

# An Algebraic Language for Specifying Quantum Networks

---

Anita Buckley<sup>1</sup> Pavel Chuprikov<sup>1</sup> Rodrigo Otoni<sup>1</sup> Robert Soulé<sup>2</sup> Robert Rand<sup>3</sup> Patrick Eugster<sup>1</sup>

<sup>1</sup> USI Lugano, Switzerland

<sup>2</sup> Yale University, USA

<sup>3</sup> University of Chicago, USA

## Quantum networks

**Quantum networks** are networks connecting quantum capable devices

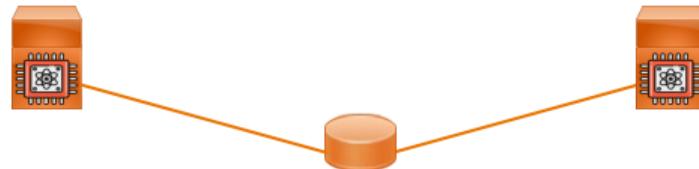
# Quantum networks

**Quantum networks** are networks connecting quantum capable devices



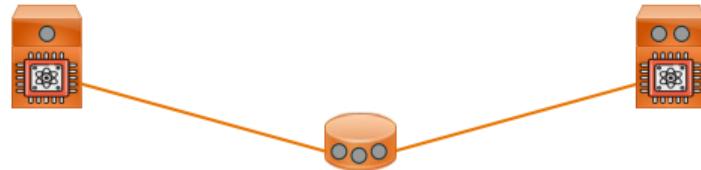
# Quantum networks

**Quantum networks** are networks connecting quantum capable devices



# Quantum networks

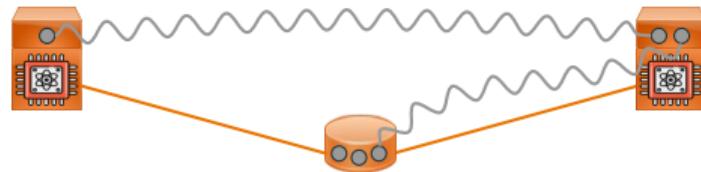
**Quantum networks** are networks connecting quantum capable devices



- **Communication qubits** designated to establish *connections* between devices

# Quantum networks

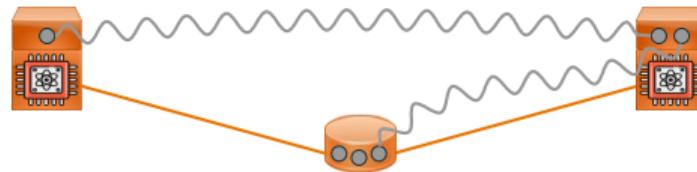
**Quantum networks** are networks connecting quantum capable devices



- **Communication qubits** designated to establish *connections* between devices
- Distributed **entanglement**: communication qubits sharing a *correlated random secret*

# Quantum networks

**Quantum networks** are networks connecting quantum capable devices



- **Communication qubits** designated to establish *connections* between devices
- Distributed entanglement: communication qubits sharing a *correlated random secret*

Benefits: **scaling of quantum computation** and **secure communication**



- teleportation
- entanglement based QKD

<sup>1</sup>[IBM Quantum: Development Roadmap 2023]

# Quantum networks are coming into reality

DOI:10.1145/3524455

A deep dive into the quantum Internet's potential to transform and disrupt.

BY LASZLO GYONGYOSI AND SANDOR IMRE

## Advances in the Quantum Internet

QUANTUM INFORMATION WILL not only reformulate our view of the nature of computation and communication but will also open up fundamentally new possibilities for realizing high-performance computer architecture and telecommunication networks. Since our data will no longer remain safe in the traditional Internet when commercial quantum computers become fully available,<sup>1,2,3,15,34</sup> there will be a need for a fundamentally different network structure: the quantum Internet.<sup>22,35,32,33,45,47</sup> While *quantum computational supremacy* refers to tasks and problems that quantum computers can solve but are beyond the capability of classical computers, the *quantum supremacy of the quantum Internet* identifies the properties and attributes that the quantum Internet offers but are unavailable in the traditional Internet.<sup>2</sup>

<sup>a</sup> While “supremacy” is a concept used to describe the theory of computational complexity<sup>44</sup> and not a specific device (like a quantum computer), the supremacy of the quantum Internet in the current context refers to the collection of those advanced networking properties and attributes that are beyond the capabilities of the traditional Internet.

The quantum Internet uses the fundamental concepts of quantum mechanics for networking (see Sidebars 1–7 in the online Supplementary Information at <https://dl.acm.org/doi/10.1145/3524455>). The main attributes of the quantum Internet are advanced quantum phenomena and protocols (such as quantum superposition and quantum entanglement, quantum teleportation, and advanced quantum coding methods), unconditional security (quantum cryptography), and an entangled network structure.

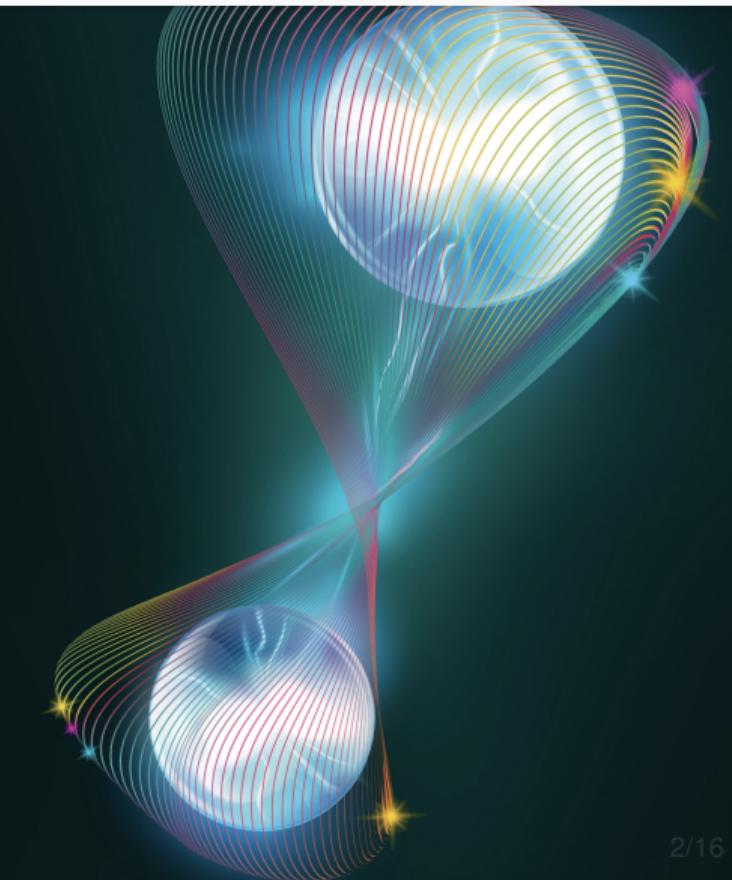
In contrast to traditional repeaters,<sup>b</sup> quantum repeaters cannot apply the receive-copy-retransmit mechanism because of the so-called no-cloning theorem, which states that it is impossible to make a perfect copy of a quantum system (see Sidebar 4). This fundamental difference between the nature of classical and quantum information does not just lead to fundamentally different networking mechanisms; it also necessitates the definition of novel networking services in a quantum Internet scenario. Quantum memories in quantum repeater units are a fundamental part of any global-scale quantum Internet. A challenge connected to quantum memory units is the noise quantum memories add to storing quantum systems. However, while quantum repeaters can be realized without requiring quantum memories, these units are, in fact, necessary to guarantee optimal performance in any high-performance quantum-networking scenario.

In 2019, the National Quantum

<sup>b</sup> Traditional repeaters rely on signal amplification.

### » key insights

- The quantum Internet is an adequate answer to the security issues that will become relevant as commercial quantum computers hit the market.
- The quantum Internet is based on the fundamentals of quantum mechanics to provide advanced, high-security network communications.
- The quantum Internet gives users many capabilities and services not available in a traditional Internet setting.



# Quantum networks are coming into reality

The screenshot shows the top navigation bar of the Nature website with links for 'Explore content', 'About the journal', and 'Publish with us'. Below this, a banner for the article 'Advances in the Quantum Internet' is displayed, featuring a dark background with colorful, glowing circular patterns resembling quantum interference or particle paths. The title 'Advances in the Quantum Internet' is prominently displayed in large, bold, white font.

## Creation of memory–memory entanglement in a metropolitan quantum network

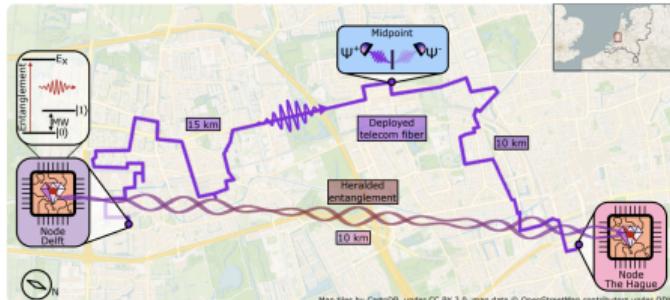
Jian-Liang Liu, Xi-Yu Luo, Yong Yu, Chao-Yang Wang, Bin Wan, Yi Hu, Jun Li, Ming-Yang Zou, Yao, Zi Yan, Da Teng, Jin-Wei Jiang, Xiao-Bing Liu, Xu-Ping Xie, Jun Zhang, Qing-He Mao, Qiang Zhang, Xiao-Hui Bao & Jian-Wei Pan

Nature 629, 579–585 (2024) | Cite this article

3190 Accesses | 87 Altmetric | Metrics

### Abstract

Quantum internet<sup>1,2</sup>, a pivotal milestone entails



DOI:10.1145/3524455

**A deep dive into the quantum Internet's potential to transform and disrupt.**

BY LASZLO GYONGYOSI AND SANDOR IMRE

## Advances in the Quantum Internet

The quantum Internet uses the fundamental concepts of quantum mechanics for networking (see Sidebars 1–7 in the online Supplementary Information at <https://doi.acm.org/doi/10.1145/3524455>). The main attributes of the quantum Internet are advanced quantum phenomena and protocols (such as quantum superposition and quantum entanglement, quantum teleportation, and advanced quantum coding methods). *unconditional security*

The screenshot shows the top navigation bar of the Science journal website with links for 'Current Issue', 'First release papers', 'Archive', 'About', 'Submit manuscript', and 'Explore content'. Below this, a banner for the article 'Realization of a multimode quantum network of remote solid-state qubits' is displayed, featuring a dark background with colorful, glowing circular patterns. The title 'Realization of a multimode quantum network of remote solid-state qubits' is prominently displayed in large, bold, white font.

## Science

HOME > SCIENCE > VOL. 372, NO. 6529 > REALIZATION OF A MULTIMODE QUANTUM NETWORK OF REMOTE SOLID-STATE QUBITS

RESEARCH ARTICLE



## Realization of a multimode quantum network of remote solid-state qubits

M. POMPU, S. L. N. HERMANS, S. BAER, H. K. C. BEUKERS, P. C. HUMPHREYS, B. N. SCHOUTEN, S. F. L. VERMEULEN, M. J. TIGELMAN, L. DOS SANTOS MARTINS, J.-L. AND R. HANGGI, +2 authors Authors Info & Affiliations

SCIENCE • 16 Apr 2021 • Vol. 372, Issue 6539 • pp. 259–264 • DOI:10.1126/science.abb1919

Published: 15 May 2024  
of nanophotonic quantum memory com network

Y.-C. Wei, D. R. Assumpcao, P.-J. Stas, Y.-Q. Huan, B. Machieloo, E.N. Sinclair, C. De Eknamkul, D. S. Levonian, M. K. Bhaskar, H. Park, M.

Cite this article

Metrics

Practical quantum networks for long-distance quantum entanglement between quantum memory nodes connected <sup>1,2,3</sup>. Here we demonstrate a two-node quantum network based on silicon-vacancy (SiV) centres in nanophotonic with a telecommunication fibre network. Remote entanglement interactions between the electron spin qubits of the SiVs heralded spin-photon entangling gate operations with time-bin entanglement storage and integrated error detection. By using quantum frequency conversion of photonic communication frequencies (1,350 nm), we demonstrate

2/16

# Quantum networks are coming into reality

**NewScientist**

Sign in | Enter search keywords

News Features Newsletters Podcasts Video Comment Culture Crosswords | This week's magazine 1145/3524455

Health Space Physics Technology Environment Mind Humans Life Mathematics Chemistry Earth Socie

Technology

## Quantum internet draws near thanks to entangled memory breakthroughs

Researchers aiming to create a secure quantum version of the internet called a quantum repeater, which doesn't yet exist - but now two teams are well on the way to building one

By Alex Wilkins

15 May 2024

Quantum networks could spread across a city

Foto: Shutterstock

Frequency conversion

Photonic time-bin qubit

TDI

Node A

Node B

SV

Microwave stripe

Nanophotonic cavity

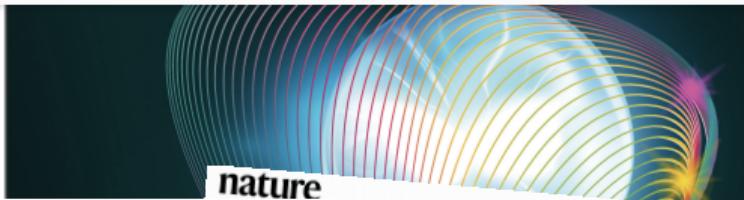
**Quantum Internet Draws Nearer**

Harvard University researchers assemble a quantum network spanning 35 kilometers across Boston, Massachusetts, linking two nodes separated by a loop of optical fiber. The fiber is a diamond with an atom-sized hole. Meanwhile, researchers at the University of Science and Technology of China entangled three nodes.

AT

○ ACM TechNews <technews-editor@acm.org>

To: Buckley Anita



**nature**

About the journal | Publish with us

Published: 15 May 2024

## of nanophotonic quantum memory com network

Y.-C. Wei, D. R. Assumpcao, P.-J. Stas, Y.-Q. Huan, B. Machieloo, E.N. Sinclair, C. De-Eknamkul, D. S. Levonian, M. K. Bhaskar, H. Park, M.

Cite this article

Metrics

## Cloud Computing Under the Cover of Quantum

Researchers at the U.K.'s University of Oxford and France's Sorbonne University demonstrated blind quantum computing using trapped ions. The quantum cloud system's "server" was made from a strontium atom (the network qubit) and a calcium ion (the memory qubit). The server does not know the electronic state of the network qubit but can still process its information via a laser-based process that entangles the network and memory qubits. The system also uses one-time-padded encryption to encode information, concealing the data and operations from the server.

2/16

Communication frequencies (1,350 nm), we demon-

## Bell pair: a pair of entangled qubits

- Fundamental *resource* in quantum networks
- *Bell pair* is a pair of entangled qubits:  
 $R \sim B$  distributed between nodes  $R$  and  $B$
- No headers: control information needs to be sent via separate classical channels



Artwork by Sandbox Studio, Chicago with Ana Kova  
Image by Andrij Borys Associates, using Shutterstock

## Bell pair: a pair of entangled qubits

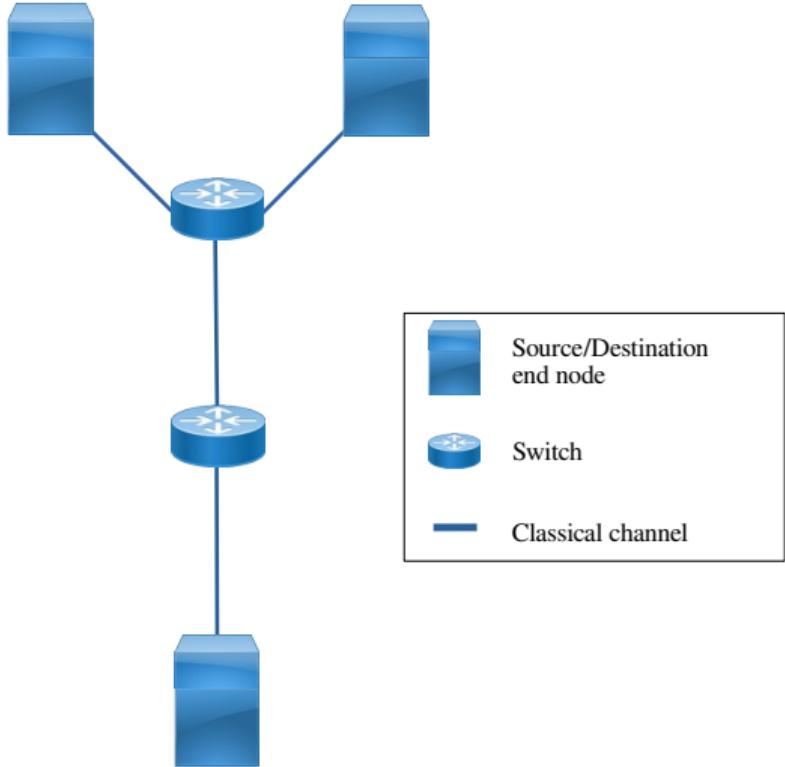
- Fundamental *resource* in quantum networks
- *Bell pair* is a pair of entangled qubits:  
 $R \sim B$  distributed between nodes  $R$  and  $B$
- No headers: control information needs to be sent via separate classical channels



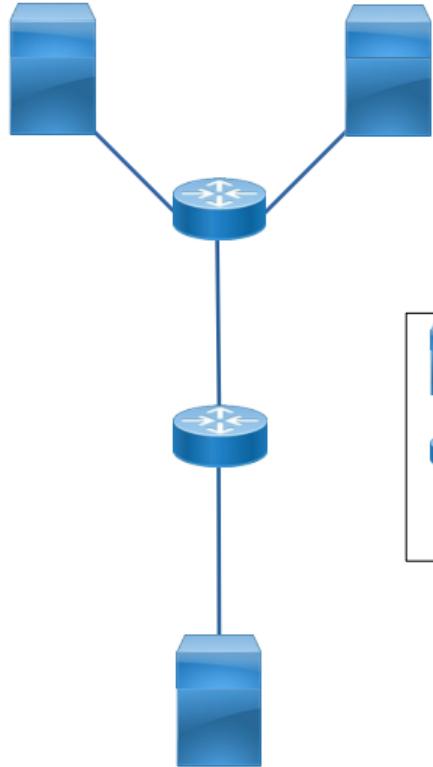
Artwork by Sandbox Studio, Chicago with Ana Kova  
Image by Andrij Borys Associates, using Shutterstock



## Classical network

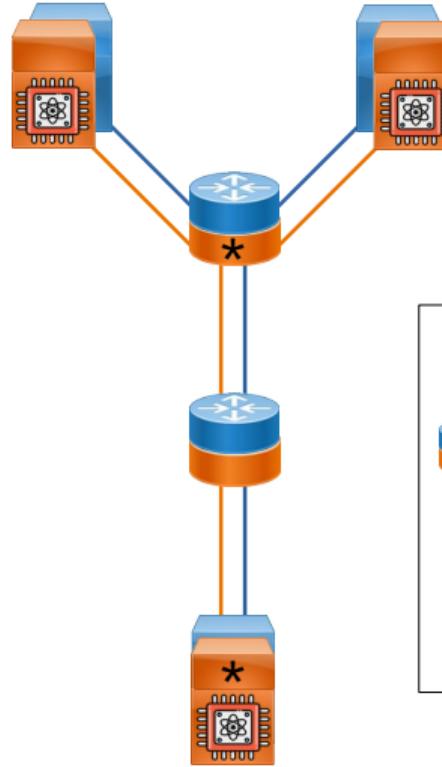


## Classical network



Source/Destination end node  
 Switch  
— Classical channel

## Quantum network <sup>1,2</sup>

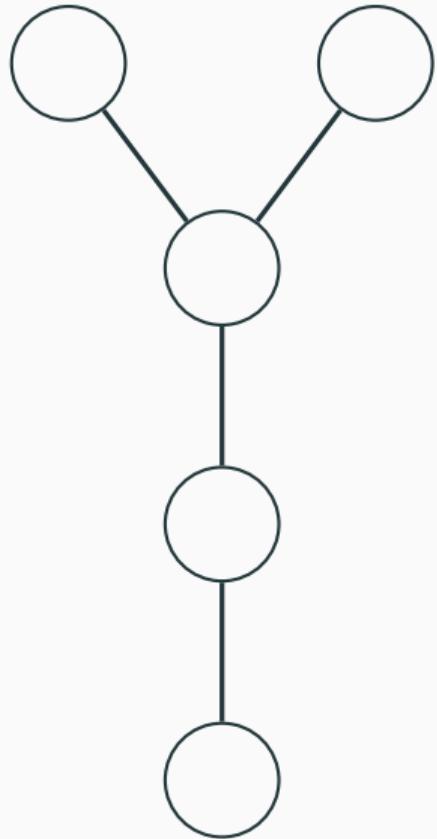


Quantum capable end node  
 Repeater with classical and quantum capabilities  
— Quantum channel  
— Classical channel  
\* Quantum source

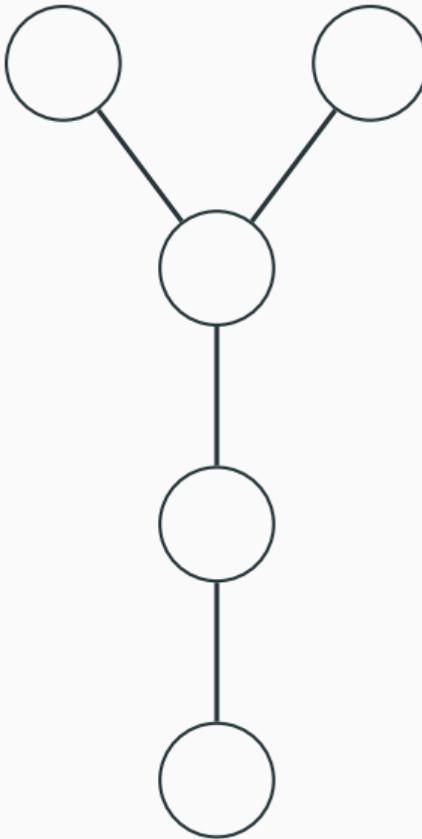
<sup>1</sup>[Kozlowski and Wehner: NANOCOM 2019],

<sup>2</sup>[Quantum Internet Research Group: RFC 9340 2023]

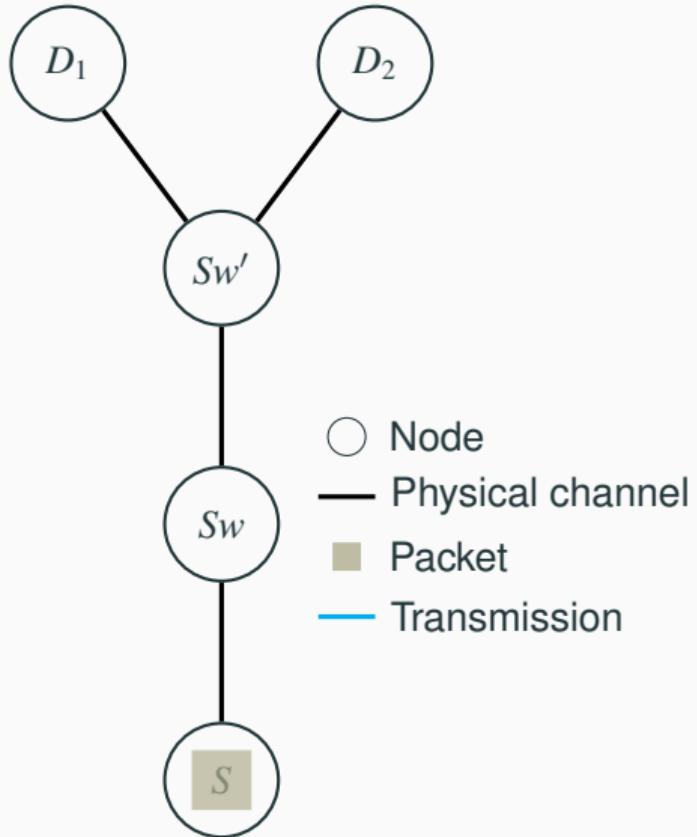
**Classical network**



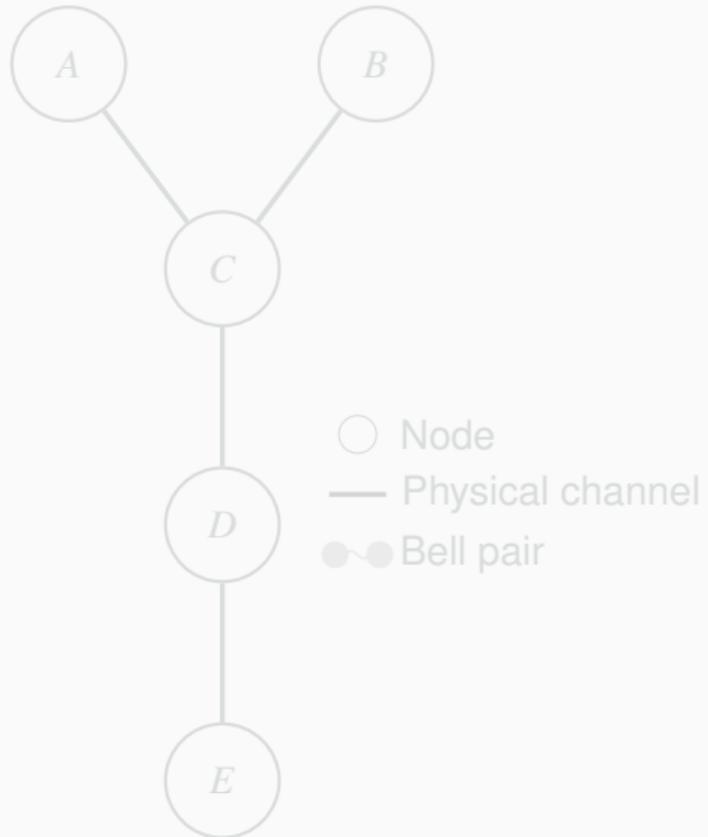
**Quantum network**



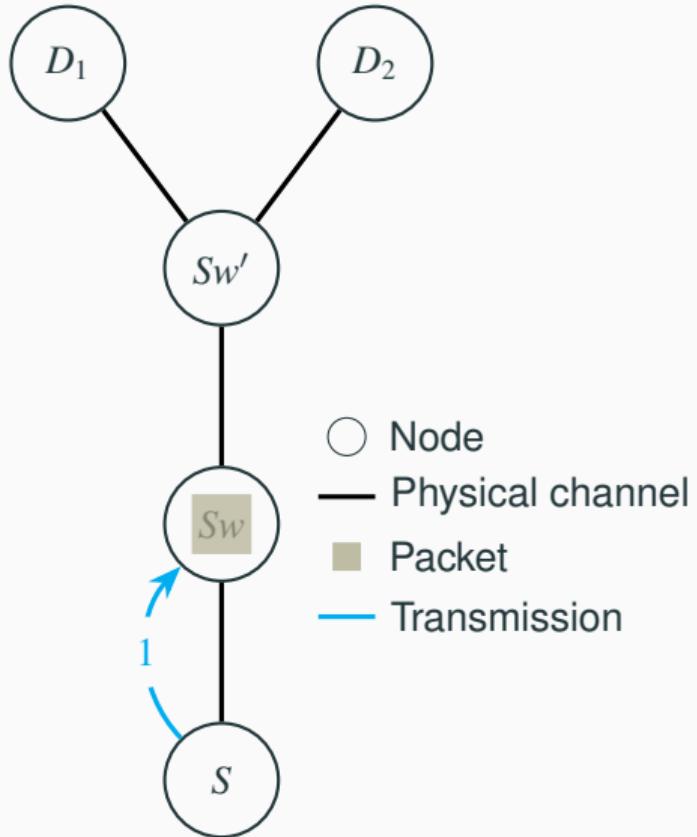
## Forwarding packets



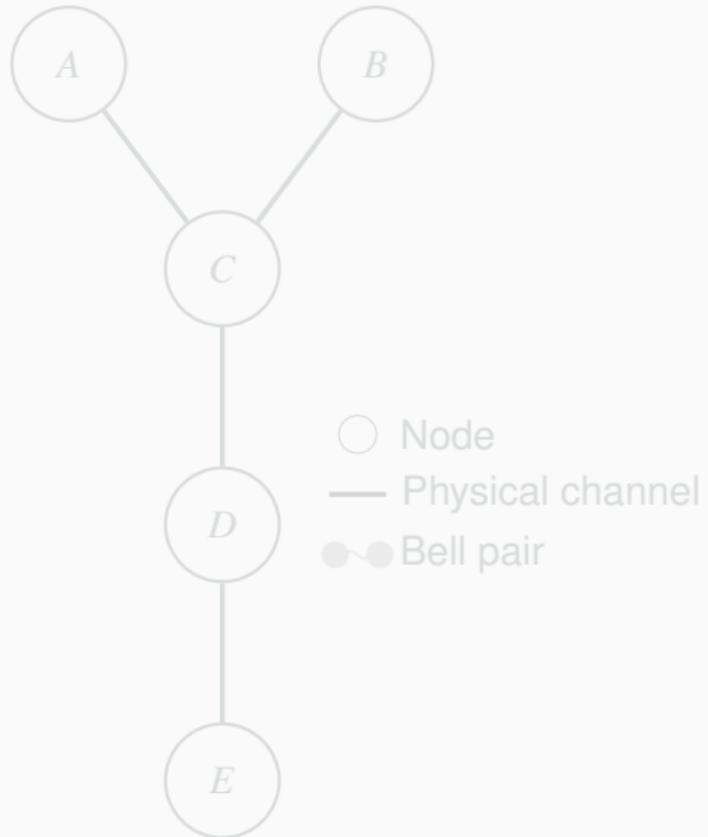
## Distributing Bell pairs



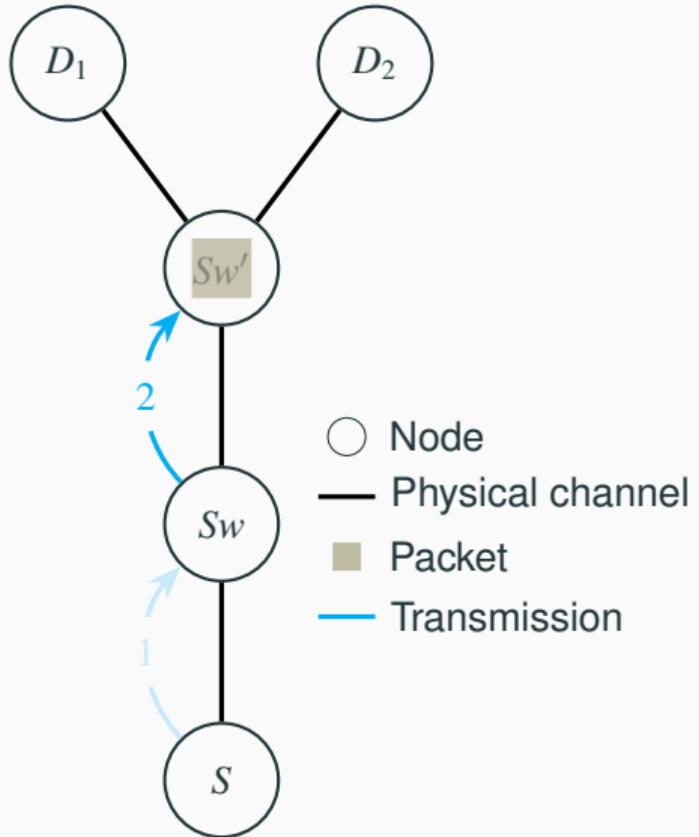
## Forwarding packets



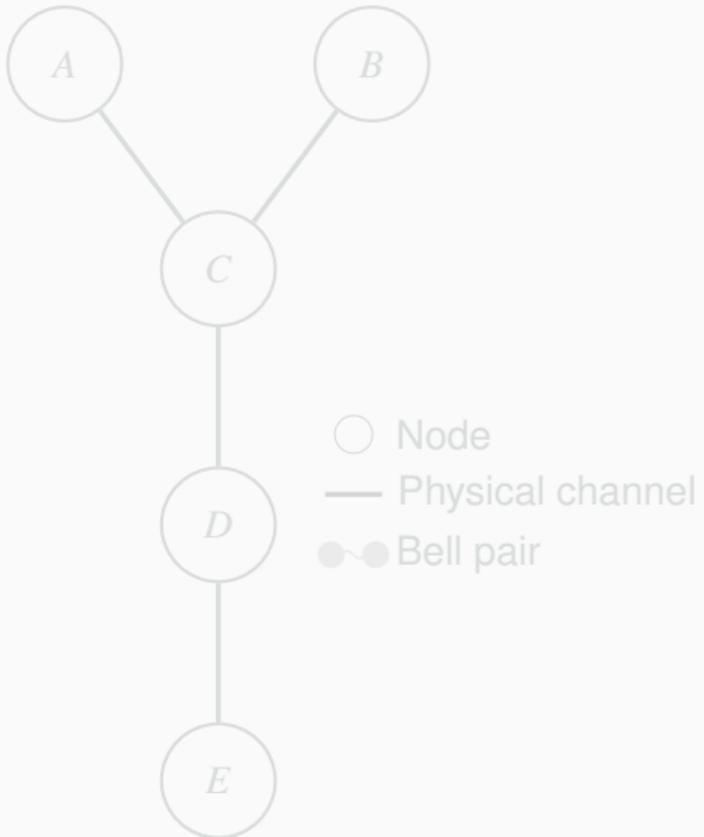
## Distributing Bell pairs



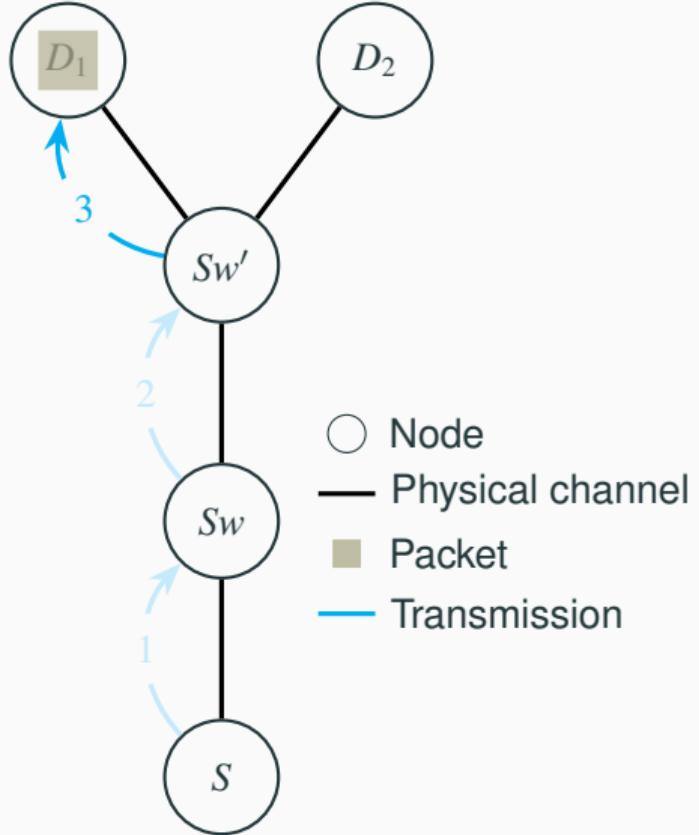
## Forwarding packets



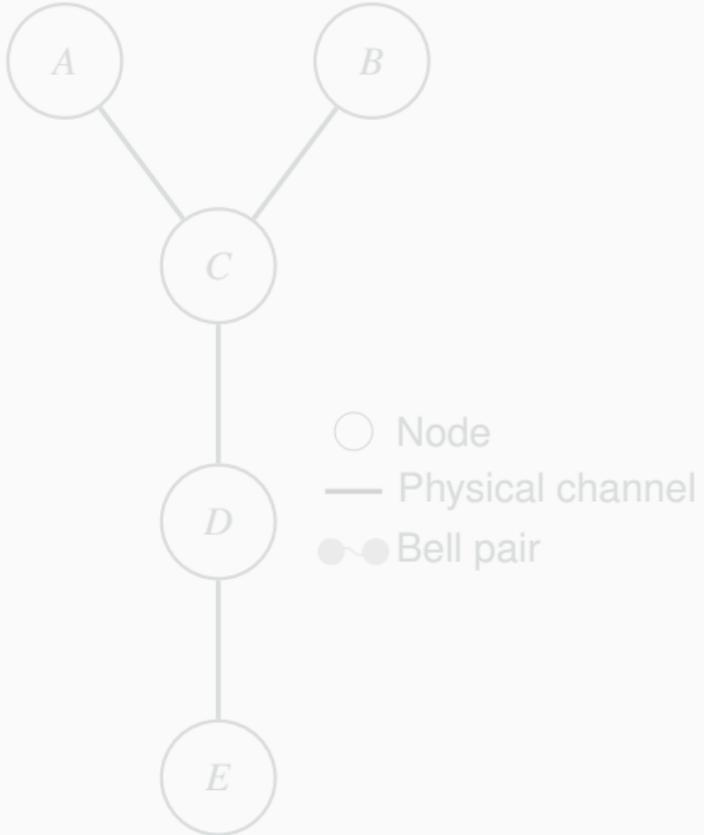
## Distributing Bell pairs



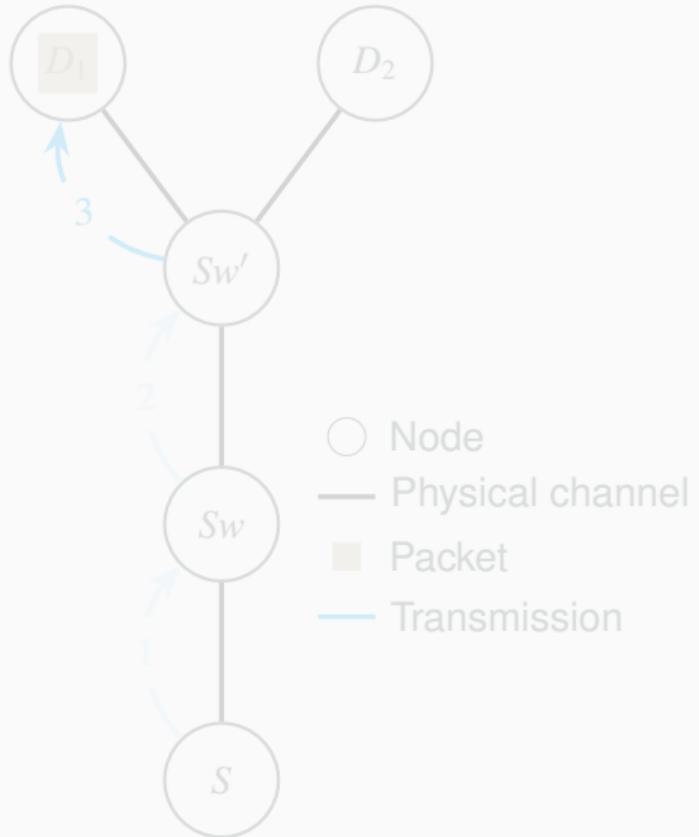
## Forwarding packets



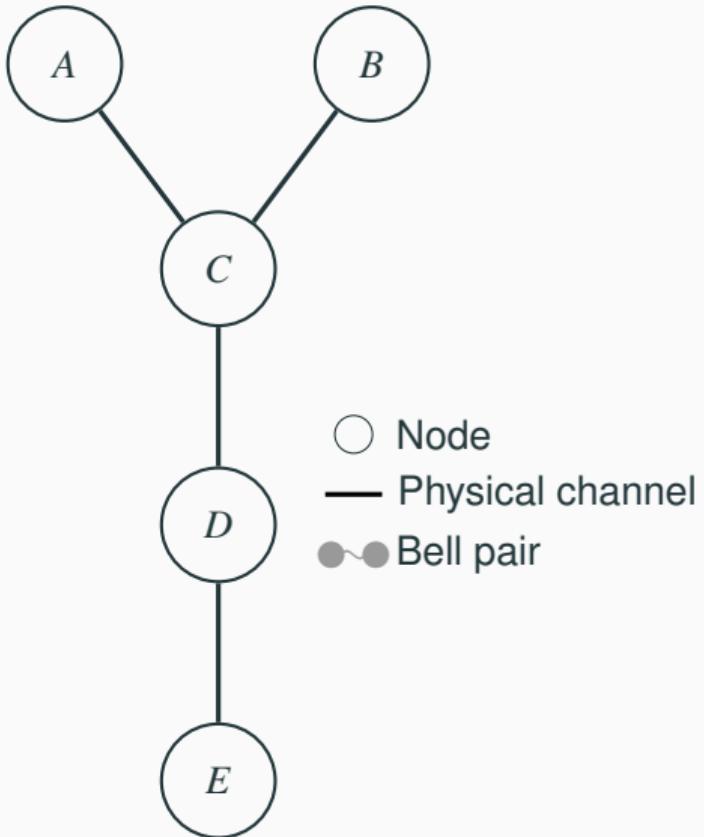
## Distributing Bell pairs



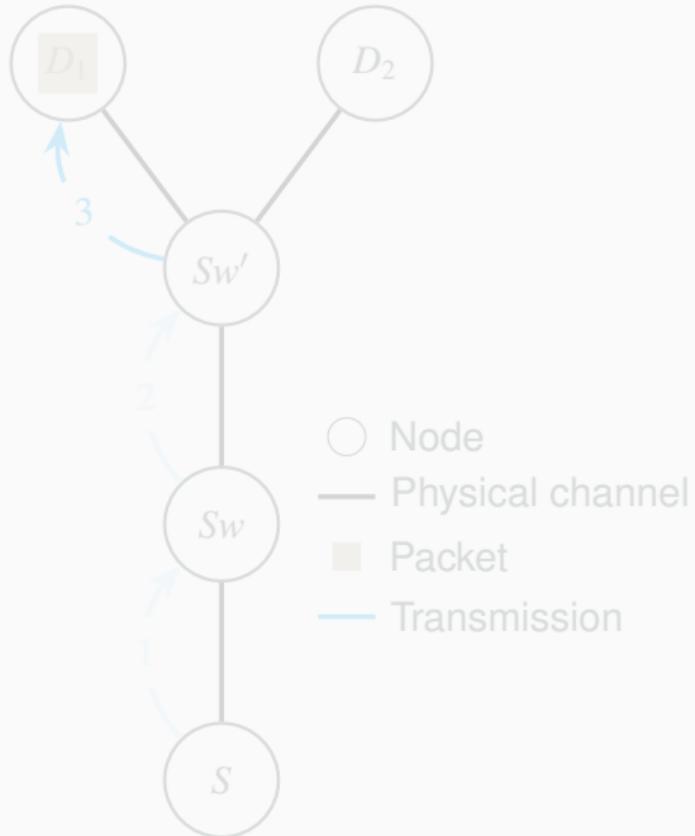
## Forwarding packets



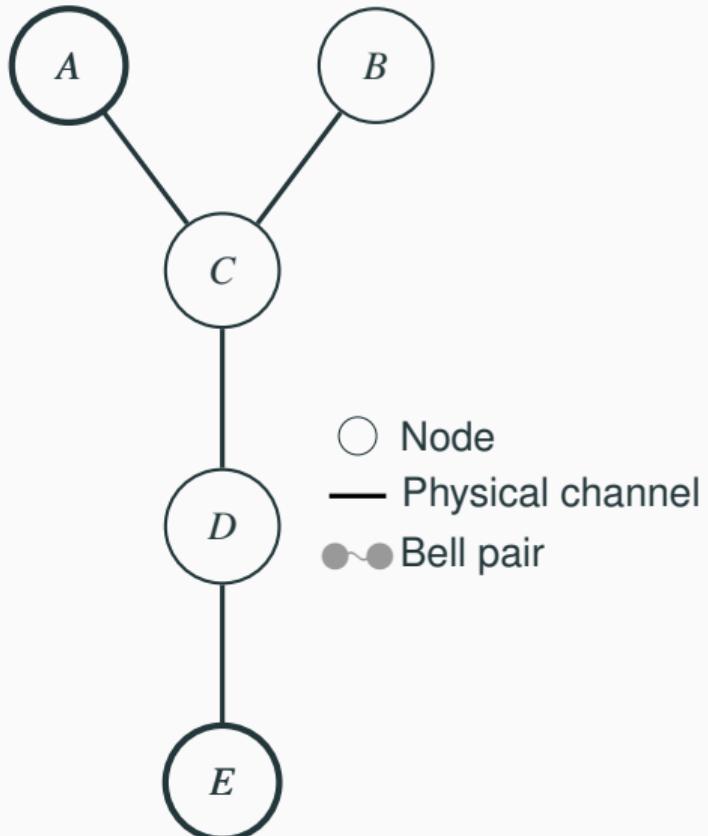
## Distributing Bell pairs



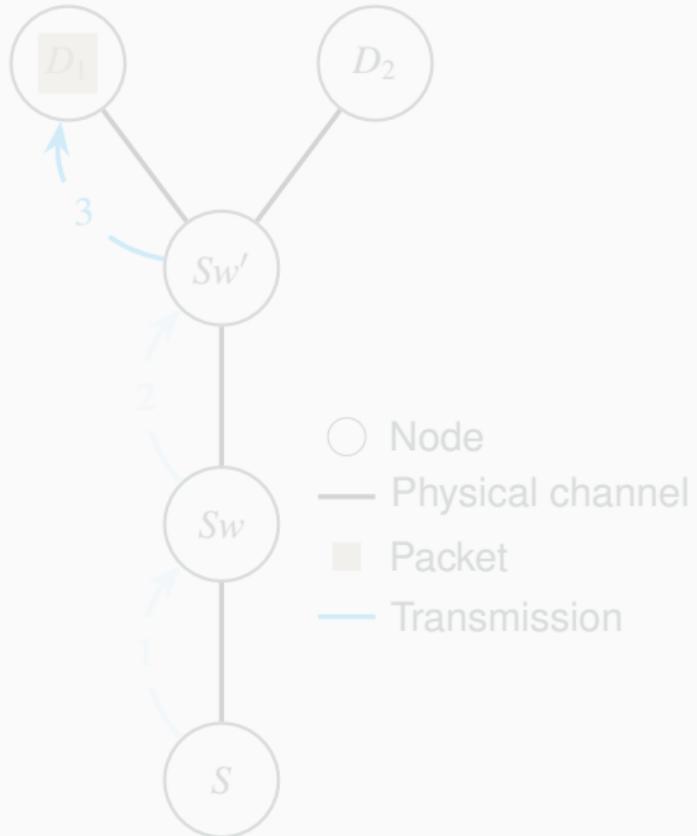
## Forwarding packets



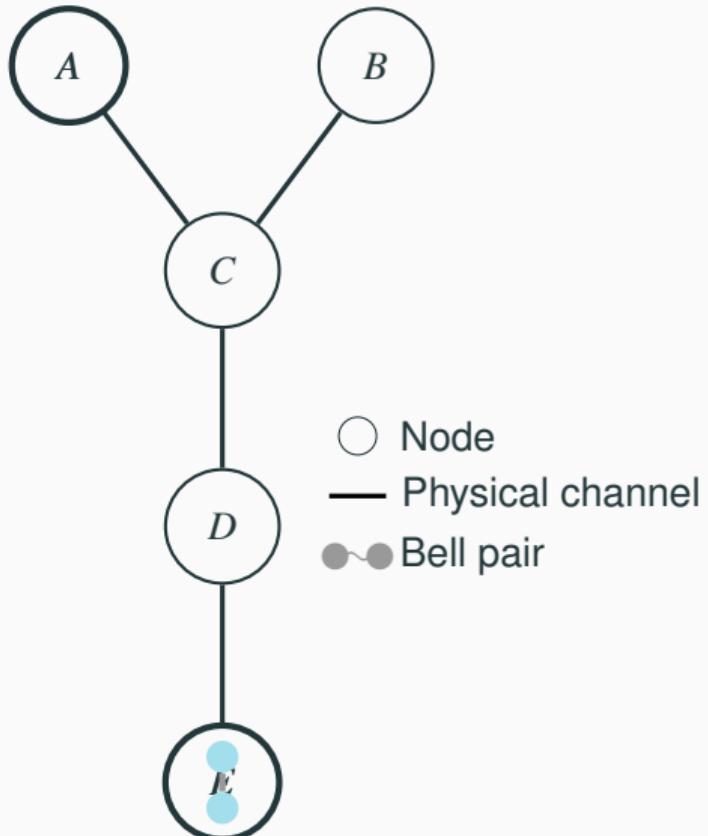
## Distributing Bell pairs



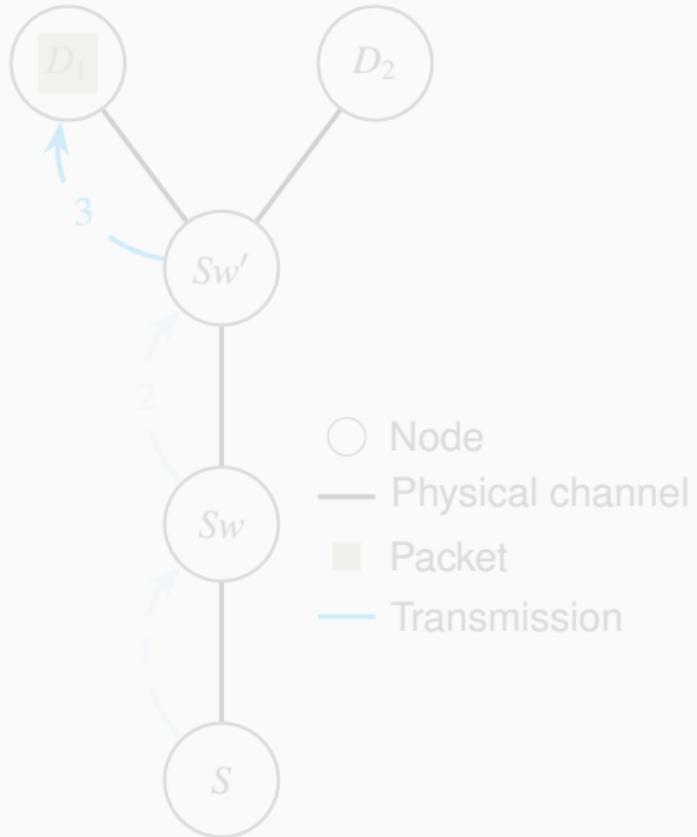
## Forwarding packets



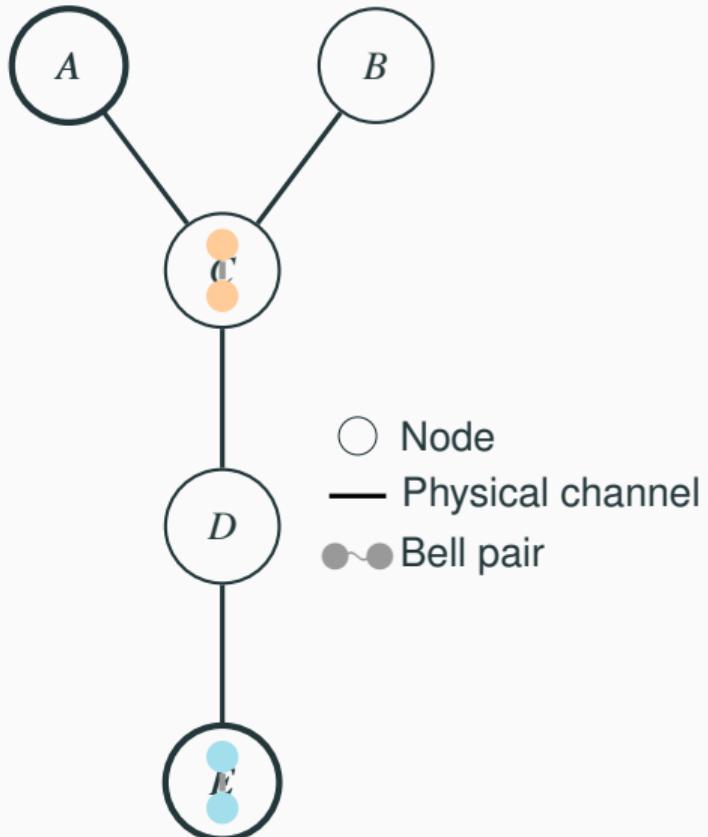
## Distributing Bell pairs



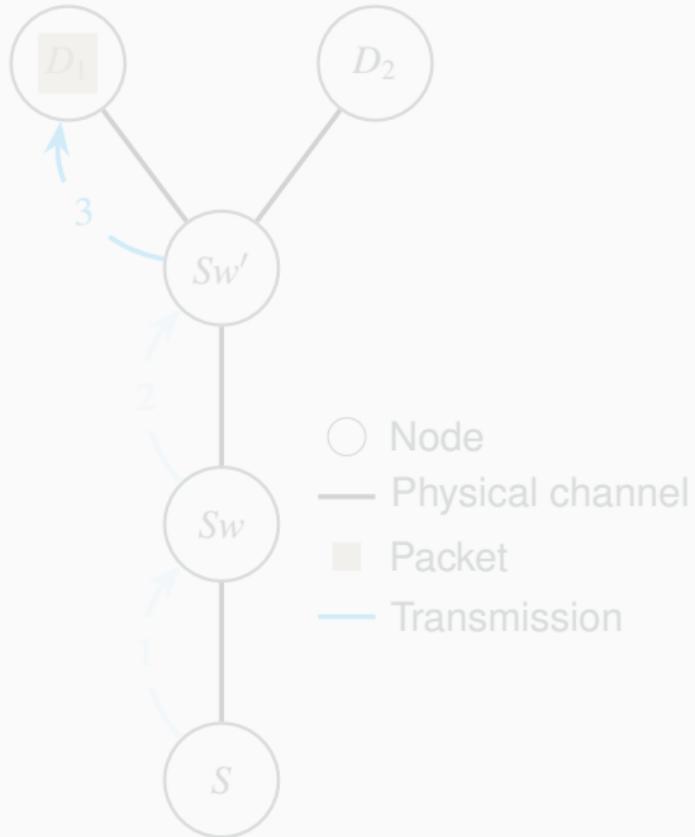
## Forwarding packets



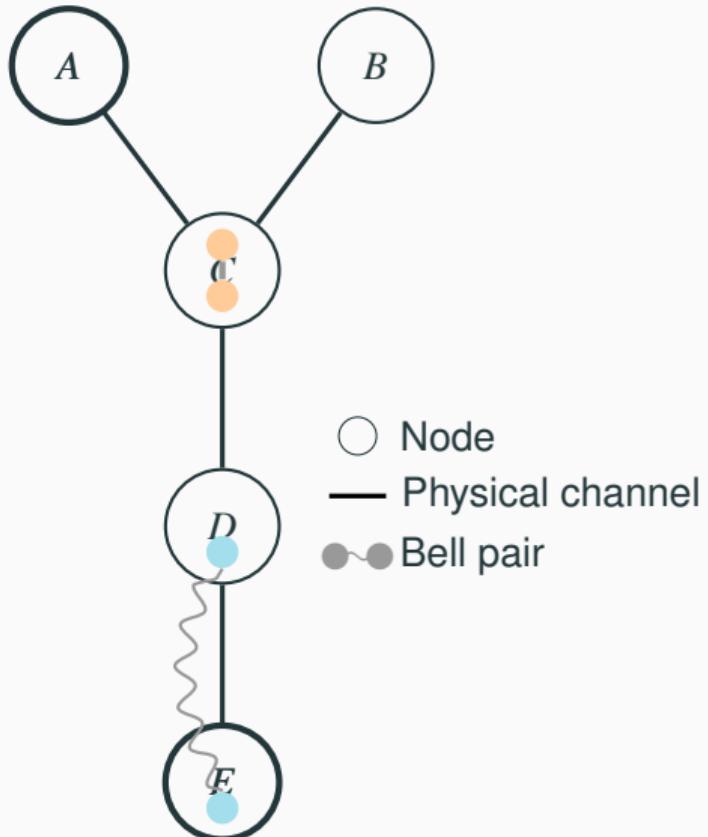
## Distributing Bell pairs



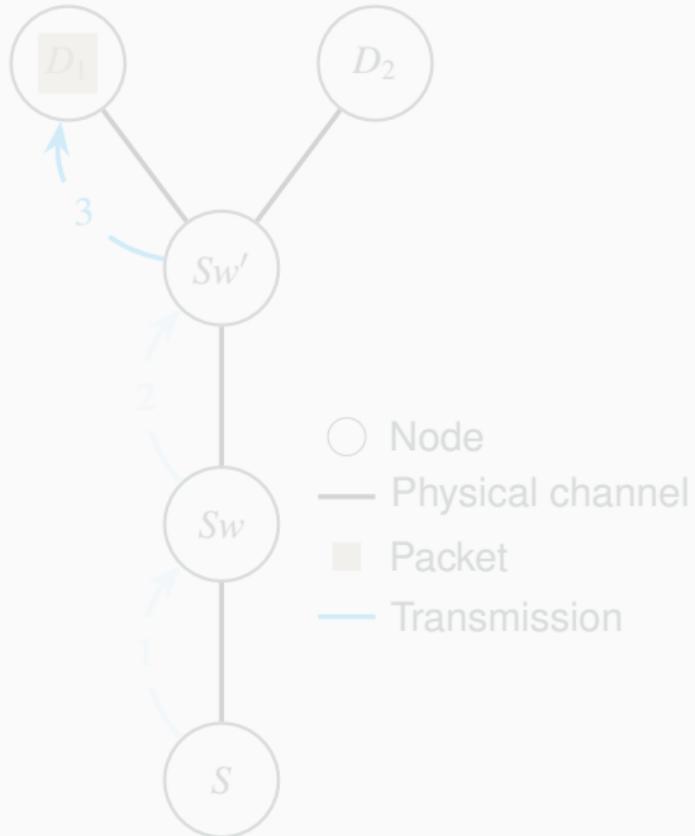
## Forwarding packets



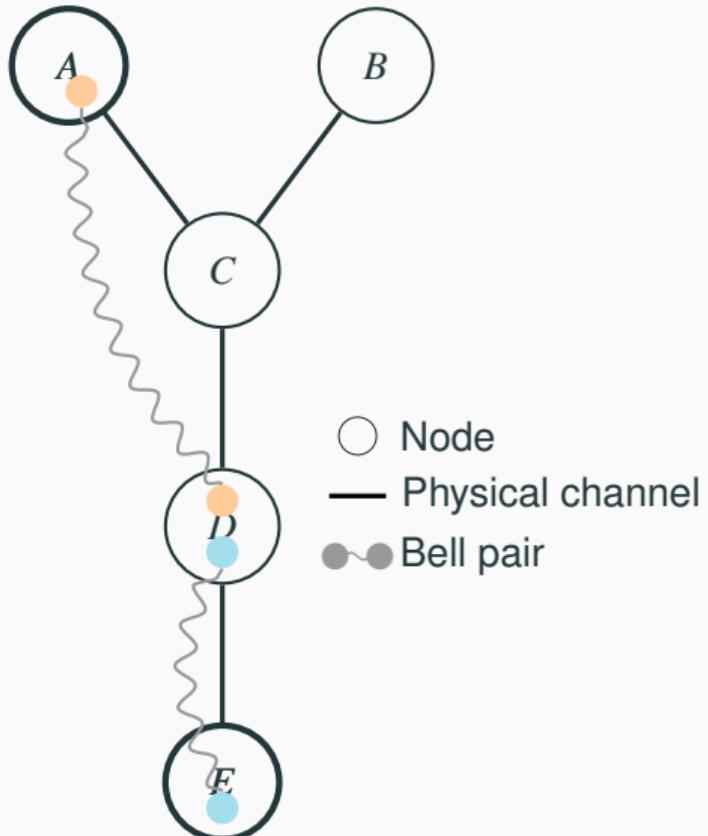
## Distributing Bell pairs



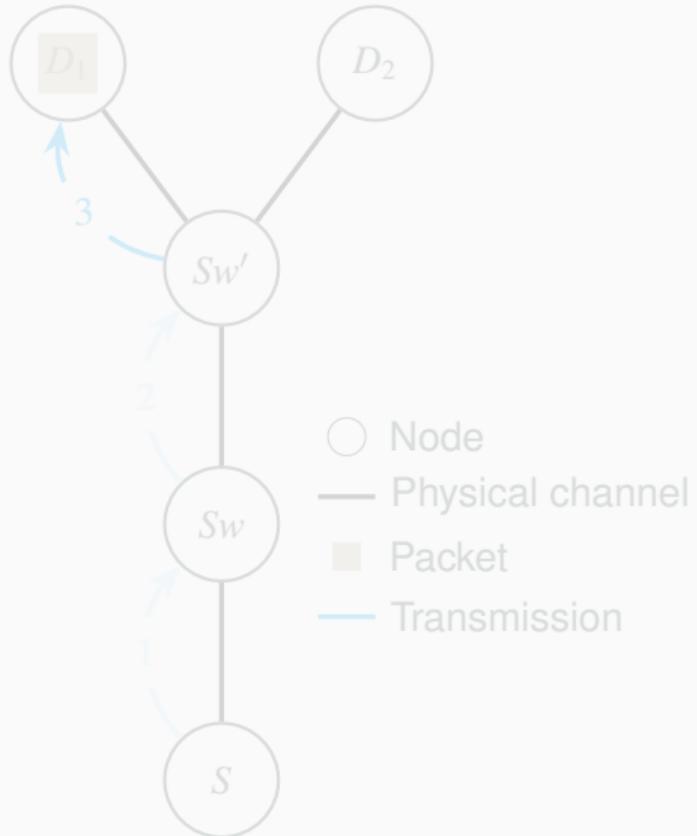
## Forwarding packets



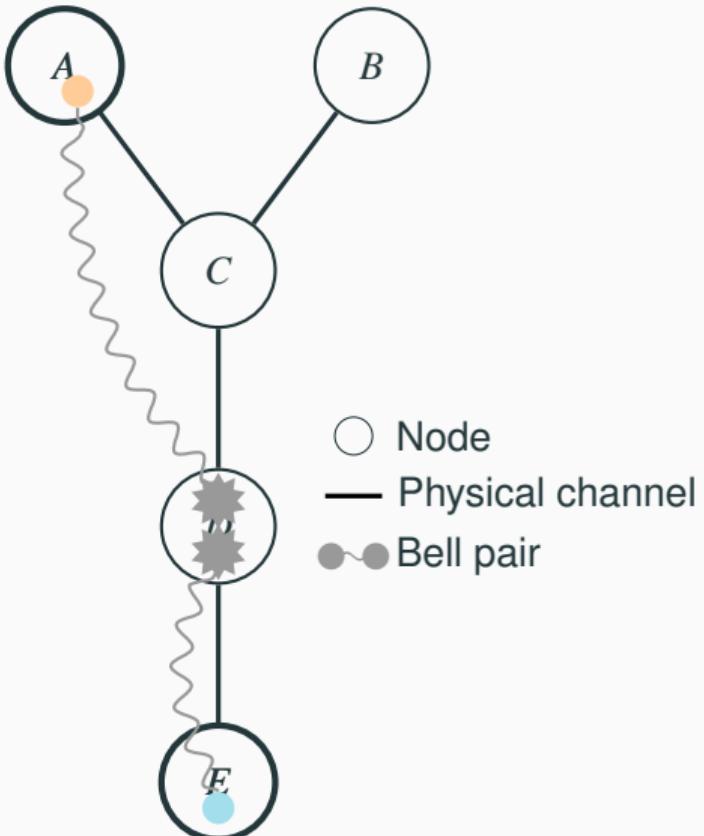
## Distributing Bell pairs



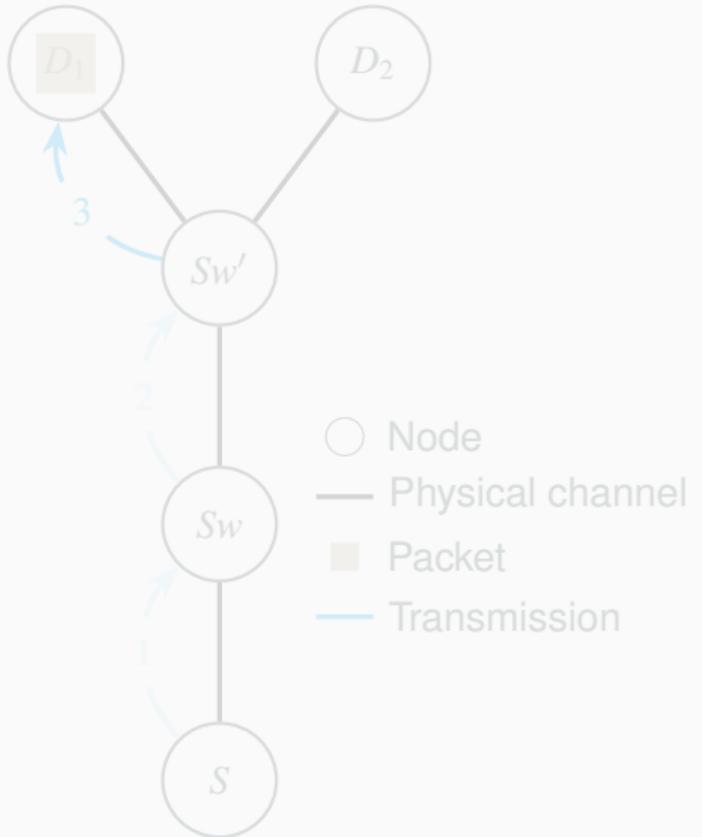
## Forwarding packets



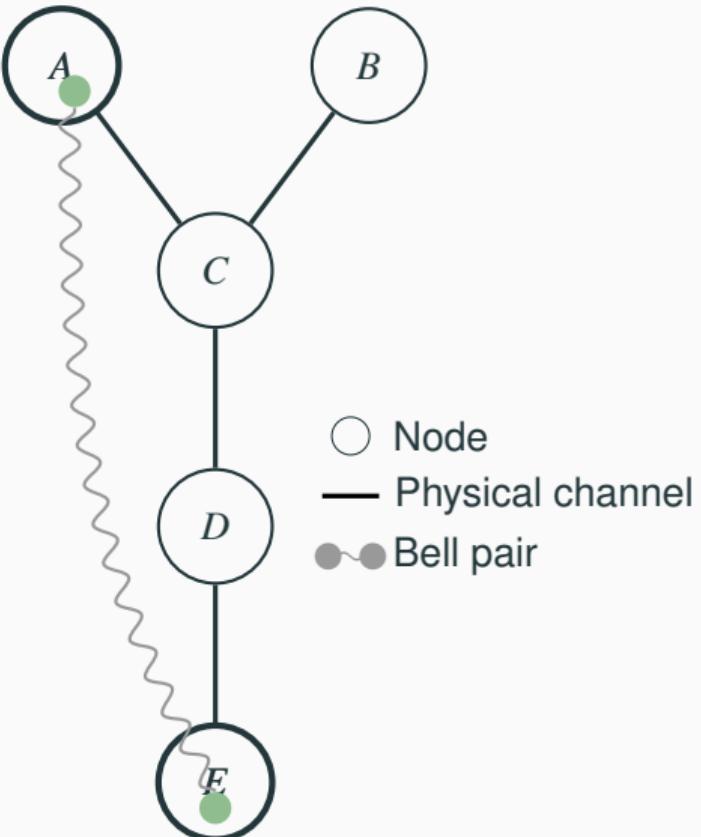
## Distributing Bell pairs



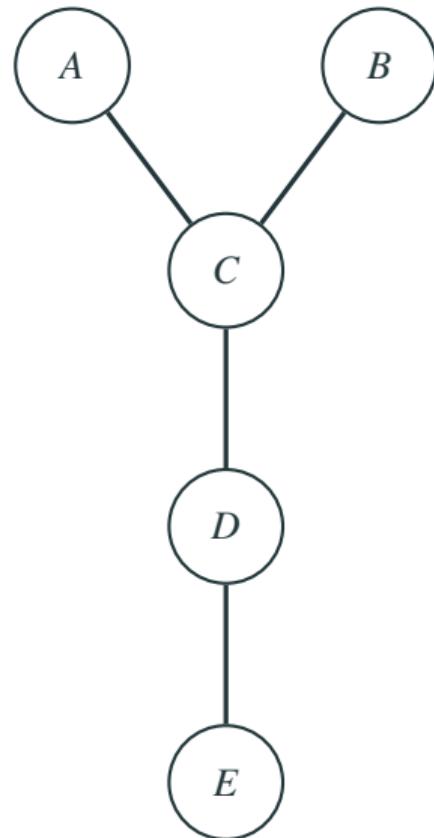
## Forwarding packets



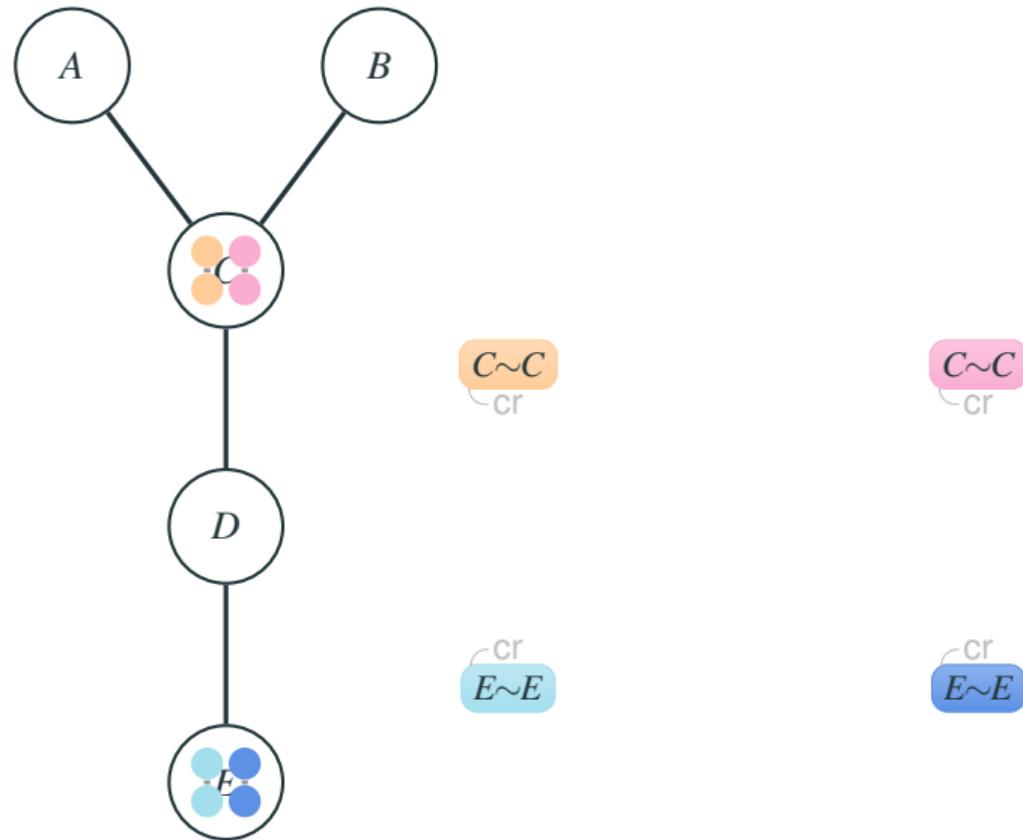
## Distributing Bell pairs



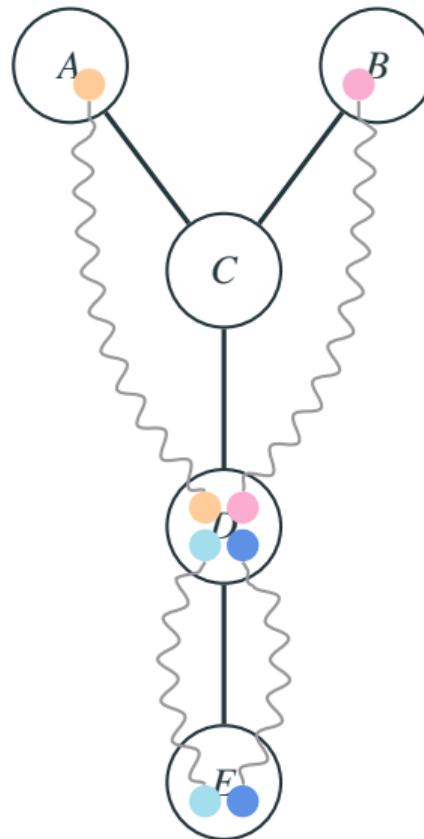
## End-to-end Bell pair generation protocol



# End-to-end Bell pair generation protocol



# End-to-end Bell pair generation protocol



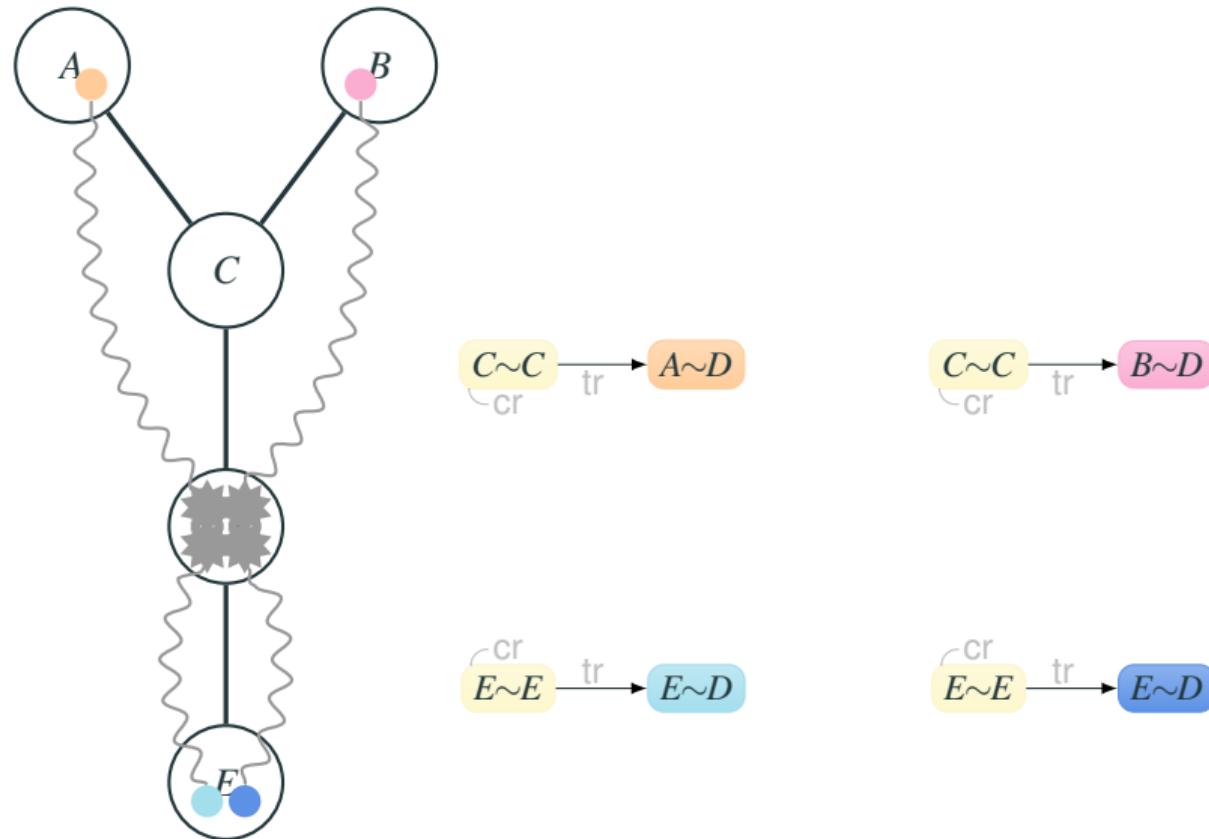
$\overset{\text{cr}}{C \sim C} \xrightarrow{\text{tr}} A \sim D$

$\overset{\text{cr}}{C \sim C} \xrightarrow{\text{tr}} B \sim D$

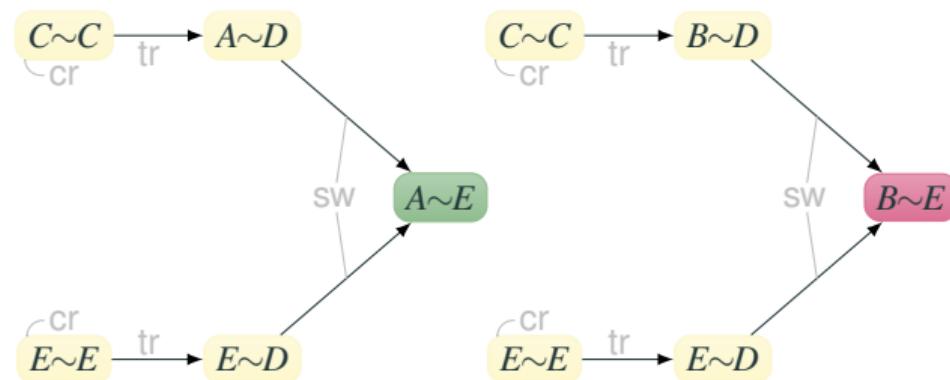
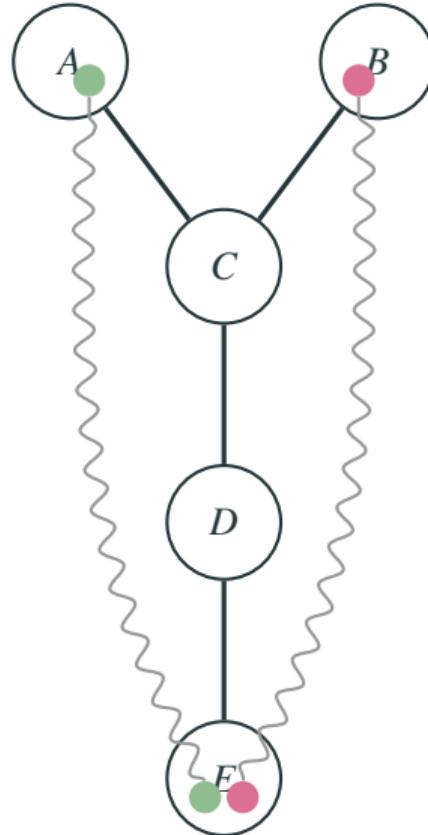
$\overset{\text{cr}}{E \sim E} \xrightarrow{\text{tr}} E \sim D$

$\overset{\text{cr}}{E \sim E} \xrightarrow{\text{tr}} E \sim D$

# End-to-end Bell pair generation protocol



# End-to-end Bell pair generation protocol



## Verification and optimization

# Verification and optimization

## PROBLEM

How to make sure that quantum networks behave as intended?

# Verification and optimization

## PROBLEM

How to make sure that quantum networks behave as intended?

- Does a protocol establish Bell pairs between the specified end nodes?

# Verification and optimization

## PROBLEM

How to make sure that quantum networks behave as intended?

- Does a protocol establish Bell pairs between the specified end nodes?
- Are two protocols equivalent?

# Verification and optimization

## PROBLEM

How to make sure that quantum networks behave as intended?

- Does a protocol establish Bell pairs between the specified end nodes?
- Are two protocols equivalent?
- Can a protocol execute with a given number of resources?

# Verification and optimization

## PROBLEM

How to make sure that quantum networks behave as intended?

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

# Verification and optimization

## PROBLEM

How to make sure that quantum networks behave as intended?

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

## SOLUTION

Provide formalism to answer these types of questions about quantum networks

# BellKAT language

# BellKAT language

Specification language for end-to-end Bell pairs generation – BellKAT

# BellKAT language

Specification language for end-to-end Bell pairs generation – **BellKAT**

# BellKAT language

Specification language for end-to-end Bell pairs generation – BellKAT

# BellKAT language

Specification language for end-to-end Bell pairs generation – **BellKAT**

- Syntax and semantics
  - provide abstractions for quantum network primitives: create cr, transmit tr, swap sw, ...
