EAQKD：基于纠缠的认证量子密钥分发

Noureldin Mohamed* (nomo89098@hbku.edu.qa)、Saif Al-Kuwari* (smalkuwari@hbku.edu.qa)
*卡塔尔量子计算中心，科学与工程学院，哈马德·本·哈利法大学，多哈，卡塔尔。

arXiv:2603.02375v1 [quant-ph] 2 Mar 2026

摘要——**量子密钥分发（QKD）所承诺的无条件安全，取决于是否具备经过认证的经典信道。然而，实际应用往往忽视这一要求，或依赖会损害长期安全性的计算假设。为应对这些挑战，本文提出基于纠缠的认证量子密钥分发（EAQKD），这是一种针对量子密码密钥交换中的关键安全与实用性限制而设计的新协议。我们的方法将量子纠缠分发与信息论认证相结合。我们通过一个全面的离散事件仿真框架评估 EAQKD 的性能，该框架依据现实的信道特性和实验设备参数构建。我们的建模纳入了实用量子光学装置的参数，包括自发参量下转换纠缠源、超导纳米线探测器以及光纤信道缺陷。结果表明，量子比特误码率始终低于 11% 的安全阈值（从 10 km 时的 1.86% 到 200 km 时的 9.27%），短距离下安全密钥率可达 1.12×10^5 比特/秒，在 200 km 时仍能保持 9.8 比特/秒的实用速率。结合量子中继器架构后，我们的分析预测，EAQKD 可将安全通信距离扩展至 500 km 以上，同时提供信息论安全保证。与 BB84、E91 和双场量子密钥分发协议的比较分析表明，EAQKD 在安全性、实用性能和实现稳健性之间实现了更优的平衡。本研究推进了量子密码学的发展，为未来量子通信网络中的安全密钥分发提供了经过严格分析的工程参考。**

关键词： 量子密钥分发、纠缠、密码学、认证、安全性

I. 引言

量子密钥分发（QKD）代表了一种革命性的密码密钥交换方法，利用量子力学的内在属性来实现信息论安全性 [2]。不同于 RSA 和 Diffie-Hellman 等经典密码方法，QKD 的安全性建立在基本物理定律之上，而非计算复杂性假设之上。随着量子计算的发展可能威胁传统密码系统的安全性，这一区别变得日益重要 [23]。

尽管量子密钥分发在理论上取得了重大进展，实际实现仍面临若干关键挑战，限制了其安全性和可部署性 [22]。采用制备-测量方式的协议（如 BB84 [1]）在使用衰减激光源实现时，仍容易遭受光子数分裂攻击 [9]。此外，针对多个量子密钥分发系统的基于探测器的侧信道攻击已被证实，危及其安全保障 [15]。类似地，实际中用于后处理的经典通信信道往往未得到充分认证，从而产生一个关键漏洞：认证假设与实际实现并不相符 [21]。缺乏可靠认证时，对手可以冒充双方，实际上分别与 Alice 和 Bob 建立量子信道，同时控制双方之间的所有经典通信（即中间人攻击）。这种认证的安全性严格取决于标签长度 t 以及伪造成功的概率 [11]:

$$P_{\text{forge}} \leq \frac{l \cdot q}{2^t} \tag{1}$$

其中， l 是消息长度， q 是认证查询的数量。最后，光纤中的传输损耗将大多数量子密钥分发系统的实际传输距离限制在约 100-200 km，除非使用量子中继器 [24]。尽管 E91 [6]等基于纠缠的协议通过贝尔不等式验证解决了其中一些挑战，但与制备-测量方法相比，它们通常只能达到较低的密钥率，并且仍然需要对经典信道进行适当的认证 [16]。近期的进展（如双场量子密钥分发） [14],改善了距离扩展特性，但也引入了与相位稳定和干涉对准相关的新实施挑战。

尽管理论上取得了这些重大进展，但在同时应对量子和经典层面的脆弱性、并在实用距离上保持可用密钥率方面，仍存在明显空白。当前大多数方法要么以牺牲密钥率为代价优先保障量子安全性（例如，标准纠缠协议），要么以增加实现复杂度为代价关注传输距离（例如，双场量子密钥分发），且经典认证层往往仍依赖计算假设。我们的研究通过开发 EAQKD协议来填补这一空白：该协议将基于纠缠的量子安全性与稳健的信息论安全的经典认证相结合，同时优化实用性能。

本文介绍纠缠辅助量子密钥分发（EAQKD），这是一种新型协议，通过结合基于纠缠的量子密钥分发的安全优势与稳健的经典认证，克服了上述局限。我们的主要贡献包括：

- 一套全面的协议设计，将量子纠缠分发与经典信道的抗量子认证相结合

通讯作者：nomo89098@hbku.edu.qa

- 非对称基选择优化，在保持安全性验证的同时显著提高密钥生成效率
- 全面评估该协议在 10 km 至 200 km 距离范围内的性能，并详细分析量子比特误码率、贝尔参数测量和安全密钥率。
- 采用纠缠纯化技术，扩展该协议的有效范围
- 与领先的量子密钥分发协议进行比较评估，展示纠缠辅助量子密钥分发在安全性、距离和实际部署能力方面的优势
- 分析量子中继器增强后的纠缠辅助量子密钥分发性能，展现其实现 500 km 以上安全密钥分发的潜力。

我们的仿真结果表明，在所有测试距离下，纠缠辅助量子密钥分发的量子比特误码率（量子比特错误率）均低于 11% 的临界安全阈值，从 10 km 时的 1.86% 到 200 km 时的 9.27% 不等。贝尔不等式测量证实了真实的量子纠缠：在 10 km 时为 $S = 2.61 \pm 0.08$，到 150 km 时降至 $S = 2.12 \pm 0.11$。短距离下的安全密钥率可达每秒 1.12×10^5 比特，在 200 km 时仍能保持约每秒 10 比特的实用速率。

本文其余部分安排如下：第二节介绍量子密钥分发的基本背景以及现有方法的局限性。第三节详细说明纠缠辅助量子密钥分发协议的设计，概述从纠缠生成到认证密钥更新的五个操作阶段。第四节介绍我们汇总的安全性分析，以及用于验证系统的离散事件仿真框架。第五节分析性能结果，重点关注密钥率、纠缠质量和纯化效应。第六节将本方法与 BB84、E91 和双场量子密钥分发协议进行比较评估。第七节考察使用量子中继器进行距离扩展的可行性，第八节则总结研究发现并展望未来工作方向。

II. 预备知识

自诞生以来，量子密钥分发取得了显著发展，每一代协议都在应对特定漏洞的同时引入了新的能力 [19]。量子密钥分发的安全性源于基本的量子原理，尤其是形式化表述如下的测量扰动原理：

$$\Delta X \cdot \Delta P \geq \frac{\hbar}{2} \tag{2}$$

其中，ΔX 和 ΔP 表示互补可观测量的不确定性。该原理确保窃听者的任何测量尝试都会必然引入可检测的扰动 [8]。

A. 制备-测量量子密钥分发协议

开创性的 BB84 协议 [1]确立了量子密钥分发中的制备-测量范式。在 BB84 中，Alice 将经典比特编码为单光子的偏振态，并在两个共轭基之间随机选择：直线基 $\{|0\rangle, |1\rangle\}$ 和对角基 $\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$。Bob 使用独立随机选择的基测量每个接收到的光子。传输完成后，Alice 和 Bob 通过认证经典信道公开各自选择的基，仅保留双方基选择一致的比特，形成筛选密钥。

