A

Calculus of Cooperation and Game-Based Reasoning about Protocol Privacy

SARA MINER MORE and PAVEL NAUMOV, McDaniel College

The article introduces a new formal system, the calculus of cooperation, for reasoning about coalitions of players in a certain class of games. The calculus is an extension of the propositional intuitionistic logic that adds a coalition parameter to intuitionistic implication. The system is shown to be sound and complete with respect to a game semantics.

One intended application of the calculus of cooperation is the verification of privacy properties in multiparty computation protocols. The article argues that such properties can be established by providing a set of strategies for a non-zero-sum, perfect information game based on the protocol. It concludes with several examples of such verifications formalized in the calculus of cooperation.

Categories and Subject Descriptors: F.3.1 [**Theory of Computation**]: Logic and Meaning of Programs

General Terms: Theory, Verification, Security

Additional Key Words and Phrases: intuitionistic logic, games, multiparty computation, privacy, formal verification

ACM Reference Format:
ACM Trans. Comput. Logic V, N, Article A (January YYYY), 21 pages.
DOI = 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

1. INTRODUCTION

In 1933, Gödel [9] proposed a translation τ of intuitionistic propositional formulas into a modal language. Formula $\tau(F)$ is obtained from formula F by placing the modality $\Box$ in front of each subformula of formula F. He proved that if F is a theorem in intuitionistic propositional calculus IPL [12], then $\tau(F)$ is provable in modal logic $S4$. The converse of this statement was later shown by McKinsey and Tarski [19]. In light of these results, intuitionistic logic can be viewed as a calculus of "boxed" formulas or formulas that make claims in some stronger, modal, sense.

In this article we introduce a certain class of games and a logical calculus for reasoning about outcomes of these games. We later apply this calculus to verify privacy properties of multiparty computation protocols. Existing formal systems for reasoning about games, such as game logic [21; 24], coalition logic [23], cooperation logic [26], and alternating-time temporal logic [1], are variations of the labeled modal logic and are rich enough to be able to reason not only about outcomes of games, but also about intermediate states of games. As we will show in the second part of this article, at least for the purposes of the verification of privacy properties of multiparty computation protocols, one only needs to be able to reason about outcomes of the games. Our proposed logical calculus does just that and, thus, it provides a more succinct logical framework for such arguments. To achieve this goal, we base our logical system not on modal logic, but on intuitionistic propositional calculus. If the systems above add

...

DOI 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

labels to modality, we add labels to the intuitionistic implication. Although Gödel's translation can not be used in order to formally embed our calculus into any existing modal logic of games, our work shows that a connection between label modality and labeled intuitionistic logic exists, but on a less formal level than in the results of Gödel, McKinsey, and Tarski.

At the center of our formal logical system is a new propositional connective $\psi \to^c \phi$ that we call *coalition-controlled implication* or controlled implication, for short. Informally, $\psi \to^c \phi$ means that a coalition of players c has a strategy to achieve ϕ if condition ψ is guaranteed to be true by the end of the game. Unlike, say, in Hoare Logic [13], statements ϕ and ψ in controlled implication are both "postconditions" in the sense that they both make claims about the outcome of the game.

Note that $\phi \to^{\varnothing} \psi$ means that ϕ implies ψ without any parties having to follow a specific strategy. Thus, this is just the standard logical implication $\phi \to \psi$. For simplicity, we will normally use the notation $\phi \to \psi$ rather than $\phi \to^{\varnothing} \psi$.

We will show the calculus of cooperation to be a sound and complete logical system (with respect to the game semantics defined later) that describes logical properties of controlled implication. An example of such a property, provable in the calculus of cooperation, is the formula

$$(\phi \to^c \psi) \to ((\psi \to^d \chi) \to (\phi \to^{c,d} \chi)),$$

where c and d are two disjoint coalitions and c, d denotes the union of these coalitions.

Another distinctive feature of the calculus of cooperation is its underlying assumption that each player makes no more than one move. This, on one hand, makes our game similar to strategic games, where each moves consists in choosing a strategy for the whole game. On the other hand, a player in our game can be viewed as a resource owned by a coalition. This view connects the calculus with linear logic [8]. However, these two logical systems differ in that resources in linear logic are identified with propositions, not implication labels. The same feature is also present in progressing collaborative systems [14].

Finally, note that although the calculus of cooperation is based on intuitionistic logic, its game semantics is considerably different from the game semantics for intuitionistic logic [17]. The latter is restricted only to very specialized two-party dialog-type games.

The paper consists of two distinct parts: Sections 2 and 3.1, in which we describe the class of game, introduce the logical system, and prove its completeness, and Section 4, where we illustrate use of the calculus for reasoning about privacy in multiparty computation protocols on several examples.

2. CALCULUS OF COOPERATION

2.1. Game Definition

Throughout this article, we will assume a fixed infinite set of player names $p, q, r, \ldots$. As syntactical objects, these player names (or, for short, "players") are similar to the atomic proposition names $A, B, C, \ldots$. An arbitrary finite set of players will be called a coalition. The set of all coalitions is denoted by $\mathcal{C}$. We will use letters $c, d, e, \ldots$ to denote coalitions.

Definition 2.1. A quadruple $\mathcal{F} = \langle S, \preceq, A, \{\rightsquigarrow^c\}_{c \in \mathcal{C}} \rangle$ is called a game frame if

(1) S is a set of "states" of the game.
(2) $\preceq$ is a transitive and reflexive "accessibility" relation between the states.
(3) $A(s)$ is a set of players called the set of "active" players in state s. The following monotonicity condition will be assumed: if $s \preceq s'$, then $A(s') \subseteq A(s)$.
(4) For any coalition c, relation $\rightsquigarrow^c$ is a binary relation between states such that

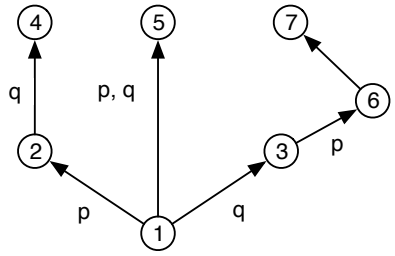

Fig. 1. A Game Frame

(a) if $p \in A(s)$ then there is s' such that $s \rightsquigarrow^p s'$,
(b) if $s \rightsquigarrow^c s'$, then $s \preceq s'$,
(c) if $s \rightsquigarrow^c s'$, then $c = A(s) \backslash A(s')$,
(d) if $s \rightsquigarrow s'$, then $s = s'$.

In the above definition, as well as through the rest of this article, we write $s \rightsquigarrow s'$ instead of $s \rightsquigarrow^{\varnothing} s'$. Informally, $s \rightsquigarrow^c s'$ means that coalition of players c can move the game from state s to state s'. Later in this article we will use notations $s \preceq s'$ and $s' \succeq s$ interchangeably.

An example game frame is given in Figure 1. In this frame, $S = \{1, 2, 3, 4, 5, 6, 7\}$ and the accessibility relation $\preceq$ is specified by the arrows on the diagram. Relation $\rightsquigarrow^c$ is defined by the arrows labeled with coalition c. Thus, for example, player p can on its own move the game from state 1 to state 2. However, it takes a coalition of players p and q to move from state 1 to state 5. Note that although state 7 is formally "accessible" from state 3, there is no coalition powerful enough to make this transition. Player p is active in states 1 and 3. Player q is active in states 1 and 2. The notion of "active" player is introduced in order to guarantee that each player will make exactly one move in the game. This appears to be a severe restriction on the type of games we consider. However, when we later consider protocol-based games, we will interpret moves as commitments of a player to a particular strategy, thus making our results applicable to a much wider class of games.

There are different claims that can be made during the game. However, we will only be interested in statements about outcomes of the game. Such statements are monotonic in the sense that once they become true they will remain true through the end of the game.

Definition 2.2. A game frame is finite if the set of states is finite and the set of active players at each state is finite.

Definition 2.3. A game is a pair $\mathcal{G} = (\mathcal{F}, \Vdash)$, where $\mathcal{F}$ is a game frame and $\Vdash$ is a relation between states of the game frame and propositional variables that satisfies the following monotonicity property: if $u \Vdash A$ and $u \preceq v$, then $v \Vdash A$.

Figure 2 specifies a game based on the game frame from Figure 1. The propositional letter A next to state 2 means that $2 \Vdash A$.

Definition 2.4. A game $(\mathcal{F}, \Vdash)$ is finite if frame $\mathcal{F}$ is finite.

Definition 2.5. For any two states u and v of a game frame and any coalition c, we use the notation $u \rightsquigarrow^c_* v$ to state that there is a chain of states $u = v_0 \rightsquigarrow^{c_0} v_1 \rightsquigarrow^{c_1} \cdots \rightsquigarrow^{c_n} v_n = v$ such that $n \geq 0$ and $c_1 \cup \cdots \cup c_n = c$.

We will write $u \rightsquigarrow_* v$ to denote $u \rightsquigarrow^{\varnothing}_* v$.

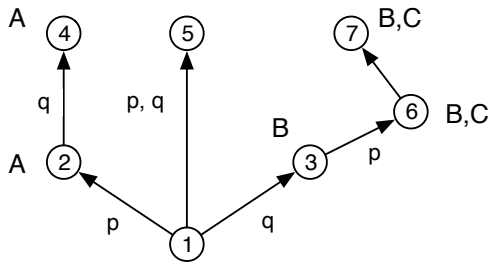

Fig. 2. A Game

LEMMA 2.6. *If* $u \rightsquigarrow_* v$ *then* $u = v$.

PROOF. See Definition 2.1, part 4d. □

2.2. Syntax and Semantics

The language of the calculus of cooperation consists of atomic propositions $A, B, C, \ldots$, player names $p, q, r, \ldots$, the constant $\bot$ denoting falsity, the disjunction symbol $\vee$, the conjunction symbol $\wedge$, the implication symbol $\rightarrow$, and parentheses.

The set of formulas in the calculus of cooperation is defined as the smallest set such that

— any atomic proposition is a formula,
— $\bot$ is a formula,
— if ϕ, ψ are formulas, then $(\phi \vee \psi)$ and $(\phi \wedge \psi)$ are formulas,
— if ϕ, ψ are formulas and c is a finite set of players ("coalition"), then $(\phi \rightarrow^c \psi)$ is a formula.

As is customary when writing a formula, we will normally not show the outer-most pair of parentheses.

Definition 2.7. For any game, the forcing relation $\Vdash$ between game states and formulas is defined as the following extension of the relation $\Vdash$ between game states and atomic propositions:

(1) $s \nVdash \bot$ for any state s,
(2) $s \Vdash \phi \wedge \psi$ if and only if $s \Vdash \phi$ and $s \Vdash \psi$,
(3) $s \Vdash \phi \vee \psi$ if and only if $s \Vdash \phi$ or $s \Vdash \psi$,
(4) $s \Vdash \phi \rightarrow^c \psi$ iff for any state $u \succeq s$, if $u \Vdash \phi$ and $c \subseteq A(u)$, then there is v such that $u \rightsquigarrow_*^c v$ and $v \Vdash \psi$.

For example, in the game from Figure 2, $1 \Vdash B \rightarrow^p C$ and $1 \Vdash A \rightarrow^p C$. The latter is true because player p is not active in any state where A is forced.

THEOREM 2.8 (MONOTONICITY). *If* $s \Vdash \phi$ *then* $s' \Vdash \phi$ *for any* $s \preceq s'$.

PROOF. Induction on the structural complexity of formula ϕ . □

Definition 2.9. We say that sequent $\Gamma \vdash^c \Delta$ is true at state s of a game iff $s \Vdash \bigwedge \Gamma \rightarrow^c \bigvee \Delta$.

In addition to the primitive symbols of the calculus of cooperation, we will also use several abbreviations. First of all, as is common in logic, by $\top$ we mean the implication $\bot \rightarrow \bot$. Second, for any player p, by $[p]$ we mean the formula $\top \rightarrow^p \bot$. From Definition 2.7, it is easy to see that $s \Vdash [p]$ if and only if player p is "committed" at state s (that

is, $p \notin A(s)$). Finally, for any coalition of players c, by $[c]$ we mean the set of formulas $\{[p] \mid p \in c\}$.

2.3. Axioms and Rules

The calculus of cooperation (CC) can be viewed as an extension of the intuitionistic propositional logic (IPL). We will present an axiomatization of the calculus which is a variation of multi-succedent Gentzen-style axiomatization of IPL (see, for example, [20]).

The two axioms of the calculus are

$$\phi \vdash^c \phi \qquad\qquad \bot \vdash^c$$

The first axiom says that if ϕ is true at some state, it will be true after any c-move. The soundness of this axiom follows from Theorem 2.8. The validity of the second axiom follows from the fact that, by Definition 2.7, formula $\bot$ is false at any state of the game.

Below we list the inference rules of our system. The soundness of several of them may not be obvious; we prove soundness below in Theorem 2.10.

The structural rules are standard contraction and weakening rules with an added coalition parameter:

$$\frac{\Gamma, \Gamma', \Gamma' \vdash^c \Delta, \Delta', \Delta'}{\Gamma, \Gamma' \vdash^c \Delta, \Delta'} \ (\mathrm{C})$$

$$\frac{\Gamma \vdash^c \Delta}{\Gamma, \Gamma' \vdash^{c,d} \Delta, \Delta'} \ (\mathrm{W})$$

The rules for disjunction are also standard rules with an added coalition parameter:

$$\frac{\phi, \Gamma \vdash^c \Delta \qquad \psi, \Gamma' \vdash^c \Delta'}{\phi \vee \psi, \Gamma, \Gamma' \vdash^c \Delta, \Delta'} \ (\mathrm{L}_\vee)$$

$$\frac{\Gamma \vdash^c \Delta, \phi, \psi}{\Gamma \vdash^c \Delta, \phi \vee \psi} \ (\mathrm{R}_\vee)$$

The three rules for conjunction are:

$$\frac{\Gamma, \phi, \psi \vdash^c \Delta}{\Gamma, \phi \wedge \psi \vdash^c \Delta} \ (\mathrm{L}_\wedge)$$

$$\frac{\Gamma \vdash^c \Delta, \phi \qquad \Gamma', [c] \vdash^d \Delta', \psi}{\Gamma, \Gamma' \vdash^{c,d} \Delta, \Delta', \phi \wedge \psi} \ (\mathrm{R}^1_\wedge)$$

$$\frac{\Gamma \vdash^c \Delta, \psi \qquad \Gamma', [c] \vdash^d \Delta', \phi}{\Gamma, \Gamma' \vdash^{c,d} \Delta, \Delta', \phi \wedge \psi} \ (\mathrm{R}^2_\wedge)$$

where in rules $(\mathrm{R}^1_\wedge)$ and $(\mathrm{R}^2_\wedge)$, coalitions c and d are assumed to be disjoint. Informally, the first of these rules says that if coalition c has a strategy for achieving ϕ and coalition d has a strategy for achieving ψ (which might rely on knowledge of the move by coalition c), then, working together, these two coalitions can achieve $\phi \wedge \psi$. The rules for coalition-controlled implication are

$$\frac{\Gamma \vdash \phi \qquad \Gamma', \psi, [c] \vdash \Delta}{\Gamma, \Gamma', \phi \to^c \psi \vdash^c \Delta} \ (\mathrm{L}_\to)$$

$$\frac{\Gamma, \phi, [d] \vdash^c \psi}{\Gamma \vdash^d \phi \to^c \psi} \ (\mathrm{R}_\to)$$

The next two rules resemble the IPL "cut" rule. We call the first rule a "cooperation" rule because it shows how strategies of two disjoint teams can be combined together.

$$\frac{\Gamma \vdash^c \Delta, \phi \qquad \Gamma', \phi, [c] \vdash^d \Delta'}{\Gamma, \Gamma' \vdash^{c,d} \Delta, \Delta'} \ (\mathrm{CP})$$

where coalitions c and d are disjoint. The name "cut" is reserved for the second rule:

$$\frac{\Gamma \vdash^c \Delta, [p] \qquad \Gamma', [p] \vdash^c \Delta'}{\Gamma, \Gamma' \vdash^c \Delta, \Delta'} \ (\mathrm{CUT})$$

where $p \notin c$. Our final rule is the self-determination rule:

$$\frac{\Gamma \vdash^c [d]}{\Gamma \vdash [c, d]} \ (\mathrm{SD})$$

where coalitions c and d are disjoint. Informally, this rule says that a player can not be become inactive through a move by a coalition that does not include this player.

2.4. Soundness

THEOREM 2.10 (SOUNDNESS). *Every sequent provable in the calculus of cooperation is true in every state of every game.*

PROOF. Induction on the size of the derivation.

Let us start with the two axioms. First, to show that $s \Vdash \phi \to^c \phi$, assume that $u \Vdash \phi$ for some $u \succeq s$ such that $c \subseteq A(u)$. Let $c = \{p_1, \dots, p_n\}$. By Definition 2.1, there is a chain $u \rightsquigarrow^{p_1} v_1 \rightsquigarrow^{p_2} \cdots \rightsquigarrow^{p_n} v_n$. Thus, $u \rightsquigarrow_*^c v_n$. By Theorem 2.8, $v_n \Vdash \phi$. Therefore, $s \Vdash \phi \to^c \phi$. To justify the second axiom, we need to show that $s \Vdash \bot \to^c \bot$. This, however, is true by Definition 2.7, since $u \nVdash \bot$ for any state u. Next, we consider the inference rules.

Rule (W).. To prove the soundness of the weakening rule, assume that $u \Vdash \bigwedge \Gamma \wedge \bigwedge \Gamma'$, for some $u \succeq s$ such that $c \cup d \subseteq A(u)$. By the rule's hypothesis, there is a state v such that $u \rightsquigarrow^c v$ and $v \Vdash \bigvee \Delta$. Let $d = \{p_1, \dots, p_n\}$. By Definition 2.1, there is a chain $v \rightsquigarrow^{p_1} v_1 \rightsquigarrow^{p_2} \cdots \rightsquigarrow^{p_n} v_n$. Thus, $u \rightsquigarrow_*^{c,d} v_n$. By Theorem 2.8, $v_n \Vdash \bigvee \Delta$. Hence, $v_n \Vdash \bigvee \Delta \vee \bigvee \Delta'$. Therefore, $s \Vdash \bigwedge \Gamma \wedge \bigwedge \Gamma' \to^{c,d} \bigvee \Delta \vee \bigvee \Delta'$. The soundness of the contraction rule (C) can be established similarly.

Rule ($\mathrm{L}_\vee$).. Assume that $u \Vdash (\phi \vee \psi) \wedge \bigwedge \Gamma \wedge \bigwedge \Gamma'$ for some $u \succeq s$, such that $c \subseteq A(u)$. Thus, either $u \Vdash \phi \wedge \bigwedge \Gamma$ or $u \Vdash \psi \wedge \bigwedge \Gamma'$. Without loss of generality, assume the former. By the first hypothesis of the rule, there is a node v such that $u \rightsquigarrow_*^c v$ and $v \Vdash \bigvee \Delta$. Hence, $v \Vdash \bigvee \Delta \vee \bigvee \Delta'$. Therefore, $s \Vdash (\phi \vee \psi) \wedge \bigwedge \Gamma \wedge \bigwedge \Gamma' \to^c \bigvee \Delta \vee \bigvee \Delta'$. The soundness of rules ($\mathrm{R}_\vee$) and ($\mathrm{L}_\wedge$) can be established similarly.

Rule ($\mathrm{R}_\wedge^1$).. Suppose that $u \Vdash \bigwedge \Gamma \wedge \bigwedge \Gamma'$ for some $u \succeq s$ such that $c \cup d \subseteq A(u)$. By the rule's first hypothesis, there is a state v such that $u \rightsquigarrow_*^c v$ and $v \Vdash \bigvee \Delta \vee \phi$. By Theorem 2.8, $v \Vdash \bigwedge \Gamma'$. Notice that $v \Vdash \bigwedge [c]$ because $u \rightsquigarrow_*^c v$ implies that each member of c is not active in v. Thus, by the second hypothesis of the rule, there is a state w such that $v \rightsquigarrow_*^d w$ and $w \Vdash \bigvee \Delta' \vee \psi$. Note that $u \rightsquigarrow_*^{c,d} w$. By Theorem 2.8, $w \Vdash \bigvee \Delta \vee \phi$.

Therefore, $w \Vdash \bigvee \Delta \vee \bigvee \Delta' \vee (\phi \wedge \psi)$. The soundness of rules ($\mathrm{R}^2_\wedge$) and (CP) can be established similarly.

Rule ($\mathrm{L}_\to$).. Consider any state $u \succeq s$ such that $c \subseteq A(u)$ $u \Vdash \bigwedge \Gamma$, $u \Vdash \bigwedge \Gamma'$, and $u \Vdash \phi \to^c \psi$. By the rule's first hypothesis, $u \Vdash \phi$. Taking into account $u \succeq u$ and $u \Vdash \phi$, we can conclude that there is a state v such that $u \rightsquigarrow^c_* v$ and $v \Vdash \psi$. By Theorem 2.8, $v \Vdash \bigwedge \Gamma$ and $v \Vdash \bigwedge \Gamma'$. Therefore, by the rule's second hypothesis, $v \Vdash \bigvee \Delta$.

Rule ($\mathrm{R}_\to$).. Assume that $u \Vdash \bigwedge \Gamma$ for some $u \succeq s$ such that $d \subseteq A(u)$. Let $d = \{p_1, \ldots, p_n\}$. By Definition 2.1, there is a chain $u \rightsquigarrow^{p_1} v_1 \rightsquigarrow^{p_2} \cdots \rightsquigarrow^{p_n} v_n$. Thus, $u \rightsquigarrow^d_* v_n$. We will show that $v_n \Vdash \phi \to^c \psi$. Indeed, let $w \succeq v_n$ be any node such that $w \Vdash \phi$ and $c \subseteq A(w)$. Note that $u \rightsquigarrow^d_* v_n$ implies that no members of coalition d are active at w. Thus, $w \Vdash [d]$. By Theorem 2.8, $w \Vdash \bigwedge \Gamma$. Hence, by the rule's hypothesis, there is a state t such that $w \rightsquigarrow^c_* t$ and $t \Vdash \psi$. Therefore, $v_n \Vdash \phi \to^c \psi$.

Rule (CUT).. Consider any state $u \succeq s$ such that $c \subseteq A(u)$ and $u \Vdash \bigwedge \Gamma \wedge \bigwedge \Gamma'$. By the rule's first hypothesis, there is a state v such that $u \rightsquigarrow^c_* v$ and either $v \Vdash \bigvee \Delta$ or $v \Vdash [p]$. In the first case, the desired result is already established. Assume that $v \Vdash [p]$. Thus, $p \notin A(v)$. Taking into account that $c = A(u) \backslash A(v)$ and $p \notin c$, we can conclude that $p \notin A(u)$. Hence, $u \Vdash [p]$. Thus, by the rule's second hypothesis, there is a state v' such that $u \rightsquigarrow^c_* v'$ and $v' \Vdash \bigvee \Delta'$. Therefore, $v' \Vdash \bigvee \Delta' \vee \bigvee \Delta'$.

Rule(SD).. Consider any $u \succeq s$ such that $u \Vdash \bigwedge \Gamma$. If there is at least one $p \in c$ such that $p \notin A(u)$, then $u \Vdash \bigvee [c, d]$. Assume that $c \subseteq A(u)$. By the rule's hypothesis, there is a state v such that $u \rightsquigarrow^c_v$ and $v \Vdash \bigvee [d]$. Thus, there is $p \in d$ such that $p \notin A(v)$. Hence, $p \notin A(u)$, because $A(u) = A(v) \cup c$ and $c \cap d = \varnothing$. Therefore, $u \Vdash \bigvee [c, d]$. □

3. COMPLETENESS AND DECIDABILITY

THEOREM 3.1 (COMPLETENESS). *If a sequent is true in every state of every finite game, then it is provable in the calculus of cooperation.*

The rest of this section is almost entirely dedicated to the proof of the above theorem. Suppose that $\Gamma \nvdash^c \Delta$. Let Φ be a finite set of formulas that contains $\Gamma \cup \Delta$ and is closed with respect to subformulas and Π be the finite set of all player names that occur in Φ and c.

3.1. Consistent Triples

Definition 3.2. For any $X, Y \subseteq \Phi$ and any $c \subseteq \Pi$, triple (X, c, Y) is called consistent if $X \nvdash^c Y$.

Note that the notation $[c]$ introduced earlier can be viewed as a "square bracket" function that maps a coalition c into the set of formulas $Z = [c]$. We will use the notation $\sqrt{Z}$ for what, essentially, is the inverse "unsquare" function:

Definition 3.3. $\sqrt{Z} = \{p \mid [p] \in Z\}$.

LEMMA 3.4. *For any consistent triple (X, c, Y), sets $\sqrt{X}$, c, and $\sqrt{Y}$ are pairwise disjoint.*

PROOF. To show that three sets are pairwise disjoint, we need to prove that any two of them have no common elements. Assume the opposite and consider three possible cases.

(1) If $p \in \sqrt{X} \cap c$, then consider derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\bot \vdash \bot}}{\vdash \bot \to \bot}\,(\mathrm{R}_{\to}) \qquad \dfrac{\dfrac{}{\bot \vdash}}{[p], \bot \vdash}\,(\mathrm{W})}{(\bot \to \bot) \to^p \bot \vdash^p}\,(\mathrm{L}_{\to})}{X \vdash^c Y}\,(\mathrm{W})$$

This contradicts the assumption that triple (X, c, Y) is consistent.

(2) If $p \in \sqrt{X} \cap \sqrt{Y}$, then consider derivation

$$\dfrac{[p] \vdash [p]}{X \vdash^c Y}\,(\mathrm{W})$$

Again, this contradicts the assumption that triple (X, c, Y) is consistent.

(3) If $p \in c \cap \sqrt{Y}$, then consider derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\bot \to \bot \vdash \bot \to \bot} \qquad \dfrac{\dfrac{}{\bot \vdash}}{[p], \bot \vdash \bot}\,(\mathrm{W})}{(\bot \to \bot) \to^p \bot, \bot \to \bot \vdash^p \bot}\,(\mathrm{L}_{\to})}{[p], \bot \to \bot \vdash^p \bot}\,(\mathrm{DEF})}{\vdash^p (\bot \to \bot) \to^p \bot}\,(\mathrm{R}_{\to})}{X \vdash^c Y}\,(\mathrm{W})$$

Once again, this contradicts the assumption that triple (X, c, Y) is consistent.

□

3.2. Saturated Triples

Definition 3.5. Triple (X, c, Y) is semi-saturated if union $\sqrt{X} \cup c \cup \sqrt{Y}$ contains all players $p \in \Pi$.

LEMMA 3.6. *If triple (X, c, Y) is consistent and semi-saturated, then Π is equal to disjoint union $\sqrt{X} \sqcup c \sqcup \sqrt{Y}$.*

PROOF. See Lemma 3.4 and Definition 3.5. □

LEMMA 3.7 (SEMI-SATURATION). *For any consistent triple (X, c, Y) there are sets $X' \supseteq X$ and $Y' \supseteq Y$ such that triple (X', c, Y') is consistent and semi-saturated.*

PROOF. It will be sufficient to show that if (X, c, Y) is a consistent triple, then for any player $p \notin c$ either triple $(X \cup \{[p]\}, c, Y)$ or triple $(X, c, Y \cup \{[p]\})$ is consistent. Indeed, assume the opposite: $[p], X \vdash^c Y$ and $X \vdash^c Y, [p]$ and consider the derivation

$$\dfrac{X \vdash^c Y, [p] \qquad [p], X \vdash^c Y}{X \vdash^c Y}\,(\mathrm{CUT})$$

This contradicts the assumption that triple (X, c, Y) is consistent. □

Definition 3.8. Triple (X, c, Y) is saturated if it is semi-saturated and $X \vdash \phi \vee \psi$ implies that $\phi \in X$ or $\psi \in X$ for any formula $\phi \vee \psi \in \Phi$.

LEMMA 3.9 (SATURATION). *For any consistent semi-saturated triple (X, c, Y) there is a set $X' \supseteq X$ such that triple (X', c, Y) is consistent and saturated.*

PROOF. It will be sufficient to show that for any consistent semi-saturated triple (X, c, Y) and any formula $\phi \vee \psi$, if $X \vdash \phi \vee \psi$, then either $(X \cup \{\phi\}, c, Y)$ or $(X \cup \{\psi\}, c, Y)$ is consistent. Indeed, assume the opposite and consider derivation

$$\dfrac{X \vdash \phi \vee \psi \qquad \dfrac{X, \phi \vdash^c Y \qquad X, \psi \vdash^c Y}{X, \phi \vee \psi \vdash^c Y}\,(\mathrm{L}_{\vee})}{X \vdash^c Y}\,(\mathrm{CP})$$

This contradicts the assumption that triple (X, c, Y) is consistent. □

3.3. Accessibility Relation $\succeq$ on Triples

Definition 3.10. We say that $(X_2, c_2, Y_2) \succeq (X_1, c_1, Y_1)$ if $X_2 \supseteq X_1$.

LEMMA 3.11. *Relation $\succeq$ is transitive and reflexive.*

PROOF. This lemma follows from Definition 3.10 and the transitivity and reflexivity of the subset relation. □

LEMMA 3.12. *If $(X_2, c_2, Y_2) \succeq (X_1, c_1, Y_1)$, then $\sqrt{X_2} \supseteq \sqrt{X_1}$.*

PROOF. If $p \in \sqrt{X_1}$, then $[p] \in X_1$. Hence, by Definition 3.10, $[p] \in X_2$. Therefore, $p \in \sqrt{X_2}$. □

LEMMA 3.13. *For any triple (X, c, Y) and any formula $\phi \to^d \psi \in \Phi$, if $X \nvdash \phi \to^d \psi$, there is a consistent saturated triple $(X', d, Y') \succeq (X, c, Y)$ such that $\phi \in X'$ and $\psi \in Y'$.*

PROOF. Consider triple $(X \cup \{\phi\}, d, \{\psi\})$. Let us first show that this triple is consistent. Assume the opposite and consider the derivation

$$\frac{X, \phi \vdash^d \psi}{X \vdash \phi \to^d \psi}\ (\mathrm{R}_{\to})$$

This contradicts the assumption that $X \nvdash \phi \to^d \psi$. Thus, $(X \cup \{\phi\}, d, \{\psi\})$ is a consistent triple. By Lemma 3.7, there is a semi-saturated consistent triple (X_1, c, Y_1) such that $X_1 \supseteq X \cup \{\phi\}$ and $Y_1 \supseteq \{\psi\}$. By Lemma 3.9, there is a saturated consistent triple (X', c, Y') such that $X' \supseteq X_1 \supseteq X \cup \{\phi\}$ and $Y' = Y_1 \supseteq \{\psi\}$. □

3.4. Move Relation $\rightsquigarrow^c$ on Triples

Definition 3.14. We say that $(X_1, c_1, Y_1) \rightsquigarrow^d (X_2, c_2, Y_2)$ if the following properties are satisfied

(1) $X_2 \supseteq X_1$,
(2) $d = \sqrt{X_2} \backslash \sqrt{X_1}$,
(3) if $d \subseteq c_1$, then $c_2 = c_1 \backslash d$ and $Y_1 \subseteq Y_2$,
(4) if $d = \varnothing$, then $(X_1, c_1, Y_1) = (X_2, c_2, Y_2)$.

LEMMA 3.15. *Relation $\succeq$ satisfies the following properties*

(1) if $u \rightsquigarrow^c v$, then $v \succeq u$,
(2) $u \rightsquigarrow v$ iff $u = v$.

PROOF. Both properties follow immediately from Definition 3.14. □

LEMMA 3.16. *For any consistent saturated triple $u = (X_u, c_u, Y_u)$ and any set of players d such that $\sqrt{X_u} \cap d = \varnothing$, $X_u \vdash \phi$, and $X_u \vdash \phi \to^d \psi$, there is a consistent saturated triple $v = (X_v, c_v, Y_v)$ such that $u \rightsquigarrow^d v$ and $X_v \vdash \psi$.*

PROOF. We will consider three cases separately.
Case 1: $d = \varnothing$. Take $v = u$. By Lemma 3.15, $u \rightsquigarrow v$. So, we only need to show that $X_u \vdash \psi$. Indeed, consider derivation

$$\dfrac{X_u \vdash \phi \to \psi \qquad \dfrac{X_u \vdash \phi \qquad \dfrac{\psi \vdash \psi}{X_u, \psi \vdash \psi}\ (\mathrm{W})}{X_u, \phi \to \psi \vdash \psi}\ (\mathrm{L}_{\to})}{X_u \vdash \psi}\ (\mathrm{CP})$$

Case 2: $d \neq \varnothing$ and $d \subseteq c_u$. We first will show that triple $(X_u \cup \{\psi\} \cup [d], c_u\backslash d, Y_u)$ is consistent. Assume the opposite. Let derivation $\mathcal{D}$ be

$$\dfrac{\dfrac{X_u \vdash \phi \qquad \dfrac{\psi \vdash \psi}{\psi, [d] \vdash \psi}\,(\text{W})}{X_u, \phi \to^d \psi \vdash^d \psi}\,(\text{L}_\to) \qquad X_u, \psi, [d] \vdash^{c_u\backslash d} Y_u}{X_u, \phi \to^d \psi \vdash^{c_u} Y_u}\,(\text{CP})$$

Consider derivation

$$\dfrac{X_u \vdash \phi \to^d \psi \qquad \dfrac{\mathcal{D}}{X_u, \phi \to^d \psi \vdash^{c_u} Y_u}}{X_u \vdash^{c_u} Y_u}\,(\text{CP})$$

This contradicts the consistency of triple u. Therefore, $(X_u \cup \{\psi\} \cup [d], c_u\backslash d, Y_u)$ is consistent. We will show that this triple is semi-saturated. Indeed,

$$\sqrt{X_u \cup \{\psi\} \cup [d]} \cup (c_u\backslash d) \cup \sqrt{Y_u} \supseteq (\sqrt{X_u} \cup d) \cup (c_u\backslash d) \cup \sqrt{Y_u} = \\ = \sqrt{X_u} \cup c_u \cup \sqrt{Y_u}.$$

Finally, $\sqrt{X_u} \cup c_u \cup \sqrt{Y_u} \supseteq \Pi$, because triple u is saturated. By Lemma 3.9, there exists a set $X' \supseteq X_u \cup \{\psi\} \cup [d]$ such that triple $v = (X', c_u\backslash d, Y_u)$ is consistent and saturated. To show that $u \rightsquigarrow^d v$, we only need to establish that $d = \sqrt{X'}\backslash\sqrt{X}$. Indeed, by Lemma 3.6, $\sqrt{X} \sqcup c_u \sqcup \sqrt{Y_u} = \Pi$ and $\sqrt{X'} \sqcup (c_u\backslash d) \sqcup \sqrt{Y_u} = \Pi$. Therefore, $d = \sqrt{X'}\backslash\sqrt{X}$. Finally, $X' \vdash \psi$ can be established through the derivation

$$\dfrac{\psi \vdash \psi}{X' \vdash \psi}\,(\text{W})$$

Case 3: $d \not\subseteq c_u$. First, we will show that the triple $(X_u \cup \{\psi\} \cup [d], \varnothing, [\Pi\backslash(\sqrt{X_u} \cup d)])$ is consistent. Assume the opposite. Let $\mathcal{D}$ be the derivation:

$$\dfrac{X_u \vdash \phi \qquad X_u, \psi, [d] \vdash [\Pi\backslash(\sqrt{X_u} \cup d)]}{X_u, \phi \to^d \psi \vdash^d [\Pi\backslash(\sqrt{X_u} \cup d)]}\,(\text{L}_\to)$$

and $\mathcal{D}_1$ be the derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{X_u \vdash \phi \to^d \psi \qquad \dfrac{\mathcal{D}}{X_u, \phi \to^d \psi \vdash^d [\Pi\backslash(\sqrt{X_u} \cup d)]}}{X_u \vdash^d [\Pi\backslash(\sqrt{X_u} \cup d)]}\,(\text{SD})}{X_u \vdash [\Pi\backslash\sqrt{X_u}]}\,(\text{Lemma 3.6})}{X_u \vdash [\sqrt{Y_u} \cup c_u]}\,(\text{R}_\vee)}{X_u \vdash [\sqrt{Y_u}], \bigvee_{p \in c_u} [p]}\,(\text{CP})$$

Note that the above derivation takes into account that $d \cup \Pi\backslash(\sqrt{X_u} \cup d) = \Pi\backslash\sqrt{X_u}$, which is true because, by an assumption of the lemma we are proving, $\sqrt{X_u} \cap d = \varnothing$. Let us also assume that $\mathcal{D}_2$ is the derivation

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\bot \vdash \bot}{\vdash \bot \to \bot}\,(\text{R}_\to) \qquad \dfrac{\bot \vdash}{[p], \bot \vdash}\,(\text{W})}{((\bot \to \bot) \to^p \bot \vdash^p)\ \ \forall p \in c_u}\,(\text{L}_\to)}{([p] \vdash^p)\ \ \forall p \in c_u}\,(\text{DEF})}{([p] \vdash^{c_u})\ \ \forall p \in c_u}\,(\text{W})}{\bigvee_{p \in c_u} [p] \vdash^{c_u}}\,(\text{L}_\vee)$$

Consider the derivation

$$\dfrac{\dfrac{\dfrac{\mathcal{D}_1}{X_u \vdash [\sqrt{Y_u}], \bigvee_{p\in c_u}[p]} \quad \dfrac{\mathcal{D}_2}{\bigvee_{p\in c_u}[p] \vdash^{c_u}}}{X_u \vdash^{c_u} [\sqrt{Y_u}]}\,(\text{CP})}{X_u \vdash^{c_u} Y_u}\,(\text{W})$$

This contradicts the consistency of triple u. Therefore, triple $(X_u \cup \{\psi\} \cup [d], \varnothing, [\Pi\backslash(\sqrt{X_u} \cup d)])$ is consistent. We will show that it is semi-saturated. Indeed,

$$\sqrt{X_u \cup \{\psi\} \cup [d] \cup \varnothing \cup \sqrt{[\Pi\backslash(\sqrt{X_u} \cup d)]}} \supseteq$$
$$\supseteq \sqrt{X_u} \cup d \cup (\Pi\backslash(\sqrt{X_u} \cup d)) = \Pi.$$

By Lemma 3.9, there is $X' \supseteq X_u \cup \{\psi\} \cup [d]$ such that triple $v = (X', \varnothing, [\Pi\backslash(\sqrt{X_u} \cup d)])$ is consistent and saturated. To show that $u \rightsquigarrow^d v$, we only need to establish that $d = \sqrt{X'}\backslash\sqrt{X}$. Indeed, by Lemma 3.6, $\sqrt{X'} \sqcup \varnothing \sqcup \sqrt{[\Pi\backslash(\sqrt{X_u} \cup d)]} = \Pi$. Hence, $\sqrt{X'} \sqcup (\Pi\backslash(\sqrt{X_u} \cup d)) = \Pi$. Thus, $\sqrt{X'} = \sqrt{X_u} \cup d$. Recall, however, that by the assumption of the lemma that we are proving, $\sqrt{X_u} \cap d = \varnothing$. Therefore, $d = \sqrt{X'}\backslash\sqrt{X}$. Finally, $X' \vdash \psi$ can be established through the derivation

$$\dfrac{\psi \vdash \psi}{X' \vdash \psi}\,(\text{W})$$

□

LEMMA 3.17. *For any $\phi \in \Phi$, any $n \geq 1$, and any chain of consistent triples:*

$$(X_1, c_1, Y_1) \rightsquigarrow^{d_1} (X_2, c_2, Y_2) \rightsquigarrow^{d_2} \dots$$
$$\dots \rightsquigarrow^{d_{n-2}} (X_{n-1}, c_{n-1}, Y_{n-1}) \rightsquigarrow^{d_{n-1}} (X_n, c_n, Y_n).$$

if $c_1 = d_1 \cup \dots \cup d_{n-1}$ and $X_n \vdash \phi$, then $\phi \notin Y_1$.

PROOF. Induction on n. If $n = 1$ and $X_1 \vdash \phi$, then we need to show that $\phi \notin Y_1$. Proof by contradiction. Let $\phi \in Y_1$. Then consider the derivation

$$\dfrac{X_1 \vdash \phi}{X_1 \vdash^{c_1} Y_1}\,(\text{W})$$

This contradicts the consistency of triple (X_1, c_1, Y_1).

Let $n > 1$. By Definition 3.14, $d_1 = c_1\backslash c_2$. Hence, $c_2 = d_2 \cup \dots \cup d_{n-1}$. Thus, by the induction hypothesis, $\phi \notin Y_2$. We are left to notice that, by Definition 3.14, $Y_1 \subseteq Y_2$. □

3.5. Canonical Frame

Definition 3.18. For any triple $u = (X, c, Y)$, let $A(u) = c \cup \sqrt{Y}$.

LEMMA 3.19. *For any two consistent semi-saturated triples u and v,*

(1) if $v \succeq u$, then $A(v) \subseteq A(u)$,
(2) if $u \rightsquigarrow^c v$ then $c = A(u)\backslash A(v)$.

PROOF. See Lemma 3.6. □

Definition 3.20. Let $\mathcal{F} = (S, A, \succeq, \rightsquigarrow)$, where S is the set of all consistent and saturated triples and A, $\succeq$ and $\rightsquigarrow$ are the function and two relations defined above.

LEMMA 3.21. *$\mathcal{F}$ is a frame.*

PROOF. See Lemma 3.11, Lemma 3.15, and Lemma 3.19. In addition, we need to show that for any consistent saturated triple $u = (X, c, Y)$ and any player $p \in A(u)$ there is a saturated consistent triple v such that $u \rightsquigarrow^p v$. We will use Lemma 3.16 to construct this v.

Note that $\sqrt{X} \cap \{p\} = \varnothing$ by Lemma 3.6 and Definition 3.18. We only need to present formulas ϕ and ψ such that $X \vdash \phi$ and $X \vdash^p \phi \to \psi$. Take $\phi = \psi = (\bot \to \bot)$ and notice that $X \vdash \phi$ follows from

$$\dfrac{\dfrac{\bot \vdash \bot}{X, \bot \vdash \bot}\,(\mathrm{W})}{X \vdash \bot \to \bot}\,(\mathrm{R}_\to)$$

and $X \vdash^p \phi \to \phi$ follows from

$$\dfrac{\dfrac{\phi \vdash \phi}{X, [p], \phi \vdash \phi}\,(\mathrm{W})}{X \vdash^p \phi \to \phi}\,(\mathrm{R}_\to)$$

□

3.6. Canonical Game

Definition 3.22. For any propositional variable A, we say that $(X, c, Y) \Vdash A$ if and only if $X \vdash A$.

LEMMA 3.23 (MAIN). *For any formula $\tau \in \Phi$ and any consistent saturated triple (X, c, Y),*

$$(X, c, Y) \Vdash \tau \textit{ if and only if } X \vdash \tau.$$

PROOF. Induction on structural complexity of formula τ.

(1) Assume that $\tau \equiv \bot$. It will be sufficient to show that $X \nvdash \bot$. Indeed, assume the opposite and consider the derivation

$$\dfrac{\dfrac{X \vdash \bot \qquad \bot \vdash}{X \vdash}\,(\mathrm{CP})}{X \vdash^c Y}\,(\mathrm{W})$$

This contradicts the consistency of triple (X, c, Y)

(2) For any propositional variable A, by Definition 3.22, $(X, c, Y) \Vdash A$ if and only if $X \vdash A$.

(3) Let τ be a conjunction of the form $\phi \wedge \psi$. If $(X, c, Y) \Vdash \phi \wedge \psi$, then $(X, c, Y) \Vdash \phi$ and $(X, c, Y) \Vdash \psi$. Hence, by the induction hypothesis, $X \vdash \phi$ and $X \vdash \psi$. By rule $(\mathrm{R}^1_\wedge)$, $X \vdash \phi \wedge \psi$.

On the other hand, suppose that $X \vdash \phi \wedge \psi$. First we will show that $X \vdash \phi$. Indeed,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\phi \vdash \phi}{X, \phi, \psi \vdash \phi}\,(\mathrm{W})}{X, \phi \wedge \psi \vdash \phi}\,(\mathrm{L}_\wedge)}{X \vdash \phi \wedge \psi \to \phi}\,(\mathrm{R}_\to) \qquad \dfrac{X \vdash \phi \wedge \psi \qquad \dfrac{\dfrac{\phi \vdash \phi}{X, \phi \vdash \phi}\,(\mathrm{W})}{X, \phi \wedge \psi \to \phi \vdash \phi}\,(\mathrm{L}_\to)}{X \vdash \phi}\,(\mathrm{CP})$$

Similarly, one can show that $X \vdash \psi$. Hence, by the induction hypothesis, $(X, c, Y) \Vdash \phi$ and $(X, c, Y) \Vdash \psi$. Therefore, $(X, c, Y) \Vdash \phi \wedge \psi$.

(4) Let τ be a disjunction of the form $\phi \vee \psi$. If $(X, c, Y) \Vdash \phi \vee \psi$, then $(X, c, Y) \Vdash \phi$ or $(X, c, Y) \Vdash \psi$. Without loss of generality, assume that $(X, c, Y) \Vdash \phi$. By the induction hypothesis, $X \vdash \phi$. Hence, by rule $(\mathrm{R}_\vee)$, $X \vdash \phi \vee \psi$.

Next, assume that $X \vdash \phi \vee \psi$. Since set X is saturated, either $\phi \in X$ or $\psi \in X$. Without loss of generality, assume the former. Consider the derivation

$$\frac{\phi \vdash \phi}{X \vdash \phi}\ (\mathrm{w})$$

Thus, $X \vdash \phi$. Hence, by the induction hypothesis, $(X, c, Y) \Vdash \phi$. Therefore, $(X, c, Y) \Vdash \phi \vee \psi$.

(5) Let formula τ be an implication of the form $\phi \to^d \psi$. First, assume that $X \vdash \phi \to^d \psi$. We will show that $(X, c, Y) \Vdash \phi \to^d \psi$. Consider any node $u = (X_u, c_u, Y_u)$ such that $u \succeq (X, c, Y)$, $u \Vdash \phi$, and $d \subseteq A(u)$. By the induction hypothesis, $u \Vdash \phi$ implies that $X_u \vdash \phi$. By Lemma 3.4, $d \subseteq A(u)$ implies that $d \cap \sqrt{X_u} = \varnothing$. Therefore, by Lemma 3.16, there is a triple $v = (X_v, c_v, Y_v) \in S$ such that $u \rightsquigarrow^d v$ and $X_v \vdash \psi$. By the induction hypothesis, $v \Vdash \psi$.
Next, we will assume that $X \nvdash \phi \to^d \psi$ and show that $(X, c, Y) \nVdash \phi \to^d \psi$. Indeed, by Lemma 3.13, there is a triple $u = (X_u, d, Y_u) \succeq (X, c, Y)$ such that $\phi \in X_u$ and $\psi \in Y_u$. By the induction hypothesis, $u \Vdash \phi$. We will now prove that $v \nVdash \psi$ for any chain $u = v_1 \rightsquigarrow^{d_1} v_2 \rightsquigarrow^{d_2} \cdots \rightsquigarrow^{d_n} v_n = v$ such that $d_1 \cup d_2 \cup \cdots \cup d_n = d$ and $n \geq 1$. Indeed, let $v = (X_v, c_v, Y_v)$. By Lemma 3.17, $\psi \in Y_u$ implies that $\psi \notin X_v$. By the induction hypothesis, $v \nVdash \psi$. Thus, $v \nVdash \psi$ for any v such that $u \rightsquigarrow^d_* v$. Therefore, $(X, c, Y) \nVdash \phi \to^d \psi$.

□

3.7. Final Steps

We are ready to finish the proof of Theorem 3.1. By our assumption, $\Gamma \nvdash^c \Delta$. Hence, (Γ, c, Δ) is a consistent triple. By Lemma 3.7 and Lemma 3.9, there is a consistent and saturated triple (Γ', c, Δ') such that $\Gamma \subseteq \Gamma'$ and $\Delta \subseteq \Delta'$.

We will show that $(\Gamma', c, \Delta') \nVdash \bigwedge \Gamma \to^c \bigvee \Delta$. Assume the opposite:

$$(\Gamma', c, \Delta') \Vdash \bigwedge \Gamma \to^c \bigvee \Delta. \tag{1}$$

Note that $\Gamma \subseteq \Gamma'$. Thus, by combination of an axiom and weakening rule, $\Gamma' \vdash \gamma$ for all $\gamma \in \Gamma$. Hence, by Lemma 3.23, $(\Gamma', c, \Delta') \Vdash \bigwedge \Gamma$. Then, by assumption (1), there is a node $v = (\Gamma_v, c_v, \Delta_v)$ such that $(\Gamma', c, \Delta') \rightsquigarrow^c v$ and $v \Vdash \bigvee \Delta$. Thus, $v \Vdash \delta_0$ for some $\delta_0 \in \Delta$. By Lemma 3.23, $\Gamma_v \vdash \delta_0$. By Lemma 3.17, $\delta_0 \notin \Delta'$. Hence, $\delta_0 \notin \Delta$. This contradicts the choice of δ_0. This concludes the proof of Theorem 3.1.

COROLLARY 3.24. *The set of all sequents provable in the calculus of cooperation is decidable.*

PROOF. Follows from the completeness with respect to the class of all *finite* games. □

4. MULTIPARTY PROTOCOLS AS GAMES

The main motivation for our development of the calculus of cooperation was our desire to find a natural formal framework for reasoning about privacy in multiparty computation protocols. In this section, we demonstrate how privacy properties in such protocols can be expressed through coalition-controlled implication in a certain game defined by the protocol. We then use the calculus of cooperation to formally verify privacy properties in several multiparty computation protocols.

Secure Multiparty Protocols.. Multiparty computation is an evaluation of a function of multiple inputs contributed by different parties. Informally, a set of collaborative

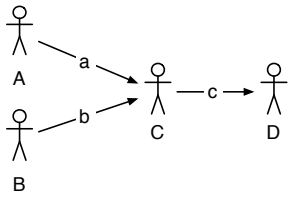

Fig. 3. Interaction Diagram for Conjunction and Exclusive Or Protocols

actions taken by the involved parties to arrive at the desired value is known as a *protocol* for the multiparty computation.

A protocol is executed over a set of *channels* connecting the parties. On these channels, messages are sent from one party to another, and sometimes from one party to the entire group. After interacting via messages sent on these channels, one or more of the parties arrives at the desired value. Informally, a protocol is considered *correct* if it leads to a successful evaluation of the desired function when all parties follow the protocol specification.

In each of the protocols we present and analyze in this article, we assume that all parties follow the protocol exactly as specified. In particular, we adopt the passive *honest-but-curious* model [4], where parties create and send messages exactly as directed by the protocol. However, we assume curiosity causes these parties to examine all information they have received, and to try to learn as much as they can about other parties' inputs. Additionally, we use a secure channel model, where it is assumed that each pair of parties is connected by a dedicated communication channel which is immune to eavesdroppers. In lieu of individual physical communication channels, it can be assumed that the secure channel is implemented using symmetric-key cryptography, as long as protection against adversaries with polynomially-bounded resources is sufficient.

The adjective *secure*, when applied to a multiparty computation protocol, captures the fact that the protocol achieves not only correctness, but some additional explicitly-stated security goals [10; 2]. One very common security goal, resiliency [6; 25; 4], involves the protocol's ability to complete the desired function evaluation despite the fact that a subset of the parties do not follow the protocol specification. Another common objective is privacy (see, for example, [16; 15]), where individual parties' input values do not leak to other parties or outsiders as a result of the protocol's execution. Our main intended application of the calculus of cooperation is privacy verification. However, it also can be used to reason about other properties of protocols.

We will use coalition-controlled implication to reason about protocols in a manner very similar to the way Hoare triples [13] are used to reason about programs. Different other logical calculi for proving [3; 7] and model checking [22; 27] general security properties have been suggested before. These works focus on low-level languages that can be used to state and verify different security properties of cryptographic protocols. The calculus of cooperation allows one to reason about privacy properties on a more abstract level that does not deal with key exchanges, encryption, or authentication issues.

4.1. Boolean Function Protocols

Conjunction Protocol.. We start with a very simple example of a four-party protocol executed on the graph in Figure 3. Under this protocol, parties A and B pick arbitrary boolean values a and b and send them to party C. Party C computes value c as the conjunction of a and b and sends the result to party D. Note that the behavior of party

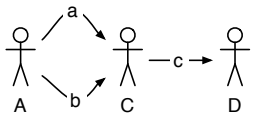

Fig. 4. Interaction Diagram for Modified Exclusive Or Protocol

C is completely deterministic, but parties A and B have choices in picking "arbitrary" values. We will consider the choices made by A and B as "moves" in a game. Clearly, parties A and B can cooperate to force any fixed boolean value of c. For instance, they can cooperate to achieve $c = 0$. In the language of the calculus of cooperation, this can be expressed as $\top \rightarrow^{A,B} c = 0$. Another property of the same protocol is that if the value of a is known to be 1, then party B can force the value of c to be 1. In our notation, this is: $a = 1 \rightarrow^{B} c = 1$.

Exclusive Or Protocol.. Our second example is also based on Figure 3, and is essentially the same protocol described above, but this time we assume that party C computes the exclusive or of bits a and b. It is easy to see that our two previous claims about the protocol: $\top \rightarrow^{A,B} c = 0$ and $a = 1 \rightarrow^{B} c = 1$ still hold. However, for the modified protocol something more interesting can be claimed: party B can force $c = 1$ no matter what the value of a is, as long as A makes the first move, and this move is known to B.[1] Expressed in the language of the calculus of cooperation, this is: $[A] \rightarrow^{B} c = 1$.

Modified Exclusive Or Protocol.. Let us now consider a modified exclusive or protocol (see Figure 4), in which bits a and b are both generated by the same party. We want to capture the idea that once bit a is sent, party A still can force condition $c = 0$ through an appropriate choice of b. For this, we will abandon our implicit assumption that players in the game are parties in the protocol. Instead, we will assume that "communication channels" (such as a and b) are the true players in the game. A protocol party could, thus, be viewed as a coalition of such channels. Using this "channels-as-players" approach, we can now state that $[a] \rightarrow^{b} c = 1$.

Of course, generally speaking, there may be some required dependency between two messages sent by the same party in a protocol. In that situation, once one of the messages is sent over the first channel, the range of available moves for the second channel is reduced.

Protocol Verification.. Multiparty protocols can specify message interdependencies that must be enforced by individual protocol parties. For example, $c = a \oplus b$ is such a specification for party C in the Exclusive Or Protocol. In this article, we distinguish between *local* and *global* properties of a multiparty protocol. A local protocol property is one that follows from the specification of the protocol for any single party; a global property is property of the protocol as a whole. For example, $a = c \rightarrow b = 0$ is a local property of the Modified Exclusive Or protocol, because it follows from $c = a \oplus b$. On the other hand, $\top \rightarrow^{a,b} c = 1$ is a global property of the protocol. *By protocol verification, we will mean the derivation of a global protocol property from local protocol properties of the protocol in the calculus of cooperation*. Below is an example of such a derivation:

[1]Note that a fundamental property of our notion of a game (implicit in Definition 2.3) is that once a party makes a move, that move becomes known to all other parties.

$$\dfrac{\dfrac{\top \vdash^{a} \top \qquad \dfrac{[a] \vdash^{b} b = \neg a \qquad \dfrac{b = \neg a \vdash c = 1}{b = \neg a, [b] \vdash c = 1}\,(\mathrm{W})}{\top, [a] \vdash^{b} c = 1}\,(\mathrm{CP})}{\top \vdash^{a,b} c = 1}\,(\mathrm{CP})}{\vdash \top \to^{a,b} c = 1}\,(\mathrm{R}_{\to})$$

where $\top \vdash^{a} \top$ is an axiom of the calculus, $[a] \vdash^{b} b = \neg a$ is a local condition for party A, and $b = \neg a \vdash c = 1$ is a local condition for party C.

Privacy Verification.. Our main intended application of the calculus of cooperation is proving *privacy* properties of multiparty protocols. For example, for the Exclusive Or protocol, knowledge of a does not reveal any information about c. More formally, this claim can be stated as follows, using the channels-as-players approach: any combination of values $\hat{a}$ and $\hat{c}$ of channels a and c that can occur in the protocol independently can also happen simultaneously. Using the language of games, if the coalition of all players in the game can force $a = \hat{a}$ and the same coalition can force $c = \hat{c}$, then this coalition can also force the conjunction $a = \hat{a} \wedge c = \hat{c}$:

$$\top \to^{a,b,c} a = \hat{a}, \top \to^{a,b,c} c = \hat{c} \quad \vdash \quad \top \to^{a,b,c} (a = \hat{a} \wedge c = \hat{c}).$$

In the statement above, we included all protocol channels, but of course only channels a and b have move choices in this particular protocol. Here is the proof of this statement in the calculus of cooperation:

$$\dfrac{\dfrac{\dfrac{\vdash^{a} a = \hat{a}}{\top \to^{a,b,c} a = \hat{a} \vdash^{a,c} a = \hat{a}}\,(\mathrm{W}) \qquad \dfrac{\dfrac{[a] \vdash^{b} b = a \oplus \hat{c}}{[a, c], \top \to^{a,b,c} c = \hat{c} \vdash^{b} b = a \oplus \hat{c}}\,(\mathrm{W}) \qquad b = a \oplus \hat{c} \vdash c = \hat{c}}{[a, c], \top \to^{a,b,c} c = \hat{c} \vdash^{b} c = \hat{c}}\,(\mathrm{CP})}{\top \to^{a,b,c} a = \hat{a}, \top \to^{a,b,c} c = \hat{c}, \top \vdash^{a,b,c} (a = \hat{a} \wedge c = \hat{c})}\,(\mathrm{R}^{1}_{\wedge})}{\top \to^{a,b,c} a = \hat{a}, \top \to^{a,b,c} c = \hat{c} \vdash \top \to^{a,b,c} (a = \hat{a} \wedge c = \hat{c})}\,(\mathrm{R}_{\to})$$

where statement $\vdash^{a} a = \hat{a}$ is a local condition at party A, statement $[a] \vdash^{b} b = a \oplus \hat{c}$ is a local condition at party B, and statement $b = a \oplus \hat{c} \vdash c = \hat{c}$ is a local condition at party C.

4.2. Dating Cryptographers Protocol

We close this article by using our logical calculus to verify privacy properties of a less trivial protocol. Though we have verified the privacy properties of Chaum's Dining Cryptographers protocol [5] using the calculus of cooperation, we found the verification too lengthy to serve as an example in this article. Instead, we demonstrate here how the calculus of cooperation can be applied to verify privacy properties of a protocol we designed to solve a problem which we call the Dating Cryptographers problem. It is a two-input version of a problem known in the literature as Anonymous Veto [11].

Description of the Problem.. Suppose that two individuals, known as Alice (A) and Bob (B), are trying to determine if they are in love with each other. Both parties fear face-to-face rejection, and therefore don't want to announce their feelings to the other person explicitly. Instead, they enlist a third party, a priest (P), to help. (If they determine that they are both in love, they will get married.) Let bits a and b, respectively, represent the feelings of Alice and Bob, where the appropriate bit has value 1 exactly when that individual is in love. However, in case one or both of them is not in love, Alice and Bob don't want to suffer the embarrassment of even allowing the priest to know the feelings of each party. With the help of the priest, they want to engage in a protocol which reveals only the conjunction of bits a and b, and (of course) any information that can be logically deduced from it.

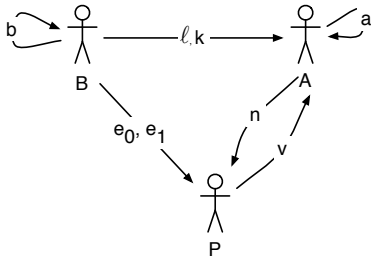

Fig. 5. Interaction Diagram for Dating Cryptographers Protocol

Description of the Protocol.. At the start of the protocol (see Figure 5), Bob knows his bit b and Alice knows her bit a. As before, we represent this internal state of each party with a self-loop indicating that the party sends this information to itself. Bob initiates the protocol by selecting a random key bit k, and a random label bit ℓ, which he sends to Alice. In addition, Bob prepares two bits e_0 and e_1, as follows. Value e_ℓ is computed as $b \oplus k$, where $\oplus$ denotes the exclusive-or operation, and the remaining value $e_{\neg\ell}$ is simply a randomly-selected bit. The value e_ℓ serves as a sort of *envelope* storing b; it looks like a random bit to anyone who does not know the key k which can unlock it. Both e-values – the envelope containing b and the one which is just a random bit – are forwarded to the priest. The idea is that Bob gives Alice the *name* of the e-value which contains b (that is, Bob gives her ℓ), and the key value k which would allow her to open the envelope. Alice then sends a bit n to the priest, requesting value e_n. Alice determines which value to request as follows. If $a = 1$, that is, if Alice is in love, then she requests the envelope named e_ℓ. She can then use the key value k to determine if Bob is too, by computing $e_\ell \oplus k$ to recover b. However, if Alice is not in love, she already knows that the result $a \wedge b = 0$; she doesn't need any information from the other parties. However, if she doesn't ask the priest for a value, the priest could reason that $a = 0$, and Alice's feelings will no longer be a secret. Therefore, when $a = 0$, Alice requests the e-value that is simply a randomly-selected value which is not related to b, the one named $e_{\neg\ell}$. The priest does not know which value contains useful information, and which contains a random value, since he is not given ℓ, and he does not know a. So the priest blindly forwards the requested value to Alice. Finally, though the channel is not displayed in Figure 5, Alice forwards the outcome $a \wedge b$ to Bob and the priest as the final step in the protocol.

First, we will show that in the dating cryptographers protocol, no information about values of a and b is revealed to the Priest. That is, any possible combination of values known to the Priest (e_0, e_1, and n), can happen together with any combination of possible values of a and b. This can be written using coalition-controlled implication as:

THEOREM 4.1.

$$\begin{array}{l} \top \rightarrow^{A,B,P} e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge n = \hat{n}, \\ \top \rightarrow^{A,B,P} a = \hat{a} \wedge b = \hat{b} \\ \vdash \\ \top \rightarrow^{A,B,P} (e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge n = \hat{n}) \wedge \\ \qquad \wedge (a = \hat{a} \wedge b = \hat{b}). \end{array}$$

In the statement of this theorem A, B, and C can be viewed as individual game players, or, as we discussed earlier, as coalitions of players (if we prefer to view channels as

game players). The proof of the above theorem could be written in the same formal form as earlier examples of verification. However, for clarity, we have inserted English comments into the proof.

PROOF. We begin by observing that according to the specification of the protocol, Bob can pick values e_0, e_1, ℓ, and b randomly. (This, of course, will determine the value of k.) In fact, if Alice has already made her move in the game, Bob can use the value of a in his choice of value of ℓ:

$$[A] \vdash^B e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge b = \hat{b} \wedge (\ell = 1 \oplus a \oplus \hat{n}). \tag{2}$$

Next, note that according to the specification of the protocol for Alice, $n = 1 \oplus \ell \oplus a$. In the other words,

$$\begin{array}{l} [B], \\ e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge b = \hat{b} \wedge (\ell = 1 \oplus a \oplus \hat{n}), \\ a = \hat{a} \\ \vdash \\ (e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge n = \hat{n}) \wedge (a = \hat{a} \wedge b = \hat{b}). \end{array}$$

The last sequent can be combined with (2) using the (CP) rule into

$$\begin{array}{l} [A], \\ a = \hat{a} \\ \vdash^B \\ (e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge n = \hat{n}) \wedge (a = \hat{a} \wedge b = \hat{b}). \end{array} \tag{3}$$

Turning again to the specification of local conditions for Alice, we observe that she is free in her choice of a. Thus, $\vdash^A a = \hat{a}$. This observation can be combined with (3) using rule (CP):

$$\vdash^{A,B} (e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge n = \hat{n}) \wedge (a = \hat{a} \wedge b = \hat{b}).$$

By the weakening rule (W),

$$\begin{array}{l} \top \\ \vdash^{A,B,P} \\ (e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge n = \hat{n}) \wedge (a = \hat{a} \wedge b = \hat{b}). \end{array}$$

By rule ($\mathrm{R}_{\rightarrow}$),

$$\begin{array}{l} \vdash \top \rightarrow^{A,B,P} (e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge n = \hat{n}) \wedge \\ \qquad\qquad \wedge (a = \hat{a} \wedge b = \hat{b}). \end{array}$$

Lastly, by the weakening rule (W),

$$\begin{array}{l} \top \rightarrow^{A,B,P} e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge n = \hat{n}, \\ \top \rightarrow^{A,B,P} a = \hat{a} \wedge b = \hat{b} \\ \vdash \\ \top \rightarrow^{A,B,P} (e_0 = \hat{e}_0 \wedge e_1 = \hat{e}_1 \wedge n = \hat{n}) \wedge \\ \qquad\qquad \wedge (a = \hat{a} \wedge b = \hat{b}). \end{array}$$

□

Our final example will show how the calculus of cooperation can be used to make and prove a *conditional* privacy statement. We will show that in the protocol for the dating cryptographers problem (if parties are assumed to be honest), *if Alice is not in love*, then she will not learn about Bob's feelings. Note that Alice only learns values of ℓ, v, and k. In the calculus of cooperation, we can state that $\hat{\ell}$, $\hat{v}$, $\hat{k}$ are values of ℓ, v, and k that can occur under condition $a = 0$, as follows:

$$a = 0 \to^{A,B,P} \ell = \hat{\ell} \wedge v = \hat{v} \wedge k = \hat{k}.$$

Similarly, $a = 0 \to^{A,B,P} b = \hat{b}$ says that $\hat{b}$ is a possible value of b that can occur under condition $a = 0$. The whole privacy statement is expressed in the following Theorem:

THEOREM 4.2.

$$\begin{array}{l} a = 0 \to^{A,B,P} \ell = \hat{\ell} \wedge v = \hat{v} \wedge k = \hat{k}, \\ a = 0 \to^{A,B,P} b = \hat{b} \\ \vdash \\ a = 0 \to^{A,B,P} \ell = \hat{\ell} \wedge v = \hat{v} \wedge k = \hat{k} \wedge b = \hat{b}. \end{array}$$

PROOF. The specification of the protocol for party P says that value v is equal to e_n (the content of n-th envelope). This can be written as

$$\begin{array}{l} n = \neg\ell \\ \ell = \hat{\ell} \wedge e_{\neg\ell} = \hat{v} \wedge k = \hat{k} \wedge b = \hat{b} \\ \vdash \\ \ell = \hat{\ell} \wedge v = \hat{v} \wedge k = \hat{k} \wedge b = \hat{b}. \end{array} \tag{4}$$

The specification of the protocol for party A says that if $a = 0$, then A should request the envelope different from envelope l:

$$a = 0 \vdash n = \neg\ell.$$

The last sequent can be combined with (4) by rule (CP) into

$$\begin{array}{l} a = 0, \\ \ell = \hat{\ell} \wedge e_{\neg\ell} = \hat{v} \wedge k = \hat{k} \wedge b = \hat{b} \\ \vdash \\ \ell = \hat{\ell} \wedge v = \hat{v} \wedge k = \hat{k} \wedge b = \hat{b}. \end{array}$$

By the weakening rule (W),

$$\begin{array}{l} [B], \\ a = 0, \\ \ell = \hat{\ell} \wedge e_{\neg\ell} = \hat{v} \wedge k = \hat{k} \wedge b = \hat{b} \\ \vdash \\ \ell = \hat{\ell} \wedge v = \hat{v} \wedge k = \hat{k} \wedge b = \hat{b}. \end{array} \tag{5}$$

Our next step is based on the observation that according to the specification of the protocol for B, this party can randomly pick values of ℓ, $e_{\neg\ell}$, k, and b. (Of course, once these values are picked, the value of e_ℓ is determined). Thus,

$$\vdash^B \ell = \hat{\ell} \wedge e_{\neg\ell} = \hat{v} \wedge k = \hat{k} \wedge b = \hat{b}.$$

The last statement in combination with (5), implies, by rule (CP), that

$$a = 0 \vdash^B \ell = \hat{\ell} \wedge v = \hat{v} \wedge k = \hat{k} \wedge b = \hat{b}. \tag{6}$$

By the weakening rule (W),

$$\begin{array}{l} a=0 \to^{A,B,P} \ell=\hat{\ell} \wedge v=\hat{v} \wedge k=\hat{k}, \\ a=0 \to^{A,B,P} b=\hat{b}, \\ a=0 \\ \vdash^{A,B,P} \\ \ell=\hat{\ell} \wedge v=\hat{v} \wedge k=\hat{k} \wedge b=\hat{b}. \end{array}$$

Therefore, by rule ($\mathrm{R}_{\to}$),

$$\begin{array}{l} a=0 \to^{A,B,P} \ell=\hat{\ell} \wedge v=\hat{v} \wedge k=\hat{k}, \\ a=0 \to^{A,B,P} b=\hat{b} \\ \vdash \\ a=0 \to^{A,B,P} \ell=\hat{\ell} \wedge v=\hat{v} \wedge k=\hat{k} \wedge b=\hat{b}. \end{array}$$

□

5. CONCLUSION

The article illustrates how an extension of the intuitionistic logic with labeled implication can be used to reason about a special class of games and how this type of reasoning can be employed for verification of privacy properties of multiparty protocols. The definition of the game that we gave was specifically targeted to protocol verification. It would be interesting to see if a similar technique could be applied to reason about outcomes of other types of games more commonly studied in game theory. Another unanswered question is possibility of cut elimination in the calculus of cooperation. This question appears to be a non-trivial one especially because the system has two cut-like rules: (CP) and (CUT), both of which will have to be eliminated simultaneously.

Acknowledgment

The authors would like to thank the anonymous reviewers for helpful comments.

REFERENCES

Rajeev Alur, Thomas A. Henzinger, and Orna Kupferman. Alternating-time temporal logic. *Journal of the ACM*, 49(5):672–713, 2002.

Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the of the Twentieth ACM Symposium on Theory of Computing*, pages 1–10. Association for Computing Machinery, 1988.

Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, 1990.

Ran Canetti, Uri Feige, Oded Goldreich, and Moni Naor. Adaptively secure multi-party computation. In *Proceedings of the Twenty-eighth ACM Symposium on Theory of Computing*, pages 639–648. Association for Computing Machinery, 1996.

David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

David Chaum, Claude Crepeau, and Ivan Damgard. Multiparty unconditionally secure protocols. In *Proceedings of the of the Twentieth ACM Symposium on Theory of Computing*, pages 11–19. Association for Computing Machinery, 1988.

Nancy Durgin, John Mitchell, and Dusko Pavlovic. A compositional logic for proving security properties of protocols. *Journal of Computer Security*, 11:677–721, 2003.

Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50(1):1–102, 1987.

Kurt Gödel. Eine interpretation des intuitionistischen aussagenkalkuls. *Ergebnisse Math. Kolloq.*, 4:39–40, 1933. English translation in: S. Feferman et al., editors, Kurt Gödel Collected Works, Vol. 1, pages 301303. Oxford University Press, Oxford, Clarendon Press, New York, 1986.

Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *Proceedings of the Nineteenth ACM Symposium on Theory of Computing*, pages 218–229. Association for Computing Machinery, 1987.

Feng Hao and Piotr Zielinski. A 2-round anonymous veto protocol. In *Proceedings of the Fourteenth Security Protocols Workshop*, 2006.

A. Heyting. Die formalen regeln der intuitionistischen logik. *Sitsungsberichte der Preussischen Akademic der Wissenschaften*, pages 42–56, 1930. English translation available in [18].

C.A.R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12:576–580, 1969.

Max Kanovich, T. Ban Kirigin, Vivek Nigam, and Andre Scedrov. Progressing collaborative systems. In *Proceedings of Workshop on Foundations of Security and Privacy (FCS-PrivMod)*, 2010.

Max Kanovich, Paul Rowe, and Andre Scedrov. Collaborative planning with privacy. In *Proceedings of the of the Twentieth IEEE Computer Security Foundations Symposium*, pages 265–278. IEEE Computer Society Press, 2007.

Yehuda Lindell and Benny Pinkas. Privacy preserving data mining. *Journal of Cryptology*, 15(3):177–206, 2002.

Paul Lorenzen. Ein dialogisches konstruktivitŁtskriterium. In *Infinitistic Methods. Proceedings of the Symposium on Foundations of Mathematics (Warszawa 1959)*, pages 193–200. Pergamon Press, 1961.

P. Mancosu, editor. *From Brouwer to Hilbert: The Debate on the Foundations of Mathematics in the 1920s*. Oxford University Press, 1998.

J. C. C. McKinsey and Alfred Tarski. Some theorems about the sentential calculi of Lewis and Heyting. *J. Symbolic Logic*, 13:1–15, 1948.

Grigori Mints. *A Short Introduction to Intuitionistic Logic*. Kluwer Academic, 2000.

Rohit Parikh. The logic of games and its applications. *Annals of Discrete Mathematics*, pages 111–140, 1985.

Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6:85–128, 1998.

M. Pauly. A modal logic for coalitional power in games. *Journal of Logic and Computation*, 12(1):149–166, 2002.

M. Pauly and R. Parikh. Game logic - an overview. *Studia Logica*, 75:165–182, 2003.

Tal Rabin and Michael Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the of the Twenty-first ACM Symposium on Theory of Computing*, pages 73–85. Association for Computing Machinery, 1989.

Wiebe van der Hoek and Michael Wooldridge. On the logic of cooperation and propositional control. *Artificial Intelligence*, 164(1-2):81–119, 2005.

Ron van der Meyden and Kaile Su. Symbolic model checking the knowledge of the dining cryptographers. In *Proceedings of the Seventeenth IEEE Computer Security Foundations Workshop*, pages 280–291, 2004.

Received July 2010; revised May 2011; accepted June 2011