



Security Proofs for QKD Protocols in Infinite Dimensions

Twesh Upadhyaya, Thomas van Himbeeck, Jie Lin, Norbert Lütkenhaus

Institute for Quantum Computing, University of Waterloo

QCrypt 2021

August 25, 2021

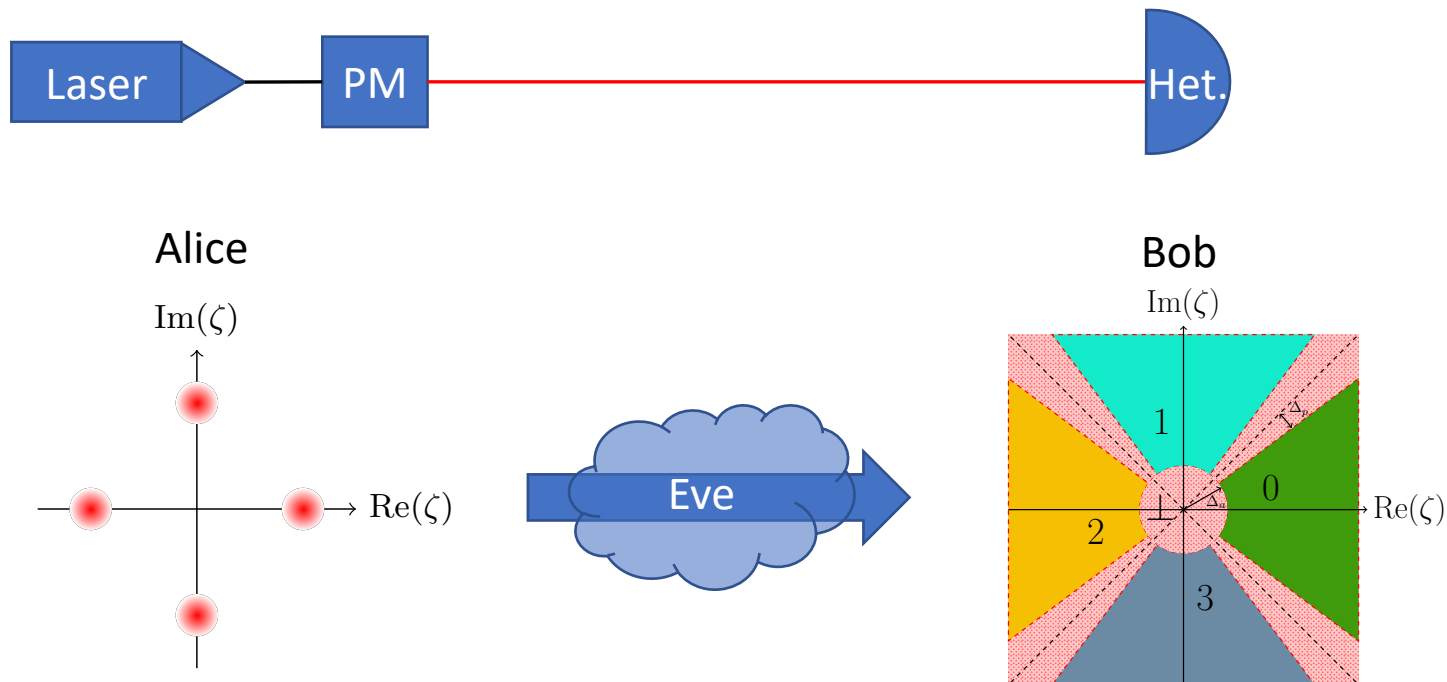
<https://doi.org/10.1103/PRXQuantum.2.020325>

Outline

- Introduction
- Dimension Reduction Method
- Application to Discrete-Modulated Continuous-Variable QKD
- Application to Unbalanced BB84
- Conclusion

