Federal Ministry of Education and Research

SENDATE FICUS

Helmut Schmidt Universität
Universität der Bundeswehr Hamburg

2018 Munich Workshop on Information Theory of Optical Fiber

Machine Learning in Heterodyne Quantum Receivers

Christian G. Schaeffer, Max Rückmann, Sebastian Kleis,

Darko Zibar

DTU

cgs@hsu-hh.de

FKZ: 16KIS0490

Motivation: Why Physical Layer Security?

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

Public key method

- ► Logical layer
- ☺ Simple to implement
- ☹ Computational secure
- ☹ Vulnerable to quantum computers
- ☹ Threat of "store now, break later"

Quantum key distribution (QKD)

- ► Physical layer
- ☺ Unconditional security
- ☺ Attacker has to break the system when it is used
- ☹ Complex and costly
- ☹ State of the art key rate $G \approx 10^{-3}$ bit/symbol @ 90 km[1]

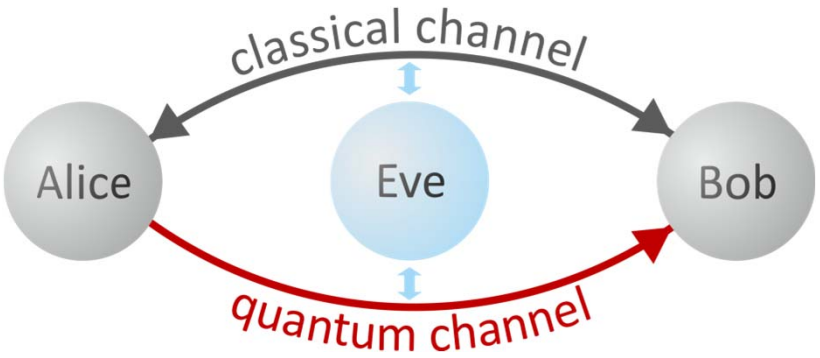
[1]D. Huang et al., Nature Scientific Reports, 2016, doi:10.1038/srep19201

Outline

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

1. The QKD principle
2. Promises and challenges of coherent detection for QKD
3. Coherent quantum PSK
   - Mutual information
   - Key rate optimization
   - Excess noise
   - Experimental setup
4. DSP design for coherent quantum communications
5. Bayesian Inference & laser phase noise
6. Conclusion & Outlook

The QKD Principle



Quantum state transmission

Reconciliation (classical)
Error correction, privacy amplification

Secret key

Encrypt public channel

- Information advantage based on quantum properties
  - Non-orthogonality of coherent states (Heisenberg uncertainty) (CV)
  - Single photon or entanglement (DV)
- A key is not transmitted but **generated after the quantum state transmission** by **interactive reconciliation** via the classical channel

Secret Key Rate

- Key rate equals information advantage

$$G = \rho \cdot I_{\mathrm{AB}} - I_{\mathrm{Eve,max}}$$

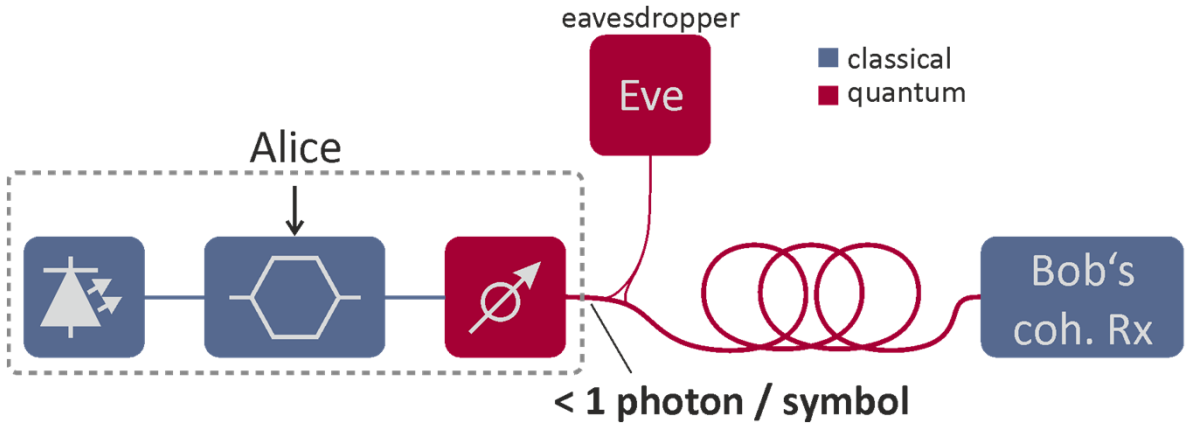
Reconciliation efficiency
- $0 \leq \rho \leq 1$

Mutual information of Alice and Bob
- Depends on signal power and receiver
- $0 \leq I_{\mathrm{AB}} \leq \log_2(M)$ [bit/symbol]

Eve's maximum information
- Depends on signal power, channel attenuation and excess noise ξ'
- $\xi' \geq 0$ [shot noise units]

- ξ': Unexplained noise power in the received signal
  - Assumed to be introduced by Eve
- For maximum key rate, the optimum signal power should be found
- **Usually $N_{\mathrm{Bob}} \ll 1$ photon per symbol**

The Coherent Quantum Channel I
Heterodyne Detection



$$\alpha_k = \sqrt{N_\mathrm{A}}\exp(j2\pi k/M)$$

$$\beta_k = \eta\alpha_k$$

η: channel transmittance

N_A: Sent photons/symbol

- Attenuation increases Heisenberg uncertainty
- Here: coherent M-PSK

$$k \xrightarrow{\text{modulate}} |\alpha_k\rangle \xrightarrow{\eta} |\beta_k\rangle \xrightarrow{\text{measure}} \beta \xrightarrow{\text{decode}} l$$

- After quantum state transmission: Estimation of $I_{\mathrm{Eve}}(\xi)$ necessary

The Optical Coherent Quantum Channel II
Heterodyne Detection

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

Promises

- High quantum efficiency
- Spectral efficiency
- Standard telecom components
- Great selectivity, WDM tolerance due to LO

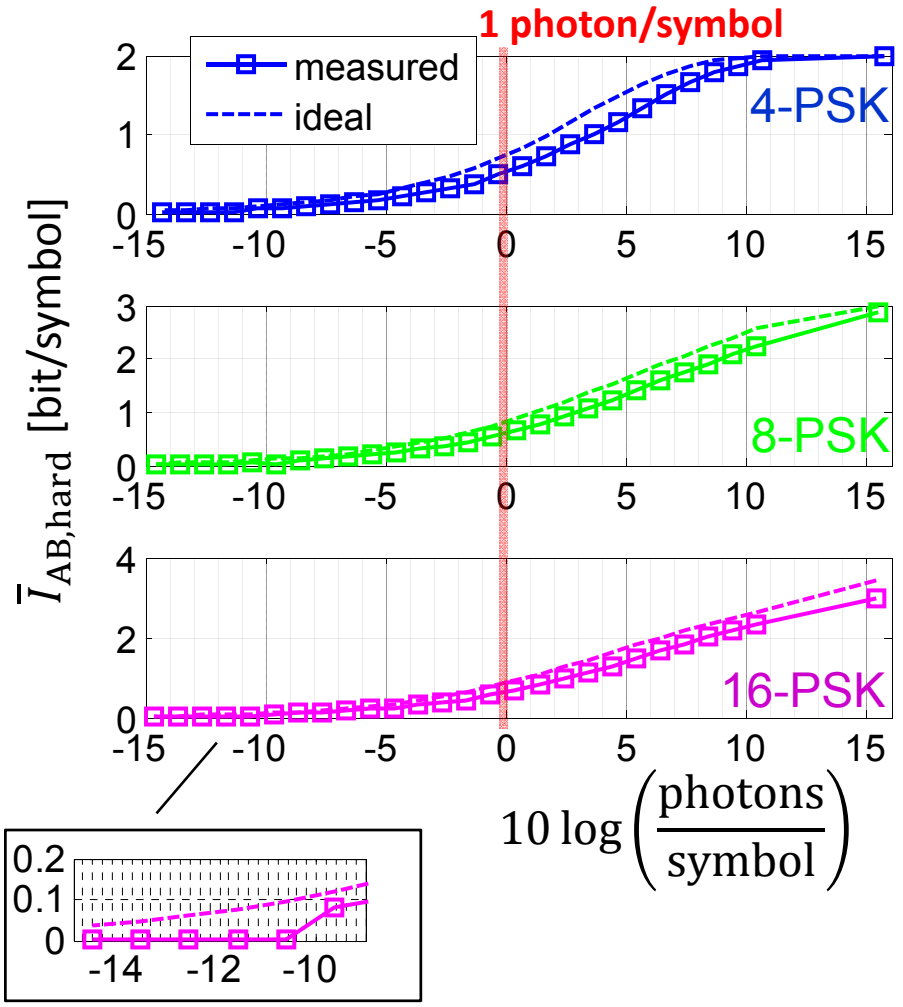
Challenges

- Local oscillator required
- Phase noise compensation
- Frequency estimation
- Synchronization
- Complex reconciliation procedure

