Proceedings of the Twelfth International Conference on the Principles of Knowledge Representation and Reasoning (KR 2010)

Independence and Functional Dependence Relations on Secrets

Robert Kelvey and **Sara Miner More** and **Pavel Naumov** and **Benjamin Sapp**

Department of Mathematics and Computer Science
McDaniel College, Westminster, Maryland 21157, USA

{*rjk002,smore,pnaumov,brs004*}*@mcdaniel.edu*

Abstract

We study logical principles connecting two relations: independence, which is known as nondeducibility in the study of information flow, and functional dependence. Two different epistemic interpretations for these relations are discussed: semantics of secrets and probabilistic semantics. A logical system sound and complete with respect to both of these semantics is introduced and is shown to be decidable.

Introduction

In this paper, we study the properties of interdependencies between pieces of information. We call these pieces *secrets* to emphasize the fact that they might be unknown to some parties.

One of the simplest relations between two secrets is *functional dependency*. We denote it as $a \rhd b$. It means that the value of secret a reveals the value of secret b. This relation is reflexive and transitive. A more general and less trivial form of functional dependency is functional dependency between sets of secrets. If A and B are two sets of secrets, then $A \rhd B$ means that, together, the values of all secrets in A reveal the values of all secrets in B. Armstrong (1974) presented the following sound and complete axiomatization of this relation:

1. *Reflexivity*: $A \rhd B$, if $A \supseteq B$,
2. *Augmentation*: $A \rhd B \to A, C \rhd B, C$,
3. *Transitivity*: $A \rhd B \to (B \rhd C \to A \rhd C)$,

where here and everywhere below A, B denotes the union of sets A and B. The above axioms are known in database literature as Armstrong's axioms (Garcia-Molina, Ullman, and Widom 2009, p. 81). Beeri, Fagin, and Howard (1977) suggested a variation of Armstrong's axioms that describe properties of multi-valued dependency.

Not all dependencies between two secrets are functional. For example, if secret a is a pair $\langle x, y\rangle$ and secret b is a pair $\langle y, z\rangle$, then there is an interdependency between these secrets in the sense that not every value of secret a is compatible with every value of secret b. However, neither $a \rhd b$ nor $b \rhd a$ is necessarily true. If there is no interdependency between two secrets, then we will say that the two secrets are *independent*. In other words, secrets a and b are independent if any possible value of secret a is compatible with any possible value of secret b. We denote this relation between two secrets by $a \parallel b$. This relation was introduced by Sutherland (1986) and is also known as *nondeducibility* in the study of information flow. Halpern and O'Neill (2008) proposed a closely related notion called f-secrecy. More and Naumov (2009b) gave a complete axiomatization of the independence relation if secrets are generated over a collaboration network with a fixed topology.

Like functional dependence, independence also can be generalized to relate two sets of secrets. If A and B are two such sets, then $A \parallel B$ means that any consistent combination of values of secrets in A is compatible with any consistent combination of values of secrets in B. Note that "consistent combination" is an important condition here since some interdependency may exist between secrets in set A even while the entire set of secrets A is independent from the secrets in set B. A sound and complete axiomatization of this independence relation between sets was given by More and Naumov (2009a):

1. *Empty Set*: $\varnothing \parallel A$,
2. *Monotonicity*: $A, B \parallel C \to A \parallel C$,
3. *Symmetry*: $A \parallel B \to B \parallel A$,
4. *Public Knowledge*: $A \parallel A \to (B \parallel C \to A, B \parallel C)$,
5. *Exchange*: $A, B \parallel C \to (A \parallel B \to A \parallel B, C)$.

Essentially the same axioms were shown by Geiger, Paz, and Pearl (1991) to provide a complete axiomatization of the independence relation between random variables in probability theory.

In this paper, we study properties that connect the independence $\parallel$ and functional dependence $\rhd$ relations. An example of such a property, which we call the Substitution Axiom, is $a \parallel b \to (b \rhd c \to a \parallel c)$. Its soundness with respect to a formally-defined semantics of secrets is shown in Theorem 1.

The main focus of this work is the independence and functional dependence relations between *single* secrets, not *sets* of secrets, as the single-secret setting already provides a non-trivial system of properties. We describe a sound and complete axiomatization of these properties, prove the decidability of our logical system, and establish the indepen-

dence (in the standard logical sense) of its axioms. We also prove the completeness of this system with respect to probabilistic event semantics in the spirit of Geiger, Paz, and Pearl (1991). In the conclusion, we discuss the extension of this work to independence and functional dependence relations defined on *sets* of secrets.

Language of Secrets

The language of secrets contains an infinite list of variables $a, b, c, \ldots$, that we will call *secret variables*. Atomic formulas in the language of secrets are $a \parallel b$ and $a \rhd b$, where a and b are any two secret variables. An arbitrary formula in the language of secrets is a boolean combination of atomic formulas. We will assume that the only primitive propositional connectives in the language are $\rightarrow$ and $\bot$. Of course, the other boolean operations can be expressed through these two connectives.

Semantics of Secrets

We define semantics of secrets in terms of *protocols* and *runs*. A protocol defines a domain for each secret variable. However, not all combinations of value assignments to secrets are necessarily valid, since interdependencies between secrets may exist. Thus, a protocol also defines the set of legitimate combinations of assignments, which we call runs. A protocol serves as a model for the logic of secrets.

