Post-selection technique with applications to quantum cryptography and the parallel repetition problem

Dejan D. Dukaric, ETH Zurich

joint work with

Matthias Christandl, LMU Munich
Robert König, Caltech
Renato Renner, ETH Zurich

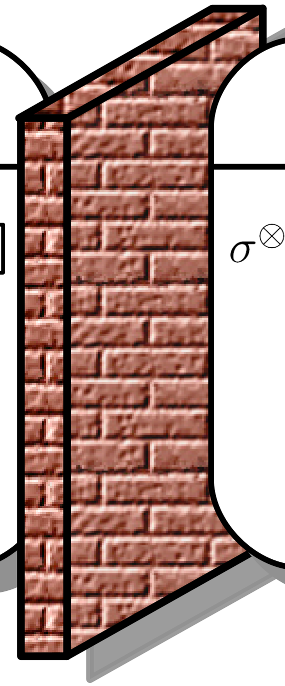
QIP, January 16, 2009, Santa Fe

Goal of Post-Selection Technique

Permutation invariant state

$|\Psi^n\rangle\langle\Psi^n| = \square\square\square\square \cdots \square$

$$\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq \;\; ??$$



Product state

$\sigma^{\otimes n} = \square \otimes \square \otimes \square \otimes \cdots \otimes \square$

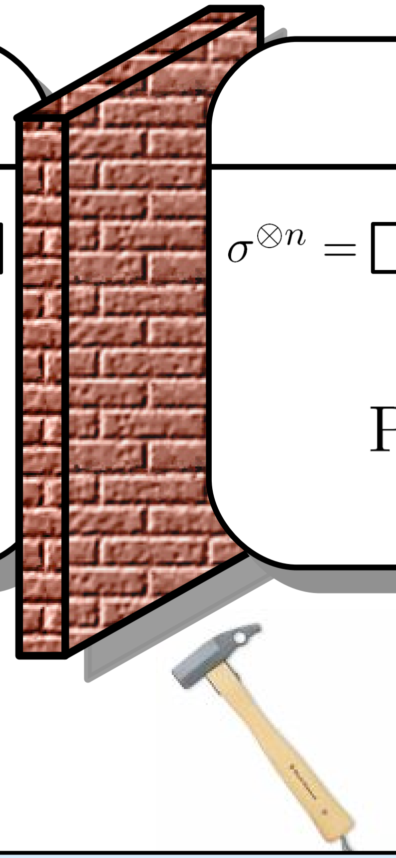
$$\Pr[\mathcal{P}(\sigma^{\otimes n}) = true] \leq 2^{-c \cdot n}$$

Goal of Post-Selection Technique

Permutation invariant state

$|\Psi^n\rangle\langle\Psi^n| = \square\square\square\square\cdots\square$

$$\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq \;??$$



Product state

$\sigma^{\otimes n} = \square \otimes \square \otimes \square \otimes \cdots \otimes \square$

$$\Pr[\mathcal{P}(\sigma^{\otimes n}) = true] \leq 2^{-c \cdot n}$$

Post-Selection “Hammer”

Main Result

Permutation invariant state

$|\Psi^n\rangle\langle\Psi^n| = \square\square\square\square\cdots\square$

$$\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq \;??$$

Product state

$\sigma^{\otimes n} = \square \otimes \square \otimes \square \otimes \cdots \otimes \square$

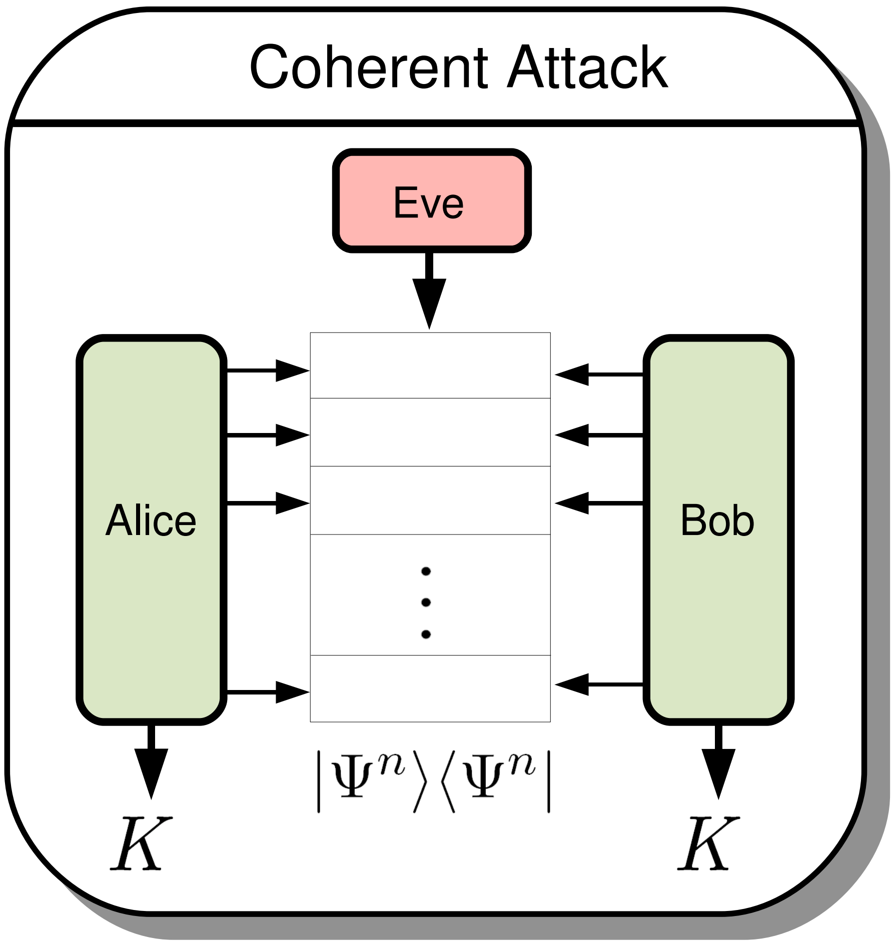
$$\Pr[\mathcal{P}(\sigma^{\otimes n}) = true] \leq 2^{-c \cdot n}$$

