How to make money with quantum mechanics

Prasanta K. Panigrahi

Indian Institute of Science Education and Research Kolkata

Outline

Introduction

- Breaking the ice

Another Look at Wiesner's Money

- Attacks
- Entanglement-Assisted Wiesner

Quantum Cheques

- Expectations
- Definitions
- Preliminaries
- Quantum Cheques Scheme

Motivation

Why do we want to think about Quantum Money?

Well, classical information can always be copied!
(includes currency notes, bonds, legal documents, anything)
It's only a matter of time and resources for an adversary.

So, Quantum Mechanics Circumvent's this problem?

Yes!
No-Cloning Theorem, Holevo's Bound, Non-Destructive Comparison of states, Heisenberg's uncertainty relation, and so many more tools for doing cryptography better.

Historical Developments

Wiesner's Money

First Real Use of Quantum Cryptography!

Inspired the BB84 Protocol!

Unpublished for a really long time!!

Randomly choose a string of $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ states and encode them in the Quantum Money with a serial no s

To verify the bank measure them in the correct basis (corresponding to s, known only to bank) later and see if measurement outcomes match

Private Key, One Time Usable

Vulnerable against adaptive attacks (and many others).

Historical Developments

Quantum Coins

Proposed by Mosca and Stebila in 2009
Gives a framework of constructing quantum coins, that are indistinguishable.

Existence of Public Key Quantum Money

Yes! Relative to a Random Oracle Model.
Proved by Aaronson in 2009.
Open: is it possible to do it without the random oracle?
Also proposed a scheme, without an Random Oracle, based on random stabilizer states.
Broken by Lutomirski in a year!

Historical Developments

Money from Knots

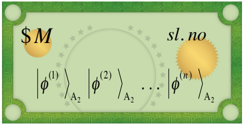
Proposed by Farhi, Gosset, Hassidim, Lutomirski, Shor in 2010
We really don't know how to analyze its security, given understanding it would require answering unsolved questions from Knot Theory

Money from Hidden Subspaces

Proposed by Aaronson and Christiano in 2012
black box security and non-black box security under plausible cryptographic assumptions
Semi-Quantum (includes classical ideas)

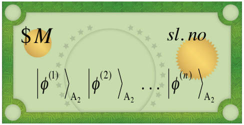
Another Look at Wiesner's Money

Wiesner Money

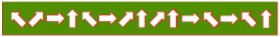

$M
sl. no
$|\phi^{(1)}\rangle_{A_2} |\phi^{(2)}\rangle_{A_2} \ldots |\phi^{(n)}\rangle_{A_2}$

$$|\phi^{(i)}\rangle \in_R \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$$

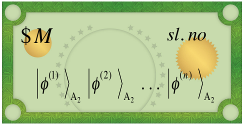
Wiesner Money

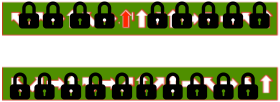

$M
sl. no
$|\phi^{(1)}\rangle_{A_2} \; |\phi^{(2)}\rangle_{A_2} \ldots |\phi^{(n)}\rangle_{A_2}$

$$|\phi^{(i)}\rangle \in_R \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$$



Wiesner Money


$\$M$
$sl.no$
$|\phi^{(1)}\rangle_{A_2}\ |\phi^{(2)}\rangle_{A_2}\ \ldots\ |\phi^{(n)}\rangle_{A_2}$



$$|\phi^{(i)}\rangle \in_R \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$$

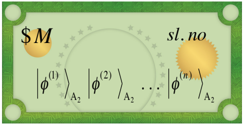
Some Attacks on Wiesner Money

Adaptive Attacks - Can learn about the states $\{0, 1, +, \}$
Quantum Zeno Attack - can to copy $\{0, 1, +, \}$
Tomography - with a single copy and strict-testing

Lutomirski, arXiv preprint arXiv:1010.0256
Molina, Vidick, and Watrous, TQC, 2012

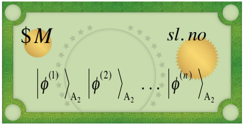
Brodutch, Nagaj, Sattath, and Unruh, arXiv:1404.1507

