

Quantum Money with Minimal Quantum

Joe Carolan

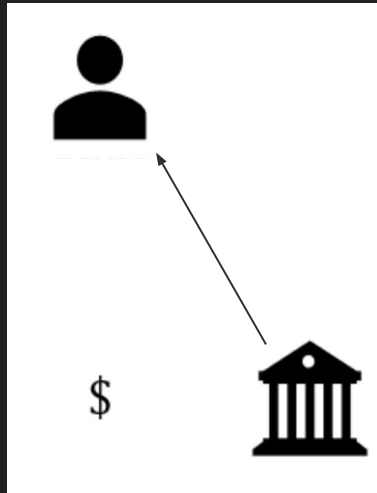
Outline

- 1) Define money
- 2) Example scheme
- 3) Semi-quantum scheme
 - a) Motivation
 - b) Intuition
 - c) Security Argument
- 4) Future directions

Physical Money

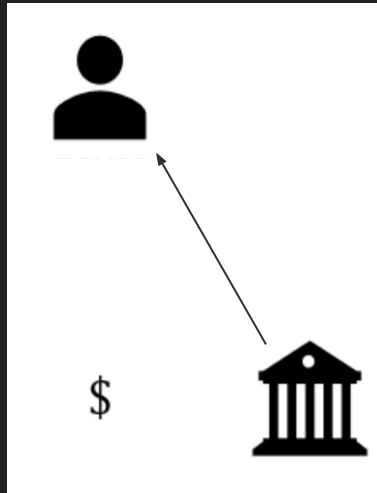
Physical Money

Minting

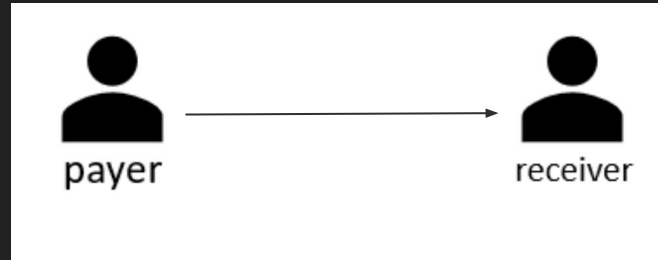


Physical Money

Minting

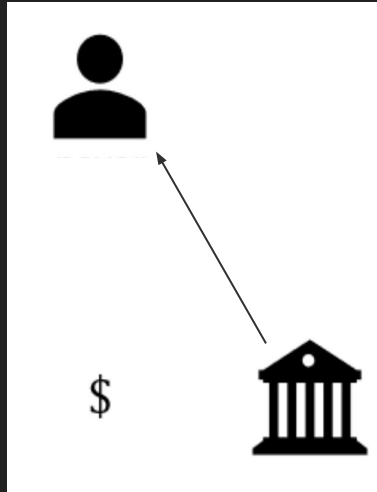


Transaction

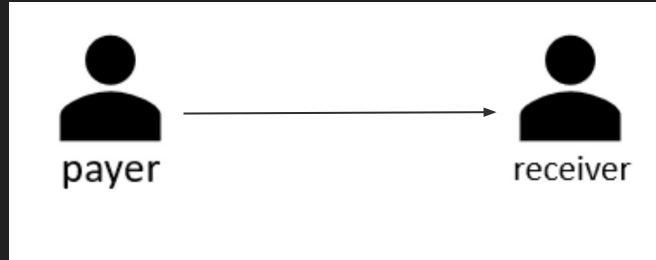


Physical Money

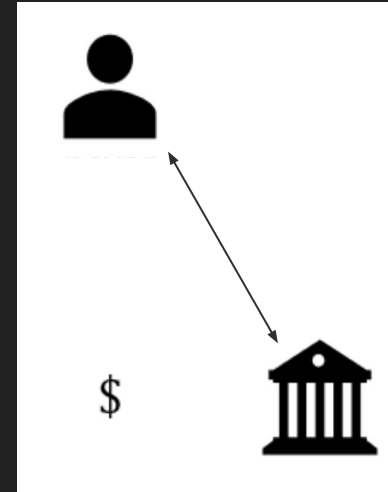
Minting



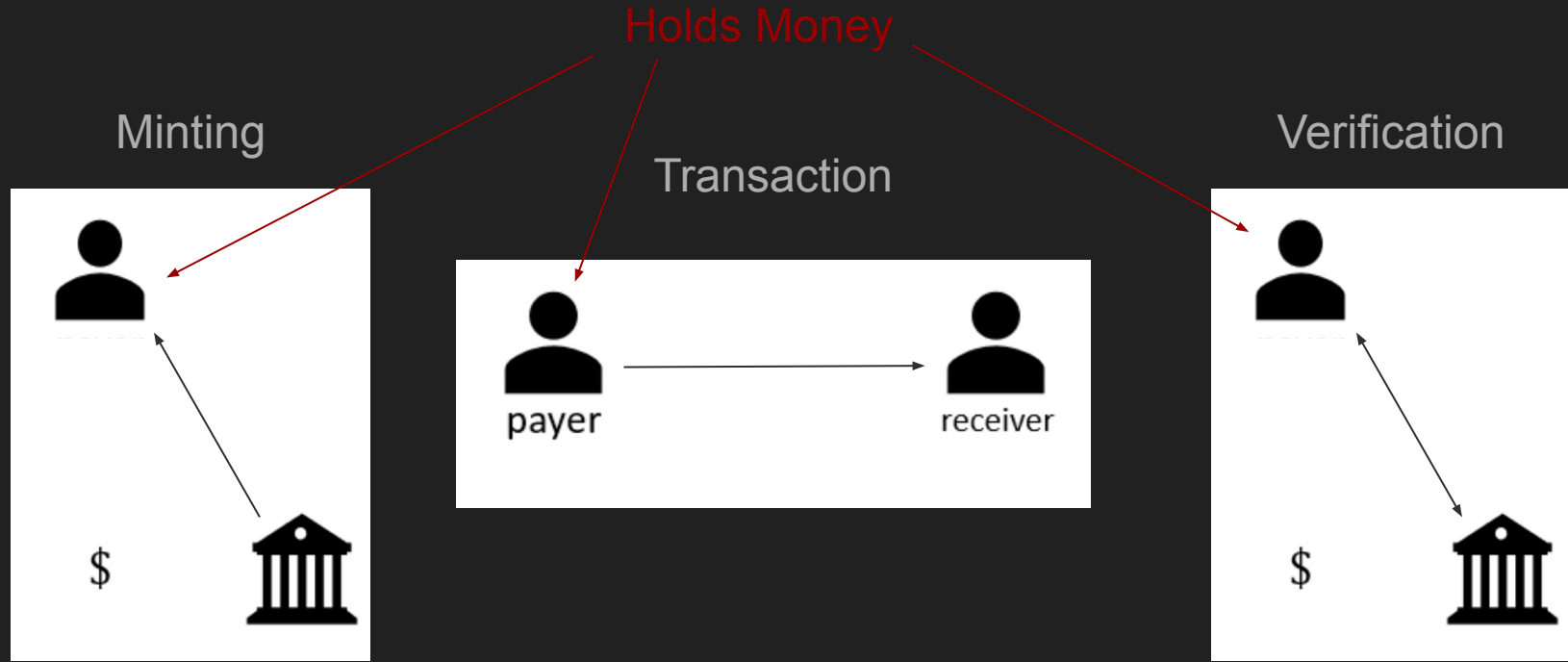
Transaction



Verification

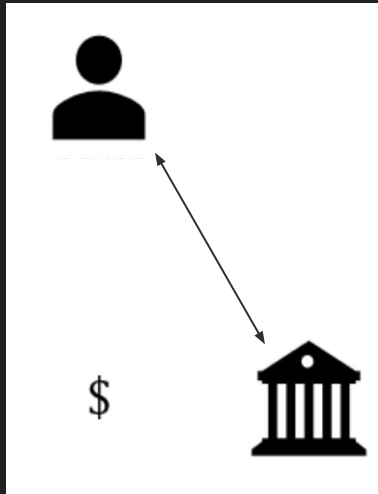


Physical Money



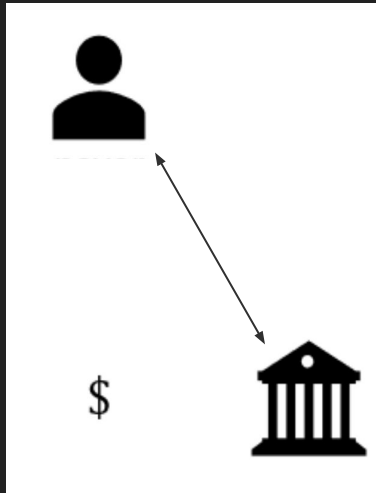
Classical Money

Minting

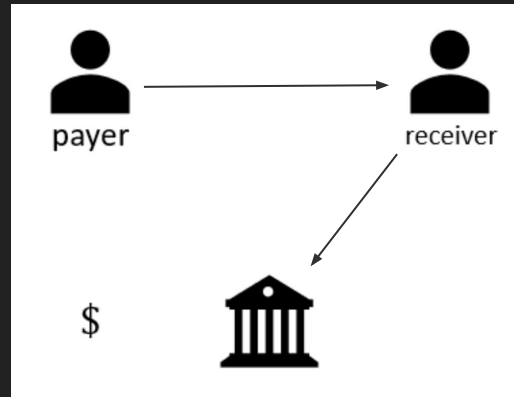


Classical Money

Minting

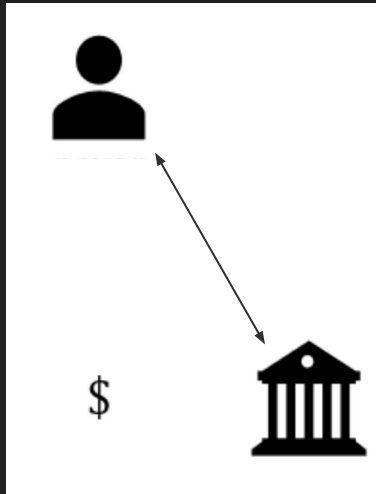


Direct (Credit)

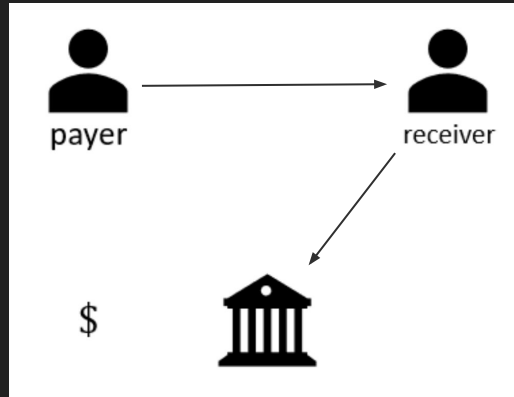


Classical Money

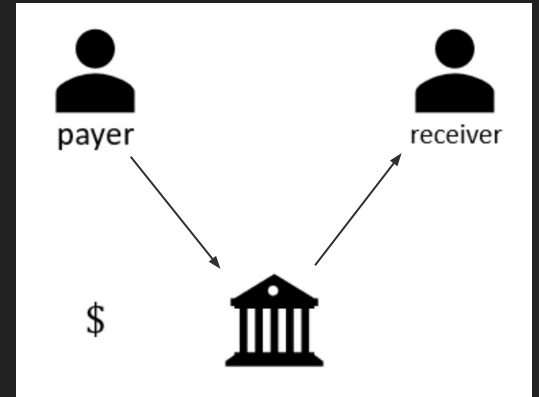
Minting



Direct (Credit)

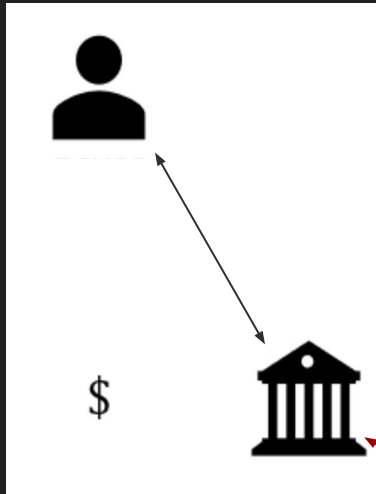


Through Bank (Wire)

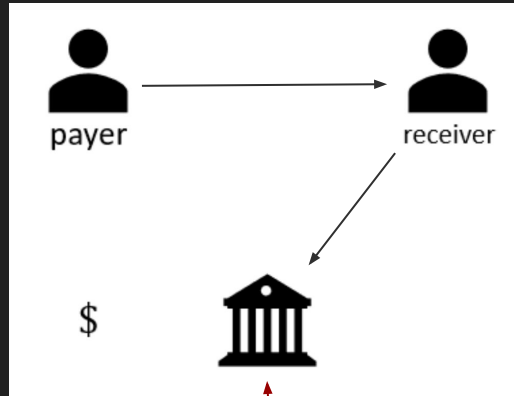


Classical Money

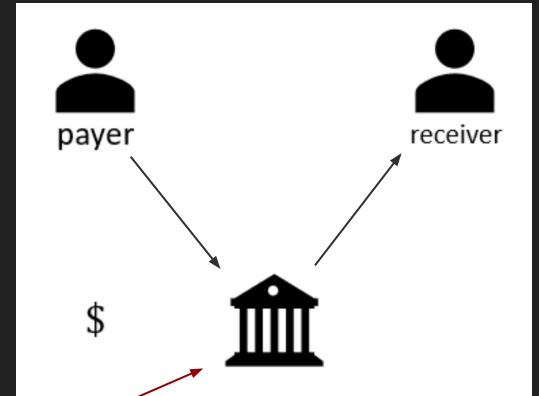
Minting



Direct (Credit)



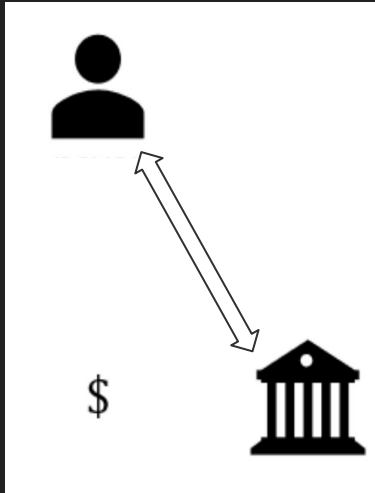
Through Bank (Wire)



Holds Money

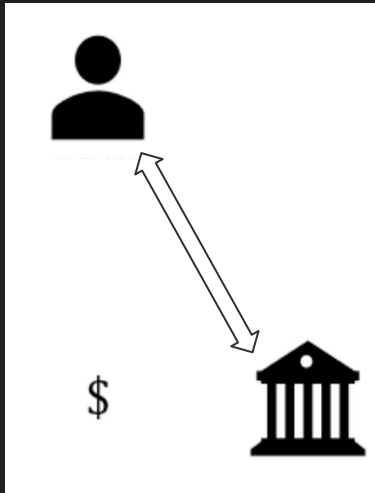
Quantum Money

Minting

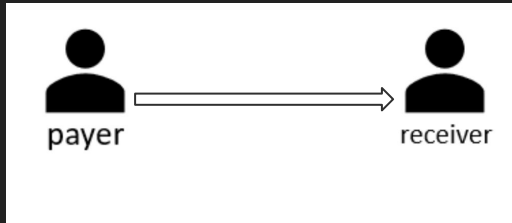


Quantum Money

Minting

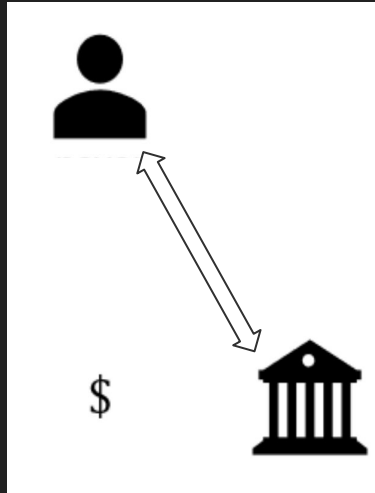


(Insecure)
Transaction

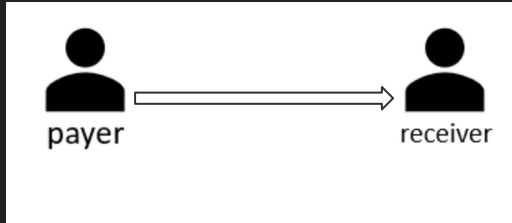


Quantum Money

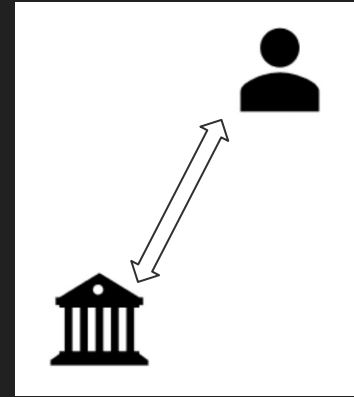
Minting



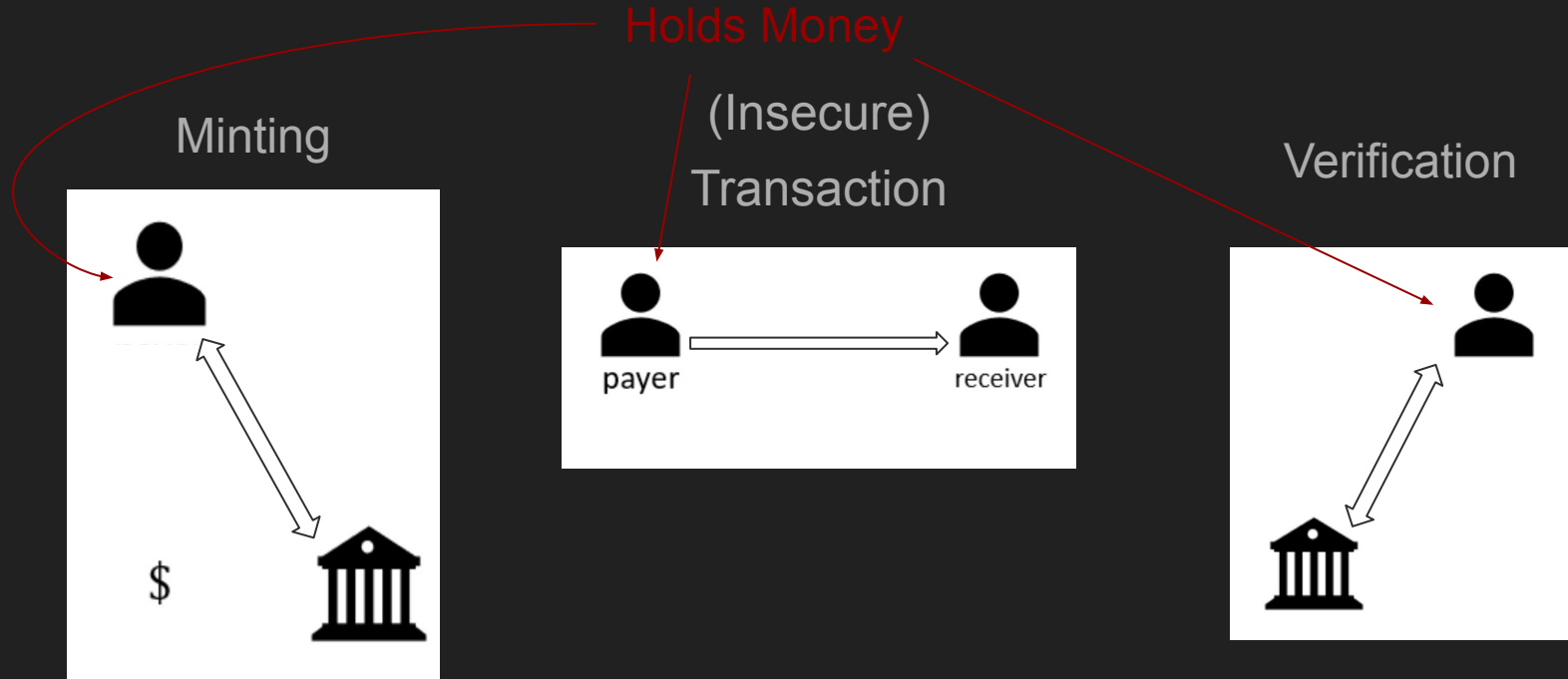
(Insecure)
Transaction



Verification



Quantum Money



Constructing Quantum Money

Constructing Quantum Money

(1) Choose a security parameter $\lambda \in \mathbb{Z}$

Constructing Quantum Money

- (1) Choose a security parameter $\lambda \in \mathbb{Z}$
- (2) Suppose post-quantum private key encryption exists

Constructing Quantum Money

- (1) Choose a security parameter $\lambda \in \mathbb{Z}$
- (2) Suppose post-quantum private key encryption exists
 - (i) $sk \leftarrow \text{keygen}(\lambda)$

Constructing Quantum Money

- (1) Choose a security parameter $\lambda \in \mathbb{Z}$
- (2) Suppose post-quantum private key encryption exists
 - (i) $sk \leftarrow \text{keygen}(\lambda)$
 - (ii) $ct \leftarrow \text{enc}(m, sk)$

Constructing Quantum Money

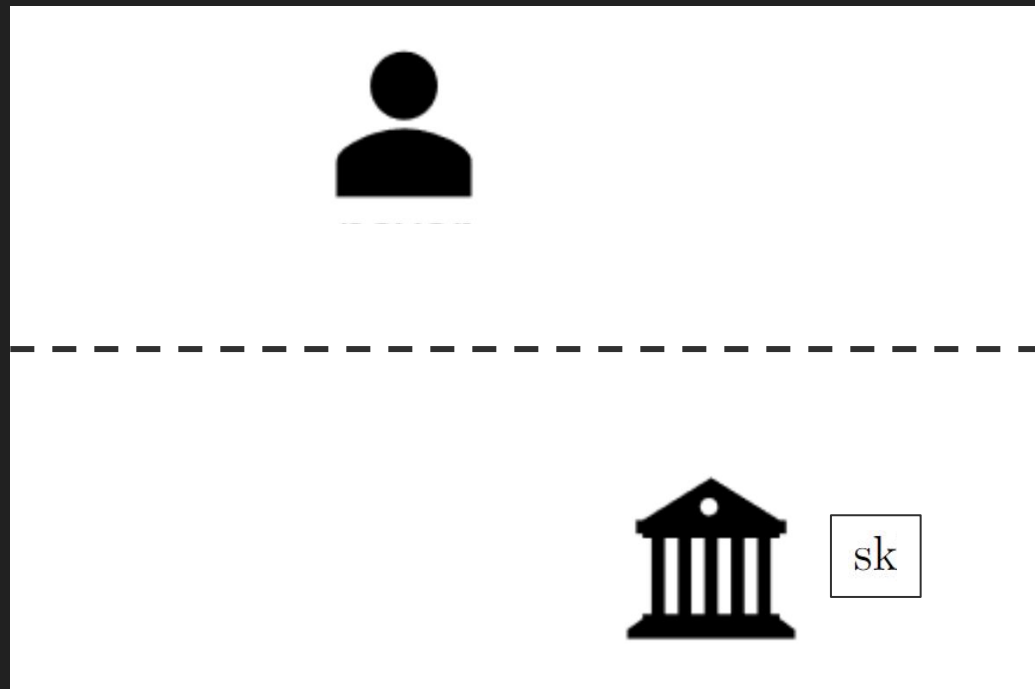
- (1) Choose a security parameter $\lambda \in \mathbb{Z}$
- (2) Suppose post-quantum private key encryption exists
 - (i) $sk \leftarrow \text{keygen}(\lambda)$
 - (ii) $ct \leftarrow \text{enc}(m, sk)$
 - (iii) $m \leftarrow \text{dec}(ct, sk)$

Constructing Quantum Money

- (1) Choose a security parameter $\lambda \in \mathbb{Z}$
- (2) Suppose post-quantum private key encryption exists
 - (i) $sk \leftarrow \text{keygen}(\lambda)$
 - (ii) $ct \leftarrow \text{enc}(m, sk)$
 - (iii) $m \leftarrow \text{dec}(ct, sk)$
- (3) Have the bank run keygen

Constructing Quantum Money

Minting



Constructing Quantum Money

Minting



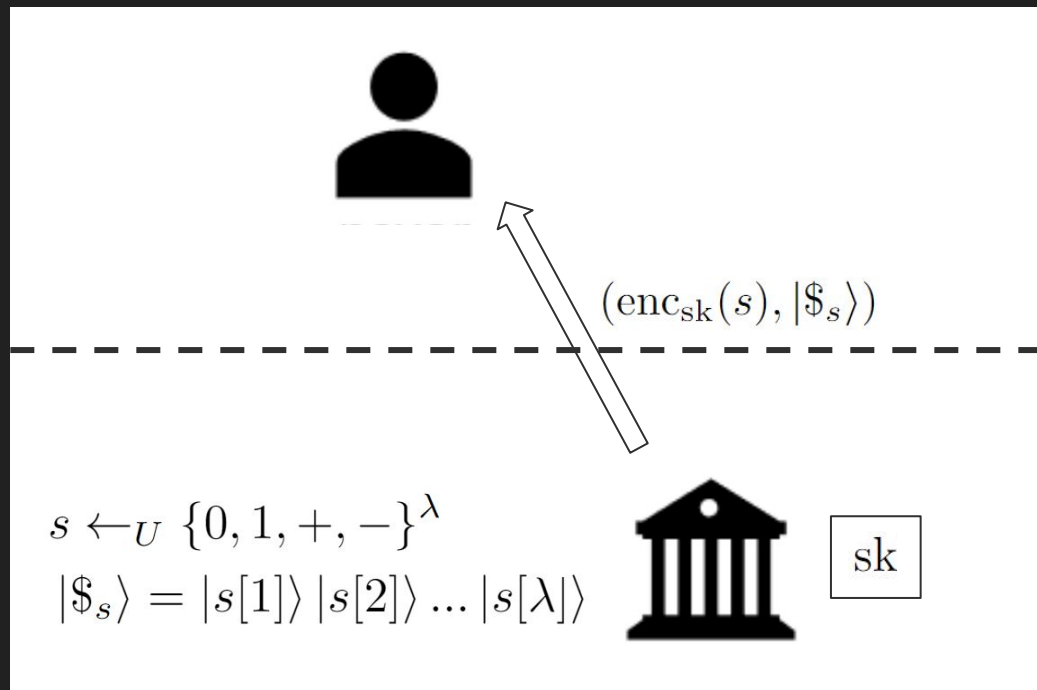
$$s \leftarrow_U \{0, 1, +, -\}^\lambda$$
$$|\$s\rangle = |s[1]\rangle |s[2]\rangle \dots |s[\lambda]\rangle$$



sk

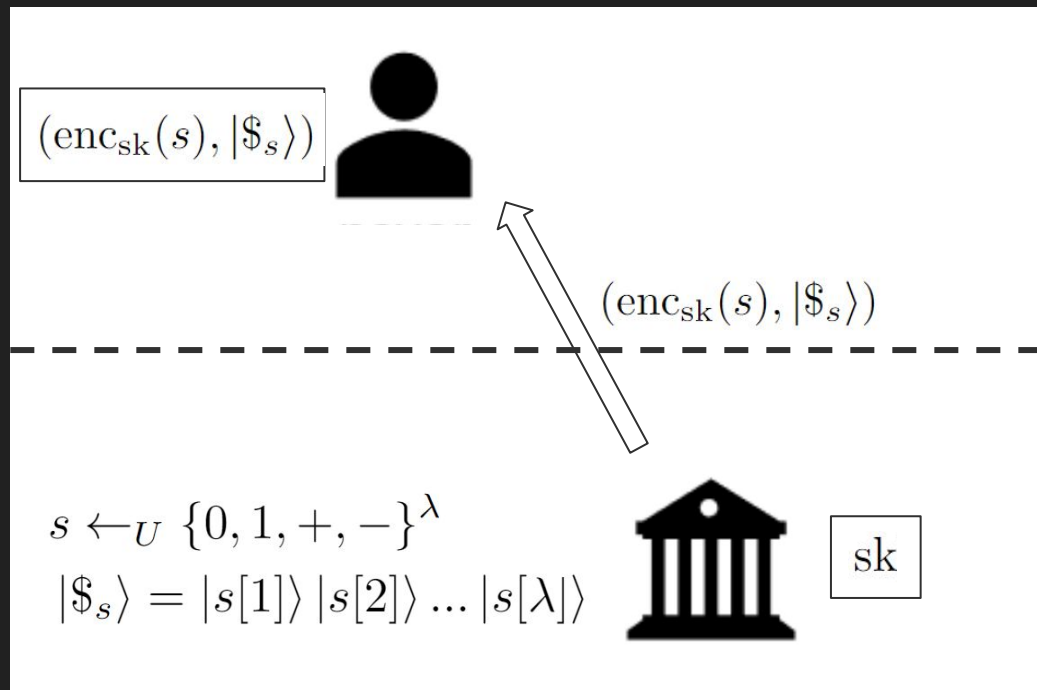
Constructing Quantum Money

Minting



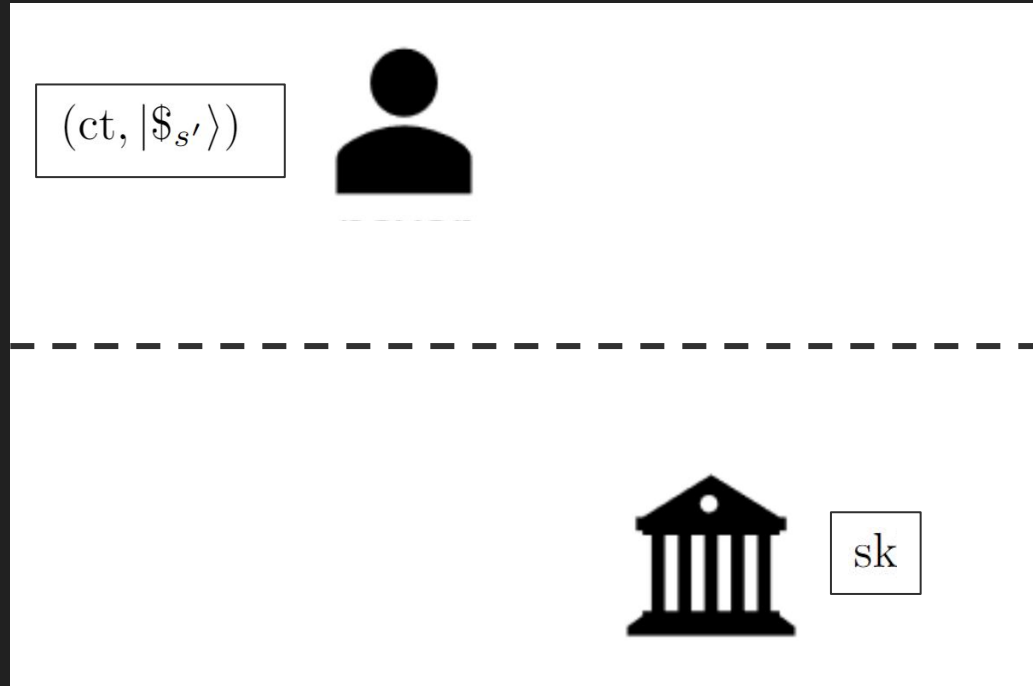
Constructing Quantum Money

Minting



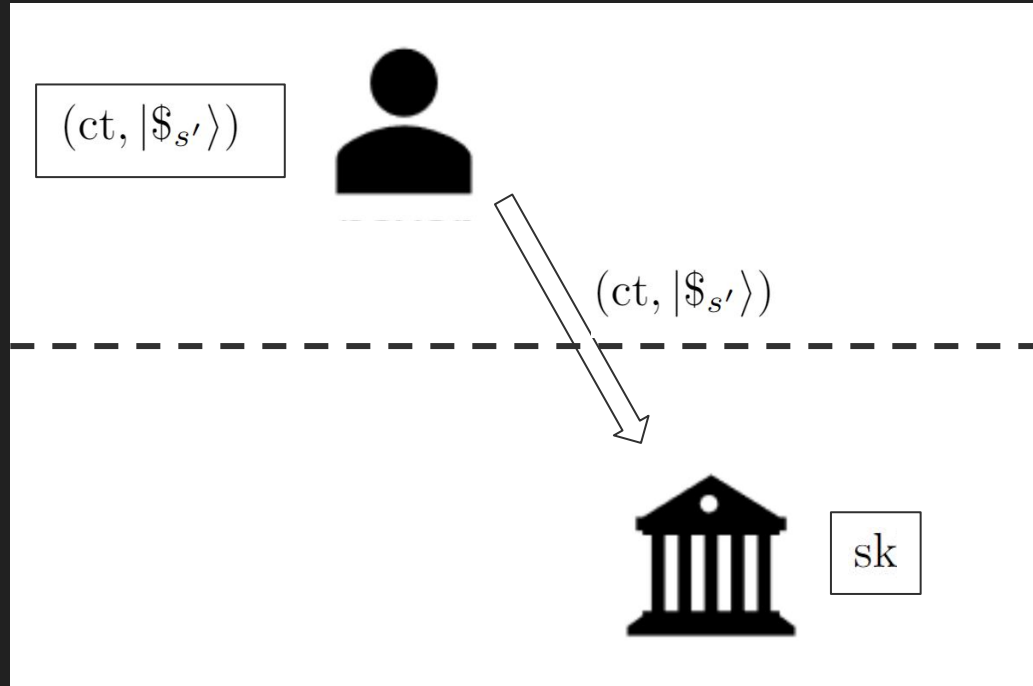
Constructing Quantum Money

Verification (1)



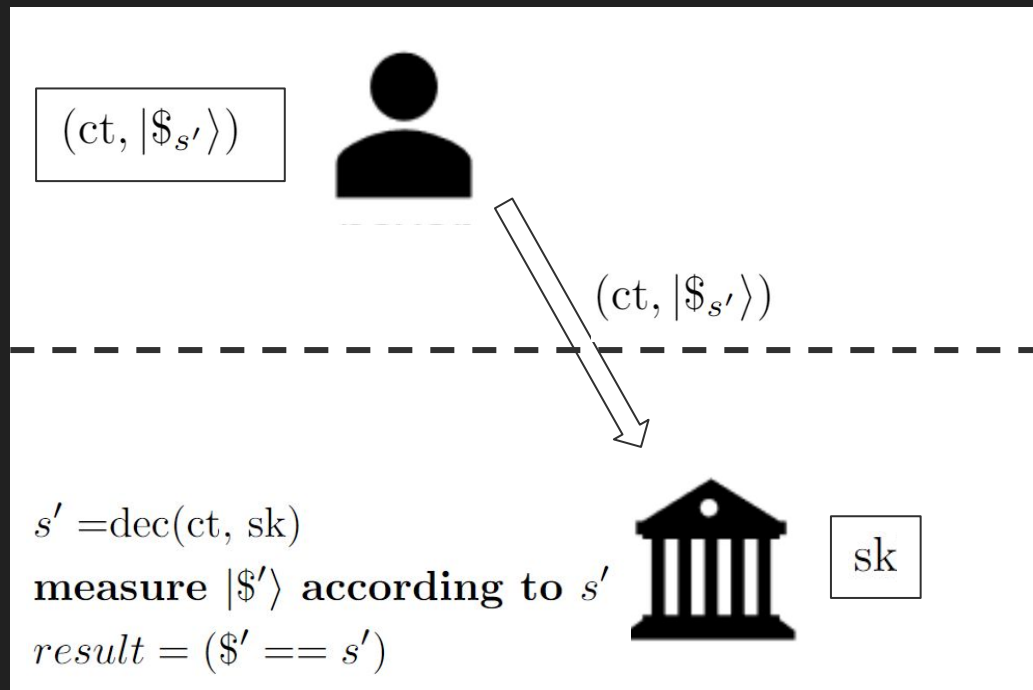
Constructing Quantum Money

Verification (1)



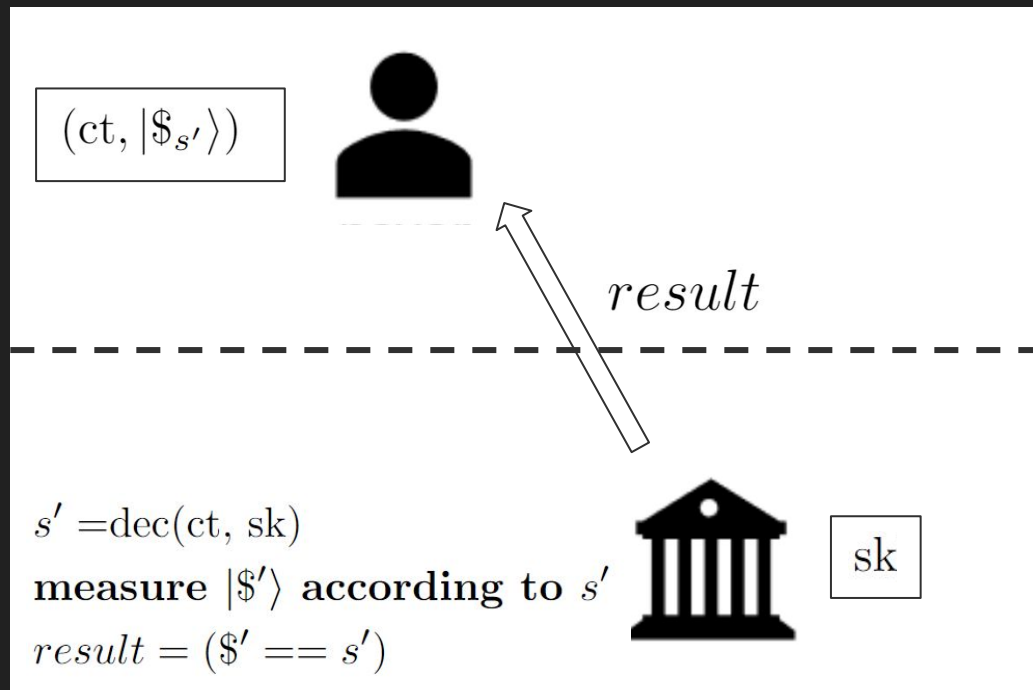
Constructing Quantum Money

Verification (1)



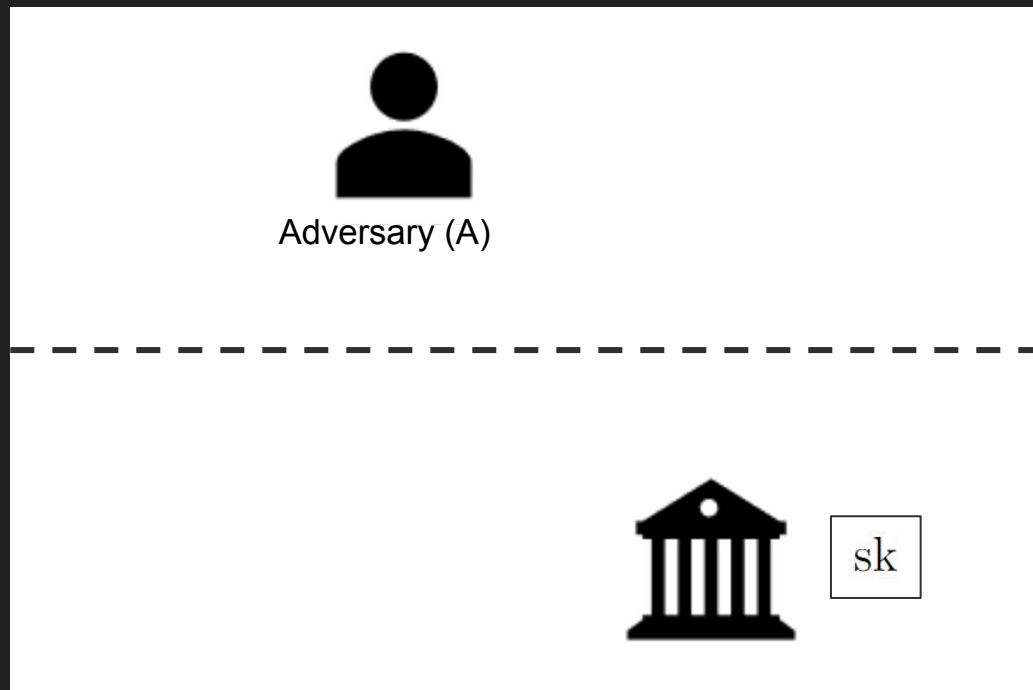
Constructing Quantum Money

Verification (2)



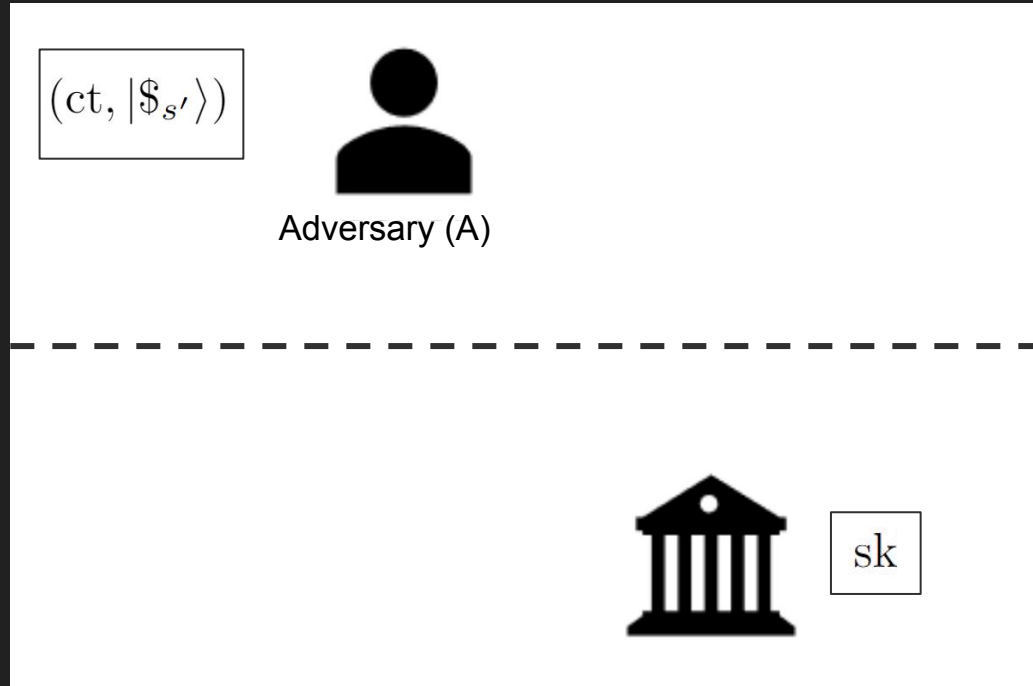
Constructing Quantum Money

Security Game (Mini scheme)



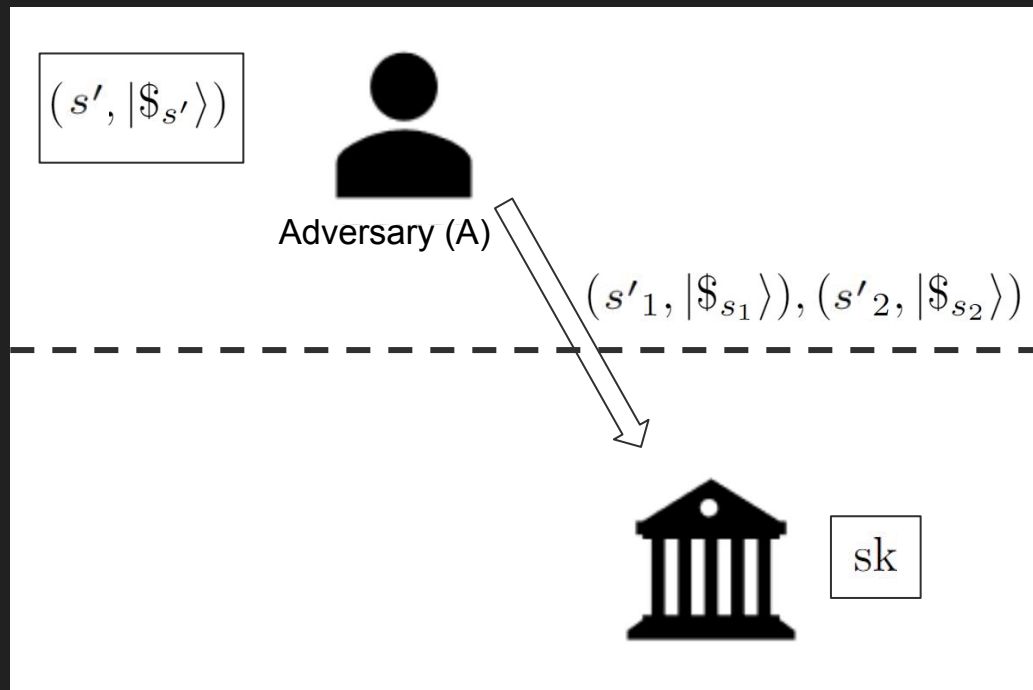
Constructing Quantum Money

Security Game (Mini scheme)



Constructing Quantum Money

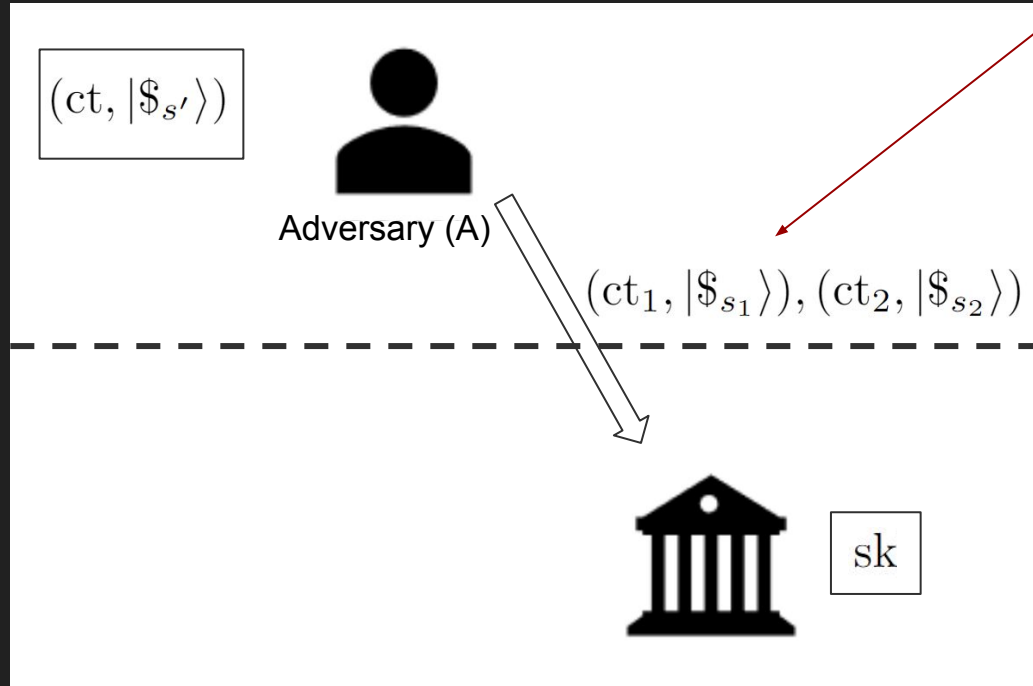
Security Game (Mini scheme)



Constructing Quantum Money

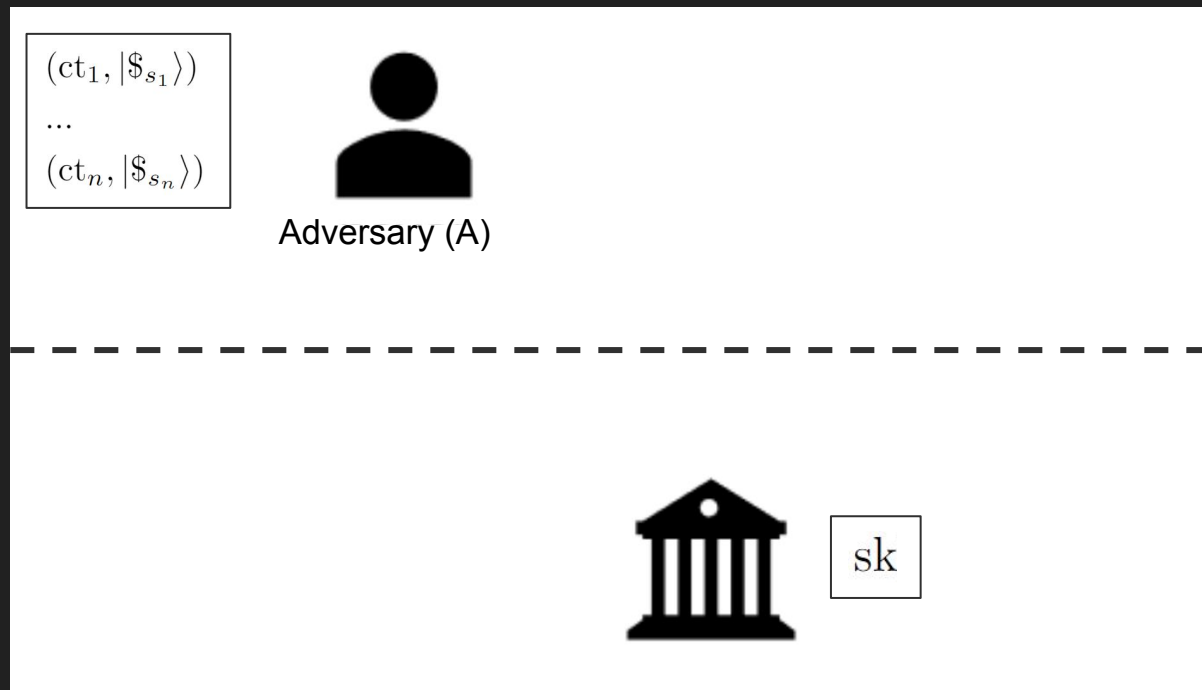
Security Game (Mini scheme)

A wins if both pass



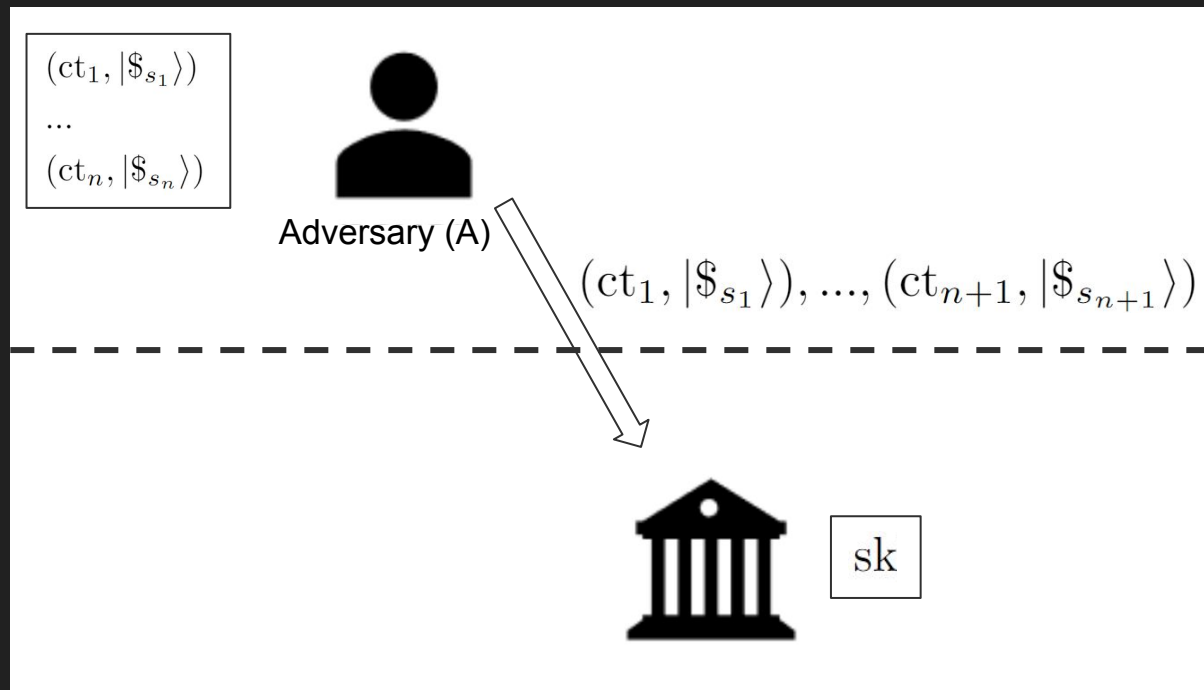
Constructing Quantum Money

Security Game (Full Scheme)



Constructing Quantum Money

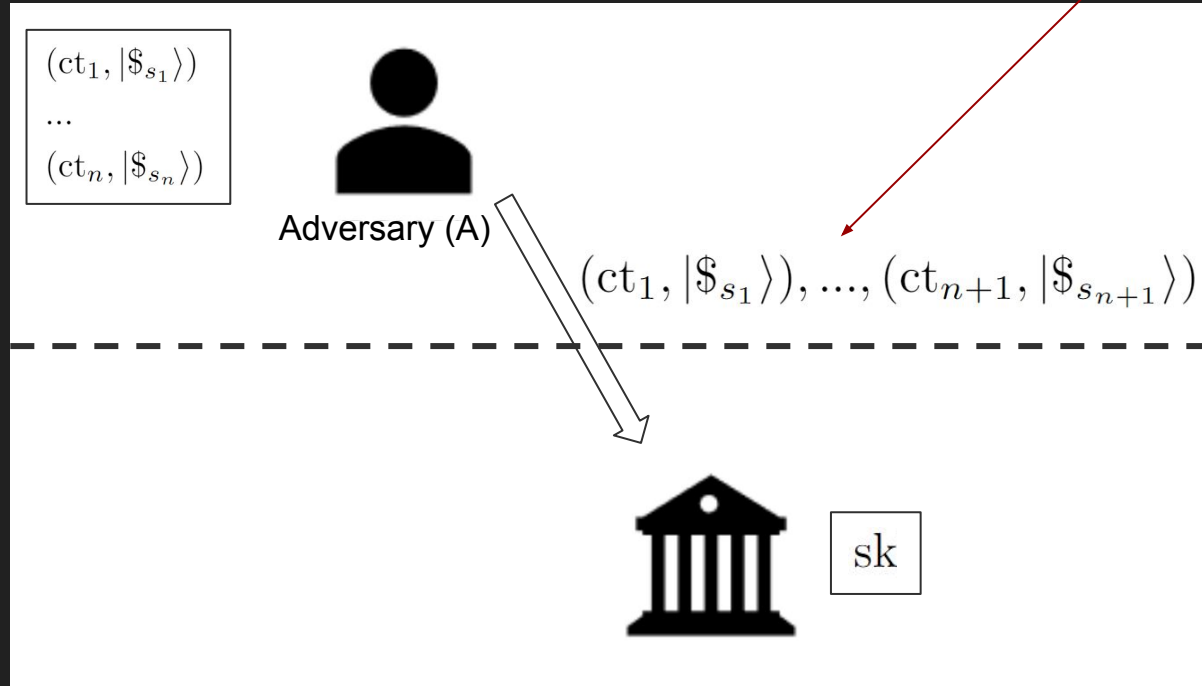
Security Game (Full Scheme)



Constructing Quantum Money

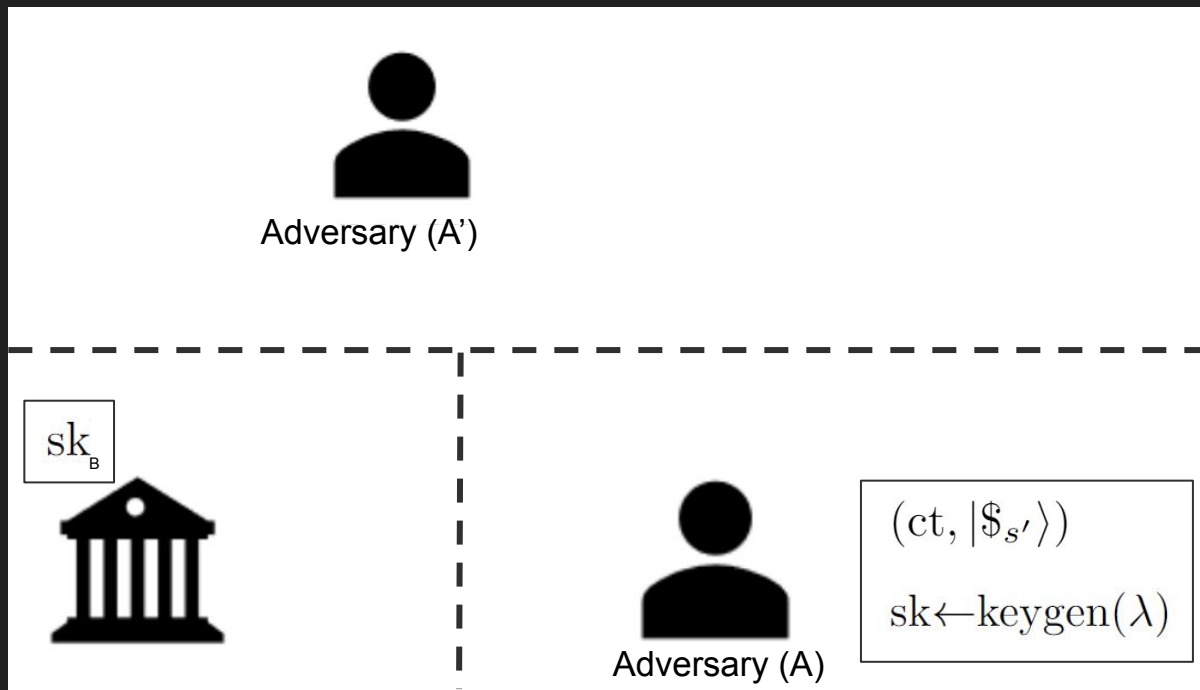
Security Game (Full Scheme)

A wins if all pass



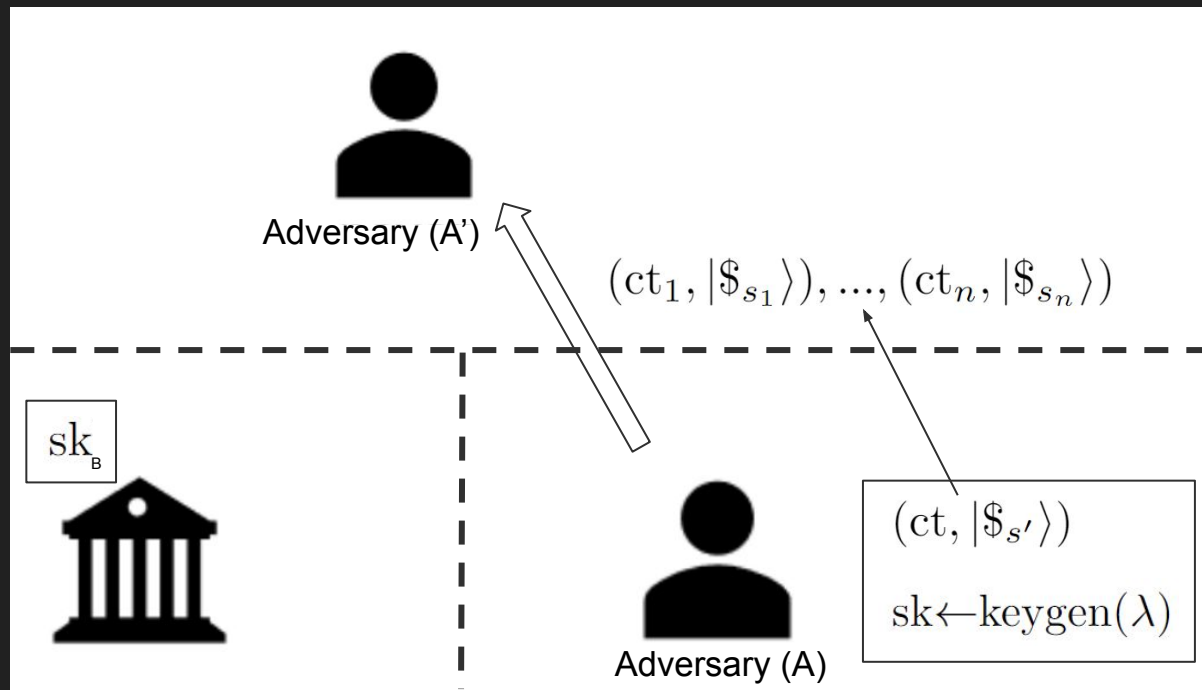
Constructing Quantum Money

Security Game (Full to Mini)



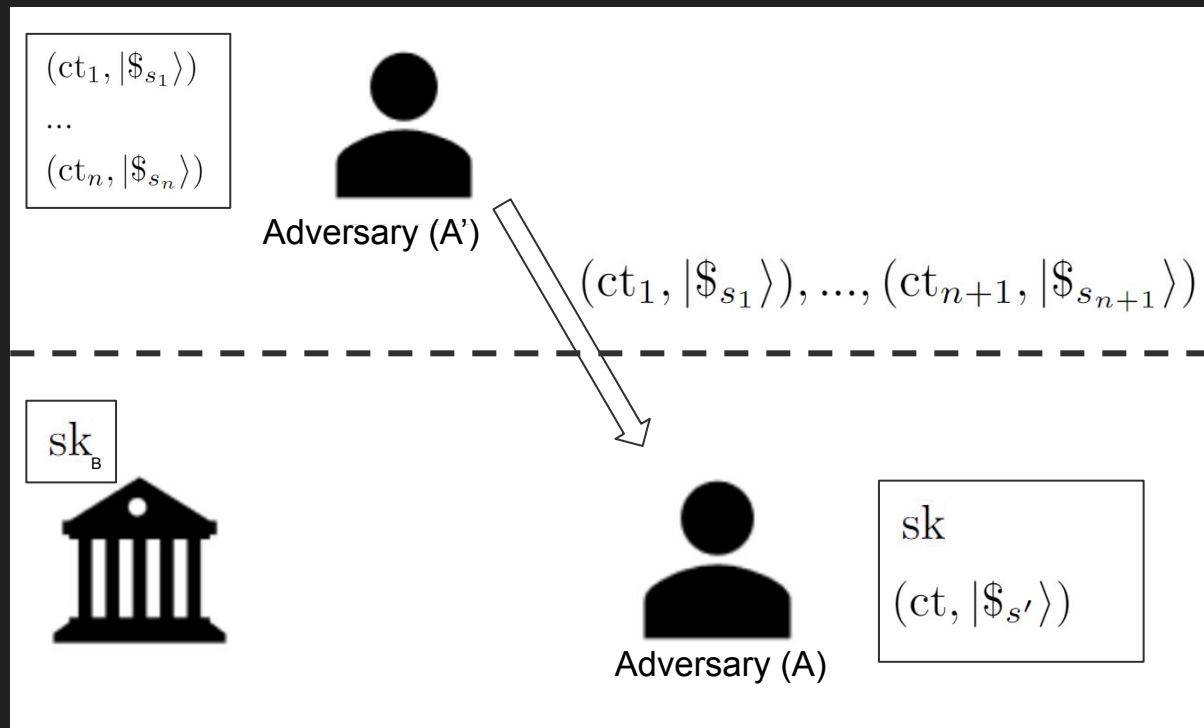
Constructing Quantum Money

Security Game (Full to Mini)



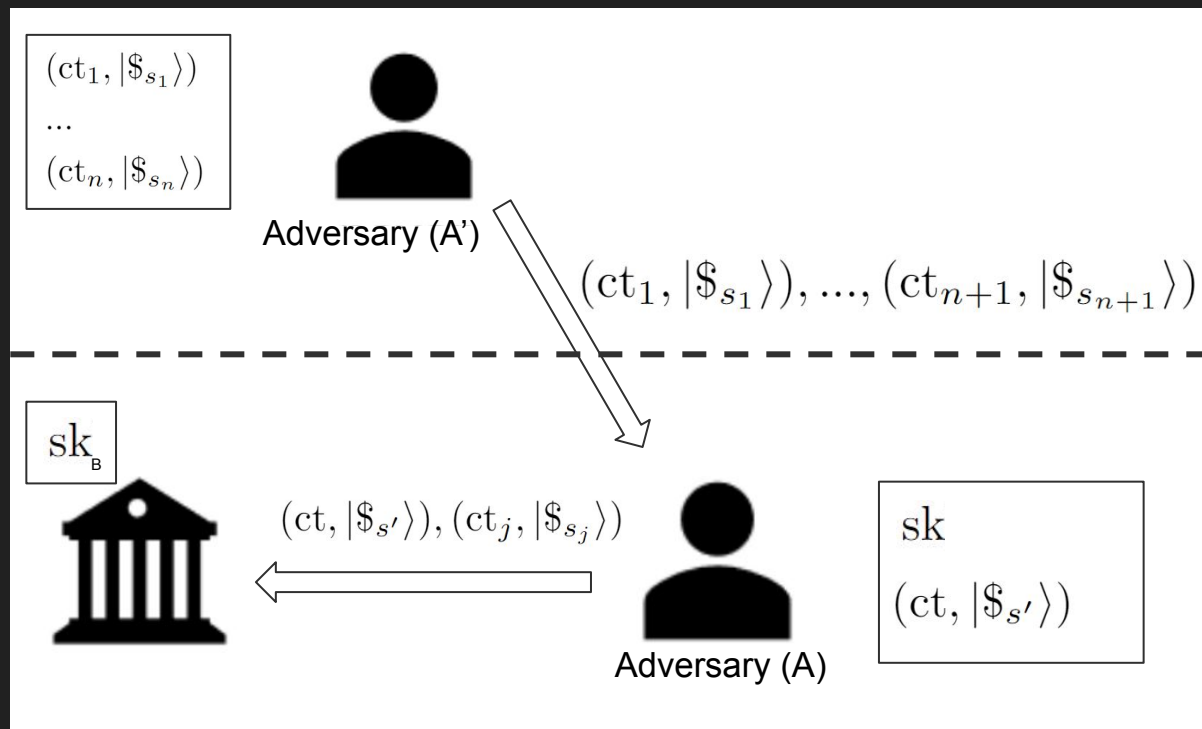
Constructing Quantum Money

Security Game (Full to Mini)



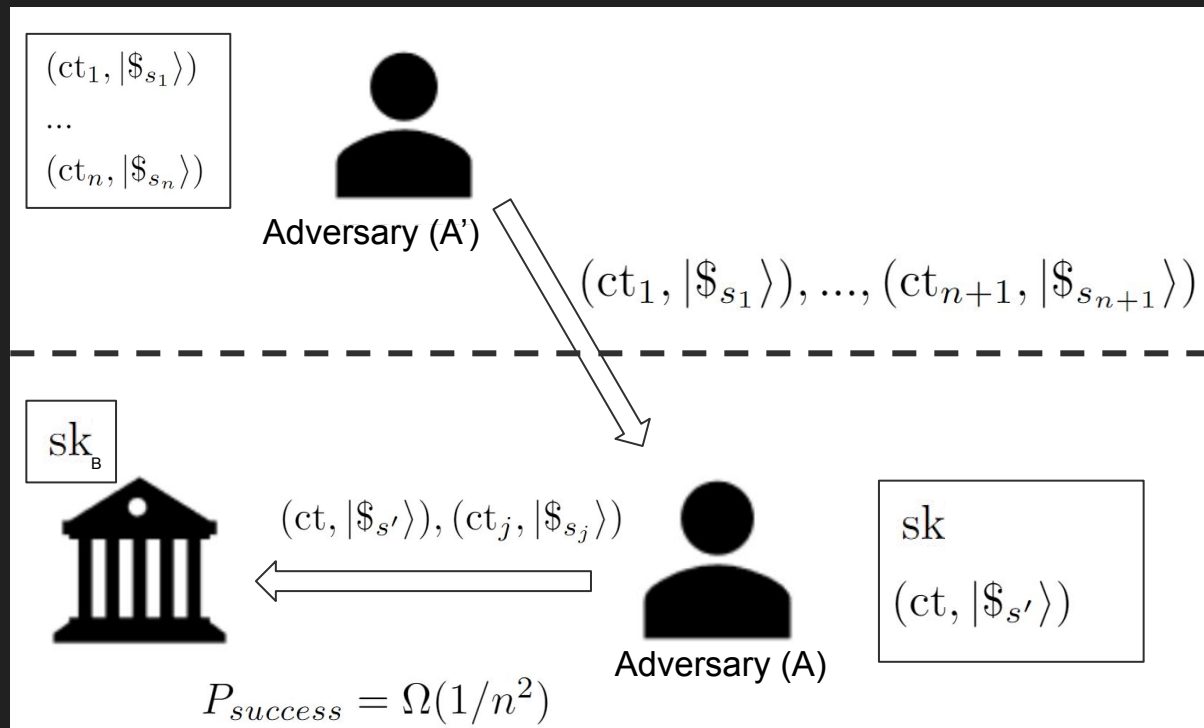
Constructing Quantum Money

Security Game (Full to Mini)



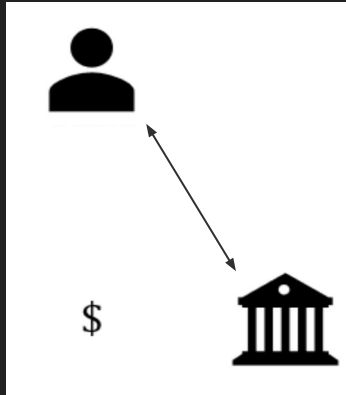
Constructing Quantum Money

Security Game (Full to Mini)

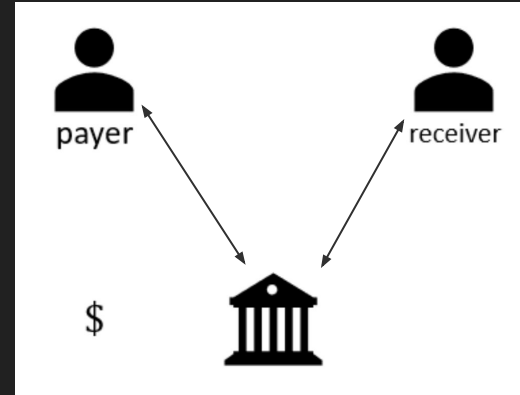


Private Key Semi-Quantum Money

Minting



Transaction



Review: Trapdoor Claw-Free Functions (TCF)

$$k, t_k \leftarrow \text{keygen}(\lambda)$$

Review: Trapdoor Claw-Free Functions (TCF)

$$k, t_k \leftarrow \text{keygen}(\lambda)$$

$$\mathcal{X} = \{0, 1\}^n$$

$$\mathcal{Y} = \{0, 1\}^m$$

Review: Trapdoor Claw-Free Functions (TCF)

$$k, t_k \leftarrow \text{keygen}(\lambda)$$

$$\mathcal{X} = \{0, 1\}^n$$

$$\mathcal{Y} = \{0, 1\}^m$$

$$\text{both injective, same range} \begin{cases} f_{k,0} : \mathcal{X} \rightarrow \mathcal{Y} \\ f_{k,1} : \mathcal{X} \rightarrow \mathcal{Y} \end{cases}$$

Review: Trapdoor Claw-Free Functions (TCF)

$$k, t_k \leftarrow \text{keygen}(\lambda)$$

$$\mathcal{X} = \{0, 1\}^n$$

$$\mathcal{Y} = \{0, 1\}^m$$

both injective, same range

$$\begin{cases} f_{k,0} : \mathcal{X} \rightarrow \mathcal{Y} \\ f_{k,1} : \mathcal{X} \rightarrow \mathcal{Y} \end{cases}$$

Claw: (x_0, x_1, y) s.t. $f_{k,0}(x_0) = f_{k,1}(x_1) = y$

Review: Trapdoor Claw-Free Functions (TCF)

$$k, t_k \leftarrow \text{keygen}(\lambda)$$

$$\mathcal{X} = \{0, 1\}^n$$

$$\mathcal{Y} = \{0, 1\}^m$$

both injective, same range $\begin{cases} f_{k,0} : \mathcal{X} \rightarrow \mathcal{Y} \\ f_{k,1} : \mathcal{X} \rightarrow \mathcal{Y} \end{cases}$

