Automated Security Analysis for Real-World IoT Devices

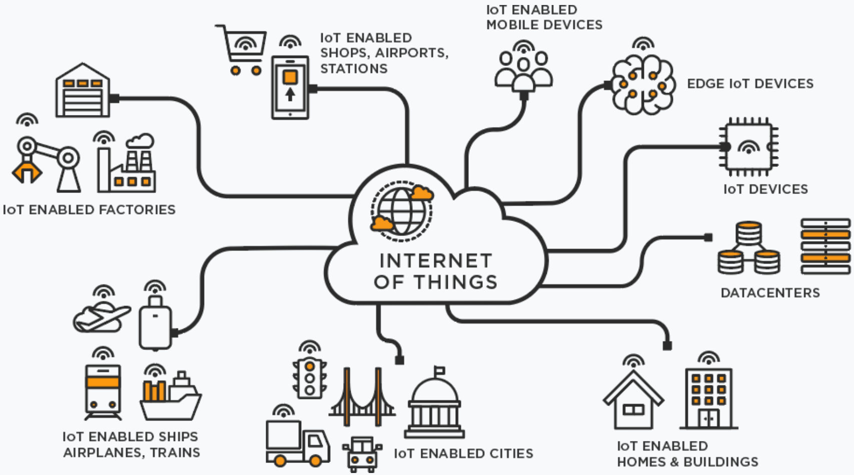
HASP'23

Lelio Brun[1] **Ichiro Hasuo**[1] **Yasushi Ono**[2] **Taro Sekiyama**[1]

[1] National Institute of Informatics, Tokyo

[2] Institute of Information Security, Yokohama

IoT Challenges


IoT ENABLED SHOPS, AIRPORTS, STATIONS
IoT ENABLED MOBILE DEVICES
EDGE IoT DEVICES
IoT DEVICES
IoT ENABLED FACTORIES
INTERNET OF THINGS
DATACENTERS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

Security is a major stake

Security is a major stake

Good candidate for ***Formal Methods***

Formal Methods

What?

Tools to perform analyses on **formal models** of systems.

Why?

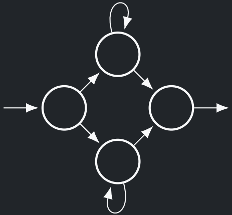
Obtain strong **mathematical guarantees** about various properties.

Examples?

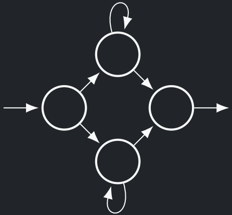
Theorem provers, model checkers, static analyzers, symbolic interpreters, . . .

Use the ***Tamarin*** security protocol verification tool to automatically analyze the security of IoT systems.

Use the ***Tamarin*** security protocol verification tool to automatically analyze the security of IoT systems.

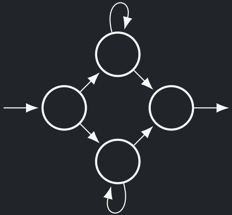


Use the ***Tamarin*** security protocol verification tool to automatically analyze the security of IoT systems.



$$\begin{cases} \phi = \forall \ldots \exists \ldots \\ \psi = \forall \ldots \\ \Sigma = \exists \ldots \end{cases}$$

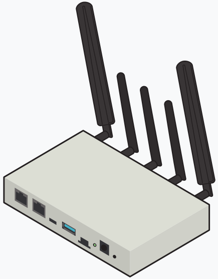
Use the ***Tamarin*** security protocol verification tool to automatically analyze the security of IoT systems.

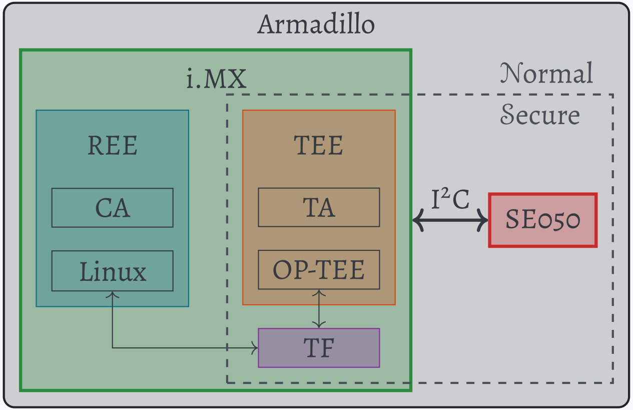


$$\begin{cases} \phi = \forall \ldots \exists \ldots \\ \psi = \forall \ldots \\ \Sigma = \exists \ldots \end{cases}$$

$$\begin{cases} \phi & \checkmark \\ \psi & \times \\ \Sigma & \infty \end{cases}$$

The Armadillo-IoT G4 platform



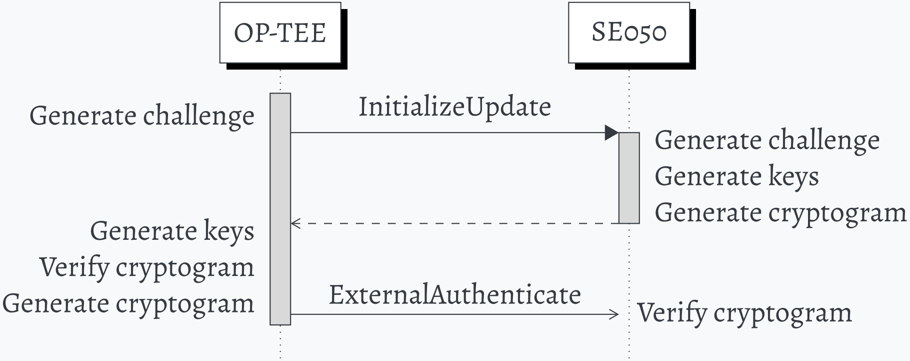


REE: Rich Execution Environment, CA: Client Application
TEE: Trusted Execution Environment, TA: Trusted Application, TF: Trusted Firmware

1. Binding process

GlobalPlatform SCP03

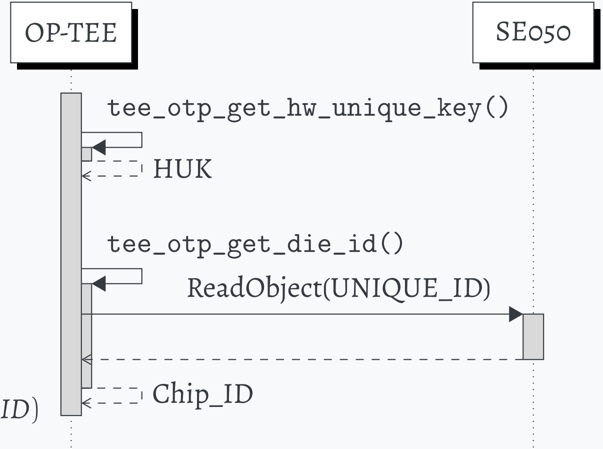
Establish an encrypted and MAC-authenticated channel over I²C



2. Deriving the Secure Storage Key

GlobalPlatform TEE Internal Core API

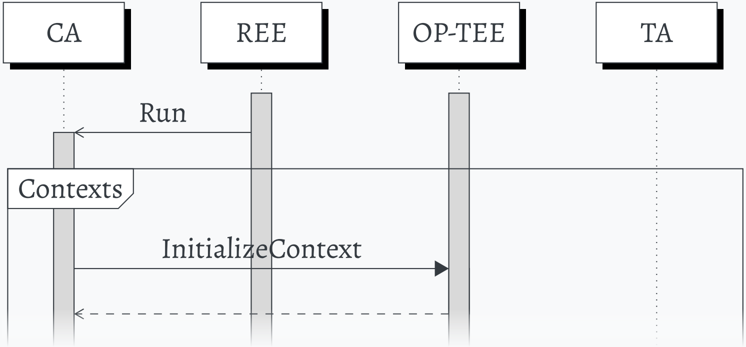
Derive the secret key used for OP-TEE encrypted file operations



$SSK = \mathsf{H}(HUK, Chip\_ID)$

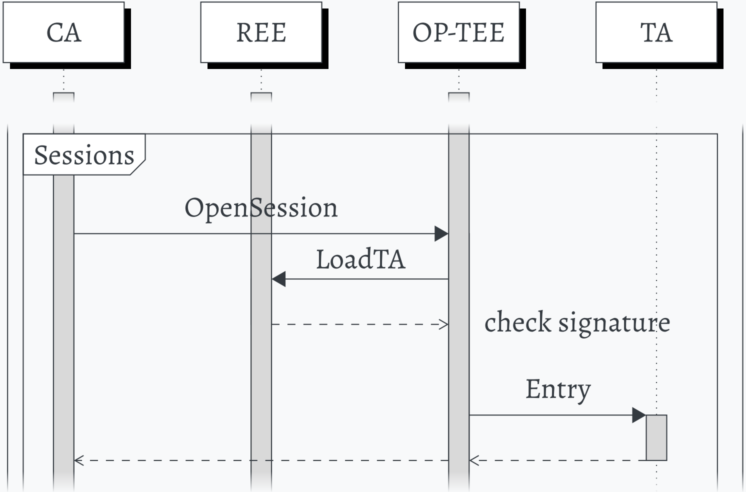
3. Executing Trusted Applications

GlobalPlatform TEE Client API



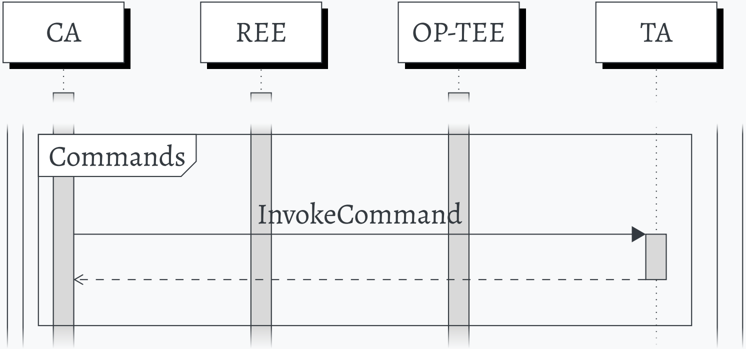
3. Executing Trusted Applications

GlobalPlatform TEE Client API



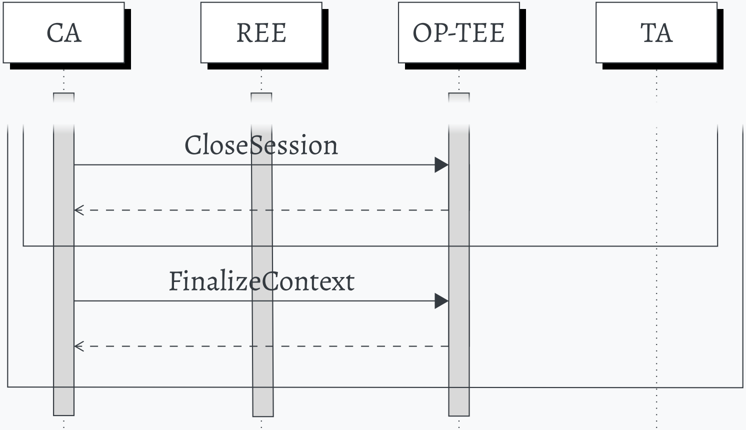
3. Executing Trusted Applications

GlobalPlatform TEE Client API



3. Executing Trusted Applications

GlobalPlatform TEE Client API



Verification of security properties

Security property: logical formula over traces (LTL-like)

1. The adversary never learns the HUK
2. The adversary never learns the Chip_ID
3. The adversary cannot impersonate the TEE when executing a TA

25 rules 8 properties 400 lines

25 rules   8 properties   400 lines

15s – 150s

Conclusion

Summary

- Extending the use of Tamarin to analyze IoT platforms as a whole
- Case study: the Armadillo device
- General model for TEE-based architectures

Discussion

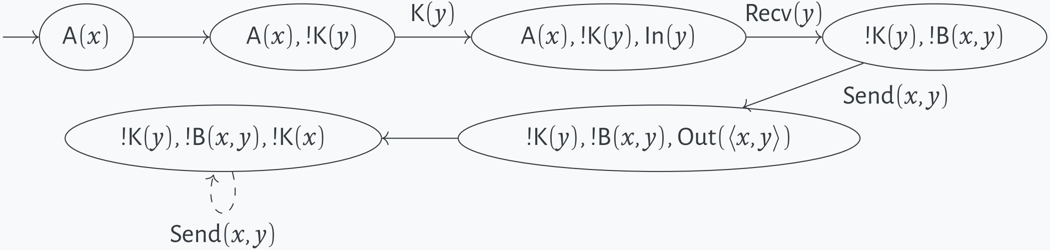
- Tamarin is a black-box
- Higher-order for TA execution
- Tampering the memory
- Compositionality

Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad\qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x, y)}\!-\![\mathsf{Recv}(y)] \qquad\qquad \frac{!\mathsf{B}(x, y)}{\mathsf{Out}(\langle x, y \rangle)}\!-\![\mathsf{Send}(x, y)]$$

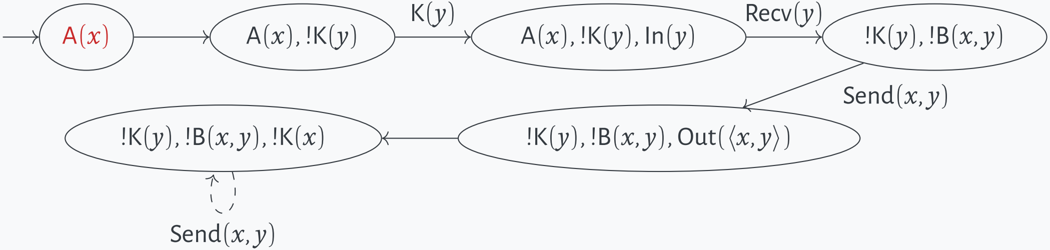
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



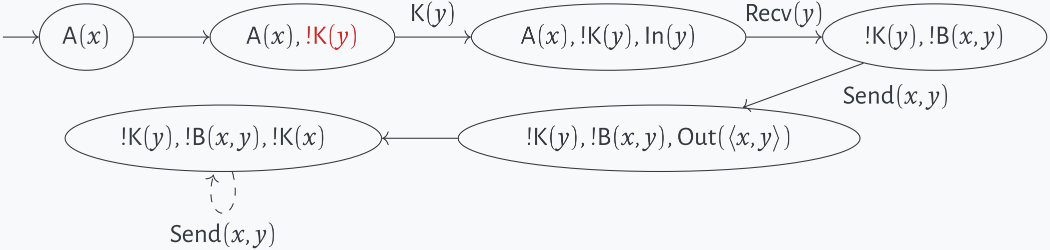
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



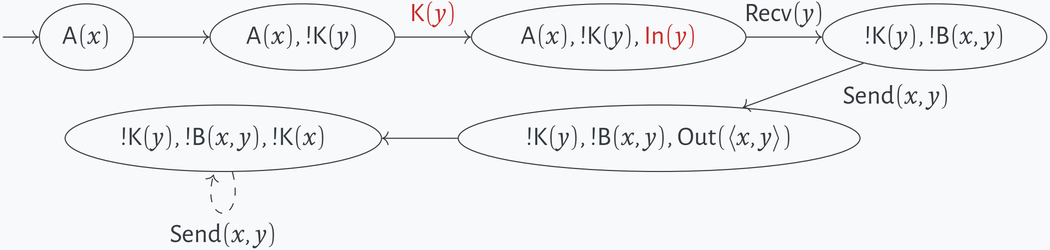
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



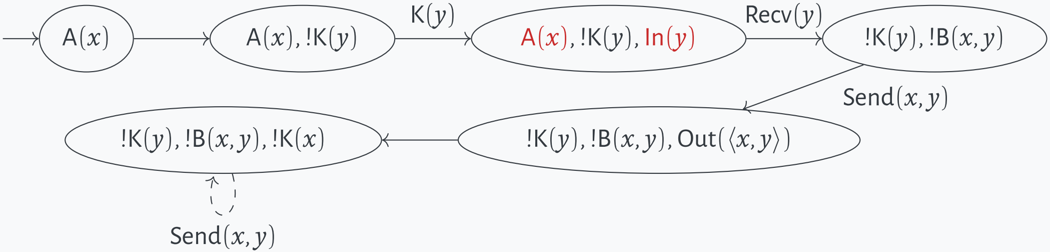
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{{\color{red}\mathsf{In}(y)} \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



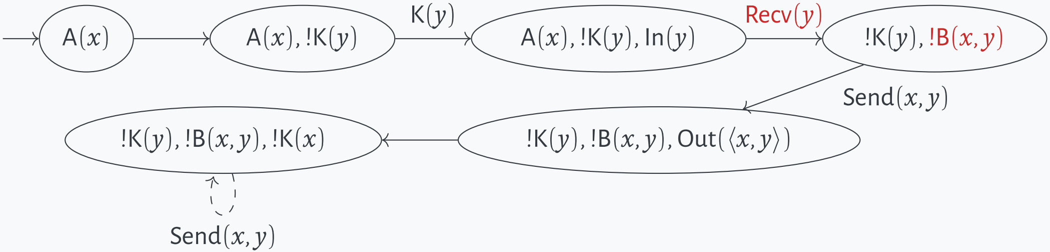
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y \rangle)}[\mathsf{Send}(x,y)]$$



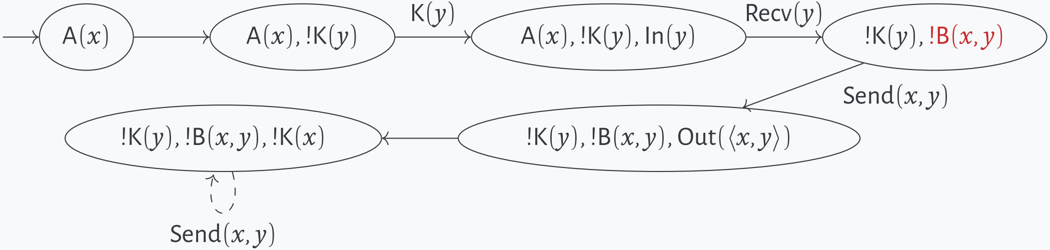
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



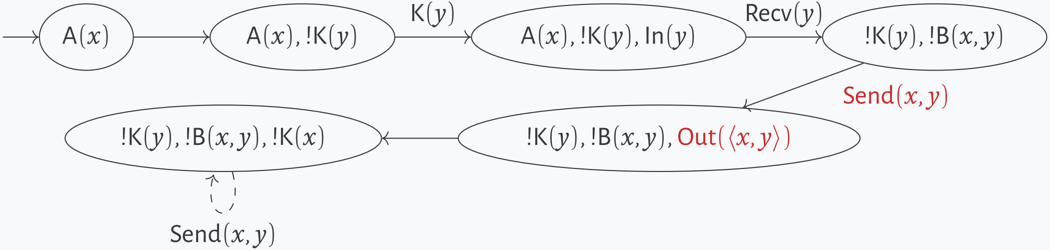
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



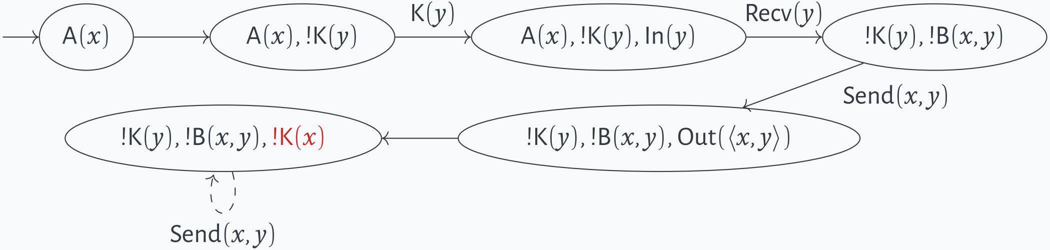
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



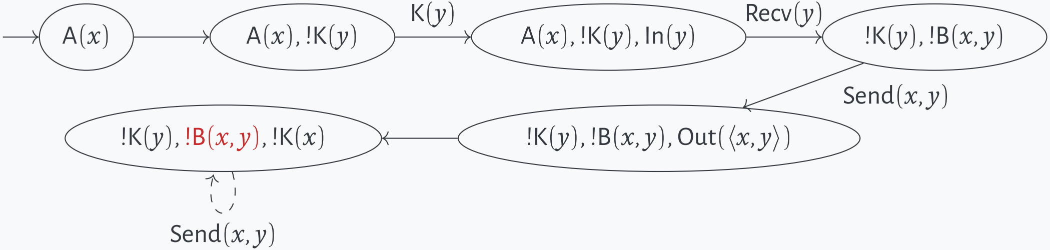
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



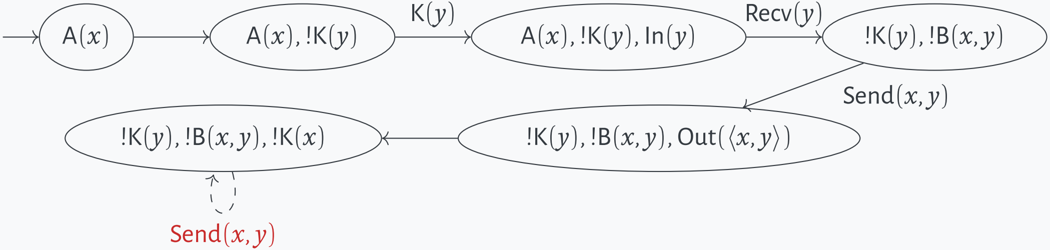
Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



Tamarin principles

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}\!-\![\mathsf{Recv}(y)] \qquad \frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}\!-\![\mathsf{Send}(x,y)]$$



A(x)
A(x), !K(y)
K(y)
A(x), !K(y), In(y)
Recv(y)
!K(y), !B(x, y)
Send(x, y)
!K(y), !B(x, y), Out(⟨x, y⟩)
!K(y), !B(x, y), !K(x)
Send(x, y)