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　 ５ 月 １０ 日現在

機関番号：２４５０６
研究種目：挑戦的研究（萌芽）
研究期間：2020～2022
課題番号：２０Ｋ２１７９５

研究課題名（和文）持続可能な社会のための任意計算によるプルーフオブワークの実現

研究課題名（英文）Realizing Proof-of-Work through arbitrary computation for a sustainable society

研究代表者
五十部　孝典（Takanori, Isobe）

兵庫県立大学・情報科学研究科・准教授

研究者番号：３０７８５４６５

交付決定額（研究期間全体）：（直接経費）　　4,900,000円

研究成果の概要（和文）：ハッシュ関数SHA-3とEven-Mansor暗号をベースとした方式を作成したSHA-3はスポンジ構造と呼ばれる構成をしており、パラメータを適切に選択することで、メモリを利用する計算が最適である問題に変換可能であることを示した。また、同様のモチベーションでEven-Mansor暗号をベースにした方式も提案した。Even-Mansor暗号もメモリを大量に利用する方が効率よく問題を解くことが可能である。SHA-3をベースにした方式は情報処理学会の論文誌に招待論文として掲載されるなど学術的に高い評価を得た。最後に、本研究の一番の目的である意味のあるプルーフオブワークを前述の技術をベースに作成した。

研究成果の学術的意義や社会的意義
本研究では，プルーフオブワークを任意の演算により実現する方法の開発をした．具体的には任意の計算をプルーフオブワーク用の問題へ変化する方法に取り組んだ．これを実現することで，現在コンセンサス毎に計算する必要のある意味のないハッシュ演算を，意味のある計算に膨大な計算リソースを使うことが可能になる．結果として，ブロックチェーンがただの非中央集権コンセンサスのためのもおのだけではなく，マイニングを分散コンピューティングプラットフォームとしても用いることが可能になり，持続可能な社会へとつながる．

研究成果の概要（英文）：The hash function SHA-3 and a method based on the Even-Mansor cipher have been developed. SHA-3, which adopts a structure called a sponge construction, demonstrated that by appropriately choosing parameters, problems that are optimal for memory-utilizing calculations can be transformed. Similarly, a method based on the Even-Mansor cipher was proposed, motivated by the same concept. The Even-Mansor cipher also allows for efficient problem-solving when a large amount of memory is utilized. The method based on SHA-3 received high academic recognition, including being published as an invited paper in the Journal of the Information Processing Society. Finally, the ultimate goal of this research is to create a meaningful Proof-of-Work based on the aforementioned techniques.

研究分野：暗号

キーワード：Proof of Work　SHA-3　Even-Mansour

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景
ブロックチェーンは，信頼できる第三者なしにコンセンサスが可能である画期的な技術であり，仮想通過以外にもスマートコントラクト等のアプリケーションがあり，今後ますます広がりを見せる．ブロックチェーンでは，プルーフオブワークと呼ばれるコンセンサスアルゴリズムを基盤技術として用いている．プルーフオブワークでは，膨大な計算量を要する問題を初めて解いた人を承認者とすることで非中央集権でのコンセンサスを実現している．その技術の根幹を担うのがハッシュ関数やデジタル署名等の暗号技術である．問題を解く作業をマイニングと呼び，ビットコインでは特定の出力になるハッシュ関数の入力を求めるという意味のない問題をプルーフオブワークとして用いている．2019 年 9 月現在では，一回のコンセンサスに 270 - 280 程度の膨大な計算量のマイニングを要し，ビットコインの場合は約 15 分毎に承認する必要があるため，この意味のない計算に地球上の多くの計算リソースが使われ，その膨大な消費電力は環境問題にもなっている．

２．研究の目的
本研究では，プルーフオブワークを任意の演算により実現する方法の開発を目指す．具体的には任意の計算をプルーフオブワーク用の問題へ変化する方法に取り組む．これが実現すれば，現在コンセンサス毎に計算する必要のある意味のないハッシュ演算を，例えば新薬開発のための解析計算や地震や気象のシミュレーション等の人類の発展のための重要な計算に膨大な計算リソースを使うことが可能になる．結果として，ブロックチェーンがただの非中央集権コンセンサスのためのもおのだけではなく，マイニングを分散コンピューティングプラットフォームとしても用いることが可能になり，持続可能な社会へとつながる．

３．研究の方法
プルーフオブワークで用いられている問題は以下の性質を満たす必要がある．
1．専門ハードウェアでの演算の効率化が困難
2．演算結果の正しさをだれでも簡単（非常に少ない計算量で）に検証可能

本研究では，任意の演算を上記の性質を満たす問題に変換することが技術的な挑戦になる．1 に関しては，マイニング用の問題を大量のメモリを用いる計算（メモリーハード計算)にすることで，ASIC 等の専門ハードウェアを作った場合のアドバンテージを軽減するアプローチが有効である．しかしながら，任意の意味のある問題自体を，メモリーハード計算にすることは難しいため，本研究では，任意の計算にメモリーハード計算をプラグインする方法をとる．例えば対象となる問題の答えをメモリーハード計算の入力とし，その演算結果をプルーフオブワークの答えとする手法が有効であると考える．さらに，提案手法は，毎回対象とする問題を変えるスキームを構成することで，専門ハードウェアの作成は困難にする．

2 に関しては，対象の問題を正しく計算したかを第三者が少ない計算量で検証できる必要がある．これを実現する技術としては，Verifiable computation という技術が知られている．しかしながらこの技術は，公開鍵暗号をベースとしているため，演算結果の正しさを証明する Proof を作成するのに膨大な計算量がかかり，問題を解くこと以外の計算が支配的になる．本研究では，効率的に計算の正しさを証明する技術の開発を行う．具体的には共通鍵暗号の要素技術をベースに Verifiable computation を構成するアプローチをとる．共通鍵暗号は基本的に，論理演算と小さなテーブルで実装可能であり，べき乗演算の必要な公開鍵暗号と比較して数百倍から数千倍高速である．仮に共通鍵暗号単独での実現が難しい場合は，既存の公開鍵暗号ベースの Verifiable computation と共通鍵暗号と組み合わせるアプローチや，ターゲット問題を細かく分割し階層的に Verifiable computation を行う方法を用いることにより実現する．

４．研究成果
メモリハード暗号として Galaxy[1]と呼ばれるアルゴリズムを作成した。Galaxy では、ストリーム暗号をベースにテーブルを生成し、そのテーブルをベースに演算を行う。つまり演算には、テーブルが必須であり、テーブルサイズをアプリケーションに応じて設定することで、暗号演算を特定のメモリサイズ以上を持つデバイスでしか実行不可能にすることが可能である。つまり、Proof of Work をこの演算ベースにすることで、特定のデバイスにバインディングすることが可能である。さらに、メモリ参照演算はハードウェアでの高速化のメリットが小さく専門ハードウェアのアドバンテージがなくなるメリットがあり、１の目的を達成可能なアルゴリズムである。暗号関数としても既存のメモリハード暗号と比較しても２倍以上の速度を達成している。さらにこのメモリハード暗号のプルーフオブワーク以外の拡張として、Leakage resilient システム Virtual Vault の設計を行った[2].本スキームでは、鍵の情報を大きなテーブルに格納すること

で、鍵とそれと等価な情報を攻撃者が入手するためには、膨大なデータをサーバ上から取得する必要があり、現実的に攻撃者からのデータ取得を不可能にする方式である。

さらに、ハッシュ関数 SHA-3 と Even-Mansor 暗号をベースとした方式を作成した。既存のプルーフオブワークでは、ハッシュ関数 SHA-2 の原像復元問題をベースに問題を作成していたが、この問題自体はメモリを利用しないため、ASIC での高速化が容易である。この問題を解決するため、別のハッシュ関数である SHA-3 を元にプルーフオブワークを設計した[3,7]。SHA-3 はスポンジ構造と呼ばれる構成をしており、パラメータを適切に選択することで、メモリを利用する計算が最適である問題に変換可能であることを示した。また、同様のモチベーションで Even-Mansor 暗号をベースにした方式も提案した[4,8]。Even-Mansor 暗号もメモリを大量に利用する方が効率よく問題を解くことが可能である。SHA-3 をベースにした方式は CSS 2020 学生論文賞を受賞し、情報処理学会の論文誌に招待論文として掲載されるなど学術的に高い評価を得た。

最後に、本研究の一番の目的である意味のあるプルーフオブワークを前述の技術をベースに作成した。具体的には、特定の意味のある問題から PoW を設計した[5,6,9]。意味のある問題としては、「遺伝的アルゴリズムをベースにした構成」をターゲットとした。遺伝的アルゴリズムは巡回セールスマン問題等の問題に使われており、 世の中で非常にニーズのあるアルゴリズムであるため、この問題を Proof of Work とすることで、意味のある計算を行うこと自体が Proof of Work になる。技術的 には、PoW では特定の計算量以上が解くのに必要であることを理論的に保証する必要がある。その問題を解決し、計算量の下限を保証する方法として Bitcoin 等に 用いられているハッシュ関数の原像復元問題と組み合わせたアルゴリズムを開発した。これにより、必ず特定の計算量がかかることを理論的に保証可能である。

〔雑誌論文〕（計 6 件 ）

1. Yuji Koike, Kosei Sakamoto, Takuya Hayashi and Takanori Isobe, "Galaxy: A Family of Stream-Cipher-Based Space-Hard Ciphers" , Australasian Conference on Information Security and Privacy (ACISP) 2020, Lecture Note in Computer Science, Part 1, vol. 12248, pp. 142-159, Springer, 2020
2. Yuji Koike, Takuya Hayashi, Jun Kurihara and Takanori Isobe, "Virtual Vault : A Practical Leakage Resilient Scheme Using Space-Hard Ciphers", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, Vol.E104-A, no.01, pp. 182-189, 2021.
3. Takaki Asanuma and Takanori Isobe, "A Proof of Work based on Preimage Problem of Variants of SHA-3 with ASIC Resistance", Journal of Information Processing, vol. 30, pp.75-83, 2021
4. Takaki Asanuma and Takanori Isobe, "A Proof of Work based on Key Recovery Problem of Cascade Block Ciphers with ASIC Resistance", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, Vol.E105-D,No.2,pp. 248-255, 2022.
5. Takaki Asanuma and Takanori Isobe, "mPoW: How to Make Proof of Work Meaningful", IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, 2023 .
6. Takaki Asanuma and Takanori Isobe, "Even-Mansour Space-hard Cipher: White-box Cryptography Cipher Meets Physically Unclonable Function", Journal of Information Processing, 2023.

〔学会発表〕（計 3 件)

7. 浅沼 岳樹，五十部 孝典 ，"SHA-3 の原像復元問題をベースにした ASIC 耐性のある Proof of Work"，コンピュータセキュリティシンポジウム（CSS） 2020（CSS2020 学生論文賞）.
8. 浅沼 岳樹，五十部 孝典 ，"Cascade なブロック暗号をベースにした ASIC 耐性のある Proof of Work"，2021 年 暗号と情報セキュリティシンポジウム(SCIS 2021) ，2021 年 1 月 .
9. 浅沼 岳樹，五十部 孝典，"mPoW: 意味のある計算による Proof of Work"，コンピュータセキュリティシンポジウム（CSS） 2021

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4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 Asanuma Takaki、Isobe Takanori	４．巻 30
２．論文標題 A Proof of Work based on Preimage Problem of Variants of SHA-3 with ASIC Resistance	５．発行年 2022年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 75～83
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.30.75	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 Asanuma Takaki、Isobe Takanori	４．巻 Vol.E105-D
２．論文標題 A Proof of Work based on Key Recovery Problem of Cascade Block Ciphers with ASIC Resistance	５．発行年 2022年
３．雑誌名 IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences	６．最初と最後の頁 not fixed
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 KOIKE Yuji、HAYASHI Takuya、KURIHARA Jun、ISOBE Takanori	４．巻 E104.A
２．論文標題 Virtual Vault: A Practical Leakage Resilient Scheme Using Space-Hard Ciphers	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 182～189
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020CIP0026	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 Koike Yuji、Sakamoto Kosei、Hayashi Takuya、Isobe Takanori	４．巻 1
２．論文標題 Galaxy: A Family of Stream-Cipher-Based Space-Hard Ciphers	５．発行年 2020年
３．雑誌名 Australasian Conference on Information Security and Privacy	６．最初と最後の頁 142～159
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-55304-3_8	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4件（うち招待講演　1件／うち国際学会　1件）

１．発表者名
浅沼 岳樹，五十部 孝典，

２．発表標題
mPoW: 意味のある計算によるProof of Work

３．学会等名
コンピュータセキュリティシンポジウム（CSS） 2021

４．発表年
2021年

１．発表者名
Asanuma Takaki、Isobe Takanori

２．発表標題
A Proof of Work based on Preimage Problem of Variants of SHA-3 with ASIC Resistance

３．学会等名
IWSEC 2021（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
浅沼 岳樹，五十部 孝典

２．発表標題
SHA-3の原像復元問題をベースにしたASIC耐性のあるProof of Work

３．学会等名
コンピュータセキュリティシンポジウム（CSS） 2020

４．発表年
2020年

１．発表者名
浅沼 岳樹，五十部 孝典

２．発表標題
Cascadeなブロック暗号をベースにしたASIC耐性のあるProof of Work

３．学会等名
2021年 暗号と情報セキュリティシンポジウム(SCIS 2021)

４．発表年
2021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