数理解析研究所講究録
第1759巻 2011年 11-14

有理関数近似を用いた秘密分散法
A Secret Sharing Scheme Using Rational Approximation

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

In this paper, a method to detect cheaters on the Shamir's (k,n) threshold secret sharing scheme is proposed using rational interpolation. When a rational interpolant is computed for l shares $D_i, i = 1,\cdots,l$, where $l > k$, then unattainable points of the rational interpolant may detect the cheaters.

1 はじめに

秘密情報を守るためには通常は鍵を用いた暗号化が行われるが，鍵を用いない秘密分散法のような手法が存在する．秘密分散法では秘密情報をいくつかの分散情報に分割して秘密情報を保持する．一方で，秘密情報を復元するためにはいくつかの分散情報を集めて計算する．これまでに多くの秘密分散法が提案されているが，古典的な手法の一つはShamirによる(k,n)閾値秘密分散法である．但し，Shamirによる(k,n)閾値秘密分散法はある種の不正について安全でないことが知られている[1, 3, 5]．この問題に対して我々は有理関数補間を用いてある条件のもとで不正者の特定を行う手法を提案している[2]．本論ではその方法を再検討し特定を行う手順について考察する．

2 秘密分散法

秘密情報Dをn個の分散情報に分割し，そのうち任意のk個の分散情報が集まれば，秘密情報Dを復元できる方法がShamir[4]とBlakleyにより提案されている．このような手法を一般に(k,n)閾値秘密分散法と呼ぶ．秘密分散法の特徴として，$k-1$個以下の分散情報の集合からは秘密情報に関する情報は一切得られない．ここで，n,kは正の整数であり，秘密情報Dは正の整数sについて$D \in \{1,2,\cdots,s-1\}$とする．

Shamirの(k,n)閾値秘密分散法では$k-1$次多項式$f(x)$の定数項をDと置き

$$f(x) = D + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1} \bmod p$$

とする．ここで$a_1,\cdots,a_{k-1}$は乱数で与えられた整数でpは素数とする．

この手法には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がある．それぞれ以下のように行う．

*kai@cs.ehime-u.ac.jp

分散段階 n 個の分散情報は相異なる $x_1, \cdots, x_n$ について $(x_1, f(x_1)), \cdots, (x_n, f(x_n))$ により得られる．これを参加者に分配する．

復元段階 n 個の分散情報のうち任意の k 個の分散情報から多項式補間を計算することにより D が得られる．

この手法で不正者が存在する場合の問題については，例えば分散情報 $(x_1, f(x_1))$ のかわりに $(x_1, f(x_1)+\epsilon)$ を与えたとき，他の $k-1$ 人の分散情報を持つ参加者は誤った情報 D' を得るのに対し，不正者だけが正しい秘密情報 D が得られることが指摘されている [3]．一般に k 個の分散情報の中に 1 つ以上の誤った分散情報が存在した場合，明らかに正しい秘密情報は得られない．また，得られた秘密情報が正しいかどうか検証もできないという問題がある．

3 有理関数補間を用いた秘密分散手法と不正者の特定

論文 [2] では以下に述べる手法を提案している．提案手法は分散情報を生成し参加者に分散する分散段階と秘密情報を復元する復元段階がある．本手法では，ディーラと参加者と復元者を想定する．ディーラは分散情報を秘密情報から生成し参加者に配布する．復元者は参加者から集めた分散情報を用いて復元計算を行う．分散段階は前節で述べた手法を用いるので，以下復元段階のみ述べる．

1. 参加者から l 個の分散情報を集める $(l > k)$.
2. $l = M + N + 1$ となる M, N を求める．但し $M - N \leq k - 1$ となるように定める．
3. 集めた分散情報 $(x_{i_1}, f(x_{i_1}), \cdots, (x_{i_l}, f(x_{i_l}))$ と，有理関数

