The Logic of Secrets

LAMAS 2020, 8 May 2020

Thomas Ågotnes
University of Bergen, Norway
Southwest University (SWU), China

Zuojun Xiong, SWU
Yuzhi Zhang, SWU

Secrets

- Of fundamental importance in, e.g.,
  - safety and security
  - cryptography
  - authentication
  - access control
  - …
  - (and in business and politics and romance and..)

What is a secret?

- "*a piece of knowledge that is hidden and intended to be kept hidden*" (Wiktionary)
- "*a piece of information that is only known by one person or a few people and should not be told to others*" (Cambridge Dictionary)
- "*something that is kept or meant to be kept unknown or unseen by others*" (Oxford English Dictionary)
- "*something kept from the knowledge of others*" (Merriam-Webster)

What is a secret?

Fundamentally about knowledge and ignorance

- *"a piece of knowledge that is hidden and intended to be kept hidden"* (Wiktionary)
- *"a piece of information that is only known by one person or a few people and should not be told to others"* (Cambridge Dictionary)
- *"something that is kept or meant to be kept unknown or unseen by others"* (Oxford English Dictionary)
- *"something kept from the knowledge of others"* (Merriam-Webster)

In this paper we

- Formalise secrets (more precisely: secretly knowing)
- Using the standard framework for reasoning about knowledge and ignorance: modal epistemic logic
- Key question: what are the (epistemic) properties of secretly knowing?
- Introduce a modality for secretly knowing and study its properties

$$S_a\varphi$$

$$a \text{ secretly knows } \varphi$$

Necessary epistemic conditions for secretly knowing

$$a \text{ secretly knows } \varphi$$

Necessary epistemic conditions for secretly knowing

$$a \text{ secretly knows } \varphi$$

(1) a knows φ

Necessary epistemic conditions for secretly knowing

$$a \text{ secretly knows } \varphi$$

(1) a knows φ $\qquad K_a\varphi$

Necessary epistemic conditions for secretly knowing

a secretly knows φ

(1) a knows φ $\qquad K_a\varphi$

(2) any other agent b does not know φ

Necessary epistemic conditions for secretly knowing

a secretly knows φ

(1) a knows φ $\qquad K_a\varphi$

(2) any other agent b does not know φ $\qquad \bigwedge_{b \neq a} \neg K_b\varphi$

Necessary epistemic conditions for secretly knowing

a secretly knows φ

(1) a knows φ $\qquad K_a\varphi$

(2) any other agent b does not know φ $\qquad \bigwedge_{b\neq a}\neg K_b\varphi$

(2') a knows that any other agent b does not know φ

Necessary epistemic conditions for secretly knowing

a secretly knows φ

(1) a knows φ $K_a\varphi$

(2) any other agent b does not know φ $\bigwedge_{b\neq a}\neg K_b\varphi$

(2') a knows that any other agent b does not know φ

$$K_a \bigwedge_{b\neq a}\neg K_b\varphi$$

Necessary epistemic conditions for secretly knowing

a secretly knows φ

(1) a knows φ $\quad K_a\varphi$

(2) any other agent b does not know φ $\quad \bigwedge_{b\neq a}\neg K_b\varphi$

(2') a knows that any other agent b does not know φ

$$K_a \bigwedge_{b\neq a}\neg K_b\varphi$$

(2") a knows that any other agent b does not know whether φ

Necessary epistemic conditions for secretly knowing

a secretly knows φ

(1) a knows φ $\qquad K_a\varphi$

(2) any other agent b does not know φ $\qquad \bigwedge_{b\neq a} \neg K_b\varphi$

(2') a knows that any other agent b does not know φ

$$K_a \bigwedge_{b\neq a} \neg K_b\varphi$$

(2'') a knows that any other agent b does not know whether φ

$$K_a \bigwedge_{b\neq a}(\neg K_b\varphi \wedge \neg K_b\neg\varphi)$$

Necessary epistemic conditions for secretly knowing

a secretly knows φ

(1) a knows φ $\qquad K_a\varphi$

(2) any other agent b does not know φ $\qquad \bigwedge_{b\neq a}\neg K_b\varphi$

(2') a knows that any other agent b does not know φ

$$K_a \bigwedge_{b\neq a}\neg K_b\varphi$$

(2'') a knows that any other agent b does not know whether φ

$$K_a \bigwedge_{b\neq a}(\neg K_b\varphi\wedge\neg K_b\neg\varphi)$$

Necessary epistemic conditions for secretly knowing

a secretly knows φ

(1) a knows φ $K_a\varphi$

(2) any other agent b does not know φ $\bigwedge_{b\neq a}\neg K_b\varphi$

(2') a knows that any other agent b does not know φ

$$K_a \bigwedge_{b\neq a}\neg K_b\varphi$$

(2'') a knows that any other agent b does not know whether φ

$$K_a \bigwedge_{b\neq a}(\neg K_b\varphi \wedge \neg K_b\neg\varphi)$$

$$K_a\varphi \wedge K_a \bigwedge_{b\neq a}\neg K_b\varphi$$

The secretly-knowing modality

$\mathcal{L}_{SK}$:

$$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid S_a\varphi$$

The secretly-knowing modality

$\mathcal{L}_{SK}$:

$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid S_a\varphi$

Epistemic model: $M = (W, \sim, V)$ $\sim_a \subseteq W \times W$ eq. rel., $V : W \to 2^{\texttt{Prop}}$

The secretly-knowing modality

$\mathcal{L}_{SK}$:

$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid S_a\varphi$

Epistemic model: $M = (W, \sim, V)$ $\quad\quad\quad\quad\quad$ $\sim_a \subseteq W \times W$ eq. rel., $V : W \to 2^{\texttt{Prop}}$

$M, w \models p$	iff	$w \in V(p)$.
$M, w \models \neg\varphi$	iff	$M, w \not\models \varphi$.
$M, w \models \varphi \wedge \psi$	iff	$M, w \models \varphi$ and $M, w \models \psi$.
$M, w \models K_a\varphi$	iff	$\forall w' \in W$, if $w \sim_a w'$, then $M, w' \models \varphi$.
$M, w \models S_a\varphi$	iff	$\forall w' \sim_a w\ M, w' \models \varphi$ and $\forall b \neq a$, $\exists u \sim_b w'\ M, u \models \neg\varphi$.

The secretly-knowing modality

$\mathcal{L}_{SK}$:

$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid S_a\varphi$

Epistemic model: $M = (W, \sim, V)$ $\quad\quad$ $\sim_a \subseteq W \times W$ eq. rel., $V : W \to 2^{\texttt{Prop}}$

$M, w \models p$	iff	$w \in V(p)$.
$M, w \models \neg\varphi$	iff	$M, w \not\models \varphi$.
$M, w \models \varphi \wedge \psi$	iff	$M, w \models \varphi$ and $M, w \models \psi$.
$M, w \models K_a\varphi$	iff	$\forall w' \in W$, if $w \sim_a w'$, then $M, w' \models \varphi$.
$M, w \models S_a\varphi$	iff	$\forall w' \sim_a w\ M, w' \models \varphi$ and $\forall b \neq a$, $\exists u \sim_b w'\ M, u \models \neg\varphi$.

Have that: $M, w \models S_a\varphi \Leftrightarrow M, w \models K_a\varphi \wedge K_a \bigwedge_{b \neq a} \neg K_b\varphi$

The secretly-knowing modality

$\mathcal{L}_S$:
$\psi ::= p \mid \neg\psi \mid (\psi \wedge \psi) \mid S_a\psi$

Epistemic model: $M = (W, \sim, V)$ $\quad\quad$ $\sim_a \subseteq W \times W$ eq. rel., $V : W \to 2^{\texttt{Prop}}$

$$
\begin{array}{lll}
M, w \models p & \text{iff} & w \in V(p). \\
M, w \models \neg\varphi & \text{iff} & M, w \not\models \varphi. \\
M, w \models \varphi \wedge \psi & \text{iff} & M, w \models \varphi \text{ and } M, w \models \psi. \\
M, w \models S_a\varphi & \text{iff} & \forall w' \sim_a w \; M, w' \models \varphi \text{ and } \forall b \neq a, \\
 & & \exists u \sim_b w' \; M, u \models \neg\varphi.
\end{array}
$$

Properties of secretly knowing: interaction axioms

Interaction axioms for S_a and K_a		
(S)	$S_a\varphi \leftrightarrow K_a\varphi \wedge K_a\Big(\bigwedge_{b\neq a} \neg K_b\varphi\Big)$	Def. of S_a
(4SK)	$S_a\varphi \rightarrow K_a S_a\varphi$	Positive secret knowledge introspection
(5SK)	$\neg S_a\varphi \rightarrow K_a\neg S_a\varphi$	Negative secret knowledge introspection
(P)	$S_a\varphi \rightarrow (K_a\varphi \wedge \neg K_b\varphi)$	Secret privacy
(NKS)	$\neg K_b S_a\varphi$	Secret unknowability
(NSK1)	$\neg S_a K_b\varphi$	Knowledge is no secret
(NSK2)	$\neg S_a \neg K_b\varphi$	Ignorance is no secret
(NC)	$K_a S_a\varphi \vee K_a\neg S_a\varphi$	Secret neg. completeness

