Mistrustful Quantum Cryptography

Adrian Kent

Centre for Quantum Computation
DAMTP, University of Cambridge

Two lectures for MIT Independent Activities Period.
2pm on 28.01.03 and 29.01.0; Sponsored by the CMI

Beyond key distribution: mistrustful cryptography

- Life requires controlled information exchange between not necessarily trusting parties. (Some cynics might say life **is** controlled information exchange between not necessarily trusting parties.)
- For example: trustable electoral systems that allow secret ballot, secure auctions, tax collection that preserves privacy, remote authentication to a computer, decisions on joint corporate (or other) ventures, job interviews, "helping the police with their enquiries", …
- Cryptography can help, at least with some of these, by regulating the information flow – instead of trusting the other party, you need only trust the cryptosystem, which if well designed is provably secure modulo reasonable assumptions.

Mistrustful cryptography: often referred to as “Post Cold War” cryptography

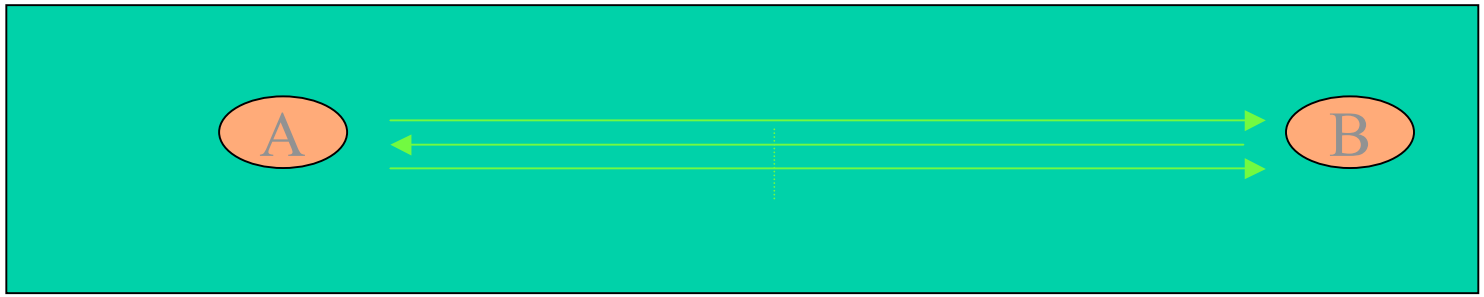
- Cold War cryptography: your aim is to communicate with your agents behind enemy lines.
- You (let’s hope) trust your agents, or at any rate trust them enough to want the message to get to them: the worry is about enemy eavesdroppers.
- Whereas in the post Cold War world…

Mistrustful cryptography and physics

- Classical cryptographers have identified key "primitives" – elementary tasks that can be used as building blocks for many mistrustful cryptographic purposes (and are often very useful in their own right). .
- Given the example of key distribution, where quantum information allows classically unattainable security, we naturally want to understand which mistrustful tasks quantum information can be useful for. We don't! (Mostly. Yet.)
- More generally, we want to know what physics can do for cryptography. We're not just interested in protocols guaranteed secure by quantum theory – any well established physics would do.
- The impossibility of signalling faster than light, guaranteed by (the standard understanding of) special relativity, is a natural candidate. And it turns out to be cryptographically important…

Standard assumptions for mistrustful cryptography

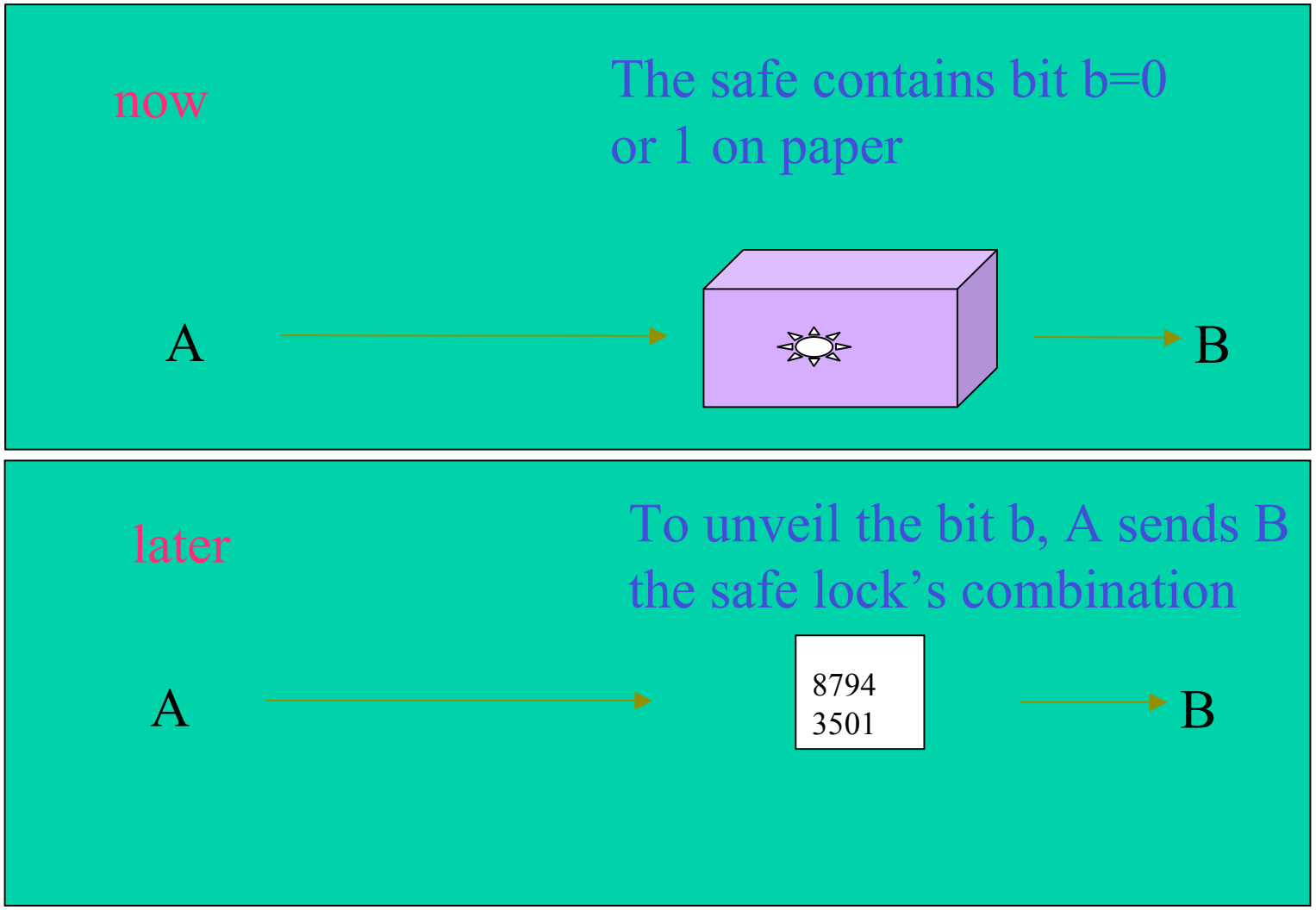
- A and B each control disjoint labs.
- They trust nothing outside their labs. Zero, zip, nada. No trusted machines, no channels with trusted properties, no trusted third parties,…
- One consequence: unless they make use of relativity and constrain their lab locations, protocols can only involve sequential exchanges of signals – there's no way of guaranteeing timings that would ensure two independent signals, from A to B and vice versa.



