基于量子 CSS 纠错码的量子公钥密码和消息认证

李 峥[①②] 马智[①③] 吕 欣[①] 冯登国[①]

[①](信息安全国家重点实验室 中国科学院研究生院 北京 100039)

[②](解放军信息工程大学电子技术学院 郑州 450004)

[③](解放军信息工程大学信息工程学院 郑州 450002)

摘 要 该文利用量子 CSS 纠错码的构造方法和一般线性码的译码是一个 NPC 问题建立了一个量子公钥密码体制。其特点是以经典信息作为密钥来加密量子消息，安全性建立在 NPC 问题量子图灵机(QTM)不可解基础之上。利用此公钥密码体制，该文还给出了一个基于量子 CSS 纠错码的消息认证方案，并证明了其安全性。

关键词 信息安全，量子密码，量子 CSS 纠错码，公钥密码，消息认证

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2005)03-0537-05

A Quantum Public-Key Cryptosystem and Message Authentication Scheme Based on Quantum CSS Error Correcting Codes

Li Zheng[①②] Ma Zhi*[①③] Lü Xin[①] Feng Deng-guo[①]

[①](*State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing* 100039, *China*)

[②](*Institute of Electronic Technology, The PLA Information Engineering University, Zhengzhou* 450004, *China*)

[③](*Institute of Information Engineering,The PLA Information Engineering University,Zhengzhou* 450002, *China*)

Abstract This paper presents a quantum public-key cryptosystem by using quantum Calderbank-Shor-Steane(CSS) error correcting codes and the NPC problem related with decoding general linear codes. It uses classical key to encrypt quantum message, and its security relies on the fact that NPC problem can not be solved on quantum Turing machines. Based on this public-key cryptosystem, this paper also gives a message authentication scheme and proves its security.

Key words Information security, Quantum cryptography, Quantum CSS error correcting codes, Public-key cryptography, Message authentication

1 引言

近年来，量子力学与信息科学相交叉的新型学科——量子信息科学发展迅速，在快速量子算法、量子纠错码、量子保密通信等各方面的研究都取得了很大的突破。同时也给现代密码学的研究带来了新思路和影响。一方面，基于量子并行计算的量子快速算法对一些建立在传统计算困难性上的密码体制构成了不可忽略的威胁，如Shor[1]给出的大整数分解算法和求解有限域上的离散对数算法以及Grover[2]给出的基于无序数据库的量子搜索算法。另一方面，基于量子力学的无条件安全的量子密钥分配的研究[3]给探索无计算假设的密码体制带来了新思路。

在量子密码学中，量子态加密和量子消息认证占有重要的地位，研究也正在逐步深入。文献[4]给出了一个量子态加密的一次一密方案，用 $2n$ 个经典比特来加密 n 个量子位，并且是最优选择。Okamoto等人[5]给出了一个可以抵御量子图灵机攻击的公钥密码以及签名机制，其方案是用经典信息作为密钥加密经典消息，安全性建立在NPC问题量子图灵机不可解的基础之上。Shor等人[6]利用量子CSS(Calderbank-Shor-Steane)纠错码简化了BB84 量子密钥分配协议的安全性证明，Barnum等人[7]则利用量子稳定子码构建了一个非交互的量子消息认证系统，其安全性是建立在量子物理机制之上的。

本文利用量子 CSS 纠错码(简称量子 CSS 码)的构造方法及一般线性码的译码问题是一个 NPC 问题和 Goppa 码有快

2004-08-10 收到, 2005-02-16 改回

国家重点基础研究发展规划 973 计划(G1999035802)，国家杰出青年科学基金(60025205)，国家自然科学基金(60273027,60403004)和中国博士后科学基金资助项目

速译码算法的特点，建立了一个基于量子 CSS 码的量子公钥密码体制。它是用经典信息作为密钥来传递量子消息，可以抵抗量子图灵机的算法攻击。最后，本文给出了一个基于量子 CSS 码的量子消息认证方案，并证明了其安全性。本文安排如下：在第 2 节中，我们简要介绍所需的量子 CSS 码和经典 Goppa 码的知识。在第 3 节中，我们利用量子 CSS 码建立了一个量子公钥密码体制，并分析了其在量子算法攻击下的安全性。在第 4 节中，我们利用此公钥密码体制给出了一个基于量子 CSS 码的量子消息认证方案，并证明了其安全性。

