

**From:** [Moody, Dustin \(Fed\)](#)  
**To:** [Moody, Dustin \(Fed\)](#)  
**Subject:** RE: pqc notes  
**Date:** Monday, February 29, 2016 3:01:00 PM

---

Visitors – Daniel, Oscar, Tsuyoshi, Jintai, (Ludovic)

---

**From:** Moody, Dustin (Fed)  
**Sent:** Monday, February 29, 2016 2:54 PM  
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>  
**Subject:** pqc notes

PQCrypto 2016 quick report.

There were over 230 people registered, of which over 150 were from outside of Asia. The next one will be in May 2017 in the Netherlands, and in Florida in March of 2018. We will probably co-locate our next workshop in Florida in 2018. There were 42 submissions, of which 16 were accepted (including 3 by Ray, Daniel, Dustin).

Notes from talks:

Mosca: thinks 50/50 chance of breaking RSA 2048 by 2031.

Talk 1: IND-CCA2 hybrid encryption scheme using QC-MDPC. Seems fast enough.

Talk 2: PRNG based on rank metric/codes. Faster than the Hamming metric version. Hard to make fast with small key sizes.

Dan: Has bet quantum computer will break RSA within 18 years. Hybrid approach good idea for code signing. Talk is about IP/DNS/TCP/TLS. Maybe can adapt to handle 1MB keys for McEliece. He'll have something quantum-resistant for people to play with on the net this year – something to do with SSL wrap?

AES talk: lists gates needed to break AES with quantum computer. Way too many to be practical. ( $2^{80}$  depth and 3000 qubits for AES-128). They still recommend moving to AES-256

PQ-security of modes: some of the modes are QCPA secure, some aren't.

Soukharev – isogeny based authenticated encryption scheme. Quantum security models. He says they have the smallest key sizes.

QKD talk – broader, honest view of the field.

Tillich – broke a code-based signature scheme using statistics/correlations. Takes 100K signatures.

Forge signatures in 1 hour on SAGE. Best Paper Award.

Ray – we broke a code-based scheme completely

Vlad – Polar codes have efficient decoding algorithm and high capacity for memoryless channels, and seem to not have much structure. Related to Reed-Muller codes, and monomial codes. They broke a scheme with  $2^{105}$  security level on a really good laptop in 14 days.

Sendrier – Analyzed the improvements in information set decoding, which has been around since 1962. Computed asymptotic complexities. The improvements are worthwhile, and give better understanding of choosing parameters.

Ernie – same as his presentation to us. Their goal is products in the 2020's are quantum-resistant. Likes hash-based signatures, but understands implementation will not be easy. Wants worldwide standards soon. Wants stateful and state-less versions.

Jeremy – showed HFEv, v- have no nontrivial differential structure.

Alan – new MQ encryption scheme, similar to ABC and ZHFE, based on extension field maps.

Decryption is very slow. Keygen slow. Big keys.

Daniel – ZHFE has slow key gen. They created a faster way to do it. From days to minutes, and

doesn't change keyspace.

Galbraith – Big challenge in knowing running times of lattice algorithms for large parameters. Trusts LWE, but uncertain on R-LWE because still lots of research ongoing. Says good security reductions leads to good security.

Oscar – did sidechannel protection for additive homomorphic R-LWE scheme. Split the key into  $r_1+r_2$  in randomized way. 4x slower than with no masking.

Gama – homomorphic LWE e-voting scheme. Lots of parts – no idea how they fit it into 12 pages (they didn't). Inspired by Helios.

Hot topics session

Fukuoka MQ challenge – half of them solved. Took 30 days, recommends not using  $GF(2)$  for MQ for  $2^{80}$ .

QcBits – implemented constant time QC-MDPC.

HIMMO challenge – small instances solved. Attack found, parameters changed.

NTRU' – system based on isomorphism of finite fields. Hides NTRU structure

GMU – framework to evaluate HW/SW for PQC systems. QC-MDPC seems fast enough.

Hash – mainly not to worry about quantum attacks for hash on preimage attacks.

China – doing lots of work in this field (500 people), spending lots of money. QKD + PKC. Focused on lattices, MQ.

Notes – what people asked me about our Call

Dan Bernstein: Look at what symmetric key standards may need to change as well. For example, 256 bits often used to derive 128 bit keys. Could have some impacts.

Google guy: How does our process ensure no backdoors?

Tanja: It would be helpful if the API provided would be compatible with supercop/ebacs.

Somebody asked if our process will slow down the y variable – (meaning the time to get algorithms standardized, implemented, and out into the field)

David Jao: recommends that we look at quantum security models, especially for key exchange. He and his group have looked at this a lot.

Mike Mosca: really likes our approach.

Jean-Pierre Tillich: Main reason he attended PQCrypto was for NIST announcement

Zheng (Security Innovation): Wants to know if we've considered a hybrid approach.

Peter Campbell (ETSI/GCHQ): will our IPR approach work? What happens with IPR after analysis phase? Are there IPR-free algorithms that can be standardized?

Entrust (CA company): They're watching the field, and want standards before they'll act. They like hash-based signatures. One of their use cases: generate a million certs/second. Another use case: need 5 or 6 signatures to load up a typical web page.

Someone from Leuven: Is IND-CCA2 overkill?

Andreas Hulsing: What's your plan for hash-based signatures? Their latest XMSS draft is likely the final version. Please communicate your plan to the public. Agreed it would be good for their draft (XMSS) and LMS to merge.

For the Q&A session, we got a lot of good feedback and questions. I didn't take notes, as they videotaped it, which should be available soon. A lot of discussion over the hybrid approach, which people seem pretty interested in.