

A Constructive Conditional Logic for Access Control: a completeness result and a sequent calculus

Valerio Genovese¹, Laura Giordano², Valentina Gliozzi³, and Gian Luca Pozzato³

¹ Computer Science and Communications Research Unit - University of Luxembourg - Walferdange, Luxembourg valerio.genovese@uni.lu

² Dipartimento di Informatica - Università del Piemonte Orientale - Alessandria, Italy
laura@mf.n.unipmn.it

³ Dipartimento di Informatica - Università degli Studi di Torino - Torino, Italy
{[gliozzi](mailto:gliozzi@di.unito.it), [pozzato](mailto:pozzato@di.unito.it)}@di.unito.it

Abstract. We define an Intuitionistic Conditional Logic for Access Control called C_{ICL} . The logic C_{ICL} is based on a conditional language allowing principals to be defined as arbitrary formulas and it includes few uncontroversial axioms of access control logics. We provide an axiomatization and a Kripke model semantics for the logic C_{ICL} , prove that the axiomatization is sound and complete with respect to the semantics, and define a sound, complete and cut-free labelled sequent calculus for it.

1 Introduction

Access control is concerned with the decision when to accept or deny a request from a *principal* (e.g., user, program) to do an operation on an object. In practice, an access control system is a product of several, often independent, distributed entities with different policies that interact in order to determine access to resources. In order to specify and reason about such systems, many formal frameworks have been proposed [1–5].

A common feature of most well-known approaches is the employment of constructive logics enriched with formulas of the form A **says** φ , intuitively meaning that the principal A *asserts* or *supports* φ to hold in the system. In [6] it is shown that an intuitionistic interpretation of the modality “says” allows to avoid unexpected conclusions that are derivable when “says” is given an axiomatization in classical logic.

The treatment of the operator “says” as a modality can be found in [7], which introduces a logical framework, FSL, based on multi-modal logic methodology. In [8] an access control logic, ICL, is defined as an extension of intuitionistic propositional logic, in which the operator **says** is given a modal interpretation in the logic S4.

In this paper we show that conditional logics [9] can provide a natural framework to define axiomatization, semantics and proof methods for access control logics. We present an intuitionistic logic, C_{ICL} , which integrates access control logics with conditional logics. We formalize the **says** operator as a conditional normal modality so that A **says** ϕ is regarded as a conditional implication $A \Rightarrow \phi$, meaning that proposition ϕ holds in all the preferred worlds for the principal A . The generality of this approach opens the way to the formalization of the so called boolean principals [8], that is, principals which are formed by boolean combination of atomic principals.

From the access control point of view, the **says** operator satisfies the axioms of the “basic logic of access control” ICL [8]. We define a sound and complete Kripke semantics for C_{ICL} as well as a sound and complete cut-free sequent calculus for it.

The paper is structured as follows. In Section 2 we introduce the axiomatization and the semantics for the intuitionistic conditional logic C_{ICL} and we compare it with existing approaches. In Section 3 we show that the axiomatization is sound and complete with respect to the semantics. In Section 4 we define a cut-free sequent calculus for C_{ICL} and we prove its soundness and completeness. Section 5 contains the conclusions and a discussion of related work.

2 The logic C_{ICL}

In this section, we introduce the conditional intuitionistic logic C_{ICL} for access control by defining its axiomatization and Kripke semantics. Then we discuss some conditional axioms which can be introduced to model properties of boolean principals, namely compound principals formed by boolean connectives. Indeed, while the basic axioms for access control are rather uncontroversial [8, 6], we believe that the same cannot yet be said about the axioms governing the behavior of boolean principals.

The formulation of the *says* modality as a conditional operator allows boolean principals to be modelled in a natural way, since in a conditional formula A **says** ϕ , both A and ϕ are arbitrary formulas. For instance, we can write, $A \wedge B$ **says** ϕ to mean that principals A and B jointly say that ϕ , and $A \vee B$ **says** ϕ to mean that principals A and B independently say that ϕ . Indeed, conditional logics provide a natural generalization of multimodal logics to the case when modalities are labelled by arbitrary formulas.

2.1 Axiom System

We define the language \mathcal{L} of the logic C_{ICL} . Let ATM be a set of atomic propositions. The formulas of \mathcal{L} are defined inductively as follows: if $P \in ATM$, then $P \in \mathcal{L}$; $\perp \in \mathcal{L}$, where \perp is a proposition which is always false; if A, φ, φ_1 and φ_2 are formulas of \mathcal{L} , then $\neg\varphi, \varphi_1 \wedge \varphi_2, \varphi_1 \vee \varphi_2, \varphi_1 \rightarrow \varphi_2$, and A **says** φ are formulas of \mathcal{L} .

The intended meaning of the formula A **says** ψ , where A and ψ are arbitrary formulas, is that *principal A says that ψ* , namely, “the principal A asserts or supports ψ ” [8]. Although the principal A is an arbitrary formula, in order to stress the fact that a formula is playing the role of a principal, we will denote it by A, B, C, \dots while we will use greek letters for arbitrary formulas.

The *axiom system* of the logic C_{ICL} contains the following axioms and inference rules:

(TAUT)	all tautologies of intuitionistic logic
(K)	A says $(\alpha \rightarrow \beta) \rightarrow (A$ says $\alpha \rightarrow A$ says $\beta)$
(UNIT)	$\alpha \rightarrow (A$ says $\alpha)$
(C4)	$(A$ says $(A$ says $\alpha)) \rightarrow (A$ says $\alpha)$
(MP)	If $\vdash \alpha$ and $\vdash \alpha \rightarrow \beta$ then $\vdash \beta$
(RCEA)	If $\vdash A \leftrightarrow B$ then $\vdash (A$ says $\gamma) \leftrightarrow (B$ says $\gamma)$
(RCK)	If $\vdash \alpha \rightarrow \beta$ then $\vdash (A$ says $\alpha) \rightarrow (A$ says $\beta)$

We say that a formula α is a theorem of the logic, and write $\vdash \alpha$ if there is a derivation of α from the above axioms and rules. We say that α can be derived from a set of formulas Γ , and write $\Gamma \vdash \alpha$, if there are $\gamma_1, \dots, \gamma_n$ in Γ such that $\vdash \gamma_1 \wedge \dots \wedge \gamma_n \rightarrow \alpha$. The rule (MP) is modus ponens. (RCEA) and (RCK) are standard inference rules for conditional logics. (RCK) plays the role of the rule of Necessitation (if $\vdash \phi$ then $\vdash \Box \phi$) in modal/multimodal logic. The axiom (K) belongs to the axiomatization of all normal modal logics and it is derivable in “normal” conditional logics. (UNIT), (K) and (C4) are the characterizing axioms of the access control logics ICL [8]. All the tautologies of intuitionistic logic are included, so that the resulting logic is an intuitionistic version of a conditional logic. As a major difference with ICL axiomatization [8], our axiomatization above also includes inference rules (RCK) and (RCEA) for the **says** modality. We will come back to comment on this in section 2.3.

2.2 Semantics

The semantics of the logic C_{ICL} is defined as follows.

