6W-1

オイラーの公式を用いた(*k*, *L*, *n*)閾値秘密分散法の提案

A (*k*, *L*, *n*) *Threshold Secret Sharing Algorithm Based on Euler's Theorem*

武田 雄人† 大場 充‡ 佐藤 康臣‡
Yuto Takeda Mitsuru Ohba Yasuomi Sato
† 広島市立大学大学院 情報科学研究科博士前期課程
Graduate School of Hiroshima City University
‡広島市立大学情報科学部
Faculty of Information Sciences, Hiroshima City University

1. はじめに

秘密情報を安全に保管する方法のひとつとして *Shamir* により提案された秘密分散法がある[1]. 秘密分散法とは秘密情報に数学的処理を行い分散符号化し，複数個の情報を生成する．この生成した全てのあるいは一定数以上の分散情報から元の秘密情報が復元可能とする．この分散情報が一定数より少ない時，それらの分散情報からは元の秘密情報が復元できないため，秘密情報を安全に保管することができる.

一般に知られている秘密分散法は (*k*, *n*)閾値法[1]で，生成した *n* 個の分散情報のうち，*k* 個以上の分散情報があれば秘密情報を復元可能することができ，*k* 個未満の分散情報からは秘密情報を復元することはできない．この復元可能な分散集合を有資格集合，復元不可能な分散集合を禁止集合と言い，有資格集合と禁止集合の対をアクセス構造と呼ぶ.

この(*k*, *n*)閾値法は符号化効率が悪いことが知られており[2]，その問題を改善した (*k*, *L*, *n*)閾値法[3]が提案されている．これは，*k* 個以上の分散情報の集合が有資格集合となり，*k*−*L* 個以下の分散情報の集合で禁止集合となり，*l*(*k*−*l*≦*l*≦*L*)個の分散情報では秘密情報 *S* に対して(*l*/*L*)*H*(*S*)の曖昧さが残る秘密分散法である．ここで *H*(*S*)は秘密情報 *S* の不確かさの程度を表す情報量である.

また，閾値に限らないアクセス構造を一般型アクセス構造と言う．これは，(*k*, *n*)閾値法や，(*k*, *L*, *n*)閾値法のように，分散情報の個数ではなく，分散情報の集合に依存する秘密分散法で，岡田ら[4]によって実現例が示されている.

本稿では，オイラーの公式を利用した三つ組み暗号[5]を応用して，一般型アクセス構造を構成可能な秘密分散法の実現方法について説明する.

2. オイラーの公式を用いた秘密分散法

2.1 オイラーの公式

オイラーの公式は，互いに素な非負整数 *a* と *n* が与えられたとき，(1)式を満たす公式である.

$$a^{\phi(n)} \equiv 1 \pmod{n} \qquad (1)$$

ただし，$\phi(n)$はオイラー関数と呼ばれ，*n* 以下の *n* と互いに素な整数の個数を与える関数である.

本提案方式は，(1)式の両辺に *a* を掛けた(2)式を用いて秘密分散法を実現する.

$$a^{\phi(n)+1} \equiv a \pmod{n} \qquad (2)$$

2.2 分散情報について

オイラーの公式を用いた秘密分散法は以下の 5 つ組で 1 つの分散情報となる.

$\{\alpha_i,\ \beta_i,\ \Gamma,\ m,\ s\}$

α_i: 分散情報に関する情報
β_i: 復元に関する情報
Γ: 秘密情報に関する情報
m : 分散情報の復元可能性についての情報
s: 法の値

本方式は集めた分散情報の個数だけではなく，後述するα_iを構成する素数$p_1,p_2,\cdots,p_k$を全て集めたかが復元の鍵となっており，その意味で閾値によらない一般型アクセス構造といえる.

2.3 分散フェーズ

秘密情報γ，必要な分散情報の個数の下限 *k*, 分散情報の全体の個数を *n* とした時の分散情報の生成方法について以下で説明する.

(1) 2 つ以上の任意個の素数を生成し，その積を求め, 法の値 *s* とする.

(2) *s* のオイラー関数$\phi(s)$を求め，(3)式を満たす整数 *a*, *b* を求める.

$$\phi(s)+1 = ab \pmod{s} \qquad (3)$$

(3) *k*個の素数$p_1,p_2,\cdots,p_k$を生成し，(4)式で定義される*m*を求める.

$$m = \sum_{i=1}^{k} p_i \qquad (4)$$

(4) 各分散情報の第 1 成分を計算するために整数e_{ij}を乱数により生成し，(5)式のようにα_iを計算し第 1 成分とする.

$$\alpha_1 = p_1^{e_{11}} p_2^{e_{12}} \cdots p_k^{e_{1k}}$$
$$\alpha_2 = p_1^{e_{21}} p_2^{e_{22}} \cdots p_k^{e_{2k}} \quad (5)$$
$$\cdots$$
$$\alpha_n = p_1^{e_{n1}} p_2^{e_{n2}} \cdots p_k^{e_{nk}}$$
$(1 \leqq i \leqq n), (1 \leqq j \leqq k), (0 \leqq e_{ij} \leqq 2)$

