Vol.2020-MPS-131 No.25
2020/12/18

一次元折り紙モデルの情報セキュリティ技術への応用

芳師渡 淳之介[1,a)]　安細 勉[1]

概要：郵便切手の問題に代表される一次元折り紙モデルは，簡潔な構造とは裏腹に，数学的に難解であり，モデルによる問題は，殆どが未解決，又は NP 完全な問題である．本研究では，そのような一次元折り紙モデルを取り上げ，情報セキュリティ技術への応用方法を検討する．現時点では，電子署名と秘密分散法への応用を考案しており，特に電子署名については，2012 年に提案された Crease width problem を用いて，当該技術を構成する手法を検討している．

キーワード：一次元折り紙モデル，秘密分散法，電子署名

Application of One-Dimensional Origami Model to Information Security Technology

Abstract: Contrary to its simple structure, the one-dimensional origami model typified by the stamp folding problem is mathematically difficult, and many problems using the model are an open problem or NP-complete. In this study, we are inspired by this property of the model as "simple and difficult", and are investigating to apply the model to information security technology. In this paper, we report on two matters, was obtained by applying the model, the secret sharing scheme be available by cloud computing and the digital signature that has quantum resistance using crease width problem.

Keywords: One-dimensional origami model，Secret sharing scheme，Digital signature

1. はじめに

本研究は，一次元折り紙モデルの性質を端緒に，当該モデルの情報セキュリティ技術への応用方法を検討するものである．本稿においては，検討中のものより，秘密分散法を 3 章 1 節で，電子署名を 3 章 2 節で報告する．

2. 準備

2.1 一次元折り紙モデル

一次元折り紙モデルとは，長さ $n \times 1$ $(n \in \mathbb{N})$ の折り目のついた長方形状の紙を，その紙が長さ 1×1 になるよう，折り目に沿って折り畳む操作を考えた時に，折り畳み前後での紙の状態を抽象化したものである [1]．ここで，紙の折り目は，短辺と並行かつ等間隔に，$n-1$ 個存在するものと定義される．モデルの記法は文献により様々であるが，本稿においては，右記の数列による記法を標準とする．

- $s_n \equiv Array(\{0,1\}, n-1)$ [*1]
  - 折り畳み前の状態を表す有限数列．0 が山折り，1 が谷折りとした時の折り目のパターンを表現している．
- $f_n \equiv \{a : Array(\{1,...,n\}, n) | n = ran(a)\}$
  - 折り畳み後の状態を表す有限数列．折り畳み後の紙のセグメント [*2] の並びを表現している．

ここで, 任意の n について, 集合 $S = \{\forall s_n\}$, 集合 $F = \{\forall f_n\}$ としたとき，$g : F \to S$ は部分写像かつ全射である．

3. 情報セキュリティ技術への応用

3.1 秘密分散法

本節では，一次元折り紙モデルを適用した秘密分散法について報告する．この秘密分散法は，クラウドコンピューティングへの適応を前提とした，計算量的安全性に基づくものである．クラウドコンピューティングに適応した秘密分散法の必要性については，文献 [2] を確認されたい．

[1] 茨城工業高等専門学校
Hitachinaka, Ibaraki 312–8508, Japan
[a)] ac19310@gm.ibaraki-ct.ac.jp

[*1] $Array(X, N) \equiv \{1,...,N\} \to X$
[*2] 折り目間の折り目のついていない領域

3.1.1 準備

$\mathcal{P} = \{P_1, P_2, ...P_m\}$ を m $(m \in \mathbb{N})$ 個のデータサーバの集合とし，$\mathcal{D} \notin \mathcal{P}$ をディーラーとする．$\mathcal{D}$ は秘密情報 S から m 個の分散情報 $\tilde{W} = W_1, W_2, ..., W_m$ を計算し，各分散情報 W_j を各サーバ P_j に配布する．

3.1.2 提案法

提案法において，秘密情報 S_i は n[bit] の情報とする．この時，S_i のビット列と数列 s_n とが対応付けられる為，$S_i = s_n$ と考えられる．具体的な構成手順を以下に示す．

[生成]

(1) ディーラーは，乱数を用いて $S_i = s_n$ から f_n を生成する．ここで，乱数は折り畳み方を与えるものとする．

(2) ディーラーは，f_n を $f_n = (x_1|x_2|...|x_m)$ として分散情報 $W_j = x_j$ に分割し，各サーバ P_j に配布する．

[復元]

