日本応用数理学会論文誌
Vol. 16, No. 1, 2006, pp. 15～25

頑強性を有する暗号の秘密分散法への応用

江村 恵太 *　野村 明人 **

*(株) 富士通北陸システムズ　**金沢大学自然科学研究科

Some applications of non-malleable cryptography to secret sharing scheme

Keita EMURA *　Akito NOMURA **

*Fujitsu Hokuriku Systems Limited

**Graduate School of Natural Science and Technology, Kanazawa University

Abstract. Multi-secret sharing scheme (multi-SSS) is the method of distributing arbitrary numbers of secret information. Moreover, as a way anyone can check that secret information has been distributed correctly, M.Stadler defined publicly verifiable secret sharing scheme (PVSS). However the security of the method of Stadler is computationally. In this paper, we proposed that multi-SSS and PVSS using unconditionally secure asymmetric encryption (USAE) which is non-malleable cryptography. By using two methods together, it is possible to check that secret information has been correctly distributed to two or more secret information, without needing computational assumption.

1　はじめに

秘密情報をどのように保存，管理するかということは重要な問題である．紛失防止のためコピーを取ると秘密情報が漏洩する危険が増す．コピーした秘密情報ごとに暗号化を行うと，暗号化鍵の管理が大変である．

秘密分散法 (secret sharing scheme : SSS) は，情報の分散 (コピー) と暗号化を同時に行う技術である．また特定のユーザが揃わなければ，秘密情報に関して何の情報も得ることができないという優れた特性を持つ．秘密分散法の重要な問題の一つとして，秘密情報が正しく分散されたことを確認することがあげられる．これを実現する方法としては，Feldman[3] の検証可能秘密分散法 (verifiable secret sharing scheme : VSS) や Stadler[7] の公開検証可能秘密分散法 (publicly verifiable secret sharing scheme : PVSS) がある．しかし，これらの方法は離散対数問題の困難さを利用しているため，安全性は計算量的である．また，通常の秘密分散法では，権限を有するユーザが揃った場合に復元される秘密情

報は常に同じであるが，復元する秘密情報をユーザの集合ごとに決定したいような場合など，複数個の秘密情報を管理する状況が考えられる．このような状況に対応するのが複数秘密分散法 (multi-secret sharing scheme : multi-SSS) [2] である．

本論文では，頑強性をもつ暗号 (non-malleable cryptography) である情報理論的に安全な非対称暗号 (unconditionally secure asymmetric encryption : USAE) を利用した multi-SSS と PVSS を提案する．2つの方法を併用することにより，計算量的仮定を必要とせずに，複数の秘密情報に対して秘密情報が正しく分散されたことを確認することが可能である．

まず2章と3章で種々の秘密分散法について説明し，4章で暗号の頑強性について述べる．5章で USAE について述べた後，6章で提案方式を説明し，7章で今後の課題について述べる．

2 Shamirのしきい値法

本章では，SSS としてよく知られている Shamir の (k,n) しきい値法の概要を述べる．$\mathcal{P}=\{U_1,U_2,\ldots,U_n\}$ をユーザの集合，K を分散する秘密の値，w_i を U_i に与えられる分散情報とする．さらに，k を 2 以上 n 以下の自然数とする．

(k,n) しきい値法とは，分散情報 $w_i(i=1,2,\ldots,n)$ のうち，任意の k 個を集めれば K を完全に復元できるが，$k-1$ 個では K に関して全く情報が得られないような分散方法をいう．

ここで秘密情報 K を復元できる $\mathcal{P}$ の部分集合 A_j をアクセス集合，すべてのアクセス集合からなる族 $\Gamma=\{A_1,A_2,\ldots,A_m\}$ をアクセス構造と定義する．また権限のない $\mathcal{P}$ の部分集合に対しては K について何の情報も得ることができないとき，完全な秘密分散共有法 (perfect secret sharing scheme) という．完全な秘密分散法は以下のように定義される．

