(2, 2, 3) ランプ型秘密分散法の提案

坂崎 尚生[1]　安細 康介[1]

概要：本稿では，Shamire の (k, n) 閾値秘密分散法と Rivest の AONT 秘密分散法を組み合わせて，$(2, 2, 3)$ ランプ型秘密分散法を提案する．機密性と可用性を両立した秘密分散法を適用する場合，$(2, 3)$ 閾値秘密分散法が最小構成となるが，本方式により，その最小構成の $(2, 3)$ 閾値秘密分散法において，分散情報のデータ長を $(2, 3)$ 閾値秘密分散法の半分に削減することができる．

キーワード：ランプ型秘密分散法，クラウド型データベース

Proposal of (2, 2, 3)-Ramp Secret Sharing Scheme

Hisao Sakazaki[1]　Kousuke Anzai[1]

Abstract: In this paper, we propose a $(2, 2, 3)$-ramp secret sharing scheme by combining Shamir's (k, n)-threshold secret sharing method and Rivest's AONT secret sharing method. It is possible to reduce the data length of the share by half even if we use the $(2, 3)$ threshold secret sharing scheme.

Keywords: ramp secret sharing scheme, cloud database

1. はじめに

近年，多くの企業では，ネットワークを介してデータセンタにデータを保管するクラウド型データベースを活用する事例が増えてきている [7]．また，公共分野においてもクラウドを利用して情報システムの集約と共同利用を進めることにより，情報システムに係る経費の削減を図っている [8][9]．

しかし，クラウド型データベースはデータを外部サーバに保管する為，委託先クラウドサービス事業者の設備等によっては，データの漏洩や消失が発生するリスクを考慮しなければならない．そこで，クラウドに預けるデータの機密性と可用性を同時に高めることができる秘密分散法が注目されている．

秘密分散法の代表例として Shamir の (k, n) 閾値秘密分散法がある [1]．Shamir の (k, n) 閾値秘密分散法では，秘密情報を n 個の分散情報に分割し，n 個の分散情報の中から任意の k 個集めれば元の秘密情報が復元できるが，$k-1$ 個以下の分散情報からでは，元の秘密情報に関する情報が全く得られないという特徴がある．それ故，分散情報の一部が漏洩しても元の秘密情報は安全であり，また，n 個の分散情報の内，$n-k$ 個以下の分散情報が消失しても，元の秘密情報を復元することが可能である．

この様に Shamir の (k, n) 閾値秘密分散法は，データの機密性と可用性を同時に高めることができる方法であるが，Shamir の (k, n) 閾値秘密分散法では，「各分散情報のデータ長を元の秘密情報のデータ長よりも小さくすることができない」という性質がある為，符号化効率が悪い．そこで，Shamir の (k, n) 閾値秘密分散法の符号化効率を向上させた (k, L, n) ランプ型秘密分散法が提案されている [2][3][4]．実際，(k, L, n) ランプ型秘密分散法は，各分散情報のデータ長を元の秘密情報のデータ長の $1/L$ まで縮小することができる為，オリジナルの Shamir の (k, n) 閾値秘密分散法と比べて符号化効率が良い．それ故，(k, L, n) ランプ型秘密分散法は，より実用的な方式と言える．

[1] (株) 日立製作所 研究開発グループ
システムイノベーションセンタ
Hitachi, Ltd., & Development Group,
Center for Technology Innovation - Systems Engineering

では，実用面から考慮した場合，(k, L, n) ランプ型秘密分散法の各パラメータ k, L, n をどのように設定するのが最適であろうか．その解として松本らは，文献 [5] にて (k, L, n) ランプ型秘密分散法におけるデータ容量，データ転送量，計算量などを総合的に考慮し，ある前提の下で $(3, 2, 4)$ ランプ型秘密分散法が魅力的な秘密分散法であることを導いている．

しかし，松本らの分析に従い $(3, 2, 4)$ ランプ型秘密分散法を適用する場合，秘密情報を 4 つの分散情報に分割する為，我々は，4 つのデータセンタを用意しなければならなくなる．現状のシステムでは，1 つのデータセンタ，若しくはバックアップも考慮して 2 つのデータセンタ程度で，運用されているケースが多い．1 センタ分の維持管理だけでもそれなりに費用が掛かると仮定すると，セキュリティ機能強化の為に，現状の設備をいきなり倍増以上させるというケースは，かなりハードルが高いと考える．

