Alice's Adventure in Quantum Wonderland

-- A New Approach to Post-Quantum Non-Malleability

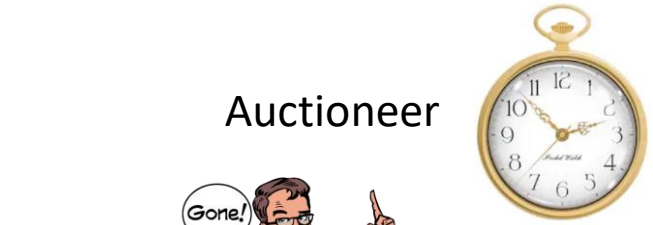
Xiao Liang

Omkant Pandey

Takashi Yamakawa

Alice Attending an Auction

Auctioneer

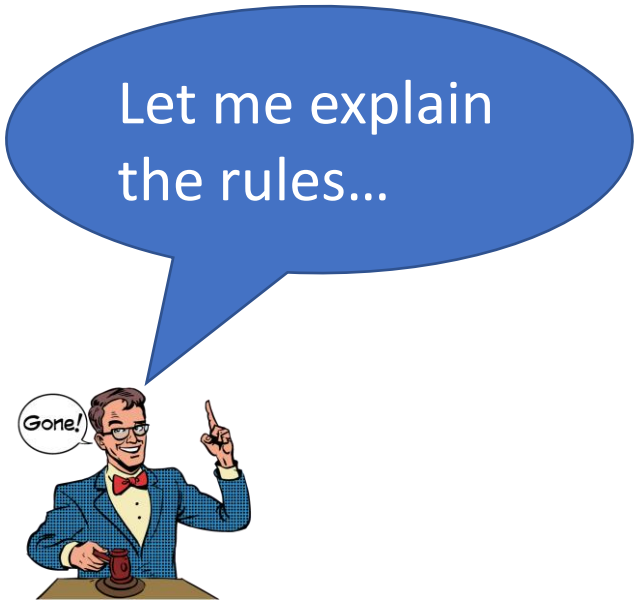


Alice Attending an Auction

Auctioneer

I really want it. Cuz it is THE watch!

