LIMA : A PQC Encryption Scheme

Martin R. Albrecht (Royal Holloway, University of London),
Yehuda Lindell (Bar-Ilan University & Unbound Tech),
Emmanuela Orsini (KU Leuven),
Valery Osheter (Unbound Tech),
Kenneth G. Paterson (Royal Holloway, University of London),
Guy Peer (Unbound Tech),
Nigel P. Smart (KU Leuven & University of Bristol & Unbound Tech).

Basic Design

Four schemes:

- IND-CPA encryption (for short messages)
- IND-CCA encyption (for short messages)
- IND-CPA KEM (for long messages)
- IND-CCA KEM (for long messages)

IND-CCA Security

The public key encryption scheme uses the FO transform to achieve this

The KEM scheme uses a method of Dent to achieve this

- Tight proof by reducing directly to ring-LWE
- Proof obtained independently by Kiltz et al as well

Special Properties

Very conservative design

Standard ring-LWE, nothing surprising.

- Tried and trusted.
- Close to the well studied FV FHE scheme

Uses SHA-3 XOF for random seed expansion

- Could obtain faster performance using AES based CTR mode, but less clear security guarantees
- Not a random oracle for example

Bells/Whistles

We give power of 2 and “safe prime” variants

Use of safe primes is to avoid potential subfield attacks in the future

- Safe primes are geometrically almost as good as power of two fields
- Safe prime cyclotomic fields allow FFT for performance
- Safe prime cyclotomics have small number of subfields.

Implementation

We do not give a machine code implementation using SSE etc

- We (and others) have found that using these extensions causes overall performance of cryptographic **systems** to slow down
- Just looking at run times of algorithms on their own is not a good measure of overall performance in the wild
- Would caution NIST against putting too much emphasis on academic measures of performance of algorithms for this reason

Patent Situation

To our knowledge the design is patent free

We have not filed any patents on the design, or implementation techniques.

For this reason did not use ciphertext compression using reconciliation

Potential Tweaks - 1

Our submission tried to use a method to avoid decryption failures by doing rejection sampling during encryption

- This does not work

If we pass to round 2 we will remove this and revert to a “standard” analysis of decryption failure

- Result will be smaller parameters
- Simpler/faster encryption times
- Faster overall performance.

Potential Tweak -2

As we tried to keep our design simple we did not try to optimize for bandwidth

If NIST consider bandwidth of high importance over simplicity, we can reduce bandwidth by

- Removing almost all low order bits of the second ciphertext component
- Applying Huffman encoding to all datatypes

Potential Tweaks - 3

Research since submission also leads us to claim that the design is also highly amenable to a distributed decryption variant which is actively secure.

- Due to the linear nature of the LWE problem
- Use of SHA-3 based XOF construction
- Use of the specific CCA constructions

Thank You

Questions?