

ITMO UNIVERSITY

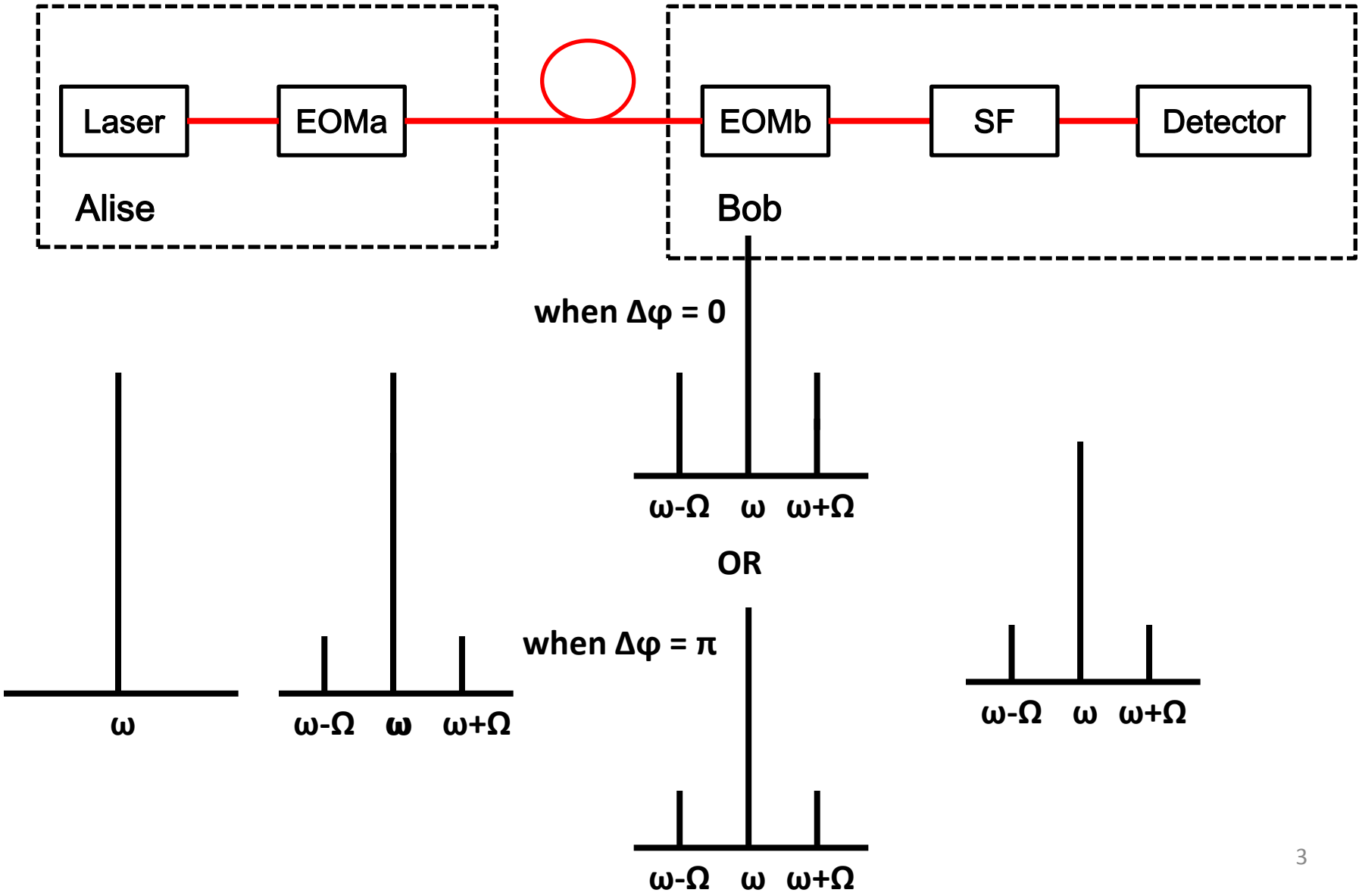
Proof of standard security analysis compatibility with a sub-carrier wave quantum communication method

Andrei Gaidash

Outline

- SCWQC basics
- Choosing EOM theory
- Dealing with two separate coherent states
- Secure key rate estimation

Sub-carrier wave quantum communication basics



Advantages of SCWQC

- ✓ Compatibility with laid standard telecom fibers
- ✓ Unidirectional – compatibility with quantum network applications
- ✓ Robustness to signal distortions – longer distance
- ✓ Spectral efficiency up to 40% – higher bitrates

*Gleim A. V. et al. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference //Optics Express (2016), V. 24, №. 3. pp. 2619-2633.

