基于纠缠辅助码的量子模糊承诺和生物认证

曹 东[1,2],宋耀良[1]
(1. 南京理工大学电子工程与光电技术学院,江苏南京 210094;2. 南京邮电大学通信与信息工程学院,江苏南京 210003)

摘 要: 本文针对经典模糊承诺体制不能有效抵抗量子算法攻击的问题,在纠缠辅助量子纠错码的基础上,结合量子哈希构造一类新的量子模糊承诺体制.利用无需自对偶约束的量子纠错码空间构建模糊承诺集产生承诺阶段所需的码字,并对其施加用于模糊证明的加噪变换,有效抵抗量子傅立叶取样攻击;提出一种量子哈希,对随机量子序列进行混淆扩散后加密,实现信息论意义上的一次一密安全.据此构建的量子模糊承诺体制可有效抵抗量子图灵机攻击.该文还给出了基于量子模糊承诺的挑战响应生物认证方案,分别对量子模糊承诺和生物认证方案在量子计算环境下的安全性作了分析,证明了其安全性和有效性.

关键词: 信息安全; 量子纠错码; 模糊承诺; 生物认证
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2012) 07-1492-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.07.034

Quantum Fuzzy Commitment and Biometric Authentication Scheme Based on Entanglement-Assisted Quantum Error-Correcting Codes

CAO Dong[1,2], SONG Yao-liang[1]
(1. *School of Electronic Engineering and Optoelectronic Technology, Nanjing University of Science and Technology, Nanjing, Jiangsu* 210094, *China*;
2. *College of Communication and Information Engineering, Nanjing University of Posts and Telecommunication, Nanjing, Jiangsu* 210003, *China*)

Abstract: Fuzzy commitment based on classical cryptographic algorithms can not resist the attack of quantum algorithms. This paper presents a quantum fuzzy commitment by using entanglement-assisted quantum error correcting codes and quantum hash. Fuzzy commitment set can be constructed from the codes space of the entanglement-assisted quantum error-correcting codes, and the quantum codes need not satisfy the requirement of self-dual constraint. In commitment phase, the code word is transformed based on commitment witness. The information process can resist quantum Fourier sampling attack. Then, we present a quantum hash algorithm. The random qubits are adjusted with diffusion and confusion, and then encrypted by using the random secret key. The security of the process is same as the one-time pad. The proposed scheme can resist the attack of quantum Turing machines. Based on the quantum fuzzy commitment, this paper also gives a quantum challenge-response biometric authentication scheme. Theoretical analysis shows that our protocol has good security and validity.

Key words: information security; quantum error correcting codes (QECC); fuzzy commitment; biometric authentication

1 引言

模糊承诺最早由 Juels A 等人在文献[1]中提出,在模糊承诺中,承诺者对承诺比特做哈希,并且承诺的内容(比特形式)和承诺证明模 2 加,把这两个结果提供给接受者;打开阶段提交的承诺证明不必和承诺阶段的证明完全相同,两者可以是某种尺度上(比如汉明距离等)的相似值即可,接受者仍可以据此成功打开承诺并且确保绑定性.与比特承诺有着明显的区别,模糊承诺以其优异的属性在许多领域有着广泛应用.既要满足隐蔽性和绑定性,又可以以不同的承诺证明打开承诺,这种看似矛盾的约束条件因巧妙利用纠错码和密码学理论而得到完美统一.模糊承诺方案由于其承诺证明的模糊特性,被广泛应用于生物识别等安全验证系统中.Emanuele M 等人提出模糊承诺的签名模板保护算法[2],依据二值化签名算法提出一种可靠签名性状的选择步骤.文献[3]在人类感知模型的基础上,比较分析了感知哈希的应用模式和评测基准等方面的问题.文献[4]对模糊承诺过程中的信息泄露作了系统性的分析.2011 年,Emile J C K 等人[5]研究了针对模糊承诺策略中如何

收稿日期:2011-10-02;修回日期:2012-04-11
基金项目:国家自然科学基金(No.41074090,No.61071145);教育部博士点专项基金(No.200802880014)

阻止基于交叉匹配的可译码攻击,安全性基于经典哈希算法.

