
# QUANTUM MONEY (& FRIENDS)

OR SATTATH

Ben-Gurion University of the Negev

# QUANTUM MONEY

- “Money that it is physically impossible to counterfeit”.

  Wiesner, ~1969

# REQUIREMENTS FROM MONEY

- It is easy for the bank to generate money
- It is easy to verify the money
- It is impossible / hard  to forge money by anyone other than the bank
  - Classical material and information, in principle, can be copied.
  - Gold, for example, has been synthesized [Miethe'1924], and no law-of-nature says that it must be expensive to do so.  Scarcity is hard to enforce.
- Unlike bits, qubits cannot be copied, by the no cloning theorem.

# PRIVATE VS. PUBLIC QUANTUM MONEY

## Private

- Only the bank can verify (using its secret key)
- Applications: bus tickets
- No need for a universal quantum computer
- Unconditional (information theoretic) security

## Public

- Everyone can verify (using the bank's public key)
- Like our current bills and coins
- Requires a universal quantum computer
- Computational security

# PRIVATE QUANTUM MONEY

- Consists of three quantum poly-time algorithms
  - $\mathrm{sk} \leftarrow Key - Gen(1^{\kappa})$
  - $|\$\rangle \leftarrow Mint_{sk}$
  - $Verify_{sk}(|\psi\rangle)$ which accepts or rejects
- Correctness: $Verify$ should accept valid money

# PUBLIC QUANTUM MONEY

- Consists of three quantum poly-time algorithms
  - $(\mathrm{sk}, \mathrm{pk}) \leftarrow Key - Gen(1^{\kappa})$
  - $|\$\rangle \leftarrow Mint_{sk}$
  - $Verify_{pk}(|\psi\rangle)$ which accepts or rejects
- Correctness: $Verify$ should accept valid money

# SECURITY DEFINITION: 1ST ATTEMPT

Negligible: decreases faster than $1/poly(\kappa)$

*For every quantum poly-time adversary $\mathcal{A}dv$:*

$$\Pr(Verify(\mathcal{A}dv(1^{\kappa}, pk) = T) \leq negl(\kappa)$$

This means no money from thin air.
This does not rule out the possibility for the adversary to turn one dollar into two dollars.

# SECURITY DEFINITION: 2ND ATTEMPT

*For every quantum poly-time adversary $\mathcal{Adv}$:*

$$\Pr(Verify^2(\mathcal{Adv}(1^\kappa, pk, |\$_1\rangle))) \leq negl(\kappa)$$

This does not rule out the possibility for the adversary to turn two dollars into three.

# SECURITY DEFINITION: 3RD ATTEMPT

*For every quantum poly-time adversary $\mathcal{Adv}$ and n:*

$$\Pr(Verify^{n+1}(\mathcal{Adv}(1^\kappa, pk, |\$_1\rangle \otimes |\$_2\rangle \otimes \cdots \otimes |\$_n\rangle))) \leq negl(\kappa)$$

A cryptographer's thermodynamic law

# ANOTHER SECURITY REQUIREMENT

- An attacker might be able to change the money so that it will fail verification the second time.
- Store 1 attack store 2:
  - Store 1 tweak their quantum money state so that it will pass verification the first time, and fail verification the second time.
  - Store 1 goes to store 2, and use the tweaked money to buy merchandise from store 2.
  - Store 2 verifies the money, and the verification passes.
  - Store 2 tries to pay with the money received from store 1. This is the second time the money is verified, and it fails.
- To fix this, we additionally require that verification is a projector: if money passes verification, it will continue to do so.[Ben-David–S'16]

# PRIVATE QUANTUM MONEY

# WIESNER'S SCHEME

- Uses the following 4 1-qubit states (sometimes called BB84 states): $|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- For each serial number $i$, the bank mints a state of the form $(\mathrm{i}, |-\rangle \otimes |1\rangle \otimes |1\rangle \otimes |+\rangle \otimes |-\rangle \otimes |0\rangle)$
- The bank maintains a classical database. For example, the $\mathrm{i}^{\mathrm{th}}$ entry is the string -11+-0.
- Verification is done by projection onto the correct state.

