

自己紹介

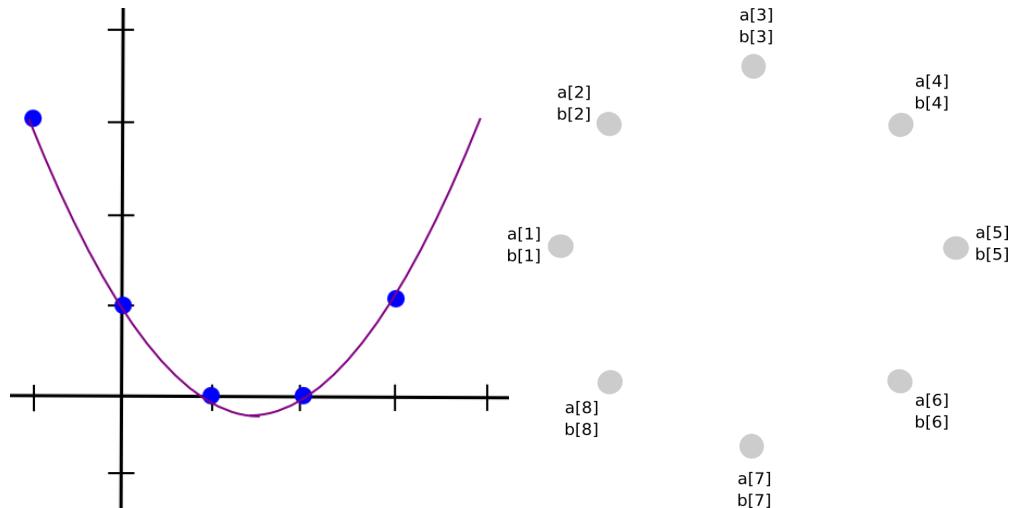


名前: 宮本 丈 職業: Bioinformatician ID: joemphilips

最近は暗号理論・ブロックチェーンの勉強にハマっています。 <- その話をします。

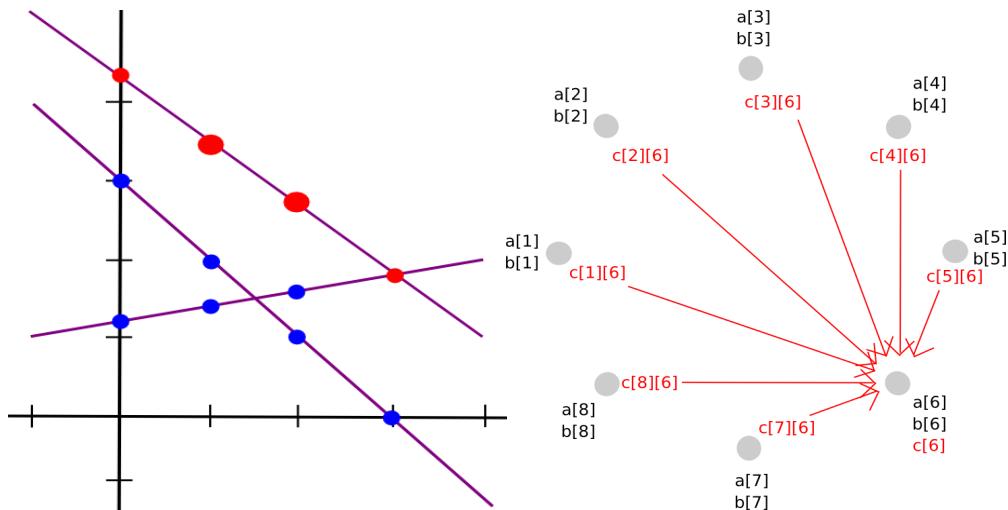
ブロックチェーンによる分散ストレージ

秘密分散で管理 -> ゼロ知識証明で、保持者にインセンティブを与える。



秘密分散上では情報を秘匿化したまま乗算と加算が可能

-> 任意の演算が可能



個人情報をデータマイニング用に「売る」ことが可能に

秘密鍵の分散管理

MのうちNが賛成したときのみ、送金(あるいはコンピュテーションの実行。IoTデバイスの操作も含む)ができる。

例えば5-of-9の分割を行った際、普通に行つただけでは、4人が集まっただけでも、秘密鍵の探索空間をかなり狭められるため、blute force することができ、危険。

