中国科学 : 物理学 力学 天文学 2027 年 第 57 卷 第 2 期 : 220312
SCIENTIA SINICA Physica, Mechanica & Astronomica physcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS
论 文

相位编码量子保密查询的光源端实际安全性分析

刘斌[1,2], 钟宇航[1], 黄伟[3], 孙涛[2], 邵闻珠[2], 穆南锟[1*]

1. 重庆大学计算机学院, 重庆 401331
2. 石河子大学网络与信息中心, 石河子 832003
3. 西南通信研究所, 保密通信全国重点实验室, 成都 610041
*联系人, E-mail: nankun.mu@cqu.edu.cn

收稿日期: 2026-04-08; 接受日期: 2026-05-14; 网络出版日期: 2026-11-24
国家自然科学基金(编号: 62472052, 62272073)资助项目

摘要 量子保密查询是解决对称隐私信息检索问题的量子方案. 本文研究了基于量子密钥分发的相位编码量子保密查询协议的安全性. 结果表明, 多光子脉冲对量子保密查询协议中参与者的隐私构成了严重威胁. 鉴于此, 本文提出了一种基于分束器阵列的检测与防御方案. 该方案利用光子在不同分光路径下的响应统计帮助诚实参与者精准量化攻击威胁, 并通过引入零探测条件编码策略有效滤除危险信号. 分析表明, 改进后的协议能有效抵御这种攻击, 从而保证了量子保密查询过程的安全性和可靠性.

关键词 量子保密查询, 相位编码, 非理想光源, 实际安全性

1 引言

随着量子计算技术的发展, 建立在计算复杂度假设上的经典密码协议面临巨大威胁. 特别是基于大整数分解难题的公钥加密算法, 在具备强大计算能力的量子计算机面前将不再安全[1,2]. 量子通信被认为是应对量子计算威胁的有效手段[3,4], 在过去几十年中取得了巨大发展, 涌现了量子密钥分发(Quantum Key Distribution, QKD)[5–12]、量子秘密共享(Quantum Secret Sharing, QSS)[13,14]、量子安全直接通信(Quantum Secure Direct Communication, QSDC)[15,16]、多方量子远程保密会议(Multiparty Quantum Remote Secret Conference, MQRSC)[17]和量子对话(Quantum Dialogue, QD)[18]等多种协议. 值得注意的是, QKD已被严格证明具有信息论安全性[4,19,20]. 目前, QKD已跨过理论实验阶段, 在实际信息保护场景得到了广泛应用. 研究表明, 量子密码在理论上具有比传统密码方案更高的安全性[21]. 此外, 为了进一步提升量子通信网络的信道容量与分布式信息处理能力, 研究人员不仅提出了基于部分纠缠与高维系统的双向层级化及循环混合量子通信架构[22,23], 还成功实现了多粒子量子操作的联合远程控制与稳健的并行非定域逻辑门构建[24,25], 这标志着量子通信协议正向更高维度和更复杂的网络架构迈进.

在对称隐私信息检索(Symmetrically Private Information Retrieval, SPIR)模型中, 用户(Alice)旨在从数据

引用格式: 刘斌, 钟宇航, 黄伟, 等. 相位编码量子保密查询的光源端实际安全性分析. 中国科学: 物理学 力学 天文学, 2027, 57: 220312
Liu B, Zhong Y H, Huang W, et al. Analysis of practical security at the source side for phase-encoded quantum private query (in Chinese). Sci Sin-Phys Mech Astron, 2027, 57: 220312, doi: 10.1360/SSPMA-2026-0261

© 2026 《中国科学》杂志社

库持有者(Bob)的数据库中检索特定条目, 同时确保查询索引的隐私性; 而数据库持有者则致力于限制用户获取的信息量, 防止其访问除查询目标之外的任何数据. 对于理想的SPIR协议而言, Bob无法获取任何关于Alice查询项目的信息, Alice也只能取得自己查询的项目信息, 无法获取其他任何条目内容. 经典SPIR协议大多基于RSA (Rivest-Shamir-Adleman)算法构建, 在具有巨大计算能力的量子计算机面前, 极易在多项式时间内被彻底破译. 量子保密查询(Quantum Private Query, QPQ)[26–32]正是为解决这一问题所提出的SPIR量子解决方案. 尽管如此, 根据不可行定理(No-Go Theorem)[33], 即使在量子密码领域, 具有信息论安全性的理想SPIR协议也是不可能实现的. 因此, QPQ协议适当放宽了安全要求: 在数据库安全性方面, 允许Alice除了查询条目外, 获取少量其他条目信息; 在用户隐私方面, Bob的不诚实行为具有欺骗敏感性, 即任何试图确定Alice查询地址的行为, 都有非零概率被检测到.

由于QPQ协议比经典SPIR协议具有更高的安全性, 受到了学术界的广泛关注. 第一个QPQ协议由意大利学者Giovannetti等人[26]于2008年提出, 随后大量的QPQ协议应运而生, 这些协议可分为两类: 基于预言机的QPQ协议[26,34,35]和基于QKD的QPQ协议[36–48]. 其中, 基于预言机的QPQ协议虽更具有理论优势, 但在传输过程中易受到噪声的影响, 通信双方都可能利用实际量子信道的损耗窃取对方隐私. 2011年, Jakobi等人[36]受SARG04协议启发[49]设计了首个基于QKD的QPQ协议, 该协议对量子信道的损耗具有耐受性, 且可借助现有QKD技术实现. 在基于QKD的QPQ协议中, 唯一利用量子技术的过程是量子不经意密钥传输(Quantum Oblivious Key Transfer, QOKT), 其密钥交换过程与QKD高度相似, 这意味着QPQ可以在现有的QKD网络上实现. 因此, 基于QKD的QPQ 协议具有极大的发展潜力和实用价值.

