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

令和　４ 年　 ５ 月 １９ 日現在

機関番号：３２６６５
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ１１３０３

研究課題名（和文）属性を考慮した階層型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）Explicit Constructions of General Secret Sharing Schemes Using Hierarchical Threshold Scheme

研究代表者
栃窪　孝也（TOCHIKUBO, Kouya）

日本大学・生産工学部・教授

研究者番号：６０４４００３８

交付決定額（研究期間全体）：（直接経費）　　2,500,000円

研究成果の概要（和文）：本研究では、(k, n)しきい値法に基づき分散情報を取得していた従来の一般アクセス構造を実現する秘密分散法を階層型秘密分散法に基づき分散情報を取得するように改良して管理者が保持する分散情報の数、および、分散情報を求める際に利用する秘密分散法の回数を削減可能な手法を提案した。提案手法では、分散情報を本来の使い方とは異なり、管理者ではなく管理者のグループ(属性)に対応させることで、安全性と効率を両立している。また、秘密分散法を画像に応用した視覚復号型秘密分散法のシェア画像にアクセス構造の階層構造の概念を拡張してシェア画像にも情報を埋め込むことが可能な拡張視覚復号型秘密分散法を提案した。

研究成果の学術的意義や社会的意義
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。暗号技術を利用する機器やシステムにおいて、その安全性を保つためには暗号化・復号で利用する鍵の安全な管理が不可欠であり、鍵の管理が必要な機器やシステムすべてが秘密分散の適用範囲であるといえる。本研究で得られた成果により、実社会においてニーズの高いアクセス構造を従来の手法よりも効率よく実現可能となり、暗号化・復号で利用する鍵の管理が必要な機器やシステムへの秘密分散法のさらなる実用化に大きく貢献できる。

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 secret sharing schemes to obtain shares by using Tassa's hierarchical threshold scheme instead of Shamir's threshold scheme. Thus, the proposed scheme is more efficient from the viewpoint of the number of secret sharing schemes to obtain shares. Furthermore, we have proposed extended visual secret sharing schemes for QR code. Our proposed schemes can embed the secret QR codes in the share images as well as the recovered image.

研究分野：情報セキュリティ

キーワード：秘密分散　アクセス構造

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

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。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 人の管理者で管理する。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。

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、Shamir が提案した(k, n)しきい値法[引用文献 ①]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。また、近年、Tassa は、(k, n)しきい値法のアクセス構造よりも広いクラスのアクセス構造を最適に実現可能な階層型秘密分散法を提案している [引用文献 ②]。管理者が 4 人以下の場合のアクセス構造は 18 通り存在する [引用文献 ③]。Shamir の(k, n)しきい値法は 18 通り中 6 通りしか実現することができなく、Tassa の階層型秘密分散法は 18 通り中 12 通りしか実現することができない。

一方、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)に関する研究も数多く行なわれている。一般アクセス構造を実現する秘密分散法は、18 通りの管理者が 4 人以下のすべてのアクセス構造を実現することができるが、どの手法も管理者に数多くの分散情報を割り当てることで実現している。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、Shamir の(k, n)しきい値法や Tassa の階層型秘密分散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、これまで提案されている一般アクセス構造を実現す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。このため、秘密分散法の実社会での利用は限定的なものであった。

２．研究の目的

管理者が 4 人以下の場合のアクセス構造は 18 通りであるが、管理者が 5 人になるとアクセス構造は 180 通りに増える [引用文献 ④]。もちろん、180 通りのアクセス構造に現在提案されている一般アクセス構造を実現する秘密分散法を適用することはできるが、その効率はまだまだ改善の余地がある。また、管理者数が多い場合、アクセス構造の総数やその情報比の上限については明らかになっていないのが現状である。任意のアクセス構造に対して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の 1 つであるが、階層構造になっている組織等での秘密分散の利用を考えた場合、Tassa の階層型秘密分散法のように、特定のアクセス構造では高い情報比を達成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。

しかしながら、企業のような階層構造の組織の場合、3 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、また、5 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アクセス構造は Tassa の階層型秘密分散法で実現可能であるが、単純な階層構造ではなく、部長 1 人とその部下の課長 3 名、または、同じ部に所属する課長 3 名と異なる部の部長 2 名では秘密を復元できるといったより現実的なアクセス構造を考えると Tassa の階層型秘密分散法では実現することができない。

