基于量子第三方的隐私数据库查询协议

张 昭* 王 洪 马 智
(解放军信息工程大学 郑州 450001)

摘 要：保障查询数据库时用户及数据库的隐私性具有重要意义。该文利用三光子 GHZ(Greenberger-Horne-Zeilinger)态的量子关联性，提出一个基于量子第三方的隐私数据库查询协议。协议对于信道损耗具有很高的容忍度，并且能够有效地抵抗第三方发动伪造量子纠缠态和量子记忆存储攻击。在第三方的帮助下，协议能够确定地控制用户获得数据库隐私信息的数量。同时，利用 Mermin-Bell 不等式进行真正的三方纠缠验证保证协议的安全性，这一思想也拓展了设备无关纠缠验证的应用领域。

关键词：密码术；数据库；隐私数据库查询； Greenberger-Horne-Zeilinger (GHZ)态；Mermin-Bell 不等式
中图分类号： TN918 **文献标识码**： A **文章编号**：1009-5896(2014)07-1667-06
DOI: 10.3724/SP.J.1146.2013.00682

Private Database Queries With a Quantum Third Party

Zhang Zhao Wang Hong Ma Zhi
(*PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: It is of great importance to guarantee the privacy of the database and users when the database is being queried. A private database queries protocol based on a quantum Third Party (TP) is proposed by utilizing the quantum correlation of three-photon Greenberger-Horne-Zeilinger (GHZ) states. The proposed protocol is highly tolerant of channel loss and robust against fake entangled state attack and quantum memory attack implemented by the third party. With the help of the TP, the amount of private information obtained by the users from the database is deterministically controllable in the proposed protocol. Furthermore, the true tripartite entanglement witness by using Mermin-Bell inequality can ensure the security of the protocol, which expands the application area of Device-Independent (DI) entanglement witnesses.

Key words: Cryptography; Database; Private database queries; Greenberger-Horne-Zeilinger (GHZ) state; Mermin-Bell inequality

1 引言

随着计算机技术和网络技术的飞速发展，数据库在各行业中的应用日益广泛。复杂、动态、开放的应用环境使得数据库面临的安全威胁越来越多。早期的数据库安全相关研究主要集中于保证数据的保密性、完整性、可靠性及可用性。已有的一些安全措施，如访问控制机制、备份恢复策略、基于角色管理等，虽然起到了一定的保护作用，但在实际应用中仍然面临不少问题。其中，比较重要的一个威胁是隐私问题，隐私泄露已成为信息共享的主要障碍之一。隐私信息检索(Private Information Retrieval, PIR)是为保障查询用户的个人隐私在公共平台上的私密性所采用的策略。用户检索数据库信息时，可以采用相关技术阻止数据库拥有者获取用户查询语句的相关信息，从而保护用户隐私。另一方面，数据库自身存在大量的敏感信息，保障数据库在提供服务时的隐私性同样是一个重要问题。如何有效地保护隐私信息，尤其是如何实现数据库应用服务的便利性与保障隐私信息安全更好地结合，是一个有意义且充满挑战性的课题。

隐私数据库查询[1](Private Database Queries, PDQs)协议是指：一个用户 Alice，希望得到一个数据库拥有者 Bob 的一部分隐私信息，但她不希望 Bob 知道她得到的是哪部分信息(用户隐私)；而且 Bob 也不希望 Alice 得到除她所感兴趣之外更多的数据库信息(数据库隐私)。在经典世界中，这类问题被 Gertner 等人[2]称为对称隐私信息检索(Symmetrically-Private Information Retrieval, SPIR)，它是 PIR[3]的一种推广(PIR 只考虑用户的隐私安全)。量子 PDQs 协议是指利用量子力学去处理这类问题，主要是利用量子力学基本原理去保护

2013-05-16 收到，2014-01-26 改回
国家 863 计划(2011AA010803)资助课题
*通信作者：张昭 zhang7967513@sina.com

用户 Alice 和数据库 Bob 的隐私安全，从而使得隐私查询能够安全地完成。量子 PDQs 协议与量子密钥分配[4](Quantum Key Distribution, QKD)协议不同。在 QKD 协议中，通信双方彼此之间互相信任，不会主动攻击对方。就算是目前很热门的 DI-QKD [5−8] 和 MDI-QKD[9](Measurement Device-Independent QKD)中，通信双方彼此之间也是互相信任的，只是攻击者可能控制了信号源或者他们的测量设备进行攻击。而在 PDQs 协议中，通信双方彼此之间互相不信任，他们都有各自不希望对方得到的隐私信息。因此，PDQs 协议需要防止对方窃取自己的隐私信息。

