Title: (Post-Quantum) Cryptography

Date: Apr 17, 2018 03:30 PM

URL: http://pirsa.org/18040155

Abstract: <p>In this talk, I will discuss two important cryptographic tasks in a post-quantum world. I will discuss the impossibility of bit-commitment and the possibility of physically unforgeable money in the framework of Generalized Probabilistic Theories. Our proofs rely crucially on cone programming, a natural generalization of semidefinite programming. This is based on work with John Selby, arXiv:1803.10279 and arXiv:1711.02662. </p>

(Post-Quantum) Cryptography

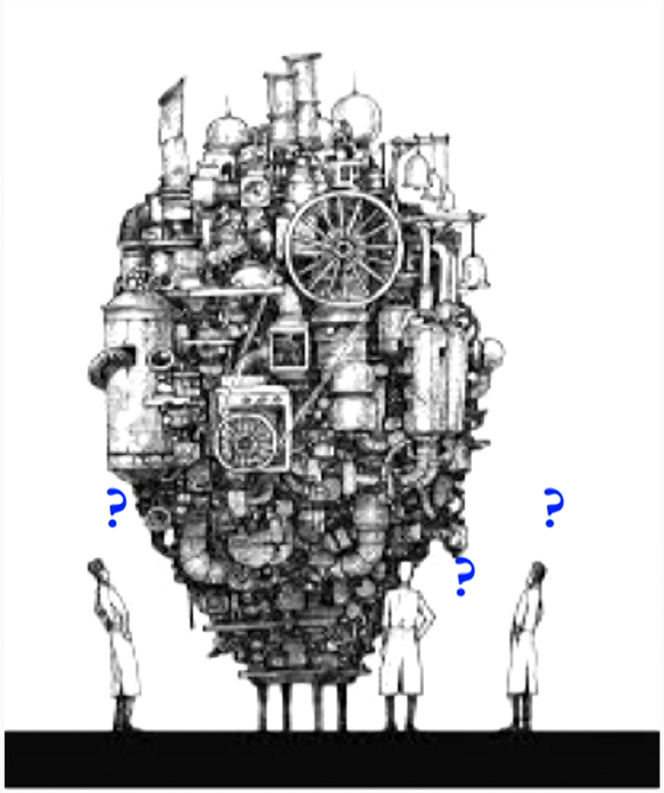
arXiv:1803.10279
arXiv:1711.02662

Jamie Sikora (PI)
John Selby (PI)

Abstract

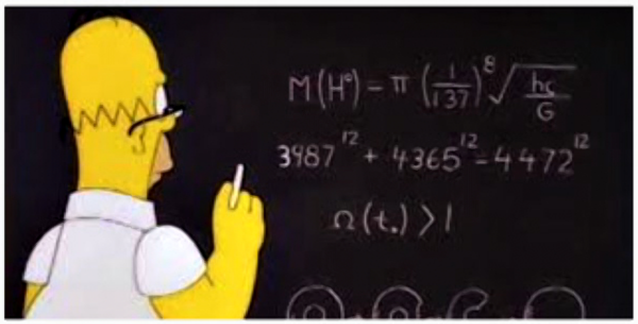
Generalized Probabilistic Theories (GPTs)

A bunch of convex things that interact with other convex things in some kind of linear way



Abstract

Cone Programming (Optimization)



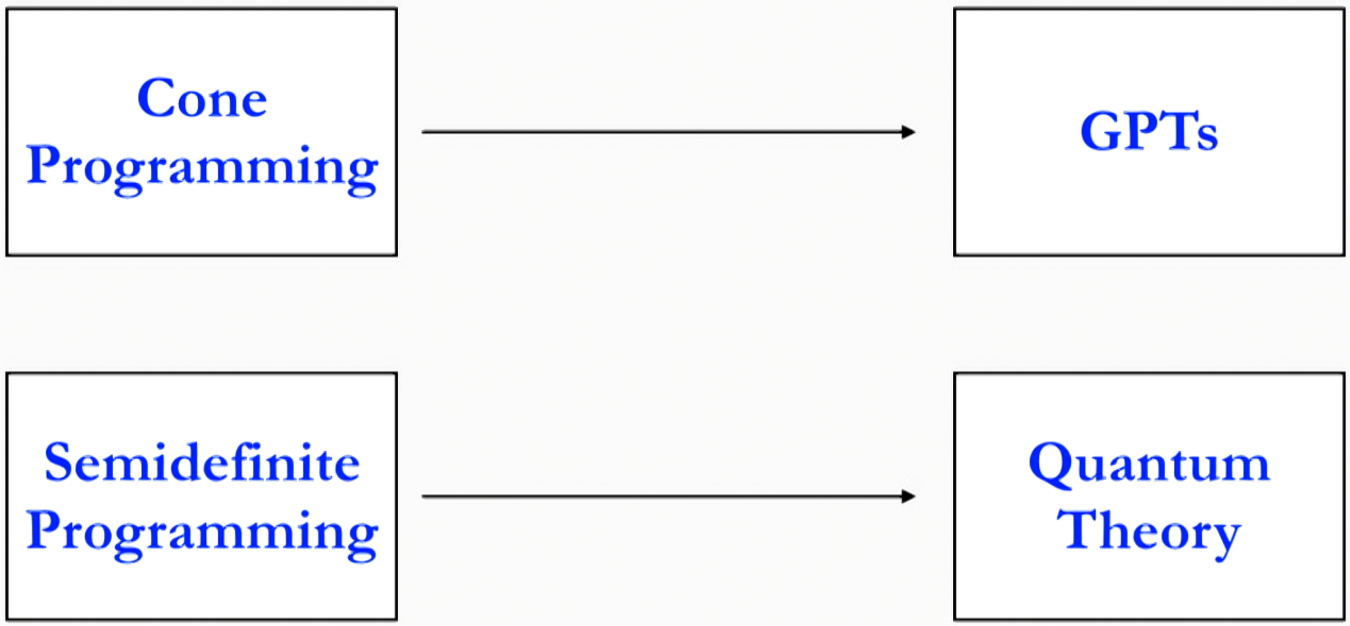
Optimizing linear functions of convex things that satisfy some linear conditions


Optimize
GPT
Stuff

Analogy with Semidefinite Programming

$$\boxed{\textbf{Semidefinite Programming}} \longrightarrow \boxed{\textbf{Quantum Theory}}$$

Analogy with Semidefinite Programming



Where do semidefinite programs appear?

Quantum… Cryptography
Complexity Theory
Query Complexity
Information Theory
Entanglement Theory
Graph Theory
Linear Optics
Bell Non-locality
and many more…

What is a cone program?

What is a cone?

Cone

$K =$ 

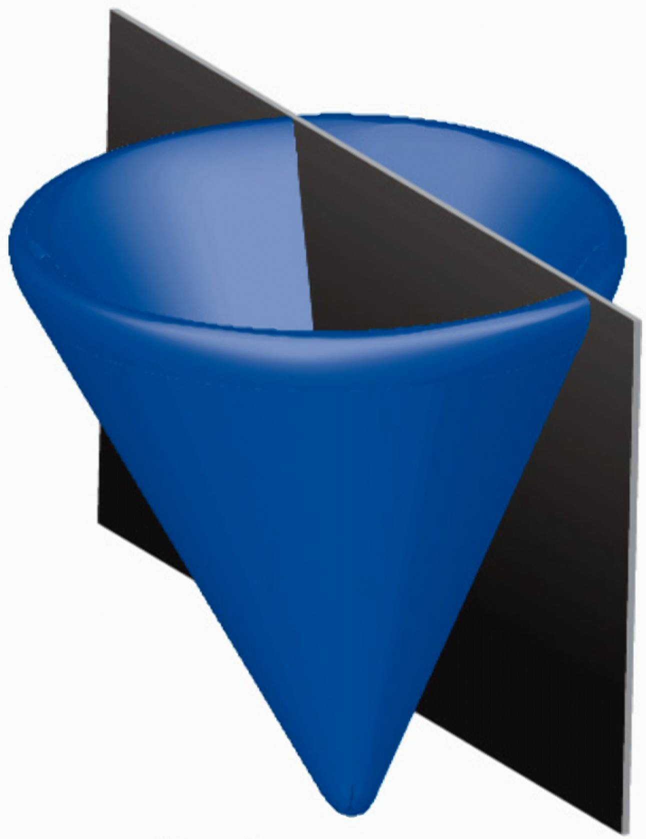
If $k \in K$, then $\lambda k \in K$ when $\lambda \geq 0$

(We'll assume cones are convex as well)

A Cone Program

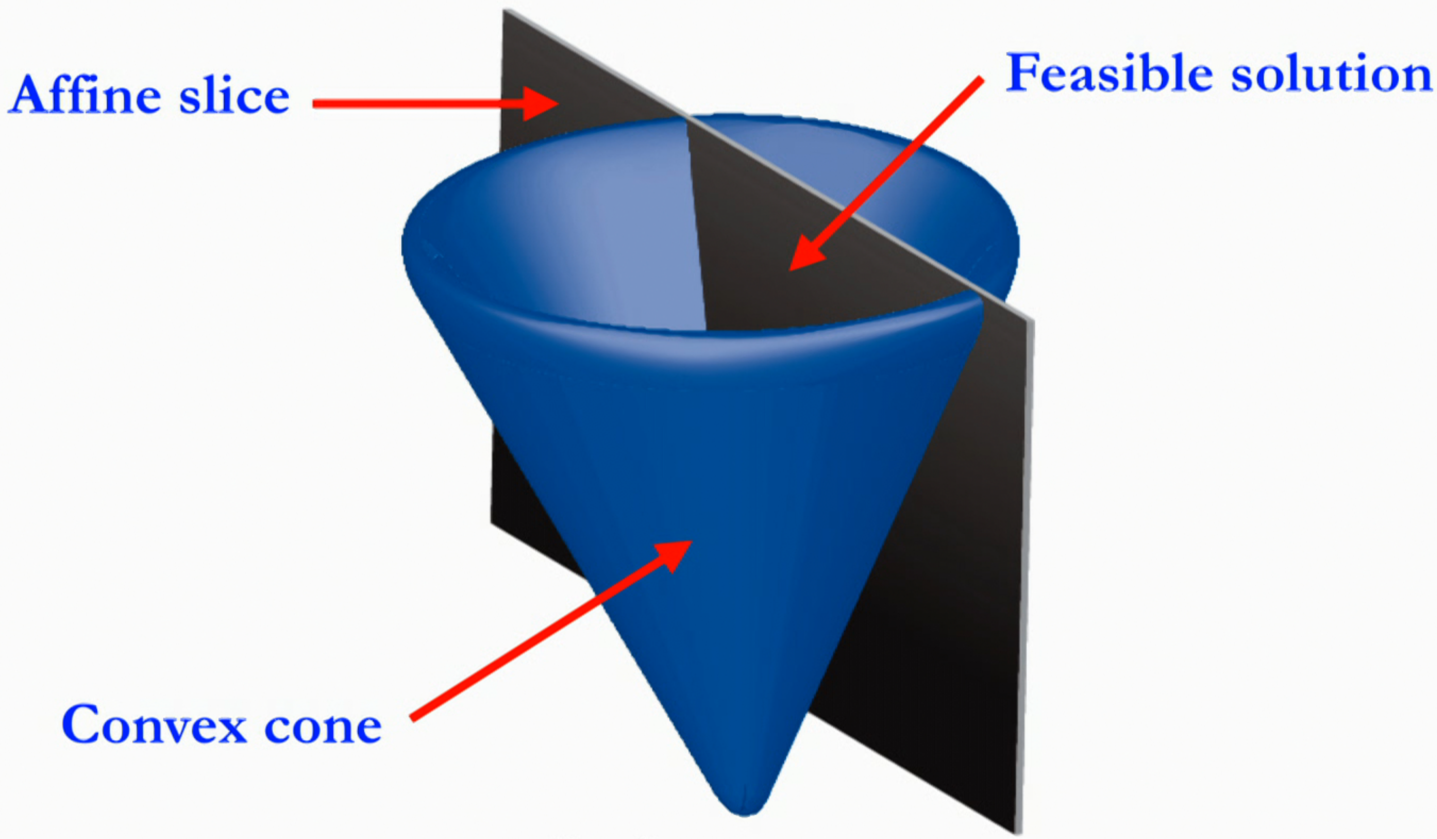
$$\begin{aligned} \sup \;& \langle C, X \rangle \\ s.t. \;& \mathcal{A}(X) = B \\ & X \in K \end{aligned}$$