本論文は上記状況に鑑みたものである．

松本らは，安全性と効率性をバランスよく設定することを前提において，$(3, 2, 4)$ ランプ型秘密分散法が魅力的な秘密分散法であることを導いているが，本論文では，敢えて安全性を想定する許容範囲まで抑え，効率性を重視することで，$(2, 2, 3)$ ランプ型秘密分散法を提案する．

本提案では，秘密分散法を適用するにあたり，「秘密情報に関する曖昧さ（エントロピー）[*1] が十分大きな場合，1 つの分散情報が与えられたときの秘密情報に関する曖昧さ（条件付エントロピー）が半減することを許容することはできないか」という問題提起をすると共に，具体的な $(2, 2, 3)$ ランプ型秘密分散法を検討した．

本論文の構成は次の通りである．

2 章では準備として，Shamir の (k, n) 閾値秘密分散法 [1] 及び (k, n) 閾値秘密分散法の符号化効率を向上させた (k, L, n) ランプ型秘密分散法 [2][3] を説明する．3 章では，効率性を重視した (k, L, n) ランプ型秘密分散法のパラメータ設定について説明し，同時に，「秘密情報に関する曖昧さ（エントロピー）が十分大きな場合，1 つの分散情報が与えられたときの秘密情報に関する曖昧さ（条件付エントロピー）が半減することを許容することはできないか」という問題提起を行う．4 章では，具体的な $(2, 2, 3)$ ランプ型秘密分散法を提案し，5 章にて，提案方式を考察すると共に本論文を纏める．

2. 秘密分散法

2.1 (k, n) 閾値秘密分散法

秘密分散法の代表例である Shamir の (k, n) 閾値秘密分散法 [1] を説明する．計算は秘密情報 s より大きい素数 p 上の有限体 $GF(p)$ 上で行われる．shamir の (k, n) 閾値秘密分散法では，秘密情報 s を定数項，乱数 $a_i \in GF(p)$ $(1 \leq i \leq k-1)$ を係数とする下記の様な $k-1$ 次多項式 $f(x)$ を定義する．

$$y = f(x) = s + \sum_{i=1}^{k-1} a_i x^i$$

この $f(x)$ 上に任意の点 (x_j, y_j) を n 個 $(1 \leq j \leq n)$ とり，各座標点 (x_j, y_j) を分散情報とする．

秘密情報の復元には，k 個の分散情報から以下の Lagrange の補間公式を用いて復元する．

$$s = f(0) = \sum_{i=1}^{k} \prod_{\substack{j=1 \\ j \neq i}} \frac{x_j}{x_j - x_i} y_i$$

2.2 (k, L, n) ランプ型秘密分散法

(k, n) 閾値秘密分散法の符号化効率を向上させた (k, L, n) ランプ型秘密分散法 [2][3] を説明する．(k, L, n) ランプ型秘密分散法は，各分散情報のデータ長を元の秘密情報のデータ長の $1/L$ まで縮小することができる．(k, L, n) ランプ型秘密分散法 [2][3] では，秘密情報 s を L 個の部分情報 $s_i (0 \leq i \leq L-1)$ に分割する．また，乱数 $a_i \in GF(p)$ $(L \leq i \leq k-1)$ を準備し，以下の $k-1$ 次多項式 $f(x)$ を定義する．

$$y = f(x) = s_0 + \sum_{i=1}^{L-1} s_i x^i + \sum_{i=L}^{k-1} a_i x^i$$

これ以降は Shamir の (k, n) 閾値秘密分散法と同様に，$f(x)$ 上に任意の点 (x_j, y_j) を分散情報として扱う．(k, L, n) ランプ型秘密分散法 [2][3] では，$k-L$ 個以下の分散情報からでは，元の秘密情報 s に関する情報が全く得られないが，分散情報が $k - t (1 \leq t < L)$ 個集まった場合，秘密情報 s に関する曖昧さ（エントロピー）が低下するという特徴がある．また，この時，ある特定の値においては分割した秘密情報 s_i の幾つかが完全に復元されてしまう場合もある．この様に中間的な情報漏れを許す秘密分散法を不完全秘密分散法と呼ぶ．

