SPIE. SECURITY+ DEFENCE

Compensation of side-channel noise infusion on the receiver side in continuous-variable quantum key distribution

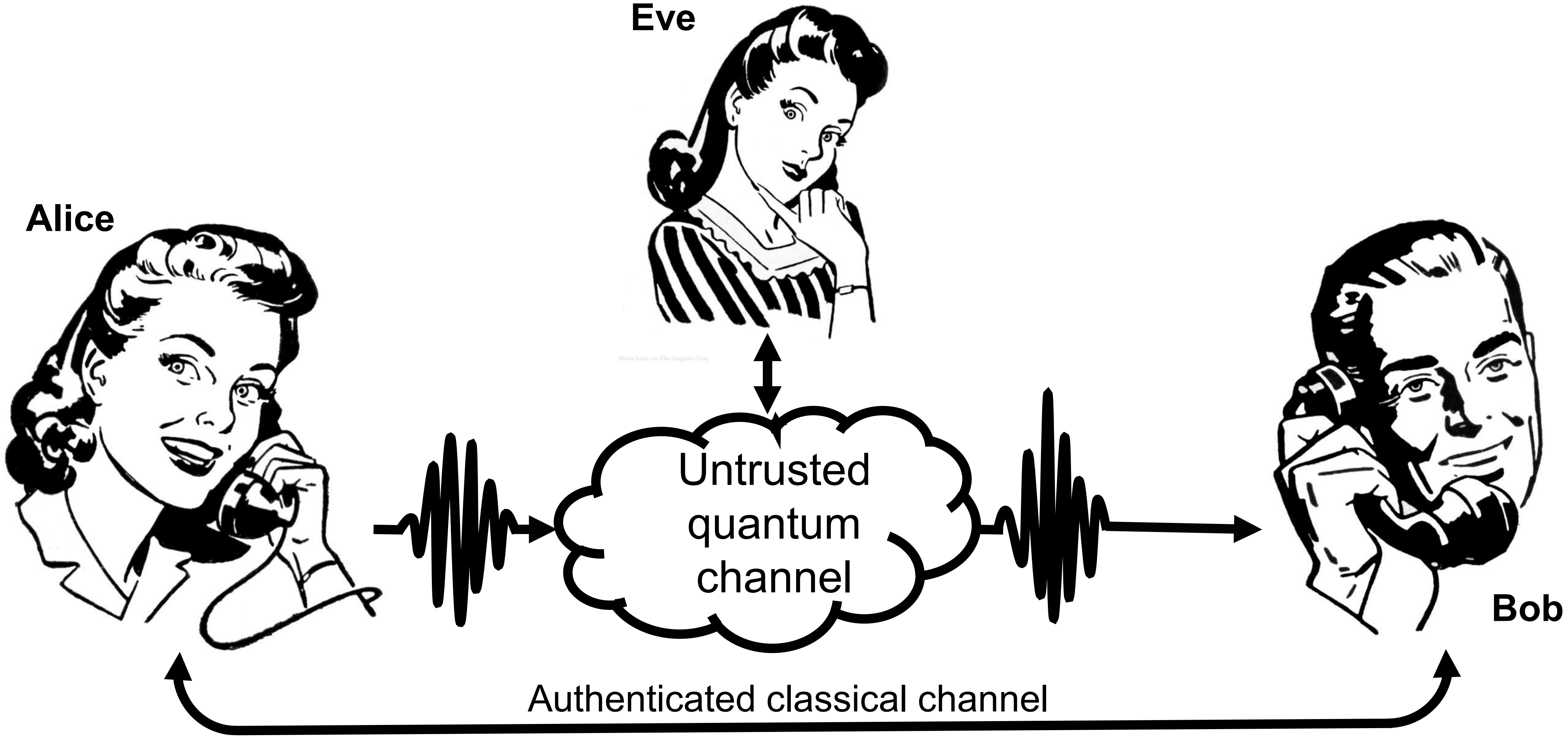
Ivan Derkach, Vladyslav C. Usenko, Radim Filip,

Department of Optics, Palacký University, Olomouc, Czech Republic

Outline

- Motivation
- Definition and types of side channels
- Side channel negative effects
- Decoupling of information leakage on sender side
- Decoupling of noise infusion on receiver side
- Summary

Quantum key distribution



Imperfections

- Trusted preparation noise can break the security in reverse reconciliation protocol [1], but can be purified [2] or tolerated in the direct reconciliation scheme [3, 4]

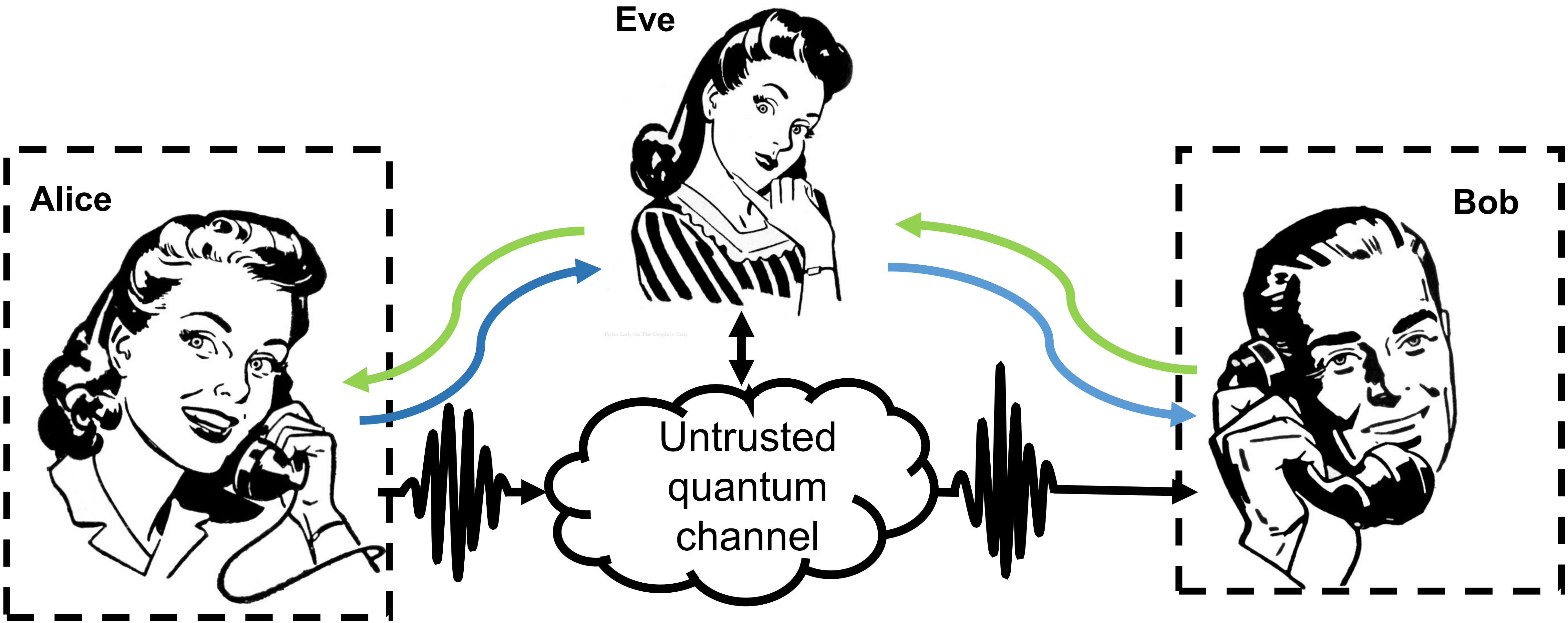
[15] R. Filip, Phys. Rev. A 77, 022310 (2008).
[16] V. C. Usenko, and R. Filip Phys. Rev. A 81, 022318 (2010).
[17] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. 105, 110501 (2010)
[18] C. Weedbrook, S. Pirandola, T. C. Ralph Phys. Rev. A 86, 022318 (2012)

