## Benchmarking Results

The table below presents benchmarking results for various cryptographic schemes, categorized by proof-of-concept (PoC) implementations. The results are visualized in a heat map, with time (cycles) on the horizontal axis and ciphertext size (bytes) on the vertical axis.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>PoC</th>
<th>Time (cycles)</th>
<th>Ciphertext Size (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto_kem</td>
<td></td>
<td>10</td>
<td>100</td>
</tr>
<tr>
<td>mceliece8192128</td>
<td></td>
<td>15</td>
<td>150</td>
</tr>
<tr>
<td>kyber90s768</td>
<td></td>
<td>20</td>
<td>200</td>
</tr>
<tr>
<td>sntrup653</td>
<td></td>
<td>25</td>
<td>250</td>
</tr>
<tr>
<td>ntrulpr857</td>
<td></td>
<td>30</td>
<td>300</td>
</tr>
<tr>
<td>ntruhps2048509</td>
<td></td>
<td>35</td>
<td>350</td>
</tr>
<tr>
<td>ntrulpr4591761</td>
<td></td>
<td>40</td>
<td>400</td>
</tr>
<tr>
<td>ntruhps4096821</td>
<td></td>
<td>45</td>
<td>450</td>
</tr>
<tr>
<td>ntruhps2048677</td>
<td></td>
<td>50</td>
<td>500</td>
</tr>
<tr>
<td>mceliece6688128</td>
<td></td>
<td>55</td>
<td>550</td>
</tr>
<tr>
<td>mceliece6688128f</td>
<td></td>
<td>60</td>
<td>600</td>
</tr>
<tr>
<td>mceliece348864</td>
<td></td>
<td>65</td>
<td>650</td>
</tr>
<tr>
<td>mceliece348864pcf</td>
<td></td>
<td>70</td>
<td>700</td>
</tr>
<tr>
<td>mceliece460896pc</td>
<td></td>
<td>75</td>
<td>750</td>
</tr>
<tr>
<td>mceliece460896</td>
<td></td>
<td>80</td>
<td>800</td>
</tr>
<tr>
<td>MHEY</td>
<td></td>
<td>85</td>
<td>850</td>
</tr>
<tr>
<td>RIVET</td>
<td></td>
<td>90</td>
<td>900</td>
</tr>
<tr>
<td>ntrukem443</td>
<td></td>
<td>95</td>
<td>950</td>
</tr>
<tr>
<td>ntrukem743</td>
<td></td>
<td>100</td>
<td>1000</td>
</tr>
<tr>
<td>ntrukem13136</td>
<td></td>
<td>105</td>
<td>1050</td>
</tr>
<tr>
<td>ntrukem1380</td>
<td></td>
<td>110</td>
<td>1100</td>
</tr>
<tr>
<td>ntrukem1380comp</td>
<td></td>
<td>115</td>
<td>1150</td>
</tr>
<tr>
<td>ntrukem443comp</td>
<td></td>
<td>120</td>
<td>1200</td>
</tr>
<tr>
<td>ntrukem743comp</td>
<td></td>
<td>125</td>
<td>1250</td>
</tr>
<tr>
<td>ntrukem13136comp</td>
<td></td>
<td>130</td>
<td>1300</td>
</tr>
<tr>
<td>ntrukem1380comp</td>
<td></td>
<td>135</td>
<td>1350</td>
</tr>
<tr>
<td>ntrukem443comp</td>
<td></td>
<td>140</td>
<td>1400</td>
</tr>
<tr>
<td>ntrukem743comp</td>
<td></td>
<td>145</td>
<td>1450</td>
</tr>
<tr>
<td>ntrukem13136comp</td>
<td></td>
<td>150</td>
<td>1500</td>
</tr>
<tr>
<td>ntrukem1380comp</td>
<td></td>
<td>155</td>
<td>1550</td>
</tr>
<tr>
<td>ntrukem443comp</td>
<td></td>
<td>160</td>
<td>1600</td>
</tr>
<tr>
<td>ntrukem743comp</td>
<td></td>
<td>165</td>
<td>1650</td>
</tr>
<tr>
<td>ntrukem13136comp</td>
<td></td>
<td>170</td>
<td>1700</td>
</tr>
<tr>
<td>ntrukem1380comp</td>
<td></td>
<td>175</td>
<td>1750</td>
</tr>
<tr>
<td>ntrukem443comp</td>
<td></td>
<td>180</td>
<td>1800</td>
</tr>
<tr>
<td>ntrukem743comp</td>
<td></td>
<td>185</td>
<td>1850</td>
</tr>
<tr>
<td>ntrukem13136comp</td>
<td></td>
<td>190</td>
<td>1900</td>
</tr>
<tr>
<td>ntrukem1380comp</td>
<td></td>
<td>195</td>
<td>1950</td>
</tr>
<tr>
<td>ntrukem443comp</td>
<td></td>
<td>200</td>
<td>2000</td>
</tr>
</tbody>
</table>

### Notes:
- "C:" means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive.
- "T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.