  - model multiround behavior, catering for highly synchronized nature of quantum networks
  - capture resource sharing (protocols competing for available Bell pairs)

# BellKAT language

Specification language for end-to-end Bell pairs generation – **BellKAT**

- Syntax and semantics
  - provide abstractions for quantum network primitives: create cr, transmit tr, swap sw, ...
  - model multiround behavior, catering for highly synchronized nature of quantum networks
  - capture resource sharing (protocols competing for available Bell pairs)
- Algebraic structure based on Kleene algebra with tests (KAT)
  - with (novel) axioms capturing round synchronization

# BellKAT language

Specification language for end-to-end Bell pairs generation – **BellKAT**

- Syntax and semantics
  - provide abstractions for quantum network primitives: create cr, transmit tr, swap sw, ...
  - model multiround behavior, catering for highly synchronized nature of quantum networks
  - capture resource sharing (protocols competing for available Bell pairs)
- Algebraic structure based on Kleene algebra with tests (KAT)
  - with (novel) axioms capturing round synchronization
- Formal results
  - proofs of soundness and completeness of equational theory
  - decidability of semantic equivalences

## BellKAT primitives – basic actions

## BellKAT primitives – basic actions

$$r \triangleright o : \textcolor{brown}{a} \mapsto \begin{cases} \textcolor{green}{o} \bowtie \textcolor{blue}{a} \setminus r & \text{if } \textcolor{red}{r} \subseteq \textcolor{brown}{a} \\ \emptyset \bowtie \textcolor{blue}{a} & \text{otherwise} \end{cases}$$

## BellKAT primitives – basic actions

required BPs

$$r \triangleright o : \textcolor{brown}{a} \mapsto \begin{cases} \textcolor{green}{o} \bowtie \textcolor{blue}{a} \setminus r & \text{if } \textcolor{red}{r} \subseteq \textcolor{brown}{a} \\ \emptyset \bowtie \textcolor{blue}{a} & \text{otherwise} \end{cases}$$

## BellKAT primitives – basic actions

$$r \triangleright o : a \mapsto \begin{cases} o \bowtie a \setminus r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$

required BPs

output BPs

The diagram illustrates the mapping of required Bell pairs (BPs) to output BPs. It features two grey rounded rectangles at the top and bottom. The top rectangle is labeled "required BPs" and the bottom one is labeled "output BPs". A curved arrow points from "required BPs" down to the primitive expression  $r \triangleright o$ . Another curved arrow points from the primitive expression up to "output BPs".

$r, o, a : \text{multisets of Bell pairs}$     $\bowtie : \text{pair of multisets of Bell pairs}$

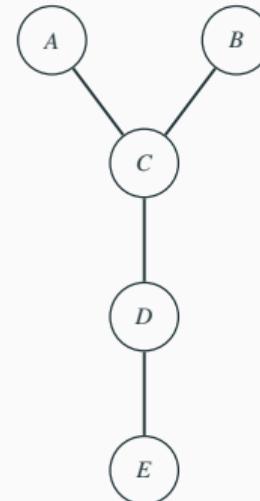
# BellKAT primitives – basic actions

required BPs

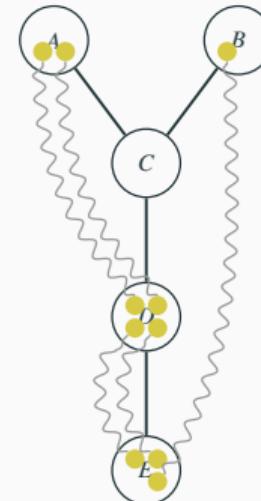
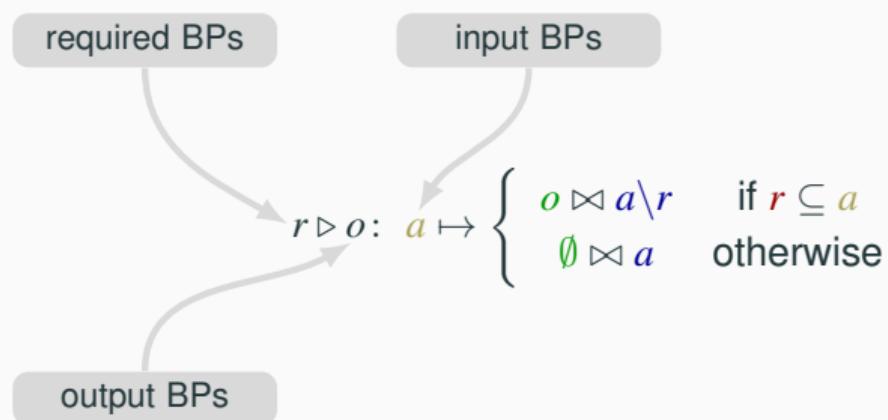
$$r \triangleright o : a \mapsto \begin{cases} o \bowtie a \setminus r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$

output BPs

Swap  $\{A \sim D, D \sim E\} \triangleright \{A \sim E\}$



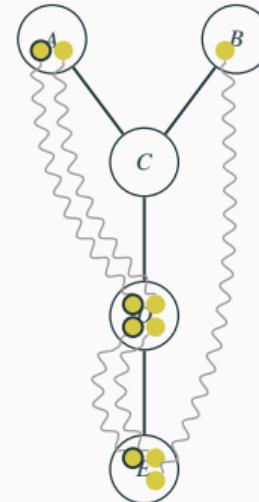
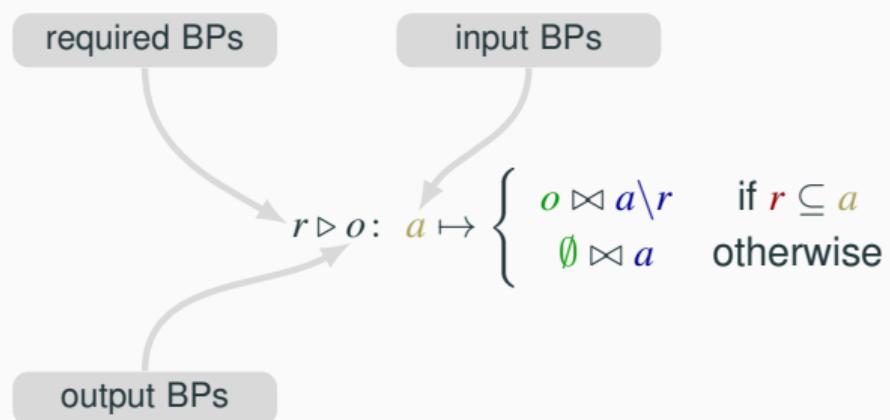
# BellKAT primitives – basic actions



Swap  $\{A \sim D, D \sim E\} \triangleright \{A \sim E\}$  acting on input  $\{A \sim D, A \sim D, D \sim E, D \sim E, B \sim E\}$

$A \sim D$        $D \sim E$        $A \sim D$        $D \sim E$        $B \sim E$

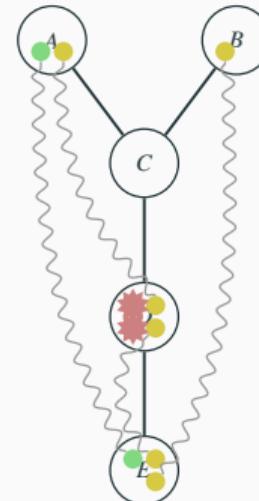
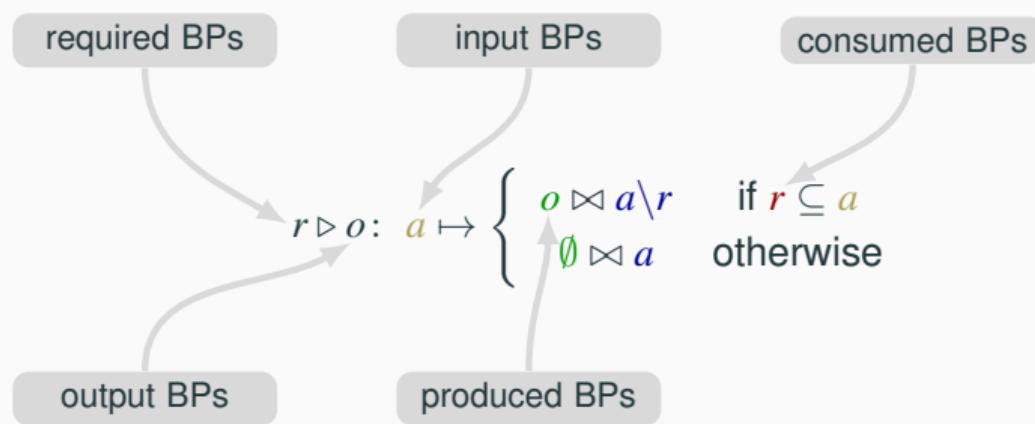
# BellKAT primitives – basic actions



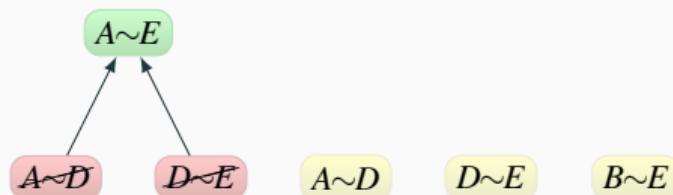
Swap  $\{A \sim D, D \sim E\} \triangleright \{A \sim E\}$  acting on input  $\{\underline{A \sim D}, A \sim D, \underline{D \sim E}, D \sim E, B \sim E\}$

$A \sim D$        $D \sim E$        $A \sim D$        $D \sim E$        $B \sim E$

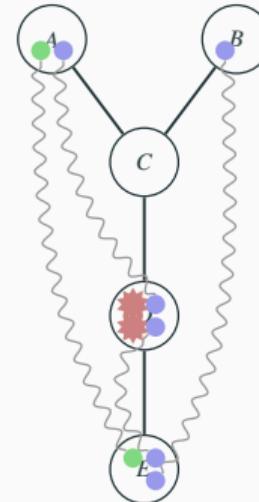
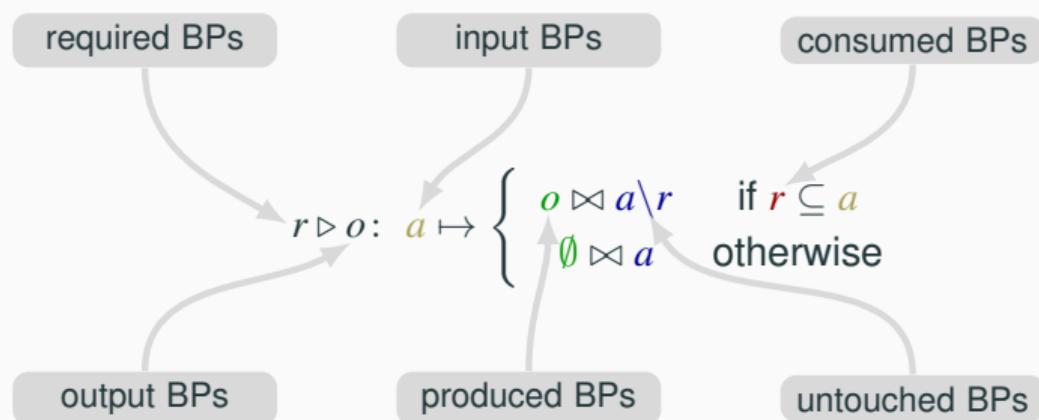
# BellKAT primitives – basic actions



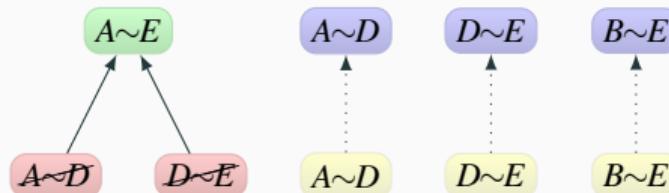
Swap  $\{A \sim D, D \sim E\} \triangleright \{A \sim E\}$  acting on input  $\{A \sim D, A \sim D, D \sim E, D \sim E, B \sim E\}$



