様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２０　日現在

機関番号：　３２６６５
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００１９２

研究課題名（和文）情報比の制約を考慮した一般アクセス構造を実現する秘密分散法の具体的な構成法

研究課題名（英文）General Secret Sharing Schemes with Restriction on Information Rates for Specified Participants

研究代表者

栃窪　孝也（TOCHIKUBO, Kouya）

日本大学・生産工学部・准教授

研究者番号：６０４４００３８

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：本研究では、すべての管理者の中から指定したグループに割り当てられる分散情報を削減可能な一般アクセス構造を実現する秘密分散法を提案した。さらに、これまでに提案されている階層構造のアクセス構造に対して最適な秘密分散法を一般アセス構造に対して適用できるように改良した手法を提案した。一般に、階層構造になっている組織において、上位の階層に属する管理者は多くの秘密を復元する権限のあるグループ(アクセス集合)に属することになるので管理する分散情報の数が膨大になってしまうが、本研究の提案手法により、上位の階層に属する管理者の管理する分散情報の数を削減することが可能である。

研究成果の概要（英文）：We have proposed a new secret sharing scheme realizing general access structures. The proposed scheme can reduce the number of shares distributed to one specified participant. We can apply the proposed scheme to the same access structure recursively. That is, the proposed scheme can reduce the number of shares distributed to another participant once again by applying the proposed scheme recursively.
Next, we have proposed new secret sharing schemes realizing general access structures. This scheme can reduce the number of shares distributed to specified participants. Thus, we can reduce the number of shares distributed to any participant who belongs to the selected subset.
Furthermore, we have proposed a new secret sharing scheme realizing general access structures. In the proposed scheme, shares are generated by Tassa's hierarchical threshold scheme instead of Shamir's threshold scheme. Thus, the proposed scheme can reduce the number of shares distributed to each participant.

研究分野：　情報セキュリティ

キーワード：　秘密分散　しきい値法　アクセス構造

１．研究開始当初の背景

秘密分散法とは、暗号で利用する鍵などの秘密情報の安全な保管で利用され、情報の盗難対策と紛失対策の両方に有効な情報化社会においてニーズの高い技術であるといえる。一般に、紛失の対策として情報のバックアップ(コピー)を作成することは効果的であるが、この場合、その分だけ盗難のリスクが高くなる。

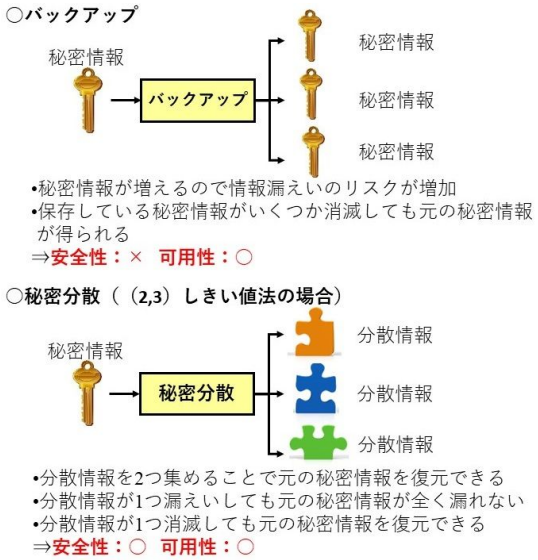

図１ バックアップと秘密分散の違い

一方、秘密分散法の基本原理であるしきい値秘密分散法((k, n)しきい値法)では、秘密情報を n 個の分散情報に分割し、得られた分散情報を n 人の管理者が管理する。秘密情報を復元する場合は、n 人の管理者の中から任意の k 人が集まり、管理している分散情報を用いて元の秘密情報を計算する。この手法は、任意の k 個の分散情報を集めれば元の秘密情報が復元できるが、k-1 個の分散情報からでは元の秘密情報に関する情報がまったく得られないということ(完全性)が情報理論的に証明されている。このため、分散情報の一部が漏えいしても元の秘密情報は安全であり、また、分散情報の一部を紛失しても元の秘密情報を復元することが可能な情報の管理を実現することができ、内部犯罪防止や災害時のデータ管理にも大変有効な技術として注目を集めている(図 1)。

