# Toward Automatic Verification of Quantum Cryptographic Protocols

Yuan Feng[1,3] and Mingsheng Ying[1,2]

1 University of Technology Sydney, Australia,
{Yuan.Feng,Mingsheng.Ying}@uts.edu.au

2 Department of Computer Science and Technology, National Laboratory for Information Science and Technology, Tsinghua University, China

3 AMSS-UTS Joint Research Laboratory for Quantum Computation, Chinese Academy of Sciences, China

## Abstract

Several quantum process algebras have been proposed and successfully applied in verification of quantum cryptographic protocols. All of the bisimulations proposed so far for quantum processes in these process algebras are state-based, implying that they only compare individual quantum states, but not a combination of them. This paper remedies this problem by introducing a novel notion of distribution-based bisimulation for quantum processes. We further propose an approximate version of this bisimulation that enables us to prove more sophisticated security properties of quantum protocols which cannot be verified using the previous bisimulations. In particular, we prove that the quantum key distribution protocol BB84 is sound and (asymptotically) secure against the intercept-resend attacks by showing that the BB84 protocol, when executed with such an attacker concurrently, is approximately bisimilar to an ideal protocol, whose soundness and security are obviously guaranteed, with at most an exponentially decreasing gap.

**1998 ACM Subject Classification** C.2.2 Protocol verification

**Keywords and phrases** Quantum cryptographic protocols, Verification, Bisimulation, Security

**Digital Object Identifier** 10.4230/LIPIcs.CONCUR.2015.441

## 1 Introduction

Quantum cryptography can provide unconditional security; it allows the realisation of cryptographic tasks that are proven or conjectured to be impossible in classical cryptography. The security of quantum cryptographic protocols is mathematically provable, based on the principles of quantum mechanics, without imposing any restrictions on the computational capacity of attackers. The proof is, however, often notoriously difficult, which is evidenced by the 50 pages long security proof of the quantum key distribution protocol BB84 [20]. It is hard to imagine such an analysis being carried out for more sophisticated quantum protocols. Thus, techniques for (semi-)automated verification of quantum protocols will be indispensable, given that quantum communication systems are already commercially available.

Process algebra has been successfully applied in the verification of classical (non-quantum) cryptographic protocols [21, 25]. One key step for such a process algebraic approach is a suitable notion of *bisimulation* which has appropriate distinguishing power and is preserved by various process constructs. Intuitively, two systems are bisimilar if and only if each observable action of one of them can be simulated by the other by performing the same observable action (possibly preceded and/or followed by some unobservable internal actions), and furthermore,

26th International Conference on Concurrency Theory (CONCUR 2015).
Editors: Luca Aceto and David de Frutos Escrig; pp. 441–455
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the resultant systems are again bisimilar. To verify a cryptographic protocol, we first give a *specification* which is an ideal protocol with obvious correctness and security, and then show that the given protocol is bisimilar (or approximately bisimilar with a small perturbation) to the specification.

In the last 10 years, several quantum process algebras like CQP [13], QPAlg [16] and qCCS [10] have been introduced, which provide an intuitive but rigorous way to model and reason about quantum communication systems. In particular, they have been adopted in verification of several popular quantum communication protocols such as Teleportation, Superdense Coding, etc. Similar to the classical case, the notion of bisimulation is crucial in the process algebra-based verification of quantum protocols. Actually, several different versions of bisimulation have been proposed for quantum processes in the recent literature [19, 27, 11, 5, 6]. A key feature of all of them is that they are state-based in the sense that they only compare individual configurations but not a combination of them. More explicitly, they are defined to be relations over configurations which are pairs of a quantum process and a density operator describing the state of environment quantum systems. However, when distributions of configurations are considered (which is inevitable for protocols where randomness is employed or quantum measurement is involved), state-based bisimulations are too discriminative – they distinguish some distributions which will never be distinguished by any outside observers, thereby providing the potential attacker of a cryptographic protocol with unrealistic power. As an extreme example, a state-based bisimulation distinguishes the distribution $p\langle \mathbf{nil}, \rho\rangle + (1-p)\langle \mathbf{nil}, \sigma\rangle$ from the single configuration $\langle \mathbf{nil}, p\rho + (1-p)\sigma\rangle$ if $\rho \neq \sigma$, where **nil** is the *dead* process incapable of performing any action.

In this paper, we propose a novel bisimulation for quantum processes which is defined directly on distributions of quantum configurations. Compared with existing bisimulations in the literature, our definition is strictly coarser (in particular, equates the two distributions presented above) and takes into account the combination of accompanied quantum states. We further define a pseudo-metric to characterise the extent to which two quantum processes are bisimilar. Note that we only consider quantum processes written in qCCS, but the main results can be generalised to other quantum process algebras like CQP and QPAlg easily.

To illustrate the utility of distribution-based bisimulation and the pseudo-metric in verification of quantum cryptographic protocols, we analyse the soundness and security of the well-known BB84 quantum key distribution protocol [4]. For the soundness, we show that when executed alone (without the presence of an attacker), BB84 is bisimilar to an ideal protocol which always returns a uniformly distributed (conditioning on a given key size) key. For the security analysis, we prove that when BB84 is executed concurrently with an intercept-resend attacker, the whole system is approximately bisimilar, with at most an exponentially decreasing gap, to an ideal protocol which never reports failure or information leakage. To the best of our knowledge, this is the first time (a weak notion of) security of BB84 is formally described and verified in the quantum process algebra approach.

*Related works.* The problem of existing bisimulations, as pointed out in the third paragraph of this section, was also noted by Kubota et al. [17]. To deal with it, they adopted two different semantics for quantum measurements. When a measurement induces a probability distribution in which all configurations have the same observable actions, it is represented semantically as a super-operator obtained by discarding the measurement outcome (thus no probabilistic branching is produced, and all post-measurement quantum states are merged). Otherwise, the measurement has the same semantics as in the original qCCS. This treatment solves the problem when probabilistic behaviours are only induced by quantum measurements. However, it does not work when probabilistic choice is included in the syntax level, as we do in describing BB84 protocol in this paper. Furthermore, it brings difficulty in deciding the right semantics of a quantum process where a measurement is involved, as determining if the observable actions of the post-measurement configurations are all the same might not be easy; sometimes it even depends on the later input from the environment. In this paper, we solve this problem by revising the definition of bisimulation, instead of the definition of semantics.

In the same paper [17], Kubota et al. applied qCCS (with the semantic modification mentioned above) to show the security of BB84. They proved that BB84 is bisimilar to an EDP-based protocol, following the proof of Shor and Preskill [26]. However, this should not be regarded as a complete security proof, as it relies on the security of the EDP-based protocol. In contrast, our approach shows the security of BB84 directly. Note that for this purpose, a notion of approximate bisimulation, which was not presented in [17], is necessary, as BB84 is secure only in the sense that the eavesdropper's information about the secure key obtained by the legitimate parties is arbitrarily small (but still can be strictly positive) when the number of qubits transmitted (called the *security parameter*) goes to infinity.

Software tools based on the quantum process algebra CQP have been developed in [2] and [3] to check the equivalence between quantum sequential programs as well as concurrent protocols. These tools were applied to verify the correctness of protocols like Teleportation, Bit Flip Error Correction Code, and Quantum Secret Sharing. However, verification of security properties in cryptographic protocols such as BB84 has not been reported yet.

Besides the process algebra approach, model-checking is another promising approach for verification of quantum cryptographic protocols. For example, by observing the fact that the quantum states appearing in BB84, when only intercept-resend eavesdroppers are considered, are all the so-called stabiliser states which can be efficiently encoded in a classical way, Nagarajan et al. [22] analysed the security of BB84 by using the probabilistic model checker PRISM [18].

## 2 Preliminaries

In this section we review the model of probabilistic labelled transition systems (pLTSs) and the notion of lifted relations. Later on we will interpret the behaviour of quantum processes in terms of pLTSs.

