Testing the Quantum Anonymous Transmission Protocol*

L. Ceragioli[a], F. Gadducci[b], G. Lomurno[b] and G. Tedeschi[c]

[a] IMT School for advanced studies Lucca, Lucca, Italy
[b] University of Pisa, Pisa, Italy
[c] Université Paris Cité, CNRS, IRIF, F-75013, Paris, France

ARTICLE INFO

Keywords:
Quantum Communication
Process Calculus
Testing Equivalence
Cryptographic Protocol
Anonymity
Formal Verification

ABSTRACT

Whereas most quantum protocols are described in natural language and rarely analysed through the lens of formal methods, modern quantum network infrastructures demand rigorous guarantees of correctness and security. Process calculi represents a natural candidate for quantum protocol verification, given their effectiveness in modeling and analysing distributed systems. In this paper, we put forward a testing semantics for a quantum extension of value-passing CCS, resorting to concrete experiments that a user can perform to investigate protocol properties. To guarantee strict adherence to the laws of quantum mechanics, we integrate an explicit treatment of non-determinism, thereby preventing unphysical behaviors such as extracting the state of a qubit without measurement-induced collapse. We put to work our formal development on a real-world case by analysing the *Quantum Anonymous Transmission Protocol*. This protocol leverages local operations and entangled state measurements to allow participants to broadcast classical bits anonymously. Using our approach, we formally prove the correctness of the protocol (showing that bits are broadcast as if over a standard classical channel) as well as its relevant security properties, namely anonymity under various attacker models.

1. Introduction

Modern communication technology is undergoing a paradigm shift driven by the practical rollout of quantum network infrastructures (Elder, Giemsa, Gunkel, Nikiforov and Wissel, 2024; Liu, Le, Ji, Yu, Farfurnik, Byrd and Stancil, 2025). Exploiting intrinsic quantum properties like entanglement and state superposition allows these networks to guarantee eavesdropping immunity at the physical layer (Bennet and Brassard, 2014) and surpass classical limits in resource efficiency (Brassard, 2003). This has led to the design of quantum protocols for a wide range of distributed tasks (Singh, Doosti, Mathur, Delavar, Mantri, Ollivier and Kashefi, 2023), including quantum key distribution (Nurhadi and Syambas, 2018) and Byzantine agreement (Ben-Or and Hassidim, 2005). Because these protocols operate in security-critical environments and incur substantial deployment costs, establishing their correctness and security through rigorous formal verification techniques is of paramount importance.

The introduction of a novel paradigm requires rethinking the verification mechanisms. We address this challenge from a foundational perspective, investigating testing semantics for lqCCS, a quantum extension of value passing CCS. Several proposals have been advanced for lqCCS (Ceragioli, Gadducci, Lomurno and Tedeschi, 2024c,b; Ceragioli, Lomurno and Tedeschi, 2025b; Ceragioli, Gadducci, Lomurno and Tedeschi, 2026), mostly taking *bimisilarity* as the behavioural equivalence of choice. Here, we investigate testing semantics, thus characterizing the distinguishing capabilities of a quantum capable observer with an operational approach (De Nicola and Hennessy, 1984; De Nicola, 1986). Tests, intended as specific processes with a distinct success state ω, have proven successful in characterizing the observable properties of systems for both the classical and the probabilistic case (van Glabbeek, 1990; Larsen and Skou, 1991; Yi and Larsen, 1992; Bernardo, De Nicola and Loreti, 2014). Noticeably, testing semantics is coarser than bisimilarity in discriminating processes based on their branching structure (De Nicola and Hennessy, 1984).

Although the behaviour of quantum systems is probabilistic in nature, simply resorting to probabilistic testing is not sufficient for modelling the unique observational limitations of quantum entities. As detailed in (Ceragioli et al., 2024c), an explicit treatment of non-determinism is needed for preventing processes from evolving with spurious moves that do

* This research is partly supported by the European Union through the MSCA-SE project QCOMICAL (Grant Agreement ID: 101182520).

lorenzo.ceragioli@imtlucca.it (L. Ceragioli); fabio.gadducci@unipi.it (F. Gadducci); giuseppe.lomurno@phd.unipi.it (G. Lomurno); gabriele.tedeschi@irif.fr (G. Tedeschi)
ORCID(s): 0000-0002-1288-9623 (L. Ceragioli); 0000-0003-0690-3051 (F. Gadducci); 0009-0000-0573-7974 (G. Lomurno); 0009-0002-5345-9141 (G. Tedeschi)

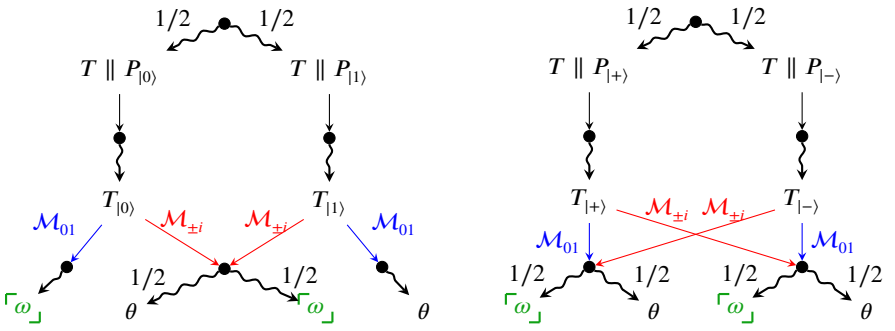


Figure 1: Observer in parallel with a qubit source.

not abide to the rules of quantum theory, e.g. revealing the state of a qubit without measurement-induced perturbation. This is true also for testing semantics, as exemplified by the following example.

Example 1. *Consider two qubit sources: the first sends a qubit either in state* $|0\rangle$ *or* $|1\rangle$ *with equal probability, the second sends a qubit either in state* $|+\rangle$ *or* $|-\rangle$*. Quantum theory deems the values of the received qubits indistinguishable, as they yield the same result under any possible measurement. Nonetheless, consider a test* T *that receives the qubit and chooses non-deterministically which measurement to perform between* $\mathcal{M}_{01}$ *and* $\mathcal{M}_{\pm i}$*. When performing* $\mathcal{M}_{01}$*, the test always succeeds if the qubit is* $|0\rangle$*, succeeds with probability* $1/2$ *if it is* $|+\rangle$ *or* $|-\rangle$*, and always fails for* $|1\rangle$*; when performing* $\mathcal{M}_{\pm i}$*, the test succeeds with probability* $1/2$*, regardless of the state of the qubit. Figure 1 presents the evolution of the two sources paired with the test, where* $P_{|\psi\rangle}$ *is a process that sends a qubit in state* $|\psi\rangle$*, and* $T_{|\psi\rangle}$ *is the observer after receiving a qubit in state* $|\psi\rangle$*. Straight arrows model actions, while the squiggly ones represent the elements of a distribution, labelled by the probability (we omit* 1*). Note that success* ω *or failure* θ *depend on the result of the measurement (success states are marked and highlighted in green). Take the system on the left. If the measurement is chosen according to the value of the received qubit, the observer can perform* $\mathcal{M}_{01}$ *when receiving* $|0\rangle$ *and* $\mathcal{M}_{\pm i}$ *otherwise, therefore obtaining the success state with probability* $3/4$*. The system on the right cannot replicate this behaviour, thus* T *distinguishes the two sources. This contradicts the prescriptions of quantum theory: it should be impossible to know the quantum state without first performing a measurement, hence such a combination of non-deterministic choices is not physically plausible.*

Following the approach of Ceragioli et al. (2024b, 2026), we adopt syntactic schedulers: we explicitly tag the possible scheduling choices and call a list of chosen tags a scheduler. Each scheduler defines a resolution, i.e. a transformation of the transition system that removes non-determinism leaving only probabilistic branching. Enriching our testing semantics with such schedulers imposes that tags are chosen coherently (Bernardo, 2022), therefore forbidding the ill-defined non-determinism that violates the prescriptions of quantum theory. For example, in the case of the two sources above, the test cannot mix the two measurements, hence we must choose either always $\mathcal{M}_{01}$ or always $\mathcal{M}_{\pm i}$. Intuitively, we proceed as follows: we associate each measurement with a different tag, visually represented as colours in Figure 1; then, we compute all and only the schedulers that chose a single tag for each execution step; finally, we compare the resulting success probabilities. For each transition systems, only two of the four possible resolutions are considered: black arrows followed by blue arrows, or black arrows followed by red arrows. Indeed, ignoring ill-defined resolutions (mixing blue and red moves) suffices to recover the indistinguishability of the two qubit sources.

Recently there has been a surge of interest in verifying quantum protocols. Yet, most of them are still only given informally in natural language (Singh et al., 2023). To foster the adoption of formal methods in modelling and verifying real-world quantum protocols, we put our approach to work on a concrete example, namely, the *Quantum Anonymous Transmission Protocol* (Christandl and Wehner, 2005). Such protocol allows any of n players to broadcast one bit of classical information anonymously. More in detail, each participant must start the protocol with a qubit in a given entangled state. The sender applies a local operation to its qubit, altering the state of all n qubits thanks to entanglement. Then, every participant measures its qubit and broadcasts the outcome. The parity of the communicated bits encodes the message of the sender. Anonymity of the protocol consists in the fact that no other player can derive the identity of the sender. Another notable property of the protocol with respect to its classical counterparts is that it is traceless: the sender can always deny having sent, even if the attacker has access to the internal states of all the players. We formalize

the protocol in lqCCS, and we employ our testing theory to prove its correctness: the bit is correctly communicated as if it were broadcast on a classical channel. In addition, no test can tell which participant is the sender, even if they have access to all the quantum data. This assessment on a real-world protocol exemplifies how our approach can certify correctness and relevant security properties.

This submission combines two of Gianluigi's strongest interests: process calculi and cybersecurity. Concrete case studies must always drive research, since only from real-world applications you may infer the right abstractions. Gianluigi has always been a strong advocate of such approach in his research work and in his teaching, and we hope that he will find that our small contribution fits in this view. The present paper can be seen as a follow-up to *Testing quantum processes*, which has been presented at the Rocco De Nicola's Festschrift (Ceragioli, Gadducci, Lomurno and Tedeschi, 2024d). There, we started investigating testing semantics for distributed quantum systems. It thus seems fitting that this submission is intended for Gianluigi's Festschrift, since he and Rocco have been partners in various projects and initiatives in cybersecurity, and frequently coauthors.

Related Works. Different proposals for behavioural equivalences have been put forward for quantum process calculi, mostly focusing on bisimulations (Lalire, 2006; Feng, Duan, Ji and Ying, 2007; Feng, Duan and Ying, 2012; Feng et al., 2007, 2012; Ceragioli et al., 2024c; Feng and Ying, 2015; Deng, 2018; Ceragioli, Gadducci, Lomurno and Tedeschi, 2024a; Ceragioli, Di Lavore, Lomurno and Tedeschi, 2025a; Ceragioli et al., 2024b, 2026). As previously argued, testing equivalences (De Nicola and Hennessy, 1984) are well-suited to capture the intuitive notion of equivalence for non-deterministic quantum systems: two processes should be equal when there is no quantum-enabled test capable of distinguishing them. Since quantum agents are essentially probabilistic systems, we resort to probabilistic testing semantics for probability *Labelled Transition Systems* (pLTSs) (Bernardo et al., 2014), extending it to the quantum case with the introduction of quantum primitives.

