Almost Public Quantum Coins

Amit Behera

Ben-Gurion University

QIP2021

Feb 5, 2021

Joint Work with **Or Sattath (BGU)**

arXiv:2002.12438

Ben-Gurion University

LIST OF CONTENTS

- Introduction
- Previous Works and our contributions.
- Construction
- Security Definition and main results
- Technical results

INTRODUCTION

UNFORGEABLE MONEY

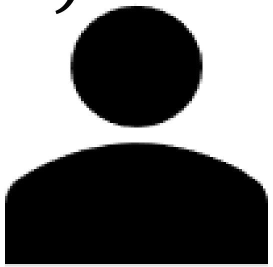
- Can money schemes be unforgeable?
- Classically not possible.
- With quantum, you can!

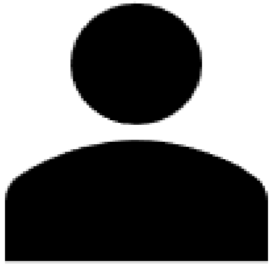
QUANTUM MONEY

$(Keygen,\ Mint,\ Verify)$

$sk \leftarrow Keygen(1^\lambda)$

$Mint(sk) \rightarrow |\$\rangle$



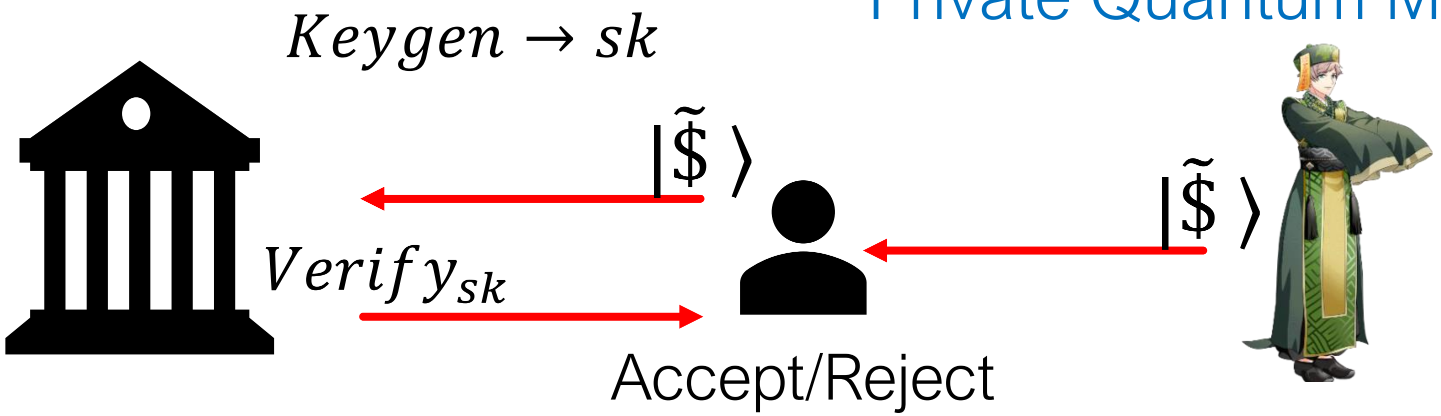


$|\tilde{\$}\rangle$

$Verify(|\tilde{\$}\rangle) \rightarrow$ Accept/Reject

PRIVATE VS PUBLIC QUANTUM MONEY

Private Quantum Money



Public Quantum Money

Public Verification

COINS VS BILLS

Indistinguishable copies

Unique serial numbers

How does it matter? Privacy!

Serial numbers can be tracked.

PREVIOUS WORKS AND OUR CONTRIBUTIONS

QUANTUM MONEY CONSTRUCTIONS

- **Private Quantum Money:** Wiesner's money, Gavinsky's quantum money scheme, etc.
- **Public Quantum Money:** Zhandry's quantum money, Farhi et al.

No public money construction based on weak and generic assumptions.

