International Journal of Advanced Engineering and Technology
ISSN: 2456-7655
Impact Factor: RJIF 5.54
www.newengineeringjournal.com
Volume 2; Issue 1; January 2018; Page No. 08-15

An entangled encryption method for quantum group signature

Kunpeng Wan[1], Hui Hu[2], Yafei Xiang[3], Xinyu Hou[4], Zhengying Cai[5*]
[1, 3, 5] College of Computer and Information Technology, China Three Gorges University, Yichang, China
[2, 4] School of Foreign Language, China Three Gorges University, Yichang, China

Abstract
Here an entangled encryption method for quantum group signature it put forward here. First, a new concept of quantum entanglement of group signatures are introduced. Some basic algebraic laws are also established for these simulation methods. Second, quantum group encryption and encryption protocols are introduced by enumerating two users' quantum cryptography. Due to the super operators maintained by the equivalence of quantum processes. Third, this article demonstrates the usefulness to verify the complex quantum protocols. Four, to reflect the method of quantum processes which can approximately realize their specifications, a strong bi-simulation of the quantized versions is defineds as a distance which is based on the bi-simulation for each pair of quantum processes to characterize their degree of similarity.

Keywords: group signature, encryption protocol, quantum encryption, quantum entanglement

1. Introduction

1.1 Related Work

Group signature is very important in information security. Schulze, Kornelius [2015] built Exome sequencing of hepatocellular carcinomas identifies new mutational signatures and potential therapeutic targets. Wirths, S [2015] extended Lasing in direct-bandgap GeSn alloy grown on Si, Tyanova, Stefka [2016] created the perseus computational platform for comprehensive analysis of (prote) omics data. Spang, Anja [2015] introduced Complex archaea that bridge the gap between prokaryotes and eukaryotes.Chiappinelli, Katherine B [2015] concerned inhibiting DNA methylation causes an interferon response in cancer via dsRNA including endogenous retroviruses. Cardoso, F [2016] evaluated 70-Gene Signature as an Aid to Treatment Decisions in Early-Stage Breast Cancer. Mertins, Philipp [2016] draw proteogenomics connects somatic mutations to signalling in breast cancer. Bleem, L. E [2015] introduced galaxy clusters discovered via the sunyaev-zel'dovich effect in the 2500-square-degree spt-sz survey.

Recently many researchers studied and applied quantum encryption. Wilde, Mark M [2017] made a research on converse bounds for private communication over quantum channels. Tan, Ru-Chao [2016] implied Quantum Color Image Encryption Algorithm Based on A Hyper-Chaotic System and Quantum Fourier Transform. Sanz, M. [2017] considered Solano, E., Entanglement classification with matrix product states. Kumari, Saru [2017] depicted On the design of a secure user authentication and key agreement scheme for wireless sensor networks. Berta, Mario discussed [2017] developed entanglement-assisted capacities of compound quantum channels. Bueno, Pablo [2016] displayed universal entanglement of singular surfaces. Ma, Jiaju [2017] etched photon-number-resolving megapixel image sensor at room temperature without avalanche gain. Martens, John C [2017] Quantum tomography for collider physics: illustrations with lepton-pair production. Ziegler, K [2017] extended controlling dynamical entanglement in a Josephson tunneling junction.

The quantum entanglement is a unique phenomenon in quantum mechanics. Olsen, M. K [2017] evaluated entanglement and asymmetric steering over two octaves of frequency difference. Zhou, Yiyu [2017] exhibited Mirhosseini, Mohammad; Fu, Dongzhi; Zhao, Jiapeng; Rafsanjani, Seyed Mohammad Hashemi; Willner, Alan E.; Boyd, Robert W. ,Sorting Photons by Radial Quantum Number. Deng, Song [2017] featured Distributed content filtering algorithm based on data label and policy expression in active distribution networks. Ermis, Orhan [2017] gave A key agreement protocol with partial backward confidentiality. Qiu, Yue [2017] illustrated An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems. Zhang, Jian [2017] implied A general framework to design secure cloud storage protocol using homomorphic, encryption scheme.

The advantage of quantum entanglement provided us a useful tool in encryption and signature. Wang, Yaping [2017] indicated Synthesis of fluorescent polymeric carbon nitride quantum dots in molten salts for security inks. He, Debiao [2017] made a modle Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography. Zhu, Feng [2017] modeled perimental long-distance quantum secure direct communication. Cao, Yuan [2017] offered Resource Assignment Strategy in Optical Networks Integrated With Quantum Key Distribution. Wu, WanQing [2017] painted Quantum Public Key Cryptosystem Based on Bell States. Wang, Yu-qi [2016] sketched Optimal Symmetric Ternary Quantum Encryption Schemes.

1.2 Organization of the Article

Section 2 introduces the concept of quantum entanglement and the definition of variables. Section 3 describes the equivalence of quantum processes in cryptographic protocols and cryptographic quantum group signatures. Section 4 includes the actual case of entanglement encryption with quantum signature and discussion.

2. Entanglement between quantum processes

Suppose there are three types of data in γ : Bool for booleans, real numbers Real for classical data, and qubits β bt for quantum data. Let γ *Var*, ranged over by γ , *r*,... and *cVar*, ranged over by *x, y*,... be the set of quantum variables and classical variables respectively. Assume that *cVar* and γ *Var* are countably infinite. Assume that a set *Exp* of classical data expressions over Real includes $\hbar$ *Var* as a subset and is ranged over by ϑ , ϑ ,... , and a set of boolean-valued expressions *BExp*, ranged over by*b, b* ,... , with the usual set of boolean operators true, false, ¬, ∧, ∨, and →. Particularly, let ϑ $\lhd\rhd$ ϑ be a boolean expression for any ϑ , ϑ ∈ *Exp* and $\lhd\rhd$ ∈ {>, <, ≥, ≤, =}. Let *cChan* be the set of classical channel names, ranged over by $\hbar$, *d*,... , and *qChan* the set of quantum channel names, ranged over by c, d,... . Let *Chan* = γ *Chan* ∪ γ *Chan*. A relabeling function *f* is a one-to-one function from *Chan* to *Chan* such that *f* ($\hbar$ *Chan*) ⊆ $\hbar$ *Chan* and *f* (γ *Chan*) ⊆ γ *Chan*.

When γ_1,..., γ_n are distinct quantum variables and the dimension *n* is understood, the indexed set { γ_1,..., γ_n } is often abbreviated to $\tilde{\gamma}$. Sometimes the string γ_1,..., γ_n is used to represent $\tilde{\gamma}$. Assume that a set of process constant schemes is ranged over by *A, B*,... . Each process constant scheme *A* is assigned a non-negative integer *ar*(*A*). If $\tilde{\tilde{\gamma}}$ is a tuple of distinct quantum variables with | $\tilde{\gamma}$ | = *ar*(*A*), then *A*($\tilde{\gamma}$) is called a process constant.

Definition 2.1 (*Quantum Process*). The set of quantum processes γ *Proc* and the free quantum variable function *qv* : γ *Proc* $\rightarrow 2^{\gamma var}$ are defined by the following rules respectively:

1. $\text{nil} \in \gamma\text{Proc}, \text{and } \text{qv}(\text{nil}) = \emptyset$;
2. $\text{A}(\tilde{\gamma}) \in \gamma\text{Proc}, \text{and } \text{qv}(\text{A}(\tilde{\gamma})) = \tilde{\gamma}$;
3. $\text{Y}.\theta \in \gamma\text{Proc}, \text{and } \text{qv}(\text{Y}.\theta) = \text{qv}(\theta)$;
4. $\hbar?\text{x}.\theta \in \gamma\text{Proc}, \text{and } \text{qv}(\hbar?\text{x}.\theta) = \text{qv}(\theta)$;
5. $\hbar!\vartheta.\theta \in \gamma\text{Proc}, \text{and } \text{qv}(\hbar!\vartheta.\theta) = \text{qv}(\theta)$;
6. $\hbar?\gamma.\theta \in \gamma\text{Proc}, \text{and } \text{qv}(\hbar?\gamma.\theta) = \text{qv}(\theta) - \{\gamma\}$;
7. $\text{If } \gamma \notin \text{qv}(\theta) \text{ then } \text{c}!\gamma.\theta \in \gamma\text{Proc}, \text{and } \text{qv}(\hbar!\gamma.\theta) = \text{qv}(\theta) \cup \{\gamma\}$
8. $\text{Z}[\tilde{\gamma}]\theta \in \gamma \text{ Pr}oc$, and $\text{qv}(\text{Z}[\tilde{\gamma}]\theta) = \text{qv}(\theta) \cup \tilde{\gamma}$;
9. $\text{M}[\tilde{\gamma}; \text{x}].\theta \in \gamma\text{Proc}, \text{and } \text{qv}(\text{M}[\tilde{\gamma}; \text{x}].\theta) = \text{qv}(\theta) \cup \tilde{\gamma}$
10. $\theta + \beta \in \gamma\text{Proc}, \text{and } \text{qv}(\theta + \beta) = \text{qv}(\theta) \cup \text{qv}(\beta)$;
11. $\text{If } \text{qv}(\theta) \cap \text{qv}(\beta) = \emptyset \text{ then } \theta \parallel \beta \in \gamma \text{ Proc}, \text{and } \text{qv}(\theta \parallel \beta) = \text{qv}(\theta) \cup \text{qv}(\beta)$;
12. $\theta[\text{ f }] \in \gamma\text{Proc}, \text{and } \text{qv}(\theta[\text{ f }]) = \text{qv}(\theta)$;
13. $\theta \setminus \text{L} \in \gamma\text{Proc}, \text{and } \text{qv}(\theta \setminus \text{L}) = \text{qv}(\theta)$;
14. if b then $\theta \in \gamma\text{Proc}, \text{and } \text{qv}(\text{if b then } \theta) = \text{qv}(\theta)$

where θ , β ∈ γ *Proc*, $\hbar$ ∈ $\hbar$ *Chan*, *x* ∈ $\hbar$ *Var*, $\hbar$ ∈ γ *Chan*, γ ∈ γ *Var*, $\tilde{\gamma}$ ⊆ γ *Var*, *e* ∈ *Exp*, *Y* is the silent action, *A*(γ) is a process constant, *f* is a relabeling function, *L* ⊆ *Chan*, *b*∈ *BExp*, $\tilde{\gamma}$ on the Hilbert space associated with $\tilde{\gamma}$. Furthermore, as *A*($\tilde{\gamma}$), there is a defining equation

$$A(\tilde{\gamma}) \overset{def}{=} \theta. \tag{2-1}$$

Where $\theta \in \gamma$ Proc with $qv(\theta) \subseteq \tilde{\gamma}$ When $\tilde{\gamma}$ = ∅, we simply denote *A*($\tilde{\gamma}$) as *A*.

For simplicity, only non-degenerate measurements are considered in this paper. This does not sacrifice the expression of γ because, as described in Section 2, non-degenerate measurements can be implemented with the aid of unitary operators, which are special cases of preserving super operators and can also be described in γ .

We usually define the free classical variables in quantum processes with a unique modification that *x* is bound by the quantum measurement prefix *M*[γ ; *x*]; If quantum process θ does not contain a free cl variable, *f v*(θ)= ∅, it is closed.

Definition 2.2 Let $R \subseteq Con \times Con$, and $\mathrm{N},\mathrm{O} \in \zeta(\mathrm{Con})$. A weight function for (N,O) with respect to R is a function $\mathrm{S}:\mathrm{supp}(\mathrm{N})\times\mathrm{supp}(\mathrm{N})\to[0,1]$ which satisfies

(1) For all $C \in supp(\mathrm{N})$ and $\zeta \in supp(O)$, $\sum_{\zeta\in\mathrm{supp}(\mathrm{O})} \mathrm{S}(\wp,\ \zeta)=\mathrm{N}(\mathrm{C}),\qquad \sum_{\wp\in\mathrm{supp}(\mathrm{N})} S(\wp,\ \zeta)=\mathrm{O}(\zeta);$

(2) If $\mathrm{S}(\wp,\zeta)>0$, then $(\wp,\zeta)\in R$;

We write $\mathrm{NR}O$ if there exists a weight function for (N, *O)* with respect to R.

