Dynamic Epistemic Logic, Protocols, and Security

Hans van Ditmarsch
Logic, University of Sevilla, Spain, hvd@us.es

personal.us.es/hvd/

- dynamic epistemic logic: public announcement logic
- protocols: from dynamic to temporal epistemic logic
- security: protocols for card deals
- future directions: security, protocol synthesis

Sevilla

Multi-agent Epistemic Logic – Syntax & Semantics

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

Structures

A *Kripke model* is a structure $M = \langle S, R, V \rangle$, where

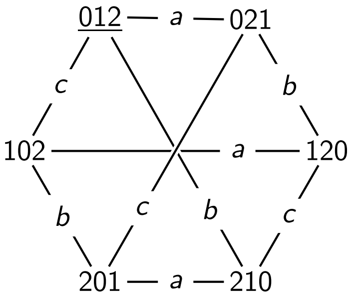
- *domain* S is a nonempty set of states;
- R yields an *accessibility relation* $R_a \subseteq S \times S$ for every $a \in A$;
- V is a *valuation* (function) $V : P \to \mathcal{P}(S)$.

If all R_a are equivalence relations $\sim_a$, M is an *epistemic model*.
A pointed epistemic model is an *epistemic state* (M, s).

Semantics

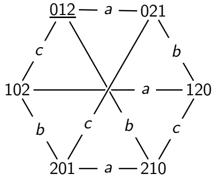
$$
\begin{array}{lll}
M, s \models p & \text{iff} & s \in V(p) \\
M, s \models (\varphi \wedge \psi) & \text{iff} & M, s \models \varphi \text{ and } M, s \models \psi \\
M, s \models \neg\varphi & \text{iff} & \text{not } (M, s \models \varphi) \\
M, s \models K_a\varphi & \text{iff} & \text{for all } t \text{ such that } s \sim_a t \text{ it holds that } M, t \models \varphi
\end{array}
$$

Three agents: Anne, Bill, Cath draw 0, 1, and 2



- Anne knows that Bill knows that Cath knows her own card: $K_a K_b(K_c 0_c \vee K_c 1_c \vee K_c 2_c)$
- Anne has card 0, but she considers it possible that Bill considers it possible that Cath knows that Anne does not have card 0: $0_a \wedge \hat{K}_a \hat{K}_b K_c \neg 0_a$

Example



$$Hexa, 012 \models \hat{K}_a \hat{K}_b K_c \neg 0_a$$
$$\Leftarrow$$
$$012 \sim_a 021 \text{ and } Hexa, 021 \models \hat{K}_b K_c \neg 0_a$$
$$\Leftarrow$$
$$021 \sim_b 120 \text{ and } Hexa, 120 \models K_c \neg 0_a$$
$$\Leftrightarrow$$
$$\sim_c(120) = \{120, 210\},\ Hexa, 120 \models \neg 0_a \text{ and } Hexa, 210 \models \neg 0_a$$
$$\Leftarrow$$
$$Hexa, 120 \not\models 0_a \text{ and } Hexa, 210 \not\models 0_a$$
$$\Leftrightarrow$$
$$120, 210 \notin V(0_a) = \{012, 021\}$$

Axiomatization

all instantiations of propositional tautologies
$K_a(\varphi \to \psi) \to (K_a\varphi \to K_a\psi)$
$K_a\varphi \to \varphi$
$K_a\varphi \to K_aK_a\varphi$
$\neg K_a\varphi \to K_a\neg K_a\varphi$
From φ and $\varphi \to \psi$, infer ψ
From φ, infer $K_a\varphi$

Intermezzo — Common knowledge

- language: $\varphi \quad ::= \quad p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid C_B\varphi$
- accessibility: $\sim_B := (\bigcup_{a \in B} \sim_a)^*$
- semantics:
  $M, s \models C_B\varphi$ iff for all $t : s \sim_B t$ implies $M, t \models \varphi$

Common knowledge has the properties of individual knowledge, and the axiomatization can be extended, e.g., with *induction*:

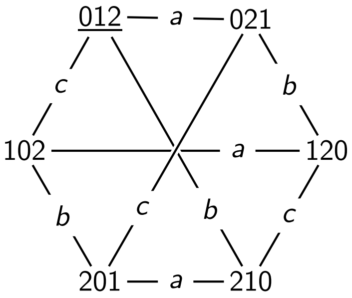
$$C_B(\varphi \rightarrow \bigwedge_{a \in B} K_a\varphi) \rightarrow (\varphi \rightarrow C_B\varphi)$$

Recent technical innovation: *conditional common knowledge* $C_B^{\psi}\varphi$

'along all the B-paths satisfying ψ it holds that φ.'

