Who am I ?

name: Joe Miyamoto Philips

Job: Bioinformatician

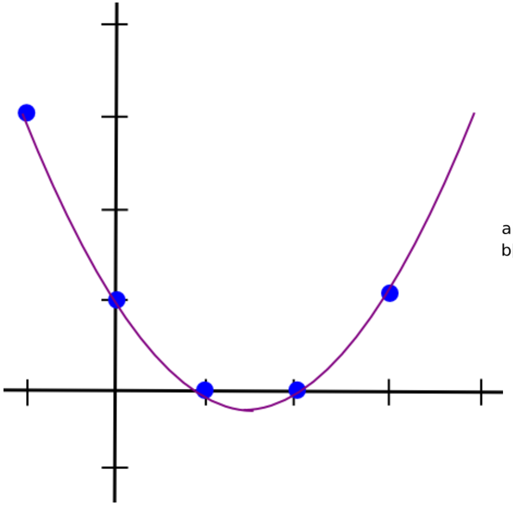
ID: joemphilips

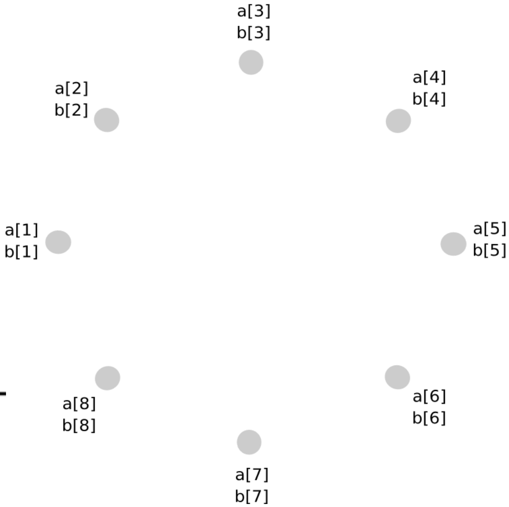
Recently I'm very crazy about BlockChain and Cryptography.

So that's today's topic.

Deccentralized storage with Blockchain.

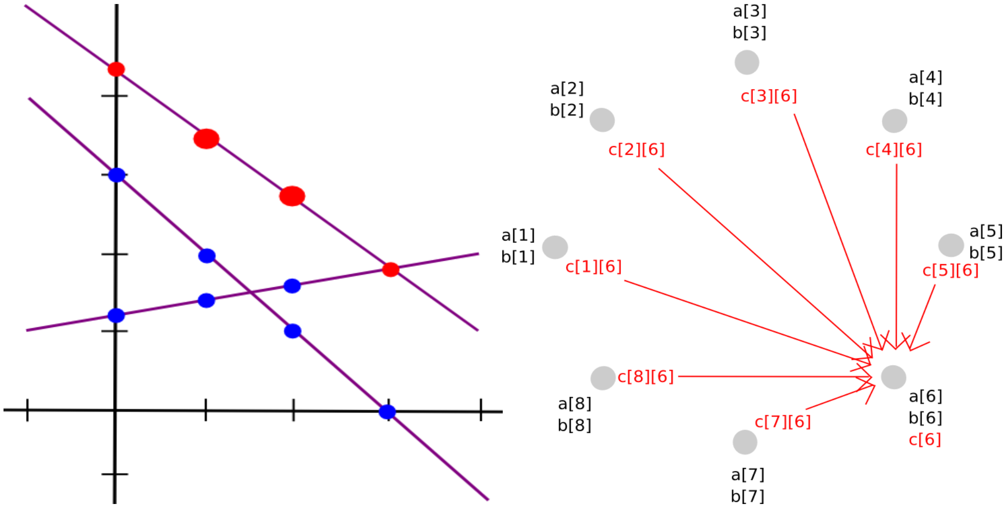
by Sahmir's secret sharing -> incentivize data holders.





Shamir's Secret Sharing

addition and multiplication without revealing data -> **any** computation could be done !



enable to *sell* personal data directly

share secret key

secret key could be reconstructed only M-of-N have approved.

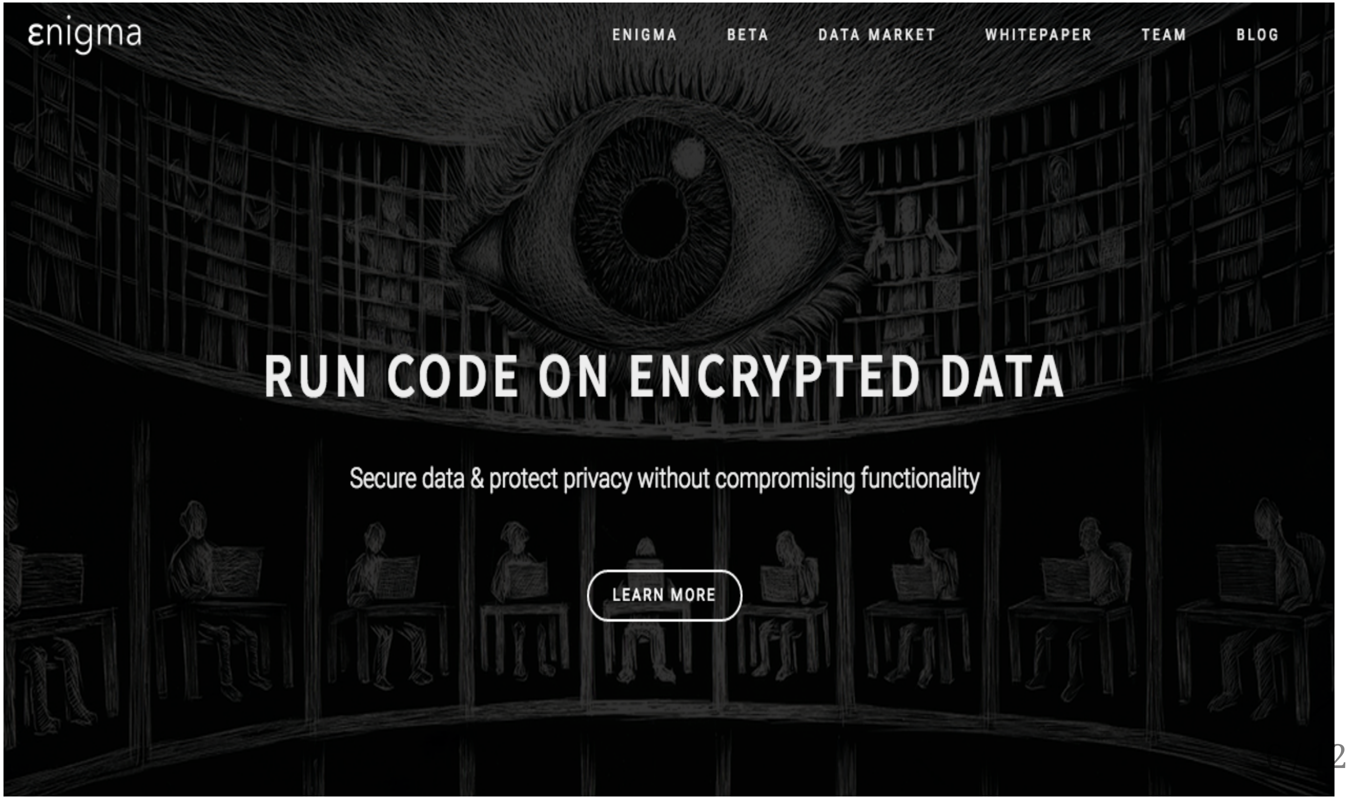
problems

SMPC are generally slow. Very slow.

1. multiplication is highly utlized function but it requires all nodes to communitate with each other.
2. Database can not be indexed, so full search needs to be done

Enigma

by Guy Zyskind, Oz Nathan, Alex ’Sandy’ Pentland


ɛnigma
ENIGMA
BETA
DATA MARKET
WHITEPAPER
TEAM
BLOG
RUN CODE ON ENCRYPTED DATA
Secure data & protect privacy without compromising functionality
LEARN MORE

Enigma

1. Make SMPC faster

- SPDZ protocol instead of Shamir's Secret Sharing.
- preprocess shares for efficient computation

2. Higher Availability of data

- save data on Distributed Hash Table
- and it's reference and metadata(e.g. who have rights to compute) on blockchain

3. Verifiable Secret Sharing

- incentivize collect computation

Enigma

- Shamir's secret Sharing -> **SPDZ protocol**

share data and it's MAC. -> Mach Faster when there are lot's of nodes

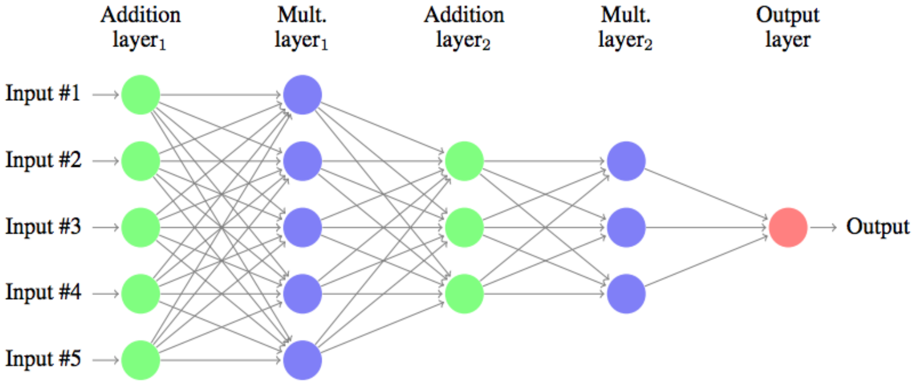


Figure 5: Feed forward flow of the secure code evaluation.

Enigma

Verifiable Secret Sharing

- Share has been made correctly … I don't know how this is done
- Computation has done correctly … part of SPDZ
- punishment … consensus Scheme used in Schelling coin

Enigma

3 kinds of storage

1. Public ledger … public blockchain maintaing access rights
2. Distributed Hash Table(DHT) … Kademlia Style
3. MPC … based on same scheme with DHT

So what?

Democratize Personal Data!

-> something "Don't be evil" companies won't be glad about.

Reference

- Enigma WhitePaper … http://enigma.media.mit.edu/enigma_full.pdf
- Secret Sharing DAO … https://blog.ethereum.org/2014/12/26/secret-sharing-daos-crypto-2-0/
- 和訳 … http://qiita.com/joemphilips/items/464bc2c6e5aa20003c59