2008 年，文献[1]提出了第 1 个量子 PDQs 协议(GLM 协议)。GLM 协议利用一个欺骗敏感策略，使得 Alice 可以检测 Bob 是否窃取了自己的隐私信息。2009 年，文献[10]给出 GLM 协议的一个原理验证实验。2010 年，文献[11]对 GLM 协议的安全性给出了详细的分析。2011 年，文献[12]基于 QKD 提出一种实用的量子 PDQs 协议(JSG 协议)。JSG 协议利用 SARG04(Scarani-Acin-Ribordy-Gisin 2004)[13] 协议使得通信双方共享了非对称的密钥，实现了 PDQs 协议的目的。同年，文献[14]基于 JSG 协议的思想提出一种灵活的量子 PDQs 协议，文中对最初由 Bob 制备的量子态引入一个变量 θ，当选择一个比较小的 θ 角时，数据库的隐私会更加安全；当选择一个比较大的 θ 角时，Bob 能够正确猜测到 Alice 隐私的概率会更低，即用户的隐私会更加安全。

本文提出一个基于量子第三方的 PDQs 协议。在协议中，第三方 Charlie 制备分发三光子 Greenberger-Horne-Zeilinger(GHZ)态给 Alice 和 Bob。然后，他们随机地选择 Y 基或 X 基(Y 基为 $\{|+y\rangle,|-y\rangle\}$，X 基为 $\{|+x\rangle,|-x\rangle\}$，其中 $|\pm x\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$，$|\pm y\rangle=(|0\rangle\pm i|1\rangle)/\sqrt{2}$)测量自己手中的 GHZ 光子，并记录测量结果。Charlie 利用三光子 GHZ 态的量子关联性，帮助 Alice 获得 Bob 的 1bit 测量结果作为 Alice 的密钥，记为 m_a。当 Bob 利用自己的测量结果加密数据库时，Alice 就可以利用 m_a 恢复出数据库某一项的秘密信息。随后，着重分析了第三方利用伪造量子态和量子存储设备窃取数据库隐私的攻击手段。为了抵抗这种攻击，本文利用 Mermin-Bell 不等式构造 S 值检测，可以准确地判断出第三方是否发动了此种攻击，达到保护数据库隐私的目的。值得注意的是，本文有一个基本要求，量子第三方 Charlie 不能与用户 Alice 或者 Bob 中的任何一方合谋。

2 协议流程

假设 Bob 数据库的长度为 N。Alice 想要得到 Bob 数据库中第 i 位的隐私信息 X_i。协议主要由 3 部分构成：GHZ 态的制备分发、攻击检测和隐私询问。具体步骤如下：

(1)GHZ 态的制备分发：

(a)Charlie 制备三光子 GHZ 态，并把其中两个光子发送给 Alice 和 Bob(三光子 GHZ 态记为：$|\mathrm{GHZ}\rangle_{\mathrm{ABC}}=(|000\rangle+|111\rangle)_{\mathrm{ABC}}/\sqrt{2}$，其中下标 A 和 B 分别表示发送给 Alice 和 Bob 的光子，下标 C 表示 Charlie 自己留下的光子)。Charlie 重复此过程足够多次，确保 Alice 和 Bob 手中至少拥有 $3N$ 个 GHZ 光子。

(b)Alice, Bob 和 Charlie 随机选择 X 基或 Y 基测量自己手中的光子，并记录所选择的测量基和得到的测量结果。

(2)攻击检测：

(a)Alice 和 Bob 各随机地选择 $N/2$ 个光子，要求 Charlie 公布对这些光子的测量基和测量结果。然后 Alice 和 Bob 相互合作，计算这些 GHZ 光子在式(1)中的 S 值，判断 Charlie 是否制备分发了 GHZ 态。当 $S=4$ 时，协议继续；否则协议需要从步骤(1)(a)重新执行；

(b)Charlie 随机地选择 N 个光子，要求 Alice 和 Bob 公布对这些光子的测量基和测量结果。通过计算这些 GHZ 光子在式(1)中的 S 值，判断是否存在外部窃听者。当 $S=4$ 时，协议继续；否则协议需要从步骤(1)(a)重新执行。

$$S=|E(1,2,2)+E(2,1,2)+E(2,2,1)-E(1,1,1)| \quad (1)$$

其中 $E(k_1,k_2,k_3)=\left\langle\prod_{j=1}^{3}A_j(\vec{n}_{k_j})\right\rangle_{\mathrm{avg}}$，$k_j=1,2$；$j=1,2,3$ 分别对应 Alice, Bob 和 Charlie；$\vec{n}_{k_j}$ 表示 j 所选择的测量方向，当 $k_j=1$ 时，$\vec{\sigma}\cdot\vec{n}_{k_j}=\sigma_x$，当 $k_j=2$ 时，$\vec{\sigma}\cdot\vec{n}_{k_j}=\sigma_y$；$A_j(\vec{n}_{k_j})$ 表示 j 沿 $\vec{n}_{k_j}$ 方向测量得到的测量结果，$A_j(\vec{n}_{k_j})=\pm1$；$\langle\cdot\rangle_{\mathrm{avg}}$ 表示均值。

(3)隐私询问：

(a)Alice 和 Bob 公布自己的测量基。根据公布的基信息，Charlie 选择一个三方都在 X 基下测量的 GHZ 态(例如第 j 个 GHZ 态)。这个 GHZ 态对应于 Alice, Bob 和 Charlie 手中的光子分别记为 Q_{A}，Q_{B} 和 Q_{C}。Charlie 公布自己对第 j 个 GHZ 态(即 Q_{C})的测量结果，并秘密地发送 j 给 Alice；

(b)Alice 根据 Charlie 发送的信息和自己的测量结果，推断 Bob 对 Q_{B} 的测量结果，如式(2)所示。然后 Alice 把 Bob 对 Q_{B} 的测量结果作为自己的密钥，记为 m_a；

$$|\mathrm{GHZ}\rangle_{\mathrm{ABC}}=\frac{1}{2}[(|+x\rangle|+x\rangle+|-x\rangle|-x\rangle)_{\mathrm{AC}}\otimes|+x\rangle_{\mathrm{B}}+(|+x\rangle|-x\rangle+|-x\rangle|+x\rangle)_{\mathrm{AC}}\otimes|-x\rangle_{\mathrm{B}}] \quad (2)$$

(c)Bob 把自己的测量结果记为 K_b。这时，Alice 知道 K_b 中某一位的比特信息 m_a，但是 Bob 不知道 m_a 的位置；

(d)Alice 计算 $p=j-i$，并秘密地把 p 发送给 Bob。Bob 计算 $C_n=X_n\oplus K_{b-p}$，并将 C_n 发送给 Alice。这时，Alice 就可以利用 m_a 解密 C_i，获得 X_i。

在步骤(3)(a)中，如果 Charlie 公开 j，则 Bob 将会知道 m_a 的位置，从而得到 Alice 的隐私；在步骤(3)(d)中，如果 Alice 公开 p，则 Charlie 就会根据 p 和 j 推断出 Alice 的隐私。因此，为了保护 Alice 的隐私，协议需要两个经典保密通信，传递的信息可以利用经典密码体制进行加密，也可以利用 QKD 协议产生的密钥加密。

此协议与利用 GHZ 态的量子秘密共享协议[15](QSS)在 GHZ 态制备分发阶段是相同的。但是，为了达到 PDQs 协议的目的，本文修改了 QSS 协议的经典信息后处理阶段。因此，在分析 GHZ 态分发过程中的安全性和 Alice 与 Bob 彼此之间的攻击时，可以利用 QSS 安全性的分析方法分析本文协议。然而，此协议与 QSS 协议也存在着不同之处。在 QSS 协议中，秘密分发者不会主动攻击下属，他对于下属是诚实的。而在量子 PDQs 协议中，只有用户 Alice 和数据库 Bob 具有自己的隐私信息，Charlie 不具有自己的隐私信息，他只是协助隐私查询顺利地进行，Alice 和 Bob 并不信任 Charlie。因此，在安全性分析阶段，还需要着重分析 Charlie 针对 Alice 和 Bob 隐私的攻击。

3　协议分析

3.1 正确性分析

该协议的正确性可以由定理 1 给出。

定理 1(正确性)　用户 Alice 能且只能得到数据库 Bob 1 bit 的隐私信息，并且 Bob 不知道 Alice 得到的是哪一比特的隐私信息。

证明　由于 Bob 数据库的隐私信息是由自己的测量结果加密，所以只要 Alice 得到 Bob 的测量结果，就能够得到 Bob 数据库的隐私信息。然而，在步骤(3)(a)中，Charlie 根据 Alice 和 Bob 公布的基信息，只选择了一个三方同时在 X 基下测量的 GHZ 态(即第 j 个 GHZ 态)作为 Alice 的密钥，并把自己对这个 GHZ 态的测量结果和位置 j 发送个 Alice。因此，Alice 根据得到的信息，只能推断出一个 Bob 的测量结果，从而只能得到 Bob 1 bit 的隐私信息。换言之，Alice 得到 Bob 隐私信息的数量是由 Charlie 控制的。

由于 Charlie 是秘密地把 j 发送给 Alice，并且在步骤(3)(d)中，Alice 计算 p 发送给 Bob，所以 Bob 不能得到 j，从而不知道 Alice 得到了哪一比特的隐私信息。　　证毕

3.2 安全性分析

在协议中，只有 Alice 和 Bob 具有隐私信息，Charlie 没有隐私信息，且要求 Charlie 不能与 Alice 或者 Bob 中的任何一方合谋。所以本节只需要从 3 个方面分析协议的安全性：一是 Charlie 对 Alice 和 Bob 隐私的攻击；二是外部窃听者的攻击；三是 Alice 和 Bob 彼此之间的攻击。

(1)Charlie 对 Alice 和 Bob 隐私的攻击　考虑 Charlie 在两种模型下的安全性：半可信的(Semi-honest)和恶意的(malicious)。在半可信的(也称诚实但好奇，honest-but-curious)模型下，Charlie 忠诚地执行协议，但同时记录他看到的所有信息。在恶意模型下，Charlie 主动攻击 Alice 和 Bob，窃取他们的隐私信息，如伪造量子纠缠态攻击和量子记忆存储攻击等。

(a)半可信的模型下：　在此模型中，Charlie 只是记录了自己看到的所有信息。所以只需要分析 Charlie 是否可以从这些信息中得到 Alice 和 Bob 的隐私即可。

由于 Charlie 只知道 Alice, Bob，自己的测量基和自己的测量结果，根据三光子 GHZ 态的量子关联性，Charlie 不能从这些已知信息中推断出 Alice 秘密发送给 Bob 的 p，以及 Alice 和 Bob 任何的测量结果，从而也就不能得到 Alice 和 Bob 的任何隐私信息。

因此，在半可信的模型下，协议是安全的。

(b)恶意的模型下：　由于 Charlie 进行主动攻击的目的是为了获取 Alice 和 Bob 的隐私信息，所以最行之有效的攻击方法是利用伪造量子纠缠态进行攻击。即 Charlie 不制备分发三光子 GHZ 态，而是制备其它量子纠缠态进行攻击。对于 Charlie 伪造的量子态，可以分为两种情况：

情况 1　Charlie 制备形如 $|\varphi\rangle_{\mathrm{A}}\otimes|\phi\rangle_{\mathrm{BC}}$ 的量子态。

Charlie 制备形如 $|\varphi\rangle_{\mathrm{A}}\otimes|\phi\rangle_{\mathrm{BC}}$ 的量子态发送给 Alice 和 Bob(其中 $|\phi\rangle_{\mathrm{BC}}$ 是任意两粒子纠缠态，$|\varphi\rangle_{\mathrm{A}}$ 是任意单比特量子态，下标 A, B, C 分别表示 Alice, Bob 和 Charlie 得到的粒子)。例如，Charlie 制备分发量子态 $|\varphi\rangle=|0\rangle_{\mathrm{A}}\otimes(|00\rangle+|11\rangle)_{\mathrm{BC}}/\sqrt{2}$ 给 Alice 和 Bob。随后，Charlie 不直接测量自己手中的光子，

