Covert Quantum Internet

Kamil Brádler,1 George Siopsis,2† and Alex Wozniakowski3‡

1 Department of Mathematics and Statistics, University of Ottawa, Ottawa, Canada
2 Department of Physics and Astronomy, The University of Tennessee, Knoxville, TN 37996-1200, U.S.A.
3 Department of Physics, Harvard University, Cambridge, MA 02138, U.S.A.

(Dated: April 25, 2017)

We apply covert quantum communication based on entanglement generated from the Minkowski vacuum to the setting of quantum computation and quantum networks. Our approach hides the generation and distribution of entanglement in quantum networks by taking advantage of relativistic quantum effects. We devise a suite of covert quantum teleportation protocols that utilize the shared entanglement, local operations, and covert classical communication to transfer or process quantum information in stealth. As an application of our covert suite, we construct two prominent examples of measurement-based quantum computation, namely the teleportation-based quantum computer and the one-way quantum computer. In the latter case we explore the covert generation of graph states, and subsequently outline a protocol for the covert implementation of universal blind quantum computation.

I. INTRODUCTION

The Internet is ubiquitous in daily life, linking a multitude of devices; but the security of the Internet is a public concern. For the exchange of sensitive information a different type of network, called the Darknet, provides anonymous connections that are strongly resistant to eavesdropping and traffic analysis. Recently, the structure and resilience of the Internet and the Darknet were analyzed, and the latter was shown to be a more robust network under various types of failures. Covert protocols for classical communication and computation supply networks with a concealing medium or object, enabling data to be transferred or processed without detection. Quantum information science provides a new perspective on the networking of devices, as well as the possible types of algorithms and protocols. In the setting of the quantum internet the network nodes generate, process, and store quantum information locally, and entanglement is distributed across the entire network. As part of the paradigm of local operations and classical communication (LOCC), quantum teleportation protocols utilize the shared entanglement to faithfully transfer quantum data from site to site or implement quantum logic gates for distributed quantum computation.

In certain situations, such as a secret government mission, quantum networks might need their communications or computations to be performed without detection. Here, we solve this problem by extending recent work on covert quantum communication to the setting of quantum computation and quantum networks. We devise a suite of covert quantum teleportation protocols taking advantage of relativistic quantum effects. We show, for instance, that quantum teleportation protocols can be performed in stealth by utilizing the entanglement present in Minkowski vacuum and covert classical communication to hide the non-local parts in quantum teleportation. In our setup we hide the generation and sharing of entanglement, without a concealing medium or object, between network nodes through the relativistic modes of the Minkowski vacuum, and covert entanglement persists at long distance. We introduce a Minkowski vacuum-assisted amplification scheme in Section 11 followed by standard entanglement distillation with covert classical communication to recover covert Bell states. The entanglement-swapping protocol with covert classical communication distributes entanglement across the network, which provides a resource for our suite of covert quantum teleportation protocols. This enables quantum data to be transferred or processed in the quantum network without detection. Thereby, the quantum network’s operations remain hidden from any adversary outside of the network. We call this the Covert Quantum Internet.
We apply our suite of covert quantum teleportation protocols to construct two prominent examples of measurement-based quantum computation [17, 18]: the teleportation-based quantum computer [19–24] and the one-way quantum computer QC$_C$ [25–27]. Teleportation-based quantum computers use the idea of gate teleportation to carry out computations. We give covert versions of gate teleportation protocols, such as the one-bit teleportation primitive [20] and the multipartite compressed teleportation (MCT) protocol [28], in Section III. We discuss universal quantum computation with covert gate teleportation in Section IV A. A one-way quantum computer QC$_C$ carries out computations solely by performing single-qubit measurements on a fixed, many-body resource state and the measurement bases determine the gate or algorithm that is implemented. We show how to covertly generate graph states, such as the topological 3D cluster state [29, 30] or the recently discovered Union Jack state with nontrivial 2D symmetry protected topological order (SPTO) [31], in Section IV B. The single-qubit measurements on the covert resource state are performed locally during implementation of a quantum algorithm, and the feed-forward of measurement outcomes is shared through covert classical communication. In addition we outline a covert implementation of the Broadbent, Fitzsimons, and Kashefi (BFK) protocol for universal blind quantum computation [32] in Section IV B. Finally, we conclude in Section V.