しかしながら、秘密分散法には秘密の分散・復元処理の演算量と保存する分散情報のサイズに関して以下のような問題がある。

(1) 一般的な(k, n)しきい値法では、秘密情報の分散・復元の処理において k-1 次多項式の演算が必要となり、暗号化鍵等の少量のデータの場合は秘密情報の分散・復元の計算量は問題にならないが、その計算量から、大量のデータの場合には適用することが難しい。このため、秘密の分散・復元を高速に実行可能なしきい値秘密分散法に関する研究も多数行われている。このような秘密の分散・復元を高速に実行可能なしきい値秘密分散法により、安全なクラウドストレージ等が実現できる。

(2) 秘密情報を復元する権限を持つ管理者のグループ(アクセス集合)の集まり(アクセス構造)という観点でみると、(k, n)しきい値法のアクセス構造は、n 人の分散情報の管理者のうち、任意の k 人以上のグループの集合となり、非常に限定的な場合のみを実現していることになる。そこで、アクセス構造を限定しない秘密分散法(一般アクセス構造を実現する秘密分散法)に関する研究が数多く行なわれているが、どの手法も管理者に数多くの分散情報を割当てることで実現しており、元の秘密情報と管理者が管理する分散情報との比(情報比)に着目すると、(k, n)しきい値法のように方式が最適な場合の情報比が 1 であるのに対し、これまで知られている手法の情報比は非常に小さくなり、効率的ではなかった。現代社会では階層構造の組織が多数存在し、また、部門の責任者は多くの情報を閲覧・管理する必要がある。しかしながら、これまでの秘密分散法の研究では、特定の管理者の情報比の制約などは考慮されておらず、このため、複雑なアクセス構造の場合は実用化されていなかった。

２．研究の目的

すべての分散情報の管理者に対し高い情報比を達成する秘密分散法の研究も非常に重要な研究テーマであるが、階層構造になっている組織において、上位の階層に属する分散情報の管理者は、多くのアクセス集合に属することになり、結果として管理する分散情報が多くなり情報比が小さくなる場合が多い。そこで、本研究では下記の 3 点を研究の目的とした。

(1) 情報比の制約を考慮した秘密分散法の分散情報の割当て方法の提案

各アクセス構造に対する実現可能な情報比の上界は、管理者数の少ない特別なアクセス構造のいくつかでは明らかになっているが、任意のアクセス構造に対する実現可能な情報比の上界は未解決である。そこで本研究でもアクセス構造の情報比の上界を求める問題と同様に、管理者数の少ない実用的な個別のアクセス構造を当初のターゲットとして情報比の制約を考慮した分散情報の割当て方法を検討する。

(2) 情報比の制約を考慮した秘密分散法の高速な分散・復元方法の提案

前述したように、秘密分散法には、秘

密の分散・復元処理の演算量と保存する分散情報のサイズという 2 つの問題点がある。(1)により、分散情報のサイズの問題点を解決しても、実用的な方式であるためには、分散・復元処理を高速に行う必要がある。このため、情報比の制約を考慮した場合の分散・復元処理の演算量を評価するとともに、高速な分散・復元方法を提案する。

(3) 情報比の制約を考慮した一般アクセス構造を実現する秘密分散法の検討

任意のアクセス構造に対して、(1)で得られた個別のアクセス構造に対する結果を一般アクセス構造に適用し、分散情報の管理者の情報比に制約を課した場合の秘密分散法の一般的な構成法を提案し、さらに、その性能を評価する。

３．研究の方法

現在の秘密分散法を使った製品・サービスのほとんどは、実現できるアクセス構造が限定されたしきい値秘密分散法を適用したものであり、このため、利用範囲は限定されている。しかしながら、企業のような階層構造の組織の場合、2 人の部長が管理する分散情報を集めれば元の秘密情報が復元でき、4 人の課長が管理する分散情報を集めれば秘密情報が復元できるといったしきい値秘密分散法では実現できないさまざまな状況が考えられる。さらに、階層構造になっている組織において、上位の階層に属する分散情報の管理者は、多くのアクセス集合に属することになり、結果として管理する分散情報が多くなり情報比が小さくなってしまう。したがって、分散情報の管理者ごとの情報比の制約までも考慮する秘密分散法は実社会におけるニーズが非常に高いと考えられる。そこで、本研究では、達成可能な情報比の上界が示されている管理者の少ないアクセス構造[引用文献①，②]を対象とし、符号語のコストを最小にする情報圧縮の手法[引用文献 ③]を応用することで情報比の制約を考慮した割当て方法を検討する。

