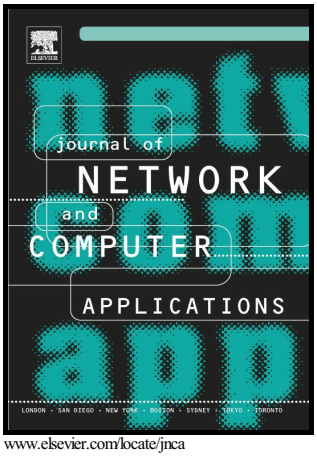
Author's Accepted Manuscript



www.elsevier.com/locate/jnca

Quantum Technique for Access Control in Cloud Computing II: Encryption and Key Distribution

Lu Zhou, Quanlong Wang, Xin Sun, Piotr Kulicki, Arcangelo Castiglione

PII: S1084-8045(17)30392-2
DOI: https://doi.org/10.1016/j.jnca.2017.11.012
Reference: YJNCA2015

To appear in: *Journal of Network and Computer Applications*

Received date: 19 May 2017
Revised date: 3 November 2017
Accepted date: 28 November 2017

Cite this article as: Lu Zhou, Quanlong Wang, Xin Sun, Piotr Kulicki and Arcangelo Castiglione, Quantum Technique for Access Control in Cloud Computing II: Encryption and Key Distribution, *Journal of Network and Computer Applications,* https://doi.org/10.1016/j.jnca.2017.11.012

Quantum Technique for Access Control in Cloud Computing II: Encryption and Key Distribution

Lu Zhou[a], Quanlong Wang[b], Xin Sun[c], Piotr Kulicki[d], Arcangelo Castiglione[e]

[a] *University of Aizu, Japan*
[b] *University of Oxford, UK*
[c] *Sun Yat-sen University, China*
[d] *The John Paul II Catholic University of Lublin, Poland*
[e] *University of Salerno, Italy*

Abstract

This is the second paper of the series of papers dealing with access control problems in cloud computing by adopting quantum techniques. In this paper we study the application of quantum encryption and quantum key distribution in the access control problem. We formalize our encryption scheme and protocol for key distribution in the setting of categorical quantum mechanics (CQM). The graphical language of CQM is used in this paper. The quantum scheme/protocol we propose possesses several advantages over existing schemes/protocols proposed in the state of the art for the same purpose. They are informationally secure and implementable by the current technology.

Keywords: quantum encryption, quantum key distribution, categorical quantum mechanics, access control

1. Introduction

This is the second paper of the series of papers dealing with access control problems in cloud computing by adopting quantum technique [30]. A simple model for the access control problem in cloud computing is shown in Fig. 1. Such a model has three components: *data owner*, *cloud* and *data user*. The

[☆] The names of the authors are ordered anti-alphabetically. Xin Sun is also affiliated with the John Paul II Catholic University of Lublin.

Email address: xin.sun.logic@gmail.com (Xin Sun)

data owner places on the cloud the encrypted data (bit or qubits) which the user wants to access. Upon receiving a data access request from the user, the data owner employs an access control policy to decide whether the user should be granted the access. Afterwards, if the access control policy says that the access should be granted to the user, then the data owner sends the corresponding key and a certificate to the user. Finally, the user sends the certificate to the cloud and gets the encrypted data, upon the successful verification of the certificate by the cloud.

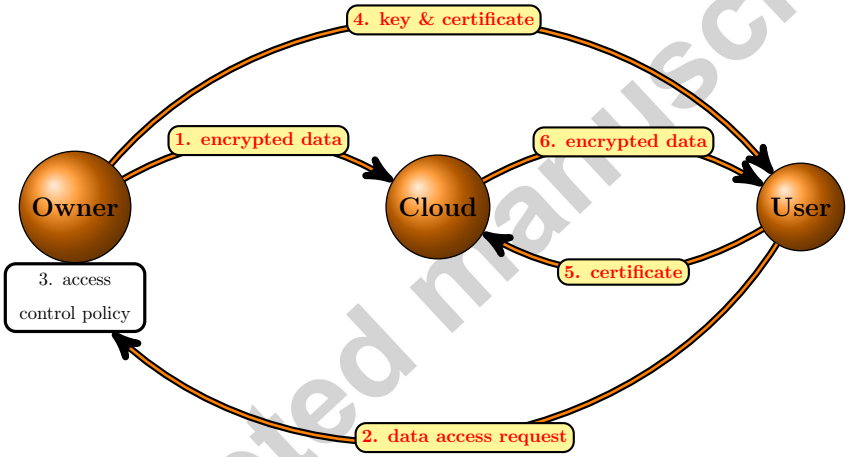


Figure 1: Data access in cloud computing.

In the first paper of this series [30], we developed quantum imperative logic as a formal language for the specification of access control policies, which helps the owner in deciding **whether** to grant access to the user or not. But **how** to grant certain access to a user? Cryptography offers a convenient tool for solving this problem. Many cryptographic solutions to the access-granting problem have been proposed [2, 6, 7, 8, 23, 24]. The basic idea is: first encrypt all resource, then assign keys for decryption to those users who are permitted

to access. More precisely, suppose we have resources $\{data_1, \ldots, data_n\}$. We first use $key_1, \ldots, key_n$ to encrypt those data. So we have $Enc_{key_1}(data_1), \ldots, Enc_{key_n}(data_n)$. Then we assign key_i to a user iff the user is permitted to access $data_i$. Therefore, encryption and key distribution plays a pivotal role in granting access. In this paper, we develop quantum techniques for encryption and key distribution, using the framework of categorical quantum mechanics (CQM).

The structure of the rest of this paper is as follows: we provide some background knowledge on categorical quantum mechanics in Section 2. Then we introduce encryption by complementary observables in Section 3. We present our quantum protocol for key distribution in Section 4 . We discuss related works in Section 5 and conclude this paper in Section 6.

