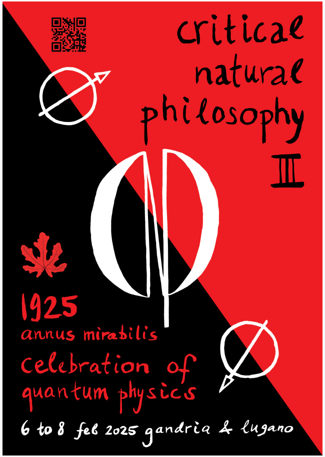
The Language of Quantum Networks

From Physical Experiment to Language

Anita Buckley

SWYSTEMS group
Università della Svizzera italiana

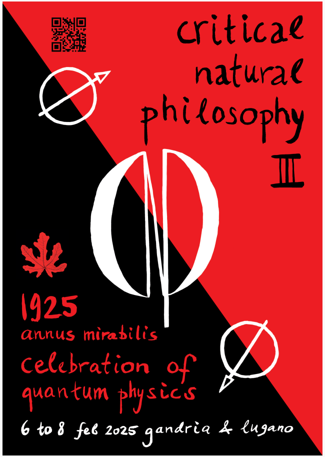


The Language of Quantum Networks

From Physical Experiment to Language

Anita Buckley

SWYSTEMS group
Università della Svizzera italiana

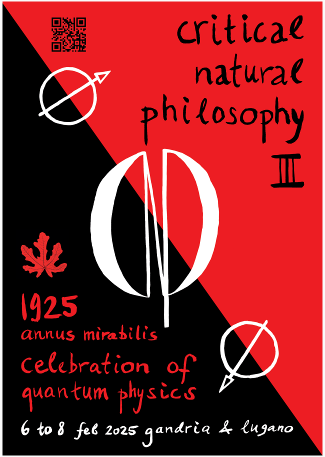


The Language of Quantum Networks

From Physical Experiment to Language

Anita Buckley

SWYSTEMS group
Università della Svizzera italiana

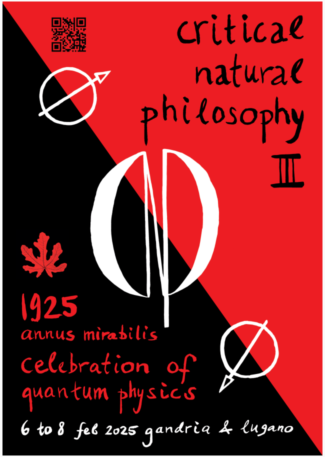


The Language of Quantum Networks

From Physical Experiment to Language

Anita Buckley

SWYSTEMS group
Università della Svizzera italiana

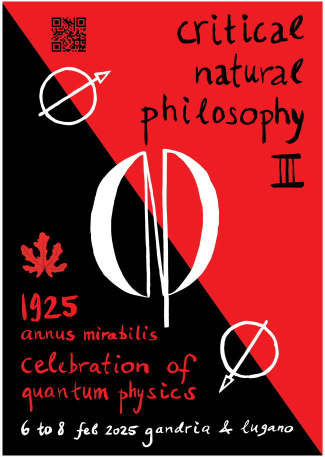


The Language of Quantum Networks

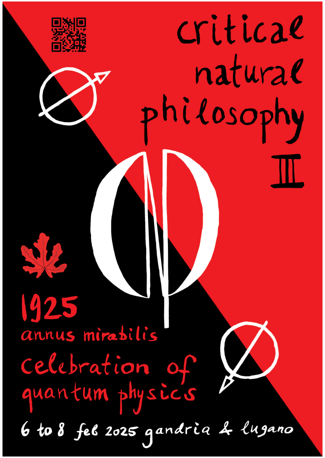
From Physical Experiment to Language

Anita Buckley

SWYSTEMS group
Università della Svizzera italiana



Reasoning



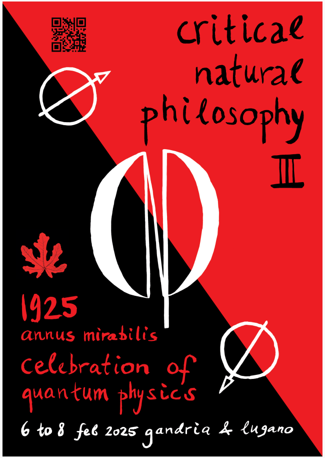
reason

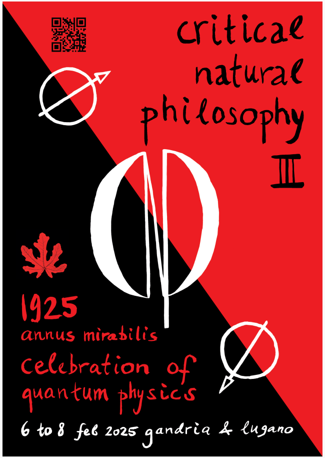
understanding

knowledge

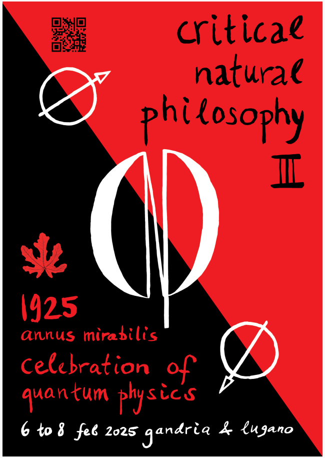
truth

limitations

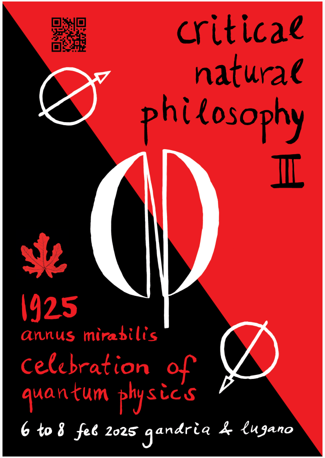

critical
natural
philosophy
III
1925
annus mirabilis
celebration of
quantum physics
6 to 8 feb 2025 gandria & lugano



- Kant: the “thorough grounding” that mathematics finds in its definitions, axioms, and demonstrations cannot be “achieved or imitated” by philosophy or physical sciences

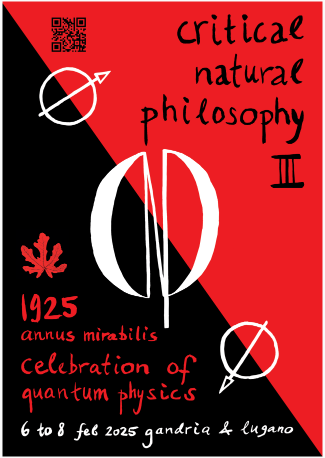


- Hegel: "reality/being $\equiv$ thought"



- Hegel: “reality/being $\equiv$ thought”
- Hilbert’s program: “truth $\equiv$ proof”

mathematical understanding = having “satisfactory” solutions that usually provide (explicitly or implicitly) mechanical procedures, which when applied to an object, determine (in finite time) whether it has the property

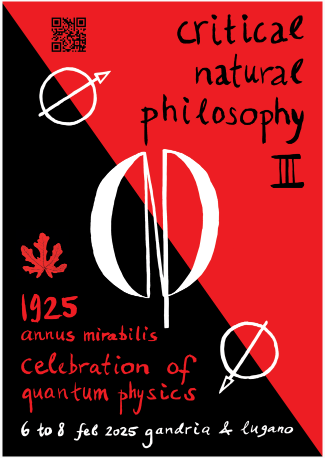


- Hegel: "reality/being $\equiv$ thought"
- Hilbert's program: "truth $\equiv$ proof"

> mathematical understanding = having "satisfactory" solutions that usually provide (explicitly or implicitly) mechanical procedures, which when applied to an object, determine (in finite time) whether it has the property

- Gödel, Church, Post, Turing: formal definitions of computation (identical in power)

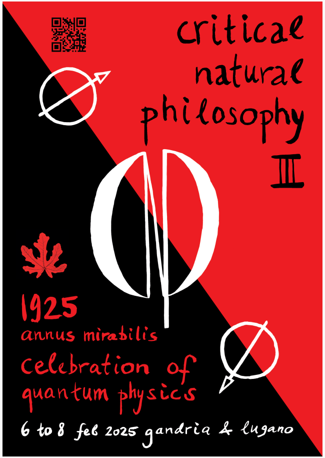
Mathematical reasoning



- Hegel: "reality/being $\equiv$ thought"
- Hilbert's program: "truth $\equiv$ proof"

mathematical understanding = having "satisfactory" solutions that usually provide (explicitly or implicitly) mechanical procedures, which when applied to an object, determine (in finite time) whether it has the property

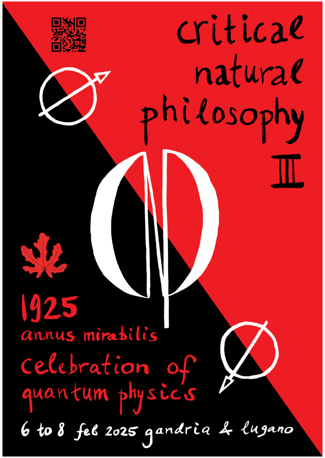
- Gödel, Church, Post, Turing: formal definitions of computation (identical in power)
- TM: limits to mathematical knowledge



hunt/gather food
run away
social activities
communication

} problem solving

Human thinking

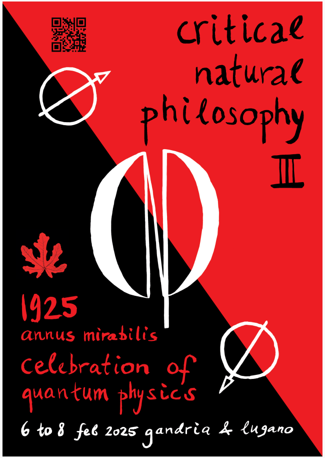


hunt/gather food
run away
social activities
communication

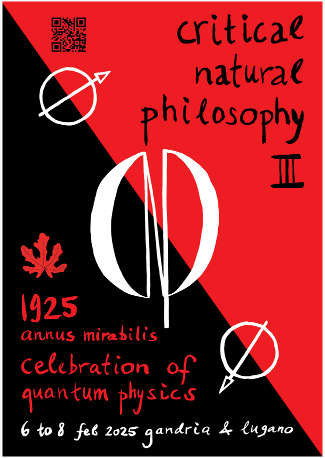
} problem solving {

relations
decomposing
grouping
language

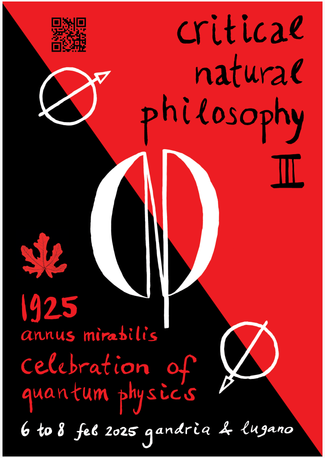
Human thinking



hunt/gather food run away social activities communication	}	problem solving	{	relations decomposing grouping language
STRUCTURE				ABSTRACTION



hunt/gather food run away social activities communication	problem solving	relations decomposing grouping language
STRUCTURE	IDENTITY	ABSTRACTION

