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　５ 年　 ６ 月 ２７ 日現在

機関番号：３２７２１
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ１１３０６

研究課題名（和文）情報のライフサイクルを考慮した秘密分散法の研究

研究課題名（英文）Research on Secret Sharing Scheme Considering Lifecycle of Information

研究代表者
土井　洋（DOI, Hiroshi）

情報セキュリティ大学院大学・その他の研究科・教授

研究者番号：７０３３８６５６

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）：秘密情報の安全な保管は情報の盗難対策や紛失対策に見られるように情報化社会において必要である．階層的秘密分散法を用いることで秘密情報の盗難や紛失への耐性に加え，秘密情報の消去容易性をも実現できる．本研究では，階層的秘密分散法などの研究を行い，XOR演算を多用する方式，IDA (Information Dispersal Algorithm) を利用する方式など，複数の高速な方式を提案した．

研究成果の学術的意義や社会的意義
情報のライフサイクルを考慮すると，生成された情報の安全な保管(盗難対策や紛失対策を含む)に加え，消去容易性をも実現できることが望ましい．秘密分散法を用いると，前者(安全な保管)は達成できるが，情報の消去に要するコストは大きくなる．本研究では，情報の安全な保管と確実な消去を実現できる高速な階層的秘密分散法を提案した．本研究成果を利用することで，生成された情報の安全な保管および確実な消去を実現できることになる．

研究成果の概要（英文）：In the information society, there is necessity for a secure information storage system that is resistant to theft and loss. Using the hierarchical secret sharing scheme, in addition to improve the resistance to theft and loss of confidential information, it is possible to erase confidential information easily. In this research, we proposed efficient hierarchical secret sharing schemes (XOR-based scheme, and IDA (Information Dispersal Algorithm)-based scheme).

研究分野：情報セキュリティ

キーワード：階層的秘密分散法　秘密分散法　暗号理論

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年，インターネットを利用した様々なサービスが提供されている．例えば記憶領域を提供することを主とするサービスを考えた場合，生成された情報のライフサイクル(活用，消去)という観点から解決すべき問題は少なくない．特に秘密情報の安全な保管は情報の盗難対策や紛失対策に見られるように情報化社会においてニーズが高い．(k,n)秘密分散法[1][2]を用いて秘密情報から n 個のシェアを生成する場合，このうち k 個以上のシェアを用いることで情報を復元でき，k 個未満のシェアからは情報を復元できないという性質を得ることができる．このように秘密分散法を用いると，秘密情報から n 個のシェアを生成し保管することで，秘密情報の盗難や紛失への耐性は向上する．しかし，秘密情報の消去には多数(n-k+1 個)のシェアを消去する必要がある．ここで階層的秘密分散法を用いると，秘密情報の削除が一部のシェア(情報の復元の際に不可欠な必須参加者に割り当てられたシェア)の削除で保証される．

階層的秘密分散法に関しては，2000 年代前半の，Tassa による安全性などの定式化と Birkhoff 補間を用いた方式に関する研究が良く知られている[3]．Tassa の手法ではシェア生成時にシェア生成多項式の微分を利用している．階層構造によっては 2 階微分が必要であるが，高速化が見込める標数 2 の有限体上では 2 階微分の結果は常に 0 となる．このため Tassa の手法による標数 2 の有限体上の階層的秘密分散法の実現はできない．我々は標数 2 の有限体上でも適用可能な微分に相当する関数(n-th order reduction)を導入し，Birkhoff 補間が適用可能であることを示した[4]．あわせて性能評価も行い，高速化も達成可能であることを示した．

高速な秘密分散法に関しては，IDA (Information Dispersal Algorithm)を利用する方法[5]や XOR 演算を多用する方法[6]などが知られているが，秘密情報の消去容易性を実現できる階層的秘密分散法への拡張について研究が必要であった．

２．研究の目的

本研究においては，秘密分散法の高速化，特に情報のライフサイクルを考慮した高速な階層的秘密分散法の提案などを目的とする．

Tassa の手法を，高速化が期待できる標数 2 の有限体上に拡張することについては，1.で述べたように，一定の結果が得られている．本研究では，高速化が期待できる IDA (Information Dispersal Algorithm)を利用する方法や，XOR 演算を多用する方法などについて，階層的秘密分散法への拡張についての研究を行う．これらの研究については(階層的ではない)構成法は知られている．必要に応じて背景にある数学的性質についても研究を行い，秘密分散法の拡張(階層的秘密分散法を含む)や利便性向上などについて研究を進める．

なお，現実的に利用可能性が高いものは({1,3},n)階層的秘密分散法である．これは 2 階層にレベル付けされた n 個のシェアのうち，最上位レベルの(必須参加者の)シェアが少なくとも 1 つ，第 2 番目以上のレベルのシェアが少なくとも 3 つあれば復元できるアクセス構造を意味する．最上位レベルのシェアを組織の少人数の責任者が管理し，第 2 位レベルのシェアを組織内の業務担当者が管理する場合などが考えられる．この場合，情報を復元するためには責任者の関与が不可欠となり，情報を消去するためには(限られた少人数の)責任者のシェアのみを全て削除すればよい．

本研究では，例えば({1,3},n)階層的秘密分散法のように，階層構造を限定した場合の高速化と利便性向上などの両立についても視野に入れる．

３．研究の方法

初年度は，IDA(Information Dispersal Algorithm)を利用する方法や，XOR 演算を多用することによる高速な階層的秘密分散法などの研究を集中的に行う．理論的な考察を進めるとともに，構成法を具体的に示しつつ，一定の環境での性能評価も行い，高速化が達成されているか確認する．

次年度以降は，前年度に得た成果を基に，性能改善，アクセス構造拡張を含む様々な機能拡張を行う．また，高速化が実現できる(階層的ではない)秘密分散法について，その背景にある数学的性質についても研究を行う．これらの数学的性質などを利用して，現実的に利用可能性が高い({1,3},n)階層的秘密分散法のように，階層構造を限定した場合の利便性向上などに関する検討なども行う．

これらの成果については国内外の研究会や論文誌等で発表する．

４．研究成果

平成 30 年度(初年度)は，IDA(Information Dispersal Algorithm)を利用する階層的秘密分散法や，XOR 演算を多用する階層的秘密分散法の研究を行い，その成果を国際会議 Information Security and Cryptology (ICISC 2018)および International Workshop on Security (IWSEC 2018) で発表した．とくに後者は，n が小さな場合において処理性能が極めて高い．

令和元年度は，平成 30 年度(初年度)の研究成果である XOR 演算を多用する階層的秘密分散法

の研究に関連して，XOR 演算を多用する(k,n)秘密分散法の理論的な分析を行った．分析の結果，シェアの生成や復元を行う行列を，巡回行列を成分とする Vandermonde 行列とみなすことで，奇素数を法とする(k,n)秘密分散法との関係を明らかにすることができた．秘密分散法の応用に関する研究の多くは奇素数を法とするものであり，それらと XOR 演算を多用するものとの関係を示せたことになる．その成果を国内で開催されたコンピュータセキュリティシンポジウム CSS2019 で発表した．

令和 2 年度は，令和元年度までの研究成果である XOR 演算を多用する(k,n)秘密分散法の理論的な分析に関する研究をさらに推進し，その成果を Journal of Information Processing (JIP) で発表した．また，高速化以外の研究として，ランプ型秘密分散法に関するものや，秘密分散法を利用した応用に関する研究も推進した．