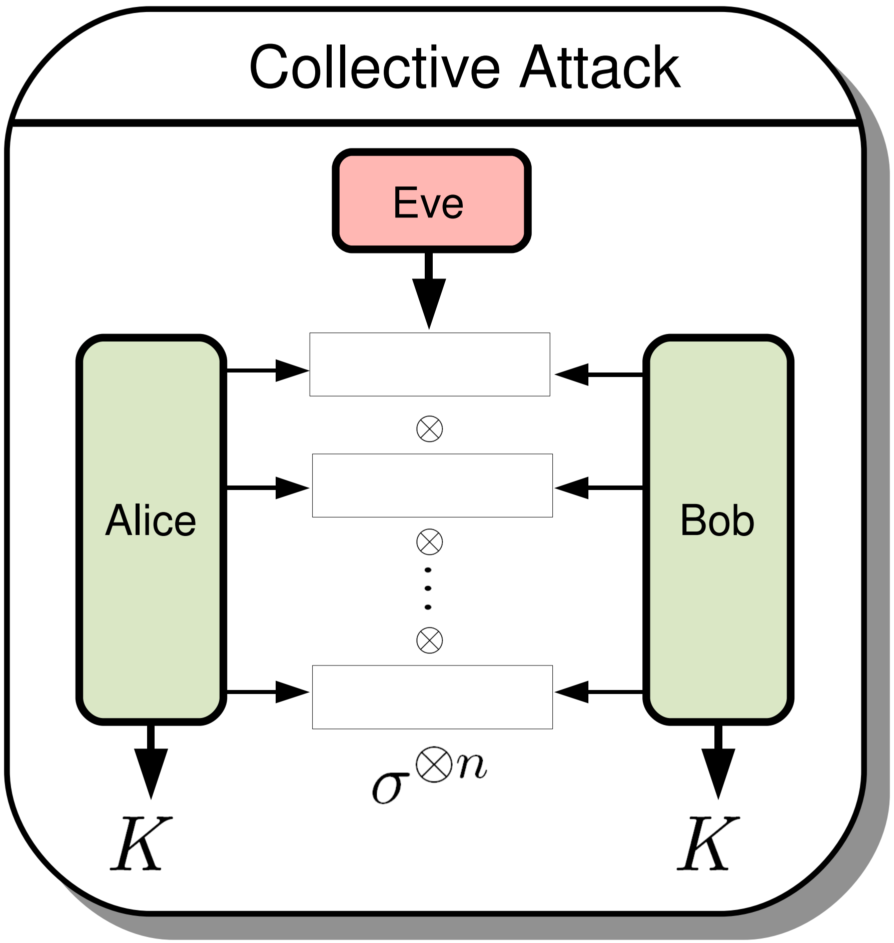
Post-Selection Technique

$$\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$$

Example 1: Quantum Key Distribution

$\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true \Leftrightarrow$ key generated starting from $|\Psi^n\rangle\langle\Psi^n|$ not secure





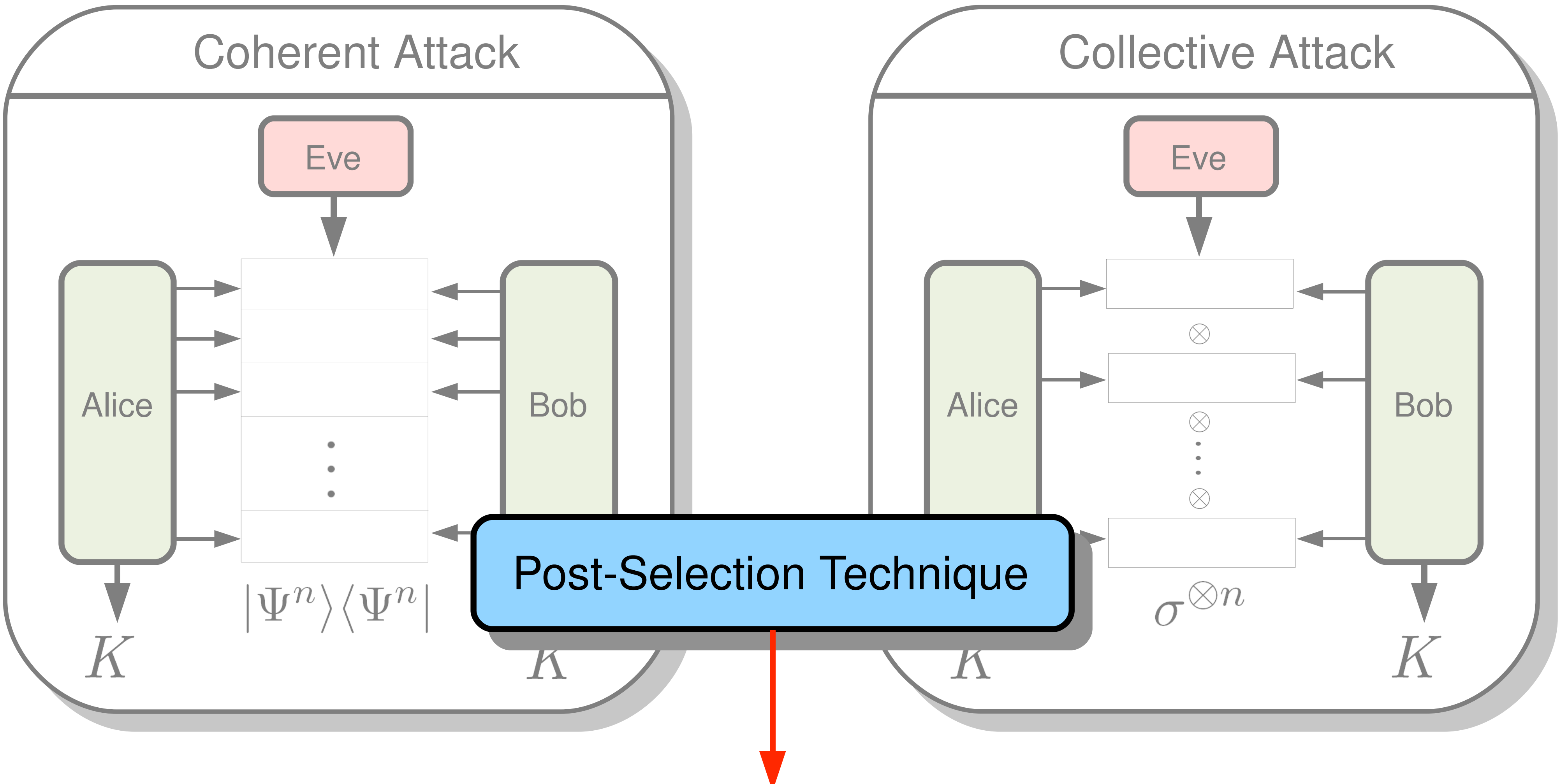
$\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq \;??$