II. COVERT COMMUNICATION

Long before the development of cryptography and encryption, one of humankind’s best techniques of secretly delivering a message was to hide the fact that a message was even delivered at all. Methods for covert quantum communication with a concealing medium, i.e., thermal noise, were considered in [33, 34], but the conclusion was that stealth capabilities vanish when the medium is absent. In [16] truly ultimate limits on covert quantum communication were presented. In this section we describe the covert generation and sharing of entanglement between Alice and Bob, or network nodes in a quantum network, without a concealing medium or object using plain two-state inertial detectors [35]. The goal is to generate entanglement from the vacuum. We describe a process which results in entangled detectors. However, the amount of entanglement is very small. We amplify it by repeating the process, thus accumulating a finite amount of entanglement from the vacuum. The fidelity of the resulting state shared by the detectors possessed by Alice and Bob is then increased close to perfection by standard distillation techniques. The previous work of some of the authors, [16], differs from the current analysis in the type of the detectors used. In both cases the detectors are inertial, but in [16] we used a pair of two two-level atoms with a time-dependent energy gap. This, however, poses a considerable challenge for the current quantum technology state-of-the-art. Here, the detectors are standard two-level atoms.

Alice and Bob are in possession of two-state detectors. The detectors couple to vacuum modes which we model by a real massless scalar field $\phi$. They are separated by a distance $L$. For definiteness, let $r = r_A \equiv (0, 0, 0)$ for Alice, and $r = r_B \equiv (0, 0, L)$ for Bob. If Alice’s (Bob’s) detector is turned on at time $t$ ($t'$), then the proper time between the two detectors while in operation is

$$\Delta s^2 = (t' - t)^2 - L^2. \quad (1)$$

We expect maximal correlations between the two detectors along the null line connecting the two events, i.e., $\Delta s = 0$, or $t' - t = L$. Thus, if Alice’s detector is turned on at $t = 0$, then optimally, Bob’s detector will be turned on at time $t' = L$.

The two-point correlator for the massless scalar field is given by

$$\Delta(t, r; t', r') = -\frac{1}{4\pi^2} \frac{1}{(t - t' - i\varepsilon)^2 - (r - r')^2}. \quad (2)$$

For best results at finite $L$, for the detectors we choose window functions centered around points at which $\Delta$ diverges (i.e., Alice and Bob are along a null line). Thus, for Alice and Bob, we choose, respectively,

$$w_A(t) = \lambda w(t), \quad w_B(t) = \lambda w(t - L), \quad w(t) = e^{-\frac{t^2}{\sigma^2}}, \quad (3)$$

where $\lambda > 0$ is a coupling constant whose value depends on the details of the detector setup. In general, it is expected to be small. $\sigma$ is the width of the time window during which the detector is turned on.
Assuming localized detectors, the Hamiltonian is
\[ H = H_A + H_B, \quad H_k = w_k(t) \left( e^{i\delta \sigma_k^+} + e^{-i\delta \sigma_k^-} \right) \phi(t, r_k) \quad (k = A, B) \]
where \( h \delta \) is the energy gap of the two states of a detector, and \( \sigma_k^\pm \) are spin ladder operators for Alice’s (Bob’s) detector.

The massless scalar field can be expanded in terms of creation and annihilation operators as
\[ \phi(t, r) = \int \frac{d^3k}{(2\pi)^3 2|k|} \left( a(k)e^{-i(k|t-k| \cdot r)} + a^\dagger(k)e^{i(k|t-k| \cdot r)} \right) \]
where \( a(k) \) annihilates the vacuum \( (a(k)|0\rangle = 0) \). The Hilbert space of the system is the tensor product of excitations of the vacuum state \( |0\rangle \), and the two-dimensional spaces of Alice and Bob spanned by \( \{|0\rangle_k, |1\rangle_k\}, k = A, B \).

Assuming an initial state \( |in\rangle = |0\rangle \otimes |0\rangle_A \otimes |0\rangle_B \), the evolution of the system is governed by the Hamiltonian \( H \). After tracing out the field degrees of freedom, it is easy to see that the final state is of the form
\[ \varrho_{AB} = \begin{bmatrix} a_1 & 0 & 0 & c_1 \\ 0 & a_2 & c_2 & 0 \\ 0 & c_2^* & b_2 & 0 \\ c_1^* & 0 & 0 & b_1 \end{bmatrix} \]
Thus the evolution of the system of the two detectors after they are switched on and off with the switching profile \( \delta \) is given by the quantum channel \( \mathcal{N} : |in\rangle \mapsto \varrho_{AB} \). The final state is in general entangled. However, the amount of entanglement is minute. To enhance the entanglement, after the detectors have been switched off and therefore decoupled from the scalar field, we bring the state of \( \phi \) back to the vacuum, and repeat the process. This can be repeated \( N \) times, where \( N \) is large enough for appreciable entanglement generation. At the \( n \)th step, we apply the channel
\[ \mathcal{N}_n : \varrho_{AB}^{(n)} \mapsto \varrho_{AB}^{(n+1)} \]
At each step, the state is of the same form as \( \varrho_{AB} \).

Using perturbation theory, we obtain
\[ \varrho_{AB} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \lambda^2 \begin{bmatrix} -2\mathcal{J}_1 & 0 & 0 & -\mathcal{J}_2^* \\ 0 & \mathcal{J}_1 & \mathcal{J}_3 & 0 \\ 0 & \mathcal{J}_3^* & \mathcal{J}_1 & 0 \\ -\mathcal{J}_2 & 0 & 0 & 0 \end{bmatrix} + \mathcal{O}(\lambda^4) \]
Explicitly, at first order in \( \lambda^2 \) we have
\[ \mathcal{J}_1 = -\frac{1}{4\pi^2} \int_{-\infty}^\infty dt \mathcal{w}(t) \int_{-\infty}^\infty dt' \mathcal{w}(t') \frac{e^{i\delta(t-t')}}{(t'-t-ic)^2} , \]
\[ \mathcal{J}_2 = -\frac{1}{4\pi^2} \int_{-\infty}^\infty dt \mathcal{w}(t) \int_{-\infty}^\infty dt' \mathcal{w}(t' - L) \frac{e^{i\delta(t+t')}}{(t'-t-ic)^2 - L^2} , \]
\[ \mathcal{J}_3 = -\frac{1}{4\pi^2} \int_{-\infty}^\infty dt \mathcal{w}(t) \int_{-\infty}^\infty dt' \mathcal{w}(t' - L) \frac{e^{i\delta(t-t')}}{(t'-t-ic)^2 - L^2} . \]
These expressions contain poles. Using the Fourier transform of the detector profile,
\[ \mathcal{w}(\omega) = \int_{-\infty}^\infty dt e^{-i\omega t} \mathcal{w}(t) = \sigma \sqrt{\pi} e^{-\sigma^2 \omega^2/4} \]
and contour integration, we arrive at expressions which are free of singularities and amenable to
numerical integration:

\[ J_1 = \frac{1}{4\pi^2} \int_0^\infty d\omega \tilde{\omega}^2 (\omega + \delta), \]

\[ J_2 = \frac{1}{4\pi^2 L} \int_0^\infty d\omega \tilde{\omega} (\omega - \delta) \tilde{\omega} (\omega + \delta) e^{-iL(\omega - \delta)} \sin \omega L, \]

\[ J_3 = \frac{1}{4\pi^2 L} \int_0^\infty d\omega \tilde{\omega}^2 (\omega + \delta) e^{-iL(\omega - \delta)} \sin \omega L. \]

(12)

After \( n \) applications of the quantum channel, we bring the system of the two detectors to the state

\[ \varrho_{AB}^{(n)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + n\lambda^2 \begin{pmatrix} -2J_1 & 0 & 0 & -J_2^* \\ 0 & J_1 & J_3 & 0 \\ 0 & J_3^* & J_1 & 0 \\ -J_2 & 0 & 0 & 0 \end{pmatrix} + \mathcal{O}(\lambda^4) \]

(13)

Thus, after \( N \) steps, the effective coupling constant becomes \( N\lambda^2 \), and entanglement is amplified.

