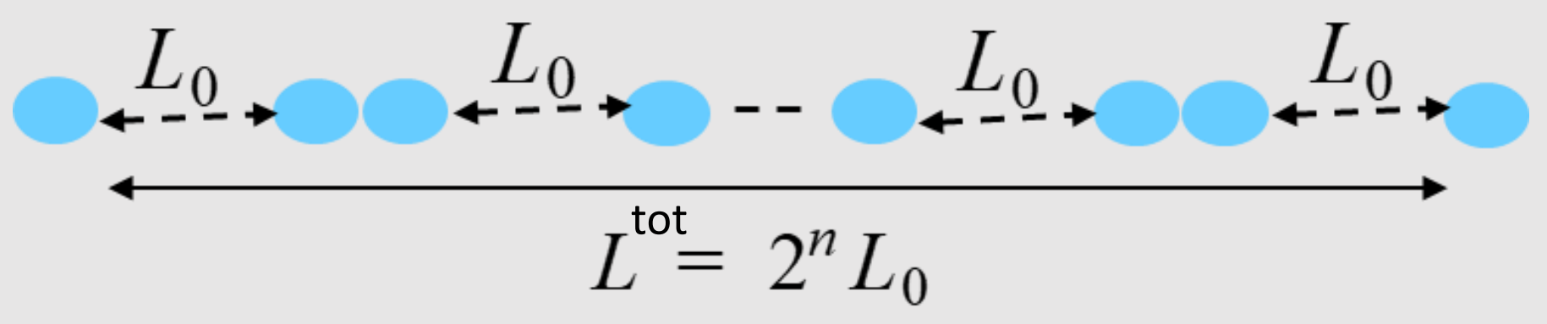
# Quantum Key Distribution over Quantum Repeaters with Encoding

Yumang Jing and Mohsen Razavi

School of Electronic and Electrical Engineering,
University of Leeds, LS2 9JT, Leeds, United Kingdom

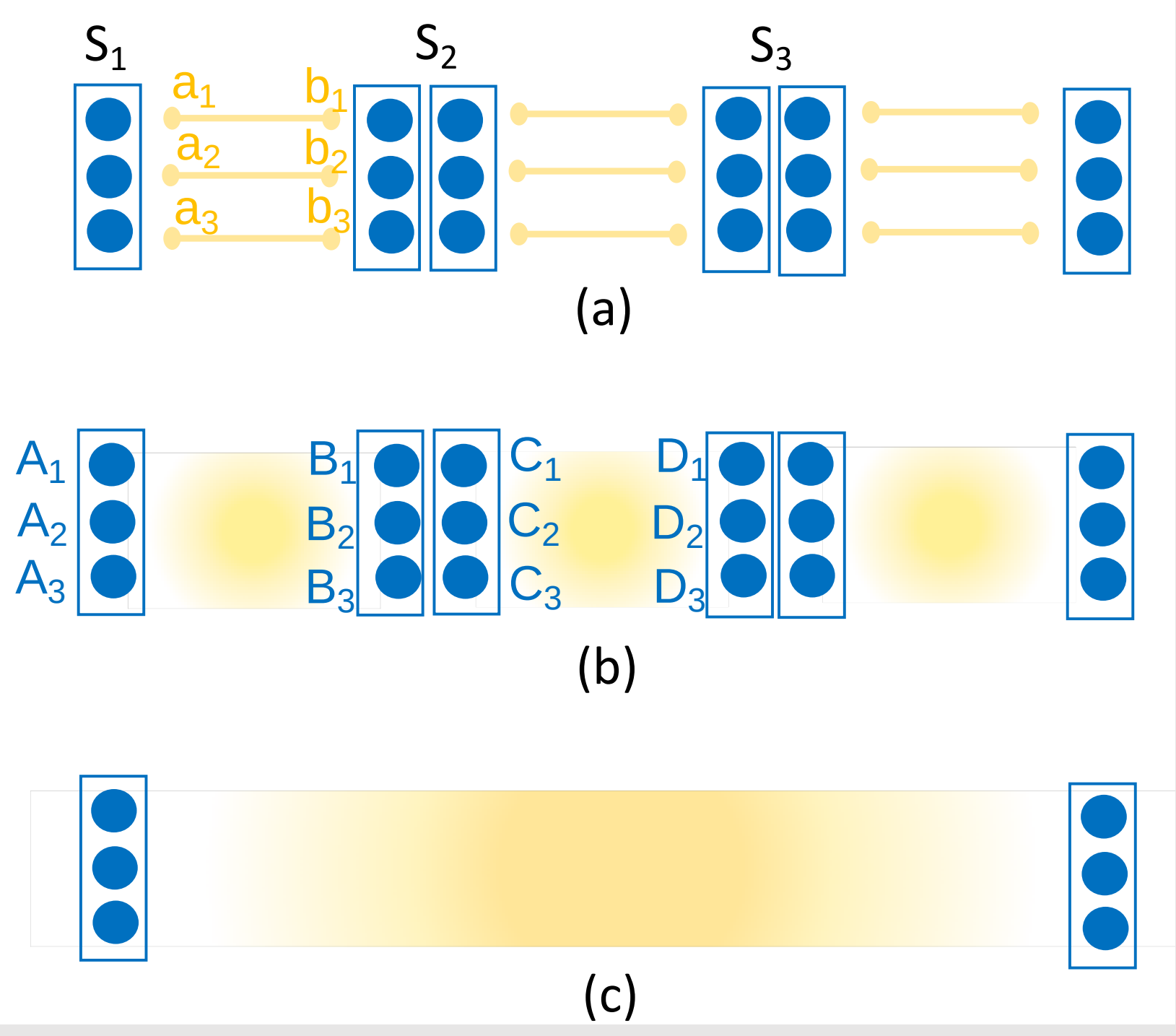
UNIVERSITY OF LEEDS

## Motivations and Objectives



- **Quantum repeaters (QRs):** An enabling technology for future quantum networks that allows efficient distribution of entanglement over long distances.
- **Main idea:** first distribute and store entanglement between short segments and then to use entanglement swapping (ES) and entanglement distillation at intermediate stations to **establish entanglement at long distances**.
- **This work:** Focuses on a scheme where entanglement distillation is achieved by using deterministic **quantum error correction codes (QECCs)** [1]; Studies the performance of a QKD system that is run over a QR with three and five-qubit repetition codes by **accounting for various sources of errors** in the setup; Specifies **the requirements** of such systems in practice for **near-term** implementation.
- **Challenge:** Simulating **erroneous quantum circuits** on a classical computer and obtaining the **analytical form of the final entangled states** after several nesting levels. The complexity of the analysis grows exponentially with the number of qubits involved. How to **minimize the required approximations** while still getting a rather accurate result within reasonable simulation times.
- **Method**: Employing a **novel hybrid numerical-analytical approach** that relies on the *linearity* of the employed quantum circuits, and the *transversality* of the code employed.
- **Results:** New post-selection techniques based on error detection; New efficient QKD decoders; New repeater architectures for NV-centre platforms

## Quantum Repeater with Encoding



**Objective:** Distribute an encoded Bell state

**Bell state:** $|00\rangle + |11\rangle \xrightarrow{\text{Encoding}}$

$$|000\rangle|000\rangle + |111\rangle|111\rangle$$

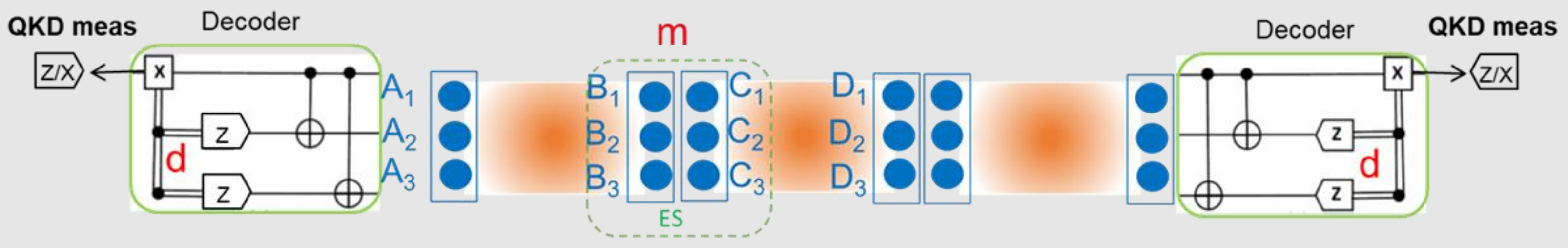
Encoded Bell state with 3-qubit repetition code

**Benefit:** We can potentially correct for error at each entanglement swapping stage

**Challenge:** error propagation due to imperfect gates (error prob $\beta$); imperfect initial states (w/ fidelity $\mathbf{F_0}$); and measurement errors (w/p $\delta$)

## Error Detection As an Effective Post-Selection Tool

- BBM92 protocol

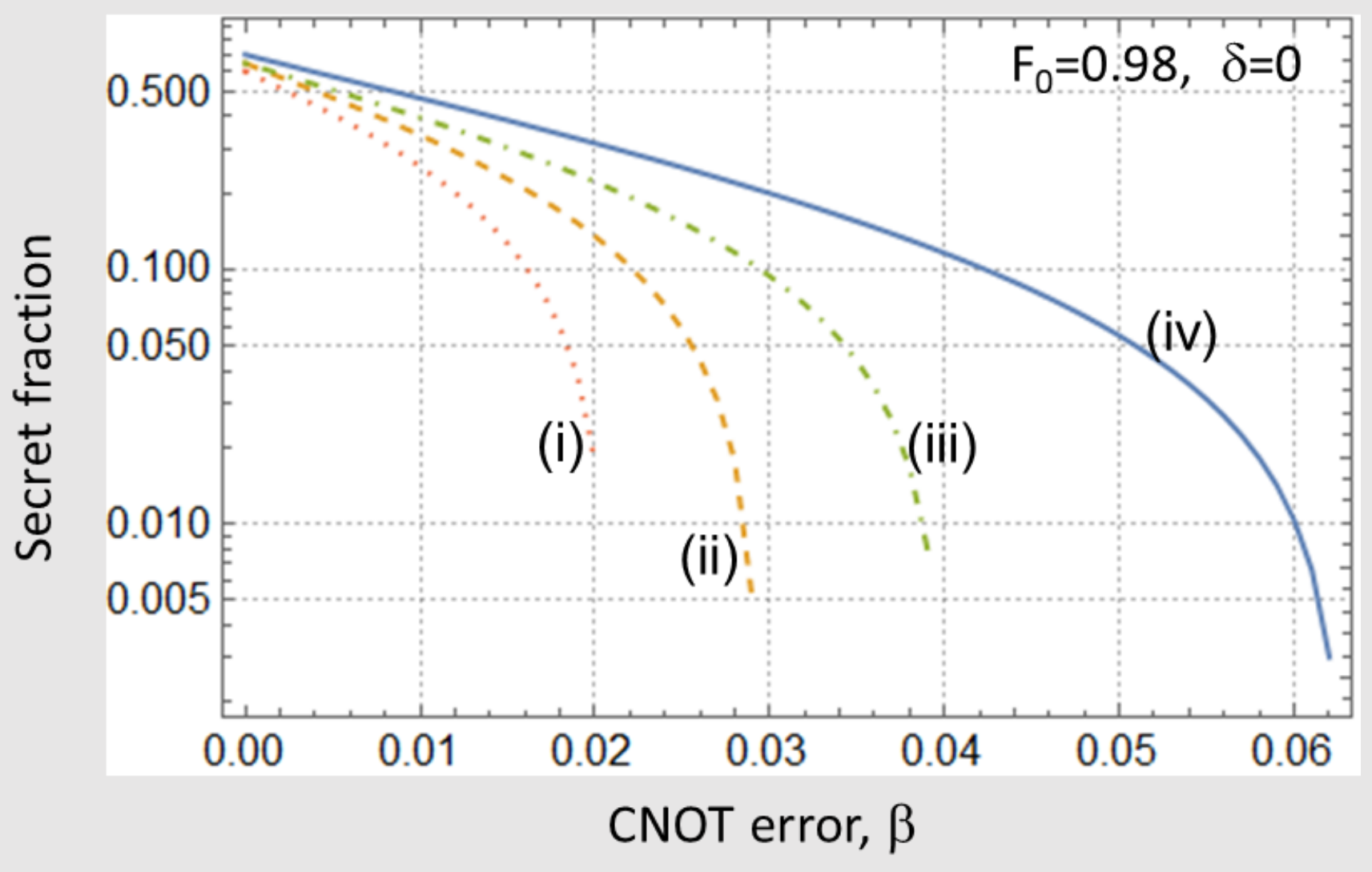


- Benchmarking question: Considering typical sources of error in the system, what can realistically be achieved and under what conditions?
- Sources of error:
  - Error in CNOT gates with prob $\beta$
  - Error in single-qubit measurements, with prob $\delta$
  - Error in the initial entangled states, with fidelity $F_0$
- Figure of merit: Secret fraction (secret key rate/distributed state )

$$R \geq 1 - h(e_{phase}) - h(e_{bit})$$

- Different QKD protocols possible:
  - (i) You let the service provider to do all necessary corrections and just give you the final decoded states; the users do not know m and d
  - (ii) The users know m, but not d
  - (iii) The users know d, but not m
  - (iv) The users know both d and m → our case of interest

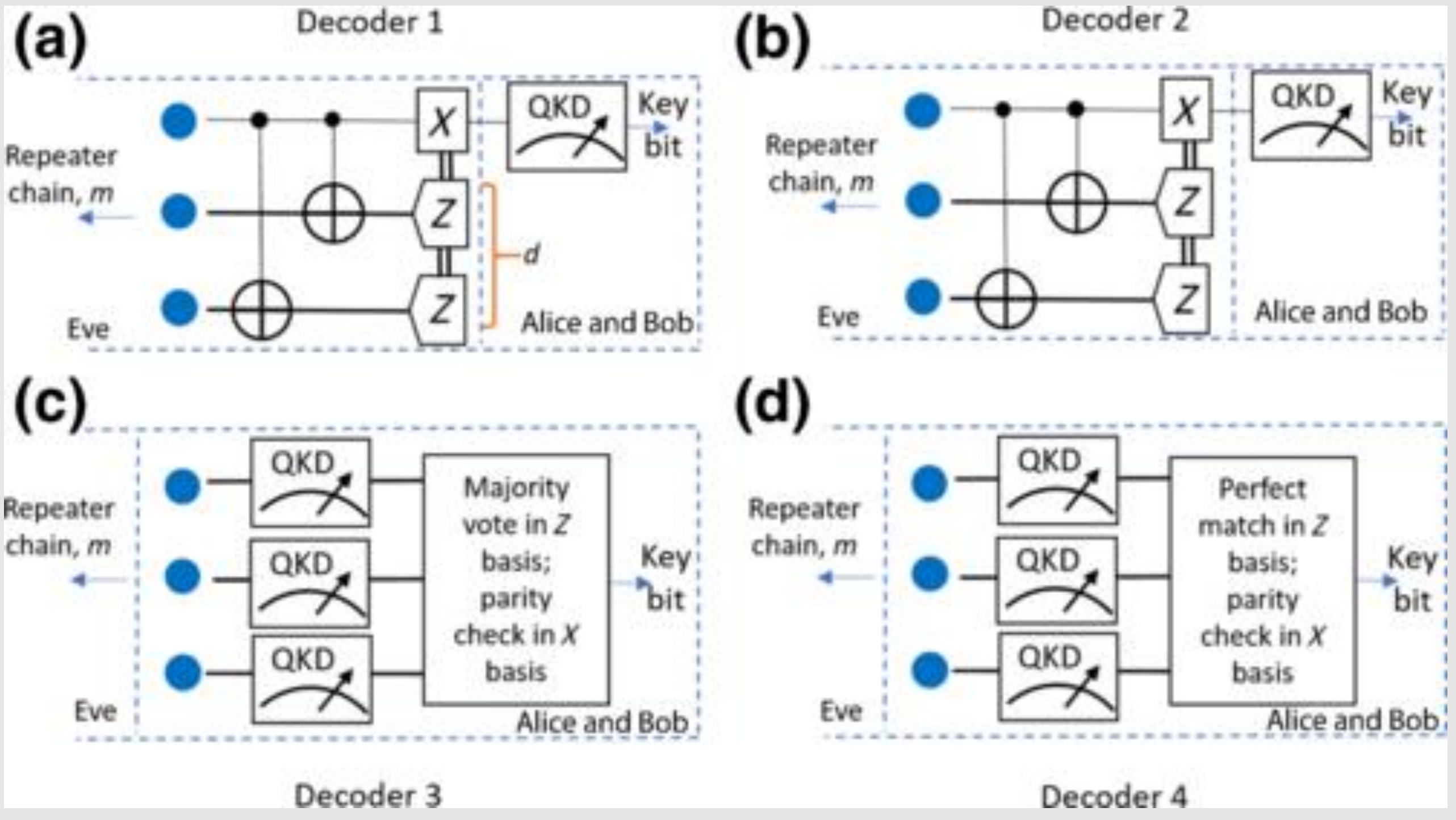
[Phys. Rev. Applied **14**, 064037 (2021)]



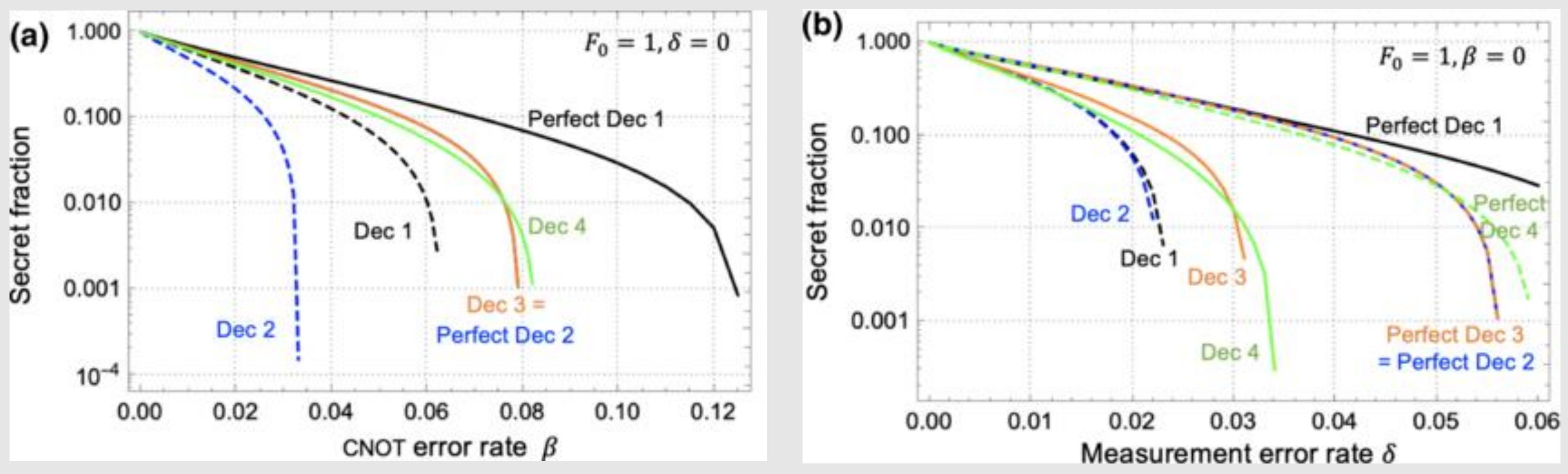
- In protocol (iv), for each pair of m and d, we effectively post-process the corresponding data together
- Question: what values of m and d result in higher key rates?
- We identify three important categories of states
  - **Good states:** when we detect no error at ES stage
  - **Bad states:** when we detect at least one error at ES stage
  - **Golden states:** When we detect no error neither at ES nor at decoding stage

- Key finding: In most practical cases, the secret key rate is dominated by that of the golden states → We can use ***error detection***, rather than error correction, as a postselection tool

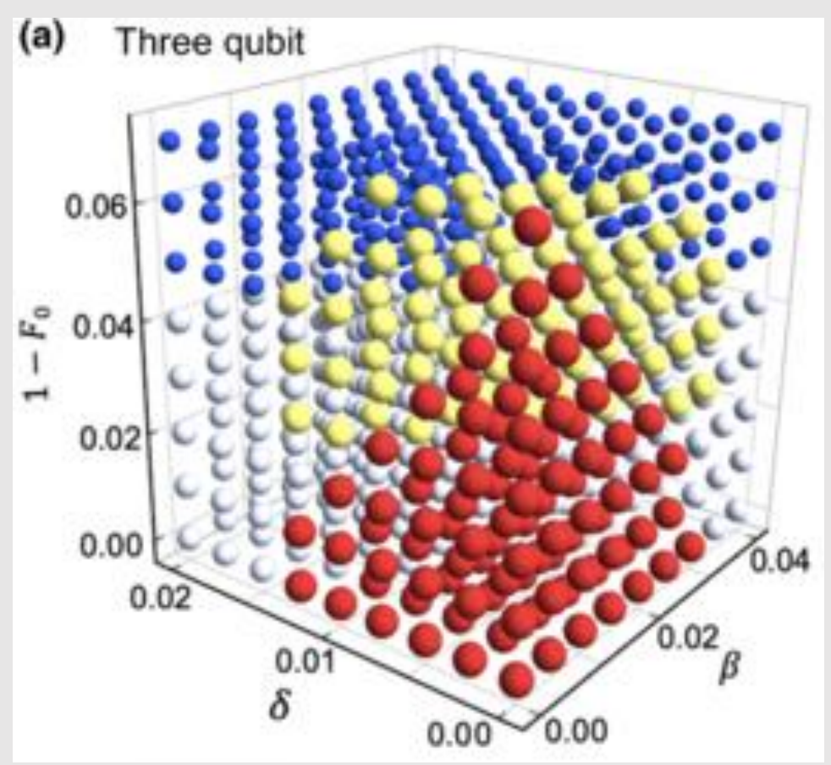
## Simple Efficient QKD Decoders



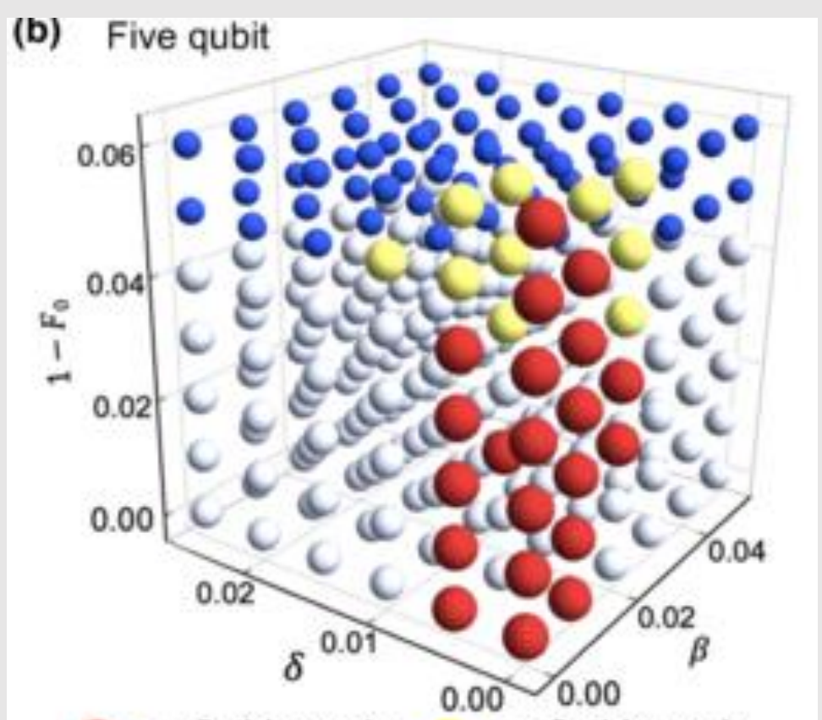
[Phys. Rev. Applied **15**, 044027 (2021)]



### 3- versus 5-qubit repetition codes at L = 1000 km

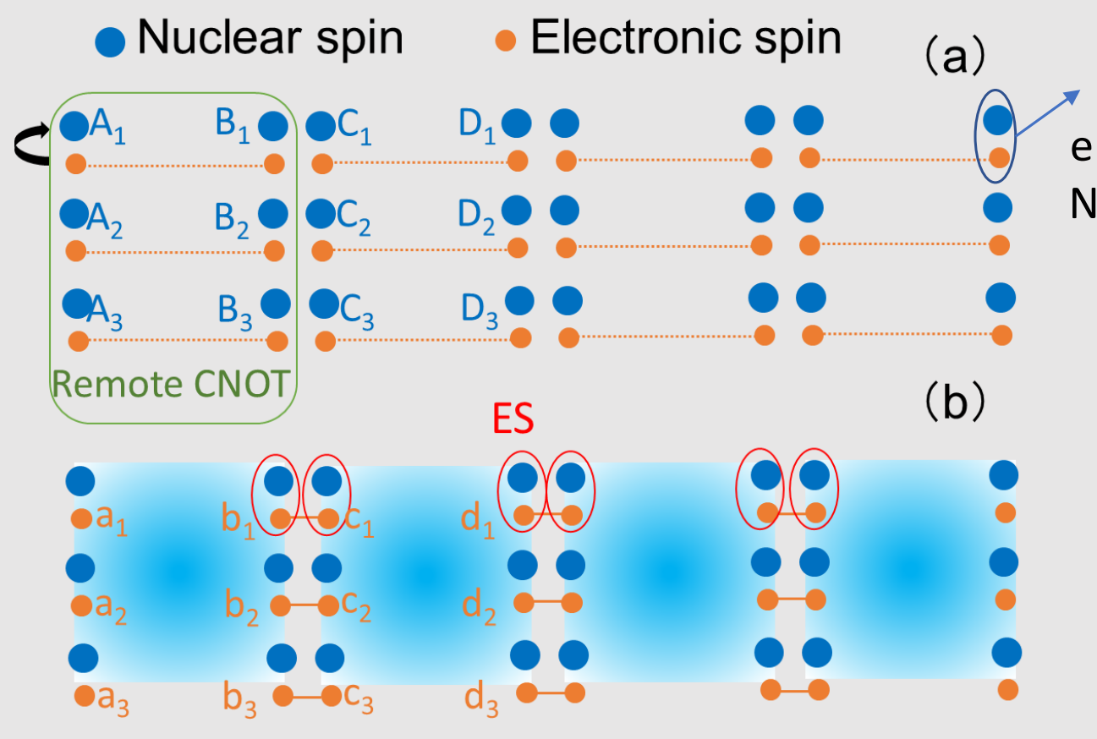


- 3-qubit codes allow for a wider range of parameters before losing to probabilistic quantum repeaters
- Symbols on graph show the protocol with maximum key rate

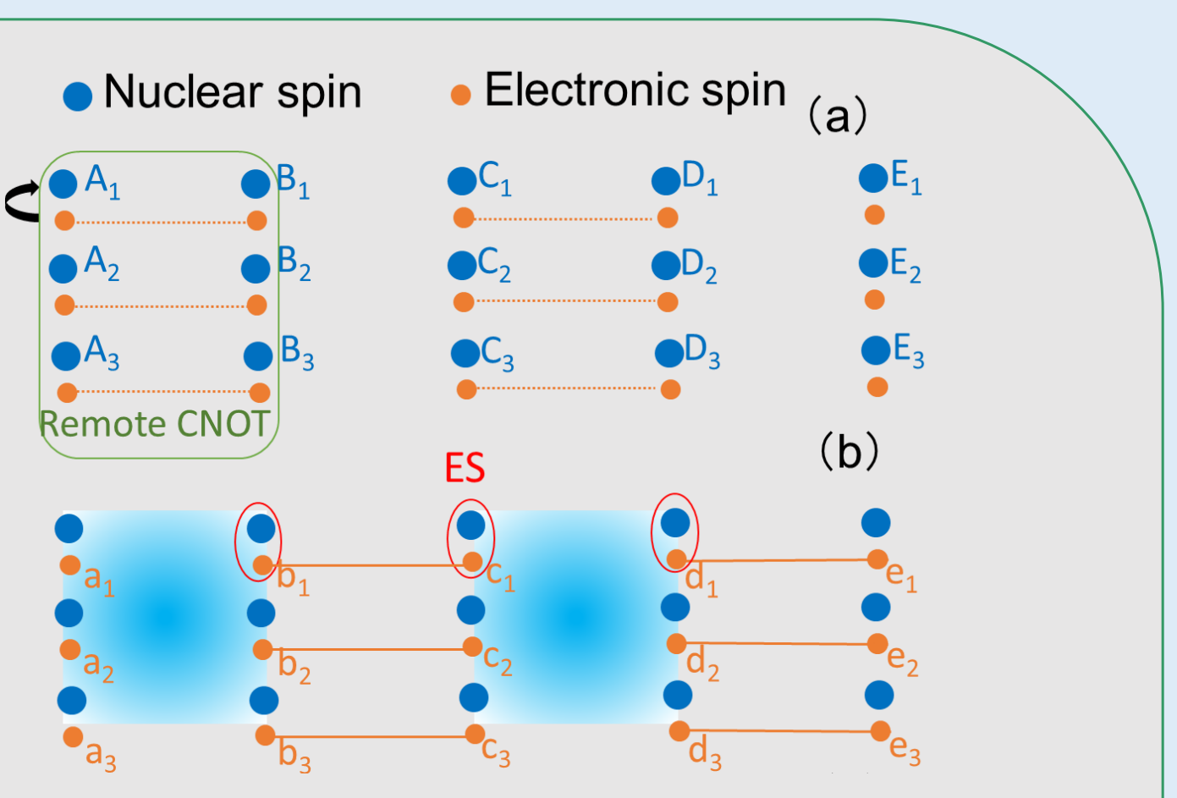


- **Take-home message:** For moderately long distances, we may not need complicated codes to get some advantage

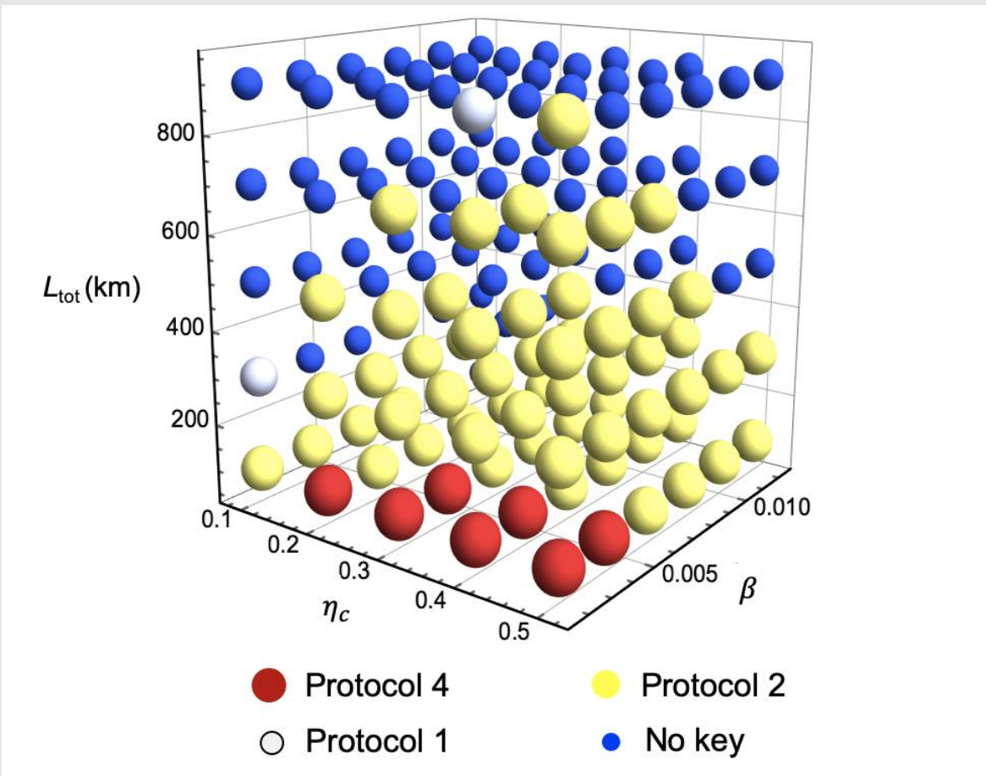
## QR with Encoding on NV Centre Platforms



**Protocol 1:** Use local entanglement between electron spins of two co-located NV centres to do ES



**Protocol 2:** Generate entanglement between electron spins of two remote NV centres to do ES



Meas. Error = 1 E -4
Electron spin coherence time = 10 ms
Nuclear spin coherence time = 10 s
$\eta_c$: Spin-photon coupling efficiency;
Protocol 4: deterministic QR with no distillation

***Near-term applications in sight!***

**More info at arXiv: 2105.14122**

* This project is funded by the European Innovative Training Network **Quantum Communications for ALL (QCALL),** project 675662, under the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015 and UK EPSRC Grant EP/M013472/1. Please visit www.qcall-itn.eu for more information.