Journey Beyond Full Abstraction:

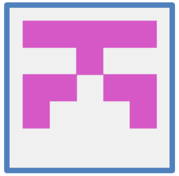
Exploring Robust Property Preservation for Secure Compilation

Carmine Abate
Inria Paris

Rob Blanco
Inria Paris

Deepak Garg
MPI-SWS

Cătălin Hrițcu
Inria Paris



Jérémy Thibault
Inria Paris

Marco Patrignani
Stanford & CISPA

https://github.com/secure-compilation/exploring-robust-property-preservation

Good programming languages provide helpful abstractions for writing more secure code

Good programming languages provide helpful abstractions for writing more secure code

- structured control flow, procedures, modules, interfaces, correctness and security specifications, ...

Good programming languages provide helpful abstractions for writing more secure code

- structured control flow, procedures, modules, interfaces, correctness and security specifications, ...

abstractions not enforced when compiling and linking with adversarial low-level code

Good programming languages provide helpful abstractions for writing more secure code

- structured control flow, procedures, modules, interfaces, correctness and security specifications, ...

abstractions not enforced when compiling and linking with adversarial low-level code

- all source-level security guarantees are lost
- **linked low-level code can read and write data and code, jump to arbitrary instructions, smash the stack**, ...

Secure compilation chains

- **Protect source-level abstractions**
  even against linked adversarial low-level code

Secure compilation chains

- Protect source-level abstractions
  even against linked adversarial low-level code
  - various **enforcement mechanisms** possible: processes, SFI, ...
  - shared responsibility: compiler, linker, loader, OS, HW

Secure compilation chains

- Protect source-level abstractions
  even against linked adversarial low-level code
  - various **enforcement mechanisms** possible: processes, SFI, ...
  - shared responsibility: compiler, linker, loader, OS, HW
- Enable source-level security reasoning
  - **if source program is secure against all source contexts then compiled program is secure against all target contexts**

Secure compilation chains

- **Protect source-level abstractions** **even against linked adversarial low-level code**
  - various **enforcement mechanisms** possible: processes, SFI, ...
  - shared responsibility: compiler, linker, loader, OS, HW
- **Enable source-level security reasoning**
  - **if source program is secure against all source contexts then compiled program is secure against all target contexts**
  - **but what should "is secure" mean?**

What properties should we robustly preserve?

What properties should we robustly preserve?

trace properties
(safety & liveness)

What properties should we robustly preserve?

hyperproperties
(noninterference)

trace properties
(safety & liveness)

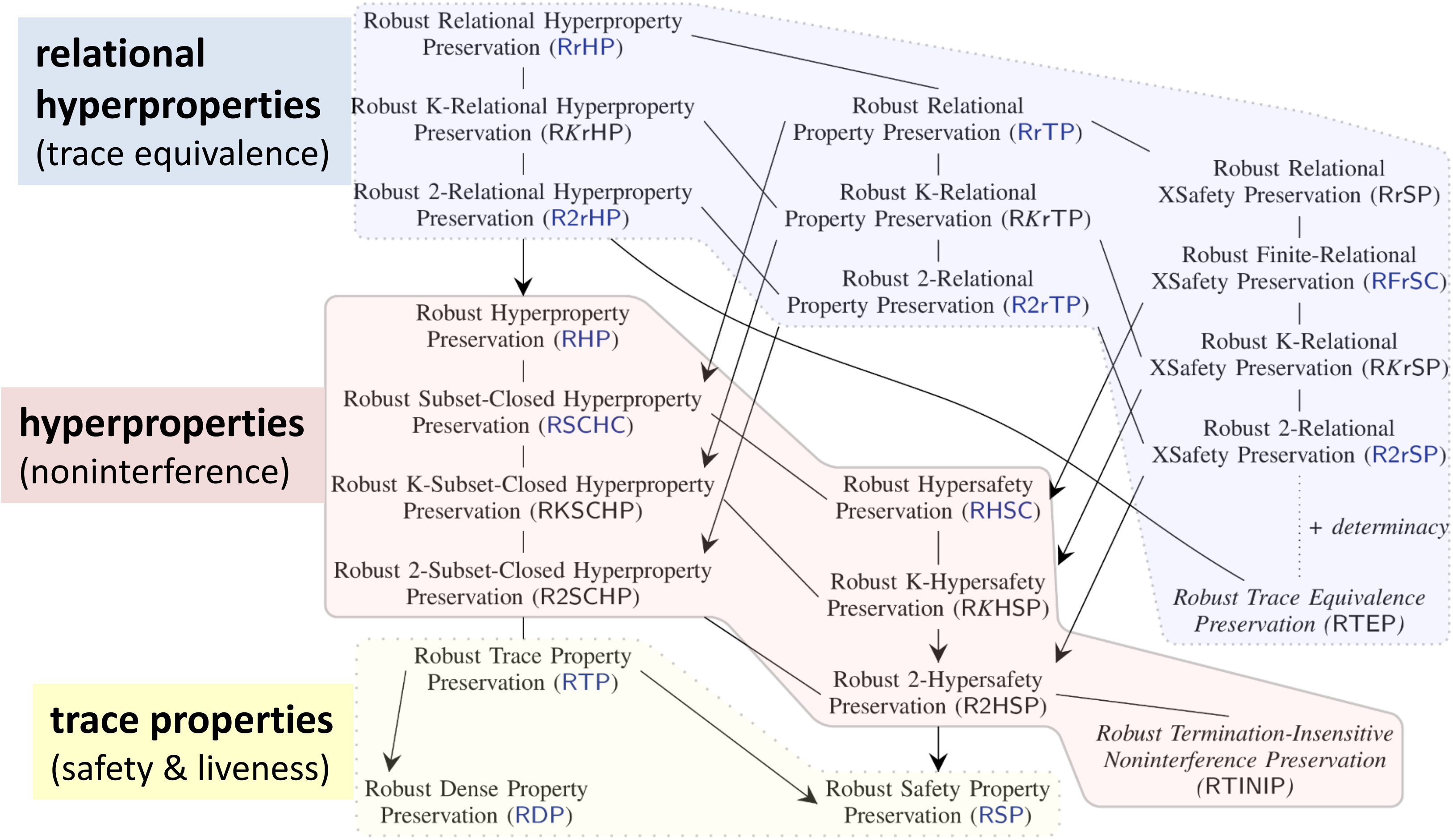
What properties should we robustly preserve?

relational hyperproperties
(trace equivalence)

hyperproperties
(noninterference)

trace properties
(safety & liveness)

What properties should we robustly preserve?



relational hyperproperties (trace equivalence)

Robust Relational Hyperproperty Preservation (RrHP)

Robust K-Relational Hyperproperty Preservation (RKrHP)

Robust 2-Relational Hyperproperty Preservation (R2rHP)

