

The background of the slide features a close-up of hands typing on a keyboard. Overlaid on the keyboard is a semi-transparent, glowing blue circular interface with a white padlock icon in the center. The interface has various lines and dots, suggesting a digital or security-related theme. The slide is divided into a white top-right section, a teal bottom-left section, and a light green bottom-right section.

Automating Security Analysis of Off-Chain Protocols

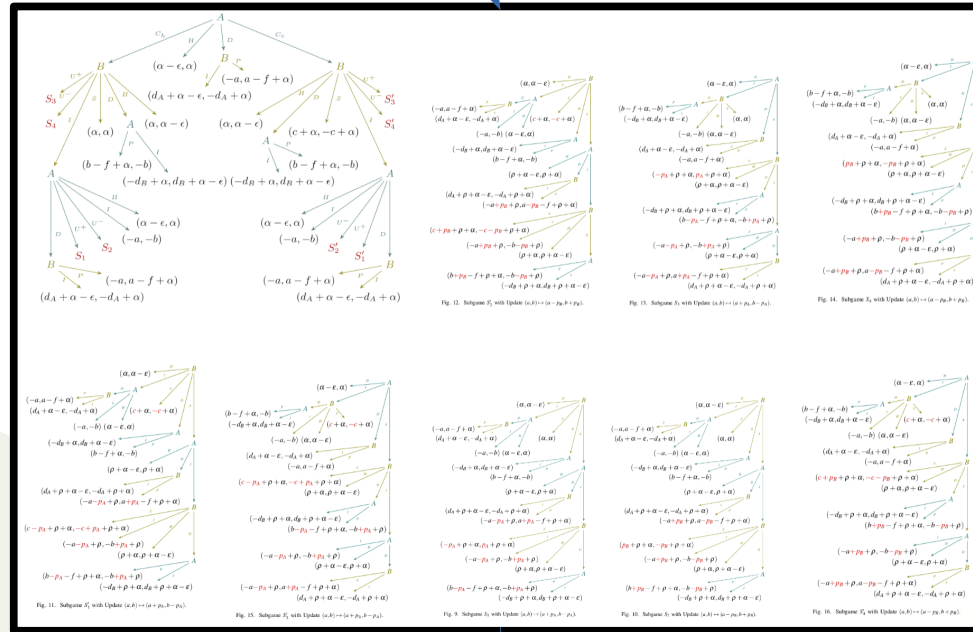
FMBC 2022

August 11
Haifa, Israel

L. Brugger, L. Kovács, A. Petković Komel,
S. Rain, and M. Rawson

Modeling Blockchain Protocols

model



The Bitcoin Lightning Network:
Scalable Off-Chain Instant Payments

Joseph Poon Thaddeus Dryja
joseph@lightning.network rx@avsomnet.org

January 14, 2016

e.g. Lightning,
Fulgor, Blitz

The bitcoin protocol volume in all c



apply



check



Towards a Game-Theoretic Security Analysis of Off-Chain Protocols

Security Properties



no profit from deviation

- ▶ **Collusion Resilience:** no subgroup of players profits from deviation
- ▶ **Practicality:** following protocol best choice in each step

