QC-MDPC McEliece kryptosystém a pre QC-LDPC McEliece kryptosystém. Náš útok sme realizovali za predpokladu, že Alica nemá možnosť zvoliť si konkrétnu podobu zašifrovaných textov, ktoré odošle Bobovi. To znamená, že náš útok je zrealizovateľný aj v prípade, že QC-LDPC McEliece kryptosystém je používaný spolu s CCA2 konverziou. Rovnako je tomu aj v prípade útoku autorov Guo, Johansson a Stankovski na QC-MDPC McEliece kryptosystém.

Náš útok sme otestovali na verzii QC-LDPC McEliece kryptosystému, ktorá využívala dekódovací algoritmus s jemným rozhodovaním. Tým sme zároveň potvrdili domnienku, že útočník môže získať informácie o súkromnom kľúči aj v prípade, že kryptosystém používa dekódovací algoritmus s jemným rozhodovaním.

Nášmu útoku a útoku od autorov Guo, Johansson a Stankovski by sa dalo zabrániť tým, že by sa dosiahlo výrazné zníženie pravdepodobnosti chyby pri dekódovaní v QC-LDPC McEliece kryptosystéme a v QC-MDPC McEliece kryptosystéme. Vo svojom článku [8] Guo, Johansson a Stankovski odporúčajú znížiť túto pravdepodobnosť na hodnotu 2^{-K}, kde K je úroveň bitovej bezpečnosti vyžadovanej od kryptosystému. V súčasnosti ale nie sú známe žiadne efektívne dekódovacie algoritmy pre QC-LDPC kódy alebo pre QC-MDPC kódy, ktoré by dokázateľne mali takú nízku pravdepodobnosť chyby. Z toho dôvodu QC-LDPC McEliece kryptosystém a QC-MDPC McEliece kryptosystém momentálne nie sú vhodné na použitie v podmienkach, v ktorých sa používa ten istý verejný kľúč po dlhšiu dobu. Naše zistenia a zistenia autorov Guo, Johansson a Stankovski ale nebránia použitiu týchto kryptosystémov v situáciách, v ktorých sa vyžadujú iba jednorazové kľúče, ako napríklad v protokoloch na výmenu kľúča.

Útok na QC-LDPC McEliece kryptosystém s využitím merania spotreby elektrickej energie

V článku [6] sme prezentovali útok na QC-LDPC McEliece kryptosystém s využitím merania spotreby elektrickej energie kryptografického zariadenia. Náš útok bol inšpirovaný útokom autorov Heyse, Moradi a Paar [9] na pôvodnú verziu McElieceovho kryptosystému. Heyse, Moradi a Paar ukázali, že v prípade jednoduchej implementácie dešifrovacieho algoritmu v pôvodnom McElieceovom kryptosystéme môže útočník pomocou merania spotreby elektrickej energie kryptografického zariadenia počas dešifrovania odhaliť maticu P, ktorá je súčasťou súkromného kľúča.

V našom článku sme ukázali, že podobné nebezpečenstvo existuje aj pri QC-LDPC McEliece kryptosystéme. Skúmali sme jednoduchú implementáciu dešifrovacieho algoritmu v QC-LDPC McEliece kryptosystéme, ktorá na dekódovanie využívala algoritmus preklápania bitov. Zistili sme, že pomocou merania spotreby elektrickej energie počas dešifrovania je možné získať informácie o pozíciách jednotiek v tajnej matici Q. Vysvetlili sme, že pomocou týchto informácií je možné maticu Q kompletne zrekonštruovať. Takisto sme vysvetlili, že kvázicyklická štruktúra matice Q umožňuje vykonať útok s menším počtom meraní. Náš útok je možné zrealizovať aj v prípade, že QC-LDPC McEliece kryptosystém je používaný spolu s CCA2 konverziou. V závere článku sme vysvetlili, že nášmu útoku sa dá predísť v prípade, že je dešifrovací algoritmus v QC-LDPC McEliece kryptosystéme implementovaný odlišným spôsobom. Odporučili sme použiť rovnaký spôsob implementácie, ako navrhli Heyse, Moradi a Paar v článku [9].

Ako už bolo spomenuté v predchádzajúcej kapitole, výsledok z nášho článku [5] implikuje, že QC-LDPC McEliece kryptosystém momentálne nie je vhodný na použitie v

podmienkach, v ktorých sa používa ten istý verejný kľúč po dlhšiu dobu. Pri našom útoku s využitím merania spotreby stačí ale útočníkovi poslať obeti výrazne menej správ ako v prípade útoku z [5]. Preto náš útok s meraním spotreby ukazuje, že ak je QC-LDPC McEliece kryptosystém implementovaný s nejakým horným limitom na počet dešifrovaní (stanoveným tak, aby nebolo možné vykonať útok z [5]), potom je ešte stále potrebné dbať na to, aby bol dešifrovací algoritmus implementovaný spôsobom, ktorý neumožní vykonať útok s využitím merania spotreby elektrickej energie.

Generovanie invertovateľných cyklických matíc s predpísaným počtom jednotiek

Ako už bolo spomenuté, výsledok z nášho článku [5] implikuje, že QC-LDPC McEliece kryptosystém momentálne nie je vhodný na použitie v podmienkach, v ktorých sa používa ten istý verejný kľúč po dlhšiu dobu. Tento výsledok ale nebráni použitiu QC-LDPC McEliece kryptosystému v situáciách, v ktorých sa vyžadujú iba jednorazové kľúče, ako napríklad v protokoloch na výmenu kľúča. V takom prípade môže ale QC-LDPC McEliece kryptosystém stále byť ohrozený útokom od autorov Shooshtari a spol.[16]. Tomuto útoku sa dá predísť tak, že rozmer cyklických blokov p sa zvolí ako nepárne číslo.

Ako súčasť súkromného kľúča v QC-LDPC McEliece kryptosystéme sa musia vygenerovať matice S a Q. Obidve tieto matice musia byť invertovateľné a zložené z cyklických blokov rozmeru $p \times p$. Okrem toho musí matica S byť hustá a matica Q naopak musí byť riedka s predpísaným počtom jednotiek. V návrhu QC-LDPC McEliece kryptosystému [2] navrhli jeho autori spôsob ako generovať matice S a Q v prípade, že p je mocninou čísla 2. V prípade, že p nie je mocninou čísla 2, navrhovaný spôsob generovania negarantuje, že výsledné matice budú invertovateľné.

V článku [7] sme sa zaoberali otázkou ako generovať matice S a Q v prípade, že p je nepárne. Najprv sme riešili otázku ako generovať invertovateľné cyklické matice s predpísaným počtom jednotiek. V článku od autorov von Maurich a Güneysu [10] bolo generovanie takýchto matíc riešené tak, že sa generovali náhodné cyklické matice s predpísaným počtom jednotiek, až kým jedna z nich nebola invertovateľná. V našom článku sme navrhli alternatívne algoritmy na generovanie invertovateľných cyklických matíc s predpísaným počtom jednotiek. V porovnaní s algoritmom od autorov von Maurich a Güneysu [10] majú naše algoritmy výhodu, že generujú matice spĺňajúce všetky požiadavky hneď na prvý pokus. Ich nevýhodou ale je, že generujú matice iba z obmedzenej množiny - nie je pomocou nich možné vygenerovať ľubovoľnú invertovateľnú cyklickú maticu s predpísaným počtom jednotiek. Pre každý z našich algoritmov sme určili veľkosť množiny možných vygenerovaných matíc. Veľkosť tejto množiny závisí od

ireducibilnej faktorizácie polynómu $x^p + 1$ (p tu označuje rozmer matice), konkrétne od stupňa d najmenšieho polynómu iného ako $x + 1$ v tejto faktorizácii. Najmenším polynómom tu myslíme polynóm najmenšieho stupňa. Na dosiahnutie veľkej množiny možných vygenerovaných matíc je potrebné zvoliť p tak, aby hodnota d bola vysoká. V článku vysvetľujeme, že hodnota d sa dá jednoducho určiť.

Následne sme v našom článku navrhli algoritmy na generovanie matíc S a Q v QC-LDPC McEliece kryptosystéme pre prípad, že rozmer cyklických blokov p je nepárny. Opäť veľkosť množiny možných vygenerovaných matíc (a tiež efektívnosť algoritmu na generovanie matice S) závisí od ireducibilnej faktorizácie polynómu $x^p + 1$ (p tu označuje rozmer cyklických blokov). Z tohto dôvodu sa ako najlepšia voľba pre rozmer cyklických blokov javí prvočíslo p také, že multiplikatívny rád čísla 2 modulo p je $p - 1$. Podľa Artinovej hypotézy o primitívnych koreňoch približne 37% prvočísel spĺňa túto podmienku [13].

Prirodzene sa ponúka použiť naše algoritmy na generovanie invertovateľných cyklických matíc s predpísaným počtom jednotiek aj pri generovaní matice H v QC-LDPC McEliece kryptosystéme a v QC-MDPC McEliece kryptosystéme. V obidvoch kryptosystémoch je užitočné, ak je posledný cyklický blok matice H invertovateľný. V našom článku ale upozorňujeme na to, že ak je hodnota d výrazne nižšia ako rozmer cyklického bloku p, potom použitie našich algoritmov by umožnilo útočníkovi vykonať výrazne efektívnejší ISD útok. V takých prípadoch odporúčame generovať posledný blok matice H metódou z [10], t.j. postupným generovaním náhodných cyklických matíc s predpísaným počtom jednotiek, až kým jedna z matíc nie je invertovateľná.