A critical discrepancy between concrete quantum systems and their process calculi modelling was noted early on (Kubota, Kakutani, Kato, Kawano and Sakurada, 2012, 2016; Davidson, 2012): processes that are physically indistinguishable may be discriminated by the proposed behavioural equivalences (e.g., the two sources of Example 1). As shown by Ceragioli et al. (2024c), this is because the standard probabilistic approach implicitly permits non-deterministic choices that do not abide the observational limitations prescribed by quantum theory. As a solution, we adopt the approach of Ceragioli et al. (2024b, 2026) by using schedulers that forbid non-deterministic choices based on unknown qubits. Scheduled semantics are introduced in Chatzikokolakis and Palamidessi (2007), and tagged processes are used in probabilistic systems for characterizing which choices are "admissible" or "realistic" (Canetti, Cheung, Kaynar, Liskov, Lynch, Pereira and Segala, 2006; Andrés, Palamidessi, van Rossum and Sokolova, 2011; Song, Feng and Zhang, 2015). A close inspiration for our tags are Chatzikokolakis and Palamidessi (2007); Chatzikokolakis, Norman and Parker (2009), where schedulers prevent processes from choosing a move based on private data, but our constraints are motivated by the physical limitations prescribed by quantum theory instead of secrecy assumptions. The formalization of Bernardo et al. (2014) considers resolutions defined directly on pLTSs, where non-determinism is resolved without the need of annotating the processes syntactically. Building on this, Bernardo (2022) constrains non-determinism by defining a set of *coherent resolutions*. This approach is alternative to ours, yet it shares the same objective and also relies on a labelling policy (although applied directly to the pLTS transitions instead of syntactic processes). However, a thorough comparison is left as future work: resolving non-determinism directly in the pLTSs is admittedly more direct and allows an elegant coalgebraic treatment (Bonchi, Sokolova and Vignudelli, 2022); however, omitting syntactic schedulers obscures the operational interpretation of the constraints that we impose on non-determinism, making it harder to verify their physical plausibility.

In Ceragioli et al. (2025b) and Ceragioli et al. (2024d), we have shown that the impact of unconstrained non-determinism is disruptive for behavioural equivalences along all the linear-time/branching-time spectrum. In particular, Ceragioli et al. (2024d) presents a preliminary version of a testing semantics for quantum processes, where ad hoc syntactic assumptions constrain non-determinism only in tests. In contrast, our current proposal is more mature: by resorting to the more standard technique of syntactic schedulers, we treat non-determinism in a coherent and physically admissible way both in processes and tests. Finally, we put to work our theoretical results on a concrete cryptographic protocol, showing how they can be used to prove security properties, in addition to guaranteeing correctness when agents act honestly. Mousavi, Peters and Schmitt (2024) reviewed the existing bisimilarites for quantum process calculi and discuss the need for a formal testing semantics, its desired features and main challenges. Among the challenging properties that they list, we address the critical one of guaranteeing adherence with respect to quantum theory with a formally grounded approach, yet still allowing for non-determinism in our process algebraic specifications.

Synopsis. In section 2 we give some background, discuss notation and recap our quantum process calculus of choice. Then, we put forward our formal testing theory for quantum systems in section 3, and we analyse the Quantum Anonymous Transmission Protocol in section 4. Finally, section 5 concludes and discusses future work.

2. Quantum Process Calculi

We provide some background on quantum computing, referring to Nielsen and Chuang (2010) for further reading. Then, we present our process calculus of choice, *linear quantum CCS* (lqCSS) from e.g. Ceragioli et al. (2024c).

2.1. Quantum Computing Fundaments and Notation

An isolated physical system is associated with a *Hilbert space* $\mathcal{H}$, i.e. a complex vector space equipped with an inner product $\langle \cdot | \cdot \rangle$. We indicate column vectors as $|\psi\rangle$ and their conjugate transpose as $\langle\psi| = |\psi\rangle^\dagger$. The states of a system are *unit vectors* in $\mathcal{H}$, i.e. vectors $|\psi\rangle$ such that $\langle\psi|\psi\rangle = 1$. A two-dimensional physical system is known as a *qubit*, and we denote its Hilbert space as $\widehat{\mathcal{H}} = \mathbb{C}^2$. The vectors $|0\rangle = (1,0)^T$ and $|1\rangle = (0,1)^T$ form the *computational basis* of $\widehat{\mathcal{H}}$. Other important states are $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, which form the *Hadamard basis*. In quantum terminology, the states in the Hadamard basis are *superpositions* with respect to the computational basis, as they are a linear combination of $|0\rangle$ and $|1\rangle$. A third basis of $\widehat{\mathcal{H}}$ contains $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$.

We represent the state space of a composite physical system as the *tensor product* of the state spaces of its components. Consider the Hilbert spaces $\mathcal{H}_A$ with $\{|\psi_i\rangle\}_{i\in I}$ one of its bases, and $\mathcal{H}_B$ with $\{|\phi_k\rangle\}_{k\in K}$ one of its bases. We let their tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ be the Hilbert space with bases $\{|\psi_i\rangle \otimes |\phi_k\rangle\}_{(i,k)\in I\times K}$, where $|\psi\rangle \otimes |\phi\rangle$ is the Kronecker product between matrices, defined as

$$\begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{m,1} & \cdots & x_{m,n} \end{bmatrix} \otimes A = \begin{bmatrix} x_{1,1}A & \cdots & x_{1,n}A \\ \vdots & \ddots & \vdots \\ x_{m,1}A & \cdots & x_{m,n}A \end{bmatrix}$$

We often omit the tensor product: we write $|\psi\phi\rangle$ for $|\psi\rangle \otimes |\phi\rangle$ and $|\psi\rangle^{\otimes n}$ for $\bigotimes_{i=1}^{n} |\psi\rangle$. We write $\widehat{\mathcal{H}}^{\otimes n}$ for the 2^n-dimensional Hilbert space defined as the tensor product of n copies of $\widehat{\mathcal{H}}$ (i.e. the possible states of n qubits). A quantum state in $\mathcal{H}_A \otimes \mathcal{H}_B$ is *separable* when it can be expressed as the Kronecker product of two vectors of $\mathcal{H}_A$ and $\mathcal{H}_B$. Otherwise, it is *entangled*, like the Bell state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

In quantum physics, the evolution of an isolated system is described by a unitary transformation. For each linear operator A on $\mathcal{H}$, its *adjoint* $A^\dagger$ is the (necessarily unique) linear operator such that $\langle\psi|A|\phi\rangle = \left\langle A^\dagger\psi \middle| \phi \right\rangle$. A linear operator U is *unitary* when $UU^\dagger = U^\dagger U = I$, with I the identity matrix. Quantum computers allow the programmer to manipulate registers via unitaries like H, X, Z and *CNOT*, which are defined by the following equalities and by linearity in all the other cases:

$$H|0\rangle = |+\rangle \quad H|1\rangle = |-\rangle \quad X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle \quad Z|+\rangle = |-\rangle \quad Z|-\rangle = |+\rangle$$
$$CNOT|10\rangle = |11\rangle \quad CNOT|11\rangle = |10\rangle \quad CNOT|0\psi\rangle = |0\psi\rangle$$

One relevant consequence of unitary evolution is the *no-cloning theorem*, telling us that there exists no unitary transformation U capable of copying quantum information, i.e. such that $U(|\psi 0\rangle) = |\psi\psi\rangle$ for all $|\psi\rangle$.

Quantum measurements describe how to extract information from a physical system. Performing a measurement on a quantum state returns a probabilistic classical result and causes the quantum state to change (i.e. to *collapse*). A measurement with k different outcomes is a set $\mathcal{M} = \{M_m\}_{m=0}^{k-1}$ of k linear operators, satisfying the *completeness* equation $\sum_{m=0}^{k-1} M_m^\dagger M_m = I$. If the state of the system is $|\psi\rangle$ before the measurement, then the probability of m-th outcome occurring is $p_m = \langle\psi|M_m|\psi\rangle$. If m is the outcome, then the state after the measurement will be $M_m|\psi\rangle / p_m$.

The simplest measurements project a state into the elements of a basis, e.g. $\mathcal{M}_{01} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and $\mathcal{M}_\pm = \{|+\rangle\langle +|, |-\rangle\langle -|\}$ for the computational and Hadamard basis of $\widehat{\mathcal{H}}$. As expected, applying $\mathcal{M}_{01}$ to $|0\rangle$ always returns the classical outcome 0 and the state $|0\rangle$. When applying the same measurement on $|+\rangle$, instead, the outcome is 0 and the state is $|0\rangle$, or 1 and $|1\rangle$ with equal probability. Symmetrically, measuring $|0\rangle$ with $\mathcal{M}_\pm$ leads to either 0 and $|+\rangle$,

$$\textsc{Nil}\ \frac{\tilde{e} \in \tilde{\Sigma}}{\Sigma \vdash \mathbf{0}_{\tilde{e}}} \qquad \textsc{Tau}\ \frac{\Sigma \vdash P}{\Sigma \vdash t{:}\tau.P} \qquad \textsc{QOp}\ \frac{U : \mathsf{Op}(n) \quad |E| = n \quad \tilde{e} \in \tilde{E} \quad E \subseteq \Sigma \quad \Sigma \vdash P}{\Sigma \vdash t{:}U(\tilde{e}).P}$$

$$\textsc{QMeas}\ \frac{\mathcal{M} : \mathsf{Meas}(n) \quad |E| = n \quad \tilde{e} \in \tilde{E} \quad E \subseteq \Sigma \quad x : \mathbb{N} \quad \Sigma \vdash P}{\Sigma \vdash t{:}\mathcal{M}(\tilde{e} \rhd x).P} \qquad \textsc{CRecv}\ \frac{c : \widehat{T} \quad x : T \in \{\mathbb{B}, \mathbb{N}\} \quad \Sigma \vdash P}{\Sigma \vdash t{:}c?x.P}$$

$$\textsc{QRecv}\ \frac{c : \widehat{\mathcal{Q}} \quad x : \mathcal{Q} \quad \Sigma \cup \{x\} \vdash P}{\Sigma \vdash t{:}c?x.P} \qquad \textsc{CSend}\ \frac{c : \widehat{T} \quad e : T \in \{\mathbb{B}, \mathbb{N}\} \quad \Sigma \vdash P}{\Sigma \vdash t{:}c!e.P} \qquad \textsc{QSend}\ \frac{c : \widehat{\mathcal{Q}} \quad e \in \Sigma \quad \Sigma \setminus \{e\} \vdash P}{\Sigma \vdash t{:}c!e.P}$$

$$\textsc{Ite}\ \frac{e : \mathbb{B} \quad \Sigma \vdash P \quad \Sigma \vdash Q}{\Sigma \vdash \textbf{if } e \textbf{ then } P \textbf{ else } Q} \qquad \textsc{Sum}\ \frac{\Sigma \vdash P \quad \Sigma \vdash Q}{\Sigma \vdash P + Q} \qquad \textsc{Par}\ \frac{\Sigma_1 \cap \Sigma_2 = \emptyset \quad \Sigma_1 \vdash P \quad \Sigma_2 \vdash Q}{\Sigma_1 \cup \Sigma_2 \vdash P \parallel Q} \qquad \textsc{Restr}\ \frac{\Sigma \vdash P}{\Sigma \vdash P \setminus c}$$

Figure 2: Typing rules for lqCCS

or 1 and $|-\rangle$, with equal probability. Finally, applying the measurement $\mathcal{M}_{\pm i} = \{|i\rangle\langle i|, |\pm i\rangle\langle \pm i|\}$ to each of $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ returns 0 and $|i\rangle$, or 1 and $|\pm i\rangle$ with equal probability.

Finally, we fix some notation about probability distributions, useful to describe the behaviour of quantum system after measurements. Given a function $\Delta : S \to [0,1]$ from a set S to the interval of real numbers $[0,1]$, we let its *support* be the set $\lceil \Delta \rceil = \{s \in S \mid \Delta(s) > 0\}$. When the support is finite, we define the *mass* of Δ as $|\Delta| = \sum_{s \in S} \Delta(s)$. A *probability distribution* $\Delta \in \mathcal{D}(S)$ over a set S is a function $\Delta : S \to [0,1]$ with finite support such that $|\Delta| = 1$. For each $s \in S$, we let $p \cdot s$ be the *point distribution* such that $(p \cdot s)(s) = p$. In general, we write a distribution Δ explicitly as $\sum_{i \in I} p_i \cdot x_i$, when $\Delta(x_i) = p_i$. For example, if a qubit is in the state $|+\rangle \in \widehat{\mathcal{H}}$, after a measurement $\mathcal{M}_{01}$ in the computational basis it will evolve in the distribution of states $\Delta = \frac{1}{2} \cdot |0\rangle\langle 0| \oplus \frac{1}{2} \cdot |1\rangle\langle 1| \in \mathcal{D}(\widehat{\mathcal{H}})$.

