社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (32)
2006／7／21

ランプ型秘密分散法の中間的な情報漏洩に関する二，三の考察

廣田 啓一† 茂木 一男††

† 日本電信電話株式会社，NTT 情報流通プラットフォーム研究所
〒 239-0847 神奈川県横須賀市光の丘 1-1
†† NTT コミュニケーションズ株式会社
〒 163-1421 東京都新宿区西新宿 3-20-2 東京オペラシティタワー 21F
E-mail: †hirota.keiichi@lab.ntt.co.jp, ††mogi.kazuo@ntt.com

あらまし 符号化効率の向上を目的として閾値秘密分散法を拡張したランプ型秘密分散法には，閾値未満の分散情報から秘密情報に関する情報が部分的に明らかになる，中間的な漏洩状態が存在する．従来その安全性はエントロピーに基づいて議論され，データ長分の安全性があるとされてきた．しかし，多項式を用いたランプ型秘密分散法では，部分情報同士の関係が簡易な一次式で得られるため，実データを対象とした場合に，1. 可能な解集合を少ない計算量で容易に探索でき，さらに，2. シンタックスやセマンティクスによる制約から探索範囲を狭められる可能性がある．本稿では，これらの問題を考察し，一つのアプローチとして，分散関数を複数連結することで，中間的な漏洩状態における探索計算量を増加させる結合型ランプスキームを提案する．

キーワード ランプ型秘密分散法，中間的な情報漏洩，分散関数，結合型ランプスキーム

A Study of Partial Disclosure Problem in Ramp Schemes Using Polynomial Function

– A Proposal of Cascaded Ramp Scheme –

Keiichi HIROTA† and Kazuo MOGI††

† NTT Information Sharing Platform Laboratories
Hikarinooka 1-1, Yokosuka-shi, Kanagawa, 239-0847 Japan
†† NTT Communications Corporation
Tokyo Opera City Tower 21F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo, 163-1421 Japan
E-mail: †hirota.keiichi@lab.ntt.co.jp, ††mogi.kazuo@ntt.com

Abstract Ramp scheme using polynomial function has "Partial Disclosure Problem" which some information about the secret leak partially from fewer shares than threshold. The safety of such situation has been discussed from the viewpoint of entropy and concluded it depends on data length of shares. However, in a ramp scheme, the relationship between the partial information of the secret can be obtained as a simple linear expression over finite field, so that adversary can 1. easily search the possible answer sets with less calculation, and 2. narrow the search range according to the restriction from data syntax and semantics when dealing with the real data. In this paper, we propose "Cascaded Ramp Scheme" in which more than two polynomial functions are cascaded by coefficients and arguments to increase search calculation cost.

Key words Ramp Scheme, Partial Disclosure Problem, Polynomial Function, Cascaded Ramp Scheme

1. はじめに

秘密情報を保護し，安全に保管するための技術として秘密分散法が注目されている．秘密分散法とは，関数を用いて秘密情報を分散符号化して複数個の分散情報を生成するもので，生成した全てのあるいは一定数以上の分散情報から元の秘密情報を復元可能とし，個々の分散情報や一定数より少ない数の分散情報からは元の秘密情報が復元できないため，秘密情報を安全に

分散保管することができる．例えば個人情報を秘密分散法により分散して保管すれば，必要数の分散情報を取得しない限り元の情報を復元できないことから，不正侵入などによる情報漏洩に対して安全性が高い．また，分散情報の幾つかが紛失した場合，または破損あるいは改竄された場合でも，一定数の分散情報があれば元の情報が復元できることから，災害や事故による情報の紛失・破損に対して安全性が高い．

一般に知られている秘密分散法は (k,n) 閾値秘密分散法 [1] [2] (以下，閾値秘密分散法) で，生成した n 個の分散情報の内，閾値 k 個以上の分散情報から秘密情報を復元可能とし，k 個未満の分散情報からは秘密情報が一切明らかにならない，いわゆる完全秘密分散法である．しかし，閾値秘密分散法では，生成した個々の分散情報のサイズが元の秘密情報のサイズと同じかそれ以上となるため，符号化効率が悪いことが知られている [3]．そこで，符号化効率の向上を目的とした拡張である (d,k,n) ランプ型閾値秘密分散法 (以下，ランプ型秘密分散法) が提案された [4] [5]．ランプ型秘密分散法では，秘密情報を予め d 個に分割して分散符号化するため，生成される分散情報のサイズは元の秘密情報のサイズより小さく，符号化効率が良い．その代わり，閾値未満であっても一定数以上の分散情報が集まると秘密情報を構成する部分情報同士の関係が求まり，秘密情報に関する何らかの知識が部分的に明らかになる中間的な漏洩状態が発生する．

従来，この中間的な漏洩状態の安全性はエントロピーに基づく考察の下に識論され，データ長分の安全性があるものとされてきた．しかし，多項式を用いたランプ型秘密分散法では部分情報同士の関係が有限体上の一次式の形で得られるため，部分情報として可能な解の集合を少ない計算量で探索でき，さらに，実データを対象とした場合，データに対するシンタックスやセマンティクスによる制約から探索範囲および解空間が狭められるため，比較的簡単に秘密情報が推定できてしまう恐れがある．

本稿では，こうした中間的な漏洩状態の問題について考察し，安全性を向上させるアプローチの一つとして，分散関数を複数連結することで中間的な漏洩状態における探索処理の計算量を増大させる，結合型ランプスキームを提案する．また，従来のランプ型秘密分散法と提案手法の計算量を比較し，数式処理ソフトを使った簡易な実験によりその効果を示す．