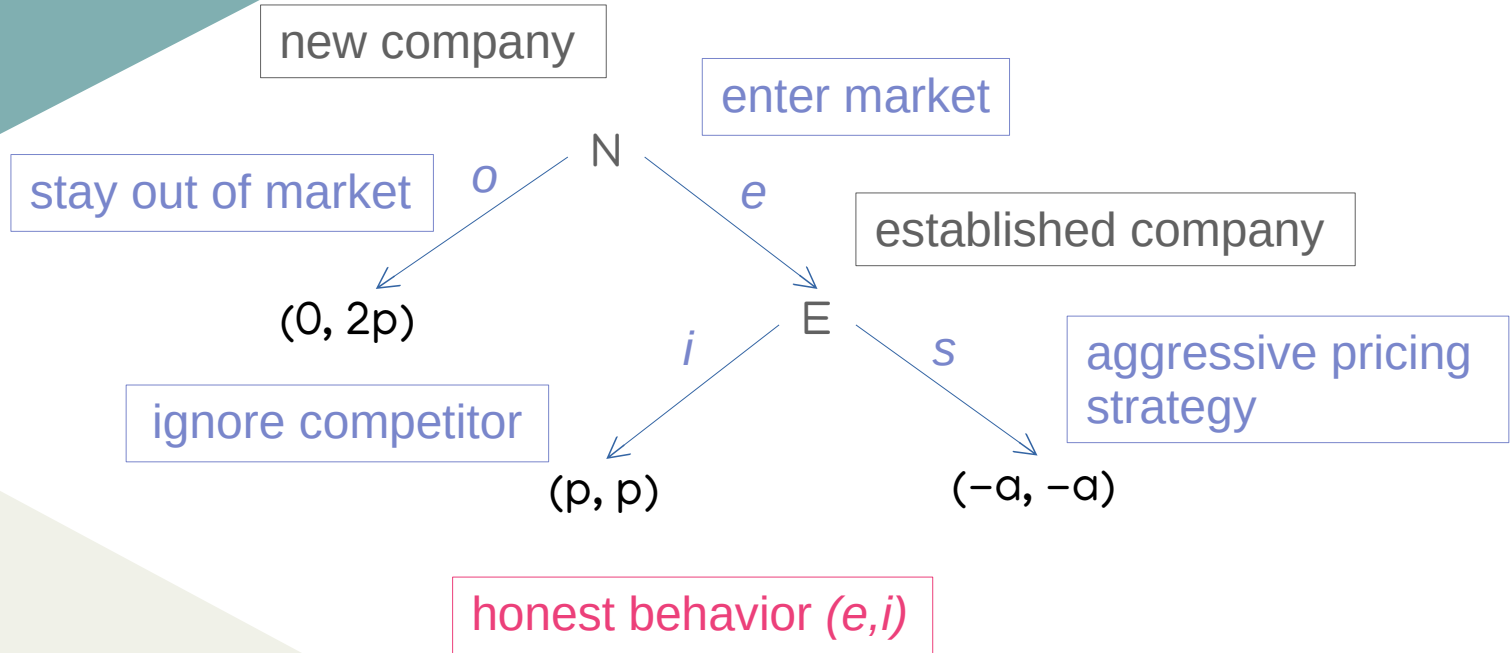


honest users cannot be harmed (lose resources)

- ▶ **Weak Immunity:** A **joint strategy** σ is called *weak immune*, if every player that follows σ gets utility ≥ 0 , regardless of how the other players behave.

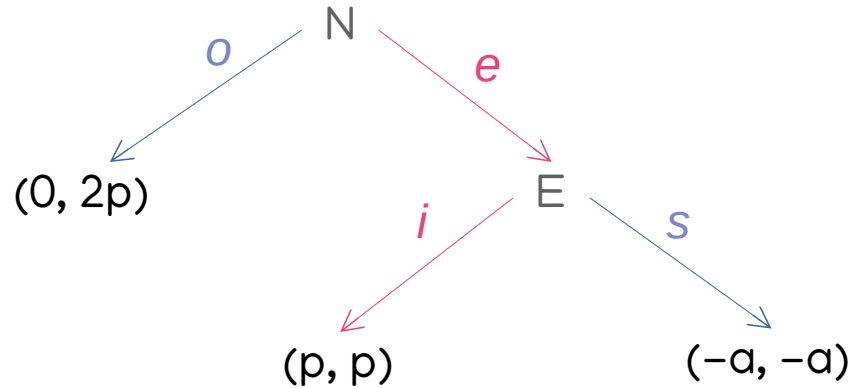
Example Game

Market Entry Game:



► $a, p > 0$ integers

Weak Immunity of Market Entry



- ▶ Is (e,i) weak immune?
- ▶ Can E be harmed (lose resources)? → NO
- ▶ Can N be harmed (lose resources)? → YES

NOT weak immune, for any $p, a > 0$!

