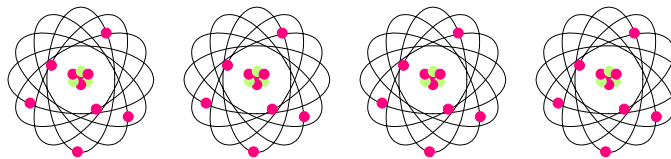
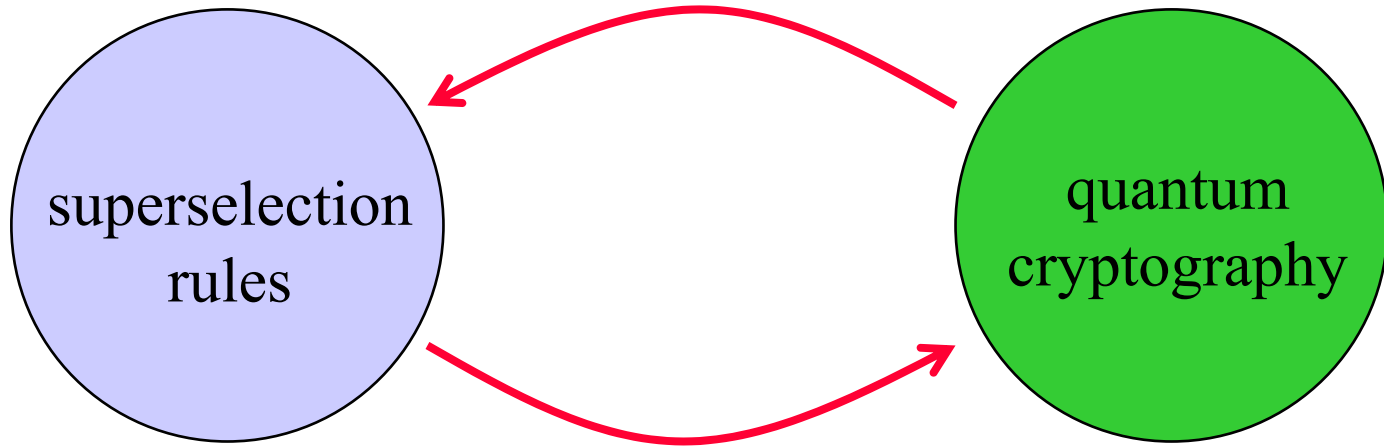


Quantum information and quantum mechanics: fundamental issues



Some important issues in quantum cryptography:

- Can we close the gap between ideal realizations of quantum key distribution (assumed in proofs of “unconditional” security) and current implementations?
- Can we extend the range of quantum key distribution well beyond the attenuation length of optical fibers?
- Can quantum protocols achieve information-theoretic security for other cryptographic tasks beyond key distribution?
- Are there “quantum one-way functions” and if so can they be used to execute cryptographic protocols with quantum-computational security?



A. Kitaev, D. Mayers, and J. Preskill, "Superselection rules and quantum protocols," quant-ph/0310088.



Kitaev



Mayers

Bit Commitment

Commitment: Alice chooses $a \in \{0,1\}$

Binding: Alice cannot change a .

Concealing: Bob cannot learn a .

Unveiling: Alice reveals and Bob verifies.

Secure if both binding and concealing.

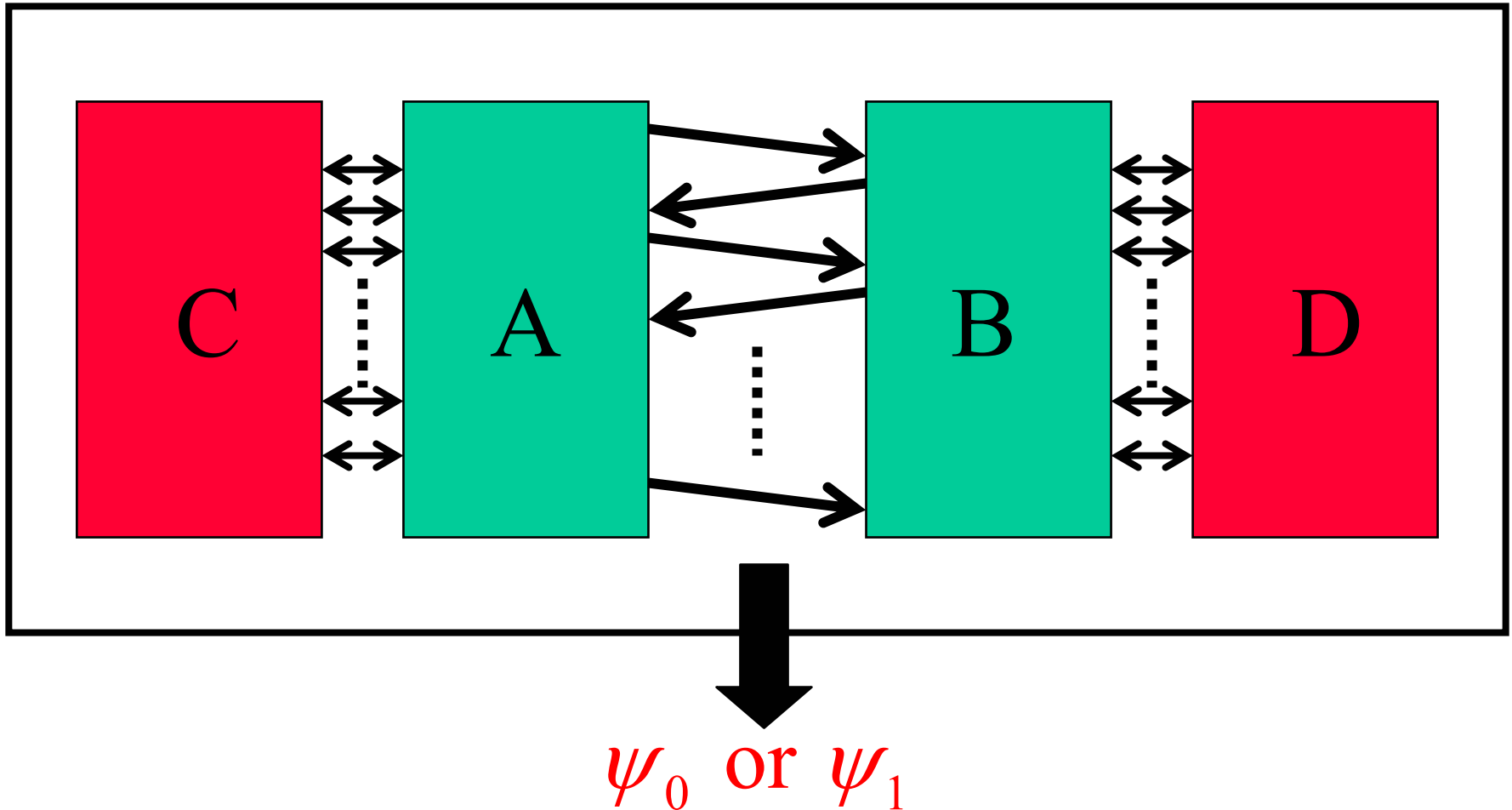
Bit Commitment

There are *computationally secure* classical bit commitment protocols.

