The asymptotic performance of coherent-one-way quantum key distribution

Róbert Trényi and Marcos Curty

Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E36310, Spain

J. González-Payo, R. Trényi, W. Wang, and M. Curty, Phys. Rev. Lett. 125, 260510 (2020)
R. Trényi and M. Curty, arXiv:2101.07192 (2021)

UNIVERSIDADE DE VIGO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662

Why is coherent-one-way (COW) QKD interesting?

Practical issue: perfect single-photon sources are challenging to realize

Why is coherent-one-way (COW) QKD interesting?

Practical issue: perfect single-photon sources are challenging to realize

↓

Phase-randomized weak coherent pulses (WCP) are used

$$\rho = \sum_{n=0}^{\infty} \frac{e^{-\mu}\mu^n}{n!} |n\rangle\langle n|$$ with intensity μ

Why is coherent-one-way (COW) QKD interesting?

Practical issue: perfect single-photon sources are challenging to realize

Phase-randomized weak coherent pulses (WCP) are used

$$\rho = \sum_{n=0}^{\infty} \frac{e^{-\mu}\mu^n}{n!} |n\rangle\langle n|$$ with intensity μ

Photon number splitting (PNS) attack seriously limits performance due to multi-photon components

Why is coherent-one-way (COW) QKD interesting?

Practical issue: perfect single-photon sources are challenging to realize

Phase-randomized weak coherent pulses (WCP) are used

$$\rho = \sum_{n=0}^{\infty} \frac{e^{-\mu}\mu^n}{n!} |n\rangle\langle n|$$ with intensity μ

Photon number splitting (PNS) attack seriously limits performance due to multi-photon components

Example: BB84 with WCPs → Secret key rate scaling $\mathcal{O}(\eta^2)$

H. Inamori et al, The European Physical Journal D 41, 3 (2007)

Why is coherent-one-way (COW) QKD interesting?

Possible solutions against the PNS attack:

- Decoy-state QKD *W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005)*
  - Different intensity settings for the WCPs
  - Achievable $\mathcal{O}(\eta)$ scaling

Why is coherent-one-way (COW) QKD interesting?

Possible solutions against the PNS attack:

- Decoy-state QKD *W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005)*
    - Different intensity settings for the WCPs
    - Achievable $\mathcal{O}(\eta)$ scaling
- Strong reference pulse technique *M. Koashi, Phys. Rev. Lett. 93, 120501 (2004)* *K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, Phys. Rev. A 80, 032302 (2009)*
    - Achievable $\mathcal{O}(\eta)$ scaling

Why is coherent-one-way (COW) QKD interesting?

Possible solutions against the PNS attack:

- Decoy-state QKD *W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005)*
  - Different intensity settings for the WCPs
  - Achievable $\mathcal{O}(\eta)$ scaling
- Strong reference pulse technique *M. Koashi, Phys. Rev. Lett. 93, 120501 (2004)* *K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, Phys. Rev. A 80, 032302 (2009)*
  - Achievable $\mathcal{O}(\eta)$ scaling
- Distributed-phase-reference (DPR) QKD
  - Differential-phase-shift (DPS) *K. Inoue et al, Phys. Rev. Lett. 89, 037902 (2002)*
  - Coherent-one-way (COW) *N. Gisin et al, arXiv quant-ph/0411022 (2004)*

Why is coherent-one-way (COW) QKD interesting?

DPR QKD:

- DPS QKD
  - Information is encoded into the phase difference between coherent pulses
  - Achievable $\mathcal{O}(\eta^{3/2})$ scaling
  - Round-robin DPS QKD $\Rightarrow$ $\mathcal{O}(\eta)$ can almost be reached

T. Sasaki, Y. Yamamoto, and M. Koashi, Nature 509, 475 (2014);

Why is coherent-one-way (COW) QKD interesting?