目前, 研究人员已提出多种基于QKD的QPQ协议[38–41], 部分学者还针对实际信道环境下的基于QKD的QPQ协议设计了相应的纠错方案[40,50,51]. 基于QKD的QPQ协议主要采用偏振编码方式, 而大多数量子系统所使用的光纤存在双折射效应, 这会导致量子信号在传输过程中偏振态持续发生变化, 进而扭曲编码信息, 增加系统误码率. 针对这一关键问题, 2025年, Liu等人[52]提出了一种灵活的基于QKD的双向通信相位编码QPQ协议, 通过对粒子执行量子操作来编码数据库信息, 稳定性更高, 更适合当前的光纤通信量子网络. 然而, 当前技术下的量子通信设备与理论模型仍然存在差异: 上述协议假设光源是完美的单光子源, 但实际应用中的光源必然会存在多光子或无光子信号的情况. 为此, 本研究着重分析了双向通信相位编码QPQ协议可能存在的实际安全漏洞, 并提出一种基于分束器阵列的检测与防御方案, 以保障其免受多光子脉冲带来的安全威胁.

2 基于QKD的相位编码QPQ协议

首先介绍基于QKD的相位编码QPQ协议. 与以往基于QKD的QPQ协议将数据库信息编码到非正交态的方式不同, 在相位编码方案中, 数据库持有者Bob通过对用户Alice发送的信号执行不同的量子操作, 完成数据库信息的编码. 为此, 设计了如下四种不同的编码幺正操作:

$$I=\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad Z=\begin{bmatrix}1&0\\0&-1\end{bmatrix},\quad S=\begin{bmatrix}1&0\\0&\mathrm{e}^{\mathrm{i}\theta}\end{bmatrix},\quad ZS=\begin{bmatrix}1&0\\0&-\mathrm{e}^{\mathrm{i}\theta}\end{bmatrix}. \tag{1}$$

上述操作可通过相位调制实现, 对应的调制参数分别为$\{0,\pi,\theta,\pi+\theta\}$, 其中$\theta\in(0,\pi)$可根据具体场景连续选择. 具体编码规则为: 幺正操作I和Z (对应相位调制0和π)用于表示经典比特0; 幺正操作S和ZS (对应相位调制θ和$\pi+\theta$)用于表示经典比特1.

步骤1: 用户Alice制备一系列量子比特$|+\rangle$并发送给数据库持有者Bob, 这里

$$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle). \tag{2}$$

步骤2: Bob对收到的量子比特随机应用四种幺正操作$\{I,S,Z,ZS\}$中的一种, 然后将其返回给Alice. 执行相位调制φ_n的操作可由如下幺正矩阵描述

$$\boldsymbol{U}=\begin{bmatrix}1&0\\0&\mathrm{e}^{\mathrm{i}\varphi_n}\end{bmatrix}, \tag{3}$$

其中, $\varphi_n\in\{0,\pi,\theta,\pi+\theta\}$. Alice收到的光子可能处于以下四种状态之一: $|+\rangle$, $|-\rangle$, $|R\rangle$和$|L\rangle$, 它们的具体形式分

别为

$$
\begin{aligned}
|+\rangle_{(\varphi=0)} &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \\
|-\rangle_{(\varphi=\pi)} &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \\
|R\rangle_{(\varphi=\theta)} &= \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{e}^{\mathrm{i}\theta}|1\rangle\right), \\
|L\rangle_{(\varphi=\pi+\theta)} &= \frac{1}{\sqrt{2}}\left(|0\rangle - \mathrm{e}^{\mathrm{i}\theta}|1\rangle\right).
\end{aligned} \tag{4}
$$

步骤3: Alice随机选择X基($\{|+\rangle, |-\rangle\}$)或Y基($\{|R\rangle, |L\rangle\}$)对每个收到的量子比特进行测量, 并随后公布成功探测和测量的光子序列号.

步骤4: 对于Bob成功操作且Alice成功测量的每个单光子, Bob公布一个经典比特“0”或“1”, 其中比特“0”对应操作I和S, 比特“1”对应操作Z和ZS, 返回的量子比特分别属于$\{|+\rangle, |R\rangle\}$或$\{|-\rangle, |L\rangle\}$.

步骤5: Alice根据自身选择的测量基、测量结果以及Bob公布的信息, 推断初始量子态. 她将能够确定的推断结果记录为对应的密钥比特, 对于无法确定的情况则标记为“?”. Alice推导原始密钥的逻辑如表1所示. 例如, 若Bob执行操作I并公布比特“0”, 则Alice只有选择Y基测量并得到结果$\{|L\rangle\}$时, 才能准确推断返回的量子态. 在生成的非对称不经意密钥中, Bob掌握所有密钥比特的完整信息, 而Alice大约能获取其中的$(\sin^2(\theta/2))/2$个比特, 且Bob无法得知Alice具体获取了哪些比特.

步骤6: 原始不经意密钥长度为$k \times N$, 其中N为数据库条目数量, k为与N相关的安全参数. 首先将该密钥平均分成k个长度为N的子串, 然后通过按位相加的方式形成稀释密钥. 此过程旨在将Alice获取的信息限制在约1个比特. 最终, Bob知晓所有比特, Alice仅知晓约1个比特, 且Bob不知道Alice具体知晓哪个比特. 若Alice在最终密钥中未获取任何比特, 则协议失败, 需重新启动. 为降低此类失败风险, 必须选择合适的安全参数k.

步骤7: 若Alice获取了最终不经意密钥中的第j个比特(确定比特), 而她想要查询的信息位于数据库的第i个条目(目标比特), 则Alice可公布一个偏移量$s = j - i$, 使确定比特与目标比特对齐. Bob根据该公布的偏移量对密钥进行循环移位, 然后利用移位后的密钥通过一次一密加密对每个数据库条目进行加密后发送给Alice. 显然, Alice可以使用移位后的密钥准确解密并检索所需条目.

