Hardware Acceleration Landscape

- **Layer-2 / zkEVM Teams**
- **Scroll**
  - PipeZK: Accelerating Zero-Knowledge Proof with a Pipelined Architecture
- **Ingonyama**
  - PipeMSM: Hardware Acceleration for Multi-Scalar Multiplication
  - Cloud-ZK: a FPGA toolkit for proof acceleration in the cloud
  - Ingonyama is building ASICs / FPGAs and is exploring production-grade systems like ZKSync, Plonky2, Halo2, etc.
  - Sparkworks: native Hardware Acceleration in Arkworks
  - Claim FPGA code achieves ~4x faster compared to ZPrize's baseline FPGA MSM
- **Supranational**
  - Sppark: Library consisting of CUDA/C++ templates that can be instantiated for a range of finite fields and elliptic curves for accelerating zero-knowledge
- **Aleo / ZPrize**
  - Accelerating MSM Operations on GPU/FPGA: Competition for speeding up MSM, using Supranational's Sppark library as a baseline benchmark.
- **Jump Crypto**
  - CycloneMSM: Novel Architecture for Accelerating MSMs on FPGA
  - CycloneNTT: Novel Architecture for Accelerating NTTs on FPGA
  - Claim subsecond 2^22 sized MSM, and 2^26 MSM in ~ 5.6 seconds
- Cysic
  - Cysic: FPGA / ASIC hybrid implementation that achieves about 1.82x – 5.63x speedup over the other FPGA implementations like PipeMSM and CycloneMSM
- **cuZK**
  - cuZK: Accelerating Zero-Knowledge Proofs with A Faster Parallel Multi-Scalar Multiplication Algorithm on GPU
- EdMSM
  - EdMSM: EdMSM: Multi-Scalar-Multiplication for recursive SNARKs and more

Table of Supported Hardware Architectures

Implementations	Supported Platforms	Full Prover	Open Source
Scroll	ASIC	YES	NO
Ingonyama	ASIC, FPGA	YES	NO, YES
Supranational	GPU	NO	YES
Aleo / ZPrize	GPU, FPGA	NO	YES
Jump Crypto	FPGA	TBD	NO
Cysic	FPGA	TBD	NO
cuZK	GPU	YES	NO