References

[1] Baldi, M., Chiaraluce, F.: Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. In: Proc. IEEE ISIT 2007, Nice, France, June 2007, pp. 2591-2595 (2007)

[2] Baldi, M., Bodrato, M., Chiaraluce, F.: A new analysis of the McEliece cryptosystem based on QC-LDPC codes. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) 6th International Conference on Security and Cryptography for Networks (SCN 2008). LNCS, vol. 5229, pp. 246-262. Springer, Berlin (2008)

[3] Berlekamp, E., McEliece, R. and Van Tilborg, H.: On the inherent intractability of certain coding problems (Corresp.). IEEE Transactions on Information Theory,

24(3), pp.384-386 (1978)

[4] Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D.: Report on post-quantum cryptography. National Institute

[5] Fabšič, T., Hromada, V., Stankovski, P., Zajac, P., Guo, Q. and Johansson, T.: A Reaction Attack on the QC-LDPC McEliece Cryptosystem. In International Workshop on Post-Quantum Cryptography (pp. 51-68). Springer, Cham. (2017)

[6] Fabšič, T., Gallo, O. and Hromada, V.: Simple power analysis attack on the QC-LDPC McEliece cryptosystem. Tatra Mountains Mathematical Publications, 67(1), pp.85-92. (2016)

[7] Fabšič, T., Grošek, O., Nemoga, K. and Zajac, P.: On generating invertible circulant binary matrices with a prescribed number of ones. Cryptography and Communications, Jul 2017. (2017)

[8] Guo, Q., Johansson, T. and Stankovski, P.: A key recovery attack on MDPC with CCA security using decoding errors. In Advances in Cryptology-ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22 (pp. 789-815). Springer Berlin Heidelberg (2016)

[9] Heyse, S., Moradi, A., and Paar, C.: Practical power analysis attacks on software implementations of McEliece. In: Sendrier, N. (eds.) Post-Quantum Cryptography, LNCS, vol. 6061, pp. 108-125. Springer International Publishing, (2010)

[10] von Maurich, I. and Güneysu, T.: Towards Side-Channel Resistant Implementations of QC-MDPC McEliece Encryption on Constrained Devices. PQCrypto, 2014, pp.266-282. (2014)

[11] R.J. McEliece: A Public-Key Cryptosystem Based On Algebraic Coding Theory. Deep Space Network Progress Report, 44:114-116 (1978)

[12] Misoczki R., Tillich J-P., Sendrier N., Barreto P.S.L.M.: MDPC-McEliece: new McEliece variants from moderate density parity-check codes. In: IEEE International Symposium on Information Theory (ISIT 2013), pp. 2069-2073. Istanbul (2013)

[13] Moree, P.: Artin's primitive root conjecture-a survey. Integers, 12(6), pp.1305-1416. (2012)

[14] Mosca, M.: Cybersecurity in an era with quantum computers: Will we be ready? Cryptology ePrint Archive, Report 2015/1075. (2015)

[15] Otmani, A., Tillich, J.P., Dallot, L.: Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. In: Proc. First International Conference on Symbolic Computation and Cryptography (SCC 2008), Beijing, China (2008)

[16] Shooshtari, M.K., Ahmadian-Attari, M., Johansson, T. and Aref, M.R.: Cryptanalysis of McEliece cryptosystem variants based on quasi-cyclic low-density parity check codes. IET Information Security, 10(4), pp.194-202. (2016)

[17] Shor, P. W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), pp. 303-332 (1999)

Part I

Introduction to the Thesis

1 Goals and Organization of the Thesis

In [67], P. W. Shor demonstrated that prime factorization and discrete logarithms can be solved in polynomial time on a quantum computer. This means that building a sufficiently large quantum computer would render currently used public key cryptosystems insecure. Many scientists now believe that building a large-scale quantum computer is merely a significant engineering challenge and some engineers even predict that within the next 20 years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use [52]. In 2016, the National Institute of Standards and Technology (NIST) has issued an announcement recognizing this threat and calling for the standardization and transition to post-quantum public key cryptography in the near future [22].

For these reasons, a lot of research in cryptography is currently focused on devising new public key cryptosystems which would be quantum-resistant. These cryptosystems have to be based on problems which cannot be efficiently solved even on a quantum computer. One of such problems is the problem of decoding a general linear code. It is known that this problem is NP-complete [10] and currently no efficient algorithms for solving NP-complete problems are known even for a quantum computer.

The first public key cryptosystem based on the problem of decoding a general linear code was proposed already in 1978 by R. J. McEliece [48]. This cryptosystem is now known as the McEliece cryptosystem, and it still remains unbroken. The cryptosystem has never been adopted widely, mainly due to the large size of the public key. Due to the threat of quantum computers, the interest in the McEliece cryptosystem has, however, risen recently and currently it is a very active topic of scientific research.

A number of variants of the McEliece cryptosystem have been proposed with the intention to reduce the size of the public key. Among these proposals are variants which employ quasi-cyclic low-density parity-check (QC-LDPC) codes. The present thesis focuses on these variants. In particular, the thesis has the following objectives:

1. *Objective 1:* To contribute to the cryptanalysis of variants of the McEliece cryptosystem based on QC-LDPC codes.

2. *Objective 2:* To propose methods to generate invertible sparse circulant matrices suitable for use in variants of the McEliece cryptosystem based on QC-LDPC codes.

The thesis is a compilation of three research papers [24, 25, 26]. The papers [24, 25] address Objective 1, while the paper [26] addresses Objective 2.

The three papers are preceded by the introductory part. In the introductory part, we review the theoretical background on the original McEliece cryptosystem and its later variants employing QC-LDPC codes, and we summarize our contributions.

2 Linear Codes

In this section, we present basic definitions regarding linear codes. Our presentation follows the presentation from [12].

A binary $[n, k]$ code is a binary *linear code* of length n and dimension k, i.e., it is a k-dimensional linear subspace of F_2^n . All codes considered in this thesis are binary.

A *generator matrix* of an $[n, k]$ code C is a $k \times n$ matrix G such that

$$C = \left\{ xG : \ x \in F_2^k \right\}.$$

We say that G generates the code C.

A *parity-check matrix* of an $[n, k]$ code C is an $(n - k) \times n$ matrix H such that

$$C = \left\{ c \in F_2^n : \ Hc^T = 0 \right\}.$$

The linear code generated by H is called the *dual code* to the code C.

A *systematic* generator matrix of an $[n, k]$ code C is a generator matrix of the form $(I_k|Q)$ where I_k is the $k \times k$ identity matrix and Q is a $k \times (n - k)$ matrix. There might not exist a systematic generator matrix for C, but there exists a systematic generator matrix for an equivalent code obtained by permuting columns of C.

The classical *decoding problem* is to find the closest codeword $c \in C$ to a given $y \in F_2^n$, assuming that there is a unique closest codeword. Here "close" means that the difference $c - y$ has a small Hamming weight.

3 McEliece Cryptosystem

The presentation in this section was inspired by the overview of the McEliece cryptosystem in [64].

3.1 Description of the McEliece Cryptosystem

The McEliece cryptosystem [48] is a public key cryptosystem based on the problem of decoding a general linear code. The essential part of the secret key in this cryptosystem is a secret linear error-correcting code with an efficient decoding algorithm. In McEliece's original proposal [48], Goppa codes with Patterson's decoding algorithm [57] were used in this role. Definitions of Goppa codes and Patterson's algorithm are not needed for understanding the later parts of this thesis, and therefore we omit them.

Suppose that the secret code is able to correct t errors. Let G be a generator matrix of the secret code of dimension $k \times n$. Bob will generate his public key G' as $G' = S \cdot G \cdot P$, where S is a secret non-singular $k \times k$ matrix and P is a secret $n \times n$ permutation matrix. Thus, Bob's private key consists of matrices G, S and P and his public key consists of the matrix G'.

Suppose Alice wants to send a message $u \in F_2^k$ to Bob. Then Alice encrypts u as $c = u \cdot G' + e$, where e is a randomly generated error vector of length n and weight t.

To recover the original message, Bob first computes $c' = c \cdot P^{-1}$. We have

$$\begin{aligned} c' &= c \cdot P^{-1} \\ &= (u \cdot S \cdot G \cdot P + e) \cdot P^{-1} \\ &= u \cdot S \cdot G + e \cdot P^{-1}. \end{aligned}$$

Thus, c' is a codeword of the Goppa code G, affected by the error vector $e \cdot P^{-1}$ of weight t. Therefore, Bob can use Patterson's algorithm [57] to decode c'. After decoding he obtains the vector $u' = u \cdot S$. Finally, he recovers u as $u = u' \cdot S^{-1}$.

3.2 Niederreiter Cryptosystem

A closely related cryptosystem was proposed by Niederreiter in 1986 [54]. The original version of the cryptosystem used generalized Reed-Solomon codes but this choice was shown to be insecure [68]. However, it was shown that when the Niederreiter cryptosystem is used with Goppa codes, then it has the same security as the McEliece cryptosystem [40].

The secret key in the Niederreiter cryptosystem consists of an $n \times n$ permutation matrix P, a non-singular $(n-k) \times (n-k)$ matrix S, and a parity-check matrix H for

a secret code of dimension k and error-correcting capability t. Using the secret key, Bob can generate his public key H' as $H' = S \cdot H \cdot P$.

If Alice wants to send Bob a message, she needs to embed the message in a vector u of length n and Hamming weight t. Afterwards, she computes the encrypted message c as $c = H' \cdot u^T$ and sends it to Bob.

To recover u, Bob firstly finds (using linear algebra) z such that $H \cdot z^T = S^{-1} \cdot c$. Then $H(z - uP^T)^T = 0$, which means that $z - uP^T$ is a codeword of the secret code. Thus, Bob can apply a decoding algorithm for the secret code to z and extract the error uP^T. After multiplication by P, Bob obtains the original message u.

3.3 Security of the McEliece Cryptosystem

The security of the McEliece Cryptosystem rests on the following two assumptions:

1. Let G' be the public key in the McEliece Cryptosystem. Let C' be the code with the generator matrix G'. There is no algorithm that can solve the decoding problem in C' (without the knowledge of the secret key) more efficiently than in an arbitrary linear code.

2. It is difficult to solve the decoding problem in an arbitrary linear code. This problem is known to be NP-hard [10].

The most efficient algorithms for solving the decoding problem in an arbitrary linear code are information-set decoding algorithms. Hence, the security level of the McEliece cryptosystem is estimated by the efficiency of information-set decoding (ISD) attacks. We review ISD attacks in Section 3.5.

Apart from ISD attacks, McEliece is also threatened by attacks which exploit the specifics of the encryption algorithm. We describe these attacks as well as methods to prevent them in Section 3.6.

3.4 Parameters and Public Key Size

The original parameters, proposed by McEliece, were $n = 1024$, $k = 524$ and $t = 50$. However, these are now considered insecure, as they offer only 50-bit security [13]. A number of other parameter choices has been proposed in the literature. We present them together with the corresponding values of the security level in Table 1. (Table 1 is a replication of a similar table presented in [64].)