DPR QKD:

- DPS QKD
  - Information is encoded into the phase difference between coherent pulses
  - Achievable $\mathcal{O}(\eta^{3/2})$ scaling
  - Round-robin DPS QKD ⇨ $\mathcal{O}(\eta)$ can almost be reached

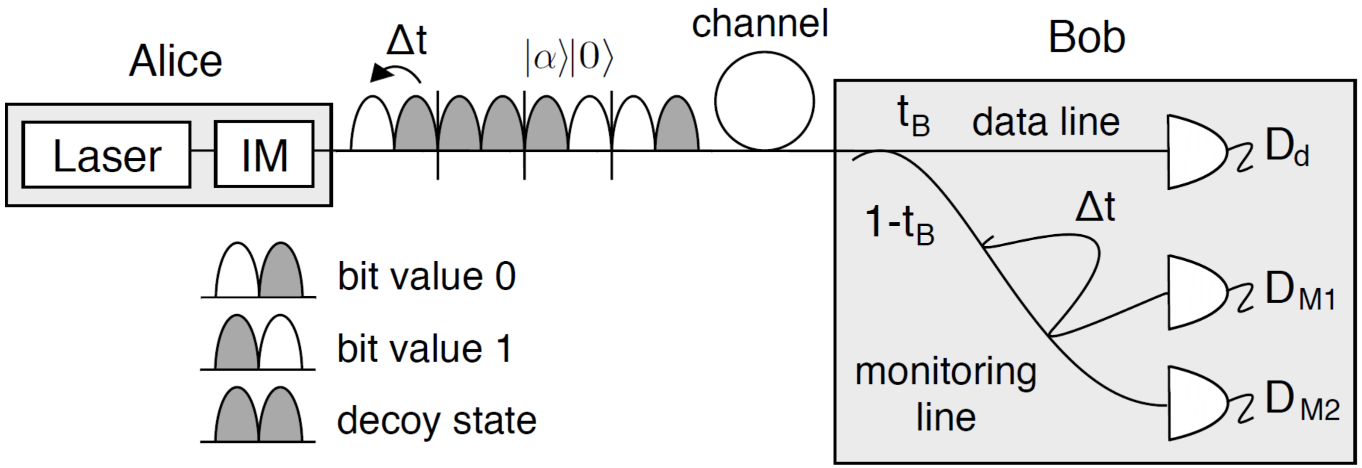
T. Sasaki, Y. Yamamoto, and M. Koashi, Nature 509, 475 (2014);

- COW QKD
  - Encoding is done by combining coherent and/or vacuum pulses
  - Security was not fully established prior to our work
    - upper bound against general attacks $\mathcal{O}(\eta)$
    - lower bound against general attacks $\mathcal{O}(\eta^2)$
    - lower bound against *collective* attacks $\mathcal{O}(\eta)$
  - Is already commercialized and long-distance experiments have been performed

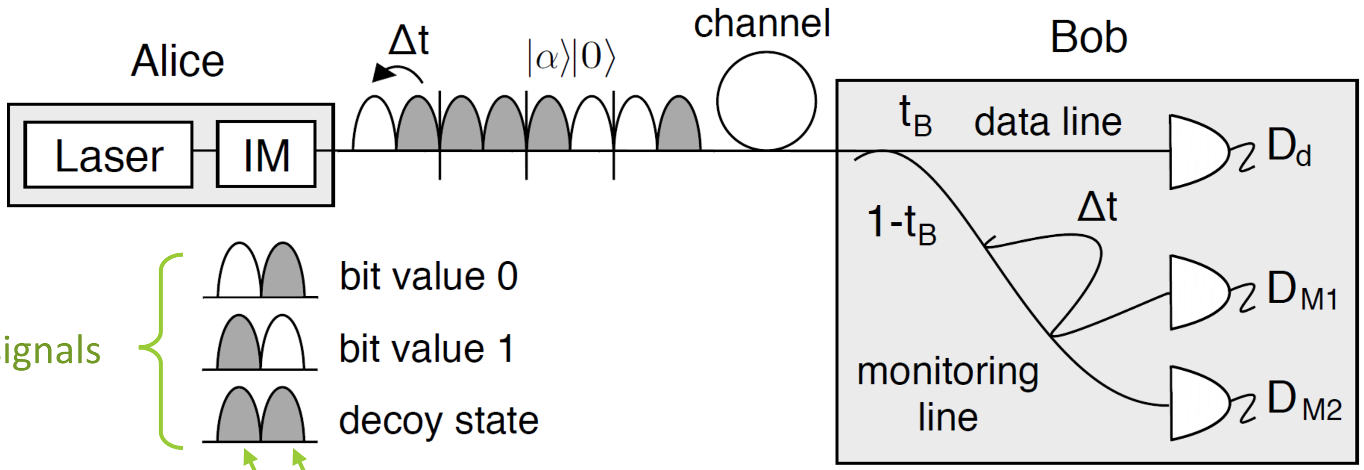
D. Stucki et al, New J. of Phys. 11, 075 003 (2009); B. Korzh et al Nat. Ph. 9, 163-168 (2015)