3 基于QKD的相位编码QPQ协议的非理想光源安全性分析

与大多数现有的基于QKD的QPQ协议一样, 上述协议是基于理想量子通信设备设计的. 然而, 现有技术下的量子通信设备与理想模型仍然存在一定差异, 这导致使用当前技术实现理论协议时, 会出现实际的安

表 1 Alice推导原始密钥的逻辑. 当Bob返回的量子比特为$|+\rangle$时, 若Alice选择X基测量必然得到$|+\rangle$; 若以1/2的概率选择Y基, 则测得$|L\rangle$的条件概率为$\sin^2(\theta/2)$. 因此, Alice取得原始密钥的概率为$(\sin^2(\theta/2))/2$

Table 1 Alice's logic for deducing the initial state. When the qubit returned by Bob is $|+\rangle$, Alice will deterministically obtain $|+\rangle$ if she chooses to measure in the X basis; if she selects the Y basis with a probability of 1/2, the conditional probability of measuring $|L\rangle$ is $\sin^2(\theta/2)$. Therefore, the probability of Alice obtaining the raw key is $(\sin^2(\theta/2))/2$

Bob的操作	Bob返回的量子比特	Alice的测量基	Alice的测量结果	Bob公布的经典比特	原始密钥
I	$\|+\rangle$	X	$\|+\rangle$	0	?
		Y	$\|R\rangle$		?
			$\|L\rangle$		0
S	$\|R\rangle$	X	$\|+\rangle$	0	?
			$\|-\rangle$		1
		Y	$\|R\rangle$		?
Z	$\|-\rangle$	X	$\|-\rangle$	1	?
		Y	$\|R\rangle$		0
			$\|L\rangle$		?
ZS	$\|L\rangle$	X	$\|+\rangle$	1	1
			$\|-\rangle$		?
		Y	$\|L\rangle$		?

全性漏洞. 由于完美单光子源在实际应用中难以实现, 协议光源通常由弱相干光源(Weak Coherent Pulse, WCP)代替. WCP中无法避免地存在多光子脉冲, 这些多光子不具有单光子的不可分割性, 会在QKD中引发光子数分裂攻击. 基于此, 多光子脉冲也会对基于QKD的QPQ协议的安全性构成严重的威胁. 本节将分析在多光子脉冲的影响下, 基于QKD的相位编码QPQ协议的实际安全性.

不诚实的用户Alice可能会通过发起各类攻击, 试图非法窃取数据库的额外信息. 一种常见的攻击方式是, 在协议步骤3中, 她不会立即对接收的光子进行测量, 而是将其存储在自身的寄存器中. 在Bob公布经典比特之后, Alice在完全预知待测系统可能处于的量子态及其对应先验概率的基本假设下, 对寄存器中存储的量子态执行无歧义量子态区分(Unambiguous State Discrimination, USD). 这种攻击方式的适用范围是攻击者允许测量结果以一定概率出现"无定论", 从而换取在得出有效结果时具有零误差的绝对准确性. 这意味着Alice能够以一定概率准确判别Bob返回的量子态, 进而实现非法信息窃取. 根据量子信息理论, 对于任意两个非正交量子态的USD测量, 其成功概率的理论上限严格受制于两量子态在希尔伯特空间中的重叠程度, 具体满足如下关系:

$$p^{\mathrm{USD}} \leqslant 1 - F(\sigma_0, \sigma_1), \tag{5}$$

其中, $F(\sigma_0, \sigma_1)$表示区分两个量子态σ_0和σ_1的保真度. 当两者处于纯态时, 保真度即为

$$\begin{aligned} F(\sigma_0, \sigma_1) &= \mathrm{tr}\sqrt{|v\rangle\langle v|w\rangle\langle w|v\rangle\langle v|} \\ &= |\langle w|v\rangle|\,\mathrm{tr}\sqrt{|v\rangle\langle v|} \\ &= |\langle w|v\rangle|. \end{aligned} \tag{6}$$

在理想情况下, 假设步骤1中的不诚实用户Alice准备了如下形式的假纠缠态:

$$|\psi\rangle = \sqrt{\varepsilon_0}|a_0\rangle_{\mathrm{a}}|0\rangle_{\mathrm{b}} + \sqrt{\varepsilon_1}|a_1\rangle_{\mathrm{a}}|1\rangle_{\mathrm{b}}, \tag{7}$$

其中, 系数满足归一化条件$\varepsilon_0 + \varepsilon_1 = 1$. 显然, 无论Bob公布的经典比特为"0"还是"1", Alice面临的USD判别成功概率在数学上是等价的. 以Bob公布"0"的情况为例, Alice需区分如下两个量子态:

$$|\psi_1\rangle = (I \otimes I)|\psi\rangle = \sqrt{\varepsilon_0}|a_0 0\rangle + \sqrt{\varepsilon_1}|a_1 1\rangle, \tag{8}$$

$$|\psi_2\rangle = (I \otimes S)|\psi\rangle = \sqrt{\varepsilon_0}|a_0 0\rangle + \mathrm{e}^{\mathrm{i}\theta}\sqrt{\varepsilon_1}|a_1 1\rangle. \tag{9}$$

根据式(5)和(6), 采用USD的成功概率为

$$\begin{aligned} P_1^{\mathrm{USD}} &= 1 - |\langle\psi_1|\psi_2\rangle| \\ &= 1 - |\varepsilon_0 + \mathrm{e}^{\mathrm{i}\theta}\varepsilon_1| \\ &= 1 - \sqrt{(\varepsilon_0+\varepsilon_1)^2 - 4\varepsilon_0\varepsilon_1\sin^2\frac{\theta}{2}} \\ &\leqslant 1 - \cos\frac{\theta}{2}. \end{aligned} \tag{10}$$

进一步考虑Alice在步骤1中发射多光子光源的情形. 以双光子光源为例, 不诚实用户Alice准备的假纠缠态可表示为

$$\begin{aligned} |\phi\rangle = &\sqrt{\varepsilon_{00}\varepsilon_{01}}|a_{00}a_{01}\rangle_{\mathrm{a}}|00\rangle_{\mathrm{b}} \\ &+ \sqrt{\varepsilon_{10}\varepsilon_{11}}|a_{10}a_{11}\rangle_{\mathrm{a}}|11\rangle_{\mathrm{b}}, \end{aligned} \tag{11}$$