Imperfections

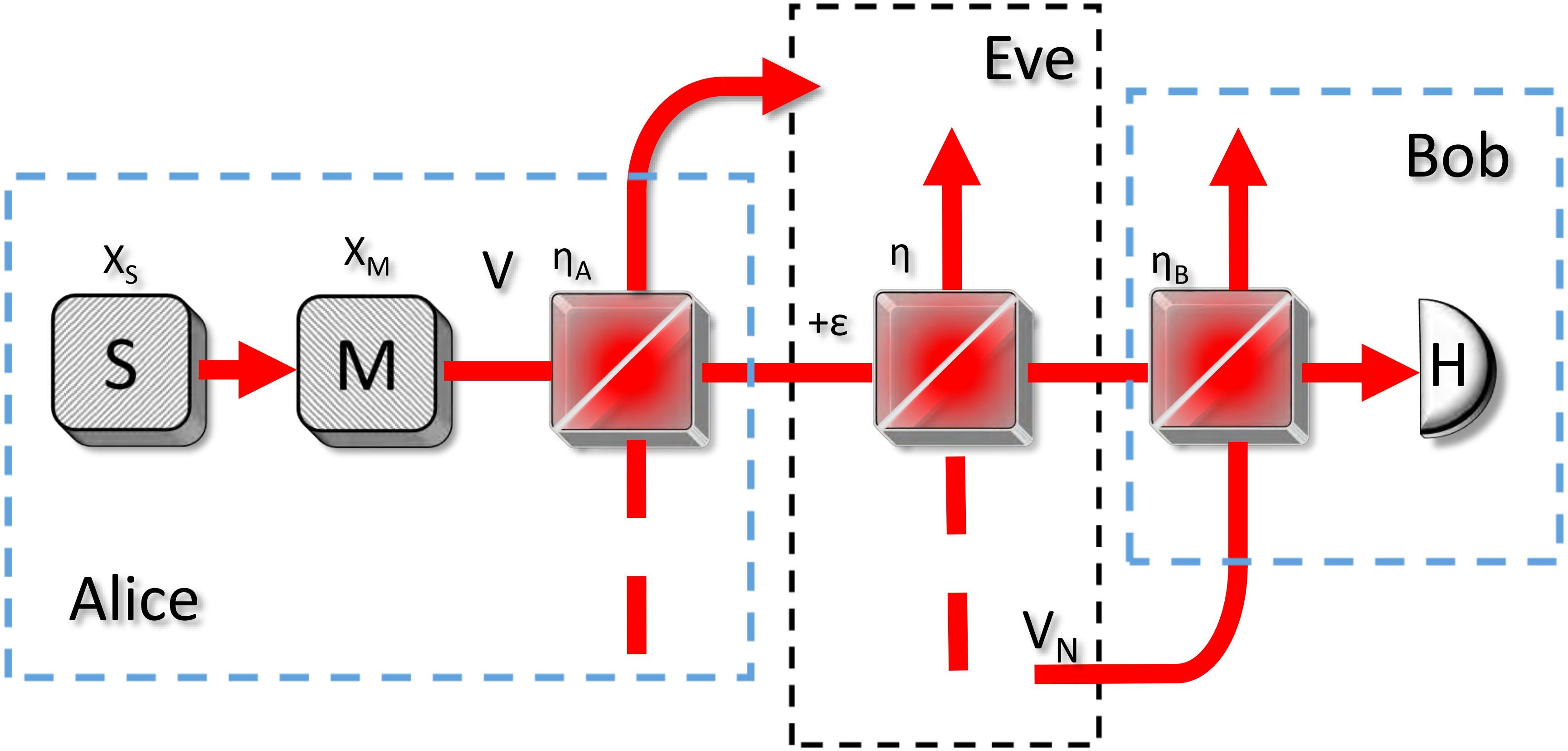
- Trusted preparation noise can break the security in reverse reconciliation protocol [1], but can be purified [2] or tolerated in the direct reconciliation scheme [3, 4]
- Trusted detection noise limits the key rate, but can be partially helpful to make the protocol more robust against the noise in the quantum channel [5]

[15] R. Filip, Phys. Rev. A 77, 022310 (2008).
[16] V. C. Usenko, and R. Filip Phys. Rev. A 81, 022318 (2010).
[17] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. 105, 110501 (2010)
[18] C. Weedbrook, S. Pirandola, T. C. Ralph Phys. Rev. A 86, 022318 (2012)
[5] R. García-Patron, N. J. Cerf, Phys. Rev. Lett. 102, 130501 (2009)

Quantum key distribution



Side channels



S – source (laser/OPO)
M – quadrature modulator
η - untrusted channel loss
ε – untrusted channel excess noise
H – homodyne detector

Side channels negative effect

Key rate for individual attacks:

$$K_{ind} = \beta I_{AB} - I_{BE}$$

Key rate for collective attacks:

$$K_{col} = \beta I_{AB} - \chi_{BE}$$

Mutual information

Sender-side loss

$$I_{AB} = \frac{1}{2}\log_2 \frac{1}{1 - \frac{\eta_A \eta V_M}{\eta_A \eta (V-1) + 1}}$$

$$I_{BE} = \frac{1}{2}\log_2 \frac{[\eta_A \eta (V-1) + 1][V - \eta_A \eta (V-1)]}{V}$$

$$K_{V\to\infty} = \log_2 \frac{1}{1 - \eta_A \eta}$$

Receiver-side noise infusion

$$I_{AB} = \frac{1}{2}\log_2 \frac{1}{1 - \frac{\eta_B \eta V_M}{\eta_B(\eta V + 1 - \eta) + (1-\eta_B)V_N}}$$

