秘密分散法および視覚復号型秘密分散法の一般的構成法に関する研究

RA 岩本 貢
情報理工学系研究科 数理情報学専攻

概 要

重要な情報を安全に管理するためには，外部からの悪意のある攻撃や記憶装置の故障等によるデータの消失など，様々な障害に対してロバストなセキュリティを確保することが求められる．本研究では，情報漏洩，情報の破損や記憶装置の故障などに耐性をもつ秘密分散法および視覚復号型秘密分散法を一般的に構成する手法を確立することを目的とする．

1 はじめに

秘密情報の管理において，秘密情報の破損や記憶媒体の故障等の脅威に対する安全性を保証するためには秘密情報のコピーを複数作成する対策が考えられるが，コピーが多いと情報は漏洩しやすくなる．このように秘密情報の安全な管理は本来矛盾した要求を含んでいる．そこで，秘密情報を複数の分散情報に分散符号化し，符号化された複数の分散情報のうち，指定されたいくつかの分散情報 (有資格集合) を集めれば秘密情報が復元できるが，それ以外の分散情報 (禁止集合) を集めても秘密情報がまったく漏洩しない方式を考える．このような方式を秘密分散法 (Secret Sharing Scheme, SSS) と呼び，破損や故障の脅威と漏洩の脅威の双方の脅威に対してロバストな秘密情報管理が可能になる．例えば，n 個の分散情報のうち，任意の k 個を集めると秘密情報が復号できるが，任意の $k-1$ 個以下の分散情報からは秘密情報が復号できないように設計された (k,n) しきい値 SSS では，$n-k$ 個以下の分散情報の破損，$k-1$ 以下の分散情報の漏洩に対してロバストな安全性が保証される．さらに一般的に，有資格集合族と禁止集合族の組で定義される一般アクセス構造に対して SSS を構成することも出来る．

SSS はさらに，情報量的な安全性が保証されている．現在よく用いられる計算量的安全性をもつ暗号システムは，計算機の急速な性能向上や量子計算機の登場の可能性などにより，安全性に問題が生じる可能性が指摘されている．これに対して，情報量的安全性をもつ暗号システムは攻撃者に無限の計算能力を仮定しても安全なシステムであり，どのような攻撃者に対してもロバストな安全性を有している．また，視覚復号型秘密分散法 (Visual SSS, VSSS) は計算機がなくても視覚を用いて瞬時に復号可能な秘密分散法であり，計算機が使えない非常時においてもロバストに復号が行える特徴をもつ．

本研究では SSS，VSSS の構成方法の提案，また安全性の理論解析などを行ったので，次節以降で説明する．

2 整数計画法による最適な複数割り当て写像の構成

従来，(k,n) しきい値 SSS は任意の k,n に対し効率よく構成できることが知られている．しかし，一般アクセス構造をもつ SSS に対する符号化法は非常に符号化効率の悪いものしか知られていなかった．そこで本研究では，一般アクセス構造をもつ SSS に対し，符号化効率の良い符号化手法を提案した [1], [2].

分散情報全体の集合を $\boldsymbol{V}=\{V_1,V_2,\ldots,V_n\}$ とし，秘密情報 S に対する有資格集合族を $\mathcal{A}_{\mathsf{Q}}$，禁止集合族を $\mathcal{A}_{\mathsf{F}}$ とする．このとき，アクセス構造 $\Gamma=\{\mathcal{A}_{\mathsf{Q}},\mathcal{A}_{\mathsf{F}}\}$ に対し S を秘密情報とする (t,m) しきい値 SSS の分散情報を $\boldsymbol{W}=\{W_1,W_2,\ldots,W_m\}$ とする．伊藤らは式 (1)–(3) で定義される複数割り当て写像 $\alpha_\Gamma:\boldsymbol{V}\to 2^{\boldsymbol{W}}$ が構成できれば任意の一般アクセス構造に対し SSS が構成できることを示した．なお，$\boldsymbol{A}\subseteq\boldsymbol{V}$ に対して，$\alpha_\Gamma(\boldsymbol{A})=\bigcup_{V\in\boldsymbol{A}}\alpha_\Gamma(V)$ と定義している．

