Quantum control attack: Towards joint estimation of protocol and hardware loopholes

«Most deadly errors arise from obsolete assumptions»
Frank Herbert, Children of Dune

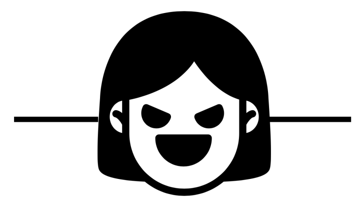
Anton Kozubov
Department of Mathematical Methods for Quantum Technologies,
Steklov Mathematical Institute of Russian Academy of Sciences;
Laboratory of Quantum Processes and Measurements, ITMO University

Kozubov A., Gaidash A., Miroshnichenko G. Quantum control attack: Towards joint estimation of protocol and hardware loopholes // Physical Review A. – 2021. – T. 104. – No. 2. – C. 022603.

Outline

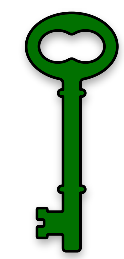
- Introduction
- Problem
- Description of the attack
- Example
- Fake-state attack
- Security notation

Preliminaries: Basic definitions



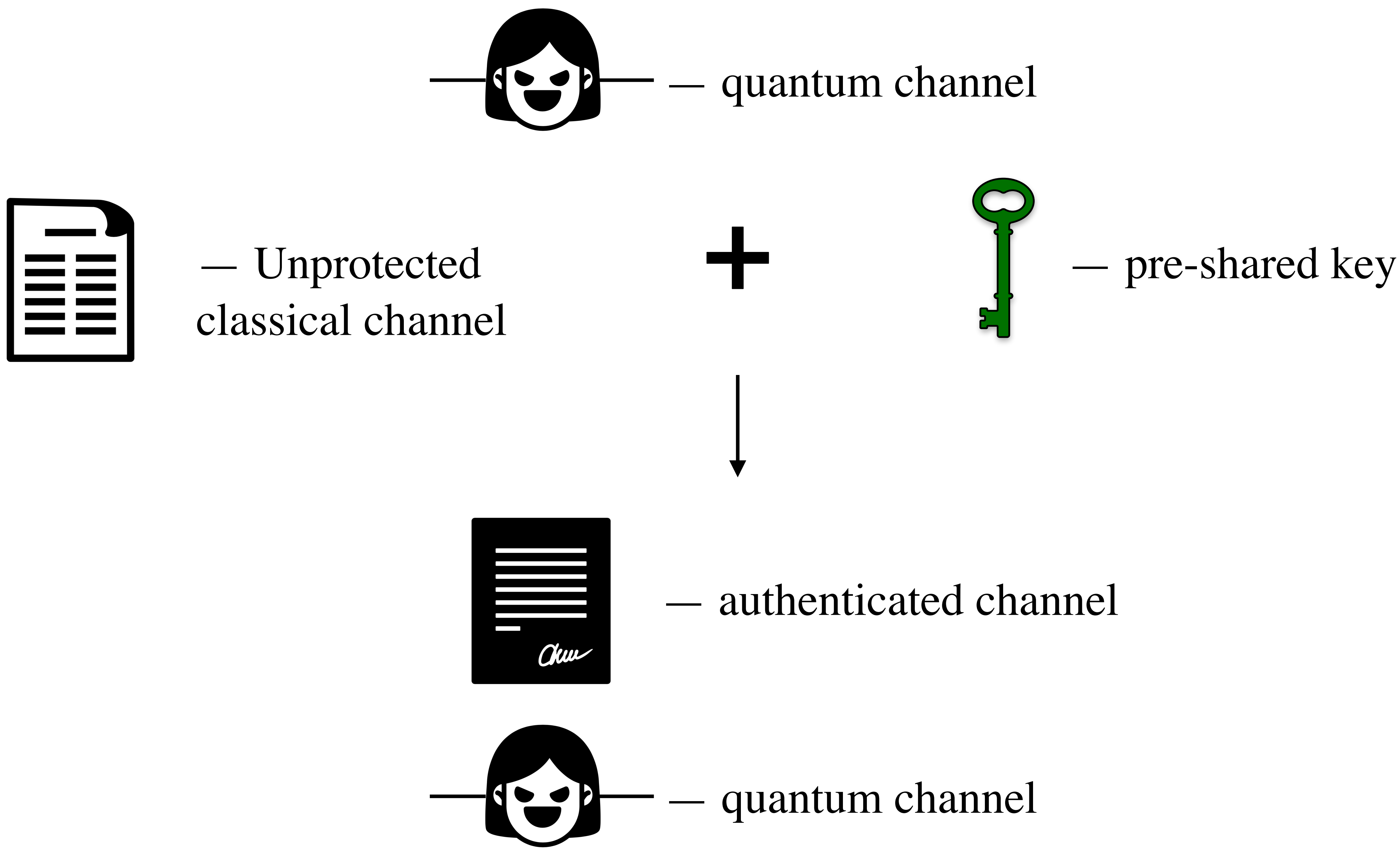
— quantum channel

— Unprotected classical channel

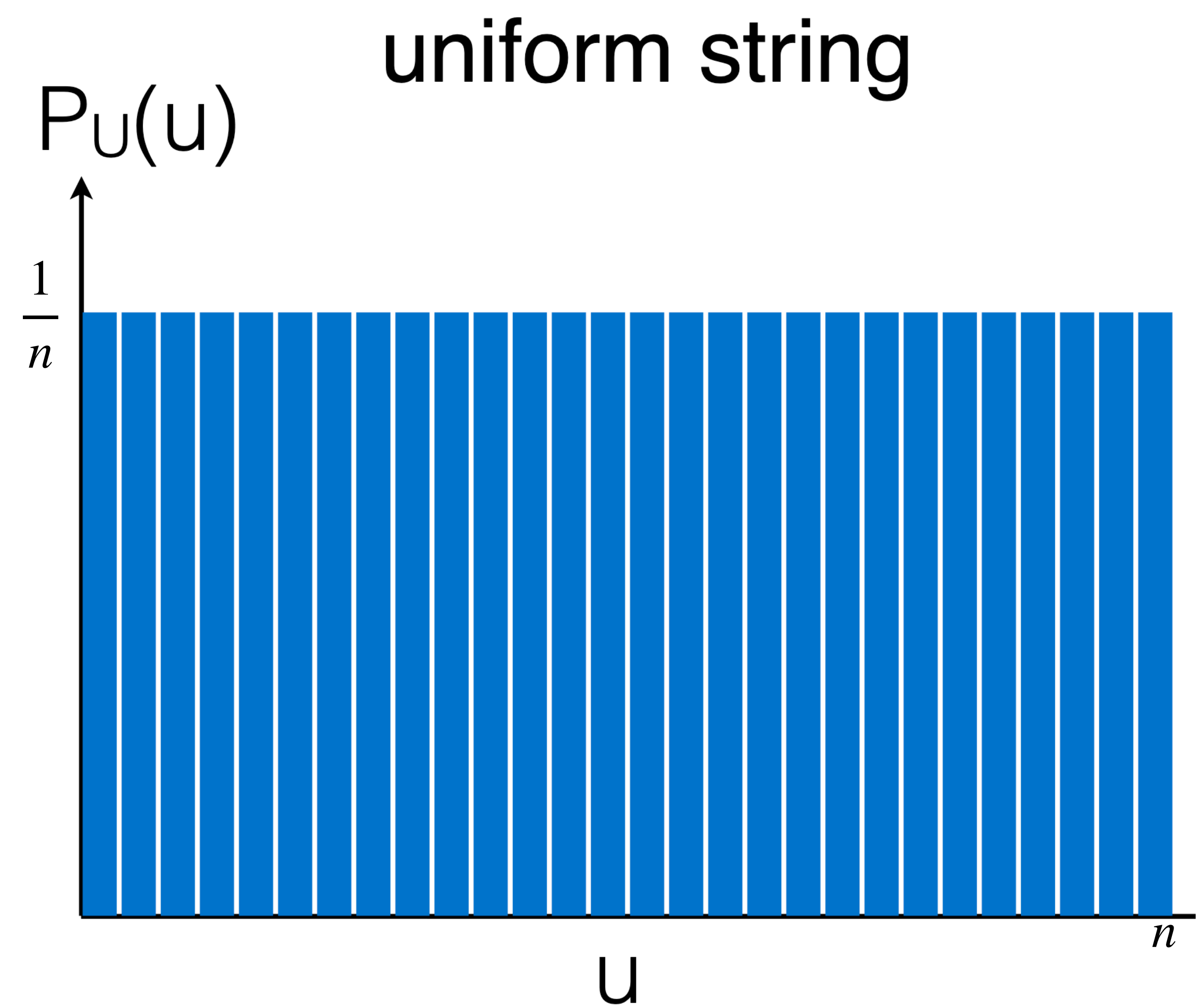


— pre-shared key

Preliminaries: Basic definitions



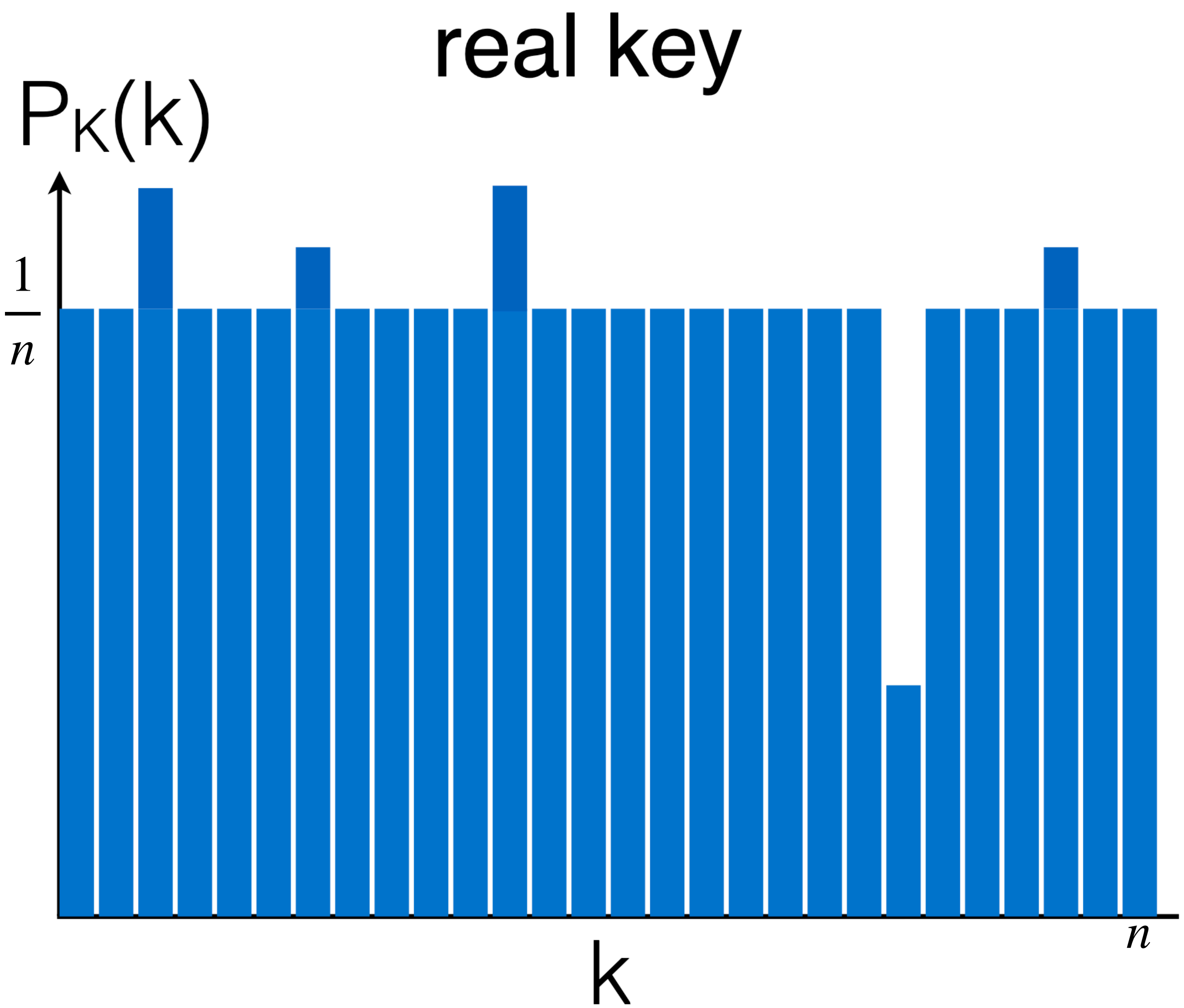
Preliminaries: ideal vs. real key

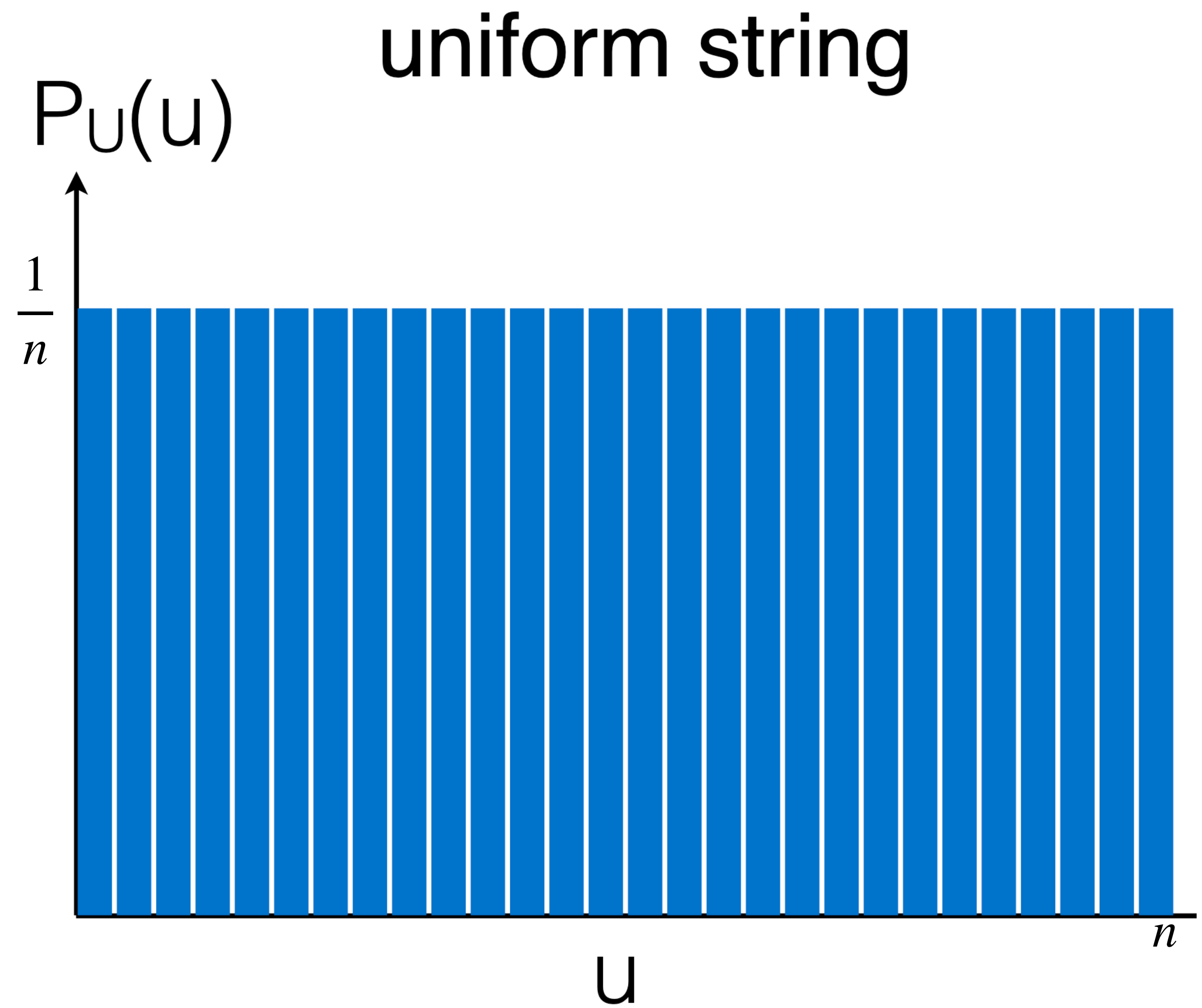


ε is trace distance between probability distribution of real key K and uniformly distributed string U.

Renato Renner, Tutorial: Finite size effect in QKD, QCrypt 2018

Preliminaries: ideal vs. real key

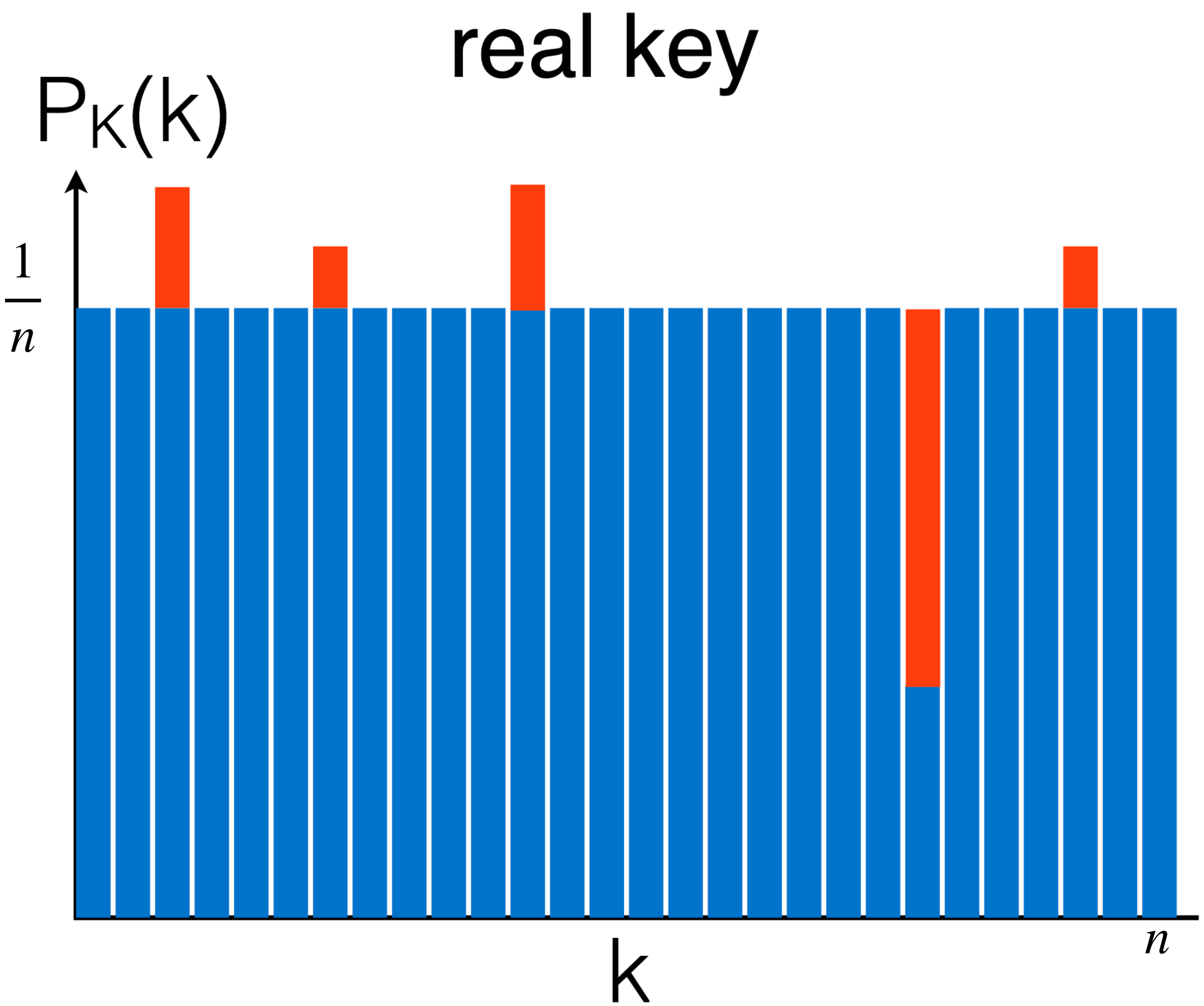


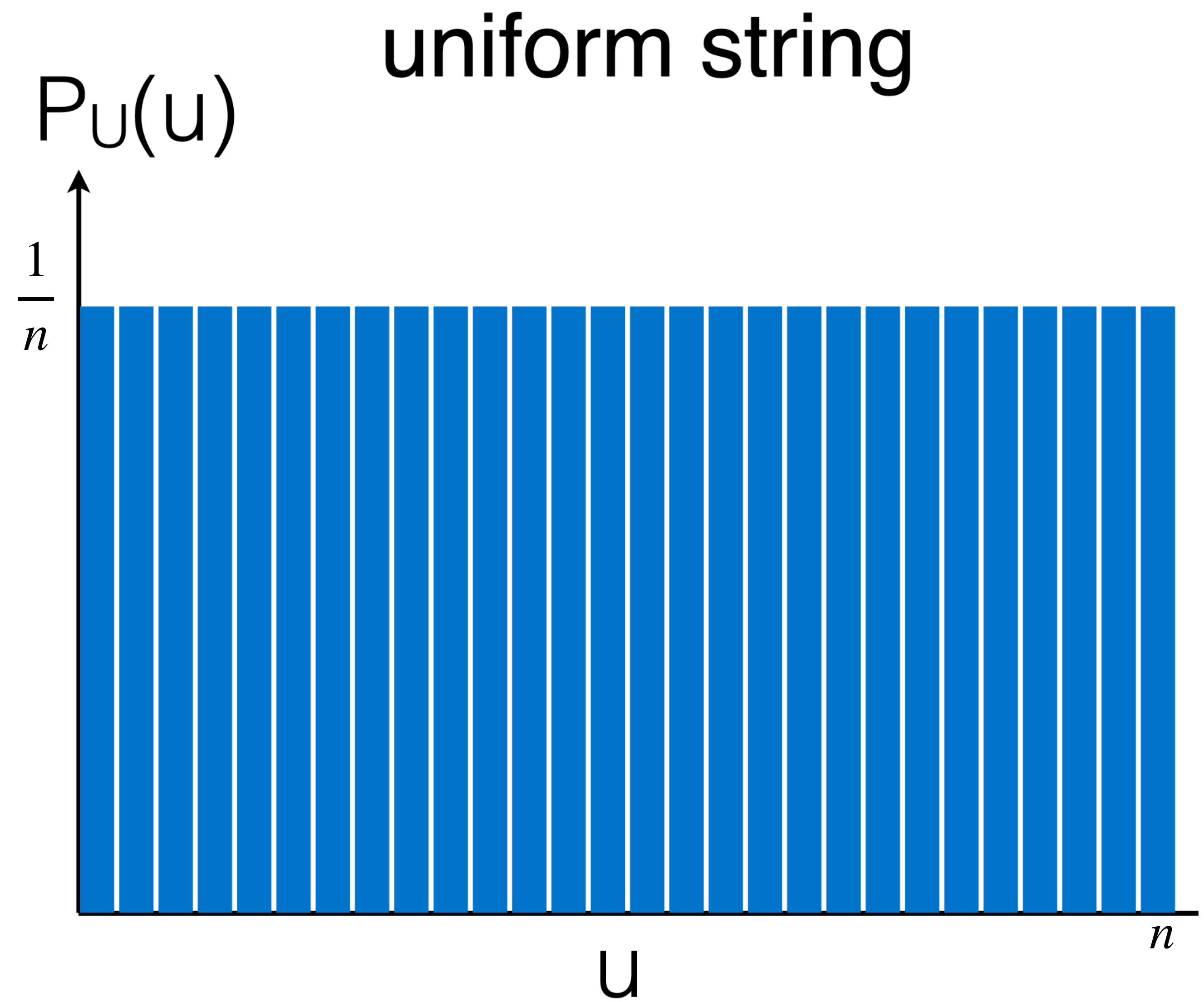


ε is trace distance between probability distribution of real key K and uniformly distributed string U.

