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

Mgr. Tomáš Fabšič

Dissertation Thesis Abstract

CONTRIBUTIONS TO THE ANALYSIS OF THE QC-LDPC MCELIECE CRYPTOSYSTEM

to obtain: the Academic Title
philosophiae doctor, PhD.

in the doctorate degree study programme: Applied Informatics
in the field of study: 9.2.9 Applied Informatics
Form of Study: full-time

Place and Date: Bratislava, 18. 8. 2017

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

Mgr. Tomáš Fabšič

Dissertation Thesis Abstract

CONTRIBUTIONS TO THE ANALYSIS OF THE QC-LDPC MCELIECE CRYPTOSYSTEM

to obtain: the Academic Title
philosophiae doctor, PhD.

in the doctorate degree study programme: Applied Informatics
in the field of study: 9.2.9 Applied Informatics
Form of Study: full-time

Place and Date: Bratislava, 18. 8. 2017

Dissertation Thesis has been prepared at: Institute of Computer Science and Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava.

Submitter: Mgr. Tomáš Fabšič
Faculty of Electrical Engineering and Information Technology
Slovak University of Technology in Bratislava
Ilkovičova 3, 812 19 Bratislava

Supervisor: prof. RNDr. Otokar Grošek, PhD.
Faculty of Electrical Engineering and Information Technology
Slovak University of Technology in Bratislava

Consultant: prof. RNDr. Peter Horák, DrSc.
University of Washington
Tacoma, WA, USA

Readers: prof. Rainer Steinwandt
Florida Atlantic University
Boca Raton, FL, USA

prof. RNDr. Štefan Porubský, DrSc.
Academy of Sciences of the Czech Republic

Dissertation Thesis Abstract was sent: .....
Dissertation Thesis Defence will be held on: ..... at .....

At: Faculty of Electrical Engineering and Information Technology,
Slovak University of Technology in Bratislava,
Ilkovičova 3, 812 19 Bratislava,
in room C502

prof. Dr. Ing. Miloš Oravec
Dean of the Faculty of Electrical Engineering and Information Technology,
Slovak University of Technology in Bratislava

Contents

1 Goals of the Thesis

In [20], 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 [17]. In 2016, the National Institute of Standards and Technology (NIST) issued an announcement recognizing this threat and calling for the standardization and transition to post-quantum public key cryptography in the near future [5].

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 [3], 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 [14]. 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 first variant employing QC-LDPC codes was presented by Baldi and Chiaraluce in [1]. However, in [18], it was discovered that an attack can be mounted on this cryptosystem, eventually recovering the private key. In response to this attack, Baldi, Bodrato and Chiaraluce presented in [2] an amended version of their cryptosystem from [1]. This amended version is immune against the attack in [18], and it is now known as the QC-LDPC McEliece cryptosystem. In 2013, a strongly related cryptosystem, the QC-MDPC McEliece cryptosystem, was published in [15]. Instead of QC-LDPC codes, the QC-MDPC McEliece cryptosystem uses codes with slightly denser parity-check matrix - quasi-cyclic moderate-density parity-check

(QC-MDPC) codes.

The thesis focuses on the QC-LDPC McEliece cryptosystem and the QC-MDPC McEliece cryptosystem. 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.

2 Our Contribution

The thesis is a compilation of three research papers [6, 7, 8]. In [6], we presented a reaction attack on the QC-LDPC McEliece cryptosystem. In [7], we presented a simple power analysis attack on the QC-LDPC McEliece cryptosystem. In [8], we presented algorithms for generating invertible circulant binary matrices with a prescribed number of ones, and we explained how these algorithms can be used in generating private keys in the QC-LDPC McEliece cryptosystem.

2.1 Reaction Attack on QC-LDPC McEliece

In [6], we presented a reaction attack on the QC-LDPC McEliece cryptosystem. The inspiration for this attack came from the work of Guo et al. [9], where a reaction attack on QC-MDPC McEliece was presented. The attack in [9] 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.

Instead of a bit-flipping algorithm, it is also possible to use a soft-decision decoding algorithm in the QC-MDPC McEliece cryptosystem. Guo et al. [9] conjectured that their attack is possible even when a soft-decision decoding algorithm is employed in the QC-MDPC McEliece cryptosystem.

Similarly as in [9], 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. However, 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 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). This allows Alice to estimate the probability of the decoding failure.

It is known that the McEliece cryptosystem in its basic form is vulnerable to a number of attacks, and that to avoid these attacks, the McEliece cryptosystem has to be used with a CCA2 conversion, such as Kobara-Imai γ conversion [12], for example. This is also true for the QC-LDPC McEliece cryptosystem and the QC-MDPC McEliece cryptosystem. Similarly as in [9], we showed that Alice can execute the attack even if she has no freedom to construct the messages sent to Bob. This implies that the attack is possible even when QC-LDPC McEliece is used with a CCA2 conversion.

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 [9] 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 [9], 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.

2.2 Power Analysis Attack on QC-LDPC McEliece

In [10], 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 [7], 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 [4], 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 [12], for example. We further observed that the same countermeasure as was proposed in [10] can be applied in QC-LDPC McEliece, as well.

As already noted in Section 2.1, the reaction attack from [6] 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 [6], 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 [6]), then a careful implementation might be needed to avoid the simple power analysis attack.