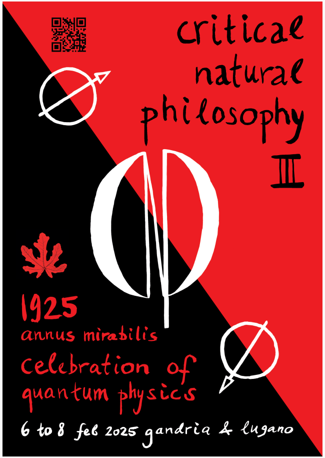


hunt/gather food
run away
social activities
communication

} problem solving {

relations
decomposing
grouping
language

COMPOSITION IDENTITY ABSTRACTION



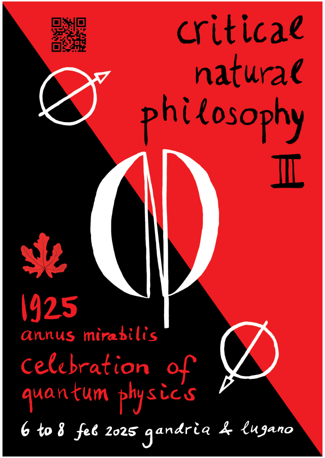
hunt/gather food
run away
social activities
communication

problem solving

relations
decomposing
grouping
language

COMPOSITION IDENTITY ABSTRACTION

CATEGORY THEORY



hunt/gather food
run away
social activities
communication

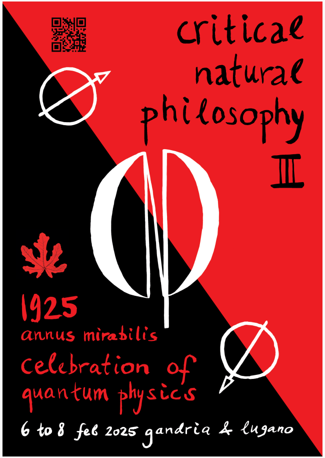
} problem solving {

relations
decomposing
grouping
language

COMPOSITION IDENTITY ABSTRACTION

CATEGORY THEORY

> Turing: “Mathematical reasoning may be regarded rather schematically as the exercise of a combination of two facilities, which we may call intuition and ingenuity.”



hunt/gather food
run away
social activities
communication

} problem solving {

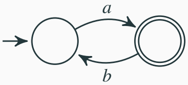
relations
decomposing
grouping
language

COMPOSITION IDENTITY ABSTRACTION

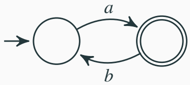
CATEGORY THEORY

Hardy: "I am interested in mathematics only as a creative art."

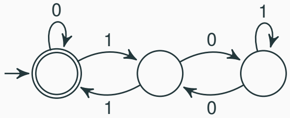
$(ab)^*a \equiv a(ba)^*$ $\{a, aba, ababa, \ldots\}$



$(ab)^*a \equiv a(ba)^*$ $\{a, aba, ababa, \ldots\}$

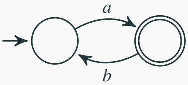


$\big(0 + 1(01^*0)^*1\big)^*$ multiples of 3

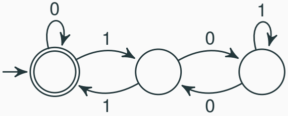


regular expressions – regular languages – finite automata

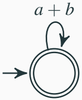
$(ab)^*a \equiv a(ba)^*$ $\{a, aba, ababa, \ldots\}$



$\big(0 + 1(01^*0)^*1\big)^*$ multiples of 3



$(a+b)^* \equiv a^*(ba^*)^*$ all strings over a, b



Kleene algebra axioms

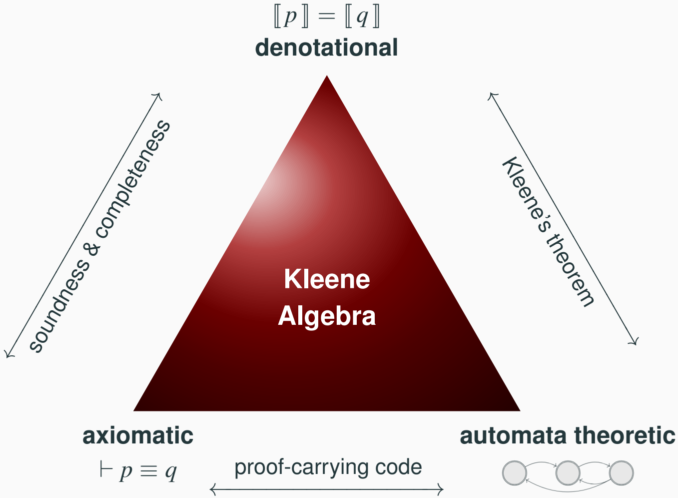
$$
\begin{array}{rcl}
p+(q+r) & \equiv & (p+q)+r \\
p+q & \equiv & q+p \\
p+0 & \equiv & p \\
p+p & \equiv & p \\
p\cdot(q\cdot r) & \equiv & (p\cdot q)\cdot r \\
1\cdot p & \equiv & p \\
p\cdot 1 & \equiv & p \\
p\cdot(q+r) & \equiv & p\cdot q+p\cdot r \\
(p+q)\cdot r & \equiv & p\cdot r+q\cdot r \\
0\cdot p & \equiv & 0 \\
p\cdot 0 & \equiv & 0 \\
1+p\cdot p^* & \equiv & p^* \\
q+p\cdot r\leq r & \Rightarrow & p^*\cdot q\leq r \\
1+p^*\cdot p & \equiv & p^* \\
p+q\cdot r\leq q & \Rightarrow & p\cdot r^*\leq q
\end{array}
$$

$(ab)^*a \equiv a(ba)^*$ $\{a, aba, ababa, \ldots\}$

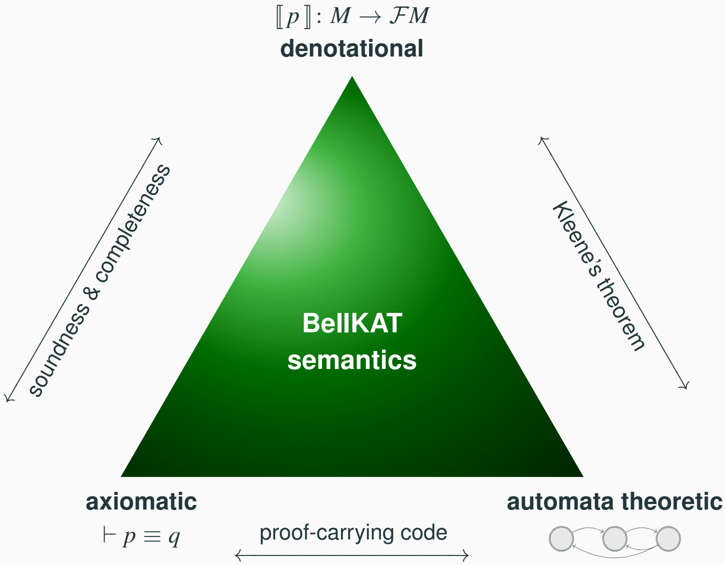
$\left(0+1(01^*0)^*1\right)^*$ multiples of 3

$(a+b)^* \equiv a^*(ba^*)^*$ all strings over a, b

Kleene algebra semantics



BellKAT semantics

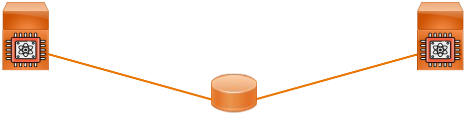


Quantum networks are networks connecting quantum capable devices

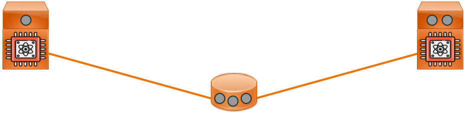
Quantum networks

Quantum networks are networks connecting quantum capable devices

Quantum networks are networks connecting quantum capable devices

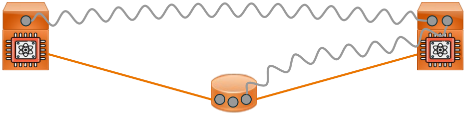


Quantum networks are networks connecting quantum capable devices



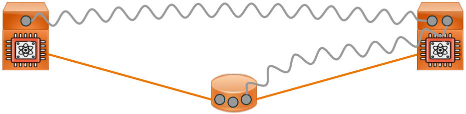
– **Communication qubits** designated to establish *connections* between devices

Quantum networks are networks connecting quantum capable devices



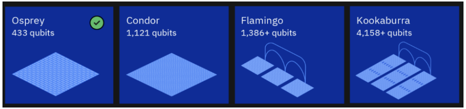
- **Communication qubits** designated to establish *connections* between devices
- Distributed **entanglement:** communication qubits sharing a *correlated random secret*

Quantum networks 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**



[1]

- teleportation
- entanglement based QKD

[1] [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,[1,2,8,15,34] there will be a need for a fundamentally different network structure: the quantum Internet.[22,25,32,33,45,47] 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.[a]

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,[b] 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 adds 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

a While "supremacy" is a concept used to describe the theory of computational complexity[1,15] 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.

b 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.**

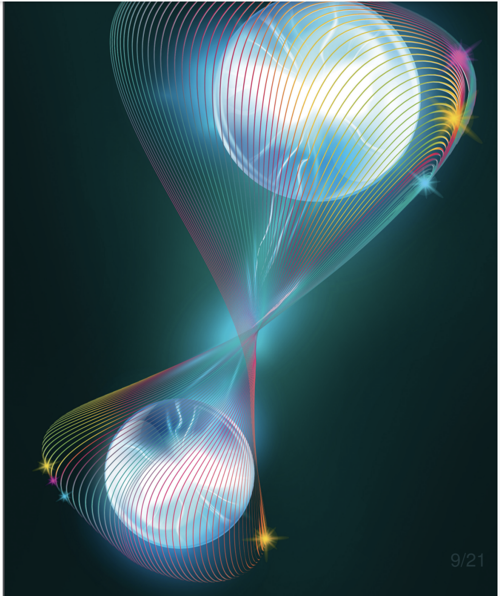
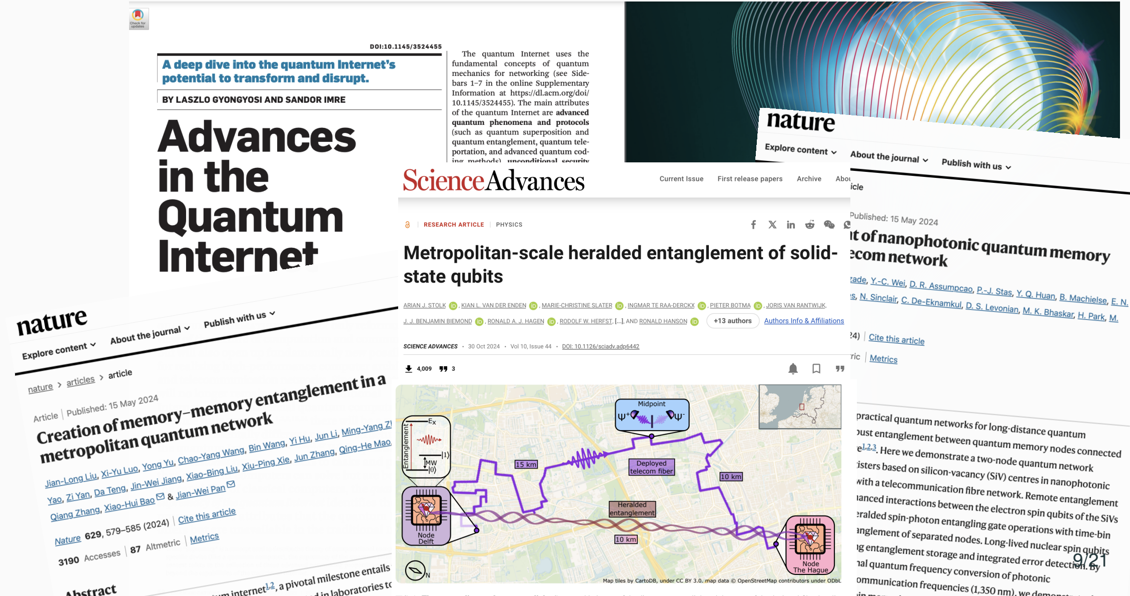


IMAGE BY ANDRIJ BORYS ASSOCIATES, USING SHUTTERSTOCK

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

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 cod-ing methods), **unconditional security**

ScienceAdvances

Current Issue · First release papers · Archive · Abou

RESEARCH ARTICLE | PHYSICS

Metropolitan-scale heralded entanglement of solid-state qubits

ARIAN J. STOLK, KIAN L. VAN DER ENDEN, MARIE-CHRISTINE SLATER, INGMAR TE RAA-DERCKX, PIETER BOTMA, JORIS VAN RANTWIJK, J. J. BENJAMIN BIEMOND, RONALD A. J. HAGEN, RODOLF W. HERFST, [...], AND RONALD HANSON +13 authors Authors Info & Affiliations

SCIENCE ADVANCES · 30 Oct 2024 · Vol 10, Issue 44 · DOI: 10.1126/sciadv.adp6442

4,009 · 3

nature

Explore content · About the journal · Publish with us

nature > articles > article

Article | Published: 15 May 2024

Creation of memory–memory entanglement in a metropolitan quantum network

Jian-Long Liu, Xi-Yu Luo, Yong Yu, Chao-Yang Wang, Bin Wang, Yi Hu, Jun Li, Ming-Yang Zh..., Yao, Zi Yan, Da Teng, Jin-Wei Jiang, Xiao-Bing Liu, Xiu-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

...um internet[1,2], a pivotal milestone entails ...d in laboratories to...

nature

Explore content · About the journal · Publish with us

...icle

Published: 15 May 2024

...t of nanophotonic quantum memory ...ecom network

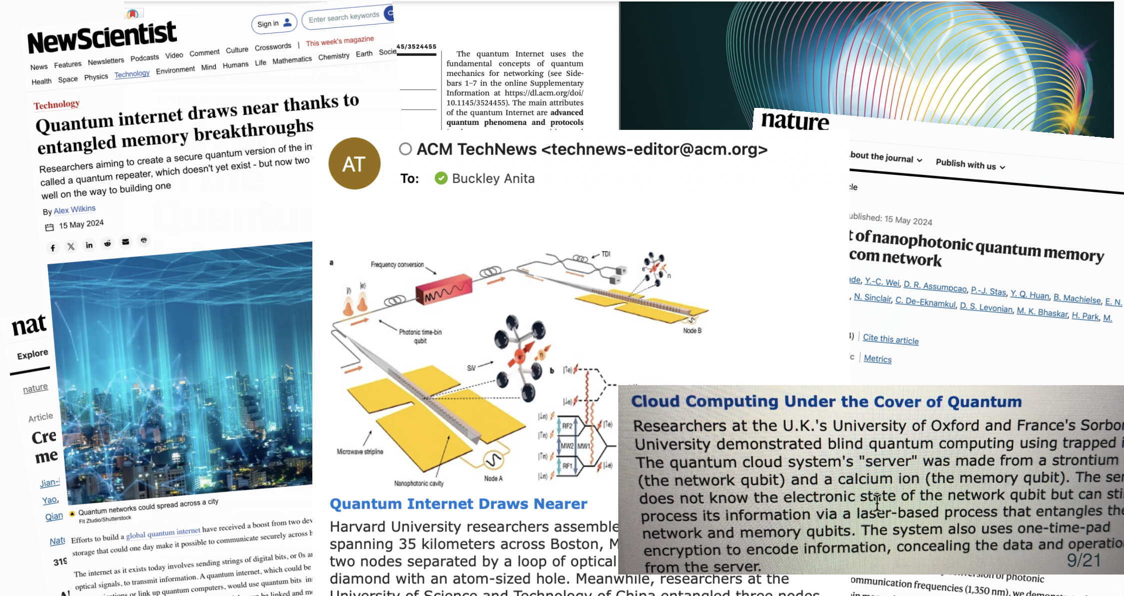
...ade, Y.-C. Wei, D. R. Assumpcao, P.-J. Stas, Y. Q. Huan, B. Machielse, E. N. ...s, N. Sinclair, C. De-Eknamkul, D. S. Levonian, M. K. Bhaskar, H. Park, M. ...

...24) | Cite this article

...ric | Metrics

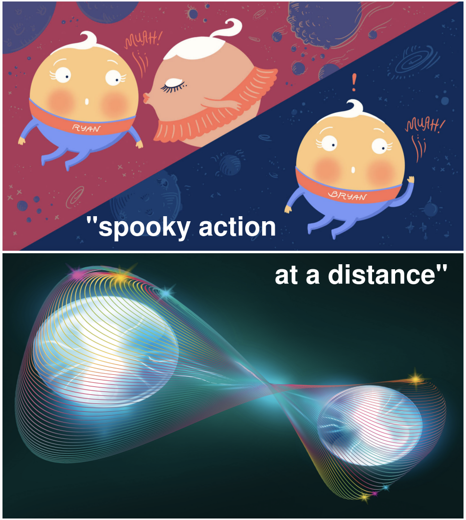
...practical quantum networks for long-distance quantum ...bust entanglement between quantum memory nodes connected ...e[1,2,3]. Here we demonstrate a two-node quantum network ...isters based on silicon-vacancy (SiV) centres in nanophotonic ...with a telecommunication fibre network. Remote entanglement ...hanced interactions between the electron spin qubits of the SiVs ...eralded spin-photon entangling gate operations with time-bin ...anglement of separated nodes. Long-lived nuclear spin qubits ...g entanglement storage and integrated error detection. By ...nal quantum frequency conversion of photonic ...ommunication frequencies (1,350 nm), we demonstr...

Quantum networks are coming into reality



Bell pair: a pair of entangled qubits

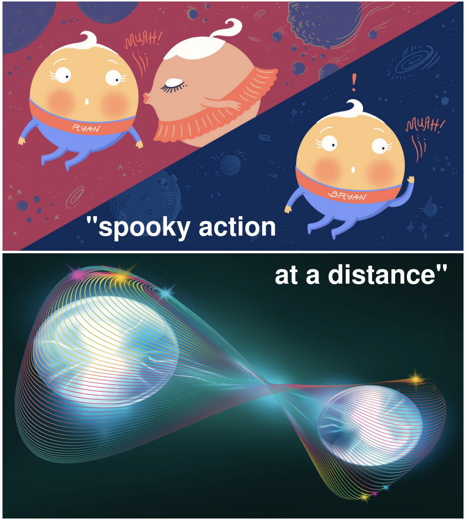
- Fundamental *resource* in quantum networks
- *Bell pair* is a pair of entangled qubits: $R{\sim}B$ distributed between nodes R and B
- No headers: control information needs to be sent via separate classical channels



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

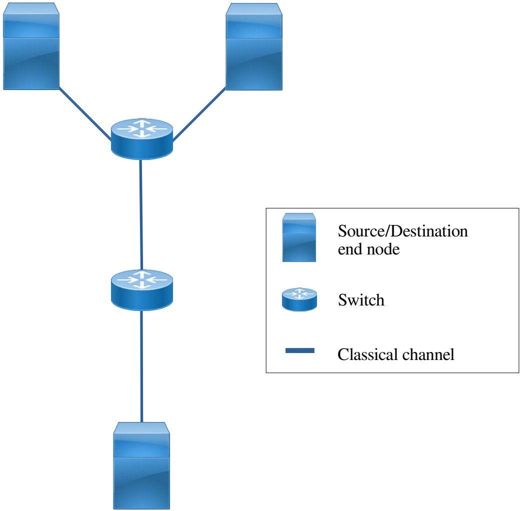
Bell pair: a pair of entangled qubits

- 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

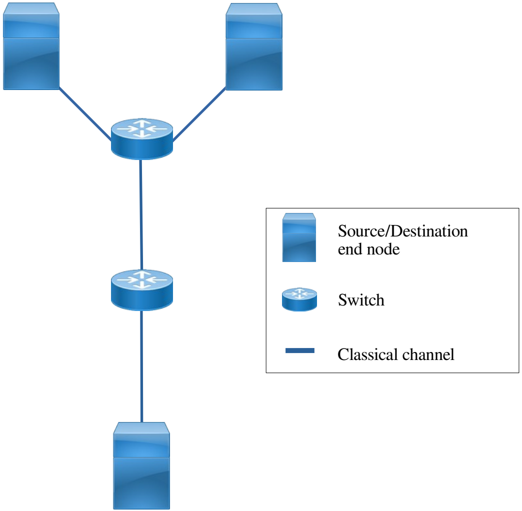


Artwork by Sandbox Studio, Chicago with Ana Kova
Image by Andrij Borys Associates, using Shutterstock

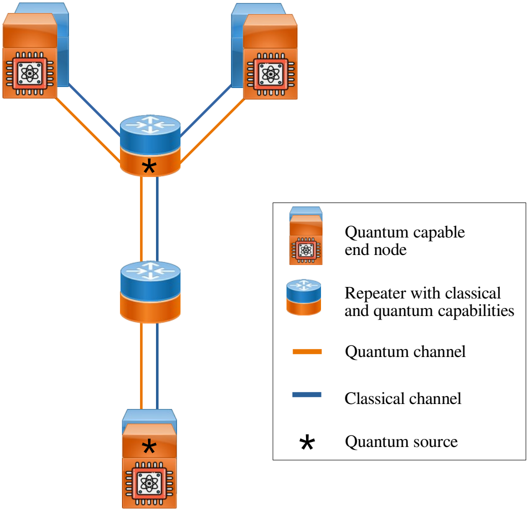
Classical network



Classical network

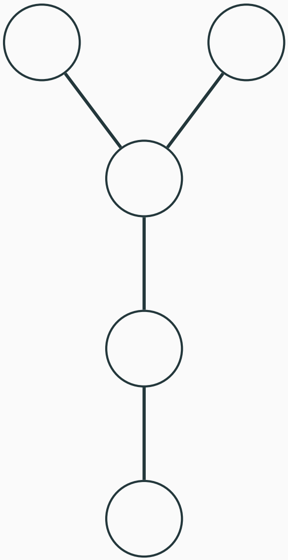


Quantum network [1,2]

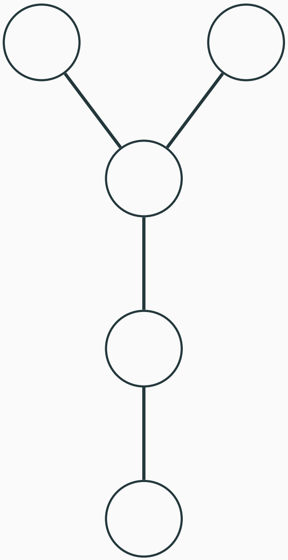


[1][Kozlowski and Wehner: NANOCOM *2019*], [2][Quantum Internet Research Group: RFC 9340 *2023*]

