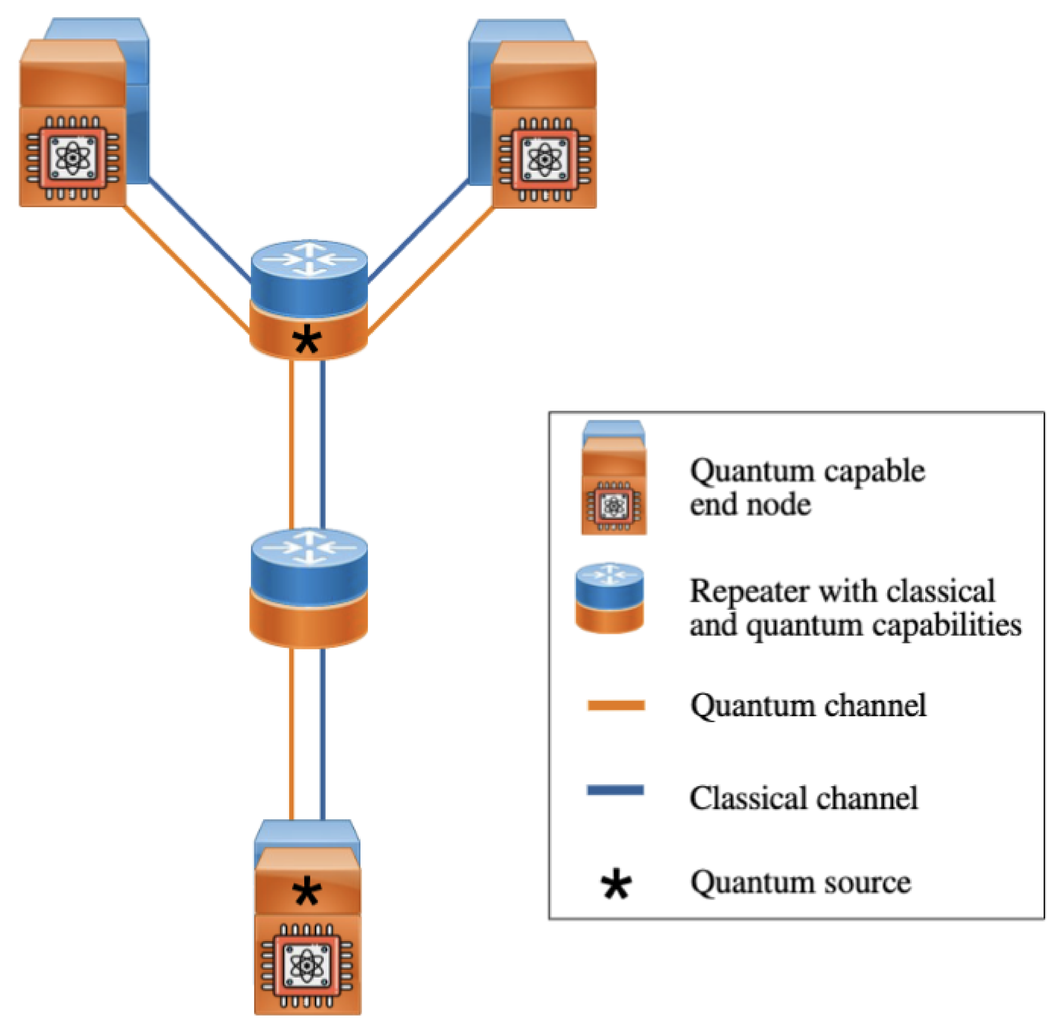
The 4th Workshop on Quantum Repeaters and Networks
11-13 September 2024, Montreux, Switzerland

An Algebraic Language for Specifying Quantum Networks

Anita Buckley[1] Pavel Chuprikov[1] Rodrigo Otoni[1] Robert Soulé[2] Robert Rand[3] Patrick Eugster[1]
anita.buckley@usi.ch pavel.chuprikov@usi.ch otonir@usi.ch robert.soule@yale.edu rand@uchicago.edu eugstp@usi.ch
USI Lugano, Switzerland[1], Yale University, USA[2], University of Chicago, USA[3]

End-to-end Bell pair distribution

We model quantum network protocols as envisioned by Quantum Internet Research Group [1]



What can go wrong?