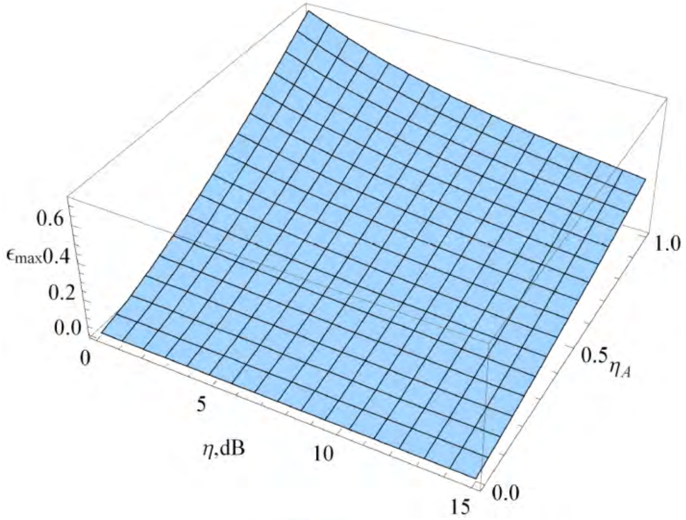
$$I_{BE} = \frac{1}{2}\log_2 \frac{\eta_B(\eta V + 1 - \eta) + (1-\eta_B)V_N}{\frac{\eta_B V}{\eta + (1-\eta)V} + \frac{1-\eta_B}{V_N}}$$

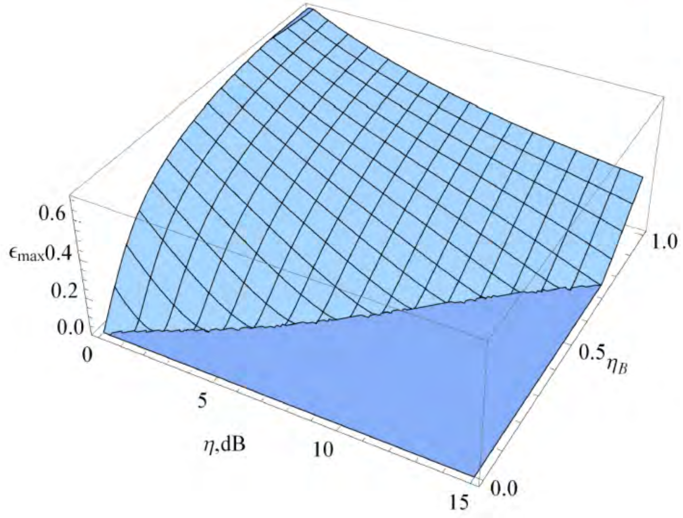
$$V_N^{max}\Big|_{\eta\to 0}^{V\to\infty} = \frac{1}{1-\eta_B}$$

Side channels negative effect

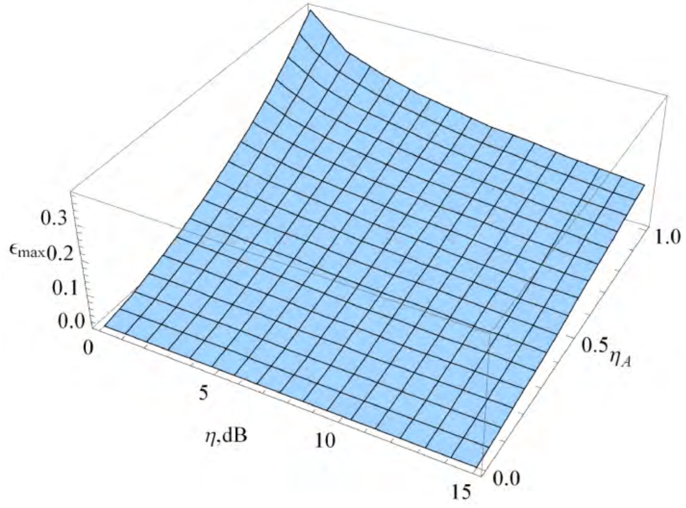
Leakage on the sender side | Noise infusion on the receiver side