Some mistrustful tasks: bit commitment

- Alice and Bob mistrust each other (as always in these lectures).
- A must give B an encrypted bit (O or 1) and later reveal it
- B must be unable to decrypt the bit for himself
- A must be unable to cheat by revealing the wrong bit: she must be genuinely committed

Pictorially...



Mistrustful tasks: remote coin tossing

- A and B exchange information and generate either a bit b, or the outcome "fail" which tells one the other cheated.
- Each is guaranteed that if they are honest, then whatever the other does:

$$\Pr(b=0) < 1/2 + \varepsilon$$
$$\Pr(b=1) < 1/2 + \varepsilon$$

ε can be made as small as desired by adjusting the parameters of the protocol

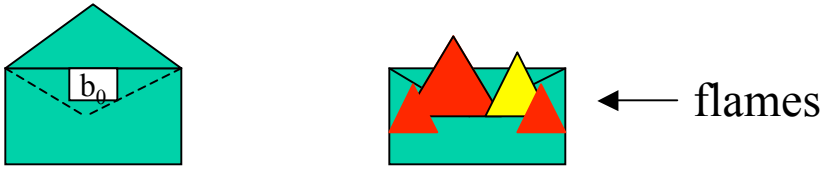
Mistrustful tasks: weak coin tossing

- A and B exchange information and generate either a bit b, or the outcome "fail" which tells one the other cheated.
- A is guaranteed that if she is honest, then whatever B does: $\Pr(b=0)<1/2+\varepsilon$
- B is guaranteed that if he is honest, then whatever A does: $\Pr(b=1)<1/2+\varepsilon$
- These guarantees are adequate if, for instance, A and B are playing a gambling game in which A wins if b=0 and B wins if b=1.

Mistrustful tasks: oblivious transfer

- Pictorially: A puts bits b_0, b_1 in 2 envelopes

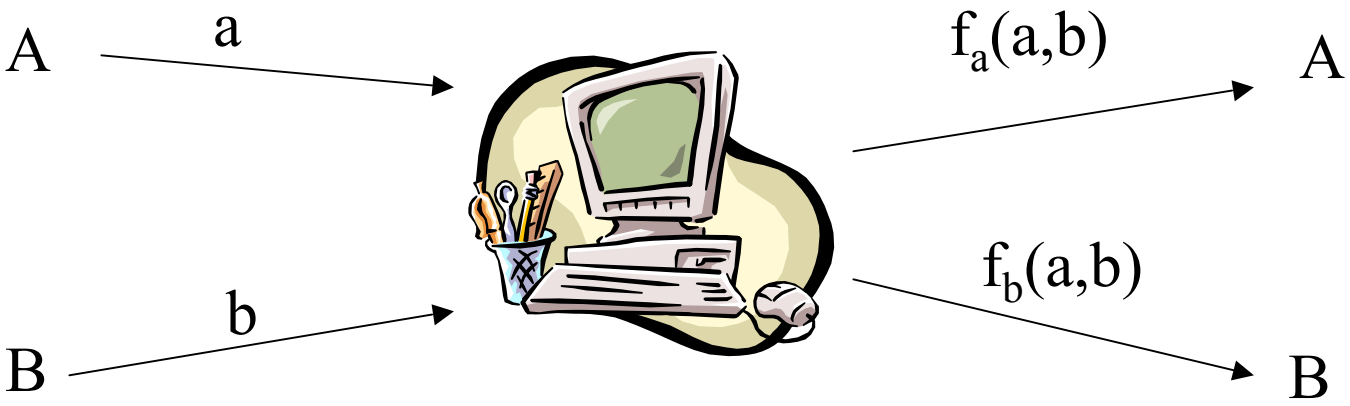
- A is (somehow) guaranteed that on receipt B will open one and burn the other unopened



- B is guaranteed that A won't find out which was opened.
- (There are several variants of OT, all equivalent.)

Mistrustful tasks: secure two-party computation

- A and B input private data as if to a trusted secure computer, which returns only specified joint functions:



- **But** of course there are no trusted devices: a cryptographic protocol has to fill the role of the computer.
- A and B need to be guaranteed that no information about their data leaks to the other party, except for that implied by the prescribed joint function.

Oblivious transfer implies bit commitment

- Suppose A and B have a secure oblivious transfer protocol. A can commit a bit b to B securely by:
- 1. A chooses N random bits c_{io} and N bits c_{i1} such that $c_{io} \oplus c_{i1} = b$ for each i.

  2. A carries out oblivious transfers of the pairs (c_{io} , c_{i1}). B opens one of each pair.

  3. A is now committed to b; to unveil it she reveals the values of all the c_{ik}.

  A can't cheat (with non-negligible chance of success), since she doesn't know which bits B opened. B can't cheat, since he gets no information about the committed bit b.

Bit Commitment Implies Coin Tossing

- Suppose A and B have a secure bit commitment protocol. They can implement coin tossing by:
- 1. A commits a random bit a to B.

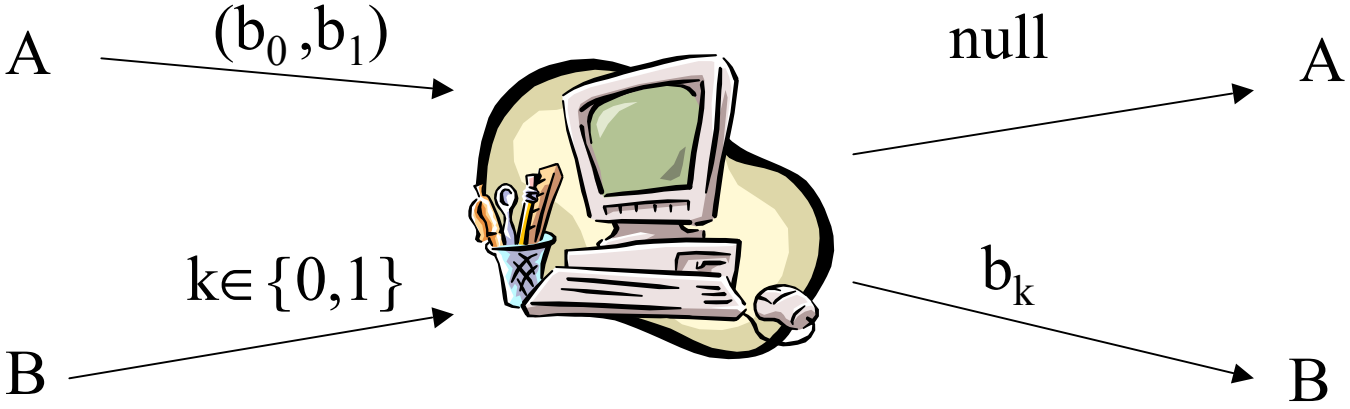
  2. B chooses a random bit b & sends it en clair to A

  3. A unveils a to B.

  4.They take a⊕b (addition mod 2) as the randomly generated bit defined by the coin tossing.
- If either A or B is honest (and the bit commitment really is secure), the other – whether they follow the protocol honestly or not – can't influence the probabilities of the coin tossing outcome.

