A cryptographic route to the reality of the quantum state[2]
QICF-2017, NIT-Patna

R. Srikanth
Poornaprajna Institute of Scientific Research
Bengaluru, India.

[2] arXiv:1708.04964

Introduction: Quantum bit commitment

- Quantum bit commitment (QBC) is a cryptographic mistrustful task: Alice commits bit a by submitting evidence E, possibly after multiple rounds of QC. Sometime later, she unveils a.
- Security requirement: Evidence binds Alice to a, while hiding a from Bob.
- Bit commitment (BC)– a primitive for important crypto-tasks, among them coin flipping, oblivious transfer, secure multi-party computation, signature schemes and zero-knowledge proofs.
- Except by invoking computational assumptions, a trusted third party or relativistic constraints on signaling (Kent 1999; 2012; Lunghi et al. 2013; 2015), secure QBC (and hence BC) conventionally not believed possible.

No-go theorem for non-relativistic QBC in std framework

(Mayers 1997; Lo & Chau 1997; Chiribella et al. 2013)

- Ensembles $\mathcal{E}^\alpha \equiv \{|\tilde{\chi}_j^\alpha\rangle = \sqrt{p_j^\alpha}\,|\chi_j^\alpha\rangle\}$ of E corresponding to commitment bit α.
- Condition for concealment from Bob: $\rho_B^0 = \rho_B^1$, where $\rho_B^\alpha = \sum_j |\tilde{\chi}_j^\alpha\rangle\langle\tilde{\chi}_j^\alpha|$ and $\alpha \in \{0,1\}$.
- To cheat, Alice submits the second register of purification $|\Psi\rangle \equiv \sum_j |\phi_j^0\rangle|\tilde{\chi}_j^0\rangle$ where $|\phi_j^0\rangle$'s form an orthonormal basis.
- To unveil α, she measures the first register in the basis $\{|\phi_j^\alpha\rangle\}$ and unveils outcome j, where $\{|\phi_j^1\rangle = \mathcal{U}|\phi_j^0\rangle\}$, (Hughston et al. 1993) $|\tilde{\chi}_k^0\rangle = \sum_j U_{jk}|\tilde{\chi}_j^1\rangle$.
- Manifestation of quantum steering (Wiseman et al. 2007).

BC in a generalized probability theory

- Interestingly, an analogous attack on a BC protocol using steering correlations can be demonstrated (DiSilvestro & Markham, 2017) in the toy nonclassical theory due to Spekkens (Spekkens, 2007), which features steering but not contextuality and nonlocality.
- Sikora and Selby (2017) find that any GPT satisfying (a) the no-restriction assumption (the state space of a physical theory determines the set of measurements) [Janotta and Lal, 2013] and (b) allowing state purification enables entanglement $\Rightarrow$ the steering required for attacks on BC of the above type.

End of road for QBC?

In response to the steering attack:

- Various works have studied cheat sensitive QBC, relaxing the hiding requirement to $\rho_0^B \neq \rho_1^B$ (He 2015, and references therein).
- It's been asked: Is this framework of mistrustful quantum cryptography broad enough to truly rule out secure QBC (He 2011, 2014, 2017; Yuen 2008 and 2012; Chen 2015; Song 2017)?
- If not, the no-QBC result, unlike no-cloning or no-signaling, is dependent on the communication framework used, and isn't fundamental.
- Our point of departure is to note & relax two assumptions in standard communication framework for QBC.

Identifying assumptions in the std. communication framework for QBC

- Two assumptions implicit in this framework: (a) Alice knows the ensembles of evidence E corresponding to either commitment; and (b) system E is quantum rather than classical.
- We find: relaxing assumption (a / b) $\rightarrow$ we obtain protocols with malicious steering operation $\mathcal{U}$ becoming (indeterminable / inexistent)
- Third protocol, extending the second to an entanglement-based setting. Without appeal to an ontological framework, we find that security $\Rightarrow$ reality of the quantum state (barring retrocausality).
- We find: both no-go theorem for BC in the std framework, as well as security of BC in relaxed framework, hold good for Spekkens toy model and a wider class GPTs, even transitive GPTs (S. Aravinda, RS and A. Pathak 2017).