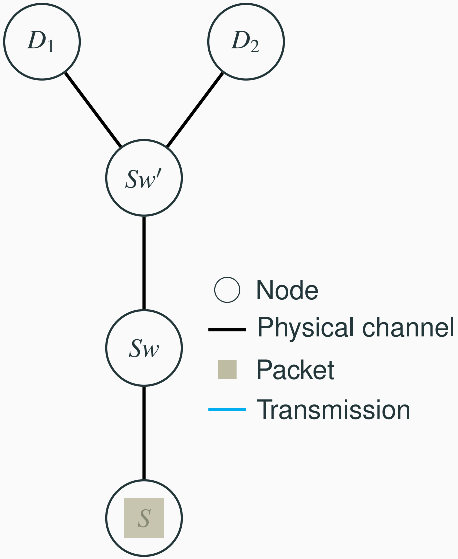
Classical network



Quantum network

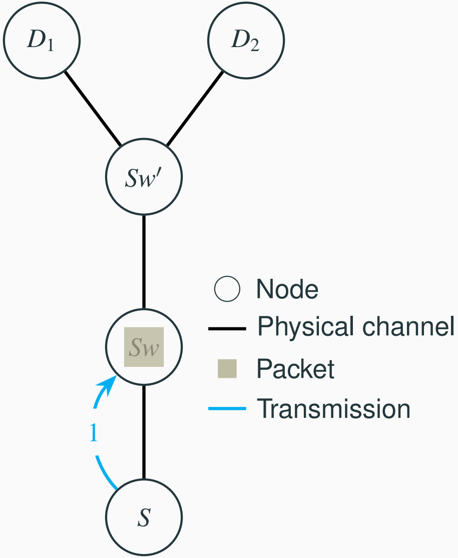


Forwarding packets



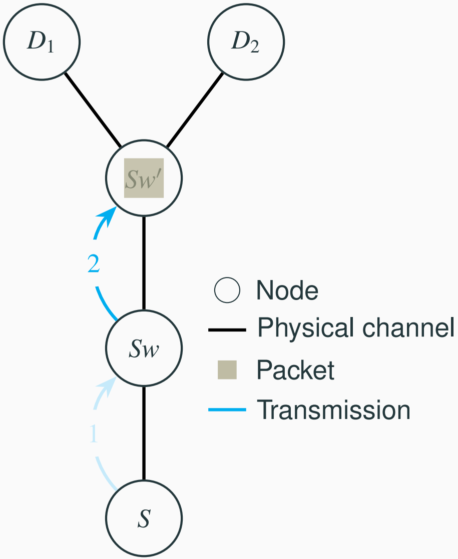
Distributing Bell pairs

Forwarding packets



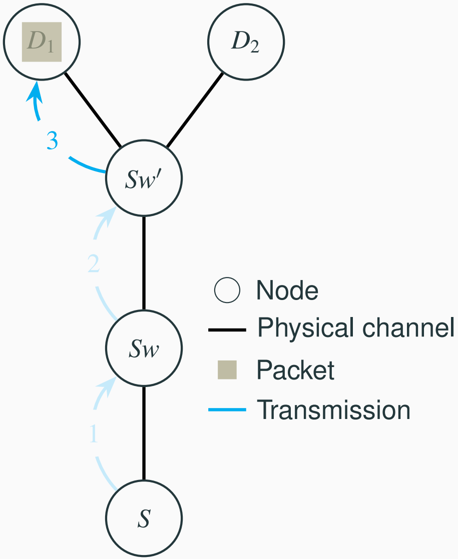
Distributing Bell pairs

Forwarding packets



Distributing Bell pairs

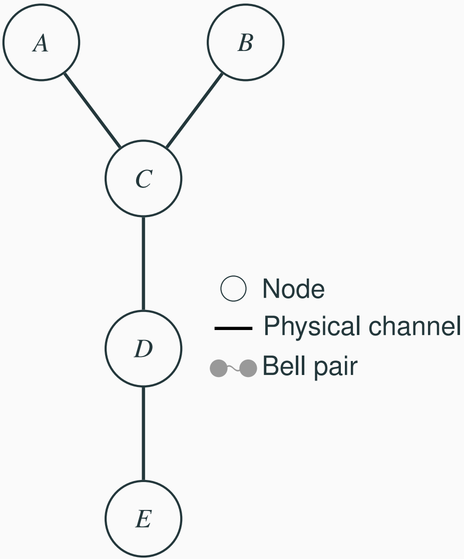
Forwarding packets



Distributing Bell pairs

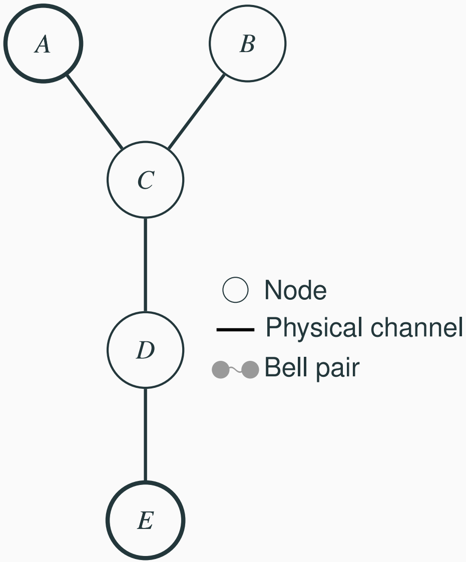
Forwarding packets

Distributing Bell pairs



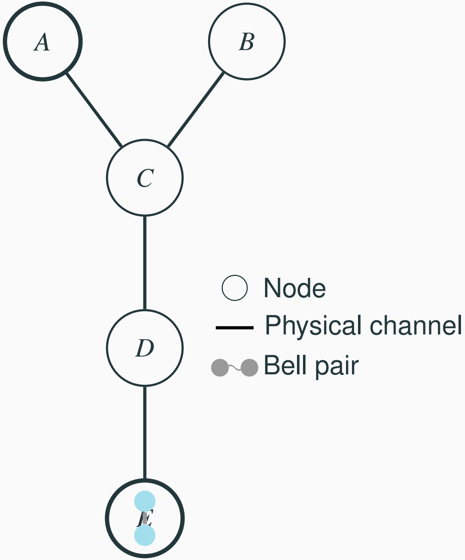
Forwarding packets

Distributing Bell pairs



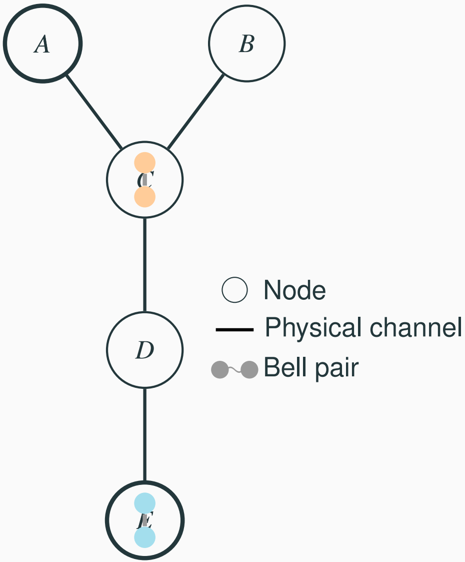
Forwarding packets

Distributing Bell pairs



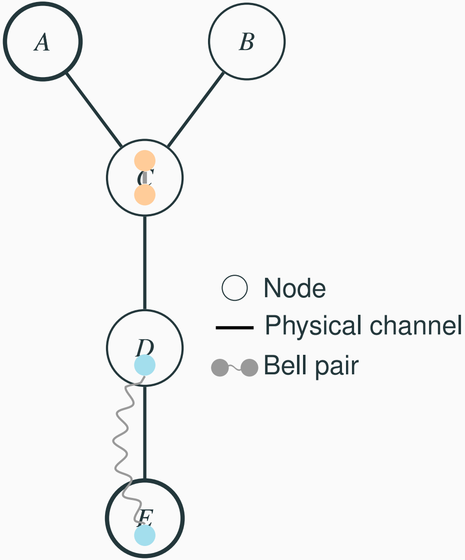
Forwarding packets

Distributing Bell pairs



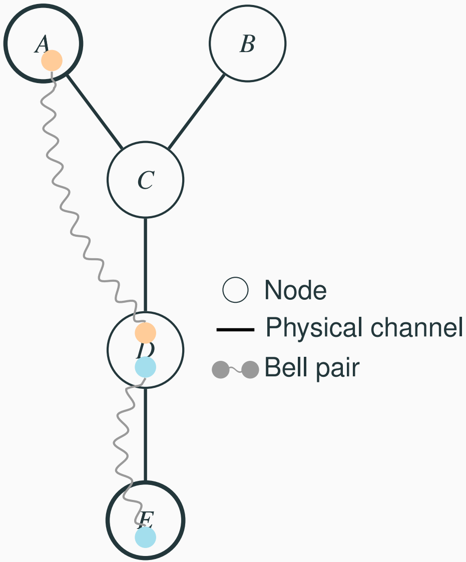
Forwarding packets

Distributing Bell pairs



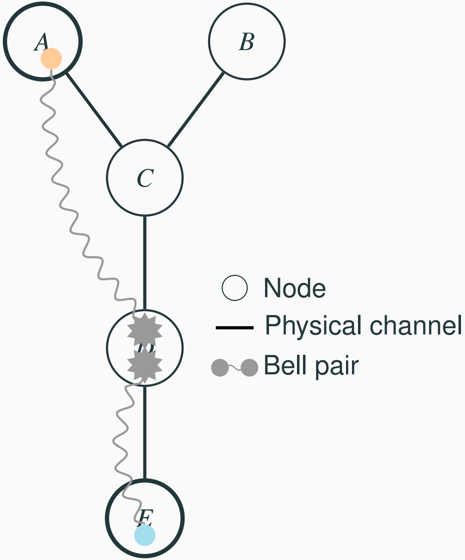
Forwarding packets

Distributing Bell pairs



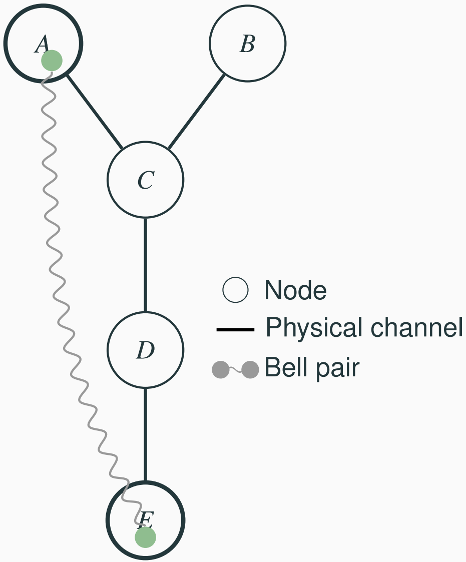
Forwarding packets

Distributing Bell pairs

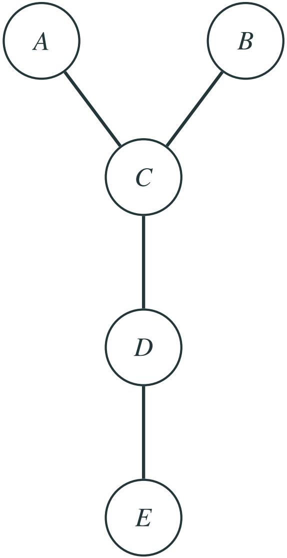


Forwarding packets

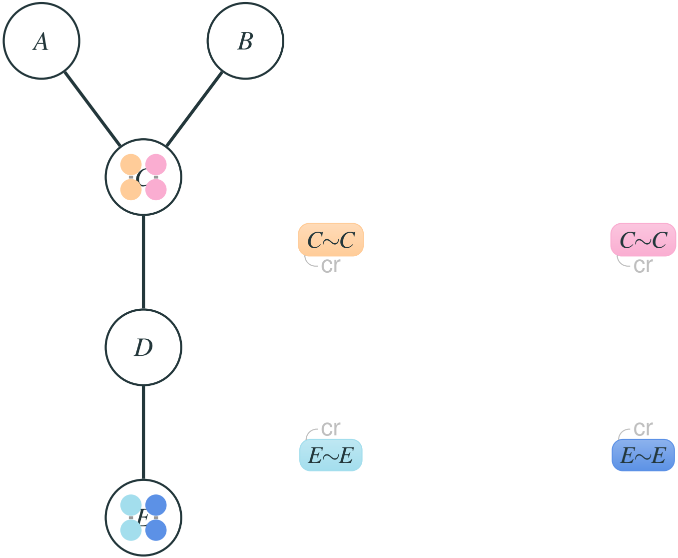
Distributing Bell pairs

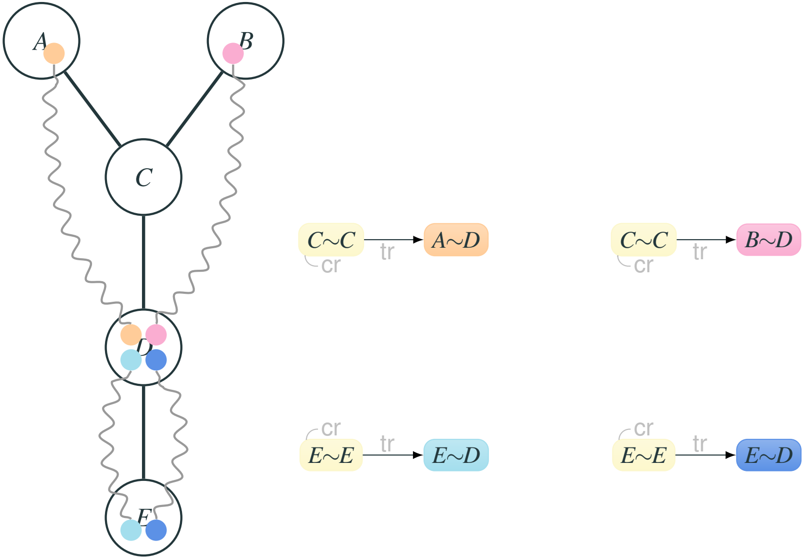


End-to-end Bell pair generation protocol

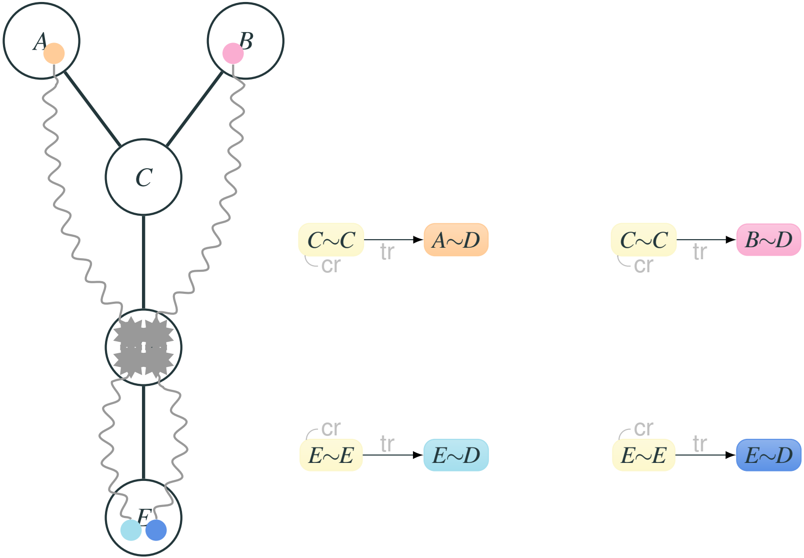


End-to-end Bell pair generation protocol

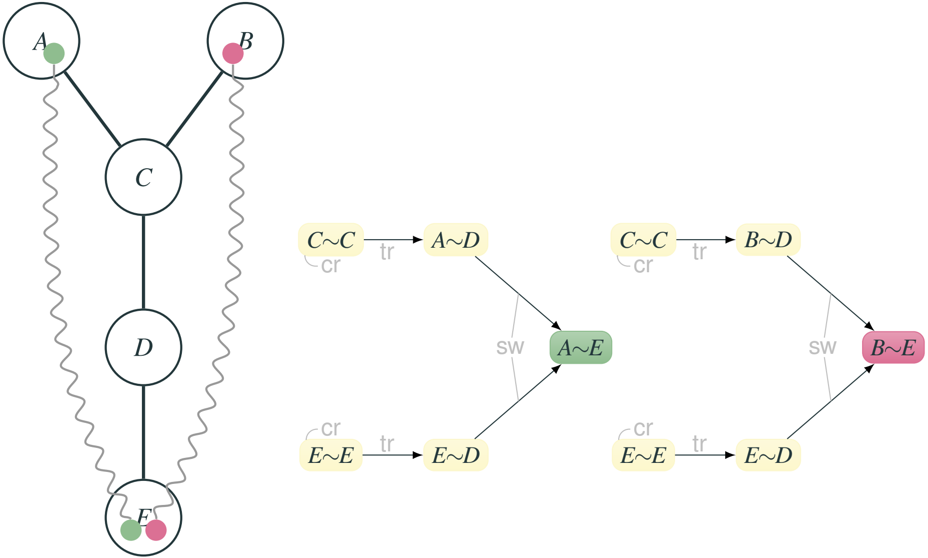



A
B
C
D
F
C∼C
cr
tr
A∼D
C∼C
cr
tr
B∼D
cr
E∼E
tr
E∼D
cr
E∼E
tr
E∼D

End-to-end Bell pair generation protocol



End-to-end Bell pair generation protocol



Verification and optimization

PROBLEM

How to make sure that quantum networks behave as intended?

PROBLEM

How to make sure that quantum networks behave as intended?

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

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?

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?

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?

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 as foundation to answer these types of questions

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 as foundation to answer these types of questions

BellKAT language

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

BellKAT language

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

BellKAT language

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

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

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

r, o, a : multisets of Bell pairs $\quad \bowtie$: pair of multisets of Bell pairs

BellKAT primitives – basic actions

required BPs

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

r, o, a : multisets of Bell pairs $\quad \bowtie$: pair of multisets of Bell pairs

BellKAT primitives – basic actions

required BPs

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

output BPs

r, o, a : multisets of Bell pairs $\quad \bowtie$: pair of multisets of Bell pairs

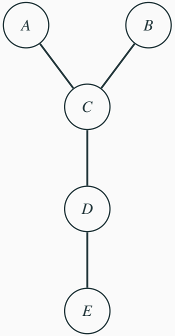
BellKAT primitives – basic actions

required BPs

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

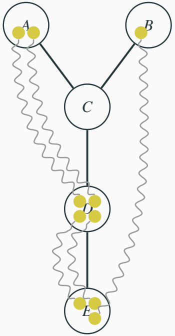
output BPs

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



required BPs — input BPs — output BPs

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



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

$A{\sim}D$ $D{\sim}E$ $A{\sim}D$ $D{\sim}E$ $B{\sim}E$

Input Bell pairs

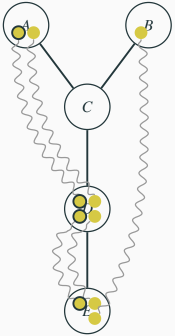
BellKAT primitives – basic actions

required BPs

input BPs

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

output BPs



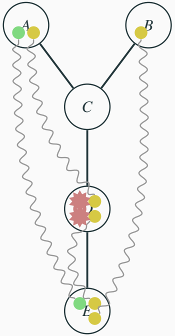
Swap $\{\{A{\sim}D, D{\sim}E\}\} \triangleright \{\{A{\sim}E\}\}$ acting on input $\{\{\underline{A{\sim}D}, A{\sim}D, \underline{D{\sim}E}, D{\sim}E, B{\sim}E\}\}$

$A{\sim}D$ $D{\sim}E$ $A{\sim}D$ $D{\sim}E$ $B{\sim}E$

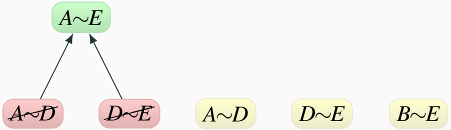
BellKAT primitives – basic actions

required BPs · input BPs · consumed BPs · output BPs · produced BPs

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



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



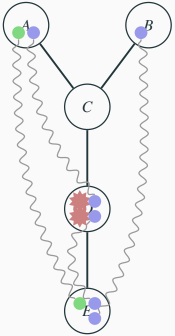
Input, consumed and produced Bell pairs

BellKAT primitives – basic actions

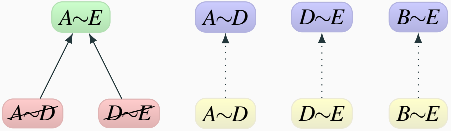
required BPs · input BPs · consumed BPs

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

output BPs · produced BPs · untouched BPs



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



Input, consumed, produced and untouched Bell pairs

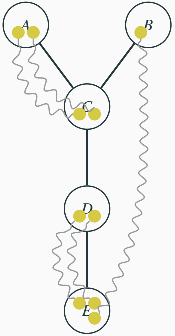
BellKAT primitives – basic actions

required BPs

input BPs

output BPs

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



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

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

Input, consumed, produced and untouched Bell pairs

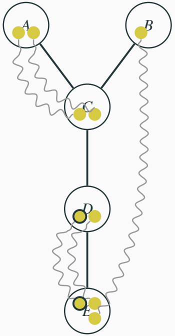