Claw: (x_0, x_1, y) s.t. $f_{k,0}(x_0) = f_{k,1}(x_1) = y$

Claw cannot be found efficiently

Review: Trapdoor Claw-Free Functions (TCF)

$$k, t_k \leftarrow \text{keygen}(\lambda)$$

$$\mathcal{X} = \{0, 1\}^n$$

$$\mathcal{Y} = \{0, 1\}^m$$

both injective, same range $\begin{cases} f_{k,0} : \mathcal{X} \rightarrow \mathcal{Y} \\ f_{k,1} : \mathcal{X} \rightarrow \mathcal{Y} \end{cases}$

Claw: (x_0, x_1, y) s.t. $f_{k,0}(x_0) = f_{k,1}(x_1) = y$

Claw cannot be found efficiently

Efficient \mathcal{A} takes $(t_k, y) \rightarrow (x_0, x_1)$

Review: Learning With Errors (LWE)

$$\mathbf{A} \leftarrow_U \mathbb{Z}_q^{n \times m}, \mathbf{s} \leftarrow_U \mathbb{Z}_q^n, \mathbf{e} \leftarrow_U \chi^m, \mathbf{u} \leftarrow_U \mathbb{Z}_q^m$$

Review: Learning With Errors (LWE)

$$\mathbf{A} \leftarrow_U \mathbb{Z}_q^{n \times m}, \mathbf{s} \leftarrow_U \mathbb{Z}_q^n, \mathbf{e} \leftarrow_U \chi^m, \mathbf{u} \leftarrow_U \mathbb{Z}_q^m$$

$$(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}) \stackrel{C}{\approx} (\mathbf{A}, \mathbf{u})$$

Review: Learning With Errors (LWE)

$$\mathbf{A} \leftarrow_U \mathbb{Z}_q^{n \times m}, \mathbf{s} \leftarrow_U \mathbb{Z}_q^n, \mathbf{e} \leftarrow_U \chi^m, \mathbf{u} \leftarrow_U \mathbb{Z}_q^m$$

$$(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}) \stackrel{C}{\approx} (\mathbf{A}, \mathbf{u})$$

(Quantumly) Hard to do better than $\frac{1}{2} + \text{negl}(\lambda)$
for some $n, m, \log(q) = \text{poly}(\lambda)$

Review: TCF from LWE

$$k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$$
$$t_k = \mathbf{s}$$

Review: TCF from LWE

$$k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$$

$$t_k = \mathbf{s}$$

$$f_{k,0}(x) = \mathbf{A}x + \mathbf{e}$$

$$f_{k,1}(x) = \mathbf{A}x + \mathbf{A}\mathbf{s} + \mathbf{e}$$

Review: TCF from LWE

$$k = (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$$

$$t_k = \mathbf{s}$$

$$f_{k,0}(x) = \mathbf{A}x + \mathbf{e}$$

$$f_{k,1}(x) = \mathbf{A}x + \mathbf{A}\mathbf{s} + \mathbf{e}$$

Given **Claw**:

$$f_{k,0}(x_0) - f_{k,1}(x_1) = \mathbf{A}\mathbf{s} \rightarrow \mathbf{s}$$

Claw States

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |0\rangle$$

Claw States

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |0\rangle$$

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |f_b(x)\rangle$$

Claw States

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |0\rangle$$

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |f_b(x)\rangle$$

$$|C\rangle |y\rangle = \frac{1}{\sqrt{2}}(|x_0\rangle |0\rangle + |x_1\rangle |1\rangle) |y\rangle$$

Claw States

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |0\rangle$$

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |f_b(x)\rangle$$

$$|C\rangle |y\rangle = \frac{1}{\sqrt{2}} (|x_0\rangle |0\rangle + |x_1\rangle |1\rangle) |y\rangle$$

Computational 

(x_b, b) w/ $f_{k,b}(x_b) = y$

Claw States

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |0\rangle$$

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |f_b(x)\rangle$$

$$|C\rangle |y\rangle = \frac{1}{\sqrt{2}}(|x_0\rangle |0\rangle + |x_1\rangle |1\rangle) |y\rangle$$

Computational 

(x_b, b) w/ $f_{k,b}(x_b) = y$

 Hadamard

(d, i) w/ $d \cdot (x_0 \oplus x_1) = i$


Claw States

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |0\rangle$$

$$\sum_{x \in \mathcal{X}, b \in \{0,1\}} |x\rangle |b\rangle |f_b(x)\rangle$$

$$|C\rangle |y\rangle = \frac{1}{\sqrt{2}}(|x_0\rangle |0\rangle + |x_1\rangle |1\rangle) |y\rangle$$

Computational 

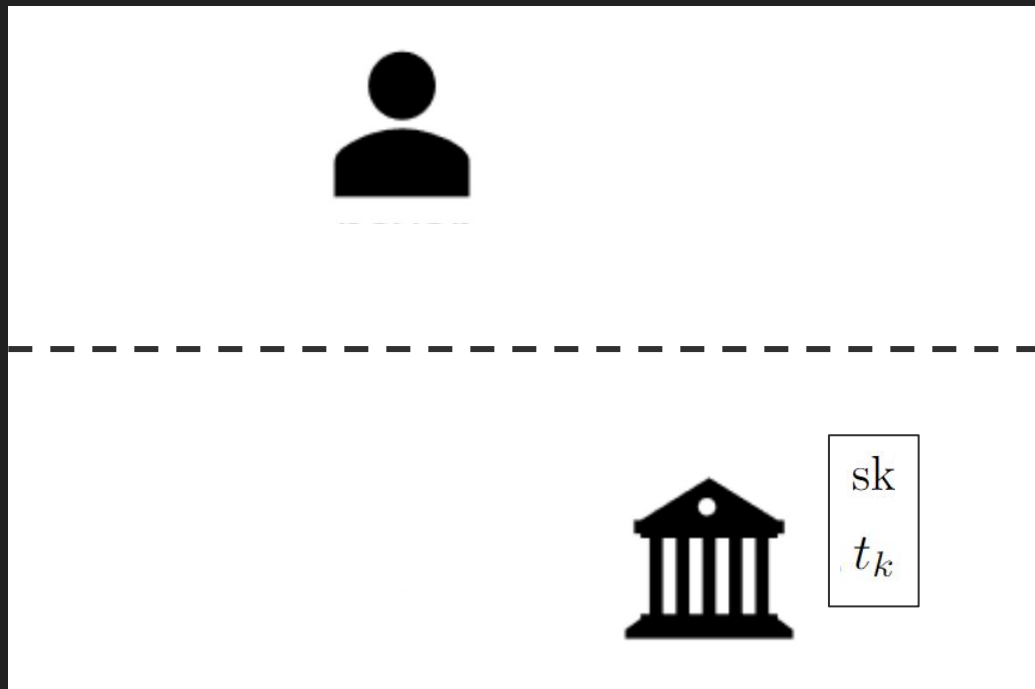
 Hadamard

$$(x_b, b) \text{ w/ } f_{k,b}(x_b) = y \longleftrightarrow \text{AHB} \text{ } \longleftrightarrow (d, i) \text{ w/ } d \cdot (x_0 \oplus x_1) = i$$

AHB: Can't get both
"1-of-2 Puzzle"

Constructing Semi-Quantum Money (Attempt 1)

Minting



Constructing Semi-Quantum Money (Attempt 1)

Minting



$$|\psi\rangle \leftarrow_U |C\rangle |y\rangle$$

$$s = y$$

$$|\$s\rangle = |C\rangle$$

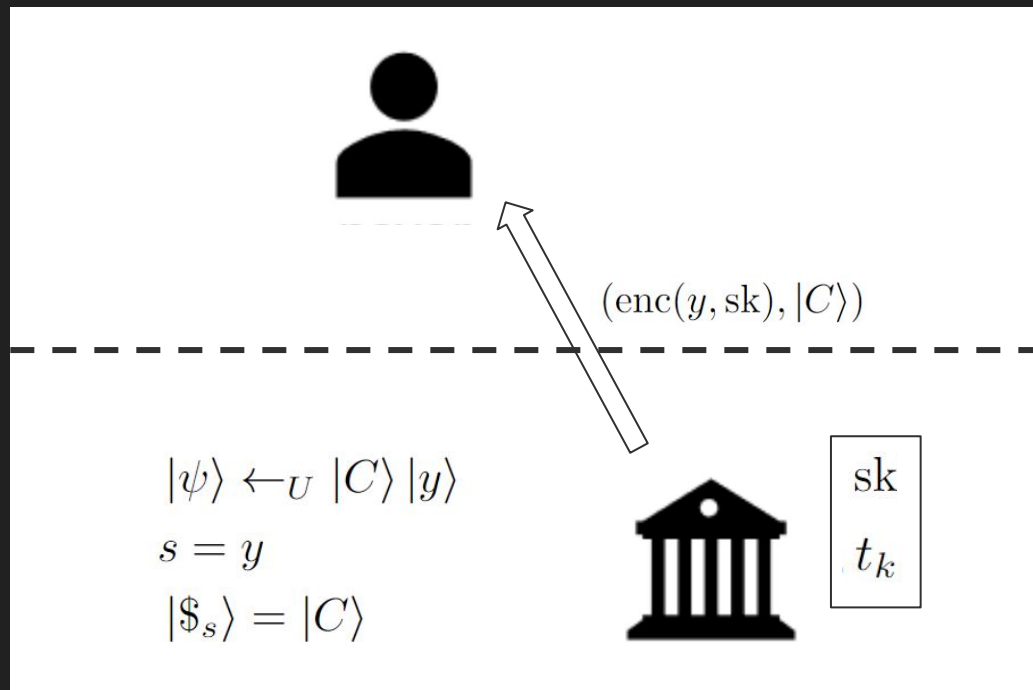


sk

t_k

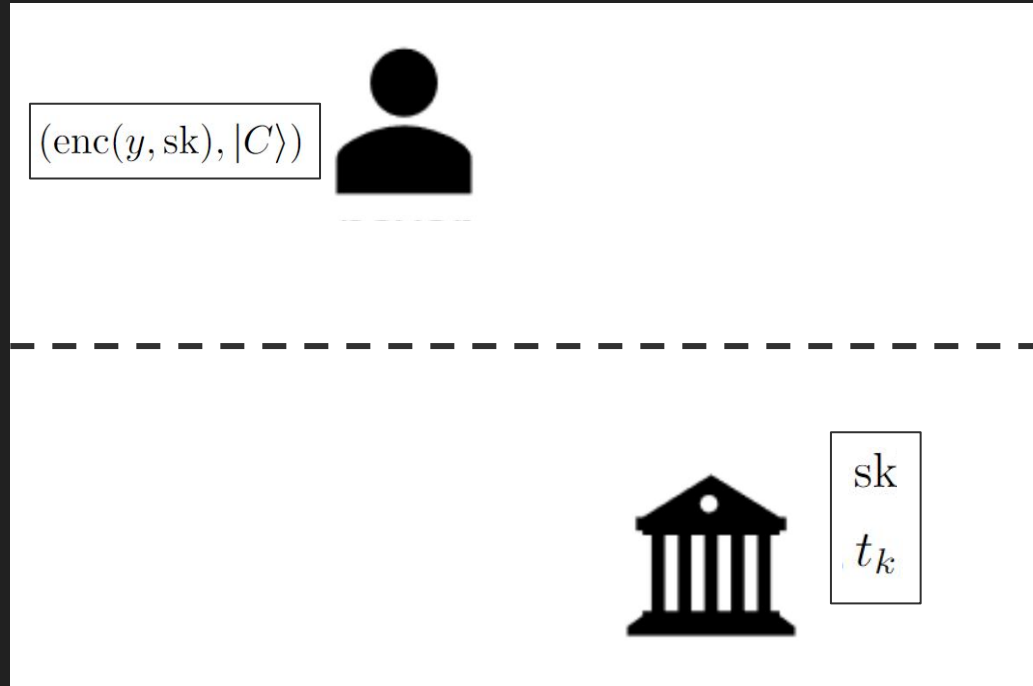
Constructing Semi-Quantum Money (Attempt 1)

Minting



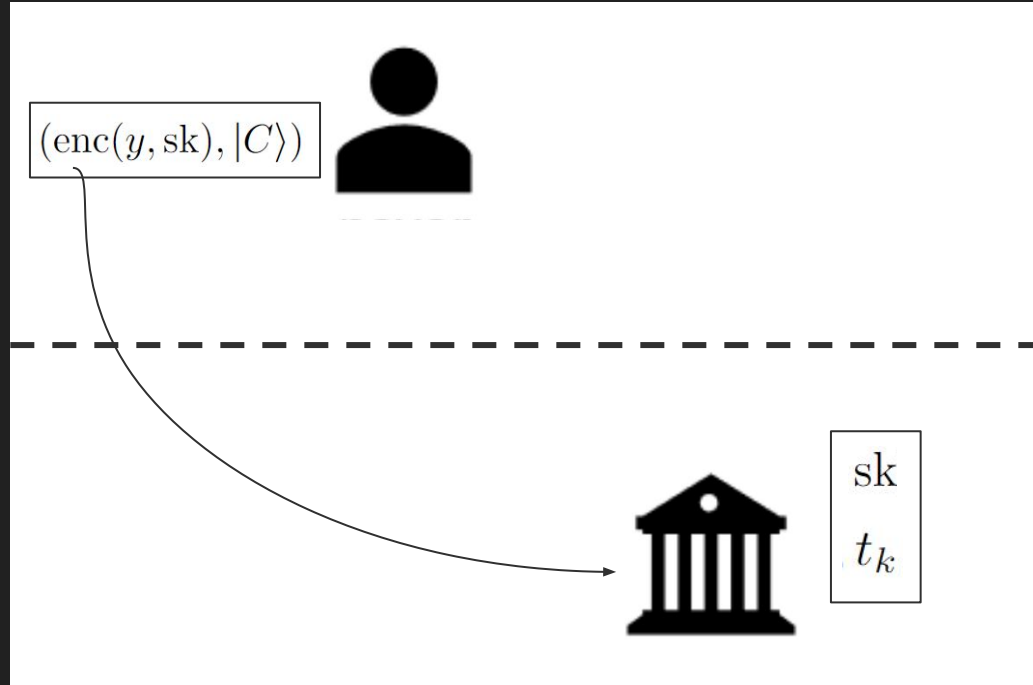
Constructing Semi-Quantum Money (Attempt 1)

Verification



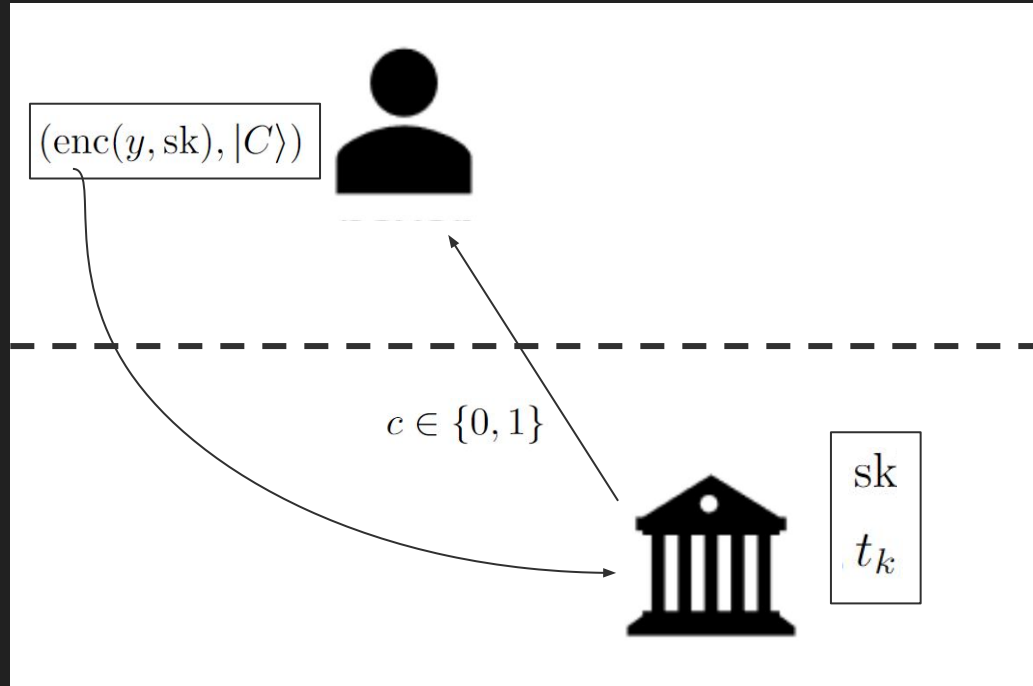
Constructing Semi-Quantum Money (Attempt 1)

Verification



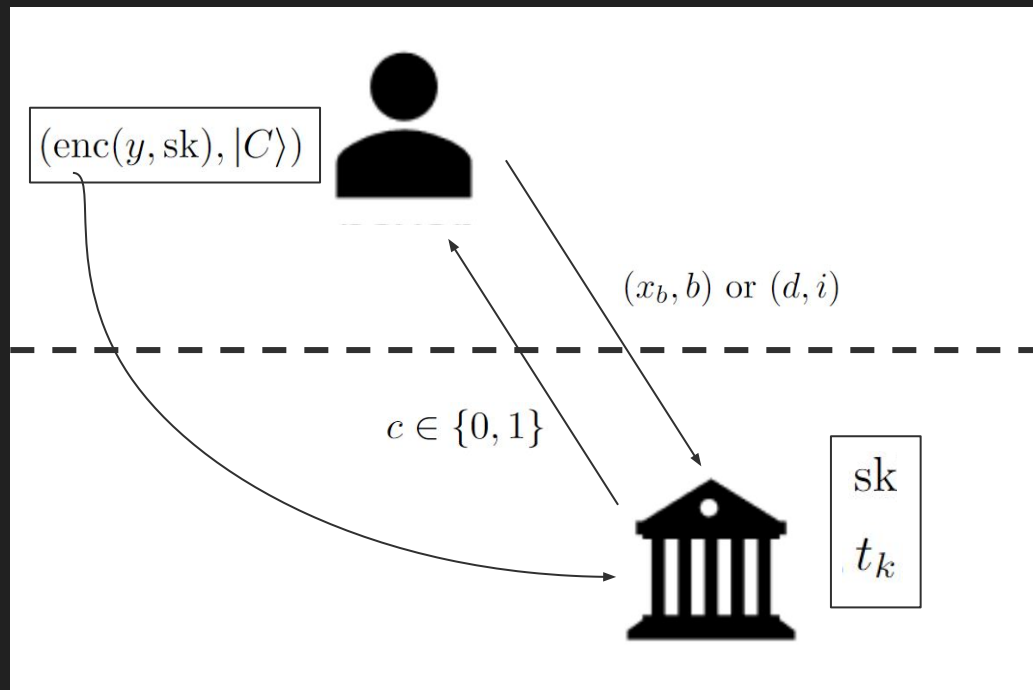
Constructing Semi-Quantum Money (Attempt 1)

