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

In recent years, the development of quantum computers and research on quantum algorithms have been active. There is concern that the practical use of quantum computers will lead to the breakage of public key cryptography, which is widely used today. In this context, there is a growing interest in Post-Quantum Cryptography that can withstand attacks using quantum computer, and the impotance of research on PQC is increasing. Since its proposal in 1978, there has been no effective decoding method for code-based cryptography, and it was selected for the fourth round of the NIST PQC standardization process. The ISD algorithm is considered to be the most effective attack on code-based cryptography. In this research, we aim to find and program a quantum circuit that implements the quantum ISD algorithm with reduced computational complexity using a quantum algorithm.

背景

近年，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いる．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**(Post-Quamtum Cryptography，以下PQC)」への関心が高まっており，NISTも現在PQCの標準化を進めている．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．解読にかかる計算量やパラメータを模索することで安全な暗号方式の構成に寄与する．

目的

本研究では，符号ベース暗号におけるシンドローム復号問題を解読する量子回路を模索することを目的とする．シンドローム復号問題の解読には量子アルゴリズムを用いたISDアルゴリズムを用いる．

符号ベース暗号

符号ベース暗号とは，符号理論における数学的に困難な問題に安全性を依拠する暗号方式のことである．符号理論に基づく公開鍵暗号方式(McEliece暗号)は1978年から存在しており，効果的な解読手法が存在しないことから現在まで用いられている．ここでは符号理論における難問として「**シンドローム復号問題**(Syndrome Decoding Problem:SDP)」を扱う．

シンドローム復号問題

正整数n, k, w，行列$\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$，ベクトル$\mathbf{s} \in \mathbb{F}_2^{n-k}$が与えられたとき，$\mathbf{He} = \mathbf{s}$かつ$wt(\mathbf{e}) = w$となる$\mathbf{e} \in \mathbb{F}_2^n$を求める．

例えば $n = 5, k = 2, w = 2$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}, \mathbf{s} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

の場合$011 \oplus 110 = 101$より解は$\mathbf{e} = 01010$となる．
SDPは実質的にNP困難であることが知られている．

ISDアルゴリズム

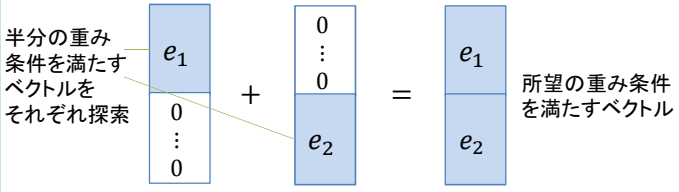
ISD(Information Set Decoding)アルゴリズムはシンドローム復号問題を最も効率的に解くと言われるアルゴリズムのクラスである．ISDアルゴリズムは共通のフレームワークが存在する．

1. ランダムな並べ替え$\mathbf{P}$を生成し，$\mathbf{H}$の列を入れ替える．
2. ガウスの消去法によりSDPを$\begin{pmatrix} \mathbf{H}' & \mathbf{0} \\ \mathbf{H}'' & \mathbf{I} \end{pmatrix}\begin{pmatrix} \mathbf{e}' \\ \mathbf{e}'' \end{pmatrix} = \begin{pmatrix} \mathbf{s}' \\ \mathbf{s}'' \end{pmatrix}$に変形する．
3. $\mathbf{H}'$及び$\mathbf{s}'$から解の候補$\mathbf{e}'$を探索する．
4. $\mathbf{e}'$が$wt(\mathbf{e}') = p, \mathbf{H}'\mathbf{e}' = \mathbf{s}'$を満たしているかチェックする．
5. 直接$\mathbf{e}''$を計算し，$wt(\mathbf{e}'\ \mathbf{e}'') = w$を満たしているかチェックする．
6. $\begin{pmatrix} \mathbf{e}' \\ \mathbf{e}'' \end{pmatrix}$に$\mathbf{P}^{-1}$をかけて解$\mathbf{e}$を得る．

現在までに様々な派生が提案されており，手法によって主にステップ3.の探索方法が異なる．

例

- 重み条件の一部を満たす解の候補を探索する
- 半分の重み条件を満たす解の候補を探索する
- 重み条件を徐々に追加し，解の候補を探索する etc.



量子ISDアルゴリズムでは，ステップ1.において状態の重ね合わせを構築し，Grover探索を用いて効率的に解の探索を行う．探索する解の候補をJohnsonグラフの直積としてモデル化し，ランダムウォークを用いてSDPを解く量子アルゴリズムも存在する．

今後の展望

引き続き文献調査を行い，量子ISDアルゴリズムの回路実装の動向を注視する．
量子回路シミュレーションライブラリQiskitを用いて量子回路実装を目指す．