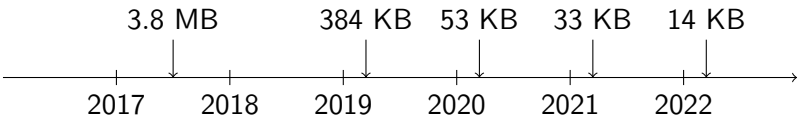
Efficient Zero-Knowledge Proofs from Lattices

Gregor Seiler

August 23, 2024

From Dark ages to modern times

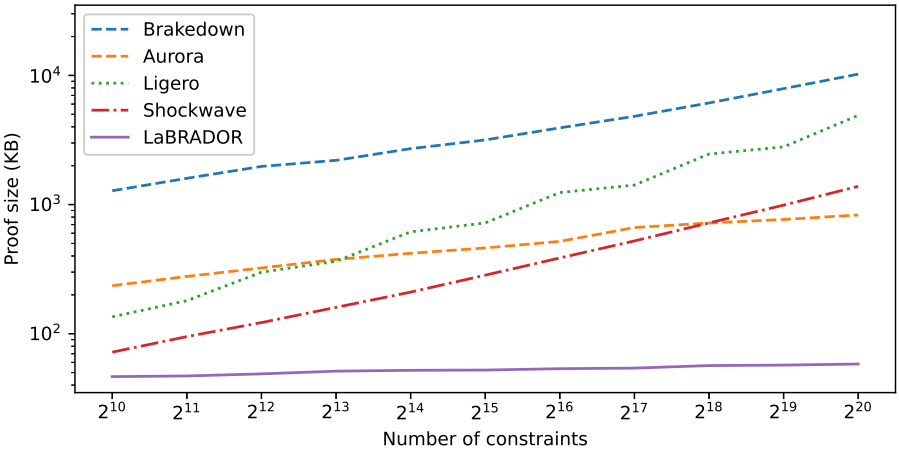
Big improvements in linear-sized lattice-based proofs over the last three years



Advantages of lattice-based proofs outside of size:

- Lattice-based schemes can be very fast (highly parallelizable polynomial arithmetic)
- No large overhead in memory requirement

Labrador: R1CS mod $2^{64} + 1$



Greyhound: Polynomial Commitments!

	2^{25}				2^{29}			
	size	comm	prove	verify	size	comm	prove	verify
Brakedown-PC	49′157 KB	36 s	3.21 s	0.703 s	181′948 KB	605 s	48.6 s	2.96 s
Ligero-PC	7′256 KB	83.9 s	3.13 s	0.338 s	28′631 KB	1590 s	51.6 s	1.57 s
FRI-PC	740 KB	168 s	185 s	0.041 s	—	—	—	—
CMNW	1′393 KB	—	—	—	3′983 KB	—	—	—
HSS	48′640 KB	30.9 s	19.6 s	1.07 s	198′656 KB	—	—	—
Greyhound	**47 KB**	**1.84 s**	**0.788 s**	**0.239 s**	**52 KB**	**72 s**	**21.7 s**	**1.61 s**