Vol.2019-DPS-178 No.35
Vol.2019-CSEC-84 No.35
2019/3/5

ランプ型秘密分散法のシェアサイズ変換方式

醍醐康夫† 柴山綸太郎† 土井洋†

概要：(k,n)しきい値秘密分散法のうち，(k,L,n)ランプ型秘密分散法ではパラメーターLによってシェアのデータサイズと安全性を調整することができる．この特性を利用すると，シェアサイズを小さくするようなLを使用することによってディスク容量を削減する，という運用もできる．本論文では，(k,L,n)ランプ型秘密分散法のシェアと，$l<L$となる(k,l,n)ランプ型秘密分散法のシェアを相互変換する方式を提案する．提案方式は，秘密情報を秘密分散法で分散して保管しておき，利用者が自身の端末で一時的に復元して利用するという用途を前提としており，簡易な処理でシェアの変換を行うものである．

キーワード：秘密分散法，Shamir の(k,n)しきい値秘密分散法，(k,L,n)ランプ型秘密分散法

How to Convert the Share Size of Ramp Secret Sharing Schemes

YASUO DAIGO† RINTARO SHIBAYAMA† HIROSHI DOI†

Abstract: Using (k,L,n) ramp secret sharing schemes, it can be controlled size and security of shares by parameter L. By using this property, for example, disk space can be saved by using L which decreases share size. In this paper, we propose a scheme which converts shares of (k,L,n) ramp secret sharing scheme to shares of (k,l,n) ramp secret sharing scheme. Although this scheme is designed for the situation that the confidential information is distributed by secret sharing scheme, and the users reconstruct it temporarily before using information, the process of converting the share is simple.

Keywords: Secret sharing scheme, Shamir's (k,n) threshold scheme, (k,L,n) Ramp secret sharing schemes

1. はじめに

企業や組織における個人情報の漏えい，紛失事故が後を絶たない．発生原因としては情報の管理ミス，誤操作，紛失・置き忘れなどの人為的ミスが多い[1]．事故が発生した場合，社会的，経済的に多大な影響が発生する可能性があるため，効果的な対策を講じる必要がある．ただし，人為的ミスを完全に防ぐことは困難であるため，発生した場合の影響を最小限に抑えることが重要である．この対策に有効な技術の 1 つとして秘密分散法がある．

1.1 秘密分散法

秘密分散法のうち，(k,n)しきい値秘密分散法を用いる場合，秘密情報の保有者（以下，ディーラー）が秘密情報からn個の断片（以下，シェア）を生成し，保管者（以下，参加者）に配布する．そして，利用者（以下，ユーザー）がしきい値であるk個以上のシェアを参加者から集めることで秘密情報を復元できる．

(k,n)しきい値秘密分散法には特性の異なる複数の方式が存在する．このうち Shamir の(k,n)しきい値秘密分散法[2]（以下，Shamir 方式）はシェアのデータサイズが秘密情報と等しくなる．ランプ型秘密分散法[3][4][5]（以下，ランプ型方式）には，Lというパラメーターが追加されており，シェアのデータサイズが秘密情報の$1/L$となる．以後，これらのパラメーターを示すために(k,L,n)という表記をする．なお，Shamir 方式は$(k,1,n)$ランプ型方式である．

Shamir 方式は情報理論的に安全であり，無限の計算リソースを用いても，k個未満のシェアからは秘密情報の部分的な情報を全く得ることができない．一方，ランプ型方式は$k-L$個以下のシェアからは部分的な情報を全く得ることができないが，$k-t$個$(1\leq t<L)$のシェアからは段階的に情報が得られる．このように，Shamir 方式とランプ型方式のシェアはシェアサイズと安全性においてトレードオフの関係にある．

なお，文献[6]によると，秘密分散法で分散したシェアの利用用途として，ユーザーが自身の端末で一時的に復元して利用することと，参加者がマルチパーティー計算を行うことが考えられる．

1.2 シェアの変換

$l<L$かつlはLの約数とする．本論文では，(k,L,n)ランプ型のシェアを作成した後，秘密を復元することなく

1. (k,L,n)ランプ型のシェアから (k,l,n)ランプ型のシェアに変換する方式，および
2. 上記 1 で変換した(k,l,n)ランプ型のシェアを(k,L,n)ランプ型のシェアに変換する方法

† 情報セキュリティ大学院大学
Institute of Information Security

Vol.2019-DPS-178 No.35
Vol.2019-CSEC-84 No.35
2019/3/5

を提案する．ランプ型方式ではLによってシェアのデータサイズと安全性を調整することができるが，提案法を用いることで随時変換できることになる．

Barwick ら[7]は Shamir 方式のシェアにおけるパラメーターkとnを変換する方式を提案している．つまり(k,n)から(k',n')への変換に相当する．

菊池ら[8][9]はランプ型のシェアと Shamir 方式のシェアを相互に変換する方式を提案している．Shamir 方式のシェアは$(k,1,n)$であるため，(k,L,n)と$(k,1,n)$の変換に相当し，後者のシェアを利用してマルチパーティー計算を行うことを想定している．

本論文では，秘密分散法で分散したシェアを「ユーザーが自身の端末で一時的に復元して利用する」という用途に限定し，安全かつ低コストなシェア変換方式を提案する．この際，変換したシェアが[3][4][5]などの(k,l,n)ランプ型のシェアの構成と異なることを許容する．

例 1

$(8,6,n)$ランプ型のシェアを，$(8,3,n)$ランプ型のシェアに変換する場合の変換前後のシェアの様子を図 1 に示す．変換することによってシェアサイズは 2 倍になってしまう．

