数理解析研究所講究録
第1930巻 2015年 112-117

Gröbner基底を用いた秘密分散法の検討

山田雅樹
Masaki Yamada
愛媛大学大学院理工学研究科
Graduate School of Science and Engineering, Ehime University *

甲斐博
Hiroshi Kai
愛媛大学大学院理工学研究科
Graduate School of Science and Engineering, Ehime University †

Abstract

本研究ではWangらが提案したGröbner基底を使った秘密分散法に注目する．Wangらの方法では参加者に分配する分散情報は2つの多項式で構成されるが，分散情報のうち1つの多項式は参加者の間で共通の多項式である．本研究では分散情報を1つの多項式で構成する方法を提案する．

1 序論

Shamir[1]とBlakley[2]によって独立に提案された秘密分散法は，秘密情報を複数の分散情報に分割し，分散情報を一定の数以上集めた場合のみ秘密情報が復元できるという暗号手法の一つである．データそのものが複数に分かれるため分散情報の1つを取得したとしてもその情報から元データを復元することはできない．また分散情報の作成に鍵を用いないため，鍵の漏洩のリスクもない．そのため高い安全性が得られる．

秘密分散法が最初に提案されてから様々な手法や課題が見つけられているが実用化のための効率化や不正者の発見のための拡張などについて現在でも活発な研究が行われている．

本研究では数式処理アルゴリズムの秘密分散法への応用を調査した．具体的には多変数連立代数方程式の解法などに用いられるGröbner基底の応用を検討する．

Wangらが既にGröbner基底を使った秘密分散法[3]を提案しているが，その方法では秘密情報から得られる複数の多項式を分散情報とする．復元段階では分散情報を集めそれらのGröbner基底を求めることで秘密情報を得ることができる．

本研究では，Wangらの方法と比較して分散情報のサイズを小さくする方法の提案を行う．

2 Wangらの秘密分散法

秘密分散法はShamir[1]とBlakley[2]によって独立に考案された．$k \leq n$を満足する2つの正の整数n, kについて，n人の参加者のうちk人集まらないと秘密情報が得られないような方法を(k, n)閾値秘密分散法

*yamada.m@hpc.cs.ehime-u.ac.jp
†kai@cs.ehime-u.ac.jp

という．秘密分散法は一般的に秘密情報を分散する分散段階と秘密情報を復元する復元段階から構成される．(k,n) 閾値秘密分散法の分散段階では，秘密情報 S からの n 個の分散情報 $D_1, D_2, \cdots, D_n$ を生成しそれぞれを参加者に配布する．復元段階では，分散された秘密情報を k 個以上集め，計算を行い秘密情報を再構成する．

Shamir の (k,n) 閾値秘密分散法は有限体上の多項式を用いて分散情報を生成する．一方，復元段階では n 人の参加者から k 個の分散情報を集め，多項式補間で秘密情報を計算する．(k,n) 閾値秘密分散法を実現する方法は多項式補間以外にも多くの方法が提案されているが，特に数式処理の理論で Gröbner 基底が利用できることを Wang らが示している．

Wang らの方法では多項式を用いて分散情報を生成する．F を任意の体とし $F[x_1, x_2, \ldots, x_m]$ を多項式環とする．ここで $x_1, \ldots, x_m$ は多項式の変数である．この時，分散情報は秘密情報を含む多項式 $g \in F[x_1, x_2, \ldots, x_m]$ と乱数により生成された n 個のランダムな多項式 $g_i \in F[x_1, x_2, \ldots, x_m]$ の組 $D_i = (g, g_i), i = 1, \cdots, n$ として構成される．

具体的には Wang らの手法の分散段階は以下のような手順になる．

アルゴリズム 1 (Wang らの (k,n) 閾値秘密分散法の分散段階)
入力: 秘密情報 S，閾値 k，分散数 n

出力: 分散情報 $(g, g_1), (g, g_2), \cdots, (g, g_n)$

方法:

1. k 個の多項式 $f_i \in F[x_1, x_2, \ldots, x_m], 1 \leq i \leq k$ をランダムに選ぶ．但し，多項式 f_i は

$$f_i \notin < f_1, \ldots, f_{i-1}, f_{i+1}, \cdots, f_k >$$

   を満たすと仮定する．
2. ランダムな行列 $B \in F^{n \times k}$ を選ぶ．但し行列 B の任意の $k \times k$ 部分行列は正則であると仮定する．
3. 多項式 g_i を次の式で求める．

$$\begin{pmatrix} g_1 \\ g_2 \\ \cdot \\ g_n \end{pmatrix} = B \times \begin{pmatrix} f_1 \\ f_2 \\ \cdot \\ f_k \end{pmatrix}$$

4. 多項式 $g = S + a_1 f_1 + a_2 f_2 + \cdots + a_k f_k$ を計算する．この時 $a_i \in F$ は乱数であり，全ての i について $a_i \neq 0$ とする．

復元段階では任意の k 個の分散情報の集合 $D = \{(g, g_{j_1}), \cdots, (g, g_{j_k})\}$ を得て，多項式集合の Gröbner 基底を求める．得られた Gröbner 基底を用いて g を簡約し秘密情報を求めることができる．Wang らの (k,n) 閾値秘密分散法の復元段階は次のようにまとめられる．

アルゴリズム 2 (Wang らの (k,n) 閾値秘密分散法の復元段階)
入力: $D = \{(g, g_{j_1}), \cdots, (g, g_{j_k})\}$

出力: 秘密情報 S

方法:

1. $< g_{j_1}, g_{j_2}, \cdots, g_{j_k} > = < f_1, f_2, \cdots, f_k >$ の Gröbner 基底 G を求める．

2. g を G で簡約し秘密情報 S を求める.

Wangらの方法が次の2つの条件を満たす場合に (k,n) 閾値秘密分散法を構成することが論文 [3] で証明されている.

条件 A $g_{j_1},\cdots,g_{j_k}$ を $g_1,\cdots,g_n$ から選ぶ任意の k 個の多項式集合とすると, $f_1,\cdots,f_k \in < g_{j_1},\cdots,g_{j_k} >$ であり, $g_{j_i} \notin < g_{j_1},\cdots,g_{j_{i-1}},g_{j_{i+1}},\cdots,g_{jk} >$ でなければならない.

条件 B B の任意の $k\times k$ 部分行列 B_1 について $(b_1,\cdots,b_k)=(a_1,\cdots,a_k)\times B_1^{-1}$ としたとき, 全ての i について $b_i \neq 0$ でなければならない.

但し, Wangらの手法の問題として, どのような $f_1,\cdots,f_k$ と B を取れば条件A および条件Bを満足するような $g_1,\cdots,g_n$ が構成的に得られるかについては論文では示されていない.

ランダムに多項式や行列を取ってみて結果的に条件A および条件Bを満足するかどうかを確認することはできるが, 計算量が多くなる. ここで, ランダムに生成する多項式の変数の数 m については, Wangらが例題で示しているのと同様に集める多項式の数 k と同じ値とするのが単純である. しかし閾値 k を大きくしようとすると変数の数が同時に増加することになる. 一般に, 変数の数の増加とともにGröbner基底の計算量は増えていくので計算時間が長くなる. 変数の数をなるべく少なくすることができればWangらの手法の効率化につながる.

また, 計算量以外のもう一つの問題として,

- 復元段階において参加者 i に渡す情報が (g_i,g) となるが, g については全員が同じ情報を持つことになりある種の無駄が生じている.

この問題について本研究では参加者に与える分散情報の一つである g_i の中に秘密情報を含めることにより分散情報のサイズを減少する方法を検討した. またその結果として変数の数を一つ少なくすることができることを示す.

3 提案手法

Wangらの手法の分散段階では秘密情報 S を隠すための多項式 $g=S+a_1f_1+a_2f_2+\cdots+a_kf_k$ を計算し g_i とともに参加者に分散情報として配布する. 復元段階では g から g_i が所属するイデアル $< f_1,\cdots,f_k >$ 要素を取り除いて秘密情報 S を得ることを行う. この考え方は提案手法でも用いる.