上述模糊承诺算法都是基于经典编码和经典密码方案的构造,对生物特征模板施以经典算法变换和处理.对于算法在后量子密码时代(post-quantum cryptography)的安全性没有作相应的分析和评估.遗憾的是,目前广泛使用的公钥密码体系比如 RSA 公钥密码、ElGamal 公钥密码、Diffie-Hellman 密钥交换以及相应哈希算法等等密码体制,在量子算法攻击下被证明是不安全的.因此经典模糊承诺的安全性受到严重威胁,研究基于量子计算环境下模糊承诺的安全问题就显得尤其迫切和重要.

量子纠错码的译码问题在文献[6]中被剑桥学者 Hsieh 等人证明是 NP 问题,本文在量子纠错码[7~9]和量子哈希函数基础上构造一种新的量子模糊承诺方案,信息处理过程可抵抗量子计算环境下的量子傅立叶取样攻击[10];接着在此基础上提出一种量子挑战响应生物认证协议,作为一种生物识别的应用,在生物统计学中的消息(比如指纹)本身在不同时间的样本就可能含有偏差(比如指纹采样方法或部位的不同导致的差异),所以在给消息添加冗余(即编码)存储模板的这种方法就不是太适用.本文提出的算法对生物特征先做量子化处理再作模糊距离变换后存储,较之其他同类算法的加密或经典哈希方法,既加强了生物特征信息的隐私安全保护性,又提高了验证过程的灵活性.

2　基于稳定子码的模糊承诺

编码 k 量子比特信息为码长 n 的稳定子码[7][$[n,k]$].由$(n-k)$个独立且对易的生成元 $M_1,\cdots,M_{n-k}$所定义,以 $M_j\in G_n, j=1,\cdots,n-k$ 为基底构成 n 量子位的 Pauli 算子群 G_n 的一个 Abel 子群 S.稳定子码 $C(S)=\{|\psi\rangle: M|\psi\rangle=|\psi\rangle, \forall M\in S\}$.忽略几率幅的码集第 j 个码字为:

$$|C_j\rangle_L=|c_{1,j}\cdots c_{k,j}\rangle_L=\Big[\prod_{i=1}^{n-k}(I+M_i)\Big]\bar{X}_1^{c_{1,j}}\cdots\bar{X}_k^{c_{k,j}}|0\cdots0\rangle$$
$$=\bar{X}_1^{c_{1,j}}\cdots\bar{X}_k^{c_{k,j}}\Big[\sum_{M\in S}M|0\cdots0\rangle\Big] \quad (1)$$

其中 $c_{1,j}\cdots c_{k,j}\in\{0,1\}, j=1,2,3,\cdots,2^k$, $C(S)=\{|C_1\rangle_L,|C_2\rangle_L,\cdots|C_j\rangle_L\cdots,|C_{2^k}\rangle_L\}$.

承诺阶段　Alice 随机选择 k 位量子比特序列$|k_j\rangle$编码为$|C_j\rangle_L$.$|k_j\rangle$作为待承诺量子比特序列.Alice 和 Bob 双方共同商定的量子哈希函数 $Q_H:\{|0\rangle,|1\rangle\}^n\to\{|0\rangle,|1\rangle\}^m$,其中 n,m 是正整数,一般情况下 $n\geqslant m$.作用于承诺比特$|k_j\rangle$得到 $Q_H(|k_j\rangle)$.随机选择与码字同构的量子伪码字$|\Phi\rangle$作为承诺证明.$|\Phi\rangle$与$|C_j\rangle_L$的广义模糊距离定义为 $\Delta=D(|\Phi\rangle,|C_j\rangle_L)$,其中$|\alpha\rangle$、$|\beta\rangle$和 $D(|\alpha\rangle,|\beta\rangle)$都表示相同长度的量子比特序列,如果序列$|\alpha\rangle$和$|\beta\rangle$中的对应项相同,则序列 $D(|\alpha\rangle,|\beta\rangle)$对应位置设置为$|0\rangle$,否则置为$|1\rangle$.然后,Alice 发送承诺$\{Q_H(|k_j\rangle),\Delta\}$给 Bob.

