偏振旋转的量子私有信息检索方案

易运晖* 朱畅华 裴昌幸 权东晓
(西安电子科技大学综合业务网理论与关键技术国家重点实验室 西安 710071)

摘 要：私有信息检索是安全多方计算的重要问题。传统对称私有信息检索(SPIR)的很多假设在量子信息机制下非常脆弱，其安全性受到挑战。目前已提出的量子私有信息检索大都不易实施，该文提出基于偏振旋转的对称量子私有信息检索协议和实验方案。实验方案利用单光子的偏振旋转产生量子密文，不需要复杂的计算，便于硬件实现。协议的无条件安全性由量子力学 Heisenberg 测不准原理及不可克隆原理保证，并增加了用户诚实性检测，在所提出的非诚实合作模型下，非诚实用户的恶意行为不会造成隐私的泄露，在安全性、鲁棒性、抗第三方窃听等方面均优于经典环境的多种方案。

关键词：量子信息处理；私有信息检索(PIR)；量子光学；量子密钥分发；偏振旋转
中图分类号：TN918 **文献标识码**： A **文章编号**：1009-5896(2012)10-2353-05
DOI: 10.3724/SP.J.1146.2012.00242

Quantum Private Information Retrieval Based on Polarization Rotation

Yi Yun-hui Zhu Chang-hua Pei Chang-xing Quan Dong-xiao
(*State Key Lab of Integrated Service Networks*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Private information retrieval is the important issue of secure multi-party computation. Many assumptions of traditional Symmetric Private Information Retrieval (SPIR) are vulnerable in quantum mechanics and the present quantum SPIR protocols are complex to implement. A symmetric quantum SPIR protocol and experiment realization scheme are proposed. This scheme bases on polarized single photons to generate the key, so it has the advantage of simple operation and easy to hardware implement. The unconditional security of the protocol is guaranteed by Heisenberg uncertainty principle and quantum no-cloning theory. Dishonest user detection is involved in the protocol, the dishonest users could not get any information by malicious behavior under the dishonest cooperation model. The proposed scheme has better performance at security, robustness, anti-third party eavesdropping than many classical SPIR schemes.

Key words: Quantum information processing; Private Information Retrieval (PIR); Quantum optics; Quantum key distribution; Polarization rotation

1 引言

随着互联网的发展，互联网中用户信息的安全性逐步受到重视。特别是在商业竞争、金融和军事等特殊场合下，用户隐私的安全性要求更加严格。私有信息检索(Private Information Retrieval, PIR)是文献[1]于 1995 年提出的问题，目的是保护用户检索数据库中数据时自身的信息不泄露。PIR 是安全多方计算的一个分支，在安全多方计算的数据库安全查询、匿名认证等领域有着广阔的前景。

私有信息检索模型中，服务器 Bob 拥有 N bit 数据：$q_1,q_2,\cdots,q_N$，用户 Alice 从 Bob 的数据库中检索索引为 $i(1\le i\le N)$ 的数据 q_i 时，需要保护 Alice 的隐私，也就是使服务器 Bob 无法得知 i。为保护用户隐私，最直接但无意义的解决方案就是 Bob 把数据 $q_1,q_2,\cdots,q_N$ 都传给 Alice，由 Alice 自己完成检索。但这个方案使数据库 Bob 的隐私没有任何安全性，这一般是不允许的。1998 年，Gertner 等人[2]提出了对称私有信息检索(Symmetrically Private Information Retrieval, SPIR)协议，在保护用户隐私的基础上，同时保护数据库内容的隐私安全，并证明了 PIR 可以在一定条件下转化为 k 个服务器的 SPIR。信息论安全的私有信息检索可以在计算能力不受限制的条件下有效地保护隐私，但是此类模型通常需要多个互不通信的数据库副本，不仅空间复杂度高，而且现实中为保证数据库副本的一致，致

2012-03-12 收到，2012-07-25 改回
国家自然科学基金(61072067)，国家重点实验室专项资金(ISN1001004)，中央高校基本科研费专项资金(K50510010004)和高等学校创新引智计划(B08038)资助课题
*通信作者：易运晖 yhyi@mail.xidian.edi.cn

