On group secrets and the metacommunicative aspects of revealing a true secret *

Alessandro Aldini[1][0000−0002−7250−5011], Davide Fazio[2][0000−0001−8136−732X], Pierluigi Graziani[3][0000−0002−8828−8920], Raffaele Mascella[4][0000−0002−1305−7853], and Mirko Tagliaferri[5][0000−0003−3875−0512]

[1] University of Urbino, Italy, alessandro.aldini@uniurb.it
[2] University of Teramo, Italy, dfazio2@unite.it
[3] University of Urbino, Italy, pierluigi.graziani@uniurb.it
[4] University of Teramo, Italy, rmascella@unite.it
[5] University of Urbino, Italy, mirko.tagliaferri@uniurb.it

Abstract. This research paper explores the logical foundations of group secrets, focusing on their preservation and the interplay of belief, knowledge, and intention inherent in secrecy among agents. Key findings establish the logical conditions under which group secrets are maintained and examine how various logical operations influence these secrets. Additionally, the paper offers insights into certain metacommunicative aspects of secret revelation, specifically when the goal is leaving the secret unknown to a targeted nescient. In particular, we provide a formal analysis of intentions crucial in communicative acts.

Keywords: Logic of Secret · Group Secret · Common Knowledge · Metacommunicative dimension · Secrets' disclosure.

1 Introduction

Secrets are integral to private and public aspects of our lives, encompassing information we wish to remain confidential. Whether it's keeping a secret recipe from competitors or protecting home banking credentials from hackers, the essence of a secret lies in the separation between those who hold the information (secret keepers) and those from whom it is hidden (nescients).

Studies on secrecy span multiple disciplines, including psychology [13, 11, 9], philosophy [2], computer science [6], management science [4, 10], and semiotics [14]. Additionally, there has been significant research on secrecy from the perspective of formal logic [8, 15], which is where our contribution lies. While previous studies have formalized key aspects of secrecy, such as the distinction

* This work was supported by the Italian Ministry of Education, University and Research through the PRIN 2022 project "Developing Kleene Logics and their Applications" (DeKLA), project code: 2022SM4XC8. The European Union has funded the work of D. Fazio and R. Mascella - NextGenerationEU under the Italian Ministry of University and Research (MUR) National Innovation Ecosystem grant ECS00000041 - VITALITY - CUP C43C22000380007.

between *knowing a secret* [15] and *(intending) to keep a secret*[6], further exploration is required.

In a recent paper [1], the authors aimed to logically investigate the concept of *keeping a true secret*, focusing on its modal and intentional components. Specifically, [1] sought to formalize propositions like "Agent *a intends* to keep φ *secret* from agent b," along with related notions. The approach carried out in [1] aligns with existing research, such as [12, 11], where secrecy is broadly defined as "an intention to keep some piece of information, known to oneself, unknown from one or more others" (cf. [12, p. 542]). However, the investigation of [1] adopted a static and descriptive perspective, deliberately excluding dynamic aspects like belief revision or interactions between secret keepers. The research outcome was a formal system bridging the existing frameworks in the literature by introducing a new tool for investigating secrecy-related intentions. Furthermore, [1] focused on secrecy involving only two agents, the nescient and the secret keeper, without favouring any specific nature of the agents. However, in many cases, the nescient and secret keepers are not individual agents but groups of agents. They can be companies, computer networks, or people. An example is represented by a national intelligence agency that intends to keep a piece of particular national security information, such as a covert operation or a strategic plan, secret from unauthorized individuals to protect the country's security and prevent internal or external threats. Or consider a division of a technology company that intends to keep a research and development project, a patented formula, or a market strategy secret from potential competitors to maintain a competitive advantage and protect intellectual property.

The concept of a group secret has attracted great attention over the past years due to its importance for understanding social dynamics within groups of agents. Processes underpinning secrecy are associated with creating boundaries, with the impacts of secrecy among the in-group often traced to the formation of strong interpersonal ties and collective identities (cf., e.g. [4]), which accounted for higher levels of social interaction and social trust. The concept of a group secret is significant within the framework of managerial sciences, with organizational secrets being subjects in point.

To provide a formal framework capable of dealing with group secrets, the system proposed by [1] can be easily extended to sets of agents as it does not presuppose any postulation about the nature of agents involved: they can stand for either individuals or collective entities whatsoever. However, members of a group of secret keepers might be related to each other through relationships and internal rules concerning the *sharing* of knowledge and secrets that a suitable system should consider. Among them, we recognize the following[7]:

S1 All members of the secret keepers' group *know* the secret φ;
S2 All members of the secret keepers' group believe that outsiders (nescients) do not know φ;

[6] See Slepian [13] for a thorough analysis of this distinction in psychology.
[7] Cf. [4] for examples in managerial contexts.

S3 All members of the secret keepers' group intend to ensure that nescients do not know/have access to φ;
S4 All secret keepers' group members do not intend to destroy/make false the information to be kept hidden.[8]

However, if we confine ourselves to S1-S4 above, we would only be considering extremely general situations as, for example, when a group of individuals intends to keep a piece of information secret from any member from another group independently, possibly not knowing that members from the same group are doing the same. However, in concrete social scenarios, it often happens that the group's members are *aware* to be part of the group of secret keepers. This fact means that:

S5 They share the common belief they all *know* the proposition to be kept secret;
S6 They share the common belief about with whom they have to keep the secret secret;
S7 They share the common belief that nescients do not know the secret;
S8 They share the common intention/commitment not to reveal the secret to the nescients and, at the same time, to preserve its truth.

As previously mentioned, several studies have explored the concept of secrecy. In particular, some of them focus on the act of revealing (sharing) a secret. From Bellman [2] to Slepian [11], these analyses have shed light on various aspects of this process. An exciting aspect of the formal study of secret-keeping is the consideration of how the group of secret-keepers can expand when a secret is disclosed with the intent that it remains confidential among the original and newly informed parties while still being kept secret from those not included in the communication.

Following Bellman [2], the act of revealing a secret introduces a *metacommunicative element*; beyond the content of the secret itself, there is an implicit communication that the information should not be shared further and that the source must be protected. However, suppose agent a reveals φ to agent b with the intent that φ remains a secret from everyone except a and b. In that case, this does not necessarily mean that a and b now constitute a group of secret keepers in the above sense as its internal dynamics might fail to fulfil S8.[9]

[8] Imagine I intend to keep the statement "*there is* a secret laboratory in Raffaello Street" secret from a targeted group of nescients. If, to keep this information concealed, I decided to destroy the laboratory, the object of the secret would no longer exist. Therefore, the secret would be missing or even pointless.

[9] Imagine a tech company developing a new product. Alice, a senior engineer, discovers a critical vulnerability in the software. She shares this information with Bob, another engineer, asking him to keep it secret. Alice intends to keep the vulnerability secret from everyone outside their circle, including others in the company. Bob agrees to keep it secret, but *does not internalize the intention of secrecy*, e.g. although he intends not to reveal the secret himself, he intends to push Alice to disclose it. Therefore, they do not reach a shared commitment to secrecy, and so they do not form a group of secret keepers under condition S8.

The present article aims to extend [1] for investigating the group and metacommunicative dimensions of secrecy intentions and revelations. To this end, the paper will be structured as follows: in Section 2, we introduce an expansion of the formal system presented in [1] aimed at providing a formal treatment of group secret; in Section 3, we attempt a formal analysis of the metacommunicative dimension of revealing a true secret; we conclude in Section 4 with a summary and suggestions for future works.

2 Formalizing group secrets

The formalization of keeping true secrets given in [1] considers the presence of at least two agents: agent a, the secret keeper, and agent b, the nescient, from whom the secret must be kept. Moreover, the definition of secrecy in [1] is based on the following key assumptions from agent a's perspective:

1. Agent a knows the object of the secret, referred to as the *secretum*. Since knowledge is assumed to be factive, the content of a's secret must be true, which justifies the term *true secret* used in [1].
2. Agent a believes that agent b does not know the *secretum*. We use belief rather than knowledge because agent a cannot directly access agent b's mental states.
3. Agent a intends to act so that the truth of the *secretum* is preserved and agent b remains unaware of the *secretum*.

Following [1], to capture these assumptions, we will use three modal operators: knowledge (K), belief (B), and intentionality (I), applied to multiple agents. The formal definition of a true secret, denoted by $S_{a,b}\varphi$, is expressed as follows (cf. [1, p. 3]):

$$S_{a,b}\varphi := K_a\varphi \wedge B_a\neg K_b\varphi \wedge I_a(\varphi \wedge \neg K_b\varphi).$$

It is worth observing that, by (3), we assume that the concept of a true secret involves the intention of preserving the truth of its content. Indeed, it might look quite strong, at first sight. After all, it is intuitively reasonable to argue that secrets might be preserved also e.g. by "destroying" their content. However, as we are dealing with intentions of secrecy concerning propositions that are *known*, making a proposition false, and so unknown to the secret keeper would inevitably result in the elimination of the main motivation to keep it secret.

2.1 A logical system for group secrets

To provide a basic axiomatization of the primitive operators employed to formalize the notion of a group secret, we introduce the formal system SC as an expansion of the system S of multi-agent normal modal logic introduced in [1] using modal operators and inference rules for common belief, common knowledge and common commitment. To this aim, we enrich the alphabet of S employing

new symbols $\mathbb{B}_C$, $\mathbb{I}_C$ and $\mathbb{K}_C$ (for any set C of agents) such that $\mathbb{B}_C\varphi$ will stand for "the group C has the common belief that φ", $\mathbb{I}_C\varphi$ will mean "the group C has the common commitment of intending to bring about a state of affairs in which φ is true" and, of course, $\mathbb{K}_C\varphi$ will be short for "The group C has the common knowledge that φ". Indeed, the above statements will be codified within our framework using the *infinite* conjunction of formulas of the form $(E^B_C)^n\varphi$, $(E^I_C)^n\varphi$, and $(E^K_C)^n\varphi$ ($n \geq 1$), respectively, where e.g. $(E^K_C)^n\varphi$ is to be meant as the n-th composition of the "every-member-of-C-knows-that" operator E^K_C. Consequently, saying that φ is a common belief (knowledge) among members of C will be equivalent to asserting that any member of C believes (knows) that φ, any member of C believes (knows) that any member of C believes (knows) that φ, and so on. Similarly, the common commitment of C towards φ will amount to say that all members of C intend to bring about a state of affairs in which φ is true, all members of C intend to bring about a state in which any member of C intends to bring about a state of affair in which φ is true, and so on.

A presentation of the system SC comes next. Let Ag be a non-empty, finite set of agents, and let Var be an infinite, countable set of variables. Let $\mathrm{Fm}_{\mathsf{SC}}$ be the smallest set of formulas generated by the following grammar:

$$\varphi := \ p \mid \neg\varphi \mid \varphi \wedge \varphi \mid I_a\varphi \mid K_a\varphi \mid B_a\varphi \mid \mathbb{K}_C\varphi \mid \mathbb{B}_C\varphi \mid \mathbb{I}_C\varphi.$$

where $p \in Var$ and $C \cup \{a\} \subseteq Ag$. As customary, we set $\varphi \vee \psi := \neg(\neg\varphi \wedge \neg\psi)$ and $\varphi \to \psi := (\neg\varphi \vee \psi)$. Following customary conventions, for any $C \subseteq Ag$ and $\varphi \in \mathrm{Fm}_{\mathsf{S}}$, we set:

$$E^\star_C\varphi := \bigwedge_{a\in C} \star_a\varphi,$$

where $\star \in \{K, B, I\}$. In other words, $E^K_C\varphi, E^I_C\varphi$, and $E^B_C\varphi$ encode the statement "all agents from C know that φ", "all agents from C intend to bring about a state of affairs in which φ is true", and "all members form C believe that φ", respectively.
The logic $\mathsf{SC} = \langle \mathrm{Fm}_{\mathsf{SC}}, \vdash_{\mathsf{SC}}\rangle$ is the *derivability* relation (to be defined as customary) induced by the axiom and inference rule schemes, for any $C \cup \{a\} \subseteq Ag$, illustrated in Table 1. We remark that $(\mathrm{RI})_I$, $(\mathrm{RI})_B$ and $(\mathrm{RI})_K$ mean that if the premise of (an instance of) the rule is a theorem, then the conclusion is.

The epistemic part of the axiomatization (A1-A7) contains nothing new and is, therefore, standard. Focusing on the intentionality operator I, axiom A8 states that any agent a is consistent with her intentions, axioms A9 and A10 express the transparency and awareness conditions (see [1] for details), respectively, and axiom A11 represents a *persistence* condition for intentionality. Having the intention to bring about a state of affairs in which φ is true entails that such an intention is preserved in all states of affairs reachable through it. This assumption does not make any commitment from a *tense* perspective, as we are concerned with a static tenseless framework. Therefore, the operator I should not be regarded as a *tense* operator. Also, it is worth observing that I, like B, is not factive and, differently from B, is not implied by K. The interested reader is referred to [1] for a thorough discussion of A1-A11. Axioms A12-A13 as well

A1	All tautologies of classical propositional logic
A2	$\star(\varphi \to \psi) \to (\star\varphi \to \star\psi)$ for any $\star \in \{B_a, K_a, I_a\}$
A3	$K_a\varphi \to \varphi$
A4	$K_a\varphi \to K_aK_a\varphi$
A5	$B_a\varphi \to \neg B_a\neg\varphi$
A6	$K_a\varphi \to B_a\varphi$
A7	$B_a\varphi \to K_aB_a\varphi$
A8	$I_a\varphi \to \neg I_a\neg\varphi$
A9	$I_a\varphi \to K_aI_a\varphi$
A10	$I_a\varphi \to I_aK_a\varphi$
A11	$I_a\varphi \to I_aI_a\varphi$
A12	$\mathbb{I}_C\varphi \to E^I_C(\varphi \wedge \mathbb{I}_C\varphi)$
A13	$\mathbb{B}_C\varphi \to E^B_C(\varphi \wedge \mathbb{B}_C\varphi)$
A14	$\mathbb{K}_C\varphi \to E^K_C(\varphi \wedge \mathbb{K}_C\varphi)$

$$\frac{\varphi \qquad \varphi \to \psi}{\psi}\ \text{RMP} \quad \text{and} \quad \frac{\varphi}{\star\varphi}\ \text{RN}_\star \quad \text{where } \star \in \{I_a, K_a, B_a\}$$

$$\frac{\varphi \to E^I_C(\psi \wedge \varphi)}{\varphi \to \mathbb{I}_C\psi}\ (\text{RI})_I \qquad \frac{\varphi \to E^B_C(\psi \wedge \varphi)}{\varphi \to \mathbb{B}_C\psi}\ (\text{RI})_B \qquad \frac{\varphi \to E^K_C(\psi \wedge \varphi)}{\varphi \to \mathbb{K}_C\psi}\ (\text{RI})_K$$

for any $C \subseteq Ag$

Table 1. Axioms and rules of SC.

as inference rules $(\text{RI})_I$, $(\text{RI})_B$, and $(\text{RI})_K$ are nothing but axioms and inference rules for common knowledge (straightforwardly extended to common belief and common intention) provided by [5]. Of course, an operator of "common intention" might look quite non-standard at first sight. However, it has a quite natural motivation. Indeed, as we are interested in group secrets, a natural desideratum is dealing with situation in which one has not only common knowledge/belief among members of a group, but also a sort of joint commitment, to be meant as an intention to preserve group's intentions (of secrecy, in our case) – see p. 9. Therefore, we have endowed the system SC with a common intention operator to make reason of statements like "everyone intends to bring about a state of affairs in which φ is true, everyone intends to bring about a state of affairs in which everyone intends that φ, and so on ....

We can now introduce the semantics for SC. Let A be a non-empty set. Recall that a binary relation $R \subseteq A \times A$ is said to be *serial* provided that, for any $i \in A$, there exists $j \in A$ such that $R(i, j)$.

Definition 1. *An* $\mathcal{S}$-frame *(a* frame*, for short) is a tuple*

$$\mathcal{F} = (W, \{R^I_a\}_{a\in Ag}, \{R^K_a\}_{a\in Ag}, \{R^B_a\}_{a\in Ag})$$

such that:

1. *W is a non-empty set of worlds (or states);*
2. *$R^B_a \subseteq W \times W$ is serial;*
3. *For any $a \in Ag$, $R^I_a \subseteq W \times W$ is serial and transitive;*
4. *For any $a \in Ag$, $R^K_a \subseteq W \times W$ is reflexive and transitive;*

5. *For any* $i, j, w \in W$*, and any* $a \in Ag$*, if* $R_a^K(i,j)$ *and* $R_a^I(j,w)$*, then* $R_a^I(i,w)$.
6. *For any* $a \in Ag$*,* $R_a^B \subseteq R_a^K$*;*
7. *For any* $i, j, w \in W$ *and* $a \in Ag$*, if* $R_a^K(i,j)$ *and* $R_a^B(j,w)$*, then* $R_a^B(i,w)$*;*
8. *For any* $i, j, w \in W$ *and* $a \in Ag$*,* $R_a^I(i,j)$ *and* $R_a^K(j,w)$ *imply* $R_a^I(i,w)$.

Definition 2. *An* $\mathcal{S}$*-model (a* model*, in brief) is a tuple*

$$\mathcal{M} = (W, \{R_a^I\}_{a\in Ag}, \{R_a^K\}_{a\in Ag}, \{R_a^B\}_{a\in Ag}, v)$$

such that

1. $(W, \{R_a^I\}_{a\in Ag}, \{R_a^K\}_{a\in Ag}, \{R_a^B\}_{a\in Ag})$ *is an* $\mathcal{S}$*-frame, and*
2. $v : Var \to \mathcal{P}(W)$ *is a mapping, called an* evaluation.

Given an $\mathcal{S}$-model $\mathcal{M} = (W, \{R_a^I\}_{a\in Ag}, \{R_a^K\}_{a\in Ag}, \{R_a^B\}_{a\in Ag}, v)$, $i \in W$, $\varphi \in \mathrm{Fm}_{\mathsf{S}}$ the notion of truth in i ($\mathcal{M}, i \models \varphi$), truth in $\mathcal{M}$ ($\mathcal{M} \models \varphi$) and truth in any $\mathcal{S}$-model ($\models_{\mathcal{S}} \varphi$) are quite standard, so we refer e.g. to [7, 5] for details. For the reader's convenience, we recap the semantic definitions of common belief, common knowledge, and common commitment (intention).

Let $\star \in \{I, B, K\}$, $C \subseteq Ag$, and $\varphi \in \mathrm{Fm}_{\mathsf{SC}}$. We define the formula $(E_C^\star)^n\varphi$, for any $n \geq 1$ as follows:

- $(E_C^\star)^1\varphi := E_C^\star\varphi$;
- $(E_C^\star)^{n+1}\varphi := E_C^\star(E_C^\star)^n\varphi$

Let $\mathcal{F} = (W, \{R_a^I\}_{a\in Ag}, \{R_a^K\}_{a\in Ag}, \{R_a^B\}_{a\in Ag})$ be an $\mathcal{S}$-model. For any $C \subseteq Ag$ and $\star \in \{I, B, K\}$, we define:

$$R_C^\star := \bigcup_{a\in C} R_a^\star.$$

Moreover, given a non-empty set A and $R \subseteq A \times A$, we will denote by R^+ its transitive closure, i.e. the *smallest* transitive relation over A containing R. It is easily seen that, for any $x, y \in A$, xR^+y iff there exist $n > 1$, $x_1, \ldots, x_n \in A$ such that $x_1 = x$, $x_n = y$ and $x_i R x_{i+1}$, for any $1 \leq i < n$.

Let $\mathcal{M} = (W, \{R_a^I\}_{a\in Ag}, \{R_a^K\}_{a\in Ag}, \{R_a^B\}_{a\in Ag}, v)$ be an $\mathcal{S}$-model, the clauses of satisfaction in $i \in W$ for common belief, common knowledge and common intention are defined, for any $C \subseteq Ag$, $i \in W$, as:

- $\mathcal{M}, i \models \mathbb{I}_C\varphi$ iff, for any $j \in W$ such that $(R_C^I)^+(i,j)$, $\mathcal{M}, j \models \varphi$;
- $\mathcal{M}, i \models \mathbb{B}_C\varphi$ iff, for any $j \in W$ such that $(R_C^B)^+(i,j)$, $\mathcal{M}, j \models \varphi$;
- $\mathcal{M}, i \models \mathbb{K}_C\varphi$ iff, for any $j \in W$ such that $(R_C^K)^+(i,j)$, $\mathcal{M}, j \models \varphi$.

The proof of the following proposition is straightforward.

Proposition 1. *Let* $\mathcal{M} = (W, \{R_a^I\}_{a\in Ag}, \{R_a^K\}_{a\in Ag}, \{R_a^B\}_{a\in Ag}, v)$*,* $C \subseteq Ag$*,* $\varphi \in \mathrm{Fm}_{\mathsf{SC}}$*, the following are equivalent:*

1. $\mathcal{M}, i \models \mathbb{I}_C\varphi$*;*
2. $\mathcal{M}, i \models (E_C^I)^n\varphi$*, for any* $n \geq 1$*;*

3. *If* $j \in W$ *and there are* $x_1, \ldots, x_n \in W$ $(n > 1)$ *such that* $x_1 = i, x_n = j$ *and, for any* $1 \leq k < n$, $R^I_{a_i}(x_k, x_{k+1})$, $a_i \in C$, *then* $\mathcal{M}, j \models \varphi$.

Moreover, the same holds upon replacing $\mathbb{I}$ *by* $\mathbb{B}$ $(\mathbb{K})$, E^I_C *by* E^B_C (E^K_C), *and* R^I_C *by* R^B_C (R^K_C).

The next result can be proven through customary arguments already thoroughly discussed in the literature. See [5, 7] for details.

Theorem 1. *For any* $\varphi \in \mathrm{Fm}_{\mathsf{SC}}$*:*

$$\vdash_{\mathsf{SC}} \varphi \textit{ iff } \models_{\mathcal{S}} \varphi.$$

Obviously, SC is a *conservative expansion* of the system S from [1].

Following [1], we have started from a notion of "keeping a true secret" involving only two agents: a secret keeper and a (alleged) nescient.
Nevertheless, a natural question arises. Is it possible to generalize such a notion to express that a *group* C of agents keeps φ secret from a group D of agents such that $C \cap D = \emptyset$? A tentative answer is relatively easy to obtain. It suffices to set:

$$S_{C,D}\varphi := \bigwedge_{a \in C, b \in D} S_{a,b}\varphi.$$

Note that, by virtue of $\vdash_{\mathsf{S}} \star(\varphi \wedge \psi) \leftrightarrow \star\varphi \wedge \star\psi$ with $\star \in \{K_a, B_a, I_a\}$ $(a \in Ag)$, one has

$$\vdash_{\mathsf{SC}} S_{C,D}\varphi \leftrightarrow \bigwedge_{a \in C} K_a\varphi \wedge \bigwedge_{a \in C} B_a(\bigwedge_{b \in D} \neg K_b\varphi) \wedge \bigwedge_{a \in C} I_a((\bigwedge_{b \in D} \neg K_b\varphi) \wedge \varphi) \quad (1)$$

or, using the more streamlined notation introduced above,

$$\vdash_{\mathsf{SC}} S_{C,D}\varphi \leftrightarrow E^K_C\varphi \wedge E^B_C(\bigwedge_{b \in D} \neg K_b\varphi) \wedge E^I_C((\bigwedge_{b \in D} \neg K_b\varphi) \wedge \varphi). \quad (2)$$

Indeed, such a notion of group secret turns out to preserve many important features of secrecy between pairs of agents, as it can be seen that, e.g., results from [1, Propositions 2 and 3] holding for $S_{a,b}$ are still valid once $S_{C,D}$ (for some non-empty $C, D \subseteq Ag$ such that $C \cap D = \emptyset$) is considered. However, an easy check shows that, e.g. agents from C need not know that other members of C intend to keep a proposition φ secret from a given agent $b \in D$ or there need not be *agreement* on secrecy intentions. A striking example is given by the fact that easy buildable Kripke models allow one to show that, for any $a, b, c \in Ag$

$$\nvdash_{\mathsf{SC}} S_{\{a,b\},\{c\}}\varphi \rightarrow \neg(S_{a,b}\varphi \vee S_{b,a}\varphi). \quad (A)$$

or

$$\nvdash_{\mathsf{SC}} S_{\{a,b\},\{c\}}\varphi \rightarrow B_b S_{a,c}\varphi, \quad (B)$$

Therefore, such a notion of a group secret falls short of capturing S5 - S8. This remark suggests that a much more sophisticated definition of secrecy is needed

to cope with more complex forms of secrecy.
The notion of a group secret formalized by (1) reveals certain limitations when it comes to encoding the full complexity of secret-sharing phenomena, e.g. in organizational contexts where a group of agents is explicitly "designated" to keep certain information secret. An example is given by company members who are requested to keep a piece of information of strategic relevance secret from outsiders. One notable issue is that (1) fails to capture whether any agent within the group is aware of the secrecy intentions of the other agents. In other words, while the formalism ensures that a group of agents collectively holds a secret, it does not guarantee that each agent understands that the other group's members are intentionally keeping the secret. Put another way, (1) does not capture the idea that secret keepers recognize that the group they are members of is the group of secret keepers.

Furthermore, (1) does not address the idea of a joint or common commitment to preserving the group's intention to keep a secret. Indeed, suppose secret keepers are aware of being part of a group designated to keep information concealed and intend to preserve the group's "mission". In that case, each member has not only the intention of keeping the information secret, but she also has the intention of preserving other members' intention of doing the same, e.g. by preserving conditions making intentions of concealment possible[10]. Without such a joint commitment, the group's "agreement" to preserve the secret need not hold, as individual agents may fail to realize the importance of maintaining the secrecy from the perspective of the group as a whole.

These shortcomings suggest that a slightly more sophisticated approach is required. In this venue, we propose a notion of *true group secret with common commitment* upon setting, for any $\varphi \in \mathrm{Fms}_{\mathsf{SC}}$, $C, D \subseteq Ag$:

$$\mathbb{S}_{C,D}\varphi := \mathbb{B}_C S_{C,D}\varphi \wedge \mathbb{I}_C S_{C,D}\varphi \wedge S_{C,D}\varphi. \tag{$\mathbb{S}$}$$

Whenever no danger of confusion will be impending, if $a, b \in Ag$, $C = \{a\}$ and $D = \{b\}$, we will write simply $\mathbb{S}_{a,b}$, $\mathbb{I}_a$ and $\mathbb{B}_a$, instead of $\mathbb{S}_{\{a\},\{b\}}$, $\mathbb{I}_{\{a\}}$ and $\mathbb{B}_{\{a\}}$, respectively.[11]

Proposition 2. *For any $\varphi \in \mathrm{Fms}_{\mathsf{SC}}$ it holds that*

$$\vdash_{\mathsf{SC}} \mathbb{S}_{a,b}\varphi \leftrightarrow S_{a,b}\varphi.$$

In other words, the concept of "intending to keep a true" secret outlined in [1] is a limit case of the concept of a group secret once only two agents, a secret keeper and a nescient, are considered. The next proposition can be proven by exploiting well-known inductive techniques.

[10] For example, if Alice and Bob are part of a group C of secret keepers, and Alice has the intention of preserving the "mission" of C, then Alice's intentions should include e.g. avoiding to threaten Bob's intention of secrecy by telling him he is no longer supposed to keep the information secret.

[11] **Some proofs of propositions that will be stated in the following pages are available in the appendix "Proofs" section after the references**

Proposition 3. *Let $\varphi \in \mathrm{Fm}_{\mathsf{SC}}$, $C \subseteq Ag$:*

1. $\vdash_{\mathsf{SC}} \mathbb{B}_C\varphi \to \mathbb{B}_C\mathbb{B}_C\varphi$;
2. $\vdash_{\mathsf{SC}} \mathbb{I}_C\varphi \to \mathbb{I}_C\mathbb{I}_C\varphi$
3. $\vdash_{\mathsf{SC}} \mathbb{K}_C\varphi \leftrightarrow \mathbb{K}_C\mathbb{K}_C\varphi$;
4. $\vdash_{\mathsf{SC}} \mathbb{K}_C\varphi \to \mathbb{B}_C\varphi$;
5. $\vdash_{\mathsf{SC}} \mathbb{K}_C\varphi \to \mathbb{B}_C\mathbb{K}_C\varphi$;

Proposition 3 presents key properties of modalities for common knowledge, belief and intention inherited from the behaviour of knowledge, belief, and intention operators. The first two items illustrate the positive introspection of common beliefs ($\mathbb{B}_C$) and intentions ($\mathbb{I}_C$). The third item deals with the idempotency of common knowledge ($\mathbb{K}_C$), which is due to the factivity of the knowledge operator K_a. The last two items establish a link between knowledge and common belief, indicating that a group's knowledge implies that the proposition is commonly believed and that there is a common belief about the group's knowledge. These properties are crucial for modelling group coordination and transparency, especially in contexts like security, cooperation, and information management. Customary semantic arguments can easily prove the next propositions.

Proposition 4. *Let $\varphi \in \mathrm{Fm}_{\mathsf{SC}}$, $C, D \subseteq Ag$, $a, b \in C$, $d \in D$. The following hold:*

1. $\vdash_{\mathsf{SC}} \neg\mathbb{S}_{C,C}\varphi$;
2. $\vdash_{\mathsf{SC}} \neg\mathbb{S}_{C,D}\top \wedge \neg\mathbb{S}_{C,D}\bot \wedge (\mathbb{S}_{C,D}\varphi \to \varphi)$;
3. $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \to B_a S_{C,D}\varphi$;
4. $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \wedge \mathbb{B}_C\mathbb{I}_C S_{C,D}\varphi \to \mathbb{B}_C\mathbb{S}_{C,D}\varphi$;
5. $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}(\mathbb{S}_{C,D}\varphi) \to \mathbb{S}_{C,D}\varphi$;
6. $\vdash_{\mathsf{SC}} \neg K_d\varphi \to \neg K_d\mathbb{S}_{C,D}\varphi$;
7. $\vdash_{\mathsf{SC}} \neg\mathbb{S}_{C,D}K_d\varphi$;
8. $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \to \neg\mathbb{S}_{C,D}\neg\varphi$;
9. $\vdash_{\mathsf{SC}} \neg\mathbb{S}_{C,D}\mathbb{K}_D\varphi$;
10. $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \to \neg(S_{a,b}\varphi \vee S_{b,a}\varphi)$.

Proposition 4 establishes some basic features of group secrets that generalize results obtained in [1, Proposition 2]. The first item is clear: no group C of secret keepers may ever intend to keep a piece of information secret to itself. Item (2) introduces limits on secrecy by establishing that secrets must be *contingent*, meaning they cannot apply to universally true ($\top$) or false ($\bot$) statements as tautologies are known to everyone (this is a side effect of logical omniscience determined by using a normal box operator for knowledge). In contrast, contradictions cannot be known by anyone (after all, we are dealing with known secrets!). Moreover, group secrets are factive. Item (3) shows that $\mathbb{S}_{C,D}$ allows us to overcome (in a specific sense) the drawback highlighted in (B). Item (4) expresses a weak form of positive introspection of secrecy concerning common belief. If φ is a group secret of C w.r.t. D and it is a common belief that there is a joint commitment in guaranteeing that all the members of C have the intention of keeping φ secret, then there is a common belief that φ is a group secret. Items

(5) to (9) highlight that, at least in a weak form, many properties of secrecy involving pairs of agents rather than groups still hold (cf. [1]). Finally, item (10) resolves the drawback in (A) by showing that no member of a group of secret-keepers can have the intention of keeping the information they are supposed to conceal a secret from each other.
Of course, one might ask if conditions from Proposition 4 might be somehow strengthened. The next proposition shows that this is not the case.

Proposition 5. *Let* $\varphi \in \mathrm{Fm}_{\mathsf{SC}}$, $C, D \subseteq Ag$. *The following hold:*

1. $\not\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \to \mathbb{B}_C\mathbb{S}_{C,D}\varphi$;
2. $\not\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \to \mathbb{S}_{C,D}(\mathbb{S}_{C,D}\varphi)$
3. $\not\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \to B_a\mathbb{S}_{C,D}\varphi$, *for any* $a \in C$;
4. $\not\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \to \mathbb{I}_C\mathbb{B}_C\mathbb{S}_{C,D}\varphi$;
5. $\not\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \to \mathbb{I}_C\mathbb{S}_{C,D}\varphi$;
6. $\not\vdash_{\mathsf{SC}} \neg\mathbb{S}_{C,D}\mathbb{I}_D\varphi$;
7. $\not\vdash_{\mathsf{SC}} \neg\mathbb{S}_{C,D}\mathbb{B}_D\varphi$.

Proposition 5 highlights the limitations and fragility of group secrets. Unlike individual secrets, group secrets do not necessarily propagate through common beliefs or intentions. The first items show that the existence of a group secret φ ($\mathbb{S}_{C,D}\varphi$) among agents from C does not imply that it is a common belief within C that φ is actually a group secret ($\mathbb{B}_C\mathbb{S}_{C,D}\varphi$). Moreover, unlike the operator $S_{a,b}$ (see [1, Proposition 2]), $\mathbb{S}_{C,D}$ is not idempotent. This reflects the complexity of maintaining secrecy in groups, where agreement might be limited to the content of the secret ("first-order secrecy") but not to the intention of keeping the secret itself ("second-order secrecy"). This is coherent with items (3)-(5), where it is shown that $\mathbb{S}_{C,D}\varphi$ fails to entail that any secret keeper recognizes φ as a group secret or that there is common intention to bring about a state of affairs in which (it is common belief that) φ is a group secret. Finally, (6) and (7) outline a kind of weakness of groups, i.e., group members D need not be aware there is a common commitment or belief about a proposition φ among them. Nevertheless, important properties of secrecy are still valid once group secrets come into play.

Proposition 6. *Let* $\varphi \in \mathrm{Fm}_{\mathsf{SC}}$ *and* $C, D \subseteq Ag$. *The following hold:*

1. *If* $\vdash_{\mathsf{SC}} \varphi \to \psi$ *and* $\vdash_{\mathsf{SC}} \psi \to \chi$, *one has* $\vdash_{\mathsf{SC}} (\mathbb{S}_{C,D}\varphi \wedge \mathbb{S}_{C,D}\chi) \to \mathbb{S}_{C,D}\psi$;
2. *For any* $n \geq 2$, $\vdash_{\mathsf{SC}} \varphi_i \to \varphi_{i+1}$ $(1 \leq i < n)$ *implies* $\vdash_{\mathsf{SC}} (\mathbb{S}_{C,D}\varphi_1 \wedge \mathbb{S}_{C,D}\varphi_n) \to \bigwedge_{i=1}^{n} \mathbb{S}_{C,D}\varphi_i$.

This proposition shows that group secrets (modelled by $\mathbb{S}_{C,D}$) still satisfy the interpolation rule. Specifically, if the group C knows φ and χ, then they can infer ψ when $\varphi \to \psi$ and $\psi \to \chi$. This result is crucial in the phenomenon of group secrets, as it ensures that the collective knowledge of C and D evolves coherently through logical reasoning, maintaining secrecy while allowing for distributed inference.
The next proposition extends to group secrets some results already proved in [1] concerning the behaviour of secrecy operators w.r.t. the main logical connectives.

Proposition 7. *Let $\varphi, \psi \in \mathrm{Fm}_{\mathsf{SC}}$, $C, D \subseteq Ag$ with $C \cap D \neq \emptyset$, and $b \in D$. The following hold:*

1. $\vdash_{\mathsf{SC}} (\mathbb{B}_C K_b \psi \vee \mathbb{I}_C K_b \psi) \to \neg \mathbb{S}_{C,D}(\varphi \to \psi)$;
2. $\vdash_{\mathsf{SC}} (\mathbb{B}_C K_b \neg\varphi \vee \mathbb{I}_C K_b \neg\varphi) \to \neg \mathbb{S}_{C,D}(\varphi \to \psi)$.
3. $\vdash_{\mathsf{SC}} (\mathbb{S}_{C,D}\varphi \wedge \mathbb{S}_{C,D}\psi) \to \mathbb{S}_{C,D}(\varphi \wedge \psi)$;
4. $\vdash_{\mathsf{SC}} (\mathbb{S}_{C,D}(\varphi \wedge \psi) \wedge \mathbb{S}_{C,D}(\varphi \vee \psi)) \to (\mathbb{S}_{C,D}\varphi \wedge \mathbb{S}_{C,D}\psi)$;
5. $\vdash_{\mathsf{SC}} (\mathbb{S}_{C,D}\varphi \wedge E^K_C \psi \wedge \mathbb{B}_C E^K_C \psi \wedge \mathbb{I}_C E^K_C \psi \wedge \mathbb{B}_C E^I_C \psi) \to \mathbb{S}_{C,D}(\varphi \wedge \psi)$;
6. $\nvdash_{\mathsf{SC}} (\mathbb{S}_{C,D}\varphi \wedge \mathbb{K}_C \psi \wedge \mathbb{I}_C \psi) \to \mathbb{S}_{C,D}(\varphi \wedge \psi)$.

Proposition 7 explores the interaction between group secrets and logical connectives. The first two items connect the truth-conditional properties of material implication and group secrecy. Indeed, (1) and (2) establish that it is impossible for a group C to intend to keep $\varphi \to \psi$ secret from members of D, if there is common belief or common intention among Cs that some member of D knows that ψ ($\neg\varphi$) Items (3) and (4) show that group secrets behave in a conjunctive manner: the secret of both φ and ψ leads to the secret of their conjunction, and the secret of their conjunction implies their individual secrets. This is strengthened by item (5) as it states the need for detailed coordination of knowledge, belief, and intention among secret keepers to hold the secret of a conjunction. Item (6) expresses the failure of a kind of "expandability" of group secrets. Namely, it is not the case that if C intends to keep φ secret from D, then adding a piece of information ψ to φ obliges C to have $\varphi \wedge \psi$ as a group secret w.r.t. D. Again, this suggests that common intention and belief included in group secrecy are limited to the content of the original secret and cannot be extended without further conditions on intentions and epistemic coordination between secret keepers.

We close this section with a proposition that makes explicit conditions under which one can derive the group secrecy of a given statement φ from the secrecy of the disjunction $\varphi \vee \psi$.

Proposition 8. *Let $\varphi, \psi \in \mathrm{Fm}_{\mathsf{SC}}$, $C, D \subseteq Ag$. Then:*

1. $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}(\varphi \vee \psi) \to ((E^K_C \varphi \wedge \mathbb{I}_C E^K_C \varphi \wedge \mathbb{B}_C(E^I_C \varphi \wedge E^K_C \varphi)) \leftrightarrow \mathbb{S}_{C,D}\varphi)$;
2. $\nvdash_{\mathsf{SC}} (\mathbb{S}_{C,D}(\varphi \vee \psi) \wedge \mathbb{K}_C \varphi \wedge \mathbb{I}_C \varphi) \to \mathbb{S}_{C,D}\varphi$.

This proposition addresses the interplay between group secret ($\mathbb{S}_{C,D}$) and some specific conditions (E^K_C, E^I_C, and $\mathbb{B}_C$) in group dynamics, particularly when a disjunction of secrets is involved. Part (1) demonstrates that if $\varphi \vee \psi$ is a group secret, then certain conditions holding on φ alone lead to equivalence with φ being a group secret alone. This result highlights the robustness of group secrecy when the group possesses detailed information. Part (2) introduces a limitation, showing that certain combinations of group conditions ($\mathbb{K}_C\varphi$ and $\mathbb{I}_C\varphi$) do not necessarily imply the group's ability to entirely derive the intention of keeping φ secret. This counterexample reflects the nuanced behaviour of group secrecy under incomplete or conflicting information and the possible lack of transparency in beliefs/intentions among secret keepers.

3 Metacommunicative aspects of revealing a secret

While in the previous section we focused on the properties of group secrets, in this section we investigate those metacommunicative aspects that underlie the formation of a group keeping a secret.

In [2], the metacommunicative dimension of telling a secret is investigated. As B.L. Bellman writes:

> Secrecy is metacommunicative because when one hears the telling of a secret, several implicit instructions accompany it and constitute its key. That includes not only how the talk is to be understood but also that the information is not to be repeated and that the source where the knowledge was obtained is to be protected [2, p. 9].

In the sequel, we aim to elaborate on Bellman's perspective by addressing the problem of formalizing the statement:

(TS) "a intends to tell c a fact φ that a keeps secret from b"

where "to tell a secret" should be interpreted according to Bellman's interpretation. First, we argue that (TS) conveys at least three different contents: (*i*) that a is actually keeping φ secret from b; (*ii*) that a intends to let c believe that φ is indeed unknown to b, i.e., that b is factively ignorant about φ; and (*iii*) that a intends to let c know that a keeps φ secret from b. Now, a natural *desideratum* of our system would be that, if (TS) is true, then it should also be true that (*iv*) "a intends to let c keeping φ secret from b" since we are assuming that a intends to bring about a state of affairs in which b does not know that φ. While apparently modeling (*i*)-(*iii*) as $S_{a,b}\varphi$, $I_aB_cT_b\varphi$, and $I_aK_cS_{a,b}\varphi$ is quite obvious, actually the formalization of "a intends to let c knowing that –" simply as I_aK_c– is not satisfactory, because of the following

$$\nvdash_{\mathsf{SC}} (S_{a,b}\varphi \wedge I_aB_cT_b\varphi \wedge I_aK_cS_{a,b}\varphi) \rightarrow I_aS_{c,b}\varphi. \tag{3}$$

One can prove the stronger

Proposition 9. *Let* $\varphi \in \mathrm{Fm}_{\mathsf{SC}}$. *Then:*

$$\nvdash_{\mathsf{SC}} (S_{a,b}\varphi \wedge I_aK_cT_b\varphi \wedge I_aK_cS_{a,b}\varphi) \rightarrow I_aS_{c,b}\varphi. \tag{4}$$

Therefore, since it is easily seen that the formula in (3) entails the one in (4), a counterexample for the latter results in a counterexample for the former. However, such an inconvenience might be avoided by formalizing the kind of "letting know that" occurring in the telling of a secret in such a way as to include an element of "persuasion" w.r.t. intentions and beliefs. More precisely, we argue (and it is intuitively plausible) that the kind of communication involved in the telling of a secret includes that if a intends to act to bring about a state of affairs in which b does not know that φ and a intends to let c knowing the secret φ, then a intends to act in such a way that c has the same belief concerning the actual

knowledge of b that φ and she intends to behave accordingly. These conditions can be formalized as instances of the following formulas:

$$P^B_{a,c}\varphi := (B_a\varphi \wedge I_a K_c B_a\varphi) \rightarrow I_a B_c\varphi, \quad P^I_{a,c}\varphi := (I_a\varphi \wedge I_a K_c I_a\varphi) \rightarrow I_a I_c\varphi. \quad (5)$$

Given the above discourse, we argue that (at least when the telling of a secret is considered) a slightly more precise formalization of "a intends to *tell* c that φ" could be the following:

$$C_{a,c}\varphi := P^I_{a,c}\varphi \wedge P^B_{a,c}\varphi \wedge I_a K_c\varphi.$$

Note that $C_{a,c}\varphi$ has been designed in such a way to *encode* but not to *entail* an element of persuasion about intentions. It is not difficult to see that:

$$\nvdash_{\mathsf{SC}} C_{a,c}\varphi \rightarrow (I_a I_c\varphi \vee I_a B_c\varphi).$$

Consequently, this operator is still general enough to cope with a range of situations wider than the one considered in this venue.
With the above definitions, we state and prove the following proposition.

Proposition 10. *The following holds:*

$$\vdash_{\mathsf{SC}} (S_{a,b}\varphi \wedge C_{a,c}T_b\varphi \wedge C_{a,c}S_{a,b}\varphi) \rightarrow (I_a S_{c,b}\varphi \wedge I_a S_{c,b}S_{a,b}\varphi).$$

However, the following final remark is in order.

Proposition 11. *For any $\varphi \in \mathrm{Fm}_{\mathsf{SC}}$, $C, D \subseteq Ag$:*

1. $\nvdash_{\mathsf{SC}} (S_{a,b}\varphi \wedge C_{a,c}T_b\varphi \wedge C_{a,c}S_{a,b}\varphi) \rightarrow I_a \mathbb{I}_{\{a,c\}} S_{\{a,c\},\{b\}}\varphi$;
2. $\nvdash_{\mathsf{SC}} (S_{a,b}\varphi \wedge C_{a,c}T_b\varphi \wedge C_{a,c}S_{a,b}\varphi) \rightarrow I_a \mathbb{S}_{\{a,c\},\{b\}}\varphi$.

The overall moral of Proposition 11 is that the intention of communicating a secret with the aim it remains so for a targeted nescient does not guarantee *per se* an intention of creating joint commitment in preserving confidentiality. Therefore, sharing a secret with the aim of becoming a group secret needs further conditions whose investigation is left to future work.

4 Conclusion

In this paper, we have investigated the logical properties of group secrets, focusing on how they can be defined. We provided a formal framework to model and analyze the conditions under which group secrets are preserved and how different types of knowledge/belief/commitment — including individual and common knowledge, belief, and intention — interact with them. In particular, our results demonstrate how logical implication and disjunction influence the persistence of secrets within groups and reveal subtle limitations in the derivation of certain types of knowledge from others. A key takeaway from our analysis is the weakness of group secrets under logical operations determined by the possible

lack of mutual transparency of secret keepers w.r.t. intentions and beliefs and the necessary conditions for agents to keep confidential information. A further insight provided by the present work concerns the concept of secret disclosure and sufficient conditions on communication under which confidentiality persists.

There are several further promising directions for future research that the present framework hints at:

1. **Temporal Evolution of Secrets and Groups:** Future work could extend the current static framework to account for the temporal evolution of secrets and group membership to understand how secrets are maintained or lost over time, primarily as agents communicate and update their knowledge.
2. **Refinement of Group Secret Management:** Investigating additional logical constraints or different agent capabilities (e.g., partial observability, the presence of contradictions, and non-monotonic reasoning) could shed some light on complex multi-agent systems in concrete scenarios.
3. **Applications to Cryptographic Protocols for Multi-Agent Systems:** The aim is to adapt and apply the current results to the modelling of real-world cryptographic protocols that involve distributed group secrets, as in the case of multi-signature protocols and secure multi-party computations [3].
4. **Incorporation of Trust and Distrust among Agents:** Another interesting direction would be to study how trust or distrust between agents affects the preservation and distribution of secrets.

References

1. Alessandro Aldini, Davide Fazio, Pierluigi Graziani, Raffaele Mascella, and Mirko Tagliaferri. The logical art of keeping a true secret. *https://arxiv.org/abs/2405.11654*, 2024.
2. Beryl L. Bellman. The paradox of secrecy. *Human Studies*, 4(1):1–24, 1981.
3. David Evans, Vladimir Kolesnikov, and Mike Rosulek. A pragmatic introduction to secure multi-party computation. *Foundations and Trends in Privacy and Security*, 2(2-3):70–246, 2018.
4. Ivan Fedorenko, Pierre Berthon, and Linda Edelman. Top secret: Integrating 20 years of research on secrecy. *Technovation*, 123:102691, 2023.
5. Joseph Y. Halpern and Yoram Moses. A guide to completeness and complexity for modal logics of knowledge and belief. *Artificial Intelligence*, 54(3):319–379, 1992.
6. Joseph Y. Halpern and Kevin R. O'Neill. Secrecy in multiagent systems. *ACM Trans. Inf. Syst. Secur.*, 12(1):5:1–5:47, 2008.
7. G. E. Hughes and M. J. Cresswell. *A companion to modal logic.* Methuen, New York, 1984.
8. Haythem O. Ismail and Merna Shafie. A commonsense theory of secrets. In Boyan Brodaric and Fabian Neuhaus, editors, *Formal Ontology in Information Systems - Proceedings of the 11th International Conference, FOIS 2020, Cancelled / Bozen-Bolzano, Italy, September 14-17, 2020*, volume 330 of *Frontiers in Artificial Intelligence and Applications*, pages 77–91. IOS Press, 2020.
9. Anita E. Kelly. *The Psychology of Secrets.* Springer New York, NY, 2002.

10. Kirsten M. Robertson, David R. Hannah, and Brenda A. Lautsch. The secret to protecting trade secrets: How to create positive secrecy climates in organizations. *Business Horizons*, 58(6):669–677, 2015. Special issue: The Magic of Secrets.
11. Michael Slepian. *The Secret Life of Secrets: How Our Inner Worlds Shape Well-Being, Relationships, and Who We Are*. Crown, 2022.
12. Michael L. Slepian. A process model of having and keeping secrets. *Psychological Review*, 129(3):542–563, 2022.
13. Michael L. Slepian, Jinseok S. Chun, and Malia F. Mason. The experience of secrecy. *Journal of Personality and Social Psychology*, 113(1):1–33, 2017.
14. Ugo Volli. Figure della reticenza. riservatezza, segreto, pudore, privacy, silenzio, sacro, storytelling. *Versus, quaderni di studi semiotici*, 130(1):19–32, 2020.
15. Zuojun Xiong and Thomas Ågotnes. The logic of secrets and the interpolation rule. *Ann. Math. Artif. Intell.*, 91(4):375–407, 2023.

PROOFS

Note

This section contains additional details on the formal proofs of the results presented in the article's main body. However, it is not meant to be an integral part of the paper but rather as a supplementary material. In case of acceptance, a pre-print version of this work and the proofs below will be made available on the CIFMA 2024 website and ArXiv.

Proposition 2.

Proof. By (S), one clearly has $\vdash_{\mathsf{SC}} \mathbb{S}_{a,b}\varphi \rightarrow S_{a,b}\varphi$. Conversely, by [1, Proposition 3], one has $\vdash_{\mathsf{SC}} S_{a,b}\varphi \rightarrow I_a^n S_{a,b}\varphi$, for any $n \geq 0$. In turn, this entails $\vdash_{\mathsf{SC}} S_{a,b}\varphi \rightarrow \mathbb{I}_a S_{a,b}\varphi$. Similarly, putting in good use [1, Proposition 2](4) and (A6), one can prove $\vdash_{\mathsf{SC}} S_{a,b}\varphi \rightarrow B_a^n S_{a,b}\varphi$, for any $n \geq 0$, and so $\vdash_{\mathsf{SC}} S_{a,b}\varphi \rightarrow \mathbb{B}_a S_{a,b}\varphi$. Consequently, one has $\vdash_{\mathsf{SC}} S_{a,b}\varphi \rightarrow \mathbb{S}_{a,b}\varphi$.

Proposition 3.

Proof. We confine ourselves to prove (5). Let $\mathcal{M}$ be an arbitrary $\mathcal{S}$-model and let $i \in W$. We prove that, for any $n \geq 1$, $\mathcal{M}, i \models (E_C^B)^n \mathbb{K}_C\varphi$. For $n = 1$, note that $\mathcal{M}, i \models \mathbb{K}_C\varphi$ implies $\mathcal{M}, i \models E_C^K \mathbb{K}_C\varphi$. (A6) and customary arguments yield $\mathcal{M}, i \models E_C^B \mathbb{K}_C\varphi$. The inductive step of the proof can be carried out similarly upon noticing that $\mathcal{M}, i \models (E_C^B)^n \mathbb{K}_{\mathbb{C}}\varphi \rightarrow (E_C^B)^n E_C^K \mathbb{K}_{\mathbb{C}}\varphi$ and $\mathcal{M}, i \models (E_C^B)^n E_C^K \mathbb{K}_{\mathbb{C}}\varphi \rightarrow (E_C^B)^n E_C^B \mathbb{K}_{\mathbb{C}}\varphi$.

Proposition 4.

Proof. (1)-(3) are direct consequences of [1, Proposition 2] and the definition of $\mathbb{S}_{C,D}$, since $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \rightarrow S_{a,b}\varphi$, for any $a \in C, b \in D$ and it is easily verified that $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \rightarrow \mathbb{B}_C S_{C,D}\varphi$ and $\vdash_{\mathsf{SC}} \mathbb{B}_C S_{C,D}\varphi \rightarrow B_a S_{C,D}\varphi$.
(4) Note that $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \rightarrow \mathbb{B}_C S_{C,D}\varphi$. Moreover, by Proposition 3 and the transitivity of material implication $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \rightarrow \mathbb{B}_C \mathbb{B}_C S_{C,D}\varphi$. Therefore, we conclude $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \wedge \mathbb{B}_C \mathbb{I}_C S_{C,D}\varphi \rightarrow \mathbb{B}_C \mathbb{B}_C S_{C,D}\varphi \wedge \mathbb{B}_C \mathbb{I}_C S_{C,D}\varphi \wedge \mathbb{B}_C S_{C,D}\varphi$. Since $\mathbb{B}_C$ distributes over conjunctions, our conclusion follows. (5) and (6) are direct consequences of (2) by means of applications of classical propositional logic and the distributivity of K_d over implication. As regards (7), $\vdash_{\mathsf{SC}} \neg \mathbb{S}_{C,D} K_d\varphi$ follows upon noticing that $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D} K_d\varphi \rightarrow S_{C,D} K_d\varphi$ and $\vdash_{\mathsf{SC}} \neg S_{C,D} K_d\varphi$, by [1, Proposition 2]. (8) By definition $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\neg\varphi \rightarrow S_{C,D}\neg\varphi$, In turn, $\vdash_{\mathsf{SC}} S_{C,D}\neg\varphi \rightarrow \neg S_{C,D}\varphi$. Our conclusion follows by $\vdash_{\mathsf{SC}} \neg S_{C,D}\varphi \rightarrow \neg \mathbb{S}_{C,D}\varphi$, the transitivity of material implication and contraposition. Finally, as regards (9), note that if $\mathcal{M}, i \models \mathbb{S}_{C,D} \mathbb{K}_D\varphi$, then $\mathcal{M}, \models S_{C,D}\varphi$ and so $\mathcal{M}, i \models E_C^K \mathbb{K}_D\varphi$. In turn, this implies $\mathcal{M}, i \models E_C^B \mathbb{K}_D\varphi$. However, one has also $\mathcal{M}, i \models E_C^B(\bigwedge_{b \in D} \neg K_b \mathbb{K}_D\varphi)$ which entails $\mathcal{M}, i \models E_C^B \neg \mathbb{K}_D\varphi$ and so $\mathcal{M}, i \models E_C^B(\mathbb{K}_D\varphi \wedge \neg \mathbb{K}_D\varphi)$ which is impossible.

Finally, as regards (10), it is easily proved that $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \rightarrow B_a K_b\varphi$, for any $a, b \in C$. Moreover, one has also $\vdash_{\mathsf{SC}} B_a K_b\varphi \rightarrow \neg S_{a,b}\varphi$ (cf. [1]). We conclude that $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \rightarrow \neg S_{a,b}\varphi$ and, using an identical argument $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi \rightarrow \neg S_{b,a}\varphi$.

Let A be a non-empty set. We set $\Delta_A = A \times A$.

Proposition 5.

Proof. As regards (1), let us consider the following model

$$\mathcal{M} = (W, \{R_a^I\}_{a\in Ag}, \{R_a^K\}_{a\in Ag}, \{R_a^B\}_{a\in Ag}, v),$$

with $W = \{i, j, k, u_1, v\}$ and, for fixed $a, b, c \in Ag$ accessibility relations defined as follows:

$R_a^K = R_a^B := \Delta_W$;
$R_a^I := \Delta_W \cup \{(j, k)\}$
$R_b^K = R_b^B := \Delta_W \cup \{(i, j)\}$;
$R_b^I := \Delta_W \setminus \{i, i\} \cup \{(k, u_1), (i, v)\}$;
$R_c^K = R_c^B = R_c^I := \Delta_W \cup \{(i, u), (j, u), (k, u), (v, u)\}$.

Moreover, let $v : Var \to \mathcal{P}(\mathrm{Fm}_{\mathsf{SC}})$ be such that $v(p) = \{i, j, k, u_1, v\}$ and $v(q) = \emptyset$, for any other $q \in Var \setminus \{p\}$. It can be verified that $\mathcal{M}$ is an $\mathcal{S}$-frame. Upon extending v to an evaluation on the whole $\mathrm{Fm}_{\mathsf{SC}}$ and setting $C = \{a, b\}$ and $D = \{c\}$ it can be seen that $\mathcal{M}, i \models \mathbb{S}_{C,D}p$ but $\mathcal{M}, i \not\models \mathbb{B}_C\mathbb{S}_{C,D}p$. (2) and (3) are direct consequences of (1).
We prove (4) and (5) at once. Consider the following model

$$\mathcal{M} = (W, \{R_a^I\}_{a\in Ag}, \{R_a^K\}_{a\in Ag}, \{R_a^B\}_{a\in Ag}, v),$$

with $W = \{i, u, j, k, w, u_1\}$ and, for fixed $a, b, c \in Ag$ accessibility relations defined as follows:

$R_a^K := \Delta_W$
$R_a^K = R_a^B := \Delta_W \cup \{(j, k)\}$;
$R_a^I := \Delta_W \setminus \{(j, j), (k, k)\} \cup \{(j, u_1), (k, u_1)\}$;
$R_b^K = R_b^B := \Delta_W$;
$R_b^I := \Delta_W \setminus \{(i, i), (k, k)\} \cup \{(i, j), (k, w)\}$;
$R_c^K = R_c^B = R_c^I := \Delta_W \cup \{(i, u), (j, u), (k, u), (u_1, u)\}$.

Moreover, let $v(p) = W \setminus \{u\}$ and $v(q) = \emptyset$ for any other $q \neq p$. One has that $\mathcal{M}$ is an $\mathcal{S}$-model and $\mathcal{M}, i \models \mathbb{S}_{C,D}p$ but $\mathcal{M}, i \not\models \mathbb{I}_C\mathbb{B}_C\mathbb{S}_{C,D}p$ as well as $\mathcal{M}, i \not\models \mathbb{I}_C\mathbb{S}_{C,D}p$.
As regards (6), let us consider the following $\mathcal{S}$-model

$$\mathcal{M} = (W, \{R_a^I\}_{a\in Ag}, \{R_a^K\}_{a\in Ag}, \{R_a^B\}_{a\in Ag}, v),$$

where $W = \{i, j, k, k_1, u, u_1, v, w\}$ and for fixed $a, b, c \in Ag$:

$R_a^K = R_a^B = R_a^I := \Delta_W$;
$R_b^K := \Delta_W \cup \{(i, j)\}$;
– $R_b^B := \Delta_W$;
– $R_b^I := \{(i, v), (i, k_1), (w, u)\} \cup \Delta_W \setminus \{(i, i), (j, j), (w, w)\}$;
– $R_c^K := \Delta_W \cup \{(i, w)\}$;

– $R_c^B := \Delta_W$;
– $R_c^I := \{(i,v),(i,u_1),(j,k),(w,u_1)\} \cup \Delta_W \smallsetminus \{(i,i),(j,j),(w,w)\}$.
– $R_d^K = R_d^B = R_d^I := \Delta_W$, for any $d \in Ag \smallsetminus \{b,c\}$.

Moreover, let $C = \{a\}$ and $D = \{b,c\}$. Also, let $v : Var \to \mathcal{P}(W)$ be such that $v(p) = \{i,j,v,k_1,w,u_1\}$ for a fixed p and $v(q) = \emptyset$, for any other $q \in Var \smallsetminus \{p\}$. Upon extending v to an evaluation on the whole $\mathrm{Fm}_{\mathsf{SC}}$, it can be seen that $\mathcal{M}, i \models \mathbb{S}_{C,D}\mathbb{I}_D p$.
To show (7), it suffices to exploit the countermodel exhibited in the proof of (6) with minor variations. Indeed, it suffices to set for fixed $a,b,c \in Ag$:

$R_a^K = R_a^B = R_a^I := \Delta_W$;
$R_b^K := \Delta_W \cup \{(i,j),(i,k_1),(j,k_1),(w,u),(i,v)\}$;
– $R_b^B := \Delta_W \cup \{(i,v),(i,k_1),(j,k_1)\}$;
– $R_b^I := \{(i,v),(i,k_1),(w,u)\} \cup \Delta_W \smallsetminus \{(i,i),(j,j),(w,w)\}$;
– $R_c^K := \Delta_W \cup \{(i,w),(j,k),(w,u_1),(i,u_1),(i,v)\}$;
– $R_c^B := \Delta_W \cup \{(j,k),(w,u_1),(i,u_1),(i,v)\}$;
– $R_c^I := \{(i,v),(i,u_1),(j,k),(w,u_1)\} \cup \Delta_W \smallsetminus \{(i,i),(j,j),(w,w)\}$.
– $R_d^K = R_d^B = R_d^I := \Delta_W$, for any $d \in Ag \smallsetminus \{b,c\}$.

A direct inspection yields that the resulting frame is still an $\mathcal{S}$-frame. Upon defining v as above, one has that $\mathcal{M}, i \models \mathbb{S}_{C,D}\mathbb{B}_D\varphi$.

Proposition 6.

Proof. (1) Let $\mathcal{M}$ be an arbitrary $\mathcal{S}$-model and $i \in W$. Assume that $\mathcal{M}, i \models \mathbb{S}_{C,D}\varphi \wedge \mathbb{S}_{C,D}\chi$. One has $\mathcal{M}, i \models S_{a,b}\varphi \wedge S_{a,b}\chi$, for any $a \in C$ and $b \in D$ and so, by [1, Proposition 4](3), $\mathcal{M}, i \models S_{a,b}\psi$ (for any $a \in C$, $b \in D$). We conclude $\mathcal{M}, i \models S_{C,D}\psi$. Moreover, Let $n \geq 1$. One has that $\mathcal{M}, i \models \mathbb{S}_{C,D}\varphi$ implies $\mathcal{M}, i \models \mathbb{I}_C S_{C,D}\varphi \wedge \mathbb{I}_C S_{C,D}\chi$. Therefore, for any $j \in W$ such that $(R_C^I)^n(i,j)$, $\mathcal{M}, j \models S_{C,D}\varphi \wedge S_{C,D}\chi$. Reasoning as above we conclude $\mathcal{M}, j \models S_{C,D}\psi$ and, since j and n are arbitrary, we have $\mathcal{M}, i \models (E_C^I)^n\psi$ for any $n \geq 1$. This means $\mathcal{M}, i \models \mathbb{I}_C S_{C,D}\psi$. Similarly, one proves $\mathcal{M}, i \models \mathbb{B}_C S_{C,D}\psi$ and so $\mathcal{M}, i \models \mathbb{S}_{C,D}\psi$.
(2) Can be proven by induction on n upon noticing that, if $n = 2$, the the statement follows from (1). If the statements holds for n, by induction hypothesis one has that $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi_1 \wedge \mathbb{S}_{C,D}\varphi_n \to \bigwedge_{1 \leq i \leq n} \mathbb{S}_{C,D}\varphi_i$. Moreover by the transitivity of classical implication one has $\vdash_{\mathsf{SC}} \varphi_1 \to \varphi_n$ and $\vdash_{\mathsf{SC}} \varphi_n \to \varphi_{n+1}$, therefore, by (1), $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}\varphi_1 \wedge \mathbb{S}_{C,D}\varphi_{n+1} \to \mathbb{S}_{C,D}\varphi_n$. Our conclusion follows by a straightforward application of classical propositional logic.

Proposition 7.

Proof. Concerning (1), just note that $\vdash_{\mathsf{SC}} \mathbb{B}_C K_b\psi \vee \mathbb{I}_C K_b\psi \to\!\!\to B_a K_b\psi \vee I_a K_b\psi$, for any $a \in C$. In turn, one has $\vdash_{\mathsf{SC}} B_a K_b\psi \vee I_a K_b\psi \to \neg S_{a,b}(\varphi \to \psi)$ from [1, Proposition 6](1), since SC is a conservative expansion of S. As a consequence, since $\vdash_{\mathsf{SC}} \mathbb{S}_{C,D}(\varphi \to \psi) \to S_{a,b}(\varphi \to \psi)$, for any $a \in C$, $b \in D$, our conclusion follows by contraposition and the transitivity of implication. (2) can be proven similarly.
As regards (3), If $\mathcal{M}, i \models \mathbb{S}_{C,D}\varphi \wedge \mathbb{S}_{C,D}\psi$, one has $\mathcal{M}, i \models \mathbb{I}_C S_{C,D}\varphi \wedge \mathbb{I}_C S_{C,D}\psi$ and

so $\mathcal{M}, i \models \mathbb{I}_C(S_{C,D}\varphi \wedge S_{C,D}\psi)$. Moreover, several applications of [1, Proposition 7](2) yield (*) $\vdash_{\mathsf{SC}} S_{C,D}\varphi \wedge S_{C,D}\psi \rightarrow S_{C,D}(\varphi \wedge \psi)$. By the distributivity of $\mathbb{I}_C$ over $\rightarrow$, one has $\vdash_{\mathsf{SC}} \mathbb{I}_C(S_{C,D}\varphi \wedge S_{C,D}\psi) \rightarrow \mathbb{I}_C S_{C,D}(\varphi \wedge \psi)$. Consequently, $\mathcal{M}, i \models \mathbb{I}_C S_{C,D}(\varphi \wedge \psi)$. Similarly, one has $\mathcal{M}, i \models \mathbb{B}_C S_{C,D}(\varphi \wedge \psi)$, while by hypothesis and by (*), we have $\mathcal{M}, i \models S_{C,D}(\varphi \wedge \psi)$. The proof of (4) is analogous. Let us consider (5). $\mathcal{M}, i \models \mathbb{S}_{C,D}\varphi \wedge \mathbb{B}_C E^K_C \psi \wedge \mathbb{B}_C E^I_C \psi$ implies $\mathcal{M}, i \models \mathbb{B}_C(S_{C,D}\varphi \wedge E^K_C\psi \wedge E^I_C\psi)$ which, by several applications of [1, Proposition 7](1), yields $\mathcal{M}, i \models \mathbb{B}_C S_{C,D}(\varphi \wedge \psi))$. Also, an easy check shows that $\mathcal{M}, i \models \mathbb{S}_{C,D}\varphi \wedge \mathbb{I}_C E^K_C \psi$ entails $\mathcal{M}, i \models \mathbb{I}_C(S_{C,D}\varphi \wedge E^K_C\psi \wedge E^I_C\psi)$ which, again by [1, Proposition 7](1) entails $\mathcal{M}, i \models \mathbb{I}_C S_{C,D}(\varphi \wedge \psi)$. Finally, $\mathcal{M}, i \models S_{C,D}(\varphi \wedge \psi)$ follows $\mathcal{M}, i \models S_{C,D}\varphi \wedge E^K_C\psi \wedge \mathbb{I}_C E^K_C \psi$, since $\mathcal{M}, i \models \mathbb{I}_C E^K_C \psi \rightarrow E^I_C \psi$.
(6) Let us consider the following model

$$\mathcal{M} = (W, \{R^I_a\}_{a\in Ag}, \{R^K_a\}_{a\in Ag}, \{R^B_a\}_{a\in Ag}, v),$$

with $W = \{i, j, k, u, w\}$ and, for fixed $a, b, c \in Ag$ accessibility relations defined as follows:

$$\begin{array}{l} R^K_a = R^B_a := \Delta_W \cup \{(i,k)\}; \\ R^I_a := \Delta_W \setminus \{(i,i),(k,k)\} \cup \{(i,w),(k,w)\}; \\ R^K_b = R^B_b := \Delta_W \cup \{(k,w),(i,w)\}; \\ R^I_b := \Delta_W \setminus \{(i,i),(k,k)\} \cup \{(i,w),(k,u)\}; \\ R^K_c = R^B_c = R^I_c := \Delta_W \cup \{i,w,k,u\} \times \{j\}. \end{array}$$

Moreover, let v be defined as $v(p) := \{i, w, k, u\}$ and $v(q) := \{i, w, k\}$, for fixed $p, q \in Var$, and let $v(r) = \emptyset$ for any other $r \in Var \setminus \{p, q\}$. Also, set $C := \{a, b\}$ and $D := \{c\}$. Upon extending v to an evaluation on the whole $\mathrm{Fm}_{\mathsf{SC}}$, one has that $\mathcal{M}, i \models \mathbb{S}_{C,D}p \wedge \mathbb{K}_C q \wedge \mathbb{I}_C q$ but $\mathcal{M}, i \not\models \mathbb{S}_{C,D}(p \wedge q)$.