BB84 的安全性基于这样一个事实：在错误的基上测量量子态会引入错误。量子比特误码率（QBER）是主要的安全参数，安全密钥率 R 为：

$$R_{\text{BB84}} = R_{\text{raw}} \cdot [1 - 2h(e)] - f(e) \cdot h(e) \tag{3}$$

其中，$R_{\text{raw}} = \eta\mu e^{-\mu}/2$ 为原始密钥率，η 为信道透射率，μ 为平均光子数，$h(e) = -e\log_2(e) - (1-e)\log_2(1-e)$ 为二元香农熵，$f(e) \geq 1$ 为纠错效率损失 [22]。

然而，制备-测量协议容易受到以下几种漏洞的影响：

- **光子数分离（PNS）攻击**：实际的单光子源通常会发射光子数服从泊松分布的脉冲。Eve 可以利用多光子脉冲，在不被探测到的情况下截获多余的光子 [9]。对于平均光子数为 μ的光源，发射多光子的概率为：

$$P(n \geq 2|\text{click}) = \frac{1 - e^{-\mu} - \mu e^{-\mu}}{1 - e^{-\mu}} \tag{4}$$

- **探测器漏洞**：时移攻击和致盲攻击会利用单光子探测器的缺陷，使 Eve 能够在不被发现的情况下控制 Bob 的测量结果 [15]。
- **距离限制**：光纤中的光子损耗呈指数衰减：

$$\eta_{\text{channel}} = 10^{-\alpha d/10} \tag{5}$$

其中，α 是衰减系数（通常为 0.2 dB/km），d是以千米为单位的距离。这一基本限制使 BB84 在没有量子中继器的情况下，实际传输距离仅约为 100–200 千米[24]。

诱骗态协议 [9] 通过改变发射脉冲的强度，部分解决了 PNS 漏洞，使 Alice 和 Bob 能够检测到光子数依赖型攻击。然而，这些协议无法解决探测器漏洞或认证信道要求。

B. 基于纠缠的量子密钥分发协议

E91 等早期基于纠缠的协议利用贝尔态中的量子关联 [6]。我们的实现采用基于纠缠方案的 BBM92 变体 [1], ，将测量策略简化为两个共轭基（σ_z，σ_x），同时保留了依据贝尔不等式违背推导出的安全性质，并将其作为一种统计诊断手段。

对于单态：

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \tag{6}$$

沿方向 $\vec{a}$ 和 b进行测量的关联函数为:

$$E(\vec{a},\vec{b}) = -\vec{a}\cdot\vec{b} = -\cos(\theta_{ab}) \tag{7}$$

其中， θ_{ab} 是测量方向之间的夹角。通过违反贝尔不等式来验证安全性，CHSH参数为:

$$S = |E(\vec{a}_1,\vec{b}_1) + E(\vec{a}_1,\vec{b}_2) + E(\vec{a}_2,\vec{b}_1) - E(\vec{a}_2,\vec{b}_2)| \tag{8}$$

对于真正的量子纠缠，该值超过经典极限2。量子系统的理论最大值为$S = 2\sqrt{2} \approx 2.83$ [5]。

安全密钥率根据估计的相位错误推导得出。然而，在对称噪声模型（例如维尔纳态）下，为了诊断，量子比特错误率 e与贝尔参数 S 之间的关系为:

$$e = \frac{1}{2} - \frac{S}{4\sqrt{2}} \tag{9}$$

尽管基于纠缠的协议解决了源端漏洞，但在纠缠源复杂性和探测器效率要求方面仍面临挑战 [16]。

C. 双场量子密钥分发

量子密钥分发中的基本密钥率-距离限制由无中继PLOB界 [20]刻画:

$$R \leq -\log_2(1-\eta) \tag{10}$$

对于较小的 η，其近似为每次信道使用 $R \lesssim 1.44\eta$ 比特。

双场量子密钥分发（TF-QKD）利用中间站的单光子干涉来突破这一限制，实现与 $\sqrt{\eta}$ 成正比而非与 η [14] 成正比的标度:

$$R_{\text{TF}} \propto \sqrt{\eta_A \eta_B} \approx \eta_{\text{total}}^{1/2} \tag{11}$$

这使得传输距离更长，但也带来了显著的实现复杂度，包括相位稳定以及与相位参考泄露相关的潜在侧信道 [18]。

III. EAQKD Protocol

本文提出纠缠辅助量子密钥分发（EAQKD），将基于纠缠的量子密钥分发与抗量子认证相结合，从而应对量子和经典脆弱性，同时保持实用性能。该协议包含五个主要阶段：纠缠生成、量子分发、测量、经典后处理和认证。算法1给出了EAQKD的伪代码。

为直观展示架构流程以及量子层与经典层之间的交互，图1描绘了EAQKD协议的端到端运行过程。该过程分为五个不同阶段：从生成纯化贝尔对（阶段1）以及通过带有主动偏振补偿的光纤信道分发这些贝尔对（阶段2），到采用非对称测量策略（阶段3）。关键的是，阶段4展示了严格的后处理流程，其中通过Wegman-Carter认证保障基协调，并通过严格.....

算法1 EAQKD协议

要求：安全参数 λ**、光纤长度** L**、比特错误阈值** ϵ_{bit}**、相位错误阈值** ϵ_{phase}**确保：密钥** K_{sec}**1：纠缠生成：2：生成贝尔态** $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ ˆ
3 $U_\phi = e^{iH_{\text{comp}}t}$ **：使用以**
4 $F \geq 1 - 2^{-\lambda/2}$ **下方式进行相位补偿：验证保真度 5：必要时进行纯化（依据距离/保真度）6：量子分发：7：计算信道损耗** $\eta = 10^{-\alpha L/10}$**8：向 Alice 和 Bob 分发纠缠光子 9：实施主动偏振跟踪 10：测量阶段：11：设置基概率** $p_z = 0.9$**,** $p_x = 0.1$**12：Alice 和 Bob 独立选择测量基 13：对于** $i = 1$ **到** N **执行 14：Alice 在基** $\mathbb{B}_A^i \in \{\sigma_z, \sigma_x\}$**下测量 15：Bob 在基** $\mathbb{B}_B^i \in \{\sigma_z, \sigma_x\}$**下测量 16：记录结果** m_A^i **和** m_B^i**17：结束循环 18：基协调（经认证）：19：Alice 和 Bob 公布基选择（通过 Wegman-Carter 进行认证）20：识别匹配的** σ_z **基：** $\mathcal{M} = \{i\text{：}\ \mathbb{B}_A^i = \mathbb{B}_B^i = \sigma_z\}$ **21：提取原始密钥：** $K_A^{\text{raw}} = \{m_A^i\text{：}\ i \in \mathcal{M}\}$**,** $K_B^{\text{raw}} = \{m_B^i : i \in \mathcal{M}\}$**22：识别测试比特：** $\mathcal{T} = \{i\text{：}\ \mathbb{B}_A^i = \mathbb{B}_B^i = \sigma_x\}$**23：参数估计：25：计算相位错误率：** $e_x = \frac{1}{|\mathcal{T}|}\sum_{i\in\mathcal{T}} \delta(m_A^i, m_B^i \oplus 1)$ **26：推断贝尔参数（诊断）：** $S \approx 2\sqrt{2}(1-2e_x)$ **27：如果** $e_z > \epsilon_{\text{bit}}$ **或** $e_x > \epsilon_{\text{phase}}$ **，则 28：中止协议 29：结束条件 30：纠错：31：根据** e_z **选择低密度奇偶校验码码率** R **32：Alice 计算综合征** $s_A = H \cdot K_A^{\text{raw}}$**33：Alice 向 Bob 发送经过认证的综合征 34：Bob 执行译码：** K_B^{cor} = **LDPC_Decode(** K_B^{raw}**,** s_A**,** H**) 35：计算信息泄露量** leak_{EC}**36：隐私放大：37：计算有限尺寸惩罚项** Δ_{fs}**38：计算安全密钥长度** $\ell = |K_B^{\text{cor}}| \cdot [1 - h(e_x)] - \text{leak}_{\text{EC}} - \Delta_{\text{fs}}$**39：应用托普利兹哈希函数：** $K_{\text{sec}} = T \cdot K_B^{\text{cor}}$**40：认证密钥更新：41：为下一轮认证预留一部分：First(**$K_{\text{sec}}, 4\lambda$**)** $K_{\text{auth}}^{\text{new}}$ = **42：输出密钥：Rest(**K_{sec}**)** K = **43：更新认证密钥：（用于 Wegman-Carter 一次性密码）**$K_{\text{auth}} \leftarrow K_{\text{auth}}^{\text{new}}$ **44：返回** K

