Security of differential phase shift QKD from relativistic principles

Martin Sandfuchs [1] Marcus Haberland [1,2] V. Vilasini [1]
Ramona Wolf [1]

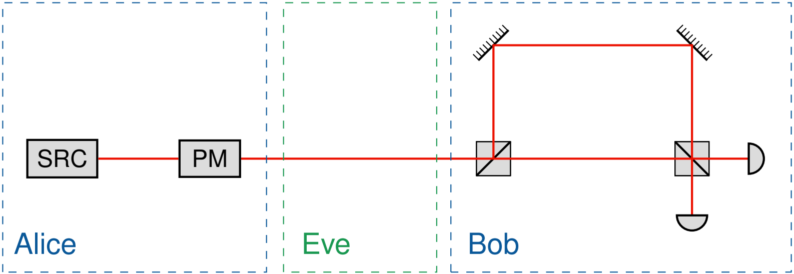
[1]Institute for Theoretical Physics, ETH Zürich, Wolfgang-Pauli-Str. 27, 8093 Zürich, Switzerland

[2]Max Planck Institute for Gravitational Physics (Albert Einstein Institute), Am Mühlenberg 1, 14476 Potsdam, Germany

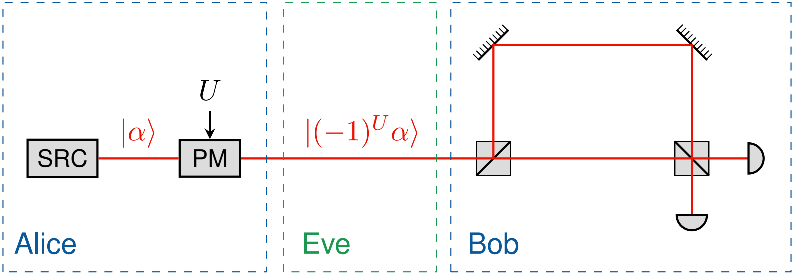
August 15, 2023

Setup

Differential phase shift (DPS) QKD

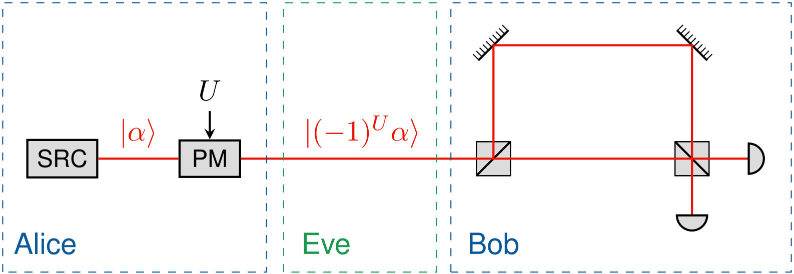


Differential phase shift (DPS) QKD



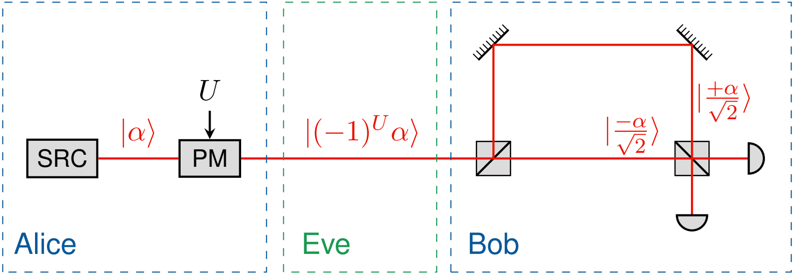
- Alice chooses a random bit U and encodes it in the phase of a coherent state.

Differential phase shift (DPS) QKD



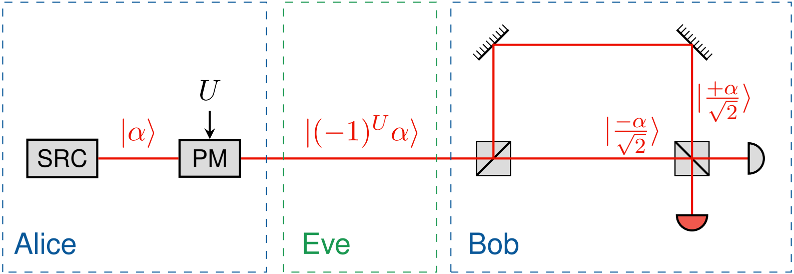
- Alice chooses a random bit U and encodes it in the phase of a coherent state.
- Bob measures the relative phase between consecutive pulses.

Differential phase shift (DPS) QKD



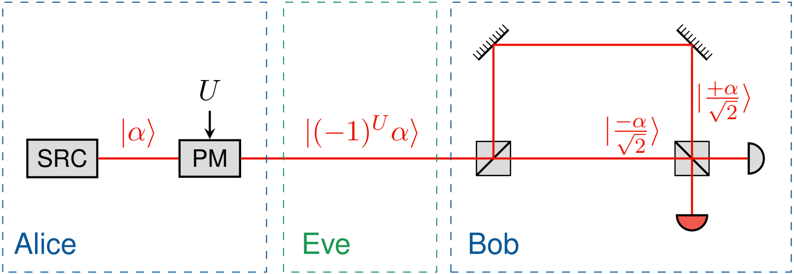
- Alice chooses a random bit U and encodes it in the phase of a coherent state.
- Bob measures the relative phase between consecutive pulses.

Differential phase shift (DPS) QKD



- Alice chooses a random bit U and encodes it in the phase of a coherent state.
- Bob measures the relative phase between consecutive pulses.

Differential phase shift (DPS) QKD



- Alice chooses a random bit U and encodes it in the phase of a coherent state.
- Bob measures the relative phase between consecutive pulses.
- If they see too many errors, they abort the protocol.

The goal of a QKD security proof is to show the following statement:

$$\rho_{K^l E} \approx_\delta \frac{\mathbb{1}_{K^l}}{2^l} \otimes \rho_E .$$

The goal of a QKD security proof is to show the following statement:

$$\rho_{K^l E} \approx_\delta \frac{\mathbb{1}_{K^l}}{2^l} \otimes \rho_E.$$

Using the *leftover hashing lemma*:

$$\delta \lesssim 2^{-\frac{1}{2}\left(H_{\min}^{\varepsilon}(X^n|E)-l\right)}.$$

The goal of a QKD security proof is to show the following statement:

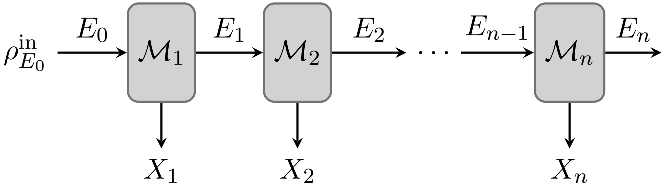
$$\rho_{K^l E} \approx_\delta \frac{\mathbb{1}_{K^l}}{2^l} \otimes \rho_E .$$

Using the *leftover hashing lemma*:

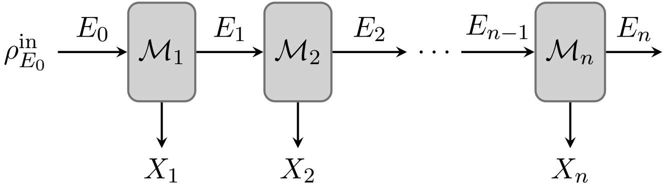
$$\delta \lesssim 2^{-\frac{1}{2}\left(H_{\min}^{\varepsilon}(X^n|E)-l\right)}.$$

$\Rightarrow$ We need a lower-bound on $H_{\min}^{\varepsilon}(X^n|E)$.

This can be achieved by the generalized entropy accumulation theorem (GEAT).



This can be achieved by the generalized entropy accumulation theorem (GEAT).

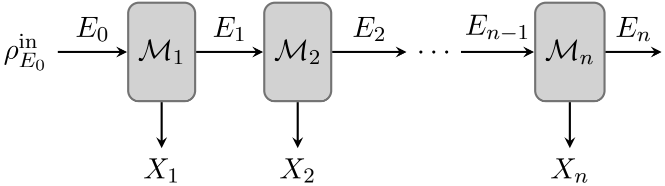


The GEAT provides the bound:

$$H^{\varepsilon}_{\min}(X^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho^{\mathrm{in}})} \geq nh - \mathcal{O}(\sqrt{n}),$$

where h is the single-round von Neumann entropy.

This can be achieved by the generalized entropy accumulation theorem (GEAT).



The GEAT provides the bound:

$$H^{\varepsilon}_{\min}(X^n|E_n)_{\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1(\rho^{\mathrm{in}})} \geq nh - \mathcal{O}(\sqrt{n}),$$

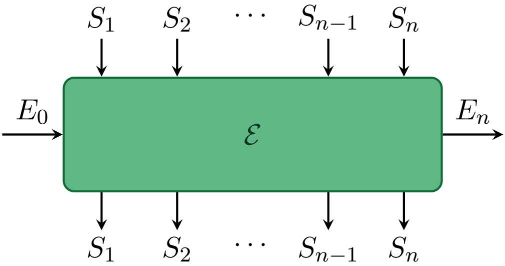
where h is the single-round von Neumann entropy.

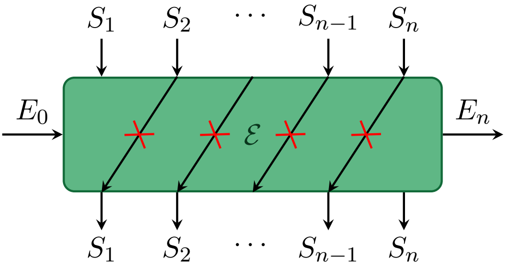
Core questions:

Q1 What are $\mathcal{M}_1, \ldots, \mathcal{M}_n$?

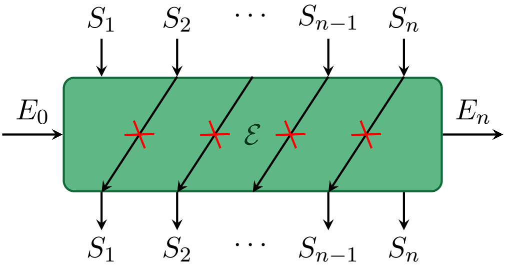
Q2 How to compute h?

Q1 What are the channels?

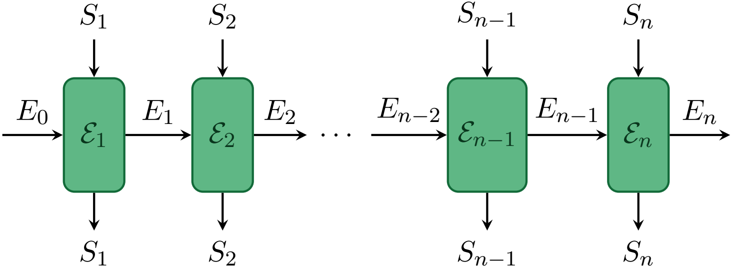

S_1 S_2 $\cdots$ S_{n-1} S_n
E_0
$\mathcal{E}$
E_n
S_1 S_2 $\cdots$ S_{n-1} S_n

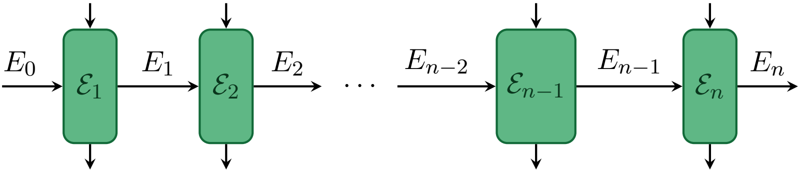


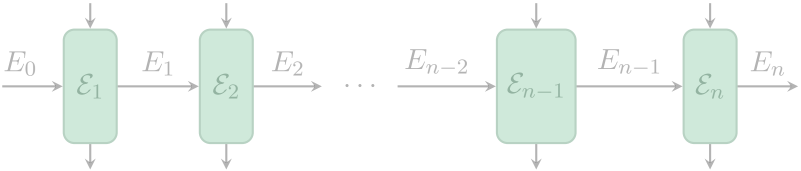
Condition: Eve does not signal from round $i+1$ to round i.



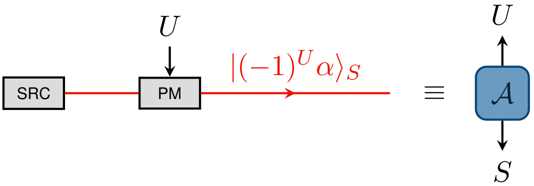
Condition: Eve does not signal from round $i+1$ to round i. Then:



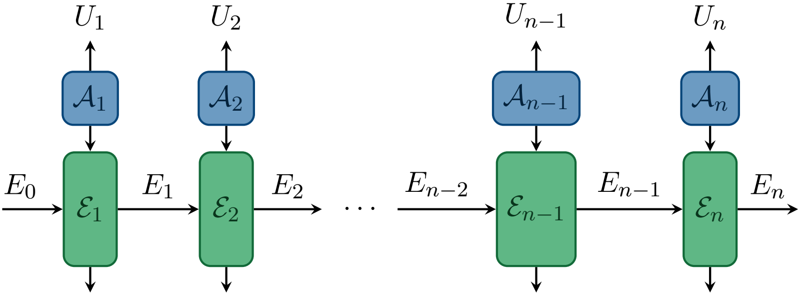

E_0
$\mathcal{E}_1$
E_1
$\mathcal{E}_2$
E_2
$\cdots$
E_{n-2}
$\mathcal{E}_{n-1}$
E_{n-1}
$\mathcal{E}_n$
E_n



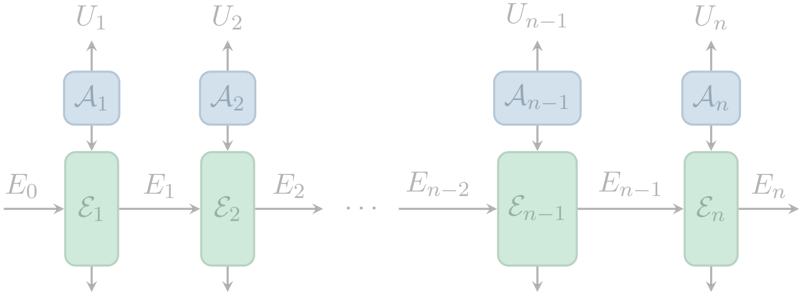
E_0
$\mathcal{E}_1$
E_1
$\mathcal{E}_2$
E_2
$\cdots$
E_{n-2}
$\mathcal{E}_{n-1}$
E_{n-1}
$\mathcal{E}_n$
E_n



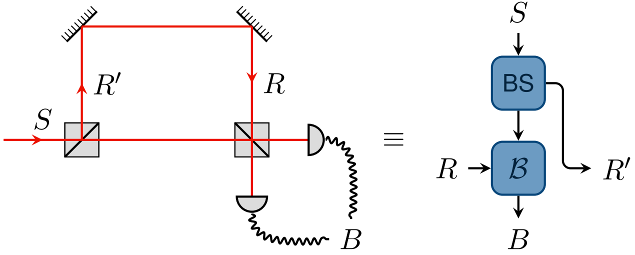
SRC
PM
U
$|(-1)^U \alpha\rangle_S$
$\equiv$
$\mathcal{A}$
U
S



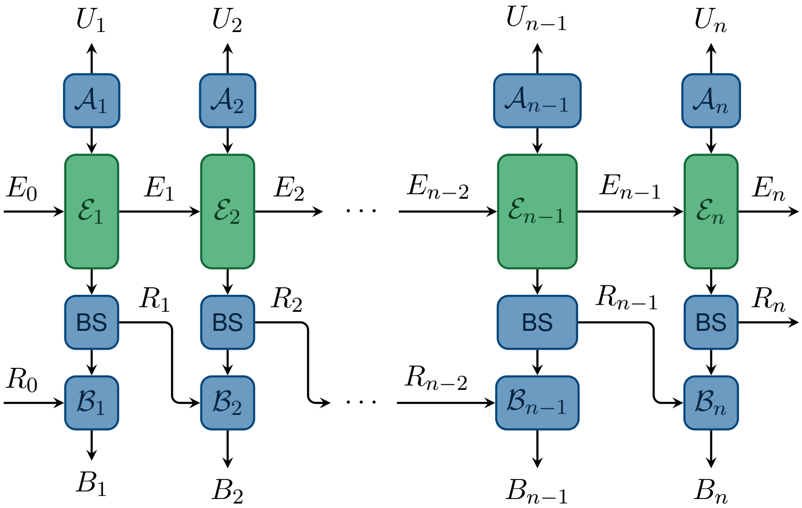
U_1
U_2
U_{n-1}
U_n
$\mathcal{A}_1$
$\mathcal{A}_2$
$\mathcal{A}_{n-1}$
$\mathcal{A}_n$
E_0
$\mathcal{E}_1$
E_1
$\mathcal{E}_2$
E_2
$\cdots$
E_{n-2}
$\mathcal{E}_{n-1}$
E_{n-1}
$\mathcal{E}_n$
E_n

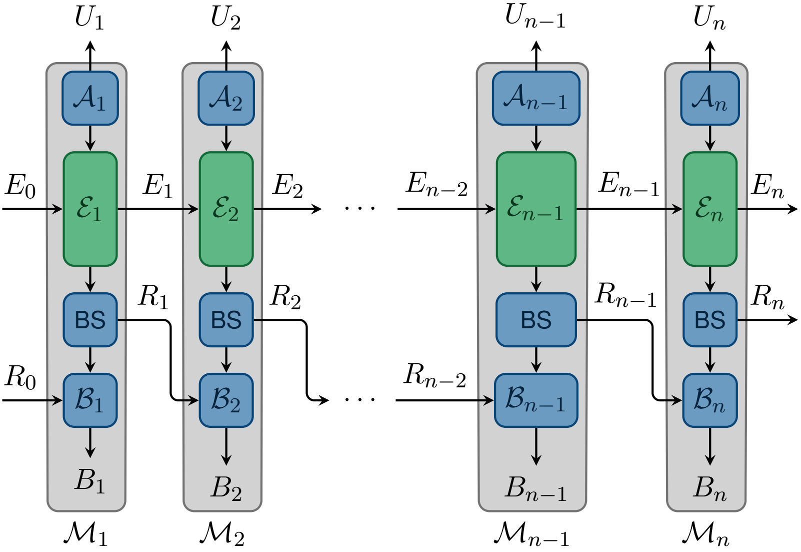


U_1
U_2
U_{n-1}
U_n
$\mathcal{A}_1$
$\mathcal{A}_2$
$\mathcal{A}_{n-1}$
$\mathcal{A}_n$
E_0
$\mathcal{E}_1$
E_1
$\mathcal{E}_2$
E_2
$\cdots$
E_{n-2}
$\mathcal{E}_{n-1}$
E_{n-1}
$\mathcal{E}_n$
E_n



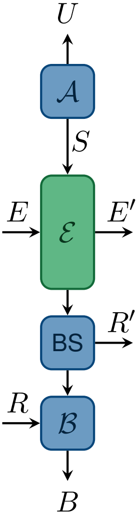
R'
R
S
B
$\equiv$
S
BS
R
$\mathcal{B}$
R'
B


U_1
U_2
U_{n-1}
U_n
$\mathcal{A}_1$
$\mathcal{A}_2$
$\mathcal{A}_{n-1}$
$\mathcal{A}_n$
E_0
$\mathcal{E}_1$
E_1
$\mathcal{E}_2$
E_2
$\cdots$
E_{n-2}
$\mathcal{E}_{n-1}$
E_{n-1}
$\mathcal{E}_n$
E_n
BS
R_1
BS
R_2
BS
R_{n-1}
BS
R_n
R_0
$\mathcal{B}_1$
$\mathcal{B}_2$
$\cdots$
R_{n-2}
$\mathcal{B}_{n-1}$
$\mathcal{B}_n$
B_1
B_2
B_{n-1}
B_n

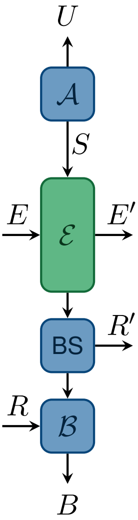


To apply the GEAT we identify: $E_i R_i \to E_i$.

Q2 How to compute the single-round entropy?



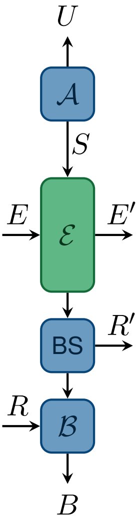
U
𝒜
S
E
ℰ
E′
BS
R′
R
ℬ
B



We work in an entanglement-based picture: Instead of Alice sending $|\pm\alpha\rangle_S$ she sends half of an entangled state:

$$|\psi\rangle_{US} = \frac{1}{\sqrt{2}}|0\rangle_U \otimes |+\alpha\rangle_S + \frac{1}{\sqrt{2}}|1\rangle_U \otimes |-\alpha\rangle_S,$$

and measures U locally to obtain her key bit.

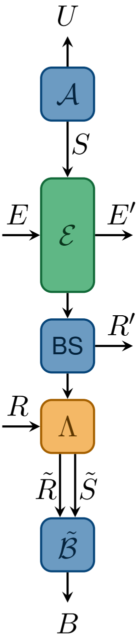


We work in an entanglement-based picture: Instead of Alice sending $|\pm\alpha\rangle_S$ she sends half of an entangled state:

$$|\psi\rangle_{US} = \frac{1}{\sqrt{2}}|0\rangle_U \otimes |+\alpha\rangle_S + \frac{1}{\sqrt{2}}|1\rangle_U \otimes |-\alpha\rangle_S,$$

and measures U locally to obtain her key bit.

Bob receives a state ρ_{SR} from Eve and performs the phase coherence measurement discussed previously.

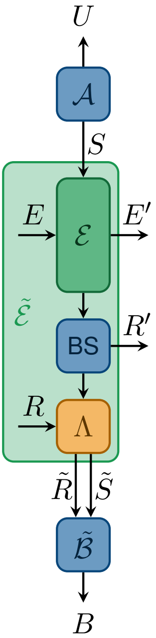


We work in an entanglement-based picture: Instead of Alice sending $|\pm\alpha\rangle_S$ she sends half of an entangled state:

$$|\psi\rangle_{US} = \frac{1}{\sqrt{2}}|0\rangle_U \otimes |+\alpha\rangle_S + \frac{1}{\sqrt{2}}|1\rangle_U \otimes |-\alpha\rangle_S,$$

and measures U locally to obtain her key bit.

Bob receives a state ρ_{SR} from Eve and performs the phase coherence measurement discussed previously.



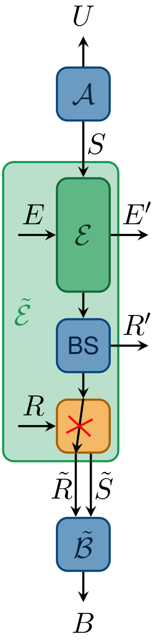
We work in an entanglement-based picture: Instead of Alice sending $|\pm\alpha\rangle_S$ she sends half of an entangled state:

$$|\psi\rangle_{US} = \frac{1}{\sqrt{2}}|0\rangle_U \otimes |+\alpha\rangle_S + \frac{1}{\sqrt{2}}|1\rangle_U \otimes |-\alpha\rangle_S,$$

and measures U locally to obtain her key bit.

Bob receives a state ρ_{SR} from Eve and performs the phase coherence measurement discussed previously.

Due to the squashing, we can assume that Eve's attack produces qubits.



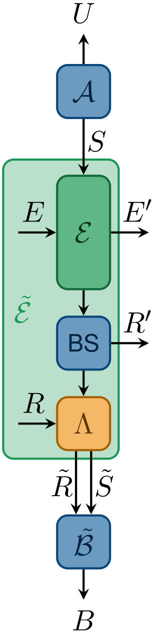
We work in an entanglement-based picture: Instead of Alice sending $|\pm\alpha\rangle_S$ she sends half of an entangled state:

$$|\psi\rangle_{US} = \frac{1}{\sqrt{2}}|0\rangle_U \otimes |+\alpha\rangle_S + \frac{1}{\sqrt{2}}|1\rangle_U \otimes |-\alpha\rangle_S,$$

and measures U locally to obtain her key bit.

Bob receives a state ρ_{SR} from Eve and performs the phase coherence measurement discussed previously.

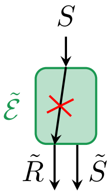
Due to the squashing, we can assume that Eve's attack produces qubits.



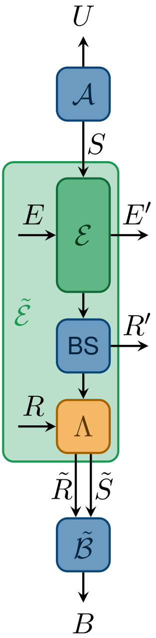
$\Rightarrow$ Optimize over all attack channels:

$$h = \inf_{\tilde{\mathcal{E}}} H(U|E'R')_{\nu(\tilde{\mathcal{E}})}$$
$$\text{s.t.} \quad \mathrm{tr}[\Gamma^{(i)}\nu] = \gamma^{(i)},$$

where the optimization is over all maps



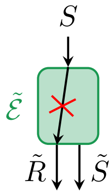
and $\nu(\tilde{\mathcal{E}})$ is the state after Alice and Bob measure $(\mathcal{I}_U \otimes \tilde{\mathcal{E}})(|\psi\rangle\langle\psi|_{US})$.



$\Rightarrow$ Optimize over all attack channels:

$$h = \inf_{\tilde{\mathcal{E}}} H(U|E'R')_{\nu(\tilde{\mathcal{E}})}$$
$$\text{s.t.} \quad \mathrm{tr}[\Gamma^{(i)}\nu] = \gamma^{(i)},$$

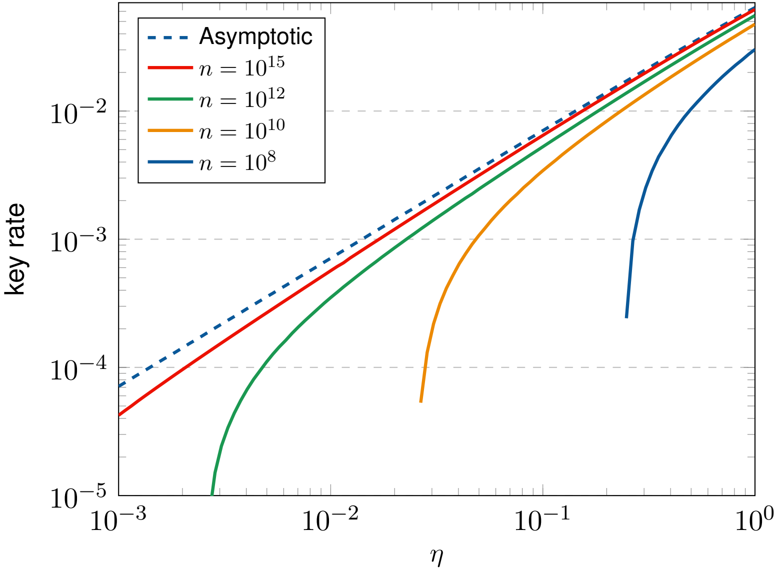
where the optimization is over all maps



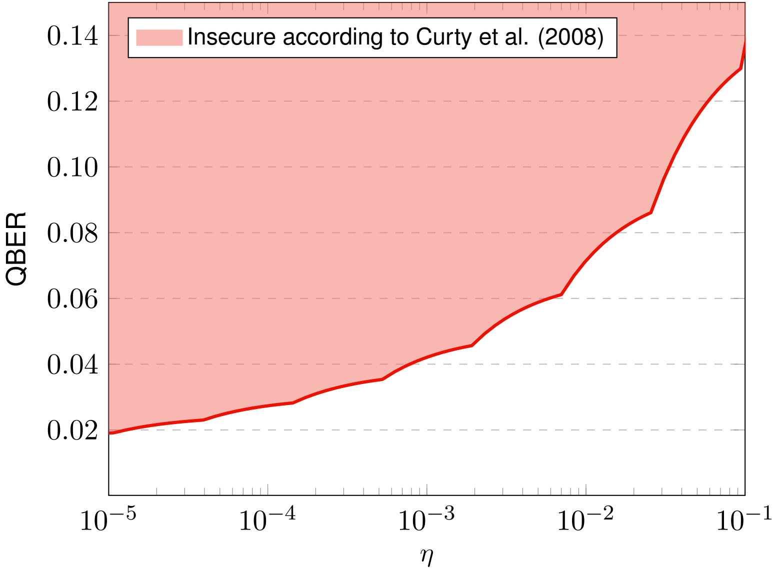
and $\nu(\tilde{\mathcal{E}})$ is the state after Alice and Bob measure $(\mathcal{I}_U \otimes \tilde{\mathcal{E}})(|\psi\rangle\langle\psi|_{US})$.

Can be solved using known optimization techniques.

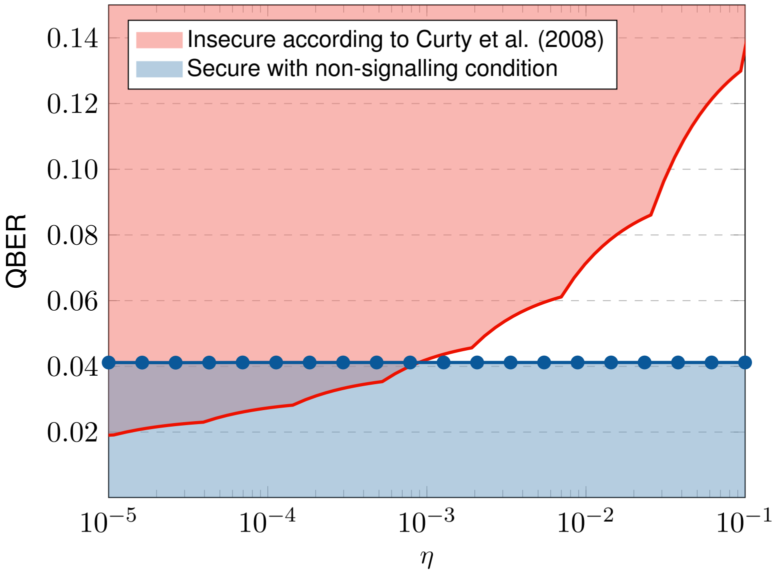
Results and Discussion



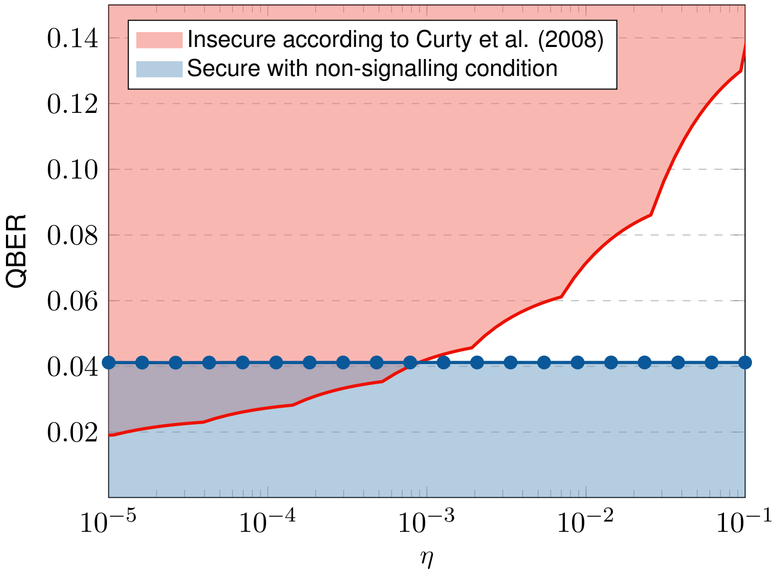
Asymptotic
$n = 10^{15}$
$n = 10^{12}$
$n = 10^{10}$
$n = 10^{8}$
key rate
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-3}
10^{-2}
10^{-1}
10^{0}
η



Insecure according to Curty et al. (2008)
0.14
0.12
0.10
0.08
0.06
0.04
0.02
QBER
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
η



Insecure according to Curty et al. (2008)
Secure with non-signalling condition
QBER
0.14
0.12
0.10
0.08
0.06
0.04
0.02
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
η



Coherent attacks on DPS are stronger than collective attacks!

Conclusion

- It is possible to prove security of the DPS protocol using the generalized entropy accumulation theorem.

- It is possible to prove security of the DPS protocol using the generalized entropy accumulation theorem.
- This requires a non-signalling constraint on Eve's attack.

- It is possible to prove security of the DPS protocol using the generalized entropy accumulation theorem.
- This requires a non-signalling constraint on Eve's attack.
- Tools from causality can be used to define the channels and evaluate single-round entropies.

- It is possible to prove security of the DPS protocol using the generalized entropy accumulation theorem.
- This requires a non-signalling constraint on Eve's attack.
- Tools from causality can be used to define the channels and evaluate single-round entropies.
- A constraint of this form is necessary if one wishes to reduce analysis to collective attacks (as the EAT and many other techniques do).

Q&A