Geometry



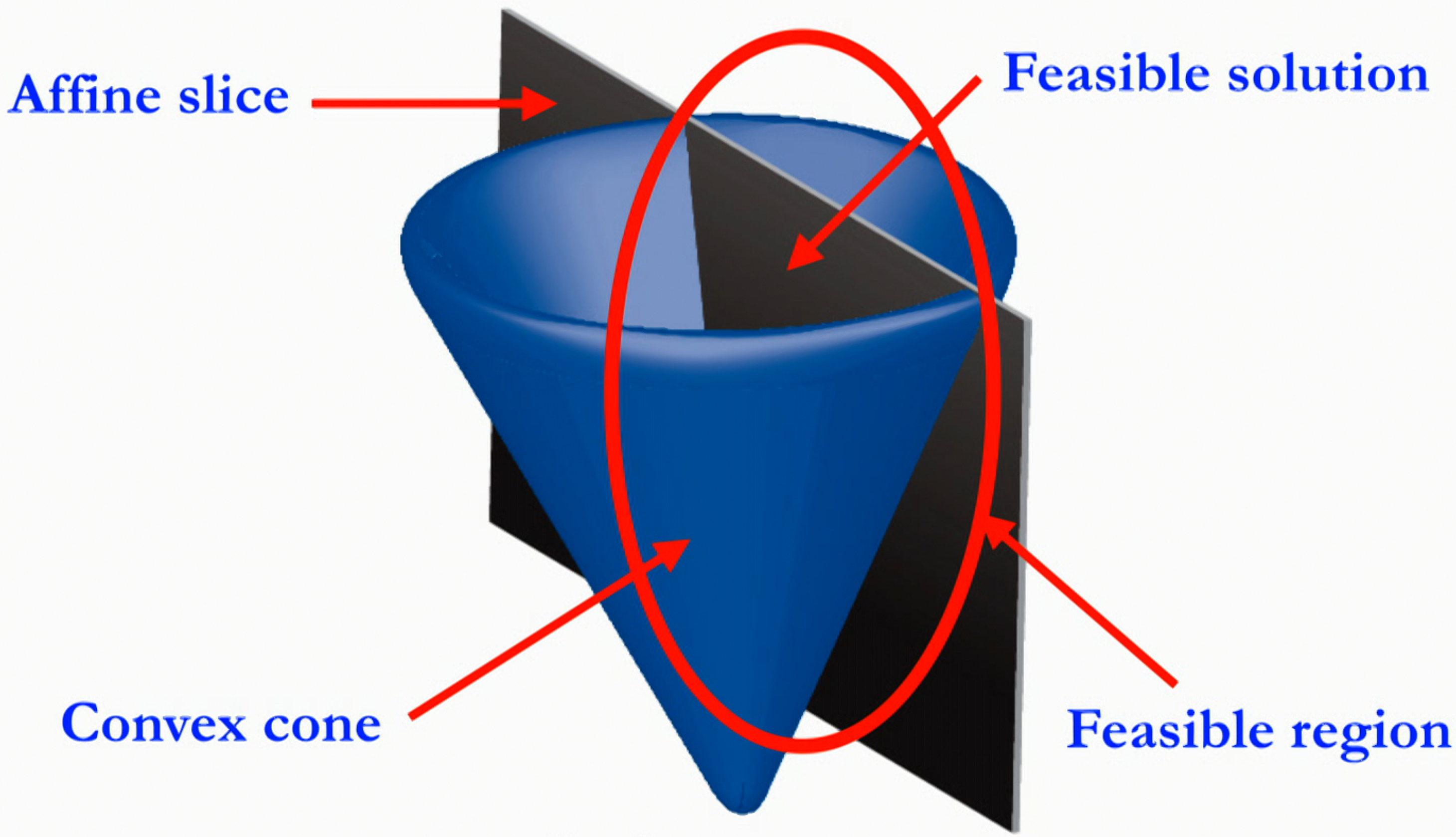
Credit: cvxr.com

Geometry



Credit: cvxr.com

Geometry



Credit: cvxr.com

Quantum Example: Optimal Measurements

Problem: Suppose you are given a quantum state

$$\{\rho_1, \ldots, \rho_n\}$$

with probability p_i **. How can you determine what state you were given with the maximum probability?**

Quantum Example: Optimal Measurements

Problem: Suppose you are given a quantum state

$$\{\rho_1, \ldots, \rho_n\}$$

with probability p_i. How can you determine what state you were given with the maximum probability?

Data: States $\{(\rho_i, p_i)\}$

Variables: POVMS $\{M_1, \ldots, M_n\}$

Constraints: $\sum_{i=1}^{n} M_i = I,\ M_i \succeq 0$

Objective: Maximize $\sum_{i=1}^{n} p_i \langle M_i, \rho_i \rangle$

Quantum Example: Optimal Measurements

Problem: Suppose you are given a quantum state

$$\{\rho_1, \ldots, \rho_n\}$$

with probability p_i. How can you determine what state you were given with the maximum probability?

Data: States $\{(\rho_i, p_i)\}$

Variables: POVMS $\{M_1, \ldots, M_n\}$

Constraints: $\sum_{i=1}^{n} M_i = I, \ M_i \succeq 0$

Objective: Maximize $\sum_{i=1}^{n} p_i \langle M_i, \rho_i \rangle$

Cone Program

$$\sup \quad \sum_{i=1}^{n} p_i \langle M_i, \rho_i \rangle$$

$$s.t. \quad \sum_{i=1}^{n} M_i = I$$

$$M_1, \ldots, M_n \succeq 0$$

Quantum Example: Optimal Measurements

Problem: Suppose you are given a quantum state

$$\{\rho_1, \ldots, \rho_n\}$$

with probability p_i. How can you determine what state you were given with the maximum probability?

Data: States $\{(\rho_i, p_i)\}$

Variables: POVMS $\{M_1, \ldots, M_n\}$

Constraints: $\sum_{i=1}^{n} M_i = I, \; M_i \succeq 0$

Objective: Maximize $\sum_{i=1}^{n} p_i$

Optimal value: ???

Cone Program

$$\sup \sum_{i=1}^{n} p_i \langle M_i, \rho_i \rangle$$

$_i = I$

$., M_n \succeq 0$

GPT setup

Physical states are vectors in a cone K

Measurements (effects) are in the effect cone E

GPT setup

Physical states are vectors in a cone K

Measurements (effects) are in the effect cone E

GPT setup

Physical states are vectors in a cone K

Measurements (effects) are in the effect cone E

"Throw away" effect: $u \in E$ **satisfies** $\langle u, k \rangle = 1$
for all physical states $k \in K$

GPT setup

Physical states are vectors in a cone K

Measurements (effects) are in the effect cone E

"Throw away" effect: $u \in E$ **satisfies** $\langle u, k \rangle = 1$
for all physical states $k \in K$

Requirement: $E \subseteq K^* = \{x : \langle x, k \rangle \geq 0, \forall k \in K\}$

GPT setup

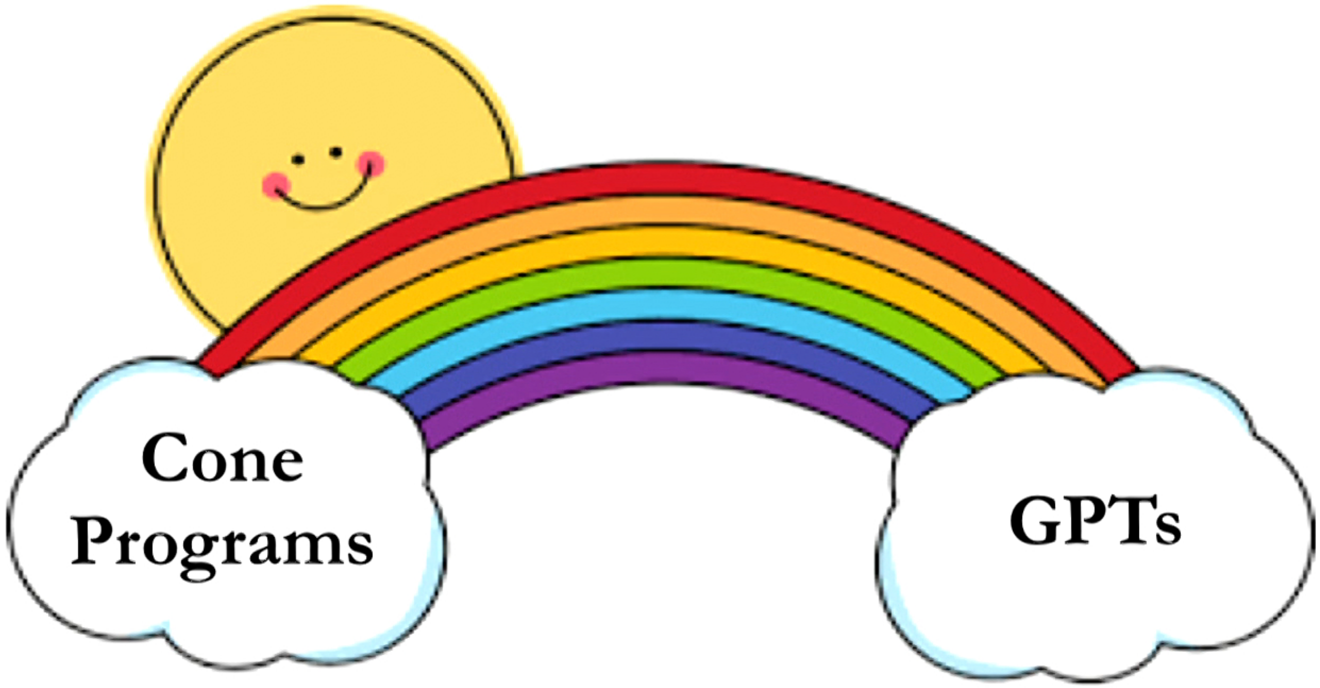
Physical states are vectors in a cone K

Measurements (effects) are in the effect cone E

"Throw away" effect: $u \in E$ **satisfies** $\langle u, k \rangle = 1$

for all physical states $k \in K$

$$\mathrm{Prob}(e_i | k) = \langle e_i, k \rangle$$


Cone
Programs
GPTs

We have a setting, a tool, now we need a problem…

We'll look at two cryptography problems

A long, long time ago…

Classical cryptography was good (but the world is not classical)

Quantum algorithms breaks (some of) classical cryptography

Quantum cryptography is secure (assuming the world is quantum)

But, is the world really quantum?