但し, 提案手法では S を隠すために各 g_i に S を加える. ここで, g_i は次のように求める.

$$\begin{pmatrix} g_1 \\ g_2 \\ \cdot \\ g_n \end{pmatrix} = \begin{pmatrix} S \\ S \\ \cdot \\ S \end{pmatrix} + B \times \begin{pmatrix} f_1 \\ f_2 \\ \cdot \\ f_{k-1} \end{pmatrix}$$

$B \in Z_p^{n\times(k-1)}$ はランダムな行列である. $f_i \in Z_p[x_1,x_2,\cdots,x_{k-1}]$ はランダムな多項式であり, $f_i \notin < f_1,\cdots,f_{i-1},f_{i+1},\cdots,f_{k-1} >$ を満足すると仮定する.

このとき, 異なる i と j について $g_{i,j}=g_i-g_j$ を求めると, 秘密情報 S が取り除かれ, 多項式 $g_{i,j}$ は

$$g_{i,j} \in < f_1,\cdots,f_{k-1} >$$

を満足すると考えられる. そこで, k 個の分散情報 $g_1,\cdots,g_k$ を集め, $k-1$ 個の多項式 $g_{1,2},g_{2,3},\cdots,g_{k-1,k}$ を求める. 提案手法での多項式の変数の数は $m=k-1$ とする. 多項式集合 $\{g_{1,2},g_{2,3},\cdots,g_{k-1,k}\}$ の

Gröbner 基底 G を求め，任意の g_i を G で割ると秘密情報 S が得られると考えられる．提案手法は次のようにまとめられる．

アルゴリズム 3 (提案手法の分散段階)
入力 秘密情報 $S \in Z_p$，閾値 k，分散数 n

出力 n 個の分散情報 $g_1, g_2, \cdots, g_n$

方法 1. $k-1$ 個のランダム多項式 $f_i \in Z_p[x_1, x_2, \cdots, x_{k-1}], 1 \leq i < k$ を生成する．

2. 行列 $B \in Z_p^{n \times (k-1)}$ を生成する．行列の要素は乱数を与える．

3. n 個の分散情報 g_i を次の式で求め，n 人の参加者に分配する．

$$\begin{pmatrix} g_1 \\ g_2 \\ \cdot \\ g_n \end{pmatrix} = \begin{pmatrix} S \\ S \\ \cdot \\ S \end{pmatrix} + B \times \begin{pmatrix} f_1 \\ f_2 \\ \cdot \\ f_{k-1} \end{pmatrix}$$

アルゴリズム 4 (提案手法の復元段階)
入力 k 個の分散情報 $g_{j_1}, g_{j_2}, \cdots, g_{j_k}$

出力 秘密情報 $S \in Z_p$

方法 1. $k-1$ 個の多項式 $g_{j_1,j_2}, g_{j_2,j_3}, \cdots, g_{j_{k-1},j_k}$ を計算する．

$$g_{j_1,j_2} = g_{j_1} - g_{j_2},\ g_{j_2,j_3} = g_{j_2} - g_{j_3},\ \cdots,\ g_{j_{k-1},j_k} = g_{j_{k-1}} - g_{j_k}$$

2. イデアル $\langle g_{j_1,j_2}, \cdots, g_{j_{k-1},j_k} \rangle$ の Gröbner 基底 G を求める．

3. いずれかの g_i の G による標準形を求める．

4. 標準形が整数であるならそれを秘密情報として出力する． 標準形が変数を含む多項式であるなら間違った分散情報が与えられていると報告してアルゴリズムを終了する．

提案手法が (k, n) 閾値秘密分散法であるための条件は，Wang らの手法と同様に，以下の 2 つが必要である．

条件 A $g_{j_1}, \cdots, g_{j_k}$ を $g_1, \cdots, g_n$ から選ぶ任意の k 個の多項式集合とする．この時，$f_1, \cdots, f_k \in < g_{j_1,j_2}, \cdots, g_{j_{k-1},j_k} >$ であり，$g_{j_{i-1},j_i} \notin < g_{j_1,j_2}, \cdots, g_{j_{i-2},j_{i-1}}, g_{j_i,j_{i+1}}, \cdots, g_{j_{k-1},j_k} >$ でなければならない．