Verification



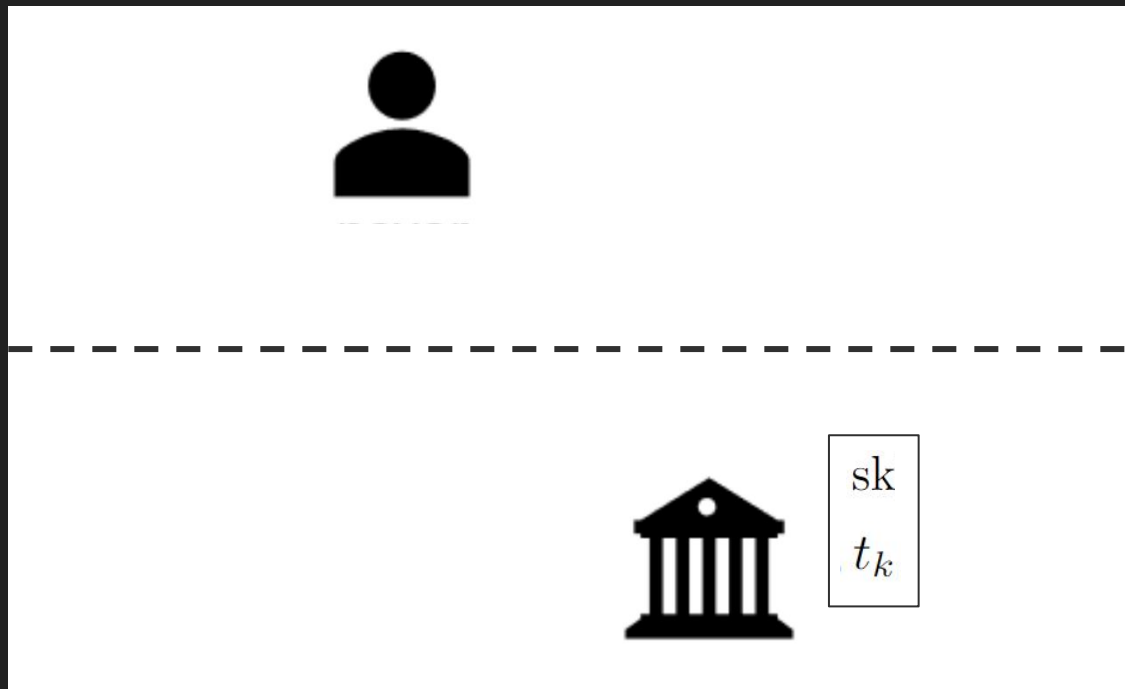
Constructing Semi-Quantum Money (Attempt 1)

Verification



Constructing Semi-Quantum Money (Attempt 2)

Minting



Constructing Semi-Quantum Money (Attempt 2)

Minting



$$|\psi\rangle \leftarrow_U |C\rangle |y\rangle$$

$$s = y$$

$$|\$s\rangle = |C\rangle$$

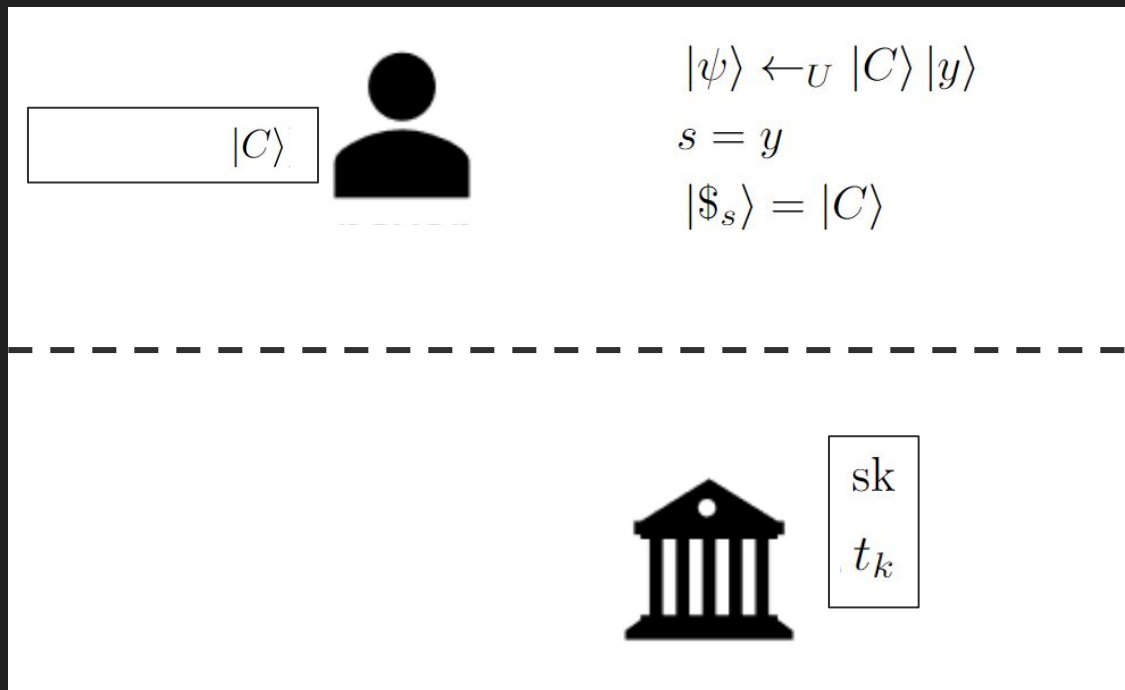


sk

t_k

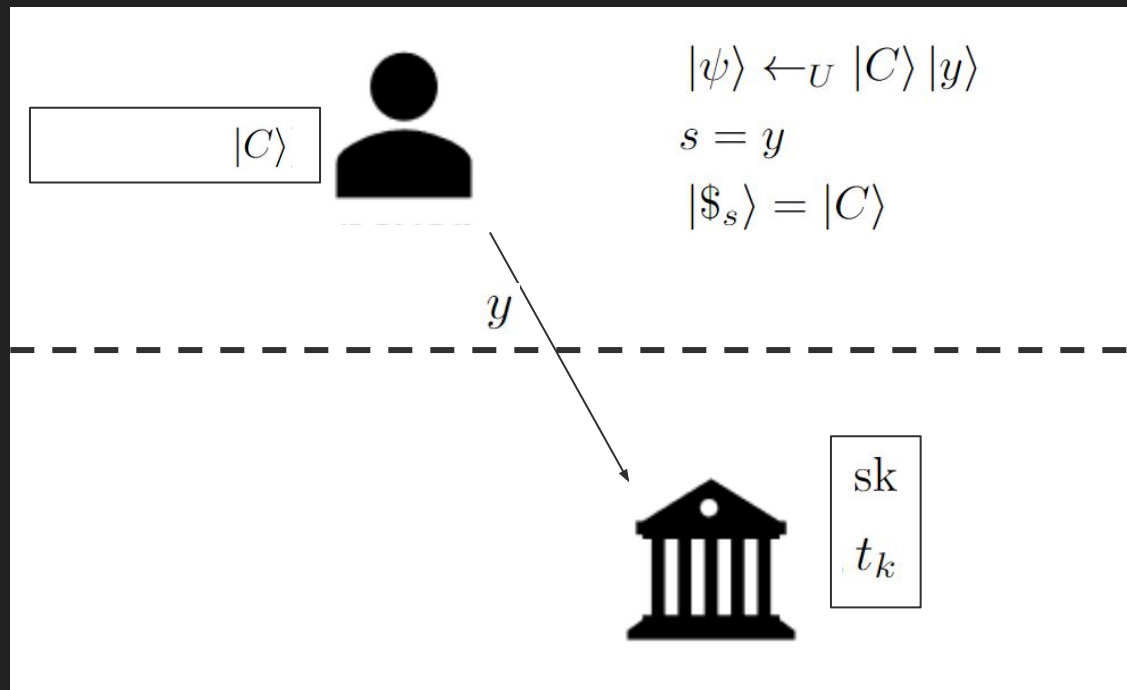
Constructing Semi-Quantum Money (Attempt 2)

Minting



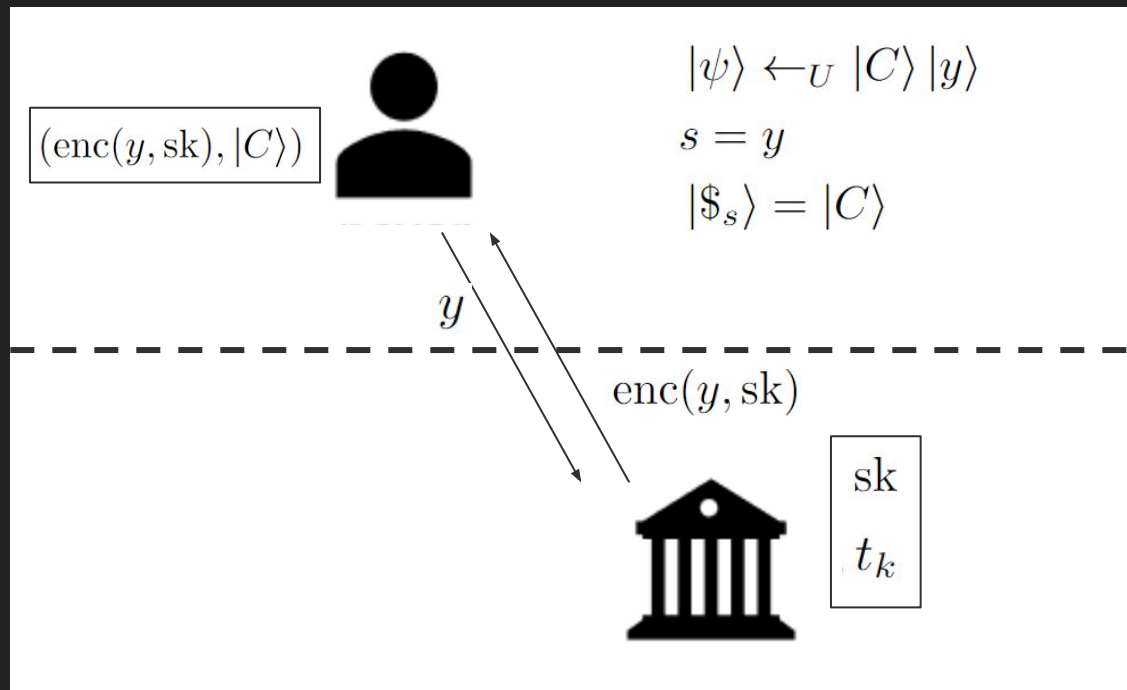
Constructing Semi-Quantum Money (Attempt 2)

Minting



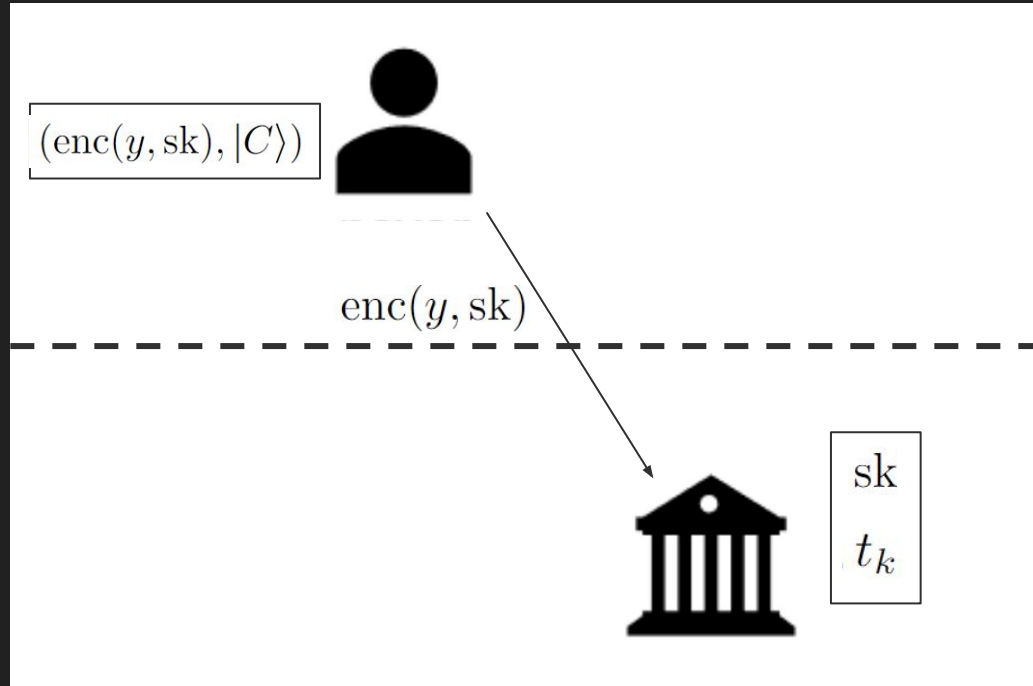
Constructing Semi-Quantum Money (Attempt 2)

Minting



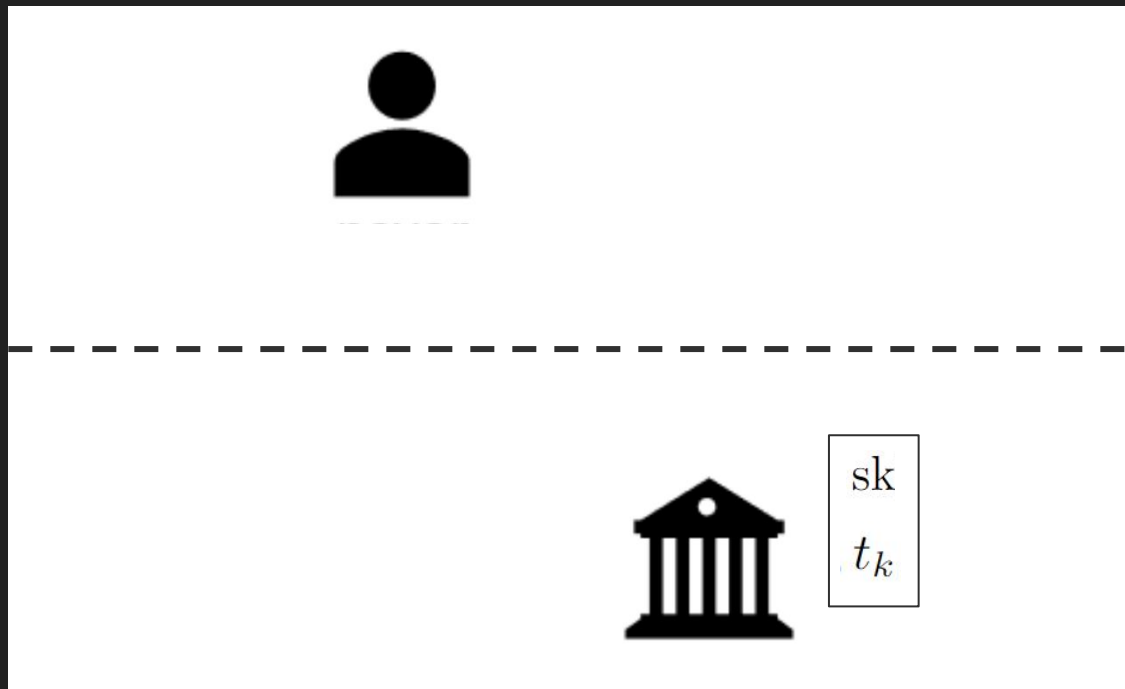
Constructing Semi-Quantum Money (Attempt 2)