### 2.1 Probabilistic labelled transition systems

A (finite-support) *probability distribution* over a set $S$ is a function $\mu : S \to [0,1]$ with $\mu(s) > 0$ for finitely many $s \in S$ and $\sum_{s\in S} \mu(s) = 1$; the support of such a $\mu$ is the set $\lceil \mu \rceil = \{ s \in S \mid \mu(s) > 0 \}$. The *point distribution* $\overline{s}$ assigns probability 1 to $s$ and 0 to all other elements of $S$, so that $\lceil \overline{s} \rceil = \{s\}$. We use $D(S)$ to denote the set of probability distributions over $S$, ranged over by $\mu, \nu$ etc. If $\sum_{i\in I} p_i = 1$ for some collection of $p_i \geq 0$, and $\mu_i \in D(S)$, then $\sum_{i\in I} p_i \cdot \mu_i \in D(S)$ is a *combined* probability distribution with $(\sum_{i\in I} p_i \cdot \mu_i)(s) = \sum_{i\in I} p_i \cdot \mu_i(s)$. We always assume the index set $I$ to be finite.

▶ **Definition 1.** A *probabilistic labelled transition system* (pLTS) is a triple $\langle S, \mathsf{Act}, \longrightarrow \rangle$, where $S$ is a set of *states*, $\mathsf{Act}$ is a set of *transition labels* with a special element $\tau$ included, and the *transition relation* $\longrightarrow$ is a subset of $S \times \mathsf{Act} \times D(S)$.

## 2.2 Lifting relations

In a pLTS actions are only performed by states, in that they are given by relations from states to distributions. But in general we allow distributions over states to perform an action. For this purpose, we *lift* these relations to distributions [7, 6].

▶ **Definition 2** (Lifting)**.** Let $\mathcal{R} \subseteq S \times D(S)$ be a relation. The lifted relation, denoted by $\mathcal{R}$ again for simplicity, is the smallest relation $\mathcal{R} \subseteq D(S) \times D(S)$ that satisfies

1. $s\mathcal{R}\nu$ implies $\overline{s}\mathcal{R}\nu$, and
2. (Linearity) $\mu_i\mathcal{R}\nu_i$ for $i \in I$ implies $(\sum_{i\in I} p_i \cdot \mu_i)\mathcal{R}(\sum_{i\in I} p_i \cdot \nu_i)$ for any $p_i \in [0,1]$ with $\sum_{i\in I} p_i = 1$.

We apply this operation to the relations $\xrightarrow{\alpha}$ in a pLTS for $\alpha \in \mathsf{Act}$. Thus as source of a relation $\xrightarrow{\alpha}$ we also allow distributions. But $\overline{s} \xrightarrow{\alpha} \mu$ is more general than $s \xrightarrow{\alpha} \mu$, because if $\overline{s} \xrightarrow{\alpha} \mu$ then there is a collection of distributions $\mu_i$ and probabilities $p_i$ such that $s \xrightarrow{\alpha} \mu_i$ for each $i \in I$ and $\mu = \sum_{i\in I} p_i \cdot \mu_i$ with $\sum_{i\in I} p_i = 1$; that is, we allow different transitions to be combined together, provided that they have the same source $s$ and the same label $\alpha$.

Sometimes we also need to lift a relation on states, say a state-based bisimulation, to distributions. This can be done by the following two steps. Let $\mathcal{R} \subseteq S \times S$ be such a relation. First, it induces a relation $\hat{\mathcal{R}} \subseteq S \times D(S)$ between states and distributions: $\hat{\mathcal{R}} := \{(s, \overline{t}) \mid s\mathcal{R}t\}$. Then we can use Definition 2 to lift $\hat{\mathcal{R}}$ to distributions. Note that when $\mathcal{R}$ is an equivalence relation over $S$, the lifted relation over $D(S)$ coincides with the lifting defined in [15].

In Definition 2, linearity tells us how to compare two linear combinations of distributions. Sometimes we need a dual notion of decomposition. Intuitively, if a relation $\mathcal{R}$ is *left-decomposable* and $\mu\mathcal{R}\nu$, then for any decomposition of $\mu$ there exists some corresponding decomposition of $\nu$.

▶ **Definition 3** (Left-decomposable)**.** A binary relation over distributions, $\mathcal{R} \subseteq D(S) \times D(S)$, is called *left-decomposable* if $(\sum_{i\in I} p_i \cdot \mu_i)\mathcal{R}\nu$ implies that $\nu$ can be written as $(\sum_{i\in I} p_i \cdot \nu_i)$ such that $\mu_i\mathcal{R}\nu_i$ for every $i \in I$.

The next lemma shows that any lifted relation is left-decomposable.

▶ **Lemma 4** ([6])**.** *For any $\mathcal{R} \subseteq S \times D(S)$ or $S \times S$, the lifted relation over distributions is left-decomposable.*

With the help of lifted relations, we are now able to define various (weak) transitions between distributions for a pLTS.

▶ **Definition 5.** Given a pLTS $\langle S, \mathsf{Act}, \longrightarrow\rangle$, we define the following transitions over distributions:

1. $\xrightarrow{\hat{\tau}}$. Let $s \xrightarrow{\hat{\tau}} \mu$ if either $s \xrightarrow{\tau} \mu$ or $\mu = \overline{s}$, and lift it to distributions;
2. $\xrightarrow{\hat{\alpha}}$ for $\alpha \neq \tau$. Let $s \xrightarrow{\hat{\alpha}} \mu$ if $s \xrightarrow{\alpha} \mu$, and lift it to distributions;
3. $\overset{\hat{\tau}}{\Longrightarrow}$. Let $\overset{\hat{\tau}}{\Longrightarrow} = (\xrightarrow{\hat{\tau}})^*$ be the reflexive and transitive closure of $\xrightarrow{\hat{\tau}}$;
4. $\overset{\hat{\alpha}}{\Longrightarrow}$ for $\alpha \neq \tau$. Let $\overset{\hat{\alpha}}{\Longrightarrow} = \overset{\hat{\tau}}{\Longrightarrow}\xrightarrow{\hat{\alpha}}\overset{\hat{\tau}}{\Longrightarrow}$. For point distributions, we often write $s \overset{\hat{\alpha}}{\Longrightarrow} \nu$ instead of $\overline{s} \overset{\hat{\alpha}}{\Longrightarrow} \nu$.

Note that here $\overset{\hat{\alpha}}{\Longrightarrow}$ is not a lifted transition. However, the next lemma shows that it is still both linear and left-decomposable.

▶ **Lemma 6** ([6])**.** *The transition relations $\overset{\hat{\alpha}}{\Longrightarrow}$ are both linear and left-decomposable.*

# 3 qCCS: Syntax and Semantics

In this section, we review the syntax and semantics of qCCS, a quantum extension of value-passing CCS introduced in [10, 27], and a notion of state-based bisimulation for qCCS processes presented in [6]. We assume the readers are familiar with the basic notions in quantum information theory; for those who are not, please refer to [23].

## 3.1 Syntax

We assume three types of data in qCCS: $\mathsf{Bool}$ for booleans, real numbers $\mathsf{Real}$ for classical data, and qubits $\mathsf{Qbt}$ for quantum data. Let $cVar$, ranged over by $x, y, \dots$, be the set of classical variables, and $qVar$, ranged over by $q, r, \dots$, the set of quantum variables. It is assumed that $cVar$ and $qVar$ are both countably infinite. We assume a set $Exp$, which includes $cVar$ as a subset and is ranged over by $e, e', \dots$, of classical expressions over $\mathsf{Real}$, and a set of boolean-valued expressions $BExp$, ranged over by $b, b', \dots$, with the usual set of boolean operators $\mathrm{tt}$, $\mathrm{ff}$, $\neg$, $\wedge$, $\vee$, and $\rightarrow$. In particular, we let $e \bowtie e'$ be a boolean expression for any $e, e' \in Exp$ and $\bowtie \in \{>, <, \geq, \leq, =\}$. We further assume that only classical variables can occur free in data expressions and boolean expressions. Let $cChan$ be the set of classical channel names, ranged over by $c, d, \dots$, and $qChan$ the set of quantum channel names, ranged over by $\mathsf{c}, \mathsf{d}, \dots$. Let $Chan = cChan \cup qChan$. A relabeling function $f$ is a one-to-one function from $Chan$ to $Chan$ such that $f(cChan) \subseteq cChan$ and $f(qChan) \subseteq qChan$.