2.2. Linear Quantum CCS

Our modelling language of choice is *linear quantum CCS* (lqCCS) (Ceragioli et al., 2024c, 2026). Our process calculus is enriched with a linear type system, reflecting the no-cloning theorem of quantum mechanics, which forbids quantum values to be copied or broadcasted. Its semantics is given as a *probabilistic LTS* (pLTS) where transitions are decorated with schedulers. Tags in the syntax name all the possible non-deterministic choices, while scheduler choices in the semantics encode the selected ones among the available tags.

In a nutshell, lqCCS is a linearly-typed version of qCCS (Feng et al., 2012), where the primitives for communication, parallelism and non-determinism of value-passing CCS (Hennessy, 1991) are extended with quantum capabilities. Moreover, we adopt syntactic tags, so that each non-deterministic choice has a distinct name.

Definition 1 (lqCCS Process Syntax)**.** *Let $\mathbb{B} \ni b, \mathbb{N} \ni n, \mathcal{Q} \ni q$ be atomic boolean values, natural numbers and qubit names, respectively. Let $\mathsf{Chan} \ni c$ be communication channels and $\mathsf{Var} \ni x$ variables. Let $\mathsf{Tag} \ni t$ be a denumerable set of tags. The syntax of lqCCS processes is defined by the productions*

$$\begin{aligned} P &::= \mathbf{0}_{\tilde{e}} \mid K \mid P \parallel P \mid \textbf{\textit{if }} e \textbf{\textit{ then }} P \textbf{\textit{ else }} P \mid P \setminus c \\ K &::= \alpha.P \mid K + K \\ \alpha &::= t{:}\tau \mid t{:}c?x \mid t{:}c!e \mid t{:}U(\tilde{e}) \mid t{:}\mathcal{M}(\tilde{e} \rhd x) \\ e &::= x \mid b \mid n \mid q \mid \neg e \mid e \vee e \mid e \leq e \mid e = e \end{aligned}$$

where $\tilde{e}$ denotes a (possibly empty) tuple $e_1, \ldots, e_n$ of expressions.

As it is common in value-passing CCS, we have action prefixes for message passing and silent actions, as well as operators for parallel composition, non-deterministic and conditional choice, and channel restriction. In addition, a process can manipulate the state of qubits via unitary transformations and measurements. We allow processes to

modify the state of qubits denoted by $\tilde{e}$ (where each expression is either a qubit q or a variable x) by applying any unitary U with $U(\tilde{e})$. We write $U : \mathrm{Op}(n)$ to indicate that U is a transformation of arity n (i.e. it acts on n qubits). The process can also perform the measurement $\mathcal{M}$ to the qubits of $\tilde{e}$, written $\mathcal{M}(\tilde{e} \triangleright x)$: the classical outcome is stored in the number variable x, and the state of the qubits is updated accordingly. In general, a symbol $\mathcal{M}$ denotes a measurement $\{M_0, \dots, M_{k-1}\}$ with k different outcomes, and we write $|\mathcal{M}|$ for the cardinality k of $\mathcal{M}$. We also write $\mathcal{M} : \mathrm{Meas}(n)$ when $\mathcal{M}$ has arity n. Finally, the process $\mathbf{0}_{\tilde{e}}$ is an idle deadlock process that maintains ownership of the qubits in $\tilde{e}$. When $\tilde{e}$ is the empty sequence, we write $\mathbf{0}$ to stress the equivalence with the nil process of standard CCS. For brevity, we omit the trailing $\mathbf{0}$, writing, e.g. $a!1$ for $a!1.\mathbf{0}$, and we often write **if** e **then** $\alpha_1.R$ **else** $\alpha_2.R$ as (**if** e **then** α_1 **else** α_2).R.

Prefixes must be annotated by tags, intended to explicitly name the choices that a scheduler can perform when running a process. For example, $t_0 : H(q_0).(t_1 : c!0.\mathbf{0}_{q_0} + t_2 : c!1.\mathbf{0}_{q_0})$ needs to tag the two branches of its non-deterministic choice differently. Note that parallel processes must be labelled differently, so that each choice selects a distinct possible evolution. In the following, we assume that processes come with their associated tags, and we sometimes omit them if they carry no special meaning, writing e.g. $c?x.\tau.c!x$ in place of $t : c?x.t : \tau.t : c!x$.

The visibility of qubits is enforced explicitly through the linear type system in Figure 2. The typing judgment $\Sigma \vdash P$ indicates that the process P is well-typed under the usage of the set of qubits $\Sigma \subseteq \mathcal{Q}$. Given a set of terms E, we write $\tilde{E}$ for the set of all tuples $\tilde{e}$ composed of all and only the elements in E (in any possible order without repetitions). Atomic values are typed by their domain set: $\mathbb{N}$ for natural numbers, $\mathbb{B}$ for boolean values, and $\mathcal{Q}$ for qubit names. Similarly, we assume that variables come associated with the type of their possible values. Channels $c \in \mathrm{Chan}$ are typed as $\widehat{\mathbb{N}}$, $\widehat{\mathbb{B}}$, and $\widehat{\mathcal{Q}}$, according to the values that they can propagate. Note that processes composed in parallel must use two disjoint sets of qubits, thus enforcing single ownership. Since the type of a process is unique, we will call Σ_P the only context which types P (when such a type exists).

Theorem 1. *Whenever $\Sigma \vdash P$ and $\Sigma' \vdash P$ then $\Sigma = \Sigma'$*

Example 2. *Consider a quantum lottery **QL** = **Pr** ∥ **An** formed by processes **Pr**, which prepares a qubit used as a source of randomness, and **An**, which receives it, measures it, and announces the winner between Alice and Bob.*

$$\mathbf{Pr} = (t_1 : X(q).t_3 : c!q.\mathbf{0}) + (t_2 : H(q).t_3 : c!q.\mathbf{0})$$
$$\mathbf{An} = t_4 : c?x.t_4 : \mathcal{M}_{01}(x \triangleright y).\mathbf{if}\ y = 0\ \mathbf{then}\ t_4 : a!1.\mathbf{0}_x\ \mathbf{else}\ t_4 : b!1.\mathbf{0}_x$$

*Intuitively, **Pr** can prepare and send a qubit by applying either X or H to its qubit q, and **An** announces that Alice wins with $a!1$ if the received qubit is found in state $|0\rangle$, or that Bob wins with $b!1$ if it is found in state $|1\rangle$. The unique typing of **QL** is $\{q\} \vdash \mathbf{QL}$, with $a, b : \widehat{\mathbb{N}}$, $c : \widehat{\mathcal{Q}}$, $y : \mathbb{N}$, and $q, x : \mathcal{Q}$. Regarding tags, t_1 and t_2 are associated with prefixes so as to guarantee that possible resolutions of the non-deterministic choice are distinguished. At the same time, the possible interleavings between **Pr** and **An** are distinguished by the fact that the former is tagged by t_1, t_2 and t_3, whereas the latter by t_4. Note that alternative tagging schemes could have been used, as long as tags uniquely determine the process evolution (this will be made precise in Definition 3 and Assumption 1 in the following). For example, t_1 and t_2 could be reused in place of t_3, whereas using t_4 in the process **Pr** would break our assumption.*

2.3. Operational Semantics

We describe a labelled semantics for lqCCS in terms of *configurations* $\langle |\psi\rangle, P\rangle \in \mathit{Conf}$, each composed by a global quantum state and a tagged lqCCS process. Given a set $\Sigma = \{q_1, \dots, q_n\} \subseteq \mathcal{Q}$ and its associated Hilbert space $\mathcal{H}_\Sigma = \widehat{\mathcal{H}}^{\otimes n}$, a global quantum state $|\psi\rangle$ is a unit vector in $\mathcal{H}_\Sigma$. The type system is extended to configurations and distributions by considering the qubits of the underlying quantum state. Let $\Sigma_{|\psi\rangle}$ be the set of qubits appearing in $|\psi\rangle$.

Definition 2 (Configuration Typing)**.** *Let $\langle |\psi\rangle, P\rangle \in \mathit{Conf}$, with P typed and $\Sigma_P \subseteq \Sigma_{|\psi\rangle}$, then we write $(\Sigma_{|\psi\rangle}, \Sigma_P) \vdash \langle |\psi\rangle, P\rangle$. Let $\Delta \in \mathcal{D}(\mathit{Conf})$, then we let $(\Sigma, \Sigma') \vdash \Delta$ if $(\Sigma, \Sigma') \vdash C$ for any $C \in \lceil \Delta \rceil$.*

Hereafter, we restrict ourselves to well-typed distributions, and denote with $\Sigma_{\overline{P}}$ the set $\Sigma_{|\psi\rangle} \setminus \Sigma_P$, i.e. the qubits in the quantum state that are not owned by the process and thus freely accessible by the environment.

Our semantics is decorated with *syntactic choices*, which resolve non-determinism by choosing a tag. The syntax of *choices* $s \in \mathit{Choice}$ for lqCCS is defined as follows

$$s ::= t \mid (t, t)$$

$$\textsc{Tau}\quad \langle |\psi\rangle, t{:}\tau.P\rangle \xrightarrow{\tau}_t 1 \cdot \langle |\psi\rangle, P\rangle \qquad \textsc{Op}\quad \langle |\psi\rangle, t{:}U(\tilde{q}).P\rangle \xrightarrow{\tau}_t 1 \cdot \langle U^{\tilde{q}}|\psi\rangle, P\rangle$$

$$\textsc{Meas}\quad \langle |\psi\rangle, t{:}\mathcal{M}(\tilde{q} \rhd x).P\rangle \xrightarrow{\tau}_t \sum_{m=0}^{|\mathcal{M}|-1} \langle\psi|M_m^{\tilde{q}}|\psi\rangle \cdot \left\langle \frac{M_m^{\tilde{q}}|\psi\rangle}{\sqrt{\langle\psi|M_m^{\tilde{q}}|\psi\rangle}}, P[^m/_x] \right\rangle$$

$$\textsc{Send}\quad \frac{e \Downarrow v}{\langle |\psi\rangle, t{:}c!e.P\rangle \xrightarrow{c!v}_t 1 \cdot \langle |\psi\rangle, P\rangle}$$

$$\textsc{Recv}\quad \frac{c : \widehat{Q} \Rightarrow v \in \Sigma_{|\psi\rangle} \setminus \Sigma_P}{\langle |\psi\rangle, t{:}c?x.P\rangle \xrightarrow{c?v}_t 1 \cdot \langle |\psi\rangle, P[^v/_x]\rangle} \qquad \textsc{IteT}\quad \frac{e \Downarrow tt \qquad \langle |\psi\rangle, P\rangle \xrightarrow{\mu}_s \Delta}{\langle |\psi\rangle, \textbf{if } e \textbf{ then } P \textbf{ else } Q\rangle \xrightarrow{\mu}_s \Delta}$$

$$\textsc{IteF}\quad \frac{e \Downarrow ff \qquad \langle |\psi\rangle, Q\rangle \xrightarrow{\mu}_s \Delta}{\langle |\psi\rangle, \textbf{if } e \textbf{ then } P \textbf{ else } Q\rangle \xrightarrow{\mu}_s \Delta}$$

$$\textsc{SumL}\quad \frac{\langle |\psi\rangle, P\rangle \xrightarrow{\mu}_s \Delta}{\langle |\psi\rangle, P + Q\rangle \xrightarrow{\mu}_s \Delta} \qquad \textsc{SumR}\quad \frac{\langle |\psi\rangle, Q\rangle \xrightarrow{\mu}_s \Delta}{\langle |\psi\rangle, P + Q\rangle \xrightarrow{\mu}_s \Delta}$$

$$\textsc{ParL}\quad \frac{\langle |\psi\rangle, P\rangle \xrightarrow{\mu}_s \Delta \qquad \mu \notin \{c?v \mid v \in \Sigma_Q\}}{\langle |\psi\rangle, P \parallel Q\rangle \xrightarrow{\mu}_s \Delta \parallel Q}$$

$$\textsc{ParR}\quad \frac{\langle |\psi\rangle, Q\rangle \xrightarrow{\mu}_s \Delta \qquad \mu \notin \{c?v \mid v \in \Sigma_P\}}{\langle |\psi\rangle, P \parallel Q\rangle \xrightarrow{\mu}_s P \parallel \Delta}$$

$$\textsc{SynchL}\quad \frac{\langle |\psi\rangle, P\rangle \xrightarrow{c!v}_t 1 \cdot \langle |\psi\rangle, P'\rangle \qquad \langle |\psi\rangle, Q\rangle \xrightarrow{c?v}_{t'} 1 \cdot \langle |\psi\rangle, Q'\rangle}{\langle |\psi\rangle, P \parallel Q\rangle \xrightarrow{\tau}_{(t,t')} 1 \cdot \langle |\psi\rangle, P' \parallel Q'\rangle}$$

$$\textsc{SynchR}\quad \frac{\langle |\psi\rangle, P\rangle \xrightarrow{c?v}_t 1 \cdot \langle |\psi\rangle, P'\rangle \qquad \langle |\psi\rangle, Q\rangle \xrightarrow{c!v}_{t'} 1 \cdot \langle |\psi\rangle, Q'\rangle}{\langle |\psi\rangle, P \parallel Q\rangle \xrightarrow{\tau}_{(t,t')} 1 \cdot \langle |\psi\rangle, P' \parallel Q'\rangle}$$

$$\textsc{Restr}\quad \frac{\langle |\psi\rangle, P\rangle \xrightarrow{\mu}_s \Delta \qquad \forall v.\mu \neq c!v, c?v}{\langle |\psi\rangle, P \setminus c\rangle \xrightarrow{\mu}_s \Delta}$$

Figure 3: Rules of lqCCS semantics.

and a *scheduler* is a finite string $\tilde{s} \in Choice^*$. At each step, a scheduler can select an action with a tag t, or a synchronization with a pair (t_1, t_2). Intuitively, tags represent available visible options, upon which the scheduler can choose (possibly using a pair of them for synchronization).

We assume a set Act of actions, containing τ, $c!v$ and $c?v$ for any channel c and value v. The semantics of lqCCS is a *scheduler probabilistic LTS*, i.e. a triple $(Conf, Act, \longrightarrow)$, with $\longrightarrow \subseteq Conf \times Act \times Choice \times \mathcal{D}(Conf)$. A transition $(\langle |\psi\rangle, P\rangle, \mu, s, \Delta) \in \longrightarrow$ is also denoted as $\langle |\psi\rangle, P\rangle \xrightarrow{\mu}_s \Delta$.

The transition relation $\longrightarrow$ is the smallest relation over configurations with closed processes that satisfies the rules in Figure 3. As expected, tagged actions require a matching choice on the transition. Expressions e are evaluated through a big step semantics $e \Downarrow v$ with v a value, i.e. either $n \in \mathbb{N}$, $b \in \mathbb{B}$, or $q \in \mathcal{Q}$. We restrict to arithmetic and logical operations, and therefore omit the rules and assume that free variables are not evaluated. In rule Op, the unitary U is applied to the qubits in $\tilde{q}$. Since $\tilde{q}$ can be smaller than the whole $\Sigma_{|\psi\rangle}$, we define $U^{\tilde{q}}$ as the unitary that acts on the whole $|\psi\rangle$ but "ignores" the qubits outside $\tilde{q}$. More precisely, $U^{\tilde{q}}$ is obtained by composing: (i) a suitable set of SWAP unitaries to bring the qubits $\tilde{q}$ in the first positions; (ii) the tensor product of the operator U with the identity on untouched qubits on the right; and (iii) the inverse of the SWAP operators of point (i) to recover the original order of qubits (Lalire, 2006). In rule Meas, given a measurement $\mathcal{M} = \{M_m\}$, we define $M_m^{\tilde{q}}$ as the identity-padded-extension of M_m as before. In the rules ParL and ParR the parallel composition of a distribution $\Delta = \sum_{i \in I} p_i \cdot \langle |\psi_i\rangle, P_i\rangle$ and a process Q is defined as $\sum_{i \in I} p_i \cdot \langle |\psi_i\rangle, P_i \parallel Q\rangle$, and similarly for the restriction $\Delta \setminus c$. Notice that in Recv we impose that a process P can only receive a qubit that is defined in the global state $|\psi\rangle$ and is not already owned by P, i.e. $v \in \Sigma_{|\psi\rangle} \setminus \Sigma_P$. Similarly, in ParL we require that P does not receive a qubit that is already owned by Q, and symmetrically in ParR. This constraints are needed to preserve linearity of qubits when processes interact with an unspecified external environment.

Example 3. *The pLTS semantics of the quantum lottery* ***QL*** *from Example 2 on quantum state* $|0\rangle\langle 0|$ *is in Figure 4, where* $\mathbf{An'}$ *stands for* $t_4 : \mathcal{M}_{01}(x \rhd y)$. $\mathbf{An''}$*, and* $\mathbf{An''}$ *for* $\textbf{if } y = 0 \textbf{ then } t_4 : a!1.\mathbf{0}_x \textbf{ else } t_4 : b!1.\mathbf{0}_x$*. To simplify the*

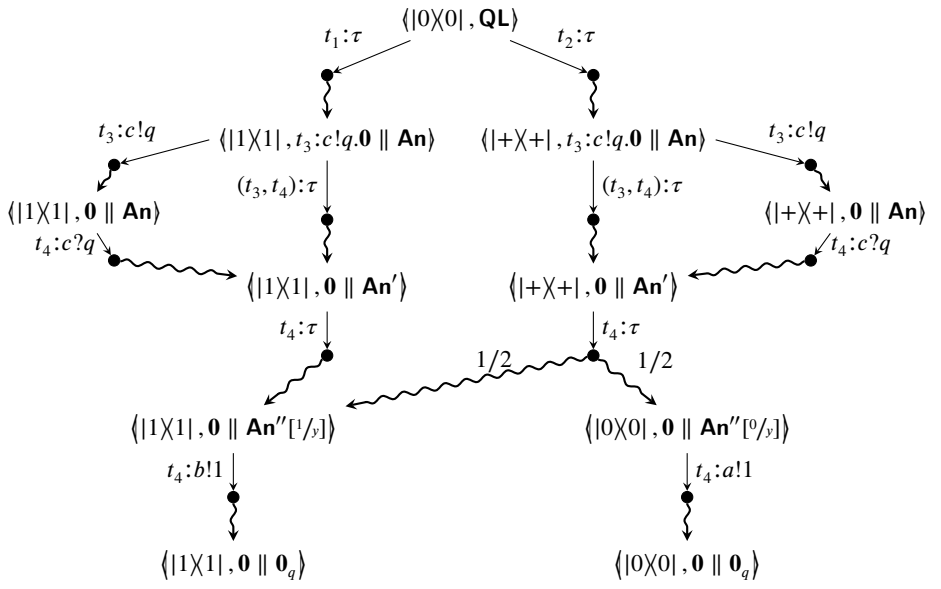


Figure 4: Semantics of the quantum lottery process.

presentation, we draw $\xrightarrow{s:\mu}$ *instead of* $\xrightarrow{\mu}_s$*. A scheduler for* ***QL*** *must decide which unitary* ***Pr*** *applies to the qubit q at the first step, either X or H, i.e. choosing either* t_1 *or* t_2*, respectively. Then, it chooses whether the qubit is sent to* ***An*** *– i.e. to reduce with* τ *and choice* (t_3, t_4) *– or to the external environment – i.e. to transition with label* $c!q$ *and choice* t_3 *(both are possible since the channel is not restricted). Intuitively, if* ***Pr*** *chooses X, then Bob will always win, otherwise either Alice or Bob will win with the same probability. Note that at the beginning, in configuration* $\langle |0\rangle\langle 0| , \boldsymbol{QL}\rangle$*, the choice* t_4 *cannot be taken because the quantum state has no qubit apart from those in* $\Sigma_{\boldsymbol{QL}}$*.*

We now formalize our assumption that scheduler choices uniquely determine the behaviour of configurations. Following the standard approach of scheduled semantics, we rely on tags that guarantees a form of determinism for processes evolution, adapting the definition of Chatzikokolakis and Palamidessi (2007); Chatzikokolakis et al. (2009) to deal with the value-passing features of lqCCS. Intuitively, a deterministic process associates a different tag to all of its available non-deterministic choices, thus any given scheduler choice s forces a unique transition $\xrightarrow{\mu}_s$. However, this is too restrictive for a labelled semantics where receptions are caused by the choices of other (sending) processes. Our schedulers, indeed, solve only the *internal* non-determinism (like $t : c!0.P + t' : c!1.Q$), and do not address the *external* one, which comes from outside input (like $c?x.P$). Thus, we introduce the class of *internally deterministic* processes, which are allowed to have multiple reductions for the same choice s only for input transitions, one for each value it can receive, like $\xrightarrow{c?0}_s$ and $\xrightarrow{c?1}_s$.

Definition 3 (Internally Deterministic Process)**.** *A process* P *is* internally deterministic *if for all* $|\psi\rangle \in \mathcal{H}_\Sigma$ *with* $\Sigma \supseteq \Sigma_P$*,* $s \in Choice$*,* $\mu, \mu' \in Act$ *and* $\Delta, \Delta' \in \mathcal{D}(Conf)$*, if* $\langle |\psi\rangle , P\rangle \xrightarrow{\mu}_s \Delta$ *and* $\langle |\psi\rangle , P\rangle \xrightarrow{\mu'}_s \Delta'$*, then either* $\mu = \mu'$ *and* $\Delta = \Delta'$*, or* $\mu \neq \mu'$ *and there exists* c*,* v *and* v' *such that* $\mu = c?v$ *and* $\mu' = c?v'$*.*

Assumption 1. *All processes considered in the following are internally deterministic.*

3. Testing Semantics of lqCCS

We now move to investigate behavioural equivalences for quantum process calculi. We propose *may* and *must* testing preorders, leading to a definition of *testing equivalence* that essentially coincides with the one of Bernardo et al. (2014), reformulated using syntactic schedulers of Chatzikokolakis and Palamidessi (2007).

Testing preorders and equivalences relate configurations that *may* or *must* pass the same tests, investigating the probability of success under a specific scheduler. To be adapted to the quantum setting, tests must be capable of

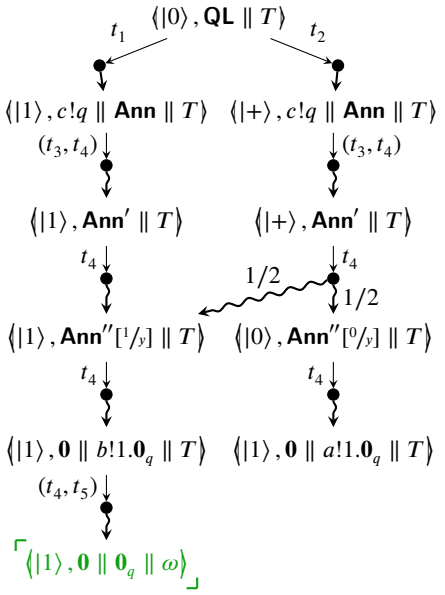


Figure 5: Semantics of **QL** with test T.

communicating on classical and quantum channels, as well as manipulating the free qubits of a configuration (including the ones received over visible channels). Our tests are generated similarly to lqCCS processes, simply by adding a deadlock symbol ω to indicate a completed successful computation (we type ω the same as $\mathbf{0}$).

