June 15, 2023: The paper [dPPRS23] is available in the IEEE SP 2023 proceedings via https://doi.ieeecomputersociety.org/10.1109/SP46215.2023.00160

Bibliography

[dPPRS23] Rafaël del Pino, Thomas Prest, Mélissa Rossi, and Markku-Juhani O. Saarinen. High-order masking of lattice signatures in quasilinear time. In *44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA, 22-25 May 2023*, pages 1168–1185. IEEE, 2023. doi:10.1109/SP46215.2023.00160.