The disadvantage of the McEliece cryptosystem is the large size of public keys. As we can see in Table 1, to achieve a security level of 80 bits or more, it is recommended to

Table 1: Recommended parameters for the McEliece cryptosystem.[64]

Sec. Level	Ref.	(n, k, t)	Public key size [kB]	
			Full	Systematic
50	[48]	(1024,524,50)	66	32
80	[12]	(2048,1751,27)	438	64
80	[53]	(1702,1219,45)	254	72
80	[16]	(2048,1696,32)	424	73
128	[13]	(3178,2384,68)	925	232
128	[16]	(4096,3604,41)	1802	217
256	[13]	(6944,5208,136)	4415	1104

use a public key of hundreds of kilobytes. In [12], it was noted that when the McEliece cryptosystem is used with a CCA2-secure[1] conversion, then the public key can be represented in systematic form without reducing the security of the system. Although this leads to a reduction in public key sizes, the reduced sizes are in tens or hundreds of kilobytes, i.e., the public keys are still significantly larger than public keys in currently used cryptosystems, such as RSA. (The public key in RSA 1024 has only approximately 0.1 kB.) The size of the public key in systematic form for various parameter choices for the McEliece cryptosystem is presented in Table 1.

3.5 Information-Set Decoding Attacks

Information-set decoding (ISD) algorithms are the most efficient known algorithms for solving the decoding problem in an arbitrary linear code, i.e. the problem on which the security of the McEliece cryptosystem relies.

The study of ISD attacks was initiated by Prange in [60]. The possibility of applying an ISD attack to the McEliece cryptosystem was already recognized by R.J. McEliece in [48]. R.J. McEliece proposed the following form of an ISD attack. Let c be a ciphertext encrypted by the McEliece cryptosystem. Select k coordinates of c. The probability that none of the selected coordinates is affected by an error is $\binom{n-t}{k}/\binom{n}{k}$. Provided that the k columns in G' corresponding to the k selected coordinates are all linearly independent, the original message can then be found simply by solving k linear equations in k unknowns. The estimated running time of the attack is then $k^3\binom{n}{k}/\binom{n-t}{k}$. In [39], a generalization of this method was introduced, allowing a small number of errors in the k selected coordinates.

[1] We discuss CCA2-secure conversions of the McEliece cryptosystem in Section 3.6

Table 2: Performance of ISD algorithms.[36]

Author(s)	Ref.	Year	$\max_{0\leq R\leq 1} \alpha\left(R, W_{GV}\right)$
Prange	[60]	1962	0.1207
MMT	[46]	2011	0.1114
BJMM	[9]	2012	0.1019
MO	[47]	2015	0.0966

The currently most efficient ISD attacks are based on Stern's algorithm [69] for finding codewords with a low Hamming weight. Let $c = u \cdot G' + e$ be a ciphertext encrypted by the McEliece cryptosystem, where e is an error vector with the Hamming weight t. Consider the matrix

$$\begin{pmatrix} G' \\ c \end{pmatrix}.$$

Consider the linear code generated by this matrix. The shortest non-zero codeword in this code (i.e., the codeword with the lowest non-zero Hamming weight) is e. Thus, one can use Stern's algorithm on this code to find the error vector e and consequently determine the plaintext u.

The standard conjecture is that the best possible generic algorithm for decoding linear codes takes exponential time for any constant asymptotic code rate R and constant asymptotic error fraction W: i.e., time $2^{(\alpha(R,W)+o(1))n}$, for some positive real number $\alpha(R, W)$ if $k/n \to R$ and $t/n \to W$ as $n \to \infty$ [13].

A number of enhanced variants of Stern's algorithm have been proposed in the literature [13, 46, 9, 47] and the best currently known ISD algorithm is by May and Ozerov [47]. However, all these efforts only managed to decrease the exponent $\alpha(R, W)$ slightly. In Table 2, we present an overview of the performance of currently existing ISD algorithms. The table is a replication of a similar table presented in [36] and it shows the average time complexity of the algorithms when W is the Gilbert-Varshamov distance $d_{GV}(n, k)$ of the code. The Gilbert-Varshamov distance is defined as $d_{GV}(n, k) = nH_2^{-1}\left(1 - \frac{k}{n}\right)$, where H_2 is the binary entropy function $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ and H_2^{-1} is its inverse defined from $[0, 1]$ to $\left[0, \frac{1}{2}\right]$. It corresponds to the largest distance for which we may still expect a unique solution to the decoding problem. In Table 2, W_{GV} is defined as $W_{GV} = \frac{d_{GV}(n,k)}{n}$.

The complexity of ISD gets lower, when the attacker only needs to decode one out of many ciphertexts. In [65], Sendrier showed that ISD attacks can be speeded up by almost $\sqrt{N}$ using N instances of the problem. When the attacker has access to an unlimited

Table 3: Performance of quantum ISD algorithms.[36]

Author(s)	Ref.	Year	$\max_{0\leq R\leq 1} \alpha\left(R, W_{GV}\right)$
Bernstein	[11]	2010	0.06035
KT	[36]	2017	0.05970
KT	[36]	2017	0.05869

number of instances, the complexity exponent is multiplied by value only slightly larger than 2/3. This attack scenario is particularly important for variants of McEliece based on QC-LDPC and QC-MDPC codes, which we discuss in Section 4. In these variants, any block-wise cyclic shift of the ciphertext provides a proper new instance of the decoding problem. The solution for the shifted ciphertext is equal to the solution for the original ciphertext, up to a block-wise cyclic shift.

The possibility of applying quantum algorithms to speed up ISD algorithms was studied in [56, 11, 36]. It has been shown that with a use of quantum algorithms the value of $\max_{0\leq R\leq 1} \alpha\left(R, W_{GV}\right)$ can be reduced to below 0.06 [36]. We present the performance of current quantum ISD algorithms in Table 3. The table is a replication of a similar table presented in [36].

3.6 CCA2 Security

Information-set decoding attacks can be avoided by selecting large enough parameters in the McEliece cryptosystem. However, McEliece is also threatened by attacks which exploit the specifics of the encryption algorithm. To prevent these attacks, McEliece must be used with a proper conversion secure against adaptive chosen-ciphertext attacks (CCA2 conversion). As stated in [64]: *In ideal case, a proper CCA2 conversion transforms the original message (plaintext) into a random string of bits (cleartext), which is then encrypted with the classical McEliece. Once the recipient decodes the whole cleartext, he can decrypt the original message, as well as verify the integrity of the ciphertext.*

3.6.1 Attacks on McEliece without a CCA2 conversion

In this section, we follow the presentation in [38].

Known-Partial-Plaintext Attack. A partial knowledge of the target plaintext reduces the computational cost of ISD attacks on the McEliece cryptosystem [18, 37]. For example, let m_l and m_r denote the left k_l bits and the remaining k_r bits in the target plaintext m. Suppose that an attacker knows m_r. Let G'_l and G'_r be the upper k_l rows

and the remaining lower k_r rows in G'. We have

$$\begin{aligned} c &= m \cdot G' + e \\ c &= m_l \cdot G'_l + m_r \cdot G'_r + e \\ c + m_r \cdot G'_r &= m_l \cdot G'_l + e. \end{aligned}$$

Since $c + m_r \cdot G'_r$ is known to the attacker, this computation shows that the attacker can learn the plaintext by performing an ISD attack on the code generated by G'_l, which has a lower dimension k_l.

Related-Message Attack [14]. Suppose that two messages m_1 and m_2 are encrypted as c_1 and c_2, respectively, where $c_1 = m_1 G' + e_1$ and $c_2 = m_2 G' + e_2$. Suppose that an attacker knows a linear relation between the plaintexts, e.g. $\delta m = m_1 + m_2$. Since $e_1 + e_2 = \delta m G' + c_1 + c_2$, the attacker knows the value of $e_1 + e_2$. Since the Hamming weight of an error vector is small compared to its length, the attacker knows that if the i-th bit in $e_1 + e_2$ is zero, then with a high probability the i-th bit is zero in both e_1 and e_2. Thus, the attacker can increase the efficiency of an ISD attack on either c_1 or c_2 by choosing k coordinates whose values are zero in $e_1 + e_2$. A special case of this attack is when messages m_1 and m_2 are identical.

Reaction Attack [31]. The attacker flips the i-th bit of the target ciphertext c. Let c' denote the flipped ciphertext. The attacker sends c' to the proper receiver and observes his/her reaction. If the receiver returns a repeat request due to an uncorrectable error, the attacker knows that with a high probability the flipped bit resulted in the ciphertext having more errors than the decoding algorithm could correct. Thus, the attacker knows that with a high probability the i-th bit of the error vector in the target ciphertext is zero. Repeating this process, the attacker can learn more information about the error vector, and thus can increase the efficiency of an ISD attack on c. A similar attack was independently proposed in [70].

Malleability Attack. Let c be the ciphertext corresponding to a plaintext m. For any vector δm of length k, an attacker can create a new ciphertext c' corresponding to $m' = m + \delta m$ even without knowing m [37, 70]. To see this, let $G'[i]$ denote the i-th row of G' and let $I = \{i_1, i_2, \dots\}$ denote the set of coordinates whose value is 1 in δm. Then the attacker can construct c' as $c' = c + \sum_{i \in I} G'[i] = (m + \delta m)G' + e$. Let us consider the chosen-ciphertext scenario, where an attacker can ask an decryption oracle to decrypt a polynomial number of ciphertexts (excluding the target ciphertext c). Then the attacker can decrypt any ciphertext c as follows. The attacker asks the oracle to decrypt c'. The oracle returns m', from which the attacker can compute m as $m = m' + \delta m$.

3.6.2 CCA2 Conversions for McEliece

In [38], Kobara and Imai studied how to convert the McEliece cryptosystem into a public key cryptosystem indistinguishable against adaptive chosen-ciphertext attacks. They observed that generic conversions by Pointcheval [59] and by Fujisaki and Okamoto [27] can be applied to McEliece for this purpose. Furthermore, Kobara and Imai proposed three new conversions specifically designed for the McEliece cryptosystem and proved that in the random oracle model breaking the indistinguishability of encryption of their conversions in an adaptive chosen-ciphertext scenario is polynomial equivalent to decrypting the whole plaintext of an arbitrarily given ciphertext of the original McEliece cryptosystem without any help of decryption oracles and any knowledge on the target plaintext.