over 300 km

The COW protocol

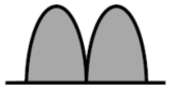


The COW protocol



signals

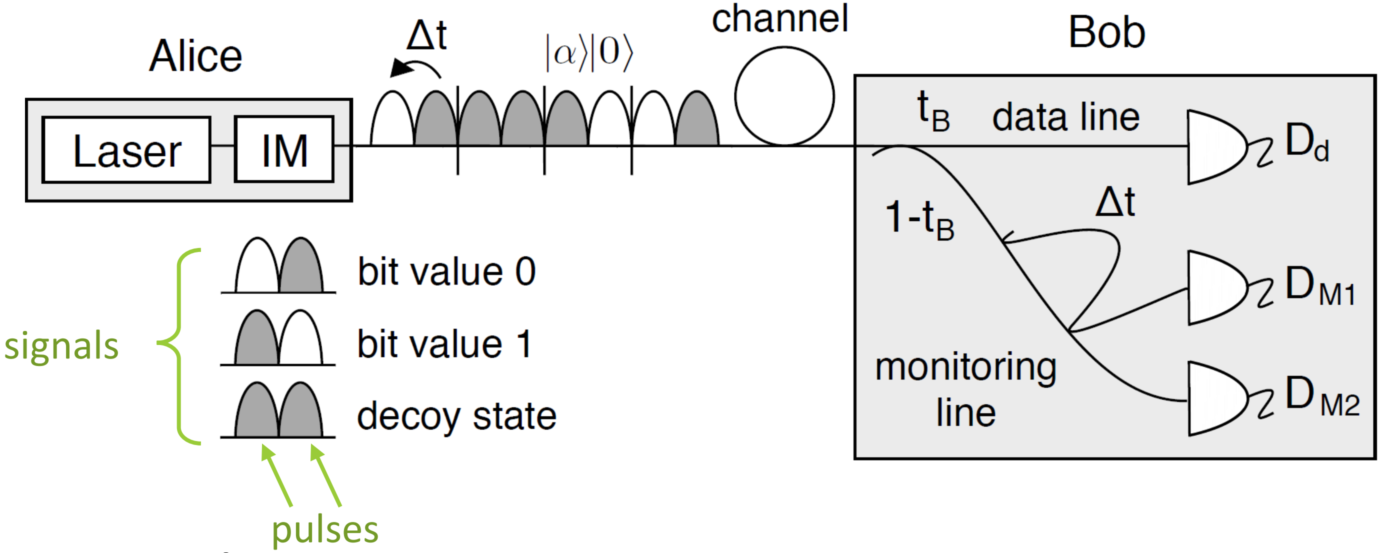
pulses

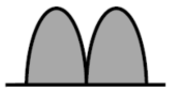


For two subsequent coherent *pulses*

D_{M2} *never* clicks

The COW protocol





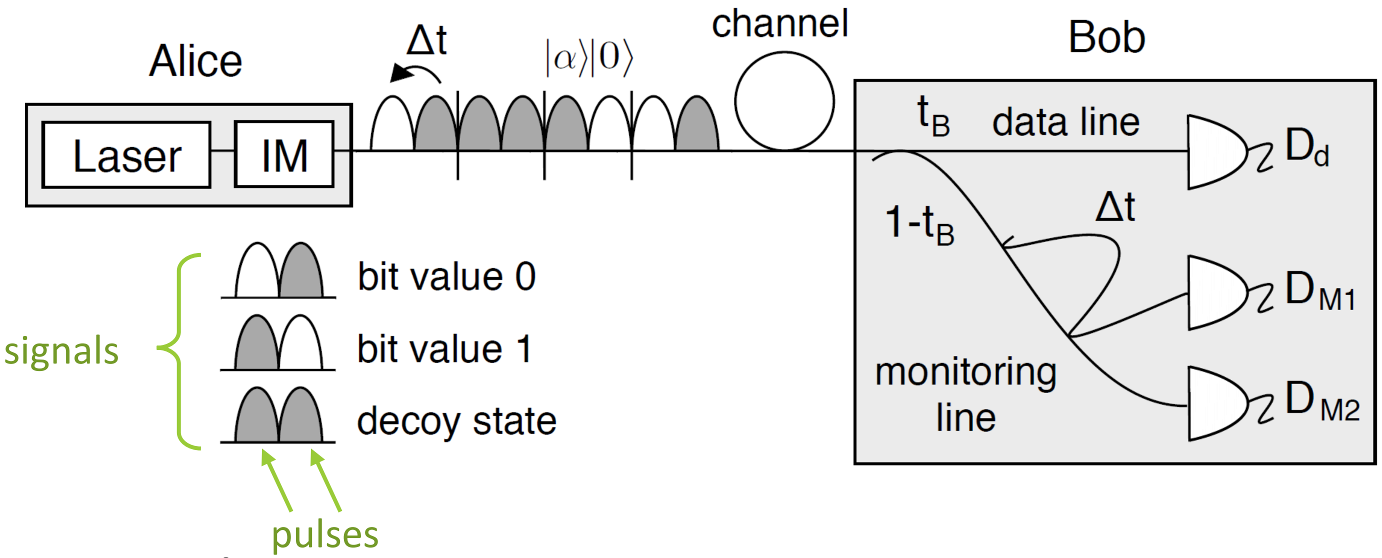
For two subsequent coherent *pulses*

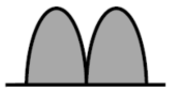
D_{M2} *never* clicks

Monitored quantities:

- Quantum bit error rate (QBER)
- Visibilities $V_s = \frac{p(\mathrm{DM1}|s) - p(\mathrm{DM2}|s)}{p(\mathrm{DM1}|s) + p(\mathrm{DM2}|s)}$ with $s \in \mathcal{S} \equiv \{d, 01, 0d, 1d, dd\}$
- For a certain value of the Gain (probability that Bob observes a detection event per signal)

The COW protocol





For two subsequent coherent *pulses*

D_{M2} *never* clicks

Monitored quantities:

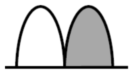
- Quantum bit error rate (QBER)
- Visibilities $V_s = \frac{p(\mathrm{DM1}|s) - p(\mathrm{DM2}|s)}{p(\mathrm{DM1}|s) + p(\mathrm{DM2}|s)}$ with $s \in \mathcal{S} \equiv \{d, 01, 0d, 1d, dd\}$
