

Coin Flipping

Philippe LABOUCHERE

Supervisor: Roger COLBECK

May 19, 2008

1

- Classical Coin Flipping
- Distance Measures
- Bit Commitment
- Quantum Coin Flipping
- Conclusion

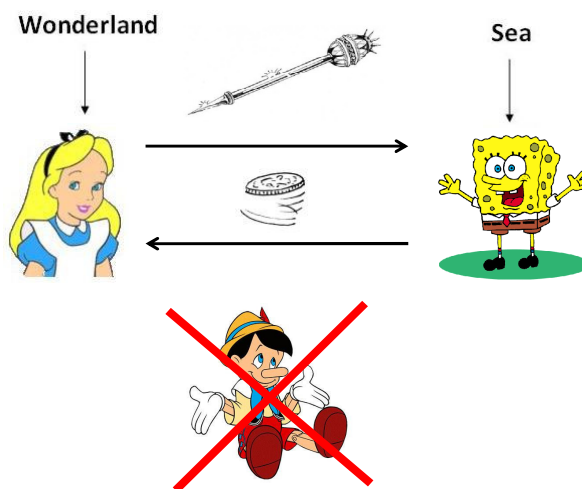
2

• Classical Coin Flipping

- Distance Measures
- Bit Commitment
- Quantum Coin Flipping
- Conclusion

3

Classical Coin Flipping



4

- Classical Coin Flipping
- **Distance Measures**
- Bit Commitment
- Quantum Coin Flipping
- Conclusion

5

Trace Distance

- Distinguishability between 2 probability distributions
- No physical process ever increases trace distance

$$D_{class}(p_x, q_x) = \frac{1}{2} \sum_x |p_x - q_x|$$



$$D_{quant}(\rho, \sigma) = \frac{1}{2} \text{Tr} |\rho - \sigma|$$

6

Fidelity

- Inner product

$$F_{class}(p_x, q_x) = \sum_x \sqrt{p_x \cdot q_x}$$



$$F_{quant}(\rho, \sigma) = \text{Tr} \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}}$$

- Uhlmann's theorem

$$F_{quant}(\rho, \sigma) = \max_{|\psi\rangle, |\phi\rangle} |\langle \psi | \phi \rangle|$$

- Fidelity is bounded

$$0 \leq F(\rho, \sigma) \leq 1$$

7

Relationship between distance measures

- Fidelity \approx ,upside-down' version of trace distance

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}$$

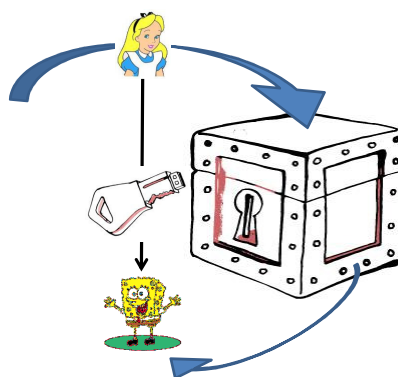
8

- Classical Coin Flipping
- Distance Measures
- **Bit Commitment**
- Quantum Coin Flipping
- Conclusion

9

Bit commitment

1. Committing phase
2. Holding phase
3. Unveiling phase



Alice doesn't trust Bob and vice-versa!

10

Impossibility of bit commitment

- Mayers '97 and Lo & Chau '97
- Bit commitment → coin flipping
- **BUT** coin flipping ~~↔~~ bit commitment
- EPR-type of attack

11

12

- Classical Coin Flipping
- Distance Measures
- Bit Commitment
- **Quantum Coin Flipping**
- Conclusion

13

Coin-Flipping Protocol

- 2 parties:
 - mistustful
 - far apart
 - do not share initial resources
 - have trusted error-free laboratories
- Absence of third + trustworthy party

14

Bias

- Balanced protocol

$$\text{Prob}_A = \text{Prob}_B = \frac{1}{2}$$

- Dishonest party

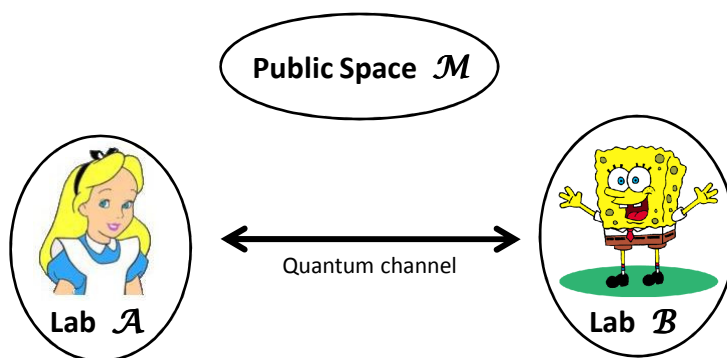
$$\text{Prob}_{b=0,1} \leq \frac{1}{2} + \epsilon$$