Robust Relational Property Preservation (RrTP)

Robust K-Relational Property Preservation (RKrTP)

Robust 2-Relational Property Preservation (R2rTP)

Robust Relational XSafety Preservation (RrSP)

Robust Finite-Relational XSafety Preservation (RFrSC)

Robust K-Relational XSafety Preservation (RKrSP)

Robust 2-Relational XSafety Preservation (R2rSP)

+ *determinacy*

Robust Trace Equivalence Preservation (RTEP)

hyperproperties (noninterference)

Robust Hyperproperty Preservation (RHP)

Robust Subset-Closed Hyperproperty Preservation (RSCHC)

Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)

Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)

Robust Hypersafety Preservation (RHSC)

Robust K-Hypersafety Preservation (RKHSP)

Robust 2-Hypersafety Preservation (R2HSP)

Robust Termination-Insensitive Noninterference Preservation (RTINIP)

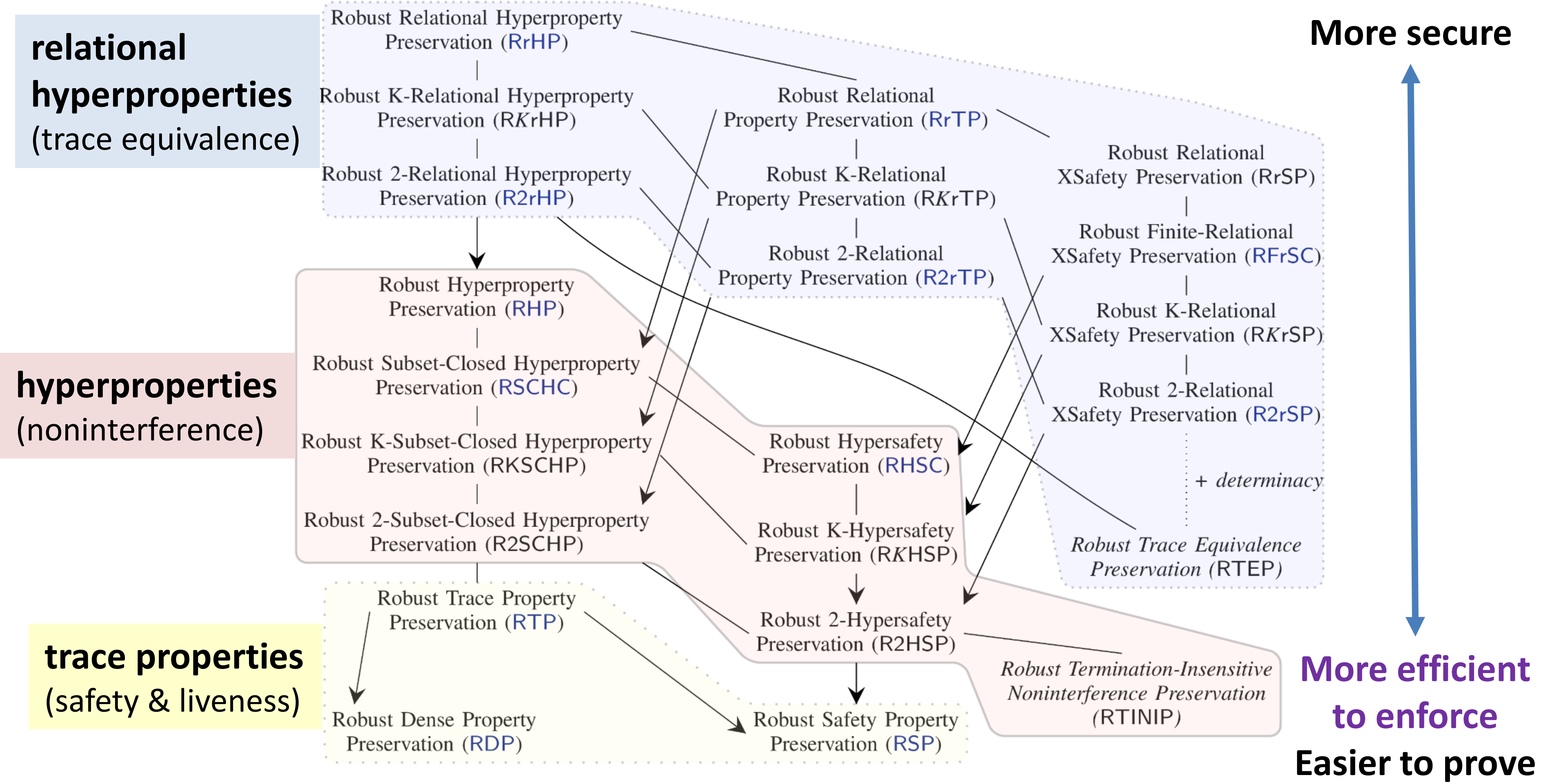
trace properties (safety & liveness)

Robust Trace Property Preservation (RTP)

Robust Dense Property Preservation (RDP)

Robust Safety Property Preservation (RSP)

What properties should we robustly preserve?



relational hyperproperties
(trace equivalence)

hyperproperties
(noninterference)

trace properties
(safety & liveness)

Robust Relational Hyperproperty Preservation (RrHP)

Robust K-Relational Hyperproperty Preservation (RKrHP)

Robust 2-Relational Hyperproperty Preservation (R2rHP)

Robust Relational Property Preservation (RrTP)

Robust K-Relational Property Preservation (RKrTP)

Robust 2-Relational Property Preservation (R2rTP)

Robust Relational XSafety Preservation (RrSP)

Robust Finite-Relational XSafety Preservation (RFrSC)

Robust K-Relational XSafety Preservation (RKrSP)

Robust 2-Relational XSafety Preservation (R2rSP)

+ *determinacy*

Robust Trace Equivalence Preservation (RTEP)

Robust Hyperproperty Preservation (RHP)

Robust Subset-Closed Hyperproperty Preservation (RSCHC)

Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)

Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)

Robust Hypersafety Preservation (RHSC)

Robust K-Hypersafety Preservation (RKHSP)

Robust 2-Hypersafety Preservation (R2HSP)

Robust Termination-Insensitive Noninterference Preservation (RTINIP)

Robust Trace Property Preservation (RTP)

Robust Dense Property Preservation (RDP)

