Sara Miner More
Pavel Naumov

An Independence Relation for Sets of Secrets

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.

Keywords: information flow, nondeducibility, formal system

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. Note however that it does not reveal the exact value of either b_2 or b_1. Thus, interdependence is not the same as functional dependence.

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, the 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 use the notation $A \parallel B$ to denote the 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 [11].

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, 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*.

The word *independence* is also used in probability theory to describe two events A and B such that $P(A \cap B) = P(A) \cdot P(B)$. The complete axiomatization for a relation capturing independence in the probabilistic sense was given by Geiger, Paz and Pearl in [3]. Surprisingly, their logical system is essentially equivalent to ours. We compare these two systems in the conclusion.

Our work is also related to the study of information flow. Most of the literature in this area, however, studies information flow from the language-based [10, 1] or probabilistic [6] points of view. Historically ([7], page 185), one of the first attempts to capture independence in our sense was undertaken by Goguen and Meseguer [4] through their notion of *noninterference* between two computing devices. Later, Sutherland [11] 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 [2] presented a related notion called *strong dependence*. Unlike nondeducibility, however, the strong dependence relation is not symmetric. More recently, Halpern and O'Neill [6] 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.

A preliminary version of this work was presented at [8]. In a related work [9], we consider an independence relation between single secrets distributed over a collaboration network with a fixed topology.

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 the 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 all $s \in \mathcal{S}$.*

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

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 all 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 all 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. $\mathcal{P} \vDash \phi \to \psi$ *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:* $A, B \parallel C \to A \parallel C$,
4. *Public Knowledge Axiom:* $A \parallel A \to (B \parallel C \to A, B \parallel C)$,
5. *Exchange Axiom:* $A, B \parallel C, D \to (A \parallel B \to (D \parallel C \to A, C \parallel B, D))$,
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 all finite sets of secrets* A *and* B,

$$\vdash A \parallel B \to B \parallel A.$$

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

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

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

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

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

Proof. This follows from the Monotonicity Axiom and Lemma 1. ∎

4. Soundness

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

PROOF. It will be sufficient to verify that $\mathcal{P} \models \phi$ for each axiom ϕ of the Logic of Secrets. Soundness of the Modus Ponens rule is trivial.

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 $\mathcal{P} \models \phi$ for all finite protocols $\mathcal{P}$, then $\vdash \phi$.*

The rest of the section contains the proof of this theorem. Assume that $\nvdash \phi$. We will construct a protocol $\mathcal{P}$ such that $\mathcal{P} \not\models \phi$. The key to this construction is the notion of a critical set given in Definition 10. We later use critical sets to distinguish valid runs from all other combinations of values of secrets.

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

DEFINITION 8. *Let Ψ be the least set that includes*

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

Let X be a maximal consistent subset of Ψ that contains $\phi \to \bot$. As usual, by consistency we mean that $X \nvdash \bot$. 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 $\mathcal{P} \not\models \phi$.

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 all $A' \subseteq A$ and $B' \subseteq B$.*

For example, suppose $X \nvdash a \parallel b, c$, but $X \vdash a \parallel b$ and $X \vdash a \parallel c$. Note that by the Empty Set Axiom we also have $X \vdash \varnothing \parallel b, c$. Therefore, $(\{a\}, \{b, c\})$ is a critical pair for set X.

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. This follows from the finiteness of sets A and B. Indeed, start with pair (A, B) and remove elements from sets A and B as long as condition $X \nvdash A \parallel B$ is satisfied. ∎

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

Proof. Assume that $X \vdash s \parallel s$ for some $s \in C$. By the Public Knowledge Axiom, $X \vdash C \backslash \{s\} \parallel D \to C \parallel D$. 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 all $s \in C$,*
3. *$r(s) = -1$, for all $s \in D$.*

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 $\mathcal{P} \models A \parallel B$, then $X \vdash A \parallel B$, for all $A, B \subseteq \mathcal{S}$.*

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 all $s \in C$,
3. $+1 = r_+(s) = -1$, for all $s \in D$.