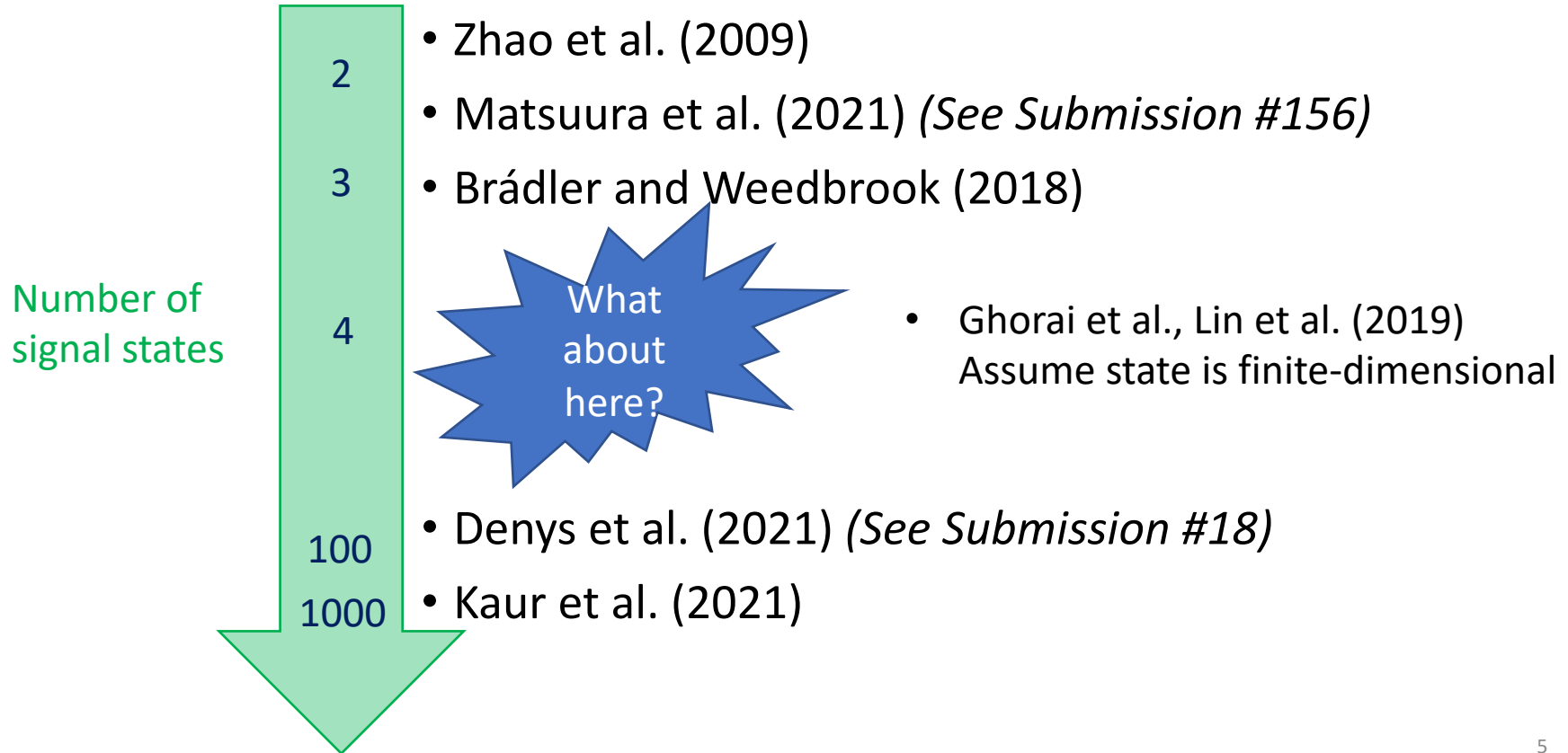
Introduction

Discrete-Modulated Continuous-Variable QKD



- Integrates with existing telecom technology
- Minimal requirements on source modulator
- **Promising candidate** for large-scale quantum-secured networks

Needed a security proof for small (but not too small!) numbers of signal states



Approaches to proving the security of DMCVQKD with four states

❌ Existing DMCVQKD security proofs?

Not for 4 states

❌ Optimality of Gaussian attacks?

Only for Gaussian modulation

❌ Squashing techniques?

Only for discrete-variable QKD


❌ Numerical key rates?