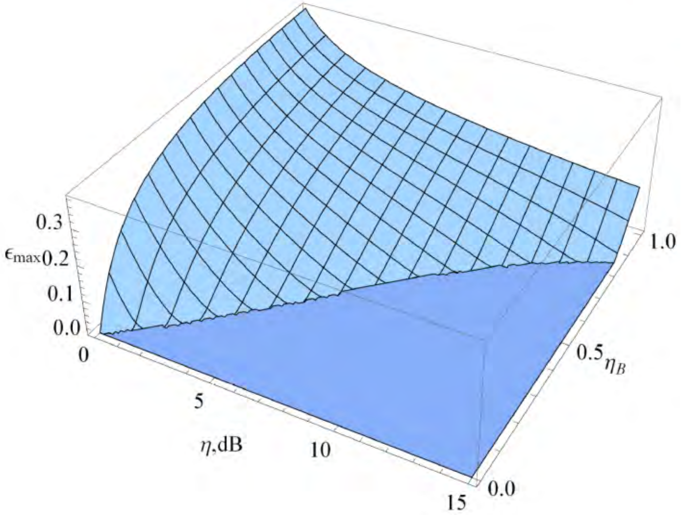
Squeezed-state protocol





Coherent-state protocol



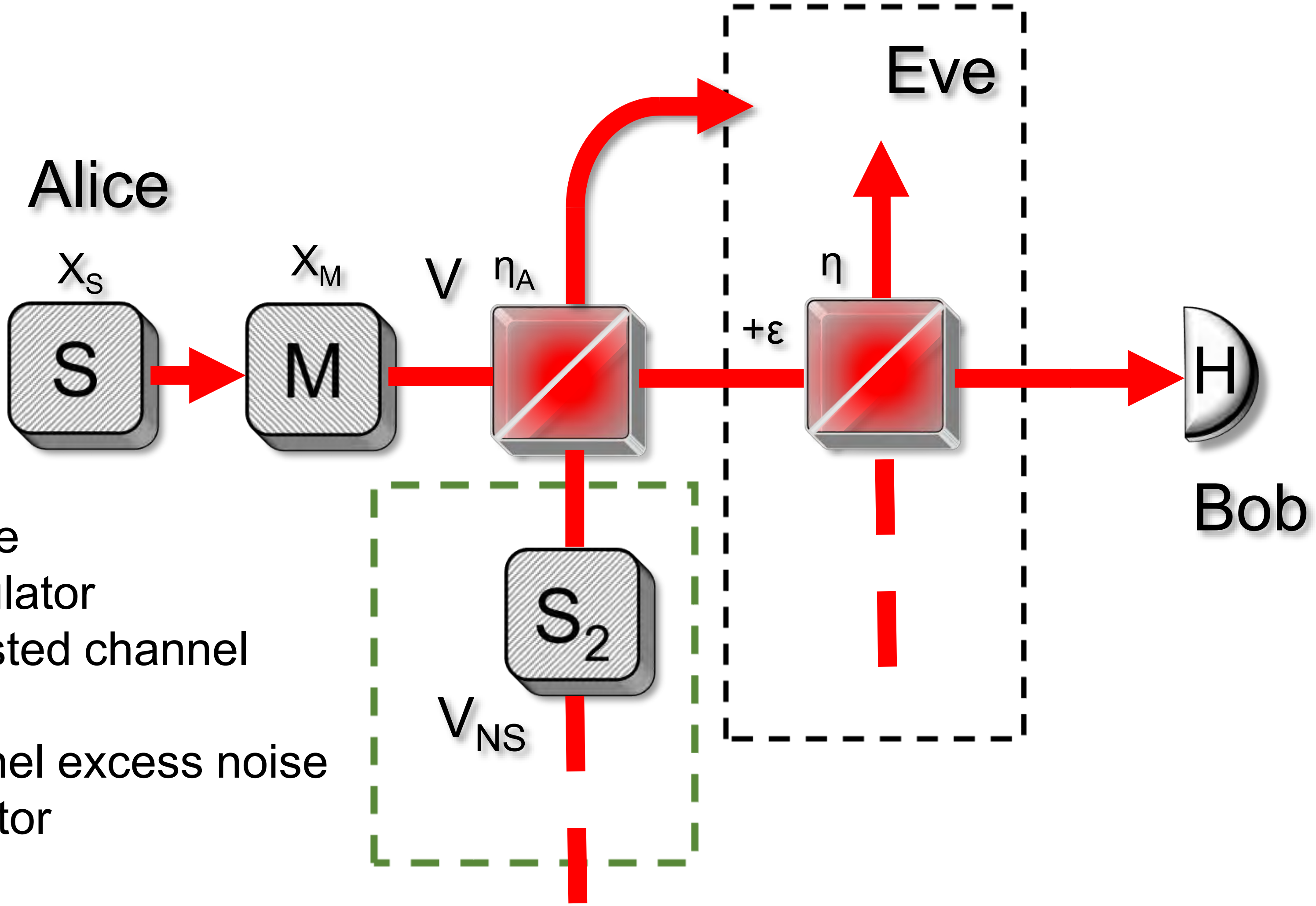


Side channels undermine the tolerance of the protocol to the channel noise ε.

Noise infusion on the receiver side leads to security break !

Decoupling of the type-A side channel

Leakage on the sender side

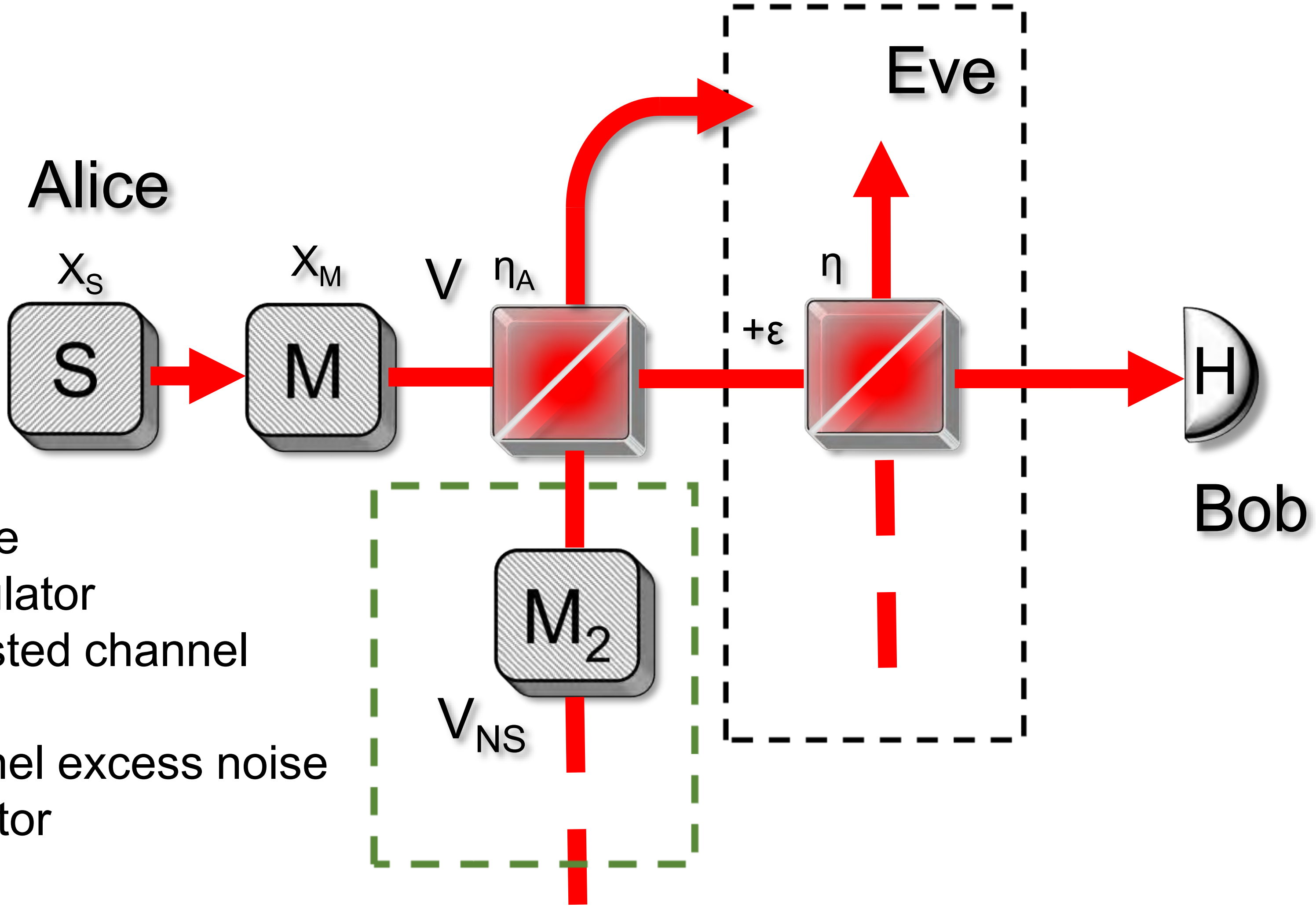


Alice replaces vacuum input of the side channel with the source of a Gaussian thermal noise (noise is unknown by definition).
Holevo bound is reduced, but mutual information between trusted parties is reduced as well.

