BDLOP

BDLOP[1] commitments are $\mathcal{O}(n)$ and support NIZK arguments of linear relation. Using MSIS with $R_q \in \mathbb{Z}_q/(X^N + 1)$, prime q, and $\log_2(N) \in \mathbb{Z}^+$.

1 Argument

References

[1] Carsten Baum and Ivan Damgård and Vadim Lyubashevsky and Sabine Oechsner and Chris Peikert, More Efficient Commitments from Structured Lattice Assumptions, Cryptology ePrint Archive, Paper 2016/997, 2016, https://eprint.iacr.org/2016/997