The conversions of Kobara and Imai have the advantage of lower data redundancy when compared to the conversions of Pointcheval and Fujisaki-Okamoto. Here, we present the most efficient conversion of Kobara and Imai, the conversion γ. We use the following notation:

- $C(n,t)$: The number of combinations taking t out of n elements.
- $Prep(m)$: Preprocessing to a message m, such as data-compression, data-padding and so on. Its inverse is represented as $Prep^{-1}()$.
- $Hash(x)$: One-way hash function of an arbitrary length binary string x to a fixed length binary string.
- $Conv(\bar{z})$: Bijective function which converts an integer $\bar{z} \in Z_N$, where $N = C(n,t)$ into the corresponding error vector z. Its inverse is represented as $Conv^{-1}()$.
- $Gen(x)$: Generator of a cryptographically secure pseudo random sequences of arbitrary length from a fixed length seed x.
- $Len(x)$: Bit-length of x.
- $Msb_{x_1}(x_2)$: The left x_1 bits of x_2.
- $Lsb_{x_1}(x_2)$: The right x_1 bits of x_2.
- $Const$: Predetermined constant used in public.
- $Rand$: Random source which generates a truly random (or computationally indistinguishable pseudo random) sequence.

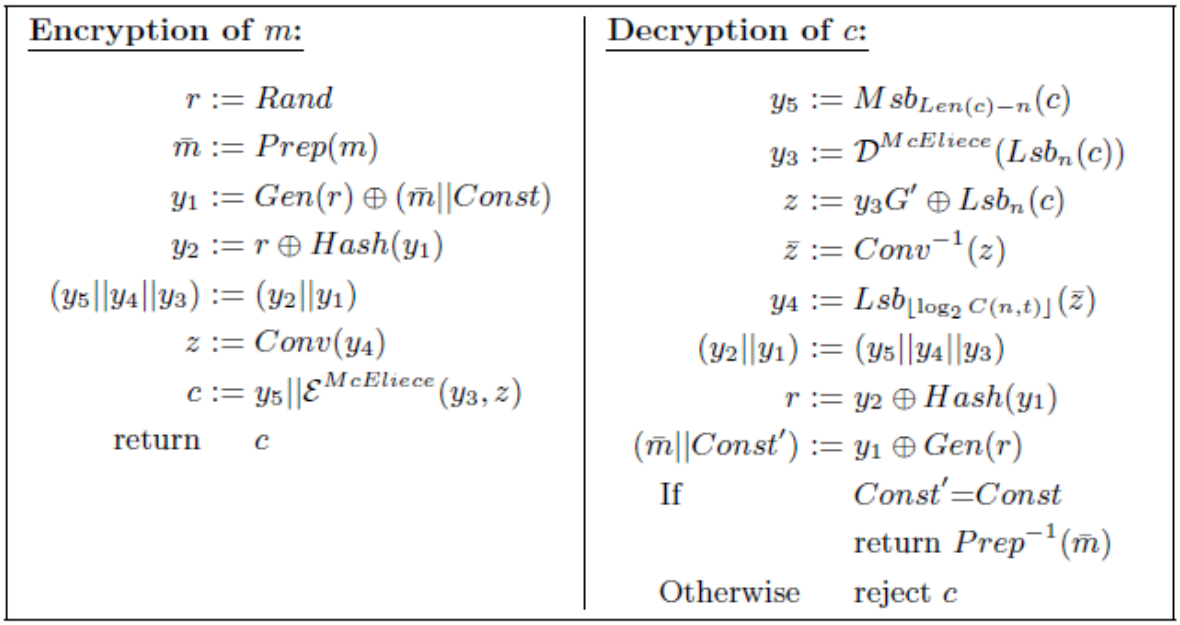

Figure 1: Kobara-Imai γ conversion [38] for the McEliece cryptosystem: $Len(y_3) = k$, $Len(y_4) = \log_2 C(n,t)$, $Len(y_5) = Len(\bar{m}) + Len(Const) + Len(r) - Len(y_4) - k$. If $Len(\bar{m}) + Len(Const) + Len(r) = Len(y_4) + k$, remove y_5.

- $\mathcal{E}^{McEliece}(x, z)$: Encryption of x using the original McEliece cryptosystem with an error vector z.
- $\mathcal{D}^{McEliece}(x)$: Decryption of x using the original McEliece cryptosystem.

We present the Kobara-Imai γ conversion in Figure 1.

4 QC-LDPC and QC-MDPC Variants of the McEliece Cryptosystem

As noted in Section 3.1, the disadvantage of the original McEliece cryptosystem is the large size of public keys. For this reason, variants of McEliece have been proposed with the ambition to reduce the size of public keys. Among these proposals are variants based on quasi-cyclic low-density parity-check (QC-LDPC) codes and quasi-cyclic moderate-density parity-check (QC-MDPC) codes. These proposals replace the secret Goppa code in the original McEliece by a QC-LDPC code or by a QC-MDPC code. Before we describe these proposals in more detail, we first review the basic theory on LDPC codes.

4.1 LDPC Codes and QC-LDPC Codes

Low-density parity-check (LDPC) codes were invented by Gallager in [28]. Here we review important definitions and decoding algorithms regarding these codes.

Definition 1. A *low-density parity-check (LDPC) code* is a binary linear code which admits a parity-check matrix H with a low number of 1s among its entries (i.e. H has a low density). Typically, 1% or fewer of the entries of H are 1s.

Definition 2. An $(n \times n)$-matrix $C = (c_{ij})_{i,j=0,\ldots,n-1}$ is called *circulant* if its rows are generated by successive cyclic right shifts of the first row. Thus, C is of the form

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & \ldots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \ldots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \ldots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \ldots & c_0 \end{pmatrix}.$$

Definition 3. A *quasi-cyclic* low-density parity-check (QC-LDPC) code is a LDPC code which admits a low-density parity-check matrix H in the form

$$H = \begin{pmatrix} H_{0,0} & H_{0,1} & \ldots & H_{0,n_0-1} \\ H_{1,0} & H_{1,1} & \ldots & H_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ H_{r_0-1,0} & H_{r_0-1,1} & \ldots & H_{r_0-1,n-1} \end{pmatrix},$$

where each $H_{i,j}$ is a $p \times p$ circulant matrix.

Definition 4. Let C be a LDPC $[n, k]$ code with a $(n-k) \times n$ low-density parity-check matrix H. To C we associate its *Tanner graph* defined as follows. Tanner graph is a

bipartite graph which has n left nodes (also called "*variable nodes*") and $n-k$ right nodes (also called "*check nodes*"). An edge between a variable node v_j and a check node c_i exists if and only if the entry h_{ij} in H is equal to one.

4.1.1 Soft-Decision Decoding of LDPC Codes

Several soft-decision decoding algorithms exist for LDPC codes. Below, we describe the Gallager Sum-Product Algorithm as presented in [63]. Let y be the vector to be decoded. We consider a special case where we assume that every bit y_j of y is erroneous with probability ϵ. Then the Gallager Sum-Product Algorithm is described in Algorithm 1. In the algorithm, $N(i)$ represents the set of variable nodes in the Tanner graph connected to the check node c_i. Similarly, $N(j)$ represents the set of check nodes connected to the variable node v_j.

Algorithm 1

INPUT: a low-density parity-check matrix H of an LDPC code and its corresponding Tanner graph; vector y to be decoded

OUTPUT: decoded codeword z or a decoding error message

---

1. **Initialization:** For all j, initialize L_j as

$$L_j = \log\left(\frac{\text{Prob}(z_j = 0|y_j)}{\text{Prob}(z_j = 1|y_j)}\right) = (-1)^{y_j}\log\left(\frac{1-\epsilon}{\epsilon}\right).$$

   Then for every pair (v_j, c_i) of a variable node v_j and a check node c_i which are connected by an edge in the Tanner graph, initialize the message going from the variable node v_j to the check node c_i as $L_{j\to i} = L_j$.

2. **Check nodes update:** For every pair (v_j, c_i) of a variable node v_j and a check node c_i which are connected by an edge in the Tanner graph, compute the message from c_i to v_j as

$$L_{i\to j} = 2\tanh^{-1}\left(\prod_{j'\in N(i)-\{j\}}\tanh\left(\frac{1}{2}L_{j'\to i}\right)\right).$$

3. **Variable nodes update:** For every pair (v_j, c_i) of a variable node v_j and a check node c_i which are connected by an edge in the Tanner graph, compute the message from v_j to c_i as

$$L_{j\to i} = L_j + \sum_{i'\in N(j)-\{i\}} L_{i'\to j}.$$

4. **Log-likelihood ratio total:** For all j compute

$$L_j^{\text{total}} = L_j + \sum_{i \in N(j)} L_{i \to j}.$$

5. **Stopping criteria:** For all j set

$$\hat{y}_j = \begin{cases} 1 & \text{if } L_j^{\text{total}} < 0, \\ 0 & \text{else,} \end{cases}$$

to obtain a vector $\hat{y}$.
If $\hat{y}H^T = 0$, return $z = \hat{y}$.
If the maximum number of iterations was reached, return a decoding error message.
Else, go to Step 2.

4.1.2 Hard-Decision Decoding of LDPC Codes

Another method to decode an LDPC code is to use a hard-decision decoding (also called "bit-flipping") algorithm. Compared to soft-decision decoding algorithms, bit-flipping algorithms are simpler but less efficient (in terms of the number of errors they can correct). These algorithms are again iterative and their principle is as follows. The variable nodes of the Tanner graph are initially filled with the bits of the received codeword c (possibly affected by errors). In each iteration, the message sent from each check node c_i to each neighboring variable node v_j is the sum of the values of all its neighboring variable nodes. Thus, the node v_j will learn whether the i-th parity-check equation is satisfied or not (i.e. whether the i-th element of Hc^T is zero or not). Thus, the node v_j can count the number of unsatisfied parity-check equations which it is involved in. If this number exceeds some threshold b, then v_j flips its value. The next iteration uses the updated values of variable nodes. The process continues until all parity-check equations are satisfied or until a maximum number of iterations is reached.