$\Pr[\mathcal{P}(\sigma^{\otimes n}) = true] \leq 2^{-c \cdot n}$

(Devetak & Winter, 2005)

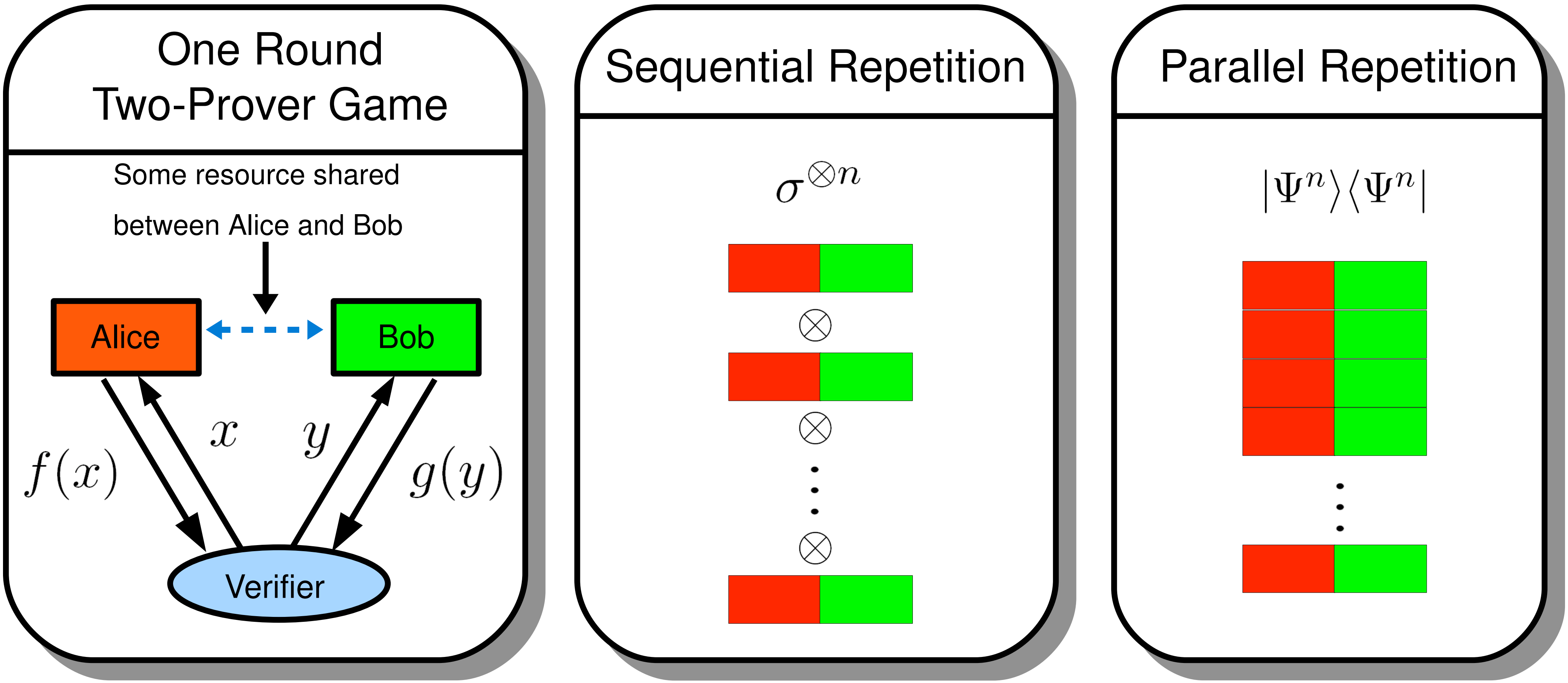
Example 1: Quantum Key Distribution

$\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true \Leftrightarrow$ key generated starting from $|\Psi^n\rangle\langle\Psi^n|$ not secure



$\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot 2^{-c \cdot n}$ ← $\Pr[\mathcal{P}(\sigma^{\otimes n}) = true] \leq 2^{-c \cdot n}$