Definition 4 (lqCCS Test Syntax)**.** *The syntax of lqCCS tests is defined by the following productions (refer to Definition 1 for α and terminal symbols).*

$$T ::= \omega \mid \mathbf{0}_{\tilde{e}} \mid J \mid T \parallel T \mid \textbf{\textit{if}}\ e\ \textbf{\textit{then}}\ T\ \textbf{\textit{else}}\ T$$
$$J ::= \alpha.T \mid J + J$$

We let Test be the set of all closed tests well-typed according to the rules in Figure 2 augmented with $\emptyset \vdash \omega$.

The operational semantics of lqCCS with tests is defined by a transition system of extended configurations $Conf_T$, i.e. couples of the form $\langle |\psi\rangle, P \parallel T\rangle$ composed of a regular process P and a test T, such that they do not have any common tags. As before, we restrict ourselves to well-typed extended configurations, where the type system is lifted to both $Conf_T$ and $\mathcal{D}(Conf_T)$ as expected. The operational semantics of lqCCS with tests is defined as a *scheduled probabilistic reduction system*, i.e. the couple $(Conf_T, \xrightarrow{\tau})$ where $\xrightarrow{\tau} \subseteq Conf_T \times Choice \times \mathcal{D}(Conf_T)$ is the τ-fragment of the labelled transition relation $\longrightarrow$.

Some auxiliary definitions are needed to describe testing equivalences. Recall that a scheduler $\tilde{s}$ is a finite sequence of choices $\tilde{s} \in Choice^*$. We introduce *probabilistic runs*, i.e. sequences of configurations that can be reached via reductions with non-zero probability.

Definition 5 (Probabilistic run)**.** *Given an extended configuration $\langle |\psi_0\rangle, P_0 \parallel T_0\rangle$ and a scheduler $\tilde{s} = s_1 s_2 \cdots s_n$, a* probabilistic run *for $\langle |\psi_0\rangle, P_0 \parallel T_0\rangle$ under $\tilde{s}$ is a sequence*

$$r = \langle |\psi_0\rangle, P_0 \parallel T_0\rangle \xrightarrow{p_1} \langle |\psi_1\rangle, P_1 \parallel T_1\rangle \xrightarrow{p_2} \cdots \xrightarrow{p_n} \langle |\psi_n\rangle, P_n \parallel T_n\rangle$$

where, for $i = 1, \ldots, n$, we have $\langle |\psi_{i-1}\rangle, P_{i-1} \parallel T_{i-1}\rangle \xrightarrow{\tau}_{s_i} \Delta_i$ for a (necessarily unique) distribution Δ_i, and $p_i = \Delta_i(\langle |\psi_i\rangle, P_i \parallel T_i\rangle) > 0$. The probability *of r is $prob(r) = \prod_{i=1}^{n} p_i$.*

Note that not all schedulers are associated with a probabilistic run, e.g. if the scheduler selects a tag that labels no reductions. We say that a scheduler $\tilde{s} \in Choice^*$ is *non-blocking* for an extended configuration $\langle |\psi_0\rangle, P_0 \parallel T_0\rangle$ if

there exists a probabilistic run for it under $\tilde{s}$. Moreover, a non-blocking scheduler is maximal if it is not a prefix of another non-blocking scheduler. Notice that if a configuration has no outgoing transitions, then the empty scheduler ϵ is the only maximal non-blocking scheduler. If instead it performs a transition with choice s, it has a non-empty set of maximal non-blocking schedulers starting with s.

We write $Sch_{(|\psi\rangle,P,T)}$ for the set of maximal non-blocking schedulers of the extended configuration $\langle |\psi\rangle, P \parallel T\rangle$.

Example 4. *Consider* $\boldsymbol{QL}$ *from Example 2 and the test* $T = t_5{:}b?x.\omega$*, which is successful if Bob wins the lottery. The scheduled reduction system of* $\langle |0\rangle, \boldsymbol{QL} \parallel T\rangle$ *is in Figure 5, where* $\boldsymbol{Ann'}$ *and* $\boldsymbol{Ann''}$ *are as in Example 3, and success states are marked and highlighted in green. A scheduler must only decide which unitary* $\boldsymbol{Pre}$ *applies to the qubit q, by choosing either* t_1 *or* t_2*. The non-blocking schedulers of* $\boldsymbol{QL} \parallel T$ *are* $t_1(t_3,t_4)t_4t_4(t_4,t_5)$ *and* $t_2(t_3,t_4)t_4t_4(t_4,t_5)$ *with their respective prefixes. One (of two) run for the scheduler* $t_2(t_3,t_4)t_4t_4$ *is*

$$\langle |0\rangle, QL \parallel T\rangle \xrightarrow{1} \langle |+\rangle, c!q \parallel Ann \parallel T\rangle \xrightarrow{1} \langle |+\rangle, Ann' \parallel T\rangle \xrightarrow{\frac{1}{2}} \langle |0\rangle, Ann''[0/y] \parallel T\rangle \xrightarrow{1} \langle |0\rangle, \mathbf{0} \parallel a!1.\mathbf{0}_q \parallel T\rangle$$

A run is successful if it reaches the success state ω. Given a lqCCS configuration, a test, and a scheduler, the success probability is the sum of the probabilities of all the successful runs.

Definition 6 (Success probability)**.** *A run* $r = \langle |\psi_0\rangle, P_0 \parallel T_0\rangle \xrightarrow{p_1} \langle |\psi_1\rangle, P_1 \parallel T_1\rangle \xrightarrow{p_2} \cdots \xrightarrow{p_n} \langle |\psi_n\rangle, P_n \parallel T_n\rangle$ *is* successful *if* $P_n \parallel T_n \equiv P' \parallel \omega$ *according to the following structural congruence:*

$$P \parallel Q \equiv Q \parallel P \quad P \parallel (Q \parallel R) \equiv (P \parallel Q) \parallel R \quad P \parallel \mathbf{0} \equiv P$$
$$\textbf{\textit{if }}tt \textbf{\textit{ then }} P \textbf{\textit{ else }} Q \equiv P \quad \textbf{\textit{if }}ff \textbf{\textit{ then }} P \textbf{\textit{ else }} Q \equiv Q$$

We denote as $Succ_{\tilde{s}}(\langle |\psi\rangle, P \parallel T\rangle)$ *the successful runs of* $\langle |\psi\rangle, P \parallel T\rangle$ *under* $\tilde{s}$*. Given a configuration* $\langle |\psi\rangle, P\rangle$*, the* success probability *of a test* T *under a non-blocking scheduler* $\tilde{s}$ *is*

$$sp_{\tilde{s}}(|\psi\rangle, P, T) = \sum\nolimits_{r \in Succ_{\tilde{s}}(\langle |\psi\rangle, P \parallel T\rangle)} prob(r).$$

Now we can define *may* and *must* preorders together with testing equivalence, following the definition of Chatzikokolakis and Palamidessi (2007).

Definition 7 (Testing Preorders and Equivalences)**.** *We define may and must testing preorders between lqCCS configurations as follows:*

$$\langle |\psi\rangle, P\rangle \preceq_{May} \langle |\phi\rangle, Q\rangle \textit{ iff}$$
$$\forall T \in Test.\ \forall \tilde{s} \in Sch_{(|\psi\rangle,P,T)}.\ \exists \tilde{t} \in Sch_{(|\phi\rangle,Q,T)} \textit{ such that } sp_{\tilde{s}}(|\psi\rangle, P, T) \leq sp_{\tilde{t}}(|\phi\rangle, Q, T)$$
$$\langle |\psi\rangle, P\rangle \preceq_{Must} \langle |\phi\rangle, Q\rangle \textit{ iff}$$
$$\forall T \in Test.\ \forall \tilde{t} \in Sch_{(|\phi\rangle,Q,T)}.\ \exists \tilde{s} \in Sch_{(|\psi\rangle,P,T)} \textit{ such that } sp_{\tilde{s}}(|\psi\rangle, P, T) \leq sp_{\tilde{t}}(|\phi\rangle, Q, T)$$

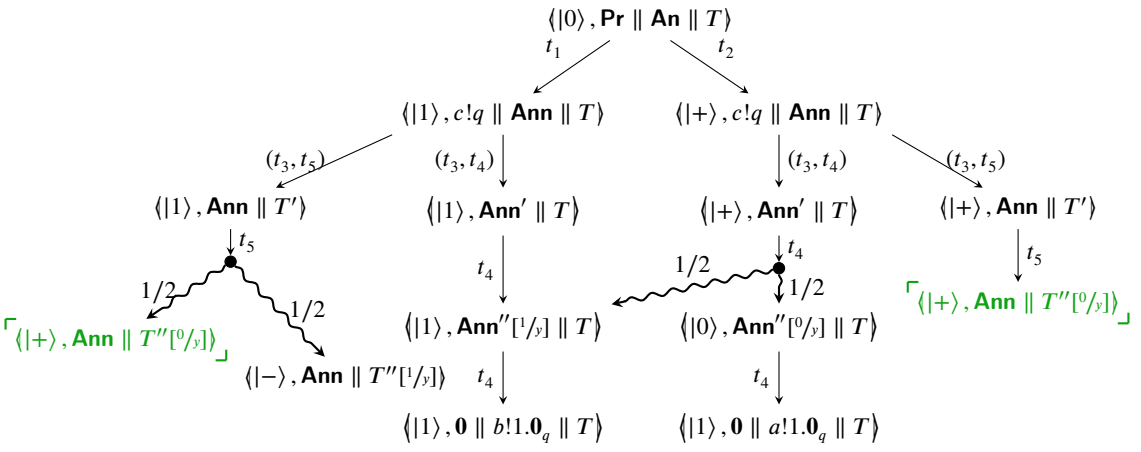
We define may equivalence $\approx_{May}$ *as* $\preceq_{May} \cap \succeq_{May}$*, and similarly for* must equivalence*. Finally,* testing equivalence $\approx_{Test}$ *is defined as* $\approx_{May} \cap \approx_{Must}$*.*

Note that these relations are probabilistic generalizations of the classical may and must preorders of De Nicola and Hennessy (1984), which can be recovered by forcing $sp_{\tilde{s}}(|\psi\rangle, P, T)$ to be only 0 or 1 in the definition above.

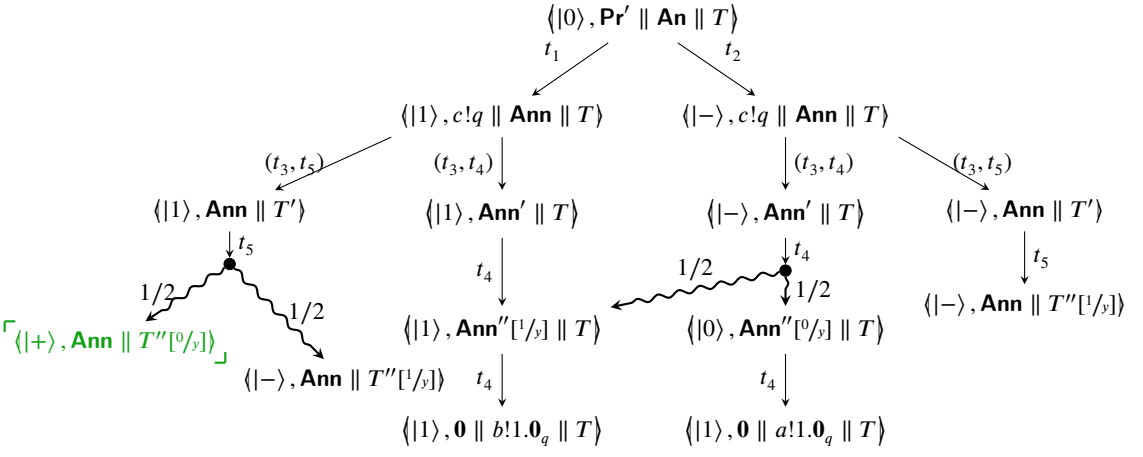
Example 5. *Going back to Example 4 we can see that the success probability under scheduler* $\tilde{s} = t_2(t_3,t_4)t_4t_4(t_4,t_5)$ *is* $\frac{1}{2}$*, while it is* 1 *under* $\tilde{s} = t_1(t_3,t_4)t_4t_4(t_4,t_5)$*.*

If we then consider $\boldsymbol{QL} \setminus c$*, thus restricting the quantum channel c, we can prove that* $\langle \mathbf{0}, t{:}b!1\rangle \preceq_{May} \langle |0\rangle, \boldsymbol{QL} \setminus c\rangle$*: the only meaningful tests on* $t{:}b!1$ *are those monitoring the channel b, and* $\boldsymbol{QL} \setminus c$ *can always output* $b!1$ *with probability 1. Instead, if we consider* $t : a!1$*, we have that* $\langle \mathbf{0}, t{:}a!1\rangle \not\preceq_{May} \langle |0\rangle, \boldsymbol{QL} \setminus c\rangle$*. Indeed, taking the test* $T = a?x.\omega$*, we have that* $sp_{\tilde{t}}(\mathbf{0}, t{:}a!1, T) = 1$*, while* $sp_{\tilde{s}}(|0\rangle, \boldsymbol{QL} \setminus c, T) \leq \frac{1}{2}$ *for any scheduler* $\tilde{s}$*.*

Noticeably, our definition of testing equivalence is consistent with the one introduced in (Bernardo et al., 2014), although here schedulers based on tags are used in place of resolutions defined over the pLTS.



(a) Semantics of **Pr** ∥ **An** ∥ **T**.



(b) Semantics of $\mathbf{Pr'} \parallel \mathbf{An} \parallel \mathbf{T}$.

Figure 6: Test T distinguishing **Pr** ∥ **An** and $\mathbf{Pr'} \parallel \mathbf{An}$

Remark 1. *By unfolding the definition, testing equivalence can be characterized as* $\langle |\psi\rangle, P\rangle \approx_{Test} \langle |\phi\rangle, Q\rangle$ *if and only if both the following conditions hold:*

$$\forall T \in Test.\ \forall \tilde{s} \in Sch_{(|\psi\rangle,P,T)}.\ \exists \tilde{t} \in Sch_{(|\phi\rangle,Q,T)} \ \text{ such that } \ sp_{\tilde{s}}(|\psi\rangle, P, T) = sp_{\tilde{t}}(|\phi\rangle, Q, T)$$
$$\forall T \in Test.\ \forall \tilde{t} \in Sch_{(|\phi\rangle,Q,T)}.\ \exists \tilde{s} \in Sch_{(|\psi\rangle,P,T)} \ \text{ such that } \ sp_{\tilde{s}}(|\psi\rangle, P, T) = sp_{\tilde{t}}(|\phi\rangle, Q, T)$$

We end this section with a final example, highlighting the importance of quantum primitives in the testing language.

Example 6. *Consider again the quantum lottery process* $\mathbf{Pr} \parallel \mathbf{An}$ *of Example 2. We suppose an alternative prepare process* $\mathbf{Pr'} = (t_1 : X(q).t_3 : c!q) + (t_2 : HX(q).t_3 : c!q)$*, which either sends* $|1\rangle$ *or* $|-\rangle$*, just as* **Pr** *either sends* $|1\rangle$ *or* $|+\rangle$*. We can investigate whether* $\mathbf{Pr} \parallel \mathbf{An} \setminus c \approx_{Test} \mathbf{Pr'} \parallel \mathbf{An} \setminus c$*. Notice how they both provide the classical outputs* $b!1$ *with either* 1 *or* $\frac{1}{2}$ *probability, and they both provide* $a!1$ *with either* 0 *or* $\frac{1}{2}$ *probability. Indeed, it is possible to prove them testing equivalent, as no test is capable of distinguishing them.*

If instead we drop the restriction on c*, we get* $\mathbf{Pr} \parallel \mathbf{An} \not\approx_{Test} \mathbf{Pr'} \parallel \mathbf{An}$*, because we have to take into account also quantum tests capable of intercepting and measuring the qubit sent on channel* c*. Indeed, a distinguishing test is* $T = (t_5 : c?q.t_5 : \mathcal{M}_{\pm}(x \rhd y).\mathbf{if}\ y = 0\ \mathbf{then}\ \omega\ \mathbf{else}\ \mathbf{0} \parallel \mathbf{0}_x$*, which generates the reduction systems in Figure 6, where* $T' = t_5 : \mathcal{M}_{\pm}(q \rhd y).T''$ *and* $T'' = \mathbf{if}\ y = 0\ \mathbf{then}\ \omega\ \mathbf{else}\ \mathbf{0} \parallel \mathbf{0}_q$*. If we fix the scheduler* $\tilde{s} = t_2(t_3, t_5)t_5$ *for* $\mathbf{Pr} \parallel \mathbf{An} \parallel T$*,*

corresponding to the rightmost path in Figure 6a, we get $sp_{\tilde{s}}(|0\rangle, \boldsymbol{Pr} \parallel \boldsymbol{An}, T) = 1$*, because* $\boldsymbol{Ann} \parallel T''[^0/_y] \equiv \boldsymbol{P} \parallel \omega$*. However, there are no schedulers for* $\boldsymbol{Pr'} \parallel \boldsymbol{An} \parallel T$ *with a success probability of* 1*, as the best-performing scheduler is* $\tilde{s}' = t_1(t_3, t_5)t_5$*, which achieves* $sp_{\tilde{s}'}(|0\rangle, \boldsymbol{Pr'} \parallel \boldsymbol{An}, T) = \frac{1}{2}$.

4. Assessing Anonymous Transmission

Hereafter, we put our formal development at work to verify the Quantum Anonymous Transmission Protocol (Christandl and Wehner, 2005). We model it in lqCCS, and discuss its correctness in terms of must testing. Then, we present and verify the relevant security properties of anonymity and tracelessness, in terms of testing equivalence. We will only provide proof sketches of our results, leaving out some details.

4.1. The Quantum Anonymous Transmission Protocol in a Nutshell

The Quantum Anonymous Transmission Protocol is among a set of n players. In each run of the protocol, a single player assumes the role of the sender, which has to communicate a classical bit to the receivers (all the other agents). Roles are not fixed, and the identity of the sender is not known: receivers only know that they are not the sender. Ideally, any agent can try to communicate at any moment, claiming the sender role when needed for the protocol run. However, in this case, collision avoidance is needed to guarantee correctness, e.g. by employing the collision detection protocol of Christandl and Wehner (2005). For simplicity, here we will assume that no collision occurs: a single agent acts as the sender for each run.

Each player has a local qubit on which to perform unitary transformations and measurements. No quantum communication is needed, but all the players have access to classical broadcast channels. Qubits are initially assumed to be in the generalized GHZ state $|GHZ\rangle = (|0\rangle^{\otimes n} + |1\rangle^{\otimes n})/\sqrt{2}$. Agents could have obtained these states beforehand at an earlier meeting or through a dedicated network. Then, the sender silently applies either I or Z on its local qubit, the first encoding a classical 0, the latter encoding 1. At this point, every participant applies an H transformation, measures its qubit and broadcasts the measured outcome. Each participant receives all the classical bits and computes their parity: the result encodes the message of the sender.

4.2. Assessing Correctness

As a first step, we model the protocol with lqCCS. We use the numbers $i, j \in N = \{1, 2, \ldots, n\}$ to index agents, and assume a channel $c_{i,j}$ intended to be used by agent i to send bits to agent j. Since our process calculus does not feature a broadcast instruction, we will simulate it through the process $c_i !!! v$ that (asynchronously) sends the value v in parallel to all other users. Formally, this operation is just syntactic sugar for:

$$c_i !!! v = \Big|\Big|_{j \neq i} t_{ij} : c_{ij} ! v.\mathbf{0}$$

For simplicity, we also define a shorthand for receiving all the broadcast values of other processes. Formally, $c_i ??? \tilde{x}.P$ receives a bit on all channels directed to i, binds the variables of the tuple $\tilde{x} = x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots x_n$, and finally continues as the process P:

$$c_i ??? \tilde{x}.P = t_i : c_{1i} ? x_1 . \ldots . t_i : c_{i-1\,i} ? x_{i-1} . t_i : c_{i+1\,i} ? x_{i+1} . \ldots . t_i : c_{ni} ? x_n . P$$

Note that we impose an order on receptions. This is done just for simplicity, and is immaterial to correctness and security properties. Note also that tags are used just to encode which agent is performing an operation, except for broadcast, where the parallel composition requires a finer granularity.

We can now represent the protocol as the class of lqCCS processes $\mathbf{QAT}_i^b$, where i indicates the sender's index and b is the transmitted bit.

$$\begin{aligned}
\mathbf{QAT}_i^b &:= \mathbf{Sender}_i^b \parallel \Big|\Big|_{j \neq i} \mathbf{Receiver}_j \\
\mathbf{Sender}_i^b &:= \textbf{if } b = 0 \textbf{ then } t_i : I(q_i).\mathbf{Receiver}_i \textbf{ else } t_i : Z(q_i).\mathbf{Receiver}_i \\
\mathbf{Receiver}_i &:= t_i : H(q_i).t_i : \mathcal{M}_{01}(q_i \rhd x_i).(c_i !!! x_i \parallel c_i ??? \tilde{x}.t_i : out_i ! \bigoplus_{j \in N} x_j \parallel \mathbf{0}_{q_i})
\end{aligned}$$

Some comments are in order. $\mathbf{QAT}_i^b$ is the parallel composition of a single sender (at index i) and $n-1$ receivers. Depending on the bit, $\mathbf{Sender}_i^b$ performs its unitary operation and then continues as if it were a receiver. $\mathbf{Receiver}_i$ performs its fixed set of operations, then broadcasts the measurement outcome, receives the other bits, computes the final value as the exclusive or of all bits, and notifies it on the visible channel out_i. A noticeable detail highlighted by the modelling is that we have no guarantees that the sender completes its operations before those of the receivers. Forcing a different behaviour would require either a synchronization phase or a shared clock. This possibility is not immediately evident in the original presentation of the protocol (Christandl and Wehner, 2005), which however preserves all its properties regardless of this unconstrained interleaving.

We model correctness though a pair of tests T_0 and T_1, which verify if the protocol correctly propagates the desired classical bit. Each of them simply expects to receive the same bit on all the *out* channels of agents. The success state ω is reached only if such bits are correctly received.

$$T_b := t{:}out_1?x_1.t{:}out_2?x_2.\ldots.t{:}out_n?x_n.\mathbf{if}\ \bigwedge_i x_i = b\ \mathbf{then}\ \omega\ \mathbf{else}\ \mathbf{0} \qquad \text{for } b \in \{0,1\}$$

We ask that both tests succeed with probability 1 and for any maximal non-blocking scheduler.

Property 1 (Correctness)**.** *Let $b \in \{0,1\}$, $i \in N$ and $\tilde{s} \in Sch_{(|GHZ\rangle, \mathbf{QAT}_i^b, T_b)}$. Then $sp_{\tilde{s}}(|GHZ\rangle, \mathbf{QAT}_i^b, T_b) = 1$.*

Proof sketch. Note that, since the scheduler is non-blocking and maximal, we will reach a point in which communications on the *out* channels are executed. We divide the proof in two steps: first we show that all schedulers are equal in terms of the state reached after completing such communication, then that the state is such that ω always occurs.