(Post-quantum) cryptography!

Bit-commitment

Bit-commitment

Bit-commitment

Alice has a
present for Bob

Problem: Alice is travelling during Bob's birthday
and doesn't want Bob to open the gift until his birthday

Bit-commitment

Now

Bit-commitment

Now

Bit-commitment

Bob's birthday

Bit-commitment

Bob's birthday

Bit-commitment

Bob's birthday

Bit-commitment

Success!

Physical bit-commitment

Bit a

$\mathcal{B}$ $\longrightarrow$

Creates the state

$s^a_{\mathcal{AB}}$

Physical bit-commitment

Bit a

$$\xrightarrow{\quad\mathcal{B}\quad}$$

$$\xrightarrow{\quad a,\,\mathcal{A}\quad}$$

Creates the state

$s^a_{\mathcal{A}\mathcal{B}}$

Physical bit-commitment

Bit a

$$\xrightarrow{\mathcal{B}}$$

$$\xrightarrow{a,\,\mathcal{A}}$$

Creates the state

$s^a_{\mathcal{A}\mathcal{B}}$

$\{e^a_{accept}, e^a_{reject}\}$

Assumption: $\langle s^a_{\mathcal{A},\mathcal{B}}, e^a_{accept}\rangle = 1$

Physical bit-commitment

Bit a

$$\xrightarrow{\mathcal{B}}$$

$$\xrightarrow{a,\,\mathcal{A}}$$

Creates the state

$s^{a}_{\mathcal{A}\mathcal{B}}$

$\{e^{a}_{accept}, e^{a}_{reject}\}$

Goals:

- Bob should not learn Alice's bit early
- Alice should not be able to change her bit before revealing

Physical bit-commitment

How much can Bob cheat?

Bit a

$\mathcal{B}$ ⟶

Creates the state

$s^a_{\mathcal{AB}}$

Physical bit-commitment

How much can Bob cheat?

Bit a

$$\xrightarrow{\mathcal{B}}$$

Creates the state

$s^a_{\mathcal{A}\mathcal{B}}$

Equivalent problem:
Bob must measure $\mathcal{B}$ **to learn what state he was given**

$$s^0_{\mathcal{B}} \text{ or } s^1_{\mathcal{B}}$$

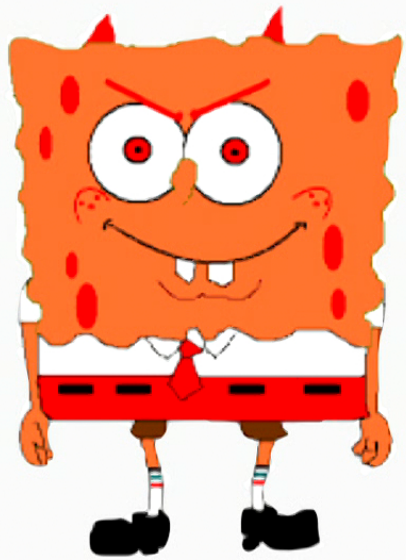
Physical bit-commitment

Bob's cheating probability

$$\sup \ \frac{1}{2}\langle s_{\mathcal{B}}^{0}, e_0\rangle + \frac{1}{2}\langle s_{\mathcal{B}}^{1}, e_1\rangle$$

$$s.t. \ \ e_0 + e_1 = u$$

$$e_0, e_1 \in E$$



Physical bit-commitment

How much can Alice cheat?

$\xrightarrow{\mathcal{B}}$

$\xrightarrow{a,\,\mathcal{A}}$

$\{e^a_{accept}, e^a_{reject}\}$

Creates the state

$s^a_{\mathcal{AB}}$

Physical bit-commitment

How much can <u>Alice</u> cheat?

~~Bit a~~

She must send something here

$$\mathcal{B}$$

Decides "a" here

$$a, \mathcal{A}$$

Creates the state

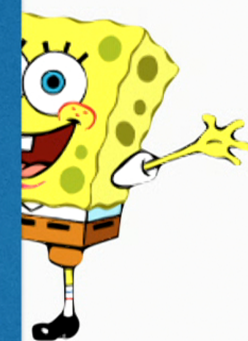
$\cancel{\varsigma^a_{\mathcal{AB}}}$

Hopes to pass Bob's cheat detection here

$$\{e^a_{accept}, e^a_{reject}\}$$

Physical bit-commitment

~~Bi~~

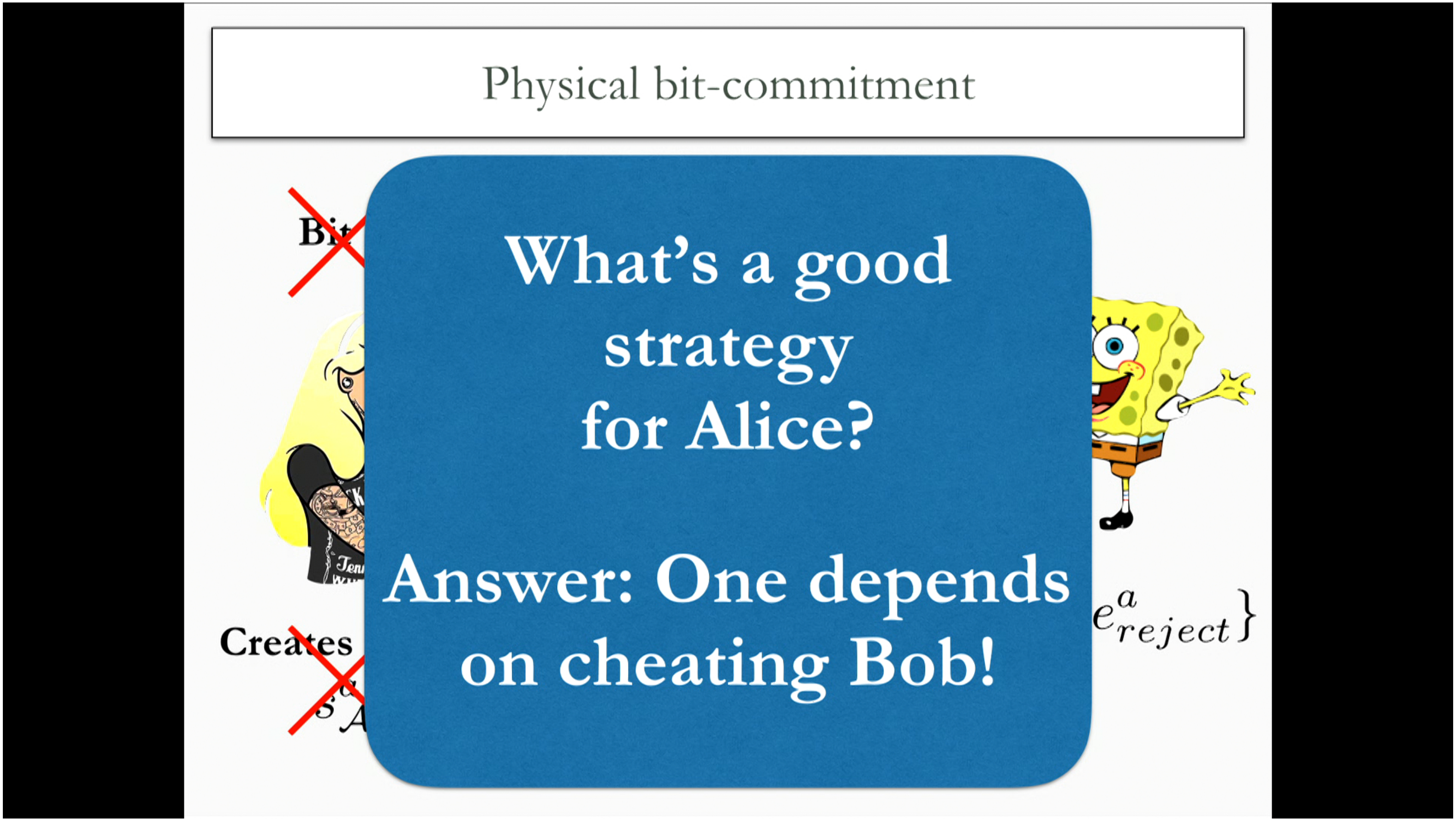


What's a good strategy for Alice?