其中, 归一化条件为$\varepsilon_{00}\varepsilon_{01} + \varepsilon_{10}\varepsilon_{11} = 1$. 当Bob公布的经典比特为"0"时, Alice需区分如下两个量子态:

$$\begin{aligned} |\phi_1\rangle &= I^{\otimes 2} \otimes I^{\otimes 2}|\phi\rangle \\ &= \sqrt{\varepsilon_{00}\varepsilon_{01}}|a_{00}a_{01}\rangle|00\rangle + \sqrt{\varepsilon_{10}\varepsilon_{11}}|a_{10}a_{11}\rangle|11\rangle, \end{aligned} \tag{12}$$

$$\begin{aligned} |\phi_2\rangle &= I^{\otimes 2} \otimes S^{\otimes 2}|\phi\rangle \\ &= \sqrt{\varepsilon_{00}\varepsilon_{01}}|a_{00}a_{01}\rangle|00\rangle \\ &\quad + \mathrm{e}^{\mathrm{i}2\theta}\sqrt{\varepsilon_{10}\varepsilon_{11}}|a_{10}a_{11}\rangle|11\rangle. \end{aligned} \tag{13}$$

对应的USD测量成功概率为

$$\begin{aligned} P_2^{\mathrm{USD}} &= 1 - |\langle\phi_1|\phi_2\rangle| \\ &= 1 - |\varepsilon_{00}\varepsilon_{01} + \mathrm{e}^{\mathrm{i}2\theta}\varepsilon_{10}\varepsilon_{11}| \\ &= 1 - \sqrt{(\varepsilon_{00}\varepsilon_{01} + \varepsilon_{10}\varepsilon_{11})^2 - 4\varepsilon_{00}\varepsilon_{01}\varepsilon_{10}\varepsilon_{11}\sin^2\theta} \\ &\leqslant 1 - |\cos\theta|. \end{aligned} \tag{14}$$

如图1所示, 在理想单光子源的情况下, Alice利用USD测量获得的成功概率略高于诚实案例, 但带来的增益并不显著. 然而, 一旦攻击者能够利用多光子源(如双光子态对应的P_2^{USD}), USD测量的优势将被急剧放大. 表2列举了在设定相位参数$\theta = 3\pi/8$时, 针对不同规模数据库(N)的多光子攻击破坏力评估. 其中, $\bar{n}$为诚实用户预期获取的条目数; n_1为利用单光子USD攻击获取的条目数; n_2为利用双光子USD攻击获取的

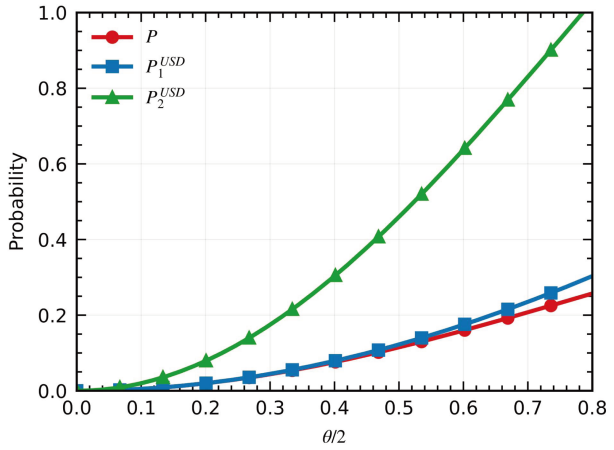

图 1 (网络版彩图)诚实用户获取确定比特的理论概率(P)与不诚实用户利用单光子(P_1^{USD})及双光子(P_2^{USD})实施USD攻击的成功概率对比

Figure 1 (Color online) Comparison of the theoretical probability (P) for an honest user to obtain a deterministic bit versus the success probabilities of USD attacks launched by a dishonest user using single-photon (P_1^{USD}) and two-photon (P_2^{USD}) sources.

表 2 针对不同规模数据库, 利用多光子脉冲进行攻击的示例($\theta = 3\pi/8$)

Table 2 Examples of attacks using multi-photon pulses on databases of different scales ($\theta = 3\pi/8$)

N	k	$\bar{n}$	n_1	n_2
10^3	3	3.68	4.79	235.26
5×10^3	4	2.84	4.03	726.15
10^4	4	5.67	8.07	1452.30
5×10^4	5	4.38	6.80	4482.61
10^5	5	8.75	13.60	8965.22
10^6	6	13.51	22.91	55343.47

条目数. 需要说明的是, 当数据库规模达到$N = 10^6$时, 若安全参数$k = 7$, 诚实用户预期获取的条目数$\bar{n}$仅为2.09个, 但此时协议失败的概率达到12.4%, 远高于正常标准. 表中的参数设定本质上反映了数据库规模、诚实用户预期获取条目数以及协议失败概率三者间的相互制约关系. 一般而言, 协议失败概率的提升会促使诚实用户获取条目数的增加. 在此基础上, 本文统一设定$\theta = 3\pi/8$以构建标准化的对比分析基准. 理论分析表明, 上述参数的具体取值对于多光子信号攻击的影响有限.

表中数据表明, 随着数据库规模的扩大, 双光子攻击导致的信息泄露量呈现出极端的非线性增长. 这意味着, 在协议安全性分析中, 多光子成分的存在会极大地提升不诚实用户利用假纠缠态进行欺骗攻击的成功率, 从而构成严重的安全隐患. 值得说明的是, USD攻击虽为QPQ协议中极具代表性的攻击手段, 但本文仅将其作为一种具体的攻击例证, 旨在直观阐明并量化多光子成分所带来的实际安全威胁. 在构建系统整体的安全性分析框架时, 我们并未对不诚实用户所采取的具体攻击策略施加任何特定假设. 接下来, 将介绍基于分束器阵列的多光子检测与防御方案以应对多光子脉冲带来的安全威胁.