QUANTUM COINS CONSTRUCTIONS

Private Quantum coin Scheme	Computational Assumption	Memory dependent	Efficiency	Unforgeability
MS10	No	No	Inefficient	Adaptive Unforgeability
JLS18	quantum secure one-way function	No	Efficient	Adaptive Unforgeability
AMR20	No	Yes	Efficient	Adaptive Unforgeability

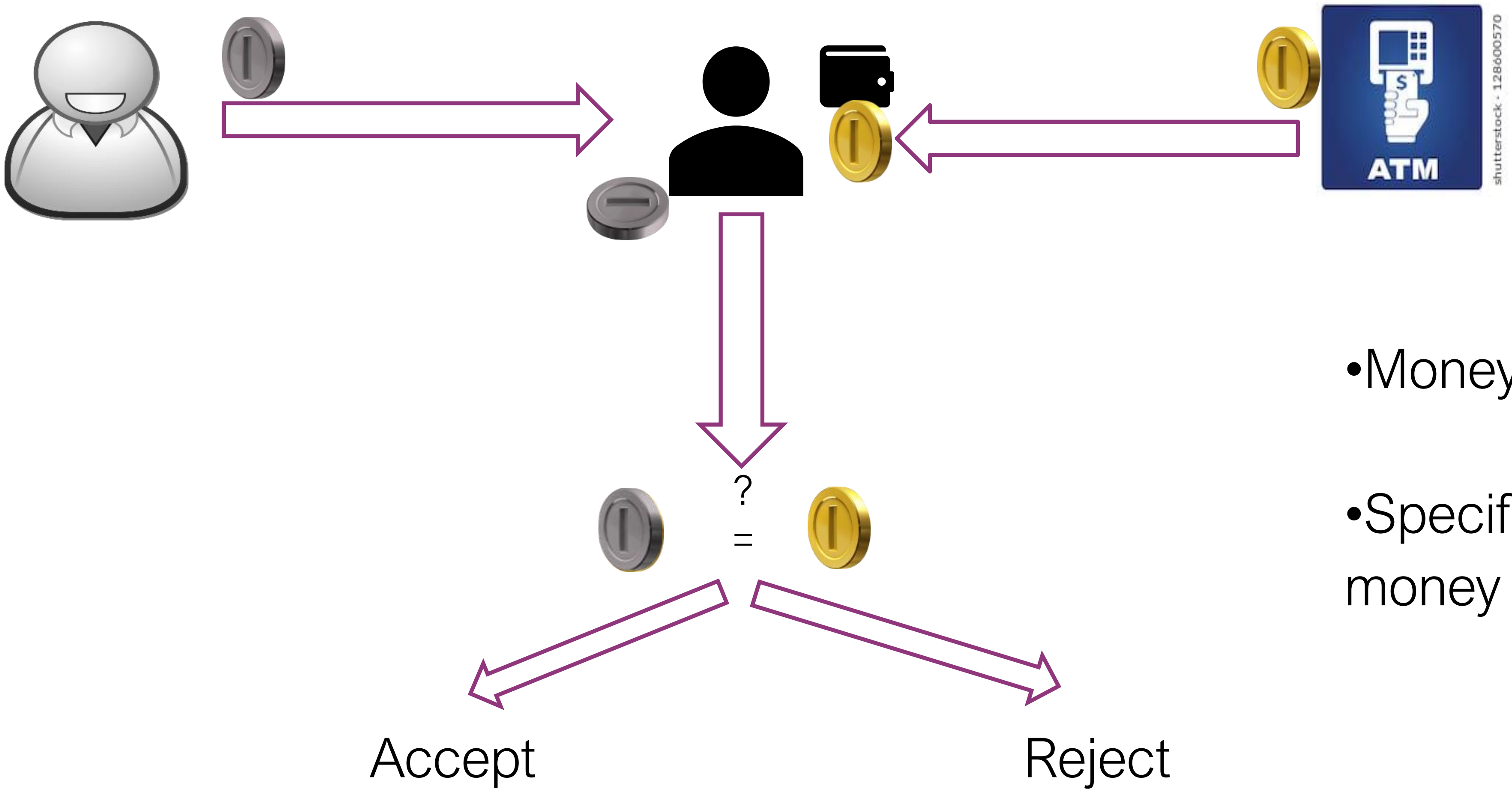
Public Quantum Coins: No candidate construction.

OUR CONTRIBUTIONS

- *Almost* Public Quantum Money from standard assumption.
- Almost Public Quantum Coin construction.
- Other meaningful notions of security.
- Comparison-based Verification.

