Secrecy Logic: $\mathcal{S}$-Secrecy Structures

George Voutsadakis
Department of Mathematics and Computer Science
Lake Superior State University
Sault Sainte Marie, MI 49783
U.S.A.
gvoutsad@lssu.edu, http://www.voutsadakis.com

June 8, 2010

Abstract

Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system. An $\mathcal{S}$-secrecy logic is a quadruple $\mathbf{K} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S \rangle$, where $\mathbf{Fm}_{\mathcal{L}}(V)$ is the algebra of $\mathcal{L}$-formulas, K, B are $\mathcal{S}$-theories, with $B \subseteq K$, and $S \subseteq K$ is such that $S \cap B = \emptyset$. K corresponds to information deducible from a knowledge base, B to information deducible from the publicly accessible (or browsable) part of the knowledge base and S is a secret set, a set of sensitive or private information that the knowledge base aims at concealing from its users. To provide models for this context, the notion of an $\mathcal{S}$-secrecy structure is introduced. It is a quadruple $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, consisting of an $\mathcal{L}$-algebra $\mathbf{A}$, two $\mathcal{S}$-filters $K_{\mathcal{A}}, B_{\mathcal{A}}$ on $\mathbf{A}$, with $B_{\mathcal{A}} \subseteq K_{\mathcal{A}}$, and a subset $S_{\mathcal{A}} \subseteq K_{\mathcal{A}}$, such that $S_{\mathcal{A}} \cap B_{\mathcal{A}} = \emptyset$. Several model theoretic/universal algebraic and categorical properties of the class of $\mathcal{S}$-secrecy structures, endowed with secrecy homomorphisms, are studied relating to various universal algebraic and categorical constructs.

1 Introduction

The work presented in this paper falls in the intersection of several areas of study. Intuitions from the theory of *abstract algebraic logic* are used to provide *categorical* and *model theoretic* results pertaining to the class of models of the *logical theory of secrecy-preserving reasoning* [1, 25]. In the remainder of this introduction, we motivate this theory and provide a few pointers to the material and the results that inspired those proven in this paper. In the next section, we

[0] *Keywords:* Secrecy-Preserving Reasoning, Abstract Algebraic Logic, Logical Matrices, Protoalgebraic Logics, First-Order Structures, Homomorphism Theorems, Regular Categories, Subdirect Products, Subdirectly Irreducible Structures
2010 AMS Subject Classification: 03C07, 03G27, 08A70

will give a more detailed presentation of the setting of secrecy-preserving reasoning, as introduced in [25]. In particular, it will be shown how this framework gives rise to our categorical and model-theoretic studies.

The advance of the internet and the widespread use of databases and information systems offer unprecedented opportunities for productive interaction and collaboration among individuals as well as across organizations in many areas of human endeavor. These capabilities for sharing information often have to be balanced against the need to protect sensitive or confidential information from unintended disclosure. Consider for instance, the following information sharing scenario:

Example: Suppose that John buys Drug A for cancer. Drug A is a generic drug and generic drugs are covered by John's insurance policy. Suppose that the exact drug that John takes is to be kept secret from his insurance company to avoid unintended or illegal consequences (such as, e.g., denying coverage or unduly increasing his premiums). If the publicly available knowledge

Drug A is a generic drug
Generic drugs are covered by insurance policy

is combined with the secret knowledge

John buys Drug A

the information

John is covered by insurance policy,

needed for reimbursement, can be inferred without disclosing the secret knowledge. □

In [25], inspired by [1], the theoretical foundations of **secrecy-preserving reasoning**, that is, the process of answering queries against knowledge bases that include secret knowledge, based on inference that may use secret knowledge without disclosing it, are developed. A very closely related approach to secrecy-preserving reasoning, that has a very similar goal and comparable scope, is that of *data privacy setting*, which has been presented in a series of papers (see, e.g., [21, 22, 20]). Yet another, more general, approach that is able to handle secrecy-preserving reasoning under a set of parameters fixing various characteristics of the context in which the reasoning process occurs (such as confidentiality policies, user awareness and enforcement policies) is termed *controlled query evaluation*. This approach was pioneered in [18] for the specific case of the enforcement policy of refusal (the alternative being lying) for both known and unknown (the two types of user awareness) secrecies (secrecies and potential secrets being the types of available confidentiality policies). In a series of subsequent publications (see, e.g., [7, 4, 5, 6]) controlled query evaluation was extended to various other combinations of the parameters and careful comparisons were presented of the different characteristics of the types of reasoning arising from varying the parameters. The readers are encouraged to consult

the literature on controlled query evaluation for more details, but also for some additional examples on secrecy-preserving reasoning.

At the heart of the approach in [25] lies a logical system $\mathcal{S}$, for which a sound and complete proof system is available. A knowledge base $\mathbf{K}$ over the logical system consists of

- a (finite) set K of sentences, representing the knowledge stored in the knowledge base, together with
- a designated subset $B \subseteq K$, representing the part of the knowledge that is publicly available, as well as
- a subset S of the deductive closure K^+ of K, that represents the sensitive or secret knowledge and is, for obvious reasons, disjoint from the set B^+, representing information deducible from publicly available knowledge.

A querying agent may ask queries against this knowledge base, which are sentences of the logical language. The knowledge base has the task of combining both public and secret information to answer these queries, while at the same time ensuring that its responses are not jeopardizing the safety status of the secret information. A more detailed presentation of the framework will be provided in Section 2. We outline, next, the connections with the other areas from which we borrow ideas in this paper.

One particular kind of a logical system that can be used as the foundation for this framework is an ordinary *deductive system* (or sentential logic) $\mathcal{S}$ in the sense of *abstract algebraic logic*, see, e.g., [11, 12]. Under this assumption, a knowledge base would consist of a (finitely based) $\mathcal{S}$-theory K of $\mathcal{S}$, together with a subtheory B of K, representing the publicly available knowledge, and a subset S of the theory K, which represents the secret knowledge and is disjoint from B. Furthermore, according to the model theory of first-order logic [10, 13, 15], the form of the structures that are appropriate as models of this theory is $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, where $\mathbf{A}$ is a universal algebra over the same signature as the deductive system $\mathcal{S}$, $K_{\mathcal{A}}$ and $B_{\mathcal{A}}$ are $\mathcal{S}$-filters on $\mathbf{A}$ in the usual sense of abstract algebraic logic, such that $B_{\mathcal{A}} \subseteq K_{\mathcal{A}}$, and $S_{\mathcal{A}}$ is a subset of the filter $K_{\mathcal{A}}$, such that $S_{\mathcal{A}} \cap B_{\mathcal{A}} = \emptyset$. These structures are termed **$\mathcal{S}$-secrecy structures**. The particularly simple form of secrecy structures allows us to study their class with respect to both several ordinary universal algebraic (model-theoretic) properties [9, 16] and several categorical properties. In particular, we will take advantage of many common features that the category of $\mathcal{S}$-secrecy structures has with concrete regular categories (see, e.g., [17]) in order to prove an analog of the well-known Birkhoff's Subdirect Representation Theorem and to characterize its subdirectly irreducible members.

The paper is organized as follows: In Section 2, we elaborate on the setting introduced in [25] for performing secrecy-preserving reasoning with knowledge bases containing secret or sensitive information. This review section is necessary for the reader to develop a sense of the context in which our categorical and model theoretic results that follow are intended to be used. In Section 3 the

main features of the central category under study are introduced. More precisely, the notion of an $\mathcal{S}$-secrecy structure, that of a secrecy homomorphism, and those of a secrecy congruence, of a subobject and of an equalizer are used to provide the first basic results pertaining to the category of $\mathcal{S}$-secrecy structures. In Section 4, products in the same category are introduced and studied. The notion of direct indecomposability is characterized in a theorem extending a well-known theorem of universal algebra and an example is given pointing out some of the differences between the two frameworks. In Section 5, the homomorphism and isomorphism theorems of universal algebra are extended to cover the case of secrecy structures. Of course, secrecy homomorphisms assume the place of algebraic homomorphisms and, also, all congruences considered are secrecy congruences. This feature reveals a close connection with the theory of the Leibniz operator in abstract algebraic logic. In Section 6, the study of several properties of the category of secrecy structures is undertaken. In fact, it is shown that the category of $\mathcal{S}$-secrecy structures shares many properties that characterize concrete regular categories [17]. In Section 7, subdirect products and strict subdirect products of secrecy structures are defined, based on the notions of direct products and subobjects of secrecy structures. Furthermore, the notion of a subdirectly irreducible and strictly subdirectly irreducible secrecy structure is also introduced. An analog of Birkhoff's Theorem for secrecy structures asserts that every secrecy structure is a strict subdirect product of strictly subdirectly irreducible secrecy structures. For finite secrecy structures the non-strict analog is also shown to hold. Subdirectly irreducible structures are characterized in Section 8, which is the last section of the paper.

2 Secrecy-Preserving Reasoning

Consider an algebraic (or logical, depending on the point of view) language type $\mathcal{L}$ and let $\mathrm{Fm}_{\mathcal{L}}(V)$ be the set of all $\mathcal{L}$-terms (or $\mathcal{L}$-formulas) with variables in a fixed denumerable set V and $\mathbf{Fm}_{\mathcal{L}}(V)$ the corresponding term or formula algebra. Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be an $\mathcal{L}$-deductive system, i.e., a pair consisting of a fixed language type $\mathcal{L}$ and a finitary and structural consequence relation $\vdash_{\mathcal{L}} \subseteq \mathcal{P}(\mathrm{Fm}_{\mathcal{L}}(V)) \times \mathrm{Fm}_{\mathcal{L}}(V)$, that is, a relation satisfying the following properties, for every $\Gamma \cup \Delta \cup \{\phi, \psi\} \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$:

1. $\Gamma \vdash_{\mathcal{S}} \phi$, if $\phi \in \Gamma$,
2. $\Gamma \vdash_{\mathcal{S}} \phi$ implies $\Delta \vdash_{\mathcal{S}} \phi$, if $\Gamma \subseteq \Delta$,
3. $\Gamma \vdash_{\mathcal{S}} \phi$ and $\Delta \vdash_{\mathcal{S}} \psi$, for all $\psi \in \Gamma$, imply $\Delta \vdash_{\mathcal{S}} \phi$,
4. $\Gamma \vdash_{\mathcal{S}} \phi$ implies $\Gamma' \vdash_{\mathcal{S}} \phi$, for some finite $\Gamma' \subseteq \Gamma$,
5. $\Gamma \vdash_{\mathcal{S}} \phi$ implies $\sigma(\Gamma) \vdash_{\mathcal{S}} \sigma(\phi)$, for every endomorphism σ of $\mathbf{Fm}_{\mathcal{L}}(V)$.

We also assume that a presentation of this deductive system in terms of a set $\mathcal{R}_{\mathcal{S}}$ of axioms and rules of inference is available, which makes it possible

to write $\mathcal{S}$-proofs in the ordinary way. Sometimes, instead of writing $\Gamma \vdash_{\mathcal{S}} \phi$, we use the equivalent notation $\phi \in C_{\mathcal{S}}(\Gamma)$ or $\phi \in \Gamma^{+}$. Since only one deductive system will be under consideration in a specific context, using the last notational convention, that hides the deductive system, is unlikely to cause any confusion.

Given a deductive system $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$, the **Frege relation** $\Lambda(\mathcal{S})$ of $\mathcal{S}$ is the equivalence relation on $\mathrm{Fm}_{\mathcal{L}}(V)$, defined, for all $\phi, \psi \in \mathrm{Fm}_{\mathcal{L}}(V)$, by

$$\langle \phi, \psi \rangle \in \Lambda(\mathcal{S}) \quad \text{iff} \quad C_{\mathcal{S}}(\phi) = C_{\mathcal{S}}(\psi).$$

This relation is used to define the Fregean hierarchy in abstract algebraic logic. In the context of secrecy, it is used to provide natural closure conditions with respect to entailment that knowledge bases and reasoners should satisfy.

Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system. An **$\mathcal{S}$-knowledge base** $\mathbf{K} = \langle K, B, S \rangle$ consists of

1. A finite set $K \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$, called the **knowledge set**;
2. A subset $B \subseteq K$, called the **browsable part**;
3. A subset $S \subseteq K^{+} \backslash B^{+}$, called the **secret part**.

Example (Continued): We take up again the example of Section 1 and show how it can be formalized in the context of a knowledge base according to the preceding definition.

Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system representing classical propositional logic and let us assume that $\mathcal{L}$ contains the connectives $\wedge$ and $\rightarrow$ (although it is sufficient that they be derived connectives). Let, also, p, q, r, s be propositional variables and assume that

p	represents "Drug A is a generic drug";
q	represents "Generic drugs are covered by insurance policy";
s	represents "John buys Drug A";
r	represents "John is covered by insurance policy".

According to the scenario played out in the example, p, q and $p \wedge q \wedge s \rightarrow r$ are public knowledge, whereas s is supposed to remain confidential. Note that, if the insurance company knows $p, q, p \wedge q \wedge s \rightarrow r$ and r, it cannot infer s.

In the formalism of an $\mathcal{S}$-knowledge base, the following $\mathbf{K} = \langle K, B, S \rangle$ could be chosen to model this scenario:

$$\begin{array}{lcl} K & = & \{p, q, s, p \wedge q \wedge s \rightarrow r\} \\ B & = & \{p, q, p \wedge q \wedge s \rightarrow r\} \\ S & = & \{s\}. \end{array}$$

A secrecy-preserving reasoner (which will be formalized below) could answer positively, if asked about the truth of r, since its truth can be inferred under $\mathcal{S}$ by K (including $S = \{s\}$), and its disclosure does not allow one to infer s, based on $B \cup \{r\}$. □

A **K-reasoner** $R : \mathrm{Fm}_{\mathcal{L}}(V) \rightarrow \{Y, U\}$ is a function that satisfies the following axioms:

1. **Inferential Closure:** $R^{-1}(Y)^+ = R^{-1}(Y)$;
2. **Yes-Axiom:** $B^+ \subseteq R^{-1}(Y) \subseteq K^+$;
3. **Secrecy Axiom:** $(K^+ \backslash R^{-1}(U))^+ \cap S = \emptyset$.

Inferential Closure ensures that every formula that is derivable by a set of formulas that the reasoner reveals must also be revealed. This is a reasonable assumption made under the hypothesis that an agent querying the knowledge base has available a reasoning engine as powerful as that of the knowledge base itself. The Yes-Axiom ensures that every formula that belongs to the browsable part is revealed by the reasoner and that every formula revealed by the reasoner is a formula derivable from the knowledge set. Finally, the Secrecy Axiom asserts that no secret knowledge is derivable from the set of formulas that the reasoner reveals to a querying agent.

Note that the definition of a knowledge base together with these three axioms imply the following conditions: First, for all $\phi, \psi \in \mathrm{Fm}_{\mathcal{L}}(V)$, if $\langle \phi, \psi \rangle \in \Lambda(\mathcal{S})$, then $R(\phi) = R(\psi)$. Second, $S \subseteq R^{-1}(U) \subseteq K^+ \backslash B^+$. Finally, because of Conditions 1 and 2, Condition 3 may be rewritten in the simpler form $R^{-1}(Y) \cap S = \emptyset$.

Given a deductive system $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ and an $\mathcal{S}$-knowledge base $\mathbf{K} = \langle K, B, S \rangle$, note that a reasoner, whose goal is to answer queries as truthfully as possible without revealing secret information, might need to hide more information than contained in the secret part due to the fact that some formulas in the secret part may be deducible from formulas not belonging to the secret part. This idea if formalized in the notion of a security or secrecy envelope [19]. A **K-secrecy envelope** or **security envelope** E is a subset $E \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$ satisfying

1. **Inferential Closure:** $(K^+ \backslash E)^+ \subseteq K^+ \backslash E$;
2. **Envelope Axiom:** $S \subseteq E \subseteq K^+ \backslash B^+$;
3. **Secrecy Axiom:** $(K^+ \backslash E)^+ \cap S = \emptyset$.

If $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ is a deductive system, $\mathbf{K} = \langle K, B, S \rangle$ an $\mathcal{S}$-knowledge base and $R : X \to \{Y, U\}$ a $\mathbf{K}$-reasoner, we define $E_R \subseteq X$ by $E_R = R^{-1}(U) \cap K^+$. Conversely, if E is a $\mathbf{K}$-secrecy envelope, we define $R_E : X \to \{Y, U\}$ by setting, for all $x \in X$,

$$R_E(x) = \begin{cases} Y, & \text{if } x \in K^+ \backslash E \\ U, & \text{otherwise} \end{cases}$$

It is not very difficult to see that these two mappings from reasoners to security envelopes and vice-versa establish a correspondence between $\mathbf{K}$-security envelopes and sets of the form $R^{-1}(U)$, where R is a $\mathbf{K}$-reasoner.

Proposition 1 *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathbf{K} = \langle K, B, S \rangle$ be an $\mathcal{S}$-knowledge base. For every $\mathbf{K}$-reasoner R, the set E_R is a $\mathbf{K}$-secrecy envelope. Conversely, for every $\mathbf{K}$-secrecy envelope E, the function R_E is a $\mathbf{K}$-reasoner.*

Moreover, for every $\mathbf{K}$*-reasoner* R *and for every* $\mathbf{K}$*-secrecy envelope* E*, we have* $R_{E_R} = R$ *and* $E_{R_E} = E$*.*

Proof: For inferential closure, note that $(K^+\backslash E_R)^+ = (K^+\backslash R^{-1}(U))^+ = R^{-1}(Y)^+ = R^{-1}(Y) = K^+\backslash R^{-1}(U) = K^+\backslash E_R$. For the Envelope Axiom, we have, by the definition of S, that $S \subseteq K^+$ and, also, that $(K^+\backslash R^{-1}(U))^+ \cap S = \emptyset$, which implies that $R^{-1}(Y) \cap S = R^{-1}(Y)^+ \cap S = \emptyset$. Hence, $S \subseteq R^{-1}(U)$, showing that $S \subseteq R^{-1}(U) \cap K^+ = E_R$. Moreover,

$$\begin{array}{rcl} E_R & = & R^{-1}(U) \cap K^+ \quad \text{(by the definition of } E_R\text{)} \\ & = & K^+\backslash R^{-1}(Y) \\ & \subseteq & K^+\backslash B^+ \quad \text{(by the Yes-Axiom).} \end{array}$$

Secrecy for E_R corresponds exactly to Secrecy for R.