For example, To commit, Alice can pick two large primes p and q , where either both p and q are congruent to $+1 \pmod{4}$ ($a=0$), or both p and q are congruent to $-1 \pmod{4}$ ($a=1$), and send the product pq to Bob. To unveil, Alice reveals the prime factors.

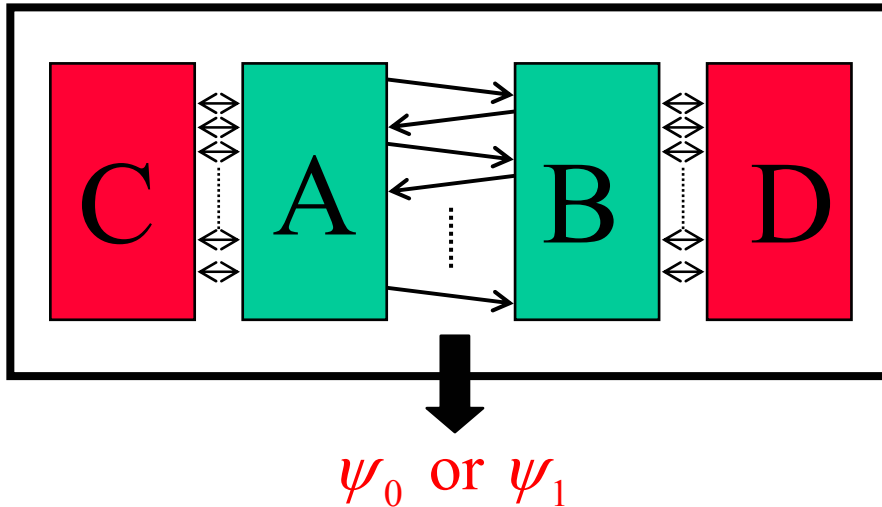
This, and other computationally secure classical bit commitment protocols, are vulnerable to quantum attacks.

Quantum Bit Commitment



Consider the purified protocol, by including an environment for Alice and an environment for Bob. All operations are unitaries, and at the end of commitment, Alice and Bob share a pure state. (Mayers and Lo-Chau, 1996)

Quantum Bit Commitment



Consider the purified protocol, by including an environment for Alice and an environment for Bob. All operations are unitaries, and at the end of commitment, Alice and Bob share a pure state.

Concealing: $\rho_{0,BD} = \rho_{1,BD}$

$\Rightarrow \psi_1 = U_{AC}\psi_0 \Rightarrow$ **Not Binding**

... without (quantum) computational assumptions.

Unconditionally secure quantum bit commitment is impossible.

What about
superselection rules?



Popescu

-- Even if we don't wish to make *computational* assumptions, our model should incorporate all *fundamental physical limitations* on the operations that can be performed by an adversary.

-- Perhaps thinking about how the restricted world (subject to superselection) and the unrestricted world can *simulate* one another can deepen our understanding of the physical meaning of superselection rules.

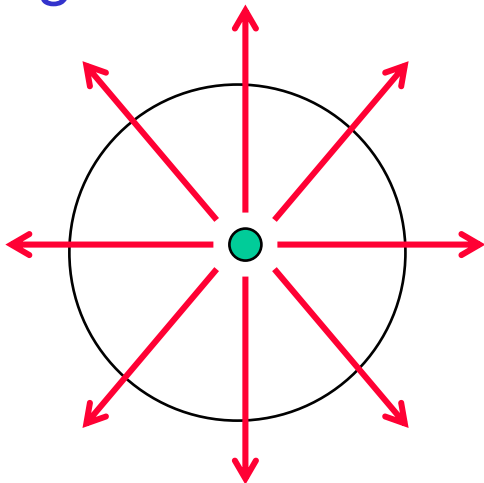
Superselection rules

A superselection rule is a decomposition of Hilbert space into sectors that are preserved by local operations.

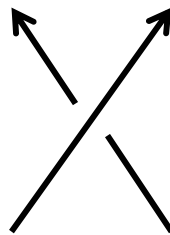
$$\mathcal{H} = \bigoplus_q \mathcal{H}_q, \quad \mathcal{O} = \bigoplus_q \mathcal{L}(\mathcal{H}_q)$$

Alice cannot change the charge in her laboratory.

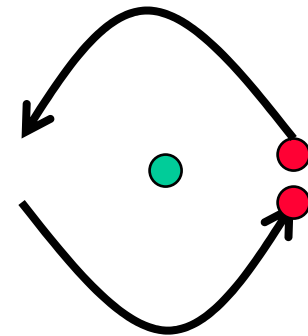
operations preserve each charge sector



electric charge



fermion



Aharonov-Bohm phase

Superselection rules

A superselection rule is a decomposition of Hilbert space into sectors that are preserved by local operations.

$$\mathcal{H} = \bigoplus_q \mathcal{H}_q, \quad \mathcal{O} = \bigoplus_q \mathcal{L}(\mathcal{H}_q)$$

Important special case: charge q labels an irreducible representation of a compact group G . Then allowed operations commute with the action of G . For example $G=U(1)$ for the case of the charge superselection rule.