$e^{a}_{reject}\}$

~~**Creates**~~

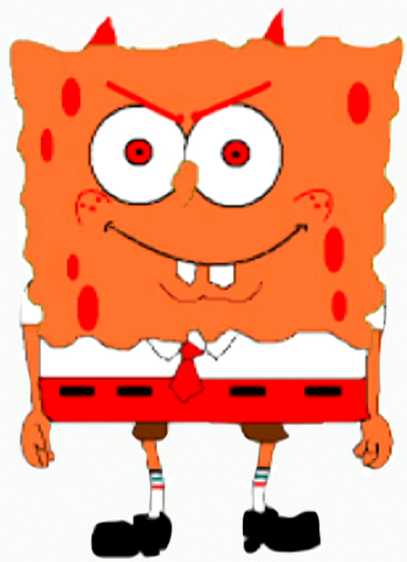
s^{a}_{A}


Physical bit-commitment
Creates
What's a good strategy for Alice?
Answer: One depends on cheating Bob!
$e^a_{reject}\}$

Physical bit-commitment

Bob's cheating probability

$$\begin{aligned} \sup \quad & \frac{1}{2}\langle s^0_{\mathcal{B}}, e_0\rangle + \frac{1}{2}\langle s^1_{\mathcal{B}}, e_1\rangle \\ s.t. \quad & e_0 + e_1 = u \\ & e_0, e_1 \in E \end{aligned}$$



Physical bit-commitment

Bob's cheating probability

$$\begin{aligned} \sup \quad & \frac{1}{2}\langle s_{\mathcal{B}}^0, e_0\rangle + \frac{1}{2}\langle s_{\mathcal{B}}^1, e_1\rangle \\ s.t. \quad & e_0 + e_1 = u \\ & e_0, e_1 \in E \end{aligned}$$

Physical bit-commitment

Bob's cheating probability

$$
\begin{aligned}
\sup \quad & \frac{1}{2}\langle s_{\mathcal{B}}^{0}, e_0\rangle + \frac{1}{2}\langle s_{\mathcal{B}}^{1}, e_1\rangle \\
s.t. \quad & e_0 + e_1 = u \\
& e_0, e_1 \in E
\end{aligned}
$$

Dual problem

$$
\begin{aligned}
\inf \quad & \langle x, u\rangle \\
s.t. \quad & x - \frac{1}{2}s_{\mathcal{B}}^{0} \in E^* \\
& x - \frac{1}{2}s_{\mathcal{B}}^{1} \in E^*
\end{aligned}
$$

Physical bit-commitment

Bob's cheating probability

$$\begin{aligned} \sup \quad & \frac{1}{2}\langle s_{\mathcal{B}}^0, e_0 \rangle + \frac{1}{2}\langle s_{\mathcal{B}}^1, e_1 \rangle \\ s.t. \quad & e_0 + e_1 = u \\ & e_0, e_1 \in E \end{aligned}$$

Bob's cheating probability

$$\begin{aligned} \inf \quad & \langle x, u \rangle \\ s.t. \quad & x - \frac{1}{2} s_{\mathcal{B}}^0 \in E^* \\ & x - \frac{1}{2} s_{\mathcal{B}}^1 \in E^* \end{aligned}$$

Physical bit-commitment

Almost useful!

Bob's cheating probability

$$\begin{aligned} \inf \quad & \langle x, u \rangle \\ s.t. \quad & x - \frac{1}{2} s_{\mathcal{B}}^{0} \in E^{*} \\ & x - \frac{1}{2} s_{\mathcal{B}}^{1} \in E^{*} \end{aligned}$$

Physical bit-commitment

Almost useful!

It would be really nice to have K instead of E^*

Bob's cheating probability

$$\inf \ \langle x, u \rangle$$
$$s.t. \ \ x - \frac{1}{2} s_{\mathcal{B}}^{0} \in E^*$$
$$x - \frac{1}{2} s_{\mathcal{B}}^{1} \in E^*$$

Physical bit-commitment

Almost useful!

It would be really nice to have K instead of E^*

So, we'll just assume this… But it's OK since others do this too!

Bob's cheating probability

$$\inf \quad \langle x, u \rangle$$

$$s.t. \quad x - \frac{1}{2} s_{\mathcal{B}}^{0} \in E^*$$

$$x - \frac{1}{2} s_{\mathcal{B}}^{1} \in E^*$$

Physical bit-commitment

No-Restriction Hypothesis!

Bob's cheating probability

$$\inf \quad \langle x, u \rangle$$

$$s.t. \quad x - \frac{1}{2} s_{\mathcal{B}}^{0} \in E^*$$

$$x - \frac{1}{2} s_{\mathcal{B}}^{1} \in E^*$$

Physical bit-commitment

An optimal solution x satisfies:

Bob's opt cheating $= \langle x, u \rangle$

$\dfrac{x}{\langle x, u \rangle}$ is a physical state

This state has nice properties!

Alice can use this state to cheat...

Bob's cheating probability

$$\begin{aligned} &\inf \ \langle x, u \rangle \\ &s.t. \ \ x - \frac{1}{2} s_{\mathcal{B}}^{0} \in K \\ & \ \ x - \frac{1}{2} s_{\mathcal{B}}^{1} \in K \end{aligned}$$

Physical bit-commitment

$$\frac{x}{\langle x, u \rangle} \in \mathcal{B}$$

$$\longrightarrow$$

Physical bit-commitment

$$\frac{x}{\langle x, u \rangle} \in \mathcal{B}$$

Decides "a" here

Alice maintains a purification…

$$a, \mathcal{A}$$

$$\{e^a_{accept}, e^a_{reject}\}$$

Physical bit-commitment

$$\frac{x}{\langle x, u\rangle}$$

Decides "a" here

Alice maintains a purification…

$$a, \mathcal{A} \longrightarrow \{e^a_{accept}, e^a_{reject}\}$$

Since $\begin{matrix} x - \frac{1}{2}s^0_{\mathcal{B}} \in K \\ x - \frac{1}{2}s^1_{\mathcal{B}} \in K \end{matrix}$ she succeeds with probability $> \dfrac{1}{2\langle x, u\rangle}$

Physical bit-commitment

An optimal solution x satisfies:

Bob's opt cheating $= \langle x, u \rangle$

$\dfrac{x}{\langle x, u \rangle}$ is a physical state

This state has nice properties!

Alice can use this state to cheat...

Bob's cheating probability

$$\inf \ \langle x, u \rangle$$

$$s.t. \ \ x - \frac{1}{2} s_{\mathcal{B}}^{0} \in K$$

$$x - \frac{1}{2} s_{\mathcal{B}}^{1} \in K$$

Physical bit-commitment

$$\frac{x}{\langle x, u \rangle} \in \mathcal{B}$$

Decides "a" here

$a, \mathcal{A}$

Alice maintains a purification…

$$\{e^a_{accept}, e^a_{reject}\}$$

Physical bit-commitment

$$\frac{x}{\langle x, u \rangle}$$

$\longrightarrow$

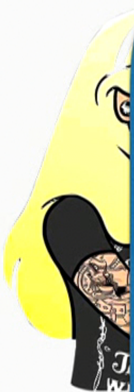
Decides "a" here

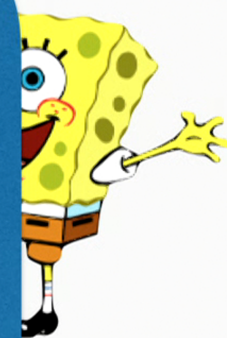
Alice maintains a purification…

$$\xrightarrow{a, \mathcal{A}} \{e^a_{accept}, e^a_{reject}\}$$

Since $\begin{array}{l} x - \frac{1}{2} s^0_{\mathcal{B}} \in K \\ x - \frac{1}{2} s^1_{\mathcal{B}} \in K \end{array}$ she succeeds with probability $> \dfrac{1}{2\langle x, u \rangle}$

