QKD with correlated sources

Margarida Pereira

Collaborators: Go Kato, Akihiro Mizutani, Marcos Curty, Kiyoshi Tamaki

UniversidadeVigo NTT MITSUBISHI ELECTRIC UNIVERSITY OF TOYAMA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662

Security of QKD

Theory vs practice

Ideal devices
No imperfections

Real devices
Imperfections

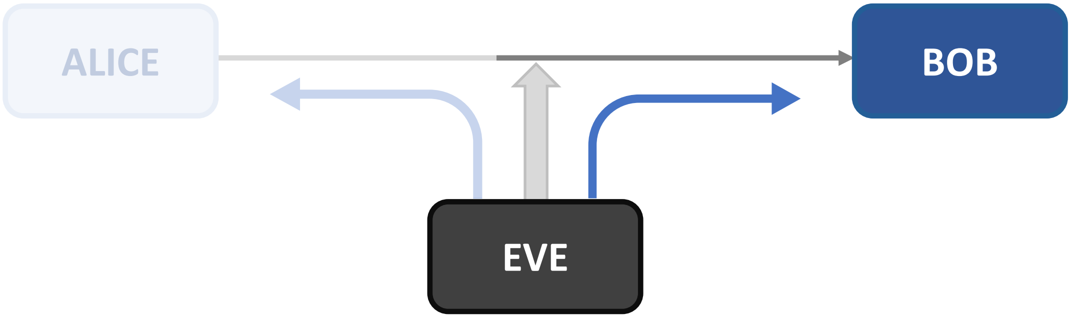
Theoretic security ≠ Implementation security [1]

[1] H.-K. Lo, M. Curty and K. Tamaki, Nat. Photonics **8**, 595-604 (2014);

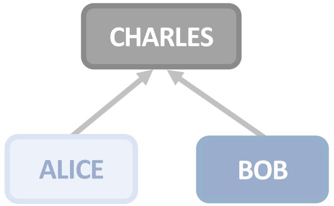
Securing the detector

Well-known detector attacks:

- Time-shift attack [2]
- Faked state attack [3,4]
- Phase-remapping attack [5]
- …



➡ Solution: **MDI-QKD** [6]



Removes all assumptions on the detectors

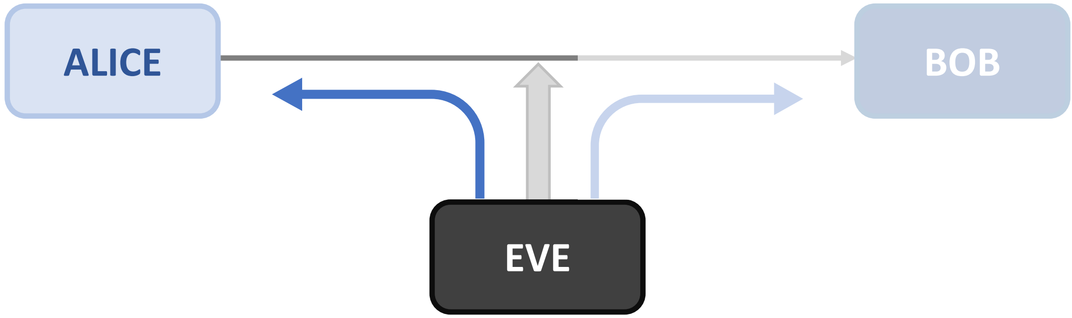
Eliminates all detector side-channel attacks

+ good performance
+ practical with current technology

[2] Y. Zhao et al., Phys. Rev. A **78**, 042333 (2008); [3] I. Gerhardt et al., Nat. Commun. **2**, 349 (2011); [4] L. Lydersen et al., Nat. Photonics **4**, 686-689 (2010); [5] F. Xu et al., New. J. Phys. **12**, (2010); [6] H.-K. Lo et al., Phys. Rev. Lett. **108**, 130501 (2012);

Securing the source

The emitted pulses are usually **assumed to be perfect**



Main source imperfections:

- State preparation flaws [7-10]
- Trojan horse attacks [10-12]
- Spontaneous information leakage [10,13]
- **Pulse correlations**

Final piece towards guaranteeing implementation security

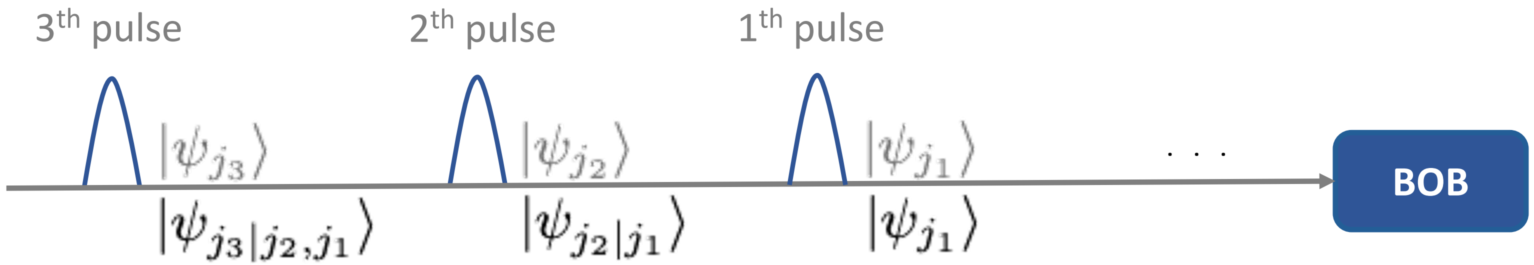
Incorporate source imperfections in the security proofs to ensure the practical security of QKD

