

# Non-interference in Constructive Authorization Logic

Deepak Garg and Frank Pfenning  
Carnegie Mellon University

# Authorization and logic

---

- Authorization
  - Deepak wants to read foo.pdf ...
  - *Should* access be granted?
  - *Why* should access be granted?
- Logic
  - admin says `may_read(deepak, foo.pdf)`
  - *Is there* a proof?
  - *What is* the proof?

# Design emphasis

---

- Proof-theoretic, cut-elimination
- Intuitionistic authorization logic
- Logical explanation of connective “says”
- Non-interference

# Example: Grey Project at CMU

---

- Office door lock has a bluetooth device and processor
- Principal approaches door with a cell phone
- Authorization dialog between cell phone and door
- Door opens (or may not)

# Example: Policy

---

- I can access my door
- My advisor can access my door
- Department Head can decide who my advisor is

# I can access my office

---

- My office is WeH 8121
- Policy: *I can access my door*
- Door challenges cell phone for a proof:  
? : deepak says open (deepak, WeH.8121)
- Cell phone signs  
deepak says open (deepak, WeH.8121)  
with my private key to get a certificate c5698h728

# I can access my office

---

- Cell phone sends c5698h728 to door
- Door verifies (cryptographically)
  - c5698h728 : deepak says open (deepak, WeH.8121)
- Door opens

# My advisor can access my office

---

- Policies:
  - My advisor can access my office
  - Department Head can decide who my advisor is
- Expressed as policy axiom
$$r1 : \forall S. \text{depthead says advisor } (S, \text{deepak}) \supset$$
$$\text{deepak says open } (S, \text{WeH.8121})$$
- Policy known to door, cell phone, advisor

# My advisor can access my office

---

- Frank (my advisor) approaches door
- Door challenges:
  - ? : deepak says open (frank, WeH.8121)
- Frank's phone asks database for a proof:
  - ? : depthead says advisor (frank, deepak)
- Database replies with a proof
  - c9722k902 : depthead says advisor (frank, deepak)

# My advisor can access my office

---

- Frank's phone now knows:
  - $r1 : \forall S. \text{depthhead says advisor } (S, \text{deepak}) \supset$   
 $\text{deepak says open } (S, \text{WeH.8121})$
  - $c9722k902 : \text{depthhead says advisor } (\text{frank}, \text{deepak})$
- Phone combines the two to produce a proof  
 $r1 [\text{frank}] (c9722k902) : \text{deepak says open } (\text{frank}, \text{WeH.8121})$
- Phone sends proof to door – Door checks proof  
– Door opens

# Grey Project

---

- Presently uses higher order logic
- Can be done with first-order logic
  - Easier proof theory

# Logic Design with Judgments

---

- Judgments are objects of knowledge
- Our judgments:
  - A true : proposition A is true
  - K affirms A : principal K affirms the truth of A
- Deductions are evidence for judgments
- Connectives defined by right and left rules
- Right and left rules must match up
  - Cut elimination

# Hypothetical Judgments

---

$A_1 \text{ true}, \dots, A_n \text{ true} \Rightarrow B \text{ true}$

$A_1 \text{ true}, \dots, A_n \text{ true} \Rightarrow K \text{ affirms } B$

$$\frac{P \text{ atomic}}{\Gamma, P \text{ true} \Rightarrow P \text{ true}} \text{ (HYP)}$$

# Implication

---

- Right rule

$$\frac{\Gamma, A \text{ true} \Rightarrow B \text{ true}}{\Gamma \Rightarrow A \supset B \text{ true}} (\supset R)$$

- Left rule

$$\frac{\Gamma \Rightarrow A \text{ true} \quad \Gamma, B \text{ true} \Rightarrow \gamma}{\Gamma, A \supset B \text{ true} \Rightarrow \gamma} (\supset L)$$

# Affirmation

---

- Affirmation is a judgment different from truth
- All principals are willing to affirm true statements

$$\frac{\Gamma \Rightarrow A \text{ true}}{\Gamma \Rightarrow K \text{ affirms } A} \text{ (affirms)}$$

# The connective “says”

---

- “says” *internalizes* the judgment “affirms”
- Right rule

$$\frac{\Gamma \Rightarrow K \text{ affirms } A}{\Gamma \Rightarrow (K \text{ says } A) \text{ true}} \text{ (says } R)$$

