Imperfect quantum oblivious transfer with one-sided security

David Reichmuth*, Ittoop Vergheese Puthoor*, Petros Wallden** and Erika Andersson*, * Heriot-Watt University, ** University of Edinburgh

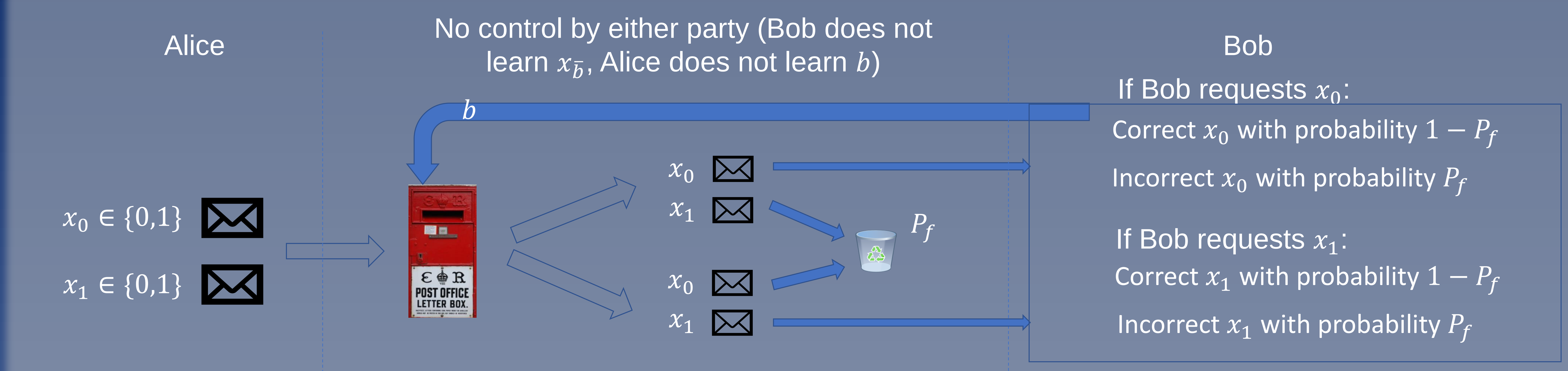
Oblivious transfer:

- Alice has two bits, x_0 and x_1
- Bob obtains x_b where $b \in \{0,1\}$ (b usually chosen by Bob)
- Alice should not learn b, Bob does not learn $x_{\bar{b}}$ (other bit)
- Why? Oblivious transfer enables multiparty computation
- Perfect quantum oblivious transfer is impossible (except if e.g. quantum memory is restricted), but there are bounds on cheating probabilities for Alice and Bob.

Imperfect oblivious transfer:

- Fails with probability P_f
- Cheating probabilities can be lower than for perfect oblivious transfer
- Part of how to deal with noise and imperfections
- Connects standard oblivious transfer and (quantum) random access codes (RACs, QRACs).

One-sided security: One party, here Alice, cannot cheat at all.

