OUKA
The University of Osaka
Institutional Knowledge Archive

Title	Quantum Reductions from One-Wayness to Unpredictability and Quantum Public Key Encryption
Author(s)	数藤, 恭平
Citation	大阪大学, 2026, 博士論文
Version Type	VoR
URL	https://doi.org/10.18910/105550
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

様式３

論　文　内　容　の　要　旨

氏　名　（　数藤恭平　）	
論文題名	Quantum Reductions from One-Wayness to Unpredictability and Quantum Public Key Encryption （量子計算・通信を前提とした一方向性から予測不可能性および量子公開鍵暗号への帰着）

論文内容の要旨

暗号理論とは、敵対者の存在を前提として暗号技術を設計する科学および実践である。公開鍵暗号は事前に秘密情報を共有していない二者間においても安全な通信を可能にし、また電子署名は情報の正当性を保証するなど、暗号技術は現代の情報社会を支える基盤技術となっている。

暗号技術の安全性を証明するために、帰着という概念が用いられる。帰着とは、ある問題を別の問題に変換することで計算量的な困難性の関係を示す手法であり、暗号理論においては、安全性の根拠や必要最小限の計算量的仮定を明らかにする役割を果たす。

一方向性関数の存在は、暗号理論における最小の計算量的仮定であることが知られている。すなわち、任意の暗号の存在には、一方向性関数の存在が本質的に必要である。一方で、一方向性関数は最小の仮定でありながら、共通鍵暗号や電子署名といった重要な暗号プリミティブを構成するには十分であることも知られている。一方向性関数からどのような暗号技術が構成可能であるかを明らかにすることは、暗号理論における重要な研究課題であり、一方向性関数から構成可能な暗号技術全体の集合は Minicrypt と呼ばれる。

量子計算および量子通信を暗号技術に取り入れることで、一方向性関数から構成可能な暗号プリミティブの範囲はさらに拡張される。例えば、古典的な設定では公開鍵暗号は一方向性関数のみからは構成できないと考えられているが、近年の研究により、量子通信路が利用可能であれば量子公開鍵暗号は一方向性関数から構成可能であることが示されている。このように、計算量的仮定の強さを変えることなく、量子計算および量子通信を導入することで、古典的な設定とは異なる結果が生じる可能性がある。量子計算および量子通信を仮定した上で、一方向性関数から構成可能な暗号技術全体の集合は MiniQCrypt と呼ばれる。量子技術の進展に伴い、これらの量子的枠組みにおける一方向性関数の役割について、改めて体系的に検討する必要がある。

本論文では、MiniQCrypt の研究分野における二つの課題に着目する。第一の課題は、一方向性から予測不可能性への量子帰着を一般化することである。古典的な一方向性から予測不可能性への帰着である Goldreich-Levin 定理は、暗号理論および計算量理論の双方において重要な役割を果たしている。その量子版は Adcock と Cleve によって示されているが、定義域が二値文字列の場合に限られており、0 から q-1 までの文字からなる場合のような、より一般的な設定への拡張は未解決問題であった。第二の課題は、より現実的な仮定の下で、一方向性関数から量子公開鍵暗号を構成することである。既存の構成では、量子公開鍵の生成に強力な量子計算機を必要とするほか、量子通信路が理想的であることを仮定しており、実用的な観点からは制約が大きい。

本論文では、MiniQCrypt におけるこれら二つの課題に対して肯定的な解答を与える。まず、一般化された一方向性から予測不可能性への量子帰着を示す。また、現実的な安全性モデルの下で、一方向性関数のみに基づく量子公開鍵暗号の構成を与える。さらに、一般化された一方向性から予測不可能性への量子帰着の応用として、Learning with Errors (LWE) 問題に対する量子 search-to-decision 帰着を構成する。

これらの結果は、量子設定における一方向性関数の役割および MiniQCrypt の構造に関する理解を深めるものである。また、量子攻撃者の存在下における耐量子暗号の安全性を理論的に解析するための基盤を与える。

様式７

論文審査の結果の要旨及び担当者

氏　　名　（　数藤　恭平　）		
論文審査担当者	（職）	氏　　名
	主 査　教 授	藤井　啓祐
	副 査　教 授	山本　俊
	副 査　教 授	真田　篤志
	副 査　教 授	河内　亮周（三重大学大学院工学研究科）

論文審査の結果の要旨

本論文は、暗号理論における最小仮定である一方向性関数を基軸として、量子計算および量子通信を導入した場合に成立する暗号理論の構造を、計算量理論的観点から体系的に明らかにしたものである。特に、量子環境下において一方向性関数から構成可能な暗号プリミティブのクラスである MiniQCrypt に焦点を当て、その理論的基盤を深化させている点に本論文の大きな特徴がある。

まず著者は、古典暗号理論において中心的役割を果たす Goldreich-Levin 定理の量子版に注目し、その定義域を二値から一般の $\mathbb{Z}_q$へと拡張する量子リダクションを与えた。これは長年未解決であった問題に対する重要な進展であり、量子計算における一方向性と予測不可能性の関係を本質的に明らかにしている。さらにこの成果を応用し、ポスト量子暗号の中核的仮定である LWE 問題に対して、量子計算を用いた探索版から判定版へのリダクションを構成し、その構造的理解を与えている。加えて、本論文では現実的な量子通信環境を考慮した量子公開鍵暗号の安全性定義を定式化し、一方向性関数のみに基づく具体的構成を与えている。特に、単一量子ビットの直積状態のみを用いる点や、量子通信路が不完全である状況を想定した安全性解析は、実装可能性の観点からも高く評価できる。

以上のように、本論文は量子計算時代における暗号理論の基礎を計算量理論的に再構築し、理論的にも実用的にも重要な貢献をなしている。量子暗号およびポスト量子暗号研究の発展という観点からの貢献も大きい。以上の理由から、本論文は博士（理学）の学位論文として十分な価値があるものと認める。