# BellKAT primitives – basic actions

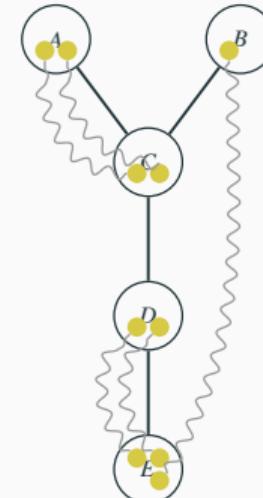
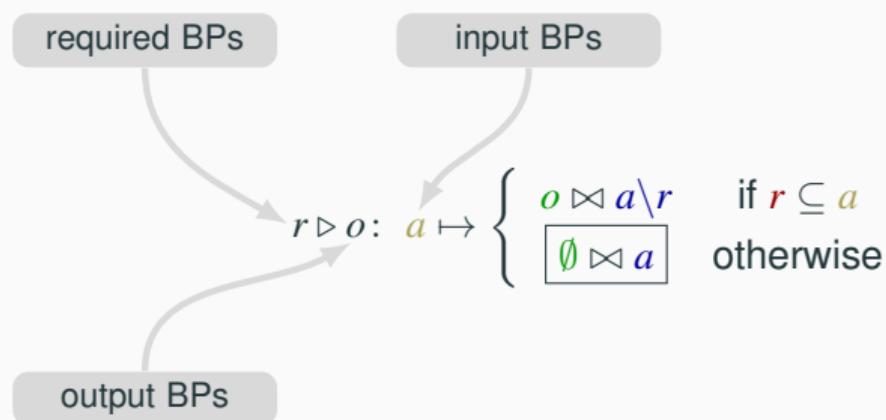


Swap  $\{A \sim D, D \sim E\} \triangleright \{A \sim E\}$  acting on input  $\{A \sim D, A \sim D, D \sim E, D \sim E, B \sim E\}$



Input, consumed, produced and untouched Bell pairs

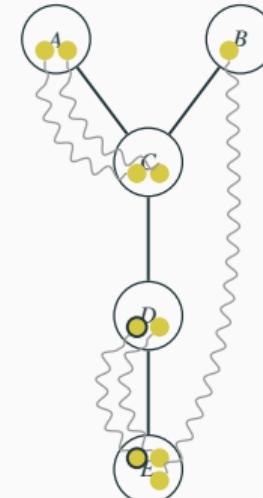
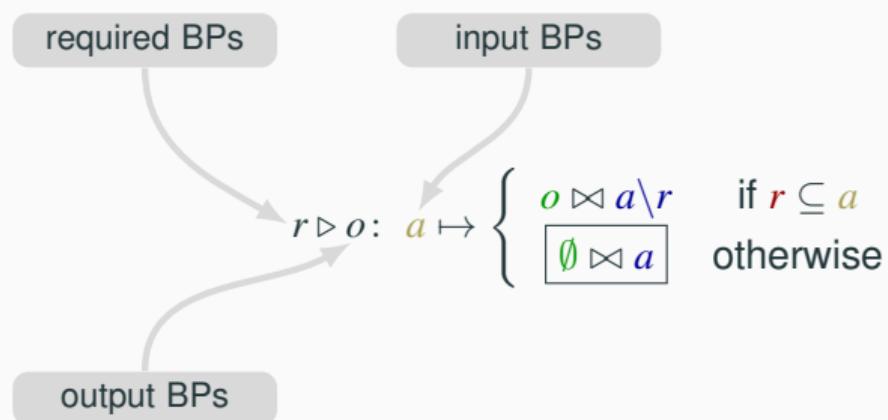
# BellKAT primitives – basic actions



Swap  $\{A \sim D, D \sim E\} \triangleright \{A \sim E\}$  acting on input  $\{A \sim C, A \sim C, D \sim E, D \sim E, B \sim E\}$

$A \sim C$      $D \sim E$      $A \sim C$      $D \sim E$      $B \sim E$

# BellKAT primitives – basic actions

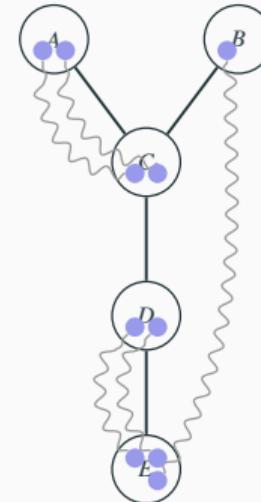
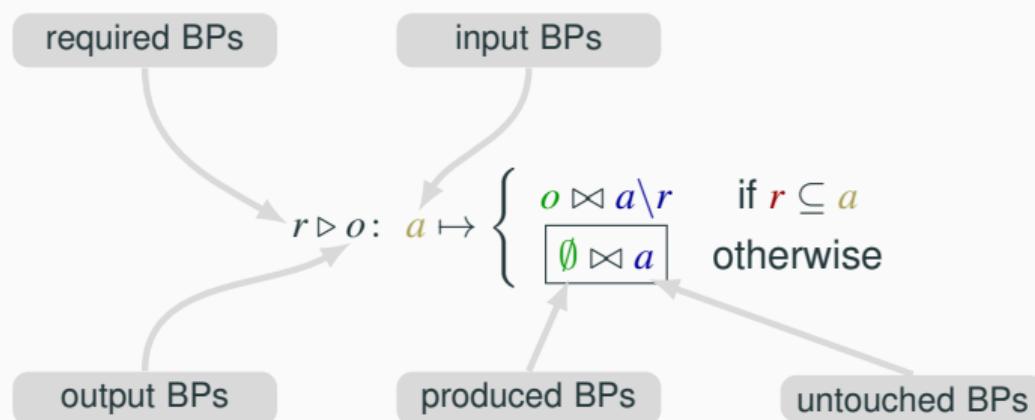


Swap  $\{A \sim D, D \sim E\} \triangleright \{A \sim E\}$  acting on input  $\{A \sim C, A \sim C, \underline{D \sim E}, D \sim E, B \sim E\}$

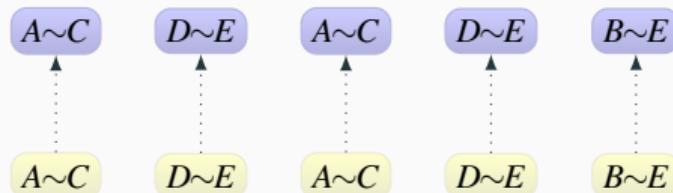
$A \sim C$      $D \sim E$      $A \sim C$      $D \sim E$      $B \sim E$

Input, consumed, produced and untouched Bell pairs

# BellKAT primitives – basic actions



Swap  $\{A \sim D, D \sim E\} \triangleright \{A \sim E\}$  acting on input  $\{A \sim C, A \sim C, \underline{D \sim E}, D \sim E, B \sim E\}$



Input, consumed, produced and untouched Bell pairs

## BellKAT primitives – basic actions

swap	$\text{sw}\langle A \sim B @ C \rangle \triangleq \{\{A \sim C, B \sim C\}\} \triangleright \{\{A \sim B\}\}$
transmit	$\text{tr}\langle A \rightarrow B \sim C \rangle \triangleq \{\{A \sim A\}\} \triangleright \{\{B \sim C\}\}$
create	$\text{cr}\langle A \rangle \triangleq \emptyset \triangleright \{\{A \sim A\}\}$
wait	$\text{wait}\langle r \rangle \triangleq r \triangleright r$
fail	$\text{fail}\langle r \rangle \triangleq r \triangleright \emptyset$

## BellKAT primitives – basic actions

swap	$\text{sw}\langle A \sim B @ C \rangle \triangleq \{\{A \sim C, B \sim C\}\} \triangleright \{\{A \sim B\}\}$
transmit	$\text{tr}\langle A \rightarrow B \sim C \rangle \triangleq \{\{A \sim A\}\} \triangleright \{\{B \sim C\}\}$
create	$\text{cr}\langle A \rangle \triangleq \emptyset \triangleright \{\{A \sim A\}\}$
wait	$\text{wait}\langle r \rangle \triangleq r \triangleright r$
fail	$\text{fail}\langle r \rangle \triangleq r \triangleright \emptyset$

## BellKAT primitives – basic actions

swap	$\text{sw}\langle A \sim B @ C \rangle \triangleq \{\{A \sim C, B \sim C\} \triangleright \{A \sim B\}$
transmit	$\text{tr}\langle A \rightarrow B \sim C \rangle \triangleq \{\{A \sim A\} \triangleright \{B \sim C\}$
create	$\text{cr}\langle A \rangle \triangleq \emptyset \triangleright \{A \sim A\}$
wait	$\text{wait}\langle r \rangle \triangleq r \triangleright r$
fail	$\text{fail}\langle r \rangle \triangleq r \triangleright \emptyset$

## BellKAT primitives – basic actions

$$\text{swap} \quad \text{sw}\langle A \sim B @ C \rangle \triangleq \{\{A \sim C, B \sim C\}\} \triangleright \{\{A \sim B\}\}$$

$$\text{transmit} \quad \text{tr}\langle A \rightarrow B \sim C \rangle \triangleq \{\{A \sim A\}\} \triangleright \{\{B \sim C\}\}$$

$$\text{create} \quad \text{cr}\langle A \rangle \triangleq \emptyset \triangleright \{\{A \sim A\}\}$$

$$\text{wait} \quad \text{wait}\langle r \rangle \triangleq r \triangleright r$$

$$\text{fail} \quad \text{fail}\langle r \rangle \triangleq r \triangleright \emptyset$$

## BellKAT primitives – basic actions

swap	$\text{sw}\langle A \sim B @ C \rangle \triangleq \{\{A \sim C, B \sim C\} \triangleright \{A \sim B\}$
transmit	$\text{tr}\langle A \rightarrow B \sim C \rangle \triangleq \{\{A \sim A\} \triangleright \{B \sim C\}$
create	$\text{cr}\langle A \rangle \triangleq \emptyset \triangleright \{A \sim A\}$
wait	$\text{wait}\langle r \rangle \triangleq r \triangleright r$
fail	$\text{fail}\langle r \rangle \triangleq r \triangleright \emptyset$

## BellKAT primitives – basic actions

swap	$\text{sw}\langle A \sim B @ C \rangle \triangleq \{\{A \sim C, B \sim C\} \triangleright \{A \sim B\}$
transmit	$\text{tr}\langle A \rightarrow B \sim C \rangle \triangleq \{\{A \sim A\} \triangleright \{B \sim C\}$
create	$\text{cr}\langle A \rangle \triangleq \emptyset \triangleright \{A \sim A\}$
wait	$\text{wait}\langle r \rangle \triangleq r \triangleright r$
fail	$\text{fail}\langle r \rangle \triangleq r \triangleright \emptyset$

# BellKAT syntax

## BellKAT syntax

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p; q \mid p^*$$

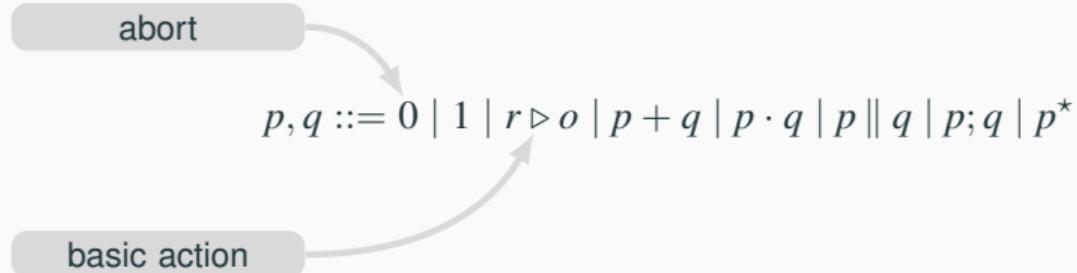
# BellKAT syntax

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p; q \mid p^*$$

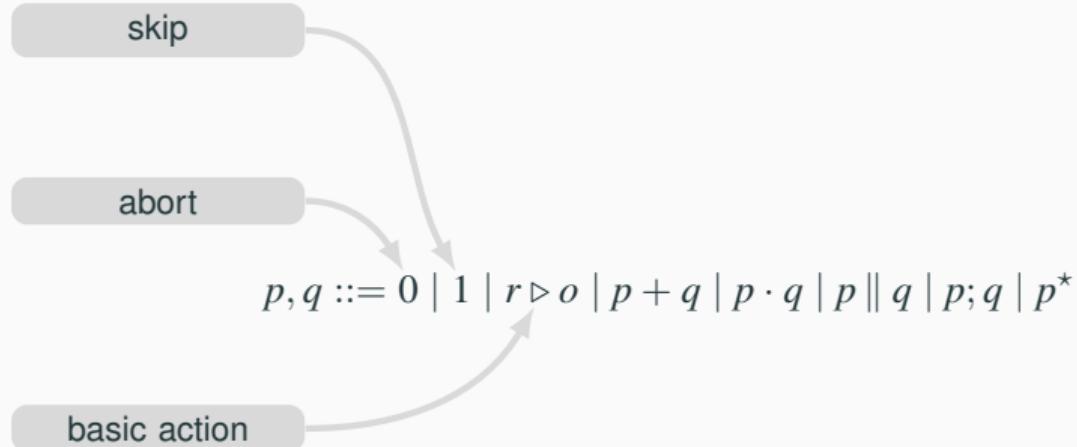
basic action



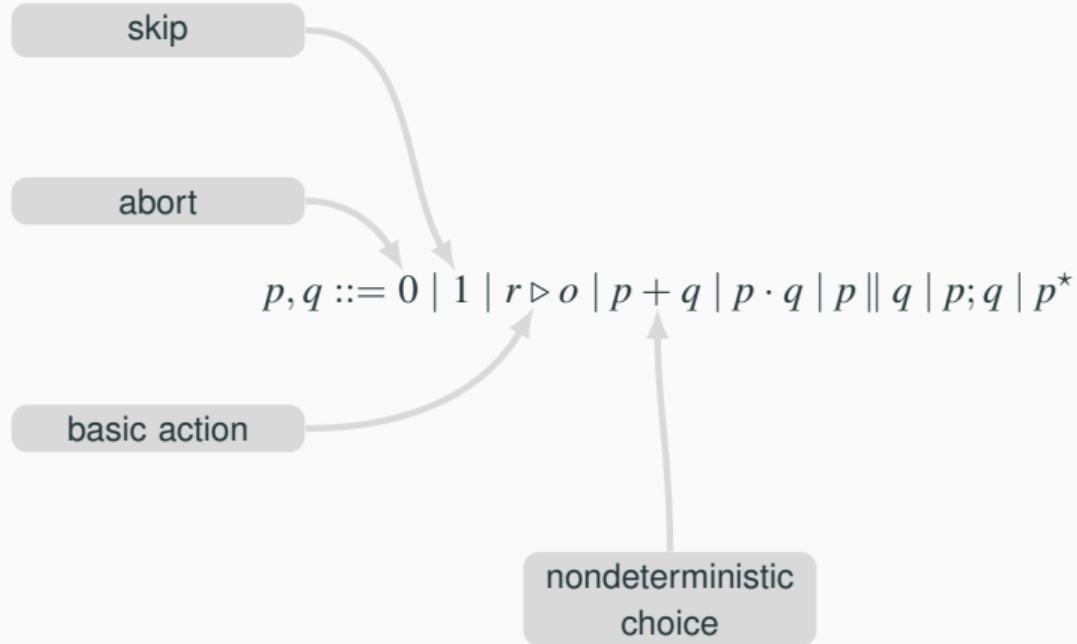
# BellKAT syntax



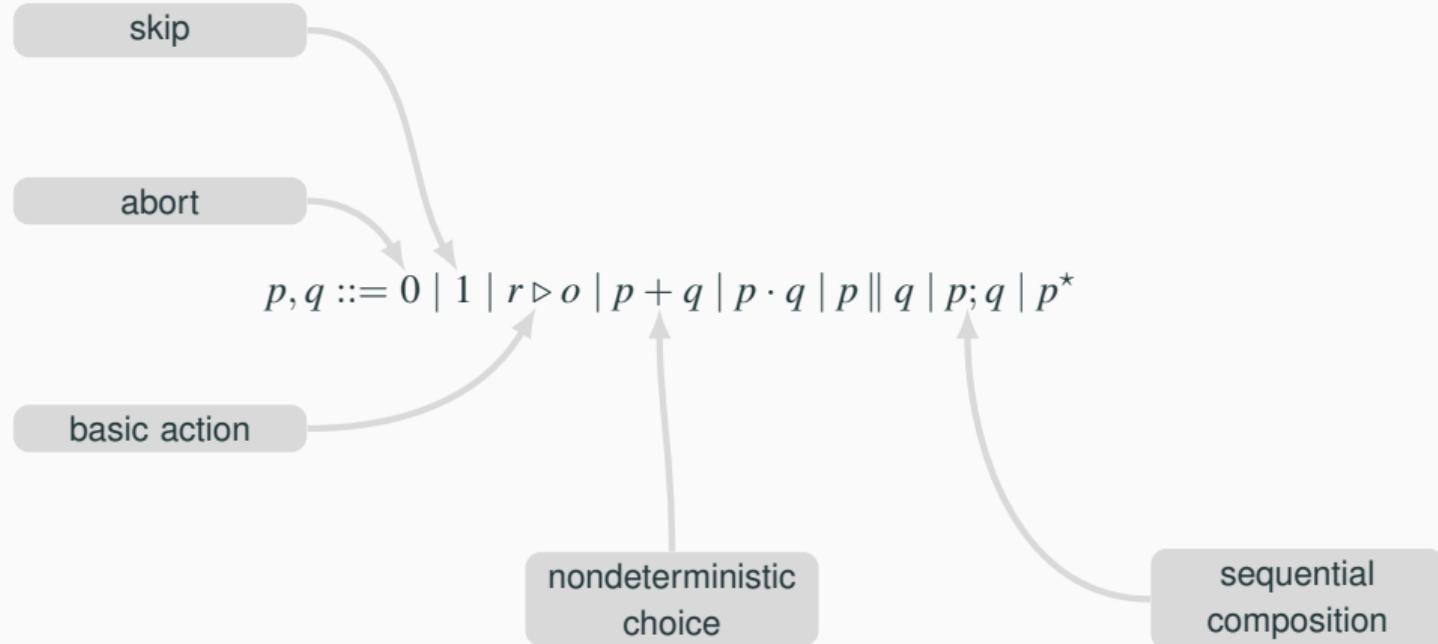
# BellKAT syntax



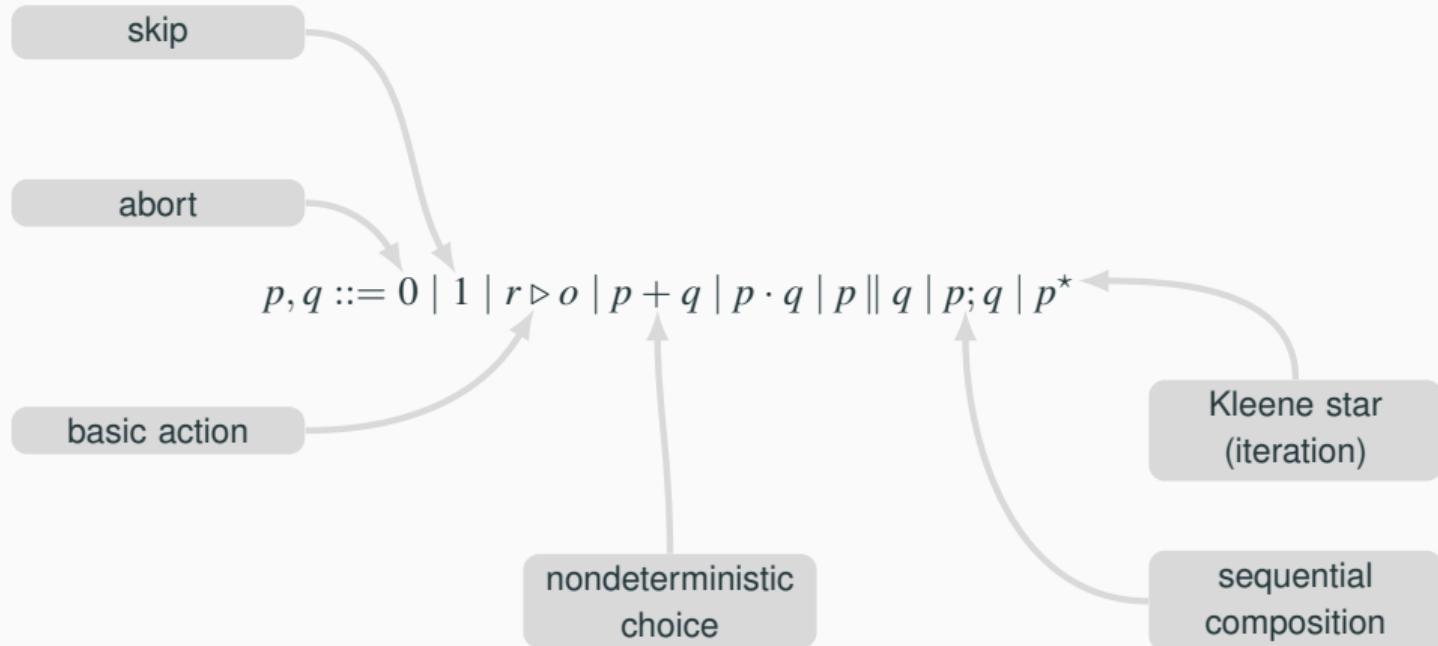
# BellKAT syntax



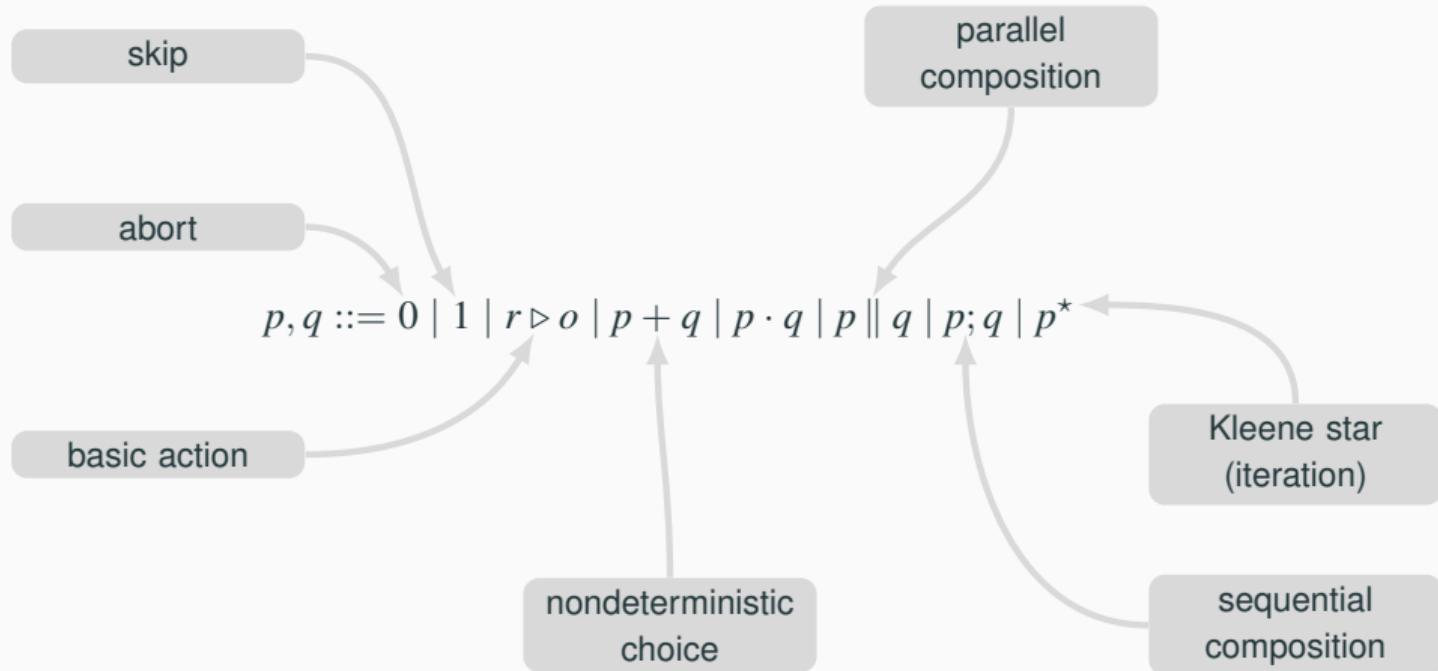
# BellKAT syntax



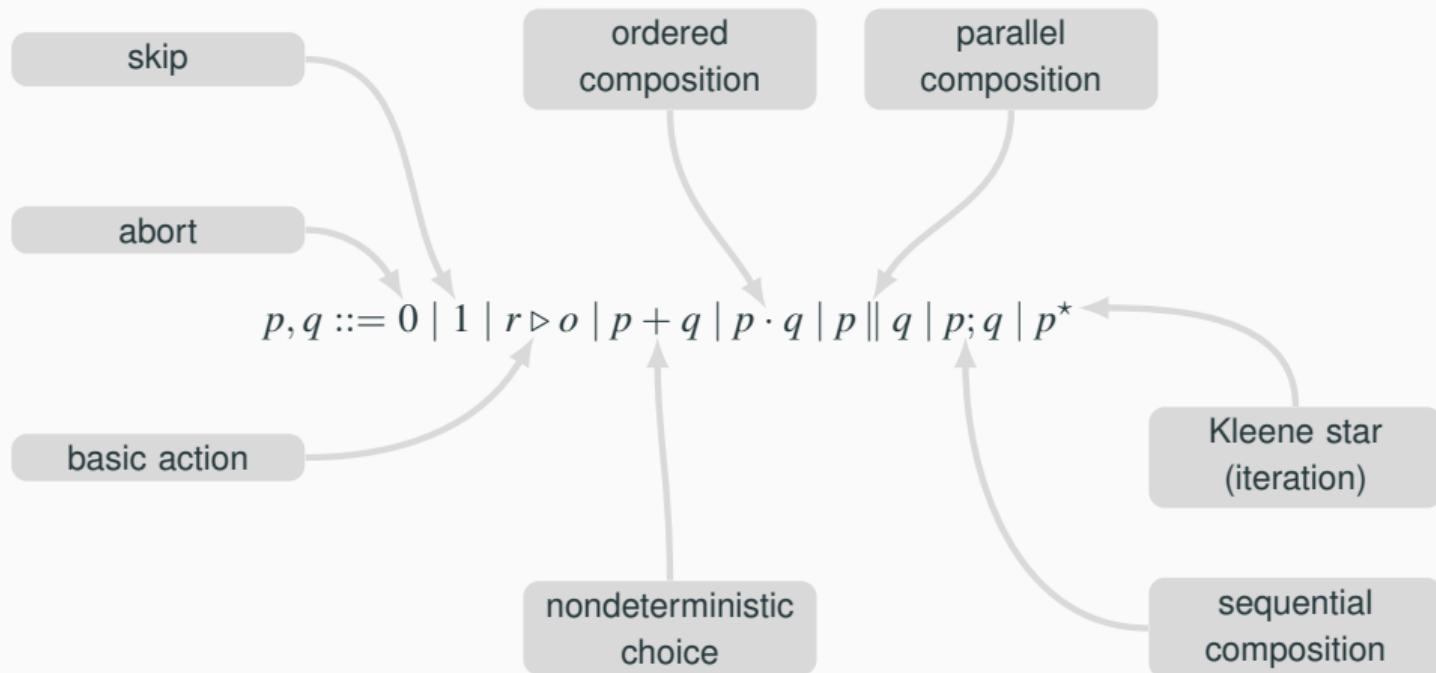
# BellKAT syntax



# BellKAT syntax

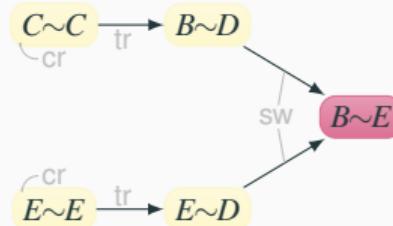
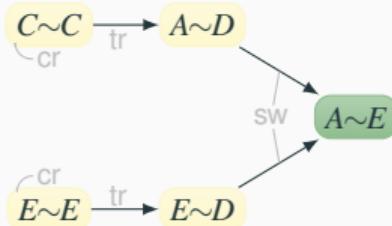


# BellKAT syntax



# Protocol specification in BellKAT

# Protocol specification in BellKAT



# Protocol specification in BellKAT



$(\text{cr}\langle C \rangle \parallel \text{cr}\langle C \rangle \parallel \text{cr}\langle E \rangle \parallel \text{cr}\langle E \rangle);$

$(\text{tr}\langle C \rightarrow A \sim D \rangle \parallel \text{tr}\langle C \rightarrow B \sim D \rangle \parallel \text{tr}\langle E \rightarrow E \sim D \rangle \parallel \text{tr}\langle E \rightarrow E \sim D \rangle);$

$(\text{sw}\langle A \sim E @ D \rangle \parallel \text{sw}\langle B \sim E @ D \rangle)$

# BellKAT at a glance

# BellKAT at a glance

## Syntax

Nodes	$N ::= A, B, C, \dots$
Bell pairs	$BP \ni bp ::= N \sim N$
Multisets	$M(BP) \ni a, b, r, o ::= \{bp_1, \dots, bp_k\}$
Tests	$T \ni t, t' ::= \begin{cases} 1 & \text{no test} \\   & b \\   & t \wedge t' \\   & t \vee t' \\   & t \uplus b \end{cases} \begin{array}{l} \text{multiset absence} \\ \text{conjunction} \\ \text{disjunction} \\ \text{multiset union} \end{array}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \triangleright o$
Policies	$P \ni p, q ::= \begin{cases} 0 & \text{abort} \\   & 1 \\   & \pi \\   & r \triangleright o \\   & [t]p \\   & p + q \\   & p \cdot q \\   & p \parallel q \\   & p ; q \\   & p^* \end{cases} \begin{array}{l} \text{skip or no-round} \\ \text{atomic action} \\ \text{basic action} \\ \text{guarded policy} \\ \text{nondeterministic choice} \\ \text{ordered composition} \\ \text{parallel composition} \\ \text{sequential composition} \\ \text{Kleene star} \end{array}$
Basic actions	$r \triangleright o ::= [1]r \triangleright o + [r]\emptyset \triangleright \emptyset$
Guarded policy	$[t]p ::= [t]\emptyset \triangleright \emptyset \cdot p$