Renato Renner, Tutorial: Finite size effect in QKD, QCrypt 2018

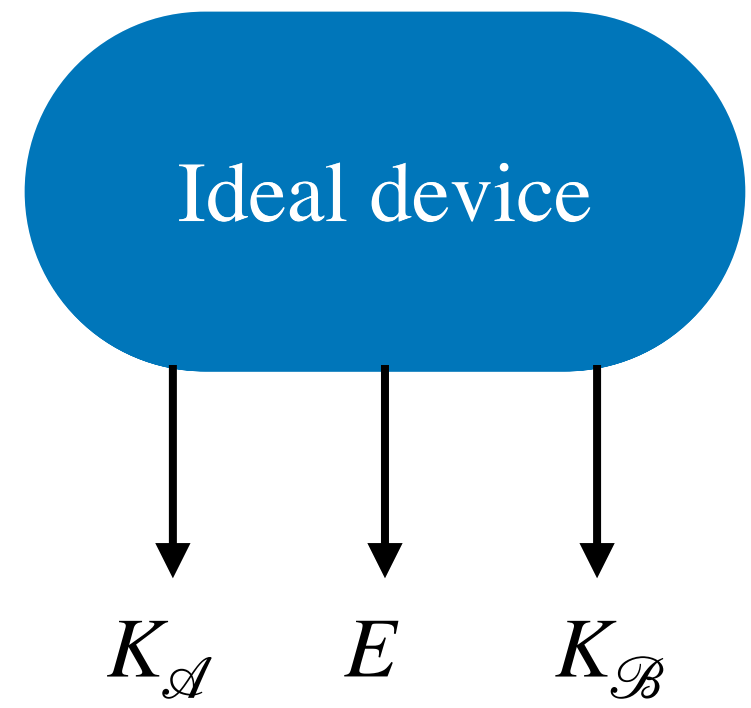
Preliminaries: ideal vs. real key





ε corresponds to weight of red area

Preliminaries: ideal vs. real world



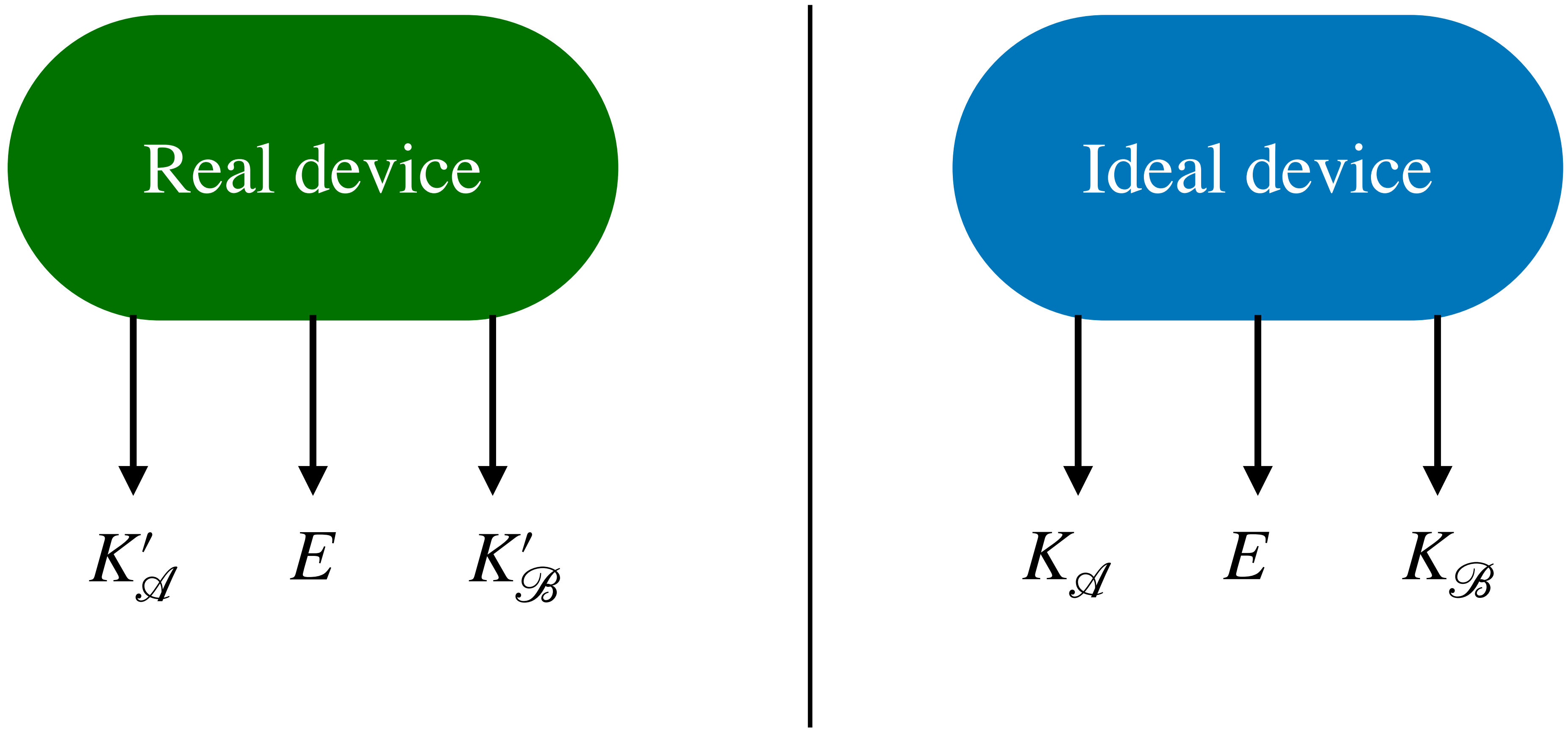
Ideal device properties:

1. Correctness: $K_{\mathscr{A}} = K_{\mathscr{B}} = K$, where K is ideal key
2. Secrecy: K should be uniformly distributed and independent of E

$$H(K|E) = 1$$

Renato Renner, Tutorial: Finite size effect in QKD, QCrypt 2018

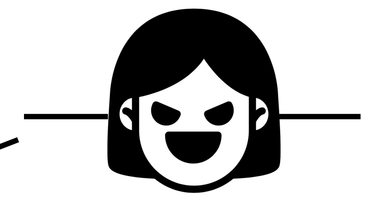
Preliminaries: ideal vs. real world



How close is our real device to the ideal one?