对量子计算、量子密码和量子纠错码的进一步介绍可参见文献[8,9]。

2 预备知识

2.1 量子 CSS 码

一个量子纠错码 $Q:[[n,k,d]]$ 就是 Hilbert 空间 $\square^{2^n}$ 的一个 2^k 维子空间，它将一个有 k 个量子位的量子态编码为 n 个量子位，并且可以纠正 $t\le(d-1)/2$ 个量子错误，且不扰动编码态。d 称为 Q 的极小距离。而量子 CSS 码 Q 可以由经典线性码构造。

定理 1[10,11] 设存在经典二元线性码 $C_1=[n,k_1,d_1]$，$C_2=[n,k_2,d_2]$，且 $C_1^{\perp}\subseteq C_2$ (于是 $n\le k_1+k_2$)。那么，存在量子码 $Q:[[n,k=k_1+k_2-n,d=\min\{d_1,d_2\}]]$。且 Q 的一组基态为

$$\left\{\ |C_w\rangle=\frac{1}{2^{\frac{n-k_1}{2}}}\sum_{\boldsymbol{v}\in C_1^{\perp}}|\boldsymbol{v}+\boldsymbol{w}\rangle\ \middle|\ \boldsymbol{w}\in C_2/C_1^{\perp}\ \right\}$$

设 C_i 的生成矩阵和校验矩阵分别为 $\boldsymbol{G}_i,\boldsymbol{H}_i$ $(i=1,2)$。由 $C_1^{\perp}\subseteq C_2$，我们不妨设 $\boldsymbol{G}_2=\begin{pmatrix}\boldsymbol{H}_1\\ \boldsymbol{D}\end{pmatrix}$，则 $\boldsymbol{D}$ 的秩为 $k=k_1+k_2-n$。对任意 k 个量子位的基态 $|\boldsymbol{m}\rangle=|m_1,\cdots,m_k\rangle$ $(\boldsymbol{m}\in\mathbb{F}_2^k)$，我们可将其编码为码字

$$\begin{aligned}|c_m\rangle&=\frac{1}{2^{(n-k_1)/2}}\sum_{\boldsymbol{v}\in C_1^{\perp}}|\boldsymbol{v}+\boldsymbol{m}\cdot\boldsymbol{D}\rangle\\&=\frac{1}{2^{(n-k_1)/2}}\sum_{\boldsymbol{v}\in C_1^{\perp}}|\boldsymbol{v}+m_1\boldsymbol{D}^{(1)}+\cdots+m_k\boldsymbol{D}^{(k)}\rangle\end{aligned}\qquad(1)$$

其中 $\boldsymbol{D}^{(j)}$ 表示 $\boldsymbol{D}$ 的第 j 行，$1\le j\le k$。因为任意量子纯态可表为基态的线性组合，所以我们可以对任意态进行编码。设 $|\varphi\rangle=\sum_{\boldsymbol{m}\in\mathbb{F}_2^k}\alpha_m|\boldsymbol{m}\rangle$ 为任意态，则将其编码为 $|\psi\rangle=\sum_{\boldsymbol{m}\in\mathbb{F}_2^k}\alpha_m|c_m\rangle$，其中 $|c_m\rangle$ 如式(1)所示。

量子态经量子信道传输时会发生量子错误 e。每个量子位上有 3 个基本的量子错误：比特错、相位错以及其复合，可以分别用 Pauli 矩阵来描述：

$$\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad \sigma_y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$$

