数理解析研究所講究録
第1712巻 2010年 171-180

マルチ秘密分散法

東邦大学　理学部　情報科学科
足立　智子, 岡崎　千恵
Toho University, Department of Information Science
Tomoko Adachi, Chie Okazaki

要旨　一つの鍵(秘密情報)を共有して複数人で管理する秘密分散法に対して、複数の鍵(秘密情報)を共有して管理するマルチ秘密分散法がある。Chien 等は、2000 年に、一方向性関数、ハッシュ関数、線形符号を用いたマルチ秘密分散法を考案した。本稿では、このマルチ秘密分散法における分散情報の配布や鍵(秘密情報)の再構築の方法を紹介する。

1. はじめに

銀行において、金庫の鍵(秘密情報)1 個を複数の重役で管理したいとする。この時、一人に鍵を渡したり、全員に合鍵を渡したりすることはリスクがあるため避けたい。ここで、重役の人数を n 人とし、重役 n 人のうち任意の t 人以上が集まれば金庫を開けられるが、t 人未満では鍵(秘密情報)を開けることができないシステムを考える。これが Shamir の (t,n) しきい値法[5]と呼ばれる秘密分散法である。秘密分散法を応用にしたセキュリティソフトウェアが開発され、2004 年に「SplitSafe」が製品化された。

さらに、鍵(秘密情報)が 1 個の秘密分散法に対して、鍵(秘密情報)が 2 個以上のマルチ秘密分散法がある。代表的なマルチ秘密分散法の一つに 2000 年に Chien 等[3]により考案された (t,n) マルチ秘密分散法がある。この Chien 等の方法を基にして、2004 年には Yang 等[6]が、2005 年には Pang & Wang[4]が、別の方法の (t,n) マルチ秘密分散法を考案している。本稿では、これらいくつかのマルチ秘密分散法の基となった Chien 等の方法を紹介する。

2 Shamir のしきい値法

秘密分散法の代表的なものとして、Shamir のしきい値法がある。1979 年、Adi Shamir は (t,n) しきい値法を考案した。(t,n) しきい値法とは、n 人の参加者の間

で鍵(秘密情報) k を分散する方法である。 n 人中任意の t 人の参加者が集まることができた時、鍵(秘密情報) k を求めることができる。しかし、 t 人未満の参加者が集まった場合は、鍵(秘密情報) k を求めることができない。したがって、 t 人未満の分散情報が流出したとしても鍵(秘密情報) k は得られず、また $n-t$ 人まで分散情報を紛失したり、破壊されたりしても、鍵(秘密情報) k を再構築することができる特徴を持つ方法である。

2.1 分散配布

秘密分散法において、鍵(秘密情報)を分けて参加者に与える分散を行う人をディーラーと呼ぶ。ディーラーは、鍵(秘密情報)を同じ条件で分割し、分割した情報(分散情報)を n 人の参加者へ配布する。

アルゴリズム 2.1　(t,n) しきい値法における分散配布

Step 1. q を素数とする。そして、鍵 k を $k \in Z_q = \{0,1,2,\cdots,q-1\}$ と決める。ディーラーは Z_q の要素から、0 ではない異なる要素 $x_1,x_2,\cdots,x_n$ を選ぶ。その値 x_i を参加者 P_i に与える。 x_i の値は公開されている。

Step 2. ディーラーは Z_q から $t-1$ 個の要素 $a_1,a_2,\cdots,a_{t-1}$ をランダムに選ぶ。

Step 3. ディーラーは $a(x)$ の式

$$a(x) = k + \sum_{j=1}^{t-1} a_j x^j \bmod q$$

を用いて $y_i = a(x_i)\ (1 \le i \le n)$ となる y_i を計算する。

Step 4. ディーラーは分散情報 y_i を参加者 P_i に与える。

以上のようにディーラーはアルゴリズム 2.1 を用いて、分散配布を行う。そして、求められた分散情報 y_i は参加者 P_i のもとへそれぞれ分散される。参加者 P_i は公開されている値 x_i と公開されていない分散情報 y_i を所持している。

2.2 鍵の再構築

鍵(秘密情報)の再構築は、 n 人の参加者の中から任意の t 人が集まった時、可能となる。ここで、ランダムに集まった t 人をわかりやすい順序にするため、添え字を変更する。例えば、 n 人の参加者のうち 3 人集まったとする。参加者のうち、 n_2,n_4,n_5 が集まったならば、添え字をそれぞれ n_1',n_2',n_3' と変更する。このような方法を用いて、整理を行うこととする。