2. ランプ型秘密分散法の中間的な情報漏洩

閾値秘密分散法としては，有限体上の多項式を分散関数として用いる Shamir の閾値秘密分散法 [1] が一般的である．Shamir の閾値秘密分散法は，秘密情報 S よりも大きな素数 P を法とし，S を定数項，P より小さい乱数 R_j $(1 \leq j \leq k-1)$ を係数とする，$k-1$ 次の多項式 $f(x)$ により秘密情報を分散符号化するもので，この分散関数 $f(x)$ に任意の番号 i $(i \in Z_P,\ i \neq 0)$ を代入して，値 $W_i = f(i)$ を生成する．この番号 i と値 W_i の組を分散情報と呼ぶ．

$$f(x) = S + \sum_{j=1}^{k-1} R_j x^j \pmod{P}^{(注1)} \tag{1}$$

分散関数は $k-1$ 次の多項式であるため，生成した n 個の分散情報の内，閾値 k 個以上の任意の分散情報を集めると，$W_i = f(i)$ に関する連立方程式を解いて，あるいは Lagrange の補完公式を用いて，元の秘密情報 S を復元できる．一方，閾値未満すなわち k 個未満の分散情報からは式が解けないため，秘密情報を復元できない．このような秘密分散法を，完全秘密分散法という．閾値秘密分散法では，生成した個々の分散情報の値 W_i のサイズ $|W_i|$ が元の秘密情報のサイズ $|S|$ に対し，$|W_i| \geqq |S|$ となることが知られている [3]．n 個の分散情報を生成すれば総情報量は $n|S|$ 以上となり，符号化効率が悪い．

一方，多項式を用いたランプ型閾値秘密分散法 [4] は，秘密情報を予め d 個の部分情報 S_t $(1 \leq t \leq d)$ に分割し，この部分情報を定数項および係数とする $k-1$ 次の多項式を使って，分散情報の値 $W_i = f(i)$ を生成するものである．

$$f(x) = \sum_{t=1}^{d} S_t x^{t-1} + \sum_{j=1}^{k-d} R_j x^{j+d-1} \pmod{P} \tag{2}$$

ランプ型秘密分散法では，生成される個々の分散情報の大きさは $|W_i| \geqq |S|/d$ と小さくなり，符号化効率が良い [6]．ただし，ランプ型秘密分散法は不完全秘密分散法 [7] であり，閾値 k 未満 $k-d+1$ 個以上の分散情報が集まった場合に，秘密情報に関する何らかの知識が部分的に漏洩する，中間的な情報漏洩状態が発生する．

2.1 中間的な情報漏洩状態

多項式を用いたランプ型秘密分散法では，一定数以上の分散情報を表す連立方程式があれば，中間的な情報漏洩状態として，乱数の項を全て消去した部分情報間の関係式が求められる．

例えば閾値 $k=3$ のランプ型秘密分散法で，秘密情報 S を 2 個の部分情報 S_1，S_2 に分割するものとすると，分散関数 $f(x)$ は次の式で表現される．

$$f(x) = S_1 + S_2 x + R x^2 \tag{3}$$

この分散関数により生成される任意の 2 個の分散情報をそれぞれ $W_a = f(a)$，$W_b = f(b)$ $(a,b \in Z_P,\ a \neq b)$ とおくと，以下の連立方程式が得られる．

$$\left.\begin{aligned} W_a &= S_1 + S_2 a + R a^2 \\ W_b &= S_1 + S_2 b + R b^2 \end{aligned}\right\} \tag{4}$$

連立方程式から乱数 R を消去することで，次のような部分情報 S_1 と S_2 の関係式を得ることができる．

$$S_2 = -\frac{a+b}{ab} S_1 + \frac{a^2 W_b - b^2 W_a}{ab(a-b)} \tag{5}$$

この関係式は一次式であるため，a, b, W_a, W_b が与えられると，仮定した S_1 に対する S_2 を少ない計算量で一意に計算でき，よって S_1，S_2 として可能な解の集合が容易に求められる．したがって，結果として秘密情報 S が推定できてしまう恐れがある．

(注1)：以降，特に明記のない限り，全ての数式は有限体 Z_P 上で計算されるものとし，$\bmod P$ は記述を省略する．

表 1　アクセス集合の解空間とエントロピー
Table 1　Access subsets and entropies.

アクセス集合	S_1	S_2	S	$H(S\|A)$
A_S	1	1	1	0
A_R	2^L	2^L	2^L	H(S)/2
A_T	2^L	1	2^L	H(S)/2
A_0	2^L	2^L	2^{2L}	H(S)

こうした中間的な漏洩状態の安全性は，従来エントロピーに基づく考察の下に議論されてきた．分散情報の任意の組み合わせの集合 A について，秘密情報 S が復元可能な組み合わせ（$|A| \geq k$）をアクセス集合 A_S とおくと，A_S では S_1，S_2 が一意に定まり，S が求まるため，そのエントロピー $H(S|A)$ は 0 である．一方，秘密情報が一切復元できない組み合わせ（$|A| \leq k-d$）の集合 A_0 では，S_1，S_2 のデータ長をそれぞれ L bit とすれば，S は $2L$ bit 分の曖昧性を持ち，そのエントロピーは $H(S)$ である．中間的な漏洩状態（$k-d < |A| < k$）のアクセス集合を A_R とおくと，S_1，S_2 はそれぞれ L bit 分の曖昧性を持つが，関係式により S_1 と S_2 が対応付けられるため，S も同様に L bit 分しか曖昧性を持たない．この時，エントロピーは $H(S)/2$ と A_S の半分になる（表 1）．

なお，多項式を用いたランプ型秘密分散法では，特殊な組み合わせとして，一部の部分情報の値が一意に求まる閾値未満の分散情報の組み合わせが存在する [8] [9]．この組み合わせを A_T（$A_T \in A_R$）とすると，例えば S_1 は L bit 分の曖昧性を持つが，S_2 が一意に定まるため，秘密情報 S としては L bit 分の曖昧性しか持たない．この時，エントロピーは A_R と同様に $H(S)/2$ である．文献 [5] [9] では，こうした集合 A_T が存在する秘密分散法を弱いランプ型秘密分散法と定義し，A_R のみを許す強いランプ型秘密分散法の構築を課題としてあげている．

2.2　中間的な漏洩状態における解空間の制約

前節で述べたように，ランプ型秘密分散法における中間的な漏洩状態では，関係式による制約で部分情報の曖昧性が制限されるため，秘密情報に関するエントロピーが減少する．しかし，部分情報の組み合わせである秘密情報 S に関して，少なくともデータ長 L bit 分の解空間があることをもって，エントロピーに基づく考察の下に安全であるとされてきた．

しかしながら，実データを対象とした場合，中間的な漏洩状態における解空間は，データに対する種々の制約に従って，データ長分の解空間よりも遥かに狭いものとなる場合がある．

例えば，分散符号化の対象となるデータが人名や住所など意味のある情報であった場合，推定した部分情報の組み合わせが取りうる解空間は，データの文字種や統語規則などのシンタックスによる制約から，あらかじめある程度狭めることができる．これにデータが人名であることのセマンティクスによる制約が加われば，解空間はさらに制限されることになる．こうした制約により解空間が制限された状態で，中間的な漏洩状態として部分情報間の関係式が明らかになれば，その関係式による解空間の制約は極めて強いものとなると考えられる（図 1）．なお，図 1 では関係式による解の制約を一線分上の点として表現した

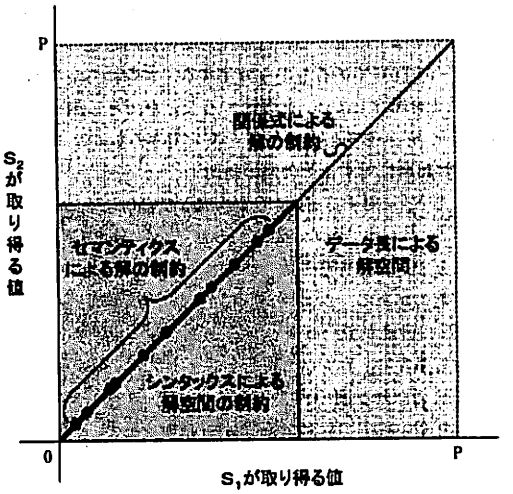

図 1　中間的な漏洩状態における制約のイメージ
Fig. 1　Image of Constraints between Partial Information.

が，部分情報間の関係式は素数 P を法とする一次式であるため，実際には離散的な値を取る．

単純な例として，個人情報である氏名を秘密情報として分散した場合の解空間について考える．氏名を姓と名 2 文字ずつ（4 byte×4 byte）の部分情報として分割した場合，データ長による解空間の広さは S_1，S_2 のそれぞれについて 4.3×10^9 で，組み合わせによる解空間の広さは単純に 1.85×10^{19} である．

これに対し，データが人名であることから，シンタックスによる解空間の制約を考える．戸籍法 [10] により，人名に使える文字は人名漢字 983 字，常用漢字 1945 字，ひらがな・カタカナ，長音・同音・同字記号の合わせて 3101 字に限定されており，したがって任意の 2 文字の組み合わせは 9.6×10^6 と，データ長による解空間の約 500 分の 1 になる．人名であることのセマンティクスを考慮すると，実際の解空間はさらに制約される．日本における戸籍上の苗字の種類は表記で約 10 万種，読みで約 30 万種 [11] と言われており，したがって，任意の 2 文字から構成される姓が有意である（人名として成立する）割合は，およそ 100 分の 1 である．

こうした解空間の制約は，中間的な漏洩状態の安全性を著しく低下させる．そもそも部分情報同士の関係式は有限体上の一次式であるため，S_1 を仮定すれば比較的少ない計算量で S_2 を算出することができる．一回の計算量を $O(1)$ で与えると，総当りによる探索処理の計算量は高々 $O(P)$ で，可能な全ての解の集合を求めることができる．シンタックス・セマンティクスによる制約に基づいて，S_1 として可能な解空間の大きさを $\lfloor S_1 \rfloor$ とおけば，計算量は $O(\lfloor S_1 \rfloor)$ で表され，制約が強ければ強いほど少ない計算量で S_2 として可能な解の集合が得られる．

なお，こうした解空間の制約に対し，分散符号化の対象となる S_1 および S_2 を予め所定の方式で符号化あるいは暗号化することで，シンタックス・セマンティクスによる制約を回避する手段も考えられる．しかしながら，秘密分散法において復元

者は閾値数の分散情報から秘密情報を復元できなければならず，したがって本稿ではそうした符号化あるいは暗号化の手段は攻撃者にとって既知であるものと仮定する．すなわち，攻撃者は任意の平文を想定して S_1 を仮定することができ，関係式により算出した S_2 から対応する平文を復元できるものとする．

2.3 解集合に対するその他の制約

仮定した S_1 に対する S_2 が関係式により得られると，今度は算出した S_2 が有意であるかどうかの判定を解空間の制約に従って行うことで，秘密情報 S として可能な解の集合をさらに制限できる可能性がある．例えば，既に名簿が流出しているなど予め S_1，S_2 の候補が分かっている場合や，S_2 に関する辞書的な情報がある場合に，そうした判定を行うオラクルを仮定すれば，S として可能な解空間の大きさ $\lfloor S \rfloor$ は $\lfloor S \rfloor = \lfloor S_2 \rfloor \leq \lfloor S_1 \rfloor$ となり，より高い確率で秘密情報 S が推定できる．

S_1 と S_2 の関係式は有限体上の一次式であるため，計算結果は離散的な値を取る．したがって，S_1 を仮定して算出した S_2 がシンタックス上およびセマンティクス上有意であるかどうかは確率的であると考えられ，この確率がデータ長による解空間内で均一であると仮定すれば，先ほどの例で算出した S_2 がシンタックス上有意である確率は約 500 分の 1 である．さらにセマンティクス上で名に関する制約も姓に関する制約と同様約 100 分の 1 とすれば，S_1 と S_2 の関係式により推定した 2 文字の姓と名が有意である組み合わせはたったの 2 通りしかない計算となる．

本稿で示したのは極端な例であるが，従来のランプ型秘密分散法の中間的な漏洩状態において部分情報の関係式が明らかになると，こうしたシンタックスやセマンティクスによる制約の下で秘密情報が推定できる危険性が高くなることを示唆している．ただし，これらの制約はデータの特性によって大きく異なり，特にデータ長とセマンティクスによる制約との関係は一様ではないため，一概に危険性は定義できない．例えば四字熟語を秘密情報とした場合，常用漢字 4 文字の取り得る組み合わせが 1.6×10^{13} 通りあるのに対し，有意な四字熟語は高々8000 語程度しか知られていない．一方，パスワードや暗号鍵などの場合は，セマンティクスによる制約はほぼないに等しい．

また，推定した秘密情報に対する制約としては，個々のデータに対するシンタックス・セマンティクスによる制約だけでなく，複数のデータの関連性により定まるリレーショナルな制約も考慮する必要がある [12]．例えば人名と口座番号との関連性から，口座番号と暗証番号の組み合わせの有意性が定まるような状況を考えれば，その危険性は無視できない．

3. 結合型ランプスキームの提案

2.2 節で示したように，中間的な漏洩状態では部分情報の関係が単純な一次式により表現されるため，少ない計算量で部分情報の組み合わせが推定でき，総当りによる探索が容易に可能である．特に，データに対してシンタックスによる制約や辞書的な制約があると探索範囲が狭められるため，その計算量は著しく小さくなる．

我々は，こうした中間的な漏洩状態における推定処理の計算量の問題は，実データを扱う上で重要であると考え，複数の分散関数を連結することで安全性の向上を図るアプローチの検討を進めている．

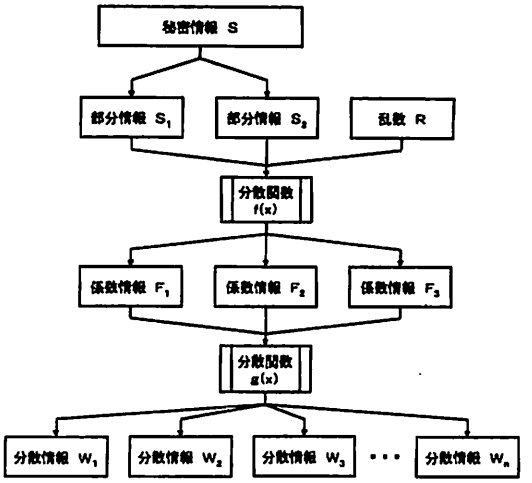

図 2 分散関数の直列による結合型ランプスキーム
Fig. 2 Image of Cascaded Ramp Scheme.

本稿では，秘密情報 S を従来のランプ型秘密分散法の分散関数 $f(x)$ を使って分散した上で，生成した分散情報群を係数とする新たな分散関数 $g(x)$ により任意の個数の分散情報を生成する，分散関数の直列による結合型ランプスキーム (Cascaded Ramp Scheme) を提案する (図 2)．

3.1 秘密情報の分散

本稿のアプローチでは，秘密情報 S を一段目の分散関数により k 個の分散情報に分散した上で，これらの分散情報を二段目の分散関数の係数として用いる．以下，順に説明する．

まず，秘密情報 S を d 個の部分情報 S_t $(1 \leq t \leq d)$ に分割し，$k-d$ 個の乱数 R_j $(1 \leq j \leq k-d)$ を生成して，素数 P を法とする従来のランプ型秘密分散法の分散関数 $f(x)$ を構成する (式 (2))．この分散関数 $f(x)$ に k 個の番号を代入して係数情報 F_i $(1 \leq i \leq k)$ を順次生成する．この時，既に生成した係数情報 F_i を次の係数情報 F_{i+1} を生成するための番号として使用する．すなわち，算出した係数情報を以下の式により再帰的に使用して，係数情報群を生成する．

$$F_i = f(F_{i-1}) \tag{6}$$

ただし，$F_i \neq 0$ かつ $F_i \neq F_j$ $(1 \leq j < i)$ とし，これを満たさない場合は乱数 R_j を再度生成し直して，分散関数 $f(x)$ を再構成する．

次に，生成した k 個の係数情報 F_i を使い，素数 P を法とする次のような分散関数 $g(x)$ を形成する．

$$g(x) = \sum_{i=1}^{k} F_i x^{i-1} \pmod{P} \tag{7}$$

この分散関数 $g(x)$ に任意の番号 i を代入して値 $W_i = g(i)$ を生成し，番号 i と値 W_i の組を分散情報とする．

3.2 秘密情報の復元

生成した n 個の分散情報に対し，任意の k 個の分散情報から元の秘密情報 S が復元できる．まず，k 個の分散情報について分散関数 $g(x)$ に基づく k 個の連立方程式をたて，これを解くことにより k 個の係数情報 F_i が求まる．

$$\begin{bmatrix} 1 & x_1 & \cdots & x_1^{k-1} \\ 1 & x_2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & \cdots & x_k^{k-1} \end{bmatrix} \begin{bmatrix} F_1 \\ F_2 \\ \vdots \\ F_k \end{bmatrix} \equiv \begin{bmatrix} W_{x_1} \\ W_{x_2} \\ \vdots \\ W_{x_k} \end{bmatrix} \tag{8}$$

k 個の係数情報 F_i が求まれば，次に分散関数 $f(x)$ に基づく k 個の連立方程式をたて，これを解くことにより d 個の部分情報 S_t と $k-d$ 個の乱数 R_j をそれぞれ求めることができる．すなわち，秘密情報 S が復元できる．

$$\begin{bmatrix} 1 & F_0 & \cdots & F_0^{k-1} \\ 1 & F_1 & \cdots & F_1^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & F_{k-1} & \cdots & F_{k-1}^{k-1} \end{bmatrix} \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ R_{k-d} \end{bmatrix} \equiv \begin{bmatrix} F_1 \\ F_2 \\ \vdots \\ F_k \end{bmatrix} \tag{9}$$