Suppose, conversely, that E is a $\mathbf{K}$-secrecy envelope. Then

$$R_E^{-1}(Y)^+ = (K^+\backslash E)^+ = K^+\backslash E = R_E^{-1}(Y),$$

and, hence, R_E is inferentially closed. For the Yes-Axiom, we have $B^+ \subseteq K^+\backslash E = R_E^{-1}(Y) \subseteq K^+$. Finally, Secrecy for R_E follows directly from Secrecy for E. The last pat of the proposition is easy to show. □

The secrecy-preserving setting that was presented in this section, motivates the introduction of $\mathcal{S}$-secrecy structures (defined in Definition 2) as the models of a secrecy-preserving framework based on the notion of a knowledge base. A structure similar to a knowledge base, but in which the knowledge set is replaced by K^+, i.e., is an $\mathcal{S}$-theory, with K not necessarily finite, and the browsable part is replaced by B^+ is called an $\mathcal{S}$-secrecy logic. Thus, an $\mathcal{S}$-secrecy logic $\mathfrak{S} = \langle \mathbf{Fm}_{\mathcal{L}}(V), K, B, S\rangle$ consists of $\mathcal{S}$-theories K, B, such that $B \subseteq K$ and a subset $S \subseteq K$, such that $S \cap B = \emptyset$. An $\mathcal{S}$-secrecy logic may be interpreted in a structure $\mathcal{A}$ consisting of an $\mathcal{L}$-algebra $\mathbf{A}$ accompanied by two $\mathcal{S}$-filters $K_{\mathcal{A}}, B_{\mathcal{A}} \in \mathrm{Fi}_{\mathcal{S}}\mathbf{A}$, such that $B_{\mathcal{A}} \subseteq K_{\mathcal{A}}$ and an arbitrary subset $S_{\mathcal{A}} \subseteq K_{\mathcal{A}}$, such that $S_{\mathcal{A}}$ and $B_{\mathcal{A}}$ are disjoint. $\mathcal{S}$-secrecy structures will be the main objects of study in the remainder of the paper. The logical aspects of the theory as well as a study of this framework from an abstract algebraic logic point of view will be presented in work that is currently in progress.

3 Category of $\mathcal{S}$-Secrecy Structures

In the sequel, we will always be referring to a fixed but arbitrary (finitary and structural) deductive system (a.k.a. sentential logic or, simply, logic) $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}}\rangle$, where $\mathcal{L}$ is a fixed algebraic type. Recall that, given an $\mathcal{L}$-algebra $\mathbf{A} = \langle A, \mathcal{L}^{\mathbf{A}}\rangle$, an $\mathcal{S}$-**filter** on $\mathbf{A}$, is a subset $F \subseteq A$, such that, for every $\Gamma \cup \{\phi\} \subseteq \mathrm{Fm}_{\mathcal{L}}(V)$, such that $\Gamma \vdash_{\mathcal{S}} \phi$, and every homomorphism $h : \mathbf{Fm}_{\mathcal{L}}(V) \to \mathbf{A}$, if $h(\Gamma) \subseteq F$, then $h(\phi) \in F$. By $\mathrm{Fi}_{\mathcal{S}}\mathbf{A}$ is denoted the collection of all $\mathcal{S}$-filters on $\mathbf{A}$.

Definition 2 *An* $\mathcal{S}$**-secrecy structure** $\mathcal{A} = \langle \mathbf{A}, K_\mathcal{A}, B_\mathcal{A}, S_\mathcal{A} \rangle$ *is a quadruple consisting of*

1. *an* $\mathcal{L}$*-algebra* $\mathbf{A} = \langle A, \mathcal{L}^\mathbf{A} \rangle$*;*
2. *two* $\mathcal{S}$*-filters* $K_\mathcal{A}, B_\mathcal{A}$ *on* $\mathbf{A}$*, such that* $B_\mathcal{A} \subseteq K_\mathcal{A}$*;*
3. *a subset* $S_\mathcal{A} \subseteq K_\mathcal{A}$*, such that* $S_\mathcal{A} \cap B_\mathcal{A} = \emptyset$*.*

The filters $K_\mathcal{A}$ and $B_\mathcal{A}$ will be referred to as the **knowledge filter** and **browsable filter** of $\mathcal{A}$, respectively, and the set $S_\mathcal{A}$ as the **secrecy set** of $\mathcal{A}$. Definition 2 is illustrated in Figure 1.

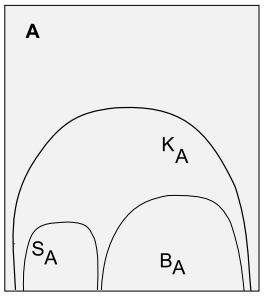


Figure 1: A secrecy structure.

Definition 3 *Let* $\mathcal{S} = \langle \mathcal{L}, \vdash_\mathcal{S} \rangle$ *be a deductive system and* $\mathcal{A} = \langle \mathbf{A}, K_\mathcal{A}, B_\mathcal{A}, S_\mathcal{A} \rangle$*,* $\mathcal{B} = \langle \mathbf{B}, K_\mathcal{B}, B_\mathcal{B}, S_\mathcal{B} \rangle$ *two* $\mathcal{S}$*-secrecy structures. A* **secrecy homomorphism** $h : \mathcal{A} \to \mathcal{B}$ **from** $\mathcal{A}$ **to** $\mathcal{B}$ *is an* $\mathcal{L}$*-homomorphism* $h : \mathbf{A} \to \mathbf{B}$*, such that*

$$h(K_\mathcal{A}) \subseteq K_\mathcal{B}, \quad h(B_\mathcal{A}) \subseteq B_\mathcal{B}, \quad h(S_\mathcal{A}) \subseteq S_\mathcal{B}.$$

h is said to be a **strict** *secrecy homomorphism if*

$$K_\mathcal{A} = h^{-1}(K_\mathcal{B}), \quad B_\mathcal{A} = h^{-1}(B_\mathcal{B}), \quad S_\mathcal{A} = h^{-1}(S_\mathcal{B}).$$

Obviously, $\mathcal{S}$-secrecy structures with secrecy homomorphisms between them form a category, which will be denoted by $\mathcal{S}$-**Str**. On the other hand, we will use the notation $\mathcal{L}$-**Alg** to denote the category of all $\mathcal{L}$-algebras with $\mathcal{L}$-algebra homomorphisms between them.

The appropriate congruences to consider in the setting of $\mathcal{S}$-secrecy structures are those congruences on the algebra reduct of a secrecy structure that are compatible with each of the filters and the secrecy set of the secrecy structure. Recall that, given an $\mathcal{L}$-algebra $\mathbf{A}$ and a set $F \subseteq A$, a congruence θ on $\mathbf{A}$ is said to be **compatible with** F if

$$\langle a, b \rangle \in \theta \text{ and } a \in F \text{ imply } b \in F, \text{ for all } a, b \in A.$$

This condition is equivalent to saying that F is a union of θ-equivalence classes.

Definition 4 *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure. A congruence θ on $\mathbf{A}$ is said to be a* **secrecy congruence on** *$\mathcal{A}$ if it is compatible with each of $K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}$.* $\mathrm{SCon}(\mathcal{A})$ *denotes the collection of all secrecy congruences on $\mathcal{A}$.*

Once secrecy congruences are defined, they may be used to define quotient secrecy structures. The construction is the familiar one from universal algebra on the algebra reducts and the familiar one from abstract algebraic logic on the knowledge and browsable filters and on the secrecy set of the secrecy structures.

Proposition 5 *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system, $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure and $\theta \in \mathrm{SCon}(\mathcal{A})$. Then the quadruple $\mathcal{A}/\theta = \langle \mathbf{A}/\theta, K_{\mathcal{A}}/\theta, B_{\mathcal{A}}/\theta, S_{\mathcal{A}}/\theta \rangle$ is an $\mathcal{S}$-secrecy structure, termed the* **quotient secrecy structure of $\mathcal{A}$ by** *the secrecy congruence θ.*

Proof:
It is known by universal algebra and abstract algebraic logic that $\mathbf{A}/\theta$ is an $\mathcal{L}$-algebra and that $K_{\mathcal{A}}/\theta, B_{\mathcal{A}}/\theta$ are $\mathcal{S}$-filters. Moreover, it is immediate that $B_{\mathcal{A}}/\theta \subseteq K_{\mathcal{A}}/\theta$ and that $S_{\mathcal{A}}/\theta \subseteq K_{\mathcal{A}}/\theta$. To see that $S_{\mathcal{A}}/\theta \cap B_{\mathcal{A}}/\theta = \emptyset$, assume that $\phi/\theta \in S_{\mathcal{A}}/\theta \cap B_{\mathcal{A}}/\theta$. Then, $\phi/\theta \in S_{\mathcal{A}}/\theta$ and $\phi/\theta \in B_{\mathcal{A}}/\theta$. But, by compatibility, these membership relations imply that $\phi \in S_{\mathcal{A}}$ and $\phi \in B_{\mathcal{A}}$. These contradict the disjointness of $S_{\mathcal{A}}$ and $B_{\mathcal{A}}$. □

Recall that given algebras $\mathbf{A} = \langle A, \mathcal{L}^{\mathbf{A}} \rangle$ and $\mathbf{B} = \langle B, \mathcal{L}^{\mathbf{B}} \rangle$ and an algebra homomorphism $h : \mathbf{A} \to \mathbf{B}$, we denote by $\mathrm{Ker}(h)$ the **kernel of** h, defined by

$$\mathrm{Ker}(h) = \{(a_1, a_2) \in A^2 : h(a_1) = h(a_2)\}.$$

This notion extends in a straightforward way to the **kernel** $\mathrm{Ker}(h)$ of a secrecy homomorphism $h : \mathcal{A} \to \mathcal{B}$ from an $\mathcal{S}$-secrecy structure $\mathcal{A}$ to an $\mathcal{S}$-secrecy structure $\mathcal{B}$. The following theorem asserts that strict secrecy homomorphisms and kernels are related exactly as strict matrix homomorphisms and kernels are related in the theory of logical matrices.

Theorem 6

1. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system, $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle, \mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}} \rangle$ $\mathcal{S}$-secrecy structures and $h : \mathcal{A} \to \mathcal{B}$ a strict secrecy homomorphism. Then, the kernel* $\mathrm{Ker}(h)$ *is a secrecy congruence on $\mathcal{A}$.*

2. *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system, $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure and $\theta \in \mathrm{SCon}(\mathcal{A})$. Then, the projection homomorphism $\pi^{\theta} : \mathbf{A} \to \mathbf{A}/\theta$ is a strict secrecy homomorphism $\pi^{\theta} : \mathcal{A} \to \mathcal{A}/\theta$.*

Proof:

1. It suffices to show that $\mathrm{Ker}(h)$ is compatible with $K_{\mathcal{A}}, B_{\mathcal{A}}$ and $S_{\mathcal{A}}$. Let $(a_1, a_2) \in \mathrm{Ker}(h)$, such that $a_1 \in K_{\mathcal{A}}$. Then $h(a_2) = h(a_1) \in h(K_{\mathcal{A}}) \subseteq K_{\mathcal{B}}$, whence, since h is strict, $a_2 \in h^{-1}(K_{\mathcal{B}}) = K_{\mathcal{A}}$. Therefore, $\mathrm{Ker}(h)$ is compatible with $K_{\mathcal{A}}$. A similar argument shows that it is also compatible with $B_{\mathcal{A}}$ and $S_{\mathcal{A}}$.

2. $\pi^\theta : \mathbf{A} \to \mathbf{A}/\theta$ is obviously an $\mathcal{L}$-algebra homomorphism. It is a strict secrecy homomorphism, since $(\pi^\theta)^{-1}(K_{\mathcal{A}/\theta}) = (\pi^\theta)^{-1}(K_{\mathcal{A}}/\theta) = K_{\mathcal{A}}$ and, similarly, for $(\pi^\theta)^{-1}(B_{\mathcal{A}/\theta})$ and $(\pi^\theta)^{-1}(S_{\mathcal{A}/\theta})$.

□

Next, we characterize subobjects in the category $\mathcal{S}$-**Str**. Sometimes, when convenient, we will also be considering the forgetful functor U from $\mathcal{S}$-**Str** to **Set** mapping a given $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ to the universe A of its $\mathcal{L}$-algebra reduct $\mathbf{A}$. The pair $(\mathcal{S}\text{-}\mathbf{Str}, U)$ forms what is known as a **concrete category**. We specialize the general definition of subobject in an arbitrary concrete category to the concrete category $(\mathcal{S}\text{-}\mathbf{Str}, U)$. A **subobject** in $(\mathcal{S}\text{-}\mathbf{Str}, U)$ is a monomorphism $m : \mathcal{A} \to \mathcal{B}$, such that, for every $f : C \to A$ in **Set**, for which there is an $h : \mathcal{C} \to \mathcal{B}$, with $h = m \circ f$ in **Set**, it also holds that $f : \mathcal{C} \to \mathcal{A}$ is a secrecy homomorphism.

It is shown, next, that subobjects in $\mathcal{S}$-**Str** are essentially subalgebras with filters and secrecy sets that are restrictions of the corresponding filters and secrecy sets of the original structures.

Proposition 7 *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle, \mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}} \rangle$ $\mathcal{S}$-secrecy structures. A secrecy monomorphism $m : \mathcal{A} \to \mathcal{B}$ is a subobject in $\mathcal{S}$-**Str** iff $m : \mathbf{A} \to \mathbf{B}$ is a subobject in $\mathcal{L}$-**Alg** and it is strict.*

Proof:

Suppose that $m : \mathbf{A} \to \mathbf{B}$ is a subobject in $\mathcal{L}$-**Alg**, $K_{\mathcal{A}} = m^{-1}(K_{\mathcal{B}})$, $B_{\mathcal{A}} = m^{-1}(B_{\mathcal{B}})$ and $S_{\mathcal{A}} = m^{-1}(S_{\mathcal{B}})$. Let $f : C \to A$ be such that, there exists $h : \mathcal{C} \to \mathcal{B}$, with $h = m \circ f$. Since $h : \mathbf{C} \to \mathbf{B}$ is an $\mathcal{L}$-**Alg**-morphism and $m : \mathbf{A} \to \mathbf{B}$ is a subobject in $\mathcal{L}$-**Alg**, $f : \mathbf{C} \to \mathbf{A}$ is an algebra homomorphism. We must show that $f : \mathcal{C} \to \mathcal{A}$ is an S-**Str**-morphism. It suffices to show that $f(K_{\mathcal{C}}) \subseteq K_{\mathcal{A}}$, $f(B_{\mathcal{C}}) \subseteq B_{\mathcal{A}}$ and $f(S_{\mathcal{C}}) \subseteq S_{\mathcal{A}}$. We only show the first inclusion. The remaining two are proven similarly. We have $f(K_{\mathcal{C}}) \subseteq m^{-1}(m(f(K_{\mathcal{C}}))) \subseteq m^{-1}(h(K_{\mathcal{C}})) \subseteq m^{-1}(K_{\mathcal{B}}) = K_{\mathcal{A}}$.

Suppose, conversely, that $m : \mathcal{A} \to \mathcal{B}$ is a subobject in S-**Str**. Let $f : C \to A$ be such that, there exists $h : \mathbf{C} \to \mathbf{B}$, with $h = m \circ f$. Consider the secrecy algebra $\mathcal{C}' = \langle \mathbf{C}, h^{-1}(K_{\mathcal{B}}), h^{-1}(B_{\mathcal{B}}), h^{-1}(S_{\mathcal{B}}) \rangle$. Then $h : \mathcal{C}' \to \mathcal{B}$ is in S-**Str**, such that $h = m \circ f$, whence, since $m : \mathcal{A} \to \mathcal{B}$ is a subobject in S-**Str**, we get that $f : \mathcal{C}' \to \mathcal{A}$ is a secrecy homomorphism. But, then, $f : \mathbf{C} \to \mathbf{A}$ is in $\mathcal{L}$-**Alg** and this proves that $m : \mathbf{A} \to \mathbf{B}$ is a subobject in $\mathcal{L}$-**Alg**.

