CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION WITH IMPERFECTIONS ON STATE PREPARATION SIDE

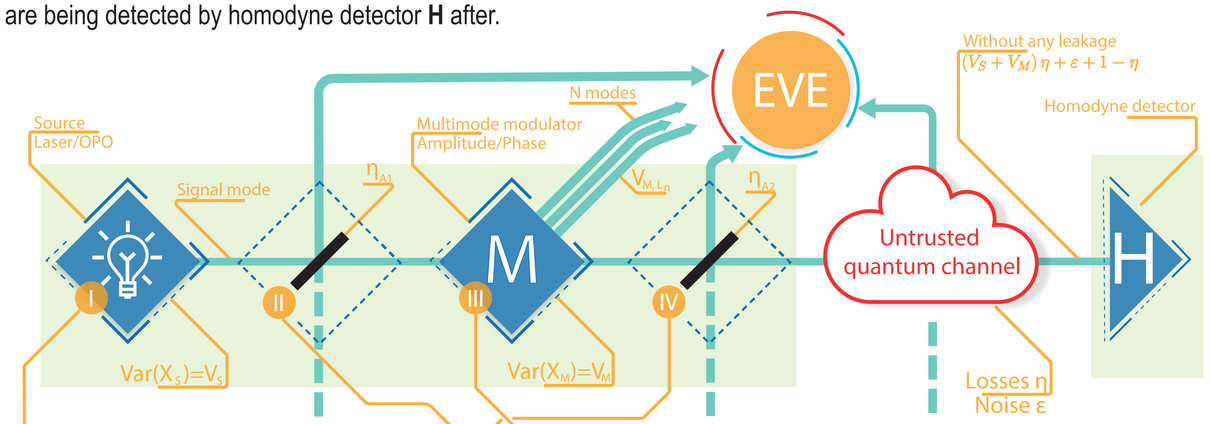
Palacký University Olomouc

Ivan Derkach, Vladyslav C. Usenko, and Radim Filip

CONTACTS

Quantum Key Distribution (QKD) is an application of quantum information science that is aimed at establishing secure communication between authenticated trusted parties, protected by the laws of physics. Practical implementations of continuous-variable (CV) QKD suffer from imperfections of real physical devices, which may be unnacounted in idealized security proofs. We show here possible imperfections, and mechanisms of information leakage from trusted state-preparation side. We provide analysis of individual and collective attacks on coherent- and squeezed-state protocols with direct and reverse reconciliation for separate preparation side imperfections.

Simplified prepare-and-measure CV QKD scheme with possible imperfections on preparation side (I-IV). Blue boxes indicate trusted stations of Alice and Bob. Source radiates Gaussian states in signal mode, that receive amplitude and phase displacement on modulator **M**. Signal states suffer from attenuation η and noise ε in untrusted quantum channel and are being detected by homodyne detector **H** after.



I PREPARATION NOISE

Reverse reconciliation: Phase-insensitive trusted preparation noise ΔV [1] was shown to be security breaking even in case of individual attacks in purely lossy untrusted channel [2,3]. In the limit of strong modulation key rate (2) is:

$$R_{V_M\to\infty}=\frac{1}{2}\left[\log_2\frac{1}{1-\eta}-\log_2\left(\eta\left[V_S+\Delta V\right]+1-\eta\right)\right]$$

Security is bounded by condition: $\Delta V<\frac{2-\eta}{1-\eta}-V_S$

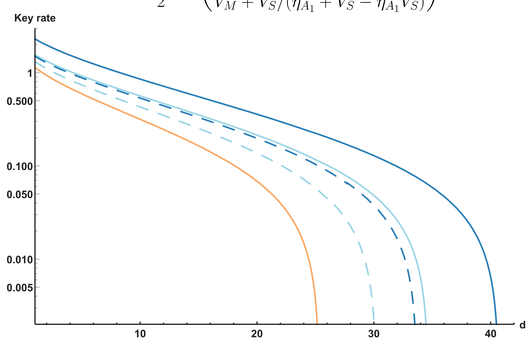
Squeezed state protocols are more robust towards such noise. ΔV limits the tolerable channel losses η and robustness to channel noise ε.

Direct reconciliation: ΔV can improve the robustness of CV QKD protocols to channel noise ε. Key rate (1,2), provided optimal noise ΔV is applied, can be improved or even turned positive if channel noise ε is strong.

