符号ベース暗号における量子ISDアルゴリズムに関する研究

A Study of quantum ISD algorithm on code-based cryptography

三浦夢生・法制倫理分科会・情報セキュリティ大学院大学

1. 研究背景

量子計算機の開発や量子アルゴリズムの研究が盛んに行われており，量子計算機が実用化されると現在広く用いられている公開鍵暗号が破られることが懸念される．その中で，量子計算機を用いた攻撃にも耐えうる耐量子計算機暗号への関心が高まっており，その研究の重要性は増している．本研究では，PQCの一つであり，NIST PQC標準化プロセス第4ラウンドにも選出されている「符号ベース暗号」の解読に関する研究を行う．暗号の解読ができるかどうか，必要な計算量がどれほどかを明らかにすることで安全に暗号を運用できるパラメータや方法が明らかになる．

2. 量子ISDアルゴリズムに関する先行研究

最も基本的なISDアルゴリズムであるPrangeのアルゴリズムに，Grover探索を用いることで計算量の削減を図った研究がある．これには既に回路実装が提案されている．

Grover探索はN個のデータベースからNの平方根程度のオーダーで所望のデータを探索する量子アルゴリズムであり，広く応用が期待されている．また量子的にランダムウォークを行い，Grover探索と組み合わせて解の候補を探索する量子Dumerアルゴリズムという手法があるが，全体の量子回路実装はされていない．格子暗号における格子ふるいという解探索手法を符号ベース暗号に応用したSieveアルゴリズムが近年提案されたが，これに関する量子的な提案は全くされておらず，量子的な計算量については明らかになっていない．

3. 今後の方針

現在提案されている古典的ISDアルゴリズムを，量子アルゴリズムを用いて計算量の削減がされたISDアルゴリズムの中でも量子回路の実装が知られていないものがある．そこで，そのような量子回路を模索し，暗号の解読にかかる計算量を明らかにすることで安全な暗号の運用に寄与していきたい．