3.3 提案手法における中間的な漏洩状態

従来のランプ型秘密分散法では，個々の分散情報が S_t および R_j に関して一次式であるため，k 個未満 $k-d+1$ 個以上の分散情報があれば，乱数 R_j を消去して部分情報 S_t だけの関係式を容易に導くことができた．

提案手法における個々の分散情報 W_i は，部分情報 S_t と乱数 R_j の式で書き表すと，従来のランプ型のような一次式ではなく，多次多項式となる．この時，$k-d+1$ 個以上の分散情報を表す連立方程式から終結式を求めることで，乱数 R_j を全て消去した部分情報 S_t だけの関係式が導出できる．ただし，提案手法では，得られる関係式もまた部分情報 S_t に関する多次多項式となるため，解候補の算出には有限体上での多項式の因数分解が必要となり，計算量が従来に比べて増加する．

なお，一段目の分散関数における乱数 R_j の最大次数を k_R，部分情報 S_t を項とする最大の次数を k_S とすると，分散関数を2個連結した場合の分散情報における乱数 R_j の最大次数 k'_R および部分情報 S_t の最大次数 k'_{S_t} は，それぞれ以下の式で与えることができる．

$$k'_R = \sum_{i=1}^{k-1}(k-1)^i + 1 \tag{10}$$

$$k'_{S_t} = (k-1)^{k-1} \tag{11}$$

さらに言えば，分散関数の連結は2個に限る必要はなく，任意の個数連結しても良い．$k-1$ 次の分散関数を c 個連結した場合の分散情報における乱数 R_j および部分情報 S_t の最大次数 k'^c_R，$k'^c_{S_t}$ はそれぞれ以下の式で与えられる．

$$k'^c_R = \{\sum_{i=1}^{k-1}(k-1)^i + 1\}^{c-1} \tag{12}$$

$$k'^c_{S_t} = (k-1)^{k-1}\{\sum_{i=1}^{k-1}(k-1)^i + 1\}^{c-2} \tag{13}$$

4. 最小構成による例示

以下では，結合型ランプスキームの最小構成として，閾値 $k=3$ で，二次の分散関数を2個連結した場合について，具体的な計算例を交えて説明する．

4.1 分散処理

まず，分散対象の秘密情報を人名「電信太郎」として，姓名2文字ずつを部分情報として分散符号化するものとする．S-JIS コードを数値化して，$S_1 = 2472841293$ (9364904D)，$S_2 = 2445187161$ (91BE9859) を得る．素数 $P = 4294967291$ (FFFFFFFB)，乱数 $R = 1234567890$ とすると，一段目の分散関数 $f(x)$ により，3個の係数情報が次のように算出される．

$$\left.\begin{aligned} F_1 &= S_1 + S_2 + R = 6152596344 \\ &\equiv 1857629053 \\ F_2 &= S_1 + S_2 F_1 + R F_1^2 \\ &= 4260229223242901271038092836 \\ &\equiv 2167034091 \\ F_3 &= S_1 + S_2 F_2 + R F_2^2 \\ &= 579757618902999139829536 4034 \\ &\equiv 2060982233 \end{aligned}\right\} \tag{14}$$

次に，これら3個の係数情報を項とする二段目の分散関数 $g(x)$ により，分散情報 $W_i = g(i)$ として任意の n 個の分散情報を生成する．

$$\left.\begin{aligned} W_1 &= F_1 + F_2 + F_3 = 6085645377 \\ &\equiv 1790678086 \\ W_2 &= F_1 + 2F_2 + 4F_3 = 14435626167 \\ &\equiv 1550724294 \\ W_3 &= F_1 + 3F_2 + 9F_3 = 26907571423 \\ &\equiv 1137767677 \\ W_4 &= F_1 + 4F_2 + 16F_3 = 43501481145 \\ &\equiv 551808235 \end{aligned}\right\} \tag{15}$$

4.2 復元処理

用いた分散関数が二次の多項式であるため，任意の3個の分散情報を集めれば，連立方程式を解いて係数情報が復元できる．

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 4 & 16 \end{bmatrix} \begin{bmatrix} F_1 \\ F_2 \\ F_3 \end{bmatrix} \equiv \begin{bmatrix} 1790678086 \\ 1550724294 \\ 551808235 \end{bmatrix} \tag{16}$$

上記を解けば，$F_1 = 1857629053$，$F_2 = 2167034091$，$F_3 = 2060982233$ が得られる．次に，係数情報に関する連立方程式を解くことで，秘密情報が復元できる．

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1857629053 & (1857629053)^2 \\ 1 & 2167034091 & (2167034091)^2 \end{bmatrix} \begin{bmatrix} S_1 \\ S_2 \\ R \end{bmatrix} \equiv \begin{bmatrix} 1857629053 \\ 2167034091 \\ 2060982233 \end{bmatrix} \tag{17}$$