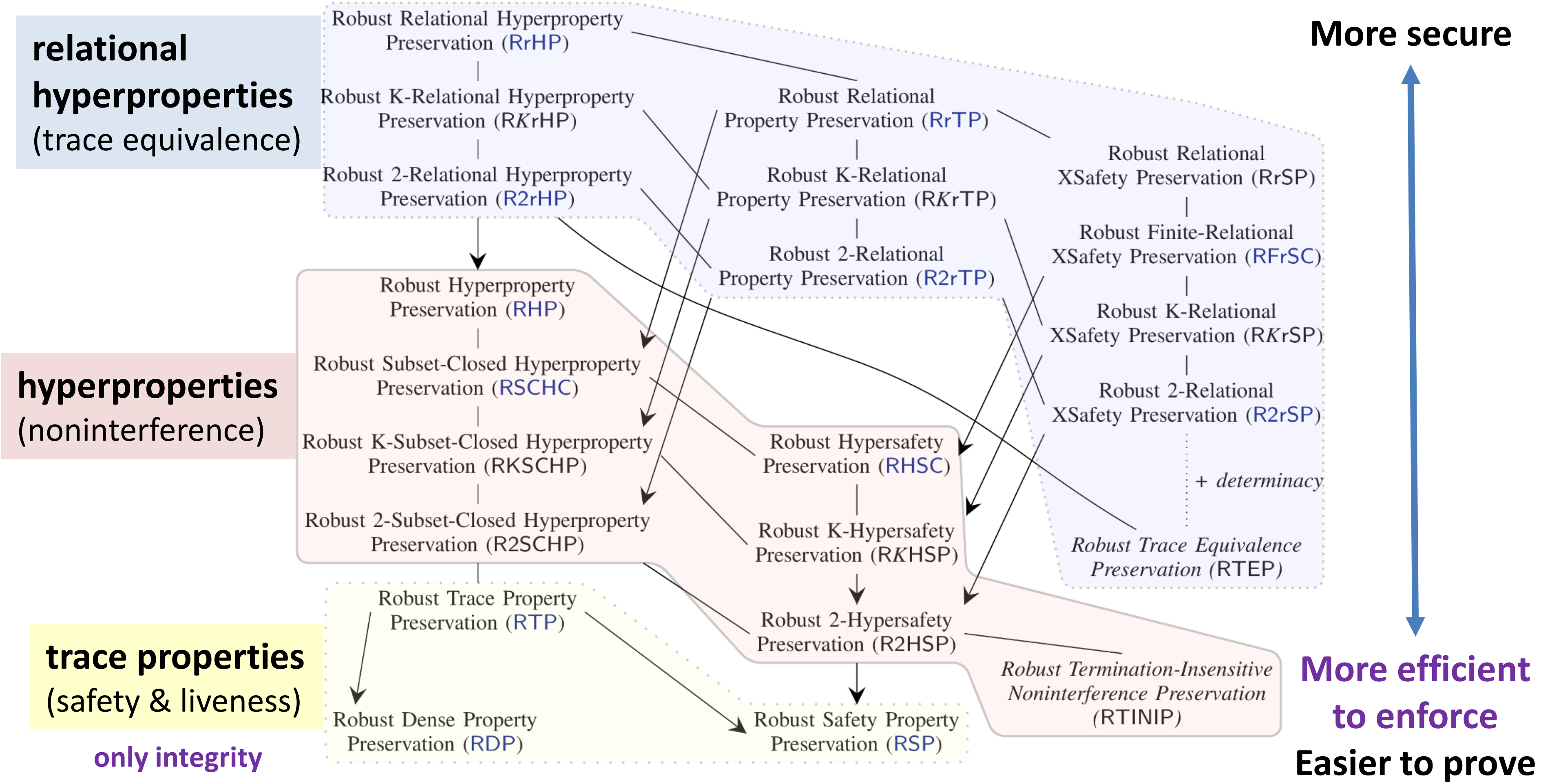
Robust Safety Property Preservation (RSP)

More secure

More efficient to enforce

Easier to prove

What properties should we robustly preserve?



relational hyperproperties
(trace equivalence)

hyperproperties
(noninterference)

trace properties
(safety & liveness)

only integrity

More secure

More efficient to enforce

Easier to prove

Robust Relational Hyperproperty Preservation (RrHP)

Robust K-Relational Hyperproperty Preservation (RKrHP)

Robust 2-Relational Hyperproperty Preservation (R2rHP)

Robust Relational Property Preservation (RrTP)

Robust K-Relational Property Preservation (RKrTP)

Robust 2-Relational Property Preservation (R2rTP)

Robust Relational XSafety Preservation (RrSP)

Robust Finite-Relational XSafety Preservation (RFrSC)

Robust K-Relational XSafety Preservation (RKrSP)

Robust 2-Relational XSafety Preservation (R2rSP)

+ *determinacy*

Robust Trace Equivalence Preservation (RTEP)

Robust Hyperproperty Preservation (RHP)

Robust Subset-Closed Hyperproperty Preservation (RSCHC)

Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)

Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)

Robust Hypersafety Preservation (RHSC)

Robust K-Hypersafety Preservation (RKHSP)

Robust 2-Hypersafety Preservation (R2HSP)

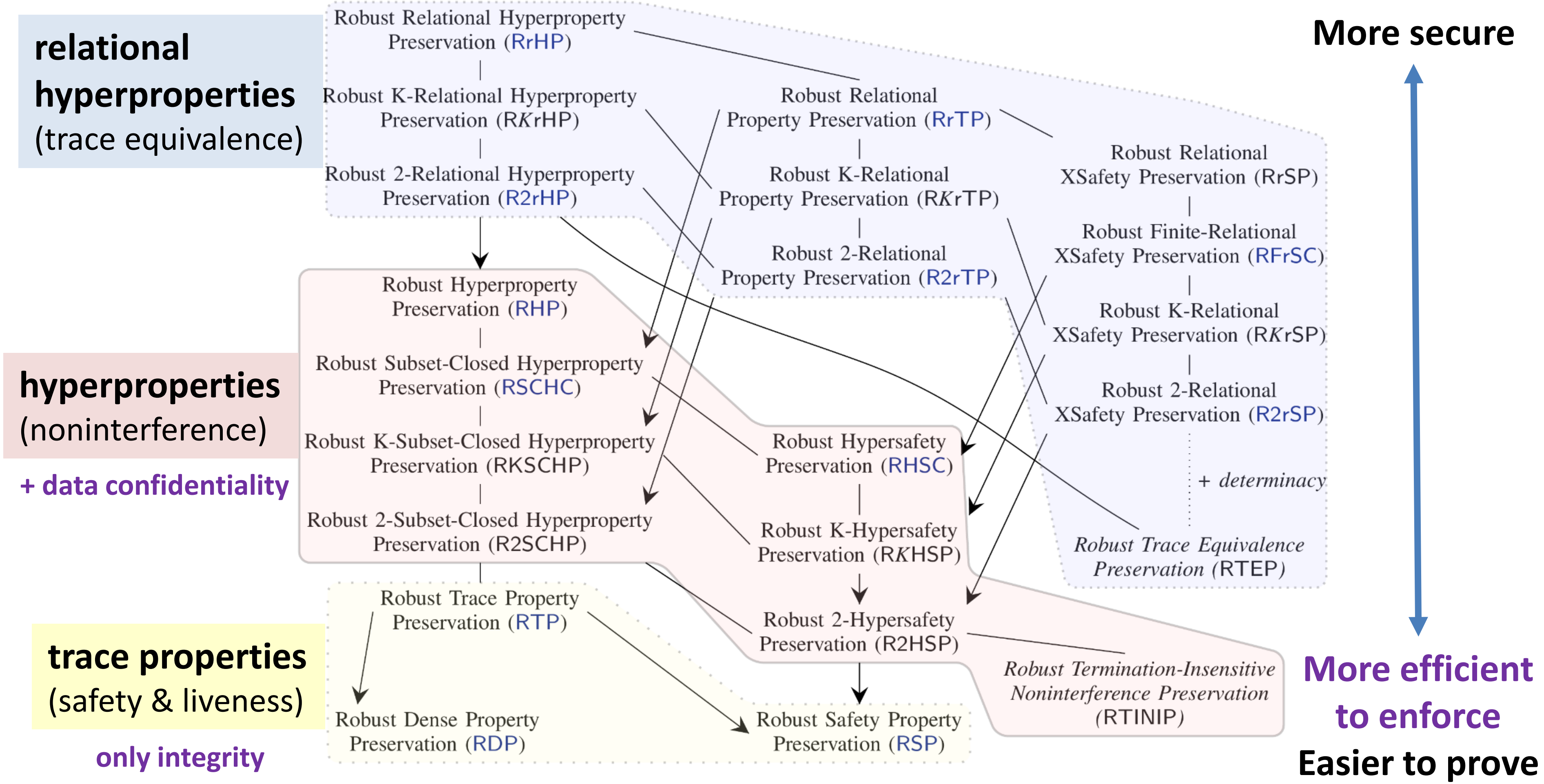
Robust Termination-Insensitive Noninterference Preservation (RTINIP)

