Almost Public Quantum Coins

Amit Behera[1] and Or Sattath[1]

[1]Computer Science Department, Ben-Gurion University

February 2, 2021

A quantum money scheme, just like in traditional classical money schemes can be a bills scheme such as Wiesner's scheme [Wie83] or a coin scheme such as [MS10]. In a bills scheme, each money state is uniquely tagged with a unique serial number whereas quantum coins are exact copies of the same state. Therefore, bills are prone to privacy related attacks.

Another important characterization of quantum money scheme is that it can be either private or public. In a private schemes, only the the bank can verify money states, using some secret information. The motivation for a public money scheme is to abolish the need to go to the bank for verification. Usually, this is done by issuing a classical public key which is used in the verification algorithm. Despite several attempts in this direction, there is still no public quantum money based on standard assumptions. However, there is another way for public verification. Consider the following scenario: you travel to a foreign country and withdraw some cash from an ATM. Later you execute a transaction in which you receive money from an untrusted source. How will you verify the authenticity of this money? You could compare it to the money that you withdrew from the bank's ATM, and accept if they look the same. We call this method *comparison-based verification*. Note that, you did not require any additional information such as a public key or other security features regarding the money. However, you do require that the money states are coins and not bills, i.e., they are indistinguishable copies of one another.

In this work, we extend the method of comparison-based verification to the quantum setting, and use it to lift a private quantum coin scheme to an *almost public quantum coin scheme*. The verification of received coins is done by comparing it to a fresh coin from the wallet. Hence, in this scheme at least one valid money state is required for verification of the money received. Technically, the comparison between two quantum money states is done by doing a projective measurement into the symmetric subspace.

User-manual The quantum coin scheme that we construct has slightly different properties compared to a true public coin. Our money scheme uses the following user-manual. A user needs a fresh coin received directly from the bank, to verify each transaction he receives, i.e., it is not that only one coin is received. However, he can spend as much coins as he wants from his wallet, including the ones that he received from others. Due to these restrictions, we call our construction an *almost public quantum coin* scheme, which also explains the title of the paper.

Comparison to a true public quantum coin scheme The only inconvenience in our scheme compared to a truly public money scheme, is that a user cannot receive more transactions than the number of fresh coins from the bank he started with. Hence, after sometime, he might have to go to the bank for refund. However, this is mostly a theoretical inconvenience.

Practically, the user will never have to go to the bank since money initially withdrawn would be enough for all his transactions, for a long period of time. For example, if a user takes 100 dollars from the bank, and suppose each public coin is worth a cent, then he essentially has 10000 cents/public coins, and is eligible to receive 10000 transactions. Moreover, he can spend the money that he received from others and therefore there is no limit on spending. This is practically enough for all his transactions, all the year round, and therefore, would have to go to the bank only once a year. We can also increase the limit of the number of receivable transactions by devaluing the worth of our coins. For instance, in the previous example, we can instead declare the worth of our public coin to be a micro-dollar, and hence if a merchant starts with 100 dollars, he would now have 10^8 public coins, and would be eligible to receive 10^8 new transactions. We show that our construction, under the user manual discussed above is rationally secure against sabotage and forgeability attacks, i.e., on average the gain of a cheating adversary and the net loss of an honest user is at most negligible. Since in real life, the users are rational entities, rational unforgeability and rational security against sabotage ensures that nobody will try to forge money or sabotage others. Hence, in all practicality, a user using our coins scheme will never feel any difference from a truly public coin scheme. Therefore, our construction is practically equivalent to a public coin scheme despite some theoretical differences.

Main results Our main result is the construction of an almost public quantum coin scheme, based on a private coin scheme, lifting most of the security guarantees of the private coin scheme to the public scheme. By instantiating our construction with the private coin construction in [JLS18] (later simplified by [BS19]), we get the following result.

Theorem 1 (Informal Main Result)**.** *Assuming quantum secure one-way functions exist, there is an almost public quantum coin scheme which is rationally secure against nonadaptive forgery.*

There has not been any public quantum money construction in the literature prior to this work, which is provably secure based on standard assumptions. This is the first construction of a money scheme that gets close to public quantum money based on standard assumptions. Similarly, by instantiating our construction with the results in Ref. [MS10] and Ref. [AMR20], we show an *inefficient* scheme and a stateful scheme respectively, with the same properties as in Theorem 1 above, which is secure even against *computationally unbounded* adversaries. The formal results are given in Theorem 16, in the main text.

Main obstacles and our solution The biggest challenge in our work is to understand how to do comparison of quantum states in comparison-based verification for quantum coins. Classically, given two classical bit strings we know their classical states and hence can compare them. However, given two unknown qubits, their quantum states remain hidden to us due to the no-cloning theorem. A natural first attempt to compare two quantum coins is to do SWAP-test on them. However, SWAP-test [BCWdW01] always accepts (even for two orthogonal states) with probability $\frac{1}{2}$ which is not enough for a quantum coin scheme. Secondly, since comparison-based verification involves coin from the wallet, one needs to make sure there are no sabotage attacks. In particular, there should be a meaningful way to get a refund of one's wallet, especially in case of failed verification, such that a honest user should not get refund lesser than what he should have had.

We tackle these obstacles as follows. We improve the naïve approach of using SWAP-test by using multiple private coins as one public coin, such that individual private coins cannot be used in a transaction. This is similar to the currencies ₥ and ¢, where a ¢ is used in transactions and is equivalent to 10 mills, but mills themselves are a unit that the users are unaware of (and

is only used "behind the scenes", e.g., to handle rounding errors by banks), and hence not used in transaction. Due to this analogy, we call a private coin $|\text{m}\rangle$ and a public coin as $|\text{c}\rangle := |\text{m}\rangle^{\kappa}$, for some fixed $\kappa \in \log^c(\lambda)$ for some $c > 1$. For verification of an alleged coin, we take a fresh coin $|\text{c}\rangle$ from the wallet, and perform a projective measurement into the symmetric subspace of the 2κ registers. The coin is accepted if the entire 2κ-register state is projected into the symmetric subspace. Suppose in this scheme an adversary with no public coins, submits an alleged coin with quantum state $|\phi\rangle$ for verification. For simplicity, suppose $|\text{m}\rangle$ is the qubit state $|1\rangle$. Since the underlying private scheme is unforgeable, the κ-register state $|\phi\rangle$ must have negligible overlap with all the computational basis state other than the all zero state. The probability of the all zeroes state to pass verification is $\frac{1}{\binom{2\kappa}{\kappa}}$, which is negligible for our choice of κ. Hence, the optimal success probability for 0 to 1 is negligible. Unfortunately, n to $n+1$ forging is possible in our scheme for large enough n. The optimal success probability scales as $\approx 1 - \frac{\kappa}{n}$ for large n, which is very close to 1 even for $n = \mathsf{poly}(\lambda)$, and hence our construction *is forgeable* according to the standard definition.

Drawbacks: Weaker notions of security The main drawbacks are the weak notions of security that we use. For more details on all these notions of security, refer to *Notions of security* in the introduction of the main text. We differ from the standard notions of unforgeability to a slightly weaker notion called rational unforgeability in order to prove our construction is unforgeable. We show in the main text (see Section 5.1) that our construction is not standard unforgeable and hence, shifting to rational unforgeability is necessary. We also deviate from the usual notion of *flexible* utility to the *all-or-nothing utility* for defining the gain of the adversary. From a theoretical point of view, the usual-manual has a few restrictions which we discussed previously. We show that the restrictions put in the user-manual, ensures and are necessary for security.

Scientific Contributions Based on the private quantum coins construction in [JLS18], we construct an almost public quantum coin scheme that is provably secure based on the existence of quantum-secure one-way function. No other public money construction is provably secure based on standard assumptions. Moreover, unlike most other schemes, our construction only requires polylogarithmic time and space. Our construction is the first quantum money scheme which achieves both public verification and is a quantum coin scheme. No construction of public quantum coins are known in the literature. Moreover, based on previous works [AMR20, MS10], we construct an unconditionally secure stateful quantum money scheme that resembles a public quantum money scheme in all practicality. The existing constructions of public money involve verification using a classical public key, and hence, cannot be unconditionally secure (see [AC13]). We circumvent this problem by using comparison-based verification. Our construction resembles a public quantum money with a quantum public key. This might be an interesting topic on its own as it might circumvent the impossibility result about public quantum money mentioned above. We introduce the notion of rational unforgeability which is a weaker yet a meaningful notion of unforgeability. Lastly, the techniques used in our construction are simple and general, and might also be useful in topics other than quantum money.

References

[AC13] S. Aaronson and P. Christiano. Quantum Money from Hidden Subspaces. *Theory of Computing*, 9:349–401, 2013, arXiv: 1203.4740.

[AMR20] G. Alagic, C. Majenz, and A. Russell. Efficient Simulation of Random States and Random Unitaries. In A. Canteaut and Y. Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part III*, volume 12107 of *Lecture Notes in Computer Science*, pages 759–787. Springer, 2020, arXiv: 1910.05729.

[BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum Fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001, arXiv: quant-ph/0102001.

[BS19] Z. Brakerski and O. Shmueli. (Pseudo) Random Quantum States with Binary Phase. In D. Hofheinz and A. Rosen, editors, *Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I*, volume 11891 of *Lecture Notes in Computer Science*, pages 229–250. Springer, 2019, arXiv: 1906.10611.

[JLS18] Z. Ji, Y. Liu, and F. Song. Pseudorandom Quantum States. In H. Shacham and A. Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 126–152. Springer, 2018, arXiv: 1711.00385.

[MS10] M. Mosca and D. Stebila. *Quantum coins*, volume 523 of *Contemp. Math.*, pages 35–47. Amer. Math. Soc., 2010, arXiv: 0911.1295.

[Wie83] S. Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.