上記を解けば，$S_1 = 2472841293$，$S_2 = 2445187161$ が得られ，秘密情報 S が正しく求められることが分かる．

4.3 中間的な漏洩状態

最小構成における中間的な漏洩状態，すなわち2個の分散情報がある場合について述べる．個々の分散情報を部分情報 S_1，S_2 と乱数 R で書き表すと，その式は S_1，S_2 について4次，R について7次の多次多項式となる．

$$\begin{aligned}W_i = {} & S_1+S_2+R+i\{S_1+S_1S_2+S_2^2+\{S_2+S_1^2+2S_1S_2\\ & +S_2^2\}R+2(S_1+S_2)R^2+R^3\}+i^2\{S_1+S_1S_2+S_1S_2^2\\ & +S_2^3+(S_1^2+S_2^4+2S_1S_2^3+S_2^3+S_1^2S_2^2+4S_1S_2^2+S_2^2\\ & +3S_1^2S_2)R+(2S_1^3S_2+4S_1^2S_2+4S_1S_2+2S_1^3+2S_2^4\\ & +6S_1S_2^3+2S_2^3+6S_1^2S_2^2+4S_1S_2^2+2S_2^2)R^2+(S_2^4\\ & +4S_1S_2^3+6S_2^3+6S_1^2S_2^2+S_2^2+12S_1S_2^2+4S_1^3S_2\\ & +6S_1^2S_2+4S_1S_2+S_2+S_1^4+4S_1^2)R^3+(4S_2^3+12S_1S_2^2\\ & +6S_2^2+12S_1^2S_2+6S_1S_2+4S_1^3+2S_1)R^4+(6S_2^2\\ & +12S_1S_2+2S_2+6S_1^2)R^5+4(S_1+S_2)R^6+R^7\} \quad (18)\end{aligned}$$

2個の分散情報を表す連立方程式から終結式を求め，乱数 R を消去することで，部分情報 S_1 と S_2 の関係式が得られる．ここでは，分散情報 W_1 と W_2 を得たものとして，数式処理ソフト Risa/Asir [13] [14] を用いて終結式の導出を行った結果，S_1 について3次，S_2 について4次，次数4の以下のような多次多項式が関係式として得られた．

$$\begin{aligned}& 1936665564S_2^4-1138639680S_2^3+S_1(-1596215899S_2^3\\ & +1290289367S_2^2-1703895075S_2-257799499)\\ & -1393397461S_2^2+S_1^2(781191675S_2^2-1645294515S_2\\ & +310492095)+2102457833S_2+S_1^3(111399563S_2\\ & +1154405104)-1390587700\equiv 0 \quad (19)\end{aligned}$$

関係式を得た後は，S_1 として可能な解の集合を使って，総当りで探索することになる．関係式に S_1 として可能な解を代入し，有限体 Z_P 上で因数分解すれば，S_2 として可能な解が得られる．例えば，仮に $S_1=2472841293$ を代入すれば，以下の式が得られる．

$$\begin{aligned}& 1936665564S_2^4+829530064S_2^3-1348473645S_2^2\\ & +900318656S_2-636093271\equiv 0 \quad (20)\end{aligned}$$

これを因数分解すれば，

$$\begin{aligned}& (S_2+1849780130)(S_2^3+906385629S_2^2\\ & +1282866770S_2+2659632255)\equiv 0 \quad (21)\end{aligned}$$

となり，$S_2=2445187161$ が求まる．

先に得た関係式 (19) が S_2 に関して4次式であるため，S_1 を仮定して因数分解した場合に，S_2 として可能な解は $\{0,1,2,4\}$ 個得られる．一方，S_1 に関しては3次式であるため，S_2 を仮定すれば S_1 として可能な解は $\{0,1,3\}$ 個得られる．したがって，S_1 よりも S_2 の方が可能な解空間が狭い場合には，S_2 による総当り探索が効率的と考えられる．

以上のように，提案手法においても，分散情報を示す多次多項式の連立方程式から終結式を導出して乱数項を消去することで，閾値未満の分散情報群から部分情報間の関係式を導出することができる(注2)．ただし，導出した関係式から秘密情報を推定するためには，部分情報の一部を仮定して代入演算した上で有限体上での因数分解を行う必要がある．これにより，総当り探索の計算量が大きく増加することが期待できる．

4.4 分散情報の特殊な組み合わせ

最小構成において，閾値未満の2個の分散情報 W_a，W_b $(a,b\in Z_P,\ a\neq b)$ に関して，次のような特殊な組み合わせがあることが分かっている．

4.4.1 分散情報の値が一致する組み合わせ

2個の分散情報の値が一致，すなわち $W_a=W_b$ が成立する分散情報の組み合わせが $(P-3)/2$ 通り存在し，この時 $a+b$ の値は定数である．また，そのような分散情報の番号 a と b の組み合わせから，S_1，S_2，R の関係式を求めることができる．

$$W_a-W_b=(F_1+F_2a+F_3a^2)-(F_1+F_2b+F_3b^2)=0 \quad (22)$$

かつ $a\neq b$ より，

$$a+b=-\frac{F_2}{F_3} \quad (23)$$

が得られる．係数情報 F_2，F_3 を S_1，S_2，R で書き表すと，次の関係式が得られる．

$$\begin{aligned}& (a+b)\{S_1+S_1S_2+S_1S_2^2+S_2^3+(S_1^2+S_2^4+2S_1S_2^3+S_2^3\\ & +S_1^2S_2^2+4S_1S_2^2+S_2^2+3S_1^2S_2)R+(2S_1^3S_2+4S_1^2S_2+4S_1S_2\\ & +2S_1^3+2S_2^4+6S_1S_2^3+2S_2^3+6S_1^2S_2^2+4S_1S_2^2+2S_2^2)R^2\\ & +(S_2^4+4S_1S_2^3+6S_2^3+6S_1^2S_2^2+S_2^2+12S_1S_2^2+4S_1^3S_2\\ & +6S_1^2S_2+4S_1S_2+S_2+S_1^4+4S_1^2)R^3+(4S_2^3+12S_1S_2^2\\ & +6S_2^2+12S_1^2S_2+6S_1S_2+4S_1^3+2S_1)R^4+(6S_2^2+12S_1S_2\\ & +2S_2+6S_1^2)R^5+4(S_1+S_2)R^6+R^7\}+S_1+S_1S_2+S_2^2\\ & +(S_2+S_1^2+2S_1S_2+S_2^2)R+2(S_1+S_2)R^2+R^3\equiv 0 \quad (24)\end{aligned}$$

