Short Integer Solution Commitments

Commitments to vectors of elements in $\mathbb{Z}_q^m$ with prime q, $m \in \mathbb{Z}^+$.

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`