アルゴリズム 2.2　(t,n) しきい値法における鍵の再構築

Step 1. 参加者 n 人中 t 人以上が集まっている。

Step 2. それぞれ値 x_i と分散情報 $y_i(1 \le i \le n)$ を $a(x)$ の式

$$a(x) = k + \sum_{j=1}^{t-1} a_j x^j \bmod q$$

に代入して計算する。

Step 3. 求められた方程式によって k と $a_1, a_2, \cdots, a_{t-1}$ を導き出す。

鍵 k を得る。

以上のように、n 人の参加者はアルゴリズム 2.2 を用いて、鍵(秘密情報)の再構築を行う。集まった分散情報 y_i と公開されている値 x_i の対応が重要である。(t,n) しきい値法の鍵(秘密情報)の再構築は多項式を用いることによって鍵(秘密情報)を得ることができる。

2.3 特徴

安全性は、Shamir のしきい値法が線形独立であることで保障される。S をある有限体 $GF(q^m)$ とし、その有限体の原始元を α とする。与えられる行列 Q は次の通りである。

$$Q = \begin{bmatrix} 1 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & \alpha & \alpha^2 & \cdots & \alpha^{q^m-1} \\ 0 & 0 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(q^m-1)2} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{(q^m-1)(k-1)} \end{bmatrix}$$

任意の $k \times k$ の小行列の行列式が Vandermonde の行列式になるため、行列 Q の任意の k 個の列ベクトルが線形独立となる。Shamir のしきい値法では、第 2 列目の行列 Q を用いる。よって、この方法は安全である。

公開値は x_i である。したがって、$x_1, x_2, \cdots, x_n$ の n 人の参加者分の値が公開されている。つまり、公開値 x_i から分散情報 y_i の数がわかる。

(t,n) しきい値法は鍵(秘密情報)の再構築が行われると、分散情報 y_i が他の人に知られてしまうため分散配布からやり直す。繰り返し使用せず分散配布から再度行い、安全性を保つ。

3. マルチ秘密分散法の準備

Chien 等の (t,n) マルチ秘密分散法では、一方向性関数、ハッシュ関数、線形符号を用いる。一方向性関数とハッシュ関数は、どちらも分散配布と鍵(秘密情報)の再構築で使用される。そして、線形符号は分散配布で使用される。第 3 節では、これらについて紹介する。

3.1 一方向性関数

一方向性関数は、暗号において中心的な役割を担うことができる。一方向性とは、順方向の計算は簡単であるが、逆方向の計算は困難である性質をいう。一方向性関数を f として考えると、x より $y=f(x)$ を計算することは簡単であるが、逆に y より x を求めることは難しい関数のことをいう。例えば、素因数分解において、x と y を $x=(p,q)$, $y=f(x)=p\times q$ とする時、x より y を計算することは簡単であるが、y より x を計算することは困難である。また、離散対数においては、p を素数、$g\in Z_p^*$ としたとき、$y=f(x)=g^x \bmod p$ とする。この時、x より y を計算することは簡単であるが、y より x を計算することは困難である。この理論は、公開鍵暗号系の構築等、さまざまな場面で重要視される。

定義 3.1　一方向性関数

次の条件を満たすものを一方向性関数と呼ぶ。

条件 1.　x を入力して $f(x)$ を出力する多項式時間アルゴリズムが存在する。

条件 2.　全ての確率的多項式アルゴリズム A に対しても、以下が成立する。

$$\Pr[A(f(x))\in f^{-1}(f(x))]<\varepsilon(|x|)$$

上記の条件を満たす時、関数 f を一方向性関数と呼ぶ。

Chien 等の (t,n) マルチ秘密分散法では、分散情報 s と整数 r から一方向性関数 $f(r,s)$ が存在すると想定した。性質をまとめると以下のようになる。

(1) s と r を与えた時、$f(r,s)$ を計算することは簡単である。
(2) s と $f(r,s)$ を与えた時、r を計算することは困難である。
(3) s が不明であるならば r はどれも $f(r,s)$ を計算することは困難である。
(4) s を与えた時、$f(r_1,s)=f(r_2,s)$ のような r_1 と r_2 の 2 個の値を計算することは困難である。ただし、$r_1\neq r_2$ である。
(5) r と $f(r,s)$ を与えた時、s を計算することは困難である。

