Problem 6. «NTRU-style equation»

Problem for a special prize!

Alice is fascinated by the NTRU cryptosystem and its simple key equation $h = f^{-1} * g \pmod q$. In the early proposal of NTRU, the cryptosystem was constructed over the ring $\mathcal{R} = \frac{\mathbb{Z}[x]}{(x^N-1)}$, where both f and g are sampled with small coefficients, typically from the set $\{-1, 0, 1\}$.

Alice assumed that choosing $N = 127$ and by sampling f, g with enough entropy would provide sufficient security, as the combinatorial cost of recovering either f or g is large, making it difficult for Bob to break. Alice published h and challenged Bob to find f and g. After a few days, however, Bob managed to recover Alice's key and explained that it is easy to attack NTRU keys using lattice reduction techniques in relatively small dimensions by constructing the lattice

$$\mathcal{L}_{CS} = \begin{pmatrix} \mathbf{I}_N & \mathsf{mat}(h) \\ \mathbf{0}_N & q \cdot \mathbf{I}_N \end{pmatrix},$$

and applying lattice reduction, where $\mathsf{mat}(h)$ is the matrix representation of h with respect to the ring $\mathcal{R}$, which in this case is a right-circulant matrix.

Alice was frustrated by this and did not want to increase N much. She started reviewing the literature and found a noncommutative variant of NTRU built over a slightly more complex ring: the group ring of the dihedral group $\mathcal{R}_{D_N} = \mathbb{Z}D_N$, where D_N denotes the dihedral group of order $2N$, defined as $D_N = \langle x, y \mid x^N = 1,\ y^2 = 1,\ xy = yx^{N-1} \rangle$. By abuse of notation, we can write

$$\mathcal{R}_{D_N} \approx \frac{\mathbb{Z}[x, y]}{\langle x, y \mid x^N = 1,\ y^2 = 1,\ xy = yx^{N-1} \rangle},$$

and any $f \in \mathcal{R}_{D_N}$ can be written, for simplicity, as $f = f_0(x) + yf_1(x)$, where $f_0(x)$ and $f_1(x)$ are two polynomials of maximum degree $N - 1$.

Alice then proposed modifying the NTRU key equation over this new noncommutative ring as

$$h = f_1^{-1} * g * f_2^{-1} \pmod q,$$

where $f_1, f_2 \in \mathcal{S}$, and $\mathcal{S}$ is defined as the commutative subring of $\mathcal{R}_{D_N}$:

$$\mathcal{S} = \{\, f \in \mathbb{Z}D_N \mid fy = yf \,\}.$$

Here, g is sampled randomly from $\mathcal{R}_{D_N}$ with small coefficients from the set $\{-1, 0, 1\}$. Alice believed that this construction would prevent Bob from applying lattice reduction directly.

However, when she gave h to Bob, he pointed out that lattice reduction could still be applied indirectly by constructing $h + yhy$, which transforms the key equation into a commutative one:

$$h+yhy \pmod q = f_1^{-1} * (g+ygy) * f_2^{-1} \pmod q = (f_1 * f_2)^{-1} * (g+ygy) \pmod q,$$

which is again an NTRU instance.

Alice, now even more determined, constructed her key as

$$h = f_1^{-1} * g * f_2^{-1} \pmod q,$$

sampling f_1, f_2 from $\mathcal{S}$ but restricting g to be sampled from

$$\mathcal{S}^- = \{f \in \mathbb{Z}D_N \mid fy = -yf\}.$$

This time, Alice is convinced that Bob cannot convert h into an NTRU-style equation and therefore cannot apply lattice attacks directly.

Could you help Bob to disprove Alice, or do you agree with her? Explain.