Example 2: Parallel Repetition of Two-Prover Games

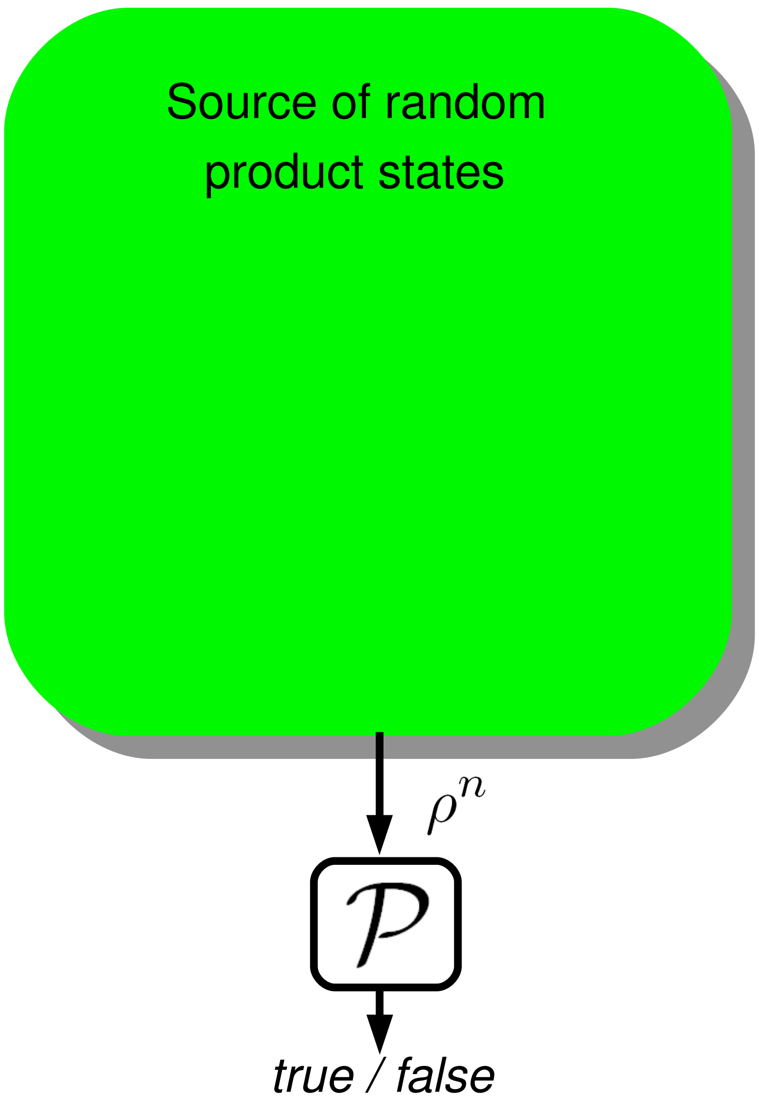


$\Rightarrow$ Post-selection technique can reduce problem to optimization problem over convex set with linear constraint function.

(Raz, 1998 / Holenstein, 2007)

How the Post-Selection Technique Works

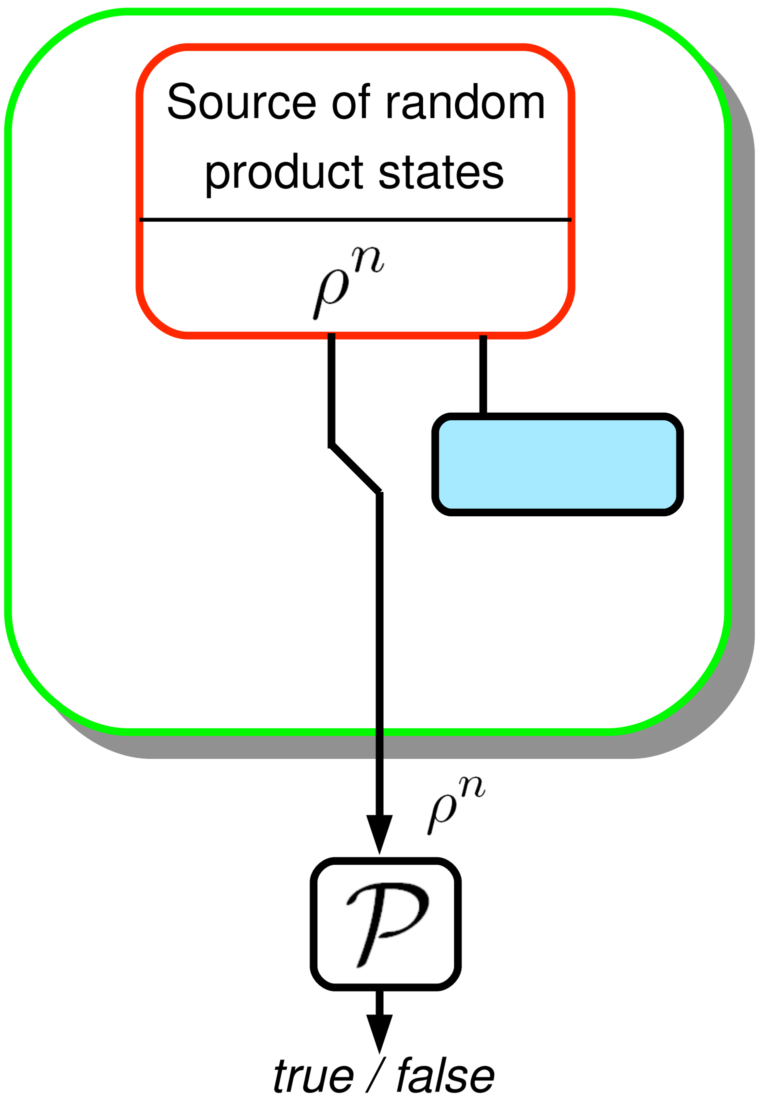
To prove: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$



Output of **green** box: $\rho^n := \int \sigma^{\otimes n} \mu(\sigma)$

How the Post-Selection Technique Works

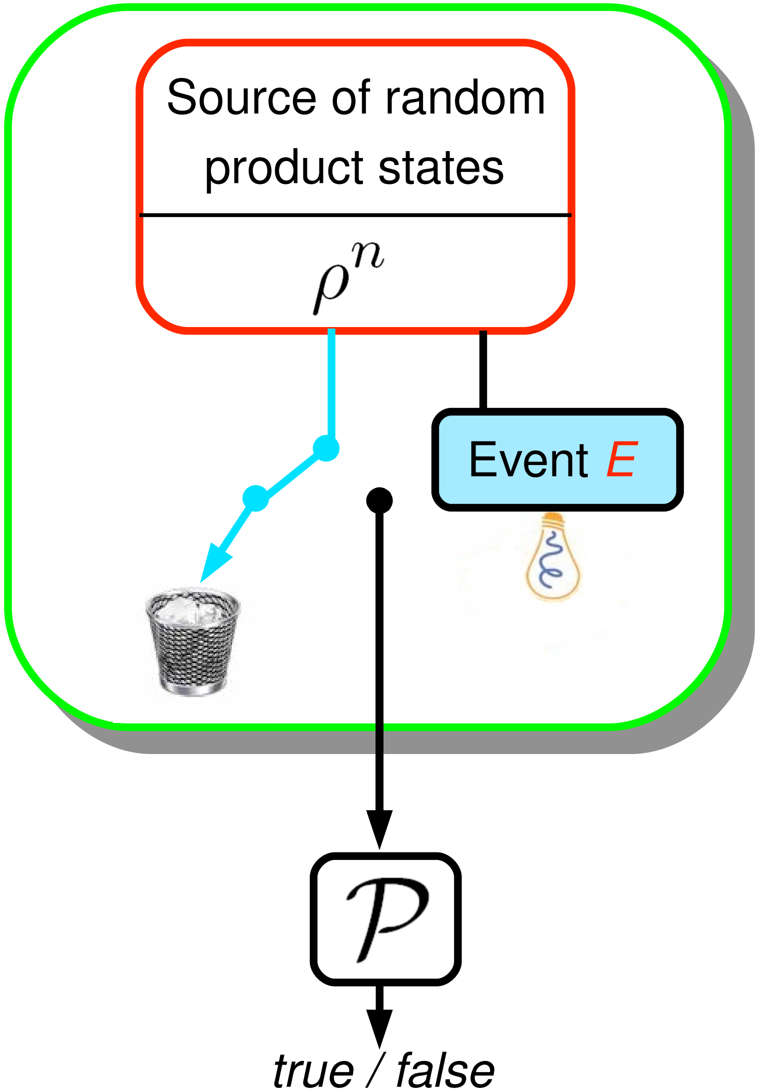
To prove: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$