2. Categorical quantum mechanics

Categorical quantum mechanics [1, 16, 17, 11, 4, 13, 14] concerns the study of quantum computation and quantum foundations using category theory, as well as the graphical language closely related to category theory. Composition of quantum systems in CQM is treated as a primitive connective, which is conveniently described by dagger symmetric monoidal category (†-SMC).

2.1. Category theory

Definition 1 (category). *A category $\mathcal{C}$ consists of:*

1. *a collection $ob(\mathcal{C})$ of objects,*
2. *for every pair of objects A, B, a set $\mathcal{C}(A, B)$ of morphisms,*
3. *for every object A, a special identity morphism: $1_A \in \mathcal{C}(A, A)$,*
4. *sequential composition operation for morphisms:*

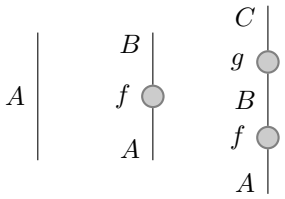
$$\circ : \mathcal{C}(B, C) \times \mathcal{C}(A, B) \to \mathcal{C}(A, C),$$

satisfying the following conditions:

(1) $\circ$ is associative on morphisms: $(h \circ g) \circ f = h \circ (g \circ f)$,

(2) $\circ$ *is unital on morphisms:* $1_B \circ f = f = f \circ 1_A$*, for all* $f \in \mathcal{C}(A, B)$*.*

We can graphically represent objects as wires and morphisms as nodes attached with an input wire and an output wire. Those graphs are read from bottom to top. In this graphical language the conditions of sequential composition, associativity and unitality become trivial.



Example 1. *In* ***FinHilb****, which is the category of finite dimensional Hilbert spaces, objects are finite dimensional Hilbert spaces over complex numbers, morphisms are linear maps. Identities are the identity function on every Hilbert space. Sequential composition is the composition of linear maps.*

Definition 2 (functor). *Let* $\mathcal{C}$ *and* $\mathcal{D}$ *be categories. A functor* $F : \mathcal{C} \to \mathcal{D}$ *is defined by*

- *for each object* $A \in ob(\mathcal{C})$ *an object* $F(A) \in ob(\mathcal{D})$*.*
- *for every morphism* $f \in \mathcal{C}(A, B)$ *a morphism* $F(f) \in \mathcal{D}(F(A), F(B))$ *such that*

$$F(f \circ g) = F(f) \circ F(g) \text{ and } F(1_A) = 1_{F(A)}.$$

Definition 3 (natural isomorphism). *Let* $F, G : \mathcal{C} \to \mathcal{D}$ *be functors. A natural transformation* $\tau : F \to G$ *is a family of morphisms in* $\mathcal{D}$*,* $\tau_A \in \mathcal{D}(F(A), G(A))$*, indexed by the objects of* $\mathcal{C}$*, such that the following square commutes:*

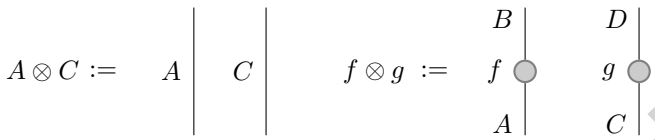
$$\begin{array}{ccc} F(A) & \xrightarrow{\tau_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow{\tau_B} & G(B) \end{array}$$

for all morphisms $f \in \mathcal{C}(A, B)$. A natural isomorphism is a natural transformation where each of the τ_A is an isomorphism. That is, there exists a morphism τ_A^{-1} such that $\tau_A^{-1} \circ \tau_A$ and $\tau_A \circ \tau_A^{-1}$ are identities.

Definition 4 (monoidal category [11]). *A monoidal category consists of the following data:*

- *a category $\mathcal{C}$,*
- *a unit object $I \in ob(\mathcal{C})$,*
- *a bifunctor $- \otimes - : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ such that*
  1. *$\otimes$ is a parallel composition operation for objects:*
  $$\otimes : ob(\mathcal{C}) \times ob(\mathcal{C}) \to ob(\mathcal{C}),$$
  2. *$\otimes$ is a parallel composition operation for morphisms:*
  $$\otimes : \mathcal{C}(A, B) \times \mathcal{C}(C, D) \to \mathcal{C}(A \otimes C, B \otimes D),$$
  3. *$\otimes$ and $\circ$ satisfy the interchange law:*
  $$(g_1 \otimes g_2) \circ (f_1 \otimes f_2) = (g_1 \circ f_1) \otimes (g_2 \circ f_2).$$
  4. $1_A \otimes 1_B = 1_{A \otimes B}$
- *two natural unit isomorphisms*
  $$\lambda_A : A \simeq I \otimes A \text{ and } \rho_A : A \simeq A \otimes I,$$
  and a natural associativity isomorphism
  $$\alpha_{A,B,C} : A \otimes (B \otimes C) \simeq (A \otimes B) \otimes C \ ,$$
  which are subject to the pentagon and triangle coherence equations, which can be found in Coecke and Paquette [15, p.209].

The bifunctor $\otimes$ is also called tensor product, which serves as parallel composition. It is graphically represented as horizontally putting two morphisms (objects) together. The unit object is represented as an empty graph. It can be easily verified that all the conditions of monoidal category trivially hold in the graphical representation.



