Dear all,

I would like to report a typo in our algorithm 4 on page 7, and a thank you to Vadim Lyubashevshy for pointing this out to us.

Line 7 of algorithm 4 should be: $(\bfu, \bfv) \gets (\bfu_0, \bfv_0) + (p\bfa\bff + \bfa\bfg)$

Line 8 of algorithm 4 should be: $||p\bfa\bff|| \leq B_s, ...$

In both cases the term $p$ is missing for $p\bfa\bff$.

This error occurs when we created the specification for submission and trying to combining two academic paper together to fit in one description.

We note that this was indeed a typo in the specification - both the implementation and the original paper captures the algorithm correctly.

Happy holidays!

Cheers,

Zhenfei Zhang