To see that $K_{\mathcal{A}} = m^{-1}(K_{\mathcal{B}})$, notice that the left-to-right inclusion is trivial. For the right-to-left inclusion, consider the set map $i_A : A \to A$ and the S-**Str** morphism $m : \langle \mathbf{A}, m^{-1}(K_{\mathcal{B}}), m^{-1}(B_{\mathcal{B}}), m^{-1}(S_{\mathcal{B}})\rangle \to \mathcal{B}$. It is such that $m \circ i_A = m$ in **Set**. Thus, since $m : \mathcal{A} \to \mathcal{B}$ is a subobject in S-**Str**, we get that $i_A : \langle \mathbf{A}, m^{-1}(K_{\mathcal{B}}), m^{-1}(B_{\mathcal{B}}), m^{-1}(S_{\mathcal{B}})\rangle \to \mathcal{A}$ is also an S-**Str** morphism. This means that $m^{-1}(K_{\mathcal{B}}) \subseteq K_{\mathcal{A}}$. The other two equalities may be proven similarly. □

Finally, we end this section with a proof that the category $\mathcal{S}$-**Str** of $\mathcal{S}$-secrecy structures has equalizers. Recall that in the category $\mathcal{L}$-**Alg** the equalizer of $g, h : \mathbf{A} \to \mathbf{B}$ is the subalgebra $\mathbf{E}$ of $\mathbf{A}$ with universe $E = \{a \in A : g(a) = h(a)\}$ together with the inclusion homomorphism $e : \mathbf{E} \hookrightarrow \mathbf{A}$.

$$\mathbf{E} \xrightarrow{\ e\ } \mathbf{A} \underset{h}{\overset{g}{\rightrightarrows}} \mathbf{B}$$

Theorem 8 *The category* $\mathcal{S}$-**Str** *has equalizers.*

Proof:
Let $g, h : \mathcal{A} \to \mathcal{B}$ be two parallel arrows in $\mathcal{S}$-**Str**. Define $\mathcal{E} = \langle \mathbf{E}, K_{\mathcal{E}}, B_{\mathcal{E}}, S_{\mathcal{E}}\rangle$ and $e : \mathcal{E} \to \mathcal{A}$ by setting $(\mathbf{E}, e)$ to be the equalizer of $g, h : \mathbf{A} \to \mathbf{B}$ in $\mathcal{L}$-**Alg** and $K_{\mathcal{E}} = e^{-1}(K_{\mathcal{A}}), B_{\mathcal{E}} = e^{-1}(B_{\mathcal{A}})$ and $S_{\mathcal{E}} = e^{-1}(S_{\mathcal{A}})$. It is easy to see, using Proposition 7, that $e : \mathcal{E} \to \mathcal{A}$ is a subobject in $\mathcal{S}$-**Str**. Given $f : \mathcal{C} \to \mathcal{A}$ in $\mathcal{S}$-**Str**, such that $g \circ f = h \circ f$,

$$\begin{array}{ccccc} \mathcal{E} & \xrightarrow{\ e\ } & \mathcal{A} & \underset{h}{\overset{g}{\rightrightarrows}} & \mathcal{B} \\ & & \uparrow f & & \\ & & \mathcal{C} & & \end{array}$$

we obtain the diagram

$$\begin{array}{ccccc} \mathbf{E} & \xrightarrow{\ e\ } & \mathbf{A} & \underset{h}{\overset{g}{\rightrightarrows}} & \mathbf{B} \\ & \overset{\bar{f}}{\nwarrow} \quad \overset{f}{\nearrow} & & & \\ & \mathbf{C} & & & \end{array}$$

in $\mathcal{L}$-**Alg** and, since $(\mathbf{E}, e)$ is an equalizer of g and f in $\mathcal{L}$-**Alg**, there exists unique $\bar{f} : \mathbf{C} \to \mathbf{E}$, such that $f = e \circ \bar{f}$. But we also have $e(\bar{f}(K_{\mathcal{C}})) = f(K_{\mathcal{C}}) \subseteq K_{\mathcal{A}}$, whence $\bar{f}(K_{\mathcal{C}}) \subseteq e^{-1}(K_{\mathcal{A}}) = K_{\mathcal{E}}$ and, similarly, $\bar{f}(B_{\mathcal{C}}) \subseteq B_{\mathcal{E}}$ and $\bar{f}(S_{\mathcal{C}}) \subseteq S_{\mathcal{E}}$. Thus, $\bar{f} : \mathcal{C} \to \mathcal{E}$ is the unique secrecy homomorphism, such that $f = e \circ \bar{f}$, showing that $(\mathcal{E}, e)$ is the equalizer of g and h in $\mathcal{S}$-**Str**. □

Summarizing, the notion of an $\mathcal{S}$-secrecy structure was defined and secrecy homomorphisms between secrecy structures were introduced giving rise to the category $\mathcal{S}$-**Str**. Secrecy congruences of $\mathcal{S}$-secrecy structures were described and they helped define the notion of a quotient secrecy structure. It was shown that strict secrecy homomorphisms and secrecy congruences are very closely related.

Subobjects in the category of $\mathcal{S}$-secrecy structures were defined following the usual definition of subobjects in concrete categories and a characterization was provided in terms of subalgebras and restrictions of filters and secrecy sets. Finally, it was proven that $\mathcal{S}$-**Str** has equalizers by extending the well-known construction of equalizers in categories of algebras.

4 Products of Secrecy Structures

Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle, \mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}} \rangle$ two $\mathcal{S}$-secrecy structures. Define the quadruple

$$\mathcal{A} \times \mathcal{B} = \langle \mathbf{A} \times \mathbf{B}, K_{\mathcal{A}} \times K_{\mathcal{B}}, B_{\mathcal{A}} \times B_{\mathcal{B}}, S_{\mathcal{A}} \times S_{\mathcal{B}} \rangle.$$

Then $\mathcal{A} \times \mathcal{B}$ is an $\mathcal{S}$-secrecy structure, called the **direct product secrecy structure** of $\mathcal{A}$ and $\mathcal{B}$. This is easy to see once we recall from abstract algebraic logic that, given a sentential logic $\mathcal{S}$, two algebras $\mathbf{A}$ and $\mathbf{B}$ and $\mathcal{S}$-filters F and G on $\mathbf{A}$ and $\mathbf{B}$, respectively, then the set $F \times G$ is also an $\mathcal{S}$-filter on the product algebra $\mathbf{A} \times \mathbf{B}$.

The following theorem lists a few properties satisfied by the direct product of two secrecy structures. The most important ones are inherited from the fact that the underlying $\mathcal{L}$-algebra of the product is the direct product of the underlying algebras of the factors in the sense of universal algebra.

Theorem 9 *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathcal{A}_i = \langle \mathbf{A}_i, K_{\mathcal{A}_i}, B_{\mathcal{A}_i}, S_{\mathcal{A}_i} \rangle$, $i = 1, 2$, be two $\mathcal{S}$-secrecy structures. Then, for $i = 1, 2$, $\pi_i : \mathcal{A}_1 \times \mathcal{A}_2 \to \mathcal{A}_i$ is a surjective secrecy homomorphism from $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$ onto $\mathcal{A}_i$. Moreover, in $\mathbf{Con}(\mathbf{A})$, we have $\mathrm{Ker}(\pi_1) \cap \mathrm{Ker}(\pi_2) = \Delta_{\mathbf{A}}, \mathrm{Ker}(\pi_1) \vee \mathrm{Ker}(\pi_2) = \nabla_{\mathbf{A}}$ and $\mathrm{Ker}(\pi_1)$ and $\mathrm{Ker}(\pi_2)$ permute. Finally, we also have $\pi_1^{-1}(K_{\mathcal{A}_1}) \cap \pi_2^{-1}(K_{\mathcal{A}_2}) = K_{\mathcal{A}_1 \times \mathcal{A}_2}$, $\pi_1^{-1}(B_{\mathcal{A}_1}) \cap \pi_2^{-1}(B_{\mathcal{A}_2}) = B_{\mathcal{A}_1 \times \mathcal{A}_2}$ and $\pi_1^{-1}(S_{\mathcal{A}_1}) \cap \pi_2^{-1}(S_{\mathcal{A}_2}) = S_{\mathcal{A}_1 \times \mathcal{A}_2}$.*

All parts of Theorem 9 follow very easily from the definitions and the corresponding universal algebraic statements (see, e.g., Theorem II.7.3 of [9]).

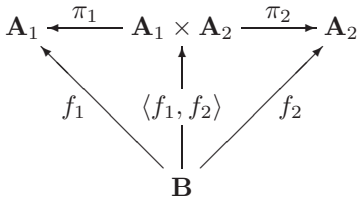
In the next proposition, it is shown that, given two $\mathcal{S}$-secrecy structures $\mathcal{A}$ and $\mathcal{B}$, the direct product $\mathcal{A} \times \mathcal{B}$, as defined above, is their product in the category $\mathcal{S}$-**Str**. Note, here, that this construction may be extended to arbitrary products $\prod_{i \in I} \mathcal{A}_i$ of arbitrary collections $\mathcal{A}_i, i \in I$, of $\mathcal{S}$-secrecy structures, as long as the index set I is not empty. For empty I, the product at the level of $\mathcal{L}$-algebras yields the trivial one-element algebra $\mathbf{1}$. It is impossible, however, to extend this definition to $\mathcal{S}$-secrecy structures: The reason is that, in that case, the condition $S_1 \cap B_1 = \emptyset$ would force S_1 or B_1 to be the empty set. This condition would, then, prevent the existence of a secrecy homomorphism from any other secrecy algebra $\mathcal{A}$, with nonempty secrecy set $S_{\mathcal{A}}$ or nonempty browsable filter $B_{\mathcal{A}}$, respectively, to $\mathbf{1}$.

Proposition 10 *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathcal{A}_i = \langle \mathbf{A}_i, K_{\mathcal{A}_i}, B_{\mathcal{A}_i}, S_{\mathcal{A}_i} \rangle, i = 1, 2$, be two $\mathcal{S}$-secrecy structures. Then the $\mathcal{S}$-secrecy structure*

$\mathcal{A}_1 \times \mathcal{A}_2$, *together with the projection secrecy homomorphisms* $\pi_i : \mathcal{A}_1 \times \mathcal{A}_2 \to \mathcal{A}_i$, $i = 1, 2$, *constitutes a product of* $\mathcal{A}_1$ *and* $\mathcal{A}_2$ *in the category* $\mathcal{S}$-**Str**.

Proof:

Given the fact that $\mathbf{A}_1 \times \mathbf{A}_2$, together with the projections, forms a product of $\mathbf{A}_1$ and $\mathbf{A}_2$ in $\mathcal{L}$-**Alg**, it suffices to show that, for every $\mathcal{B} = \langle \mathbf{B}, K_\mathcal{B}, B_\mathcal{B}, S_\mathcal{B} \rangle$ and every secrecy homomorphisms $f_i : \mathcal{B} \to \mathcal{A}_i, i = 1, 2$, the unique $\mathcal{L}$-**Alg** homomorphism $\langle f_1, f_2 \rangle : \mathbf{B} \to \mathbf{A}_1 \times \mathbf{A}_2$, that completes the diagram



is also a secrecy homomorphism $\langle f_1, f_2 \rangle : \mathcal{B} \to \mathcal{A}_1 \times \mathcal{A}_2$. We have, indeed, for all $b \in K_\mathcal{B}$,

$$\begin{array}{rcl} \langle f_1, f_2 \rangle(b) & = & \langle f_1(b), f_2(b) \rangle \\ & \subseteq & K_{\mathcal{A}_1} \times K_{\mathcal{A}_2} \\ & = & K_{\mathcal{A}_1 \times \mathcal{A}_2}, \end{array}$$

whence $\langle f_1, f_2 \rangle(K_\mathcal{B}) \subseteq K_{\mathcal{A}_1 \times \mathcal{A}_2}$ and, similarly, $\langle f_1, f_2 \rangle(B_\mathcal{B}) \subseteq B_{\mathcal{A}_1 \times \mathcal{A}_2}$ and $\langle f_1, f_2 \rangle(S_\mathcal{B}) \subseteq S_{\mathcal{A}_1 \times \mathcal{A}_2}$. This proves that $\langle f_1, f_2 \rangle : \mathcal{B} \to \mathcal{A}_1 \times \mathcal{A}_2$ is a secrecy homomorphism. □

Product congruences are defined next. The goal is to generalize the well-known theorem of universal algebra characterizing direct products of algebras in terms of factor congruences. It will be shown in Theorem 12 that, given two product congruences on a secrecy structure, the structure can be decomposed into the direct product of two secrecy structures. Recall that, given an $\mathcal{L}$-algebra $\mathbf{A}$, a congruence $\theta \in \mathrm{Con}(\mathbf{A})$ is a **factor congruence** if there exists a congruence $\theta^* \in \mathrm{Con}(\mathbf{A})$, such that $\theta \cap \theta^* = \Delta_\mathbf{A}$, $\theta \vee \theta^* = \nabla_\mathbf{A}$ and θ and θ^* permute. In that case, θ, θ^* are referred to as a **pair of factor congruences** on $\mathbf{A}$.

Definition 11 *Let* $\mathcal{S} = \langle \mathcal{L}, \vdash_\mathcal{S} \rangle$ *be a deductive system and* $\mathcal{A} = \langle \mathbf{A}, K_\mathcal{A}, B_\mathcal{A}, S_\mathcal{A} \rangle$ *an* $\mathcal{S}$*-secrecy structure. A congruence* $\theta \in \mathrm{Con}(\mathbf{A})$ *is a* **product congruence** *if*

- *there exists a congruence* $\theta^* \in \mathrm{Con}(\mathbf{A})$*, such that* θ *and* θ^* *is a pair of factor congruences;*
- $K_\mathcal{A}/\theta$ *and* $K_\mathcal{A}/\theta^*$ *are* $\mathcal{S}$*-filters on* $\mathbf{A}/\theta$ *and* $\mathbf{A}/\theta^*$*, respectively, and* $K_\mathcal{A} = \pi^{-1}(K_\mathcal{A}/\theta) \cap \pi^{*^{-1}}(K_\mathcal{A}/\theta^*)$*, where* π, π^* *are the natural projections;*
- *Similarly for the browsable filters and the secrecy sets.*

Given a pair of product congruences θ', θ'' on $\mathbf{A}$, set

$$K_{\mathcal{A}'} = \{a/\theta' : a \in K_{\mathcal{A}}\}, B_{\mathcal{A}'} = \{a/\theta' : a \in B_{\mathcal{A}}\} \text{ and } S_{\mathcal{A}'} = \{a/\theta' : a \in S_{\mathcal{A}}\},$$

and, similarly,

$$K_{\mathcal{A}''} = \{a/\theta'' : a \in K_{\mathcal{A}}\}, B_{\mathcal{A}''} = \{a/\theta'' : a \in B_{\mathcal{A}}\} \text{ and } S_{\mathcal{A}''} = \{a/\theta'' : a \in S_{\mathcal{A}}\}.$$

Then, define the $\mathcal{S}$-secrecy structures $\mathcal{A}'$ and $\mathcal{A}''$ as follows:

$$\mathcal{A}' = \langle \mathbf{A}/\theta', K_{\mathcal{A}'}, B_{\mathcal{A}'}, S_{\mathcal{A}'} \rangle, \quad \mathcal{A}'' = \langle \mathbf{A}/\theta'', K_{\mathcal{A}''}, B_{\mathcal{A}''}, S_{\mathcal{A}''} \rangle.$$

Theorem 12 *Let $\mathcal{S} = \langle \mathcal{L}, \vdash_{\mathcal{S}} \rangle$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure. If θ', θ'' is a pair of product congruences on $\mathcal{A}$, then $\mathcal{A} \cong \mathcal{A}' \times \mathcal{A}''$ under the secrecy isomorphism $h(a) = \langle a/\theta', a/\theta'' \rangle$, for every $a \in A$.*

Proof:
We know (Theorem II.7.5 of [9]) that $h : \mathbf{A} \cong \mathbf{A}/\theta' \times \mathbf{A}/\theta''$. It is easy to see, by the definition of product congruences, that $h(K_{\mathcal{A}}) = K_{\mathcal{A}/\theta'} \times K_{\mathcal{A}/\theta''}$ and, similarly, for $B_{\mathcal{A}}$ and $S_{\mathcal{A}}$. □

Definition 13 *An $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ is called* **trivial** *if its underlying $\mathcal{L}$-algebra $\mathbf{A}$ is trivial. $\mathcal{A}$ is* **(directly) indecomposable** *if $\mathcal{A}$ is not isomorphic to a direct product of two nontrivial secrecy structures.*

It is not difficult to see that there exist either one or four trivial $\mathcal{S}$-secrecy structures depending on whether or not the deductive system $\mathcal{S}$ has theorems. If $\mathcal{S}$ does not have theorems then the following are trivial $\mathcal{S}$-secrecy structures:

$$\begin{aligned}
\mathcal{T}_0 &= \langle \mathbf{1}, \{0\}, \{0\}, \emptyset \rangle, \\
\mathcal{T}_1 &= \langle \mathbf{1}, \{0\}, \emptyset, \emptyset \rangle, \\
\mathcal{T}_2 &= \langle \mathbf{1}, \{0\}, \emptyset, \{0\} \rangle, \\
\mathcal{T}_3 &= \langle \mathbf{1}, \emptyset, \emptyset, \emptyset \rangle.
\end{aligned}$$

On the other hand, if $\mathcal{S}$ does have theorems, then all its $\mathcal{S}$-filters are non-empty, whence only $\mathcal{T}_0$ is a valid $\mathcal{S}$-secrecy structure.

Theorems 9 and 12 yield immediately a characterization of direct indecomposability of $\mathcal{S}$-secrecy structures in terms of the non-existence of non-trivial product congruences.

Corollary 14 *Let $\mathcal{S}$ be a deductive system. An $\mathcal{S}$-secrecy structure $\mathcal{A}$ is directly indecomposable iff the only product congruences on $\mathbf{A}$ are $\Delta_{\mathbf{A}}$ and $\nabla_{\mathbf{A}}$.*

Finally, Theorem 15, an analog of Theorem II.7.10 of [9] for $\mathcal{S}$-secrecy structures, asserts that every finite $\mathcal{S}$-secrecy structure can be decomposed into a direct product of directly indecomposable $\mathcal{S}$-secrecy structures.

Theorem 15 *Let $\mathcal{S}$ be a deductive system. Every finite $\mathcal{S}$-secrecy structure is isomorphic to a direct product of directly indecomposable $\mathcal{S}$-secrecy structures.*

Proof:
Let $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ be a finite $\mathcal{S}$-secrecy structure. We proceed by induction on the cardinality of A. If $\mathbf{A} = \mathbf{1}$ is trivial, with universe $\{0\}$, then $\mathcal{A}$ can be either of $\mathcal{T}_0, \ldots, \mathcal{T}_3$. In all cases except the second, $\mathcal{A}$ is obviously directly indecomposable. In the second case, $\langle \mathbf{1}, \{0\}, \emptyset, \emptyset \rangle \cong \langle \mathbf{1}, \{0\}, \{0\}, \emptyset \rangle \times \langle \mathbf{1}, \{0\}, \emptyset, \{0\} \rangle$ and the two structures on the right are directly indecomposable $\mathcal{S}$-secrecy structures. (Since they are also trivial structures, $\mathcal{T}_2$ is also directly indecomposable.) Suppose, next, that $\mathcal{A}$ is a nontrivial finite $\mathcal{S}$-secrecy structure, such that, for every $\mathcal{S}$-secrecy structure $\mathcal{B}$, with $|B| < |A|$, $\mathcal{B}$ is isomorphic to a direct product of directly indecomposable $\mathcal{S}$-secrecy structures. If $\mathcal{A}$ is directly indecomposable, then there is nothing to prove. If not, then, there exist nontrivial $\mathcal{S}$-secrecy structures $\mathcal{B}, \mathcal{C}$, such that $\mathcal{A} \cong \mathcal{B} \times \mathcal{C}$. But, then, by the induction hypothesis, $\mathcal{B} \cong \mathcal{B}_1 \times \cdots \times \mathcal{B}_n$ and $\mathcal{C} \cong \mathcal{C}_1 \times \cdots \times \mathcal{C}_m$, with $\mathcal{B}_i, 1 \leq i \leq n$ and $\mathcal{C}_j, 1 \leq j \leq m$, directly indecomposable. Therefore

$$\mathcal{A} \cong \mathcal{B} \times \mathcal{C} \cong \mathcal{B}_1 \times \cdots \times \mathcal{B}_n \times \mathcal{C}_1 \times \cdots \times \mathcal{C}_m,$$

showing that $\mathcal{A}$ is also a direct product of directly indecomposable $\mathcal{S}$-secrecy structures. □

Note that a direct product decomposition $\mathcal{A} \cong \prod_{i=1}^{n} \mathcal{A}_i$ of an $\mathcal{S}$-secrecy structure $\mathcal{A}$ into (not necessarily directly indecomposable) $\mathcal{S}$-secrecy structures $\mathcal{A}_i, i = 1, \ldots, n$, implies that there exists a direct product decomposition of the $\mathcal{L}$-algebra $\mathbf{A}$ into factors $\mathbf{A}_i$. The converse, however, does not hold. A direct product decomposition of $\mathbf{A}$ into (not necessarily directly indecomposable) factors $\mathbf{A}_i, i = 1, \ldots, n$, does not necessarily yield a direct decomposition of $\mathcal{A}$ into a direct product of $\mathcal{S}$-secrecy structures $\mathcal{A}_i$, $i = 1, \ldots, n$, with underlying algebraic reducts $\mathbf{A}_i, i = 1, \ldots, n$, respectively. Moreover, it may be that, whereas $\mathcal{A} \cong \prod_{i=1}^{n} \mathcal{A}_i$ is a decomposition into directly indecomposable $\mathcal{S}$-secrecy structures, the corresponding direct decomposition of $\mathbf{A}$ is not into directly indecomposable $\mathcal{L}$-algebras. To illustrate these points consider the $\mathcal{S}$-secrecy structure $\mathcal{F} = \langle \mathbf{F}, \{0, a, b, 1\}, \{1\}, \{a, b\} \rangle$, with underlying $\mathcal{L}$-algebra the finite distributive lattice $\mathbf{F}$ over the language $\mathcal{L} = \langle \{\wedge, \vee\}, \{\wedge, \vee \mapsto 2\} \rangle$, depicted on the left-hand side in Figure 2. Whereas it is clear that $\mathbf{F}$ has a direct product decomposition into the direct product of two copies of the 2-element chain, depicted on the right-hand side in Figure 2, the $\mathcal{S}$-secrecy structure $\mathcal{F}$ is directly indecomposable.