而是利用量子存储设备储存起来，等到 Bob 公布了自己的测量基后，利用与 Bob 相同的测量基测量自己手中的光子。根据式(3)中不同测量基下的展开式，Charlie 可以得到和 Bob 相关联的测量结果。

$$\begin{aligned}&\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{\mathrm{BC}}\\&=\frac{1}{\sqrt{2}}(|+x\rangle|+x\rangle+|-x\rangle|-x\rangle)_{\mathrm{BC}}\\&=\frac{1}{\sqrt{2}}(|+y\rangle|-y\rangle+|-y\rangle|+y\rangle)_{\mathrm{BC}}\end{aligned}\tag{3}$$

然后，Charlie 可以利用这些相关联的测量结果窃取 Bob 数据库的隐私信息。例如，Charlie 假冒 Alice 向 Bob 发送伪造的 p'，让 Bob 利用这个 p' 移动自己的测量结果，加密数据库 X_n，并发送 C_n。这时，Charlie 就可以通过自己的测量结果解密出 C_n，从而得到数据库的隐私。

我们发现当 Charlie 发动此类攻击时，制备的量子态 $|\varphi\rangle_{\mathrm{A}}\otimes|\phi\rangle_{\mathrm{BC}}$ 恰好是一种可两分的三方纠缠态，它并不是一个真正的三方纠缠态，所以可以通过利用 Mermin-Bell 不等式去检测 Alice, Bob 和 Charlie 三方共享的量子态，从而抵抗 Charlie 发动这种伪造量子态攻击。

由于只有 Alice 和 Bob 拥有隐私信息，他们更希望协议是安全的，所以为了保证自己隐私的安全性，Alice 和 Bob 可以相互合作检测 Charlie 的忠实性。在步骤(2)(a)中，Alice 和 Bob 相互合作，各随机地选择 $N/2$ 个光子，要求 Charlie 公布对这些光子的测量基和测量结果。然后计算式(1)中的 S 值：

①当 Charlie 制备分发 GHZ 态时，通过对式(1)进行简单的计算，得到

$$S=4\tag{4}$$

②当 Charlie 发动上述攻击，制备分发量子态 $|\varphi\rangle_{\mathrm{A}}\otimes|\phi\rangle_{\mathrm{BC}}$ 给 Alice 和 Bob 时，根据 Mermin-Bell 不等式在进行真正三方纠缠验证时的违背值，能够得到

$$S\le 2\sqrt{2}\tag{5}$$

因此，通过构造的 S 值检测，协议能够有效地抵抗 Charlie 发动这类可两分三方纠缠态的伪造量子态攻击。

并且 Mermin-Bell 不等式验证是一个与设备无关的纠缠验证，它与 Alice, Bob 和 Charlie 三方的测量设备无关。因此，在检测 Charlie 是否制备分发 $|\varphi\rangle_{\mathrm{A}}\otimes|\phi\rangle_{\mathrm{BC}}$ 型量子态时，并不需要假定 Charlie 执行了什么样的测量，或者 Charlie 是否控制了 Alice 和 Bob 的测量装置。即当 Charlie 在步骤(2)(a)中故意公布错误的测量基和测量结果时，协议也能够通过 S 值检测出来。

情况 2 Charlie 制备其他真正的三方纠缠态。

Charlie 还可以利用其他真正的三方纠缠态去窃取 Bob 数据库的隐私信息。

例如，量子纠缠态 $(|+x\rangle|+x\rangle|+x\rangle+|-x\rangle|-x\rangle|-x\rangle)_{\mathrm{ABC}}/\sqrt{2}$。当 Charlie 和 Bob 都选择 X 基测量时，Charlie 能够得到 Bob 所有的测量结果，从而得到 Bob 的隐私信息。

我们发现只有当 Charlie 可以从分发的三方纠缠态中得到 Bob 的测量结果时，这个纠缠态才会对 Charlie 有意义。所以，这类三方纠缠态包含如下 4 种形式：

$$\left.\begin{aligned}&(|+x\rangle|+x\rangle|a\rangle+|-x\rangle|-x\rangle|b\rangle)_{\mathrm{ABC}}/\sqrt{2}\\&(|+x\rangle|-x\rangle|a\rangle+|-x\rangle|+x\rangle|b\rangle)_{\mathrm{ABC}}/\sqrt{2}\\&(|+y\rangle|+y\rangle|a\rangle+|-y\rangle|-y\rangle|b\rangle)_{\mathrm{ABC}}/\sqrt{2}\\&(|+y\rangle|-y\rangle|a\rangle+|-y\rangle|+y\rangle|b\rangle)_{\mathrm{ABC}}/\sqrt{2}\end{aligned}\right\}\tag{6}$$

