Ligero

ZKVM: To Compile Or Precompile

Muthu Venkitasubramaniam

Co-founder/CEO, Ligero Inc.

Our Vision

Useful and Usable Privacy Tools

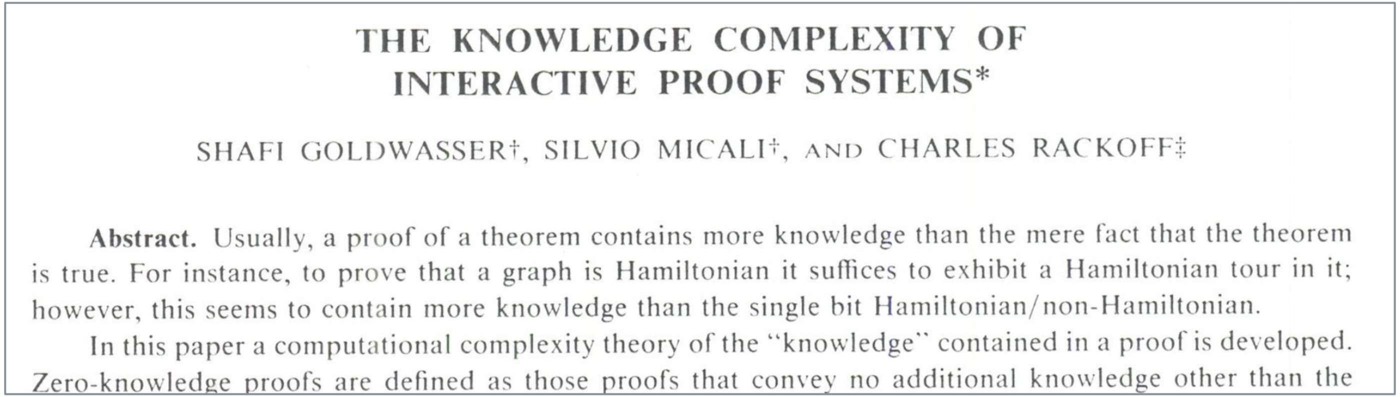
w/ zero infra cost

What if ZK prover cost goes to zero?

✔ Prove quickly, privately, and cheaply

Zero cost = Zero additional cost

On your device/server!



THE KNOWLEDGE COMPLEXITY OF INTERACTIVE PROOF SYSTEMS*

SHAFI GOLDWASSER†, SILVIO MICALI†, AND CHARLES RACKOFF‡

Abstract. Usually, a proof of a theorem contains more knowledge than the mere fact that the theorem is true. For instance, to prove that a graph is Hamiltonian it suffices to exhibit a Hamiltonian tour in it; however, this seems to contain more knowledge than the single bit Hamiltonian/non-Hamiltonian.

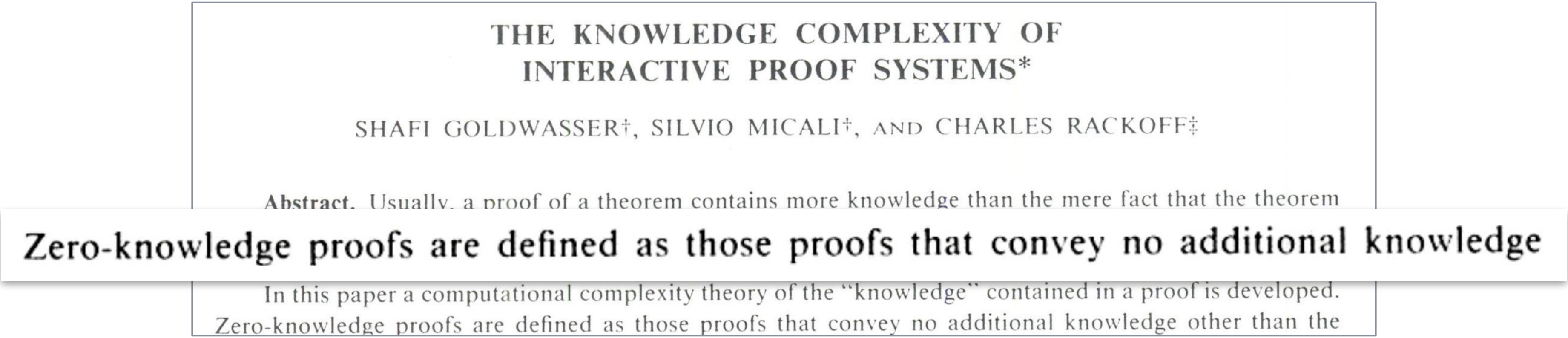
In this paper a computational complexity theory of the "knowledge" contained in a proof is developed. Zero-knowledge proofs are defined as those proofs that convey no additional knowledge other than the

What if ZK prover cost goes to zero?