[7] T. Honjo et al., Opt. Lett. **29**, 2797-2799 (2004); [8] Z. Tang et al., Phys. Rev. A **93**, 042308 (2016); [9] K. Tamaki et al., Phys. Rev. A **90**, 052314 (2014); [10] M. Pereira et al., npj Quantum Information **5**, 62 (2019); [11] A. Vakhitov et al., J. Mod. Opt. **48**, 2023 (2001); [12] M. Lucamarini et al., Phys. Rev. X **5**, 031030 (2015); [13] F. Xu et al., Phys. Rev. A **92**, 032305 (2015);

Pulse correlations

How?
Arise due to memory effects of practical modulation devices

Occur when the state of the emitted pulses depend on the previous setting choices j_k made by Alice



➡ **Problem in practical high-speed QKD systems** [14,15]

[14] K.-i. Yoshino et al., npj Quantum Information **4**, 8 (2018); [15] F. Grünenfelder, et. al, preprint on arXiv:2007.15447 (2020);

Pulse correlations II

It is believed that pulse correlations are **negligibly small**

But in high-speed QKD systems they cannot be ignored [14,15]

It is believed that pulse correlations are **very hard to model** mathematically

Previous works have considered only restricted scenarios [15,16]

→ Our work: <u>Security framework to deal with arbitrary pulse correlations</u> [17]

Key point

Leaked information encoded in subsequent pulses is regarded as a side-channel for each of the emitted pulses

[14] K.-i. Yoshino et al., npj Quantum Information **4**, 8 (2018); [15] F. Grünenfelder, et. al, preprint on arXiv:2007.15447 (2020); [16] A. Mizutani et al., npj Quantum Information **5**, 8 (2019); [17] M. Pereira et al., in press, preprint on arXiv:1908.08261 (2019);

Security with correlated sources

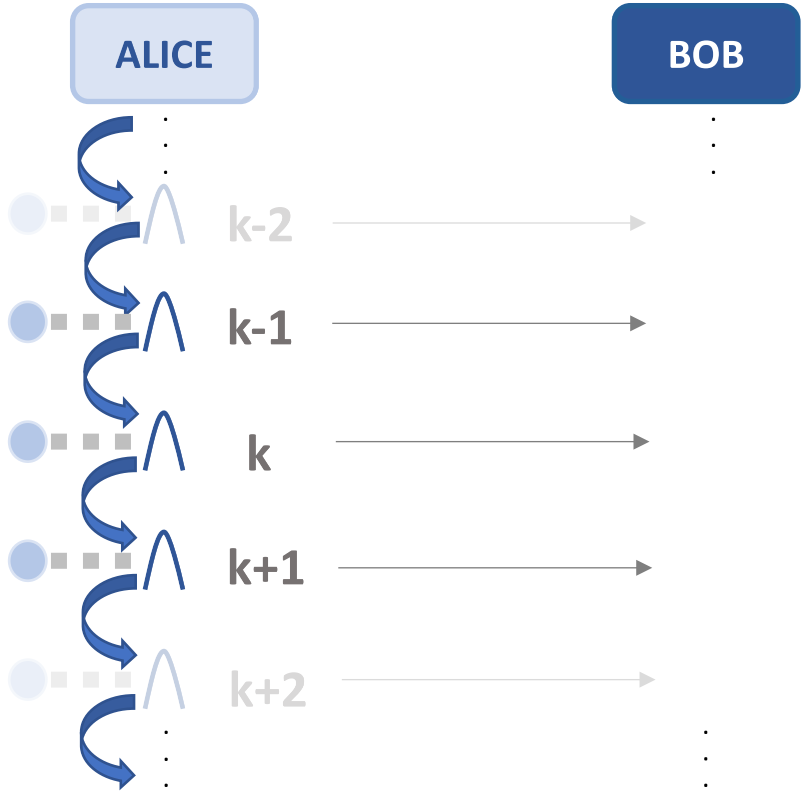
Nearest neighbour pulse correlations

Three-state protocol

Alice chooses $|\psi_j\rangle_B$ with $j \in \{0_Z, 1_Z, 0_X\}$, and sends the pulse in the prepared state to Bob

Entanglement-based virtual protocol

Alice prepares n ancilla systems A and n pulses in the following state and sends system B to Bob



$$|\Psi\rangle_{AB} = \sum_{j_1} |j_1\rangle_{A_1} |\psi_{j_1}\rangle_{B_1} \sum_{j_2} |j_2\rangle_{A_2} |\psi_{j_2|j_1}\rangle_{B_2} \cdots \sum_{j_n} |j_n\rangle_{A_n} |\psi_{j_n|j_{n-1}}\rangle_{B_n}$$

