MDPC-McEliece: New McEliece Variants From Moderate Density Parity-Check Codes

Rafael Misoczki[1] and Jean-Pierre Tillich[1] and Nicolas Sendrier[1] and Paulo S. L. M. Barreto[2]

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

Recently, several variants of the McEliece cryptosystem [1] based on low-density parity-check (LDPC) codes have been proposed [2–6]. When combined with quasi-cyclic structure, these proposals provide very small key sizes. LDPC codes are characterized by the existence of low weight dual codewords, used to perform an efficient iterative decoding. In order to avoid attacks aimed at recovering such codewords, these last proposals have suggested to replace the permutation matrix used in the original McEliece cryptosystem by an $n \times n$ matrix Q of small constant row and column weight m, in order to increase the dual codeword weight. In summary, the last QC-LDPC proposal [6] can be described as follows. Let H be an $r \times n$ sparse parity-check matrix of an (n, r, w)-LDPC code $\mathcal{C}$ of length n, codimension r, dimension $k = n - r$ and row weight w able to correct t errors using LDPC decoding techniques, S be a $k \times k$ invertible matrix and Q be as described above. The private key is the triple (S, H, Q) and the public key is the $k \times n$ matrix $G' = S^{-1}\ G\ Q^{-1}$, where G is a generator matrix of $\mathcal{C}$. All matrices are block-circulant. The encryption process for a message m of length k is: $x = m\ G' + e$, where e is an error vector randomly chosen of length n and weight t. The decryption process starts with: $x' = x\ Q = m\ S^{-1}\ G + \mathbf{e}\ \mathbf{Q}$, followed by the correction of mt errors in x' and finally by the computation of m from a right multiplication by S. The crucial step during the decryption refers to the product eQ, where the number of errors is increased by a factor of m. Therefore the private code must be able to correct up to mt errors. Our proposal comes from two simple but not trivial observations over this cryptosystem.

1. The private code has an error correction capability very close to mt, whilst the public code has an error correction capability much higher than t.
2. When increasing t by λ errors, this aforementioned scheme must provide a private code able to correct $m\lambda$ more errors, due to the propagation of the errors performed by the matrix Q.

These two facts imply that we have much more freedom to increase t (the number of errors added during the encryption process) using a code with higher density, as exemplified through the public code of this scheme, than the aforementioned variant. To be more precise, this moderate density must be high enough to avoid key recovery attacks, while still allows decoding for a secure amount of errors. In this sense, we introduce the moderate density parity-check codes (MPDC, for short) which respect all of these constraints, resulting in a better decoding process and allowing the private and public codes being permutation equivalent. Therefore we present two new McEliece variants: one using MDPC codes and other employing quasi-cyclic MDPC codes. The private key is the code representation which allows for efficient decoding (i.e, the sparse parity-check matrix) and the public key is simply the dense generation matrix of the code. The encryption and decryption is as usual for the original McEliece cryptosystem.

One of the main benefits of our work refers to its security reduction. Basically, the security of the McEliece cryptosystem is based on two assumptions: the pseudo-randomness of the employed code family and the hardness of decoding a generic linear code. It is namely proved in [7] and further discussed in [8] that if an attacker is not able to distinguish the underlying code from a random code, then he is challenged to decode a generic linear code, a problem proved to be NP-complete [9]. The pseudo-randomness, in fact the key security, is often the weak spot even for Goppa codes. In [10] a distinguisher for high rate Goppa codes is presented. However, regarding our proposal, it is quite natural to consider that the only way of distinguishing MDPC codes from random codes is by being able to find dual codewords of moderate weight (these are precisely the rows of the secret parity-check matrix used in the decoding process). If we make such an hypothesis, since algorithms for decoding a random linear code and finding low weight codewords are basically of the same nature and complexity, both key and message security of our scheme

boil down to the same coding-theory problem: low weight codeword finding. This provides a strong argument in favor of the security of this new scheme.

Regarding its practical security, we used the variants of the information set decoding (ISD) technique for the parameters selection. We also take into account the estimations provided in [11], when multiple instances and solutions of the syndrome decoding problem are available (this is exactly what happens for MDPC codes), reducing then the workfactor for ISD. As practical results, using the quasi-cyclic structure, we succeed to achieve extremely small public keys: for 80-bits of security our public key has only 4800 bits. Regarding the MDPC variant, the absence of structure further reduces the ways for structural attacks in the price of huge public keys.

References

1. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report **44** (1978) 114–116
2. Monico, C., Rosenthal, J., Shokrollahi, A.: Using low density parity check codes in the McEliece cryptosystem. In: IEEE International Symposium on Information Theory – ISIT'2000, Sorrento, Italy, IEEE (2000) 215
3. Baldi, M., Chiaraluce, F., Garello, R.: 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 (ICEE'06). (2006) 305–310
4. Baldi, M., Chiaraluce, F., Garello, R., Mininni, F.: Quasi-cyclic low-density parity-check codes in the McEliece cryptosystem. In: Communications, 2007. ICC '07. IEEE International Conference on. (2007) 951 –956
5. Baldi, M., Chiaraluce, F.: Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. In: Information Theory, 2007. ISIT 2007. IEEE International Symposium on. (2007) 2591 –2595
6. Baldi, M., Bodrato, M., Chiaraluce, F.: A new analysis of the McEliece cryptosystem based on QC-LDPC codes. In: Proceedings of the 6th international conference on Security and Cryptography for Networks. SCN '08, Berlin, Heidelberg, Springer-Verlag (2008) 246–262
7. Courtois, N., Finiasz, M., Sendrier, N.: How to achieve a McEliece-based digital signature scheme. In: Advances in Cryptology – Asiacrypt'2001. Volume 2248 of Lecture Notes in Computer Science., Gold Coast, Australia, Springer (2001) 157–174
8. Sendrier, N.: On the use of structured codes in code based cryptography. In Nikova, S., Preneel, B., Storme, L., eds.: Coding Theory and Cryptography III. Contactforum. Koninklijke Vlaamse Academie van België voor Wetenschaeppen en Kunsten (2009) 59–68
9. Berlekamp, E., McEliece, R., van Tilborg, H.: On the inherent intractability of certain coding problems (corresp.). Information Theory, IEEE Transactions on **24**(3) (1978) 384 – 386
10. Faugère, J.C., Gauthier, V., Otmani, A., Perret, L., Tillich, J.P.: A distinguisher for high rate McEliece cryptosystems. In: ITW 2011, Paraty, Brazil (2011) 282–286
11. Sendrier, N.: Decoding one out of many. In Yang, B.Y., ed.: Post-Quantum Cryptography. Volume 7071 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg (2011) 51–67 10.1007/978-3-642-25405-5-4.