We often abbreviate the indexed set $\{q_1, \dots, q_n\}$ to $\tilde{q}$ when $q_1, \dots, q_n$ are distinct quantum variables and the dimension $n$ is understood. Sometimes we also use $\tilde{q}$ to denote the string $q_1 \dots q_n$. We assume a set of process constant schemes, ranged over by $A, B, \dots$. Assigned to each process constant scheme $A$ there are two non-negative integers $ar_c(A)$ and $ar_q(A)$. If $\tilde{x}$ is a tuple of classical variables with $|\tilde{x}| = ar_c(A)$, and $\tilde{q}$ a tuple of distinct quantum variables with $|\tilde{q}| = ar_q(A)$, then $A(\tilde{x}, \tilde{q})$ is called a process constant. When $ar_c(A) = ar_q(A) = 0$, we also denote by $A$ the (unique) process constant produced by $A$.

The syntax of qCCS terms can be given by the Backus-Naur form as

$$\begin{array}{rcl} t & ::= & \mathbf{nil} \mid A(\tilde{e}, \tilde{q}) \mid \alpha.t \mid t + t \mid t \| t \mid t \backslash L \mid t[f] \mid \mathbf{if}\ b\ \mathbf{then}\ t \\ \alpha & ::= & \tau \mid c?x \mid c!e \mid \mathsf{c}?q \mid \mathsf{c}!q \mid \mathcal{E}[\tilde{q}] \mid M[\tilde{q}; x] \end{array}$$

where $c \in cChan$, $x \in cVar$, $\mathsf{c} \in qChan$, $q \in qVar$, $\tilde{q} \subseteq qVar$, $e \in Exp$, $\tilde{e} \subseteq Exp$, $\tau$ is the silent action, $A$ is a process constant scheme, $f$ is a relabeling function, $L \subseteq Chan$, $b \in BExp$, $\mathcal{E}$ and $M$ are respectively a super-operator and a quantum measurement applying on the Hilbert space associated with the systems $\tilde{q}$.

To exclude quantum processes which are not physically implementable, we also require $q \notin qv(t)$ in $\mathsf{c}!q.t$ and $qv(t) \cap qv(u) = \emptyset$ in $t \| u$, where for a process term $t$, $qv(t)$ is the set of its free quantum variables which are not bound by quantum input $\mathsf{c}?q$. The notion of free classical variables in quantum processes can be defined in the usual way with the only modification that the quantum measurement prefix $M[\tilde{q}; x]$ has binding power on $x$. A quantum process term $t$ is closed if it contains no free classical variables, *i.e.*, $fv(t) = \emptyset$. We let $\mathcal{T}$, ranged over by $t, u, \cdots$, be the set of all qCCS terms, and $\mathcal{P}$, ranged over by $P, Q, \cdots$, the set of closed terms. To complete the definition of qCCS syntax, we assume that for each process constant $A(\tilde{x}, \tilde{q})$, there is a defining equation $A(\tilde{x}, \tilde{q}) := t$ where $fv(t) \subseteq \tilde{x}$ and $qv(t) \subseteq \tilde{q}$. Throughout the paper we implicitly assume the convention that process terms are identified up to $\alpha$-conversion.

The process constructs we give here are quite similar to those in classical CCS, and they also have similar intuitive meanings: **nil** stands for a process which does not perform any action; $c?x$ and $c!e$ are respectively classical input and classical output, while $\mathsf{c}?q$ and $\mathsf{c}!q$ are their quantum counterparts. $\mathcal{E}[\tilde{q}]$ denotes the action of performing the quantum operation $\mathcal{E}$ on the qubits $\tilde{q}$ while $M[\tilde{q};x]$ measures the qubits $\tilde{q}$ according to $M$ and stores the measurement outcome into the classical variable $x$. $+$ models nondeterministic choice: $t+u$ behaves like either $t$ or $u$ depending on the choice of the environment. $\|$ denotes the usual parallel composition. The operators $\backslash L$ and $[f]$ model restriction and relabeling, respectively: $t\backslash L$ behaves like $t$ but any action through the channels in $L$ is forbidden, and $t[f]$ behaves like $t$ where each channel name is replaced by its image under the relabeling function $f$. Finally, **if** $b$ **then** $t$ is the standard conditional choice where $t$ can be executed only if $b$ evaluates to tt.

An evaluation $\psi$ is a function from $cVar$ to $\mathsf{Real}$; it can be extended in an obvious way to functions from $Exp$ to $\mathsf{Real}$ and from $BExp$ to $\{\text{tt}, \text{ff}\}$, and finally, from $\mathcal{T}$ to $\mathcal{P}$. For simplicity, we still use $\psi$ to denote these extensions. Let $\psi\{v/x\}$ be the evaluation which differs from $\psi$ only in that it maps $x$ to $v$.

## 3.2 Transitional semantics

For each quantum variable $q \in qVar$, we assume a 2-dimensional Hilbert space $\mathcal{H}_q$ to be the state space of the $q$-system. For any $V \subseteq qVar$, we denote $\mathcal{H}_V = \bigotimes_{q\in V} \mathcal{H}_q$. In particular, $\mathcal{H} = \mathcal{H}_{qVar}$ is the state space of the whole environment consisting of all the quantum variables. Note that $\mathcal{H}$ is a countably-infinite dimensional Hilbert space. For any $V \subseteq qVar$ we denote by $\overline{V}$ the complement set of $V$ in $qVar$.

Suppose $P$ is a closed quantum process. A pair of the form $\langle P, \rho\rangle$ is called a configuration, where $\rho \in \mathcal{D}(\mathcal{H})$ is a density operator on $\mathcal{H}$.[1] The set of configurations is denoted by $Con$, and ranged over by $\mathcal{C}, \mathcal{D}, \ldots$. Let

$$\mathsf{Act} \quad = \quad \{\tau\} \cup \{c?v, c!v \mid c \in cChan, v \in \mathsf{Real}\} \cup \{\mathsf{c}?r, \mathsf{c}!r \mid \mathsf{c} \in qChan, r \in qVar\}.$$

For each $\alpha \in \mathsf{Act}$, we define the bound quantum variables $qbv(\alpha)$ of $\alpha$ as $qbv(\mathsf{c}?r) = \{r\}$ and $qbv(\alpha) = \emptyset$ if $\alpha$ is not a quantum input. The channel names used in action $\alpha$ is denoted by $cn(\alpha)$; that is, $cn(c?v) = cn(c!v) = \{c\}$, $cn(\mathsf{c}?r) = cn(\mathsf{c}!r) = \{\mathsf{c}\}$, and $cn(\tau) = \emptyset$. We also extend the relabelling function to $\mathsf{Act}$ in an obvious way. Then the transitional semantics of qCCS can be given by a pLTS $\langle Con, \mathsf{Act}, \longrightarrow\rangle$, where $\longrightarrow \subseteq Con \times \mathsf{Act} \times D(Con)$ is the smallest relation satisfying the inference rules depicted in Fig. 1. The symmetric forms for rules $Par$, $Com_C$, $Com_Q$, and $Sum$ are omitted. We abuse the notation slightly by writing $\mathcal{C} \xrightarrow{\alpha} \mathcal{D}$ if $\mathcal{C} \xrightarrow{\alpha} \overline{\mathcal{D}}$. We also use the obvious extension of the function $\|$ on configurations to distributions. To be precise, if $\mu = \sum_{i\in I} p_i\langle P_i, \rho_i\rangle$ then $\mu\|Q$ denotes the distribution $\sum_{i\in I} p_i\langle P_i\|Q, \rho_i\rangle$. Similar extension applies to $\mu[f]$ and $\mu\backslash L$.

## 3.3 State-based bisimulation

In this subsection, we recall the basic definitions and properties of the state-based bisimulation introduced in [6]. Let $\mathcal{C} = \langle P, \rho\rangle$ be a configuration and $\mathcal{E}$ a super-operator. We denote $qv(\mathcal{C}) = qv(P)$, $\text{env}(\mathcal{C}) = \text{tr}_{qv(P)}(\rho)$ being the quantum *environment* of process $P$ in $\mathcal{C}$, and $\mathcal{E}(\mathcal{C}) = \langle P, \mathcal{E}(\rho)\rangle$. Furthermore, for distribution $\mu = \sum_i p_i\mathcal{C}_i$ with $p_i > 0$ for each $i$, we write $qv(\mu) = \bigcup_i qv(\mathcal{C}_i)$, $\text{env}(\mu) = \sum_i p_i \cdot \text{env}(\mathcal{C}_i)$, and $\mathcal{E}(\mu) = \sum_i p_i\mathcal{E}(\mathcal{C}_i)$. For any $V \subseteq qVar$, denote by $SO(\mathcal{H}_V)$ the set of super-operators on $\mathcal{H}_V$.