We present, next, a definition and a lemma from [9] (see Definition II.7.13 and Lemma II.7.14, respectively), that will help us to identify in Theorem 18 necessary and sufficient conditions for an $\mathcal{S}$-secrecy structure to be a subobject in $\mathcal{S}$-**Str** of a given direct product of a collection of $\mathcal{S}$-secrecy structures. We start with defining separation of points.

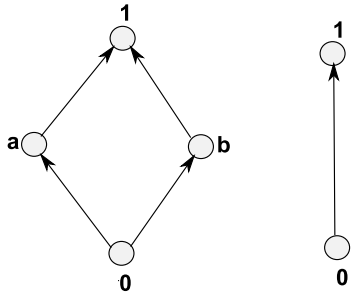


Figure 2: A finite distributive lattice.

Definition 16 *Let A and B be sets and $h : A \to B$ a function. If $a_1, a_2 \in A$, h is said to* **separate** *a_1 and a_2 if $h(a_1) \neq h(a_2)$. The maps $h_i : A \to A_i, i \in I$,* **separate points** *if for each $a_1, a_2 \in A$, with $a_1 \neq a_2$, there is an $i \in I$, such that $h_i(a_1) \neq h_i(a_2)$.*

The following lemma uses the terminology of Definition 16 to characterize those families of functions $h_i : A \to A_i, i \in I$, from a set A to a collection of sets A_i, whose product $h : A \to \prod_{i \in I} A_i$ is injective.

Lemma 17 (Lemma II.7.14 of [9]) *For an indexed family of maps $h_i : A \to A_i$, $i \in I$, the following are equivalent:*

(a) The maps h_i separate points.

(b) $h : A \to \prod_{i \in I} A_i$, defined, for every $a \in A$, by $h(a) = \langle h_i(a) : i \in I \rangle$, is injective.

(c) $\bigcap_{i \in I} \mathrm{Ker}(h_i) = \Delta_A$.

Theorem 18 undertakes the task of providing necessary and sufficient conditions for a given $\mathcal{S}$-secrecy structure to be a substructure of a direct product of $\mathcal{S}$-secrecy structures. Having such conditions is very useful for the study of subdirect products. But this will be postponed until the last two sections of the paper. For the universal algebraic analog of this result, see Theorem II.7.15 of [9].

Theorem 18 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, $\mathcal{A}_i = \langle \mathbf{A}_i, K_{\mathcal{A}_i}, B_{\mathcal{A}_i}, S_{\mathcal{A}_i} \rangle$, $i \in I$, be $\mathcal{S}$-secrecy structures. Let $h_i : \mathcal{A} \to \mathcal{A}_i, i \in I$, be an indexed family of secrecy homomorphisms, such that*

$$\bigcap_{i \in I} h_i^{-1}(K_{\mathcal{A}_i}) = K_{\mathcal{A}}, \bigcap_{i \in I} h_i^{-1}(B_{\mathcal{A}_i}) = B_{\mathcal{A}} \text{ and } \bigcap_{i \in I} h_i^{-1}(S_{\mathcal{A}_i}) = S_{\mathcal{A}}. \qquad (1)$$

*Then, the natural homomorphism $h : \mathcal{A} \to \prod_{i \in I} \mathcal{A}_i$, defined by $h(a) = \langle h_i(a) : i \in I \rangle$, for all $a \in A$, is a subobject in $\mathcal{S}$-**Str** iff $\bigcap_{i \in I} \mathrm{Ker}(h_i) = \Delta_{\mathcal{A}}$ iff the maps h_i separate points.*

Proof:

Taking into account Proposition 7 and Lemma 17, we only need to show that $h^{-1}(K_{\prod_{i\in I}\mathcal{A}_i}) = \bigcap_{i\in I} h_i^{-1}(K_{\mathcal{A}_i})$ and, similarly,

$$h^{-1}(B_{\prod_{i\in I}\mathcal{A}_i}) = \bigcap_{i\in I} h_i^{-1}(B_{\mathcal{A}_i}) \text{ and } h^{-1}(S_{\prod_{i\in I}\mathcal{A}_i}) = \bigcap_{i\in I} h_i^{-1}(S_{\mathcal{A}_i}).$$

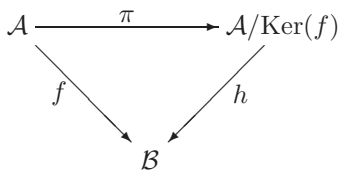
But these follow from Conditions (1) and the definition of $\prod_{i\in I}\mathcal{A}_i$. □

Summarizing, we have defined the notion of a direct product of $\mathcal{S}$-secrecy structures and shown that direct products are in fact categorical products in $\mathcal{S}$-**Str**. A characterization was given in terms of product congruences, which are factor congruences of universal algebras, satisfying some additional conditions that help streamline the $\mathcal{S}$-filters and secrecy sets of the product with those of its generated factors. The trivial $\mathcal{S}$-secrecy structures, i.e., those having a trivial algebraic reduct, were listed. Based on these, a criterion for the direct indecomposability of $\mathcal{S}$-secrecy structures was established and, moreover, it was shown that every finite $\mathcal{S}$-secrecy structure can be decomposed into a direct product of directly indecomposable factors. Finally, borrowing the notion of separation of points from universal algebra, we were able to provide necessary and sufficient conditions for an $\mathcal{S}$-secrecy structure to be a substructure of a direct product of $\mathcal{S}$-secrecy structures.

5 Secrecy Homomorphism Theorems

In this section, we extend the four universal algebraic homomorphism theorems to cover the case of $\mathcal{S}$-secrecy structures. We start with the classical homomorphism theorem (see, e.g., Theorem II.6.12 of [9]). Recall that, by Theorem 6, given $\mathcal{S}$-secrecy structures $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle, \mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}}\rangle$ and a strict secrecy homomorphism $h : \mathcal{A} \to \mathcal{B}$, the kernel $\mathrm{Ker}(h)$ is a secrecy congruence on $\mathcal{A}$ and, conversely, given an $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle$ and $\theta \in \mathrm{SCon}(\mathcal{A})$, the projection homomorphism $\pi^\theta : \mathbf{A} \to \mathbf{A}/\theta$ is a strict secrecy homomorphism $\pi^\theta : \mathcal{A} \to \mathcal{A}/\theta$.

Theorem 19 (Secrecy Homomorphism Theorem) *Let $\mathcal{S}$ be a deductive system, $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle, \mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}}\rangle$ be $\mathcal{S}$-secrecy structures and $f : \mathcal{A} \twoheadrightarrow \mathcal{B}$ a strict surjective secrecy homomorphism. Then, there exists a secrecy isomorphism $h : \mathcal{A}/\mathrm{Ker}(f) \to \mathcal{B}$, such that $f = h \circ \pi$, where $\pi : \mathcal{A} \to \mathcal{A}/\mathrm{Ker}(f)$ is the natural projection secrecy homomorphism.*



Proof:
The mapping $h : A/\mathrm{Ker}(f) \to B$ is defined, as usual, by

$$h(a/\mathrm{Ker}(f)) = f(a), \text{ for all } a \in A.$$

It is well-known that h is a well-defined algebra isomorphism $h : \mathbf{A}/\mathrm{Ker}(f) \to \mathbf{B}$, such that $f = h \circ \pi$. Thus, it suffices to show that $h(K_{\mathcal{A}/\mathrm{Ker}(f)}) = K_{\mathcal{B}}$ and, similarly, $h(B_{\mathcal{A}/\mathrm{Ker}(f)}) = B_{\mathcal{B}}$ and $h(S_{\mathcal{A}/\mathrm{Ker}(f)}) = S_{\mathcal{B}}$. We show the first equality in detail: Let $a/\mathrm{Ker}(f) \in K_{\mathcal{A}/\mathrm{Ker}(f)} = K_{\mathcal{A}}/\mathrm{Ker}(f)$. Since f is a strict secrecy homomorphism, $\mathrm{Ker}(f)$ is compatible with $K_{\mathcal{A}}$. Therefore $a \in K_{\mathcal{A}}$. This implies that $h(a/\mathrm{Ker}(f)) = f(a) \in f(K_{\mathcal{A}}) \subseteq K_{\mathcal{B}}$ and proves the left-to-right inclusion. To show the reverse inclusion, suppose that $b \in K_{\mathcal{B}}$. Then, since $f : \mathcal{A} \to \mathcal{B}$ is strict and surjective, there exists $a \in K_{\mathcal{A}}$, such that $f(a) = b$. Thus, we have $b = f(a) = h(a/\mathrm{Ker}(f)) \in h(K_{\mathcal{A}}/\mathrm{Ker}(f)) = h(K_{\mathcal{A}/\mathrm{Ker}(f)})$. This proves the right-to-left inclusion. □

We proceed with an analog of the Second Isomorphism Theorem of universal algebra (see, e.g., Theorem II.6.15 of [9]) for $\mathcal{S}$-secrecy structures.

Theorem 20 (Second Secrecy Isomorphism Theorem) *Let $\mathcal{S}$ be a deductive system, $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ an $\mathcal{S}$-secrecy structure and $\theta, \eta \in \mathrm{SCon}(\mathcal{A})$, such that $\theta \subseteq \eta$. Then, the mapping $h : (\mathcal{A}/\theta)/(\eta/\theta) \to \mathcal{A}/\eta$ defined by*

$$h((a/\theta)/(\eta/\theta)) = a/\eta, \text{ for all } a \in A,$$

is a secrecy isomorphism from $(\mathcal{A}/\theta)/(\eta/\theta)$ to $\mathcal{A}/\eta$.

Proof:
First, notice that η/θ is a secrecy congruence on $\mathcal{A}/\theta$. To show compatibility of η/θ with $K_{\mathcal{A}/\theta} = K_{\mathcal{A}}/\theta$, assume that $\langle a/\theta, b/\theta \rangle \in \eta/\theta$ and $a/\theta \in K_{\mathcal{A}}/\theta$. Then $\langle a, b \rangle \in \eta$ and $a \in K_{\mathcal{A}}$, by the compatibility of θ with $K_{\mathcal{A}}$. Therefore $b \in K_{\mathcal{A}}$, by the compatibility of η with $K_{\mathcal{A}}$. Thus, $b/\theta \in K_{\mathcal{A}}/\theta = K_{\mathcal{A}/\theta}$. Similarly, it may be shown that η/θ is also compatible with $B_{\mathcal{A}/\theta}$ and $S_{\mathcal{A}/\theta}$.

It is known from universal algebra that $h : (\mathbf{A}/\theta)/(\eta/\theta) \to \mathbf{A}/\eta$, defined by $h((a/\theta)/(\eta/\theta)) = a/\eta$, for all $a \in A$, is an algebra isomorphism. So it suffices to show that it preserves the $\mathcal{S}$-filters and the secrecy sets. Since all three equalities may be shown similarly, we only show in detail that $h(K_{(\mathcal{A}/\theta)/(\eta/\theta)}) = K_{\mathcal{A}/\eta}$. Suppose that $a/\eta = h(K_{(\mathcal{A}/\theta)/(\eta/\theta)}) = h(K_{\mathcal{A}/\theta}/(\eta/\theta)) = h((K_{\mathcal{A}}/\theta)/(\eta/\theta))$. Thus, there exists $b \in K_{\mathcal{A}}$, such that $a/\eta = h((b/\theta)/(\eta/\theta)) = b/\eta$. Hence, by the compatibility of η with $K_{\mathcal{A}}$, $a \in K_{\mathcal{A}}$, showing that $a/\eta \in K_{\mathcal{A}}/\eta = K_{\mathcal{A}/\eta}$. If, conversely, $a/\eta \in K_{\mathcal{A}/\eta} = K_{\mathcal{A}}/\eta$, we get that $a \in K_{\mathcal{A}}$, whence $a/\eta = h((a/\theta)/(\eta/\theta)) \in h((K_{\mathcal{A}}/\theta)/(\eta/\theta)) = h(K_{(\mathcal{A}/\theta)/(\eta/\theta)})$. □

Let $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ be an $\mathcal{S}$-secrecy structure. An $\mathcal{S}$-secrecy structure $\mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}} \rangle$ is called a **secrecy substructure** of $\mathcal{A}$, written $\mathcal{B} \leq \mathcal{A}$, if $\mathbf{B}$ is an $\mathcal{L}$-subalgebra of $\mathbf{A}$ and $K_{\mathcal{B}} = K_{\mathcal{A}} \cap B$, $B_{\mathcal{B}} = B_{\mathcal{A}} \cap B$ and $S_{\mathcal{B}} = S_{\mathcal{A}} \cap B$, i.e., if the inclusion morphism $i : \mathcal{B} \hookrightarrow \mathcal{A}$ is a subobject in $\mathcal{S}$-**Str**, according to the definition in Section 3 and the characterization in Proposition 7.

Next, we adapt Definition II.6.16 of [9] to accommodate $\mathcal{S}$-secrecy structures. This definition will supply the needed notions and notation to enable the formulation of an analog of the Third Isomorphism Theorem for $\mathcal{S}$-secrecy structures.

Definition 21 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ be an $\mathcal{S}$-secrecy structure. Suppose B is a subset of A and $\theta \in \mathrm{SCon}(\mathcal{A})$. Let $B^{\theta} = \{a \in A : B \cap a/\theta \neq \emptyset\}$. Let $\mathbf{B}^{\theta}$ be the subalgebra of A generated by B^{θ} and*

$$K_{\mathcal{B}^{\theta}} = K_{\mathcal{A}} \cap B^{\theta}, B_{\mathcal{B}^{\theta}} = B_{\mathcal{A}} \cap B^{\theta}, S_{\mathcal{B}^{\theta}} = S_{\mathcal{A}} \cap B^{\theta}.$$

Also define $\theta\restriction_B = \theta \cap B^2$, the restriction of θ to B.

It is well-known from universal algebra that, if $\mathbf{B} = \langle B, \mathcal{L}^{\mathbf{B}} \rangle$ is a subalgebra of $\mathbf{A}$, the universe of $\mathbf{B}^{\theta}$ is B^{θ} and that the restriction of θ to B is a congruence on $\mathbf{B}$. Moreover, the Third Isomorphism Theorem asserts that $\mathbf{B}/\theta\restriction_B \cong \mathbf{B}^{\theta}/\theta\restriction_{B^{\theta}}$ (see, e.g., Lemma II.6.17 and Theorem II.6.18 of [9]). We proceed, next, to extend these results to the framework of $\mathcal{S}$-secrecy structures and secrecy congruences.

Lemma 22 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, $\mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}} \rangle$ be $\mathcal{S}$-secrecy structures, such that $\mathcal{B} \leq \mathcal{A}$, and $\theta \in \mathrm{SCon}(\mathcal{A})$.*

1. *$\mathcal{B}^{\theta} = \langle \mathbf{B}^{\theta}, K_{\mathcal{B}^{\theta}}, B_{\mathcal{B}^{\theta}}, S_{\mathcal{B}^{\theta}} \rangle$ is a secrecy substructure of $\mathcal{A}$, whose underlying algebraic reduct has universe B^{θ}.*

2. *$\theta\restriction_B$ is a secrecy congruence on $\mathcal{B}$.*

Proof:

1. We know, by the corresponding universal algebraic result (Lemma II.6.17 of [9]), that $\mathbf{B}^{\theta}$ is a subalgebra of $\mathbf{A}$, with universe B^{θ}. This, together with the definitions of $K_{\mathcal{B}^{\theta}}, B_{\mathcal{B}^{\theta}}$ and $S_{\mathcal{B}^{\theta}}$, yield, taking into account Proposition 7, that $\mathcal{B}^{\theta}$ is an $\mathcal{S}$-secrecy substructure of $\mathcal{A}$.

2. Since, again, it is known that $\theta\restriction_B$ is a congruence on $\mathbf{B}$, it suffices to show that it is compatible with the $\mathcal{S}$-filters and the secrecy set of $\mathcal{B}$. These compatibility relations follow directly from the corresponding compatibility relations assumed for $\mathcal{A}$. For instance, if $\langle b_1, b_2 \rangle \in \theta\restriction_B$ and $b_1 \in K_{\mathcal{B}}$, then $\langle b_1, b_2 \rangle \in \theta$ and $b_1 \in K_{\mathcal{A}}$, whence $b_2 \in K_{\mathcal{A}}$, showing that $b_2 \in K_{\mathcal{A}} \cap B = K_{\mathcal{B}}$. □

Having Lemma 22 at hand, it now makes sense to formulate the generalization of the Third Isomorphism Theorem of universal algebra (Theorem II.6.18 of [9]) for $\mathcal{S}$-secrecy structures.

