A non-interactive XOR quantum oblivious transfer protocol

Lara Stroh[1], Robert Stárek[2], Nikola Horová[2], Ittoop V. Puthoor[1], Miloslav Dušek[2], Erika Andersson[1]

[1] IPAQS, Heriot-Watt University, UK [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] → focus on obtaining smallest possible cheating probabilities for (unrestricted) dishonest parties.
- "Reversing" a protocol: Bob sends a quantum state and Alice measures a received state, while still implementing OT from Alice to Bob → allows us to implement OT both ways, even if one party can only send quantum states, and other party can only receive them [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.

References

[1] J. Kilian, in *Proc. 20th Annu. ACM Symposium Theory of Comput. (STOC '88)* (1988), pp. 20-31.
[2] D. Mayers, *Phys. Rev. Lett.*, vol. 78, no. 17, pp. 3414–3417, 1997.
[3] H.-K. Lo, *Phys. Rev. A*, vol. 56, no. 2, pp. 1154– 1162, 1997.
[4] C. Crépeau, and M. Sántha, in *Advances in Cryptology — EUROCRYPT '91* (1991), p. 106.
[5] S. Kundu, J. Sikora, and E. Y. -Z. Tan, A device-independent protocol for XOR oblivious transfer, *arXiv:2006.06671* (2020).
[6] R. Amiri *et al.*, *PRX Quantum*, vol. 2, no. 1, 010335, 2021.

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:

$$|\phi_{00}\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \quad |\phi_{01}\rangle = \frac{1}{\sqrt{3}}(|0\rangle - |1\rangle + |2\rangle),$$
$$|\phi_{11}\rangle = \frac{1}{\sqrt{3}}(|0\rangle - |1\rangle - |2\rangle), \quad |\phi_{10}\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle - |2\rangle).$$

Actions: (1) Alice chooses the random bits x_0, x_1, sends $|\phi_{x_0 x_1}\rangle$ to Bob.

(2) Bob performs an unambiguous state elimination measurement on the qutrit state to eliminate two out of the four possible states → Bob can deduce either x_0, x_1, or $x_2 = x_0 \oplus x_1$. His outcome is given by (y, b), where $b \in \{0,1,2\}$ and $y = x_b$.

(3) Bob sends $r = (b + B + B) \bmod 3$ to Alice.

(4) Let $x'_c = x_{(c+r) \bmod 3}$ for $c \in \{0,1,2\}$. To Bob, Alice sends

$$(s_0, s_1) = \begin{cases} (x'_0 \oplus X_0, x'_1 \oplus X_1) & \text{if } r = 0. \\ (x'_1 \oplus X_0, x'_2 \oplus X_1) & \text{if } r = 1. \\ (x'_2 \oplus X_0, x'_0 \oplus X_1) & \text{if } r = 2. \end{cases}$$

Output: Bob outputs $y' = y \oplus s_B$, where, for $B = 2$, $s_2 = s_0 \oplus s_1$.

- 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:

$$|\phi_{x_0=0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle), \quad |\phi_{x_0=1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle),$$
$$|\phi_{x_1=0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\phi_{x_1=1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$
$$|\phi_{x_2=0}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |\phi_{x_2=1}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle).$$

Actions: (1) Bob chooses b and the random bit y, sends $|\phi_{x_b=y}\rangle$ to Alice.

(2) Alice performs a measurement with measurement operators

$$\Pi_{00} = \frac{1}{4}(|0\rangle + |1\rangle + |2\rangle)(\langle 0| + \langle 1| + \langle 2|), \quad \Pi_{01} = \frac{1}{4}(|0\rangle - |1\rangle + |2\rangle)(\langle 0| - \langle 1| + \langle 2|),$$
$$\Pi_{11} = \frac{1}{4}(|0\rangle - |1\rangle - |2\rangle)(\langle 0| - \langle 1| - \langle 2|), \quad \Pi_{10} = \frac{1}{4}(|0\rangle + |1\rangle - |2\rangle)(\langle 0| + \langle 1| - \langle 2|)$$

on the received qutrit state, obtains outcome (x_0, x_1).

(3) Alice sends (t_0, t_1) to Bob, where, for $c \in \{0,1\}$, $t_c = x_c \oplus X_c$.

Output: Bob outputs $y' = y \oplus t_B$, where, for b= 2, $t_2 = t_0 \oplus t_1$.

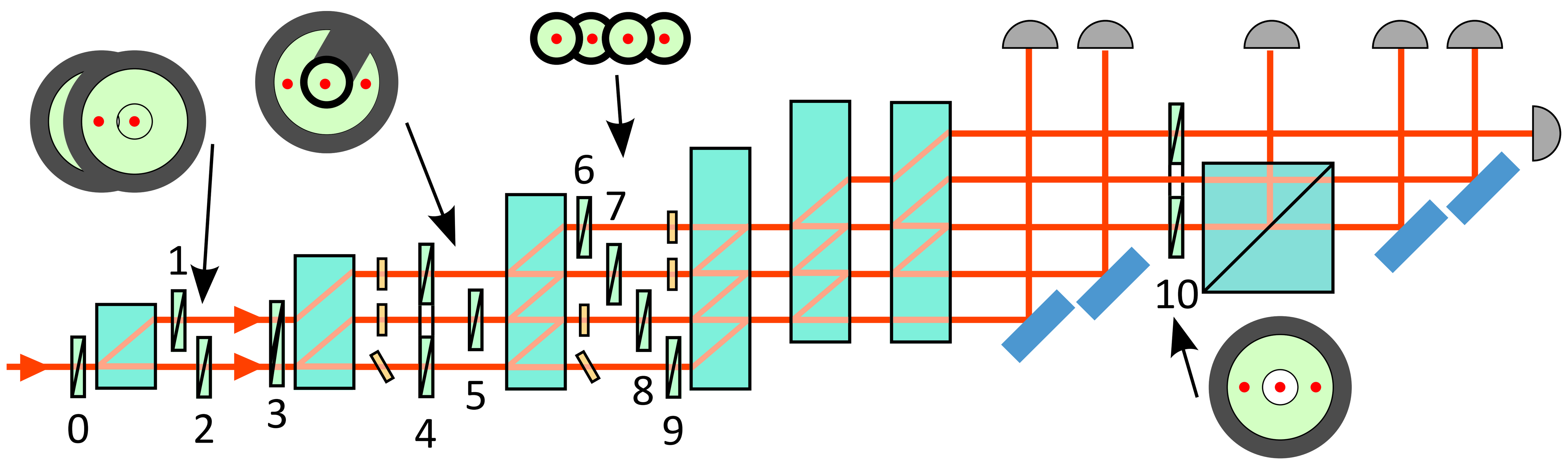
- Classical post-processing (Step (3)) added to the reversed XOT protocol to ensure Alice can actively choose the values of her bits.
- Cheating probabilities:

Bob: $B^r_{OT} = 3/4$ 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^r_{OT}.)

Alice: $A^r_{OT} = 1/2$ 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



HERIOT WATT UNIVERSITY
Palacký University Olomouc
EPSRC Engineering and Physical Sciences Research Council
QUANTUM COMMUNICATIONS HUB