Pre-Verification



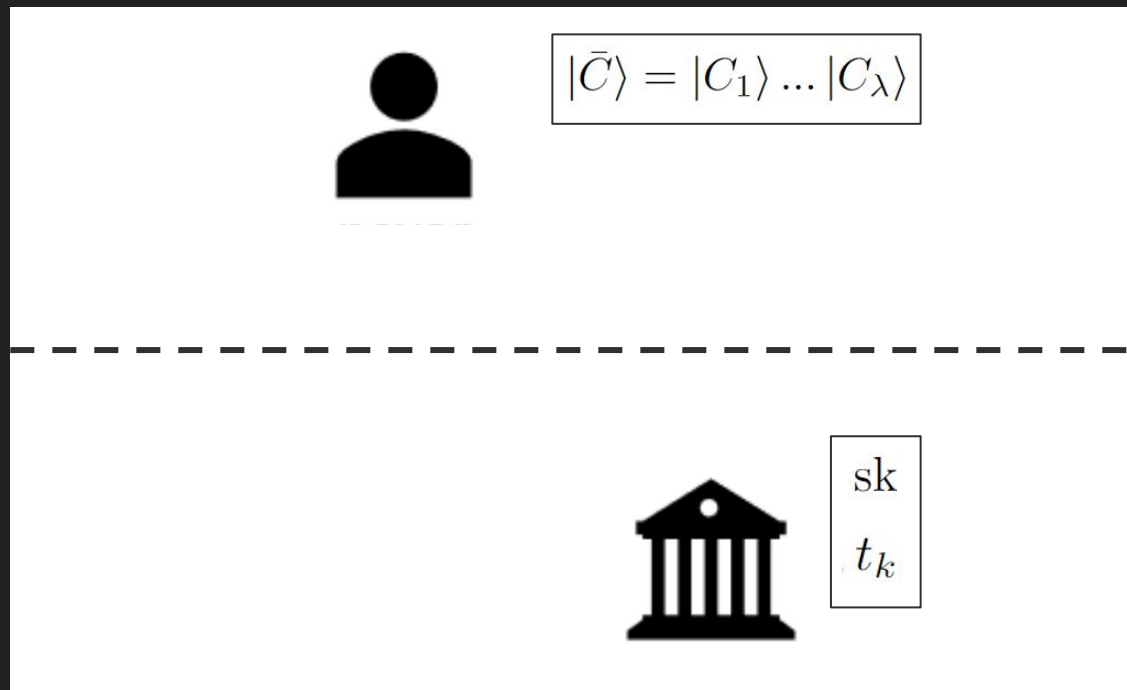
Constructing Semi-Quantum Money

Minting



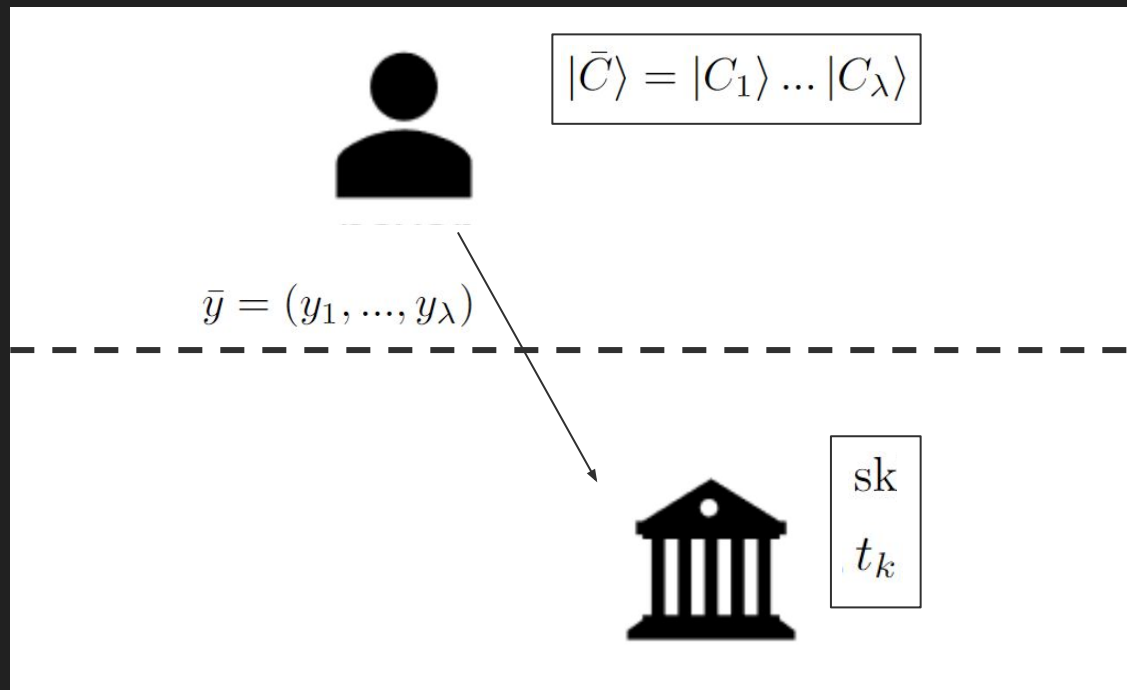
Constructing Semi-Quantum Money

Minting



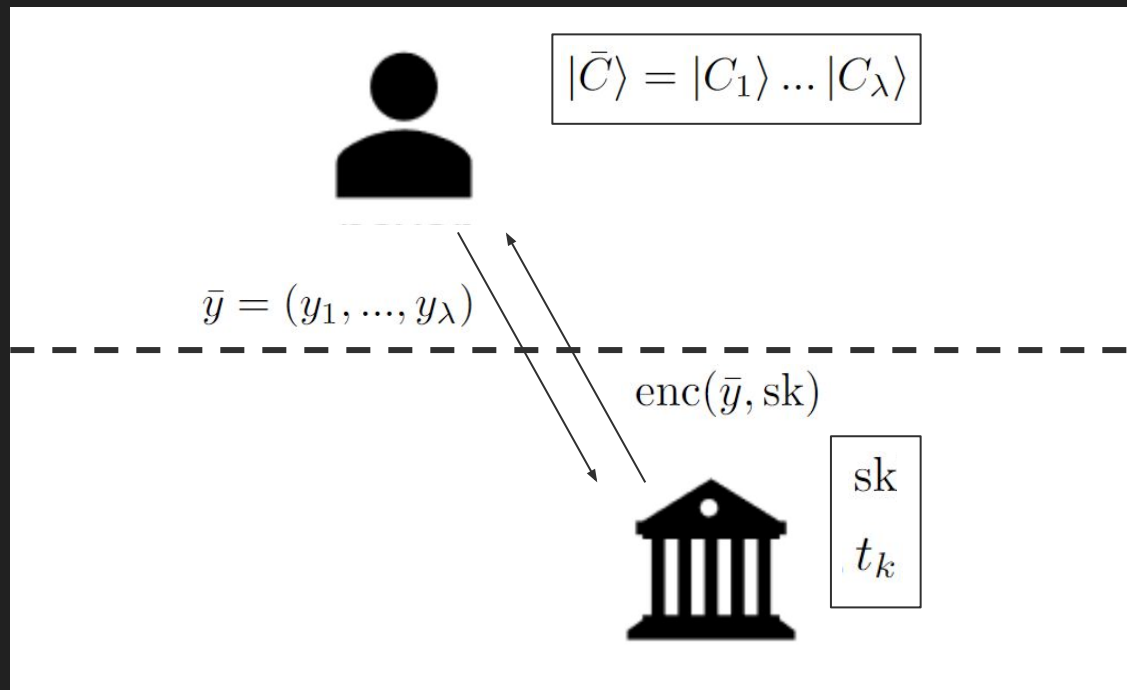
Constructing Semi-Quantum Money

Minting



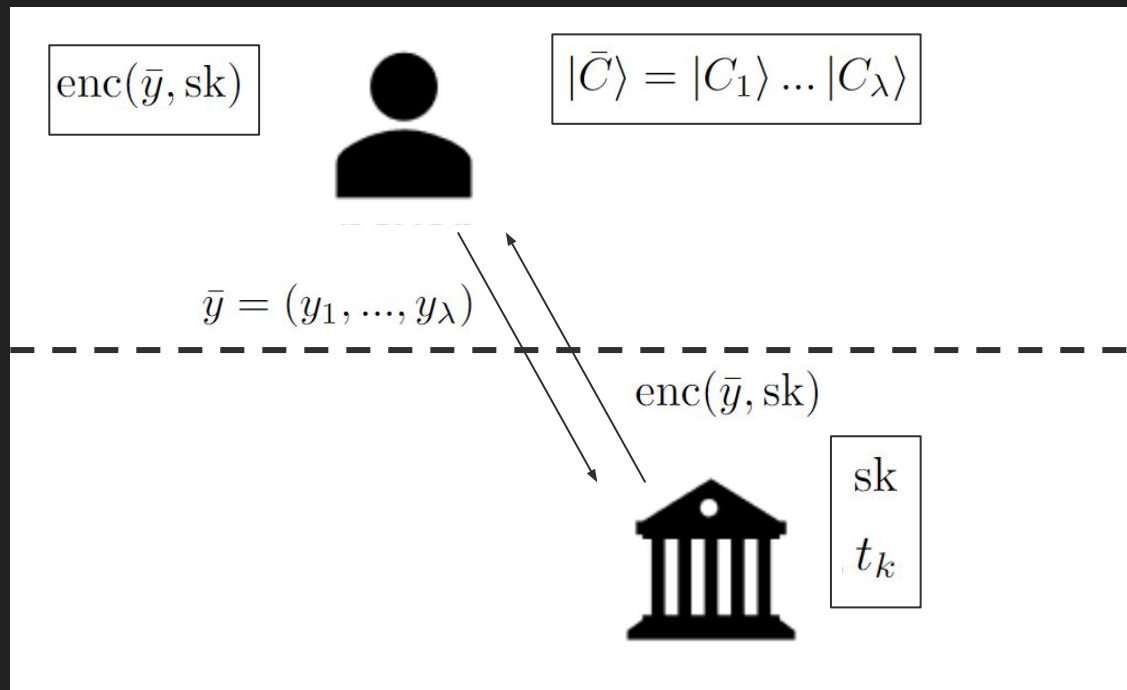
Constructing Semi-Quantum Money

Minting



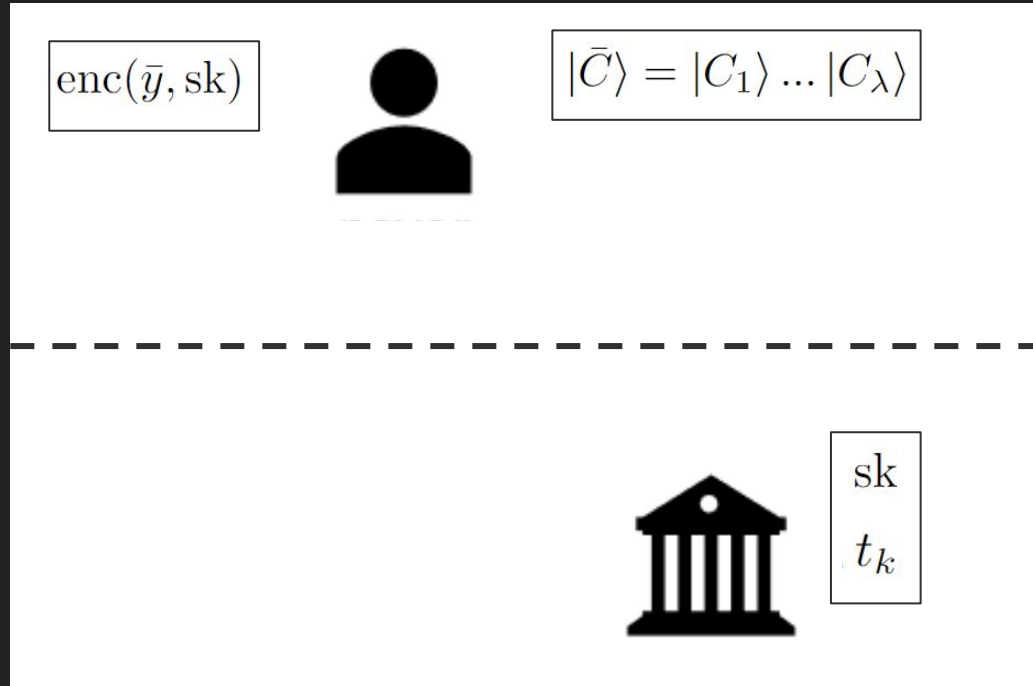
Constructing Semi-Quantum Money

Minting



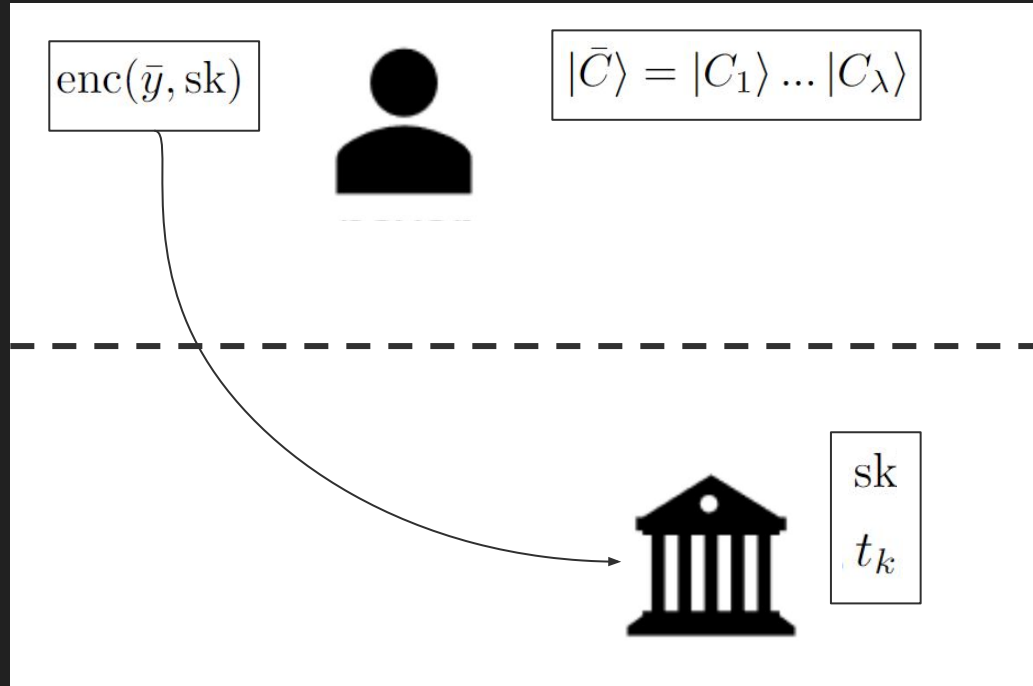
Constructing Semi-Quantum Money

Verification



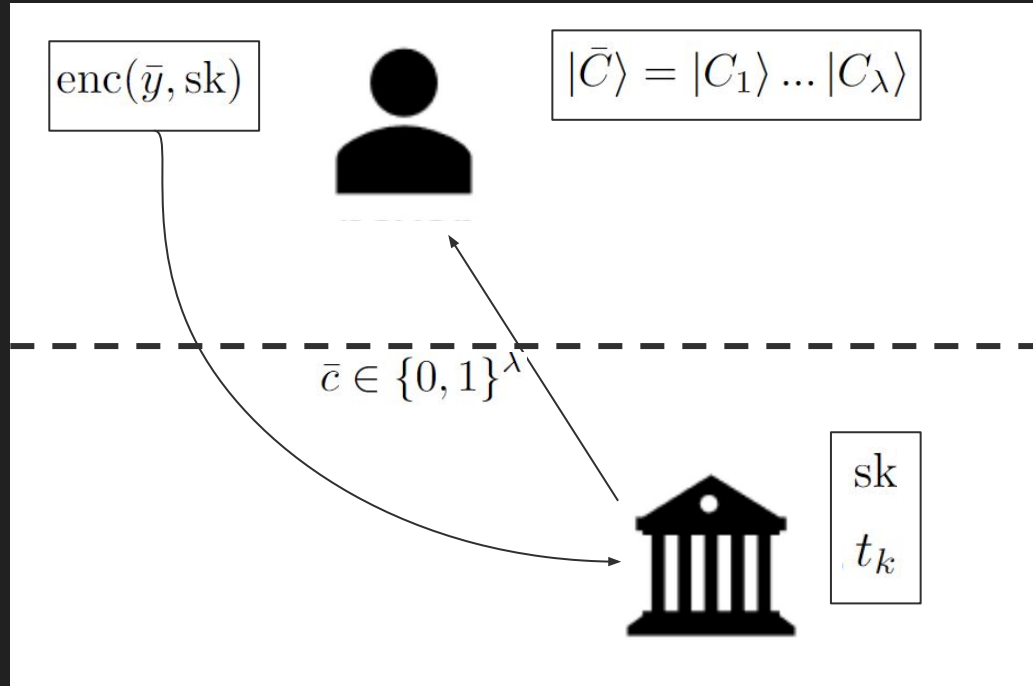
Constructing Semi-Quantum Money

Verification



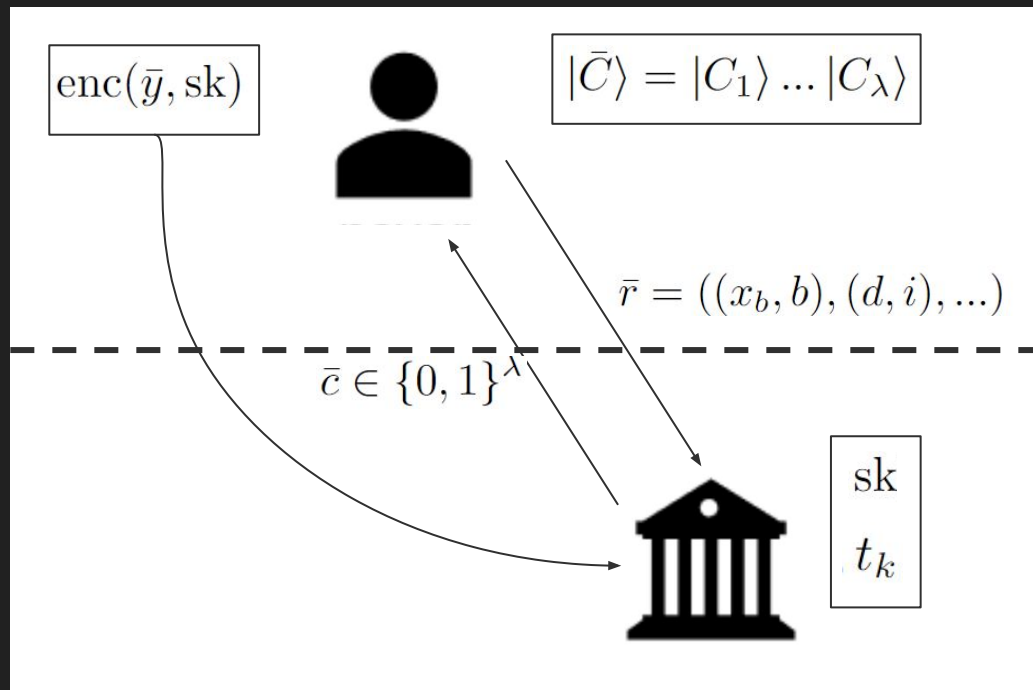
Constructing Semi-Quantum Money

Verification



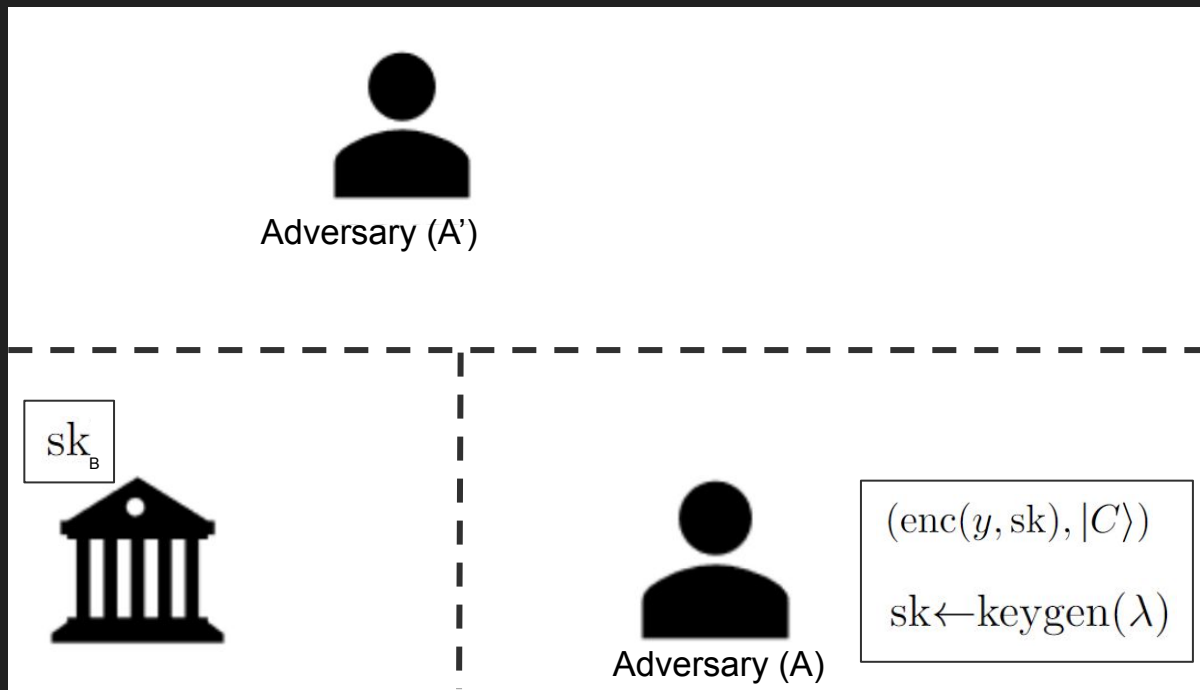
Constructing Semi-Quantum Money

Verification



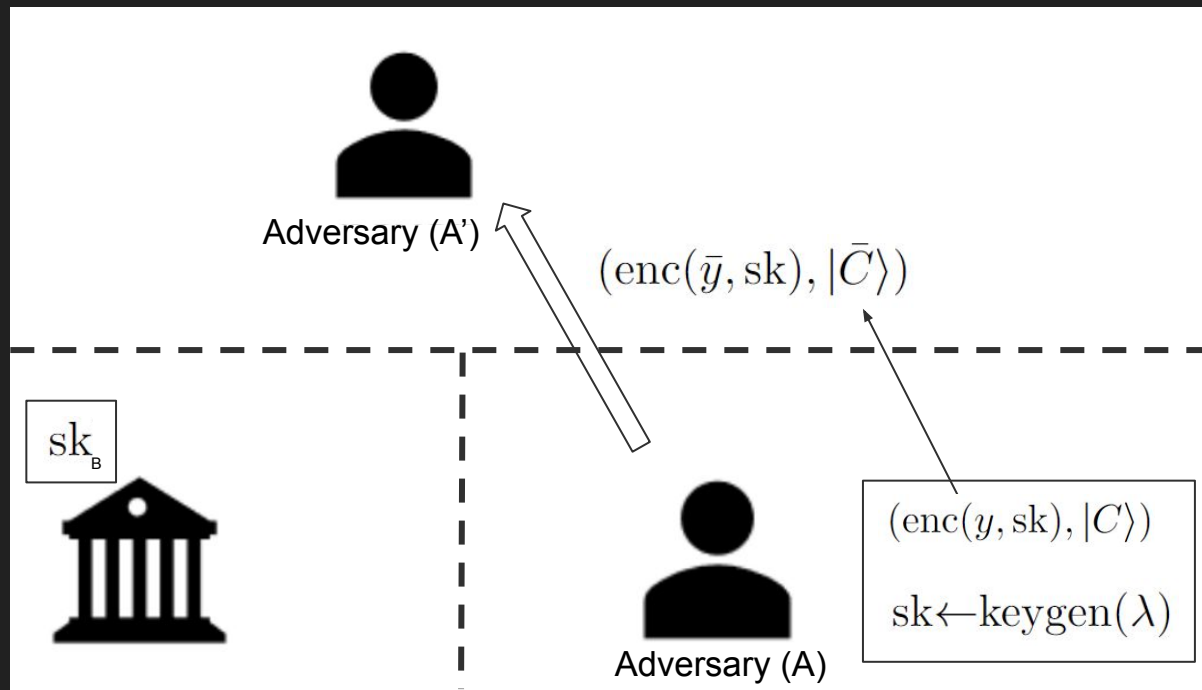
Constructing Quantum Money

Many-to-One Reduction



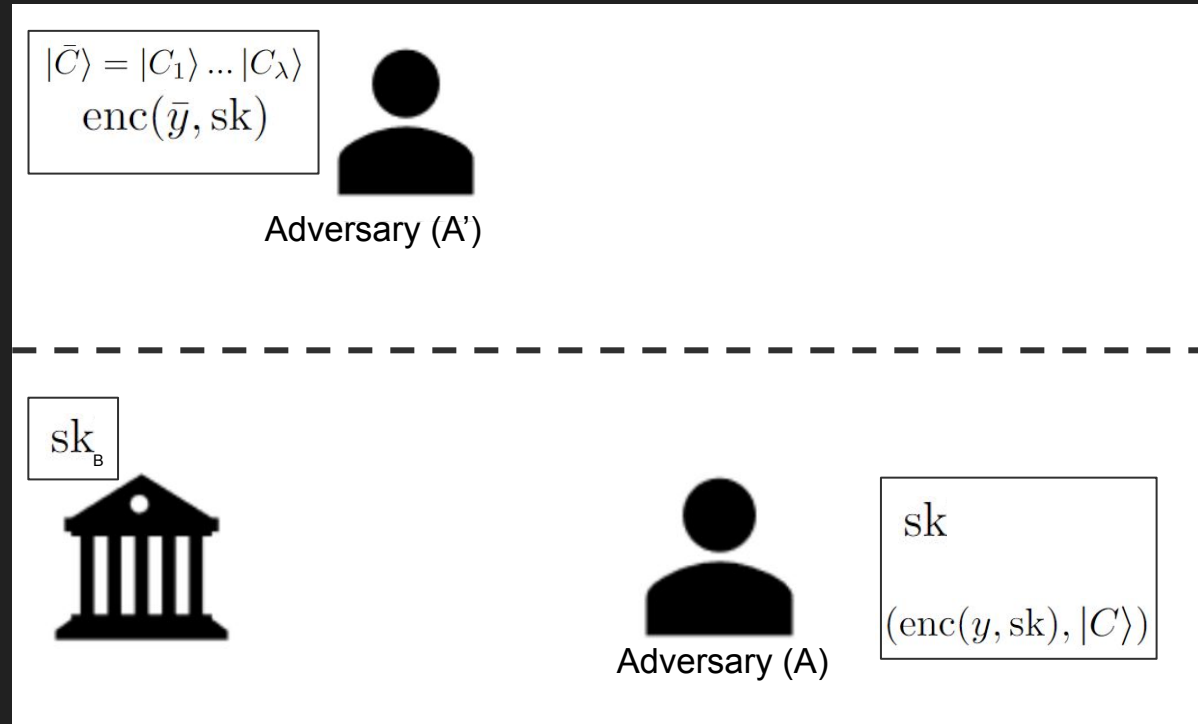
Constructing Quantum Money

Many-to-One Reduction



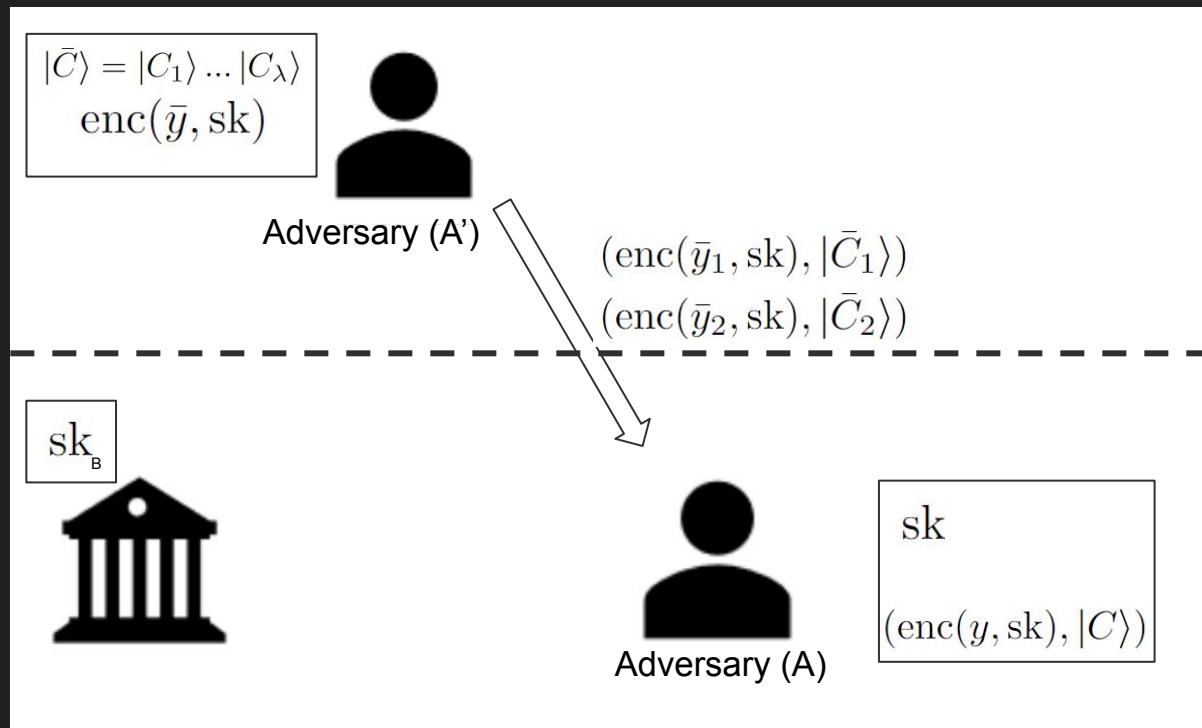