Robust Trace Property Preservation (RTP)

Robust Dense Property Preservation (RDP)

Robust Safety Property Preservation (RSP)

What properties should we robustly preserve?



relational hyperproperties (trace equivalence)

hyperproperties (noninterference)

+ data confidentiality

trace properties (safety & liveness)

only integrity

More secure

More efficient to enforce

Easier to prove

Robust Relational Hyperproperty Preservation (RrHP)

Robust K-Relational Hyperproperty Preservation (RKrHP)

Robust 2-Relational Hyperproperty Preservation (R2rHP)

Robust Relational Property Preservation (RrTP)

Robust K-Relational Property Preservation (RKrTP)

Robust 2-Relational Property Preservation (R2rTP)

Robust Relational XSafety Preservation (RrSP)

Robust Finite-Relational XSafety Preservation (RFrSC)

Robust K-Relational XSafety Preservation (RKrSP)

Robust 2-Relational XSafety Preservation (R2rSP)

+ *determinacy*

Robust Trace Equivalence Preservation (RTEP)

Robust Hyperproperty Preservation (RHP)

Robust Subset-Closed Hyperproperty Preservation (RSCHC)

Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)

Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)

Robust Hypersafety Preservation (RHSC)

Robust K-Hypersafety Preservation (RKHSP)

Robust 2-Hypersafety Preservation (R2HSP)

Robust Termination-Insensitive Noninterference Preservation (RTINIP)

Robust Trace Property Preservation (RTP)

Robust Dense Property Preservation (RDP)

Robust Safety Property Preservation (RSP)

What properties should we robustly preserve?

relational hyperproperties
(trace equivalence)

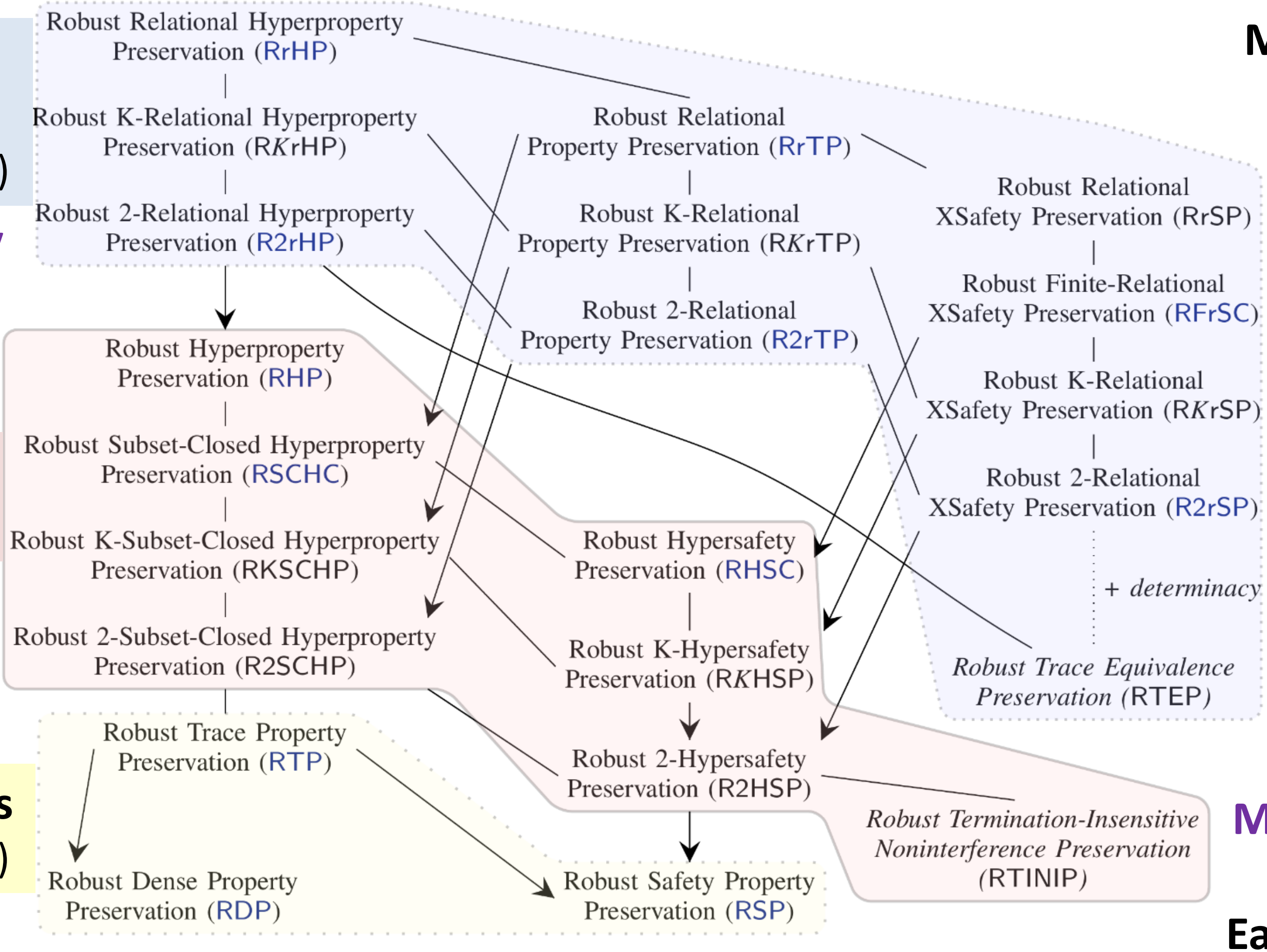
+ code confidentiality

hyperproperties
(noninterference)