条件 B B の $(k-1) \times (k-1)$ 部分行列 B_1 と B_2 を次のような行列とする．

$$B_1 = \begin{pmatrix} b_{j_1,1} & b_{j_1,2} & \cdots & b_{j_1,k-1} \\ b_{j_2,1} & b_{j_2,2} & \cdots & b_{j_2,k-1} \\ \vdots & \vdots & & \vdots \\ b_{j_{k-1},1} & b_{j_{k-1},2} & \cdots & b_{j_{k-1},k-1} \end{pmatrix}$$

$$B_2 = \begin{pmatrix} b_{j_2,1} & b_{j_2,2} & \cdots & b_{j_2,k-1} \\ b_{j_3,1} & b_{j_3,2} & \cdots & b_{j_3,k-1} \\ \vdots & \vdots & & \vdots \\ b_{j_k,1} & b_{j_k,2} & \cdots & b_{j_k,k-1} \end{pmatrix}$$

この時,

$$\begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,k-1} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,k-1} \\ \vdots & \vdots & & \vdots \\ c_{k,1} & c_{k,2} & \cdots & c_{k,k-1} \end{pmatrix} = \begin{pmatrix} b_{j_1,1} & b_{j_1,2} & \cdots & b_{j_1,k-1} \\ b_{j_2,1} & b_{j_2,2} & \cdots & b_{j_2,k-1} \\ \vdots & \vdots & & \vdots \\ b_{j_k,1} & b_{j_k,2} & \cdots & b_{j_k,k-1} \end{pmatrix} \times (B_1 - B_2)^{-1}$$

を計算したとき，全ての i,j について $c_{i,j} \neq 0$ でなければならない.

ここで示した条件 A および条件 B を満足するとき，提案法は (k,n) 閾値秘密分散法になる．この証明は Wang らが証明した方法と同じようにできる.

今，k 人の参加者が秘密情報を得ようと考えたと仮定する．$< f_1, \cdots, f_k >=< g_{j_1,j_2}, \cdots, g_{j_{k-1},j_k} >$ であるので，$< f_1, \cdots, f_k >$ の Gröbner 基底 G あるいは $< g_{j_1,j_2}, \cdots, g_{j_{k-1},j_k} >$ の Gröbner 基底 G' により任意の g_i の標準形を求めると秘密情報 S が得られる.

また閾値より少ない $k-1$ 人の参加者が秘密情報を得ようと考えたと仮定する．$< g_{j_1,j_2}, \cdots, g_{j_{k-2},j_{k-1}} >$ の Gröbner 基底を G_1 と書く．もし G_1 による $g_{j_1}, \cdots, g_{j_k}$ の標準形が S になったと仮定する.

定義より次の関係式が成り立つことに注意する.

$$\begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_{k-1} \end{pmatrix} = (B_1 - B_2)^{-1} \times \begin{pmatrix} g_{j_1,j_2} \\ g_{j_2,j_3} \\ \vdots \\ g_{j_{k-1},j_k} \end{pmatrix}$$

$g_{j_1}, \cdots, g_{j_k}$ の定義より，

$$\begin{pmatrix} g_{j_1} \\ g_{j_2} \\ \vdots \\ g_k \end{pmatrix} = \begin{pmatrix} S \\ S \\ \vdots \\ S \end{pmatrix} + \begin{pmatrix} b_{j_1,1} & b_{j_1,2} & \cdots & b_{j_1,k-1} \\ b_{j_2,1} & b_{j_2,2} & \cdots & b_{j_2,k-1} \\ \vdots & \vdots & & \vdots \\ b_{j_k,1} & b_{j_k,2} & \cdots & b_{j_k,k-1} \end{pmatrix} \times \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_{k-1} \end{pmatrix}$$

この式は次のように書くことが出来る.