## Test semantics

$$\begin{aligned} \langle t \rangle &\in M(BP) \rightarrow \{\top, \perp\} \\ \langle 1 \rangle a &\triangleq \top & \langle t \uplus b \rangle a &\triangleq (\langle t \rangle a \setminus b \wedge b \subseteq a) \vee \langle b \rangle a \\ \langle b \rangle a &\triangleq b \not\subseteq a & \langle t \square t' \rangle a &\triangleq \langle t \rangle a \square \langle t' \rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee \end{aligned}$$

## Single round semantics

$$\begin{aligned} \langle p \rangle &\in M(BP) \rightarrow \mathcal{P}(M(BP) \times M(BP)) \\ \langle \emptyset \rangle a &\triangleq \emptyset \\ \langle 1 \rangle a &\triangleq \{\emptyset \bowtie a\} \\ \langle [t]r \triangleright o \rangle a &\triangleq \begin{cases} \{o \bowtie a \mid r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\ \langle p + q \rangle a &\triangleq \langle (p) \rangle a \cup \langle (q) \rangle a \\ \langle p \cdot q \rangle a &\triangleq \langle (p) \cdot \langle (q) \rangle \rangle a \\ \langle p \parallel q \rangle a &\triangleq \langle (p) \parallel \langle (q) \rangle \rangle a \end{aligned}$$

## Multi-round semantics

$$\begin{aligned} \llbracket p \rrbracket &\in M(BP) \rightarrow \mathcal{P}(M(BP)) \\ \llbracket \omega \rrbracket_a &\in M(BP) \rightarrow \mathcal{P}(M(BP)), \text{ where } \omega = \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k \\ \llbracket \omega \rrbracket_a &\triangleq \bigcup_{a \in I(p)} \llbracket \omega \rrbracket_a \\ \llbracket e \rrbracket_a &\triangleq \{a\} \\ \llbracket [t]r \triangleright o \rrbracket_a &\triangleq \begin{cases} \{o \bowtie a \mid r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\ \llbracket \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k \rrbracket_a &\triangleq \langle \llbracket \pi_1 \rrbracket_a \bullet \llbracket \pi_2 \rrbracket_a \ddagger \dots \ddagger \llbracket \pi_k \rrbracket_a \rangle_a \end{aligned}$$

## KA axioms

$$\begin{array}{llll} (p + q) + r \equiv p + (q + r) & \text{KA-PLUS-ASSOC} & p ; 1 \equiv p & \text{KA-SEQ-ONE} \\ p + q \equiv q + p & \text{KA-PLUS-COMM} & 1 ; p \equiv p & \text{KA-ONE-SEQ} \\ p + 0 \equiv p & \text{KA-PLUS-ZERO} & 0 ; p \equiv 0 & \text{KA-ZERO-SEQ} \\ p + p \equiv p & \text{KA-PLUS-IDEM} & p ; 0 \equiv 0 & \text{KA-SEQ-ZERO} \\ (p ; q) ; r \equiv p ; (q ; r) & \text{KA-SEQ-ASSOC} & 1 + p ; p^* \equiv p^* & \text{KA-UNROLL-L} \\ p ; (q + r) \equiv p ; q + p ; r & \text{KA-SEQ-DIST-L} & p ; r \leq r \Rightarrow p^* ; r \leq r & \text{KA-LFP-L} \\ (p + q) ; r \equiv p ; r + q ; r & \text{KA-SEQ-DIST-R} & 1 + p^* ; p \equiv p^* & \text{KA-UNROLL-R} \\ & & r ; p \leq r \Rightarrow r ; p^* \leq r & \text{KA-LFP-R} \end{array}$$

## SKA axioms for ||

$$\begin{array}{llll} (p \parallel q) \parallel r \equiv p \parallel (q \parallel r) & \text{SKA-PRL-ASSOC} & p \parallel q \equiv q \parallel p & \text{SKA-PRL-COMM} \\ p \parallel (q + r) \equiv p \parallel q + p \parallel r & \text{SKA-PRL-DIST} & 1 \parallel p \equiv p & \text{SKA-ONE-PRL} \\ (x : p) \parallel (y : q) \equiv (x \parallel y) : (p \parallel q) & \text{SKA-PRL-SEQ} & 0 \parallel p \equiv 0 & \text{SKA-ZERO-PRL} \end{array}$$

## SKA axioms for ·

$$\begin{array}{llll} (p \cdot q) \cdot r \equiv p \cdot (q \cdot r) & \text{SKA-ORD-ASSOC} & 1 \cdot p \equiv p & \text{SKA-ONE-ORD} \\ p \cdot (q + r) \equiv p \cdot q + p \cdot r & \text{SKA-ORD-DIST-L} & p \cdot 1 \equiv p & \text{SKA-ORD-ONE} \\ (p + q) \cdot r \equiv p \cdot r + q \cdot r & \text{SKA-ORD-DIST-R} & 0 \cdot p \equiv 0 & \text{SKA-ZERO-ORD} \\ (x : p) \cdot (y : q) \equiv (x \cdot y) : (p \cdot q) & \text{SKA-ORD-SEQ} & p \cdot 0 \equiv 0 & \text{SKA-ORD-ZERO} \end{array}$$

## Boolean axioms (in addition to monotone axioms)

$$\begin{array}{llll} 1 \sqcup b = 1 & \text{BOOL-ONE-U} & (t \wedge t') \sqcup b = t \uplus b \wedge t' \uplus b & \text{BOOL-CONJ-U-DIST} \\ b \wedge (b \wedge b') \equiv b & \text{BOOL-CONJ-SUBSET} & (t \vee t') \sqcup b = t \uplus b \vee t' \uplus b & \text{BOOL-DISJ-U-DIST} \\ b \vee b' \equiv b \uplus b' & \text{BOOL-DISJ-U} & & \end{array}$$

## Network axioms

$$\begin{array}{llll} [t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' & \text{NET-ORD} \\ [t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' & \text{NET-PRL} \end{array}$$

## Single round axioms

$$\begin{array}{llll} \langle p \parallel p' \rangle \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q') & \text{SR-EXC} \\ \langle b \wedge t \rangle r \triangleright o \equiv \langle (r \cup b) \wedge t \rangle r \triangleright o & \text{SR-CAN} \\ \langle \emptyset \rangle r \triangleright o \equiv 0 & \text{SR-ZERO} \\ \llbracket t \rrbracket r \triangleright o + \llbracket t' \rrbracket r \triangleright o \equiv \llbracket t \vee t' \rrbracket r \triangleright o & \text{SR-PLUS} \end{array}$$

# BellKAT at a glance

## Syntax

Nodes	$N ::= A, B, C, \dots$
Bell pairs	$BP \ni bp ::= N\text{-}N$
Multisets	$M(BP) \ni a, b, r, o ::= \{bp_1, \dots, bp_k\}$
Tests	$T \ni t, t' ::= \begin{cases} 1 & \text{no test} \\   & \text{multiset absence} \\   & t \wedge t' \\   & t \vee t' \\   & t \uplus b \\   & t \otimes b \end{cases}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \triangleright o$
Policies	$P \ni p, q ::= \begin{cases} 0 & \text{abort} \\   & 1 \\   & \pi \\   & r \triangleright o \\   & [t]p \\   & p + q \\   & p \cdot q \\   & p \parallel q \\   & p ; q \\   & p^* \end{cases}$
Basic actions	$r \triangleright o ::= [1]r \triangleright o + [r]\emptyset \triangleright \emptyset$
Guarded policy	$[t]p ::= [t]\emptyset \triangleright \emptyset \cdot p$

## Test semantics

$$\begin{array}{ll} \langle t \rangle \in M(BP) \rightarrow \{\top, \perp\} & \\ \langle 1 \rangle a \triangleq \top & \langle t \uplus b \rangle a \triangleq (\langle t \rangle a \setminus b \wedge b \subseteq a) \vee \langle b \rangle a \\ \langle b \rangle a \triangleq b \not\subseteq a & \langle t \square t' \rangle a \triangleq \langle t \rangle a \square \langle t' \rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee \end{array}$$

## Single round semantics

$$\begin{array}{ll} \langle p \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP) \times M(BP)) & \\ \langle \emptyset \rangle a \triangleq \emptyset & \\ \langle 1 \rangle a \triangleq \{ \emptyset \mapsto a \} & \\ \langle [t]r \triangleright o \rangle a \triangleq \begin{cases} \{ o \mapsto a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} & \\ \langle p + q \rangle a \triangleq \langle p \rangle a \cup \langle q \rangle a & \\ \langle p \cdot q \rangle a \triangleq \langle (p) \cdot (q) \rangle a & \\ \langle p \parallel q \rangle a \triangleq \langle (p) \parallel (q) \rangle a & \end{array}$$

## Multi-round semantics

$$\begin{array}{ll} \llbracket p \rrbracket \in M(BP) \rightarrow \mathcal{P}(M(BP)) & \\ \llbracket \omega \rrbracket_I \in M(BP) \rightarrow \mathcal{P}(M(BP)), \text{ where } \omega = \pi_1 \circ \pi_2 \circ \dots \circ \pi_k & \\ \llbracket p \rrbracket a \triangleq \bigcup_{o \in I(p)} \llbracket \omega \rrbracket_I a & \\ \llbracket \epsilon \rrbracket_I a \triangleq \{ a \} & \\ \llbracket [t]r \triangleright o \rrbracket a \triangleq \begin{cases} \{ o \uplus a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} & \\ \llbracket \pi_1 \circ \pi_2 \circ \dots \circ \pi_k \rrbracket_I a \triangleq (\llbracket \pi_1 \rrbracket_I \bullet \llbracket \pi_2 \circ \dots \circ \pi_k \rrbracket_I) a & \end{array}$$

## KA axioms

$$\begin{array}{llll} (p + q) + r \equiv p + (q + r) & \text{KA-PLUS-ASSOC} & p ; 1 \equiv p & \text{KA-SEQ-ONE} \\ p + q \equiv q + p & \text{KA-PLUS-COMM} & 1 ; p \equiv p & \text{KA-ONE-SEQ} \\ p + 0 \equiv p & \text{KA-PLUS-ZERO} & 0 ; p \equiv 0 & \text{KA-ZERO-SEQ} \\ p + p \equiv p & \text{KA-PLUS-IDEM} & p ; 0 \equiv 0 & \text{KA-SEQ-ZERO} \\ (p ; q) ; r \equiv p ; (q ; r) & \text{KA-SEQ-ASSOC} & 1 + p ; p^* \equiv p^* & \text{KA-UNROLL-L} \\ p ; (q + r) \equiv p ; q + p ; r & \text{KA-SEQ-DIST-L} & p ; r \leq r \Rightarrow p^* ; r \leq r & \text{KA-LFP-L} \\ (p + q) ; r \equiv p ; r + q ; r & \text{KA-SEQ-DIST-R} & 1 + p^* ; p \equiv p^* & \text{KA-UNROLL-R} \\ & & r ; p \leq r \Rightarrow r ; p^* \leq r & \text{KA-LFP-R} \end{array}$$

## SKA axioms for ||

$$\begin{array}{llll} (p \parallel q) \parallel r \equiv p \parallel (q \parallel r) & \text{SKA-PRL-ASSOC} & p \parallel q \equiv q \parallel p & \text{SKA-PRL-COMM} \\ p \parallel (q + r) \equiv p \parallel q + p \parallel r & \text{SKA-PRL-DIST} & 1 \parallel p \equiv p & \text{SKA-ONE-PRL} \\ (x ; p) \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q) & \text{SKA-PRL-SEQ} & 0 \parallel p \equiv 0 & \text{SKA-ZERO-PRL} \end{array}$$

## SKA axioms for ·

$$\begin{array}{llll} (p \cdot q) \cdot r \equiv p \cdot (q \cdot r) & \text{SKA-ORD-ASSOC} & 1 \cdot p \equiv p & \text{SKA-ONE-ORD} \\ p \cdot (q + r) \equiv p \cdot q + p \cdot r & \text{SKA-ORD-DIST-L} & p \cdot 1 \equiv p & \text{SKA-ORD-ONE} \\ (p + q) \cdot r \equiv p \cdot r + q \cdot r & \text{SKA-ORD-DIST-R} & 0 \cdot p \equiv 0 & \text{SKA-ZERO-ORD} \\ (x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q) & \text{SKA-ORD-SEQ} & p \cdot 0 \equiv 0 & \text{SKA-ORD-ZERO} \end{array}$$

## Boolean axioms (in addition to monotone axioms)

$$\begin{array}{llll} 1 \uplus b \equiv 1 & \text{BOOL-ONE-U} & (t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b & \text{BOOL-CONJ-U-DIST} \\ b \wedge (b \wedge b') \equiv b & \text{BOOL-CONJ-SUBSET} & (t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b & \text{BOOL-DISJ-U-DIST} \\ b \vee b' \equiv b \cup b' & \text{BOOL-DISJ-U} & & \end{array}$$

## Network axioms

$$\begin{array}{llll} [t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \wedge r)] \hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' & \text{NET-ORD} \\ [t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)] \hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' & \text{NET-PRL} \end{array}$$

## Single round axioms

$$\begin{array}{llll} \llbracket p \rrbracket \parallel \emptyset \equiv 1 & \text{SR-ONE} & (p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q') & \text{SR-EXC} \\ \llbracket \emptyset \rrbracket r \triangleright o \equiv 0 & \text{SR-ZERO} & [b \wedge t]r \triangleright o \equiv [(r \cup b) \wedge t]r \triangleright o & \text{SR-CAN} \\ \llbracket t \rrbracket r \triangleright o \parallel [t']r \triangleright o \equiv [t \vee t']r \triangleright o & & [t]r \triangleright o + [t']r \triangleright o \equiv [t \vee t']r \triangleright o & \text{SR-PLUS} \end{array}$$

# BellKAT at a glance

## Syntax

Nodes	$N ::= A, B, C, \dots$
Bell pairs	$BP \ni bp ::= N\text{-}N$
Multisets	$M(BP) \ni a, b, r, o ::= \{bp_1, \dots, bp_k\}$
Tests	$T \ni t, t' ::= \begin{cases} 1 & \text{no test} \\   & \\ b & \text{multiset absence} \\   & \\ t \wedge t' & \text{conjunction} \\   & \\ t \vee t' & \text{disjunction} \\   & \\ t \uplus b & \text{multiset union} \end{cases}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \triangleright o$
Policies	$P \ni p, q ::= \begin{cases} 0 & \text{abort} \\   & \\ 1 & \text{skip or no-round} \\   & \\ \pi & \text{atomic action} \\   & \\ r \triangleright o & \text{basic action} \\   & \\ [t]p & \text{guarded policy} \\   & \\ p + q & \text{nondeterministic choice} \\   & \\ p \cdot q & \text{ordered composition} \\   & \\ p \parallel q & \text{parallel composition} \\   & \\ p ; q & \text{sequential composition} \\   & \\ p^* & \text{Kleene star} \end{cases}$
Basic actions	$r \triangleright o ::= [1]r \triangleright o + [r]\emptyset \triangleright \emptyset$
Guarded policy	$[t]p ::= [t]\emptyset \triangleright \emptyset \cdot p$

## Test semantics

$$\begin{array}{ll} \langle t \rangle \in M(BP) \rightarrow \{\top, \perp\} & \\ \langle 1 \rangle a \triangleq \top & \langle t \uplus b \rangle a \triangleq (\langle t \rangle a \wedge b \wedge b \subseteq a) \vee \langle b \rangle a \\ \langle b \rangle a \triangleq b \not\subseteq a & \langle t \square t' \rangle a \triangleq \langle t \rangle a \Box \langle t' \rangle a, \text{ where } \Box \text{ is either } \wedge \text{ or } \vee \end{array}$$

## Single round semantics

$$\begin{array}{ll} \langle p \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP) \times M(BP)) & \\ \langle \emptyset \rangle a \triangleq \emptyset & \\ \langle 1 \rangle a \triangleq \{\emptyset \triangleright a\} & \\ \langle [t]r \triangleright o \rangle a \triangleq \begin{cases} \{o \triangleright a \mid r\} & \text{if } r \subseteq a \\ \emptyset & \text{otherwise} \end{cases} & \\ \langle p + q \rangle a \triangleq \langle p \rangle a \cup \langle q \rangle a & \\ \langle p \cdot q \rangle a \triangleq \langle (p) \cdot (q) \rangle a & \\ \langle p \parallel q \rangle a \triangleq \langle (p) \parallel (q) \rangle a & \end{array}$$

## Multi-round semantics

$$\begin{array}{ll} \langle p \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP)) & \\ \langle \omega \rangle_I \in M(BP) \rightarrow \mathcal{P}(M(BP)), \text{ where } \omega = \pi_1 \circ \pi_2 \circ \dots \circ \pi_k & \\ \langle p \rangle a \triangleq \bigcup_{\omega \in I(p)} \langle \omega \rangle_I a & \\ \langle \epsilon \rangle a \triangleq \{a\} & \\ \langle [t]r \triangleright o \rangle a \triangleq \begin{cases} \{o \triangleright a \mid r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} & \\ \langle \pi_1 \circ \pi_2 \circ \dots \circ \pi_k \rangle_I a \triangleq \langle \langle \pi_1 \rangle_I \bullet \langle \pi_2 \rangle_I \circ \dots \circ \langle \pi_k \rangle_I \rangle_I a & \end{array}$$

## KA axioms

$$\begin{array}{llll} (p + q) + r \equiv p + (q + r) & \text{KA-Plus-Assoc} & p ; 1 \equiv p & \text{KA-SEQ-ONE} \\ p + q \equiv q + p & \text{KA-Plus-Comm} & 1 ; p \equiv p & \text{KA-ONE-SEQ} \\ p + 0 \equiv p & \text{KA-Plus-Zero} & 0 ; p \equiv 0 & \text{KA-ZERO-SEQ} \\ p + p \equiv p & \text{KA-Plus-IDEM} & p ; 0 \equiv 0 & \text{KA-SEQ-ZERO} \\ (p ; q) ; r \equiv p ; (q ; r) & \text{KA-SEQ-ASSOC} & 1 + p ; p^* \equiv p^* & \text{KA-UNROLL-L} \\ p ; (q + r) \equiv p ; q + p ; r & \text{KA-SEQ-DIST-L} & p ; r \leq r \Rightarrow p^* ; r \leq r & \text{KA-LFP-L} \\ (p + q) ; r \equiv p ; r + q ; r & \text{KA-SEQ-DIST-R} & 1 + p^* ; p \equiv p^* & \text{KA-UNROLL-R} \\ & & r ; p \leq r \Rightarrow r ; p^* \leq r & \text{KA-LFP-R} \end{array}$$

## SKA axioms for ||

$$\begin{array}{llll} (p \parallel q) \parallel r \equiv p \parallel (q \parallel r) & \text{SKA-PRL-ASSOC} & p \parallel q \equiv q \parallel p & \text{SKA-PRL-COMM} \\ p \parallel (q + r) \equiv p \parallel q + p \parallel r & \text{SKA-PRL-DIST} & 1 \parallel p \equiv p & \text{SKA-ONE-PRL} \\ (x ; p) \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q) & \text{SKA-PRL-SEQ} & 0 \parallel p \equiv 0 & \text{SKA-ZERO-PRL} \end{array}$$

## SKA axioms for ·

$$\begin{array}{llll} (p \cdot q) \cdot r \equiv p \cdot (q \cdot r) & \text{SKA-ORD-ASSOC} & 1 \cdot p \equiv p & \text{SKA-ONE-ORD} \\ p \cdot (q + r) \equiv p \cdot q + p \cdot r & \text{SKA-ORD-DIST-L} & p \cdot 1 \equiv p & \text{SKA-ORD-ONE} \\ (p + q) \cdot r \equiv p \cdot r + q \cdot r & \text{SKA-ORD-DIST-R} & 0 \cdot p \equiv 0 & \text{SKA-ZERO-ORD} \\ (x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q) & \text{SKA-ORD-SEQ} & p \cdot 0 \equiv 0 & \text{SKA-ORD-ZERO} \end{array}$$

## Boolean axioms (in addition to monotone axioms)

$$1 \uplus b \equiv 1 \quad \text{BOOL-ONE-U} \quad (t \wedge t') \uplus b = t \uplus b \wedge t' \uplus b, \text{ BOOL-COMM-U-DIST}$$

$$r \triangleright o ::= [1]r \triangleright o + [r]\emptyset \triangleright \emptyset \quad \begin{array}{ll} \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' & \text{NET-ORD} \\ [t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \uplus t') \wedge (t' \uplus t)]\hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' \end{array} \quad \text{NET-PRL}$$

## Single round axioms

$$\begin{array}{llll} [1]r \triangleright \emptyset \equiv 1 & \text{SR-ONE} & (p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q') & \text{SR-EXC} \\ [\emptyset]r \triangleright o \equiv 0 & \text{SR-ZERO} & [b \wedge t]r \triangleright o \equiv [(r \cup b) \wedge t]r \triangleright o & \text{SR-CAN} \\ [t]r \triangleright o + [t']r' \triangleright o' \equiv [t \vee t']r \triangleright o & & [t]r \triangleright o + [t']r \triangleright o \equiv [t \vee t']r \triangleright o & \text{SR-PLUS} \end{array}$$

## Basic actions

# BellKAT at a glance

Syntax	
Nodes	$N ::= A, B, C, \dots$
Bell pairs	$BP \ni bp ::= N\text{-}N$
Multisets	$M(BP) \ni a, b, r, o ::= \{\{bp_1, \dots, bp_k\}\}$
Tests	$T \ni t, t' ::= \begin{cases} 1 & \text{no test} \\ b & \text{multiset absence} \\ t \wedge t' & \text{conjunction} \\ t \vee t' & \text{disjunction} \\ t \uplus b & \text{multiset union} \end{cases}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \blacktriangleright o$
Policies	$p \ni p, q ::= \begin{cases} 0 & \text{abort} \\ 1 & \text{skip or no-round} \\ \pi & \text{atomic action} \\ r \blacktriangleright o & \text{basic action} \\ [t]p & \text{guarded policy} \\ p + q & \text{nondeterministic choice} \\ p \cdot q & \text{ordered composition} \\ p \parallel q & \text{parallel composition} \\ p ; q & \text{sequential composition} \\ p^* & \text{Kleene star} \end{cases}$
Basic actions	$r \blacktriangleright o ::= [\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$
Guarded policy	$[t]p ::= [t]\emptyset \blacktriangleright \emptyset \cdot p$
Test semantics	$\langle t \rangle \in M(BP) \rightarrow \{\top, \perp\}$
	$\langle \mathbb{1} \rangle a \triangleq \top$
	$\langle b \rangle a \triangleq b \not\subseteq a$
	$\langle t \rangle a \triangleq \top$
	$\langle t \wedge b \rangle a \triangleq (\langle t \rangle a \wedge b \wedge b \subseteq a) \vee \langle b \rangle a$
	$\langle t \wedge t' \rangle a \triangleq \langle t \rangle a \wedge \langle t' \rangle a, \text{ where } \square \text{ is either } \wedge \text{ or } \vee$
Single round semantics	$(p) \in M(BP) \rightarrow \mathcal{P}(M(BP) \times M(BP))$
	$\langle \emptyset \rangle a \triangleq \emptyset$
	$\langle \mathbb{1} \rangle a \triangleq \{\emptyset \blacktriangleright a\}$
	$\langle [t]r \blacktriangleright o \rangle a \triangleq \begin{cases} \{o \blacktriangleright a \mid r\} & \text{if } r \subseteq a \\ \emptyset & \text{otherwise} \end{cases}$
	$\langle p + q \rangle a \triangleq \langle p \rangle a \cup \langle q \rangle a$
	$\langle p \cdot q \rangle a \triangleq (\langle p \rangle \cdot \langle q \rangle) a$
	$\langle p \parallel q \rangle a \triangleq (\langle p \rangle \parallel \langle q \rangle) a$
Multi-round semantics	$\llbracket p \rrbracket \in M(BP) \rightarrow \mathcal{P}(M(BP))$
	$\llbracket \omega \rrbracket_I \in M(BP) \rightarrow \mathcal{P}(M(BP)), \text{ where } \omega = \pi_1 \ddot{\wedge} \pi_2 \ddot{\wedge} \dots \ddot{\wedge} \pi_k$
	$\llbracket p \rrbracket a \triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a$
	$\llbracket \epsilon \rrbracket a \triangleq \{a\}$
	$\llbracket [t]r \blacktriangleright o \rrbracket a \triangleq \begin{cases} \{o \blacktriangleright a \mid r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$
	$\llbracket \pi_1 \ddot{\wedge} \pi_2 \ddot{\wedge} \dots \ddot{\wedge} \pi_k \rrbracket_I a \triangleq (\llbracket \pi_1 \rrbracket_I \bullet \llbracket \pi_2 \rrbracket_I \ddot{\wedge} \dots \ddot{\wedge} \llbracket \pi_k \rrbracket_I) a$

Atomic actions

$\Pi \ni \pi, x, y ::= [t]r \blacktriangleright o$

( $x ; p \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q)$ ) SKA-PRL-SEQ

$0 \parallel p \equiv 0$  SKA-ZERO-PRL

SKA axioms for  $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$  SKA-ORD-ASSOC

$1 \cdot p \equiv p$  SKA-ONE-ORD

$p \cdot (q + r) \equiv p \cdot q + p \cdot r$  SKA-ORD-DIST-L

$p \cdot 1 \equiv p$  SKA-ORD-ONE

$(p + q) \cdot r \equiv p \cdot r + q \cdot r$  SKA-ORD-DIST-R

$0 \cdot p \equiv 0$  SKA-ZERO-ORD

$(x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q)$  SKA-ORD-SIQ

$p \cdot 0 \equiv 0$  SKA-ORD-ZERO

Boolean axioms (in addition to monotone axioms)

$1 \uplus b \equiv 1$  BOOL-ONE-U

$(t \wedge t') \uplus b = t \uplus b \wedge t' \uplus b$ , BOOL-COMM-U-DIST

Basic actions

$r \blacktriangleright o ::= [\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$

INCLUSIVE AXIOMS

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \wedge r)]\hat{r} \blacktriangleright \hat{o}$  if  $\hat{r} = r \uplus r'$  and  $\hat{o} = o \uplus o'$  NET-ORD

$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$  if  $\hat{r} = r \uplus r'$  and  $\hat{o} = o \uplus o'$  NET-PRL

Single round axioms

$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$  SR-EXC

$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$  SR-CAN

$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$  SR-PLUS

# BellKAT at a glance

Syntax	
Nodes	$N ::= A, B, C, \dots$
Bell pairs	$BP \ni bp ::= N\text{-}N$
Multisets	$M(BP) \ni a, b, r, o ::= \{\{bp_1, \dots, bp_k\}\}$
Tests	$T \ni t, t' ::= \begin{cases} 1 & \text{no test} \\ b & \text{multiset absence} \\ t \wedge t' & \text{conjunction} \\ t \vee t' & \text{disjunction} \\ t \uplus b & \text{multiset union} \end{cases}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \blacktriangleright o$
Policies	$p \ni p, q ::= \begin{cases} 0 & \text{abort} \\ 1 & \text{skip or no-round} \\ \pi & \text{atomic action} \\ r \blacktriangleright o & \text{basic action} \\ [t]p & \text{guarded policy} \\ p + q & \text{nondeterministic choice} \\ p \cdot q & \text{ordered composition} \\ p \parallel q & \text{parallel composition} \\ p ; q & \text{sequential composition} \\ p^* & \text{Kleene star} \end{cases}$
Basic actions	$r \blacktriangleright o ::= [\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$
Guarded policy	$[t]p ::= [t]\emptyset \blacktriangleright \emptyset \cdot p$
Test semantics	$\langle t \rangle \in M(BP) \rightarrow \{\top, \perp\}$
	$\langle \mathbb{1} \rangle a \triangleq \top$
	$\langle \mathbb{1} \rangle a \triangleq b \not\subseteq a$
	$\langle \mathbb{1} \rangle a \triangleq \emptyset$
	$\langle \mathbb{1} \rangle a \triangleq \{\emptyset \bowtie a\}$
	$\langle \mathbb{1} \rangle a \triangleq \begin{cases} \{o \bowtie a \mid r\} & \text{if } r \subseteq a \\ \emptyset & \text{otherwise} \end{cases}$
	$\langle t \wedge t' \rangle a \triangleq \langle t \rangle a \wedge \langle t' \rangle a$
	$\langle t \vee t' \rangle a \triangleq \langle t \rangle a \vee \langle t' \rangle a$
	$\langle t \parallel t' \rangle a \triangleq \langle t \rangle a \parallel \langle t' \rangle a$
	$\langle t \cdot t' \rangle a \triangleq \langle t \rangle a \cdot \langle t' \rangle a$
	$\langle t + t' \rangle a \triangleq \langle t \rangle a + \langle t' \rangle a$
	$\langle t ; t' \rangle a \triangleq \langle t \rangle a ; \langle t' \rangle a$
	$\langle t^* \rangle a \triangleq \langle t \rangle a \cdot \langle t^* \rangle a$

## KA axioms

$(p + q) + r \equiv p + (q + r)$	KA-PLUS-ASSOC	$p ; 1 \equiv p$	KA-SEQ-ONE
$p + q \equiv q + p$	KA-PLUS-COMM	$1 ; p \equiv p$	KA-ONE-SEQ
$p + 0 \equiv p$	KA-PLUS-ZERO	$0 ; p \equiv 0$	KA-ZERO-SEQ
$p + p \equiv p$	KA-PLUS-IDEM	$p ; 0 \equiv 0$	KA-SEQ-ZERO
$(p + q) \cdot r \equiv p ; (q ; r)$	KA-SEQ-ASSOC	$1 + p ; p^* \equiv p^*$	KA-UNROLL-L
$p ;$	Tests	$T \ni t, t'$	A-LFP-L
$(p ;$		$r ; p \Rightarrow r \Rightarrow r ; p^* \leq r$	INROLL-R
			KA-LFP-R

## Atomic actions

$$\Pi \ni \pi, x, y ::= [t]r \blacktriangleright o$$

$$(x ; p) \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q) \quad \text{SKA-PRL-SEQ} \quad 0 \parallel p \equiv 0 \quad \text{SKA-ZERO-PRL}$$

## SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-ORD-ASSOC	$1 \cdot p \equiv p$	SKA-ONE-ORD
$p \cdot (q + r) \equiv p \cdot q + p \cdot r$	SKA-ORD-DIST-L	$p \cdot 1 \equiv p$	SKA-ORD-ONE
$(p + q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-ORD-DIST-R	$0 \cdot p \equiv 0$	SKA-ZERO-ORD
$(x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q)$	SKA-ORD-SEQ	$p \cdot 0 \equiv 0$	SKA-ORD-ZERO

## Boolean axioms (in addition to monotone axioms)

$$1 \uplus b \equiv 1 \quad \text{BOOL-ONE-U}$$

$(t \wedge t') \cdot a = t \cdot a \wedge t' \cdot a$ ,  $(t \vee t') \cdot a = t \cdot a \vee t' \cdot a$ ,  $t \parallel a = t \cdot a + t' \cdot a$

