发布日期 xxxx 00, 0000，当前版本日期 xxxx 00, 0000。数字对象标识符

BB84 协议完成时间分析

SOUNAK KAR[1] 和 JEAN-YVES LE BOUDEC[1]，（IEEE 会士）[1]瑞士洛桑联邦理工学院（电子邮件：firstname.lastname@epfl.ch）

arXiv:2304.10218v1 [cs.PF] 20 Apr 2023

摘要 BB84 量子密钥分发（QKD）协议基于这样一种思想：发送方和接收方可以对一定比例的隐形传态量子比特进行协调，以检测窃听或噪声，并将其余量子比特解码为私钥。在现有硬件基础设施下，量子态的退相干给实现完美或高效的量子隐形传态带来了重大挑战，这意味着基于量子隐形传态的协议必须多次运行才能观察到成功。因此，此类协议的性能分析通常关注完成时间，即直到成功所需的时间，而非单次尝试的持续时间。此外，由于退相干，一次尝试能否成功通常取决于该次尝试各个阶段的持续时间，因为在将生成阶段成功或失败的情况通知相关各方时，量子态必须在存储器中等待。在本研究中，我们分析了这样一种情形下 BB84 协议完成时间的性能：发送方和接收方通过单个量子中继器连接，且二者之间唯一的量子信道未遭受任何对抗性攻击。假设量子隐形传态的生成阶段和通信阶段具有特定的分布形式，我们提出了一种计算完成时间矩母函数（MGF）的方法，并据此推导出累积分布函数（CDF）的估计值以及尾概率的上界。该结果有助于我们根据量子隐形传态各基本阶段的特征参数，评估完成时间的（尾部）行为，而无需多次运行协议。我们还提出了一种高效的仿真方案，通过将完成时间表示为聚合的隐形传态时间来生成完成时间。我们通过数值方法将该方法与全规模仿真进行比较，发现两者吻合良好。

索引词 量子通信，量子密钥分发，仿真。

I. 引言

量子隐形传态使得相隔一定物理距离的节点之间能够传输量子信息。与经典通信不同，现有可用于实现量子隐形传态的硬件效率不高，这意味着必须多次尝试才能成功完成一次量子隐形传态。因此，更有意义的是考虑量子隐形传态的完成时间，即成功所需的时间，而非单次尝试的持续时间。此外，量子隐形传态尝试各阶段的持续时间决定了相关量子比特的退相干程度，进而影响尝试能否成功。这种现象在量子通信中很常见 [1], ，其中尝试会重复进行，且其成功与否通常

取决于每次尝试的具体细节。 [3]–[5] 中的作者在离散时间框架下对这种行为进行了建模，以分析某些量子通信模块的完成时间。

在这项工作中，我们将他们的方法扩展到连续时间框架，并对 BB84 协议的完成时间进行性能分析 [6]。我们的重点在于协议在现实硬件基础设施下的执行，而非其安全性。具体而言，我们假设用户通过一个第一代中继器 [2]，相连，即该中继器不依赖量子纠错，并且他们之间的量子信道未遭受任何攻击。在这种良性环境下，BB84 协议可能因硬件效率低下或量子态退相干而失败，例如，协议的通信阶段就可能出现这种情况。在我们的建模中，局部操作和经典通信（LOCC）阶段均具有正持续时间，以计入这些时间段内退相干的影响。

我们的首要贡献是给出一个矩母函数公式，用于描述相关阶段持续时间不可忽略且为随机值时的完成时间。随后，可以利用该矩母函数求出完成时间累积分布函数 的拉普拉斯变换，再通过反演得到累积分布函数。我们还运用切尔诺夫方法推导出尾概率的时延界。该结果有助于我们了解完成时间随隐形传态基本阶段参数的变化情况，而无需反复运行协议这一繁琐过程。值得注意的是，在其他因素保持不变的情况下，此框架中的完成时间也可作为存在窃听者时完成时间的基准。

我们的第二项贡献是提出一种快速仿真方案，用于生成协议的完成时间。关于有攻击或无攻击情况下 BB84 协议仿真的研究已相当丰富 [8]–[12] ，这些研究侧重于获取密钥率或窃听检测概率。所有这些研究都对协议的各个阶段进行仿真，以实现最终目标。在这项工作中，我们证明，如果只想获取完成时间，就没有必要这样做；我们假设相关阶段的持续时间服从某些分布。在这些假设下，我们首先表明，传送一个量子比特所需的总时间可以用 Coxian 相位型分布很好地近似，而这种分布可以高效聚合，用于仿真 BB84 协议的完成时间。

本文其余部分安排如下：我们将在第 II 节介绍 BB84 协议的系统设置和主要结果，并在第 III 节阐述相关方法与证明。接下来，我们将在第 IV 节介绍仿真方案，并在第 V 节对推导得到的结果进行数值评估。

II. BB84 协议的假设与主要结果

A. 设置与假设

本节首先回顾 BB84 协议 [6]的基本特征。在该协议中，发送方 Alice 使用两种基中的一种对长度为 n 的二进制顺序中的每一位进行编码，其中所选基是均匀随机选取的。选定基后，使用该基中的正交态对 0 和 1 进行编码。例如，Alice 可以使用水平-垂直基中的光子偏振来编码 Bin(n, $1/2$) 位，其中，水平偏振光子（$|0\rangle$）表示 0，垂直偏振光子（$|1\rangle$）表示 1；同时，使用对角偏振基对其余比特进行编码，其中，对角偏振光子（$|+\rangle$）和反对角偏振光子（$|-\rangle$）分别表示 0 和 1。Bob 接收到编码后的量子比特后，会使用两种基中的一种对其进行测量，所选基同样是均匀随机选取的。随后，Alice 和 Bob 公布各自对每一位所使用的基，并保留双方所用基一致的那些比特，这种情况发生的比特数为 Bin($n, 1/2$)。从这些比特中随机抽取一个样本，如果样本中有一定比例的比特相匹配，则认为协议成功。剩余比特随后用作密钥。为了分析该协议，我们进一步作出以下假设：

A1 **单信道：** Alice 和 Bob 通过单个量子信道相连，这意味着

量子比特是按顺序传送的。A2 **单个中继器：** Alice 和 Bob 的距离恰好足以通过单个量子中继器相连。A3 **无窃听：** 在包含密钥数据的量子比特传送期间，信道上没有发生窃听。

A4链路建模：根据 [4], ，我们将节点与中继器之间的基本链路建模为 Werner 状态 [13]。具有 Werner 参数 w 的 Werner 状态表示为：

$$\frac{1+3w}{4}|\Phi^+\rangle\langle\Phi^+| + \frac{1-w}{4}\Big(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\Big),$$

其中 $|\Phi^+\rangle$，$|\Phi^-\rangle$，$|\Psi^+\rangle$，和 $|\Psi^-\rangle$ 表示贝尔态。若未立即使用，链路上的退相干效应可由以下公式表示：

$$w(t) = w_0 e^{-t/t_c}, \tag{1}$$

其中，$w(t)$ 表示生成后经过时间 t 的链路的 Werner 参数，w_0 表示新生成链路的 Werner 参数，而 t_c 表示所涉及存储器的联合相干时间。在具有两个 Werner 参数分别为 w_A 和 w_B 的基本链路的中继器处进行贝尔态测量（BSM）后，将生成一个端到端链路，其 Werner 参数为 $w_A \cdot w_B$。

A5 **单量子比特退相干：**为了描述单个量子比特在内存中等待期间的退相干，我们采用 [14], [15] 中的退相位和非对称振幅阻尼噪声模型：

$$\mathcal{N}_t(\rho) = (1-p(t))(M_0\rho M_0^\dagger + M_1\rho M_1^\dagger) + p(t)Z(M_0\rho M_0^\dagger + M_1\rho M_1^\dagger)Z, \tag{2}$$

其中，密度矩阵 ρ （分别为 $\mathcal{N}_t(\rho)$）表示系统在时刻 0（分别为时刻 t）的状态，$p(t) = (1-e^{-t/t_{de}})/2$ 及

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma(t)} \end{bmatrix},\ M_1 = \begin{bmatrix} 0 & \sqrt{\gamma(t)} \\ 0 & 0 \end{bmatrix},$$

其中 $\gamma(t) = 1 - e^{-t/t_{da}}$。这里，$t_{da}$ 和 t_{de} 分别是表征相关存储器中振幅阻尼效应和退相位效应的两个常数。

A6 **单个阶段的持续时间：**我们假设，量子隐形传态各原子阶段（将在下文介绍）的持续时间，以及协调阶段（Alice 和 Bob 在此阶段检查协议是否成功）的持续时间，均服从参数如表 1 所示的移位指数分布。

在假设 A2 下，量子隐形传态过程按以下顺序执行：

- 阶段 LINK-GEN：在用户（Alice/Bob）与中继器之间建立链路级纠缠。
- 阶段 L-COMM：随后立即将 LINK-GEN 阶段成功或故障的情况告知用户和中继器。请注意，Alice 和 Bob 的 LINK-GEN 与 L-COMM 并行运行。
- 阶段 S-COMM：一旦两条链路均成功生成，中继器便执行贝尔态测量（BSM）；若测量成功，则 Alice 和 Bob 之间会建立端到端纠缠。测量操作直接发生故障的概率为 $(1-p_{交换})$。否则，测量结果会告知 Alice 和 Bob。
- 传输通信阶段：Alice 和 Bob 一旦共享纠缠资源，便立即开始量子隐形传态。在此过程中，Alice 会将测量结果发送给 Bob，Bob 随后对自己的量子比特施加酉操作。

回想一下，所有量子比特完成隐形传态后，Alice 和 Bob 会对其中一部分量子比特的测量结果进行核对，并判断该协议是否成功。我们将相应阶段称为协调通信。请注意，如果任何中间阶段发生故障，该协议会立即重新启动。

陈述其中一些主要结果所需的基本符号见表 1。图 1 根据上述阶段示意了该协议的完成时间。

V0：BB84 协议的一个简化版本，其中 Bob 在 Alice 编码所用的同一基上测量所有量子比特，并将它们全部用于协调，V1：BB84 协议的实际版本，n：一次 BB84 尝试中进行量子隐形传态的量子比特数，α：在 Alice 和 Bob 的基相同的量子比特中，抽样量子比特所占的比例，β：协议成功所需的测量结果一致的最低比例，$M_Z(t) = \mathsf{E}(e^{tZ})$ 对于随机变量 Z，$W_{n,c}$：版本 V0 的完成时间，W_n：版本 V1 的完成时间，T_{GA}（分别为 T_{GB}）：Alice（分别为 Bob）与中继器之间 LINK-GEN 阶段的持续时间，服从独立同分布的 SE($\lambda_{\text{gen}}, a_{\text{gen}}$)，$p_{\text{gen}}$：链路生成尝试的成功概率，$T_{CA}$（分别为 T_{CB}）：Alice（分别为 Bob）与中继器之间 L-COMM 阶段的持续时间，服从独立同分布的 SE($\lambda_{\text{com}}, a_{\text{com}}$)，$p_{\text{swap}}$：中继器处贝尔态测量的成功概率，$T_C$：S-COMM 阶段的持续时间，服从 SE($\lambda_{\text{swap}}, a_{\text{swap}}$)，$w_0$（分别为 w）：新生成链路（分别为一般时刻链路）的 Werner 参数，t_c：中继器处贝尔态测量所涉存储器的联合相干时间，T_C'：T-COMM 阶段的持续时间，服从 SE($\lambda_{\text{AB}}, a_{\text{AB}}$)，$t_{de}$（分别为 t_{da}）：相关量子存储器的退相位（分别为振幅阻尼）常数，K_C：协调阶段 K-COMM 的持续时间，服从 SE(λ_{AB}, a_{AB})，T_{HA}（分别为 T_{HB}）：从开始链路级纠缠生成到 Alice（分别为 Bob）检测到成功所经历的总时间，$V_A = T_{HA} + T_{CA}$,$V_B = T_{HB} + T_{CB}$,T_γ：一次量子隐形传态尝试中失败的交换试验的总持续时间，X：单次量子隐形传态尝试的持续时间，即 $X = T_\gamma + \max\{V_A, V_B\} + T_C' + T_C''$,$Y$：指示变量，表示 Bob 对某个量子比特的测量结果是否与 Alice 的结果一致。

表 1：主要符号。

B. 主要结果

本节陈述在假设 A1 - A6 下关于 BB84 协议完成时间的主要结果。

定理 1 (版本 V1 的完成时间)。 *BB84* 协议完成时间 (W_n) 的矩母函数为：

$$M_{W_n}(t) = \frac{M_{K_C}(t) D_n(t)}{1 - M_{K_C}(t)(M_X^n(t) - D_n(t))} \ , \quad (3)$$

其中 $M_X^n(t) = (M_X(t))^n$ 和

$$D_n(t) \triangleq \sum_{k=1}^{\lceil \alpha n \rceil} M^{(1)}(t; k, \lceil \beta k \rceil) M_X^{n-k}(t) \frac{1}{2^n} \sum_{\frac{k-1}{\alpha} < j \leq \frac{k}{\alpha}} \binom{n}{j}. \quad (4)$$

对于 $j \leq l$, $M^{(1)}(t;\ l, j)$ 定义如下：

$$\begin{aligned} M^{(1)}(t; l, 0) &\triangleq (m_0(t) + m_1(t))^l \ , \\ M^{(1)}(t; l, l) &\triangleq m_1^l(t) \ , \quad l \in \mathbb{N} \ . \end{aligned} \quad (5)$$

此外，对于 $l \geq 2$, $1 \leq j \leq l-2$:

$$\begin{aligned} M^{(1)}(t; l, j) \triangleq & \sum_{k=0}^{1} \binom{l-k}{j} m_0^{l-k-j}(t) m_1^{j+k}(t) \\ & + m_1(t) \sum_{k=j}^{l-2} (m_0(t) + m_1(t))^{l-1-k} \\ & \binom{k}{j} m_0^{k-j}(t) m_1^j(t) \ , \end{aligned} \quad (6)$$

and

$$M^{(1)}(t; l, l-1) \triangleq m_1^l(t) + \binom{l}{1} m_0(t) m_1^{l-1}(t) \ .$$

请注意，$m_0^l(t)$（分别为 $m_1^l(t)$）表示 $(m_0(t))^l$（分别为 $m_1^l(t)$）。此外，

$$\begin{aligned} m_1(t) &\triangleq \mathsf{E}\left(e^{tX} Y\right) = \mathsf{E}\left(e^{tX} | Y = 1\right) \mathsf{P}\left(Y = 1\right), \\ m_0(t) &\triangleq \mathsf{E}\left(e^{tX}(1 - Y)\right) \\ &= \mathsf{E}\left(e^{tX} | Y = 0\right) \mathsf{P}\left(Y = 0\right) \ . \end{aligned} \quad (7)$$

(7) 的右端可以表示为量子隐形传态各原子阶段持续时间的函数，具体如下：

$$m_1(t)=\frac{1}{4}M_{T_\gamma}(t)\Bigg(2I(t,\infty)M_{T_C'}(t)M_{T_C''}(t)+w_0^2I(t,t_c)M_{T_C'}(t-\frac{1}{t_c})\Big(M_{T_C''}(t-\frac{1}{t_{da}})+M_{T_C''}\big(t-\frac{1}{t_{de}}-\frac{1}{2t_{da}}\big)\Big)\Bigg),\quad with \tag{8}$$

$$M_{T_\gamma}(t)=\frac{p_{swap}}{1-(1-p_{swap})M_{T_C'}(t)I(t,\infty)}\ ,$$

and

$$I(t,s)\triangleq \mathsf{E}\left(e^{t\max\{V_A,V_B\}}e^{-\frac{|V_A-V_B|+T_{CA}+T_{CB}}{s}}\right). \tag{9}$$

此外，

$$M_X(t)=M_{T_\gamma}(t)I(t,\infty)M_{T_C'}(t)M_{T_C''}(t)\ . \tag{10}$$

由于 $m_0(t)=M_X(t)-m_1(t)$，我们可以通过代入 $m_1(t)$和$M_X(t)$的表达式来计算。 $I(t,s)$ 的计算过程见第 *III* 节 *C*。

利用定理 1，我们可以推导出 W_n 的累积分布函数（CDF）及其尾概率的一个上界，如下所示。

推论 1 (W_n的累积分布函数)。对于 $s>0$,

$$\mathsf{P}(W_n\le s)=\mathcal{L}^{-1}\{F(t)\}(s),\ with\quad F(t)\triangleq\frac{M_{W_n}(-t)}{t} \tag{11}$$

其中， $\mathcal{L}^{-1}$ 表示拉普拉斯逆变换。式(11) 的数值计算过程将在第 *III-C* 节中介绍。

证明。令 f_n 和 F_n 分别为 W_n的概率密度函数和累积分布函数。将函数 $h(t)$的拉普拉斯变换记为 $\mathcal{L}\{h(t)\}(s)$，则有 $\mathcal{L}\{f_n(t)\}(s)=M_{W_n}(-s)$。由于 $F_n^{'}=f_n$ 且$F_n(0)=0$(当 $W_n>0$时)，因此 $\mathcal{L}\{F_n(t)\}(s)=M_{W_n}(-s)/s$，由此得到式 (11)。 □

推论 2 （V1 版本完成时间的尾界）。 使用切尔诺夫方法，

$$\mathsf{P}(W_n>s)\le\inf_{t\in[0,b)}e^{-ts}M_{W_n}(t)\ , \tag{12}$$

其中 $b=$上标$\{t\in\mathbb{R}:\ M_{W_n}(t)<\infty\}$。注意，对于任意 $t\in[0,b)$， $e^{-ts}M_{W_n}(t)$ 都是 $\mathsf{P}(W_n>s)$ 的一个有效上界，我们使用该上界在第 *III* 节 *-C* 中进行数值计算。

证明。直接对 W_n应用 Chernoff 方法即可得到结论。 □

III. 结果的方法与证明

A. 背景

接下来 [3]–[5]，我们首先用各试验单元的持续时间来表示易发生故障的协议的完成时间 W 。我们假设每次试验都有一个生成阶段，该阶段取决于 r 个相互独立的任务。我们用 T_1、T_2、.....、T_r表示这些任务的持续时间。任务完成后，会立即发生测量/检测事件，该事件以 p(L_1、L_2、.....、L_r、θ)的概率成功，其中 $\{L_i\}_{i\in[r]}$ 是完全决定 $\{T_i\}_{i\in[r]}$的潜变量，而 θ 是反映底层物理系统效率的参数。如果测量事件失败，过程会立即重新开始，并持续进行，直到观察到成功为止。请注意，必须适当地传达该事件成功或失败的信息，以便终止过程或继续下一次试验。我们将试验的这一部分称为通信阶段，其持续时间记为 T_C。我们假设 T_C 与 $\{L_i\}_{i\in[r]}$ 相互独立，并且各次试验也相互独立。如果测量事件耗时不可忽略，我们可以将 T_C 视为测量事件和通信事件所对应的总时间。在这种情况下，通信阶段称为局部操作和经典通信阶段。有关完成时间的示意图，请参见图2。

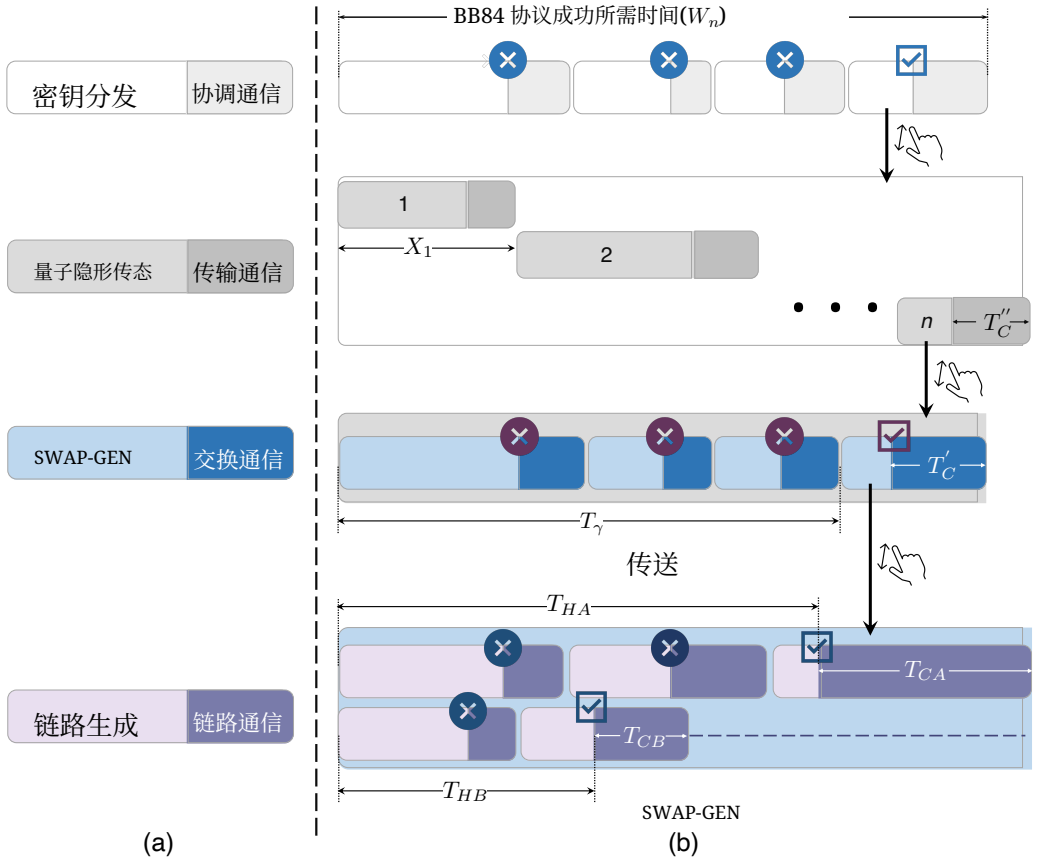


图 1：BB84 协议完成时间示意图（W_n）：（**a**）描述一个试验单元；如（**b**）所示，独立试验会重复进行，直到成功，但第二行除外。图示未按比例绘制。一次 BB84 尝试包含两个阶段：量子比特的量子隐形传态（KEY-DIST）和协调（K-COMM）。KEY-DIST 包含 n 顺序执行的 TELEPORT+T-COMM 试验，每次试验的持续时间服从 X。W_n 的矩母函数通过式 (28) 与 X 相关。TELEPORT 单元中的每次试验由 SWAP-GEN 和 S-COMM 阶段组成。S-COMM 表示将中继器处贝尔态测量（BSM）的成功/故障情况通信给端系统。此外，SWAP-GEN 的持续时间为两个模块持续时间的最大值：每个模块代表链路级纠缠生成的完成时间，其试验单元包含 LINK-GEN（端系统与中继器之间的链路级纠缠生成）和 L-COMM（LINK-GEN 成功/故障情况的通信）阶段。最后一行的虚线表示一条链路必须等待另一条链路成功所需的时间。用于标注的变量定义见表 1。