Secure two-party computation implies oblivious transfer

In fact, oblivious transfer is just a special case of secure 2-party computation:



Kilian (1988) showed the converse (which is not at all obvious): oblivious transfer implies general secure multi-party computations.

Nonrelativistic classical crypto: a hierarchy of primitives

A & B generate a random bit;
A wants 0;
B wants 1.
Both know this.

Weak coin tossing

A & B generate a random bit by exchanging data

Coin tossing

A encrypts a bit for B and later unveils it

Bit commitment

A sends 2 bits; B gets the one of his choice; A can't tell which.

Oblivious transfer

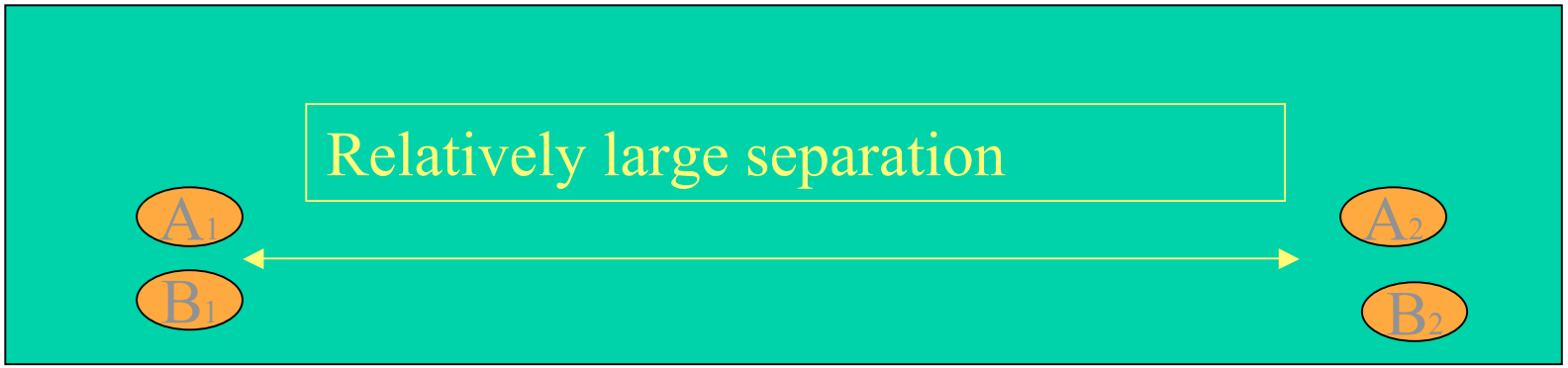
A & B input private data a & b and receive joint functions $f_A(a,b)$ & $f_B(a,b)$

Secure 2-party computation

X → Y Y can be securely implemented by a secure black box implementing X, and classical information exchanges

How relativity could help

Let A and B each control two separate sites, arranged so:



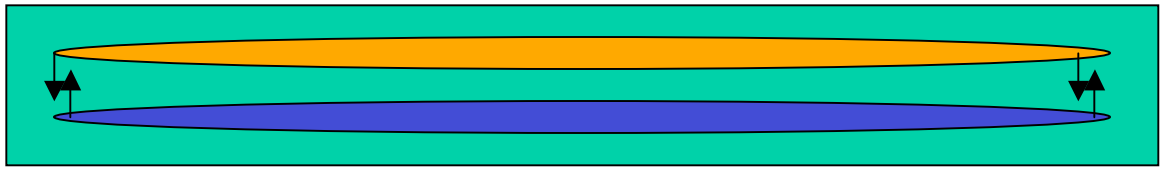
NB This configuration requires no trust: each party can ensure security by checking the times at which they sent and received messages.

A and B can thus send messages A_1 _ B_1 and B_2 _ A_2 which are guaranteed to be independent.

Relativity and trust

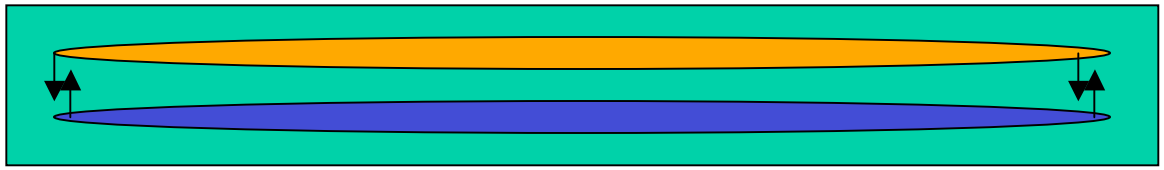
- It's interesting to consider exactly what A and B need to take on trust

- A needs to know the separation between her sites; similarly B. Even this requires trust in something (if only the locations of distant stars) outside the laboratories. True cryptographic paranoiacs would thus prefer an arrangement in which A and B can verify the separations from within the labs:



More on relativity and trust

- A and B still need, of course, to have faith in physics.
- In particular, they need to believe that spacetime is (at least approximately – and approximately is good enough) Minkowski in the region to which the parties have access.
- So: no wormholes, no surreptitious introduction of very very dense massive objects by one party, …
- Practically speaking, for crypto in the Solar System in the foreseeable future, these aren't (I would suggest) serious concerns.