Entanglement-Assisted Wiesner Money


$M
sl. no
$|\phi^{(1)}\rangle_{A_2}\ |\phi^{(2)}\rangle_{A_2}\ \ldots\ |\phi^{(n)}\rangle_{A_2}$

$$|\phi^{(i)}\rangle \in_R \{|\Psi^+\rangle, |\Psi^-\rangle, |\Phi^+\rangle, |\Phi^-\rangle\}$$

Entanglement-Assisted Wiesner Money


$M
sl. no
$|\phi^{(1)}\rangle_{A_2} |\phi^{(2)}\rangle_{A_2} \ldots |\phi^{(n)}\rangle_{A_2}$

$$|\phi^{(i)}\rangle \in_R \{|\Psi^+\rangle, |\Psi^-\rangle, |\Phi^+\rangle, |\Phi^-\rangle\}$$

Minting-Money

The bank generates a random string s (the serial number) and b (secret bit string)

The bank prepares n maximally entangled qubits, $\left|\varphi_{AB}^{(i)}\right\rangle$ (chosen using b from a set of Bell states).

The bank keeps $(s, b, \left|\varphi_{A}^{(i)}\right\rangle)$ and gives out $(s, \left|\varphi_{B}^{(i)}\right\rangle)$, for each i as the money.

Verifying-Money

The money, $(s, \left|\varphi_B^{(i)}\right\rangle)$, when given to the Bank, the bank looks up $(s, b, \left|\varphi_A^{(i)}\right\rangle)$, so that it now has access to $(s, b, \left|\varphi_A^{(i)}\right\rangle, \left|\varphi_B^{(i)}\right\rangle)$

The Bank Chooses a random subset, X (of size γ) of qubits $(\left|\varphi_{AB}^{(i)}\right\rangle)$, and the puts the rest in Y, (X union Y is the set of all qubits, X intersection Y is empty)

For the qubits in X, the Bank performs a (non-destructive) bell state discrimination with $\left|\varphi_{AB}^{(i)}\right\rangle$. If they agree' with b, the bank declares the money to be Valid, otherwise, Invalid.

For the qubits in Y, the Bank uses two sources of randomness R_1, R_2, and simulates the CHSH game with them. If the fraction of qubit pairs that win the game is less than $(cos^2\pi/8) * |Y|$, then abort the protocol, else

the bank replaces the qubits in Y with the corresponding Bell States according to b, and return the money in the world.

Security Proof (idea)

- Eve cannot share correlation with the Bank's qubits (monogamy)
- Cannot clone! (No cloning, violate monogamy)
- Aspiring criminal cannot (probabilistically) determine the bell state, given only a single copy of the states. (Bell state discrimination under LOCC implies creating entanglement with LOCC, i.e. impossible, hence cannot modify a currency $ to $
- The money works even after the n-th transaction. (parallel repetitive games)

Advantages

- Better Security Properties
- All previously attacks against Wiesner don't work here
- Notion for Device Independence.

Quantum Cheques

Expectations

A cheque is expected to have the following properties

- A trusted bank or any of its (semi-trusted) branches must be able to verify the authenticity of a cheque.
- An issuer, after issuing a cheque, must not be able to disavow issuing it.
- No adversary must be able to counterfeit a cheque under some issuer's name or use a cheque more than once to withdraw money.

Definitions

Informally, a Quantum Cheque Scheme consists of three algorithms,

- KeyGen, which takes as input a security parameter and probabilistically generates a 'cheque book' and key for the issuer.
- Sign, which takes as input the issuer's key and amount to be signed, and produces a quantum state χ called a Cheque.
- Verify, which takes in as input the key, and the alleged cheque χ and decides its (in)validity.

Properties

The Scheme is said to have a completeness error ϵ, if $\forall$ valid cheques χ,

$$Pr\left[Verify(\chi)\ accepts\right] \geq 1-\epsilon,$$

The Scheme is said to have a soundness error δ, if $\forall$ counterfeiters $\mathcal{C}$,

$$Pr\left[X' \setminus X \neq \varnothing : X' \leftarrow \mathcal{C}(X)\right] \leq \delta,$$

where $X = \{\chi_1, \chi_2, \cdots, \chi_q\}$, $\mathcal{C}$ is a counterfeiter that Counterfeits a cheque (formally defined later) that outputs $X' = \{\chi'_1, \chi'_2, \cdots, \chi'_{q'}\}$, that *Verify* accepts, and $\varnothing$ denotes an empty set.