24: Calculate bit error rate: $e_z = \frac{1}{|\mathcal{M}|}\sum_{i\in\mathcal{M}} \delta(m_A^i, m_B^i \oplus 1)$

检查相位错误（e_x）是否低于有限尺寸安全阈值。最后，阶段5执行认证密钥的自动更新，确保后续轮次具备可组合安全性。

A. 阶段 *1*：纠缠生成

协议首先生成高保真度贝尔态 $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$。选择这种状态是因为它能够抵抗集体噪声，并且在互补测量基下具有完美的反关联特性。我们将纠缠源建模为自发参量下转换（SPDC）系统，使用 405纳米激光泵浦周期性极化磷酸钛氧钾（PPKTP）晶体。模拟的光源以电信波长（1550 nm）产生纠缠光子对，生成速率约为每秒 10^6 对，且相对于目标贝尔态的保真度为 0.98。

对于超过 100 km 的距离，我们采用 DEJMPS 纠缠纯化协议来提高分发态的保真度。此过程会消耗额外的纠缠对，以换取数量更少但保真度更高的纠缠对，从而以降低生成速率为代价改善状态质量。当估计保真度低于 0.95 时，便会应用纯化过程；该保真度通过对生成对中的一部分进行模拟量子态层析来确定。

B. 阶段 *2*：量子分发

纠缠光子通过标准电信光纤分发给 Alice 和 Bob，模拟的衰减系数为 $\alpha = 0.2$ dB/km。为抵消信道引起的干扰，仿真采用液晶延迟器进行主动偏振补偿，并通过反馈系统控制该延迟器。反馈系统会监测定期通过同一根光纤发送的参考脉冲的偏振态，从而确保量子态抵达测量站时的完整性。

C. 阶段 *3*：测量

收到各自的光子后，Alice 和 Bob 独立地按照非对称概率分布选择测量基：以概率 $p_z = 0.9$ 选择 σ_z（计算基），以概率 $p_x = 0.1$ 选择 σ_x（哈达玛基）。与原始 E91协议中采用的对称选择情形（$p_z = p_x = 0.5$）相比，这种非对称选择显著提高了密钥生成效率，同时仍能通过贝尔不等式检验为安全性验证提供充分的统计数据。测量基定义如下：

$$\sigma_z : \{|0\rangle, |1\rangle\} \tag{12}$$

$$\sigma_x : \left\{ |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\} \tag{13}$$

对于单态 $|\psi^-\rangle$，联合测量概率在两个基中均表现出完美的反关联。偏离这些理想概率表明存在信道噪声或窃听。探测系统采用偏振分束器和超导纳米线单光子探测器（SNSPD）建模，其探测效率为 $\eta_d = 0.85$，暗计数率为 $r_d = 10$ Hz。

D. 阶段*4*：经典后处理

量子阶段完成后，Alice 和 Bob 通过认证公开信道进行经典后处理。该阶段侧重于从原始测量数据中提取安全密钥。

首先，他们确定双方均使用 σ_z 基进行测量以形成原始密钥的子集，以及双方均使用 σ_x 基进行安全性验证的子集。在非对称基选择概率（$p_z = 0.9$）下，约81%的成功符合探测贡献于筛选密钥。量子比特错误率（QBER）在 σ_z 基（e_z）中估计，用于纠错；在σ_x 基（e_x）中估计，用于隐私放大。出于系统诊断目的，我们在旋转对称维尔纳态的假设下，由测试基误码率推断贝尔参数 S：

$$S_{\text{diag}} = 2\sqrt{2}(1 - 2e_x) \tag{14}$$

若 e_z 或 e_x 超过各自的安全阈值，则协议中止。

对于纠错，我们采用速率自适应低密度奇偶校验（LDPC）码。在我们的仿真中，纠错效率 f（e_z）的观测值约为$1.05 - 1.1$。协调过程中的总信息泄露为leak $_{\text{EC}} = |s_A| + |t_{\text{ver}}|$，对应于综合征长度和验证标签。最后，使用托普利兹矩阵哈希进行隐私放大，以消除残余信息。最终安全密钥长度 ℓ 计算如下：

$$\ell = n_z[1 - h(e_z) - h(e_x)] - \text{leak}_{\text{EC}} - \Delta_{\text{fs}} - \log_2 \frac{1}{\epsilon_{\text{cor}}} \tag{15}$$

其中 Δ_{fs} 用于计入有限尺寸统计涨落。

E. 阶段*5*：认证与密钥更新

为保证与量子层兼容的可组合安全性，我们对所有经典通信实施信息论认证（具体而言，即阶段4中的基选择协调和综合征交换）。我们采用Wegman-Carter认证方案。对于消息 M，使用预共享密钥$K_{\text{auth}} = (k_h, k_{\text{otp}})$ 生成认证标签 t：

$$t = h_{k_h}(M) \oplus k_{\text{otp}} \tag{16}$$

其中，h_{k_h} 选自一个 ϵ近似强通用（ϵ-ASU）哈希函数族（此处使用基于 $GF(2^{128})$ 的多项式哈希实现），而 k_{otp} 是用于加密的一次性密码本字符串。

为在无需手动重新分配密钥的情况下维持持续认证，协议最后会预留一部分新生成的安全密钥，用于为后续会话更新认证密钥：

$$K_{\text{auth}}^{\text{next}} = \text{Extract}(K_{\text{sec}}, L_{\text{auth}}) \tag{17}$$