✔ Prove quickly, privately, and cheaply

Zero cost = Zero additional cost

On your device/server!



THE KNOWLEDGE COMPLEXITY OF INTERACTIVE PROOF SYSTEMS*

SHAFI GOLDWASSER†, SILVIO MICALI†, AND CHARLES RACKOFF‡

Abstract. Usually, a proof of a theorem contains more knowledge than the mere fact that the theorem

Zero-knowledge proofs are defined as those proofs that convey no additional knowledge

In this paper a computational complexity theory of the "knowledge" contained in a proof is developed.

Zero-knowledge proofs are defined as those proofs that convey no additional knowledge other than the

What if ZK prover cost goes to zero?

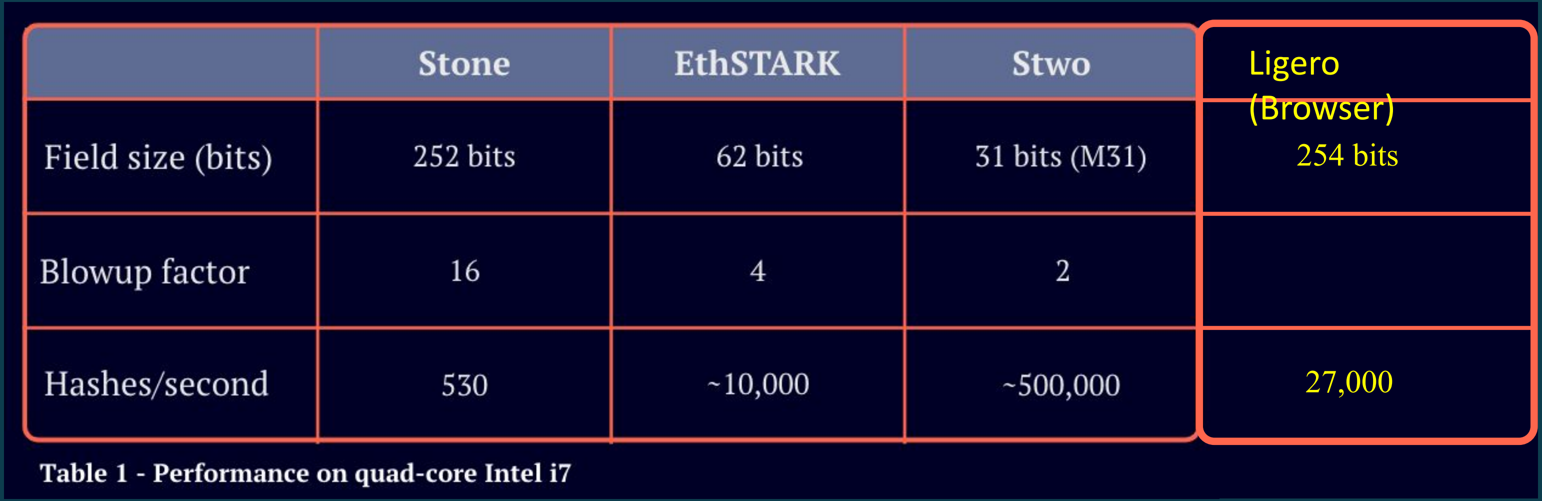
1. Limitless scalability
   - Fast and cheap L2s
   - Real-time Eth proofs by anyone!
2. Solve Interop
3. Verifable/private offchain compute
   - Identity, Oracles, AI, Databases

What can you prove from a browser?

- 1K – Fibonacci (25)
- 1M – Keyless login (Oauth)
- 5M – Proof of Twitter email
- 50M – 5K EdDSA verifications
- 200M – 1M Poseidon hashes
- 1B – Ethereum block proving
- 100B – LLM inference

Ligero

Introducing the Ligero ZK Platform



	Stone	EthSTARK	Stwo	Ligero (Browser)
Field size (bits)	252 bits	62 bits	31 bits (M31)	254 bits
Blowup factor	16	4	2	
Hashes/second	530	~10,000	~500,000	27,000

Table 1 - Performance on quad-core Intel i7

Our Vision

Useful and Usable Privacy Tools

w/ zero additional infra cost

Useful Privacy

Privacy for Individuals = Client-side proving

- Seamless Logins and Authentication (zkLogin, zkEmail)
- Disclosure with Maximal Privacy (zkTLS)
- Verifiable credentials (investor accreditation, EUID, DPP)

Privacy for Orgs = zkValidiums

- Asset Tokenization
- Offchain Compute

Usable Privacy

- Standard toolchain =
- Affordable hardware =
- Portable implementation =
- Privacy-default approach =

Today, Privacy comes with tradeoffs!