对 $a\in\{x,y,z\},\boldsymbol{r}=(r_1,\cdots,r_n)\in\mathbb{F}_2^n$，我们令 $\sigma_a^{[\boldsymbol{r}]}=\sigma_a^{[r_1]}\otimes\cdots\otimes\sigma_a^{[r_n]}$ 来表示一个 n 量子位上的量子错误，其中

$$\sigma_a^{[r_i]}=\begin{cases}I, & r_i=0\\ \sigma_a, & r_i=1\end{cases}$$

则 $\sigma_x^{[r]}$ 和 $\sigma_z^{[r]}$ 的所有特征值只有 ±1。则 n 量子位上的量子错误可表示为 $e=\sigma_x^{[\boldsymbol{X}]}\sigma_z^{[\boldsymbol{Z}]}$，其中 $\boldsymbol{X}=(x_1,\cdots,x_n)$，$\boldsymbol{Z}=(z_1,\cdots,z_n)\in\mathbb{F}_2^n$。为方便起见，我们也用 $e=(\boldsymbol{X}\,|\,\boldsymbol{Z})\in\mathbb{F}_2^{2n}$ 来描述此量子错误，那么它在 n 个量子位的基态 $|\boldsymbol{V}\rangle=|v_1,\cdots,v_n\rangle$ $(\boldsymbol{V}\in\mathbb{F}_2^n)$上的作用为

$$e|\boldsymbol{V}\rangle=(-1)^{\boldsymbol{Z}\cdot\boldsymbol{V}}|\boldsymbol{X}+\boldsymbol{V}\rangle=(-1)^{z_1v_1+\cdots+z_nv_n}|x_1+v_1,\cdots,x_n+v_n\rangle\qquad(2)$$

类似于经典纠错码，我们要利用校验子测量来查错和纠错。设量子态 $|\psi\rangle\in Q$ 发生了量子错误 $e=\sigma_x^{[X]}\sigma_z^{[\boldsymbol{Z}]}$，得到出错态 $e|\psi\rangle$。设 $\boldsymbol{H}_1^{(i)},\boldsymbol{H}_2^{(j)}$ 分别表示 $\boldsymbol{H}_1$ 的第 i 行和 $\boldsymbol{H}_2$ 的第 j 行，$1\le i\le n-k_1,1\le j\le n-k_2$。对 $e|\psi\rangle$，我们测量 $\sigma_x^{[\boldsymbol{H}_1^{(i)}]}$ 的特征值：

$$\sigma_x^{[\boldsymbol{H}_1^{(i)}]}e|\psi\rangle=(-1)^{\boldsymbol{H}_1^{(i)}\cdot\boldsymbol{Z}^{\mathrm{T}}}e|\psi\rangle,\quad 1\le i\le n-k_1$$

从而获得校验子 $\boldsymbol{H}_1\cdot\boldsymbol{Z}^{\mathrm{T}}=(\boldsymbol{H}_1^{(1)}\cdot\boldsymbol{Z}^{\mathrm{T}},\cdots,\boldsymbol{H}_1^{(n-k_1)}\cdot\boldsymbol{Z}^{\mathrm{T}})$。并由此求出相位错 $\sigma_z^{[\boldsymbol{Z}]}$。同理，测量 $\sigma_z^{[\boldsymbol{H}_2^{(j)}]}$ 的特征值，得到校验子 $\boldsymbol{H}_2\cdot\boldsymbol{X}^{\mathrm{T}}$，从而获取比特错 $\sigma_x^{[X]}$。这样我们就查出错误 $e=\sigma_x^{[\boldsymbol{X}]}\sigma_z^{[\boldsymbol{Z}]}$。若 $w_Q(e)\le t=\dfrac{\min\{d_1,d_2\}-1}{2}$，这里 $w_Q(e)=\#\{1\le i\le n\,|\,(x_i,z_i)\ne(0,0)\}$，那么由经典纠错码的译码知识我们知道从校验子 $\boldsymbol{H}_1\cdot\boldsymbol{Z}^{\mathrm{T}}$ 和 $\boldsymbol{H}_2\cdot\boldsymbol{X}^{\mathrm{T}}$ 可以分别唯一地得到 $\boldsymbol{X}$ 和 $\boldsymbol{Z}$，从而得到错误 e。

2.2 经典二元 Goppa 码

经典 Goppa 码是一类线性码，它的最主要优点是某些子类可以达到 Gilbert-Varshamov 界。同时因为其有快速译码算法，且不等价码类的个数很大，因此自 1978 年 McEliece 用 Goppa码构造公钥密码体制以来，它开始被用于构造各种密码体制和消息认证码[12]。此处我们只考虑经典二元Goppa码。