How to make sure (in a formal way) that quantum network protocols behave as intended?

- Does a protocol establish Bell pairs between the specified end nodes?
- When are two protocols equivalent?
- Can a protocol execute with a given number of resources?
- Can protocols run in parallel without interfering with each other?

Our approach

Provide a formalism to aid in answering these types of questions about quantum networks

- BellKAT – language to specify quantum networks based on a novel algebraic structure
- Soundness and completeness of BellKAT's axioms w.r.t. their corresponding semantics
- Decidability result for checking semantic equivalence of quantum network protocols
- Prototype tool for automated reasoning about protocols

Primitive actions

A Bell pair between two quantum network nodes A and B is denoted as $A{\sim}B$.
Basic action $r \triangleright o$ requires a multiset of Bell pairs r and produces from it Bell pairs in multiset o.

swap	$\mathsf{sw}\langle A{\sim}B \,@\, C\rangle$	$\triangleq \{\!\{A{\sim}C, B{\sim}C\}\!\} \triangleright \{\!\{A{\sim}B\}\!\}$
transmit	$\mathsf{tr}\langle A \to B{\sim}C\rangle$	$\triangleq \{\!\{A{\sim}A\}\!\} \triangleright \{\!\{B{\sim}C\}\!\}$
create	$\mathsf{cr}\langle A\rangle$	$\triangleq \emptyset \triangleright \{\!\{A{\sim}A\}\!\}$
wait	$\mathsf{wait}\langle r\rangle$	$\triangleq r \triangleright r$
fail	$\mathsf{fail}\langle r\rangle$	$\triangleq r \triangleright \emptyset$
distill	$\mathsf{distill}\langle A{\sim}B\rangle$	$\triangleq \{\!\{A{\sim}B, A{\sim}B\}\!\} \triangleright \{\!\{A{\sim}B\}\!\} + \{\!\{A{\sim}B, A{\sim}B\}\!\} \triangleright \emptyset$

Acknowledgments

This work is supported by Hasler Foundation grant 23086, Swiss National Science Foundation (SNF) grant 197353, US Air Force Office of Scientific Research (AFOSR) award FA95502110051, and US National Science Foundation (NSF) Expedition in Computing (EPiQC) grant CCF-1730449.

References

[1] W. Kozlowski, S. Wehner, R. V. Meter, B. Rijsman, A. S. Cacciapuoti, M. Caleffi, and S. Nagayama, "Architectural Principles for a Quantum Internet," RFC 9340, QIRG-IRTF, 2023.

[2] M. Pompili, S. L. N. Hermans, S. Baier *et al.*, "Realization of a Multinode Quantum Network of Remote Solid-State Qubits," *Science*, vol. 372, no. 6539, pp. 259–264, 2021.

[3] A. Buckley, P. Chuprikov, R. Otoni, R. Soulé, R. Rand, and P. Eugster, "An Algebraic Language for Specifying Quantum Networks," in *PLDI'24*, 2024, pp. 1–23.

[4] A. Buckley, P. Chuprikov, R. Otoni, R. Rand, R. Soulé, and P. Eugster, "Towards an Algebraic Specification of Quantum Networks," in *QuNet'23*, 2023, p. 7–12.