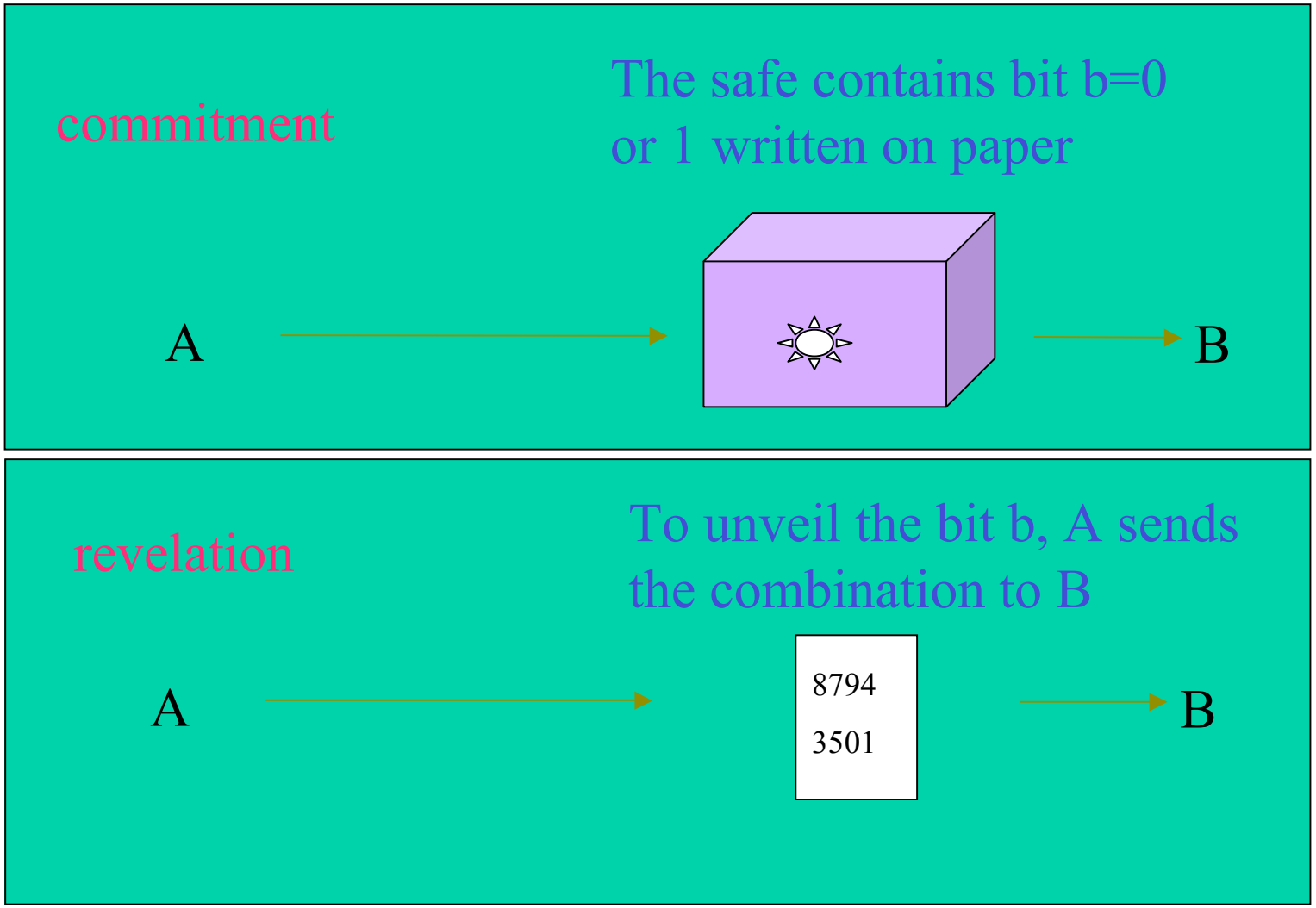
Terminology

- We say a protocol is **unconditionally secure** (with respect to some underlying physical theory – usually quantum theory or special relativity or both) if we can prove it is secure without assuming any restriction on the parties' technological capabilities.
- So, in analysing such protocols we assume no limits on the parties' computational capacity or speed, their memory storage, …

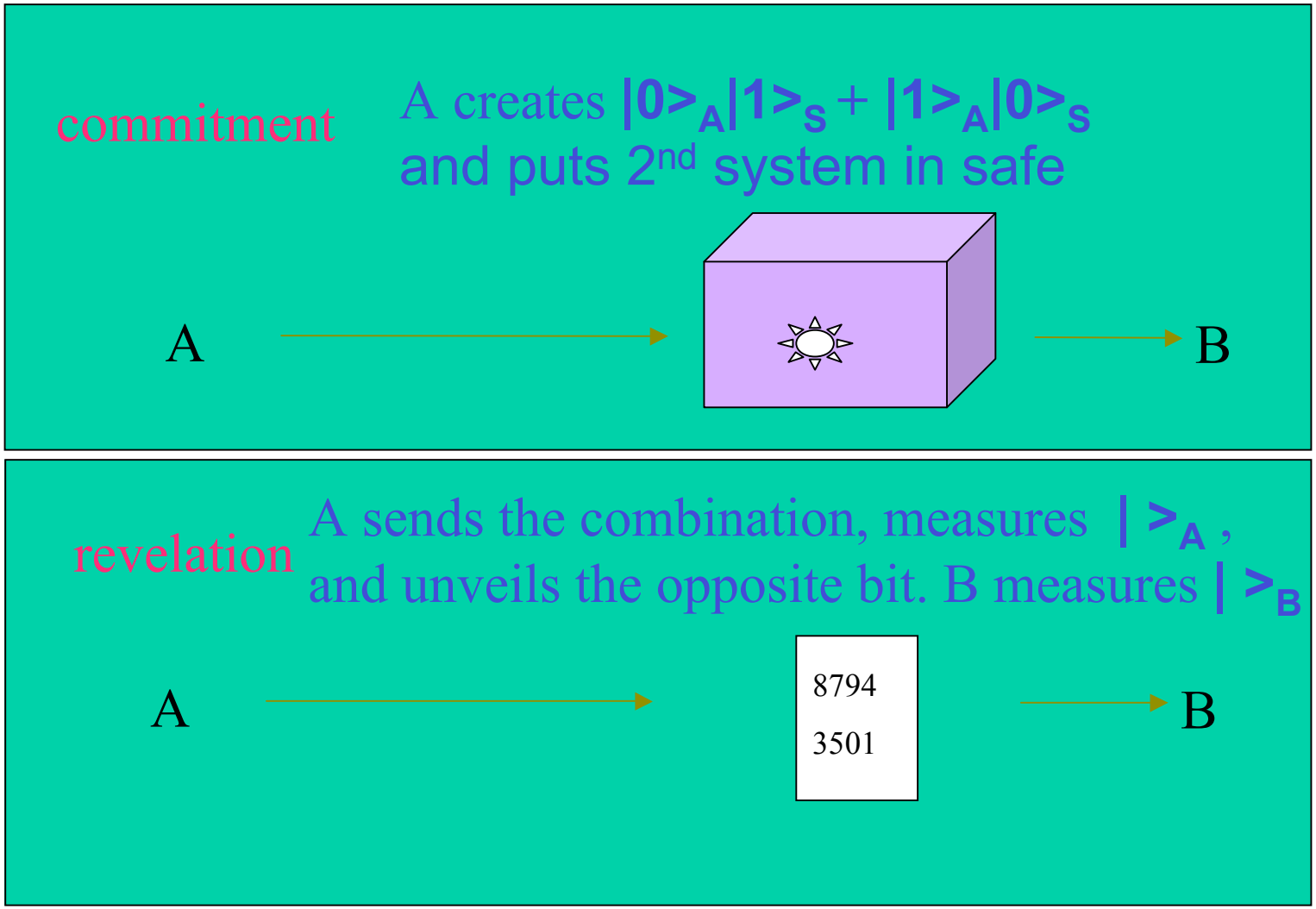
Quantum information and cryptography

- We can try to use quantum information to devise unconditionally secure implementations of tasks that can't be implemented with unconditional security using classical information – cf. quantum key distribution.
- Here the task – in this case the distribution of a shared secret classical random key – is unaltered; quantum information just gives a new (and better) way of implementing.
- But we also need to consider the possibility that the very definition of a task needs to be extended when we take quantum information into account: cf the example of bit commitment, to be considered in the next slides.
- As we're also beginning to learn, using quantum information also motivates the definition of completely new cryptographically useful tasks.