Lemma 2.3 *Suppose* N, O, $m \in \zeta(Con)$, R, $\mathrm{R}'\subseteq \mathrm{Con}\times\mathrm{Con}$.

(1) NRO *if and only if* $\mathrm{NR}^{-1}\mathrm{O}$.

(2) *If* NRO *and* $\mathrm{OR}^{-1}\omega$, *then* $\mathrm{N}(\mathrm{R}\circ\mathrm{R}')\omega$.

(3) *If* $\mathrm{R}\subseteq\mathrm{R}'$, *then* NRO *implies* $\mathrm{NR}'\mathrm{O}$.

The following lemma gives an equivalent characterization of the ascending relation on $\zeta(Con)$, which comes directly from the original ascending relation on *Con* , independent of the weight function

3. Encryption in quantum group signature

Definition 3.1. The relation $\Rightarrow\subseteq\zeta(\mathrm{Con})\times\zeta(\mathrm{Con})$ is defined as the smallest relation to meet the following conditions:

(1) $\wp\Rightarrow\wp$;

(2) if $\wp\xrightarrow{\mathrm{Y}}\mathrm{N}$ and $\mathrm{N}\Rightarrow\mathrm{O}$, then $\wp\Rightarrow\mathrm{O}$;

(3) if $\mathrm{N}=\sum_{i\in I}\Re_i\wp_i$ and for any $i\in I,\wp_i\Rightarrow\mathrm{O}_i$ for some O_i then $\mathrm{N}=\sum_{i\in I}\Re_i\mathrm{O}_i$.

As pointed out by Deng *et al*. [2005] and Desharnais *et al*. [2002, 2010], it's essential for defining weak bisimulations of probabilistic processes to combine different transitions with the same weak flag. Therefore, paragraph (3) is added to definition 3.1.

For any $\mathrm{N},\mathrm{O}\in\zeta(\mathrm{Con})$and $s=\alpha_1\cdots\alpha_n\in Act^*$, we say that N can evolve into O by a

weak s-transition, denoted by $\mathrm{N}\overset{s}{\Rightarrow}\mathrm{O}$, if there exist $\mathrm{N}_1,\cdots,\mathrm{N}_{n+1},\mathrm{O}_1,\cdots,\mathrm{O}_n\in D(\mathrm{Con})$, such that $\mathrm{N}\Rightarrow\mathrm{N}_1,\mathrm{N}_{n+1}=\mathrm{O}$, and for each $i=1,\cdots,n,\mathrm{N}_i\xrightarrow{\alpha_i}\mathrm{O}_i$ and $\mathrm{O}_i\Rightarrow\mathrm{N}_{i+1}$.

Note that $\mathrm{N}\Rightarrow\xrightarrow{\alpha}\mathrm{O}$ differs from $\mathrm{N}\overset{\alpha}{\Rightarrow}\mathrm{O}$. For the former, the last action of every execution branch from N to O must be α. However, for the latter, the action α that appears in each branch is not necessarily the last.

The following lemma comes directly from Proposition 3.1 in Deng *et al*. [2007].

Lemma 3.2. *If* $\mathrm{N}\overset{s}{\Rightarrow}\mathrm{O}$, *and* $\mathrm{N}=\sum_{i\in I}\Re_i\mathrm{N}_i$ *where* $\Re_i>0$ *for each* $i\in I$, *then for any*

$i\in I,\mathrm{N}_i\overset{s}{\Rightarrow}\mathrm{O}_i$ *for some* O_i *such that* $\mathrm{O}=\sum_{i\in I}\Re_i\mathrm{O}_i$ *Conversely, if for each* $i\in I,\mathrm{N}_i\overset{s}{\Rightarrow}\mathrm{O}_i$,

then $\mathrm{N}\overset{s}{\Rightarrow}\mathrm{O}$ *where* $\mathrm{N}=\sum_{i\in I}\Re_i\mathrm{N}_i,\mathrm{O}=\sum_{i\in I}\Re_i\mathrm{O}_i,\Re_i>0$ *for each* $i\in I$, *and* $\sum_{i\in I}\Re_i=1$.

By Lemma 3.4, the transitivity of weak transitions is shown.

Lemma 3.5. *If* $\mathrm{N}\Rightarrow\mathrm{O}$ *and* $\mathrm{O}\Rightarrow\omega$,*then* $\mathrm{N}\Rightarrow\omega$.

PROOF. It can be provable by using clauses (1)-(3) in Definition 3.1 to summarize the depth of the inferred action $\mathrm{N}\Rightarrow\mathrm{O}$:

If $\mathrm{O}\Rightarrow\mathrm{N}$, then $N\Rightarrow\omega$ holds trivially.

Suppose $\mathrm{N}=\wp,\wp\xrightarrow{\mathrm{Y}}N'$, and $\mathrm{N}'\Rightarrow\mathrm{O}$. Then by induction, we derive $\mathrm{N}'\Rightarrow\omega$. Thus $\mathrm{N}\Rightarrow\omega$ by definition.

Suppose $\mathrm{N}=\sum_{i\in I}\Re_i\wp_i$, for any $i\in I,\wp_i\Rightarrow O_i$ for some O_i and $\mathrm{O}=\sum_{i\in I}\Re_i\mathrm{O}_i$. Then by Lemma 3.2, we have $\mathrm{O}_i\Rightarrow\omega_i$ for some ω_i such that $\omega=\sum_{i\in I}\Re_i\omega_i$ Now by induction, $\wp_i\Rightarrow\omega_i$, and then $\mathrm{N}\Rightarrow\omega$ by Lemma 3.2.

To conclude this subsection, Lemma 3.3 can be extended to the weak transition case.

Lemma 3.6. *If* $\langle\theta,\mathrm{T}\rangle\overset{s}{\Rightarrow}\mathrm{N}$, *then:*

(1) $tr(\mathrm{T})=tr(\mathrm{N})$;

(2) *there exist a set of super-operators* $\{\mathrm{Z}_i:i\in I\}$ *and projectors* $\{\mathrm{E}_i:i\in I\}$, *both acting on* $\mathrm{H}_{q\upsilon(\theta)\rfloor b\upsilon(s)}$ *where* $b\upsilon(\alpha_1\cdots\alpha_n)=b\upsilon(\alpha_1)\cup\cdots b\upsilon(\alpha_n),\sum_{i\in I}\mathrm{E}_i=I$ *such that for any* $\mathrm{J}\in D(\mathrm{H}),\langle\theta,\mathrm{J}\rangle\overset{s}{\Rightarrow}\sum_{i\in I}\gamma_i^J\langle\theta_i,\mathrm{Z}_i(J)\rangle$

where $\gamma_i^{\mathrm{J}}=tr(\mathrm{E}_iJ)$;

(3) *for any t super-operator E acting on* $\mathrm{H}_{\overline{q\upsilon(\theta)\cup b\upsilon(s)}}$, *we have* $\langle\theta, \mathrm{Z}(\mathrm{T})\rangle \overset{s}{\Rightarrow} \mathrm{Z}(\mathrm{N})$.

PROOF. Note that from Lemma 3.3 (1), if $0 \xrightarrow{\alpha} \mathbb{N}$ then $tr(\mathrm{O}) = tr(\mathrm{N})$. So to prove (1), only needs to show $tr(\mathrm{O}) = tr(\mathrm{N})$ provided that $0 \Rightarrow \mathbb{N}$. It can be provable by using clauses (1)-(3) in Definition 3.1 to summarize the depth of the inferred action $\mathrm{N} \Rightarrow \mathrm{O}$:
If $0 = \mathrm{N}$, then $tr(O) = tr(\mathrm{N})$ holds trivially.
Suppose $\mathrm{O} = \langle\theta, \mathrm{T}\rangle, \langle\theta, T\rangle \xrightarrow{\mathrm{Y}} \omega$, and $\omega \Rightarrow \mathrm{N}$. Then there exists $tr(\mathrm{N}) = tr(\omega) = tr(\mathrm{T})$, where the first and the second equation are derived by inducting and Lemma 3.3(1) respectively.

Suppose $\mathrm{O} = \sum_{i\in I} \Re_i \wp_i$, for any $i \in I, \wp_i \Rightarrow \mathrm{O}_i$ for some O_i and $\mathrm{N} = \sum_{i\in I} \Re_i \mathrm{O}_i$. Then by induction, $tr(\mathrm{O}_i) = tr(\wp_i)$. Thus $tr(\mathrm{N}) = \sum_{i\in I} \Re_i tr(\mathrm{O}_i) = \sum_{i\in I} \Re_i tr(\wp_i) = tr(\mathrm{O})$.

Though the proofs of (2) and (3) are more complicated, the method is similar. Therefore, the detail is omitted here.
Like the classical process algebra, the summation combiner cannot maintain weak bisimilarity. In order to solve this problem, the concept of equality between quantum processes based on $\approx$ is introduced
Definition 3.18. Both $\langle\theta, \mathrm{T}\rangle$ and $\langle\beta, \mathrm{J}\rangle$ are considered equal, denoted by $\langle\theta, \mathrm{T}\rangle \cong \langle\beta, \mathrm{J}\rangle$, if $q\upsilon(\theta) = q\upsilon(\beta), tr_{q\upsilon(\theta)}(\mathrm{T}) = tr_{q\upsilon(\beta)}(\mathrm{J})$, and:

(1) *Whenever* $\langle\theta, \mathrm{T}\rangle \xrightarrow{\hbar?\gamma} \mathrm{N}$, *then* $\langle\beta, \mathrm{J}\rangle \Rightarrow \xrightarrow{\hbar?\gamma} \mathrm{O}$ *for some* 0 *such that for any trace- preserving super-operator* $\mathbb{Z}$ *acting on* $\mathrm{H}_{\overline{q\upsilon(\mathrm{N})-\{\gamma\}}}, Z(\mathrm{N}) \approx Z(\mathrm{O})$;

(2) *whenever* $\langle\theta, \mathrm{T}\rangle \xrightarrow{\alpha} \mathrm{N}$ *where* α *is not a quantum input, then there exists* O *such that* $\langle\beta, \mathrm{J}\rangle \overset{\hat{\alpha}}{\Rightarrow} O$ *and* $\mathrm{N} \approx \mathrm{O}$*; and the symmetric conditions of (1) and (2).*

For $\theta, \beta \in \gamma\mathrm{Proc}, \theta \cong \beta$ if and only if for any quantum state $\mathrm{T} \in D(H)$ and any indexed set $\tilde{\mathrm{O}}$ of classical values, $\langle\theta\{\tilde{O}/\tilde{\chi}\}, \mathrm{T}\rangle \approx \langle\beta\{\tilde{O}/\tilde{\chi}\}, T\rangle$ where $\tilde{\chi} = f\upsilon(\theta) \cup f\upsilon(\beta)$.

Note that when $\approx$ is replaced by $\cong$, all weak bisimulation relations, which have been proved in the examples of previous sections, are also valid. The following properties are not difficult to show.

Theorem 3.7

(3) $\cong$ *is an equivalence relation;*
(4) $\theta \sim \beta$ *implies* $\theta \cong \beta$, *and* $\theta \cong \beta$, *implies* $\theta \approx \beta$;
(5) *if* $\theta \approx \beta$ *then* $\mathrm{a}.\theta \cong \mathrm{a}.\beta$ *for* $a \in \{\mathrm{Y}, \hbar?\chi, \hbar!\vartheta, \hbar?\gamma, \hbar!\gamma, \mathrm{Z}[\tilde{\gamma}], M[\tilde{\gamma}; \chi]\}$
(6) $\theta \cong \beta$ *if and only if* $\theta + \mathrm{R} \approx \beta + \mathrm{R}$ *for all* $\mathrm{R} \in \gamma\mathrm{Proc}$.

