Protecting data against physics

The possible invention of large scale quantum computers poses a serious threat to modern cryptography. Quantum computers can easily break most modern public key cryptography and in order to keep data safe new algorithms has to be used. The currently used algorithms were, however, chosen for a reason and finding good replacements requires evaluation of the options.

Imagine a world where computers can take advantage of the mystical properties of quantum particles. This would give them unprecedented powers and would allow them to easily break most modern cryptographic solutions with negligible effort. All is not lost though, and there are cryptography that even quantum computers cannot break. These do, however, often have large keys or slow runtime, something that is unacceptable in a world where we do not want to wait for anything. In order to choose a worthy successor for the then worthless algorithms the candidates need to be compared and evaluated.
The alternative algorithms can be divided into five categories; code-based, lattice-based, supersingular isogenic Diffie-Hellman (SIDH), multivariate and hash-based. The multivariate methods have proved hard to keep secure if they are used for anything other than signatures and the hash-based methods cannot be used for anything else. For these reasons only algorithms from the first three categories have been considered.

With an age of about 40 years the, by far, oldest and most well studied of the categories are the code-based. These algorithms are fast, but use enormous keys that renders them practically unusable in devices with limited memory.

An idea that is a lot newer is SIDH. These algorithms enjoy small keys that can be compressed to become even smaller, but they are really slow and the theory they are based on is a lot more complicated than that of the others.

The winner is found in between, both in age and performance, in the form of lattice-based cryptography. These algorithms provide a good trade-off between performance and key size and have, for this reason, been a hot research area during the last couple of years. More specifically the algorithm that performed best overall is called NTRU and was invented and patented about 20 years ago. It works by encoding the message as a polynomial which is then cloaked by adding a randomly chosen polynomial encrypted with the public key. The cloaking can then only be removed by someone who knows the private key, which, in combination with some modular arithmetic, can be used to extract the message.