Choosing EOM theory

Classical theory of EOM

VS

Quantum theory of EOM

There is a trade-off between accuracy and simplicity

Classical theory of EOM

$$A\cdot\exp(i\omega t)\cdot\exp(i\cdot m\cdot\sin(\Omega t))$$

Jacobi – Anger expansion:

$$A\cdot\exp(i\omega t)\cdot\sum_n J_n(m)\cdot\exp(in\Omega t)$$

$$A\cdot J_0(m)\cdot\exp(i\omega t)+A\cdot J_1(m)\cdot\exp\left[i(\omega+\Omega)t\right]+$$
$$+A\cdot J_{-1}(m)\cdot\exp\left[i(\omega-\Omega)t\right]+\ldots$$

Quantum theory of EOM

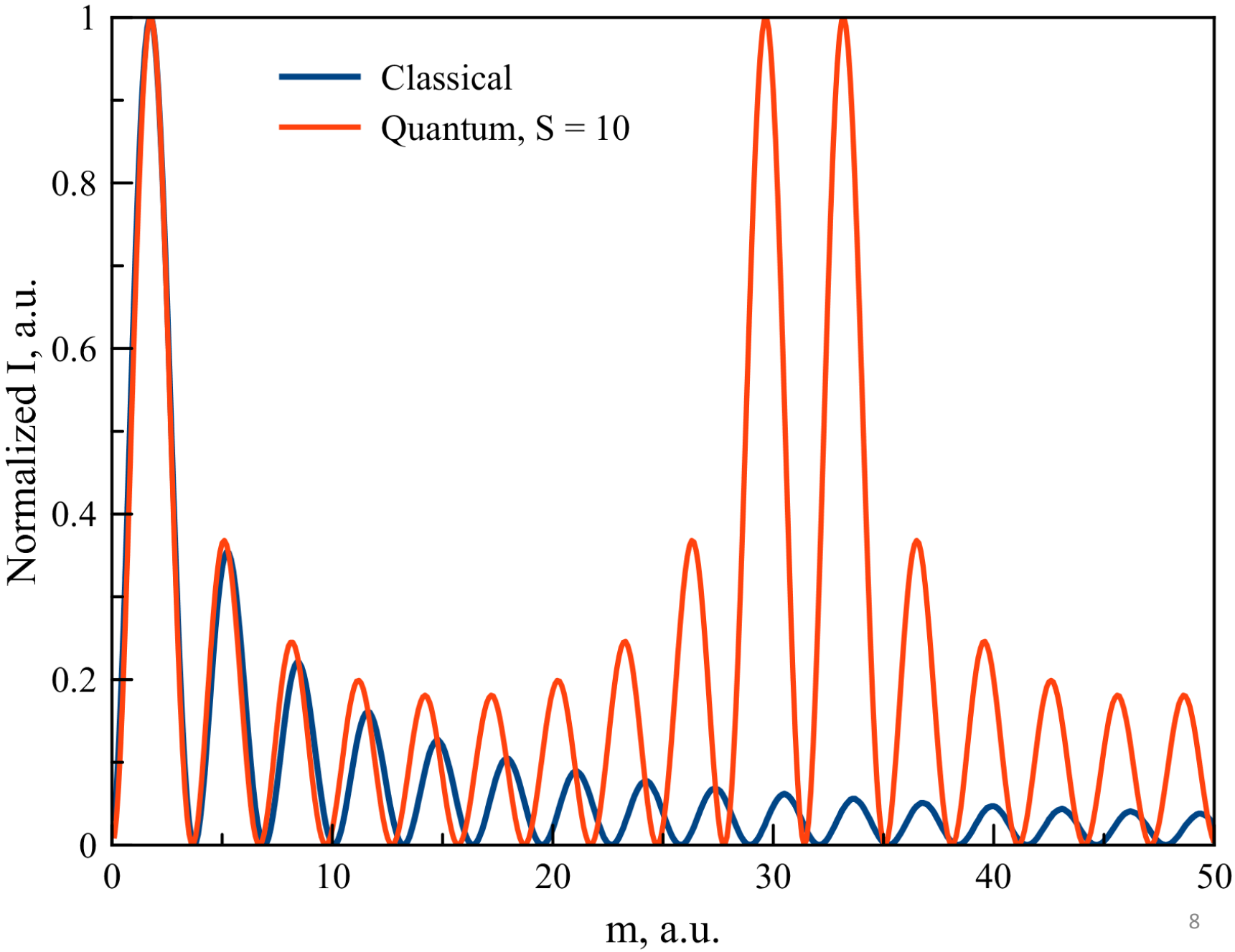
Solve Schrodinger's equations with Hamiltonian as following:

$$H_0 = \Omega \sum_{m=1} (m a_m^{\dagger} a_m) + \gamma \exp[-i\tilde{\Omega} t] \cdot \sum_{m=1} (f(m) a_m a_{m+1}^{\dagger}) +$$
$$+ \exp[i\tilde{\Omega} t] \cdot \sum_{m=1} (f(m) a_m^{\dagger} a_{m+1})$$