[1] As $\mathcal{H}$ is infinite dimensional, $\rho$ should be understood as a density operator on some finite dimensional subspace of $\mathcal{H}$ which contains $\mathcal{H}_{qv(P)}$.

$$\textit{Tau}\qquad \frac{}{\langle \tau.P,\rho\rangle \xrightarrow{\tau} \langle P,\rho\rangle}$$

$$\textit{Out}_C\qquad \frac{v=[\![e]\!]}{\langle c!e.P,\rho\rangle \xrightarrow{c!v} \langle P,\rho\rangle}$$

$$\textit{Out}_Q\qquad \frac{}{\langle \mathsf{c}!q.P,\rho\rangle \xrightarrow{\mathsf{c}!q} \langle P,\rho\rangle}$$

$$\textit{Meas}\qquad \frac{M=\sum_{i\in I}\lambda_i E^i,\ \ p_i=\mathrm{tr}(E^i_{\tilde{r}}\rho)>0}{\langle M[\tilde{r};x].P,\rho\rangle \xrightarrow{\tau} \sum_{i\in I} p_i\langle P\{\lambda_i/x\}, E^i_{\tilde{r}}\rho E^i_{\tilde{r}}/p_i\rangle}$$

$$\textit{Com}_C\qquad \frac{\langle P_1,\rho\rangle \xrightarrow{c?v} \langle P_1',\rho\rangle,\ \ \langle P_2,\rho\rangle \xrightarrow{c!v} \langle P_2',\rho\rangle}{\langle P_1\|P_2,\rho\rangle \xrightarrow{\tau} \langle P_1'\|P_2',\rho\rangle}$$

$$\textit{Sum}\qquad \frac{\langle P,\rho\rangle \xrightarrow{\alpha} \mu}{\langle P+Q,\rho\rangle \xrightarrow{\alpha} \mu}$$

$$\textit{Cho}\qquad \frac{\langle P,\rho\rangle \xrightarrow{\alpha} \mu,\ \ [\![b]\!]=\mathrm{tt}}{\langle \textbf{if } b \textbf{ then } P,\rho\rangle \xrightarrow{\alpha} \mu}$$

$$\textit{Def}\qquad \frac{\langle t\{\tilde{v}/\tilde{x},\tilde{r}/\tilde{q}\},\rho\rangle \xrightarrow{\alpha} \mu,\ \ A(\tilde{x},\tilde{q}):=t,\ \ \tilde{v}=[\![\tilde{e}]\!]}{\langle A(\tilde{e},\tilde{r}),\rho\rangle \xrightarrow{\alpha} \mu}$$

$$\textit{Inp}_C\qquad \frac{v\in \mathsf{Real}}{\langle c?x.t,\rho\rangle \xrightarrow{c?v} \langle t\{v/x\},\rho\rangle}$$

$$\textit{Inp}_Q\qquad \frac{r\notin qv(\mathsf{c}?q.P)}{\langle \mathsf{c}?q.P,\rho\rangle \xrightarrow{\mathsf{c}?r} \langle P\{r/q\},\rho\rangle}$$

$$\textit{Oper}\qquad \frac{}{\langle \mathcal{E}[\tilde{r}].P,\rho\rangle \xrightarrow{\tau} \langle P,\mathcal{E}_{\tilde{r}}(\rho)\rangle}$$

$$\textit{Par}\qquad \frac{\langle P_1,\rho\rangle \xrightarrow{\alpha} \mu,\ \ qbv(\alpha)\cap qv(P_2)=\emptyset}{\langle P_1\|P_2,\rho\rangle \xrightarrow{\alpha} \mu\|P_2}$$

$$\textit{Com}_Q\qquad \frac{\langle P_1,\rho\rangle \xrightarrow{\mathsf{c}?r} \langle P_1',\rho\rangle,\quad \langle P_2,\rho\rangle \xrightarrow{\mathsf{c}!r} \langle P_2',\rho\rangle}{\langle P_1\|P_2,\rho\rangle \xrightarrow{\tau} \langle P_1'\|P_2',\rho\rangle}$$

$$\textit{Rel}\qquad \frac{\langle P,\rho\rangle \xrightarrow{\alpha} \mu}{\langle P[f],\rho\rangle \xrightarrow{f(\alpha)} \mu[f]}$$

$$\textit{Res}\qquad \frac{\langle P,\rho\rangle \xrightarrow{\alpha} \mu,\ \ cn(\alpha)\cap L=\emptyset}{\langle P\backslash L,\rho\rangle \xrightarrow{\alpha} \mu\backslash L}$$

**Figure 1** Transitional semantics of qCCS.

▶ **Definition 7.** A relation $\mathcal{R}\subseteq \mathit{Con}\times\mathit{Con}$ is closed under super-operator application if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies $\mathcal{E}(\mathcal{C})\mathcal{R}\mathcal{E}(\mathcal{D})$ for all $\mathcal{E}\in SO(\mathcal{H}_{\overline{qv(\mathcal{C})\cup qv(\mathcal{D})}})$. More generally, a relation $\mathcal{R}\subseteq D(\mathit{Con})\times D(\mathit{Con})$ is closed under super-operator application if $\mu\mathcal{R}\nu$ implies $\mathcal{E}(\mu)\mathcal{R}\mathcal{E}(\nu)$ for all $\mathcal{E}\in SO(\mathcal{H}_{\overline{qv(\mu)\cup qv(\nu)}})$.

▶ **Definition 8.**

1. A symmetric relation $\mathcal{R}\subseteq \mathit{Con}\times\mathit{Con}$ is called a *state-based ground bisimulation* if $\mathcal{C}\mathcal{R}\mathcal{D}$ implies that
   **(i)** $qv(\mathcal{C})=qv(\mathcal{D})$, and $\mathrm{env}(\mathcal{C})=\mathrm{env}(\mathcal{D})$,
   **(ii)** whenever $\mathcal{C}\xrightarrow{\alpha}\mu$, there exists $\nu$ such that $\mathcal{D}\overset{\hat{\alpha}}{\Longrightarrow}\nu$ and $\mu\mathcal{R}\nu$.
2. A relation $\mathcal{R}$ is a *state-based bisimulation* if it is a state-based ground bisimulation, and is closed under super-operator application.
3. Two quantum configurations $\mathcal{C}$ and $\mathcal{D}$ are state-based bisimilar, denoted by $\mathcal{C}\approx_s\mathcal{D}$, if there exists a state-based bisimulation $\mathcal{R}$ such that $\mathcal{C}\mathcal{R}\mathcal{D}$;
4. Two quantum process terms $t$ and $u$ are state-based bisimilar, denoted by $t\approx_s u$, if for any quantum state $\rho\in\mathcal{D}(\mathcal{H})$ and any evaluation $\psi$, $\langle t\psi,\rho\rangle\approx_s\langle u\psi,\rho\rangle$.

Note that in Clause 1.(ii) of the above definition, $\mu\mathcal{R}\nu$ means $\mu$ and $\nu$ are related by the relation lifted from $\mathcal{R}$. The following theorem is taken from [6].

▶ **Theorem 9.**

1. *The bisimilarity relation $\approx_s$ is the largest state-based bisimulation on Con, and it is an equivalence relation.*
2. *As a lifted relation on $D(\mathit{Con})$, $\approx_s$ is both linear and left-decomposable.*

## 4 Distribution-based bisimulation

Note that in [8], it has already been shown by examples that state-based bisimulation is sometimes too discriminative for probabilistic automata. These examples certainly work for quantum processes as well. Furthermore, as the following example indicates, the problem becomes more serious in the quantum setting, as the accompanied quantum states can and should be combined when simulating each other.