Only for finite dimensions

... at least not directly

Steps of a generic QKD protocol

Q

1. Establish a state ρ_{AB}
 2. Measure subsystems
- 

C

3. Parameter estimation
4. Announcements and sifting
5. Key map
6. Error correction
7. Privacy amplification

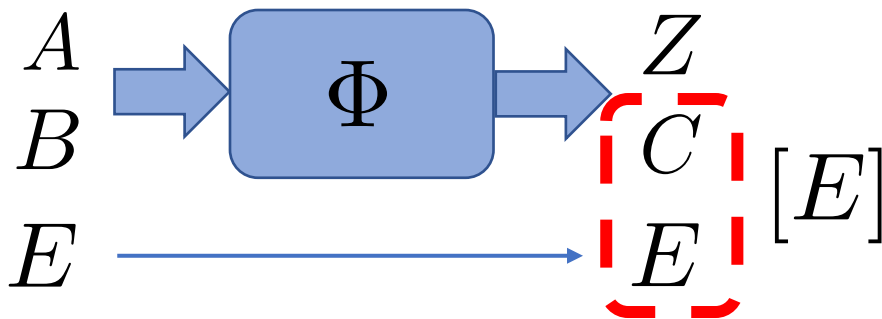
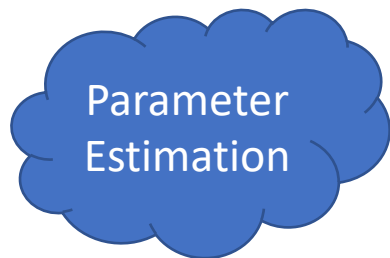
The key rate can be formulated as a convex minimization over states, and solved numerically

- Asymptotic, collective attacks (IID)
- Devetak-Winter formula:

$$R^\infty = \inf_{\rho_{AB} \in \mathbf{S}_\infty} [f(\rho_{AB})] - \delta_{EC}^{leak}$$

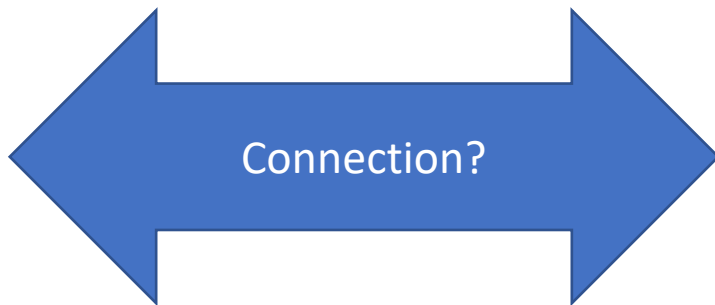
|||

$$H(Z|[E])_{\Phi(\rho_{ABE})}$$



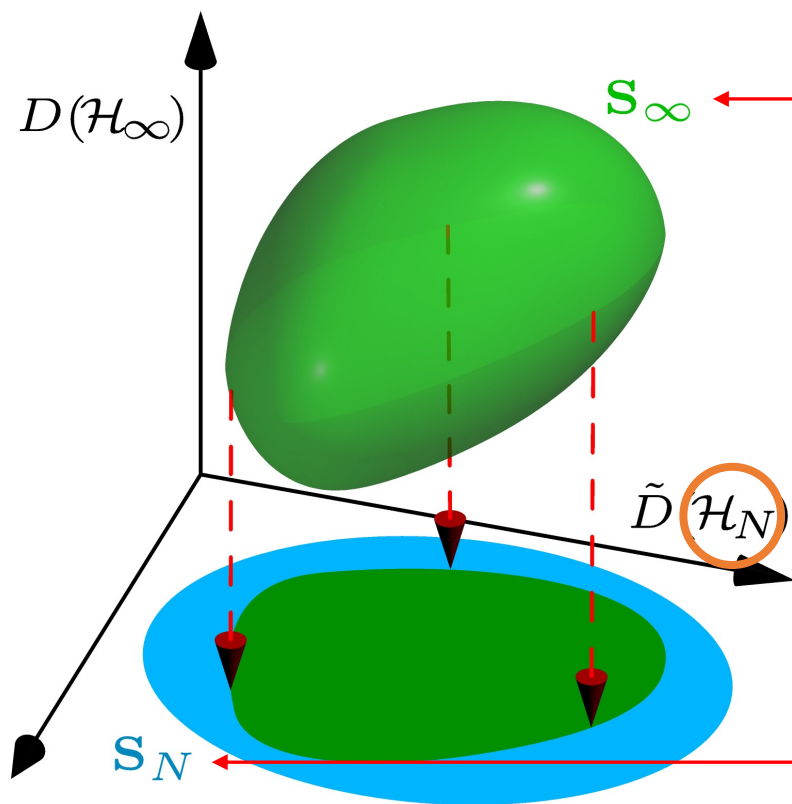
How can we lower bound infinite-dimensional minimizations, given a numerical framework for lower bounding finite-dimensional ones?