打开阶段　Alice 选择可纠错误集$\{E_l\}\in G_n$ 中满足条件的任一算子 E_τ,其中 G_n 为 n 量子比特 Pauli 群.选择条件是 $E_i,E_j\in\{E_l\}$,满足

$$E_i^\dagger E_j\in S\bigcup(G_n-N(S)) \quad (2)$$

其中 $N(S)$为对应于 S 的正规化子群.E_τ 作用得到$|\Phi'\rangle=E_\tau|\Phi\rangle$.发送承诺信息$|k_j\rangle$和模糊证明$|\Phi'\rangle$给 Bob.接受者 Bob 计算

$$Q_H(De(D(|\Phi'\rangle,\Delta)))=Q_H(De(D(|\Phi'\rangle,D(|\Phi\rangle,|C_j\rangle_L))))=\Xi \quad (3)$$

其中 $De()$为稳定子码译码算法.如果 $\Xi=Q_H(|k_j\rangle)$接收承诺$|k_j\rangle$,否则拒绝.

3　采用纠缠辅助量子纠错码的模糊承诺构造新方法

稳定子量子纠错码(包括 CSS 码)是对一类经典码的量子化构造,这类经典码必须满足对偶包含约束.这类约束条件对于短码情况下不难满足,但是对于高效率编码(比如 Turbo 码、LDPC 码等等码长较长的线性码)的量子化构造障碍较大.文献[12]提出纠缠辅助的方法有效地解决了这一困难,对于非对易稳定子群可以被嵌入到更大的空间而满足对易,无需满足对偶包含约束,就可以构造符合量子码空间定义的量子纠错码.该方法有效推广了量子码的构造法,即自正交经典码构造标准量子码,非自正交经典码构造纠缠辅助码.鉴于纠缠辅助量子纠错码的显著优点和广泛的应用价值,下面基于纠缠辅助量子码构造量子模糊承诺.

设群 $S=\{S_{iso},S_{sym}\}$即由子群 S_{iso}和 S_{sym}构造,两子群规模分别为 2^{n-k-c}和 2^{2c}.Alice 和 Bob 之间共享 c 个最大纠缠态(纠缠比特)$|\Phi\rangle^{\otimes c}$.Alice 利用纠缠辅助形式编码 k 量子比特消息$|\varphi\rangle$到码长 n 的纠缠辅助码

$$En:|\varphi\rangle\to|\varphi\rangle_L=\boldsymbol{U}^{-1}(|\boldsymbol{0}\rangle\otimes|\Phi\rangle^{\otimes c}\otimes|\varphi\rangle) \quad (4)$$

状态$|\boldsymbol{0}\rangle$表示 $l=(n-k-c)$辅助量子比特,其中幺正矩阵 $\boldsymbol{U}$ 满足 $S_0\boldsymbol{U}=\boldsymbol{U}S$

$$S_0=\{S_{0\_iso},S_{0\_sym}\},$$
$$S_{0\_iso}=\{Z_1,\cdots,Z_l\},$$
$$S_{0\_sym}=\{Z_{l+1},\cdots,Z_{l+c},X_{l+1},\cdots,X_{l+c}\} \quad (5)$$

构成码空间$\{|\varphi\rangle_L\}=\{|\varphi_1\rangle_L,|\varphi_2\rangle_L,\cdots,|\varphi_j\rangle_L,\cdots,|\varphi_{2^k}\rangle_L\}, j=1,2,3,\cdots,2^k$.纠缠辅助码可纠错误集 $\boldsymbol{E}_e$,对于所有 $E_a,E_b\in\boldsymbol{E}_e$, $E_a^\dagger E_b\in S_{iso}\bigcup(G_n-Z(\{S_{iso},S_{sym}\}))$.

承诺阶段　Alice 随机选择 k 位量子比特序列$|k_j\rangle$

(根据正交基$\{|0\rangle,|1\rangle\}$上)通过纠缠辅助量子纠错码编码为$|\varphi_j\rangle_L$(码集$\{|\varphi\rangle_L\}$).$|k_j\rangle$作为待承诺量子比特序列.Alice 根据量子哈希函数 $Q_{He}:\{|0\rangle,|1\rangle\}^n\rightarrow\{|0\rangle,|1\rangle\}^m$作用于承诺比特$|k_j\rangle$得 $Q_{He}(|k_j\rangle)$.选择与码字同构的量子伪码字$|\phi\rangle$作为承诺证明,计算任意错误算子 $E_1,E_2,\cdots,E_i,\cdots,E_t\in\boldsymbol{E}_e$ 作用$|\phi\rangle$得到模糊集

$$\{E_1|\phi\rangle,E_2|\phi\rangle,\cdots,E_i|\phi\rangle,\cdots,E_t|\phi\rangle\} \tag{6}$$

$|\phi\rangle$与$|\varphi_j\rangle_L$ 的广义模糊距离 $\Delta_e=D_e(|\phi\rangle,|\varphi_j\rangle_L)$.Alice 发送承诺$\{Q_{He}(|k_j\rangle),\Delta_e\}$给 Bob.

打开阶段 Alice 选择模糊集中的元素 $E_i|\phi\rangle$(表示为Δ_e')作为模糊证明和承诺信息$|k_j\rangle$一起发送给 Bob.接受者 Bob 首先计算模糊码字 $F_{Ci}=D_e(E_i|\phi\rangle,\Delta_e)$,接着计算

$$Dec_{EA}(F_{Ci})=\Big(\sum_{\boldsymbol{a},\boldsymbol{a}_1,\boldsymbol{a}_2}X^{a}Z^{b}|\boldsymbol{0}\rangle\langle\boldsymbol{0}|(X^{\boldsymbol{a}}Z^{\boldsymbol{b}})^{\dagger}|\boldsymbol{a}_1,\boldsymbol{a}_2\rangle\langle\boldsymbol{a}_1,\boldsymbol{a}_2|\otimes X^{\alpha(\boldsymbol{a},\boldsymbol{a}_1,\boldsymbol{a}_2)}Z^{\beta(\boldsymbol{a},\boldsymbol{a}_1,\boldsymbol{a}_2)}|\phi\rangle\Big)\hat{\boldsymbol{U}} \tag{7}$$

其中 $Dec_{EA}()$为纠缠辅助码译码算法,$|\boldsymbol{a}_1,\boldsymbol{a}_2\rangle=(Z^{a_1}X^{a_2}\otimes I^{B})|\Phi\rangle^{\otimes c}$[11].

然后计算散列值

$$Q_{He}(Dec_{EA}(F_{Ci}))=\Im \tag{8}$$

对比如果 $\Im=Q_{He}(|k_j\rangle)$,那么接收承诺$|k_j\rangle$,否则拒绝 Alice 的承诺.

4 基于量子模糊承诺的挑战响应生物认证

生物特征(比如指纹、虹膜等)即使是同一个体在不同时刻采样或采样时的细微差异,也会导致样本差异.所以给消息添加冗余实施编码这种方法不适用于此.本方案中不是将承诺信息作为信源消息进行编码,而是直接将不同个体生物特征对应到已构建的量子码字空间中的元素.本节提出一种基于量子模糊承诺的挑战响应生物验证协议.下面以指纹生物识别为例讨论量子挑战响应生物验证协议实现过程.

首先采集指纹特征图像进行预处理,在此过程中可以采用信源编码去冗余、考虑高灰度等级提高图像精度等等,这方面不是本文研究重点.简略计,将指纹图像从左到右从上到下按照二值图像黑点对应$|1\rangle$白点对应$|0\rangle$构建量子比特序列表示二维图像.接着与上文介绍的量子码字空间中的码字对照.选择空间中最接近的码字对应采样样本,以该码字取代采样样本作为模糊承诺信息.定义密钥生成算法和加解密算法[1]

$$KeyGen(|\psi\rangle)\Rightarrow\{PriK(|\psi\rangle),PubK(|\psi\rangle)\} \tag{9}$$

表示密钥生成算法 $KeyGen(|\psi\rangle)$根据种子$|\psi\rangle$生成的私钥 $PriK(|\psi\rangle)$和公钥 $PubK(|\psi\rangle)$.

$$Encry[PubK(|\psi\rangle),\Re] \tag{10}$$

表示加密算法 $Encry[\cdot]$利用公钥 $PubK(|\psi\rangle)$对消息 $\Re$ 加密.

$$Decry[PriK(|\psi\rangle),Messa] \tag{11}$$

表示解密算法 $Decry[\cdot]$利用私钥 $PriK(|\psi\rangle)$解密消息 $Messa$.

注册阶段的步骤如下:

(1)用户随机选取正交基$\{|0\rangle,|1\rangle\}$上的 k 位量子比特序列$|k_j\rangle$,系统通过纠缠辅助量子纠错码编码为$|\varphi_j\rangle_L$,认证系统计算散列 $Q_{He}(|k_j\rangle)$.

(2)用户提供注册指纹样本$|\phi\rangle$,由上述条件可知,该样本是正交基$\{|0\rangle,|1\rangle\}$上与码字$|\varphi_j\rangle_L$ 同长度的 n 量子比特序列,且其中量子比特$|1\rangle$总数(重量)大于纠缠辅助量子纠错码纠错能力 t.认证系统计算 $\Delta_e=D_e(|\varphi\rangle,|\varphi_j\rangle_L)$,构造模糊承诺集$\{Q_{He}(|k_j\rangle),\Delta_e\}$.

(3)认证系统计算 $KeyGen(|k_j\rangle)\Rightarrow\{PriK(|k_j\rangle),PubK(|k_j\rangle)\}$,然后存储用户注册信息集$\{PriK(|k_j\rangle),PubK(|k_j\rangle)\}\cup\{Q_{He}(|k_j\rangle),\Delta_e\}$.

认证阶段的步骤如下:

(1)用户提供认证指纹样本$|\phi'\rangle$(与注册时样本同源但必然有细微差异),尝试打开模糊承诺$\{Q_{He}(|k_j\rangle),\Delta_e\}$.

(2)如果成功打开承诺则获得$|k_j\rangle$,如果失败则回到第一步,持续数次失败中止认证.

(3)利用$|k_j\rangle$从 $KeyGen(|k_j\rangle)$获得$\{PriK(|k_j\rangle),PubK(|k_j\rangle)\}$.

(4)认证系统发送给用户一个随机消息 $Messa$,用户利用获得的私钥 $PriK(|k_j\rangle)$对该消息实施签名 $Decry[PriK(|k_j\rangle),Messa]=\xi$ 并提交认证系统.

(5)系统对比验证 $Encry[PubK(|k_j\rangle),\xi]$与 $Messa$,完全相同则验证通过.

本方法的优点是不直接存储用户生物特征信息(指纹),因此攻击者即使能够进入数据库也不能获得用户生物特征信息.也没有直接利用指纹作为唯一认证信息,而是作为模糊密钥使用,不用担心密钥更换的风险,极大降低密钥管理复杂度.

该生物认证协议安全性基于本文提出的量子模糊承诺,接下来予以分析.

5 安全性分析

本节讨论分析两方面的安全性,一方面分析量子模糊承诺满足隐蔽性和绑定性;另一方面是关于在此基础上构造的生物认证的安全性分析.

5.1 量子模糊承诺的安全性

首先分析隐蔽性,承诺阶段承诺者 Alice 提供$\{Q_{He}(|k_j\rangle),\Delta_e\}$,其中 Δ_e 和散列函数值 $Q_{He}(|k_j\rangle)$都分别包含$|\varphi_j\rangle_L$ 中部分信息,不诚实的 Bob 企图欺骗,希望在 Alice 打开阶段之前获得承诺信息$|k_j\rangle$.他可以通过两

条途径:(1)是尝试基于 Δ_e 猜测 $|\varphi_j\rangle_L$ 的估计值 $|\hat{\varphi}_j\rangle$ 进而译码得到 $|\hat{k}_j\rangle$;(2)是寻找散列函数 $Q_{He}(|k_j\rangle)$ 的碰撞值,寻求满足

$$Q_{He}(|k_j\rangle) = Q_{He}(|\hat{k}_j\rangle) \tag{12}$$

的 $|\hat{k}_j\rangle$ 值.先分析第一种情况:由于 Δ_e 包含 $|\varphi_j\rangle_L$ 的部分码结构信息,Bob 试图利用量子码译码方法得到承诺信息,Δ_e 是与 $|\varphi_j\rangle_L$ 同样 n 量子比特位的伪码字,并且其 $|1\rangle$ 总数大于纠错能力 t,如果 Bob 直接据此进行译码,由于超出量子纠错码的纠错能力,显然不可能得到正确码字 $|\varphi_j\rangle_L$.认证系统计算 $\Delta_e = D_e(|\phi\rangle, |\varphi_j\rangle_L)$ 的过程类似于量子纠错码受到的错误算子作用,结果是将其映射到子空间上,确实存在一般意义上的最优化译码,即根据错误校正子译码策略寻找最可能错误,寻找错误码字最接近的可能合法码字,即量子最大似然译码.文献[6]、[10]中详细证明了非简并量子最大似然译码和简并量子最大似然译码同等都是 NP 问题,并且此类问题即使是在量子傅立叶取样分析情况下也不能有效求解,即意味着量子图灵机不能有效对算法实施攻击.因此,在 Alice 未提供模糊证明前,也即在打开阶段之前 Bob 不能成功欺骗.接下来分析第二种攻击情况,即寻找哈希函数 $Q_{He}(|k_j\rangle)$ 的碰撞值,注册阶段用户随机选取的量子比特序列 $|k_j\rangle$ 是 2^k 维希尔伯特空间的项之一,Bob 为了猜测承诺比特 $|k_j\rangle$,相当于寻找和哈希值等于 $Q_{He}(|k_j\rangle)$ 码字,对于这一搜索复杂度直接决定于变量 k 的取值,一般情况下选取适当大的 k 使量子序列张成的 2^k 维希尔伯特空间足够大,可以避免产生碰撞做到所需安全的要求,具体在接下来的绑定性分析会进一步讨论,并且在生物认证安全性分析中结合量子哈希算法过程进行讨论.

绑定性分析,在承诺打开阶段如果不诚实 Alice 希望欺骗,即打开阶段呈现给 Bob 的是与当初承诺相异的比特,那么 Alice 就必须寻找哈希碰撞,即和哈希值 $Q_{He}(|k_j\rangle)$ 相同而与码字 $|\varphi_j\rangle_L(|k_j\rangle$ 对应的码字)不同的另外的码字比如 $|\varphi_j''\rangle_L$.并且更重要的前提是需要构造可以产生碰撞的承诺证明对 $(\Delta_e'', \Delta_e''')$,其中 Δ_e'' 是诚实承诺证明,Δ_e''' 是可以成功欺骗的承诺证明,但是 $D_e(\Delta_e', \Delta_e'')$ 和 $D_e(\Delta_e', \Delta_e''')$ 处于不相同邻域里,作为证明来看,Δ_e'' 和 Δ_e''' 不能被作为彼此代替的模糊承诺证明,因为假设在可以彼此替代的情况下,并且欺骗承诺证明 Δ_e''' 又可以提供译码得到欺骗承诺码字 $|\varphi_j'''\rangle_L$,同时其经过译码然后再哈希运算得到的结果等同于 $Q_{He}(|k_j\rangle)$,此条件无法满足.所以本方法确保 Alice 无法成功欺骗,即协议满足绑定性.

5.2　生物认证的安全性分析

与量子模糊承诺安全性相比,基于量子模糊承诺构造的挑战响应生物认证的安全性要关注的重点有所区别.前者关注承诺发送者与接收者之间的隐蔽性以及绑定性安全;后者关注的是访问者注册信息的存储(或传输)的安全,以及认证系统在接收访问者的认证过程避免被攻击者仿冒合法用户并通过欺骗侵入系统.

先分析注册信息的存储安全,在用户注册阶段系统会产生哈希值 $Q_{He}(|k_j\rangle)$ 和广义模糊距离 Δ_e 并存储在中心数据库,要求攻击者即使获取到数据 $\{Q_{He}(|k_j\rangle), \Delta_e\}$ 也不能够从中解读到任何有效信息.关于 $Q_{He}(|k_j\rangle)$ 的数据安全,先从量子哈希算法方面讨论:类似于经典哈希算法的首要要求是单向函数特性,在量子计算环境下,量子测量可以使量子态发生塌陷并且是一个不可逆过程,但是不适宜用于构造量子哈希函数.因为量子测量往往是对量子比特作正交化投影,导致的塌陷必然使得量子信息的丢失,而且这种信息丢失是不可预期的,会存在大量不同初始量子态经测量后塌陷到相同末态,这是发生了我们最不愿看到的所谓哈希碰撞.因此,类似于在经典哈希算法构造中有一大类是基于对称密码算法的,构造的映射关系 $H:\{0,1\}^n \to \{0,1\}^m$ 中,令 $n = m$(一般情况下是压缩映射,即 $n > m$),可以最大程度上避免碰撞发生.我们构造如下一种量子哈希算法,并以此分析哈希值的存储安全:构造半交换门(Semi-Swap)如图 1.

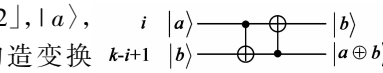

图1　半交换门

其中 $i = 1,2,\cdots,\lfloor k/2 \rfloor$,$|a\rangle$,$|b\rangle \in \{|0\rangle, |1\rangle\}$ 构造变换 $G[\cdot]$,作用于量子比特序列 $|k_j\rangle$ 实施混淆扩散得到新的 k 量子比特序列 $G[|k_j\rangle] = |\kappa_j\rangle^{\otimes k}$;接着构造如下算子集 $\{P_{uv}\} = \{I_{00}, X_{01}, Y_{10}, Z_{11}\}$,其中下标 $uv \in GF(2^2)$,I 是等同算子,X、Y 和 Z 是 Pauli 算子.以序列 $|k_j\rangle$ 一一映射到扩域 $GF(2^2)$ 上的序列 ζ 作为密钥,根据密钥从算子集 $\{P_{uv}\}$ 中选择对应算子,对 $G[|k_j\rangle]$ 实施变换 $\mathfrak{X}\{\cdot\}$:

$$\mathfrak{X}\{\zeta, G[|k_j\rangle]\} = (P_{uv}\{|\kappa_j\rangle\})^{\otimes k} \tag{13}$$

综合上面的所有变换过程,即得到量子哈希值 $Q_{He}(|k_j\rangle) = (P_{uv}\{|\kappa_j\rangle\})^{\otimes k}$.整个哈希过程首先是对序列 $|k_j\rangle$ 实施混淆扩散,然后是利用序列 $|k_j\rangle$ 确定密钥选择 $\{P_{uv}\}$ 中的算子分别对置乱 $|\kappa_j\rangle^{\otimes k}$ 逐位变换,实现等长加密,采用的密钥来自序列 $|k_j\rangle$ 本身,对于攻击者来说,即使算法公开,可是密钥未知由序列 $|k_j\rangle$ 决定,序列 $|k_j\rangle$ 是在每次注册阶段随机产生的,该加密过程的安全性类似于经典环境的一次一密密码,所以最后得到的哈希值的存储是安全的.

现在分析广义模糊距离 Δ_e 的数据安全,注册阶段认证系统计算 $\Delta_e = D_e(|\phi\rangle, |\varphi_j\rangle_L)$,在效果上可以把指

纹样本$|\phi\rangle$看成是信道错误矢量(噪声),作用于码字$|\varphi_j\rangle_L$,得到的结果为广义模糊距离Δ_e,相当于经过噪声信道作用的码字.由于指纹样本$|\phi\rangle$重量大于编码$|k_j\rangle$到$|\varphi_j\rangle_L$的纠错能力t,所以对于攻击者来说即使译码算法公开,也不能够正确译码得到$|k_j\rangle$,这一安全基于前述量子纠错码的译码是 NP 问题,此处不再累述.

接下来分析认证过程攻击者仿冒合法用户并通过欺骗侵入系统的问题,这一安全问题紧密关联刚才Δ_e的数据安全问题的分析:合法用户提供认证指纹样本$|\phi'\rangle$,应该是与注册时样本同源但必然有细微差异(这也是模糊承诺的实质),系统在认证阶段计算$\Delta_e' = D_e(\Delta_e, |\phi'\rangle)$,由于$|\phi\rangle$和$|\phi'\rangle$都是来自同一合法用户的指纹样本,存在细微差别但是在模糊阈值范围里,系统计算的Δ_e'相当于码字$|\varphi_j\rangle_L$中少于t位经过错误算子作用,因此可以被正确译码得到$|k_j\rangle$;可是如果攻击者提供认证指纹样本$|\varphi''\rangle$必然与$|\phi\rangle$相差较大且超过模糊阈值(在系统看来样本源来自不同个体,应予拒绝),系统执行$\Delta_e'' = D_e(\Delta_e, |\phi''\rangle)$再译码,由于$\Delta_e''$受到作用的错误序列的重量大于$t$,所以不能被成功译码得到$|k_j\rangle$,攻击者不能成功实施入侵.

