Toy Examples in Post-Quantum (PQ) Cryptography

Peter Lablans | CEO/CTO at LabCyfer | Published March 15, 2025

Post Quantum (PQ) Cryptography

The best way to learn a cryptographic primitive is a simple example, called a toy example. Unfortunately, most explanations on novel PQ cryptography are dense in mathematics and difficult to understand. The need for explanation of PQ PKI is especially urgent after acceptance of Kyber as the new NIST FIPS 203 Standard and being implemented by service providers.

A really outstanding, simple and easy-to-understand toy example is currently available in a series of short video lectures by the world-renowned cryptographer Prof. Dr. Alfred Menezes.

The Purpose of Toy Examples

Computer cryptography is complex. And modern concepts even more so than the old Caesar Cipher or the Enigma machine. One way to explain and/or illustrate advanced computer cryptography is by what are called Toy Examples. A Toy Example uses simplified and usually smaller parameters of an encryption

method, for instance, to explain data flow and the intermediate computational results. But, preferably it uses all the same math as the production method.

This may be exemplified by the explanation of RSA key exchange by Wikipedia. Currently, RSA may require computational parameters that are at least 2048-bits in size. Those are numbers with over 600 digits. That is unpractical to explain how RSA works. The Wikipedia article uses smaller parameters like p=61 and q=53, which allows a reader to better follow the data flow and perform the operations in a simple computer program.

It allows a user to get an impression of what takes place in the innards of an advanced cryptographic method, without getting overwhelmed by operationally large parameters.

Modern, Novel Post Quantum (PQ) Cryptography

Truly “modern” cryptographic methods pertain, for instance, to post-quantum (PQ) methods that are just now being issued in standard form. An example is Kyber, which has been issued as FIPS-203, or entitled: Module-Lattice-Based Key-Encapsulation Mechanism Standard. If you want to learn about truly modern post-quantum cryptography, publication FIPS 203 is unfortunately NOT the way to go. As a standard, it seems to be intended for cryptographers, not for the layperson.

Modern post-quantum cryptography explanations seem to be dominated by articles that are basically unreadable for non-mathematicians. Articles that try to explain the concepts, like Learning With Errors (LWE), often oversimplify or fail to convey the underlying logic. LWE introduces an error vector to obscure plaintext during encryption. The challenge lies in recovering the original plaintext, which is possible due to specific properties of the error when processed correctly. LWE relies on selecting the appropriate error vector and rounding a computation at the receiving end to recover the plaintext error-free. This is the “magic trick” in Kyber and is hard to explain concisely. Making introductory articles on LWE difficult for the average cryptography enthusiast. I know because I’ve tried, only to return to advanced textbooks.

A Simple Kyber/FIPS-203 Toy Example

To my surprise and delight, I came across a series of lectures on FIPS 203 and FIPS 204 by Prof. Dr. Alfred Menezes (of Handbook of Applied Cryptography fame). His handbook serves as a reference rather than self-training material.

His video lectures on FIPS-203 (Kyber) and FIPS-204 (Dilithium) are an absolute “stand-alone” and “must-watch” for those interested but mystified by aspects of Post-Quantum (PQ) cryptography and LWE.

Do yourself a favor and watch these Menezes Lectures on novel post-quantum PKI Kyber and Signatures Dilithium at cryptography101.ca.