Logics for Access Control: A Conditional Approach

Valerio Genovese[1], Laura Giordano[2], Valentina Gliozzi[3], and Gian Luca Pozzato[3]

[1] University of Luxembourg and Università degli Studi di Torino - Italy
valerio.genovese@uni.lu
[2] Dipartimento di Informatica - Università del Piemonte Orientale - Alessandria, Italy
laura@mfn.unipmn.it
[3] Dipartimento di Informatica - Università degli Studi di Torino - Torino, Italy
{gliozzi,pozzato}@di.unito.it

Abstract. In this paper we provide a reconstruction of access control logics within constructive conditional logics, by regarding the assertion A **says** ϕ, whose intended meaning is that *principal* A *says that* ϕ, as a conditional implication. We identify the conditional axioms needed to capture the basic properties of the "says" operator and to provide a proper definition of boolean principals. Most of these axioms are standard axioms of conditional logics. We provide a Kripke model semantics for the logic and we prove that the axiomatization is sound and complete with respect to the semantics. Also, we define a sound, complete and cut-free labelled sequent calculus for it.

1 Introduction

Access control is concerned with the decision of accepting or denying 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.

In [7] 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. The treatment of the operator **says** as a modality can be also found in [8], which introduces a logical framework, FSL, based on multi-modal logic methodology.

Even if there is some agreement on looking at the says construct as a modal operator, the *correspondence theory* between its axiomatizations and the underlying (Kripke-syle) semantics is left unexplored. By correspondence theory we mean identifying canonical properties for well-known access control axioms, i.e., first-order conditions of Kripke structures that are *necessary* and *sufficient* for the corresponding axiom to hold. This approach raise several challenges because axiom of access control are not standard in modal literature and their correspondence with the underlying semantics is

mainly unexplored. Identifying canonical properties for well-known axioms for access control permits to study them separately and naturally yields completeness for logics that adopt *any* combination of them. This methodology is significant if we want logic to be employed to compare different access control models, because different systems adopts different axioms depending on the specific application domain.

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, $\mathsf{Cond}_{\mathrm{ACL}}$, 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 allows a natural formalization of boolean principals [7], that is, principals which are formed by boolean combination of atomic principals.

From the access control point of view, the **says** operator satisfies some basic axioms of access control logics [7, 10]. We define a sound and complete Kripke semantics for $\mathsf{Cond}_{\mathrm{ACL}}$ 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 $\mathsf{Cond}_{\mathrm{ACL}}$ 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 $\mathsf{Cond}_{\mathrm{ACL}}$. Section 6 contains the conclusions and a discussion of related work.

2 The logic $\mathsf{Cond}_{\mathrm{ACL}}$

In this section, we introduce the conditional intuitionistic logic $\mathsf{Cond}_{\mathrm{ACL}}$ for access control by defining its axiomatization and Kripke semantics. 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 $\mathsf{Cond}_{\mathrm{ACL}}$. Let ATM be a set of atomic propositions. The formulas of $\mathcal{L}$ are defined inductively as follows: if $P \in ATM$, then $P \in \mathcal{L}$; $\bot \in \mathcal{L}$, where $\bot$ 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** φ, where A and φ are arbitrary formulas, is that *principal A says that φ*, namely, "the principal A asserts or supports φ" [7]. 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 $A, B, C, \ldots$ while we will use greek letters for arbitrary formulas.

The axiomatization of $\mathsf{Cond}_{\mathrm{ACL}}$ contains few basic axioms for access control logics [7, 6], as well as few additional axioms governing the behavior of boolean principals.

Basic Axioms. The *axiom system* of the logic $\mathsf{Cond}_{\mathrm{ACL}}$ contains the following axioms and inference rules, which are intended to capture the basic properties of the **says** operator.

(TAUT)	all tautologies of intuitionistic logic
(K)	A **says** $(\alpha \to \beta) \to (A$ **says** $\alpha \to A$ **says** $\beta)$
(UNIT)	$\alpha \to (A$ **says** $\alpha)$
(C)	A **says** $(A$ **says** $\alpha \to \alpha)$
(MP)	If $\vdash \alpha$ and $\vdash \alpha \to \beta$ then $\vdash \beta$
(RCEA)	If $\vdash A \leftrightarrow B$ then $\vdash (A$ **says** $\gamma) \leftrightarrow (B$ **says** $\gamma)$
(RCK)	If $\vdash \alpha \to \beta$ then $\vdash (A$ **says** $\alpha) \to (A$ **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 $\gamma_1, \ldots \gamma_n$ in Γ such that $\vdash \gamma_1 \wedge \ldots \wedge \gamma_n \to \alpha$. 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) and (K) are the characterizing axioms of the access control logics ICL [7], while (C) has been included in the axiomatization of the logic DTL_0 in [10].