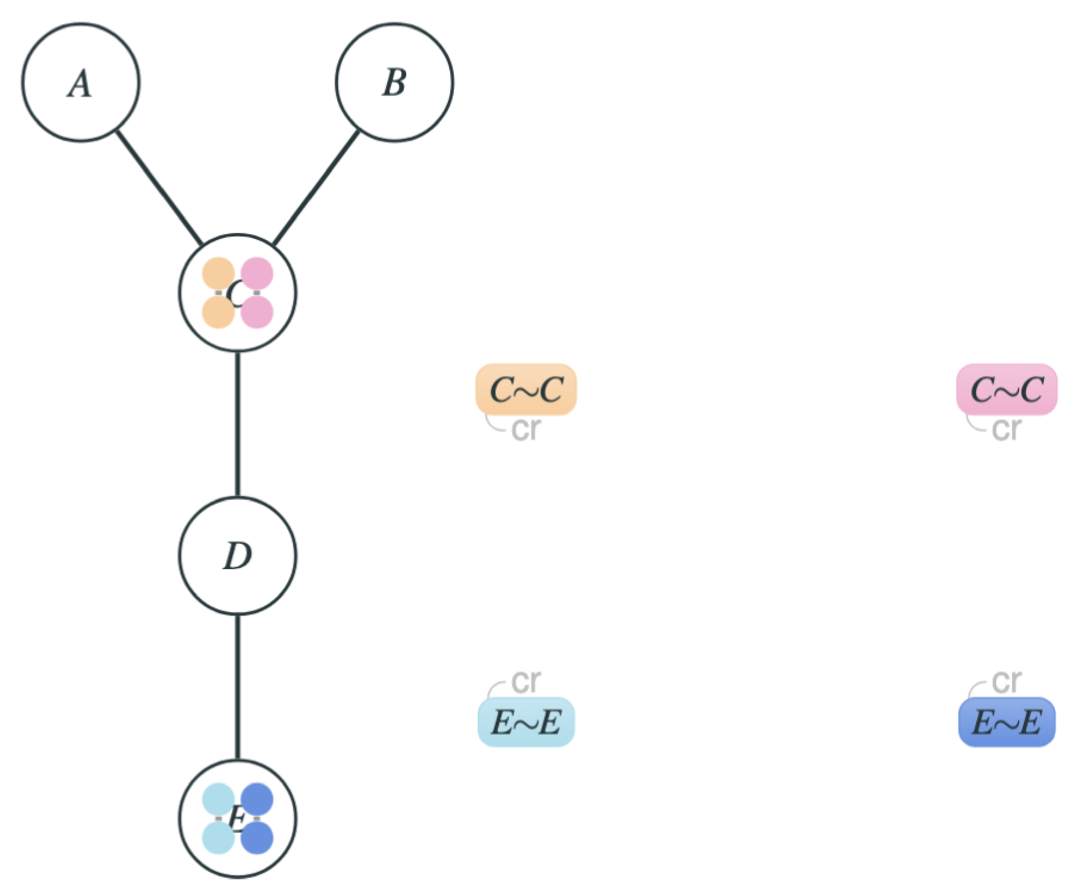
Reasoning about protocols – toy example

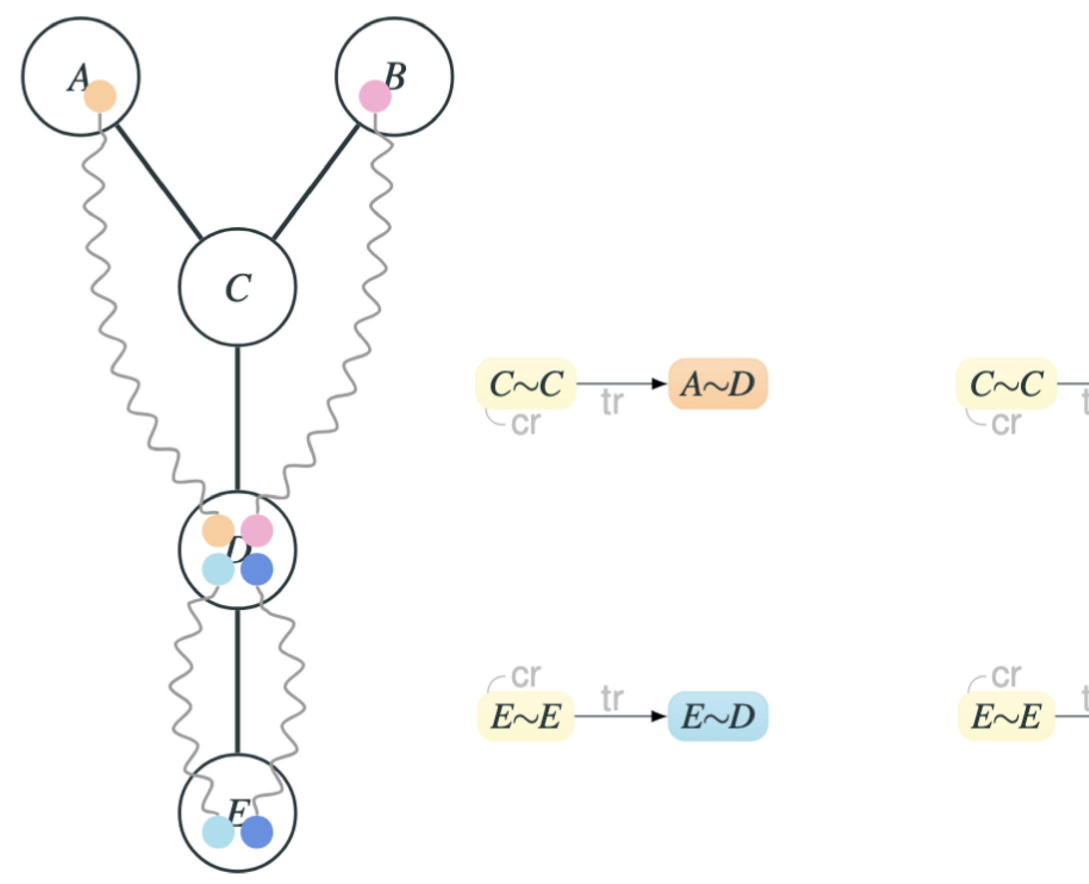
Protocol that in parallel generates Bell pairs $A{\sim}E$ and $B{\sim}E$