But there is a richer classification (especially in two spatial dimensions, where q can be the charge of a nonabelian anyon):

$$\mathcal{H}_q = \bigoplus_{q_A, q_B} \mathcal{H}_{A, q_A} \otimes \mathcal{H}_{B, q_B} \otimes V_q^{q_A, q_B}$$



vector space
describes fusion of
charge sectors

Superselection rules

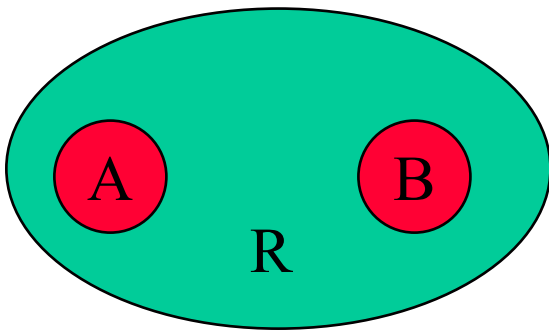
Naively, the superselection rule means that the relative phase in a superposition of states with different charge is unobservable.

$$|\psi\rangle = \alpha |q=0\rangle + \beta e^{i\varphi} |q=1\rangle$$

unobservable

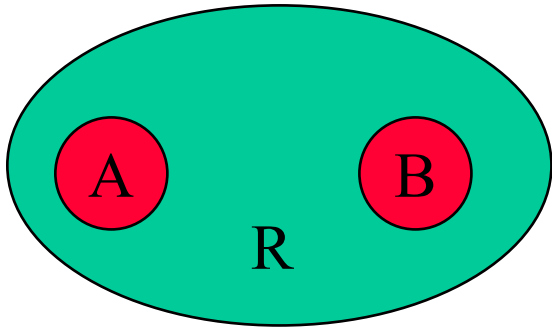
However, this conclusion might be evaded in the presence of a charge reservoir (“condensate”) that provides a reference phase standard.

$$|\psi\rangle_A = \sum_q \psi_q e^{i\varphi_q} |q\rangle_A \Rightarrow \sum_q \psi_q e^{i\varphi_q} | -q\rangle_R \otimes |q\rangle_A$$



Phases become observable if the reservoir remains accessible. (Cf. superconductor, or shared optical phase standard.)

Superselection rules

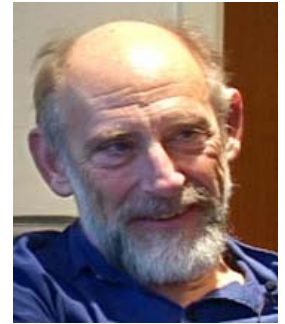


Phases become observable if the reservoir remains accessible. (Cf. superconductor, or shared optical phase standard.)

“We suggest that, contrary to a widespread belief, interference may be possible between states with different charges.” Phys. Rev. 155, 1428-1431 (1967).



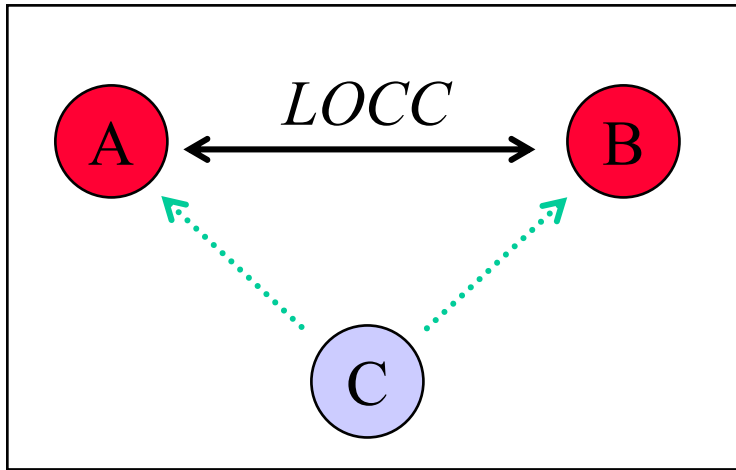
Aharonov



Susskind

“Our conclusion is that coherence between different values of an additive conserved quantity Q is really a way of speaking about the special interference effects which occur when the source and detectors of particles are correlated and coherently share a fixed amount of Q between them.”

Data Hiding



Charlie distributes one of two mutually orthogonal (pure) quantum states to Alice and Bob, who are limited to *charge-conserving* local operations and classical communication.

E.g.,
$$|\pm\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0,1\rangle_{AB} \pm |1,0\rangle_{AB} \right)$$

The relative phase is completely inaccessible locally, but the hidden bit can be unlocked if Alice and Bob establish correlated charge reservoirs through quantum communication. Do superselection rules enhance security beyond the LOCC model?

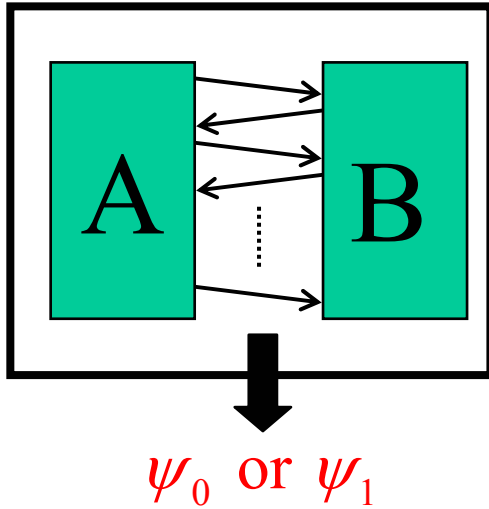


Verstraete



Cirac

Back to quantum bit commitment



First suppose that the total charge shared by Alice and Bob is trivial (fuses trivially with other charge sectors). Then, quite generally, the charges held by Alice and Bob are perfectly (anti)-correlated:

$$\mathcal{H}_1 = \bigoplus_q \mathcal{H}_{A,q} \otimes \mathcal{H}_{B,\bar{q}}$$

Thus, if Alice has a definite charge, then Bob does, too.

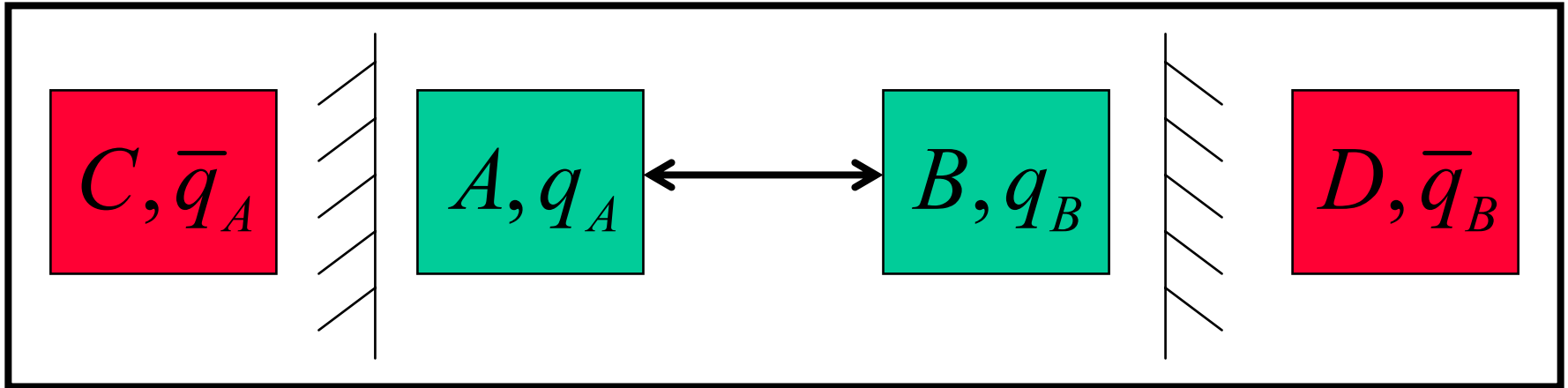
$$|\psi_0\rangle = \sum_q \sqrt{p_q} |\psi_{0,\bar{q}}\rangle_A \otimes |\psi_{0,q}\rangle_B$$