OUR CONSTRUCTION

COMPARISON-BASED VERIFICATION



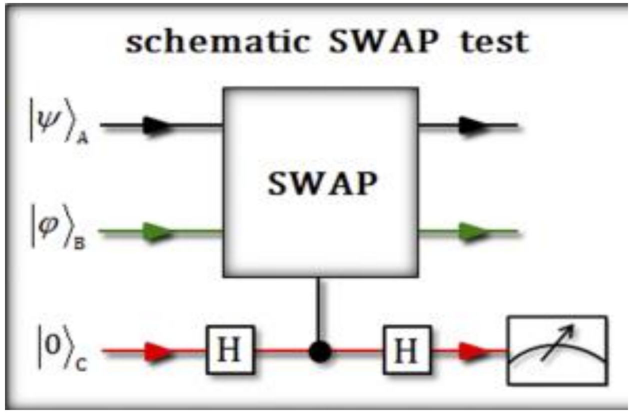
<u>Observations</u>

- Money states should be identical.
- Specific security features of the money not required.

CHALLENGE IN QUANTUM SETTING

How to compare two quantum states?

- Attempt: SWAP TEST?
  - Accepts product states with probability $\geq \frac{1}{2}$.
  - 0 to 1 forging possible.



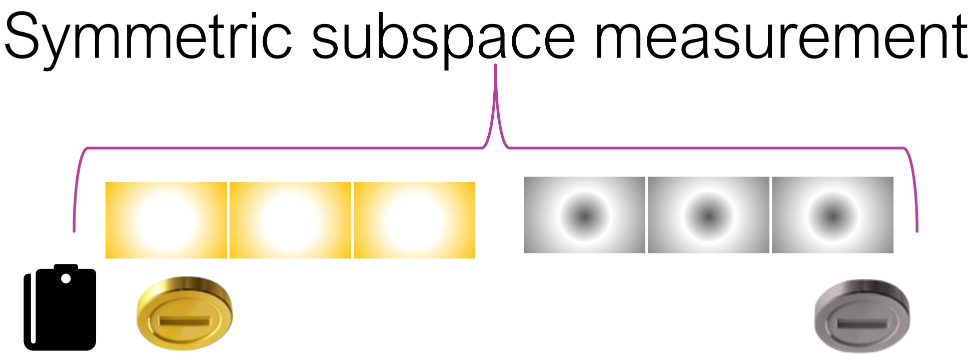
- Solution: Symmetric subspace projective measurement.
  - Each coin is k mini coins/registers.
  - Measurement projecting onto the Symmetric subspace of $2k$ registers.

OUR CONSTRUCTION

Public Quantum Coin

Private Quantum Coin *Keygen, Mint, Verify* $|\text{₥}\rangle$

- Keygen: Same as *Keygen*
- Mint: Repeat *Mint* k times. $|\text{¢}\rangle = |\text{₥}\rangle^{\otimes k}$
- Verify: Comparison-based verification.



Symmetric subspace over m registers

$Sym(\mathcal{H}^{\otimes m})$: m register pure states invariant under any permutation of registers.

SECURITY DEFINITION AND MAIN RESULTS

UNFORGEABILITY GAME (INFORMAL)

Challenger

$|\$\rangle^{\otimes n}$

Adversary

$Verify\,()$

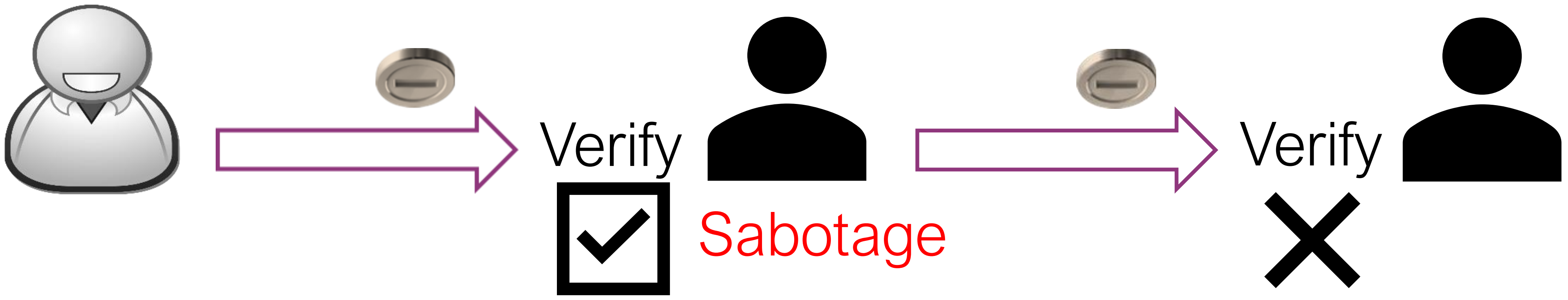
$\rho_1\rho_2 \ldots \rho_m$

With overwhelming probability

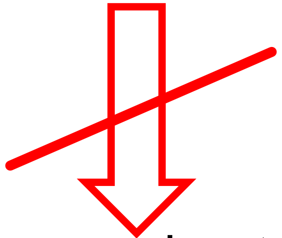
Standard Unforgeability: $\#\ successful\ verifications \leq n$.