Relaxing assumption (a)

- Let Alice lack full knowledge of $\{|\tilde{\chi}_j^{\alpha}\rangle\}$, say because of secret choices of Bob, and thus of cheat unitary $\mathcal{U}$.
- But this may over-empower Bob. Thus, let $\{|\tilde{\chi}_j^{\alpha}\rangle\}$ also depend on secret parameters held by Alice.
- Thus, some sort of two-way secrecy needed: protocol must be "double-blind".
- Forms the basis of our protocol P1.

Relaxing assumption (b)

- QBC protocol with classical evidence E trivially protected against the steering attack in QM or a GPT.
- This doesn't reduce to classical BC (Goldreich 2009), which is only computationally secure: given intermediate stages involving quantum (nonclassical) communication and operations.
- Instead, a protocol relaxing (b) can be thought of as realizing a "classical-valued quantum one-way function".
- But other attacks would still exist. Design must ensure that privacy of Bob's input will bind Alice, while the privacy of Alice's input will provide the requisite one-wayness to conceal the commitment. $\Rightarrow$ double-blindness
- Basis of our protocol P2.

Three phases of a BC protocol

1. Commit phase: Alice submits evidene E.
2. Holding phase: of arbitrary time, during which commitment stays "alive".
3. Unveiling phase: Alice submits additional evidence.

Protocol P1: Commit phase

$(C1)_{P1}$ Bob transmits to Alice $2n$ "single-blind" (i.e., unknown to Alice) random qubit states $|\phi_j^{(\alpha)}\rangle \in \{|0\rangle, |1\rangle, |\pm\rangle\}$, where $\alpha \in \{0, 1\}$, $0 \leq j < n$, indicating the two sets to her. (Alternatively, he could submit halves of Bell states, deferring measurement in X or Z basis on the "home" qubits until later.) Additionally, he supplies Q extra qubits prepared in pure states unknown to her (or as halves of singlets), where $Q \gg n$.

$(C2)_{P1}$ Alice prepares Q "decoy" qubits by quantum encrypting the states of the extra qubits. We denote the $2Q$ bits of encryption information $\mathcal{R}_Q$. To commit to bit a, she inserts the n states $|\phi_j^{(a)}\rangle$ at positions W among the Q decoys, and then rearranges all $n + Q$ qubits using permutation $\mathcal{P}$.

$(C3)_{P1}$ She transmits back to Bob these $n + Q$ qubits as evidence E of her commitment.

Protocol P1: Unveil phase

$(\mathrm{U1})_{P1}$ Alice announces a, $\mathcal{P}$, $\mathcal{R}_Q$ and positions W. She returns the n qubits of her non-commit state $|\phi_j^{(\bar{a})}\rangle$.

$(\mathrm{U2})_{P1}$ Bob extracts the n commit qubits from evidence E using information and $\mathcal{P}$ and W. He verifies that they are the states $|\phi_j^{(a)}\rangle$. Further, he verifies that the n non-commit qubits returned in step $(\mathrm{U1})_{P1}$ are the states $|\phi_j^{(\bar{a})}\rangle$. Finally, using information $\mathcal{P}$ and $\mathcal{R}_Q$, he checks that the Q decoys are indeed the extra qubits sent by him.

Protocol P1: Security against Bob

- Basic idea: "Commitment signal" swamped by large decoy noise: State of evidence with him:

$$\rho_B^a = \mathcal{P}\left[\bigotimes_j \left(|\phi_j^{(a)}\rangle\langle\phi_j^{(a)}|\right) \otimes \left[\frac{\mathbb{I}}{2}\right]^{\otimes Q}\right], \tag{1}$$

  where $\mathcal{P}$ is to him a random permutation.

