文章编号:1007-5321(2019)04-0038-05 DOI:10.13190/j.jbupt.2018-287

高效的多比特量子公钥加密方案

郑世慧, 闻 楷, 谷利泽
(北京邮电大学 网络空间安全学院, 北京 100876)

摘要: 在量子计算机问世后,目前广泛使用的公钥密码体制将被破译,故而急需提出新的可替换的抗量子计算攻击的公钥密码体制. 结合量子比特旋转变换和经典的单向函数(Hash 函数)构建了一个多比特的量子公钥加密方案,分析结果显示,该方案可以抵制前向搜索和选择密文攻击,而且加密相同长度的明文所需的公钥量子比特数比 Kawachi 等的方案显著降低.

关 键 词: 多比特量子公钥加密; 选择密文攻击; 前向搜索攻击
中图分类号: O413 **文献标志码**: A

An Efficient Multi-Bit Quantum Public Key Encryption Scheme

ZHENG Shi-hui, WEN Kai, GU Li-ze
(School of Cyberspace, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: After the advent of quantum computers, the widely used public key cryptosystem will be broken, so it is urgent to propose new public key schemes to resistant quantum computing attacks. A single qubit-rotation transformation and classical one-way functions (Hash functions) are used to construct a multi-qubit quantum public key encryption scheme. The analysis results show that the new scheme is against the known forward search attack and a chosen ciphertext attack. Furthermore, the number of public key qubits used in the new scheme is obviously lower than that in the scheme presented by Kawachi et al.

Key words: multi-bit quantum public key encryption; chosen ciphertext attack; forward search attack

由于量子计算对经典公钥密码体制的威胁,基于格等困难问题的后量子公钥体制和基于量子物理特性的公钥体制受到广泛关注. 量子公钥加密方案简单归为 2 类:明文为未知状态的量子比特,或者明文为经典比特. 基于量子物理特性构造公钥密码体制的思想由 Gottesman 和 Chuang[1] 于 2001 年首次提出. 2005 年,Gottesman[2] 提出一个对量子态的公钥加密方案. 同年,Kawachi 等[3] 基于全翻转置换下量子态的不可区分性($QSCD_{ff}$, computational distinguishability of two quantum states generated via fully flipped permutations)问题提出首个对经典比特的加密方案,随后,他们将上述比特方案推广到一个基于全翻转循环置换下量子态的不可区分性($QSCD_{cyc}$, computational distinguishability of two quantum states generated via cyclic permutations)问题的多比特加密方案[4],其中公钥的长度随加密的明文长度呈线性增长. 2008 年,Nikolopoulos[5] 基于单量子比特旋转操作提出一个高效的方案,一年后,Nikolopoulos 等[6] 提出该方案的前向搜索攻击 (FSA, forward search attack),并以牺牲效率为代价提出一个改进方案. 2012 年,Seyfarth 等[7] 对改进方案给出一个新的攻击分析,但是攻击效果并不如前向搜索攻击. 2014

收稿日期: 2018-11-19
基金项目: 国家自然科学基金项目(61502048); 国家科技重大专项项目(2017YFB0803001)
作者简介: 郑世慧(1979—), 女, 副教授, E-mail: shihuizh@bupt.edu.cn.

年，Zheng 等[8]也提出一个改进方案，该方案有解密错误，但是其效率较文献[6]中的方案有所提高. 同年，Wu 等[9]提出一个基于量子搜索算法的多比特公钥加密方案（事实上，该消息的每个比特的加密都是相互独立）. 2015 年，Luo 等[10]基于量子完善加密提出一个量子比特方案；2018 年，Wu 等[11]基于 Bell 态也提出一个比特加密方案. 目前的量子公钥加密方案多是单比特的量子公钥加密，只有 Kawachi 等[4]将 $\mathrm{QSCD}_{\mathrm{ff}}$ 问题进行推广，构造了一个多比特的加密方案. 笔者首先基于 Nikolopoulos[5]在 2008 年提出的单比特旋转陷门函数给出一个多比特的量子公钥加密方案，从已知的惟公钥攻击、惟密文攻击（前向搜索攻击）和选择密文攻击等方面对其进行安全性评估；然后，从公钥使用量、密文扩展方面与 Kawachi 等[4]提出的多比特方案的效率进行对比分析，可以看出，在公钥长度方面具有明显优势. 此外，笔者提出的构造方式有望推广到其他单比特的方案，向多比特方案扩展.