(6) r_i と $f(r_i,s)$ を与えた時、$f(r',s)$ を計算することは困難である。ただし、$r' \neq r_1$ である。

3.2 ハッシュ関数

ハッシュ関数は、署名等で用いられ、近年暗号において基本的な構成要素の一つとなっている。l 個の記号を含むメッセージを送ろうとする時、署名はもっと短くし、k 個の記号を含むとする。

定義 3.2 ハッシュ関数

次の条件を満たす時、l 個の記号の集合から k 個の記号の集合への関数がハッシュ関数である。

条件 1. 同じ $h(x)$ を与える 2 つの異なる x の値を見出すことを実行できない。

条件 2. h の像の中の y を与えられて、$h(x)=y$ であるような x を見出すことを実行できない。

上記の条件を満たす時、h をハッシュ関数と呼ぶ。

署名では、例えば、長い文書に対しては署名が膨大になってしまったり、安全性を保つため複雑な計算を使う時遅くなってしまったりする問題がある。ハッシュ関数は任意の長さの文書に対して、決められた大きさで生成することが可能である。S が安全な署名であると仮定する。メッセージ m に対して安全鍵 k を含む署名を $S(k,m)$ と定義する。h をハッシュ関数とすると $F(x,y)=h(S(x,y))$ となる。

3.3 線形符号

線形符号は、誤り訂正符号で用いられる符号の一つである。$F=\{0,1\}$ を位数 2 の有限体 $GF(2)$ とすると、F^N を F 上の N 次元線形空間とする。符号 $C(\subset F^n)$ が F^N のある K 次元部分空間となる時、符号 C は長さ N の K 次元線形符号である。これを (N,K) 線形符号と表記する。

Chien 等の (t,n) マルチ秘密分散法では、線形符号を用いた生成行列 G を扱う。$GF(2^m)$ 上で $N>K$ の (N,K) 線形符号は $N\times K$ の生成行列 G によって定義される。ここで、N は長さであり、K は線形符号の大きさである。これを $G(N,K)$ と表記する。行列 I は $K\times K$ の単位行列である。そして、行列 M は g が $GF(2^m)$ の

原始元であり、$K<2^m$の$(N-K)\times K$行列$[g^{(i-1)(j-1)}]$である。行列Iと行列Mは次の通りに表す。

$$I=\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{bmatrix}$$

$$M=\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & g & g^2 & \cdots & g^{K-1}\\ 1 & g^2 & g^4 & \cdots & g^{2(K-1)}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & g^{N-K-1} & g^{(N-K-1)2} & \cdots & g^{(N-K-1)(K-1)}\end{bmatrix}$$

行列Gは行列Iと行列Mを縦に並べた行列$\begin{bmatrix}I\\M\end{bmatrix}$である。行列$D$は線形符号の大きさ$K$のベクトルとし、$D=(d_1,d_2,\cdots,d_k)^T$とする。この時、行列$V$は行列$G$と行列$D$の積であり、$V=(v_1,v_2,\cdots,v_n)^T$と表す。Chien等の$(t,n)$マルチ秘密分散法では、行列$V=G\times D$から、$c_i=\sum_{j=1}^{K} g^{(i-1)(j-1)}d_j$, $1\le i\le N-K$である。

4. Chien等のマルチ秘密分散法

マルチ秘密分散法の代表的なものとして、Chien等の(t,n)マルチ秘密分散法がある。2000年、Hung-Yu ChienとJinn-Ke JanとYu-Min Tsengによって(t,n)マルチ秘密分散法が考案された。これはn人の参加者の間でp個の鍵(秘密情報)$d_1,d_2,\cdots,d_p$を分散する方法である。任意のt人の参加者が集まることができた場合、鍵(秘密情報)$d_1,d_2,\cdots,d_p$を求めることができる。しかし、t人未満が集まった場合、鍵(秘密情報)$d_1,d_2,\cdots,d_p$を求めることができない。Chien等の(t,n)マルチ秘密分散法は、線形符号に基づいている。分散情報sと整数rから一方向性関数$f(r,s)$を用いる。また、$f(r,s)$はハッシュ関数である。