- On can show that fidelity $F(Q,n) \equiv \mathcal{F}\left(\rho_B^a, \left(\frac{\mathbb{I}}{2}\right)^{\otimes(Q+n)}\right)$ satisfies

$$F(Q,n) \geq 1 - 2^{-Q(1-H(n/Q))}, \tag{2}$$

  (for details, see arXiv:1607.01768 Appendix 1)

Protocol P1: Security against Alice

- **Key point:** Steering based attack not possible because cheat unitary $\mathcal{U}$ such that $|\tilde{\chi}_k^0\rangle = \sum_j U_{jk}|\tilde{\chi}_j^1\rangle$ depends on commit ensembles (they needn't be!!) and the ensembles are unknown to her: $\mathcal{U}$ can't be computed by her.
- **Other attacks:**
  1. Can't include both $|\phi_j^0\rangle$ and $|\phi_k^1\rangle$ among the decoys– because (1) she must return non-commit qubits; (2) quantum disencrypted decoys must match his preparation.
  2. Can't use port-based teleportation (Ishizaka 2008;2009) because decoys must be quantum disencryptable to Bob's prepared states.
  3. Other, more obvious (simpler) attacks can be ruled out.

Superposition attack on P1: less dangerous

- Bob still vulnerable to a probabilistic attack:
- With a quantum computer, Alice produces the state:

$$\sum_{a=0}^{1} \gamma_a |a\rangle_{A'} \otimes |\Phi^{(\bar{a})}\rangle_{\text{keep}} \otimes |\Phi^{(a)}\rangle_{\text{encrypt}}, \tag{3}$$

  Alice can unveil bit α with probability $|\gamma_\alpha|^2$.
- Thus, P1 lacks classical certification (CC) of commit bit.
- Lack of CC is a feature shared with some other proposed QBC protocols, such as the relativistic BC protocols.

Protocol P2: Commit phase

$(C1)_{P2}$ Alice transmits to Bob $2n$ qubits randomly prepared in states $|\psi_k\rangle \in \{|0\rangle, |1\rangle, |\pm\rangle\}$.

$(C2)_{P2}$ Bob randomizes their each basis (by random application of I or H); randomizes their bits by quantum encryption, and randomizes position via permutation $\mathcal{P}$.

$(C3)_{P2}$ Bob returns these double-blind states, denoted $|\phi_j\rangle$.

$(C4)_{P2}$ Alice picks out n of the transmitted states, and asks Bob to reveal his randomizing operations, to check that they are indeed qubits she had sent. These n check qubits are discarded. If check fails, protocol aborted.

$(C5)_{P2}$ To commit to $a = 0$ (resp., $a = 1$), she measures the remaining n states $|\phi_j\rangle$ in basis Z (resp., X). The n-bit random outcome string is denoted M.

$(C6)_{P2}$ She announces M as evidence of her commitment.

Protocol P2: Unveil phase:

$(U1)_{P2}$ Alice announces a and her preparation information of the qubits $|\psi_k\rangle$.

$(U2)_{P2}$ From the latter, Bob obtains complete classical knowledge of all $2n$ states $|\phi_j\rangle$.

$(U3)_{P2}$ Bob verifies that the string M is compatible with the measurement of states $|\phi_j\rangle$ in the basis Z (resp., X) if $a = 0$ (resp., $a = 1$).

Protocol P2: Security against Bob

- Before Unveiling, he lacks classical knowledge of $|\psi_j\rangle$, and hence of $|\phi_k\rangle$. Therefore, M reveals to him nothing about a.
- Let $\mathcal{R}$ denote the classical information about Bob's randomization operations. Then P2 satisfies the condition:

$$H(\alpha|M,\mathcal{R}) = 1, \tag{4}$$

  i.e., the conditioning on information M and $\mathcal{R}$ does not lower his ignorance about her commitment.
- Bob can't substitute his own states in step $(C3)_{P2}$, nor measure Alice's qubits, since such actions would generate disturbance as that would be detected in her check $(C4)_{P2}$.

Protocol P2: Security against Alice

- Steering or superposition attack trivially impossible– evidence E is *classical* information. Malicious steering operation $\mathcal{U}$ simply doesn't exist. But other attacks must be ruled out.
- She's maximally ignorant of states by measuring which she generates string M. Thus, she can't confidently unveil a fake measurement basis.
- The scrambling action important. Without it, Alice can launch a local entanglement attack described below.

Protocol P2: Security against Alice (contd.)

