"秘密分散"

伊藤 愛実

○ 鍵の分散管理

↓

無くしても良いようにコピーを多くすれば、完全に紛失してしまうことは減る。

↓ しかし…

鍵情報が漏れてしまう可能性は増える

⇓ これを解決する方法として。。。

秘密分散がある!!

＜秘密分散＞

・秘密を複数に分ける

→ 分散された秘密(シェア)からは元に秘密は分からない。

↳ 分けたピース のこと…

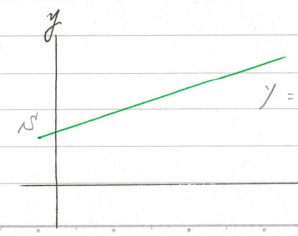
例えばピザ→

{ ○秘密の数字sをn個のシェアに分ける。
、n個のシェアを集めれば、秘密を復元可能 }

⇓

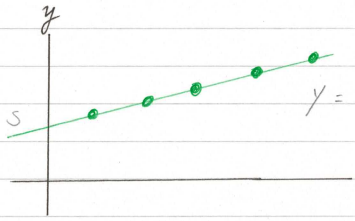
(n,n)-しきい値秘密分散

☆(n,2)-しきい値秘密分散①



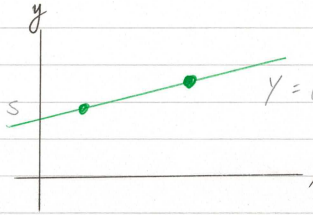
シェアが2個以上集まれば、秘密が復元可能

☆ $(n, 2)$ - しきい値秘密分散 ②



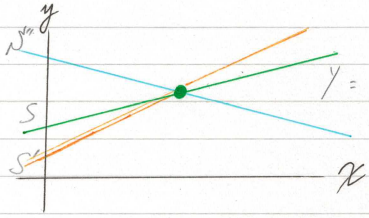
直線の傾き a をランダムに選ぶ

☆ $(n, 2)$ - しきい値秘密分散 ③



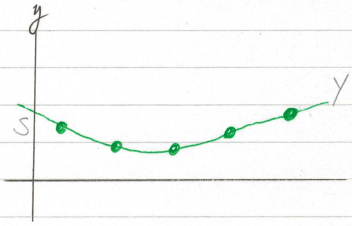
2つの点を通る直線は一意的

☆ $(n, 2)$ - しきい値秘密分散 ④



1点だけを通る直線は無限個

☆ $(n, 3)$ - しきい値秘密分散



このような式を、多項式

任意の3つのシェアで、s を復元できる

(n, k) - しきい値秘密分散 の場合

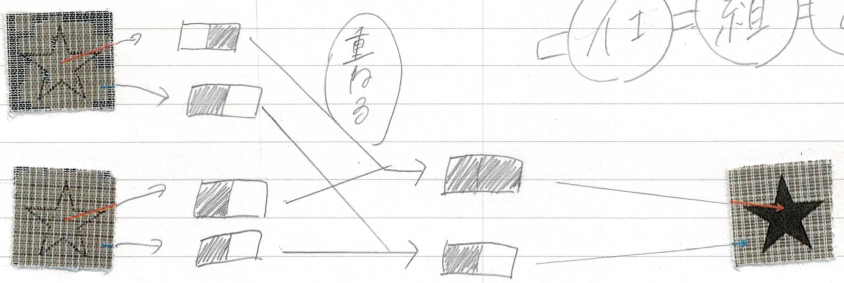
↓

シェアが k 個以上集まれば、秘密が復元できる。

NO.

DATE

< 視覚復号型秘密分散 >

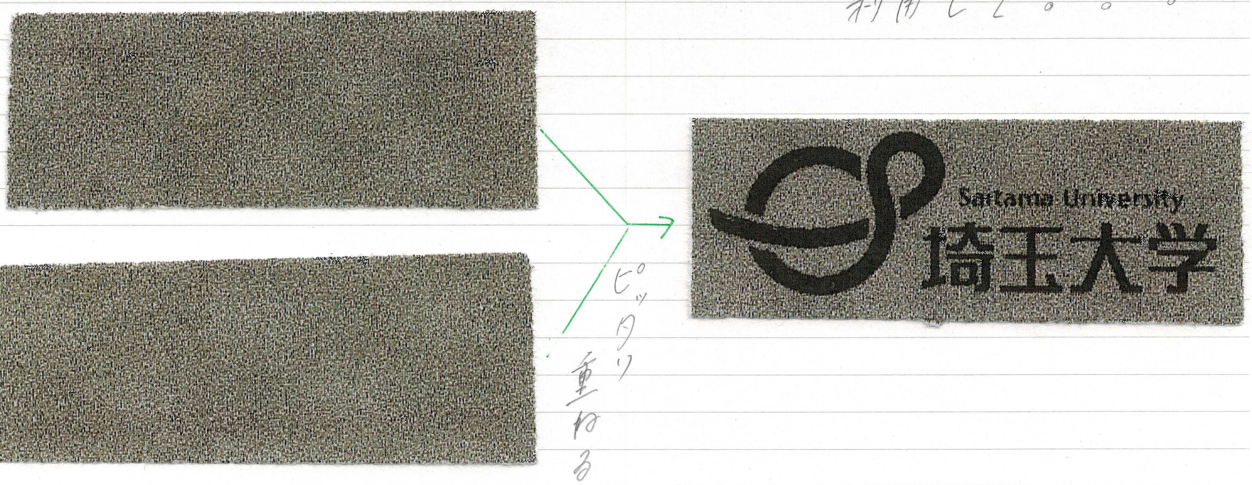


仕組み

こうして、できる!!

この仕組みを

利用して。。。



< 感想 >

秘密分散ということを知ったので、これからの生活でも生かしていけたらいいなと思います。また、上にはった、「埼玉大学」のシェアには驚きました。ピッタリ重ねることで、できるので、色々な事もやってみたいなと思いました!!