$$|\psi_1\rangle = \sum_q \sqrt{p_q} |\psi_{1,\bar{q}}\rangle_A \otimes |\psi_{1,q}\rangle_B$$

If the purified protocol is concealing, then the probability that Bob's charge is q does not depend on the value of the bit $a \in \{0,1\}$. Furthermore, Bob's density operator is independent of a in each charge sector.

Thus, Alice can do a unitary conditioned on the charge q that rotates $|\psi_0\rangle$ to $|\psi_1\rangle$. (Concealing \rightarrow not binding.) For any additive (abelian) charge, this argument applies even if the total charge is nontrivial.

A trivial-charge purification



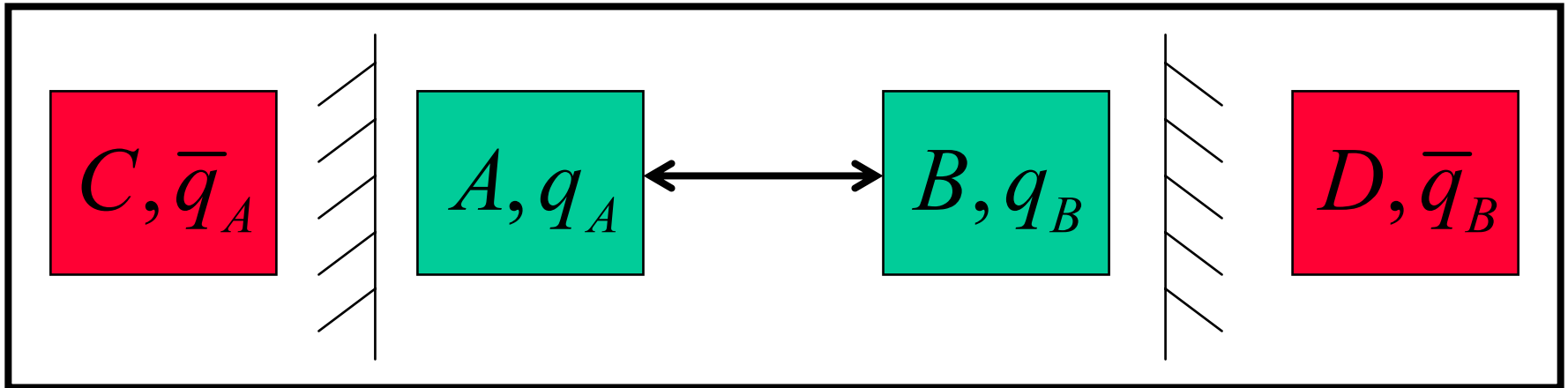
At the beginning of the protocol, each party has a *compensating* charge, which is never touched in the honest protocol.

A cheater could seize control of the compensating charge. (For example, Alice could throw away the initial state called for in the honest protocol, and replace it with a trivially charged state that she controls).

For an honest party, it doesn't matter whether the compensating charge is present or not.

Therefore, a protocol with nonzero total charge can be no more secure than a protocol in which each party starts with trivial charge. (True not just for bit commitment, but for general n -party protocols.)

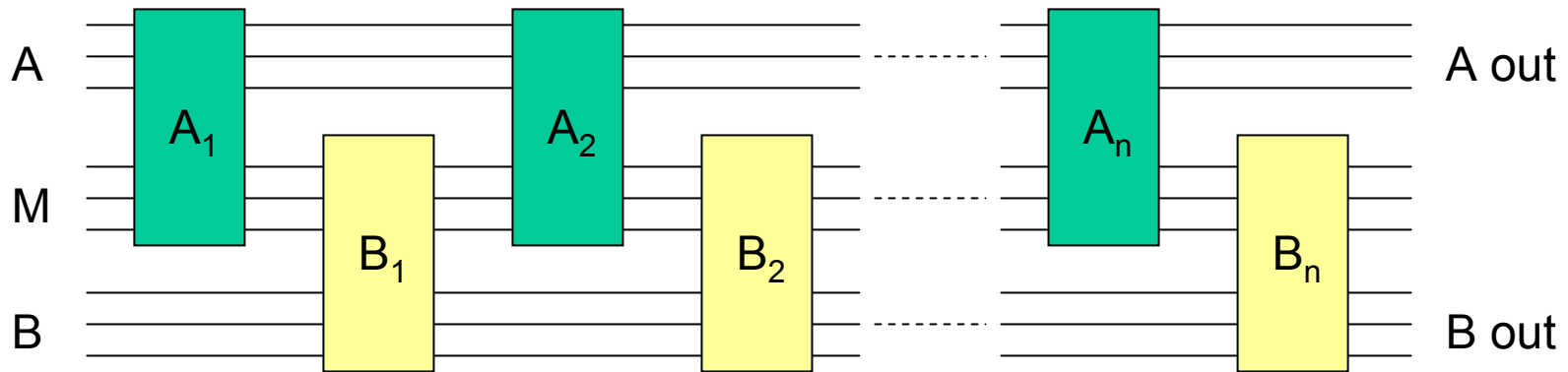
Quantum bit commitment and superselection



Theorem: Unconditionally secure quantum bit commitment is impossible, even in a world subject to superselection rules.

(Really a simple extension of the Mayers-Lo-Chau theorem.)

