A Changes made for the Second Round version of LUOV

The changes between the first round version and the second round version of LUOV are the following:

- **Updated parameters.** Compared to other NIST Round 1 MQ schemes it was clear that the parameter choice of LUOV was too conservative. Therefore we dropped the "10% in the exponent" security margin that we had in the Round I version of the document. The updated parameters result in a faster signature scheme with smaller keys and signatures.
- **Add a salt.** The second round version of includes a 16-byte salt to each message. This improves the security of LUOV against side-channel attacks and fault injection attack.
- **Choose vinegar variables randomly.** In a previous version of LUOV the vinegar variables were chosen deterministically. In the second round version they are chosen at random. This improves the security of LUOV against side-channel attacks and fault injection attacks. Moreover this makes it possible to do most of the signing work offline which makes LUOV suitable for applications were a very low signing latency is required.
- **Sampling public map from PRNG.** To improve the efficiency of sampling the public map we have introduced ChaCha8 as an option. We also sample the public map in sets of 16 polynomials. This makes it possible to evaluate multiple instances of the PRNG (Keccak or ChaCha8) in parallel for improved efficiency. Moreover this allows for implementations with a smaller memory footprint.
- **Add an AVX2 optimized implementation.** We report on the cycle count of our AVX2 optimized implementation, as well as the variant that uses precomputation on the secret key and public key.
- **Add a generic C implementation with online and offline signing phases.** See Sect. 4.5