Code-Beispiele: Darstellungsvarianten

Demo

August 10, 2025

1 Inline und kurzer Block

Inline-Befehl im Text: `zokrates compile -i circuits/basic/filter_range.zok`.

Kurzer Block ohne Rahmen:

```
zokrates compile -i circuits/basic/filter_range.zok -o filter_range.out
zokrates setup
zokrates compute-witness -a 42 0 100
zokrates generate-proof
```

2 Frameder Code mit Hintergrund

Success

```
python -m venv iot_zk_env && source iot_zk_env/bin/activate && pip install -r
    requirements.txt
bash build_zokrates_nova.sh
bash run_evaluation.sh --phase compile
```

3 Nummerierte Schritte mit Snippets

1. Kompilieren

   Info

   ```
   [listing only,numbers=none]
   zokrates compile -i circuits/basic/min_max.zok
   ```

2. Beweis erzeugen

   Info

   ```
   [listing only,numbers=none]
   zokrates generate-proof
   ```

3. Verifizieren

Warning

```
[listing only,numbers=none]
zokrates verify
```

4 Zweispaltig: Code links, Erklärung rechts

```
def _prepare_circuit_inputs(readings, batch_size):
    filtered = [r for r in readings if 0 <= r <= 100]
    return [filtered[i:i+batch_size] for i in range(0, len(filtered), batch_size)]
```

Erläuterung: Beispielhafte Batching-Funktion (Python). Erst Filterung, dann Gruppen in Blöcke der Größe *batch_size*.

5 Pseudocode mit algorithmicx

Algorithm 1 Systemauswahl in Abhängigkeit von Datenmenge und RAM

Input: n (Datenmenge), M (RAM), R (Echtzeitanforderung)
if $M < 10\,\text{MB}$ **then**
    Wähle **Recursive SNARKs** (RAM-limitierte Umgebung)
else if $n < 85$ and $R =$ hoch **then**
    Wähle **Standard SNARKs** (geringe Latenz)
else if $85 \leq n \leq 171$ **then**
    Fall-zu-Fall-Entscheidung (Speicher/Netz/Privacy)
else
    Wähle **Recursive SNARKs**
end if

6 Hybrid: Pseudocode mit farbigem Info-Header

Recursive vs. Standard Selection

Input: n (items), M (RAM in MB), R (real-time)
Hint: Prefer recursion if memory is the bottleneck or $n > 171$.

Input: n, M, R
if $M < 10\,\text{MB}$ **then**
    Choose Recursive SNARKs (RAM constraint)
else if $n < 85$ and $R =$ critical **then**
    Choose Standard SNARKs (low latency)
else if $85 \leq n \leq 171$ **then**
    Evaluate storage/network/privacy trade-offs
else
    Choose Recursive SNARKs
end if

Command: `bash run_evaluation.sh -phase compile`

7 Lange Zeile mit automatischem Umbruch

```
python demo.py --input data/raw/iot_readings_1_month.json --batch-size 240 --prove
    recursive --export /home/ramon/bachelor/data/visualizations --log-level INFO
```