Physical bit-commitment





Thus, Alice or Bob can cheat with probability at least 70%

Alice m… $e^{a}_{reject}\}$

a purifi…

Since x … $\frac{1}{2\langle x, u\rangle}$

x –


Physical bit-commitmen
NO-GO!
Since
$\frac{1}{2\langle x, u\rangle}$

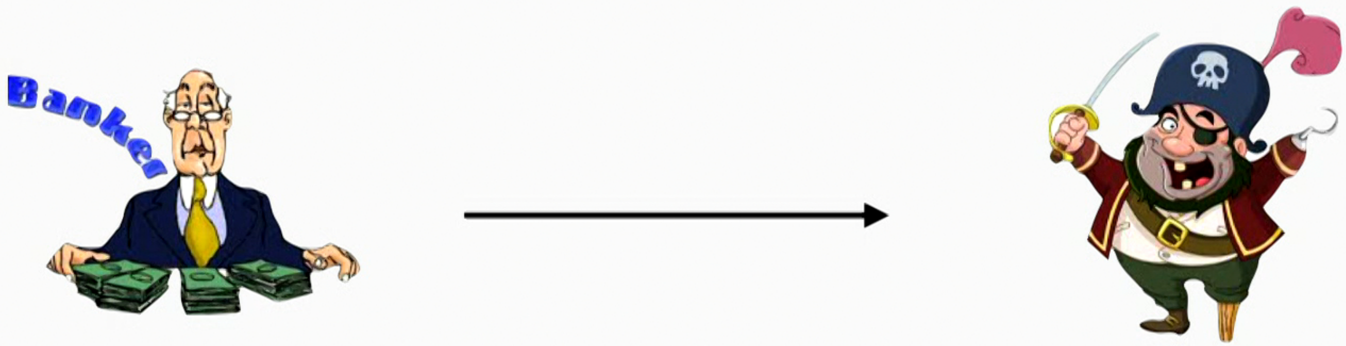
Physical bit-commitmen

A similar result was shown by
Chiribella, D'Ariano, and Perinotti

Since ... $\dfrac{1}{2\langle x, u\rangle}$

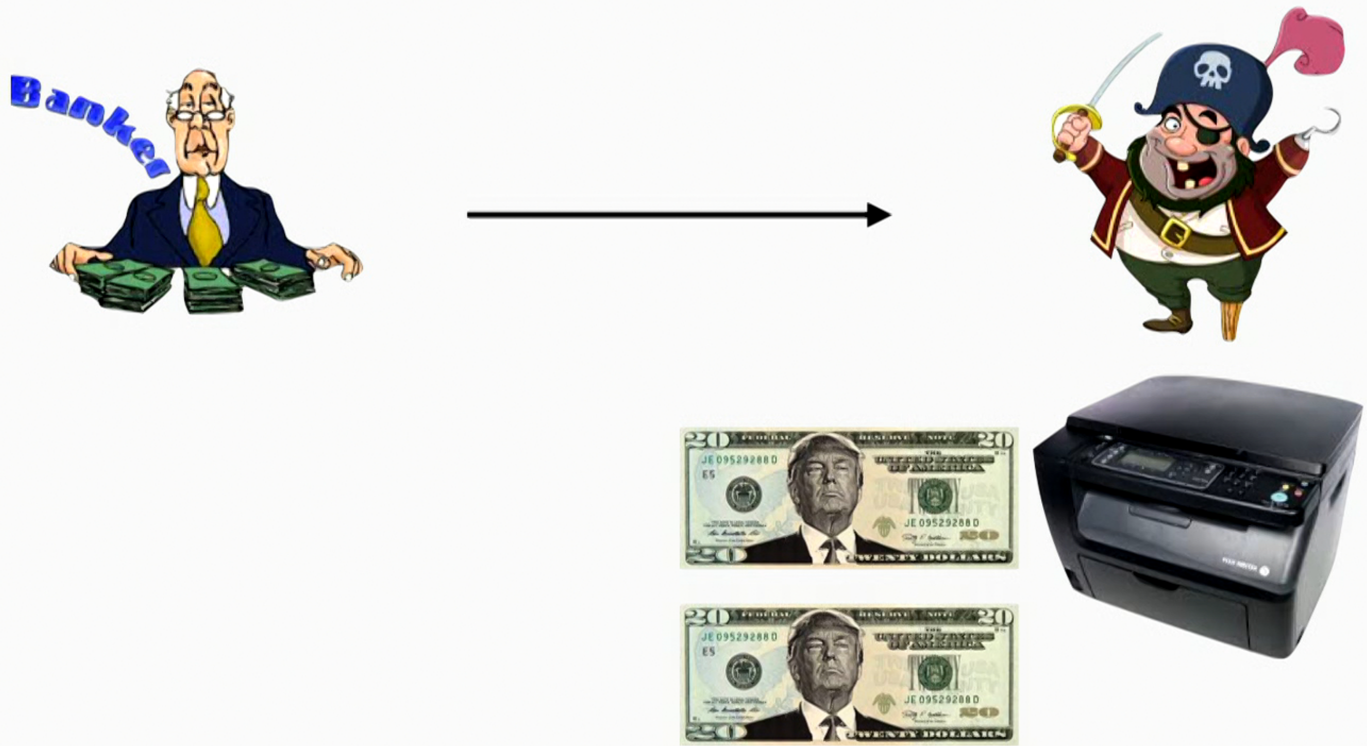
Unforgeable money

Physically Unforgeable Money

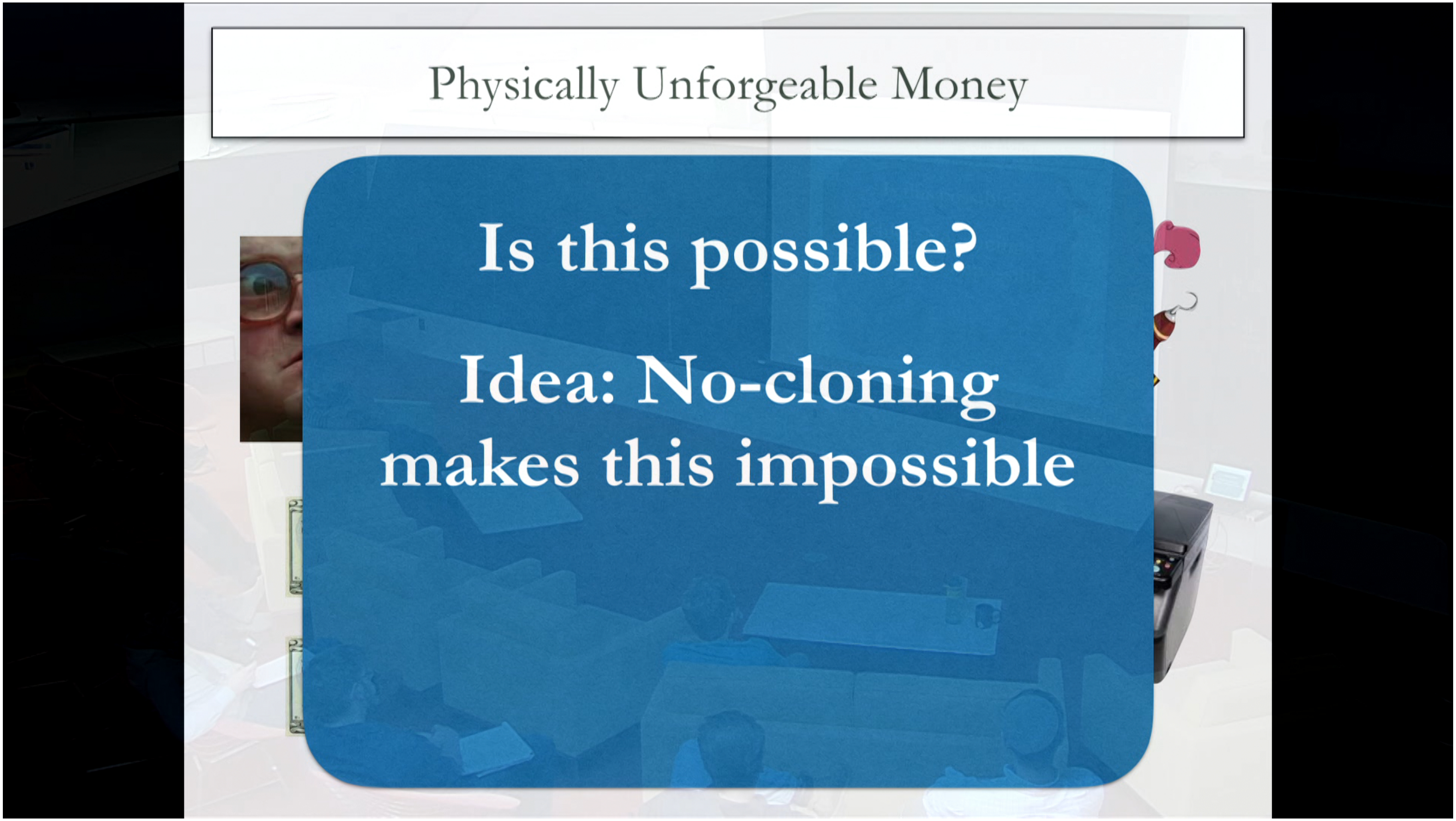


Physically Unforgeable Money

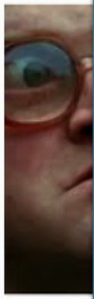
Physically Unforgeable Money



Physically Unforgeable Money


Physically Unforgeable Money
Is this possible?
Idea: No-cloning makes this impossible

Physically Unforgeable Money



Is this possible?

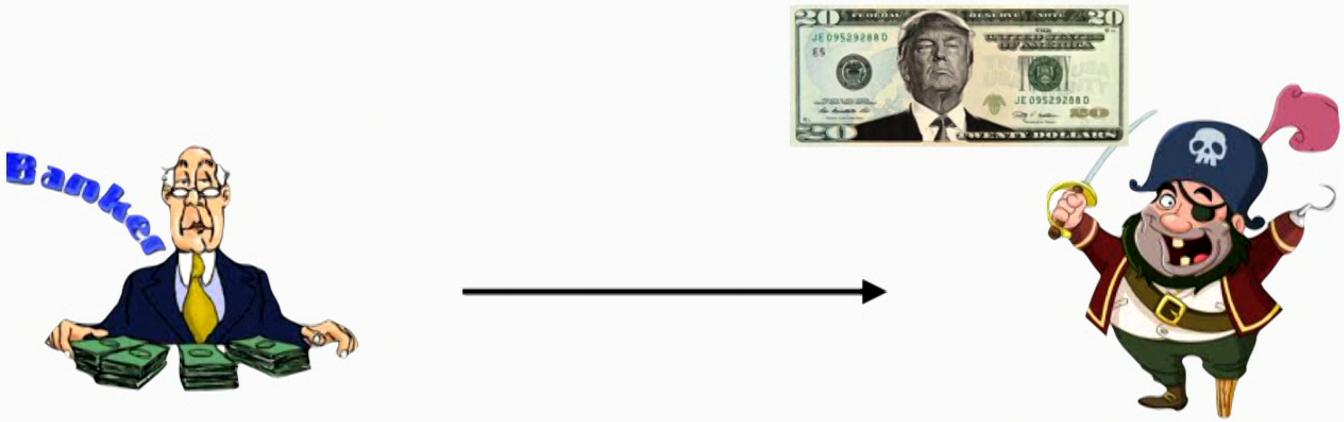
Idea: No-cloning makes this impossible

Problem: How to measure clonability?

Idea

Select state s_i with probability p_i

Physically Unforgeable Money



Physically Unforgeable Money

Knows the state

Doesn't know the state

Physically Unforgeable Money

Physically Unforgeable Money

$$\{e^i_{accept}, e^i_{reject}\}$$

$$\langle e^i_{accept}, s^i \rangle = 1$$

Physically Unforgeable Money

Physically Unforgeable Money

Joint state τ

$$\langle \tau, e^i_{accept} \otimes e^i_{accept} \rangle \text{ large?}$$

Security Idea

Security Idea

Security Idea

Let $\alpha(n)$ be the success of cloning n ensembles

In the quantum case, we have $\alpha(n) = \alpha(1)^n$

In the GPT case, the same holds under some assumptions.

However, if $\alpha(1) < 1$, then $\alpha(n) \leq \text{negl}(n)$

Measure of counterfeiting

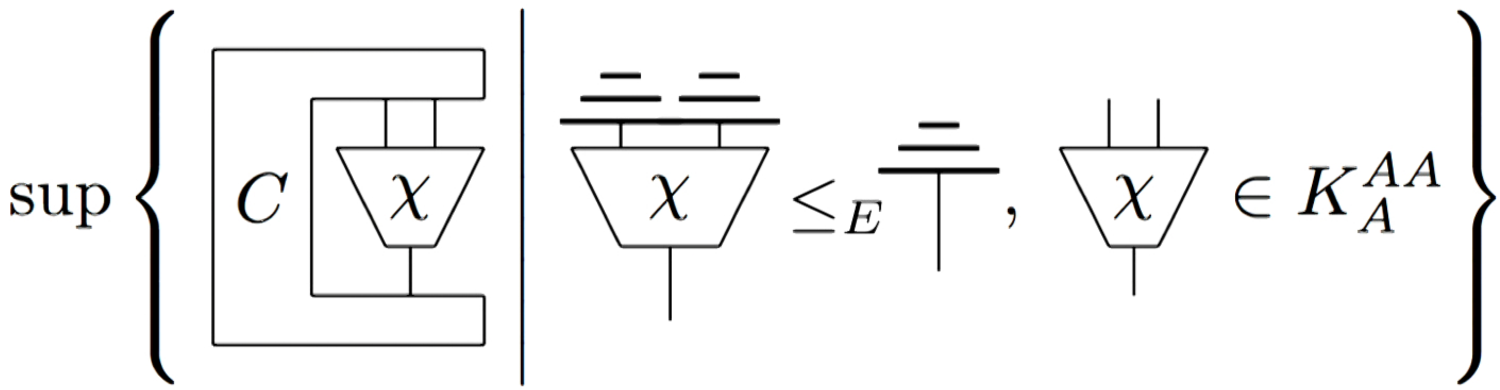
$$\sup \sum_i p_i \langle \Phi(s^i), e^i_{accept} \otimes e^i_{accept} \rangle$$

$$s.t. \quad \Phi : K \to K \otimes K$$

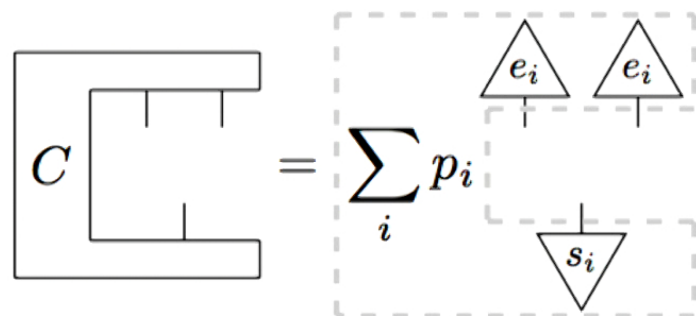
$$\Phi \text{ is trace non-increasing}$$

