Secret Share 概要

秘密分散の方法としては、シャミアの秘密分散法を使っています。

分割、結合の方法は、

(2, 2) 2分割 2結合
(2, 3) 3分割 2結合
(3, 3) 3分割 3結合
(3, 5) 5分割 3結合

この4つの方法をサポートしています。

分散後の、各分散片は、源データよりも、80バイト程度大きなものになります。

認証機能は、持たせていません。

誤り訂正符号は、使っていません。

計算は、ガロア体を使って行っています。
生成する分散片は、ガロア体の連立方程式の係数の羅列というようなものになります。

ランダムオラクル性というようなものを持たせています。
そのため、試行のたびに、必ず、異なる分散片を生成します。

取り扱い可能なファイル(データ)のサイズには、制限は設けていません。

しかし、

1 MB くらい

が、現実的な最大サイズになると考えています。

その理由は、「結合」にかかる所要時間です

「シャミアの秘密分散法」を使っての、秘密分散の結合には、膨大な時間がかかります。

1MB	1分程度、1分以下
15MB くらい	5分〜15分程度
150MB くらい	1時間〜3時間程度

こんな感じです。(速い実行機では、もっと速いとは思います。)

ただ、分散の方には、これほどの所要時間はかかりません

ふつう、結合の 1/10 程度の時間で済みます。

しかし、結合の方には、これくらいの時間がかかります。

また、3分割、5分割という分散の個数には関わりなしに、3結合は、結合に、
2結合の3倍以上の時間がかかります。

3結合は、単純に、2結合の3倍の時間が、かかるからです。

古い Windows XP 機で、158 MB の乱数に対して、

(3, 5) 5分割 3結合

を実行すると、所要時間は、

分散... 12分24秒
結合... 3時間10分

となりました。

3結合の結合には、相当な時間がかかります。