Mean photon number per mode depending on interaction time:

$$\mu_{\Delta m}(t) = \left| d^{S}_{\Delta m,0}(2\beta) \right|^2 \cdot \mu_{\Delta m}(0)$$

$$d^{S}_{\Delta m,0}(2\beta) \xrightarrow{S \to \infty} J_{\Delta m}(m)$$


Classical
Quantum, S = 10
Normalized I, a.u.
m, a.u.
0
0.2
0.4
0.6
0.8
1
0
10
20
30
40
50

Coherent states

Coherent state expressed in number of photons state terms:

$$|\alpha\rangle = \exp\left(\frac{-|\alpha|^2}{2}\right) \cdot \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

State describing two separate coherent states at both modes:

$$|\alpha_i\rangle \otimes |\alpha_j\rangle = \exp\left(-|\alpha|^2\right) \cdot \sum_n \sum_k \frac{\alpha_i^{\,n} \cdot \alpha_j^{\,k}}{\sqrt{n!} \cdot \sqrt{k!}} |n\rangle \otimes |k\rangle$$

Coherent states

Expand sum as a table filled with terms:

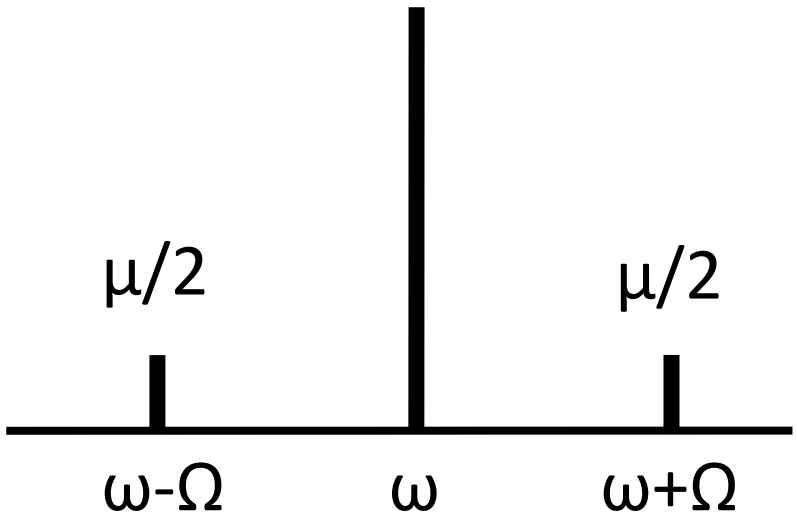
$$|\alpha_i\rangle \otimes |\alpha_j\rangle = \exp\left(-|\alpha|^2\right) \cdot \sum_n \sum_k \frac{\alpha_i^{\,n} \cdot \alpha_j^{\,k}}{\sqrt{n!} \cdot \sqrt{k!}} |n\rangle \otimes |k\rangle$$

$\frac{\alpha_i^0 \cdot \alpha_j^0}{\sqrt{0!} \cdot \sqrt{0!}} \lvert 0\rangle \otimes \lvert 0\rangle$	$\frac{\alpha_i^0 \cdot \alpha_j^1}{\sqrt{0!} \cdot \sqrt{1!}} \lvert 0\rangle \otimes \lvert 1\rangle$	$\frac{\alpha_i^0 \cdot \alpha_j^2}{\sqrt{0!} \cdot \sqrt{2!}} \lvert 0\rangle \otimes \lvert 2\rangle$	$\cdots$
$\frac{\alpha_i^1 \cdot \alpha_j^0}{\sqrt{1!} \cdot \sqrt{0!}} \lvert 1\rangle \otimes \lvert 0\rangle$	$\frac{\alpha_i^1 \cdot \alpha_j^1}{\sqrt{1!} \cdot \sqrt{1!}} \lvert 1\rangle \otimes \lvert 1\rangle$		
$\frac{\alpha_i^2 \cdot \alpha_j^0}{\sqrt{2!} \cdot \sqrt{0!}} \lvert 2\rangle \otimes \lvert 0\rangle$		$\ddots$	
$\vdots$			

$$|\alpha_{i+j}\rangle = \exp\left(-|\alpha|^2\right) \cdot \sum_n \sum_{k=0}^{n} \frac{\alpha_i^{\,n-k} \cdot \alpha_j^{\,k}}{\sqrt{(n-k)!} \cdot \sqrt{k!}} |n_{i+j}\rangle$$