4. Examples and analysis

To illustrate the expressiveness of γ, there are some examples.

Example 4.4. Superdense coding [Bennett and Wiesner 1992] is a quantum protocol. As long as the sender and receiver have a priori share on the maximum entangled state, by delievering one qubit two bits of classical information will be transmitted. The agreement is as follows. Make $|\psi\rangle = (|11\rangle + |00\rangle)/\sqrt{2}$ the entangled state shared between Alice and Bob. Alice applies a Pauli operator on $|\psi\rangle$ qubit, according to which, Alice wishes to transmit which of the four possibilities and send its qubit to BobWith the two qubits in hand, Bob performs a perfect discrimination among the possible states (they are actually the four Bell states $\{\mathrm{J}^{\mathrm{i}} \otimes \mathrm{I}|\psi\rangle : \mathrm{i} = 0,1,2,3\}$ where a^{i} are defined in Section 2) and retrieves the information Alice has sent.

What is shown is how to describe the protocol of superdense coding with γ. Suppose *M* is a 2-qubit measurement such that $\mathrm{M} = \sum_{\mathrm{i}=0}^{3} i|\tilde{i}\rangle\langle\tilde{i}|$, where $\tilde{i}$ is the binary expansion of i. Suppose *CN* be the controlled-not operator and *H* Hadamard operator. Then the quantum processes participated in superdense coding protocol can be defined as follows.

$$
\begin{aligned}
&Alice_s = \hbar?x.\sum_{0\le i\le 3}(if\ x = i\ then\ \mathrm{J}^{i}[\gamma_1].\vartheta!\gamma_1.nil)\\
&Bob_s = \vartheta?\gamma_1.CN[\gamma_1,\gamma_2].H[\gamma_1].M[\gamma_1,\gamma_2;x].d!x.nil \qquad (4\text{-}1)\\
&Sdc = (Alice_s \,||\, Bob_s)\setminus\{\vartheta\}
\end{aligned}
$$

For any $\mathrm{T} \in \zeta(\mathrm{H} \xrightarrow[\gamma_1,\gamma_2]{})$ *and* $\mathrm{N} \in \{0,1,2,3\}$ *, there exists the transition* $\left\langle Sdc, \left[\left|\psi\right\rangle\right]_{\gamma_1,\gamma_2} \otimes \mathrm{T} \right\rangle$

$$
\begin{aligned}
&\xrightarrow{\vartheta?V} \left\langle \left(\left(\sum_{0\le i\le 3} (if\ \mathrm{O} = i\ then\ \mathrm{J}^i[\gamma_1].\vartheta!\gamma_1.nil) \right) \| Bob_s \right) \backslash \{\vartheta\}, \left[\left|\psi\right\rangle\right]_{\gamma_1,\gamma_2} \otimes \mathrm{T} \right\rangle \\
&\xrightarrow{Y} \left((\vartheta!\gamma_1.nil \parallel Bobs) \backslash \{e\}, J^{\mathrm{O}}_{\gamma_1}([\left|\psi\right\rangle]) \otimes T \right) \\
&\xrightarrow{Y} \left\langle (nil \parallel CN[\gamma_1,\gamma_2].H[\gamma_1].M[\gamma_1,\gamma_2;x].d!x.nil) \backslash \{\vartheta\}, (\left[\left|\psi\right\rangle\right]) \otimes \mathrm{T} \right\rangle \\
&\xrightarrow{Y} \left\langle (nil \parallel H[\gamma_1].M[\gamma_1,\gamma_2;x].d!x.nil) \backslash \{\vartheta\}, CN_{\gamma_1,\gamma_2}\left(\mathrm{J}^{\mathrm{O}}_{\gamma_1}(\left[\left|\psi\right\rangle\right])\right) \otimes T \right\rangle \\
&\xrightarrow{Y} \left\langle (nil \parallel M[\gamma_1,\gamma_2;x].d!x.nil) \backslash \{\vartheta\}, \left[\left|\tilde{\mathrm{O}}\right\rangle\right]_{\gamma_1,\gamma_2} \otimes T \right\rangle \\
&\xrightarrow{Y} \left\langle (nil \parallel d!\mathrm{O}.nil) \backslash \{\vartheta\}, \left[\left|\tilde{\mathrm{O}}\right\rangle\right]_{\gamma_1,\gamma_2} \otimes \mathrm{T} \right\rangle \\
&\xrightarrow{d!v} \left\langle (nil \parallel nil) \backslash \{\vartheta\}, \left[\left|\tilde{\mathrm{O}}\right\rangle\right]_{\gamma_1,\gamma_2} \otimes T \right\rangle
\end{aligned}
\tag{4-2}
$$

Example 4.5. As one of the most im-portant protocols in quantum information, theory Quantum teleportation [Bennett *et al*. 1993] can transmit unknown quantum state by sending only classical information by using the maximally entangled state shared between sender and receiver. And it acts as a key compoment in many other communication protocols. The agreement is as follows. Assuming $\left|\psi\right\rangle_{\gamma_1,\gamma_2}$ the entanglement state shared between the sender Alice and the receiver Bob, Alice and Bob respectively maintain $\gamma\ 1$ and γ_2. Let γ be the state of the quantum system where Alice wants to transfer to Bob. Fisrt she applies quantum control-not operations on γ and γ_1 with *q* the control qubit and γ_1 the target, then Hadamard operator *H* on γ. Based on the computational basis, she then measures γ and γ_1, and sends the mea-surement result to Bob. When a classical bit is received from Alice, Bob applies a Pauli operator on his qubit γ_2 to recover the original state of γ.

Let M, *CN*, *H,* and $\mathrm{J}^{\mathrm{i}}, \mathrm{i} = 0,\ldots,3$ be defined similarly in Example 4.4. Then the quantum processes, which are involved in teleportation protocol, are defined as follows

$$
\begin{aligned}
&Alice_t = \hbar?\gamma.CN[\gamma,\gamma_1].H[\gamma].M[\gamma,\gamma_1;x]\vartheta!x.nil \\
&Bob_t = \vartheta?\gamma_1.\sum_{0\le i\le 3}\left(if x = i then \mathrm{J}^i\left[\gamma_2\right].d!\gamma_2.nil\right) \\
&Tel = (Alice_t \parallel Bob_t) \backslash \{\vartheta\}
\end{aligned}
\tag{4-4}
$$

For any $\mathrm{T} \in \zeta(\mathrm{H} \xrightarrow[\gamma_1,\gamma_2]{})$ *, we have*

$$
\begin{aligned}
&\left\langle Tel, \left[\left|\psi\right\rangle\right]_{\gamma_1,\ \gamma_2} \otimes \mathrm{T} \right\rangle \\
&\xrightarrow{\vartheta?r} \left\langle \left(CN[r,\gamma_1].H[r].M[r,\gamma_1;x].\vartheta!x.nil \| Bob_t\right) \backslash \{\vartheta\}, \left[\left|\psi\right\rangle\right]_{\gamma_1,\gamma_2} \otimes \mathrm{T} \right\rangle \\
&\xrightarrow{Y} \left(\left(H[r].M[r,\gamma_1;x].\vartheta!x.nil \| Bob_t\right) \backslash \{\vartheta\}, CN_{r,\gamma_1}([\left|\psi\right\rangle]_{\gamma_1,\gamma_2}) \otimes T \right) \\
&\xrightarrow{Y} \left\langle (nil \parallel M[\gamma_1,\gamma_2;x].\vartheta!x.nil \| Bob_t) \backslash \{\vartheta\}, \sum_{0\le j\le 3} \frac{1}{4}\left[\left|\tilde{j}\right\rangle\right]_{r,\gamma_1} \otimes J^j_{\gamma_2} T \right\rangle \\
&\quad \tfrac{1}{4} \bullet \left(\vartheta!0.nil \| Bob_t\right) \backslash \{\vartheta\}, \left[\left|00\right\rangle\right]_{r,\gamma_1} \otimes \mathrm{J}^j_{q_2} T \\
&\xrightarrow{Y} \boxplus \tfrac{1}{4} \bullet \left(\vartheta!1.nil \| Bob_t\right) \backslash \{\vartheta\}, \left[\left|01\right\rangle\right]_{r,\gamma_1} \otimes J^j_{\gamma_2} T \\
&\quad \boxplus \tfrac{1}{4} \bullet \left(\vartheta!2.nil \| Bob_t\right) \backslash \{\vartheta\}, \left[\left|10\right\rangle\right]_{r,\gamma_1} \otimes J^j_{\gamma_2} T \\
&\quad \boxplus \tfrac{1}{4} \bullet \left(\vartheta!3.nil \| Bob_t\right) \backslash \{\vartheta\}, \left[\left|11\right\rangle\right]_{r,\gamma_1} \otimes J^j_{\gamma_2} T
\end{aligned}
\tag{4-5}
$$

Here Eq. (3) is calculated as follows. Notice that any $\mathrm{T} \in \zeta\left(\mathrm{H} \xrightarrow[\{q_1,q_2\}]{}\right)$ can be decomposed as $\mathrm{T} = \sum_{0 \le i \le 3} \gamma_i \left[\!\left| \psi_i \right\rangle\!\right]_r \otimes \mathrm{T}_i$ where $\left|\psi_0\right\rangle = \left|0\right\rangle, \left|\psi_0\right\rangle = \left|1\right\rangle, \left|\psi_2\right\rangle = \left(\left|0\right\rangle + \left|1\right\rangle\right)/\sqrt{2}$, and $\left|\psi_3\right\rangle = \left(\left|0\right\rangle - \left|1\right\rangle\right)/\sqrt{2}$ |. Then it is easy to derive that

$$\begin{aligned}
\mathrm{H}_{\mathrm{r}}(\mathrm{CN}_{\mathrm{r},\gamma_1} \otimes \left[\!\left|\Psi\right\rangle\!\right]_{\gamma_1,\gamma_2} \otimes \mathrm{T})) &= \frac{\gamma_0}{4}\left[\!\left|000\right\rangle + \left|011\right\rangle + \left|100\right\rangle + \left|111\right\rangle\right]_{\mathrm{r},\gamma_1,\gamma_2} \otimes \mathrm{T}_0 \\
&+ \frac{\gamma_1}{4}\left[\!\left|001\right\rangle + \left|010\right\rangle + \left|101\right\rangle + \left|110\right\rangle\right]_{\mathrm{r},\gamma_1,\gamma_2} \otimes T_1 \\
&+ \frac{\gamma_2}{4}\left[\!\left|00\,\text{-}\right\rangle + \left|01\,\text{-}\right\rangle + \left|10\,+\right\rangle + \left|11\,+\right\rangle\right]_{\mathrm{r},\gamma_1,\gamma_2} \otimes T_2 \\
&+ \frac{\gamma_3}{4}\left[\!\left|00\,\text{-}\right\rangle - \left|01\,\text{-}\right\rangle + \left|10\,+\right\rangle + \left|11\,+\right\rangle\right]_{\mathrm{r},\gamma_1,\gamma_2} \otimes T_3 \\
&= \frac{1}{4}\left[\!\left|00\right\rangle\right]_{\mathrm{r},\gamma_1} \otimes T + \frac{1}{4}\left[\!\left|01\right\rangle\right]_{\mathrm{r},\gamma_1} \otimes J^1_{\gamma_2}(T) \\
&+ \frac{1}{4}\left[\!\left|10\right\rangle\right]_{\mathrm{r},\gamma_1} \otimes \mathrm{J}^2_{\gamma_2}(T) + \frac{1}{4}\left[\!\left|11\right\rangle\right]_{\mathrm{r},\gamma_1} \otimes \mathrm{J}^3_{\gamma_2}(T)
\end{aligned} \tag{4-6}$$

Example 3,6 (Encode Quantum Circuits with γ). There are two kinds of gates in uantum circuits. One is unitary gates and another is the quantum measurements. Now what is shown is to encode them using γ . For simplicity, quantum channels are allowed to input and output multiple qubits. If *n* qubits can be communicated through c at the same time, there will be the quantum channel c as c^n. That is, the quantum capacity of $\hbar^n$ is *n* quantum bits.