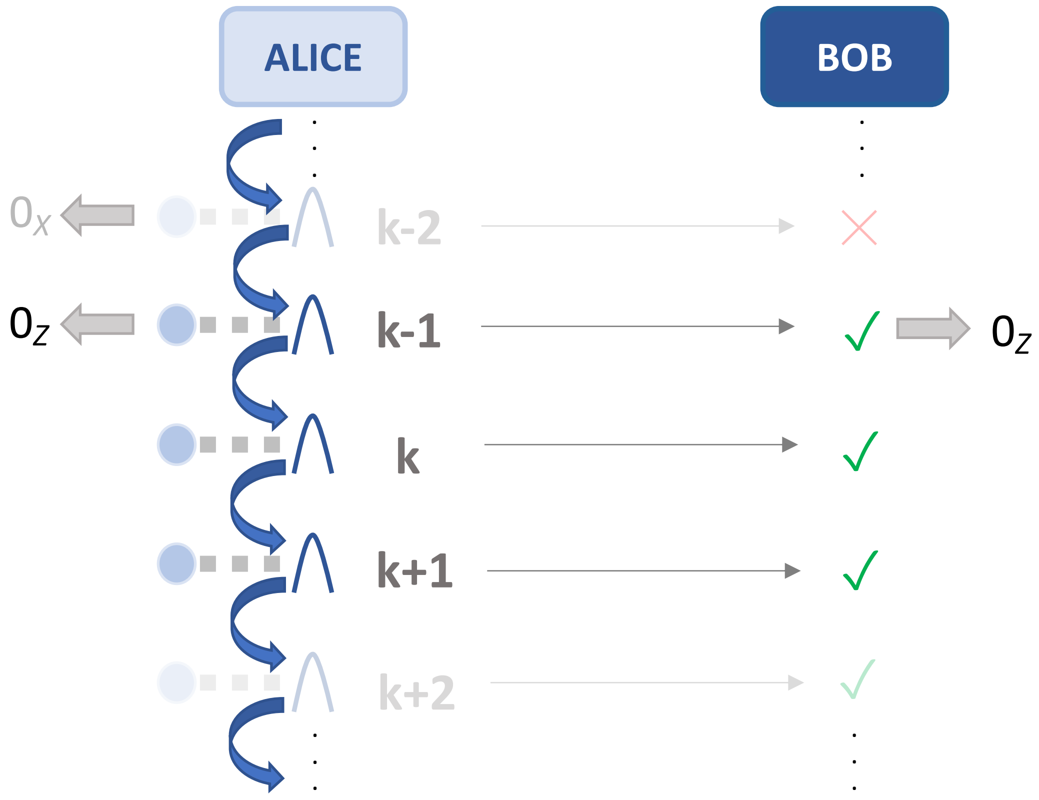
Security with correlated sources

Entanglement-based virtual protocol

Bob obtains click events for some of the received signals

Alice and Bob perform measurements on their local systems to generate the raw data for the experiment

Consider the complementary scenario[18] to **estimate the phase error rate**



[18] M. Koashi, New J. Phys. **11**, 045018 (2009);