To quantify the results, we use the singlet fraction of \( \varrho \) defined as

\[ F(\varrho) = \max_{\Phi} \langle \Phi | \varrho | \Phi \rangle, \quad |\Phi\rangle = U_A \otimes U_B \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB}). \]

(14)

We have optimized the singlet fraction using perturbation theory numerically to second order in

\[ \lambda^2. \]

We have shown above explicit analytic expressions at first order in \( \lambda^2 \). We have also obtained second-order analytical expressions, but not included here for brevity. Their derivation is based on the expansion of two two-level detectors to an arbitrary perturbative order in \( \lambda^2 \). Using these second-order analytical expressions, we have calculated the singlet fraction numerically. Its behavior is shown in Fig. 1 and 2. For a wide range of parameters of the system, we obtain \( F > 1/2 \), showing entanglement extraction from the vacuum. More precisely, there are known two-qubit entangled states where \( F < 1/2 \), but in our case the entanglement of formation (EOF) is zero whenever \( F \leq 1/2 \), and positive otherwise. The iteratively collected entanglement through the Minkowski vacuum-assisted amplification scheme is shown in figure Fig. 2. As the number of iterations increases, the original minute amount of entanglement reaches quite substantial values. When measured as the singlet fraction, it goes well above 1/2 and a corresponding increase is

\[ \text{FIG. 1. The singlet fraction vs. the distance } L \text{ of the two detectors for different values of their energy gap. The number of iterations is } N = 500, \lambda^2 = 0.01, \text{ and } \sigma = 10 \mu s. \]

\[ F(\varrho) \text{ vs. } L \text{ [km]} \]

\[ \delta = 200 \text{ kHz} \]
\[ \delta = 140 \text{ kHz} \]
\[ \delta = 100 \text{ kHz} \]

\[ F(\varrho) \text{ vs. } L \text{ [km]} \]
FIG. 2. The singlet fraction $F(\kappa)$ vs. the distance $L$ of the two detectors at different stages of entanglement amplification for $\lambda^2 = 0.01, \delta = 100$ kHz, and $\sigma = 10$ $\mu$s.

documented for the EOF as well. Recall that the EOF is a true entanglement measure for two qubits. As in the case of Fig. 1, the actual calculation is done to the second order in $\lambda^2$. After the amplification process is completed, we perform standard distillation on many copies of the iterated state in order to arrive at a nearly perfect maximally entangled state. Thus, we produce a covert Bell state shared between Alice’s and Bob’s detectors.

III. COVERT QUANTUM TELEPORTATION

The quantum teleportation protocol was introduced by Bennett et al. [38]. Recently, the protocol was found to have a 3D topological structure using the quon language [39]; and Pirandola and Braunstein cite teleportation as the “most promising mechanism for a future quantum internet” [14]. To implement the protocol for two parties: a sender, Alice, disassembles an unknown quantum state at her location; and a receiver, Bob, reconstructs the quantum state identically at his location. In order for the reconstruction to succeed, Alice and Bob prearrange to share the Bell state, which is utilized as a resource for the protocol. In addition, the parties share some purely classical information.

The idea of covertly implementing the quantum teleportation protocol involves hiding the non-local parts, i.e., distribution of the entangled resource state and classical communication of measurement outcomes. In [14] we presented the covert generation and distribution of the Bell state, shared by Alice and Bob. Covert classical communication hides the transfer of the measurement outcomes from Alice to Bob. Thus, we establish a protocol for the hidden transfer of quantum data between Alice and Bob, or network nodes.