其中 $|a\rangle$ 和 $|b\rangle$ 是任意两个正交的单比特量子态。同样地，通过计算这些三方纠缠态的 S 值，发现 $S\le 2\sqrt{2}$ (这是因为真正的三方纠缠态在某些测量方向上能够违背 Mermin-Bell 不等式，达到最大的违背值。但是 Charlie 制备的这些量子纠缠态在 X 基和 Y 基下不能达到最大的违背值)。这说明构造的 S 值检测也能够抵抗 Charlie 发动这类三方纠缠态的伪造量子态攻击。

此外，如果此时 Charlie 按要求发送 GHZ 态，在检测窃听通过之后，对于剩余的非检测 GHZ 态，Charlie 不能等 Alice 和 Bob 都公开测量基之后，再选取合适的测量基获取 Bob 的测量结果。因为在第 2 节“协议流程”中“GHZ 态的制备分发”，要求制备的 GHZ 态形式为 $|\mathrm{GHZ}\rangle_{\mathrm{ABC}}=(|000\rangle+|111\rangle)_{\mathrm{ABC}}/\sqrt{2}$，即 Z 基下的 GHZ 态；而“隐私询问”中用到的密钥是 Alice, Bob 和 Charlie 三方都在 X 基下测量的结果。检测窃听通过之后，就能保证 GHZ 态是 Z 基下的 GHZ 态。Charlie 想得到 X 基下 Bob 的测量结果，就必须知道 Alice 的测量结果(这点由 Z 基下 GHZ 态在 X 基下展开的表达式保证)，而 Alice 只公布测量基，并没有公布任何她的测量结果，因此在只知道 Alice 和 Bob 的测量基的情况下，Charlie 无法得到 Bob 的测量结果。

综上所述，通过利用 Mermin-Bell 不等式进行纠缠检测，协议在恶意模型下，对于 Charlie 的这种伪造量子纠缠态攻击也是安全的。

(2)外部窃听者的攻击 文献[16]给出了 CHSH 不等式在外部窃听者影响下的形式，即

$$S=\left(\int\rho\left(\vec{n}_a,\vec{n}_b\right)\mathrm{d}\,\vec{n}_a\,\mathrm{d}\,\vec{n}_b\right)\left[\left(\vec{a}_1\cdot\vec{n}_a\right)\left(\vec{b}_1\cdot\vec{n}_b\right)-\left(\vec{a}_1\cdot\vec{n}_a\right)\left(\vec{b}_3\cdot\vec{n}_b\right)+\left(\vec{a}_3\cdot\vec{n}_a\right)\left(\vec{b}_1\cdot\vec{n}_b\right)+\left(\vec{a}_3\cdot\vec{n}_a\right)\left(\vec{b}_3\cdot\vec{n}_b\right)\right] \tag{7}$$

其中 $\vec{a}_1,\vec{a}_3$ 是 Alice 的测量方向；$\vec{b}_1,\vec{b}_3$ 是 Bob 的测量方向；$\vec{n}_a,\vec{n}_b$ 分别为攻击者拦截测量 Alice 和 Bob 光子的测量方向。

本文利用文献[16]中的思想研究外部窃听者 Eve 对本文提出协议的攻击。在 GHZ 态制备和分发阶段，由于这时的 GHZ 粒子还没有携带任何关于 Alice 和 Bob 的隐私信息，所以当外部窃听者 Eve 在这时发动攻击时，他将得不到任何关于 Alice 和 Bob 的隐私信息。当 GHZ 粒子分发到 Alice 和 Bob 的手中后，Eve 更难获得 Alice 和 Bob 任何的隐私信息。所以，Eve 最佳的攻击是控制 Charlie 制备分发的 GHZ 态。为了抵抗 Eve 的这种攻击手段，在步骤(2)(b)中，协议利用 Mermin-Bell 不等式进行纠缠检测，判断是否存在外部窃听者 Eve。