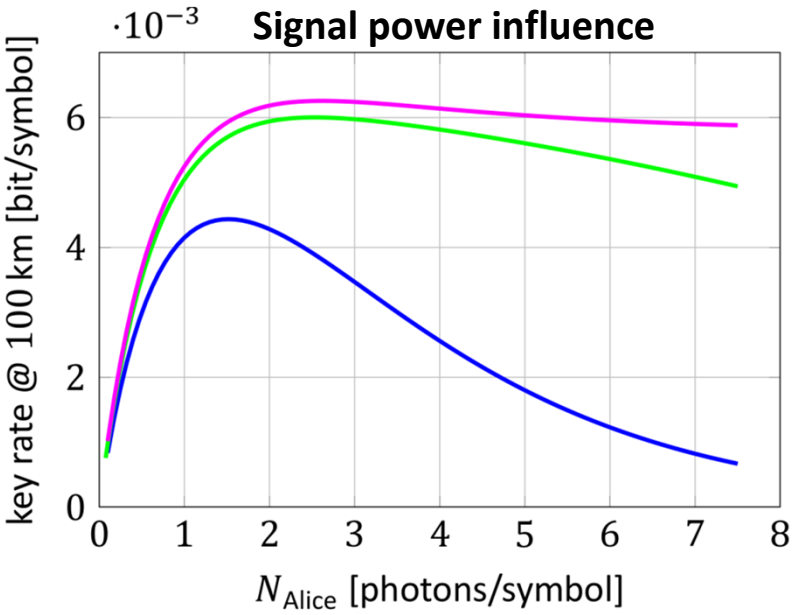
- Challenges not solved yet
- To date, only prototype systems for coherent QKD do exist

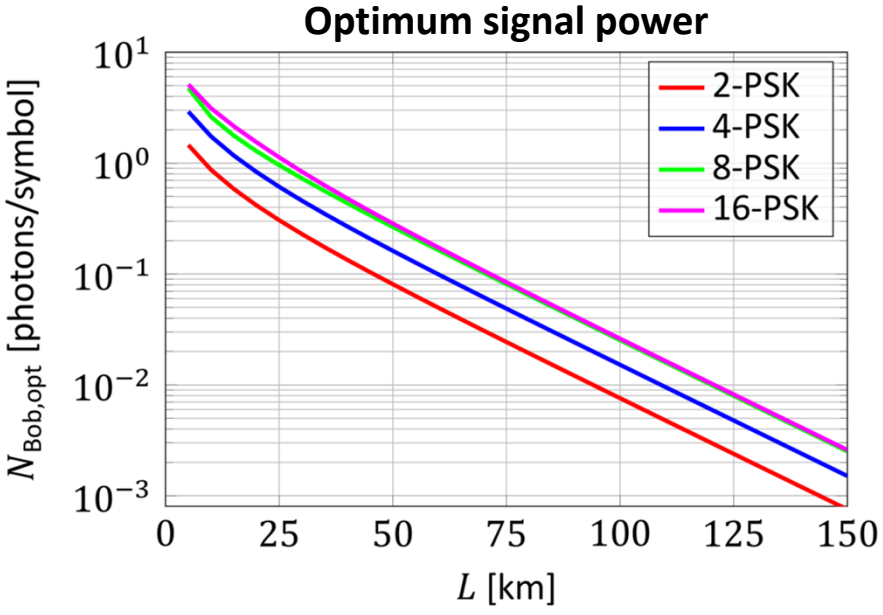
Typical Experimental Results on Mutual Information (Back to Back)

- Lowest power dependent on pilot signal power ratio (18 dB)
- Experimental evaluation of $\bar{I}_{\mathrm{AB,hard}}$
  - Penalty: ~ 2 dB
  - 1 dB due to Rx quantum efficiency
  - 0,5 dB due to electronic noise
- Experimental raw key rate
  - Optimize Alice's power level considering receiver characteristics
  - Found MI penalty serves as worst case estimate for key rate penalty



Properties of Quantum PSK





- Optimization of optical power
  - Beam splitter attack
  - Hard decision
  - Ideal reconciliation
- $\text{SNR}_{\text{ideal}} = N_{\text{Bob}}$

Very weak signal
at long distances

Excess Noise Estimation

- Key rate: $G = \rho \cdot I_{\mathrm{AB}} - I_{\mathrm{Eve,max}}(\xi')$
- Excess noise determines Eve's max. Information
- Alice reveals part of her symbols $\alpha(k)$
- Power components of the received signal

$\alpha(k)$	Alice's symbols
$\beta(k)$	Bob's noisy symbols
η	detector quantum efficiency
t	channel transmittance

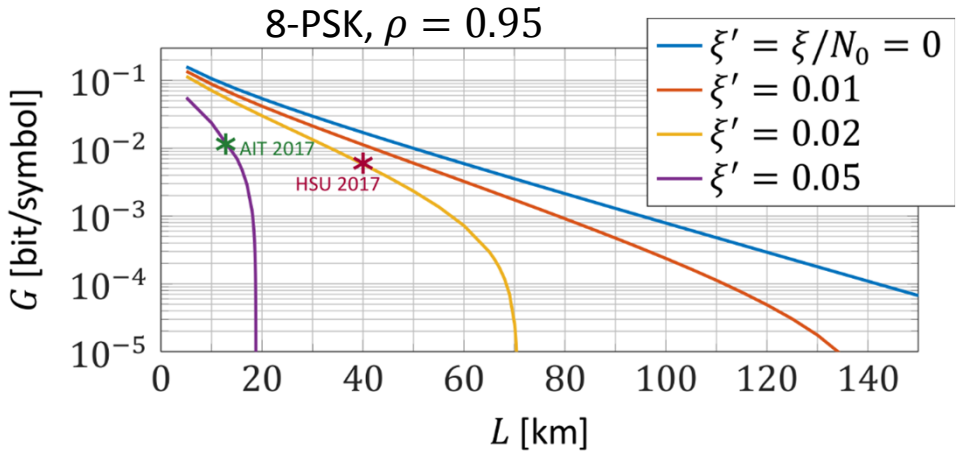
$$P_{\mathrm{Bob}} = \eta t P_{\mathrm{Alice}} + N_0 + N_{\mathrm{el}} + \eta t \xi$$

total power estimation
$\hat{P}_{Bob} = \overline{|\beta(k)|^2}$

signal power estimation
$\hat{P}_{\mathrm{Q}} = |\mathrm{Cov}(\alpha, \beta^*)|^2$

shot noise, electronic noise
calibrated before transmission

Excess noise
Residual power

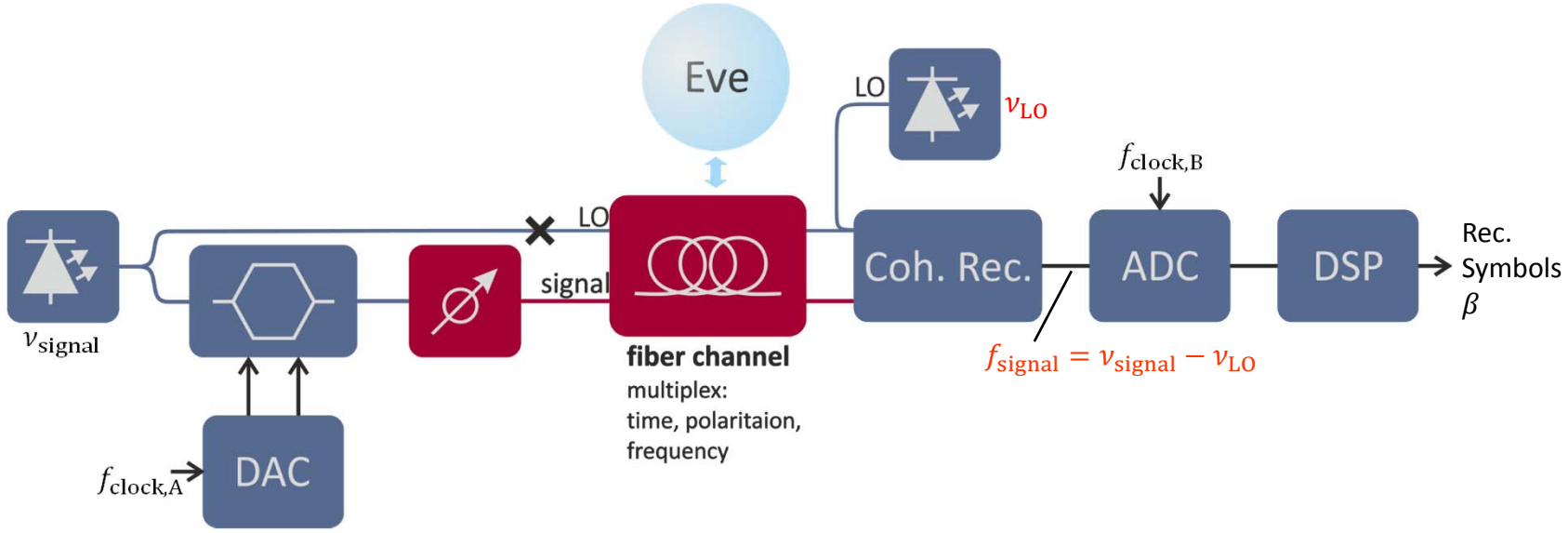


Key rate and achievable distance very sensitive to ξ'!

