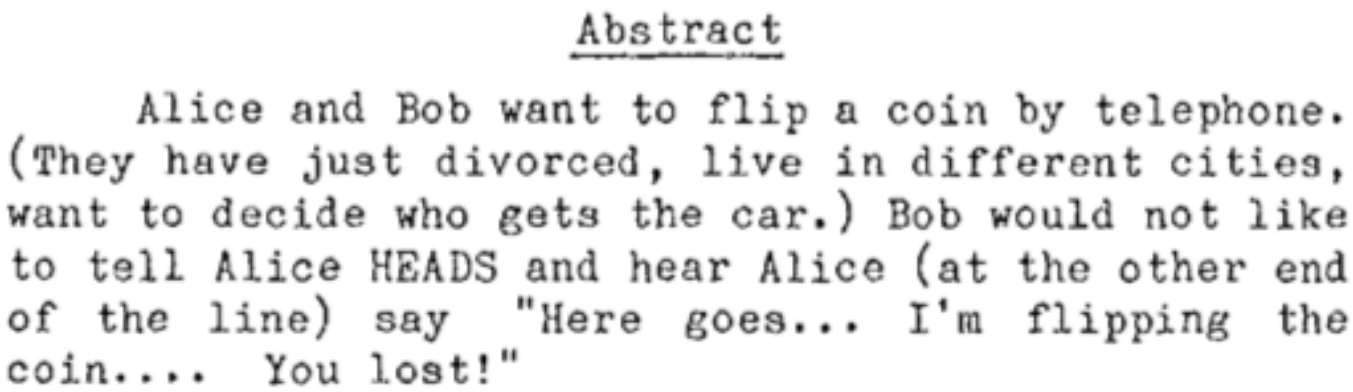
Alice (and Bob) in Wonderland

H. Bierlee N. Kankava

Uppsala University

π-day 2019

Problem statement



Abstract

Alice and Bob want to flip a coin by telephone. (They have just divorced, live in different cities, want to decide who gets the car.) Bob would not like to tell Alice HEADS and hear Alice (at the other end of the line) say "Here goes... I'm flipping the coin.... You lost!"

Figure: From *COIN FLIPPING BY TELEPHONE: A PROTOCOL FOR SOLVING IMPOSSIBLE PROBLEMS* by M. Blum (1981)

A classical solution: lock-box analogy

1. Alice writes down her call (heads/tails) on paper and locks it in a box
2. Alice sends the box (but not the key) to Bob
3. Bob tosses the coin and reports the outcome to Alice
4. Alice reveals who won and sends her key to Bob so he can verify Alice's claim

Relies on the unsure assumption that Bob cannot open the box, in other words: *computational hardness*.

Presentation overview

Quantum cryptography: Public key distribution and coin tossing
by Charles H. Bennett and G. Brassard (1984)

- ~~Problem statement~~
- Recap: behaviour of polarised photons
- Remote quantum coin-toss protocol
- Drawbacks
- Questions

Recap: behaviour of polarised photons

"presentation/res/""photon-behaviour".png

Quantum Coin-Toss Protocol

"presentation/res/""coin-table".pdf

Quantum Coin-Toss Protocol

"presentation/res/""coin-table".pdf

Quantum Coin-Toss Protocol

"presentation/res/""coin-table".pdf

Quantum Coin-Toss Protocol

"presentation/res/""coin-table".pdf

And now: ..volunteers?

Drawbacks

- We need *good* quantum hardware..
  - Otherwise Alice might accidentally send multiple photons, allowing Bob to measure multiple times and guess the filter with $> 50\%$ probability
- ..but we don't want *perfect* quantum hardware.
  - Otherwise Alice could cheat by 'entangling' photons with the so-called Einstein-Podolsky-Rosen effect
  - In practice likely impossible to achieve

First experimental quantum coin-toss already performed at the Laboratory for Communication and Processing of Information (LTCI) in Paris!

Conclusion

- By the properties of quantum mechanics, it is impossible to cheat:
  - Alice cannot cheat, because she can predict only one table with 100% accuracy, but not the other
  - Bob cannot cheat, because the photons give no information as to the basis he has to guess

- So we rely on the *laws of physics* instead of on *computational complexity*

Questions..?

Thank you for listening!

Report, slides and demo source code available at:
`https://github.com/hbierlee/quantum-coin-toss`