Flashproofs
Efficient Zero-Knowledge Arguments of Range & Polynomial Evaluation with Transparent Setup

Nan Wang and Sid Chi-Kin Chau

Asiacrypt 2022
Our contributions

- Discrete logarithm (DL) assumption
- Transparent (non-trusted) setup
- $\Sigma$-protocol
- No pairing operations

- Zero-Knowledge Argument of Range
  - proves a committed value $x$ lies in a specific range
  - $x \in [0, 2^{32} - 1], x \in [0, 2^{64} - 1]$

- Zero-Knowledge Argument of Polynomial Evaluation
  - proves two committed values $x$ and $y$ satisfy a public polynomial relation
  \[ y = x^{64} + 1, y = \prod_{i=1}^{64} (x - i) = 0 \]
Zero-Knowledge Argument of Knowledge

• A zero-knowledge proof allows a prover to convince a verifier of the truth of a statement without revealing any secret information.

• An argument is computationally sound proof that no probabilistic polynomial-time provers are able to deceive a verifier into falsely accepting it.

• More formally, given an NP-language L, a prover aims to convince a verifier of knowing a witness $\omega$ for a statement $u \in L$.
  
  • Completeness: A prover can convince a verifier of $u \in L$, if $u \in L$
  
  • Soundness: A prover cannot convince a verifier of $u \in L$, if $u \not\in L$.

  • Zero-knowledge: The proof reveals nothing except the truth that $u \in L$. 
### Σ-Protocol

- An efficient approach for constructing honest verifier zero-knowledge proofs
- 3-round interactive protocol
- Non-interactive protocol via Fiat-Shamir transform

![Diagram of Σ-Protocol]

<table>
<thead>
<tr>
<th>Prover</th>
<th>Verifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>sends a message $m$</td>
<td>replies with a random challenge $e$</td>
</tr>
<tr>
<td>common input $u$</td>
<td>responds with $z$</td>
</tr>
</tbody>
</table>

accept or reject based on $(u, m, e, z)$
Zero-Knowledge Arguments of Range

- Prove a committed value is in the range $[0, 2^N - 1]$
- A new variant of the bit-decomposition approach
- Tailored to confidential transactions on blockchain platforms
- Prove the transfer amount is non-negative and the balance has sufficient funds for the transfer amount
- $O(N^{2/3})$ communication and verification efficiency
- Achieve comparable verification gas costs to that of the most efficient zkSNARK (Groth16)
- Support the aggregation of multiple arguments for further efficiency improvement
Bit-Decomposition

\[ y = \sum_{i=0}^{N-1} 2^i b_i, \quad b_i \in \{0,1\} \implies y \in [0,2^N - 1] \]

- Bulletproof is a popular generic-purpose zero-knowledge argument, which can instantiate a zero-knowledge range argument.
- It uses a variant of the bit-decomposition approach to achieve O(log N) communication cost and O(N) proving and verification.
Our Technique

Prover:

\[ y = \sum_{i=0}^{N-1} 2^ib_i \Rightarrow \begin{pmatrix}
2^0b_0 & \cdots & 2^{K-1}b_{K-1} \\
2^Kb_K & \cdots & 2^{K+K-1}b_{K+K-1} \\
\vdots & \ddots & \vdots \\
2^{(L-1)K}b_{(L-1)K} & \cdots & 2^{(L-1)K+K-1}b_{(L-1)K+K-1}
\end{pmatrix} = \begin{pmatrix}
w_0 & \cdots & w_{K-1} \\
w_K & \cdots & w_{K+K-1} \\
\vdots & \ddots & \vdots \\
w_{(L-1)K} & \cdots & w_{(L-1)K+K-1}
\end{pmatrix}
\]

\[
\begin{pmatrix}
w_0 & \cdots & w_{K-1} \\
w_K & \cdots & w_{K+K-1} \\
\vdots & \ddots & \vdots \\
w_{(L-1)K} & \cdots & w_{(L-1)K+K-1}
\end{pmatrix} \cdot \begin{pmatrix}
e_0 \\
\vdots \\
e_{K-1}
\end{pmatrix} + \begin{pmatrix}
r_0 \\
\vdots \\
r_{L-1}
\end{pmatrix} = \begin{pmatrix}
v_0 \\
\vdots \\
v_{L-1}
\end{pmatrix}
\]

\[ v_l = \sum_{k=0}^{K-1} w_{lK+k}e_k + r_l \]

Verifier:

\[ f_l = \sum_{k=0}^{K-1} 2^{lK+k}e_k - v_l = \sum_{k=0}^{K-1} (2^{lK+k} - w_{lK+k})e_k - r_l \]
Our Technique