Example 2. ***FinHilb*** *is a monoidal category. In* ***FinHilb****, parallel composition is the tensor product of Hilbert spaces. I is the field of complex numbers* $\mathbb{C}$*, which is a 1-dimensional Hilbert space. The left- and right-unit natural isomorphisms are respectively*

$$\lambda_A : A \to \mathbb{C} \otimes A :: a \mapsto 1 \otimes a \text{ and } \rho_A := A \to A \otimes \mathbb{C} :: a \mapsto a \otimes 1.$$

The associativity natural isomorphism is

$$\alpha_{A,B,C} := A \otimes (B \otimes C) \to (A \otimes B) \otimes C :: a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c.$$

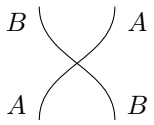
Definition 5 (symmetric monoidal category [20]). *A monoidal category is symmetric if it is equipped with a natural isomorphism called swap:*

$$\sigma_{A,B} : A \otimes B \to B \otimes A$$

defined for all objects A, B*, satisfying:*

- $\sigma_{B,A} \circ \sigma_{A,B} = 1_{A \otimes B}$,
- $\lambda_A^{-1} \circ \sigma_{A,I} = \rho_A^{-1}$,
- $(\sigma_{C,A} \otimes 1_B) \circ \alpha_{C,A,B} \circ \sigma_{A \otimes B,C} = \alpha_{A,C,B} \circ (1_A \otimes \sigma_{B,C}) \circ \alpha_{A,B,C}^{-1}$.

The swap morphism is graphically represented as the following:

$\sigma_{A,B} :=$ 

Definition 6 (dagger functor † [14, 28]). *A dagger functor for a symmetric monoidal category is an operation † that satisfies the following:*

- *is unaltering on objects and identity morphisms:* $A^\dagger = A, 1_A^\dagger = 1_A$,
- *reserves morphisms:* $(f : A \to B)^\dagger := f^\dagger : B \to A$,
- *is involutive:* $(f^\dagger)^\dagger = f$,
- *and respects the symmetric monoidal category structure:*

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger \qquad (f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$$
$$\sigma_{A,B}^\dagger = \sigma_{B,A} \qquad \alpha_{A,B,C}^\dagger = \alpha_{A,B,C}^{-1} \qquad \lambda_A^\dagger = \lambda_A^{-1}.$$

In the graphical language, if we apply the dagger functor to a graph, then the graph reflects vertically.

Definition 7 (dagger symmetric monoidal category [14]). *A dagger symmetric monoidal category (†-SMC) is a symmetric monoidal category equipped with a dagger functor.*

Example 3. ***FinHilb*** *is a †-SMC. In* ***FinHilb****, the swap for every Hilbert space* A, B *is the natural isomorphism*

$$\sigma_{A,B} := A \otimes B \to B \otimes A :: a \otimes b \mapsto b \otimes a.$$

† *is the adjoin (transpose conjugate) operator.*

Definition 8 (self-dual dagger compact category [14]). *A self-dual dagger compact category is a †-SMC in which for each object* A *there is a morphism* $\eta_A : I \to (A \otimes A)$*:*

1. $(\eta_A^\dagger \otimes 1_A) \circ (1_A \otimes \eta_A) = 1_A$

2. $\sigma_{A,A} \circ \eta_A = \eta_A$

Graphically, the compact structure η_A and its adjoin $\eta_A^\dagger$ are respectively represented by a cup and a cap:

$\eta_A :=$  $\eta_A^\dagger :=$ 

The compactness graphically means that the following is satisfied:

In every monoidal category $\mathcal{C}$, a morphism $s \in \mathcal{C}(I, I)$ is called a scalar, which is understood as a number. Graphically, we represent scalars as diamonds:

Example 4. *In* ***FinHilb****, scalars form the field of complex numbers* $\mathbb{C}$*.*

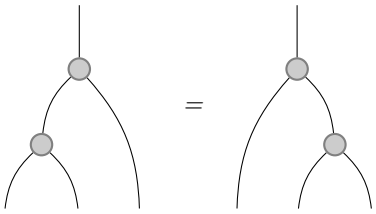
2.2. Frobenius algebra and observable

Definition 9 (Frobenius algebra [12]). *Let* $\mathcal{C}$ *be a monoidal category. A Frobenius algebra on* $\mathcal{C}$ *is an object* A *together with (****m****ultiply,* ***u****nit,* ***c****opy, and* ***d****elete) morphisms*

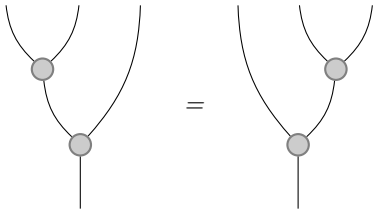
$$m : A \otimes A \to A \qquad u : I \to A \qquad c : A \to A \otimes A \qquad d : A \to I.$$

satisfying the following equations:

- *associativity:* $m \circ (m \otimes 1_A) = m \circ (1_A \otimes m)$*. Graphically, associativity is visualized as the following:*

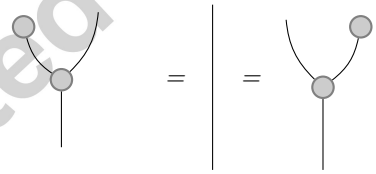


- *coassociativity:* $(c \otimes 1_A) \circ c = (1_A \otimes c) \circ c$. *Graphically,*

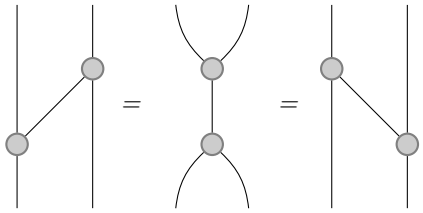


- *unitality:* $m \circ (u \otimes 1_A) = 1_A = m \circ (1_A \otimes u)$. *Graphically,*

- *counitality:* $(d \otimes 1_A) \circ c = 1_A = (1_A \otimes d) \circ c$. *Graphically,*

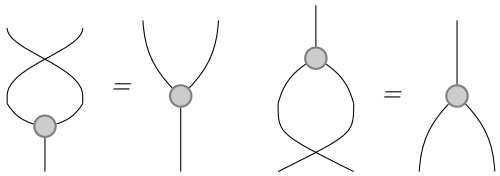


- *Frobenius condition:* $(1_A \otimes m) \circ (c \otimes 1_A) = c \circ m = (m \otimes 1_A) \circ (1_A \otimes c)$. *Graphically,*



Definition 10 (commutative Frobenius algebra [12]). *A Frobenius algebra is commutative when the following equations hold:*

$$\sigma_{A,A} \circ c = c \qquad m \circ \sigma_{A,A} = m.$$



Definition 11 (dagger commutative Frobenius algebra [12]). *A dagger commutative Frobenius algebra on a dagger symmetric monoidal category is a commutative Frobenius algebra that additionally satisfies the following equations:* $c = m^\dagger$, $d = u^\dagger$.