Definition 1. A C_{ICL} model has the form $\mathcal{M} = (S, \leq, \{R_A\}, h)$ where: $S \neq \emptyset$ is a set of items called worlds; \leq is a partial order over S ; R_A is a binary relation on S associated with the formula A ; h is an evaluation function $ATM \rightarrow Pow(S)$ that associates to each atomic proposition P the set of worlds x in which P is true.

We define the truth conditions of formulas with respect to worlds in a model \mathcal{M} , by the relation $\mathcal{M}, x \models \phi$, as follows. We use $[[\phi]]$ to denote $\{y \in S \mid \mathcal{M}, y \models \phi\}$.

1. $\mathcal{M}, t \models P \in ATM$ iff, for all s such that $t \leq s$, $s \in h(P)$
2. $\mathcal{M}, t \models \varphi \wedge \psi$ iff $\mathcal{M}, t \models \varphi$ and $\mathcal{M}, t \models \psi$
3. $\mathcal{M}, t \models \varphi \vee \psi$ iff $\mathcal{M}, t \models \varphi$ or $\mathcal{M}, t \models \psi$
4. $\mathcal{M}, t \models \varphi \rightarrow \psi$ iff for all s such that $t \leq s$ (if $\mathcal{M}, s \models \varphi$ then $\mathcal{M}, s \models \psi$)
5. $\mathcal{M}, t \models \neg \varphi$ iff, for all s such that $t \leq s$, $\mathcal{M}, s \not\models \varphi$
6. $\mathcal{M}, t \not\models \perp$
7. $\mathcal{M}, t \models A \text{ says } \psi$ iff, for all s such that $tR_A s$, $\mathcal{M}, s \models \psi$.

We say that ϕ is valid in a model \mathcal{M} if $\mathcal{M}, t \models \phi$ for all $t \in S$. We say that ϕ is valid tout court (and write $\models \phi$) if ϕ is valid in every model. We extend the notion of validity to a set of formulas Γ in the obvious way: for all t , $\mathcal{M}, t \models \Gamma$ if $\mathcal{M}, t \models \psi$ for all $\psi \in \Gamma$. Last, we say that ϕ is a logical consequence of Γ (and write $\Gamma \models \phi$) if, for all models \mathcal{M} , for all worlds t , if $\mathcal{M}, t \models \Gamma$, then $\mathcal{M}, t \models \phi$.

The relations \leq and R_A must satisfy the following conditions:

- (a) $\forall t, s, z \in S$, if $s \leq t$ and $tR_A z$ then $sR_A z$;
- (b) $\forall t, s \in S$, if $sR_A t$, then $s \leq t$;
- (c) $\forall t, s \in S$, if $sR_A t$, then $\exists z \in S$ such that $sR_A z$ and $zR_A t$
- (d) if $[[A]] = [[B]]$, then $R_A = R_B$,

Conditions (b) and (c) are, respectively, the semantic conditions associated with the axioms (UNIT) and (C4), while condition (a) is needed to enforce the property that a formula true in a world t is also true in all worlds reachable from s by the relation \leq

(i.e., in all worlds s such that $t \leq s$). Condition (d) is the well-known condition for normality in conditional logics, claiming that the accessibility relation R_A is associated with the semantic interpretation of A .

Observe that, in the semantics above, the binary relation R_A plays the role of the selection function f , which is used in most formulations of conditional logic semantics. In particular, $sR_A t$ corresponds to $t \in f(A, s)$, and conditions (a), (b), (c) and (d) above are indeed conditions on the selection function f , as usual in conditional logics.

It is worth noticing that the notion of logical consequence defined above can be used to verify that a request φ of a principal A is compliant with a set of policies. Intuitively, given a set of formulas Γ representing policies, we say that A is compliant with Γ iff $\Gamma, A \text{ says } \varphi \models \varphi$. For instance, if Γ contains the following formulas:

$$\begin{aligned} & ((\text{admin says deletefile1}) \rightarrow \text{deletefile1}) \\ & \text{admin says } (\text{Bob says deletefile1} \rightarrow \text{deletefile1}) \end{aligned}$$

we obtain that

$$\Gamma, \text{Bob says deletefile1} \models \text{deletefile1}$$

2.3 Discussion

Before proving the soundness and completeness result for the logic C_{ICL} , we want to comment about our approach for allowing boolean principals as compared with the approach proposed by Garg and Abadi in [8]. Also, we discuss which axioms and properties could be possibly added to the logic C_{ICL} to capture the intended properties of boolean principals.

Garg and Abadi [8] have defined a logic ICL as an extension of intuitionistic propositional logic, whose axiomatization includes “all the inference rules of intuitionistic propositional logic” as well as the axioms (UNIT), (K) and (C4) above, called (unit), (cuc), and (idem), respectively. While the inference rule (RCK) is derivable from ICL axiomatization, as a difference with our axiomatization, their axiomatization does not include the inference rule (RCEA) which allows to deal with equivalent principals.

In [8] Garg and Abadi provide a translation of the logic ICL to modal logic S4. In particular, they translate the formula $A \text{ says } \phi$ to $\Box(A \vee \phi')$, where ϕ' is the translation of ϕ according to a variant of Gödel translation from intuitionistic logic to S4.

For what concerns non-atomic principals, Garg and Abadi [8] introduce the logic $\text{ICL}^{\mathcal{B}}$ for defining boolean principals. In $\text{ICL}^{\mathcal{B}}$, $A \wedge B \text{ says } \phi$ is the same as $A \text{ says } \phi \wedge B \text{ says } \phi$, while $A \vee B \text{ says } \phi$ means that, by combining the statements of A and B , ϕ can be concluded. We can observe that the interpretation of conjunction and disjunction between principals we have given in this paper is actually the opposite one. In fact, our interpretation of the statement $A \wedge B \text{ says } \phi$ is that A and B jointly (combining their statements) say that ϕ . It comes from the interpretation of the statement as a conditional implication: A and B (conjointly) conditionally prove ϕ . Similarly, our interpretation of the statement $A \vee B \text{ says } \phi$ is that A and B disjointly (independently) say that ϕ , which comes from the reading of the conditional formula as A and B (disjointly) conditionally prove ϕ . Due to this, let us say, superficial difference, the properties that Garg and Abadi

discuss for $A \wedge B$ **says** ϕ are relevant for our statement $A \vee B$ **says** ϕ and, vice-versa, the properties they discuss for $A \vee B$ **says** ϕ are relevant for our statement $A \wedge B$ **says** ϕ .

The conditional logic we have defined is rather weak, as it does not contain specific axioms which would enforce intended properties of boolean principals, as those discussed in [8]. Let us now consider some of them.