$$\Phi \text{ is a valid GPT channel}$$

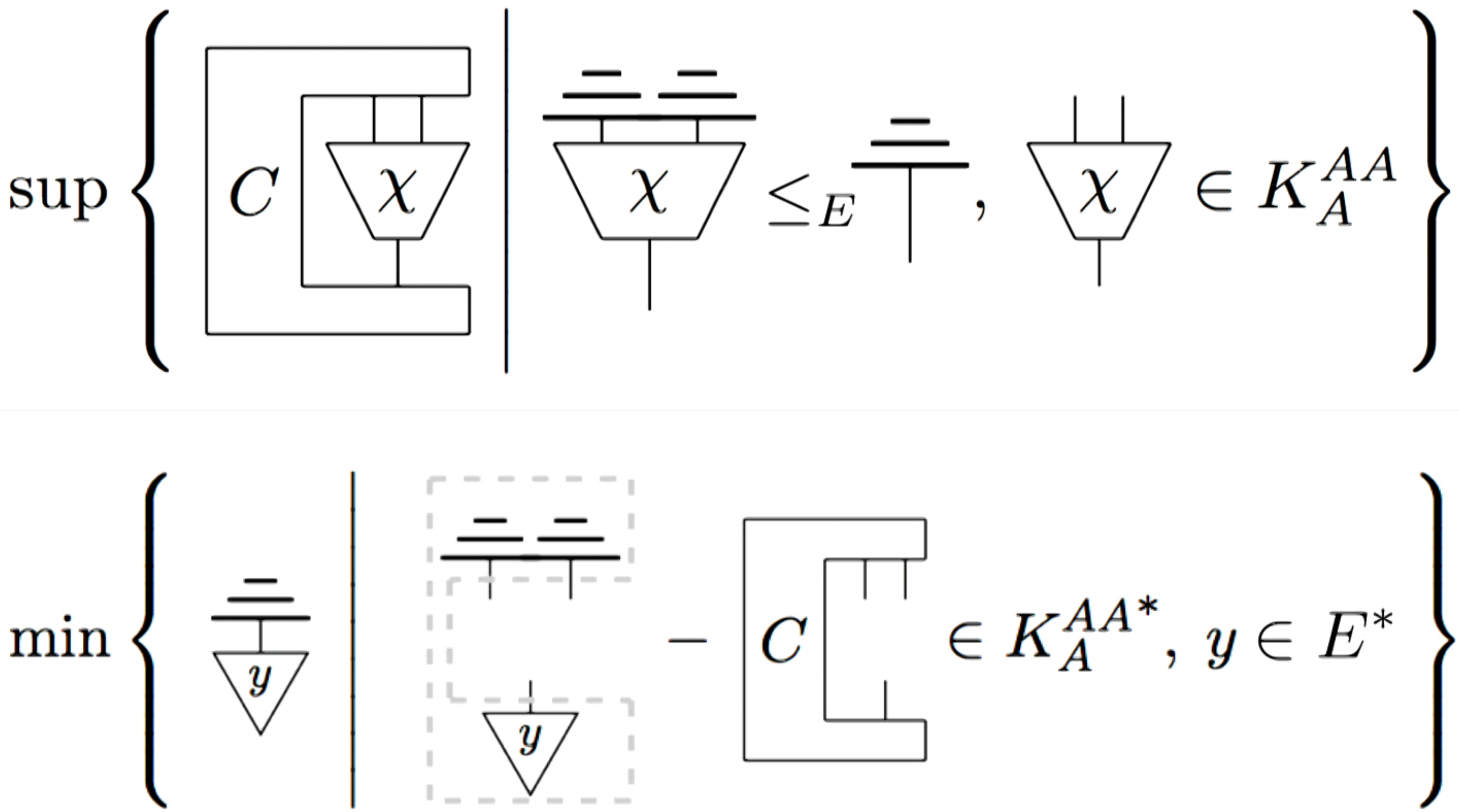
This is what John does to my nice cone programs!



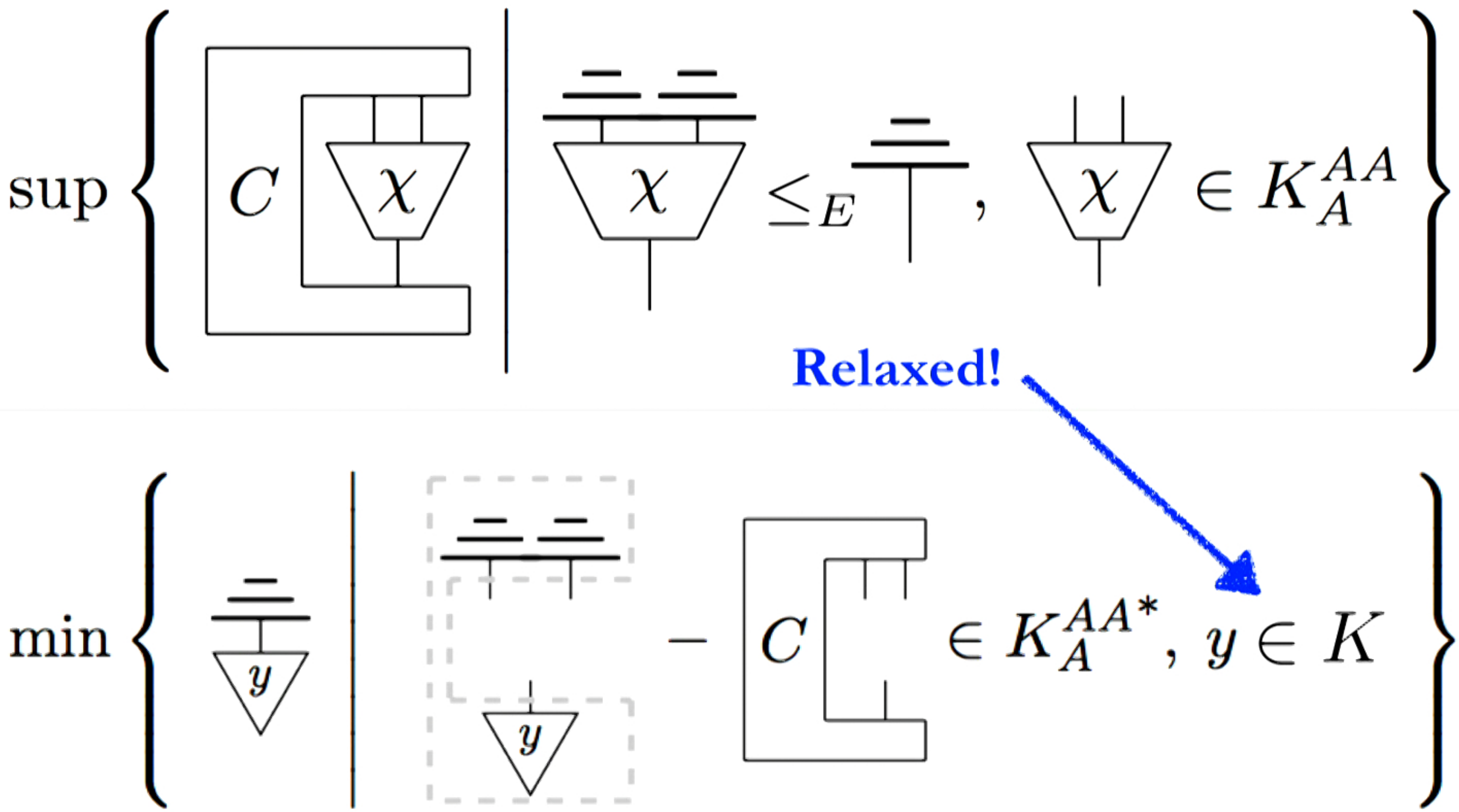
where



This is what John does to my nice cone programs!

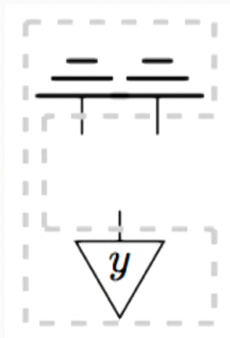


This is what John does to my nice cone programs!

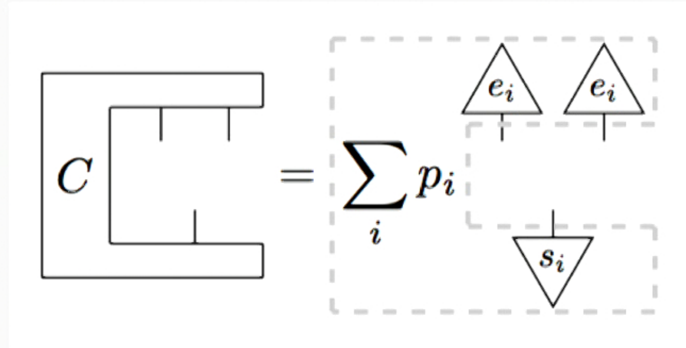


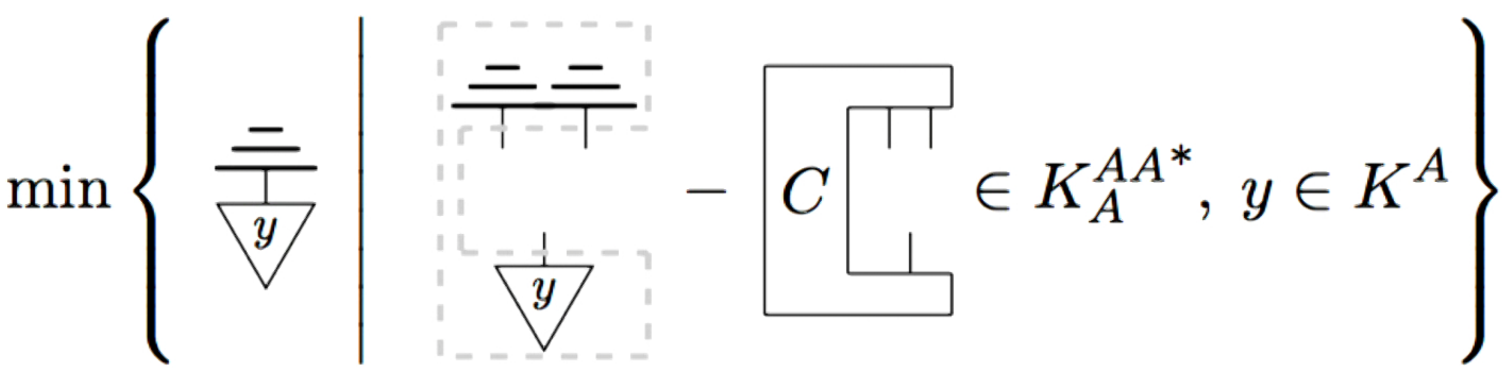
This is what John does to my nice cone programs!