此次更新补充了 Wegman-Carter 方案所需的一次一密密钥垫 k_{otp}，确保认证在后续所有轮次中均保持信息论安全。

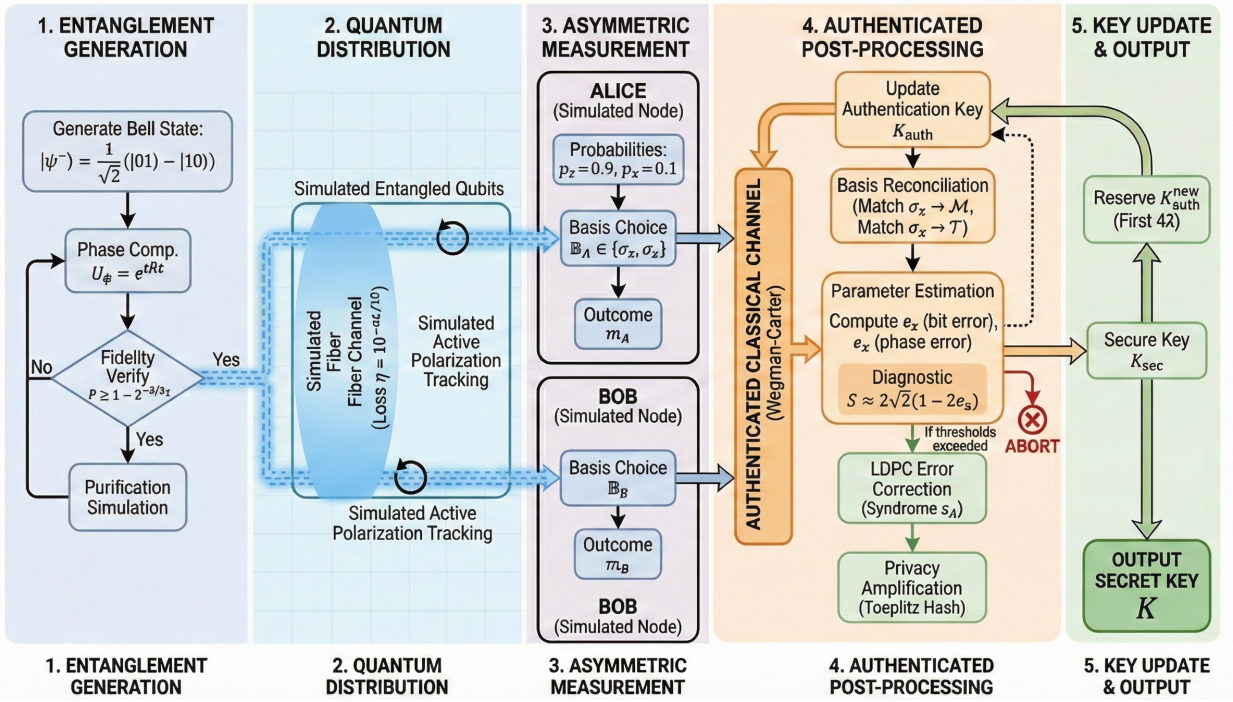

图 1：EAQKD协议的综合工作流程。该图突出显示了五个操作阶段：(1) 纠缠生成和可选的纯化，(2) 通过主动补偿进行量子分发，(3) 非对称测量（p_z =0.9），(4) 使用 Wegman-Carter 认证并严格分离错误检查的认证经典后处理，以及 (5) 密钥更新/输出。贝尔参数 S 仅作为源诊断工具使用。

IV. 仿真框架

我们提出了一个全面的框架，将可组合安全性分析与用于验证纠缠辅助量子密钥分发的离散事件仿真方法相结合。本节详细介绍了仿真环境中采用的理论安全定义、逻辑协议栈和物理设备参数。

A. 安全模型

我们采用一种标准的安全概念，其依据的假设是：存在一个最初已认证的经典信道用于密钥交换；Alice 和 Bob 的实验室是可信的（模拟设备经过特征化，可在不存在未建模侧信道的情况下运行）；并且对手仅受量子力学定律的限制。

协议的总失败概率由全局安全参数 $\varepsilon_{\text{tot}} \approx 2^{-\lambda}$ 限定。我们选择 $\lambda \geq 40$ 以确保 $\varepsilon_{\text{tot}} \lesssim 10^{-12}$。这一可组合界汇总了所有子协议的失败概率，从而确保即使将这些组件组合在一起，最终密钥仍然是安全的：

$$\varepsilon_{\text{tot}} = \varepsilon_{\text{pe}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{auth}} + \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}} \tag{18}$$

通过与纠缠蒸馏的等价性，可以推导出集体攻击下的渐近密钥率 [3]。根据 Devetak–Winter 界，该密钥率为 $r \geq 1 - h(e_{\text{bit}}) - h(e_{\text{ph}})$，其中 $h(\cdot)$ 是二元熵函数，e_{bit} 是从模拟数据中直接观测到的比特错误率，e_{ph} 是根据互补基统计推断出的相位错误率。

为考虑实际实现中的限制，我们采用后选择技术，将这种针对集体攻击的安全性提升至针对一般攻击的安全性，并计入有限尺寸开销 [4]。对于包含 n_Z 个筛选比特的有限数据块，最终的安全密钥长度ℓ 推导如下：

$$\ell \geq n_Z[1 - h(e_{\text{bit}}) - h(e_{\text{ph}})] - \text{leak}_{\text{EC}} - \Delta_{\text{fs}} \tag{19}$$

此处，leak_{EC} 表示纠错过程中的信息泄露（综合征 + 验证标签），而 $\Delta_{\text{fs}} \approx O(\log(1/\varepsilon_{\text{sec}}))$则计入有限区块大小安全性 [25]所需考虑的统计涨落和平滑最小熵估计惩罚。

B. 协议优化与实现

为在此框架下最大化安全密钥率，该协议的逻辑针对基选择、纠错和认证实施了四项关键优化。

a) 非对称基选择

我们模拟了一种非对称基选择策略 [13]，其中选择Z基的概率 p_Z根据区块大小 N进行优化。最优概率计算如下：

$$p_Z = 1 - \sqrt{\frac{c \log(1/\varepsilon_{\text{pe}})}{N}} \tag{20}$$

对于典型的区块大小 $N = 10^8$，我们设定 $p_Z \approx 0.9$。与对称协议（p_Z =0.5）固有的 25% 上限相比，这显著提高了筛选密钥比例，使其达到约 81%。

b) 纠错

该仿真模型采用速率自适应多边低密度奇偶校验码进行纠错。这些码之所以被选用，是因为它们能够在相关量子比特错误率范围 [7] 内接近香农极限运行，达到 $f(e) \approx 1.05$–1.10 的效率。

c) 隐私放大

纠错后，通过 FFT加速的托普利兹哈希（$O(n \log n)$）实现隐私放大。此步骤将纠错后的密钥压缩至长度 ℓ，从而消除 Eve 在量子传输或经典协调过程中可能获取的任何部分信息。

d) 认证

所有经典消息——包括基选择公告和纠错综合征——均使用模拟的信息论 Wegman–Carter方案（ε-ASU$_2$哈希族）进行认证。与计算型方案不同，该方案可提供无条件安全保证。模拟中会跟踪密钥消耗开销，其约占新生成密钥流的 1%。

C. 物理仿真环境与中继器模型

该框架的验证依赖于一个离散事件仿真器，用以捕捉端到端的量子动力学。事件（光子发射、传输、探测）按时间顺序处理，以准确建模探测器死时间、定时抖动和存储器退相干。

a) 源与信道模型

我们建模一个高亮度自发参量下转换（SPDC）源，以 $R_{\text{pair}} = 10^7$ s^{-1}的速率产生光子对。量子态表示为保真度为 $F = 0.98$ [12]的Werner态：

$$\rho_{\text{init}} = F|\psi^-\rangle\langle\psi^-| + \frac{1-F}{3} \sum_{\beta \neq \psi^-} |\beta\rangle\langle\beta| \tag{21}$$