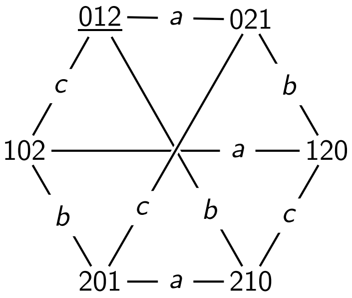
We have that $C_B^{\top}\varphi$ iff $C_B\varphi$.

Public announcements: Example



- After Anne says that she does not have card 1, Cath knows that Bill has card 1.
- After Anne says that she does not have card 1, Cath knows Anne's card.
- Bill still doesn't know Anne's card after that.

Example



- After Anne says that she does not have card 1, Cath knows that Bill has card 1.
  $[\neg 1_a] K_c 1_b$
- After Anne says that she does not have card 1, Cath knows Anne's card.
  $[\neg 1_a](K_c 0_a \vee K_c 1_a \vee K_c 2_a)$
- Bill still doesn't know Anne's card after that:
  $[\neg 1_a]\neg(K_b 0_a \vee K_b 1_a \vee K_b 2_a)$

Public Announcement Logic: language

$$\varphi \quad ::= \quad p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid C_B\varphi \mid [\varphi]\varphi$$

Write $\langle\varphi\rangle\psi$ for $\neg[\varphi]\neg\psi$

For $[\varphi]\psi$ read "after the announcement of φ, ψ (is true)."

For $\langle\varphi\rangle\psi$ read "φ is true and after the announcement of φ, ψ."

Public Announcement Logic: semantics

The effect of the public announcement of φ is the restriction of the epistemic state to all states where φ holds. So, 'announce φ' can be seen as an epistemic state transformer, with a corresponding dynamic modal operator $[\varphi]$.

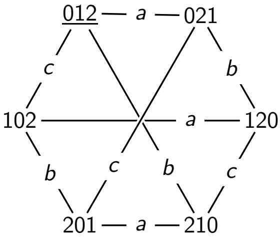
'φ is the announcement'
means
'φ is publicly and truthfully announced'.

$$M, s \models [\varphi]\psi \quad \text{iff} \quad (M, s \models \varphi \text{ implies } M|\varphi, s \models \psi)$$

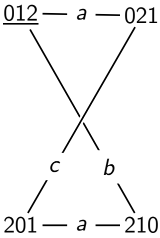
$M|\varphi := \langle S', \sim', V' \rangle$:

$$\begin{array}{lcll} S' & := & [\![\varphi]\!]_M & := \{s \in S \mid M, s \models \varphi\} \\ \sim'_a & := & \sim_a \cap ([\![\varphi]\!]_M \times [\![\varphi]\!]_M) & \\ V'(p) & := & V(p) \cap [\![\varphi]\!]_M & \end{array}$$

Example announcement in Hexa



$\Rightarrow$



$Hexa, 012 \models \langle \neg 1_a \rangle K_c 0_a$

$\Leftrightarrow$

$Hexa, 012 \models \neg 1_a$ and $Hexa|\neg 1_a, 012 \models K_c 0_a$

$\Leftrightarrow$

$Hexa, 012 \models \neg 1_a$ and $(Hexa|\neg 1_a, 012 \models 0_a$ and $\sim_c(012) = \{012\})$

$\Leftarrow$

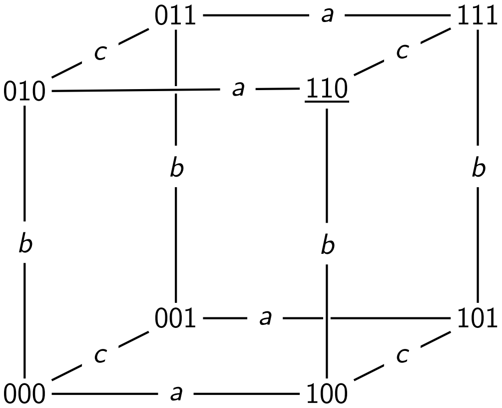
$012 \neq V(1_a)$ and $012 \in V'(0_a)$

A dynamic epistemic logic classic

Muddy Children

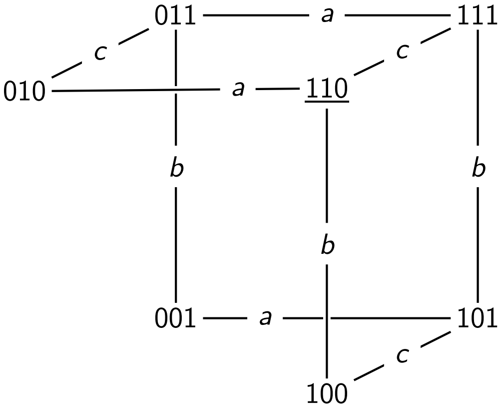
A group of children has been playing outside and are called back into the house by their father. The children gather round him. As one may imagine, some of them have become dirty from the play and in particular: they may have mud on their forehead. Children can only see whether other children are muddy, and not if there is any mud on their own forehead. All this is commonly known, and the children are, obviously, perfect logicians. Father now says: "At least one of you has mud on his or her forehead." And then: "Will those who know whether they are muddy please step forward." If nobody steps forward, father keeps repeating the request. What happens?

