シャミアの秘密共有

https://dl.acm.org/doi/pdf/10.1145/359168.359176

仕組みの概要

秘密の分割: 秘密S（例: 秘密鍵）を多項式f(x) = S + a_1x + a_2x² + ... + a_{t-1}x^{t-1}（t-1次）で表現。係数a_iはランダム、有限体上で計算。

シェアの配布: n人の参加者に点(x_i, f(x_i))を配布。x_iは各参加者のID。

復元: t個以上のシェア{(x_i, f(x_i))}を集め、Lagrange補間法で多項式f(x)を再構築し、f(0)=Sを計算。

閾値性: t未満のシェアでは秘密Sの情報が漏洩しない（情報理論的安全性）。

特徴

閾値（t, n）: n人にシェアを配り、t人以上で復元可能。

安全性: t-1人以下では秘密の推測が不可能。

効率的: 単純な多項式計算で実装可能。

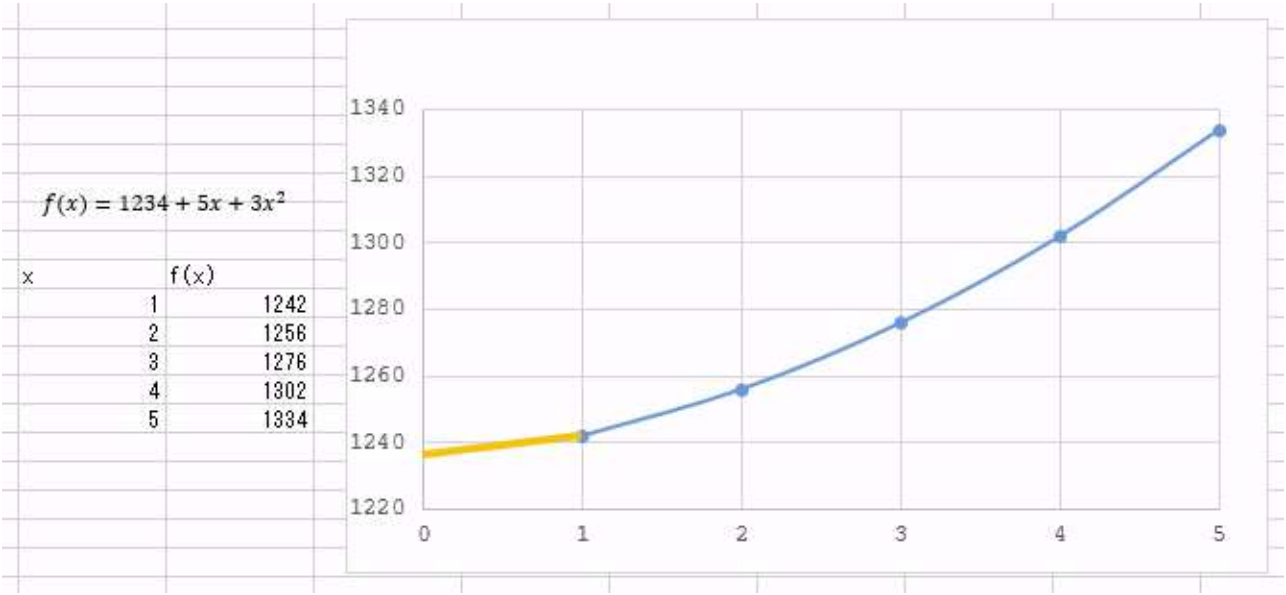
例

秘密S=1234、n=5、t=3の場合：

ランダムな2次多項式f(x)=1234 + a_1x + a_2x²を生成。

5人に点(f(1), f(2), ..., f(5))を配布。

任意の3点でf(x)を補間し、f(0)=1234を復元。



ここでは適当に線を引いたが、t がわかっているなら f(x) の形も分かるので何か程よい補完方程式があるのだと思う。

ラグランジュ補間 - Wikipedia