Improved LDPC and QC-LDPC McEliece variants

Rafael Misoczki[1] Jean-Pierre Tillich[1]
Nicolas Sendrier[1] Paulo Barreto[2]

[1]Project SECRET, INRIA-Rocquencourt
Rocquencourt, France
[2]Escola Politécnica, University of São Paulo
São Paulo, Brazil

May 9, 2012
Lyngby, Denmark
Code-based Cryptography Workshop 2012

Outline

LDPC and Quasi-cyclic codes

Previous LDPC/QC-LDPC McEliece variants

Improved LDPC/QC-LDPC McEliece variants

Security assessment

Benefits

Conclusion

LDPC and Quasi-cyclic codes

A low-density parity-check code is a linear code which admits a sparse parity-check matrix.

- Error correction capability depends on sparsity of H
- Low complexity for decoding
- There is no known distinguisher

A quasi-cyclic code is a linear code composed by n_0 cyclic blocks such that any cyclic shift of a codeword by n_0 positions is also a codeword.

- Compact representation
- Efficient processing (isomorphic to the algebra of polynomials modulo $x^p - 1$)

QC-LDPC codes

Parameters:

- $r = r_0 p$
- $n = n_0 p$
- $k = k_0 p$

We are interested in: $r_0 = 1$:

$$H = [H_0 | H_1 | \ldots | H_{n_0 - 1}]$$

H_i: $p \times p$ circulant matrix with low row/column weight d_v:

$$H_i = \begin{bmatrix} h_0 & h_1 & h_2 & \ldots & h_{p-1} \\ h_{p-1} & h_0 & h_1 & \ldots & h_{p-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & h_3 & \ldots & h_0 \end{bmatrix}$$

Previous LDPC/QC-LDPC McEliece variants

Proposals with security flaws in red:

- [MRS00]: LDPC codes
- [BCG06], [BCGM07], [BC07], (BBC08): QC-LDPC codes

Private Key:

$$(S, H, Q)$$

Public Key:

$$G' = S^{-1} \cdot G \cdot Q^{-1}$$

H: $r \times n$ sparse parity-check matrix with low column weight d_v
S: $k \times k$ dense circulant matrix
Q: $n \times n$ sparse circulant matrix with row/column weight m

Encryption:

$$x = u \cdot G' + e$$
$$wt(e) \leq t'$$

Decryption:

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

Decode $t = mt'$ errors in x'.

Previous LDPC/QC-LDPC McEliece variants

Private parity-check matrix H with **very low weight** d_v:

- Attacks on the dual of the public code through low weight codeword finding algorithms.

Usage of **transformation matrices** in order to increase the codeword weight of the dual of the public code:

- Attacks on the constrained structure of such transformation matrices.

Improved LDPC/QC-LDPC McEliece variants

Our approach:

1. Remove the transformation matrices:
    - Reduces the venues for mounting structural attacks
2. Increase the weight d_v:
    - High enough to avoid low weight codeword attacks on the dual code
    - Low enough to allow LDPC decoding for a secure amount of errors

Improved LDPC/QC-LDPC McEliece variants

Key generation

1. Select a (QC-)LDPC code: a $r \times n$ parity-check matrix H
2. Compute its $k \times n$ generator matrix G in systematic form

Private key: H Public key: G

Encryption

1. Select a vector e of length n and weight t
2. Compute $x = m \cdot G + e$

Decryption

1. Using H, decode $x = m \cdot G + e$ to obtain mG
2. Extract the plaintext from the first k indices of mG

Security assessment

- Security reduction
- Practical security

Security reduction

In [Sen09], a security reduction for Niederreiter cryptosystem:

Can be solved on average		Can be broken?
1. Distinguishing problem 2. Decoding problem	$\Leftarrow$	McEliece/Niederreiter cryptosystems

Distinguishing problem:

- Recently addressed for high rate Goppa codes. [FOPT10]

Security reduction

The same approach can be applied to our proposal:

Decoding problem

- Solved through low weight codeword finding

Distinguishing problem

- Sought structure: sparsity
- Solved through low weight codeword finding

But now both problems converge to low weight codeword finding!

Practical security

Two kinds of attacks:

- Decoding attacks: can be solved through low weight codeword finding algorithms
- Key-recovering attacks: for LDPC codes, can be solved through low weight codeword finding algorithms

The best algorithms: variants of Information Set Decoding technique, in special, the iterative algorithm [Ste89][1].

[1] Improvements in [BLP08], [FS09], [BLP11].

Practical security

Low weight codeword finding:

- Decoding One Out of Many (DOOM) [Sen11]: The work factor is sensitively reduced when the attacker possesses multiple instances of the decoding problem and wants to solve only one of them
- Is the most threatening for our proposal: there exist at least r low weight codewords on the dual of the public code

Practical security

DOOM:

It gains a factor of $N_s/\sqrt{N_i}$, in comparison with general information set decoding techniques

- N_i: Number of available instances of the decoding problem
- N_s: Number of solutions of these instances

Example: $N_i = N_s = N$:

$$WF_{doom} = \frac{WF_{isd}}{N_s/\sqrt{N_i}} = \frac{WF_{isd}}{\sqrt{N}}$$

Practical security

Key-recovering attacks

- N_i: 1 (corresponding to the syndrome zero)
- N_s: r

LDPC case: There is no gain

- The attacker must find r low weight codewords

$$WF_{doom} = \frac{WF_{isd}}{r/\sqrt{1}} \cdot r = WF_{isd}$$

QC-LDPC case: There is a gain

- Only one low weight codeword is enough to define the code

$$WF_{doom} = \frac{WF_{isd}}{r}$$

Practical security

Decoding attacks

LDPC case: There is no gain

QC-LDPC case: There is the usual gain of DOOM

- $N_i = N_s = r$ (all possible cyclic shifts of the syndrome)

$$WF_{doom} = \frac{WF_{isd}}{r/\sqrt{r}} \cdot r = \frac{WF_{isd}}{\sqrt{r}}$$

A taste of the QC-LDPC parameters...