What is bit commitment? Here's a standard (but quantumly ambiguous) metaphor



So if A puts a qubit in a secure safe: is <u>that</u> a quantum bit commitment? [I'll argue yes.]



Three things that could be required of a quantum bit commitment

(1) Must have a certificate of classicality – a guarantee that Alice committed a definite classical bit.

[Too strong – requires something that isn't needed for many applications of BC. It's also easy to show this is impossible – see later.]

(2) Must guarantee security where a classical BC would: The security of (some, all, your favourite) tasks that use the bit commitment as a subprotocol should be guaranteed if it would be for a secure classical bit commitment. [If we ask for all tasks, we're back to (1). If not: which tasks? Why those?]

(3) Must guarantee unalterability. A may commit quantum superpositions – so long as she can't influence the probabilities of 0 and 1 being unveiled. [Seems right to me: consistent with Mayers & Lo-Chau; natural e.g. if the commitment is used for a later-to-be-revealed prediction. **But NB** it means that quantum BC doesn't guarantee security for everything that classical BC would. We need to consider the composability of quantum crypto protocols separately.]

More precisely…

- **Let p_0 be A's probability of successfully unveiling a 0 if she chooses the optimum strategy for this after the initial commitment; similarly p_1.**
- **_ is a security parameter which can be made as small as required.**
- **A classical bit commitment protocol should guarantee that for any commitment either $p_0 <$ _ or $p_1 <$ _**
- **The "qubit in a safe" doesn't ensure this.**
- **The natural definition for quantum protocols is that for any commitment the protocol guarantees $p_0 + p_1 < 1 +$ _**
- **That is, whatever A does after commitment, she has no more "wiggle room" than she would have had she classically committed a randomly chosen bit.**

Classically Certified Bit Commitment is Impossible

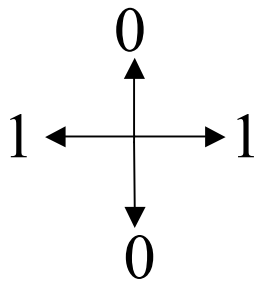
- We can think of Alice as running her side of the protocol with a quantum computer, and inputting $|0\rangle$ or $|1\rangle$ to commit the classical bits 0 or 1.
- Moreover, the Church of the Larger Hilbert Space tells us we can treat everything in the protocol – all random choices, all measurements, … – as if kept at the quantum level. (In fact, the basic proof works even if we treat classical info as qualitatively distinct from quantum.)
- The end result of a $|0\rangle$ or $|1\rangle$ commitment is thus a shared state $\_0$ or $\_1$. Security against Bob implies $Tr_A(\_0) \approx Tr_A(\_1) = \rho_B$.
- So if Alice inputs $\alpha |0\rangle + \beta |1\rangle$, the shared state is $\_ = \alpha \_0 + \beta \_1$, and $Tr_A(\_) \approx \rho_B$.
- Hence Bob can't tell if a superposed state is committed. QED.
- [cf the Wootters-Zurek proof of no-cloning]

Comments on the impossibility of classically certified bit commitment

- NB: this is not the Mayers-Lo-Chau no-go theorem, which – as we'll see later – says that unconditionally secure non-relativistic quantum bit commitment is impossible, even if no classical certification is required.
- The same argument shows that unconditionally secure classically certified oblivious transfer is impossible – Bob can input $\alpha |0\rangle + \beta |1\rangle$ and obtain $\alpha |0\rangle|b_0\rangle + \beta |1\rangle|b_1\rangle$.
- It also shows that unconditionally secure classically certified multi-party computation is impossible – there is no way to guarantee that the parties don't input superpositions of data.

The BB84 bit commitment protocol

- To understand Mayers and Lo-Chau's essential insight, it's useful first to consider the Bennett-Brassard (BB84) quantum bit commitment protocol:
- BB84: to commit to 0, A sends B a string of N states independently randomly chosen from the orthogonal basis |0>,|1>.



- To commit to 1, she sends a string randomly chosen from the basis |+>,|->.
- To unveil, she reveals the N states; hence the basis choice and the committed bit.

Security of BB84 bit commitment

- If A honestly follows the commitment protocol and commits a string of form $|0\rangle|0\rangle|1\rangle|0\rangle\ldots$ or $|+\rangle|+\rangle|-\rangle|-\rangle\ldots$, she has essentially no chance of successfully cheating at the unveiling stage.
- In any case, B cannot distinguish a 0 and 1 commitment; in both cases the density matrix for each state in the string is _ I .
- But (as BB pointed out), A can cheat by making N singlets $|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B = |+\rangle_A|-\rangle_B - |-\rangle_A|+\rangle_B$, sending the second state from each to B – so the ostensible commitment states are actually entangled with states still under A's control – and then measuring the A states in the basis $|0\rangle,|1\rangle$ or $|+\rangle|-\rangle$ depending whether she wants to unveil a 0 or 1.
- In other words, the protocol is secure against B, but completely insecure against A, who can unveil whatever she pleases.

Mayers-Lo-Chau argument

- First key point: a would-be cheater can keep everything on their side of a BC protocol at the quantum level. Any random choice of a quantum state can be replaced by a "quantum dice" $\sum_i (p_i)^{1/2} |i\rangle|\Psi_i\rangle$ – just as in the EPR attack on BB84; any measurement by an interaction with an ancilla; etc. So we can take the end result of a 0 or 1 commitment to be a shared pure state $|\Psi_0\rangle$ or $|\Psi_1\rangle$.
- Second key point: security against Bob implies $Tr_A(\rho_0) \approx Tr_A(\rho_1) = \rho_B$. But a result of Hughston-Jozsa-Wootters implies that in this case there exists a local unitary operation U_A which Alice can apply, such that $U_A \rho_0 \approx \rho_1$. Moreover, Alice can derive U_A from the definition of the protocol. So Alice can cheat by following the commitment protocol for a 0, and then applying U_A and revealing 1 if she wants to change her mind, and the probability of her being detected in this cheating is small.
- Mayers (alone) showed how to handle the case when $Tr_A(\rho_0) \approx Tr_A(\rho_1)$ rather than $Tr_A(\rho_0) = Tr_A(\rho_1)$. Mayers also pointed out that the argument holds even if the protocol includes some communications (publication in the New York Times, say) that are taken to be indubitably classical rather than quantum.

Isn't the Mayers-Lo-Chau theorem the end of the quantum bit commitment story?