In $(C1)_{P2}$ she sends half a singlet $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This becomes:

Bob's action	Alice's state
II, IZ	$\|00\rangle \pm \|11\rangle$
IX, IY	$\|01\rangle \pm \|10\rangle$
HI, HX	$\|0+\rangle \pm \|1-\rangle$
HZ, HY	$\|0-\rangle \pm \|1+\rangle$,

(5)

Alice measures in Bell basis $\{|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle\}$. Suppose she finds outcome $|00\rangle - |11\rangle$. From Eq. (5) it follows that Bob couldn't have applied the three operations: II, IX, IY.

Protocol P2: Why Bob must randomize qubit positions

The 4 honest states that would result under Bob's remaining 5 possible randomization actions are:

$\|\psi_j\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
IZ	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$
HI	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$
HX	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$
HY	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$
HZ	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$

(6)

Alice announces an arbitrary bit as measurement outcome in step $(C6)_{P2}$, say $M_j = 0$. To unveil $a = 0$ (resp., $a = 1$), she must claim $|\psi_j\rangle = |0\rangle$ (resp., $|\psi_j\rangle = |-\rangle$), since all 5 states in this column consistent with claimed outcome M_j upon her measuring Z (resp., X);
whereas if $M_j = 1$, then to unveil $a = 0$ (resp., $a = 1$), she must claim $|\psi_j\rangle = |1\rangle$ (resp., $|\psi_j\rangle = |+\rangle$).
Given exponentially large number of permututations to scramble his qubits, Alice has hardly partner the right two entangled qubits.

Protocol P3: Motivation

- Simple extension of protocol P2 to a nonlocal scenario, such that security proof of P3 reduces to that of P2.
- P3 is proposed, not as an actual protocol for practical use, but instead to point out that security of P3 has foundational implications for the nature of the quantum state.
- It's argued that P3's security implies the reality of the quantum state– employing only operational considerations and without recourse to any ontological framework.

Protocol P3: Commit phase

- Same as P2, except: In $(C3)_{P3}$, Bob additionally transmits $\frac{n}{2}$ halves of singlets.
- In $(C5)_{P3}$, additionally Alice measures the singlet-halves sent by Bob in the basis Z (resp., X) basis, if corresponding bit in the second half of M is 0 (resp. 1). Outcomes constitute $\frac{n}{2}$-bit string M_2.
- In $(C6)_{P3}$, Alice transmits the first $\frac{n}{2}$ bits of M as before (denote this string by M_1). Further, she transmits the $\frac{n}{2}$ bits M_2.
- Thus, Alice's evidence E is the classical string $M_1 * M_2$.

Protocol P3: Unveil phase

- Similar to that of Protocol P2, except:
  In $(\mathrm{U1})_{P3}$, Alice additionally transmits $\overline{M_1}$, which is the remaining $\frac{n}{2}$ bits of M.
- In $(\mathrm{U3})_{P3}$, Bob checks that the outcomes M_2 are compatible with measuring his halves of the singlets in the bases specified by $\overline{M_1}$.

Security sketch of P3

- In protocol P3, set $n \to 2n$, and suppose that Alice and Bob ignore the M_2 part.
- Resulting protocol at least as secure as protocol P2 on n bits. $\Longrightarrow$ P3 secure, given the security of P2.
- Nota: M_2 reaches Bob at the end of the commit phase, entailing that the singlet halves on his side are already remotely prepared.

Physical interpretation of P3's security

- Conventionally: Suppose distant stationary players Alice and Bob measure an entangled quantum state, in their common reference frame (Chronology: Alice $\rightarrow$ Bob)
- According to Alice, there's a **spacelike** update to the description of Bob's state after her measurement.
- But, Bob's reduced density operator ρ_B remains unchanged. If he measures subsequently, the joint statistics will be independent of the time-ordering of their measurements.
- Such nonlocal correlations don't admit a "clean" causal story in that $\neg\exists$ definite time ordering behind correlations (cf. Suarez 2001).
- This situation lies at the heart of the dilemma regarding whether Bob's state's changed status as a result of Alice's measurement is an *objective* transformation (i.e., a genuine ontological change in the state of Nature) or a *subjective* transformation (i.e., just a Bayesian or epistemic update of her knowledge state) concerning his system's quantum state.

How does that situation change now?