S - source
M - modulator
η - untrusted channel loss
ε – channel excess noise
H - detector

Decoupling of the type-A side channel

Leakage on the sender side

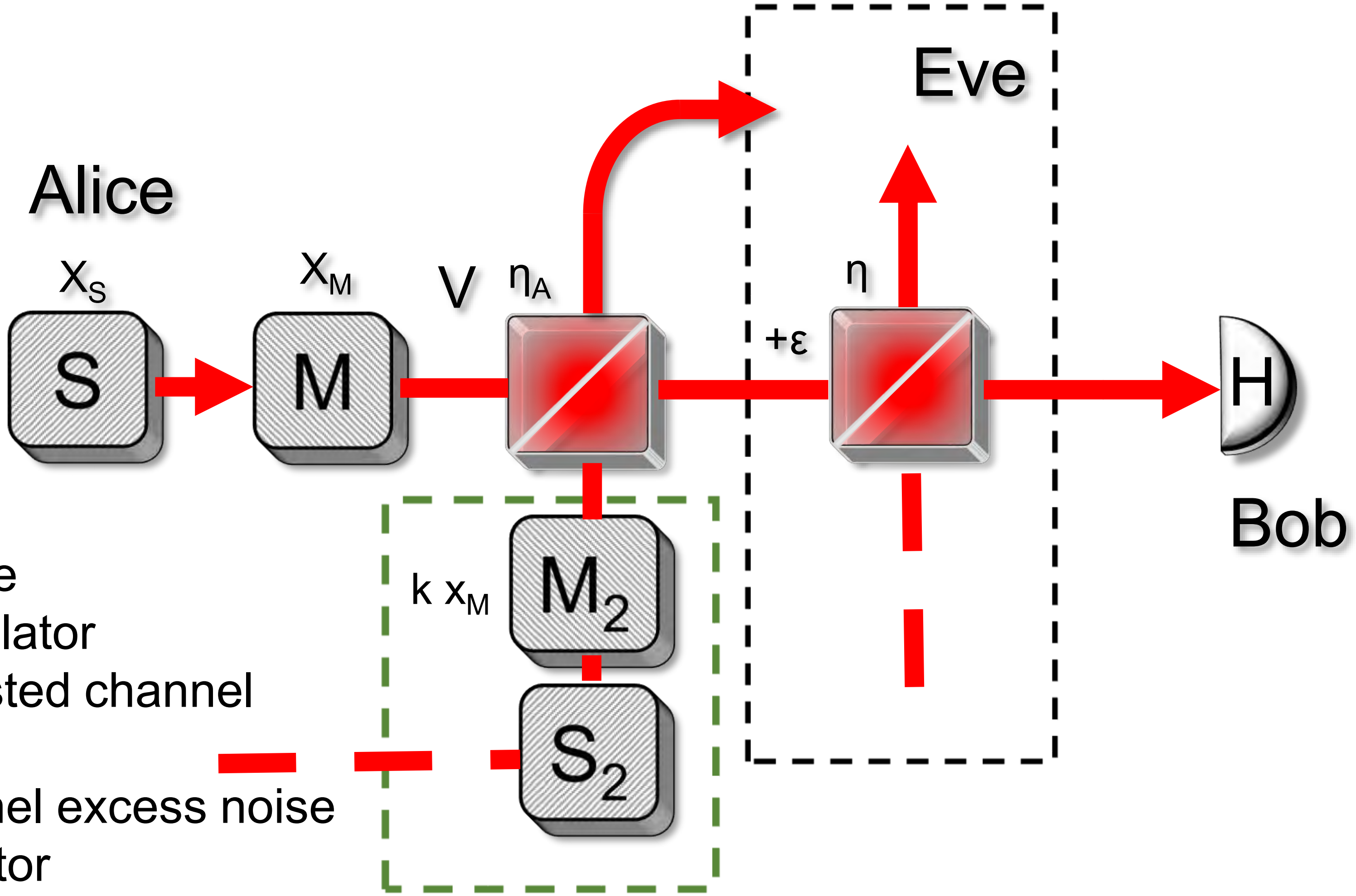


S - source
M - modulator
η - untrusted channel loss
ε – channel excess noise
H - detector

Alice replaces vacuum input of the side channel with modulator.
The modulation is independent from the main modulation but contributes to the trusted-side data and to correlation with the receiver.
Mutual information between trusted parties is increased, but the information leakage from the main channel is increased as well.

Decoupling of the type-A side channel

Leakage on the sender side



S - source
M - modulator
η - untrusted channel loss
ε – channel excess noise
H - detector

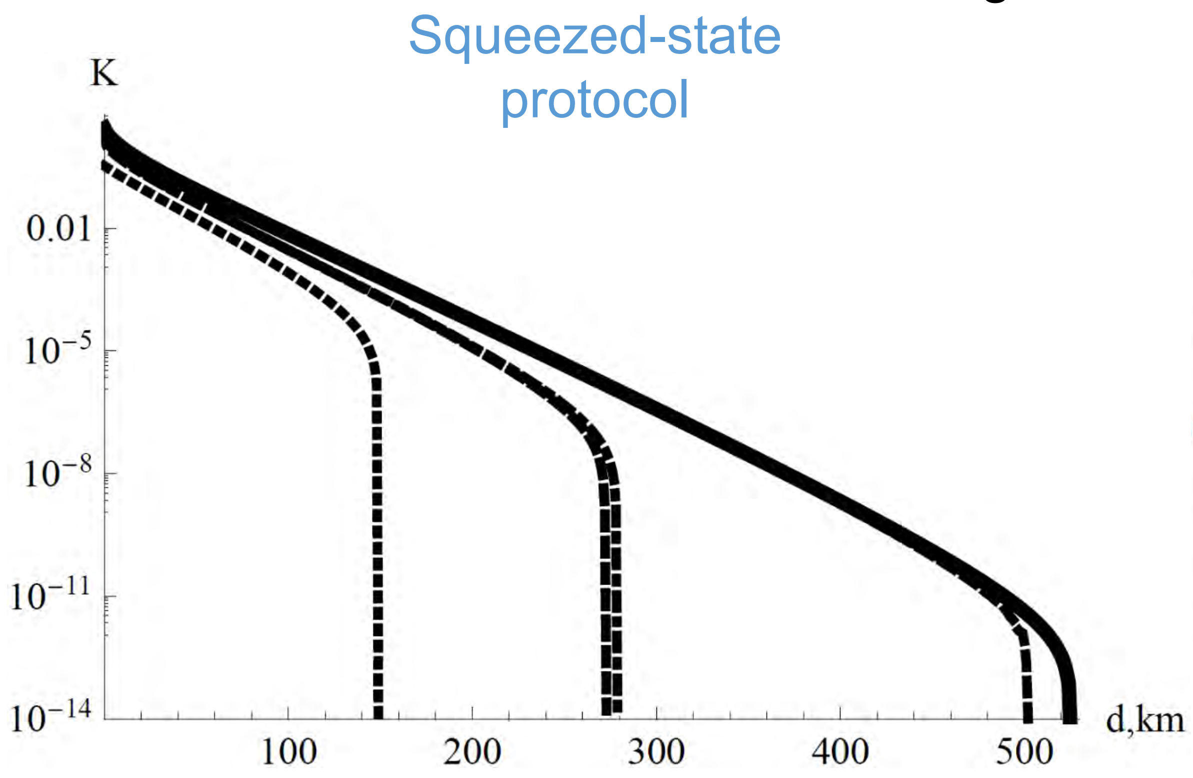
Alice replaces vacuum input of side channel with modulator. The modulation is correlated to the main modulation performed on the signal, and optionally squeezed.

