Question 3

Observe the following:

$$\begin{aligned} A\mathbf{z} &= A(\mathbf{y} + c\mathbf{s}) \\ &= \mathbf{w} + cA\mathbf{s} \\ &= \mathbf{w} + c(\mathbf{t} - \mathbf{e}) \end{aligned}$$

Assuming that c is invertible, re-arranging the equation above gives us:

$$\mathbf{e} = \mathbf{t} - c^{-1}(A\mathbf{z} - \mathbf{w})$$

From here we can attempt to recover the secret key $\mathbf{s}$ by solving $A\mathbf{s} = \mathbf{t} - \mathbf{e}$. While this is an instance of inhomogeneous SIS, with proto-Dilithium A is a wide matrix, which makes SIS easier to solve. In the lecture notes, we simply assume that wide SIS is "too easy".