(5) (2)で計算したaを(6)式のようにk個の整数$x_1,x_2,\cdots,x_k$の和となるように分解し，素数$p_1,p_2,\cdots,p_k$と1対1対応させる．

$$a = x_1 + x_2 + \cdots x_k$$
$$p_i \Rightarrow x_i (1 \leqq i \leqq k) \quad (6)$$

(6) (4)で生成したe_{ij}と(5)で求めたx_iを利用し，(7)式によって，β_iを計算し第2成分とする．

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1k} \\ e_{21} & e_{22} & \cdots & e_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ e_{n1} & e_{n2} & \cdots & e_{nk} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} \quad (7)$$
$(1 \leqq i \leqq n), (1 \leqq j \leqq k), (0 \leqq e_{ij} \leqq 2)$

(7) (8)式を用いて，(2)で求めた b と秘密情報γを用いて第3成分Γを作成する．

$$\gamma^b \equiv \Gamma \pmod{s} \quad (8)$$

(8) (1)～(7)で求めた情報でn個の5つ組を作り，分散情報とする．

2.4 復元フェーズ

必要な分散情報の個数の下限である k 個以上の分散情報を利用して，秘密情報を復元する方法を以下で説明する．

(1) 集めた秘密情報の第 1 成分から，素数p_1，$p_2 \cdots p_k$を求める．

(2) (1)で求められた素数の和を計算し，第4成分mと等しくなるか判定する．等しくならなければ，まだ不足している素数があると判断される．この素数は(4)で定義される変数x_iと一対一対応するため，個数に不足が生じると，以降の処理が正しく行えない．したがって,分散情報の集合から秘密情報を復元することができない．

(3) (1)で求めた素数を用いて第1成分で割ってゆくことで,構成する指数部分$e_{ij}$$(1 \leqq i \leqq n), (1 \leqq j \leqq k)$を求める．

(4) 集めた分散情報の中からk個の第2成分を選択し，e_{ij}とk個の素数p_1，$p_2 \cdots p_k$に一対一対応する変数$x_1,x_2,\cdots,x_k$を用いて(9)式のk元連立一次方程式を立てる．このとき，(9)式の右辺の係数部のランクがkとならなければ，連立方程式は解けない．このため，ランクがkとなるように分散情報を選ばなければならない．

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_k \end{pmatrix} = \begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1k} \\ e_{21} & e_{22} & \cdots & e_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ e_{k1} & e_{k2} & \cdots & e_{kk} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} \quad (9)$$

(5) この連立方程式を解き，変数$x_1,x_2,\cdots,x_k$の解を求める．

(6) 連立方程式の解$x_1,x_2,\cdots,x_k$の和aを計算する．

(7) aと第3成分Γを用いて，(10)式のように秘密情報を復元する．

$$\Gamma^a \equiv \gamma \pmod{s} \quad (10)$$

これは(2)式の性質を利用して，(11)式のような処理を経て求められる式である．

$$\Gamma^a \equiv (\gamma^b)^a \equiv \gamma^{\phi(s)+1} \equiv \gamma \pmod{s} \quad (11)$$

3. まとめと今後の課題

本稿では，オイラーの公式を用いた一般型アクセス構造を持つ秘密分散法の実現アルゴリズムについて述べた．

今後の課題として，この方式を実際に実装・実験を行い評価することや，情報理論的な解析を行い，その安全性の検証や符号化率を求めることがあげられる．しかし，各分散情報が 5 つ組みであるため，直感的に提案方式は符号化効率が悪いことが考えられる．そのため，符号化効率を小さくする符号化法を同時に考える必要がある．

また，分散フェーズの(4)における整数e_{ij}の生成を乱数に依存していては，乱数の発生の状態により，分散情報からもとの秘密情報を復元できない可能性も考えられる．このため，整数e_{ij}決定するための効率的な方法を考える必要がある．

参考文献

[1]*Shamir,A.:How to Share a Secret, Communication of the ACM,Vol.*22,*No.*11,*pp.*612-613,1979.
[2]*Karnin,E.D.,Greene,J.W.andHellman,M.E.:On Secret Sharing Systems, IEEE Trans.Inf.Theory, Vol.IT-*29,*pp.*25-41,1983
[3]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. J*68 *A, No.*9, *pp.* 945-952,1985
[4]*K.Okada and K.Kurosawa*:*Lower bound on the size of shares of nonperfect secret sharing schemes, Advances in Crypology-ASIACRYPT'*94, *LNCS* 917,*Springer-Verlag,pp*34-41,1994
[5]六角晃子:オイラーの公式を用いた 3 つ組み暗号とその評価, 広島市立大学卒業論文, 2004