$$d = ||\rho_{K'E} - \omega_K \otimes \sigma_E||_1 \leq \varepsilon$$

Preliminaries: Basic loopholes



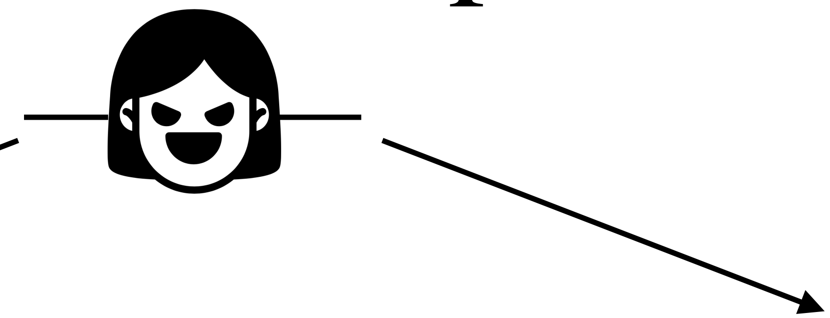
Protocol loopholes

Can be considered as attacks on quantum states in the quantum channel

Hardware loopholes

Can be considered as attacks on utilized hardware

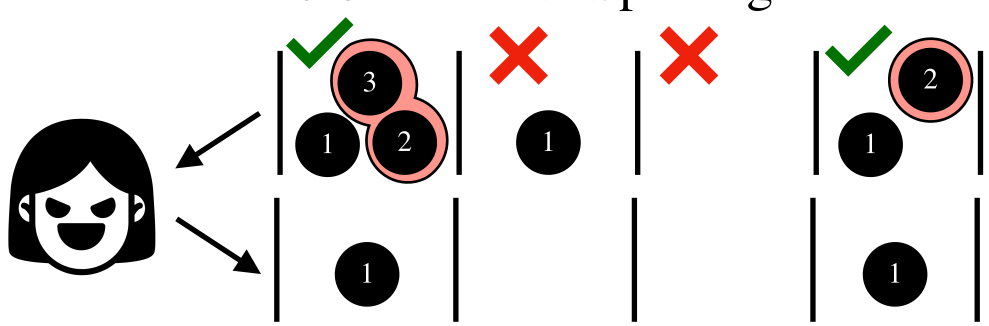
Preliminaries: Basic loopholes



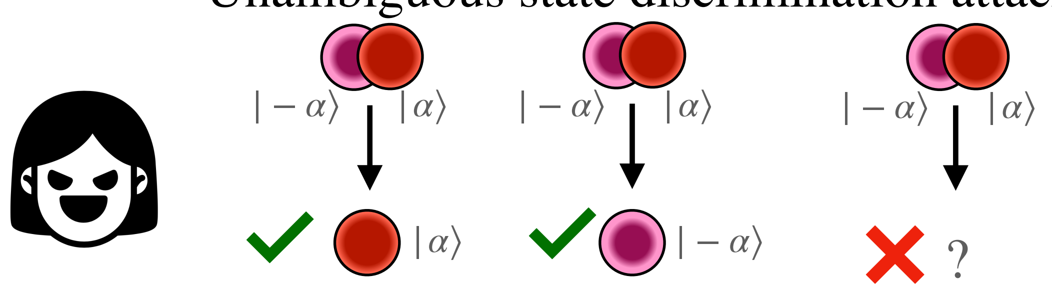
Protocol loopholes

Can be considered as attacks on quantum states in the quantum channel

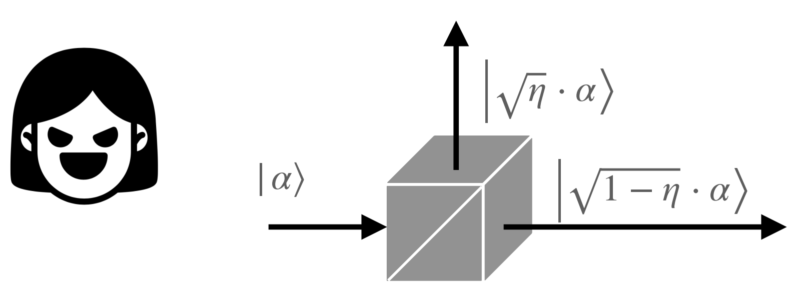
Photon Number Splitting attack



Unambiguous state discrimination attack



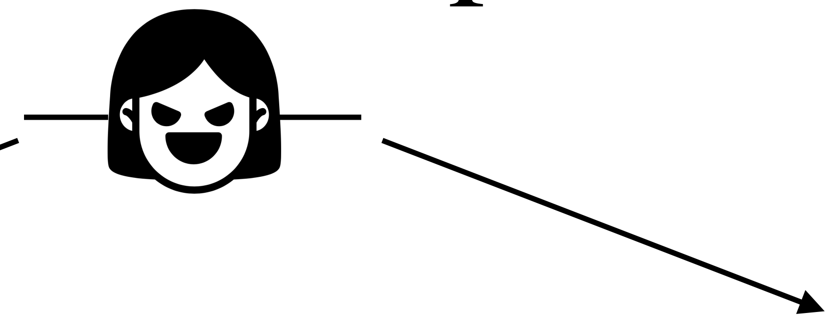
Beam splitting attack



Hardware loopholes

Can be considered as attacks on utilized hardware

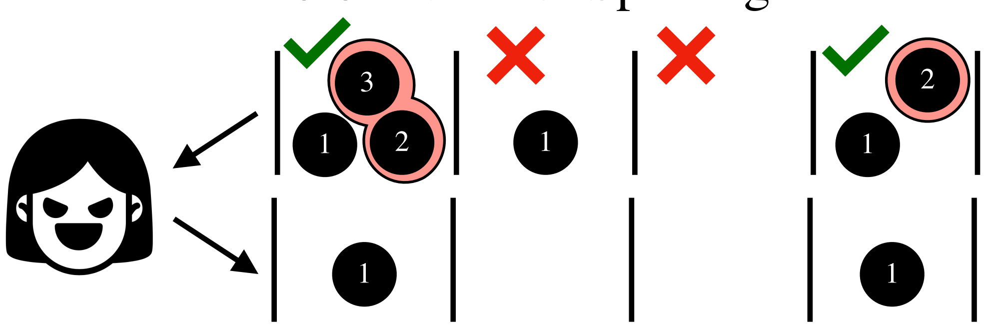
Preliminaries: Basic loopholes



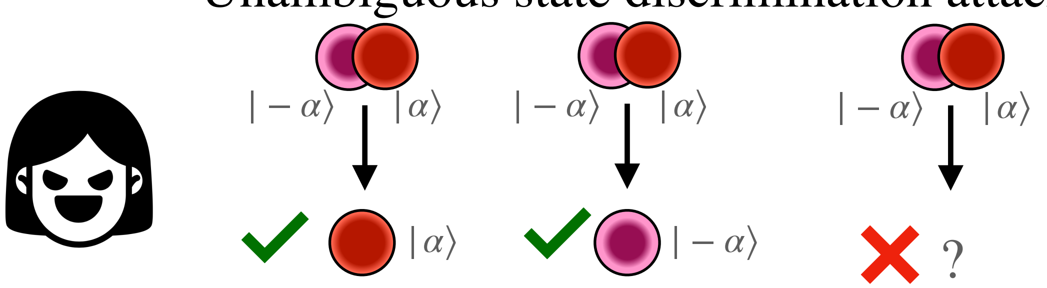
Protocol loopholes

Can be considered as attacks on quantum states in the quantum channel

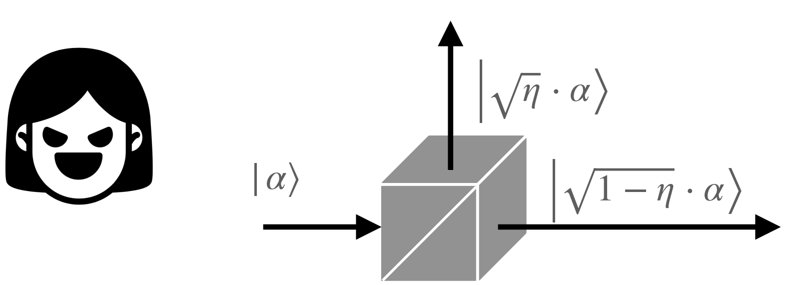
Photon Number Splitting attack



Unambiguous state discrimination attack



Beam splitting attack



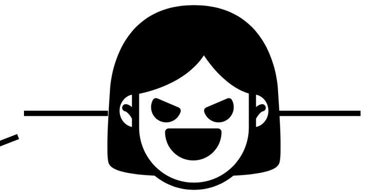
Hardware loopholes

Can be considered as attacks on utilized hardware

Non-ideal equipment

Flawed devices

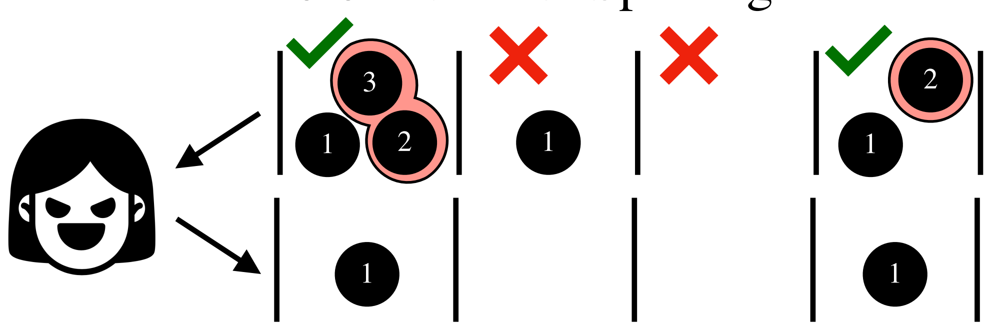
Preliminaries: Basic loopholes



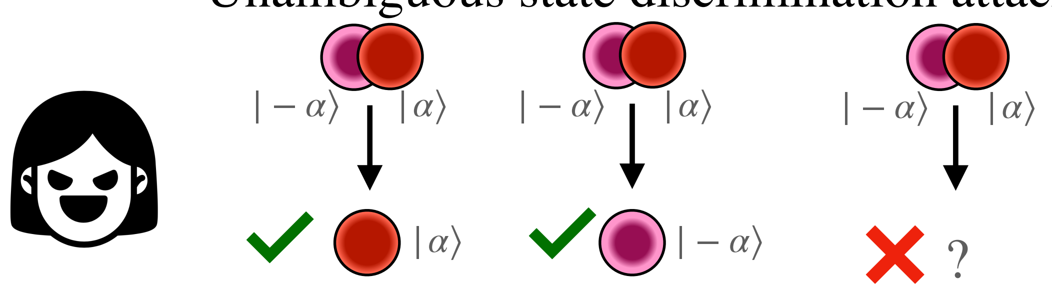
Protocol loopholes

Can be considered as attacks on quantum states in the quantum channel

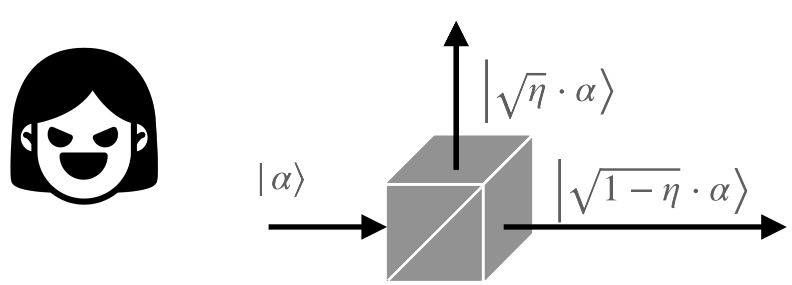
Photon Number Splitting attack



Unambiguous state discrimination attack



Beam splitting attack



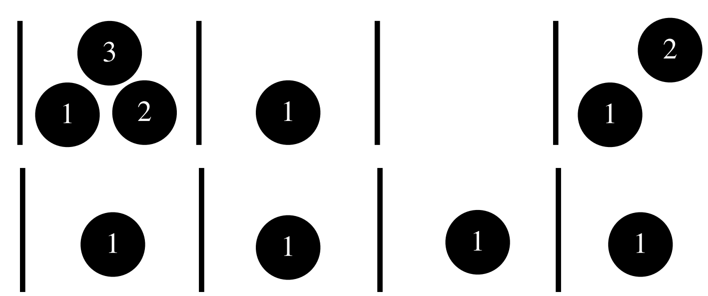
Hardware loopholes

Can be considered as attacks on utilized hardware

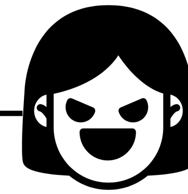
Non-ideal equipment

Flawed devices

Leaky source



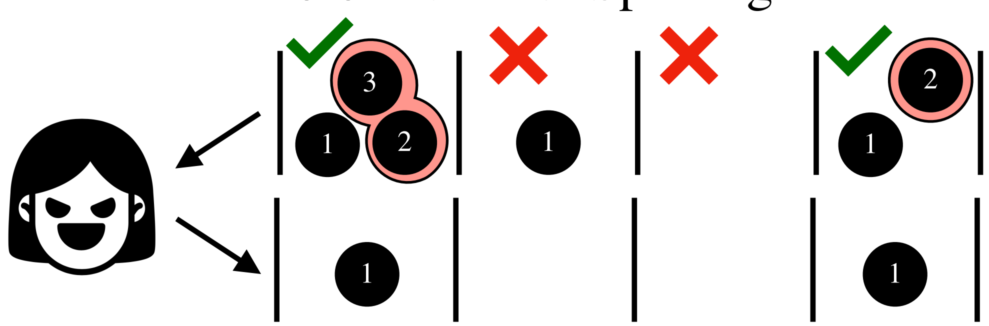
Preliminaries: Basic loopholes



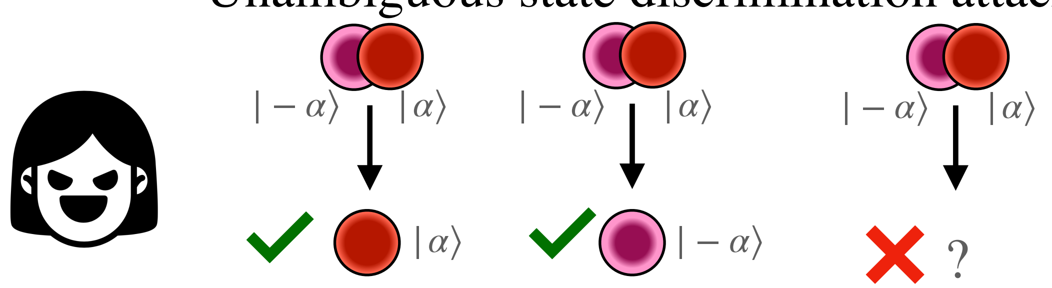
Protocol loopholes

Can be considered as attacks on quantum states in the quantum channel

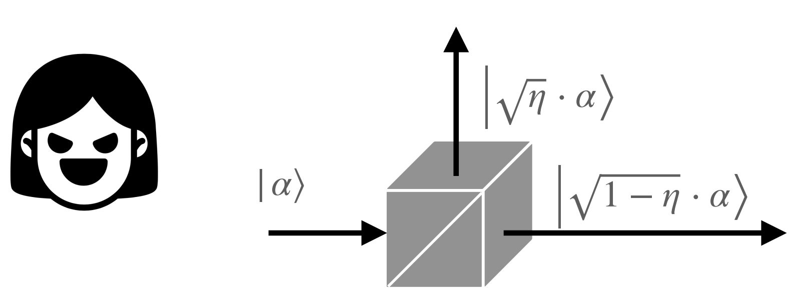
Photon Number Splitting attack



Unambiguous state discrimination attack



Beam splitting attack

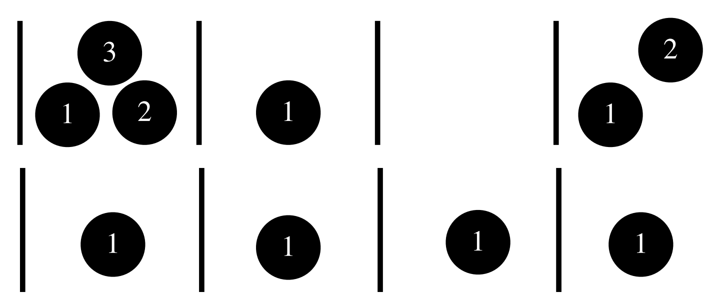


Hardware loopholes

Can be considered as attacks on utilized hardware

Non-ideal equipment

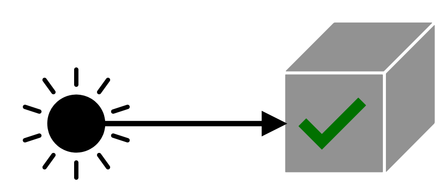
Leaky source



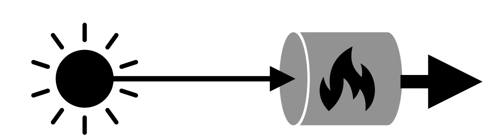
Flawed devices

Optical properties manipulations

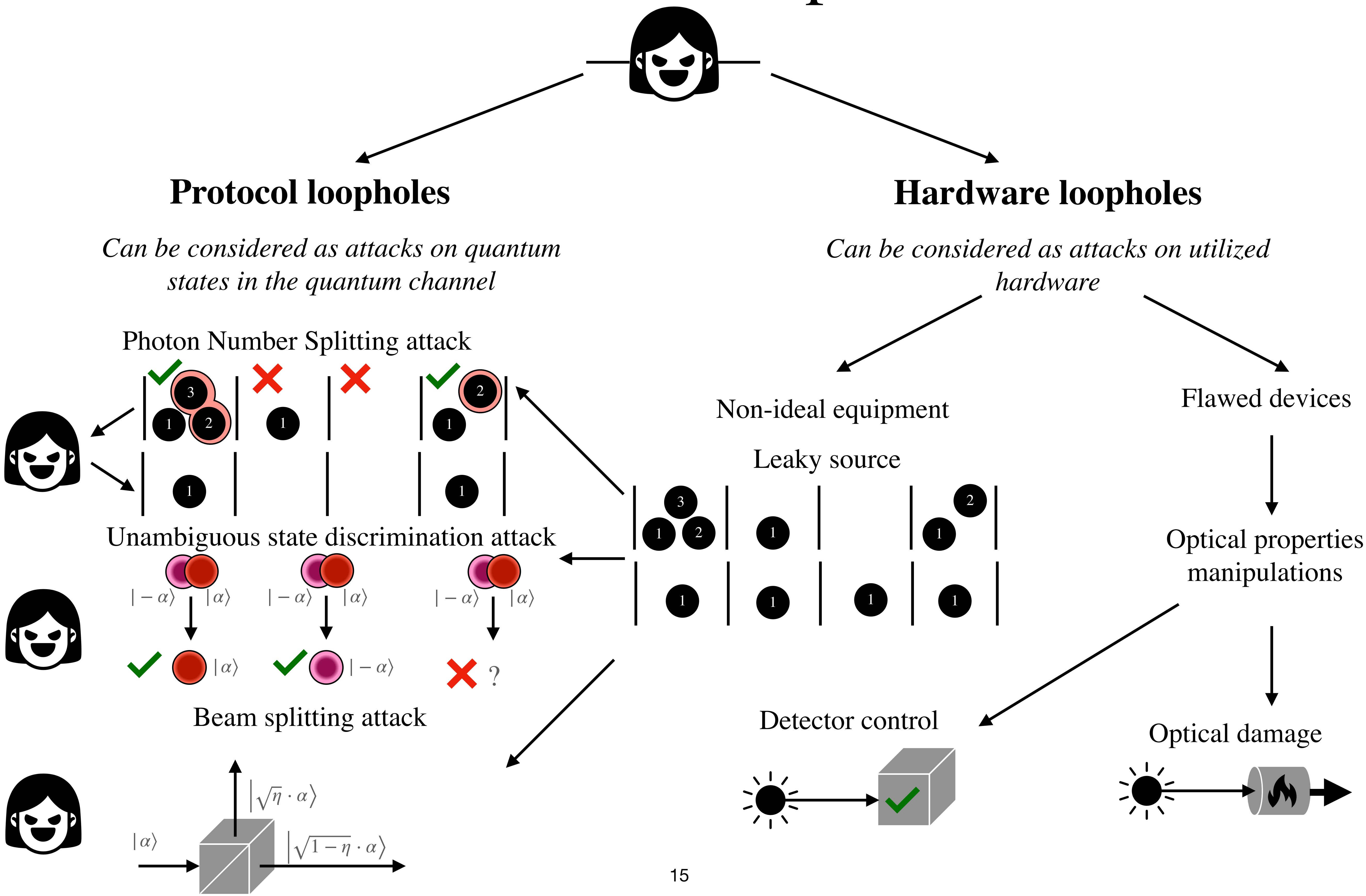
Detector control



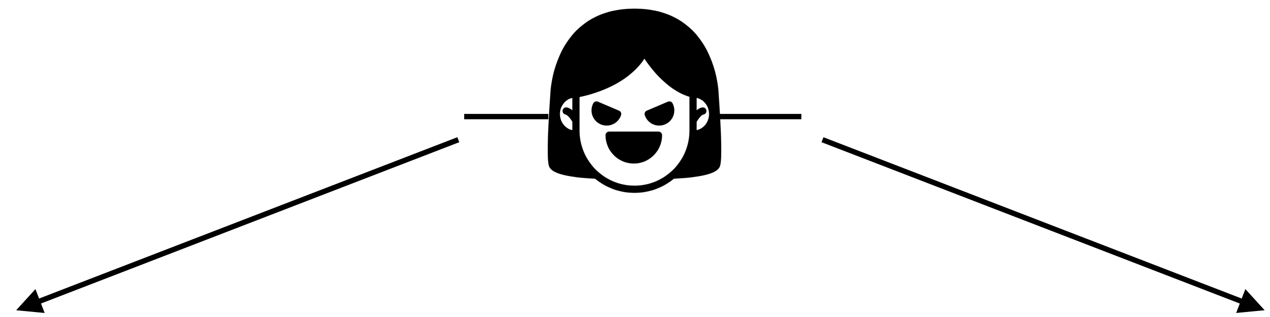
Optical damage



Preliminaries: Basic loopholes



Problem

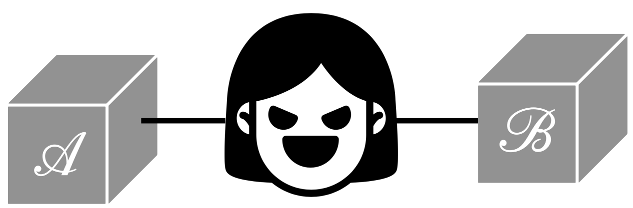


Protocol loopholes

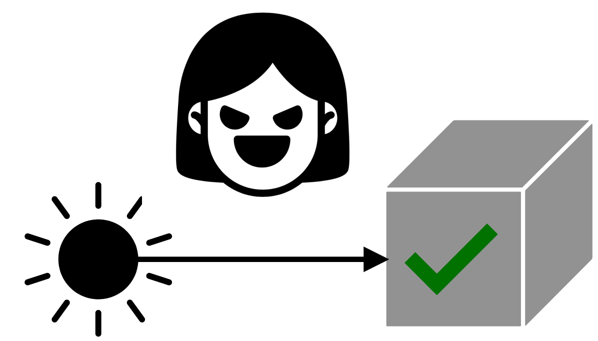
Hardware loopholes

intercept-resend attack

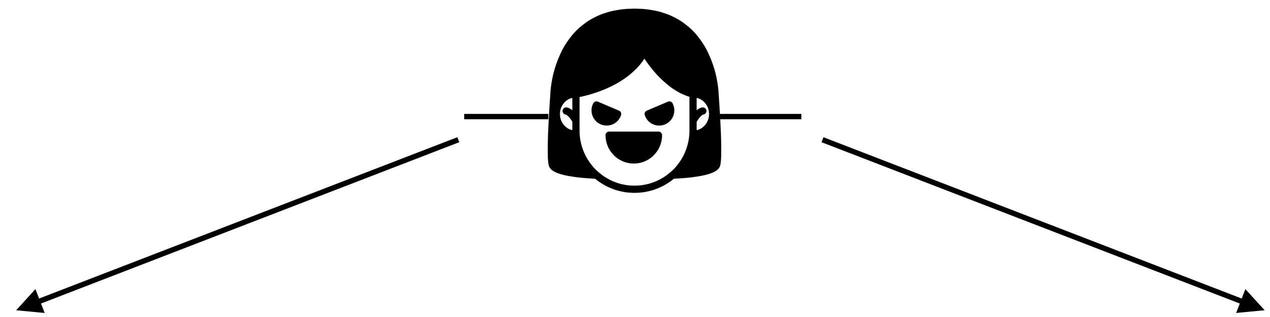
Detector control



+



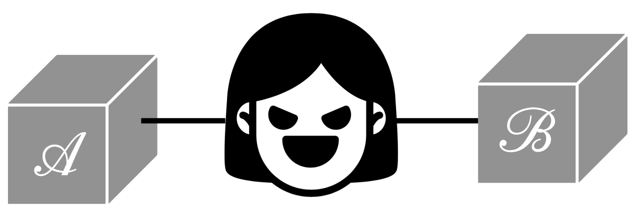
Problem



Protocol loopholes

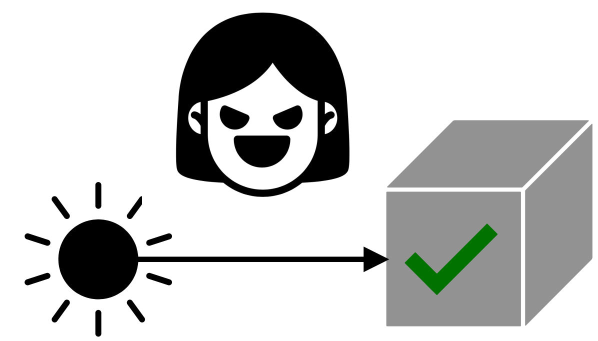
Hardware loopholes

intercept-resend attack



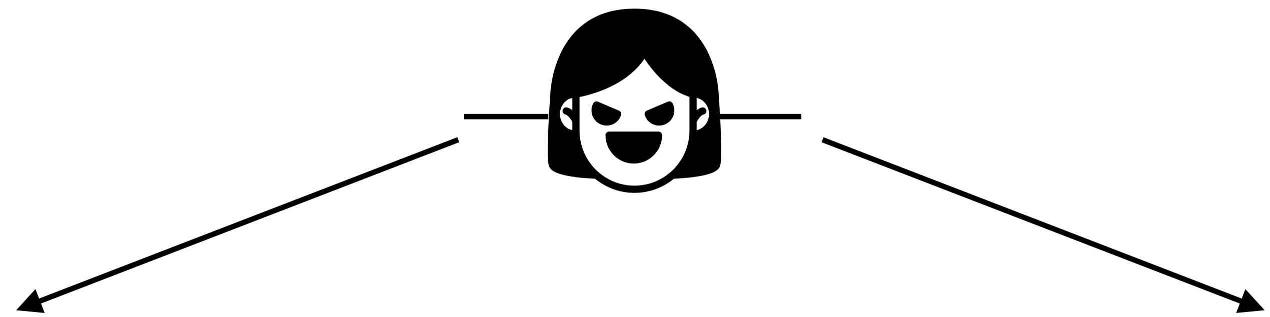
+

Detector control



- Strict quantum description is absent;
- No consideration of state imposing to Bob

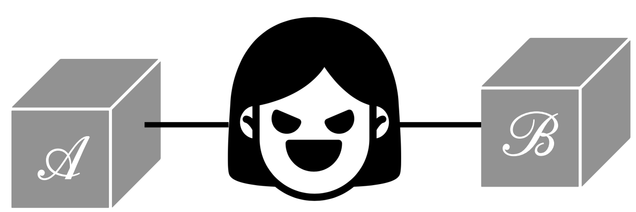
Problem



Protocol loopholes

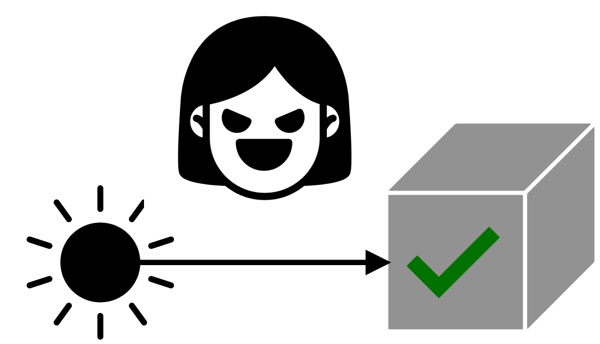
Hardware loopholes

intercept-resend attack



+

Detector control



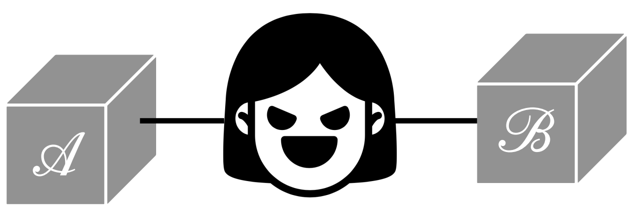
- Strict quantum description is absent;
- No consideration of state imposing to Bob

- Usually considered without state discrimination attacks;
- State discrimination probabilities not considered

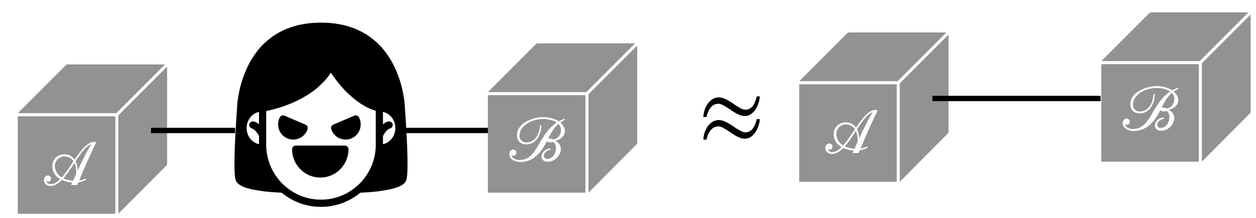
Problem

Conditions for successful eavesdropping

Information supremacy



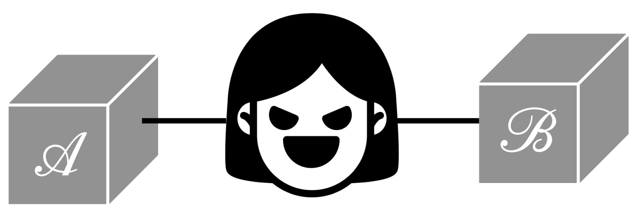
Statistics preservation

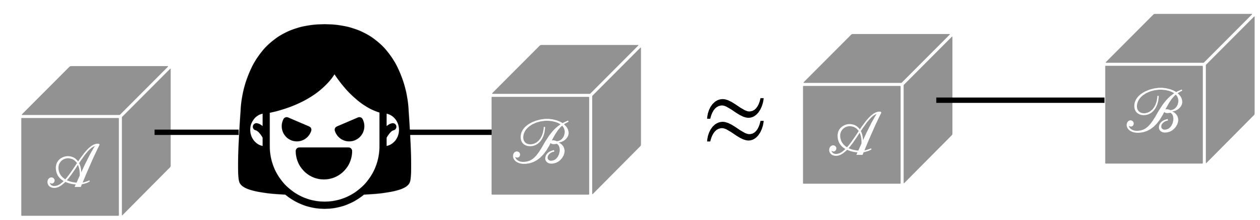


Problem

Conditions for successful eavesdropping

Information supremacy **+** **Statistics preservation**





$$A \to E \to B,$$

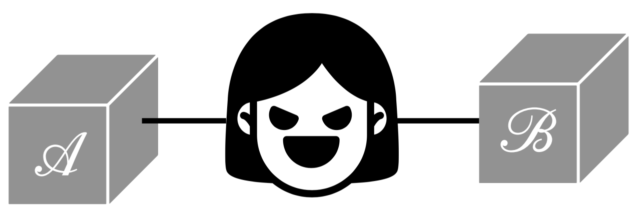
$$I(A;E) \geq I(A;B),$$

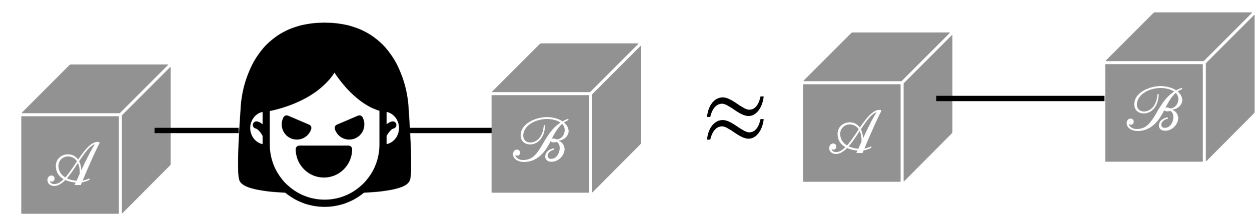
$$I(X;Y) = H(X) - H(X \mid Y)\,.$$

Problem

Conditions for successful eavesdropping

Information supremacy **+** **Statistics preservation**





$$A \to E \to B,$$

$$I(A;E) \geq I(A;B),$$

$$I(X;Y) = H(X) - H(X\,|\,Y)\,.$$

Detection rate preservation

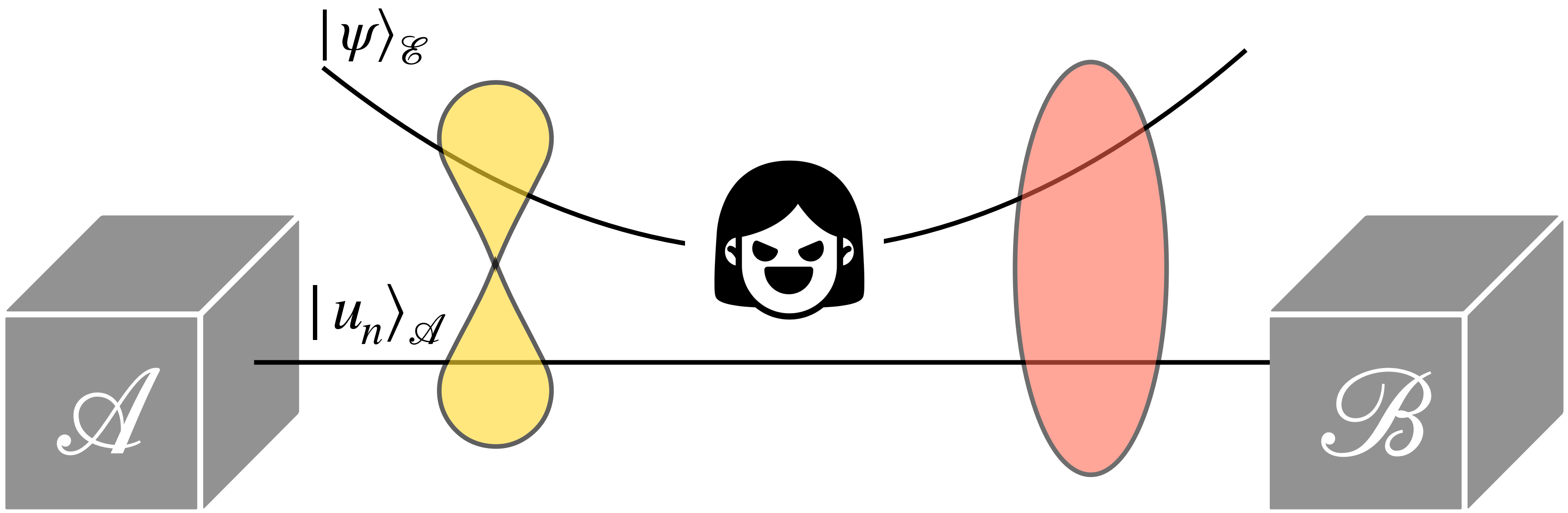
$$\sum_{b\neq 0} \mathscr{P}(b\,|\,a) \leq \sum_{b\neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a),$$