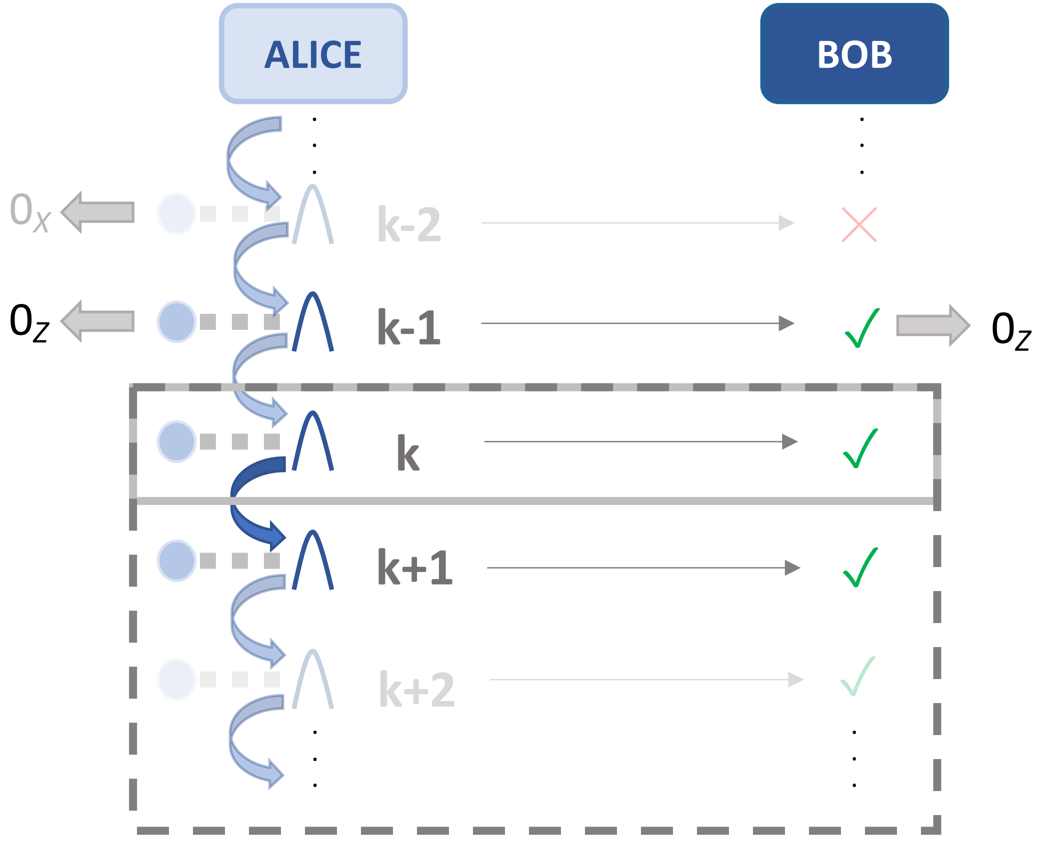
Security with correlated sources

Estimating the phase error rate

Estimate the probability of phase error by considering any attack on a particular detected pulse ⟶ **k^{th} pulse**

Security against **coherent attacks**: use Azuma's[19] or Kato's inequality[20], Post-selection technique[21] or Entropy accumulation theorem[22]

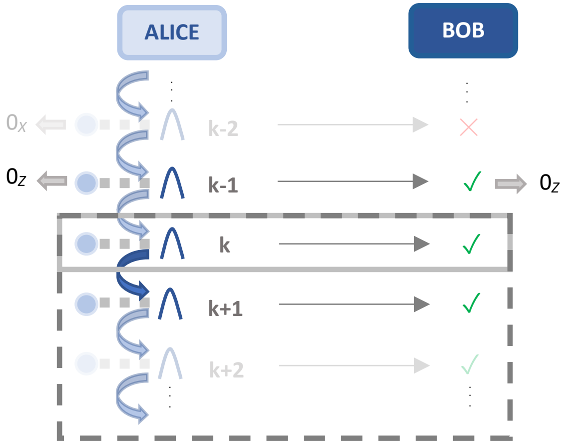
If we can estimate the phase error probability in this case, the security of the protocol follows



[19] K. Azuma, Tohoku Mathematical Journal **19**, 357-367 (1967); [20] G. Kato, preprint on arXiv:2002.04357 (2020); [21] M. Christandl, R. König and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009); [22] F. Dupuis, O. Fawzi and R. Renner, preprint on arXiv:1607.01796 (2016);

Pulse with a side-channel

Nearest neighbour pulse correlations



Assume that Alice already measured her first *k-1* ancillas

$$|j'_1\rangle_{A_1} |\psi_{j'_1}\rangle_{B_1} \cdots |j'_{k-1}\rangle_{A_{k-1}} |\psi_{j'_{k-1}|j'_{k-2}}\rangle_{B_{k-1}} \sum_{j_k} |j_k\rangle_{A_k} |\psi_{j_k|j'_{k-1}}\rangle_{B_k} \sum_{j_{k+1}} |j_{k+1}\rangle_{A_{k+1}} |\psi_{j_{k+1}|j_k}\rangle_{B_{k+1}} \cdots \sum_{j_n} |j_n\rangle_{A_n} |\psi_{j_n|j_{n-1}}\rangle_{B_n}$$

$$\underbrace{\sum_{j_{k+1}} |j_{k+1}\rangle_{A_{k+1},\cdots,A_n,B_{k+2},\cdots,B_n,} |\psi_{j_{k+1}|j_k}\rangle_{B_{k+1}}}_{\downarrow}$$

$$|\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}$$

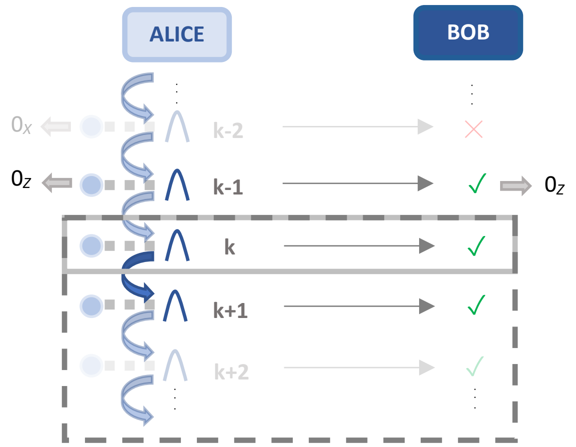
The terms after $\sum_{j_{k+1}}$ depend on the setting j_k and we can treat them as just a single state

$$\Rightarrow |j'_1\rangle_{A_1} |\psi_{j'_1}\rangle_{B_1} \cdots |j'_{k-1}\rangle_{A_{k-1}} |\psi_{j'_{k-1}|j'_{k-2}}\rangle_{B_{k-1}} \sum_{j_k} |j_k\rangle_{A_k} |\psi_{j_k|j'_{k-1}}\rangle_{B_k} \boxed{|\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}}$$