Definition 1 *A protocol is a pair $\langle \mathcal{D}, \mathcal{R} \rangle$, where*

1. *$\mathcal{D}$ is a function that assigns to each secret variable a set (the domain of the secret variable),*
2. *$\mathcal{R}$ is a set of functions, called "runs", such that each function r in this set maps each secret variable a into an element $r(a)$ of $\mathcal{D}(a)$.*

Next, we present formal definitions of the independence and functional dependence relations that were described in the introduction.

Definition 2 *For any protocol $\mathcal{P} = \langle \mathcal{D}, \mathcal{R} \rangle$,*

1. *$\mathcal{P} \models a \parallel b$ if for any runs $r_1, r_2 \in \mathcal{R}$ there is a run $r \in \mathcal{R}$ such that $r(a) = r_1(a)$ and $r(b) = r_2(b)$.*
2. *$\mathcal{P} \models a \rhd b$ if for any runs $r_1, r_2 \in \mathcal{R}$, if $r_1(a) = r_2(a)$, then $r_1(b) = r_2(b)$.*

The relation $\models$ is extended in the standard way to a relation $\mathcal{P} \models \phi$ between a protocol $\mathcal{P}$ and an arbitrary (not necessarily atomic) formula ϕ in the language of secrets.

Axiomatization

In this section we describe a formal logical system for the predicates $\parallel$ and $\rhd$. This system is defined in the propositional language. One also can look at it as the universal fragment of the first-order theory of these two predicates.

This system, like earlier systems defined by More and Naumov (2009a; 2009b), belongs to the set of deductive systems that capture properties of secrets. In general, we refer to such systems as *logics of secrets*. Since this paper is focused on only one such system, in this paper we simply call it*the Logic of Secrets*.

Before listing the axioms of the Logic of Secrets, it will be helpful to discuss the meaning of the statement $a \parallel a$. Note that under Definition 2, $\mathcal{P} \models a \parallel a$ means that any two runs of protocol $\mathcal{P}$ agree on their values of a. Thus, secret a has just one value under this protocol. This means that a is not really a "secret" in the ordinary sense. We will call such secret variables *public knowledge*. In the axioms we introduce below, both the Universal Independence and Universal Dependence Axioms contain the assumption that secret a is public knowledge.

Definition 3 *The Logic of Secrets consists of the following axioms, where a, b, and c are arbitrary secret variables:*

1. *Reflexivity:* $a \rhd a$,
2. *Transitivity:* $a \rhd b \rightarrow (b \rhd c \rightarrow a \rhd c)$,
3. *Symmetry:* $a \parallel b \rightarrow b \parallel a$,
4. *Universal Independence:* $a \parallel a \rightarrow a \parallel b$,
5. *Universal Dependence:* $a \parallel a \rightarrow b \rhd a$,
6. *Substitution:* $a \parallel b \rightarrow (b \rhd c \rightarrow a \parallel c)$.

We write $\Psi \vdash \phi$ to state that formula ϕ is provable in the Logic of Secrets from the set of formulas Ψ.

In the following theorem, we prove the soundness of the above system with respect to the semantics of secrets.

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

Proof. It will be sufficient to show that each of the six axioms above is valid for any protocol $\mathcal{P}$.

Reflexivity. If $r_1(a) = r_1(a)$, then clearly $r_1(a) = r_1(a)$.

Transitivity. Assume $\mathcal{P} \models a \rhd b$ and $\mathcal{P} \models b \rhd c$. Let $r_1(a) = r_2(a)$. Thus, $r_1(b) = r_2(b)$. Therefore, $r_1(c) = r_2(c)$.

Symmetry. This axiom follows from the symmetry of the equality relation.

Universal Independence. Assume that $\mathcal{P} \models a \parallel a$. We will show that $\mathcal{P} \vdash a \parallel b$. Indeed, let r_1 and r_2 be any two runs. We need to show that there is a run r such that $r(a) = r_1(a)$ and $r(b) = r_2(b)$. We will show that r_2 could serve as r. Indeed, by assumption $\mathcal{P} \models a \parallel a$, there is a run r' such that $r_1(a) = r'(a) = r_2(a)$. Hence, $r_2(a) = r_1(a)$. At the same time, obviously, $r_2(b) = r_2(b)$.

Universal Dependence. Assume that $\mathcal{P} \models a \parallel a$. We will show that $\mathcal{P} \vdash b \rhd a$. Let r_1 and r_2 be any two runs such that $r_1(b) = r_2(b)$. We will show that $r_1(a) = r_2(a)$. By assumption $\mathcal{P} \models a \parallel a$, there is a run r such that $r_1(a) = r(a) = r_2(a)$. Therefore, $r_1(a) = r_2(a)$.

Substitution. Assume that $\mathcal{P} \models a \parallel b$ and $\mathcal{P} \models b \rhd c$. We will show that $\mathcal{P} \models a \parallel c$. Indeed, let $r_1, r_2 \in \mathcal{R}$. By the first assumption, there is $r \in \mathcal{R}$ such that $r(a) = r_1(a)$ and $r(b) = r_2(b)$. By the second assumption, $r(b) = r_2(b)$ implies that $r(c) = r_2(c)$. Therefore, $r(a) = r_1(a)$ and $r(c) = r_2(c)$.