Error rate preservation

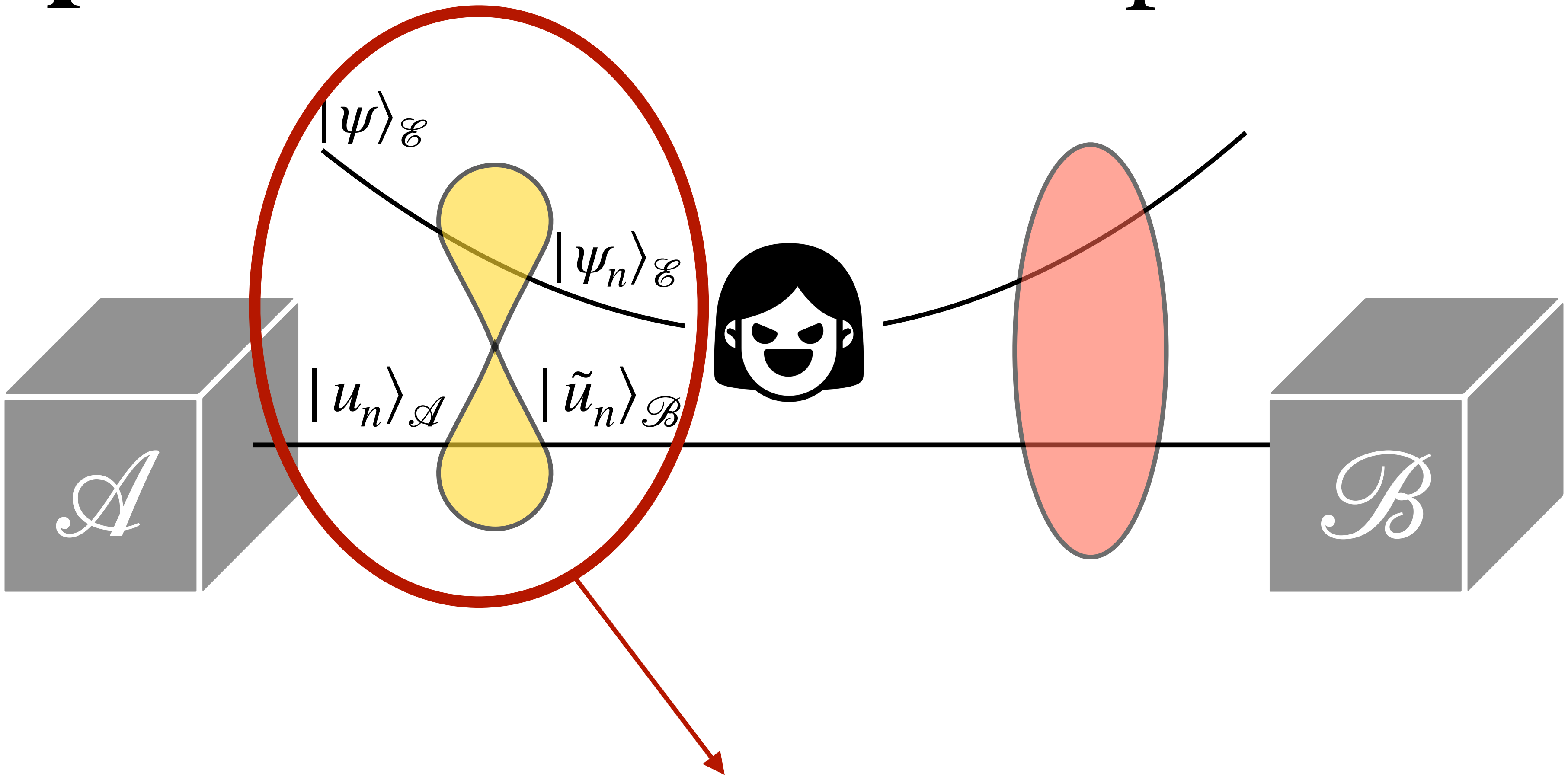
$$\sum_{b\neq a,0} \mathscr{P}(b\,|\,a) \geq \sum_{b\neq a,0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a),$$

$$\tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a) = \sum_{e} \mathscr{P}^{\mathscr{E}}(b\,|\,e)\mathscr{P}^{\mathscr{E}}(e\,|\,a)\,.$$

Description of the attack: Step 1

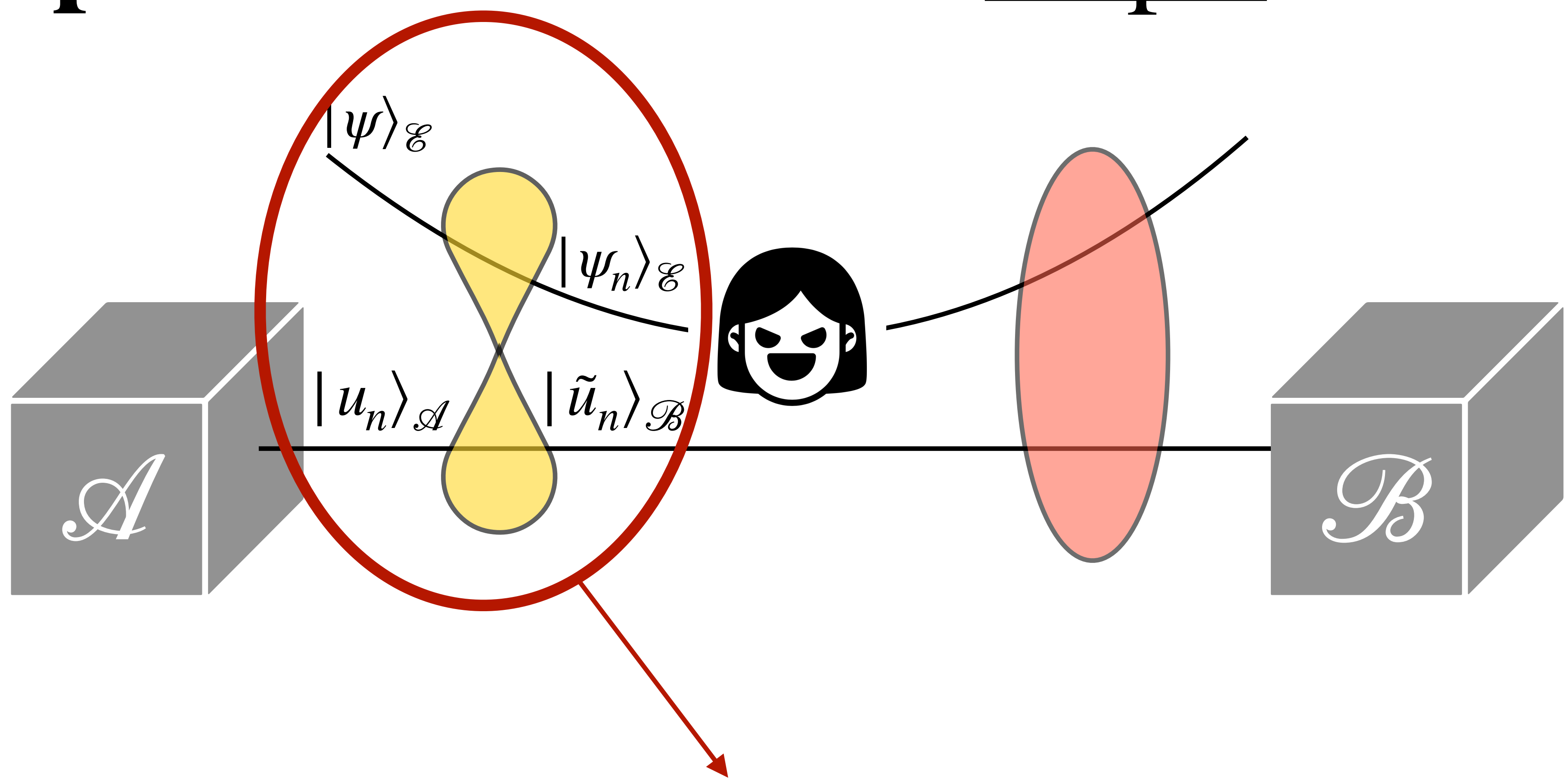


Description of the attack: Step 1

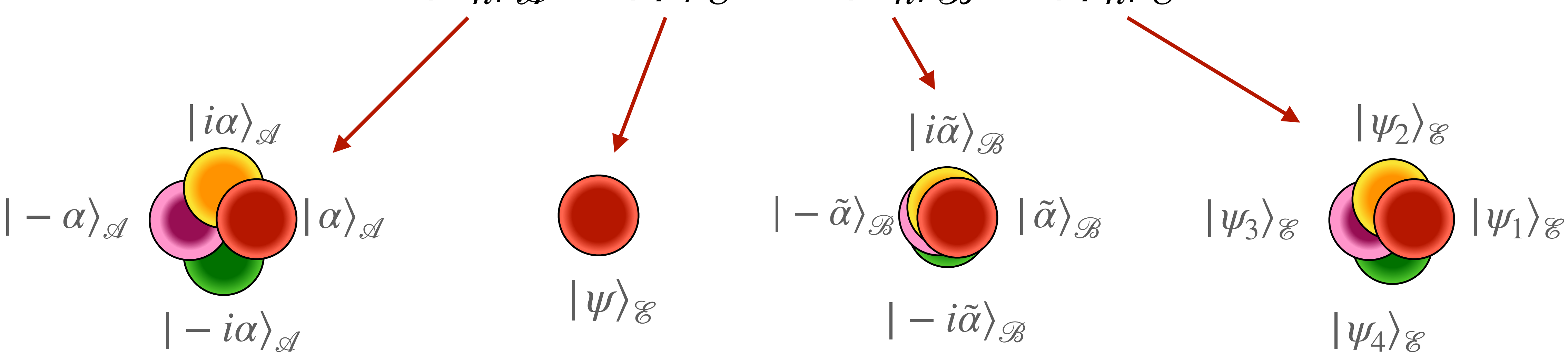


$$|u_n\rangle_{\mathscr{A}} \otimes |\psi\rangle_{\mathscr{E}} \xrightarrow{U_{\mathscr{A}\mathscr{E}}} |\tilde{u}_n\rangle_{\mathscr{B}} \otimes |\psi_n\rangle_{\mathscr{E}},$$

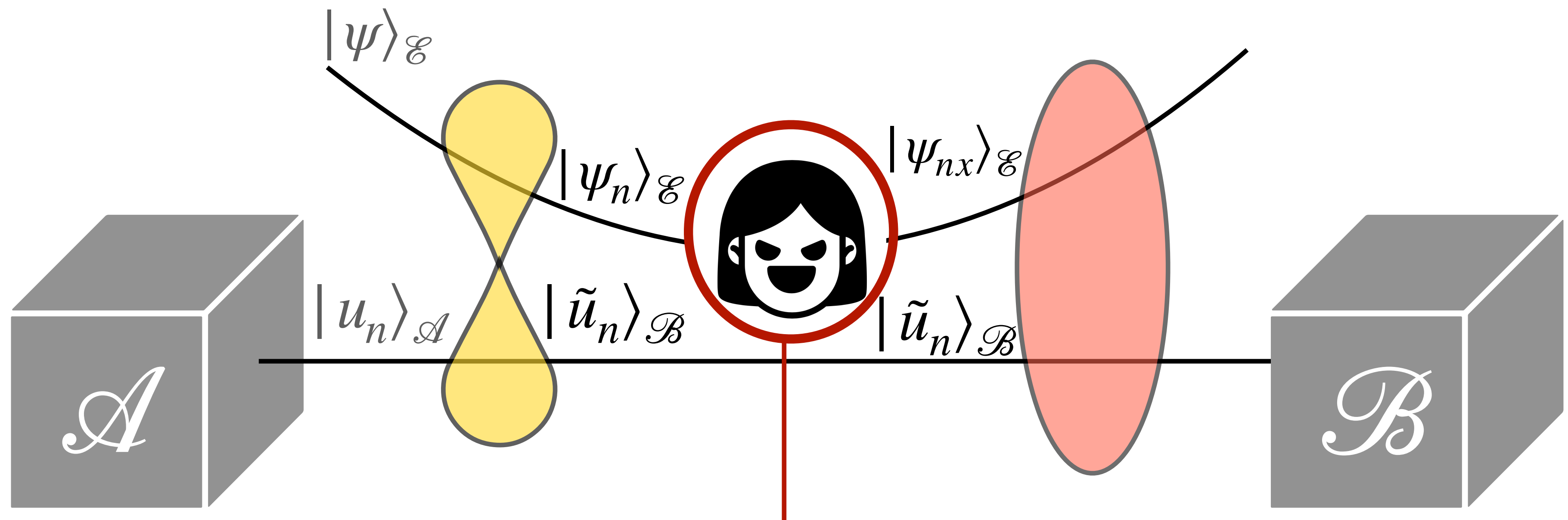
Description of the attack: Step 1



$$|u_n\rangle_{\mathscr{A}} \otimes |\psi\rangle_{\mathscr{E}} \xrightarrow{U_{\mathscr{A}\mathscr{E}}} |\tilde{u}_n\rangle_{\mathscr{B}} \otimes |\psi_n\rangle_{\mathscr{E}},$$



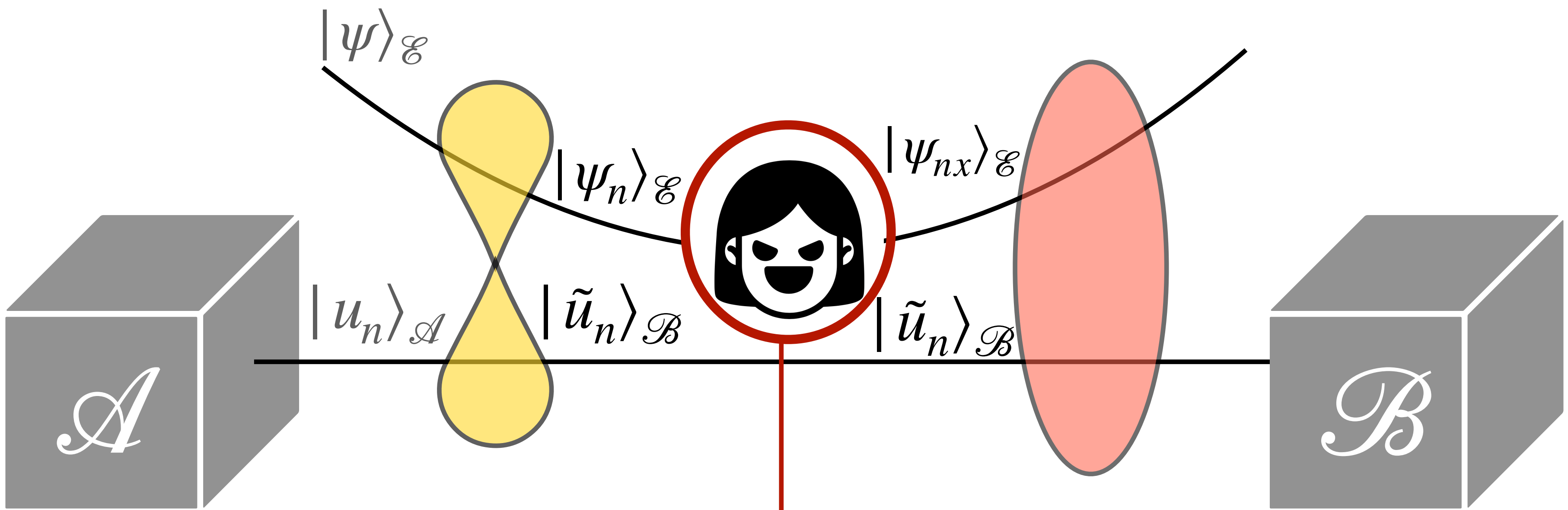
Description of the attack: Step 2



$$\mathbb{I} = \sum_x M^x_{\mathscr{E}\mathscr{B}}, \quad M^x_{\mathscr{E}\mathscr{B}} = \mathbb{I}_{\mathscr{B}} \otimes A^x_{\mathscr{E}}, \quad K^x_{\mathscr{B}\mathscr{E}} = V^x_{\mathscr{B}\mathscr{E}} \sqrt{M^x_{\mathscr{E}\mathscr{B}}},$$

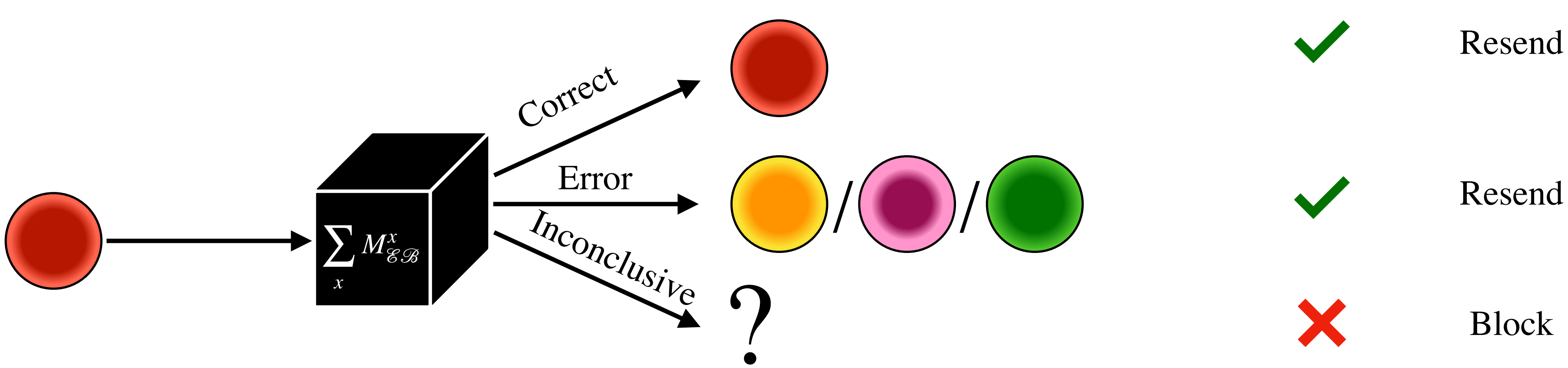
$$|\psi_{nx}\rangle_{\mathscr{E}} = \frac{\sqrt{A^x_{\mathscr{E}}}\,|\psi_n\rangle_{\mathscr{E}}}{\sqrt{\mathscr{P}(x\,|\,n)}}, \quad \mathscr{P}(x\,|\,n) = Tr_{\mathscr{E}}\left(A^x_{\mathscr{E}}\,|\psi_n\rangle_{\mathscr{E}}\langle\psi_n|\right).$$

Description of the attack: Step 2

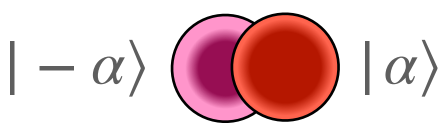


$$\mathbb{I} = \sum_x M^x_{\mathcal{EB}}, \quad M^x_{\mathcal{EB}} = \mathbb{I}_\mathcal{B} \otimes A^x_\mathcal{E}, \quad K^x_{\mathcal{BE}} = V^x_{\mathcal{BE}} \sqrt{M^x_{\mathcal{EB}}},$$

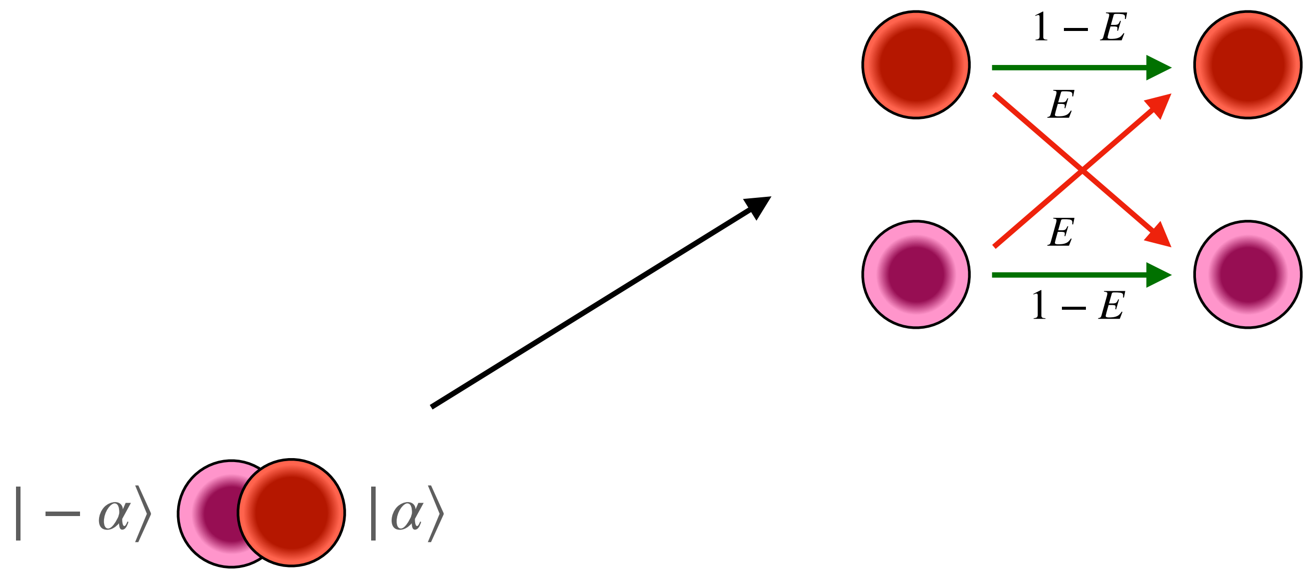
$$|\psi_{nx}\rangle_\mathcal{E} = \frac{\sqrt{A^x_\mathcal{E}}\,|\psi_n\rangle_\mathcal{E}}{\sqrt{\mathcal{P}(x\,|\,n)}}, \quad \mathcal{P}(x\,|\,n) = Tr_\mathcal{E}\left(A^x_\mathcal{E}\,|\psi_n\rangle_\mathcal{E}\langle\psi_n|\right).$$