使这种假设通常很难成立。因此，只需要一个服务器的计算安全的私有信息检索成为研究热点[3−5]。

量子信息学是近 20 年发展起来，由量子力学、信息科学和计算机科学相结合的新型交叉学科。目前已有的计算安全的私有信息检索大都基于公钥密码学或一些附加的计算困难性假设，而这些基础在量子计算机制下变得非常脆弱，其安全性受到挑战。2004 年，文献[6]将量子信息处理应用到 PIR 中，提出了量子对称私有信息检索(QSPIR)技术，其后文献[7,8]对多种量子私有信息检索技术进行了研究。与传统 SPIR 相比，QSPIR 都是无条件也就是信息论安全的，但相关的研究一般都基于半诚实模型，且还未见具体实施方案。本文利用目前比较成熟的单光子态，结合量子密钥分发[9](Quantum Key Distribution, QKD)和量子安全直传[10,11] (Quantum Secure Direct Communication, QSDC)试验平台，设计了“非诚实合作模型”下的 QSPIR 协议及其实现方案，在安全性、鲁棒性、抗窃听等方面均优于经典环境中的各类 SPIR 方案。

2 整体方案

设单光子原始量子态$|\phi\rangle = a|0\rangle + b|1\rangle$，信道中单光子偏振角度的旋转角度为$\delta$，通过信道后量子态为$|\phi'\rangle$，则有

$$|\phi'\rangle = R_Z(\delta)|\phi\rangle \tag{1}$$

式中 $R_Z(\delta) = \begin{pmatrix} \cos\delta & \sin\delta \\ -\sin\delta & \cos\delta \end{pmatrix}$，且有

$$R_Z(\alpha)R_Z(\beta) = R_Z(\alpha+\beta) \tag{2}$$

设对$|\phi'\rangle$测量结果正确的概率为P，则

$$P = \cos^2\delta \tag{3}$$

既当对发送方的单光子偏振角度旋转δ后，接收方能够以$\cos^2\delta$的概率正确收到发送方的信息[12]，而发送方不知道接收方正确收到的是哪些数据。本文利用上述特点以及量子不可克隆、测不准原理(不确定性)等特点，设计了基于单光子的 QSPIR 协议。实验方案如图 1 所示，服务器和计算机通过量子信道和经典信道 2 个信道完成信息检索。量子信道中，用户 Alice 控制发端电路产生相应的光脉冲，光脉冲经过偏振滤镜和衰减器后形成单光子，Alice 通过电控偏振控制器 PC1 进行偏振编码，再通过电控偏振控制器 PC2 对编码后的单光子进行偏振旋转。携带着信息的光子通过量子信道传输到达接收端，经电控偏振控制器 PC3 再次偏振旋转后，通过偏振分束器(PBS)送入单光子探测器(SPD)，这样服务器 Bob 在同步脉冲的控制下就完成了量子信息的接收。同

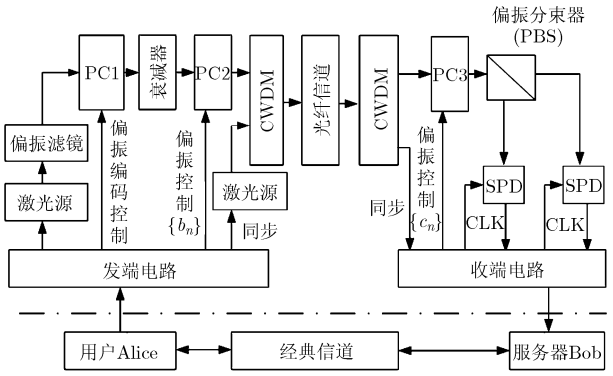

图 1 QPIR 系统原理框图

时，为了保证接收端的严格同步，使 SPD 的探测窗口在单光子到来时刻同步打开，服务器通过激光源发出的同步光脉冲信号经稀疏波分复用器(CWDM)复用到光纤信道上，用于控制接收方的开启门。此外，服务器 Bob 和用户 Alice 通过经典信道完成余信息的交互。