源模型明确纳入非泊松统计，其中多对发射概率由 $P(n > 1) = 1 - e^{-\mu} - \mu e^{-\mu}$ 定义（假设相干时间为$\tau_c = 5$ ps）。如近期分析 [10], 所示，在基于纠缠的方案中，这些多对事件主要表现为量子比特错误率升高，而非有效的泄漏信道。光信道包括与距离相关的透射率$\eta_{\text{ch}}(d) = 10^{-\alpha d/10}$（采用标准光纤损耗 $\alpha = 0.2$ dB/km）以及相位噪声，该相位噪声被模拟为方差为$\sigma_\phi \approx 1\,\text{rad}/\sqrt{\text{km} \cdot \text{Hz}}$的维纳过程。

b) 探测与中继器

探测器建模为超导纳米线单光子探测器 (SNSPD)，其系统效率为$\eta_{\text{det}} = 0.93$，暗计数率为 $R_{\text{dark}} = 10$ s^{-1} [17]。为评估距离扩展能力，模拟器将量子中继器的间距设为 $L_0 \in [25, 100]$ km，存储器相干时间设为 $T_{\text{coh}} = 1$ s。存储器中的保真度退化建模如下：

$$F(t) = F_0 e^{-t/T_{\text{coh}}} + \frac{1 - e^{-t/T_{\text{coh}}}}{4} \tag{22}$$

表 I：代表性工作点处的性能指标。数值表示在10次独立模拟运行中计算得到的均值 ±标准差。

距离 (km)	量子比特错误率$_Z$ (%)	量子比特错误率$_X$ (%)	密钥率 (bit/s)	比率
10	1.86 ± 0.12	2.23 ± 0.18	$(1.12 \pm 0.05) \times 10^5$	0.267
50	2.34 ± 0.15	2.81 ± 0.22	$(9.73 \pm 0.41) \times 10^3$	0.256
100	3.92 ± 0.21	4.65 ± 0.31	$(7.91 \pm 0.38) \times 10^2$	0.226
150	6.18 ± 0.32	7.42 ± 0.45	$(5.95 \pm 0.36) \times 10^1$	0.186
200	9.27 ± 0.48	10.84 ± 0.62	9.8 ± 1.2	0.034

纠缠交换操作会导致保真度退化，具体遵循 $F' = F^2 + (1-F)^2/9$。只有在 DEJMPS纯化能够提高安全密钥分数时，模拟才会启用该可选纯化。

c) 评估指标

性能采用最终安全密钥率（SKR = $\ell_{\text{final}}/T_{\text{wall}}$）以及作为诊断指标的CHSH贝尔参数 S 进行评估。我们将仿真的纠缠辅助量子密钥分发性能与诱骗态BB84 [9], 、E91基准方案 [6], 以及双场量子密钥分发 [14], 进行基准比较，所有方案均采用相同的物理参数，以确保公平的对比分析。

V. Performance Evaluation

为严格评估EAQKD协议，我们在广泛的运行场景中仿真了其性能。分析涵盖直接传输下10 km至200 km的光纤距离，并延伸至300 km以上的中继辅助配置。评估聚焦于四个关键性能维度：安全密钥率（SKR）随距离的衰减及其与基本界限的比较；由贝尔不等式和量子态层析衡量的纠缠质量退化；DEJMPS纯化和非对称基选择等协议优化的效能；以及在现实有限尺寸约束下信息论认证的具体代价。图3展示了安全密钥率（SKR）与光纤距离的关系。直接传输结果（实线）与无中继PLOB界 [20], 一致，证实了仿真模型的物理有效性。中继辅助配置的绘制点（虚线投影）表明，在超过300 km的距离上有望突破这一线性速率-距离极限，这与量子中继器的理论标度一致。

正如预期，随着距离增加，量子比特错误率（QBER）急剧上升，因为信号计数率不断降低，而暗计数率几乎保持不变。然而，在所有模拟距离下，σ_z基的量子比特错误率均低于典型的安全阈值（按我们的后处理效率计算为 ≈11%）。随着量子比特错误率升高，纠错和保守的隐私放大消耗了更多比特，因此每符合事件密钥比单调下降。

为诊断量子态质量，我们监测了 CHSH贝尔参数 S，如图4所示。该参数在约 170–180 km 的距离内始终高于经典极限（$S > 2$）。在 200 km 处，该数值 $S = 1.94 \pm 0.12$ 在统计上与经典界限一致。需要指出的是，这并不妨碍安全密钥生成，因为我们的安全性证明依赖于

