From: pqc-forum@list.nist.gov on behalf of Julian <lordriotglacier@gmail.com>
Sent: Thursday, July 20, 2023 3:43 AM
To: pqc-forum
Subject: [pqc-forum] Round 1, Additional Signatures, OFFICIAL COMMENT: Squirrels

Dear Squirrels submitters,

I'm confused about the relationship between HNF shapes on co-cyclic lattices.

I test some lattices, for example:

[2, 0, 154]
[0, 1, 125]
[0, 0, 205]

the lattice based on this basis matrix is co-cyclic, but its HNF is different from what was mentioned in the document 2.2:

It seems that a co-cyclic lattice does not necessarily have this property.

Based on this, I'm curious about the density of this kind of lattices, is it going to be the same as 85% of co-cyclic lattices?

Best regards,

Julian
--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/61df813d-095b-4a0f-8802-30991ea4d3d3n%40list.nist.gov.

From: pqc-forum@list.nist.gov on behalf of Mehdi Tibouchi <mehdi.tibouchi@normalesup.org>
Sent: Thursday, July 20, 2023 10:26 AM
To: Julian
Cc: pqc-forum
Subject: Re: [pqc-forum] Round 1, Additional Signatures, OFFICIAL COMMENT: Squirrels

Dear Julian,

Good question! The techniques from the Nguyen-Shparlinski cocyclic lattices paper should extend to this case, but we don't have the result yet. We will look into it.

We can however carry out the counting argument in the special case of a squarefree determinant D (which is the case that occurs in Squirrels).
Note that lattices with such a squarefree determinant are all cocyclic since the only abelian group of order D is Z/DZ.

To count the lattices of determinant D, it suffices to count the HNFs. In such an HNF, each of the prime factors p of D will occur at exactly one position i_p on the diagonal, and the number of HNFs with the pattern (i_p)_{p|D} is \prod_{p|D} p^{i_p-1}. Therefore, the total number of lattices of determinant D is exactly:

N(D) = \prod_{p|D} (1 + p + ⋯ + p^{n-1}) = \prod_{p|D} (p^n-1)/(p-1)

and of those, exactly D^{n-1} have an HNF of the form we desire (namely with diagonal (1,...,1,D)). The proportion is therefore:

D^{n-1} / N(D) = \prod_{p|D} p^{n-1}(p-1) / (p^n-1)

which is always greater than phi(D)/D and converges to that value as
n->\infty.

In our case, we fix D as a product of distinct primes that are moderately large (31 bits), which makes the probability of having the required HNF shape very close to 1. For example, it is above 1-2^{-23} for parameter set Squirrels-I (in other words, a random lattice of determinant D will be rejected in key generation with probability < 2^{-23}). The situation would be different with D divisible by many small primes. However, the arguments of Paz and Schnorr saying that all lattices are arbitrarily close to cocylic lattices still hold when we consider only cocyclic lattices whose determinant does not have small prime factors.

Anyway, we will try to carry out the density computation in the style of Nguyen-Shparlinski and send an update accordingly.

Best regards,

--
The Squirrels team.

On Thu, Jul 20, 2023 at 12:42:31AM -0700, Julian wrote:
> Dear Squirrels submitters,