From: Moody, Dustin (Fed)
To: Apon, Daniel C. (Fed)
Subject: RE: Are you interested in starting an (exploratory) research project with me?
Date: Monday, April 8, 2019 8:23:00 AM

Daniel,

I'm no expert in this particular sort of question, but I'd be happy to learn more and see where it goes.

Dustin

From: Apon, Daniel C. (Fed)
Sent: Sunday, April 7, 2019 3:57 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Are you interested in starting an (exploratory) research project with me?

Hi Dustin,

There is this classic (tight) result on the robustness of Learning with Errors: https://www.microsoft.com/en-us/research/wp-content/uploads/2017/01/2010-Robustness_Learning_Errors_Assumption.pdf

Intuitively, it says that if the LWE secret (of length n = \securityparameter) is drawn from an arbitrary distribution (so long as it has sufficiently high, k = \omega(log(n)), min-entropy), that the resulting problem is no harder than a standard LWE instance with secret-length of k.

The motivating question has been to ask whether some algebraically-structured lattice problem also enjoys this entropic-security property. For example, can I sample the coefficient-vector of a RLWE or MLWE secret from an arbitrary distribution (conditioned on sufficient min-entropy) and retain security proportional to the entropy with which I sample the secret polynomial?

After exploring this for quite a while, I've somewhat come to the conclusion that entropic-security for algebraically-structured LWE does NOT hold, so long as the ambient space is commutative (which rules out RLWE and MLWE completely).

The residual question is then to ask whether there is some form of non-commutative, algebraically-structured LWE which retains 'standard security' and also has entropic-security. (On some level, I am happy treating this as a purely asymptotic, 'theoretical' question, and not worrying too strongly about the exact notion of 'standard security' involved here at the moment.)

As such, I've just begun trying to explore 'weird' formulations of the short vector problem (SVP) in 'weird' lattices. The latest example on my mind is to consider some non-standard lattice problem over the strange ring \Z[x,y] / <x^n-1, y^n-1>, and then consider all of the relevant NTRU-like terms according to quaternion algebra -- this seems like a very minimal way (though, not fleshed out yet) to construct a hard lattice problem over non-commutative algebra.

That said, while I'm generally looking for any formulation of a hard lattice problem in non-commutative algebra that would enable an entropic-security type of reduction (in the asymptotic sense -- I care more about basic feasibility of such a result right now; not whether such a result is remotely instantiable at practical parameters), one direction that seemed interesting to me was whether you could define a hard lattice problem over a (multivariate) ring defined by elliptic curve polynomial equations.

For (wild) example (without much thought into it yet), consider the standard-form Weierstrass equation $y^2 = x^3 + ax + b$.

Re-write this as the polynomial $x^3 - y^2 + ax + b - 1$.

Define the ring $R_q := \mathbb{Z}_q[x,y] / \langle x^3 - y^2 + ax + b - 1 \rangle$ for some a, b.

Now, consider an LWE-type equation over R_q:
$a*s+e$

What security properties can be shown about instances like $(a, a*s+e)$ over this "strange" lattice?

Let me know if you're interested,
--Daniel