$(a \neq b)$

Properties of secretly knowing: interaction axioms between agents

Interaction axioms for S_a and S_b		
(Ex1)	$S_a\varphi \to \neg S_b\varphi$	Secret exclusivity
(Ex2)	$S_a\neg S_a\varphi \to \neg S_b\neg S_b\varphi$	Higher-order secret exclusivity
(N1)	$\neg S_a S_b\varphi$	No secret secrets
(N2)	$\neg S_a\neg S_b\varphi$	No secret non-secrets

Properties of secretly knowing: basic principles

Axioms for S_a		
(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

Properties of secretly knowing: basic principles

Axioms for S_a		
(K)	$S_a(\varphi \rightarrow \psi) \rightarrow (S_a\varphi \rightarrow S_a\psi)$	Secret distribution
(T)	$S_a\varphi \rightarrow \varphi$	Secret veridicality
(4)	$S_a\varphi \rightarrow S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \rightarrow S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \rightarrow \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

Properties of secretly knowing: basic principles

Axioms for S_a		
(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

(5) $\neg S_a\varphi \to S_a\neg S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a		
(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

(5) $\not\models \neg S_a\varphi \to S_a\neg S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a

(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets

Rules for S_a

(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

(5) $\not\models \neg S_a\varphi \to S_a\neg S_a\varphi$

(Nec) $\models \varphi \;\Rightarrow\; \models S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a

(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets

Rules for S_a

(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

(5) $\not\models \neg S_a\varphi \to S_a\neg S_a\varphi$

(Nec) $\models \varphi \not\Rightarrow \models S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a		
(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

(5) $\not\models \neg S_a\varphi \to S_a\neg S_a\varphi$

(Nec) $\models \varphi \not\Rightarrow \models S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a

(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets

Rules for S_a

(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

(5) $\not\models \neg S_a\varphi \to S_a\neg S_a\varphi$

(Nec) $\models \varphi \not\Rightarrow \models S_a\varphi$

$\not\models \neg S_a\neg(\varphi \to \psi) \to (\neg S_a\neg\varphi \to \neg S_a\neg\psi)$

$\not\models \neg S_a(\varphi \to \psi) \to (\neg S_a\varphi \to \neg S_a\psi)$

Properties of secretly knowing: basic principles

Axioms for S_a

(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets

Rules for S_a

(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

(5) $\not\models \neg S_a\varphi \to S_a\neg S_a\varphi$ (Nec) $\models \varphi \not\Rightarrow \models S_a\varphi$

$\not\models \neg S_a\neg(\varphi \to \psi) \to (\neg S_a\neg\varphi \to \neg S_a\neg\psi)$ $\not\models \neg S_a(\varphi \to \psi) \to (\neg S_a\varphi \to \neg S_a\psi)$

(RM) $\models \varphi \to \psi \not\Rightarrow \models S_a\varphi \to S_a\psi$

Properties of secretly knowing: basic principles

Axioms for S_a

(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \land S_a\psi) \to S_a(\varphi \land \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets

Rules for S_a

(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

(5) $\not\models \neg S_a\varphi \to S_a\neg S_a\varphi$

(Nec) $\models \varphi \not\Rightarrow\ \models S_a\varphi$

$\not\models \neg S_a\neg(\varphi \to \psi) \to (\neg S_a\neg\varphi \to \neg S_a\neg\psi)$

$\not\models \neg S_a(\varphi \to \psi) \to (\neg S_a\varphi \to \neg S_a\psi)$

(RM) $\models \varphi \to \psi \not\Rightarrow\ \models S_a\varphi \to S_a\psi$

$\not\models S_a(\varphi \land \psi) \to S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a

(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets

Rules for S_a

(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

(5) $\not\models \neg S_a\varphi \to S_a\neg S_a\varphi$

(Nec) $\models \varphi \not\Rightarrow\ \models S_a\varphi$

$\not\models \neg S_a\neg(\varphi \to \psi) \to (\neg S_a\neg\varphi \to \neg S_a\neg\psi)$

$\not\models \neg S_a(\varphi \to \psi) \to (\neg S_a\varphi \to \neg S_a\psi)$

(RM) $\models \varphi \to \psi \not\Rightarrow\ \models S_a\varphi \to S_a\psi$

$\not\models S_a(\varphi \wedge \psi) \to S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a

(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
$(\top)$	$\neg S_a\top$	No tautological secrets
$(\bot)$	$\neg S_a\bot$	No contradictory secrets

Rules for S_a

(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

K+C+RE = ECK = the weakest non-normal modal logic with *neighbourhood semantics*

(RM) $\models \varphi \to \psi \not\Rightarrow \; \models S_a\varphi \to S_a\psi$ $\not\models S_a(\varphi \wedge \psi) \to S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a

(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
$(\top)$	$\neg S_a\top$	No tautological secrets
$(\bot)$	$\neg S_a\bot$	No contradictory secrets

Rules for S_a

$$M, w \models S_a\varphi \quad \text{iff} \quad \forall w' \sim_a w \; M, w' \models \varphi \text{ and } \forall b \neq a \; \exists u \sim_b w' \; M, u \models \neg\varphi.$$

K+C+RE = ECK = the weakest non-normal modal logic with *neighbourhood semantics*

(RM) $\models \varphi \to \psi \not\Rightarrow \; \models S_a\varphi \to S_a\psi$ $\qquad \not\models S_a(\varphi \wedge \psi) \to S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a		
(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
$(\top)$	$\neg S_a\top$	No tautological secrets
$(\bot)$	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

K+C+RE = ECK = the weakest non-normal modal logic with *neighbourhood semantics*

(RM) $\models \varphi \to \psi \not\Rightarrow \;\models S_a\varphi \to S_a\psi$ $\not\models S_a(\varphi \wedge \psi) \to S_a\varphi$

Properties of secretly knowing: basic principles

Axioms for S_a		
(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
$(\top)$	$\neg S_a\top$	No tautological secrets
$(\bot)$	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

K+C+RE = ECK = the weakest non-normal modal logic with *neighbourhood semantics*

S_a is a ECKT4-modality

Towards completeness

Axioms for S_a		
(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

Towards completeness

Axioms for S_a		
(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

Conjecture: The language with a single S_a modality is completely axiomatised by ECKT4+$\top$

Towards completeness

Axioms for S_a

(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution

Existing results:

ECK: completeness proof (for neighbourhood semantics) by van der Putte and McNamara currently under submission

ECK4: non-trival extension

(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

Conjecture: The language with a single S_a modality is completely axiomatised by ECKT4+T

Towards completeness

Axioms for S_a		
(K)	$S_a(\varphi \to \psi) \to (S_a\varphi \to S_a\psi)$	Secret distribution
(T)	$S_a\varphi \to \varphi$	Secret veridicality
(4)	$S_a\varphi \to S_aS_a\varphi$	Secret introspection
(C)	$(S_a\varphi \wedge S_a\psi) \to S_a(\varphi \wedge \psi)$	Secret combination
(D)	$S_a\varphi \to \neg S_a\neg\varphi$	Secrets partiallity
($\top$)	$\neg S_a\top$	No tautological secrets
($\bot$)	$\neg S_a\bot$	No contradictory secrets
Rules for S_a		
(RE)	From $\varphi \leftrightarrow \psi$ infer $S_a\varphi \leftrightarrow S_a\psi$	Replacement of equivalents
(Nnec)	From φ infer $\neg S_a\varphi$	Negative necessitation
(Dnec)	From φ infer $\neg S_a\neg\varphi$	Diamond necessitation

Conjecture: The language with a single S_a modality is completely axiomatised by ECKT4+$\top$

Related work

- Gossip protocols (Attamah et al., 2014; Apt et al., 2016; Attamah et al., 2017; Apt et al., 2018)

- Modal logics of access control (Abadi et al., 1993; Abadi, 2003; Garg and Abadi, 2008; Aceto et al., 2010; Fong, 2011)

- Secrets most often taken as a primary notion rather than derived from more primitive models of knowledge

  - E.g., Attamah et al. 2014/2017:

$$a \text{ knows the secret of } b\text{:} \quad K_a B \vee K_a \neg B$$

Common knowledge, belief, and dynamics of lying (suggestion from reviewer)

$$C_{\{a,b\}}(K_a\varphi \wedge \neg K_b\varphi)$$

Common knowledge, belief, and dynamics of lying (suggestion from reviewer)

$$C_{\{a,b\}}(K_a\varphi \wedge \neg K_b\varphi)$$

$$C_{\{a,b\}}(B_a\neg\varphi \wedge \neg B_b\neg\varphi)$$

precond. for "a is lying to b"
(van Ditmarsch, 2013)

Common knowledge, belief, and dynamics of lying (suggestion from reviewer)

$\not\models S_a\varphi \to C_{\{a,b\}}(K_a\varphi \wedge \neg K_b\varphi)$

$C_{\{a,b\}}(B_a\neg\varphi \wedge \neg B_b\neg\varphi)$

precond. for "a is lying to b"
(van Ditmarsch, 2013)

Road ahead

- Generalisation: "…*known by a few people…*"
  - Group knowledge
- Secrets vs. mysteries
- We abstracted away all non-epistemic properties of secrets, such as *intention*
  - *"…intended to be kept hidden…"*