Hi, Secret Network!

I'm Youngjoon Lee, blockchain engineer working on some projects based on Cosmos SDK/Tendermint.

Thank you for building this great secure network.

I would like to ask if there is any potential risk of the shared seed leakage. For example, I guess any malicious node operators could change the implementation of the secretcli configure-secret [master-cert] [encrypted-seed]

to decrypt the encrypted seed via Rust SGX SDK, and write the decrypted seed to the log file or so (without sealing).

I understood that the on-chain computation with secure contracts is safe because the secure contract is basically a smart contract (cosmwasm) that is already approved by validators and cannot be changed permenantly. But, I'm concerned about the off-chain logics that deal with the encrypted seed, which can be potentially executed in the secure enclave if malicious node operators modify the source code by themselves.

I would like to ask if there is any discussions related to my concern. Please correct me if I didn't understand it correctly.

Thank you!