draft-josefsson-mceliece-03

Classic McEliece @ CFRG IETF123

Simon Josefsson <simon@josefsson.org>

The Problem

- We have a security problem right now with attackers recording RSA/ECC ciphertexts to decrypt with future quantum computers. Post-quantum KEMs are trying to solve this, but which KEMs should CFRG endorse?

Limiting attention to NIST's KEMs adds security risks

- Cryptanalysis has broken many KEMs already, so short lists are worrisome. HQC had a flaw announced after NIST selected it this year. Lattice attacks are continuing to get better (e.g., a paper to appear at Crypto 2025 says Kyber-768 is 11.9 bits below NIST's required security level). Including McEliece in CFRG's portfolio is attractive since McEliece has the strongest security track record of all available options.

Moving targets add security risks

- Classic McEliece has never needed a security patch. Its exact security level was studied in, e.g., https://eprint.iacr.org/2021/1634 at Eurocrypt 2022 and https://eprint.iacr.org/2023/940 at Crypto 2024. It has a tight proof of QROM IND-CCA2 security assuming purely the one-wayness of the original McEliece system studied in many more papers.

Will anyone use it? See mceliece.org

- Adva Network Security: "Our real-world use-case ... Encrypted layer 1 optical transport solutions (OTNsec) wi
- Arch Linux integration of libmceliece into AUR (starting 2024)
- bench.cr.yp.to: benchmarks of software for many cryptosystems including Classic McEliece
- Botan software library (C++): many cryptosystems including Classic McEliece (starting with Botan 3.7.0 in 202
- Bouncy Castle software library (Java, C#): many cryptosystems including Classic McEliece
- BSI recommendations: two cryptosystems, including Classic McEliece (`mceliece460896` and larger), are "cry "at BSI, we support international standardization of ... Classic McEliece" (2022); "cryptographically suitable to information" (2024)
- classic-mceliece-rust software library: pure Rust implementation of Classic McEliece
- Crypto4A: "Crypto4A currently uses Classic McEliece in all of its HSMs for three important use cases"
- Debian integration of libmceliece (starting 2023; scheduled for release in 2025 in Debian 13)
- Ericsson: "We strongly think NIST should standardize Classic McEliece, which has properties that makes it the
- libgcrypt software library: starting with 1.11.0 (2024), includes gcrypt-mceliece patches to support Classic Mc
- libmcleece: file-encryption software using Classic McEliece
- liboqs software library: various cryptosystems including Classic McEliece
- mceliece-arm-m4: speed-optimized Classic McEliece software for ARM Cortex-M4
- McEliece attack challenges (started in 2019, ongoing)
- McOutsourcing: space-optimized Classic McEliece software for ARM Cortex-M4
- McTiny: fast Classic McEliece key erasure for tiny network servers
- Mullvad VPN software: 2022 announcement of Classic McEliece experiment on some servers, 2022 announce
- ncsc.nl recommendation (2022) of three cryptosystems, including Classic McEliece
- node-mceliece-nist software library: Node.js bindings for Classic McEliece
- Nym mixnet: "We are also putting Classic McEliece into production in Nym" (2025)
- openssh-mceliece: how to patch OpenSSH to support Classic McEliece (`mceliece6688128`)
- pqc-classic-mceliece: FPGA implementation of Classic McEliece
- PQClean repository: various cryptosystems including Classic McEliece

The Draft

- Based on public ISO 20230419 contribution
- F and non-F variant naming need some awareness – maps to implementation names but not application protocol names
- Recommends use with Chempat hybrid combiner
- HPKE integration to be added in separate draft
- Ready to be published as a stable reference for Internet applications that use this conservative algorithm

public key	private key	ciphertext	session key	
261120	6492	96	32	mceliece348864
524160	13608	156	32	mceliece460896
1044992	13932	208	32	mceliece6688128
1047319	13948	194	32	mceliece6960119
1357824	14120	208	32	mceliece8192128

Credits

- Classic McEliece Team:
  - 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, SandboxAQ
  - Ingo von Maurich, self
  - Rafael Misoczki, Google
  - Edoardo Persichetti, Florida Atlantic University
  - Christiane Peters, self
  - 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
  -