本研究では、単純な階層構造ではなく実社会においてより現実的なアクセス構造を効率よく実現する秘密分散法の開発を目指す。

３．研究の方法

本研究では、しきい値法や従来の階層型秘密分散法では実現できないアクセス構造すべてを対象にするのではなく、実社会でニーズが高いと考えられる属性までも考慮した階層構造のアクセス構造に限定して効率のよい秘密分散法を求めることが目標である。そこで、本研究では以下の手順で研究を進める。

(1)管理者数の少ないアクセス構造の評価・分類

これまでに、18 通りの管理者が 4 人以下の場合のアクセス構造のすべてを評価し、Tassa の階層型秘密分散法でも実現できないアクセス構造が多数存在することを明らかにしている。本研究では、管理者が 5 人の 180 通りのアクセス構造を当初のターゲットとして、階層型のアクセス構造として表せるかどうか、また、管理者の属性を考慮した場合にうまく適合するかどうかを評価・分類し、その結果を管理者数をさらに増やしたアクセス構造に適用する。

(2)属性を考慮したアクセス構造を効率よく実現可能な秘密分散法の検討

Tassa の階層型秘密分散法の手法や一般アクセス構造を実現する秘密分散法での手法を拡張することで、属性を考慮したアクセス構造を効率よく実現可能な秘密分散法の具体的な構成法を提案し、さらに、その効率を評価する。なお、提案する手法は、効率がよいことも重要であるが、従来の秘密分散法のように秘密を復元する権限のないグループ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が情報理論的に証明されているものでなければならない。

４．研究成果

当初のターゲットである管理者が 5 人の 180 通りのすべてのアクセス構造に対して 2003 年に提案された岩本らの(k, n)しきい値法と整数計画法に基づく秘密分散法[引用文献 ⑤]を実装して、最適となるアクセス集合の数は、平均割り当て数で効率を評価する場合は 31 通り、最大割り当て数で効率を評価する場合は 14 通りであることを明らかにした。また、岩本らの(k, n)しきい値法と整数計画法に基づく秘密分散法に Stinson の提案した分割構成法を組み合わせることで、平均割り当て数で効率を評価する場合は 70 通り、最大割り当て数で効率を評価する場合は 79 通りのアクセス集合で岩本らの手法を単体で適用するより効率が良いことを明らかにした。また、具体的な分散情報の割り当てアルゴリズムが明らかになっている一般アクセス構造を実現する従来の秘密分散法では、管理者に割り当てる分散情報は(k, n)しきい値法に基づいて生成されている。一方、本研究で得られた提案手法では、分散情報は 2 階層の Tassa の秘密分散法により分散情報を生成することで、管理者が保持する分散情報の数を削減している。Tassa の階層型秘密分散法は、分散情報の管理者に割り当てる分散情報を生成する方式であり、分散情報には管理者が対応する。一方、提案手法では、分散情報を本来の使い方とは異なり、管理者ではなく管理者のグループ(属性)に対応させることで安全性と効率を両立している。さらに、2003 年に提案された岩本らのしきい値型のアクセス構造(GTAS)に基づく複数割り当て法に加えて、2018 年に提案された江利口らの 2 つのアクセス構造(CCAS、DCAS)に基づく複数割り当て法[引用文献 ⑥]を管理者が 5 人の 180 通りのすべてのアクセス構造に適用して分散情報の管理者に割り当てられる情報のサイズを評価し、岩本らの手法を拡張した江利口らの手法も同様に管理者が 5 人の 180 通りのすべてのアクセス構造に適用して効率を評価した。そして、属性を考慮したアクセス構造を効率よく実現可能な秘密分散法の具体的な構成法を明らかにするために管理者 4 人のアクセス構造から構成可能な管理者 5 人のアクセス構造を明らかにした。