BellKAT primitives – basic actions

required BPs

input BPs

output BPs

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



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

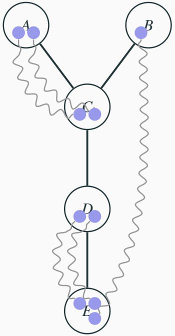
$A{\sim}C$ $D{\sim}E$ $A{\sim}C$ $D{\sim}E$ $B{\sim}E$

Input, consumed, produced and untouched Bell pairs

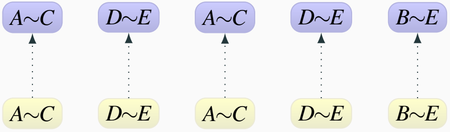
required BPs — input BPs

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

output BPs — produced BPs — untouched BPs



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	$\mathsf{sw}\langle A{\sim}B \,@\, C\rangle \triangleq \{\!\{A{\sim}C, B{\sim}C\}\!\} \triangleright \{\!\{A{\sim}B\}\!\}$
transmit	$\mathsf{tr}\langle A \rightarrow B{\sim}C\rangle \triangleq \{\!\{A{\sim}A\}\!\} \triangleright \{\!\{B{\sim}C\}\!\}$
create	$\mathsf{cr}\langle A\rangle \triangleq \emptyset \triangleright \{\!\{A{\sim}A\}\!\}$
wait	$\mathsf{wait}\langle r\rangle \triangleq r \triangleright r$
drop	$\mathsf{drop}\langle r\rangle \triangleq r \triangleright \emptyset$

BellKAT primitives – basic actions

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

BellKAT primitives – basic actions

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

BellKAT primitives – basic actions

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

BellKAT primitives – basic actions

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

BellKAT primitives – basic actions

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

BellKAT syntax

BellKAT syntax

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

BellKAT syntax

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

basic action

BellKAT syntax

abort

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

basic action

BellKAT syntax

skip

abort

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

basic action

BellKAT syntax

skip

abort

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

basic action

nondeterministic choice

BellKAT syntax

skip

abort

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

basic action

nondeterministic choice

sequential composition

BellKAT syntax

skip

abort

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

basic action

nondeterministic choice

Kleene star (iteration)

sequential composition

BellKAT syntax

skip

abort

basic action

parallel composition

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

Kleene star (iteration)

nondeterministic choice

sequential composition

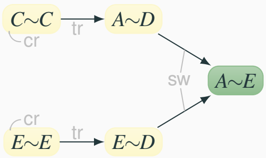
BellKAT syntax

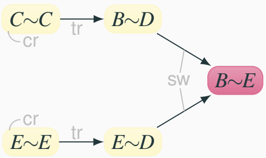
$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p \,;\, q \mid p^{\star}$$

- skip: 1
- abort: 0
- basic action: $r \triangleright o$
- nondeterministic choice: $p + q$
- ordered composition: $p \cdot q$
- parallel composition: $p \parallel q$
- sequential composition: $p \,;\, q$
- Kleene star (iteration): $p^{\star}$

Protocol specification in BellKAT

Protocol specification in BellKAT





Protocol specification in BellKAT

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

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

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

BellKAT at a glance

BellKAT at a glance

Syntax

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

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(BP) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \,\square\, t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP))$$

$$(\!| 0 |\!) a \triangleq \emptyset$$

$$(\!| 1 |\!) a \triangleq \{ \emptyset \bowtie a \}$$

$$(\!| [t]r \blacktriangleright o |\!) a \triangleq \begin{cases} \{ o \bowtie a \setminus r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!) a \triangleq (\!| p |\!) a \cup (\!| q |\!) a$$

$$(\!| p \cdot q |\!) a \triangleq ((\!| p |\!) \cdot (\!| q |\!)) a$$

$$(\!| p \parallel q |\!) a \triangleq ((\!| p |\!) \parallel (\!| q |\!)) a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$$

$$[\![\omega]\!]_I \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k$$

$$[\![p]\!] a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{ a \}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{ o \uplus a \setminus r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I) a$$

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	$1 + p\,;p^\star \equiv p^\star$	KA-Unroll-L
$p\,;(q+r) \equiv p\,;q + p\,;r$	KA-Seq-Dist-L	$p\,;r \le r \Rightarrow p^\star\,;r \le r$	KA-Lfp-L
$(p+q)\,;r \equiv p\,;r + q\,;r$	KA-Seq-Dist-R	$1 + p^\star\,;p \equiv p^\star$	KA-Unroll-R
		$r\,;p \le r \Rightarrow r\,;p^\star \le r$	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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	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

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \le (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