Output of **green** + **red** box: $\rho^n := \int \sigma^{\otimes n} \mu(\sigma)$

How the Post-Selection Technique Works

To prove: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$



Output of **red** box: $\rho^n := \int \sigma^{\otimes n} \mu(\sigma)$

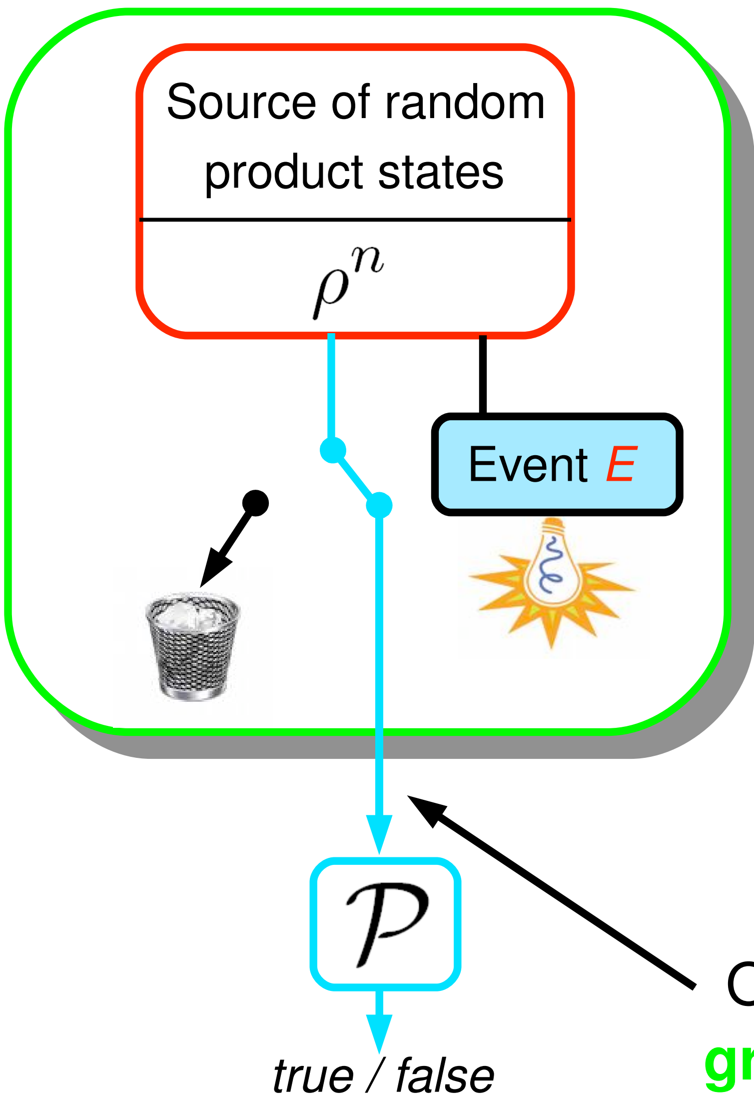
Perform measurement inside the event box:

1. if event *E* does not occur then
   $\Rightarrow$ switch turns to the left

2. if event *E* occurs then
   $\Rightarrow$ switch turns to the right

How the Post-Selection Technique Works

<u>To prove</u>: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$



Output of **red** box: $\rho^n := \int \sigma^{\otimes n} \mu(\sigma)$

<u>Perform measurement inside the event box:</u>

1. if event E does not occur then
   $\Rightarrow$ switch turns to the left

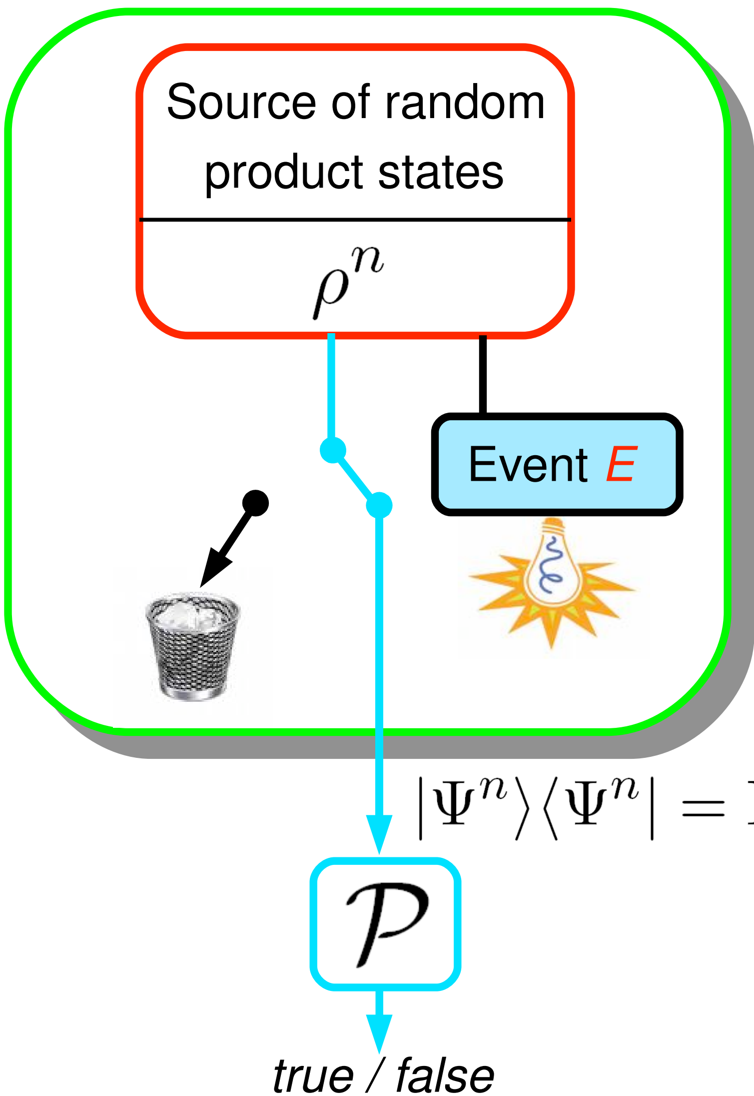
2. if event E occurs then
   $\Rightarrow$ switch turns to the right