Muddy Children



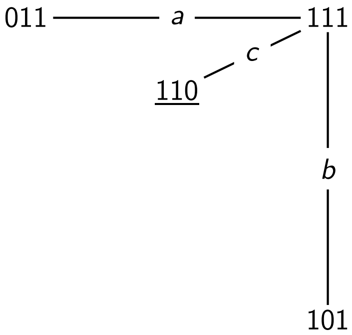
Given: The children can see each other

Muddy Children



After: At least one of you has mud on his or her forehead.

Muddy Children



After: Will those who know whether they are muddy please step forward?

Muddy Children

<u>1</u>10

After: Will those who know whether they are muddy please step forward?

On the origin of Muddy Children

On the origin of Muddy Children

German translation of Rabelais' Gargantua et Pantagruel:
Gottlob Regis, *Meister Franz Rabelais der Arzeney Doctoren Gargantua und Pantagruel, usw.*, Barth, Leipzig, 1832.

Ungelacht pfetz ich dich. Gesellschaftsspiel. Jeder zwickt seinen rechten Nachbar an Kinn oder Nase; wenn er lacht, giebt er ein Pfand. Zwei von der Gesellschaft sind nämlich im Complot und haben einen verkohlten Korkstöpsel, woran sie sich die Finger, und mithin denen, die sie zupfen, die Gesichter schwärzen. Diese werden nun um so lächerlicher, weil jeder glaubt, man lache über den anderen.

I pinch you without laughing. Parlour game. Everybody pinches his right neighbour into chin or nose; if one laughs, one must give a pledge. Two in the round have secretly blackened their fingers on a charred piece of cork, and hence will blacken the faces of their neighbours. These neighbours make a fool of themselves, since they both think that everybody is laughing about the other one.

Axiomatization of public announcement logic

$[\varphi]p \leftrightarrow (\varphi \rightarrow p)$
$[\varphi]\neg\psi \leftrightarrow (\varphi \rightarrow \neg[\varphi]\psi)$
$[\varphi](\psi \wedge \chi) \leftrightarrow ([\varphi]\psi \wedge [\varphi]\chi)$
$[\varphi]K_a\psi \leftrightarrow (\varphi \rightarrow K_a[\varphi]\psi)$
$[\varphi][\psi]\chi \leftrightarrow [\varphi \wedge [\varphi]\psi]\chi$
From φ, infer $[\psi]\varphi$
From $\chi \rightarrow [\varphi]\psi$ and $\chi \wedge \varphi \rightarrow E_B\chi$, infer $\chi \rightarrow [\varphi]C_B\psi$

Expressivity (Plaza, Gerbrandy): *Every formula in the language of public announcement logic without common knowledge is equivalent to a formula in the language of epistemic logic.*

Announcement and relativized common knowledge

$[\varphi]C_B^{\chi}\psi \leftrightarrow C_B^{\varphi \wedge [\varphi]\chi}[\varphi]\psi$

Sequence of announcements

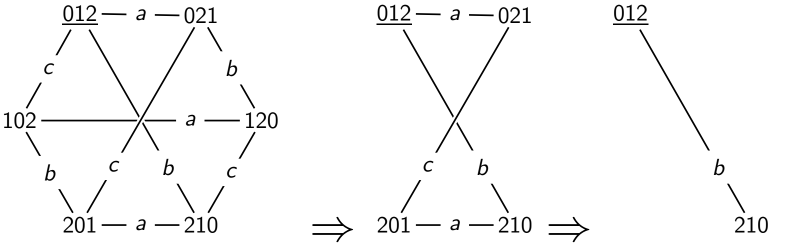
$$[\varphi][\psi]\chi \leftrightarrow [\varphi \wedge [\varphi]\psi]\chi$$