2.3 Generating Invertible Circulant Matrices with a Prescribed Number of Ones

As noted in Section 2.1, 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 [19]. 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 [2], 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 [8], we studied how to construct matrices S and Q when p is odd, which is the requirement to avoid the attack from [19]. We firstly studied how to construct invertible circulant binary matrices with a prescribed number of ones. In [13], 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 [11]. 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 [13], 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 [16].

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 information-set decoding 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 [13].

3 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] BitPunch, https://github.com/FrUh/BitPunch

[5] 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)

[6] 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)

[7] 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)

[8] 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)

[9] 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)

[10] 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)

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

[12] 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)

[13] 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)

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

[15] 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)

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

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

[18] 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)

[19] 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)

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

4 Publications

4.1 Papers Included in the Thesis

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)

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)

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)

4.2 Other Publications

Fabšič, T., Grošek, O., Nemoga, K. and Zajac, P.: On constructing invertible circulant binary $(n \times n)$-matrices with $n^2/2$ ones. In CECC 2015: Book of abstracts: 15th Central European conference on cryptology. Klagenfurt am Wörthersee, Austria. July 8-10, 2015. Alpen-Adria Universität Klagenfurt, pp. 10–12. (2015)

Fabšič, T., Gallo, O.: Acoustic cryptanalysis. In Grošek, O., Helleseth, T., Kholosha, A., Nemoga, K., Semaev, I., Zajac, P. (eds.): Norwegian-Slovakian Workshop in Crypto, Bergen, Norway. February 8 - 10, 2016. Bratislava : Slovak University of Technology, 2016, pp. 34–38. (2016)

Fabšič, T., Gallo, O., Hromada, V.: Simple power analysis of McEliece cryptosystem on STM32F4 and Altera cyclone. In Grošek, O., Helleseth, T., Kholosha, A., Nemoga, K., Semaev, I., Zajac, P. (eds.): Norwegian-Slovakian Workshop in

Crypto, Bergen, Norway. February 8 - 10, 2016. Bratislava : Slovak University of Technology, 2016, pp. 57–58. (2016)

Fabšič, T., Gallo, O., Hromada, V.: Demonstration of the Acoustic Cryptanalysis. In CryptArchi 2017: Proceedings: 15th International Workshop on Cryptographic Architectures Embedded in Logic Devices. Smolenice, Slovakia. June 18-21, 2017. Jean Monnet University in Saint-Etienne, pp. 11, 129–135. (2017)

5 Citations

Kindberg cites the paper *A Reaction Attack on the QC-LDPC McEliece Cryptosystem* in Kindberg, M.: A usability study of post-quantum algorithms, Master's Thesis, Lund University, 2017.

6 Conference and Seminar Talks

Event: Seminar CRYPTO, FEI STU, Bratislava
Year: 2014
Title of the Talk: Methods of Multivariate Statistical Analysis in Side-Channel Attacks

Event: Seminar CRYPTO, FEI STU, Bratislava
Year: 2014
Title of the Talk: Acoustic Cryptanalysis

Event: Seminar CRYPTO, FEI STU, Bratislava
Year: 2015
Title of the Talk: Planar Mappings

Event: 15th Central European conference on cryptology (CECC 2015), Klagenfurt, Austria
Year: 2015
Title of the Talk: On constructing invertible circulant binary $(n \times n)$-matrices with $n^2/2$ ones

Event: Seminar CRYPTO, FEI STU, Bratislava
Year: 2015

Title of the Talk: Circulant Matrices

Event: Norwegian-Slovakian Workshop in Crypto, Bergen, Norway
Year: 2016
Title of the Talk: Acoustic Cryptanalysis

Event: 16th Central European conference on cryptology (CECC 2016), Piešťany, Slovakia
Year: 2016
Title of the Talk: Tutorial on Acoustic Cryptanalysis (with Ondrej Gallo)

Event: ArcticCrypt 2016, Longyearbyen, Svalbard (Norway)
Year: 2016
Title of the Talk: On generating invertible circulant binary matrices with a prescribed number of ones

Event: CRYPTO Seminar, Worcester Polytechnic Institute, USA
Year: 2016
Title of the Talk: Acoustic Cryptanalysis

Event: PQCrypto 2017: The Eighth International Conference on Post-Quantum Cryptography, Utrecht, Netherlands
Year: 2017
Title of the Talk: A Reaction Attack on the QC-LDPC McEliece Cryptosystem

7 Participation in Research Projects

Name of the Project: NATO SfP 984520 Secure Implementation of Post-Quantum Cryptography
Project Director: prof. RNDr. Otokar Grošek, PhD.

Name of the Project: VEGA 1/0159/17 Secure Post-Quantum Cryptography
Project Director: doc. Ing. Pavol Zajac, PhD.

Name of the Project: SK06-IV-01-001 Cryptography Brings Security and Freedom
Project Director: prof. RNDr. Otokar Grošek, PhD.

Name of the Project: APVV-0586-11 Power Analysis Attacks on Digital Signa-

tures and Countermeasures
Project Directors: Ing. Michal Varchola, PhD., prof. RNDr. Otokar Grošek, PhD.

Name of the Project: VEGA 1/0173/13 Privacy on Mobile Devices
Project Director: doc. Ing. Pavol Zajac, PhD.

8 Súhrn (in Slovak)

Prezentovaná práca sa zaoberá QC-LDPC McEliece kryptosystémom a QC-MDPC McEliece kryptosystémom. Obidva kryptosystémy patria medzi kandidátov pre postkvantovú 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.