So I wanted to announce that I finished the first version of FAPKC0 cipher and Gonzalez-Llamas homomorphic cipher based on it.

FAPKC is a family of ciphers based on composition of finite automata. Since finite automata are computational devices, they can do more than just encryption, so homomorphic operations are possible, and also functional encryption and white-box obfuscation.

This cryptosystem is extremely robust, fast and easy to use. It should be possible to obfuscate actual programs written in programming languages, not some abstract algebraic description of the problem.

Homomorphic encryption could be used to enhance Ethereum with privacy features, like a smart contract with secret state.

Some minor modifications to Gonzalez-Llamas homomorphic scheme could yield a working obfuscation algorithm. With obfuscation a whole new set of possibilities open, that will have huge impact on Ethereum and other blockchains.

- Obfuscation could be used to speed up boot time of nodes joining the network. Instead of verifying the blockchain from the beginning, they could rely on a trusted proof that certain checkpoint is valid.
- Obfuscation could be used to offload execution of smart contracts to the user itself. Miners will not have to execute contracts (only ensure the order of the methods called), the users will excersise their own computing power.
- Obfuscation could be used to control resources outside the blockchain, if the obfuscated program is embedded the credentials.

Please test the code here:

GitHub

haael/white-box-fapkc

White-box cryptography based on FAPKC algorithm. Contribute to haael/white-box-fapkc development by creating an account on GitHub.

(Please run the script automaton.py

.)

I wrote a simple program that converts ASCII strings to lowercase. The script can perform conversion to lowercase on ciphertext.

I am calling for feedback! Anyone who wants to help, please contact me.