Hi

I’m posting these questions because I couldn’t find anything on the topic anywhere.

I could have been mislead because every time I ask for or look for a way to generate a private key for SCRT, I am invited to use some browser extension to do it.

However, this is absolutely not what I am looking for.

What I am looking for is:

- From a random number, what is the computation I have to do to generate a private key?
- What are the characteristics of this random number? (number of bits, something else?)
- How can I derive a public key from that private key?
- What is the protocol to generate a transaction on the blockchain?

I am asking these because I want to be as safe as possible and therefore I want to do all of these steps on an air gap computer and definitely not use browser extensions which I would not be able to review