定義1：完全な秘密分散共有法

権限を持たないユーザの集合 $X\notin\Gamma$ が揃っていても，任意の $K\in\boldsymbol{F}_p$ に対し，それが秘密情報である確率は $1/p$ である．

Shamir の (k,n) しきい値法

p を n と K より大きい素数とし，演算はすべて有限体 $\boldsymbol{F}_p$ 上で行う．

1. $a_i\in\boldsymbol{F}_p$ $(i=1,2,\ldots,k-2)$, $a_{k-1}\in\boldsymbol{F}_p^*$ をランダムに選び，$k-1$ 次多項式 $f(x)=K+\sum_{i=1}^{k-1}a_ix^i$ をつくる．
2. ユーザ U_i $(i=1,2,\ldots,n)$ に分散情報として $w_i=(i,f(i))$ を与える．
3. f は $k-1$ 次多項式なので，k 個以上の w_i $(i=1,2,\ldots,n)$ がわかればラグランジュ補間を利用して f が復元でき，従って K を復元することができる．

$k-1$ 次多項式のグラフは，グラフ上の $k-1$ 個の座標がわかっても，残り1つの座標がわからないと元の多項式は確定しない．よって $k-1$ 人以下のユーザが揃っても，K に関する情報を何も得ることはできない．よって (k,n) しきい値法は完全な秘密分散共有法である．

3 検証可能秘密分散法

本章では，VSS と PVSS について簡単に解説する．

まず Feldman[3] による VSS を述べる．Shamir の (k,n) しきい値法における $k-1$ 次多項式を $f(x)=K+\sum_{i=1}^{k-1}a_ix^i$ とする．q を $q-1$ が p の倍数となるような素数とする．このような q は Dirichlet の算術級数定理により存在する．さらに g を $\boldsymbol{F}_q^*$ の元で位数が p のものとする．

Feldman の VSS

1. ディーラーは $g^K, g^{a_1}, \ldots, g^{a_{k-1}}$ を公開する．
2. U_i は自分の分散情報 $(i, f(i))$ より $g^K \prod_{j=1}^{k-1} g^{a_j i^j} \stackrel{?}{\equiv} g^{f(i)} \bmod q$ を検証する．

Feldman の方式のように U_i が一人で自分の分散情報の正当性を検証する VSS を非対話式 (non-interactive) という．Feldmann の方式では，分散情報をそのまま用いて検証しているため，各ユーザは自分の分散情報の正当性しか検証できない．他のユーザの分散情報の正当性も検証できる方法としては，Stadler[7] による公開検証可能秘密分散法 (publicly verifiable secret sharing scheme : PVSS) がある．

PVSS のアイディアは分散情報を暗号化し公開するというものであり，誰でも秘密情報が正しく分散されたことを確認できる．用いた暗号が破られないかぎり，公開暗号文から分散情報はわからない．この公開暗号文に対して検証を行うことにより，他のユーザに対しても分散情報の正当性を検証することができる．PVSS においても対話式 (interactive) と非対話式があり，Stadler[7] ではユーザとディーラーの間で情報のやりとりが必要な方法を対話式，そうでないものを非対話式と定義している．

4 暗号の頑強性

公開鍵暗号系の安全性には，強秘匿性 (semantic secure)，識別不可能性 (indistinguishability)，頑強性 (non-malleability) と呼ばれるものがあり，それぞれ次のように定義される．

定義 2：公開鍵暗号系の安全性

強秘匿性

平文 M に対する暗号文 C を与えられたとき，攻撃者は C の平文である M に関してどんな情報も入手できない．

識別不可能性

平文 M_0 と M_1 とそのどちらかの暗号文 C^* が与えられたとき，攻撃者がどちらの平文に対する暗号文であるか識別できない．

頑強性

平文 M に対する暗号文 $C=E(M)$ と非自明な関数 F が与えられたとき，$F(M)$ に対する暗号文を求めることができない．ここで E は暗号化関数である．