To describe a dagger commutative Frobenius algebra, we only need to describe the multiply and the unit, and define copy and delete by the dagger functor.

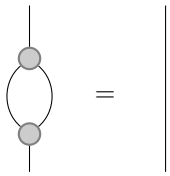
Example 5. *Consider the* †*-SMC* ***FinHilb****,* $\mathbb{C}^n$ *is an object of* ***FinHilb****. Consider the orthonormal basis* $\{|0\rangle, \ldots, |n-1\rangle\}$*. Note that to specify a linear map between Hilbert spaces, we only need to specify the functionality of the map on an orthonormal basis. Now we let*

1. $M_{\mathbb{C}^n} : \mathbb{C}^n \otimes \mathbb{C}^n \to \mathbb{C}^n :: |i\rangle \otimes |j\rangle \mapsto \begin{cases} |i\rangle & i{=}j \\ 0 & i \neq j \end{cases}$
2. $U_{\mathbb{C}^n} : \mathbb{C} \to \mathbb{C}^n :: 1 \mapsto \sum_{i=0}^{n-1} |i\rangle$
3. $C_{\mathbb{C}^n} : \mathbb{C}^n \to \mathbb{C}^n \otimes \mathbb{C}^n :: |i\rangle \mapsto |i\rangle \otimes |i\rangle$
4. $D_{\mathbb{C}^n} : \mathbb{C}^n \to \mathbb{C} :: |i\rangle \mapsto 1$

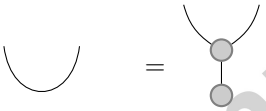
Then $FroA_{\mathbb{C}^n} = (\mathbb{C}^n, M_{\mathbb{C}^n}, U_{\mathbb{C}^n}, C_{\mathbb{C}^n}, D_{\mathbb{C}^n})$ *is a dagger commutative Frobenius algebra.*

3. Encryption by complementary observables

Definition 12 (observable structure [11]). *An observable structure in a †-SMC is a dagger commutative Frobenius algebra (A, m, u) such that $m \circ m^\dagger = 1_A$. Graphically,*



An observable structure (A, m, u) induce a self-dual when setting $\eta_A = m^\dagger \circ u$.

$\eta_A :=$ 

Example 6. *Consider the object $\mathbb{C}^2$ in **FinHilb**, let*

1. $m_z^\dagger : \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2 :: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$
2. $u_z : \mathbb{C} \to \mathbb{C}^2 :: 1 \mapsto |0\rangle + |1\rangle$

Then $O_z = (\mathbb{C}^2, m_z, u_z)$ is an observable structure.

Example 7. *For $\mathbb{C}^2$ in **FinHilb**, let*

1. $m_x^\dagger : \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2 :: \begin{cases} |+\rangle \mapsto |++\rangle \\ |-\rangle \mapsto |--\rangle \end{cases}$
2. $u_x : \mathbb{C} \to \mathbb{C}^2 :: 1 \mapsto |+\rangle + |-\rangle$

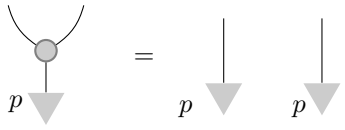
Then $O_x = (\mathbb{C}^2, m_x, u_x)$ is an observable structure.

Example 8. *For $\mathbb{C}^2$ in **FinHilb**, let $|\boldsymbol{i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|\bar{\boldsymbol{i}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$*

1. $m_y^\dagger : \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2 :: \begin{cases} |\boldsymbol{i}\rangle \mapsto |\boldsymbol{ii}\rangle \\ |\bar{\boldsymbol{i}}\rangle \mapsto |\overline{\boldsymbol{ii}}\rangle \end{cases}$
2. $u_y : \mathbb{C} \to \mathbb{C}^2 :: 1 \mapsto |\boldsymbol{i}\rangle + |\bar{\boldsymbol{i}}\rangle$

Then $O_y = (\mathbb{C}^2, m_y, u_y)$ is an observable structure.

Definition 13 (copyable point [11]). *Let $\mathcal{C}$ be a †-SMC and (A, m, u) be a Frobenius algebra on $\mathcal{C}$. A copyable point of a (A, m, u) is a point $p : I \to A$ such that $c \circ p = p \otimes p$.*



Definition 14 (conjugate [11]). *Let $f : A \to B$ be a morphism. Its conjugate $f_* : A \to B$ is defined as*

$$f_* := (1_B \otimes \eta_B^\dagger) \circ (1_A \otimes f \otimes B) \circ (\eta_A \otimes 1_B).$$

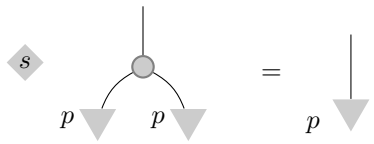
A morphism f is self-conjugate if $f = f_*$. Graphically, the conjugate of f is the horizontal reflection of f. Therefore, a self conjugate morphism is invariant under horizontal reflection.

Example 9. *Numbers/scalars are morphisms from I to I. In **FinHilb**, a number is self-conjugate iff it is a real number.*

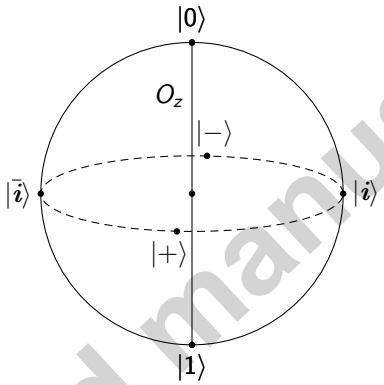
Definition 15 (classical points [11]). *Given an observable structure (A, m, u), a point $p : I \to A$ is classical in this structure if it is self-conjugate, copyable and $u^\dagger \circ p = 1$.*

Example 10. *For the observable structure O_z, $|0\rangle$ and $|1\rangle$ are classical points. For O_x, $|+\rangle$ and $|-\rangle$ are classical points. More generally, every diameter in Bloch sphere is an observable structure and the two endpoints of the diameter are the classical points of the corresponding observable structure.*

Definition 16 (unbiased points [11]). *Given an observable structure (A, m, u), a point $p : I \to A$ is unbiased for this structure if there is a scaler $s : I \to I$ such that $s \otimes (m \circ (p \otimes p)) = p$, i.e.*



Example 11. *For the observable structure O_z, $|+\rangle, |-\rangle, |\boldsymbol{i}\rangle$ and $|\bar{\boldsymbol{i}}\rangle$ are unbiased points. More generally, every point that lies on the equator of the Bloch sphere is an unbiased point for O_z. The collection of all unbiased points of an observable structure forms a circle that passes the center of the ball and is perpendicular to the diameter corresponding to the observable structure.*



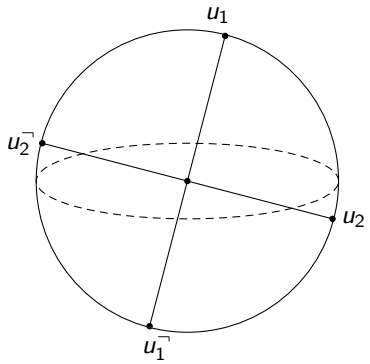
3.1. Complementary observable

Definition 17 (complementary observable [11]). *Two observables (A, m_1, u_1) and (A, m_2, u_2) in a †-SMC is complementary if the following are satisfied:*

- *COMP1 : whenever $k : I \to A$ is classical for (m_1, u_1), it is unbiased for (m_2, u_2).*
- *COMP2: whenever $k : I \to A$ is classical for (m_2, u_2), it is unbiased for (m_1, u_1).*

Every observable of qubits $(\mathbb{C}^2, m, u)$ has two classical points. We denote them by u and $u^\neg$ respectively.

Example 12. *In **FinHilb**, for the object $\mathbb{C}^2$, O_x, O_y and O_z are pairwise complementary. More generally, every two perpendicular diameters in the Bloch sphere represent two complementary observables.*



3.2. Encryption by phase shift over complementary observables

Coecke *et al* [11] showed that a phase shift of an observable of qubits $(\mathbb{C}^2, m, u)$ is isomorphic to a matrix $|u\rangle\langle u| + e^{i\alpha}|u^\neg\rangle\langle u^\neg|$, in which $\alpha \in [0, 2\pi)$. We use $S(\alpha)$ to represent the phase shift which is isomorphic to $|u\rangle\langle u|+e^{i\alpha}|u^\neg\rangle\langle u^\neg|$.

For two complementary observables of qubits $(\mathcal{C}^2, m_1, u_1)$ and $(\mathcal{C}^2, m_2, u_2)$, there is a unique observable of qubits $(\mathbb{C}^2, m_3, u_3)$ which is complementary to both $(\mathbb{C}^2, m_1, u_1)$ and $(\mathcal{C}^2, m_2, u_2)$. The phase shift $S_3(\frac{\pi}{2})$ of $(\mathbb{C}^2, m_3, u_3)$ maps u_1 to u_2, u_2 to $u_1^\neg$, $u_1^\neg$ to $u_2^\neg$ and $u_2^\neg$ to u_1. The result of applying $S_3(\frac{\pi}{2})$ to $\{u_1, u_2, u_1^\neg, u_2^\neg\}$ is summarized in Table 1.

state \ morphism	$S_3(0)$	$S_3(\frac{\pi}{2})$	$S_3(\pi)$	$S_3(\frac{3\pi}{2})$
u_1	u_1	u_2	$u_1^\neg$	$u_2^\neg$
u_2	u_2	$u_1^\neg$	$u_2^\neg$	u_1
$u_1^\neg$	$u_1^\neg$	$u_2^\neg$	u_1	u_2
$u_2^\neg$	$u_2^\neg$	u_1	u_2	$u_1^\neg$

Table 1: Encryption by phase shift

Remark 1. *The phase shift $S(\frac{\pi}{2})$ is a generalization of the $\sqrt{NOT}$ operator in quantum computational logic [9, 21, 18, 22, 10]. Indeed, the matrix representation of $\sqrt{NOT}$ is $\frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix}$, which is exactly $|+\rangle\langle+| + e^{\frac{\pi}{2}i}|-\rangle\langle-|$, the*

phase shift $S_x(\frac{\pi}{2})$ *of the observable* O_x.

Definition 18 (key space). *For two complementary observables of qubits* ($\mathbb{C}^2$, m_1, u_1) *and* ($\mathcal{C}^2, m_2, u_2$)*, the key space they induce is* $\{S_3(0), S_3(\frac{\pi}{2}), S_3(\pi), S_3(\frac{3\pi}{2})\}$.

Definition 19 (encryption by complementary observables). *For two complementary observables of qubits* ($\mathbb{C}^2$, m_1, u_1) *and* ($\mathbb{C}^2, m_2, u_2$)*, we let* $Key = \{S_3(0), S_3(\frac{\pi}{2}), S_3(\pi), S_3(\frac{3\pi}{2})\}$. *An encryption by complementary observables is a function* $Enc : Key \times \mathbb{C}^2 \mapsto \mathbb{C}^2$ *which maps a qubit* $|\alpha\rangle$ *to* $S|\alpha\rangle$*, where* $S \in Key$.

We will also use $Enc_S(|\alpha\rangle)$ to denote $Enc(S, |\alpha\rangle)$.

Definition 20 (informationally secure). *An encryption scheme is informationally secure if for every qubit* $|\alpha\rangle$*, if we encrypt it by taking keys according to a uniform probability distribution over the key space* $\{key_1, \ldots, key_n\}$*, then the result is a totally mixed state, i.e., the uniform probability distribution of* $\{Enc_{key_1}(|\alpha\rangle), \ldots, Enc_{key_n}(|\alpha\rangle)\}$ *is a totally mixed state.*

We remind the readers that the totally mixed state of a qubit is represented by the density matrix $\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. In the Bloch ball, the totally mixed state is represented by the center of the ball. For two complementary observables of qubits $(\mathcal{C}^2, m_1, u_1)$ and $(\mathcal{C}^2, m_2, u_2)$, a probability distribution ϕ over $\{u_1, u_1^{\neg}, u_2, u_2^{\neg}\}$ such that $\phi(u_1) = \phi(u_1^{\neg})$ and $\phi(u_2) = \phi(u_2^{\neg})$ is always a totally mixed state.

Theorem 1. *Encryption by complementary observables of qubits is informationally secure.*

Proof: Let ($\mathbb{C}^2$, m_1, u_1) and ($\mathbb{C}^2, m_2, u_2$) be an arbitrary pair of complementary observables of qubits. Let $Key = \{S_3(0), S_3(\frac{\pi}{2}), S_3(\pi), S_3(\frac{3\pi}{2})\}$ be the key space induced by this pair of complementary observables.

For the qubit u_1, after encryption by complementary observables we get a uniform probability distribution over $\{u_1, u_1^{\neg}, u_2, u_2^{\neg}\}$, which is a totally mixed state. Similarly, for the qubit $u_1^{\neg}$, after encryption by complementary observables we also get a uniform probability distribution over $\{u_1, u_1^{\neg}, u_2, u_2^{\neg}\}$.

Now, take u_1 and $u_1^\neg$ as the basis of qubits. Then every qubit $|\alpha\rangle = au_1 + bu_1^\neg$ for some $a, b \in \mathbb{C}$ such that $|a^2| + |b^2| = 1$. If we encrypt $|\alpha\rangle$ by complementary observables we get a uniform probability distribution over $\{au_1 + bu_1^\neg, au_2 + bu_2^\neg, bu_1 + au_1^\neg, bu_2 + au_2^\neg\}$, which is still a totally mixed state. □

4. Key distribution: generalized quantum three-pass protocol

A three-pass protocol in cryptography [25] is a protocol which enables one party to securely send a message to a second party by exchanging three encrypted messages. The essential idea of the three-pass protocol is that each party has private keys for encryption and decryption and they use their keys independently, first to encrypt the message, and then to decrypt the message.

Informally, the three-pass protocol for Alice to secretly send an object to Bob works as follows

1. Alice puts the object into a box, locks the box and mails it to Bob.
2. Bob adds his own lock to the box and sends it back to Alice.
3. Alice removes her lock and sends the box back to Bob.

This protocol can be implemented by using the exclusive-OR operation $\oplus$ in classical cryptography:

1. For a bit x, Alice encrypts it with her key k_a and then sends the encrypted bit $(x \oplus k_a)$ to Bob.
2. Bob encrypts the encrypted bit with his key k_b and sends $(x \oplus k_a) \oplus k_b$ to Alice.
3. Alice decrypts what she received by k_a and obtains $((x \oplus k_a) \oplus k_b) \oplus k_a = x \oplus k_b$. She then sends $x \oplus k_b$ to Bob.

The weakness of the above implementation is that if an eavesdropper copies the three messages $x \oplus k_a$, $(x \oplus k_a) \oplus k_b$ and $x \oplus k_b$, then he can deduce x from those messages because $(x \oplus k_a) \oplus ((x \oplus k_a) \oplus k_b) \oplus (x \oplus k_b) = x$. To overcome this weakness, Kanamori and Yoo [19] propose a quantum implementation of the three-pass protocol. Thanks to the quantum no-cloning theorem [31, 26],

the quantum three-pass protocol is resistant to eavesdroppers. A disadvantage of Kanamori and Yoo's quantum three-pass protocol is that the key space of their encryption is an infinite set. Recently, Qiu *et al* [27] developed another quantum three-pass protocol in the framework of CQM such that the size of the key space is significantly smaller. In this paper, we further generalize the protocol proposed in [27].

Given two complemenytary observables of qubits $(\mathbb{C}^2, m_1, u_1)$ and $(\mathbb{C}^2, m_2, u_2)$, we use a pair of classical points from an observable structure, say u_1 and $u_1^{\neg}$, to encode 0 and 1, respectively. Our key space for encryption and decryption is $Key = \{S_3(0), S_3(\frac{\pi}{2}),\ S_3(\pi), S_3(\frac{3\pi}{2})\}$. We let $(k, k^\dagger)$ be a pair of encryption/decryption keys, where $k^\dagger = S_3(2\pi - \frac{i\pi}{2})$ for $k = S_3(\frac{i\pi}{2})$.

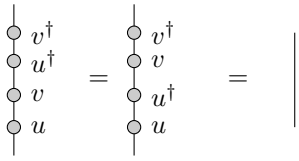
Our quantum three-pass protocol for Alice to send a qubit $|\alpha\rangle$ to Bob is composed of the following steps:

1. Alice randomly generates her private key $k_a \in Key$. Bob randomly generates his private key $k_b \in Key$.
2. Alice encrypts $|\alpha\rangle$ by k_a and sends $Enc(k_a, |\alpha\rangle) = k_a|\alpha\rangle$ to Bob.
3. Bob encrypts the received ciphertext $k_a|\alpha\rangle$ by k_b and sends $k_b k_a|\alpha\rangle$ to Alice.
4. Alice decrypts $k_b k_a|\alpha\rangle$ by $k_a^\dagger$ and sends $k_a^\dagger k_b k_a|\alpha\rangle$ to Bob.
5. Bob decrypts $k_a^\dagger k_b k_a|\alpha\rangle$ by k_b and obtains $k_b^\dagger k_a^\dagger k_b k_a|\alpha\rangle$.

This protocol can be used by the data owner to send his key and certificate to the user, as shown by the Step 4 depicted in Figure 1. The correctness of our protocol is guaranteed by commutativity of phase shift over complementary observables.

Theorem 2. *The quantum three-pass protocol is correct.*

Proof: Suppose Alice chooses u as her key and Bob chooses v as his key, then we have the following graphical derivation:



which means that the sequential composition of the operations of the 2 parties applied in the protocol is equivalent to an identity operator. Therefore, the qubit is correctly transferred. □

The security of most existing protocols of key distribution for access control in cloud environments relies on the computational complexity of problems like prime factorization. Therefore once a quantum computer is built, their protocol may be compromised in polynomial time [29]. Conversely, our protocol is secure with respect to quantum computers, since it provides informational security, due to the complementarity of observables. Here a key distribution protocol is informationally secure if the data

Theorem 3. *The quantum three-pass protocol is informationally secure in the sense that the qubit being transmitted at every stage of the protocol is a totally mixed state.*

Proof: This is a simple consequence of Theorem 1 and 2. □

5. Related work

The quantum one-time pad encryption scheme [5] is probably the most well-known encryption scheme in quantum cryptography. The key space for quantum one-time pad is $\{I, X, Z, XZ\}$. While this key space is much like a result of trial and error, our encryption scheme is more systematic and has a deeper theoretic background, besides ensuring the same security as quantum one-time pad.

The first and yet most influential protocol for quantum key distribution is developed by Bennett and Brassard [3], known as the BB84 protocol. In the BB84 protocol, more than a half of the transmitted qubits has to be disregarded. The quantum three-pass protocol is more efficient in the sense that no transmitted qubit has to be disregarded. Moreover, the quantum three-pass protocol

can be used to secretly send quantum data, while BB84 cannot. The quantum three-pass protocol introduced in [27] makes use of phase shift over two specific complementary observables, namely, the O_x and O_z observable. The three-pass protocol introduced in this paper is more general, in the sense that the two complementary observables do not have to be the O_x and O_z observable.

6. Conclusion

In this paper we study the application of quantum encryption and quantum key distribution in the access control problem. The quantum scheme/protocol we propose in this paper has various advantages over existing schemes/protocols proposed for the same purpose. They are informationally secure and implementable by the current technology. We remark that implementing quantum cryptographic protocols is much easier than building quantum computers. Many quantum cryptographic protocols have been realized in laboratories tens of years ago. Moreover, nowadays there are commercial companies selling devices for quantum key distribution and the technologies needed to implement the protocols in the paper are the same as the technologies needed for quantum key distribution that has been realized by commercial companies.

Acknowledgment

Xin Sun and Piotr Kulicki has been supported by the National Science Centre of Poland (BEETHOVEN, UMO-2014/15/G/HS1/04514).

Reference

[1] Abramsky S, Coecke B. A categorical semantics of quantum protocols. In: 19th IEEE Symposium on Logic in Computer Science (LICS 2004), 14-17 July 2004, Turku, Finland, Proceedings. IEEE Computer Society; 2004. p. 415–25. URL: https://doi.org/10.1109/LICS.2004.1319636. doi:10.1109/LICS.2004.1319636.

[2] Akl SG, Taylor PD. Cryptographic solution to a problem of access control in a hierarchy. ACM Trans Comput Syst 1983;1(3):239–48. URL: http://doi.acm.org/10.1145/357369.357372. doi:10.1145/357369.357372.

[3] Bennetta C, GillesBrassard . Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. 1984. p. 175–9.

[4] Bian X, Wang Q. Graphical calculus for qutrit systems. IEICE Transactions 2015;98-A(1):391–9. URL: http://search.ieice.org/bin/summary.php?id=e98-a_1_391.

[5] Boykin PO, Roychowdhury V. Optimal encryption of quantum bits. Physical Review A 2003;67:645–8.

[6] Castiglione A, Santis AD, Masucci B, Palmieri F, Castiglione A, Huang X. Cryptographic hierarchical access control for dynamic structures. IEEE Trans Information Forensics and Security 2016;11(10):2349–64. URL: http://dx.doi.org/10.1109/TIFS.2016.2581147. doi:10.1109/TIFS.2016.2581147.

[7] Castiglione A, Santis AD, Masucci B, Palmieri F, Castiglione A, Li J, Huang X. Hierarchical and shared access control. IEEE Trans Information Forensics and Security 2016;11(4):850–65. URL: http://dx.doi.org/10.1109/TIFS.2015.2512533. doi:10.1109/TIFS.2015.2512533.

[8] Castiglione A, Santis AD, Masucci B, Palmieri F, Huang X, Castiglione A. Supporting dynamic updates in storage clouds with the akl-taylor scheme.