Rules for Auction

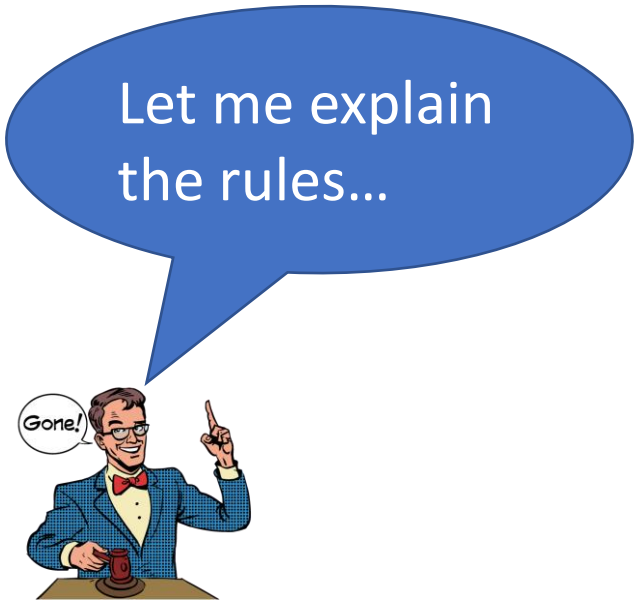


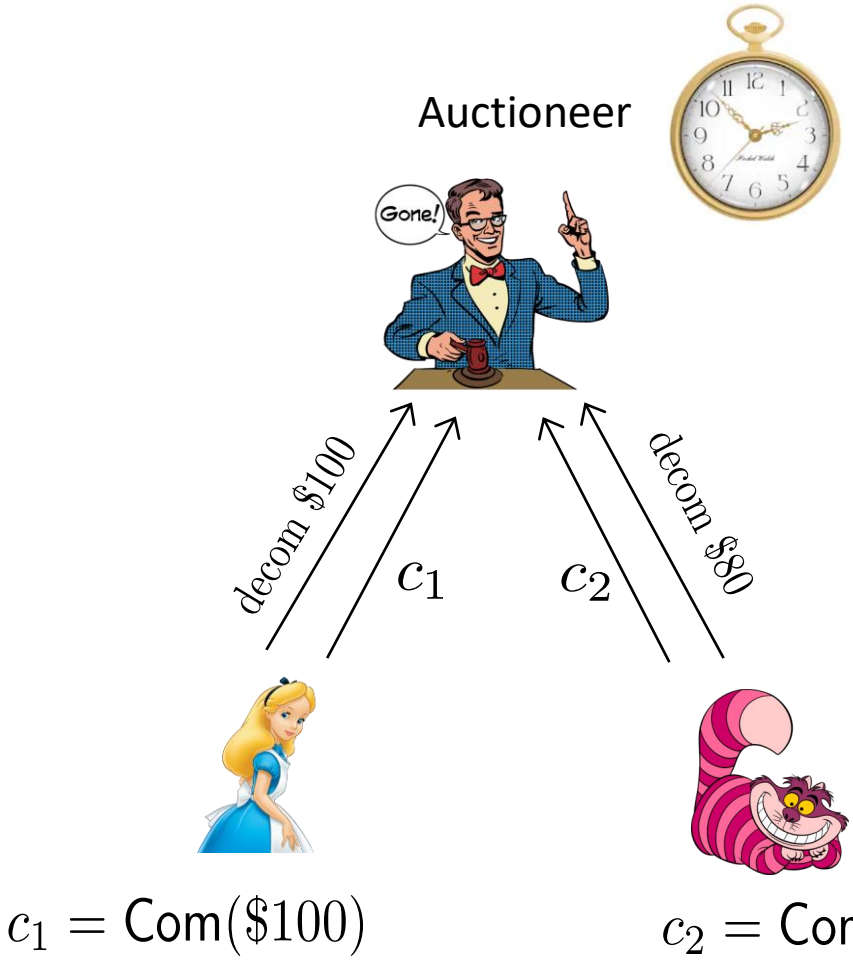
c_1 c_2

$c_1 = \mathsf{Com}(\$100)$

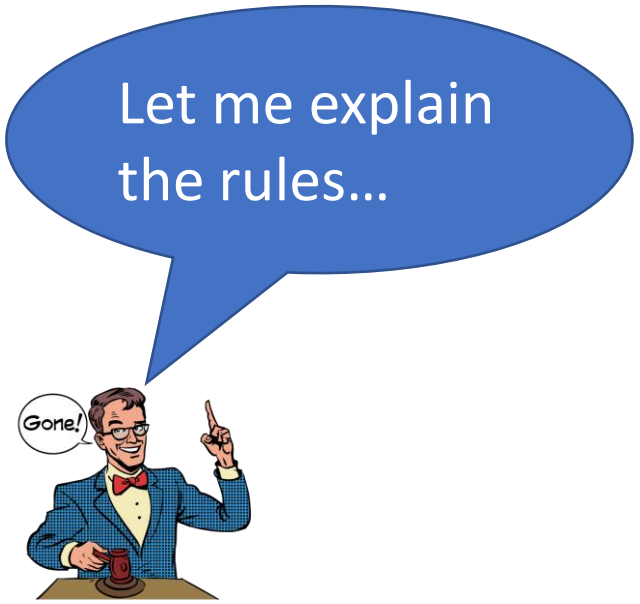
$c_2 = \mathsf{Com}(\$80)$

Rules for Auction





Rules for Auction



Alice: $100
Cat: $80

Auctioneer

Alice won!

$\mathsf{decom}\ \$100$ c_1 c_2 $\mathsf{decom}\ \$80$

$c_1 = \mathsf{Com}(\$100)$

$c_2 = \mathsf{Com}(\$80)$

Potential Attacks

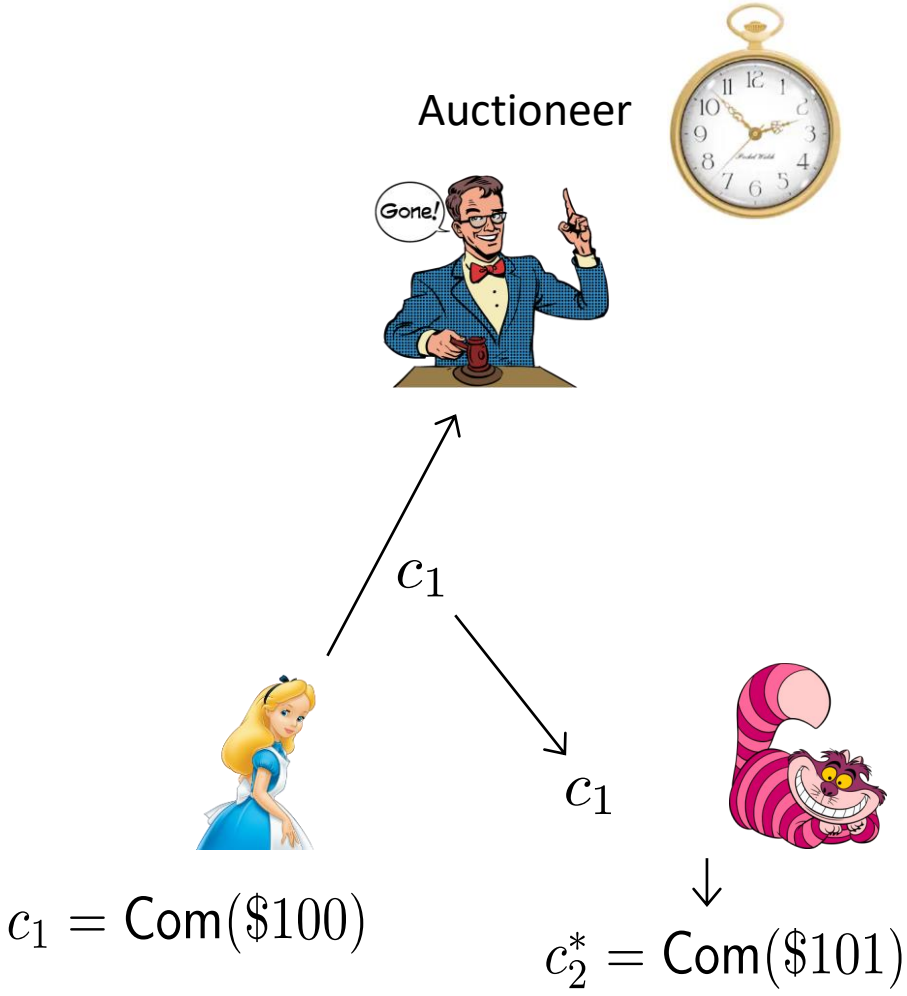
After appearing in so many crypto papers,
Alice now is already a cryptographer ….

Potential Attacks

After appearing in so many crypto papers,
Alice now is already a cryptographer ….