▶ **Example 10.** Let $M = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$ be a two-outcome measurement according to the computational basis, and $\mathcal{E}$ a super-operator with the Kraus operators being $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$. Let $\rho$ be a density operator on $\mathcal{H}_{\overline{\{q\}}}$, and $\mathcal{C} := \langle M[q;x].\mathbf{nil}, |+\rangle_q\langle +| \otimes \rho\rangle$ and $\mathcal{D} := \langle \mathcal{E}[q].\mathbf{nil}, |+\rangle_q\langle +| \otimes \rho\rangle$ be two configurations where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Note that in the process $M[q;x].\mathbf{nil}$, the measurement outcome is never used (as $x \notin fv(\mathbf{nil})$), while the effect of $\mathcal{E}[q]$ is exactly measuring the system $q$ according to $M$, but ignoring the measurement outcome. Thus we definitely would like to regard $\mathcal{C}$ and $\mathcal{D}$ as being bisimilar[2].

However, we can show that $\mathcal{C} \not\approx_s \mathcal{D}$. Let $\mathcal{C}_0 = \langle \mathbf{nil}, |0\rangle_q\langle 0| \otimes \rho\rangle$, $\mathcal{C}_1 = \langle \mathbf{nil}, |1\rangle_q\langle 1| \otimes \rho\rangle$, $\mathcal{C}_I = \langle \mathbf{nil}, I_q/2 \otimes \rho\rangle$, and $\mu = \frac{1}{2}\mathcal{C}_0 + \frac{1}{2}\mathcal{C}_1$. Then obviously $\mu \not\approx_s \overline{\mathcal{C}_I}$, as otherwise by the left-decompositivity of $\approx_s$ we must have both $\mathcal{C}_0 \approx_s \mathcal{C}_I$ and $\mathcal{C}_1 \approx_s \mathcal{C}_I$, which is impossible.

Actually, the argument in Example 10 applies to *any* bisimulation which is state-based: by Lemma 4, any bisimilation between distributions which is lifted from configurations is left-decomposable, hence discriminating $\mathcal{C}$ and $\mathcal{D}$. Therefore, to make these two obviously indistinguishable configurations bisimilar, we have to define bisimulation relation *directly* on distributions, rather than on configurations and then lift it to distributions.

For this purpose, we extend the distribution-based bisimulation introduced in [9] to our quantum setting. A distribution $\mu$ is said to be *transition consistent*, if for any $\mathcal{C} \in \lceil \mu \rceil$ and $\alpha \neq \tau$, $\mathcal{C} \overset{\hat{\alpha}}{\Longrightarrow} \nu_{\mathcal{C}}$ for some $\nu_{\mathcal{C}}$ implies $\mu \overset{\hat{\alpha}}{\Longrightarrow} \nu$ for some $\nu$, i.e., all configurations in its support have the same set of enabled visible actions (possibly after some invisible transitions). Furthermore, a decomposition $\mu = \sum_{i\in I} p_i \cdot \mu_i$, $p_i > 0$ for each $i \in I$, is a *tc-decomposition* of $\mu$ if for each $i \in I$, $\mu_i$ is transition consistent.

▶ **Definition 11.**

1. A symmetric relation $\mathcal{R} \subseteq D(Con) \times D(Con)$ is called a *(distribution-based) ground bisimulation* if for any $\mu, \nu \in D(Con)$, $\mu\mathcal{R}\nu$ implies that
   - **(i)** $qv(\mu) = qv(\nu)$, and $\mathrm{env}(\mu) = \mathrm{env}(\nu)$,
   - **(ii)** whenever $\mu \xrightarrow{\hat{\alpha}} \mu'$, there exists $\nu'$ such that $\nu \overset{\hat{\alpha}}{\Longrightarrow} \nu'$ and $\mu'\mathcal{R}\nu'$,
   - **(iii)** if $\mu$ is not transition consistent, and $\mu = \sum_{i\in I} p_i \cdot \mu_i$ is a tc-decomposition, then $\nu \overset{\hat{\tau}}{\Longrightarrow} \sum_{i\in I} p_i \cdot \nu_i$ such that for each $i$, $\mu_i\mathcal{R}\nu_i$.
2. A relation $\mathcal{R}$ is a *(distribution-based) bisimulation* if it is a ground bisimulation, and is closed under super-operator application.

In contrast with Definition 8.1, the above definition has an additional requirement Clause 1.(iii). This clause is crucial for distribution-based bisimulation, as the transition $\mu \xrightarrow{\hat{\alpha}} \mu'$ in Clause 1.(ii) is possible only when $\mu$ is transition consistent for $\alpha$. That is, all configurations in the support of $\mu$ can perform weak $\alpha$-transition. For those actions for which $\mu$ is not

[2] Note that $\mathcal{C}$ and $\mathcal{D}$ would be regarded as 'semantically identical' in [17], instead of '(distribution-based) bisimilar' as we do in this paper, since the semantics of $M[q;x]$ in this case is represented as $\mathcal{E}[q]$ *by definition.*

transition consistent, we must first split $\mu$ into transition consistent components, and then compare them with the corresponding components of $\nu$ individually.

The bisimilarity $\approx$ for quantum configurations and for quantum process terms are defined similarly as in the state-based case. The next theorem collects some useful properties of the distribution-based bisimilarity.

▶ **Theorem 12.**

1. *The bisimilarity relation $\approx$ is the largest bisimulation on $D(Con)$, and it is an equivalence relation.*
2. *$\approx$ is linear, but not left-decomposable.*

A direct consequence of Theorem 12 is a deciding algorithm for the bisimilarity between recursion-free quantum configurations, which is sufficient for most practical quantum cryptographic protocols. First, as pointed out in [12], any recursion-free quantum processes can be modified to be free of quantum input, so that the bisimilarity between them can be verified by only examining the ground bisimulation. Second, it has been proved in [14, Lemma 1] that every linear bisimulation $\mathcal{R}$ corresponds to a matrix $E$, so that two distributions $\mu$ and $\nu$ are related by $\mathcal{R}$ if and only if $(\mu - \nu)E = 0$, where distributions are seen as vectors. As our ground bisimulation for quantum processes is indeed linear, the algorithm presented in [14], with slight changes, can be used to decide it. For the sake of space limit, we omit the details here, and refer interested readers to [14].

To conclude this section, we would like to show that our distribution-based bisimulation is weaker than its state-based counterpart presented in Definition 8.

▶ **Theorem 13.** *Let $\mu, \nu \in D(Con)$. Then $\mu \approx_s \nu$ implies $\mu \approx \nu$, but $\mu \approx \nu$ does not necessarily imply $\mu \approx_s \nu$. In particular, we have in Example 10 that $\mu \approx \overline{\mathcal{C}_I}$ and $\mathcal{C} \approx \mathcal{D}$.*

## 5 Bisimulation metric

In the previous section, only *exact* bisimulation is presented where two quantum processes are either bisimilar or non-bisimilar. Obviously, such a bisimulation cannot capture the idea that a quantum process *approximately* implements its specification. To measure the behavioural distance between processes, the notion of approximate bisimulation and the bisimulation distance for qCCS processes were introduced in [27]. This section is devoted to extending this approximate bisimulation to distribution-based case. Note that approximate bisimulation has been investigated in probabilistic process algebra and probabilistic labelled transition systems in the context of security analysis [24, 1].

Recall that the trace distance of $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ is defined to be $d(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_{\mathrm{tr}}$ where $\|\cdot\|_{\mathrm{tr}}$ denotes the trace norm. We have the following definition.

▶ **Definition 14.** Given $\lambda \in [0, 1]$, a symmetric relation $\mathcal{R}$ over $D(Con)$ which is closed under super-operator application is a $\lambda$-bisimulation if for any $\mu\mathcal{R}\nu$, we have

1. $qv(\mu) = qv(\nu)$, and $d(\mathrm{env}(\mu), \mathrm{env}(\nu)) \leq \lambda$,
2. whenever $\mu \xrightarrow{\hat{\alpha}} \mu'$, there exists $\nu'$ such that $\nu \overset{\hat{\alpha}}{\Longrightarrow} \nu'$ and $\mu'\mathcal{R}\nu'$,
3. if $\mu$ is not transition consistent, and $\mu = \sum_{i\in I} p_i \cdot \mu_i$ is a tc-decomposition, then $\nu \overset{\hat{\tau}}{\Longrightarrow} \sum_{i\in I} p_i \cdot \nu_i$ such that $\sum_{i:\mu_i\mathcal{R}\nu_i} p_i \geq 1 - \lambda$.

By induction, we can show easily that $\mu \xrightarrow{\hat{\alpha}} \mu'$ can be replaced by $\mu \overset{\hat{\alpha}}{\Longrightarrow} \mu'$ in Clause (2).