命题 1。 *(i)* 假设生成阶段中的 r 个任务并行运行。 完成时间由此给出：矩母函数

$$M_W(t) = \frac{\mathsf{E}(e^{tT_C})\mathsf{E}\left(e^{t\max_{i\in[r]}T_i}p_\theta(\mathbf{L}^{(1)})\right)}{1-\mathsf{E}(e^{tT_C})\mathsf{E}\left(e^{t\max_{i\in[r]}T_i}(1-p_\theta(\mathbf{L}^{(1)}))\right)}, \tag{13}$$

W：协议的完成时间，T_1，T_2、.....、T_r：GENERATE 阶段各组成任务的持续时间，L_1，L_2、.....、L_r：完全决定GENERATE 阶段持续时间以及测量事件成功概率的潜变量，θ：测量的硬件效率参数，p（L_1，L_2、.....、L_r，θ）：测量事件的成功概率，T_C：COMMUNICATE/局部操作和经典通信阶段的持续时间。表 2：第 III-A 节中用于描述易发生故障协议的符号。

对于 $\mathsf{E}\big(e^{tT_C}\big(e^{t\max_{i\in[r]}T_i}(1-p_\theta(\mathbf{L}^{(1)}))\big)\big)<1$，结果只需观察到，当任务按顺序执行时 $U_j=\sum_{i=1}^r T_i^{(j)}+T_C^{(j)}$，并仿照 (i) 部分的证明即可得出。 □

接下来的结果有助于推导完成时间 W 的尾界。

命题 2. 设 $I_1, I_2, \ldots, I_r, I_C$ 分别为随机变量 $T_1, T_2, \ldots, T_r, T_C$ 的矩母函数存在的零点邻域。此外，设 I_0 表示 $G(t)=\mathsf{E}(e^{tU_1}(1-p_\theta(\mathbf{L}^{(1)})))<1$ 的零点邻域。那么 W 的矩母函数在 $\bigcap_{l\in[r]\cup\{0,C\}} I_l$ 中存在。

证明。参见第 VI-A 节。 □

推论 3. 若 $T_1, T_2, \ldots, T_r, T_C$ 是次指数分布，则 W 也是次指数分布。

Proof. See Sect. VI-A. □

推论 3 基本上保证了 W 的矩母函数在零点邻域内存在，这意味着我们可以应用切尔诺夫方法来获得尾概率的上界：

$$\mathsf{P}(W>s)\le \inf_{t\in[0,b)} e^{-ts}\mathsf{E}(e^{tW}), \qquad (16)$$

其中 $b=\sup\{t\in\mathbb{R}: M_W(t)<\infty\}$.

B. 主要结果的证明

本节安排如下：首先，我们推导给定纠缠资源的 Werner 参数时一次量子隐形传态尝试的成功概率，以及在量子隐形传态过程中 Alice 将其测量结果发送给 Bob 所需的时间。随后利用该结果证明，

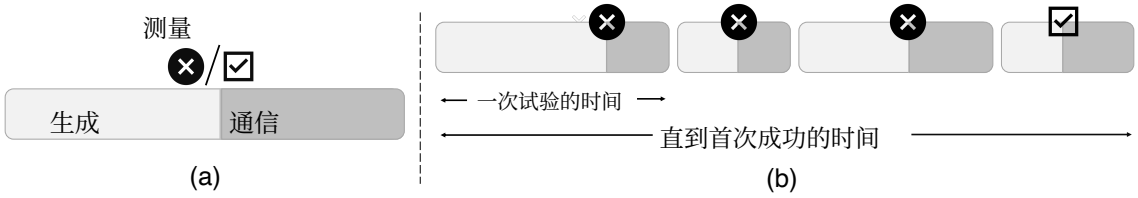


图 2：易发生故障的协议完成时间示意图：**(a)** 每次试验都从生成阶段开始，随后发生测量/检测事件，产生成功 (✓) 或故障 (×)。测量结果通常取决于生成阶段的细节，并在通信/LOCC 阶段告知相关参与方。两个阶段的持续时间是随机且相互独立的。重复进行相互独立的试验，直至测量事件产生成功结果；完成时间如 **(b)** 所示。

式 (8) 和 (10) 中 m_1 与 M_X 的表达式是有效的。接下来，我们推导完成简化版本 V0 的完成时间，这有助于我们按照定理 1 中的陈述计算实际版本的矩母函数。

引理 1. 假设量子隐形传态始于由 *Werner* 参数 w 给定的纠缠资源。我们还将 *Alice* 在量子隐形传态过程中向 *Bob* 发送测量结果所需的时间记为 $T_C^{''}$ （见表 *1*）。那么，根据这些量，量子隐形传态的成功概率可表示为：

$$\begin{aligned} p_\Lambda \triangleq & \mathsf{P}\left(Y=1|w,T_C^{''}\right) \\ =& \frac{1}{4}\left(2+we^{-T_C^{''}/t_{da}}+we^{-T_C^{''}(1/t_{de}+1/2t_{da})}\right) . \end{aligned}$$

回顾一下， t_{de} 和 t_{da} 分别表示刻画退相位噪声和振幅阻尼噪声对 *Bob* 的量子存储器影响的常数。

证明。 我们从 Alice 和 Bob 在数据量子比特 $|\phi\rangle = a\,|0\rangle + b\,|1\rangle$ 的标准量子隐形传态协议各阶段中的联合态密度矩阵表示开始；这一表示可见于标准教材，尤其是将 $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 作为纠缠资源时。下文假设 Alice 持有数据量子比特 $|\phi\rangle$，而 $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ 由 Alice 和 Bob 共享。这是计算一次量子隐形传态尝试成功概率的必要步骤，因为在 BB84 密钥分发示例中，量子隐形传态开始时使用的纠缠资源是一般的 Werner 态，而不是 $|\Phi^+\rangle$。按照约定，第一和第二个量子比特属于 Alice，第三个属于 Bob。如果量子比特未按自然顺序排列，则会在包含相关状态的括号外明确标出其索引。标准量子隐形传态协议的各阶段

with $|\Psi^+\rangle$ 可以写成如下形式：

$$
\begin{aligned}
&\frac{1}{2}\left(|01\rangle\langle 01|+|01\rangle\langle 10|+|10\rangle\langle 01|+|10\rangle\langle 10|\right)_{13}\left(a^2|0\rangle\langle 0|+a^*b|1\rangle\langle 0|+ab^*|0\rangle\langle 1|+b^2|1\rangle\langle 1|\right)_2\\
=&\frac{a^2}{2}\left(|001\rangle\langle 001|+|001\rangle\langle 100|+|100\rangle\langle 001|+|100\rangle\langle 100|\right)+\frac{a^*b}{2}\left(|011\rangle\langle 001|+|011\rangle\langle 100|+|110\rangle\langle 001|\right.\\
&\left.+|110\rangle\langle 100|\right)+\frac{ab^*}{2}\left(|001\rangle\langle 011|+|001\rangle\langle 110|+|100\rangle\langle 011|+|100\rangle\langle 110|\right)+\frac{b^2}{2}\left(|011\rangle\langle 011|+|011\rangle\langle 110|\right.\\
&\left.+|110\rangle\langle 011|+|110\rangle\langle 110|\right)\\
\xrightarrow{O_1}&\frac{a^2}{2}\left(|001\rangle\langle 001|+|001\rangle\langle 110|+|110\rangle\langle 001|+|110\rangle\langle 110|\right)+\frac{a^*b}{2}\left(|011\rangle\langle 001|+|011\rangle\langle 110|+|100\rangle\langle 001|\right.\\
&\left.+|100\rangle\langle 110|\right)+\frac{ab^*}{2}\left(|001\rangle\langle 011|+|001\rangle\langle 100|+|110\rangle\langle 011|+|110\rangle\langle 100|\right)+\frac{b^2}{2}\left(|011\rangle\langle 011|+|011\rangle\langle 100|\right.\\
&\left.+|100\rangle\langle 011|+|100\rangle\langle 100|\right)\\
\xrightarrow{O_2}&\frac{a^2}{4}\left(|001\rangle\langle 001|+|001\rangle\langle 110|+|110\rangle\langle 001|+|110\rangle\langle 110|+|011\rangle\langle 001|+|011\rangle\langle 110|+|100\rangle\langle 001|+|100\rangle\langle 110|\right.\\
&\left.+|001\rangle\langle 011|+|001\rangle\langle 100|+|110\rangle\langle 011|+|110\rangle\langle 100|+|011\rangle\langle 011|+|011\rangle\langle 100|+|100\rangle\langle 011|+|100\rangle\langle 100|\right)\\
&+\frac{a^*b}{4}(\ldots)+\frac{ab^*}{4}(\ldots)+\frac{b^2}{4}(\ldots)\\
=&\frac{1}{4}|00\rangle\langle 00|\left(a^2|1\rangle\langle 1|+a^*b|0\rangle\langle 1|+ab^*|1\rangle\langle 0|+b^2|0\rangle\langle 0|\right)+\frac{1}{4}|01\rangle\langle 01|\left(a^2|0\rangle\langle 0|+a^*b|1\rangle\langle 0|+ab^*|0\rangle\langle 1|\right.\\
&\left.+b^2|1\rangle\langle 1|\right)+\frac{1}{4}|10\rangle\langle 10|\left(a^2|1\rangle\langle 1|-a^*b|0\rangle\langle 1|-ab^*|1\rangle\langle 0|+b^2|0\rangle\langle 0|\right)+\frac{1}{4}|11\rangle\langle 11|\left(a^2|0\rangle\langle 0|-a^*b|1\rangle\langle 0|\right.\\
&\left.-ab^*|0\rangle\langle 1|+b^2|1\rangle\langle 1|\right)+\rho_0\ ,
\end{aligned}
\tag{17}
$$

其中，ρ_0 表示在标准基下测量时不会对最终态产生任何贡献的残余项。此外，操作 O_1 和 O_2 分别表示受控非门$_{12}$ 和 $H_1\otimes I_2$。因此，如果量子隐形传态以 $p_1|\Phi^+\rangle\langle\Phi^+|+p_2|\Phi^-\rangle\langle\Phi^-|+p_3|\Psi^+\rangle\langle\Psi^+|+p_4|\Psi^-\rangle\langle\Psi^-|$ 作为纠缠资源，那么在 Alice 测量之前，系统的（未归一化）状态为：

$$
\begin{aligned}
&|00\rangle\langle 00|\left(p_1|\phi\rangle\langle\phi|+p_2|\phi_z\rangle\langle\phi_z|+p_3|\phi_x\rangle\langle\phi_x|+p_4|\phi_y\rangle\langle\phi_y|\right)+|01\rangle\langle 01|\left(p_1|\phi_x\rangle\langle\phi_x|+p_2|\phi_y\rangle\langle\phi_y|\right.\\
&\left.+p_3|\phi\rangle\langle\phi|+p_4|\phi_z\rangle\langle\phi_z|\right)+|10\rangle\langle 10|\left(p_1|\phi_z\rangle\langle\phi_z|+p_2|\phi\rangle\langle\phi|+p_3|\phi_y\rangle\langle\phi_y|+p_4|\phi_x\rangle\langle\phi_x|\right)\\
&+|11\rangle\langle 11|\left(p_1|\phi_y\rangle\langle\phi_y|+p_2|\phi_x\rangle\langle\phi_x|+p_3|\phi_z\rangle\langle\phi_z|+p_4|\phi\rangle\langle\phi|\right)+\rho_{00}\ ,
\end{aligned}
\tag{18}
$$

其中，ρ_{00} 表示不参与测量结果的项，而 $|\phi_x\rangle, |\phi_y\rangle$ 和 $|\phi_z\rangle$ 分别表示对 $|\phi\rangle$进行泡利 X、XZ 和 Z 旋转。现在将 Alice 测量后 Bob 的量子比特状态记为 $\rho(|\phi\rangle)$。由于传递测量结果需要时间 $T_C^{''}$，Bob 在应用酉操作之前（根据测量结果，对某个 $l,k\in\{0,1\}$ 施加 Z^lX^k）的量子比特状态为 $\mathcal{N}_{T_C^{''}}(\rho)$。

回顾 BB84 协议，数据量子比特 $|\phi\rangle\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$，对于由 Werner 参数 w, $p_1=(1+3w)/4$, $p_2=p_3=p_4=(1-w)/4$ 指定的纠缠资源，将 $|\phi\rangle$ 和 $\{p_i\}_{i=1}^4$ 的值代入式 (18)，状态 $\rho(|\phi\rangle)$ 可以进一步简化为：

$$
\rho(|\phi\rangle)=\frac{1+w}{2}|\phi\rangle\langle\phi|+\frac{1-w}{2}|\phi'\rangle\langle\phi'| \quad \text{or} \quad \frac{1-w}{2}|\phi\rangle\langle\phi|+\frac{1+w}{2}|\phi'\rangle\langle\phi'|\ ,
$$

每种情况出现的概率均为 $1/2$。这里，$|\phi'\rangle$ 将 $(|0\rangle, |1\rangle, |+\rangle, |-\rangle)$ 映射为 $(|1\rangle, |0\rangle, |-\rangle, |+\rangle)$。注意，Bob 在 $\mathcal{N}_{T_C''}(\rho(|\phi\rangle))$ 上施加适当的酉变换 $(Z^l X^k)$，以恢复 $|\phi\rangle\langle\phi|$。此外，

$$\mathcal{N}_{T_C''}(|0\rangle\langle 0|) = |0\rangle\langle 0| \ , \quad \mathcal{N}_{T_C''}(|1\rangle\langle 1|) = \gamma(\cdot)\,|0\rangle\langle 0| + \big(1-\gamma(\cdot)\big)\,|1\rangle\langle 1| \ ,$$

$$\mathcal{N}_{T_C''}(|\phi\rangle\langle\phi|) = \frac{1+(1-2p(\cdot))\sqrt{1-\gamma(\cdot)}}{2}\,|\phi\rangle\langle\phi| + \frac{1-(1-2p(\cdot))\sqrt{1-\gamma(\cdot)}}{2}\,|\phi'\rangle\langle\phi'|\,, |\phi\rangle \in \{|+\rangle, |-\rangle\},$$

为简洁起见，我们省略了 $\gamma(T_C'')$ 和 $p(T_C'')$ 中的参数 T_C''。这意味着：

$$\mathcal{N}_{T_C''}(\rho(|0\rangle)) = \begin{cases} \left(\frac{1+w}{2} + \gamma(\cdot)\frac{1-w}{2}\right)|0\rangle\langle 0| + (1-\gamma(\cdot))\frac{1-w}{2}\,|1\rangle\langle 1|\,, & \text{w.p. } \frac{1}{2} \\ \left(\frac{1-w}{2} + \gamma(\cdot)\frac{1+w}{2}\right)|0\rangle\langle 0| + (1-\gamma(\cdot))\frac{1+w}{2}\,|1\rangle\langle 1|\,, & \text{w.p. } \frac{1}{2}. \end{cases}$$

现在，我们可以计算 Bob 恢复 $|0\rangle$ 的概率为 $(1+w-w\gamma(\cdot))/2$，结果表明，$|\phi\rangle = |1\rangle$ 的恢复概率也相同。另一方面，Bob 成功恢复 $|+\rangle$ 或 $|-\rangle$ 的概率为 $(1+w(1-2p(\cdot))\sqrt{1-\gamma(\cdot)})/2$。由于在 BB84 协议中，四个数据量子比特出现的可能性均相等，因此我们有

$$\begin{aligned} p_\Lambda =& \frac{1}{4}\big(1 + w - w\gamma(T_C'') + 1 + w(1-2p(T_C''))\sqrt{1-\gamma(T_C'')}\big) \\ =& \frac{1}{4}\big(2 + we^{-T_C''/t_{da}} + we^{-T_C''(1/t_{de}+1/2t_{da})}\big) \ . \end{aligned}$$

□

（*8*）的证明（8）和（10）。首先，请读者参阅图 1，其中展示了单个量子比特的量子隐形传态持续时间，并标注了其组成阶段及各自的持续时间。回顾一下，T_{HA}（分别为 T_{HB}）表示 Alice（分别为 Bob）成功生成链路级纠缠所需的时间，而对此事件的通信需要花费 T_{CA}（分别为 T_{CB}）的时间。为了推导式（8）中 $M_{T_\gamma}(t)$ 的表达式，我们首先注意到，交换故障时间 T_γ 由 $(\text{Geo}(p_{\text{swap}}) - 1)$ 次相互独立的交换试验组成，每次试验的持续时间均为 $\max\{T_{HA}+T_{CA}, T_{HB}+T_{CB}\} + T_C'$。现在应用（13），即可得到所给出的表达式。

现在，(10) 中 $M_X(t)$ 的表达式可由表 1 给出的量子比特隐形传态时间 X 的分解得出：

$$X = T_\gamma + \max\{V_A, V_B\} + T_C' + T_C'' \ , \quad (19)$$

（9）中 $I(t,\ s)$ 的定义，以及上述右侧各分量相互独立这一事实。

接下来，我们建立 $m_1(t)$的公式。根据假设 A4，一次成功的交换因此会导致一个 Alice 与 Bob 之间的端到端纠缠，其特征由 Werner 参数表征：

$$w_0^2 e^{-(|T_{HA}+T_{CA}-T_{HB}-T_{CB}|+T_{CA}+T_{CB})/t_c} \ ,$$

其中，w_0 表示新生成链路的 Werner 参数，t_c 表示相关存储器的联合相干时间。传送还需要 T_C' 时间才能启动，因此开始时具有以下纠缠资源：

$$w = w_0^2 e^{-(|V_A-V_B|+T_{CA}+T_{CB}+T_C')/t_c} \ .$$

回忆表 1 中，$V_A = T_{HA} + T_{CA}$（B 的情况则为）。当 Alice 发送测量结果时（在时间跨度 T_C'' 内），Bob 的量子比特发生的退相干由假设 A5 中描述的噪声模型刻画。根据引理 1，给定（$T_{HA}, T_{CA}, T_{HB}, T_{CB}, T_C', T_C''$），量子隐形传态尝试成功的概率为

$$p_\Lambda = \frac{1}{4}\big(2 + we^{-T_C''/t_{da}} + we^{-T_C''(\frac{1}{t_{de}}+\frac{1}{2t_{da}})}\big). \quad (20)$$

由于 $m_1(t) = \mathsf{E}(e^{tX}Y)$，我们现在可以使用 X 和 P $\left(Y=1|w,T_C''\right)$ 的表达式来计算期望，从而得到公式 (8)。 □

现在我们证明引理 2，该引理有助于我们将实际版本 V1 的完成时间的矩母函数表示为定理 1 中形式化定义的形式。

引理 2（V0 版本的完成时间）。 我们定义 $c = \lceil \beta n \rceil$。*V0* 版本的完成时间 $(W_{n,\,c})$ 的矩母函数为：

$$M_{W_{n,c}}(t) = \frac{M_{K_C}(t) M^{(1)}(t; n, c)}{1 - M_{K_C}(t) M^{(0)}(t; n, c)} \ ,$$

其中 $M^{(1)}$ 在定理 *1* 中定义，且

$$M^{(0)}(t; l, j) = (m_0(t) + m_1(t))^l - M^{(1)}(t; l, j). \tag{21}$$

证明。 回顾一下，在 V0 版本中，Bob 使用与 Alice 编码时相同的基对所有隐形传态量子比特进行测量，并且所有这些量子比特都用于协调。我们用 X_i 表示第 i 个量子比特的量子隐形传态持续时间。此外，令 Y_i 为一个指示变量，当 Bob 对第 i 个量子比特的测量结果与 Alice 最初编码的结果一致时，取值为 1。因此，$(X_i,\ Y_i) \overset{iid}{\sim} (X,\ Y)$。此外，一次 BB84 尝试的持续时间为：$K_C + \sum_{i=1}^{n} X_i$。现在，令 c 表示协议的成功阈值，即当且仅当 $\sum_{i=1}^{n} Y_i \geq c$ 时，一次 BB84 尝试才算成功。因此，利用命题 1 的第 (ii) 部分，我们得到：

$$M_{W_{n,c}}(t) = \frac{M_{K_C}(t)\mathsf{E}(e^{t\sum_{i=1}^{n} X_i} \mathbb{1}_{\sum_{i=1}^{n} Y_i \geq c})}{1 - M_{K_C}(t)\mathsf{E}(e^{t\sum_{i=1}^{n} X_i} \mathbb{1}_{\sum_{i=1}^{n} Y_i < c})}. \tag{22}$$