4 基于分束器阵列的多光子攻击检测与防御方案

在实际基于WCP的QPQ协议中, 不诚实用户Alice极易利用光源中固有的多光子脉冲实施攻击, 极大地提升其获取数据库非法信息的成功率. 针对这一威胁, 我们从量子力学中光子的不可分割性中汲取物理灵感, 提出了一种基于分束器阵列的多光子检测与防御方案, 巧妙利用空间分流引发的符合响应特征来实现对危险信号的精准检测与被动压制. 该方案在数据库持有者Bob的编码端口引入多光子检测模块, 可评估实际到达Bob端的多光子比例, 并通过零探测条件编码策略压制多光子攻击. 为直观展示本方案的防御机制, 图2给出了改进后的QPQ协议示意图. 在面临攻击与正常通信时, 该模块的物理响应存在本质差异:

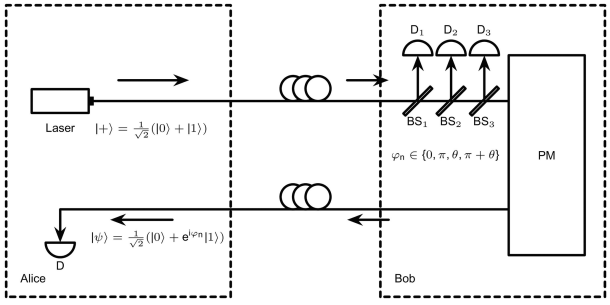

图 2 改进的双向量子通信协议示意图. 其中, PM为相位调制器, D为探测器. Bob端引入了由分束器(BS_1–BS_3)和探测器(D_1–D_3)组成的光子检测模块以防范多光子攻击

Figure 2 Schematic diagram of the improved bidirectional quantum communication protocol. PM denotes the phase modulator, D denotes the detector. A photon monitoring module consisting of beam splitters (BS_1–BS_3) and detectors (D_1–D_3) is introduced at Bob's side to defend against multi-photon attacks.

当Alice企图利用多光子脉冲窃取额外信息时, 该脉冲需先穿透分束器阵列. 依据光子在分束器中的独立传输与概率散射特性, 包含多个光子的脉冲极易在分光路径中被分散, 从而触发一个或多个探测器产生响应; 相反, 正常的单光子脉冲则有确定的概率无损穿透该模块, 直达后端的相位调制器.

接下来, 说明数据库持有者Bob进行的操作. Bob对收到的量子比特执行相位调制$\boldsymbol{U}$ (即I, S, Z和ZS操作)之前, 在其编码端口接入多光子检测模块. 该模块由三个级联的分光比为50:50的分束器以及三个对应的光子探测器(D_1, D_2和D_3)组成. 在该光路构型下, 入射光脉冲依次穿过各分束器, 其透射端最终连接到Bob的相位调制器, 而反射端分别连接至D_1, D_2和D_3. 在此装置下, 单个光子到达D_1, D_2和D_3的概率分别为1/2, 1/4和1/8, 成功到达相位调制器的概率为1/8.

基于上述硬件装置, Bob可通过统计探测器阵列的响应特征来实现光子数分布的评估. 探测器阵列响应规律如表3所示. 该规律基于光子行为独立性假设, 即脉冲内的各光子在经过分束器阵列时的分光行为遵循统计独立分布. 由于Alice连续不断地制备信号脉冲, 在脉冲数为N的通信周期内, Bob依据探测器的触发情况将响应事件划分为零响应事件(N_0)、单响应事件(N_1)以及符合响应事件(N_2). 由于单光子在任一时刻仅能触发单一探测器, 排除探测器自身暗计数引发的偶发响应, 系统中的符合响应事件N_2的唯一真实物理来源即为多光子脉冲. 此外, 鉴于WCP的光子数分布满足泊松统计规律, 高阶脉冲发生的概率随光子数增加而呈指数级衰减, 为了简化模型同时兼顾安全性, 我们提取双光子的理论响应特征来构建基础反演模型. 需要强调的是, 此反演模型旨在通过估计多光子概率, 从而确立协议的安全性界限评估, 而非对量子态分布进行绝对精确的层析.

基于上述物理框架, 结合分束器的透射与反射概率分布, 构建包含真空态比例P_0、单光子比例P_1与多光子比例P_m的理论计数方程组为

$$\begin{cases} \dfrac{N_2}{N} = \dfrac{7}{16}P_m, \\ \dfrac{N_1}{N} = \dfrac{7}{8}P_1 + \dfrac{35}{64}P_m, \\ P_0 + P_1 + P_m = 1. \end{cases} \tag{15}$$

通过求解上述方程组, Bob可以得到经过光纤信道衰减后到达其编码端口的光子数分布, 即

$$\begin{cases} P_m = \dfrac{16}{7}\dfrac{N_2}{N}, \\ P_1 = \dfrac{8}{7}\left(\dfrac{N_1}{N} - \dfrac{5}{4}\dfrac{N_2}{N}\right). \end{cases} \tag{16}$$

必须明确的是, 上述模型虽然将所有符合计数均按双光子($n = 2$)的响应权重进行折算, 但并没有低估高阶多光子带来的安全威胁, 反而在严格意义上构成了信道中真实多光子总比例的安全上界. 具体证明如下: 设η_n为包含n个光子的脉冲穿过分束器阵列后, 触发至少两个探测器(即产生符合计数)的概率. 显然, 随着光子数n的增加, 脉冲在不同分光路径中散布并触发多个探测器的概率必然增长, 即对于任意$n > 2$, 恒有$\eta_n > \eta_2$. 在实际物理过程中, 探测器阵列记录的真实符合计数总和N_2是所有$n \geqslant 2$阶多光子成分综合贡献的结果, 其具体展开式为

$$\begin{aligned} N_2 &= N\sum_{n=2}^{\infty}\eta_n P_n \\ &= N(\eta_2 P_2 + \eta_3 P_3 + \eta_4 P_4 + \cdots), \end{aligned} \tag{17}$$

其中, P_n为脉冲中包含n个光子的真实概率. 而在参数反演方程中, 计算所得的多光子概率(即P_m)是保守地将所有符合计数事件均归因于双光子触发, 其公式为

$$P_m = \frac{1}{\eta_2}\frac{N_2}{N}. \tag{18}$$

将真实符合计数N_2的展开式代入该反演公式, 可得

$$\begin{aligned} P_m &= \sum_{n=2}^{\infty}\frac{\eta_n}{\eta_2}P_n \\ &= P_2 + \frac{\eta_3}{\eta_2}P_3 + \frac{\eta_4}{\eta_2}P_4 + \cdots. \end{aligned} \tag{19}$$

鉴于当$n > 2$时, 权重系数$\eta_n/\eta_2 > 1$恒成立, 上述展开式必然满足以下不等式关系:

$$P_m > P_2 + P_3 + P_4 + \cdots = P_m^{\text{true}}, \tag{20}$$

表 3 探测器阵列响应规律

Table 3 Response law of detector array

光源类型	零响应概率	单响应概率	双响应概率
单光子	1/8	7/8	0
双光子	1/64	35/64	7/16

其中, P_m^{true}为真实存在的包含高阶成分的总多光子概率. 上述推导严密地证明了, 基于双光子模型的近似反演巧妙利用了探测器阵列对高阶光子的非线性响应特性, 将极少量的高阶多光子事件过度折算、放大为了数量更多的双光子事件, 从而确保了所评估的多光子比例绝对安全.