3. パラメータ k, L, n の選択

3.1 松本らの考察

松本らは，文献 [5] にて実用面から各パラメータ k, L, n をどのように選択するべきかを考察している．松本らは，安全性と効率性から要件を定義し，その要件から最適なパラメータを設定した．松本らの考察を要約すると以下である (詳しくは文献 [5] 参照)．

[*1] 秘密情報 s に関する曖昧さ (エントロピー) とは，事象系 $S = \{s_1, s_2, \cdots, s_n\}$ に対して事象 s_i が起こる生起確率を $p(s_i)$ としたときの平均情報量 $H(S)$ のことであり，$H(S) = -\sum_{i=1}^{n} p(s_i) \log_2 p(s_i)$ で計算される．

【安全性】

(P1)分散情報 1 個から得られる秘密情報に関する曖昧さは 0 個の場合と変わらない. i.e. $1 \leq k - L$

(P2)分散情報が 1 個失われても秘密情報が復元できる. i.e. $k \leq n - 1$

【効率性[*2]】

(Q1)分散情報の総データ量は元の秘密情報のデータ量の 2 倍以下に抑えたい．尚，分散情報の総データ量は n/L に比例する.

(Q2)データ受け入れコスト (データセンタの運用費, 接続コスト等) は n に比例する為，n は小さい方がよい.

松本らの要件によると (P1)(P2) より, $L \leq n - 2$ が得られ，(Q1) より，$n/L \leq 2$ が得られる．故に L を消去すると $4 \leq n$ となる．ここで (Q2) より，$n = 4$ が導き出され，同時に $L = 2, k = 3$ が決まる.

松本らが推薦している $(3, 2, 4)$ ランプ型秘密分散法は，秘密情報を 4 個の分散情報に分散し，3 個以上の分散情報から秘密情報を復元できる秘密分散法であり，秘密情報に関する曖昧さ（エントロピー）は，図 1 に示す様に，分散情報が 1 個の場合は 0 個の場合と変わらず，2 個の分散情報ではエントロピーが半減する不完全秘密分散法である.

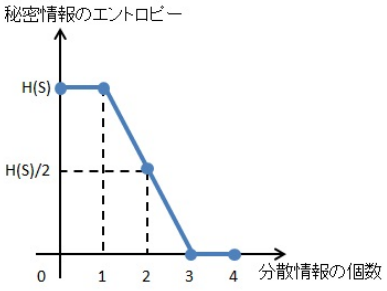

図 1 (3,2,4) ランプ型秘密分散法の特性

3.2 効率性を重視したパラメータ設定

重要な情報を扱う大規模システムでは，大災害に備えて，日本東西や海外にバックアップデータを分散させていることが多い．本論文では，上記状況に鑑み，現状 2 か所のデータセンタにマスタデータとバックアップデータが管理されている大規模システムを想定する．また，同センタで取り扱うデータは，個人情報などの機微な情報を管理するものとし，できるだけ機密性を高めたいとする.

本論文では，この現状システムを AsIs システムと呼ぶ．そして我々は，AsIs システムに対して秘密分散法の導入を試み，より機密性を高めた新たな ToBe システムを構築す

[*2] 効率性の要件は，松本らの文献 [5] では，8 個の要件を挙げているが，ここでは，ポイントとなる 2 つの要件を要約した形で記述する．詳しくは文献 [5] 参照.

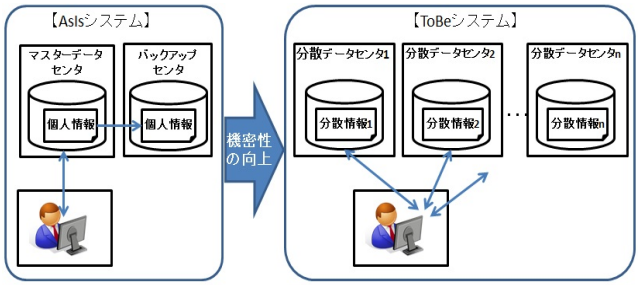

図 2 AsIs システムと ToBe システム

ることを考える．尚，ここでは，ToBe システムに必要なデータセンタの数を n とする（図 2 参照）.

この場合，松本らが推薦している (3,2,4) ランプ型秘密分散が理想的とはいえ，現状 2 センタの AsIs システムに (3,2,4) ランプ型秘密分散を適用して ToBe システムにするには，あと 2 センタ分の増資が必要となる。

我々が想定しているような大規模システムでは，1 センタ分の維持管理だけでもそれなりに費用が掛かると仮定すると，セキュリティ機能強化の為に現状の設備をいきなり倍増させるというケースは，秘密分散法の導入に向けて，かなりハードルが高いと考える.

