南華大學科技學院資訊管理學系

碩士論文

Department of Information Management
College of Science and Technology
Nanhua University

Master Thesis

一個非糾纏的量子貨幣系統

A Quantum Money System Without Entanglement

許淑媚

Shu-Mei Hsu

指導教授：王昌斌 博士

周志賢 博士

Advisor: Chang-Bin Wang, Ph.D.

Jue-Sam Chou, Ph.D.

中華民國 109 年 5 月

May 2020

南華大學

科技學院資訊管理學系

碩士學位論文

一個非糾纏的量子貨幣系統

A Quantum Money System Without Entanglement

研究生：許淑媚

經考試合格特此證明

口試委員：周志榮

[illegible]

阮金聲

邱宏彬

指導教授：[illegible] 周志榮

系主任(所長)：[illegible]

口試日期：中華民國 109 年 5 月 6 日

南 華 大 學 碩 士 班 研 究 生

論 文 指 導 教 授 推 薦 函

_資訊管理_系碩士班_ 許淑媚 _君所提之論文

A Quantum Money System Without Entanglement

係由本人指導撰述，同意提付審查。

指導教授 周志賢

109年 5 月11日

南華大學資訊管理學系碩士論文著作財產權同意書

立書人：許淑媚 之碩士畢業論文

中文題目： 一個非糾纏的量子貨幣系統

英文題目： A Quantum Money System Without Entanglement

指導教授：王昌斌 和 周志賢 博士

學生與指導老師就本篇論文內容及資料其著作財產權歸屬如下：

■ 共同享有著作權

□ 共同享有著作權，學生願「拋棄」著作財產權

□ 學生獨自享有著作財產權

學　　生：許淑媚（請親自簽名）

指導老師：王昌斌（請親自簽名）

周志賢（請親自簽名）

中華民國 109 年 05 月 11 月

誌謝

重拾書本就讀研究所，是我送給自己的四十歲禮物，而鼓勵我退怯腳步的是我的大學同學－希盈。感謝她熱情的提供我相關的就讀資訊與資源，讓我更有勇氣面對此挑戰。在就讀期間，非常感謝授課老師的幽默風趣以及班上同學的相互幫助，讓我覺得犧牲假日時間讀書並不是一件很痛苦的事情，反而變成了一段美好的回憶。碩一的生活雖然辛苦，但是只要是與同學們在一起，無論是讀書、考試、打報告 等也變成了一種樂趣。在此我要感謝兩年來一直陪伴我的同學－怡如、育其和詠涵。

在研究的這條路程中，我最應該要感謝王昌斌教授和周志賢教授的帶領，讓我開啟量子世代的大門，從完全不理解量子態到能運算量子協商密鑰、量子隱形傳輸以及研究量子錢並完成此篇論文，這一年多以來，在每周的討論以及指導中，兩位老師們都對我十分包容，也常給予我很大的鼓勵，讓我對這完全陌生的領域，產生了繼續研究的樂趣。未來仍要繼續跟兩位老師學習，希望能更理解這門神祕的量子力學理論並將其用於加強資訊安全上。

最後，我還得感謝我的老公，可以讓我擁有許多自由的讀書時間。就算我每次熬夜打報告時會干擾到他的睡眠，他也從不抱怨。

人的一生中，想要成就某件事，除了自身的努力之外，在獨自邁進的旅程中，也需要遇到許許多多的貴人相助，我很幸運的在就讀的兩年時光裡，遇到了這些貴人－老師、學姐、同學以及學弟妹們，讓我能快樂並順利的完成學業。謹以此文表達我深摯的謝意。

許淑媚 謹誌

2020 年 5 月

一個非糾纏的量子貨幣系統

學生：許淑媚　　指導教授：王昌斌博士

周志賢博士

南華大學　資訊管理學系碩士班

摘要

隨著量子信息技術的不斷突破以及對比特幣去中心化議題的熱烈討論，量子貨幣的思想也逐漸成為近來的關注焦點。因此，一些密碼學學者也紛紛提出了量子貨幣方案的設計。然而，它們的方案中大多數都要求客戶和銀行必須事先共享密鑰，並且只有銀行才能驗證量子貨幣的真實性。而這樣的設計方式，可能會遭受罪犯的攻擊，因為身份驗證過程不是即時性的，也因此，降低了商業交易的時效性。

由於這些原因，在本文中，我們基於 chen 等人可公開驗證的量子簽章以及量子盲簽名方案和其電子現金系統等基礎，提出了一種量子貨幣系統，此系統使用可公開驗證的量子簽章方案取得許可證，並通過量子貨幣簽章方案的現金系統架構來建立取款和支付協議。此外，我們還進行了相關的安全分析以支持我們的理論。

關鍵詞：量子貨幣、量子非對稱密碼學、量子簽名、量子盲簽名

A Quantum Money System Without Entanglement

Student: Shu-Mei Hsu Advisor: Chang-Bin Wang, Ph.D.
Jue-Sam Chou, Ph.D.

Department of Information Management
Nanhua University
Master Thesis

ABSTRACT

With the continuous breakthrough of quantum information technology and heat discussion of Bitcoin, the idea of quantum money has gradually become the attention focus recently. As such, several cryptographic scholars have proposed quantum money schemes. However, most of them require the customer and bank to share a secret key in advance, and only the bank can verify the authenticity of the quantum money. This may suffer criminals' attacks, because the authentication process is not real time. Thus, reduces the validity of commercial transactions.

For these reasons, in this article, based on chen et al.'s publicly verifiable quantum signature and quantum blind signature schemes, and their electronic cash system, we propose a quantum money scheme that uses the publicly verifiable quantum signature scheme to obtain a license, and establish a withdrawal and a payment protocol through the usage of quantum blind signature by referring to their cash system architecture. In addition, we also make relevant security analysis to support our theory.

Keywords: Quantum money, Quantum asymmetric cryptography, Quantum signature, Quantum blind signature

Directory

指導教授推薦函..... Ⅰ

著作財產權同意書.....Ⅱ

誌謝.....Ⅲ

中文摘要.....Ⅳ

ABSTRACT.....Ⅴ

Directory..... Ⅵ

Chart catalogue.....Ⅷ

Table directory.....Ⅸ

1. Introduction.....**1**

2. Literature review.....**3**

2.1. A publicly verifiable quantum signature scheme based on asymmetric quantum cryptography without entanglement.....3

2.2. A publicly verifiable quantum blind signature scheme without entanglement based on asymmetric cryptography.....6

3. The proposed scheme.....**10**

3.1. Design philosophy.....11

3.1.1. License issuing.....12

3.1.2. Withdrawal protocol.....12

3.1.3. Owner tracing.....13

3.2. System set-up.....13
3.3. License-issuing protocol.....14
3.4. Withdrawal protocol.....15
3.5. Payment protocol.....18
3.6. Deposit protocol.....20
3.7. Quantum money owner tracing.....21
4. Security analysis.....22
4.1. Unforgeability.....22
4.2. Non-repudiation.....24
4.3. Verifiability.....24
4.4. Untraceability.....25
4.5. Anonymity revocation.....26
5. Comparisons.....27
6. Conclusion.....28
7. Reference.....29