Concerning the statement $A \vee B$ **says** ϕ , we could expect that A and B disjointly (independently) say that ϕ if both A says ϕ and B says ϕ . This property can be captured by the following axiom:

$$A \text{ says } \phi \wedge B \text{ says } \phi \rightarrow A \vee B \text{ says } \phi$$

which corresponds to the well known axiom (CA) of conditional logics [9]. Similarly, we could expect that the converse axiom

$$A \vee B \text{ says } \phi \rightarrow A \text{ says } \phi \wedge B \text{ says } \phi$$

holds. The two axioms together would enforce the property that A and B disjointly say that ϕ if and only if A says that ϕ and B says that ϕ . Mutatis mutandis, this appears to be a wanted property, according to [8]. Concerning the statement $A \wedge B$ **says** ϕ , we could expect that A and B jointly say that ϕ when A (or B) alone says that ϕ . This condition could be enforced by introducing the following axiom

$$A \text{ says } \phi \rightarrow A \wedge B \text{ says } \phi$$

which, however, is a very controversial axiom of conditional logics, called monotonicity.

The impact of the addition of the above axioms to the axiomatization of the logic C_{ICL} has to be studied. While we could expect the addition of the axiom (CA) and its converse to be harmless, the same cannot be said for the monotonicity axiom, whose introduction could cause the logic to collapse or become inconsistent.

3 Soundness and Completeness

In this section we prove that the axiomatization given above is sound and complete with respect to the semantics of Definition 1.

Theorem 1 (Soundness). *The axiomatization of the logic C_{ICL} given in Section 2.1 is sound w.r.t. the semantics in Definition 1: given a formula $\varphi \in \mathcal{L}$, if $\Gamma \vdash \varphi$, then $\Gamma \models \varphi$.*

Proof. It is easy to prove that each axiom is a valid formula and, for each inference rule, if the antecedent of the rule is a valid formula, the consequence of the rule is also a valid formula. □

The completeness proof we present is based on the proof of completeness for the Kripke semantics of intuitionistic logic in [10] (see section 6, page 87) and extends it to deal with the modalities **says** in the language and, more precisely, with the interplay between the relation \leq and the accessibility relations R_A associated with the modalities.

Definition 2 (Consistency). Γ is consistent iff $\Gamma \not\vdash \perp$. If Γ has an infinite number of formulas, we say that Γ is consistent iff there are no finite $\Gamma_0 \subset \Gamma$ such that $\Gamma_0 \vdash \perp$.

Definition 3 (Saturation). Let Γ be a set of well formed formulas, we say that Γ is saturated iff 1. Γ is consistent; 2. if $\Gamma \vdash \varphi$, then $\varphi \in \Gamma$; 3. if $\Gamma \vdash \varphi \vee \psi$, then $\Gamma \vdash \varphi$ or $\Gamma \vdash \psi$.

Lemma 1 (Saturated Extensions). Suppose $\Gamma \not\vdash \varphi$, then there is a saturated extension Γ^* of Γ such that $\Gamma^* \not\vdash \varphi$.

The proof can be done by transfinite induction as in [10].

Lemma 2. Let Γ be a set of formulas and let $\Delta = \{\varphi : A \text{ says } \varphi \in \Gamma\}$. If $\Delta \vdash \psi$, then $\Gamma \vdash A \text{ says } \psi$.

Proof. Suppose there is a derivation of ψ from Δ . Then, there must be a finite set of formulas $\{\varphi_1, \dots, \varphi_n\} \subseteq \Delta$ such that $\{\varphi_1, \dots, \varphi_n\} \vdash \psi$. By definition of \vdash , $\vdash \varphi_1 \wedge \dots \wedge \varphi_n \rightarrow \psi$. By (RCK) and (K), $\vdash A \text{ says } \varphi_1 \wedge \dots \wedge A \text{ says } \varphi_n \rightarrow A \text{ says } \psi$, and from definition of \vdash (and since $A \text{ says } \varphi_i \in \Gamma$ for all $i = 1, \dots, n$) we conclude that $\Gamma \vdash A \text{ says } \psi$. \square

Definition 4 (Canonical model construction). Let Γ_0 be any saturated set of formulas. Then we define $\mathbf{M} = (S, \leq, \{R_A\}, \Gamma_0, h)$ such that: S is the set of all saturated $\Gamma \supseteq \Gamma_0$; $\Gamma_1 \leq \Gamma_2$ iff $\Gamma_1 \subseteq \Gamma_2$; $\Gamma_1 R_A \Gamma_2$ iff $\{\alpha \mid A \text{ says } \alpha \in \Gamma_1\} \subseteq \Gamma_2$; for all $P \in \text{ATM}$, $h(P) = \{\Gamma \in S \mid P \in \Gamma\}$.

Observe that in the above construction, $\Gamma_0 \in S$.

Lemma 3. For all $\Gamma \in S$ and each wff formula φ , we have that $\Gamma \models \varphi$ iff $\varphi \in \Gamma$.

Proof. By induction on the complexity of φ . In case φ is an atomic formula, the lemma holds by definition. For $\varphi \equiv \phi \wedge \psi$ the proof is easy and therefore omitted. For $\varphi \equiv \phi \vee \psi$, then $\Gamma \models \phi \vee \psi \Leftrightarrow (\Gamma \models \phi \text{ or } \Gamma \models \psi) \Leftrightarrow (\phi \in \Gamma \text{ or } \psi \in \Gamma) \Leftrightarrow \phi \vee \psi \in \Gamma$ (by the saturation of Γ). For $\varphi \equiv \phi \rightarrow \psi$, suppose $\Gamma \models \phi \rightarrow \psi$. Then for all saturated $\Gamma' \supset \Gamma$ we have that if $\Gamma' \models \phi$, then $\Gamma' \models \psi$. Assume $\Gamma \not\vdash \phi \rightarrow \psi$, then $\Gamma \cup \{\phi\} \not\vdash \psi$; let Γ' be a saturated extension of $\Gamma \cup \{\phi\}$ such that $\Gamma' \not\vdash \psi$, then $\Gamma' \models \phi$ but not $\Gamma' \models \psi$ (induction hypothesis); this contradicts $\Gamma \models \phi \rightarrow \psi$, hence $\Gamma \vdash \phi \rightarrow \psi$. As Γ is saturated, by condition 2 in Definition 3, $\phi \rightarrow \psi \in \Gamma$. The converse is trivial. For $\varphi \equiv A \text{ says } \phi$, suppose $\Gamma \models A \text{ says } \phi$. Hence, for all Γ' such that $\Gamma R_A \Gamma'$, $\Gamma' \models \phi$. By inductive hypothesis, $\phi \in \Gamma'$. Let $\Delta = \{\alpha : A \text{ says } \alpha \in \Gamma\}$. By construction, $\Gamma' \supseteq \Delta$. Assume, for a contradiction, that $A \text{ says } \phi \notin \Gamma$. By condition 2 in Definition 3, $\Gamma \not\vdash A \text{ says } \phi$. Then, by Lemma 2, $\Delta \not\vdash \phi$. By Lemma 1, there is a saturated extension Δ^* of Δ such that $\Delta^* \not\vdash \phi$. This contradicts the fact that, for all Γ' such that $\Gamma R_A \Gamma'$, $\phi \in \Gamma'$. The converse is trivial. \square

Lemma 4. Let \mathbf{M} be the canonical model as defined in Definition 4. \mathbf{M} satisfies the semantic conditions (a), (b), (c), and (d).