Security	n_0	n	k	d_v	t	pub. key	syndrome
80	2	9200	4600	45	84	4600	4600
128	2	16384	8192	63	115	8192	8192
256	2	120000	60000	189	367	60000	60000

Public key and syndrome sizes in bits

Benefits

Security reduction converges to only one problem:

- Low weight codeword finding

Removing the transformation matrices:

- Reduce the private key size
- Improve the efficiency of decryption step

QC-LDPC variant:

- Very compact public-keys

LDPC variant:

- Further reduces the ways for structural attacks

Conclusion

LDPC codes seem to be very useful for cryptography purposes:

- Less structured than Goppa codes
- Quite close from random linear codes
- Quasi-cyclicity can be successfully applied in order to obtain very small public keys

Future works:

- Applicability to other cryptographic primitives
- Implementation issues
- ...

Questions?

Thanks for your attention!

rafael.misoczki@inria.fr

References

BBC08 M. Baldi, M. Bodrato, and F. Chiaraluce. A new analysis of the mceliece cryptosystem based on qc-ldpc codes. In Proceedings of the 6th interna- tional conference on Security and Cryptography for Networks, SCN 08, pages 246262. Springer-Verlag, Berlin, Heidelberg, 2008. ISBN 978-3-540- 85854-6. doi:http://dx.doi.org/10.1007/978-3-540-85855-3 17.

BC07 M. Baldi and F. Chiaraluce. Cryptanalysis of a new instance of mceliece cryptosystem based on qc-ldpc codes. In Information Theory, 2007. ISIT 2007. IEEE International Symposium on, pages 2591 2595. june 2007. doi:10.1109/ISIT.2007.4557609.

BCG06 M. Baldi, F. Chiaraluce, and R. Garello. On the usage of quasi-cyclic low- density parity-check codes in the mceliece cryptosystem. In Proceedings of the First International Conference on Communication and Electronics (ICEE06), pages 305310. October 2006.

BCGM07 M. Baldi, F. Chiaraluce, R. Garello, and F. Mininni. Quasi-cyclic low- density parity-check codes in the mceliece cryptosystem. In Communica- tions, 2007. ICC 07. IEEE International Conference on, pages 951 956. june 2007. doi:10.1109/ICC.2007.161.

BLP08 D. J. Bernstein, T. Lange, and C. Peters. Attacking and defending the mceliece cryptosystem. In Proceedings of the 2nd International Workshop on Post-Quantum Cryptography, PQCrypto 08, pages 3146. Springer- Verlag, Berlin, Heidelberg, 2008. ISBN 978-3-540-88402-6. doi:10.1007/ 978-3-540-88403-3 3.

BLP11 D. Bernstein, T. Lange, and C. Peters. Smaller decoding exponents: Ball-collision decoding. In P. Rogaway, editor, Advances in Cryptology CRYPTO 2011, volume 6841 of Lecture Notes in Computer Science, pages 743760. Springer Berlin / Heidelberg, 2011. ISBN 978-3-642-22791-2. 10.1007/978-3-642-22792-942.

CC98 A. Canteaut and F. Chabaud. A new algorithm for finding minimum- weight words in a linear code: application to mcelieces cryptosystem and to narrow-sense bch codes of length 511. Information Theory, IEEE Transac- tions on, 44(1):367 378, jan 1998. ISSN 0018-9448. doi:10.1109/18.651067.

FOPT10 J.-C. Faugére, A. Otmani, L. Perret, and J.-P. Tillich. A distinguisher for high rate mceliece cryptosystems. Yet Another Conference on Cryptography (YACC'10), 2010, Porquerolles Island, France.

MRS00 C. Monico, J. Rosenthal, and A. Shokrollahi. Using low density parity check codes in the mceliece cryptosystem. In Information Theory, 2000. Proceedings. IEEE International Symposium on, page 215. 2000. doi:10. 1109/ISIT.2000.866513.

Sen09 N. Sendrier. On the use of structured codes in code based cryptography. In S. Nikova, B. Preneel, and L. Storme, editors, Coding Theory and Cryp- tography III, Contactforum, pages 5968. Koninklijke Vlaamse Academie van Belgi voor Wetenschaeppen en Kunsten, 2009.

Sen11 N. Sendrier. Decoding one out of many. In B.-Y. Yang, editor, Post- Quantum Cryptography, volume 7071 of Lecture Notes in Computer Sci- ence, pages 5167. Springer Berlin / Heidelberg, 2011. ISBN 978-3-642- 25404-8. 10.1007/978-3-642-25405-5-4.

Ste89 J. Stern. A method for finding codewords of small weight. In G. Cohen and J. Wolfmann, editors, Coding Theory and Applications, volume 388 of Lecture Notes in Computer Science, pages 106113. Springer, 1989.