From: D. J. Bernstein <djb@cr.yp.to>
Sent: Monday, May 28, 2018 10:50 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Classic McEliece
Attachments: signature.asc

Edoardo Persichetti and I have a new paper "Towards KEM Unification"
available here:

https://cr.yp.to/papers/tightkem-20180528.pdf

This paper presents a complete tight ROM IND-CCA2 security proof for the "RandomizeSessionKeys"/"SimpleKEM" conversion used in Classic McEliece, assuming nothing beyond OW-CPA security for the underlying PKE. To support auditing, the proof is factored into simpler theorems via a new notion of ROM "IND-Hash" security, and the proof of each theorem is spelled out in full detail.

As an illustration of the importance of auditing, the paper presents counterexamples to HHK Theorem 3.6 and HHK Theorem 3.5.

Classic McEliece has a second layer of defense: before it applies SimpleKEM, it uses Dent's idea of adding a confirmation hash to the PKE.
The submission stated an expectation that this dual-defense system would allow a tight ROM security proof, and outlined a way to modify Dent's proof to achieve this. The new paper shows in full detail that SimpleKEM has a tight ROM security proof even _without_ this second layer of defense. This immediately implies a tight ROM security proof for the dual-defense system, since ROM confirmation tightly preserves OW-CPA.

This paper is also progress towards a tight QROM proof. The Classic McEliece submission stated an expectation that the tight SXY proof of "PR-CPA => QROM IND-CCA2" would apply to SimpleKEM, with the caveat that PR-CPA could be easier to break than OW-CPA. SXY subsequently replaced PR-CPA with DS (ciphertext unrecognizability), which does not eliminate this caveat but does reduce it. We now expect the SXY proof to factor as tight "DS => QROM IND-Hash" composed with tight "QROM IND-Hash => QROM IND-CCA2", where the second part is proven in the same way as our "ROM IND-Hash => ROM IND-CCA2" theorem. QROM IND-Hash is even closer to OW-CPA than DS is, so our expected tight "QROM IND-Hash => QROM IND-CCA2" will further reduce the caveat.

Our theorems are stated in the same level of generality as Dent's Theorem 8: we start from any correct deterministic PKE. Other NIST submissions that start from correct deterministic PKEs (e.g., any other submissions applying Dent's Theorem 8) can switch to SimpleKEM (or the variants of SimpleKEM discussed in the paper, such as the dual-defense system in Classic McEliece) and can then apply the same theorems.

Submissions with probabilistic PKEs can derandomize the PKEs and then apply the same theorems. Derandomization does not tightly preserve OW-CPA, but OW-CPA can be plausibly assumed after derandomization. Proof strategies that instead start from IND-CPA appear to be compatible with the same KEMs.

PKEs that are only partially correct (i.e., that have decryption
failures) can also be converted to KEMs in the same ways, but our security analysis does not include this case. As an alternative that is easier to audit, most of those submissions can easily tweak parameters to eliminate decryption failures without much loss of performance.

---Dan

From: D. J. Bernstein <djb@cr.yp.to>
Sent: Thursday, June 28, 2018 10:32 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Classic McEliece
Attachments: signature.asc

The Classic McEliece team has posted a document "Classic McEliece vs. NTS-KEM" available here:

https://classic.mceliece.org/nist/vsntskem-20180629.pdf

---Dan

From: KennyPaterson@gmail.com
Sent: Monday, October 01, 2018 1:06 PM
To: pqc-forum
Cc: pqc-comments; djb@cr.yp.to; Carlos.Cid@rhul.ac.uk; Martin.Albrecht@rhul.ac.uk; cjt@post-quantum.com; kenny.paterson@rhul.ac.uk; mt@post-quantum.com
Subject: Re: OFFICIAL COMMENT: Classic McEliece

We are grateful to the "Classic McEliece Comparison Task Force" for their report comparing NTS-KEM and Classic McEliece.