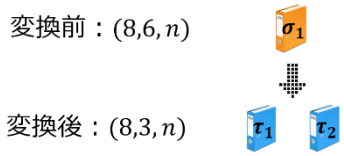

図 1　シェアサイズの比較

しかしながら，変換することによって安全性は向上する．ランプ型方式は$k-t$個$(1 \le t < L)$のシェアからは段階的に情報が得られるという特性があるため，$(8,6,n)$では 3 個以上のシェアから漏洩するのに対して，$(8,3,n)$では 6 個以上のシェアから漏洩するようになる．つまり，何らかの情報を得ることができるシェアの最小数が増えるため，安全性が向上することになる．図 1 に示した例にもとづき，シェアのデータサイズと安全性について表 1 にまとめる．

表 1　シェアのデータサイズと安全性の比較

	データサイズ	安全性
$(8,6,n)$	秘密情報のサイズの 1/6	3 個以上で漏洩
$(8,3,n)$	秘密情報のサイズの 1/3	6 個以上で漏洩

2. 先行研究

提案方式に関連する Shamir 方式，ランプ型方式，および菊池らのシェア変換方式について述べる．

2.1 Shamir 方式

Shamir 方式[2]は，ディーラーが秘密情報をn個のシェアに分散し，そのうち，しきい値であるk個を集めることで秘密情報を復元できるという特性を持つ．シェア生成には，シェア生成用多項式

$$f(x) = s + f_1 x + \cdots + f_{k-1} x^{k-1} \bmod p$$

を用いる．ここでsは秘密情報，pは素数であり，参加者iのシェアは$f(i) \bmod p$となる．

シェアサイズは秘密情報と同一になるため，n人の参加者がいる場合，シェアサイズの合計はn倍になる．例えば 1GB の秘密情報を$(k,8)$しきい値法で 8 個のシェアに分散した場合，合計で 8GB になる．

Shamir 方式は情報理論的に安全であり，無限の計算リソースを用いても，しきい値未満のシェアからは秘密情報の部分的な情報を全く得ることができない．また，$n-k$個未満のシェアを紛失したり破損したりしても残りのシェアから秘密情報を復元できる．

2.2 ランプ型方式

ランプ型方式とは，Blakley ら[3]と山本[4]がそれぞれ独立して発表した情報の分散手法である．Shamir 方式においてシェアのサイズが大きくなってしまうという課題に対する解決策として考案された．

ランプ型方式は，Shamir 方式と同様にn個のシェアのうち任意のk個を集めれば秘密情報を得ることができるが，Lというパラメーターが追加されている．そして，$k-L$個以下のシェアからは部分的な情報を全く得ることができないが，$k-t$個$(1 \le t < L)$のシェアからは段階的に情報が得られる．また，シェアサイズが秘密情報の$1/L$となる．すなわち安全性は低下するがシェアサイズは削減される．例えば 1GB の秘密情報を$(k,4,8)$ランプ型で 8 個のシェアに分散した場合，合計で 2GB になる．なお，Lが 1 のものは Shamir 方式と同じ特性を持つ．

ランプ型方式には弱いランプ型方式（以下，弱い方式）と強いランプ型方式（以下，強い方式）が存在する．秘密情報の組を$s^L = (s_0, \ldots, s_{L-1})$，$n$個のシェアを$\sigma_1, \ldots, \sigma_n$とすると，次の 2 つの条件をすべて満たす方式が強い方式，条件 1 のみを満たす方式が弱い方式となる[4][10]．

条件 1

$0 \le t \le L$のtに対して，任意の$k-t$個のシェア$\sigma_1, \ldots, \sigma_{k-t}$が次の式を満たす．

$$H(s^L | \sigma_1, \ldots, \sigma_{k-t}) = \frac{t}{L} H(s^L)$$

Vol.2019-DPS-178 No.35
Vol.2019-CSEC-84 No.35
2019/3/5

条件 2

$1 \le t \le L$のtに対して，任意の$k-t$個のシェア$\sigma_1, \ldots, \sigma_{k-t}$と$s^L = (s_0, \ldots, s_{L-1})$の任意の$t$個の組$(s_{u1}, \ldots, s_{ut})$が次の式を満たす．

$$H(s_{u1}, \ldots, s_{ut} | \sigma_1, \ldots, \sigma_{k-t}) = \frac{t}{L} H(s^L)$$

本論文では弱い方式を扱うが，弱い方式のシェア生成にはShamir方式と異なるシェア生成用多項式[11]

$g(x) = s_0 + \cdots + s_{L-1}x^{L-1} + g_L x^L + \cdots + g_{k-1}x^{k-1} \bmod p$

を用いる．ここで$s^L = (s_0, \ldots, s_{L-1})$は秘密情報，$p$は素数であり，参加者$i$のシェアは$g(i) \bmod p$となる．

2.3 菊池らのシェア変換方式

菊池らのシェア変換方式[8][9]を用いると，ランプ型のシェアとShamir方式のシェアを相互に変換できる．実際，参加者間でマルチパーティープロトコルを実行し，(k, L, n)ランプ型のシェアと，マルチパーティー計算で扱いやすいShamir方式のシェアとの変換を達成している．すなわち，(k, L, n)ランプ型と$(k, 1, n)$ランプ型の相互変換を実現していることになる．

3. モデル

提案方式においては，ディーラー，参加者，ユーザーの他に，シェアを変換するための変換情報の生成者（以下，コンバーター）というエンティティが存在するモデルを考える．

ディーラーは秘密情報を扱うため，秘密情報の分散時以外は処理を行わない．そこで，変換時には，秘密情報を扱わずに変換情報を生成するだけの役割を持つコンバーターを設ける．