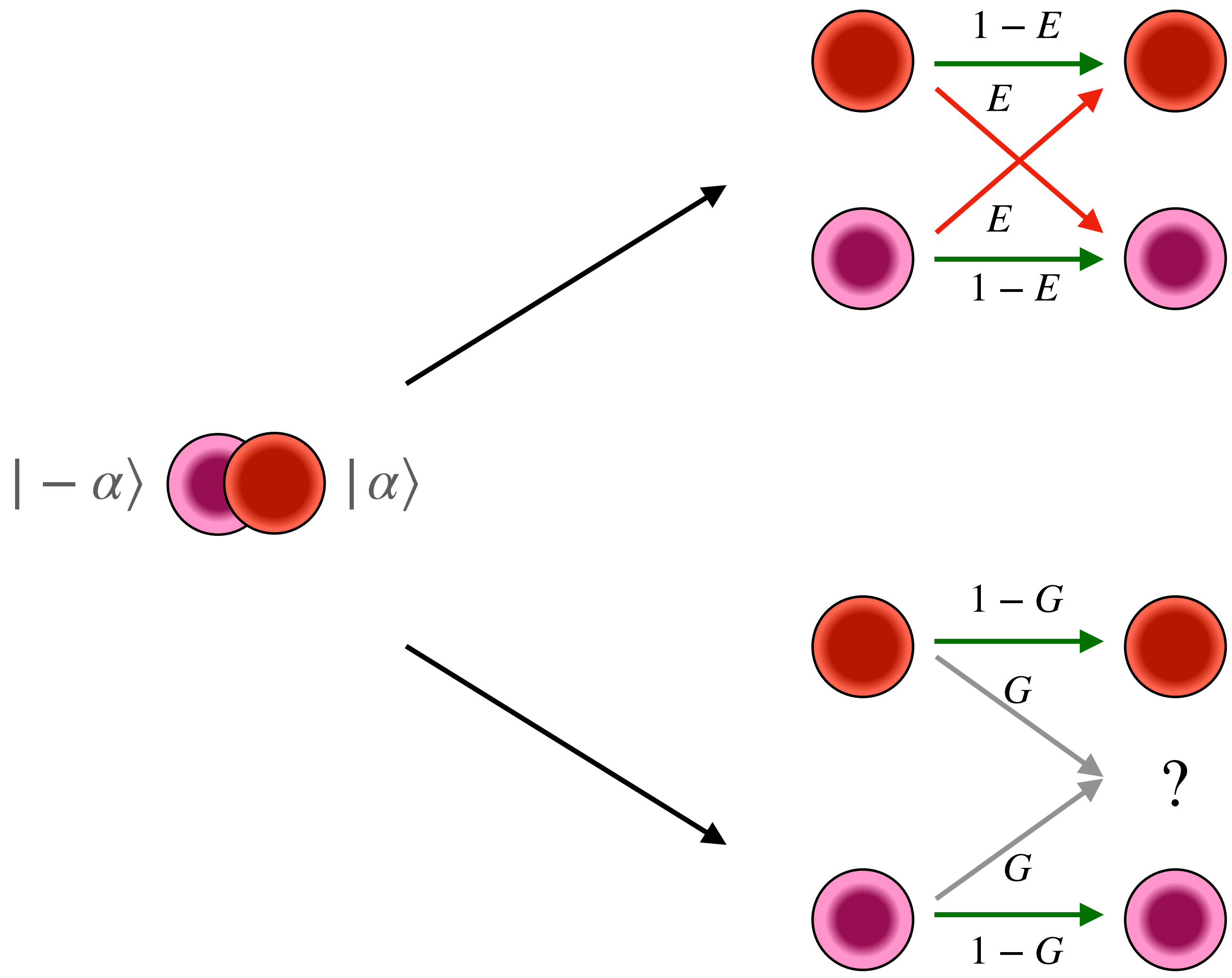
Example of the measurement



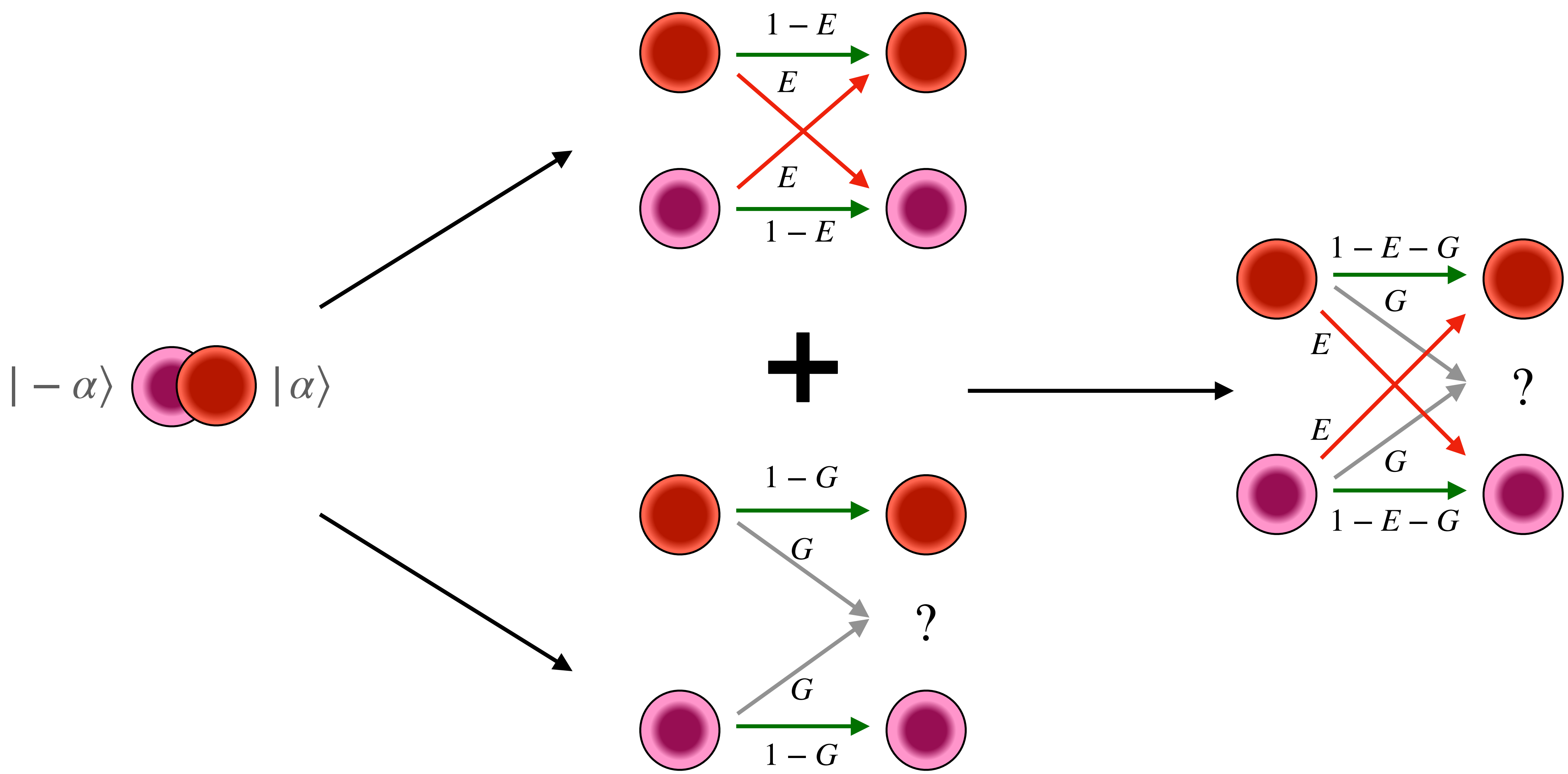
Example of the measurement



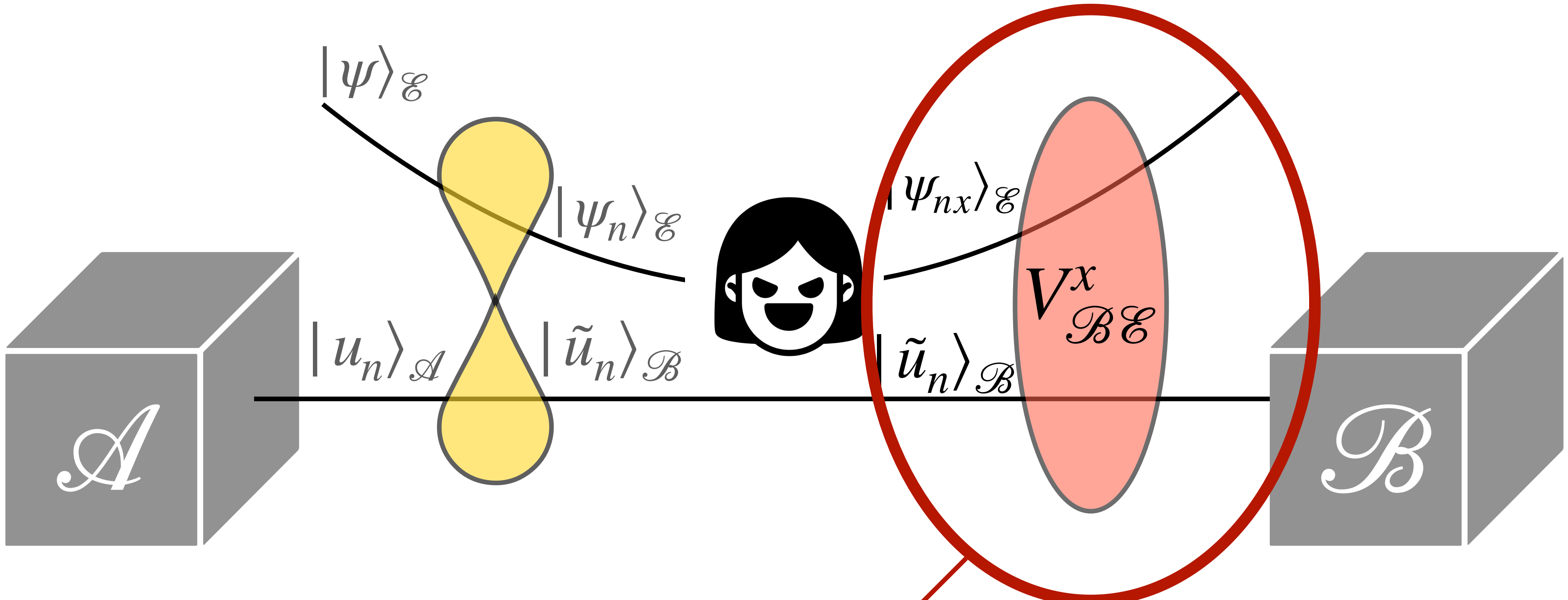
Example of the measurement



Example of the measurement



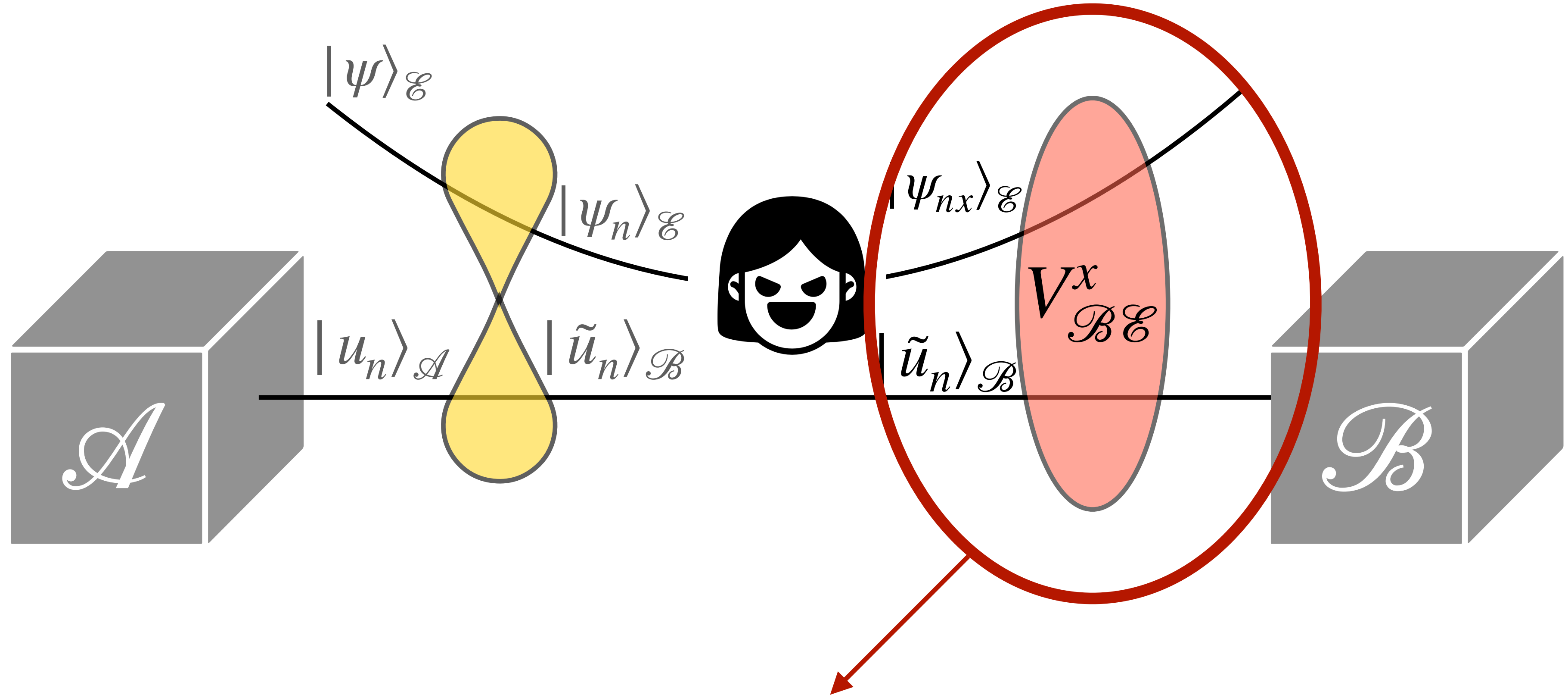
Description of the attack: Step 3



$$|\tilde{u}_n\rangle_{\mathscr{B}} \otimes |\psi_{nx}\rangle_{\mathscr{E}} \xrightarrow{V^x_{\mathscr{B}\mathscr{E}}} |\tilde{u}_{nx}\rangle_{\mathscr{B}} \otimes |\tilde{\psi}_{nx}\rangle_{\mathscr{E}},$$

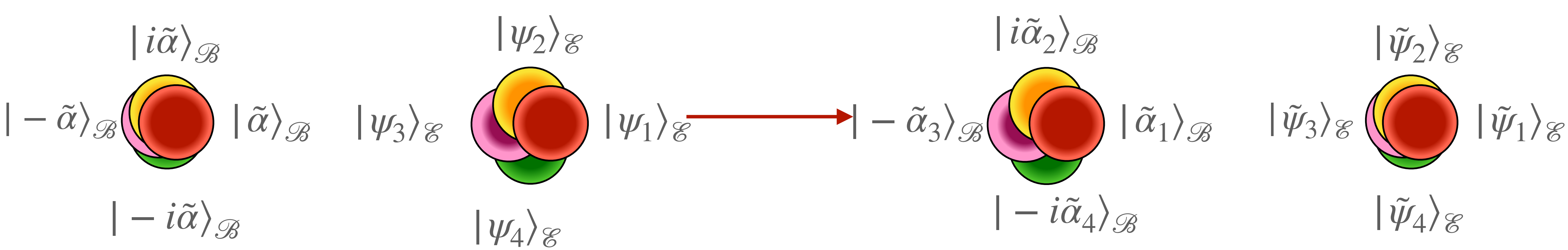
$$_{\mathscr{B}}\langle \tilde{u}_k | \tilde{u}_n \rangle_{\mathscr{B}\mathscr{E}}\langle \psi_{kx'} | \psi_{nx} \rangle_{\mathscr{E}} =_{\mathscr{B}} \langle \tilde{u}_{kx'} | \tilde{u}_{nx} \rangle_{\mathscr{B}\mathscr{E}}\langle \tilde{\psi}_{kx'} | \tilde{\psi}_{nx} \rangle_{\mathscr{E}} \,.$$

Description of the attack: Step 3



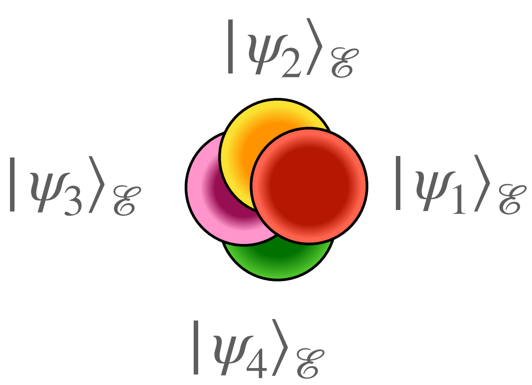
$$|\tilde{u}_n\rangle_{\mathscr{B}} \otimes |\psi_{nx}\rangle_{\mathscr{E}} \xrightarrow{V^x_{\mathscr{B}\mathscr{E}}} |\tilde{u}_{nx}\rangle_{\mathscr{B}} \otimes |\tilde{\psi}_{nx}\rangle_{\mathscr{E}},$$

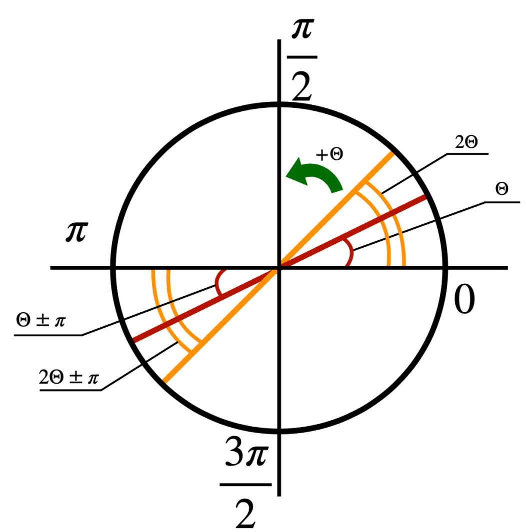
$${}_{\mathscr{B}}\langle \tilde{u}_k | \tilde{u}_n \rangle_{\mathscr{B}\mathscr{E}}\langle \psi_{kx'} | \psi_{nx} \rangle_{\mathscr{E}} = {}_{\mathscr{B}}\langle \tilde{u}_{kx'} | \tilde{u}_{nx} \rangle_{\mathscr{B}\mathscr{E}}\langle \tilde{\psi}_{kx'} | \tilde{\psi}_{nx} \rangle_{\mathscr{E}}\,.$$