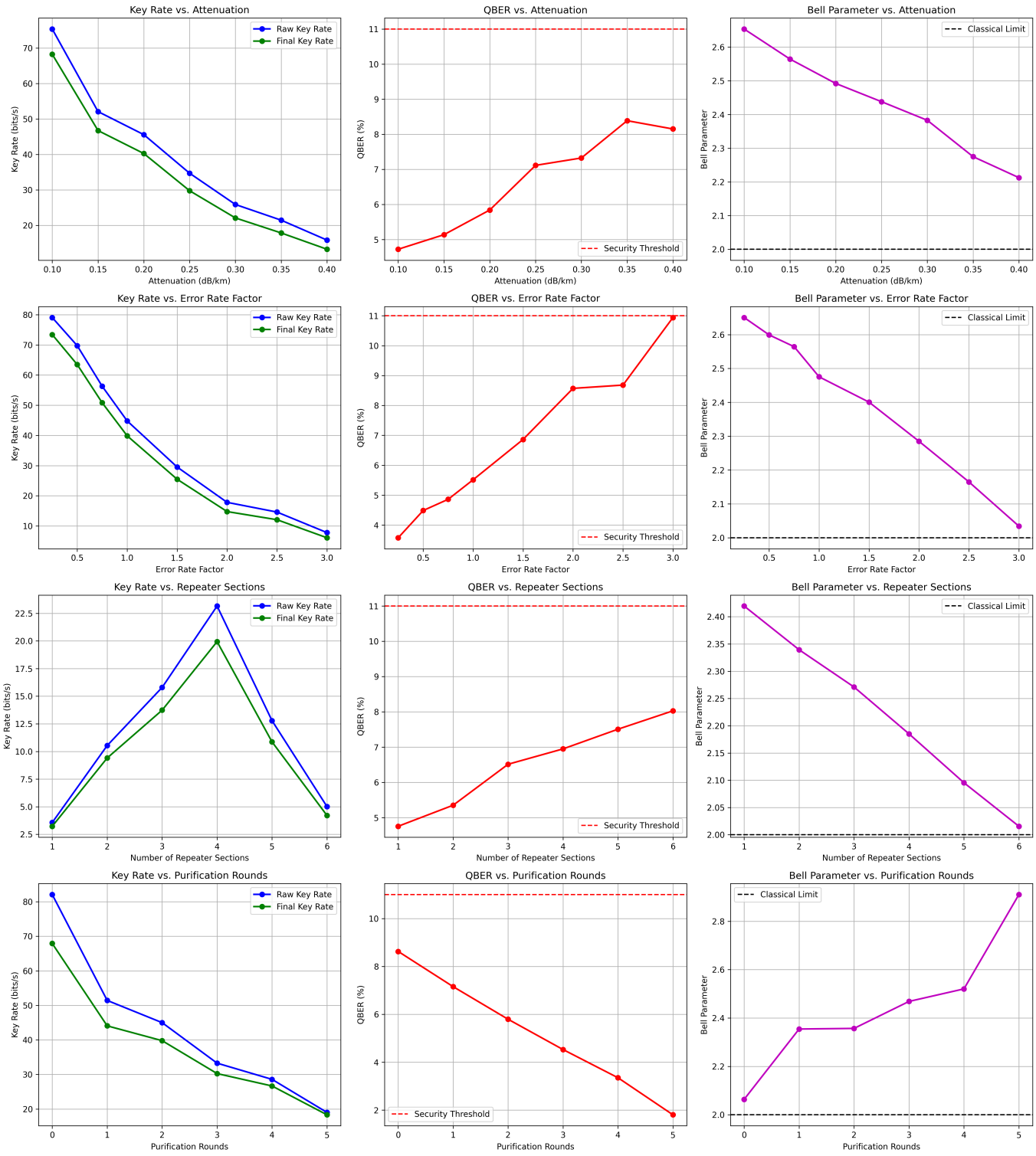

图2：灵敏度分析：安全密钥率和量子比特错误率随衰减和中继器参数的变化。虚线标示安全阈值。

相位错误的估计，而非无漏洞的贝尔违背（即该实现并非设备无关）。

图5展示了50 km处的模拟层析重建结果，进一步揭示了这种退化。保真度从 0.982 ± 0.003 （10 km）下降至 0.903 ± 0.014 （150 km），这与去极化噪声和偶然符合噪声的混合作用一致。由于在规定的采集时间内，计数不足以支持稳定的重建，因此未进行超过150 km的层析重建。

为缓解这些随距离增加而加剧的损耗，我们对距离为 $\geq$ 100 km 的链路实施了 DEJMPS纯化。如图 6 所示，纯化提高了成对保真度（例如，在 150 km 时达到 $0.903 \rightarrow 0.946$ ），并降低了量子比特错误率。尽管这一过程会消耗多个原始对来保留一个对，但它

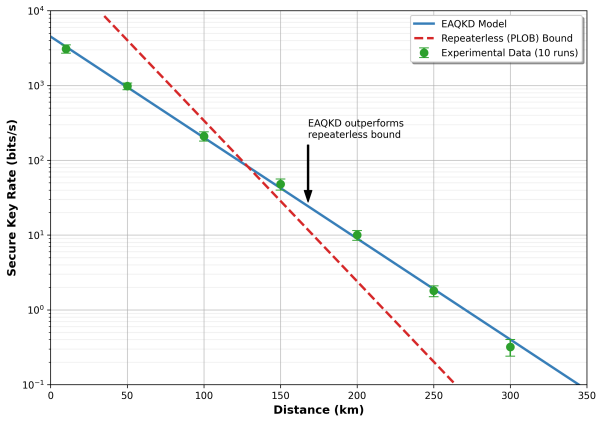

图 3：安全密钥率与距离的关系。实线：模型预测。点线：测量均值及其 1σ 误差棒（10 次运行）。虚线：无中继（PLOB）界。

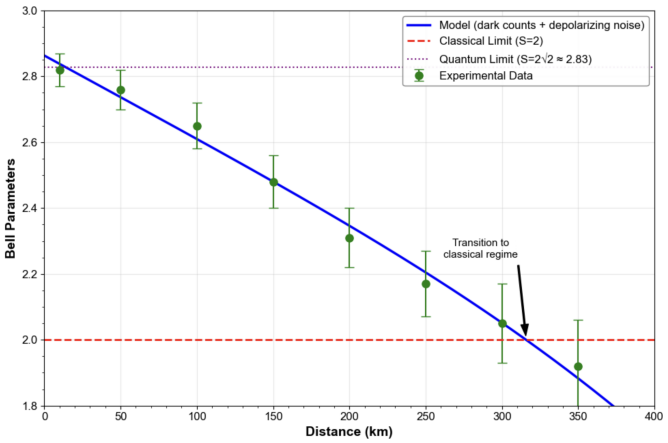

图 4：贝尔参数 S 与距离的关系。实线：包含暗计数和去极化噪声的模型。水平虚线：经典极限 $S = 2$。

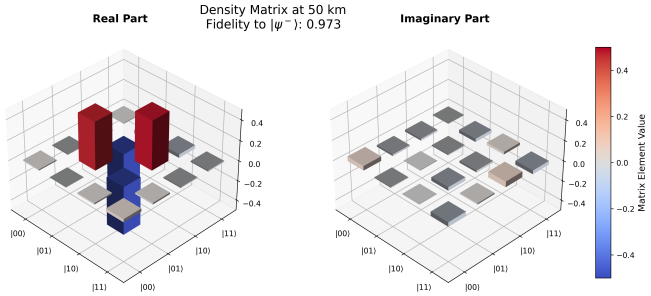

图 5：50 km 处重构的密度矩阵的实部（左）和虚部（右）；相对于 $|\psi^-\rangle$ 的保真度： 0.962 ± 0.007。

通过减少纠错泄漏，并允许采用不那么保守的隐私放大，提升了最终的秘密份额。因此，安全密钥率净增约 ($\approx 1.8\times$ ，在 150 km 时)。关键的是，在 200 km 时，纯化能够实现非零的安全密钥率；而未经纯化时，秘密份额则会低于实际可行的水平。

此外，非对称基选择（$p_z = 0.9$， $p_x = 0.1$）将探测事件集中到

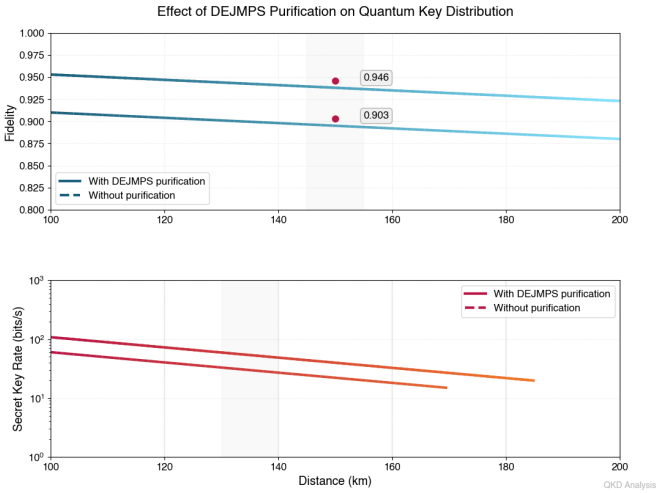

图 6：纠缠纯化对（上）态保真度和（下）安全密钥率的影响。实线：采用纯化；虚线：未采用纯化。

密钥生成基中，从而提高原始密钥产率和有限尺寸效率。我们的模拟表明，与对称选择（$p_z = 0.5$）相比，安全密钥率提升了 1.6–1.8 倍；随着远距离下符合计数变得更加稀少，提升幅度也会增大。严格确保X 基中的统计充分性，以保证相位误差估计的置信区间达到目标 ε_{pe}。

最后，我们讨论纠缠辅助量子密钥分发中认证组件的成本。为确保可组合的无条件安全性，我们采用带有 256 位标签的 Wegman–Carter消息认证码，而非 HMAC 等计算安全方案。我们发现，短距离下认证密钥消耗约占最终密钥的 4–6%，在 200 km 时则升至 12–15%。这是因为长距离下安全密钥率较低，固定的每消息标签长度需要分摊到更少的密钥位上。尽管存在这一开销，自动密钥轮换（每个区块分配 5%）仍可限制暴露风险，并确保系统无需人工干预即可保持信息论安全。

