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　６ 年　 ６ 月 ２０ 日現在

機関番号：８２６３６
研究種目：基盤研究(C)（一般）
研究期間：2019～2023
課題番号：１９Ｋ１１８３５

研究課題名（和文）セキュリティレベルを更新可能とするアクセス構造を備えた最適秘密分散に関する研究

研究課題名（英文）Optimal Secret Sharing for Proactive Access Structures

研究代表者
吉田　真紀（Yoshida, Maki）

国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所・主任研究員

研究者番号：５０３３５３８７

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：従来研究における秘密分散のセキュリティレベルの定義と，暗号応用先の要件を元に，セキュリティレベルの更新を可能にするアクセス構造を備えた秘密分散の定義を検討した．従来の鍵管理を想定した定義では単調構造（モノトーン）だが，本研究では単調なアクセス構造以外も対象にすることで，鍵管理における多様かつ柔軟な被害の封じ込めを可能にし，暗号応用先の幅を広げた．そして従来および新たな暗号応用先における秘密分散の定義との互換性の確認し，重要特性（演算可能性・正しさ検証）と暗号応用に不可欠な特性の担保とシェアサイズの最小化が両立可能であることを明らかにした．

研究成果の学術的意義や社会的意義
本研究の学術的意義は，暗号応用に不可欠な各種特性の担保とシェアサイズの最小化の達成である．社会的意義は，それにより秘密鍵を復元することなく分散したままで電子署名や秘密計算など処理が可能になり，秘密鍵が晒されるリスクを削減したことである．

研究成果の概要（英文）：Based on the previous definition of secret sharing and the major requirements of cryptographic applications, we extended the definition so that an access structure allows updating of the security level including not only the monotonous structures but also non-monotone access structures. This expands the range of cryptographic applications. Expanded. We also confirmed the feasibility of optimality in conventional and new cryptographic applications while ensuring important properties (correctness and verifiability) and essential properties for cryptographic applications.

研究分野：情報セキュリティ

キーワード：秘密分散　最適　アクセス構造

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

ビットコインなどの暗号通貨の爆発的な普及により暗号の秘密鍵そのものが金銭価値をもち，2014 年 2 月マウントゴックスからの約 470 億円相当のビットコイン流出や，2018 年 1 月コインチェックからの約 580 億円相当の NEM 流出など，鍵流出・紛失が深刻な問題になっている．日々高度化・巧妙化する攻撃に対して，システムへの侵入を完全に防止することは不可能なため，被害を封じ込める(局所化・無効化する) 対策が極めて重要になる．

被害を局所化・無効化する代表的なセキュリティ技術として，秘密分散が精力的に研究開発されている．秘密分散では，秘密分散では，元の情報を複数のシェアに分散して秘匿でき，一部のシェアが欠損しても残りのシェアから元の情報を復元できる．シェアの流出や欠損の状況に応じてセキュリティレベルの更新を可能にすることで，さらなる攻撃の被害を封じ込めることができる．

秘密分散においてセキュリティレベルは秘密情報の各種エントロピー，確率分布，残り候補数で定義されており，更新ではそれらの細かい調整が不可欠である．しかし，秘密分散のセキュリティレベルの更新に関する従来研究では，シェアからの復元則を定めるアクセス構造はしきい値型とランプ型に限られ，全情報が一度に入手されるか，入手量の細かい調整ができない．その結果，秘密情報の復元に要するシェア数は更新できるが，復元に至るまでのセキュリティレベルの更新ができない．さらに，暗号通貨における電子署名などの暗号応用に不可欠な，シェア上の準同型性，加法性，乗法性の担保が考慮されておらず，かつ大量の鍵情報を扱う実応用に不可欠なシェアの最小化が未解決である．

２．研究の目的

秘密分散において，セキュリティレベルの更新を可能とし，暗号応用において不可欠となるシェア上の準同型性，加法性，乗法性を，更新後も担保するアクセス構造を実現しつつ，実応用において不可欠なシェアサイズの最小化を達成する最適な秘密分散を明らかにすることである．

３．研究の方法

本研究の目的を達成するため，以下について明らかにする．

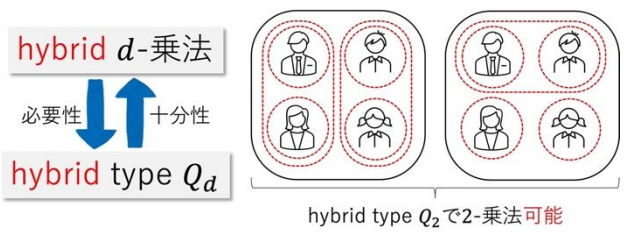
(a) セキュリティレベルの更新を可能にするアクセス構造を備えた秘密分散の定義
(b) 暗号応用に不可欠なシェア上の各種特性を担保する更新
(c) 実応用に不可欠なシェアサイズの最小化を達成する最適な秘密分散

４．研究成果

2019 年度は，従来研究における秘密分散のセキュリティレベルの定義と，暗号応用先の要件を元に，セキュリティレベルの更新を可能にするアクセス構造を備えた秘密分散の定義を検討した．従来の鍵管理を想定した定義では単調構造（モノトーン）だが，本研究では単調なアクセス構造以外も対象にすることで，鍵管理における多様かつ柔軟な被害の封じ込めを可能にし，暗号応用先の幅を広げた．そして，従来および新たな暗号応用における秘密分散の定義との互換性の確認として，（１）まず定義から求まるシェアと乱数のサイズの下界を導出し，（２）さらに暗号応用先であるシェアした秘密の上での演算と正しさ検証の実現可能性を証明した．

2020 年度は，暗号応用として，従来の鍵管理を想定した単調構造（モノトーン）と，秘密計算や通信，条件付き情報開示を想定した一般構造について，重要特性（演算可能性・正しさ検証）の担保と最適化を達成した．これにより，鍵管理における多様かつ効率的な被害の封じ込めを可能にし，暗号応用先の効率を向上させた．

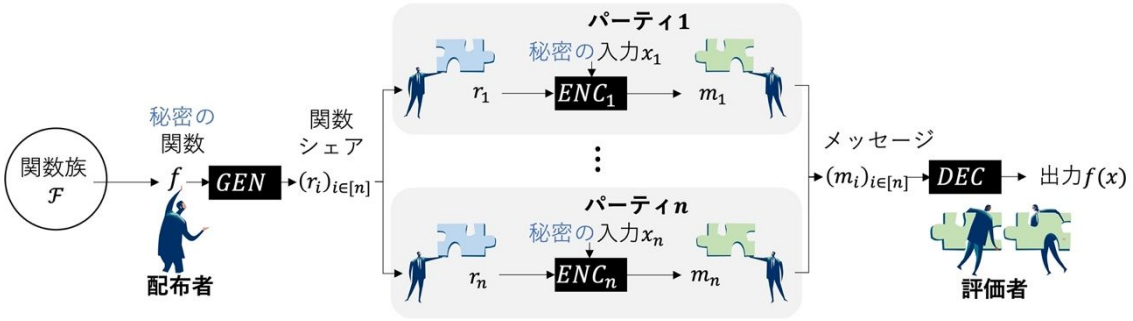
2021 年度は，更新において暗号応用に不可欠な特性の担保とシェアサイズの最小化が両立可能であることを明らかにするため以下を実施した．（１）更新によって異なるアクセス構造が混在する最も一般的な状況において特性が担保されるための必要条件を導出し，（２）その必要条件が十分条件でもあることを証明するためシェアサイズが最小となる構成法を提案した（右図ではアクセス構造が最も簡明になる$d=2$を例示）．



2022 年度は，更新において暗号応用に不可欠な特性の担保とシェアサイズの最小化が両立可能であることを明らかにするために，前年度から対象クラスを拡張して以下を実施した．（１）更新によって異なるアクセス構造が混在する最も一般的な状況において特性が担保されるための必要十分条件を導出し，（２）その必要条件が十分条件でもあることを証明するため具体的な構成法を提案した．

2023 年度は，前年度の拡張した定義に基づき以下を実施した．（１）これまでに最適化されていない暗号機能の関数クラス（下図における関数族は任意）について通信複雑性の下限を改善し，

（２）これまでに最適化されていない暗号機能の関数クラスについて通信複雑性の上限を改善し，最適な構成法を提案した．



５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　5件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Maki Yoshida	４．巻 1
２．論文標題 On the Communication Complexity of Private Function Sharing and Computation	５．発行年 2023年
３．雑誌名 2023 IEEE International Symposium on Information Theory (ISIT2023)	６．最初と最後の頁 258-263
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 Maki Yoshida	４．巻 1
２．論文標題 Hybrid Multiplicative Non-perfect Secret Sharing	５．発行年 2022年
３．雑誌名 2022 IEEE International Symposium on Information Theory (ISIT2022)	６．最初と最後の頁 649-653
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISIT50566.2022.9834640	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 Satoshi Obana, Maki Yoshida	４．巻 II
２．論文標題 Efficient Constructions of Non-interactive Secure Multiparty Computation from Pairwise Independent Hashing	５．発行年 2020年
３．雑誌名 Proceedings of the 17th International Joint Conference on e-Business and Telecommunications	６．最初と最後の頁 322-329
掲載論文のDOI（デジタルオブジェクト識別子） 10.5220/0009819203220329	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 Maki Yoshida, Satoshi Obana	４．巻 -
２．論文標題 Compact Verifiably Multiplicative Secret Sharing	５．発行年 2020年
３．雑誌名 Proceedings of the International Symposium on Information Theory and Its Applications 2020	６．最初と最後の頁 437-441
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.C03-4	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 河内 亮周， 吉田 真紀	４．巻 -
２．論文標題 秘密同時メッセージと条件付き秘密開示に対する乱数長下界	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予稿集	６．最初と最後の頁 --
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 Maki Yoshida, Satoshi Obana	４．巻 65(5)
２．論文標題 Verifiably Multiplicative Secret Sharing	５．発行年 2019年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 3233-3245
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2018.2886262	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 吉田真紀，尾花賢	４．巻 2F3-2
２．論文標題 検証可能な乗法秘密分散の効率向上	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 （CSS2019）予稿集	６．最初と最後の頁 1-5
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4件（うち招待講演　1件／うち国際学会　0件）

１．発表者名 吉田 真紀
２．発表標題 非対話型秘密計算の通信量
３．学会等名 2023年度冬のLAシンポジウム
４．発表年 2024年

１．発表者名
河内 亮周，吉田 真紀

２．発表標題
秘密同時通信と条件付き秘密開示に対する乱数複雑度

３．学会等名
2021年度冬のLAシンポジウム

４．発表年
2022年

１．発表者名
吉田真紀

２．発表標題
秘密分散の最適性について

３．学会等名
第20回情報科学技術フォーラム(FIT2021)トップカンファレンスセッション（招待講演）

４．発表年
2021年

１．発表者名
河内亮周，吉田真紀

２．発表標題
Private Simultaneous Messages および Conditional Disclosure of Secrets に関する情報理論的下界

３．学会等名
2019年度冬のLAシンポジウム

４．発表年
2020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