Anne does not have card 1, and Cath now knows Anne's card.
Sequence of two announcements:

$$\neg 1_a \ ; \ (K_c 0_a \vee K_c 1_a \vee K_c 2_a)$$

Single announcement:

$$\neg 1_a \wedge [\neg 1_a](K_c 0_a \vee K_c 1_a \vee K_c 2_a)$$



Unsuccessful updates

Postulate of success:

$$\varphi \rightarrow \langle \varphi \rangle C_A \varphi$$

Announcement of a *fact* always makes it public:

$$\models [p] C_A p$$

Announcements of non-facts do not have to make them public:

$$\not\models [\varphi] C_A \varphi$$

It can be even worse:

$$\models [p \wedge \neg K_a p] \neg (p \wedge \neg K_a p)$$

$$0 \;\text{———}\; a \;\text{———}\; \underline{1} \qquad \xRightarrow[p \wedge \neg K_a p]{} \qquad \underline{1}$$

Unsuccessful updates

Successful formulas: $[\varphi]\varphi$ is valid.
Because $[\varphi]\varphi$ iff $[\varphi]C_A\varphi$ iff $\varphi \rightarrow [\varphi]C_A\varphi$

Which formulas are successful?

- $C_A\varphi$, for any φ in the language (but *only* public knowledge)
- the language fragment of positive formulas
  $\varphi ::= p|\neg p|\varphi \vee \varphi|\varphi \wedge \varphi|K_a\varphi|[\neg\varphi]\varphi$.
- the formula $\neg Kp$, ...
- *single-agent characterization of successful by Holliday & Icard*

Unsuccessful updates

At least I cannot learn from my own announcements...

So ignorance may become knowledge,
but at least knowledge may not become ignorance...

Unsuccessful updates

At least I cannot learn from my own announcements...

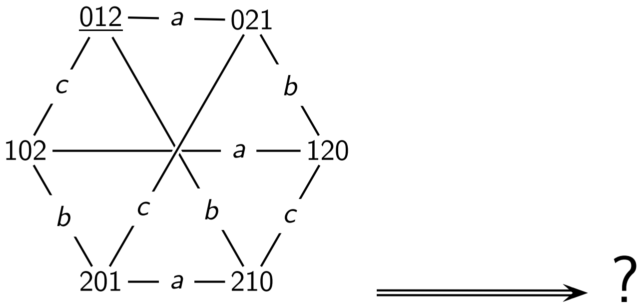
So ignorance may become knowledge,
but at least knowledge may not become ignorance...

Wrong again, same example...
Add an agent i with identity access on the model ('the observer').
After agent i announces $K_i(p \wedge \neg K_a p)$, this formula is false.
Agent i becomes ignorant (about that) from her own announcement.
(E.g.) Agent i becomes knowledgeable about $K_a p$!

$$0 \overset{a}{\text{———}} \underline{1} \quad \xRightarrow[K_i(p \wedge \neg K_a p)]{} \quad \underline{1}$$

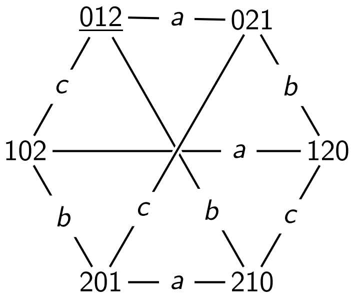
Intermezzo — More complex dynamics (= non-public)

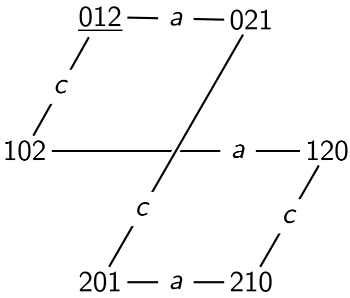
(Anne holds 0, Bill holds 1, and Cath holds 2.) Anne shows (only) Bill her card. (She shows card 0.) Cath cannot see the face of the shown card, but notices that a card is being shown.



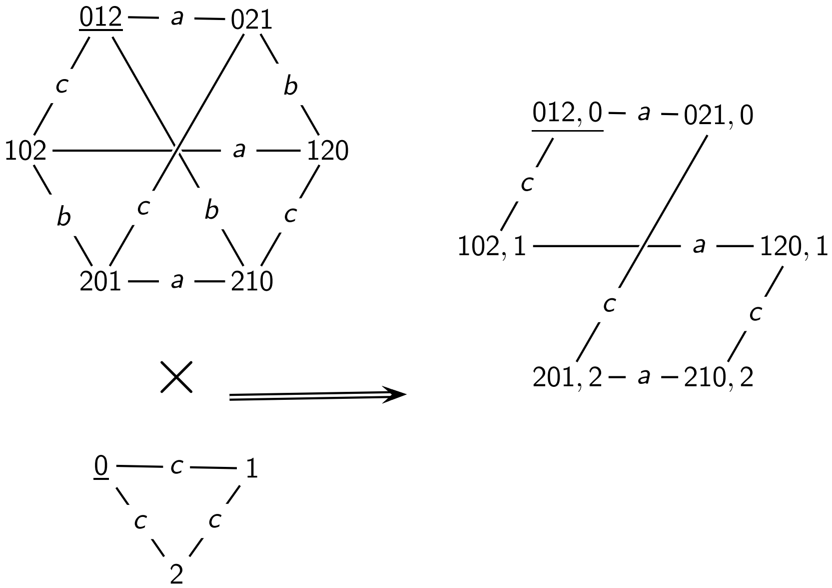
Intermezzo — More complex dynamics (= non-public)

(Anne holds 0, Bill holds 1, and Cath holds 2.) Anne shows (only) Bill her card. (She shows card 0.) Cath cannot see the face of the shown card, but notices that a card is being shown.





