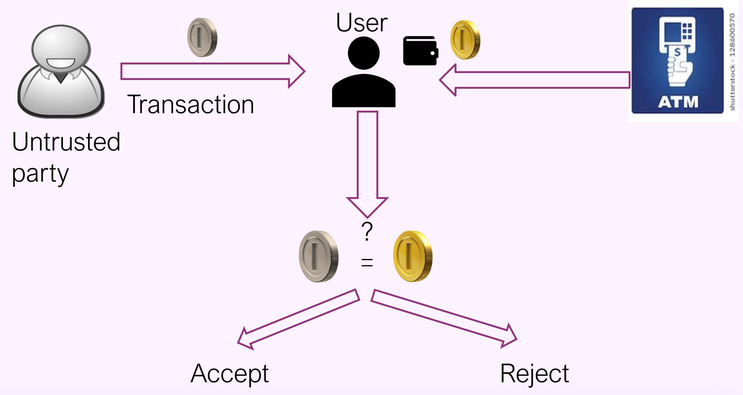
Almost Public Quantum Coins

Amit Behera, Or Sattath
Ben-Gurion University, Israel

Coins	Bills
All money state are indistinguishable copies, and hence can't be tracked.	Every money bill is marked with unique serial numbers and hence can be tracked.

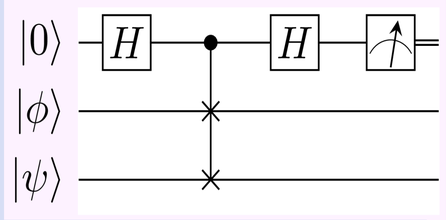
Goal: Construction of public quantum coins from private quantum coins.

Motivation: Comparison based Verification



1. Works for coins not for bills.
2. Specific security features of the money not required.

How to compare quantum states?



SWAP Test: Always passes with prob at least half. → 1 to 2 forging is trivial!

Symmetric subspace measurement

- Symmetric subspace over n registers - space of all states, invariant under any permutation of the registers.
- Symmetric subspace measurement – Projective measurement into the symmetric subspace.
- For two registers, it is the same as the SWAP test.

Main protocol

$\kappa :=$ poly-logarithmic function of λ.
$|\mathfrak{m}\rangle :=$ a private coin.
$|¢\rangle :=$ a public coin.
$Verify_{|¢\rangle} :=$ Public verification.
$Verify_{sk} :=$ Private verification.

- $Keygen(1^{\lambda})$ - Run private scheme's Keygen, to generate sk.
- $Mint(sk)$ – Use the private scheme's mint κ times to prepare $|¢\rangle = |\mathfrak{m}\rangle^{\otimes\kappa}$.
- $Verify_{|¢\rangle}(|\phi\rangle)$- Symmetric subspace measurement on 2κ registers of $|¢\rangle$ and $|\mathfrak{m}\rangle$, and accept on success.
- $Verify_{sk}(|\phi\rangle)$- Run private scheme's count $Count$ on $|\phi\rangle$ and accept with prob. $\frac{Count(|\phi\rangle)}{\kappa}$.

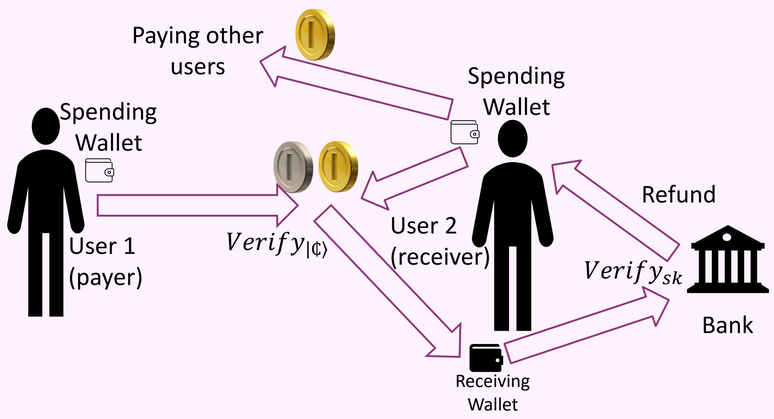
Rational Unforgeability

Rational unforgeaility - On expectation, one cannot pass more than n verifications starting with n coins.
(No rational user would forge)

Issues with the scheme

1. Standard forging still possible and only rational unforgeability holds.
2. Own money might get destroyed due to pubic verification.
3. Need a way to recover own money after failed verification.
4. Spending money received form others directly can lead to traceability attacks.

Restriction: User manual



Security guarantees

- The money scheme is (nonadaptive) rationally unforgeable.
- Under the restrictions in the user manual, it is secure against sabotage attacks (rationally), and also traceability attacks.

Read the Full Paper at: https://arxiv.org/pdf/2002.12438.pdf