一种基于密钥回收的量子加密算法*)

李恕海　王育民

(西安电子科技大学综合业务网络国家重点实验室　西安 710071)

摘　要　基于Damgard等人的密钥回收算法，提出了一种更有效的新型量子加密算法。使用通用的哈希函数来检测窃听，如果没有监测到窃听，加解密双方共享的密钥可以被安全地重复使用，否则需要抛弃并重新协商与明文等长的密钥串。在加密经典明文的同时，也为剩余未加密的明文协商密钥。当协商好的密钥量与剩余的明文相同时，就可以使用一次一密来加密从而避免反馈是否存在窃听以及重新协商密钥的过程，显著提高了加密效率。

关键词　量子密码学，密钥回收，认证加密

An Efficient Quantum Cipher with Key Recycling Scheme

LI Shu-Hai　WANG YU-Min

(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)

Abstract　Based on the quantum key recycling scheme, a novel efficient quantum cipher is proposed. Employing the universal hashing functions to detect eavesdropping, if there is no any eavesdropping detected, then the two parties can recycling the whole key without comprising security, otherwise a key string with the length of plaintext block has to be discarded. The keys used to encrypt the remaining plaintext block in classical one time pad are also generated to avoid the feedback on whether there exists eavesdropping during the process of quantum encryptions. Such strategy improves the efficiency of the quantum key recycling scheme greatly.

Keywords　Quantum cryptology, Key recycling, Authenticated encryptions

作为唯一可证明无条件安全的密码学资源，量子密码正逐渐接近实际的安全领域。除了实现安全的量子密钥协商[2]以外，能加密量子和经典信息的量子加密算法[1,3,5]也不断出现，并在各类安全性指标上同样具有明显的优势。本文提出了一种有效的量子加密算法，利用量子密码学的窃听监测特性在加密经典明文信息的同时，又融合了密钥协商，通过认证码来检测窃听者Eve的不合法行为。如果没有发现窃听原密钥，可以回收重复使用，从而将两类量子密码体制有效地结合起来，提高了加密信息的效率。

1　量子加密算法与Hash函数描述

这里使用文[4]提出的H_1作为基本的加密单元。Alice向Bob发送使用量子状态加密的经典明文$m\in P=\{0,1\}^{2l}$，它们共享一串经典的密钥比特$(k,r)\in P=\{0,1\}^{2l}$，得到的量子密文$|c\rangle=H^kX^r(|m\rangle)=H^k(|m\oplus r\rangle)$。这里$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$是Hadamard变换，$X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$是比特翻转变换，$H^kX^r=H^{k_1}X^{r_1}\otimes H^{k_2}X^{r_2}\otimes\cdots\otimes H^{k_l}X^{r_l}$即根据$k_i$和$r_i$($k$和$r$的二进制表达式的第$i$位)的值来决定是否在第$i$个量子比特上执行$H$和$X$，这等价于BB84[2]编码。当Bob收到$|c\rangle$后，使用$H^kX^r$的逆变换$X^rH^k$恢复出$|m\rangle$，然后使用平行测量基$\{|0\rangle,|1\rangle\}$测量得到$m$。下面考虑该量子加密算法的安全特性。

对任意的(k,r)和$(k',r')\in P=\{0,1\}^{2l}$，注意到

$$\sum_{m\in P}\frac{1}{2^{2l}}H^kX^r|m\rangle\langle m|X^rH^k=\sum_{m\in P}\frac{1}{2^{2l}}H^{k'}X^{r'}|m\rangle\langle m|X^{r'}H^{k'} \quad (1)$$

任何密钥加密m都会生成同样的密度矩阵，确保了密钥的安全性[4]。同样，对任意的m和m'，

$$\sum_{k,r\in P}\frac{1}{2^l}H^kX^r|m\rangle\langle m|X^rH^k=\sum_{k,r\in P}\frac{1}{2^l}H^kX^r|m'\rangle\langle m'|X^rH^k \quad (2)$$

任何明文都被加密成同样的密度矩阵，保证了明文信息的安全性[1]。为了验证明文信息的有效性，Alice和Bob需要如下函数集。

Hash函数集：$H_{2l,\mu}=\{h_u:\{0,1\}^{2l}\to\{0,1\}^{\mu},\ u\in\{0,1\}^{\mu}\}_u$是一族满足如下条件的函数，对于任意的$a\neq b\in\{0,1\}^{2l}$，碰撞概率满足：

$$Pr(h_u(a)=h_u(b)|a\neq b)<2^{-\mu} \quad (3)$$

2　密钥的回收与协商

Alice和Bob之间可以通过量子信道和认证的公开经典信道进行通信，窃听者Eve在认证经典信道上可以做被动攻击，即可以窃听Alice和Bob的经典通信但不能更改；在量子信道上可以做主动攻击，即她可以对Alice和Bob之间发送的量子做任何转换和测量。假设Alice要加密的经典明文序列为$\{m_i\}$，$\{m_i\in P,1\leqslant i\leqslant N\}$，Alice和Bob共享长为$4l+3\mu$比特的随机初始密钥串$(\hat{k},\hat{r},u)=(k_1k_2k_3,\ r_1r_2r_3,\ u)$，$k_i,r_i\in P\ (i=1,2)$，以及$k_3,r_3,u\in\{0,1\}^{\mu}$，使用量子加密算法$H_1$加密明文$m_i$，随机数$s_i\in P$和认证码$R=h_u(m_i\|s_i)$。并设置计数器$I$来记录Alice和Bob使用$h_u$认证成功的次数。

1) Alice加密消息m_i，密文分为三个部分

$$|c_i\rangle=H^{k_i}X^{\hat{r}_i}(m_i,s_i,R)=H^{k_1}(|m_i\oplus r_1\rangle)\otimes H^{k_2}(|s_i\oplus r_2\rangle)\otimes H^{k_3}(|R\oplus r_3\rangle) \quad (4)$$

2) Bob使用$(\hat{k},\hat{r},u)$解密$|c_i'\rangle$，得到$X^{\hat{r}}H^{\hat{k}}|c_i'\rangle$，然后

*)国家自然科学基金资助项目(60473027)。李恕海　博士研究生。

使用平行基测量得到的量子状态，分别得到 m'，s'，R'。然后进入认证阶段，如果 $R'=h_u(m'\|s')$ 成立，那么 Bob 就认为加密有效，即 $|c_i'>$ 来自 Alice 而不是 Eve，$(\hat{k},\hat{r},u)$ 可以被安全地回收并且 I 增加 1 次。否则，Alice 和 Bob 抛弃与 m 长度相同的密钥串，同时 I 减少一次。如果 $I>0$，那么用 s_I 代替抛弃的 l 个比特然后重新加密。当 $I=0$ 时，Alice 和 Bob 重新协商 l 个比特的密钥。

3) 如果认证成功的次数 $I\geqslant N/2$，那么 Alice 和 Bob 回收所有相应的 $\{s_j\}$，使用一次一密的方法来加密剩余的明文 $\{m_{i+1},\cdots,m_N\}$，得到 $c_{i+j}=m_{i+j}\oplus s_j$ $(1\leqslant j\leqslant I)$，然后发送给 Bob。Bob 使用同样的 $\{s_j\}$ 解密恢复出 m_{i+j}。

3 安全性分析

明文的安全性以及唯密文攻击由式(1)，(2)可以保证，下面考虑已知明文攻击下的密钥安全性。我们使用量子信息论分析 Eve 的攻击策略。假设有 $n=2^{2(2l+\mu)}$ 个状态 $\rho_X=|c_i><c_i|$，Alice 选取密文 ρ_X 的概率为 p_X，$X=0,\cdots,n$。Eve 必须测量 ρ_X 来获得信息，其测量策略可以用 POVM 测量描述，其测量算子 $\{E_y\}=\{E_0,\cdots,E_m\}$，满足 $\forall y$，$E_y=E_y^+$，$\sum_y E_y=I_n$（I_n 表示 n 维的单位矩阵）。测量结果为 $y\in Y$，所以 Eve 对 ρ_X 进行测量获得有关 X 的信息量可表示为

$$H(X:Y)=H(X)+H(Y)-H(X,Y)=\sum_x p_x\sum_y p(y|x)\log\frac{P(y|x)}{\sum_{x\in X}p_x P(y|x')} \tag{5}$$

这里 $P(y|x)=tr(E_y\rho_X)$。Eve 想要破解密钥，就是分辨 Alice 如何在密文空间 $C=\{|0>,|1>,|+>,|->\}^{\otimes(2l+\mu)}$ 中选择 $|c_i>$，其中 $|+>=(|0>+|1>)/\sqrt{2}$，$|->=(|0>-|1>)/\sqrt{2}$。

首先要证明，只要认证成功，Eve 有关 $|c_i>$ 的信息量为指数无穷小，即 Bob 收到的 $|c_i'>$ 与原密文 $|c_i>$ 的保真度为 $1-\exp[-O(n)]$。这个论述等价于一旦发生 Eve 的窃听，则 Bob 认证不成功的概率为 $1-\exp[-O(n)]$。Alice 和 Bob 在 $\{0,1\}^{(4l+3\mu)}$ 上随机选择 $(\hat{k},\hat{r},u)$，所以 $|c_i>$ 在 C 上均匀分布。由不可克隆定理[6]，Eve 得到 $|c_i>$，同时 Bob 也得到同样的量子状态的概率为 $\Pr(|c_i>=|c'_i>|m_i)=2^{-(4l+2\mu)}$，所以 Bob 解密 $|c'_i>$，得到的明文部分 a 和认证部分 $R'=h_u(b)$ 分别在 $\{0,1\}^{2l}$ 和 $\{0,1\}^{\mu}$ 上也服从均匀分布，因此由全概率公式和 *Hash* 函数的碰撞概率(3)可得到：

$$\begin{aligned}\Pr(R'=h_u(a))&=\Pr(h_u(a)=h_u(b)|a=b)\Pr(a=b)\\&+\Pr(h_u(a)=h_u(b)|a\neq b)\Pr(a\neq b)<2^{-(\mu+1)}+2^{-2\mu}\end{aligned} \tag{6}$$