定义 1[13] 设 $g(z)$ 为有限域 $\mathbb{F}_{2^m}$ 上次数为 t 的多项式。令 $L=\{\gamma_0,\gamma_1,\cdots,\gamma_{n-1}\}\subset\mathbb{F}_{2^m}$ 满足 $|L|=n$ 且 $g(\gamma_i)\ne0$，$0\le i\le n-1$，则Goppa多项式为 $g(z)$ 的Goppa码 $\Gamma(L,g(z))$ 定义为集合

$$\left\{ \boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in \mathbb{F}_2^n \left| \sum_{i=0}^{n-1}\frac{c_i}{z-\gamma_i}\equiv 0 \bmod g(z) \right. \right\}。$$

由定义 1 我们易知 Goppa 码 $\Gamma(L,g(z))$ 是由 L 和 $g(z)$ 唯一决定的二元线性码，且其参数为 $[n,k\ge n-mt,d\ge t+1]$。由有限域的相关计算结果我们可知Goppa码的不等价码类数目很大，也为用 Goppa 码构造公钥密码体制创造了条件。

3　量子公钥密码体制

3.1 体制描述

我们利用量子 CSS 纠错码的构造方法，一般经典线性码的译码问题是一个 NPC 问题和 Goppa 码有快速译码算法的特点给出一个量子公钥密码体制。

设 $C_i=\Gamma(L_i,g_i(z))=[n,k_i,d_i]$ $(i=1,2)$ 均为二元 Goppa 码，且 $C_1^{\perp}\subseteq C_2$，$d=\min\{d_1,d_2\}$，$t=\left\lfloor\frac{d-1}{2}\right\rfloor$，$k=k_1+k_2-n$。明文空间为 $\square^{2^k}$，密文空间为 $\square^{2^n}$。

密钥生成

随机选取 C_i 的生成矩阵 $\boldsymbol{G_i}$ 和校验矩阵 $\boldsymbol{H_i}$ $(i=1,2)$ 使得 $\boldsymbol{G}_2=\begin{pmatrix}\boldsymbol{H}_1\\ \boldsymbol{D}\end{pmatrix}$，则 $\boldsymbol{D}$ 的秩为 $k=k_1+k_2-n$。保密 $L_i,g_i(z)$ $(i=1,2)$ 作为私钥，公开 $\boldsymbol{G}_2,\boldsymbol{H}_1$ 作为公钥。

加密过程

随机选取错误 $e=\sigma_x^{[\boldsymbol{X}]}\sigma_z^{[\boldsymbol{Z}]}=(\boldsymbol{X}\mid\boldsymbol{Z})=(x_1,\cdots,x_n\mid z_1,\cdots,z_n)$, $w_{\mathrm{Q}}(e)\le t$。对于任意一个明文，即 k 个量子位的量子态 $|\varphi\rangle=\sum_{\boldsymbol{m}\in\mathbb{F}_2^k}\alpha_m|\boldsymbol{m}\rangle\in\square^{2^k}$，将其加密为

$$|\Psi\rangle=e\sum_{\boldsymbol{m}\in\mathbb{F}_2^k}\alpha_m|c_m\rangle \tag{3}$$

其中 $|c_m\rangle$ 如式(1)所示，e 的作用如式(2)所示。

这里需要说明的是量子计算过程是对量子态的酉演化过程。而量子态的酉演化均可以用有限个量子逻辑门(如量子 CNOT 门和单比特量子门)来实现。因此我们的加密过程可以用具体的量子线路来实现。首先设计编码线路完成编码操作

$$U_Q:\ U_Q(|\varphi\rangle|0\rangle)=U_Q\left(\sum_{\boldsymbol{m}\in\mathbb{F}_2^k}\alpha_m|\boldsymbol{m}\rangle|0\rangle\right)=\sum_{\boldsymbol{m}\in\mathbb{F}_2^k}\alpha_m|c_m\rangle=|\psi\rangle$$

这里 $|0\rangle$ 表示 $n-k$ 个辅助量子位，初态均制备为 $|0\rangle$。然后再对编码态 $|\psi\rangle$ 施加酉变换 e，从而得到加密态 $|\Psi\rangle=e\sum_{\boldsymbol{m}\in\mathbb{F}_2^k}\alpha_m|c_m\rangle$。