4.1 分散配布

マルチ秘密分散法において、参加者P_iに与える分散情報s_iや鍵(秘密情報)2個以上を一括に管理が行えるように配布を行う人をディーラーと呼ぶ。ディーラ

ーは、分散情報s_iを参加者P_iに与え、同じ条件で鍵(秘密情報)2個以上を一括にして分散する配布を行う。

アルゴリズム4.1　(t,n)マルチ秘密分散法における分散配布

Step 1. ディーラーはn人の参加者P_iにp個の鍵を分散させる前に分散情報$s_1,s_2,\cdots,s_n$をランダムに選ぶ。そして、分散情報s_iを参加者P_iに与える。

Step 2. 整数rをランダムに選び、$f(r,s_i)\ i=1,2,\cdots,n$を計算する。$f(r,s_i)$は$GF(2^m)$の元である。そして、この生成元をgとおく。

Step 3. 生成元gより行列Gを構成する。行列Gは行列Iと行列Mを縦に並べた行列である。行列Iは$(p+n)\times(p+n)$の単位行列であり、行列Mは$(p+n-t)\times(p+n)$の行列である。

$$I=\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{bmatrix}$$

$$M=\begin{bmatrix}1 & 1 & \cdots & 1\\ 1 & g^{1} & \cdots & g^{p+n-t}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & g^{p+n-t-1} & \cdots & g^{(p+n-t-1)(p+n-t)}\end{bmatrix}$$

$$G=\begin{bmatrix}I\\ M\end{bmatrix}$$

Step 4. p個の鍵を$d_1,d_2,\cdots,d_p$とし、これは$GF(2^m)$の元である。そして、行列Dを以下とおく。

$$D=(d_1,d_2,\cdots,d_p,f(r,s_1),f(r,s_2),\cdots,f(r,s_n))^T$$

このとき、ディーラーは次の$V=G\times D$を持っている。

$$V = G \times D = \begin{bmatrix} I \\ M \end{bmatrix} \times D$$

$$= \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ 1 & g^{1} & \cdots & g^{p+n-t} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & g^{p+n-t-1} & \cdots & g^{(p+n-t-1)(p+n-t)} \end{bmatrix} \times \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_p \\ f(r,s_1) \\ f(r,s_2) \\ \vdots \\ f(r,s_n) \end{bmatrix}$$

よって、行列Vをまとめると以下のようになる。

$$V = (d_1, d_2, \cdots d_p, f(r,s_1), f(r,s_2), \cdots, f(r,s_n), c_1, c_2, \cdots, c_{p+n-t})^T$$

$$c_i = \sum_{j=1}^{p} g^{(i-1)(j-1)} d_j + \sum_{j=p+1}^{p+n} g^{(i-1)(j-1)} f(r,s_{j-p}), \quad 1 \le i \le p+n-t$$

Step 5. 安全な方法で$r, c_1, c_2, \cdots, c_{p+n-t}$を公表する。

以上のようにディーラーはアルゴリズム 4.1 を用いて、分散配布を行う。そして、求められた分散情報s_iは参加者P_iのもとへそれぞれ分散される。参加者P_iは分散情報s_iを持ち、公開されている情報は$r, c_1, c_2, \cdots, c_{p+n-t}$である。この情報を安全な方法で公表するとは、理由は公開値を変更されると鍵(秘密情報)の再構築が不可能となるためである。安全な経路によって公開することが重要である。

4.2 鍵の再構築

鍵の再構築は、n人の参加者の中から任意のt人が集まった時、可能となる。Shamir のしきい値法と同様に、添え字の変更を行うこととする。

アルゴリズム 4.2　(t,n)マルチ秘密分散法における鍵の再構築

Step 1.　n人中t人以上が集まっている。

Step 2. それぞれが持っている分散情報s_iから$f(r,s_i)$を求める。

Step 3. 公開されている$c_1, c_2, \cdots, c_{p+n-t}$へ求められた$f(r,s_i)$を代入する。

$$
\begin{aligned}
c_1 &= d_1 + d_2 + \cdots + d_p + f(r,s_1) + f(r,s_2) + \cdots f(r,s_n) \\
c_2 &= d_1 + g^1 d_2 + \cdots + g^{p-1} d_p \\
&\quad + g^p f(r,s_1) + g^{p+1}(r,s_2) + \cdots g^{p+n-1} f(r,s_n) \\
&\vdots \\
c_{p+n-t} &= d_1 + g^{p+n-t-1} d_2 + \cdots + g^{(p+n-t-1)(p-1)} d_p + g^{(p+n-t-q)p} f(r,s_1) \\
&\quad + g^{(p+n-t-1)(p+1)} f(r,s_2) + \cdots + g^{(p+n-t-)(p+n-1)} f(r,s_n)
\end{aligned}
$$