由于 Eve 不知道 Alice, Bob 和 Charlie 将会选择哪个测量基进行测量，所以当 Eve 攻击这些 GHZ 态时，他的介入相当于引入一个物理实在量。这时构造的 S 值变为

$$S=\left|\left(\int\rho(\vec{n}_a,\vec{n}_b,\vec{n}_c)\mathrm{d}\,\vec{n}_a\,\mathrm{d}\,\vec{n}_b\,\mathrm{d}\,\vec{n}_c\right)[f_2+f_3+f_4-f_5]\right| \tag{8}$$

$$\left.\begin{aligned}f_2&=(\vec{n}_1\cdot\vec{n}_a)(\vec{n}_2\cdot\vec{n}_b)(\vec{n}_2\cdot\vec{n}_c);\ f_3=(\vec{n}_2\cdot\vec{n}_a)(\vec{n}_1\cdot\vec{n}_b)(\vec{n}_2\cdot\vec{n}_c)\\f_4&=(\vec{n}_2\cdot\vec{n}_a)(\vec{n}_2\cdot\vec{n}_b)(\vec{n}_1\cdot\vec{n}_c);\ f_5=(\vec{n}_1\cdot\vec{n}_a)(\vec{n}_1\cdot\vec{n}_b)(\vec{n}_1\cdot\vec{n}_c)\end{aligned}\right\} \tag{9}$$

其中 $\vec{n}_a,\vec{n}_b,\vec{n}_c$ 分别为 Eve 测量 Alice, Bob 和 Charlie 粒子的方向。通过简单的计算，得到 $S\le 2\sqrt{2}$ 。与式(4)中的 S 值相矛盾，这说明利用 S 值检测能够发现外部窃听者是否存在。因此，通过利用 S 值检测，协议能够有效地抵抗外部窃听者。

(3)Alice 和 Bob 彼此之间的攻击　由于拦截重发和纠缠辅助攻击都会影响 GHZ 态的量子关联性，所以通过步骤(2)(b)的 S 值检测，协议还能够杜绝 Alice 和 Bob 发动拦截重发和纠缠辅助攻击。并且由于三方都是选择 X 基和 Y 基测量自己手中的光子，所以当 Alice 发动量子存储攻击时(即 Alice 不直接测量自己手中的光子，而是等到 Bob 公布测量基后，利用与 Bob 相同的测量基测量自己手中的光子)，她不能从自己的测量结果中推断出 Bob 的测量结果，这时的量子存储攻击也就没有意义了。因此，在 S 值的检测下和三光子 GHZ 态量子关联性的保护下，Alice 和 Bob 不能得到对方的隐私信息。协议是安全的。

3.3 讨论

(1)PDQs 协议的目的和 Mermin-Bell 不等式纠缠检测共同决定三方随机选择 X 基和 Y 基测量自己手中的光子。

(a)由于隐私数据库查询协议需要 Alice 得到 Bob 某一位的隐私信息，并且 Bob 不知道 Alice 得到的是哪一位，所以协议需要 Alice 能够得到 Bob 某一位的测量结果，并且不被 Bob 得知。这时，可以利用三光子 GHZ 态在 X 基下测量的关联性，即当三方都选择 X 基测量时，任意两方的测量结果可以确定第三方的测量结果。协议可以让 Charlie 帮助 Alice 得到 Bob 的一个测量结果，并且 Bob 不知道 Alice 得到的是哪一个。Alice 可以通过这个测量结果获得 Bob 数据库中自己想要得到的隐私信息，而 Bob 不知道 Alice 获得了哪一位信息。这样就达到了隐私查询的目的。

(b)在进行 Mermin-Bell 不等式纠缠检测时，协议需要 Alice, Bob 和 Charlie 在自己的测量基下能够达到最大的 S 值。并且，在 Charlie 伪造纠缠态攻击的情况 2 中，Charlie 伪造的这些真正的三方纠缠态在 Alice, Bob 和 Charlie 自己选择的测量基下达不到最大的 S 值，这样协议才能够抵抗 Charlie 的这类攻击。

通过 Matlab 编程计算，最后得出 Alice, Bob 和 Charlie 三方选择 X 基和 Y 基进行测量时，能够同时满足上面两个条件。

(2)协议对信道损失的抵抗能力　本协议对信道损失具有很强的容忍性。信道损失只在纠缠粒子的分发阶段存在，这时，由于这些纠缠粒子并没有携带任何的隐私信息，所以 Alice 和 Bob 丢失的粒子对得到隐私信息没有任何帮助。所以不论是 Charlie，还是外部攻击者利用信道损失发动攻击，Alice 和 Bob 的隐私信息都不会受到威胁。因此，协议对于信道中丢失粒子具有很强的容忍性。

4　结论

假设第三方不能与合法用户合谋，本文提出一个基于量子第三方确定的隐私数据库查询协议。在协议中，第三方帮助用户得到数据库的部分隐私信息。同时，限定用户可以得到数据库隐私信息的数量，保护着数据库的隐私信息。进一步，协议利用 Mermin-Bell 不等式构造 S 值检测，判断第三方是否发动伪造量子态攻击去窃取数据库的隐私信息，确保第三方得不到任何用户和数据库的隐私信息。协议能够确定地控制用户得到数据库隐私信息的数量，并且对于信息损耗有着很强的容忍性。此外，

利用 Mermin-Bell 不等式保证协议的安全性，为设备无关的纠缠验证提供了一个新的应用环境。

参 考 文 献

[1] Giovannetti V, Lloyd S, and Maccone L. Quantum private queries[J]. *Physical Review Letters*, 2008, 100(230502): 1–4.

[2] Gertner Y, Ishai Y, Kushilevitz E, *et al*.. Protecting data privacy in private information retrieval schemes[J]. *Journal of Computer and Systems Sciences*, 2000, 60(3): 592–629.

[3] Chor B, Goldreich O, Kushilevitz E, *et al*.. Private information retrieval[J]. *Journal of the ACM*, 1998, 45(6): 965–981.

[4] Bennett C H and Brassard G. Quantum cryptography: public-key distribution and coin tossing[C]. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984: 175–179.

[5] Barrett J, Hardy L, and Kent A. No signaling and quantum key distribution[J]. *Physical Review Letters*, 2005, 95(010503): 1–4.

[6] Branciard C, Cavalcanti E G, Walborn S P, *et al*.. One-sided device-independent quantum key distribution: security, feasibility, and the connection with steering[J]. *Physical Review A*, 2012, 85(010301(R)): 1–5.

[7] Barrett J, Colbeck R, and Kent A. Unconditionally secure device-independent quantum key distribution with only two devices[J]. *Physical Review A*, 2012, 86(062326): 1–10.

[8] Barrett J, Colbeck R, and Kent A. Memory attacks on device-independent quantum cryptography[J]. *Physical Review Letters*, 2013, 110(010503): 1–5.

[9] Lo H K, Curty M, and Qi Bing. Measurement- device-independent quantum key distribution[J]. *Physical Review Letters*, 2012, 108(130503): 1–5.

[10] Martini F D, Giovannetti V, Lloyd S, *et al*.. Experimental quantum private queries with linear optics[J]. *Physical Review A*, 2009, 80(010302): 1–4.

[11] Giovannetti V, Lloyd S, and Maccone L. Quantum private queries: security analysis[J]. *IEEE Transactions on Information Theory,* 2010, 56(7): 3465–3477.

[12] Jakobi M, Simon C, Gisin N, *et al*.. Practical private database queries based on a quantum-key-distribution protocol[J]. *Physical Review A*, 2011, 83(022301): 1–6.

[13] Scarani V, Acín A, Ribordy G, *et al*.. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations[J]. *Physical Review Letters*, 2004, 92(057901): 1–4.

[14] Gao F, Liu B, Wen Q, *et al*.. Flexible quantum private queries based on quantum key distribution[J]. *Optics Express*, 2011, 20(16): 17411-20, DOI:10.1364/OE.20.017411.

[15] Hillery M, Bužek V, and Berthiaume A. Quantum secret sharing[J]. *Physical Review A*, 1999, 59(3): 1829–1834.

[16] Ekert K. Quantum cryptography based on Bell's theorem[J]. *Physical Review Letters*, 1991, 67(6): 661–663.

张 昭： 男，1989 年生，硕士生，研究方向为量子密码协议.

王 洪： 男，1985 年生，博士生，研究方向为量子算法与量子密码.

马 智： 女，1973 年生，教授，硕士生导师，研究方向为量子编码和量子密码.