量子比特承诺

Quantum Bit Commitment

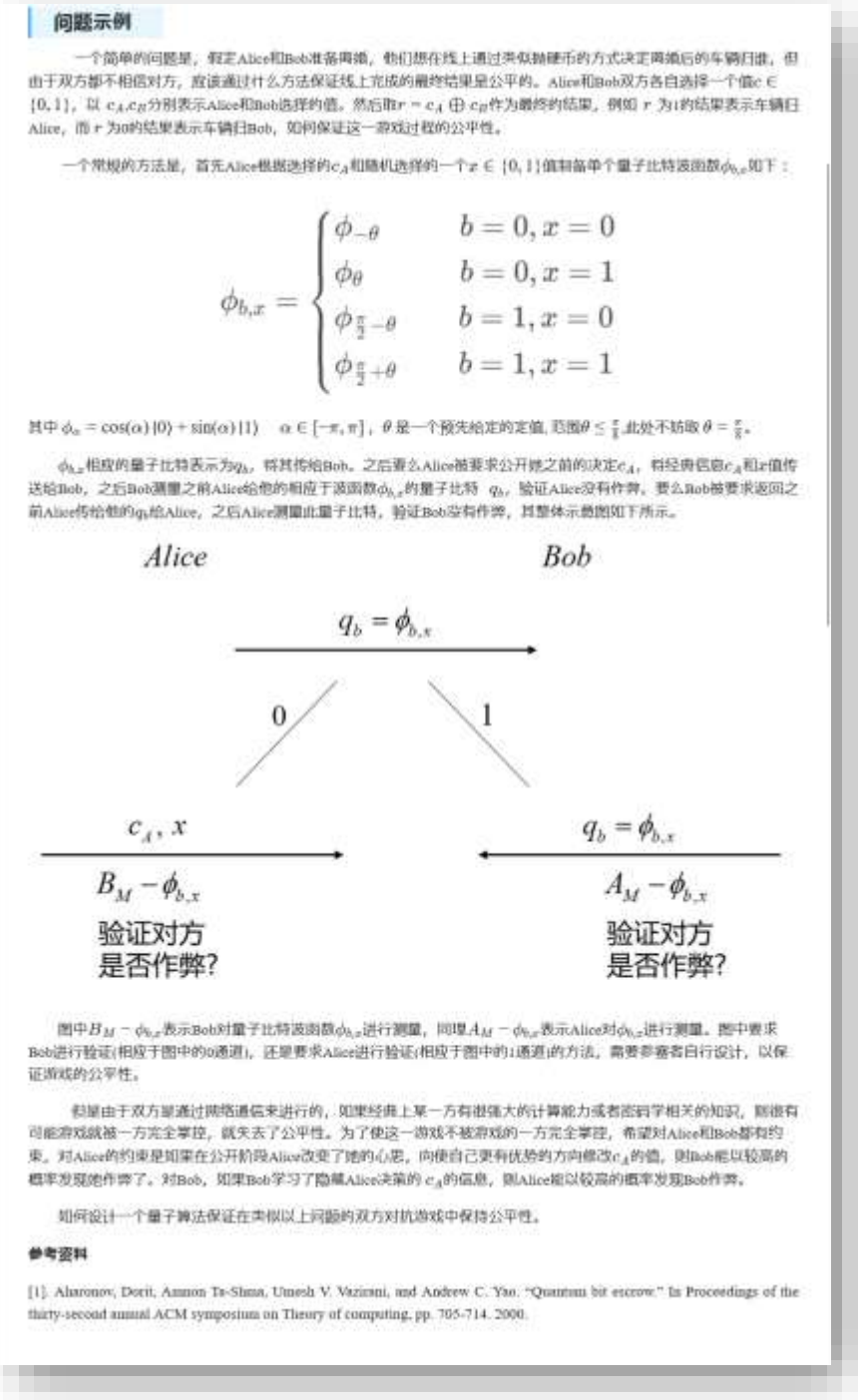
VHAKTYR

2023/9/11

比特承诺

- https://zhuanlan.zhihu.com/p/150514744

- 用来干啥的
  - A向B承诺一个秘密x，B不能立刻得知详情
  - 等到秘密可揭示时，A告知x'，B检查是否x=x'
- 难点
  - 公开之前，B不能得知x （保密性）
  - 承诺之后，A不能再修改x （绑定性）



问题示例

一个简单的问题是，假定Alice和Bob准备离婚，他们想在线上通过类似抛硬币的方式决定离婚后的车辆归谁，但由于双方都不相信对方，应该通过什么方法保证线上完成的最终结果是公平的。Alice和Bob双方各自选择一个值$c \in \{0,1\}$，以 c_A, c_B分别表示Alice和Bob选择的值。然后取$r = c_A \oplus c_B$作为最终的结果，例如 r 为1的结果表示车辆归Alice，而 r 为0的结果表示车辆归Bob，如何保证这一游戏过程的公平性。

一个常规的方法是，首先Alice根据选择的c_A和随机选择的一个$x \in \{0,1\}$值制备单个量子比特返回函数$\phi_{b,x}$如下：

$$\phi_{b,x} = \begin{cases} \phi_{-\theta} & b=0, x=0 \\ \phi_{\theta} & b=0, x=1 \\ \phi_{\frac{\pi}{2}-\theta} & b=1, x=0 \\ \phi_{\frac{\pi}{2}+\theta} & b=1, x=1 \end{cases}$$

其中 $\phi_\alpha = \cos(\alpha)|0\rangle + \sin(\alpha)|1\rangle \quad \alpha \in [-\pi, \pi]$，$\theta$ 是一个预先给定的定值，范围$\theta \leq \frac{\pi}{8}$，此处不妨取 $\theta = \frac{\pi}{8}$。