Intermezzo — Anne shows card 0 to Bill



Dynamic and temporal epistemic logic

- *Executing an action is like time moving on:*
  Dynamic epistemic logic and temporal epistemic logic are related.
- A player can choose which card to show to another player:
  The relation is with branching time temporal logic.
- Sequences of actions correspond to histories.
  Accessibility satisfies *synchronicity*, *perfect recall*, *no miracles*

Synchronicity:
Indistinguishable sequences of actions are of equal length;
Perfect recall:
If sequences of $n+1$ actions are indistinguishable, then
the sequences of the first n actions are also indistinguishable;
No miracles:
If sequences of n actions are indistinguishable and actions executed there are indistinguishable, then the lengthened sequences of $n+1$ actions are also indistinguishable.

Dynamic and temporal epistemic logic – protocols

You may wish to constrain what actions are possible:

- Even if you have the red card, you may not be allowed to show it;
- Anne sees that Bill is muddy, but she may not announce it. She may only announce if she knows whether she is muddy.

The allowed actions are prescribed in a *protocol*:
a prefix-closed set of sequences of actions.

Axioms are now conditional to executability of actions, e.g.:

$$[\varphi]K\psi \;\leftrightarrow\; (\langle\varphi\rangle\top \rightarrow K[\varphi]\psi)$$

Dynamic and temporal epistemic logic – protocols

You may wish to constrain what actions are possible:

- Even if you have the red card, you may not be allowed to show it;
- Anne sees that Bill is muddy, but she may not announce it. She may only announce if she knows whether she is muddy.

The allowed actions are prescribed in a *protocol*:
a prefix-closed set of sequences of actions.

Axioms are now conditional to executability of actions, e.g.:

$$[\varphi]K\psi \;\leftrightarrow\; (\langle\varphi\rangle\top \rightarrow K[\varphi]\psi)$$

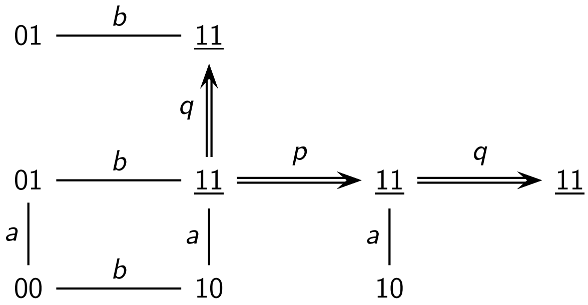
This used to be:

$$[\varphi]K\psi \;\leftrightarrow\; (\varphi \rightarrow K[\varphi]\psi)$$

Dynamic epistemic and temporal epistemic logic – forest

Given an epistemic model, and a protocol, we can grow a *forest*.

Example: agent a knows whether p, agent b knows whether q.
The allowed announcements are: q, p, 'first p then q' (*not* $\top$!).



Dynamic epistemic and temporal epistemic logic – forest

Forest consisting of four trees.
The protocol is $\{\mathsf{s}''', \mathsf{s}', \mathsf{s}'\mathsf{s}''\}$. (I.e.: q, p, $p; q$)

$$
\begin{tikzcd}
(01, \mathsf{s}''') \arrow[r, dash, "b"] & (11, \mathsf{s}''') & & \\
01 \arrow[u, "\mathsf{s}'''"] \arrow[r, dash, "b"] \arrow[d, dash, "a"'] & \underline{11} \arrow[u, "\mathsf{s}'''"] \arrow[r, "\mathsf{s}'"] \arrow[d, dash, "a"'] & (11, \mathsf{s}') \arrow[r, "\mathsf{s}''"] \arrow[d, dash, "a"'] & (11, \mathsf{s}', \mathsf{s}'') \\
00 \arrow[r, dash, "b"] & 10 \arrow[r, "\mathsf{s}'"] & (10, \mathsf{s}') &
\end{tikzcd}
$$

In the most basic approach, expressions like $[p][q]C_{ab}(p \wedge q)$ are translated with *labelled* temporal operators, i.e., as $X_{\mathsf{s}'} X_{\mathsf{s}''} C_{ab}(p \wedge q)$. There are also approaches with full-fledged future and past operators.

Public communication of secrets: Russian Cards

From a pack of seven known cards $0, 1, 2, 3, 4, 5, 6$ Alice (a) and Bob (b) each draw three cards and Eve (c) gets the remaining card. How can Alice and Bob openly (publicly) inform each other about their cards, without Eve learning of any of their cards who holds it?

Public communication of secrets: Russian Cards

From a pack of seven known cards $0, 1, 2, 3, 4, 5, 6$ Alice (a) and Bob (b) each draw three cards and Eve (c) gets the remaining card. How can Alice and Bob openly (publicly) inform each other about their cards, without Eve learning of any of their cards who holds it?

- Presented at Moscow Mathematics Olympiad 2000.
- Thomas Kirkman, *On a problem in combinations*, Cambridge and Dublin Mathematical Journal 2: 191-204, 1847.

Public communication of secrets: Russian Cards

> From a pack of seven known cards $0, 1, 2, 3, 4, 5, 6$ Alice (a) and Bob (b) each draw three cards and Eve (c) gets the remaining card. How can Alice and Bob openly (publicly) inform each other about their cards, without Eve learning of any of their cards who holds it?

Suppose Alice draws $\{0, 1, 2\}$, Bob draws $\{3, 4, 5\}$, and Eve 6.

Public communication of secrets: Russian Cards

> From a pack of seven known cards $0, 1, 2, 3, 4, 5, 6$ Alice (a) and Bob (b) each draw three cards and Eve (c) gets the remaining card. How can Alice and Bob openly (publicly) inform each other about their cards, without Eve learning of any of their cards who holds it?

Suppose Alice draws $\{0, 1, 2\}$, Bob draws $\{3, 4, 5\}$, and Eve 6.

Public communication of secrets: Russian Cards

> From a pack of seven known cards $0, 1, 2, 3, 4, 5, 6$ Alice (a) and Bob (b) each draw three cards and Eve (c) gets the remaining card. How can Alice and Bob openly (publicly) inform each other about their cards, without Eve learning of any of their cards who holds it?

Suppose Alice draws $\{0, 1, 2\}$, Bob draws $\{3, 4, 5\}$, and Eve 6.

Bad:
Alice says "I have 012, or Bob has 012," and
Bob then says "I have 345, or Alice has 345."
Good:
Alice says "I have one of 012, 034, 056, 135, 246," and
Bob then says "Eve has card 6."

Card deals

Structures (interpreted system, Kripke model, state transition s.)

Players only know their own cards.
A hand of cards is a local state.
A deal of cards is a global state.

Logic (public announcement logic)

q_a		agent a holds card q.
ijk_a	$(i_a \wedge j_a \wedge k_a)$	agent a's hand of cards is $\{i, j, k\}$.

Epistemic postconditions

Bob informs Alice	aknowsbs	$\bigwedge(ijk_b \rightarrow K_a ijk_b)$
Alice informs Bob	bknowsas	$\bigwedge(ijk_a \rightarrow K_b ijk_a)$
Eve remains ignorant	cignorant	$\bigwedge(\neg K_c q_a \wedge \neg K_c q_b)$