(1) \[ f_l \cdot v_l = \sum_{k=0}^{K-1} w_{lK+k}(2^{lK+k} - w_{lK+k})e_k^2 + \left(\sum_{k=0, j=1}^{k=K-2} t_{k,j}e_{k,j} + \sum_{k=0}^{K-1} q_k e_k + q_K\right) \quad e_{k,j} = e_k \cdot e_j, \quad k \neq j \]

\[ w_{lK+k}(2^{lK+k} - w_{lK+k}) = 0 \implies w_{lK+k} \in \{0, 2^{lK+k}\} \]

(2) \[ \sum_{l=0}^{L-1} v_l = \sum_{k=0}^{K-1} s_k e_k + s_K, \quad s_k = \sum_{l=0}^{L-1} w_{lK+k}, \quad s_K = \sum_{l=0}^{L-1} r_l \]

(3) \[ y = \sum_{k=0}^{K-1} s_k \]

When \( K \approx \lfloor N^{\frac{1}{3}} \rfloor \), both communication and verification costs achieve the minimum.

\[ |\Pi| = L + 2K + \frac{K(K-1)}{2} + 4 = \left\lfloor \frac{N}{K} \right\rfloor + \frac{K^2}{2} + \frac{3K}{2} + 4 \]
Our Optimisation Technique

64-bit: \((e_k)_{k=0}^{K-1} = (e^{-1}, e, e^4, e^5)\)

\[ f_l \cdot v_l = w_{10} e^{10} + w_8 e^8 + w_5 e^2 + w_-2 e^{-2} \]

\[ + w_9 e^9 + w_6 e^6 + w_5 e^5 + w_4 e^4 + w_3 e^3 + w_1 e + w_-1 e^{-1} + w_0 \]

\(=0\)

<table>
<thead>
<tr>
<th>(a) Values of ((L, K))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(N)</td>
</tr>
<tr>
<td>(L)</td>
</tr>
<tr>
<td>(K)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(b) Comparison of range arguments for 64-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Original Work</td>
</tr>
<tr>
<td>Optimised Work</td>
</tr>
<tr>
<td>Saving</td>
</tr>
</tbody>
</table>
# Efficiency Comparison with Bulletproof

<table>
<thead>
<tr>
<th></th>
<th>$N$</th>
<th>8</th>
<th>10</th>
<th>12</th>
<th>14</th>
<th>16</th>
<th>18</th>
<th>20</th>
<th>22</th>
<th>32</th>
<th>52</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prover</strong></td>
<td>Bulletproof</td>
<td>116</td>
<td>238</td>
<td>238</td>
<td>238</td>
<td>238</td>
<td>480</td>
<td>480</td>
<td>480</td>
<td>480</td>
<td>962</td>
<td>962</td>
</tr>
<tr>
<td>No. of Exp ($G$)</td>
<td>This work</td>
<td>21</td>
<td>24</td>
<td>27</td>
<td>30</td>
<td>33</td>
<td>36</td>
<td>39</td>
<td>42</td>
<td>80</td>
<td>122</td>
<td>146</td>
</tr>
<tr>
<td><strong>Verifier</strong></td>
<td>Bulletproof</td>
<td>56</td>
<td>98</td>
<td>98</td>
<td>98</td>
<td>98</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>342</td>
<td>342</td>
</tr>
<tr>
<td>No. of Exp ($G$)</td>
<td>This work</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>22</td>
<td>27</td>
<td>30</td>
</tr>
<tr>
<td><strong>Proof Size</strong></td>
<td>(Byte)</td>
<td>Bulletproof</td>
<td>482</td>
<td>546</td>
<td>546</td>
<td>546</td>
<td>546</td>
<td>610</td>
<td>610</td>
<td>610</td>
<td>610</td>
<td>674</td>
</tr>
<tr>
<td></td>
<td>This work</td>
<td>385</td>
<td>417</td>
<td>449</td>
<td>481</td>
<td>513</td>
<td>545</td>
<td>577</td>
<td>609</td>
<td>738</td>
<td>898</td>
<td>994</td>
</tr>
</tbody>
</table>

![Graph showing efficiency comparison between Flashproof and Bulletproof](image)
# Gas Cost Comparison

<table>
<thead>
<tr>
<th>Type</th>
<th>Transparent Setup</th>
<th>Gas Cost</th>
<th>Ether</th>
<th>USD</th>
<th>Proof Size (Byte)</th>
</tr>
</thead>
<tbody>
<tr>
<td>zkSNARK (Groth16)</td>
<td>✗</td>
<td>220,100</td>
<td>0.0033</td>
<td>$5.8</td>
<td>192</td>
</tr>
<tr>
<td>This work (32-bit)</td>
<td>✓</td>
<td>233,250</td>
<td>0.0035</td>
<td>$6.1</td>
<td>738</td>
</tr>
<tr>
<td>This work (64-bit)</td>
<td>✓</td>
<td>314,140</td>
<td>0.00471</td>
<td>$8.2</td>
<td>994</td>
</tr>
<tr>
<td>CKLR21 (32-bit)*</td>
<td>✓</td>
<td>330,868</td>
<td>0.00496</td>
<td>$8.7</td>
<td>827</td>
</tr>
<tr>
<td>CKLR21 (64-bit)*</td>
<td>✓</td>
<td>454,301</td>
<td>0.00681</td>
<td>$11.9</td>
<td>964</td>
</tr>
<tr>
<td>zkSNARK (SONIC, Helped)*</td>
<td>✗</td>
<td>492,000</td>
<td>0.00738</td>
<td>$12.9</td>
<td>385</td>
</tr>
<tr>
<td>zkSNARK (SONIC, Unhelped)*</td>
<td>✗</td>
<td>655,000</td>
<td>0.00983</td>
<td>$17.2</td>
<td>1155</td>
</tr>
<tr>
<td>zkSNARK (BCTV14)</td>
<td>✗</td>
<td>773,124</td>
<td>0.0116</td>
<td>$20.2</td>
<td>288</td>
</tr>
<tr>
<td>Bulletproofs (32-bit)</td>
<td>✓</td>
<td>2,046,252</td>
<td>0.03069</td>
<td>$53.6</td>
<td>610</td>
</tr>
<tr>
<td>Bulletproofs (64-bit)</td>
<td>✓</td>
<td>3,703,549</td>
<td>0.05555</td>
<td>$96.9</td>
<td>674</td>
</tr>
</tbody>
</table>

- Gas price: 15 gwei (Etherscan), Ether price: $1745 USD (Coindesk), UTC 11:15 am 12/09/2022
- * indicates the gas costs are estimated
Zero-Knowledge Argument of Polynomial Evaluation

- Builds on the work of Bayer & Groth (BG13, Eurocrypt 13)

- Two zero-knowledge protocols optimised for the polynomials of lower-degree $N \in [3,2^9]$ and higher-degree $N > 2^9$.

- Instantiates the membership argument by constructing a polynomial function
  \[ y = \prod_{i=1}^{I} (x - i) = 0 \text{ for a public list } i \in [1,\ldots,I]. \]

- Combined with the range argument, it can be used to satisfy complex mathematical relations by leveraging the Maclaurin series

  \[
  y = \sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} \ldots
  \]

  \[
  y = e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} \ldots
  \]

- Achieves $O(\sqrt{\log N})$ efficiency in communication and verification (group exponentiation) for the aggregation of multiple arguments satisfying different polynomial relations and sharing the same inputs
# Efficiency Comparison

<table>
<thead>
<tr>
<th>Type</th>
<th>Bulletproofs</th>
<th>BG13</th>
<th>This Work (4.2) ( \text{Lower-Deg } N \in [3, 2^9] )</th>
<th>This Work (4.3) ( \text{Higher-Deg } N &gt; 2^9 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prover No. of Exp (( \mathbb{G} ))</td>
<td>15( N + 2 \log N - 10 )</td>
<td>8 ( \log N - 4 )</td>
<td>4 ( \log N + 2 )</td>
<td>3 ( \log N + 3 \sqrt{\log N} + 2 )</td>
</tr>
<tr>
<td>Verifier No. of Exp (( \mathbb{G} ))</td>
<td>5( N + 2 \log N + 10 )</td>
<td>7 ( \log N - 1 )</td>
<td>2 ( \log N + 7 )</td>
<td>( \log N + 3 \sqrt{\log N} + 6 )</td>
</tr>
<tr>
<td>Proof Size No. of Elements</td>
<td>2 ( \log N + 8 ) (( \mathbb{G} ))</td>
<td>4 ( \log N - 2 ) (( \mathbb{G} ))</td>
<td>( \log N + 3 ) (( \mathbb{G} ))</td>
<td>2 ( \sqrt{\log N} + 3 ) (( \mathbb{G} ))</td>
</tr>
<tr>
<td>No. of Elements</td>
<td>5 (( \mathbb{Z}_p ))</td>
<td>3 ( \log N ) (( \mathbb{Z}_p ))</td>
<td>( \log N + 3 ) (( \mathbb{Z}_p ))</td>
<td>( \log N + \sqrt{\log N} + 4 ) (( \mathbb{Z}_p ))</td>
</tr>
</tbody>
</table>

![Graph showing running time vs. degree of univariate monomials](image.png)
Thanks!