From:	Martin Tomlinson <mt@post-quantum.com>
Sent:	Sunday, June 2, 2019 5:32 AM
To:	pqc-comments
Cc:	pqc-forum@list.nist.gov
Subject:	ROUND 2 OFFICIAL COMMENT: Classic McEliece
Attachments:	Message signed with OpenPGP using GPGMail.asc

Further to my comment about ISARA's recent US patent covering lattice based submissions, I have discovered that ISARA also have a US patent, US9912479, which is a KEM patent using McEliece, granted in 2018. It appears to cover the IP of Classic McEliece and may well cover other code based submissions.

--Martin

--

PQ Solutions Limited (trading as 'Post-Quantum') is a private limited company incorporated in England and Wales
with registered number 06808505.

This email is meant only for the intended recipient. If you have received
this email in error, any review, use, dissemination, distribution, or
copying of this email is strictly prohibited. Please notify us immediately
of the error by return email and please delete this message from your
system. Thank you in advance for your cooperation.

For more information
about Post-Quantum, please visit https://www.post-quantum.com/
In the course of our business relationship,
we may collect, store and transfer information about you. Please see our
privacy notice at https://www.post-quantum.com/privacy-notice/ to learn about how we use this
information.

From: D. J. Bernstein <djb@cr.yp.to>
Sent: Sunday, June 2, 2019 10:25 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] ROUND 2 OFFICIAL COMMENT: Classic McEliece
Attachments: signature.asc

I've been working on an analysis of post-quantum patents, and I'm confident that US9912479 won't survive a court case. (Obviously it's easier for everybody if ISARA simply gives up the patent rather than frivolously forcing litigation.)

This patent is similar to the Gaborit--Aguilar Melchor patent in that it covers a broad range of submissions to NIST, not just Classic McEliece.
The big difference is that the Gaborit--Aguilar Melchor patent was filed _before_ the relevant scientific literature, while this patent was filed _after_ the relevant scientific literature.

In case anyone ends up in litigation about patent 9912479, here's prior art that directly kills claim 1 of the patent:

* https://eprint.iacr.org/2016/461, May 2016 version, Figure 2.2.
  (The patent application was filed June 2017.)

This is a special case of https://eprint.iacr.org/2002/174.pdf, Theorem 4, which builds a KEM that produces a session key and confirmation by hashing a random PKE input. The special case here (Streamlined NTRU Prime 4591^761) uses a particular PKE where the input is a random weight-w vector.

(For people not familiar with patent law: If a previous publication has all the elements of a claim then the claim is automatically invalid. One doesn't need to analyze obviousness. The patent holder can't escape by saying that the prior art is more specific than the claim; patent law doesn't let you patent generalizations of prior art.)

The records of ISARA's discussions with the patent office show that the examiner identified an earlier publication with all the same elements, and that ISARA got around this only by saying that this publication used a _random_ vector while ISARA had invented _pseudorandom_ vectors. I've skipped this ridiculous issue by pointing to prior art where the random vectors are indisputably derived from output of a PRNG.

The same prior art https://eprint.iacr.org/2016/461 also directly kills most of the other claims in the patent, still without an obviousness analysis. Some of the claims are artificially narrowed to McEliece, but there are at least four independent ways to kill those claims:

* Take the prior art cited by the examiner, and point to any number
  of sources (the Ferguson--Schneier book, NIST DRBG standards, etc.)
  explaining in detail that "random" numbers in cryptography are
  normally generated pseudorandomly. This still doesn't need an
  obviousness analysis.

* Take https://eprint.iacr.org/2002/174.pdf, Theorem 4, as prior art.
  The theorem has interchangeable parts---it explicitly lets you plug
  in any "deterministic encryption algorithm that is secure in the
  OW-CPA model"---so it's obvious to try anything that's identified
  in the literature as a deterministic OW-CPA encryption algorithm.

https://persichetti.webs.com/Thesis%20Final.pdf identifies McEliece as a deterministic OW-CPA encryption algorithm.

* Take https://eprint.iacr.org/2016/461 as prior art, and argue that replacing NTRU with McEliece is an obvious variation, given the literature drawing analogies between NTRU and McEliece. (Of course this is how ISARA came up with this "invention" in the first place. I recommend that researchers avoid collaborating with ISARA, and avoid allowing ISARA people to review paper submissions.)

* After killing claim 1 on the basis of prior art, point out that ISARA certainly knew this prior art and thus engaged in what's called "inequitable conduct" under patent law. This automatically kills all the other claims of the patent.

---Dan (speaking for myself)