Proof. We have to prove that

- (a) $\forall \Gamma, \Gamma', \Gamma'' \in S$, if $\Gamma \leq \Gamma'$ and $\Gamma' R_A \Gamma''$ then $\Gamma R_A \Gamma''$
- (b) $\forall \Gamma, \Gamma' \in S$, if $\Gamma R_A \Gamma'$ then $\Gamma \leq \Gamma'$.
- (c) $\forall \Gamma, \Gamma' \in S$, if $\Gamma R_A \Gamma'$, then $\exists \Gamma'' \in S$ such that $\Gamma R_A \Gamma''$ and $\Gamma'' R_A \Gamma'$
- (d) $\forall \Gamma, \Gamma' \in S$, if $\Gamma R_A \Gamma'$ and $\vdash A \leftrightarrow B$ then $\Gamma R_B \Gamma'$.

The proof is straightforward. As an example, let us prove point (b). Given a saturated set Γ , we have to show that if $\Gamma R_A \Gamma'$ then $\Gamma \leq \Gamma'$. Assume that $\Gamma R_A \Gamma'$ and let $\alpha \in \Gamma$. By saturation of Γ and by (UNIT), $\alpha \rightarrow A$ says $\alpha \in \Gamma$. By (MP), A says $\alpha \in \Gamma$. Hence, by construction of the canonical model, $\alpha \in \Gamma'$. Therefore, $\Gamma \leq \Gamma'$. \square

By the above lemmas, we can conclude that:

Theorem 2 (Completeness). *The axiomatization of the logic C_{ICL} given in Section 2.1 is complete with respect to the semantics in Definition 1: given a formula $\varphi \in \mathcal{L}$, if $\Gamma \models \varphi$, then $\Gamma \vdash \varphi$.*

Proof. For a contradiction, suppose $\Gamma \not\vdash \varphi$. Then by Lemma 1 there is a saturated extension Γ^* of Γ such that $\Gamma^* \not\vdash \varphi$. By Definition 4 and Lemmas 3 and 4, we conclude that there is a (canonical) model $\mathbf{M} = (S, \leq, \{R_A\}, \Gamma^*, h)$ such that $\mathbf{M}, \Gamma^* \models \Gamma^*$ and $\mathbf{M}, \Gamma^* \not\models \varphi$. Since $\Gamma \subseteq \Gamma^*$, also $\mathbf{M}, \Gamma^* \models \Gamma$. It follows that φ is not a logical consequence of Γ , i.e. $\Gamma \not\models \varphi$. \square

4 A sequent calculus for C_{ICL}

In this section we present a sequent calculus for C_{ICL} . Our calculus is called $\text{Seq}_{C_{ICL}}$ and it makes use of labels to represent possible worlds, following the line of [11]. We are able to give an analytic, cut-free calculus for the logic C_{ICL} . The completeness of the calculus is an immediate consequence of the admissibility of cut.

In addition to the language \mathcal{L} of the logic C_{ICL} , we consider a denumerable alphabet of labels \mathcal{A} , whose elements are denoted by x, y, z, \dots . There are three types of labelled formulas:

1. *world formulas*, denoted by $x : A$, where $x \in \mathcal{A}$ and $A \in \mathcal{L}$, used to represent that the formula A holds in a world x ;
2. *transition formulas*, denoted by $x \xrightarrow{A} y$, representing that $x R_A y$;
3. *order formulas* of the form $y \geq x$ representing the partial order relation \leq .

A *sequent* is a pair $\langle \Gamma, \Delta \rangle$, usually denoted with $\Gamma \Rightarrow \Delta$, where Γ and Δ are multisets of labelled formulas. The intuitive meaning of a sequent $\Gamma \Rightarrow \Delta$ is: every model that satisfies all labelled formulas of Γ in the respective worlds (specified by the labels) satisfies at least one of the labelled formulas of Δ (in those worlds). This is made precise by the notion of *validity* of a sequent given in the next definition:

Definition 5 (Sequent validity). Given a model $\mathcal{M} = (S, \leq, \{R_A\}, h)$ for \mathcal{L} , and a label alphabet \mathcal{A} , we consider a mapping $I : \mathcal{A} \rightarrow S$. Let F be a labelled formula, we define $\mathcal{M} \models_I F$ as follows:

- $\mathcal{M} \models_I x : A$ iff $\mathcal{M}, I(x) \models A$
- $\mathcal{M} \models_I x \xrightarrow{A} y$ iff $I(x)R_AI(y)$
- $\mathcal{M} \models_I y \geq x$ iff $I(x) \leq I(y)$

We say that $\Gamma \Rightarrow \Delta$ is valid in \mathcal{M} if, for every mapping $I : \mathcal{A} \rightarrow S$, if $\mathcal{M} \models_I F$ for every $F \in \Gamma$, then $\mathcal{M} \models_I G$ for some $G \in \Delta$. We say that $\Gamma \Rightarrow \Delta$ is valid in C_{ICL} if it is valid in every \mathcal{M} .

In Figure 1 we present the rules of the calculus $\text{Seq}_{C_{ICL}}$ for C_{ICL} . As usual, we say that a sequent $\Gamma \Rightarrow \Delta$ is *derivable* in $\text{Seq}_{C_{ICL}}$ if it admits a *derivation*. A derivation is a tree whose nodes are sequents. A branch is a sequence of nodes $\Gamma_1 \Rightarrow \Delta_1, \Gamma_2 \Rightarrow \Delta_2, \dots, \Gamma_n \Rightarrow \Delta_n, \dots$. Each node $\Gamma_i \Rightarrow \Delta_i$ is obtained from its immediate successor $\Gamma_{i-1} \Rightarrow \Delta_{i-1}$ by applying *backward* a rule of $\text{Seq}_{C_{ICL}}$, having $\Gamma_{i-1} \Rightarrow \Delta_{i-1}$ as the conclusion and $\Gamma_i \Rightarrow \Delta_i$ as one of its premises. A branch is closed if one of its nodes is an instance of axioms, namely (AX) , (AX_{\geq}) , and (AX_{\perp}) , otherwise it is open. We say that a tree is closed if all its branches are closed. A sequent $\Gamma \Rightarrow \Delta$ has a derivation in $\text{Seq}_{C_{ICL}}$ if there is a closed tree having $\Gamma \Rightarrow \Delta$ as a root.

As an example, in Figure 2 we show a derivation in $\text{Seq}_{C_{ICL}}$ of an instance of the axiom (UNIT). In order to show that the formula $\alpha \rightarrow (A \text{ says } \alpha)$ is valid, we build a derivation in $\text{Seq}_{C_{ICL}}$ for the sequent $\Rightarrow u : \alpha \rightarrow (A \text{ says } \alpha)$.

As an another example, in Figure 3 we show a derivation in $\text{Seq}_{C_{ICL}}$ of an instance of the axiom (C4).

The calculus $\text{Seq}_{C_{ICL}}$ is sound and complete for the logic C_{ICL} , that is to say a formula $F \in \mathcal{L}$ is valid in C_{ICL} if and only if the sequent $\Rightarrow u : F$ is derivable in $\text{Seq}_{C_{ICL}}$. In order to prove this, we first need to show some basic structural properties of the calculus. First, we introduce the notion of complexity of a labelled formula:

Definition 6 (Complexity of a labelled formula $\text{cp}(F)$). We define the complexity of a labelled formula F as follows: $\text{cp}(x : A) = 2 * |A|$; $\text{cp}(x \xrightarrow{A} y) = 2 * |A| + 1$; $\text{cp}(y \geq x) = 2$, where $|A|$ is the number of symbols occurring in the string representing the formula A .