$\boxtimes$

Set Semantics

In this section we introduce an alternate semantics for the Logic of Secrets. This semantics is a technical tool that we use to obtain our main results. We will use set semantics to prove the decidability and completeness of the Logic of Secrets with respect to the semantics of secrets defined earlier. Later, we will define a probabilistic semantics for the Logic of Secrets, and we will use set semantics once again to prove the completeness of the Logic of Secrets with respect to the probabilistic semantics.

Definition 4 *A set semantics is a pair $\langle X, \tau \rangle$, where X is an arbitrary finite set and τ is a function from secret variables into subsets of X.*

Definition 5 *For any set semantics $\mathcal{S} = \langle X, \tau \rangle$ we define the meaning of atomic formulas in the language of secrets as follows:*

1. *$\mathcal{S} \vDash a \parallel b$ if and only if $\tau(a) \cap \tau(b) = \varnothing$,*
2. *$\mathcal{S} \vDash a \rhd b$ if and only if $\tau(a) \supseteq \tau(b)$.*

The relation $\vDash$ can be extended in the standard way to a relation $\mathcal{S} \vDash \phi$ between a set semantics $\mathcal{S}$ and arbitrary (not necessarily atomic) formula ϕ in the language of secrets.

The soundness of the Logic of Secrets with respect to the semantics of sets is demonstrated in the theorem below.

Theorem 2 *If $\vdash \phi$, then $\mathcal{S} \vDash \phi$, for any set semantics $\mathcal{S}$.*

Proof. The soundness of the Reflexivity and Transitivity Axioms follows from the reflexivity and transitivity of the superset relation. The soundness of the Symmetry Axiom follows from the symmetry of intersection. The soundness of the Universal Independence and Universal Dependence Axioms follows from the fact that $\mathcal{S} \vDash a \parallel a$ implies that $\tau(a)$ is empty. Finally, to prove the soundness of the Substitution Axiom, we only need to note that $\tau(a) \cap \tau(b) = \varnothing$ and $\tau(b) \supseteq \tau(c)$ imply that $\tau(a) \cap \tau(c) = \varnothing$. ⊠

Next, we prove that the Logic of Secrets is complete with respect to this set semantics.

Theorem 3 *If $\mathcal{S} \vDash \phi$ for any set semantics $\mathcal{S}$, then $\vdash \phi$.*

Proof. Assume that $\nvdash \phi$. Let V be the finite set of all secret variables that appear in ϕ, and let Ψ be a maximal consistent set of formulas that only use variables from V such that $\phi \notin \Psi$. For any $u, v \in V$ we select a new symbol $x_{u,v}$. We are now ready to define a semantics $\mathcal{S} = \langle X, \tau \rangle$.

1. $X = \{x_{u,v} \mid \Psi \nvdash u \parallel v\}$,
2. $\tau(a) = \{x_{u,v} \mid \Psi \vdash a \rhd u \text{ or } \Psi \vdash a \rhd v\}$.

Lemma 1 *For any $a, b \in V$, $\mathcal{S} \vDash a \parallel b$ if and only if $\Psi \vdash a \parallel b$.*

Proof. ($\Rightarrow$) : Assume that $\Psi \nvdash a \parallel b$. Thus, $x_{a,b} \in X$. By the Reflexivity Axiom, $\vdash a \rhd a$ and $\vdash b \rhd b$. Hence, $x_{a,b} \in \tau(a)$ and $x_{a,b} \in \tau(b)$. Thus, $\tau(a) \cap \tau(b) \neq \varnothing$. Therefore, $\mathcal{S} \nvDash a \parallel b$.
($\Leftarrow$) : Suppose that $\Psi \vdash a \parallel b$, but $\mathcal{S} \nvDash a \parallel b$. Thus, there is $x_{c,d} \in X$ such that $x_{c,d} \in \tau(a) \cap \tau(b)$. Hence, $\Psi \vdash a \rhd c$ or $\Psi \vdash a \rhd d$, and, at the same time, $\Psi \vdash b \rhd c$ or $\Psi \vdash b \rhd d$. We will consider four separate cases:

Case 1: $\Psi \vdash a \rhd c$ and $\Psi \vdash b \rhd d$. From $\Psi \vdash a \parallel b$ by the Substitution Axiom, we get $\Psi \vdash a \parallel d$. By the Symmetry Axiom, $\Psi \vdash d \parallel a$. Again by the Substitution Axiom, $\Psi \vdash d \parallel c$. Again by Symmetry, $\Psi \vdash c \parallel d$. Hence, $x_{c,d} \notin X$. Contradiction.

Case 2: $\Psi \vdash a \rhd d$ and $\Psi \vdash b \rhd c$. Similar to Case 1.

Case 3: $\Psi \vdash a \rhd c$ and $\Psi \vdash b \rhd c$. By the Substitution Axiom, $\Psi \vdash a \parallel c$. By the Symmetry Axiom, $\Psi \vdash c \parallel a$. Again by Substitution, $\Psi \vdash c \parallel c$. By the Universal Independence Axiom, $\Psi \vdash c \parallel d$. Hence, $x_{c,d} \notin X$. Contradiction.

Case 4: $\Psi \vdash a \rhd d$ and $\Psi \vdash b \rhd d$. Similar to Case 3.