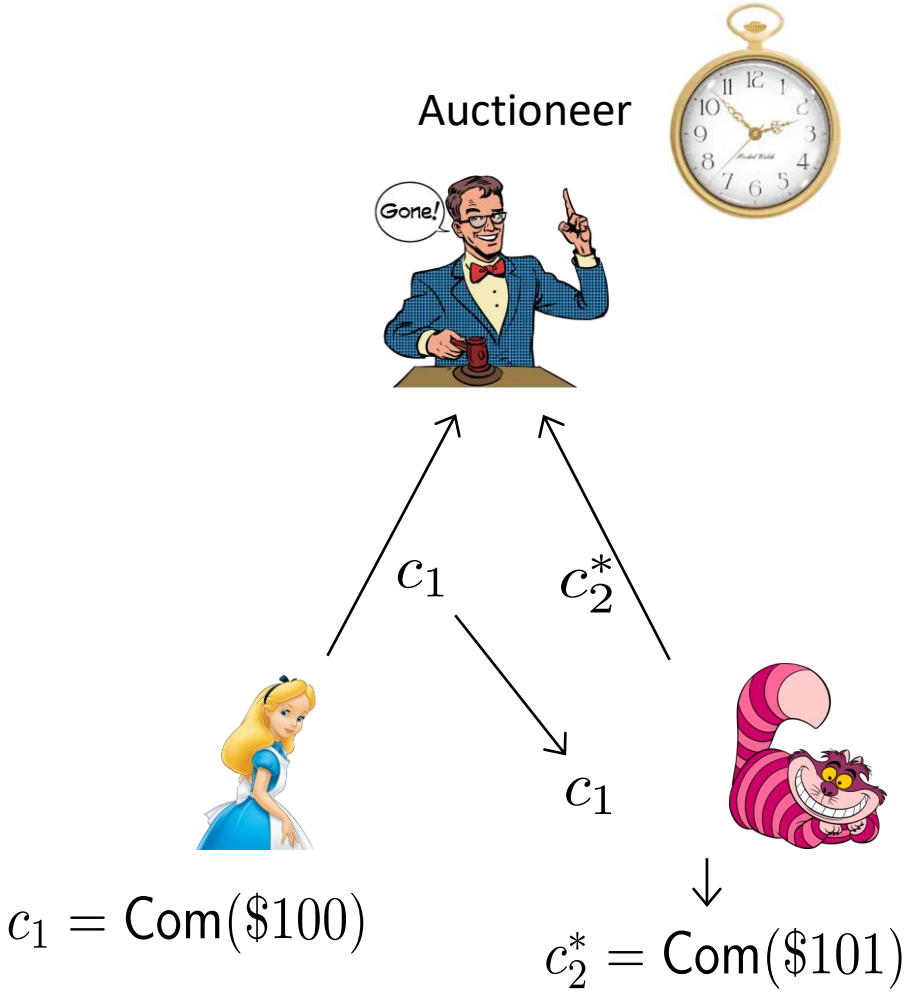
Potential Attacks

After appearing in so many crypto papers,
Alice now is already a cryptographer ….



Potential Attacks

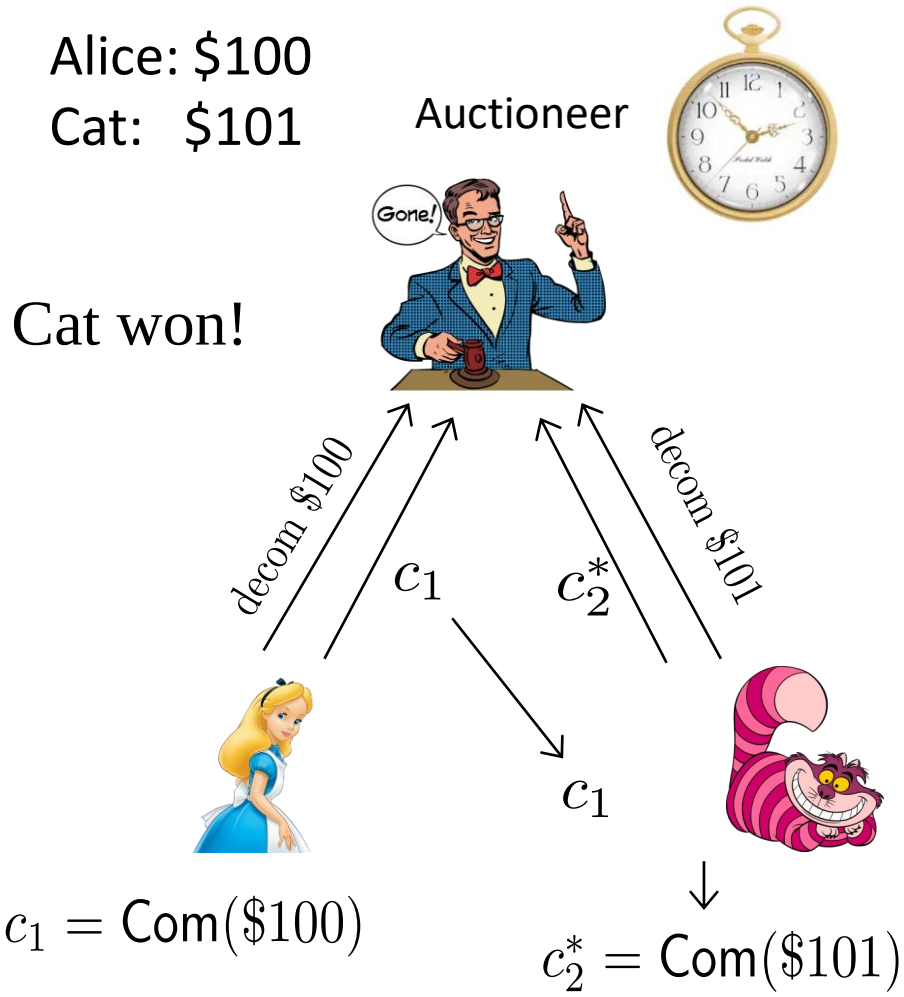
After appearing in so many crypto papers,
Alice now is already a cryptographer ….



Potential Attacks

After appearing in so many crypto papers,
Alice now is already a cryptographer ….

Alice: $100
Cat: $101



Potential Attacks

After appearing in so many crypto papers,
Alice now is already a cryptographer ….

Emm… Make sense. Do you have any suggestions? We care about customers' security

Alice: $100
Cat: $101

Auctioneer

Cat won!

decom $100

c_1

c_2^*

decom $101

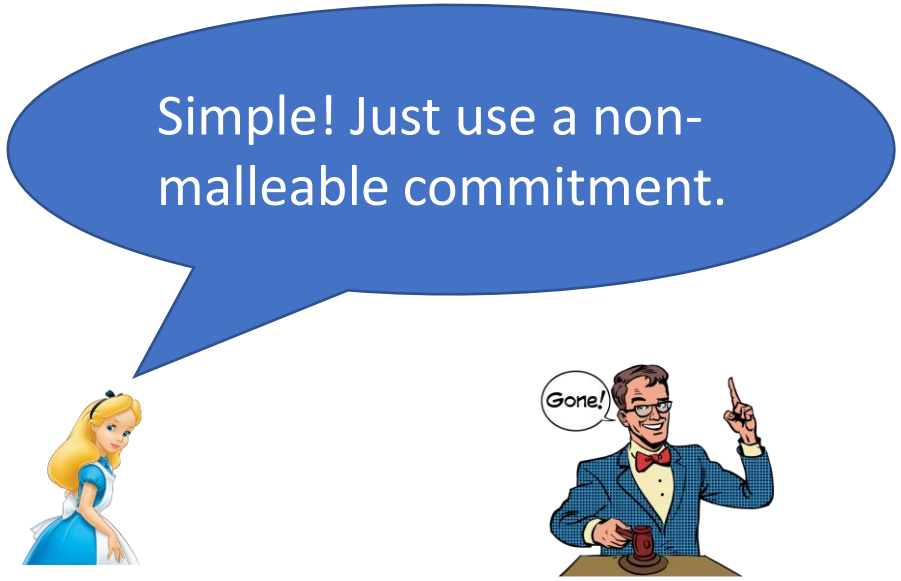
c_1

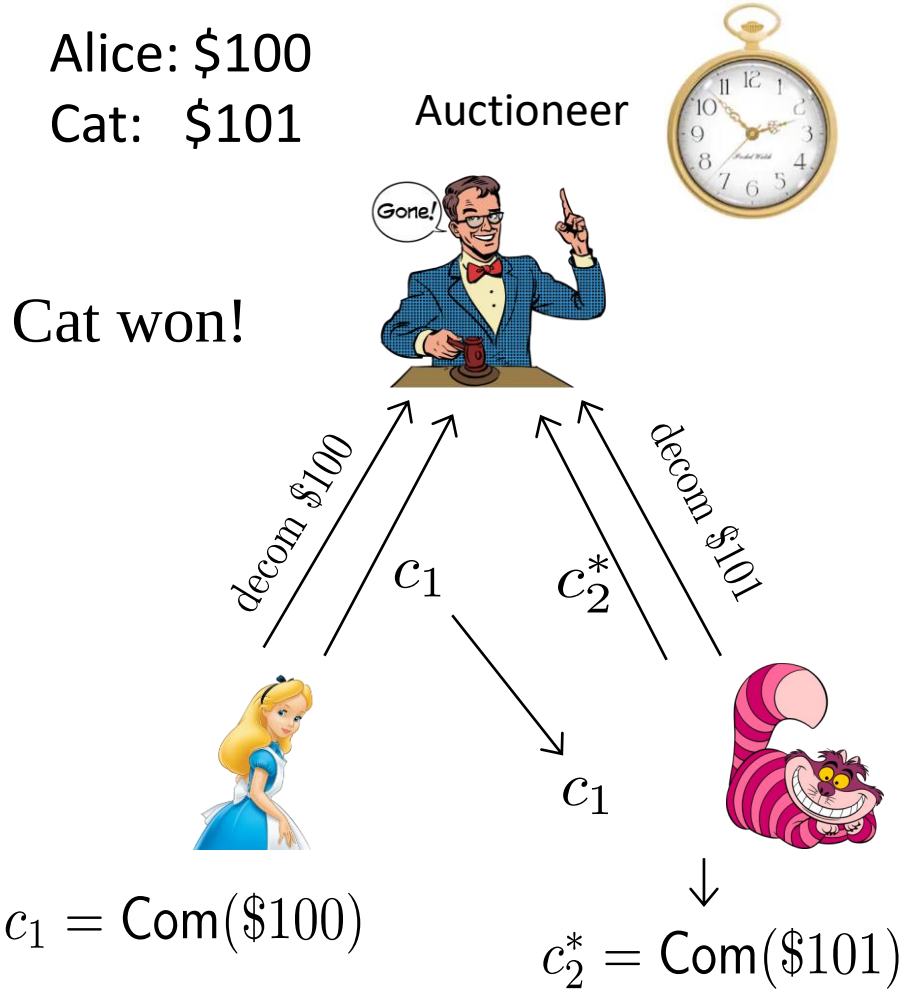
$c_1 = \mathsf{Com}(\$100)$

$c_2^* = \mathsf{Com}(\$101)$

Potential Attacks

After appearing in so many crypto papers,
Alice now is already a cryptographer ….





Potential Attacks

After appearing in so many crypto papers,
Alice now is already a cryptographer ….

Good idea! We'll adapt this strategy.

