Impossibility of composable Oblivious Transfer in relativistic quantum cryptography

Lorenzo Laneve[1], Lídia del Rio[2]

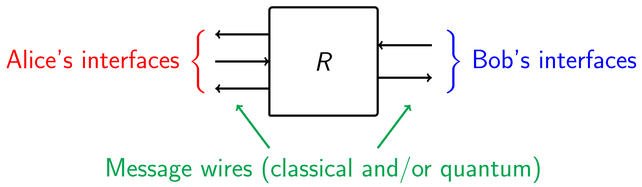
[1]Department of Computer Science, ETH Zürich, 8092 Zurich, Switzerland, [2]Institute for Theoretical Physics, ETH Zürich, 8093 Zurich, Switzerland

arXiv:2106.11200

ETH zürich

A resource theory of cryptography

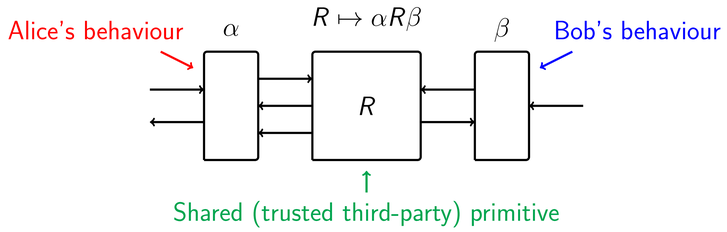
In the *Abstract Cryptography framework* [1], primitives and protocols are represented through *resources*, black boxes with inputs and outputs.



Special relativity: R cannot process faster than the speed of light! [2]

Composing resources

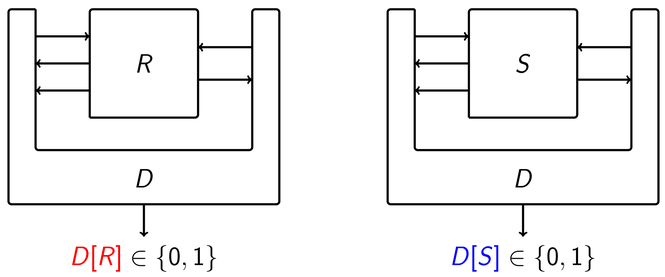
The framework defines composing operations between resources.



The pair (α, β) can be seen as a *protocol*.

Distinguishers

Resources observing other resources, and returning a bit $b \in \{0,1\}$.



$$d^D(R,S) = \left|\mathbb{P}\left[D[R]=1\right] - \mathbb{P}\left[D[S]=1\right]\right|$$

Advantage = statistical distance

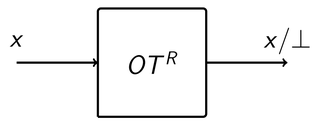
Two resources R, S are ε-close if and only if

$$R \approx_\varepsilon S \iff \delta(R,S) := \sup_D d^D(R,S) \leq \varepsilon$$

Composability $\implies \delta$ is a (pseudo-)metric between resources!

Oblivious Transfer

A (Rabin) Oblivious Transfer takes a bit x from Alice and delivers it to Bob with probability $\frac{1}{2}$.

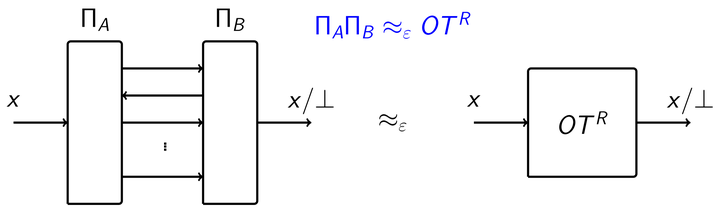


Equivalence result: other versions of OT, equivalence between versions in the relativistic quantum setting.

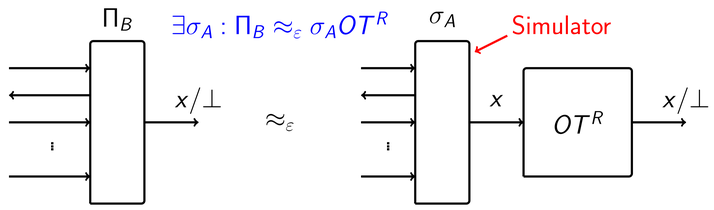
Security against dishonest behaviour

A protocol $\Pi = (\Pi_A, \Pi_B)$ between Alice and Bob ε-constructs the Rabin Oblivious Transfer if and only if the following conditions hold:

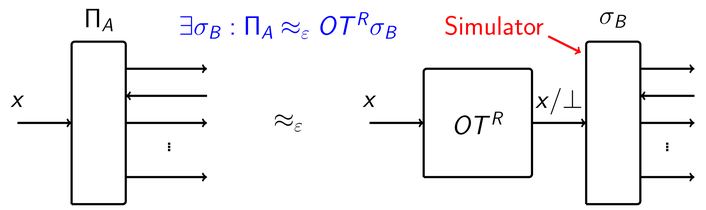
Correctness: both parties are honest $\Rightarrow$ protocol indistinguishable from OT.



Countering dishonest Alice: honest Bob always sees something indistinguishable from an OT on his interface regardless of Alice's behaviour.



Countering dishonest Bob: honest Alice always sees something indistinguishable from an OT on his interface regardless of Bob's behaviour.



The probability that the honest construction fails, as well as the probabilities that one of the parties manages to cheat is bounded by ε.

Impossibility of Oblivious Transfer

Theorem. *For any $\varepsilon < \frac{1}{24}$, no protocol $\Pi = (\Pi_A, \Pi_B)$ ε-constructs the Rabin OT, be it classical, quantum, and/or relativistic.*

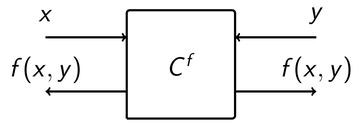
Note: $\frac{1}{24}$ is the advantage of some distinguisher!

Corollary. *Oblivious Transfer of s-bit strings is impossible to ε-construct, for*

$$\varepsilon < \frac{1}{12}\left(1 - \frac{1}{2^s}\right)$$

Impossibility of Multi Party Computation

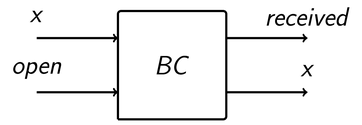
Theorem. *Two-party computation of $f(x,y) = xy$ is impossible to ε-construct, for $\varepsilon < \frac{1}{12}$.*



$\implies$ **Relativistic quantum multi party computation is impossible!**

Mutual construction with Bit Commitment

Alice commits to a bit x, Bob receives x only when Alice opens the commit.



Theorem. *Bit Commitment can be $o(1)$-constructed from n instances of Oblivious Transfer, and viceversa.* (Adapted from Unruh's construction [3])

References

[1] U. Maurer and R. Renner. Abstract cryptography. In B. Chazelle, editor, *The Second Symposium on Innovations in Computer Science, ICS 2011*. Tsinghua University Press, 1 2011.

[2] C. Portmann, C. Matt, U. Maurer, R. Renner, and B. Tackmann. Causal boxes: Quantum information-processing systems closed under composition. *IEEE Transactions on Information Theory*, 63(5):3277–3305, 2017.

[3] D. Unruh. Universally composable quantum multi-party computation. In H. Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, pages 486–505, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.