Dear all,

We are grateful to Dr. Philippe Gaborit for pointing out a more precise asymptotic estimate on the classical hardness of underlying LPN variant considered in our Lepton proposal. In particular, for sublinear error rate $k/n = o(1)$ and coding rate $R = 1/3$ the complexity should be $O(n^3)2^{1.75k}$, where $1.75 \approx 3 \log(1/(1-R))$ and factor $O(n^3)$ accounts for the cost of Gaussian elimination and is often omitted. The implication is that we need to use larger values for $k$ and $n$ and re-evaluate the performance in the next update of the proposal. Looking back now, it seems that our implementation was too good (efficient) to be true (secure), i.e., half of the CPU cycles in encryption/decryption were spent on SHA-3 for randomness generation, so we are expecting something reasonably good when adjusted to larger parameters.

We stress our security reductions are not affected. Our original intention of using exact $k$-out-of-$n$ distribution to replace rate $(k/n)$-Bernoulli in LPN was to facilitate noise sampling and to hopefully lift security (without giving formal proofs). Now we are convinced that the latter wishful claim is not true: our LPN variant is just as hard as standard LPN of the same noise rate (up to a constant factor in the exponent), just as we proved in Lemma 2 of the proposal.

Best regards,

The Lepton Team