Theorem 23 (Third Secrecy Isomorphism Theorem) *Let $\mathcal{S}$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, $\mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}} \rangle$ be $\mathcal{S}$-secrecy structures, such that $\mathcal{B} \leq \mathcal{A}$, and $\theta \in \mathrm{SCon}(\mathcal{A})$. Then $\mathcal{B}/\theta\restriction_B \cong \mathcal{B}^{\theta}/\theta\restriction_{B^{\theta}}$.*

Proof:

All quotients involved make sense due to Lemma 22. Furthermore, since, by Theorem II.6.18 of [9], $\mathbf{B}/\theta\restriction_\theta \cong \mathbf{B}^\theta/\theta\restriction_{B^\theta}$ via the algebra isomorphism

$$h(b/\theta\restriction_B) = b/\theta\restriction_{B^\theta}, \text{ for all } b \in B,$$

it suffices to show that $h(K_{\mathcal{B}/\theta\restriction_B}) = K_{\mathcal{B}^\theta/\theta\restriction_{B^\theta}}$ and, similarly, $h(B_{\mathcal{B}/\theta\restriction_B}) = B_{\mathcal{B}^\theta/\theta\restriction_{B^\theta}}$ and $h(S_{\mathcal{B}/\theta\restriction_B}) = S_{\mathcal{B}^\theta/\theta\restriction_{B^\theta}}$. But all these relations are straightforward based on the corresponding definitions. □

To prove a version of the Correspondence Theorem of universal algebra (Theorem II.6.20 of [9]) for secrecy structures, we define, as in the theory of logical matrices, the largest secrecy congruence on an $\mathcal{S}$-secrecy structure $\mathcal{A}$. This is the largest congruence on the underlying algebra $\mathbf{A}$, that is compatible with both the knowledge and the browsable filters and with the secrecy set of $\mathcal{A}$. We first show that such a congruence always exists.

Theorem 24 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_\mathcal{A}, B_\mathcal{A}, S_\mathcal{A}\rangle$ be an $\mathcal{S}$-secrecy structure. Then, there exists a largest congruence $\Omega(\mathcal{A})$ on $\mathbf{A}$ compatible with each of $K_\mathcal{A}, B_\mathcal{A}, S_\mathcal{A}$. Thus,* $\mathrm{SCon}(\mathcal{A})$ *has the structure of a complete lattice and* $\mathbf{SCon}(\mathcal{A}) \cong [\Delta_\mathcal{A}, \Omega(\mathcal{A})]$*, where the latter is viewed as an interval in* $\mathbf{Con}(\mathbf{A})$.

Proof:

As in the case of logical matrices, notice that $\Delta_\mathcal{A}$ is compatible with each filter and with the secrecy set and, also, that the collection $\mathcal{C}$ of all congruences on $\mathbf{A}$ having this property has a maximal element and is closed under congruence joins. The existence of the maximal element may be shown by an application of Zorn's Lemma. That the congruence join of two congruences that are compatible with a given subset of A is also a congruence compatible with the same set is a well-known fact from the theory of logical matrices (see, e.g., [11]). The existence of a maximal element and the closedness under joins yield immediately that there exists a unique maximal element in $\mathcal{C}$. This element is the one denoted by $\Omega(\mathcal{A})$. □

The secrecy congruence $\Omega(\mathcal{A})$, whose existence is asserted in Theorem 24, will be called the **Leibniz secrecy congruence** of $\mathcal{A}$. The Secrecy Correspondence Theorem states that, given a secrecy congruence θ on a secrecy structure $\mathcal{A}$, the lattice of all secrecy congruences of the quotient secrecy structure $\mathcal{A}/\theta$ is isomorphic to the interval $[\theta, \Omega(\mathcal{A})]$ in the lattice of secrecy congruences of $\mathcal{A}$.

Theorem 25 (Secrecy Correspondence Theorem) *Let $\mathcal{S}$ be a deductive system, $\mathcal{A} = \langle \mathbf{A}, K_\mathcal{A}, B_\mathcal{A}, S_\mathcal{A}\rangle$ be an $\mathcal{S}$-secrecy structure and $\theta \in \mathrm{SCon}(\mathcal{A})$. Then, the function h with domain $[\theta, \Omega(\mathcal{A})]$, defined by $h(\eta) = \eta/\theta$, for all $\eta \in [\theta, \Omega(\mathcal{A})]$, is a lattice isomorphism from $[\theta, \Omega(\mathcal{A})]$ to $\mathbf{SCon}(\mathcal{A}/\theta)$, where $[\theta, \Omega(\mathcal{A})]$ is viewed as a sublattice of $\mathbf{SCon}(\mathcal{A})$.*

Proof:

The mapping h is injective because it is injective on the set of all congruences of $\mathbf{A}$ including θ. To see that it is surjective, suppose that $\eta' \in \mathrm{SCon}(\mathcal{A}/\theta)$. Let $\eta = \{\langle a, b\rangle \in A^2 : \langle a/\theta, b/\theta\rangle \in \eta'\}$. We have

- $\eta \in \mathrm{Con}(\mathbf{A})$: Follows directly from the fact that $\eta' \in \mathrm{Con}(\mathbf{A}/\theta)$.
- $\eta \in \mathrm{SCon}(\mathcal{A})$: Let us show in detail that η is compatible with $K_{\mathcal{A}}$. Suppose, to this end, that $\langle a, b\rangle \in \eta$ and $a \in K_{\mathcal{A}}$. Then $\langle a/\theta, b/\theta\rangle \in \eta'$ and $a/\theta \in K_{\mathcal{A}}/\theta = K_{\mathcal{A}/\theta}$. Thus, since $\eta' \in \mathrm{SCon}(\mathcal{A}/\theta)$, we get that $b/\theta \in K_{\mathcal{A}}/\theta$. Since $\theta \in \mathrm{SCon}(\mathcal{A})$, we must have $b \in K_{\mathcal{A}}$. Therefore, η is in fact compatible with $K_{\mathcal{A}}$. Compatibility with each of $B_{\mathcal{A}}$ and $S_{\mathcal{A}}$ may be proven similarly.
- $\theta \leq \eta$: $\langle a, b\rangle \in \theta$ implies $\langle a/\theta, b/\theta\rangle \in \Delta_{\mathcal{A}/\theta} \subseteq \eta'$, whence $\langle a, b\rangle \in \eta$.
- $\eta' = \eta/\theta = h(\eta)$.

Thus, h is also surjective. Finally, the fact that $\langle a/\theta, b/\theta\rangle \in \eta/\theta$ iff $\langle a, b\rangle \in \eta$ implies that $\eta_1 \leq \eta_2$ iff $\eta_1/\theta \leq \eta_2/\theta$, i.e., that h is a lattice isomorphism. ■

Summarizing, in this section analogs of the well-known Homomorphism Theorem and Isomorphism Theorems of universal algebra were provided for $\mathcal{S}$-secrecy structures. Theorem 19 provided an analog of the Homomorphism Theorem, Theorem 20 an analog of the Second Isomorphism Theorem and Theorem 23 an analog of the Third Isomorphism Theorem. Finally, to prove Theorem 25, an analog of the Correspondence Theorem, the notion of the Leibniz secrecy congruence of an $\mathcal{S}$-secrecy structure was introduced, which is the largest secrecy congruence on the structure, and it was asserted that it exists for every $\mathcal{S}$-secrecy structure, in a way similar to the existence of the Leibniz congruence of an $\mathcal{S}$-matrix in the theory of abstract algebraic logic.

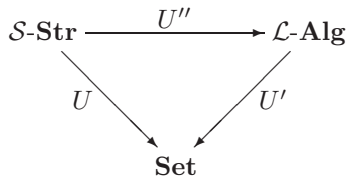
6 Properties Related to Regularity

In this section, we show that the category $\mathcal{S}$-**Str** shares many of the properties that define a regular concrete category. For general categorical definitions and notation, the reader is referred to the standard references [2, 8, 14]. Specifically for material pertaining to the existence and characterization of subdirect products in regular concrete categories we refer to the works by Pultr and Vinárek [17, 23, 24]. We start by proving that the forgetful functor $U : \mathcal{S}$-**Str** $\rightarrow$ **Set** from the category of $\mathcal{S}$-secrecy structures to the category of small sets, that forgets both the algebraic structure and the filters and secrecy set of an $\mathcal{S}$-secrecy structure preserves all small limits.

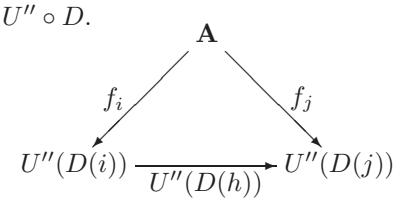
Proposition 26 *Let $\mathcal{S}$ be a deductive system. Then, the forgetfull functor $U :$ $\mathcal{S}$-**Str** $\rightarrow$ **Set**, with $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle \overset{U}{\mapsto} A$, preserves all small limits.*

Proof:

It is well-known that the forgetful functor $U' : \mathcal{L}\text{-}\mathbf{Alg} \to \mathbf{Set}$ preserves all small limits. Thus, it suffices to show (see the diagram below) that the forgetful functor $U'' : \mathcal{S}\text{-}\mathbf{Str} \to \mathcal{L}\text{-}\mathbf{Alg}$ preserves all small limits.



Suppose to this end that (L, l) is a limit of the small diagram $D : I \to \mathcal{S}\text{-}\mathbf{Str}$ in the category $\mathcal{S}\text{-}\mathbf{Str}$. Consider the corresponding diagram $U'' \circ D : I \to \mathcal{L}\text{-}\mathbf{Alg}$. We must show that $(U''(L), U''(l))$ is a limit of $U'' \circ D$ in $\mathcal{L}\text{-}\mathbf{Alg}$. Let $(\mathbf{A}, f)$ be a cone in $\mathcal{L}\text{-}\mathbf{Alg}$ over $U'' \circ D$.



Construct the quadruple $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, where $K_{\mathcal{A}} = \bigcap_{i \in |I|} f_i^{-1}(K_{D(i)})$ and, similarly, $B_{\mathcal{A}} = \bigcap_{i \in |I|} f_i^{-1}(B_{D(i)})$ and $S_{\mathcal{A}} = \bigcap_{i \in |I|} f_i^{-1}(S_{D(i)})$. It is not difficult to see that $\mathcal{A}$ is an $\mathcal{S}$-secrecy structure and that $f_i' : \mathcal{A} \to D(i)$, with $U''(f_i') = f_i$, is a secrecy homomorphism. Thus, since (L, l) is a limit of D in $\mathcal{S}\text{-}\mathbf{Str}$, there exists a unique secrecy homomorphism $m : \mathcal{A} \to L$, such that $l_i \circ m = f_i'$, for all $i \in |I|$. The algebra homomorphism $U''(m)$ may now be shown to be the unique morphism in $\mathcal{L}\text{-}\mathbf{Alg}$ such that $U''(l_i) \circ U''(m) = f_i$. $\square$

The following result asserts that, given a bijection between two sets and an $\mathcal{S}$-secrecy structure on its codomain, one may endow the domain with an $\mathcal{S}$-secrecy structure so that the given bijection becomes a secrecy isomorphism.

Proposition 27 *Given a deductive system $\mathcal{S}$, if A is a set, $\mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}} \rangle$ an $\mathcal{S}$-secrecy structure and $f : A \to B$ a bijection, then, there exists an $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, such that $f : \mathcal{A} \to \mathcal{B}$ is a secrecy isomorphism.*

Proof:

This is fairly obvious. Based on f, viewed as a "renaming" of the elements of B, we endow A with both an algebraic and a secrecy structure, resulting in an $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$, in such a way that $f : \mathcal{A} \to \mathcal{B}$ is a secrecy isomorphism identical with f on A. $\square$

By the definition of the forgetful functor $U : \mathcal{S}\text{-}\mathbf{Str} \to \mathbf{Set}$, we obtain

Proposition 28 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A}$ an $\mathcal{S}$-secrecy structure. If $h : \mathcal{A} \to \mathcal{A}$ is a secrecy isomorphism and $U(h) = i_A$, then $h = i_{\mathcal{A}}$.*

Motivated by Definition 1.3 of [17], we define, for a set X, the preordered class $\mathcal{S}$-$\mathbf{Str}_X = (\{\mathcal{A} : U(\mathcal{A}) = X\}, \prec)$ by setting $\mathcal{A} \prec \mathcal{B}$ iff the identity $i_X : X \to X$ is a secrecy homomorphism $i_X : \mathcal{A} \to \mathcal{B}$. A meet of $\mathcal{A}_i, i \in I$, in $\mathcal{S}$-$\mathbf{Str}_X$, if it exists, will be denoted by $\bigwedge_{i\in I} \mathcal{A}_i$.

Proposition 29 *Let $\mathcal{S}$ be a deductive system. For every set X, the collection $\mathcal{S}$-$\mathbf{Str}_X$ is a set and it is finite for finite X, provided that $\mathcal{L}$ is finite.*

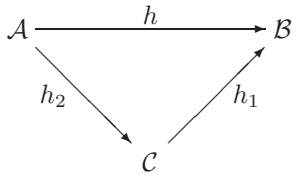
Proof:
This is a consequence of the fact that, given a universe $X \in |\mathbf{Set}|$, there exists only a set of $\mathcal{L}$-algebraic structures on X and only a set of subsets and, therefore, also of triples of subsets, of X. A similar reasoning yields finiteness in case X is finite, provided that $\mathcal{L}$ is finite. □

Moreover, it can be easily seen that, $\mathcal{S}$-$\mathbf{Str}_X$ is a partially ordered set and, also, that, as partially ordered sets, $\mathcal{S}$-$\mathbf{Str}_X$ and $\mathcal{S}$-$\mathbf{Str}_Y$ are isomorphic, whenever there is a bijection between the underlying universes X and Y.

Corollary 30 *For every set X, the pre-ordered set $\mathcal{S}$-$\mathbf{Str}_X$ is a partially ordered set and every bijection $f : X \to Y$, induces an isomorphism $\mathcal{S}$-$\mathbf{Str}_X \cong \mathcal{S}$-$\mathbf{Str}_Y$.*

Finally, in Proposition 31, one of the key results of this section that will be used in Section 8 to provide characterizations of subdirectly irreducible structures, it is asserted that, similarly with the case of arbitrary concrete categories (see Section 1 of [17]), every secrecy homomorphism admits a subobject decomposition into an onto set mapping followed by a subobject in $\mathcal{S}$-$\mathbf{Str}$.

Proposition 31 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_\mathcal{A}, B_\mathcal{A}, S_\mathcal{A}\rangle, \mathcal{B} = \langle \mathbf{B}, K_\mathcal{B}, B_\mathcal{B}, S_\mathcal{B}\rangle$ two $\mathcal{S}$-secrecy structures. For every secrecy homomorphism $h : \mathcal{A} \to \mathcal{B}$, there is an $\mathcal{S}$-secrecy structure $\mathcal{C}$ and a decomposition $h = h_1 \circ h_2$,*



called a **subobject decomposition**, *with $h_1 : \mathcal{C} \to \mathcal{B}$ a subobject in $\mathcal{S}$-$\mathbf{Str}$ and $h_2 : A \to C$ onto.*

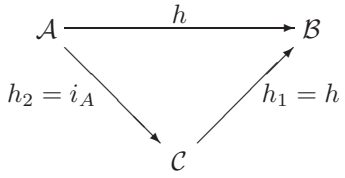
Proof:
Let $h : \mathcal{A} \to \mathcal{B}$ be a secrecy homomorphism. Since it is an algebra homomorphism $h : \mathbf{A} \to \mathbf{B}$, there exists, by the Homomorphism Theorem of universal algebra, a surjective algebra homomorphism $h_2 : \mathbf{A} \to \mathbf{A}/\mathrm{Ker}(h)$, with $h_2(a) = a/\mathrm{Ker}(h)$, for all $a \in A$, and an algebra monomorphism $h_1 : \mathbf{A}/\mathrm{Ker}(h) \to \mathbf{B}$, with $h_1(a/\mathrm{Ker}(h)) = h(a)$, for all $a \in A$. Define on $A/\mathrm{Ker}(h)$ the sets

$$K_\mathcal{C} = h_1^{-1}(K_\mathcal{B}), \quad B_\mathcal{C} = h_1^{-1}(B_\mathcal{B}), \quad S_\mathcal{C} = h_1^{-1}(S_\mathcal{B}).$$

Let $\mathcal{C} = \langle \mathbf{A}/\mathrm{Ker}(h), K_{\mathcal{C}}, B_{\mathcal{C}}, S_{\mathcal{C}} \rangle$. Obviously, $h_2 : A \to A/\mathrm{Ker}(h)$ is an onto set function and $h_1 : \mathcal{C} \to \mathcal{B}$, is a well-defined secrecy homomorphism that is also a subobject in $\mathcal{S}$-**Str**. Indeed, if $a \in A$, we have $a/\mathrm{Ker}(h) \in K_{\mathcal{C}}$ iff $a/\mathrm{Ker}(h) \in h_1^{-1}(K_{\mathcal{B}})$ iff $h_1(a/\mathrm{Ker}(h)) \in K_{\mathcal{B}}$. One may show similarly that $h_1^{-1}(B_{\mathcal{B}}) = B_{\mathcal{C}}$ and $h_1^{-1}(S_{\mathcal{B}}) = S_{\mathcal{C}}$. By Proposition 7, this shows that h_1 is a subobject in $\mathcal{S}$-**Str**. □

In the following corollary, it is asserted that, if one insists that the onto mapping $h_2 : A \to C$ in the subobject decomposition of an injective secrecy morphism $h : \mathcal{A} \to \mathcal{B}$ be such that $h_2 = i_A : \mathcal{A} \prec \mathcal{C}$, then the subobject decomposition is unique. This is the analog of Proposition 1.6 of [17] for $\mathcal{S}$-secrecy structures.