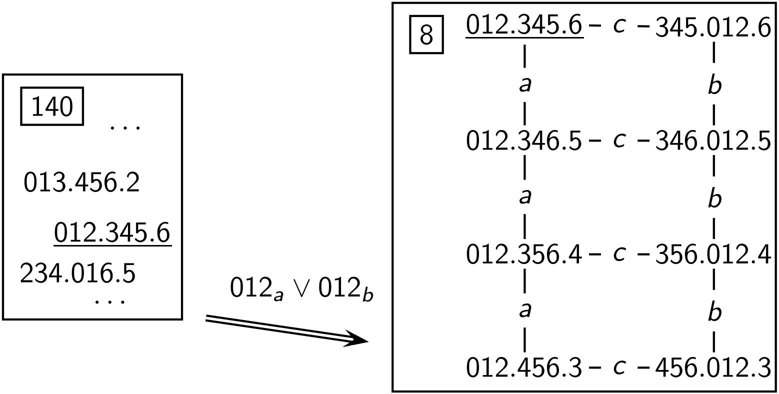
Public communication of secrets: bad

An insider says "Alice has $\{0,1,2\}$ *or Bob has* $\{0,1,2\}$*."*

$$012.345.6 \models [012_a \vee 012_b]\text{cignorant}$$

Alice says "I have $\{0,1,2\}$ *or Bob has* $\{0,1,2\}$*."*

$$012.345.6 \not\models [K_a(012_a \vee 012_b)]\text{cignorant}$$



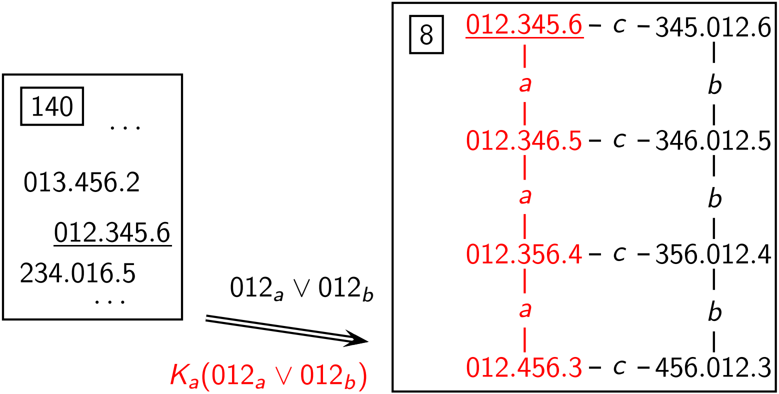
Public communication of secrets: bad

An insider says "Alice has $\{0,1,2\}$ *or Bob has* $\{0,1,2\}$*."*

$$012.345.6 \models [012_a \vee 012_b]\text{cignorant}$$

Alice says "I have $\{0,1,2\}$ *or Bob has* $\{0,1,2\}$*."*

$$012.345.6 \not\models [K_a(012_a \vee 012_b)]\text{cignorant}$$



Public communication of secrets: also bad

Alice says "I don't have card 6."

$$012.345.6 \models [K_a \neg 6_a]\text{cignorant}$$
$$012.345.6 \not\models [K_a \neg 6_a] K_a\text{cignorant}$$

Public communication of secrets: almost good

Alice says "I have $\{0, 1, 2\}$*, or I have none of these cards."*
Eve is ignorant after Alice's announcement.
Alice knows that Eve is ignorant.
Eve doesn't know that Alice knows that Eve is ignorant.
But Eve may assume that Alice knows that Eve is ignorant.
That is informative for Eve!

$$012.345.6 \models [K_a(012_a \vee \neg(0_a \vee 1_a \vee 2_a))]\text{cignorant}$$
$$012.345.6 \models [K_a(012_a \vee \neg(0_a \vee 1_a \vee 2_a))]K_a\text{cignorant}$$
$$012.345.6 \not\models [K_a(012_a \vee \neg(0_a \vee 1_a \vee 2_a))]K_c K_a\text{cignorant}$$
$$012.345.6 \models [K_a(012_a \vee \neg(0_a \vee 1_a \vee 2_a))][K_a\text{cignorant}]\neg\text{cignorant}$$

$$012.345.6 \models [K_a(012_a \vee \neg(0_a \vee 1_a \vee 2_a))][K_a\text{cignorant}]\neg K_a\text{cignorant}$$

Alice reveals her cards, *because* she intends to keep them secret.

Public communication of secrets: almost good

$\boxed{140}$ . . .

013.456.2

$\underline{012.345.6}$

234.016.5

. . .

$\boxed{20}$

$$
\begin{tikzcd}
\underline{012.345.6} \arrow[r, dash, "a"] \arrow[d, dash, "c"] & 012.346.5 \arrow[r, dash, "a"] \arrow[d, dash, "c"] & 012.356.4 \arrow[r, dash, "a"] \arrow[d, dash, "c"] & 012.456.3 \arrow[d, dash, "c"] \\
345.012.6 \arrow[r, dash, "b"] \arrow[d, dash, "a"] & 346.012.5 \arrow[r, dash, "b"] \arrow[d, dash, "a"] & 356.012.4 \arrow[r, dash, "b"] \arrow[d, dash, "a"] & 456.012.3 \arrow[d, dash, "a"] \\
345.016.2 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 346.015.2 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 356.014.2 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 456.013.2 \arrow[d, dash, "a"] \\
345.026.1 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 346.025.1 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 356.024.1 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 456.023.1 \arrow[d, dash, "a"] \\
345.126.0 \arrow[r, dash, "c"] & 346.125.0 \arrow[r, dash, "c"] & 356.124.0 \arrow[r, dash, "c"] & 456.123.0
\end{tikzcd}
$$

Public communication of secrets: almost good

$\boxed{140}$ . . .

013.456.2

<u>012.345.6</u>

234.016.5

. . .