在获取光子统计信息的基础上, 引入零探测条件编码策略以实现对多光子脉冲的被动压制. 具体而言, Bob当且仅当D_1, D_2和D_3均未响应时, 才启动相位调制器对该脉冲进行编码并返回Alice; 反之, 若有任何探测器响应, 则直接丢弃该脉冲. 由于光子是独立传输的, 包含n个光子的脉冲完全穿透该检测模块的概率服从$T_n = (1/8)^n$的指数衰减规律. 例如, 单光子穿透概率为$T_1 = 1/8$, 双光子穿透概率为$T_2 = 1/64$. 因此, 在Bob最终执行编码的有效脉冲样本中, 多光子成分的比重被显著压缩为

$$R = \frac{P_m \cdot T_2}{P_1 \cdot T_1 + P_m \cdot T_2}. \tag{21}$$

相较于初始输入比例P_m/P_1, 该零探测条件编码策略利用了多光子更易触发探测器的物理本质, 将危险的多光子泄露率急剧削减了1个数量级, 从而从源头上极大限制了攻击者的信息获取能力.

结合光子探测器计数与有效编码中多光子比例, Bob可以进行严密的攻击检测与安全性评估. 我们采用最坏情况假设, 即假定信道中的传输损耗完全由单光子承担, 而Alice优先且无损地获得了Bob返回的所有多光子脉冲. 基于此假设, Bob预估向Alice暴露的多光子总数上限为

$$M = N_0 \times R. \tag{22}$$

结合协议步骤3中Alice在接收端声明的光子成功探测与测量结果, 可确定Alice的有效测量总数为$k \times N$. 由此可得, 最大信息泄露比例为

$$\tau = \frac{M}{k \times N}. \tag{23}$$

考虑到实际物理信道中多光子脉冲不可避免地会经历传输损耗, 真实返回Alice端的多光子比例必然受到该数学上界τ的严格约束.

在确立最大信息泄露比例τ后, 可进一步量化评估该被动防御方案的安全效能. 根据协议的步骤6, 不诚实用户Alice需准确获取k个原始密钥比特才能确定1个最终的密钥比特. 在最坏情况假设下, Alice对占比上限为τ的多光子脉冲拥有100%的信息获取能力; 而对剩余占比为$1-\tau$的安全单光子脉冲, 其只能以P_1^{USD}的成功率实施USD测量. 因此, Alice获取单个最终密钥比特的概率上限P_k遵循二项式分布展开, 可严格表述为

$$P_k < \sum_{i=0}^{k} \binom{k}{i} \tau^{k-i} (1-\tau)^i (P_1^{\text{USD}})^i. \tag{24}$$

本方案的防御性能如表4所示. 数据表明, 尽管被动防御方案极大压制了多光子攻击的破坏力, 但不诚实Alice实际获取的有效条目数仍显著高于理论预期. 针对这一问题, 我们引入Gao等人[40]提出的进一步后处理方法. 该方法要求通信双方生成g个最终不经意密钥; Alice依据确定比特与目标条目的位置关系逐一公布g个偏移量, 随后Bob与Alice依次使用这些偏移密钥完成数据库的多重加密与解密操作. 表5量化展示了经过20次独立模拟, 不同g值下Alice的最优信息获取量. 根据模拟结果, 在大多数情况下, $g = 2$或$g = 3$是合理的选择.

此外, 实际探测器的死时间效应对系统的安全性影响呈现出高度的复杂性. 一方面, 在统计与参数反演

表 4 针对不同规模数据库, 本方案在$\tau = 0.1$和$\tau = 0.05$时的多光子攻击防御效果($\theta = 3\pi/8$)

Table 4 Defense performance of the proposed scheme against multi-photon attacks at $\tau = 0.1$ and $\tau = 0.05$ for various database scales ($\theta = 3\pi/8$)

N	k	$\bar{n}$	n_2	$\tau = 0.1$	$\tau = 0.05$
10^3	3	3.68	235.26	15.94	9.28
5×10^3	4	2.84	726.15	20.06	9.74
10^4	4	5.67	1452.30	40.12	19.49
5×10^4	5	4.38	4482.61	50.49	20.47
10^5	5	8.75	8965.22	100.97	40.95
10^6	6	13.51	55343.47	254.13	86.03

表 5 不同g与τ下, Alice的最优信息获取量模拟结果($N = 10^5, k = 5$)

Table 5 Simulation results of the optimal information gain by Alice under different g and τ ($N = 10^5, k = 5$)

g	$\tau = 0$	$\tau = 0.2$	$\tau = 0.1$	$\tau = 0.05$
1	8.40	417.35	95.00	39.95
2	1.05	9.90	3.55	2.10
3	1.00	3.65	2.00	1.20

层面上, 死时间会导致符合计数的漏计. 例如, 当多光子脉冲本应同时触发D_1和D_2时, 若D_1恰巧处于恢复期, 该事件将被系统错误地降级记录为单响应事件, 导致N_1虚高而N_2被严重低估. 这将直接致使模型计算出的多光子比例P_m低于信道真实值, 给攻击者留下潜在的窃听空间. 另一方面, 在物理传输层面上, 死时间效应对协议又存在一定的增益作用: 当多光子脉冲中的部分光子落入处于死时间的探测器而被吸收, 且其余探测器未响应时, 协议将触发零探测条件编码. 此时, 到达编码端口的剩余光子大概率已降级为单光子, 这相当于在物理层面消除了多光子的隐患, 对协议安全性起到了保护作用. 综合上述双重机制, 探测器非理想特性对系统最终安全容量的影响十分复杂. 鉴于本文现阶段的研究重点聚焦于光源端的实际安全性分析, 关于探测器死时间等接收端复杂硬件参数的定量建模, 将留待后续研究作进一步探讨.