## Basic actions

$$r \blacktriangleright o ::= [\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$$

## IN/OUT AXIOMS

$$\begin{aligned} [t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' &\equiv [t \wedge (t' \wedge r)]\hat{r} \blacktriangleright \hat{o} && \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' && \text{NET-ORD} \\ [t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' &\equiv [(t \uplus t') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o} && \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' && \text{NET-PRL} \end{aligned}$$

## Single round axioms

$[1]p \blacktriangleright \emptyset \equiv 1$	SR-ONE	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	SR-EXC
$[\emptyset]p \blacktriangleright o \equiv 0$	SR-ZERO	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	SR-CAN
$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	SR-PLUS

# BellKAT at a glance

## Syntax

Nodes	$N ::= A, B, C, \dots$
BP pairs	$BP \ni bp ::= N \sim N$
Multisets	$M(BP) \ni a, b, r, o ::= \{bp_1, \dots, bp_k\}$
Tests	$T \ni t, t' ::= \begin{cases} \perp & \text{no test} \\   & \text{multiset absence} \\   & t \wedge t' \\   & t \vee t' \\   & t \uplus b \\   & t \uplus b \end{cases}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \triangleright o$
Policies	$p \ni p, q ::= \begin{cases} 0 & \text{abort} \\   & 1 \\   & \pi \\   & r \triangleright o \\   & [t]p \\   & p + q \\   & p \cdot q \\   & p \parallel q \\   & p : q \\   & p^* \end{cases}$
Basic actions	$r \triangleright o ::= [\perp]r \triangleright o + [r]\emptyset \triangleright \emptyset$
Guarded policy	$[t]p ::= [t]\emptyset \triangleright \emptyset \cdot p$

## Test semantics

$$\begin{array}{ll} \langle t \rangle a \in M(BP) \rightarrow \{\top, \perp\} & \\ \langle \perp \rangle a \triangleq \top & \langle t \uplus b \rangle a \triangleq (\langle t \rangle a \setminus b \wedge b \subseteq a) \vee \langle b \rangle a \\ \langle b \rangle a \triangleq b \not\subseteq a & \langle t \square t' \rangle a \triangleq \langle t \rangle a \square \langle t' \rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee \end{array}$$

## Single round semantics

$$\begin{array}{ll} \langle p \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP) \times M(BP)) & \\ \langle \perp \rangle a \triangleq \emptyset & \\ \langle 1 \rangle a \triangleq \{ \mathbf{0} \bowtie a \} & \\ \langle [t]r \triangleright o \rangle a \triangleq \begin{cases} \{ o \bowtie a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} & \\ \langle p + q \rangle a \triangleq \langle (p) \rangle a \cup \langle (q) \rangle a & \\ \langle p \cdot q \rangle a \triangleq \langle (p) \cdot \langle (q) \rangle \rangle a & \\ \langle p \parallel q \rangle a \triangleq \langle (p) \parallel \langle (q) \rangle \rangle a & \end{array}$$

## Multi-round semantics

$$\begin{array}{ll} \langle p \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP)) & \\ \langle \omega \rangle_I \in M(BP) \rightarrow \mathcal{P}(M(BP)), \text{ where } \omega = \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k & \\ \langle p \rangle a \triangleq \bigcup_{\omega \in I(p)} \langle \omega \rangle_I a & \\ \langle e \rangle a \triangleq \{ a \} & \\ \langle [t]r \triangleright o \rangle a \triangleq \begin{cases} \{ o \bowtie a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} & \\ \langle \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k \rangle a \triangleq \langle \langle \pi_1 \rangle \bullet \langle \pi_2 \ddagger \dots \ddagger \pi_k \rangle \rangle a & \end{array}$$

## KA axioms

$$\begin{array}{llll} (p + q) + r \equiv p + (q + r) & \text{KA-PLUS-ASSOC} & p ; 1 \equiv p & \text{KA-SEQ-ONE} \\ p + q \equiv q + p & \text{KA-PLUS-COMM} & 1 ; p \equiv p & \text{KA-ONE-SEQ} \\ p + 0 \equiv p & \text{KA-PLUS-ZERO} & 0 ; p \equiv 0 & \text{KA-ZERO-SEQ} \\ p + p \equiv p & \text{KA-PLUS-IDEM} & p ; 0 \equiv 0 & \text{KA-SEQ-ZERO} \\ (p ; q) ; r \equiv p ; (q ; r) & \text{KA-SEQ-ASSOC} & 1 + p ; p^* \equiv p^* & \text{KA-UNROLL-L} \\ p ; (q + r) \equiv p ; q + p ; r & \text{KA-SEQ-DIST-L} & p ; r \leq r \Rightarrow p^* ; r \leq r & \text{KA-LFP-L} \\ (p + q) ; r \equiv p ; r + q ; r & \text{KA-SEQ-DIST-R} & 1 + p^* ; p \equiv p^* & \text{KA-UNROLL-R} \\ & & r ; p \leq r \Rightarrow r ; p^* \leq r & \text{KA-LFP-R} \end{array}$$

## SKA axioms for ||

$$\begin{array}{llll} (p \parallel q) \parallel r \equiv p \parallel (q \parallel r) & \text{SKA-PRL-ASSOC} & p \parallel q \equiv q \parallel p & \text{SKA-PRL-COMM} \\ p \parallel (q + r) \equiv p \parallel q + p \parallel r & \text{SKA-PRL-DIST} & 1 \parallel p \equiv p & \text{SKA-ONE-PRL} \\ (x ; p) \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q) & \text{SKA-PRL-SEQ} & 0 \parallel p \equiv 0 & \text{SKA-ZERO-PRL} \end{array}$$

## SKA axioms for ·

$$\begin{array}{llll} (p \cdot q) \cdot r \equiv p \cdot (q \cdot r) & \text{SKA-ORD-ASSOC} & 1 \cdot p \equiv p & \text{SKA-ONE-ORD} \\ p \cdot (q + r) \equiv p \cdot q + p \cdot r & \text{SKA-ORD-DIST-L} & p \cdot 1 \equiv p & \text{SKA-ORD-ONE} \\ (p + q) \cdot r \equiv p \cdot r + q \cdot r & \text{SKA-ORD-DIST-R} & 0 \cdot p \equiv 0 & \text{SKA-ZERO-ORD} \\ (x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q) & \text{SKA-ORD-SEQ} & p \cdot 0 \equiv 0 & \text{SKA-ORD-ZERO} \end{array}$$

## Boolean axioms (in addition to monotone axioms)

$$\begin{array}{llll} 1 \wedge b \equiv 1 & \text{BOOL-ONE-U} & (t \wedge t') \wedge b \equiv t \wedge b \wedge t' \wedge b & \text{BOOL-CONJ-U-DIST} \\ b \wedge (b \wedge b') \equiv b & \text{BOOL-CONJ-SUBSET} & (t \vee t') \wedge b \equiv t \vee b \vee t' \vee b & \text{BOOL-DISJ-U-DIST} \\ b \vee b' \equiv b \cup b' & \text{BOOL-DISJ-U} & & \end{array}$$

## Network axioms

$$\begin{array}{llll} [t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \wedge r)] \hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' & \text{NET-ORD} \\ [t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)] \hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \uplus r' \text{ and } \hat{o} = o \uplus o' & \text{NET-PRL} \end{array}$$

## Single round axioms

$$\begin{array}{llll} [\perp] \emptyset \triangleright \emptyset \equiv 1 & \text{SR-ONE} & (p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q') & \text{SR-EXC} \\ [\emptyset]r \triangleright o \equiv 0 & \text{SR-ZERO} & [b \wedge t]r \triangleright o \equiv [(r \cup b) \wedge t]r \triangleright o & \text{SR-CAN} \\ [t]r \triangleright o + [t']r \triangleright o \equiv [t \vee t']r \triangleright o & & [t]r \triangleright o + [t']r \triangleright o \equiv [t \vee t']r \triangleright o & \text{SR-PLUS} \end{array}$$

# BellKAT at a glance

Syntax

Nodes	$N ::= A, B, C, \dots$			
Bell pairs	$BP \ni bp ::= N\text{-}N$			
Multisets	$\mathcal{M}(BP) \ni a, b, r, o ::= \{\!\{bp_1, \dots, bp_k\}\!\}$			
Tests	$T \ni t, t' ::= \begin{cases} 1 & \text{no test} \\ b & \text{multiset absence} \\ 1 \wedge t' & \text{conjunction} \end{cases}$			
		KA axioms		
		$(p + q) + r \equiv p + (q + r)$	KA-PLUS-ASSOC	$p ; 1 \equiv p$
		$p + q \equiv q + p$	KA-PLUS-COMM	$1 ; p \equiv p$
				KA-SEQ-ONE
				KA-ONE-SEQ

## Multi-round semantics

$$\begin{aligned} \llbracket p \rrbracket &\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP)) \\ \llbracket \omega \rrbracket_I &\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 ; \pi_2 ; \dots ; \pi_k \\ \llbracket p \rrbracket_I a &\triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a \\ \llbracket \epsilon \rrbracket_I a &\triangleq \{a\} \\ \llbracket [t]r \triangleright o \rrbracket_I a &\triangleq \begin{cases} \{o \sqcup a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \end{aligned}$$

$$\begin{array}{ll} \langle t \rangle a = \top & \langle t \rangle a \subseteq a \\ \langle b \rangle a \triangleq b \not\subseteq a & \langle t \square t' \rangle a \triangleq \langle t \rangle a \square \langle t' \rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee \end{array}$$

### Single round semantics

$$\begin{aligned} \langle p \rangle &\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP)) \\ \langle \emptyset \rangle a &\triangleq \emptyset \\ \langle 1 \rangle a &\triangleq \{\emptyset \bowtie a\} \\ \langle [t]r \triangleright o \rangle a &\triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\ \langle p + q \rangle a &\triangleq \langle p \rangle a \cup \langle q \rangle a \\ \langle p \cdot q \rangle a &\triangleq (\langle p \rangle \cdot \langle q \rangle) a \\ \langle p \parallel q \rangle a &\triangleq (\langle p \rangle \parallel \langle q \rangle) a \end{aligned}$$

### Multi-round semantics

$$\begin{aligned} \llbracket p \rrbracket &\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP)) \\ \llbracket \omega \rrbracket_I &\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 ; \pi_2 ; \dots ; \pi_k \\ \llbracket p \rrbracket_I a &\triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a \\ \llbracket \epsilon \rrbracket_I a &\triangleq \{a\} \\ \llbracket [t]r \triangleright o \rrbracket_I a &\triangleq \begin{cases} \{o \sqcup a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\ \llbracket \pi_1 ; \pi_2 ; \dots ; \pi_k \rrbracket_I a &\triangleq (\llbracket \pi_1 \rrbracket_I \bullet \llbracket \pi_2 \rrbracket_I \bullet \dots \bullet \llbracket \pi_k \rrbracket_I) a \end{aligned}$$

$$(x : p) \cdot (y : q) \equiv (x \cdot y) ; (p \cdot q) \quad \text{SKA-ORD-SEQ} \quad p \cdot 0 \equiv 0 \quad \text{SKA-ORD-ZERO}$$

Boolean axioms (in addition to monotone axioms)

$$\begin{array}{ll} 1 \wedge b \equiv 1 & \text{BOOL-ONE-U} \\ b \wedge (b \wedge b') \equiv b & \text{BOOL-CONJ-SUBSET} \quad (t \wedge t') \wedge b \equiv t \wedge b \wedge t' \wedge b \quad \text{BOOL-CONJ-U-DIST} \\ b \vee b' \equiv b \cup b' & \text{BOOL-DISJ-U} \quad (t \vee t') \vee b \equiv t \vee b \vee t' \vee b \quad \text{BOOL-DISJ-U-DIST} \end{array}$$

Network axioms

$$\begin{array}{ll} [t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \wedge r)]\hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \wedge r' \text{ and } \hat{o} = o \sqcup o' \quad \text{NET-ORD} \\ [t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \sqcup r') \wedge (t' \wedge r)]\hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \wedge r' \text{ and } \hat{o} = o \sqcup o' \quad \text{NET-PRL} \end{array}$$

Single round axioms

$$\begin{array}{ll} [\mathbb{1}] \parallel p' \triangleright \emptyset \equiv 1 & \text{SR-ONE} \quad (p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q') \quad \text{SR-EXC} \\ [\emptyset]r \triangleright o \equiv 0 & \text{SR-ZERO} \quad [b \wedge t]r \triangleright o \equiv [(r \cup b) \wedge t]r \triangleright o \quad \text{SR-CAN} \\ [t]r \triangleright o + [t']r \triangleright o \equiv [t \vee t']r \triangleright o & \text{SR-PLUS} \end{array}$$

# BellKAT at a glance

Syntax

Nodes

 $N ::= A, B, C, \dots$ 

BP pairs

 $BP \ni bp ::= N \sim N$ 

Multisets

 $M(BP) \ni a, b \in \omega \text{ s.t. } \llbracket a \rrbracket_B = \llbracket b \rrbracket_B$ 

Tests

 $M(BP) \ni a, b \in \omega \text{ s.t. } \llbracket a \rrbracket_B = \llbracket b \rrbracket_B$ 

Atomic action  
Policies

## Single round semantics

Basic actions  
Guarded policy

$$\begin{array}{c} | \quad p^* \\ r \triangleright o ::= [\mathbb{1}]r \triangleright o + [r]\emptyset \triangleright \emptyset \\ [t]p ::= [t]\emptyset \triangleright \emptyset \cdot p \end{array}$$

$$\begin{aligned} \langle p \rangle &\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP)) \\ \langle \emptyset \rangle a &\triangleq \emptyset \\ \langle 1 \rangle a &\triangleq \{\emptyset \bowtie a\} \\ \langle [t]r \triangleright o \rangle a &\triangleq \begin{cases} \{o \bowtie a \mid r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \end{aligned}$$

KA axioms

SKA axioms for  $\cdot$

$$\begin{array}{lll} (p \cdot q) \cdot r \equiv p \cdot (q \cdot r) & \text{SKA-ORD-ASSOC} & 1 \cdot p \equiv p \\ p \cdot (q + r) \equiv p \cdot q + p \cdot r & \text{SKA-ORD-DIST-L} & p \cdot 1 \equiv p \\ (p + q) \cdot r \equiv p \cdot r + q \cdot r & \text{SKA-ORD-DIST-R} & 0 \cdot p \equiv 0 \\ (x \cdot p) \cdot (y \cdot q) \equiv (x \cdot y) \cdot (p \cdot q) & \text{SKA-ORD-SIQ} & p \cdot 0 \equiv 0 \end{array}$$

Boolean axioms (in addition to monotone axioms)

$$\begin{array}{lll} 1 \wedge b \equiv 1 & \text{BOOL-ONE-U} & (t \wedge t') \vee b \equiv t \vee b \wedge t' \vee b \quad \text{BOOL-CONJ-U-DIST} \\ b \wedge (b \vee b') \equiv b & \text{BOOL-CONJ-SUBSET} & (t \vee t') \wedge b \equiv t \wedge b \vee t' \wedge b \quad \text{BOOL-DISJ-U-DIST} \\ b \vee b' \equiv b \cup b' & \text{BOOL-DISJ-U} & \end{array}$$

Network axioms

$$\begin{array}{lll} [t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \vee r)]\hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \vee r' \text{ and } \hat{o} = o \vee o' & \text{NET-ORD} \\ [t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \vee r') \wedge (t' \vee r)]\hat{r} \triangleright \hat{o} & \text{if } \hat{r} = r \vee r' \text{ and } \hat{o} = o \vee o' & \text{NET-PRL} \end{array}$$

Single round axioms

$$\begin{array}{lll} \llbracket p \parallel p' \rrbracket \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q') & \text{SR-EXC} & \\ \llbracket \mathbb{1} \rrbracket \emptyset \triangleright \emptyset \equiv 1 & \text{SR-ONE} & \llbracket b \wedge t \rrbracket r \triangleright o \equiv \llbracket (r \cup b) \wedge t \rrbracket r \triangleright o & \text{SR-CAN} \\ \llbracket \emptyset \rrbracket r \triangleright o \equiv 0 & \text{SR-ZERO} & \llbracket t \rrbracket r \triangleright o + [t']r \triangleright o \equiv [t \vee t']r \triangleright o & \text{SR-PLUS} \end{array}$$

Test semantics

$$\begin{array}{ll} \langle t \rangle \in \mathcal{M}(BP) \rightarrow \{\top, \perp\} & \\ \langle \mathbb{1} \rangle a \triangleq \top & \langle t \wedge b \rangle a \triangleq \langle \mathbb{1} \rangle a \setminus b \wedge b \subseteq a \vee \langle b \rangle a \\ \langle b \rangle a \triangleq b \not\subseteq a & \langle t \square t' \rangle a \triangleq \langle t \rangle a \square \langle t' \rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee \end{array}$$

Single round semantics

$$\begin{array}{ll} \langle p \rangle &\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP)) \\ \langle \emptyset \rangle a &\triangleq \emptyset \\ \langle 1 \rangle a &\triangleq \{\emptyset \bowtie a\} \\ \langle [t]r \triangleright o \rangle a &\triangleq \begin{cases} \{o \bowtie a \mid r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\ \langle p + q \rangle a &\triangleq \langle p \rangle a \cup \langle q \rangle a \\ \langle p \cdot q \rangle a &\triangleq (\langle p \rangle \cdot \langle q \rangle) a \\ \langle p \parallel q \rangle a &\triangleq (\langle p \rangle \parallel \langle q \rangle) a \end{array}$$

Multi-round semantics

$$\begin{array}{ll} \llbracket p \rrbracket &\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP)) \\ \llbracket p \rrbracket_I &\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 \ddot{\wedge} \pi_2 \ddot{\wedge} \dots \ddot{\wedge} \pi_k \\ \llbracket p \rrbracket a &\triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a \\ \llbracket e \rrbracket a &\triangleq \{a\} \\ \llbracket [t]r \triangleright o \rrbracket a &\triangleq \begin{cases} \{o \bowtie a \mid r\} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\ \llbracket \pi_1 \ddot{\wedge} \pi_2 \ddot{\wedge} \dots \ddot{\wedge} \pi_k \rrbracket a &\triangleq (\llbracket \pi_1 \rrbracket \parallel \llbracket \pi_2 \rrbracket \parallel \dots \parallel \llbracket \pi_k \rrbracket) a \end{array}$$

# BellKAT at a glance

## Syntax

Nodes	$N ::= A, B, C, \dots$
Bell pairs	$BP \ni bp ::= N\text{-}N$
Multisets	$M(BP) \ni a, b, r, o ::= \{\!\{bp_1, \dots, bp_k\}\!\}$
Tests	$T \ni t, t' ::= \begin{cases} \perp & \text{no test} \\   & \text{multiset absence} \\   & t \wedge t' & \text{conjunction} \\   & t \vee t' & \text{disjunction} \\   & t \uplus b & \text{multiset union} \end{cases}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \triangleright o$
Policies	$P \ni p, q ::= \begin{cases} 0 & \text{abort} \\   & 1 & \text{skip or no-round} \\   & \pi & \text{atomic action} \\   & r \triangleright o & \text{basic action} \\   & [t]p & \text{guarded policy} \\   & p + q & \text{nondeterministic choice} \\   & p \cdot q & \text{ordered composition} \\   & p \parallel q & \text{parallel composition} \\   & p ; q & \text{sequential composition} \\   & p^* & \text{Kleene star} \end{cases}$
Basic actions	$r \triangleright o ::= [\perp]r \triangleright o + [r]\emptyset \triangleright \emptyset$
Guarded policy	$[t]p ::= [t]\emptyset \triangleright \emptyset \cdot p$
Test semantics	$\langle t \rangle \in M(BP) \rightarrow \{\top, \perp\}$
	$\langle \perp \rangle a \triangleq \top$
	$\langle \perp \rangle a \triangleq b \not\subseteq a$
	$\langle t \wedge b \rangle a \triangleq (\langle t \rangle a \setminus b \wedge b \subseteq a) \vee \langle \{b\}a \rangle$
	$\langle t \wedge t' \rangle a \triangleq \langle t \rangle a \square \langle t' \rangle a, \text{ where } \square \text{ is either } \wedge \text{ or } \vee$
Single round semantics	$\langle p \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP) \times M(BP))$
	$\langle \emptyset \rangle a \triangleq \emptyset$
	$\langle 1 \rangle a \triangleq \{ \theta \mapsto a \}$
	$\langle [t]r \triangleright o \rangle a \triangleq \begin{cases} \{ o \mapsto a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$
	$\langle p + q \rangle a \triangleq \langle (p) \rangle a \cup \langle (q) \rangle a$
	$\langle p \cdot q \rangle a \triangleq \langle (p) \cdot \langle (q) \rangle \rangle a$
	$\langle p \parallel q \rangle a \triangleq \langle (p) \parallel \langle (q) \rangle \rangle a$
Multi-round semantics	$\langle \llbracket p \rrbracket \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP))$
	$\llbracket \omega \rrbracket_I \in M(BP) \rightarrow \mathcal{P}(M(BP)), \text{ where } \omega = \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k$
	$\llbracket p \rrbracket a \triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a$
	$\llbracket e \rrbracket a \triangleq \{ a \}$
	$\llbracket [t]r \triangleright o \rrbracket a \triangleq \begin{cases} \{ o \uplus a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$
	$\llbracket \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k \rrbracket a \triangleq (\llbracket \pi_1 \rrbracket a \bullet \llbracket \pi_2 \rrbracket a \bullet \dots \bullet \llbracket \pi_k \rrbracket a)$

## KA axioms

$(p + q) + r \equiv p + (q + r)$	KA-PLUS-ASSOC	$p ; 1 \equiv p$	KA-SEQ-ONE
$p + q \equiv q + p$	KA-PLUS-COMM	$1 ; p \equiv p$	KA-ONE-SEQ
$p + 0 \equiv p$	KA-PLUS-ZERO	$0 ; p \equiv 0$	KA-ZERO-SEQ
$p + p \equiv p$	KA-PLUS-IDEM	$p ; 0 \equiv 0$	KA-SEQ-ZERO
$(p ; q) ; r \equiv p ; (q ; r)$	KA-SEQ-ASSOC	$1 + p ; p^* \equiv p^*$	KA-UNROLL-L
$p ; (q + r) \equiv p ; q + p ; r$	KA-SEQ-DIST-L	$p ; r \leq r \Rightarrow p^* ; r \leq r$	KA-LFP-L
$(p + q) ; r \equiv p ; r + q ; r$	KA-SEQ-DIST-R	$1 + p^* ; p \equiv p^*$	KA-UNROLL-R
		$r ; p \leq r \Rightarrow r ; p^* \leq r$	KA-LFP-R

## SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-PRL-ASSOC	$p \parallel q \equiv q \parallel p$	SKA-PRL-COMM
$p \parallel (q + r) \equiv p \parallel q + p \parallel r$	SKA-PRL-DIST	$1 \parallel p \equiv p$	SKA-ONE-PRL
$(x ; p) \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q)$	SKA-PRL-SEQ	$0 \parallel p \equiv 0$	SKA-ZERO-PRL

## SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-ORD-ASSOC	$1 \cdot p \equiv p$	SKA-ONE-ORD
$p \cdot (q + r) \equiv p \cdot q + p \cdot r$	SKA-ORD-DIST-L	$p \cdot 1 \equiv p$	SKA-ORD-ONE
$(p + q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-ORD-DIST-R	$0 \cdot p \equiv 0$	SKA-ZERO-ORD
$(x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q)$	SKA-ORD-SEQ	$p \cdot 0 \equiv 0$	SKA-ORD-ZERO

## Boolean axioms (in addition to monotone axioms)

$1 \sqcup b \equiv 1$	BOOL-ONE-U	$(t \wedge t') \sqcup b \equiv t \sqcup b \wedge t' \sqcup b$	BOOL-CONJ-U-DIST
$b \wedge (b \sqcup b') \equiv b$	BOOL-CONJ-SUBSET	$(t \vee t') \sqcup b \equiv t \vee b \wedge t' \vee b$	BOOL-DISJ-U-DIST
$b \vee b' \equiv b \cup b'$	BOOL-DISJ-U		

## Network axioms

$[t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \sqcup r)]\hat{r} \triangleright \hat{o}$		if $\hat{r} = r \wedge r'$ and $\hat{o} = o \sqcup o'$	NET-ORD
$[t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \sqcup r') \wedge (t' \sqcup r)]\hat{r} \triangleright \hat{o}$		if $\hat{r} = r \wedge r'$ and $\hat{o} = o \sqcup o'$	NET-PRL

## Single round axioms

$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$		SR-EXC	
$[1] \emptyset \triangleright \emptyset \equiv 1$	SR-ONE	$[b \wedge t]r \triangleright o \equiv [(r \cup b) \wedge t]r \triangleright o$	SR-CAN
$[0]r \triangleright o \equiv 0$	SR-ZERO	$[t]r \triangleright o + [t']r \triangleright o \equiv [t \vee t']r \triangleright o$	SR-PLUS

# BellKAT at a glance

## Syntax

Nodes	$N ::= A, B, C, \dots$
Bell pairs	$BP \ni bp ::= N \multimap N$
Multisets	$M(BP) \ni a, b, r, o ::= \{\!\{bp_1, \dots, bp_k\}\!}$
Tests	$T \ni t, t' ::= \begin{cases} \perp & \text{no test} \\   & b \text{ multiset absence} \\   & t \wedge t' \text{ conjunction} \\   & t \vee t' \text{ disjunction} \\   & t \uplus b \text{ multiset union} \end{cases}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \triangleright o$
Policies	$P \ni p, q ::= \begin{cases} 0 & \text{abort} \\   & 1 \text{ skip or no-round} \\   & \pi \text{ atomic action} \\   & r \triangleright o \text{ basic action} \\   & [t]p \text{ guarded policy} \\   & p + q \text{ nondeterministic choice} \\   & p \cdot q \text{ ordered composition} \\   & p \parallel q \text{ parallel composition} \\   & p ; q \text{ sequential composition} \\   & p^* \text{ Kleene star} \end{cases}$
Basic actions	$r \triangleright o ::= [\perp]r \triangleright o + [r]\emptyset \triangleright \emptyset$
Guarded policy	$[t]p ::= [t]\emptyset \triangleright \emptyset \cdot p$
Test semantics	$\langle t \rangle \in M(BP) \rightarrow \{\top, \perp\}$
	$\langle \perp \rangle a \triangleq \top$
	$\langle t \wedge b \rangle a \triangleq (\langle t \rangle a \setminus b \wedge b \subseteq a) \vee \langle b \rangle a$
	$\langle \perp \square t' \rangle a \triangleq \langle t \rangle a \square \langle t' \rangle a, \text{ where } \square \text{ is either } \wedge \text{ or } \vee$
Single round semantics	$\langle p \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP) \times M(BP))$
	$\langle \emptyset \rangle a \triangleq \emptyset$
	$\langle 1 \rangle a \triangleq \{ \theta \multimap a \}$
	$\langle [t]r \triangleright o \rangle a \triangleq \begin{cases} \{ o \multimap a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$
	$\langle p + q \rangle a \triangleq \langle p \rangle a \cup \langle q \rangle a$
	$\langle p \cdot q \rangle a \triangleq (\langle p \rangle \cdot \langle q \rangle) a$
	$\langle p \parallel q \rangle a \triangleq (\langle p \rangle \parallel \langle q \rangle) a$
Multi-round semantics	$\langle \llbracket p \rrbracket \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP))$
	$\llbracket \omega \rrbracket_I \in M(BP) \rightarrow \mathcal{P}(M(BP)), \text{ where } \omega = \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k$
	$\llbracket p \rrbracket a \triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a$
	$\llbracket e \rrbracket a \triangleq \{ a \}$
	$\llbracket [t]r \triangleright o \rrbracket a \triangleq \begin{cases} \{ o \uplus a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$
	$\llbracket \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k \rrbracket a \triangleq (\llbracket \pi_1 \rrbracket a \bullet \llbracket \pi_2 \rrbracket a \bullet \dots \bullet \llbracket \pi_k \rrbracket a)$

## KA axioms

$(p + q) + r \equiv p + (q + r)$	KA-PLUS-ASSOC	$p ; 1 \equiv p$	KA-SEQ-ONE
$p + q \equiv q + p$	KA-PLUS-COMM	$1 ; p \equiv p$	KA-ONE-SEQ
$p + 0 \equiv p$	KA-PLUS-ZERO	$0 ; p \equiv 0$	KA-ZERO-SEQ
$p + p \equiv p$	KA-PLUS-IDEM	$p ; 0 \equiv 0$	KA-SEQ-ZERO
$(p ; q) ; r \equiv p ; (q ; r)$	KA-SEQ-ASSOC	$1 + p ; p^* \equiv p^*$	KA-UNROLL-L
$p ; (q + r) \equiv p ; q + p ; r$	KA-SEQ-DIST-L	$p ; r \leq r \Rightarrow p^* ; r \leq r$	KA-LFP-L
$(p + q) ; r \equiv p ; r + q ; r$	KA-SEQ-DIST-R	$1 + p^* ; p \equiv p^*$	KA-UNROLL-R
		$r ; p \leq r \Rightarrow r ; p^* \leq r$	KA-LFP-R

## SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-PRL-ASSOC	$p \parallel q \equiv q \parallel p$	SKA-PRL-COMM
$p \parallel (q + r) \equiv p \parallel q + p \parallel r$	SKA-PRL-DIST	$1 \parallel p \equiv p$	SKA-ONE-PRL
$(x ; p) \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q)$	SKA-PRL-SEQ	$0 \parallel p \equiv 0$	SKA-ZERO-PRL

## SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-ORD-ASSOC	$1 \cdot p \equiv p$	SKA-ONE-ORD
$p \cdot (q + r) \equiv p \cdot q + p \cdot r$	SKA-ORD-DIST-L	$p \cdot 1 \equiv p$	SKA-ORD-ONE
$(p + q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-ORD-DIST-R	$0 \cdot p \equiv 0$	SKA-ZERO-ORD
$(x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q)$	SKA-ORD-SEQ	$p \cdot 0 \equiv 0$	SKA-ORD-ZERO

## Boolean axioms (in addition to monotone axioms)

$\perp \wedge b \equiv \perp$	BOOL-ONE-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	BOOL-CONJ-U-DIST
$b \wedge (b \uplus b') \equiv b$	BOOL-CONJ-SUBSET	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	BOOL-DISJ-U-DIST
$b \vee b' \equiv b \uplus b'$	BOOL-DISJ-U		

