Applications and Use Cases for the Quantum Internet

https://www.ietf.org/id/draft-irtf-qirg-quantum-internet-use-cases-07.txt

Chonggang Wang, Akbar Rahman, Ruidong Li, Melchior Aelmans, Kaushik Chakraborty

IETF 111, QIRG, July 29, 2021

Background of Present I-D v07

- (Mar 10, 2021) v04 was presented in IETF 110.
  - (Mar 29, 2021) v05 was uploaded to address comments received during IETF 110.
  - (May 3, 2021) v06 was uploaded to address the comments on references for “Fast Byzantine negotiation”
- (Jul 12, 2021) v07 was uploaded for IETF 111
  - Added Kaushik Chakraborty (The University of Edinburgh) as a co-author
  - Added three application examples: quantum money, quantum imaging, and quantum chemistry
  - Added the definition for a few terms: ERP Pairs, entanglement swapping, quantum teleportation
  - Some editorial changes and improvements throughput the document

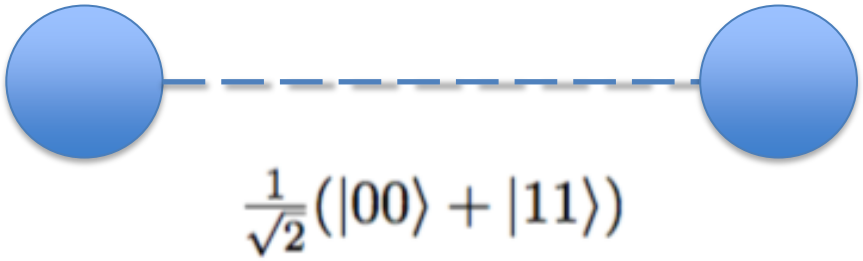
Major Updates since IETF 110

- **2:** Added the definition for several terms:
  - EPR Pairs, Entanglement Swapping, Quantum Teleportation
- **3.2.1:** Added “quantum money” as an additional application
- **3.2.2:** Added “quantum imaging” as an additional application
- **3.2.3:** Added “quantum chemistry” as an additional application
- **4.1:** Added description on MDI-QKD and CV-QKD
- **5.** Made some changes for further clarification

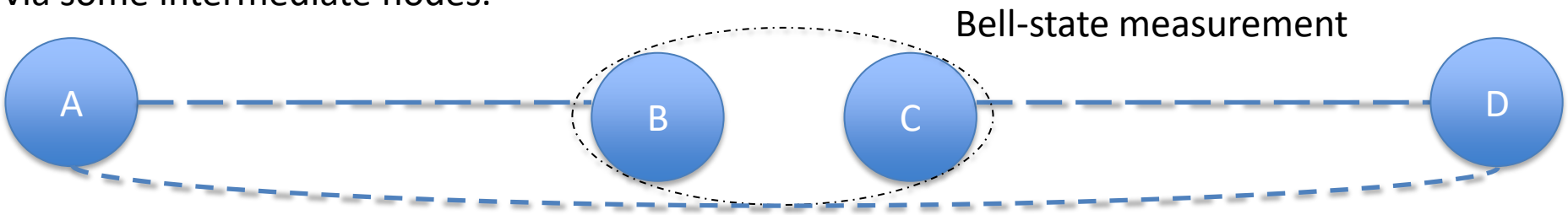
Terms and Acronyms List

(pp.4) EPR-Pairs: A special type of two-qubits quantum states.