ECOC 20117: HSU P2.SC6.26
Influence of the SNR of Pilot Tones on the Carrier Phase Estimation in Coherent Quantum Receivers, *Sebastian Kleis;*
AITR P2.SC6.10
High-Rate Continuous-Variables Quantum Key Distribution with Piloted-Disciplined Local Oscillator,*Bernhard Schrenk*

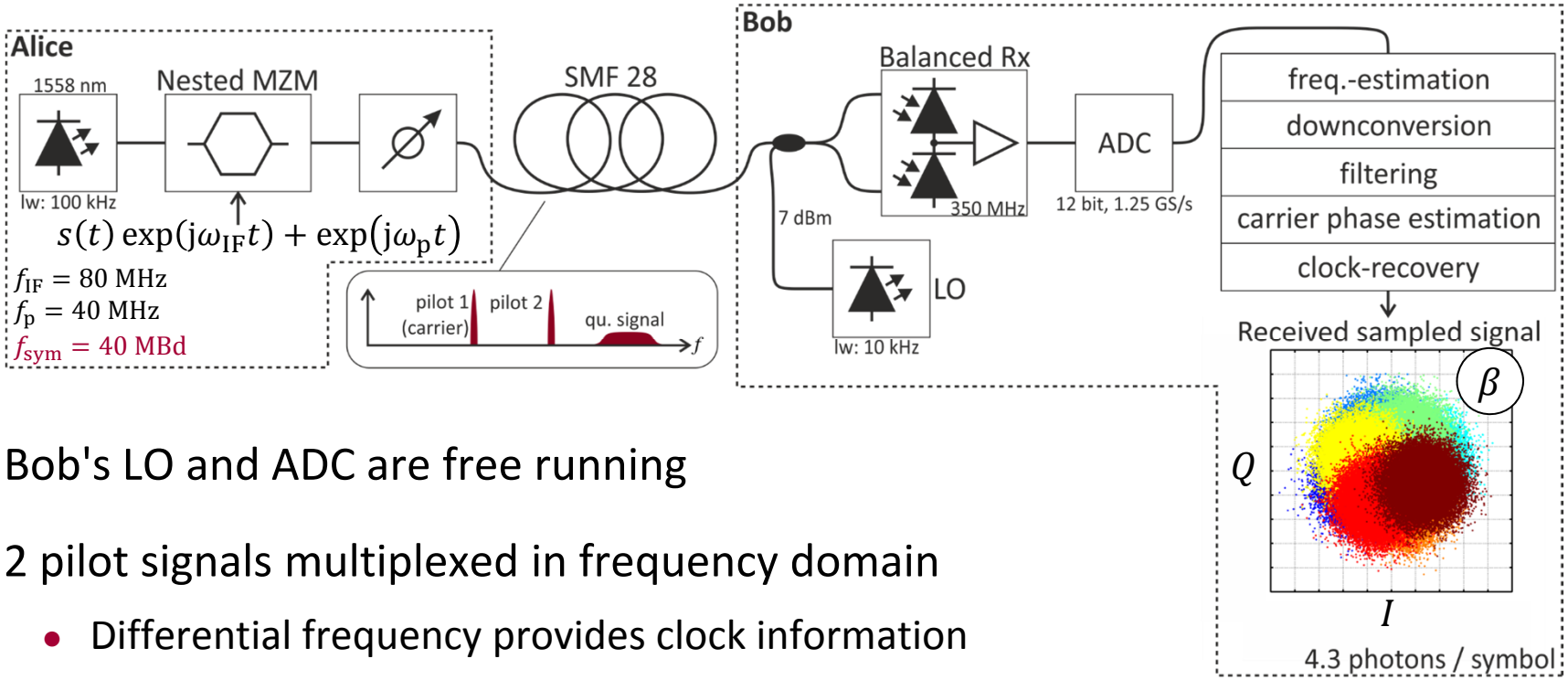
General Coherent Quantum System

- Major challenges: Laser phase noise and clock synchronization



- Remote LO is a common approach but problematic
  - Eve has access to the LO
  - Limited reach due to attenuated LO
- Our approach: Heterodyne with real LO
  - The DSP has to compensate laser freqency noise and perform clock recovery!

Experimental Heterodyne Quantum PSK System[2]

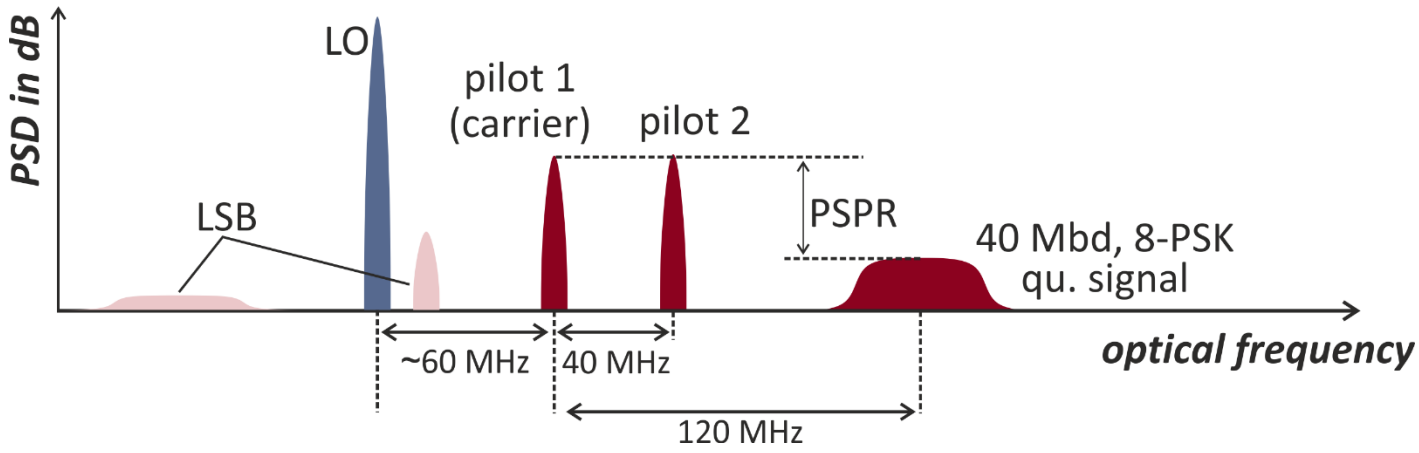


- Bob's LO and ADC are free running
- 2 pilot signals multiplexed in frequency domain
  - Differential frequency provides clock information
- Power ratio between pilots and signal limited by dynamic range of the components (DAC, modulator, balanced Rx, ADC)
  - Pilots exhibit low SNR, too

[2]S. Kleis and C. G. Schaeffer, Optics Letters, 2017, doi:10.1364/OL.42.001588

Details of The Received Signal

- Received optical signal before balanced detection



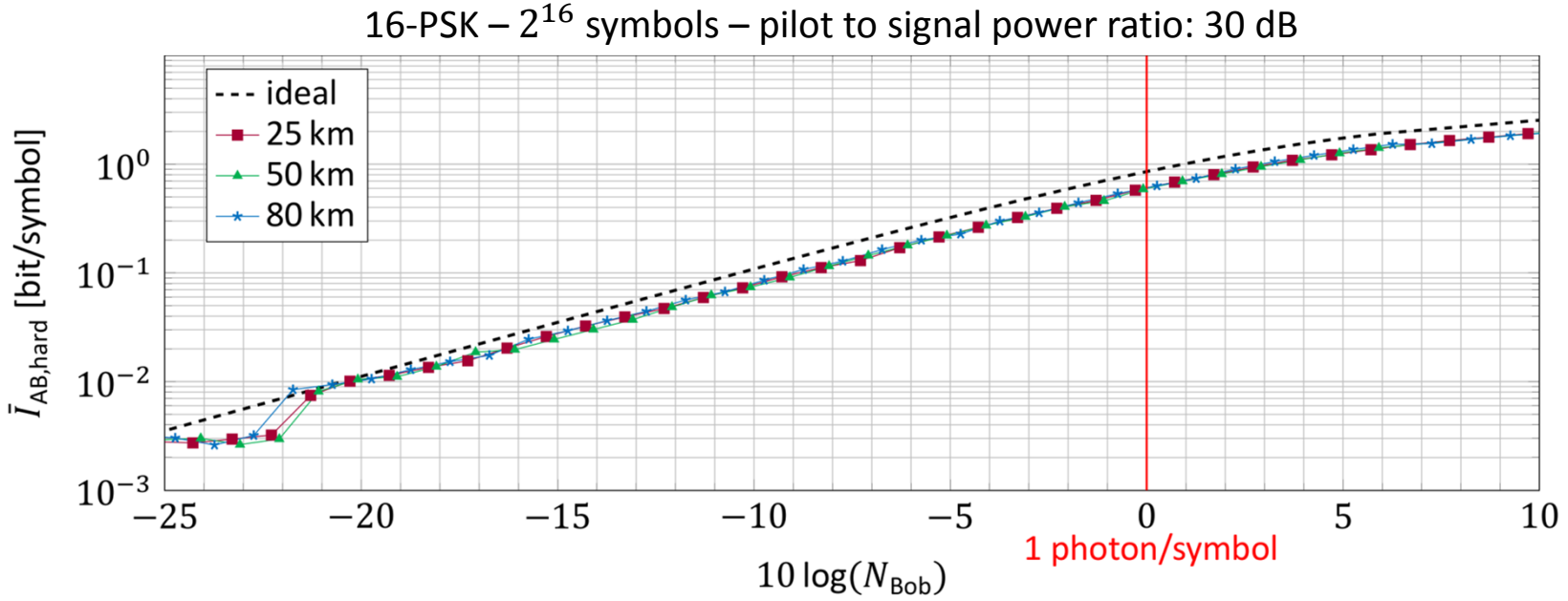
- Pilots are equal in power
- The **pilot to signal power ratio (PSPR)** is the power ratio between one pilot and the quantum signal
- Pilot 2 provides clock information

Design of DSP for Ultra Low SNR

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

- No known algorithms can deal with such low SNR → **pilot signals necessary!**
- Frequency estimation
  - *Classical system:*
    Coarse estimation only, residual offset is corrected by carrier phase estimation
  - *Quantum system:*
    Critical problem, residual offsets directly translate into phase errors
- Carrier phase estimation
  - *Classical system*: Based on modulated signal, e. g. "Viterbi & Viterbi"
  - *Quantum system*:
    Based on pilot signals, accuracy very important for the key rate
- Clock/timing recovery
  - *Classical system*: Based on modulated signal, e. g. "filter and square"
  - *Quantum system:*
    Pilot signals must contain clock information, precision critical for the key rate

Experimental Results at Different Fiber Lengths



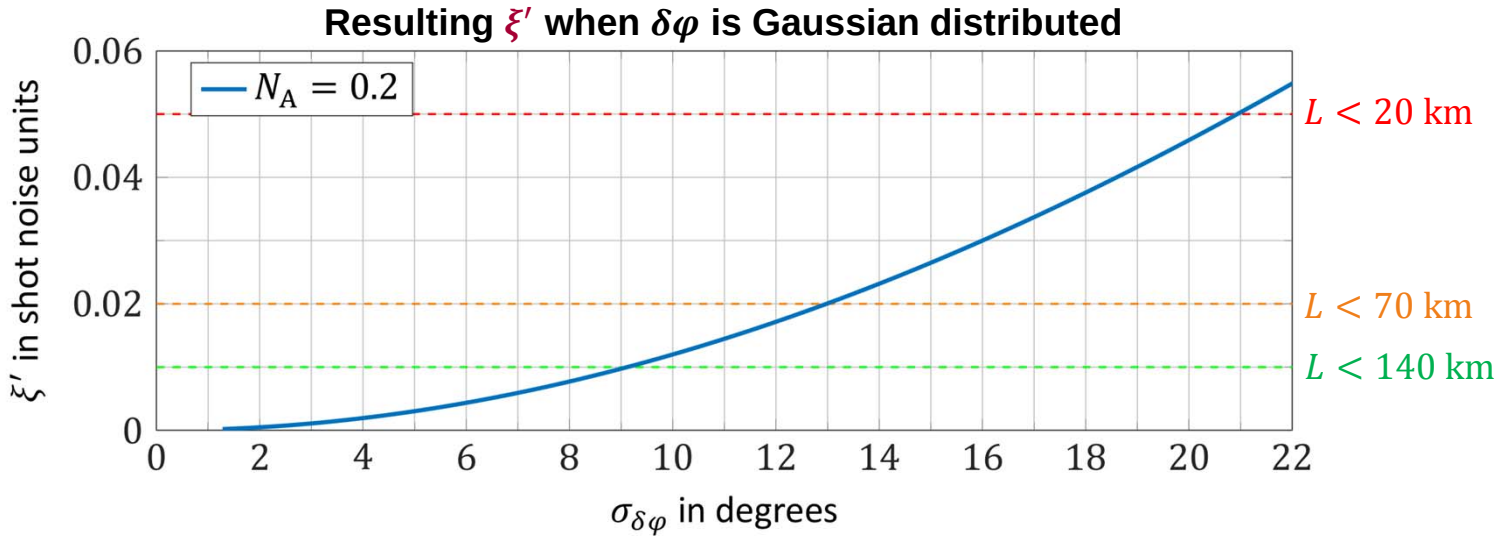
- Here, no influence of fiber length → CD compensation not necessary
- Penalty of < 2 dB (thermal noise, quantum efficiency)
- Less than 10^{-2} photons per symbol detectable!
- Setup shows great stability, repeatability of results

Impact of a Phase Error $\delta\varphi$ in the Received Symbols

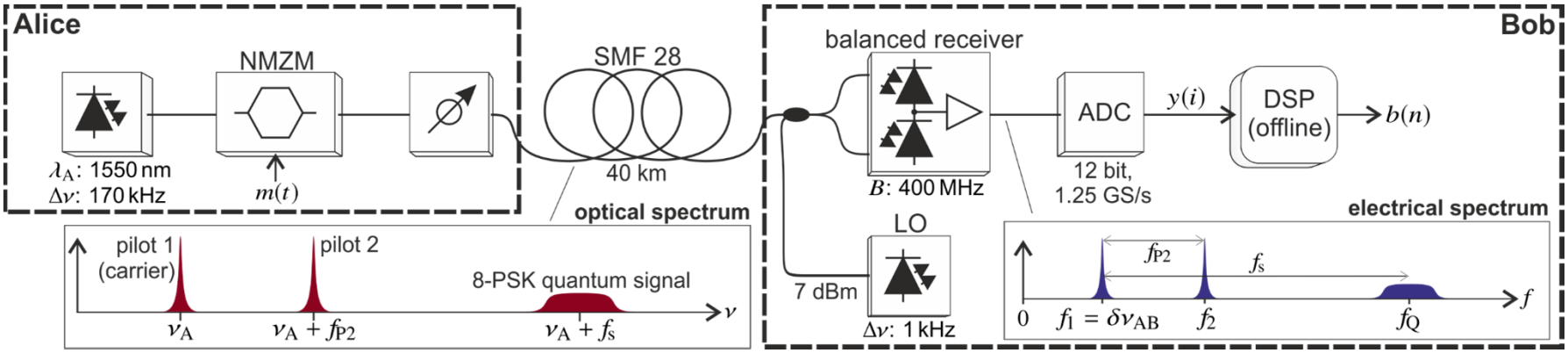
- With phase/frequency distortion: $\langle \hat{P}_{\mathrm{Q}} \rangle < P_{\mathrm{Q}}$
- Underestimation of P_{Q} ⇒ Overestimation of ξ'

$$\xi' = 2N_{\mathrm{A}}\left[1 - \frac{\hat{P}_{\mathrm{Q}}}{P_{\mathrm{Q}}}\right]$$
$$= 2N_{\mathrm{A}}\Delta\hat{P}_{\mathrm{Q}}$$
$$= 2N_{\mathrm{A}}[1 - \langle\cos(\delta\varphi)\rangle^2]$$

$\hat{P}_{\mathrm{Q}}$	Estimated quantum Signal power
$\Delta\hat{P}_{\mathrm{Q}}$	Signal power underestimation factor
N_{A}	Alice's power in photons/symbol
$\delta\varphi$	Phase error
ξ'	Excess noise



Experimental heterodyne quantum communication system[1]



Experimental parameters:

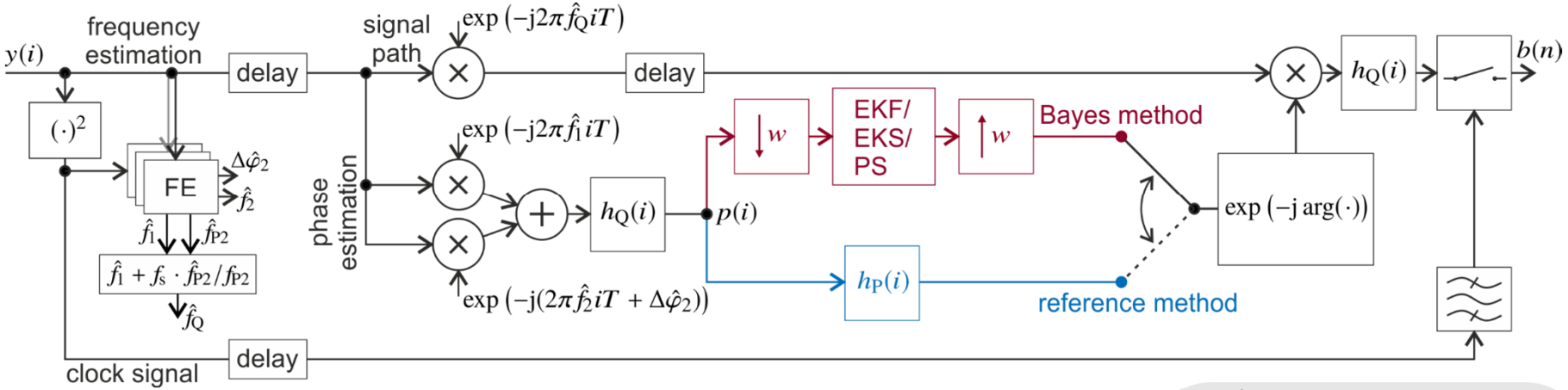
Format	8-PSK
Symbol rate	40 MBd
f_{P2}	40 MHz
f_s	120 MHz

- Bob's LO and ADC are free running
- Two pilots provide frequency, phase and clock information
  - Fixed pilot to signal power ratio (PSPR)
  - Limited by linearity and dynamic range of components
  - The pilots should be weak, too!

[1] S. Kleis, C. G. Schaeffer, *"Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals"*, Optics Letters 42(8), 2017.