Side-channel information about the k^{th} pulse

Pulse with a side-channel II

Nearest neighbour pulse correlations



$$|j_1'\rangle_{A_1}|\psi_{j_1'}\rangle_{B_1}\cdots|j_{k-1}'\rangle_{A_{k-1}}|\psi_{j_{k-1}'}\rangle_{B_{k-1}}\sum_{j_k}|j_k\rangle_{A_k}|\psi_{j_k}\rangle_{B_k}|\lambda\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}$$

$$\sum_{j_{k+1}}|j_{k+1}\rangle_{A_{k+1}}|\psi_{j_{k+1}}\rangle_{B_{k+1}}\cdots\sum_{j_n}|j_n\rangle_{A_n}|\psi_{j_n}\rangle_{B_n}$$

with pulse correlations

$$|j_1'\rangle_{A_1}|\psi_{j_1'}\rangle_{B_1}\cdots|j_{k-1}'\rangle_{A_{k-1}}|\psi_{j_{k-1}'|j_{k-2}'}\rangle_{B_{k-1}}\sum_{j_k}|j_k\rangle_{A_k}|\psi_{j_k|j_{k-1}'}\rangle_{B_k}|\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}$$

Obtain the probability of a phase error by considering any attack on the systems $A_{k+1},\cdots,A_n,B_k,\cdots,B_n$ ⟹ **Security with correlated pulses is guaranteed!**

Protocol with pulse correlations

A protocol where Alice prepares the states $\{|\psi_{j_k|j_{k-1}'}\rangle_{B_k}|\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}\}_{j_k\in\{0_Z,1_Z,0_X\}}$ for any pulse *k* and sends systems $A_{k+1},\cdots,A_n,B_k,\cdots,B_n$ to Bob

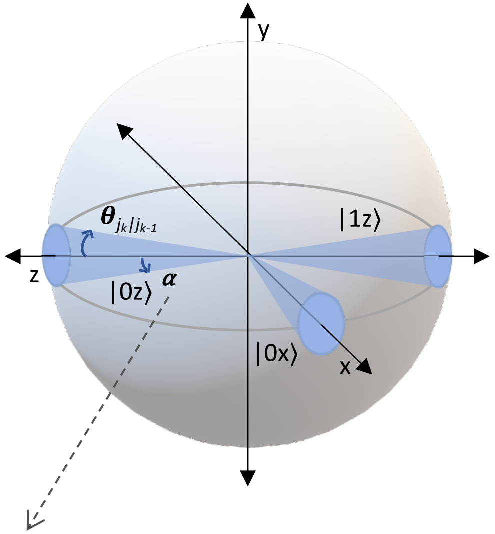
Modelling pulse correlations

Nearest neighbour pulse correlations

Particular device model for pulse correlations

$$\boxed{|\psi_{j_k|j_{k-1}}\rangle_{B_k} = \sqrt{1-\epsilon}\,|\phi_{j_k}\rangle_{B_k} + e^{i\theta_{j_k|j_{k-1}}}\sqrt{\epsilon}\,|\phi_{j_k}^{\perp}\rangle_{B_k}}$$

Idealised state



Angle associated with $\sqrt{1-\epsilon}$

More generally, ϵ could also depend on $j_k|j_{k-1}$

Recall: The states $|\psi_{j_k|j'_{k-1}}\rangle_{B_k}|\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}$ can be expressed as

$$|\psi_{j_k|j'_{k-1}}\rangle_{B_k}\sum_{j_{k+1}}|j_{k+1}\rangle_{A_{k+1},\cdots,A_n,B_{k+2},\cdots,B_n}|\psi_{j_{k+1}|j_k}\rangle_{B_{k+1}}$$

$$=: (1-\epsilon)|\phi_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n} + \sqrt{1-(1-\epsilon)^2}\,|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}$$

Modelling pulse correlations II

Nearest neighbour pulse correlations

Recall: Particular device model for pulse correlations

$$|\psi_{j_k|j'_{k-1}}\rangle_{B_k} = \sqrt{1-\epsilon}\,|\phi_{j_k}\rangle_{B_k} + e^{i\theta_{j_k|j'_{k-1}}}\sqrt{\epsilon}\,|\phi^{\perp}_{j_k}\rangle_{B_k}$$

$$|\psi_{j_k|j'_{k-1}}\rangle_{B_k}|\lambda_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_{k+1},\cdots,B_n}$$

$$=: (1-\epsilon)\underbrace{|\phi_{j_k}\rangle_{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}}_{\text{Qubit state}} + \sqrt{1-(1-\epsilon)^2}\,|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_{\boxed{A_{k+1},\cdots,A_n,B_k,B_{k+1},\cdots,B_n}^{B}}$$

$$|\phi_{j_k}\rangle_{B_k}\sum_{j_{k+1}}|j_{k+1}\rangle_{A_{k+1},\cdots,A_n,B_{k+2},\cdots,B_n}|\phi_{j_{k+1}}\rangle_{B_{k+1}}$$

Alice's systems

Fictitiously consider an attack on $A_{k+1},\cdots,A_n$

By simplifying the notation, we can express the state of the kth pulse as

$$\boxed{|\psi_{j_k|j'_{k-1}}\rangle_B = (1-\epsilon)\,|\phi_{j_k}\rangle_B + \sqrt{1-(1-\epsilon)^2}\,|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_B}\ *$$

*Model compatible with our previous work that incorporates other main source imperfections

[10] M. Pereira, M. Curty and K. Tamaki, npj Quantum Information **5**, 62 (2019);