II PREMODULATION CHANNEL

Side channel leakage prior to modulation is modelled as interaction of signal with vacuum mode on beamsplitter with coupling ratio η_{A1}. The main aspect of such channel is that it provides correlations with the signal to external party and corrupts the initial carries states. Premodulation channel does not affect coherent-state protocol, however squeezed-state protocol remains superior in terms of key rate (1,2) and channel noise ε tolerance for **direct** and **reverse reconciliation** protocols. Establishment of correlations provides additional advantage to adversary comparing to the case of preparation noise ΔV. The advantage is the highest for lossless untrusted channel (η=0) and in terms of (1) is

$$A=\frac{1}{2}\log_2\left(\frac{1+V_M+\eta_{A_1}(V_S-1)}{V_M+V_S/(\eta_{A_1}+V_S-\eta_{A_1}V_S)}\right)$$



Secure distance *d* in a standard telecom fiber (with an attenuation of *−0.2dB/km*) in the case of collective attacks for coherent-state protocol (orange) and squeezed-state protocol with V_S = 1/10, 1/2 (dark and light blue respectively). Premodulation channel coupling ratio η_{A1} = 1/2 (dashed lines) and 1 i.e., the absence of the channel (solid lines). Modulation variance is optimized for given parameters, β = 97%, ε = 5%.

Premodulation channel reduces secure distance of squeezed-state protocol. However even small squeezing allows to achieve longer distances. Upper bound on the influence of premodulation channel (η_{A1} = 0) is determined by the performance of the coherent-state protocol.

IV POSTMODULATION CHANNEL

Side channel leakage after modulation [4] is modelled as interaction of signal with vacuum mode on beamsplitter with coupling ratio η_{A2}. Postmodulation channel for any reconciliation type substantially increases sensitivity to channel noise ε. Provided noiseless channel (ε=0), and infinite squeezing and modulation $V_S, V_M \to \infty$ key rate (1) is:

$$R_{V\to\infty}=l\log_2\frac{1}{1-\eta_{A_2}\eta}$$

(*l*= 1 for the squeezed-state protocol and *l* = 1/2 for the coherent-state one)

The effect of postmodulation channel can be fully compensated if optimal correlated modulation is applied to the input of the side channel. For squeezed-state protocol the vacuum input has to be replaced with the source of squeezed states to fully compensate such leakage. Under optimal weight postmodulation channel is equal to premodulation channel (II) with scaled signal modulation.

METHODS

Gaussian states of light can be completely described in terms of covariance matrices [5,6]. We define the security against individual and collective attacks, as the positivity of the key rate:

$$R_{ind}=\beta I_{AB}-I_E\ ;(1)$$

Mutual information: $I_{XY}=\frac{1}{2}\log_2\left[\frac{V_X}{V_{X|Y}}\right];(3)$

Symplectic eigenvalues of respective covariance matrix

$$R_{col}=\beta I_{AB}-\chi_E;(2)$$

Holevo bound: $\chi_E=S(E)-S(E|B);(4)$

$$S(E)=\sum_{i=1}^{N}G\left(\frac{\lambda_i-1}{2}\right);$$

Post-processing efficiency; Von Neumann entropy; Bosonic entropy function

III MULTIMODE MODULATION LEAKAGE

The modulator can have a multimodal structure (N+1 modes) with auxiliary modes being directly available to the adversary. Modulation applied to N leakage modes may differ from the signal modulation $V_M/V_{M,Ln}$=k. **k=0** - leakage mode is not modulated; **k<1** - mode receives fraction of signal modulation; **k>1** - amplitude/phase displacement correspond to Gaussian distribution that has higher variance than that of the signal mode.
The case of N leakage modes can be reduced to single effective mode characterized by variance: $V_{L_{eff}}=\frac{N}{\sum_n^N V_{L_n}^{-1}}$
and modulation ratio: $k_{eff}=k\sqrt{N}$

Direct reconciliation protocol is extremely sensitive to the information leakage due to additional source mode. The key rate (1) in lossless and noiseless channel is:

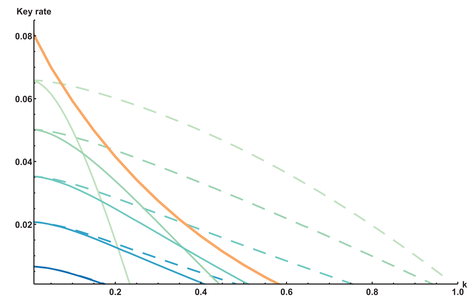
$$R_{DR}|_{\varepsilon=0}^{\eta\to1}=\frac{1}{2}\log_2\left[\frac{V_M+V_S}{k^2V_M+V_S}\right]$$

Reverse reconciliation protocols can tolerate such leakage to some extent. The key rate (1) in the limit of strong modulation is:

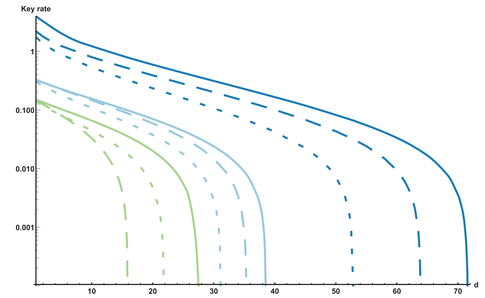
$$R_{RR}|_{V_M\to\infty}=-\frac{1}{2}\log_2\left[\left(1-\eta+\frac{\eta k^2}{V_S(1+k^2)}\right)(1+\eta(V_S-1))\right]$$

To achieve higher performance squeezing must be optimized:

$$V_S^{opt}|_{V_M\to\infty}=\sqrt{\frac{k^2}{1+k^2}}.$$



Performance of squeezed-state protocol with a leakage from the modulator under collective attacks. Key rate dependency on modulation ratio k in the case of excess modulation for different values of squeezing (starting from top) V_S =0.1, 0.3, 0.5, 0.7, 0.9 *SNU*. Solid lines correspond to $V_L = V_S$ i.e. initial state in leakage mode being the same as signal, (thick, orange line represents the protocol with optimized squeezing); dashed lines correspond to V_L = 1 i.e. leakage mode input is vacuum state. β = 95%, channel losses η = 0.1, excess noise ε = 1%, modulation variance V_M is optimized for the given parameters.
Squeezed-state protocol is sensitive, especially for high squeezing, to leakage. (Provided source outputs identical states) Security breaks when leakage is larger than half of signal modulation. Squeezing optimization is beneficial but not sufficient to maintain security for arbitrary amounts of leakage.



Secure distance *d* in a standard telecom fiber (with an attenuation of *−0.2dB/km*) under collective attacks in the case of modulation leakage for different values of ratio between additional and signal states variances k = 0 (blue), 1 (light blue), 1.5 (light green) for optimized squeezed state protocol (solid lines), squeezed-state protocol (dashed lines) $V_{X,L} = V_{X,S}$= 1/2 and coherent state protocol $V_{X,L} = V_{X,S}$= 1 (dotted lines). Modulation variance V_M is optimized for given parameters, excess noise ε = 1%, post-processing efficiency β = 97%.

The distance is shortened by modulation leakage. Squeezing optimization allows to achieve overall longer secure distances. Comparing unoptimized squeezing- and coherent-state protocols, the first one prevails under weak leakage k <1, the latter under stronger leakage k > 1.

CONCLUSIONS

While device- and measurement-device independent QKD protocols remain experimentally challenging and are limited to high transmittance untrusted channels, efficient, robust and stable CV QKD can be realized by proper set-up characterization, identification of possible sources of side information available to an eavesdropper, and taking them into account in security analysis. Side channels on preparation side decrease secure key rate and robusntess to channel noise, however can be tolerated up to some extent, and in some cases their effect can even be fully compensated. Preparation noise and multimode modulation leakage can be security breaking even in purely lossy untrusted channels. Characterization of equipment and consequent optimization of state squeezing and modulation is crucial for secure and efficient key distribution.

REFERENCES

[1] Usenko, Filip, Entropy 18, 20 (2016); [2] Filip, Phys. Rev. A, **77**, 022310 (2008); [3] Usenko, Filip, Phys. Rev. A, **81**, 022318 (2010); [4] Derkach, Usenko, Filip, Phys. Rev. A **93**, 0322309 (2016); [5] Wolf et al., Phys. Rev. Lett. **96**, 080502 (2006); [6] Weedbrook et al., Rev. Mod. Phys. 84, 621 (2012)