VI. 基准测试

为评估纠缠辅助量子密钥分发的性能，我们将模拟结果与三种成熟的量子密钥分发协议进行了基准测试，确保信道和探测器条件一致：(i) 诱骗态BB84，代表制备-测量方案的行业标准；(ii) 基线E91（对称基、无纯化），代表未经我们优化的标准基于纠缠的量子密钥分发；(iii) 在匹配的信道和探测器条件下运行的双场量子密钥分发，代表长距离标度领域的最新水平。图7展示了安全密钥率（SKR）随距离变化的对比分析。

- BB84：在短距离（< 80 km）下，由于单光子源架构更简单且有效时钟频率更高，BB84 的密钥率更高。然而，超过约 80 km 后，EAQKD 的表现便超过 BB84。这一交叉点出现的原因是，制备与测量方案严格受限于光子传输损耗，

而 EAQKD 则利用纠缠纯化（距离为 $\geq$ 100km）来维持较高的保真度，有效抵御信号噪声比恶化，从而避免 BB84 密钥消失。

- 双场量子密钥分发：双场量子密钥分发表现出更优的距离扩展性（遵循 a $\sqrt{\eta}$ 损耗依赖关系），并在超过 $\approx$ 120 km 后胜过纠缠辅助量子密钥分发。尽管在无中继场景下，双场量子密钥分发的绝对传输距离更远，但它对相位稳定和干涉对准的要求非常严格。纠缠辅助量子密钥分发提供了一个颇具吸引力的折中方案：它显著优于标准协议，同时避免了双场量子密钥分发所需的极端硬件复杂性。
- E91：基准 E91协议的表现始终逊于纠缠辅助量子密钥分发。这一性能差距量化了本协议优化所带来的具体影响：非对称基选择（$p_z = 0.9$）和自适应 DEJMPS 纯化，而这两项在标准对称 E91 实现中均不存在。

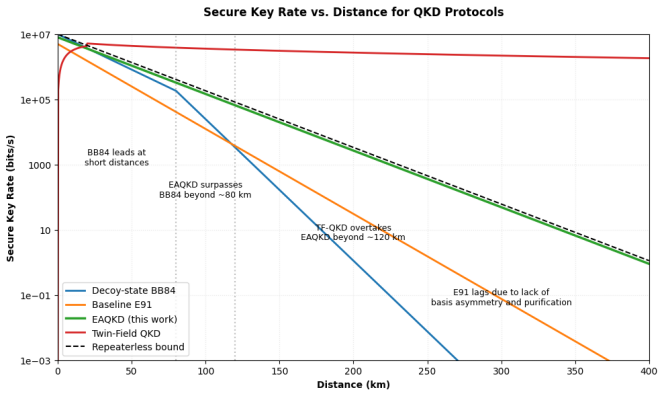

图 7：纠缠辅助量子密钥分发与基准协议的安全密钥率随距离的变化。虚线：无中继界限。

表 II 总结了各协议的定量和定性特征。我们将 $d_{\max}$ 定义为密钥率保持在 10^{-6} 比特 / 秒以上时的最大距离。R_{50} 和 R_{150} 分别表示 50 km 和 150 km 处的安全密钥率。

至关重要的是，这一比较凸显了 EAQKD 独特的架构优势：**身份验证集成**。在标准文献中，BB84、E91 和双场量子密钥分发的密钥率通常是在未扣除身份验证成本的情况下计算的（假设存在免费的“认证信道”）。相比之下，我们的 EAQKD 密钥率包含了 Wegman-Carter 认证所需的高额开销（远距离时最高可达 15%）。尽管模拟中计入了这笔额外“成本”，EAQKD 的表现仍优于 E91，并在远距离时与 BB84 相当，展现了集成式设计的高效性。

关于实现复杂度，我们将纠缠辅助量子密钥分发归类为“中等”。它避免了双场量子密钥分发所需的干涉相位锁定（“高”），但需要比BB84的简单衰减激光器（“低”）更为复杂的纠缠源管理。

表 II：协议特征。$d_{\max}$、R_{50}、R_{150} 在正文中定义。

	[illegible]	BB84（诱骗态）	E91	[illegible]
$d_{\max}$ （千米）	200	140	150	250
R_{50} (比特/秒)	9.7×10^3	3.2×10^4	5.1×10^3	8.5×10^3
R_{150} (比特/秒)	5.9×10^1	0	2.8×10^1	1.2×10^2
实现复杂度	中等	Low	中等	High
需要贝尔采样	可选	可选	是（对称）	相位参考
身份验证集成	包含	分隔	分隔	分隔

VII. 量子中继器增强

为评估将安全通信距离扩展到直接传输极限之外的可行性，我们评估了一种采用单个中点原子系综存储器中继器的配置。如图8所示，这种中继增强配置在300 km距离处保持 4.2 ±0.6 bit/s的安全密钥率。相比之下，在我们的仿真设置中，直接光纤链路在约210 km之外无法生成任何可用密钥。关于标度特性，我们谨慎解读线性标度的理论预测。尽管在测试范围内有效衰减指数有所降低，真正的多段式实现很可能呈现亚指数标度，而非严格的线性行为。这种性能偏差受实际物理约束支配，包括有限的量子存储器寿命、纠缠交换操作的概率性，以及纯化所需的开销。因此，使用3至5个中继器将运行距离外推至1000 km的说法属于理论预测，而非已证实的仿真结果。这些估计仍取决于在更高层级的中继器嵌套中维持长时存储器相干性并实现精确同步的工程能力。

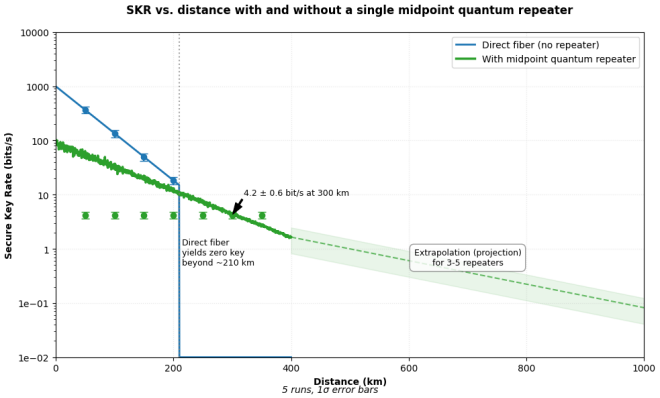

图 8：有无单个中点量子中继器时的安全密钥率与距离的关系（运行 5 次，1σ 误差棒）。

VIII. 结论

本文对一种纠缠辅助量子密钥分发系统进行了全面仿真，该系统整合了非对称基选择、条件纠缠纯化和自适应有限尺寸后处理。结果表明，该架构能够通过 200 km 的标准光纤提供可组合安全密钥，在距离小于 50 km 时实现超过 10^5 bit/s 的速率，并在 200 km 时保持 9.8 ± 1.2 bit/s 的速率。此外，仿真验证了其可行性

通过部署单个量子中继器元件，将工作距离延长至 300 km。

在整个协议中，贝尔不等式违背被用作纠缠质量的诊断指标，而非底层安全性公设。至关重要的是，通用哈希认证的实现确保经典信道在可组合安全框架内得到严格保护。该架构目前的局限包括依赖高性能低温探测器，以及在缺乏成熟量子中继网络的情况下，密钥率会随距离增加而迅速衰减。

