A non-interactive XOR quantum oblivious transfer protocol

Lara Stroh\textsuperscript{1}, Robert Stárek\textsuperscript{2}, Nikola Horová\textsuperscript{3}, Ittoop V. Puthoor\textsuperscript{1}, Miloslav Dušek\textsuperscript{2}, Erika Andersson\textsuperscript{1}

\textsuperscript{1}PAQS, Heriot-Watt University, UK \hspace{1cm} \textsuperscript{2}Department of Optics, Palacký University, Olomouc, Czech Republic

Background

- XOR oblivious transfer (XOT) is a variant of oblivious transfer (OT), a cryptographic primitive important for multi-party computations [1].
- General idea of XOT:
  - Alice sends two bits to Bob.
  - Bob can learn either the first bit or the second bit or their XOR, but not more than that.
  - Alice cannot know what he has learned.
- Perfect quantum OT is impossible with information-theoretic security [2,3] to focus on obtaining smallest possible cheating probabilities for (unrestricted) dishonest parties.
- “Reversing” a protocol: Bob sends a quantum state and Alice receives a quantum state, and other party can only receive quantum states, and other party can only receive quantum states then [4].

Strengths of Protocol 1

- Same cheating probabilities as interactive version [5], even with no testing by Bob.
- Best possible non-interactive quantum XOT protocol using pure symmetric states.
- Trade-off relation between Alice’s and Bob’s cheating probabilities in an optimal classical XOT protocol is beaten by quantum protocol → quantum advantage.

Protocol 1: Non-interactive quantum XOT

Inputs: Sender Alice has two bits $X_0, X_1$, Receiver Bob has $B \in \{0,1,2\}$ as input.

Qutrit states:
- $|\phi_0\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$.
- $|\phi_1\rangle = \frac{1}{\sqrt{3}}(|00\rangle - |11\rangle - |22\rangle)$.
- $|\psi_0\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$.
- $|\psi_1\rangle = \frac{1}{\sqrt{3}}(|00\rangle - |11\rangle - |22\rangle)$.

Actions:
1. (Alice) Chooses the random bits $x_0, x_1$, sends $|\phi_{x_0x_1}\rangle$ to Bob. (2) Bob performs an unambiguous state elimination measurement on the qutrit state to eliminate two out of the four possible states $|\psi_b\rangle$ Bob can deduce either $x_0, x_1$ or $x_2 = x_0 \oplus x_1$.  (3) Bob sends $r = (b + B + B) \text{mod} 3$ to Alice. (4) Let $x'_c = x_{(c+r)} \text{mod} 3$ for $c \in \{0,1,2\}$. To Bob, Alice sends $(s_0, s_1) = \left( x'_0 \oplus x'_{0'} \oplus x'_1 \oplus x'_{1'} \right)$ if $r = 0$. $(x'_1 \oplus x'_0 \oplus x'_2 \oplus x'_{2'})$ if $r = 1$. $(x'_2 \oplus x'_0 \oplus x'_3 \oplus x'_{3'})$ if $r = 2$.

Output: Bob outputs $y' = y \oplus s_p$, where, for $B = 0, s_2 = s_0 \oplus s_1$.

- Adapted from non-device independent interactive protocol in [5] → advantages: no need for entanglement and have non-interactive protocol.
- Classical post-processing (Steps (3) and (4)) added to resulting semi-random XOT protocol to ensure Bob can actively choose the bit he wants to obtain.
- Cheating probabilities:
  - Bob: $B_{OT} = 3/4$ By using a minimum-error measurement.
  - Alice: $A_{OT} = 1/2$ By sending one of the states $|0\rangle, |1\rangle$, or $|2\rangle$ instead. (No need for testing by Bob as does not decrease $A_{OT}$)

Protocol 2: Reversed non-interactive quantum XOT

Inputs: Sender Bob has $B \in \{0,1,2\}$ and the random bit $y$, Receiver Alice has two bits $X_0, X_1$ as input.

Qutrit states:
- $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle + |22\rangle)$. $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle - |22\rangle)$. $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle + |22\rangle)$. $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle - |22\rangle)$. $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle + |22\rangle)$. $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle - |22\rangle)$. $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle + |22\rangle)$. $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle - |22\rangle)$. $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle + |22\rangle)$. $|\phi_{x_0x_1} = \frac{1}{\sqrt{2}} (|00\rangle - |22\rangle).$

Actions: (1) Bob chooses $b$ and the random bit $y$, sends $|\phi_{yB}\rangle$ to Alice. (2) Alice performs a measurement with measurement operators $\Pi_{00} = \frac{1}{4}(|0\rangle + |3\rangle)\langle 0| + |3\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|). \Pi_{01} = \frac{1}{4}(|0\rangle - |3\rangle)\langle 0| - |3\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|). \Pi_{11} = \frac{1}{4}(|0\rangle - |3\rangle)\langle 0| - |3\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|) + \Pi_{01}$. (3) Alice sends $(x_0, x_2)$ to Bob, where, for $c \in \{0,1,2\}$, $t_2 = x_c \oplus X_c$.

Output: Bob outputs $y' = y \oplus t_p$, where, for $B = 2, t_2 = t_0 \oplus t_1$. (4) Classical post-processing (Step (3)) added to the reversed XOT protocol to ensure Alice can actively choose the values of her bits. (5) Cheating probabilities:
- Bob: $B_{OT} = 3/4$ By sending one of the states $(|0\rangle + |1\rangle + |2\rangle)/\sqrt{3}$, $(|0\rangle - |1\rangle + |2\rangle)/\sqrt{3}$, $(|0\rangle - |1\rangle + |2\rangle)/\sqrt{3}$, or $(-|0\rangle - |1\rangle + |2\rangle)/\sqrt{3}$ instead. (No need for testing by Alice as does not decrease $B_{OT}$)
- Alice: $A_{OT} = 1/2$ By using a minimum-error measurement.

On-going experimental work

- Realising an optical implementation of both protocols, including their cheating strategies:
  - Encoding qutrits into a single photon (photon’s path and polarization [6]).
  - Realising measurements by a reconfigurable interferometric network (with beam displacers and waveplates) and single-photon detection.
- Detailed scheme of the experimental setup:
  - Various combinations of standard, small, and ring waveplates
  - Beam-displacers (semi-transparent blue boxes)
  - Glass plates (orange boxes) for phase tuning

References