Alice: $100
Cat: $101

Auctioneer

Cat won!

decom $100

c_1

c_2^*

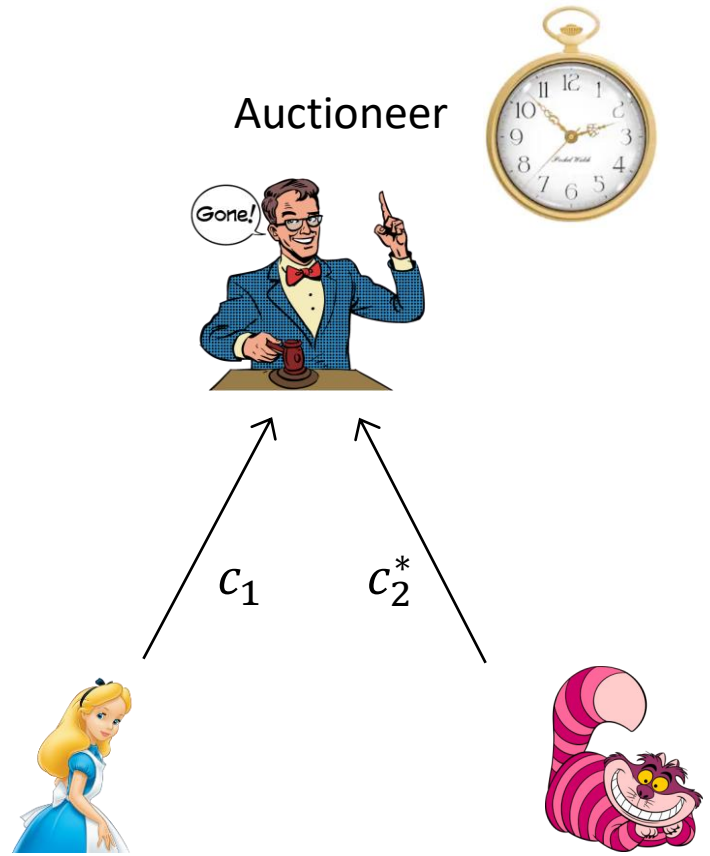
decom $101

c_1

$c_1 = \mathsf{Com}(\$100)$

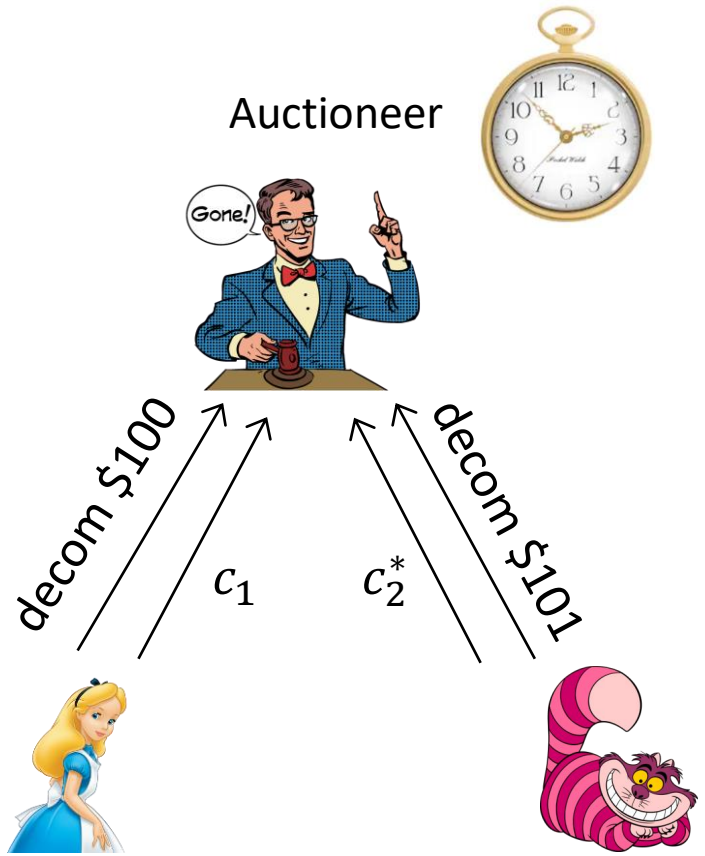
$c_2^* = \mathsf{Com}(\$101)$

Day of Auction



$$c_1 = NMCom(\$100)$$

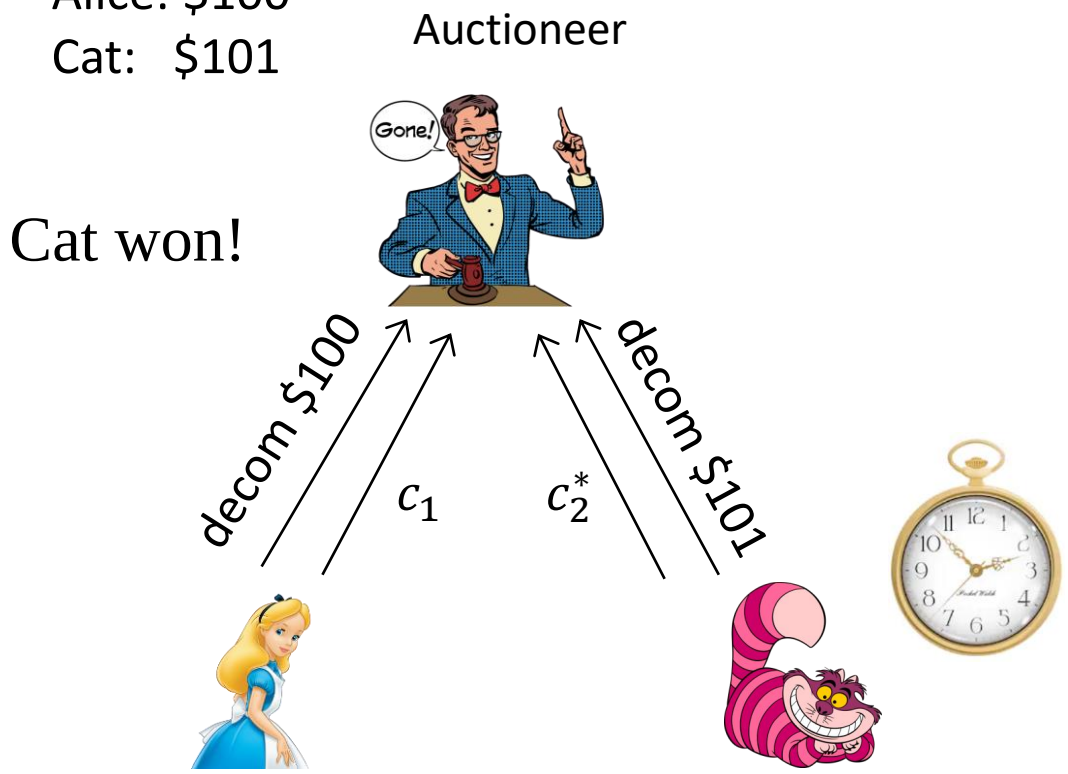
Day of Auction



$$c_1 = NMCom(\$100)$$

Day of Auction

Alice: $100
Cat: $101



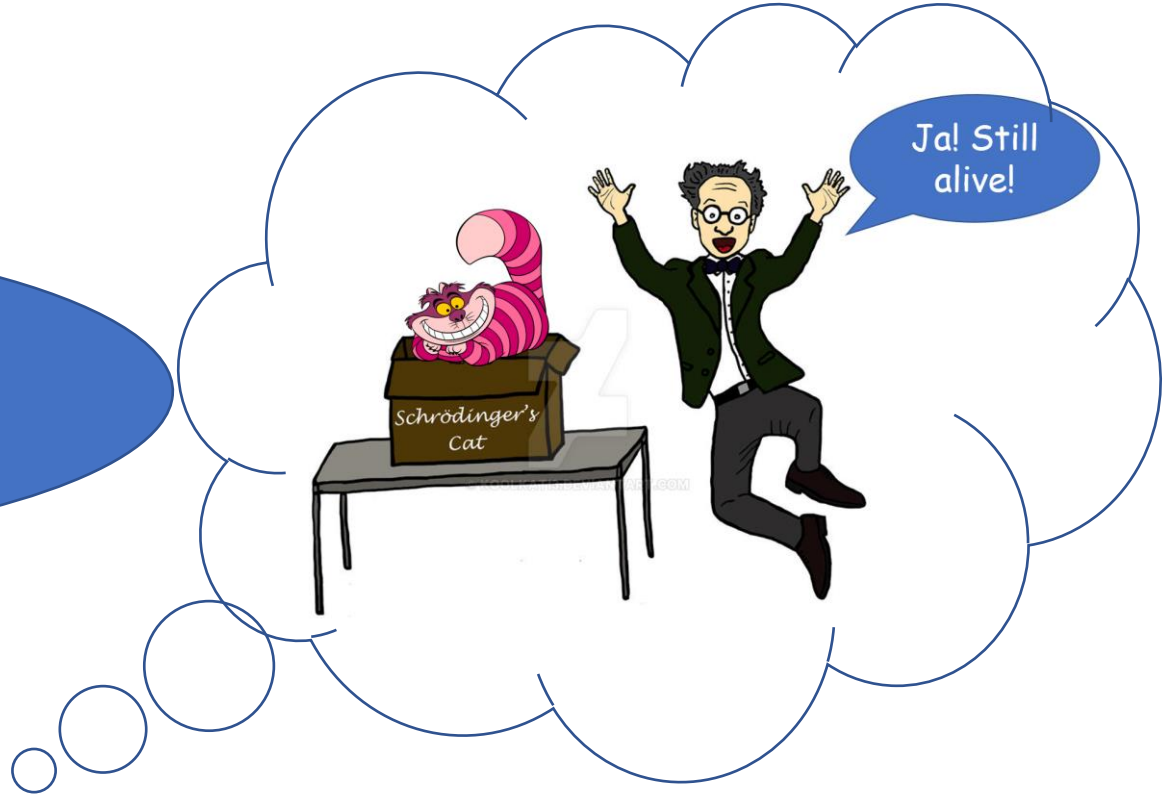
$$c_1 = NMCom(\$100)$$

Schrödinger's Cat

Surprising, ha? Alice, you aren’t the only one who gets into research papers.

Schrödinger's Cat

I’m actually Schrödinger’s cat.
That crazy guy performed
thousands of experiments on me!

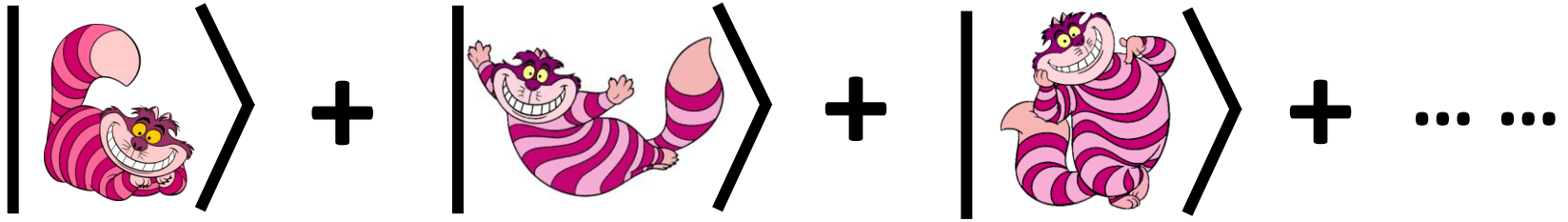


Schröding

WARNING: MENTAL EXPERIMENTS ONLY!

Schrödinger's Cat

Eventually, I gain Quantum Power!



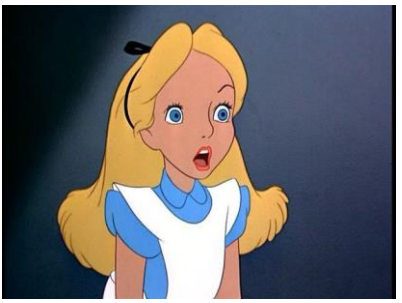
Schrödinger's Cat

Quantum! Beyond your Imagination…

$$|\text{Cheshire Cat}\rangle + |\text{Cheshire Cat}\rangle + |\text{Cheshire Cat}\rangle + |\text{Tom}\rangle$$

$$+ |\text{Cat}\rangle + |\text{Puss in Boots}\rangle + |\text{Garfield}\rangle + |\text{Catwoman}\rangle$$

? !



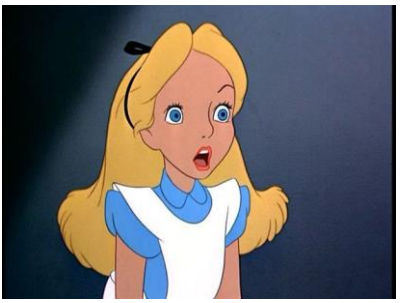
$$+ |\text{Felix}\rangle + |\text{Luna}\rangle + |\text{Gatomon}\rangle + |\text{Hello Kitty}\rangle + \cdots\cdots$$

Schrödinger's Cat

Quantum! Beyond your Imagination…

$$|\ \rangle + |\ \rangle + |\ \rangle + |\ \rangle + |\ \rangle + |\ \rangle + |\ \rangle + 0 \cdot |\ \rangle$$

? !



$$+ |\ \rangle + |\ \rangle + |\ \rangle + |\ \rangle + \cdots\ \cdots$$

Day of Auction (In Multiverse)

Day of Auction (In Multiverse)

Alice’s Lesson

Learn your lesson, Alice! Classical NMCom may NOT be non-malleable in the quantum setting.

Friends, Help!

What should I do now?

Friends, Help!

What should I do now?

Friends, Help!

What should I do now?

Sorry Alice, we're late. But we eventually get quantumly-secure non-malleable commitments!

Friends, Help!

But I don’t have quantum power.

Friends, Help!

But I don’t have quantum power.

Totally Fine! To run our protocol, honest parties can be classical! It’s “Post-Quantum”!

Friends, Help!

But the auctioneer also cares about interaction complexity...

Friends, Help!

This is also fine. Our protocol is constant-round!

But the auctioneer also cares about interaction complexity...

Friends, Help!

What about the assumptions?
If you go as crazy as iO, I don't think the auctioneer will buy it.

Friends, Help!

What about the assumptions? If you go as crazy as iO, I don't think the auctioneer will buy it.

No Worries. We only use the minimal assumption of OWFs! Of course, post-quantum OWFs.

Friends, Help!

But the auction already happened.

Friends, Help!

Hey, I’m Time. I can rewind you back to the beginning of the auction!

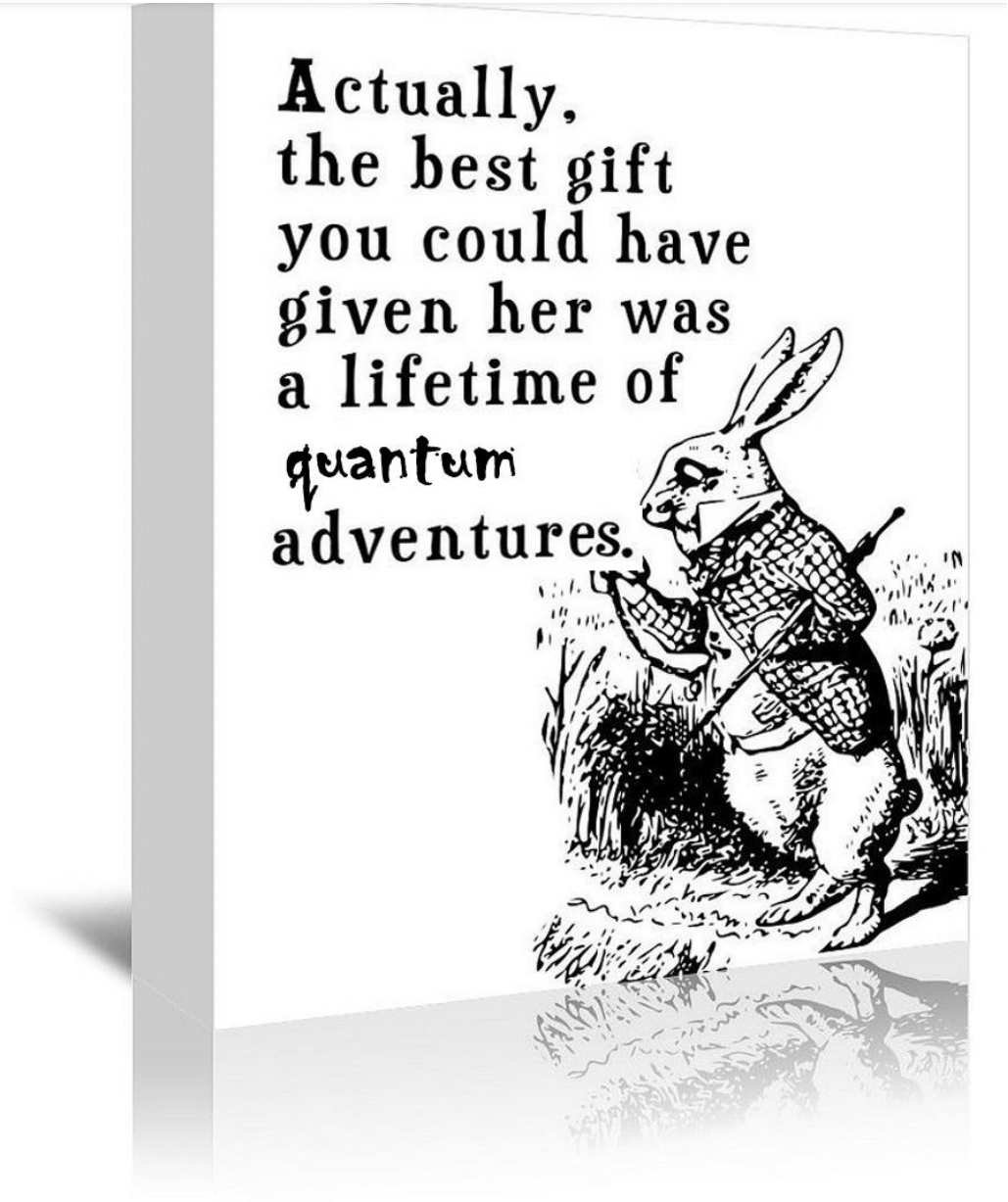
But the auction already happened.

