秘密分散法構築におけるユーザフレンドリーなUIの提案・評価・考察

三浦 夢生
（木更津工業高等専門学校 専攻科 制御・情報システム工学専攻）

Proposal, Evaluation and Discussion of user-friendly UI for Secret Sharing scheme construction

Yu Miura
(Advanced Control and Information Engineering Course, National Institute of Technology, Kisarazu College)

In modern society, spreads cloud or online service and a lot of important information (e.g. personal data) is transmitted and received. Cyber-attacks against companies and organizations are increasing year by year, and the damage caused by ransomware, one of them, is expanding. In this study, I deals with a scheme called secret sharing. By using this scheme, we can reduce the risk of loss or theft of the secret. and allows managers to adjust discretion per role by using hierarchical one. The purpose is designing intuitive and user-friendly UI for people who don't know too much about secret sharing and proposing easy to use secret sharing tool even individuals. In an evaluation, I ask testers to use the proposed UI and the conventional CLI-based UI, and conduct a questionnaire survey and analysis of whether the UI is "visually easy to understand", "easy to operate", and "time required to build a secret sharing system".

Keywords: Secret Sharing, cryptgraphy, Shamir's Secret Sharing, User Interface

1 まえがき

近年，クラウド及びオンラインサービスが企業や一般家庭において広く普及し [1], [2]，個人情報などの多くの重要な情報がやり取りされている．その中で企業・団体等に対するサイバー攻撃は年々増加しており，その中の一つであるランサムウェアによる被害は拡大している [3]．IPA の情報セキュリティ 10 大脅威においても，機密情報を狙った攻撃は大きな影響を与えるとされる [4]．これらは機密情報やアクセス権の集中管理によって攻撃を受けた際のリスクが高まるためであり，最小限の適切なアクセス管理が重要である．しかし，無闇な機密情報のコピーや，アクセス権限の厳重化ではかえってリスクが高まる [5]．

これらのリスク低減のため機密情報の分散管理及びアクセス権限の柔軟な付与ができる「秘密分散 [6]」という技術を用いる．秘密分散によって情報の漏洩・紛失のリスクを低減し，またこれを階層化することによって管理者の役割ごとの裁量を調節できる手法を UI のバックエンドに採用する．フロントエンドサイドでは，秘密分散を詳しく知らないユーザでも直感的に利用しやすい UI の設計をする．本研究では個人で気軽に利用できるような秘密分散ツールの設計・提案を行い，UI によってどの程度秘密分散ツールが利用しやすくなったかアンケート調査し，提案 UI の有用性や改善点について考察することを目的とする．

実装には，ユーザの環境を選ばずブラウザで動作する Javascript と，そのフレームワークである React.js を主として用いる．React.js は GUI 作成に特化した Javascript フレームワークであり，SPA(Single Page Application) を作成しやすい画面遷移のない実装が可能となり，ユーザ側での画面読み込みや通信負荷を減らすことができる．

アンケート調査ではコマンドラインライクな UI と木構造を模した提案 UI を用意し，それぞれファイルを秘密分散する課題を遂行してもらい，それにかかった時間の計測，使用感に関する質問への回答を求める．

2 前提知識

2.1 Shamir の秘密分散法

秘密分散法とは，まず対象となる秘密情報をあるアルゴリズムを用いてシェアと呼ばれる分散情報を作成し，そのシェアを管理する人・端末に配布し管理・保管する手法である．元の秘密情報を得る際には，管理されたシェアを必要な数だけ集め，復元アルゴリズムによって復元する．

いくつかある秘密分散法のうち，本研究では Shamir の秘密分散法 [10] を用いている．この手法

は (k, n) しきい値秘密分散法とも呼ばれ，シェアを n 個生成し，k 個のシェアを集めることで秘密情報の復元が可能であるが，$(k-1)$ 個以下のシェアからは復元は不可能である．

シェアを生成するアルゴリズムは，まず Eq.1 のような秘密情報 S を定数項とするランダムな $k-1$ 次多項式を定める．

$$f(x) = S + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{1}$$

管理に参加する人や端末の数 i に対し，$f(1), f(2), \ldots, f(i)$ を計算し，配布する．

復元の際は，k 個のシェア $(j, f(j))$ を集めて k 個の式を立て，連立方程式を解くことで秘密情報 S を得る．k 個のシェアは同じ多項式から生成されたものであればよく，任意のものを用いればよい．

またこのときラグランジュ補間を用い，Eq.2, Eq.3 において $x = 0$ の場合を計算することで，多項式のうち定数項のみ，つまり元の秘密情報を得ることができる．

$$L(x) = \sum_{i=0}^{k} y_i l_i(x) \tag{2}$$

$$l_i(x) = \prod_{j=0, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} \tag{3}$$

2.2 拡大体

体とは集合に対して加法，乗法の二つの二項演算を定めた代数的構造のことであり，加法，乗法のどちらに関しても結合法則・交換法則・分配法則が成り立ち，単位元及び逆元が存在する．また前提として，集合の二つの要素に対して，その二項演算の結果が集合の中に存在することも条件である．これらのことから，体の要素は加減乗除に閉じているといえる ?．これを踏まえて拡大体 K' とは，ある体 K に代数的構造を損なわないように元 $\alpha \notin K$ を追加して得られる体のことである．このとき，K' は K を含んでおり，K は K' の部分体ともいう．また，K' では K で定義された演算をそのまま用いることができる [12]．

本研究では $GF(2) = \{0, 1\}$ という二つの要素をもつ体を拡大し $GF(2^8)$ という集合を扱う．まず $GF(2)$ における演算を Table.1 及び Table.2 のように定義する．この体は整数を 2 で割った剰余によって構成された集合と見ることもできる．

この演算を踏まえて $GF(2)$ を拡大し $GF(2^8)$ を構成する．このとき，既約多項式という概念を導入すると，$GF(2^8)$ において 2 の剰余の集合と扱えたように，$GF(2^8)$ は既約多項式による剰余の集合とすることができる．本研究では既約多項式 $x^8 + x^4 + x^3 + x^2 + 1$ を用いたため，$GF(2^8)$ の各元は係数が 0 または 1 の 7 次式である．

Table1. 加法の演算表

+	0	1
0	0	1
1	1	0

Table2. 乗法の演算表

+	0	1
0	0	1
1	1	0

$GF(2^8)$ において，加法は Table.1 より各次数の項の排他的論理和となるため，7 次までの項の係数を 8bit の列として見ることで，コンピュータで扱いやすい演算となる．減法について，$1 \equiv -1 \bmod 2$ であるため，加法と同じ演算を用いることができる．

乗法は各元の算術的な積をとり，既約多項式による剰余を求めることで定義される．除法についても 0 除算を除いて体の定義から逆元が存在するため剰余の計算をすることで求めることができる．

ここで仮想的に既約多項式の根 α を考える．この根は体上には存在しないが，この根は体の原始元であり，体の要素は原始元のべき乗によって巡回的に生成される．このことから，多項式による表記と原始元のべき乗による表記を対応させることで多項式の積を実装せずに体上の乗除が可能となる [13]．

3 実装

3.1 バックエンド

3.2 フロントエンド

4 アンケート調査

5 結果・考察

実験途中により結果は省略

6 まとめ

7 今後の展望

参考文献

(1) 総務省, “デジタルで支える暮らしと経済”, 情報通信白書, pp.156-159, July 2020.
(2) 総務省, “デジタルで支える暮らしと経済”, 情報通信白書, pp.313-315, July 2020.
(3) 警察庁, “令和3年におけるサイバー空間をめぐる脅威の情勢等について”, 警察庁 広報資料, pp.3-5, April 2022.
(4) 独立行政法人情報処理推進機構セキュリティセンター, “情報セキュリティ10大脅威”, 情報処理推進機構, pp.36-39, March 2022.
(5) 独立行政法人情報処理推進機構, “組織における内部不正防止ガイドライン”, 情報処理推進機構, pp.40-44, April 2022.

(6) 西川律子, “秘密分散法の概要”, 沖テクニカルレビュー 第205号, pp.70-71, January 2006.
(7) 独立行政法人情報処理推進機構, “企業における営業秘密に関する実態調査2020”, 調査実態報告書, pp.44-47, March 2020.
(8) 株式会社エスロジカル, “マル秘分散”, http://www.ma-bu.com/, 閲覧日Dec 2021.
(9) Jon Frisby, “ssss”, https://github.com/MrJoy/ssss, 閲覧日Dec 2021.
(10) A Shamir, “How to share a secret”, Communications of ACM, Vol.22, pp.612-613, April 1979.
(11) 野崎昭宏, “納得する群・環・体”, 講談社, 第1版, pp.136-137, May 2016.
(12) 汐崎陽, “情報・符号理論の基礎”, オーム社, 第2版, pp.90-91, May 2019.
(13) 野崎昭宏, “納得する群・環・体”, 講談社, 第1版, pp.160-176, May 2016.
(14) 高荒亮, 岩村惠一, “XORを用いた高速な(k, L, n)ランプ型秘密分散法に関する研究”, コンピュータセキュリティシンポジウム2009(CS2009)論文集, Vol.2009, pp.1-6, October 2011.
(15) 青野成俊, 岩村惠一, “実用観点からみた秘密分散法に関する一考察”, コンピュータセキュリティシンポジウム2009(CS2009)論文集, Vol.2009, pp.1-6, October 2011.