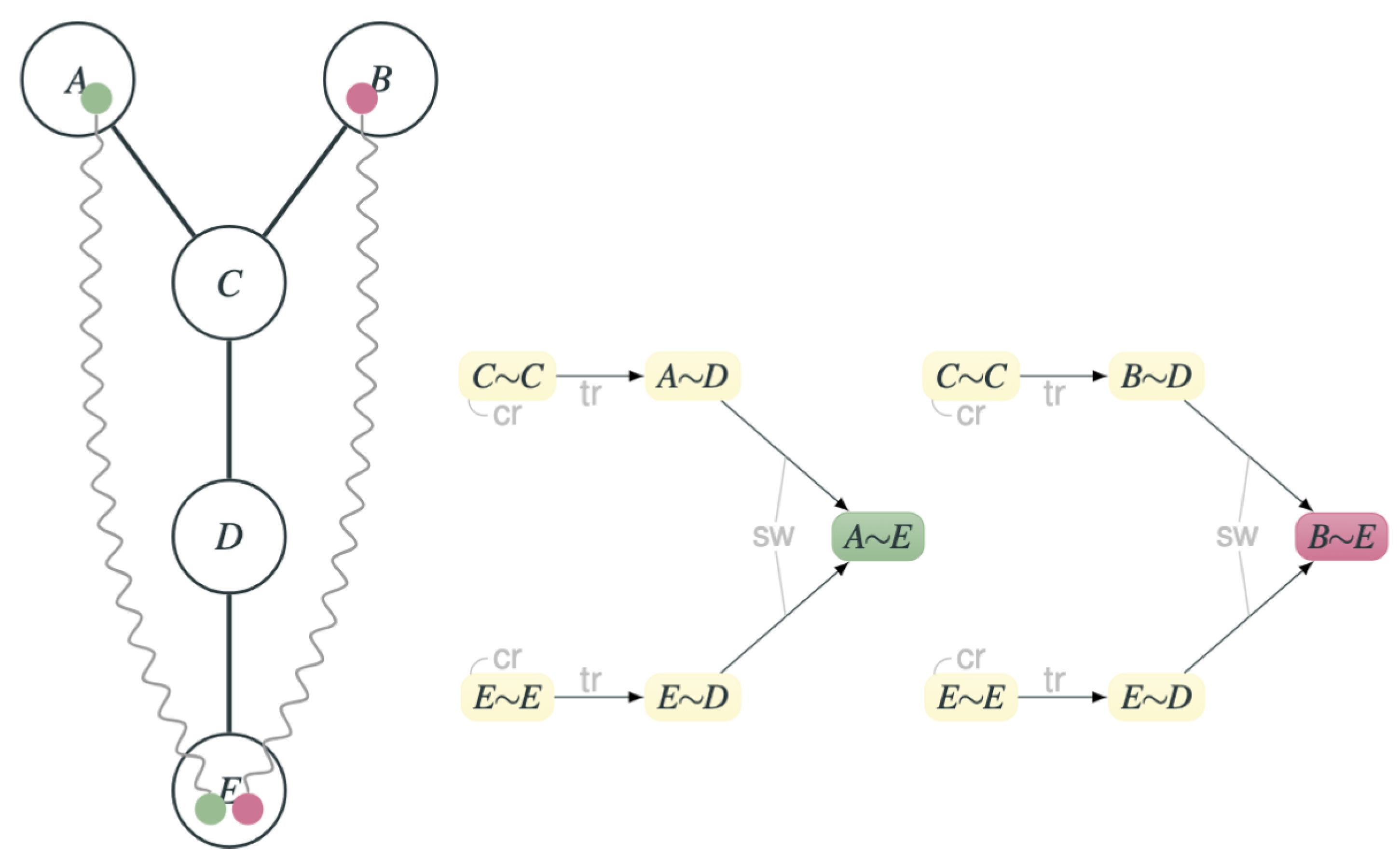
$$(\mathsf{cr}\langle C\rangle \cdot \mathsf{cr}\langle C\rangle \parallel \mathsf{cr}\langle E\rangle \cdot \mathsf{cr}\langle E\rangle);$$
$$(\mathsf{tr}\langle C \to A{\sim}D\rangle \parallel \mathsf{tr}\langle C \to B{\sim}D\rangle \parallel \mathsf{tr}\langle E \to E{\sim}D\rangle \parallel \mathsf{tr}\langle E \to E{\sim}D\rangle);$$
$$(\mathsf{sw}\langle A{\sim}E \,@\, D\rangle \parallel \mathsf{sw}\langle B{\sim}E \,@\, D\rangle)$$