+ data confidentiality

trace properties
(safety & liveness)

only integrity



Robust Relational Hyperproperty Preservation (RrHP)

Robust K-Relational Hyperproperty Preservation (RKrHP)

Robust 2-Relational Hyperproperty Preservation (R2rHP)

Robust Relational Property Preservation (RrTP)

Robust K-Relational Property Preservation (RKrTP)

Robust 2-Relational Property Preservation (R2rTP)

Robust Relational XSafety Preservation (RrSP)

Robust Finite-Relational XSafety Preservation (RFrSC)

Robust K-Relational XSafety Preservation (RKrSP)

Robust 2-Relational XSafety Preservation (R2rSP)

+ *determinacy*

Robust Trace Equivalence Preservation (RTEP)

Robust Hyperproperty Preservation (RHP)

Robust Subset-Closed Hyperproperty Preservation (RSCHC)

Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)

Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)

Robust Hypersafety Preservation (RHSC)

Robust K-Hypersafety Preservation (RKHSP)

Robust 2-Hypersafety Preservation (R2HSP)

Robust Termination-Insensitive Noninterference Preservation (RTINIP)

Robust Trace Property Preservation (RTP)

Robust Dense Property Preservation (RDP)

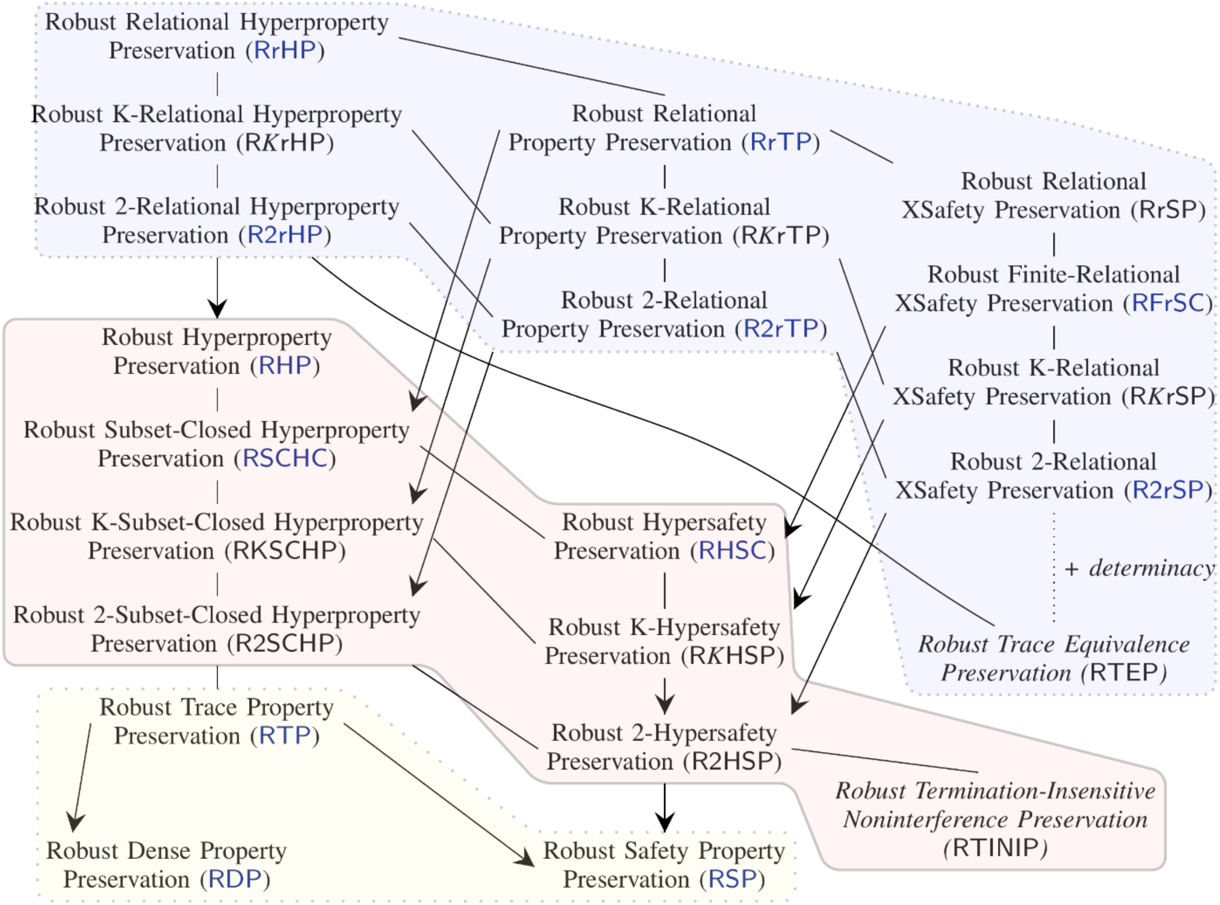
Robust Safety Property Preservation (RSP)

More secure

More efficient to enforce

Easier to prove

Journey Beyond Full Abstraction



Robust Relational Hyperproperty Preservation (RrHP)

Robust K-Relational Hyperproperty Preservation (R*K*rHP)

Robust 2-Relational Hyperproperty Preservation (R2rHP)

Robust Relational Property Preservation (RrTP)

Robust K-Relational Property Preservation (R*K*rTP)

Robust 2-Relational Property Preservation (R2rTP)

Robust Relational XSafety Preservation (RrSP)

Robust Finite-Relational XSafety Preservation (RFrSC)

Robust K-Relational XSafety Preservation (R*K*rSP)

Robust 2-Relational XSafety Preservation (R2rSP)

+ *determinacy*

Robust Trace Equivalence Preservation (RTEP)

Robust Hyperproperty Preservation (RHP)

Robust Subset-Closed Hyperproperty Preservation (RSCHC)

Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)

Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)

Robust Hypersafety Preservation (RHSC)

Robust K-Hypersafety Preservation (R*K*HSP)

Robust 2-Hypersafety Preservation (R2HSP)

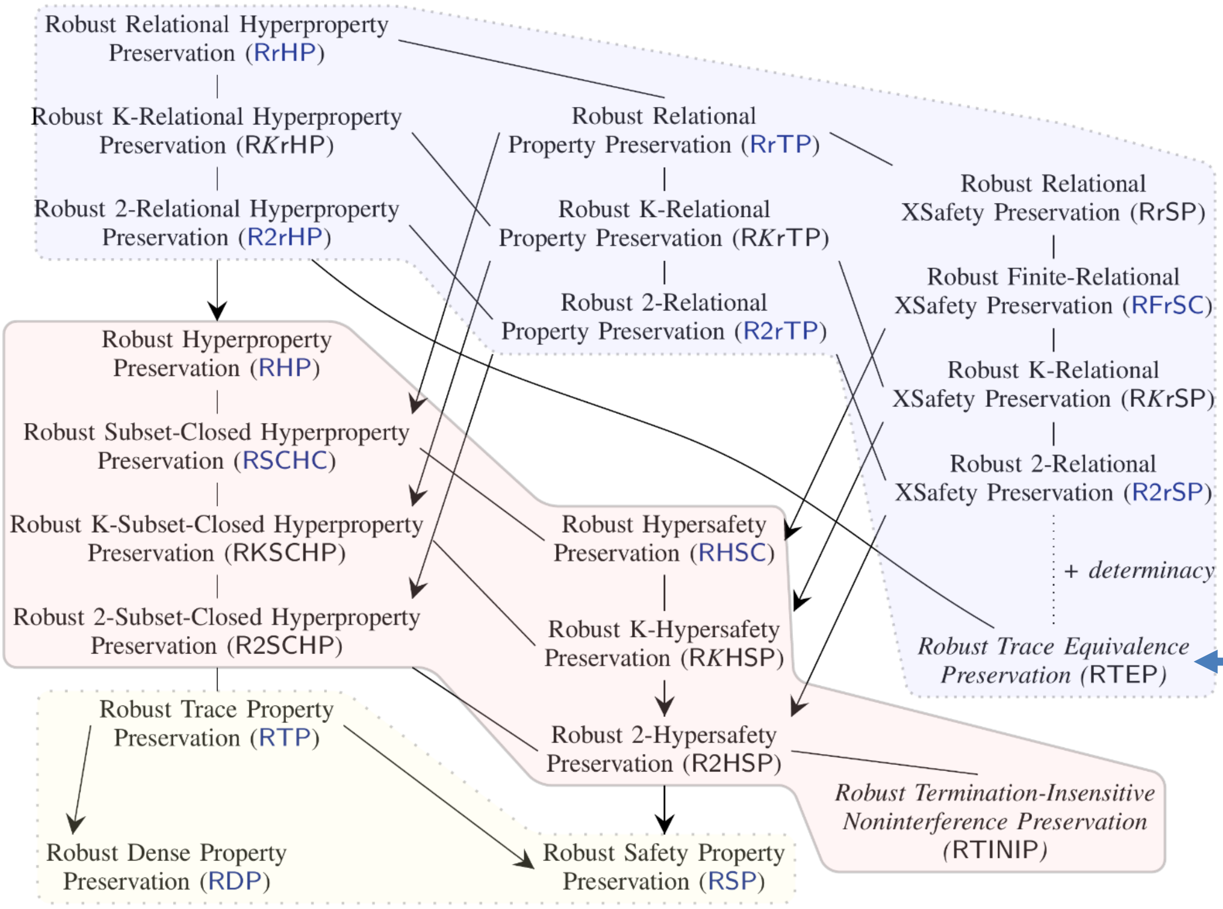
Robust Termination-Insensitive Noninterference Preservation (RTINIP)

Robust Trace Property Preservation (RTP)

Robust Dense Property Preservation (RDP)

Robust Safety Property Preservation (RSP)

Journey Beyond Full Abstraction



Robust Relational Hyperproperty Preservation (RrHP)

Robust K-Relational Hyperproperty Preservation (RKrHP)

Robust 2-Relational Hyperproperty Preservation (R2rHP)

Robust Relational Property Preservation (RrTP)

Robust K-Relational Property Preservation (RKrTP)

Robust 2-Relational Property Preservation (R2rTP)

Robust Relational XSafety Preservation (RrSP)

Robust Finite-Relational XSafety Preservation (RFrSC)

Robust K-Relational XSafety Preservation (RKrSP)

Robust 2-Relational XSafety Preservation (R2rSP)

+ *determinacy*

Robust Trace Equivalence Preservation (RTEP)

Robust Hyperproperty Preservation (RHP)

Robust Subset-Closed Hyperproperty Preservation (RSCHC)

Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)

Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)

Robust Hypersafety Preservation (RHSC)

Robust K-Hypersafety Preservation (RKHSP)

Robust 2-Hypersafety Preservation (R2HSP)

Robust Termination-Insensitive Noninterference Preservation (RTINIP)

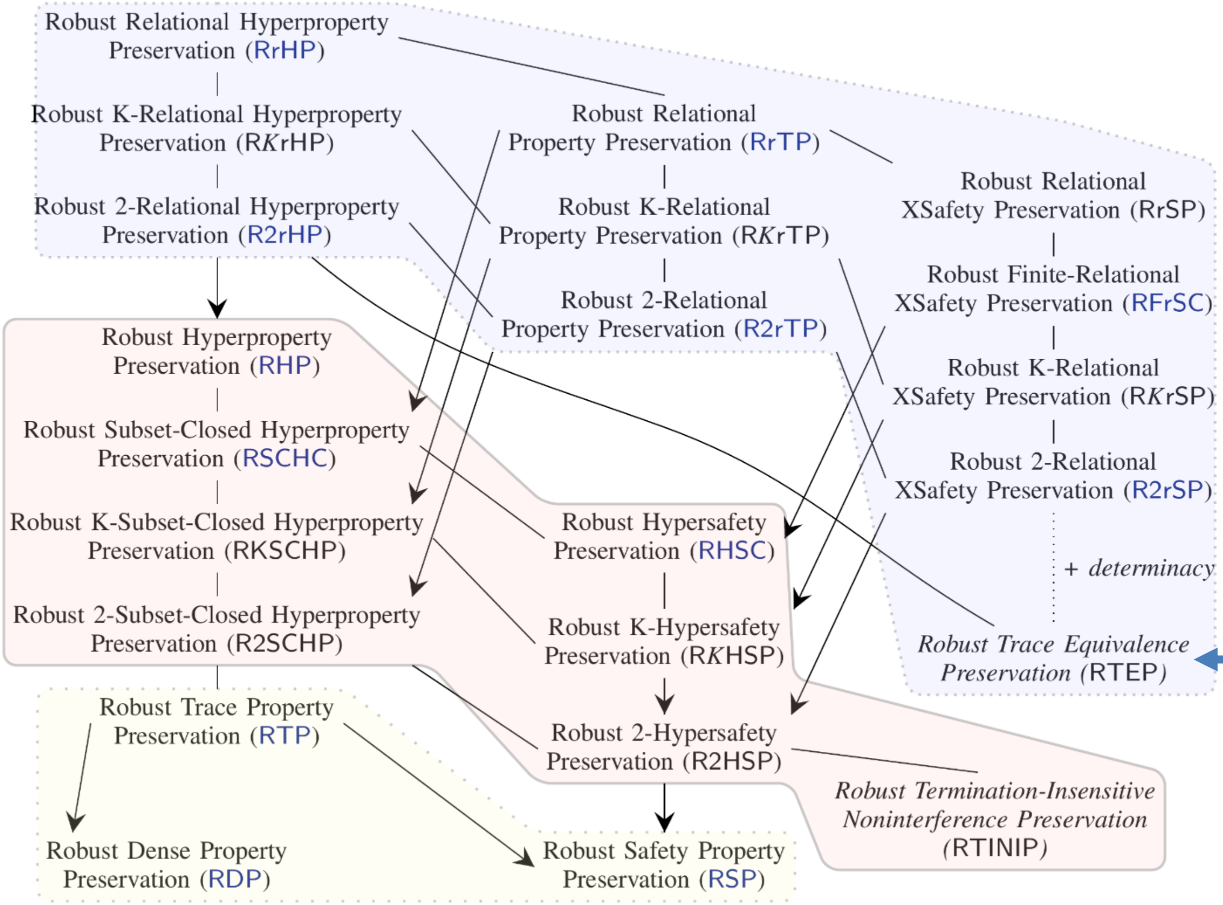
Robust Trace Property Preservation (RTP)