$$r(x) = \frac{a_0 + a_1 x + \cdots + a_M x^M}{1 + b_1 x + \cdots + b_N x^N}$$

に対して $f(x_{i_j}) = r_{M,N}(x_{i_j}), j = 1, \cdots, l$ となるように有理関数の係数を定める．

4. 結果に応じた内容を各参加者に返す．

この復元段階において M, N の取り方が問題となるが，$M = k - 1 + N$ のように取ると，$l = k + 2N$ になる．不正者が存在する場合を考えると，正しい分散情報は $f(x)$ 上の点であるが，不正者は $f(x)$ を知らないため不正な分散情報が $f(x)$ 上の点になる確率は低い．不正な分散情報を少数（N 以下）含むようなデータ集合で有理関数補間を求めると，論文 [2] で述べたように全ての不正な分散情報は到達不能点となって現れる．到達不能点は分子と分母の多項式の GCD の計算によりその位置を計算できる．GCD を取り除き有理関数を既約にすると $f(x)$ が得られる．但し，どのように不正が検知されて特定できるかは示されていない．

4 不正者の検知と特定

前節の有理関数で不正者がいなければ結果は多項式 $f(x)$ となる．不正者が存在する場合は多項式または有理関数となる可能性がある．結果が有理関数になれば確実に不正者がいることは検知できる．多項式になる場合は Tompa 法を用いると，$k-1$ 人の不正者が存在する場合，残りの 1 人の参加者が不正を検知できる確率が

$$1 - \frac{(s-1)(k-1)}{p-k}$$

であることが示されている．すなわちpを十分に大きくすると検知確率を上げることができる．得られた秘密情報Dが$D > s-1$かどうかを確認することにより検知できる．

結果が有理関数になる場合，

- 到達不能点をGCD計算により除去して多項式になる
- 既約にしても有理関数になる

の2通りが考えられる．前者の場合は秘密情報が$D < s$の場合は高い確率で正しい秘密情報が得られていると予想できる．またこの時，到達不能点の位置が不正な分散情報の値である．既約にしても有理関数の場合はN個以上の不正が含まれることが予想される．検知だけでなく特定を行う場合は，任意の分散情報を加えて復元する．

以上の考察により復元者が不正者の特定をするためには以下の手順が一つの方法として考えられる．

Step 1 $r_{M,N}(x)$が多項式になるなら以下の手順を行う．

1. 秘密情報Dが$D < s$ならば，Dを秘密情報として返す．
2. 秘密情報Dが$D > s-1$ならば不正者が存在するので，分散情報を2つ加えて$M = M+1, N = N+1$として再度$r_{M,N}$を計算する．Step 1に戻る．

Step 2 $r_{M,N}(x)$が有理関数になるなら以下の手順を行う．

1. 既約にすると多項式になるなら次の手順を行う．
   (a) 秘密情報Dが$D < s$ならば，Dを秘密情報として返す．不正者はGCDの根で与えられる．
   (b) 秘密情報Dが$D > s-1$ならば不正者が存在するので，分散情報を2つ加えて$M = M+1, N = N+1$として再度$r_{M,N}$を計算する．Step 1に戻る．
2. 既約にしても有理関数になるならば不正者が存在するので，分散情報を2つ加えて$M = M+1, N = N+1$として再度$r_{M,N}$を計算する．Step 1に戻る．

但し，この手続において$M + N + 1 < n$を仮定する．

5 おわりに

本論で提案した手法により高い確率で正しい秘密情報が得られると考えられる．しかし，その値の導出や確率を上げる手法の検討は今後の課題である．また，pが大きくなると分散情報の値が大きくなる．(k, L, n)閾値秘密分散法のような分散情報の大きさを制限する手法の検討も重要である．

参 考 文 献

[1] Marco Carpentieri, A perfect threshold secret sharing scheme to identify cheaters, Designs, Codes and Cryptography, Volume 5, Number 3, pp.183-187, 1995.

[2] 藤原名穂, 甲斐博, 有理関数補間を用いた秘密分散法の一考察, 情報処理学会コンピュータセキュリティシンポジウム論文集, pp.959-962, 2008.

[3] Josep Rifa-Coma, How to avoid the cheaters succeeding in the key sharing scheme, Designs, Codes and Cryptography, Volume 3, pp.221-228, 1993.

[4] Adi Shamir, How to share a secret, Communications of the ACM, Volume 22, Issue 11, pp.612-613, 1979.

[5] Martin Tompa and Heather Woll, How to share a secret with cheaters, Journal of Cryptology, Volume 1, Number 2, pp.133-138, 1988.