そうかと言って，現状の 2 センタのまま秘密分散法を導入しようとすると，必然的に $k = 2$ となり，$(2, 2)$ 秘密分散法のみが適用候補なる．$(2, 2)$ 秘密分散法を適用した場合，ToBe システムは AsIs システムと比べて元データを秘密分散化させている分，機密性は向上する．しかし，データを復元するには両センタに管理されている分散情報が必要である為，どちらか片方のセンタが故障した場合，元データを復元することができなくなる．つまり，$(2, 2)$ 秘密分散法を適用した ToBe システムは，バックアップシステムを具備している AsIs システムより，可用性は低下している.

一方 $n = 3$ の場合，AsIs システムからデータセンタを 1 つ増やすことになるが，秘密分散法を適用するおかげで，機密性を向上させることができ，また，$k = 2$ とすることで，3 センタ中，1 つのデータセンタが故障した場合でも，復旧可能なシステムにすることができる[*3].

それ故，AsIs システムに秘密分散法を適用する場合，$n = 3$ が現実的と考える.

しかし，$n = 3$ の場合のランプ型秘密分散法を考えると，(P1)(P2) の条件より，$L = 1$ となり，符号化効率が Shamir の $(2, 3)$ 閾値秘密分散法と変わらなくなってしまう.

どうして $n = 3$ の場合，ランプ型秘密分散法を用いても符号化効率を上げることができなくなってしまうかというと，それは（P1) の条件があるからである.

[*3] 1 センタのダウン率を ϵ とし，どのセンタもダウン率が等しいと仮定する．また，あるセンタがダウンした際，速やかにそのセンタを復旧させるとし，同時に複数センタがダウンする確率を $\epsilon^n \fallingdotseq 0$ $(n \geq 2)$ とした場合，AsIs システムの稼働率は $1\text{-}\epsilon^2 \fallingdotseq 1$ であり，ToBe システムの稼働率も $1 - 3\epsilon^2 + 2\epsilon^3 \fallingdotseq 1$ となる.

(P1) の条件とは，「分散データ 1 個から得られる秘密データに関する曖昧さは 0 個の場合と変わらない」というものであった．この条件があるからこそ「分散情報をクラウドセンタに預けても，秘密情報は全く漏洩しない」という特徴を打ち出せるのであるが，本論文では，敢えてこの条件を下げて検討した．本論文での問題提起は以下である．

「そもそもランプ型秘密分散法は，中間的な情報漏れを許す不完全秘密分散法であるのだから，情報理論的に元データの復元が困難であれば，クラウドセンタに預けた 1 つの分散情報から，ある程度の情報漏れを許容することはできないものであろうか．」

つまり，秘密情報 s に関する曖昧さ（エントロピー）$H(S)$ が十分大きければ，クラウドセンタに分散情報を預けた時点で，例えそのエントロピーが半減し，$H(S)/2$ になってしまっても，1 つ分散情報のみからでは元の秘密情報 s を復元することが情報理論的に困難であれば，AsIs システムと比べて機密性の向上を果たすことになるのではないかというものである．勿論この問題は，そのシステムを利用する際のサービスレベル契約（SLA：Service Level Agreement）により，利用者が認めるか否かに関与する問題であり，エントロピー $H(S)/2$ が安全か否かを問う問題ではない．

そこで我々は，「秘密情報 s を復元することが情報理論的に困難であれば，エントロピーの半減を許容する」という SLA の下，図 3 の様な，(2,2,3) ランプ型秘密分散法を考察した．

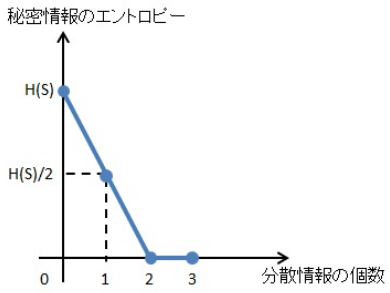

図 3 (2,2,3) ランプ型秘密分散法の特性

本 (2,2,3) ランプ型秘密分散法の特徴は，分散情報をデータセンタに預けた時点で，秘密情報 s に関するエントロピー $H(S)$ が半減するが，1 つの分散情報からでは，秘密情報 s を完全に復元することは難しいという点である．尚，(2,2,3) ランプ型秘密分散法では，分散情報の総データ量は，秘密情報 s のデータ長の $n/L = 3/2$ となっている．

