

```

Last login: Mon Mar 14 14:06:22 on ttys001
→ ~ cd /Users/shming/Documents/MerkleTreeCircuit
→ MerkleTreeCircuit circom merklecircuit.circom --r1cs --wasm --sym --c
template instances: 1
non-linear constraints: 0
linear constraints: 0
public inputs: 4
public outputs: 1
private inputs: 7
private outputs: 0
wires: 12
labels: 13
Written successfully: ./merklecircuit.r1cs
Written successfully: ./merklecircuit.sym
Written successfully: ./merklecircuit_cpp/merklecircuit.cpp and ./merklecircuit_
cpp/merklecircuit.dat
Written successfully: ./merklecircuit_cpp/main.cpp, circom.hpp, calcwit.hpp, cal
cwit.cpp, fr.hpp, fr.cpp, fr.asm and Makefile
Written successfully: ./merklecircuit_js/merklecircuit.wasm
Everything went okay, circom safe
→ MerkleTreeCircuit

```

```

→ MerkleTreeCircuit ./execute_4circuit.sh
zsh: permission denied: ./execute_4circuit.sh
→ MerkleTreeCircuit chmod +x ./execute_4circuit.sh
→ MerkleTreeCircuit ./execute_4circuit.sh
./execute_4circuit.sh: line 1: //Creating: No such file or directory
./execute_4circuit.sh: line 2: //circom: No such file or directory
/Users/shming/Documents/MerkleTreeCircuit/merklecircuit_js/witness_calculator.js:123
    throw new Error(`Not all inputs have been set. Only ${input_counter} out of ${this.instance.exports.getInputSize()}`);
    ^
Error: Not all inputs have been set. Only 4 out of 11
    at WitnessCalculator._doCalculateWitness (/Users/shming/Documents/MerkleTreeCircuit/merklecircuit_js/witness_calculator.js:123:12)
    at WitnessCalculator.calculateWTNSBin (/Users/shming/Documents/MerkleTreeCircuit/merklecircuit_js/witness_calculator.js:168:20)
    at /Users/shming/Documents/MerkleTreeCircuit/merklecircuit_js/generate_witness.js:15:38

Node.js v17.6.0
cp: witness.wtns: No such file or directory
[DEBUG] snarkJS: tauG1: 100000
[DEBUG] snarkJS: Calculating First Challenge Hash
[DEBUG] snarkJS: Calculate Initial Hash: tauG1
[DEBUG] snarkJS: Calculate Initial Hash: tauG2
[DEBUG] snarkJS: Calculate Initial Hash: alphaTauG1
[DEBUG] snarkJS: Calculate Initial Hash: betaTauG1
[DEBUG] snarkJS: Blank Contribution Hash:
786a02f7 42015903 c6c6fd85 2552d272
912f4740 e1584761 8a86e217 f71f5419
d25e1031 afee5853 13896444 934eb04b
903a685b 1448b755 d56f701a fe9be2ce
[INFO] snarkJS: First Contribution Hash:
e27d7e51 abd16bb3 c46609c7 5e963b5f
dbe25b00 c0b93a4c 528b569a d4b50fda
d9926ff2 781f4bae fac213db 214f30af
e681f7be 5c1f973c c567c817 e871f958
Enter a random text. (Entropy):

```

```
Enter a random text. (Entropy): fewfwefwguiweriu
[DEBUG] snarkJS: Calculating First Challenge Hash
[DEBUG] snarkJS: Calculate Initial Hash: tauG1
[DEBUG] snarkJS: Calculate Initial Hash: tauG2
[DEBUG] snarkJS: Calculate Initial Hash: alphaTauG1
[DEBUG] snarkJS: Calculate Initial Hash: betaTauG1
[DEBUG] snarkJS: processing: tauG1: 0/131071
[DEBUG] snarkJS: processing: tauG1: 16384/131071
[DEBUG] snarkJS: processing: tauG1: 32768/131071
[DEBUG] snarkJS: processing: tauG1: 49152/131071
[DEBUG] snarkJS: processing: tauG1: 65536/131071
[DEBUG] snarkJS: processing: tauG1: 81920/131071
[DEBUG] snarkJS: processing: tauG1: 98304/131071
[DEBUG] snarkJS: processing: tauG1: 114688/131071
[DEBUG] snarkJS: processing: tauG2: 0/65536
[DEBUG] snarkJS: processing: tauG2: 8192/65536
[DEBUG] snarkJS: processing: tauG2: 16384/65536
[DEBUG] snarkJS: processing: tauG2: 24576/65536
[DEBUG] snarkJS: processing: tauG2: 32768/65536
[DEBUG] snarkJS: processing: tauG2: 40960/65536
[DEBUG] snarkJS: processing: tauG2: 49152/65536
[DEBUG] snarkJS: processing: tauG2: 57344/65536
[DEBUG] snarkJS: processing: alphaTauG1: 0/65536
[DEBUG] snarkJS: processing: alphaTauG1: 16384/65536
[DEBUG] snarkJS: processing: alphaTauG1: 32768/65536
[DEBUG] snarkJS: processing: alphaTauG1: 49152/65536
[DEBUG] snarkJS: processing: betaTauG1: 0/65536
[DEBUG] snarkJS: processing: betaTauG1: 16384/65536
[DEBUG] snarkJS: processing: betaTauG1: 32768/65536
[DEBUG] snarkJS: processing: betaTauG1: 49152/65536
[DEBUG] snarkJS: processing: betaTauG2: 0/1
[INFO] snarkJS: Contribution Response Hash imported:
      1d95726e b077ef62 896bf1ed c9476bf1
      9b351f7e 0b95e00e 3584ffe2 7450f844
      e4aa6f7a 48f76b8a f4dabcd9 a65b591f
      dac07e2a 181aa7d5 2cf8269a 0b7bc01d
[INFO] snarkJS: Next Challenge Hash:
      5c4e531f 9bf06e8d 4ff70cec 8bf853b0
      e5b05629 4f0987a4 67f43bfe 3022993f
      0a0e683b 5c3ce756 f03f2657 544489bc
      e12af666 61076329 70f1cff7 d74c0e9d
[DEBUG] snarkJS: Starting section: tauG1
[DEBUG] snarkJS: tauG1: fft 0 mix start: 0/1
[DEBUG] snarkJS: tauG1: fft 0 mix end: 0/1
[DEBUG] snarkJS: tauG1: fft 1 mix start: 0/1
[DEBUG] snarkJS: tauG1: fft 1 mix end: 0/1
[DEBUG] snarkJS: tauG1: fft 2 mix start: 0/1
[DEBUG] snarkJS: tauG1: fft 2 mix end: 0/1
[DEBUG] snarkJS: tauG1: fft 3 mix start: 0/1
[DEBUG] snarkJS: tauG1: fft 3 mix end: 0/1
```

[DEBUG] snarkJS: betaTauG1: fft 16 join 16/16 1/1 1/4

[INFO] snarkJS: Reading r1cs

[INFO] snarkJS: Reading tauG1

[INFO] snarkJS: Reading tauG2

[INFO] snarkJS: Reading alphatauG1

[INFO] snarkJS: Reading betatauG1

[INFO] snarkJS: Circuit hash:

6b1dcd86 b76c77e3 02bc52fa bea77164

8dc697d9 b5f77ac6 4bd1807d eff444b4

e963330c 435312d9 70a010ae c7ca7a4b

df1dda4c ada67287 6b472003 0dd35929