Chart catalogue

Fig. 1. 方案架構圖 Outline of proposed scheme……**11**

Fig. 2. 許可證發放協議流程圖 License-issuing protocol……**16**

Fig. 3.提款協議流程圖 Withdrawal protocol……**16**

Fig. 4.付款協議流程圖 Payment protocol……**19**

Fig. 5.存款協議流程圖 Deposit protocol……**20**

Table directory

Table 1. 符號定義 Notations definitions.....**10**

Table 2. 與文獻比較結果 Comparison results with the literature.....**27**

1. Introduction

Traditional digital currency has received extensive and in-depth research. The focus is on how to improve the security of transactions [1-4]. However, digital currency has a natural flaw that bits can be easily copied and its security is based on computational infeasibility. The former makes it fragile and the latter becomes computational insecure after the quantum computer emerged. For these reasons, people try to use no-cloning theorem of quantum state to produce money in quantum version, which hopefully eliminate the possibility of money counterfeiting, making the money no longer need to base on computational hardness. Hence, in such field the Heisenberg's uncertainty principle [5] and no-cloning theorem [6, 23, 24] make quantum money the earliest interest area in quantum information theory, because both theorems guarantee that forging quantum money is impossible. Thus, after Wiesner had proposed a new quantum cryptographic scheme in 1983 [7], which became a well-known quantum money, several quantum money generation and verification schemes were proposed [8-12]. Among the excellent proposed schemes, two verify the authenticity of quantum money via using private key quantum system [7-8], where the verification is executed by a trusted third party. The others are public key quantum systems [10-12], in which the verification can be executed by anyone. Yet, we found that schemes [8, 9, 10, 12] are based on the computational infeasibility of verifying the traditional signature. In other words, the security of their schemes is not on the quantum

level. They rely on the computation hardness of traditional computer. Scheme [11] is good quantum Bitcoin protocols. However, we found that Ikeda et al.'s protocol is traceable, because it uses the remitter's signature to verify the coin owner. In 2020, Horodecki et al. [25] propose a semi-device-independent quantum money. Their scheme is a good idea in implementation. Nevertheless, it verifies quantum money based on probability. It is not in a deterministic way. Thus, is not suitable to be applied in real world transactions.

Allenson et al. [20, 21] argued that a quantum public key money scheme should have the following characteristics:

(1) There are effective algorithms for generating quantum money states

(2) No need to communicate with the bank, anyone can verify quantum money,

(3) No one can clone the quantum money

In view of these features, we use a quantum public key system to design quantum money, in which anyone can verify the quantum money by himself.

The rest of this article is described as follows. In Section 2, we review both the publicly verifiable quantum signature [13] and the quantum blind signature scheme [14]. Then, by using both reviewed schemes and referring to the protocol architectures in [1], we design quantum money in Section 3. The security analysis of the proposed is introduced in Section 4. We compare the security of the proposed with the state-of-the-art and list the results in Table 2. Then, a conclusion is given in Section 6.

2. Literature review

In this section, we review two of Chen et al's quantum signature schemes. Based on which, we establish our quantum money system. One is quantum signature scheme [13] and the other is quantum blind signature scheme [14]. The security of the two schemes was confirmed in the respective security analysis of their articles. For clarity, the definitions of used notations can be referred to the original schemes.

2.1. A publicly verifiable quantum signature scheme based on asymmetric quantum cryptography without entanglement [13]

Their signature scheme includes three phases: (a) key generation phase, (b) signature phase, and (c) verification phase. We describe them as follows:

(a) Key generation phase

This phase is the same as in [17] that the system prepares for each system member j's quantum public key/private key pair as $|\varphi_{pk}\rangle_j$ /($S_j\theta_n$)$_j$, where $|\varphi_{pk}\rangle_j$ = $\otimes_{j=1}^{n} R^{(j)}(S_j\theta_n)_j|0_z\rangle$.

(b) Signature stage

In this phase, the signer A signs on a message *m* by using the following steps.

1. Selects a random number set r_0 in GF(2^n) [15], and denotes its j^{th} element as r_{0j}.

2. Computes

$H(m, r_{0j}) = q_j * (S_j)_A + r_j = W_{1j}, \qquad hq_j = H(q_j, r_j, (S_j\theta_n)_A),$

/ In the following, for simplicity, we will omit the subscript j for the* j^{th} *element of respective variables' sets (* $r_{0j}, q_j, r_j, w_j, hq_j, \theta_{1j}, \theta_{2j}, Q\theta_j, W_j, W_{1j}, Q_j, X_{1j}, X_{2j}, sr_j, srh_j, hm_j, hw_j, Y_j, P_{1j}, P_{2j}, hrs_j, hwr_j$*), for j=1 to n. */*

$X_1 = (q-1)\left(S_j\right)_A, \qquad X_2 = (1 + \frac{3r}{q-1}(S_j^{-1})_A),$

$W = QW_1 + Qr$

$Q = H(m, r_1, (S_j\theta_n)_A, X_1, X_2),$

$= Q(q * (S_j)_A + 2r),$

$hw = H(W, r, (S_j)_A), \qquad hrs = H(\mathrm{r}_0, (S_j\theta_n)_A),$

$hwr = H(W, hrs), \qquad QX_1X_2 = Q((q-1)(S_j)_A) + 3Qr,$

$sr = (S_j)_A + r, \qquad srh = sr + H(hw, QX_1X_2),$

$Y = W - QX_1X_2 - 2(S_j)_A - r - H(hw, QX_1X_2)$

$= W - QX_1X_2 - (S_j)_A - srh,$

$P_1 = (q-2)r(S_j)_A, \qquad P_2 = r^{-1}(1 + \frac{2r - Htot}{q-2}(S_j^{-1})_A),$

$Htot = H(m, \mathrm{r}_0, hq, Q, X_1, X_2, P_1, Y, hw, sr, hrs, hwr),$

$hm = H(m, \mathrm{r}_0, hq, Q, X_1, X_2, \mathrm{Y}, P_1, P_2, \mathrm{hw}, \mathrm{sr}, \mathrm{hrs}, \mathrm{hwr}).$

3. The generated quantum signature $|Sig\rangle_A$ = Rotates tensor product of n qubits $|0_z\rangle$, the states $|0_z\rangle^{\otimes n}$, *to* $\bigotimes_{j=1}^{n} \mathrm{R}^{(j)}(\mathrm{W} + \mathrm{hm})_j\theta_n|0_z\rangle$.

4. Sends { m, r_0, hq, Q, X_1, X_2, Y, P_1, P_2, hw, sr, hrs, hwr } through a classical

channel, and $|Sig\rangle_A$ through a quantum channel, to the verifier B.

(c) Verification phase

Upon receiving $\{ m, \mathrm{r}_0, hq, Q, X_1, X_2, \mathrm{Y}, P_1, P_2, \mathrm{hw}, \mathrm{sr}, \mathrm{hrs}, \mathrm{hwr}, |Sig\rangle_A \}$, verifier B performs the verification operation by using the following steps.

1. Computes

$hm = H(m, \mathrm{r}_0, hq, Q, X_1, X_2, \mathrm{Y}, P_1, P_2, \mathrm{hw}, \mathrm{sr}, \mathrm{hrs}, \mathrm{hwr})$,

$Htot = H(m, \mathrm{r}_0, hq, Q, X_1, X_2, \mathrm{Y}, P_1, P_2, \mathrm{hw}, \mathrm{sr}, \mathrm{hrs}, \mathrm{hwr})$,

$srh = sr + H(hw, QX_1X_2)$, *H(Y), and* $QX_1X_2, H(srh + QX_1X_2 + Y, hrs)$.

2. Compares to see if $hwr = H(srh + QX_1X_2 + Y, hrs)$, if the equation doesn't hold, continues; else, rejects.

3. Computes and compares to see if $(X_1X_2 - P_1P_2) = \mathrm{sr} + Htot$, if the equation holds, continues; else, rejects.

4. If $H(Y) < Y$, computes $\theta_1 = Y - H(Y)$, $Q\theta = hm + srh + QX_1X_2 + \theta_1$, else computes $\theta_2 = H(Y) - Y$, $Q\theta = hm + srh + QX_1X_2 - \theta_2$.

5. Performs inverse rotation operation $\mathrm{R}^{(\mathrm{j})}(\mathrm{Q}\theta)$ on $|Sig\rangle_A$, obtaining $|\mathrm{Z}\rangle$.