Robust Dense Property Preservation (RDP)

Robust Safety Property Preservation (RSP)

without internal nondeterminism,
full abstraction is here

Journey Beyond Full Abstraction



Robust Relational Hyperproperty Preservation (RrHP)

Robust K-Relational Hyperproperty Preservation (R*K*rHP)

Robust 2-Relational Hyperproperty Preservation (R2rHP)

Robust Relational Property Preservation (RrTP)

Robust K-Relational Property Preservation (R*K*rTP)

Robust 2-Relational Property Preservation (R2rTP)

Robust Relational XSafety Preservation (RrSP)

Robust Finite-Relational XSafety Preservation (RFrSC)

Robust K-Relational XSafety Preservation (R*K*rSP)

Robust 2-Relational XSafety Preservation (R2rSP)

+ *determinacy*

Robust Trace Equivalence Preservation (RTEP)

Robust Hyperproperty Preservation (RHP)

Robust Subset-Closed Hyperproperty Preservation (RSCHC)

Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)

Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)

Robust Hypersafety Preservation (RHSC)

Robust K-Hypersafety Preservation (R*K*HSP)

Robust 2-Hypersafety Preservation (R2HSP)

Robust Termination-Insensitive Noninterference Preservation (RTINIP)

Robust Trace Property Preservation (RTP)

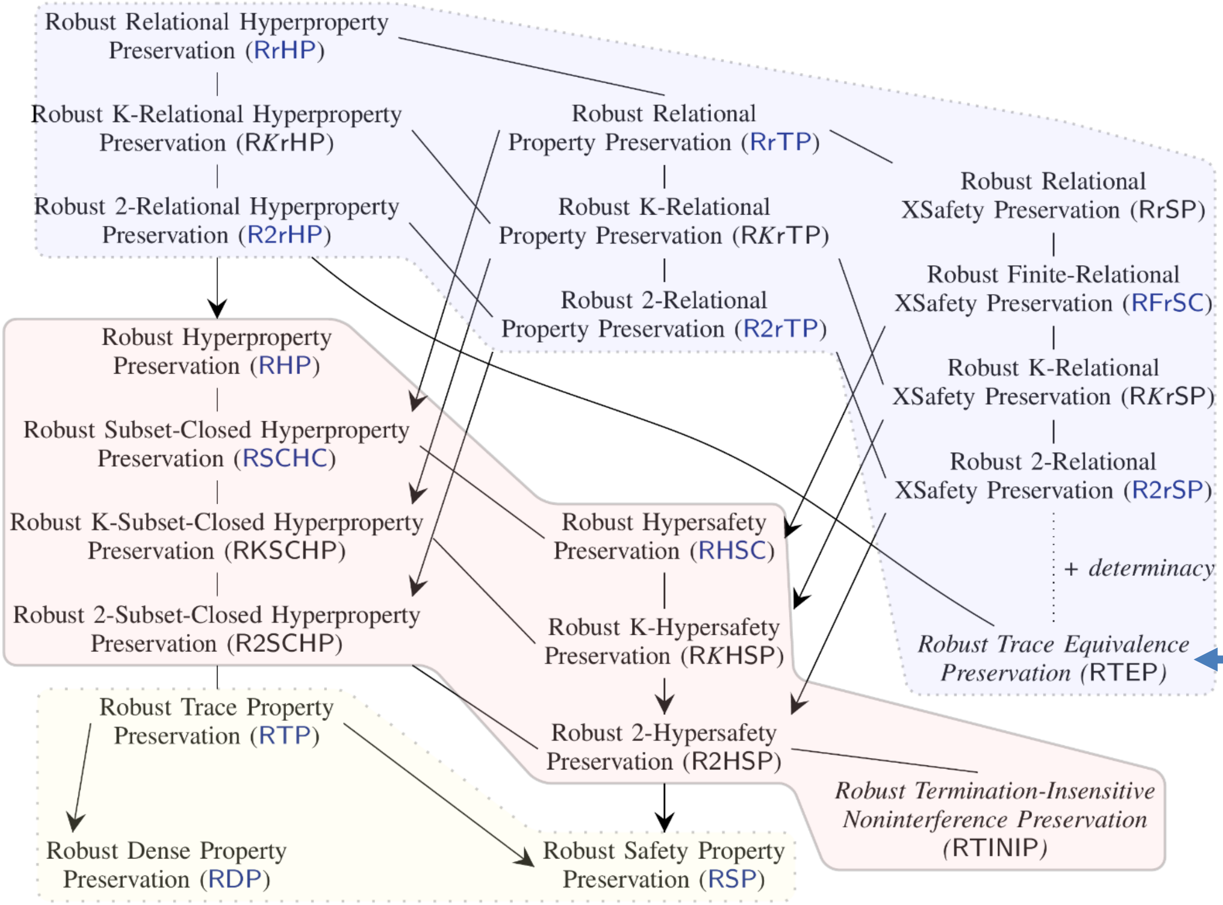
Robust Dense Property Preservation (RDP)