(1) データサーバ $P_1, ...P_m$ は，復元要求を受け取り，各々に対応する分散情報 $W_1, ..., W_m$ を送信する．

(2) 秘密情報を復元するユーザは，受信した分散情報 $W_1, ..., W_m$ から f_n を得る．

(3) ユーザは，f_n から秘密情報 $S_i = s_n$ を復元する．

3.1.3 評価

簡略化のため，生成における f_n の分割を m 等分であるとする．この時，提案法における分散情報の定義より，分散情報 W_j あたりのデータサイズ $D(W_j)$ は，

$$D(W_j) = \frac{n}{m}k$$

である．(k は，f_n の一要素あたりのサイズを表す.)
クラウドコンピューティングへの適応という前提から，$D(W_j)$ は条件式 $D(W_j) < n$ を満たす必要がある．ここで，条件式は $D(W_j) = \frac{n}{m}k$ であるから，$k < m$ と書き換えることができる．従って，適切な k と m を設定することで，本提案法は計算量的安全性に基づく秘密分散法の目的を果たすことができる．

例えば $n = 1$[GB] の場合，f_n の各要素は 33[bit] あれば，取りうる値を全て表現できるから，条件式は，$33 < m$ となる．ここで，分散数を $m = 66$ とすると，分散情報のデータサイズ $D(W_j) \approx 500$[MB] となり，分散情報 W_j を元の秘密情報の半分のサイズとすることができる．

3.2 電子署名

本節では，一次元折り紙モデルを適用した電子署名について，その検討事項を報告する．なお，量子コンピュータの台頭に備えるという目的の下，耐量子性を持つものについて検討している．

3.2.1 Crease width problem

Crease width problem は，2012 年に提唱された問題である [3]．一次元折り紙モデルに対して，折り目幅 *3 という概念を導入し，その折り目幅の最大値，または合計値が最小な場合の折り畳み状態を探索する．この内，特に最大値が最小なものを探索する場合では，強い NP 完全性を持つことが証明されている．

*3 折り畳み後の紙において，折り目間に挟まっている紙の枚数

3.2.2 提案法

先述の Crease width problem から折り目幅を導入し，モデルから利用可能な要素を増やすことで構築を行う．そのために，まず折り目幅を以下に示す数列として定義する．

- $w_n \equiv \{a : Array(\{0, ..., n-2\}, n-1)$
  $|(w_n(i) = y - x - 1 | f_n(x) = i, f_n(y) = i+1\}$
  - 各セグメント間の折り目幅を表す有限数列．要素 $w_n(i)$ は，セグメント i とセグメント $i+1$ の間の折り目幅を表現している．

ここで f_n は予め定まっているとする．

Crease width problem より，s_n から f_n を求める問題は NP 完全であるが，折り目幅を導入することで，s_n と w_n を組み合わせれば，f_n を多項式時間で求めることが可能となる．この関係性から，例えば H を暗号学的に安全なハッシュ関数として，以下のような雛形が構成できる．ここで，f_n を秘密鍵，f_n による w_n を公開鍵とし，公開鍵は予め検証者が持っているものとする．

(1) 署名者は，平文 m をハッシュ関数 H によって，$H(m)$ に変換する．

(2) 署名者は，秘密鍵 f_n を用いて $H(m)$ を署名文 $S(m)$ に変換し送信する．この時，署名文と同時に f_n から生成された s_n も送信する．

(3) 検証者は，署名者から受け取った $S(m)$ と s_n，および公開鍵 w_n から $H(m)$ を計算し，検証を行う．

この雛形は，NP 完全問題を理論的背景としていることから，耐量子性を持つため，量子コンピュータの台頭に備えるという目的は達成したものとなっている．しかしながら，現状は一度きりの使い捨てであるため，実用に耐えるものではなく，改善が望まれる．

4. おわりに

記載した提案法はどちらも，理論的には新しいが，実用には届いていない．故に今後，更に検討を重ねていきたい．

参考文献

[1] M.Gardner.: The Combinatorics of paper folding, in:*Wheels, Life and Other Mathematical Amusements*, W.H.Freeman and Company, 60-73,1983

[2] 高橋 慧, 小林 士郎, 岩村 惠市.: 記憶容量削減と計算量的安全性および復元の独立性を実現するクラウドに適した秘密分散法, 情報処理学会論文誌, Vol.54, No.9, 2146-2155, 2013

[3] Takuya Umesato, Tshiki Saitoh, Ryuhei Uehara, Hiro Ito, Yoshio Okamoto.: *The Complexity of the stamp folding problem*, Theoretical Computer Science, 497, 13-19, 2013