- For a certain value of the Gain (probability that Bob observes a detection event per signal)

Its secret key rate scales with at most $\mathcal{O}(\eta^2)$

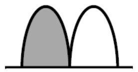
Weak points of the COW

- Linearly independent signal states

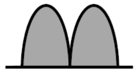
$|0\rangle|\alpha\rangle$

$|\varphi_0\rangle$  bit value 0

$|\alpha\rangle|0\rangle$

$|\varphi_1\rangle$  bit value 1

$|\alpha\rangle|\alpha\rangle$

$|\varphi_2\rangle$  decoy state

$$|\langle\varphi_0|\varphi_1\rangle| = e^{-|\alpha|^2}$$
$$|\langle\varphi_0|\varphi_2\rangle| = e^{-|\alpha|^2/2}$$

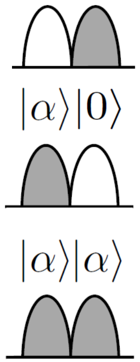
Unambiguous state discrimination (USD)

(Probability of having an inconclusive result $\geq q_{USD}$)

Eve can avoid misidentifying signal states

Weak points of the COW

- Linearly independent signal states



$|\varphi_0\rangle$ bit value 0

$|\varphi_1\rangle$ bit value 1

$|\varphi_2\rangle$ decoy state

$$|\langle\varphi_0|\varphi_1\rangle| = e^{-|\alpha|^2}$$
$$|\langle\varphi_0|\varphi_2\rangle| = e^{-|\alpha|^2/2}$$