## Network axioms

$[t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	NET-ORD
$[t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \uplus t') \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	NET-PRL

## Single round axioms

$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	SR-EXC
$[b \wedge t]r \triangleright o \equiv [b \parallel t]r \triangleright o \equiv [(r \cup b) \wedge t]r \triangleright o$	SR-CAN
$[t]r \triangleright o + [t']r \triangleright o \equiv [t \vee t']r \triangleright o$	SR-PLUS

# BellKAT at a glance

## Syntax

Nodes	$N ::= A, B, C, \dots$
Bell pairs	$BP \ni bp ::= N \multimap N$
Multisets	$M(BP) \ni a, b, r, o ::= \{\!\{bp_1, \dots, bp_k\}\!}$
Tests	$T \ni t, t' ::= \begin{cases} 1 & \text{no test} \\   & b \text{ multiset absence} \\   & t \wedge t' \text{ conjunction} \\   & t \vee t' \text{ disjunction} \\   & t \uplus b \text{ multiset union} \end{cases}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \triangleright o$
Policies	$P \ni p, q ::= \begin{cases} 0 & \text{abort} \\   & 1 \text{ skip or no-round} \\   & \pi \text{ atomic action} \\   & r \triangleright o \text{ basic action} \\   & [t]p \text{ guarded policy} \\   & p + q \text{ nondeterministic choice} \\   & p \cdot q \text{ ordered composition} \\   & p \parallel q \text{ parallel composition} \\   & p ; q \text{ sequential composition} \\   & p^* \text{ Kleene star} \end{cases}$
Basic actions	$r \triangleright o ::= [\mathbb{1}]r \triangleright o + [r]\emptyset \triangleright \emptyset$
Guarded policy	$[t]p ::= [t]\emptyset \triangleright \emptyset \cdot p$
Test semantics	$\langle t \rangle \in M(BP) \rightarrow \{\top, \perp\}$
	$\langle \mathbb{1} \rangle a \triangleq \top$
	$\langle t \uplus b \rangle a \triangleq (\langle t \rangle a \setminus b \wedge b \subseteq a) \vee \langle b \rangle a$
	$\langle \mathbb{0} \rangle a \triangleq b \not\subseteq a$
	$\langle t \square t' \rangle a \triangleq \langle t \rangle a \square \langle t' \rangle a, \text{ where } \square \text{ is either } \wedge \text{ or } \vee$
Single round semantics	$\langle p \rangle \in M(BP) \rightarrow \mathcal{P}(M(BP) \times M(BP))$
	$\langle \mathbb{0} \rangle a \triangleq \emptyset$
	$\langle \mathbb{1} \rangle a \triangleq \{ \theta \multimap a \}$
	$\langle [t]r \triangleright o \rangle a \triangleq \begin{cases} \{ o \multimap a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$
	$\langle p + q \rangle a \triangleq \langle p \rangle a \cup \langle q \rangle a$
	$\langle p \cdot q \rangle a \triangleq (\langle p \rangle \cdot \langle q \rangle) a$
	$\langle p \parallel q \rangle a \triangleq (\langle p \rangle \parallel \langle q \rangle) a$
Multi-round semantics	$\llbracket p \rrbracket \in M(BP) \rightarrow \mathcal{P}(M(BP))$
	$\llbracket \omega \rrbracket_I \in M(BP) \rightarrow \mathcal{P}(M(BP)), \text{ where } \omega = \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k$
	$\llbracket p \rrbracket a \triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a$
	$\llbracket e \rrbracket a \triangleq \{ a \}$
	$\llbracket [t]r \triangleright o \rrbracket a \triangleq \begin{cases} \{ o \uplus a \mid r \} & \text{if } r \subseteq a \text{ and } \langle t \rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$
	$\llbracket \pi_1 \ddagger \pi_2 \ddagger \dots \ddagger \pi_k \rrbracket a \triangleq (\llbracket \pi_1 \rrbracket a \bullet \llbracket \pi_2 \rrbracket a \bullet \dots \bullet \llbracket \pi_k \rrbracket a)$

## KA axioms

$(p + q) + r \equiv p + (q + r)$	KA-PLUS-ASSOC	$p ; 1 \equiv p$	KA-SEQ-ONE
$p + q \equiv q + p$	KA-PLUS-COMM	$1 ; p \equiv p$	KA-ONE-SEQ
$p + 0 \equiv p$	KA-PLUS-ZERO	$0 ; p \equiv 0$	KA-ZERO-SEQ
$p + p \equiv p$	KA-PLUS-IDEM	$p ; 0 \equiv 0$	KA-SEQ-ZERO
$(p ; q) ; r \equiv p ; (q ; r)$	KA-SEQ-ASSOC	$1 + p ; p^* \equiv p^*$	KA-UNROLL-L
$p ; (q + r) \equiv p ; q + p ; r$	KA-SEQ-DIST-L	$p ; r \leq r \Rightarrow p^* ; r \leq r$	KA-LFP-L
$(p + q) ; r \equiv p ; r + q ; r$	KA-SEQ-DIST-R	$1 + p^* ; p \equiv p^*$	KA-UNROLL-R
		$r ; p \leq r \Rightarrow r ; p^* \leq r$	KA-LFP-R

## SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-PRL-ASSOC	$p \parallel q \equiv q \parallel p$	SKA-PRL-COMM
$p \parallel (q + r) \equiv p \parallel q + p \parallel r$	SKA-PRL-DIST	$1 \parallel p \equiv p$	SKA-ONE-PRL
$(x ; p) \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q)$	SKA-PRL-SEQ	$0 \parallel p \equiv 0$	SKA-ZERO-PRL

## SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-ORD-ASSOC	$1 \cdot p \equiv p$	SKA-ONE-ORD
$p \cdot (q + r) \equiv p \cdot q + p \cdot r$	SKA-ORD-DIST-L	$p \cdot 1 \equiv p$	SKA-ORD-ONE
$(p + q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-ORD-DIST-R	$0 \cdot p \equiv 0$	SKA-ZERO-ORD
$(x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q)$	SKA-ORD-SEQ	$p \cdot 0 \equiv 0$	SKA-ORD-ZERO

## Boolean axioms (in addition to monotone axioms)

$1 \wedge b \equiv 1$	BOOL-ONE-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	BOOL-CONJ-U-DIST
$b \wedge (b \uplus b') \equiv b$	BOOL-CONJ-SUBSET	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	BOOL-DISJ-U-DIST
$b \vee b' \equiv b \uplus b'$	BOOL-DISJ-U		

## Network axioms

$[t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	NET-ORD
$[t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \uplus t') \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	NET-PRL

## Single round axioms

$\langle p \parallel p' \rangle \cdot \langle q \parallel q' \rangle \leq (p \cdot q) \parallel (p' \cdot q')$	SR-EXC
$[b \wedge t]r \triangleright o \equiv \llbracket b \rrbracket_I r \triangleright o$	SR-CAN
$[t]r \triangleright o + [t']r' \triangleright o' \equiv [t \vee t']r \triangleright o$	SR-PLUS

# BellKAT at a glance

## Syntax

Nodes	$N ::= A, B, C, \dots$
Bell pairs	$BP \ni bp ::= N\text{-}N$
Multisets	$\mathcal{M}(BP) \ni a, b, r, o ::= \{\!\{bp_1, \dots, bp_k\}\!}$
Tests	$T \ni t, t' ::= \begin{cases} \mathbb{1} & \text{no test} \\   & \\   & b & \text{multiset absence} \\   & t \wedge t' & \text{conjunction} \\   & t \vee t' & \text{disjunction} \\   & t \uplus b & \text{multiset union} \end{cases}$
Atomic actions	$\Pi \ni \pi, x, y ::= [t]r \triangleright o$
Policies	$P \ni p, q ::= \begin{cases} 0 & \text{abort} \\   & 1 & \text{skip or no-round} \\   & \pi & \text{atomic action} \\   & r \triangleright o & \text{basic action} \\   & [t]p & \text{guarded policy} \\   & p + q & \text{nondeterministic choice} \\   & p \cdot a & \text{ordered composition} \end{cases}$

## Network axioms

$$[t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o}$$

$$[t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o}$$

$(p)$	$\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP))$
$(0)a$	$\triangleq \emptyset$
$(1)a$	$\triangleq \{\emptyset \ni a\}$
$([t]r \triangleright o)a$	$\triangleq \begin{cases} \{o \ni a \setminus r\} & \text{if } r \subseteq a \text{ and } \{t\}a = \top \\ \emptyset & \text{otherwise} \end{cases}$
$(p + q)a$	$\triangleq (p \parallel a) \cup (q \parallel a)$
$(p \cdot q)a$	$\triangleq ((p) \cdot (q))a$
$(p \parallel q)a$	$\triangleq ((p) \parallel (q))a$

## Multi-round semantics

$\llbracket p \rrbracket$	$\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP))$
$\llbracket \omega \rrbracket_I$	$\in \mathcal{M}(BP) \rightarrow \mathcal{P}(\mathcal{M}(BP))$ , where $\omega = \pi_1 \ddot{\wedge} \pi_2 \ddot{\wedge} \dots \ddot{\wedge} \pi_k$
$\llbracket p \rrbracket a$	$\triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a$
$\llbracket e \rrbracket a$	$\triangleq \{a\}$
$\llbracket [t]r \triangleright o \rrbracket_I a$	$\triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \{t\}a = \top \\ \emptyset & \text{otherwise} \end{cases}$
$\llbracket \pi_1 \ddot{\wedge} \pi_2 \ddot{\wedge} \dots \ddot{\wedge} \pi_k \rrbracket_I a$	$\triangleq (\llbracket \pi_1 \rrbracket_I \bullet \llbracket \pi_2 \rrbracket_I \ddot{\wedge} \dots \ddot{\wedge} \llbracket \pi_k \rrbracket_I) a$

## KA axioms

$(p + q) + r \equiv p + (q + r)$	KA-PLUS-ASSOC	$p ; 1 \equiv p$	KA-SEQ-ONE
$p + q \equiv q + p$	KA-PLUS-COMM	$1 ; p \equiv p$	KA-ONE-SEQ
$p + 0 \equiv p$	KA-PLUS-ZERO	$0 ; p \equiv 0$	KA-ZERO-SEQ
$p + p \equiv p$	KA-PLUS-IDEM	$p ; 0 \equiv 0$	KA-SEQ-ZERO
$(p ; q) ; r \equiv p ; (q ; r)$	KA-SEQ-ASSOC	$1 + p ; p^* \equiv p^*$	KA-UNROLL-L
$p ; (q + r) \equiv p ; q + p ; r$	KA-SEQ-DIST-L	$p ; r \leq r \Rightarrow p^* ; r \leq r$	KA-LFP-L
$(p + q) ; r \equiv p ; r + q ; r$	KA-SEQ-DIST-R	$1 + p^* ; p \equiv p^*$	KA-UNROLL-R
		$r ; p \leq r \Rightarrow r ; p^* \leq r$	KA-LFP-R

## SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-PRL-ASSOC	$p \parallel q \equiv q \parallel p$	SKA-PRL-COMM
$p \parallel (q + r) \equiv p \parallel q + p \parallel r$	SKA-PRL-DIST	$1 \parallel p \equiv p$	SKA-ONE-PRL
$; p \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q)$	SKA-PRL-SEQ	$0 \parallel p \equiv 0$	SKA-ZERO-PRL

## Axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-ORD-ASSOC	$1 \cdot p \equiv p$	SKA-ONE-ORD
$p \cdot (q + r) \equiv p \cdot q + p \cdot r$	SKA-ORD-DIST-L	$p \cdot 1 \equiv p$	SKA-ORD-ONE
$(p + q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-ORD-DIST-R	$0 \cdot p \equiv 0$	SKA-ZERO-ORD
$; p \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q)$	SKA-ORD-SEQ	$p \cdot 0 \equiv 0$	SKA-ORD-ZERO

can axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	BOOL-ONE-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	BOOL-CONJ-U-DIST
$b \wedge (b \uplus b') \equiv b$	BOOL-CONJ-SUBSET	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	BOOL-DISJ-U-DIST
$b \vee b' \equiv b \cup b'$	BOOL-DISJ-U		

## Network axioms

$[t]r \triangleright o \cdot [t']r' \triangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o}$		if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	NET-ORD
$[t]r \triangleright o \parallel [t']r' \triangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \triangleright \hat{o}$		if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	NET-PRL

## Single round axioms

$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	SR-EXC
$[t] \emptyset \triangleright o \equiv 1$	SR-ONE
$[\emptyset]r \triangleright o \equiv 0$	SR-ZERO
$[t]r \triangleright o + [t']r' \triangleright o' \equiv [t \vee t']r \triangleright o$	SR-PLUS

## Formal results

*Definition 4.7 (Normal form of policies).* A policy  $p$  is in normal form if it is a finite sum, s.t. every summand has a unique  $(r, o)$  pair with the corresponding  $t$  in canonical form w.r.t.  $r$  and  $t \neq r$ :

$$p = \sum [t]r \blacktriangleright o$$

**PROPOSITION 4.1 (SOUNDNESS AND COMPLETENESS).** Let  $p, q$  be single round policies. Then  $p$  and  $q$  are provably equivalent by the BellKAT axioms if and only if  $\llbracket p \rrbracket = \llbracket q \rrbracket$ .

**THEOREM 4.2 (SOUNDNESS AND COMPLETENESS W.R.T. STANDARD INTERPRETATION).** Policies  $p, q$  are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is,  $I(p) = I(q)$  if and only if  $\vdash p \equiv q$ .

**THEOREM 4.3 (SOUNDNESS OF MULTI-ROUND POLICIES).** If policies  $p, q \in P$  are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is,  $\vdash p \equiv q \implies \llbracket p \rrbracket = \llbracket q \rrbracket$ .

## Formal results

*Definition 4.7 (Normal form of policies).* A policy  $p$  is in normal form if it is a finite sum, s.t. every summand has a unique  $(r, o)$  pair with the corresponding  $t$  in canonical form w.r.t.  $r$  and  $t \neq r$ :

$$p = \sum [t]r \blacktriangleright o$$

**PROPOSITION 4.1 (SOUNDNESS AND COMPLETENESS).** Let  $p, q$  be single round policies. Then  $p$  and  $q$  are provably equivalent by the BellKAT axioms if and only if  $\llbracket p \rrbracket = \llbracket q \rrbracket$ .

**THEOREM 4.2 (SOUNDNESS AND COMPLETENESS W.R.T. STANDARD INTERPRETATION).** Policies  $p, q$  are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is,  $I(p) = I(q)$  if and only if  $\vdash p \equiv q$ .

**THEOREM 4.3 (SOUNDNESS OF MULTI-ROUND POLICIES).** If policies  $p, q \in P$  are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is,  $\vdash p \equiv q \implies \llbracket p \rrbracket = \llbracket q \rrbracket$ .

## Formal results

*Definition 4.7 (Normal form of policies).* A policy  $p$  is in normal form if it is a finite sum, s.t. every summand has a unique  $(r, o)$  pair with the corresponding  $t$  in canonical form w.r.t.  $r$  and  $t \neq r$ :

$$p = \sum [t]r \blacktriangleright o$$



**PROPOSITION 4.1 (SOUNDNESS AND COMPLETENESS).** Let  $p, q$  be single round policies. Then  $p$  and  $q$  are provably equivalent by the BellKAT axioms if and only if  $\llbracket p \rrbracket = \llbracket q \rrbracket$ .

**THEOREM 4.2 (SOUNDNESS AND COMPLETENESS W.R.T. STANDARD INTERPRETATION).** Policies  $p, q$  are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is,  $I(p) = I(q)$  if and only if  $\vdash p \equiv q$ .

**THEOREM 4.3 (SOUNDNESS OF MULTI-ROUND POLICIES).** If policies  $p, q \in P$  are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is,  $\vdash p \equiv q \implies \llbracket p \rrbracket = \llbracket q \rrbracket$ .

## Formal results

*Definition 4.7 (Normal form of policies).* A policy  $p$  is in normal form if it is a finite sum, s.t. every summand has a unique  $(r, o)$  pair with the corresponding  $t$  in canonical form w.r.t.  $r$  and  $t \neq r$ :

$$p = \sum [t]r \blacktriangleright o$$



**PROPOSITION 4.1 (SOUNDNESS AND COMPLETENESS).** Let  $p, q$  be single round policies. Then  $p$  and  $q$  are provably equivalent by the BellKAT axioms if and only if  $\llbracket p \rrbracket = \llbracket q \rrbracket$ .

**THEOREM 4.2 (SOUNDNESS AND COMPLETENESS W.R.T. STANDARD INTERPRETATION).** Policies  $p, q$  are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is,  $I(p) = I(q)$  if and only if  $\vdash p \equiv q$ .

**THEOREM 4.3 (SOUNDNESS OF MULTI-ROUND POLICIES).** If policies  $p, q \in P$  are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is,  $\vdash p \equiv q \implies \llbracket p \rrbracket = \llbracket q \rrbracket$ .

## Formal results

*Definition 4.7 (Normal form of policies).* A policy  $p$  is in normal form if it is a finite sum, s.t. every summand has a unique  $(r, o)$  pair with the corresponding  $t$  in canonical form w.r.t.  $r$  and  $t \neq r$ :

$$p = \sum [t]r \blacktriangleright o$$



**PROPOSITION 4.1 (SOUNDNESS AND COMPLETENESS).** Let  $p, q$  be single round policies. Then  $p$  and  $q$  are provably equivalent by the BellKAT axioms if and only if  $\llbracket p \rrbracket = \llbracket q \rrbracket$ .

**THEOREM 4.2 (SOUNDNESS AND COMPLETENESS W.R.T. STANDARD INTERPRETATION).** Policies  $p, q$  are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is,  $I(p) = I(q)$  if and only if  $\vdash p \equiv q$ .



**THEOREM 4.3 (SOUNDNESS OF MULTI-ROUND POLICIES).** If policies  $p, q \in P$  are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is,  $\vdash p \equiv q \implies \llbracket p \rrbracket = \llbracket q \rrbracket$ .

## Decidability

**THEOREM 4.4.** *If  $p$  and  $q$  are valid policies with respect to  $N_0 \subseteq N$ , then  $\llbracket p \rrbracket =_{N_0} \llbracket q \rrbracket$  is decidable.*

# Decidability

**THEOREM 4.4.** *If  $p$  and  $q$  are valid policies with respect to  $\mathcal{N}_0 \subseteq \mathcal{N}$ , then  $\llbracket p \rrbracket =_{\mathcal{N}_0} \llbracket q \rrbracket$  is decidable.*

*Reachability property:* Does protocol  $p$  always or never generate an entangled pair  $A \sim E$

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

# Decidability

**THEOREM 4.4.** *If  $p$  and  $q$  are valid policies with respect to  $\mathcal{N}_0 \subseteq \mathcal{N}$ , then  $\llbracket p \rrbracket =_{\mathcal{N}_0} \llbracket q \rrbracket$  is decidable.*

*Reachability property:* Does protocol  $p$  always or never generate an entangled pair  $A \sim E$

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



Verify more protocol properties with the BellKAT artifact!

# Summary

- 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



# Summary

- 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



THANK YOU!

## Expressing failures

$$r \triangleright o + r \triangleright \emptyset \triangleq r \triangleright o + \text{fail}\langle r \rangle$$

---

Bell pairs: consumed, produced and untouched

## Expressing failures

$$r \triangleright o + r \triangleright \emptyset \triangleq r \triangleright o + \text{fail}(r)$$

Distill  $\{\!\{A\!\sim\! D, A\!\sim\! D\}\!\} \triangleright \{\!\{A\!\sim\! D\}\!\} + \{\!\{A\!\sim\! D, A\!\sim\! D\}\!\} \triangleright \emptyset$  on input  $\{\!\{\underline{A\!\sim\! D}, \underline{A\!\sim\! D}, D\!\sim\! E, D\!\sim\! E, A\!\sim\! E\}\!\}$

---

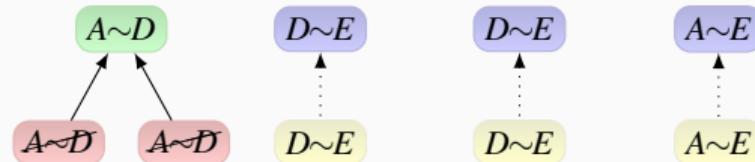
Bell pairs: consumed, produced and untouched

# Expressing failures

$$r \triangleright o + r \triangleright \emptyset \triangleq r \triangleright o + \text{fail}(r)$$

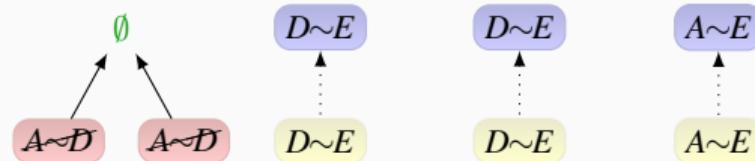
Distill  $\{\underline{A \sim D}, \underline{A \sim D}\} \triangleright \{\underline{A \sim D}\} + \{\underline{A \sim D}, \underline{A \sim D}\} \triangleright \emptyset$  on input  $\{\underline{A \sim D}, \underline{A \sim D}, \underline{D \sim E}, \underline{D \sim E}, \underline{A \sim E}\}$

succeed :



input :

fail :



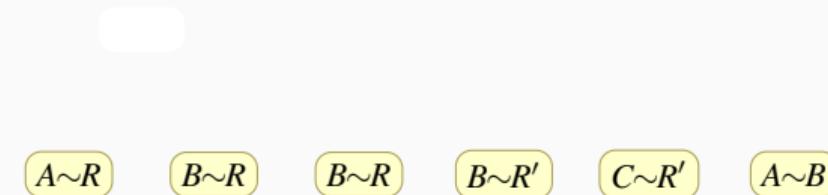
input :

Bell pairs: **consumed**, **produced** and **untouched**

# Single round protocols

## Parallel composition

$\text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R' \rangle$  acts on  $\{A \sim R, B \sim R, B \sim R, B \sim R', C \sim R', A \sim B\}$



The order of basic actions is independent for this input multiset, thus:

$$\text{sw}\langle A \sim R, B \sim R, B \sim R, B \sim R' @ R \rangle = \text{sw}\langle A \sim R, B \sim R' @ R \rangle = \text{sw}\langle A \sim R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim R' \rangle$$

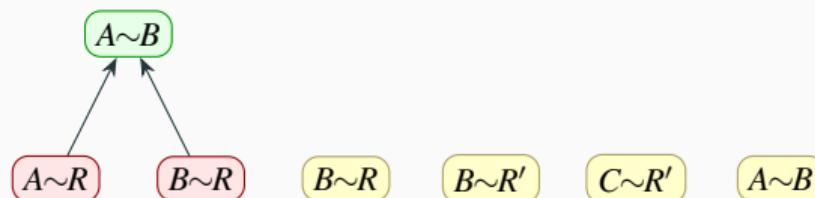
---

Input Bell pairs

# Single round protocols

## Parallel composition

sw $\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R' \rangle$  acts on  $\{\underline{A \sim R}, \underline{B \sim R}, B \sim R, B \sim R', C \sim R', A \sim B\}$



The order of basic actions is independent for this input multiset, thus:

$$\text{sw}\langle A \sim R, B \sim R' \rightarrow B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R' \rangle = \text{sw}\langle A \sim R @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R' \rangle$$

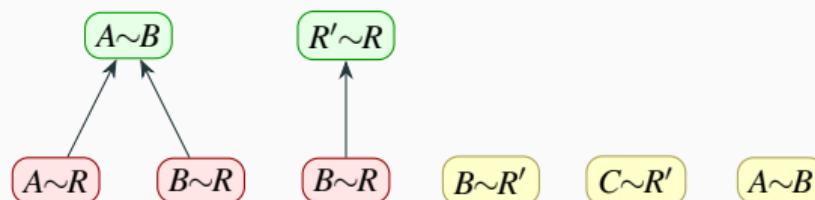
---

Bell pairs: **input** and **consumed**, **produced**

# Single round protocols

## Parallel composition

$\text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \| \text{sw}\langle B \sim C @ R' \rangle$  acts on  $\{A \sim R, B \sim R, B \sim R, B \sim R', C \sim R', A \sim B\}$



The order of basic actions is independent for this input multiset, thus:

$$\text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \| \text{sw}\langle B \sim C @ R' \rangle = \text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \| \text{sw}\langle B \sim C @ R'$$

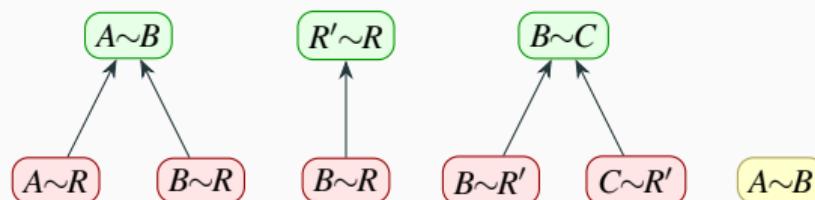
---

Bell pairs: **input** and **consumed**, **produced**

# Single round protocols

## Parallel composition

$\text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R' \rangle$  acts on  $\{A \sim R, B \sim R, B \sim R, \underline{B \sim R'}, \underline{C \sim R'}, A \sim B\}$



The order of basic actions is independent for this input multiset, thus:

$$\text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R' \rangle = \text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R'$$

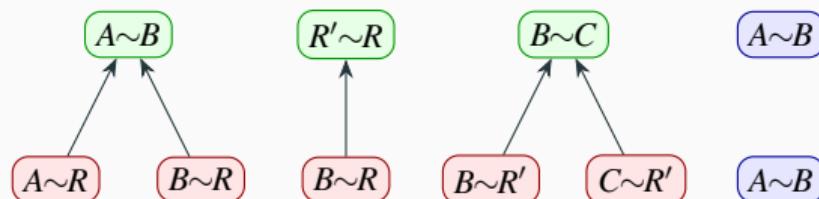
---

Bell pairs: **input** and **consumed**, **produced**

# Single round protocols

## Parallel composition

$\text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R' \rangle$  acts on  $\{A \sim R, B \sim R, B \sim R, B \sim R', C \sim R', A \sim B\}$



The order of basic actions is independent for this input multiset, thus:

$$\text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R' \rangle = \text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \| \text{sw}\langle B \sim C @ R' \rangle$$

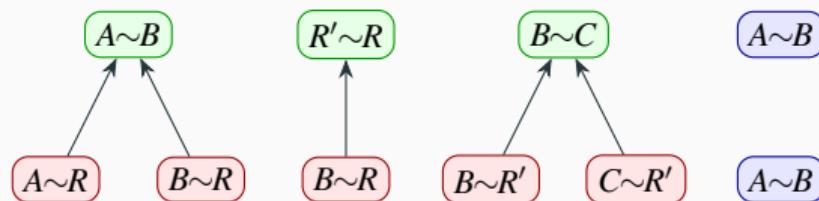
---

Bell pairs: **consumed**, **produced** and **untouched**

# Single round protocols

## Parallel composition

$\text{sw}\langle A \sim B @ R \rangle \parallel \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \parallel \text{sw}\langle B \sim C @ R' \rangle$  acts on  $\{A \sim R, B \sim R, B \sim R, B \sim R', C \sim R', A \sim B\}$



The order of basic actions is independent for this input multiset, thus:

$$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle = \text{sw}\langle A \sim B @ R \rangle \parallel \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \parallel \text{sw}\langle B \sim C @ R' \rangle$$

---

Bell pairs: **consumed**, **produced** and **untouched**

## Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \| \text{sw}\langle B \sim C @ R' \rangle$

$A \sim R$      $B \sim R$      $A \sim R$      $B \sim R'$      $C \sim R'$      $A \sim B$

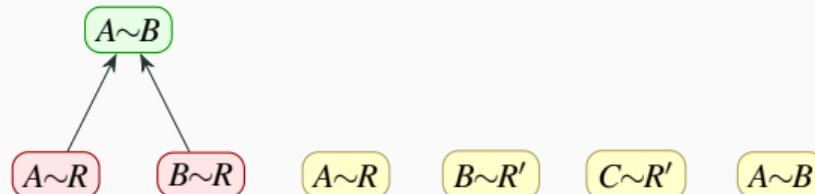
$\text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \| \text{sw}\langle A \sim B @ R \rangle \| \text{sw}\langle B \sim C @ R' \rangle$

---

Bell pairs: **input** and **consumed**, **produced**

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



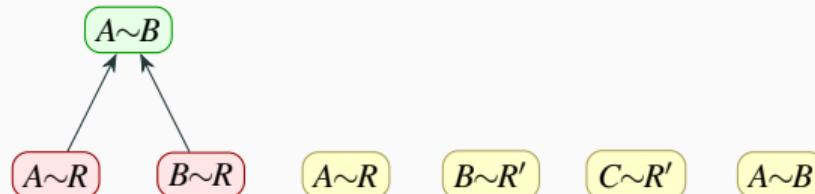
$\text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$

---

Bell pairs: **input** and **consumed**, **produced**

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



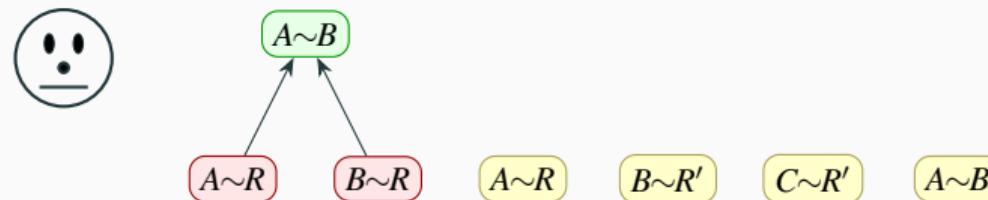
$\text{tr}\langle B \sim R \rightarrow R' \sim R' \rangle \cdot \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$

---

Bell pairs: **input** and **consumed**, **produced**

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



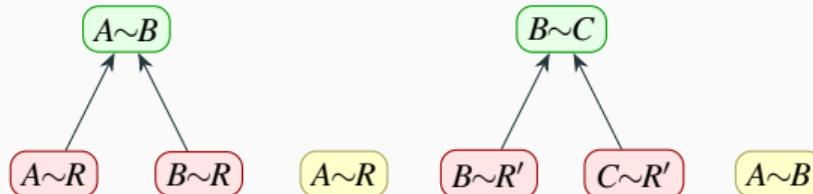
$\text{if } B \sim R = R' \sim R \text{ then } \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$

---

Bell pairs: **input** and **consumed**, **produced**

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



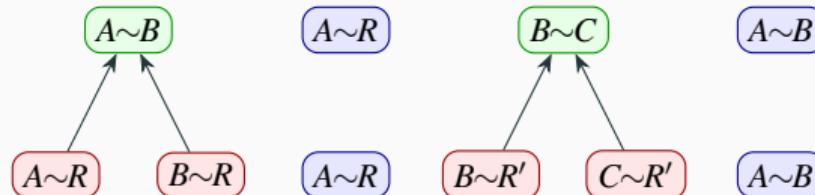
$\text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$

---

<sup>2</sup>Bell pairs: **input** and **consumed**, **produced**.

