https://eprint.iacr.org/2019/1496