このモデルを認めるのであれば，データセンタ 1 つ分の増資で，AsIs システムより機密性が高く，総データ量が AsIs システム[*4] より少ない ToBe システムを構築することができる．

[*4] AsIs システムはマスタデータおよびバックアップデータを必要とする為，総データ量は秘密情報 s のデータ長の 2 倍になっており，ToBe システムの 3/2 より大きい．

4. $(2,2,3)$ ランプ型秘密分散法

本章では，$(2,2,3)$ ランプ型秘密分散法を提案する．

$(2,2,3)$ ランプ型秘密分散法は，(k,k,n) ランプ型秘密分散法の $k=2, n=3$ の時であるので，ここでは，(k,k,n) ランプ型秘密分散の構成法について考察する．

4.1 (k,k,n) ランプ型秘密分散法の実現に向けての課題

(k,k,n) ランプ型秘密分散法は，2.2 節の (k,L,n) ランプ型秘密分散法を単純に拡張しただけでは，うまくいかない．なぜなら (k,L,n) ランプ型秘密分散法を単純に拡張しようとすると，秘密情報 s を k 個の部分情報 s_i $(0 \le i \le k-1)$ に分割し，以下の $k-1$ 次多項式 $f(x)$ を定義することになる．

$$y = f(x) = s_0 + \sum_{i=1}^{k-1} s_i x^i. \qquad (1)$$

しかし，この場合，秘密情報 s が同じであれば，$f(x)$ は常に同じ代数曲線となり，分散情報となる $f(x)$ 上の座標点 (x_i, y_i) も x 座標が同じならば，常に同じ値になってしまうからである．従って，もし，一つのデータセンタで，同じ値の 2 つの分散情報を管理しているような状況が起きた場合，「それらの元データは同じものである確率が高い」と推測できてしまう．

つまり，同じ秘密情報 s からでも，毎回異なる分散情報になるように (k,k,n) ランプ型秘密分散法を構成する必要がある．

そこで，我々は，秘密情報 s を AONT 秘密分散法 [6] を用いて毎回異なる値になるように予め変換し，変換した値を乱数とみなして，式 1 を用いて (k,k,n) ランプ型秘密分散法を構築する．これにより，同じ秘密情報 s からでも，毎回異なる分散情報になるように (k,k,n) ランプ型秘密分散法を構成することができる．

4.2 提案方式

ここでは，Shamire の (k,n) 閾値秘密分散法と Rivest の AONT 秘密分散法を組み合わせた (k,k,n) ランプ型秘密分散法を説明する．

提案方式では，秘密情報 s を AONT で用いるブロック暗号 $E()$ のブロック長 b 毎に分割する．ここでは下記の様に秘密情報 s を m 個のブロックに分割したとして説明する．

$$s = s_0||s_1||\cdots||s_{m-1}.$$

尚，記号 “||”は，データの連結を表す．

そしてブロック化された秘密情報 s を AONT 秘密分散法 [6]（Algorithm 1）を用いて毎回異なる値になるよう変換する．

まず，ランダムキー $K \in \{0,1\}^b$ を任意に選び，ブロック暗号 $E()$ を用いて，

$$s'_i = s_i \oplus E(K,i) \quad \text{for } i = 0,1,\cdots,m-1$$

を計算する．尚，ブロック暗号 $E()$ の初期値 IV は固定とする．

そして，最終ブロック s'_m は，別途，以下を計算する．

$$s'_m = K \oplus h_0 \oplus h_i \oplus \cdots \oplus h_{m-1}$$

尚，$h_i = E(K_0, s'_i \oplus i)$ であり，K_0 は固定の鍵とする．

即ち提案方式では，事前準備として予め秘密情報 $s = s_0||s_1||\cdots||s_{m-1}$ を AONT[6] を用いて $s' = s'_0||s'_1||\cdots||s'_{m-1}||s'_m$ に変換している．この時, AONT の性質上, 全ての s'_i が揃わない限り, 秘密情報 s を復元することはできない．また, 同じ秘密情報 s に対して, ランダムキー K を変えることにより, 別の値 $s'' = s''_0||s''_1||\cdots||s''_{m-1}||s''_m$ を出力することができる．