- Finite-dimensional numerics framework
(See Submission #227)
- Infinite-dimensional protocol



Dimension Reduction Method

Inf.-dim minimization is lower-bounded by a fin.-dim one, minus a small correction term



Main Dimension Reduction Theorem

$$\inf_{\rho \in S_\infty} f(\rho) \geq \inf_{\tilde{\rho} \in S_N} f(\tilde{\rho}) - \Delta W$$

Four quantities are needed to apply the dimension reduction theorem

1. Finite subspace to work in: \mathcal{H}_N, Π
 2. Bound on weight outside this subspace: W
 3. Correction term: Δ
 4. Finite-dimensional feasible set: \mathbf{S}_N
-
- Protocol-specific
- Protocol-agnostic

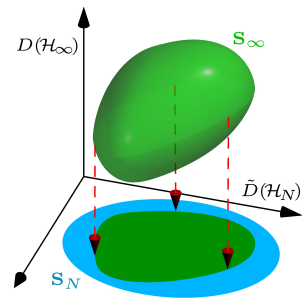
Choosing the finite subspace and bounding the weight are protocol-specific steps

- Commutation relations important
- Bound on weight:

$$W \geq \sup_{\rho \in \mathbf{S}_\infty} \text{Tr}(\rho \bar{\Pi})$$

- Useful relation:

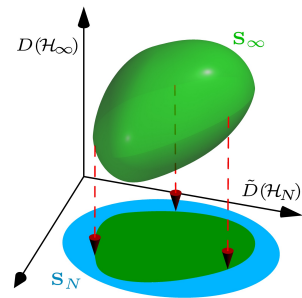
$$\begin{aligned} F(\rho, \Pi \rho \Pi) &= \text{Tr}(\rho \Pi) \\ &\geq 1 - W \end{aligned}$$



$$\Pi + \bar{\Pi} = \mathbb{1}$$

Deriving a general form of the correction term

- Limits how much the objective function f can increase under the projection Π



- For every state $\rho \in \mathbf{S}_\infty$

$$F(\rho, \Pi\rho\Pi) \geq 1 - W \implies f(\Pi\rho\Pi) \leq f(\rho) + \Delta(W)$$

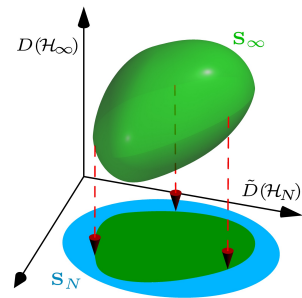
- **Uniformly Close to Decreasing Under Projection**

$$\Delta(W) = \sqrt{2W - W^2} \log_2 |Z| + \left(1 + \sqrt{2W - W^2}\right) h \left(\frac{\sqrt{2W - W^2}}{1 + \sqrt{2W - W^2}} \right)$$

Specifying the feasible set for the finite-dimensional optimization

- Must satisfy

$$\mathbf{S}_N \supseteq \Pi \mathbf{S}_\infty \Pi$$



- Different approaches, depending on properties of observables

$\mathbf{S}_\infty = \{ \rho \in \text{Pos}(\mathcal{H}_\infty) : \text{Tr}(\rho) = 1$		$\mathbf{S}_N = \{ \tilde{\rho} \in \text{Pos}(\mathcal{H}_N) : 1 - W \leq \text{Tr}(\tilde{\rho}) \leq 1$
$\text{Tr}_B(\rho) = \tau_A$		$\ \text{Tr}_B(\tilde{\rho}) - \tau_A \ _1 \leq 2\sqrt{W}$
$\text{Tr}(\rho \Gamma_i) = \gamma_i \}$		$\gamma_i - W \ \Gamma_i\ _\infty \leq \text{Tr}(\tilde{\rho} \Gamma_i) \leq \gamma_i \}$