Gottesman and Chuang considered a variant of the teleportation protocol in which Bob’s reconstructed quantum state differed from Alice’s original quantum state [19]. In this elegant version of teleportation the fault-tolerant construction of certain quantum gates was developed. Later, Zhou et al. extended the teleportation method of gate construction by introducing the one-bit teleportation primitive, which enabled a class of gates in the Clifford hierarchy to be recursively constructed [20]. As an example, this includes the controlled rotations that appear in Shor’s factoring algorithm [40]. Zhou et al. and Eisert et al. first considered the minimal resources required for the implementation of certain remote quantum gates [20, 21]. A generalization of these methods, called the multipartite compressed teleportation (MCT) protocol, enables the efficient sharing of multipartite, non-local quantum gates in which the protocol does not reduce to compositions of bipartite teleportation [28]. Furthermore, the MCT protocol allows a quantum network to share a controlled gate with multiple targets.

The scheme for the covert teleportation of quantum states is adaptable to the variants of the protocol that teleport quantum gates. For instance, the covert teleportation of a controlled-NOT gate
utilizes one covert Bell state, local operations, and covert classical communication of measurement outcomes. The covert recursive construction with one bit teleportation [20] utilizes instances of the covert, controlled-NOT gate, local operations, and covert classical communication of the ancillary state preparation and measurement outcomes. In the MCT protocol the resource state is either the Greenberger-Horne-Zeilinger state (GHZ), or |Max⟩ as first introduced in [41], depending upon the particular non-local quantum gate [28]. Both multipartite resource states can be constructed from simpler Bell states [41, 42], thus covert Bell states can be distilled into covert |GHZ⟩ or |Max⟩ with local operations and covert classical communication.

IV. COVERT MEASUREMENT-BASED QUANTUM COMPUTATION

A. Teleportation-Based Quantum Computation

The teleportation-based approach to quantum computation uses the idea of gate teleportation to affect quantum computation [19–24, 28]. Given the ability to perform single-qubit gates, the teleportation of either a controlled-NOT gate or a controlled-Z gate is universal for quantum computation. Hence, a covert implementation of a universal teleportation-based quantum computer is achieved with covert Bell states, local operations that include all single-qubit gates, and covert classical communication of measurement outcomes. Alternative universal quantum gate sets can be constructed through the covert MCT protocol or the covert recursive construction with the one-bit teleportation primitive.

B. One-Way Quantum Computation

Another prominent example of measurement-based quantum computation is the one-way quantum computer QC_C, which was introduced by Raussendorf and Briegel [25, 26]. The idea of QC_C is to prepare a fixed, many-body resource state in which quantum computations are carried out solely through single-qubit measurements on the resource state and classical feed-forward of measurement outcomes [17, 18]. Cluster states, a sub-class of graph states, are the archetypal resource state, whereby topological 3D cluster states are utilized in fault-tolerant versions of QC_C [29, 30]. Universal resource states for QC_C have been widely studied [18, 29, 30, 32, 43], and recently the universal Union Jack state with nontrivial 2D symmetry protected topological order (SPTO) was found [31].

A one-way quantum computation proceeds with a classical input that specifies the data and program. A graph state is generated by preparing each vertex qubit in a graph in the fiducial starting state |+⟩ ≡ 1/√2(|0⟩ + |1⟩), and applying a controlled-Z gate to every pair of qubits connected by an edge in the graph. Since controlled-Z gates mutually commute, the production of a graph state is independent of the order of operations. Next, a sequence of adaptive single-qubit measurements is implemented on certain qubits in the graph, whereby the measurement bases depend upon the specified program as well as the previous measurement outcomes. A classical computer determines which measurement directions are chosen during every step of the computation.

To covertly implement QC_C the classical input that specifies the data and program needs to be shared by covert classical communication. The graph state is generated by applying the covert, controlled-Z gate to each pair of fiducial qubits connected by an edge in the graph. The single-qubit measurements are applied locally. The classical computer that determines the measurement directions is offline, and covert protocols for communication [3–5] and computation [6–8] are utilized.