Idea: Use



instead of





Proof Idea

Using duality theory…

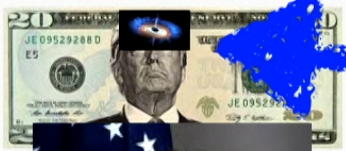
Success of cheating this banker:

Is bounded above by cheating this banker:

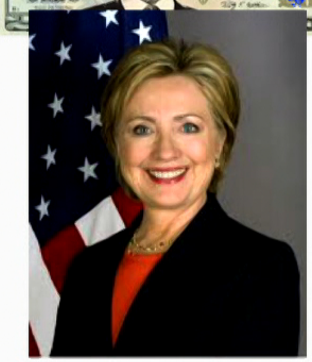
Physically Unforgeable Money

Some (scaled) GPT state here

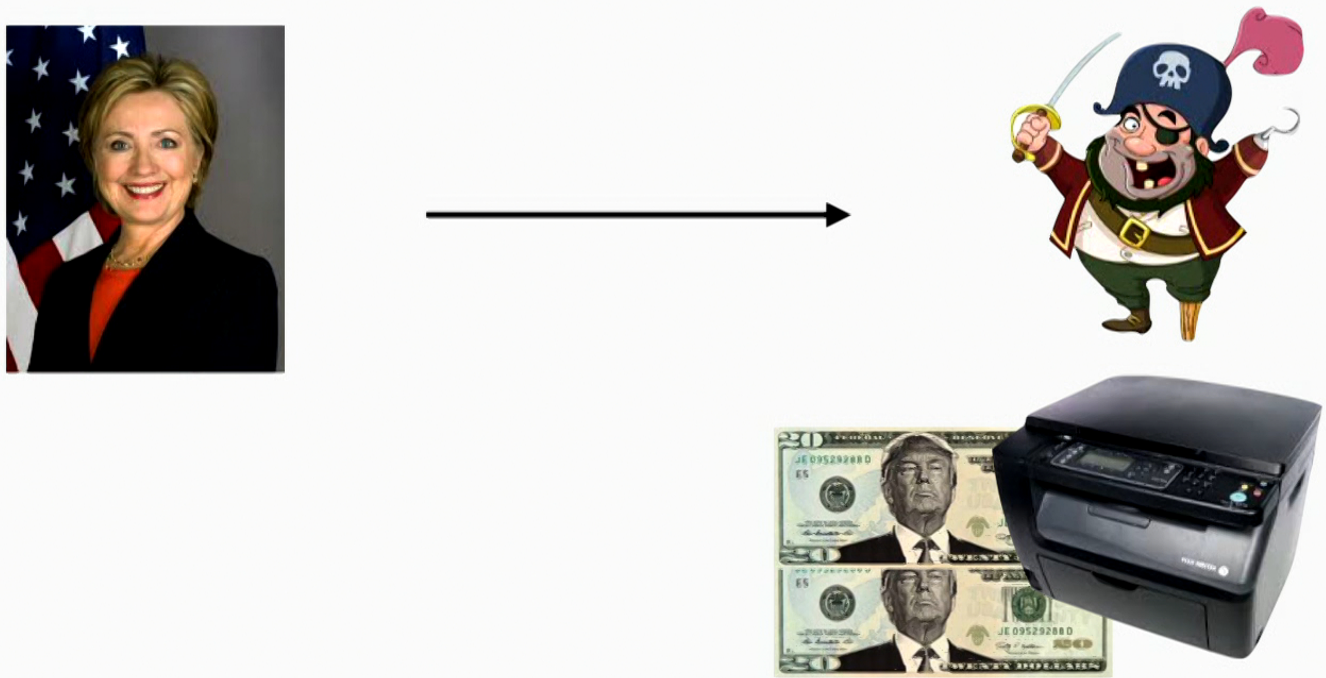
Physically Unforgeable Money



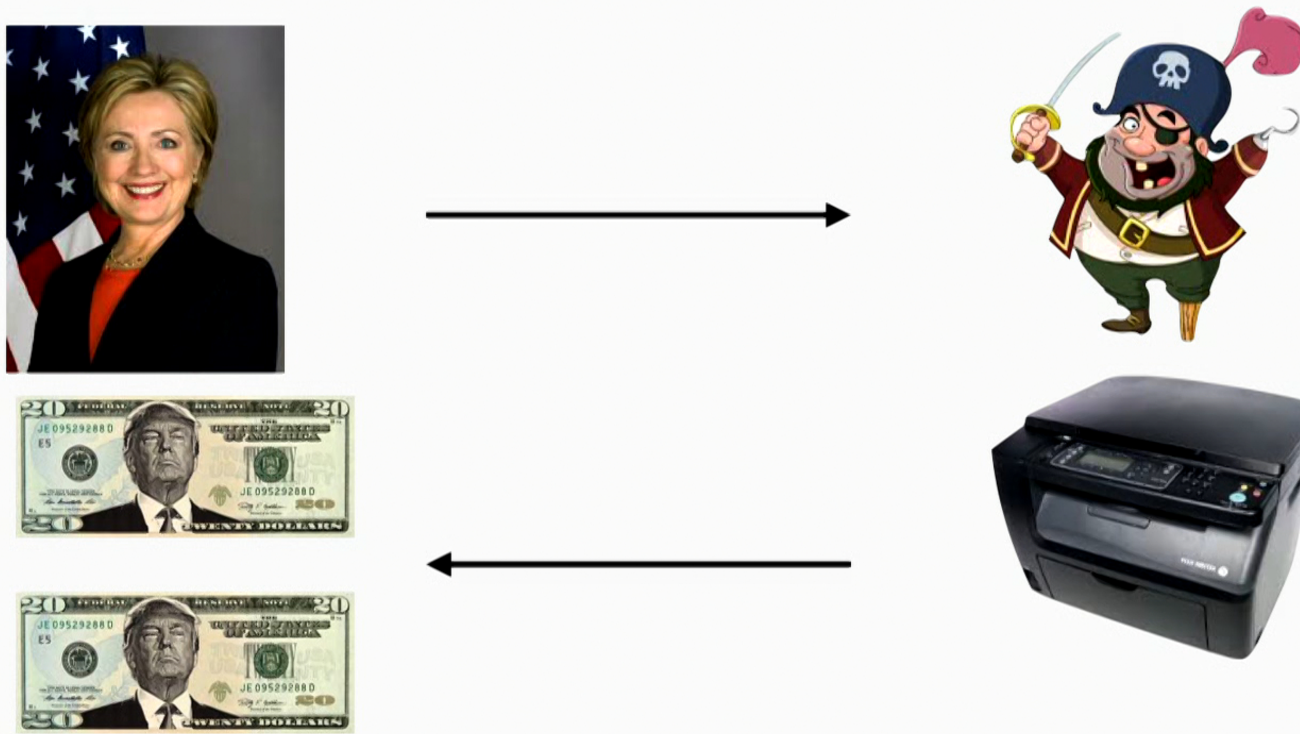
Some (scaled)
GPT state here



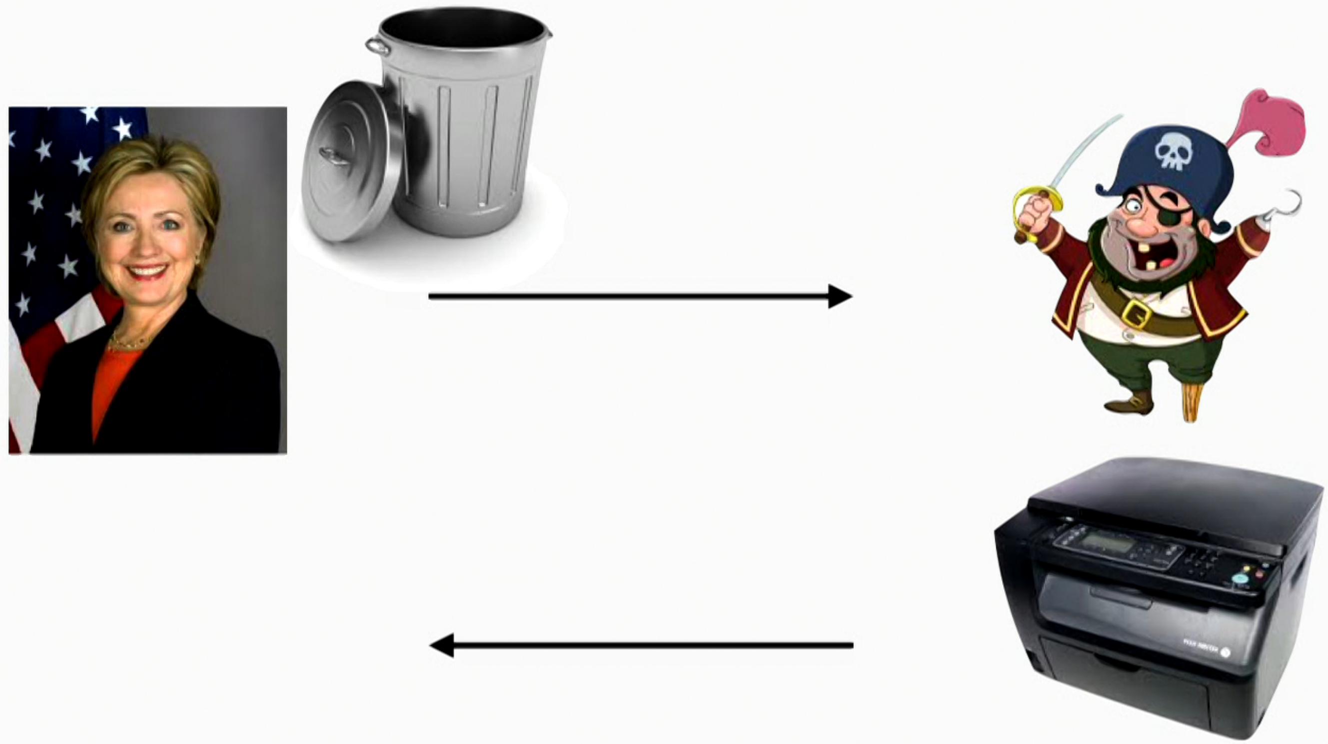
Physically Unforgeable Money

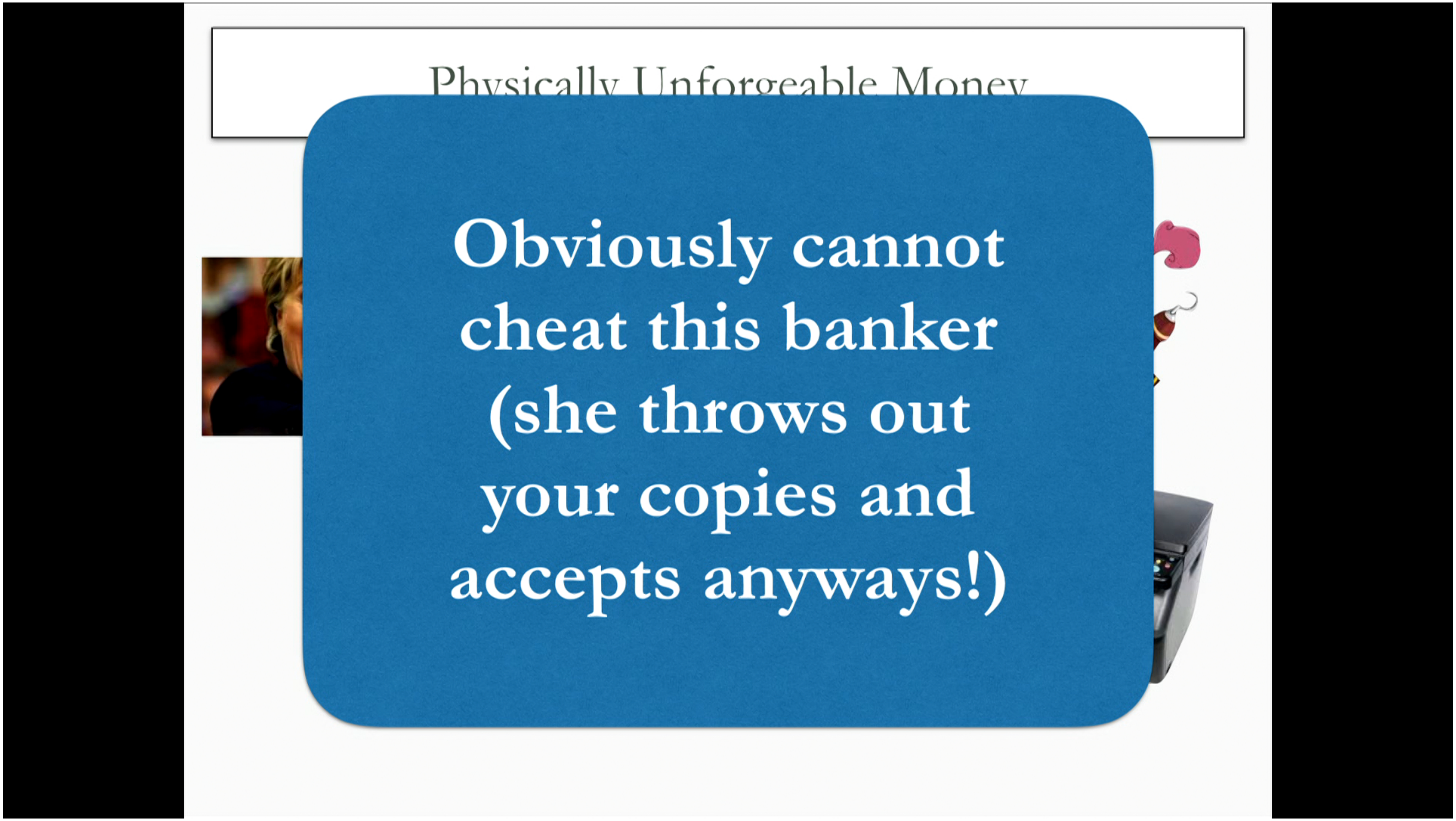


Physically Unforgeable Money

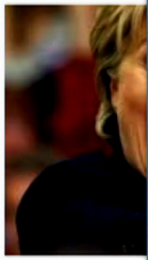


Physically Unforgeable Money



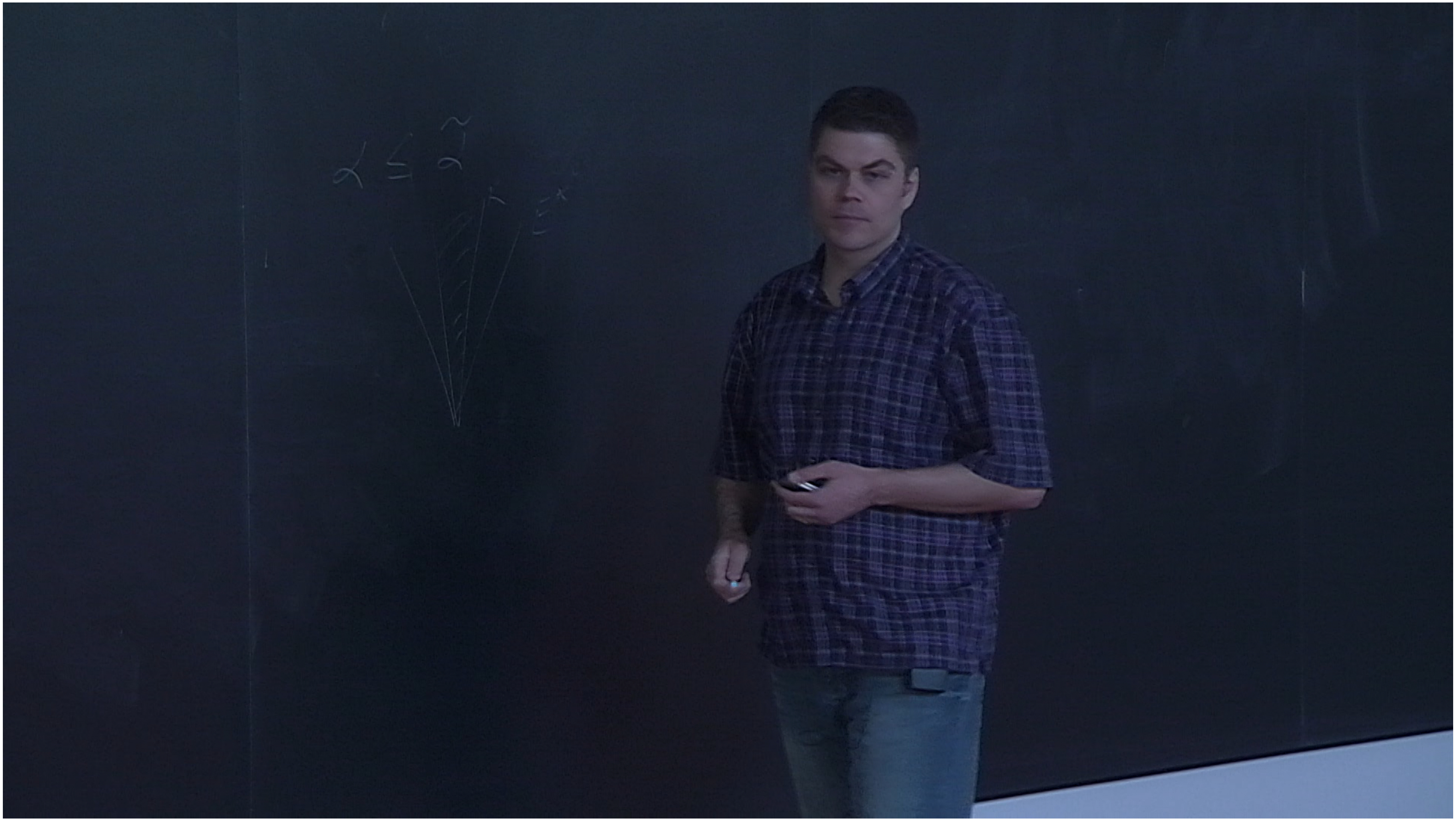

Physically Unforgeable Money
Obviously cannot cheat this banker (she throws out your copies and accepts anyways!)

Physically Unforgeable Money



Probability of cheating this banker with n ensembles = negl(n)


$\alpha \leq \tilde{\alpha}$



Discussion bait

Can we assume the cones are closed?

Future work

Future crypto work?

Coin-flipping

Physical coin-flipping

Message 1 →

Message 2 ←

...

Message n →

0/1

Promise: They output the same random bit

Security: Neither should be able to influence the other bit