Superselection rules in quantum cryptography



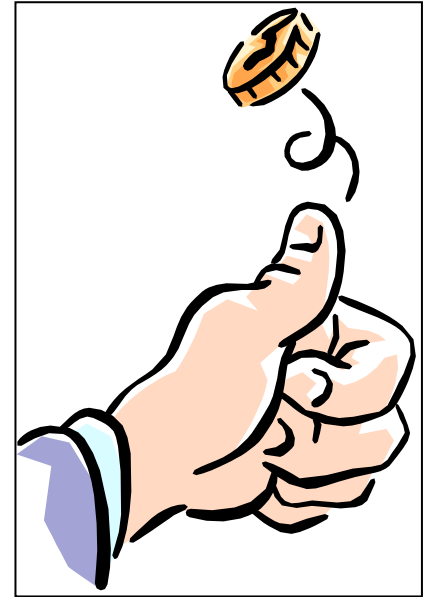
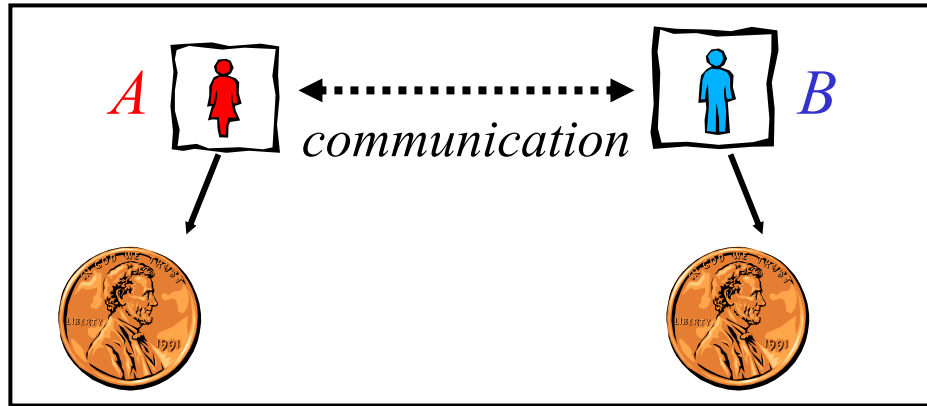
Consider a *quantum game*, in which Alice and Bob have private systems A and B, and a message system M that they pass back and forth a finite number of times until, to end the game, both make local measurements.

If both Alice and Bob play by the rules, the game achieves a particular goal (for example, an unbiased coin flip known to both parties).

But what if one of the parties *cheats*? We say that the game is *secure* if neither party, by departing from the protocol, can significantly bias the outcome of the other party's final measurement.

Quantum coin flipping

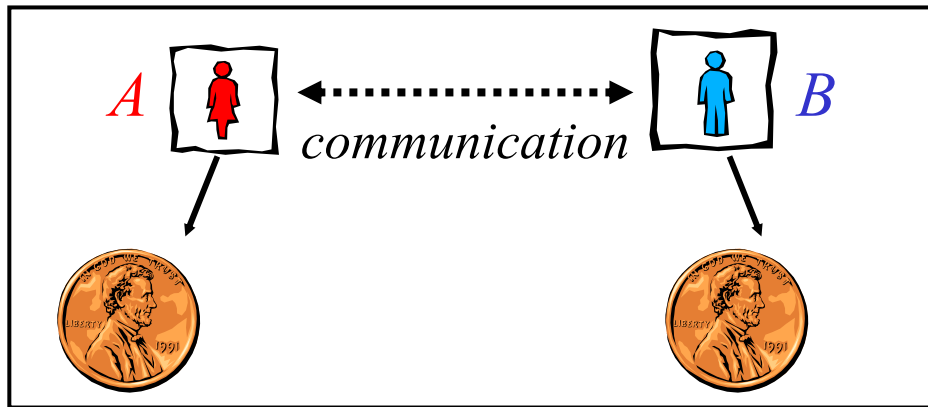
Alice (in Ventura) and Bob (in Pasadena) want to flip a fair coin “over the telephone” --- they have just divorced, and need to decide who gets the house.



We'd like to devise a game in which Alice and Bob takes turns, where each player prints out the outcome of the coin flip at the end of the game. The players should agree on the outcome when they play honestly; furthermore, neither player should be able to bias the other player's outcome by cheating.

Quantum coin flipping

We'd like to devise a game in which Alice and Bob takes turns, where each player prints out the outcome of the coin flip at the end of the game. The players should agree on the outcome when they play honestly; furthermore, neither player should be able to bias the other player's outcome by cheating.



There is no such *classical* protocol with *information-theoretic* security. Suppose Alice wins if the outcome is heads, and Bob wins if the outcome is tails. Then one player or the other has a strategy that ensures a win every time!

But there are quantum coin flipping in protocols in which neither player by cheating can force either outcome to occur with a probability greater than $\frac{3}{4}$, even if the cheating player uses an arbitrary strategy allowed by the laws of quantum physics (Ambainis, Spekkens-Rudolf). Is even better security possible?

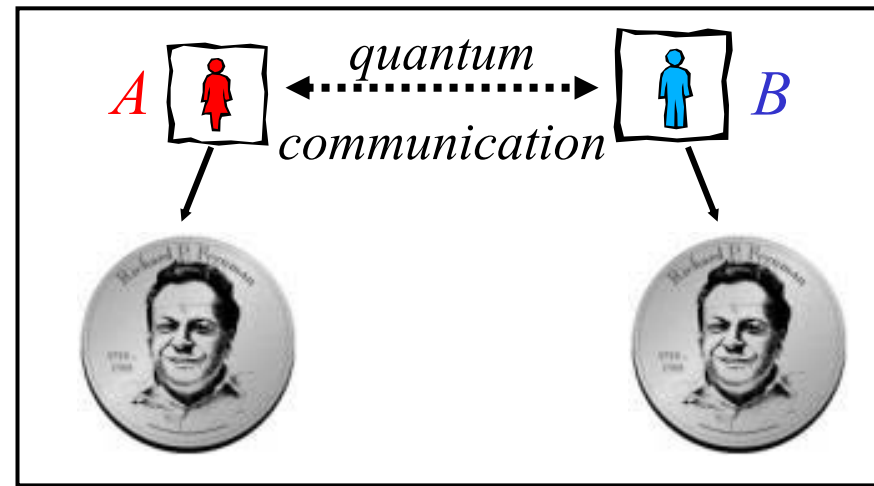
Quantum coin flipping



Kitaev



Ambainis



Strong coin flipping: Neither player can force *either* outcome with probability greater than $\frac{1}{2} + \varepsilon$.

Weak coin flipping: Neither player can force a *win* with probability greater than $\frac{1}{2} + \varepsilon$.

Kitaev: Strong coin tossing is *impossible* with bias

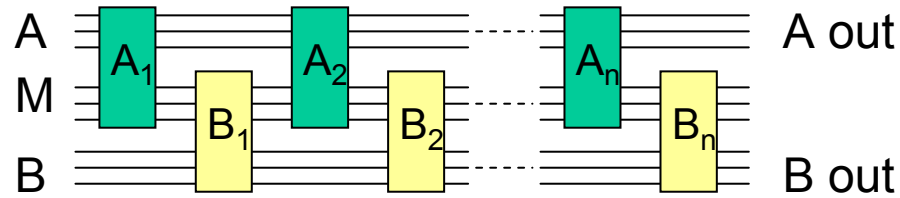
$$\varepsilon < 1/\sqrt{2} - 1/2 \cong .207.$$

Ambainis: Weak coin tossing with bias ε requires at least

$\Omega(\log \log(1/\varepsilon))$ rounds of communication.

Can the bias be arbitrarily small? An important open problem!

Superselection rules in quantum cryptography



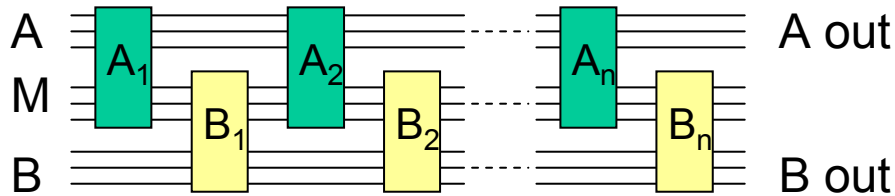
Do limitations on security derived in the unrestricted world (“ U -world”) also apply in the invariant world (“ I -world”)?

Claim: A cryptographic task can be securely realized in the “ I -world” if and only if it can be securely realized in the *unrestricted world* “ U -world”.

We give two proofs, using different methods, and which apply under different conditions:

- charge is labeled by an irreducible representation of a compact group. G -noninvariant operations can be simulated using the charge reservoir. (Applies to n -party games in which $k < n$ parties cheat.)
- general charges. Recipient of a message can check that it could have been sent by a party who performed charge conserving operations, and reject it otherwise. (Applies only to two-party protocols.)

Superselection rules in quantum cryptography



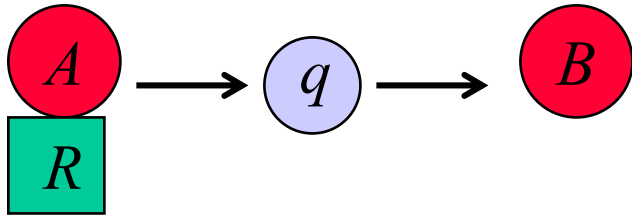
Security: how does Alice's cheating affect Bob's measurement?
 how does Bob's cheating affect Alice's measurement?

<i>I</i> -world	<i>U</i> -world
P	\tilde{P}
A'	\tilde{A}'
B'	\tilde{B}'

Given an *I*-world game P , there is a corresponding *U*-world game \tilde{P} such that the honest games yield the same distribution of outcomes. Furthermore, for any cheating strategy \tilde{A}' by Alice in game \tilde{P} there exists an equivalent strategy A' in the game P . (Equivalent means that Bob's measurement outcome has the same probability distribution in both cases.) Similarly, for any cheating strategy \tilde{B}' by Bob in game \tilde{P} there exists an equivalent strategy B' in the game P .

We then say that \tilde{P} simulates P .

Reference systems



Operations are required to be G -invariant. Cheating Alice can simulate charge nonconserving operations by borrowing from the charge reservoir R .

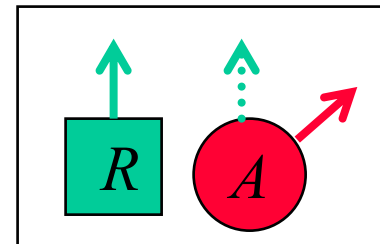
Suppose that the system R transforms as the (left) regular representation of the group G :

$$U(g) |\phi\rangle_R = |g\phi\rangle_R$$

Alice can simulate a (not necessarily G -invariant) linear operator M with the G -invariant operator M^{inv} :

$$M_A \Rightarrow M_{RA}^{inv} = \sum_{\phi \in G} (|\phi\rangle\langle\phi|)_R \otimes (U(\phi) M U(\phi)^{-1})_A$$

M^{inv} rotates the relative orientation of A and G , which has an invariant meaning.



Reference systems

Properties of $M_{RA}^{inv} = \sum_{\phi \in G} (|\phi\rangle\langle\phi|)_R \otimes (U(\phi)M U(\phi)^{-1})_A$

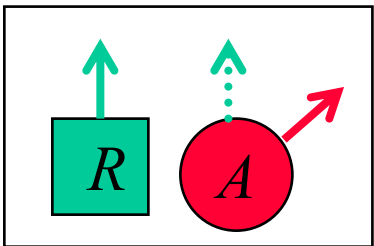
1) G-invariance: $M^{inv} = (U(g) \otimes U(g)) M^{inv} (U(g)^{-1} \otimes U(g)^{-1})$

2) Representation: $M_1^{inv} M_2^{inv} = (M_1 M_2)^{inv}$

3) M G-invariant $\Rightarrow M^{inv} = I_R \otimes M_A$

4) If ρ G-invariant and $\text{tr } \rho_R = 1$, then

$$\text{tr } M^{inv} (\rho_R \otimes \rho) = \text{tr } (M \rho)$$



If the state of A is G-invariant, then measurements in the U -world can be faithfully simulated by measurements in the I -world.

Simulating a cheating strategy

In the *I*-world game, the initial state is a product of invariant states $\rho_A \otimes \rho_B \otimes \rho_M$

In the honest game Bob measures $V^\dagger E_B V$

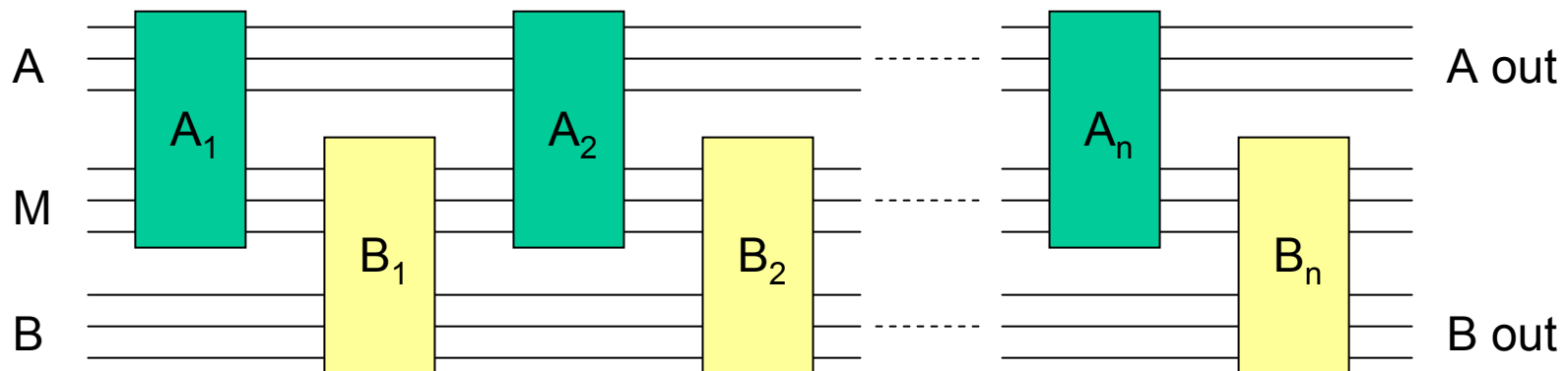
where $V = B_n A_n \cdots B_2 A_2 B_1 A_1$

If Alice cheats (in the *U*-world), Bob measures

$V'^\dagger E_B V'$ instead, where $V' = B_n A'_n \cdots B_2 A'_2 B_1 A'_1$

and A'_j need not be *G*-invariant.

<i>I</i> -world	<i>U</i> -world
P	\tilde{P}
A'	\tilde{A}'
B'	\tilde{B}'



Simulating a cheating strategy

If Alice cheats (in the U -world), Bob measures

$$V'^{\dagger} E_B V' \quad \text{where} \quad V' = B_n A'_n \cdots B_2 A'_2 B_1 A'_1$$

and A'_j need not be G -invariant.

In the I -world, Alice can achieve an equivalent result by using a reference system and applying A_j^{inv}

I -world	U -world
P	\tilde{P}
A'	\tilde{A}'
B'	\tilde{B}'

This works because $B_j = B_j^{inv}$ and $E_B = E_B^{inv}$; therefore, the effect of replacing A'_j by A_j^{inv} is that Bob measures $(V'^{\dagger} E_B V')^{inv}$.

Since the initial state is invariant, $V'^{\dagger} E_B V'$ and $(V'^{\dagger} E_B V')^{inv}$ have the same expectation value --- therefore Alice's cheating strategy in the I -world game is equivalent to her strategy in the U -world game.

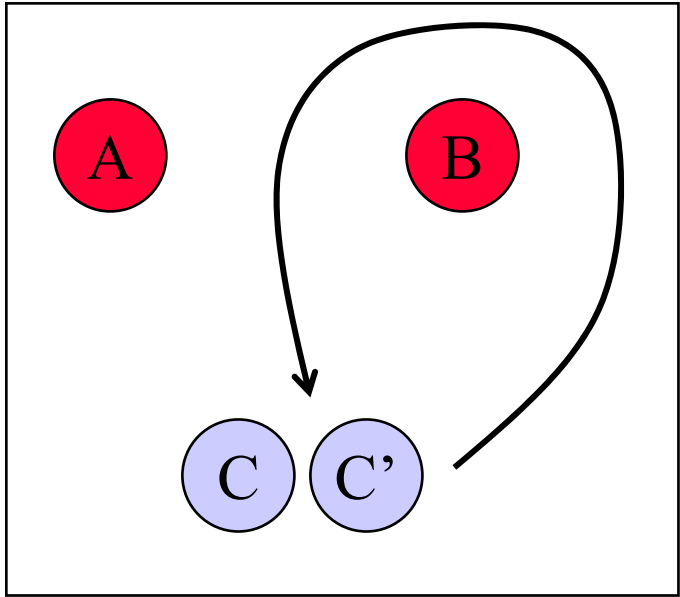
Superselection rules in quantum cryptography

A similar argument applies to n -party protocols: the k cheating parties share access to a reference system.

Theorem: Suppose that in the I -world all quantum operations are required to be G -invariant, where G is a compact Lie group, and in the U -world quantum operations are unrestricted. For any n -party I -world game P , there is a U -world game \tilde{P} that simulates P .

In particular, Kitaev's lower bound on the bias in strong quantum coin tossing, and Ambainis's lower bound on the number of rounds in weak coin tossing, which apply in the U -world, also apply to the I -world.

Cryptography with anyons?



In a three-party setting, suppose that Charlie splits his charge into two parts, and sends one part on a voyage around Bob's lab. This operation can induce a change in Charlie's charge, accompanied by a compensating change in the total charge held jointly by Alice and Bob.

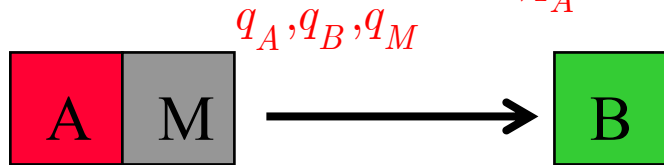
Thus Charlie can alter the state shared by Alice and Bob without interacting directly with either Alice or Bob.

We will stick with the two-party case...

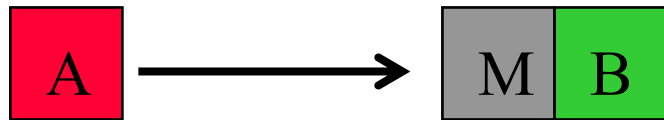
Simulating an I -world game

We may assume that the total charge is trivial:

$$\mathcal{H}_1 = \bigoplus_{q_A, q_B, q_M} \mathcal{H}_{A, q_A} \otimes \mathcal{H}_{B, q_B} \otimes \mathcal{H}_{M, q_M} \otimes V_1^{q_A, q_B, q_M}$$



Charges split: $\bar{q}_B \rightarrow q_A \otimes q_M$



Charges fuse: $q_M \otimes q_B \rightarrow \bar{q}_A$

In the I -world protocol, when Bob receives a message, he “knows” both the charge that Alice held before sending the message (\bar{q}_B), and the charge Alice retained after sending the message (q_A).

In the honest U -world protocol, Alice and Bob respect local conservation of a fictitious “charge.” Each party needs to be able to check whether the other party obeyed charge conservation, and abort the game when nonconservation is detected.

I -world	U -world
P	\tilde{P}
A'	\tilde{A}'
B'	\tilde{B}'

Simulating an I -world game

In the I -world: $\mathcal{H}_1 = \bigoplus_{q_A, q_B, q_M} \mathcal{H}_{A, q_A} \otimes \mathcal{H}_{B, q_B} \otimes \mathcal{H}_{M, q_M} \otimes V_1^{q_A, q_B, q_M}$

In the U -world:

$$\tilde{\mathcal{H}} = \bigoplus_{q_1, q_2, q_A, q_B, q_M} \mathcal{H}_{A, q_1} \otimes \mathcal{H}_{B, q_2} \otimes \underbrace{\mathcal{H}_{M, q_M} \otimes V_1^{q_A, q_B, q_M}}_{\text{message}}$$

While the vector space $V_1^{q_A, q_B, q_M}$ is an intrinsic property in the I -world, in the U -world protocol \tilde{P} it must be regarded as an explicit part of the message, encoded in qubits. A message sent in \tilde{P} and a message sent in P have the same “format” if the conditions $q_1 = q_A$ and $q_2 = q_B$ are imposed.

Therefore, in \tilde{P} Alice checks (coherently) that $q_1 = q_A$ when she receives a message, and Bob checks that $q_2 = q_B$ when he receives a message. If the check fails, the game aborts.

I -world	U -world
P	\tilde{P}
A'	\tilde{A}'
B'	\tilde{B}'

Simulating an I -world game

In \tilde{P} Alice checks (coherently) that $q_1 = q_A$ when she receives a message, and Bob checks that $q_2 = q_B$ when he receives a message. If the check fails, the game aborts.

In the honest game, the checks always succeed, and \tilde{P} is equivalent to P .

Suppose Alice cheats. Then if Bob's check succeeds, the message he receives could have been sent if Alice respected charge conservation.

But Bob's check might fail; we must show that there is an equivalent I -world cheating strategy in which Alice stops the game herself with the same probability:

$$A_k = \sum_{q_B} \Pi_{q_B} \tilde{A}_k \Pi_{q_B}$$

charge
projector

A_k conserves charge, and agrees with \tilde{A}_k in each charge block.

I -world	U -world
P	\tilde{P}
A'	\tilde{A}'
B'	\tilde{B}'

Superselection rules in quantum cryptography

Theorem: For any two-party game P in the I -world, there is a U -world game \tilde{P} that simulates P .

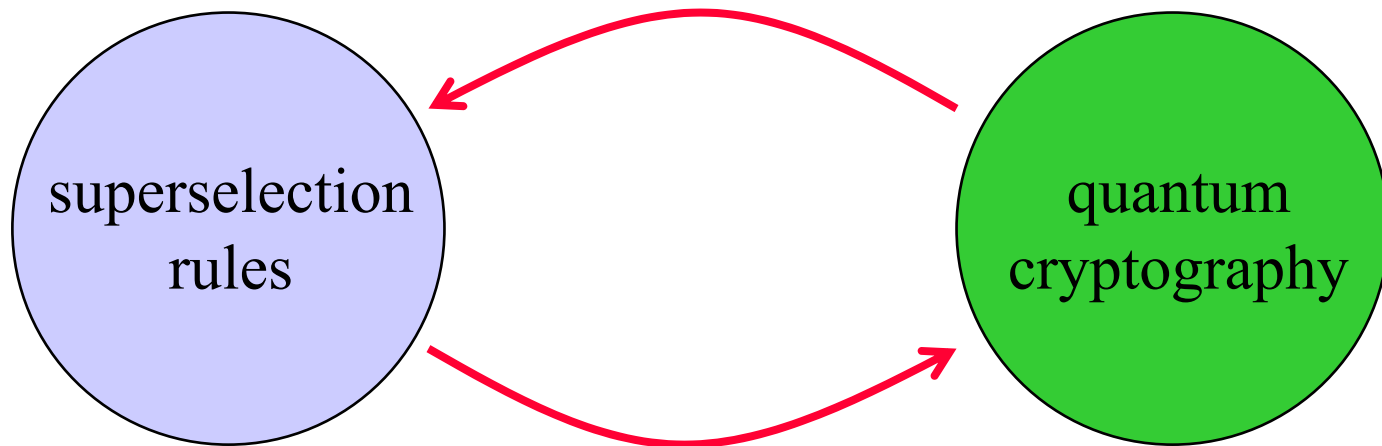
In particular, Kitaev's lower bound on the bias in strong quantum coin tossing, and Ambainis's lower bound on the number of rounds in weak coin tossing, which apply in the U -world, also apply to the I -world.

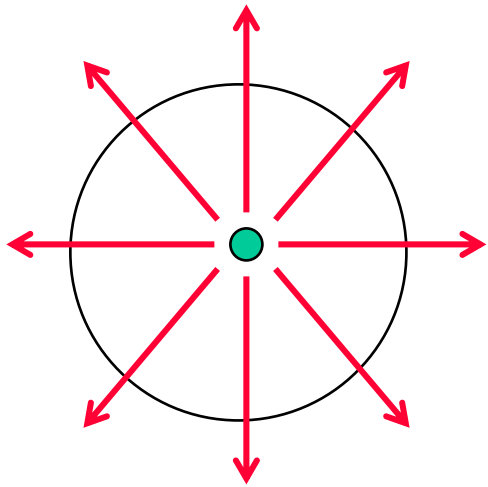
In contrast to our previous result, this theorem applies to arbitrary superselection rules, but only to two party protocols.

Superselection rules in quantum cryptography

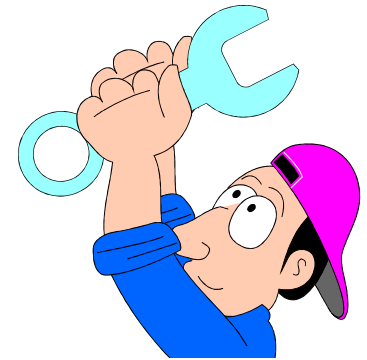
Superselection rules do not enhance the (information theoretic) security of quantum cryptographic protocols:

- Unconditionally secure quantum bit commitment is impossible.
- Security in the G -invariant world implies security in the U -world (n parties).
- Security in the I -world implies security in the U -world (two parties, but general locally conserved charge).





Superselection rules vs. engineering



With finite resources we cannot create a condensate that fills an infinite universe.

But for a fixed protocol, we can nullify the impact of local charge conservation through suitable feats of engineering...