$\boxed{20}$

$$
\begin{tikzcd}[column sep=small]
\underline{012.345.6} \arrow[r, dash, "a"] \arrow[d, dash, "c"] & 012.346.5 \arrow[r, dash, "a"] \arrow[d, dash, "c"] & 012.356.4 \arrow[r, dash, "a"] \arrow[d, dash, "c"] & 012.456.3 \arrow[d, dash, "c"] \\
345.012.6 \arrow[r, dash, "b"] \arrow[d, dash, "a"] & 346.012.5 \arrow[r, dash, "b"] \arrow[d, dash, "a"] & 356.012.4 \arrow[r, dash, "b"] \arrow[d, dash, "a"] & 456.012.3 \arrow[d, dash, "a"] \\
345.016.2 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 346.015.2 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 356.014.2 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 456.013.2 \arrow[d, dash, "a"] \\
345.026.1 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 346.025.1 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 356.024.1 \arrow[r, dash, "c"] \arrow[d, dash, "a"] & 456.023.1 \arrow[d, dash, "a"] \\
345.126.0 \arrow[r, dash, "c"] & 346.125.0 \arrow[r, dash, "c"] & 356.124.0 \arrow[r, dash, "c"] & 456.123.0
\end{tikzcd}
$$

Public communication of secrets

Safe announcements guarantee public preservation of ignorance.

$[\varphi]$	announcement of φ (by an observer)
$[K_a\varphi]$	announcement of φ (by agent/Alice)
$[K_a\varphi \wedge [K_a\varphi]C_{abc}\text{cignorant}]$	safe announcement of φ
$[K_a\varphi][C_{abc}\text{cignorant}]$	

Good protocols produce finite sequences of safe announcements s.t.

$$C_{abc}(\text{aknowsbs} \wedge \text{bknowsas} \wedge \text{cignorant})$$

Public communication of secrets: good

A: "I have one of 012 034 056 135 246," B: "C has 6."

Initially, there are $\binom{7}{3} \cdot \binom{4}{3} = 140$ card deals.

Public communication of secrets: good

A: "I have one of 012 034 056 135 246," B: "C has 6."

Initially, there are $\binom{7}{3} \cdot \binom{4}{3} = 140$ card deals.

After A's announcement.

012.345.6	012.346.5	012.356.4	012.456.3			
034.125.6	034.126.5			034.156.2	034.256.1	
		056.123.4	056.124.3	056.134.2	056.234.1	
135.024.6		135.026.4		135.046.2		135.246.0
	246.013.5		246.015.3		246.035.1	246.135.0

Public communication of secrets: good

A: "I have one of 012 034 056 135 246," B: "C has 6."

Initially, there are $\binom{7}{3} \cdot \binom{4}{3} = 140$ card deals.

After A's announcement.
After B's announcement.

012.345.6	012.346.5	012.356.4	012.456.3			
034.125.6	034.126.5			034.156.2	034.256.1	
		056.123.4	056.124.3	056.134.2	056.234.1	
135.024.6		135.026.4		135.046.2		135.246.0
	246.013.5		246.015.3		246.035.1	246.135.0

Cryptography with card deals

- Russian cards is case $(3, 3, 1)$ of general case (a, b, c)
- Russian cards is length 2; arbitrary finite length protocols
- Other secrets than individual cards (distributed systems)
- What other information leaks while sharing the secret? (combinatorial designs)
- How does this relate to key encryption and key decryption?

More on protocols, temporal and dynamic logics:

- Epistemic protocol synthesis (cards or otherwise)
- Various relations to temporal epistemic logics and model checking

Infinite card deals and key encryption

From protocols for card deals to protocols with key encryption.

- Suppose we have an infinite set of cards.
- In Russian Cards, actual hand 012 is weakened in the message to 012 034 056 135 146 234 256: a finite disjunction of hands.
- Given infinitely many cards, we can weaken the actual hand in the message to an infinite disjunction. “My hand of cards is 012 or 034 or ...”
- The operation of weakining to an infinite disjunction is like applying a one-way function: encryption.
- A player holding infinitely many cards, can eliminite infinitely many disjuncts from such a message. He has the power of decryption.
- To be continued...

Some references

- van Ditmarsch et al., *Dynamic Epistemic Logic*, Springer
- Fischer & Wright, *Bounds on secret key exchange using a random deal of cards*, Journal of Cryptography
- Stiglic, *Computations with a deck of cards*, TCS
- Albert et al., *Safe communication for card players by combinatorial designs for two-step protocols*, AJC
- Atkinson, van Ditmarsch, Roehling, *Avoiding bias in cards cryptography*, AJC
- van Ditmarsch et al., *Secure communication of local states in multi-agent systems*, LiS, ESSLLI 2010
- van Ditmarsch, *The Russian Cards problem*, Studia Logica
- van Ditmarsch, *The case of the hidden hand*, JANCL

Feria de Sevilla