6 结论

本文利用纠缠辅助量子纠错码和量子哈希函数给出了一个量子模糊承诺方案,并利用此承诺方案构造量子挑战响应生物认证方案.该量子模糊承诺方案的提出,推广了量子安全协议的研究领域,对量子身份认证和量子安全多方计算的研究提供了新的思路,进一步的研究可以包括多用户环境下多方量子模糊承诺以及提高量子生物识别性能与生物模板信息存储与传输的安全性.

参考文献

[1] Juels A, Wattenberg M. A fuzzy commitment scheme [A]. The 6th ACM Conference on Computer and Communications Security [C]. New York: ACM Press, 1999. 28 – 36.

[2] Emanuele M, Patrizio C. Fuzzy Commitment for Function Based Signature Template Protection [J]. IEEE Signal Processing Letters, 2010, 17(3): 249 – 252.

[3] 牛夏牧,焦玉华.感知哈希综述[J].电子学报,2008,36(7):1405 – 1411.
Niu Xia-mu, Jiao Yu-hua. An overview of perceptual hashing [J]. Acta Electronica Sinica, 2008, 36(7): 1405 – 1411. (in Chinese)

[4] Tanya I, Frans M J W. Information Leakage in Fuzzy Commitment Schemes [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 337 – 348.

[5] Emile J C K, Jeroen B, Tom A M K, Ileana B, and Raymond N J V. Preventing the Decodability Attack Based Cross-Matching in a Fuzzy Commitment Scheme [J]. IEEE Transactions on Information Forensics and Security, 2011, 6(1): 107 – 121.

[6] Hsieh M H, Francois L G. NP-hardness of decoding quantum error correction codes [J]. Physical Review A, 2011, 83(5): 052331.

[7] Gottesman D. A theory of fault-tolerant quantum computation [J]. Physical Review A, 1998, 57(1): 127 – 137.

[8] 肖芳英,陈汉武,刘志昊,李志强,刘文杰.有限域上非本原 BCH 码的对偶包含判定[J].电子学报,2010,38(8):1858 – 1861.
Xiao Fang-ying, Chen Han-wu, Liu Zhi-hao, Li Zhi-qiang, Liu Wen-jie. Dual-containing determination method for non-primitive BCH codes over finite field [J]. Acta Electronica Sinica, 2010, 38(8): 1858 – 1861. (in Chinese)

[9] Brun T, Devetak I, and Hsieh M H. Correcting quantum errors with entanglement [J]. Science, 2006, 314(5798): 436 – 439.

[10] Hang D, Cristopher M, Alexander R. The McEliece Cryptosystem Resists Quantum Fourier Sampling Attacks [EB/OL]. [2011-02-20]. http://arxiv.org/abs/arXiv:1008.2390.

[11] Brun T, Devetak I, and Hsieh M H. Catalytic quantum error correction. [DB/OL]. [2011-02-20]. http://arxiv.org/abs/0608027v2.

[12] Devetak I, Brun T, and Hsieh M H. Entanglement-assisted quantum error-correcting codes[A]. New Trends Mathematical Physics [C]. Heidelberg: Springer Science + Business Media Press, 2009. 161 – 172.

作者简介

曹 东(通讯作者) 男,1974 年生于江苏淮安,博士研究生,主要研究方向为量子信息与量子通信,量子纠错码,量子密码.
E-mail: caodongcn@gmail.com

宋耀良 男,1960 年生于江苏无锡,中国电子学会高级会员,教授,博士生导师,主要研究方向为自适应信号处理,量子信息、通信系统理论与设计.
E-mail: ylsong@mail.njust.edu.cn