- This cryptographic scenario of QBC imposes temporal asymmetry between the agents. A natural time ordering exists: committer Alice $\rightarrow$ verifier Bob.
- EPR-certificate: $2 \times \frac{n}{2}$-bit basis+outcome specification, that can pass Bob's check for outcome-matching in step $(\mathrm{U3})_{P3}$ *with complete certainty*, in support of some commitment.
- In the terminology of [**EPR35**], the EPR-certificate associates an "element of reality" to the commitment encoded in the $\frac{n}{2}$ home qubits of Bob.
- Security of P3 $\Rightarrow$ after Alice's entanglement breaking event $\mathfrak{B}$ in $(\mathrm{C5})_{P3}$, Alice can help construct an EPR-certificate for commitment a and none for $\bar{a}$ (though she may not have the certificate's complete classical description.)
- Her commit action remotely irreversibly prepares Bob's state in such a way that it breaks the symmetry that priorly existed between both commitments.

Where to position the symmetry breaking (SB)?

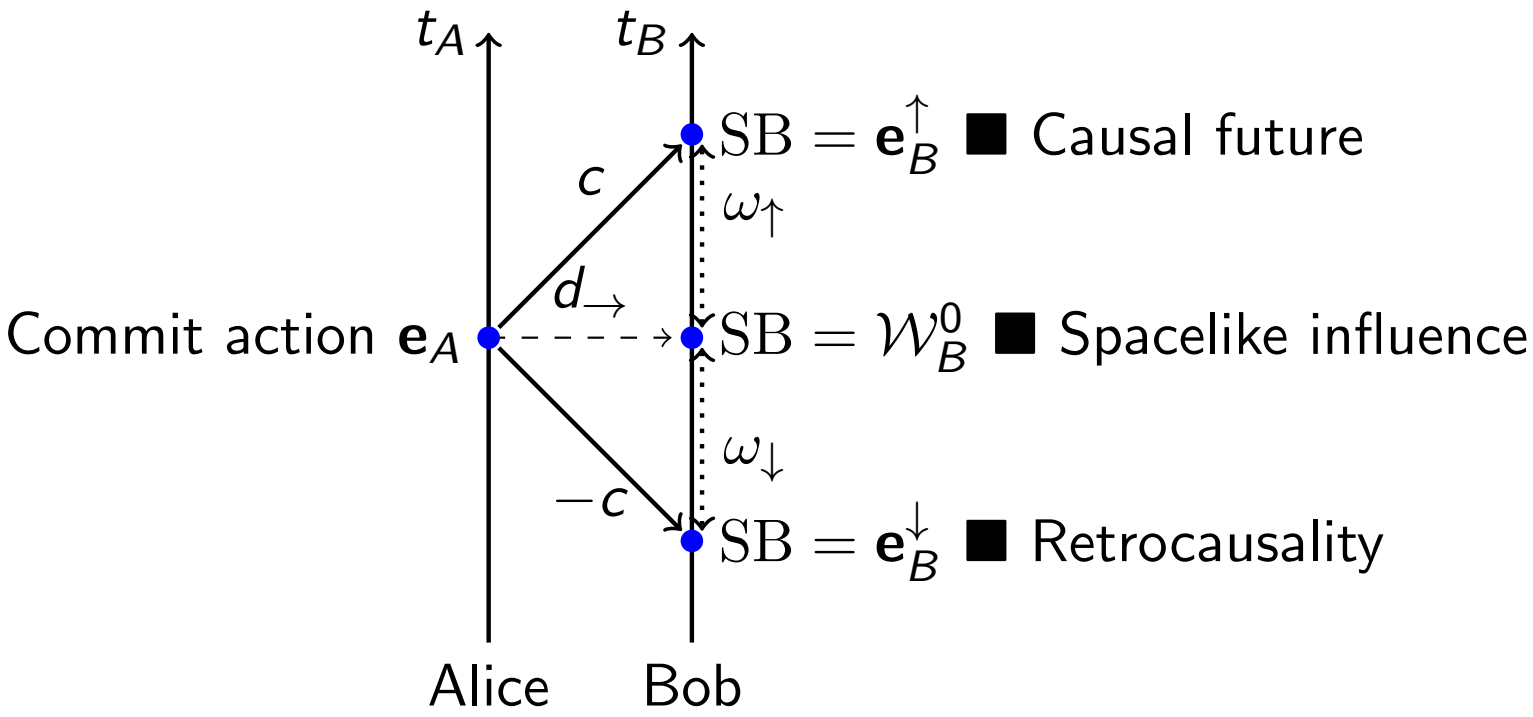

Figure : Alice and Bob are distant, stationary observers. Problem is: Alice's choice must be causally correlated with symmetry breaking.
$\mathrm{SB} \equiv e_B^{\uparrow} \Rightarrow$ correlation breakdown– ruled out by loop-hole free tests of Bell's inequality (Hensen et al. [2015])
$\mathrm{SB} = e_B^{\downarrow}$ or $\mathcal{W}_B^0$?

Spacelike influence

- Barring retrocausality, symmetry breaking is associated with a spacelike influence.
- No overt conflict with relativistic no-signaling, since it is only a verifiable transformation, and not unilaterally detectable.
- But relativistic causality forbids any dynamic mechanism $\Rightarrow$ quantum state vector itself, whose reduction forms the basis for predicting the broken symmetry, must supply this causal channel.
- In this sense, the state vector is a real entity.
- Note that this argument requires no assumptions about an ontological model for QM (Leifer, 2014).

Helpful analogy

In computational complexity, two basic classes are **P** (set of problems that are easy to compute) and **NP** (whose yes-certificate can be easily verified.) State transformations (Bob's, in this case) may be thought of as measurement analogues: those that are unilaterally detected (**D**) vs those that can be verified (**V**).

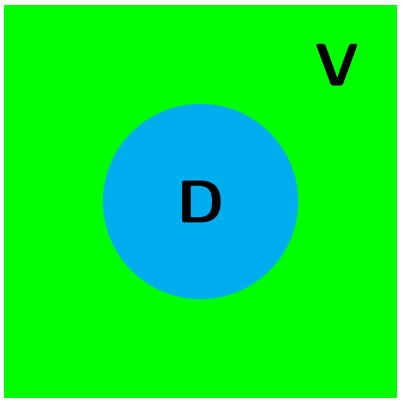