Algorithm 1: AONT

INPUT: $s = s_0||s_1||\cdots||s_{m-1}$, K_0
OUTPUT: $s' = s'_0||s'_1||\cdots||s'_{m-1}||s'_m$

(1) $K \leftarrow \{0,1\}^b$
(2) $s'_i \leftarrow s_i \oplus E(K,i)$ for $i = 0,1,\cdots,m-1$
(3) $h_i \leftarrow E(K_0, s'_i \oplus i)$ for $i = 0,1,\cdots,m-1$
(4) $s'_m \leftarrow K \oplus h_0 \oplus h_i \oplus \cdots \oplus h_{m-1}$
(5) $s' \leftarrow s'_0||s'_1||\cdots||s'_{m-1}||s'_m$
(6) **return** s'

次に提案方式では，AONT 変換後の s' に対して，k 個ずつグループ化し，以下の代数曲線 $y = f_r(x)$ を l 個 $(0 \le r \le l-1)$ 生成する．尚，簡単の為，ここでは $m+1$ が k で割り切れるとし，$m+1 = kl$ として説明する．

$$y = f_r(x) = s'_{rk+0} + \sum_{i=1}^{k-1} s'_{rk+i} x^i, \quad \text{for } 0 \le r \le l-1$$

そして各代数曲線 $f_r(x)$ に対し, $f_r(x)$ 上の点 $(x_j, f_r(x_j))$ を n 個 $(1 \le j \le n)$ とる．この作業を $0 \le r \le l-1$ まで繰り返し，$x = x_j$ に対応する各 y 座標を連結した $d_j = (x_j,\ f_0(x_j)||f_1(x_j)||\cdots||f_{l-1}(x_j))$ を分散情報とする (Algrithm 2)．

Algorithm 2: Sharing

INPUT: $s' = s'_0||s'_1||\cdots||s'_{m-1}||s'_m$
$x_1, x_2, \cdots, x_n$
OUTPUT: $d_1 = (x_1,\ f_0(x_1)||f_1(x_1)||\cdots||f_{l-1}(x_1))$,
$d_2 = (x_2,\ f_0(x_2)||f_1(x_2)||\cdots||f_{l-1}(x_2))$,
$\cdots$
$d_n = (x_n,\ f_0(x_n)||f_1(x_n)||\cdots||f_{l-1}(x_n))$

(1) $f_r(x_j) \leftarrow s'_{rk+0} + \sum_{i=1}^{k-1} s'_{rk+i} x_j^i$, for $0 \le r \le l-1,\ 1 \le j \le n$
(2) $y_j \leftarrow f_1(x_j)||f_2(x_j)||\cdots||f_l(x_j)$, for $1 \le j \le n$
(3) $d_j \leftarrow (x_j, y_j)$ for $1 \le j \le n$
(4) **return** $d_1, d_2, \cdots, d_n$

秘密情報の復元には，分散情報 d_j を k 個取得する．そして，分散情報 $d_j = (x_j,\ f_0(x_j)||f_1(x_j)||\cdots||f_{l-1}(x_j))$ の y 座標を l 分割して, 座標点 $(x_j,\ f_r(x_j))$ を l 個 $(0 \le r \le l-1)$ 生成する．

そしてパラメータ r 毎に Lagrange の補間公式を繰り返し用いて代数曲線 $f_r(x)$ の定数及び全係数を復元し，全ての代数曲線 $f_r(x)$ $(0 \le r \le l-1)$ から得られた定数及び全係数を順番通りに結合することにより，$s' = s'_0||s'_1||\cdots||s'_{m-1}||s'_m$ を復元する (Algorithm 3)．尚，Algorith 3 では，関数 $L()$ を Lagrange の補間公式を繰り返し用いた関数とし，k 個の座標点から一意に特定される代数曲線の定数及び全係数を出力するものとする．