Rational Unforgeability: $\mathbf{E}(\#\ successful\ verifications) \leq n$.

IS UNFORGEABILITY ENOUGH?



Unforgeability, Completeness



Security against Sabotage

SABOTAGE GAME (INFORMAL)

$Accept_2$ = coins accepted

$Verify()$ ← $\rho'_1, \rho'_2, \dots \rho'_m$

Merchant 2

$Accept_1$ = coins accepted

$Verify()$ ← $\rho_1, \rho_2, \dots \rho_m$

Merchant 1

Adversary

Standard Security against Sabotage: $Accept_1 \leq Accept_2$.

With overwhelming probability

Rational Security against Sabotage: $\mathbf{E}(Accept_1) \leq \mathbf{E}(Accept_2)$.

LIFTING RESULT

Unforgeable

Private Quantum Coin Scheme

MS10, JLS18, AMR20

Our construction

Rationally Secure Public Quantum Coins

MAIN RESULT

One-Way Functions exist

Rationally Secure Public Quantum Coins

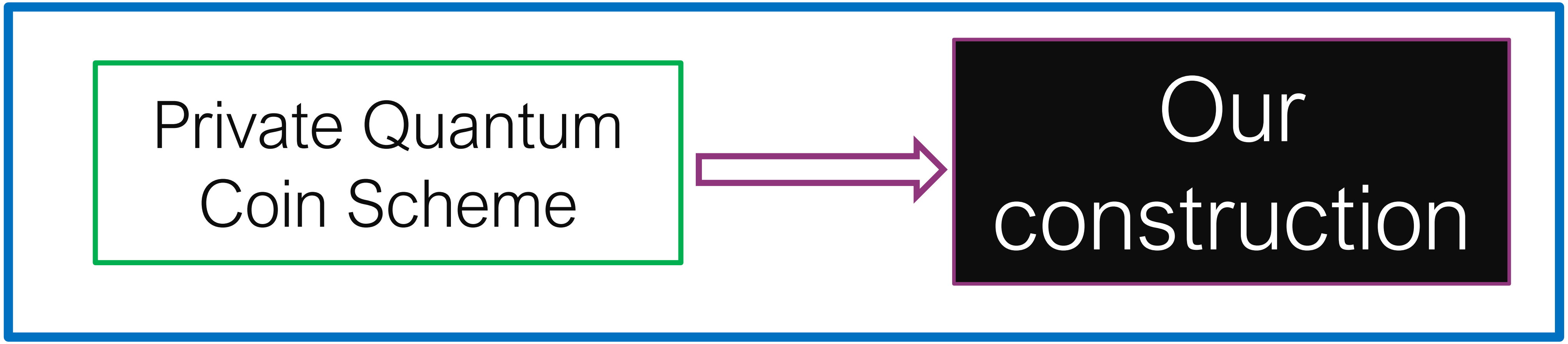
Our construction

JLS18

Based on One-Way Functions

Rationally Secure Public Quantum Coins

OTHER RESULTS



Resulting Public Quantum Coin Construction		
Private Coins Scheme	**Memory dependent**	**Efficiency**
MS10	No	Inefficient
AMR20	Yes	Efficient

PROPERTIES OF OUR CONSTRUCTION

Negatives

1. Rational Secure.
2. Fresh coin required for every received transaction.

Positives

1. Real world adversaries are rational.
2. Need to visit the bank only once in a while.

Practically, no less than a public quantum coin scheme!