Unambiguous state discrimination (USD)

(Probability of having an inconclusive result $\geq q_{USD}$)

Eve can avoid misidentifying signal states

- Vacuum pulses in the signal states inherently break the coherence between the signals

Eve can exploit to have perfect values for the monitored quantities

The sequential attack against the COW

- Eve measures every signal one-by-one using USD

Emitting probability	Alice's signal	E_0	E_1	E_2	E_3
$(1-f)/2$	$\|\varphi_0\rangle$	q_s^s	0	0	q_{inc}^s
$(1-f)/2$	$\|\varphi_1\rangle$	0	q_s^s	0	q_{inc}^s
f	$\|\varphi_2\rangle$	0	0	q_s^d	q_{inc}^d

Eve's POVM elements

H. Sugimoto et al, Phys. Rev. A 82, 032338 (2010)

For given f and α → p_c is maximized

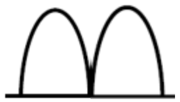
The sequential attack against the COW

- Eve measures every signal one-by-one using USD

Emitting probability	Alice's signal	Eve's POVM elements E_0	E_1	E_2	E_3
$(1-f)/2$	$\lvert\varphi_0\rangle$	$q_{\mathrm{s}}^{\mathrm{s}}$	0	0	$q_{\mathrm{inc}}^{\mathrm{s}}$
$(1-f)/2$	$\lvert\varphi_1\rangle$	0	$q_{\mathrm{s}}^{\mathrm{s}}$	0	$q_{\mathrm{inc}}^{\mathrm{s}}$
f	$\lvert\varphi_2\rangle$	0	0	$q_{\mathrm{s}}^{\mathrm{d}}$	$q_{\mathrm{inc}}^{\mathrm{d}}$

H. Sugimoto et al, Phys. Rev. A 82, 032338 (2010)

→ For given f and α → p_c is maximized

- Inconclusive results → she resends vacuum signals 

The sequential attack against the COW

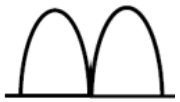
- Eve measures every signal one-by-one using USD

Eve's POVM elements

Emitting probability	Alice's signal	E_0	E_1	E_2	E_3
$(1-f)/2$	$\|\varphi_0\rangle$	q_s^s	0	0	q_{inc}^s
$(1-f)/2$	$\|\varphi_1\rangle$	0	q_s^s	0	q_{inc}^s
f	$\|\varphi_2\rangle$	0	0	q_s^d	q_{inc}^d

H. Sugimoto et al, Phys. Rev. A 82, 032338 (2010)

$\Rightarrow$ For given f and α $\Rightarrow$ p_c is maximized

- Inconclusive results $\Rightarrow$ she resends vacuum signals 
- She collects consecutive conclusive results

The sequential attack against the COW

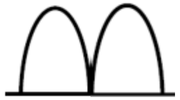
- Eve measures every signal one-by-one using USD

Eve's POVM elements

Emitting probability	Alice's signal	E_0	E_1	E_2	E_3
$(1-f)/2$	$\vert\varphi_0\rangle$	q_s^s	0	0	$q_\mathrm{inc}^\mathrm{s}$
$(1-f)/2$	$\vert\varphi_1\rangle$	0	q_s^s	0	$q_\mathrm{inc}^\mathrm{s}$
f	$\vert\varphi_2\rangle$	0	0	q_s^d	$q_\mathrm{inc}^\mathrm{d}$

H. Sugimoto et al, Phys. Rev. A 82, 032338 (2010)

For given f and α → p_c is maximized

- Inconclusive results → she resends vacuum signals 
- She collects consecutive conclusive results
- Based on these results she prepares new signal states and resends them to Bob

The sequential attack against the COW

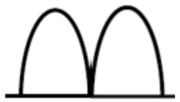
- Eve measures every signal one-by-one using USD