Privacy vs Compliance

Does privacy require trading off regulatory compliance?

Privacy vs Cost

Does privacy require access to heavy infrastructure?

Privacy vs Usability

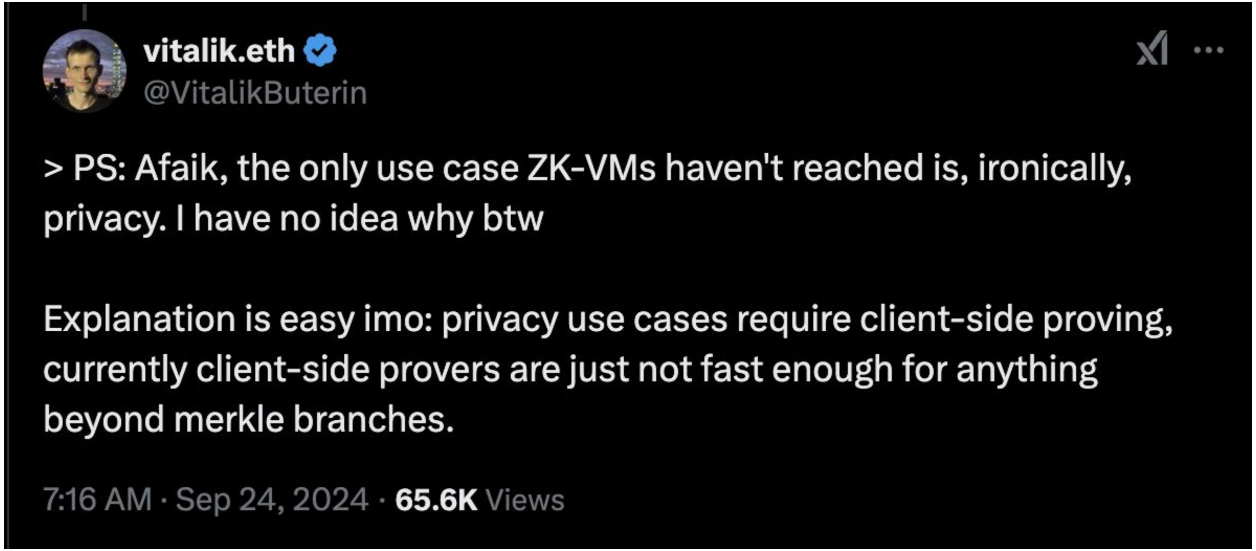
Do we need specialized toolchains to develop privacy solutions?

Privacy vs Trust

Does privacy require trusted intermediaries?

Modern ZK Falls Short

- ZK-SNARKs require huge memory
- STARK-based ZK don’t run client-side yet
- Most ZK’s are built only for verifiability
- ZKs that offer privacy require specialized toolchains



vitalik.eth
@VitalikButerin

> PS: Afaik, the only use case ZK-VMs haven't reached is, ironically, privacy. I have no idea why btw

Explanation is easy imo: privacy use cases require client-side proving, currently client-side provers are just not fast enough for anything beyond merkle branches.

7:16 AM · Sep 24, 2024 · 65.6K Views

We are challenging the status quo!

Ligero

Ligetron: The ZK behind our tech

Ligetron ZK by Ligero Inc.