3 协议流程

假设用户 Alice 要从服务器 Bob 中检索数据，数据库中数据数为 N, Alice 检索的索引为 i，则偏振旋转量子对称私有信息检索(PR-QSPIR)协议的执行步骤如下：

(1)Alice 提交检索申请后，Bob 任意选择一个角度θ_0作为基本的角度并向 Alice 公布，双方都可以得到含 M 个偏振旋转角度的集合θ, $\theta = \{\theta_m = \theta_0 + (m-1)[\pi/(2M)] \mid m = 1,2,3,\cdots,M\}$。

(2) Alice 准备随机序列$\{a_n\}$和$\{b_n\}$, Bob 准备随机序列$\{c_n\}$。这 3 个序列长度均为 $L(L>N)$，其中 $C=L-N$ 为信道检测所需的比特数。$\{a_n\}$序列中元素取值为 0 或 1; $\{b_n\}$为 Alice 端偏振旋转角度随机序列; $\{c_n\}$为 Bob 端偏振旋转角度随机序列，其中$b_n, c_n \in \theta$。

(3) Alice 对信息序列$\{a_n\}$按照 0 对应于$|H\rangle$, 1 对应于$|V\rangle$的规则进行编码，也就是控制 PC1 为 0° 或者 90°; 同时按照$\{b_n\}$控制 PC2 的偏振旋转角度，亦即对光子进行$R(b_n)$变换。

(4) Bob 根据同步对收到光子进行编号。为验证信道的安全性，Bob 从接收的光子中随机选取 $L-N$ 个比特作为校验序列，通知 Alice 自己已经收到校验序列光子的序号并要求 Alice 公布对应的$\{a_n\}$和$\{b_n\}$，并对光子进行偏振控制和测量，得到测量结果$\{d_n\}$，然后根据$\{a_n\}$和$\{d_n\}$计算误码率验证信道的安全性；如果信道不安全则放弃此次检索。在确认信道安全后，Bob 检测 Alice 是否诚实，也就是检测 Alice 公布序列的随机性，如果偏差太大，则认

为 Alice 不诚实，放弃此次检索。

(5)Bob 接收其余光子时，根据 $\{c_n\}$ 中对应的元素控制 PC3 的偏振旋转角度，既对光子进行 $R(-c_n)$ 变换；Bob 对接收的光子进行测量将 $|H\rangle$ 记为 0, $|V\rangle$ 记为 1，得到长度为 N 的结果序列 $\{d_n'\}$；并将所收到的光子的序号通知 Alice。

(6)Alice 抛弃 $\{a_n\}$, $\{b_n\}$ 中的校验序列得到 $\{a_n'\}$ 和 $\{b_n'\}$, Bob 抛弃 $\{c_n\}$ 中的校验序列得到 $\{c_n'\}$，其序列长度都为 N。这样，$\{d_n'\}$ 就是 $\{a_n'\}$ 编码后偏振角度旋转 $\{b_n'-c_n'\}$ 得到的测量结果，如果 $\{b_n'-c_n'\}$ =0，则 Bob 可以准确得到 Alice 发送的 a_n'，否则 Bob 得到的将是不确定的数值。

(7) Bob 向 Alice 公布其余光子的 $\{c_n'\}$, Alice 找到 $\{b_n'-c_n'\}$ 中为 0 的项，得到其索引 j，也就是 Alice 判断出 $\{a_n'\}$ 和 $\{d_n'\}$ 一定相等的位置。但此位置索引和所要检索的索引 i 不同，因此 Alice 需要将 $\{a_n'\}$ 循环移动 $j-i$ 位，使 $\{a_n'\}$ 和 $\{d_n'\}$ 相等的位置和检索比特的索引相同，并将 $j-i$ 发送给 Bob。如果 $\{b_n'-c_n'\}$ 中不存在 0 项，则需要返回步骤(1)。