また、一般に、任意のアクセス構造を対象とした方式とある特別なアクセスでのみ非常に効率のよい方式は異なる。このため、本研究では、任意のアクセス構造を対象としたものだけではなく、実社会で利用される可能性が高い特定のアクセス構造に対して効率のよい方式の両方を扱う。(k，n)しきい値法のアクセス構造の場合には、高速に秘密情報の分散・復元できるしきい値秘密分散法[引用文献 ④，⑤]により、高速な分散・復元処理を実現可能である。本研究では、(k，n)しきい値法のアクセス構造の場合に秘密情報の分散・復元処理を高速にできる手法を応用し、情報比に制約がある場合でも高速な分散・復元処理を実現可能な方式を検討すると共に、その効率を評価する。

秘密分散法のアクセス構造は管理者の集合の集合族であり、集合族の元の個数を評価する際に用いる組合せ論的な手法は秘密分散アルゴリズムを検討する上でも有効である。そこで、得られた結果を基に、従来の一般アクセス構造を実現可能な秘密分散法を一般化することで、組合せ論的な考察から情報比の制約を満足する効率のよい秘密分散法を導き出す。さらに、本研究では、一般アクセス構造の場合の秘密情報の分散・復元処理の効率を評価する。

４．研究成果

本研究では、実社会で利用される可能性が高い特定のアクセス構造に対して効率のよい方式だけではなく、任意のアクセス構造を対象とした方式の両方を扱う。一般に、階層構造になっている組織において、上位の階層に属する管理者は多くの秘密を復元する権限のあるグループ(アクセス集合)に属することになる。本研究では、秘密を復元する権限のあるグループに制約のない一般アクセス構造を実現する手法を対象としている。一般アクセス構造を実現する秘密分散法は、極小アクセス構造、または、極大非アクセス構造に基づいている。

本研究では、指定した管理者に割当てられる分散情報の数を削減可能な極小アクセス構造に基づく一般アクセス構造を実現する秘密分散法を提案した。そして、管理者数が 4 人以下のすべてのアクセス構造に対して提案方式を適用して分散情報の管理者ごとの分散情報の割当て数などを明らかにし、提案手法の有効性を検証した。さらに、この手法を再帰的に適用可能な手法を提案し、管理者数が 5 人のすべての場合である 180 通りのアクセス構造における分散情報の管理者ごとの割当て数の最大値や管理者全体の割り当て数の平均値などを明らかにし、提案手法の有効性を検証した。また、1887 年に伊藤、斎藤、西関が分散情報の管理者に複数の分散情報割り当てる複数割り当て法や 1988 年に Benaloh と Leichter による単調回路の理論を応用した手法などの従来手法[引用文献⑥，⑦]についても 180 通りのアクセス構造すべてに適用して提案手法の有効性を検証した。提案手法を再帰的に適用した場合、180 通りのアクセス構造すべてにおいて、伊藤、斎藤、西関の手法および Benaloh と Leichter の手法よりも割当て数の最大値が小さくなるか等しいことが分かった。なお、この手法では、分散情報は(k，n)しきい値法により求めるため、高速に秘密情報の分散・復元できるしきい値秘密分散法[引用文献④，⑤]により、高速な分散・復元処理を実現可能である。

さらに、秘密分散法には、上述した情報比に関する課題だけではなく、秘密情報の分散および復元処理の演算量という課題もある。

(k, n)しきい値法のアクセス構造の場合に秘密情報の分散・復元処理を高速にできる手法は提案されているが、本研究では、管理者数が4人以下のすべてのアクセス構造の中で(k, n)しきい値法で実現できないアクセス構造のすべてに対して排他的論理和演算のみで高速に秘密情報の分散および復元が可能な秘密分散法を提案した。