TECHNICAL RESULTS

1. 0 TO 1 UNFORGEABILITY
2. OPTIMAL $n \rightarrow n+1$ FORGERY

0 TO 1 UNFORGEABILITY

Private coin

$|\not{m}\rangle = |1\rangle \in \mathbb{C}^2$

Public coin

$|¢\rangle = |1\rangle^{\otimes k}$

$|\phi\rangle \approx |0\rangle^{\otimes k}$

Verify

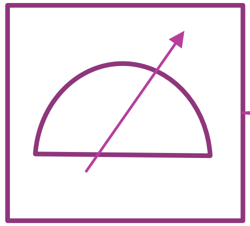
Unforgeability of private scheme

Hamming weight on measuring $|\phi\rangle = 0$

Verify:

$|1\rangle^{\otimes k} \otimes |0\rangle^{\otimes k}$

$|¢\rangle \quad |\phi\rangle$



$\Pi_{Sym}, I - \Pi_{Sym}$

$$\frac{1}{\sqrt{\binom{2k}{k}}} \sum_{\substack{b \in \{0,1\}^{2k} \\ wt(b)=k}} \otimes_{i=1}^{2k} |b_i\rangle$$

$Sym^{\perp}$

Accept

Reject

Forgery probability

$$\frac{1}{\binom{2k}{k}}$$

Negligible!

OPTIMAL FORGERY $n \to n+1$

Public coin:

$|¢\rangle = |1\rangle^{\otimes k} \in \mathcal{H}^{\otimes k}$

$|¢\rangle^{\otimes n}$

$|\phi\rangle$

$(n+1)k$ registers

Hamming weight on measuring $|\phi\rangle \leq nk$

Verify($|\phi\rangle$) $\xrightarrow{Sym}$ Accept

$\xrightarrow{Sym^{\perp}}$ Reject

$|¢\rangle$

Forgery probability

Maximize$_{|\phi\rangle}$ $|\Pi_{Sym}(|1\rangle^{\otimes k} \otimes |\phi\rangle)|^2$

USING PROPERTIES OF SYMMETRIC SUBSPACE

$$|\phi\rangle \in Sym\left(\mathcal{H}^{\otimes(n+1)k}\right)^{\perp} \Longrightarrow \Pi_{Sym}(|1\rangle^{\otimes k} \otimes |\phi\rangle) = 0$$

Forging Probability

Maximize $|\phi\rangle$ $\quad |\Pi_{Sym}(|1\rangle^{\otimes k} \otimes |\phi\rangle)|^2$

$|\phi_{opt}\rangle \in Sym\left(\mathcal{H}^{\otimes(n+1)k}\right)$

Hamming weight on measuring $|\phi\rangle \leq nk$

BASIS FOR SYMMETRIC SUBSPACE

$Sym(\mathcal{H}^{\otimes m})$ $\quad \{|Sym_j\rangle\}_{0 \le j \le m}$ $\quad |Sym_j\rangle = \frac{1}{\sqrt{\binom{m}{j}}} \sum_{\substack{b \in \{0,1\}^m \\ wt(b) = j}} \otimes_{i=1}^{m} |b_i\rangle$

1. Hamming weight on measuring $|Sym_j\rangle = j$.

2. $(\langle 1|^{\otimes k} \otimes \langle Sym_i|)\Pi_{Sym}(|1\rangle^{\otimes k} \otimes |Sym_j\rangle) = 0.$

3. $|\Pi_{Sym}(|1\rangle^{\otimes k} \otimes |Sym_j\rangle)|^2 = \frac{\binom{m}{j}}{\binom{m+k}{j+k}} \uparrow \qquad j \uparrow$

OPTIMAL FORGER $n \to n+1$

$$|\phi_{opt}\rangle \in \{|Sym_j\rangle\}_{j \le nk}$$

$$|\phi_{opt}\rangle = |Sym_{nk}\rangle$$

Maximize $_{|\phi\rangle}$ $|\Pi_{Sym}(|1\rangle^{\otimes k} \otimes |\phi\rangle)|^2$

- Hamming weight on measuring $|\phi\rangle \le nk$.
- $|\phi\rangle \in Sym(\mathcal{H}^{\otimes (n+1)k})$.

Not Standard Unforgeable

Optimal forgery probability

$$|\Pi_{Sym}(|1\rangle^{\otimes k} \otimes |Sym_{nk}\rangle)|^2 = \frac{\binom{(n+1)k}{nk}}{\binom{(n+2)k}{(n+1)k}} \approx \left(1 - \frac{1}{n}\right)^k \to 1$$

$as\ n \to \infty$

SUMMARY OF TECHNICAL RESULTS

- 0 to 1 Unforgeability.

- Optimal n to $n+1$ forgery.
  - Our construction is standard forgeable.
  - Our construction is rational unforgeable.

DISCUSSIONS AND OPEN QUESTIONS

- Can comparison-based verification be useful – quantum copy-protection, quantum tokens for digital signatures, secure software leasing, etc?
- Does there exist (standard) unforgeable public quantum money scheme from standard assumptions?

Thank You