Constructing Quantum Money

Many-to-One Reduction



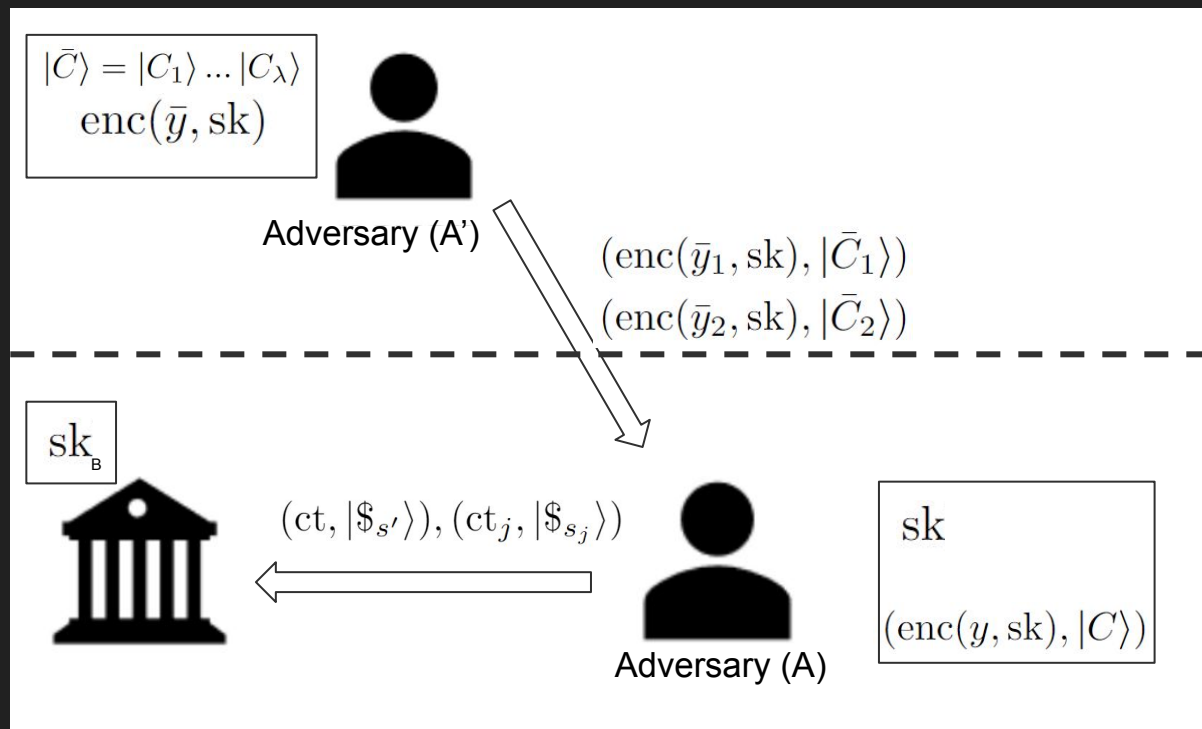
Constructing Quantum Money

Many-to-One Reduction



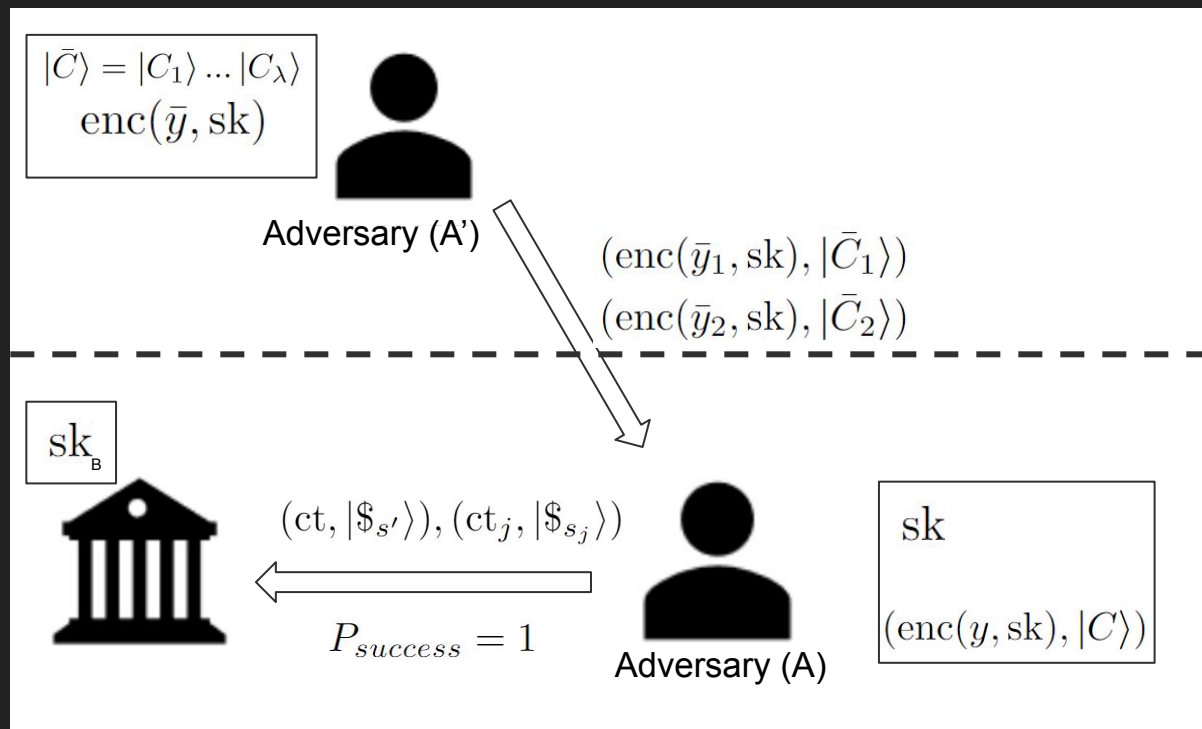
Constructing Quantum Money

Many-to-One Reduction



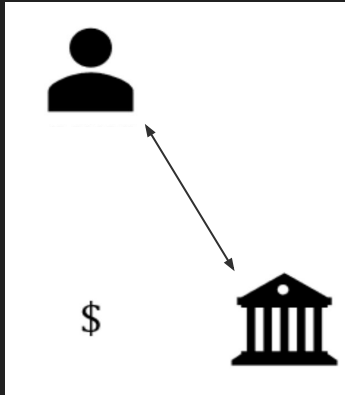
Constructing Quantum Money

Many-to-One Reduction

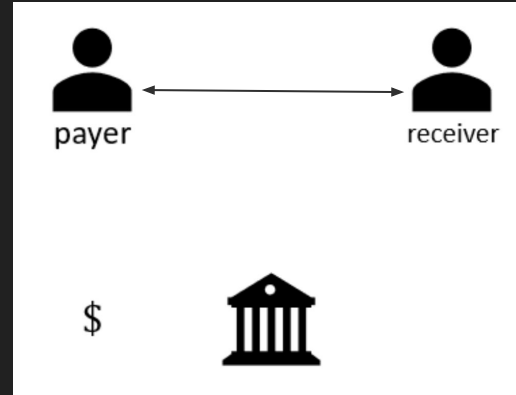


Public Key Setting

Minting



Secure (!) Transaction



References

- [RS19] R. Radian, O. Sattath, “Semi-quantum money,” <https://arxiv.org/abs/1908.08889> (2019)
- [W83] S. Wiesner, “Conjugate coding,” “<https://dl.acm.org/doi/10.1145/1008908.1008920>” (1983)
- [BCMVV21] Z. Brakerski et. al, “A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device,” [1804.00640.pdf \(arxiv.org\)](#) (2018)
- [AGKZ22] Amos et. al, “One-Shot Signatures and Applications to Hybrid Quantum/Classical Authentication,” <https://par.nsf.gov/servlets/purl/10164786> (2022)
- [S22] O. Shmueli, “Semi-Quantum Tokenized Signatures,” <https://eprint.iacr.org/2022/228.pdf> (2022)