Validity of quantum physics.

1. The inner-products $\gamma$

2. No information about $x$

3. Alice sets $x$

4. Bob chooses a basis with $x$

Assumptions common to all QKD protocols:

- Lower bound on asymptotic key rate per round [4]:
- $R = R_{\text{Asym}}(A|E;B_{\text{succ}}) - H_{2}(Q\text{BER})p(\text{succ})$ (1)
- QBER, $p(\text{succ})$ estimated from the data $p(b|x,y)$
- Estimation of $H_{\text{Asym}}(A|E;B_{\text{succ}})$ can be relaxed to a hierarchy of semi-definite programs (SDPs) using solely $p(b|x,y)$ and $\gamma_{x,x'}$ [5].

Main results:

- Protocol with one partially trusted party and a complete untrusted receiver (in comparison to [1]).
- No assumptions on the receiver: proof against attacks on detectors (in comparison to [2]).
- Simple prepare-and-measure implementation, no need for entanglement (in comparison to [3]).

References: