So here, I proposed the idea of a nothing-up-my-sleeve cryptosystem.

A nothing-up-my-sleeve computation essentially is a cryptographic algorithm that allows one to prove without any trusted setup that he has obtained some output f(x)

of the function f

without knowing anything about the input x

other than its existence. These nothing-up-my-sleeve computations could be used to remove the need of a trusted setup in a zk-SNARK.

A nothing-up-my-sleeve computation generator is a function D

produced without a trusted setup where for each circuit C

and string x

, there is some input c

to the circuit C

such that D(C)(x)=C(c)

but where little to no information about c

other than what can be deduced from C

and C(c)

can be obtained.

I do not have any idea about the mathematics needed to construct nothing-up-my-sleeve computations. I suspect the mathematics needed to construct these nothing-up-my-sleeve computations is beyond any mathematics that we have today since nothing-up-my-sleeve computations do not seem to be producible even with a cryptographic program obfuscator and since cryptographic program obfuscators (once mathematicians come up with some that are efficient enough to use in practice) could be used to easily construct nearly any kind of proposed cryptosystem.

Nevertheless, even though I suspect that nothing-up-my-sleeve computations are probably extremely difficult to produce in practice, this notion may be worthwhile to investigate since it only takes one instance of a nothing-up-my-sleeve computation in order to remove any worry about any ‘toxic waste’ produced in any cryptosystem such as zk-SNARKs requiring a trusted setup.