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



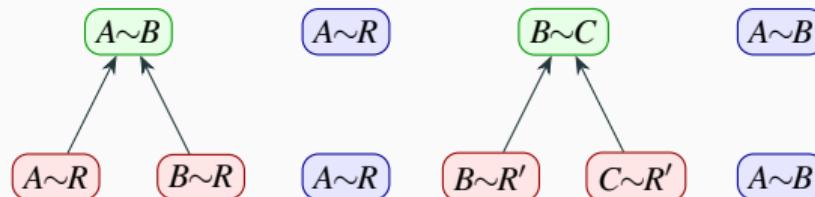
$\text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$

---

Bell pairs: **consumed**, **produced** and **untouched**

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



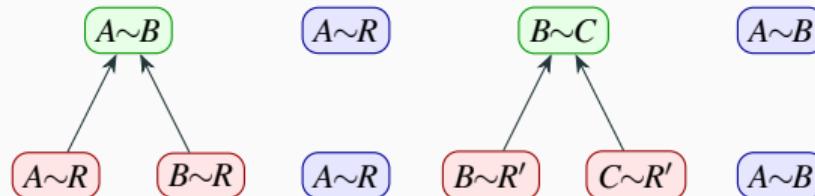
$\text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



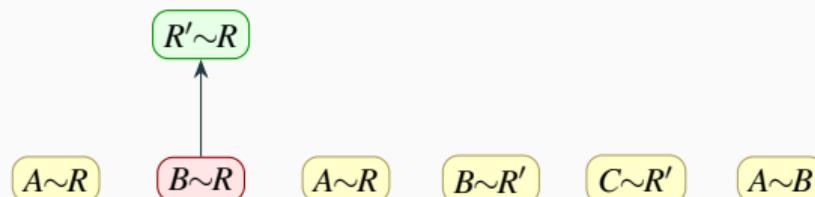
Bell pairs: **consumed**, **produced** and **untouched**

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



$\text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$

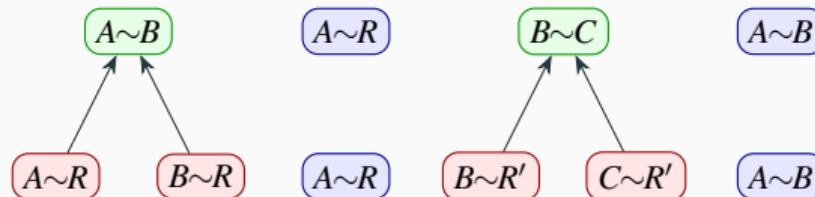


---

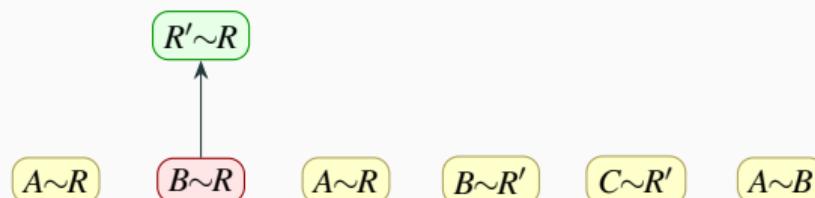
Bell pairs: **consumed**, **produced** and **untouched**

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



$\text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$

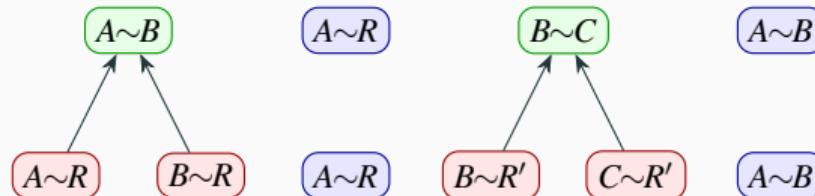


---

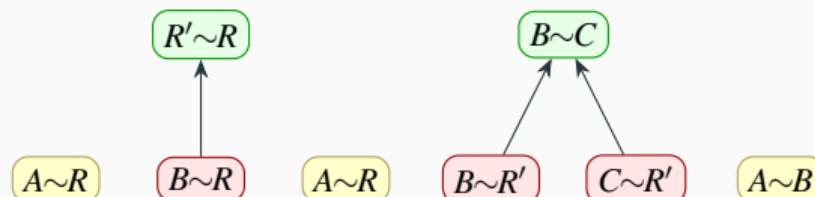
Bell pairs: **consumed**, **produced** and **untouched**

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



$\text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$

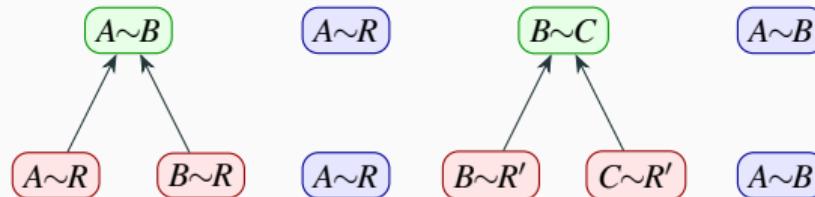


---

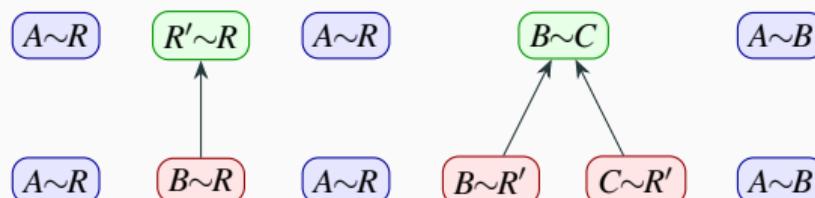
Bell pairs: **consumed**, **produced** and **untouched**

# Parallel composition vs. ordered composition

$\text{sw}\langle A \sim B @ R \rangle \cdot \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$



$\text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \cdot \text{sw}\langle A \sim B @ R \rangle \cdot \text{sw}\langle B \sim C @ R' \rangle$

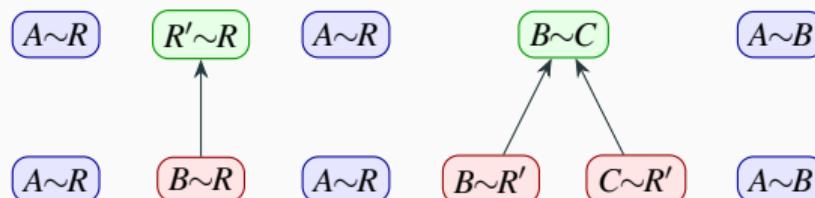
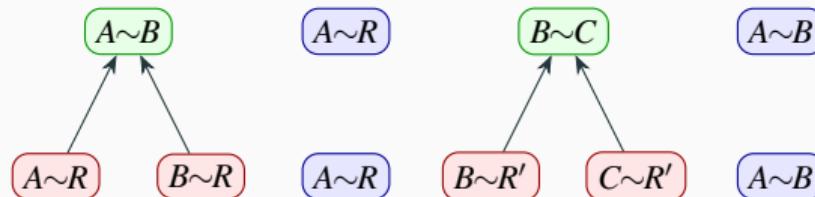


---

Bell pairs: **consumed**, **produced** and **untouched**

# Parallel composition vs. ordered composition

$$\text{sw}\langle A \sim B @ R \rangle \| \text{tr}\langle B \sim R \rightarrow R' \sim R \rangle \| \text{sw}\langle B \sim C @ R' \rangle$$



---

Bell pairs: **consumed**, **produced** and **untouched**

## Verification - properties with a classical analogue

- *Reachability.* Will the execution of our protocol generate  $A \sim C$ ?

## Verification - properties with a classical analogue

- *Reachability.* Will the execution of our protocol generate  $A \sim C$ ?
- *Waypoint Correctness.* Does our protocol ever perform a swap at node  $B$ ?

## Verification - properties with a classical analogue

- *Reachability.* Will the execution of our protocol generate  $A \sim C$ ?
- *Waypoint Correctness.* Does our protocol ever perform a swap at node  $B$ ?
- *Traffic (Protocol) Isolation.* Can we prove non-interference in a composition of Protocols I and II?

## Verification - properties with a classical analogue

- *Reachability.* Will the execution of our protocol generate  $A \sim C$ ?
- *Waypoint Correctness.* Does our protocol ever perform a swap at node  $B$ ?
- *Traffic (Protocol) Isolation.* Can we prove non-interference in a composition of Protocols I and II?
- *Compilation.* Can we ensure correct compilation to individual devices?

## Verification - properties specific to quantum

- *Resource Utilization.* What is the number of required memory locations and communication qubits? For how many rounds must a Bell pair wait in the memory?

## Verification - properties specific to quantum

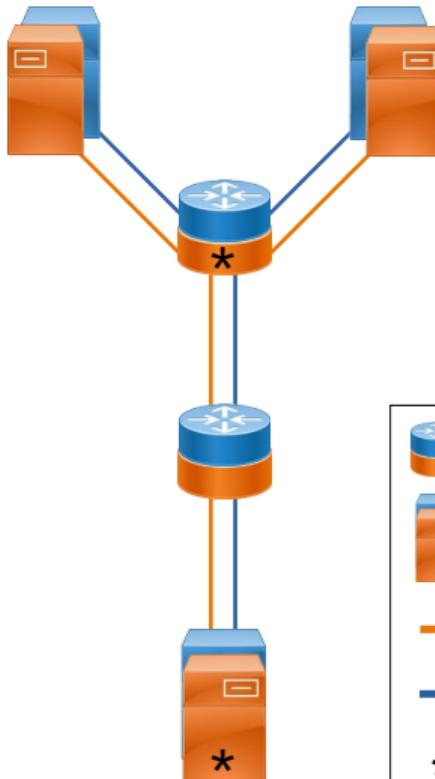
- *Resource Utilization.* What is the number of required memory locations and communication qubits? For how many rounds must a Bell pair wait in the memory?
- *Quality of Service.* Do the generated Bell pairs have the required fidelity or capacity?

## Verification - properties specific to quantum

- *Resource Utilization.* What is the number of required memory locations and communication qubits? For how many rounds must a Bell pair wait in the memory?
- *Quality of Service.* Do the generated Bell pairs have the required fidelity or capacity?
- *Compilation.* Can we minimize the number of accesses to the network global state?



# Quantum network

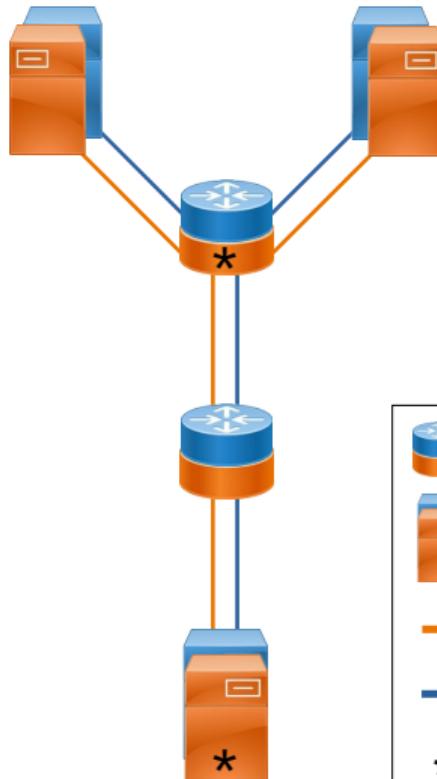


**What/Key service:**  
providing *communication services* to distributed quantum applications

**How:** end-to-end  
Bell pair distribution<sup>2</sup>

<sup>1</sup>[Kozlowski, Wehner NANOCOM 2019], <sup>2</sup>[RFC 9340 IRTF–QIRG 2023]

# Quantum network



**What/Key service:**  
providing *communication services* to distributed quantum applications

1 **How:** end-to-end  
Bell pair distribution<sup>2</sup>

secure communication

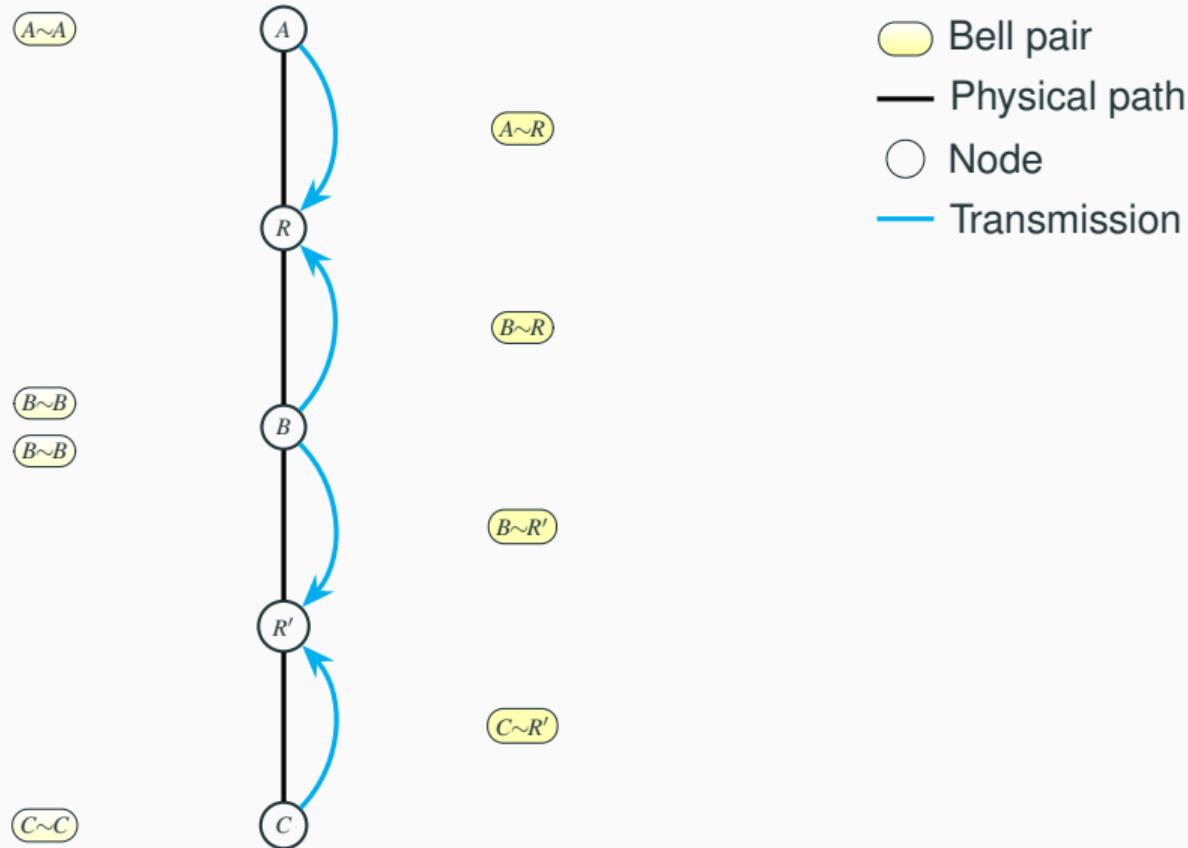
secure quantum computing in the cloud

clock synchronization  
password identification  
position verification

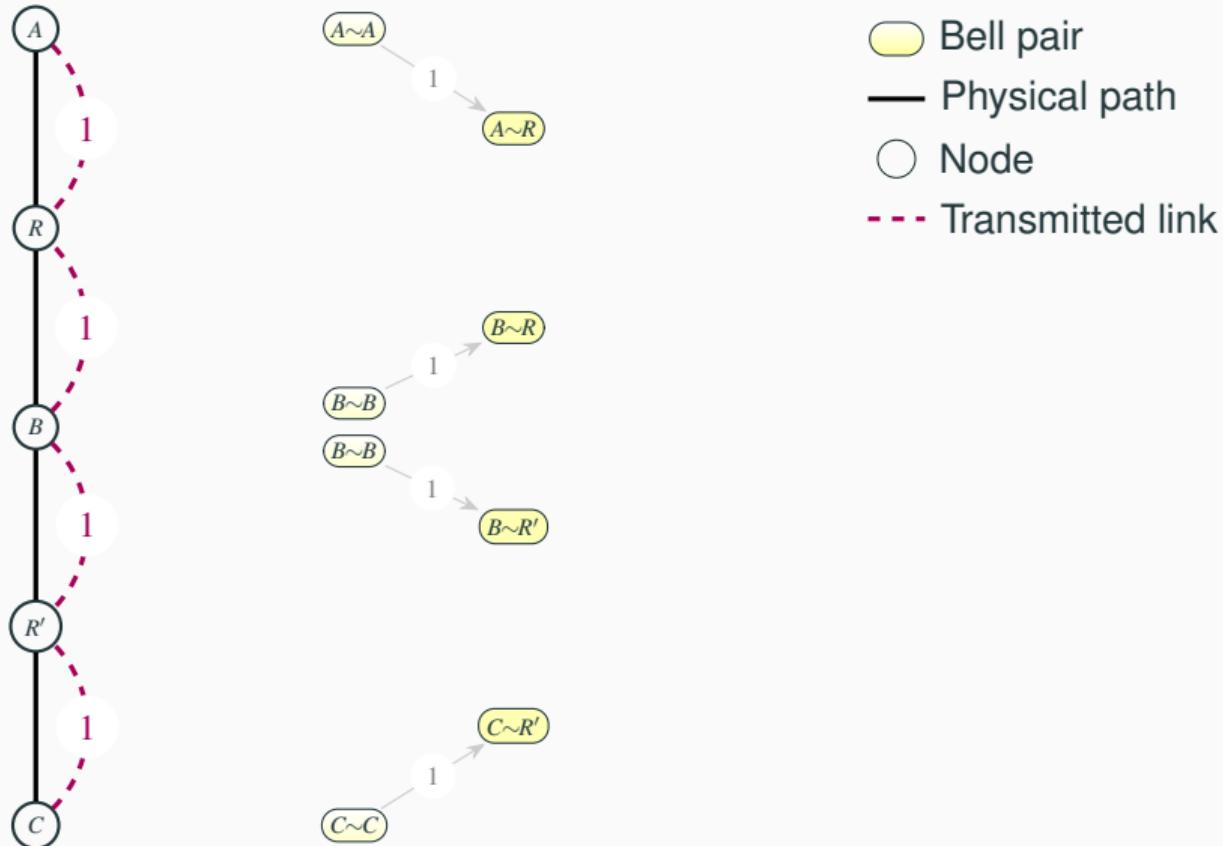
quantum computing clusters

<sup>1</sup>[Kozlowski, Wehner NANOCOM 2019], <sup>2</sup>[RFC 9340 IRTF–QIRG 2023]

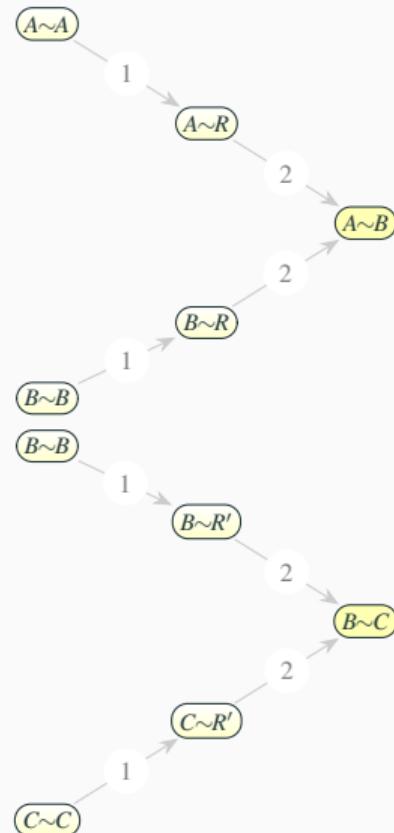
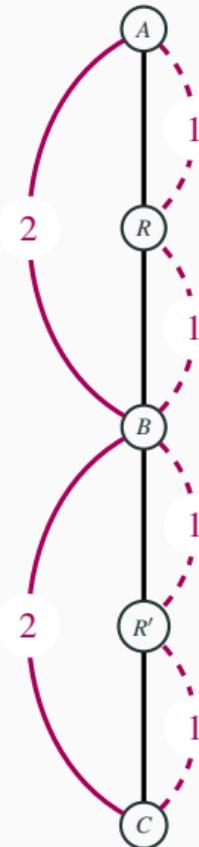
# Bell pair generation: Protocol I



## Bell pair generation: Protocol I, round 1

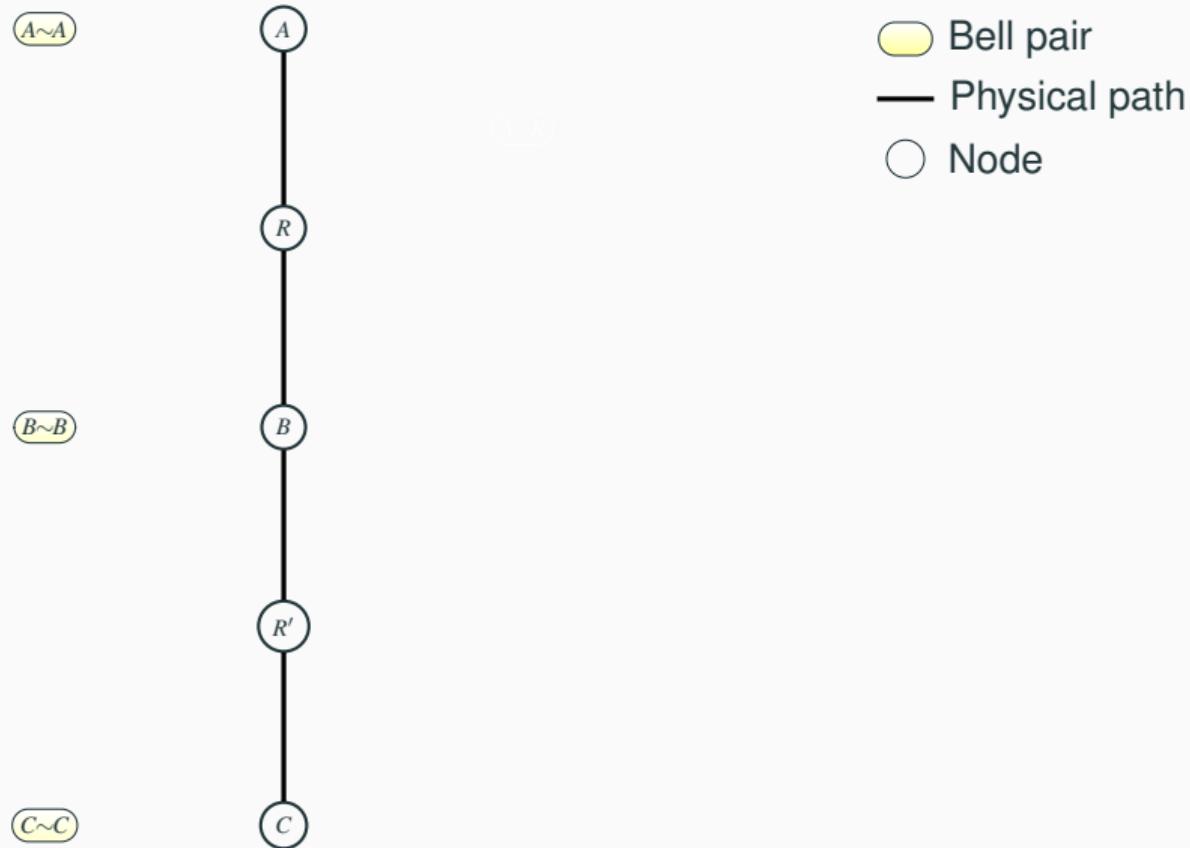


## Bell pair generation: Protocol I, round 2

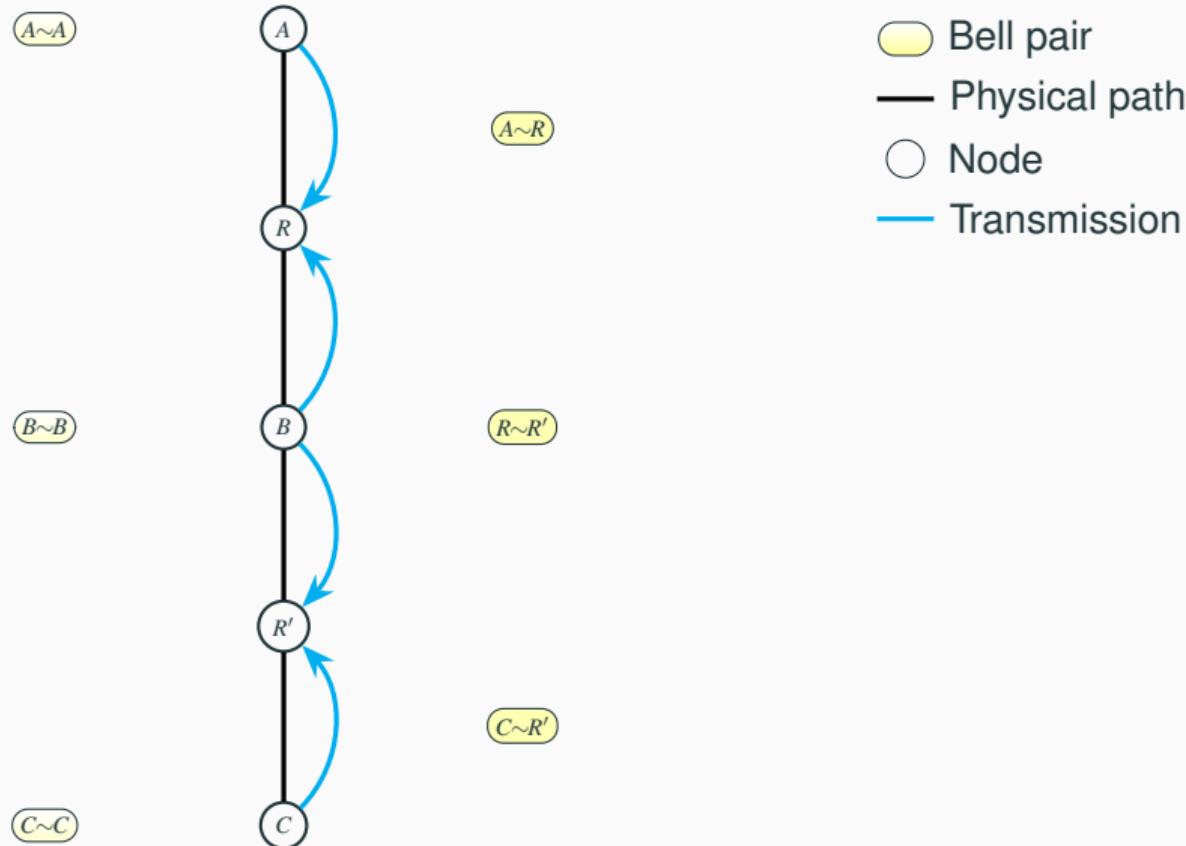


- Bell pair
- Physical path
- Node
- Transmitted link
- Swapped link

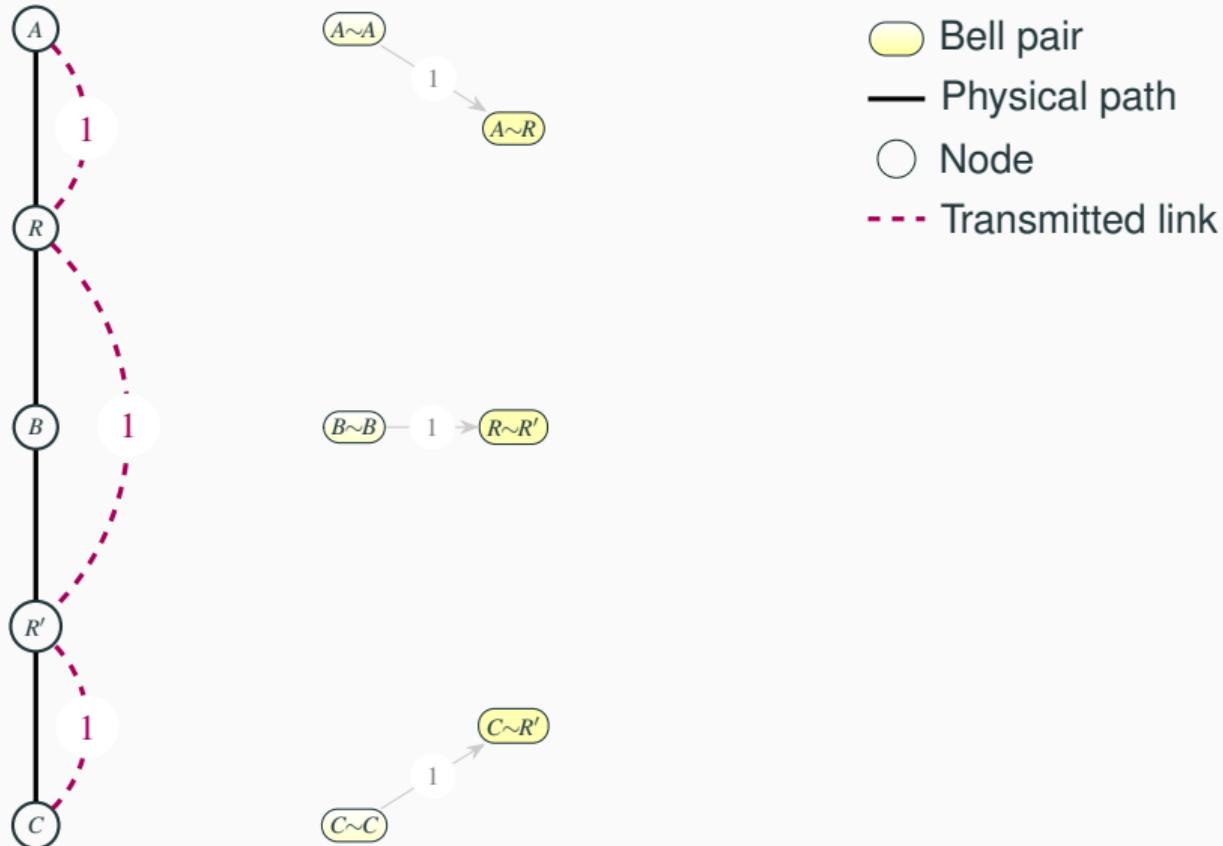
## Bell pair generation: Protocol II



## Bell pair generation: Protocol II



## Bell pair generation: Protocol II, round 1



## Bell pair generation: Protocol II, round 2