4.2 Description of the QC-LDPC McEliece Cryptosystem

The possibility of using LDPC codes in the McEliece cryptosystem was firstly studied in [50]. The authors, however, concluded that the low density of LDPC codes does not allow a reduction in the public key size, since the passage from the secret key to the public key must involve a dense transformation matrix. Otherwise, the secret key can be extracted from the public key.

In [2], Baldi and Chiaraluce proposed to use QC-LDPC codes in the McEliece cryptosystem to reduce the size of the public key. Their cryptosystem is now known as the QC-LDPC McEliece cryptosystem. The proposal was later amended in [3] to prevent the attacks of Otmani, Tillich and Dallot [55]. Here we present the version of the cryptosystem from [3].

A part of the private key in the QC-LDPC McEliece cryptosystem is formed by an $(n-k) \times n$ low-density parity-check matrix H of an LDPC code able to correct t errors. The matrix H is formed by a row $\{H_0, \ldots, H_{n_0-1}\}$ of $n_0 = n/(n-k)$ binary circulant blocks of size $p \times p$, where $p = n - k$. Each block has a row weight (i.e. the number of ones in a row) equal to a number w. If H_{n_0-1} is invertible, a generator matrix G for the code can be obtained as

$$G = \left[\begin{array}{c|c} & \left(H_{n_0-1}^{-1} \cdot H_0\right)^T \\ \mathbf{I} & \vdots \\ & \left(H_{n_0-1}^{-1} \cdot H_{n_0-2}\right)^T \end{array}\right].$$

The remaining part of the private key is formed by two other matrices; a dense invertible $k \times k$ matrix S and a sparse invertible $n \times n$ matrix Q. The matrices S and Q are formed by blocks of circulant $p \times p$ matrices. In addition, Q has a fixed row weight m. The public key is then computed as $G' = S^{-1} \cdot G \cdot Q^{-1}$.

Encryption is done as follows. Let the original message be u. Alice encrypts u as $x = u \cdot G' + e$, where e is a randomly generated error vector of length n and Hamming weight $w_{\mathrm{H}}(e) = t' \leq \frac{t}{m}$.

When Bob receives the encrypted message x, he first computes

$$x' = x \cdot Q = u \cdot S^{-1} \cdot G + e \cdot Q.$$

The vector x' is a codeword of the LDPC code chosen by Bob (corresponding to the information vector $u' = u \cdot S^{-1}$), affected by the error vector $e \cdot Q$, whose maximum weight is t. Bob is able to correct all the errors with very high probability by means of an LDPC decoding algorithm, thus recovering u'. Finally, Bob recovers u by multiplying u' by S.

4.3 Remarks on the QC-LDPC McEliece Cryptosystem

Remark 1. The public key G' in the QC-LDPC McEliece Cryptosystem is a matrix composed of blocks of $p \times p$ circulant matrices. This allows a more efficient representation of the public key.

Remark 2. The method of masking the secret code in the QC-LDPC McEliece Cryptosystem is very similar to the method in the original McEliece cryptosystem, except in QC-LDPC McEliece a matrix Q with a fixed row weight m is used instead of a permutation matrix P. The denser matrix Q is used in order to prevent the dual code to the public code to contain words with a very small Hamming weight. If such words were present in the dual code, then they could be found using Stern's algorithm. This could possibly lead to the construction of a low-density parity-check matrix for the public code, which could be used to decode ciphertexts.

Remark 3. In their first proposal of the QC-LDPC McEliece cryptosystem in [2], Baldi and Chiaraluce suggested the matrix S to be sparse and the matrix Q to have block-diagonal structure, meaning that the only nonzero blocks in Q would appear along the diagonal. In [55], Otmani, Tillich and Dallot, however, showed that these two features make the cryptosystem vulnerable against a structural attack. In reaction to these findings, Baldi, Bodrato and Chiaraluce proposed a new version of their cryptosystem in [3]. The new version uses a dense matrix S and a matrix Q which is no longer block-diagonal, and is therefore immune against the attack from [55].

Remark 4. In [2] and [3], Baldi, Bodrato and Chiaraluce proposed to construct the secret matrix H by the technique of random difference families [2], in order to avoid short cycles in the corresponding Tanner graph. It is known that the presence of short cycles deteriorates decoding properties of LDPC codes. However, in [4], Baldi, Bianchi and Chiaraluce showed that in LDPC codes with parameters as in the QC-LDPC McEliece cryptosystem, the impact of short cycles on decoding properties of the code is not significant and they concluded that blocks in the matrix H can be generated at random from the set of circulant matrices with w ones in a row.

Remark 5. The security and the complexity of the QC-LDPC McEliece cryptosystem is further analyzed in [5].

Remark 6. In [6], Baldi et al. showed that a better error correction performance can be achieved in the QC-LDPC McEliece cryptosystem if circulant blocks in the matrix H are allowed to have mutually different row weights.

Remark 7. In [4], Baldi et al. proposed a procedure for selecting the density of the private parity-check matrix H, based on the security level and the decryption complexity.

4.4 MDPC Codes and QC-MDPC Codes

In [49], Misoczki et al. introduced MDPC codes QC-MDPC codes.

Definition 5. A *moderate-density parity-check (MDPC) code* is a binary linear code which admits a parity-check matrix H with a number of 1s which is higher than in LDPC codes but which is still low. More precisely, the number of 1s in a row of H scales in $O(\sqrt{n \log n})$, where n is the length of the code.

Definition 6. A *quasi-cyclic* moderate-density parity-check (QC-MDPC) code is an MDPC code which admits a moderate-density parity-check matrix H in the form

$$H = \begin{pmatrix} H_{0,0} & H_{0,1} & \dots & H_{0,n_0-1} \\ H_{1,0} & H_{1,1} & \dots & H_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ H_{r_0-1,0} & H_{r_0-1,1} & \dots & H_{r_0-1,n-1} \end{pmatrix},$$

where each $H_{i,j}$ is a $p \times p$ circulant matrix.

Similarly as in LDPC codes, we can associate a Tanner graph to an MDPC code and we can use soft-decision and hard-decision decoding algorithms to decode these codes.

4.5 Description of the QC-MDPC McEliece Cryptosystem

Misoczki et al. introduced MDPC codes and QC-MDPC codes, in order to propose new cryptosystems - the MDPC McEliece cryptosystem and the QC-MDPC McEliece cryptosystem [49]. Here we describe the QC-MDPC McEliece cryptosystem.

The private key in the QC-MDPC McEliece cryptosystem is formed by an $(n-k) \times n$ moderate-density parity-check matrix H of an MDPC code able to correct t errors. The matrix H is formed by a row $\{H_0, \dots, H_{n_0-1}\}$ of $n_0 = n/(n-k)$ binary circulant blocks of size $p \times p$, where $p = n - k$. Each row of H has its weight (i.e. the number of ones in the row) equal to a number $\tilde{w}$.

The public key is a generator matrix G of the MDPC code. If H_{n_0-1} is invertible, G can be obtained as

$$G = \left[\begin{array}{c|c} & \left(H_{n_0-1}^{-1} \cdot H_0\right)^T \\ \mathbf{I} & \vdots \\ & \left(H_{n_0-1}^{-1} \cdot H_{n_0-2}\right)^T \end{array}\right].$$

As remarked by Misoczki et al., if the cryptosystem is used with a suitable CCA2 conversion, the public key can be in systematic form without threatening the security of the cryptosystem.

Encryption is done as follows. Let the original message be u. Alice encrypts u as $x = u \cdot G + e$, where e is a randomly generated error vector of length n and Hamming weight $w_{\mathrm{H}}(e) = t$.

To decrypt the message x, Bob can use a soft-decision or a hard-decision decoding algorithm to remove the error vector e from x. Afterwards, Bob can recover the original message u simply by linear algebra (or he can read it from first k entries of the vector $x - e$ in case G is in systematic form).

4.6 Remarks on the QC-MDPC McEliece Cryptosystem

Remark 8. The public key G in the QC-MDPC McEliece cryptosystem is a matrix composed of blocks of $p \times p$ circulant matrices. This allows a more efficient representation of the public key.

Remark 9. Apart from the QC-MDPC McEliece cryptosystem, Misoczki et al. also proposed a version of the McEliece cryptosystem based on MDPC codes which do not feature the quasi-cyclic property. However, in that case, the public key does not have the nice feature of being composed by blocks of circulant matrices. This leads to significantly larger public keys.

Remark 10. In the original proposal of the QC-MDPC McEliece cryptosystem in [49], the matrix H has the property that its rows have a constant weight $\tilde{w}$. In many subsequent papers on this cryptosystem, this property is replaced by the stricter property that in every circulant block of H every row has a constant weight $\frac{\tilde{w}}{n_0}$.

Remark 11. In [29], Guo and Johansson proposed a variant of the QC-MDPC McEliece cryptosystem working over a larger finite field then F_2.

Remark 12. In [7], Baldi et al. proposed a variant of the QC-MDPC McEliece cryptosystem where real-valued errors are added to a message during encryption.

Remark 13. For the protection against timing side-channel attacks, it is useful to have a constant-time decryption. In [19], Chaulet and Sendrier studied how to design an efficient constant-time decoder for the QC-MDPC McEliece cryptosystem.

4.7 Parameters and Public Key Sizes

In [3], Baldi et al. proposed two sets of parameters for the QC-LDPC McEliece cryptosystem. We present these parameters in Table 4. In this table, we also present sizes of the corresponding public keys, assuming that the public keys are in systematic form.

In [49], Misoczki et al. proposed parameters for the QC-MDPC McEliece cryptosystem for various security levels. We present their parameters in Table 5. Again, we present sizes of the corresponding public keys, assuming that the public keys are in systematic form.

Table 4: Recommended parameters for the QC-LDPC McEliece cryptosystem.[3]

Security level	n_0	n	p	t'	w	m	Public key size [kB]
71	4	16384	4096	27	13	7	≈ 1.5
80	3	24576	8192	40	13	11	≈ 2.0

Table 5: Recommended parameters for the QC-MDPC McEliece cryptosystem.[49]

Security level	n_0	n	p	$\tilde{w}$	t	Public key size [kB]
80	2	9602	4801	90	84	≈ 0.6
80	3	10779	3593	153	53	≈ 0.9
80	4	12316	3079	220	42	≈ 1.2
128	2	19714	9857	142	134	≈ 1.2
128	3	22299	7433	243	85	≈ 1.9
128	4	27212	6803	340	68	≈ 2.5
256	2	65542	32771	274	264	≈ 4.1
256	3	67593	22531	465	167	≈ 5.6
256	4	81932	20483	644	137	≈ 7.7

In Table 6, we present a comparison of public key sizes in QC-LDPC McEliece, QC-MDPC McEliece and the original McEliece with Goppa codes. We assume that public keys are in systematic form.

4.8 Security of QC-LDPC and QC-MDPC Variants of the McEliece Cryptosystem

Similarly as the original McEliece cryptosystem, the security of the QC-LDPC and the QC-MDPC McEliece cryptosystems relies on the following two assumptions:

1. It is impossible to extract an information from the public key which would allow to decode the corresponding code more efficiently than an arbitrary linear code.

Table 6: Comparison of public key sizes in QC-LDPC McEliece, QC-MDPC McEliece and the original McEliece with Goppa codes. Sizes are approximate and are in kilobytes.

Security level	QC-LDPC [3]	QC-MDPC [49]	Goppa [12]
80	2.0	0.6	57.6
128	-	1.2	192.2
256	-	4.1	958.5

2. It is difficult to solve the decoding problem in an arbitrary linear code.

Like in the original McEliece cryptosystem, the most efficient algorithms threatening the security of the QC-LDPC and the QC-MDPC McEliece cryptosystems are ISD algorithms. However, unlike in the original McEliece where ISD algorithms can be used only to recover plaintexts, in QC-LDPC and QC-MDPC McEliece ISD can also be used to reconstruct the secret key. This can happen provided that the public code contains codewords with sufficiently small Hamming weight as we described in Remark 2 in Section 4.3.

For QC-LDPC and QC-MDPC McEliece, the reduction in the complexity of ISD attacks associated with the task of decoding one out of many ciphertexts [65] is particularly relevant, since in these variants any block-wise cyclic shift of the ciphertext provides a proper new instance of the decoding problem. The solution for the shifted ciphertext is equal to the solution for the original ciphertext, up to a block-wise cyclic shift.

Like the original McEliece, QC-LDPC and QC-MDPC McEliece are also vulnerable to the attacks described in Section 3.6.1, but can be protected against these attacks by conversions from Section 3.6.2.

4.8.1 Squaring Attacks

In [41] and [66], it was shown that when the value of the block size p in the QC-LDPC and the QC-MDPC McEliece cryptosystems is even, then a more efficient ISD attack can be built.

4.8.2 Rational Reconstruction Attack and Weak Keys in the QC-MDPC McEliece cryptosystem

In [8], Bardet et al. introduced the rational reconstruction attack on the QC-MDPC McEliece cryptosystem. They showed that private keys satisfying certain hypotheses can be recovered through this attack and they estimated the number of these weak keys.

4.8.3 Reaction Attack on the QC-MDPC McEliece Cryptosystem

In [30], Guo et al. presented a reaction attack on the QC-MDPC McEliece cryptosystem. They demonstrated that if the QC-MDPC McEliece cryptosystem employes a bit-flipping decoding algorithm in its decryption procedure, then there exists a dangerous dependence between the probability of decoding error and the secret key.

Guo et al. demonstrated their attack on a version of the cryptosystem with two blocks in the secret parity-check matrix H. Since the blocks are circulant, the block H_0 is determined by its first row h_0. They showed that an attacker who sends a large number of messages encrypted by the public key, and for each message learns whether it was

successfully decrypted, can learn distances between ones in h_0. The distance between two ones in positions p_1 and p_2, $p_2 > p_1$, in h_0 is defined as $\min\{p_2 - p_1, p - (p_2 - p_1)\}$, where p is the length of h_0 (i.e. the distance is computed cyclically). With the knowledge of distances in h_0, the attacker can reconstruct h_0 and recover the private key.

Guo et al. considered two different scenarios in their paper. In the first scenario, the attacker is allowed to choose the error vector e that is added to the message during encryption. In the second scenario, the attacker has no such freedom and the error vector is always chosen at random. In both scenarios, the attacker constructs for every $d \in \{1, \ldots p/2\}$ the set Σ_d of messages where the error vector contains the distance d. Guo et al. observed that if d is present in h_0, then the estimate for the probability of the decoding failure based on the set Σ_d is smaller than the estimate obtained from Σ_d when d is not present in h_0. Thus, after computing estimates for the probability of the decoding failure from each Σ_d, the attacker can learn which distances are present in h_0.

The successful execution of the attack in the second scenario implies that the attack is possible even when QC-MDPC McEliece is used with a CCA2-secure conversion, such as Kobara-Imai γ conversion [38], for example.

Guo et al. also conjectured that their attack is possible even when the cryptosystem uses a soft-decision decoding algorithm in its decryption procedure.

To avoid the attack, Guo et al. suggested that the probability of the decoding error should be approximately 2^{-K}, where K is the security level required from the cryptosystem. Some preliminary work in the direction of reducing the probability of the decoding error was done in [19]. However, at present no efficient decoding algorithms for MDPC codes exist that would provably have as low probability of the decoding error as advised by Guo et al.. Until this issue is resolved, the QC-MDPC McEliece cryptosystem cannot be securely used in circumstances where a long-term use of keys is required. However, it seems that QC-MDPC McEliece can still be used in situations where ephemeral keys are required, such as in key exchange protocols.

4.9 Implementations and Side-Channel Attacks

Implementation of the QC-MDPC McEliece cryptosystem has received considerable attention in [15, 33, 42, 43, 44]. The cryptosystem was also implemented in the cryptographic library BitPunch [17] developed at FEI STU.

A CCA-secure hybrid encryption protocol using the Niederreiter cryptosystem with QC-MDPC codes was implemented in [45]. The protocol is based on the proposal in [58]. In [23], Chou presented QcBits. QcBits is an implementation of a variant of the protocol

in [58], and it again features the Niederreiter cryptosystem with QC-MDPC codes. In addition, QcBits operates in constant time, which is a useful protection against timing side-channel attacks.

In [43], von Maurich and Güneysu showed that AVR/ARM microcontroller implementations of QC-MDPC McEliece can be vulnerable against simple power analysis attacks. In addition, they proposed countermeasures to prevent their attacks and to make their implementation run in constant time.

In [20, 21], differential power analysis attacks were presented on a lightweight FPGA implementation of QC-MDPC McEliece from [42] and possible countermeasures were discussed.

In [62], Rossi et al. presented a differential power analysis attack on QcBits [23] and proposed a countermeasure.

5 Our Contribution

We contributed to the analysis of the QC-LDPC McEliece cryptosystem in papers [24, 25, 26].

5.1 Reaction Attack on QC-LDPC McEliece

In [24], we presented a reaction attack on the QC-LDPC McEliece cryptosystem. The inspiration for this attack came from the work of Guo et al. [30], where a reaction attack on QC-MDPC McEliece was presented (a description of the attack in [30] is presented in Section 4.8.3).

Similarly as in [30], we showed that there exists a dependence between the secret matrix H and the failure probability of a decoding algorithm in the QC-LDPC McEliece cryptosystem. In addition, we observed that there also exists a dependence between the failure probability and the matrix Q. We argued that these dependencies leak enough information to allow an attacker to construct a sparse parity-check matrix for the public code. This parity-check matrix can then be used for decrypting ciphertexts.

To exploit this vulnerability, an attacker (Alice) has to send to a victim (Bob) a large number of messages encrypted by Bob's public key. We assumed, that for each message Alice will learn whether Bob successfully decrypted it or not (for instance, Alice can receive a message resend request in case of a decryption failure). We showed that with these information Alice can learn distances between ones in rows in circulant blocks of H and distances between ones in rows in circulant blocks of Q. We defined the distance between two ones in positions p_1 and p_2, $p_2 > p_1$, as $\min\{p_2 - p_1, p - (p_2 - p_1)\}$, where p is the dimension of circulant blocks in H and Q. We showed that, with the knowledge of distances in H and Q, Alice can reconstruct the matrix $\tilde{H} = H \times Q^T$, which is a sparse parity-check matrix for the public code and which can be used for decrypting ciphertexts.

To learn distances in H and Q, Alice constructs for every $d \in \{1, \dots p/2\}$ the set Σ_d as follows. Σ_d is the set of those messages sent to Bob where the error vector contains the distance d. We observed that the estimate for the probability of the decoding failure based on the set Σ_d is smaller when d is present in H and that it is even smaller when d is present in Q. Thus, after computing estimates for the probability of the decoding failure from each Σ_d, Alice can learn which distances are in H and which are in Q.

Similarly as in [30], we showed that Alice can execute the attack even if she has no freedom to choose what error vectors are added to the messages sent to Bob, i.e. the error vectors are generated randomly. This implies that the attack is possible even when QC-

LDPC McEliece is used with a CCA2-secure conversion, such as Kobara-Imai γ conversion [38], for example.

We verified our attack ideas on a version of the QC-LDPC McEliece cryptosystem which employed a soft-decision decoding algorithm. Thus, our results also confirm the conjecture from [30] that soft-decision decoding algorithms can be vulnerable to leak information about the secret parity-check matrix.

To prevent an attacker to learn distances in H and Q, it would help if the probability of the decoding failure decreased dramatically. In [30], Guo et al. suggested that the probability of the decoding error should be approximately 2^{-K}, where K is the security level required from the cryptosystem. To our best knowledge, however, no efficient LDPC decoding algorithms currently exist that would provably have such negligible probability of the decoding error. Similarly as QC-MDPC McEliece, the QC-LDPC McEliece cryptosystem, therefore, currently appears not suitable for use in circumstances where a long-term use of keys is required. However, it seems that it can still be used in situations where ephemeral keys are required, such as in key exchange protocols.

5.2 Power Analysis Attack on QC-LDPC McEliece

In [32], it was shown that a naive implementation of the decryption algorithm in the original McEliece cryptosystem allows an attacker to recover the secret matrix P by measuring the power consumption. In [25], we demonstrated that a similar threat is present in QC-LDPC McEliece, as well.