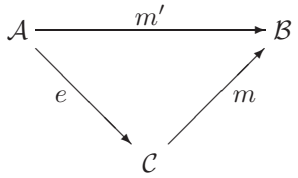
Corollary 32 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle, \mathcal{B} = \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}} \rangle$ two $\mathcal{S}$-secrecy structures. For every injective secrecy homomorphism $h : \mathcal{A} \to \mathcal{B}$, there exists exactly one subobject decomposition $h = h_1 \circ h_2$, such that $h_2 = i_A : \mathcal{A} \prec \mathcal{C}$:*



Proof:
Obviously, the set mappings satisfying the hypothesis are unique and are given by $h_1 = h$ and $h_2 = i_A$. Since h_1 is supposed to be a subobject in $\mathcal{S}$-**Str**, we must have $\mathcal{C} = \langle \mathbf{A}, h^{-1}(K_{\mathcal{B}}), h^{-1}(B_{\mathcal{B}}), h^{-1}(S_{\mathcal{B}}) \rangle$. This also satisfies $i_A : \mathcal{A} \prec \mathcal{C}$, since we have $a \in K_{\mathcal{A}}$ implies $h(a) \in K_{\mathcal{B}}$ and, therefore, $a \in h^{-1}(K_{\mathcal{B}})$ and, similarly, for the browsable filters and the secret sets. □

Lemma 34 shows that the existence of a subobject $m : \mathcal{A} \to \mathcal{B}$ between two finite $\mathcal{S}$-secrecy structures, such that $\mathcal{A} \prec \mathcal{B}$ forces the two structures to be identical. For its proof, we will employ Proposition 33.

Proposition 33 *Let $\mathcal{S}$ be a deductive system and $m' : \mathcal{A} \to \mathcal{B}$, $e : \mathcal{A} \to \mathcal{C}$ and $m : \mathcal{C} \to \mathcal{B}$ secrecy homomorphisms, such that*



*$m' = m \circ e$ is a subobject in $\mathcal{S}$-**Str** and e is onto. Then e is a secrecy isomorphism.*

Proof:

Let $e' : C \to A$ be such that $e \circ e' = i_C$. Then $m' \circ e' \circ e = m \circ e \circ e' \circ e = m \circ e$, whence, since e is onto, we get that $m' \circ e' = m$. Thus, since m' is a subobject and $m : \mathcal{C} \to \mathcal{B}$ is a secrecy homomorphism, $e' : \mathcal{C} \to \mathcal{A}$ must also be a secrecy homomorphism. But $e \circ e' = i_C$ and, because $m' \circ e' \circ e = m \circ e = m'$, it is also the case that $e' \circ e = i_A$, showing that e is a secrecy isomorphism. □

Lemma 34 *Let $\mathcal{S}$ be a deductive system. If X is a finite set, $\mathcal{A}, \mathcal{B} \in \mathcal{S}\text{-}\mathbf{Str}_X$, with $\mathcal{A} \prec \mathcal{B}$, and there exists a subobject $m : \mathcal{A} \to \mathcal{B}$ then $\mathcal{A} = \mathcal{B}$.*

Proof:
Denote by $i : \mathcal{A} \prec \mathcal{B}$ the secrecy homomorphism, that is identical with i_X on X. By Proposition 33, m is a secrecy isomorphism. Set $h = m^{-1} \circ i : \mathcal{A} \to \mathcal{A}$. This is a monomorphism. Taking into account the fact that X is finite, we conclude that $h^n = i_{\mathcal{A}}$, for some $n > 0$. Thus, h is an isomorphism, showing that i is an isomorphism by Proposition 28. □

Proposition 35, an analog of Proposition 1.8 of [17] for $\mathcal{S}$-secrecy structures, relates subobjects of direct products of secrecy structures built on the diagonal with meets in the partially ordered class $\mathcal{S}\text{-}\mathbf{Str}_X$, for a given set X.

Proposition 35 *Let $\mathcal{S}$ be a deductive system.*

1. *If $\mathcal{A} = \bigwedge_{i \in I} \mathcal{A}_i$ is a meet in $\mathcal{S}\text{-}\mathbf{Str}_X$, then $m : \mathcal{A} \to \prod_{i \in I} \mathcal{A}_i$ defined by $m(a) = \langle a : i \in I \rangle$, for all $a \in X$, is a subobject in $\mathcal{S}\text{-}\mathbf{Str}$.*
2. *If $\mathcal{A}_i, i \in I$, are in $\mathcal{S}\text{-}\mathbf{Str}_X$ and the diagonal mapping $d : X \to X^I$ carries a subobject $m : \mathcal{A} \to \prod_{i \in I} \mathcal{A}_i$ in $\mathcal{S}\text{-}\mathbf{Str}$, then $\mathcal{A} = \bigwedge_{i \in I} A_i$.*

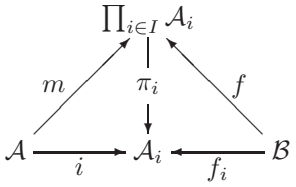
Proof:

1. Corollary 32 may be used to prove this part (see proof of Proposition 1.8 of [17]). Alternatively, it is easy to see that $m : \mathbf{A} \to \prod_{i \in I} \mathbf{A}_i$ is a subobject in $\mathcal{L}\text{-}\mathbf{Alg}$ and, also, that, for all $a \in A$, we have

$$\begin{array}{lll} a \in m^{-1}(K_{\prod_{i \in I} \mathcal{A}_i}) & \text{iff} & m(a) \in K_{\prod_{i \in I} \mathcal{A}_i} \\ & \text{iff} & \langle a : i \in I \rangle \in \prod_{i \in I} K_{\mathcal{A}_i} \\ & \text{iff} & a \in K_{\mathcal{A}_i}, i \in I, \\ & \text{iff} & a \in K_{\bigwedge_{i \in I} \mathcal{A}_i} \\ & \text{iff} & a \in K_{\mathcal{A}}. \end{array}$$

   and, similarly, for the browsable filters and the secret sets.

2. Let $m : \mathcal{A} \to \prod_{i \in I} \mathcal{A}_i$ be the subobject mapping that acts like the diagonal on X. Let, also, $f_i : \mathcal{B} \prec \mathcal{A}_i$ and set $f = \prod_{i \in I} f_i$ (see diagram below).



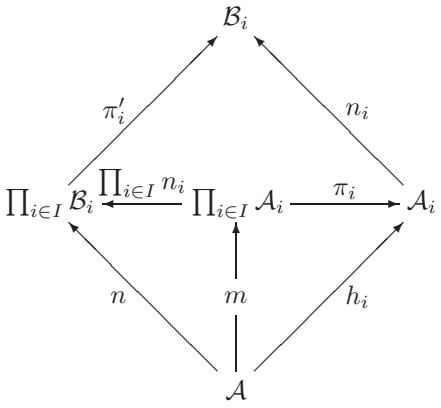
Then, in **Set**, we have $\pi_i \circ f = i_X = \pi_i \circ m$, for all $i \in I$, whence $f = m = m \circ i_X$. Thus, since m is a subobject, we get that $i_X : \mathcal{B} \to \mathcal{A}$ is a secrecy homomorphism, showing that $\mathcal{B}$ is the meet of the $\mathcal{A}_i$ in $\mathcal{S}$-$\mathbf{Str}_X$. □

Finally, we conclude this section by showing that, every subobject $n : \mathcal{A} \to \prod_{i\in I} \mathcal{B}_i$ may be decomposed into a subobject of a product having surjective components (i.e., a subdirect product, as defined in Definition 37) followed by a product of subobjects.

Proposition 36 *Let $\mathcal{S}$ be a deductive system and $n : \mathcal{A} \to \prod_{i\in I} \mathcal{B}_i$ be a subobject in $\mathcal{S}$-**Str**. Then, there exists subobjects $n_i : \mathcal{A}_i \to \mathcal{B}_i$ and $m : \mathcal{A} \to \prod_{i\in I} \mathcal{A}_i$ in $\mathcal{S}$-**Str**, such that $n = \prod_{i\in I} n_i \circ m$ and $\pi_i \circ m$ is onto.*

Proof:

Let $\pi'_i : \prod_{i\in I} \mathcal{B}_i \to \mathcal{B}_i$, $i \in I$, be the projection secrecy homomorphisms and $\pi'_i \circ n = n_i \circ h_i$ subobject decompositions, for all $i \in I$ (see diagram below).



We get

$$\begin{aligned} \pi'_i \circ \prod_{i\in I} n_i \circ m &= n_i \circ \pi_i \circ m \\ &= n_i \circ h_i \\ &= \pi'_i \circ n, \end{aligned}$$

whence $\prod_{i\in I} n_i \circ m = n$, showing that m is a subobject, since n is, by hypothesis, a subobject (see Proposition 1.2 (2) of [17]). □

Summarizing, in this section, we have studied properties related to regular concrete categories as applied to the category $\mathcal{S}$-**Str** of $\mathcal{S}$-secrecy structures. In Proposition 26 it was shown that the forgetful functor from the category of $\mathcal{S}$-secrecy structures to the category of small sets preserves all small limits. Given a set X, the pre-ordered class $\mathcal{S}$-$\mathbf{Str}_X$ of all $\mathcal{S}$-secrecy structures with universe X was defined and in Proposition 29 it was asserted that this class is finite, whenever X and $\mathcal{L}$ are finite. Moreover, in Corollary 30 it was shown that it is actually a partially ordered class. The existence of the key notion of subobject decomposition of a secrecy homomorphism was the content of Proposition 31 and Corollary 32 showed that, in case the homomorphism is

injective, the decomposition has a unique canonical representative. Proposition 35 established some useful connections between subobjects of direct products of $\mathcal{S}$-secrecy structures with universe X, supported by the diagonal mapping, and meets in the partially ordered set $\mathcal{S}\text{-}\mathbf{Str}_X$. Finally, in Proposition 36 the decomposition of an arbitrary subobject of a direct product structure into a subdirect product and a product of subobjects was obtained. All the properties studied in this section are known to hold for arbitrary regular concrete categories (see, e.g., [17]).

7 Subdirect Products and Irreducibility

In the remainder of the paper, we study subdirect products, subdirect representations and subdirect irreducibility for $\mathcal{S}$-secrecy structures. We draw from relevant results in universal algebra as well as from results that hold for arbitrary regular concrete categories. We start by defining subdirect products for $\mathcal{S}$-secrecy structures.

Definition 37 *Let $\mathcal{S}$ be a deductive system. An $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ is a* (**strict**) **subdirect product** *of an indexed family $\{\mathcal{A}_i\}_{i \in I}$ of $\mathcal{S}$-secrecy structures if*

1. *$\mathcal{A} \leq \prod_{i \in I} \mathcal{A}_i$, i.e., $\mathcal{A}$ is a secrecy substructure of the product $\prod_{i \in I} \mathcal{A}_i$;*
2. *$\pi_i : \mathcal{A} \to \mathcal{A}_i$ is a (strict) surjective secrecy homomorphism, for all $i \in I$, where $\pi_i : \prod_{i \in I} \mathcal{A}_i \to \mathcal{A}$ is the projection secrecy homomorphism.*

A secrecy embedding $h : \mathcal{A} \to \prod_{i \in I} \mathcal{A}_i$ is a (**strict**) **subdirect embedding** if $h(\mathcal{A})$ is an $\mathcal{S}$-secrecy structure and a (strict) subdirect product of the secrecy structures $\mathcal{A}_i$. It is shown, next, inspired by Lemma II.8.2 of [9], that given a collection of secrecy congruences on an $\mathcal{S}$-secrecy structure $\mathcal{A}$, whose intersection is the identity, one may define a strict subdirect embedding of $\mathcal{A}$ into the product of the quotient secrecy structures.

Lemma 38 *Let $\mathcal{S}$ be a deductive system, $\mathcal{A}$ an $\mathcal{S}$-secrecy structure and θ_i, $i \in I$, secrecy congruences on $\mathbf{A}$, such that $\bigcap_{i \in I} \theta_i = \Delta_{\mathcal{A}}$. Then $e : \mathcal{A} \to \prod_{i \in I} \mathcal{A}_i$, defined by $e(a) = \langle a/\theta_i : i \in I \rangle$, is a strict subdirect embedding of secrecy structures.*

Proof:
The fact that $e : \mathbf{A} \to \prod_{i \in I} \mathbf{A}/\theta_i$ is a subdirect embedding of $\mathcal{L}$-algebras is given by the corresponding universal algebraic result (see Lemma II.8.2 of [9]). Moreover, by the compatibility of θ_i with each of the theories and the secrecy sets, we get $e^{-1}(K_{\prod_{i \in I} \mathcal{A}/\theta_i}) = e^{-1}(\prod_{i \in I} K_{\mathcal{A}/\theta_i}) = e^{-1}(\prod_{i \in I} K_{\mathcal{A}}/\theta_i) = K_{\mathcal{A}}$ and, similarly, $e^{-1}(B_{\prod_{i \in I} \mathcal{A}/\theta_i}) = B_{\mathcal{A}}$ and $e^{-1}(S_{\prod_{i \in I} \mathcal{A}/\theta_i}) = S_{\mathcal{A}}$. □

An $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ is **(finitely) subdirectly irreducible**, denoted by (FSI) SI, if, for every subdirect embedding $n : \mathcal{A} \to$

$\prod_{i\in I}\mathcal{A}_i$, (I finite), at least one of $\pi_i \circ n : \mathcal{A} \to \mathcal{A}_i$ is a secrecy isomorphism. Moreover, $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle$ is **strictly (finitely) subdirectly irreducible**, denoted by (SFSI) SSI, if, for every strict subdirect embedding $n : \mathcal{A} \to \prod_{i\in I}\mathcal{A}_i$, (I finite), at least one of $\pi_i \circ n : \mathcal{A} \to \mathcal{A}_i$ is a secrecy isomorphism.

The following theorem characterizes strictly subdirectly irreducible $\mathcal{S}$-secrecy structures $\mathcal{A}$ by means of the existence of a monolith in the lattice of all secrecy congruences $\mathbf{SCon}(\mathcal{A})$. This result generalizes Theorem II.8.4 of [9], an analog characterizing subdirectly irreducible universal algebras.

Theorem 39 *Let $\mathcal{S}$ be a deductive system. An $\mathcal{S}$-secrecy structure $\mathcal{A}$ is strictly subdirectly irreducible iff $\mathcal{A}$ is trivial or there exists a minimum secrecy congruence θ in $\mathrm{SCon}(\mathcal{A})\backslash\{\Delta_{\mathcal{A}}\}$. This minimum element $\bigcap(\mathrm{SCon}(\mathcal{A})\backslash\{\Delta_{\mathcal{A}}\})$ is a principal secrecy congruence of $\mathcal{A}$, which is a monolith in the lattice of all secrecy congruences of $\mathcal{A}$.*

Proof:

If $\mathcal{A}$ is not trivial and $\mathrm{SCon}(\mathcal{A})\backslash\{\Delta_{\mathcal{A}}\}$ has no minimum element, then the natural map $e : \mathcal{A} \to \prod_{i\in I}\mathcal{A}/\theta_i$, defined in Lemma 38, is a subdirect embedding. Since $\mathcal{A} \to \mathcal{A}/\theta$ is not injective for any $\theta \in I$, it follows that $\mathcal{A}$ is not strictly subdirectly irreducible.

If $\mathcal{A}$ is trivial and $e : \mathcal{A} \to \prod_{i\in I}\mathcal{A}_i$ is a strict subdirect embedding then, it can be easily checked that at least one of the factors has to be an isomorphic trivial $\mathcal{S}$-secrecy algebra to the original, which shows that $\mathcal{A}$ is strictly subdirectly irreducible. So suppose that $\mathcal{A}$ is not trivial and let $e : \mathcal{A} \to \prod_{i\in I}\mathcal{A}_i$ be a strict subdirect embedding. Consider $\theta = \bigcap(\mathrm{SCon}(\mathcal{A})\backslash\{\Delta_{\mathcal{A}}\}) \neq \Delta_{\mathcal{A}}$. Choose $\langle a, b\rangle \in \theta$, with $a \neq b$. For some $i \in I$, $e(a)_i \neq e(b)_i$. Hence $\langle a, b\rangle \notin \mathrm{Ker}(\pi_i \circ e)$. Thus $\theta \not\subseteq \mathrm{Ker}(\pi_i \circ e)$. Since $\mathrm{Ker}(\pi_i \circ e) \in \mathrm{SCon}(\mathcal{A})$, this implies $\mathrm{Ker}(\pi_i \circ e) = \Delta_{\mathcal{A}}$ and, therefore, $\pi_i \circ e : \mathcal{A} \to \mathcal{A}_i$ is a secrecy isomorphism. Consequently $\mathcal{A}$ is strictly subdirectly irreducible.

Now, if $\mathrm{SCon}(\mathcal{A})\backslash\{\Delta_{\mathcal{A}}\}$ has a minimum element θ, then, for any $\langle a, b\rangle \in \theta$, with $a \neq b$, we have that the secrecy congruence $\Theta^{\mathcal{A}}(a, b)$ generated by $\langle a, b\rangle$ satisfies $\Theta^{\mathcal{A}}(a, b) \subseteq \theta$ and, hence, $\theta = \Theta^{\mathcal{A}}(a, b)$. □

We define, next, the notion of weak subdirect irreducibility. Informally speaking, an $\mathcal{S}$-secrecy structure $\mathcal{A}$ is weakly subdirectly irreducible if the class of all structures that do not admit $\mathcal{A}$ as a subobject is closed under non-empty products. Note here, the addition of the condition that products be nonempty, that was not needed in the case of arbitrary regular concrete categories (see, e.g., Section 2 of [17], modulo a slightly modified notation). It will then be shown that, for finite $\mathcal{S}$-secrecy structures, subdirect irreducibility is equivalent to weak subdirect irreducibility, an analog for $\mathcal{S}$-secrecy structures of Lemma 2.3 of [17].

Let $\mathcal{A}$ be an $\mathcal{S}$-secrecy structure. Denote by $\mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$ the full subcategory of $\mathcal{S}$-$\mathbf{Str}$ generated by all objects $\mathcal{B}$, such that there does not exist a subobject $\mathcal{A} \to \mathcal{B}$. An $\mathcal{S}$-secrecy structure $\mathcal{A}$ is **weakly** (**finitely**) **subdirectly irreducible** (WSI (WFSI))) if $\mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$ is closed under nonempty (finite) products.

Lemma 40 *Let $\mathcal{S}$ be a deductive system. A finite $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ is* SI (FSI) *iff it is* WSI (WFSI).

Proof:

Suppose, first, that $\mathcal{A}$ is subdirectly irreducible. Let $\mathcal{B}_i, i \in I \neq \emptyset$, be a collection of $\mathcal{S}$-secrecy structures in $\mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$. Assume that $\prod_{i\in I} \mathcal{B}_i$ is not in $\mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$. Thus, there exists a subobject $n : \mathcal{A} \to \prod_{i\in I} \mathcal{B}_i$. Consider the secrecy morphism $m : \mathcal{A} \to \prod_{i\in I} \mathcal{A}_i$, given in Proposition 36 (using the same notation). Since $\mathcal{A}$ is subdirectly irreducible, there exists $i_0 \in I$, such that $\pi_{i_0} \circ m : \mathcal{A} \to \mathcal{A}_{i_0}$ is a secrecy isomorphism. But, then, $n_{i_0} \circ \pi_{i_0} \circ m : \mathcal{A} \to \mathcal{B}_{i_0}$ is a subobject, which contradicts the fact that $\mathcal{B}_{i_0}$ is in $\mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$.

Suppose, conversely, that $\mathcal{S}$-$\mathbf{Str}_{\neg_{\mathcal{A}}}$ is closed under nonempty products. Let $m : \mathcal{A} \to \prod_{i\in I} \mathcal{A}_i$ be a subobject, such that $\pi_i \circ m : \mathcal{A} \to \mathcal{A}_i$ is onto, for every $i \in I$. Since $\prod_{i\in I} \mathcal{A}_i$ is not in $\mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$ (due to the fact that m is a subobject), there exists an $i_0 \in I$, such that $\mathcal{A}_{i_0}$ is not in $\mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$ either. Thus, there exists a subobject $n : \mathcal{A} \to \mathcal{A}_{i_0}$. Since $\pi_{i_0} \circ m : \mathcal{A} \to \mathcal{A}_{i_0}$ is onto, $|A| = |A_{i_0}|$, and, this being finite, n is onto. Thus, it is an isomorphism. Set $f = n^{-1} \circ \pi_{i_0} \circ m : \mathcal{A} \to \mathcal{A}$ and observe that this is injective and, for sufficiently large k, $f^k = i_A$. Thus, f is an isomorphism and, hence, $\pi_{i_0} \circ m = n \circ f$ is also an isomorphism. □

In Lemma 41, it is shown that, whenever a finite $\mathcal{S}$-secrecy structure is embeddable into a direct product of structures, then , it is also embeddable into a product consisting only of finitely many of the factors.

Lemma 41 *Let $\mathcal{S}$ be a deductive system, $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ be a finite $\mathcal{S}$-secrecy structure and assume that $m : \mathcal{A} \to \prod_{i\in I} \mathcal{A}_i$ is a subobject in $\mathcal{S}$-$\mathbf{Str}$. Then, there exists a finite $J \subseteq I$ and a subobject $n : \mathcal{A} \to \prod_{j\in J} \mathcal{A}_j$.*

Proof:

For every pair $a, b \in A$, with $a \neq b$, we have that $m(a) \neq m(b)$. Thus, there exists $i_{a,b} \in I$, such that $m(a)(i_{a,b}) \neq m(b)(i_{a,b})$. Moreover, for every $a \notin K_{\mathcal{A}}$, we have $m(a) \notin \prod_{i\in I} K_{\mathcal{A}_i}$, whence, there exists k_a, such that $m(a)(k_a) \notin K_{\mathcal{A}_{k_a}}$. Similarly, for $a \notin B_{\mathcal{A}}$, we get an $l_a \in I$, such that $m(a)(l_a) \notin B_{\mathcal{A}_{l_a}}$ and, for every $a \notin S_{\mathcal{A}}$, we get an $s_a \in I$, such that $m(a)(s_a) \notin S_{\mathcal{A}_{s_a}}$. Let $J = \{i_{a,b} : a \neq b\} \cup \{k_a; a \notin K_{\mathcal{A}}\} \cup \{l_a : a \notin B_{\mathcal{A}}\} \cup \{s_a : a \notin S_{\mathcal{A}}\}$. Notice that $J \subseteq I$ is finite. Consider the mapping $n : A \to \prod_{j\in J} A_j$, defined by $n(c)(j) = m(c)(j)$, for all $c \in A$. This map induces a subobject $n : \mathbf{A} \to \prod_{j\in J} \mathbf{A}_j$ in $\mathcal{L}$-$\mathbf{Alg}$. To see that this is also a subobject in $\mathcal{S}$-$\mathbf{Str}$, notice that

$$\begin{array}{rcl} K_{\mathcal{A}} & = & m^{-1}(K_{\prod_{i\in I} \mathcal{A}_i}) \\ & = & \bigcap_{i\in I} (\pi_i \circ m)^{-1}(K_{\mathcal{A}_i}) \\ & \subseteq & \bigcap_{j\in J} (\pi_j \circ n)^{-1}(K_{\mathcal{A}_j}) \\ & = & n^{-1}(\prod_{j\in J} K_{\mathcal{A}_j}) \\ & = & n^{-1}(K_{\prod_{j\in J} \mathcal{A}_j}). \end{array}$$

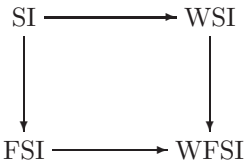
On the other hand, if $a \notin K_{\mathcal{A}}$, then $m(a) \notin K_{\mathcal{A}_{k_a}}$, whence $a \notin n^{-1}(K_{\prod_{j\in J} \mathcal{A}_j})$. Thus, we get that $K_{\mathcal{A}} = n^{-1}(K_{\prod_{j\in J} \mathcal{A}_j})$. Similarly, one sees that $B_{\mathcal{A}} = n^{-1}(B_{\prod_{j\in J} \mathcal{A}_j})$ and $S_{\mathcal{A}} = n^{-1}(S_{\prod_{j\in J} \mathcal{A}_j})$. □

Lemmas 40 and 41 establish the following corollary asserting the equivalence for finite $\mathcal{S}$-secrecy structures of being subdirectly irreducible, finitely subdirectly irreducible and weakly (finitely) subdirectly irreducible.

Corollary 42 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ a finite $\mathcal{S}$-secrecy structure. Then, the following statements are equivalent:*

1. *$\mathcal{A}$ is subdirectly irreducible;*
2. *$\mathcal{A}$ is finitely subdirectly irreducible;*
3. *$\mathcal{A}$ is weakly (finitely) subdirectly irreducible.*

In general, the following diagram of implications holds between the four notions of subdirect irreducibility (See Remark 2.4 of [24] for a similar diagram in the case of semiregular categories; be aware, however, of slight modifications in the definitions involved.):



The two horizontal implications can be shown exactly as was the left-to-right implication in the proof of Theorem 40.

Finally, we conclude this section by providing a strict analog of Birkhoff's Subdirect Representation Theorem for $\mathcal{S}$-secrecy structures. The original version [3] states that every algebra is isomorphic to a subdirect product of subdirectly irreducible algebras. We also present in Proposition 45 an analog of Proposition 2.6 of [17] for $\mathcal{S}$-secrecy structures, which states that every finite $\mathcal{S}$-secrecy structure is expressible as a subdirect product of finitely many subdirectly irreducible structures.

Theorem 43 (Birkhoff's Analog) *Let $\mathcal{S}$ be a deductive system. Every $\mathcal{S}$-secrecy structure $\mathcal{A}$ is isomorphic to a strict subdirect product of strictly subdirectly irreducible $\mathcal{S}$-secrecy structures (which are strict homomorphic images of $\mathcal{A}$).*

Proof:

We know that all trivial structures are subdirectly irreducible. So we only need to condider the case of nontrivial $\mathcal{A}$. For $a, b \in A$, with $a \neq b$, we can find, using Zorn's lemma, a secrecy congruence $\theta_{a,b}$ of $\mathcal{A}$, which is maximal with respect to the property $\langle a, b \rangle \notin \theta_{a,b}$. As $\bigcap_{a \neq b} \theta_{a,b} = \Delta_{\mathcal{A}}$, we can apply Lemma 38 to show that $\mathcal{A}$ is strictly subdirectly embeddable in the product of the indexed family of $\mathcal{S}$-secrecy structures $\{\mathcal{A}/\theta_{a,b}\}_{a \neq b}$. It suffices now to show that each of these secrecy structures is strictly subdirectly irreducible. If not, then there exists a minimum congruence $\theta/\theta_{a,b}$ in $\mathrm{SCon}(\mathcal{A}/\theta_{a,b}) \backslash \{\Delta_{\mathcal{A}/\theta_{a,b}}\}$,

such that $\theta/\theta_{a,b} = \bigcap(\mathrm{SCon}(\mathcal{A}/\theta_{a,b})\backslash\{\Delta_{\mathcal{A}/\theta_{a,b}}\})$. But, then, by Theorem 25, there exists a minimum congruence $\theta \in \mathrm{SCon}(\mathcal{A})$, such that $\theta_{a,b} \subsetneqq \theta$. By the maximality of $\theta_{a,b}$ with respect to $\langle a, b\rangle \notin \theta_{a,b}$, this implies that $\langle a, b\rangle \in \theta$. Thus, since $\theta \in \mathrm{SCon}(\mathcal{A})$, i.e., $\theta \subseteq \Omega(\mathcal{A})$, we get that $\langle a, b\rangle \in \Omega(\mathcal{A})$. But then $\Theta^{\mathcal{A}}(a, b) \vee^{\mathcal{A}} \theta_{a,b}$, the secrecy join of the secrecy congruence $\Theta^{\mathcal{A}}(a, b)$, generated by $\langle a, b\rangle$, and of $\theta_{a,b}$, is the smallest secrecy congruence in $[\theta_{a,b}, \Omega(\mathcal{A})]\backslash\{\theta_{a,b}\}$, showing that $\mathcal{A}/\theta_{a,b}$ is subdirectly irreducible. □

Combining with Lemma 41, we get immediately the following

Corollary 44 *Let $\mathcal{S}$ be a deductive system. Every finite $\mathcal{S}$-secrecy structure $\mathcal{A}$ is isomorphic to a strict subdirect product of finitely many strictly subdirectly irreducible $\mathcal{S}$-secrecy structures.*

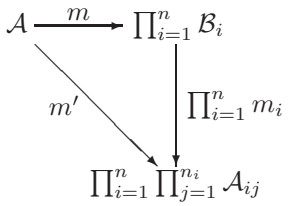
Indeed, using Lemma 41, any strict subdirect embedding of $\mathcal{A}$ into a direct product of strictly subdirectly irreducible $\mathcal{S}$-secrecy structures may be reduced to a subdirect embedding into the product of finitely many of these structures while retaining the property of being strict.

Proposition 45 *Let $\mathcal{S}$ be a deductive system. Every finite $\mathcal{S}$-secrecy structure $\mathcal{A}$ is isomorphic to a subdirect product of finitely many subdirectly irreducible $\mathcal{S}$-secrecy structures.*

Proof:

This proof uses the technique used for the proof of Proposition 45 of [17], which addresses the finite case in an arbitrary regular concrete category that is closed under finite products.

Suppose that the set of all finite secrecy structures that are not representable as subdirect products of finite subdirectly irreducible secrecy structures is nonempty. Then, consider a partial ordering of the finite $\mathcal{S}$-secrecy structures, such that $\langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle \leq \langle \mathbf{B}, K_{\mathcal{B}}, B_{\mathcal{B}}, S_{\mathcal{B}}\rangle$ iff $|A| \leq |B|, |K_{\mathcal{A}}| \leq |K_{\mathcal{B}}|, |B_{\mathcal{A}}| \leq |B_{\mathcal{B}}|$ and $|S_{\mathcal{A}}| \leq |S_{\mathcal{B}}|$. It is clear that there exists a $\leq$-minimal structure in the set of all finite structures that are not representable as subdirect products of finite subdirectly irreducible $\mathcal{S}$-secrecy structures that has minimum cardinality, call it $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}}\rangle$. Obviously, $\mathcal{A}$ cannot be itself subdirectly irreducible. Thus, there exists a subobject $m : \mathcal{A} \to \prod_{i=1}^{n} \mathcal{B}_i$, with $\pi_i \circ m : \mathcal{A} \to \mathcal{B}_i$ a surjective secrecy homomorphism that is not a secrecy isomorphism, for all $i = 1, \ldots, n$. Since $\mathcal{A}$ is $\leq$-minimal with respect to the property of being subdirectly representable, there exist subdirect products $m_i : \mathcal{B}_i \to \prod_{j=1}^{n_i} \mathcal{A}_{ij}$, with $\mathcal{A}_{ij}$ subdirectly irreducible and $\pi_{ij} \circ m_i$ onto, for every $i = 1, \ldots, n, j = 1, \ldots, n_i$. Consider $m' = \prod_{i=1}^{n} m_i \circ m : \mathcal{A} \to \prod_{i=1}^{n} \prod_{j=1}^{n_i} \mathcal{A}_{ij}$.



We get that m' is a subobject and $\pi_{ij} \circ \pi'_i \circ m' = \pi_{ij} \circ m_i \circ \pi_i \circ m$ is onto and $\mathcal{A}$ is subdirectly representable. □

Summarizing, in this section we introduced and studied subdirect products of $\mathcal{S}$-secrecy structures. In Lemma 38, it was shown that a collection of secrecy congruences on an $\mathcal{S}$-secrecy structure, whose meet is the identity, induces a subdirect embedding of the structure into the product of the corresponding quotient secrecy structures. After defining subdirectly irreducible and strictly subdirectly irreducible $\mathcal{S}$-secrecy structures, a characterization of the latter was provided in Theorem 39 in terms of the existence of a minimum secrecy congruence different from the identity in the lattice of secrecy congruences. Furthermore, the notion of a weakly subdirectly irreducible $\mathcal{S}$-secrecy structure $\mathcal{A}$ was defined in terms of the closure under nonempty products of the full subcategory of structures with objects those structures that do not admit $\mathcal{A}$ as a subobject. In Lemma 40, it was shown that subdirect irreducibility and weak subdirect irreducibility coincide for finite $\mathcal{S}$-secrecy structures. Finally, in Theorem 43 an strict analog of Birkhoff's Subdirect Representation Theorem was proven and in Proposition 45 a similar result, asserting that every finite $\mathcal{S}$-secrecy structure may be expressed as a subdirect product of finitely many subdirectly irreducible structures, was given.

8 Subdirectly Irreducibles

In this section, our goal is to provide some alternative characterizations of subdirect irreducibility. We start by first introducing the notions of a maximal and of a weakly maximal $\mathcal{S}$-secrecy structures.

An $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ in $\mathcal{S}$-$\mathbf{Str}_X$ is **maximal** if it is maximal in $\mathcal{S}$-$\mathbf{Str}_X$. It is **weakly maximal** if, for all $\mathcal{B} \in \mathcal{S}$-$\mathbf{Str}_X$, such that $\mathcal{A} \prec \mathcal{B}$, there exists a subobject $m : \mathcal{A} \rightarrowtail \mathcal{B}$.

Next, meet irreducible and weakly meet irreducible $\mathcal{S}$-secrecy structures are defined.

An $\mathcal{S}$-secrecy structure $\mathcal{A}$ in $\mathcal{S}$-$\mathbf{Str}_X$ is said to be **(finitely) meet irreducible** if $\mathcal{A} = \bigwedge_{i \in I} \mathcal{A}_i$ (I finite) implies that $\mathcal{A} = \mathcal{A}_i$, for some $i \in I$. It is said to be **weakly (finitely) meet irreducible** if $\mathcal{A} = \bigwedge_{i \in I} \mathcal{A}_i$ (I finite) implies that there exists an $i \in I$ and a subobject $m : \mathcal{A} \rightarrowtail \mathcal{A}_i$.

Finally, the notion of a monomorphic system in $\mathcal{S}$-$\mathbf{Str}$ is defined. Monomorphic systems will be used in Theorem 46, an analog of the first part of Theorem 3.3 of [17], to characterize subdirectly irreducible maximal $\mathcal{S}$-secrecy structures. As the reader will notice, monomorphic systems are very closely related to the notion of separation of points, as given in Definition 16.

A **monomorphic system** in $\mathcal{S}$-$\mathbf{Str}$ is a system of secrecy homomorphisms $\{m_i : \mathcal{A} \rightarrowtail \mathcal{B}_i\}_{i \in I}$, such that, if $m_i(a) = m_i(b)$, for all $i \in I$, then $a = b$.

Theorem 46 *Let $\mathcal{S}$ be a deductive system. A maximal $\mathcal{S}$-secrecy structure $\mathcal{A} = \langle \mathbf{A}, K_{\mathcal{A}}, B_{\mathcal{A}}, S_{\mathcal{A}} \rangle$ is (finitely) subdirectly irreducible iff, for every (finite)*

monomorphic system $\{m_i : \mathcal{A} \to \mathcal{B}_i\}_{i\in I}$*, there exists* $i \in I$*, such that* m_i *is a monomorphism.*

Proof:

Suppose that $\mathcal{A}$ is maximal. We assume, first, that there exists a monomorphic system $\{m_i : \mathcal{A} \to \mathcal{B}_i\}_{i\in I}$, such that m_i is not a monomorphism for any $i \in I$, and, using Lemma 40, prove that $\mathcal{A}$ is not subdirectly irreducible. (Note that the direction used here does not require that $\mathcal{A}$ be finite.) If $\{m_i : \mathcal{A} \to \mathcal{B}_i\}_{i\in I}$ is a monomorphic system, such that no m_i is a monomorphism, we may assume, without loss of generality, by Corollary 32, that every m_i is onto. Define $m : \mathcal{A} \to \prod_{i=1}^{n} \mathcal{B}_i$ by $m(a) = \langle m_i(a) : i \in I\rangle$. This is a monomorphism. Moreover, by Proposition 31, we get a subobject decomposition $m = m' \circ m''$, with $m'' : \mathcal{A} \prec \mathcal{A}'$. Therefore, by the maximality of $\mathcal{A}$ in $\mathcal{S}$-$\mathbf{Str}_X$, $m'' = i_A$ and $m = m'$ is a subobject. Since, obviously, the $\mathcal{B}_i$'s are in $\mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$, we get, by Lemma 40, that $\mathcal{A}$ is not subdirectly irreducible.