＜頑強性の模式図＞

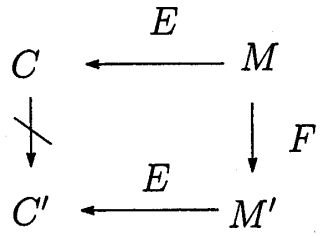

Fig.1 non-malleability

注意 RSA 暗号 [5] は頑強性をみたさない．実際，RSA 暗号の暗号文を $C = M^e \bmod N$ とするとき，$C' = C^2 \bmod N$ を計算すると，C' は M^2 の暗号文である．

公開鍵暗号が強秘匿性をみたす必要十分条件は，識別不可能性をみたすことである．また適応的選択暗号文攻撃 (adaptive chosen ciphertext attack) のもと，公開鍵暗号が頑強性をみたすことと識別不可能性をみたすことは等価であることが示されている [1]．ここで適応的選択暗号文攻撃とは，攻撃者が自由に暗号文を生成し，それに対応する平文を得ることができるという状況での攻撃をいう．

5 情報理論的に安全な非対称暗号

本章では，情報理論的に安全な非対称暗号 (unconditionally secure asymmetric encryption : USAE) [4] について述べる．非対称暗号と公開鍵暗号は暗号化鍵と秘密鍵が異なるという点では同じであるが，非対称暗号は暗号化鍵を公開しないという点で異なる．

次のモデルを考える．

モデル

1. 参加者は n 人の送信者 $\{S_1, S_2, \ldots, S_n\}$，受信者 R，TI (Trustd Initializer) の $n+2$ 人である．
2. 送信者のうちの任意の一人が受信者に暗号化したメッセージを送る．
3. 鍵の生成および配布は TI が行う．
4. 送信者以外のユーザが結託しても、結託人数が $k-1$ 人以下ならば暗号化したメッセージから元のメッセージに関する情報は何も得ることはできない．

多項式を利用した USAE [4]

p を n より大きな素数とする．

1, セットアップ

1. TI は有限体 $\boldsymbol{F}_p$ の元を係数とする 0 でない $k-1$ 次多項式 $f_1(x)$, $f_2(x)$ をランダムに選ぶ．
2. TI は $\boldsymbol{F}_p$ の元 b で $f_2(b) \neq 0$ を満たすものを n 個選び，それらを $b_1, b_2, \ldots, b_n$ とする．さらに，$B = \{b_1, b_2, \ldots, b_n\}$ を参加者に公開する．
3. TI は $f_1(x)$ と $f_2(x)$ を R に復号化鍵として，また $\{b_i, f_1(b_i), f_2(b_i)\}$ を S_i $(i = 1, 2, \ldots, n)$ に暗号化鍵として与える．

2, 暗号化と送信

送信者 S_i は，メッセージ $M(\in \boldsymbol{F}_p)$ から $C' = f_1(b_i)+M\cdot f_2(b_i)$ を計算し，$C = \{b_i, C'\}$ を R に送る．

3, 復号化

受信者 R は $f_1(x)$, $f_2(x)$ と C を用いて $M = (C' - f_1(b_i))/f_2(b_i)$ と復号化する．

[4] の中で，この方式がモデルを実現し，また頑強性を満たすことが証明されている．

注意 今，メッセージ M_1, $M_2(\in \boldsymbol{F}_p)$ が同じ暗号化鍵 $f_1(b_i)$, $f_2(b_i)$ で暗号化されているとし，それぞれの暗号文を C_1, C_2 とする．このとき (M_1, C_1), (M_2, C_2) から暗号化鍵 $f_1(b_i)$, $f_2(b_i)$ が計算できてしまう．この適応的選択暗号文攻撃を避けるためには，[4] にもあるように使い捨て (one-time) 方式で行う必要がある．