Example of the attack: problem statement

Considered set of states



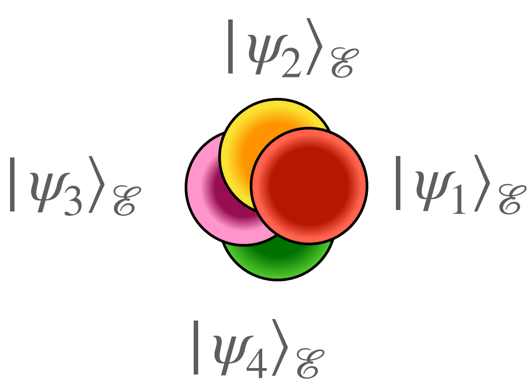


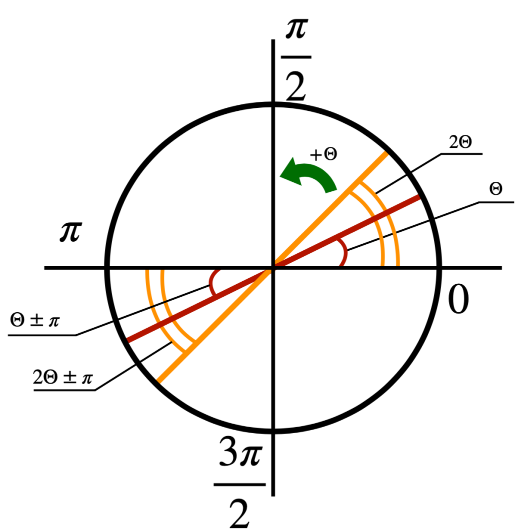
$$|\psi_n\rangle \equiv |\alpha e^{i\phi_n}\rangle, \quad \phi_n = \frac{\pi}{N}n, \quad n = 2N, \quad p_n = \frac{1}{2N}$$

$$w = \langle\psi_n|\psi_m\rangle = e^{-|\alpha|^2(1-e^{-i(\phi_n-\phi_m)})},$$

Example of the attack: problem statement

Considered set of states

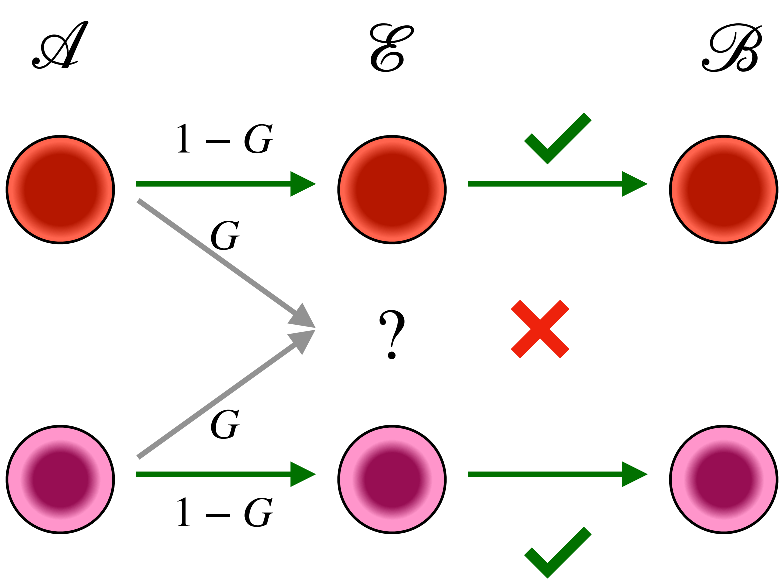




$$|\psi_n\rangle \equiv |\alpha e^{i\phi_n}\rangle, \quad \phi_n = \frac{\pi}{N}n, \quad n = 2N, \quad p_n = \frac{1}{2N}$$

$$w = \langle\psi_n|\psi_m\rangle = e^{-|\alpha|^2(1-e^{-i(\phi_n-\phi_m)})},$$

Successful attack conditions



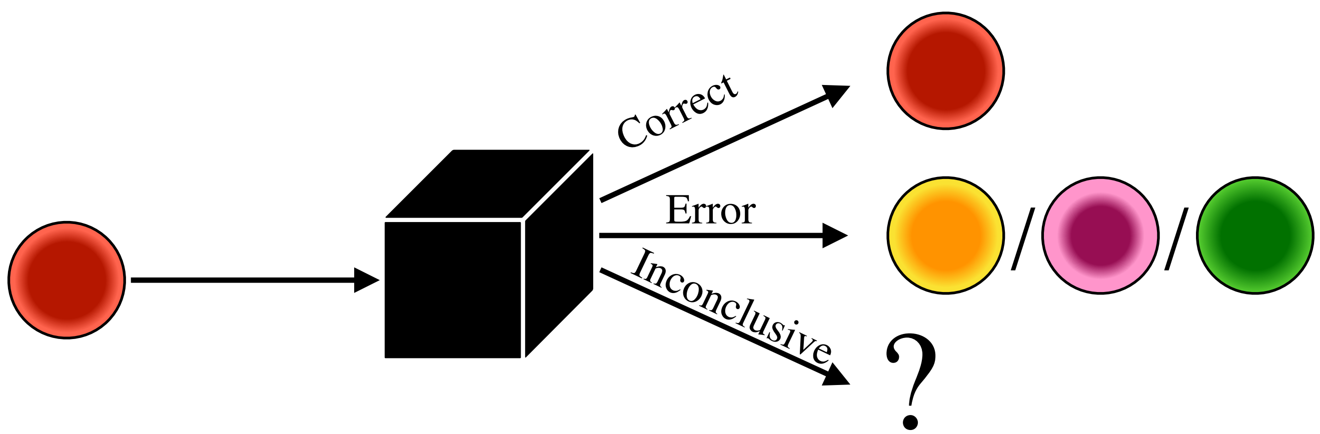
$$\mathscr{P}(b|a) \geq \mathscr{P}_U \cdot \delta_{ab},$$

$$\mathscr{P}^{\mathscr{E}}(e|a) \equiv \mathscr{P}_U \cdot \delta_{ea} \qquad \mathscr{P}^{\mathscr{E}}(b|e) \equiv \delta_{be}$$

$$\sum_{b\neq a,0}\sum_{e}\mathscr{P}^{\mathscr{E}}(b|e)\mathscr{P}^{\mathscr{E}}(e|a) \equiv \sum_{b\neq a,0}\mathscr{P}_U\delta_{ab} = 0$$

Example of the attack: Eve's measurement

Eavesdropper's measurement



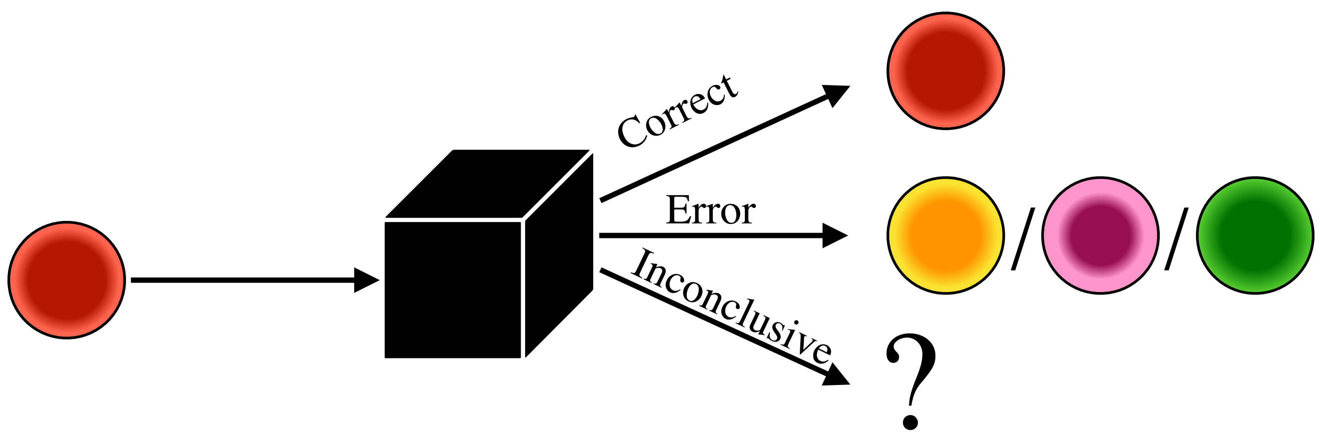
$$\hat{A}_n = \mathscr{P}\,|\varphi_n\rangle\langle\varphi_n|, \qquad \hat{A}_0 = \hat{I} - \sum_{n=1}^{2N} \hat{A}_n$$

$$|\varphi_n\rangle = \frac{(1-w)\,|\psi_n^{\perp}\rangle + w\,|\psi_n\rangle}{\sqrt{C}},$$

$$C = (1-w)^2\nu + w(2-w), \quad \langle\psi_n^{\perp}|\psi_m\rangle = \delta_{nm}$$

Example of the attack: Eve’s measurement

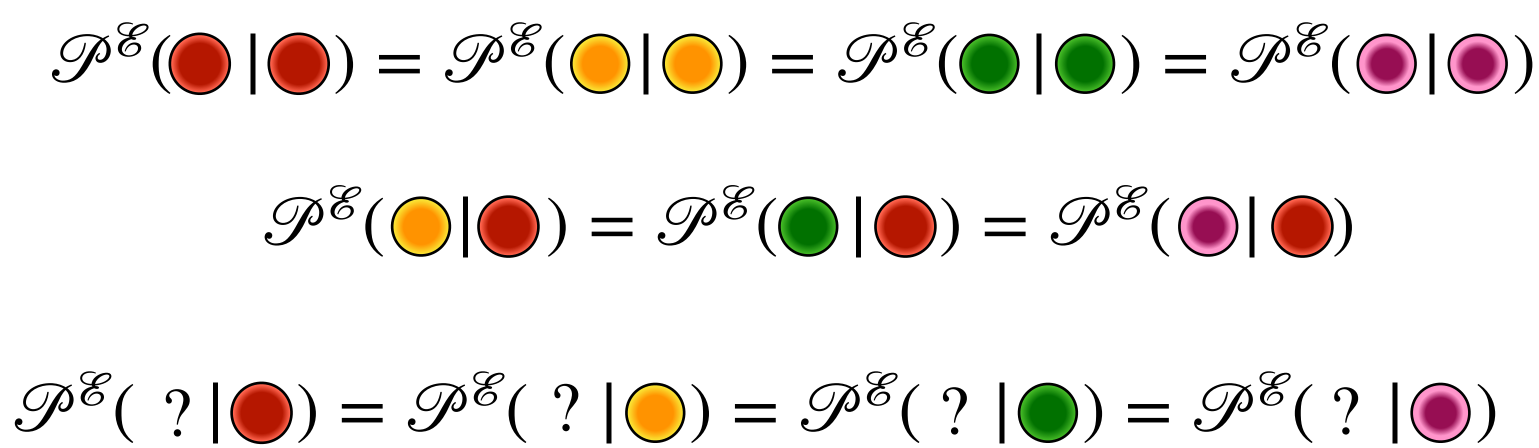
Eavesdropper’s measurement



$$\hat{A}_n = \mathscr{P}\,|\varphi_n\rangle\langle\varphi_n|, \qquad \hat{A}_0 = \hat{I} - \sum_{n=1}^{2N} \hat{A}_n$$

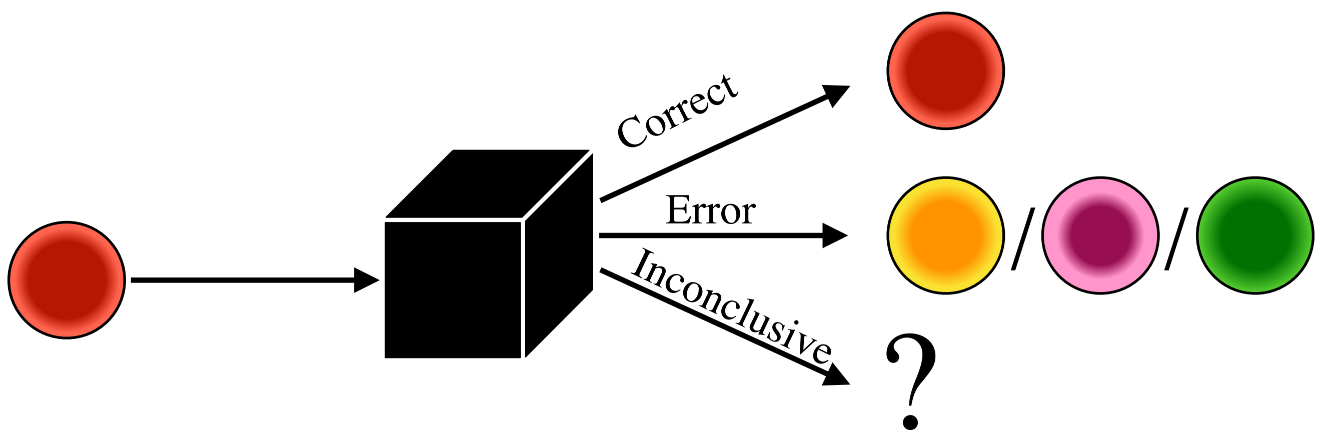
$$|\varphi_n\rangle = \frac{(1-w)\,|\psi_n^{\perp}\rangle + w\,|\psi_n\rangle}{\sqrt{C}},$$

$$C = (1-w)^2\nu + w(2-w), \qquad \langle\psi_n^{\perp}|\psi_m\rangle = \delta_{nm}$$



Example of the attack: Eve's measurement

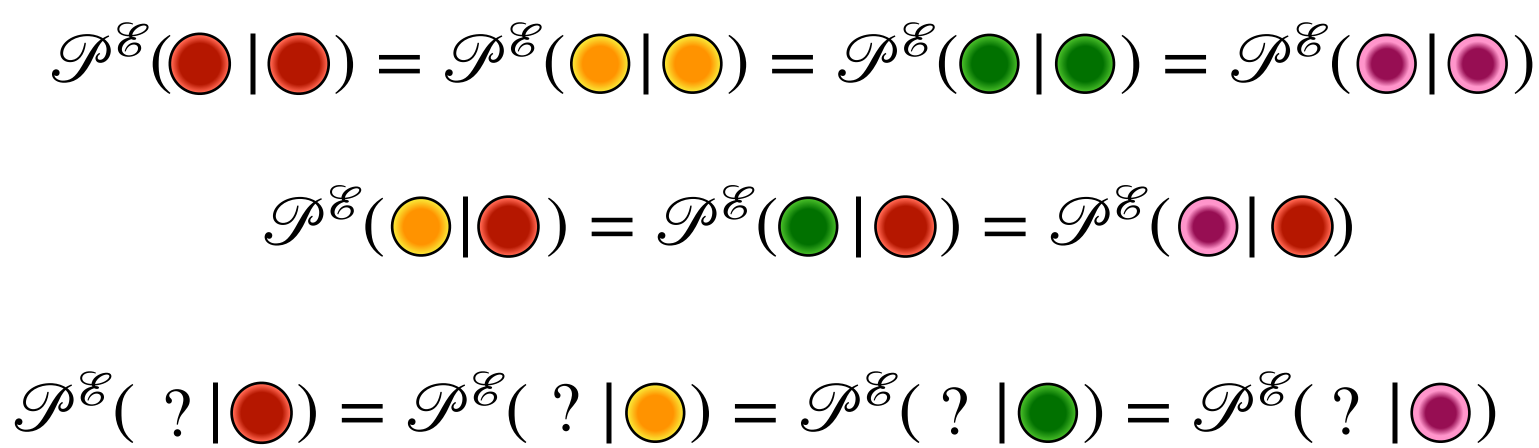
Eavesdropper's measurement



$$\hat{A}_n = \mathscr{P}_n |\varphi_n\rangle\langle\varphi_n|, \quad \hat{A}_0 = \hat{I} - \sum_{n=1}^{2N} \hat{A}_n$$

$$|\varphi_n\rangle = \frac{(1-w)|\psi_n^{\perp}\rangle + w|\psi_n\rangle}{\sqrt{C}},$$

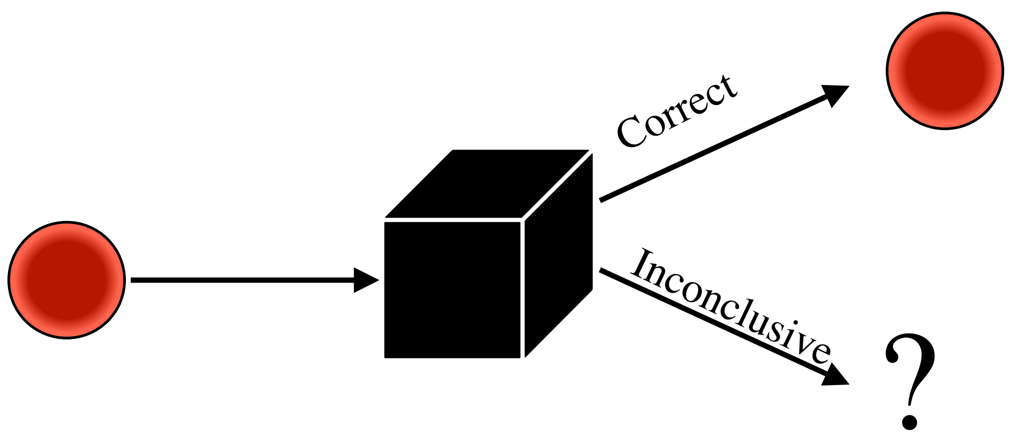
$$C = (1-w)^2\nu + w(2-w), \quad \langle\psi_n^{\perp}|\psi_m\rangle = \delta_{nm}$$

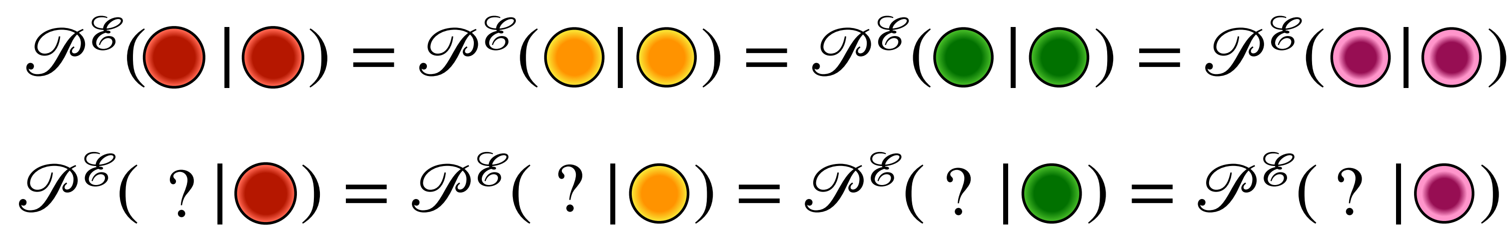


$$\boxed{\mathscr{P}^{\mathscr{E}}(m|n) = \langle\psi_n|\hat{A}_m|\psi_n\rangle = \mathscr{P}\cdot\left(\frac{(1-w^2)\delta_{nm}}{C} + \frac{w^2|\langle\psi_n|\psi_m\rangle|^2}{C}\right)}$$

Example of the attack: Eve’s measurement

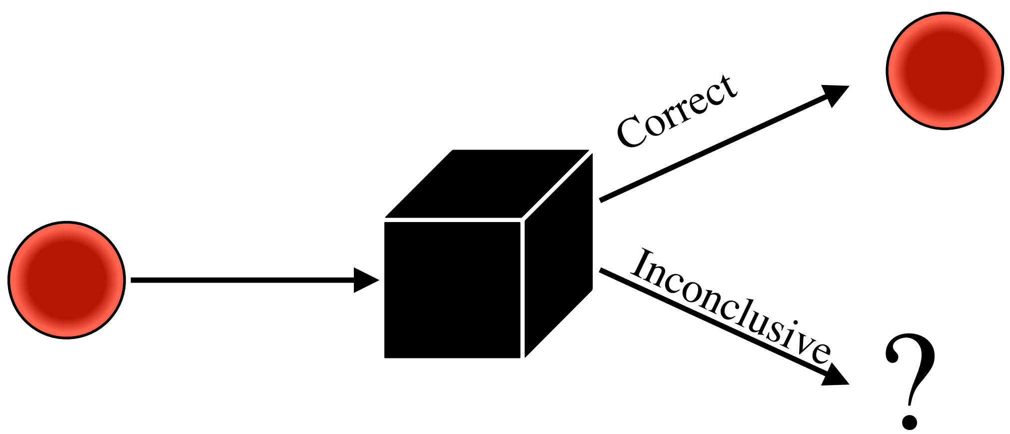
Eavesdropper’s measurement

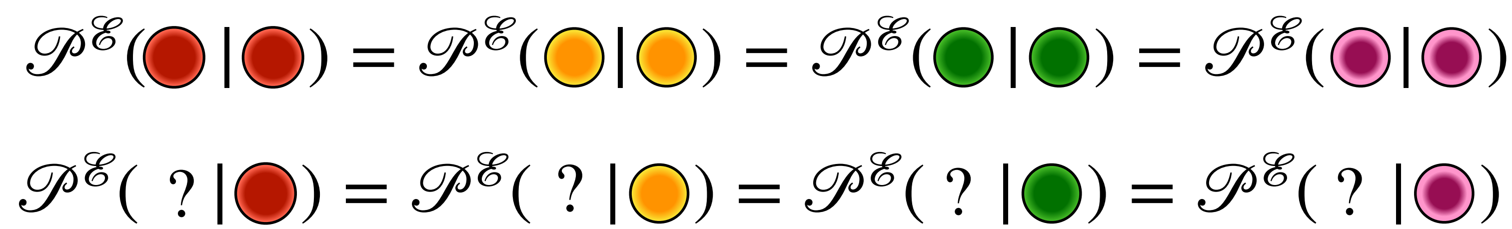




Example of the attack: Eve’s measurement

Eavesdropper’s measurement



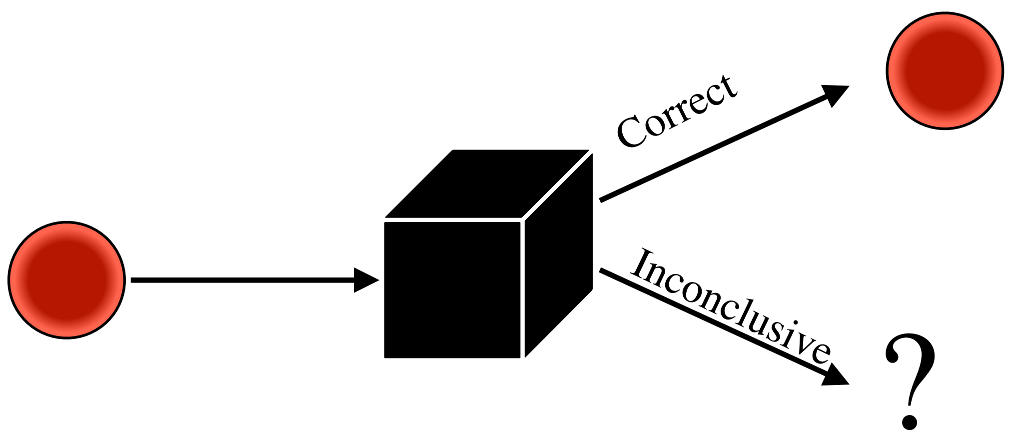


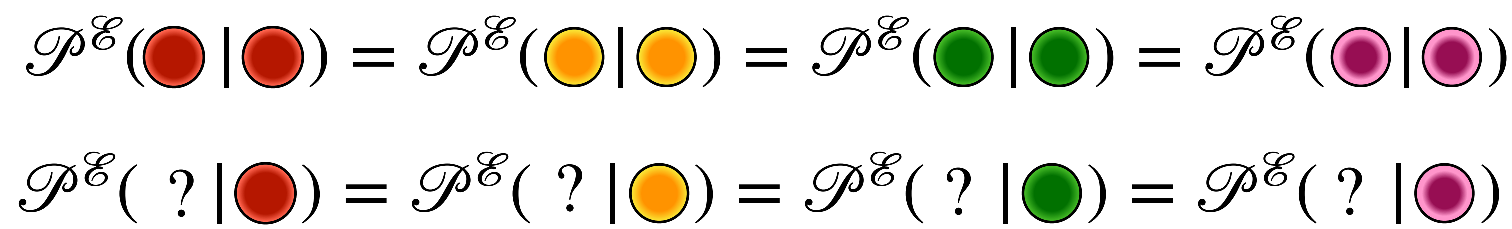
Optimization condition

$$\det\left(\hat{I} - \mathscr{P} \sum_{n=1}^{2N} |\varphi_n\rangle\langle\varphi_n|\right) = 0.$$