6. Performs rotation operation $\mathrm{R}^{(\mathrm{j})}\mathrm{H}(\mathrm{Y})$ on $|\varphi_{\mathrm{pk}}\rangle_{\mathrm{A}}$, obtaining $|\mathrm{Z}'\rangle$.

7. Measures both states $|\mathrm{Z}\rangle$ and $|\mathrm{Z}'\rangle$, and compares the outcomes to see if they are equal. If so, B accepts; otherwise, he rejects.

2.2. A publicly verifiable quantum blind signature scheme without entanglement based on asymmetric cryptography [14]

Their signature scheme contains five phases: (a) initial stage, (b) blind signature phase, (c) verification blind signature phase, (d) unblinding phase, and (e) verification phase. We describe them as follows:

(a) Initial stage

Signer A randomly picks, a random number set r_1 with order n and prepares a message m, then calculates $\mathrm{M_{Aj}} = \mathrm{r_{1j}} + \mathrm{S_{Aj}} + \mathrm{H(m)}$, $sh_{Aj} = \mathrm{H}(M_{Aj}, S_{Aj})$, $SM_{Aj} = M_{Aj} + sh_{Aj}$ for j=1 to n. A then passes SM_A and sh_A to B, for B to blindly sign on the blind message M_A.

(b) Blind signature generation phase

After receiving the blind messages SM_A and sh_A from A, B performs the following steps to do the blind signature phase.

1. Calculates $M_{Aj} = SM_{Aj} - sh_{Aj}$

2. Randomly picks a random number set r_2 with order n,

Calculates $H(M_{Aj}, r_{2j}) = W_{1j} = q_j S_{Bj} + r_j$,

/* For abbreviation, we omit the subscript j in the following computations*/

$X_1 = (q-2)(M_A)S_j,$ $X_2 = (\theta_n + r(q-2)^{-1}S_j^{-1}),$

$Q = H(M_A, S_B, M_A, X_1, X_2),$ $X_1X_2 = (q-2)M_A(S_j\theta_n)_B + rM_A,$

$QX_1X_2 = QM_A((q-2)(S_j\theta_n)_B + r),$ $W = (QW_1 + 2Qr)M_A + (S_j\theta_n)_B,$

$Y_B = W - QX_1X_2 - (S_j\theta_n)_B,$ $K = 2Q(S_B + r)$

$W = W + M_A$

3. Performs a rotation operation $\hat{R}^{(j)}(W_j)$ on $|\varphi_{pkj}\rangle_A$, where $j = 1$ to n, obtaining $|Z\rangle_B$.

4. If $H = (Y_B) < Y_B$

Case 1: Computes $a_1 = Y_B - H(Y_B), a = -a_1,\ Qa = -QX_1X_2 + a$

Else

Case 2: Computes $a = H(Y_B) - Y_B, a = +a_1,\ Qa = -QX_1X_2 + a$

5. Computes $P_1 = H(sh_A, H(M_A, S_B, Y_B, K, a, sh_A),\ M_A, H(Y_B), K, a)$, $Ba = P_1 + Qa + M_A$

6. Performs ro $\hat{R}^{(j)}(Ba_j\theta_n)$ on $|Z\rangle_B$, obtaining $|BSig\rangle_B$.

7. Transfers $\{M_A, SM_A, H(Y_B), H(M_A, S_B, Y_B, K, a, sh_A), H(P_1), K, a, |BSig\rangle_B\}$ to A for unblinding.

8. Transmits $\{ID_A, M_A, Y_B\}$ to T's storage for preserving the traceability. Here, T represents a trusted third party.

(c) Blind signature verification phase

After receiving the message $\{M_A, SM_A, H(Y_B), H(M_A, S_B, Y_B, K, a, sh_A), H(P_1), K, a, |BSig\rangle_B\}$ from B, A performs the following unblinding steps.

1. Calculates $M'_A = SM_A - H(M_A, \mathrm{S_A})$ and compare to see if M'_A equals to M_A. If yes, continues with the following steps; otherwise, rejects.

2. Computes $\mathrm{P}'_1 = \mathrm{H}(\mathrm{H}(\mathrm{M_A}, \mathrm{S_A}), \mathrm{H}(\mathrm{M_A}, \mathrm{S_B}, \mathrm{Y_B}, \mathrm{K}, a, \mathrm{sh_A}), \mathrm{M_A}, \mathrm{H}(\mathrm{Y_B}), \mathrm{K}, a)$, if $\mathrm{H}(\mathrm{P}'_1) = \mathrm{H}(\mathrm{P}_1)$, continues; else, rejects.

3. Computes $\mathrm{Va} = \mathrm{H}(\mathrm{Y_B}) + \mathrm{P}_1 + \mathrm{S_A} + \mathrm{M_A}$

4. Performs ro $\widehat{\mathrm{R}}^{(\mathrm{j})}(\mathrm{Va_j}\theta_n)$ on $|\varphi_{\mathrm{pk}}\rangle_{\mathrm{B}}$, obtaining$|\mathrm{Z}'\rangle$.

5. Measures both states $|\mathrm{BSig}\rangle_{\mathrm{B}}$ and $|\mathrm{Z}'\rangle$, compares the outcomes to see if they are equal. If they are, A accepts; otherwise, rejects.

(d) Unblinding phase

In this phase, A pre-unblind $|\mathrm{BSig}\rangle_{\mathrm{B}}$ to $|\mathrm{BSig}\rangle_{\mathrm{B}}$ with angle $(\mathrm{S_A} + \mathrm{S_B} + \mathrm{Y_B} + \mathrm{M_A})_{\mathrm{j}}\theta_n$ by using the following steps.

1. Computes $\mathrm{P}a = \mathrm{P}'_1 + a$

2. Performs rro, $\widehat{\mathrm{R}}^{(\mathrm{j})}(\mathrm{P}a_{\mathrm{j}}\,\theta_n)$ on $|\mathrm{BSig}\rangle_{\mathrm{B}}$, obtaining $|\mathrm{BSig}\rangle_{\mathrm{B}}$ with angle $(\mathrm{S_A} + \mathrm{S_B} + \mathrm{Y_B} + \mathrm{M_A})_{\mathrm{j}}\theta_n$

Subsequently, A further unblind $|\mathrm{BSig}\rangle_{\mathrm{B}}$ to $|\mathrm{uBS}\rangle_{\mathrm{B}}$ with angle $((S_A + S_B + H(m)K + P_2 + r_K + H(m))_{\mathrm{j}}\theta_n$ by performing the following steps.

3. Randomly selects r_K and computes

$Y_{A2} = (K - r_1) + 2(S_J\theta_n)_A$, $Y_{A3} = H(m)(r_1) - 2H(m)(S_J\theta_n)_A + (S_J\theta_n)_A + r_K$,

$Y_{A4} = H(M)Y_{A2} + Y_{A3}$ $P_2 = H(H(m), Y_{A2}, Y_{A3}, Y_{A4})$,

$= H(m)K + r_K + S_A$,

$t = r_1 + S_A$ $Ua = P_2 + r_K - (r_1 + S_A)(K + 1)$

Lets $Usa = S_A + S_B + Y_B - r_1K - S_Ak + P_2 + r_K + H(m)$

$= S_A + S_B + H(m)K + P_2 + r_K + H(m)$

4. Performs ro $\widehat{R}^{(j)}(Ua_j\,\theta_n)$ on $|BSig\rangle_B$, obtaining $|uBS\rangle_B$ with degree $(Usa_j\,\theta_n)$, for j=1 to n.

