Classic McEliece: conservative code-based cryptography

23 October 2022

Principal submitter

This submission is from the following team, listed in alphabetical order:

- Martin R. Albrecht, Information Security Group, Royal Holloway, University of London
- Daniel J. Bernstein, University of Illinois at Chicago and Ruhr University Bochum
- Tung Chou, Academia Sinica
- Carlos Cid, Simula UiB and Okinawa Institute of Science and Technology
- Jan Gilcher, ETH Zürich
- Tanja Lange, Eindhoven University of Technology
- Varun Maram, ETH Zürich
- Ingo von Maurich, self
- Rafael Misoczki, Google
- Ruben Niederhagen, Academia Sinica and University of Southern Denmark
- Kenneth G. Paterson, ETH Zürich
- Edoardo Persichetti, Florida Atlantic University
- Christiane Peters, self
- Peter Schwabe, Max Planck Institute for Security and Privacy & Radboud University
- Nicolas Sendrier, Inria
- Jakub Szefer, Yale University
- Cen Jung Tjhai, PQ Solutions Ltd.
- Martin Tomlinson, PQ Solutions Ltd. and University of Plymouth
- Wen Wang, Yale University

E-mail address (preferred): `authorcontact-mceliece-merged@box.cr.yp.to`

Telephone (if absolutely necessary): +1-312-996-3422. Postal address (if absolutely necessary): Daniel J. Bernstein, Department of Computer Science, University of Illinois at Chicago, 851 S. Morgan (M/C 152), Room 1120 SEO, Chicago, IL 60607–7053.

Auxiliary submitters: There are no auxiliary submitters. The principal submitter is the team listed above.

Inventors/developers: The inventors/developers of this submission are the same as the principal submitter. Relevant prior work is credited where appropriate.

Owner: Same as submitter.

Signature: ×. See also printed version of "Statement by Each Submitter".

Document generated with the help of `pqskeleton` version 20190309.

Contents

1 Introduction

The first code-based public-key cryptosystem was introduced in 1978 by McEliece [4]. The public key specifies a random binary Goppa code. A ciphertext is a codeword plus random errors. The private key allows efficient decoding: extracting the codeword from the ciphertext, identifying and removing the errors.

The McEliece system was designed to be one-way (OW-CPA), meaning that an attacker cannot efficiently find the codeword from a ciphertext and public key, when the codeword is chosen randomly. The security level of the McEliece system has remained remarkably stable, despite dozens of attack papers over 40 years. The original McEliece parameters were designed for only 2^{64} security, but the system easily scales up to “overkill” parameters that provide ample security margin against advances in computer technology, including quantum computers.

The McEliece system has prompted a tremendous amount of followup work. Some of this work improves efficiency while clearly preserving security:[1] this includes a “dual” PKE proposed by Niederreiter [5], software speedups such as [1], and hardware speedups such as [3].

Furthermore, it is now well known how to efficiently convert an OW-CPA PKE into a KEM that is IND-CCA2 secure against all ROM attacks. This conversion is tight, preserving the security level, under two assumptions that are satisfied by the McEliece PKE: first, the PKE is deterministic (i.e., decryption recovers all randomness that was used); second, the PKE has no decryption failures for valid ciphertexts. Even better, recent work [2] achieves similar tightness for a broader class of attacks, namely QROM attacks. The risk that a hash-function-specific attack could be faster than a ROM or QROM attack is addressed by the standard practice of selecting a well-studied, high-security, “unstructured” hash function.

This submission *Classic McEliece* (CM) brings all of this together. It presents a KEM designed for IND-CCA2 security at a very high security level, even against quantum computers. The KEM is built conservatively from a PKE designed for OW-CPA security, namely Niederreiter’s dual version of McEliece’s PKE using binary Goppa codes. Every level of the construction is designed so that future cryptographic auditors can be confident in the long-term security of post-quantum public-key encryption.

2 General algorithm specification (part of 2.B.1)

See the separate “cryptosystem specification” document.

[1] Other work includes McEliece variants whose security has not been studied as thoroughly. For example, many proposals replace binary Goppa codes with other families of codes, and lattice-based cryptography replaces “codeword plus random errors” with “lattice point plus random errors”. Code-based cryptography and lattice-based cryptography are two of the main types of candidates identified in NIST’s call for Post-Quantum Cryptography Standardization. This submission focuses on the classic McEliece system precisely because of how thoroughly it has been studied.

3 List of parameter sets (part of 2.B.1)

See the separate "cryptosystem specification" document.

4 Design rationale (part of 2.B.1)

See the separate "design rationale" document.

5 Detailed performance analysis (2.B.2)

See the separate "guide for implementors" document.

6 Expected strength (2.B.4) in general

See the separate "guide for security reviewers" document.

7 Expected strength (2.B.4) for each parameter set

See the separate "guide for security reviewers" document.

8 Analysis of known attacks (2.B.5)

See the separate "guide for security reviewers" document.

9 Advantages and limitations (2.B.6)

See the separate "design rationale" document.

References

[1] Daniel J. Bernstein, Tung Chou, and Peter Schwabe. McBits: Fast constant-time code-based cryptography. In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems—CHES 2013—15th International Workshop, Santa*

Barbara, CA, USA, August 20-23, 2013. Proceedings, volume 8086 of *Lecture Notes in Computer Science*, pages 250–272. Springer, 2013. https://tungchou.github.io/papers/mcbits.pdf.

[2] Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti. Tighter proofs of CCA security in the quantum random oracle model. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography—17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part II*, volume 11892 of *Lecture Notes in Computer Science*, pages 61–90. Springer, 2019. https://eprint.iacr.org/2019/590.

[3] Po-Jen Chen, Tung Chou, Sanjay Deshpande, Norman Lahr, Ruben Niederhagen, Jakub Szefer, and Wen Wang. Complete and improved FPGA implementation of Classic McEliece. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2022(3):71–113, 2022. https://doi.org/10.46586/tches.v2022.i3.71-113.

[4] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical report, NASA, 1978. https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

[5] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.