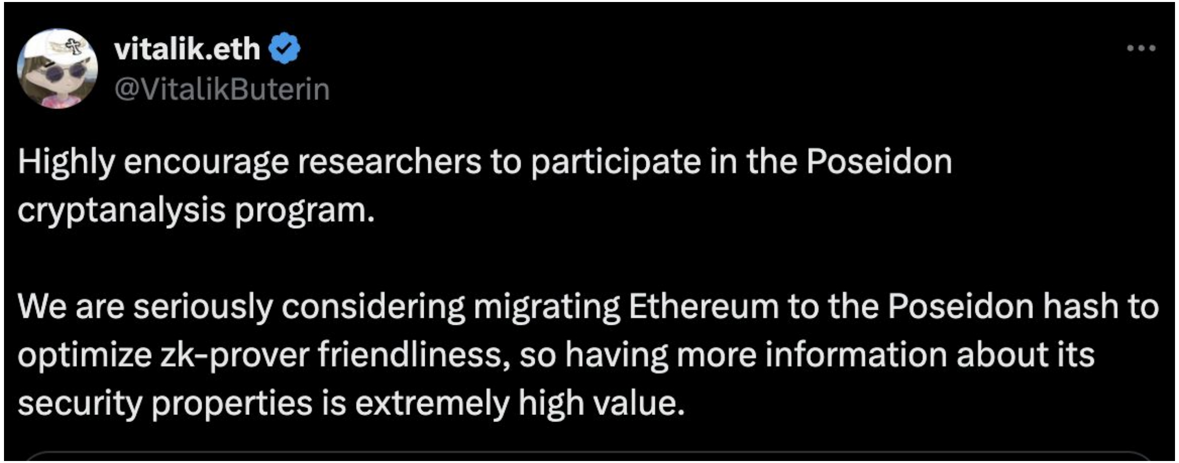
- Ligetron ZK* is (the only) memory-efficient hash-based ZK
- Ligetron is ZK by default
- Ligetron is a zkVM = zkWASM
- A scalable/portable implementation using WebGPUs

* Published at 2024 IEEE Symposium on Security and Privacy

What’s the secret ingredient?

1. Hash-based
2. Code interleaving
   - Sharding without recursive composition
3. Memory-efficiency
   - Witness and constraints can be streamed

Comparison



vitalik.eth
@VitalikButerin

Highly encourage researchers to participate in the Poseidon cryptanalysis program.

We are seriously considering migrating Ethereum to the Poseidon hash to optimize zk-prover friendliness, so having more information about its security properties is extremely high value.

Ligero

M1: 250 KHz – 1 MHz
M4: 500 KHz – 6 MHz

~27,000 Poseidon hash/s

*Hz measures constraints per

Our Roadmap

Today, build end-to-end ZK Apps from your browser using C++, Rust

Coming Soon

- Plug-and-play identity (integrate Circom)
- Scalable privacy: zkValidiums w/ offchain private compute

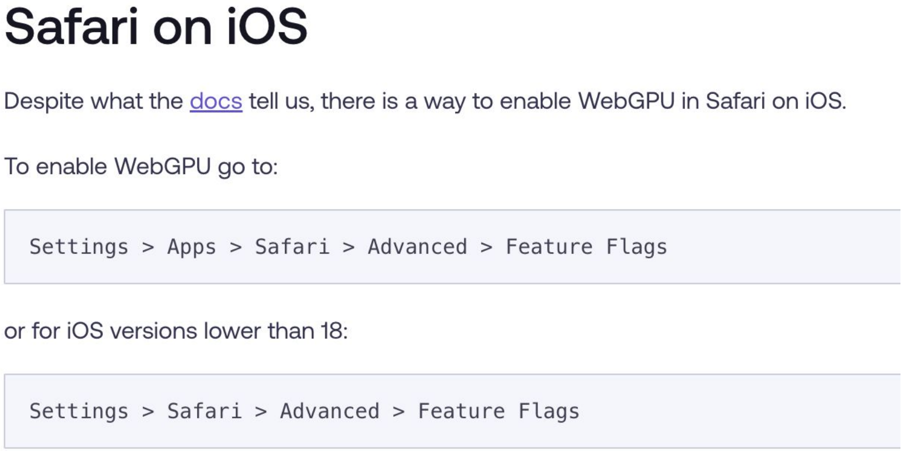
Next, Phase

- Cross-linking zk languages (Noir, Cairo)
- Ethereum block proving
- Arbitrary AI computation (Onnx)

STAY TUNED!

Want to test how fast your browser can generate Ligero proofs?

Open platform.ligetron.com/speedtest



Safari on iOS

Despite what the docs tell us, there is a way to enable WebGPU in Safari on iOS.

To enable WebGPU go to:

```
Settings > Apps > Safari > Advanced > Feature Flags
```

or for iOS versions lower than 18:

```
Settings > Safari > Advanced > Feature Flags
```

Want to test how fast your browser can generate Ligero proofs?

Open platform.ligetron.com/speedtest

Ligero

Ligetron ZK Development Platform

- ✔ Build **Anywhere** – All you need is a browser.
- ✔ Build in **Any Language** – C/C++, Rust, Circom
- ✔ Run **Everywhere** – Mobile, Laptop, Server, Raspberry PI

ZK Anywhere Everywhere

platform.ligetron.com

www.ligero-inc.com

𝕏 @ligero_inc

We are hiring!