(8)Bob 根据 $j-i$ 对 $\{d_n'\}$ 进行移位得到 $\{k_n\}$，此时 $\{a_n'\}$ 和 $\{k_n\}$ 第 i 位一定相同。然后 Bob 利用 $\{k_n\}$ 和数据库内的数据进行异或，并将加密后的数据送给 Alice。

(9)Alice 用 $\{a_n'\}$ 对接收的数据进行异或，并选取第 i 个比特作为检索结果。

N=6, C=4, M=2 时，Alice 需要检索检索号 i=1 的协议实现过程见表 1。Alice 最后可以确定 $\{a_n\}\oplus\{k_n\}$ 的第 1 个比特为 0，但其它位都不确定，这样就可以从 Bob 发送过来的 $\{q_n\}$ 中取得自己所需的比特 q_1，但并不知道其它比特是否正确。同时，Bob 没有得到 Alice 索引的任何信息。

4　性能分析

目前，多数 PIR 模型中假设用户 Alice 和服务器 Bob 是诚实的，都会严格正确地执行协议，但在协议完成后双方会试图从中间结果中获取额外的隐私消息，也就是常说的半诚实模型。

本文中在半诚实模型的基础上，构造了更为真实的“非诚实合作”模型。也就是说 Alice, Bob 都可能试图不遵守协议来获取更多的信息，但不阻止协议的执行，主要假设如下：

(1) Alice 和 Bob 都试图合作完成本次检索，因此不用假的数据欺骗对方，也就是说 Alice 提交的索引和 Bob 给出的数据都是真实的。

(2) Alice 和 Bob 都足够聪明，可能试图在不影响协议执行的情况下，改变中间的数据来获得对方的隐私，但不采取会影响协议执行的举动。比如，其中一方若不采取 $\{\theta_n\}$ 做为偏振旋转角度的集合则会导致检索到错误的数据，因此双方都不会采取这种行为。

(3)Alice 和 Bob 都足够理智，不以放弃自己的隐私为目的获取对方的数据。

4.1 隐私安全分析

由于用户 Alice 随机产生且不公布有效的 $\{a_n\}$

表 1 PR-QSPIR 协议的实现过程

$\{a_n\}$ (Alice)	1	0	0	0	1	1	0	1	0	1
$\{b_n\}$ (Alice)	0	0	0	$\pi/4$	$\pi/4$	0	$\pi/4$	0	$\pi/4$	$\pi/4$
光子序列(Alice)	↑	→	→	↘	↘	↑	↗	↑	↗	↘
$\{c_n\}$ (Bob)		$\pi/4$	0			$\pi/4$	0	$\pi/4$	0	
测量基(Bob)	+	×	+	×	×	×	+	×	+	×
$\{a_n\}$, $\{d_n\}$ 校验	√			√	√					√
$\{a_n'\}$ (Alice)		0	0			1	0	1	0	
$\{b_n'\}$ (Alice)		0	0			0	$\pi/4$	0	$\pi/4$	
$\{d_n'\}$ (Bob)		?	0			?	?	?	?	
$\{b_n'-c_n'\}$ (Alice)		$-\pi/4$	0			$-\pi/4$	$-\pi/4$	$-\pi/4$	$\pi/4$	
$j-i$ (Alice)	1									
$\{k_n\}$ (Bob)	0 ? ? ? ? ?									
$\{q_n\}$	q_1 q_2 q_3 q_4 q_5 q_6									
$\{a_n\}\oplus(\{q_n\}\oplus\{k_n\})$	q_1 ? ? ? ? ?									