このモデルにおけるシェア変換時の様子を図 2 に示す．ディーラーはあらかじめ参加者iに(k, L, n)ランプ型のシェアσ_iを分散している．シェア変換時，コンバーターは参加者iに変換情報u_iを分散する．この後，参加者は変換情報u_iと保管しているシェアσ_iを用いて(k, l, n)ランプ型のシェアτ_iに変換する．変換した(k, l, n)ランプ型のシェアτ_iは[3][4][5]などの(k, l, n)ランプ型のシェアの構成と異なることを許容する．

安全性については，シェア変換時の変換情報とシェアの漏えいなどの意図的な流出について考える．参加者が複数のシェア（例えば，図 1 のように 2 個）を保有する場合，これらが攻撃者にすべて知られる場合について考える．逆に，部分的に（例えば，2 個のうちの 1 個のみが）攻撃者に知られる場合は対象外とする．

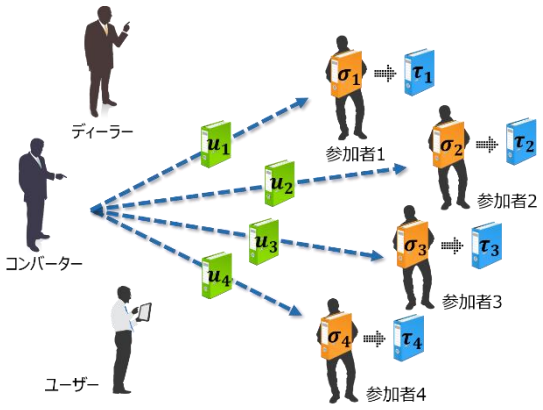

図 2　シェア変換時の様子

仮定 1

エンティティの振る舞いや，それらの間の通信路に関して次のような仮定を置く．同様の仮定は文献[12]でも用いられている．

1. ディーラー，コンバーター，参加者やユーザーの間に安全な通信路が存在する．
2. 参加者は変換後に，変換情報と変換前のシェアを破棄する．

ただし，参加者の一部が攻撃を行う場合は，後者の仮定を設けない．すなわち，不正な参加者iは変換情報u_iや変換前のシェアσ_iを保存することも想定する．

3.1 用語と記号

秘密情報は個人情報や機密情報などの秘匿すべき情報であり，シェアは秘密分散法によって秘密情報を分散した断片である．また，変換情報はシェアを変換するための情報である．

ディーラーは秘密情報の保有者であり，それを分散する．参加者はディーラーが分散したシェアを保管する．ユーザーは秘密情報の利用者であり，復元するために参加者からシェアを収集する．コンバーターは変換情報の生成者であり，それを分散する．

本論文で用いるランプ型のシェア生成においてはシェア生成用多項式を用いる．pを素数とし，特に断らない限りシェア生成用多項式を用いた演算やシェアの四則演算は$\mathbb{Z}_p$上で行う．

本論文では，$L = l \cdot d \ (l < L)$として(k, L, n)ランプ型方式と(k, l, n)ランプ型方式について議論する．このため，(k, L, n)ランプ型のシェアから(k, l, n)ランプ型のシェアに変換した場合，変換後のシェアサイズはd倍となる．

参加者には1からnまでの識別子が付与されている．シェア復元などで参加者を指定する場合は，識別子を定める関数iを用い$i(j)$などと表記する．

(k, L, n)ランプ型のシェア生成用多項式を$g(x)$，シェアを

Vol.2019-DPS-178 No.35
Vol.2019-CSEC-84 No.35
2019/3/5

$\sigma(i(j))$と表記する $(1 \le j \le n)$. 変換後の (k,l,n)ランプ型のシェア生成用多項式を$h_i(x)$，シェアを$\tau(i(j))$と表記する $(1 \le j \le n)$. 更に，(k,l,n)ランプ型から(k,L,n)ランプ型へ変換したシェアを$\bar{\sigma}(i(j))$と表記する $(1 \le j \le n)$.

なお， (k,L,n)ランプ型と(k,l,n)ランプ型との変換においては変換情報生成用多項式を用いるが，(k,L,n)ランプ型から(k,l,n)ランプ型への変換では$u_i(x)$と表記し，(k,l,n)ランプ型から(k,L,n)ランプ型への変換では$v(x)$と表記する．変換情報は各々$u_i(i(j))$や$v(i(j))$となる $(1 \le j \le n)$.

秘密情報はs_iと表記する $(0 \le i < L)$.

3.2 安全性

本モデルにおいては，ディーラーやコンバーターは不正を行わないものと仮定する．その上で安全性の考え方についてインフォーマルに述べる．

(k,L,n)ランプ型のシェア$\sigma(i)$については，任意のk個のシェア$\{\sigma(i(1)),..,\sigma(i(k))\}$から秘密$s^L = (s_0,\dots,s_{L-1})$を復元できることに加え，条件 1 を満たすことが求められる．

変換後の(k,l,n)ランプ型のシェア$\tau(i)$については，任意の k 個のシェア $\{\tau(i(1)),..,\tau(i(k))\}$ から秘密 $s^L = (s_0,\dots,s_{L-1})$を復元できることに加え，$0 \le t \le l$の$t$に対して条件 1 を満たすことが求められる．

変換時に参加者が結託する場合については，以下のように考える．$1 \le t < L$として，参加者$\{i(1),..,i(k-t)\}$が結託する場合を考える．その際，参加者$i(j)$は変換前後のシェア$\sigma(i(j)),\tau(i(j)),\bar{\sigma}(i(j))$に加え，変換情報$u(i(j)),v(i(j))$も利用できる．$(k,L,n)$ランプ型のシェアと$(k,l,n)$ランプ型のシェアの相互変換については，安全性の低い(k,L,n)ランプ型のシェアよりも安全性が低下しないことを定義とする．例えば，(k,L,n)ランプ型のシェアから(k,l,n)ランプ型のシェアへ変換する場合，条件 1 において，

$$H\left(s^L \middle| \{\sigma(i(j)),\tau(i(j)),u(i(j))\}_{1\le j\le k-t}\right) = \frac{t}{L}H(s^L)$$

