Simulations of Photonic Quantum Networks for Performance Analysis and Experiment Design

Xiaoliang Wu*†, Joaquin Chung*, Alexander Kolar*‡, Eugene Wang*,
Tian Zhong§, Rajkumar Kettimuthu*, Martin Suchara*
*Argonne National Laboratory, Lemont, IL. USA, †Illinois Institute of Technology, Chicago, IL, USA,
‡Northwestern University, Evanston, IL, USA, §University of Chicago, Chicago, IL, USA

***Abstract*—This work models metropolitan-scale photonic quantum networks that use time bin encoding for quantum key distribution and quantum state teleportation. We develop and validate theoretical models by comparing them with prior experimental results. We use our newly developed simulator of quantum network communication, called SeQUeNCe, to perform simulations at the individual photon level with picosecond resolution. The simulator integrates accurate models of optical components including light sources, interferometers, detectors, beam splitters, and telecommunication fiber, allowing studies of their complex interactions. Optical quantum networks have been generating significant interest because of their ability to provide secure communication, enable new functionality such as clock synchronization with unprecedented accuracy, and reduce the communication complexity of certain distributed computing problems. In the past few years experimental demonstrations moved from table-top experiments to metropolitan-scale deployments and long-distance repeater network prototypes. As the number of optical components in these experiments increases, simulation tools such as SeQUeNCe will simplify experiment planning and accelerate designs of new network protocols. The modular design of our tool will also allow modeling future technologies such as network nodes with quantum memories and quantum transducers as they become available.**

I. Introduction

Quantum communication networks promise to revolutionize our lives by enabling new applications. Although the best known applications are in security [1]–[4], quantum networks will also allow fundamental advances in fields such as distributed computing, sensing, and metrology. For example, quantum communication allows solving some distributed computational tasks with exponential reduction in communication complexity [5] where the use of classical communication would require transmission of an exponentially larger number of bits to solve the same problem. Quantum networks can be also used to synchronize clocks with unprecedented accuracy [6], and connect quantum sensors to detect earthquakes or locate natural resources more efficiently [7].

The urgency to build quantum networks has been fueled by recent advances in manufacturing quantum computer prototypes with increasing number of qubits [8]–[10]. Once built, quantum computers can use Shor's factoring algorithm [11] to break all major cryptosystems used for public key encryption, digital signatures, and key establishment. This problem is recognized by governments worldwide; NSA recently announced [12] its intent to discontinue the use of RSA, DH and DSA protocols for classified information. The possible solutions are to either develop new quantum-resistant public-key cryptographic algorithms [13] or use quantum networks for quantum key distribution (QKD) [1], [14] in conjunction with private-key cryptography.

Recent breakthroughs in quantum photonics enable experimental realizations of long-distance quantum communication networks. Development of superconducting nanowire single-photon detectors (SNSPDs) [15] that use new materials and packaging improved detection efficiency above 90% and reduced dark counts below 100 counts per second [16]. Other recent advances include, for example, fast counting electronics that allows transfer of single photon triggered electrical pulses at rates in excess of 100 MHz [17], [18].

Several experimental efforts that aim to build long-distance photonic quantum networks with increasing complexity are underway. These include a 30-mile optical fiber link connecting Argonne and Fermilab to test long-distance communication [19]; FQNET, an onsite teleportation and entanglement experiment at Fermilab [20]; a 2,000-kilometer-long fiber-optic link between Beijing and Shanghai [21]; and projects in the Netherlands [22], the United Kingdom [23], and South Korea [24]. As the size of these experimental networks increases and new technologies are developed, there is an increased need to model the behavior and interactions of these complex systems, and to predict experiment results before they are realized.

Our work builds a Simulator of QUantum Network Communication (SeQUeNCe) that models quantum hardware and network protocols and simulates transmission of individual photon pulses and control messages with picosecond accuracy. SeQUeNCe can be used to quantify network scalability and performance, perform hardware and software parameter tuning, and aid with experiment planning and design. Our simulator supports both polarization encoding and time bin encoding [25] of quantum information. We focus primarily on time bin encoding due to its robustness against decoherence, making it ideally suited for long-distance quantum communication.

We simulate QKD and teleportation networks and compare our results with experiments. Our simulation of raw key bit

This material is based upon work supported by Laboratory Directed Research and Development (LDRD) funding from Argonne National Laboratory, provided by the Director, Office of Science, of the U.S. Department of Energy under contract DE-AC02-06CH11357.

error rate, key throughput, and latency matches the results reported in an experiment that constructed a QKD network in laboratory conditions with varying fiber length of up to 120 km [26]. We also faithfully model a real-world deployment of a metropolitan quantum teleportation network [27].

This work makes the following contributions:

- we build and demonstrate the use of a quantum network simulator that tracks individual photons with picosecond resolution;
- we provide accurate models of optical components such as light sources, interferometers, detectors, and beam splitters;
- we develop suitable simulation models for time bin encoded quantum information;
- we implement the BB84 [1], Cascade [28], and quantum teleportation [29] protocols;
- and we compare our simulation results against experimental realizations of QKD [26] and teleportation [27].

In the past, simulations were used to perform numeric studies of quantum network algorithms and protocols in isolation [30]–[34] or focused on quantum network applications [35]. Two recently developed simulators, NetSquid [36] and our SeQUeNCe, allow comprehensive modeling of quantum hardware, quantum network protocols, and studies of their interaction. The modular design of the simulators allows adding models of new hardware and software as they become available.

Section II provides background on quantum communication, QKD and quantum teleportation. Readers familiar with these concepts can proceed directly to Section III, which describes the optical components we model and their parameters. Simulation setup and results of QKD are described in Section IV, and the setup and results for quantum state teleportation are in Section V. Section VI summarizes our work and outlines future directions.

II. Background: Quantum Communication

The development of quantum physics has opened up new opportunities in many well-established fields such as communication, cryptography, and metrology. Quantum entanglement, a quantum state of two or more objects that are correlated in such a way that they cannot be described by factorizable individual states, is the foundation for many new applications in these fields. Superposition of quantum states can be experimentally realized by entangling various physical properties of a quantum object, such as an atom, an ion, or a photon. Among all the physical systems suitable for implementing quantum information processing, the photon is an unbeatable choice for long-distance transmission of quantum information because of its limited interaction with the environment and other photons. To date, photonic entanglement has been demonstrated in many degrees of freedom, such as polarization, momentum, frequency, and time-bin encoding. It has been extensively used for testing the validity of quantum mechanics, superdense encoding of classical information [37], [38], and the security limits of today's quantum key distribution (QKD) technology [38]–[40].

QKD [1] and quantum state teleportation [29] are the two best known applications for quantum communication networks. QKD is used to create a secret shared key for secure communication with an insecure classic channel. Quantum teleportation allows quantum information, which cannot be extracted to classic bits, to be transferred from one quantum particle to another particle.

A. Quantum Key Distribution

QKD is a technique for secure distribution of keys to be used for encrypting and decrypting messages that allows the two communicating parties to detect the presence of any eavesdropper. This is an important and unique property that results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. Any third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented that detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure; otherwise, no secure key is possible and communication is aborted. The security of QKD is guaranteed by the laws of quantum mechanics, in contrast to traditional key distribution protocols that rely on the assumption that certain problems are computationally difficult.

The most well-known QKD technique was proposed by Charles H. Bennett and Gilles Brassard in 1984, describing a protocol that would come to be known as BB84 [1]. The sender (Alice) and the receiver (Bob) are connected by a quantum communication channel which allows quantum states to be transmitted. In addition, they communicate via a public classical channel. The security of the protocol comes from encoding the information in non-orthogonal states or conjugate states. Any two pairs of conjugate states, and the two states within a pair orthogonal to each other, can be used for BB84 protocol. Quantum mechanics ensures that these states cannot in general be measured without disturbing the measurement result on the other conjugate states.

In BB84, Alice first prepares her photon randomly in one of the two orthogonal quantum states in either basis to denote a bit 0 or 1. Then she randomly selects one of her two conjugate basis to send the photon to Bob. Bob randomly decides on which one of the conjugate basis he measures the photon from Alice, and he records the measurement result. After Alice and Bob repeat the above procedure for all the bits they communicate, they announce over the public channel their choices of basis for sending and measuring the bit. Alice and Bob both discard bits where they did not use the same basis, which is half on average, leaving the other half as sifted keys.

To check for the presence of an adversary (Eve) eavesdropping on the communication, Alice and Bob compare a certain

subset of their remaining bit strings. If Eve has gained any information about the photons' polarization, this introduces errors in Bob's measurements. If more than a certain percentage of bits differ, they abort the key and try again. The percentage of error is chosen so that if the number of bits known to Eve is less than this value, privacy amplification [41] can be used to reduce Eve's knowledge of the key to an arbitrarily small amount.

B. Quantum State Teleportation

Utilizing quantum entanglement shared between two physically separate parties, an arbitrary quantum state or a qubit can be faithfully transferred from one party to the other. This process is known as quantum state teleportation [29], and is depicted in Figure 1. Specifically, one physical implementation involves the generation of polarization or time-bin photonic entanglement (which is most suitable for fiber-based communication) using spontaneous parametric down-conversion in a nonlinear crystal. One qubit of the entangled state then undergoes a joint measurement with a single photonic qubit encoded into a weak coherent state, resulting in the destruction of the single qubit and its recreation in place of the remaining, formerly entangled, qubit. By sending the entangled state over a fiber or free-space optical link, teleportation of a qubit can be achieved even though no quantum information is physically transmitted through the channel. The fidelity of the teleportation protocol, measured by comparing the final teleported qubit with the original one, will depend on the quality of the entanglement and any error induced during the joint measurement. To date, quantum teleportation has been successfully demonstrated in experiments in laboratory settings as well as in real-world fiber-optic [27] and free-space satellite links [42]. The distance of teleportation has also reached up to 143 km using free-space telescopes [43]. Quantum teleportation still remains a key component of complex quantum networking protocols, including entanglement swapping and quantum repeaters.

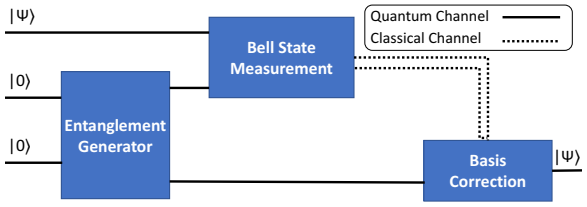


Fig. 1: Teleportation of quantum state $|\Psi\rangle$

III. Modeling Photonic Quantum Networks

Here we describe how our simulator models the behavior of optical components, and tracks transmission of individual photons and the associated quantum states. Our tool allows the user to configure the parameters of each simulation to closely model the behavior of experimental setups, and the modular design allows easy implementation and testing of new hardware and software components.