By the above definition, we have that all the rules of $\text{Seq}_{C_{ICL}}$ introduce in the premise(s) only formulas having a smaller complexity with respect to the formula to which the rule is applied.

Lemma 5 (Height-preserving admissibility of weakening). Given any formula F , if a sequent $\Gamma \Rightarrow \Delta$ has a derivation of height h , then $\Gamma \Rightarrow \Delta, F$ and $\Gamma, F \Rightarrow \Delta$ have a derivation of height $h' \leq h$.

Lemma 6 (Height-preserving label substitution). If a sequent $\Gamma \Rightarrow \Delta$ has a derivation of height h , then $\Gamma[x/y] \Rightarrow \Delta[x/y]$ has a derivation of height $h' \leq h$, where $\Gamma[x/y] \Rightarrow \Delta[x/y]$ is the sequent obtained from $\Gamma \Rightarrow \Delta$ by replacing all occurrences of the label x by the label y .

$\frac{}{(AX)} \Gamma, F \Rightarrow \Delta, F$ <small>F either $x : P, P \in ATM$ or $y \geq x$</small>	$(AX_{\perp}) \Gamma, x : \perp \Rightarrow \Delta$	$(AX_{\geq}) \Gamma \Rightarrow \Delta, x \geq x$
$\frac{\Gamma, y \geq x, y : A \Rightarrow \Delta, y : B}{\Gamma \Rightarrow \Delta, x : A \rightarrow B} (\rightarrow R)$ <small>y new</small>	$\frac{\Gamma, x : A \rightarrow B \Rightarrow \Delta, y \geq x \quad \Gamma, x : A \rightarrow B \Rightarrow \Delta, y : A \quad \Gamma, x : A \rightarrow B, y : B \Rightarrow \Delta}{\Gamma, x : A \rightarrow B \Rightarrow \Delta} (\rightarrow L)$	
$\frac{\Gamma, y \geq x \Rightarrow \Delta, y : A \quad \Gamma, y \geq x \Rightarrow \Delta, y : B}{\Gamma \Rightarrow \Delta, x : A \wedge B} (\wedge R)$ <small>y new</small>		$\frac{\Gamma, x : A \wedge B \Rightarrow \Delta, y \geq x \quad \Gamma, x : A \wedge B, y : A, y : B \Rightarrow \Delta}{\Gamma, x : A \wedge B \Rightarrow \Delta} (\wedge L)$
$\frac{\Gamma, y \geq x \Rightarrow \Delta, y : A, y : B}{\Gamma \Rightarrow \Delta, x : A \vee B} (\vee R)$ <small>y new</small>		$\frac{\Gamma, x : A \vee B \Rightarrow \Delta, y \geq x \quad \Gamma, x : A \vee B, y : A \Rightarrow \Delta \quad \Gamma, x : A \vee B, y : B \Rightarrow \Delta}{\Gamma, x : A \vee B \Rightarrow \Delta} (\vee L)$
$\frac{\Gamma, y \geq x, y : A \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, x : \neg A} (\neg R)$ <small>y new</small>		$\frac{\Gamma, x : \neg A \Rightarrow \Delta, y \geq x \quad \Gamma, x : \neg A \Rightarrow \Delta, y : A}{\Gamma, x : \neg A \Rightarrow \Delta} (\neg L)$
$\frac{\Gamma, y \geq x, y \xrightarrow{A} z \Rightarrow \Delta, z : B}{\Gamma \Rightarrow \Delta, x : A \text{ says } B} (\text{says } R)$ <small>y and z new</small>		$\frac{\Gamma, x : P \Rightarrow \Delta, y \geq x \quad \Gamma, x : P, y : P \Rightarrow \Delta}{P \in ATM \quad \Gamma, x : P \Rightarrow \Delta} (ATM)$
$\frac{\Gamma, x : A \text{ says } B \Rightarrow \Delta, y \geq x \quad \Gamma, x : A \text{ says } B \Rightarrow \Delta, y \xrightarrow{A} z \quad \Gamma, x : A \text{ says } B, z : B \Rightarrow \Delta}{\Gamma, x : A \text{ says } B \Rightarrow \Delta} (\text{says } L)$		
$\frac{\Rightarrow u : A \rightarrow B \quad \Rightarrow u : B \rightarrow A}{\Gamma, x \xrightarrow{A} y \Rightarrow \Delta, x \xrightarrow{B} y} (EQ)$		$\frac{\Gamma, z \geq x, z \geq y, y \geq x \Rightarrow \Delta}{\Gamma, z \geq y, y \geq x \Rightarrow \Delta} (Trans)$
$\frac{\Gamma, y \geq x, x \xrightarrow{A} y \Rightarrow \Delta}{\Gamma, x \xrightarrow{A} y \Rightarrow \Delta} (Unit)$		$\frac{\Gamma, x \xrightarrow{A} y, x \xrightarrow{A} z, z \xrightarrow{A} y \Rightarrow \Delta}{z \text{ new} \quad \Gamma, x \xrightarrow{A} y \Rightarrow \Delta} (C4)$

Fig. 1. The sequent calculus $\text{Seq}_{C_{ICL}}$.

$$\begin{array}{c}
 \frac{}{(AX)} \dots, z \geq x \Rightarrow z : \alpha, z \geq x \quad \frac{}{(AX)} \dots, x : \alpha, z : \alpha \Rightarrow z : \alpha \\
 \frac{}{(ATM)} \frac{z \geq x, z \geq y, y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha}{z \geq y, y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha} \\
 \frac{}{(Trans)} \frac{z \geq y, y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha}{y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha} \\
 \frac{}{(Unit)} \frac{y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha}{x \geq u, x : \alpha \Rightarrow x : A \text{ says } \alpha} \\
 \frac{}{(\text{says } R)} \frac{x \geq u, x : \alpha \Rightarrow x : A \text{ says } \alpha}{\Rightarrow u : \alpha \rightarrow (A \text{ says } \alpha)} \\
 \frac{}{(\rightarrow R)} \Rightarrow u : \alpha \rightarrow (A \text{ says } \alpha)
 \end{array}$$

Fig. 2. A derivation in $\text{Seq}_{C_{ICL}}$ for (UNIT).

$$\begin{array}{c}
\frac{}{y \geq x \Rightarrow y \geq x} (AX) \quad \frac{}{y \xrightarrow{A} w \Rightarrow y \xrightarrow{A} w} (AX) \quad \frac{}{\Rightarrow w \geq w} (AX_{\geq}) \quad \frac{}{w \xrightarrow{A} z \Rightarrow w \xrightarrow{A} z} (AX) \quad \frac{}{z : \alpha \Rightarrow z : \alpha} (AX) \\
\frac{}{\dots, w \xrightarrow{A} z, w : A \text{ says } \alpha \Rightarrow z : \alpha} (\text{says } L) \\
\hline
\frac{}{\dots, y \xrightarrow{A} w, w \xrightarrow{A} z, x : A \text{ says } (A \text{ says } \alpha) \Rightarrow z : \alpha} (C4) \\
\frac{}{y \geq x, x \geq u, y \xrightarrow{A} z, x : A \text{ says } (A \text{ says } \alpha) \Rightarrow z : \alpha} (\text{says } R) \\
\frac{}{x \geq u, x : A \text{ says } (A \text{ says } \alpha) \Rightarrow x : A \text{ says } \alpha} (\rightarrow R) \\
\hline
\frac{}{\Rightarrow u : (A \text{ says } (A \text{ says } \alpha)) \rightarrow (A \text{ says } \alpha)}
\end{array}$$

Fig. 3. A derivation in $\text{Seq}_{C_{ICL}}$ for (C4).