なお，階層的秘密分散法においては，識別子の割り当て方によっては復元できない場合が生じうる．具体的には，k や n の値と識別子の割り当て方が復元可能性に影響する．高速化を実現可能な XOR 演算を多用する階層的秘密分散法においても，やはり識別子の割り当て方によっては復元できないという現象は生じる．研究期間後半において，令和元年度と 2 年度の成果などを用いて復元可能性についての理論研究も進めた．その結果，シェアの生成や復元を行う行列を，巡回行列を成分とする Vandermonde 行列とみなすことができることから利用できる数学的性質を用いて，(n や k が小さな場合の)分析を行うことができた．そして，巡回行列の階数に関する既存の定理などを用いて，識別子の割り当て方によらず復元可能な場合，および識別子の割り当て方によって復元不可能な場合の理論的な説明に成功した．これらについては，k=3 の場合(現実的に利用可能性が高い({1,3},n)階層的秘密分散法も含まれる)に識別子の割り当て方によらず復元できる方式(今まで提案してきた方式の改良)を提案し，2023 年暗号と情報セキュリティシンポジウム SCIS2023 で発表した．

参考文献

[1] Shamir, “How to share a secret,” Comm. ACM, vol.22, No.11, pp.612-613 (1979).
[2] Blakley, “Safeguarding cryptographic keys,” AFIPS, vol.48, pp.313-317 (1979).
[3] Tassa, “Hierarchical Threshold Secret Sharing,” Journal of Cryptology, vol.20 (2), pp.237-264 (2007).
[4] Shima, Doi, “A Hierarchical Secret Sharing Scheme over Finite Fields of Characteristic 2,” Journal of Information Processing, vol.25, pp.875-883 (2017).
[5] Krawczyk, “Secret sharing made short,” CRYPTO 1993, LNCS773, pp.136-146 (1994).
[6] Kurihara, Kiyomoto, Fukushima, Tanaka, “On a Fast (k,n)-Threshold Secret Sharing Scheme,” IEICE Trans. Fundamentals, E91-A(9), pp.2365-2378 (2008).

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　3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 Koji Shima, Hiroshi Doi	４．巻 29
２．論文標題 New Proof Techniques Using the Properties of Circulant Matrices for XOR-based (k, n) Threshold Secret Sharing Schemes	５．発行年 2021年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 266-274
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.29.266	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 島幸司，土井洋	４．巻 2021
２．論文標題 改良版XORベース階層的秘密分散法についての考察	５．発行年 2021年
３．雑誌名 2021年暗号と情報セキュリティシンポジウム論文集	６．最初と最後の頁 1-8
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 無
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 島幸司，土井洋	４．巻 2019
２．論文標題 XORベース秘密分散法の新しい証明法	５．発行年 2019年
３．雑誌名 コンピュータセキュリティシンポジウム2019論文集	６．最初と最後の頁 839-846
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 無
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 Shima Koji、Doi Hiroshi	４．巻 11049
２．論文標題 XOR-Based Hierarchical Secret Sharing Scheme	５．発行年 2018年
３．雑誌名 Proc. of IWSEC 2018, Lecture Notes in Computer Science	６．最初と最後の頁 206～223
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-97916-8_14	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 Shima Koji、Doi Hiroshi	4．巻 11396
2．論文標題 A Hierarchical Secret Sharing Scheme Based on Information Dispersal Techniques	5．発行年 2019年
3．雑誌名 Proc. of ICISC 2018, Lecture Notes in Computer Science	6．最初と最後の頁 217～232
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-12146-4_14	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 醍醐康夫，柴山綸太郎，土井洋	4．巻 2019-CSEC-84
2．論文標題 ランプ型秘密分散法のシェアサイズ変換方式	5．発行年 2019年
3．雑誌名 研究報告コンピュータセキュリティ（CSEC）	6．最初と最後の頁 1 - 8
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 無
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 島幸司，土井洋	4．巻 2023
2．論文標題 階層的秘密分散法と参加者の識別子割り当て問題の考察	5．発行年 2023年
3．雑誌名 2023年暗号と情報セキュリティシンポジウム論文集	6．最初と最後の頁 1-8
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 無
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1件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 橋本真，土井洋
2．発表標題 タクシーデータの保護と利活用に関する考察
3．学会等名 情報処理学会 第84回全国大会
4．発表年 2022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
研究協力者	島　幸司 (Shima Koji)		
研究協力者	醍醐　康夫 (Daigo Yasuo)		
研究協力者	柴山　綸太郎 (Shibayama Rintaro)		
研究協力者	橋本　真 (Hashimoto Shin)		

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