- Short answer: No!
- Longer answer: Not when relativistic protocols are taken into account.
- Mayers & Lo-Chau show that a wide class of quantum BC protocols based on sequential q info exchanges are insecure by every reasonable definition of security.
- But the MLC proofs don't apply (and MLC don't claim they apply) to relativistic schemes where indefinitely continuing communications sustain the commitment. (AK, 1999)
- Which is one reason why we need to decide the definition of quantum BC – I'll use the $\mathbf{p_0 + p_1 < 1 + \_}$ condition.
- [There is also some discussion about whether the MLC proofs apply to non-relativistic schemes that use fermions: see Mayers, quant-ph/0212159, responding to a point raised by Popescu. Some attempts to find other loopholes in MLC have been circulated; I'm not aware of any convincing ones.]

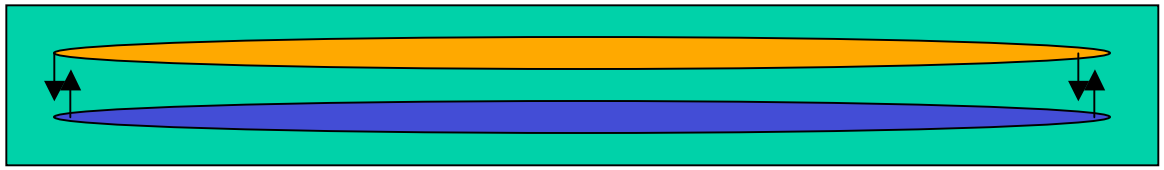
A warm-up exercise in relativistic cryptography: coin tossing

- A chooses a random bit a and sends it to B from the left site.

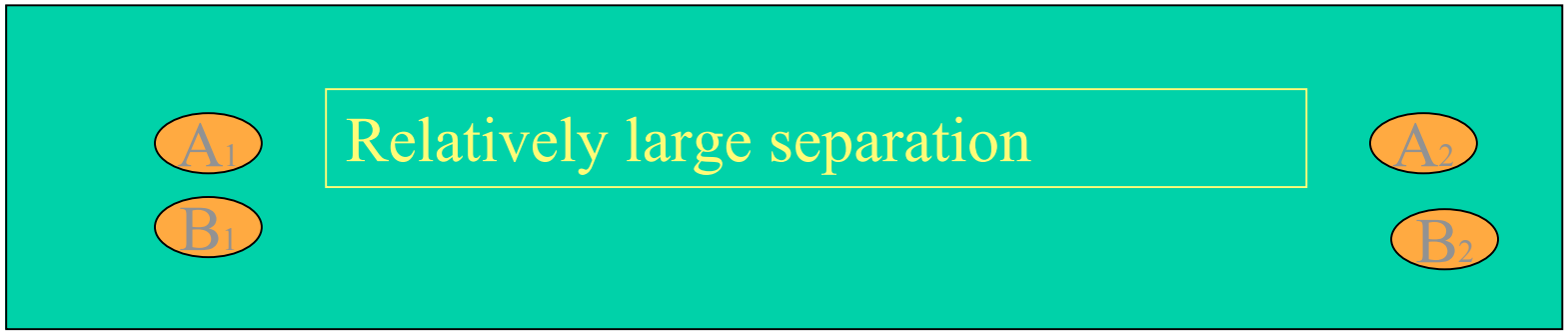
  B chooses a random bit b and sends it to A from the right site.

  The timings and separations are chosen so that both are guaranteed that the bits were generated independently of one another.

- They take a⊕b (addition mod 2) as the randomly generated bit defined by the coin tossing.



Temporarily secure relativistic bit commitment (Ben-Or et al 1988; relativistic version due to Brassard et al 1998)



- A and B agree a large number N: all calculations done modulo N.
- A_1 and A_2 fix a random number m prior to the protocol
- A_1 and A_2 occupy separate locations as above
- B_1 sends A_1 two distinct random numbers n_0 and n_1
- A_1 returns $(m + n_b)$ to commit bit b
- A_2 is committed until the signal containing the n_i could have reached her. During this interval she can send m to B_2 to unveil.

Quantum strategies for Alice in a temporary relativistic bit commitment (cf Brassard et al 1998)

- A_1 and A_2 can share a bit state $a|0\rangle_1|0\rangle_2 + b|1\rangle_1|1\rangle_2$ and a random number state $\_{}_i |i\rangle_1|i\rangle_2$ prior to the protocol.
- B_1 sends A_1 two distinct random numbers n_0 and n_1
- Equipped with a quantum computer, A_1 runs the protocol using her parts of the bit and random number states, and measures an output k which is returned to B_1 . The joint state is now

$a|0\rangle_1 \,|\, n_0 - k \rangle_1 |0\rangle_2 \,|\, n_0 - k\rangle_2 + b|1\rangle_1 \,|\, n_1 - k \rangle_1 |1\rangle_2 \,|\, n_1 - k\rangle_2$

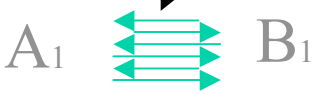
- A_2 can measure her random number state and send the result to B_2 to reveal the bit, which until this point is indeterminate: classicality of the committed bit is not guaranteed.
- But there is temporary security: we can prove that no quantum strategy allows the A_i to make $\mathbf{p_0 + p_1 > 1 + \_}$

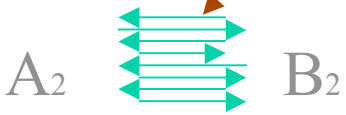
Secure bit commitment using relativity (AK, Phys Rev Lett **83** (1999) 1447)

Alice maintains the bit commitment indefinitely by sequentially committing the random "keys" used in each commitment subprotocol:

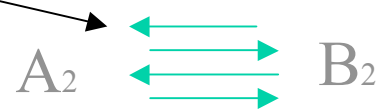
But note the exponentially growing communication cost

