Problem 5. «Understand the Oracle»

Bob challenges Alice by providing a matrix $\mathbf{B} \in \mathbb{Z}^{2n\times 2n}$ and asks her to find an integer vector $\mathbf{g} \in \mathbb{Z}^{2n}$ that is short in the Euclidean norm and satisfies $\mathbf{Bf} = \mathbf{g}$, for some $\mathbf{f} \in \mathbb{Z}^{2n}$.

Alice possesses a magical oracle capable of finding short vectors in dimension n, and it can be invoked any number of times. Bob further guarantees to Alice that there exists a way to reduce the dimension of $\mathbf{B}$ to n, and that adding any two coefficients of the vector $\mathbf{g}$ yields a small value. The first time, Bob challenged Alice by giving the matrix

$$\mathbf{B} = \begin{pmatrix} \mathbf{H}_0 & \mathbf{H}_1 \\ \mathbf{H}_1 & \mathbf{H}_0 \end{pmatrix}.$$

Alice quickly realized that if she splits $\mathbf{g}$ as $(\mathbf{g}_0, \mathbf{g}_1)$, then she can provide the oracle with the matrix $\mathbf{B}_0 = \mathbf{H}_0 + \mathbf{H}_1$ of dimension n, such that $\mathbf{B}_0(\mathbf{f}_0 + \mathbf{f}_1) = (\mathbf{g}_0 + \mathbf{g}_1)$ holds. Since $\mathbf{g}_0 + \mathbf{g}_1$ is still a short vector (by Bob's guarantee), the oracle can find $\mathbf{g}_0 + \mathbf{g}_1$. Similarly, she can invoke the oracle with $\mathbf{B}_1 = \mathbf{H}_0 - \mathbf{H}_1$ to obtain the vector $\mathbf{g}_0 - \mathbf{g}_1$, and ultimately recover $\mathbf{g}$.

Bob then made the challenge harder and gave Alice a matrix of the form

$$\mathbf{B} = \begin{pmatrix} \mathbf{H}_0 & \mathbf{H}_1 \\ \mathbf{H}_1{}^T & \mathbf{H}_0{}^T \end{pmatrix},$$

where $\mathbf{H}_0$ is a right circulant matrix and $\mathbf{H}_1$ is a left-circulant matrix, and $\mathbf{H}_0^T, \mathbf{H}_1^T$ denote the transposes of $\mathbf{H}_0$ and $\mathbf{H}_1$, respectively. Can you help Alice to reduce this matrix to dimension n so that she can use the oracle?

Note 1: We say that $\mathbf{H}_0$ is a *right circulant matrix* if it has the form $\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix}$,

and similarly $\mathbf{H}_1$ is a *left circulant matrix* if it has the form $\begin{pmatrix} b_0 & b_1 & \dots & b_{n-1} \\ b_1 & b_2 & \dots & b_0 \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1} & b_0 & \dots & b_{n-2} \end{pmatrix}$.

Note 2: This problem is related to lattice-based cryptography, as finding the short vector $\mathbf{g}$ corresponds to solving the Shortest Vector Problem (SVP) in the lattice generated by $\mathbf{B}$.