Digital Signal Processing Routine

- Block wise procedure for signals of arbitrary length



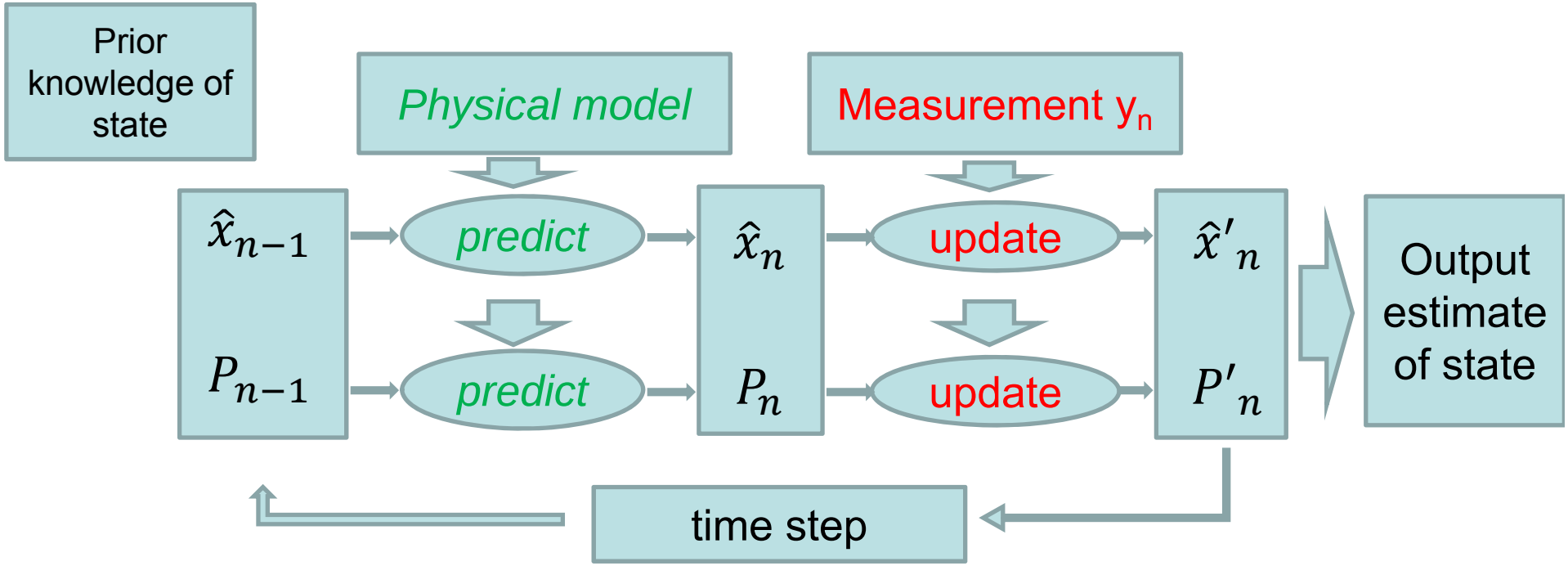
- Pilot SNR improvement by coherent superposition
- Approach for phase estimation
  - **Previously**: Nyquist filter with optimized bandwidth
  - **Novel**: Bayesian inference
  - Methods can be switched for comparison

$\hat{f}$	Estimated frequencies
$\Delta\hat{\varphi}_2$	Estimated initial pilot phase
$h(i)$	Zero roll-off Nyquist filter
$p(i)$	Combined pilot
EKF/ EKS/ PS	Extended Kalman Filter/ Extended Kalman Smoother/ Particle Smoother
w	Resampling factor

Bayesian Inference Methods [2]

- Purpose is to compute the state of a phenomenon when only the measurements are observed
- Recursive methods: $\hat{x}_n = f(\hat{x}_{n-1}, y_n)$
- The information of a new measurement is used to update the old information

$\hat{x}_n$	n-th estimate
y_n	n-th measurement



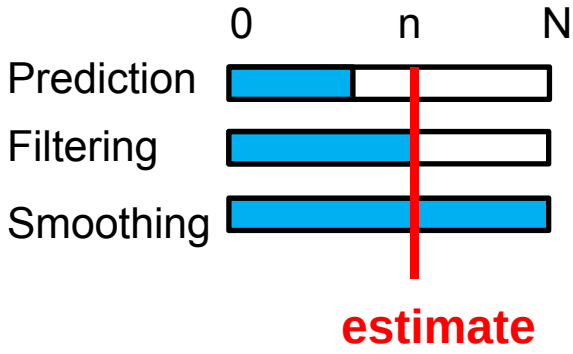
[2] S. Särkkä, Bayesian filtering and smoothing. Cambridge University Press, 2013, vol. 3.

Bayesian Inference Methods [2]

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

$\hat{x}_n$	n-th estimate
y_n	n-th measurement

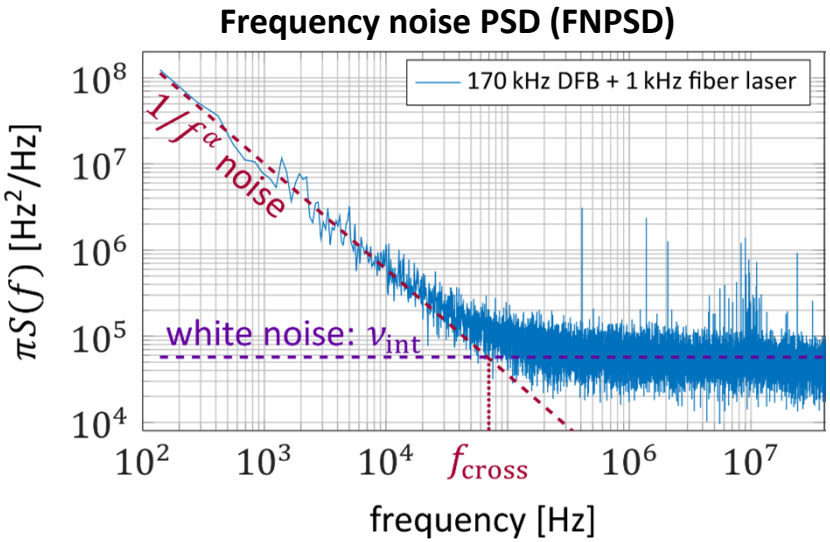
- Recursive methods: $\hat{x}_n = f(\hat{x}_{n-1}, y_n)$
- Provide optimal estimates if the state space model is exact
- **Filters:** To estimate x_n, measurements $y_{1:n}$ are taken into account
- **Smoothers:** For x_n, all measurements $y_{1:N}$ are taken into account
- **Extended Kalman filter/smoother**
  - Analytical method
  - Extension of Kalman filter to non-linear models
  - Approximation by linearization

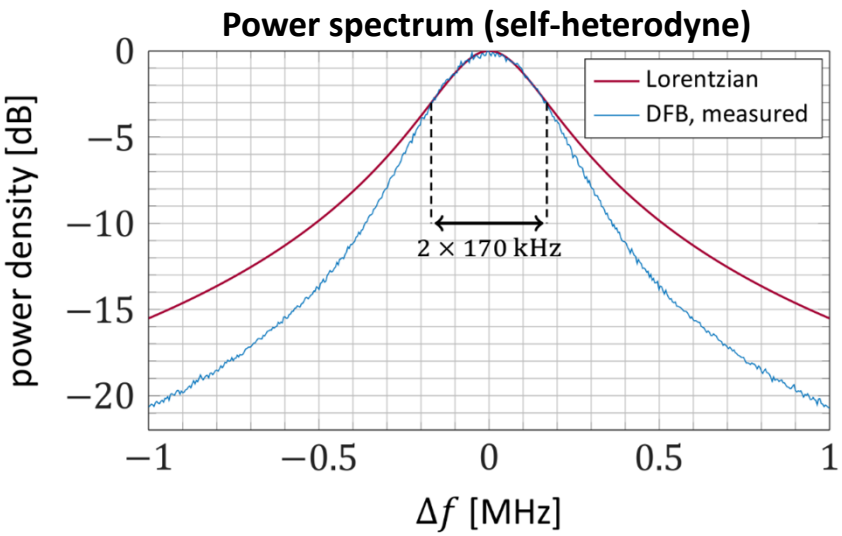


- **Particle filter/smoother**
  - Statistical method (Particles are randomly chosen)
  - No approximation involved
  - Converges to optimum for large number of particles (computationally heavy)

[2] S. Särkkä, Bayesian filtering and smoothing. Cambridge University Press, 2013, vol. 3.

Measured Laser Phase Noise Characteristics





- White frequency noise ⟺ Lorentzian line, **not here!**
- Strong $1/f^{\alpha}$ frequency noise component
- Three parameters describe the frequency noise: ν_{int}, f_{cross}, α
- These parameters should be included in the state space model for Bayesian inference

State space model including $1/f^2$ noise

- Process

$$\mathbf{x}_n = f(\mathbf{x}_{n-1}) + \mathbf{q}_{n-1}$$

$$\begin{bmatrix}\Omega_n \\ \varphi_n\end{bmatrix} = \begin{bmatrix}1 & 0 \\ 1 & 1\end{bmatrix}\begin{bmatrix}\Omega_{n-1} \\ \varphi_{n-1}\end{bmatrix} + \begin{bmatrix}q_{\Omega,n-1} \\ q_{\varphi,n-1}\end{bmatrix}$$

Ω_n:	Frequency to include $1/f^2$ - noise
φ_n:	Signal phase
$\mathbf{q}_n$, $\mathbf{r}_n$:	WGN processes