Proposition 8.

Proof. As regards (1), let $\mathcal{M}$ be an arbitrary $\mathcal{S}$-model and $i \in W$. Suppose $\mathcal{M}, i \models \mathbb{S}_{C,D}(\varphi \vee \psi)$. Note that, by multiple applications of [1, Proposition 9](1), one has (*) $\vdash_{\mathsf{SC}} S_{C,D}(\varphi \vee \psi) \wedge E^K_C\varphi \wedge E^I_C\varphi \rightarrow S_{C,D}\varphi$. Now, assume $\mathcal{M}, i \models (E^K_C\varphi \wedge \mathbb{I}_C E^K_C \varphi \wedge \mathbb{B}_C(E^I_C\varphi \wedge E^K_C\varphi))$. By $\mathcal{M}, i \models \mathbb{I}_C\varphi$, we obtain $\mathcal{M}, i \models E^I_C\varphi$. So, by the previous observation, it follows that $\mathcal{M}, i \models S_{C,D}\varphi$. Moreover, routine arguments yield that $\mathcal{M}, i \models \mathbb{S}_{C,D}(\varphi \vee \psi) \wedge \mathbb{I}_C E^I_C\varphi$ entails $\mathcal{M}, i \models \mathbb{I}_C(S_{C,D}(\varphi \vee \psi) \wedge E^I_C\varphi \wedge E^K_C\varphi)$. Therefore, as (*) and the distributivity of $\mathbb{I}_C$ over implication yields $\mathcal{M}, i \models \mathbb{I}_C(S_{C,D}(\varphi \vee \psi) \wedge E^K_C\varphi \wedge E^I_C\varphi) \rightarrow \mathbb{I}_C S_{C,D}\varphi$, we conclude $\mathcal{M}, i \models \mathbb{I}_C S_{C,D}\varphi$. To show that $\mathcal{M}, i \models \mathbb{B}_C S_{C,D}\varphi$ we apply an analogous argument upon considering that $\mathbb{M}, i \models \mathbb{S}_{C,D}(\varphi\vee\psi)\wedge\mathbb{B}_C(E^I_C\varphi\wedge E^K_C\varphi)$ implies $\mathcal{M}, i \models \mathbb{B}_C(S_{C,D}(\varphi \vee \psi) \wedge E^I_C\varphi \wedge E^K_C\varphi)$. Conversely, if $\mathcal{M}, i \models \mathbb{S}_{C,D}\varphi$, then one has $\mathcal{M}, i \models \mathbb{B}_C(S_{C,D}\varphi)$ and so also $\mathcal{M}, i \models \mathbb{B}_C(E^K_C\varphi \wedge E^I_C\varphi)$. Moreover, by $\mathcal{M}, i \models S_{C,D}\varphi \wedge \mathbb{I}_C S_{C,D}\varphi$, we have $\mathcal{M}, i \models E^K_C\varphi \wedge \mathbb{I}_C E^K_C\varphi$.
A finite countermodel for (2) can be rovided upon taking into account (1), as e.g. it is easily shown that $\not\vdash_{\mathsf{SC}} \mathbb{K}_C\varphi \wedge \mathbb{I}_C\varphi \rightarrow \mathbb{I}_C E^K_C\varphi$.

Proposition 9.

Proof. To prove the claim, let us consider the model

$$\mathcal{M} = (W = \{i, j, w\}, \{R_a^I\}_{a \in Ag}, \{R_a^K\}_{a \in Ag}, \{R_a^B\}_{a \in Ag}, v)$$

such that for some $a, b \in Ag$ with $a \neq c$

- $R_a^I = R_a^B = R_a^K := \Delta_W$;
- $R_c^I := \{(i, w), (w, w), (j, j)\}$;
- $R_c^K = R_c^B := \Delta_W$,

and, for any other $b \in Ag$ such that $b \neq a, c$

- $R_b^B = R_b^K := \Delta_W \cup \{(i, j)\}$;
- $R_b^I := \Delta_W$.

Moreover, let v be such that, for a fixed $p \in Var$, $v(p) = \{i, w\}$. One has $\mathcal{M}, i \models S_{a,b}p \wedge I_a K_c T_b p \wedge I_a K_c S_{a,b} p$. However, $\mathcal{M}, i \not\models I_a S_{c,b} p$, since $\mathcal{M}, i \not\models I_c \neg K_b p$.

Proposition 10.

Proof. Let $\mathcal{M}$ be an arbitrary $\mathcal{S}$-model and let $i \in W$. Note that $\mathcal{M}, i \models C_{a,c} S_{a,b} \varphi$ implies $\mathcal{M}, i \models I_a K_c S_{a,b} \varphi$ which, in turn, implies $\mathcal{M}, i \models I_a K_c I_a T_b \varphi$; moreover, by $\mathcal{M}, i \models S_{a,b}\varphi$ one has also $\mathcal{M}, i \models I_a T_b \varphi$. Therefore, by $\mathcal{M}, i \models C_{a,c} T_b \varphi$, we have $\mathcal{M}, i \models I_a I_c T_b \varphi$. Also, by $\mathcal{M}, i \models C_{a,c} T_b \varphi$, we have $\mathcal{M}, i \models I_a K_c(\varphi \wedge \neg K_b \varphi)$ and so $\mathcal{M}, i \models I_a K_c \varphi$ and $\mathcal{M}, i \models I_a K_c \neg K_b \varphi$. Therefore, we conclude $\mathcal{M}, i \models I_a K_c \varphi \wedge I_a B_c \neg K_b \varphi \wedge I_a I_c T_b \varphi$ which, by the distributivity of I_a over $\wedge$ boils down to $\mathcal{M}, i \models I_a S_{c,b} \varphi$. In order to prove $\mathcal{M}, i \models I_a S_{c,b} S_{a,b} \varphi$ we first observe that $\mathcal{M}, i \models C_{a,c} S_{a,b} \varphi$ entails $\mathcal{M}, i \models I_a K_c S_{a,b} \varphi$. Also, since $\mathcal{M}, i \models S_{a,b}\varphi$, one has $\mathcal{M}, i \models I_a S_{a,b} \varphi$ ([1, Proposition 2](5)), and we have $\mathcal{M}, i \models I_a I_c S_{a,b} \varphi$. Now, by [1, Proposition 15](5), we have

$$\vdash_{\mathsf{SC}} S_{c,b}\varphi \wedge K_c S_{a,b}\varphi \rightarrow (I_c S_{a,b}\varphi \rightarrow S_{c,b}(S_{a,b}\varphi)).$$

Using customary arguments, one has $\vdash_{\mathsf{SC}} I_a(S_{c,b}\varphi \wedge K_c S_{a,b}\varphi) \rightarrow I_a(I_c S_{a,b}\varphi \rightarrow S_{c,b}(S_{a,b}\varphi))$ and $\vdash_{\mathsf{SC}} I_a S_{c,b}\varphi \wedge I_a K_c S_{a,b}\varphi \rightarrow (I_a I_c S_{a,b}\varphi \rightarrow I_a S_{c,b}(S_{a,b}\varphi))$. Consequently, we have also $\mathcal{M}, i \models I_a S_{c,b}(S_{a,b}\varphi)$.

Proposition 11.

Proof. (2) is a direct consequence of (1). Let us prove (1). Let us consider the structure

$$\mathcal{M} = (\{i, w, u, k, l, m, n, v\}, \{R_a^I\}_{a \in Ag}, \{R_a^K\}_{a \in Ag}, \{R_a^B\}_{a \in Ag}, v),$$

such that, for fixed $a, b, c \in Ag$ accessibility relations are defined as follows:

$R_a^K = R_a^B := \Delta_W \cup \{(i, k)\}$;
$R_a^I := \Delta_W \setminus \{(m, m)\} \cup \{(i, k), (m, l), (i, w)\}$;
$R_b^K = R_b^B = R_b^I := \Delta_W \cup ((W \setminus \{v\}) \times \{u\}) \cup \{(n, v)\}$;
$R_c^K = R_c^B := \Delta_W \cup \{i, w, k, u\} \times \{j\}$;
$R_c^I := \Delta_W \setminus \{(i, i), (l, l)\} \cup \{(i, m), (l, n)\}$.

Moreover, let v be such that $v(p) = W \setminus \{u\}$ and $v(q) = \emptyset$ for any other $q \in Var \setminus \{p\}$. Upon extending v to an evaluation on the whole $\mathrm{Fm}_{\mathsf{SC}}$, one has that $\mathcal{M}, i \models S_{a,b}\varphi \wedge C_{a,c} T_b \varphi \wedge C_{a,c} S_{a,b} \varphi$ but $\mathcal{M}, i \not\models I_a I_c I_a I_c \neg K_b \varphi$. So we conclude $\mathcal{M}, i \not\models I_a \mathbb{I}_{\{a,c\}} S_{\{a,c\},\{b\}} \varphi$