A_1 commits key string m_2 to B_1 using key string m_3

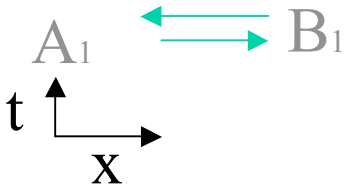


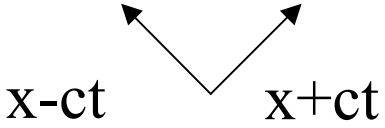


A_2 commits the key m_1 to B_2 using key string m_2



A_1 commits the bit b to B_1 using the key m_1

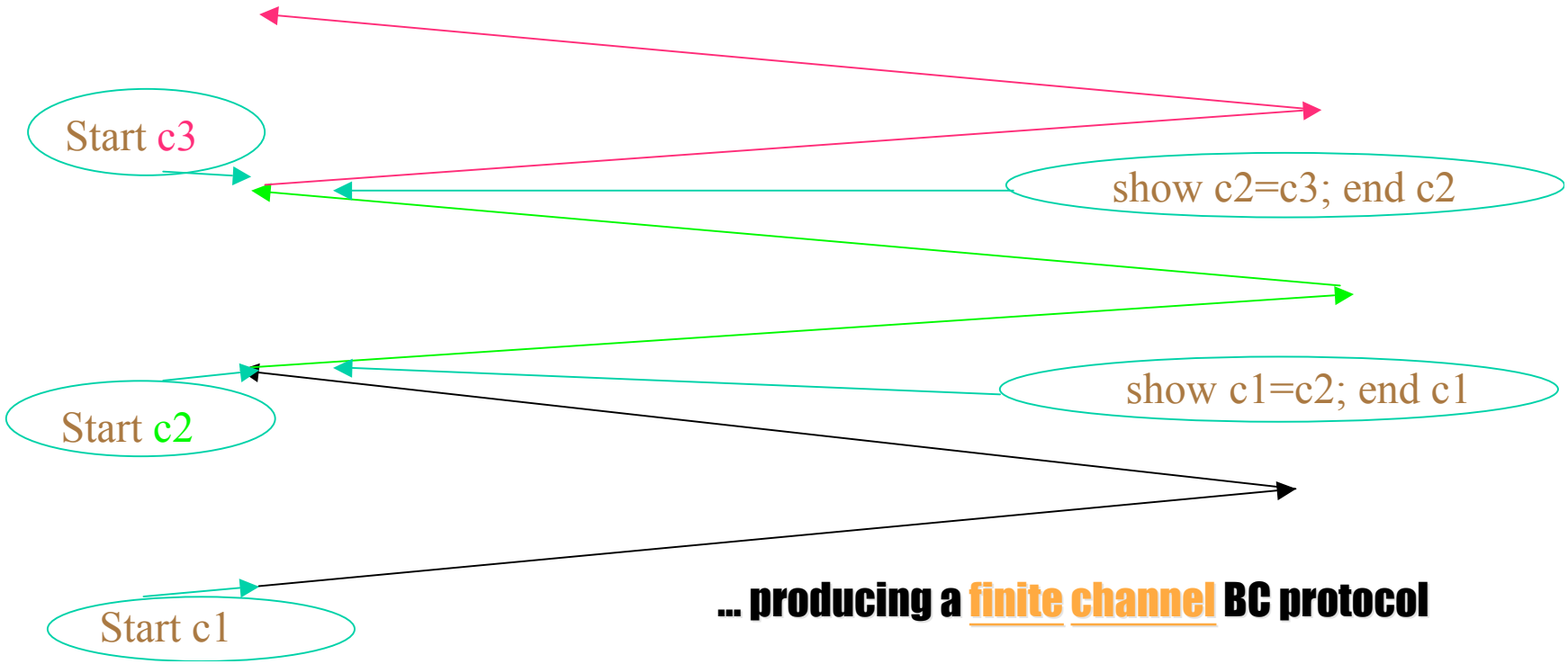




The use of linking bit commitments

(cf. AK quant-ph/9906103 latest version (Dec 2002))

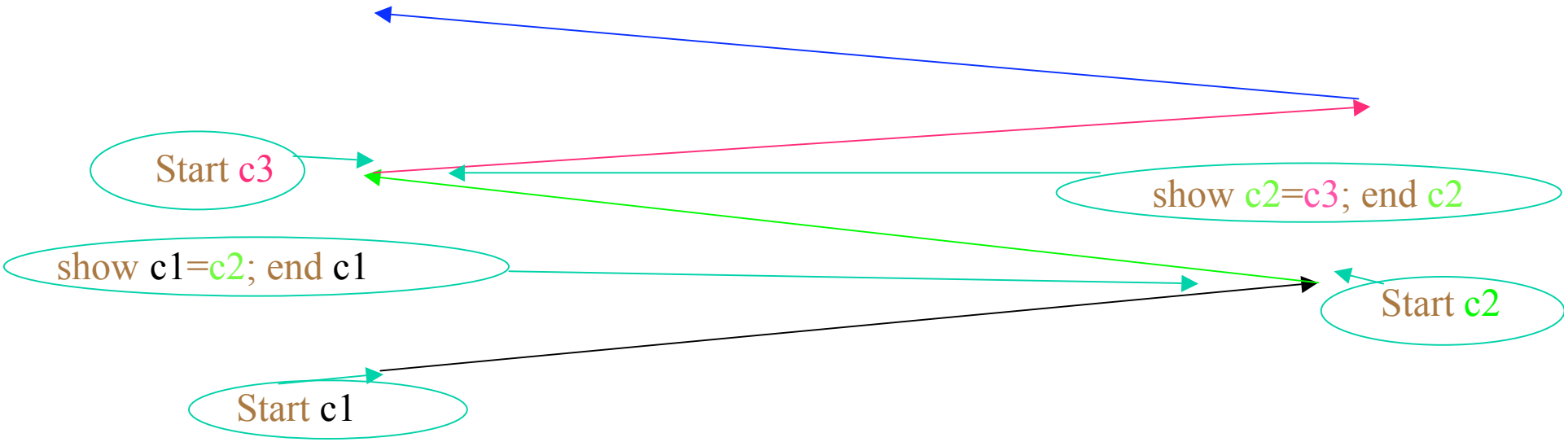
There is a trick (original AK method inefficient; thanks to Claude Crepeau for suggesting a better method due to Rudich) which allows A to persuade B that two relativistic commitments are of the same bit, without revealing the bit. She can then proceed as follows…



… producing a finite channel BC protocol

Cheat sensitive relativistic bit commitment: lower security, less communication

If A and B are willing to settle for a protocol secure against A and perfectly cheat-sensitive against B – he can read the bit but he will surely be caught – they can save a round of communication.
[A might be happy enough with this, if the cost to B of being caught is high compared to the value of reading the bit.]

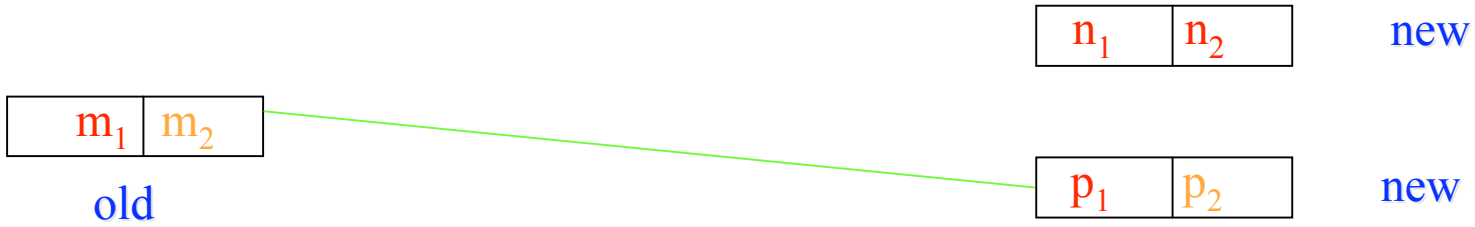


Rudich's scheme (slightly adapted for relativistic BC)

1. A commits b redundantly by giving B N pairs of committed bits, the first chosen randomly and the second so each pair XORs to b.