Quantum One Way Functions

A quantum one way function is defined as,

$$\Psi : k \times |0\rangle^{\otimes n} \rightarrow |\psi_k\rangle \,,$$

where $k \in \{0,1\}^*$ and $|\psi_k\rangle$ is a $n-$qubit quantum state, such that,

- Ψ is easy to compute, i.e., there exists a polynomial-time algorithm that can evaluate $\Psi(k, |0\rangle^{\otimes n})$ and outputs $|\psi_k\rangle$,
- Ψ is hard to invert, i.e., given $|\psi_k\rangle$, it is difficult to compute k

Quantum One Way Functions : Continued

Note: This can be done in agreement with Holevo's Theorem, which limits the amount of classical information that can be extracted from a quantum state

For a binary string, k, of length L, and C copies of $|\psi_k\rangle$, one can only learn almost Cn bits of information. By having $L >> Cn$, one could achieve a one way function, that is impossible to invert.

The distance between two qubit states $|\phi\rangle$ and $|\phi'\rangle$ is defined as $\sqrt{1 - |\langle\phi|\phi'\rangle|^2}$.

Using volumetric analysis, it may be seen that there exists n qubit states $\{|\phi_k\rangle^{\otimes n}\}$, such that $\left\langle {\phi_k}^{\otimes n} | {\phi_{k'}}^{\otimes n} \right\rangle \leq \delta$ for $k \neq k'$. Buhrman et al., showed for $\delta = 0.9$, the size of the set can be $2^{O(2^n)}$.

but,

Swap Test

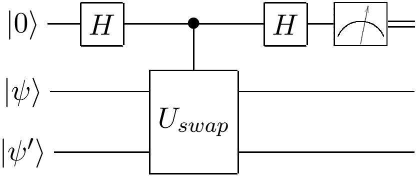


Figure: The Fredkin Gate that compares quantum states ψ and ψ', (non-destructively, if $\psi = \psi'$) with an additional ancilla qubit

The optics community uses a Multiport to realize a Fredkin Gate

Digital Signature Scheme

A digital signature scheme, Π, is a 6-tuple $(M, \Sigma, U, Gen, Sign, Vrfy)$, where,

- M is the finite set of valid messages, Σ is the finite set of valid signatures, and U is the finite set of users.
- The key-generation algorithm, Gen, takes in a security parameter 1^k, and outputs the $Sign, Vrfy$ algorithms and the public parameters.
- The signing algorithm, $Sign$, is a mapping, $Sign : M \times U \to \Sigma$
- The verification algorithm, $Vrfy$, is a mapping, $Vrfy : M \times \Sigma \times U \to \{True, False\}$.

Informally, a digital signature scheme, Π, must satisfy the following security conditions

1. Unforgeability: Except with a negligible (under a polynomial factor) probability, it should be impossible for an adversary to produce a valid signature
2. Non-repudiation: Except with a negligible (under a polynomial factor) probability, the signer should not be able disavow a legitimate signature.

Alice (with an unique *id*) and the Bank create a shared key k

Alice and the Bank agree on a digital signature scheme Π, and Alice declares her public key, pk

Bank Prepares a string of GHZ states

$$\left|\phi^{(i)}\right\rangle_{GHZ} = \frac{1}{\sqrt{2}} \left(\left|0^{(i)}\right\rangle_{A_1} \left|0^{(i)}\right\rangle_{A_2} \left|0^{(i)}\right\rangle_{B} + \left|1^{(i)}\right\rangle_{A_1} \left|1^{(i)}\right\rangle_{A_2} \left|1^{(i)}\right\rangle_{B} \right)$$

for $i = 1$ to $l(n)$, where $l(n)$ is the security parameter

The Bank gives 2 of 3 qubits from each GHZ state to Alice, that she later uses as the cheque book

Alice now holds $(id, pk, sk, s, k, \{\left|\phi^{(i)}\right\rangle_{A_1}, \left|\phi^{(i)}\right\rangle_{A_2}\}_{i=1:l})$

and the Bank holds $(id, pk, s, k, \{\left|\phi^{(i)}\right\rangle_{B}\}_{i=1:l})$,

Sign

To Sign a cheque worth amount M, Alice generates a random number $r \leftarrow U_{\{0,1\}^L}$

Alice prepares l states $\{\left|\psi_M^{(i)}\right\rangle\}_{i=1:l}$ corresponding to the amount M using the one way function $g : \{0,1\}^* \times |0\rangle \rightarrow |\psi\rangle$, as $\{\left|\psi_M^{(i)}\right\rangle = g(M||r||i)\}_{i=1:l}$.

At this point Abby, if wishes to, can optionally, also verify the states $\{\left|\psi_M^{(i)}\right\rangle\}_{i=1:l}$, by computing $\{\left|\psi_M^{,(i)}\right\rangle\}_{i=1:l} = \{g(M||r||i)\}_{i=1:l}$ and performing a non-destructive swap test using a Fredkin Gate.

Sign: cont'd

To create the cheque, Alice uses one of her entangled qubits, $\left|\phi^{(i)}\right\rangle_{A_1}$, (with serial number s) to encode $\left|\psi_M^{(i)}\right\rangle$ and performs a bell measurement and does a necessary error correction in $\left|\phi^{(i)}\right\rangle_{A_2}$
Alice also signs the serial number s as $\sigma \leftarrow Sign_{sk}(s)$.
Alice finally produces a Quantum Cheque

$$\chi = (id, s, r, \sigma, M, \{\left|\phi^{(i)}\right\rangle_{A_2}\}_{i=1:l})$$

and gives it to Abby.

Verify

Abby when produces the Quantum Cheque $\chi = (id, s, r, \sigma, M, \{\left|\phi^{(i)}\right\rangle_{A_2}\}_{i=1:l})$ at any of the valid branches of the bank

The branch communicates (securely) with the Bank's main branch, and checks the validity of the (id, s) pair and runs a verification using $Vrfy_{pk}(\sigma, s)$. If (id, s) and σ is invalid, the branch destroys the cheque and aborts. Else, the respective branch continues with the verification.

The main branch now performs a measurement, in the Hadamard basis, on its copy of $\left|\phi^{(i)}\right\rangle_B$, to obtain outcomes $|+\rangle$ or $|-\rangle$ and communicates (securely) the results via a classical channel to the appropriate Branch.

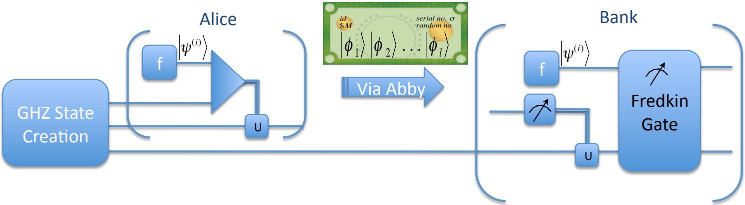
Based on the outcome, the Branch performs the suitable Pauli Matrix (for error correction) on $\left|\phi^{(i)}\right\rangle_{A_2}$, to recover $\left|\psi_M^{(i)}\right\rangle$.

This is done l times for each of $\{\left|\phi^{(i)}\right\rangle_{A_2}\}_{i=1:l}$, to recover $\{\left|\psi_M^{(i)}\right\rangle\}_{i=1:l}$.

Verify:cont'd

The Bank (or branch) accepts the cheque if the swap tests pass, i.e., if $\{\left\langle \psi_M^{(i)} | \psi_M^{,(i)} \right\rangle \geq \kappa\}_{i=1:l}$, where κ is the thresholding constant, that serve as security parameters determined by the bank. The Branch rejects and aborts the transaction otherwise, and also destroys the cheque.

Schematic Diagram



Thanks for your attention

Joint work with Subhayan Roy Moulick, IISER-K
Entanglement Assisted Wiesner: in-preparation
Quantum Cheques: arXiv:1505.05251