6 提案方式

ここではUSAEを利用した複数秘密分散法 (multi-SSS) と公開検証可秘密分散法 (PVSS) を提案する．通常の秘密分散法では，k 人集まった場合に復元できる秘密情報は1つであるが，復元できる秘密情報を複数個に拡張する (提案方式1)．また提案方式1ではしきい値アクセス構造モデルを考えたが，一般アクセス構造を実現できるように拡張する (提案方式2)．また提案方式2では公開情報を制限することにより，復元できる秘密情報にも制限を加えることができる．すなわち復元する秘密情報をユーザの集合ごとに決定したいような場合に有効である．また提案方式 1 および提案方式 2 に応用可能な完全な PVSS を提案する (提案方式3)．

ユーザの集合を $\mathcal{P} = \{U_1, U_2, \ldots, U_n\}$ とし，ID_i $(i = 1, 2, \ldots, n)$ をユーザ U_i のIDナンバーとする．さらに，信頼できる機関をディーラーとする．

以下では，p を素数とし，計算はすべて有限体 $\boldsymbol{F}_p$ 上で行うものとする．

提案方式 1 : multi-(k,n) threshold scheme using USAE

モデル 1

1. 秘密情報は複数個ある．
2. 分散情報は各ユーザに対して2つである．
3. k を 2 以上 n 以下の自然数とする．ユーザが k 人集まるとどの秘密情報も復元できる．
4. 完全な秘密分散法である．
5. 秘密情報の分散はディーラーが行う．

複数の秘密情報を $(K_1, K_2, \ldots, K_l) \in \boldsymbol{F}_p^l$ とする．このモデルを実現するためのセットアップおよび秘密情報の復元は以下の通り行う．

ディーラーによる分散情報の生成および配布

1. $\boldsymbol{F}_p$ の元を係数とする $k-1$ 次多項式 $f(x)$, $g(x)$ を生成する．ただし，$g(0) \neq 0$ とする．

2. $s_i = f(ID_i)$, $v_i = g(ID_i)$ $(i = 1, 2, \ldots, n)$ を計算し, (s_i, v_i) をユーザ U_i に配布する.

ディーラーによる公開情報の生成および公開

1. K_j $(j = 1, 2, \ldots, l)$ と異なる $K_0 \in \boldsymbol{F}_p^*$ をランダムに選ぶ.
2. $K_j = f(0) + K_j' \cdot g(0)$ をみたす K_j', $(j = 1, 2, \ldots, l)$ を計算する.
3. $d_0 = f(0) + K_0 \cdot g(0)$ を計算する.
4. 写像 $\pi_j : \boldsymbol{F}_p \to \boldsymbol{F}_p$ $(j = 1, 2, \ldots, l)$ で $\pi_j(K_0) = K_j'$ をみたすものを構成する.
5. π_j $(j = 1, 2, \ldots, l)$ と d_0 を公開する.

ユーザ k 人による秘密情報の復元

1. $f(x)$, $g(x)$ 上の点がそれぞれ k 個わかるので, $f(x)$, $g(x)$ が確定し $f(0)$, $g(0)$ が求まる.
2. $f(0)$, $g(0)$ と公開情報 d_0 から K_0 が求まる.
3. K_0 と公開情報 π_j から K_j' が求まる.
4. $f(0)$, $g(0)$, K_j' から K_j が求まる.

＜提案方式 1 の模式図＞

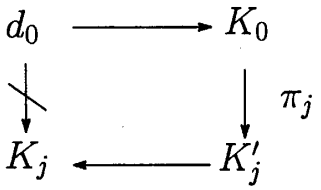

Fig.2 the proposal method 1

定理 6.1 提案方式 1 はモデル 1 を実現している.
(証明)

1. モデルの条件 3 については, 上記「ユーザ k 人による秘密情報の復元」によりわかる. $\mathcal{P}$ のメンバが k 人以上揃わなければ $f(x)$ と $g(x)$ は復元できず, $f(0)$ と $g(0)$ に関する情報は何も得られない. 任意の $f(0)$ と $g(0)$ に対して, K_0 と d_0 は 1 対 1 に対応するので, d_0 から K_0 に関する情報を得ることはできない.
2. $f(0)$, $g(0)$ がわからない状況では, USAE の頑強性より任意の非自明な写像 $\pi_j : \boldsymbol{F}_p \to \boldsymbol{F}_p$ に対して, $K_j' = \pi_j(K_0)$ を平文としたときの暗号文にあたる K_j を求めることはできない. □

提案方式 2 : general multi-secret scheme using USAE

提案方式 1 では k 人以上のユーザが揃うと全ての秘密情報を復元することができた. 方式 2 では, 一般アクセス構造を実現できるように拡張する.