Arbitrarily long range pulse correlations

- The analysis also applies to arbitrarily long range pulse correlations [17]

  The k^{th} pulse may depend on all the previous setting choices

- Even in the case of long range pulse correlations it is straightforward to obtain a state similar to $\left|\psi_{j_k|j'_{k-1}}\right\rangle_B = (1-\epsilon)\left|\phi_{j_k}\right\rangle_B + \sqrt{1-(1-\epsilon)^2}\left|\phi^{\perp}_{j_k|j'_{k-1}}\right\rangle_B$

Key point

The framework is valid for arbitrarily long range pulse correlations

[17] M. Pereira, G. Kato, A. Mizutani, M. Curty and K. Tamaki, in press, preprint on arXiv 1908.08261 (2019);

Security with correlated sources II

Recall: In the presence of pulse correlations the emitted states are

$$\boxed{|\psi_{j_k|j'_{k-1}}\rangle_B = (1-\epsilon)\,|\phi_{j_k}\rangle_B + \sqrt{1-(1-\epsilon)^2}\,|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_B}$$

Pulse correlations can be regarded as a side-channel

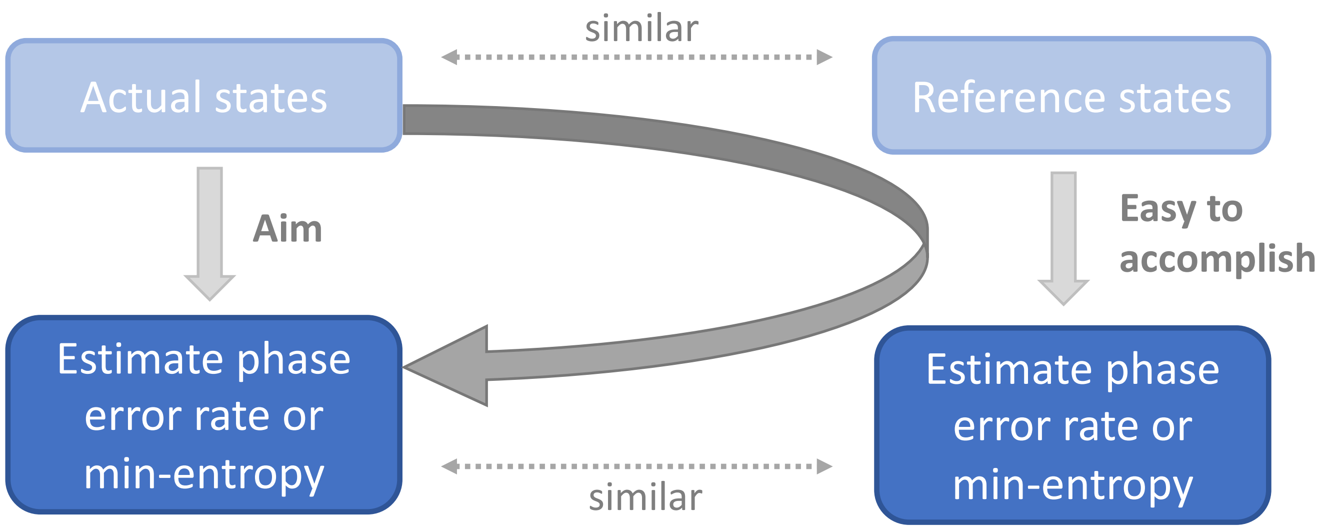
Simply use existing security proofs that deal with side-channels

- Require a full characterisation of side-channel state
- Have a poor performance

⟹ Solution: Reference Technique[17]

[17] M. Pereira, G. Kato, A. Mizutani, M. Curty and K. Tamaki, in press, preprint on arXiv 1908.08261 (2019);

Reference technique



Use reference states as intermediate parameters to estimate the quantities required for the security proof

Key point

Framework for security proofs to deal with any device imperfections

Choosing the reference states

- Select reference states that are similar to the actual states
- Convenient to select reference states that are in a qubit space
  Use directly the **loss-tolerant protocol**[9]

Example: **Three-state protocol** with nearest neighbour pulse correlations

Recall: Each pulse emission from a correlated source can be expressed as

$$|\psi_{j_k|j_{k-1}}\rangle_B = (1-\epsilon)\boxed{|\phi_{j_k}\rangle_B} + \sqrt{1-(1-\epsilon)^2}\,|\phi^{\perp}_{j_k|j_{k-1}}\rangle_B \quad \text{for } j_k \in \{0_Z, 1_Z, 0_X\}$$

Reference states

Actual states

[9] K. Tamaki, M. Curty, G. Kato, H.-K. Lo and K. Azuma, Phys. Rev. A **90**, 052314 (2014);

Choosing the reference states II

Actual states ⟷ similar ⟷ Reference states

$$|\phi_{0_Z}\rangle_B = |0_Z\rangle_B$$
$$|\phi_{1_Z}\rangle_B = -\sin\left(\frac{\delta}{2}\right)|0_Z\rangle_B + \cos\left(\frac{\delta}{2}\right)|1_Z\rangle_B$$
$$|\phi_{0_X}\rangle_B = \cos\left(\frac{\pi}{4}+\frac{\delta}{4}\right)|0_Z\rangle_B + \sin\left(\frac{\pi}{4}+\frac{\delta}{4}\right)|1_Z\rangle_B$$