A. Modeling Optical Components

Time-bin-based QKD and quantum state teleportation uses attenuated laser pulses at telecom wavelengths; optical fiber for quantum and classical communication; single-photon detectors capable of accurately recording photon arrival times; and a variety of optical components that allow creation of entangled photon pairs, photon splitting, and interference. SeQUeNCe models these optical components as follows.

Light source is a pulsed laser that generates attenuated pulses at telecom wavelengths with frequency f. The light source can generate photons in an arbitrary quantum state, and the number of emitted photons in each pulse follows a Poisson distribution with mean photon number μ. The time-bin [25] qubit state is represented by $|\psi\rangle = \alpha|e\rangle + \beta e^{i\phi}|l\rangle$, where $|e\rangle$ and $|l\rangle$ denote early and late temporal modes, respectively; ϕ is a phase-factor; and α and β are real numbers. When a photon with quantum state $|\psi\rangle = \alpha|e\rangle + \beta e^{i\phi}|l\rangle$ is measured, it is found in the early time-bin with probability $|\alpha|^2$ or the late time-bin with probability $|\beta e^{i\phi}|^2$. Thus, α and β satisfy $\alpha^2 + \beta^2 = 1$.

Spontaneous parametric down-conversion (SPDC) is a photon pair source that converts high-energy photons into pairs of entangled, lower energy photons. In a commonly used apparatus, a strong pump beam with frequency f_{SPDC} is directed at a nonlinear optical crystal. Most of the photons continue through the crystal, but some undergo a down-conversion, producing entangled photons. The number of entangled pairs per pulse follows a Poisson distribution with mean μ_{SPDC}. The time-bin entangled photons are generated in the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|e\rangle|e\rangle + |l\rangle|l\rangle)$

Quantum channel (QC) is an optical fiber used to transmit photons encoding quantum states. We model the propagation time of the photons in the channel as $\frac{L}{c^*}$, where L denotes the length of fiber and c^* denotes the speed of light in the fiber. The loss rate of a quantum channel is $10^{-\frac{L\cdot\alpha_o}{10}}$, where α_o is the attenuation measured in dB/km.

Classical channel (CC) is an optical fiber used for classical communication. In a typical setup separate optical fiber is used for the quantum and classical channels. We use the same propagation delay model for the quantum and classical channel. For simplicity, we assume no loss and perfect reliability of the classical channel. Constant delay is added to the classical communication to model transmission delay, queuing delay, and processing delay.

Single-Photon Detector (SPD) is able to detect individual photons and specify their arrival times. An SPD generates an electrical signal upon absorption of each photon. The detector efficiency η is the probability that a photon is successfully detected each time it hits the detector. After absorption of each photon, the detector must cool down for a constant time before it can detect the subsequent photon. This "dead time" is the inverse of the count rate. Another property of the SPD is the "dark count" rate, giving the average number of false positive detections per second caused by stray photons and electrical noise. We model dark count events as a Poisson process.

Beam splitter (BS) splits an incident beam of photons to one of two paths. A polarizing beam splitter separates the photons based on polarization, whereas a non-polarizing beam splitter either transmits or reflects the photons with a given probability. In our simulation, we use a transmission probability of 50% for non-polarizing beam splitters (denoted as a 50/50 beam splitter). After passing the 50/50 beam splitter, the quantum states of the photons remain unchanged.

Mach-Zehnder interferometer (MZI) is used to measure relative phase between states in superposition. An MZI consists of a 50/50 BS and a coupler (itself a 50/50 BS), as shown in Figure 2. There are two paths of different lengths between the BS and the coupler. The path length difference can be adjusted to change the delay difference of the two paths. The additional delay on the longer path must be equal to the separation of the time-bins and longer than the coherence length of the photon to achieve a time-bin measurement. This delay ensures that the two time-bins arrive at the same time at the coupler, resulting in measurable interference. A phase modulator is also placed on the longer path (not shown in the figure). By changing the phase modulator, the photon quantum state can be measured in the X-basis $\{|\pm\rangle = \frac{|e\rangle \pm |l\rangle}{\sqrt{2}}\}$ or Y-basis $\{|\pm i\rangle = \frac{|e\rangle \pm i|l\rangle}{\sqrt{2}}\}$.

Bell state measurement (BSM) measures the quantum state of two photons. A BSM of time-bin states consists of a 50/50 BS and two SPDs. A complete BSM projects the quantum state of any two-photon state deterministically and unambiguously onto one of the four maximally entangled Bell states. However, building a complete BSM using linear optics is impossible without auxiliary photons [44]. Our BSM design can distinguish only two Bell states:

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|e\rangle|l\rangle + |l\rangle|e\rangle)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|e\rangle|l\rangle - |l\rangle|e\rangle)$$

this is done through the use of a 50/50 BS to ensure the incident photons are indistinguishable followed by two SPDs to measure and distinguish the two Bell states, as described in [44].

B. Optical Component Interactions

When using BB84 for QKD with time-bin-encoded qubits, SeQUeNCe encodes a bit value 0 (1) into the quantum state $|e\rangle$ ($|l\rangle$) in the Z-basis, while the same bit value 0 (1) will be encoded into the quantum state $|+\rangle$ ($|-\rangle$) in the X-basis. A photon may be measured in either the Z- or X-basis. The Z-basis measurement uses a single detector and early or late detection time is used to distinguish between the $|e\rangle$ and $|l\rangle$ states. The X-basis measurement of the photon is performed by two detectors after an MZI and the states $|+\rangle$ and $|-\rangle$ are distinguished by which detector is triggered during the late time-bin. Tables I and II show the probability of arrival time for the Z- and X-basis measurement, respectively, for four different quantum states $|+\rangle$, $|-\rangle$, $|e\rangle$, and $|l\rangle$. Note that there is only a 25% detection efficiency for the $|+\rangle$ and $|-\rangle$ states when measured in the X-basis, compared with the 100% efficiency of $|e\rangle$ and $|l\rangle$ state detection in the Z-basis.

TABLE I: Quantum state measured by Z-basis arrival time probability. Bold entries denote measurement events used to distinguish $|e\rangle$ and $|l\rangle$ states.

Input State	Detector	Early	Late
$\|+\rangle$	#1	50%	50%
$\|-\rangle$	#1	50%	50%
$\|e\rangle$	#1	**100%**	0%
$\|l\rangle$	#1	0%	**100%**

TABLE II: Quantum state measured by X-basis arrival time probability. Bold entries denote measurement events used to distinguish $|+\rangle$ and $|-\rangle$ states.

Input State	Detector	Early	Late	Late late
$\|+\rangle$	#0	12.5%	**25%**	12.5%
	#1	12.5%	**0%**	12.5%
$\|-\rangle$	#0	12.5%	**0%**	12.5%
	#1	12.5%	**25%**	12.5%
$\|e\rangle$	#0	25%	25%	0%
	#1	25%	25%	0%
$\|l\rangle$	#0	0%	25%	25%
	#1	0%	25%	25%

IV. Quantum Key Distribution

This section describes the setup and results for our QKD simulation.

A. Physical Connectivity and Protocol Implementation

Figure 2 shows the simulated experimental setup of QKD where Alice and Bob generate a shared random key using the BB84 and Cascade protocols. All components in our simulation share a global clock, which eliminates the need to simulate time synchronization components.

Alice uses a light source to generate photons in an arbitrary quantum state and then sends them to Bob over a quantum channel. Bob uses an optical switch to send each photon to either an SPD or MZI. If a photon is sent directly to the SPD, it is measured in the Z-basis. If the photon is sent through the MZI it is measured in the X-basis by the two SPDs. The classical communication of the BB84 protocol between Alice and Bob occurs on the classical channel.

SeQUeNCe implements and simulates the BB84, Cascade and privacy amplification protocols that are used in succession to generate the raw key, ensure key consistency, and maintain key privacy, respectively.

The QKD protocol stack is simulated by performing the following steps:

1) Alice prepares a random stream of bits, chooses either the Z- or X-basis for each bit at random, encodes the bit in the chosen basis, and transmits it to Bob.
2) Bob randomly chooses either the Z or X measurement basis for each received photon and measures the encoded state.

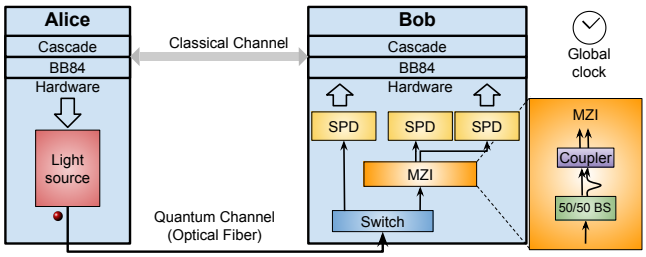


Fig. 2: QKD setup. Alice and Bob create a shared secret key: the quantum channel is used to transmit time-bin-encoded photons; the switch determines whether the photons are measured in the X- or Z-basis; BB84 and Cascade protocols are implemented in Alice and Bob.

3) Bob periodically sends his measurement basis list to Alice who determine which bases match; bits with matching encoding and measurement bases are used by Alice and Bob as the raw key.
4) The raw key is passed to the Cascade protocol that corrects any errors that could have occurred during transmission or measurement. Checksums sent on the public classical channel are used to correct the errors.
5) Privacy amplification protocol is used to ensure that the eavesdropper cannot use any information learned by intercepting messages on the public classical channel in the previous step.

Both the encoding and detection processes follow the interaction models described in Section III-B.

B. Experimental Setup and Results

We simulated two experiments described in [26] that quantify the quantum bit error ratio (QBER) and throughput of QKD protocols. The experimental setup in [26] matches the one shown in Figure 2. We selected the parameters of our simulation to match the parameters of the optical components in the experiment. The frequency of the light source is 2 MHz and the mean photon number is $\mu = 0.1$. Photons are transmitted on an optical fiber with attenuation $\alpha_o = 0.2$ dB/km. Bob's overall detection efficiency as defined in [26] is $\eta_{Bob} = 0.045$. To achieve the same detection efficiency, we adjusted the efficiency of our detectors in Bob denoted by η. For our BB84 implementation, if a photon is measured in the Z-basis (with probability $P_Z = 50\%$), the detection efficiency is η. If a photon is measured in the X-basis (with probability $P_X = 50\%$) there is only a 25% probability of getting a distinguishable result (see Table II). Thus the expected detection efficiency is given by

$$\eta_{Bob} = P_Z \cdot \eta + P_X \cdot 0.25 \cdot \eta = 0.625\eta. \tag{1}$$

To achieve the overall efficiency $\eta_{Bob} = 0.045$ we set the efficiency of our detectors at Bob to $\eta = 0.072$. Another parameter reported in [26] is the probability of an error count per clock cycle (P_e). This error in the experiment comes from the dark count of the detector and stray light from the intense clock laser that is not fully blocked by a filter. We mimic these processes by adjusting the dark count of our detectors to an appropriate value. Using the values $P_e = 8.5 \times 10^{-7}$ from [26] and our 2 ns measurement clock cycle, we obtain a dark count $= \frac{P_e}{\text{clock cycle}} = 425$ counts per second. Since the count rate and time resolution of detectors are not specified in [26], we set the count rate to 1×10^7 /s and time resolution to 10 ps, which are typical parameters used in state-of-the-art detectors.

In our simulation, we measured the QBER of BB84 as a function of the fiber length L varying from 1 km to 120 km in 10 km increments. For each fiber length, we generate ten 256-bit keys to measure the QBER. Figure 3 depicts the theoretical QBER (solid line) and measured QBER (blue squares). The theoretical QBER can be written as follows [26]:

$$QBER = \frac{0.5 \cdot P_e}{0.5 \times \mu 10^{-\alpha_o L/10} \eta_{Bob} + P_e}. \tag{2}$$

We observe that the simulated values match the theoretical prediction. In [26], the modulation error from the phase modulator introduced a constant error rate, around 3.3%. After adding an additional 3.3% error, our simulator produces results (red diamond) similar to those measured in [26]. When the fiber length increases from 100 km to 120 km, the measured QBER in [26] exceeds the expected error rate. These unknown errors do not manifest themselves in our simulation.

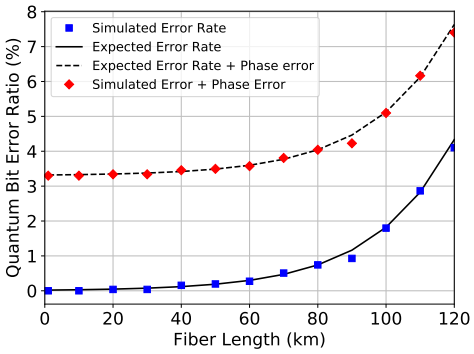


Fig. 3: QBER of the BB84 protocol

We also simulated the raw bit rate and key formation rate (see Figure 4). The raw bit rate is the throughput of the BB84 protocol that generates a shared key with some errors. The key formation rate is the throughput of the Cascade protocol with privacy amplification, which corrects error bits and hashes the raw key to a shorter key. We chose 10240 bits as the size of the frame in Cascade. After error correction, one frame was hashed to a frame of $10240 - t - s$ bits, where t is the number of disclosed bits and $s = 5000$ is a security parameter. Similar to [26], the throughput of both protocols decreases exponentially with increasing fiber length. The gap between the throughput of BB84 and Cascade comes from the security parameter and disclosed bits that increase as QBER increases. In [26], the key formation rate has a large drop when the fiber length increases from 100 km to 120 km.

This drop is not shown in our simulation results. Since the authors did not explain the reason for this drop, we conjecture that their privacy amplification protocol increases the security parameter as QBER increases, whereas our implementation uses a constant value.

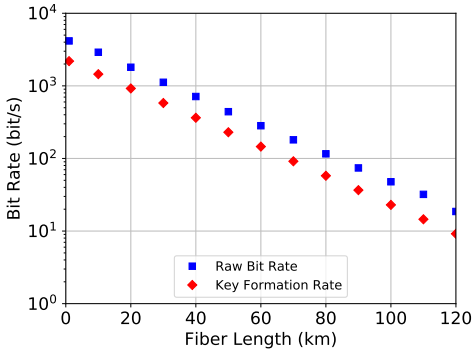


Fig. 4: Throughput of the BB84 (raw bit rate) and Cascade protocol with privacy amplification (key formation rate)

When we measure the throughput of Cascade, we observe that it decreases exponentially with increasing distance. For a 1 km fiber, the latency of Cascade is 2.4 seconds. However, when the fiber length increases to 120 km, the latency of Cascade increases to 524.9 seconds. The latency is large due to the need to construct an entire frame before Cascade can remove any errors. The frame size of Cascade is 10,240 bits, much longer than the 256 bits needed to produce a single key. The latency needed to perform the error correction procedures is negligible compared to the frame construction time. The error correction time is only 1.5 seconds for the maximum simulated fiber length of 120 km.

To determine if the latency of Cascade can be decreased, we simulate the use of a light source with higher frequencies f. The results are shown in Figure 5. We observe that higher light source frequencies reduce the latency of Cascade. For an 80 MHz light source over a 120 km fiber, the latency of Cascade is only 14.6 seconds, and the frame construction and error correction contribute 13.1 and 1.5 seconds, respectively. We conclude that a high-frequency light source can decrease the frame construction time.

The QBER and throughput simulations demonstrate the functionality and accuracy of SeQUeNCe. The reconfigurability of SeQUeNCe enables us to quickly perform a number of simulations with different parameters for each optical component and gain insight which changes have the most impact on the overall network performance.

V. Quantum State Teleportation

A. Physical Connectivity and Protocol Implementation

Figure 6 shows the simulated experimental setup of quantum state teleportation. Our simulation includes three nodes: Alice, Bob, and Charlie, with quantum channel and classical channel between Alice-Charlie and Charlie-Bob. In the teleportation protocol, Alice creates a target photon with an arbitrary

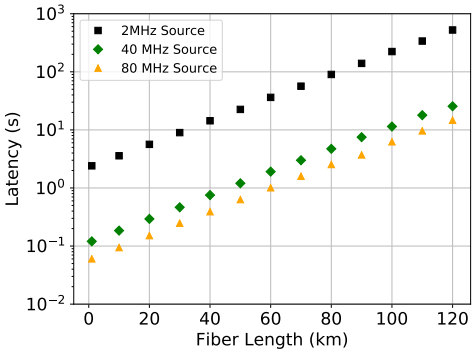


Fig. 5: Latency of the Cascade protocol with different frequencies of the light source

quantum state $|\psi_t\rangle$ and sends it to Charlie on the quantum channel. Bob creates a pair of entangled photons using the SPDC source. One of the photons is kept by Bob (idle photon), and the other photon is sent to Charlie (signal photon) using a quantum channel. The global clock and synchronization between Alice and Bob ensure that both the target photon and signal photon arrive at the BSM at the same time. When two photons are measured by the BSM, the quantum state of the photon pair is projected to one of the four Bell states. However, our BSM can distinguish projection only to the states $|\Psi^+\rangle$ or $|\Psi^-\rangle$. After the BSM, the state of the idle photon is changed to either $\sigma_x|\psi_t\rangle$ in the case of a $|\Psi^+\rangle$ measurement or to $\sigma_x\sigma_z|\psi_t\rangle$ in the case of a $|\Psi^-\rangle$ measurement, where σ_x and σ_z are Pauli-X and -Z gates respectively. The effect of measurement on the states used in our simulation is illustrated in Table III.

TABLE III: Quantum state of idle photon after BSM

Target Photon State Before BSM	Idle Photon After $\|\Psi^+\rangle$ Measurement	Idle Photon After $\|\Psi^-\rangle$ Measurement
$\|e\rangle$	$\|l\rangle$	$\|l\rangle$
$\|l\rangle$	$\|e\rangle$	$-\|e\rangle$
$\|+\rangle$	$\|+\rangle$	$-\|-\rangle$
$\|-\rangle$	$-\|-\rangle$	$\|+\rangle$

The result of the BSM is sent through the classical channel to Bob. Bob then measures the idle photon in a chosen basis and uses the result of the BSM at Charlie to correct the measurement if necessary. Success of the quantum state teleportation is determined by comparison with the state prepared by Alice.

B. Parameters and Simulation Results

For our simulation, we use optical component parameters consistent with the experiment in [27]. The only notable difference is addition of a delay fiber between Bob's SPDC source and measurement. Alice uses a light source with parameters $f = 80$ MHz, $\mu = 0.014$ to generate target photons in any of the four quantum states $|e\rangle$, $|l\rangle$, $|+\rangle$, $|-\rangle$. These photons are sent to Charlie over a fiber with length 6.2 km and a loss rate of 6 dB. Bob uses an SPDC source with parameters $f_{SPDC} = 80$

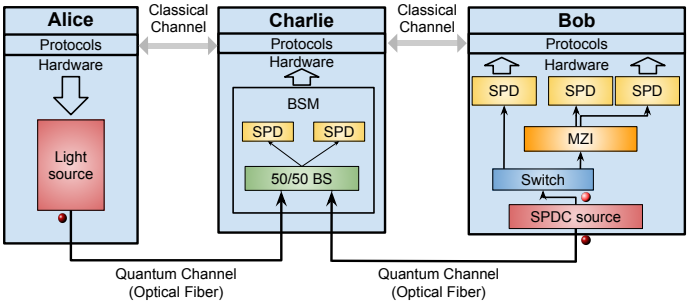


Fig. 6: Quantum teleportation architecture. Alice emits photons with arbitrary quantum state to Charlie. Bob creates a pair of entangled photons and send one of it to Charlie. Charlie receives two photon simultaneously and measures them by BSM. BSM results are sent to Bob for correction a posteriori if necessary.

MHz, $\mu_{SPDC} = 0.045$ to generate pairs of perfectly entangled photons. The length of the fiber between Bob and Charlie is 11.1 km with a loss of 5.7 dB, while the delay fiber in Bob's node has a length of 11.11 km with a total loss of 2.2 dB. Before the simulation, Alice and Bob have coordinated the times for emitting photons to ensure their two photons arrive at the BSM at the same time. The detectors in the BSM have a detection efficiency $\eta = 0.7$, dark count rate 1000 /s, time resolution = 150 ps, and count rate = 2.5×10^7 /s.