解密过程

(1)设 $\boldsymbol{H}_1^{(i)},\boldsymbol{H}_2^{(j)}$ 分别表示 $\boldsymbol{H}_1$ 的第 i 行和 $\boldsymbol{H}_2$ 的第 j 行，$1\le i\le n-k_1,1\le j\le n-k_2$。分别测量 $\sigma_x^{[\boldsymbol{H}_1^{(i)}]},\sigma_z^{[\boldsymbol{H}_2^{(j)}]}$ 的特征值 $(-1)^{z(i)}$ 和 $(-1)^{x(j)}$ $(z(i),x(j)\in\mathbb{F}_2)$，得到校验子 $\boldsymbol{Y}_1$ 和 $\boldsymbol{Y}_2$。即

$$\sigma_x^{[\boldsymbol{H}_1^{(i)}]}|\Psi\rangle=(-1)^{z(i)}|\Psi\rangle,\quad 1\le i\le n-k_1$$

$$\sigma_z^{[\boldsymbol{H}_2^{(j)}]}|\Psi\rangle=(-1)^{x(j)}|\Psi\rangle,\quad 1\le j\le n-k_2$$

$$\boldsymbol{Y}_1=(z(1),\cdots,z(n-k_1))$$
$$\boldsymbol{Y}_2=(x(1),\cdots,x(n-k_2))$$

这里需要说明的是在校验子测量线路中，我们引入辅助量子位来记录校验子，并不破坏加密态。

(2)求 $\boldsymbol{Z}=(z_1,\cdots,z_n)$，$\boldsymbol{X}=(x_1,\cdots,x_n)\in\mathbb{F}_2^n$ 使得

$$\boldsymbol{H}_1\cdot\boldsymbol{Z}^{\mathrm{T}}=\boldsymbol{Y}_1^{\mathrm{T}},\quad \boldsymbol{H}_2\cdot\boldsymbol{X}^{\mathrm{T}}=\boldsymbol{Y}_2^{\mathrm{T}}$$

则错误 $e=\sigma_x^{[\boldsymbol{X}]}\sigma_z^{[\boldsymbol{Z}]}$。由 2.1 节中的分析我们知道错误 e 是可以唯一得到的。

(3)纠错：$e|\Psi\rangle=|\psi\rangle$。根据上面求出的错误 $e=\sigma_x^{[X]}\sigma_z^{[Z]}$，对加密态 $|\Psi\rangle$ 实施酉变换 e，从而得到编码态 $|\psi\rangle$。纠错过程实质上是对出错比特位执行相应酉变换的过程，每一个比特位的酉变换都可以由一个 Pauli 矩阵来描述。这可以由具体的量子纠错线路来完成。

(4)译码：从 $|\psi\rangle$ 恢复出明文 $|\varphi\rangle$。量子译码线路实质是量子编码线路的逆过程，可以由一个多项式时间的量子线路族 $\{C_n\}$ 来实现，同时也可以用一个多项式时间的QTM来描述。

3.2 安全性分析

该方案是基于计算假设的公钥密码方案，其安全性建立在NPC问题对于QTM仍为难解问题的基础之上。用计算复杂度理论来分析，可以类似于经典复杂度类P，BPP，来定义量子计算复杂度类EQP，BQP。EQP定义为QTM在多项式时间内可以精确接受的一组语言，BQP定义为一组QTM可以以不小于 2/3 的概率在多项式时间内接受的语言。Bernstein等人[14]证明了 $P\subseteq$ EQP；BPP $\subseteq$ BQP $\subseteq$ PSPASE；Bennett等人[15]证明了对于随机均匀选择的oracle，QTM以概率 1 在时间 $o(2^{n/2})$ 内不能求解NP类问题。并同时证明对于随机均匀选择的置换oracle，QTM以概率 1 在时间 $o(2^{n/3})$ 内不能求解 NP $\cap$ co - NP 问题。可见 BQP 类并不比 NP 类大。到目前为止，尚没有有效的量子算法可以解决 NPC 问题。很多研究[6]认为： NPC 问题对于概率性QTM(PQTM)是难解问题。

我们提出的量子公钥密码体制，其安全性建立在一般线性码的译码问题是一个 NPC 问题和 Goppa 码有快速译码算法的基础之上，这与经典的 McEliece 公钥密码体制一致，因此可以抵抗已有的攻击，如 Lee-Brickell 攻击等。同时我们

知道 Goppa 码由 Goppa 多项式 $g(z)$ 和有序集 L 唯一决定。从公钥 G_2, H_1 若想获得 Goppa 码 C_1, C_2 的快速译码算法，即获得 $g(z)$ 和 L，利用 Grover 量子搜索算法的复杂度为 $O((2^{mt}n!)^{1/2})$，因此通过搜索攻破此量子公钥密码体制是不可行的。因此我们可以保证此量子公钥密码体制的计算安全性。当然，它也存在着需存储的密钥量大，信息率较低等弱点。

4 量子消息认证方案

4.1 认证方案

消息认证是与消息加密密切相关的密码方案。设想通信双方在一个不安全的通信信道上传递消息，有敌手可以控制信道并能够篡改传递的消息。消息认证的任务就是要判断一个由发送方发送的原始消息是否被篡改。利用上节给出的公钥密码体制，本文给出了一个基于量子 CSS 码的认证方案。方案描述如下。

密钥生成

每一个通信实体均利用第 3 节密钥生成算法随机生成各自的公钥和私钥。现在设 Alice 向 Bob 发送消息。Alice 和 Bob 协商好随机串 $\boldsymbol{k}=(\boldsymbol{k}_1 \mid \boldsymbol{k}_2) \in \mathbb{F}_2^{2k}$ 和 $e=(\boldsymbol{X} \mid \boldsymbol{Z}) \in \mathbb{F}_2^{2n}$，$w_Q(e) \le t$。

签名过程

(1) 设 Alice 发送的消息为 k 量子比特长的纯态 $|\phi\rangle = \sum_{\boldsymbol{m}\in\mathbb{F}_2^k} \beta_{\boldsymbol{m}} |m\rangle$。Alice 用密钥 $\boldsymbol{k}$ 加密 $|\phi\rangle$ 生成量子态

$$|\varphi\rangle = \sum_{\boldsymbol{m}\in\mathbb{F}_2^k} \beta_{\boldsymbol{m}} (-1)^{\boldsymbol{k}_2\cdot\boldsymbol{m}} |\boldsymbol{k}_1+\boldsymbol{m}\rangle = \sum_{\boldsymbol{m}\in\mathbb{F}_2^k} \alpha_m |\boldsymbol{m}\rangle \tag{4}$$

(2)Alice 利用 B 的公钥，如式(3)所示，将 $|\varphi\rangle$ 编码为 $|\Psi\rangle = e\sum_{\boldsymbol{m}\in\mathbb{F}_2^k} \alpha_{\boldsymbol{m}} |c_{\boldsymbol{m}}\rangle$。然后将 $|\Psi\rangle$ 发送给 Bob。

验证过程

(1)对于 Bob 来说，他收到的是一个 n 量子位的混合态，用 ρ' 表示。同第 3 节解密过程(1), (2)步，Bob 对 ρ' 进行校验子测量并计算出错误 e'。若 $e' \ne e$，则认证失败。否则，接受 ρ' 并按照第 3 节解密过程(3), (4)步纠错译码得到 ρ。

(2) Bob 用密钥 k 解密 ρ 得到明文消息 $|\phi\rangle$，解密过程为加密过程酉变换的逆变换。

4.2 安全性分析

定理 2 4.1 节中给出的认证方案是一个安全的消息认证系统，其合理性错误为 $O\left(2^{-2k}\left(\sum_{i=1}^{t}\binom{n}{i}3^i\right)^{-1}\right)$。

证明 协议的完整性：如果在整个通信过程中没有敌手 Adv 的介入，Bob 在通信后拥有的量子态 ρ' 与 Alice 发送的消息 $|\Psi\rangle\langle\Psi|$ 是相同的。那么 Bob 通过测量校验子计算出的错误 e' 和密钥 e 相同，则通过认证。因此认证方案满足完全性条件。