5. Transmits $\{H(m), Y_{A2}, Y_{A3}, |uBS\rangle_B, P_2\}$ to any verifier C.

6. Transmits $\{Y_B, H(m), |uBS\rangle_B\}$ through a secure authenticated channel to T for preserving the traceability.

(e) Verification phase

After receiving the unblinded signature message $\{H(m), Y_{A2}, Y_{A3}, |uBS\rangle_B, P_2\}$ from A, C performs the following steps to verify the unblind signature $|uBS\rangle_B$.

1. Computes $Y_{A4} = H(m)(Y_{A2}) + Y_{A3} = H(m)K + r_K(S_J\theta_n)_A$

2. Computes $P_2 = H(H(m), Y_{A2}, Y_{A3}, Y_{A4})$, $VUa = P_2 + Y_{A4} + H(m)$

3. Performs ro $\hat{R}^{(j)}(VUa_j\,\theta_n)$ on $|\varphi_{pk}\rangle_B$, obtaining $|Z'\rangle_B$

4. Compares the measure results of $|uBS\rangle_B$ and $|Z'\rangle_B$, if they are equal, accepts; otherwise, rejects.

3. The proposed scheme

In this section, we follow the protocol architectures in [1] to show the design philosophy of our scheme in Section 3.1, then delineate the system setup in Section 3.2, and the five protocols: license issuing, withdrawal, payment, deposit, and quantum money owner tracing in Section 3.3 through 3.7, respectively. Before that, we list the definitions of used notations of the proposed in Table 1.

Table 1. Notations definitions

m_T	The customer C's license secret message m_T which equals $H(ID_C \| Date \| K_{CT})$, the hash value generated by using C's identity (ID_C) concatenated with current Date, and the secret key (K_{CT}) shared between C and T.
$H(m_C)$	The one-way hash value of message m_C, which is to be blindly signed by the bank B.
$\|Sig\rangle_T$	The quantum state represents T's signature, which has n qubits in length, and its j^{th} qubit equals that T performs rotation $\hat{R}^{(j)}(W + hm)_j\theta_n$ on $\|0_z\rangle$, where W, hm are the midway sets of calculated values, with each set containing n numbers in the finite Galois field GF(2^n).
LST	a License Secret Token
M_c	M_C is the set of m's blind hash messages with each element j in the form $M_{Cj} = r_{1j} + S_{Cj} + H(m_C)$, where r_{1j}, S_{Cj} represent the j^{th} element in random number set r_1 and C's secret set S_C, respectively.
CNO	a selected random number for withdrawed quantum money
Value	the amount of money withdrawed
$\|BSig\rangle_B$	The quantum state represents B's blind signature, which has n qubits in length and its j^{th} qubit angle equals to the one that B performs rotation $\hat{R}^{(j)}(W + Ba + M_C)_j\theta_n$ on $\|\varphi_{pk}\rangle_{Cj}$.
$\|uBS\rangle_B$	The quantum state represents B's unblind signature, which is the result of C's performing rro $\hat{R}^{(j)}(P_1 + a + (K+1)(r_1 + S_C) - P_2 - r_k)_j\theta_n$ on $\|BSig\rangle_B$, Where P_1, a, r_1K, P_2, r_k are the intermediate set of calculated values, with each set containing n numbers in the finite Galois field GF(2^n).

$Y_{A2}, Y_{A3,} P_2$	The intermediate sets with each having n elements in the finite Galois field GF(2^n)
Y_B	Y_B is the set of intermediate messages with each element in the form $Y_B = W - QX_1X_2 - (S_j\theta_n)_B$, which is used as one of the trace message stored in T's storage.

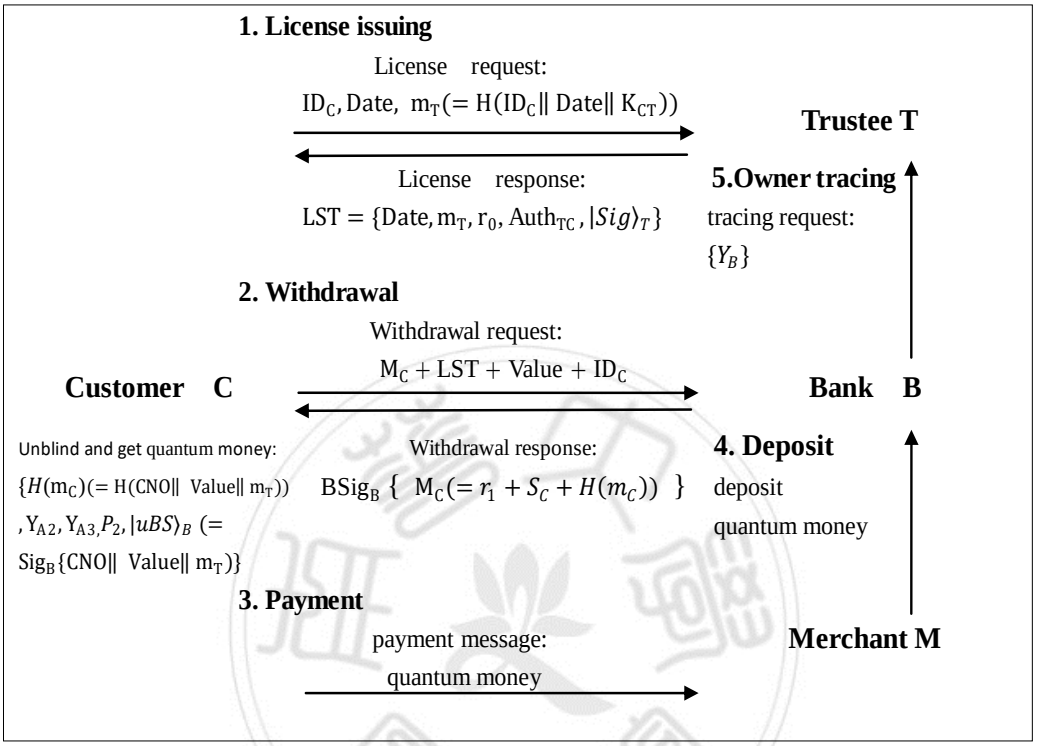

Fig. 1. Outline of proposed scheme.

3.1. Design philosophy

Fig. 1 outlines the design philosophy of our scheme. For simplicity, we omit session key encryption in the message flows, as it can be implemented by using BB84 protocol [22] to negotiate a session key for encrypting the message transmitted; for example, the encryption on the withdrawal request. Our scheme contains five protocols: (a) license issuing, (b) withdrawal, (c) payment, (d) deposit, and (e) owner tracing. It has four roles Customer C, Trustee T, Bank B, and Merchant M. For emphasis, we first

briefly describe three of the protocols below. They are license issuing, withdrawal protocol, and owner tracing, as shown in Section 3.1.1 through 3.1.3, respectively.

3.1.1. License issuing

The license issued in this protocol mainly consists of two parts: (1) the license secret message (m_T) which equals $H(ID_C \| Date \| K_{CT})$, the hash value generated by using C's identity (ID_C) concatenated with current Date, and the secret key K_{CT} shared between C and T, (2) $|Sig\rangle_T$ which is to be verified by B when C uses it in the withdrawal protocol.

3.1.2. Withdrawal protocol

This protocol allows C to withdraw quantum money $\{H(m_C)(= H(CNO \| Value \| m_T)), Y_{A2}, Y_{A3}, P_2, |uBS\rangle_B (= Sig_B\{CNO \| Value \| m_T\})$, where $m_C = CNO \| Value \| m_T$ and $m_T = H(ID_C \| Date \| K_{CT})$ form bank B. C randomly picks a number set r_1 to compute $M_{Cj} = r_{1j} + S_{Cj} + H(m_C)$. Then, transmits M_C together with LST, Value, ID_C to bank B. B then blindly signs on M_C, obtaining $|BSig\rangle_B$. After that, $|BSig\rangle_B$ is passed back to C for her unblinding, obtaining $|uBS\rangle_B$, which is B's signature on the concatenations of CNO, Value, and m_T; i.e., $Sig_B\{CNO \| Value \| m_T\}$, as shown in Fig. 1. Here, we do not want B to know what m_C is, because if this happens, B can link the quantum money to ID_C, this violates the money anonymity.

3.1.3. Owner tracing

When any quantum money misuse occurs, B can ask trustee T for revealing C's identity by referring to his database. Prior to this, B should send C's identity (ID_C), $M_C\,(=r_1+S_C+H(m_C))$ and the intermediate process parameters Y_B, $H(m_C)$, $|uBS\rangle_B$, to T's storage in the final stages of both B's blind signature phase and C's unblinding phase, so that when a dispute occurs, the owner can be traced. Here, $\mathrm{M_C}$ stands for $\mathrm{M_A}$ in the original scheme [13].

After outlined the design philosophy, below we show the complete proposed in Section 3.3 through 3.7, respectively.

3.2. System set-up

As for public/ private key pair generation, we adopt the same key pair generation phase as in Kaushik et al.'s scheme〔17〕, where the system establishes a public-private key pair for each system member by preparing n-qubit states$|0_z\rangle^{\otimes n}$. Then, rotate the angle of member j's private key $S_j\theta_n$ to genetate his/ her public key $\left|\varphi_{pk}\right\rangle_j = \otimes_{j=1}^{n} R^{(j)}(S_j\theta_n)_j|0_z\rangle$. In addition, each member j prepares a secret key K_{jT} shared with T, which T stores in its database for confirming the identity of the license requesting party.

3.3. License-issuing protocol

In our scheme, before withdrawing quantum money from a bank, the customer C needs to ask trustee T for issuing him a license. The following sub-phases describe the protocol, which are also illustrated in Fig. 2.

(a) Request license phase

C sends $\{ID_C, Date, H(ID_C \| Date \| K_{CT})\}$ to T, where Date is current timestamp and $H(ID_C \| Date \| K_{CT})$ is the hash value generated by concatenating C's identity, Date, and the secret key K_{CT} shared between C and T.

(b) License issue phase

Upon receiving the message from C, T performs the following steps.

1. Checks whether ID_C is correct in T's database and Date is valid. If they are not, T rejects the request.

2. Uses ID_C and Date and shared secret key K_{CT} to compute the hash value and checks whether it is equal to the received $H(ID_C \| Date \| K_{CT})$. If it is, T believes that C is the intended party; otherwise, he rejects the request.

3. Selects a random number set r_0 and sign on $m_T = H(ID_C \| Date \| K_{CT})$ (refer to Section 2.1.(b)).

4. Computes the intermediate process parameters $\mathrm{Auth_{TC}}$= {hq, Q, X_1, X_2, Y, P_1, P_2, hw, sr, hrs, hwr}

5. The generated quantum signature $|Sig\rangle_T$ = Rotates state $|0_z\rangle^{\otimes n}$ to $\bigotimes_{j=1}^{n} \mathrm{R^{(j)}}(\mathrm{W} + \mathrm{hm})_j \theta_n |0_z\rangle$.

6. Sends LST= $\{Date,\ m_T,\ r_0,\ Auth_{TC},\ |Sig\rangle_T\}$ to C by sending C $\{Date, m_T, r_0, Auth_{TC}\}$ through a classical channel, and $|Sig\rangle_T$ through a quantum channel.

(c) License verification phase

After receiving the message from T, C computes $H(ID_C \| Date \| K_{CT})$ and checks to see whether it is equal to the received m_T. If it is, C performs the verification operation (refer to Section 2.1. (c) for more details). He measures both states $|Z_T\rangle$ and $|Z_T'\rangle$, and compares the outcomes to see if they are equal. If so, C obtains LST.

3.4. Withdrawal protocol

In this protocol, both customer C and bank B together perform the blind signature function for C to withdraw the quantum money. What follows are descriptions of the protocol, which are also illustrated in Fig. 3.

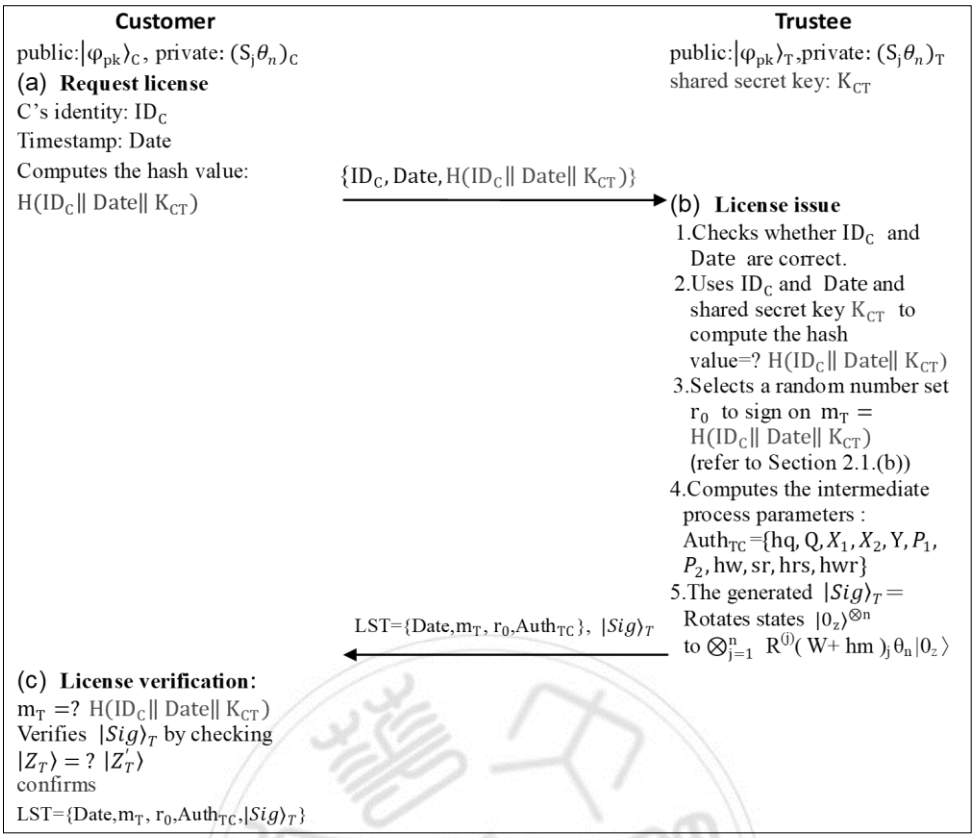

Fig. 2. License-issuing protocol.