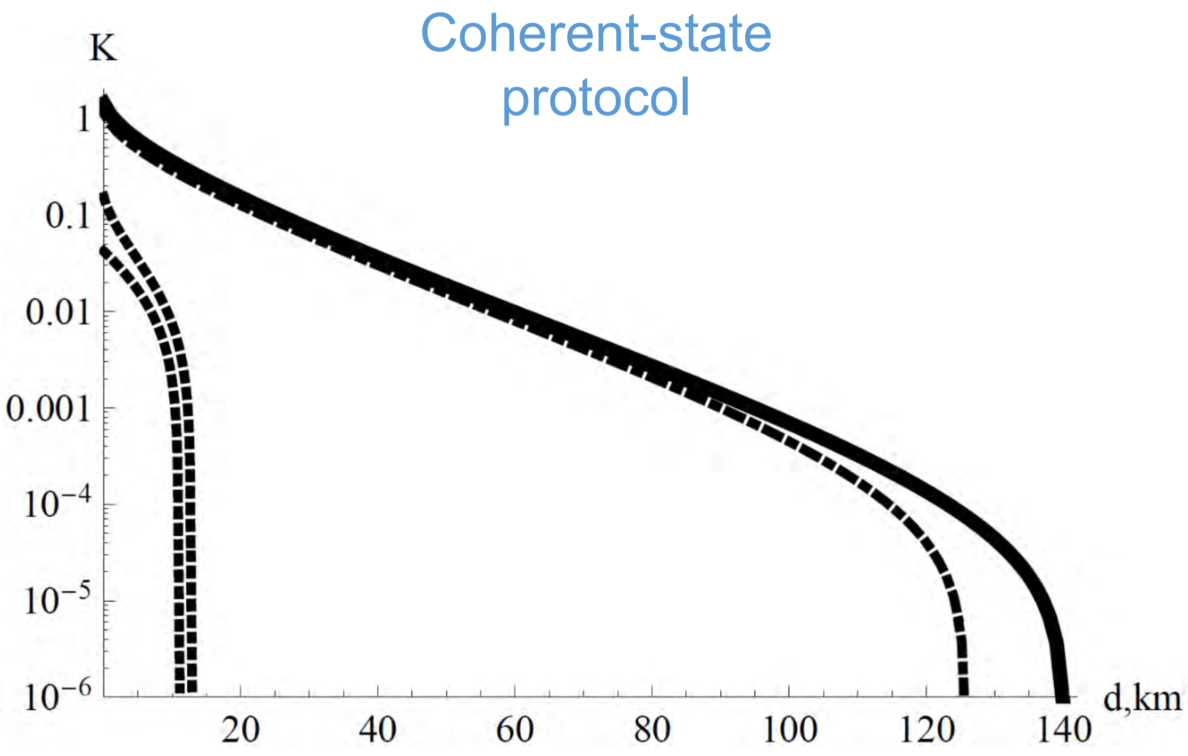
$$k_{opt} = \sqrt{(1-\eta_A)/\eta_A}$$

Optimal correlated modulation shifts side-channel attack from the modulated signal to signal state before modulation. Optimizing the parameters allows to **completely decouple and decorrelate** side channel output from the signal mode.