$$\begin{pmatrix} g_{j_1} \\ g_{j_2} \\ \vdots \\ g_k \end{pmatrix} = \begin{pmatrix} S \\ S \\ \vdots \\ S \end{pmatrix} + \begin{pmatrix} b_{j_1,1} & b_{j_1,2} & \cdots & b_{j_1,k-1} \\ b_{j_2,1} & b_{j_2,2} & \cdots & b_{j_2,k-1} \\ \vdots & \vdots & & \vdots \\ b_{j_k,1} & b_{j_k,2} & \cdots & b_{j_k,k-1} \end{pmatrix} \times (B_1 - B_2)^{-1} \times \begin{pmatrix} g_{j_1,j_2} \\ g_{j_2,j_3} \\ \vdots \\ g_{j_{k-1},j_k} \end{pmatrix}$$

任意の j_i について $g_{j_i} - S \in < g_{j_1,j_2}, \cdots, g_{j_{k-2},j_{k-1}} >$ と仮定しているので $c_{j_i,k-1} g_{j_{k-1},j_k} \in < g_{j_1,j_2}, \cdots, g_{j_{k-2},j_{k-1}} >$ とならなければならない．条件 B より $c_{j_i,k-1} \neq 0$ と仮定しているので，$g_{j_{k-1},j_k} \in < g_{j_1,j_2}, \cdots, g_{j_{k-2},j_{k-1}} >$ が得られるが，これは条件 A に反する．よって G_1 による $g_{j_1}, \cdots, g_{j_k}$ の標準形が S になることはない．つまり閾値より小さい分散情報を集めても秘密情報は得られない.

4 提案手法の例

本節では提案手法の例について示す．秘密情報を $K = 11 \in Z_{101}$ とする．この時，$(3,4)$ 閾値法を考える．$k = 3$ なので $k-1 = 2$ 個のランダム多項式を生成する.

$$f_1 = 3xy + 32y + 6, f_2 = 16xy + 76x + 28y + 11$$

次に以下のような 4×2 行列 B を作成する.

$$B = \begin{pmatrix} 64 & 54 \\ 18 & 1 \\ 3 & 56 \\ 86 & 93 \end{pmatrix}$$

$\{f_1, f_2\}$ および B は条件 A と条件 B を満足する. 分散情報 g_i を次の式で求め, n 人の参加者に分配する.

$$\begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \\ 11 \\ 11 \end{pmatrix} + \begin{pmatrix} 64 & 54 \\ 18 & 1 \\ 3 & 56 \\ 86 & 93 \end{pmatrix} \times \begin{pmatrix} 3xy + 32y + 6 \\ 16xy + 76x + 28y + 11 \end{pmatrix}$$

$$= \begin{pmatrix} 46xy + 64x + 25y + 80 \\ 70xy + 76x + 99y + 29 \\ 97xy + 14x + 48y + 39 \\ 29xy + 99x + 3y + 35 \end{pmatrix}$$

復元段階では 3 個の分散情報 g_1, g_2, g_3 が得られたと仮定する. 次の多項式を計算する.

$$g_{1,2} = g_1 - g_2 = 77xy + 89x + 27y + 51, g_{2,3} = g_2 - g_3 = 74xy + 62x + 51y + 91$$

イデアル $\langle g_{1,2}, g_{2,3} \rangle$ の Gröbner 基底 G を求める.

$$G = \{x + 69y + 17, y^2 + 24y + 19\}$$

4 個の多項式 g_i をどれでもいいので G による標準形を求めると, 秘密情報 11 が出力される.

5 結論

本研究では Wang らにより提案された Gröbner 基底を用いた方法の改良を検討した. 提案手法では分散情報となる多項式の数が 1 つにする方法を示した. また Wang らの方法と比較して多項式の変数の数が 1 つだけ減少する. 今後の課題として, 計算機実験を行い計算時間の評価や, 不正検知・不正者特定の方法の検討などが挙げられる.

参 献

[1] Adi Shamir, How to Share a Secret, Communications of the ACM, Vol.22, Issue 11, pp.612-613, 1979.

[2] G.R Blakley, Safeguarding cryptographic keys, Proceedings of the National Computer Conference, Vol. 48, pp.313-317, 1979.

[3] Wang Mingsheng, Feng Dengguo and Wang Guilin, Secret Sharing Schemes Based on Computer Algebra, Journal of Software, Vol. 13, pp.143-148, 2002.