We considered a naive implementation of the decryption algorithm in the QC-LDPC McEliece cryptosystem. Our implementation was based on the project BitPunch [17] and featured a bit-flipping algorithm in the decoding procedure. We demonstrated that this implementation leaks information about positions of ones in the secret matrix Q. We argued that an adversary, who sends a victim ciphertexts with Hamming weight 1 and measures the power consumption during the decryption, can completely recover the matrix Q. In addition, we remarked that the quasi-cyclic nature of the matrix Q allows to accelerate the attack significantly. This attack is possible even when QC-LDPC McEliece is used with the Kobara-Imai γ conversion [38], for example. We further observed that the same countermeasure as was proposed in [32] can be applied in QC-LDPC McEliece, as well.

As already noted in Section 5.1, the reaction attack from [24] suggests that the QC-LDPC McEliece cryptosystem might not be suitable for the deployment in circumstances where a long-term use of keys is required. Compared to the reaction attack in [24], the

adversary needs to send significantly fewer ciphertexts in the simple power analysis attack. Therefore, our result shows that if QC-LDPC McEliece was deployed with some upper bound on the number of decryptions it can perform (designed to prevent the reaction attack from [24]), then a careful implementation might be needed to avoid the simple power analysis attack.

5.3 Generating Invertible Circulant Matrices with a Prescribed Number of Ones

As noted in Section 5.1, the QC-LDPC McEliece cryptosystem appears not suitable for the deployment in circumstances where a long-term use of keys is required. However, it seems that it can still be used in situations where ephemeral keys are required, such as in key exchange protocols. In such situations, the cryptosystem is still threatened by the squaring attack described in [66]. To avoid this attack, the dimension of circulant blocks in the cryptosystem has to be odd.

QC-LDPC McEliece requires generating matrices S and Q, which are invertible and are composed of blocks of circulant matrices of the dimension p. In addition, S is dense and Q is sparse with a prescribed low number of ones in a row. In [3], Baldi et al. proposed a method how to construct matrices satisfying these requirements for the case when p is a power of 2. In case p is not a power of 2, their method, however, does not necessarily produce an invertible matrix.

In [26], we studied how to construct matrices S and Q when p is odd, which is the requirement to avoid the attack from [66]. We firstly studied how to construct invertible circulant binary matrices with a prescribed number of ones. In [43], this problem was solved by repeatedly generating random circulant matrices with the prescribed number of ones until an invertible matrix was obtained. The number of all invertible circulant matrices of a given size over $\mathbb{Z}_2$ can be computed by a formula [35]. Therefore, if a circulant binary matrix with a random number of ones was generated, the probability of the matrix being invertible could be computed. However, to the best of our knowledge, no general formula for computing the number of invertible circulant binary matrices of a given size and with a prescribed number of ones exists. Therefore, except for special cases, the expected number of repeated generations cannot be directly computed and can be only estimated by simulations. These extra generations and the associated extra invertibility tests can be costly in terms of time and in terms of entropy needed to generate extra random bits.

We proposed alternative algorithms for generating invertible circulant matrices with

a prescribed number of ones. Compared with the approach from [43], our algorithms have the advantage that they generate matrices satisfying all the requirements on the first attempt. On the other hand, their disadvantage is that they generate matrices from a smaller pool. For each of our algorithms a formula for the size of the pool was derived. Thus, a user is allowed to evaluate whether the size of the pool is sufficient for his/her application. The size of the pool depends on the degree d of a smallest polynomial (in terms of degree) other than $x + 1$ appearing in the irreducible factorization of $x^p + 1$ (p represents the size of the matrix). In order to achieve a large pool, the value of p should be chosen so that this degree is large. As we explain in the paper, the value of d can be easily determined.

Subsequently, we proposed algorithms to construct matrices S and Q in the QC-LDPC McEliece cryptosystem. Our algorithms assume that the size of blocks in S and Q is odd. Again, the size of the pool (and also the efficiency of the algorithm for S) depends on the irreducible factorization of $x^p + 1$ (here p represents the size of blocks). With this in mind, the best choice for the block size appears to be a prime p such that the multiplicative order of 2 modulo p is equal to $p - 1$. According to Artin's conjecture on primitive roots, approximately 37% of primes satisfy this condition [51].

It might be tempting to use our algorithms for generating invertible circulant matrices with a prescribed number of ones in the construction of the parity-check matrix H in the QC-LDPC McEliece cryptosystem and the QC-MDPC McEliece cryptosystem. In both these cryptosystem, it is useful if the last circulant block of H is invertible. However, we explained that in cases when d is significantly smaller than p, using our algorithm might allow an adversary to build a much more efficient ISD attack. In such cases, we recommend to generate the last block of H by repeatedly generating random circulant matrices with the prescribed number of ones until an invertible matrix is obtained, as was done in [43].

References

[1] Baldi, M.: QC-LDPC code-based cryptography. Springer Science & Business, (2014)

[2] Baldi, M., Chiaraluce, F.: Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. In: Proc. IEEE ISIT 2007, Nice, France, June 2007, pp. 2591-2595 (2007)

[3] Baldi, M., Bodrato, M., Chiaraluce, F.: A new analysis of the McEliece cryptosystem based on QC-LDPC codes. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) 6th International Conference on Security and Cryptography for Networks (SCN 2008). LNCS, vol. 5229, pp. 246-262. Springer, Berlin (2008)

[4] Baldi, M., Bianchi, M. and Chiaraluce, F.: Optimization of the parity-check matrix density in QC-LDPC code-based McEliece cryptosystems. In Communications Workshops (ICC), 2013 IEEE International Conference on (pp. 707-711). IEEE. (2013)

[5] Baldi, M., Bianchi, M. and Chiaraluce, F.: Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes. IET Information Security, 7(3), pp.212-220. (2013)

[6] Baldi, M., Bianchi, M., Maturo, N. and Chiaraluce, F.: Improving the efficiency of the LDPC code-based McEliece cryptosystem through irregular codes. In Computers and Communications (ISCC), 2013 IEEE Symposium on (pp. 000197-000202). IEEE. (2013)

[7] Baldi, M., Santini, P. and Chiaraluce, F.: Soft McEliece: MDPC code-based McEliece cryptosystems with very compact keys through real-valued intentional errors. In Information Theory (ISIT), 2016 IEEE International Symposium on (pp. 795-799). IEEE. (2016)

[8] Bardet, M., Dragoi, V., Luque, J.G. and Otmani, A.: Weak keys for the quasi-cyclic MDPC public key encryption scheme. In International Conference on Cryptology in Africa (pp. 346-367). Springer International Publishing. (2016)

[9] Becker, A., Joux, A., May, A. and Meurer, A.: Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 520-536). Springer Berlin Heidelberg (2012)

[10] Berlekamp, E., McEliece, R. and Van Tilborg, H.: On the inherent intractability of certain coding problems (Corresp.). IEEE Transactions on Information Theory, 24(3), pp.384-386 (1978)

[11] Bernstein, D.J.: Grover vs. mceliece. In International Workshop on Post-Quantum Cryptography (pp. 73-80). Springer, Berlin, Heidelberg. (2010)

[12] Bernstein, D.J., Lange, T. and Peters, C.: Attacking and defending the McEliece cryptosystem. In International Workshop on Post-Quantum Cryptography (pp. 31-46). Springer Berlin Heidelberg (2008)

[13] Bernstein, D.J., Lange, T. and Peters, C.: Smaller decoding exponents: ball-collision decoding. In Annual Cryptology Conference (pp. 743-760). Springer Berlin Heidelberg (2011)

[14] Berson, T.A.: Failure of the McEliece public-key cryptosystem under message-resend and related-message attack. In Annual International Cryptology Conference (pp. 213-220). Springer Berlin Heidelberg (1997)

[15] Biasi, F.P., Barreto, P.S., Misoczki, R. and Ruggiero, W.V.: Scaling efficient code-based cryptosystems for embedded platforms. Journal of Cryptographic Engineering, 4(2), pp.123-134. (2014)

[16] Biswas, B. and Sendrier, N.: McEliece cryptosystem implementation: Theory and practice. In International Workshop on Post-Quantum Cryptography (pp. 47-62). Springer Berlin Heidelberg (2008)

[17] BitPunch, https://github.com/FrUh/BitPunch

[18] Canteaut, A. and Sendrier, N.: Cryptanalysis of the original McEliece cryptosystem. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 187-199). Springer Berlin Heidelberg (1998)

[19] Chaulet, J. and Sendrier, N.: Worst case QC-MDPC decoder for McEliece cryptosystem. In Information Theory (ISIT), 2016 IEEE International Symposium on (pp. 1366-1370). IEEE. (2016)

[20] Chen, C., Eisenbarth, T., Von Maurich, I. and Steinwandt, R.: Differential power analysis of a McEliece cryptosystem. In International Conference on Applied Cryptography and Network Security (pp. 538-556). Springer, Cham. (2015)

[21] Chen, C., Eisenbarth, T., von Maurich, I. and Steinwandt, R.: Horizontal and vertical side channel analysis of a Mceliece cryptosystem. IEEE Transactions on Information Forensics and Security, 11(6), pp.1093-1105. (2016)

[22] Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D.: Report on post-quantum cryptography. National Institute of Standards and Technology (NIST), NISTIR 8105 Draft, U.S. Department of Commerce, February 2016. (2016)

[23] Chou, T.: QcBits: constant-time small-key code-based cryptography. In International Conference on Cryptographic Hardware and Embedded Systems (pp. 280-300). Springer Berlin Heidelberg. (2016)

[24] Fabšič, T., Hromada, V., Stankovski, P., Zajac, P., Guo, Q. and Johansson, T.: A Reaction Attack on the QC-LDPC McEliece Cryptosystem. In International Workshop on Post-Quantum Cryptography (pp. 51-68). Springer, Cham. (2017)

[25] Fabšič, T., Gallo, O. and Hromada, V.: Simple power analysis attack on the QC-LDPC McEliece cryptosystem. Tatra Mountains Mathematical Publications, 67(1), pp.85-92. (2016)

[26] Fabšič, T., Grošek, O., Nemoga, K. and Zajac, P.: On generating invertible circulant binary matrices with a prescribed number of ones. Cryptography and Communications, Jul 2017. (2017)