Step1. A critical point in the proof is that the operations of different agents commute, in the sense that if the ordering in which two agent acts is unconstrained, then the results of any possible interleaving coincide. Formally, we let $agents(s) \subseteq N$ be the set of agents acting when moving with choice s. If

$$\langle |\psi\rangle, P \parallel T\rangle \xrightarrow{p_1} \langle |\psi_1\rangle, P_1 \parallel T_1\rangle \xrightarrow{p_2} \langle |\psi_2\rangle, P_2 \parallel T_2\rangle$$

is a probabilistic run with scheduler $\tilde{s} = s_1 s_2 \cdots s_n$ with $agents(s_1) \cap agents(s_2) = \emptyset$, and if $\tilde{s}' = s_2 s_1 \cdots s_n$ is non-blocking, then we have that

$$\langle |\psi\rangle, P \parallel T\rangle \xrightarrow{p_1'} \left\langle \left|\psi_1'\right\rangle, P_1' \parallel T_1' \right\rangle \xrightarrow{p_2'} \langle |\psi_2\rangle, P_2 \parallel T_2\rangle$$

is a probabilistic run with $\tilde{s}'$, and $p_1 p_2 = p_1' p_2'$. We can prove this commutativity by cases on the operations performed by agents: if both are classical communications, then it is guaranteed by the fact that channels are private to agents; if one is classical and the other is a unitary transformation or measurement, then it is trivially true; finally, if both are quantum operations it follows from the fact that $(L \otimes I^{\otimes k})(I^{\otimes d} \otimes L') = L \otimes L'$ for any linear operator L, L' of size d and k, since each agent acts on its own qubit only, with unitary transformation and measurements implicitly tensored with the identity.

Step2. For simplicity, we represent $|GHZ\rangle$ in the Hadamard basis: to do so, we substitute $|0\rangle$ and $|1\rangle$ with $(|+\rangle + |-\rangle)/\sqrt{2}$ and $(|+\rangle - |-\rangle)/\sqrt{2}$, respectively.

$$\begin{aligned}
|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}) &= \frac{1}{\sqrt{2}}\left(\left(\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)\right)^{\otimes n} + \left(\frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)\right)^{\otimes n}\right) = \\
&= \frac{1}{2^{\frac{n+1}{2}}}((|+\rangle + |-\rangle)^{\otimes n} + (|+\rangle - |-\rangle)^{\otimes n}) = \\
&= \frac{1}{2^{\frac{n+1}{2}}}\left(\left(\sum_{x\in\{+,-\}^n} |x\rangle\right) + \left(\sum_{x\in\{+,-\}^n} (-1)^{\zeta_-(x)}|x\rangle\right)\right) = \\
&= \frac{1}{2^{\frac{n+1}{2}}}\left(\sum_{x\in\{+,-\}^n} |x\rangle + (-1)^{\zeta_-(x)}|x\rangle\right)
\end{aligned}$$

where $\zeta_y(x)$ returns the number of y elements in the string x. Note that, because of $(-1)^{\zeta_-(x)}$, strings x where $-$ appears an odd number of times cancel out, whereas those in which the number is even are taken twice. Thus, we can write

$$|GHZ\rangle = \frac{1}{2^{\frac{n-1}{2}}} \sum_{x \in \{+,-\}^n \text{ with } \zeta_-(x) \text{ even}} |x\rangle$$

Thanks to the result of the previous step, we consider a specific scheduler. Assume that the sender starts by performing its unitary application. We consider the two cases of T_0 and T_1 separately. Consider T_0, then the identity is applied, leaving the quantum state unchanged. The protocol follows by letting each receiver apply their H locally. We chose to consider a scheduler where each of the receivers acts before any of them performs a measurement. The resulting state is thus $H^{\otimes n}|GHZ\rangle$, i.e. it is obtained by replacing $|0\rangle$ and $|1\rangle$ for $|+\rangle$ and $|-\rangle$ respectively.

$$H^{\otimes n}|GHZ\rangle = \frac{1}{2^{\frac{n-1}{2}}} \sum_{x \in \{0,1\}^n \text{ with } \zeta_1(x) \text{ even}} |x\rangle$$

Now, assume that measurements are performed one after the other. The overall result is a measurement on the standard basis of $\mathcal{H}^{\otimes n}$, i.e. each state with an even number of $|1\rangle$ has the same probability of occur, while an odd number of $|1\rangle$ is impossible. The remaining steps are trivial, and correctness derives from the fact that communication is reliable and the exclusive or operator will find an even number of bits at 1.

For T_1, we note that applying Z corresponds to exchanging $|+\rangle$ and $|-\rangle$. Since this is applied to just one qubit, it is easy to show that

$$H^{\otimes n}\left(\bigotimes_{j=1}^{i-1} I \otimes Z \otimes \bigotimes_{j=i+1}^{n} I\right)|GHZ\rangle = \frac{1}{2^{\frac{n-1}{2}}} \sum_{x \in \{0,1\}^n \text{ with } \zeta_1(x) \text{ odd}} |x\rangle$$

The remaining part of the proof coincides with the one for T_0. □

4.3. Evaluating Security Properties

Anonymity of the protocol consists in the fact that no other player can derive the identity of the sender: no one can determine his identity within the set of possible senders, even when monitoring all transmissions by following the path of all messages and reading them. In particular, receivers should not learn the identity of the sende. We verify this property by proving that no test can tell which participant is the sender. Formally,

Property 2 (External Attacker Anonymity)**.** *Let $b \in \{0,1\}$,and $(i,j) \in N \times N$. Then*

$$\left\langle |GHZ\rangle, \boldsymbol{QAT}_i^b \right\rangle \approx_{Test} \left\langle |GHZ\rangle, \boldsymbol{QAT}_j^b \right\rangle$$

Proof sketch. It is a corollary of the next property. □

Anonymity of the protocol is resistant also to active attackers that can compromise other participants different from the sender, if at least two processes remain honest. Let $M \subset N$ be the set of compromised agents' indexes, with $N \setminus M$ containing at least two indexes. We model the attacked protocol $\mathbf{Q\hat{A}T}_i$ as before, but we omit compromised agents. This means that we describe a system with M free qubits not owned by any process, thus controllable by the attacker.

$$\mathbf{Q\hat{A}T}_i^b := \mathbf{Sender}_i^b \parallel \Big|\Big|_{j \neq i \in N \setminus M} \mathbf{Receiver}_j \qquad \text{with } i \in N \setminus M$$

To model a specific attacker, we could use tests of the form $T = \mathbf{Attacker} \parallel ||_{j \in M} \mathbf{Compromised}_j$ with **Attacker** a process determining the identity of the sender thanks to the information provided by the compromised agents $\mathbf{Compromised}_j$. Instead of explicitly modelling each possible attack strategy, we implicitly consider all of them by the universal quantification of testing equivalence.

Property 3 (Internal Attacker Anonymity)**.** *Let $b \in \{0,1\}$, and $(i,j) \in (N \setminus M) \times (N \setminus M)$. Then*

$$\left\langle |GHZ\rangle, \boldsymbol{Q\hat{A}T}_i^b \right\rangle \approx_{Test} \left\langle |GHZ\rangle, \boldsymbol{Q\hat{A}T}_j^b \right\rangle$$

Proof sketch. Consider the alternative characterization of testing equivalence of Remark 1. Given a generic test T and a scheduler $\tilde{s}_i$ for $\left\langle |GHZ\rangle, \mathbf{Q\hat{A}T}_i^b \parallel T \right\rangle$, we build the scheduler $\tilde{s}_j$ for $\left\langle |GHZ\rangle, \mathbf{Q\hat{A}T}_j^b \parallel T \right\rangle$ simply by replacing each occurrence of i with j (and vice versa) in the tags of $\tilde{s}_i$. In the following, we prove that the success probability of $\left\langle |GHZ\rangle, \mathbf{Q\hat{A}T}_i^b \parallel T \right\rangle$ with $\tilde{s}_i$ coincides with the one of $\left\langle |GHZ\rangle, \mathbf{Q\hat{A}T}_j^b \parallel T \right\rangle$ with $\tilde{s}_j$.

A critical point in the proof is that, thanks to their locality, quantum operations performed by any agent (included the compromised ones) commute with any operation performed by some other agent. Formally, if both $s_1 s_2 \tilde{s}$ and $s_2 s_1 \tilde{s}$ are non-blocking schedulers and s_1 causes a quantum operation, then if $\langle |\psi\rangle, P \parallel T\rangle \xrightarrow{p_1} \langle |\psi_1\rangle, P_1 \parallel T_1\rangle \xrightarrow{p_2} \langle |\psi_2\rangle, P_2 \parallel T_2\rangle$ is a run of $s_1 s_2$, a run for $s_2 s_1$ exists $\langle |\psi\rangle, P \parallel T\rangle \xrightarrow{p_1'} \left\langle |\psi_1'\rangle, P_1' \parallel T_1' \right\rangle \xrightarrow{p_2'} \left\langle |\psi_{2'}\rangle, P_2' \parallel T_2' \right\rangle$ such that the final states and overall probability coincide ($|\psi_2\rangle = |\psi_{2'}\rangle$ and $p_1 p_2 = p_1' p_2'$). Thus, for $\tilde{s}_i$, we will only consider schedulers that start with all the quantum operations of the sender, followed by the ones of honest agents.

The identity of the sender is not revealed by the classical bit that it broadcasts: such bits are always in a fair probability distribution. More in detail, assume that the state is GHZ, i.e. the sender applied the I unitary. After applying H, the measurement in the standard basis of the sender's qubit has two possible outcomes (without loss of generality assume the first qubit is acted upon):

the state decays as $\frac{1}{\sqrt{2}}(|00\ldots0\rangle + |01\ldots1\rangle)$ with classical outcome 0 and probability $1/2$, or

the state decays as $\frac{1}{\sqrt{2}}(|10\ldots0\rangle - |11\ldots1\rangle)$ with classical outcome 1 and probability $1/2$.

Instead, the same operation on GHZ after a phase flip (caused by the sender's Z unitary) has outcomes:

the state decays as $\frac{1}{\sqrt{2}}(|00\ldots0\rangle - |01\ldots1\rangle)$ with classical outcome 0 and probability $1/2$, or

the state decays as $\frac{1}{\sqrt{2}}(|10\ldots0\rangle + |11\ldots1\rangle)$ with classical outcome 1 and probability $1/2$.

In both cases the outcome is uniformly random, and thus no information can be gained by observing it. Furthermore, the other qubits are still entangled in a (smaller) GHZ state, possibly with a phase flip applied if the outcome is 1, meaning that the analysis is equal also for the measurements of other honest participants.

At the end of this phase in which honest participants act, the compromised ones can freely observe their local quantum state (defined via the partial trace), which however will always be either $|GHZ\rangle$ of size m or $(I^{\otimes(m-1)} \otimes Z)|GHZ\rangle$ based on the b bit. By construction of $\tilde{s}_j$, it will replicate the actions performed by $\tilde{s}_i$ starting from the same quantum state. We conclude that no test can discriminate between $\mathbf{Q\hat{A}T}_i^b$ and $\mathbf{Q\hat{A}T}_j^b$ because all broadcast values are perfectly random, (even for the sender) and the set of reachable quantum states and their respective probability is independent of the sender's identity. □

There is also an even higher security guarantees of the protocol, marking an advantage with respect to its classical counterparts. Namely, the protocol is *traceless*: the sender can always deny having sent, even if the attacker have access to the internal states of all the players. This means that there is no private information left in the quantum states, thus there is no need to protect or destroy it.

We modify our lqCCS model by making the quantum state visible.

$$\mathbf{Q\ddot{A}T}_i^b := \mathbf{S\ddot{e}nder}_i^b \parallel \Big|\Big|_{j \neq i \in N \setminus M} \mathbf{R\ddot{e}ceiver}_j \qquad \text{with } i \in N \setminus M$$

$$\mathbf{S\ddot{e}nder}_i^b := \textbf{if } b = 0 \textbf{ then } t_i{:}I(q_i).\mathbf{R\ddot{e}ceiver}_i \textbf{ else } t_i{:}Z(q_i).\mathbf{R\ddot{e}ceiver}_i$$

$$\mathbf{R\ddot{e}ceiver}_i := t_i{:}H(q_i).t_i{:}\mathcal{M}_{01}(q_i \triangleright x_i).(c_i !!! x_i \parallel c_i ??? \tilde{x}.t_i{:}out_i!\bigoplus_{j \in N} x_j \parallel t_i'{:}qout_i!q_i)$$

Note that $\mathbf{Q\ddot{A}T}_i^b$ is obtained by adding a trailing $qout_i!q_i$ to the behaviour of each agent, with $qout_i$ a dedicated quantum channel of agent i.