- Left rule

$$\frac{\Gamma, A \text{ true} \Rightarrow K \text{ affirms } C}{\Gamma, (K \text{ says } A) \text{ true} \Rightarrow K \text{ affirms } C} \text{ (says } L)$$

# “K says” is a Strong Monad

---

- K-indexed family of strong monads

$$\vdash A \supset K \text{ says } A$$

$$\vdash A \supset B \supset (K \text{ says } A) \supset (K \text{ says } B)$$

$$\vdash (K \text{ says } A) \supset (A \supset K \text{ says } C) \supset K \text{ says } C$$

$$\vdash (K \text{ says } (K \text{ says } A)) \supset K \text{ says } A$$

- Corresponds to the lax modality from lax logic [dePaiva et al '98]

# Cut-elimination

---

- Cut is global soundness
  1. If  $\Gamma \Rightarrow A$  true and  $\Gamma, A$  true  $\Rightarrow J$ , then  $\Gamma \Rightarrow J$ .
  2. If  $\Gamma \Rightarrow K$  affirms  $A$  and  $\Gamma, A$  true  $\Rightarrow K$  affirms  $C$ , then  $\Gamma \Rightarrow K$  affirms  $C$ .
- Proof by structural induction
- Mechanically verified with Twelf

# Identity

---

- Identity is global completeness

For every  $A$ :  $\Gamma, A \text{ true} \Rightarrow A \text{ true}$ .

- Proof by induction on  $A$

# Consequences

---

- Consistency:

$\not\Rightarrow \perp$  true

$\not\Rightarrow ((K \text{ says } \perp) \supset \perp)$  true

- Subformula property
- Independence: More connectives can be added through right and left rules
- *Non-interference* properties

# Non-interference

---

- Principals are independent in the logic
- In the absence of explicit connections, assumption “K says A” cannot affect provability of “L says B”
- Only dependence via policies
- Simple non-interference theorem:  
If  $\Gamma$  and  $J$  are quantifier free and do not mention principal  $K$ , then  $\Gamma, (K \text{ says } A) \text{ true} \Rightarrow J$  iff  $\Gamma \Rightarrow J$ .
- Refined version in paper

# Affirmation flow

---

- More sophisticated properties involving *flow of affirmation* can be proved

- Example:

$r1 : \forall S. \text{depthhead says advisor } (S, \text{deepak}) \supset$

$\text{deepak says open } (S, \text{WeH.8121})$

$r2 : \text{deepak says open } (\text{deepak}, \text{WeH.8121})$

Affirmation flow relation:

$\text{depthhead.advisor} \leq \text{deepak.open}$

# Affirmation flow

---

- Let  $\Gamma = \{r1, r2\}$
- For this  $\Gamma$ ,  
depthhead.open  $\not\leq$  deepak.open

$\Gamma$ , depthhead says open(X, Y)  $\Rightarrow$  deepak says open(Z, U)

iff

$\Gamma \Rightarrow$  deepak says open(Z, U)

# Affirmation Flow: Decidability

---

- Theorem: Relation  $\leq$  is decidable for all policies
  - (Whole logic is undecidable)
- Gives an approximate method to automatically analyze policies for possible consequences

# Further Work: Linear + Knowledge extensions

---

- “Use once” authorization
- Possessed resources (e.g. money)
- Resource based transactions like credit card authorization, etc.
- Proof-theory straightforward
- Non-interference analysis might be much harder – not yet explored

# Most Closely Related Work

---

- [Abadi, Burrows, Lampson, Plotkin'93]  
propositional, rich calculus of principals
- [De Treville'02] Binder  
datalog fragment, decidable, logic programming, modality unclear
- [Abadi, ICFP'06 to appear] Non-interference properties using DCC

# Conclusion

---

- Contributions
  - Intuitionistic authorization logic
  - Affirmation is indexed family of strong monads
  - Simple proof theory, cut-elimination
  - Meta-theoretic analysis (Non-interference)
- Future Work
  - Real examples
  - Linear extensions (proof theory done)
  - Implementation of linear extensions
  - Temporal features (e.g. short lived certificates)