[27] Fujisaki, E. and Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In Annual International Cryptology Conference (pp. 537-554). Springer Berlin Heidelberg (1999)

[28] Gallager, R.: Low-density parity-check codes. IRE Transactions on information theory, 8(1), pp.21-28. (1962)

[29] Guo, Q. and Johansson, T.: A p-ary MDPC scheme. In Information Theory (ISIT), 2016 IEEE International Symposium on (pp. 1356-1360). IEEE. (2016)

[30] Guo, Q., Johansson, T. and Stankovski, P.: A key recovery attack on MDPC with CCA security using decoding errors. In Advances in Cryptology-ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22 (pp. 789-815). Springer Berlin Heidelberg (2016)

[31] Hall, C., Goldberg, I. and Schneier, B.: Reaction attacks against several public-key cryptosystem. In International Conference on Information and Communications Security (pp. 2-12). Springer Berlin Heidelberg (1999)

[32] Heyse, S., Moradi, A., and Paar, C.: Practical power analysis attacks on software implementations of McEliece. In: Sendrier, N. (eds.) Post-Quantum Cryptography, LNCS, vol. 6061, pp. 108-125. Springer International Publishing, (2010)

[33] Heyse, S., von Maurich, I. and Güneysu, T.: Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 273-292). Springer, Berlin, Heidelberg. (2013)

[34] Hill, R.: A first course in coding theory. Oxford University Press (1986)

[35] Jungnickel, D.: Finite Fields: Structure and Arithmetics, B.I. Wissenschaftsverlag, (1993)

[36] Kachigar, G. and Tillich, J.P.: Quantum information set decoding algorithms. In International Workshop on Post-Quantum Cryptography (pp. 69-89). Springer, Cham. (2017)

[37] Kobara, K. and Imai, H.: Countermeasure against reaction attacks. In The 2000 Symposium on Cryptography and Information Security: A12 (2000)

[38] Kobara, K. and Imai, H.: Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC. In International Workshop on Public Key Cryptography (pp. 19-35). Springer Berlin Heidelberg (2001)

[39] Lee, P.J. and Brickell, E.F.: An observation on the security of McEliece's public-key cryptosystem. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 275-280). Springer Berlin Heidelberg (1988)

[40] Li, Y.X., Deng, R.H. and Wang, X.M.: On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Transactions on Information Theory, 40(1), pp.271-273. (1994)

[41] Londahl, C., Johansson, T., Shooshtari, M. K., Ahmadian-Attari, M., Aref, M. R.: Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension. Designs, Codes and Cryptography, pp. 1-19. Springer US, (2015)

[42] von Maurich, I. and Güneysu, T.: Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable devices. In Proceedings of the conference on Design, Automation & Test in Europe (p. 38). European Design and Automation Association. (2014)

[43] von Maurich, I. and Güneysu, T.: Towards Side-Channel Resistant Implementations of QC-MDPC McEliece Encryption on Constrained Devices. PQCrypto, 2014, pp.266-282. (2014)

[44] von Maurich, I., Oder, T. and Güneysu, T.: Implementing QC-MDPC McEliece Encryption. ACM Transactions on Embedded Computing Systems (TECS), 14(3), p.44. (2015)

[45] von Maurich, I., Heberle, L. and Güneysu, T.: IND-CCA secure hybrid encryption from QC-MDPC niederreiter. In International Workshop on Post-Quantum Cryptography (pp. 1-17). Springer International Publishing. (2016)

[46] May, A., Meurer, A. and Thomae, E.: Decoding Random Linear Codes in $\tilde{\mathcal{O}}(2^{0.054n})$. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 107-124). Springer Berlin Heidelberg (2011)

[47] May, A. and Ozerov, I.: On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes. In EUROCRYPT (1) pp. 203-228. (2015)

[48] R.J. McEliece: A Public-Key Cryptosystem Based On Algebraic Coding Theory. Deep Space Network Progress Report, 44:114-116 (1978)

[49] Misoczki R., Tillich J-P., Sendrier N., Barreto P.S.L.M.: MDPC-McEliece: new McEliece variants from moderate density parity-check codes. In: IEEE International Symposium on Information Theory (ISIT 2013), pp. 2069-2073. Istanbul (2013)

[50] Monico, C., Rosenthal, J. and Shokrollahi, A.: Using low density parity check codes in the McEliece cryptosystem. In Information Theory, 2000. Proceedings. IEEE International Symposium on (p. 215). IEEE. (2000)

[51] Moree, P.: Artin's primitive root conjecture-a survey. Integers, 12(6), pp.1305-1416. (2012)

[52] Mosca, M.: Cybersecurity in an era with quantum computers: Will we be ready? Cryptology ePrint Archive, Report 2015/1075. (2015)

[53] Niebuhr, R., Meziani, M., Bulygin, S. and Buchmann, J.: Selecting parameters for secure McEliece-based cryptosystems. International Journal of Information Security, 11(3), pp.137-147. (2012)

[54] Niederreiter, H.: Knapsack-type cryptosystem based on algebraic coding theory. Problems of control and information theory, 15(2), pp.157-166. (1986)

[55] Otmani, A., Tillich, J.P., Dallot, L.: Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. In: Proc. First International Conference on Symbolic Computation and Cryptography (SCC 2008), Beijing, China (2008)

[56] Overbeck, R. and Sendrier, N.: Code-based cryptography. In Post-quantum cryptography (pp. 95-145). Springer Berlin Heidelberg. (2009)

[57] N. J. Patterson: The algebraic decoding of Goppa codes. Information Theory, IEEE Transactions on 21.2 (1975): 203-207, (1975)

[58] Persichetti, E.: Secure and anonymous hybrid encryption from coding theory. In International Workshop on Post-Quantum Cryptography (pp. 174-187). Springer, Berlin, Heidelberg. (2013)

[59] Pointcheval, D.: Chosen-ciphertext security for any one-way cryptosystem. In International Workshop on Public Key Cryptography (pp. 129-146). Springer Berlin Heidelberg (2000)

[60] Prange, E.: The use of information sets in decoding cyclic codes. IRE Transactions on Information Theory, 8(5), pp.5-9. (1962)

[61] Radford M. N.: Software for Low Density Parity Check (LDPC) codes, http://www.cs.utoronto.ca/~radford/ldpc.software.html

[62] Rossi, M., Hamburg, M., Hutter, M. and Marson, M.E.: A Side-Channel Assisted Cryptanalytic Attack Against QcBits. In Cryptology ePrint Archive, Report 2017/596. (2017)

[63] Ryan, W. and Lin, S.: Channel codes: classical and modern. Cambridge University Press. (2009)

[64] Repka, M. and Zajac, P.: Overview of the McEliece Cryptosystem and its Security. Tatra Mountains Mathematical Publications, 60(1), pp.57-83 (2014)

[65] Sendrier, N.: Decoding one out of many. in: Post-Quantum Cryptography, 4th Internat. Workshop-PQCrypto 2011, Taipei, Taiwan, 2011 (B.-Y. Yang, ed.), Lecture Notes in Comput. Sci., Vol. 7071, Springer, Berlin, 2011, pp. 51-67. (2011)

[66] Shooshtari, M.K., Ahmadian-Attari, M., Johansson, T. and Aref, M.R.: Cryptanalysis of McEliece cryptosystem variants based on quasi-cyclic low-density parity check codes. IET Information Security, 10(4), pp.194-202. (2016)

[67] Shor, P. W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), pp. 303-332 (1999)

[68] Sidelnikov, V.M. and Shestakov, S.O.: On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Mathematics and Applications, 2(4), pp.439-444. (1992)

[69] Stern, J.: A method for finding codewords of small weight. In: Wolfmann, J., Cohen, G. (eds.) Coding Theory 1988. LNCS, vol. 388, pp. 106-113. Springer, Heidelberg (1989)

[70] Sun, H.M.: Further cryptanalysis of the McEliece public-key cryptosystem. IEEE communications letters, 4(1), pp.18-19. (2000)

Part II

A Reaction Attack on the QC-LDPC McEliece Cryptosystem

A Reaction Attack on the QC-LDPC McEliece Cryptosystem[†]

Tomáš Fabšič[‡], Viliam Hromada[‡], Paul Stankovski[§], Pavol Zajac[‡], Qian Guo[§] and Thomas Johansson[§]

The paper is available at the following websites:

https://link.springer.com/chapter/10.1007/978-3-319-59879-6_4

and

https://eprint.iacr.org/2017/494

[†]Support by grant VEGA 1/0159/17 is acknowledged.

[‡]Slovak University of Technology in Bratislava, Faculty of Electrical Engineering and Information Technology, Ilkovičova 3, 81219 Bratislava, Slovak Republic

[§]Department of Electrical and Information Technology, Lund University, Lund, Sweden

Part III

Simple Power Analysis Attack on the QC-LDPC McEliece Cryptosystem

Simple Power Analysis Attack on the QC-LDPC McEliece Cryptosystem*

Tomáš Fabšič†, Ondrej Gallo†, Viliam Hromada†

The paper is available at the following website:

https://www.degruyter.com/downloadpdf/j/tmmp.2016.67.issue-1/tmmp-2016-0032/tmmp-2016-0032.pdf

*This work was supported by NATO's Public Diplomacy Division in the framework of "Science for Peace", Project MD.SFPP 984520.

†Slovak University of Technology in Bratislava, Faculty of Electrical Engineering and Information Technology, Ilkovičova 3, 81219 Bratislava, Slovak Republic

Part IV

On Generating Invertible Circulant Binary Matrices with a Prescribed Number of Ones

On Generating Invertible Circulant Binary Matrices with a Prescribed Number of Ones*

Tomáš Fabšič†, Otokar Grošek†, Karol Nemoga‡and Pavol Zajac†

The paper is available at the following website:

https://link.springer.com/article/10.1007/s12095-017-0239-4

*This work is a partial result of the Research and Development Operational Programme for the project International centre of excellence for research of intelligent and secure information-communication technologies and systems, ITMS 26240120039, co-funded by the ERDF.

†Slovak University of Technology in Bratislava, Faculty of Electrical Engineering and Information Technology, Ilkovičova 3, 81219 Bratislava, Slovak Republic

‡Slovak Academy of Sciences, Mathematical Institute, Štefánikova 49, 814 73 Bratislava, Slovak Republic