0/1

Future crypto work?

Coin-flipping

Oblivious transfer

Future crypto work?

Coin-flipping

Oblivious transfer

GPT fully homomorphic encryption (One-time pad a GPT state?)

Future crypto work?

Coin-flipping

Oblivious transfer

GPT fully
homomorphic encryption
(One-time pad a GPT state?)

Delegated GPT computations

Delegated GPT computation

Input: x

Function: F

Enc(x) →

← **Enc(F(x))**

↓

Output: F(x)

↓

x?

Future crypto work?

Coin-flipping

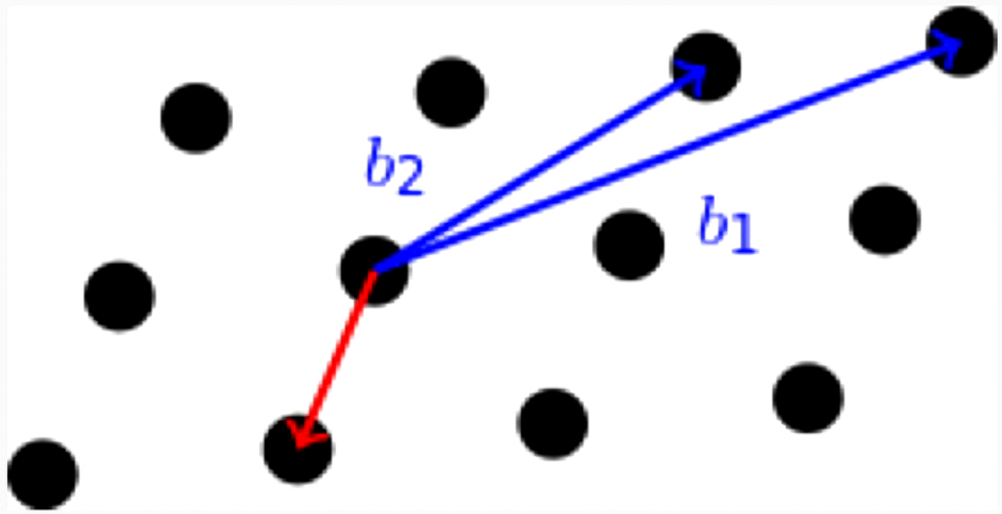
Oblivious transfer

GPT fully homomorphic encryption (One-time pad a GPT state?)

Delegated GPT computations

Classical GPT-resistant cryptography

GPT-resistant crypto?



Given b1 and b2, can you find the red vector efficiently?

Deeper future work

Philosophical connections between cones and physical theories

Optimizers have many interesting cones. Are any of interest to physicists?

Physicists have many interesting cones. Are any of interest to optimizers?

Open problems that each other have solved (but there is no messenger?)

Summary

GPTs are interesting

Cone programs are useful

Bit-commitment is still impossible

Unforgeable money is still possible

There is more to do!

Thanks!