論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Cryptographic Obfuscation Based on Secret Key Primitives
著者(和文)	北川冬航
Author(English)	Fuyuki Kitagawa
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第11063号, 授与年月日:2019年3月26日, 学位の種別:課程博士, 審査員:田中 圭介,伊藤 利昭,尾形 わかは,鹿島 亮,森 立平,藤崎 英一郎
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第11063号, Conferred date:2019/3/26, Degree Type:Course doctor, Examiner:,,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	審査の要旨
Type(English)	Exam Summary

（博士課程）

論文審査の要旨及び審査員

報告番号	甲第　　号		学位申請者氏名		北川 冬航	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	田中 圭介	教授	審査員	森 立平	助教
	審査員	伊東 利哉	教授		藤崎 英一郎	特定教授
		尾形 わかは	教授			
		鹿島　亮	准教授			

論文審査の要旨（2000 字程度）

本論文は「Cryptographic Obfuscation Based on Secret-Key Primitives（暗号学的難読化の秘密鍵技術に基づく構成）」と題し、英文 4 章よりなる。

プログラム難読化は実行内容を変えることなくプログラムをあえて読みにくくする技術であり、リバースエンジニアリングからプログラムコードの持つ情報を守ることを意図して使用される。このようなプログラム難読化は工学の現場において非常に盛んに使用されているが、それらの工学的難読化は安全性に関し一切の保証がなく、実際に多くの工学的難読化に対し攻撃が知られている。このような背景に基づき、暗号学的に安全性が保証された難読化を実現すべく、暗号学的難読化の研究が始まった。暗号学的難読化は暗号学の中でも最も盛んに研究が行われている分野の一つであり、その中でも識別不可能性難読と呼ばれる暗号学的難読化の研究が広く行われている。

現在知られている識別不可能性難読化は全て、公開鍵暗号を含意する技術に基づいて構成されている。すなわち、公開鍵暗号を含意しない秘密鍵技術のみに基づいて、識別不可能性難読化を実現できるかどうかはまだ分かっていない。暗号学的要素技術として識別不可能性難読化をより理解するために、この問題を明らかにすることは暗号学における重要な課題と考えられている。本論文では、この未解決問題に取り組み、肯定的な結果を得た。具体的には、秘密鍵関数型暗号という秘密鍵要素技術のみを用いて、識別不可能性難読化を実現可能であることを示した。本論文の具体的構成は以下の通りである。

第 1 章「Introduction」では、本研究の背景、目的及び成果を述べている。

第 2 章「Preliminaries」では、本研究の内容を述べるために必要な暗号学的要素技術を説明している。

第 3 章「IO for All Circuits from Collusion-Resistant SKFE」では、識別不可能性難読化を秘密鍵関数型暗号に基づいて構成する手法を示す。提案する構成では、構成要素の秘密鍵関数型暗号は、結託耐性と呼ばれる復号鍵を無制限に発行可能であるという性質を満たすことが要求される。本章の具体的な内容は以下の通りである。3.1 章において、本章にて提案する構成の概要を示す。3.2 章において、本論文で用いる穴あけ可能秘密鍵関数型暗号、及びそのいくつかの安全性を定義する。そして、3.3 章及び 3.4 章において結託耐性を満たす秘密鍵関数型暗号から穴あけ可能秘密鍵関数型暗号を構成する手法を示す。最後に 3.5 章において、穴あけ可能秘密鍵関数型

暗号から識別不可能性難読化を構成する手法を示す。

第 4 章「Collusion-Resistant SKFE from Succinct SKFE」では、秘密鍵関数型暗号において発行可能な復号鍵の数を増やす手法を示す。具体的には、succinctness という暗号文のサイズに関する性質を満たし復号鍵を一つのみ発行可能である秘密鍵関数型暗号を用いて、結託耐性を満たす秘密鍵関数型暗号を構成する手法を示す。この結果を 3 章の結果と組み合わせることにより、succinctness を満たし復号鍵を一つのみ発行可能である秘密鍵関数型暗号から識別不可能性難読化を構成可能であることが示される。本章の具体的内容は以下の通りである。最初に 4.1 章において、本章にて提案する構成の概要を示す。次に 4.2 章において、本章において用いる index 付き秘密鍵関数型暗号を定義する。そして 4.3 章及び 4.4 章において、本章の主構成において用いる、いくつかの基本構成を示す。4.5 章では、4.3 章及び 4.4 章において導入した構成手法を組み合わせて、succinctness を満たし復号鍵を一つのみ発行可能である秘密鍵関数型暗号を用いて、結託耐性を満たす秘密鍵関数型暗号を構成する手法を示す。加えて、最後に 4.6 章では、本章において用いた技法を用いて、秘密鍵関数型暗号の暗号文サイズを一般的に削減可能であることを示す。

以上を要するに、本論文は識別不可能性難読化が公開鍵技術を一切用いることなく、秘密鍵技術である秘密鍵関数型暗号のみに基づいて、構成可能であることを示している。また加えて、その構成の際に秘密鍵関数型暗号が満たすべき条件に関する考察を行い、具体的には結託耐性または succinctness のどちらか一方を満たす秘密鍵関数型暗号があれば、識別不可能性難読化を構成可能であることを示した。これらの結果は、暗号学的要素技術として識別不可能性難読化をより理解する上で非常に重要であり、今後の識別不可能性難読化の研究に対し、有用な知見を与えると考えられ、その成果は理学上貢献するところ大である。よって、本論文は博士（理学）の学位論文として十分価値があるものと認める。