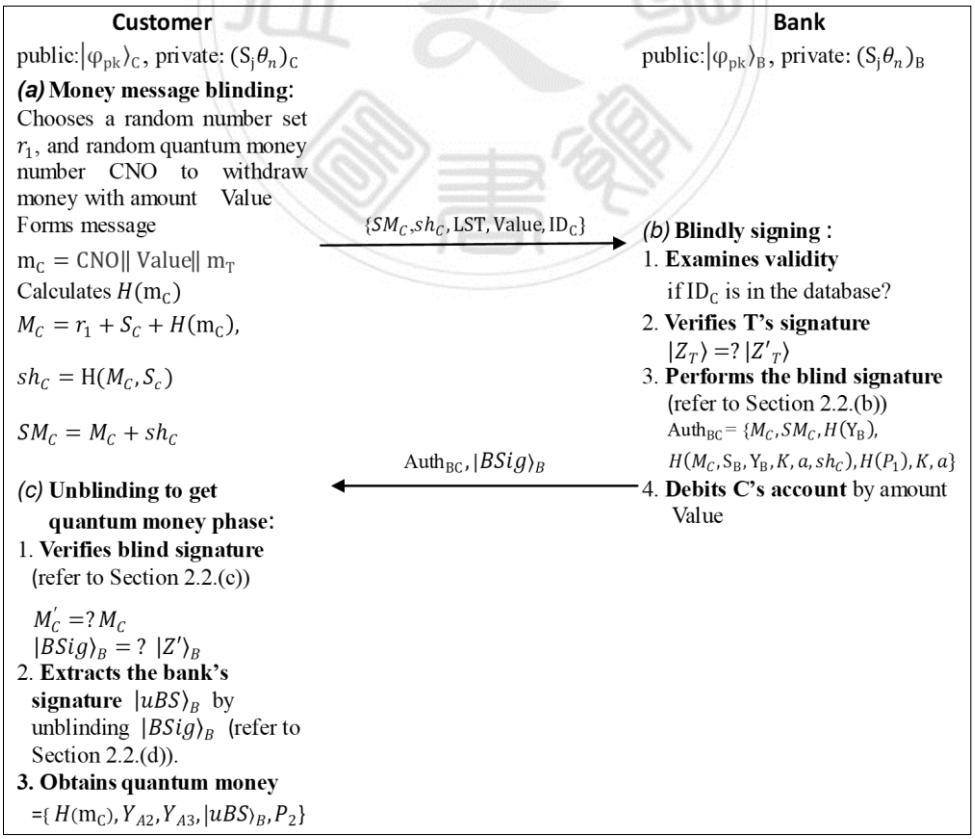

Fig. 3. Withdrawal protocol.

(a) Money message $H(\mathrm{m_C})$ blinding phase

C chooses a random number setr$_1$, arandom quantum moneynumber (CNO), and computes m_T= H (ID_C||Date||$\mathrm{K_{CT}}$) to withdraw the amount of money (Value) from the bank. He prepares message $\mathrm{m_C} = \mathrm{CNO||Value||m_T}$, and calculates $H(\mathrm{m_C})$, $M_C = r_1 + S_C + H(m_C)$, $sh_C = \mathrm{H}(M_C, S_c)$. After that he adds up $SM_C = M_C + sh_C$ and sends { SM_C, sh_C, LST, Value, $\mathrm{ID_C}$ } to B. If C wants to protect his identity, he can use BB84 protocol [22] for negotiating a session key with B to encrypt the transmission. This encryption does not affect the money anonymity.

(b) B's blindly signing phase

Upon receiving the message from C, B performs the following steps.

1. B checks whether $\mathrm{ID_C}$ is legal. If not, he rejects the request.

2. B performs the operation to verify T's signature (refer to Section 2.1.(c)). Measures both resultant states $|Z_T\rangle$ and $|Z_T'\rangle$, and comparesthe results to see if they are equal. If they are not, B rejects the request.

3. B computes $M_C = (SM_C - sh_C)$ and uses it to perform the blind signature phase (refer to Section 2.2.(b)).

4. Debits C's account by the withdrawal amount Value.

5. Transfers $\mathrm{Auth_{BC}}$={M_C, $SM_C, H(\mathrm{Y_B})$, $H(M_C, \mathrm{S_B}, \mathrm{Y_B}, K, a, sh_C)$, $H(P_1)$, K, a }and

$|\mathrm{BSig}\rangle_{\mathrm{B}}$ to C for unblinding.

6. Transmits $\{\mathrm{ID_C},\ \mathrm{M_C},\ \mathrm{Y_B}\}$ to T's storage for preserving the traceability.

(c) Unblinding to get quantum money phase

After receiving the message from B, C first uses the received AuthB to verify the blind signature , $|\mathrm{BSig}\rangle_{\mathrm{B}}$, to see whether it is correct (refer to Section 2.2. (c)). If so, he subsequently unblinds the blind signature by using the following steps (refer to Section 2.2. (d)) to get quantum money.

1. Verifiesthe blind signature by checking whether both $M_C' = M_C$ and $|BSig\rangle_B = |\mathrm{Z}'\rangle_{\mathrm{B}}$ are correct, where C obtains $|Z'\rangle_B$ by ro $\widehat{\mathrm{R}}^{(\mathrm{j})}(\mathrm{Va_j}\theta_n)$ on $\left|\psi_{pk}\right\rangle_B$.If they are, C continues.

2. Extracts the bank's signature$|uBS\rangle_B$byunblinding$|BSig\rangle_B$.

3. Obtains quantum money $\{H(\mathrm{m_C}), Y_{A2}, Y_{A3}, |uBS\rangle_B, P_2\}$, where $\mathrm{m_C}$ equals $\mathrm{CNO}\|\mathrm{Value}\|\mathrm{m_T}$.

3.5. Payment protocol

In this protocol, customer C can anonymously pay his quantum money $\{H(\mathrm{m_C}), Y_{A2}, Y_{A3}, |uBS\rangle_B, P_2\}$ to merchant M. The protocolis described as follows, which is also illustrated in Fig. 4.

(a) Quantum moneytransferring

C transmits quantum money $\{H(\mathrm{m_C}), Y_{A2}, Y_{A3}, |uBS\rangle_B, P_2\}$ to M.

(b) Quantum moneyverifying

M verifies the quantum money by checking whether $|uBS\rangle_B$ and $|Z'\rangle_B$ are equal (refer to Section2.2.(e)). If this check is correct, M accepts the payment; otherwise, he rejects.

In this protocol, the merchant does not need to know who the payer is. This makes it an anonymous payment to ensure the privacy of the buyer. Certainly, the protocol can be modified to function as a named payment if needed; for example, the customer and the merchant can perform mutual authentication ahead. The implementation can refer to Diffie-Hellman quantum session key establishment protocol [18].

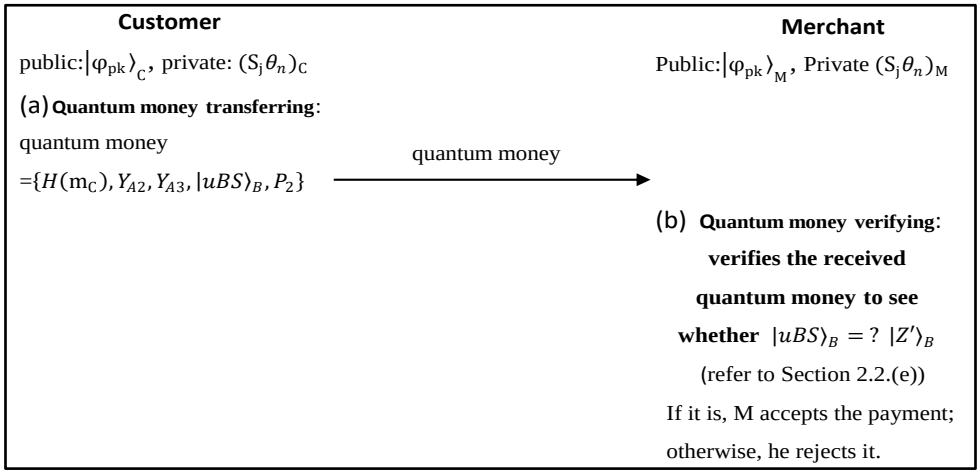

Fig. 4. Payment protocol.

3.6. Deposit protocol

In this protocol, M deposits the received quantum money to his bank account. The protocol is described as follows and illustrated in Fig. 5:

(a) Quantum money depositing:

M transmits quantum money $\{H(\mathrm{m_C}), Y_{A2}, Y_{A3}, |uBS\rangle_B, P_2\}$ together with his identity $\{\mathrm{ID_M}\}$ to B.