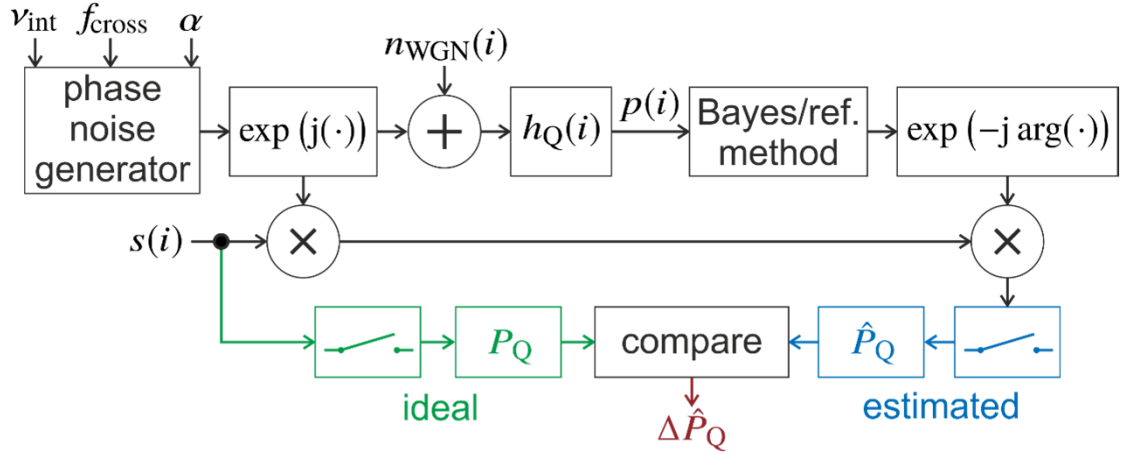
- Exact model for $\frac{1}{f^2}$ - noise ($\alpha = 2$)
- $\frac{1}{f^\alpha}$ -noise with $\alpha \neq 2$ not feasible due to an infinite number of poles [3]
  - Results in an infinite number of state space variables
  - **Measured:** $\alpha \approx 1.23$
  - To reduce the impact of that mismatch, $f_{\text{cross,model}} := \frac{f_{\text{cross}}}{2}$
- Measurement of the pilot quadratures with a coherent receiver

$$\mathbf{y}_n = \mathbf{x}_n + \mathbf{r}_n \qquad \begin{bmatrix}y_{\text{I},n} \\ y_{\text{Q},n}\end{bmatrix} = \hat{y}\begin{bmatrix}\cos(\varphi_n) \\ \sin(\varphi_n)\end{bmatrix} + \begin{bmatrix}r_{\text{I},n} \\ r_{\text{Q},n}\end{bmatrix}$$

[3] N. J. Kasdin, “Discrete simulation of colored noise and stochastic processes and $1/f^\alpha$ power law noise generation,” Proceedings of the IEEE, vol. 83, no. 5, pp. 802–827, 1995.

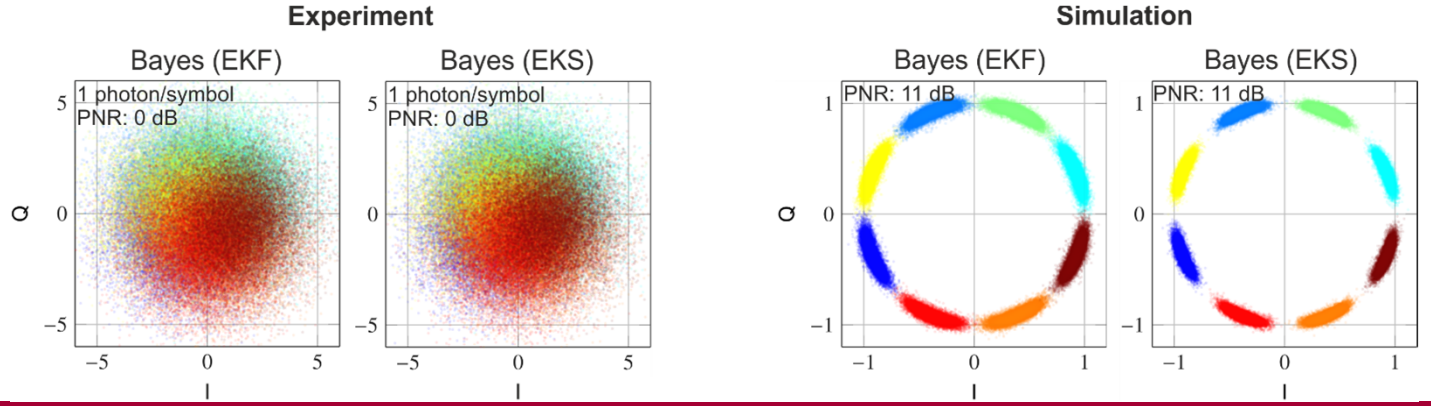
Simulation Model for $\Delta\hat{P}_{\mathrm{Q}}$

- Block diagram

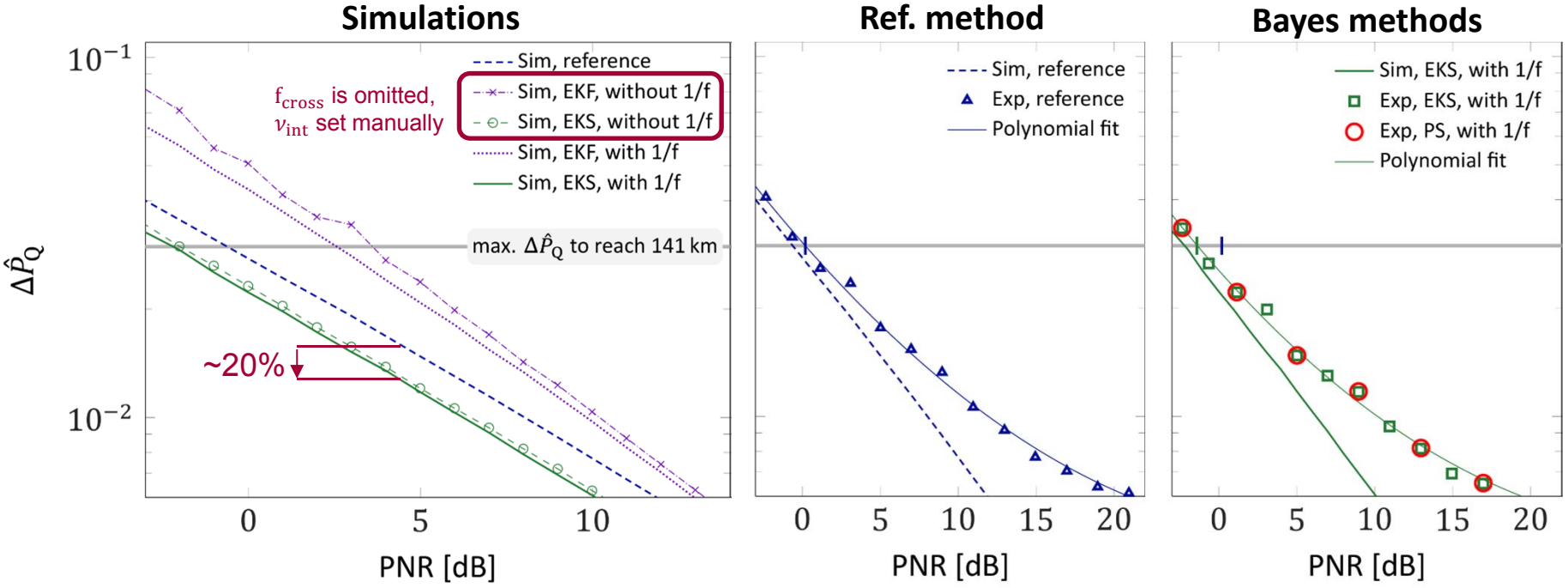


$s(i)$	Nyquist-shaped 8-PSK signal
$\hat{P}_{\mathrm{Q}}$	Power estimator for quantum signal
$\Delta\hat{P}_{\mathrm{Q}}$	Signal power underestimation factor
$n_{\mathrm{WGN}}(i)$	White Gaussian noise
PNR	Pilot to noise ratio (SNR of $p(i)$)

- Only additive Gaussian noise and phase noise included
- Signal constellations after phase correction



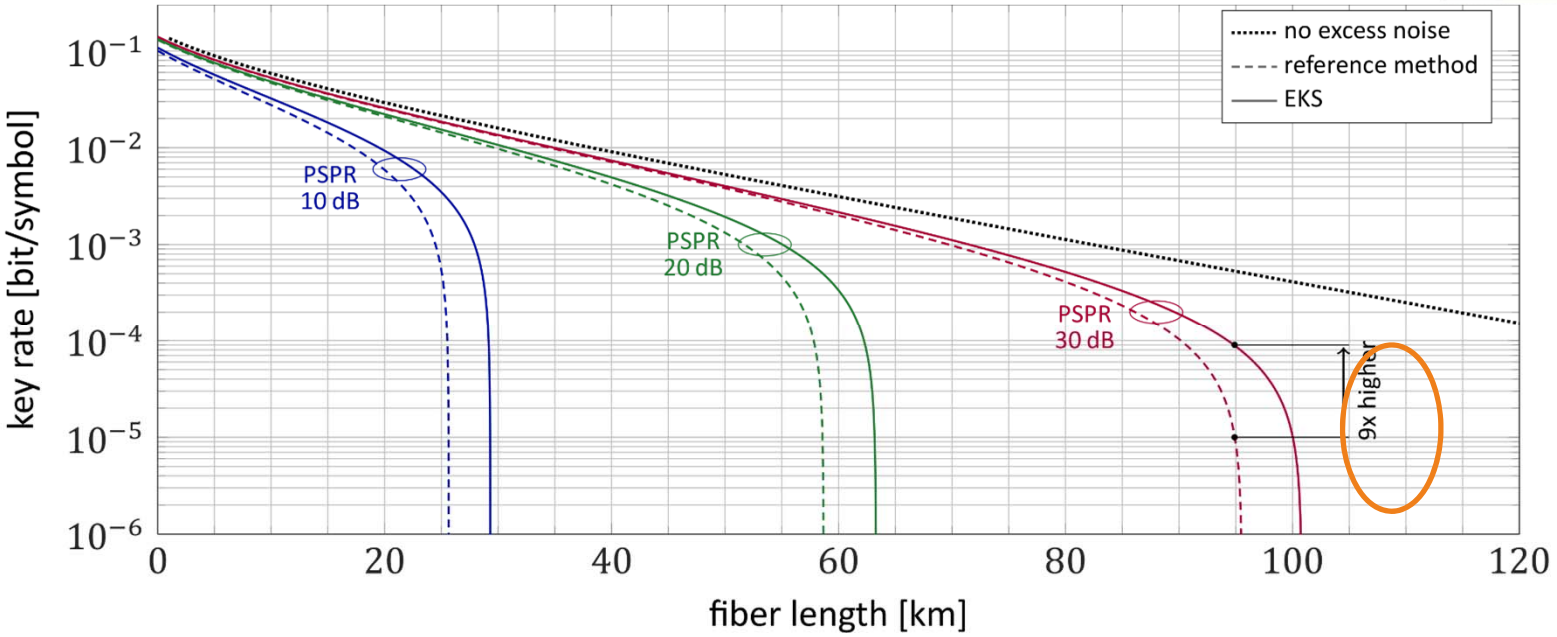
Experimental and Simulation Results



- It is beneficial to include f_{cross} in the model
  - Better performance / no manual adjustment necessary
- The EKS method outperforms the reference by **20%**
- PS and EKS show same performance
  → Indicates optimum for given state space model

S. Kleis, C. G. Schaeffer, *"Improving the Secret Key Rate of Coherent Quantum Key Distribution with Bayesian Inference"*, JLT October 2018.

