Homewor6

Read the following materials and answer questions.

1. Ethereum mining Algorithm: https://github.com/ethereum/wiki/wiki/Ethash

2. (Optional) Ethereum mining CUDA/OpenCL: https://github.com/ethereum-mining/ethminer

   Kernels are in libethash-cuda & libethash-cl directory

3. Equihash algorithm: https://www.cryptolux.org/images/b/b9/Equihash.pdf

4. (Optional) Equihash mining code in CUDA: https://github.com/tpruvot/ccminer/tree/windows/equi

5. News about Equihash ASIC Miners: https://www.ccn.com/bitmain-to-release-first-zcash-asic-miner/

Questions:

Ethash and Equihash achieve ASIC resistance via memory-hard. Use your own word to explain their rationale. Do you think memory-hard problems are sufficient for achieving ASIC resistance?

How does Ethash achieve memory-hard? Suppose the current parameter of Ethash requires 3G of memory but one want to solve Ethash with only 1.5G memory. Can he/she do it? How much slower his/her algorithm will be? Why?

How does Equihash achieve memory-hard? What if someone tries to solve Equihash with half of the required memory? How much slower his/her algorithm will be? Why?

Why equihash claims to be ASIC-resistant but people have developed an ASIC miner that mines ZCash equihash 10X faster?
(Hint: ZCash uses equihash with the parameter N=200 and K=9. Estimate how much memory it would require to solve ZCash equihash? ASIC uses SRAM which is roughly $5 per MB.)

Do you think it is possible to stop specialized hardware design with proof-of-work puzzles like ethash and equihash? Why? (Open question)