数理解析研究所講究録
第1655巻 2009年 66-74

様相論理による通信の安全性の記述

産業技術総合研究所　竹内泉 (Takeuti Izumi)
AIST

1　序

通信の安全性とは、必要に応じて、秘匿しなければならないものは秘匿され、開示しなければならないものは開示される、という性質である。

嘗ては、通信の安全性の研究では、ある人に対しては情報を全て開示し、ある人には全て秘匿する、という安全性の研究が盛んであった。このような安全性のためには、暗号函数が研究された。暗号函数は、鍵があれば複合できて、情報が全て開示される、鍵がなければ複合できず、情報は全て秘匿される、という性質を充たすものである。

近年は、通信内容の一部を開示し、一部を秘匿する、とう種類の安全性が議論されている。例えば無記名投票の例では、投票の集計結果は開示されるが、個々の投票の内容は秘匿されなければならない。このような安全性を実現するには、暗号函数の研究だけでは足りず、通信のプロトコルの研究が必要である。

プロトコルの性質を研究するには、その性質を記述することから始めなければならない。性質を記述することの利点は、その性質が議論の対象となることである。具体的には以下の利点がある。まず第一には、求められる性質を記述することにより、プロトコル設計の目標となる。第二には、目標通りにプロトコルが設計されているかどうかを検討することが出来る。この検討作業により、プロトコルが要求されている性質を充たすことが保証される。第三に、プロトコルの性質の限界を示すことが出来る。以上の理由により、プロトコルの安全性を記述することが必要である。

本稿では、様相論理によって通信プロトコルの安全性を記述することを提案する。

2 様相論理

通信の安全性とは、情報を秘匿し、また開示することの性質であった。秘匿、開示とは、通信の参加者がそれを知らない、または知る、ということである。よって安全性の記述には、知識の様相論理を用いるのが妥当である。

本稿では、知識を表す様相を加えた命題論理を用いる。この論理では、通常の命題論理の構文規則に加えて

F が論理式ならば $\mathsf{K}_a F$、$\mathsf{C}_{a_1 \ldots a_n} F$ も論理式である

という構文規則を持つ。この様相の意味はこのようなものである。

$\mathsf{K}_a F$ は「a は F を知っている」を表す

$\mathsf{C}_{a_1 \ldots a_n} F$ は「$a_1 \ldots a_n$ の間で F は共有知識である」を表す

3 開示と秘匿の非対照性

論理によって〈知っている〉ことを示すのは容易である。知らされた内容を表す論理式から、演繹によって当該の論理式を演繹できれば、それを〈知っている〉ことが示される。

一方で、〈知らない〉ことを示すのは容易ではない。P を知らされていなくとも、Q と Q ⊃ P を知らされれば、P を知ってしまうからである。

この議論は文献 [1] に詳しい。

4 三人の会食問題

通信による部分的な情報の秘匿と開示の例として、〈三人の会食〉問題を取り挙げる。

〈三人の会食〉問題とは、このような問題である。(文献 [2])

ある日、三人が会食をした。支払いの段になって、既に支払いが済んでいることが分かった。三人の内の誰かが一人で全部支払ったか、あるいは、三人以外の誰かが支払ったのである。三人はお互いの正確をよく知っているので、このような状況では一部だけ支払うというようなことは三人の内の誰もしないということは相互諒解があった。ここで三人はこう考えた。三人の内の誰かが支払ったのか、他の誰かが支払ったのかは知りたい。しかし、もし三人の内の誰かが支払っていた場合、それが誰かは秘密にしておきたい。

さて、どうやってこの要求を満足させるか。

それには、硬貨を三枚使う。硬貨を三枚投げる。その結果は、三人がそれぞれ異なる二枚の硬貨の裏表を視る。三人を A、B、C と呼ぶ。第一硬貨は A と B だけが視る。第二硬貨は B と C だけが視る。第三硬貨は C と A だけが視る。そして各人は、自分が視た硬貨の内の表だった硬貨の数と、自分が支払ったという命題の真偽値との和を取る。命題の真偽値とは、真ならば 1、偽ならば 0 である。そしてその和の奇偶を他の二人に報告する。

例えば、視た硬貨が両方表であり、自分が支払っていなければ、2+0 なので偶数と報告する。視た硬貨の内片方が表であり、自分が支払ったのであれば、1+1 なので偶数と報告する。

これにより、三人の内の誰かが支払ったのか、他の誰かが支払ったのかは知ることが出来、なおかつ、もし三人の内の誰かが支払っていた場合、それが誰かは秘密にしておくことが出来る。