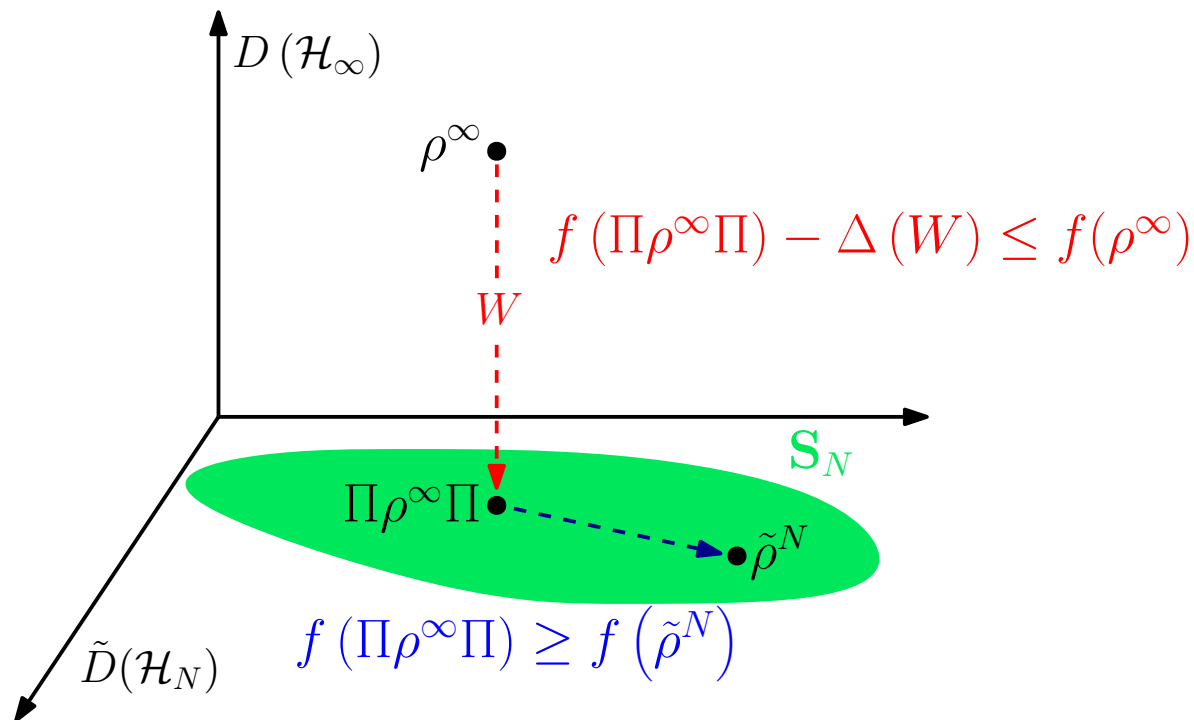
Revisiting and proving theorem statement

$$\underbrace{\inf_{\rho \in \mathbf{S}_\infty} f(\rho)}_{f(\rho^\infty)} \geq \underbrace{\inf_{\tilde{\rho} \in \mathbf{S}_N} f(\tilde{\rho})}_{f(\tilde{\rho}^N)} - \Delta(W)$$

Recall

UCDUP: Δ

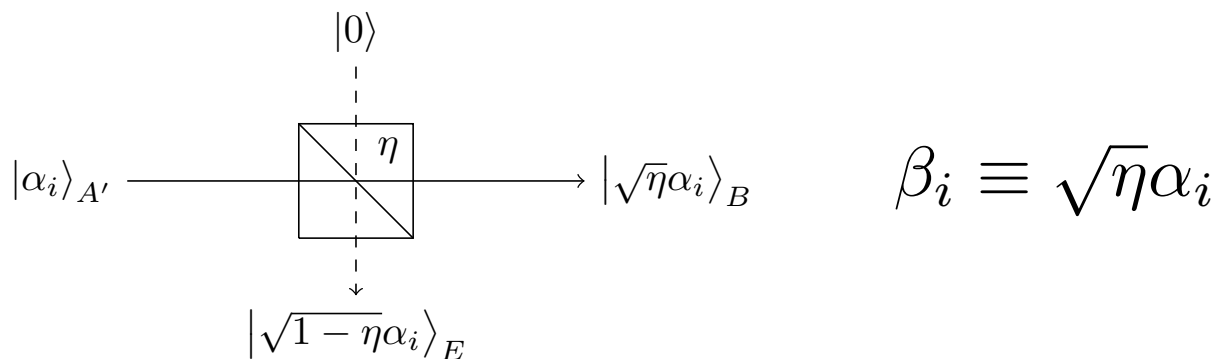
$$\mathbf{S}_N \supseteq \Pi \mathbf{S}_\infty \Pi$$



Discrete-Modulated Continuous-Variable QKD

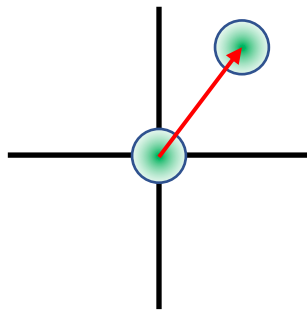
Loss-only scenario provides useful intuition for application of dimension reduction method