ただし，この関係式は分散情報の連立方程式から派生したものであり，終結式を求めても部分情報同士の新たな関係式が得られることはなく，提案手法の安全性に影響はないと考えられる．

4.4.2 係数情報 F_2 が一意に求まる組み合わせ

任意の2個の分散情報について，$a+b\equiv 0$ の関係が成り立つ時，係数情報 F_2 が一意に求まり，同時に F_1 と F_3 の関係式が求まる [8]．

$$\left.\begin{aligned}W_a &= f(a)=F_1+F_2a+F_3a^2\\ W_b &= f(P-a)=F_1-F_2a+F_3a^2\end{aligned}\right\} \quad (25)$$

より，

$$F_2=\frac{W_a-W_b}{2a} \quad (26)$$

$$2F_1+2F_3a^2=W_a+W_b \quad (27)$$

(注2)：Risa/Asir では，最小構成以外は終結式の導出途中で停止し，関係式を確認することはできなかった．

が得られる．

ただし，この組み合わせから係数情報 F_2 の値が一意に特定できても，F_2 は元々 S_1，S_2，R からなる分散情報であるため，F_2 から部分情報の値を推定することはできない．また，これらの関係式は分散情報の連立方程式から派生したものであり，終結式を求めても部分情報同士の新たな関係式が得られることはなく，提案手法の安全性に影響はないと考えられる．

5. 計算量と処理時間の評価

本稿における提案は，分散関数を複数連結して係数情報を再帰的に使用することで生成される分散情報を多次多項化し，中間的な漏洩状態における秘密情報の推定にかかる計算量を増加させることを目的としている．

そこで，最小構成の結合型ランプスキームと従来のランプ型秘密分散法を数式処理ソフト Risa/Asir 上で簡易に実装し，分散処理，復元処理および推定処理のそれぞれについて処理時間を計測し，評価を行った．

5.1 分散処理

最小構成では，秘密情報の分散時に 2 回の分散処理を行う．初回の分散処理では閾値 k 個分の係数情報を生成するだけなので，n 個の分散情報を生成する計算量は高々 $O(n+k)$ である．ただし，生成する分散情報の個数により見た目上の速度は $(n+k)/n$ 倍となる．

図 3 に，1 回の処理で 10 万個の分散情報を生成した場合と，5 個の分散情報を 2 万回生成した場合の計測結果を示す．

後者について比較すると，提案手法の処理時間はランプ型秘密分散法のほぼ 1.6 倍である．なお，グラフ上でデータ長が 32 bit を境に処理時間が大きく増加しているのは Risa/Asir のデータ型および処理構造によるもので，同様の理由から 64 bit の場合は逆に処理時間が減少している．

5.2 復元処理

最小構成では，秘密情報の復元時には分散時と同様 2 回復元処理を行う必要がある．したがって，計算量的には単純に 2 倍になると考えられる．

図 4 に，40 個の分散情報から任意の 3 個を選ぶ全ての組み合わせについて復元処理を行った場合と，3 個の分散情報から単純に 1 万回復元処理を行った場合の計測結果を示す．

従来のランプ型ではデータ長によらずほぼ処理時間が一定であるのに対して，結合型ランプスキームではデータ長に比例する形で，処理時間が増加していることが分かる．これは，係数情報群から秘密情報を復元する際に，データ長に従った大きな値が分散情報の番号として使用されるためで，有限体上での剰余演算が処理時間に影響しているものと思われる．

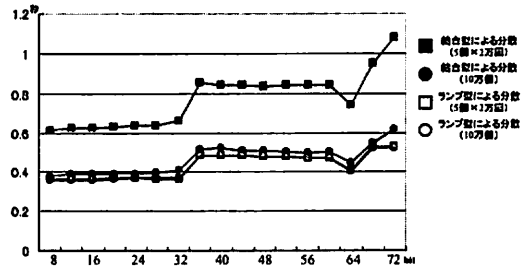

図 3 分散処理における処理時間の計測結果

Fig. 3 Calculation time in dispersion process.

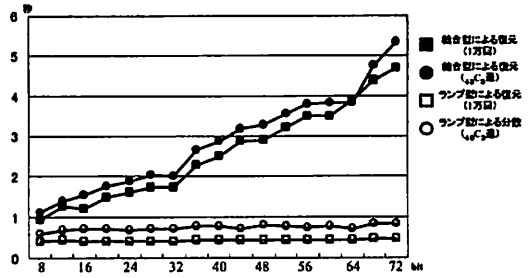

図 4 復元処理における処理時間の計測結果

Fig. 4 Calculation time in reconstruction process.

5.3 推定処理

最後に，中間的な漏洩状態における秘密情報の推定処理として，分散情報 W_1 と W_2 から関係式を導出し，総当りによる探索を行う場合の処理時間を計測した．

図 5 に，2 個の分散情報から関係式を予め導出した上で，1×10^4 通りの S_1 を仮定して S_2 の算出を行った場合と，逆に S_2 を 1×10^4 通りに仮定して S_1 の算出を行った場合の計測結果を示す．

ランプ型秘密分散法の場合，関係式は簡易な一次式であるため，一定の範囲内での探索にかかる処理時間はきわめて短く，ほぼ一瞬で完了する．これに対し，提案する結合型ランプスキームでは，データ長に従って処理時間が大きく増加している．これは，仮定した S_1 ないしは S_2 を代入して有限体上で演算した上で因数分解を行っているためで，分散関数の次数および連結の個数を増やして分散情報の次数を高めれば，処理時間がさらに増加することは明らかである．最小構成の場合，得られる関係式が S_1 について 3 次，S_2 について 4 次であるため，S_1 を仮定しての推定処理の方が処理時間を要している．なお，終結式の計算による関係式の導出にかかる処理時間は，推定処理の中のごく一部と考えられるため，特に評価はしていない．

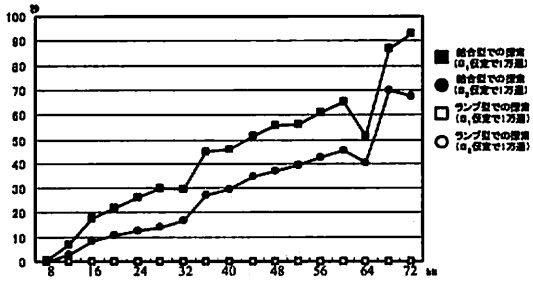

図 5 推定処理における処理時間の計測結果

Fig. 5 calculation time in estimation process

表 2 推定処理における計測結果と全探索時間の推定結果
Table 2 Estimated calculation time for full range search.