Example of the attack: Eve's measurement

Eavesdropper's measurement





Optimization condition

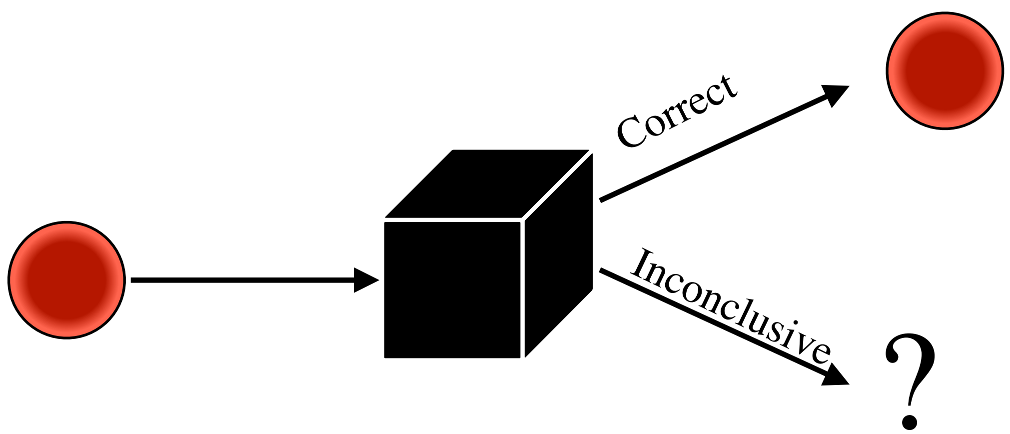
$$\det(\hat{I} - \mathscr{P} \sum_{n=1}^{2N} |\varphi_n\rangle\langle\varphi_n|) = 0.$$

Solution

Iff $\mathscr{P}$ equals to reciprocal maximal eigenvalue of $\sum_{n=1}^{2N} |\varphi_n\rangle\langle\varphi_n|$

Example of the attack: Eve's measurement

Eavesdropper's measurement



$$\mathscr{P}^{\mathscr{E}}({\color{red}\bullet}|{\color{red}\bullet}) = \mathscr{P}^{\mathscr{E}}({\color{orange}\bullet}|{\color{orange}\bullet}) = \mathscr{P}^{\mathscr{E}}({\color{green}\bullet}|{\color{green}\bullet}) = \mathscr{P}^{\mathscr{E}}({\color{magenta}\bullet}|{\color{magenta}\bullet}),$$

$$\mathscr{P}^{\mathscr{E}}(\ ?\ |{\color{red}\bullet}) = \mathscr{P}^{\mathscr{E}}(\ ?\ |{\color{orange}\bullet}) = \mathscr{P}^{\mathscr{E}}(\ ?\ |{\color{green}\bullet}) = \mathscr{P}^{\mathscr{E}}(\ ?\ |{\color{magenta}\bullet})$$

Optimization condition

$$\det(\hat{I} - \mathscr{P}\sum_{n=1}^{2N}|\varphi_n\rangle\langle\varphi_n|) = 0.$$

$\longrightarrow$

Solution

Iff $\mathscr{P}$ equals to reciprocal maximal eigenvalue of $\sum_{n=1}^{2N}|\varphi_n\rangle\langle\varphi_n|$

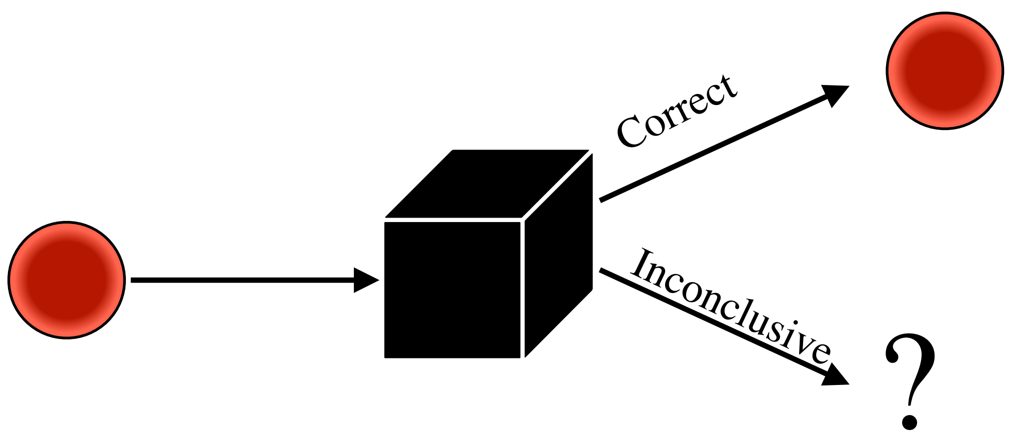
$$\sum_{n=1}^{2N}|\varphi_n\rangle\langle\varphi_n|\theta_k\rangle = \lambda_k|\theta_k\rangle,$$

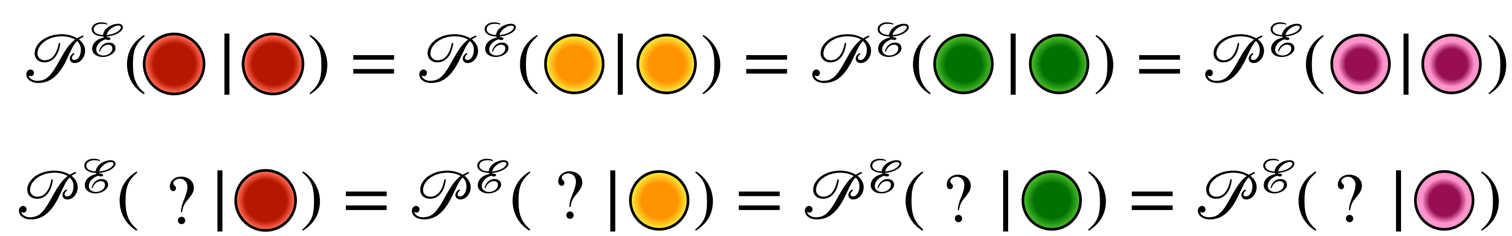
$$\lambda_k = \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\varphi_{2N}|\varphi_n\rangle,$$

$$|\theta_k\rangle = \frac{1}{\sqrt{2N\lambda_k}}\sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}|\varphi_n\rangle,$$

Example of the attack: Eve's measurement

Eavesdropper's measurement





Optimization condition

$$\det(\hat{I} - \mathscr{P} \sum_{n=1}^{2N} |\varphi_n\rangle\langle\varphi_n|) = 0.$$

Solution

Iff $\mathscr{P}$ equals to reciprocal maximal eigenvalue of $\sum_{n=1}^{2N} |\varphi_n\rangle\langle\varphi_n|$

$$\sum_{n=1}^{2N} |\varphi_n\rangle\langle\varphi_n|\theta_k\rangle = \lambda_k|\theta_k\rangle,$$

$$\lambda_k = \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\varphi_{2N}|\varphi_n\rangle,$$

$$|\theta_k\rangle = \frac{1}{\sqrt{2N\lambda_k}} \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}|\varphi_n\rangle,$$

$$\frac{1}{\mathscr{P}} = \max_k \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\varphi_{2N}|\varphi_n\rangle$$

$$\max_k \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\psi_{2N}^{\perp}|\psi_n^{\perp}\rangle = \left(\min_k \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\psi_{2N}|\psi_n\rangle\right)^{-1}$$

$$\boxed{\mathscr{P}_U \approx \sum_{q=0}^{2N-1} \frac{2N}{q!(2N-1-q)!}\left(\frac{|\alpha|^2}{2}\right)^{2N-1} \approx \frac{2N}{(2N-1)!}(|\alpha|^2)^{2N-1}.}$$

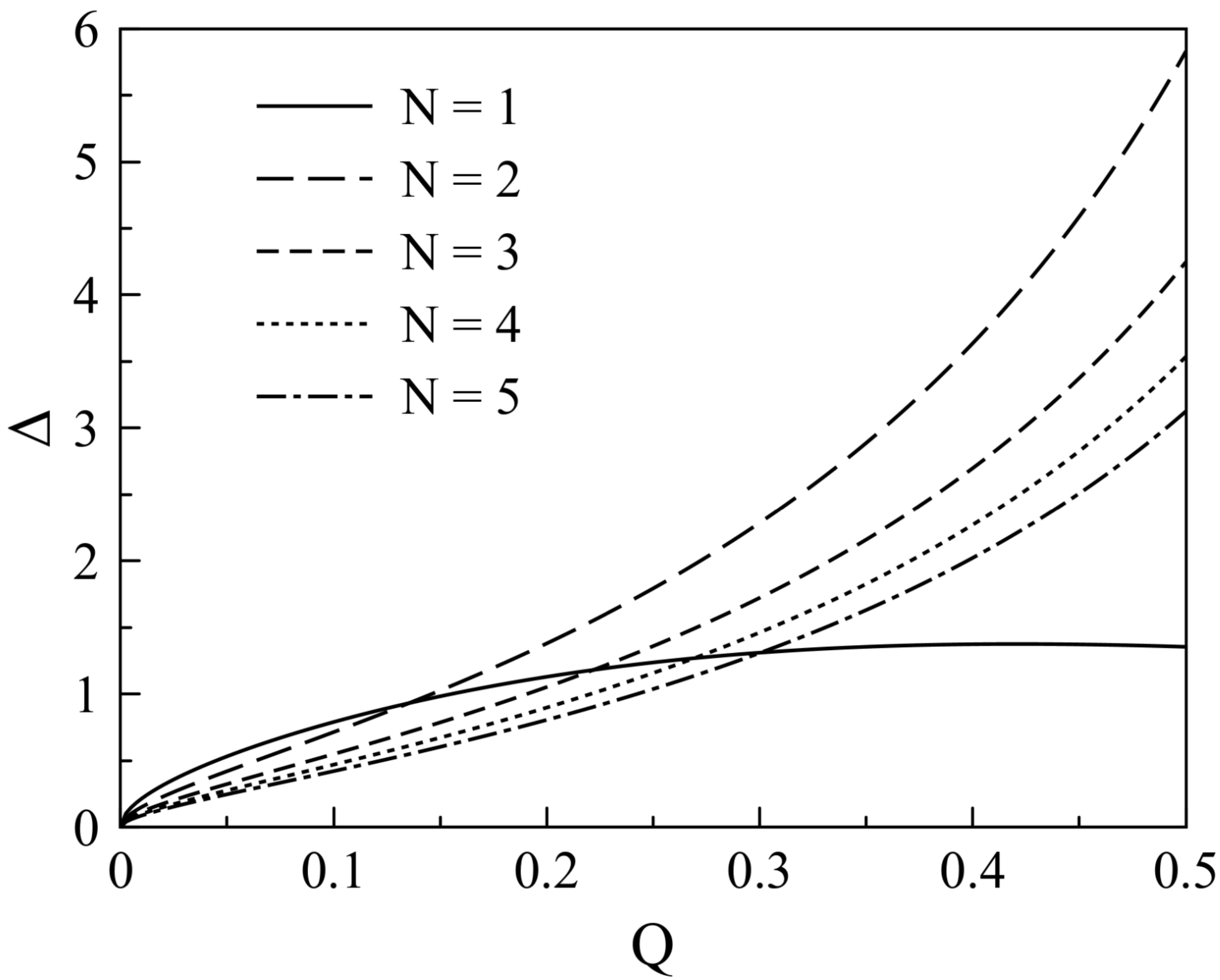
Example of the attack: Eve's measurement

Eavesdropper's measurement

$$|\psi_n\rangle \equiv |\alpha e^{i\phi_n}\rangle,\ \phi_n = \frac{\pi}{N}n,\ n = 2N,$$

$$\mathcal{Q}^{\mathcal{E}}(m) = \frac{\sum_{m\neq n,0} \tilde{\mathcal{P}}^{\mathcal{E}}(m\,|\,n)}{\sum_{m\neq 0} \tilde{\mathcal{P}}^{\mathcal{E}}(m\,|\,n)}$$

Example of the attack: Eve’s measurement



Relative difference Δ of detection rate with introduced error $\sum_{m\neq 0}\mathscr{P}^{\mathscr{E}}(m\,|\,n)$ compare to unambiguous state discrimination probability $\mathscr{P}_U$ (no errors) dependent on expected quantum bit error rate $\mathscr{Q}$ for different number of signal states defined by $2N$. Simulations were performed for symmetric coherent states with phase-coding, mean-photon number $|\alpha|^2 = 0.1$

Eavesdropper’s measurement

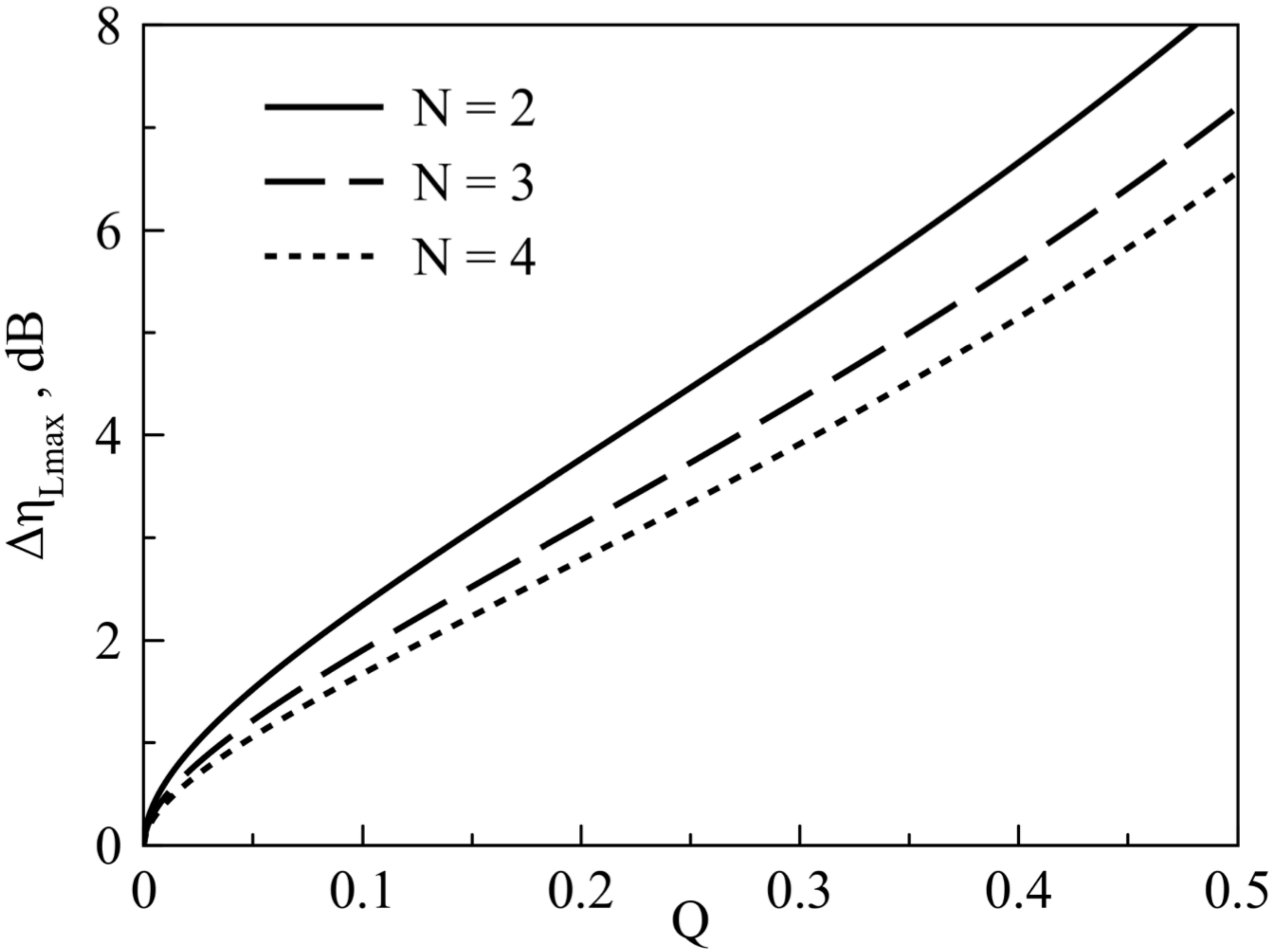
$$|\psi_n\rangle \equiv |\alpha e^{i\phi_n}\rangle,\ \phi_n = \frac{\pi}{N}n,\ n = 2N,$$

$$\mathscr{Q}^{\mathscr{E}}(m) = \frac{\sum_{m\neq n,0}\tilde{\mathscr{P}}^{\mathscr{E}}(m\,|\,n)}{\sum_{m\neq 0}\tilde{\mathscr{P}}^{\mathscr{E}}(m\,|\,n)}$$

$$\Delta = \frac{\boxed{\sum_{m\neq 0}\tilde{\mathscr{P}}^{\mathscr{E}}(m\,|\,n)\big|_{w=w_0}} - \mathscr{P}_U}{\mathscr{P}_U}$$

$$\sum_n \tilde{\mathscr{P}}^{\mathscr{E}}(n\,|\,n) + \sum_{m\neq n,0}\tilde{\mathscr{P}}^{\mathscr{E}}(m\,|\,n)$$

Example of the attack: Comparison

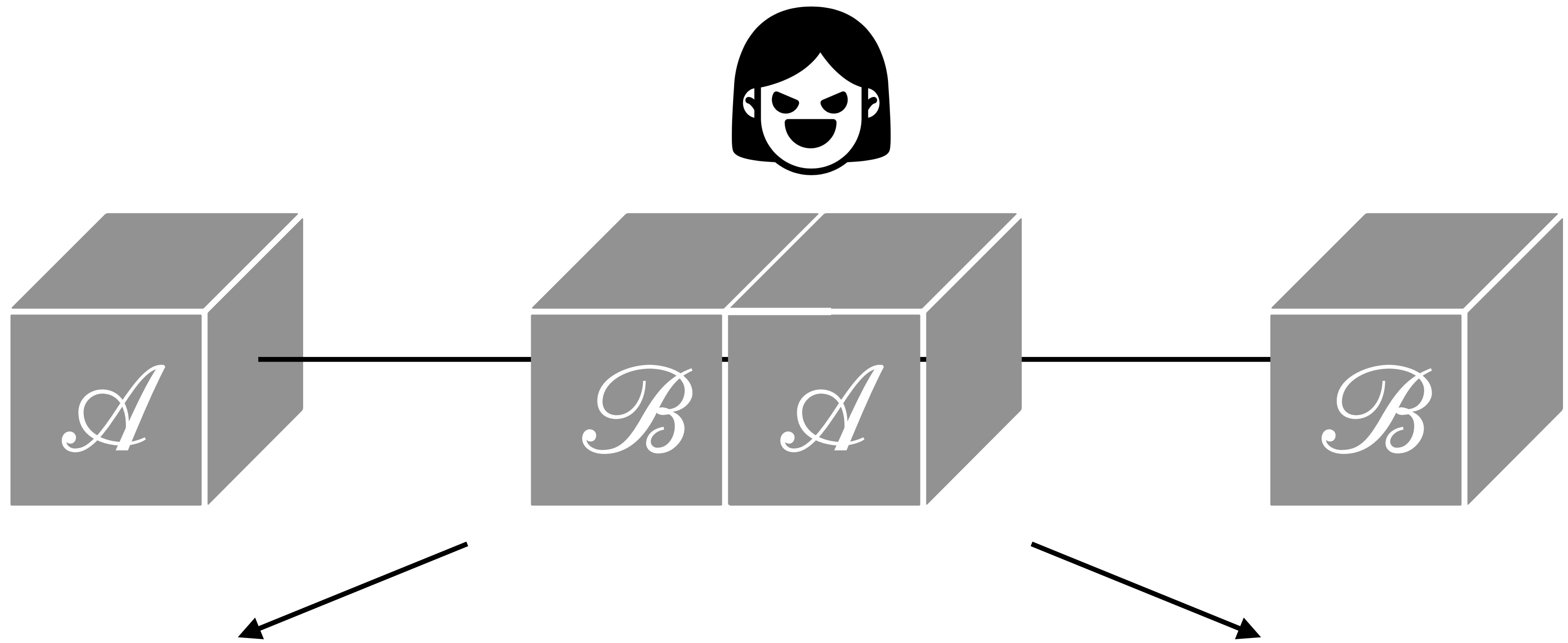


Difference $\Delta\eta_{Lmax}$ between maximal allowed η_L in case of simple USD and proposed modified USD that takes into account errors dependent on expected quantum bit error rate $\mathcal{Q}$ for different number of signal states defined by $2N$. Simulations were performed for symmetric coherent states with phase-coding, mean-photon number $|\alpha|^2 = 0.1, \quad \eta_B\eta_D = 0.05$.

$$c\,|\,\alpha\,|^2\eta_L\eta_B\eta_D \le \sum_{m\neq 0} \tilde{\mathcal{P}}^{\mathcal{E}}(m\,|\,n)\,|_{w=w_0},$$

- η_L is attenuation coefficient due to losses in the channel,
- η_B is attenuation coefficient due to losses at Bob's side,
- η_D is detection efficiency.

