For continuity, this document defines exactly the same KEM as the round-3 Classic McEliece submission. This definition is presented as a list of changes to the separate “cryptosystem specification” document. Security analysis of this KEM continues to be encouraged.

The changes are as follows. Remove “of length $mt$” from the description of $C$ in the table of notation. Replace the steps that define $\text{Encap}$ with the following:

1. Use $\text{FixedWeight}$ to generate a vector $e \in \mathbb{F}_2^n$ of weight $t$.
2. Compute $C_0 = \text{Encode}(e, T)$.
3. Compute $C_1 = \text{H}(2, e)$. Put $C = (C_0, C_1)$.
4. Compute $K = \text{H}(1, e, C)$.
5. Output ciphertext $C$ and session key $K$.

Replace the steps that define $\text{Decap}$ with the following:

1. Split the ciphertext $C$ as $(C_0, C_1)$ with $C_0 \in \mathbb{F}_{2^m}$ and $C_1 \in \mathbb{F}_2^\ell$.
2. Set $b \leftarrow 1$.
3. Extract $s \in \mathbb{F}_2^n$ and $\Gamma' = (g, \alpha'_0, \alpha'_1, \ldots, \alpha'_{n-1})$ from the private key.
4. Compute $e \leftarrow \text{Decode}(C_0, \Gamma')$. If $e = \perp$, set $e \leftarrow s$ and $b \leftarrow 0$.
5. Compute $C_1' = \text{H}(2, e)$.
6. If $C_1' \neq C_1$, set $e \leftarrow s$ and $b \leftarrow 0$.
7. Compute $K = \text{H}(b, e, C)$.
8. Output session key $K$.

In the description of symmetric-cryptography parameters, replace “byte 0 or 1” with “byte 0 or 1 or 2”. Replace the description of the representation of ciphertexts as byte strings with the following: “A ciphertext $C$ has two components: $C_0 \in \mathbb{F}_{2^m}$ and $C_1 \in \mathbb{F}_2^\ell$. The ciphertext is represented as the concatenation of the $\lceil mt/8 \rceil$-byte string representing $C_0$ and the $\lceil \ell/8 \rceil$-byte string representing $C_1.$” Replace the description of the representation of hash inputs as byte strings with the following: “There are three types of hash inputs: $(2, v)$; $(1, v, C)$; and $(0, v, C)$. Here $v \in \mathbb{F}_2^n$, and $C$ is a ciphertext. The initial 0, 1, or 2 is represented as a byte. The vector $v$ is represented as the next $\lceil n/8 \rceil$ bytes. The ciphertext, if present, is represented as the next $\lceil mt/8 \rceil + \lceil \ell/8 \rceil$ bytes. All hash inputs thus begin with byte 0, 1, or 2, as mentioned earlier.”