Topological 3D cluster states provide a pathway towards large-scale distributed quantum computation [15] by combining the universality of 2D cluster states with the topological error-correcting capabilities of the toric code [44]. Quantum computation is performed on a 3D cluster state via a temporal sequence of single-qubit measurements, which leaves a non-trivial cluster topology that embeds a fault-tolerant quantum circuit [29, 30]. To generate the computational resource state fiducial qubits are located at the center of faces and edges of an elementary cell; see Figure 2, page 5 of [30]. Controlled-Z gates are applied from each face qubit to each neighboring edge qubit. The elementary cell is tiled in 3D to form a topological cluster state. Hence, the covert generation of the topological 3D cluster state follows from the discussion above.
The universal 2D cluster state was shown to have trivial 2D symmetry protected topological order (SPTO) and nontrivial 1D SPTO, whereas the universal Union Jack state was found to possess nontrivial 2D SPTO \cite{31}. The Union Jack state is generated by preparing fiducial qubits, and applying a controlled-controlled-Z gate to every triangular cell in the graph. The resulting universal resource state has the advantageous property of being Pauli universal, meaning that single-qubit measurements in the Pauli bases on the Union Jack state can implement arbitrary quantum computations. The feature of Pauli universality is forbidden for the 2D cluster state, as implied by the Gottesman-Knill theorem, since the state is generated by an element from the Clifford group \cite{45}. In other words single-qubit measurements in the Pauli bases on the 2D cluster state are efficiently simulated on a classical computer. The covert generation of the Union Jack state is a simple modification of the aforementioned scheme with controlled-Z gates for graph states. Namely, covert teleportation applies a doubly controlled-Z gate to fiducial qubits in triangular cells.

BFK introduced a universal blind quantum computation protocol \cite{32}, which exploits measurement-based quantum computation to allow a client, Alice, with limited quantum computing power to delegate a computation to a quantum server, Bob. The premise of the BFK protocol is that Alice’s inputs, computations, and outputs are unknown to Bob \cite{32,46}. In what follows we outline a covert implementation of the basic steps in the BFK protocol, by hiding the communication rounds between Alice and Bob.

**Protocol** Covert BFK universal blind quantum computation

1. The preparation stage
   For each column \(x = 1, \ldots, n\)
   For each row \(y = 1, \ldots, m\)
   (a) Alice prepares qubits \(|\psi_{x,y}\rangle\) such that
   \[
   |\psi_{x,y}\rangle \in \left\{ \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i\theta_{x,y}} |1\rangle \right) \mid \theta_{x,y} = 0, \pi/4, \ldots, 7\pi/4 \right\},
   \]
   and transfers each qubit to Bob via covert teleportation.
   (b) Bob generates an entangled brickwork state \(G_{n \times m}\) \cite{32} from all the qubits received, applying a controlled-Z gate to qubits joined by an edge.

2. Interaction and measurement stage
   For each column \(x = 1, \ldots, n\)
   For each row \(y = 1, \ldots, m\)
   (a) Alice computes \(\phi'_{x,y}\) based on the real measurement angle \(\phi_{x,y}\) and the previous measurement results.
   (b) Alice chooses \(r_{x,y} \in \{0, 1\}\) and computes the angle
   \[
   \delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}.
   \]
   (c) Alice sends \(\delta_{x,y}\) to Bob via covert classical communication.
   (d) Bob measures \(|\psi_{x,y}\rangle\) in the basis \(\{ |0\rangle + e^{i\delta_{x,y}} |1\rangle \}\), then sends the measurement outcome to Alice via covert classical communication.
   (e) If \(r_{x,y} = 1\) above, then Alice flips the measurement outcome bit; otherwise she does nothing.