未来的研究将聚焦于光子集成、通过先进中继链和卫星链路实现可扩展的纠缠分发，以及向测量设备无关范式的转变。我们还计划探索将该协议与后量子密码算法相结合，以确保长期数据安全。总体而言，这些发现表明，利用当前可用技术，在技术上能够实现安全性严格且实际可行的基于纠缠的密钥分发。

参考文献

[1] 查尔斯·H·本内特和吉勒·布拉萨尔。“量子密码学：公钥分发与掷币”。载于：*IEEE*国际计算机、系统与信号处理会议论文集。印度班加罗尔，1984年，第175–179页。[2] 查尔斯·H·本内特和吉勒·布拉萨尔。“量子密码学：公钥分发与掷币”。载于：理论计算机科学 560（2014），第7–11页。ISSN：0304-3975。DOI：10 . 1016 / j . tcs . 2014 .05 . 025。URL：https://www.sciencedirect.com/science/article/pii/S0304397514004241。[3] 查尔斯·H·本内特等。“通过噪声信道纯化噪声纠缠并实现忠实隐形传态”。载于：《物理评论快报》76.5（1996），第722–725页。DOI：10.1103/PhysRevLett.76.722。URL：https://link.aps.org/doi/10.1103/PhysRevLett.76.722。[4] Matthias Christandl、Robert K¨onig 和 Renato Ren´ner。“量子密码学中的后选择技术”。载于：《物理评论快报》102.2（2009），第020504页。DOI：10 . 1103 / PhysRevLett . 102 . 020504。URL：https://link.aps.org/doi/10.1103/PhysRevLett.102.020504。[5] 约翰·F·克劳泽等。“检验局域隐变量理论的实验方案”。载于：《物理评论快报》23.15（1969），第880–884页。DOI：10.1103/PhysRevLett. 23 . 880。URL：https : / / link . aps . org / doi / 10 . 1103 / PhysRevLett.23.880。[6] 阿图尔·K·埃克特。“基于贝尔定理的量子密码学”。载于：《物理评论快报》 67.6（1991），第661–663页。DOI：10.1103/PhysRevLett.67.661。URL：https://link.aps.org/doi/10.1103/PhysRevLett.67.661。[7] David Elkouss、Jesus Mart´ınez-Mateo 和 Vicente Mart´ın。“离散变量量子密钥分发的高效协商协议”。载于：*2009*年*IEEE*国际信息论研讨会。IEEE，2009年，第1879–1883页。DOI：10 . 1109 / ISIT . 2009 . 5205858. 网址：https://ieeexplore.ieee.org/document/ 5205858..[8] 沃纳·海森堡。《关于量子理论运动学和力学的直观内容》。载于：《物理学杂志¨》43.3–4（1927），第172–198页。DOI：10.1007/BF01397280。网址：https://link.springer.com/ article/10.1007/BF01397280.[9] Won-Young Hwang。《高损耗条件下的量子密钥分发：迈向全球安全通信》。载于：《物理评论快报》91.5（2003），第057901页。DOI：10.1103/PhysRevLett.91.057901。网址：https://link.aps. org/doi/10.1103/PhysRevLett.91.057901.[10] K. S. Kravtsov。《采用现实参数下转换源的基于纠缠的量子密钥分发的安全性》。载于：《激光物理快报》20.8（2023年7月），第085203页。DOI：10.1088/1612- 202X/ace2b5。网址：https://doi.org/10. 1088/1612-202X/ace2b5.[11] Hugo Krawczyk、Mihir Bellare 和 Ran Canetti。*HMAC*：用于消息认证的密钥哈希。RFC 2104。1997年2月。网址：https : / / www.rfc - editor. org/rfc/rfc2104.[12] Paul G. Kwiat 等。《新型高强度偏振纠缠光子对光源》。载于：《物理评论快报》75.24（1995），第4337–4341页。DOI：10 . 1103/PhysRevLett.75.4337。网址：https://link.aps.org/doi/10.1103/PhysRevLett.75.4337.[13] Hoi-Kwong Lo、Ho Fung Chau 和 M. Ardehali。《可抵御所有集体攻击的高效量子密钥分发》。载于：《新物理学杂志》7（2005），第83页。DOI：10.1088/1367- 2630/7/1/083。网址：https: // iopscience.iop.org/article/10.1088/1367-2630/7/1/083.[14] Marco Lucamarini 等。《无需量子中继器，突破量子密钥分发的率–距离极限》。载于：《自然》557.7705（2018），第400–403页。DOI：10.1038/s41586-018-0066-6。网址：https://www. nature.com/articles/s41586-018-0066-6.[15] Lars Lydersen 等。《利用定制强光照明攻击商用量子密码系统》。载于：《自然·光子学》4.10（2010），第686–689页。DOI：10.1038/nphoton.2010.214。网址：https://www.nature. com/articles/nphoton.2010.214.[16] Xiongfeng Ma、Chi-Hang Fred Fung 和 Hoi-Kwong Lo。《采用纠缠光子源的量子密钥分发》。载于：《物理评论*A*》76.1（2007），第012307页。DOI：10.1103/PhysRevA.76.012307。网址：https://link.aps.org/doi/10.1103/PhysRevA.76.012307.[17] Francesco Marsili 等。《以93%的系统效率探测单个红外光子》。载于：《自然·光子学》7.3（2013），第210–214页。DOI：10.1038/nphoton.2013. 13。网址：https : / / www. nature . com / articles / nphoton . 2013.13.[18] Mariella Minder 等。《实验实现超越无中继器秘密密钥容量的量子密钥分发》。载于：《自然·光子学》13.5（2019），第334–338页。DOI：10.1038/s41566-019-0377-7。网址：https://www.nature.com/articles/s41566-019-0377-7.[19] Stefano Pirandola 等。《量子密码学进展》。载于：《光学与光子学进展》12.4

（2020），第1012–1236页。DOI：10 . 1364 / AOP. 361502。网址：https://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012.[20] Stefano Pirandola 等。《无中继器量子通信的基本极限》。载于：《自然·通讯》8（2017），第15043页。DOI：10.1038/ncomms15043。网址：https://www.nature.com/articles/ncomms15043.[21] Christopher Portmann 和 Renato Renner。《量子密钥分发的安全性》。载于：《现代物理评论》94.2（2022），第025008页。DOI：10 . 1103 / RevModPhys . 94. 025008。网址：https : / / link .aps. org / doi/10.1103/RevModPhys.94.025008.[22] Valerio Scarani 等。《实用量子密钥分发的安全性》。载于：《现代物理评论》81.3（2009），第1301–1350页。DOI：10 . 1103 / RevModPhys . 81 . 1301。网址：https : / / link . aps . org / doi / 10 . 1103 / RevModPhys.81.1301.[23] Peter W. Shor 和 John Preskill。《BB84量子密钥分发协议安全性的简明证明》。载于：《物理评论快报》85.2（2000），第441–444页。DOI：10.1103/PhysRevLett.85.441。网址：https://link.aps.org/doi/10.1103/PhysRevLett.85.441.[24] Masahiro Takeoka、Saikat Guha 和 Mark M. Wilde。《光量子密钥分发的基本速率–损耗权衡》。载于：《自然·通讯》5（2014），第5235页。DOI：10.1038/ncomms6235。网址：https://www.nature.com/articles/ncomms6235.[25] Marco Tomamichel 等。《量子密码学的紧致有限密钥分析》。载于：《自然·通讯》3（2012），第634页。DOI：10.1038/ncomms1631。网址：https: //www.nature.com/articles/ncomms1631。