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

Test semantics

$$(\!|t|\!) \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$(\!|\mathbb{1}|\!)a \triangleq \top \qquad (\!|t \uplus b|\!)a \triangleq ((\!|t|\!)a \setminus b \wedge b \subseteq a) \vee (\!|b|\!)a$$

$$(\!|b|\!)a \triangleq b \not\subseteq a \qquad (\!|t \,\square\, t'|\!)a \triangleq (\!|t|\!)a \,\square\, (\!|t'|\!)a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!|p|\!) \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))$$

$$(\!|0|\!)a \triangleq \emptyset$$

$$(\!|1|\!)a \triangleq \{\emptyset \bowtie a\}$$

$$(\!|[t]r \blacktriangleright o|\!)a \triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } (\!|t|\!)a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!|p + q|\!)a \triangleq (\!|p|\!)a \cup (\!|q|\!)a$$

$$(\!|p \cdot q|\!)a \triangleq ((\!|p|\!) \cdot (\!|q|\!))a$$

$$(\!|p \parallel q|\!)a \triangleq ((\!|p|\!) \parallel (\!|q|\!))a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))$$

$$[\![\omega]\!]_I \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k$$

$$[\![p]\!]a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } (\!|t|\!)a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I)a$$

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	$1 + p \;;\; p^\star \equiv p^\star$	KA-Unroll-L
$p \;;\; (q+r) \equiv p \;;\; q + p \;;\; r$	KA-Seq-Dist-L	$p \;;\; r \leq r \Rightarrow p^\star \;;\; r \leq r$	KA-Lfp-L
$(p+q) \;;\; r \equiv p \;;\; r + q \;;\; r$	KA-Seq-Dist-R	$1 + p^\star \;;\; p \equiv p^\star$	KA-Unroll-R
		$r \;;\; p \leq r \Rightarrow r \;;\; p^\star \leq r$	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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	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

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

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

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \sqcap t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \sqcap \langle\!| t' |\!\rangle a, \text{ with } \sqcap \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))$$

$$(\!| 0 |\!) a \triangleq \emptyset$$

$$(\!| 1 |\!) a \triangleq \{ \emptyset \bowtie a \}$$

$$(\!| [t]r \blacktriangleright o |\!) a \triangleq \begin{cases} \{ o \bowtie a \setminus r \} & \text{if } r \subseteq a \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!) a \triangleq (\!| p |\!) a \cup (\!| q |\!) a$$

$$(\!| p \cdot q |\!) a \triangleq ((\!| p |\!) \cdot (\!| q |\!)) a$$

$$(\!| p \parallel q |\!) a \triangleq ((\!| p |\!) \parallel (\!| q |\!)) a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))$$

$$[\![\omega]\!]_I \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k$$

$$[\![p]\!] a \triangleq \bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{ a \}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{ o \uplus a \setminus r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I) a$$

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	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p\,;(q+r) \equiv p\,;q + p\,;r$	KA-Seq-Dist-L	$p\,;r \leq r \Rightarrow p^\star\,;r \leq r$	KA-Lfp-L
$(p+q)\,;r \equiv p\,;r + q\,;r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r\,;p \leq r \Rightarrow r\,;p^\star \leq r$	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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist

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

Network axioms

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

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

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \sqcap t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \sqcap \langle\!| t' |\!\rangle a, \text{ with } \sqcap \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))$$

$$(\!| 0 |\!)a \triangleq \emptyset$$

$$(\!| 1 |\!)a \triangleq \{\emptyset \bowtie a\}$$

$$(\!| [t]r \blacktriangleright o |\!)a \triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \ldots \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!)a \triangleq (\!| p |\!)a \cup (\!| q |\!)a$$

$$(\!| p \cdot q |\!)a \triangleq ((\!| p |\!) \cdot (\!| q |\!))a$$

$$(\!| p \parallel q |\!)a \triangleq ((\!| p |\!) \parallel (\!| q |\!))a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))$$

$$[\![\omega]\!]_I \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 ⨟ \pi_2 ⨟ \ldots ⨟ \pi_k$$

$$[\![p]\!]a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 ⨟ \pi_2 ⨟ \ldots ⨟ \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 ⨟ \ldots ⨟ \pi_k]\!]_I)a$$

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	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p \,;\, (q+r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \leq r \Rightarrow p^\star \,;\, r \leq r$	KA-Lfp-L
$(p+q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r \,;\, p \leq r \Rightarrow r \,;\, p^\star \leq r$	KA-Lfp-R

SKA axioms for $\parallel$

$(x \,;\, p) \parallel (y \,;\, q) \equiv (x \parallel y) \,;\, (p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

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

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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist

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

Network axioms

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

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

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(BP) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \sqcap t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \sqcap \langle\!| t' |\!\rangle a, \text{ with } \sqcap \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP))$$

$$(\!| 0 |\!) a \triangleq \emptyset$$

$$(\!| 1 |\!) a \triangleq \{ \emptyset \bowtie a \}$$

$$(\!| [t]r \blacktriangleright o |\!) a \triangleq \begin{cases} \{ o \bowtie a \setminus r \} & \text{if } r \subseteq a \ldots \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!) a \triangleq (\!| p |\!) a \cup (\!| q |\!) a$$

$$(\!| p \cdot q |\!) a \triangleq ((\!| p |\!) \cdot (\!| q |\!)) a$$

$$(\!| p \parallel q |\!) a \triangleq ((\!| p |\!) \parallel (\!| q |\!)) a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$$

$$[\![\omega]\!]_I \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k$$

$$[\![p]\!] a \triangleq \bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{ a \}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{ o \uplus a \setminus r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I) a$$

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	$1 + p ; p^\star \equiv p^\star$	KA-Unroll-L
$p ; ($ …			KA-Lfp-L
$(p$ …			KA-Unroll-R
		$r ; p \leq r \Rightarrow r ; p^\star \leq r$	KA-Lfp-R

SKA axioms for ∥

$(x;p) \parallel (y;q) \equiv (x \parallel y);(p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for ·

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist

Network axioms

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

Tests $T \ni t, t'$

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

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

BellKAT at a glance

Syntax

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

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \,\square\, t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))$$

$$(\!| 0 |\!) a \triangleq \emptyset$$

$$(\!| 1 |\!) a \triangleq \{\emptyset \bowtie a\}$$

$$(\!| [t]r \blacktriangleright o |\!) a \triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!) a \triangleq (\!| p |\!) a \cup (\!| q |\!) a$$

$$(\!| p \cdot q |\!) a \triangleq ((\!| p |\!) \cdot (\!| q |\!)) a$$

$$(\!| p \parallel q |\!) a \triangleq ((\!| p |\!) \parallel (\!| q |\!)) a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))$$

$$[\![\omega]\!]_I \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \,⨾\, \pi_2 \,⨾\, \dots \,⨾\, \pi_k$$

$$[\![p]\!] a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \,⨾\, \pi_2 \,⨾\, \dots \,⨾\, \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \,⨾\, \dots \,⨾\, \pi_k]\!]_I) a$$

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	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p \,;\, (q + r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \leq r \Rightarrow p^\star \,;\, r \leq r$	KA-Lfp-L
$(p + q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r \,;\, p \leq r \Rightarrow r \,;\, p^\star \leq r$	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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	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

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	N ::=	$A, B, C, \ldots$	
Bell pairs	BP ∋ bp ::=	N~N	
Multisets	$\mathcal{M}(\mathrm{BP}) \ni a, b, r, o$ ::=	$\{\!\{ bp_1, \ldots, bp_k \}\!\}$	
Tests	$T \ni t, t'$ ::=	$\mathbb{1}$	*no test*
	|	b	*multiset absence*
	|	$t \wedge t'$	*conjunction*

Multi-round semantics

$$
\begin{array}{rcl}
[\![p]\!] & \in & \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})) \\
[\![\omega]\!]_I & \in & \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \mathbin{⨾} \pi_2 \mathbin{⨾} \ldots \mathbin{⨾} \pi_k \\
[\![p]\!]a & \triangleq & \bigcup_{\omega \in I(p)} [\![\omega]\!]_I a \\
[\![\epsilon]\!]_I a & \triangleq & \{ a \} \\
[\![[t]r \blacktriangleright o]\!]_I a & \triangleq & \begin{cases} \{ o \uplus a \backslash r \} & \text{if } r \subseteq a \text{ and } (\!|t|\!)a = \top \\ \emptyset & \text{otherwise} \end{cases}
\end{array}
$$

$(\!|\mathbb{1}|\!)a \equiv \top$ $\qquad$ $(\!|t \uplus b|\!)a \equiv ((\!|t|\!)a \setminus b \wedge b \subseteq a) \vee (\!|b|\!)a$

$(\!|b|\!)a \triangleq b \not\subseteq a$ $\qquad$ $(\!|t \square t'|\!)a \triangleq (\!|t|\!)a \square (\!|t'|\!)a$, with $\square$ is either $\wedge$ or $\vee$

Single round semantics

$$
\begin{array}{rcl}
(\!|p|\!) & \in & \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP})) \\
(\!|0|\!)a & \triangleq & \emptyset \\
(\!|1|\!)a & \triangleq & \{ \emptyset \bowtie a \} \\
(\!|[t]r \blacktriangleright o|\!)a & \triangleq & \begin{cases} \{ o \bowtie a \backslash r \} & \text{if } r \subseteq a \text{ and } (\!|t|\!)a = \top \\ \emptyset & \text{otherwise} \end{cases} \\
(\!|p + q|\!)a & \triangleq & (\!|p|\!)a \cup (\!|q|\!)a \\
(\!|p \cdot q|\!)a & \triangleq & ((\!|p|\!) \cdot (\!|q|\!))a \\
(\!|p \parallel q|\!)a & \triangleq & ((\!|p|\!) \parallel (\!|q|\!))a
\end{array}
$$