V. CONCLUSION

A quantum internet is a manifest platform for quantum cryptography, sensor networks, and large-scale networked quantum computing. We developed a quantum internet that hides its operations by exploiting features of relativistic quantum information. In particular, we used properties of the Minkowski vacuum to hide the generation and distribution of entanglement in quantum networks, which provides a resource for covert quantum teleportation, thus enabling the faithful transmission of quantum data from site to site without detection, as well as the construction of universal quantum computers that carry out quantum logic operations in stealth. We anticipate further
protocols being constructed covertly. For instance, graph states can be generated covertly, which could be used in the study of preexisting protocols and algorithms that require graph states. We are working on the experimental details of our setup towards a proof-of-principle demonstration in the near future.

ACKNOWLEDGMENTS

This material is based upon work supported by the U.S. Air Force Office of Scientific Research under award number FA9550-17-1-0083. The authors also acknowledge support from the U.S. Office of Naval Research (ONR) under award number N00014-15-1-2646.

[1] Paul Syverson, David Goldschlag, and Michael Reed, Anonymous connections and onion routing, *IEEE Symposium on Security and Privacy* (1997). [doi:10.1109/SECPRI.1997.601314]

[2] Manilo De Domenico and Alex Arenas, Modeling structure and resilience of the dark network, *Phys. Rev. E* 95, 022313 (2017). [doi:10.1103/PhysRevE.95.022313]

[3] Seonwoo Lee, Robert Baxley, Mary Ann Weitnauer, and Brett Walkenhorst, Achieving undetectable communication, *IEEE Journal of Selected Topics in Signal Processing* vol. 9 no. 7, 1195–1205 (2015). [doi:10.1109/JSTSP.2015.2421477]

[4] Tamara Sobers, Boulat Bash, Sakat Guha, Don Towsley, and Dennis Goeckel, Covert communication in the presence of an uninformed jammer, (2016). [https://arxiv.org/abs/1605.00127]

[5] Pritam Mukherjee and Sennur Ulukus, Covert bits through queues, *IEEE Conference on Communications and Network Security*, (2016). [doi:10.1109/CNS.2016.7860561]

[6] Luis von Ahn, Nicholas Hopper, and John Langford, covert-party computation, In STOC ’05 *Proceedings of the 37th annual ACM symposium on Theory of computing*, 513–522, New York, NY, USA, 2005, ACM Press.

[7] Nishanth Chandran, Vipul Goyal, Rafail Ostrovsky, and Amit Sahai, Covert multi-party computation, *IEEE Symposium on Foundations of Computer Science*, (2007). [doi:10.1109/FOCS.2007.61]

[8] Stanislaw Jarecki, Practical covert authentication, *Public-Key Cryptography-PKC 2014*, Lecture notes in Computer Science, vol. 8383, (2014). [doi:10.1007/978-3-642-54631-0˙35]

[9] Ignacio Cirac, Peter Zoller, H. Jeff Kimble, and Hideo Mabuchi, Quantum state transfer and entanglement distribution among distant nodes in a quantum network, *Phys. Rev. Lett.* 78, 3221 (1997). [doi:10.1103/PhysRevLett.78.3221]

[10] H. Jeff Kimble, The quantum internet, *Nature* 453, 1023–1030 (2008). [doi:10.1038/nature07127]

[11] Rod Van Meter, Quantum networking, John Wiley & Sons, 2014. [doi:10.1002/9781118648919]

[12] Ignacio Cirac, Artur Ekert, Susana Huelga, and Chiara Macchiavello, Distributed quantum computation over noisy channels, *Phys. Rev. A* 59, 4249 (1999). [doi:10.1103/PhysRevA.59.4249]

[13] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel Braunstein, Advances in quantum teleportation, *Nature Photonics* 9, 641–652 (2015). [doi:10.1038/nphoton.2015.154]

[14] Stefano Pirandola and Samuel Braunstein, Physics: unite to build a quantum internet, *Nature* 532, 169–171 (2016). [doi:10.1038/532169a]

[15] Rodney Van Meter and Simon Devitt, The path to scalable distributed quantum computing, *Computer* vol. 49, 31–42 (2016). [doi:10.1109/MC.2016.291]

[16] Kamil Brádler, Timjan Kalajdzievski, George Siopsis, and Christian Weedbrook, Absolutely covert quantum communication, (2016). [https://arxiv.org/abs/1607.05916]