1　Nikolopoulos[5]的单比特公钥加密方案

首先回顾一下 Nikolopoulos 在 2008 年提出的基于旋转变换的单比特加密方案. 令 $\{|0_z\rangle,|1_z\rangle\}$ 是 Hilbert 空间的一组正交基. 一个在 $x-z$ 平面上的量子比特可记为 $|\varphi(\theta)\rangle=\cos\frac{\theta}{2}|0_z\rangle+\sin\frac{\theta}{2}|1_z\rangle$，$\theta\in[0,2\pi)$.

定义一个绕轴 y 旋转的酉变换 $R_\theta(s)=\mathrm{e}^{-\mathrm{i}s\theta\gamma/2}$，其中 $\gamma=\mathrm{i}(|1_z\rangle\langle 0_z|-|0_z\rangle\langle 1_z|)$，$s$ 为整数，θ 取值同上. 显然，该酉变换满足交换律，即 $R_{\theta_1}(s_1)R_{\theta_2}(s_2)=R_{\theta_2}(s_2)R_{\theta_1}(s_1)$.

1.1　密钥生成

1）生成一个安全参数 n，令 $\theta_n=\frac{\pi}{2^n}$；

2）选择一个 n bit 长的随机整数 s；

3）制备一个量子比特 $|0_z\rangle$，并对该量子比特作酉变换 $R_{\theta_n}(s)$，则其状态变为

$$|\varphi(s\theta_n)\rangle=\cos\frac{s\theta_n}{2}|0_z\rangle+\sin\frac{s\theta_n}{2}|1_z\rangle \quad (1)$$

4）重复步骤 1）和 2）（至多重复制备 N_c 次）.

Alice 的公钥是量子比特 $|\varphi(s\theta_n)\rangle$（最多 N_c 份）；她的私钥是 (n,s).

1.2　加密过程

对于一个明文比特 $p\in\{0,1\}$，计算密文状态 $|c\rangle=R_\pi(p)|\varphi(s\theta_n)\rangle$.

1.3　解密过程

对于收到的量子比特 $|c\rangle$，首先计算 $|p\rangle=R_{\theta_n}(-s)|c\rangle$，然后对其测量，则可以 1 的概率恢复明文 p.

Nikolopoulos[5]提出基于 Swap Test 电路的前向安全搜索攻击，利用公钥的副本和密文量子态比较，从而以 3/4 的正确概率得到明文. 2009 年，Nikolopoulos[6]又提出一种 Symmetric Test 电路，将攻击成功的概率提高到 $q=(N-1)/N$，N 为攻击者可以获得的公钥副本个数. 为此，他们提出一个改进方案. 然而，为了使攻击者的优势 ε 可忽略，加密 1 bit 明文，密文扩展为 $O(N|\mathrm{lb}\varepsilon+1|)$ 量子比特. 上面描述的是 Nikolopoulos 在 2008 年提出的基础加解密方案. 为了方便下面多比特加密方案的描述，上述加密过程简记为 $\mathbb{E}(|\varphi(s\theta_n)\rangle,p)$，解密过程简记为 $\mathbb{D}(s,n,|c\rangle)$.

2　多比特公钥加密方案

方案同样分为密钥生成、加密和解密 3 个部分. 长消息被切割成固定长度的分块分别进行加密. 下面的方案中每块明文加密时可以使用一个公钥副本（$N_d=m+l+n'$），现实应用中也可以规定每个明文块加密使用某个公钥比特的 N_d 个副本.