そして s' が復元されたら AONT の逆変換により，秘密情報 s を取得する (Algorithm 4)．

Algorithm 3: Restoration

INPUT: $d_{j_1} = (x_{j_1},\ f_1(x_{j_1})||f_2(x_{j_1})||\cdots||f_l(x_{j_1}))$,
$d_{j_2} = (x_{j_2},\ f_1(x_{j_2})||f_2(x_{j_2})||\cdots||f_l(x_{j_2}))$,
$\cdots$
$d_{j_k} = (x_{j_k},\ f_1(x_{j_k})||f_2(x_{j_k})||\cdots||f_l(x_{j_k}))$
OUTPUT: $s' = s'_0||s'_1||\cdots||s'_{m-1}||s'_m$

(1) $s'_{rk+0}, s'_{rk+1}, \cdots, s'_{rk+k-1} \leftarrow L((x_{j_1}, f_r(x_{j_1})), (x_{j_2}, f_r(x_{j_2}), \cdots, (x_{j_k}, f_r(x_{j_k}))$ for $0 \le r \le l-1$
(2) $s' \leftarrow s'_0||s'_1||\cdots||s'_{m-1}||s'_m$
(3) **return** s'

Algorithm 4: AONT^{-1}

INPUT: $s' = s'_0||s'_1||\cdots||s'_{m-1}||s'_m$, K_0
OUTPUT: $s = s_0||s_1||\cdots||s_{m-1}$

(1) $h_i \leftarrow E(K_0, s'_i \oplus i)$ for $i = 0,1,\cdots,m-1$
(2) $K \leftarrow s'_m \oplus h_0 \oplus h_i \oplus \cdots \oplus h_{m-1}$
(3) $s_i \leftarrow s'_i \oplus E(K,i)$ for $i = 0,1,\cdots,m-1$
(4) $s \leftarrow s_0||s_1||\cdots||s_{m-1}$
(5) **return** s'

図 4 にて $k = 2, n = 3$ の時の $(2,2,3)$ ランプ型秘密分散法における分散化と復元化を図示する．

5. 考察とまとめ

5.1 提案方式に関する考察

提案方式ついて考察する．

本提案方式の (2,2,3) ランプ型秘密分散法の分散情報は，$x_1 = 1, x_2 = 2, x_3 = 3$ のとすると以下であることが分かる．

分散情報 $d_1 = (1, s'_0 + 1s'_1||s'_2 + 1s'_3||\cdots||s'_{2l-2} + 1s'_{2l-1})$
分散情報 $d_2 = (2, s'_0 + 2s'_1||s'_2 + 2s'_3||\cdots||s'_{2l-2} + 2s'_{2l-1})$
分散情報 $d_3 = (3, s'_0 + 3s'_1||s'_2 + 3s'_3||\cdots||s'_{2l-2} + 3s'_{2l-1})$

提案方式は，AONT で変換したブロックを 2 個づつに区切って, 区切られた 2 つのブロック s'_{2i}, s'_{2i+1} $(0 \le i \le l-1)$