Impact on the Secret Key Rate



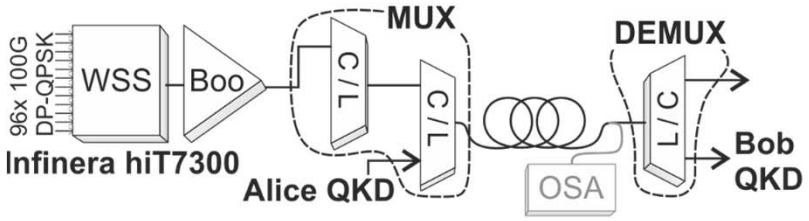
- The realized PSPR has a very strong influence
- The EKS method improves the system
  - Significantly higher key rate
  - Extended reach
  - More efficient tuning (no optimization required)

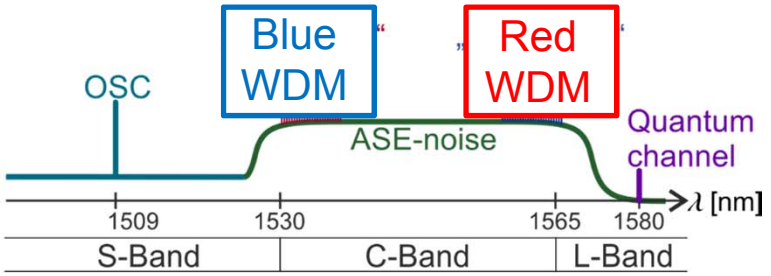
A. Becir et al., "Continuous-Variable Quantum Key Distribution Protocols With Eight-State Discrete Modulation," International Journal of Quantum Information, vol. 10, no. 1, p. 1250004, 2012.

Combining the Quantum Channel with Infinera's Commercial WDM System

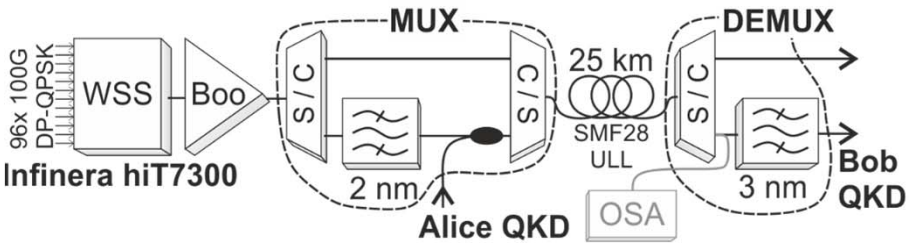
HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

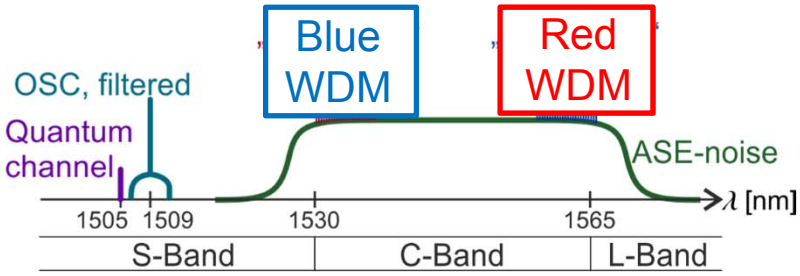
- L-Band configuration





- S-Band configuration

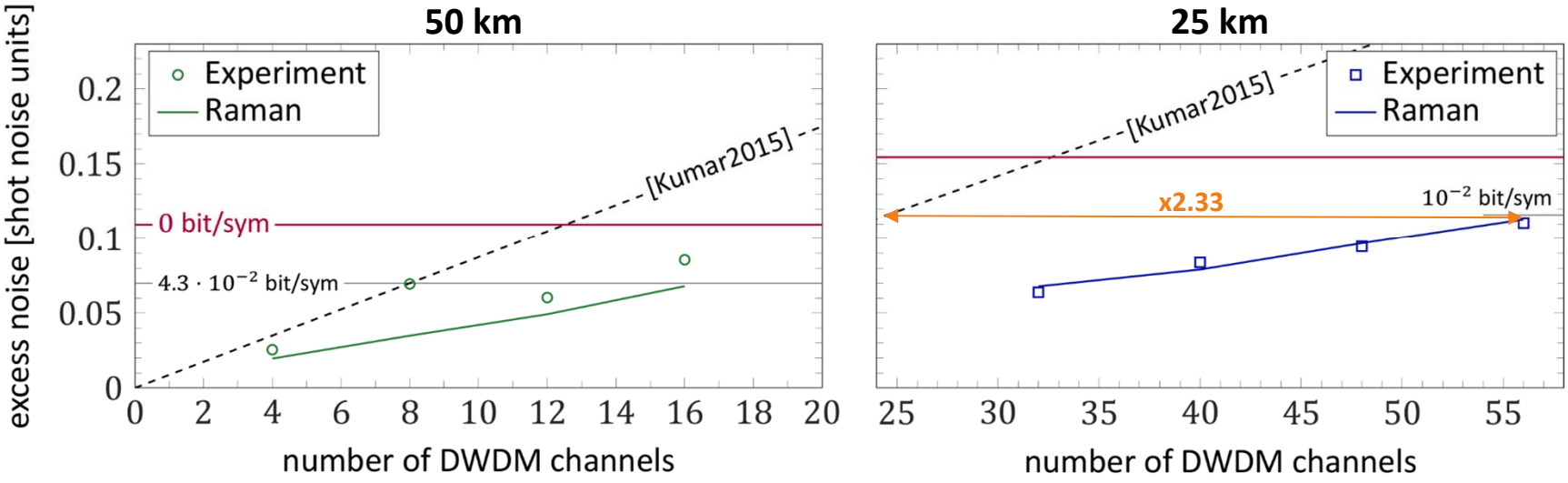




- Prior to experiments, noise contributions are measured with an OSA to predict the performance
- Quantum signal is Gaussian modulated!

infinera
coriant

Experimental Results for S-Band – „Red WDM“ – -3dBm/ch



- High tolerance also at large number of channels!
  - More than 56 of the 96 C-Band channels at 25km!
  - High flexibility for the C-Band DWDM system
  - Advantage compared to [Eriksson2018], where a narrow local minimum is used

[Eriksson2018]: 18ch, 13.7dBm, 10km
This work: 56ch, 14.5dBm, 25km

Parameters for 25 km (50 km)	
Launch power	2.42 ph/sym (1.99)
Reconciliation eff.	0.95
El. Noise power	0.18 SNU
Key rate w/o excess noise	5.3×10^{-2} bit/sym (1.4×10^{-2})
No. evaluated qu. symbols per data point	1.5×10^{8}

Conclusion

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

- Quantum communications can be realized very similar to classical systems
- The DSP must perform the same tasks but under significantly different conditions
- Shown: Feasibility for signal powers lower than 10^{-2} photons per symbol with standard components only
- Laser phase noise is a limiting factor for the achievable reach in CV-QKD systems
- Bayesian smoothers can improve the system
  - Better performance in terms of key rate and reach
  - No try and error optimization required
  - EKS and PS show best performance
  - EKS is preferred due to lower computational complexity
- Coexistence of QKD and WDM investigated

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

Thanks for your attention.

Some references:

Zibar, Darko ; Piels, Molly ; Jones, Rasmus Thomas ; Schaeffer, C. G.: „ Machine Learning Techniques in Optical Communication“, 41st European Conference on Optical Communication (ECOC), paper **Th.2.6.1**

S. Kleis, C. G. Schaeffer, "Improving the Secret Key Rate of Coherent Quantum Key Distribution with Bayesian Inference", IEEE JLT October 2018.