Coherent states

$$\left|\alpha_{i+j}\right\rangle = \left|\sqrt{2}\cdot\alpha_{i=j}\right\rangle = \exp\left(\frac{-\left|\sqrt{2}\cdot\alpha\right|^2}{2}\right)\cdot\sum_n \frac{(\sqrt{2}\cdot\alpha)^n}{\sqrt{n!}}\left|n_{i+j}\right\rangle$$

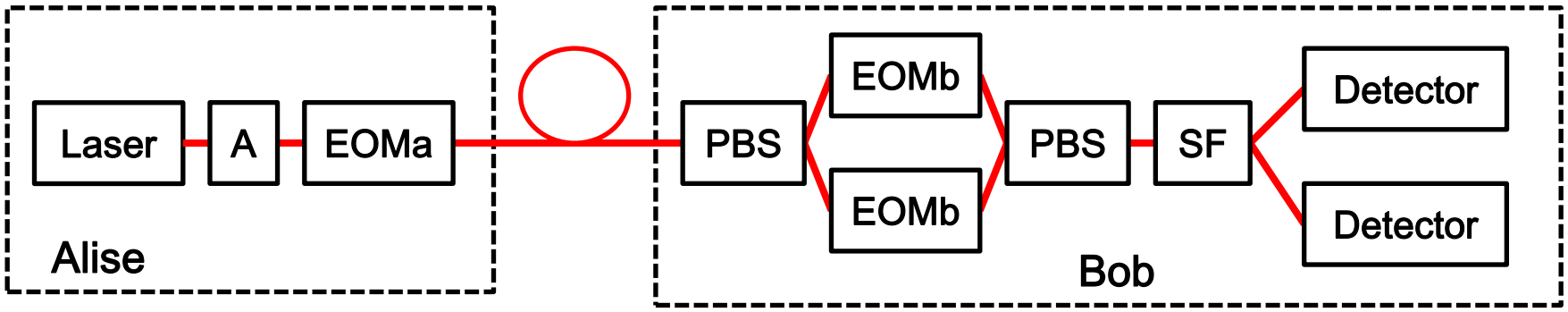


$$\mu_{i+j} = 2\mu_{i=j} = \left|\alpha_{i+j}\right|^2$$

$$J_1^2(m)\cdot\mu_{in} - \frac{\mu}{2} = 0$$

Parameters of QKD system

$\mu_{in} = 27.3$	$\beta = 6.4$ dB	$\Delta = 0.5$
$\mu = 1$	$p_{dark} = 10^{-7}$	SF= 30 dB
$m = 0.273$	QE = 10%	F = 100 MHz
$\alpha = 0.17$ dB/km	$\phi_{err} = 10^{o}$	



Secure key rate

Mean photon number per discrete time interval:

$$I(L,\Delta\varphi)=\mu_{in}\cdot 2\cdot J_1^2\left[2\cdot m\cdot\cos\left(\frac{\Delta\varphi+\varphi_{err}}{2}\right)\right]\cdot 10^{\frac{-\alpha\cdot L-\beta}{10}}\cdot QE$$

Carrier brightening:

$$I_C(L)=\mu_{in}\cdot J_0^2\left(2\cdot m\right)\cdot 10^{\frac{-\alpha\cdot L-\beta-SF}{10}}\cdot QE$$

Visibility depending on distance:

$$V(L)=\max\left(\frac{I(L,0)-\left[I(L,\pi)+I_C(L)+p_{dark}\right]}{I(L,0)+\left[I(L,\pi)+I_C(L)+p_{dark}\right]},0\right)$$

Secure key rate

Quantum bit error rate depending on visibility and misfire rates:

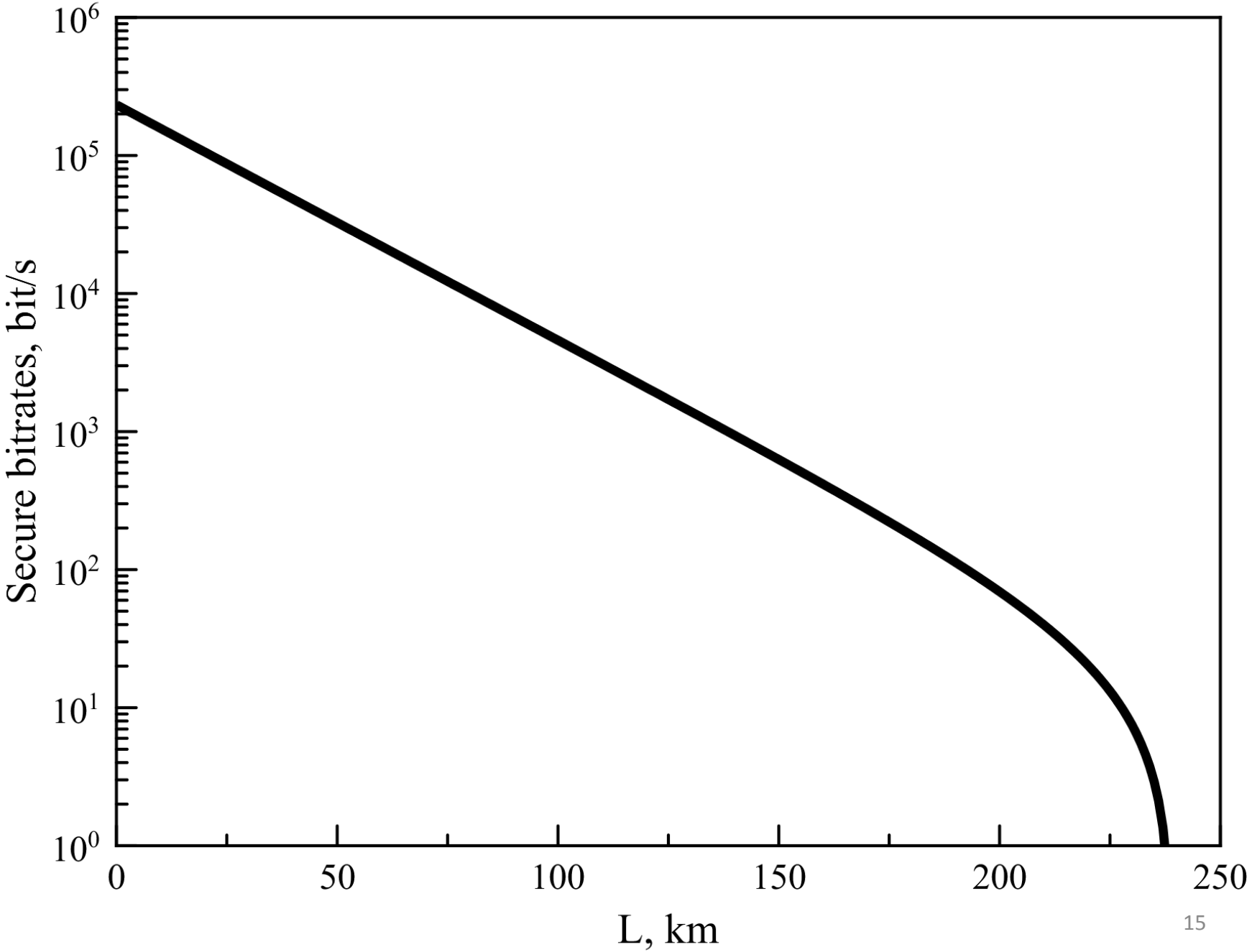
$$Q(L)=\frac{1-V(L)}{2}+\min\left[\frac{p_{dark}+I_C(L)}{2\cdot\left(I_{ave}(L)+p_{dark}+I_C(L)\right)},0.5\right]$$

Averaged mean photon number over all phase states:

$$I_{ave}(L)=\frac{I(L,0)+I(L,\pi)+2\cdot I(L,\pi/2)}{4}$$

Final form of secure key rate expression:

$$R(L)=\max\left(1-\Delta-H\left(\frac{Q(L)}{1-\Delta}\right)-H\left(Q(L)\right),0\right)\cdot\frac{I_{ave}(L)}{4}\cdot F$$


Secure bitrates, bit/s
10^6
10^5
10^4
10^3
10^2
10^1
10^0
0
50
100
150
200
250
L, km

Conclusion

- Classical EOM theory can be used for SCWQKD
- United coherent state approach for both side bands can be implemented
- New and more accurate approach for secure key rate calculation is demonstrated



ITMO UNIVERSITY

Thank you!