まず、知るとこが出来る方を説明する。

変数 p_A、p_B、p_C、q_1、q_2、q_3、r_A、r_B、r_C はそれぞれ以下の命題の真偽値を値とする。

p_A …… A が支払った
p_B …… B が支払った
p_C …… C が支払った
q_1 …… 第一硬貨は表
q_2 …… 第二硬貨は表
q_3 …… 第三硬貨は表

r_A …… A の報告は偶数
r_B …… B の報告は偶数
r_C …… C の報告は偶数

すると以下が成り立つ。

$$\begin{array}{rcl} r_A & = & p_A + q_1 + q_3 \pmod 2 \\ r_B & = & p_B + q_1 + q_2 \\ r_C & = & p_C + q_2 + q_3 \\ \hline r_A + r_B + r_C & = & p_A + p_B + p_C + 2q_1 + 2q_2 + 2q_3 \\ & = & p_A + p_B + p_C \end{array}$$

支払ったのは一人いるか、または誰でもないかのいずれかである。よって三人の報告の和の奇偶を視れば、誰かが支払ったか誰も支払っていないかが分かる。

次に逆側、知ることが出来ない方を説明する。

例えば、硬貨が三枚とも表であり、A が支払った場合を考える。

$r_A = p_A + q_1 + q_3 = 1$
$r_B = p_B + q_1 + q_2 = 0$
$r_C = p_C + q_2 + q_3 = 0 \pmod 2$

C が値を知っている変数は p_C、q_2、q_3、r_A、r_B、r_C のみである。$p_A = 0$、$p_B = 1$、$q_1 = 0$ であっても、$r_A = 1$、$r_B = 0$ となる。C は第一硬貨を視ていないので、$p_A = 1$、$p_B = 0$、$q_1 = 1$ なのか、$p_A = 0$、$p_B = 1$、$q_1 = 0$ なのか区別が付かない。よって A が支払ったのか B が支払ったのか知ることが出来ない。

5 様相命題論理による形式化の妥当性

以上の議論を様相命題論理によって形式化する。

〈分かる〉側の議論の形式化は容易である。妥当な公理を用意し、〈分かる〉ことを演繹すればよい。

〈分かならい〉ことを示すには、何らかの工夫が必要である。本稿では、〈分かる〉ことが演繹できないことによって〈分かならい〉ことを示す。健全性と完全性を視たす意味論の許では、演繹できないことは、反例となるモデルがあることと等価である。

以上の目的を果たすたには、健全かつ完全な公理系と意味論であって、妥当なものを定義しなければならない。公理系と意味論が健全性と完全性を充たすことは妥当性の必要条件であるが、十分条件ではない。公理系が強過ぎ、モデルが少な過ぎる場合には、本来は〈知らない〉ものまでも〈知っている〉と判定していまう。逆に、公理系が弱過ぎ、モデルが多過ぎる場合には、本来は〈知っている〉ものを〈知らない〉と判断してしまう。

何が妥当であるか、という問題は形式化される問題ではない。形式化の対象となる議論をよく反映しているか否かによって総合的に判断されるものである。

6 構文

様相命題論理の構文を以下のように定める。

参加者：$a \in A = \{a_1, a_2, ...\}$ ：有限集合

論理式：$F ::= Atom \mid \neg F \mid F \wedge F \mid \mathsf{K}_a F \mid \mathsf{C}_{a_1 ... a_n} F$

略記法：$F \supset G \equiv \neg(F \wedge \neg G)$

$F \vee G \equiv \neg F \supset G$

$F \oplus G \equiv (F \wedge \neg G) \vee (G \wedge \neg F)$

$\mathsf{P}_a F \equiv \neg \mathsf{K}_a \neg F$

$(\mathsf{K}_{a_1 ... a_n}) F \equiv \mathsf{K}_{a_1} F \wedge ... \wedge \mathsf{K}_{a_n} F$

7 意味論

様相命題論理の意味論を以下のように定める。

- $W = \{w_1, w_2, ...\}$ ：可能世界の集合（有限集合）
- $V \subset Atom \times W$ ：各原子命題の各可能世界に於ける成否の関係

  $w \models p \iff p \overset{V}{\sim} w$
- $R(a) \subset W \times W$ ：各参加者 a に対して定められた、可能世界の同値関係