5 讨论和结论

本文在基于QKD的相位编码QPQ协议的基础上, 提出了一种适用于非理想光源环境且能容忍信道损失的基于分束器阵列的多光子攻击检测与防御方案. 该方案通过在数据库持有者端引入被动式多光子检测模块, 将探测器阵列的响应统计特征与理论光子数分布模型相结合, 从而能够评估并判断协议的实际安全状况.

在安全性分析层面, 我们具体分析了不诚实用户利用多光子脉冲实施光子数分裂攻击的场景. 针对这类攻击, 该方案通过统计探测器的零响应、单响应以及符合响应事件, 精确反演出经过信道衰减后到达Bob接收端的多光子概率与单光子概率, 并创造性地采用了零探测条件编码策略. 由于包含多个光子的脉冲相较于单光子更容易触发探测器, 一旦检测到异常响应即舍弃当前脉冲, 该策略能够被动且高效地过滤掉大部分危险的多光子成分. 在此基础上, 通过采纳最坏情况假设, 将所有信道传输损耗归于安全单光子, 严格推导出了最大信息泄露比例的数学上界.

尽管如此, 本方案在实际应用中仍面临一定的局限性. 现实物理环境的复杂性极易干扰硬件设备的理想性能, 例如分束器分光比例的偏移和探测器非完美的探测效率等. 这些非理想因素的引入, 不仅增加了构建高精度光子统计响应模型的复杂度, 也为理论方程组的严密反演与求解带来了不可忽视的挑战.

此外, 本方案采用的零探测条件编码策略在提升系统安全性的同时, 不可避免地引发了安全性与通信效率之间的权衡. 理论计算表明, 光子在穿过级联分束器阵列时, 即便是安全的单光子脉冲, 也有高达87.5%的概率触发探测器而被系统主动拦截并丢弃. 这种被动过滤机制虽然从物理层面上高效压制了多光子, 但代价是有效信号的衰减与密钥生成率的下降. 然而, 考虑到现实中基于WCP制备的脉冲绝大部分为不携带光子的真空态, 真正包含光子的有效脉冲比例本就极为有限. 此外, 在近几年研究较热的双场量子密钥分发与相位匹配量子密钥分发等前沿协议中, 同样存在大比例丢弃信号的筛选机制. 因此, 尽管本方案的通信效率存在较大的下降幅度, 但以适当的效率折损为代价来弥补多光子脉冲带来的致命安全漏洞, 在实际量子通信系统的工程应用中是完全可以接受的.

总而言之, 尽管引入分束器阵列的防御策略极大地弥补了QPQ协议在非理想光源下的安全漏洞, 但面对日益复杂的量子攻击手段与现实环境的物理约束, 仍需对其理论模型与容错机制展开深入优化, 以切实保障协议在未来实际部署中的长期可靠性与高效性.

参考文献

1 Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe: IEEE, 1994. 126–134

2 Grover L K. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. New York: ACM, 1996. 212–219

3 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195

4 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444

5 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Theor Comput Sci, 2014, 560: 7–11
6 Gisin N, Thew R. Quantum communication. Nat Photon, 2007, 1: 165–171
7 Noh T G. Counterfactual quantum cryptography. Phys Rev Lett, 2009, 103: 230501
8 Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance. Nature, 2014, 509: 475–478
9 Zhou C, Wang X Y, Zhang Z G, et al. Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes. Sci China-Phys Mech Astron, 2021, 64: 260311
10 Zhang W, van Leent T, Redeker K, et al. A device-independent quantum key distribution system for distant users. Nature, 2022, 607: 687–691
11 Yan P S, Zhou L, Zhong W, et al. Advances in quantum entanglement purification. Sci China-Phys Mech Astron, 2023, 66: 250301
12 Li H W, Hao C P, Chen Z J, et al. Security of quantum key distribution with virtual mutually unbiased bases. Sci China-Phys Mech Astron, 2024, 67: 270313
13 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834
14 Xie Y, Liu B, Li X Y, et al. Decoy state quantum secret sharing protocol with collective detection (in Chinese). Sci Sin-Phys Mech Astron, 2025, 55: 240322 [谢颖, 刘斌, 李星雨, 等. 诱骗态联合检测窃听量子秘密共享协议. 中国科学: 物理学 力学 天文学, 2025, 55: 240322]
15 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302
16 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317
17 Li X H, Li C Y, Deng F G, et al. Multiparty quantum remote secret conference. Chin Phys Lett, 2007, 24: 23–26
18 Nguyen B A. Quantum dialogue. Phys Lett A, 2004, 328: 6–10
19 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050–2056
20 Lu H, Fung C H F, Cai Q. Two-way deterministic quantum key distribution against detector-side-channel attacks. Phys Rev A, 2013, 88: 044302
21 Dulek Y, Grilo A B, Jeffery S, et al. Secure multi-party quantum computation with a dishonest majority. In: Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2020. 729–758
22 Jing R H, Huang Y B, Yang J, et al. Deterministic bidirectional hierarchical teleportation of an arbitrary high-dimensional multi-particle state with a partially entangled quantum channel. Eur Phys J Plus, 2024, 139: 894
23 Lu N S, Ye D X, He L M, et al. Probabilistic bidirectional controlled cyclic hybrid quantum communication of arbitrary m-qudit states via high-dimensional partially entangled state (in Chinese). Sci Sin-Phys Mech Astron, 2026, 56: 100313 [陆霓诗, 叶当鑫, 何良明, 等. 基于部分纠缠态的任意高维多粒子态概率双向循环可控混合远程传送. 中国科学: 物理学 力学 天文学, 2026, 56: 100313]
24 Jing R, Lan Q, Zhou P. Hierarchical controlled joint remote implementation of the partially unknown operations of m qudits via m high-dimensional entangled states. Entropy, 2024, 26: 857
25 Xie Q Z, Lu N S, Huang P W, et al. Robust hyperparallel nonlocal operation assisted by diamond nitrogen-vacancy center coupled to a single-side optical microcavity (in Chinese). Sci Sin-Phys Mech Astron, 2025, 55: 100312 [谢倩珠, 陆霓诗, 黄培文, 等. 基于金刚石NV色芯极化-时间两自由度并行稳健非定域控制非门的远程实现. 中国科学: 物理学 力学 天文学, 2025, 55: 100312]
26 Giovannetti V, Lloyd S, Maccone L. Quantum private queries. Phys Rev Lett, 2008, 100: 230502
27 Wei C Y, Cai X Q, Liu B, et al. A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. IEEE Trans Comput, 2018, 67: 2–8
28 Liu B, Xia S, Xiao D, et al. Decoy-state method for quantum-key-distribution-based quantum private query. Sci China-Phys Mech Astron, 2022, 65: 240312
29 Yang Y G, Sun S J, Xu P, et al. Flexible protocol for quantum private query based on B92 protocol. Quantum Inf Process, 2014, 13: 805–813
30 Shen Z, Shao W, Li Z, et al. Cryptanalysis and improvement to the quantum private query protocol for enhancing database privacy. Commun Theor Phys, 2025, 77: 065108
31 Sun H, Xing D, Dou Z, et al. Unidirectional quantum private comparison based on quantum private query. Chin Phys B, 2025, 34: 050308
32 Deng Z, Sun H, Zhang K, et al. A novel quantum private query protocol and its application in private set intersection. Sci Rep, 2025, 15: 35758
33 Lo H K. Insecurity of quantum secure computations. Phys Rev A, 1997, 56: 1154–1162
34 Olejnik L. Secure quantum private information retrieval using phase-encoded queries. Phys Rev A, 2011, 84: 022313
35 Xiao H, Huang W H, Zhou M. An efficient quantum private query protocol based on oracle and Grover iteration. Int J Theor Phys, 2019, 58: 3025–3035
36 Jakobi M, Simon C, Gisin N, et al. Practical private database queries based on a quantum-key-distribution protocol. Phys Rev A, 2011, 83: 022301
37 Gao F, Liu B, Wen Q Y, et al. Flexible quantum private queries based on quantum key distribution. Opt Express, 2012, 20: 17411–17420
38 Zhang J L, Guo F Z, Gao F, et al. Private database queries based on counterfactual quantum key distribution. Phys Rev A, 2013, 88: 022334

