論文 / 著書情報
Article / Book Information

題目(和文)	ペアリングに基づく暗号方式の型変換の理論
Title(English)	Theory of Type Conversion for Pairing-based Crypto Schemes
著者(和文)	星野文学
Author(English)	Fumitaka Hoshino
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11067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,伊東 利哉,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11067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	星野　文学	
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「Theory of Type Conversion for Pairing-based Crypto Schemes（ペアリングに基づく暗号方式の型変換の理論）」と題し、英文 8 章よりなる。

ペアリングとは高度な暗号方式の設計に用いられる数学的な関数のことである。現在までに様々なペアリングの実装方法が提案されているが、それらはペアリングへの入力の型に基づいて、対称ペアリングと非対称ペアリングに分類される。対称ペアリングの方が構造が単純な為、暗号設計において以前は対称ペアリングが非常に良く使用された。しかし、対称ペアリングの有力な実装方法に対する暗号解析技術が急速に進展したため、現在では非対称ペアリングが好んで使われるようになっている。

既に膨大な数の対称ペアリングを用いた暗号方式が提案されているため、機能、安全性および性能を損なうことなく対称ペアリングに基づく暗号方式を非対称ペアリングに基づく暗号方式に自動的に翻訳する方法、即ちペアリングに基づく暗号方式の型変換の方法が研究されてきた。しかし既知の方法では数十程度までのペアリング関数で構成される比較的小規模な暗号方式についてのみ、そのような型変換が可能であった。

本論文では、まず計算量理論に基づき、型変換の問題の困難性に関する解析を行っている。次に 0-1 整数計画法に基づく実用的な型変換アルゴリズムを提案している。そしてこのアルゴリズムを実装し、いくつかの中規模な暗号方式について、実際にこのアルゴリズムで初めて型変換が可能になった事を報告している。また、人工的に生成されたランダムな暗号方式の型変換に関して実験を行い、型変換に要する時間が従来の方法よりも 100 倍から 100 万倍程度高速化した事を報告している。

第１章「Introduction」では、本研究の背景、目的および成果の概要を述べている。

第２章「Preliminary」では、本研究の内容を述べるために必要な用語や技術の説明を行っている。

第３章「Conversion Based on Dependency Graphs」では、機能と安全性を保証したまま暗号方式の型変換を行う為のフレームワークを提案する。そこでは、暗号方式を構成する機能、文法、困難性の仮定、安全性概念、安全性の帰着などから型変換に関係するデータフローを全て抽出した依存関係グラフの概念を導入し、機能と安全性を保証したまま暗号方式の型変換を行うのに十分な４つの条件を示している。

第４章「Theory of Bilinear-Type Conversion」では、性能の保証を無視し、機能と安全性を保証する(即ち第３章の４つの条件を満足する)型変換について、もし可能ならそのような型変換を実際に行う多項式時間アルゴリズムを提案している。また、性能の保証を、機能と安全性を保証する型変換の最適化問題として捉え、その最悪時の困難性を MinSAT と呼ばれる問題の NP 困難性に帰着している。

第５章「Finding Optimal Valid Split with IP」では、第４章の最適化問題を踏まえ、0-1 整数計画法に基づく、機能、安全性および性能を保証する、実用的な型変換アルゴリズムを提案している。

第６章「Performance」では、第５章で提案されたアルゴリズムの実装評価を行っている。数百程度のペアリング関数で構成される幾つかの中規模の暗号方式について、実際にこのアルゴリズムで初めて型変換が可能になった事を報告している。また、数十程度のペアリング関数で構成される人工的に生成されたランダムな暗号方式の型変換に関して実験を行い、型変換に要する時間が従来の方法よりも 100 倍から 100 万倍 程度高速化した事を報告している。

第７章「Using Conversion in Cryptographic Design」では、ペアリングを用いた暗号方式の設計に対して、型変換がどのように役立つかをいくつかの実例を挙げて説明している。

第８章「Conclusion」では、本研究の成果についてまとめ、今後の研究課題について述べている。

以上を要するに、本論文は、機能、安全性および性能を損なうことなく対称ペアリングに基づく暗号方式を非対称ペアリングに基づく暗号方式に自動的に翻訳する方法を提案し、実際にその効果を示したもので、提案の適用性、有用性、発展性は高く、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。