Lemma 7 (Height-preserving invertibility of rules). *Let $\Gamma \Rightarrow \Delta$ be an instance of the conclusion of a rule R of $\text{Seq}_{C_{ICL}}$, with R different from (EQ) . If $\Gamma \Rightarrow \Delta$ is derivable, then the premise(s) of R is (are) derivable with a derivation of (at most) the same height.*

Lemma 8 (Height-preserving admissibility of contraction). *If a sequent $\Gamma \Rightarrow \Delta, F, F$ is derivable in $\text{Seq}_{C_{ICL}}$, then there is a derivation of no greater height of $\Gamma \Rightarrow \Delta, F$, and if a sequent $\Gamma, F, F \Rightarrow \Delta$ is derivable in $\text{Seq}_{C_{ICL}}$, then there is a derivation of no greater height of $\Gamma, F \Rightarrow \Delta$.*

We now consider the cut rule:

$$\frac{\Gamma \Rightarrow \Delta, F \quad \Gamma, F \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} (cut)$$

where F is any labelled formula. We prove that this rule is admissible in the calculus $\text{Seq}_{C_{ICL}}$. The standard proof of admissibility of cut proceeds by a double induction over the complexity of F and the sum of the heights of the derivations of the two premises of (cut) , in the sense that we replace one cut by one or several cuts on formulas of smaller complexity, or on sequents derived by shorter derivations. However, in our calculus $\text{Seq}_{C_{ICL}}$ the standard proof does not work in one case, presented in the proof

of Theorem 3 below, namely the case in which F is a transition formula $x \xrightarrow{A} y$, the left premise is obtained by an application of (EQ) and the right premise is obtained by an application of $(C4)$. Therefore, in order to prove the admissibility of cut for $\text{Seq}_{C_{ICL}}$,

we proceed as follows. First of all, we represent with $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$ a sequent containing any number of transitions labelled with the formula A ; moreover, if $\Rightarrow u : A \rightarrow A'$ and $\Rightarrow u : A' \rightarrow A$ are derivable, we denote with $\Gamma^* \Rightarrow \Delta^*$ the sequent obtained by replacing any number of transitions labelled with A with the same transitions labelled with A' in $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$. We prove that cut is admissible by “splitting” the notion of cut in two propositions:

Theorem 3. *In $\text{Seq}_{C_{ICL}}$, the following propositions hold:*

- (A) If $\Gamma \Rightarrow \Delta, F$ and $\Gamma, F \Rightarrow \Delta$ are derivable, so $\Gamma \Rightarrow \Delta$, i.e. the rule (*cut*) is admissible in Seq_{ICL} ;
- (B) if (I) $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$ is derivable with a derivation of height h , (II) $\Rightarrow u : A \rightarrow A'$ and (III) $\Rightarrow u : A' \rightarrow A$ are derivable, so $\Gamma^* \Rightarrow \Delta^*$ with a derivation of height $h' \leq h$.

Proof. By double mutual induction on the complexity of the cut formula and on the height of the derivation. To prove (A), the induction on the height is intended as usual as the sum of the heights of the premises of the cut inference; to prove (B), the induction on the height is intended as the height of the derivation of $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$. We have several cases:

- Base for (A): one of the two premises of (*cut*) is an axiom. To save space, we only present the case in which $\Gamma \Rightarrow \Delta, F$ is an instance of (*AX*) since $F \in \Gamma$. We have that $\Gamma = \Gamma', F$; the right premise of (*cut*) is, therefore, $\Gamma', F, F \Rightarrow \Delta$ and, since contraction is admissible (Lemma 8), we have that also $\Gamma', F \Rightarrow \Delta$, i.e. $\Gamma \Rightarrow \Delta$, is derivable. The other cases are omitted to save space.
- Base for (B): if $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$ is an axiom, so $\Gamma^* \Rightarrow \Delta^*$, since axioms do not involve transition formulas.
- Inductive step for (A): we distinguish the following two cases:
 - the last step of *one* of the two premises is obtained by a rule in which F is *not* the principal formula. We further distinguish two subcases: (i) one of the sequents, say $\Gamma, F \Rightarrow \Delta$ is obtained by the (*EQ*) rule, where F is not principal. The premises of (*EQ*) do not contain F , since this rule only involves two transition formulas belonging to Γ and Δ . Therefore, we have a proof of $\Gamma \Rightarrow \Delta$ by a direct application of (*EQ*) to it; (ii) the sequent where F is not principal is derived by any rule R, except the (*EQ*) rule. This case is standard, we can permute R over the cut, i.e. we cut the premise(s) of R and then we apply R to the result of cut.
 - F is the principal formula in the last step of *both* derivations of the premises of the cut inference. There are seven subcases: F is introduced a) by ($\wedge R$) - ($\wedge L$), b) by ($\vee R$) - ($\vee L$), c) by ($\rightarrow R$) - ($\rightarrow L$), d) by (**says** R) - (**says** L), e) by (*EQ*) on the left and on the right, f) by (*EQ*) on the left and by (*C4*) on the right, and g) by (*EQ*) on the left and by (*Unit*) on the right. The list is exhaustive. Due to space limitations, here we only present the most interesting case f). We have the following derivation:

$$\begin{array}{c}
 \frac{\frac{\Rightarrow u : A' \rightarrow A}{\Rightarrow u : A \rightarrow A'} \quad (EQ) \quad (2) \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, x \xrightarrow{A} z, z \xrightarrow{A} y \Rightarrow \Delta}{(1) \Gamma', x \xrightarrow{A'} y \Rightarrow \Delta, x \xrightarrow{A} y \quad \Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y \Rightarrow \Delta} \quad (C4)}{\Gamma', x \xrightarrow{A'} y \Rightarrow \Delta} \quad (cut)
 \end{array}$$

By (2) and Proposition (B), we have a derivation of at most the same height also for (2') $\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A} y, x \xrightarrow{A'} z, z \xrightarrow{A'} y \Rightarrow \Delta$. By Lemma 5, from (1) we have a derivation of (1') $\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A'} z, z \xrightarrow{A'} y \Rightarrow \Delta, x \xrightarrow{A} y$. By cutting (1') and (2'), we obtain a derivation of $\Gamma', x \xrightarrow{A'} y, x \xrightarrow{A'} z, z \xrightarrow{A'} y \Rightarrow \Delta$ (this cut

is eliminable by inductive hypothesis on the height of the derivations), then we can conclude by an application of (C4).