39 Liu B, Gao F, Huang W, et al. QKD-based quantum private query without a failure probability. Sci China-Phys Mech Astron, 2015, 58: 100301

40 Gao F, Liu B, Huang W, et al. Postprocessing of the oblivious key in quantum private query. IEEE J Sel Top Quantum Electron, 2015, 21: 98–108

41 Xu S W, Sun Y, Lin S. Quantum private query based on single-photon interference. Quantum Inf Process, 2016, 15: 3301–3310

42 Maitra A, Paul G, Roy S. Device-independent quantum private query. Phys Rev A, 2017, 95: 042344

43 Gao F, Qin S J, Huang W, et al. Quantum private query: A new kind of practical quantum cryptographic protocol. Sci China-Phys Mech Astron, 2019, 62: 070301

44 Liu D M, Yan L L, Xu S H, et al. New flexible quantum private query protocol against rotation noise. Quantum Inf Process, 2021, 20: 49

45 Zhang X, Qin S, Zhang X, et al. Security loophole and improvement of quantum private query protocol based on W state. Int J Theor Phys, 2023, 62: 162

46 Liu D, Li J, Chen X, et al. Quantum private query protocol based on counterfactual quantum key distribution with noiseless attack. Quantum Inf Process, 2024, 23: 352

47 Wei C Y, Wang Q L, Cai X Q, et al. Improving user privacy in practical quantum private query with group honesty checking. Adv Quantum Tech, 2025, 8: 2400429

48 Liu B, Huang J, Huang W, et al. Analysis and defense against joint-measurement attacks to quantum private query protocols for multi-rounds. Sci China-Phys Mech Astron, 2025, 68: 280311

49 Scarani V, Acín A, Ribordy G, et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys Rev Lett, 2004, 92: 057901

50 Chan P, Lucio-Martinez I, Mo X, et al. Performing private database queries in a real-world environment using a quantum protocol. Sci Rep, 2014, 4: 5233

51 Wei C Y, Cai X Q, Wang T Y, et al. Error tolerance bound in QKD-based quantum private query. IEEE J Sel Areas Commun, 2020, 38: 517–527

52 Liu B, Li X, Gong B, et al. Quantum-key-distribution-based quantum private query with phase encoding. Adv Quantum Tech, 2026, 9: e00471

Analysis of practical security at the source side for phase-encoded quantum private query

LIU Bin[1,2], ZHONG YuHang[1], HUANG Wei[3], SUN Tao[2], SHAO WenZhu[2] & MU NanKun[1*]

[1]*College of Computer Science, Chongqing University, Chongqing 401331, China*
[2]*Network and Information Center, Shihezi University, Shihezi 832003, China*
[3]*National Key Laboratory of Secure Communication, Southwest Institute of Communication, Chengdu 610041, China*
**Corresponding author (email: nankun.mu@cqu.edu.cn)*

Quantum private query (QPQ) is a quantum solution to the symmetric private information retrieval (SPIR) problem. This work investigates the security of a phase-encoded quantum private query protocol based on quantum key distribution (QKD). The results demonstrate that multi-photon pulses pose a severe threat to the privacy of participants in the QPQ protocol. In light of this, this work proposes a monitoring and defense scheme based on a beam-splitter array. This scheme utilizes the response statistics of photons across different splitting paths to enable honest participants to accurately quantify the attack threat, and effectively filters out dangerous signals by introducing a zero-detection conditional encoding strategy. Analysis indicates that the improved protocol can effectively resist such attacks, thereby ensuring the security and reliability of the quantum private query process.

quantum private query, phase-encoding, non-ideal light source, practical security

doi: 10.1360/SSPMA-2026-0261