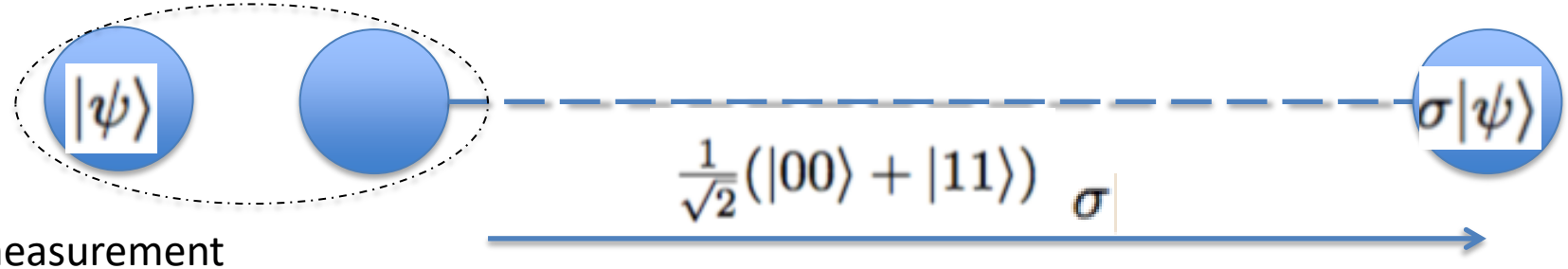
The two qubits show correlations that cannot be observed in classical information theory.



(pp.4) Entanglement Swapping: It is a process of sharing an entanglement between two distant parties via some intermediate nodes.



(pp.5) Quantum Teleportation: A technique for transferring quantum information via local operations and classical communication (LOCC).



Major Update #2: New Application Examples

3.2.1. Quantum Cryptography Applications

- (pp.7)Quantum Money - The main security requirement of money is unforgeability. A quantum money scheme aims to fulfill by exploiting the no-cloning property of the unknown quantum states. Though the original idea of quantum money dates back to 1970, these early protocols allow only the issuing bank to verify a quantum banknote. However, the recent protocols that are called public-key quantum money [Zhandry] allow anyone to verify the banknotes locally.

3.2.2. Quantum Sensor Applications

- (pp.7) Quantum Imaging - The highly sensitive quantum sensors show great potential in improving the domain of magnetoencephalography. Unlike the current classical strategies, with the help of a network of quantum sensors, it is possible to measure the magnetic fields generated by the flow of current through neuronal assemblies in the brain while the subject is moving. It reveals the dynamics of the networks of neurons inside the human brain on a millisecond timescale. This kind of imaging capability could improve the diagnosis and monitoring the conditions like attention-deficit-hyperactivity disorder [Hill].

3.2.3. Quantum Computing Applications

- (pp.8) Quantum Chemistry - Quantum chemistry is one of the most promising quantum computing applications that can outperform the classical strategy using only a few hundred qubits quantum computers. Using the NISQ devices, the quantum algorithms manage to determine the molecular energies of the small molecules within chemical accuracy [YudongCao]. However, due to the short coherence time of the quantum devices, it is still difficult to simulate larger molecules.

Major Update #3: MDI-QKD & CV-QKD

4.1. Secure Communication Setup

- (pp.13) QKD provides an information-theoretical way to share secret keys between two parties in the presence of Eve. However, this is true in theory, and there is a significant gap between theory and practice. By exploiting the imperfection of the detectors Eve can gain information about the shared key [FeihuXu]. To avoid such side-channel attacks in [Lo], the researchers provide a QKD protocol called Measurement Device-Independent (MDI) QKD that allows two users (a transmitter "Alice" and a receiver "Bob") to communicate with perfect security, even if the (measurement) hardware they are using has been tampered with (e.g., by an eavesdropper) and thus is not trusted. It is achieved by measuring correlations between signals from Alice and Bob rather than the actual signals themselves.

- (pp.13) QKD protocols based on Continuous Variable (CV-QKD) have recently seen plenty of interest as it only requires telecommunications equipment that is readily available and is also in common use industry-wide. This kind of technology is a potentially high-performance technique for secure key distribution over limited distances. The recent demonstration of CV-QKD shows compatibility with classical coherent detection schemes that are widely used for high bandwidth classical communication systems [Grosshans].

Next Steps

draft-irtf-qirg-quantum-internet-use-cases-07

- v07 is stable now.

- Do Chairs/QIRG think that the draft v07 is ready for RG Last Call?
  - This question was raised in the last IETF 109/IETF110; as a result, detailed reviews have been conducted and completed.
  - Comments from detailed reviews have been addressed in v07.