⊠

Lemma 2 *For any $a, b \in V$, $\mathcal{S} \vDash a \rhd b$ if and only if $\Psi \vdash a \rhd b$.*

Proof. ($\Rightarrow$) : Assume that $\Psi \nvdash a \rhd b$. By the Universal Dependence Axiom, $\Psi \nvdash b \parallel b$. Hence $x_{b,b} \in X$. At the same time, $\Psi \nvdash a \rhd b$ implies that $x_{b,b} \notin \tau(a)$. On the other hand, by the Reflexivity Axiom, $\vdash b \rhd b$. Hence, $x_{b,b} \in \tau(b)$. Thus, $\tau(a) \not\supseteq \tau(b)$. Therefore, $\mathcal{S} \nvDash a \rhd b$.
($\Leftarrow$) : Assume $\Psi \vdash a \rhd b$. We will show that $\tau(a) \supseteq \tau(b)$. Indeed, let $x_{c,d} \in \tau(b)$. Thus, either $\Psi \vdash b \rhd c$ or $\Psi \vdash b \rhd d$. Without loss of generality, assume that $\Psi \vdash b \rhd c$. By the Transitivity Axiom, $\Psi \vdash a \rhd c$. Therefore, $x_{c,d} \in \tau(a)$. ⊠

Lemma 3 *For any formula ψ using only secret variables from V, $\mathcal{S} \vDash \psi$ if and only if $\Psi \vdash \psi$.*

Proof. Induction on structural complexity of formula ψ. The base cases are given in Lemma 1 and Lemma 2. ⊠

The statement of Theorem 3 follows from Lemma 3 and the assumption $\phi \notin \Psi$. ⊠

Corollary 1 *The Logic of Secrets is decidable.*

Proof. This logic has a finite axiomatization and is complete with respect to the semantics of *finite* sets. ⊠

Semantics of Secrets: Completeness

In this section, we prove that the Logic of Secrets is complete with respect to the semantics of secrets.

Theorem 4 *If $\mathcal{P} \vDash \phi$ for every finite protocol $\mathcal{P}$, then $\vdash \phi$.*

Proof. Assume that $\nvdash \phi$. By Theorem 3, there is a set semantics $\mathcal{S} = \langle X, \tau \rangle$ such that $\mathcal{S} \nvDash \phi$. We will define a protocol $\mathcal{P} = \langle \mathcal{D}, \mathcal{R} \rangle$ such that $\mathcal{P} \nvDash \phi$. First, for any secret a, let $\mathcal{D}(a)$ be the set of all boolean functions on $\tau(a)$. Second, let $\mathcal{R}$ be the set of all functions r such that for all secret variables a and b and for any $x \in \tau(a) \cap \tau(b)$, we have $r(a)(x) = r(b)(x)$.

Lemma 4 *$\mathcal{S} \vDash a \parallel b$ if and only if $\mathcal{P} \vDash a \parallel b$.*

Proof. ($\Rightarrow$) : Assume $\mathcal{S} \vDash a \parallel b$. Thus, $\tau(a) \cap \tau(b) = \varnothing$. Consider any two runs r_1 and r_2 of protocol $\mathcal{P}$. We will show that there is a run $r \in \mathcal{R}$ such that $r(a)(x) = r_1(a)(x)$

for any $x \in \tau(a)$ and $r(b)(x) = r_2(b)(x)$ for any $x \in \tau(b)$. Indeed, consider function

$$r(s)(x) = \begin{cases} r_1(s)(x) & \text{if } x \in \tau(a), \\ r_2(s)(x) & \text{if } x \notin \tau(a). \end{cases}$$

First, we will show that $r \in \mathcal{R}$ using a proof by contradiction. Assume there are secret variables c and d and $y \in \tau(c) \cap \tau(d)$ such that $r(c)(y) \neq r(d)(y)$. Note that if $y \notin \tau(a)$, then $r_2(c)(y) = r(c)(y) \neq r(d)(y) = r_2(d)(y)$. Hence, $r_2 \notin \mathcal{R}$. On the other hand, if $y \in \tau(a)$, then $r_1(c)(y) = r(c)(y) \neq r(d)(y) = r_1(d)(y)$. Hence, $r_1 \notin \mathcal{R}$.

Next, notice that, by the definition of r, we have $r(a)(x) = r_1(a)(x)$ for any $x \in \tau(a)$. We now only need to show that $r(b)(x) = r_2(b)(x)$ for any $x \in \tau(b)$. Indeed, this is true because $\tau(a) \cap \tau(b) = \varnothing$.

($\Leftarrow$) : Suppose that $\mathcal{S} \nvDash a \parallel b$. Thus, there is $x_0 \in \tau(a) \cap \tau(b)$. Consider two boolean functions r_1 and r_2 such that $r_1(s)(x) = 0$ for any $x \in \tau(s)$ and

$$r_2(s)(x) = \begin{cases} 1 & \text{if } x = x_0, \\ 0 & \text{otherwise.} \end{cases}$$

Note that if $x \in \tau(c) \cap \tau(d)$, then, by definition, $r_1(c)(x) = r_1(d)(x)$ and $r_2(c)(x) = r_2(d)(x)$. Thus, $r_1, r_2 \in \mathcal{R}$. We will show that there is no such run $r \in \mathcal{R}$ that $r(a) = r_1(a)$ and $r(b) = r_2(b)$. Indeed, $r_1(a)(x_0) = 0$ and $r_2(b)(x_0) = 1$. ⊠

Lemma 5 *$\mathcal{S} \vDash a \rhd b$ if and only if $\mathcal{P} \vDash a \rhd b$.*

Proof. ($\Rightarrow$) : Assume $\mathcal{S} \vDash a \rhd b$. Thus, $\tau(a) \supseteq \tau(b)$. Consider any two runs $r_1, r_2 \in \mathcal{R}$ such that $r_1(a) = r_2(a)$. We will show that $r_1(b) = r_2(b)$. In other words, $r_1(b)(x) = r_2(b)(x)$ for any $x \in \tau(b)$. Since $\tau(a) \supseteq \tau(b)$ and $r_1, r_2 \in \mathcal{R}$, we have $r_1(b)(x) = r_1(a)(x) = r_2(a)(x) = r_2(b)(x)$.