Then the unitary gate implementing *U* can be defined as a process constant $\mathrm{N}(\mathrm{U}), \mathrm{qv}(N(\mathrm{U})) = \emptyset$, with the defining equation

$$\mathrm{N}(\mathrm{U}) \overset{\deg}{=} \hbar^{\mathrm{n}}?\tilde{\gamma}.\mathrm{U}[\tilde{\gamma}].\mathrm{d}^{\mathrm{n}}!\tilde{\gamma}.N(\mathrm{U}) . \tag{4-7}$$

We set $ar(\mathrm{N}(\mathrm{U})) = n$.

Then the measurement gate can be defined as

$$M(\mathrm{M}) \overset{\deg}{=} \hbar^{\mathrm{n}}?\tilde{\gamma}.M[\tilde{\gamma};\mathrm{x}].\mathrm{e}!\mathrm{x}.\mathrm{d}^{\mathrm{n}}!\tilde{\gamma}.M(\mathrm{M}) . \tag{4-8}$$

We set $\mathrm{ar}(\mathrm{M}(\mathrm{M})) = \mathrm{n}$.

For any $\mathrm{T} \in D(\mathrm{H})$, we have

$$\begin{aligned}
\left\langle \mathrm{U}(\mathrm{U}), \mathrm{T} \right\rangle &\xrightarrow{\hbar^{\mathrm{n}}?\tilde{\mathrm{r}}} \langle\, \mathrm{U}[\tilde{\mathrm{r}}].\mathrm{d}^{\mathrm{n}}!\tilde{\mathrm{r}}.\mathrm{N}(\mathrm{U}), T) \\
&\xrightarrow{\mathrm{Y}} \langle\, \mathrm{d}^{\mathrm{n}}!\tilde{\mathrm{r}}.N(\mathrm{U}), U_{\tilde{\mathrm{r}}} T U^{+}_{\tilde{\mathrm{r}}}) \\
&\xrightarrow{\mathrm{d}^{\mathrm{n}}!\tilde{\mathrm{r}}} \langle\, N(\mathrm{U}), U_{\tilde{\mathrm{r}}} T U^{+}_{\tilde{\mathrm{r}}})
\end{aligned} \tag{4-9}$$

And

$$\begin{aligned}
(\mathrm{M}(\mathrm{M}), \mathrm{T}) &\xrightarrow{\hbar^{\mathrm{n}}?\tilde{\mathrm{r}}} \left\langle M[\tilde{r};x].\vartheta!x.d^n!\tilde{\mathrm{r}}.\mathrm{M}(\mathrm{M}), T \right\rangle \\
&\xrightarrow{\mathrm{Y}} \boxplus_{\mathrm{i}\in\mathrm{I}} \theta_i \bullet \left\langle \vartheta!\lambda_i.d^n!\tilde{\mathrm{r}}.\mathrm{M}(\mathrm{M}), E^{+}_{\tilde{\mathrm{r}}} T E^{+}_{\tilde{\mathrm{r}}} / \theta_i \right\rangle
\end{aligned} \tag{4-10}$$

where $\mathrm{M} = \sum_{i \in \mathrm{I}} \lambda_i \mathrm{E}^{\mathrm{i}}$ and $\theta_{\mathrm{i}} = \mathrm{tr}(\mathrm{E}^{\mathrm{i}}_{\tilde{\mathrm{r}}}\mathrm{T})/\mathrm{tr}(T)$. Now for each $\mathrm{i} \in \mathrm{I}$

$$(\vartheta!\lambda_{\mathrm{i}}.\mathrm{dn}!.\mathrm{M}(\mathrm{M}), E^i_{\tilde{\mathrm{r}}} T E^i_{\tilde{\mathrm{r}}} / \theta_i) \xrightarrow{\vartheta!\lambda_{\mathrm{i}}} \left\langle d^n!\tilde{\mathrm{r}}.\mathrm{M}(\mathrm{M}), E^i_{\tilde{\mathrm{r}}} T E^i_{\tilde{\mathrm{r}}} / \theta_i \right\rangle \xrightarrow{d^n!\tilde{\mathrm{r}}} \left\langle \mathrm{M}(\mathrm{M}), E^i_{\tilde{\mathrm{r}}} T E^i_{\tilde{\mathrm{r}}} / \theta_i \right\rangle \tag{4-11}$$

5. Conclusions and further work

By introducing the general notion of entanglement and group signature among quantum processes, which is the Quantum Encryption in Group Signatures. The quantum cryptography of two users is also enumerated to introduce quantum group encryption and encryption protocols. Obviously, the (approximate) strong bi-simulations previously mentioned are too different since the internal behavior caused by the local quantum operations and (classical or quantum) communications also needs to be perfectly matched by a bimodulus quantum process. Take it for example. A formal model q is proposed, which is a quantum extension of classical value-transmitted that models and critically models the behavior of quantum distributed and quantum communication protocols analysis. The notion of strong / weak bi-simulations of quantum processes in q is defined and they are preserved by a variety of process builders, including parallel combinations of classical and quantum communications. These are the first consistent equivalents of process algebra proposed so far for modeling quantum communication systems. A strong approximate version of the bi-simulations is also proposed to describe the distance between two quantum processes. Though they are not strongly dual simulations, according to a variety of examples, they can fully demonstrate the expressiveness of q and techniques of proving presented in this article.