因此，当 Eve 引入窃听时，Bob 认证成功的概率为 $\exp[-O(\mu)]$，即只要 Eve 想要获取有关 $|c_i>$ 的信息，必然会导致原密码状态 $|c_i>$ 的改变，从而导致解密出的明文与认证码在各自的取值域上完全随机，使得认证不成功的概率以指数趋近于 1。当认证成功时，$|c_i>$ 被 Eve 的窃听行为干扰的概率为 $1-\exp[-O(\mu)]$，故 Eve 得到有关 $|c_i>$ 的信息量为指数无穷小就无法获得有关密钥的信息。

下面需要证明，如果认证失败，那么 Eve 获得有关密钥的信息量小于明文长度 l。假设 Eve 可以在 $|c_i>$ 上执行任何测量，试图恢复密钥。由于 s_i 与密钥串 $(\hat{k},\hat{r},u)$ 相互独立且未知，因此(4)式中含 s_i 的项并不给出任何有关密钥的信息，故 Eve 只能从 $H^{k_1}(|m_i\oplus r_i>)$ 中得到有关 (k_1,r_1) 的信息 $H(K_1,R_1:Y)$。该部分密文的密度矩阵为

$$\rho_x{}^1=H^{k_1}|m_i\oplus r_1><m_i\oplus r_1|H^{k_1} \tag{7}$$

因为 Alice 和 Bob 在 $\{0,1\}^{2l}$ 均匀地随机选取 (k_1,r_1)，所以 $\rho_x{}^1$ 在 $\{|0><0|,|1><1|,|+><+|,|-><-|\}^{\oplus l}$ 上也均匀分布。根据 Holevo 界[6]，对任何 $\{E_y\}$，测量结果 Y 给出关于 Alice 以概率 p_x^1 选取 ρ_x^1 信息量满足如下关系：

$$H(K_1,R_1:Y)\leqslant S(\rho)-\sum_x p_x{}^1 S(\rho_x{}^1) \tag{8}$$

这里 $\rho=\sum_x p_x{}^1\rho_x{}^1$，$S(\rho)=-\mathrm{tr}(\rho\log\rho)$ 是 ρ 的 Von Neumann 熵。显然，ρ_x^1 是纯态，可知 $S(\rho_x)=0$，并且 $p_x^1=(1/2)^{4l}$。可得

$$\rho=\frac{1}{2^{4l}}\sum_{(k_1,r_1)\in\{0,1\}^{2l}}\rho_x{}^1=(\frac{1}{2}I)^{\otimes l} \tag{9}$$

所以 $S(\rho)=l$ 比特。由 Holevo 界可知，Eve 可获得有关密钥的信息量 $H(K_1,R_1:Y)<l$ 比特。因此剩余的密钥不确定性为

$$H(\hat{K},\hat{R},U|Y)=H(\hat{K},\hat{R},U)-H(K_1,R_1:Y)>3l+3\mu \text{ 比特} \tag{10}$$

Alice 和 Bob 在这种情况下必须重新协商 l 比特密钥，才能继续加密下一个明文分组。由于 Alice 和 Bob 在加密明文 $\{m_1,\cdots,m_{i-1}\}$ 的同时也协商了密钥串 $\{s_j\}$，$(1\leqslant j\leqslant I)$，如果 $I>0$，那么他们使用 s_I 来取代抛弃的密钥比特，从而避免了再次协商这一过程，提高了加密效率。

结论 加密效率比较：假设有 x 次认证失败，那么文[3]中的加密算法需要重新协商 xl 个密钥比特，而只要 $I>0$，我们的算法无需重新协商密钥。并且，当 $I\geqslant N/2$ 后，加解密双方就不必再使用量子加密，直接利用一次一密在经典信道上加密剩余的明文，避免了文[3]中的认证和窃听检测过程。本文提出的这种与量子密钥协商相结合的加密方式，通过引入随机数使认证过程更加有效，同时利用量子信息论使安全性分析更简洁。

参 考 文 献

1 Ambainis A, Mosca M, Tapp A, et al. Private quantum channels. In: The 41st IEEE Symposium on Foundations of Computer Science—FOCS 2000. Los Alamitos: IEEE, 2000. 547～553

2 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proc. IEEE Int Conf. on Computers, Systems, and Signal Processing, Bangalore, New York: IEEE, 1984. 175～179

3 Damgård I B, Pedersen T B, Salvail L. A quantum cipher with near optimal key-recycling. Crypto 2005, LNCS 3621. Berlin: Springer-Verlag, 2005. 494～510

4 Damgård I B, Pedersen T B, Salvail L. On the key-uncertainty of quantum ciphers and the computational security of one-way quantum transmission. In: Advances in Cryptology-- EUROCRYPT 2004, LNCS 3027, Heidelberg: Springer-Verlag, 2004. 91～108

5 Leung D W. Quantum vernam cipher. Quantum Information and Computation, 2002, 2(1): 14～34

6 Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000. 528～536