Eve's POVM elements

Emitting probability	Alice's signal	E_0	E_1	E_2	E_3
$(1-f)/2$	$\lvert\varphi_0\rangle$	q_s^s	0	0	q_{inc}^s
$(1-f)/2$	$\lvert\varphi_1\rangle$	0	q_s^s	0	q_{inc}^s
f	$\lvert\varphi_2\rangle$	0	0	q_s^d	q_{inc}^d

H. Sugimoto et al, Phys. Rev. A 82, 032338 (2010)

For given f and α → p_c is maximized

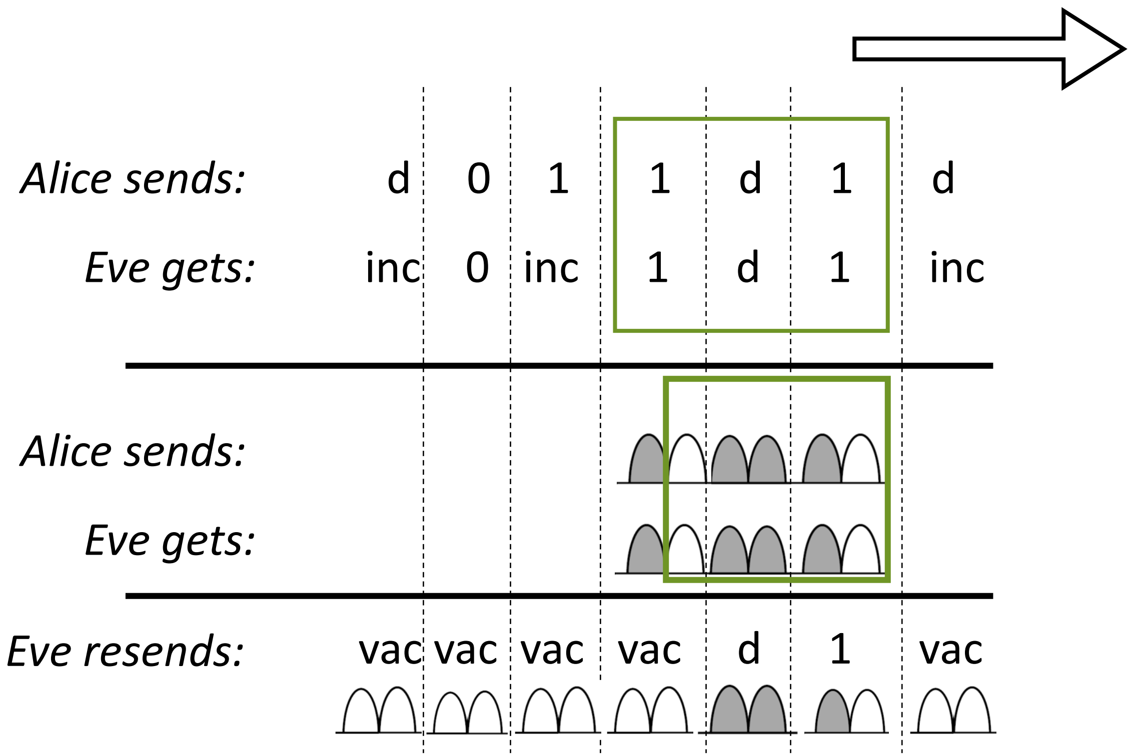
- Inconclusive results → she resends vacuum signals 
- She collects consecutive conclusive results
- Based on these results she prepares new signal states and resends them to Bob
- Intercept-resend type of attack → entanglement breaking channel

M. Curty et al, Phys. Rev. Lett. 92, 217903 (2004)

No secret key can be distilled

The sequential attack against the COW

- Eve only resends blocks or sub-blocks that are bordered by vacuum *pulses*

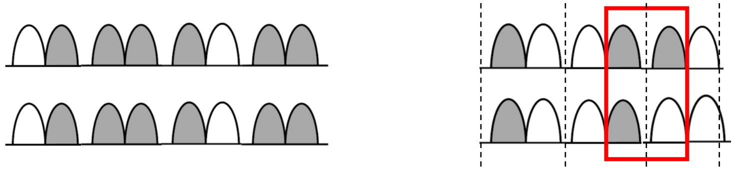


Why is this necessary?