Axioms for boolean principals. The axioms introduced above do not enforce by themselves any intended property of boolean principals. In this subsection, we discuss the properties that are intended for boolean principals and we introduce axioms which capture such properties. Specifically, we focus on the intended meaning of conjunctions and disjunctions among principals.

Our interpretation of the statement $A \wedge B$ **says** ϕ 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 (jointly) conditionally prove ϕ. Instead, our interpretation of the statement $A \vee B$ **says** ϕ 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.

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

$$A \textbf{ says } \phi \wedge B \textbf{ says } \phi \to A \vee B \textbf{ says } \phi$$

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

$$A \vee B \textbf{ says } \phi \to A \textbf{ says } \phi \wedge B \textbf{ says } \phi$$

holds. The two axioms together enforce the property that A and B disjointly say that ϕ if and only if A says that ϕ and B says that ϕ .

Concerning the statement $A \wedge B$ **says** ϕ, we expect that A and B jointly say that ϕ when either A or B says that ϕ. This condition can be enforced by introducing the axiom

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

which, although is a very controversial axiom of conditional logics, called monotonicity[4], is proved to be armless in this intuitionistic setting. We would like to have the property that if $A \wedge B$ **says** ϕ then, by combining the statements of A and B, ϕ can be concluded. This is not equivalent to saying that either A says ϕ or B says ϕ. Indeed, this last property would correspond to axiom $(A \wedge B \textbf{ says } \phi) \rightarrow (A \textbf{ says } \phi) \vee (B \textbf{ says } \phi)$, which is too strong and not wanted. In the following we show that this property can be captured in a first order axiomatization.

Although we do not put any restriction to the language, in the following we will limit our consideration to principals obtained by boolean combination (conjunction and disjunction) of atomic principals and of the principal $\bot$. Although a principal can be an arbitrary propositional formula (including negation and implication), no specific properties are intended for such formulas, and no specific axioms are introduced for them.

The axiomatization of $\mathsf{Cond}_{\mathrm{ACL}}$ includes (in addition) the following axioms:

(CA)	$A \textbf{ says } \phi \wedge B \textbf{ says } \phi \rightarrow A \vee B \textbf{ says } \phi$
(CA-conv)	$A \vee B \textbf{ says } \phi \rightarrow A \textbf{ says } \phi$
(Mon)	$A \textbf{ says } \phi \rightarrow A \wedge B \textbf{ says } \phi$
(DT)	$A \wedge B \textbf{ says } \phi \rightarrow (A \textbf{ says } (B \rightarrow \phi))$
(ID)	$A \textbf{ says } A$

The first three axioms are those introduced above. (DT) and (ID) are used together to enforce the property that if $A \wedge B$ **says** ϕ then, by combining the statements of A and B, ϕ can be concluded. The two axioms allow propositions representing principals to occur on the right of the **says** modality. The intended meaning of (DT) is that, if $A \wedge B$ **says** ϕ, then A says that ϕ holds in all B worlds (worlds visible to the principal B). The meaning of (ID) is that "A says that principal A is visible". We will come back to the meaning of these axioms when describing the semantic conditions associated with the axioms.

It can be shown that:

Theorem 1. *The above axiomatization is consistent.*

Proof. Consistency immediately follows from the fact that, by replacing A **says** B with the intuitionistic implication $A \rightarrow B$, we obtain axioms which are derivable in intuitionistic logic.

□

[4] In general, conditional logics only allow weaker forms of monotonicity, encoded, for instance, by the axiom (CV) of Lewis' logic VC.

Let us observe that the above interpretation of conjunction and disjunction between principals is different from the one given in the logic ICL$^{\mathcal{B}}$ [7], which actually adopts the opposite interpretation of $\wedge$ and $\vee$: in Garg and Abadi's logic ICL$^{\mathcal{B}}$, $A \wedge B$ **says** ϕ is the same as A **says** $\phi \wedge B$ **says** ϕ, while $A \vee B$ **says** ϕ means that, by combining the statements of A and B, ϕ can be concluded. Due to this, let us say, superficial difference, the properties of the principal $A \wedge B$ in our logic are properties of the principal $A \vee B$ in their logic, and vice-versa, the properties of the principal $A \vee B$ in our logic are properties of the principal $A \wedge B$ in their logic.

Observe that the axioms, (trust), (untrust) and (cuc') of the logic ICL$^{\mathcal{B}}$ are not derivable from our axiomatization. Also, the addition of the axiom (untrust) $\top$ **says** $\bot$ to our axiomatization would entail that for all principals A, A **says** $\bot$, which is an unwanted property.