The approximate bisimilarity $\overset{\lambda}{\approx}$ for quantum configurations and for quantum process terms are defined similarly as in the exact bisimulation case. Furthermore, we define the bisimulation distance between distributions as $d_b(\mu, \nu) = \inf\{\lambda \geq 0 \mid \mu \overset{\lambda}{\approx} \nu\}$ and the bisimulation distance between process terms as $d_b(t, u) = \inf\{\lambda \geq 0 \mid \forall \psi \text{ and } \rho \in \mathcal{D}(\mathcal{H}), \langle t\psi, \rho\rangle \overset{\lambda}{\approx} \langle u\psi, \rho\rangle\}$. Here we assume that $\inf \emptyset = 1$. The next theorem shows that $d_b$ is indeed a pseudo-metric with $\approx$ being its kernel.

▶ **Theorem 15.**

1. *The bisimulation distance $d_b$ is a pseudo-metric on $D(Con)$.*
2. *For any $\mu, \nu \in D(Con)$, $\mu \approx \nu$ if and only if $d_b(\mu, \nu) = 0$.*

## 6 An illustrative example

For the ease of notations, we extend the syntax of qCCS a little bit by allowing probabilistic choice in the syntax level[3]; that is, we assume $\sum_{i\in I} p_i t_i \in \mathcal{T}$ whenever $t_i \in \mathcal{T}$ and $p_i \geq 0$ for each $i \in I$ with $\sum_{i\in I} p_i = 1$. We further extend the transitional semantics in Fig. 1 by adding the following transition rule:

$$Dist \; \frac{}{\langle \sum_{i\in I} p_i t_i, \rho\rangle \xrightarrow{\tau} \sum_{i\in I} p_i \langle t_i, \rho\rangle}.$$

We also introduce the syntax sugar **if** $b$ **then** $t$ **else** $u$ to be the abbreviation of **if** $b$ **then** $t$ + **if** $\neg b$ **then** $u$.

BB84, the first quantum key distribution protocol developed by Bennett and Brassard in 1984 [4], provides a provably secure way to create a private key between two parties, say, Alice and Bob, with the help of a classical authenticated channel and a quantum insecure channel between them. Its security relies on the basic property of quantum mechanics that information gain about a quantum state is only possible at the expense of changing the state, if all the possible states are not orthogonal. The basic BB84 protocol with security parameter $n$ goes as follows:

**(1)** Alice randomly generates two strings $\tilde{B}_a$ and $\tilde{K}_a$ of bits, each with size $n$.

**(2)** Alice prepares a string of qubits $\tilde{q}$, with size $n$, such that the $i$th qubit of $\tilde{q}$ is $|x_y\rangle$ where $x$ and $y$ are the $i$th bits of $\tilde{B}_a$ and $\tilde{K}_a$, respectively, and $|0_0\rangle = |0\rangle$, $|0_1\rangle = |1\rangle$, $|1_0\rangle = |+\rangle$, and $|1_1\rangle = |-\rangle$. Here $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$.

**(3)** Alice sends the qubit string $\tilde{q}$ to Bob.

**(4)** Bob randomly generates a string of bits $\tilde{B}_b$ with size $n$.

**(5)** Bob measures each qubit received from Alice according to a basis determined by the bits he generated: if the $i$th bit of $\tilde{B}_b$ is $k$ then he measures with $\{|k_0\rangle, |k_1\rangle\}$, $k = 0, 1$. Let the measurement results be $\tilde{K}_b$, again a string of bits with size $n$.

**(6)** Bob sends his measurement bases $\tilde{B}_b$ back to Alice, and upon receiving the information, Alice sends her bases $\tilde{B}_a$ to Bob.

**(7)** Alice and Bob determine at which positions the bit strings $\tilde{B}_a$ and $\tilde{B}_b$ are equal. They discard the bits in $\tilde{K}_a$ and $\tilde{K}_b$ where the corresponding bits of $\tilde{B}_a$ and $\tilde{B}_b$ do not match.

After the execution of the basic BB84 protocol above, the remaining bits of $\tilde{K}_a$ and $\tilde{K}_b$, denoted by $\tilde{K}'_a$ and $\tilde{K}'_b$ respectively, should be the same, provided that the channels used are perfect, and no eavesdropper exists.

To detect a potential eavesdropper Eve, Alice and Bob proceed as follows:

[3] Note that this extension will not change the expressive power of qCCS and all the results obtained in this paper, as probabilistic choices can be simulated by quantum measurements preceded by appropriate quantum state preparation.

**(8)** Alice randomly chooses $\lceil|\tilde{K}'_a|/2\rceil$ bits of $\tilde{K}'_a$, denoted by $\tilde{K}''_a$, and sends to Bob $\tilde{K}''_a$ and its indexes in $\tilde{K}'_a$.

**(9)** Upon receiving the information from Alice, Bob sends back to Alice his substring $\tilde{K}''_b$ of $\tilde{K}'_b$ at the indexes received from Alice.

**(10)** Alice and Bob check if the strings $\tilde{K}''_a$ and $\tilde{K}''_b$ are equal. If yes, then the remaining substring $\tilde{K}^f_a$ (resp. $\tilde{K}^f_b$) of $\tilde{K}'_a$ (resp. $\tilde{K}'_b$) by deleting $\tilde{K}''_a$ (resp. $\tilde{K}''_b$) is the secure key shared by Alice (reps. Bob). Otherwise, an eavesdropper (or too much noise in the channels) is detected, and the protocol halts without generating any secure keys.

For simplicity, we omit the processes of information reconciliation and privacy amplification. Now we describe the basic BB84 protocol [Steps (1)–(7)] in qCCS as follows.

$$\begin{aligned}
\mathit{Alice}(n) &:= \sum_{\tilde{B}_a,\tilde{K}_a\in\{0,1\}^n} \frac{1}{2^{2n}} \mathit{Set}_{\tilde{K}_a}[\tilde{q}].H_{\tilde{B}_a}[\tilde{q}].\mathsf{A2B}!\tilde{q}.\,\mathit{Wait}_A(\tilde{B}_a,\tilde{K}_a)\\
\mathit{Wait}_A(\tilde{B}_a,\tilde{K}_a) &:= \mathit{b2a}?\tilde{B}_b.\mathit{a2b}!\tilde{B}_a.\mathit{key}_a!\mathit{cmp}(\tilde{K}_a,\tilde{B}_a,\tilde{B}_b).\mathbf{nil}\\
\mathit{Bob}(n) &:= \mathsf{A2B}?\tilde{q}.\sum_{\tilde{B}_b\in\{0,1\}^n} \frac{1}{2^n} M_{\tilde{B}_b}[\tilde{q};\tilde{K}_b].\mathit{Set}_{\tilde{0}}[\tilde{q}].\mathit{b2a}!\tilde{B}_b.\,\mathit{Wait}_B(\tilde{B}_b,\tilde{K}_b)\\
\mathit{Wait}_B(\tilde{B}_b,\tilde{K}_b) &:= \mathit{a2b}?\tilde{B}_a.\mathit{key}_b!\mathit{cmp}(\tilde{K}_b,\tilde{B}_a,\tilde{B}_b).\mathbf{nil}\\
\mathit{BB84}(n) &:= \mathit{Alice}(n)\|\mathit{Bob}(n)
\end{aligned}$$

where $\mathit{Set}_{\tilde{K}_a}[\tilde{q}]$ sets the $i$th qubit of $\tilde{q}$ to the state $|\tilde{K}_a(i)\rangle$, $H_{\tilde{B}_a}[\tilde{q}]$ applies $H$ or does nothing on the $i$th qubit of $\tilde{q}$ depending on whether the $i$th bit of $\tilde{B}_a$ is 1 or 0, and $M_{\tilde{B}_b}[\tilde{q};\tilde{K}_b]$ is the quantum measurement on $\tilde{q}$ according to the bases determined by $\tilde{B}_b$, i.e., for each $1\le i\le n$, it measures $q_i$ with respect to the basis $\{|0\rangle,|1\rangle\}$ (resp. $\{|+\rangle,|-\rangle\}$) if $\tilde{B}_b(i)=0$ (resp. 1), and stores the result into $\tilde{K}_b(i)$. The function *cmp* takes a triple of bit-strings $\tilde{x},\tilde{y},\tilde{z}$ with the same size as inputs, and returns the substring of $\tilde{x}$ where the corresponding bits of $\tilde{y}$ and $\tilde{z}$ match. When $\tilde{y}$ and $\tilde{z}$ match nowhere, we let $\mathit{cmp}(\tilde{x},\tilde{y},\tilde{z})=\epsilon$, the empty string. We add the operation $\mathit{Set}_{\tilde{0}}[\tilde{q}]$ in $\mathit{Bob}(n)$ for technical reasons: it makes the ideal specifications defined below simple.