- In loss-only scenario, key rate is analytically determined



$$\langle \hat{n} \rangle = 0$$

$$\iff |0\rangle$$



$$\langle \hat{n}_{\beta_i} \rangle = 0$$

$$\iff |\beta_i\rangle$$

Recall: four quantities are needed to apply the dimension reduction theorem

1. Finite subspace to work in: \mathcal{H}_N, Π

2. Bound on weight outside this subspace: W

3. Correction term: Δ

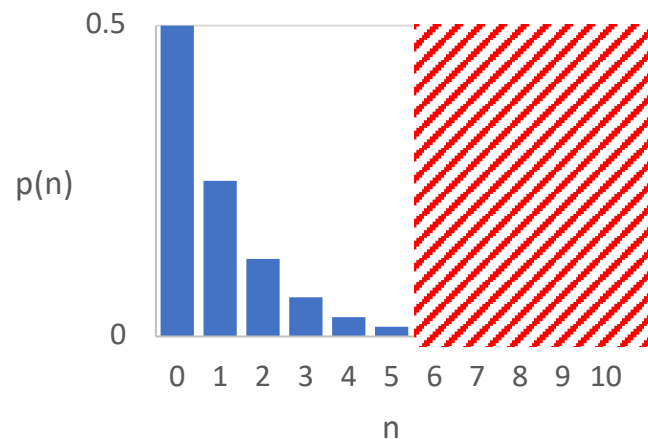
4. Finite-dimensional feasible set: \mathbf{S}_N

} Protocol-specific

} Protocol-agnostic

The finite subspace is built from displaced Fock bases

- Expect displaced thermal states
- Choose conditional projection accordingly



$$\Pi^N \equiv \sum_i |i\rangle\langle i|_A \otimes \Pi_{B_{\beta_i}}^N$$

$$\Pi_{B_{\beta_i}}^N = \sum_{n=0}^N |n_{\beta_i}\rangle\langle n_{\beta_i}|$$

The weight is calculated using SDP duality

- Split into conditional weights: $W = \sum_i p(i) W_i$

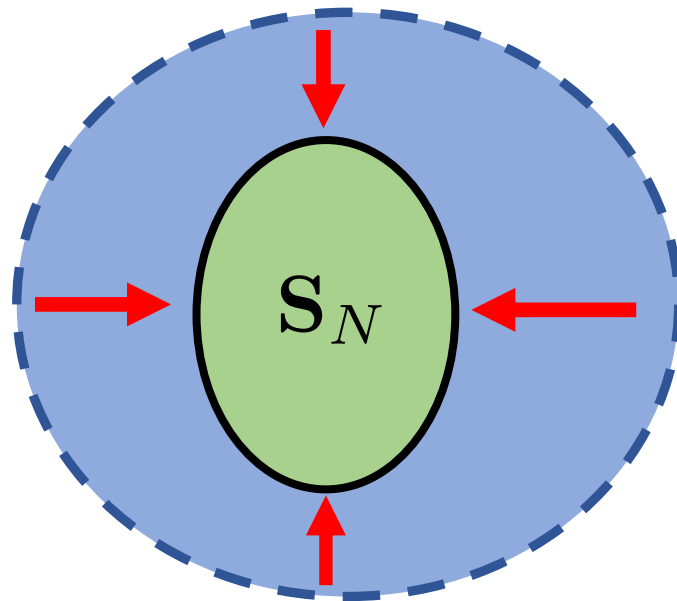
$$\frac{\langle \hat{n}_{\beta_i}^2 \rangle - \langle \hat{n}_{\beta_i} \rangle}{N(N+1)} = W_i \geq \begin{array}{ll} \underset{\rho}{\text{maximize:}} & \text{Tr}(\bar{\Pi}_{B_{\beta_i}}^N \rho) \\ \text{subject to:} & \text{Tr}(\rho) = 1 \\ & \text{Tr}(\hat{n}_{\beta_i} \rho) = \langle \hat{n}_{\beta_i} \rangle \\ & \text{Tr}(\hat{n}_{\beta_i}^2 \rho) = \langle \hat{n}_{\beta_i}^2 \rangle \\ & \rho \in \text{Pos}(\mathcal{H}_B) \end{array}$$