# OPTIMAL COUNTERFEITING [MOLINA-VIDICK-WATROUS'12]

- Theorem [Molina-Vidick-Watrous'12]: optimal* counterfeiting probability of Wiesner's scheme is $\left(\frac{3}{4}\right)^n$.

*some caveats

# CLASSICAL VERIFIABILITY

- Classically verifiable QM: interactive classical verification between the bank and the user. [Gavinsky'12, Molina-Vidick-Watrous'12, Pastawski et al.'12, Georgiou-Kerenidis'15, Ben-David–S'16]
- Molina-Vidick-Watrous's scheme: the bank asks the user to measure each of the qubits in a random (standard / Hadamard) basis, and compare the results only when the qubits were encoded in that basis.

# NOISE TOLERANT SCHEMES [PASTAWSKI ET AL.'12]

- In an ideal setting, we could reject the quantum money state even if one qubit do not pass the measurement.
- Pastawski et al. proved explicit bounds on a variant of Wiesner's scheme, that require only $\approx 0.85$ of the qubits to pass verification.

# KEEPING THE DATABASE SMALL [BENNETT ET AL.'82]

- Instead of keeping a database, we can keep one secret key k, and use a pseudo-random function $f_k(i)$ as the key for the $i^{th}$ bill.
- Requires computational assumptions.

# IS QUANTUM MONEY BETTER?

- No copying of the quantum money is an overkill. We only need to solve the double spending problem. Simpler if we allow the bank to maintain a database / state.
- Alternative classical private money:
  - Money is a long  random bit-string. The bank keeps all the bit-string that were issued, and were not spent in a database.
  - Verification is done by checking whether the bit-string appears in the database. The money is removed from the data-base if it is spent.

# IS PRIVATE QUANTUM MONEY BETTER?

- What are the advantages of private quantum money?
  - No need to maintain a database / state.
  - Several branches of the bank can work simultanously, without communication.

# ANONYMITY: COINS VS. BILLS [MOSCA-STEBILA'10]

- Bills have serial numbers, which can be used to track people.
- Coins are indistinguishable, and provide anonymity.
- In Mosca and Stebila's  private scheme, all quantum money states are the same, and therefore provide anonymity, in a similar manner to coins.
  - In Ref. [Tokunaga-Okamoto-Imoto'03 , anonymity is achieved using a different approach.

# PUBLIC QUANTUM MONEY

# PUBLIC QUANTUM MONEY FROM HIDDEN SUBSPACES [AARONSON-CHRISTIANO'12]

Linear algebra background:

- Let $A \preccurlyeq \mathbb{F}_2^{2n}$ be a subspace of dimension $n$.
- Example: n=2. $\mathbb{F}_2^4$ consists of 16 vectors 0000,0001,…,1111.
- Addition: $0110 \oplus 0011 = 0101$
- A could be {0000,0110,0011,0101} which is of dimension 2.
- Fact 1: Given a basis for A, there's an efficient quantum circuit that prepares $|A\rangle = \frac{1}{\sqrt{2^n}} \sum_{a \in A} |a\rangle$.
- For the previous example, $|A\rangle = \frac{1}{\sqrt{4}} (|0000\rangle + |0110\rangle + |0011\rangle + |0101\rangle)$
- Eventually, this is the quantum money state: $|\$\rangle = |A\rangle$.