- Maximum bias

$$\epsilon_{\max} = (\text{Prob}_A, \text{Prob}_B) - \frac{1}{2}$$

15

Yao's model (I)



$$\mathcal{U} = \mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$$

16

Yao's model (II)

$$|\psi_0\rangle = |\psi_{A,0}\rangle \otimes |\psi_{M,0}\rangle \otimes |\psi_{B,0}\rangle$$



$$\textcircled{0}. \quad |\psi_{A,0}\rangle \text{ \& \ } |\psi_{MB,0}\rangle$$

$$\textcircled{1}. \quad (U_{AM} \otimes I_B) |\psi_0\rangle$$

$$\textcircled{2}. \quad (I_A \otimes U_{MB})(U_{AM} \otimes I_B) |\psi_0\rangle$$

$$\textcircled{N}. \quad (\Pi_A \otimes I_M \otimes \Pi_B) (\dots) (U_{AM} \otimes I_B) |\psi_0\rangle$$

17

Yao's model (III)

- Strategies

$$\sigma_A = (|\psi_{A,0}\rangle; U_{A,1}, \dots, U_{A,N-1}; \Pi_A) \in \Sigma_A$$

$$\sigma_B = (|\psi_{B,0}\rangle; U_{B,2}, \dots, U_{B,N}; \Pi_B) \in \Sigma_B$$

- Probability of getting bit value $b \in \{0,1\}$

$$\text{Prob}(\sigma_A, \sigma_B; b, b') = \text{Tr}[(\Pi_{A,b} \otimes I_M \otimes \Pi_{B,b'}) |\psi_N\rangle]$$

18

Strong Coin Tossing

- No party can fix in advance bit value
- 3 possible outcomes: 0, 1 or „fail“
- No a priori desired result
 - => 4 parameters $\epsilon_A^0, \epsilon_A^1, \epsilon_B^0, \epsilon_B^1 < \frac{1}{2}$
- Aim: prevent bias of coin's outcome from opponent

19

A protocol with $\epsilon = 0.25$ (I)

- Ambainis '02, Spekkens & Rudolph '02
- Step by step:

①.



Alice chooses a random bit value $b = 0$ or 1
a random value $x = 0$ or 1

sends the corresponding state
to Bob

$$|\phi_{b,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \text{if } b=0, x=0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } b=0, x=1 \\ \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle) & \text{if } b=1, x=0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle) & \text{if } b=1, x=1 \end{cases}$$

20

A protocol with $\varepsilon = 0.25$ (II)

2.



Bob chooses a random bit value $b' = 0$ or 1
and sends it to Alice

a) Alice sends b & x to Bob

3.



b) Bob measures received state $|\phi_{b,x}\rangle$
and checks for its correctness

• outcome is not $|\phi_{b,x}\rangle \Rightarrow$ Alice cheats!
-----Communication aborts-----

• outcome is $|\phi_{b,x}\rangle \Rightarrow$ result of coin flip is $b \oplus b'$

21

A protocol with $\varepsilon = 0.25$ (III)

- 2 cases: a) Alice is honest, Bob is dishonest
b) Alice is dishonest, Bob is honest

$$\bullet \text{ (a) } \rho_{b=0} = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \rho_{b=1} = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1/2 \end{pmatrix}$$

$$= |\phi_{0,0}\rangle\langle\phi_{0,0}| \& |\phi_{0,1}\rangle\langle\phi_{0,1}| \quad = |\phi_{1,0}\rangle\langle\phi_{1,0}| \& |\phi_{1,1}\rangle\langle\phi_{1,1}|$$

\rightarrow both with 50%

\rightarrow probability that Bob achieves $b \oplus b' = 0$ is at
most $\frac{3}{4} \rightarrow \frac{1}{2}(1 + D(\rho_0, \rho_1))$

22

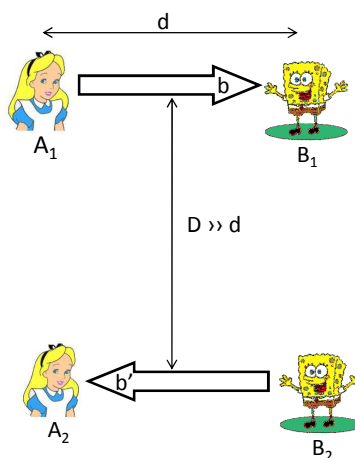
A protocol with $\varepsilon = 0.25$ (IV)