Inf Sci 2017;387:56–74. URL: http://dx.doi.org/10.1016/j.ins.2016.08.093. doi:10.1016/j.ins.2016.08.093.

[9] Cattaneo G, Chiara MLD, Giuntini R, Leporini R. An unsharp logic from quantum computation. International Journal of Theoretical Physics 2004;43(7):1803–17. URL: https://doi.org/10.1023/B:IJTP.0000048821.56239.cb. doi:10.1023/B:IJTP.0000048821.56239.cb.

[10] Chiara MD, Giuntini R, Sergioli G, Leporini R. A many-valued approach to quantum computational logics. Fuzzy Sets and Systems 2016;URL: http://www.sciencedirect.com/science/article/pii/S0165011416304560. doi:https://doi.org/10.1016/j.fss.2016.12.015.

[11] Coecke B, Duncan R. Interacting quantum observables: categorical algebra and diagrammatics. New Journal of Physics 2011;13(043016):1–85.

[12] Coecke B, Heunen C, Kissinger A. Compositional quantum logic. In: Coecke B, Ong L, Panangaden P, editors. Computation, Logic, Games, and Quantum Foundations. The Many Facets of Samson Abramsky - Essays Dedicated to Samson Abramsky on the Occasion of His 60th Birthday. Springer; volume 7860 of *Lecture Notes in Computer Science*; 2013. p. 21–36. URL: https://doi.org/10.1007/978-3-642-38164-5_3. doi:10.1007/978-3-642-38164-5_3.

[13] Coecke B, Heunen C, Kissinger A. Categories of quantum and classical channels. Quantum Information Processing 2016;15(12):5179–209. URL: https://doi.org/10.1007/s11128-014-0837-4. doi:10.1007/s11128-014-0837-4.

[14] Coecke B, Kissinger A. Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning. Cambridge University Press, 2017.

[15] Coecke B, Paquette É. Categories for the Practising Physicist; Berlin, Heidelberg: Springer Berlin Heidelberg. p. 173–286. URL: https://doi.

org/10.1007/978-3-642-12821-9_3. doi:10.1007/978-3-642-12821-9_3.

[16] Coecke B, Perdrix S. Environment and classical channels in categorical quantum mechanics. Logical Methods in Computer Science 2010;8(4). URL: https://doi.org/10.2168/LMCS-8(4:14)2012. doi:10.2168/LMCS-8(4:14)2012.

[17] Coecke B, Wang Q, Wang B, Wang Y, Zhang Q. Graphical calculus for quantum key distribution (extended abstract). Electr Notes Theor Comput Sci 2011;270(2):231–49. URL: https://doi.org/10.1016/j.entcs.2011.01.034. doi:10.1016/j.entcs.2011.01.034.

[18] Giuntini R, Ledda A, Paoli F. Expanding quasi-mv algebras by a quantum operator. Studia Logica 2007;87(1):99–128. URL: https://doi.org/10.1007/s11225-007-9079-0. doi:10.1007/s11225-007-9079-0.

[19] Kanamori Y, Yoo S. Quantum three-pass protocol: Key distribution using quantum superposition states. International Journal of Network Security and Its Applications 2009;1(2):64–70.

[20] Lane SM. Categories for the Working Mathematician. Springer-Verlag, 1998.

[21] Ledda A, Konig M, Paoli F, Giuntini R. Mv-algebras and quantum computation. Studia Logica 2006;82(2):245–70. URL: https://doi.org/10.1007/s11225-006-7202-2. doi:10.1007/s11225-006-7202-2.

[22] Ledda A, Sergioli G. Towards quantum computational logics. International Journal of Theoretical Physics 2010;49(12):3158–65. URL: https://doi.org/10.1007/s10773-010-0368-4. doi:10.1007/s10773-010-0368-4.

[23] Liu Z, Huang X, Hu Z, Khan MK, Seo H, Zhou L. On emerging family of elliptic curves to secure internet of things: ECC comes of age. IEEE Trans Dependable Sec Comput 2017;14(3):237–48. URL: https://doi.org/10.1109/TDSC.2016.2577022. doi:10.1109/TDSC.2016.2577022.

[24] Liu Z, Weng J, Hu Z, Seo H. Efficient elliptic curve cryptography for embedded devices. ACM Trans Embedded Comput Syst 2017;16(2):53:1–53:18. URL: http://doi.acm.org/10.1145/2967103. doi:10.1145/2967103.

[25] Massey J. An introduction to contemporary cryptology. Proceedings of the IEEE 1988;76:533–49.

[26] Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge University Press, 2011.

[27] Qiu L, Sun X, Xu J. Categorical quantum cryptography for access control in cloud computing. Soft Computing 2017;URL: https://doi.org/10.1007/s00500-017-2688-2. doi:10.1007/s00500-017-2688-2.

[28] Selinger P. Dagger compact closed categories and completely positive maps: (extended abstract). Electr Notes Theor Comput Sci 2007;170:139–63. URL: https://doi.org/10.1016/j.entcs.2006.12.018. doi:10.1016/j.entcs.2006.12.018.

[29] Shor PW. Polynominal time algorithms for discrete logarithms and factoring on a quantum computer. In: Adleman LM, Huang MA, editors. Algorithmic Number Theory, First International Symposium, ANTS-I, Ithaca, NY, USA, May 6-9, 1994, Proceedings. Springer; volume 877 of *Lecture Notes in Computer Science*; 1994. p. 289. URL: http://dx.doi.org/10.1007/3-540-58691-1_68. doi:10.1007/3-540-58691-1_68.

[30] Sun X, Wang Q, Kulicki P, Zhao X. Quantum technique for access control in cloud computing I: Quantum imperative logic. Studia Logica 2017;:– Submitted.

[31] Yanofsky N, Mannucci M. Quantum Computing for Computer Scientists. Cambridge University Press, 2008.