2.2 Semantics

The semantics of the logic $\mathsf{Cond}_{\mathrm{ACL}}$ is defined as follows.

Definition 1. *A* $\mathsf{Cond}_{\mathrm{ACL}}$ *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* $ATM \longrightarrow Pow(S)$ *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. $\mathcal{M}, t \not\models \bot$
7. $\mathcal{M}, t \models A$ **says** ψ *iff, for all* s *such that* tR_As, $\mathcal{M}, s \vDash \psi$.

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:

(S-Int) $\forall t, s, z \in S$, if $s \leq t$ and tR_Az then sR_Az;
(S- UNIT) $\forall t, s \in S$, if sR_At, then $s \leq t$;
(S-C) $\forall t, s, z \in S$, if sR_At and $t \leq z$, then zR_Az;
(S-CA) $R_{A\vee B}(t) = R_A(t) \cup R_B(t)$.
(S-Mon) $\forall t, s, z \in S$, if $sR_{A\wedge B}t$, then sR_At and sR_Bt;
(S-DT) $\forall t, s, z \in S$, if sR_At and $t \leq z$, and $z \in [|B|]$, then $sR_{A\wedge B}z$;
(S-ID) $\forall t, s \in S$, if sR_At, then $t \in [|A|]$;

(S-RCEA) if $[|A|] = [|B|]$, then $R_A = R_B$.

Condition (S-Int) enforces the property that when a formula A **says** ϕ true in a world t, it is also true in all worlds reachable from s by the relation $\leq$ (i.e., in all worlds s such that $t \leq s$). All the other semantic conditions are those associated with the axioms of the logic, apart from condition (S-RCEA), which 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. (S-CA) is the semantic condition for both axioms (CA) and its converse.

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_At corresponds to $t \in f([|A|], s)$, and the conditions above are indeed conditions on the selection function f, as usual in conditional logics. Note also that the semantic conditions for some of the axioms, as for instance (DT), slightly departs from the semantic condition usually given to these axioms in conditional logic. This is due to the fact that $\mathsf{Cond}_{\mathrm{ACL}}$ is an intuitionistic conditional logic and the implication occurring within axioms is intuitionistic implication.

Concerning the interpretation of boolean conditionals and, in particular, of the conjunction between principals, it can be proved that, from the semantic conditions of (Monotonicity), (ID) and (DT) it follows that:

$$R_{A \wedge B}(t) = R_A(t) \cap R_B(t).$$

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 Γ, A **says** $\phi \models \phi$. For instance, if Γ contains the following formulas:

$Admin1$ **says** $(SU\_user1 \rightarrow write\_perm\_user1)$
$Admin2$ **says** SU_user1
$((Admin1 \wedge Admin2)$ **says** $delete\_file1) \rightarrow delete\_file1$
$Admin1 \wedge Admin2$ **says** $((write\_perm\_user1 \wedge user1$ **says** $delete\_file1) \rightarrow delete\_file1)$
$user1$ **says** $delete\_file1$

we obtain that $\Gamma, user1$ **says** $deletefile1 \models delete\_file1$.

3 Soundness and Completeness

In this section we prove that the axiomatization of the logic $\mathsf{Cond}_{\mathrm{ACL}}$ given above is sound and complete with respect to the semantics of Definition 1.

Theorem 2 (Soundness). *Given a formula $\varphi \in \mathcal{L}$, if $\vdash \varphi$, then $\models \varphi$.*

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 [11] 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). *Let Γ be a set of well formed formulas. Γ is consistent iff $\Gamma \nvdash \bot$. 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 $\Gamma_0 \vdash \bot$.*

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). *Let Γ be a set of well formed formulas. Suppose $\Gamma \nvdash \varphi$, then there is a saturated extension Γ^* such that $\Gamma^* \nvdash \varphi$.*

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

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

□

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

Lemma 3. *For all $\Gamma \in S$ and each wff formula φ, we have that $\mathbf{M}, \Gamma \models \varphi$ 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 left to the reader. For $\varphi \equiv \phi \vee \psi$, then $\Gamma \models \phi \vee \psi \Leftrightarrow (\Gamma \models \phi$ or $\Gamma \models \psi) \Leftrightarrow (\phi \in \Gamma$ 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 $\Gamma \nvdash \phi \rightarrow \psi$, then $\Gamma \cup \{\phi\} \nvdash \psi$; let Γ' be a saturated extension of $\Gamma \cup \{\phi\}$ such that $\Gamma' \nvdash \psi$, 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 $\varphi \equiv A$ **says** ϕ, suppose $\Gamma \models A$ **says** ϕ. Hence, for all Γ' such that $\Gamma R_A \Gamma'$, $\Gamma' \models \phi$. By inductive hypothesis, $\phi \in \Gamma'$. Let $\Delta = \{\alpha : A$ **says** $\alpha \in \Gamma\}$. By construction, $\Gamma' \supseteq \Delta$. Assume, for a contradiction, that A **says** $\phi \notin \Gamma$. By condition 2 in Definition 3, $\Gamma \nvdash A$ **says** ϕ. Then, by Lemma 2, $\Delta \nvdash \phi$. By Lemma 1, there is a saturated extension Δ^* of Δ such that $\Delta^* \nvdash \phi$, i.e. $\phi \notin \Delta^*$. By definition of R_A, $\Gamma R_A \Delta^*$. This contradicts the fact that, for all Γ' such that $\Gamma R_A \Gamma'$, $\phi \in \Gamma'$. The converse is trivial.

□

Lemma 4. *Let* $\mathbf{M}$ *be the canonical model as defined in Definition 4.* $\mathbf{M}$ *satisfies the semantic conditions (S-Int), (S-UNIT), (S-C), (S-CA), (S-Mon), (S-DT), (S-ID), and (S-RCEA).*

Proof. We have to prove that

(S-Int) $\forall \Gamma, \Gamma', \Gamma'' \in S$, if $\Gamma \leq \Gamma'$ and $\Gamma' R_A \Gamma''$ then $\Gamma R_A \Gamma''$
(S-UNIT) $\forall \Gamma, \Gamma' \in S$, if $\Gamma R_A \Gamma'$ then $\Gamma \leq \Gamma'$.
(S-C) $\forall \Gamma, \Gamma', \Gamma'' \in S$, if $\Gamma R_A \Gamma'$, and $\Gamma' \leq \Gamma''$, then $\Gamma'' R_A \Gamma''$
(S-CA) $\forall \Gamma, \Gamma' \in S$, $\Gamma R_A \Gamma'$ or $\Gamma R_B \Gamma'$, iff $\Gamma R_{A \vee B} \Gamma'$
(S-Mon) $\forall \Gamma, \Gamma' \in S$, if $\Gamma R_{A \wedge B} \Gamma'$, then $\Gamma R_A \Gamma'$ and $\Gamma R_B \Gamma'$
(S-DT) $\forall \Gamma, \Gamma', \Gamma'' \in S$, if $\Gamma R_A \Gamma'$ and $\Gamma' \leq \Gamma''$, and $\Gamma'' \in [|B|]$, then $\Gamma R_{A \wedge B} \Gamma''$;
(S-ID) $\forall \Gamma, \Gamma' \in S$, if $\Gamma R_A \Gamma'$, then $\Gamma' \in [|A|]$
(S-RCEA) $\forall \Gamma, \Gamma' \in S$, if $\vdash A \leftrightarrow B$, then $\Gamma R_A \Gamma'$ if and only if $\Gamma R_B \Gamma'$.

The proof is straightforward. As an example, let us prove (S-DT). We have to show that if $\Gamma R_A \Gamma'$, $\Gamma' \leq \Gamma''$, and $\Gamma'' \in [|B|]$, then $\Gamma R_{A \wedge B} \Gamma''$, i.e. $\{\phi$ such that $A \wedge B$ **says** $\phi \in \Gamma\} \subseteq \Gamma''$. For all such ϕ, by (DT), A **says** $(B \rightarrow \phi) \in \Gamma$, hence by definition of R_A, $B \rightarrow \phi \in \Gamma'$, and by definition of $\leq$, $B \rightarrow \phi \in \Gamma''$. Furthermore, also $B \in \Gamma''$ by Lemma 3. By deductive closure of Γ'', we conclude that $\phi \in \Gamma''$.

□

By the above lemmas, we can conclude that the axiomatization of the logic $\mathsf{Cond}_{\mathrm{ACL}}$ given in Section 2.1 is complete with respect to the semantics in Definition 1:

Theorem 3 (Completeness). *Given a formula* $\varphi \in \mathcal{L}$*, if* $\models \varphi$*, then* $\vdash \varphi$*.*

Proof. For a contradiction, suppose $\nvdash \varphi$. Then by Lemma 1 there is a saturated extension Γ^* such that $\Gamma^* \nvdash \varphi$, hence $\varphi \notin \Gamma^*$. By Definition 4 and Lemmas 3 and 4, we conclude that there is a (canonical) model $\mathbf{M} = (S, \leq, \{R_A\}, h)$, with $\Gamma^* \in S$, such that $\mathbf{M}, \Gamma^* \not\models \varphi$. It follows that φ is not logically valid, i.e. $\not\models \varphi$.