- All operators are diagonal in respective displaced Fock basis

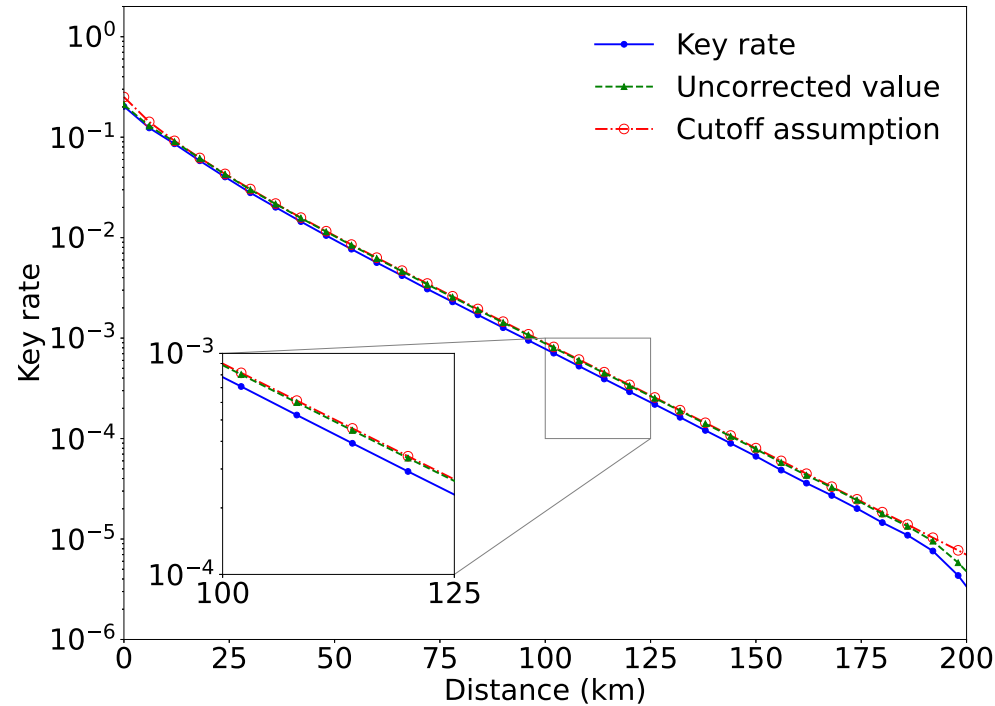
Remaining steps of dimension reduction method are protocol-agnostic

- Simply use the general correction term $\Delta(W)$
- Plug in specific observables to the generic form of finite set

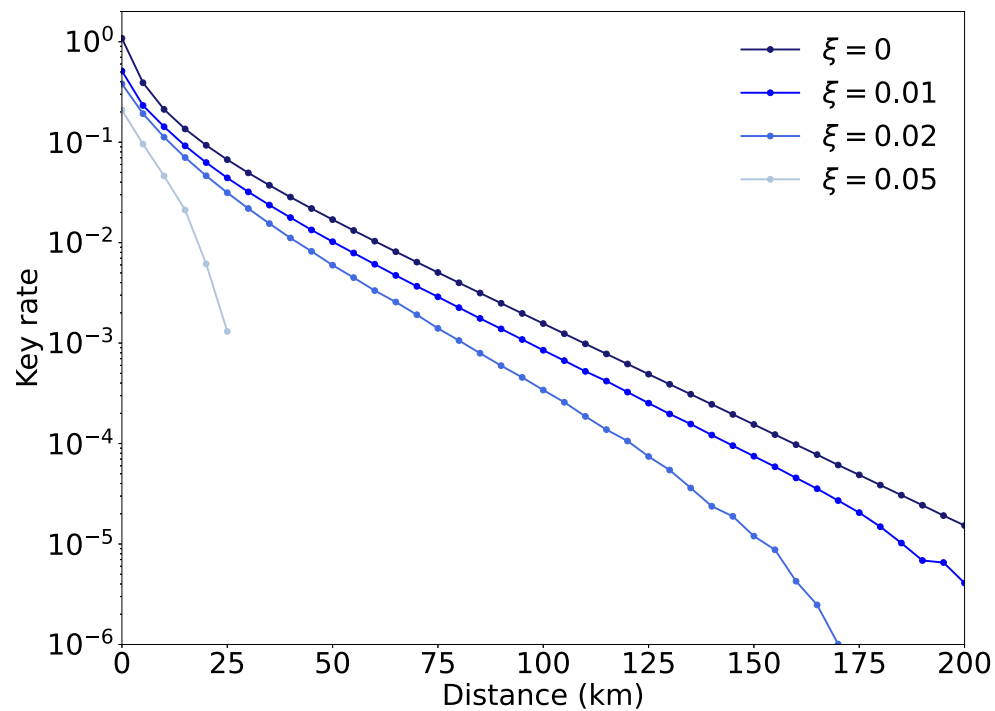
$$\Pi^N \longleftrightarrow \Gamma_i$$



Dimension reduction removes unrealistic cutoff assumption with hardly any impact on key rate