State preparation flaws

Deviation of the phase modulation from the intended value

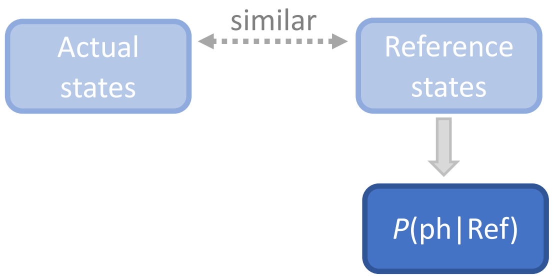
$$\boxed{|\psi_{j_k|j_{k-1}}\rangle_B = (1-\epsilon)\boxed{|\phi_{j_k}\rangle_B} + \sqrt{1-(1-\epsilon)^2}\,|\phi^{\perp}_{j_k|j_{k-1}}\rangle_B}$$

for $j_k \in \{0_Z, 1_Z, 0_X\}$

Reference states **Actual states**

Obtaining the reference formula

Aim: expression for *P*(ph|Ref)



By directly employing the **loss-tolerant protocol**[9] we find that

Coefficients

$$\frac{P(\mathrm{ph}|\mathrm{Ref})}{P_{Z_A} P_{Z_B}} = \sum_{j,\beta} a_{j,\beta} Y_{j,\beta}^{\mathrm{Ref}}$$

Conditional probabilities associated with the reference states

Alice's setting choice

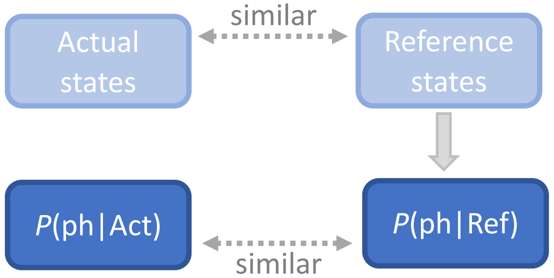
Bob's measurement

- This derivation is purely mathematical
- ***P*(ph|Ref) cannot be used directly in the security proof**

[9] K. Tamaki, M. Curty, G. Kato, H.-K. Lo and K. Azuma, Phys. Rev. A **90**, 052314 (2014);

Deviation evaluation

Aim: expression for *P*(ph|Act)



Transform the expression for *P*(ph|Ref) into an expression for *P*(ph|Act) by using the following bound

$$\boxed{g^L\left(Y^{\mathrm{Act}}, |\langle A|\, R\rangle|\right) \leq Y^{\mathrm{Ref}} \leq g^U\left(Y^{\mathrm{Act}}, |\langle A|\, R\rangle|\right)}$$

Bound used in the Lo-Preskill's analysis[23]

Recall: $\dfrac{P(\mathrm{ph}|\mathrm{Ref})}{P_{Z_A}P_{Z_B}} = \sum_{j,\beta} a_{j,\beta} Y^{\mathrm{Ref}}_{j,\beta}$

$$g^L\left(\frac{P(\mathrm{ph}|\mathrm{Act})}{P_{Z_A}P_{Z_B}}, |\langle A_{(\mathrm{vir})}|\, R_{(\mathrm{vir})}\rangle|\right) \leq \sum_{j,\beta|a_{j,\beta}>0} a_{j,\beta}\, g^U\left(\frac{P(j,\beta|\mathrm{Act})}{P_j P_{X_B}}, |\langle A_j|\, R_j\rangle|\right) + \sum_{j,\beta|a_{j,\beta}<0} a_{j,\beta}\, g^L\left(\frac{P(j,\beta|\mathrm{Act})}{P_j P_{X_B}}, |\langle A_j|\, R_j\rangle|\right)$$

Solve for *P*(ph|Act)!

[23] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 431-458 (2007);

Employing the reference technique

Recall: The emitted states can be expressed as

$$|\psi_{j_k|j_{k-1}}\rangle_B = (1-\epsilon)\,|\phi_{j_k}\rangle_B + \sqrt{1-(1-\epsilon)^2}\,|\phi^{\perp}_{j_k|j_{k-1}}\rangle_B$$

Actual states

Reference technique

Estimate phase error rate or min-entropy

$$R \geq Y_Z[1 - h(e_{\text{ph}}) - f h(e_{\text{bit}})]$$

Secret key rate

Aside:

The GLLP type security proofs [23, 24] and the GLT protocol [10] can be regarded as a special case of the reference technique

To prove the security we **only** require an upper bound on the coefficient ϵ

No characterisation is needed for the side-channel states!

