Post Quantum Identity Based Encryption

In our last blog (which you really need to read first before reading this one) we pointed out that Post-Quantum cryptography as based on the Ring Learning with Errors (RLWE) problem, can actually be quite easy to understand, despite its rather terrifying terminology.

Its based on this one-way function

$$B=As+e$$

Where A and B are "large" polynomials and s and e are "small" polynomials. Given A, s and e, its easy to calculate B, its just a multiplication followed by an addition. However given B and A, its very hard to calculate s and e. Even a quantum computer can't do it. That's why we call it one-way.

In the terminology of cryptography s would be a private key, and B would be the matching public key. The large polynomial A is often a globally known randomly generated value. Typically a user would generate their own secret s and random error polynomial e, and from that calculate their public key B which they could distribute to anyone that wanted to communicate with them.

Now here at MIRACL we are big believers in Identity Based Cryptography (IBC). One of the pillars of IBC is IBE – Identity Based Encryption. And the big idea here is that your identity **is** your public key. And your identity might just be your email address.

Clearly that's not going to work immediately here, as the user just gets to choose s and e and has very little control over what B looks like – its just a large polynomial which certainly won't look anything like an email address.

So lets go back and change things a little. Instead of A being "randomly generated" let us craftily construct it so that while it certainly looks random, it actually isn't. In the terminology of cryptography we are going to insert a trapdoor, access to which is not available to the general public, but rather is only known to a trusted authority. Given access to this trapdoor the trusted authority can "push" any public key back through the supposedly one-way function to find matching s and e values. (And its easy to come up with a consistent and known-to-all method to map an email address to a large polynomial).

So now an individual can approach this trusted authority, show their identity (and prove their right to it), have it mapped to a large polynomial and be issued with the matching secret key. And now instead of distributing and proving their legitimate ownership of a large random looking public key, they just need to distribute their email address!

After that proceed just as described in the last blog.

This is the IBE method proposed by Ducas, Lyubashevsky and Prest in 2014. We have implemented this scheme using our MIRACL library. While creating the trapdoor is quite time-consuming, this only needs to be done once. Encryption and decryption are both extremely fast.