注：↑, ↓, ↗, ↘ 分别表示偏振态为垂直，水平，45°和135°；

+ 和 × 分别表示测量基为直基(垂直，水平)和斜基(45°和135°)；

√表示符合规律；

? 表示不确定数。

和$\{b_n\}$，而且 Bob 的测量结果是由量子力学测不准原理保证的，因此 Bob 不能多次测量或者从测量结果$\{d_n\}$中得到用户索引的任何信息。同时，Alice 传递的$j-i$是 Alice 根据 Bob 公布的$\{c_n\}$计算出的$\{b_n-c_n\}$而得到的，由于不能得到$\{b_n\}$，所以 Bob 也不能从中得到索引 i 的任何信息。因此，即使 Bob 是非诚实的，在步骤(6)欺骗 Alice 产生更多的数据，也无法得到索引的信息，用户 Alice 的隐私是严格保密的。

由于最终的数据库扰码$\{k_n\}$是 Bob 测量后的结果，因此 Bob 为保证隐私不被泄露，一定会保证$c_n^{'}$的随机性；同时，校验序列是 Bob 随机抽取且要求 Alice 公布的，所以如果 Alice 的随机性太偏离要求的概率分布，Bob 也会发现 Alice 的不诚实，导致检索失败，因此 Alice 的序列随机性不会太偏离要求。这样即使 Alice 采用对自己有利的$\{a_n\}$和$\{b_n\}$，由于量子测不准的原理，也只能提高互信息量，而不能获得 Bob 的测量结果，也就是无法获得$\{k_n\}$，这样 Bob 的数据是具有私密性的。

分析协议可知，Alice 可以由$\{a_n\},\{b_n\}$和$\{c_n\}$分析$\{d_n\}$，特别是当$\{b_n\}$和$\{c_n\}$对应项相同时，Alice 一定能够知道$\{d_n\}$的相应数据。所以，本协议中 Bob 的隐私并不是完全安全的，会有少量信息泄露。下面我们分析 Alice 能够得到的最大信息量。

根据协议可知，Alice 发送的量子态最终的偏振旋转角度为$b_n^{'}-c_n^{'}$，接收方 Bob 可以以$\cos^2(b_n^{'}-c_n^{'})$的概率正确收到 Alice 的数据[12]。设此时 Alice 和 Bob 的互信息量$I(a;b)$，则根据互信息量的定义可得

$$\begin{aligned}I(a;b)=H(b)-H(b\mid a)=1+\cos^2(b_n^{'}-c_n^{'})\\ \cdot\log_2\cos^2(b_n^{'}-c_n^{'})+\sin^2(b_n^{'}-c_n^{'})\\ \cdot\log_2\sin^2(b_n^{'}-c_n^{'})\end{aligned}\tag{4}$$

显然$I(a;b)$是$b_n^{'}-c_n^{'}$的函数，且以$\pi/2$为周期，因此不失一般性，在隐私安全分析中，都认为$b_n^{'}\in[0,\pi/2)$，$c_n^{'}\in[0,\pi/2)$。由于可以检测 Alice 的随机性，所以可以认为$b_n^{'}$和$c_n^{'}$都是$\left[0,\ \dfrac{\pi(M-1)}{2M}\right]$区间上的等概分布。此时$b_n^{'}-c_n^{'}$服从以下分布：

$$P\left(b_n^{'}-c_n^{'}=\frac{k\pi}{2M}\right)=\frac{M-|k|}{M^2},\ -M+1\le k\le M-1\tag{5}$$

这样 Alice 和 Bob 的互信息量为

$$I(A,B)=I(B,A)=\sum_{j=0}^{1}\sum_{i=0}^{1}p(x_iy_j)\log_2\frac{p(x_i/y_j)}{p(x_i)}\tag{6}$$

由于 Alice 随机选择 0,1，所以

$$p(x_0)=p(x_1)=1/2\tag{7}$$

而信道转移概率

$$p(y_j/x_i)=\begin{cases}\displaystyle\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\cos^2\left(\frac{k\pi}{2M}\right),\ i=j\\ \displaystyle\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\sin^2\left(\frac{k\pi}{2M}\right),\ i\ne j\end{cases}\tag{8}$$

则有

$$p(x_iy_j)=\begin{cases}\dfrac{1}{2}\displaystyle\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\cos^2\left(\frac{k\pi}{2M}\right),\ i=j\\ \dfrac{1}{2}\displaystyle\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\sin^2\left(\frac{k\pi}{2M}\right),\ i\ne j\end{cases}\tag{9}$$

