

## 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
- [CloudZK](#): 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.
- Here are the [results](#)

#### ❖ Jump Crypto

- [CycloneMSM](#): FPGA Acceleration of Multi-Scalar Multiplication
- [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

Teams	Implementations	Supported Hardware Platforms	Full Prover	Open Source
Scroll	PipeZK	ASIC	YES	NO
Ingonyama	PipeMSM, CloudZK, Sparkworks	ASIC, FPGA	YES	NO, YES
Supranational	Sppark	GPU	NO	YES
Aleo (ZPrize)	N/A	GPU, FPGA	NO	YES
Jump Crypto	CycloneMSM, CycloneNTT	FPGA	NO	NO
Cysic	Cysic	FPGA	TBD	NO
cuZK	cuZK	GPU	YES	NO
EdMSM	EdMSM	N/A	NO	NO