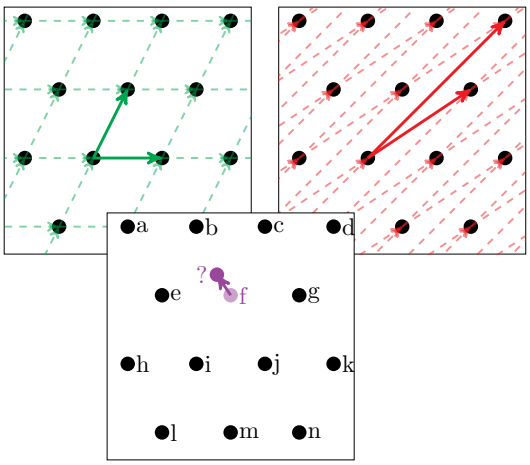
Lattice cryptography: from cryptanalysis to New Foundations

Woerden, W.P.J. van



Summary

This thesis is primarily about lattices. Not in dimension two or three which we can still visualize, but in hundreds, sometimes thousands of dimensions. These high dimensions bring with them a lot of computational problems. Questions that are easy in two dimensions, can be very hard in higher dimensions. And these hard problems give rise to cryptography.

Cryptography aims to make communications secure in case the connection is overheard or influenced. Surprisingly enough, this can be done without the communicating parties agreeing in advance on a secret code language. This requires problems which are hard in general, yet can be solved if certain secret key information is known. If only the recipient is familiar with that secret key, then only that person can read the message, and no one else. Think of a safe with a padlock. Anyone can put a message in the safe and push the lock shut, but only the owner of the key can unlock the safe (effortlessly).

Lattice problems are ideally suited for such an encryption, with the added advantage that they do not appear to be efficiently solvable even by quantum computers. The idea is as follows. A lattice, despite its high dimension, can be described by a few arrows (see figure). A description with long arrows (red) hereby forms the safe with padlock and a description with short arrows (green) hereby forms the key. Finding such a short description, given a long description, is called reduction and is hard computational problem. If we think of a lattice point as a letter, it can be encrypted by moving the lattice point slightly outside the lattice. Recovering the original location, and thus

decrypting the message, is called decoding. Decoding is generally hard except with a short description, the key.

Part II and III deal with cryptanalysis asking the central question: exactly how hard is it to read the encrypted message? We can find out the key (reduce), or break open the lock by force (decrypt). In Chapter 4, we show how, using modern algorithms and graphic cards, we are able to reduce a lattice in dimension 180, 25 dimensions more than the old record. In Chapter 5, we analyse an algorithm, which after some preliminary work, can decode many points in the same lattice. In Chapter 6 we discuss that lattices used in cryptography are often somewhat oddly shaped, for example by containing lattice points that are too close together. These deviations make reduction or decoding often considerably easier than you might expect, given the high dimension. We deal in Chapter 7 with so-called NTRU lattices, which have been used in cryptography since 1996. These lattices have in some cases an even larger deviation than expected, and we predict for the first time exactly how this affects their security.

Unfortunately, these deviations are inherently present in all lattices currently in use. Remarkable lattices, which have smaller deviations but are still decodable, actually do exist and would theoretically be safer. The problem is that these remarkable lattices are known to everyone, including their short description, making them currently unusable. In Part IV, we show that the short description can still be hidden, simply by rotating the lattice, where now the rotation is the key. In Chapter 9, we substantiate why finding the rotation is hard. In Chapter 10, we show how this can theoretically be used to encrypt or digitally sign messages, and give a practical demonstration in the form of a highly efficient digital signature called HAWK.

In the stand-alone Chapter 8, we show that well-known notions and algorithms for lattices, are also translatable into linear codes, a kind of finite analogue to lattices. Among others, we transfer the famous LLL reduction algorithm to linear codes.