耐量子計算機暗号における符号暗号

Cryptography in quantum computer cryptography

安光一平・ネットワーク分科会・情報セキュリティ大学院大学

1.研究背景

現在通信の安全性を守っている暗号は量子コンピューターが実用化されると、その安全性の根拠とされている数学的な問題が攻略されてしまう。これに対応するため、様々な量子コンピュータに耐性のある暗号(耐量子計算機暗号)がNISTで提案されている。種類は多々あり、最も研究が進められている耐量子計算機暗号は格子暗号であるが、私は符号暗号に着目する。

2.符号暗号

符号理論を利用した暗号であり、安全性はシンドローム復号問題を解く計算の困難性に基づいている。
量子コンピュータに耐性がある。
-シンドローム復号問題-
$(H, y^T) \in \mathbb{F}^{(n-k) \times n} \times \mathbb{F}^{(n-k)}$に対して、
入力(H, y^T)
出力(x) // $Hx^T = y^T$,$\omega(x)=w$

3. なぜ符号暗号か

耐量子計算機暗号では格子暗号が主な研究対象になっているが、今後格子に対する有力な攻撃が発見されると深刻な状況に陥る。そのため、原理の違う耐量子計算機暗号も準備する必要がある。

4.符号暗号に関する先行研究

ABDGZ暗号という安全性証明のなされた暗号がある。巡回行列のシンドローム復号問題の困難性に基づいた暗号であり、
非常に高速な復号アルゴリズムと、数千ビットという小さな鍵サイズを実現できる。
しかし、組織巡回符号という特殊な符号を使っているため、これに対する有効な攻撃がある可能性があるなど、安全性上の懸念がある。
-組織巡回符号-
以下のパリティ検査行列を持つ巡回符号

$$H = \begin{pmatrix} I_n & 0 & \cdots & 0 & A_1 \\ 0 & I_n & & & A_2 \\ & & \ddots & & \vdots \\ 0 & & \cdots & I_n & A_\ell \end{pmatrix} \in \mathbb{F}^{\ell n \times sn}$$

A_1 A_lは $n \times n$ 巡回行列

$$A_i = rot((q_r)^{(i)})(i = 1 \cdots)$$

5.今後の方針

符号暗号は長らく安全性証明が無く、さらに鍵と暗号文のサイズに懸念が残っていた。そこで、格子暗号の方法論を符号暗号に応用する研究が提案されている。このもとで、格子暗号で培われた方法を符号暗号に生かすことでサイズも小さく安全証明のつく方法を模索していきたい。