Step 4. 代入によって得られた $p+n-t$ 本の方程式を解く。

Step 5. 導かれた解から鍵 $d_1, d_2, \cdots, d_p$ を得る。

以上のように、n 人の参加者はアルゴリズム 4.2 を用いて、鍵(秘密情報)の再構築を行う。分散情報 s_i と公開されている整数 r より $f(r,s_i)$ を求め、それを公開されている c_i に代入することが Chien 等の (t,n) マルチ秘密分散法において重要である。Chien 等の (t,n) マルチ秘密分散法は Shamir の (t,n) しきい値法と同様に多項式を用いて鍵(秘密情報)の再構築を行う。

4.3 特徴

Chien 等のマルチ秘密分散法では、$p+n-t$ 本の方程式を用いている。その中の未知の変数の数は、$d_1, d_2, \cdots, d_p, f(r,s_1), f(r,s_2), \cdots, f(r,s_n)$ の $p+n$ 個である。安全性は、方程式の数より未知の変数の数の方が t 個多いことから鍵(秘密情報)を導き出すことは不可能である点から保障される。Chien 等の (t,n) マルチ秘密分散法は、n 人中 t 人以上が集まることによって導くことができる条件であることを考えると $p+n-t$ 本の方程式より未知の変数が多いため安全性が保障される。よって、Chien 等の (t,n) マルチ秘密分散法は t 人が集まって初めて鍵(秘密情報)を再構築できる方法である。

公開値は $r, c_1, c_2, \cdots, c_{p+n-t}$ であり、公開する数は $p+n-t+1$ 個である。特徴としては、p 個の鍵(秘密情報)の p が大きい時に、公開する数が他のマルチ秘密分散法と比べてほとんどの場合において少なくて済む。

分散情報 $s_1, s_2, \cdots, s_n$ が $f(r,s_i)$ として計算され参加者 P_i に知られるため、繰り返し用いることができる。なぜなら、再構築する際に他の人に知られる情報は $f(r,s_i)$ であるため、整数 r を毎回ランダムに決める $f(r,s_i)$ の分散情報 s_i は一方向性関数により十分保護されるからである。繰り返しアルゴリズム 4.2 を用いることが可能である。

5. 終わりに

本稿では、一つの鍵(秘密情報)を分割し、分散する秘密分散法として、Shamirの(t,n)しきい値法を扱った。さらに、マルチ秘密分散法として、複数の鍵(秘密情報)を一括し、複数の人でこの一括したグループを秘密分散法で管理するChien 等の(t,n)マルチ秘密分散法を扱った。秘密分散法は、多項式を用いたShamirのしきい値法以外にも、中国人剰余定理を用いたAsmuth & Bloomの方法[1]がある。また、中国人剰余定理に基づいたマルチ秘密分散法として、Chan & Changの方法[2]がある。

参考文献

[1] C. Asmuth and J. Bloom: A modular approach to key safeguarding. *IEEE Trans. Informat*, Theory, vol. 29 no. 2(1983), pp. 208-210.

[2] Chao-Wen Chan, Chin-Chen Chang: A scheme for threshold multi-secret sharing. *Applied Mathematics and Computation*, vol. 166 no. 1(2005), pp. 1-14

[3] Hung-Yu Chien, Jinne-Ke Jan, Yuh-Min Tseng: A practical (t,n) Multi-Secret Sharing Scheme. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. E83-A no. 12 (2000), pp. 2762-2765.

[4] Liao-Jun Pang, Yu-Ming Wang: A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing. *Applied Mathematics and Computation*, vol. 167 no. 2(2005), pp. 840-848.

[5] Adi Shamir: How to share a secret. *Communications of ACM*, vol. 22(1978), pp. 120-126.

[6] Chou-Chen Yang, Ting-Yi Chang, Min-Shiang Hwang: A (t,n) multi-secret sharing scheme. *Applied Mathematics and Computation*, vol. 151 no. 2 (2004), pp. 483-490.