$$|\alpha_\Gamma(\boldsymbol{A})|\geq t \qquad \text{if } \boldsymbol{A}\in\mathcal{A}_{\mathsf{Q}} \tag{1}$$

$$|\alpha_\Gamma(\boldsymbol{A})|\leq t-1 \text{ if } \boldsymbol{A}\in\mathcal{A}_{\mathsf{F}} \tag{2}$$

$$\alpha_\Gamma(\boldsymbol{V})=\boldsymbol{W} \tag{3}$$

さらに伊藤らは，任意の一般アクセス構造に対して複数割り当て写像を実現する方法として cumulative map と呼ばれる方式を提案している．しかし，cumulative map は，アクセス構造 Γ が (k,n) しきい値法に近いと符号化効率が悪くなることが指摘されている．ここで符号化効率は，分散情報 V_i の符号化レートの平均値または最悪値で定義され，複数割り

当て写像 α_Γ を用いる場合はそれぞれ，

$$\tilde{\rho} = \frac{1}{n}\sum_{i=1}^{n} |\alpha_\Gamma(V_i)|, \quad \tilde{\rho} = \max_{1\le i\le n} |\alpha_\Gamma(V_i)| \quad (4)$$

と書くことが出来る．以下では，平均レート $\tilde{\rho}$ を最小化する複数割り当て写像を整数計画写像を用いて構成する．そのために，複数割り当て写像 α_Γ に対して 2^n 個存在する $\boldsymbol{W}$ の部分集合 $\boldsymbol{X}_{[k]_2^n}$，$k = 0, 1, 2, \ldots, N$ を次式で定義する．

$$\boldsymbol{X}_{[k]_2^n} = \left[\bigcap_{i:[k]_2^{n,i}=1} \alpha_\Gamma(V_i)\right] \cap \left[\bigcap_{i:[k]_2^{n,i}=0} \overline{\alpha_\Gamma(V_i)}\right] \quad (5)$$

ここで $N = 2^n - 1$，$[k]_2^n$ は非負整数 k を n ビットの 2 進数表示したもの，$[k]_2^{n,i}$ は $[k]_2^n$ の下から i ビット目を指す．例えば，$[5]_2^4 = 0101$，$[5]_2^{4,1} = [5]_2^{4,3} = 1$ である．式 (5) において例えば $n = 3$ の場合は，$\boldsymbol{X}_{101} = \alpha_\Gamma(V_1) \cap \overline{\alpha_\Gamma(V_2)} \cap \alpha_\Gamma(V_3)$ となる．容易に分かるように，$\boldsymbol{X}_k$，$k = 0, 1, \ldots, N$ は次を満たす．

$$\boldsymbol{X}_0 = \emptyset \quad (6)$$

$$\boldsymbol{X}_k \cap \boldsymbol{X}_{k'} = \emptyset \ \text{ if } k \neq k' \quad (7)$$

$$\alpha_\Gamma(V_i) = \bigcup_{k:[k]_2^{n,i}=1} \boldsymbol{X}_k \quad (8)$$

$$\alpha_\Gamma(\boldsymbol{A}) = \bigcup_{k=1}^{N} \boldsymbol{X}_k - \bigcup_{\substack{k:[k]_2^{n,i}=0 \\ \text{for all } V_i\in\boldsymbol{A}}} \boldsymbol{X}_k \quad (9)$$

$$\alpha_\Gamma(\boldsymbol{V}) = \bigcup_{k=1}^{N} \boldsymbol{X}_k \quad (10)$$

式 (6) から，$\boldsymbol{X}_0$ は考える必要がないので，以下では $\boldsymbol{X}_k$, $k = 1, 2, \ldots, N$ のみを考える．また，式 (7), (9) から $|\boldsymbol{X}_k| = x_k$ と置くと

$$|\alpha_\Gamma(\boldsymbol{A})| = \sum_{k=1}^{N} x_k - \sum_{\substack{k:[k]_2^{n,i}=0 \\ \text{for all } V_i\in\boldsymbol{A}}} x_k \quad (11)$$