モデル 2

1. 秘密情報は複数個ある.
2. 分散情報は各ユーザに対して 2 つである.
3. 任意のアクセス構造を実現できる.
4. 完全な秘密分散法である.

5. 秘密情報の分散はディーラーが行う.

アクセス構造を $\Gamma=\{A_1, A_2, \ldots, A_m\}$ とし, A_r $(r=1,2,\ldots,m)$ に含まれるユーザの人数を n_r とする. さらに, 複数の秘密情報を $\{K_1, K_2, \ldots, K_l\} \in \boldsymbol{F}_p^l$ とする.

ディーラーによる分散情報および公開情報の生成

1. 各ユーザの分散情報 $(s_i,\ v_i) \in \boldsymbol{F}_p^2$ $(i=1,2,\ldots,n)$ をランダムに選ぶ.
2. 各アクセス集合 A_r $(r=1,2,\ldots,m)$ に対して, (ID_i, s_i) $(U_i \in A_r)$ を通る高々 n_r-1 次多項式 $f_r(x)$ と (ID_i, v_i) $(U_i \in A_r)$ を通る高々 n_r-1 次多項式 $g_r(x)$ を求める. もし $g_r(0)=0$ となった場合は, v_i を取り直して $g_r(0) \neq 0$ を満たすようにする.
3. 各アクセス集合 A_r $(r=1,2,\ldots,m)$ に対して, K_j $(j=1,2,\ldots,l)$ と異なる値 $K_{0,r} \in \boldsymbol{F}_p^*$ を選ぶ. $K_{0,r}$ は, アクセス集合ごとに異なるように選ぶものとする.
4. $K_j = f_r(0) + K'_{j,r} \cdot g_r(0)$ をみたす $K'_{j,r}$, $(j=1,2,\ldots,l,\ r=1,2,\ldots,m)$ を計算する.
5. $d_{0,r} = f_r(0) + K_{0,r} \cdot g_r(0)$ $(r=1,2,\ldots,m)$ を計算する.
6. 写像 $\pi_{j,r} : \boldsymbol{F}_p \to \boldsymbol{F}_p$ $(j=1,2,\ldots,l,\ r=1,2,\ldots,m)$ で $\pi_{j,r}(K_{0,r}) = K'_{j,r}$ をみたすものを構成し $d_{0,r}$ と共に公開する.
7. ユーザ $U_i (i=1,2,\ldots,n)$ に $(s_i,\ v_i)$ を配布する.

アクセス集合に属するユーザによる秘密情報の復元

1. アクセス集合 A_r に属するユーザが揃うと, 多項式 $f_r(x)$, $g_r(x)$ が求まり, $f_r(0)$, $g_r(0)$ が計算できる.
2. 公開情報 $d_{0,r}$ を用いて $K_{0,r}$ が計算できる.
3. 公開情報 $\pi_{j,r}$ と $f_r(0)$, $g_r(0)$ を用いて, $K'_{j,r}$ および K_j が復元できる.

<提案方式2の模式図>

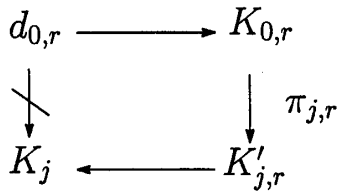

Fig.3 the proposal method 2

定理6.2 提案方式2はモデル2を実現している.

(証明)
任意のアクセス集合 A_r に対して, $g_r(x)$ を選ぶことができる. 安全性は提案方式1と同様である. □

注意 提案方式2では, どのアクセス集合もすべての秘密情報を復元できる. しかし, 公開情報を制限することにより, 復元できる秘密情報にも制限を加えることができる.