协议的合理性：加密过程(如式(4)所示)实质上是量子一次一密方案[4]。量子一次一密方案的特点是对于任何 k 个量子位的明文，密文都对应一个完全的混合态 $\frac{1}{2^k}I$。由量子力学原理，即使敌手 Adv 控制了通信信道，也无法从发送的量子态中得到关于明文 $|\phi\rangle$ 的任何信息。如果 Adv 随机制备一个混合态 ρ'，她只能以 $\frac{1}{2^{2k}}$ 的概率猜到正确的 k，以 $\left(\sum_{i=1}^{t}\binom{n}{i}3^i\right)^{-1}$ 的概率猜到 Alice 使用的错误 e。那么 Bob 收到 ρ' 后执行验证过程，Adv 欺骗成功的概率为 $O\left(2^{-2k}\left(\sum_{i=1}^{t}\binom{n}{i}3^i\right)^{-1}\right)$。因此此认证方案是一个合理性错误为 $O\left(2^{-2k}\left(\sum_{i=1}^{t}\binom{n}{i}3^i\right)^{-1}\right)$ 的安全的消息认证方案。证毕

5 结束语

本文利用量子 CSS 纠错码给出了一个以经典信息作为密钥加密量子消息的量子公钥密码体制。并利用此公钥体制给出了一个消息认证方案。基于量子纠错码的量子公钥密码体制的提出，拓宽了量子密码学的研究领域，对量子消息认证和数字签名方案的研究提供了新思路。

参考文献

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 1997, 26(5): 1484 – 1509.

[2] Grover L K. A fast Quantum mechanical algorithm for database search. Proc. of 28th Annual ACM Symposium on Theory of Computing (STOC), Philadelphia, Pennsylvania, USA, 1996: 212 – 219.

[3] Bennett C H, Brassard G. Quantum cryptography reinvented. *ACM SIGACT News*, 1987, 18: 51 – 53.

[4] Boykin P O, Roychowdhury V. Optimal encryption of quantum bits. http://arxiv.org/abs/ quant-ph/0003059, 2000.

[5] Okamoto T, Tanaka K, Uchiyama S. Quantum public-key cryptosystems. Proc. of Crypto'2000, Santa Barbara, California, USA, LNCS 1880, Springer, 2000: 147 – 165.

[6] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Physics Review Letter*, 2000, 85, 441 – 444.

[7] Barnum H, Crepeau C, Gottesman D, *et al*.. Authentication of quantum messages. Proc. of 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02), Vancouver, Canada, 2002: 449 – 458.

[8] Nielson M, Chuang I. Quantum Computation and Quantum Information. Cambridge, UK: Cambridge University Press, 2000: 425 – 493.

[9] 马智. 量子纠错码的研究及构造. [博士论文], 中国科学技术大学，2002 年 12 月.

[10] Calderbank A R, Shor P W. Good quantum error-correcting codes exist. *Physics Review A*, 1996, 54: 1098 – 1105.

[11] Steane A M. Multiple particle interference and quantum error correction. *Proc. Roy. Soc. Lond. A*, 1996, 452: 2551 – 2577.

[12] 王新梅，马文平，武传坤. 纠错密码理论. 北京: 人民邮电出版社，2001: 106 – 136.

[13] Van Lint J H. Introduction to Coding Theory. New York, USA: Springer Verlag, 1982: 107 – 115.

[14] Bernstein E, Vazirani U. Quantum complexity theory. *SIAM Journal on Computing*, 1997, 26(5): 1411 – 1484.

[15] Bennett C H, Bernstein E, Brassard G, *et al*.. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 1997, 26(5): 1510 – 1523.

李　峥：　男，1971 年生，副教授，研究方向为密码学、信息安全理论与技术. E-mail: lizheng_zz@sina.com

马　智：　女，1973 年生，副教授，研究方向为密码学、编码学和量子信息理论. E-mail: ma_zhi@163.com

吕　欣：　男，1977 年生，博士生，研究方向为网络信息安全理论与技术. E-mail: lx@is.ac.cn

冯登国：　男，1958 年生，研究员，博士生导师，信息安全国家重点实验室主任.研究方向为网络信息安全理论与密码学.