	範囲内探索 (1 万通)		全探索 (推定値)	
データ長	ランプ型	結合型	ランプ型	結合型
16 bit	0.0736	17.96	0.4822	1.176×10^2
32 bit	0.0624	29.54	2.684×10^4	1.269×10^7
48 bit	0.0719	55.73	2.023×10^9	1.569×10^{12}
64 bit	0.0532	51.56	9.814×10^{13}	9.511×10^{16}

また，表 2 に，計測結果から推定した，データ長分の解空間の全探索に要する時間を示す．データ長にもよるが，提案手法における中間的な漏洩状態の推定処理にかかる時間は，ランプ型秘密分散法に比べて大きく増加している．数式処理ソフト上での簡易な実装であるため一概には言えないが，安全性の向上について提案手法が有効であるものと考える．

6. おわりに

本稿では，ランプ型秘密分散法の中間的な漏洩状態における解空間の制約と安全性の関係について考察し，安全性の向上を図る一つのアプローチとして，複数の分散関数を結合することにより，秘密情報の推定を困難にする結合型ランプスキームを提案した．

提案手法は，入力された秘密情報に対し，まず一段目の分散関数により閾値個の係数情報を生成し，生成した係数情報からなる二段目の分散関数を用いて，任意の個数の分散情報を生成するもので，係数情報の生成の際に既に生成した係数情報を再帰的に用いることで，最終的に生成される分散情報における乱数および部分情報の次数を高めている．これにより，中間的な漏洩状態において，終結式の計算による分散情報からの関係式の導出と，有限体上での代入演算および多項式の因数分解による関係式からの秘密情報の推定処理にかかる計算量が大きく増加する(注3)．

最小構成による提案手法を数式処理ソフト Risa/Asir 上で簡易に実装し，従来のランプ型秘密分散法との間で処理時間の比較を行った．結果として，分散処理および復元処理における処理時間の増加が僅かであるのに対し，閾値未満の分散情報から可能な解集合の探索を行う推定処理では，処理時間が大きく増加することが確認できた．よって，提案手法はランプ型秘密分散法における中間的な漏洩状態の安全性を向上させる有効なアプローチであると言える．

また，本手法で生成された分散情報の閾値未満の組み合わせから一部の部分情報の値が一意に求まることはない．すなわち，文献 [5] [9] で定義される，強いランプ型秘密分散法が提案手法により実現できたものと考えられる．

文 献

[1] Shamir, A.: How to Share a Secret, *Communications of the ACM*, Vol. 22, No. 11, pp. 612–613, 1979.

[2] Blakley, G. R.: Safeguarding cryptographic keys, *Proc. AFIPS 1979 National Computer Conference*, AFIPS, pp. 313–317, 1979.

[3] Karnin, E.D., Greene, J.W. and Hellman, M.E.: On Secret Sharing Systems, IEEE Trans. Inf. Theory, Vol. IT-29, pp. 35–41, 1983.

[4] Blakley, G. R. and Meadows, C.: Security of Ramp Scheme, *Proc. Of Crypto'84*, Lecture Notes in Computer Science, No. 196, pp. 242–268, 1984.

[5] 山本博資: (k,L,n) しきい値秘密分散システム, 信学論 (A), Vol. J68A, No. 9, pp. 945–952, 1985.

[6] Ogata, W. and Kurosawa, K.: Some Basic Properties of General Nonperfect Secret Sharing Schemes, *Journal of Universal Computer Science*, Vol. 4, No. 8, pp. 690–704, 1998.

[7] Ogata, W., Kurosawa, K. and Tsujii, S.: Nonperfect Secret Sharing Schemes, Proceedings of Auscrypt '92, LNCS718, pp. 56–66, 1992.

[8] 廣田啓一, 北原亮, 遠藤雅和, 山室雅司: ランプ型閾値秘密分散法における部分情報の復元制御, 信学技報, Vol. 103, No. 416, pp. 57–64, 2003.

[9] 岩本貢, 山本博資: 一般アクセス構造に対する強い秘密保護特性を持つランプ型秘密分散法, 第 27 回情報理論とその応用シンポジウム (SITA2004) 予稿集, pp. 331-334, 2004.

[10] 野沢太三: 法務省令第 66 号 戸籍法施行規則の一部を改正する省令, 官報, 平成 16 年号外第 213 号, pp. 1–5, 2004.

[11] 丹羽基二編: 日本苗字大辞典, 芳文館, 1996.

[12] 本村憲史, 橋本誠志, 井上明, 金田重郎: ネットワーク上での情報統合に対するプライバシー保護, 情処論, Vol. 41, No. 11, pp. 2985–3000, 2000.

[13] 野呂正行他: Risa/Asir, http://www.math.kobe-u.ac.jp/Asir

[14] 野呂正行: Risa/Asir, 数式処理 J.JSSAC, Vol. 9, No. 1, pp. 3–10, 2002.

(注3): なお，本稿に示した以外の方法で，閾値未満の分散情報から秘密情報が推定できる可能性が現時点では否定できない．機会をあらためて検討したい．