($\Leftarrow$) : Suppose that $\mathcal{S} \nvDash a \rhd b$. Thus, there is $x_0 \in \tau(b) \backslash \tau(a)$. Consider two boolean functions r_1 and r_2 such that $r_1(s)(x) = 0$ for any $x \in \tau(s)$ and

$$r_2(s)(x) = \begin{cases} 1 & \text{if } x = x_0, \\ 0 & \text{otherwise.} \end{cases}$$

As was shown in the proof of Lemma 4, $r_1, r_2 \in \mathcal{R}$. At the same time, by the definition, $r_1(a)(x) = 0 = r_2(a)(x)$ for any $x \in \tau(a)$ and $r_1(b)(x_0) = 0 \neq 1 = r_2(b)(x_0)$. Therefore, $\mathcal{P} \nvDash a \rhd b$. ⊠

Lemma 6 *For any formula ψ that is only using secret variables from V, $\mathcal{S} \vDash \psi$ if and only if $\mathcal{P} \vDash \psi$.*

Proof. Induction on structural complexity of formula ψ. The base case is given in Lemma 4 and Lemma 5. ⊠

The statement of Theorem 4 follows from Lemma 6 and the assumption that $\mathcal{S} \nvDash \phi$. ⊠

Probabilistic Semantics

Recall (Kolmogorov 1933) that probability space as a triple $K = (\Omega, \mathfrak{S}, \mu)$ such that

1. Ω is a non-empty "sample" set,
2. $\mathfrak{S}$ ("σ-algebra of events") is a subset of 2^Ω closed with respect to complementation and countable unions,
3. μ ("probability") is a measure on $\mathfrak{S}$ such that $\mu(\Omega) = 1$.

Given any probability space $K = (\Omega, \mathfrak{S}, \mu)$, we will use letters $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... to denote subsets of $\mathfrak{S}$ that are closed with respect to complementation and countable unions. Such subsets of $\mathfrak{S}$ will also be referred to as σ-algebras.

Our goal is to describe a probabilistic semantics for our logical system. In the spirit of Geiger, Paz, and Pearl (1991), we interpret $\parallel$ as an independence relation between two σ-algebras:

Definition 6 *For any two σ-algebras $\mathfrak{A}$ and $\mathfrak{B}$, $K \vDash \mathfrak{A} \parallel \mathfrak{B}$ if and only if*

$$\forall A \in \mathfrak{A}\ \forall B \in \mathfrak{B}\ (\mu(A \cap B) = \mu(A) \cdot \mu(B)).$$

For the symbol $\rhd$ we suggest the following probabilistic interpretation:

Definition 7 *$K \vDash \mathfrak{A} \rhd \mathfrak{B}$ if and only if*

$$\forall B \in \mathfrak{B}\ \exists A \in \mathfrak{A}\ (\mu(A \triangle B) = 0),$$

where $\triangle$ is the symmetric difference operation on sets.

Proposition 1 *If $K \vDash \mathfrak{A} \parallel \mathfrak{A}$, then $\mu(A) \in \{0, 1\}$ for any $A \in \mathfrak{A}$.*

Proof. By the definition of independence, $\mu(A) \cdot \mu(A) = \mu(A)$. Thus, $\mu(A) \in \{0, 1\}$. ⊠

Below, we prove the soundness of the Logic of Secrets with respect to this probabilistic semantics.

Theorem 5 *If $\vdash \phi$, then $K \vDash \phi$ for any K.*

Proof. We will show the soundness of each of the six axioms with respect to probabilistic semantics.

Reflexivity. We need to show that $K \vDash \mathfrak{A} \rhd \mathfrak{A}$ for any σ-algebra $\mathfrak{A}$. Indeed, for any $A \in \mathfrak{A}$ consider $B = A$ and note that $\mu(A \triangle B) = \mu(A \triangle A) = \mu(\varnothing) = 0$.

Transitivity. Assume $K \vDash \mathfrak{A} \rhd \mathfrak{B}$ and $K \vDash \mathfrak{B} \rhd \mathfrak{C}$. We will show that $K \vDash \mathfrak{A} \rhd \mathfrak{C}$. Indeed, let $C \in \mathfrak{C}$. By the second assumption, there is $B \in \mathfrak{B}$ such that $\mu(B \triangle C) = 0$. By the first assumption, there is set $A \in \mathfrak{A}$ such that $\mu(A \triangle B) = 0$. Using the definition of symmetric difference, $A \triangle C = (A \setminus C) \cup (C \setminus A) = (A \setminus B \setminus C) \cup ((A \cap B) \setminus C) \cup (C \setminus B \setminus A) \cup ((C \cap B) \setminus A) \subseteq (A \setminus B) \cup (B \setminus C) \cup (C \setminus B) \cup (B \setminus A) = (A \triangle B) \cup (B \triangle C)$. Therefore, $\mu(A \triangle C) \leq \mu(A \triangle B) + \mu(B \triangle C) = 0 + 0 = 0$.

Symmetry. Note that $\mu(A \cap B) = \mu(B \cap A)$ and $\mu(A) \cdot \mu(B) = \mu(B) \cdot \mu(A)$. Therefore, $K \vDash \mathfrak{A} \parallel \mathfrak{B}$ if and only if $K \vDash \mathfrak{B} \parallel \mathfrak{A}$.

Universal Independence. Suppose that $K \Vdash \mathfrak{A} \parallel \mathfrak{A}$. By Proposition 1, $\mu(A) \in \{0, 1\}$ for any $A \in \mathfrak{A}$. Consider any $A \in \mathfrak{A}, B \in \mathfrak{B}$.

If $\mu(A) = 1$, then $\mu(\bar{A}) = 0$. Thus, $\mu(B \setminus A) = 0$. Therefore, $\mu(A \cap B) = \mu(B) - \mu(B \setminus A) = \mu(B) = 1 \cdot \mu(B) = \mu(A) \cdot \mu(B)$.

If $\mu(A) = 0$, then $\mu(A \cap B) \leq \mu(A) = 0$. Thus, $\mu(A \cap B) = 0$. Therefore, $\mu(A \cap B) = 0 = 0 \cdot \mu(B) = \mu(A) \cdot \mu(B)$.

Universal Dependence. Suppose that $K \Vdash \mathfrak{A} \parallel \mathfrak{A}$. By Proposition 1, $\mu(A) \in \{0, 1\}$ for any $A \in \mathfrak{A}$. Consider any $A \in \mathfrak{A}$.

If $\mu(A) = 0$, then let $B = \varnothing \in \mathfrak{B}$. Thus, $\mu(A \triangle B) \leq \mu(A \cup B) \leq \mu(A) + \mu(B) = 0 + 0 = 0$. Hence, $\mu(A \triangle B) = 0$.

If $\mu(A) = 1$, then let $B = \Omega \in \mathfrak{B}$. Thus, $\mu(A \triangle B) = \mu(A \triangle \Omega) = \mu(\Omega \setminus A) = 1 - \mu(A) = 0$.

Substitution. Assume $K \vDash \mathfrak{A} \parallel \mathfrak{B}$ and $K \vDash \mathfrak{B} \rhd \mathfrak{C}$. To show $K \vDash \mathfrak{A} \parallel \mathfrak{C}$, consider any $A \in \mathfrak{A}$ and $C \in \mathfrak{C}$. By the second assumption, there is $B \in \mathfrak{B}$, such that $\mu(B \triangle C) = 0$. By the first assumption, $\mu(A \cap B) = \mu(A) \cdot \mu(B)$.

First of all, note that $\mu(A \cap B) - \mu(A \cap C) = \mu((A \cap B) \setminus C) \leq \mu(B \setminus C) \leq \mu(B \triangle C) = 0$ Similarly, $\mu(A \cap C) - \mu(A \cap B) \leq 0$. Thus, $\mu(A \cap B) = \mu(A \cap C)$.

Second, observe that $\mu(A)\mu(B) - \mu(A)\mu(C) = \mu(A)(\mu(B) - \mu(C)) \leq \mu(A)\mu(B \setminus C) \leq \mu(A)\mu(B \triangle A) = \mu(A) \cdot 0 = 0$. Similarly, $\mu(A)\mu(C) - \mu(A)\mu(B) \leq 0$. Hence, $\mu(A)\mu(B) = \mu(A)\mu(C)$.

Therefore, $\mu(A \cap C) = \mu(A \cap B) = \mu(A)\mu(B) = \mu(A)\mu(C)$. ⊠

Now, we turn to the proof that the Logic of Secrets is complete with respect to probabilistic semantics.

Theorem 6 *If $K \vDash \phi$ for any K, then $\vdash \phi$.*

Proof. Assume $\nvdash \phi$. By Theorem 3, there is a finite set semantics $\mathcal{S} = \langle X, \tau \rangle$, such that $\mathcal{S} \nvDash \phi$. We will define finite probability space $K = (\Omega, \mathfrak{S}, \mu)$ as follows:

1. $\Omega = 2^X$ (we will think about this set as set of all boolean functions on X),
2. $\mathfrak{S}$ is the σ-algebra of all subsets: $\mathfrak{S} = 2^\Omega$,
3. $\mu(A) = |A|/|\Omega|$, for any $A \subseteq \Omega$.

For any $Y = y_1, \ldots, y_k \subseteq X$ and any propositional formula $\psi(p_1, \ldots, p_k)$ we define the cylinder

$$C_Y(\psi) = \{\omega \in \Omega \mid \psi(\omega(y_1), \ldots, \omega(y_k))\}$$

and the cylinder algebra

$$\mathfrak{C}_Y = \{C_Y(\psi) \mid \psi(p_1, \ldots, p_k) \text{ is a propositional formula}\}.$$

Lemma 7 *$\mathfrak{C}_Y$ is a σ-algebra.*

Proof. Since Ω is finite, it will be sufficient to prove that $\mathfrak{C}_Y$ is closed with respect to complementation and union. Indeed, $\overline{C_Y(\psi)} = C_Y(\neg\psi)$ and $C_Y(\psi) \cup C_Y(\chi) = C_Y(\psi \vee \chi)$. ⊠

Lemma 8 $\mu(C_Y(\psi)) = 2^{-|Y|} \times |\{b \in \{0,1\}^{|Y|} \mid \psi(b)\}|$.

Proof.

$$\begin{aligned} \mu(C_Y(\psi)) &= \frac{|C_Y(\psi)|}{|\Omega|} = \\ &= \frac{2^{|X|-|Y|} \times |\{b \in \{0,1\}^{|Y|} \mid \psi(b)\}|}{2^{|X|}}. \end{aligned}$$

⊠

Lemma 9 *$K \vDash \mathfrak{C}_Y \parallel \mathfrak{C}_Z$ if and only if $Y \cap Z = \varnothing$.*

Proof. ($\Rightarrow$) : Assume that $x \in Y \cap Z \neq \varnothing$. Consider $C = \{\omega \in \Omega \mid \omega(x) = 1\}$. Note that $C \in \mathfrak{C}_Y$ and $C \in \mathfrak{C}_Z$. At the same time, by Lemma 8,

$$\mu(C) = 2^{-1} \times |\{b \in \{0,1\}^1 \mid b\}| = 2^{-1} \times 1 = \frac{1}{2}.$$

Thus, $\mu(C \cap C) = \mu(C) = 1/2 \neq 1/4 = \mu(C) \cdot \mu(C)$. Therefore, $K \nvDash \mathfrak{C}_Y \parallel \mathfrak{C}_Z$.
($\Leftarrow$) : Suppose that $Y \cap Z = \varnothing$. Consider any $C_Y(\psi) \in \mathfrak{C}_Y$ and any $C_Z(\chi) \in \mathfrak{C}_Z$. By Lemma 8,

$$\begin{aligned} \mu(C_Y(\psi) \cap C_Z(\chi)) = \mu(C_{Y \cup Z}(\psi \wedge \chi)) = \\ = 2^{-|Y \cup Z|} \times |\{b \in \{0,1\}^{|Y \cup Z|} \mid \psi(b) \wedge \chi(b)\}| = \\ = 2^{-|Y|} \times |\{b \in \{0,1\}^{|Y|} \mid \psi(b)\}| \times \\ \times 2^{-|Z|} \times |\{b \in \{0,1\}^{|Z|} \mid \chi(b)\}| = \\ = \mu(C_Y(\psi)) \times \mu(C_Z(\chi)). \end{aligned}$$

⊠

Lemma 10 *$K \vDash \mathfrak{C}_Y \rhd \mathfrak{C}_Z$ if and only if $Y \supseteq Z$.*

Proof. ($\Rightarrow$) : Assume that $x \in Z \setminus Y$. Since Ω is finite and μ is non-zero on any non-emty subset of Ω, $\mu(A \triangle B) = 0$ if and only if $A = B$. Thus, it will be sufficient to construct a cylinder C such that $C \in \mathfrak{C}_Z$, but $C \notin \mathfrak{C}_Y$. Note that $C = \{\omega \in \Omega \mid \omega(x) = 1\}$ is such a cylinder.
($\Leftarrow$) : By the definition of cylinder algebra, $Y \supseteq Z$ implies that $\mathfrak{C}_Y \supseteq \mathfrak{C}_Z$. Therefore, $K \vDash \mathfrak{C}_Y \rhd \mathfrak{C}_Z$. ⊠

Lemma 11 *$K \vDash \psi$ if and only if $\mathcal{S} \vDash \psi$, for any ψ.*

Proof. Induction on structural complexity of ψ. Base cases follow from Lemma 9 and Lemma 10. ⊠

A special case of Lemma 11 is $\psi \equiv \neg\phi$. Thus, $K \nvDash \phi$. This completes proof of Theorem 6. ⊠

Independence of Axioms

In this section, we will prove that each of the axioms in our system is logically independent from the other axioms. This is done by defining non-standard semantics for predicates $\parallel$ and $\rhd$.

Theorem 7 *The Reflexivity Axiom is independent from the other axioms.*

Proof. Consider a semantics under which both $a \parallel b$ and $a \rhd b$ are always false. Then the Reflexivity Axiom is false. However, the remaining axioms are trivially true. ⊠

Theorem 8 *The Transitivity Axiom is independent from the other axioms.*

Proof. Consider a semantics under which secret variables are interpreted as integer numbers, relation $a \parallel b$ is defined to be always false and relation $a \rhd b$ is true if and only if $|a - b| \leq 1$. Note that formula $a \rhd b \rightarrow (b \rhd c \rightarrow a \rhd c)$

is false if $a = 1$, $b = 2$, and $c = 3$. Thus, the Transitivity Axiom is not valid for this semantics. However, it is easy to see that the remaining axioms are valid for all integer values of a and b. ⊠

Theorem 9 *The Symmetry Axiom is independent from the other axioms.*

Proof. Assume that $a \parallel b$ is interpreted as the relation $a > b$ on integer numbers and $a \rhd b$ as relation $\geq$. Note that formula $a \parallel b \rightarrow b \parallel a$ is false if $a = 1$ and $b = 2$. Hence, the Symmetry Axiom is false under this semantics. The remaining axioms, however, are true for all integer values of a and b. ⊠

Theorem 10 *The Universal Independence Axiom is independent from the other axioms.*

