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