  $R(a)$ の意味は、a から視て区別できない、という意味である。

この W、V、R と、ある $w \in W$ より成る四つ組 (W, V, R, w) をモデルと呼ぶ。モデル (W, V, R, w) と論理式 F の間の関係 $(W, V, R, w) \models F$ を以下のように定義する。$(W, V, R, w) \models F$ は省略して単に $w \models F$ と書く。

$$w \models p \iff p \overset{V}{\sim} w, \qquad (p \in Atom)$$
$$w \models \neg F \iff w \not\models F$$
$$w \models F \wedge G \iff w \models F \,\&\, w \models G$$
$$w \models \mathsf{K}_a F \iff \forall w' \overset{R(a)}{\sim} w.\ w' \models F$$
$$w \models \mathsf{C}_{a_1 \ldots a_n} F \iff$$
$$w \models F \,\&\, w \models \mathsf{K}_{a_1 \ldots a_n} F \,\&\, w \models \mathsf{K}_{a_1 \ldots a_n}{}^2 F$$
$$\&\, w \models \mathsf{K}_{a_1 \ldots a_n}{}^3 F \,\&\, w \models \mathsf{K}_{a_1 \ldots a_n}{}^4 F \,\&\, \cdots$$

$\mathsf{K}_a F$ の意味は、a から視て区別できない可能世界全てに於いて F が成り立つ、といっている。もし a から視て区別できない可能世界の中で、ある世界では F が成り立ち、また別のある世界では $\neg F$ が成り立つような場合には、a は F か否かを知らない、ということになる。

$\mathsf{C}_{a_1 \ldots a_n} F$ であるとは、まず F である。次に $\mathsf{K}_{a_1 \ldots a_n} F$ である。つまり a_1、$\cdots$ a_n の全てが F と知っている。次に $\mathsf{K}_{a_1 \ldots a_n}(\mathsf{K}_{a_1 \ldots a_n} F)$ である。つまりそのことを a_1、$\cdots$ a_n の全てが知っている。更にそのことを a_1、$\cdots$ a_n の全てが知っていて、なおかつそのことを a_1、$\cdots$ a_n の全てが知っていて、と無限に続く、ということである。

8 公理系

公理系は以下の規則より成る。

（分離規則）

$$\frac{F \supset G \qquad F}{G}$$

（必然性規則）

$$\frac{F}{\mathsf{K}_a F}, \quad \frac{F}{\mathsf{C}_{a_1 \ldots a_n} F}$$

（共有知識規則）

$$\frac{\mathsf{C}_{a_1 \ldots a_n} H \supset G \supset F \wedge \mathsf{K}_{a_1 \ldots a_n} G}{\mathsf{C}_{a_1 \ldots a_n} H \supset G \supset \mathsf{C}_{a_1 \ldots a_n} F}$$

（始式）

・トートロジー　・(K) $\mathsf{K}_a(F \supset G) \supset \mathsf{K}_a F \supset \mathsf{K}_a G$

・(T) $\mathsf{K}_a F \supset F$　・(4) $\mathsf{K}_a F \supset \mathsf{K}_a \mathsf{K}_a F$　・(5) $\mathsf{P}_a F \supset \mathsf{K}_a \mathsf{P}_a F$

・(C) $\mathsf{C}_{a_1 \ldots a_n} F \supset F$,　$\mathsf{C}_{a_1 \ldots a_n} F \supset K_{a_i} \mathsf{C}_{a_1 \ldots a_n} F$

この公理系と先の意味論の間には健全性と完全性が成り立つ。（文献[3]）

9　妥当性に関する議論

先に挙げた〈三人の会食〉問題のための形式化としてこの公理系と意味論が妥当であるかどうかは議論が必要である。この公理系はK、T、4、5の公理を持つ、所謂S5の公理系である。嘗てはS4の公理系によって形式化されたこともあった。（文献[4]）しかし、近年は公理5が妥当であるという考えが広まっている。本稿もまた、この形式化が妥当であるとの立場に立つ。

10　分かることの証明

〈分かる〉ことを示すのは容易である。与えられた仮定を論理式で書き下し、推論規則によって〈分かる〉ことを演繹する。

まず与えられた仮定は以下の通りである。

$$\mathsf{C}_{ABC}((p_A \wedge \neg p_B \wedge \neg p_C) \vee (\neg p_A \wedge p_B \wedge \neg p_C) \vee (\neg p_A \wedge \neg p_B \wedge p_C) \vee (\neg p_A \wedge \neg p_B \wedge \neg p_C))$$

