§ Groth16

witnesses

① What transformations the inputs go through ?

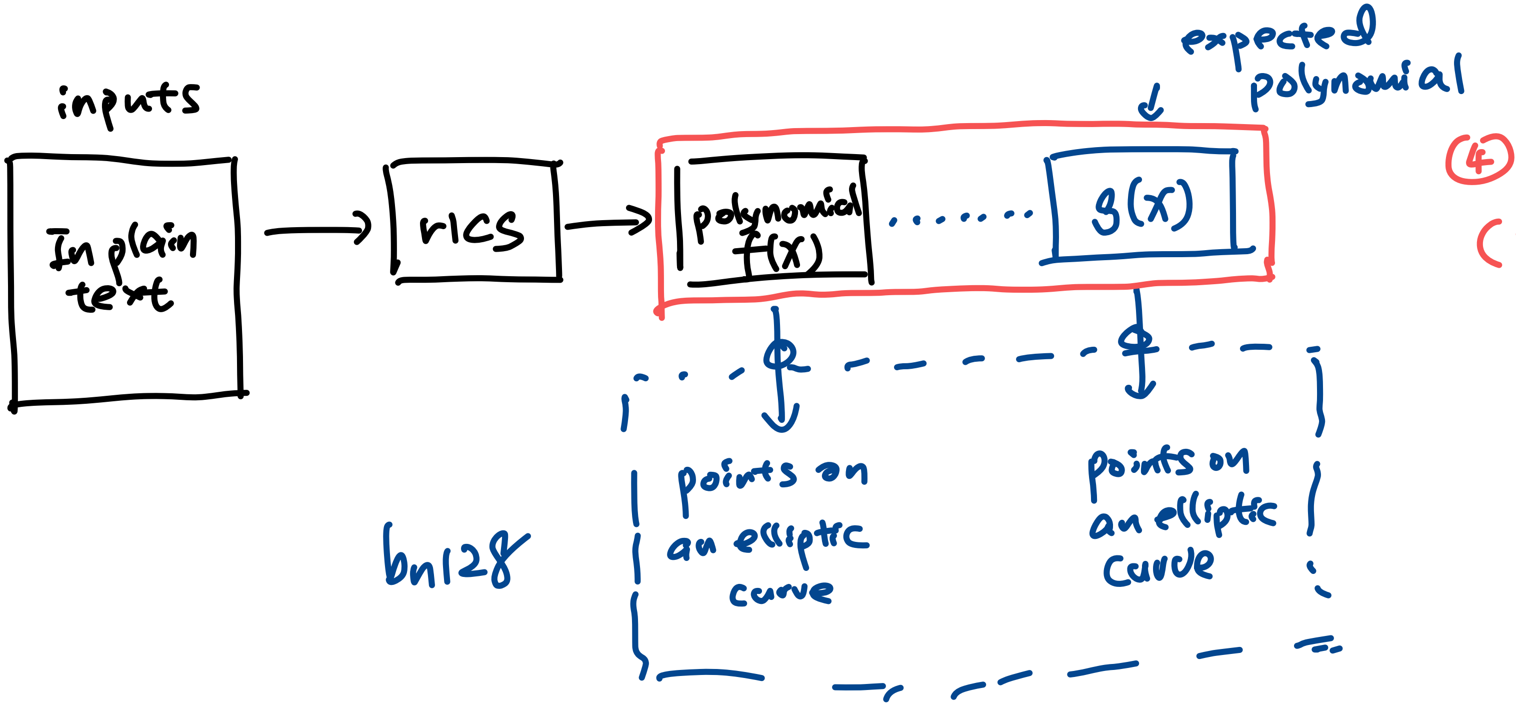
② What is the alternative proving statement .

③ What makes it work ?