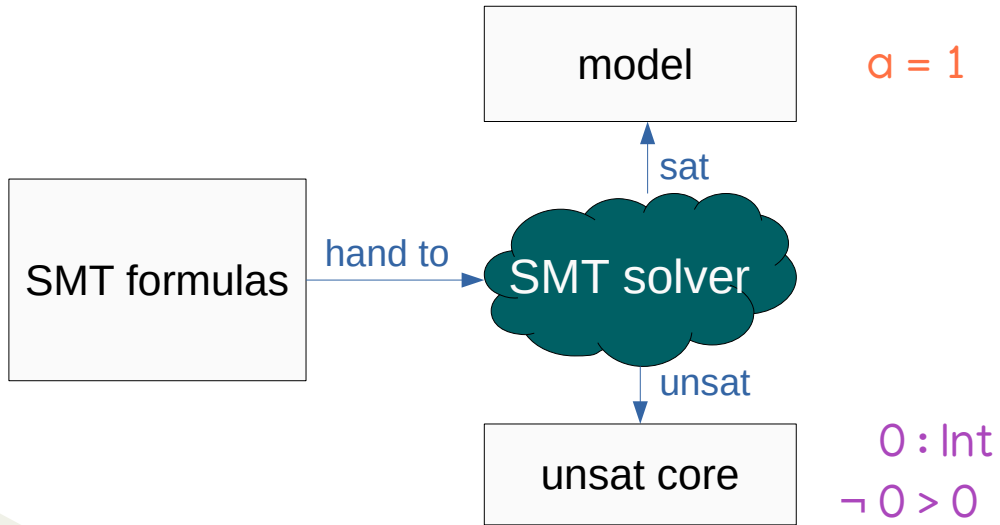
SMT Solving

Example 1:

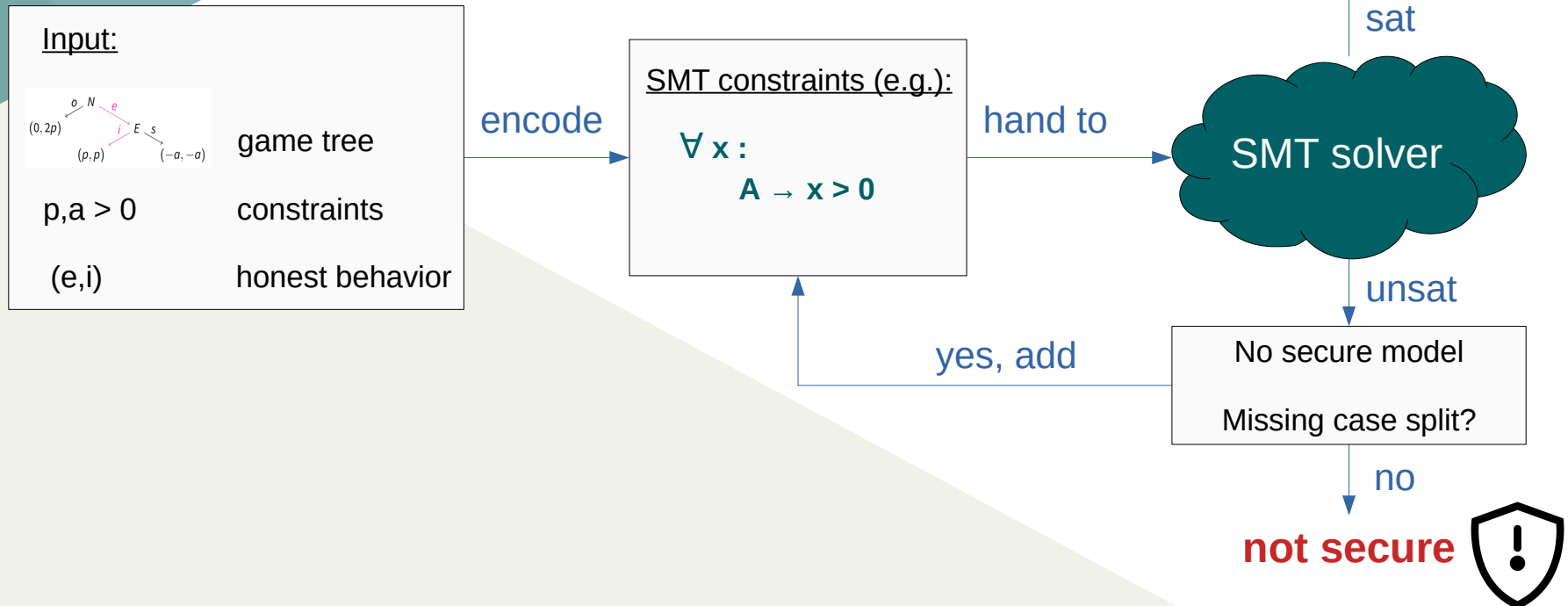
$a : \text{Int}$
 $a > 0$

Example 2:

$\forall a : \text{Int} . a > 0$

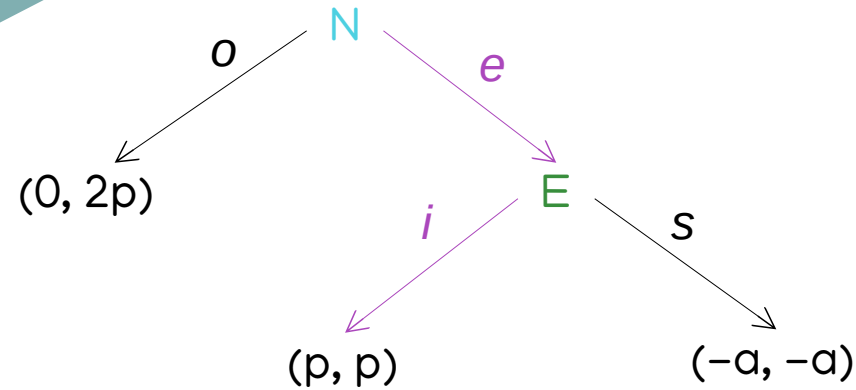


Automation Framework



Encoding Weak Immunity

$a, p > 0$ integers



$\forall p, a \text{ Int} : (a > 0 \wedge p > 0) \rightarrow$

$(o \vee e) \wedge (i \vee s) \wedge$

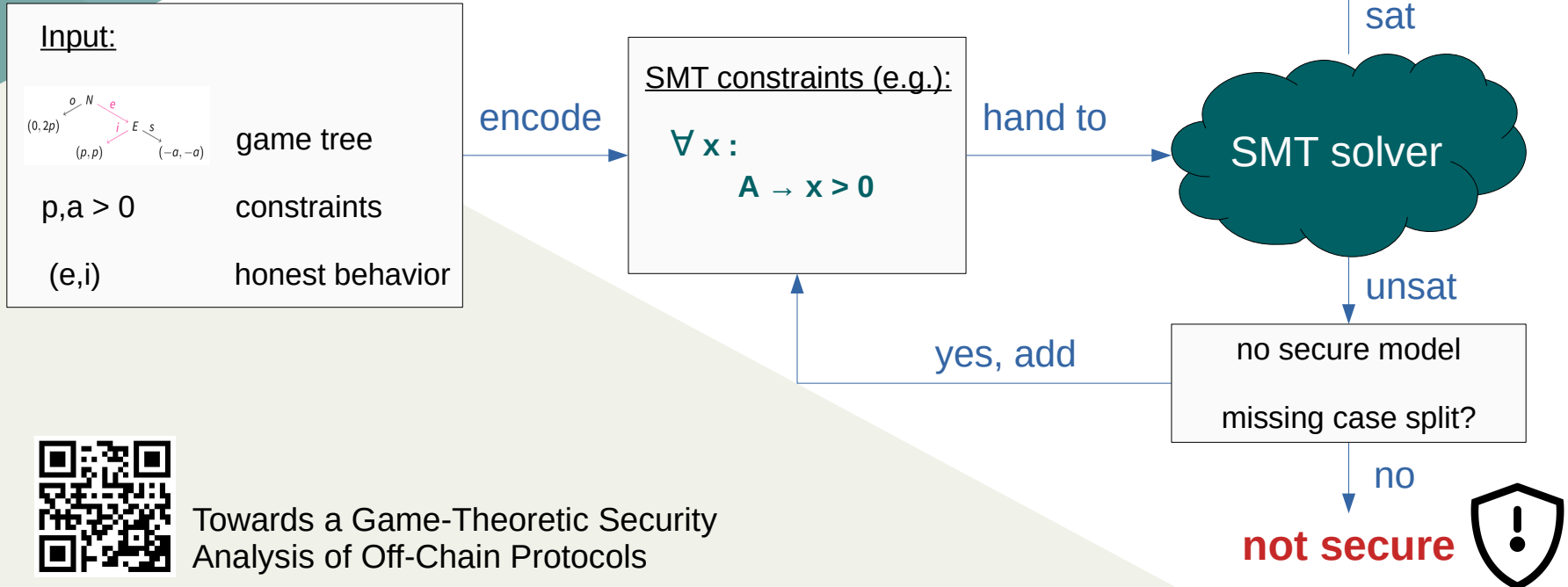
$\neg(o \wedge e) \wedge \neg(i \wedge s) \wedge$

$e \wedge i \wedge$

$(o \rightarrow 0 \geq 0) \wedge (e \rightarrow p \geq 0 \wedge -a \geq 0) \wedge$

$(2p \geq 0) \wedge (i \rightarrow p \geq 0) \wedge (s \rightarrow -a \geq 0)$

Take Away



Towards a Game-Theoretic Security Analysis of Off-Chain Protocols