• Inductive step for (B): we have to consider all possible derivations of $\Gamma[x_i \xrightarrow{A} y_i] \Rightarrow \Delta[u_j \xrightarrow{A} v_j]$. We only present the most interesting case, namely the one the derivation ends as follows:

$$\frac{\Rightarrow (3) u : A \rightarrow A'' \qquad \Rightarrow (4) u : A'' \rightarrow A}{\Gamma[x_i \xrightarrow{A} y_i], x \xrightarrow{A} y \Rightarrow \Delta[u_j \xrightarrow{A} v_j], x \xrightarrow{A''} y} (EQ)$$

We have to show that there is a derivation also for $\Gamma^*, x \xrightarrow{A'} y \Rightarrow \Delta^*, x \xrightarrow{A''} y$. Since the rule $(\rightarrow R)$ is invertible (Lemma 7), since (5) $\Rightarrow u : A \rightarrow A'$ and (6) $\Rightarrow u : A' \rightarrow A$ are derivable, we have derivations also for (5') $x \geq u, x : A \Rightarrow x : A'$, (6') $x \geq u, x : A' \Rightarrow x : A$, and since we have derivations for (3) and (4), also (3') $x \geq u, x : A \Rightarrow x : A''$ and (4') $x \geq u, x : A'' \Rightarrow x : A$ are derivable. By applying the inductive hypothesis of Proposition A on the complexity of the cut formula, we can cut (5') and (4') to obtain a derivation of (7) $x \geq u, x : A'' \Rightarrow x : A'$, as well as (6') and (3') to obtain a derivation of (8) $x \geq u, x : A' \Rightarrow x : A''$. We can conclude as follows:

$$\frac{\frac{(7) x \geq u, x : A'' \Rightarrow x : A'}{\Rightarrow u : A'' \rightarrow A'} (\rightarrow R) \quad \frac{(8) x \geq u, x : A' \Rightarrow x : A''}{\Rightarrow u : A' \rightarrow A''} (\rightarrow R)}{\Gamma[x_i \xrightarrow{A} y_i], x \xrightarrow{A'} y \Rightarrow \Delta[u_j \xrightarrow{A} v_j], x \xrightarrow{A''} y} (EQ)$$

□

Theorem 4 (Soundness of $\text{Seq}_{C_{\text{ICL}}}$). *If $\Gamma \Rightarrow \Delta$ is derivable, then $\Gamma \Rightarrow \Delta$ is valid in the sense of Definition 5.*

Proof. By induction on the height of the derivation of $\Gamma \Rightarrow \Delta$. To save space, we only present the inductive step for the case in which the derivation of $\Gamma', x \xrightarrow{A} y \Rightarrow \Delta$ ends by an application of (*Unit*): by inductive hypothesis, the premise $\Gamma', x \xrightarrow{A} y, y \geq x \Rightarrow \Delta$ is a valid sequent. By absurd, the conclusion is not, i.e. there is a model \mathcal{M} and a function I such that $\mathcal{M} \models_I F$ for every $F \in \Gamma'$, $\mathcal{M} \models_I x \xrightarrow{A} y$ (i.e., $I(x)R_A I(y)$), whereas $\mathcal{M} \not\models_I G$ for any $G \in \Delta$. By Condition (b) in Definition 1, we have that, since $I(x)R_A I(y)$, also $I(x) \leq I(y)$, then $\mathcal{M} \models_I y \geq x$, against the validity of the premise. □

Theorem 5 (Completeness of $\text{Seq}_{C_{\text{ICL}}}$). *If $\Gamma \Rightarrow \Delta$ is valid in the sense of Definition 5, then $\Gamma \Rightarrow \Delta$ is derivable.*

Proof. We prove that the axioms are derivable and that the set of derivable formulas is closed under (MP), (RCEA), and (RCK). In Figure 2 we have shown a derivation of the axiom (UNIT). In Figure 3 we have shown a derivation of the axiom (C4). Derivations for (K) and (TAUT) are omitted for the lack of space. For (MP), suppose we have a derivation for (i) $\Rightarrow x : A$ and (ii) $\Rightarrow x : A \rightarrow B$. Since weakening is admissible (Lemma 5), we have that also (i') $\Rightarrow x : A, x : B$ and (ii') $x : A \Rightarrow x : A \rightarrow B, x : B$

have a derivation in $\text{Seq}_{C_{\text{ICL}}}$. Since (cut) is admissible (Theorem 3), we can conclude that $\Rightarrow x : B$ is derivable as follows:

$$\frac{\frac{\frac{\dots, \Rightarrow x \geq x, x : B}{\dots, x : A \Rightarrow x : A, x : B} \quad \frac{\dots, x : B \Rightarrow x : B}{x : A \Rightarrow x : B} (\rightarrow L)}{(ii') x : A \Rightarrow x : A \rightarrow B, x : B} \quad x : A \Rightarrow x : B}{(i') \Rightarrow x : A, x : B} \quad x : A \Rightarrow x : B}{\Rightarrow x : B} (cut)$$

For (RCEA), we proceed as follows. As usual, $\vdash A \leftrightarrow B$ is a shorthand for $\vdash A \rightarrow B$ and $\vdash B \rightarrow A$. Suppose we have a derivation for $\Rightarrow u : A \rightarrow B$ and for $\Rightarrow u : B \rightarrow A$. We have that also $\Rightarrow u : (A \text{ says } C) \rightarrow (B \text{ says } C)$ has a derivation in $\text{Seq}_{C_{\text{ICL}}}$ (the other half is symmetric):

$$\frac{\frac{\frac{\Rightarrow u : A \rightarrow B \quad \Rightarrow u : B \rightarrow A}{y \xrightarrow{B} z \Rightarrow y \xrightarrow{A} z} (EQ)}{y \geq x \Rightarrow y \geq x} \quad z : C \Rightarrow z : C}{y \geq x, x \geq u, x : A \text{ says } C, y \xrightarrow{B} z \Rightarrow z : C} (\text{ says } L)}{\frac{x \geq u, x : A \text{ says } C \Rightarrow x : B \text{ says } C}{\Rightarrow u : (A \text{ says } C) \rightarrow (B \text{ says } C)} (\rightarrow R)} (\text{ says } R)$$

For (RCK), suppose there is a derivation in $\text{Seq}_{C_{\text{ICL}}}$ for $\Rightarrow y : A \rightarrow B$. Since $(\rightarrow R)$ is invertible (Lemma 7), we have also a derivation of $(I) z \geq y, z : A \Rightarrow z : B$ and, by weakening (Lemma 5), of $(I') z \geq y, y \geq x, y \xrightarrow{C} z, x \geq u, x : C \text{ says } A, z : A \Rightarrow z : B$, from which we conclude:

$$\frac{\frac{\frac{y \geq x \Rightarrow y \geq x \quad (I') z \geq y, \dots, z : A \Rightarrow z : B}{y \xrightarrow{C} z \Rightarrow y \xrightarrow{C} z} (Unit)}{y \geq x, y \xrightarrow{C} z, x \geq u, x : C \text{ says } A \Rightarrow z : B} (\text{ says } L)}{\frac{x \geq u, x : C \text{ says } A \Rightarrow x : C \text{ says } B}{\Rightarrow u : (C \text{ says } A) \rightarrow (C \text{ says } B)} (\rightarrow R)} (\text{ says } R)$$

□

Completeness of $\text{Seq}_{C_{\text{ICL}}}$ with respect to C_{ICL} models of Definition 1 immediately follows from the completeness of the axiomatization of C_{ICL} with respect to the semantics, shown in Theorem 2. We have that a formula $\varphi \in \mathcal{L}$ is valid if and only if the sequent $\Rightarrow u : \varphi$ has a derivation in $\text{Seq}_{C_{\text{ICL}}}$.