定义如下

$$\bar{M}^{(1)}(t; l, j) \triangleq \mathsf{E}(e^{t\sum_{i=1}^{l} X_i} \mathbb{1}_{\sum_{i=1}^{l} Y_i \geq j}) \ ,$$
$$\bar{M}^{(0)}(t; l, j) \triangleq \mathsf{E}(e^{t\sum_{i=1}^{l} X_i} \mathbb{1}_{\sum_{i=1}^{l} Y_i < j}) \ .$$

为了完成证明，我们需要证明 $\bar{M}^{(1)} \equiv M^{(1)}$ 和 $\bar{M}^{(0)} \equiv M^{(0)}$。注意，$\bar{M}^{(1)}(t; 1, 0) = m_0(t) + m_1(t)$，且 $\bar{M}^{(1)}(t; 1, 1) = m_1(t)$。由于 $(X_i, Y_i) \overset{iid}{\sim} (X, Y)$，

$$\begin{aligned} \bar{M}^{(1)}(t; l, 0) &= (m_0(t) + m_1(t))^l \ , \\ \bar{M}^{(1)}(t; l, l) &= m_1^l(t) \ , \quad l \in \mathbb{N} \ . \end{aligned} \tag{23}$$

现在，对于 $l \geq 2, 1 \leq j \leq l$，

$$\begin{aligned} &\bar{M}^{(1)}(t; l, j) \\ &= \mathsf{E}\big(e^{t\sum_{i=1}^{l} X_i}(\mathbb{1}_{Y_1=0}\mathbb{1}_{\sum_{i=2}^{l} Y_i \geq j} \\ &\quad + \mathbb{1}_{Y_1=1}\mathbb{1}_{\sum_{i=2}^{l} Y_i \geq j-1})\big) \\ &= \mathsf{E}(e^{tX_1}\mathbb{1}_{Y_1=0})\mathsf{E}(e^{t\sum_{i=2}^{l} X_i}\mathbb{1}_{\sum_{i=2}^{l} Y_i \geq j}) \\ &\quad + \mathsf{E}(e^{tX_1}\mathbb{1}_{Y_1=1})\mathsf{E}(e^{t\sum_{i=2}^{l} X_i}\mathbb{1}_{\sum_{i=2}^{l} Y_i \geq j-1}) \\ &= m_0(t)\bar{M}^{(1)}(t; l-1, j) \\ &\quad + m_1(t)\bar{M}^{(1)}(t; l-1, j-1) \ . \end{aligned} \tag{24}$$

这里，第二个和第三个等式由以下事实得出：$(X_i,\ Y_i) \overset{iid}{\sim} (X,\ Y)$。

为求解递推关系，我们引入以下简写：$a_{l,\,j} = \bar{M}^{(1)}(t;\ l,\ j)$、$m_0 = m_0(t)$ 和 $m_1 = m_1(t)$。因此，$a_{1,\,0} = m_0 + m_1$、$a_{1,\,1} = m_1$，且对于 $l \geq 2$，$1 \leq j \leq l-1$，

$$a_{l,j} = m_0 a_{l-1,j} + m_1 a_{l-1,j-1} \ . \tag{25}$$

此外，(23) 可改写为：

$$a_{l,0} = (m_0 + m_1)^l, \quad a_{l,l} = m_1^l, \quad l \in \mathbb{N}. \tag{26}$$

现在定义生成函数：

$$A_l(x) \triangleq \sum_{j=0}^{l} a_{l,j} x^j, \quad l \in \mathbb{N} \ .$$

将 (25) 两边乘以 x^j 并对 $1 \leq j \leq l-1$ 求和，可得对于 $l \geq 2$：

$$\begin{aligned} A_l(x) = &(m_0 + m_1 x) A_{l-1}(x) \\ &+ (m_0 + m_1)^{l-1} m_1 \ , \end{aligned} \tag{27}$$

其中 $A_1(x) = m_0 + m_1 + m_1 x$。注意，我们使用了 (26) 得到 (27)。对于 $l \geq 2$，在 (27) 中递归代入可得：

$$\begin{aligned} A_l(x) &= (m_0 + m_1 x)^{l-1} A_1(x) \\ &+ m_1 \sum_{k=0}^{l-2} (m_0 + m_1 x)^k (m_0 + m_1)^{l-1-k} \ , \end{aligned}$$

经过一些计算后，得到：

$$a_{l,l-1} = m_1^l + \binom{l}{1} m_0 m_1^{l-1} ,$$
$$a_{l,j} = \binom{l}{j} m_0^{l-j} m_1^j + \binom{l-1}{j} m_0^{l-1-j} m_1^{j+1} + m_1 \sum_{k=j}^{l-2} (m_0+m_1)^{l-1-k} \binom{k}{j} m_0^{k-j} m_1^j ,$$

对于 $1 \le j \le l-2$。现在很容易看出 $\bar{M}^1 \equiv M^1$ $(e^{tX}) = m_0\ t\ +()()$。此外，E $m_1\ t$ $\bar{M}^0 \equiv M^0$ $()()$，由此可得 $()()$。 □

定理 *1* 的证明。回想一下，在 Bob 的测量基与 Alice 一致的 B ∼Bin($n, 1/2$) 个量子比特中，会不放回地抽取 $B_1 = \lceil \alpha B \rceil$ 个进行正确性检查；如果至少有 β 比例的样本中对应测量结果匹配，则协议被视为成功。协议必须重复运行，直到 $B_1 \ge 1$。令 Z_i 表示伯努利随机变量，当且仅当抽取了第 i 个量子比特时取值为 1，即 $B_1 = \sum_{i=1}^n Z_i$。此外，令 k_i（$i \in [B_1]$）表示满足 $Z_{k_i} = 1$ 的索引。因此，当 $B_1 \ge 1$ 且 $\sum_{i=1}^{B_1} Y_{k_i} \ge \beta B_1$ 时，协议成功；其中 Y_j 是指示变量，当 Bob 对第 j 个量子比特的测量结果与其原始值一致时取值为 1。记

$$\bar{D}_n(t) \triangleq \mathsf{E}(e^{t\sum_1^n X_i} \mathbb{1}_{\sum_{i=1}^{B_1} Y_{k_i} \ge \beta B_1} \mathbb{1}_{B_1 \ge 1}), \quad (28)$$

我们有：

$$M_{W_n}(t) = \frac{M_{K_C}(t)\bar{D}_n(t)}{1 - M_{K_C}(t)(M_X^n(t) - \bar{D}_n(t))} ,$$

由于命题 1 的第 (ii) 部分。现在我们证明确实如此_ $D_n \equiv D_n$。注意到

$$\begin{aligned}\bar{D}_n(t) &= \sum_{k=1}^{\lceil \alpha n \rceil} M^{(1)}(t; k, \lceil \beta k \rceil) M_X^{n-k}(t) \\ &\quad \mathsf{P}(B_1 = k) \\ &= \sum_{k=1}^{\lceil \alpha n \rceil} M^{(1)}(t; k, \lceil \beta k \rceil) M_X^{n-k}(t) \\ &\quad \frac{1}{2^n} \sum_{\frac{k-1}{\alpha} < j \le \frac{k}{\alpha}} \binom{n}{j},\end{aligned}$$

由此完成证明。 □

C. 完成时间的累积分布函数和尾概率的数值计算

我们首先介绍式 (9) 中 $I(t,\ s)$ 的数值计算，随后将用它对 $M_{W_n}(t)$ 进行数值计算。注意，T_{HA}（分别为 T_{HB}）等于 N_A（分别为 N_B）次链路生成试验和 $N_A - 1$（分别为 $N_B - 1$）次链路通信试验所需时长之和，其中 N_A（分别为 N_B）表示 Alice（分别为 Bob）成功建立链路级纠缠所需的试验次数，即 N_A，$N_B \overset{iid}{\sim}$ 几何分布(p_{gen})。此外，T_{HA}和 T_{HB} 相互独立同分布。现在，

$$\begin{aligned}&I(t,s) \\ =&\mathsf{E}\left(e^{t\max\{V_A,V_B\}} e^{-\frac{|V_A - V_B| + T_{CA} + T_{CB}}{s}}\right) \\ =&2e^{(t-\frac{2}{s})a_{\text{com}}} \left(\frac{\lambda_{\text{com}}}{\lambda_{\text{com}} + \frac{2}{s} - t} - \frac{2\lambda_{\text{com}}}{2\lambda_{\text{com}} + \frac{2}{s} - t}\right) \\ &\mathsf{E}\left(e^{(\lambda_{\text{com}} + \frac{1}{s})T_{HA}} e^{-(\lambda_{\text{com}} + \frac{1}{s} - t)T_{HB}} \mathbb{1}_{T_{HB} > T_{HA}}\right) \\ &+ \frac{\lambda_{\text{com}}}{\lambda_{\text{com}} + \frac{2}{s} - t} \mathsf{E}\left(e^{\frac{1}{s}T_{HA}} e^{-(\frac{1}{s} - t)T_{HB}} \mathbb{1}_{T_{HB} > T_{HA}}\right).\end{aligned}$$

为了评估这一期望，我们推导了形如 E $\left(e^{\eta T_{HA}} e^{-(\eta - t)T_{HB}} \mathbb{1}_{T_{HB} > T_{HA}}\right)$ 的量的表达式。注意到 $T_{HA} = \sum_{i=1}^{N_A} T_{GA}^{(i)} + \sum_{i=1}^{N_A - 1} T_{CA}^{(i)}$，其中 [1] $T_{GA}^{(i)} \overset{iid}{\sim} T_{GA}$和 $T_{CA}^{(i)} \overset{iid}{\sim} T_{CA}$ $S_{GA}^{(j)} =$。我们进一 $\sum_{i=1}^{j} T_{GA}^{\ i}$ $S_{CA}^{(j)} = \sum_{i=1}^{j} T_{CA}^{(i)}$ 步记 $()$，（B 的情况类似）。显然，对于 $j \in \mathbb{N}$（B 的情况类似），$S_{GA}^{(j)} \overset{d}{=} ja_{\text{gen}} +$ $j\ \lambda_{\text{gen}}$ $S_{CA}^{(j)} \overset{d}{=}$ $ja_{\text{com}} +$ $j\ \lambda_{\text{com}}$ $S_{GA}^{(j)}$ $S_{CA}^{(j)}$ 伽马分布(,)、伽马分布(,) 以及 和 相互独立。因此，

$$\begin{aligned}&\mathsf{E}\left(e^{\eta T_{HA}} e^{-(\eta - t)T_{HB}} \mathbb{1}_{T_{HB} > T_{HA}}\right) \\ =&p_{\text{gen}}^2 \sum_{l=0}^{\infty} \sum_{k=0}^{\infty} (1 - p_{\text{gen}})^{k+l} \mathsf{E}\Big(e^{\eta(S_{GA}^{(l+1)} + S_{CA}^{(l)})} \\ &e^{-(\eta - t)(S_{GB}^{(k+1)} + S_{CB}^{(k)})} \\ &\mathbb{1}_{S_{GB}^{(k+1)} + S_{CB}^{(k)} > S_{GA}^{(l+1)} + S_{CA}^{(l)}}\Big) .\end{aligned} \quad (29)$$

[1]形如 $\sum_1^0$ 的求和按约定为零。

我们通过数值积分计算式 (29) 求和项中的期望值。由于对于 $j \in \mathbb{N}$，$S_{GA}^{(j)}$ 和 $S_{CA}^{(j)}$ 相互独立，且其对应的概率密度函数（移位伽马分布）已知，因此这一计算过程较为简单。随后，我们对该求和进行计算，直至达到某个截断点（例如 $0 \le l \le$128, $0 \le k \le 128$）。由于我们只需要在 $s = \infty$ 和 $s = t_{\text{coh}}$ 处计算 $I(t, s)$，因此仅需针对 $\eta = \lambda_{\text{com}} + 1/t_{\text{coh}}, 1/t_{\text{coh}}, \lambda_{\text{com}}, 0$ 计算式 (29)。

根据（11），为了计算 W_n 的累积分布函数（CDF），我们使用现成的数值拉普拉斯逆变换算法，例如 Python 的 mpmath 库中的 invertlaplace。此外，我们按以下方式数值计算 Chernoff 界：

$$\mathsf{P}(W_n > s) \le \min_{j \in [r]} \{e^{-ts} M_{W_n}(t_j)\} \ ,$$

其中，$M_{W_n}(t_j) < \infty$ 和 $r \in \mathbb{N}$，例如 10。需要注意的是，这是一个近似界，因为 $M_{W_n}(t_j)$ 是通过公式 (29) 进行数值估计的。在未来的工作中，我们计划计算该估计的误差界，从而进一步得到尾概率的上界。

IV. BB84 协议完成时间的合成仿真

如第 II 节所示，要成功实现 BB84 协议，就需要重复进行隐形传态试验，而每次试验又由多个生成和通信阶段组成。因此，模拟该协议的完成时间（W_n）非常耗时。为此，我们提出一种算法，可在各个阶段的持续时间服从移位指数分布（假设 A6），且相应参数已知或可估计时，高效模拟持续时间 W_n。

请回想一下，作为 BB84 协议的一部分，部分隐形传态量子比特会接受正确性检查，其余则用作密钥比特，即不进行检查。所提出算法的核心思想是求出直到完成时未检查量子比特数、成功隐形传态的量子比特数以及未成功隐形传态的量子比特数的分布。随后，我们对单个量子比特的隐形传态时间拟合一个分布 (i) 无条件情况下，(ii) 给定量子隐形传态尝试成功，以及 (iii) 给定尝试以故障告终。最终持续时间 W_n 由以下各项的总和给出：(i) 汇总后的无条件隐形传态时间，(ii) 汇总后的成功隐形传态时间，(iii) 汇总后的失败隐形传态时间，以及 (iv) 总协调时间。我们的方案之所以能够加速，是因为只要为单量子比特传送时间选择适当的分布，无论量子比特 n 的数量是多少，这种汇总后的持续时间都能通过固定数量的步骤进行模拟。请注意，只有在假设模拟过程将重复执行大量次时，这种方法才有优势。在这种情况下，分布拟合只需进行一次，其结果可供后续模拟重复使用，从而使这种方法更具优势。

下一个结果指出，如果已知各阶段持续时间在一次尝试成功或失败条件下的分布，则可以反向模拟易发生故障的协议的完成时间。该结果只需对式 (13) 中的矩母函数重新排列各项即可得出。

引理 3. 设 Y是一个伯努利随机变量，X、W、T_C是随机变量，且满足

$$\mathsf{E}\big(e^{tW}\big) = \frac{M_{T_C}(t)\mathsf{E}\big(e^{tX}\mathbb{1}_{Y=1}\big)}{1 - M_{T_C}(t)\mathsf{E}\big(e^{tX}\mathbb{1}_{Y=0}\big)},$$

其中 $M_{T_C}(t) = \mathsf{E}\big(e^{tT_C}\big)$，且 X和 T_C 的矩母函数存在于零点邻域内。于是，

$$W \stackrel{d}{=} \tilde{W} = \sum_{j=1}^{N} T_j + \sum_{j=1}^{N-1} X_j^{(0)} + X_1^{(1)},$$

其中，T_j、$X_j^{(0)}$、$X_j^{(1)}$ 和 N 相互独立地取自以下已知分布：$T_j \overset{iid}{\sim} T_C$、$X_j^{(0)} \overset{iid}{\sim} X|Y=0$、$X_j^{(1)} \overset{iid}{\sim} X|Y=1$（对应 $j \in \mathbb{N}$），以及 $N \sim$ 几何分布$(\mathsf{P}(Y=1))$。

证明。参见第 VI-A 节。 □

现在让我们回顾一下第 II 节中 BB84 协议的几个特征：当至少有一个量子比特被抽样，且在抽样量子比特中，特定比例（β）实现了忠实的量子隐形传态时，该协议即被视为成功。沿用此前的符号表示，来自

引理 3 和第 II 节，令 N 表示首次成功之前协议必须运行的次数。也就是说，

$$N \sim \text{Geo}(\mathsf{P}(U=1)) \ , \quad \text{where}$$
$$U = \mathbb{1}_{\sum_{i=1}^{B_1} Y_{k_i} \geq \beta B_1} \mathbb{1}_{B_1 \geq 1} \ ,$$

以及 k_i 对于 $i \in [B_1]$ 的值表示满足 $Z_{k_i} = 1$ 的所有索引。应用引理 3，(3) 得：

$$W_n \stackrel{d}{=} \tilde{W}_n = \sum_{j=1}^{N} T_j + \sum_{j=1}^{N-1} V_j^{(0)} + V_1^{(1)} \ , \quad (30)$$

其中 $T_j \stackrel{iid}{\sim} T_C$，$V_j^{(l)} \stackrel{iid}{\sim} \sum_{i=1}^{n} X_i | U=l$，对于 $l \in \{0,1\}$，$j \in \mathbb{N}$，以及 $N \sim \text{Geo}(\mathsf{P}(U=1))$。

现在，考虑一次 BB84 试验，令 N_S 和 N_F 分别表示在抽取的量子比特中，成功传送的量子比特数和发生故障的量子比特数，即

$$N_S = \sum_{i=1}^{B_1} Y_{k_i} \ , \quad N_F = \sum_{i=1}^{B_1} (1 - Y_{k_i}) \ .$$

以下结果给出了模拟 $V_j^{(0)}$ 和 $V_j^{(1)}$ 的一种方法。

命题 3. 令 $(N_S^{(l)}, N_F^{(l)}) \sim (N_S, N_F) | U = l$ 对于 $l \in \{0,1\}$。则，

$$V_j^{(l)} \stackrel{d}{=} \tilde{V}_l = \sum_{i=1}^{N_S^{(l)}} X_i^{(1)} + \sum_{i=1}^{N_F^{(l)}} X_i^{(0)} + \sum_{i=1}^{n-N_S^{(l)}-N_F^{(l)}} X_i \ ,$$

其中，$X_j^{(l)} \stackrel{iid}{\sim} X_1 | Y = l$、$l \in \{0,1\}$ 以及右侧的所有求和项均彼此独立抽取，并且也与 $(N_S^{(l)}, N_F^{(l)})$ 相互独立。

Proof. See Sect. VI-A. □

现在，只要能够模拟 (i) 协议运行次数 N，(ii) 一次试验中量子隐形传态成功和故障的条件计数 $(N_S, N_F)|U$，以及 (iii) 单量子比特传送的持续时间，我们就可以结合命题 3 使用 (30) 来模拟 W_n，即协议的完成时间。

分布为 X、$X|Y=1$ 和 $X|Y=0$。为了模拟 N，我们观察到

$$\begin{aligned} &P(U=1) \\ &= \sum_{k=1}^{\lceil \alpha n \rceil} \mathsf{P}\left(\sum_{j=1}^{k} Y_{i_j} \geq \beta k \right) \mathsf{P}(B_1 = k) \\ &= \sum_{k=1}^{\lceil \alpha n \rceil} \mathsf{P}\Big(\text{Bin}(k, m_1(0)) \geq \beta k\Big) \frac{1}{2^n} \sum_{\frac{k-1}{\alpha} < j \leq \frac{k}{\alpha}} \binom{n}{j}, \end{aligned}$$

其中我们利用了 Y_i服从参数为 $= m_1(0)$的独立同分布伯努利分布这一事实。记$P(U=1) = p_1$，

$$\begin{aligned} &\mathsf{P}(N_S = s, N_F = f | U = 0) \\ &= (1 - \mathbb{1}_{\frac{s}{s+f} \geq \beta}) \, \mathsf{P}\Big(\text{Bin}(s+f, m_1(0)) = s\Big) \\ &\quad \frac{1}{2^n} \sum_{\frac{s+f-1}{\alpha} < j \leq \frac{s+f}{\alpha}} \binom{n}{j} \quad (1-p_1)^{-1}. \end{aligned} \quad (31)$$

同样，

$$\begin{aligned} &\mathsf{P}(N_S = s, N_F = f | U = 1) \\ &= \mathsf{P}(N_S = s, N_F = f, U = 1) p_1^{-1} \\ &= \mathbb{1}_{\frac{s}{s+f} \geq \beta} \, \mathsf{P}\Big(\text{Bin}(s+f, m_1(0)) = s\Big) \\ &\quad \frac{1}{2^n} \sum_{\frac{s+f-1}{\alpha} < j \leq \frac{s+f}{\alpha}} \binom{n}{j} \quad p_1^{-1} \ . \end{aligned} \quad (32)$$

最后，我们需要一种方法来从单量子比特传送时间的分布中进行模拟：X、$X|Y=1$ 和 $X|Y=0$。我们采用矩估计法，使用三个移位 Coxian 相位型分布对其进行近似。需要注意的是，量子比特隐形传态时间的矩可以利用 (8) 和 (10) 计算得到。这些方程还有助于我们确定移位量，结果表明，三个分布的移位量均为 $a_W = a_{\text{gen}} + a_{\text{com}} + a_{\text{swap}} + a_{\text{AB}}$。由于具有 d 个阶段的 Coxian 相位型分布包含 $(2d-1)$ 个参数，因此我们可以将前 $(2d-1)$ 阶矩表示为这些参数的函数，并通过令其等于由 (8) 和 (10) 得到的矩来求解这些参数。需要注意的是，分布拟合只需执行一次，其结果可在后续模拟实验中重复使用。

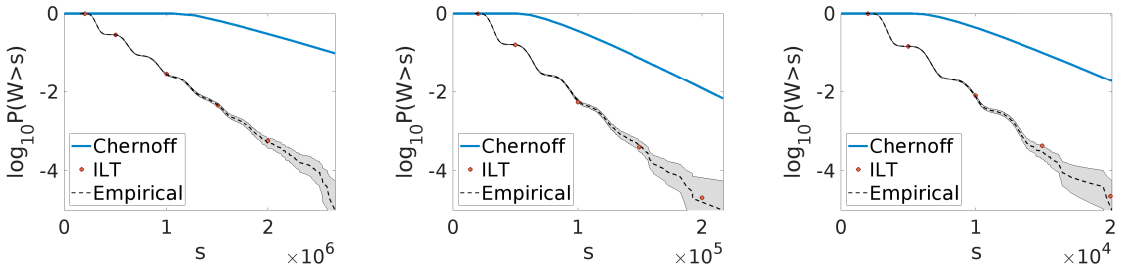
算法 1： BB84 协议完成时间的合成仿真 **数据：** $n \in \mathbb{N}$, $\alpha > 0$, $\beta > 0$, $a_{\text{gen}} > 0$,$a_{\text{com}} > 0$, $a_{\text{swap}} > 0$, $a_{\text{AB}} > 0$, $\lambda_{\text{gen}} > 0$,$\lambda_{\text{com}} > 0$, $\lambda_{\text{swap}} > 0$, $\lambda_{\text{AB}} > 0$,$0 < p_{\text{gen}} < 1$, $0 < p_{\text{swap}} < 1$, $t_c > 0$,$t_{de} > 0$ $t_{da} > 0$ $d \in \mathbb{N}$, , . **结果：** a_{gen}, 预处理： $a_{\text{swap}} + a_{\text{AB}}$ $p_1 \leftarrow \sum_{k=1}^{\lceil \alpha n \rceil}$ $k\ m_1\ 0 \geq$ P(Bin(, ( )) βk) $\frac{1}{2^n} \sum_{\frac{k-1}{\alpha} < j \leq \frac{k}{\alpha}} \binom{n}{j}$ ； 通过矩匹配估计 $(\lambda_1^{(1)}, \ldots, \lambda_d^{(1)}, q_1^{(1)}, \ldots, q_{d-1}^{(1)})$，用于$X|Y = 1$；通过矩匹配估计 $(\lambda_1^{(0)}, \ldots, \lambda_d^{(0)}, q_1^{(0)}, \ldots, q_{d-1}^{(0)})$，用于$X|Y = 0$；通过矩匹配估计 $(\lambda_1^{(u)}, \ldots, \lambda_d^{(u)}, q_1^{(u)}, \ldots, q_{d-1}^{(u)})$，用于 X；仿真：抽取 $N \sim$ Geo(p_1)；根据 (32) 抽取 (S_0, F_0)；对于 $i = 1:$ $N - 1$ 执行 抽取 (S_i, F_i)，根据 (31)；结束 $S \leftarrow \sum_{j=0}^{N-1} S_i$；$F \leftarrow \sum_{j=0}^{N-1} F_i$；$N \leftarrow nN - S - F$；$A_0 \leftarrow S$；抽取 $W_A^{(0)} \sim$ Gamma($A_0, \lambda_1^{(1)}$)；$B_0 \leftarrow F$；抽取 $W_B^{(0)} \sim$ Gamma($B_0, \lambda_1^{(0)}$)；$C_0 \leftarrow N$；抽取 $W_C^{(0)} \sim$ Gamma($C_0, \lambda_1^{(u)}$)；对于 $i = 1:$ $d - 1$ 执行 抽取 $A_i \sim$ Bin($A_{i-1}, q_i^{(1)}$)；抽取 $W_A^{(i)} \sim$ Gamma($A_i, \lambda_{i+1}^{(1)}$)；抽取 $B_i \sim$ Bin($B_{i-1}, q_i^{(0)}$)；抽取 $W_B^{(i)} \sim$ Gamma($B_i, \lambda_{i+1}^{(0)}$)；抽取 $C_i \sim$ Bin($C_{i-1}, q_i^{(u)}$)；抽取 $W_C^{(i)} \sim$ Gamma($C_i, \lambda_{i+1}^{(u)}$)；结束 抽取 $C \sim$ $N\ \lambda_{AB}$ $W_n \leftarrow N a_{AB} + C + n N a_W + \sum_{i=0}^{d-1} W_A^{\,i} + W_B^{(i)} + W_C^{\,i}$. Gamma(,) (( ) ( ))

选择 Coxian 相位型分布，是因为其独立同分布随机变量之和可以用紧凑形式表示，因此能够高效模拟。请注意，参数为 $(\lambda_1, \ldots, \lambda_d, q_1, \ldots, q_{d-1})$ 的 k 个独立同分布 Coxian 相位型随机变量之和服从 $\sum_{l=1}^{d}$ 伽马分布(D_l, λ_l)，其中 D_l ∼服从 D_{l-1}, q_{l-1} 的二项分布，适用于 $l \geq 2$ 和 $D_1 = k$。我们的方法之所以高效，是因为平均每次观测只需模拟 ($2d+1+\frac{2}{p_1}$) 个随机变量，而全规模方法则需要 ($\frac{1}{1-(1-p_{\text{gen}})^{()}}$ $+1$ ((— $\sqrt{2+4(1-p_{\text{gen}})^{()}}$) $\frac{1}{p_{\text{swap}}} + 1$)) $\frac{1}{p_1}$ 个。回顾一下，$p_1 =$P ($U \equiv 1$) 表示中继器处可观测的贝尔态测量故障概率，$(1 - p_{\text{swap}})$，而 p_{gen} 表示链路级纠缠生成的成功概率。

完整的仿真方案已在算法 1 中形式化。我们还将我们的方法与基于 10^6 观测数据的全规模仿真进行了比较：(i) 图 4 对比了两种方法的输出直方图；(ii) 图 5 展示了这些输出的 QQ 图。在合成方法中，我们采用具有 7 个阶段的 Coxian 阶段型分布，因为它们的拟合效果相当理想。仿真所用参数的完整列表见第 V 节。

V. 数值评估

在本节中，我们通过数值计算评估前文第 II 节推导的累积分布函数估计和尾部界。图中的时间单位为平均链路级纠缠生成时间。对于 BB84 协议的完成时间，我们首先运行全规模仿真，并将界限/估计值与经验互补累积分布函数进行比较。图 3 展示了纠缠生成概率 $\{10^{-1}, 10^{-2}, 10^{-3}\}$ 取三个不同值时的比较结果，以反映不同的硬件效率水平。在实验中，我们假设 LINK-GEN、链路通信和交换通信阶段服从 SE($_{1\,2}$, 2) 分布，即 $a_{\text{gen}} = a_{\text{com}} = a_{\text{swap}} = \frac{1}{2}$ 和 $\lambda_{\text{gen}} = \lambda_{\text{com}} = \lambda_{\text{swap}} = 2$；而传输通信和协调通信阶段假设服从 SE(1, 1) 分布，即 $a_{\text{AB}} = 1$ 和 $\lambda_{\text{AB}} = 1$。新链路的 Werner 参数



(a) $p_{\text{gen}} = 10^{-3}$ (b) $p_{\text{gen}} = 10^{-2}$ (c) $p_{\text{gen}} = 10^{-1}$

图 3：通过拉普拉斯逆变换（“ILT”）和 Chernoff 界（“Chernoff”）得到的累积分布函数数值估计，与 BB84 协议 $n = 50$ 个量子比特的完成时间（W_n）的经验尾概率（“Empirical”）对比；阴影区域表示根据 [16，定理 2.4] 计算的互补累积分布函数的 95% 置信区间。经验分布通过运行全规模仿真获得；仿真的参数完整列表见第 V 节。时间单位：平均链路级纠缠生成时间。

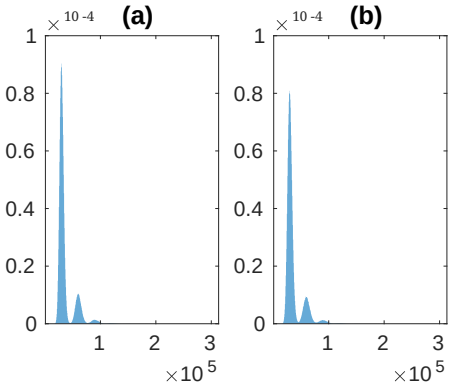


图 4：协议完成时间 W_n 的经验密度比较，分别来自（**a**）全规模仿真和（**b**）合成仿真。参数：$n = 50$ 个量子比特；链路生成成功概率 $p_{\text{gen}} = 10^{-2}$；其他参数见第 V 节。

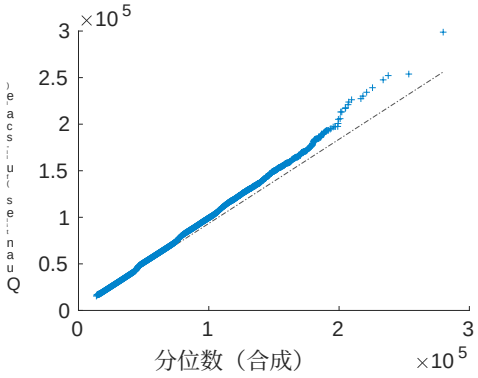


图 5：采用全规模仿真和合成仿真得到的协议完成时间的 Q-Q 图；实验设置与图 4 相同。

假设为 $w_0 = 0.98$。此外，表征存储器退相干的常数取为$t_c = t_{de} = t_{da} = 4 \times 10^4$。我们对 $n = 50$ 个量子比特运行 BB84 协议，同时选择具有相同测量基的量子比特中的 $\alpha = 30\%$ 用于协调。如果我们至少抽取一个量子比特用于协调，则认为协议成功

并且在至少$\beta = 95\%$的情况下，测量结果是一致的。在图 3 所示的结果图中，我们可以看到，对于采样点，我们对累积分布函数（CDF）的估计与经验累积分布函数非常吻合。

接下来，我们将在第 IV 节展示仿真方案的有效性。我们比较了采用该方案生成的协议完成时间与全规模仿真所得结果；全规模仿真针对纠缠生成概率为10^{-2} 的系统进行，其他因素则与图 3 中相同。

我们在图 4 中比较了由此得到的经验密度，并在图 5 中展示了 Q-Q 图。我们观察到这两种方法的结果吻合良好。

VI. 结论

在本研究中，我们对 BB84 协议的完成时间进行了性能分析。我们的设置假设发送方和接收方通过单个量子中继器连接，且两者之间的量子信道中不存在窃听。不过，为了反映当前的量子硬件标准，我们考虑了传送阶段中每个单独阶段发生故障的可能性，并将由此产生的退相干对协议性能的影响纳入考量。随后，我们提供了一种计算完成时间的矩母函数（MGF）的方法，据此可以通过拉普拉斯逆变换估算累积分布函数（CDF），并为相应的尾概率计算数值上界。基于对各个阶段持续时间分布所作的若干假设，我们还提出了一种高效的完成时间仿真方案。该仿真方案基于这样一种思路：单量子比特传送时间可以用 Coxian 相位型分布进行良好近似，并可通过高效聚合该分布得到整个协议的完成时间。

附录

A. 延后证明

命题 *2* 的证明。对于 $t \leq 0$,

$$e^{t \max_{i\in[n]} T_i} p_\theta(\mathbf{L}_1) \leq e^{tT_1} \ .$$

同理，对于 $t > 0$,

$$e^{t \max_{i\in[n]} T_i} p_\theta(\mathbf{L}_1) \leq e^{t \sum_{j=1}^n T_j} \ .$$

由于 $M_{T_C}(t) \geq 0$，对于 $t \in \mathbb{R}$，我们有：

$$\begin{aligned} &M_{T_C}(t)\mathsf{E}\left(e^{t \max_{i\in[n]} T_i} p_\theta(\mathbf{L}_1)\right) \\ \leq &M_{T_C}(t) \max\left\{\mathsf{E}(e^{tT_1}), \prod_{j=1}^n \mathsf{E}(e^{tT_j})\right\} \ . \end{aligned}$$

右端在 $\bigcap_{l\in[n]\cup\{c\}} I_l$ 上有限。(13) 式右端的分母也同样如此。

此外，(13) 式第二行的无穷和在 I_0 上收敛，从而证明了该结论。 □

命题 *3* 的证明。回顾一下，如果一个随机变量的矩母函数在零点邻域内存在，则该随机变量是次指数型的。因此，根据假设，只需证明 I_0 非空。对于 $t_1 < t_2$ 和 $t_1,\ t_2 \in \cap_{i\in[n]\cup\{C\}} I_l$,

$$\begin{aligned} &G(t_2) - G(t_1) \\ =&\mathsf{E}\left((e^{t_2 X_1} - e^{t_1 X_1})(1 - p_\theta(\mathbf{L}_1))\right) \\ \leq&\mathsf{E}(e^{t_2 X_1}) - \mathsf{E}(e^{t_1 X_1}) \ . \end{aligned}$$

因此，X_1 的矩母函数在 $\cap_{i\in[n]\cup\{C\}} I_l$中的连续性意味着 G的连续性。此外，除去平凡情形 $p_\theta(\mathbf{L}_1) \equiv 0$，$G(0) = \mathsf{E}(1 - p_\theta(\mathbf{L}_1)) < 1$。由于$G$是连续的，因此 I_0 非空，这正是我们所要证明的。 □

引理 *3* 的证明。记 $p_l = P(Y = l)$ 和 $\phi_l(t) = \mathsf{E}\left(e^{tX_1^{(l)}}\right) = \mathsf{E}\left(e^{tX} \mathbb{1}_{Y=l}\right)/p_l$ 对于 $l \in \{0, 1\}$,

$$\begin{aligned} &\mathsf{E}\left(e^{t\tilde{W}}\right) \\ =&M_{T_C}(t)\phi_1(t) \sum_{j=0}^{\infty} p_0^j p_1 (M_{T_C}(t)\phi_0(t))^j \\ =&\frac{p_1 M_{T_C}(t)\phi_1(t)}{1 - p_0 M_{T_C}(t)\phi_0(t)} \\ =&\mathsf{E}\left(e^{tW}\right) \ . \end{aligned}$$

按照推论 3 的论证，$\tilde{W}$和 W 的矩母函数在零点邻域内存在，这意味着 $W \stackrel{d}{=} \tilde{W}$。

□

命题 *3* 的证明。注意到

$$
\begin{aligned}
&\mathsf{E}\Big(e^{tV_j^{(l)}}\Big)\\
=&\mathsf{E}\Big(e^{t\sum_1^n X_i}|U=l\Big)\\
=&\sum_{k,d}\mathsf{E}\big(e^{t\sum_1^n X_i}|\sum_1^n Y_iZ_i=k,\sum_1^n Z_i=d,U=l\big)\\
&\quad\mathsf{P}\big(\sum_1^n Y_iZ_i=k,\sum_1^n Z_i=d|U=l\big)\\
=&\sum_{k,d}\mathsf{E}\big(e^{t\sum_1^n X_i}|\sum_1^n Y_iZ_i=k,\sum_1^n Z_i=d\big)\\
&\quad\mathsf{P}\big(\sum_1^n Y_iZ_i=k,\sum_1^n Z_i=d|U=l\big)\ ,
\end{aligned}
$$

其中，最后一个等式根据 U 的定义得出。现在，对于 $X\sim X_1$ 和 $Y\sim Y_1$,

$$
\begin{aligned}
&\mathsf{E}\big(e^{t\sum_1^n X_i}|\sum_1^n Y_iZ_i=k,\sum_1^n Z_i=d\big)\\
=&\sum_{r=k}^{k+n-d}\mathsf{E}\big(e^{t\sum_1^n X_i}|\sum_1^n Y_i=r,\sum_1^n Y_iZ_i=k,\\
&\quad\sum_1^n Z_i=d\big)\mathsf{P}\big(\sum_1^n Y_i=r|\sum_1^n Y_iZ_i=k,\\
&\quad\sum_1^n Z_i=d\big)\\
=&\sum_{r=k}^{k+n-d}\mathsf{E}\big(e^{t\sum_1^n X_i}|\sum_1^n Y_i=r\big)\\
&\quad\mathsf{P}\big(\sum_1^n Y_i=r|\sum_1^n Y_iZ_i=k,\sum_1^n Z_i=d\big)\\
=&\mathsf{E}^k\big(e^{tX}|Y=1\big)\mathsf{E}^{d-k}\big(e^{tX}|Y=0\big)\\
&\quad\sum_{r=0}^{n-d}\binom{n-d}{r}\mathsf{E}^r\big(e^{tX}|Y=1\big)(\mathsf{P}\left(Y=1\right))^r\\
&\quad\mathsf{E}^{n-d-r}\big(e^{tX}|Y=0\big)(\mathsf{P}\left(Y=0\right))^{n-d-r}\\
=&\mathsf{E}^k\big(e^{tX}|Y=1\big)\mathsf{E}^{d-k}\big(e^{tX}|Y=0\big)\mathsf{E}^{n-d}\big(e^{tX}\big).
\end{aligned}
$$

因此，

$$
\begin{aligned}
&\mathsf{E}\Big(e^{tV_j^{(l)}}\Big)\\
=&\sum_{k,d}\mathsf{E}^k\big(e^{tX}|Y=1\big)\mathsf{E}^{d-k}\big(e^{tX}|Y=0\big)\\
&\quad\mathsf{E}^{n-d}\big(e^{tX}\big)\mathsf{P}\big(\sum_1^n Y_iZ_i=k,\sum_1^n Z_i=d|U=l\big)\\
=&\sum_{k,d}\mathsf{E}^k\big(e^{tX}|Y=1\big)\mathsf{E}^{d}\big(e^{tX}|Y=0\big)\\
&\quad\mathsf{E}^{n-d-k}\big(e^{tX}\big)\mathsf{P}\big(N_S=k,N_F=d|U=l\big)\ ,
\end{aligned}
$$

which establishes $V_j^{(l)}\overset{d}{=}\tilde{V}_l$ for $l\in\{0,1\}$. □

参考文献

[1] Van Meter, R.，《量子网络》，John Wiley & Sons, 2014 年。[2] Munro, W.J.、Azuma, K.、Tamaki, K. 和 Nemoto, K.，《量子中继器内部》，IEEE《量子电子学精选主题期刊》，21(3)，第 78-90 页，2015 年。[3] Brand, S.、Coopmans, T. 和 Elkouss, D.，《量子中继链中等待时间和保真度的高效计算》，IEEE《通信领域精选期刊》，38(3)，第 619-639 页，2020 年。[4] Li, B.、Coopmans, T. 和 Elkouss, D.，《量子中继链中截断参数的高效优化》，载于 2020 年 IEEE 国际量子计算与工程会议（QCE）论文集，第 158-168 页，2020 年。[5] Coopmans, T.、Brand, S. 和 Elkouss, D.，《远距离纠缠交付时间的改进解析界》，《物理评论 A》，第 105 卷，第 1 期，第 012608 页，2022 年。[6] Bennett C.H. 和 Brassard G.，《量子密码学：公钥分发与抛硬币》，国际计算机、系统与信号处理会议，第 175-179 页，1984 年。[7] Bahadur, R.R. 和 Ranga Rao, R.，《关于样本均值的偏差》，《数理统计年刊》，31(4)，第 1015-1027 页，1960 年。[8] Qiao, H. 和 Chen, X.Y.，《退极化信道中的 BB84 量子密钥分发仿真》，载于第 14 届青年通信会议论文集，第 123-129 页，2009 年。[9] Sahoo, J.R. 和 Satapathy, S.，《通过模型检验对 BB84 协议进行仿真与分析》，《国际工程科学与技术期刊》（IJEST），3(7)，2011 年。[10] Halip, N.H.M.、Mokhtar, M. 和 Buhari, A.，《对 Bennet 和 Brassard 84 协议及 Eve 攻击的仿真》，载于 2014 年 IEEE 第五届光子学国际会议（ICP）论文集，第 29-31 页。IEEE，2014 年。[11] Jasim, O.K.、Abbas, S.、El-Horbaty, E.S.M. 和 Salem, A.B.M.，《量子密钥分发：仿真与特性分析》，《计算机科学 Procedia》，65，第 701-710 页，2015 年。[12] Mina, M.Z. 和 Simion, E.，《涉及窃听的可扩展 BB84 协议仿真》，载于《信息技术与通信创新安全解决方案：第 13 届国际会议 SecITC》，布加勒斯特，

罗马尼亚，11月19日至20日，修订精选论文 13（第91-109页）。Springer International Publishing，2021年。[13] Werner, R.F.，《具有爱因斯坦-波多尔斯基-罗森关联且允许隐变量模型的量子态》，Physical Review A，40(8)，第4277页，1989年。[14] Nielsen, M.A. 和 Chuang, I.，《量子计算与量子信息》，2002年。[15] Vardoyan, G.、Skrzypczyk, M. 和 Wehner, S.，《关于这项……》

量子性能评估：两种分布式量子架构”，《ACM SIGMETRICS 性能评估评论》，49(3)，第 30–31 页，2022 年。[16] Le Boudec, J.Y.，《计算机与通信系统性能评估》，EPFL 出版社，2010 年。