Secret Share Overview

Shamir's secret sharing scheme is used as a method of secret sharing.

The method supported of share and combine is following 4 ways:

- (2, 2) 2 share 2 combine
- (2, 3) 3 share 2 combine
- (3, 3) 3 share 3 combine
- (3, 5) 5 share 3 combine

After sharing, each share piece is about 80 bytes larger than the source data.

It does not have an authentication function.

Error correction code is not used.

The calculation is done using the Galois field.

The generated share piece is like a series of coefficients of Galois field of simultaneous equations.

It has something like random oracle.
Therefore, each attempt always produces a different piece of variance.

There is no limit on the size of files (data) that can be handled.

However, I think that

about 1 MB

will be the realistic maximum size.

The reason is the time it takes to “combine“.
The combine of secret sharing using "Shamia's secret sharing scheme" takes a lot of time.

1MB	about 1 minute or less
about 15MB	about 5 to 15 minutes
about 150MB	about 1 hour to 3 hours

It is like this. (I think it's faster with a fast machine.)

However, it does not take so much time for share.

Usually, it takes about 1/10 of the time for combine.

However, combine takes much time.

Also, regardless of the number of variances of 3 and 5 share, 3 combine take more than three times as long as 2 combine.

3 combine is simply 3 times longer than 2 combine.

On an old Windows XP machine, running (3, 5) 5 share 3 combine on a random number of 158 MB takes such times:

share ... 12 minutes 24 seconds

combine ... 3 hours 10 minutes

Combining for 3 combine takes a considerable amount of time.