- Polynomial Comparison

④ Trusted Setup

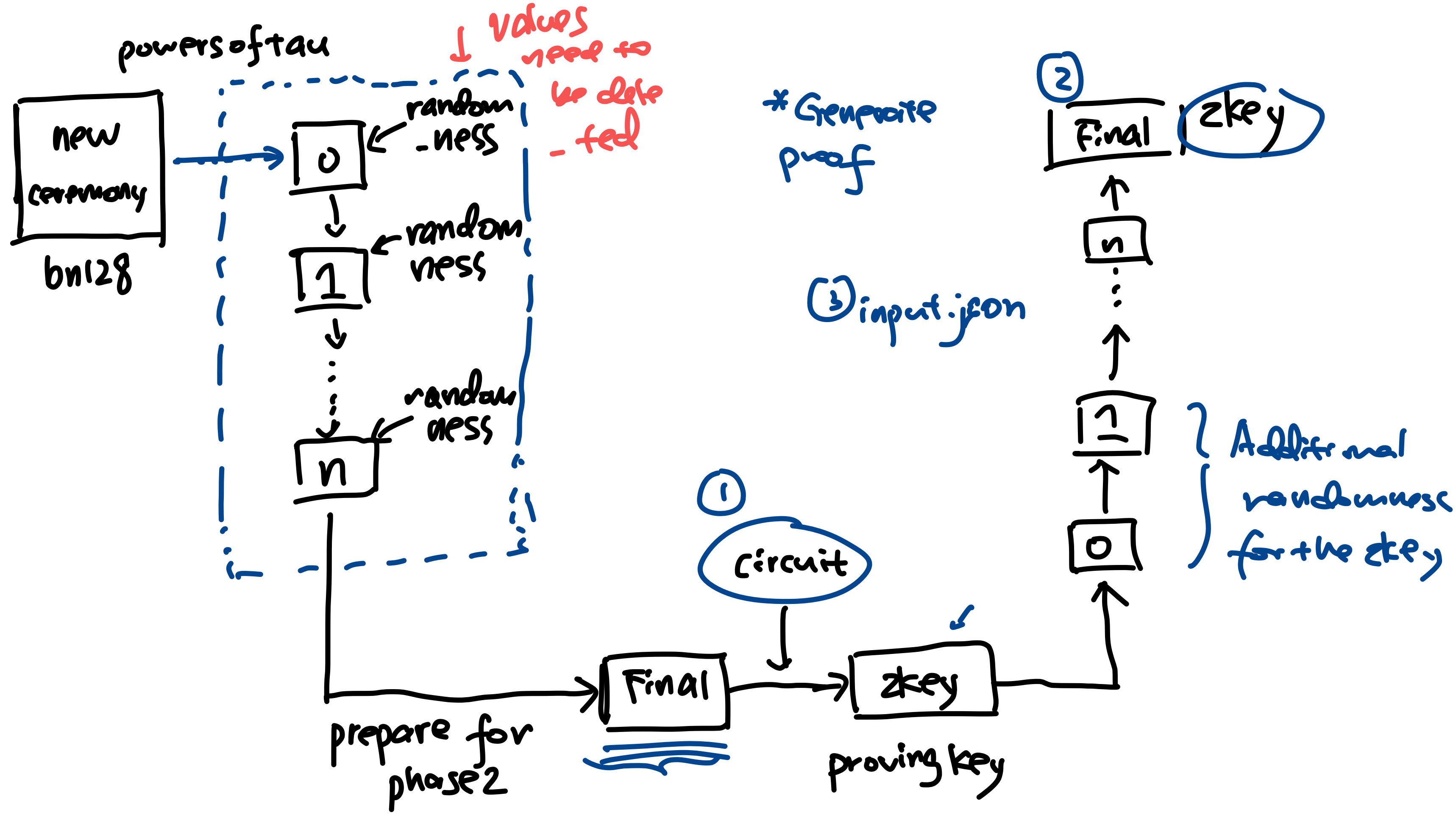
(randomness setup)



analogous to

$x \to 300^x$

§ Groth16 Setup Procedure


powersoftau
values need to be dele-ted
new ceremony
bn128
0
randomness
1
randomness
n
randomness
prepare for phase2
Final
① circuit
zkey
proving key
0
1
n
Additional randomness for the zkey
② Final zkey
* Generate proof
③ input.json