2.1　密钥生成

1）生成一个安全参数 n，令 $\theta_n=\frac{\pi}{2^n}$；

2）选择一个随机数向量 $\boldsymbol{S}=(s_1,s_2,\cdots,s_{N_d})$，其中每个分量 $s_j(1\leqslant j\leqslant N_d)$ 都是两两独立的 n bit 长的随机整数；

3）制备 N_d 个量子比特 $|0_z\rangle^{\otimes N_d}$，并对第 j 个量子比特实施酉操作 $R_{\theta_n}(s_j)$，则其状态变化为

$$|\varphi(s_j\theta_n)\rangle=\cos\frac{s_j\theta_n}{2}|0_z\rangle+\sin\frac{s_j\theta_n}{2}|1_z\rangle \quad (2)$$

4）重复步骤 2）和 3）（至多重复制备 N_c 次）.

Alice 的每份公钥是 N_d 个量子比特串 $|\varphi_S(\theta_n)\rangle=\otimes_{j=1}^{N_d}|\varphi(s_j\theta_n)\rangle$，共制备 N_c 份；其私钥为 (n,S).

令 H、G 和 W 分别是输出为 $m+l$、n' 和 l bit 的 Hash 函数.

2.2　加密过程

将明文切割成 m bit 长的块分别进行加密，当不足 m bit 时，填充到 m bit（填充一个结束位 1 和足够多的 0）；每个明文块 M 分别执行下述步骤进行

加密:

1) 选择一个 n' 比特的随机数 r;

2) 计算 $\alpha = W(M \| r)$;

3) 计算 2 个中间值 $t_1 = H(r) \oplus (M \| \alpha)$ 和 $t_2 = G(t_1) \oplus r$;

4) 使用第 1 节中的加密算法逐比特加密比特串 $T = t_1 \| t_2$ 得到密文量子比特串;

$$|C\rangle = \otimes_{j=1}^{m+n'+l} |c_j\rangle = \otimes_{j=1}^{m+n'+l} |\mathbb{E}(\varphi(s_j\theta_n), T_j)\rangle \tag{3}$$

2.3 解密过程

1) 使用第 1 节中的解密算法从密文量子态 $|C\rangle = \otimes_{j=1}^{m+n'+l} |c_j\rangle$ 中逐一恢复出中间比特串 $T' = T'_1 T'_2 \cdots T'_{m+n'+l}$,其中 $T'_j = \mathbb{D}(s_j, n, |c_j\rangle)$, $j = 1, 2, \cdots, m+n'+l$;

2) 将 T' 分成两份,T' 的前 $m+l$ bit 记为 t'_1,后 n' bit 记为 t'_2;

3) 顺序计算 $r' = G(t'_1) \oplus t'_2$ 和 $T'' = H(r') \oplus t'_1$;

4) 取 T'' 的前 m bit 记为 M',后 l bit 记为 α';

5) 计算 $W(M' \| r')$ 并与 α' 比较,若相等,则输出 M';否则程序终止.

当所有的密文块顺利执行完上述解密操作后,解密程序停止.

3 安全性分析

3.1 私钥安全性

Alice 的每份公钥是 N_d 长的量子比特串 $|\varphi_S(\theta_n)\rangle = \otimes_{j=1}^{N_d} |\varphi(s_j\theta_n)\rangle$,共制备 N_c 份;其私钥是 (n, S). 简单来说,lb$n$ 表示每个量子公钥比特包含的信息比特数(经典). 根据 Holevo 定理[12]可知,每份公钥长度 N_d 和公钥的总份数 N_c 满足下列条件:

$$\mathrm{lb}(n_1 - n_2) + N_d \left(\frac{n_1 + n_2}{2}\right) \geqslant N_d N_c \tag{4}$$

其中 $n \in [n_1, n_2]$,n_1、n_2 为大整数. 则攻击者 Eve 不可能从他获取的 N ($N \leqslant N_c$) 份公钥副本中得到 Alice 的私钥信息.

