秘密分散法における準同型性を活用したシェアの二階層化

Tow-stratification of the shares utilizing homomorphism in the secret sharing scheme

倉上高史　藤吉正明　貴家仁志
Takashi Kurakami　Masaaki Fujiyoshi　Hitoshi Kiya

首都大学東京システムデザイン学部情報通信システム工学コース
Dept. of Information and Communication Systems Engineering, Tokyo Metropolitan University

1　はじめに

本稿では，秘密分散法の準同型性に基づく，秘密分散法の新しい応用を提案する．ネットワーク上で個人情報が取り扱われるにつれ，情報処理への個人情報保護技術の適用が急務となっている．平文を秘匿したまま演算することが可能な秘密計算が検討され，その代表的な方法である準同型暗号が広く研究されている [1][2]．特に，暗号化したままあらゆる情報処理が可能な完全準同型暗号も提案されている [2] が，計算量が大きいため，実用的でない．本稿では，(k,n) しきい値型の秘密分散法 [1] の加法に関する群準同型性による統計処理を暗号領域で行うことで，シェアの二階層化を行うことを提案する．

2　暗号領域での秘密分散法

暗号領域での秘密分散法 [3] は，(k,n) しきい値型で生成したシェアを，加法群準同型暗号で暗号化する手法である．加法群準同型暗号は，二つの平文をそれぞれ x,y とし，暗号化関数を E，復号化関数を D とすると，以下の性質を持つ公開鍵暗号である．

$$x + y = D(E(x) * E(y)) \tag{1}$$

また，暗号化されたシェアから暗号化された秘密情報を復元可能である．暗号化により，シェアと秘密情報を保護できるため，通常の (k,n) しきい値型よりもセキュアな秘密分散法となっている．この手法に基づき，統計情報と個別情報を，異なる階層でセキュアに運用可能な秘密計算方式を提案する．

3　提案法

秘密分散法の加法に関する準同型性から，秘密情報を扱うことなく統計情報を算出できる．準同型性は，$\mathbf{F}$ を $n \times k$ の vandermonde 行列として，s_i を秘密情報 $(1 \le i \le m)$，$\mathbf{a}_i$ を乱数行列とすると，以下の式で示される．

$$\sum_{i=1}^{m} \mathbf{F} \begin{pmatrix} s_i \\ a_{i,1} \\ \vdots \\ a_{i,k-1} \end{pmatrix} = \mathbf{F} \begin{pmatrix} s_1 + s_2 + \cdots + s_m \\ a_{1,1} + a_{2,1} + \cdots + a_{m,1} \\ \vdots \\ a_{1,k-1} + a_{2,k-1} + \cdots + a_{m,k-1} \end{pmatrix} \tag{2}$$

提案法では，秘密分散法のシェアの二階層化を行う．第一階層は各秘密情報にアクセス可能な n 個の通常のシェアで形成される階層である．第二階層は統計結果にアクセス可能な l $(k \le l \le n)$ 個のシェアで形成される階層であり，準同型性に基づき生成される．これは (k,l) しきい値型に相当する．シェアを二階層化することで，一つの秘密分散処理で扱う情報を二種類としている．以上を図 1 にまとめる．これにより，従来からのシェアの数による重要度の設定に加え，シェアの種類でも重要度を設定することができるようになり，運用の幅が広がることが期待される．

加法群準同型暗号と秘密分散法の加法に関する準同型性とを併用することで，セキュアな統計処理を行うことが可能となっている．

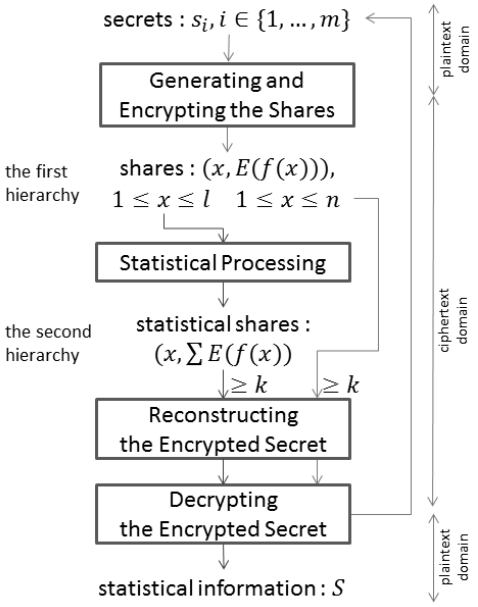

図 1　シェア二階層化秘密分散法のモデル図

4　おわりに

本稿では，秘密分散法の準同型性を用いて，シェアの二階層化を行った．二階層化により，統計情報と各秘密情報を同時に運用可能な秘密計算方式を提案した．また，暗号化秘密分散法にシェアの二層化を行うことで，統計処理をセキュアに行うことが可能となる．

参考文献

[1] A. Shamir, “How to share a secret,” Commun. ACM, vol.22, pp.612-613, Nov. 1979

[2] C. Gentry, “A fully homomorphic encryption scheme,” PhD thesis, Stanford University (2009)

[3] B. Zhao and E. Delp, “Secret Sharing in the Encrypted Domain,” Proceedings of the 46th IEEE ICC 2011, Kyoto, Japan, 5-9 Jun. 2011.