□

4 A sequent calculus for $\mathsf{Cond}_{\mathbf{ACL}}$

In this section we present a cut-free sequent calculus for $\mathsf{Cond}_{\mathrm{ACL}}$. Our calculus is called $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ and it makes use of labels to represent possible worlds, following the line of SeqS, a sequent calculus for standard conditional logics introduced in [12]. The completeness of the calculus is an immediate consequence of the admissibility of cut.

In addiction to the language $\mathcal{L}$ of the logic $\mathsf{Cond}_{\mathrm{ACL}}$, we consider a denumerable alphabet of labels $\mathcal{A}$, whose elements are denoted by $x, y, z, \ldots$. There are three types of labelled formulas:

1. *world formulas*, denoted by $x : \alpha$, where $x \in \mathcal{A}$ and $\alpha \in \mathcal{L}$, used to represent that the formula α holds in a world x;

2. *transition formulas*, denoted by $x \xrightarrow{A} y$, representing that xR_Ay;
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 $I : \mathcal{A} \to S$. *Let F be a labelled formula, we define $\mathcal{M} \models_I F$ as follows:*

- $\mathcal{M} \models_I x : \alpha$ *iff* $\mathcal{M}, I(x) \models \alpha$
- $\mathcal{M} \models_I x \xrightarrow{A} y$ *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 $I : \mathcal{A} \to S$, 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* $\mathsf{Cond}_{\mathrm{ACL}}$ *if it is valid in every $\mathcal{M}$.*

In Figure 1 we present the rules of the calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for $\mathsf{Cond}_{\mathrm{ACL}}$. As usual, we say that a sequent $\Gamma \Rightarrow \Delta$ is *derivable* in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ if it admits a *derivation*. A derivation is a tree whose nodes are sequents. A branch is a sequence of nodes $\Gamma_1 \Rightarrow \Delta_1, \Gamma_2 \Rightarrow \Delta_2, \ldots, \Gamma_n \Rightarrow \Delta_n, \ldots$ 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 $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, 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 $(AX_{\bot})$, 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 $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ if there is a closed tree having $\Gamma \Rightarrow \Delta$ as a root.

The rule (EQ) is used in order to support the rule (RCEA): if a sequent $\Gamma, x \xrightarrow{A} y \Rightarrow \Delta, x \xrightarrow{B} y$ has to be proved, then the calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ checks whether A and B are equivalent, i.e. $A \leftrightarrow B$. To this aim, the (EQ) rule introduces a branch in the backward derivation, trying to find a proof for both sequents $u : A \Rightarrow u : B$ and $u : B \Rightarrow u : A$.

As an example, in Figure 2 we show a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ of an instance of the axiom (UNIT). In order to show that the formula $\alpha \to (A \textbf{ says } \alpha)$ is valid, we build a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for the sequent $\Rightarrow u : \alpha \to (A \textbf{ says } \alpha)$.

As a further example, in Figure 3 we show a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ of an instance of the axiom (C).

The calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ is sound and complete for the logic $\mathsf{Cond}_{\mathrm{ACL}}$, that is to say a formula $\psi \in \mathcal{L}$ is valid in $\mathsf{Cond}_{\mathrm{ACL}}$ if and only if the sequent $\Rightarrow u : \psi$ is derivable in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$. 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). *We define the complexity of a labelled formula F as follows: cp $(x : \varphi) = 2 * \mid \varphi \mid$; cp $(x \xrightarrow{A} y) = 2 * \mid A \mid +1$; cp $(y \geq x) = 2$, where $\mid \phi \mid$ is the number of symbols occurring in the string representing the formula ϕ.*

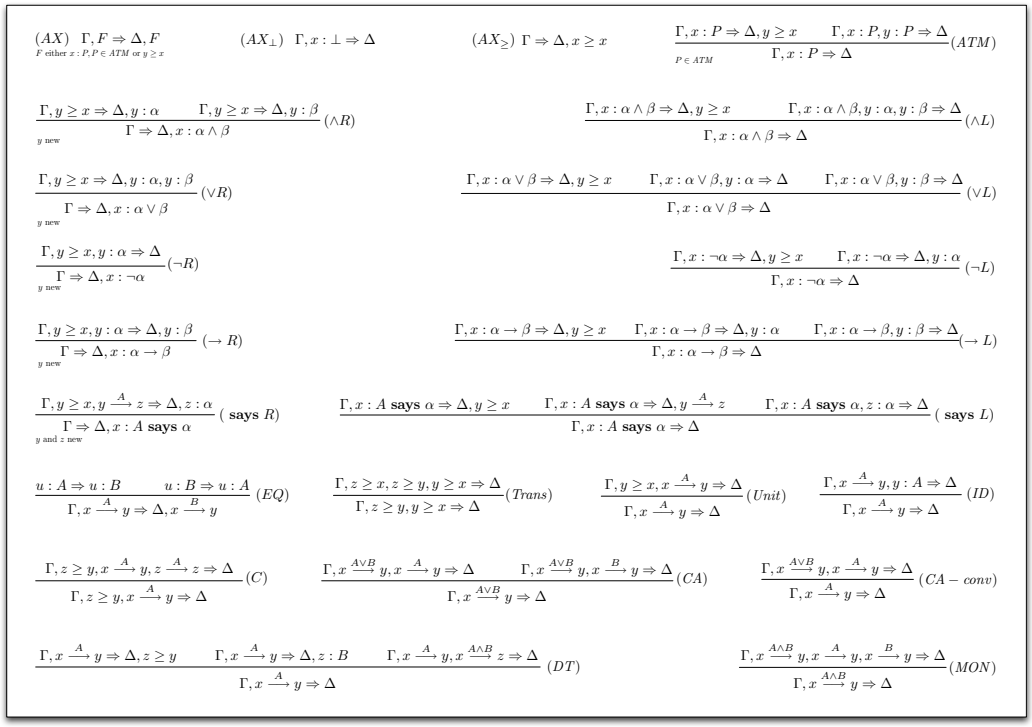

Fig. 1. The sequent calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$.

The following properties hold in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$:

Lemma 5 (Height-preserving admissibility of weakening). *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.*

Lemma 7 (Height-preserving invertibility of rules). *Let $\Gamma \Rightarrow \Delta$ be an instance of the conclusion of a rule R of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, 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 $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, 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 $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, then there is a derivation of no greater height of $\Gamma, F \Rightarrow \Delta$.*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\ldots, z \geq x \Rightarrow z : \alpha, z \geq x}(AX) \quad \dfrac{}{\ldots, x : \alpha, z : \alpha \Rightarrow z : \alpha}(AX)}{z \geq x, z \geq y, y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha}(ATM)}{z \geq y, y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha}(Trans)}{y \geq x, x \geq u, x : \alpha, y \xrightarrow{A} z \Rightarrow z : \alpha}(Unit)}{x \geq u, x : \alpha \Rightarrow x : A \textbf{ says } \alpha}(\textbf{ says } R)}{\Rightarrow u : \alpha \rightarrow (A \textbf{ says } \alpha)}(\rightarrow R)$$

Fig. 2. A derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for (UNIT).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Rightarrow w \geq w}(AX_{\geq}) \quad \dfrac{}{w \xrightarrow{A} w \Rightarrow w \xrightarrow{A} w}(AX) \quad \dfrac{}{w : \alpha \Rightarrow w : \alpha}(AX)}{w \geq y, x \geq u, x \xrightarrow{A} y, w \xrightarrow{A} w, w : A \textbf{ says } \alpha \Rightarrow w : \alpha}(\textbf{ says } L)}{w \geq y, x \geq u, x \xrightarrow{A} y, w : A \textbf{ says } \alpha \Rightarrow w : \alpha}(C)}{x \geq u, x \xrightarrow{A} y \Rightarrow y : (A \textbf{ says } \alpha) \rightarrow \alpha}(\rightarrow R)}{\Rightarrow u : A \textbf{ says } ((A \textbf{ says } \alpha) \rightarrow \alpha)}(\textbf{ says } R)$$

Fig. 3. A derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ for (C).

Lemma 9. *A sequent* $\Rightarrow x : A \rightarrow B$ *is derivable in* $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ *if and only if the sequent* $x : A \Rightarrow x : B$ *is derivable in* $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$.