[23] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 431-458 (2007); [24] D. Gottsman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quantum Inf. Comput. **4**, 325-360 (2004); [10] M. Pereira, M. Curty and K. Tamaki, npj Quantum Information **5**, 62 (2019);

QKD with correlated sources

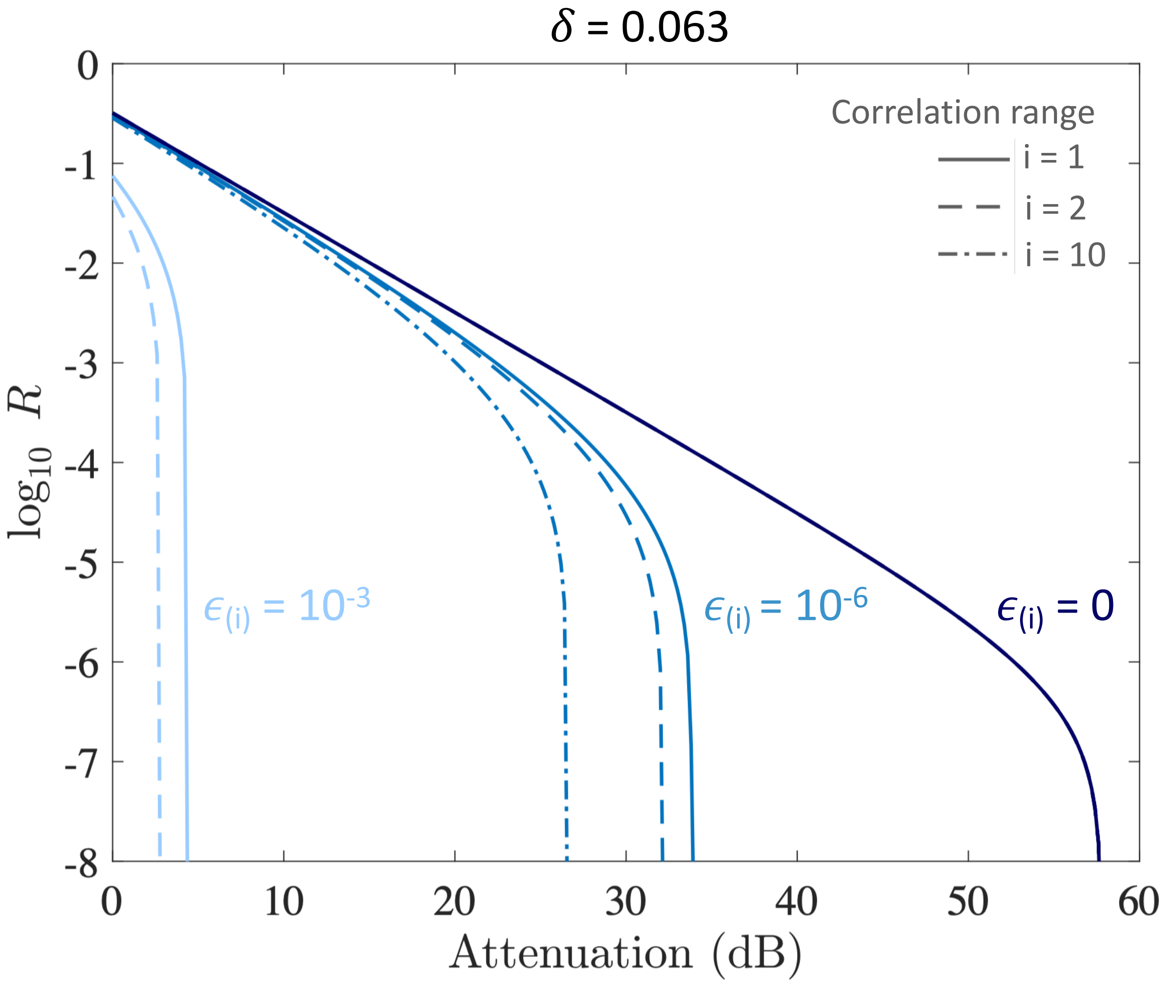
Using the reference technique with pulse correlations

As the deviation between the actual and the reference states increases the secret key rate decreases

When ϵ is small enough, one can consider very long pulse correlations while ensuring the security of QKD

Recall: The emitted states can be expressed as

$$|\psi_{j_k|j_{k-1}}\rangle_B = (1-\epsilon)\,|\phi_{j_k}\rangle_B + \sqrt{1-(1-\epsilon)^2}\,|\phi^{\perp}_{j_k|j_{k-1}}\rangle_B$$



Conclusion

- We have introduced a **simple formalism to deal with pulse correlations** – the final piece for securing the source

- We have demonstrated that the state of an emitted pulse in the presence of correlations has the form $|\psi_{j_k|j'_{k-1}}\rangle_B = (1-\epsilon)\,|\phi_{j_k}\rangle_B + \sqrt{1-(1-\epsilon)^2}\,|\phi^{\perp}_{j_k|j'_{k-1}}\rangle_B$

- Our formalism is compatible with a previous security proof [10] that already incorporates state preparation flaws, Trojan horse attacks and spontaneous leakage of information

[10] M. Pereira, M. Curty and K. Tamaki, npj Quantum Information **5**, 62 (2019);

Conclusion II

- We have proposed a new **framework for security proofs** that guarantees high secret key rates in the presence of flawed, leaky and correlated sources

- By combining this work with an MDI-QKD type of protocol one can guarantee the implementation security of QKD
  Check out our latest work! [25]

- The next step is to adapt our analysis to the decoy-state method and consider pulse correlations in the intensity modulator

[25] A. Navarrete, M. Pereira, M. Curty and K. Tamaki, preprint on arXiv:2007.03364 (2020);