そこで、秘密鍵の4倍のランダム配列を秘密鍵に加えてサイズを大きくし、分散管理させることで探索空間を広く保つ。

問題点

SMPCは遅い

1. 乗算は極めて使用頻度の高い演算であるが、乗算のたびに通信をする必要がある。例えば大小比較や統合判定ですら複数の和と積から構成される
2. データベースのインデックスを作るとそこから情報漏えいするため全探索しなくてはならない。

Enigma

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

The image shows the Enigma homepage. At the top left is the word "enigma". At the top right are navigation links: ENIGMA, BETA, DATA MARKET, WHITEPAPER, TEAM, and BLOG. Below these links is a large, detailed illustration of a human eye looking forward. The eye is set against a background of a grid of small figures of people sitting at desks, suggesting a surveillance or data processing environment. In the center of the grid, the text "RUN CODE ON ENCRYPTED DATA" is displayed in large, bold, white capital letters. Below this, a smaller line of text reads "Secure data & protect privacy without compromising functionality". A white button with the text "LEARN MORE" is positioned in the lower center of the grid area. The overall aesthetic is dark and moody.

Enigma

1. SMPCを早くする。
 - SPDZプロトコルに基づいた前処理 ... ネットワーキングを少なくする。
 - 最初に処理全体をコンパイルすれば、後半に行くに連れて参加ノード数を減らせる。
2. ブロックチェーン
 - ポインタ ... データの場所
 - メタデータ ... Read, Write, Compute(要約統計量の計算には使用できるが、データそのものは見れない)がどの秘密鍵に対して与えられるかを分散台帳で管理
3. 計算が正しく行われたかをチェックする仕組み(Verifiable Secret Sharing)を導入

Enigma

SMPCを早くする

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

データとそのMAC値とを単純に分割して保持しておくことで、ノード数が大きくて
も通信量を減らせる。

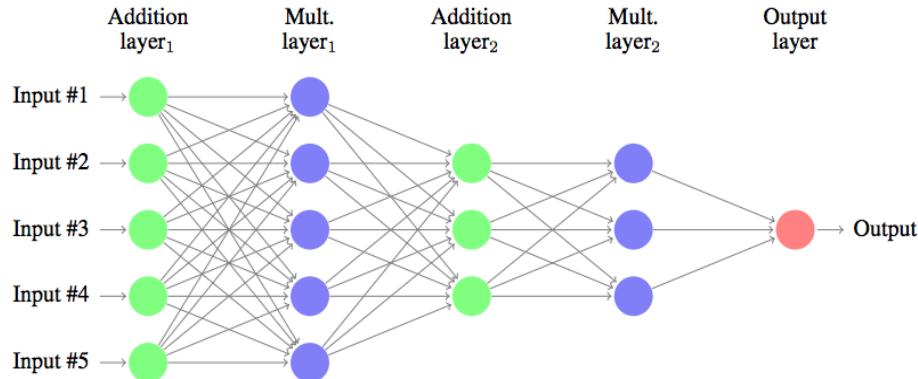


Figure 5: Feed forward flow of the secure code evaluation.

Enigma

Verifiable Secret Sharing

- 正しく分散化されていること ... Benaloh's Scheme
- 計算が正しく完了したこと ... SPDZ
- 懲罰 ... 間違った計算をした場合、Schelling合意形成のスキーマに基づいて罰則を与える。

ブロックチェーンと3種のストレージ

1. 分散台帳 ... データの場所とアクセス権を管理する(Append Only)
2. Distributed Hash Table(DHT) ... ノード間にまたがる巨大なストレージ、暗号化においてただのストレージとしても使える。
3. MPC ... DHTと同じだが、台帳がOKすれば計算に使用できる。

で、どうなるの？

データの民主化！

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>