To show the correctness of basic BB84 protocol, we first put $\mathit{BB84}(n)$ in a *test environment* defined as follows

$$\begin{aligned}
\mathit{Test} &:= \mathit{key}_a?k_a.\mathit{key}_b?k_b.\mathbf{if}\ k_a=k_b\ \mathbf{then}\ \mathit{key}!k_a.\mathbf{nil}\ \mathbf{else}\ \mathit{fail}!0.\mathbf{nil}\\
\mathit{BB84}_{\mathit{test}}(n) &:= (\mathit{BB84}(n)\|\mathit{Test})\backslash\{\mathit{a2b},\mathit{b2a},\mathsf{A2B},\mathit{key}_a,\mathit{key}_b\}
\end{aligned}$$

For the ideal *specification* of $\mathit{BB84}_{\mathit{test}}(n)$, we would like it to satisfy the following three conditions: (1) it is correct, in the sense that it will never perform $\mathit{fail}!0$; (2) the generated key $\tilde{x}$ with $|\tilde{x}|=i$ is uniformly distributed for each $i\le n$. That is, for any $\tilde{x}$ with $|\tilde{x}|=i$, $\Pr(\tilde{x}\text{ is the key obtained}\mid\text{key-length}=i)=1/2^i$; (3) The length of the obtained key follows the unbiased binomial distribution. That is, for each $i\le n$, $\Pr(\text{key-length}=i)=\binom{n}{i}/2^n$. Thus we can let

$$\mathit{BB84}_{\mathit{spec}}(n) := \sum_{i=0}^{n}\sum_{\tilde{x}\in\{0,1\}^i}\frac{\binom{n}{i}}{2^{n+i}}\mathit{Set}_{\tilde{0}}[\tilde{q}].\mathit{key}!\tilde{x}.\mathbf{nil}.$$

It is tedious but routine to check that $\mathit{BB84}_{\mathit{test}}(n)\approx\mathit{BB84}_{\mathit{spec}}(n)$ for any $n$.

Now we proceed to describe the protocol that detects potential eavesdroppers [Steps

(1)–(10)]. Let

$$\begin{aligned}
\mathit{Alice}'(n) &:= (\mathit{Alice}(n)\|\mathit{key}_a?\tilde{K}'_a.\sum_{\tilde{x}\subseteq\{1,\ldots,m\}}^{|\tilde{x}|=k}\frac{1}{\binom{m}{k}}\mathit{a2b}!\tilde{x}.\mathit{a2b}!\mathit{SubStr}(\tilde{K}'_a,\tilde{x}).\mathit{b2a}?\tilde{K}''_b.\\
&\qquad(\textbf{if } \mathit{SubStr}(\tilde{K}'_a,\tilde{x})=\tilde{K}''_b \textbf{ then } \mathit{key}'_a!\mathit{RemStr}(\tilde{K}'_a,\tilde{x}).\textbf{nil}))\backslash\{\mathit{key}_a\}\\
\mathit{Bob}'(n) &:= (\mathit{Bob}(n)\|\mathit{key}_b?\tilde{K}'_b.\mathit{a2b}?\tilde{x}.\mathit{a2b}?\tilde{K}''_a.\mathit{b2a}!\mathit{SubStr}(\tilde{K}'_b,\tilde{x}).\\
&\qquad(\textbf{if } \mathit{SubStr}(\tilde{K}'_b,\tilde{x})=\tilde{K}''_a \textbf{ then } \mathit{key}'_b!\mathit{RemStr}(\tilde{K}'_b,\tilde{x}).\textbf{nil}))\backslash\{\mathit{key}_b\}\\
\mathit{BB84}'(n) &:= \mathit{Alice}'(n)\|\mathit{Bob}'(n)
\end{aligned}$$

where $m = |\tilde{K}'_a|$ and $k = \lceil m/2\rceil$, the function $\mathit{SubStr}(\tilde{K}'_a,\tilde{x})$ returns the substring of $\tilde{K}'_a$ at the indexes specified by $\tilde{x}$, and $\mathit{RemStr}(\tilde{K}'_a,\tilde{x})$ returns the remaining substring of $\tilde{K}'_a$ by deleting $\mathit{SubStr}(\tilde{K}'_a,\tilde{x})$.

To get a taste of the security of BB84 protocol, we consider a special case where Eve's strategy is to simply measure the qubits sent by Alice, according to randomly guessed bases, to get the keys and resend these qubits to Bob. That is, we define

$$\mathit{Eve}(n) := \mathsf{A2E}?\tilde{q}.\sum_{\tilde{B}_e\in\{0,1\}^n}\frac{1}{2^n}M_{\tilde{B}_e}[\tilde{q};\tilde{K}_e].\mathit{key}'_e!\tilde{K}_e.\mathsf{E2B}!\tilde{q}.\textbf{nil}$$

Again, we put $\mathit{BB84}'(n)$ in a test environment, but now the environment includes the presence of Eve:

$$\begin{aligned}
\mathit{Test}' &:= \mathit{key}'_a?\tilde{x}.\mathit{key}'_b?\tilde{y}.\mathit{key}'_e?\tilde{z}.(\textbf{if } \tilde{x}\neq\tilde{y} \textbf{ then } \mathit{fail}!0.\textbf{nil}\\
&\qquad\qquad\qquad\qquad\qquad \textbf{else } (\textbf{if } \tilde{x}=\tilde{z} \textbf{ then } \mathit{hacked}!0.\textbf{nil}))\\
\mathit{BB84}'_{test}(n) &:= (\mathit{Alice}'(n)[f_a]\|\mathit{Bob}'(n)[f_b]\|\mathit{Eve}(n)\|\mathit{Test}')\backslash L
\end{aligned}$$

where $L = \{\mathit{a2b}, \mathit{b2a}, \mathsf{A2E}, \mathsf{E2B}, \mathit{key}'_a, \mathit{key}'_b, \mathit{key}'_e\}$, $f_a(\mathsf{A2B}) = \mathsf{A2E}$, and $f_b(\mathsf{A2B}) = \mathsf{E2B}$.

Now, to show the *security* of BB84,[4] it suffices to prove the following property:

$$\mathit{BB84}'_{test}(n) \overset{c^n}{\approx} \mathit{Set}_{\tilde{0}}[\tilde{q}].\textbf{nil} \tag{1}$$

where $c = 1/2 + \sqrt{3}/4 < 1$. Thus $d_b(\mathit{BB84}'_{test}(n), \mathit{Set}_{\tilde{0}}[\tilde{q}].\textbf{nil}) \leq c^n$. That is, the testing system is just like a protocol which only sets the quantum qubits $\tilde{q}$ to $|\tilde{0}\rangle\langle\tilde{0}|$. As the process $\mathit{Set}_{\tilde{0}}[\tilde{q}].\textbf{nil}$ never performs *fail*!0 or *hacked*!0, this indicates that the *insecurity degree* of BB84 is at most $c^n$, which decreases exponentially to 0 when $n$ tends to infinity.

To show Eq.(1), take arbitrarily $\rho \in \mathcal{D}(\mathcal{H})$, and let $\mathcal{C} = \langle \mathit{BB84}'_{test}(n), \rho\rangle$ and $\mathcal{D} = \langle \mathit{Set}_{\tilde{0}}[\tilde{q}].\textbf{nil}, \rho\rangle$. Basically, we only need to compute the total probability of $\mathcal{C}$ eventually performing *fail*!0 or *hacked*!0. The reason is, they are the only visible actions of $\mathcal{C}$ ($\mathcal{D}$ does not perform any visible action at all), and also the only actions which contribute to possible transition inconsistency of distributions obtained from $\mathcal{C}$. If the total probability of their appearance is upper bounded by $c^n$, then $\mathcal{C}$ and $\mathcal{D}$ are $c^n$-bisimilar.

For each qubit sent by Alice, Eve chooses the wrong basis with probability 1/2, and in this case if Bob measures this qubit according to the correct basis he will get an incorrect result with probability 1/2. Thus for each qubit that Bob guesses the correct basis, the

[4] Here we adopt a weak notion of security: by secure we mean the eavesdropper ends up with a false key string. A stronger and more practical notion of security should take into account the mutual information between the keys held by the legitimate parties and the eavesdropper. We leave the analysis of BB84 with respect to this notion of security for future work.

probability that Alice and Bob get different key bits is 1/4. Furthermore, for each $i$-length raw key generated by the basic BB84, Alice and Bob will compare $i/2$ key bits during the eavesdropper-detection phase. The probability that they fail to detect the eavesdropper is then $(3/4)^{i/2}$. Note that only when the eavesdropper is not detected, the protocol proceeds. Hence the probability of observing *fail*!0 or *hacked*!0 is upper bounded by

$$\sum_{i=0}^{n} \sum_{\tilde{x}\in\{0,1\}^i} \frac{\binom{n}{i}}{2^{n+i}}(3/4)^{i/2} = \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}(3/4)^{i/2} = c^n.$$

## 7 Conclusion and Future work

In this paper, we have proposed a novel notion of distribution-based bisimulation for quantum processes in qCCS. In contrast with previous bisimulations introduced in the literature, our definition is reasonably weaker in that it equates some intuitively bisimilar processes which are not bisimilar according to the previous definitions, thus is more useful in applications. We further defined a bisimulation distance to characterise the extent to which two processes are bisimilar. As an application, we applied the notions of distribution-based bisimulation and bisimulation distance to show that the quantum key distribution protocol BB84 is sound and secure against the intercept-resend attacker. To the best of our knowledge, this is the first time in the literature that the (asymptotic) security of BB84 has been analysed in the framework of a quantum process algebra.

There are still many questions remaining for further study. Firstly, as pointed out in Section 6, the notion of security we adopted for the analysis of BB84 is a rather weak one. In quantum information field, people normally use the mutual information between the states held by legitimate parties and the eavesdropper to quantify the leakage of secure information. To perform a security analysis of BB84 in terms of this stronger notion of security and against more complex model of attack beyond the intercept-resend one studied in the current paper is one of the future directions we are pursuing.

Secondly, bisimilarity checking is usually a very tedious and routine task which can barely be done by hand. This issue becomes more serious when the number of parties involved and the round of communications increase. To deal with this problem, making the process algebra approach more applicable for the analysis of general quantum cryptographic protocols, we are going to develop a software tool for automated bisimilarity checking. In the theoretical aspect, we will explore the possibility of extending symbolic bisimulation proposed in [12] to distribution-based case, to decrease the computational complexity of determining bisimilarity.

Finally, as shown in [9], distribution-based bisimulation is not a congruence in general, unless restricted to distributed schedulers. However, as argued by the authors of [9], non-distributed schedulers, which are responsible for the incongruence, are actually very unrealistic and do not appear in real-world applications. To show that our distribution-based bisimulation is a congruence for qCCS processes under distributed schedulers and to study the implication of distributed schedulers for quantum cryptographic protocols are also topics worthy of further consideration.

**Acknowledgement.** This work was partially supported by Australian Research Council (Grant No. DP130102764). Y. F. is also supported by the National Natural Science Foundation of China (Grant Nos. 61428208 and 61472412) and the CAS/SAFEA International Partnership Program for Creative Research Team.

## References

1 A. Aldini and A. Di Pierro. Estimating the maximum information leakage. *International Journal of Information Security*, 7(3):219–242, 2008.

2 Ebrahim Ardeshir-Larijani, Simon J Gay, and Rajagopal Nagarajan. Equivalence checking of quantum protocols. In *TACAS'13*, pages 478–492. Springer, 2013.

3 Ebrahim Ardeshir-Larijani, Simon J Gay, and Rajagopal Nagarajan. Verification of concurrent quantum protocols by equivalence checking. In *TACAS'14*, pages 500–514. Springer, 2014.

4 C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computer, Systems and Signal Processing*, pages 175–179, 1984.

5 T. A. S. Davidson. *Formal Verification Techniques using Quantum Process Calculus.* PhD thesis, University of Warwick, 2011.

6 Y. Deng and Y. Feng. Open bisimulation for quantum processes. In *TCS'12: Proceedings of the 7th IFIP TC 1/WG 202 international conference on Theoretical Computer Science.* Springer-Verlag, September 2012. Full Version available at http://arxiv.org/abs/1201.0416.

7 Yuxin Deng, Rob van Glabbeek, Matthew Hennessy, and Carroll Morgan. Testing finitary probabilistic processes (extended abstract). In *CONCUR'09*, pages 274–288. Springer, 2009.

8 Laurent Doyen, Thomas A Henzinger, and Jean-Francois Raskin. Equivalence of labeled Markov chains. *International Journal of Foundations of Computer Science*, 19(03):549–563, 2008.

9 Christian Eisentraut, Jens Chr Godskesen, Holger Hermanns, Lei Song, and Lijun Zhang. Late Weak Bisimulation for Markov Automata. *http://arxiv.org/abs/1202.4116*, February 2012.

10 Y. Feng, R. Duan, Z. Ji, and M. Ying. Probabilistic bisimulations for quantum processes. *Information and Computation*, 205(11):1608–1639, November 2007.

11 Y. Feng, R. Duan, and M. Ying. Bisimulations for quantum processes. In Mooly Sagiv, editor, *POPL'11*, pages 523–534, 2011.

12 Yuan Feng, Yuxin Deng, and Mingsheng Ying. Symbolic bisimulation for quantum processes. *ACM Transactions on Computational Logic*, 15(2):14:1–14:32, May 2014.

13 S. J. Gay and R. Nagarajan. Communicating quantum processes. In J. Palsberg and M. Abadi, editors, *POPL'05*, pages 145–157, 2005.

14 Holger Hermanns, Jan Krcál, and Jan Kretínský. Probabilistic bisimulation: Naturally on distributions. In Paolo Baldan and Daniele Gorla, editors, *CONCUR'14*. Springer, 2014.

15 B. Jonsson, W. Yi, and K. G. Larsen. Probabilistic extensions of process algebras. In *Handbook of process algebra*, pages 685–710. North-Holland, Amsterdam, 2001.

16 P. Jorrand and M. Lalire. Toward a quantum process algebra. In P. Selinger, editor, *QPL'04*, page 111, 2004.

17 Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano, and Hideki Sakurada. Application of a process calculus to security proofs of quantum protocols. In *FCS'12*, pages 141–147, 2012.

18 M Kwiatkowska, G Norman, and D Parker. PRISM 2.0: a tool for probabilistic model checking. In *QEST'04*, pages 322–323, September 2004.

19 Marie Lalire. Relations among quantum processes: Bisimilarity and congruence. *Mathematical Structures in Computer Science*, 16(3):407–428, 2006.

20 Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406, 2001.

21 J Mitchell, A Ramanathan, A Scedrov, and V Teague. A Probabilistic Polynomial-time Calculus For Analysis of Cryptographic Protocols: (Preliminary Report). *Electronic Notes in Theoretical Computer Science*, 45:280–310, December 2000.

22 Rajagopal Nagarajan, Nikolaos Papanikolaou, Garry Bowen, and Simon Gay. An automated analysis of the security of quantum key distribution. In *SecCo'05*, 2005.

23 M. Nielsen and I. Chuang. *Quantum computation and quantum information.* Cambridge university press, 2000.

24 A. Di Pierro, C. Hankin, and H. Wiklicky. Measuring the confinement of probabilistic systems. *Theoretical Computer Science*, 340(1):3–56, 2005.

25 Ajith Ramanathan, John Mitchell, Andre Scedrov, and Vanessa Teague. Probabilistic bisimulation and equivalence for security analysis of network protocols. In *FOSSACS'04*, pages 468–483. Springer, Berlin, 2004.

26 Peter W Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.

27 M. Ying, Y. Feng, R. Duan, and Z. Ji. An algebra of quantum processes. *ACM Transactions on Computational Logic*, 10(3):1–36, April 2009.