可知

$$p(y_i)=1/2,\ \ i=0,1\tag{10}$$

$$p(x_j/y_i)=\begin{cases}\displaystyle\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\cos^2\left(\frac{k\pi}{2M}\right),\ i=j\\ \displaystyle\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\sin^2\left(\frac{k\pi}{2M}\right),\ i\ne j\end{cases}\tag{11}$$

因此，

$$\begin{aligned}I(A,B)=I(B,A)=\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\cos^2\left(\frac{k\pi}{2M}\right)\\ \cdot\log_2\left(2\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\cos^2\left(\frac{k\pi}{2M}\right)\right)\\ +\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\sin^2\left(\frac{k\pi}{2M}\right)\\ \cdot\log_2\left(2\sum_{k=-N+1}^{N-1}\frac{(M-|k|)}{M^2}\sin^2\left(\frac{k\pi}{2M}\right)\right)\end{aligned}\tag{12}$$

图 2 是$I(A,B)$随 M 变化的曲线，由图中可以看出当 M>20 以后，互信息量变化就很小，因此当 N 较小时，应使$N\cdot I(A,B)$大于 1，保证平均每次检索都有 1 个比特可以匹配；当 N 较大时不妨取 M 为 20，这时$I(A,B)\approx0.123$，Alice 所能得到 Bob 的最大信息量约为$N/8$，此时可以采用密性放大来保护 Bob 的隐私。

一种简单的密性放大方案如下：当 N 较大时，$\{b_n\}$和$\{c_n\}$对应项相等的概率也大，Alice 能够得到

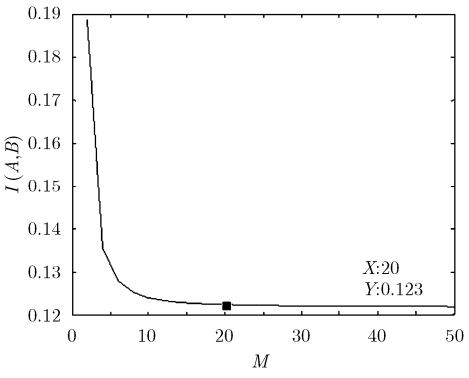

图 2 $I(A,B)$和 M 的关系

多个 $b_n^{'}-c_n^{'}$ 为 0 的项，也就是存在 $j_1,j_2,\cdots$。因此可以要求 Alice 返回多个 $j-i$，然后 Bob 移位生成多个 $\{k_n\}$，将这些序列异或后得到最终的数据库加密 $\{k_n\}$，这样可以大大提高 Bob 的隐私安全性。

因此，对于数据库 Bob 来说这种方案的隐私虽然不是严格保密的(Alice 存在知道多个比特的可能性)，但具有好的隐私安全性。

4.2 第三方窃听安全性分析

根据量子力学的原理，Eve 不可能在不影响非正交的两个量子态的基础上，分辨两个量子态，从而使 Alice 和 Bob 在检测过程中发现错误，导致窃听被发现。假如窃听者 Eve 使用探针与 Alice 的量子态相互作用完成测量或者 Eve 采取替换光子的方法，则必然不可避免地要干扰光子状态，必然会在检测过程中发现错误，从而被发现。拒绝服务攻击是指 Eve 只是对光子进行随机的操作来破坏传输的信息，则也必然会扰乱光子的状态，通过检测过程也是可以发现的。因此在数据传送前，Eve 的窃听都会被发现，这样 Eve 不能获取任何一方的有效数据。

4.3 复杂度分析

整个协议在量子密钥分发协议(QKD)的基础上改动很小，其通信复杂度和量子密钥分发协议相同。因此本协议在结合了私有信息检索和量子密钥的基础上，通信复杂度基本保持不变。

为计算协议所需计算量 C，不妨取 L=2N。按照协议流程，计算量主要是在(4), (7), (8), (9)几个步骤，其中第(4)步进行校验所需运算量为 L–N=N；第(7)步进行比较所需运算量为 N+1；第(8)步加密所需运算量为 N；第(9)步解密所需运算量为 N。