が成り立つ．ここで，$\boldsymbol{x} = [x_1, x_2, \ldots, x_N]$ とし，ベクトル $\boldsymbol{a}(\boldsymbol{A}) = [a(\boldsymbol{A})_1, a(\boldsymbol{A})_2, \ldots, a(\boldsymbol{A})_N] \in \{0,1\}^N$ を $\boldsymbol{A} = \{V_{i_1}, V_{i_2}, \ldots, V_{i_u}\}$ に対して

$$a(\boldsymbol{A})_k = \begin{cases} 0 & \text{if } [k]_2^{n,i_1} = \cdots = [k]_2^{n,i_u} = 0 \\ 1 & \text{otherwise.} \end{cases} \quad (12)$$

と定義すると式 (11) の右辺は $\boldsymbol{a}(\boldsymbol{A}) \cdot \boldsymbol{x}$ と書ける．最後に，$[k]_2^n$ のハミング重みを h_k と定義し，$\boldsymbol{h} = [h_1, h_2, \ldots, h_N] \in \mathbb{Z}^N$ とすると，式 (8) から，

$$\sum_{i=1}^{n} |\alpha_\Gamma(V_i)| = \sum_{i=1}^{n} \sum_{k:[k]_2^{n,i}=1} x_k = \sum_{k=1}^{N} h_k x_k = \boldsymbol{h}\cdot\boldsymbol{x} \quad (13)$$

が成り立つ．以上から，複数割り当て写像の条件式 (1), (2) に式 (13) を加えて平均レート $\tilde{\rho}$ を最小化する複数割り当て写像，$\tilde{\alpha}$ を与える整数計画問題が次のように定式化できる．なお，ほぼ同様の手法で最悪レートを最適化することも可能である．

$$\begin{array}{lll} \text{minimize} & \boldsymbol{h}\cdot\boldsymbol{x} & \\ \text{subject to} & \boldsymbol{a}(\boldsymbol{A})\cdot\boldsymbol{x} \ge t & \text{for all } \ \boldsymbol{A}\in\mathcal{A}_{\mathsf{Q}} \\ & \boldsymbol{a}(\boldsymbol{A})\cdot\boldsymbol{x} \le t-1 & \text{for all } \ \boldsymbol{A}\in\mathcal{A}_{\mathsf{F}} \\ & \boldsymbol{x} \ge \boldsymbol{0} & \end{array}$$

以上のように構成した整数計画法によって得られた最適な複数割り当て写像が cumulative map より符号化効率が数倍良くなるアクセス構造が存在することを確認した．

3 複数の画像を符号化可能な視覚復号型秘密分散法

VSSS に関しては，複数の画像を秘密画像とする手法ついて考察した．従来の複数画像を符号化可能な VSSS は白黒 2 値画像に対するものしか知られておらず，さらにそのうちいくつかの VSSS の定義では，復号された秘密画像が他の秘密画像に関する情報を洩らしてしまうような場合があった．そこで我々は，一般アクセス構造に対して画像を複数隠すことのできる VSSS に対して，復号された画像が他の画像に関する情報を全く洩らさないように厳密な定義を与え，そのような定義を満足する VSSS の構成法を与えた．この VSSS の定義はカラー濃淡画像を扱うことができ，従来のほとんどの VSSS の定義を特殊な場合として含んでいる．

本研究は主に 2002 年度に行われたが，2003 年に国際会議で発表し [3]，学術雑誌に掲載された [4].

参考文献

[1] 岩本貢，山本博資，小川博久: (k, n) しきい値法と整数計画法と整数計画法による秘密分散法の一般的構成法，信学技報，vol.103, no.61, (2003).

[2] Iwamoto, M., Yamamoto, H., and Ogawa. H.: Optimal Multiple Assignments Based on Integer Programming in Secret Sharing Schemes with General Access Structures, submitted to Journal of Cryptology, (2003).

[3] Iwamoto, M. and Yamamoto, H.: Visual Secret Sharing Schemes for Plural Secret Images, Proc. of IEEE ISIT 2003, p.283, (2003).

[4] Iwamoto M. and Yamamoto, H.: A Construction Method of Visual Secret Sharing Schemes for Plural Secret Images, IEICE Trans. on Fundamentals, vol.E86.A, no.10, pp.2577–2588, (2003).