Output of **green** box $= \Pr[E]^{-1} \cdot \mathrm{Tr}_{R^n}\left((id_{\mathcal{H}^n} \otimes E_{R^n})\rho_{\mathcal{H}^n R^n}\right)$

How the Post-Selection Technique Works

<u>To prove</u>: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$

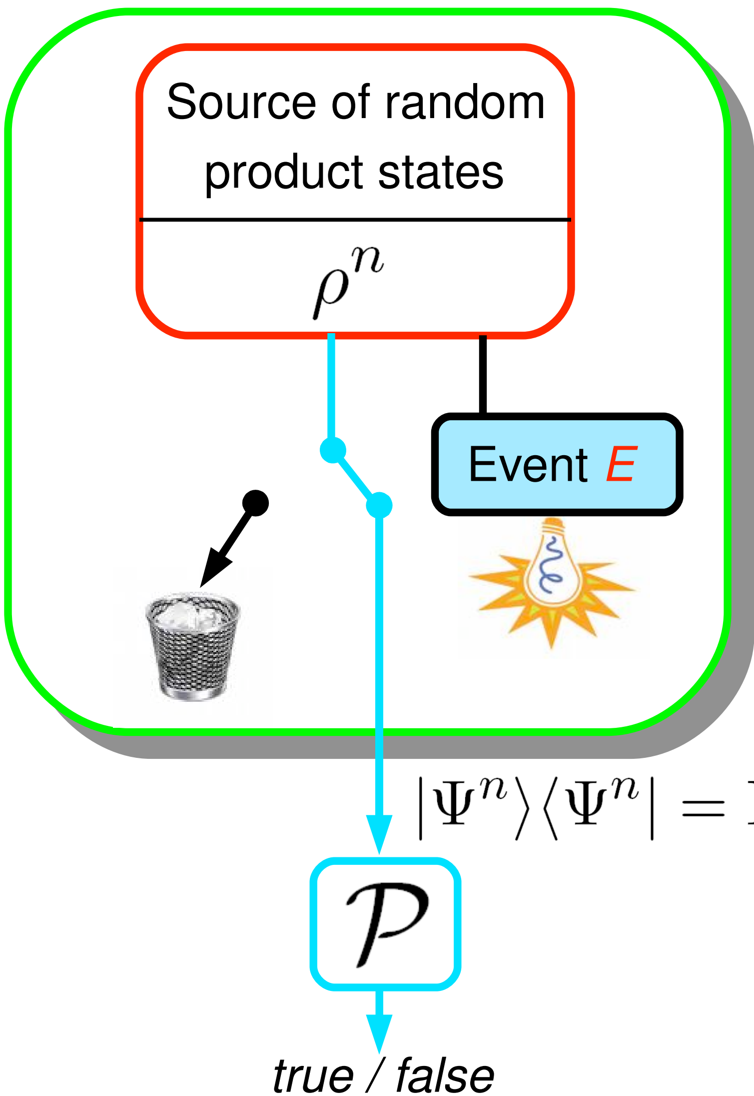
<u>Lemma</u>: There exists a measurement such that if event *E* occurs, the input to $\mathcal{P}$ is $|\Psi^n\rangle$ and $\Pr[E] > 1/poly(n)$



$$|\Psi^n\rangle\langle\Psi^n| = \Pr[E]^{-1} \cdot \mathrm{Tr}_{R^n}\left((id_{\mathcal{H}^n} \otimes E_{R^n})\rho_{\mathcal{H}^n R^n}\right)$$

How the Post-Selection Technique Works

<u>To prove</u>: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$



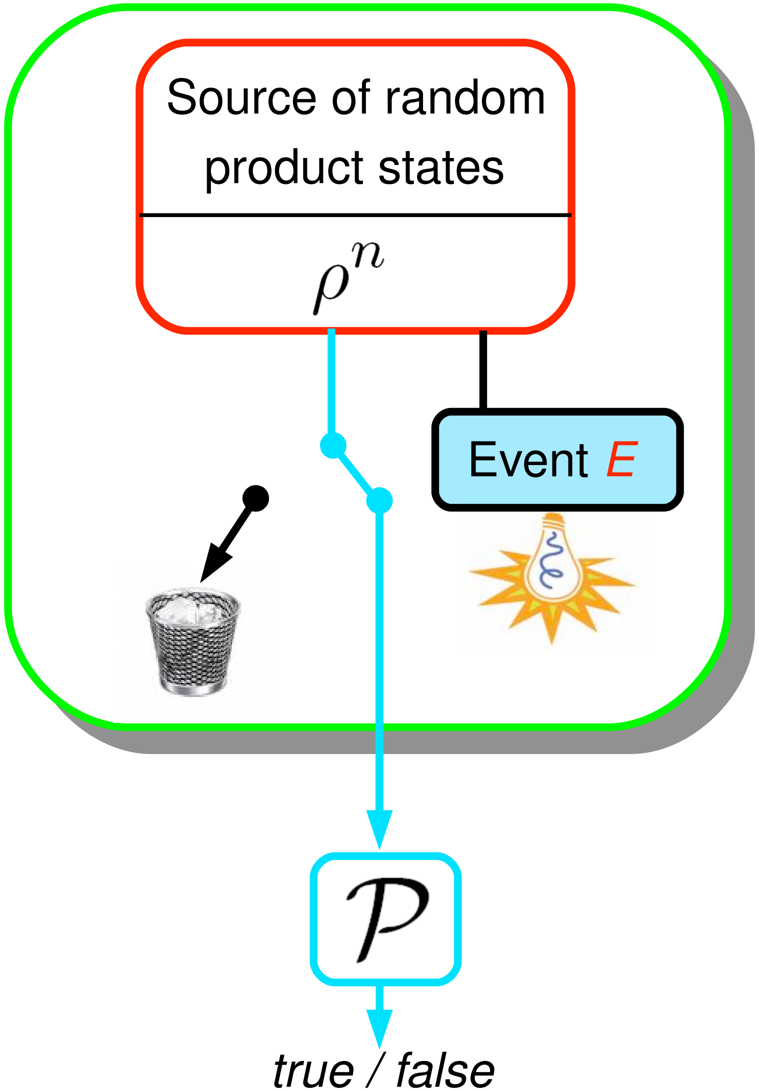
<u>Lemma</u>: There exists a measurement such that if event E occurs, the input to $\mathcal{P}$ is $|\Psi^n\rangle$ and $\Pr[E] > 1/poly(n)$

<u>Remark</u>: The polynomial factor depends on the dimension of the Hilbert space, i.e., $poly(n) \sim n^{\dim(\mathcal{H})}$

$$|\Psi^n\rangle\langle\Psi^n| = \Pr[E]^{-1} \cdot \mathrm{Tr}_{R^n}\left((id_{\mathcal{H}^n} \otimes E_{R^n})\rho_{\mathcal{H}^n R^n}\right)$$

How the Post-Selection Technique Works

To prove: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$

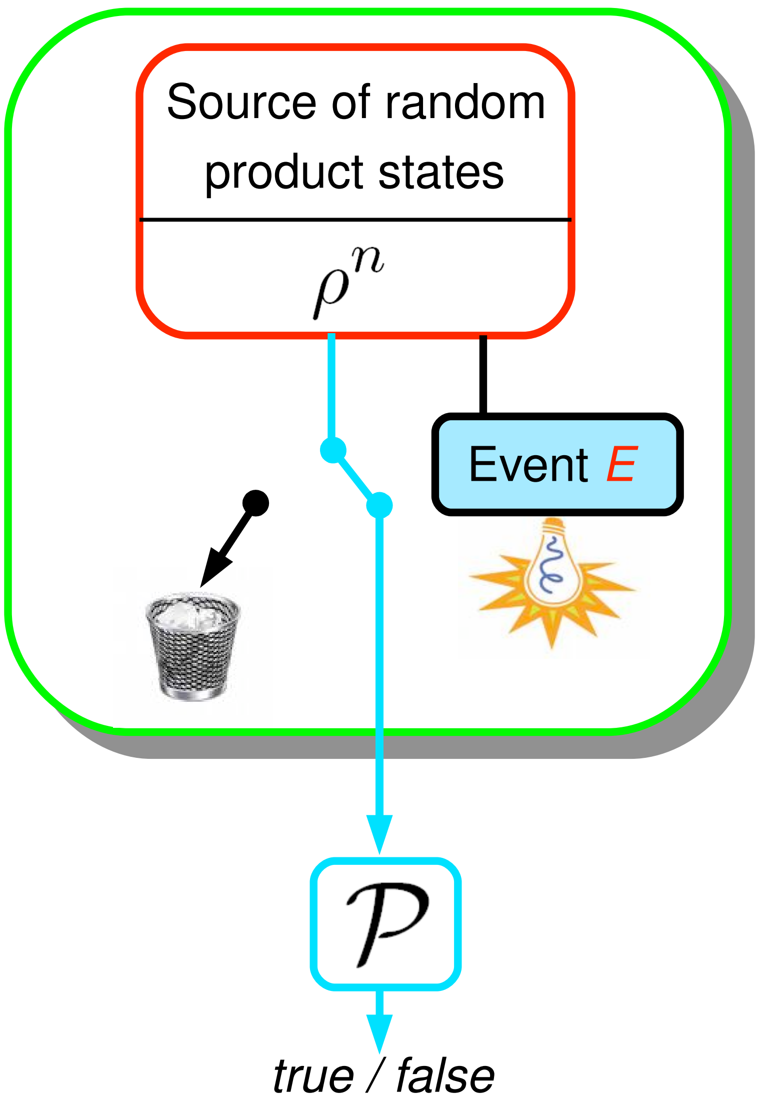


Lemma: There exists a measurement such that if event *E* occurs, the input to $\mathcal{P}$ is $|\Psi^n\rangle$ and $\Pr[E] > 1/poly(n)$

$$\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] = \Pr[\mathcal{P}(\rho^n) = true|E]$$

How the Post-Selection Technique Works

To prove: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$



Lemma: There exists a measurement such that if event E occurs, the input to $\mathcal{P}$ is $|\Psi^n\rangle$ and $\Pr[E] > 1/poly(n)$

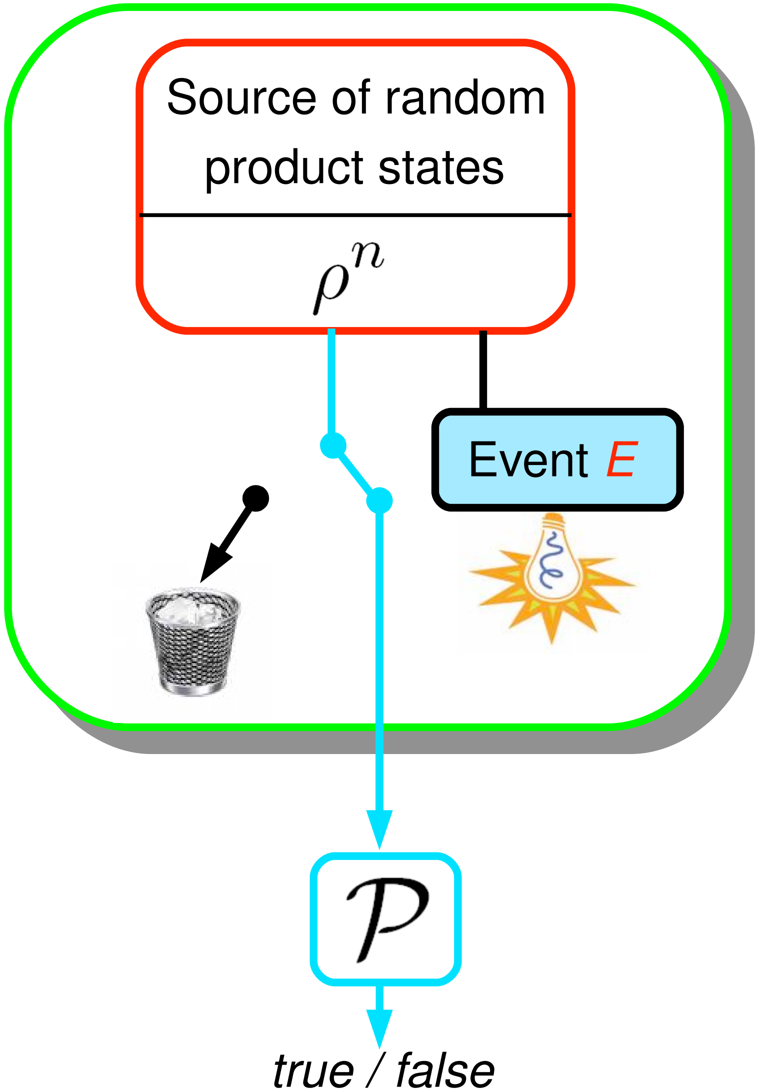
.

$$\begin{aligned} \Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] &= \Pr[\mathcal{P}(\rho^n) = true|E] \\ &\leq \Pr[\mathcal{P}(\sigma^{\otimes n}) = true|E] \end{aligned}$$

$$\rho^n := \int \sigma^{\otimes n} \mu(\sigma)$$

How the Post-Selection Technique Works

<u>To prove</u>: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$



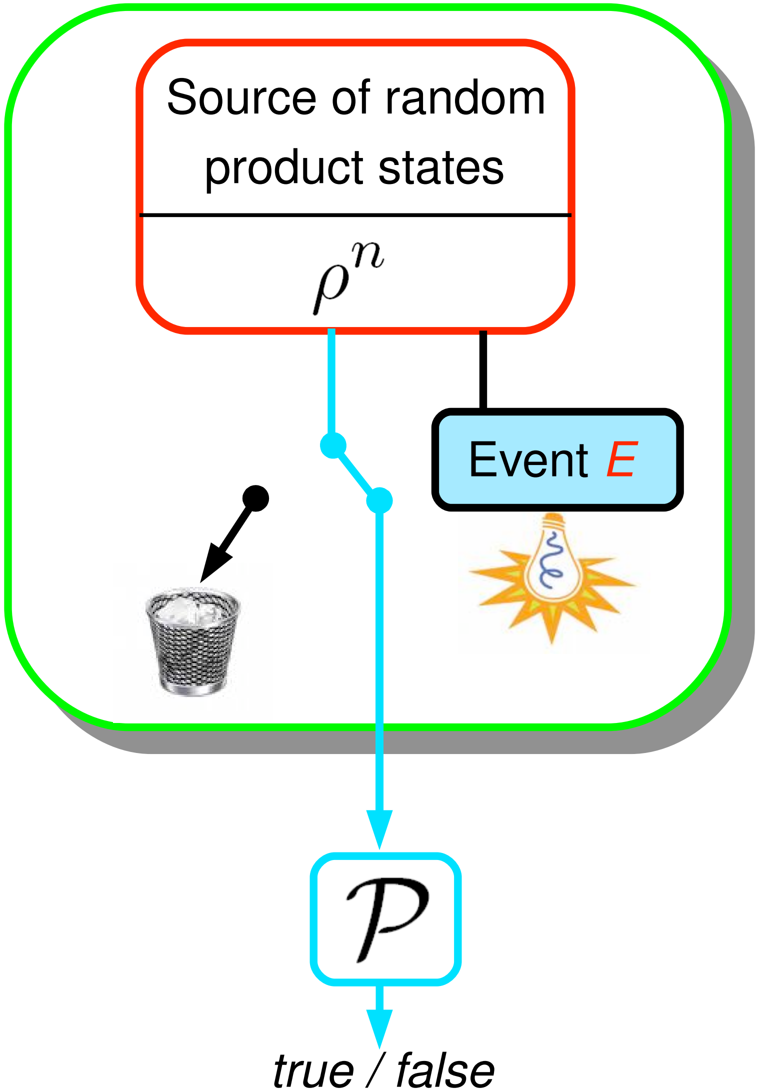
<u>Lemma</u>: There exists a measurement such that if event *E* occurs, the input to $\mathcal{P}$ is $|\Psi^n\rangle$ and $\Pr[E] > 1/poly(n)$

.

$$\begin{aligned}
\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] &= \Pr[\mathcal{P}(\rho^n) = true|E] \\
&\leq \Pr[\mathcal{P}(\sigma^{\otimes n}) = true|E] \\
&= \frac{1}{\Pr[E]} \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true \wedge E] \\
&\leq \frac{1}{\Pr[E]} \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]
\end{aligned}$$

How the Post-Selection Technique Works

<u>To prove</u>: $\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] \leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]$



<u>Lemma</u>: There exists a measurement such that if event E occurs, the input to $\mathcal{P}$ is $|\Psi^n\rangle$ and $\Pr[E] > 1/poly(n)$

.

$$
\begin{aligned}
\Pr[\mathcal{P}(|\Psi^n\rangle\langle\Psi^n|) = true] &= \Pr[\mathcal{P}(\rho^n) = true|E] \\
&\leq \Pr[\mathcal{P}(\sigma^{\otimes n}) = true|E] \\
&= \frac{1}{\Pr[E]} \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true \wedge E] \\
&\leq \frac{1}{\Pr[E]} \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true] \\
&\leq poly(n) \cdot \Pr[\mathcal{P}(\sigma^{\otimes n}) = true]
\end{aligned}
$$

Lemma

Conclusions and Open Problems

- Proving upper bound for product states gives upper bound for symmetric states (only polynomially worse)
- Easier to handle than exponential de Finetti theorem
- Gives better bounds

- Simplification for general parallel repetition problems?
- How to generalize the technique to infinite dimensional systems?

Any Questions?

For more information see: arXiv:0809.3019 (Phys. Rev. Lett. 102, 020504 (2009))