平成 13 年度卒業研究		
入学年度　平成 10 年度	学籍番号　10117935	氏名　　白木 宏幸
論文題目　量子情報のセキュアな伝送のための量子誤り訂正符号の検討		中野研究室

1　はじめに

量子情報の安全な伝送方法について考察する．従来，量子情報の安全な伝送方法として，暗号化によって盗聴者に情報を与えない吾妻-番プロトコルが提案されているが，盗聴者の攻撃で壊された量子情報を修復する機能は明示されていなかった．しかし，量子非複製定理により，量子情報にはバックアップをとっておくことができないという古典的データにはなかった制約があるため，真に安全と呼ぶためには，盗聴による破壊に対する情報復元機能が必要ではないだろうか．

このため，本研究では，このプロトコルに“ 壊された量子情報の復元 ”機能を付加し，より安全なプロトコルに改良することを目的としている．その方法論として，量子誤り訂正符号を適用することを考える．具体的には，特定位置誤り訂正可能な量子符号を提案し，プロトコル改良のために利用することを考察する．

2　吾妻-番プロトコル

吾妻-番プロトコルの暗号化及び認証の手続きの部分について概説する．暗号化及び認証の一連の手続きは，

(1) データ用量子ビットの暗号化

(2) 認証用量子ビットの付加

(3) データ及び認証用量子ビットの暗号化

から成る．以下に其々のステップについて説明する．ただし，n-量子ビットの状態を $|\Psi_n^{\mathrm{Q}}\rangle$ と表し，署名を表す量子状態を $|a^{\mathrm{S}}\rangle$ と表す．また，其々をデータ用量子ビット，及び認証用量子ビットと呼ぶ．

(1)　unitary 作用素の集合 $\mathcal{M}_n$ に属する作用素 $\hat{U}^{\mathrm{Q}}$ をランダムに作用させる．

(2)　k 番目の量子ビットに $|a_k^{\mathrm{S}}\rangle \in \{|0^{\mathrm{S}}\rangle, |1^{\mathrm{S}}\rangle\}$ を付加．

(3)　下式の unitary 作用素 $\hat{V}_\alpha^{\mathrm{QS}}$ を作用させる．

$$\hat{V}_\alpha^{\mathrm{QS}} = \bigotimes_{k=1}^{n} [(\hat{L}^{Q} \otimes \hat{L}^{\mathrm{S}})\hat{U}_{\mathrm{C-NOT}}^{\mathrm{QS}}]$$

ただし，α は $4n$ ビットの古典情報の暗号鍵であり，送信者があらかじめ準備した unitary 作用素の集合 $\mathcal{L}$ から無作為に選んだ $\hat{L}^{\mathrm{Q}}$,$\hat{L}^{\mathrm{S}}$ を其々定めている．

3　改良プロトコル

1 量子ビット伝送において，$(3,1)$ 符号化による特定位置量子誤り訂正符号 [1] を吾妻-番プロトコルに適用する．本来，1 量子ビット誤り訂正には最低でも $(5,1)$ 符号化が必要であることが知られているが，訂正可能な位置を限ることで，より単純な $(3,1)$ 符号で，これを実現させた．

以下，改良プロトコルについて説明する．ただし，其々の記号は 2 節で用いたものと同義とする．

＜ 送信者側での手続き ＞

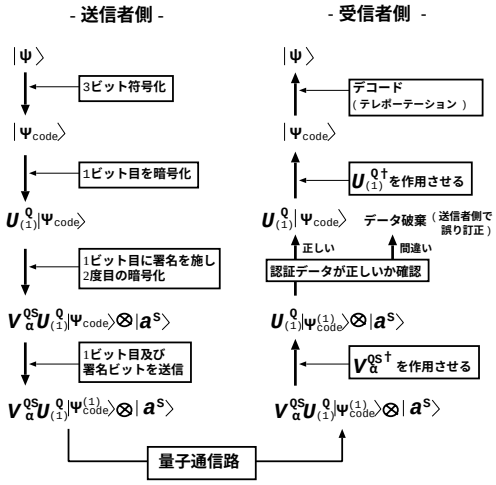
1. 3 ビット符号化．
$$|\psi\rangle = |\Psi_1^{\mathrm{Q}}\rangle \equiv c_0|0\rangle + c_1|1\rangle$$
$$\longrightarrow |\Psi_{\mathrm{code}}\rangle = \frac{1}{\sqrt{2}}\{c_0(|00\rangle + |11\rangle)|0\rangle + c_1(|00\rangle - |11\rangle)|1\rangle\}$$
2. 1 量子ビット目を暗号化． 添え字 (1) は 1 量子ビット目に作用させていることを示し， 以下も同様の記号を用いる．
$$|\Psi_{\mathrm{code}}\rangle \rightarrow \hat{U}_{(1)}^{\mathrm{Q}}|\Psi_{\mathrm{code}}\rangle$$
3. 1 量子ビット目に署名を施し，2 度目の暗号化を行う
$$\hat{U}_{(1)}^{\mathrm{Q}}|\Psi_{\mathrm{code}}\rangle \rightarrow \hat{V}_\alpha^{\mathrm{QS}}\hat{U}_{(1)}^{\mathrm{Q}}|\Psi_{\mathrm{code}}\rangle \otimes |a^{\mathrm{S}}\rangle$$
4. 送信者は，1 量子ビット目と署名ビットを受信者に送る．

＜ 受信者側での手続き ＞

1. 受け取った 1 量子ビット目と認証ビットに対し，$\hat{V}_\alpha^{\mathrm{QS}\dagger}$ を作用させる．
2. 認証データが正しいかどうか確認する．
3. 正しければ，1 量子ビット目に $\hat{U}_{(1)}^{\mathrm{Q}\dagger}$ を作用させる．そして送信者側での測定と局所的操作 (量子テレポーテーション) により，量子情報 $|\psi\rangle$ を取り出す．
4. 誤っていれば，受信者はデータを破棄し，送信側で 2 量子ビット目の測定と局所的操作を行うことにより，量子情報を復元する．再送する場合は，再び送信者側での手続き 1 からを繰り返す．

なお，古典通信路でのやり取りや暗号化鍵のため，BB84 プロトコルなどで共有された乱数を必要に応じて利用するものとする．

以下に改良プロトコルの概要図を示す．



本研究では，更に送信する 1 量子ビット目に関しては，盗聴者の如何なる von Neumann 測定にも対処可能 [2] であることを確認した．

4　まとめ

吾妻-番プロトコルに盗聴により壊された量子情報の復元機能を付加するため，量子誤り訂正符号の適用を考察した．その結果，このプロトコルに必要なのは特定位置量子誤り訂正であり，(3,1) 符号という非常に簡単なものを利用するだけで，1 量子ビット伝送においては盗聴者の如何なる von Neumann 測定にも対処できることを示した．今後は 2 量子ビット以上の量子情報伝送を実現する量子誤り訂正符号について検討する．

参考文献

[1] 白木, 宇佐見, 臼田, 内匠, 第 24 回情報理論とその応用シンポジウム, pp.859-862, 2001.

[2] 白木, 宇佐見, 臼田, 内匠, 2002 年電子情報通信学会総合大会, 発表予定.