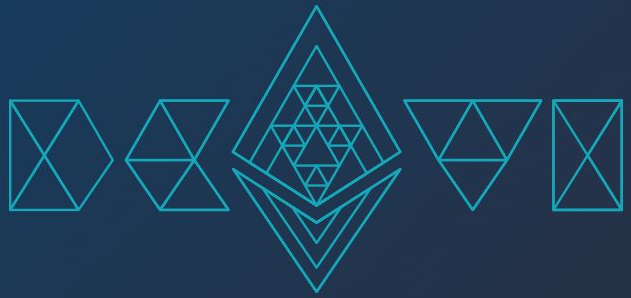


Vampire, a Novel, Cheap to Verify, zkSNARK

Helger Lipmaa
Simula UiB

Janno Siim
Simula UiB

Michał Zając
Nethermind

NETHERMIND

From **Count** to **Vampire**

Vampire

- Novel zkSNARK for **R1CSLite**
- **Universal** and **updatable**
- Based on **Marlin**, but highly optimized
- Only **4G + 2F** elements
- Communication-vise: very close to **Groth16**
- Only two sumchecks

Count

- **Univariate** sumcheck
- Best communication efficiency: **1G**
- Very good computational complexity:
- almost **linear**

How to make SNARKs shorter?

NETHERMIND

zkSNARK **building blocks** and efficiency

Relation

What relation we are showing?

Arithmetization matters

Sumcheck

How many sumchecks do we make?

What sumcheck arguments do we use?

Lincheck

Do we even need them?

PCS

What do we commit to?

What commitments do we open?

NETHERMIND

zkSNARK **building blocks** and efficiency

	Marlin	Vampire
Relation	R1CS	R1CSLite
Sumcheck	2x Aurora	1x Count + 1x Aurora
Lincheck	Yes	Not needed :)
Polynomial commitment scheme	KZG, batched	KZG, highly batched

R1CS vs **R1CSLite**

NETHERMIND

R1CS

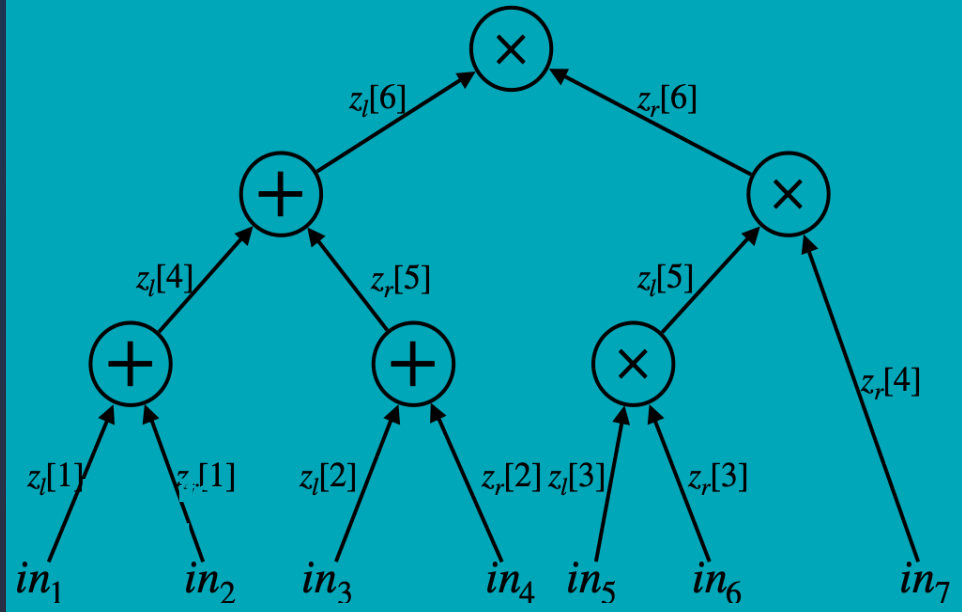
3 matrices
Need to show relation between the matrices **and** about the matrices

$$\underbrace{A \cdot z}_{z_A} \circ \underbrace{B \cdot z}_{z_B} = \underbrace{C \cdot z}_{z_C}$$

R1CSLite

1 matrix

$$Wz = 0$$



$$Wz = 0$$

$$\forall x \sum_y W[x,y]z[y] = 0$$

$$\forall x \sum_y W(x,y)z(y) = 0$$

$$\cdots$$

$$\alpha \leftarrow_{\$} \mathbb{F}$$

$$\sum_y \underbrace{W(\alpha,y)z(y)}_{f(y)} = 0$$

Count - the new sumcheck

NETHERMIND

Count new sumcheck argument

$$\sum_{h \in H} f(h) = v$$

Aurora:

2G

Needs FFT

Count

1G

Doesn't need FFT

Easy to run in parallel

$$\sum_{h \in H} f(h) = v$$

$$\sum_{y \in H} f(y) = f(0) \cdot |H|$$

Assume that the prover cannot send polynomials with non-zero coefficient next to **X^d**

$$g(X) = g_0 + g_1 X + \ldots g_{d-1} X^{d-1} + g_{d+1} X^{d+1} + \ldots$$

$\mathcal{P}$ $\xrightarrow{\quad f'(X) = f(X)X^d - \frac{v}{|H|}X^d \quad}$ $\mathcal{V}$

$$f(X) = f_0 + f_1 X + \ldots f_k X^k$$

$$f'(X) = f_0 X^d - \frac{v}{|H|} X^d + f_1 X^{d+1} + \ldots$$

Highly batched **KZG**

NETHERMIND

What we can **batch**?

Batch openings of **multiple** polynomials evaluated at a **single** point

$$f_1(z), f_2(z), \ldots, f_k(z)$$

Batch openings of **multiple** polynomials at **multiple** points

$$f_1(z_1), f_2(z_2), \ldots, f_k(z_k)$$

eprint.iacr.org/2022/**406**.pdf

NETHERMIND

michal@nethermind.io

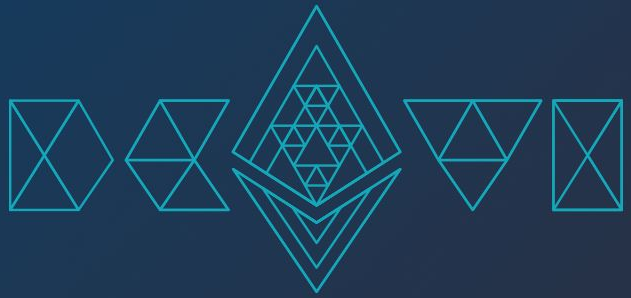
Counting Vampires: From Univariate Sumcheck to Updatable ZK-SNARK*

Version 2.0, Thursday 23rd June, 2022, 12:58

Helger Lipmaa[1], Janno Siim[1], and Michał Zając[2]

[1] Simula UiB, Bergen, Norway
[2] Nethermind, London, UK

NETHERMIND



Thank you!

Michał Zając

Nethermind

michal@nethermind.io

@mpfzajac