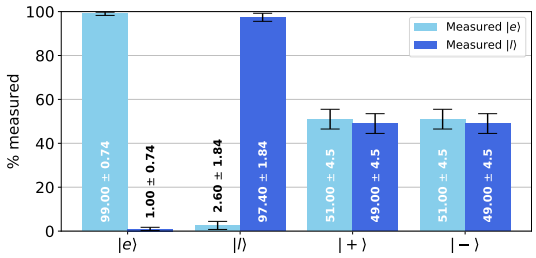
The idle photons are then measured in either the X- or Z-bases. Depending on the result of the BSM at Charlie, the state measured at Bob may be altered post-measurement according to Table III to record the correct result. For quantum states $|e\rangle$ and $|l\rangle$, any successful BSM flips the measured result. For quantum states $|+\rangle$ and $|-\rangle$, measured results will be flipped if the quantum state is projected to $|\Psi^-\rangle$.

For each of the four teleported states, 100 qubits were measured at Bob in both the X- and Z-basis. The simulation was repeated 10 times, and the average percentage of qubits measured in each basis state as well as the standard deviation were recorded. These results are shown in Figure 7.

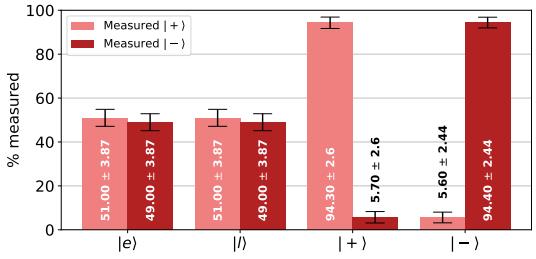
In the first graph, depicting the Z-basis measurement, the $|e\rangle$ and $|l\rangle$ states are easily distinguishable as expected, while the $|+\rangle$ and $|-\rangle$ states are indistinguishable. For the X-basis measurement shown in the second graph, the $|+\rangle$ and $|-\rangle$ states can be distinguished while the $|e\rangle$ and $|l\rangle$ states are indistinguishable.

A small error on the order of 1-2% present in the Z-basis measurements is consistent with errors caused by multiphoton emission events and detector dark counts. Larger errors of approximately 5% are present in the X-basis measurements. These errors are due to the lower efficiency of the X-basis measurement and due to the fact that a detection error by any of the two detectors used by Bob causes an error. Additional phase error is introduced by Alice during qubit preparation as well.

These results validate that the states generated by Alice were successfully teleported to Bob. When measured, the idle



(a) Z-basis measurement results



(b) X-basis measurement results

Fig. 7: Measured quantum state of the idle photon after BSM in our simulation

photon at Bob is usually found in the same state as the photon that had been prepared by Alice and sent to Charlie after taking into account basis correction communicated on the classical channel. Our results also validate that SeQUeNCe is able to track errors originating in the imperfect optical components.

VI. Outlook and Future Work

In this paper we developed models of optical network components and integrated them into our new simulator of quantum network communication. We performed simulations of quantum key distribution and quantum teleportation at the individual photon level and successfully matched our results with prior experiments.

Our simulator uses a modular design and can be easily extended to model new physical processes and optical components. Advances in material science promise to deliver new components such as long-coherence-time memories or improved photon detectors in the near future. The simulation techniques we develop can be used to quantify the benefits of these advances and to understand which improvements are the most valuable.

As the size of experimental quantum networks increases, the value of simulation tools that can predict the complex behavior of these systems will increase. Simulations will be also needed to optimize the placement and integration of optical quantum network components with the goal to build network architectures that can support the scalability, latency, throughput and security needs of the disparate quantum network applications in the post-Moore world.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7–11, 2014.

[2] A. M. Childs, "Secure assisted quantum computation," *Quantum Info. Comput.*, vol. 5, no. 6, pp. 456–466, Sep. 2005.

[3] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, "Secure identification and QKD in the bounded-quantum-storage model," *Theor. Comput. Sci.*, vol. 560, no. P1, pp. 12–26, Dec. 2014.

[4] J. Kaniewski and S. Wehner, "Device-independent two-party cryptography secure against sequential attacks," *New Journal of Physics*, vol. 18, no. 5, p. 055004, 2016.

[5] G. Brassard, "Quantum communication complexity: a survey," in *Proceedings. 34th International Symposium on Multiple-Valued Logic*, May 2004, pp. 56–.

[6] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, "Quantum clock synchronization based on shared prior entanglement," *Phys. Rev. Lett.*, vol. 85, pp. 2010–2013, Aug 2000.

[7] C. Freier, M. Hauth, V. Schkolnik, B. Leykauf, M. Schilling, H. Wziontek, H.-G. Scherneck, J. Müller, and A. Peters, "Mobile quantum gravity sensor with unprecedented stability," *Journal of Physics: Conference Series*, vol. 723, no. 1, p. 012050, 2016.

[8] J. Kelly, "A preview of Bristlecone, Google's new quantum processor," Google AI Blog, https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html, Mar 2018.

[9] W. Knight, "IBM raises the bar with a 50-qubit quantum computer," MIT Technology Review, https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/, Nov 2017.