5 Conclusions

We have defined an intuitionistic conditional logic for Access Control (C_{ICL}) by providing an axiomatization, a Kripke model semantics and a cut-free sequent calculus.

From an axiomatic point of view, the employment of constructive logics for access control has been put forward by Abadi in [6], where he shows that from (UNIT) axiom in classical logic we can deduce $A \textbf{says } \varphi \rightarrow (\varphi \vee A \textbf{says } \psi)$. The previous axiom is called (Escalation) and it represents a rather degenerate interpretation of says, i.e., if A says φ , either φ is permitted or the principal can say *anything*. On the contrary, if we interpret the **says** within an intuitionistic logic we can avoid (Escalation). More generally, as put forward in [12, 13], constructive logics are well suited for reasoning about authorization, because constructive proofs preserve the justification of statements during reasoning and, therefore, information about accountability is not lost. Classical logics, instead, allows proofs that discard evidence. For instance, we can prove ψ using a classical logic by proving $\varphi \rightarrow \psi$ and $\neg\varphi \rightarrow \psi$, since from these theorems we can conclude $(\varphi \vee \neg\varphi) \rightarrow \psi$, hence $\top \rightarrow \psi$.

From a logical point of view, several formal systems have been developed in the recent years [1, 2, 14, 3–5]. Up to authors knowledge, the only works that introduce a logic for access control with a Kripke semantics, a calculus and a completeness result are [15, 8]. In [15], principals are atomic and they cannot be combined, moreover the underlying semantics is constructive S4 enriched with *views*, i.e. a mapping from worlds to sets of principals, this approach breaks the useful bound between axioms of **says** and accessibility relationships and, as a consequence, [15] does not provide canonical properties for its axioms. As already mentioned, in [8] is provided an axiomatization of ICL, a sequent calculus for it and a translation of ICL into modal logic S4. It also presents extensions of ICL for dealing with delegation (ICL^{\Rightarrow}) and with boolean principals ($\text{ICL}^{\mathcal{B}}$).

In this work, we have proven that the axiomatization of the intuitionistic conditional logic C_{ICL} is sound and complete with respect to the semantics. Moreover, we have provided a cut-free, labelled, sequent calculus for this logic. In C_{ICL} , principals are defined as arbitrary formulas. The generality of the language makes it possible to formalize, for instance, the so called boolean principals [8], that is, principals which are formed by boolean combinations of atomic principals. For the time being, C_{ICL} only includes few uncontroversial axioms of access control logics but it can be extended in order to cope with richer axioms, as well as with the well known notion of “speaks for”. Other issue to be tackled are the complexity of the logic C_{ICL} and the termination and complexity of the sequent calculus $\text{Seq}_{C_{\text{ICL}}}$. This is what we plan to do in future work.

Acknowledgements

The work has been partially supported by Regione Piemonte, Project “ICT4Law - *ICT Converging on Law: Next Generation Services for Citizens, Enterprises, Public Administration and Policymakers*”. Valerio Genovese is supported by the National Research Fund, Luxembourg. This paper extends [16], where some preliminary results are presented.

References

1. Abadi, M., Burrows, M., Lampson, B.W., Plotkin, G.D.: A calculus for access control in distributed systems. In: *Advances in Cryptology, 11th Annual International Cryptology Con-*

- ference (CRYPTO). (1991) 1–23
2. Bertolissi, C., Fernández, M., Barker, S.: Dynamic event-based access control as term rewriting. In: *Data and Applications Security XXI, 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec)*. (2007) 195–210
 3. Gurevich, Y., Roy, A.: Operational semantics for DKAL: Application and analysis. In: *Trust, Privacy and Security in Digital Business, 6th International Conference (TrustBus)*. (2009) 149–158
 4. Lesniewski-Laas, C., Ford, B., Strauss, J., Morris, R., Kaashoek, M.F.: Alpaca: extensible authorization for distributed services. In: *Proceedings of the 2007 ACM Conference on Computer and Communications Security (CCS)*. (2007) 432–444
 5. Li, N., Grosz, B.N., Feigenbaum, J.: Delegation logic: A logic-based approach to distributed authorization. *ACM Trans. Inf. Syst. Secur.* **6**(1) (2003) 128–171
 6. Abadi, M.: Variations in access control logic. In: *DEON*. (2008) 96–109
 7. Boella, G., Gabbay, D., Genovese, V., van der Torre, L.: Fibred security language. *Studia Logica* **92**(3) (2009) 395–436
 8. Garg, D., Abadi, M.: A modal deconstruction of access control logics. In: *11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS)*, Budapest, Hungary (2008) 216–230
 9. Nute, D.: *Topics in Conditional Logic*. Reidel, Dordrecht (1980)
 10. Troelstra, A., van Dalen, D.: *Constructivism in Mathematics: An Introduction*. North-Holland Publishing, Amsterdam
 11. Olivetti, N., Pozzato, G.L., Schwind, C.B.: A Sequent Calculus and a Theorem Prover for Standard Conditional Logics. *ACM Transactions on Computational Logics (ToCL)* **8**(4) (2007)
 12. Garg, D., Pfenning, F.: Non-interference in constructive authorization logic. In: *19th IEEE Computer Security Foundations Workshop, (CSFW-19)*, 5-7 July 2006, Venice, Italy. (2006) 283–296
 13. Sire, E.G., Schneider, F., Walsh, K.: Nexus authorization logic (nal): Design rationale and applications. Technical report, Cornell Computing and Information Science Technical Report (January 2009) Available at <http://hdl.handle.net/1813/13679>.
 14. Garg, D., Bauer, L., Bowers, K.D., Pfenning, F., Reiter, M.K.: A linear logic of authorization and knowledge. In: *European Symposium on Research in Computer Security (ESORICS)*. (2006) 297–312
 15. Garg, D.: Principal centric reasoning in constructive authorization logic. In: *Informal Proceedings of Intuitionistic Modal Logic and Application (IMLA)*. (2008) Full version available as Carnegie Mellon Technical Report CMU-CS-09-120.
 16. Genovese, V., Giordano, L., Gliozzi, V., Pozzato, G.L.: A constructive conditional logic for access control: a preliminary report. To appear in *Proceedings of ECAI 2010 (19th European Conference on Artificial Intelligence)*.