# Modifications to the 2nd Round Submission

We applied the following changes to our submission.

1. **Additional Submitters**: We added two new members to our team: Matthias Kannwischer and Jacques Patarin.

2. **Website**: We created a website for the rainbow signature scheme (www.pqcrainbow.org), where you can find the current submission data (this file), the most recent software implementation as well as a list of references related to our scheme.

3. **Name Change of the Rainbow variants**: We decided to change the name of the Rainbow variant cyclicRainbow (c.f. 2nd round submission) into CZ-Rainbow (circumzenithal Rainbow). In meteorology, a circumzenithal Rainbow is an upside down Rainbow. By using this name, we want to emphasize that CZ-Rainbow inverts the usual key generation of the Rainbow scheme. We further want to emphasize that CZ-Rainbow does not use any cyclic structure at all.

4. **Parameter Choice**:
   For simplicity, we drop the letters in the parameter proposals and denote the three parameter proposals simply by I, III and V (according to the three security categories). Furthermore, due to some refinements in the complexity analysis of the Rainbow Band Separation and improvements in the MinRank attack (see Section 9 of our submission and our post in the PQ forum), we adapted the proposed parameters slightly. We therefore have

   - **I**: $\mathbb{F}$=GF(16), $(v_1, o_1, o_2) = (36, 32, 32)$ for the NIST security categories I and II,
   - **III**: $\mathbb{F}$= GF(256), $(v_1, o_1, o_2) = (68, 32, 48)$ for the NIST security categories III and IV and
   - **V**: $\mathbb{F}$=GF(256), $(v_1, o_1, o_2) = (96, 36, 64)$ for the NIST security category V.