An Independence Relation for Sets of Secrets

Sara Miner More and Pavel Naumov

Department of Mathematics and Computer Science
McDaniel College, Westminster, Maryland 21157, USA
{smore,pnaumov}@mcdaniel.edu

Abstract. A relation between two secrets, known in the literature as *nondeducibility*, was originally introduced by Sutherland. We extend it to a relation between sets of secrets that we call *independence*. This paper proposes a formal logical system for the independence relation, proves the completeness of the system with respect to a semantics of secrets, and shows that all axioms of the system are logically independent.

1 Introduction

In this paper we study interdependence between secrets. For example, if b_1, b_2, and b_3 are secrets with boolean values, then $b_1 \oplus b_2 \oplus b_3 = 0$ is an example of interdependence. If an interdependence between secrets is fixed and is publicly known, then knowledge of one secret may reveal something about the other secrets. In the above example, knowing the value of secret b_1 reveals whether or not secrets b_2 and b_3 are equal.

Let us now suppose that $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_k\}$ are two sets of secrets that are not interdependent. That is, knowledge of values $a_1, \dots, a_n$ reveals no information about values $b_1, \dots, b_k$. In this case we say that the sets of secrets A and B are *independent*. We will use the notation $A \parallel B$ to denote independence of A and B. If $n = k = 1$, then the independence predicate is essentially equivalent to the "no information flow" relation introduced by Sutherland [1].

In this work, we study properties of the independence predicate that are true regardless of the publicly-known interdependencies between secrets that may exist. For example, for any three secrets a, b, and c, if secrets a and b together reveal no information about secret c, then secret a alone will also reveal no information about secret c:

$$a, b \parallel c \to a \parallel c$$

A less obvious property of independence that can be expressed in propositional language and which is true regardless of the set of interdependencies that exist is:

$$a, b \parallel c \to (a \parallel b \to a \parallel b, c) \tag{1}$$

Below, we introduce a set of axioms for the independence predicate and prove the completeness of our logical system with respect to a semantics of secrets. In

particular, property (1) above will follow from these axioms. We call this logical system *Logic of Secrets*.

Our work is related to the study of information flow. Most of the literature in this area, however, studies information flow from the language-based [2, 3] or probabilistic [4, 5] points of view. Historically ([6], page 185), one of the first attempts to capture independence in our sense was undertaken by Goguen and Meseguer [7] through their notion of *noninterference* between two computing devices. Later, Sutherland [1] introduced his *no information flow* relation, which is essentially our independence relation restricted to single-element sets. This relation has since become known in the literature as *nondeducibility*. Cohen [8] presented a related notion called *strong dependence*. Unlike nondeducibility, however, the strong dependence relation is not symmetric. More recently, Halpern and O'Neill [4, 5] introduced f-secrecy to reason about multiparty protocols. In our notation, f-secrecy is a version of the nondeducibility predicate whose left or right side contains a certain function of the secret rather than the secret itself. However, all of these works focus on the application of the independence relation in the analysis of secure protocols, whereas the main focus of our work is on logical properties of the relation itself.

2 Semantics of Secrets

In this section we define a formal semantics for the independence relation.

Throughout the rest of this paper we assume that there is a fixed infinite set of "secret variables": $a, b, c, \ldots$. Intuitively, these variables can be viewed as names of secrets. A structure that serves as a model of the Logic of Secrets will be called a *protocol*. A protocol specifies names of the secret variables used, their possible values, and all publicly known interdependencies between secrets. The last of these is given as an explicit specification of all legitimate combinations of secret values, which we call "runs". Occasionally, we will refer to secret variables as just "secrets".

Definition 1. *A protocol is an arbitrary triple $\mathcal{P} = \langle \mathcal{S}, \mathcal{V}, \mathcal{R} \rangle$, where*

1. *$\mathcal{S}$ is a subset of the set of secret variables.*
2. *$\mathcal{V}$ is an arbitrary function that maps a secret variable $s \in \mathcal{S}$ into an arbitrary "set of values" of this secret $\mathcal{V}(s)$.*
3. *$\mathcal{R}$ is a set of functions, called runs of the protocol, such that each run r assigns a value $r(s) \in \mathcal{V}(s)$ to each secret variable $s \in \mathcal{S}$.*

For any protocol $\mathcal{P}$, by $\mathcal{R}(\mathcal{P})$ we mean the set of all runs of this protocol.

Definition 2. *A protocol $\mathcal{P} = \langle \mathcal{S}, \mathcal{V}, \mathcal{R} \rangle$ is finite if set $\mathcal{S}$ is finite and $\mathcal{V}(s)$ is finite for any $s \in \mathcal{S}$.*

In the following definition, and in the remainder of the paper, we write $f =_X g$ if $f(x) = g(x)$ for any $x \in X$.

Definition 3. *A set of secret variables $A \subseteq \mathcal{S}$ is independent from a set of secret variables $B \subseteq \mathcal{S}$ under protocol $\mathcal{P}$, if for any runs $r_1, r_2 \in \mathcal{R}(\mathcal{P})$ there is a run $r \in \mathcal{R}(\mathcal{P})$ such that $r =_A r_1$ and $r =_B r_2$.*

A special case of the independence predicate is the statement "the set of variables A is independent from the set of variables A". This statement, by definition, means that $r_1 =_A r_2$ for any runs $r_1, r_2 \in \mathcal{R}(\mathcal{P})$. In other words, for any $a \in A$, value $r(a)$ is the same for all runs $r \in \mathcal{R}(\mathcal{P})$. Thus, all secrets in A have fixed known values, and we will say that A is "public knowledge".

Definition 4. *The language of secrets consists of secret variables $a, b, c \ldots$, the independence predicate $\|$, implication $\rightarrow$, and false constant $\bot$. The set of formulas in this language is recursively defined as follows:*

1. *$\bot$ is a formula,*
2. *$X \parallel Y$ is a formula, for any two finite sets of secret variables X and Y,*
3. *if ϕ and ψ are formulas, then $\phi \rightarrow \psi$ is a formula.*

The language of secrets is similar to the universal fragment of propositional logic where $a_1, \ldots, a_n \parallel b_1, \ldots, b_k$ is a predicate of arity $n+k$. The difference, however, is that predicates in first order logic have a fixed arity, while our predicate $\|$ does not.

Definition 5. *We define a binary relation $\vDash$ between a protocol $\mathcal{P}$ and a formula ϕ by induction on the structural complexity of ϕ as follows:*

1. *$\mathcal{P} \nvDash \bot$,*
2. *$\mathcal{P} \vDash X \parallel Y$ if and only if X and Y are independent under $\mathcal{P}$,*
3. *$\mathcal{P} \vDash \phi \rightarrow \psi$ if and only if $\mathcal{P} \nvDash \phi$ or $\mathcal{P} \vDash \psi$.*

3 Logic of Secrets

Definition 6. *The Logic of Secrets is defined by the following axioms and inference rule:*

1. *All propositional tautologies in the language of secrets,*
2. *Empty Set Axiom: $\varnothing \parallel A$,*
3. *Monotonicity Axiom: $A, B \parallel C \rightarrow A \parallel C$,*
4. *Public Knowledge Axiom: $A \parallel A \rightarrow (B \parallel C \rightarrow A, B \parallel C)$,*
5. *Exchange Axiom: $A, B \parallel C, D \rightarrow (A \parallel B \rightarrow (D \parallel C \rightarrow A, C \parallel B, D))$,*
6. *Modus Ponens inference rule.*

Above and everywhere below, by A, B we mean $A \cup B$. As usual, we will write $X \vdash \phi$ if formula ϕ can be derived in the Logic of Secrets possibly using additional hypotheses from set X.

Lemma 1 (symmetry). *For any finite sets of secrets A and B,*

$$\vdash A \parallel B \rightarrow B \parallel A.$$

Proof. By Exchange Axiom, $\varnothing, A \parallel B, \varnothing \rightarrow (\varnothing \parallel A \rightarrow (\varnothing \parallel B \rightarrow \varnothing, B \parallel A, \varnothing))$. Taking into account Empty Set Axiom, $\varnothing A \parallel B, \varnothing \rightarrow \varnothing, B \parallel A, \varnothing$. Thus, $A \parallel B \rightarrow B \parallel A$.

As an example, let us now prove property (1) from these axioms. For convenience, we repeat the property below:

$$a, b \parallel c \rightarrow (a \parallel b \rightarrow a \parallel b, c)$$

By assuming $A = \{a\}$, $B = \{b\}$, $C = \varnothing$, and $D = \{c\}$ in Exchange Axiom, we get $a, b \parallel c \rightarrow (a \parallel b \rightarrow (c \parallel \varnothing \rightarrow a \parallel b, c))$. Thus, it will be sufficient to prove that $c \parallel \varnothing$. This, in turn, follows from Empty Set Axiom and Lemma 1.

Lemma 2. *If $X \vdash A \parallel B$, then $X \vdash A' \parallel B'$ for any $A' \subseteq A$ and $B' \subseteq B$.*

Proof. Follows from Monotonicity Axiom and Lemma 1.

4 Soundness

Theorem 1. *If $\vdash \phi$, then $\mathcal{P} \vDash \phi$ for any protocol $\mathcal{P}$.*

Proof. It will be sufficient to verify that $\mathcal{P} \vDash \phi$ for each axiom ϕ of the Logic of Secrets.

Empty Set Axiom. Consider any two runs $r_1, r_2 \in \mathcal{R}(\mathcal{P})$. Let $r = r_2$. It is easy to see that $r =_{\varnothing} r_1$ and $r =_A r_2$.

Monotonicity Axiom. Consider any two runs $r_1, r_2 \in \mathcal{R}(\mathcal{P})$. If $r =_{A,B} r_1$ and $r =_C r_2$, then $r =_A r_1$ and $r =_C r_2$.

Public Knowledge Axiom. Assume that $A \parallel A$ and $B \parallel C$. Consider any two runs $r_1, r_2 \in \mathcal{R}(\mathcal{P})$. By the assumption that $B \parallel C$, there is a run $r \in \mathcal{R}(\mathcal{P})$ such that $r =_B r_1$ and $r =_C r_2$. It will be sufficient to show that $r =_A r_1$. Indeed, by the assumption $A \parallel A$, there is a run $r' \in \mathcal{R}(\mathcal{P})$ such that $r =_A r' =_A r_1$. Therefore, $r =_A r_1$.

Exchange Axiom. Consider any two runs $r_1, r_2 \in \mathcal{R}(\mathcal{P})$. By the assumption that $A \parallel B$, there is a run $r_3 \in \mathcal{R}(\mathcal{P})$ such that $r_3 =_A r_1$ and $r_3 =_B r_2$. Since $D \parallel C$, there is a run $r_4 \in \mathcal{P}$ such that $r_4 =_D r_2$ and $r_4 =_C r_1$. Finally, by the assumption the $A, B \parallel C, D$, there is a run $r \in \mathcal{R}(\mathcal{P})$ such that $r =_{A,B} r_3$ and $r =_{C,D} r_4$. Thus, $r =_A r_3 =_A r_1$, $r =_C r_4 =_C r_1$, $r =_B r_3 =_B r_2$, and $r =_D r_4 =_D r_2$. Therefore, $r =_{A,C} r_1$ and $r =_{B,D} r_2$.

5 Completeness

Theorem 2. *If $\mathcal{P} \vDash \phi$ for any finite protocol $\mathcal{P}$, then $\vdash \phi$.*

The rest of the section contains the proof of this theorem. Assume that $\nvdash \phi$.

Definition 7. *Let $\mathcal{S}$ be the set of all secret variables appearing in ϕ.*

Definition 8. *Let Ψ be the minimal set that includes*

1. *all subformulas of ϕ and their negations,*
2. *$A \parallel B$ and $\neg(A \parallel B)$ for any $A, B \subseteq \mathcal{S}$*

Let X be a maximal consistent subset of Ψ that contains $\neg\phi$. We proceed now to define a finite protocol $\mathcal{P} = \langle \mathcal{S}, \mathcal{V}, \mathcal{R} \rangle$ such that $\mathcal{S}$ is the defined above set of secret variables. Later we will show that $\mathcal{P} \nvDash \phi$.

Definition 9. *For any secret $s \in \mathcal{S}$, we define set of values $\mathcal{V}(s)$ as follows:*

1. *if $X \vdash s \parallel s$, then $\mathcal{V}(s) = \{0\}$,*
2. *if $X \nvdash s \parallel s$, then $\mathcal{V}(s) = \{-1, 0, 1\}$.*

Next, we introduce terminology that allows us to define the set $\mathcal{R}$ of valid runs on protocol $\mathcal{P}$.

Definition 10. *A pair $(A, B) \in 2^{\mathcal{S}} \times 2^{\mathcal{S}}$ is called critical if*

1. *$X \nvdash A \parallel B$,*
2. *if $X \nvdash A' \parallel B'$, then $A = A'$ and $B = B'$, for any $A' \subseteq A$ and $B' \subseteq B$.*

Lemma 3. *For any pair $(A, B) \in 2^{\mathcal{S}} \times 2^{\mathcal{S}}$ such that $X \nvdash A \parallel B$, there is a critical pair (A', B') such that $A' \subseteq A$ and $B' \subseteq B$.*

Proof. Follows from finiteness of sets A and B.

Lemma 4. *If (C, D) is a critical pair, then $X \nvdash s \parallel s$ for any $s \in C \cup D$.*

Proof. Assume that $X \vdash s \parallel s$ for some $s \in C$. By Public Knowledge Axiom, $X \vdash C \backslash \{s\} \parallel D \rightarrow C \parallel D$. On the other hand, by the definition of critical pair, $X \nvdash C \parallel D$. Thus, $X \nvdash C \backslash \{s\} \parallel D$, which is a contradiction with the definition of critical pair. Therefore, $X \nvdash s \parallel s$. Case $s \in D$ is similar, due to Lemma 1.

Definition 11. *A run r is called void if there are sets of secrets C, D such that*

1. *pair (C, D) is critical,*
2. *$r(s) = 1$, for any $s \in C$,*
3. *$r(s) = -1$, for any $s \in D$.*

Definition 12. *Let $\mathcal{R}$ be the set of all runs that are not void.*

This concludes the definition of the finite protocol $\mathcal{P} = \langle \mathcal{S}, \mathcal{V}, \mathcal{R} \rangle$.

Lemma 5. *If $\mathcal{P} \vDash A \parallel B$, then $X \vdash A \parallel B$, for any $A, B \subseteq \mathcal{S}$.*

Proof. Assume that $X \nvdash A \parallel B$. By Lemma 3, there is a critical pair (A', B') such that $A' \subseteq A$ and $B' \subseteq B$. Consider runs r_+ and r_- such that for any secret s:

$$r_+(s) = \begin{cases} +1 & \text{if } X \nvdash s \parallel s \\ 0 & \text{otherwise} \end{cases}$$

$$r_-(s) = \begin{cases} -1 & \text{if } X \nvdash s \parallel s \\ 0 & \text{otherwise} \end{cases}$$

We will show that $r_+, r_- \in \mathcal{R}$. Let us start by showing that $r_+ \in \mathcal{R}$. Indeed, assume the opposite. Then there are $C, D \subseteq \mathcal{S}$ such that, taking into account Lemma 4 and Definition 11,

1. pair (C, D) is critical,
2. $+1 = r_+(s) = +1$, for any $s \in C$,
3. $+1 = r_+(s) = -1$, for any $s \in D$,

Note that the last statement implies that D is empty. Thus, by Empty Set Axiom, $\vdash D \parallel C$. By Lemma 1, $\vdash C \parallel D$. This contradicts the fact that (C, D) is a critical pair.

We now will prove that $r_- \in \mathcal{R}$. As in the previous case, assume the opposite. Hence, there are sets of secrets C, D such that, taking into account Lemma 4 and Definition 11,

1. pair (C, D) is critical,
2. $-1 = r_-(s) = +1$, for any $s \in C$,
3. $-1 = r_-(s) = -1$, for any $s \in D$,

Note that the second statement implies C is empty. Thus, by Empty Set Axiom, $\vdash C \parallel D$, which contradicts the fact that (C, D) is a critical pair.

We are ready to show that $\mathcal{P} \nvDash A \parallel B$. Indeed, by Definition 11, there is no run $r \in \mathcal{R}$ such that $\forall s \in A'\ (r(s) = +1)$ and $\forall s \in B'\ (r(s) = -1)$. Hence, there is no run $r \in \mathcal{R}$ such that $\forall s \in A'\ (r(s) = r_+(s))$ and $\forall s \in B'\ (r(s) = r_-(s))$. Finally, since $A' \subseteq A$ and $B' \subseteq B$, there is no run $r \in \mathcal{R}$ such that $\forall s \in A\ (r(s) = r_+(s))$ and $\forall s \in B\ (r(s) = r_-(s))$. Therefore, $\mathcal{P} \nvDash A \parallel B$.

Lemma 6. *If $X \vdash A \parallel B$, then $\mathcal{P} \vDash A \parallel B$.*

Proof. Assume that $X \vdash A \parallel B$. Consider any two runs $r_1, r_2 \in \mathcal{R}$. We need to find a run $r \in \mathcal{R}$ such that $\forall s \in A\ (r(s) = r_1(s))$ and $\forall s \in B\ (r(s) = r_2(s))$. Consider run r, defined as

$$r(s) = \begin{cases} r_1(s) & \text{if } s \in A \\ r_2(s) & \text{if } s \in B \\ 0 & \text{otherwise} \end{cases}$$

We will start by proving that run r is well-defined. For this, we need to show that $r_1(s) = r_2(s)$ if $s \in A \cap B$. Indeed, consider any $s \in A \cap B$. Note that

$X \vdash A \parallel B$. Thus, by Lemma 2, $X \vdash s \parallel s$. Hence, by Definition 9, $\mathcal{V}(s) = \{0\}$. Therefore, $r_1(s) = r_2(s)$.

We now only need to show that $r \in \mathcal{R}$. In other words, we need to show that run r is not void. Assume the opposite. Hence, there are sets of secrets $C, D \subseteq \mathcal{S}$ such that

1. (C, D) is a critical pair,
2. $r(s) = +1$, for any $s \in C$,
3. $r(s) = -1$, for any $s \in D$.

Note that $r(s) = 0$ for any $s \notin A \cup B$. Thus,

$$C = (C \cap A) \cup (C \cap B) \tag{2}$$

$$D = (D \cap A) \cup (D \cap B) \tag{3}$$

Case 1: $(C \cap A, D \cap A) = (C, D)$. Thus, $C \subseteq A$ and $D \subseteq A$. Hence $r_1(s) = r(s) = +1$, for any $s \in C$, and $r_1(s) = r(s) = -1$, for any $s \in D$. Therefore, r_1 is void, which is a contradiction.
Case 2: $(C \cap B, D \cap B) = (C, D)$. Similar to Case 1.
Case 3: $(C \cap A, D \cap A) \neq (C, D)$ and $(C \cap B, D \cap B) \neq (C, D)$. Since (C, D) is a critical pair, these two statements imply that

$$X \vdash C \cap A \parallel D \cap A \tag{4}$$

and

$$X \vdash C \cap B \parallel D \cap B. \tag{5}$$

Note that by the assumption of the theorem, $X \vdash A \parallel B$. Thus, by Lemma 2,

$$X \vdash C \cap A, D \cap A \parallel C \cap B, D \cap B$$

By Exchange Axiom, using (4), (5), and Lemma 1,

$$X \vdash C \cap A, C \cap B \parallel D \cap A, D \cap B$$

Taking in to account (2) and (3), $X \vdash C \parallel D$, which contradicts the fact that the pair (C, D) is critical.

Lemma 7. *For any $\psi \in \Psi$, $\mathcal{P} \vDash \psi$ if and only if $\psi \in X$.*

Proof. We use induction on the structural complexity of ψ.

1. If $\psi \equiv \bot$, then $\mathcal{P} \nVdash \bot$ and, since X is consistent, $X \nvdash \bot$.
2. If $\psi \equiv \psi_1 \rightarrow \psi_2$, then $\mathcal{P} \nVdash \psi$ if and only if $\mathcal{P} \vDash \psi_1$ and $\mathcal{P} \nvDash \psi_2$. Thus, by the induction hypothesis, $\mathcal{P} \nVdash \psi$ if and only if $X \vdash \psi_1$ and $X \nvdash \psi_2$. Hence, since X is a maximal and consistent set of formulas, $\mathcal{P} \vDash \psi$ if and only if $\psi \in X$.
3. $\psi \equiv A \parallel B$. See Lemma 5 and Lemma 6.

Finally, we note that Theorem 2 follows from the previous lemma.

6 Axiom Independence

In this section we will prove that each of the axioms of the Logic of Secrets is independent from the other axioms. This is done by defining non-standard semantics for the independence predicate.

Theorem 3. *Empty Set Axiom is not provable from the other axioms.*

Proof. Consider a new semantics of the independence predicate under which $A \parallel B$ is false for all sets of secret variables A and B. Under this non-standard semantics, Empty Set Axiom is false, but Monotonicity, Public Knowledge, and Exchange Axioms are true. Therefore, Empty Set Axiom is independent from the other axioms.

Theorem 4. *Monotonicity Axiom is not provable from the other axioms.*

Proof. Fix an arbitrary secret variable s_0. Consider a new semantics of the independence predicate under which $A \parallel B$ is true if and only if at least one of the following conditions is true:

1. A is empty,
2. B is empty,
3. $s_0 \in A \cup B$.

Let us show that this definition satisfies Empty Set, Public Knowledge, and Exchange axioms, and does not satisfy Monotonicity axiom.

Empty Set Axiom. $A \parallel \varnothing$ because $\varnothing$ is an empty set.

Public Knowledge Axiom. Assume that $A \parallel A$ and $B \parallel C$. The first of these statements implies that either A is empty or $s_0 \in A$. If A is empty, then $A, B = B$. Hence, $B \parallel C$ implies $A, B \parallel C$. Suppose $s_0 \in A$. Thus, $s_0 \in A \cup B \cup C$, and therefore, $A, B \parallel C$.

Exchange Axiom. Assume that $A, B \parallel C, D$ as well as $A \parallel B$ and $D \parallel C$. If $s_0 \in A \cup B \cup C \cup D$, then $A, C \parallel B, D$ is true. Suppose that $s \notin A \cup B \cup C \cup D$. Thus, $A \parallel B$ and $D \parallel C$ imply that one set out of A and B and one set out of C and D are empty. If empty sets are A and C or B and D, then $A, C \parallel B, D$ is true. So, it will be sufficient to consider the case when A and D are empty or B and C are empty.

1. First, consider the case where A and D are empty. Assumption $A, B \parallel C, D$ implies that $B \parallel C$. Hence, either B or C is empty. Therefore, either $B \cup D$ or $A \cup C$ is empty. Thus, $A, C \parallel B, D$.
2. Second, consider the case where B and C are empty. Assumption $A, B \parallel C, D$ implies that $A \parallel D$. Hence, either A or D is empty. Therefore, either $A \cup C$ or $B \cup D$ is empty. Thus, $A, C \parallel B, D$.

Monotonicity Axiom. Let t and u be secret variables different from variable s_0. Consider any protocol $\mathcal{P}$ and sets $A = \{t\}$, $B = \{s_0\}$, and $C = \{u\}$. By definition, $\mathcal{P} \vDash A, B \parallel C$, but $\mathcal{P} \nvDash A \parallel C$.

Theorem 5. *Public Knowledge Axiom is not provable from the other axioms.*

Proof. Consider a new semantics of the independence predicate under which secret variables are interpreted as nodes of a certain undirected graph. Independence predicate $A \parallel B$ is true if and only if there is *no* crossing edge that connects a node from set A with a node from set B. It is easy to see that Empty Set Axiom and Monotonicity Axiom are true under this interpretation.

Exchange Axiom. Suppose that $A, B \parallel C, D$, as well as $A \parallel B$ and $D \parallel C$. We will need to show that $A, C \parallel B, D$. Assume the opposite: there is a crossing edge e from $A \cup C$ to $B \cup D$. There are four cases to consider: (a) if e goes from A to B, then $A \parallel B$ is false, (b) if e goes from A to D, then $A, B \parallel C, D$ is false, (c) if e goes from C to B, then $A, B \parallel C, D$ is false, (d) if e goes from C to D, then $D \parallel C$ is false.

Public Knowledge Axiom. Finally, we will show that there is a graph G and sets of nodes A, B, and C, for which $A \parallel A \rightarrow (B \parallel C \rightarrow A, B \parallel C)$ is false. Let graph G consist of only three nodes a, b, and c. Assume that (a, c) is the only edge of this graph. Note that $a \parallel a$ and $b \parallel b$ are true, but $a, b \parallel c$ is false.

Theorem 6. *Secret Exchange Axiom is not provable from the other axioms.*

Proof. Consider a non-standard semantics for independence predicate under which $A \parallel B$ stands for "set A is empty". It is easy to see that Empty Set Axiom, Monotonicity Axiom, and Public Knowledge Axiom are true under this interpretation. At the same time, if sets A, B, and D are empty and set C is not, then Exchange Axiom is false.

7 Conclusion

In this paper, we have introduced a logical system that describes properties of independence between two sets of secret variables. Naturally, one can ask about an independence predicate for three or more sets of secret variables. For example, an independence predicate for three sets A, B, and C could be defined as

$$A \parallel B \parallel C \quad \Longleftrightarrow \quad \forall r_1, r_2, r_3 \; \exists r \; (r =_A r_1 \wedge r =_B r_2 \wedge r =_C r_3).$$

We conclude with the observation that independence predicates that have more than two sets of arguments can be expressed through the two-argument independence predicate studied in this paper. For example, it can be shown that $A \parallel B \parallel C$ is logically equivalent to the conjunction $(A \parallel B) \wedge (A, B \parallel C)$.

References

1. Sutherland, D.: A model of information. In: Proceedings of Ninth National Computer Security Conference. (1986) 175–183
2. Sabelfeld, A., Myers, A.C.: Language-based information-flow security. IEEE Journal on Selected Areas in Communications **21**(1) (2003) 5–19

3. Amtoft, T., Banerjee, A.: A logic for information flow analysis with an application to forward slicing of simple imperative programs. Sci. Comput. Program. **64**(1) (2007) 3–28
4. Halpern, J., O'Neill, K.: Secrecy in multiagent systems. In: Proceedings of the Fifteenth IEEE Computer Security Foundations Workshop. (2002) 32–46
5. Halpern, J.Y., O'Neill, K.R.: Secrecy in multiagent systems. ACM Trans. Inf. Syst. Secur. **12**(1) (2008) 1–47
6. MacKenzie, D.: Mechanizing Proof: Computing, Risk, and Trust. MIT Press (2004)
7. Goguen, J.A., Meseguer, J.: Security policies and security models. In: Proceedings of IEEE Symposium on Security and Privacy. (1982) 11–20
8. Cohen, E.: Information transmission in computational systems. In: Proceedings of Sixth ACM Symposium on Operating Systems Principles, Association for Computing Machinery (1977) 113–139