Proof. Let $a \parallel b$ be interpreted as the relation $a = b = 0$ on the integers and $a \rhd b$ as the relation $a = b \vee b = 0$. Then $a \parallel a \rightarrow a \parallel b$ is false and the remaining axioms are true. ⊠

Theorem 11 *The Universal Dependence Axiom is independent from the other axioms.*

Proof. Let $a \parallel b$ be interpreted as the relation $a = 0 \vee b = 0$ on integer numbers, and $a \rhd b$ as the relation $a = b$. Then $a \parallel a \rightarrow b \rhd a$ is false and the remaining axioms are true. ⊠

Theorem 12 *The Substitution Axiom is independent from the other axioms.*

Proof. Suppose that $a \parallel b$ is interpreted as the relation $a \neq b$ on integer numbers, and $a \rhd b$ is interpreted as the relation $a \geq b$. If $a = c = 1$ and $b = 2$, then $a \parallel b \rightarrow (b \rhd c \rightarrow a \parallel c)$ is false. However, the remaining axioms are trivially true for all values of a, b, and c. ⊠

Conclusion: Dependencies Between Sets

In this paper, we have considered a logical system for independence and functional dependence relations between single secrets. This is a first step towards a more general investigation of the interaction of the two relations between *sets* of secrets. The language of sets of secrets is more expressive than the language of single secrets, and is capable of capturing deeper properties connecting the independence and functional dependence relations. For example, below is a non-trivial property relating the two predicates:

$$A, B \parallel C, D \wedge A, B, C \rhd E \wedge B, C, D \rhd E \rightarrow B, C \rhd E.$$

To justify this property, we first assume that for some protocol $\mathcal{P} = \langle \mathcal{D}, \mathcal{R} \rangle$, we have $\mathcal{P} \models A, B || C, D$ in addition to $\mathcal{P} \models A, B, C \rhd E$ and $\mathcal{P} \models B, C, D \rhd E$. We will use the notation $r_1 =_S r_2$ to indicate that $\forall s \in S$, $r_1(s) = r_2(s)$, where r_1 and r_2 are runs and S is a set of secrets. Next, suppose we have $r_1, r_2 \in \mathcal{R}$ such that $r_1 =_{B,C} r_2$. We must demonstrate that $r_1 =_E r_2$. By the assumption that $\mathcal{P} \models A, B || C, D$, there exists some $r \in \mathcal{R}$ such that $r =_{A,B} r_1$ and $r =_{C,D} r_2$. Since $r_1 =_{B,C} r_2$, we have $r =_{A,B,C} r_1$ and $r =_{B,C,D} r_2$. Finally, using the assumptions that $\mathcal{P} \models A, B, C \rhd E$ and $\mathcal{P} \models B, C, D \rhd E$, we conclude that $r_1 =_E r =_E r_2$, as desired.

A sound and complete logical system in the setting of sets of secrets would combine Armstrong's axioms for functional dependency listed in the introduction, and the axioms for independence of sets of secrets presented by More and Naumov (2009a). Furthermore, the system would include additional statements connecting these two relations, including the property presented above, as well as set-based versions of the Universal Dependence and Substitution Axioms discussed in this paper:

$$A \parallel A \rightarrow (B \rhd C \rightarrow B \rhd A, C),$$

$$A \parallel B \rightarrow (B \rhd C \rightarrow A \parallel C).$$

A complete axiomatization of these properties remains an open problem.

References

Armstrong, W. W. 1974. Dependency structures of data base relationships. In *Information processing 74 (Proc. IFIP Congress, Stockholm, 1974)*. Amsterdam: North-Holland. 580–583.

Beeri, C.; Fagin, R.; and Howard, J. H. 1977. A complete axiomatization for functional and multivalued dependencies in database relations. In *SIGMOD '77: Proceedings of the 1977 ACM SIGMOD international conference on Management of data*, 47–61. New York, NY, USA: ACM.

Garcia-Molina, H.; Ullman, J.; and Widom, J. 2009. *Database Systems: The Complete Book*. Prentice-Hall, second edition.

Geiger, D.; Paz, A.; and Pearl, J. 1991. Axioms and algorithms for inferences involving probabilistic independence. *Inform. and Comput.* 91(1):128–141.

Halpern, J. Y., and O'Neill, K. R. 2002. Secrecy in multiagent systems. In *Proceedings of the Fifteenth IEEE Computer Security Foundations Workshop*, 32–46.

Halpern, J. Y., and O'Neill, K. R. 2008. Secrecy in multiagent systems. *ACM Trans. Inf. Syst. Secur.* 12(1):1–47. (originally appeared as (Halpern and O'Neill 2002)).

Kolmogorov, A. N. 1933. *Grundbegriffe der Wahrscheinlichkeitsrechnung*. Springer.

Miner More, S., and Naumov, P. 2009a. An independence relation for sets of secrets. In Ono, H.; Kanazawa, M.; and de Queiroz, R., eds., *Proceedings of 16th Workshop on Logic, Language, Information and Computation (Tokyo, 2009), LNAI 5514*, 296–304. Springer.

Miner More, S., and Naumov, P. 2009b. On interdependence of secrets in collaboration networks. In *Proceedings of 12th Conference on Theoretical Aspects of Rationality and Knowledge (Stanford University, 2009)*, 208–217.

Sutherland, D. 1986. A model of information. In *Proceedings of Ninth National Computer Security Conference*, 175–183.