# PUBLIC QUANTUM MONEY FROM HIDDEN SUBSPACES

- Let $A^{\perp} = \{b \in \mathbb{F}_2^{2n} | a \cdot b = \sum_{i=1}^{2n} a_i \cdot b_i = 0 \, mod \, 2 \; \forall a \in A\}$
- Fact 2: $\mathrm{H}^{\otimes 2n}|A\rangle = |A^{\perp}\rangle = \frac{1}{\sqrt{2^n}} \sum_{b \in A^{\perp}} |b\rangle$
- Let $\Pi_A$ be the projection onto all the elements of A, and similarly, $\Pi_{A^{\perp}}$
- Fact 3: $\mathrm{H}^{\otimes 2n} \Pi_{A^{\perp}} H^{\otimes 2n} \Pi_A = |A\rangle\langle A|$ . (Nice exercise!)
- Conclusions: Given membership oracles to $A$ and $A^{\perp}$ we can verify $|A\rangle$.
- Fact 4: For a random A, and these membership oracles, Grover's algorithm takes $O\left(\sqrt{\frac{2^{2n}}{2^n}}\right) = O(2^{n/2})$ queries to generate $|A\rangle$, and this is asymptotically optimal.
- Fact 5: For a random A, and one copy of $|A\rangle$, the success probability of the optimal cloner is exponentially small.
- Computational no-cloning theorem [AC'12]: For a random A, one copy of $|A\rangle$ and membership oracles, $\Omega(2^{n/2})$ queries are required in order to clone $|A\rangle$. This gives the weak definition of quantum money, relative to an oracle

# PUBLIC QUANTUM MONEY FROM HIDDEN SUBSPACES

- How do we get rid of the oracle?
- Original construction used polynomials to hide the subspace.
- Their scheme is completely broken, using Gröbner basis techniques [Pena-Faugère-Perret'15] and the single copy-tomography attack [Farhi et al.'12] by Paul Christiano, which is reported in [Ben-David–S'16]
- Fixed in Ref. [Zhandry'18], using indistinguishability obfuscation (iO). Provably secure, based on general assumptions!

# PUBLIC QUANTUM MONEY FROM KNOTS [FARHI ET AL.'12]

- Another construction, based on beautiful knot theory. No security proof.
- Interesting feature: even a rogue mint cannot generate two quantum states with the same serial number. The money in circulation can be made publicly verifiable.

# ATTACK VECTORS FOR QUANTUM MONEY: SINGLE COPY TOMOGRAPHY [FARHI ET AL.'10]

- What can we learn about the quantum money state?
  - We further assume that the verification is a rank-1 projection onto the money state, and that the state is returned after verification.
  - We can measure it with respect to any two outcome measurement M, without destroying the state! Therefore, we can approximate $\langle \$ | M | \$ \rangle$.
  - In particular we can do local tomography of the money state.
  - Conclusion: a quantum money state of a projective public scheme cannot be a tensor product state!
- We can do that even when the state is returned only if the state passes verification by using "protective measurements" [Aharonov-Vaidman'93]!
- This can be used to preform an adaptive attack on Wiesner's scheme, if money is returned after successful verification [Nagaj et al.'12]

# EXPERIMENTAL DEMONSTRATIONS

- *A variant of Wiesner's scheme, setup close to standard QKD [Bozzio et al.'18].*
- *Experimental attacks on variants of Wiesner's scheme [Bartkiewicz et al.'17]*
- *No experiment demonstrated storage (using quantum memory).*

# EXTENSIONS OF QUANTUM MONEY

Is there a way for me to convince you that I gave you a “random” number?

- return “10001101”
- return rand()

Classically, this cannot be done! Can be done in the quantum setting!

# QUANTUM LIGHTNING [ZHANDRY'18]

- A quantum lightning scheme is also a public quantum money with other interesting properties.
- A quantum lightning is a pair $(|\$\rangle, r)$, where $|\$\rangle$ certifies that $r$ was generated in a random manner (has lots of entropy).
- The idea: it is exponentially hard to generate two quantum money states with the same $r$.
- For quantum money, the serial number helps verifying the quantum state. Here the roles are flipped.
- Version updated a few days ago, still not peer-reviewed. Uses non-standard hardness assumptions.

# QUANTUM COPY PROTECTION [AARONSON'09]

- A compiler which takes a classical Boolean circuit and outputs a quantum state.
- The quantum state can be used to run the original circuit.
- It is impossible to pirate the program: two different people can't evaluate the program on random inputs without communicating, given one copy-protected program.
- You can only lend the program to a friend, like a book.
- Candidate construction for point functions. Major open problem.