Note that the last statement implies that D is empty. Thus, by the 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 all $s \in C$,
3. $-1 = r_-(s) = -1$, for all $s \in D$.

Note that the second statement implies C is empty. Thus, by the 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 a 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 all $s \in C$,
3. $r(s) = -1$, for all $s \in D$.

Note that $r(s) = 0$ for all $s \notin A \cup B$. Thus, sets C and D must be subsets of $A \cup B$. In other words,

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

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

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 all $s \in C$, and $r_1(s) = r(s) = -1$, for all $s \in D$. 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 $(C \cap B, D \cap B) \neq (C, D)$. Hence, either $C \cap A$ is a proper subset of C or $D \cap A$ is a proper subset of D. Since (C, D) is a critical pair,

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

Similarly, $(C \cap B, D \cap B) \neq (C, D)$ implies that either $C \cap B$ is a proper subset of C or $D \cap B$ is a proper subset of D. Again due to the fact that (C, D) is a critical pair,

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

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

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

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

LEMMA 7. *For all $\psi \in \Psi$, $\mathcal{P} \vDash \psi$ if and only if $X \vdash \psi$.*

PROOF. We use induction on the structural complexity of ψ and rely on the fact that X is a maximal consistent set of formulas.

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 consistent set of formulas, $\mathcal{P} \vDash \psi$ if and only if $X \vdash \psi$.
3. $\psi \equiv A \parallel B$. See Lemma 5 and Lemma 6.

■

Finally, we note that Lemma 7 implies that $\mathcal{P} \nvDash \phi$ because, by our original assumption, $X \nvdash \phi$. This completes the proof of Theorem 2.

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. *The 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, the Empty Set Axiom is false, but the Monotonicity, Public Knowledge, and Exchange Axioms are true. Therefore, the Empty Set Axiom is independent from the other axioms. ■

THEOREM 4. *The 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 the Empty Set, Public Knowledge, and Exchange Axioms, and does not satisfy the Monotonicity Axiom.

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

The 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, $A, B \parallel C$.

The 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.

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, so either $B \cup D$ or $A \cup C$ is empty. Thus, $A, C \parallel B, D$. The case where B and C are empty is similar.

The 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. *The 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 the Empty Set and Monotonicity Axioms are true under this interpretation.

The Exchange Axiom. Suppose that $A, B \parallel C, D$, and $A \parallel B$, as well as $D \parallel C$. 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.

The 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 in this graph. Note that $a \parallel a$ and $b \parallel b$ are true, but $a, b \parallel c$ is false. ■

THEOREM 6. *The 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 the Empty Set, Monotonicity, and Public Knowledge Axioms are true under this interpretation. At the same time, if sets A, B, and D are empty and set C is not, then the Exchange Axiom is false. ■

7. Conclusions

7.1. Probabilistic Interpretation

As mentioned in the introduction, Geiger, Paz, and Pearl [3] developed a complete logical system for a relation describing probabilistic independence. In their system, variables are interpreted as events and $a_1, \ldots, a_n \parallel b_1, \ldots, b_n$ as the statement that events $a_1, \ldots, a_n$ are probabilistically independent from events $b_1, \ldots, b_n$. Their system and our system are essentially equivalent, with two technical exceptions. First, they explicitly assume that the same event cannot appear on both sides of the independence predicate. Thus, their language lacks a notion equivalent to our "public knowledge" and, as a result, their system does not include our Public Knowledge Axiom. If one modified their system by allowing the same event to appear on both sides of the independence predicate, than $a \parallel a$ would have the meaning "the probability of event a is either 0 or 1". Our Public Knowledge Axiom is clearly valid under this interpretation.