Our response to the report is as follows:

Chapter 2 (ciphertext size): we agree that the two schemes have identical ciphertext sizes. The NTS-KEM official submission is of course definitive in comparison to any talk the authors of the document may have heard.

Chapter 3 (ciphertext details): here the report essentially reiterates details that can be found in the first step of our security proof for NTS-KEM, see Appendix E of the NTS-KEM submission. We don't agree that our specification is any more complex than that of Classic McEliece.

Chapter 4 (patent status): the patent status of NTS-KEM and Classic McEliece are identical. The status of GB2532242 ("Public Key Cryptosystem using Error Correcting Codes") at the UK patent office is abandoned. The status of US20150163060 ("Methods, systems and apparatus for public key encryption using error correcting codes") at the US patent office is also abandoned. There are no other patents filed that cover NTS-KEM and this has been confirmed by both US and UK patent offices.

Chapter 5 (chosen-ciphertext attacks): both schemes have tight proofs in the ROM. The NTS-KEM proof was included in the original submission to NIST, while the one for Classic McEliece only became available post-submission, in IACR eprint 2018/526. In the light of QROM proof techniques that have emerged after the submission deadline, adopting implicit rejection might be a good idea. We will consider making a tweak to NTS-KEM to this effect.

Chapter 6 (systematic form): here, the report seems to be mostly concerned about key generation. We agree that "abort-and-repeat" may be more appropriate as a key generation strategy than NTS-KEM's non-constant-time approach in some applications. But we would point out that there are other applications where the performance gain of NTS-KEM's approach is warranted.

Chapter 7 (permutation security): the "Classic McEliece Comparison Task Force" can be assured that our security analysis assumes a non-malicious permutation update procedure during key generation.

Chapter 8 (compressed secret keys): being able to store only a short seed from which private keys can be regenerated could be a useful feature. We agree that in this case the pivoting strategy needs to be specified to avoid the requirement of storing column permutations.

Chapter 9 (polynomials): this chapter speculates about possible security gains and losses from NTS-KEM adopting square-free polynomials as opposed to irreducible polynomials as used in Classic McEliece. We find it interesting but inconclusive either way.

Chapter 10 (public keys): The report points out that NTS-KEM keys are 4 bytes larger than Classic McEliece keys in the specification, and also that those extra 4 bytes are not treated consistently in the NTS-KEM submission. We will of course address the second issue, but would also point out that the minimum key size in the different proposed NTS-KEM instantiations is more than 300Kbytes, so arguing about 4 bytes seems petty.

Chapter 11 (allowing reduced n): as we discuss in the NTS-KEM submission, we believe that fixing n = 2^m gives a good trade-off between security, simplicity of implementation and flexibility of parameter choices. We are aware that this is a subjective issue, as too surely are the members of the "Classic McEliece Comparison Task Force".

Chapter 12 (specific parameter sets): we agree that NTS-KEM targets security levels 1, 3 and 5 while Classic McEliece is more restricted in only targeting level 5.

Chapter 13 (miscellaneous sloppiness): we thank the "Classic McEliece Comparison Task Force" for the two comments in this section.

Chapter 14 (current software): we agree that constant-time software is what should eventually be targeted. We don't agree that Classic McEliece having such software now is a "major advantage". The NIST process will run for some years, and if NTS-KEM advances further in the process, then constant-time software for it will be produced.

A closing remark on authorship: The covering e-mail announcing the availability of the report refers to its authors as being "The Classic McEliece team" whereas the report refers to a "Classic McEliece Comparison Task Force".

Best wishes,

Martin Albrecht, Carlos Cid, Kenny Paterson, Cen Jung Tjhai, Martin Tomlinson
The NTS-KEM design team

On Friday, 29 June 2018 03:32:25 UTC+1, D. J. Bernstein wrote:

> The Classic McEliece team has posted a document "Classic McEliece vs.
> NTS-KEM" available here:
>
> https://classic.mceliece.org/nist/vsntskem-20180629.pdf
>
> ---Dan