A later gives B 2N more pairs with the same property. Want that:
(I) A persuades B that the two redundant commitments are to the same bit.
(II) B gets no information about the bit b
(III) N of the new pairs survive unrevealed, to be reused as a commitment of b.

2. B chooses random groups of 3 pairs (1 old, 2 new). From each group he chooses one of the new pairs to compare with the old.



3. A says if the pairs are identical ($(m_1,p_1)=(m_2,p_2)$) or opposite ($m_1 \neq p_1$ and $m_2 \neq p_2$).

4. B then chooses entry 1 or entry 2; A reveals the chosen entry from each pair – i.e. m_1 and p_1 or (here) m_2 and p_2. B checks A's claims were consistent.

5. The other new pair (here n_1 & n_2) survives as part of a reusable commitment of b.

Comments

- Proof of security against all classical attacks given in latest version of q-ph/9906103.
- It is easy to see that the protocol is immune to a Mayers-Lo-Chau cheating attack.
- Security against all quantum attacks is conjectured; proof remains to be completed.
- Using conservative guesstimates of parameter values which should offer pretty good security, require ~8000 bits exchanged per round for BC or ~800 for CSBC.
- At 10 GHz, allowing a small factor for A's processing time and requiring a separation 10 times the round length, this requires separations of ~30 or 3 km between the sites.
- We could maybe do better: the schemes described may not be optimally efficient, or even close to optimal.

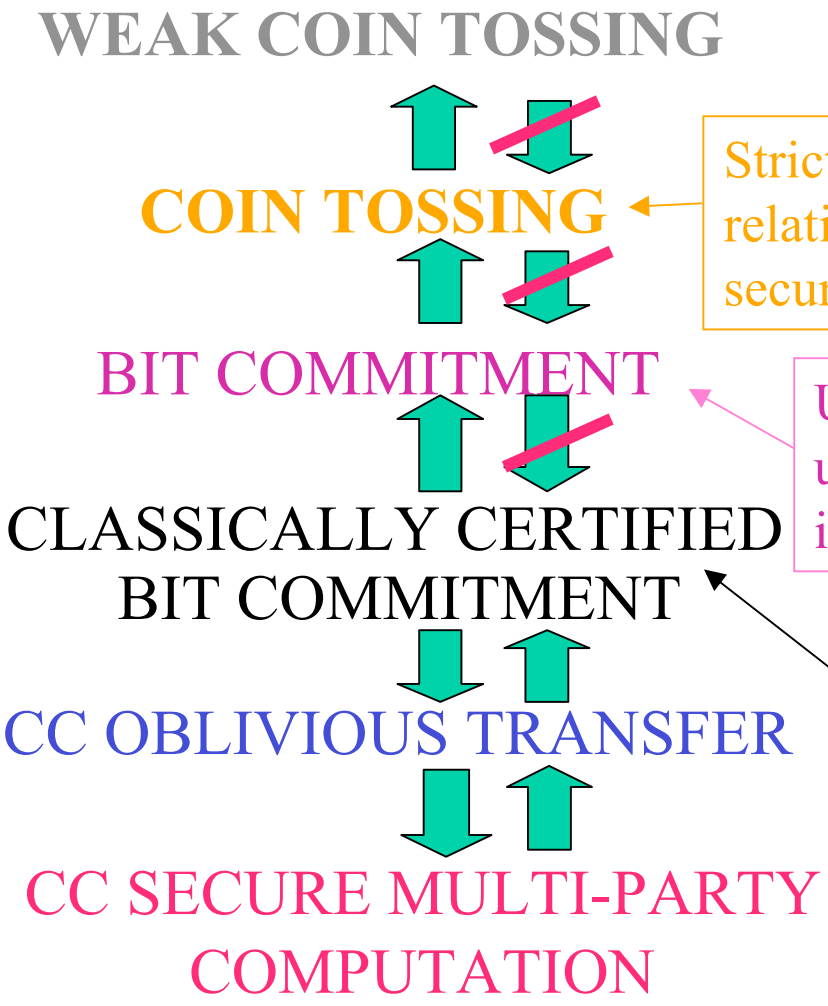
Some remarks on deniability

- Deniability is an intriguing and surprisingly subtle issue in cryptography. For instance, as Beaver recently pointed out, the BB84 protocol for QKD, when it uses standard privacy amplification, decouples the notions of secrecy and deniability for a one-time pad. The pad generated is (effectively) secret, but isn't deniable – if A and B are forced to take the police step by step through their protocol, they can't produce a credible fake transcript.
- The relativistic protocols considered here achieve what initially seems self-contradictory: deniable bit commitment. Alice can walk away and extract herself from the commitment at any time. Even if later she's forced to produce an unveiling, she can produce an unfalsifiable lie. This isn't true of any standard (i.e. computationally secure, classical, non-relativistic) bit commitment protocol.
- Note: there is a short "window of undeniability": if A_1 and A_2 are forced to unveil before they have a chance to communicate, they can't concoct a credible lie.
- Deniability may not be so important for bit commitment *per se*. It clearly is for some tasks – for instance voting schemes – in which bit commitment is a subprotocol.

Morals to be drawn from considering bit commitment

- Extending definitions to the quantum realm is not trivial; there are at least three superficially plausible definitions of quantum bit commitment, for example.
- Adopting the $\mathbf{p_0 + p_1 < 1 + \_}$ condition, consistent with Mayers-Lo-Chau's analyses, we see their no-go theorem for unconditionally secure bit commitment can be evaded using relativistic constraints.
- Deniable bit commitment is also, surprisingly, possible.
- Relativistic cryptography (classical or quantum) offers a promising new direction to explore.
- New distinctions and new properties arise in quantum crypto: cheat sensitive protocols exist, tasks can be defined with or without classical certification, ….
- Related questions remain to be explored for oblivious transfer, secure multi-party computation, …

Summary: a quantum hierarchy



Strictly weaker than bit commitment. Simple relativistic protocol exists. Believed that no secure non-relativistic quantum protocols exist.

Unconditionally secure protocols possible using relativistic crypto: impossible with q info alone.

CCBC generates all other mistrustful primitives. **But** unconditionally secure implementation is impossible, even using q info **and** relativity.

X ⟶ Y Y can be securely implemented by a secure black box implementing X and quantum information exchanges

Conclusions…

- Mistrustful quantum crypto is presently much less well developed than quantum key distribution (and NB security proof for QKD it took 15 years!)
- Since unconditionally secure certificates of classicality are impossible, we need to consider schemes based on (quantum) computational or other technological assumptions.
- But as the cases of bit commitment and coin tossing illustrate, relativistic crypto does have considerable scope. The only tasks known to be impossible even when combining quantum information and relativistic crypto are those excluded by the simple "no certificates of classicality" argument. Perhaps everything else is possible?