If, on the other hand, $\mathcal{A}$ is not subdirectly irreducible, then, there exists a subdirect decomposition $m : \mathcal{A} \to \prod_{i=1}^{n} \mathcal{B}_i$, with $\pi_i \circ m$ not a secrecy isomorphism. Obviously, $\{\pi_i \circ m : \mathcal{A} \to \mathcal{B}_i\}_{i\in I}$ is a monomorphic system. If we assume that, for some $k \in I$, $\pi_k \circ m : \mathcal{A} \to \mathcal{B}_k$ is a monomorphism, then, we may take, without loss of generality, by Proposition 27, that $B_k = A$ and $\pi_k \circ m = i_A$. Thus, $A \prec B_k$ and $A \neq B_k$, which contradicts the maximality of $\mathcal{A}$. □

A similar theorem holds characterizing weakly subdirectly irreducible weakly maximal $\mathcal{S}$-structures in terms of monomorphic systems containing components that are themselves monomorphisms.

Theorem 47 *Let* $\mathcal{S}$ *be a deductive system and* $\mathcal{A}$ *be a weakly maximal secrecy structure. Then* $\mathcal{A}$ *is weakly (finitely) subdirectly irreducible iff for every (finite) monomorphic system* $\{m_i : \mathcal{A} \to \mathcal{B}_i\}_{i\in I}$*, there exists* $i \in I$*, such that* m_i *is a monomorphism.*

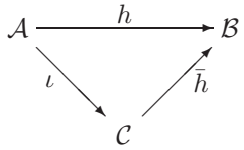
Proof:

Suppose that $\mathcal{A}$ is weakly maximal. Consider a monomorphic system $\{m_i : \mathcal{A} \to \mathcal{B}_i\}_{i\in I}$, such that for no $i \in I$ does there exist a subobject $n : \mathcal{A} \to \mathcal{B}_i$, i.e., such that $\mathcal{B}_i \in \mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$, for all $i \in I$. We assume without loss of generality, by Corollary 32, that every m_i is onto. Define, as in the proof of Theorem 46, $m : \mathcal{A} \to \prod_{i=1}^{n} \mathcal{B}_i$ by $m(a) = \langle m_i(a) : i \in I\rangle$. This is a monomorphism. Moreover, by Proposition 31, we get a subobject decomposition $m = m' \circ m''$, with $m'' : \mathcal{A} \prec \mathcal{A}'$. Therefore, by the weak maximality of $\mathcal{A}$, there exists a subobject $n'' : \mathcal{A} \to \mathcal{A}'$ and, hence, $m = m' \circ n'' : \mathcal{A} \to \prod_{i\in I} \mathcal{B}_i$ is a subobject. Thus, $\mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}$ is not closed under nonempty products, which shows that $\mathcal{A}$ is not weakly subdirectly irreducible.

If, on the other hand, $\mathcal{A}$ is not weakly subdirectly irreducible, then, there exists a collection $\mathcal{B}_i \in \mathcal{S}$-$\mathbf{Str}_{\neg\mathcal{A}}, i \in I$, and a subobject $m : \mathcal{A} \to \prod_{i\in I} \mathcal{B}_i$. Thus, $\{\pi_i \circ m : \mathcal{A} \to \mathcal{B}_i\}_{i\in I}$ is a monomorphic system whereas $\pi_i \circ m : \mathcal{A} \to \mathcal{B}_i$ is not a subobject for any $i \in I$. □

In Proposition 48, we establish a sufficient condition under which a non-maximal meet irreducible $\mathcal{S}$-secrecy structure is subdirectly irreducible. A similar sufficient condition under which a weakly meet-irreducible $\mathcal{S}$-secrecy structure is weakly subdirectly irreducible is established in Proposition 49.

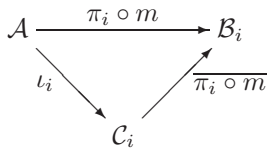
Proposition 48 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A}$ a non-maximal (finitely) meet irreducible $\mathcal{S}$-secrecy structure. Assume that, for all surjective $h : \mathcal{A} \to \mathcal{B}$, that is not a secrecy isomorphism, there exist $\iota : \mathcal{A} \prec \mathcal{C}$, $\mathcal{A} \neq \mathcal{C}$, and $\bar{h} : \mathcal{C} \to \mathcal{B}$, such that $\bar{h} \circ \iota = h$.*



Then $\mathcal{A}$ is (finitely) subdirectly irreducible.

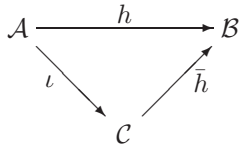
Proof:

Suppose that $\mathcal{A}$ is not subdirectly irreducible. Thus, there exists a subdirect representation $m : \mathcal{A} \to \prod_{i \in I} \mathcal{B}_i$, with no $\pi_i \circ m : \mathcal{A} \to \mathcal{B}_i$ a secrecy isomorphism. Therefore, since $\pi_i \circ m$ is surjective, for all $i \in I$, there exist, by hypothesis, $\iota_i : \mathcal{A} \prec \mathcal{C}_i$, $\mathcal{A} \neq \mathcal{C}_i$, and $\overline{\pi_i \circ m} : \mathcal{C}_i \to \mathcal{B}_i$,



such that $\overline{\pi_i \circ m} \circ \iota_i = \pi_i \circ m$. In that case $\mathcal{A} = \bigwedge_{i \in I} \mathcal{C}_i$ and $\mathcal{A} \neq \mathcal{C}_i$, for all $i \in I$, whence $\mathcal{A}$ is not meet irreducible. □

Proposition 49 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A}$ a weakly (finitely) meet irreducible $\mathcal{S}$-secrecy structure and assume that, for all $h : \mathcal{A} \to \mathcal{B}$, such that $\mathcal{B} \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, there exist $\iota : \mathcal{A} \prec \mathcal{C}$, $\mathcal{A} \neq \mathcal{C}$, with $\mathcal{C} \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, and $\bar{h} : \mathcal{C} \to \mathcal{B}$, such that $\bar{h} \circ \iota = h$.*

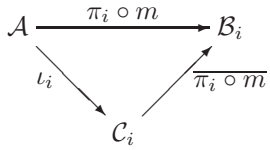


Then $\mathcal{A}$ is weakly (finitely) subdirectly irreducible.

Proof:

Suppose that $\mathcal{A}$ is not weakly subdirectly irreducible. Thus, there exist $\mathcal{B}_i \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, and a subobject $m : \mathcal{A} \to \prod_{i \in I} \mathcal{B}_i$. Consider $\pi_i \circ m : \mathcal{A} \to \mathcal{B}_i$,

where $\mathcal{B}_i \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, for every $i \in I$. By hypothesis, there exists $\iota_i : \mathcal{A} \prec \mathcal{C}_i$, $\mathcal{A} \neq \mathcal{C}_i$, $\mathcal{C}_i \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, and $\overline{\pi_i \circ m} : \mathcal{C}_i \to \mathcal{B}_i$,



such that $\overline{\pi_i \circ m} \circ \iota_i = \pi_i \circ m$. In that case $\mathcal{A} = \bigwedge_{i\in I} \mathcal{C}_i$ but for no $i \in I$, does there exist a subobject $\mathcal{A} \to \mathcal{C}_i$, whence $\mathcal{A}$ is not weakly meet irreducible. □

In Lemma 50 the converse of Proposition 48 is established. Namely, it is shown that a finitely subdirectly irreducible non-maximal $\mathcal{S}$-secrecy structure always satisfies the condition appearing in the hypothesis of Proposition 48. The analogous converse to Proposition 49 will also be shown to hold in Lemma 51, that follows.

Lemma 50 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A}$ be a non-maximal $\mathcal{S}$-secrecy structure. If $\mathcal{A}$ is finitely subdirectly irreducible, then, for every surjective secrecy homomorphism $h : \mathcal{A} \to \mathcal{B}$, that is not a secrecy isomorphism, there exists an $\iota : \mathcal{A} \prec \mathcal{C}, \mathcal{A} \neq \mathcal{C}$ and an $\bar{h} : \mathcal{C} \to \mathcal{B}$, such that $\bar{h} \circ \iota = h$.*

Proof:
Since $\mathcal{A}$ is not maximal, there exists $\iota : \mathcal{A} \prec \mathcal{C}$, with $\mathcal{A} \neq \mathcal{C}$. Suppose that a surjective $h : \mathcal{A} \to \mathcal{B}$, that is not an isomorphism, does not satisfy the property of the lemma. Define $m : \mathcal{A} \to \mathcal{B} \times \mathcal{C}$ by $m(a) = \langle h(a), \iota(a)\rangle$, for every $a \in A$. Then, there exists a subobject decomposition $m = m' \circ \iota'$, with $\iota' : \mathcal{A} \prec \mathcal{A}'$. By hypothesis, since $h = (\pi_1 \circ m') \circ \iota'$, we obtain that $\mathcal{A} = \mathcal{A}'$, $m = m'$ and $\mathcal{A}$ is not finitely subdirectly irreducible. □

Lemma 51 *Let $\mathcal{S}$ be a deductive system and $\mathcal{A}$ a non-weakly maximal $\mathcal{S}$-secrecy structure. If $\mathcal{A}$ is weakly finitely subdirectly irreducible, then, for every secrecy homomorphism $h : \mathcal{A} \to \mathcal{B}$, with $\mathcal{B} \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, there exists an $\iota : \mathcal{A} \prec \mathcal{C}, \mathcal{A} \neq \mathcal{C}$, with $\mathcal{C} \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, and a $\bar{h} : \mathcal{C} \to \mathcal{B}$, such that $\bar{h} \circ \iota = h$.*

Proof:
Let $h : \mathcal{A} \to \mathcal{B}$, with $\mathcal{B} \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, that does not satisfy the statement of the lemma. Since $\mathcal{A}$ is not weakly maximal, there exists $\iota : \mathcal{A} \prec \mathcal{C}$, $\mathcal{A} \neq \mathcal{C}$ and $\mathcal{C} \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$. Define $m : \mathcal{A} \to \mathcal{B} \times \mathcal{C}$ as in the proof of Lemma 50. Then, there exists a subobject decomposition $m = m' \circ \iota'$, with $\iota' : \mathcal{A} \prec \mathcal{A}'$. Since $h = (\pi_1 \circ m') \circ \iota'$ and h was assumed to not satisfy the statement of the lemma, there exists a subobject $n : \mathcal{A} \to \mathcal{A}'$ and $m' \circ n : \mathcal{A} \to \mathcal{B} \times \mathcal{C}$ is a subobject. Thus $\mathcal{B} \times \mathcal{C} \notin \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$. Thus, since $\mathcal{B}, \mathcal{C} \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, we obtain that $\mathcal{A}$ is not weakly finitely subdirectly irreducible. □

Our work culminates in Theorems 52 and 53, which characterize subdirectly irreducible and weakly subdirectly irreducible $\mathcal{S}$-secrecy algebras, respectively. These two theorems are analogs of Theorems 3.6 and 3.7, respectively of [24], which hold for arbitrary semiregular concrete categories with products.

Theorem 52 *Let $\mathcal{S}$ be a deductive system. An $\mathcal{S}$-secrecy structure $\mathcal{A}$ is (finitely) subdirectly irreducible iff either $\mathcal{A}$ is maximal and, for any (finite) monomorphic system $\{m_i : \mathcal{A} \to \mathcal{B}_i\}_{i\in I}$, there exists an $i \in I$, such that m_i is a monomorphism, or $\mathcal{A}$ is not maximal, it is (finitely) meet irreducible and, for every surjective $h : \mathcal{A} \to \mathcal{B}$, not a secrecy isomorphism, there exists an $\iota : \mathcal{A} \prec \mathcal{C}, \mathcal{A} \neq \mathcal{C}$, and a $\bar{h} : \mathcal{C} \to \mathcal{B}$, such that $\bar{h} \circ \iota = h$.*

Proof:
Follows from Proposition 35, Lemma 41, Theorem 46, Proposition 48 and Lemma 50. □

Theorem 53 *Let $\mathcal{S}$ be a deductive system. An $\mathcal{S}$-secrecy structure $\mathcal{A}$ is weakly (finitely) subdirectly irreducible iff either $\mathcal{A}$ is weakly maximal and, for any (finite) monomorphic system $\{m_i : \mathcal{A} \to \mathcal{B}_i\}_{i\in I}$, there exists an $i \in I$ and a subobject $n : \mathcal{A} \to \mathcal{B}_i$, or $\mathcal{A}$ is not weakly maximal, it is weakly (finitely) meet irreducible and, for every $h : \mathcal{A} \to \mathcal{B}$, with $\mathcal{B} \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, there exists an $\iota : \mathcal{A} \prec \mathcal{C}, \mathcal{A} \neq \mathcal{C}$, with $\mathcal{C} \in \mathcal{S}\text{-}\mathbf{Str}_{\neg\mathcal{A}}$, and a $\bar{h} : \mathcal{C} \to \mathcal{B}$, such that $\bar{h} \circ \iota = h$.*

Proof:
Follows from Proposition 35, Lemma 41, Theorem 47, Proposition 49 and Lemma 51. □

Summarizing, in this section the notions of a maximal, weakly maximal, meet irreducible and weakly meet irreducible $\mathcal{S}$-secrecy structures were defined. Moreover, monomorphic systems in the category $\mathcal{S}$-**Str** were introduced. In Theorem 46, subdirectly irreducible maximal secrecy structures were characterized in terms of the existence of a monomorphic component for all suitable monomorphic systems. A similar characterization was given in Theorem 47 for weakly subdirectly irreducible weakly maximal secrecy structures. Propositions 48 and 49 and Lemmas 50 and 51, on the other hand, deal with characterizations of subdirectly irreducible non-maximal and weakly subdirectly irreducible non-weakly maximal $\mathcal{S}$-secrecy structures. Theorems 52 and 53 put together all these results providing complete characterizations of subdirectly irreducible and weakly subdirectly irreducible $\mathcal{S}$-secrecy structures, respectively.

In ongoing work, the model theoretic aspects of the theory will be studied. For this purpose, one introduces $\mathcal{S}$-secrecy filters and $\mathcal{S}$-secrecy matrices, that play in $\mathcal{S}$-secrecy logic a role analogous to that of $\mathcal{S}$-filters and $\mathcal{S}$-matrices in abstract algebraic logic. Furthermore, based on these notions, one may define a hierarchy of secrecy logics similar to the abstract algebraic logic hierarchy based on the Leibniz operator. This will also be a focal point in future work.

References

[1] Bao, J., Slutzki, G. and Honavar, V.: Privacy-preserving reasoning on the semantic web. *Web Intelligence*, 791–797 (2007).

[2] Barr, M. and Wells, C.: *Category Theory for Computing Science, Third Edition*, Montréal, Les Publications CRM 1999.

[3] Birkhoff, G.: Subdirect unions in universal algebra, *Bulletin of the American Mathematical Society* 50(10), 764–768 (1944).

[4] Biskup, J.: For unknown secrecies refusal is better than lying, *Data Knowl. Eng.* 33(1), 1–23 (2000).

[5] Biskup, J. and Bonatti, P.A.: Lying versus refusal for known potential secrets, *Data Knowl. Eng.* 38(2), 199–222 (2001).

[6] Biskup, J. and Bonatti, P.A.: Controlled query evaluation for known policies by combining lying and refusal, *Ann. Math. Artif. Intell.* 40(1-2), 37–62 (2004).

[7] Bonatti, P.A., Kraus, S. and Subrahmanian, V.S.: Foundations of secure deductive databases, *IEEE Trans. Knowl. Data Eng.* 7(3), 406–422 (1995).

[8] Borceux, F.: *Handbook of Categorical Algebra, Volume 1*, Cambridge, Cambridge University Press 1994.

[9] Burris, S. and Sankappanavar, H.P.: *A Course in Universal Algebra*, Berlin, Springer-Verlag 1981.

[10] Chang, C.C. and Keisler, H.J.: *Model Theory*, Amsterdam, North-Holland Publishing Company 1990.

[11] Czelakowski, J.: *Protoalgebraic Logics*, Dordrecht, Kluwer Academic Publishers 2001.

[12] Font, J.M., Jansana, R. and Pigozzi, D.: A survey of abstract algebraic logic, *Studia Logica* 74(1-2), 13–97 (2003).

[13] Hodges, W.: *Model Theory*, Cambridge, Cambridge University Press 1993.

[14] Mac Lane, S.: *Categories for the Working Mathematician, Second edition*, Berlin, Springer-Verlag 1998.

[15] Marker, D.: *Model Theory: An Introduction*, Berlin, Springer-Verlag 2002.

[16] McKenzie, R., McNulty, G.F. and Taylor, W.: *Algebras, Lattices, Varieties*, Monterey, Wadsworth & Brooks/Cole 1987.

[17] Pultr, A. and Vinárek, J.: Productive classes and subdirect irreducibility, in particular for graphs, *Discrete Mathematics* 20, 159–176 (1977).

[18] Sicherman, G.L., de Jonge, W. and van de Riet, R.P.: Answering queries without revealing secrets, *ACM Trans. Database Syst.* 8(1), 41–59 (1983).

[19] Slutzki, G., Voutsadakis, G. and Honavar, V.: Secrecy preserving reasoning using secrecy envelopes, Technical report, Ames, Iowa State University 2009.

[20] Stoffel, K. and Studer, T.: Provable data privacy, In Kim Viborg Andersen, John K. Debenham, and Roland Wagner, editors, *DEXA*, *Lecture Notes in Computer Science* 3588, 324–332 (2005).

[21] Stouppa, P. and Studer, T.: A formal model of data privacy, In Irina Virbitskaite and Andrei Voronkov, editors, *Ershov Memorial Conference*, *Lecture Notes in Computer Science* 4378, 400–408 (2006).

[22] Stouppa, P. and Studer, T.: Data privacy for knowledge bases, In Sergei N. Artëmov and Anil Nerode, editors, *LFCS*, *Lecture Notes in Computer Science* 5407, 409–421 (2009).

[23] Vinárek, J.: Remarks on subdirect representations in categories, *Commentationes Mathematicae Universitatis Carolinae* 19(1), 63–70 (1978).

[24] Vinárek, J.: On subdirect irreducibility and its variants, *Czechoslovak Mathematical Journal* 32(1), 116–128 (1982).

[25] Voutsadakis, G., Slutzki, G. and Honavar, V.: Secrecy preserving reasoning over entailment systems theory and applications. Technical report, Ames, Iowa State University 2009.