なお、本研究では、秘密分散法を画像に応用した視覚復号型秘密分散法のシェア画像にアクセス構造の階層構造の概念を拡張してシェア画像にも情報を埋め込むことが可能な拡張視覚復号型秘密分散法も提案している。視覚復号型秘密分散法とは、秘密分散法を画像に応用した手法であり、1994 年に Naor と Shamir が提案している[引用文献 ⑦]。視覚復号型秘密分散法では、秘密にしたい画像を複数枚のシェアと呼ばれる画像に分散処理し、そのシェア画像単体からでは元の秘密の画像はわからないが、あらかじめ定められたしきい値以上のシェア画像を重ね合わせることにより、元の秘密の画像を復元することのできる秘密情報の分散管理方式である。従来手法には、読みだすことのできる情報量に制限があるものやシェア画像が白いピクセルと黒いピクセルがランダムに配置された砂嵐画像になってしまうという問題があった。一方、提案の(2, 2)しきい値拡張視覚復号型秘密分散法の場合、2 枚のシェア画像を重ねることにより、秘密の QR コードを復元することができるとともに、2 枚のシェア画像も砂嵐画像ではなく、それぞれ秘密の QR コードとは異なる別の QR コードを埋め込むことができる。さらに、これを拡張して(2, 3)しきい値拡張視覚復号型秘密分散法を QR コードに適用する手法も提案した。提案手法は、QR コードの誤り訂正能力を用いないため復元画像で読みだすことのできる情報量に制限がないのが特徴である。

<引用文献>

① A. Shamir, How to share a secret, Comm. ACM, Vol. 22, No. 11, pp. 612-613, 1979
② T. Tassa, Hierarchical threshold secret sharing, Journal of Cryptology Vol. 20, pp. 237-264, 2007
③ D. R. Stinson, Cryptography: theory and practice 3rd edition, CRC Press, 2005
④ Wen-Ai Jackson and Keith M. Marin, Perfect secret sharing schemes on five participants, Designs, Codes and Cryptography, Vol. 9, Issue 3, pp. 267-286, 1996
⑤ 岩本 貢, 山本 博資, 小川 博久, (k, n)しきい値法と整数計画法による秘密分散法の一般的構成法, 電子情報通信学会技術研究報告 ISEC, 情報セキュリティ Vol. 103 No. 61, pp. 63-70, 2003
⑥ 江利口 礼央, 國廣 昇, 岩本 貢, いくつかの理想的な秘密分散法を用いた最適な複数割り当て法, The 41st Symposium on Information Theory and its Applications (SITA2018), 2018
⑦ M. Naor and A. Shamir, Visual cryptography, LNCS, vol. 950, pp. 1-12, 1995

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 大川直也 栃窪孝也	４．巻 62
２．論文標題 QRコードへ適用可能な拡張視覚復号型秘密分散法	５．発行年 2021年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1476-1486
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kouya Tochikubo	４．巻 E102-A
２．論文標題 General Secret Sharing Schemes Using Hierarchical Threshold Scheme	５．発行年 2019年
３．雑誌名 IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1037-1047
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 岡﨑太介　栃窪孝也
２．発表標題 EASとして構成可能な管理者が5人以下のアクセス構造に関する考察
３．学会等名 第54回日本大学生産工学部学術講演会
４．発表年 2021年

１．発表者名 岡﨑太介　栃窪孝也
２．発表標題 管理者が5人の場合の管理者を追加可能な秘密分散法に関する一考察
３．学会等名 2021年電子情報通信学会 総合大会
４．発表年 2021年

１．発表者名
大川直也　栃窪 孝也

２．発表標題
拡張視覚復号型秘密分散法のQRコードへの適用

３．学会等名
情報処理学会第コンピュータセキュリティ研究発(CSEC), 2019-CSEC-87(8)

４．発表年
2019年

１．発表者名
Kouya Tochikubo

２．発表標題
New general secret sharing scheme using hierarchical threshold scheme: improvement of information rates for specified participants

３．学会等名
6th International Conference on Information Systems Security and Privacy (ICISSP 2020)（国際学会）

４．発表年
2020年

１．発表者名
新間祐太郎　栃窪孝也

２．発表標題
5人の管理者の場合の複数割り当て法による情報比の評価

３．学会等名
電子情報通信学会情報通信システムセキュリティ研究会(ICSS), ICSS2019-70

４．発表年
2020年

１．発表者名
大川直也　栃窪 孝也

２．発表標題
(2,3)しきい値拡張視覚復号型秘密分散法のQRコードへの適用

３．学会等名
電子情報通信学会情報セキュリティ研究会(ISEC), ISEC2019-98

４．発表年
2020年

１．発表者名 新間祐太郎 栃窪孝也
２．発表標題 5人の管理者の場合の整数計画法と分割構成法による秘密分散法
３．学会等名 情報処理学会 第81回全国大会
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関