[10] J. Hsu, "CES 2018: Intel's 49-qubit chip shoots for quantum supermacy," IEEE Spectrum, https://spectrum.ieee.org/tech-talk/computing/hardware/intels-49qubit-chip-aims-for-quantum-supremacy, Jan 2018.

[11] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[12] "Commercial National Security Algorithm suite," National Security Agency, https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm, Aug 2019.

[13] "Post-Quantum Crypto Project," National Institute of Standards and Technology, http://csrc.nist.gov/groups/ST/post-quantum-crypto/, Aug 2019.

[14] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, p. 661, 1991.

[15] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, "Picosecond superconducting single-photon optical detector," *Applied Physics Letters*, vol. 79, no. 6, pp. 705–707, 2001.

[16] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," *Nature Photonics*, vol. 7, p. 210, Feb 2013.

[17] T. Ortlepp, M. Hofherr, L. Fritzsch, S. Engert, K. Ilin, D. Rall, H. Toepfer, H.-G. Meyer, and M. Siegel, "Demonstration of digital readout circuit for superconducting nanowire single photon detector," *Opt. Express*, vol. 19, no. 19, pp. 18 593–18 601, Sep 2011.

[18] Q. Zhao, T. Jia, M. Gu, C. Wan, L. Zhang, W. Xu, L. Kang, J. Chen, and P. Wu, "Counting rate enhancements in superconducting nanowire single-photon detectors with improved readout circuits," *Opt. Lett.*, vol. 39, no. 7, pp. 1869–1872, Apr 2014.

[19] L. Lerner, "Quantum network to test unhackable communications," https://www.anl.gov/article/quantum-network-to-test-unhackable-communications, Oct. 2018.

[20] INQNET, "Fermilab quantum network (FQNET)," http://inqnet.caltech.edu/fqnet/.

[21] "China opens 2,000-km quantum communication line," State Council of the People's Republic of China, http://english.gov.cn/news/photos/2017/09/30/content_281475894651400.htm, Aug 2019.

[22] D. Castelvecchi, "The quantum internet has arrived (and it hasn't)," *Nature*, vol. 554, pp. 289–292, Feb. 2018.

[23] University of Cambridge, "Cambridge launches UK's first quantum network," https://www.cam.ac.uk/research/news/cambridge-launches-uks-first-quantum-network.

[24] N. Walenta and L. Oesterling, "Quantum networks: Photons hold key to data security," Photonics Media, https://www.photonics.com/Articles/Quantum_Networks_Photons_Hold_Key_to_Data/a60541, Aug 2019.

[25] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, "Pulsed energy-time entangled twin-photon source for quantum communication," *Physical Review Letters*, vol. 82, no. 12, p. 2594, 1999.

[26] C. Gobby, Z. Yuan, and A. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters*, vol. 84, no. 19, pp. 3762–3764, 2004.

[27] R. Valivarthi, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, W. Tittel *et al.*, "Quantum teleportation across a metropolitan fibre network," *Nature Photonics*, vol. 10, no. 10, p. 676, 2016.

[28] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1993, pp. 410–423.

[29] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, vol. 70, no. 13, p. 1895, 1993.

[30] L. Hu, H. Liu, and Y. Lin, "Parameter optimization of Cascade in quantum key distribution," *Optik*, vol. 181, pp. 156 – 162, 2019.

[31] M. Mehic, O. Maurhart, S. Rass, and M. Voznak, "Implementation of quantum key distribution network simulation module in the network simulator ns-3," *Quantum Information Processing*, vol. 16, no. 10, p. 253, 2017.

[32] M. Niemiec, Ł. Romański, and M. Święty, "Quantum cryptography protocol simulator," in *International Conference on Multimedia Communications, Services and Security*. Springer, 2011, pp. 286–292.

[33] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol Cascade," *arXiv preprint arXiv:1407.3257*, 2014.

[34] A. Pereszlenyi, "Simulation of quantum key distribution with noisy channels," in *Proceedings of the 8th International Conference on Telecommunications, 2005. ConTEL 2005.*, vol. 1. IEEE, 2005, pp. 203–210.

[35] A. Dahlberg and S. Wehner, "SimulaQron—a simulator for developing quantum internet software," *Quantum Science and Technology*, vol. 4, no. 1, p. 015001, Sept. 2018.

[36] "Netsquid: Network simulator for quantum information using discrete events," https://netsquid.org/, Aug 2019.

[37] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, "Generation of hyperentangled photon pairs," *Physical Review Letters*, vol. 95, no. 26, p. 260501, 2005.

[38] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, "Beating the channel capacity limit for linear photonic superdense coding," *Nature Physics*, vol. 4, no. 4, p. 282, 2008.

[39] I. Marcikic, H. De Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, "Distribution of time-bin entangled qubits over 50 km of optical fiber," *Physical Review Letters*, vol. 93, no. 18, p. 180502, 2004.

[40] T. Kim, I. S. genannt Wersborg, F. N. Wong, and J. H. Shapiro, "Complete physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 protocol," *Physical Review A*, vol. 75, no. 4, p. 042327, 2007.

[41] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[42] J.-G. Ren *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, pp. 70 EP –, 08 2017.

[43] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward," *Nature*, vol. 489, pp. 269 EP –, 09 2012.

[44] R. Valivarthi *et al.*, "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors," *Optics Express*, vol. 22, no. 20, pp. 24 497–24 506, 2014.