3.2 前向搜索攻击

假设攻击者可以在信道上截获密文,并进行前向搜索攻击. 下面以密文仅为 1 块为例,分情况讨论攻击者成功的概率.

情况 1 假设攻击者可以利用 Symmetric Test 电路,在解密过程的第 1 步完全正确地恢复 T' 的所有比特,那么攻击者可完全正确恢复明文块 M. 已知 Symmetric Test 电路正确恢复每个经典比特的概率为 q,那么此时攻击成功的概率为 $\Pr_1 = q^{m+n'+l}$.

由文献[6]可知,对于 $1-N$ 比较问题,当 2 个粒子不相等时仍然输出 0 的概率(错误概率)为 $\frac{1+N\lambda^2}{N+1}$,其中 N 为攻击者可以获得的公钥副本份数,λ 为被比较的 2 个量子态的内积模(此时 $\lambda = 0$);而当 2 个粒子相等时,$\lambda = 1$,Symmetric Test 电路以 1 的概率输出 0(正确概率),所以

$$\begin{aligned} q &= \Pr[\text{output} = 0 \,|\, \text{equal}] \cdot \Pr[\text{equal}] + \\ &\Pr[\text{output} = 1 \,|\, \text{unequal}] \cdot \Pr[\text{unequal}] = \\ &1 \cdot \frac{1}{2} + \left(1 - \frac{1}{N+1}\right) \cdot \frac{1}{2} = \frac{2N+1}{2(N+1)} \end{aligned} \tag{5}$$

情况 2 假设攻击者利用 Symmetric Test 电路,在解密过程的第 1 步恢复出的 T' 有错误,那么攻击者成功的概率为 $\Pr_2 = \frac{1}{2^m}(1 - q^{m+n'+l})$.

假设攻击者利用 Symmetric Test 电路恢复出的 t'_1 有 a bit 正确(条件成立的概率为 $q^a(1-q)^{m+l-a}$,t'_2 有 b bit 正确(条件成立的概率为 $q^b(1-q)^{n'-b}$),那么攻击者可以在步骤 2) ~ 5) 恢复正确明文块的概率为 $1/2^m$,换句话说,将 H 和 G 看作是随机函数,那么,攻击者使用错误的 t'_1(或者 t'_2)计算出的 $T'' = H(G(t'_1) \oplus t'_2) \oplus t'_1$ 的前 m 个比特正确的概率为 $1/2^m$. 因此,

$$\begin{aligned} \Pr_2 = &\left[\sum_{a=1}^{m+l-1} q^a(1-q)^{m+l-a} \sum_{b=0}^{n'} q^b(1-q)^{n'-b} \cdot \frac{1}{2^m}\right] + \\ &\left[q^{m+l} \sum_{b=0}^{n'-1} q^b(1-q)^{n'-b} \cdot \frac{1}{2^m}\right] = \\ &\frac{1}{2^m}\left[\sum_{a=0}^{m+l} q^a(1-q)^{m+l-a} \sum_{b=0}^{n'} q^b(1-q)^{n'-b} - \right. \\ &\left. q^{m+l} q^{n'}\right] = \frac{1}{2^m}(1 - q^{m+n'+l}) \end{aligned} \tag{6}$$

由上述 2 种情况可知,攻击者成功恢复 1 块明文的概率为

$$\Pr = \Pr_1 + \Pr_2 = \frac{1}{2^m} + q^{m+l+n'} - \frac{1}{2^m} q^{m+l+n'} \tag{7}$$

特别地,当明文长度为 1 bit 时,该方案中攻击者的优势为

$$\begin{aligned} A &= \Pr - \frac{1}{2} = \\ &\left(\frac{1}{2} + q^{1+l+n'} - \frac{1}{2} q^{1+l+n'}\right) - \frac{1}{2} = \frac{q^{1+l+n'}}{2} \end{aligned} \tag{8}$$

与 Nikolopoulos 等[6]提出的方案类似,若要上述优

势可忽略，即$A=\frac{q^{1+l+n'}}{2}<\varepsilon$，那么$l+n'\geqslant\left|\frac{1+\mathrm{lb}\varepsilon}{\mathrm{lb}q}\right|$.

在式(5)中，当N较大，即攻击者获得较多公钥副本，若要使攻击者优势可忽略，则$l+n'$非常大，意味着加密 1 bit 明文时，密文扩展非常大. 假设$N_d\leqslant N_c$，那么加密 1 块消息可以使用公钥$\varphi(s_j\theta_n)$的N_d个副本，若$[N_c/N_d]=N+1$较小，则密文扩展较低.

3.3　选择密文攻击

在上述前向搜索攻击中，假设攻击者只能截获到密文，事实上，对于攻击者还可能对截获到的密文C^*进行伪装$\overline{C}$，将伪装后的密文发送给解密预示请求解密，然后根据解密预示返回的明文$\overline{M}$(伪装的密文$\overline{C}$所对应的明文)，计算获取截获到密文C^*所对应明文M^*，称之为选择密文攻击.

对于文献[5-6]中提出的方案，攻击者只需要对截获到密文的每个量子状态进行旋转操作$R_\pi(u_j)$，$u_j\in\{0,1\}$，若共有奇数个u_j取值为 1，则令M^*的值与解密预示返回值$\overline{M}$相反；否则令M^*的值等于解密预示返回值$\overline{M}$.

然而，上述多比特方案中，攻击者很难成功实施选择密文攻击，因为有如下 2 种情况.

情况 1　如果攻击者修改了密文C^*(此处的修改特指对密文量子态执行$R_\theta(u_j)$操作，其中$u_j=1$，$1\leqslant j\leqslant m+l+n'$，$0<\theta<\pi$. 首先在解密预示进行第 1 步操作时，若某个$u_j=1$，将以平均 1/2 的概率使得$\overline{T}$第$j$ bit 翻转.

首先，以$\overline{T}$第j bit 由 0 翻转为 1 为例，则表示在该比特测量前状态由$|0_z\rangle$被攻击者篡改成了$\cos\frac{\theta}{2}|0_z\rangle+\sin\frac{\theta}{2}|1_z\rangle$，此时进行测量得到$|1_z\rangle$的概率为$\sin^2(\theta/2)$，因为$0<\theta<\pi$，故平均概率为$\frac{1}{\pi}\int_0^\pi\sin^2(\theta/2)\,\mathrm{d}\theta=1/2$.

其次，经过第 2)～4)步解密操作后，恢复出的$\overline{M}$、$\overline{r}$和$\overline{\alpha}$满足$W(\overline{M}\,\|\,\overline{r})$与$\overline{\alpha}$相等的概率为$1/2^l$. 如果$l$足够大，则第 5)步解密预示以很大的概率检测出密文被篡改，那么解密预示直接停止，攻击者无法拿到$\overline{M}$.

另一方面，即使篡改没有被检测到，攻击者很难获得$\overline{T}$(未知)经过H、G的扩散和混淆作用后生成的$\overline{M}$与目标明文M^*的关系，故攻击者无法从解密预示返回的明文$\overline{M}$获得目标明文M^*的信息，只能随机猜测M^*.

情况 2　如果攻击者修改了密文C^*(此处的修改特指$R_\pi(u_j)$操作，其中$u_j=1$，$1\leqslant j\leqslant m+l+n'$)，那么，解密预示执行完解密第 1)步解密操作后，比特串$\overline{T}$第j bit 以 1 的概率发生翻转. 同理，经过第 2)至 4)步解密操作后，恢复出的$\overline{M}$、$\overline{r}$、$\overline{\alpha}$满足$W(\overline{M}\,\|\,\overline{r})$与$\overline{\alpha}$相等的概率为$1/2^l$. 如果$l$足够大，则第 5)步解密预示以很大的概率检测出密文被篡改，那么解密预示直接停止，攻击者无法拿到$\overline{M}$. 同样，即使篡改没有被检测到，$\overline{T}$(未知)经过H、G的扩散和混淆作用后生成的$\overline{M}$与目标明文M^*的关系攻击者很难获得，故攻击者无法从解密预示返回的明文$\overline{M}$获得目标明文M^*的信息，只能随机猜测M^*.

综上所述，攻击者试图通过上述选择密文攻击恢复明文的复杂度小于直接猜测M^*的概率.

注意，上述分析中没有考虑下列情况：如果攻击者修改了密文C^*(此处的修改特指对密文量子态执行$R_\theta(u_j)$操作($u_j=1$，$1\leqslant j\leqslant m+l+n'$，$0<\theta<\pi$)，则在解密预示进行第 1 步操作时，若某个$u_j=1$，将以平均 1/2 的概率使得$\overline{T}$第$j$ bit 保持不变，此时，攻击者将获得和目标明文M^*完全一致的返回明文$\overline{M}$. 因为在经典密码中，若攻击者发送给解密预示的请求密文$\overline{C}$与攻击者的目标密文C^*相同，则通过日志和审计系统容易发现. 然而在量子攻击中，对量子比特状态的变化不容易监测，所以，在攻击模型中，应该将上述条件修改为攻击者解密预示返回的明文$\overline{M}$与攻击者的目标明文M^*不同.

4　效率分析

Kawachi 等[4]提出的多比特方案中，明文为 lb$m$经典比特，每份公钥长为m个量子态，每个量子态为$O(n\mathrm{lb}n)$量子比特(n为安全参数)，私钥为$O(n\mathrm{lb}n!)$量子比特，密文为$n\mathrm{lb}n$量子比特.

Hayashi 等[13]证明若攻击者获得公钥的界为$N=O(n\mathrm{lb}n/(m\mathrm{lb}m))$，则该多比特方案具有信息论不可区分性.

第 2 节提出多比特量子公钥加密方案中，明文分块长度为m经典比特，每份公钥长为N_d个量子比特(至多生成N_d份，$N\leqslant N_c$)，私钥为$\mathrm{lb}n+nN_d$经典比特(n为安全参数)，密文为$m+n'+l$量子比特.

设攻击者利用前向搜索攻击，成功恢复明文的概率为$\Pr=\frac{1}{2^m}+q^{m+l+n'}-\frac{1}{2^m}q^{m+l+n'}$，若要其概率近

似于随机猜测目标明文的 M^* 的概率 $1/2^m$，那么，$q^{m+n'+l}(1-1/2^m)<q^{m+n'+l}<\varepsilon$，$\varepsilon$ 为一个可忽略的数，$q=(2N+1)/2(N+1)$（N 为攻击者可以获得的公钥拷贝份数）. 密文长度满足下列条件 $m+n'+l\geqslant\frac{\ln\varepsilon}{\ln q}>\frac{|\ln\varepsilon|}{\ln(2N+2)}$，进一步约为 $m+n'+l\geqslant\frac{\ln\varepsilon}{\ln q}>\frac{n}{\ln(2N+2)}$，因为 n 为安全参数，故而 $\varepsilon\leqslant\frac{1}{2^n}$.

显然，同样的明文分块长度下，Kawachi 等[4]方案中的公钥随安全参数 n 增长而使指数增长，而新方案呈线性增长趋势；但是 Kawachi 等[4]的方案中密文扩展是安全参数的多项式函数，由于新方案前向搜索攻击，密文扩展亦随安全参数 n 增长而线性增长.

5 结束语

提出了一种新的多比特（明文为经典比特串）量子公钥加密方案，并使用目前已知的攻击方法对其进行了安全分析，结果表明，在安全参数足够大的情况下新方案是安全的. 直观上看，笔者提出的构造方法同样适用于将其他比特方案[3,8-11]扩展为多比特方案，也就是加密的第4）步替换为使用其他逐步特加密算法依次加密 $T=t_1\parallel t_2$. 此外在保障安全的前提下是否可以进一步简化加解密过程，或者如何在特殊应用，如图像信息加密[14-16]场景下优化方案效率，是下一步需要探讨的问题.

参考文献：

[1] Gottesman D, Chuang I. Quantum digital signatures[EB/OL]. 2001(2001-05-08)[2018-05-16]. https://arxiv.org/abs/quant-ph/0105032.

[2] Gottesman D. Quantum public key cryptography with information-theoretic security [EB/OL]. 2005(2005-12-08)[2018-05-16]. https://www.perimeterinstitute.ca/personal/dgottesman/Public-key.ppt.

[3] Kawachi A, Koshiba T, Nishimura H, et al. Computational indistinguishability between quantum states and its cryptographic application[C]// Advances in Cryptology-EUROCRYPT 2005, Lecture Notes in Computer Science. New York: Springer, 2005: 268-284.

[4] Kawachi A, Koshiba T, Nishimura H, et al. Computational indistinguishability between quantum states and its cryptographic application [J]. Journal of Cryptology, 2012, 25(3): 528-555.

[5] Nikolopoulos G M. Applications of single-qubit rotations in quantum public-key cryptography[J]. Physical Review A, 2008(77): 032348.

[6] Nikolopoulos G M, Ioannou L M. Deterministic quantum-public-key encryption: forward search attack and randomization [J]. Physical Review A, 2009(79): 042327.

[7] Seyfarth U, Nikolopoulos G M, Alber G. Symmetries and security of a quantum-public-key encryption based on single-qubit rotations [J]. Physical Review A, 2012(85): 022342.

[8] Zheng Shihui, Gu Lize, Xiao Da. Bit-oriented quantum public key probabilistic encryption schemes [J]. International Journal of Theoretical Physics, 2014, 53(1): 116-124.

[9] Wu C, Yang L. Bit-oriented quantum public-key encryption based on quantum perfect encryption [J]. Quantum Information Processing, 2016(15): 3285.

[10] Luo Wenjun, Liu Guanli. Asymmetrical quantum encryption protocol based on quantum search algorithm [J]. China Communications, 2014(9): 104-111.

[11] Wu W, Cai Q, Zhang H, et al. Bit-oriented quantum public-key cryptosystem based on bell states [J]. International Journal of Theoretical Physics, 2018 (57): 1705.

[12] Holevo A S. Statistical problems in quantum physics [C]// Proceedings of the Second Japan-USSR Symposium on Probability Theory, Lecture Notes in Mathematics. Berlin: Springer-Verlag, 1973: 104-119.

[13] Hayashi M, Kawachi A, Kobayashi H. Quantum measurements for hidden subgroup problems with optimal sample complexity [J]. Quantum Information and Computation Journal, 2008(8): 345-358.

[14] Zhou Nanrun, Chen Weiwei, Yan Xingyu, et al. Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system [J]. Quantum Information Processing, 2018, 17(6): 137.

[15] Zhou Nanrun, Yan Xingyu, Liang Haoran, et al. Multi-image encryption scheme based on quantum 3D Arnold transform and scaled zhongtang chaotic system [J]. Quantum Information Processing, 2018, 17(12): 338.

[16] Zhou Nanrun, Hua Tianxiang, Gong Lihua, et al. Quantum image encryption based on generalized Arnold transform and double random phase encoding [J]. Quantum Information Processing, 2015, 14(4): 1193-1213.