Lower bound on the key rate

Leakage on the sender side

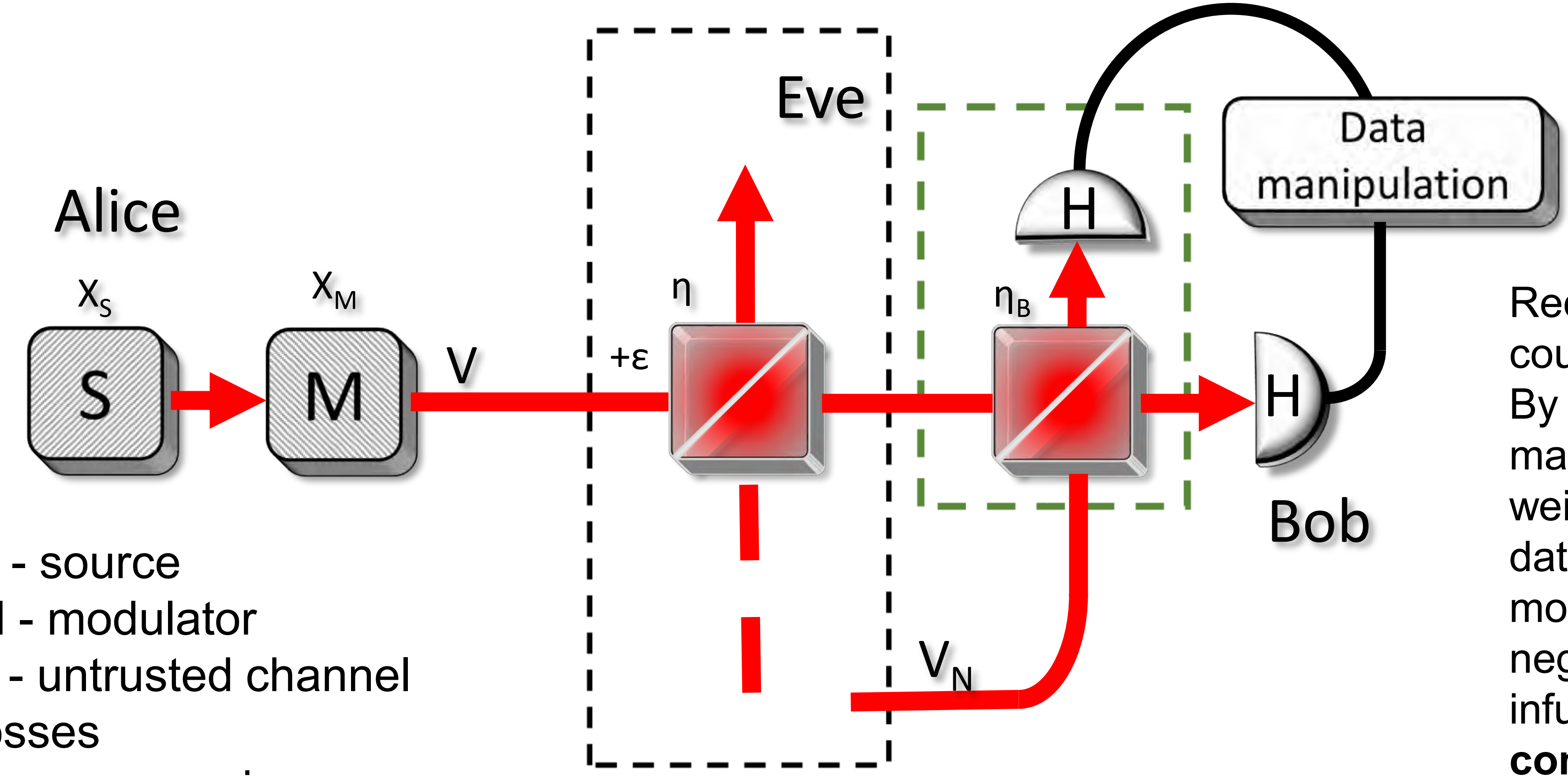




Channel losses: −0.2dB/km, Reconciliation algorith effiency: 95%, Untrusted channel excess noise: 5%, sender side side channel coupling: 0.4, Modulation variance is optimized for given parameters.

Decoupling of the type-B side channel

Noise infusion on the receiver side



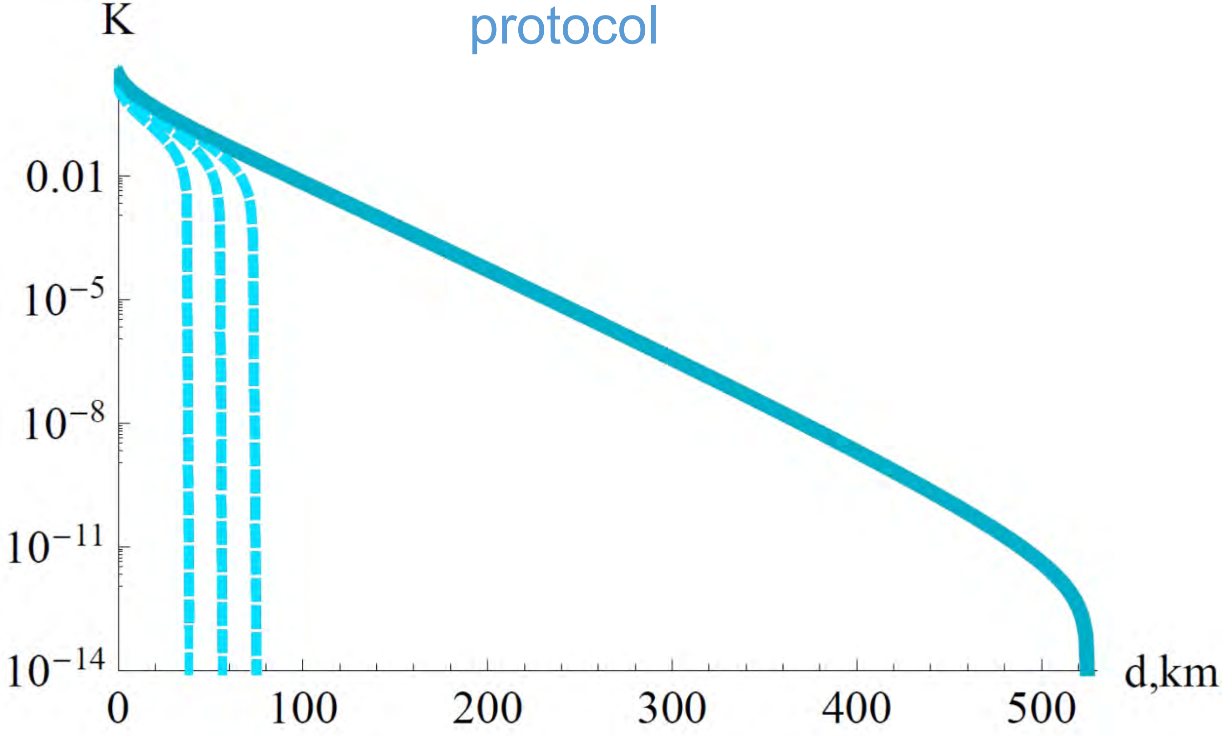
S - source
M - modulator
η - untrusted channel losses
ε - excess noise
H - detector

Receiver can monitor the coupling output.
By applying proper manipulation (optimally weighed subtraction) on the data from the main and the monitoring detector the negative influence of the noise infusion can be **fully compensated**.

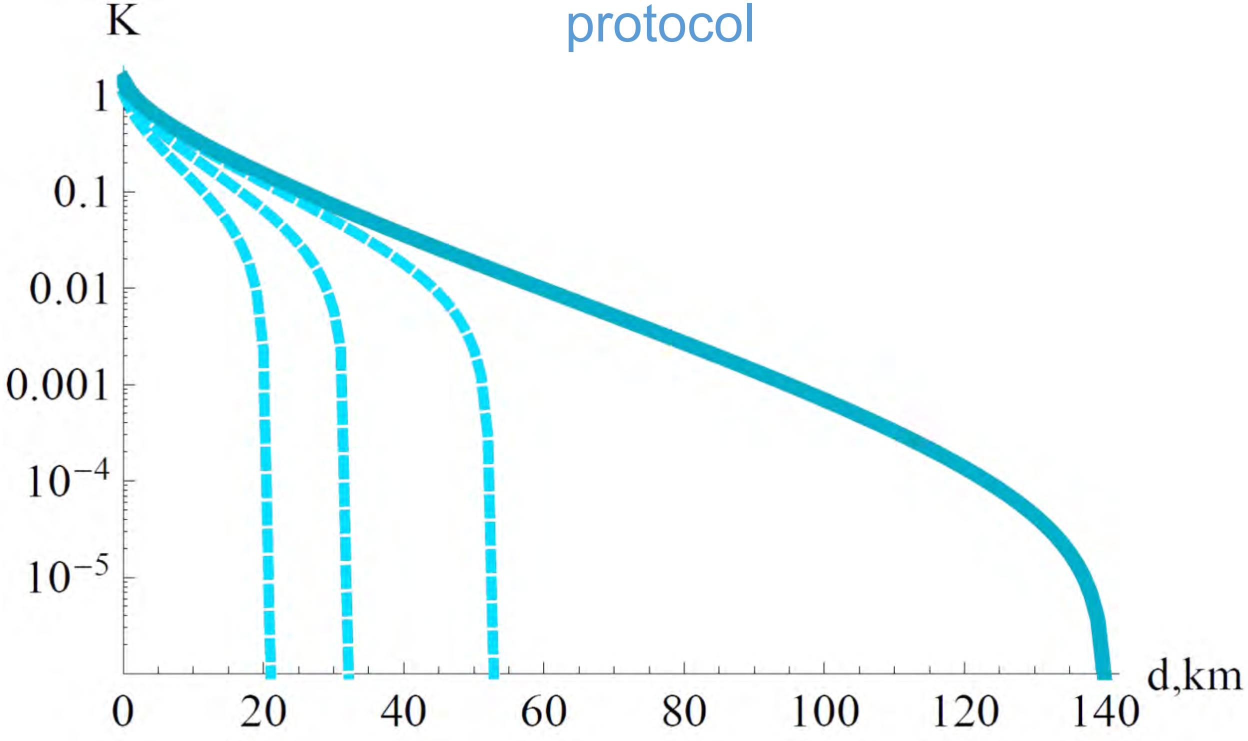
Lower bound on the key rate

Noise infusion on the receiver side

Squeezed-state protocol



Coherent-state protocol



Channel losses: −0.2dB/km, Reconciliation algorith effiency: 95%, Untrusted channel excess noise: 5%, Receiver side noise infusing side channel coupling: 0.5, 0.7, 0.9, Infused noise variance: 1.05