则有 $C=N+(N+1)+N+N=4N+1$。

因此协议的运算复杂度为 $O(N)$，比目前的私有信息检索协议复杂度高。但本文协议不需要复杂的运算，只需要简单的异或运算(判决相等也可以用异或实现)，可以直接硬件实现。

5 结论

(1)本文基于量子单光子提出 PR-QSPIR 实验方案，协议是无条件安全或者说是信息论安全；方案不需要量子存储器，便于硬件实现。(2)本文提出了非诚实合作模型，设计了 PR- QSPIR 协议，能够有效检测和防止双方的不诚实举 s 动。(3)采用量子态作为有效的检测机制，具有更高的安全性和更强的鲁棒性。

参 考 文 献

[1] Benny C, Oded G, Eyal K, *et al*.. Private information retrieval[C]. IEEE 36th Annual Symposium on Foundations of Computer Science, Milwaukee, WI, USA, October 23, 1995: 41–50.

[2] Gertner Y, Ishai Y, Eyal K, *et al*.. Protecting data privacy in private information retrieval schemes[C]. 13th Annual ACM Symposium on Theory of Computing, Dallas, TX, USA, May 23–26, 1998: 151–160.

[3] Ryan H, Femi O, and Ian G. Practical PIR for electronic commerce[C]. 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, October 17, 2011: 677–689.

[4] Zhong Hong, Yi Lei, Yu Zhao, *et al*.. Fully-homomorphic encryption based SPIR[C]. 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Wuhan, China, Sept. 23–25, 2011: 3–6.

[5] Toru N, Shunsuke I, Daisuke I, *et al*.. Anonymous authentication systems based on private information retrieval[C]. 1st International Conference on Networked Digital Technologies, Ostrava, Czech Republic, July 28, 2009: 53–58.

[6] Iordanis K and Wolf D. Quantum symmetrically-private information retrieval[J]. *Information Processing Letter*, 2004, 90(5): 109–114.

[7] Vittorio G, Seth L, Cone M, *et al*.. Quantum private queries: security analysis[J]. *IEEE Transactions on Information Theory*, 2010, 56(7): 3465–3477.

[8] Lukasz O. Secure quantum private information retrieval using phase-encoded queries[J]. *Physical Review A-Atomic, Molecular, and Optical Physics*, 2011, 84(8): 022313–022316.

[9] 权东晓, 裴昌幸, 刘丹, 等. 基于单光子的单向量子安全通信协议[J]. 物理学报, 2010, 59(4): 2493–2497.
Quan Dong-xiao, Pei Chang-xing, Liu Dan, *et al*.. One-way quantum secure direct communication protocol based on single photons[J]. *Acta Physics Sinica,* 2010, 59(4): 2493–2497.

[10] 赵生妹, 李苗苗, 郑宝玉. 一种基于量子纠错编码的量子密钥分配协议[J]. 电子与信息学报, 2009, 31(4): 954–957.
Zhao Sheng-mei, Li Miao-miao, and Zheng Bao-yu. A novel quantum key distribution protocol based on quantum error correction code[J]. *Journal of Electronics & Information Technology*, 2009, 31(4): 954–957.

[11] Liu Dan, Pei Chang-xing, Quan Dong-xiao, *et al*.. A new quantum secure direct communication scheme with authentication[J]. *Chinese Physics Letter*, 2010, 27(5): 050306.

[12] 刘丹, 裴昌幸, 权东晓. 测量基对 BB84 协议安全性影响[J]. 电子与信息学报, 2011, 33(1): 228–230.
Liu Dan, Pei Chang-xing, and Quan Dong-xiao. Measurement bases impact on the security of BB84 protocol[J]. *Journal of Electronics & Information Technology*, 2011, 33(1): 228–230.

易运晖：　男，1975 年生，副教授，在职博士生，研究方向为量子信息处理、量子通信.

朱畅华：　男，1973 年生，副教授，研究方向为量子信息处理、量子通信.

裴昌幸：　男，1945 年生，教授，研究方向为量子信息通信.

权东晓：　女，1980 年生，副教授，研究方向为量子通信、通信网理论与技术.