Robust Safety Property Preservation (RSP)

without internal nondeterminism, **full abstraction is here**

doesn't imply any of our criteria
(even assuming compiler correctness)

Journey Beyond Full Abstraction

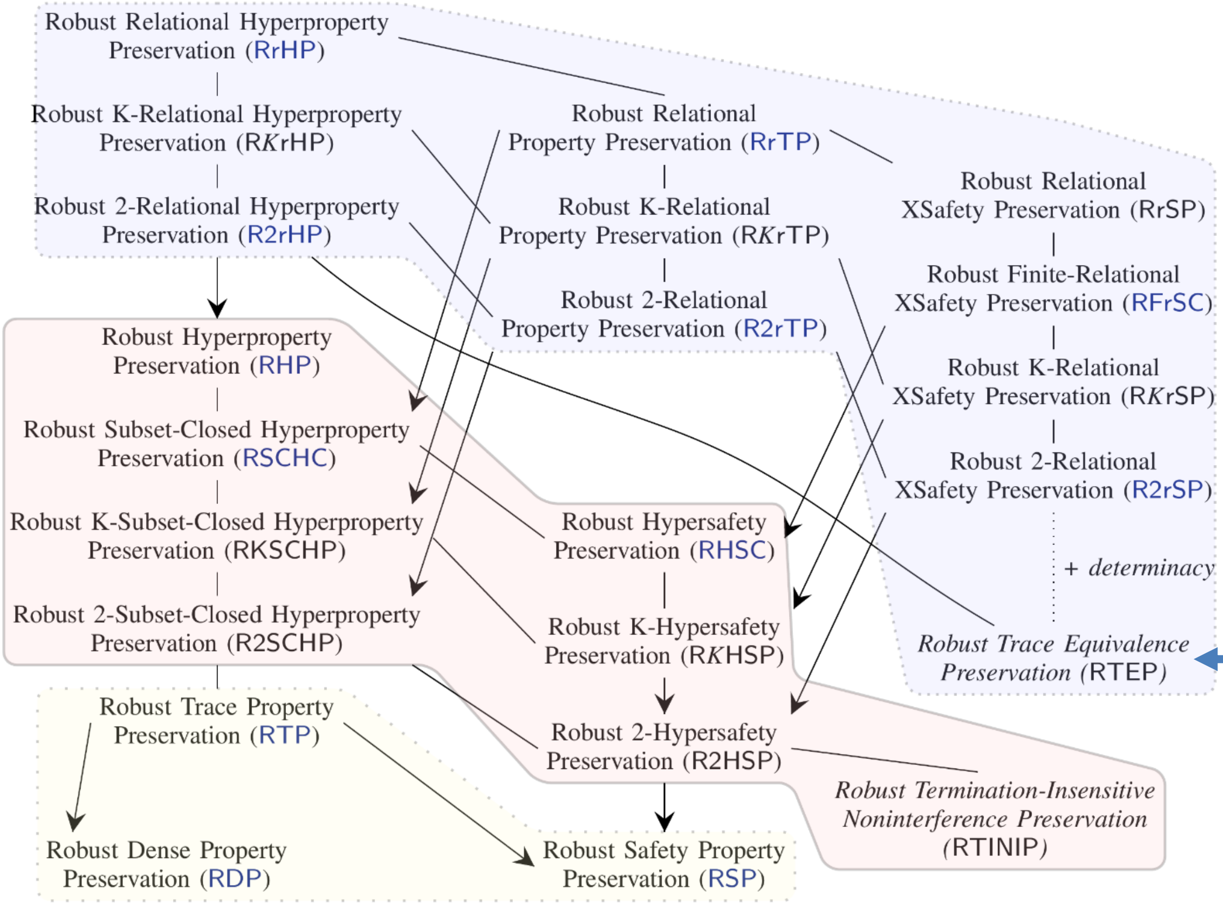

Robust Relational Hyperproperty Preservation (RrHP)
Robust K-Relational Hyperproperty Preservation (RKrHP)
Robust 2-Relational Hyperproperty Preservation (R2rHP)
Robust Relational Property Preservation (RrTP)
Robust K-Relational Property Preservation (RKrTP)
Robust 2-Relational Property Preservation (R2rTP)
Robust Relational XSafety Preservation (RrSP)
Robust Finite-Relational XSafety Preservation (RFrSC)
Robust K-Relational XSafety Preservation (RKrSP)
Robust 2-Relational XSafety Preservation (R2rSP)
+ determinacy
Robust Trace Equivalence Preservation (RTEP)
Robust Hyperproperty Preservation (RHP)
Robust Subset-Closed Hyperproperty Preservation (RSCHC)
Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)
Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)
Robust Hypersafety Preservation (RHSC)
Robust K-Hypersafety Preservation (RKHSP)
Robust 2-Hypersafety Preservation (R2HSP)
Robust Termination-Insensitive Noninterference Preservation (RTINIP)
Robust Trace Property Preservation (RTP)
Robust Dense Property Preservation (RDP)
Robust Safety Property Preservation (RSP)

without internal nondeterminism,
full abstraction is here

doesn't imply any of our criteria
(even assuming compiler correctness)

no one-size-fits-all criterion!

Journey Beyond Full Abstraction



Robust Relational Hyperproperty Preservation (RrHP)

Robust K-Relational Hyperproperty Preservation (RKrHP)

Robust 2-Relational Hyperproperty Preservation (R2rHP)

Robust Relational Property Preservation (RrTP)

Robust K-Relational Property Preservation (RKrTP)

Robust 2-Relational Property Preservation (R2rTP)

Robust Relational XSafety Preservation (RrSP)

Robust Finite-Relational XSafety Preservation (RFrSC)

Robust K-Relational XSafety Preservation (RKrSP)

Robust 2-Relational XSafety Preservation (R2rSP)

+ determinacy

Robust Trace Equivalence Preservation (RTEP)

Robust Hyperproperty Preservation (RHP)

Robust Subset-Closed Hyperproperty Preservation (RSCHC)

Robust K-Subset-Closed Hyperproperty Preservation (RKSCHP)

Robust 2-Subset-Closed Hyperproperty Preservation (R2SCHP)

Robust Hypersafety Preservation (RHSC)

Robust K-Hypersafety Preservation (RKHSP)

Robust 2-Hypersafety Preservation (R2HSP)

Robust Termination-Insensitive Noninterference Preservation (RTINIP)

Robust Trace Property Preservation (RTP)

Robust Dense Property Preservation (RDP)

Robust Safety Property Preservation (RSP)

PostDocs &
Starting Researchers
@ Inria Paris

without internal nondeterminism,
full abstraction is here

doesn't imply any of our criteria
(even assuming compiler correctness)

no one-size-fits-all criterion!