Reachability property Does protocol p always or never generate an entangled pair $A{\sim}E$?

$$p; [1]\{\!\{A{\sim}E\}\!\} \blacktriangleright \{\!\{A{\sim}E\}\!\} \equiv_{\mathcal{N}_0} p \quad \text{or} \quad p; [\neg\{\!\{A{\sim}E\}\!\}]\emptyset \blacktriangleright \emptyset \equiv_{\mathcal{N}_0} p$$







Reasoning about protocols – real-world example

Repeater swap protocol of [2] on the repeater chain $A - C - D - E$

Protocol repeatedly generates and distills each Bell pair $A{\sim}D$ and $E{\sim}D$ in parallel until both distillations succeed, and after both Bell pairs are made available, it swaps them to generate $A{\sim}E$:

$$\Big(\big(p_d; ([b]\, p_d)^\star\big) \parallel \big(p'_d; ([b']\, p'_d)^\star\big)\Big); \mathsf{sw}\langle A{\sim}E \,@\, D\rangle$$

where p_d, p'_d generate and distill Bell pairs $A{\sim}D$, $E{\sim}D$ and b, b' test for their absence, respectively,

$$p_d = \big(\mathsf{cr}\langle C\rangle \cdot \mathsf{cr}\langle C\rangle\big); \big(\mathsf{tr}\langle C \to A{\sim}D\rangle \parallel \mathsf{tr}\langle C \to A{\sim}D\rangle\big); \mathsf{di}\langle A{\sim}D\rangle$$
$$p'_d = \big(\mathsf{cr}\langle E\rangle \cdot \mathsf{cr}\langle E\rangle\big); \big(\mathsf{tr}\langle E \to E{\sim}D\rangle \parallel \mathsf{tr}\langle E \to E{\sim}D\rangle\big); \mathsf{di}\langle E{\sim}D\rangle$$

For more details see our papers [3,4] and our verification tool `https://github.com/swystems/bellkat`. Contact: anita.buckley@usi.ch