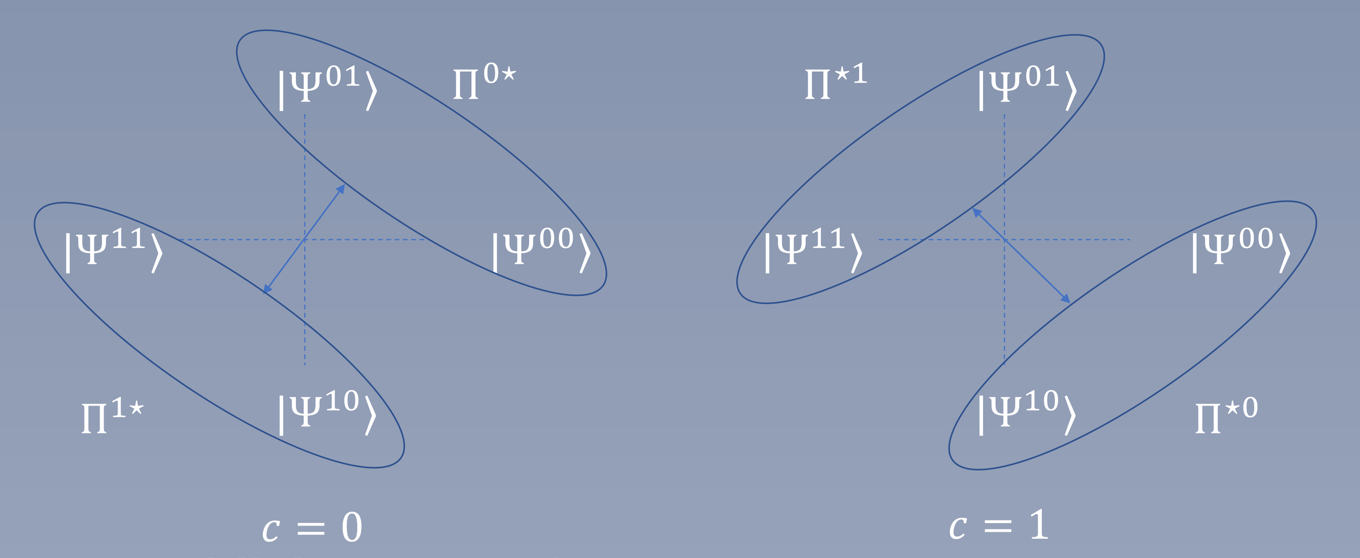


Complete Oblivious Transfer, $P_f = 0$:

- Protocol does not fail (complete) BUT
- Imperfect security against Alice and Bob; if one of them cannot cheat, then the other party necessarily cheats perfectly.

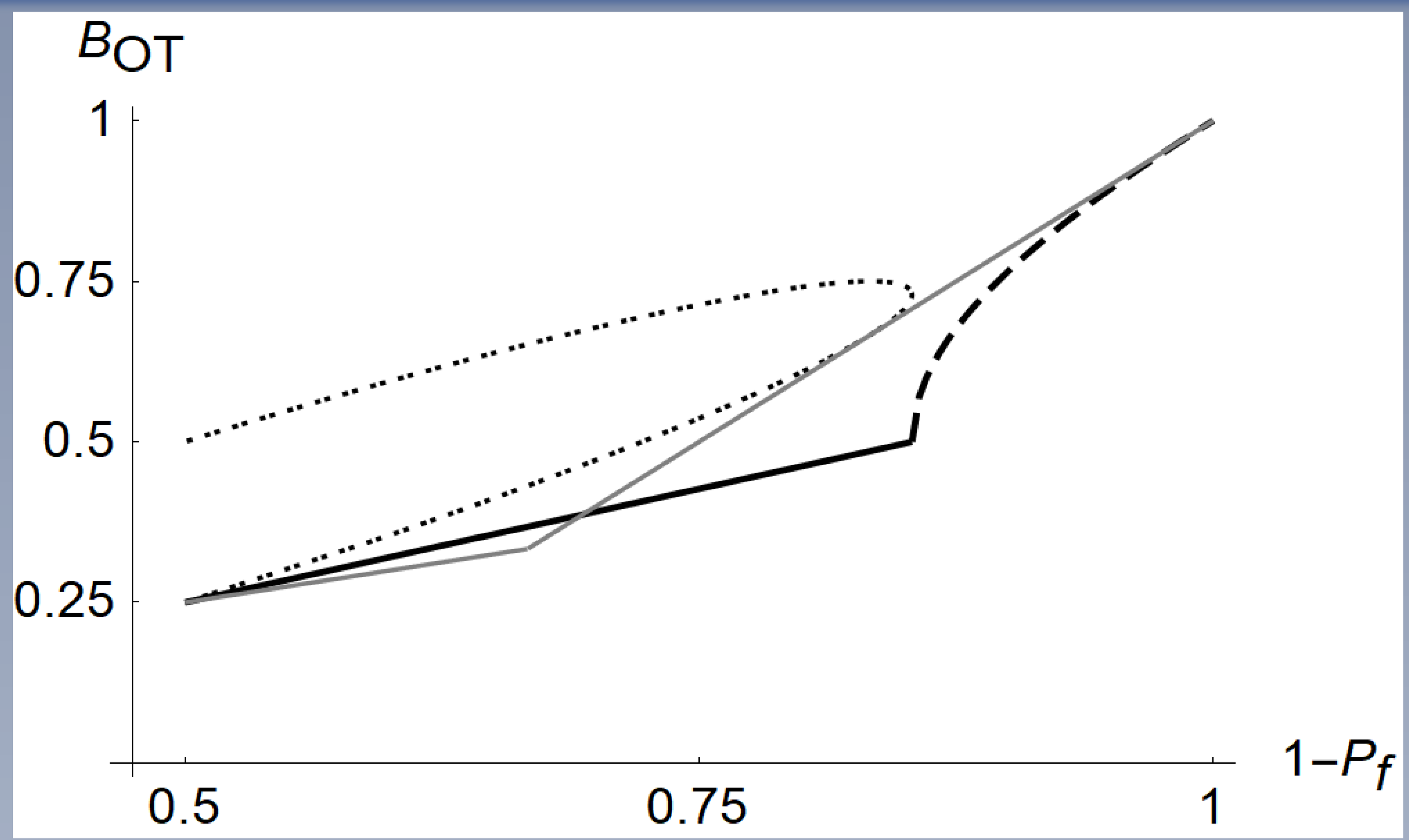
Incomplete Oblivious Transfer, $P_f \neq 0$:

- Protocol sometimes fails BUT
- Even when Alice cannot cheat at all (better than with a random guess), Bob's cheating probability is limited.



Quantum Oblivious Transfer

- Alice sends one of four symmetric pure quantum states $|\psi^{x_0 x_1}\rangle$
- Limited security against Alice: Bob performs a fixed POVM with $\{\Pi^{0\star}, \Pi^{1\star}, \Pi^{\star 0}, \Pi^{\star 1}\}$. Completeness ($P_f = 0$) possible.
- **One-sided security against Alice by no-signalling**: Bob chooses measurement $\{\Pi^{0\star}, \Pi^{1\star}\}$ for $b = 0$, $\{\Pi^{\star 0}, \Pi^{\star 1}\}$ for $b = 1$. Completeness not possible, $P_f \neq 0$.



Optimal protocols using symmetric pure states

For a given failure probability P_f, Bob's cheating probability B_{OT} is as low as possible and vice versa.

Protocols with qubits and ququarts (2 qubits) are optimal quantum protocols using symmetric pure states

Qubit states (optimal) – solid line
Qutrit states (suboptimal) – dotted line
Ququart states (optimal) – dashed line
Best possible classical protocols – grey line
The optimal quantum protocols beat the best possible classical protocols in the region $1 - P_f \gtrsim 0.69$.

Coherent state protocols – surprisingly poor performance

$|\Psi^i\rangle|\Psi^j\rangle = |\pm\alpha/\sqrt{2}\rangle|\pm\alpha/\sqrt{2}\rangle$

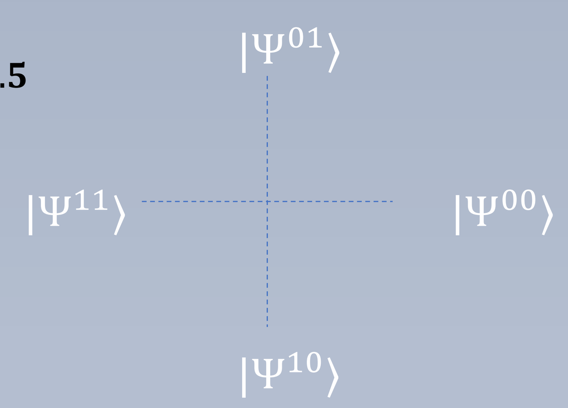
$i,j \to |\alpha,\alpha,\alpha,-\alpha\rangle, |\alpha,\alpha,-\alpha,\alpha\rangle, \ldots$

Phase-encode states $ij \to |\pm(i)\alpha\rangle$

with optimal measurement for Bob and with homodyne detection

Cheating Success Bound for Bob B_{OT}

- What state was prepared?
- Measurement: $\pi^{ij} = p^{ij}\hat{\rho}^{-0.5}\hat{\rho}^{ij}\hat{\rho}^{-0.5}$
- Gram Matrix $G_{kl} = \langle\Psi_k|\Psi_l\rangle$
  - $f = \langle\Psi^{00}|\Psi^{01}\rangle$, $f^* = \langle\Psi^{01}|\Psi^{00}\rangle$, $g = \langle\Psi^{00}|\Psi^{11}\rangle$
  - Find Eigenvalues λ_i
  - $B_{OT} = \frac{1}{16}\left|\sum_i \lambda_i\right|^2$



- $B_{OT} = \frac{1}{16}\left(\sqrt{1 + 2\Re(F) + G} + \sqrt{1 - 2\Re(F) + G} + \sqrt{1 + 2\Im(F) - G} + \sqrt{1 - 2\Im(F) - G}\right)^2$

Failure Probability P_f

- Lowest possible P_f for a given cheating probability for Bob:
  - Distinguishability of mixed states
  - Re-express in orthogonal basis $|B_k\rangle = \sum_l \mathrm{Exp}\left[\frac{i2\pi kl}{N}\right]|\Psi_l\rangle$
  - Eigenvalues of $(\rho_{c=1} - \rho_{c=0}) \to \eta_i$
  - $P_f = \frac{1}{2}\left(1 - \frac{1}{2}\sum_i |\eta_i|\right)$
  - $P_f = \frac{1}{2}\left(1 - \frac{1}{2}\sqrt{1 - G^2 + 2\sqrt{(1+G)^2\Im(F)^2 + (1-G)^2\Re(F)^2 - 4\Re(F)^2\Im(F)^2} - (\ldots)}\right)$