Figure : **D** (detectable) and **V** (verifiable) transformations. Classically, only **D** admissible.

Resources

- Our argument for reality didn't require quantum nonlocality but only quantum remote state preparation, a weaker resource.
- The steering-based attack on bit commitment in the standard framework possible (DiSilvestro & Markham, 2017) in Spekkens' toy theory (Spekkens 2007), a theory without nonlocality, but permitting teleportation and steering.
- Our protocols P1, P2 and P3 can also be formulated securely in the toy theory.
- Our argument applied to Spekkens toy theory would imply the reality of the so-called "epistemic states" of the toy theory !

Conclusions and discussions– 1

- The no-go theorem for quantum bit commitment (QBC) in the standard non-relativistic framework is a consequence of Alice exploiting quantum steering to unveil either commit bit.
- Holds true in Spekkens' toy theory and GPTs that support steering.
- Various authors have questioned whether the generality of this framework.
- In line with this, we identified two implicit assumptions: (a) that Alice's submitted evidence exists in an ensemble known to her; and (b) that E is a quantum– and not a classical– system.
- Relaxing (a), we construct a QBC protocol (P1), where security arises from Alice's inability to determine the malicious steering operator $\mathcal{U}$.
- However, protocol P1 still allows Alice's superposition attack $\Rightarrow$ lacks certificate of classicality (CC), in common with various relativistic bit commitment protocols.
- Relaxing assumption (b), we present a second QBC protocol (P2), where security arises from the inexistence of $\mathcal{U}$. Guarantees CC.

Conclusions and discussions– 2

- Finally, we propose a third protocol that extends P2 in an entanglement setting.
- Alice's free will + P3's security entails a directed superluminal *influence* (not signaling).
- Influence can't be attributed to a signal or dynamical mechanism $\Rightarrow$ reality of the quantum state.
- Both the insecurity of BC in the standard framework, and its security in the relaxed framework, appear to hold in any GPT that admits remote preparation (nonlocality not necessary).
- The security argument can similarly be used to establish the reality of the quantum (nonclassical) state in the GPT. – "Poison is the cure".

Thank you!