Friends, Help!

Hey, I’m Time. I can rewind you back to the beginning of the auction!

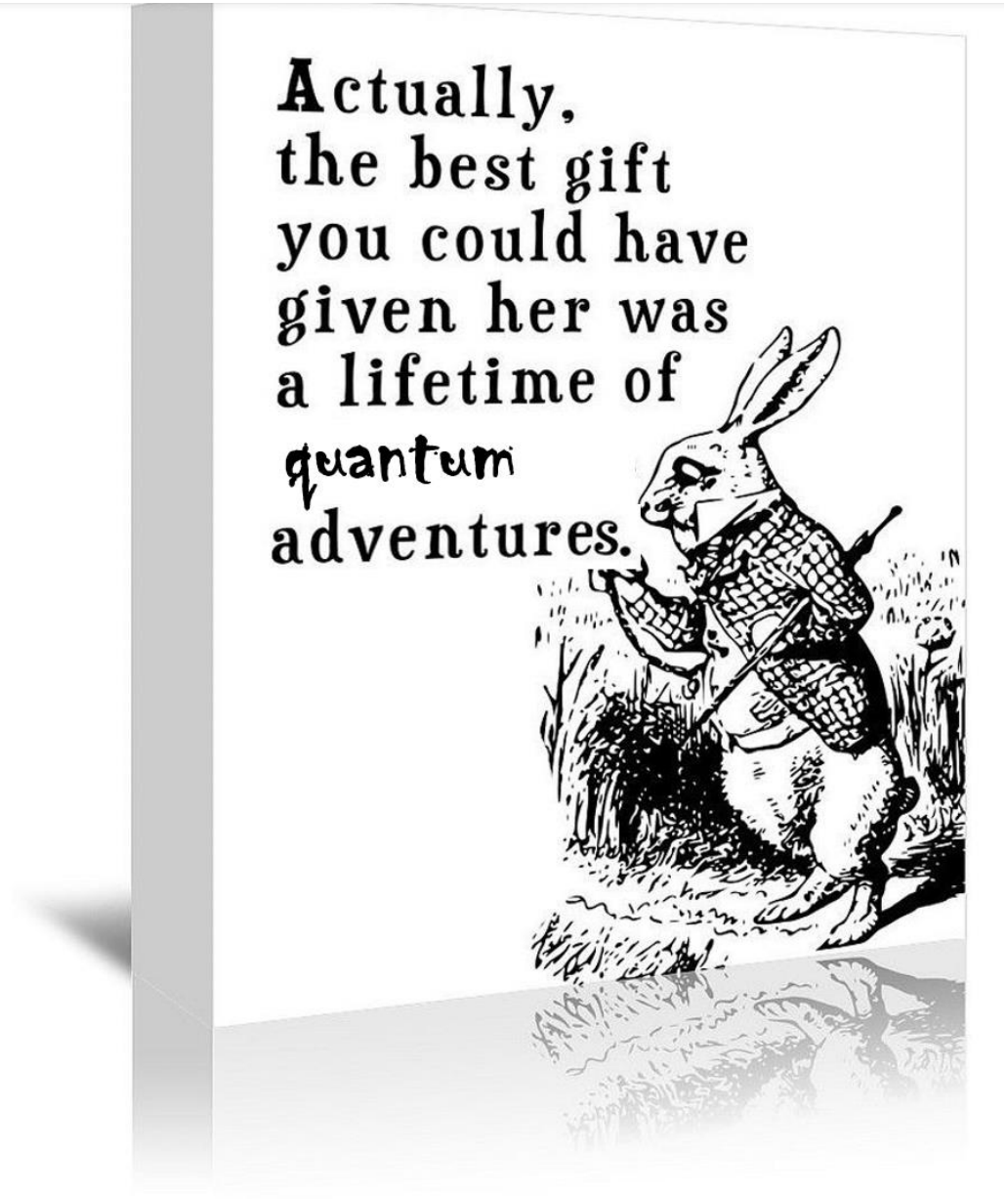
That’s cool. Let’s go!

Thank You!



Link to our paper: [ia.cr/2022/907](ia.cr/2022/907)

Thank You!



Quiz: From which manga does this cat come from?

Prize: Find Omkant to redeem your free drink.

Link to our paper: ia.cr/2022/907