Multi-round semantics

$$
\begin{array}{rcl}
[\![p]\!] & \in & \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})) \\
[\![\omega]\!]_I & \in & \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \mathbin{⨾} \pi_2 \mathbin{⨾} \ldots \mathbin{⨾} \pi_k \\
[\![p]\!]a & \triangleq & \bigcup_{\omega \in I(p)} [\![\omega]\!]_I a \\
[\![\epsilon]\!]_I a & \triangleq & \{ a \} \\
[\![[t]r \blacktriangleright o]\!]_I a & \triangleq & \begin{cases} \{ o \uplus a \backslash r \} & \text{if } r \subseteq a \text{ and } (\!|t|\!)a = \top \\ \emptyset & \text{otherwise} \end{cases}
\end{array}
$$

$$[\![\pi_1 \mathbin{⨾} \pi_2 \mathbin{⨾} \ldots \mathbin{⨾} \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \mathbin{⨾} \ldots \mathbin{⨾} \pi_k]\!]_I)a$$

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

$(x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	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

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$N ::=$	$A, B, C, \ldots$
Bell pairs	$BP \ni bp ::=$	$N \sim N$
Multisets		
Tests		
Atomic action		
Policies		
	$\mid$ p^*	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$

Single round semantics

$$
\begin{aligned}
(\!| p |\!) &\in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP)) \\
(\!| 0 |\!) a &\triangleq \emptyset \\
(\!| 1 |\!) a &\triangleq \{ \emptyset \bowtie a \} \\
(\!| [t]r \blacktriangleright o |\!) a &\triangleq \begin{cases} \{ o \bowtie a \backslash r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}
\end{aligned}
$$

Test semantics

$$
\begin{aligned}
\langle\!| t |\!\rangle &\in \mathcal{M}(BP) \to \{\top, \bot\} \\
\langle\!| \mathbb{1} |\!\rangle a &\triangleq \top \qquad & \langle\!| t \uplus b |\!\rangle a &\triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a \\
\langle\!| b |\!\rangle a &\triangleq b \not\subseteq a \qquad & \langle\!| t \,\square\, t' |\!\rangle a &\triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee
\end{aligned}
$$

Single round semantics

$$
\begin{aligned}
(\!| p |\!) &\in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP)) \\
(\!| 0 |\!) a &\triangleq \emptyset \\
(\!| 1 |\!) a &\triangleq \{ \emptyset \bowtie a \} \\
(\!| [t]r \blacktriangleright o |\!) a &\triangleq \begin{cases} \{ o \bowtie a \backslash r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\
(\!| p + q |\!) a &\triangleq (\!| p |\!) a \cup (\!| q |\!) a \\
(\!| p \cdot q |\!) a &\triangleq ((\!| p |\!) \cdot (\!| q |\!)) a \\
(\!| p \parallel q |\!) a &\triangleq ((\!| p |\!) \parallel (\!| q |\!)) a
\end{aligned}
$$

Multi-round semantics

$$
\begin{aligned}
[\![p]\!] &\in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)) \\
[\![\omega]\!]_I &\in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 ; \pi_2 ; \ldots ; \pi_k \\
[\![p]\!] a &\triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a \\
[\![\epsilon]\!]_I a &\triangleq \{ a \} \\
[\![[t]r \blacktriangleright o]\!]_I a &\triangleq \begin{cases} \{ o \uplus a \backslash r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\
[\![\pi_1 ; \pi_2 ; \ldots ; \pi_k]\!]_I a &\triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 ; \ldots ; \pi_k]\!]_I) a
\end{aligned}
$$

KA axioms

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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	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

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

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

Test semantics

$$\langle\!|t|\!\rangle \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\langle\!|\mathbb{1}|\!\rangle a \triangleq \top \qquad \langle\!|t \uplus b|\!\rangle a \triangleq (\langle\!|t|\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!|b|\!\rangle a$$

$$\langle\!|b|\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!|t \,\square\, t'|\!\rangle a \triangleq \langle\!|t|\!\rangle a \,\square\, \langle\!|t'|\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$\begin{aligned}
(\!|p|\!) &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))\\
(\!|0|\!)a &\triangleq \emptyset\\
(\!|1|\!)a &\triangleq \{\emptyset \bowtie a\}\\
(\!|[t]r \blacktriangleright o|\!)a &\triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!|t|\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}\\
(\!|p + q|\!)a &\triangleq (\!|p|\!)a \cup (\!|q|\!)a\\
(\!|p \cdot q|\!)a &\triangleq ((\!|p|\!) \cdot (\!|q|\!))a\\
(\!|p \parallel q|\!)a &\triangleq ((\!|p|\!) \parallel (\!|q|\!))a
\end{aligned}$$

Multi-round semantics

$$\begin{aligned}
[\![p]\!] &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))\\
[\![\omega]\!]_I &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k\\
[\![p]\!]a &\triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a\\
[\![\epsilon]\!]_I a &\triangleq \{a\}\\
[\![[t]r \blacktriangleright o]\!]_I a &\triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!|t|\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}\\
[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a &\triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I)a
\end{aligned}$$

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	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p \,;\, (q + r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \leq r \Rightarrow p^\star \,;\, r \leq r$	KA-Lfp-L
$(p + q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r \,;\, p \leq r \Rightarrow r \,;\, p^\star \leq r$	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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	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

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	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
$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

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

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\begin{array}{lll@{\qquad}lll}
\langle\!| \mathbb{1} |\!\rangle a & \triangleq & \top & \langle\!| t \uplus b |\!\rangle a & \triangleq & (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a \\
\langle\!| b |\!\rangle a & \triangleq & b \not\subseteq a & \langle\!| t \,\square\, t' |\!\rangle a & \triangleq & \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee
\end{array}$$

Single round semantics

$$\begin{array}{rcl}
(\!| p |\!) & \in & \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP})) \\
(\!| 0 |\!) a & \triangleq & \emptyset \\
(\!| 1 |\!) a & \triangleq & \{ \emptyset \bowtie a \} \\
(\!| [t]r \blacktriangleright o |\!) a & \triangleq & \begin{cases} \{ o \bowtie a \setminus r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\
(\!| p + q |\!) a & \triangleq & (\!| p |\!) a \cup (\!| q |\!) a \\
(\!| p \cdot q |\!) a & \triangleq & ((\!| p |\!) \cdot (\!| q |\!)) a \\
(\!| p \parallel q |\!) a & \triangleq & ((\!| p |\!) \parallel (\!| q |\!)) a
\end{array}$$

Multi-round semantics

$$\begin{array}{rcl}
[\![p]\!] & \in & \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})) \\
[\![\omega]\!]_I & \in & \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k \\
[\![p]\!] a & \triangleq & \bigcup_{\omega \in I(p)} [\![\omega]\!]_I a \\
[\![\epsilon]\!]_I a & \triangleq & \{ a \} \\
[\![[t]r \blacktriangleright o]\!]_I a & \triangleq & \begin{cases} \{ o \uplus a \setminus r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases} \\
[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a & \triangleq & ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I) a
\end{array}$$

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	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p \,;\, (q+r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \leq r \Rightarrow p^\star \,;\, r \leq r$	KA-Lfp-L
$(p+q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r \,;\, p \leq r \Rightarrow r \,;\, p^\star \leq r$	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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	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

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

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

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \,\square\, t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))$$

$$(\!| 0 |\!) a \triangleq \emptyset$$

$$(\!| 1 |\!) a \triangleq \{\emptyset \bowtie a\}$$

$$(\!| [t]r \blacktriangleright o |\!) a \triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!) a \triangleq (\!| p |\!) a \cup (\!| q |\!) a$$

$$(\!| p \cdot q |\!) a \triangleq ((\!| p |\!) \cdot (\!| q |\!)) a$$

$$(\!| p \parallel q |\!) a \triangleq ((\!| p |\!) \parallel (\!| q |\!)) a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))$$

$$[\![\omega]\!]_I \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \,⨟\, \pi_2 \,⨟\, \ldots \,⨟\, \pi_k$$

$$[\![p]\!] a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \,⨟\, \pi_2 \,⨟\, \ldots \,⨟\, \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \,⨟\, \ldots \,⨟\, \pi_k]\!]_I) a$$

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	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p \,;\, (q+r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \leq r \Rightarrow p^\star \,;\, r \leq r$	KA-Lfp-L
$(p+q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r \,;\, p \leq r \Rightarrow r \,;\, p^\star \leq r$	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)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	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

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Network axioms

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

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

Syntax

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

$(\!| p |\!) \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP))$

$(\!| 0 |\!)a \triangleq \emptyset$

$(\!| 1 |\!)a \triangleq \{\emptyset \bowtie a\}$

$(\!| [t]r \blacktriangleright o |\!)a \triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } (\!| t |\!)a = \top \\ \emptyset & \text{otherwise} \end{cases}$

$(\!| p + q |\!)a \triangleq (\!| p |\!)a \cup (\!| q |\!)a$

$(\!| p \cdot q |\!)a \triangleq ((\!| p |\!) \cdot (\!| q |\!))a$

$(\!| p \parallel q |\!)a \triangleq ((\!| p |\!) \parallel (\!| q |\!))a$

Multi-round semantics

$[\![p]\!] \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$

$[\![\omega]\!]_I \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$, where $\omega = \pi_1 ⨟ \pi_2 ⨟ \ldots ⨟ \pi_k$

$[\![p]\!]a \triangleq \bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$

$[\![\epsilon]\!]_I a \triangleq \{a\}$

$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } (\!| t |\!)a = \top \\ \emptyset & \text{otherwise} \end{cases}$

$[\![\pi_1 ⨟ \pi_2 ⨟ \ldots ⨟ \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 ⨟ \ldots ⨟ \pi_k]\!]_I)a$

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	$1 + p ; p^\star \equiv p^\star$	KA-Unroll-L
$p ; (q+r) \equiv p ; q + p ; r$	KA-Seq-Dist-L	$p ; r \leq r \Rightarrow p^\star ; r \leq r$	KA-Lfp-L
$(p+q) ; r \equiv p ; r + q ; r$	KA-Seq-Dist-R	$1 + p^\star ; p \equiv p^\star$	KA-Unroll-R
		$r ; p \leq r \Rightarrow r ; p^\star \leq r$	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

ean 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

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

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus