様式VI

博士学位論文調査報告書

論 文 題 目

A Study of Non-Interactive Zero-Knowledge Proof Systems in a Black-Box Framework
（非対話ゼロ知識証明のブラックボックス構成に関する研究）

申請者氏名

山下　恭佑

最 終 学 歴　　平成　２７年　３月
京都大学大学院情報学研究科 数理工学専攻 修士課程　修了
令和　３年　３月
京都大学大学院情報学研究科 社会情報学専攻 博士後期課程
研究指導認定見込

学 識 確 認　　令和　　年　　月　　日（論文博士のみ）

論文調査委員　京都大学大学院情報学研究科
（調査委員長）　教　授　神田 崇行

論文調査委員　京都大学大学院情報学研究科
教　授　吉川 正俊

論文調査委員　京都大学大学院情報学研究科
教　授　岡部 寿男

（ 続紙 1 ）

京都大学	博士（情報学）	氏名	山下　恭佑
論文題目	A Study of Non-Interactive Zero-Knowledge Proof Systems in a Black-Box Framework （非対話ゼロ知識証明のブラックボックス構成に関する研究）		

（論文内容の要旨）

非対話証明とは、秘密情報を保持している証明者が任意の検証者に一方的にデータを送るだけでその秘密情報がある公開された関係を満たすこと（すなわちある公開情報が特定の言語に属すること）を納得させる技術である。本論文は特に、関係式を満たすこと以外には秘密に関する情報を一切漏洩しない非対話ゼロ知識証明（Non-Interactive Zero-Knowledge Proof System: NIZK）に関するものである。1988年にBlumらによってその概念が紹介されて以来 NIZK は暗号理論の発展に重要な役割を果たしてきたが、近年では暗号通貨において送金額の秘匿や公平な取引の実現のために用いられるなど急速に実用化が進んでいる。有用性の観点からはどのようなNP言語に対しても証明ができることが望ましいが、効率の良いNIZKは証明対象の言語が特定の数学的構造に依存して限定されることが多い。そのような限定的な言語に対するNIZKを構成部品として抽象的に扱った場合にどのようなことが可能であるかについてはあまり多くの知見が得られていない。

暗号技術を構成部品として扱った場合の理論的性質を探究するために有用な技術がブラックボックス構成である。すなわちある暗号技術の実装がオラクルとして与えられ、それを用いて他の暗号技術が構成できるか否かを検証することで、その暗号技術にとって本質的に必要な性質を明らかにすることができる。本論文では初めにNIZKをオラクルとして扱う際に考慮すべき点について知見を得る。次に限定的な言語に対するNIZKの典型的な利用方法について、ブラックボックス構成による限界を探究する。本博士論文は全六章から構成されている。

第一章では研究の背景と概要が述べられている。NIZKの概念を説明した後にその具体的なアプリケーションをいくつか紹介し、類似の機能を有する他の暗号技術との比較を行っている。その後、ブラックボックス構成の概念を説明し、特に本論文と関連の深い先行研究を紹介し、最後に本論文における個別の成果について概説している。

第二章では、第三章以降で用いられる記法や用語の定義のほか、NIZKなどの暗号技術の正式な定義、ブラックボックス構成の正式な定義などを与えている。

第三章から第五章では、個別の研究成果について述べている。

第三章では、NIZKオラクルの新たな定式化を提案している。NIZKをオラクルとして扱うブラックボックス構成において、従来はNIZKを外部から乱数を受け入れるオラクルとして定式化していた。本章では乱数を受け入れないオラクルでNIZKを定式化しても従来のオラクルと同様のブラックボックス構成（不）可能性の結果が得られることを示し、この簡略化がオラクルの能力に大きな影響を与えないことを示した。

第四、五章ではNIZKの証明する言語を拡張する一般的な方法が存在するか否かを考察している。NIZKは通常NP言語に対する証明を行うため、NP完全言語を証明できるNIZKを構成することが好ましい。そのためのアプローチの一つとして、まず限定された言語に対する効率的なNIZKを構成し、次にその言語を拡張してNP言語に対する効率的なNIZKを構成するというアプローチが考えられる。本論文では、個別の言語の特徴に依存しないブラックボックス構成による限り、言語拡張は不可能であるという否定的な結果を示している。

第四章では2つの異なる言語の秘密が等しい（これを等式言語と呼ぶ）ことを証明するNIZKが、それぞれの言語に対するNIZKからブラックボックス構成できないことを証明している。等式言語に対するNIZKは暗号理論において公開鍵暗号の安全性を向上させる手段として知られ、近年では暗号通貨のプライバシー保護や公平な取引のために実用されている重要な技術である。本章の結果は、等式言語に対するNIZKを構成するためには個別の数学的構造に依存した構成が必要であることを示唆するものである。

実在する等式言語に対するNIZKはCommit-and-Proveと呼ばれる手法で実現されていることが多い。そのようなNIZKを特に CP-NIZK と呼ぶ。CP-NIZK を用いることで、第四章で示された不可能性は回避できる。そこで第五章では、CP-NIZK が等式言語以外の言語拡張を許すかどうかについて探求している。特に、NP言語L_0とL_1に対するCP-NIZKがそれぞれ与えられたときに論理和言語 L_0 OR L_1に対するNIZKがブラックボックス構成不可能であることを証明している。論理和言語は電子投票における投票内容の正当性を規定するなど広い応用を持つ実用的な言語である。CP-NIZKという強力な手法であっても論理和言語に対するNIZKがブラックボックス構成できないことは、言語拡張によってNP完全言語に対するNIZKを構成することの難しさを強く示唆している。

第六章では、本論文の結論を述べている。本研究を通してNIZKを構成部品として用いる場合の条件やその限界についての知見をまとめている。これらの結果より、新たな仮定が表れるたびに、その仮定の特徴を利用して効率的なNP完全言語に対するNIZKの構成を模索することが必要になると結論している。

（続紙 ２ ）

（論文審査の結果の要旨）

本研究の対象である非対話ゼロ知識証明（NIZK）は安全な電子投票やブロックチェーン上の商取引を実現するための有用な暗号技術であり、本論文で取り組んでいるブラックボックス構成可能性の研究は、量子計算機など計算機技術の変化に対応して今後出現しうる様々な暗号技術に基づいて効率的なNIZKを構成するためのフレームワーク構築に貢献するものである。また、ブラックボックス的な方法では構成できないことを示す不可能性の証明についても、追加的な性質の付与や別の技術に基づく構成を模索することを促すという意義がある。本論文第一章ではではこれら実社会におけるNIZKの重要性が述べられており、研究動機が明確に示されている。

本研究ではNIZKのブラックボックス構成に関して三つの結果を得ている。まず第三章ではNIZKを抽象的なオラクルとして扱うための定式化に注目し、外部から与えられた乱数をオラクルが利用する従来の定式化に対して、乱数を利用しない簡略化された定式化を提唱し、その有用性が従来と変わらないことを述べている。定式化の簡略化は、それを用いた理論的証明が容易になることを意味し、NIZKのブラックボックス構成フレームワーク構築への貢献が期待できる結果である。

続く第四・五章では限定された言語に対するNIZKからより広い言語に対するNIZKを構成する言語拡張の問題に取り組んでいる。限定的な言語に対するNIZKは言語の特徴を利用した効率的な構成が期待できるため、限定的な言語を拡張してNP完全言語に対する効率的なNIZKを構成することは現実的なアプローチの一つである。第四章では、二つの言語に共通する秘密が存在することを証明するいわゆる等式言語のNIZKが、元となるそれぞれの言語に対するNIZKをブラックボックス的に組み合わせる方法では構成できないことを証明している。一方、CP-NIZKと呼ばれる特殊なNIZKに基づく場合には、共通のコミットメント方式を持つという追加的な条件下で等式言語のNIZKがブラックボックス的に構成できることが知られている。このため、第五章ではCP-NIZKに基づく言語拡張の可能性を探求し、二つの言語の論理和からなるいわゆる論理和言語が、元となるそれぞれの言語に対するCP-NIZKをブラックボックス的に組み合わせる方法では構成できないことを証明している。なお、第四章の結果は最も標準的に抽象化されたNIZKに関するものであり、CP-NIZKはそのようなNIZKの特殊な場合にすぎない。CP-NIZKから等式言語NIZKがブラックボックス構成できても、標準的なNIZKからの構成は非自明である。したがって、第五章においてCP-NIZKを前提とした場合を論じることは第四章の研究意義を毀損するものではない。このように、暗号技術の理論的な限界に関する知見を得ることがブラックボックス構成研究の大きな意義の一つである。第四・五章の結果から、一般的なNIZKからのブラックボックス構成では不可能な等式言語のNIZKを実現できるCP-NIZKのような高い能力のものに基づいてさえ、論理和言語がブラックボックス的な方法では構成できないことが分かる。論理和言語は広い応用を持つ言語であり、第四・五章の結果は理論と実用の両面で意義のある結果である。

以上により、本論文は博士（情報学）の学位論文として価値あるものと認める。また、令和３年２月２２日、論文内容とそれに関連した事項について諮問を行った結果、合格と認めた。また、本論文のインターネットでの全文公表についても支障がないことを確認した。

要旨公開可能日：　　2021　年　4月　1日以降