Fake-state attack



«Guess» the state

Impose the state

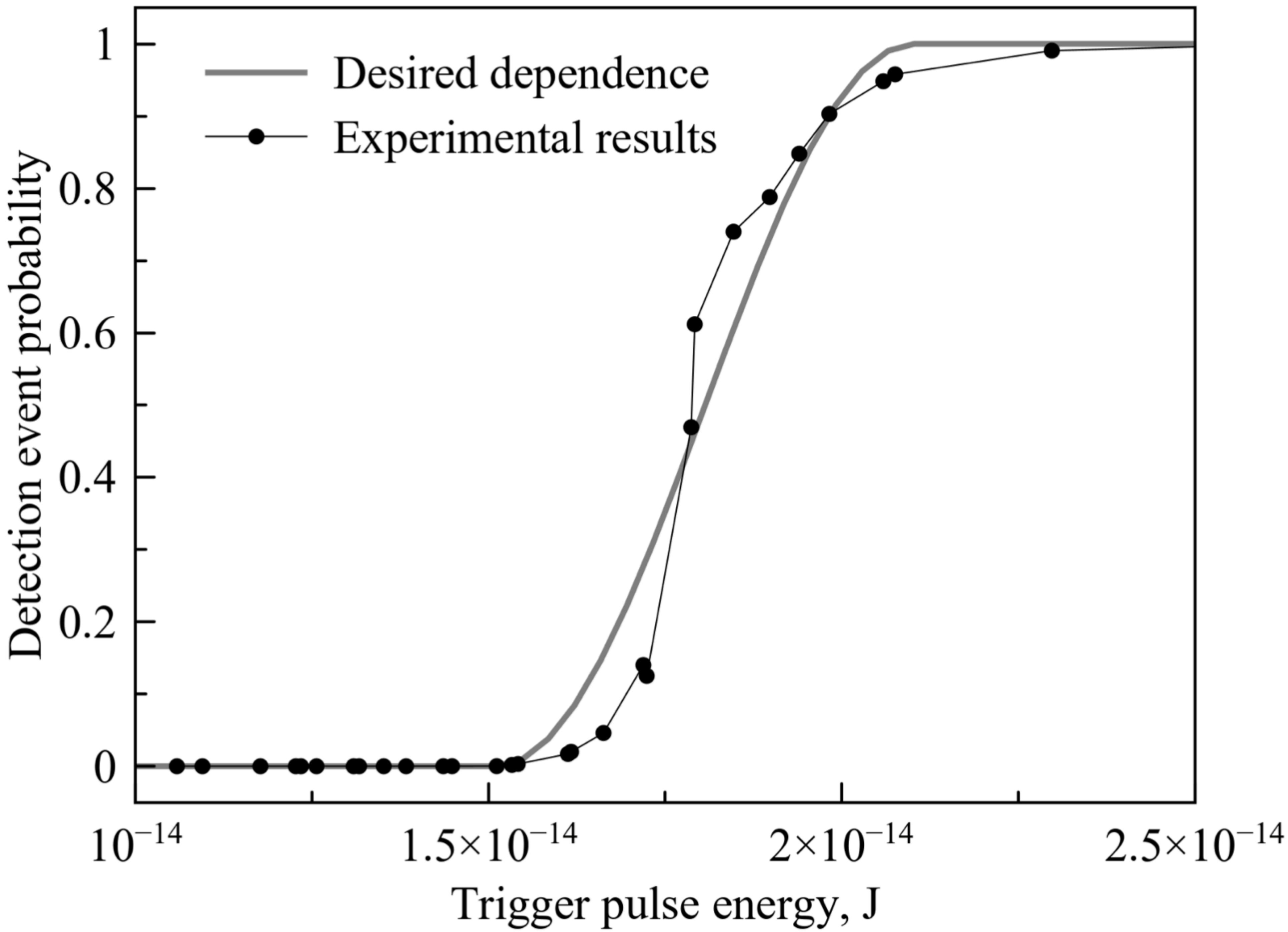
$\Delta\phi_{\mathscr{E}\mathscr{B}} = 0 \longrightarrow$ ✓

$\Delta\phi_{\mathscr{E}\mathscr{B}} = \pi \longrightarrow$ ✗

$\Delta\phi_{\mathscr{E}\mathscr{B}} \neq 0 \longrightarrow$ ✗

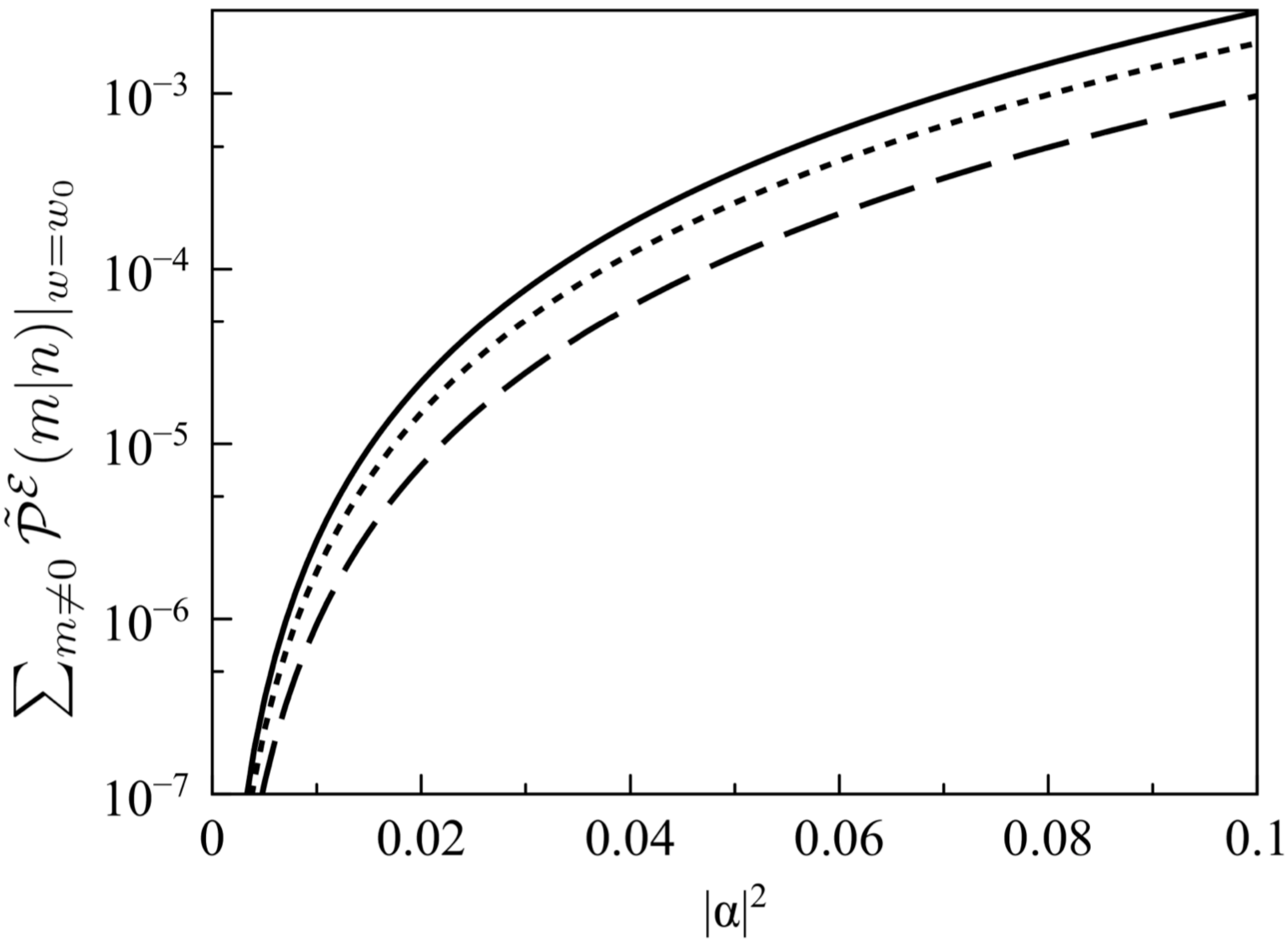
$\Delta\phi_{\mathscr{E}\mathscr{B}} \neq \pi \longrightarrow$ ✓

Fake-state attack



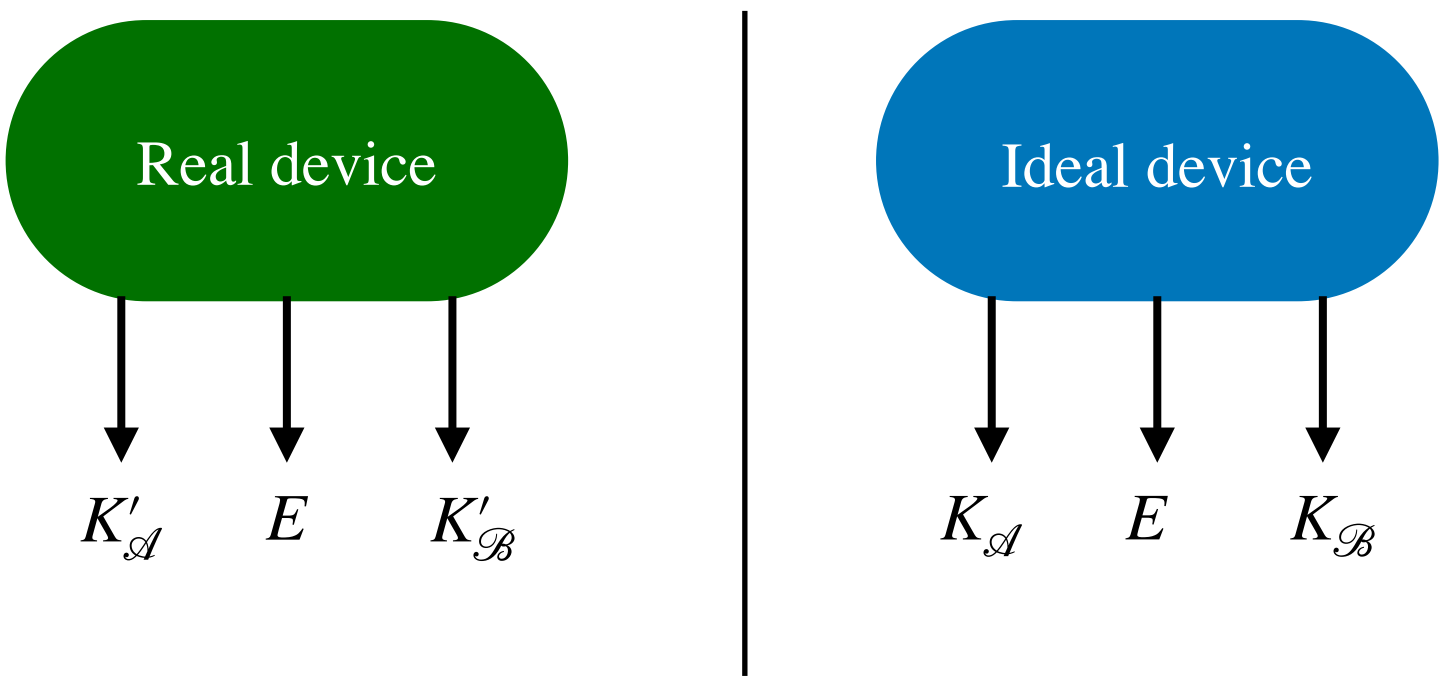
Dependence of detection event probability on trigger pulse energy. Dotted line represents actual experimental data from for 35 nW blinding power as an example that demonstrates typical shape of the curve. Solid grey line is desired shape of detector response that can mimic detection probability dependent on phase difference in the interferometric scheme.

Fake-state attack



Dependencies of detection rate with introduced error $\sum_{m\neq 0}\mathscr{P}^{\mathscr{E}}(m|n)$ from mean photon number for different types of state imposing. Solid line corresponds to the case then $\mathscr{P}^{\mathscr{E}}(b|e)=\frac{2N-1}{2N}$. Doted line corresponds to the case the $\mathscr{P}^{\mathscr{E}}(b|e)$ has harmonic-like (phase-difference dependence) behaviour. Dash line corresponds to the case then $\mathscr{P}^{\mathscr{E}}(b|e)=\frac{1}{2N}$

Security notation



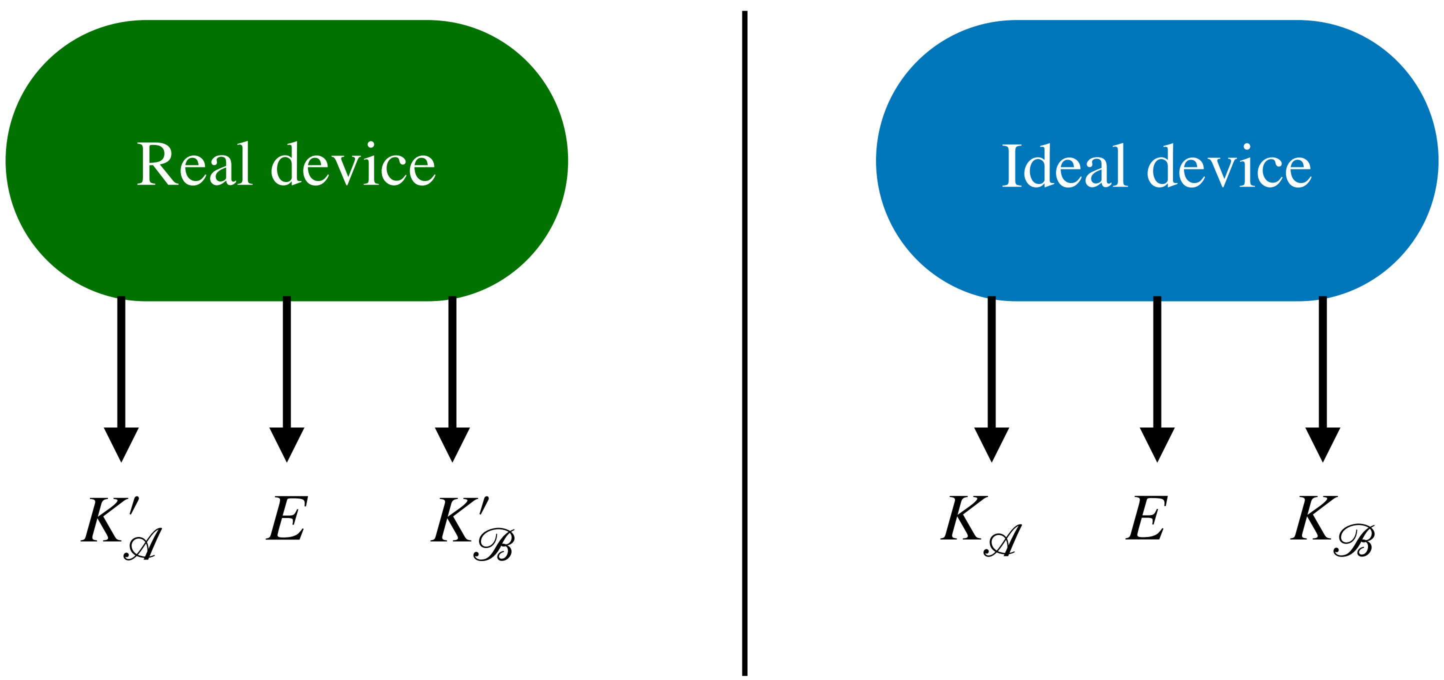
$$n_0 \sum_{b \neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a) + z\sqrt{\sigma^{\mathscr{E}}} < n_0 \sum_{b \neq 0} \mathscr{P}(b\,|\,a) - z\sqrt{\sigma},$$

$$\sigma^{\mathscr{E}} = n_0 \sum_{b \neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a)\Big(1 - \sum_{b \neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a)\Big),$$

$$\sigma = n_0 \sum_{b \neq 0} \mathscr{P}(b\,|\,a)\Big(1 - \sum_{b \neq 0} \mathscr{P}(b\,|\,a)\Big),$$

- n_0 is the number of sent states,
- z is the arbitrary number of standard deviations σ and $\sigma^{\mathscr{E}}$ within the confidence interval according to the so-called ``three--sigma rule''

Security notation



$$n_0 \sum_{b\neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a) + z\sqrt{\sigma^{\mathscr{E}}} < n_0 \sum_{b\neq 0} \mathscr{P}(b\,|\,a) - z\sqrt{\sigma},$$

$$\sigma^{\mathscr{E}} = n_0 \sum_{b\neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a)\Big(1 - \sum_{b\neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a)\Big),$$

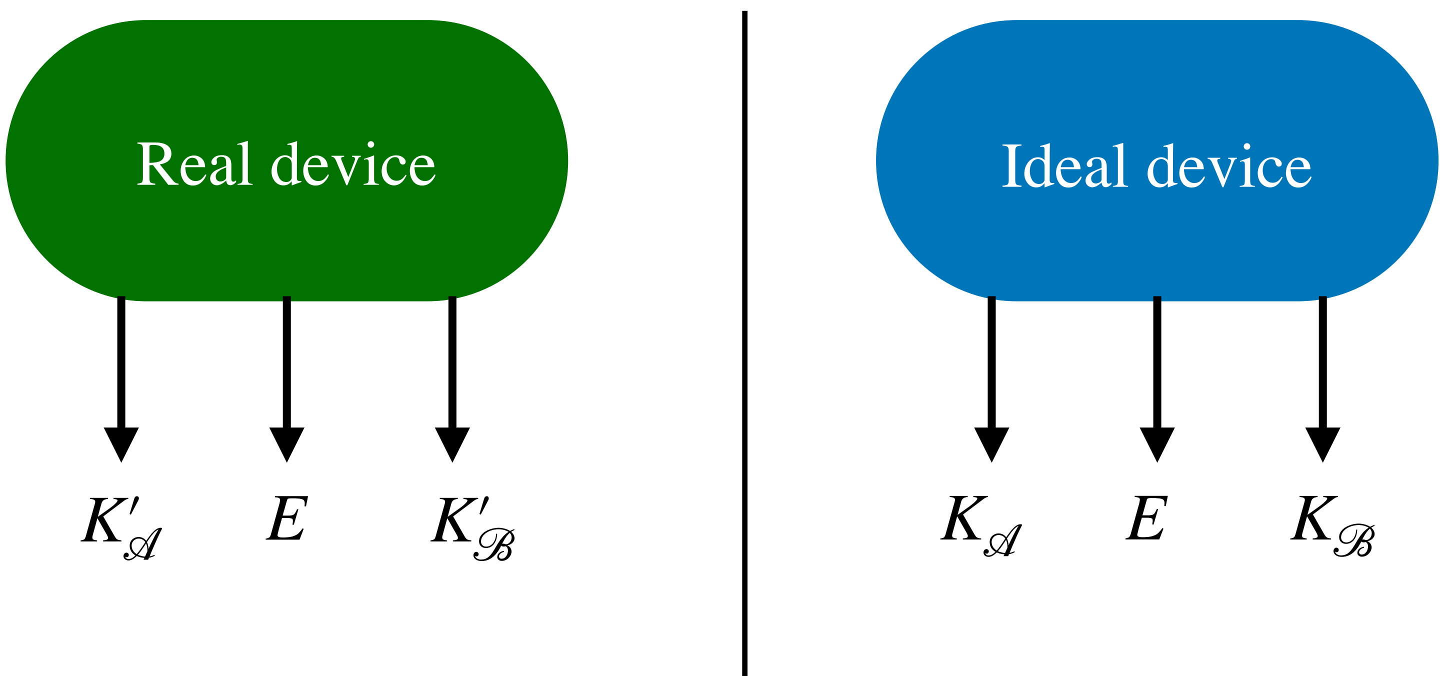
$$\sigma = n_0 \sum_{b\neq 0} \mathscr{P}(b\,|\,a)\Big(1 - \sum_{b\neq 0} \mathscr{P}(b\,|\,a)\Big),$$

- n_0 is the number of sent states,
- z is the arbitrary number of standard deviations σ and $\sigma^{\mathscr{E}}$ within the confidence interval according to the so-called ``three--sigma rule''

$$\varepsilon_{QC} = 1 - \mathrm{erf}(\frac{z_0}{\sqrt{2}})$$

$$z_0 = \frac{n_0 \sum_{b\neq 0} \left(\mathscr{P}(b\,|\,a) - \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a)\right)}{\sqrt{\sigma^{\mathscr{E}}} + \sqrt{\sigma}}.$$

Security notation



$$n_0 \sum_{b \neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a) + z\sqrt{\sigma^{\mathscr{E}}} < n_0 \sum_{b \neq 0} \mathscr{P}(b\,|\,a) - z\sqrt{\sigma},$$

$$\sigma^{\mathscr{E}} = n_0 \sum_{b \neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a)\Big(1 - \sum_{b \neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a)\Big),$$

$$\sigma = n_0 \sum_{b \neq 0} \mathscr{P}(b\,|\,a)\Big(1 - \sum_{b \neq 0} \mathscr{P}(b\,|\,a)\Big),$$

- n_0 is the number of sent states,
- z is the arbitrary number of standard deviations σ and $\sigma^{\mathscr{E}}$ within the confidence interval according to the so-called ``three--sigma rule''

$$\varepsilon_{QC} = 1 - \mathrm{erf}\Big(\frac{z_0}{\sqrt{2}}\Big)$$

$$z_0 = \frac{n_0 \sum_{b \neq 0} \big(\mathscr{P}(b\,|\,a) - \tilde{\mathscr{P}}^{\mathscr{E}}(b\,|\,a)\big)}{\sqrt{\sigma^{\mathscr{E}}} + \sqrt{\sigma}}.$$

$$d = ||\rho_{K'E} - \omega_K \otimes \sigma_E||_1 \leq \varepsilon \longrightarrow \boxed{\varepsilon_{Attack} = \varepsilon_{QC} \cdot \varepsilon_{DF}.}$$

Thank you!

avkozubov@itmo.ru

Kozubov A., Gaidash A., Miroshnichenko G. Quantum control attack: Towards joint estimation of protocol and hardware loopholes // Physical Review A. – 2021. – T. 104. – No. 2. – C. 022603.