# QUANTUM TOKENS FOR DIGITAL SIGNATURES [BEN-DAVID– S'16]

- You go on vacation, and want to delegate the ability to sign one and only one message to your friend.
- Simplification for this talk: the message is one bit.
- You give your friend an Aaronson-Christiano quantum money state $|A\rangle$.
- To sign the message 0, the friend measures in the standard basis, and gets an element of $A$.
- To sign the message 0, the friend measures in the Hadamard basis and gets an element of $A^{\perp}$.
- Main theorem: given $A$, it is hard to find one element of $A$ and another from $A^{\perp}$.

# DISPENSABLE BACKDOORS [CHUNG ET AL.'18]

- Currently: governments want manufacturers to have backdoors. FBI-Apple encryption dispute.
- Problems:
  - Backdoors provide too much power to the government.
  - If backdoor is leaked / discovered, bad guys can use it to break to all the devices.
- Proposed solution:
  - Several dispensable backdoors supplied by the manufacturer to the government. Each dispensable backdoor can be used to unlock only one device, chosen by the government.
  - Underlying construction: tokens for digital signatures. Signed message of the device ID can be used to unlock the device.

# DISPENSABLE BACKDOORS (2)

- Advantages:
  - Limited power to the government.
  - Limited damage if the government's dispensable backdoors are stolen.
- Disadvantages:
  - Too much power to the manufacturer. No way to know whether they are abusing it.
  - Users may want not to use a scheme with a back-door. May raise ethical concerns, and demands to forbid schemes without back-doors.

# ETHICAL RESPONSIBILITIES

- Politics is about the division of power.
- Cryptography has changed, and will change the division of power.
- Are we moving power from the individuals to the organizations, or from the organizations to the individuals.
- We have the power to influence this.

which will be the largest and the most technologically advanced in the world. This quantum network will be applied to national strategies such as "the Belt and Road", which will realize large-scale quantum secure communication in the fields of government, finance, energy and civil-military integration, etc.. [redacted] will become a world-class quantum key service provider, which will promote the strategic emerging industries, and make important contributions to national economic and national security.

which will be the largest and the most technologically advanced in the world. This quantum network will be applied to national strategies such as “the Belt and Road”, which will realize large-scale quantum secure communication in the fields of government, finance, energy and civil-military integration, etc..

Alice & Bob,

will become a world-class quantum key service provider, which will promote the strategic emerging industries, and make important contributions to national economic and national security.

# OPEN PROBLEMS

- Experimental demonstrations of quantum money, including storage (requires quantum memory).
- Anonymous public quantum coins
- Stronger security definitions for quantum money?
- Upgrade path from Bitcoin to quantum money

# OPEN PROBLEMS (2)

- Provably secure public quantum money, from standard assumptions (without Indistiuguishability obfuscation).
- Constructions of copy-protecting programs other than point functions? Applications?
- Quantum Tokens for other tasks? Revocable decryption tokens?
- Atomic swap: changing quantum $ to quantum RNB in a trustless manner.

- [Bozzio et al.'18] Bozzio, M., Orieux, A., Vidarte, L. T., Zaquine, I., Kerenidis, I., & Diamanti, E. (2018). Experimental investigation of practical unforgeable quantum money. npj Quantum Information, 4(1), 5.
- [Chung et al'.18] Chung, K. M., Georgiou, M., Lai, C. Y., & Zikas, V. (2018). Cryptography with Dispensable Backdoors, IACR eprint 2018/352.
- [Farhi et al.'10] Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., Nagaj, D., & Shor, P. (2010). Quantum state restoration and single-copy tomography for ground states of hamiltonians. Physical review letters, 105(19), 190503.
- [Farhi et al.'12] Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., & Shor, P. (2012). Quantum money from knots. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference* (pp. 276-289). ACM.
- [Gavinsky'12] Gavinsky, D. (2012). Quantum money with classical verification. In *Computational Complexity (CCC), 2012 IEEE 27th Annual Conference on* (pp. 42-52). IEEE.
- [Georgiou-Kerenidis'15] Georgiou, M., & Kerenidis, I. (2015). New constructions for quantum money. In LIPIcs-Leibniz International Proceedings in Informatics (Vol. 44). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
- [Molina-Watrous-Visick'12] Molina, A., Vidick, T., & Watrous, J. (2012). Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. In *Conference on Quantum Computation, Communication, and Cryptography* (pp. 45-64). Springer.