が成り立つことが求められる．

4. 提案方式

本論文では，$L = l \cdot d$のとき，(k,L,n)ランプ型のシェアを，秘密情報を復元することなく，(k,l,n)ランプ型のシェアに変換する方式を提案する．ランプ型方式ではLによってシェアのデータサイズと安全性を調整することができるが，提案方式を用いることで随時変換できることになる．

なお，提案方式において使用するランプ型方式は弱い方式とする．

4.1 構成

提案方式は分散，変換，復元から構成される．分散ではディーラーがシェアを生成して参加者に分散する．変換ではコンバーターが変換情報を生成して参加者に分散し，参加者がシェアの変換を行う．復元はユーザーが参加者から任意のk個のシェアを集めて秘密情報を復元する．

4.1.1 分散

文献[11]の(k,L,n)ランプ型と同一である．ディーラーは$k-L$個の乱数g_iを生成し，$s_0,\dots,s_{L-1}$をL個の秘密情報とするシェア生成用多項式

$$g(x) = s_0 + \cdots s_{L-1}x^{L-1} + g_L x^L + \cdots + g_{k-1}x^{k-1}$$

を生成する．ディーラーはn個のシェア$\sigma(i)$を生成して参加者iに分散する．

4.1.2 (k,L,n)ランプ型から(k,l,n)ランプ型への変換

プロアクティブ法[13]の概念を応用し，秘密情報の一部を乱数でマスクする処理を用いて実現する．

まず，コンバーターは 4. 1. 1 節で生成されたシェア生成用多項式に含まれる秘密情報の一部$(s_l,\dots s_{L-1})$をマスクするために$L-l$個の乱数$(r_l,\dots r_{L-1})$を生成する．この乱数r_iから$(0,\dots,r_l,\dots r_{L-1})$を秘密とする$(k,L,n)$ランプ型のシェア生成用多項式$u_1(x)$を生成する．また，乱数$r_i$のうち$l$個ずつ$(r_{(m-1)\cdot l},\dots,r_{(m-1)\cdot l+l-1})$を秘密とする$(k,l,n)$ランプ型のシェア生成用多項式$u_m(x)$を生成する $(2 \le m \le d)$．$u_1(x)$と$u_m(x)$は

$$u_1(x) = r_l x^l + \cdots + r_{L-1}x^{L-1} + u_L x^L + \cdots + u_{k-1}x^{k-1}$$
$$u_m(x) = u_{m,0} + \cdots + u_{m,k-1}x^{k-1} \qquad (2 \le m \le d)$$
$$u_{m,j} = r_{(m-1)\cdot l+j} \qquad (0 \le j < l)$$

となる．次に，コンバーターは参加者i $(1 \le i \le n)$の変換情報$u(i) = (u_1(i),\dots,u_d(i))$を生成し分散する．

参加者iは保管している変換元のシェア$\sigma(i)$に変換情報$u_1(i)$を加えて

$$\tau_1(i) = \sigma(i) + u_1(i)$$

とする．ここでシェア生成用多項式の係数が変更されるため，秘密情報の一部をマスクすることができる．また，$\tau_m(i) = u_m(i)$ $(2 \le m \le d)$とし，変換後のシェア$\tau(i) = (\tau_1(i),\dots,\tau_d(i))$を得る．

最後に，参加者i $(1 \le i \le n)$はシェア$\sigma(i)$を破棄し，コンバーターは変換情報生成用多項式や変換情報$u(i)$を破棄する．

例 2

シェアサイズの小さい$(8,6,n)$ランプ型のシェアから安全性の高い$(8,3,n)$ランプ型のシェアへ変換する様子を図 3 に示す．各ブロックは各情報の生成用多項式における係数を表している．①は参加者が保管している変換前の$(8,6,n)$

Vol.2019-DPS-178 No.35
Vol.2019-CSEC-84 No.35
2019/3/5

ランプ型のシェア，②は変換情報，③は変換後の$(8,3,n)$ランプ型のシェアである．

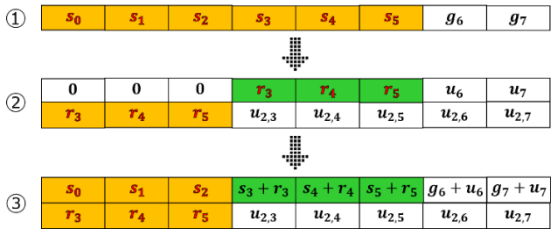

図 3　$(8,6,n)$から$(8,3,n)$への変換

4.1.3 (k,l,n)ランプ型から(k,L,n)ランプ型への変換

$\tau_1(x)$の秘密情報の一部をマスクしている乱数$(r_l,\dots r_{L-1})$を外すことで実現する．

コンバーターは，乱数$(r_l,\dots r_{L-1})$を復元するために必要なシェアの一部$(\tau_2(i(j)),\dots,\tau_d(i(j)))$を任意の$k$個集める．次に多項式補間手法を用いて，集めたシェアから$L-l$個の乱数$(r_l,\dots r_{L-1})$を得る．次に，この乱数r_iから$(0,\dots,r_l,\dots r_{L-1})$を秘密とする$(k,L,n)$ランプ型のシェア生成用多項式

$$v(x)=r_l x^l+\cdots+r_{L-1}x^{L-1}+v_L x^L+\cdots+v_{k-1}x^{k-1}$$

を生成する．次に，コンバーターは参加者$i\ (1\le i<n)$の変換情報$v(i)$を生成し分散する．

参加者iは保管しているシェアの一部$\tau_1(i)$と変換情報$v(i)$から

$$\bar{\sigma}(i)=\tau_1(i)-v(i)$$

を計算し，変換後のシェアを得る．ここでシェア生成用多項式の係数のうち，乱数$(r_l,\dots r_{L-1})$でマスクされていた部分のマスクが外れるため，$s_0,\dots,s_{L-1}$をL個の秘密情報とする(k,L,n)ランプ型のシェアになる．

最後に，参加者$i\ (1\le i\le n)$はシェア$\tau_m(i)\ (1\le m\le d)$を破棄し，コンバーターは変換情報生成用多項式や変換情報$v(i)$を破棄する．

例 3

安全性の高い$(8,3,n)$ランプ型のシェアからシェアサイズの小さい$(8,6,n)$ランプ型のシェアへ変換する様子を図 4 に示す．各ブロックは各情報の生成用多項式における係数を表している．①は参加者が保管している変換前の$(8,3,n)$ランプ型のシェア，②は変換情報，③は変換後の$(8,6,n)$ランプ型のシェアである．

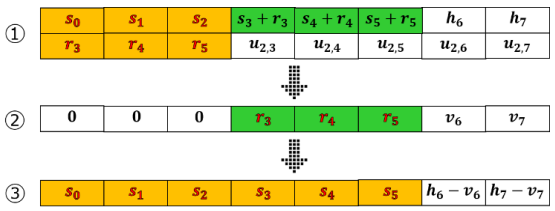

図 4　$(8,3,n)$から$(8,6,n)$への変換

4.1.4 復元

ユーザーは，参加者から秘密情報を復元するために必要な任意のk個のシェアを集め，多項式補間手法を用いて，集めたシェアからシェア生成用多項式の係数を得る．

(k,L,n)ランプ型のシェアである$\sigma(i(j))$や$\bar{\sigma}(i(j))$から計算した場合はL個の秘密情報$s_0,\dots,s_{L-1}$を得ることができる．一方，(k,l,n)ランプ型へ変換されたシェアから計算した場合は，この状態ではまだL個の秘密情報$s_0,\dots,s_{L-1}$が得られていない．しかし，マスク用の乱数$(r_l,\dots r_{L-1})$も復元されるので，L個の秘密情報$s_0,\dots,s_{L-1}$を得ることができる．

5. 安全性

3.2 節で述べた安全性を満たすことを示す．

構成法から(k,L,n)ランプ型のシェア$\sigma(i),\bar{\sigma}(i)$は[3][4][5]などの$(k,L,n)$ランプ型のシェアであるので，3.2 節で述べた安全性を満たす．

変換後の(k,l,n)ランプ型のシェアについては，[3][4][5]などのシェアとは形式が異なる．そこで，定理 1 で復元性を，定理 2 および定理 3 で段階的に秘密情報が得られることを示す．

変換時に参加者が結託する場合については，定理 4 および定理 5 で示す．これは例えば，$(8,6,n)$ランプ型のシェアから$(8,3,n)$ランプ型のシェアへの変換の場合，シェアを持ち寄ったとしても，安全性の低い$(8,6,n)$ランプ型よりも安全性が低下しない，ということである．

これらの定理を証明するための性質として，2 つの補題を整理する．

補題 1

$k-1$次の多項式

$$g(x)=g_0+\cdots+g_{k-1}x^{k-1}\ mod\ p$$

について，$b(<k)$個の$\sigma(i(j))=g(i(j))(1\le j\le b)$が与えられたとき，多項式の$k-b$個の係数$g_i\in\mathbb{Z}_p\ (0\le i<k-b)$を任意に定める．このとき，与えられた

$$\sigma(i(j))=g(i(j))\qquad(1\le j\le b)\qquad(1)$$

を満たす係数$g_i\ (k-b\le i<k)$が一意に定まる．

証明

付録 A.1 を参照のこと．

補題 2

$L=l\cdot d, k-L<b<k$とする．シェア生成用多項式

$$h_m(x)=h_{m,0}+\cdots+h_{m,k-1}x^{k-1}\ mod\ p\ \ (1\le m\le d)$$

を

Vol.2019-DPS-178 No.35
Vol.2019-CSEC-84 No.35
2019/3/5

$$h_1(x) = s_0 + \cdots + s_{l-1}x^{l-1} + (s_l + r_l)x^l + \cdots + (s_{L-1} + r_{L-1})x^{L-1} + h_{1,L}x^L + \cdots + h_{1,k-1}x^{k-1} \quad (2)$$

$$h_m(x) = r_{(m-1)\cdot l} + \cdots + r_{(m-1)\cdot l+l-1}x^{l-1} + h_{m,l}x^l + \cdots + h_{m,k-1}x^{k-1} \quad (2 \le m \le d) \quad (3)$$

とする．また，$i(1), \dots, i(b) \in \{1, \dots, n\}$に対し$b \cdot d$個のシェア

$$\tau_m\big(i(j)\big) = h_m\big(i(j)\big) \quad (1 \le j \le b, 1 \le m \le d) \quad (4)$$

が与えられたとする．式(2)の$s_{(m-1)\cdot l+i}$ $(0 \le i < k-b, 1 \le m \le d)$を任意に定めたとき，式(4)を満たす多項式$h_m(x)$が一意に定まる．

証明

付録 A. 2 を参照のこと．

(k, L, n)ランプ型から(k, l, n)ランプ型へ変換したシェア$\tau(i)$が(k, l, n)ランプ型の性質を有することを示す. まず, 任意のk個のシェアから，$s^L = (s_0, \dots, s_{L-1})$を計算できることを定理 1 で示す．

定理 1

任意の$i(1), \dots, i(k) \in \{1, \dots, n\}$に対し，変換後のシェア$\tau(i(j))$ $(1 \le j \le k)$から$s^L = (s_0, \dots, s_{L-1})$を計算できる．

証明

$\tau(i(j)) = \{\tau_1\big(i(j)\big), \cdots, \tau_d(i(j))\}$であり，各$\tau_m(x)$ $(1 \le m < d)$は$k-1$次の多項式である．よって$\{\tau_m(i(j))\}_{1 \le j \le k}$から多項式補間手法を用いて多項式$\tau_m(x)$の係数を全て求めることができる．すると，シェアの構成方法から$s^L = (s_0, \dots, s_{L-1})$を計算できる．

次に，$k-t$個$(0 \le t < l)$のシェアから段階的に秘密が漏れることを定理 2 で示す．

定理 2

$0 \le t < l$とする．任意の$k-t$個のシェア$\tau(i(1)), \dots, \tau(i(k-t))$に対して$H\big(s^L \big| \tau(i(1)), \dots, \tau(i(k-t))\big) = \frac{t}{l}H(s^L)$が成り立つ．

証明

$\mathbb{Z}_p$上で考えているので，$\frac{t}{l}H(s^L) = t \cdot d \cdot log\, p$であること，すなわち秘密$s^L$として$p^{t \cdot d}$通りの候補があることを示せばよいが，これは補題 2 より成り立つ．

最後に，$k-l$個のシェアからは秘密が全く漏れないことを定理 3 で示す．この結果，$k-l$個以下のシェアからは秘密が全く漏れないことも従う．

定理 3

任意の$k-l$個のシェア$\tau(i(1)), \dots, \tau(i(k-l))$に対して，$H\big(s^L \big| \tau(i(1)), \dots, \tau(i(k-l))\big) = H(s^L)$が成り立つ．

証明

$\tau\big(i(j)\big)$の第m成分について考える．これは$k-1$次多項式$h_m(x)$を用いて$\tau_m\big(i(j)\big) = h_m\big(i(j)\big)$と表せる．$s^L = (s_0, \dots, s_{L-1})$や$(r_l, \dots, r_{L-1})$を用いると，式(2)および式(3)となる．本定理を証明するためには任意の$(s_0, \dots, s_{L-1})$に対して，

$$\tau_m\big(i(j)\big) = h_m\big(i(j)\big) \quad (5)$$

となるような$h_m(x)$が存在することを示せばよい. 補題 1 より，(5)式を満たして$h_{1,i} = s_i$ $(0 \le i < l)$となる多項式$h_1(x)$が存在する．同様に，(5)式を満たして$h_{m,i} = h_{1,(m-1)\cdot l+i} - s_{(m-1)\cdot l+i}$ $(0 \le i < l, 2 \le m \le d)$となる多項式$h_m(x)$も存在する．よって定理は証明できた．

一部の参加者が変換前後のシェアと変換情報を用いて，$s^L = (s_0, \dots, s_{L-1})$に関する情報を得ることができないことを検証する．具体的には，(k, L, n)ランプ型のシェアから(k, l, n)ランプ型のシェアへ変換する場合に$k-t$個$(0 < t \le L)$の変換前後のシェアと変換情報を用いる攻撃者を想定する．ランプ型を用いているので変換前のシェアから秘密は段階的に漏れている （$H(s^L|\sigma_1, \dots, \sigma_{k-t}) = \frac{t}{L}H(s^L)$となる）．

よって変換後のシェアと変換情報を用いてさらに秘密が漏れないことを定理 4 で示す．

定理 4

$0 < t \le L$とする．任意の$k-t$個の変換前のシェア$\sigma(i(1)), \dots, \sigma(i(k-t))$，変換後のシェア$\tau(i(1)), \dots, \tau(i(k-t))$，および変換情報$u(i(1)), \cdots, u(i(k-t))$に対して，

$$H\left(s^L \middle| \begin{matrix} \sigma\big(i(1)\big), \dots, \sigma\big(i(k-t)\big), \tau\big(i(1)\big), \dots, \tau\big(i(k-t)\big), \\ u\big(i(1)\big), \cdots, u(i(k-t)) \end{matrix}\right) = \frac{t}{L}H(s^L)$$

が成り立つ．

証明

変換前のシェア$\sigma(i(1)), \dots, \sigma\big(i(k-t)\big)$はランプ型のシェアであるので，

$$H\left(s^L \middle| \sigma(i(1)), \dots, \sigma\big(i(k-t)\big)\right) = \frac{t}{L}H(s^L)$$

が成り立つ．変換情報および変換後のシェアはコンバーターが生成するが，コンバーターは秘密情報を何も使っていない．したがって，参加者$i(1), \dots, i(k-t) \in \{1, \dots, n\}$もコンバーターと同様の分布で変換情報および変換後のシェアを生成することができる．

Vol.2019-DPS-178 No.35
Vol.2019-CSEC-84 No.35
2019/3/5

参加者が同様の分布で生成した変換情報および変換後のシェア$\tau'(i(j)), u'(i(j))$ $(1 \le j \le k-t)$について，

$$H\left(s^L \middle| \sigma(i(1)), \dots, \sigma(i(k-t))\right)$$
$$= H\left(s^L \middle| \begin{matrix}\sigma(i(1)), \dots, \sigma(i(k-t)), \tau'^{(i(1))}, \dots, \tau'^{(i(k-t))}, \\ u'(i(1)), \cdots, u'(i(k-t))\end{matrix}\right)$$
$$= H\left(s^L \middle| \begin{matrix}\sigma(i(1)), \dots, \sigma(i(k-t)), \tau(i(1)), \dots, \tau(i(k-t)), \\ u(i(1)), \cdots, u(i(k-t))\end{matrix}\right)$$
$$= \frac{t}{L} H(s^L)$$

である．よって，定理が成り立つ．

最後に，(k,l,n)ランプ型のシェアから(k,L,n)ランプ型のシェアへ変換する場合に$k-t$個$(0 < t \le L)$の変換前後のシェアと変換情報を用いる攻撃者について考える．(k,l,n)ランプ型のシェア$\tau(i(1)), \cdots, \tau(i(k-t))$，変換情報$v(i(1)), \cdots, v(i(k-t))$，および変換後の$(k,L,n)$ランプ型のシェア$\bar{\sigma}(i(1)), \cdots, \bar{\sigma}(i(k-t))$を用いてさらに秘密が漏れないことを定理 5 で示す．

定理 5

$0 < t \le L$とする．任意の$k-t$個の(k,l,n)ランプ型のシェア$\tau(i(1)), \dots, \tau(i(k-t))$，変換後のシェア$\bar{\sigma}(i(1)), \dots, \bar{\sigma}(i(k-t))$，および変換情報$v(i(1)), \cdots, v(i(k-t))$に対して，

$$H\left(s^L \middle| \begin{matrix}\tau(i(1)), \dots, \tau(i(k-t)), \bar{\sigma}(i(1)), \dots, \bar{\sigma}(i(k-t)), \\ v(i(1)), \cdots, v(i(k-t))\end{matrix}\right) = \frac{t}{L} H(s^L)$$

が成り立つ．

証明

構成法から，変換後のシェア$\bar{\sigma}(i(1)), \dots, \bar{\sigma}(i(k-t))$は最初に分散された$(k,L,n)$ランプ型のシェア$\sigma(i(1)), \dots, \sigma(i(k-t))$と同様に$(k,L,n)$ランプ型のシェアである（シェア生成用多項式の乱数部分は異なる）．

ここで，参加者$i(1), \dots, i(k-t) \in \{1, \dots, n\}$は$\sigma(i(1)), \dots, \sigma(i(k-t))$から$(k,l,n)$ランプ型のシェアへ変換する$u(i(1)), \cdots, u(i(k-t)))$を生成し，さらに$\tau(i(1)), \dots, \tau(i(k-t))$と$v(i(1)), \cdots, v(i(k-t))$，および$\bar{\sigma}(i(1)), \dots, \bar{\sigma}(i(k-t))$を生成することができる．すると

$$H\left(s^L \middle| \sigma(i(1)), \dots, \sigma(i(k-t))\right)$$
$$= H\left(s^L \middle| \begin{matrix}\tau(i(1)), \dots, \tau(i(k-t)), \bar{\sigma}(i(1)), \dots, \bar{\sigma}(i(k-t)), \\ v(i(1)), \cdots, v(i(k-t))\end{matrix}\right)$$
$$= \frac{t}{L} H(s^L)$$

である．よって定理が成り立つ．

6. 考察

提案方式はコンバーターが存在するモデルであるが，コンバーターは秘密情報を有していない．よって，コンバーターの不正による影響は少ないと考えられる．

なお，(k,l,n)ランプ型への変換においては，[3][4][5]のような通常の(k,l,n)ランプ型のシェアとは構成（シェア生成用多項式）が異なる．シェア生成用多項式のどの部分を乱数でマスクしたかなどの情報，すなわち，L,lについて参加者や利用者などが知る必要がある．

7. おわりに

秘密情報を秘密分散法で分散して保管しておき，利用者が自身の端末で一時的に復元して利用する，という用途を前提として，(k,L,n)ランプ型のシェアと，データサイズと安全性の異なる(k,l,n)ランプ型のシェアを相互変換する方式を提案した．

強い方式への適用や，3 つ以上のLパラメーター変換（例えば，$(8,6,n)$，$(8,3,n)$，$(8,2,n)$ランプ型などの逐次変換）等については，別途報告する予定である．

また，提案方式にはコンバーターが存在するが，マルチパーティープロトコルを使用して変換情報を生成するようにすれば参加者だけで変換が実現できるので，[8][9]などと比較したい．

謝辞　本研究の一部は JSPS 科研費 18K11306 の助成を受けた．

参考文献

[1] 日本ネットワークセキュリティ協会. “2017 年 情報セキュリティインシデントに関する調査報告書【速報版】”, 2018
[2] Adi Shamir. “How to Share a Secret”, Massachusetts Institute of Technology, 1979
[3] G.R. Blakley, C. Meadows. “Security of ramp schemes”, Proc. CRYPTO 1984, by G.R. Blakley, and D. Chaum eds. vol.196, pp.242–268, Lect. Notes Comput. Sci., Springer-Verlag, 1985
[4] 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
[5] ISO/IEC 19592-2:2017 “Information technology - Security techniques - Secret sharing - Part 2: Fundamental mechanisms”, 2017
[6] 千田浩司, 五十嵐大, 濱田浩気, 菊池亮, 冨士仁, 高橋克巳. “マルチパーティ計算に適用可能な計算量的ショート秘密分散”, 第 29 回 暗号と情報セキュリティシンポジウム（SCIS2012）, 2012
[7] S.G. Barwick, W.-A. Jackson, K.M. Martin. “Updating the Parameters of a Threshold Scheme by Minimal Broadcast”, IEEE Transactions on Information Theory, vol.51, Issue 2, February, 2005

[8] Ryo Kikuchi, Dai Ikarashi, Koki Hamada, Koji Chida. “Adaptively and Unconditionally Secure Conversion Protocols between Ramp and Linear Secret Sharing”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, vol.E98-A, No.1, pp.223-231, 2015.
[9] 菊池亮，五十嵐大，濱田浩気，千田浩司. “秘密計算に適した秘密分散とコンパクトな秘密分散との相互変換プロトコル”， 第 31 回 暗号と情報セキュリティシンポジウム（SCIS2014）, 2014
[10] 滝澤克則, 西新幹彦. “多項式補間法による強いランプ型しきい値秘密分散法”, 電子情報通信学会技術研究報告, IEICE technical report 109(143), pp.127-129, 2009-07-16
[11] 栗原淳, 松本隆太郎, 植松友彦. “線形符号の相対パラメータによって表される秘密分散法の安全性”, IEICE Fundamentals Review Vol.9, No.1, 2015
[12] 今田丈雅, 松浦幹太. “ブロックチェーンと秘密分散法を用いた情報ライフサイクル制御”, Computer Security Symposium 2017, October, 2017
[13] Amir Herzberg, Stanislaw Jarecki, Hugo Krawczyk, Moti Yung. “PROACTIVE SECRET SHARING Or: How to Cope With Perpetual Leakage”, IBM T.J. Watson Research Center, October 15, 1998

付録 A

A.1 補題 1 の証明

$b(<k)$ 個の $\sigma(i(j))\ (1 \le j \le b)$ が与えられたとする．$\sigma(i(j))$は式(1)の係数を用いて

$$\begin{pmatrix} 1 & i(1) & \cdots & i(1)^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & i(b) & \cdots & i(b)^{k-1} \end{pmatrix}\begin{pmatrix} g_0 \\ \vdots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} \sigma(i(1)) \\ \vdots \\ \sigma(i(b)) \end{pmatrix} \quad \text{(A1)}$$

と表せる．このとき，$g_0, \dots, g_{k-b-1} \in \mathbb{Z}_p$を任意に定めたとする．(A1)式を変形すると

$$\begin{pmatrix} 1 & i(1) & \cdots & i(1)^{k-b-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & i(b) & \cdots & i(b)^{k-b-1} \end{pmatrix}\begin{pmatrix} g_0 \\ \vdots \\ g_{k-b-1} \end{pmatrix} + \begin{pmatrix} i(1)^{k-b} & \cdots & i(1)^{k-1} \\ \vdots & \ddots & \vdots \\ i(b)^{k-b} & \cdots & i(b)^{k-1} \end{pmatrix}\begin{pmatrix} g_{k-b} \\ \vdots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} \sigma(i(1)) \\ \vdots \\ \sigma(i(b)) \end{pmatrix}$$

となる．ここで

$$\begin{pmatrix} \Delta_1 \\ \vdots \\ \Delta_b \end{pmatrix} = \begin{pmatrix} 1 & i(1) & \cdots & i(1)^{k-b-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & i(b) & \cdots & i(b)^{k-b-1} \end{pmatrix}\begin{pmatrix} g_0 \\ \vdots \\ g_{k-b-1} \end{pmatrix}$$

と置くと

$$\begin{pmatrix} i(1)^{k-b} & \cdots & i(1)^{k-1} \\ \vdots & \ddots & \vdots \\ i(b)^{k-b} & \cdots & i(b)^{k-1} \end{pmatrix}\begin{pmatrix} g_{k-b} \\ \vdots \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} \sigma(i(1)) - \Delta_1 \\ \vdots \\ \sigma(i(b)) - \Delta_b \end{pmatrix} \quad \text{(A2)}$$

となり，左辺の$k_0 \times k_0$行列は

$$\begin{pmatrix} i(1)^{k-b} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & i(b)^{k-b} \end{pmatrix}\begin{pmatrix} 1 & i(1) & \cdots & i(1)^{b-1} \\ 1 & \vdots & \ddots & \vdots \\ 1 & i(b) & \cdots & i(b)^{b-1} \end{pmatrix}$$

と対角行列とヴァンデルモンド行列の積の形に変形でき，この行列は逆行列を持つ．式(A1)を満たす係数$g_i(k-b \le i < k)$が一意に定まる．よって補題が成り立つ．

A.2 補題 2 の証明

式(2)の$k-1$次のシェア生成用多項式についてb個のシェア $h_1(i(j))\ (1 \le j \le b)$が与えられたとき，秘密$s_i \in \mathbb{Z}_p$ $(0 \le i < k-b)$を任意に定める．このとき，補題 1 より係数$h_{1,j}\ (k-b \le j < k)$が

$$h_1(x) = s_0 + \cdots + s_{k-b-1}x^{k-b-1} + h_{1,k-b}x^{k-b} + \cdots + h_{1,k-1}x^{k-1} \quad \text{(A3)}$$

のように一意に定まる．一方，式(3)において乱数 $r_{(m-1)\cdot l+i} \in \mathbb{Z}_p\ (0 \le i < k-b, 2 \le m \le d)$を任意に定める．このとき，補題 1 より式(3)を満たす係数$h_{m,j}(k-b \le j < k, 2 \le m \le d)$が

$$h_m(x) = r_{(m-1)\cdot l} + \cdots + r_{(m-1)\cdot l+k-b-1}x^{k-b-1} + h_{m,k-b}x^{k-b} + \cdots + h_{m,k-1}x^{k-1} \quad \text{(A4)}$$

のように一意に定まる．ここで，式(A4)において $r_{(m-1)\cdot l+i}\ (0 \le i < k-b, 2 \le m \le d)$は任意の値であるため，式(A3)で定めたい任意の$s_{(m-1)\cdot l+i}\ (0 \le i < k-b, 2 \le m \le d)$について$r_{(m-1)\cdot l+i} = h_{1,(m-1)\cdot l+i} - s_{(m-1)\cdot l+i}$とすることができる．

よって，$s_{(m-1)\cdot l+i}\ (0 \le i < k-b, 1 \le m \le d)$を任意に定めたとき，式(4)を満たす係数$h_{m,i}(k-b \le i < k, 1 \le m \le d)$が一意に定まる．