We now consider the cut rule:

$$\dfrac{\Gamma \Rightarrow \Delta, F \qquad \Gamma, F \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}(cut)$$

where F is any labelled formula. We prove that this rule is admissible in the calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$. 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 $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ the standard proof does not work in case the cutting formula F is a transition formula $x \xrightarrow{A} y$ derived by an application of (EQ) in the left premise, and by an application of one of the following rules: $(C), (CA), (CA - conv), (DT), (MON)$ in the right premise. In order to prove the admissibility of cut for $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, 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 $u : A \Rightarrow u : A'$ and $u : A' \Rightarrow u : A$ are derivable, we denote with $\Gamma^{\star} \Rightarrow \Delta^{\star}$ 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 4. *In $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$, the following propositions hold:*

- *(A) If $\Gamma \Rightarrow \Delta, F$ and $\Gamma, F \Rightarrow \Delta$ are derivable, so is $\Gamma \Rightarrow \Delta$, i.e. the rule (cut) is admissible in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$;*
- *(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) $u : A \Rightarrow A'$ and (III) $u : A' \Rightarrow A$ are derivable, then $\Gamma^\star \Rightarrow \Delta^\star$ is derivable with a derivation of height $h' \leq h$.*

Theorem 5 (Soundness of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$). *If $\Gamma \Rightarrow \Delta$ is derivable, then $\Gamma \Rightarrow \Delta$ is valid in the sense of Definition 5.*

Theorem 6 (Completeness of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$). *If $\Gamma \Rightarrow \Delta$ is valid in the sense of Definition 5, then $\Gamma \Rightarrow \Delta$ is derivable.*

Completeness of $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$ with respect to $\mathsf{Cond}_{\mathrm{ACL}}$ models of Definition 1 immediately follows from the completeness of the axiomatization of $\mathsf{Cond}_{\mathrm{ACL}}$ with respect to the semantics, shown in Theorem 3. We have that a formula $\varphi \in \mathcal{L}$ is valid if and only if the sequent $\Rightarrow u : \varphi$ has a derivation in $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$.

5 Related Work

The formal study of properties of access control logics is a recent research trend. As reported in [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 example, we can prove G using a classical logic by proving $F \rightarrow G$ and $\neg F \rightarrow G$, since from these theorems we can conclude $(F \vee \neg F) \rightarrow G$, hence $\top \rightarrow G$.

Abadi in [14] presents a formal study about connections between many possible axiomatizations of the says, as well as higher-level policy constructs such as delegation (speaks-for) and control. Abadi provides a strong argument to use constructivism in logic for access control, in fact he shows that from a well-known axiom like Unit in a classical logic we can deduce K says $\varphi \rightarrow (\varphi \vee K$ says $\psi)$. The axiom above is called *Escalation* and it represents a rather degenerate interpretation of says, i.e., if a principal says φ then, 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.

Even if there exist several authorization logics that employ the says modality, a limited amount of work has been done to study the formal logical properties of says, speaks-for and other constructs. In the following, we report the three different approaches adopted to study access control logics themselves.

Garg and Abadi [15] translate existing access control logics into S4 by relying on a slight simplification of Gödel's translation from intuitionistic logic to S4, and extending it to formulas of the form A says φ.

Garg [10] adopts an ad-hoc version of constructive S4 called DTL_0 and embeds existing approaches into it. Constructive S4 has been chosen because of its intuitionistic Kripke semantics which DTL_0 extends by adding *views* [10], i.e., a mapping from worlds to sets of principals.

Boella et al. [8] define a logical framework called FSL[5], based on Gabbay's Fibring semantics [16] by looking at says as a (fibred) modal operator.

However, adopting a fixed semantics like S4 does not permit to study the *correspondence theory* between axioms of access control logics and Kripke structures. Suppose we look at says as a principal indexed modality $\Box_K$, if we rely on S4 we would have as an axiom $\Box_K\varphi \rightarrow \varphi$, which means: *everything* that K says is permitted. To overcome this problem, both in [10, 15], Kripke semantics is sweetened with the addition of *views* which relativize the reasoning to a subset of worlds. Although this approach provides sound and complete semantics, it breaks the useful bound between modal axioms and semantic relations of Kripke structures.

6 Conclusion

We defined an intuitionistic conditional logic for Access Control called $\mathsf{Cond}_{\mathrm{ACL}}$.

The major contribution of our conditional approach w.r.t. works in [10, 15] is the identification of canonical properties for axioms of the logic (in particular Unit and C), i.e., first-order conditions on Kripke structures that are *necessary* and *sufficient* for the corresponding axiom to hold. In [8, 17, 18] we identify canonical properties for other access control axioms (e.g., C4, speaks-for, hand-off[6]).

We believe that this methodology has several advantages. First, the formalization of first-order constraints on Kripke structures shows that we do not need the full power and complexity of second-order quantification, this result has been proved for speaks-for relationship in [15] but our approach also applies to all other second-order well-known axioms for which we identify canonical properties. The fact that, from a semantic viewpoint, modal logic axiom schemas are not really second-order is a well-known result of modern modal logic and, by looking at **says** as a conditional modality, we managed to apply the same methodology to access control logics.