S. Kleis, C. G. Schaeffer, "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals", Optics Letters 42(8), 2017.

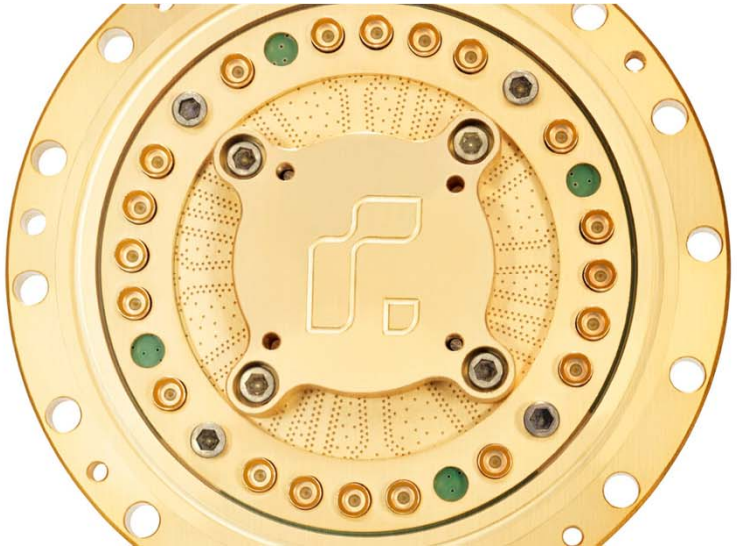
Quantum Computers

- They are coming:

Google unveiled Bristlecone, with 72 quantum qubits

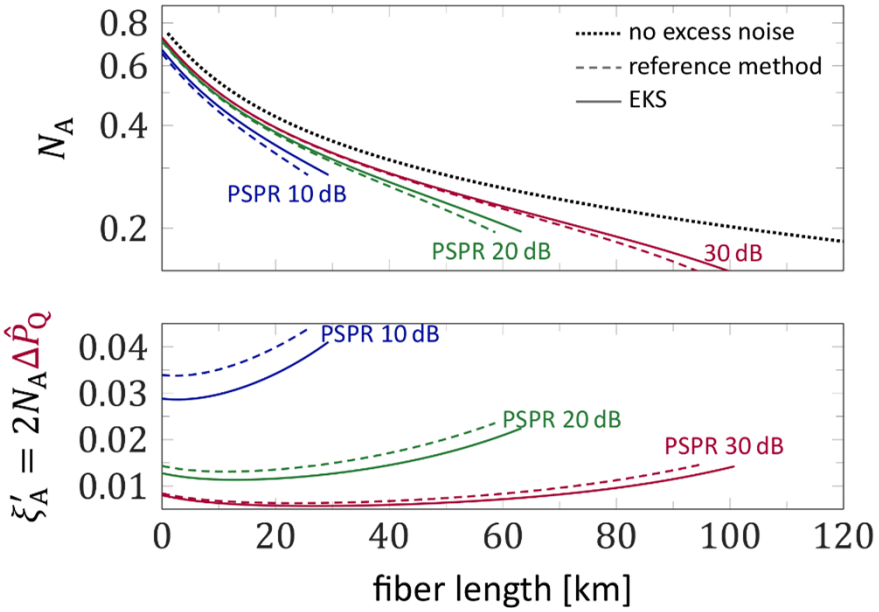
The next phase of quantum Computing: Rigetti 128

https://www.rigetti.com/



Key Rate Optimization Details

- Key rates are calculated according to 8-PSK security proof [3]
  - Optimization of N_A required
  - Key rate also depends on: $\Delta\hat{P}_\mathrm{Q}$, η, ρ, L, N_el
  - $\Delta\hat{P}_\mathrm{Q}$ depends on N_A and the PNR
    → Polynomial fits are included in the optimization



N_A	Alice's photons/symbol
$\Delta\hat{P}_\mathrm{Q}$	Signal power underestimation factor
η	Receiver efficiency
ρ	Reconciliation efficiency
L	Fiber length
N_el	Electronic noise power
PNR	Pilot to noise ratio

Scenario parameters

fiber loss	0.2 dB/km
ρ	0.95
N_el	0.2 N_0
η	0.51

[3] A. Becir et al., "Continuous-Variable Quantum Key Distribution Protocols With Eight-State Discrete Modulation," International Journal of Quantum Information, vol. 10, no. 1, p. 1250004, 2012.

The Extended Kalman Filter algorithm

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

- Prediction

$$\hat{\varphi}_n^- = \hat{\varphi}_{n-1}$$

$$\mathbf{P}_n^- = \mathbf{P}_{n-1} + \mathbf{Q}_{n-1}$$

φ_n:	Measured phase
$\hat{\varphi}_n$:	Filtered phase
$\mathbf{Q}_n$, $\mathbf{R}_n$:	Covariance matrices of, $\mathbf{q}$, $\mathbf{r}$
$\mathbf{H}_\mathbf{x}(\varphi)$:	Jacobian matrix of h with respect to $\mathbf{x}$ around φ

- Update

$$v_n = \varphi_n - h(\hat{\varphi}_n^-)$$

$$S_n = \mathbf{H}_\mathbf{x}(\hat{\varphi}_n^-)\mathbf{P}_n^-\mathbf{H}_\mathbf{x}^\mathrm{T}(\hat{\varphi}_n^-) + \mathbf{H}_\mathbf{r}(\hat{\varphi}_n^-)\mathbf{R}_n^-\mathbf{H}_\mathbf{r}^\mathrm{T}(\hat{\varphi}_n^-)$$

$$K_n = \mathbf{P}_n^-\mathbf{H}_\mathbf{x}^\mathrm{T}(\hat{\varphi}_n^-)S_n^{-1}$$

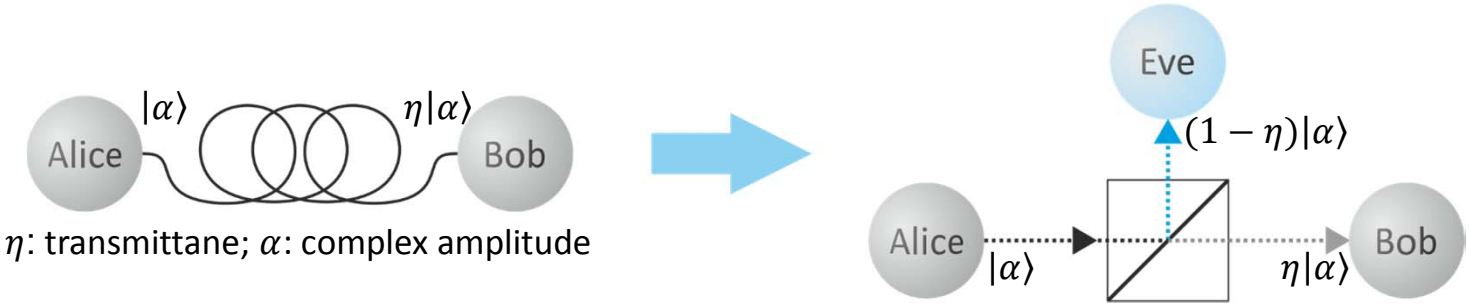
$$\hat{\varphi}_n = \hat{\varphi}_n^- + K_n v_n$$

$$\mathbf{P}_n = \mathbf{P}_n^- - K_n S_n K_n^{-1}$$

- Currently in progress: Integration into existing DSP procedure

Strongest Passive Attack[5]

- Beam splitter attack: Eve replaces channel by loss-less beam splitter



- Direct reconciliation:

$$G = \rho I_{\mathrm{AB}}(\eta, |\alpha|) - I_{\mathrm{AE}}(1-\eta, |\alpha|) \rightarrow \text{no key for } \eta < 0.5$$

- Reverse reconciliation:

$$G = \rho I_{\mathrm{AB}}(\eta, |\alpha|) - I_{\mathrm{BE}}(1-\eta, |\alpha|) \rightarrow \text{key for any } \eta$$

[5]G. van Assche, *"Quantum Cryptography and Secret Key Distillation"*, Cambridge University Press, 2006

Eve‘s Information

HELMUT SCHMIDT UNIVERSITÄT
Universität der Bundeswehr Hamburg

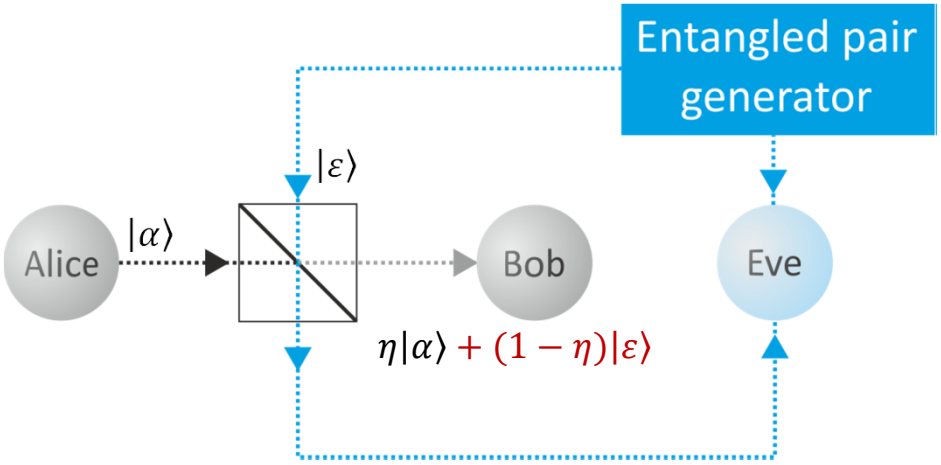
- Scenario:
  - Beam splitter attack
  - Eve uses a perfect coherent receiver (with measurement outcome ε)
  - Bob applies hard decision

$$I_{\mathrm{BE,hard}}(\varepsilon) = \log_2(M) + \sum_{l=0}^{M} p(l|\varepsilon)\log_2[p(l|\varepsilon)]$$

$$I_{\mathrm{BE,hard}} = \int p(\varepsilon) I_{\mathrm{BE,hard}}(\varepsilon)\,\mathrm{d}\varepsilon$$

General Active Attack Scenario (with Excess Noise)

- Entanglement cloner attack[2]
- Generalization of the beam splitter attack



- Eve increases I_{BE} by introducing one half of an entangled pair $|\varepsilon\rangle$, generated by her.
- This additional correlation between Eve and Bob induces excess noise ξ' in Bob‘s received signal

[2]G. van Assche, *“Quantum Cryptography and Secret Key Distillation“*, Cambridge University Press, 2006