In spite of considering such a powerful attacker, no test can tell which participant is the sender.

Property 4 (Tracelessness)**.** *Let* $b \in \{0,1\}$*, and* $(i,j) \in (N \setminus M) \times (N \setminus M)$*. Then*

$$\left\langle |GHZ\rangle, \ddot{\boldsymbol{AT}}_i^b \right\rangle \approx_{Test} \left\langle |GHZ\rangle, \ddot{\boldsymbol{AT}}_j^b \right\rangle$$

Proof. The proof follows the argument for Property 3. In particular, we can consider only the non-blocking schedulers where quantum operations of honest participants are performed in advance. Assume that $b = 0$. Then, we reach a configuration with quantum state $|x\rangle \otimes |GHZ\rangle_m$ if $\zeta_1(x)$ is even or $|x\rangle \otimes (I \otimes Z)\,|GHZ\rangle_m$ if $\zeta_1(x)$ is odd, for some $x \in \{0,1\}^{(n-m)}$ with equal probability. Similarly, if $b = 1$, we reach $|x\rangle \otimes |GHZ\rangle_m$ if $\zeta_1(x)$ is odd or $|x\rangle \otimes (I \otimes Z)\,|GHZ\rangle_m$ if $\zeta_1(x)$ is even. Thus, neither the reachable states, nor their relative probability are influenced by the sender's identity. □

5. Conclusions and Future Work

We have presented a testing semantics for a quantum extension of value-passing CCS, where tag-based syntactic schedulers ensure compliance with the observability limitations prescribed by the principles of quantum theory, namely, that revealing the state of a qubit unavoidably implies measurement-induced collapse. Our formal development allowed us to analyse the Quantum Anonymous Transmission Protocol, proving that it correctly broadcasts classical bits while guaranteeing robust security properties, namely anonymity for various attacker models. Through this real-world case study we also demonstrate the practical utility and expressiveness of our framework.

Several promising directions for future work remain. We plan to investigate the compositionality properties of our testing preorders to understand how verified subsystems behave when scaled into larger, complex quantum networks. Moreover, we will investigate decision procedures for our testing preorder via alternative labelled characterizations (Hennessy and Ingólfsdóttir, 1993; Cleaveland and Riely, 1994; Nicola and Pugliese, 2000; Bernardi, Castellani, Laforgue and Stefanesco, 2025; Bernardi, Férée and Lopez, 2026). This would significantly ease the burden of proving protocols properties, paving the way for the automated verification of next-generation quantum communication protocols.

References

Andrés, M.E., Palamidessi, C., van Rossum, P., Sokolova, A., 2011. Information hiding in probabilistic concurrent systems. Theoretical Computer Science 412, 3072–3089.

Ben-Or, M., Hassidim, A., 2005. Fast quantum byzantine agreement, in: STOC 2005, ACM. p. 481–485. doi:10.1145/1060590.1060662.

Bennet, C.H., Brassard, G., 2014. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science 560, 7–11. doi:10.1016/j.tcs.2014.05.025.

Bernardi, G., Castellani, I., Laforgue, P., Stefanesco, L., 2025. Constructive characterisations of the must-preorder for asynchrony, in: Vafeiadis, V. (Ed.), ESOP 2025, Springer. pp. 88–116. doi:10.1007/978-3-031-91118-7_4.

Bernardi, G., Férée, H., Lopez, G., 2026. A uniform characterisation of the (a)synchronous must-preorder. URL: https://hal.science/hal-05602369, doi:10.4230/LIPIcs. working paper or preprint.

Bernardo, M., 2022. Probabilistic trace and testing semantics: The importance of being coherent. Foundations and Trends in Programming Languages 7, 244–332. doi:10.1561/2500000056.

Bernardo, M., De Nicola, R., Loreti, M., 2014. Revisiting trace and testing equivalences for nondeterministic and probabilistic processes. Logical Methods in Computer Science 10.

Bonchi, F., Sokolova, A., Vignudelli, V., 2022. The theory of traces for systems with nondeterminism, probability, and termination. Logical Methods in Computer Science Volume 18, Issue 2. URL: https://lmcs.episciences.org/6261, doi:10.46298/lmcs-18(2:21)2022.

Brassard, G., 2003. Quantum communication complexity. Foundations of Physics 33, 1593–1616. doi:10.1023/A:1026009100467.

Canetti, R., Cheung, L., Kaynar, D.K., Liskov, M.D., Lynch, N.A., Pereira, O., Segala, R., 2006. Time-bounded task-PIOAs: A framework for analyzing security protocols, in: Dolev, S. (Ed.), DISC 2006, Springer. pp. 238–253.

Ceragioli, L., Di Lavore, E., Lomurno, G., Tedeschi, G., 2025a. A coalgebraic model of quantum bisimulation, in: Johnson, M., Myers, D.J. (Eds.), ACT 2024, Open Publishing Association. p. 249–269. doi:10.4204/eptcs.429.14.

Ceragioli, L., Gadducci, F., Lomurno, G., Tedeschi, G., 2024a. Effect semantics for quantum process calculi, in: Majumdar, R., Silva, A. (Eds.), CONCUR 2024, Schloss Dagstuhl - Leibniz-Zentrum für Informatik. pp. 16:1–16:22.

Ceragioli, L., Gadducci, F., Lomurno, G., Tedeschi, G., 2024b. Quantum bisimilarity is a congruence under physically admissible schedulers, in: Kiselyov, O. (Ed.), APLAS 2024, Springer. pp. 176–195. doi:10.1007/978-981-97-8943-6_9.

Ceragioli, L., Gadducci, F., Lomurno, G., Tedeschi, G., 2024c. Quantum bisimilarity via barbs and contexts: Curbing the power of non-deterministic observers. Proceedings of the ACM on Programming Languages 8, 43:1269–43:1297.

Ceragioli, L., Gadducci, F., Lomurno, G., Tedeschi, G., 2024d. Testing quantum processes, in: Margaria, T., Steffen, B. (Eds.), ISoLA 2024, Part I, Springer. pp. 132–151. doi:10.1007/978-3-031-73709-1_9.

Ceragioli, L., Gadducci, F., Lomurno, G., Tedeschi, G., 2026. Verification of quantum protocols adopting physically admissible schedulers. ACM Transactions on Quantum Computing URL: https://doi.org/10.1145/3830909, doi:10.1145/3830909. just Accepted.

Ceragioli, L., Lomurno, G., Tedeschi, G., 2025b. Reconciling quantum theory and process equivalence via physically admissible schedulers, in: Tutu, I. (Ed.), WADT 2024, Springer. pp. 111–133. doi:10.1007/978-3-031-88930-1_6.

Chatzikokolakis, K., Norman, G., Parker, D., 2009. Bisimulation for demonic schedulers, in: de Alfaro, L. (Ed.), FOSSACS 2009, Springer. pp. 318–332.

Chatzikokolakis, K., Palamidessi, C., 2007. Making random choices invisible to the scheduler, in: Caires, L., Vasconcelos, V.T. (Eds.), CONCUR 2007, Springer. pp. 42–58.

Christandl, M., Wehner, S., 2005. Quantum anonymous transmissions, in: Roy, B. (Ed.), ASIACRYPT 2005, Springer. pp. 217–235.

Cleaveland, R., Riely, J., 1994. Testing-based abstractions for value-passing systems, in: Jonsson, B., Parrow, J. (Eds.), CONCUR 1994, Springer. pp. 417–432. doi:10.1007/978-3-540-48654-1_31.

Davidson, T.A.S., 2012. Formal Verification Techniques Using Quantum Process Calculus. Ph.D. thesis. University of Warwick, UK.

De Nicola, R., 1986. Testing Equivalences and Fully Abstract Models for Communicating Systems. Ph.D. thesis. University of Edinburgh, UK.

De Nicola, R., Hennessy, M., 1984. Testing equivalences for processes. Theoretical Computer Science 34, 83–133.

Deng, Y., 2018. Bisimulations for probabilistic and quantum processes, in: Schewe, S., Zhang, L. (Eds.), CONCUR 2018, Schloss Dagstuhl - Leibniz-Zentrum für Informatik. pp. 2:1–2:14.

Elder, K., Giemsa, D., Gunkel, M., Nikiforov, O., Wissel, F., 2024. Pan-European QKD deployments within the EuroQCI initiative, in: ECOC 2024, pp. 1770–1772.

Feng, Y., Duan, R., Ji, Z., Ying, M., 2007. Probabilistic bisimulations for quantum processes. Information and Computation 205, 1608–1639. doi:10.1016/j.ic.2007.08.001.

Feng, Y., Duan, R., Ying, M., 2012. Bisimulation for quantum processes. ACM Transactions on Programming Languages and Systems 34, 17:1–17:43.

Feng, Y., Ying, M., 2015. Toward automatic verification of quantum cryptographic protocols, in: Aceto, L., de Frutos-Escrig, D. (Eds.), CONCUR 2015, Schloss Dagstuhl - Leibniz-Zentrum für Informatik. pp. 441–455.

van Glabbeek, R.J., 1990. The linear time-branching time spectrum (extended abstract), in: Baeten, J.C.M., Klop, J.W. (Eds.), CONCUR 1990, Springer. pp. 278–297. doi:10.1007/BFB0039066.

Hennessy, M., 1991. A proof system for communicating processes with value-passing. Formal Aspects of Computing 3, 346–366. doi:10.1007/BF01642508.

Hennessy, M., Ingólfsdóttir, A., 1993. A theory of communicating processes with value passing. Information and Computation 107, 202–236. doi:10.1006/INCO.1993.1067.

Kubota, T., Kakutani, Y., Kato, G., Kawano, Y., Sakurada, H., 2012. Application of a process calculus to security proofs of quantum protocols, in: Arabnia, H.R., Gravvanis, G.A., Solo, A.M.G. (Eds.), FCS 2012, CSREA Press. pp. 141–147.

Kubota, T., Kakutani, Y., Kato, G., Kawano, Y., Sakurada, H., 2016. Semi-automated verification of security proofs of quantum cryptographic protocols. Journal of Symbolic Computation 73, 192–220.

Lalire, M., 2006. Relations among quantum processes: Bisimilarity and congruence. Mathematical Structures in Computer Science 16, 407–428.

Larsen, K.G., Skou, A., 1991. Bisimulation through probabilistic testing. Information and Computation 94, 1–28.

Liu, J., Le, T., Ji, T., Yu, R., Farfurnik, D., Byrd, G., Stancil, D., 2025. The road to quantum internet: Progress in quantum network testbeds and major demonstrations. Progress in Quantum Electronics 99, 100551. doi:10.1016/j.pquantelec.2024.100551.

Mousavi, M.R., Peters, K., Schmitt, A., 2024. Towards a formal testing theory for quantum processes, in: Margaria, T., Steffen, B. (Eds.), ISoLA 2024, Springer. pp. 111–131. doi:10.1007/978-3-031-73709-1_8.

Nicola, R.D., Pugliese, R., 2000. Linda-based applicative and imperative process algebras. Theoretical Computer Science 238, 389–437. doi:10.1016/S0304-3975(99)00339-4.

Nielsen, M.A., Chuang, I.L., 2010. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press.

Nurhadi, A.I., Syambas, N.R., 2018. Quantum key distribution (QKD) protocols: A survey, in: ICWT 2018, IEEE Computer Society. pp. 1–5.

Singh, S., Doosti, M., Mathur, N., Delavar, M., Mantri, A., Ollivier, H., Kashefi, E., 2023. Towards a unified quantum protocol framework: Classification, implementation, and use cases. CoRR abs/2310.12780.

Song, L., Feng, Y., Zhang, L., 2015. Decentralized bisimulation for multiagent systems, in: Weiss, G., Yolum, P., Bordini, R.H., Elkind, E. (Eds.), AAMAS 2015, ACM. pp. 209–217.

Yi, W., Larsen, K.G., 1992. Testing probabilistic and nondeterministic processes, in: Jr., R.J.L., Uyar, M.Ü. (Eds.), PSTV 1992, North-Holland. pp. 47–61.