- (b)
 1. Symmetrization of Alice's strategy $\rightarrow \rho'$
 2. Max. probability of convincing Bob of a bit value b : $F(\rho', \rho_b)^2$
 3. Max. probability of convincing Bob of both bit values b : $\frac{1}{2} (F(\rho', \rho_0)^2 + F(\rho', \rho_1)^2)$
 4. $F(\rho', \rho_b) = \text{Tr} \sqrt{\sqrt{\rho'} \rho_b \sqrt{\rho'}} \Rightarrow$ extremization: $\frac{3}{4}$

23

Relativistic protocol

- Trusted agents
- Simultaneous communication
- Result $b \oplus b'$
- Security: $v_{\text{signal}} < c$



24

Weak Coin Tossing

- Alice & Bob have a preferred outcome



- 2 parameters $\varepsilon_A^1, \varepsilon_B^0 < \frac{1}{2}$

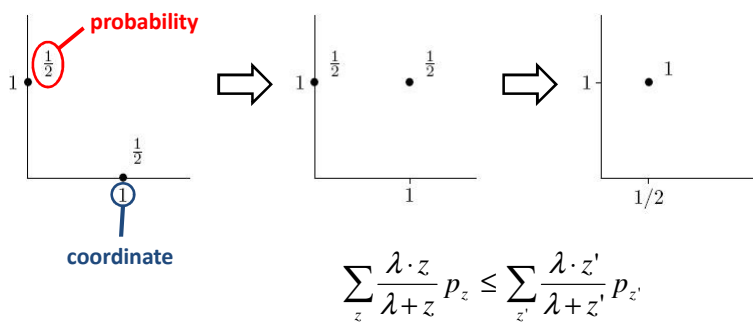
- Zero-sum game

	Alice	Bob
$b \oplus b' = 1$	1	-1
$b \oplus b' = 0$	-1	1
other	0	0

25

Kitaev's formalism

- Mapping from 'point games' to coin tossing protocols



26

- Classical Coin Flipping
- Distance Measures
- Bit Commitment
- Quantum Coin Flipping
- **Conclusion**

28

Take aways (I)

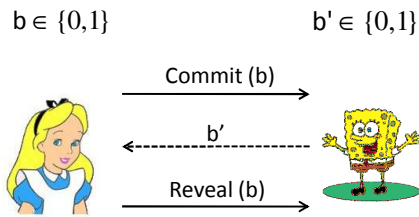
- Ideal coin tossing is impossible (Mayers '96, Lo & Chau '97)
- Non-ideal coin tossing is possible with a bias ϵ

	Best Protocol	Best Lower Bound
Strong Coin Tossing	$\epsilon = 0.25$ (Ambainis '02)	$\epsilon \approx 0.21$ (Kitaev '03)
Weak Coin Flipping	$\epsilon \rightarrow 0$ if #steps $\rightarrow \infty$ (Kitaev, Mochon '07)	$\epsilon > 0, \log(\log 1/\epsilon)$ rounds (Ambainis '02)

29

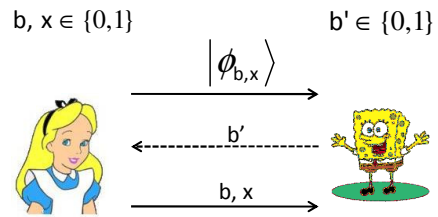
Take aways (II)

Classical Coin Flipping



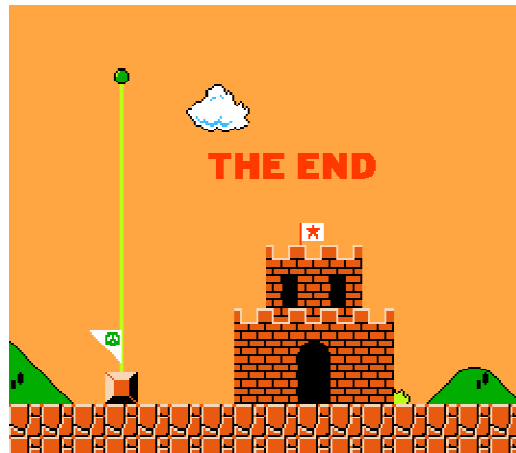
Result: $(b + b') \bmod 2$

Quantum Coin Flipping



Result: $(b + b') \bmod 2$

30



31