|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Protocols | Prover’s complexity | | | Verifier’s complexity | Proof size |
|  | computation | communication | rounds |  |  |
| Ligero |  |  | 4 |  |  |
| Bulletproofs |  |  |  |  |  |
| 2D |  |  | 5 |  |  |
| 3D |  |  |  |  |  |

In bulletproofs: q is the linear constraint: and such that is of rank .