$\phi_{b,x}$相应的量子比特表示为q_b，将其传给Bob。之后要么Alice被要求公开她之前的决定c_A，将经典信息c_A和x值传送给Bob，之后Bob测量之前Alice给他的相应于返回函数$\phi_{b,x}$的量子比特 q_b，验证Alice没有作弊。要么Bob被要求返回之前Alice传给他的q_b给Alice，之后Alice测量此量子比特，验证Bob没有作弊，其整体示意图如下所示。

图中$B_M - \phi_{b,x}$表示Bob对量子比特返回函数$\phi_{b,x}$进行测量，同理$A_M - \phi_{b,x}$表示Alice对$\phi_{b,x}$进行测量。图中要求Bob进行验证(相应于图中的0通道)，还是要求Alice进行验证(相应于图中的1通道)的方法，需要参赛者自行设计，以保证游戏的公平性。

假设由于双方是通过网络通信来进行的，如果经典上某一方有很强大的计算能力或者密码学相关的知识，则很有可能游戏就被一方完全掌控，就失去了公平性。为了使这一游戏不被游戏的一方完全掌控，希望对Alice和Bob都有约束。对Alice的约束是如果在公开阶段Alice改变了她的心思，向使自己更有优势的方向修改c_A的值，则Bob能以较高的概率发现她作弊了。对Bob，如果Bob学习了隐藏Alice决策的 c_A的信息，则Alice能以较高的概率发现Bob作弊。

如何设计一个量子算法保证在类似以上问题的双方对抗游戏中保持公平性。

参考资料

[1]. Aharonov, Dorit, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. "Quantum bit escrow." In Proceedings of the thirty-second annual ACM symposium on Theory of computing, pp. 705-714. 2000.

比特承诺的实现

- 经典比特承诺
  - 承诺阶段：A把秘密x写在纸上装进密码箱，保留钥匙而把密码箱交给B
  - 公开阶段：A把钥匙给B并告知x’，B打开箱子验证x=x’
  - 不安全：B可以暴力穷举密码，提前知道x
- 量子比特承诺
  - 承诺阶段：A发送一串正基+(x=0)或斜基X(x=1)的基态光子，B随机选择基作测量，并记录所用基和测量结果
  - 公开阶段：A告知x和所发送的光子串的态，B核对使用正确的基作测量的那些结果是否完全一致
  - 量子通信的绝对安全性？🤔

量子比特承诺：示例

- A想要作承诺 x=1
  - A用斜基 X 制备光子串 ↗ ↗ ↖ ↗ ↖ ↖ ↖ ↗ ↗ ↖ ↗ ↗
- B用一串随机基来测量 +XX+X++X+X+X
  - 若B猜对了基，测量结果就是原始偏振方向：用 X 测 ↗ 得到 ↗
  - 否则以等概率投影到另一个基的两个轴向：用 + 测 ↗ 得到 ↑ 或 →
  - 假设B测量结果是 ↑ ↗ ↖ → ↖ → → ↗ ↑ ↖ → ↗
- A告知自己的承诺x和制备的光子串基态序列
- 如果A告诉B承诺是 x=1，检查一致
  - B用斜基X测读的部分结果：↗ ↖ ↖ ↗ ↖ ↗ ⟹ 011010
  - 对应于A告知的光子串方向：↗ ↖ ↖ ↗ ↖ ↗ ⟹ 011010
- 如果A告诉B承诺是 x=0，检查不一致
  - B检查用正基+测读的部分结果：↑ → → → ↑ → ⟹ 10001
  - 对应于A告知的光子串方向：↗ ↗ ↖ ↖ ↗ ↗ ⟹ 001100
- 绑定性：A承诺后无法反悔，除非A完美猜中B的所有测量结果
- 保密性：B无法提前得知A的承诺，除非A制备的光子方向不够正交

☑ ✕

转写规则：
任意一个方向读作 0
与之正交的方向读作 1

MLC no-go Theorem!!

- **不存在满足信息论安全的理论最强绑定性的量子比特承诺方案**
  - Hoi-Kwong Lo & Hoi Fung Chau (1996)
  - Dominic Mayers (1996)
  - “绝对安全性”：密文不会给攻击者提供任何有关于明文的信息
- 但是……纠缠态！
  - “作用在一个qubit上，非局域性地，另一个qubit也会受影响”
  - 如果A不是制备一串单光子，而是制备一串纠缠光子对……
    - 发送其中一个光子而自己保留另一个光子
    - 可以通过来在保留光子上作酉变换来改变B的测量概率幅
    - 几乎能完全主导B的测量结果，最大化自己猜对的概率
- 打破了绑定性，Alice可以不被Bob察觉地欺骗！

量子比特承诺攻击：示例

- A想要欺骗B，就要在公开阶段猜对B的测量结果
- 以一个传输单元为例，A制备纠缠态 ↗↗ + ↖↖ 而非单光子 ↗
  - 写成dirac记号形式就是 $|\psi\rangle = x|00\rangle + y|11\rangle$ $(x < y)$
- 存在一个酉变换 U (也就是一个单比特量子门) 使得
  - $(\mathrm{U@I})|\psi\rangle = ax|00\rangle + cy|01\rangle + bx|10\rangle + dy|11\rangle$
  - Alice持有左边这个高位qubit，她把 U 门作用其上
  - 变换了基底，振幅也重新分配
- 对每个传输单元，Alice选择合适的U
  - 提高ay/cy两项振幅，Bob测量结果为1的概率就更高；反之同理
  - 此时Alice宣布自己之前制备的光子态是 $|1\rangle$，就实现了欺骗

不妨记：
$\mathrm{U}|0\rangle = a|0\rangle + b|1\rangle$
$\mathrm{U}|1\rangle = c|0\rangle + d|1\rangle$