さらに、すべての管理者の中から指定したグループに割り当てられる分散情報を削減可能な極大非アクセス集合に基づく一般アクセス構造を実現する秘密分散法を提案した。一般に、階層構造になっている組織において、上位の階層に属する管理者は多くの秘密を復元する権限のあるグループ(アクセス集合)に属することになるので管理する分散情報の数が膨大になってしまうが、この提案手法により、上位の階層に属する管理者の管理する分散情報の数を削減することが可能である。この手法も分散情報は(k, n)しきい値法により求めるため、高速な分散・復元処理が実現可能である。

さらに、これまでに提案されている階層構造のアクセス構造に対して最適な秘密分散法である Tassa の階層型秘密分散法[引用文献 ⑧]を一般アセス構造に対して適用できるように改良した極大非アクセス集合に基づく手法を提案した。この手法においても、上位の階層に属する管理者の管理する分散情報の数を削減することが可能である。

<引用文献>

① D. R. Stinson, Decomposition constructions for secret sharing schemes, IEEE Trans. Inform. Theory, vol. IT-40, pp. 118-125, 1994
② M. V. Dijk, On the information rate of perfect secret sharing schemes, Designs, Codes and Cryptography, vol.6, no.2, pp. 143-169(1995)
③ 岩田 賢一, 森井 昌克, 植松 友彦, コスト最小を目的とする情報源圧縮について, 信学技報 IT, vol.96, no.311, pp.13-18(1996)
④ 藤井吉弘, 栃窪孝也, 保坂範和, 多田美奈子, 加藤岳久, 排他的論理和を用いた(k, n)しきい値法の構成法, 信学技報, vol. 107, no. 44, ISEC2007-5, pp. 31-38(2007)
⑤ 保坂 範和, 栃窪 孝也, 藤井 吉弘, 多田 美奈子, 加藤 岳久, 2 値行列に基づく(2, n)しきい値秘密分散法, 2007 年暗号と情報セキュリティシンポジウム予稿集, 2D1-4(2007)
⑥ M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing general access structure, Proc. IEEE Globecom '87, pp.99-102(1987)
⑦ J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, Proc. of CRYPTO '88, pp.27-35(1988)
⑧ T. Tassa, Hierarchical threshold secret sharing, Journal of Cryptology Vol. 20, pp.237-264(2007)

５．主な発表論文等

〔雑誌論文〕（計１件）

① K. Tochikubo, New general secret sharing scheme based on unauthorized subsets: improvement of information rates for specified participants, Journal of Information Processing, vol. 24, No.5, pp.772-780 査読有 (2016)
DOI:10.2197/ipsjjip.24.772

〔学会発表〕（計６件）

① U. Itoh, K. Tochikubo, Recursive general secret sharing scheme based on authorized subsets, Proc. of 2018 7th International Conference on Information and Electronics Engineering (ICIEE 2018) (2018)
② K. Tochikubo, Multiple assignment secret sharing scheme using hierarchical threshold scheme, Proc. of The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017) (2017)
③ 佐藤 真之, 栃窪 孝也, 排他的論理和演算を用いた秘密分散法に関する一考察, 電子情報通信学会 2017 総合大会, A-7-9 (2017)
④ 伊藤 詩子, 栃窪 孝也, 極小アクセス集合に基づく一般アクセス構造を実現する秘密分散法の情報比の評価, 情報処理学会 第 79 回全国大会, 6W-06 (2017)
⑤ K. Tochikubo, Improvement of information rates for specified participants in general secret sharing schemes, Proc. of 14th International Conference on Privacy, Security and Trust (PST2016) (2016)
⑥ 伊藤 詩子, 栃窪 孝也, 極小アクセス集合に基づく秘密分散法の情報比, 電子情報通信学会 2016 総合大会, A-7-18 (2016)

６．研究組織

(1)研究代表者

栃窪 孝也（TOCHIKUBO, Kouya）
日本大学・生産工学部・准教授
研究者番号：６０４４００３８