…三人の内の誰かが一人で支払ったか、誰も支払っていないかのいずれかである

$$\mathsf{C}_{ABC}(\mathsf{C}_{AB} q_1 \vee \mathsf{C}_{AB} \neg q_1)$$

…第一硬貨の裏表の情報はAとBで共有している

$$\mathsf{C}_{ABC}(\mathsf{C}_{BC} q_2 \vee \mathsf{C}_{BC} \neg q_2)$$

…第二硬貨の裏表の情報はBとCで共有している

$$\mathsf{C}_{ABC}(\mathsf{C}_{CA} q_3 \vee \mathsf{C}_{CA} \neg q_3)$$

…第三硬貨の裏表の情報はCとAで共有している

$\mathsf{C}_{ABC}(p_A \oplus q_1 \oplus q_3) \vee \mathsf{C}_{ABC}\neg(p_A \oplus q_1 \oplus q_3)$ … A の報告
$\mathsf{C}_{ABC}(p_B \oplus q_1 \oplus q_2) \vee \mathsf{C}_{ABC}\neg(p_B \oplus q_1 \oplus q_2)$ … B の報告
$\mathsf{C}_{ABC}(p_B \oplus q_1 \oplus q_2) \vee \mathsf{C}_{ABC}\neg(p_B \oplus q_1 \oplus q_2)$ … C の報告

各論理式はそれぞれ、点線以降の内容が共有知識であることを表している。

この7条の連言を Ass と書く。

この Ass から、先の計算によって

$$\mathsf{C}_{ABC}(p_A \vee p_B \vee p_C) \vee \mathsf{C}_{ABC}\neg(p_A \vee p_B \vee p_C)$$

（誰かが支払ったか、誰も支払っていないか、が共有知識である）
が導出される。2 を法とした計算を命題論理で模倣することは容易である。

11 分からないことの証明

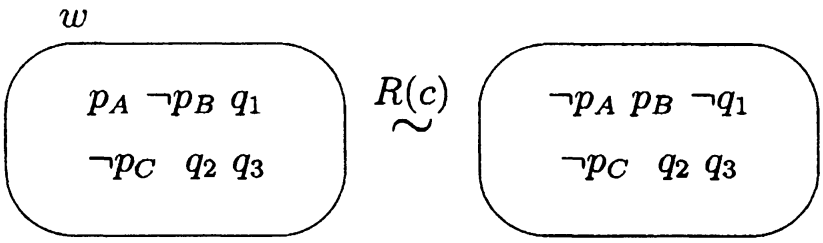
〈分からない〉ことを示すには、〈知っている〉が演繹されないことを言う。そのためには、公理系と意味論の間には完全性が成り立つので、〈知っている〉の反例を構成すればよい。この問題の過程は硬貨を投げる行為を含むので、任意の硬貨の裏表の組み合わせに対して、反例を構成する必要がある。即ち、

$$\forall\xi_1 \in \{q_1, \neg q_1\}.\ \forall\xi_2 \in \{q_2, \neg q_2\}.\ \forall\xi_3 \in \{q_3, \neg q_3\}.\ \exists W.\ \exists w \in W.$$
$$w \models Ass \wedge \xi_1 \wedge \xi_2 \wedge \xi_3 \wedge p_A \wedge \mathsf{P}_C p_B$$

（任意の硬貨の裏表の組合せに対して、支払ったのは A だが、
C は B が支払ったのかも知れないと思っている、
となるようなモデルが存在する）
となる。問題は A、B、C に対して対象なので、これが充たされれば、問題の要請は充たされる。

ξ_i の組み合わせ8通り全て示す必要があるが、構成の仕方は同様なので、一通りの組み合わせだけを示す。

例： $\xi_1 = q_1,\ \xi_2 = q_2,\ \xi_3 = q_3$



このモデルは条件を充たし、〈知っている〉の反例となる。

12 今後の課題

先の問題では、Ass の中では様相記号は正にしか出現していない。このように様相記号は正にしか出現していない論理式には標準的モデルが存在する。この標準的モデルを使うことによって反例の構成が簡明になることが期待される。

本稿では時間を取り扱わなかった。また、参加者は特定されていた。時間の取り扱い、及び不特定多数の参加者を量化する論理の開発は今後の課題である。

文献

[1] 八杉満利子・小田宗兵衛「体系からの脱出：証明論による解析」『科学基礎論研究』第96号（第28巻2号）33–38頁, 2001

[2] David Chaum: 'The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability', J. Cryptology 1(1), pp. 65–75, 1988

[3] J. Y. Halpern et-al: 'Complete Axiomatization for Reasoning About Knowledge and Time', SIAM Journal on Computing 33(2), pp. 674–703, 2004

[4] Sato, Masahiko: 'Kripke-type models for some modal logics', Publications of the research institute for mathematical sciences 13 (2), pp. 381–468, 1977