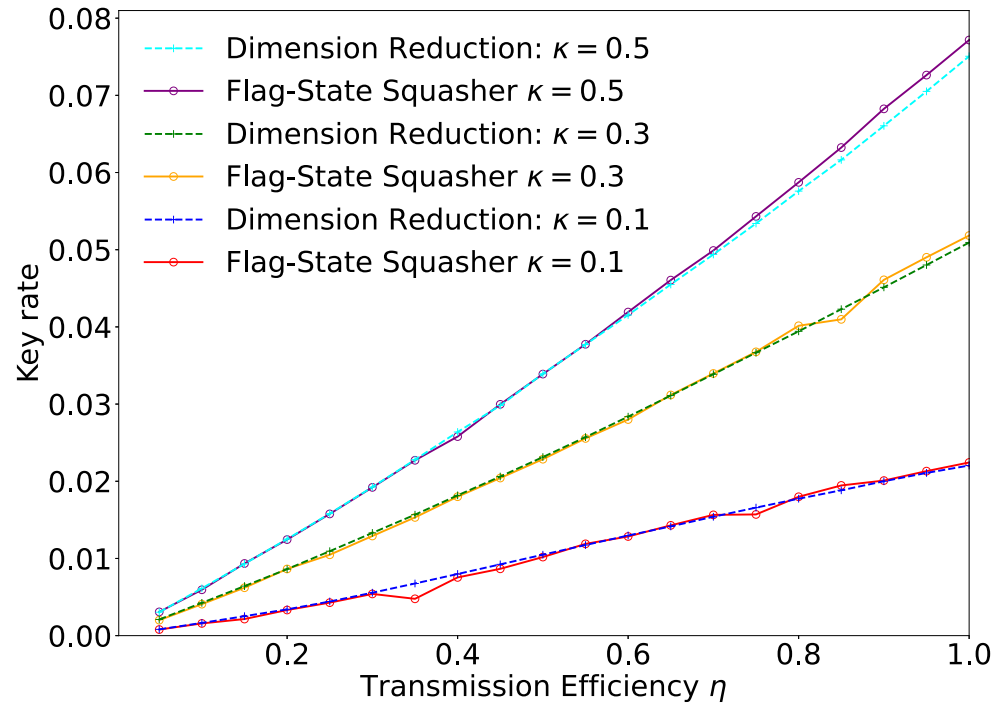


Representative key rates for DMCVQKD



Application to Unbalanced BB84

Dimension reduction gives near-identical results to flag-state squasher but with an improved runtime



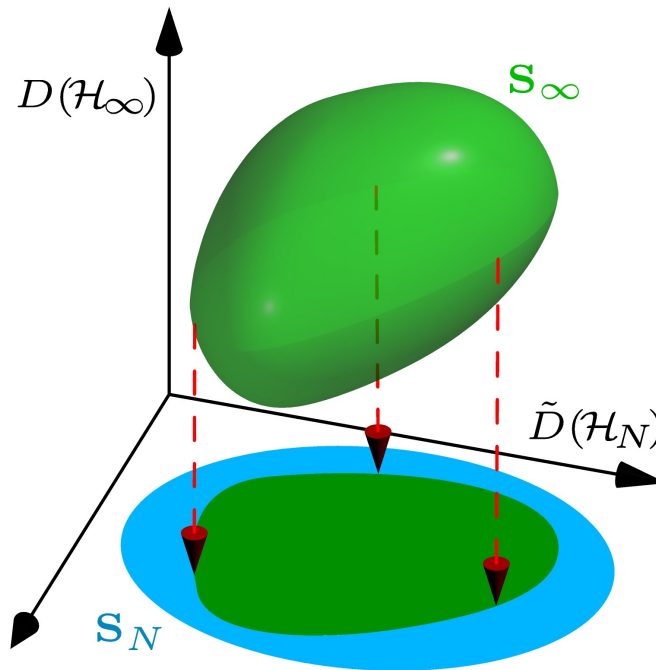
Conclusion

Summary

- Dimension reduction method
- DMCVQKD security proof
- Alternative for DV protocols

Future Work

- Apply to other protocols
- Finite-key analysis
- DMCVQKD protocol optimization



Thank you! Any questions?

<https://doi.org/10.1103/PRXQuantum.2.020325>