The second difference between the system of Geiger, Paz and Pearl and our system is that they use a weaker form of our Exchange Axiom:

$$A, B \parallel C \rightarrow (A \parallel B \rightarrow A \parallel B, C). \tag{6}$$

Our Exchange Axiom does not follow from principle (6) alone, but our axiom does follow from (6), our Monotonicity Axiom, and a Symmetry Axiom

(which is Lemma 1 in our system and a stand-alone new axiom in theirs). To see this, assume $A, B \parallel C, D$ and $A \parallel B$, as well as $D \parallel C$. We will prove that $A, C \parallel B, D$. First, by the Monotonicity Axiom, $A, B \parallel C, D$ implies $B \parallel C, D$. By the Symmetry Axiom, $C, D \parallel B$. From assumption $D \parallel C$, the Symmetry Axiom, and (6),

$$C \parallel D, B. \tag{7}$$

Next, let us return to assumption $A, B \parallel C, D$. Taking into account $A \parallel B$ and (6), we have $A \parallel B, C, D$. By Symmetry, $B, C, D \parallel A$. Again by (6), and using (7), we have $B, D \parallel A, C$. Finally, by Symmetry, $A, C \parallel B, D$.

7.2. Multiple Independence

In this paper, we 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 as is done for single secrets in [9]. For example, an independence predicate for three sets A, B, and C could be defined as

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

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

Acknowledgements. The authors would like to thank Joe Halpern for pointing out the connection to Geiger, Paz, and Pearl [3], and the anonymous reviewers for their comments.

References

[1] Amtoft, Torben, and Anindya Banerjee, 'A logic for information flow analysis with an application to forward slicing of simple imperative programs', *Sci. Comput. Program.*, 64 (2007), 1, 3–28.

[2] Cohen, Ellis, 'Information transmission in computational systems', in *Proceedings of Sixth ACM Symposium on Operating Systems Principles*, Association for Computing Machinery, 1977, pp. 113–139.

[3] Geiger, Dan, Azaria Paz, and Judea Pearl, 'Axioms and algorithms for inferences involving probabilistic independence', *Inform. and Comput.*, 91 (1991), 1, 128–141.

[4] Goguen, Joseph A, and José Meseguer, 'Security policies and security models', in *Proceedings of IEEE Symposium on Security and Privacy*, 1982, pp. 11–20.

[5] Halpern, Joseph Y., and Kevin R. O'Neill, 'Secrecy in multiagent systems', in *Proceedings of the Fifteenth IEEE Computer Security Foundations Workshop*, 2002, pp. 32–46.

[6] Halpern, Joseph Y., and Kevin R. O'Neill, 'Secrecy in multiagent systems', *ACM Trans. Inf. Syst. Secur.*, 12 (2008), 1, 1–47. (originally appeared as [5]).

[7] MacKenzie, Donald, *Mechanizing Proof: Computing, Risk, and Trust*, MIT Press, 2004.

[8] Miner More, Sara, and Pavel Naumov, 'An independence relation for sets of secrets', in H. Ono, M. Kanazawa, and R. de Queiroz, (eds.), *Proceedings of 16th Workshop on Logic, Language, Information and Computation (Tokyo, 2009), LNAI 5514*, Springer, 2009, pp. 296–304.

[9] Miner More, Sara, and Pavel Naumov, 'On interdependence of secrets in collaboration networks', in *Proceedings of 12th Conference on Theoretical Aspects of Rationality and Knowledge (Stanford University, 2009)*, 2009, pp. 208–217.

[10] Sabelfeld, Andrei, and Andrew C. Myers, 'Language-based information-flow security', *IEEE Journal on Selected Areas in Communications*, 21 (2003), 1, 5–19.

[11] Sutherland, David, 'A model of information', in *Proceedings of Ninth National Computer Security Conference*, 1986, pp. 175–183.

Sara Miner More
Department of Mathematics and Computer Science
McDaniel College
Westminster, Maryland 21157, USA
smore@mcdaniel.edu

Pavel Naumov
Department of Mathematics and Computer Science
McDaniel College
Westminster, Maryland 21157, USA
pnaumov@mcdaniel.edu