Alice sends:	d	1	1	0	d	1	d	d	0	1	0	1	0
Eve gets:	inc	inc	inc	0	d	1	d	inc	0	1	0	inc	0

Alice sends:

Eve gets:

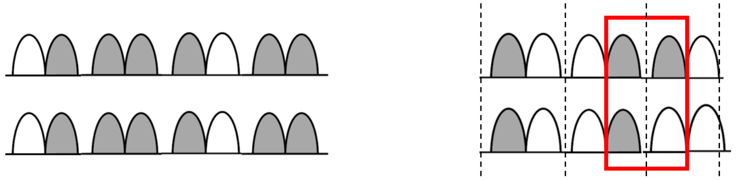


Why is this necessary?

Alice sends:	d	1	1	0	d	1	d	d	0	1	0	1	0
Eve gets:	inc	inc	inc	0	d	1	d	inc	0	1	0	inc	0

Alice sends:

Eve gets:



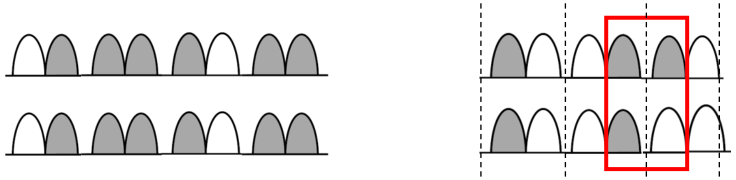
Eve would break the coherence

Why is this necessary?

Alice sends:	d	1	1	0	d	1	d	d	0	1	0	1	0
Eve gets:	inc	inc	inc	0	d	1	d	inc	0	1	0	inc	0

Alice sends:

Eve gets:



Eve would break the coherence

- USD → no misidentified state → QBER=0
- Eve avoids breaking the coherence with her strategy → $V_s = 1$

Zero-error attack

Upper security bound

J. González-Payo, R. Trényi, W. Wang, and M. Curty, Phys. Rev. Lett. 125, 260510 (2020)

Given f, α

↓

Optimal USD

↓

$q_{\mathrm{inc}}(f, \alpha)$

↓ given Eve's strategy

$G_{\mathrm{zero}}(f, \alpha)$ (QBER=0 and $V_s = 1$ below this gain value)

↓

Any experiment with $G(f, \alpha, \eta) \leq G_{\mathrm{zero}}(f, \alpha)$ is insecure

Upper security bound

Given f: $\forall\eta\ \exists\alpha_{\max}(f,\eta)$ such that $\underbrace{G_{\text{zero}}(f,\alpha_{\max}) < G(f,\alpha_{\max},\eta)}_{\text{To be safe from the zero-error attack}}$

Upper security bound

$$\text{Given } f\text{: } \forall\eta\ \exists\alpha_{\max}(f,\eta) \text{ such that } \underbrace{G_{\text{zero}}(f,\alpha_{\max}) < G(f,\alpha_{\max},\eta)}_{\text{To be safe from the zero-error attack}}$$

If α is too large → signal states are more orthogonal → USD is easier
↓
G_{zero} is too large ← less inconclusive results

Upper security bound

Given f: $\forall\eta\ \exists\alpha_{\text{max}}(f,\eta)$ such that $\underbrace{G_{\text{zero}}(f,\alpha_{\text{max}}) < G(f,\alpha_{\text{max}},\eta)}_{\text{To be safe from the zero-error attack}}$

If α is too large → signal states are more orthogonal → USD is easier

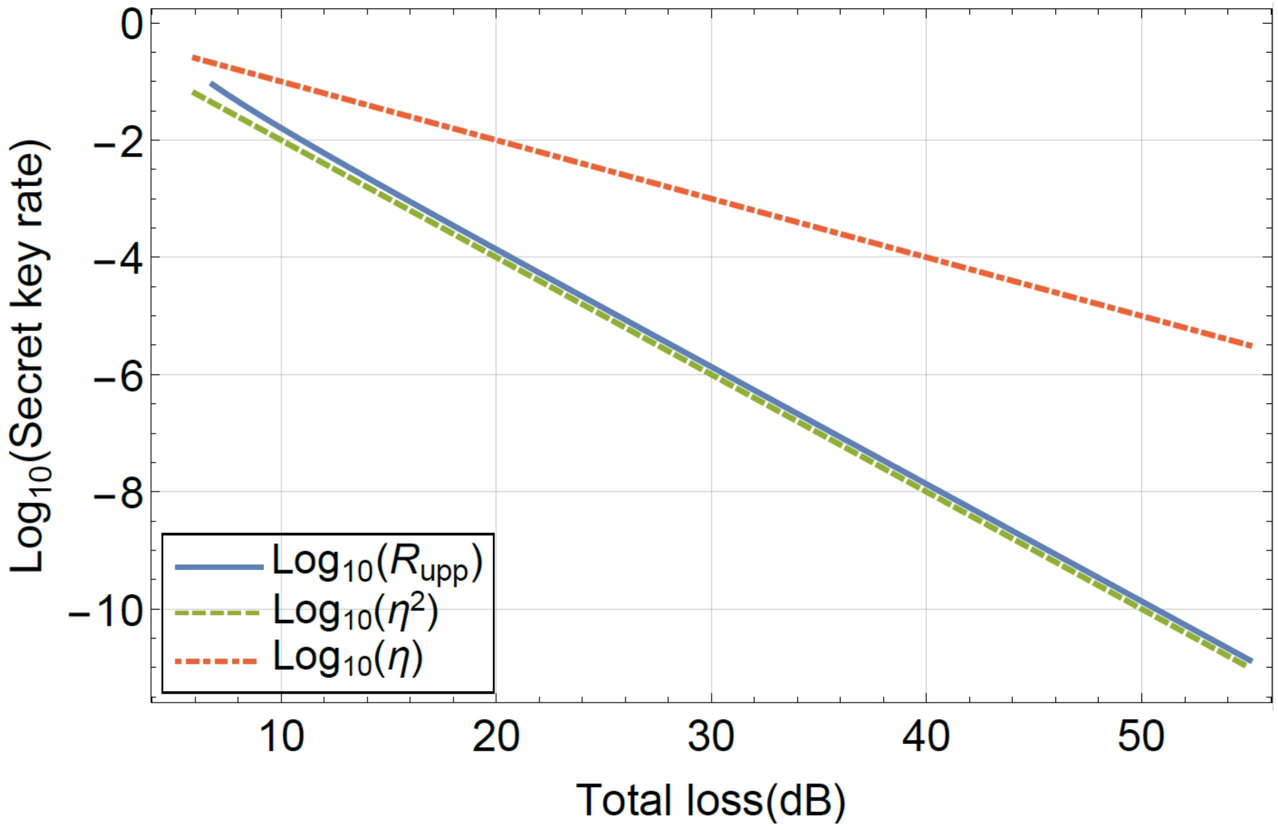
↓

G_{zero} is too large ← less inconclusive results

Trivial upper bound for the secret key rate:

$$K \leq (1-f)\eta|\alpha_{\max}(f,\eta)|^2 \equiv R_{\text{upp}}$$

Evaluation of the bound



A real life example

μ	f	η_{D}	p_{d}	t_{B}	α_{att} (dB/km)
0.5	0.1 [36]	0.77 [49]	2×10^{-8} [49]	0.9 [21]	0.2

COW is insecure after 22.6 km

Conclusions and outlook

- The asymptotic scaling of the COW protocol is quadratic in the system’s transmittance

Conclusions and outlook

- The asymptotic scaling of the COW protocol is quadratic in the system's transmittance

- Makes it inappropriate for long distance QKD

Conclusions and outlook

- The asymptotic scaling of the COW protocol is quadratic in the system's transmittance
- Makes it inappropriate for long distance QKD
- COW serves as an example where coherent attacks are more powerful than collective attacks

Conclusions and outlook

- To achieve the hoped linear scaling the scheme has to be modified

Conclusions and outlook

- To achieve the hoped linear scaling the scheme has to be modified
- More quantities to be monitored
- Checking coherence between non-adjacent coherent pulses
- Adding extra states

Conclusions and outlook

- To achieve the hoped linear scaling the scheme has to be modified
- More quantities to be monitored
- Checking coherence between non-adjacent coherent pulses
- Adding extra states

- Less simple implementation is needed