[17] Richard Jozsa, An introduction to measurement based quantum computation, (2005). [https://arxiv.org/abs/quant-ph/0508124]

[18] Hans Briegel, Daniel Browne, Wolfgang Dür, Robert Raussendorf and Maarten Van den Nest, Measurement-based quantum computation, *Nature Physics* 19–26, (2009). [doi:10.1038/nphys1157]

[19] Daniel Gottesman and Isaac Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, *Nature* 402, 390–393 (1999). [doi:10.1038/46503]

[20] Xinlan Zhou, Debbie Leung, and Isaac Chuang, Methodology for quantum logic gate construction, *Phys. Rev. A* 62, 052316 (2000). [doi:10.1103/PhysRevA.62.052316]

[21] Jens Eisert, Kurt Jacobs, Polykarpos Papadopoulos, and Martin Plenio, Optimal local implementation of nonlocal quantum gates, *Phys. Rev. A* 62, 052317 (2000). [doi:10.1103/PhysRevA.62.052317]

[22] Michael Nielsen, Quantum computation by measurement and quantum memory, *Physics Letters A* Vol. 308, Issues 2–3, 96–100, (2003). [doi:10.1016/S0375-9601(02)01803-0]

[23] Debbie Leung, Quantum computation by measurements, *IJQI* Vol. 308, No. 1, 33–43, (2004). [doi:10.1142/S0219749904000855]
[24] Andrew Childs, Debbie Leung, and Michael Nielsen, Unified derivations of measurement-based schemes for quantum computation, \textit{Phys. Rev. A} 71, 032318 (2005). \texttt{doi:10.1103/PhysRevA.71.032318}

[25] Robert Raussendorf and Hans Briegel, A one-way quantum computer, \textit{Phys. Rev. Lett.} 86, 5188 (2001). \texttt{doi:10.1103/PhysRevLett.86.5188}

[26] Robert Raussendorf and Hans Briegel, Computational model underlying the one-way quantum computer, \textit{Quantum information & Computation} 2, 443–486 (2002).

[27] Robert Raussendorf, Daniel Browne, and Hans Briegel, Measurement-based quantum computation on cluster states, \textit{Phys. Rev. A} 68, 022312 (2003). \texttt{doi:10.1103/PhysRevA.68.022312}

[28] Robert Raussendorf and Hans Briegel, A one-way quantum computer, \textit{Phys. Rev. Lett.} 86, 5188 (2001). \texttt{doi:10.1103/PhysRevLett.86.5188}

[29] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[30] Robert Raussendorf, Daniel Browne, and Hans Briegel, Measurement-based quantum computation on cluster states, \textit{Phys. Rev. A} 68, 022312 (2003). \texttt{doi:10.1103/PhysRevA.68.022312}

[31] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[32] Robert Raussendorf and Kovid Goyal, Topological fault-tolerance in cluster state quantum computation, \textit{New J. Phys.} 9 (2007). \texttt{doi:10.1088/1367-2630/9/6/199}

[33] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[34] Robert Raussendorf, Jim Harrington, and Kovid Goyal, Topological fault-tolerance in cluster state quantum computation, \textit{New J. Phys.} 9 (2007). \texttt{doi:10.1088/1367-2630/9/6/199}

[35] Robert Raussendorf, Dan Browne, and Hans Briegel, Measurement-based quantum computation on cluster states, \textit{Phys. Rev. A} 68, 022312 (2003). \texttt{doi:10.1103/PhysRevA.68.022312}

[36] Robert Raussendorf and Kovid Goyal, Topological fault-tolerance in cluster state quantum computation, \textit{Quantum information & Computation} 2, 443–486 (2002).

[37] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[38] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[39] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[40] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[41] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[42] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[43] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[44] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[45] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}

[46] Robert Raussendorf and Jim Harrington, Fault-tolerant quantum computation with high threshold in two dimensions, \textit{Phys. Rev. Lett.} 98, 190504 (2007). \texttt{doi:10.1103/PhysRevLett.98.190504}