Second, the identification of canonical properties for access control axioms provides a natural deconstruction of access control logics. By deconstruction we intend the possibility to craft access control logics that adopt *any* combination of axioms for which there exists canonical properties. Garg and Abadi in [15] provide a translation into S4 of an access control logic with Unit and C4, but they do not define the semantic properties of the axioms with respect to the view based semantics. This limits the flexibility of the adopted semantics. For instance, although not all access control systems adopt Unit as an axiom [4, 19, 3], the translation in [15] does not provide an embedding in S4 for an access control logic without Unit. In particular, the approach in [15] does not provide a general methodology to deconstruct access control logics. In our approach, instead, we can formalize a logic and a calculus without Unit which is still sound and complete, by dropping the semantic condition S-UNIT and the corresponding rule $(Unit)$ in the calculus.

In this work, we have proven that the axiomatization of the intuitionistic conditional logic $\mathsf{Cond}_{\mathrm{ACL}}$ is sound and complete with respect to the semantics. Moreovoer, we

[5] Fibred Security Language.

[6] For a detailed discussion about these axioms see [14].

have provided a cut-free, labelled, sequent calculus for this logic. In $\mathsf{Cond}_{\mathrm{ACL}}$, principals are defined as arbitrary formulas. The generality of the language makes it possible to formalize, for instance, the so called boolean principals [7], that is, principals which are formed by boolean combinations of atomic principals. For the time being, $\mathsf{Cond}_{\mathrm{ACL}}$ only includes few 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". We believe that choosing axioms for access control logics depends on the needs of security practitioners. With $\mathsf{Cond}_{\mathrm{ACL}}$ we show that, by looking at **says** as a conditional modality, we can offer a formal framework to study axioms of access control via canonical properties on the semantics and to build calculi to carry out automated deduction. Other issues to be tackled are the complexity of the logic $\mathsf{Cond}_{\mathrm{ACL}}$ and the termination and complexity of the sequent calculus $\mathcal{S}_{\mathsf{Cond}_{\mathrm{ACL}}}$. This is what we plan to do for 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.

References

1. Abadi, M., Burrows, M., Lampson, B.W., Plotkin, G.D.: A calculus for access control in distributed systems. In: CRYPTO 91. 1–23
2. Bertolissi, C., Fernández, M., Barker, S.: Dynamic event-based access control as term rewriting. In: DBSec07. 195–210
3. Gurevich, Y., Roy, A.: Operational semantics for DKAL: Application and analysis. In: TrustBus 2009. 149–158
4. Lesniewski-Laas, C., Ford, B., Strauss, J., Morris, R., Kaashoek, M.F.: Alpaca: extensible authorization for distributed services. In: Proc. of ACM CCS 2007. 432–444
5. Li, N., Grosof, 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: DEON08. 96–109
7. Garg, D., Abadi, M.: A modal deconstruction of access control logics. In: FoSSaCS 08, Budapest, Hungary 216–230
8. Boella, G., Gabbay, D., Genovese, V., van der Torre, L.: Fibred security language. Studia Logica **92**(3) (2009) 395–436
9. Nute, D.: Topics in Conditional Logic. Reidel, Dordrecht (1980)
10. Garg, D.: Principal centric reasoning in constructive authorization logic. In: Informal Proc. of IMLA. (2008)
11. Troelstra, A., van Dalen, D.: Constructivism in Mathematics: An Introduction. North-Holland Publishing, Amsterdam
12. Olivetti, N., Pozzato, G.L., Schwind, C.B.: A Sequent Calculus and a Theorem Prover for Standard Conditional Logics. ACM Transactions on Computational Logics **8**(4) (2007)
13. Garg, D., Pfenning, F.: Non-interference in constructive authorization logic. In: CSFW-19. (2006) 283–296
14. Abadi, M.: Variations in access control logic. In: 9th International Conference on Deontic Logic in Computer Science (DEON). (2008) 96–109
15. Garg, D., Abadi, M.: A modal deconstruction of access control logics. In: FoSSaCS 08, Budapest, Hungary 216–230

16. Gabbay, D.M.: Fibring logics. Oxford University Press (1999)
17. Genovese, V., Giordano, L., Gliozzi, V., Pozzato, G.: A constructive conditional logic for access control: a preliminary report. In: ECAI 2010 (to appear)
18. Modal Access Control Logic: Axiomatization, S., Proving, F.T.: D. m. gabbay and v. genovese and d. rispoli and l. van der torre. In: (to appear)
19. Becker, M.Y., Fournet, C., Gordon, A.D.: Design and semantics of a decentralized authorization language. In: 20th IEEE Computer Security Foundations Symposium (CSF). (2007) 3–15