Summary

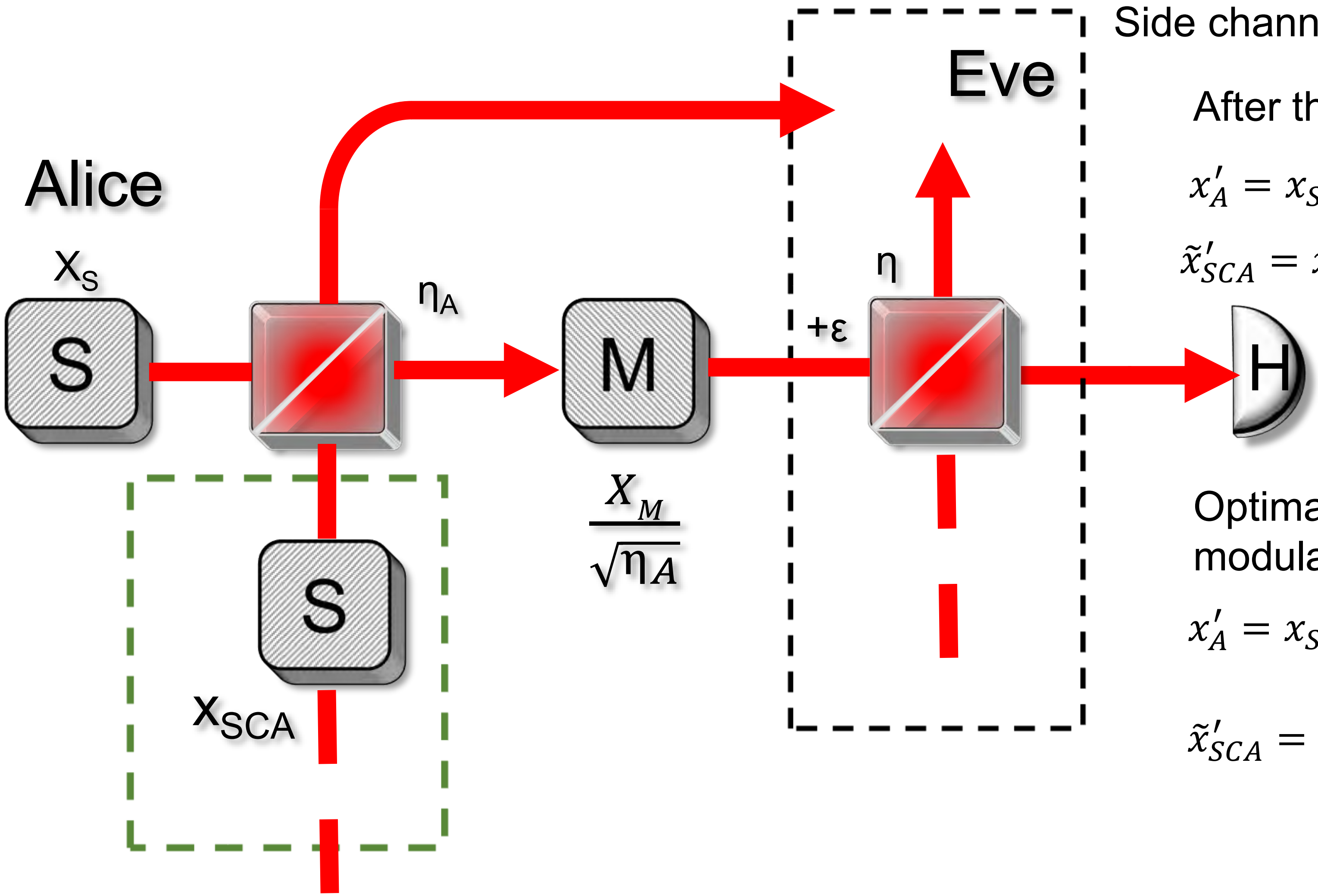
- Information leakage on the sender side decreases the key rate and increases sensitivity of the protocol to the channel noise. However by applying additional modulation and optionally squeezing to the input of side channel the negative impact can be decreased or even eliminated completely.

- Noise infusion on sender side can completely break the security of the protocols even upon pure channel loss. Nevertheless introduction of proper monitoring on the output of side channel allows to fully compensate the negative influence.

Thank you for your attention!

Work supported by projects: FP7 BRISQ2 and 13-27533J of Czech Science Foundation

Sender-side side channel decoupling



Side channel A input: $x'_{SCA} = x_{SCA} + \mathrm{k}x_M$

After the coupling:

$$x'_A = x_S\sqrt{\eta_A} + x_{SCA}\sqrt{1-\eta_A} + x_M\left(\sqrt{\eta_A} + k\sqrt{1-\eta_A}\right)$$

$$\tilde{x}'_{SCA} = x_{SCA}\sqrt{\eta_A} - x_S\sqrt{1-\eta_A} + x_M\left(k\sqrt{\eta_A} - \sqrt{1-\eta_A}\right)$$

$$k = \sqrt{{(1-\eta_A)}/{\eta_A}} \equiv k_{opt}$$

Optimal correlated modulation effect:

$$x'_A = x_S\sqrt{\eta_A} + x_{SCA}\sqrt{1-\eta_A} + {x_M}/{\sqrt{\eta_A}}$$

$$\tilde{x}'_{SCA} = x_{SCA}\sqrt{\eta_A} - x_S\sqrt{1-\eta_A}$$

Receiver-side side channel decoupling

After noise infusion: $x'_B = x_B\sqrt{\eta_B} + x_{SCB}\sqrt{1-\eta_B}$

$$x'_{SCB} = -x_B\sqrt{1-\eta_B} + x_{SCB}\sqrt{\eta_B}$$

Weighed subtraction: $\Delta x = g x'_B - g' x'_{SCB}$

g=$\sqrt{\eta_B}$ g'=$\sqrt{1-\eta_B}$

$$\Delta x = x_B$$