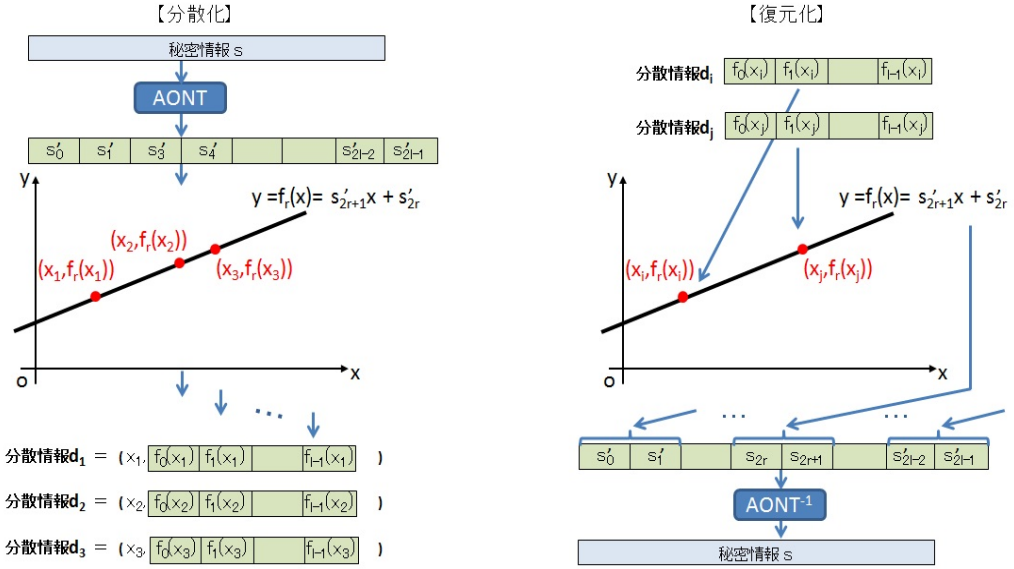

図 4 (2,2,3) ランプ型秘密分散法の分散化と復元化

を夫々足し合わせて $s'_{2i}+1s'_{2i+1}$，$s'_{2i}+2s'_{2i+1}$，$s'_{2i}+3s'_{2i+1}$ としたものを新たなブロックとしたものであり，それ故，分散情報のデータ長は，秘密情報 s のデータ長の半分になっている[*5]．

つまり提案方式は，3 個の分散データ中，2 個の分散データから秘密情報 s を復元可能で且つ，分散情報のデータ長が秘密情報 s のデータ長の 1/2 となる (2,2,3) ランプ型秘密分散法になっていることが分かる．

しかし安全性に関して考察してみると，提案方式は，AONT で変換したブロックを 3 つの分散情報に分散する方法を提供しているにすぎないことに気づく．

提案方式では，分散情報は AONT で変換した 2 つのブロック同士を数回足し合わせた値になっている為，1 つの分散情報からでは AONT で変換したブロックそのものを取得することはできないという特徴があるが，秘密情報 s に関するエントロピーは AONT の変換方法に依存する．

つまり我々は目標は，秘密情報 s に関するエントロピーが $H(s)/2$ となることを許す情報理論的安全な (2,2,3) ランプ型秘密分散法を確立することであったが，ランダムキー K のデータ長が秘密情報 s のデータ長と比べて小さいとき，提案方式では $H(s|d_i) < H(s)/2$ となっている．

5.2 まとめ

本論文では、効率性を重視した (k, L, n) ランプ型秘密分散法に関して，「秘密情報に関する曖昧さ（エントロピー）が十分大きな場合，1 つの分散情報が与えられたときの秘密情報に関する曖昧さ（エントロピー）が半減することを許容することはできないか」という問題提起を行った．

そして，具体的に，Shamire の (k, n) 閾値秘密分散法と Rivest の AONT 秘密分散法を組み合わせた $(2, 2, 3)$ ランプ型秘密分散法を提案した．本提案方式では秘密情報 s に関する条件付エントロピー $H(s|d_i)$ が目標としていた $H(s)/2$ より小さくなってしまったが，分散情報のデータ長が秘密情報 s のデータ長の 1/2 となる (2,2,3) ランプ型秘密分散法になっている．

今後は，多項式補間による秘密分散法だけでなく，排他的論理和による秘密分散法 [4] も視野に入れ秘密情報 s に関するエントロピーが $H(s)/2$ となる情報理論的安全な (2,2,3) ランプ型秘密分散法について検討をする．

[*5] AONT の変換により，分散情報が 1 ブロック分増加する場合もある

参考文献

[1] A. Shamir, “How to share a secret,” Communications of the ACM, Vol.22, No.11, pp.12-613 (1979).

[2] G.R. Blakley, “Security of ramp schemes,” Crypto’84, pp.242-268 (1984).

[3] 山本博資, “(k,L,n) しきい値秘密分散システム,” 電子通信学会論文誌, Vol. J68-A, No.9, pp.945-952 (1985).

[4] 高荒亮, 岩村恵市, “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,” CSS2009, B9-3 (2009).

[5] 松本勉, 清藤武暢, 鴨志田昭輝, 新谷敏文, 佐藤敦, “セキュアデータ保管サービス向け高速秘密分散方式,” SCIS2012, 1E2-4, (2012).

[6] R. L. Rivest, “All-or-nothing encryption and the package transform,” Fast Software Encryption FSE’97, Lecture Notes in Computer Science Vol. 1267, pp. 210-218 (1997).

[7] “国内のお客様の導入事例 Powered by AWS クラウド,” https://aws.amazon.com/jp/solutions/case-studies-jp/ [Accessed July 2017]

[8] “自治体クラウドポータルサイト”, 総務省, http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/lg-cloud/ [Accessed July 2017]

[9] “戸籍システム検討ワーキング”, 法務省, http://www.moj.go.jp/MINJI/koseki_system_index.html [Accessed July 2017]