

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

	1.	Intr	roduc	tion		•	•		•			•		•										•	2
7	(2.	Tern	ns an	d Acr	onym	s Li	st	•	•	•••	•	•	•	•	• •	•	•	•	•	•	•	•	•	•	3
	3.	Quar	ntum 🛛	Inter	net	App]	ica	ati	on	s.															5
	3	3.1.	Over	view																					5
	-	3.2.	Class	sific	atio	n hv	Δr	on l	ic	ati	on		ag	P											5
		2 2	1 /	Juant		nvnt	1'' ''''''''''''''''''''''''''''''''''	 	hv	4 C I	-1-	ica	,~5 +i	ond		•	•	•	•	•	•	•	•	•	6
		2.2.		Zuant		гурс	.ogi	ah	, 1 J	Ар	μı.		ICT	OIIS	•••	•	•	•	•	•	•	•	•	•	C C
	•	×3.2.	.2. (Juant	um S	ensc	pr /	Abb)11	саτ	10	าร	•	•	•••	•	•	•	•	•	•	•	•	•	6
	-	3.2.	.3. (Quant	um C	ompu	itir	١g	Ар	pli	cat	tic	ns		• •	•	•	•	•	•	•	•	•	•	7
	3	3.3.	Cont	rol v	's Da	ta F	lar	ne	C1	ass	if:	Lca	nti	on		•		•	•	•	•	•	•	•	7
	4.	Sele	ected	Quar	ntum	Inte	erne	et	Us	e C	ase	es													9
	4	1.1.	Secu	re Co	ommun	icat	ior	n S	Set	up															9
	4	1.2	Secu	ce Ou	iantu	m Co	mpi	ıti	nσ	wi	th	Pr	•iv	ac	/ P	re	ser	rv?	ati	on				-	12
	4	1.2.	Secu	re Qu	antu	m Co	mpu	uti	ng	wi +i	th	Pr	i۷	acy	/ P	re	ser	rva	ati	on	1	•	•	•	12 15
	4	1.2. 1.3.	Secu Dist	re Qu ribut	iantu ed Q	m Co uant	ompu :um	uti Co	ng	wi uti	th ng	Pr •	iv •	acy •	/ P 	re •	ser •	rva •	iti •	lor •	•	•			12 15
4	2 2 5.	1.2. 1.3. Gene	Secu Dist eral	re Qu ribut Requi	iantu ed Q. reme	m Co uant nts	ompu um	uti Cc	ng pmp	wi uti 	th ng	Pr •	iv	acy	/ P 	re	ser •	rva •	iti	lon •	•				12 15 18
4	2 2 5.	1.2. 1.3. Gene 5.1.	Secu Dist eral Back	re Qu ribut Requi grour	iantu ed Q reme nd .	m Co uant nts	ompu um	uti Co	ing omp	wi uti • •	th ng ·	Pr • •	`iv	acy • •	/ P 	re • •	ser • •	rva • •	ati	lon • •	•				12 15 18 18
4	2 2 5.	1.2. 4.3. Gene 5.1. 5.2.	Secu Dist eral I Back Requ	re Qu ribut Requi grour ireme	iantu ed Q reme id . ents	m Co uant nts 	ompu :um	uti Co	ing omp ·	wi uti • •	th ng	Pr • • •	`iv	acy	/ P · · · · ·	re	ser	rva	ati	lon • •	•				12 15 18 18 20
4	2 2 5. 5 5.	4.2. Gene 5.1. 5.2. Cond	Secur Dist eral Back Requi	re Qu ribut Requi grour ireme on .	iantu ed Q reme id . ents	m Co uant nts · ·	ompu :um	uti Co · ·	ing omp	wi uti • • • •	th ng	Pr • • •	`iv	acy	/ P · · · · · ·	re	ser • • •	rva	ati	Lon • •	•				12 15 18 18 20 21
4	2 2 5. 5. 5. 5. 5. 7.	1.2. Gene 5.1. 5.2. Cono IANA	Secur Dist eral Back Requi clusic	re Qu ribut Requi grour ireme on . sider	iantu ed Q reme nd . ents	m Cc uant nts · · · · · ·	ompu :um	uti Co	ing omp	wi uti • • • •	th ng	Pr • • • •	`iv	acy	/ P 	re	ser • • •	rva	ati	lon	· · ·		· · · ·		12 15 18 18 20 21 21
4	2 2 5. 5. 5. 5. 7. 8	4.2. Gene 5.1. 5.2. Cond IANA	Secur Dist eral Back Requi clusic Con:	re Qu ribut Requi grour ireme on . sider	iantu ed Q reme nd . ents ratio	m Co uant nts 	ompu :um	uti Co	ing omp	wi uti 	th ng	Pr • • • •	`iv	acy	/ P · · · · · ·	re	ser	°Va	ati	lon	• • • •			• • • •	12 15 18 18 20 21 21 21 22
4	2 2 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5.	1.2. Gene 5.1. 5.2. Conc IANA Secu	Secur Dist eral Back Requi clusio Cons urity	re Qu ribut Requi grour ireme on . sider Cons	iantu ed Q reme nd . ents atio sider	m Co uant nts ns . atic	ompu cum	uti Co	ing omp	wi uti • • • • • •	th ng	Pr • • • •	`iv	acy	/ P 	re	ser	rva	ati	Lon	· · ·	· · · ·	· · · ·		12 15 18 20 21 21 22
4	5. 5. 6. 7. 8. 9.	1.2. Gene 5.1. 5.2. Conc IANA Secu Ackr	Secur Dist eral Back Requ clusic Con urity nowled	re Qu ribut Requi grour ireme on . sider Cons dgmer	antu ed Q reme d . ents ratio sider	m Co uant nts ns . atic	ompu ium ons	uti Co · · ·	ng omp	wi uti 	th ng	Pr • • • • •	`iv	acy	/ P -	re	ser	rva	ati • • • •	lor • • • •	· · · ·	· · · · · · · · ·	· · · · · · · · · · ·		12 15 18 20 21 21 22 23
•	 4 5 6 7 8 9 10 	1.2. Gene 5.1. 5.2. Conc IANA Secu Ackr	Secur Dist eral I Back Requi clusio Cons urity nowled	re Qu ribut Requi grour ireme on . sider cons dgmer ive R	antu ed Q reme nd . ents ratio sider nts . Refer	m Co uant nts ns . atic ence	ompu ium ons	uti Co	ing omp	wi uti 	th ng	Pr • • • • • • • •	`iv	acy • • • • • • • •	/ P 	re	ser	rva	ati	Lor	• • • • • • • • •	· · · · · · · · · · · · · · · · · · ·	· · · · ·	· · · · · · · · · · · ·	12 15 18 20 21 21 22 23 23

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).



 $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

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 highperformance 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.