(b) Quantum money verifying:

B verifies the quantum money by checking whether $|\mathrm{uBS}\rangle_\mathrm{B}$ and $|\mathrm{Z}'\rangle_\mathrm{B}$ are equal. (refer to Section 2.2. (e)). If this check passes, B proceeds to examine whether the quantum money is fresh. If so, he accepts and credits M's account; otherwise, B asks trustee T for revealing the identity of the dishonest customer.

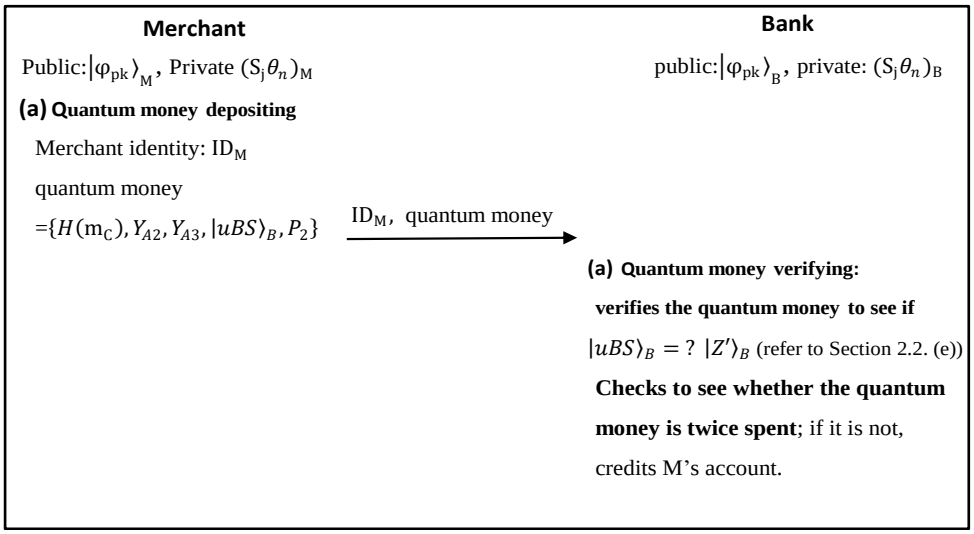

Fig. 5. Deposit protocol.

3.7. Quantum money owner tracing

In the proposed scheme, if the quantum money (=$\{H(\mathrm{m_C}), Y_{A2}, Y_{A3}, |uBS\rangle_B, P_2\}$) is spent twice or abused by a criminal, the bank or a law enforcement agency can ask trustee T to revoke the anonymity of the quantum money by providing $H(\mathrm{m_C})$ to T. Upon receiving the request, T uses $H(\mathrm{m_C})$ to find Y_B from its database to reveal the quantum money owner's identity (refer to Section 2.2(b) and 2.2(d), where B had ever sent $\{ID_C, M_C, Y_B\}$, and C sent $\{Y_B, H(\mathrm{m_C}), |uBS\rangle_B\}$ to T, respectively).

4. Security analysis

This section shows how the proposed scheme satisfies the following five security properties: unforgeability, non-repudiation, verifiability, untraceability and anonymity revocation, which a quantum money system should possess as argued in [20-21].

4.1. Unforgeability

In the payment protocol, a merchant can obtain a customer's quantum money message, $H(\mathrm{m_C})$, which might also be stolen by an adversary. If this happens, we need to know whether the adversary can launch the following two forgery cases without performing withdrawal protocol with the bank: (1) successfully forge the quantum money by only changing $H(\mathrm{m_C})$ to $H(m_C{}')$ to pass bank B's verification, or (2) use the obtained quantum money to forge another valid quantum money without performing withdrawal protocol. In either case, we show why the proposed scheme can resist the respective attack.

Case (1): Can an adversary successfully forge the quantum money by only modifying $H(\mathrm{m_C})$ without performing a withdrawal protocol to pass bank B's verification?

The following will show how this attempt fails.

In this case, assume that E only changes $H(\mathrm{m_C})$ to $H(m_C{}')$ and keeps the other parameters unchanged. This will alter P_2 (= $H(H(\mathrm{m_C}), Y_{A2}, Y_{A3}, Y_{A4})$) and Y_{A4}(=$H(\mathrm{m_C})Y_{A2} + \mathrm{Y_{A3}} = \mathrm{H(m_C)K} + \mathrm{r} + \mathrm{SA}$), because $Y'_{A4} = H(m_C{}')Y_{A2} + Y_{A3}$ and $P'_2 = H(H(m_C{}'), Y_{A2}, Y_{A3}, \mathrm{Y'_{A4}})$. E then transmits $\{H(m_C{}'), Y_{A2}, Y_{A3}, |uBS\rangle_B, P'_2\}$ to the verifier B. However, the state $|Z'\rangle_B$ that C obtains by rotating a degree on $\left|\psi_{pk}\right\rangle_B$ will not equal to $|uBS\rangle_B$ which C gets after the unblinding phase, as shown in step (4) of Section 2.2.(d), because $H(m_C{}')$ in $\mathrm{Y'_{A4}}$ is not equal to $H(\mathrm{m_C})$ in $|uBS\rangle_B$. From this, we can easily see that E cannot pass B's verification by only change $H(\mathrm{m_C})$ to $H(m_C{}')$. Therefore, E's such attack fails.

Case (2): Can an adversary use the obtained quantum money from B to forge another valid quantum money?

Under this case, assume that the adversary forges quantum money, $\{H(\mathrm{m_C}), Y_{A2}, Y_{A3}, |uBS\rangle_B, P_2\}$, without performing the withdrawal protocol. Even if the adversary can change CNO or any other parameter, he cannot pass the merchant's verification in the payment protocol. This is because E doesn't know B's secret $(S_j\theta_n)_B$ to add up with $Y'_{A4} + P'_2$ in forming $|Z'\rangle_B$. That is, E does not have the knowledge of $|Z'\rangle_B$'s angle to make the comparison of $|Z'\rangle_B$ and $|uBS\rangle_B$ equal.

Therefore, E's such attack fails. The details can be seen in Section 2.2. (e)

4.2. Non-repudiation

The bank can't deny that $|uBS\rangle_B$ is the signature he signed. This is due to the fact that when merchant M wants to verify the quantum money, he constructs the state $|Z'\rangle_B$ as shown in step (d) of Section 2.2. by rotating an angel $Y_{A4} + P_2 + \mathrm{H(m)}$ on B's quantum public key $\left|\psi_{pk}\right\rangle_B$. The result is finally measured and compared with the measurement outcome of state $|uBS\rangle_B$. Therefore, B cannot deny that he had blindly signed on the message $H(\mathrm{m_C})$. Moreover, $\mathrm{m_C}$ $(= \mathrm{CNO}\| \mathrm{Value}\| \mathrm{m_T})$ contains the random quantum money number, CNO, and C's identity $\mathrm{ID_C}$ in m_T(=H($\mathrm{ID_C}\|$ Date$\|$ $\mathrm{K_{CT}}$)), so if needed, m_T can be computed with the help of T by using $\mathrm{K_{CT}}$. Thus, C cannot deny that he has paid the quantum money that B had ever blindly signed.

4.3. Verifiability

In this section, we illustrate that both the identity of the money owner and the money it self are verifiable. That is, we will show both the LST $(= \{\mathrm{Date}, \mathrm{m_T}, \mathrm{r}, \mathrm{Auth_{TC}}, |\mathrm{Sig}\rangle_\mathrm{T}\})$ and quantum money $(= \{\mathrm{H(m_C)}, \mathrm{Y_{A2}}, \mathrm{Y_{A3}}, |\mathrm{uBS}\rangle_\mathrm{B}, \mathrm{P_2}\})$ are verifiable in the proposed scheme. Firstly, when customer C wants to withdraw

quantum money, he sends LST to the bank, B can then verify T's signature $|Sig\rangle_T$ by using T's quantum public key $|\psi_{pk}\rangle_T$ (refer to Section 2.1.(c)). Secondly, when customer C wants to pay quantum money to the merchant, M can verify that $|uBS\rangle_B$ is B's valid signature on $H(\mathrm{m_C})$ by ro $\hat{R}^{(j)}(H(\mathrm{m_C})Y_{A2} + Y_{A3} + H(\mathrm{m_C}) + P_2)$ on B's quantum public key $|\psi_{pk}\rangle_B$ (refer to Section 2.2.(e)). Thus, the quantum money is verifiable**.**

4.4. Untraceability

Our quantum money is untraceable. The two reasons given below demonstrate why the proposed scheme possesses untraceability.

Reason 1:

In the withdrawal protocol, when customer C wants to withdraw quantum money from B, he must provide the bank with his identity, $\mathrm{ID_C}$, LST, and the blind quantum money number CNO in $\mathrm{M_C}$ (=$(SM_C - sh_C)$=$r_1 + S_C + H(\mathrm{m_C})$). Although the bank knows the customer's identity, it has no knowledge of either CNO or $\mathrm{m_T}$, because they both are hashed in $\mathrm{H(m_C)}$ (=$H(CNO\|\ \mathrm{Value}\|\ \mathrm{m_T})$) by using an unconditionally secure one-way hash function [19]. After authenticated the customer's identity, the bank blindly signs on $H(\mathrm{m_C})$, and outputs ablind signature state, $|\mathrm{BSig}\rangle_\mathrm{B}$, to the

customer. The customer then unblindsit by performing ro $\hat{R}^{(j)}(Ua_j\theta_n)$ on $|BSig\rangle_B$. As a result, the bank cannot link any parameter in quantum money, including $|uBS\rangle_B$, to the customer's identity.

Reason 2:

Similarly, in the payment protocol, when a merchant receives quantum money, $\{H(\mathrm{m_C}), Y_{A2}, Y_{A3}, |uBS\rangle_B, P_2\}$, from a customer, he cannot know the identity embedded in the $H(\mathrm{m_C})$ because $H(\mathrm{m_C})$ $(= H(CNO\| \mathrm{Value}\| \mathrm{m_T})$) and $\mathrm{m_T}$ (=$\mathrm{H(ID_C\|Date\|K_{CT})}$) is a one-way hash function value. Hence, anyone who learns $H(\mathrm{m_C})$ cannot obtain any useful information about the owner's identity due to the one-way property of the hash function.

4.5. Anonymity revocation

Anonymity revocation means revealing the owner's identity embedded in quantum money when a double spending happens. In Section 3.7, we have already illustrated how the proposed includes this anonymity revocation mechanism.

5. Comparisons

In this section, we compare our scheme with the literature [8, 9, 10, 11, 12, 25] and list the results in Table 2. We found only the proposed can satisfy the five quantum money security features, unforgeability, non-repudiation, verifiability, untraceability and anonymity revocation, which a quantum money system should possess as argued in [20-21].

Table 2. Comparison results with the literature

Schemes	Disadvantage
[8]	Q
[9]	Q
[10]	Q
[11]	T
[12]	Q
[25]	U
The proposed	None

Q: traditional signature verification, not quantum level security

U: Undeterministic Money verification

T: Money owner traceable

6. Conclusion

In this article, we proposed a quantum money scheme based on quantum public key system. Our scheme not only is concise and simple in concept when compared with the existed schemes in literature, but also is verifiable by anyone, which greatly enhances the transaction efficiency in the commercial world. After cryptanalysis, we confirmed that our scheme possesses the four needed properties, unforgeability, on-repudiation, verifiability, and untraceability, as required in a typical quantum money system. We have proven its security. Thus, our quantum money is practical and easy to be applied worldwide in real life.

7. References

[1] Chen, Y., Chou, J. S., Sun, H. M., & Cho, M. H. (2011). A novel electronic cash system with trustee-based anonymity revocation from pairing. Electronic Commerce Research and Applications, 10(6), 673-682.

[2] Chen, X., Zhang, F., & Liu, S. (2007). ID-based restrictive partially blind signatures and applications. Journal of Systems and Software, 80(2), 164-171.

[3] Eslami, Z., & Talebi, M. (2011). A new untraceable off-line electronic cash system. Electronic Commerce Research and Applications, 10(1), 59-66.

[4] Hu, X., & Huang, S. (2008). Analysis of ID-based restrictive partially blind signatures and applications. Journal of Systems and Software, 81(11), 1951-1954.

[5] Busch, P., Heinonen, T., & Lahti, P. (2007). Heisenberg's uncertainty principle. Physics Reports, 452(6), 155-176.

[6] Wootters, W. K., & Zurek, W. H. (2009). The no-cloning theorem. Physics Today, 62(2), 76-77.

[7] Wiesner, S. (1983). Conjugate coding. ACM Sigact News, 15(1), 78-88.

[8] Gavinsky, D. (2012, June). Quantum money with classical verification. In 2012 IEEE 27th Conference on Computational Complexity (pp. 42-52). IEEE.

[9] Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., & Shor, P. (2012, January). Quantum money from knots. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (pp. 276-289).

[10] Ben-David, S., & Sattath, O. (2016). Quantum tokens for digital signatures. arXiv preprint arXiv:1609.09047.

[11] Ikeda, K. (2018, July). qBitcoin: a peer-to-peer quantum cash system. In Science and Information Conference (pp. 763-771). Springer, Cham.

[12] Jogenfors, J. (2019, May). Quantum Bitcoin: An Anonymous, Distributed, and Secure Currency Secured by the No-Cloning Theorem of Quantum Mechanics. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 245-252). IEEE.

[13] Chen, Y., Chou, J. S., Zhou, F. Q., & Wang, C. L. (2019). A publicly verifiable quantum signature scheme based on asymmetric quantum cryptography. IACR Cryptology ePrint Archive, 2019, 24.

[14] Chen, Y., Chou, J. S., Wang, L. C., & Chou, Y. Y. A publicly verifiable quantum blind signature scheme without entanglement based on asymmetric cryptography.

[15] Stallings, W. (2006). Cryptography and network security, 4/E. Pearson Education India.

[16] Xu, R., Huang, L., Yang, W., & He, L. (2011). Quantum group blind signature scheme without entanglement. Optics Communications, 284(14), 3654-3658.

[17] Bennett, C. H., & Brassard, G. (2020). Quantum cryptography: Public key distribution and coin tossing. arXiv preprint arXiv:2003.06557.

[18] Chen, Y., Hsiang, C., Wang, L. C., Chou, Y. Y., & Chou, J. S. A Diffie-Hellman quantum session key establishment protocol without entanglement.

[19] Zeng, G. (2010). *Quantum private communication*. Springer Publishing Company, Incorporated.

[20] Aaronson, S., Farhi, E., Gosset, D., Hassidim, A., Kelner, J., & Lutomirski, A. (2012). Quantum money. Communications of the ACM, 55(8), 84-92.

[21] Lutomirski, A., Aaronson, S., Farhi, E., Gosset, D., Hassidim, A., Kelner, J., & Shor, P. (2009). Breaking and making quantum money: toward a new quantum cryptographic protocol. arXiv preprint arXiv:0912.3825.

[22] Sergienko, A. V. (Ed.). (2018). *Quantum communications and cryptography*. CRC press.

[23] Lvovsky, A. I. (2018). *Quantum Physics*. Quantum Physics, Undergraduate Lecture Notes in Physics. ISBN 978-3-662-56582-7. Springer-Verlag GmbH Germany, part of Springer Nature, 2018.

[24] Zygelman, B. (2018). *A First Introduction to Quantum Computing and Information* (pp. 1-233). Springer.

[25] Horodecki, K., & Stankiewicz, M. (2020). Semi-Device-Independent Quantum Money. New Journal of Physics.