例 $A_1=\{U_1, U_2\}$, $A_2=\{U_2, U_3\}$, $A_3=\{U_3, U_4\}$ をアクセス集合とし, $K_j \in \boldsymbol{F}_p$ $(j=1,2,3,4)$ を秘密情報する. A_1 に対して, (ID_1, s_1), (ID_2, s_2) を通る直線を $f_1(x)$, (ID_1, v_1), (ID_2, v_2) を通る直線を $g_1(x)$ とする. アクセス集合 A_2, A_3 に対しても同様に $f_2(x)$, $g_2(x)$,

$f_3(x)$, $g_3(x)$ を定める．ディーラーは $K_{0,1}, K_{0,2}, K_{0,3}$ をランダムに選び，$d_{0,r} = f_r(0) + K_{0,r} \cdot g_r(0)$ $(r = 1, 2, 3)$ を公開する．次に，$K'_{j,r} = (K_j - f_r(0))/g_r(0)$ を計算し，写像 $\pi_{j,k} : \boldsymbol{F}_p \to \boldsymbol{F}_p$ で $\pi_{j,r}(K_{0,r}) = K'_{j,r}$ を満たすものを構成する．提案方式 2 ではすべての $\pi_{j,r}$ を公開するが，ここでは $\pi_{1,1}, \pi_{2,1}, \pi_{2,2}, \pi_{3,2}, \pi_{3,3}, \pi_{4,3}$ だけ公開する．このとき A_1 のメンバが揃えば K_1, K_2 を，A_2 のメンバが揃えば K_2, K_3 を，A_3 のメンバが揃えば K_3, K_4 を復元することができる．

提案方式 3 : Unconditionally Secure PVSS using USAE

モデル 3

1. 各ユーザへの分散情報は 2 つである．
2. k を 2 以上 n 以下の自然数とする．ユーザが k 人集まると，その k 人に配布された分散情報が正しいかどうか検証できる．

ディーラーによる分散情報と公開情報の生成

1. $\boldsymbol{F}_p$ の元を係数とする $k-1$ 次多項式 $f(x)$, $g(x)$ を生成する．ただし，$g(0) \neq 0$ とする．
2. $s_i = f(ID_i)$, $v_i = g(ID_i)$ $(i = 1, 2, \ldots, n)$ を計算し，(s_i, v_i) をユーザ U_i に配布する．
3. $K_0 \in \boldsymbol{F}_p^*$ をランダムに選び，$d_0 = f(0) + K_0 \cdot g(0)$ を計算する．
4. K_0 と異なる K' をランダムに選び，$K = f(0) + K' \cdot g(0)$ を計算する．
5. 写像 $\pi : \boldsymbol{F}_p \to \boldsymbol{F}_p$ で $\pi(K_0) = K'$ をみたすものを構成する．
6. d_0, K, π を公開する．

ユーザ k 人による分散情報の検証

1. ユーザが k 人揃うと提案方式 1 と同様に $f(0)$, $g(0)$, K_0 を求めることができる．
2. K_0 と公開情報 π を用いて K' を求める．さらに，$f(0)$, $g(0)$ を用いて K を計算し，これが公開されている K の値と等しいことを検証する．

＜提案方式 3 の模式図＞

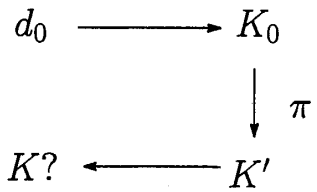

Fig.4 the proposal method 3

$f(0)$, $g(0)$ が復元できたときに，分散情報は正しいと判断することができる．そこでこの検証を通過した場合に，$f(0)$, $g(0)$ が復元されている確率について考察する．

ここでは，π として 1 次関数を選んだ場合について考え，$\pi(t) = at + b$ $(a \in \boldsymbol{F}_p,\ b \in \boldsymbol{F}_p^*)$ とする．

定理 6.3 $(a-1)K_0 + b \neq 0$ とする．このとき正規のユーザが k 人集まって，正規の手続き (検証に合格) で導いた値が $f(0), g(0)$ と一致する確率は $1 - \dfrac{p-2}{p(p-1)} \fallingdotseq 1 - \dfrac{1}{p}$ である．

（証明）

$d_0 = x + K_0 \cdot y$, $K = x + K' \cdot y$, $\pi(K_0) = a \cdot K_0 + b = K'$, $a \in \boldsymbol{F}_p$, $b \in \boldsymbol{F}_p^*$ とする．公開情報 d_0, a, b, K を固定するとき，二つの関係式

$$\begin{cases} d_0 = x + K_0 \cdot y \\ K = x + K' \cdot y = x + (aK_0 + b)y \end{cases}$$

を同時にみたす $(x, y) \in \boldsymbol{F}_p \times \boldsymbol{F}_p^*$ は $p-1$ 組存在することを証明する．

これを x, y に関する連立方程式と見て行列表示すると

$$\begin{pmatrix} 1 & K_0 \\ 1 & aK_0 + b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} d_0 \\ K \end{pmatrix}$$

となり，$(a-1)K_0 + b \neq 0$ の条件の下で解くと

$$\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{(a-1)K_0 + b} \begin{pmatrix} aK_0 + b & -K_0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} d_0 \\ K \end{pmatrix} = \frac{1}{(a-1)K_0 + b} \begin{pmatrix} (ad_0 - K)K_0 + bd_0 \\ -d_0 + K \end{pmatrix}$$

となる．ここで，$K_0 \in \boldsymbol{F}_p^*$ を動かすと $\begin{pmatrix} x \\ y \end{pmatrix}$ は $p-1$ 組存在する．実際，$a \neq 1$ のときは y が $p-1$ 通り動き，$a = 1$ のときは $d_0 \neq K$ より x が $p-1$ 通り動く．従って，正しくない x, y で 正しい K を復元できるものは $p-2$ 組ある．一方 x, y をランダムに選ぶ選び方は $p(p-1)$ 通りあるので，求める確率は $1 - \dfrac{p-2}{p(p-1)}$ である． □

π における a, b の値によっては，公開情報 a, b, d_0, K の値から $f(0)$ または $g(0)$ の値が確定してしまう場合がある．

定理 6.4 $(a-1)K_0 + b \neq 0$ の仮定の下で，$f(0)$, $g(0)$ が確定するための必要十分条件は，「$a = 1$ または $b = 0$」である．

（証明）

定理 6.3 の証明において，x または y が一意的に定まる条件を求めればよい．

1. y が K_0 の値によらず一定の値をとるのは $a = 1$ のときである．このとき，
   $(a-1)K_0 + b \neq 0$ より $b \neq 0$ であり，常に $y = \dfrac{-d_0 + K}{b}$ である．
2. x が K_0 によらず一定の値をとる場合を考える．

   case1 $b = 0$ のとき：

   $$(a-1)K_0 + b \neq 0 \text{ より } a \neq 1 \text{ であり，常に } x = \frac{ad_0 - K}{a-1} \text{ である．}$$

   case2 $b \neq 0$ のとき：

   $$x = \frac{(ad_0 - K)K_0 + bd_0}{(a-1)K_0 + b} \text{が } K_0 \text{の値によらず一定}$$
   $$\Longleftrightarrow 2 \text{つのベクトル } (ad_0 - K, bd_0),\ (a-1, b) \text{ が平行}$$
   $$\Longleftrightarrow K = d_0$$

このとき，$x+(aK_0+b)y = x+K_0y$ となり，$(a-1)K_0+b \neq 0$ に反する．
逆に $a=1$ または $b=0$ のとき，それぞれ x, y が一定であることは明らか． □

以上のことから π を適切に選べば，公開情報から $f(0)$, $g(0)$ は一意的には決まらない．よって提案方式3により計算量的な仮定をおくことなしに，正しく秘密情報が分散されたことを確認することができる．

注意：ディーラーとユーザの間に情報のやり取りがないため，PVSSとしては非対話的である．しかしアクセス集合に属するユーザ全員が揃わないと確認ができないので，この方法はVSSとしては対話的である．そこでこの提案方式3は，秘密情報を復元する際に併用することで，復元される秘密情報の正当性を確認するといった用途に利用できる．

応用例 1（提案方式 3 の提案方式 1 への応用）
2つの提案方式において，同じ k, $f(x)$, $g(x)$, (s_i, v_i) を用いる．提案方式 3 の手続きを事前に行うことにより，分散情報の正当性や復元された秘密情報の正当性を検証できる．

応用例 2（提案方式 3 の提案方式 2 への応用）
アクセス集合 A_r のユーザが秘密情報 K_j を復元したいとする．まず提案方式3を利用して，つまり π を用いて K が復元できることを確認する．$f_k(0)$ と $g_k(0)$ が正しいことが保証されるので，$\pi_{j,k}$ を用いて K_j を復元すればよい．

7 まとめと今後の課題

本論文において，USAEを利用した複数秘密分散法と公開検証可能秘密分散法を提案した．複数秘密分散法においては一般アクセス構造を実現でき，ユーザが管理する分散情報は，秘密情報の個数に依存せず常に2つである．公開検証可能秘密分散法においては，ユーザ間の情報のやり取りが必要なものの，複数秘密分散法と併用することにより有効である．またいずれも完全な秘密分散法を実現している．今後の課題として，提案方式3で正しい秘密情報が復元されなかったときに，どのユーザが間違った分散情報を提出したのかを特定することなどが挙げられる．

謝辞 貴重なご指摘をいただきました査読者の方々に感謝致します．

参考文献

[1] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, “Relations among notions of security for publickey encryption schemes”, Advances in Cryptology - CRYPTO '98, Lecture Notes in Computer Science 1462 (1998), 26-45.

[2] C. Blundo, A. De Santis, G. Di Crescenzo, A. Giorgio Gaggia and U. Vaccaro,“ Multi-secret sharing schemes ”, Advances in Cryptology – CRYPTO '94, Lecture Notes in Computer Science 839 (1994), 150-163.

[3] P. Feldman, "A Practical Scheme for Non-Interactive Verifiable Secret Sharing" ,Proceeding of the IEEE 28th Annual Symposium on Foundations of Computer Science (1987), 427-437.

[4] G. Hanaoka, J. Shikata, Y. Hanaoka, and H. Imai, " Unconditionally Secure Anonymous Encryption and Group Authentication ", Advances in Cryptology – ASIACRYPT 2002, Lecture Notes in Computer Science 2501 (2002), 81-99.

[5] R. L. Rivest, A. Shamir, and L. M. Adleman, " A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol21(1978),120-126.

[6] A. Shamir, " How to share a secret " Communication of the ACM, vol.22, (1979), pp 612-613

[7] M.Stadler, " Publicly Verifiable Secret Sharing ", Advances in Cryptology – EUROCRYPT '96, Lecture Notes in Computer Science 1070(1996), 190-199.

江村恵太 (非会員)
〒921-8611 石川県金沢市増泉3丁目4番30号 k-emura@jp.fujitsu.com
平成14年 金沢大学工学部機能機械工学科卒. 平成16年 同大学院自然科学研究科機械科学専攻博士前期課程修了. 工学修士. 現在 (株) 富士通北陸システムズ勤務.

野村明人 (正会員)
〒920-1192 金沢市角間町金沢大学総合教育棟 anomura@t.kanazawa-u.ac.jp
昭和60年 富山大学理学部数学科卒. 昭和62年 金沢大学大学院修士課程理学研究科修了. 平成3年 同大学大学院博士課程自然科学研究科修了. 学術博士. 平成11年 同大学工学部講師. 平成16年同大学大学院自然科学研究科助教授. 整数論とその応用に関する研究に従事. 日本数学会, 日本電子情報通信学会会員

(2004年7月29日受付)
(2005年7月20日最終稿受付)