Another interesting direction that is worth researching is to expand the application scope of γ to model and to analyze the security of quantum cryptographic systems. The SPI calculus [Abadi and Gordon 1997] has been very successful in cryptographic protocol analysis by introducing cryptographic primitives, such as constructors for encryption and decryption. Take BB84 quantum key distribution protocol for example, a similar extension of γ will provide tools for analyzing quantum cryptographic protocols.

6. Acknowledgments

This research was supported by the National Natural Science Foundation of China (No. 71471102), and Yichang University Applied Basic Research Project in China (Grant No. A17-302-a13).

7. References

1. Schulze Kornelius, Imbeaud Sandrine, Letouze Eric, Alexandrov Ludmil B, Calderaro Julien, Rebouissou Sandra, *et al*. Jessica, Exome sequencing of hepatocellular carcinomas identifies new mutational signatures and potential therapeutic targets, Nature Genetics [J]. 2015; 47(5):505-u106.
2. Wirths S, Geiger R, von den Driesch N, Mussler G, Stoica T, Mantl S, Ikonic Z, *et al*. Lasing in direct-bandgap GeSn alloy grown on Si: Nature Photonics [J]. 2015; 9(2):88-92.
3. Tyanova Stefka, Temu Tikira, Sinitcyn Pavel, Carlson Arthur, Hein Marco Y, Geiger Tamar, *et al*. The Perseus computational platform for comprehensive analysis of (prote) omics data, Nature Methods [J]. 2016; 13(9):731-740.
4. Spang Anja, Saw Jimmy H, Jorgensen Steffen L, Zaremba-Niedzwiedzka Katarzyna, Martijn Joran, Lind Anders E, *et al*. Complex archaea that bridge the gap between prokaryotes and eukaryotes, Nature [J]. 2015; 521(7551):173- +.
5. Chiappinelli Katherine B, Strissel Pamela L, Desrichard Alexis, Li Huili, Henke Christine, *et al*. Inhibiting DNA Methylation Causes an Interferon Response in Cancer via dsRNA Including Endogenous Retroviruses, CELL [J]. 2015; 162(5):974-986.
6. Cardoso F, van't Veer LJ, Bogaerts J, Slaets L, Viale G, Delaloge S Pierga JY, *et al*. 70-Gene Signature as an Aid to Treatment Decisions in Early-Stage Breast Cancer, New England journal of medicine [J]. 2016; 375(8):717-729.
7. Mertins Philipp, Mani DR, Ruggles Kelly V, Gillette Michael A, Clauser Karl R, *et al*. Proteogenomics connects somatic mutations to signalling in breast cancer, Nature [J]. 2016; 534(7605):55-+.
8. Bleem LE, Stalder B, de Haan T, Aird KA, Allen SW, Applegate DE, *et al*. Galaxy clusters discovered via the sunyaev-zel'dovich effect in the 2500-square-degree spt-sz survey, astrophysical journal supplement series [J]. 2015; 216(2), - .
9. Wilde Mark M, Tomamichel Marco, Berta Mario. Converse Bounds for Private Communication Over Quantum Channels, IEEE transactions on information theory [J]. 2017; 63(3):1792-1817.
10. Tan Ru-Chao, Lei Tong, Zhao Qing-Min, Gong Li-Hua, Zhou Zhi-Hong. Quantum Color Image Encryption Algorithm Based on A Hyper-Chaotic System and Quantum Fourier Transform, International journal of theoretical physics [J]. 2016; 55(12):5368-5384.
11. Sanz M, Egusquiza IL, Di Candia R, Saberi H, Lamata L, Solano E. Entanglement classification with matrix product states, Scientific Reports [J], 2017; 6.- .
12. Kumari Saru, Das Ashok Kumar, Wazid Mohammad, Li Xiong, Wu Fan, Choo Kim-Kwang Raymond, Khan. Muhammad Khurram, On the design of a secure user authentication and key agreement scheme for wireless sensor networks, concurrency and computation-practice & experience [J]. 2017; 29(23), - .
13. Berta Mario, Gharibyan Hrant. Walter, Michael, Entanglement-Assisted Capacities of Compound Quantum Channels, IEEE transactions on information theory [J]. 2017; 63(5):3306-3321.

14. Bueno Pablo, Myers Robert C, Witczak-Krempa. William, Universal entanglement of singular surfaces, fortschritte der physik-progress of physics [J]. 2016; 64(4-5):345-348.
15. Ma Jiaju, Masoodian Saleh, Starkey Dakota A, Fossum Eric R. Photon-number-resolving megapixel image sensor at room temperature without avalanche gain, Optica [J]. 2017; 4(12):1474-1481.
16. Martens John C, Ralston John P, Takaki JD. Tapia Quantum tomography for collider physics: illustrations with lepton-pair production, European Physical Journal C [J]. 2017; 31(32).
17. Ziegler K. Controlling dynamical entanglement in a Josephson tunneling junction, International journal of modern physics B [J]. 2017; 31(32).
18. Olsen MK. Entanglement and asymmetric steering over two octaves of frequency difference, Physical Review A [J]. 2017; 96(6).
19. Zhou Yiyu, Mirhosseini Mohammad, Fu Dongzhi, Zhao Jiapeng, Rafsanjani Seyed Mohammad Hashemi, *et al*. Sorting Photons by Radial Quantum Number, Physical review letters [J]. 2017; 119(26).
20. Deng Song, Yue Dong, Zhou Aihua, Fu Xiong, Yang Lechan, Xue Yu. Distributed content filtering algorithm based on data label and policy expression in active distribution networks,. Neurocomputing [J]. 2017; 270:159-169.
21. Ermis Orhan, Bahtiyar Serif, Anarim Emin, Caglayan M. Ufuk, A key agreement protocol with partial backward confidentiality, Computer Networks [J]. 2017; 129:159-177.
22. Qiu Yue, Ma Maode, Chen Shuo. An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems, Computer Networks [J]. 2017; 129:306-318.