Vampire, a Novel, Cheap to Verify, zkSNARK

Helger Lipmaa  
Simula UiB

Janno Siim  
Simula UiB

Michał Zając  
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?
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?
<table>
<thead>
<tr>
<th>zkSNARK building blocks and efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relation</strong></td>
</tr>
<tr>
<td>R1CS</td>
</tr>
<tr>
<td><strong>Sumcheck</strong></td>
</tr>
<tr>
<td><strong>Lincheck</strong></td>
</tr>
<tr>
<td><strong>Polynomial commitment scheme</strong></td>
</tr>
</tbody>
</table>
R1CS vs R1CSSLite
R1CS
3 matrices
Need to show relation between the matrices and about the matrices

\[ A \cdot z \odot B \cdot z = C \cdot z \]

\[ \{ z, z_A, z_B, z_C \} \]

R1CSLite
1 matrix

\[ Wz = 0 \]
\[ W z = 0 \]

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

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

\[ \sum_y W(\alpha, y) z(y) = 0 \]

\[ \alpha \leftarrow F \]
Count - the new sumcheck
$\sum_{h \in H} f(h) = \nu$

**Aurora:**
- 2G
- Needs FFT

**Count**
- 1G
- Doesn’t need FFT
- Easy to run in parallel

*Count* new sumcheck argument
\[ \sum_{h \in H} f(h) = v \]

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

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

\[ f'(X) = f(X) X^d - \frac{v}{|H|} X^d \]

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

\[ f'(X) = f_0 X^d - \frac{v}{|H|} X^d + f_1 X^{d+1} + \ldots \]
Highly batched KZG
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

\[ f_1(z_1), f_2(z_2), \ldots, f_k(z_k) \]
Counting Vampires: From Univariate Sumcheck to Updatable ZK-SNARK*

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

Helger Lipmaa¹, Janno Siim¹, and Michał Zając²

¹ Simula UiB, Bergen, Norway
² Nethermind, London, UK
Thank you!

Michał Zając
Nethermind
michal@nethermind.io

@mpfzajac