社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

項正規表現に基づくSpi計算の機密性検証

田代　善彦† 　坂部　俊樹†† 　酒井　正彦†† 　草刈　圭一朗†† 　西田　直樹††

†, †† 名古屋大学大学院情報科学研究科
〒 464–8603 名古屋市千種区不老町
E-mail: †tashiro@sakabe.i.is.nagoya-ac.jp, ††{sakabe,sakai,kusari,nishida}@is.nagoya-u.ac.jp

あらまし　π計算に暗号化機能を加えた並行計算モデルであるspi計算を用いることにより，機密性の定式化とその検証が可能である．これまでに，spi計算に基づいた機密性検証の発見的手法は示されているが，自動検証手法の開発が望まれる．本稿では，spi計算の下で機密性の定式化を行い，プロセスが機密性を守る十分条件を与えるとともに，項正規表現を用いた十分条件の判定手法を提案する．

キーワード　spi計算，機密性検証，項正規表現

Secrecy Verification of Spi Calculus based on Term Regular Expressions

Yoshihiko TASHIRO†, Toshiki SAKABE††, Masahiko SAKAI††,

Keiichirou KUSAKARI††, and Naoki NISHIDA††

†, †† Graduate School of Information Science, Nagoya University
Furou–chou, Chikusa–ku, Nagoya, 464–8603, Japan
E-mail: †tashiro@sakabe.i.is.nagoya-ac.jp, ††{sakabe,sakai,kusari,nishida}@is.nagoya-u.ac.jp

Abstract　By using spi calculus, which is an extension of π calculus with cryptographic primitives, we can formulate and verify secrecy of processes. It is desired to develop automatic methods for verifying secrecy of processes although there were several heuristic methods studied so far. In this paper, for the automation of secrecy verifications in spi calculus, we first formulate secrecy of processes and give a sufficient condition for the secrecy. We then propose a method for deciding the sufficient condition based on term regular expressions.

Key words　spi calculus, secrecy verification, term regular expressions

1. はじめに

近年，ネットワーク通信の発展に伴い，セキュリティの重要性が増してきている．また，ネットワークの大規模化や複雑化により，通信の検証は困難であり，自動化の観点から形式的な手法に基づく検証法の開発が必要である．形式的検証手法の1つとして，spi計算を用いる手法[1]が挙げられる．spi計算はπ計算に暗号化の機能を加えた並行計算モデルであり，暗号化を用いた通信の安全性検証が可能である．spi計算での検証は以下の手順で行われる．

（1） 通信手順をspi計算で記述する．
（2） セキュリティ仕様を記述する．
（3） (1)のモデルが(2)の仕様を満たすか判定する．

(1)のモデル記述は比較的容易に行える．(2)のセキュリティ仕様記述については機密性がすでに提案されている[3]．機密性とは秘密の情報が外部に漏れないことを保証する性質である．(3)については文献[1]で発見的検証手法が示されている．文献[2], [3]では機密性の定義を述べているのみで検証手法は提案されていない．

本稿では，spi計算における機密性検証の自動化を目標として，まず，機密性の定式化を行う．等価なプロセスに対して，機密性が一致するように文献[3]を拡張する．次に，spi計算のプロセスが機密性を守るための十分条件を与え，その正しさを示す．十分条件はプロセスが出力する情報を外部が利用しても秘密情報がわからなければ，機密性は保障されるという考えに基づいて与える．最後に，spi計算の項を正規表現として表した十分条件の判定手法を提案する．

2. 準　　備

本稿で扱うspi計算の構文と意味論[1]について述べる．

まず，spi 計算の構文を与える．

$L, M, N ::=$	term
n	name
x	variable
$\{M\}_n$	encription

名前と変数は十分に存在すると仮定する．$\{M\}_n$ は M を鍵 n で暗号化した暗号文を表す．

$P, Q, R ::=$	process
$\overline{M}\langle N\rangle.P$	output
$M(x).P$	input
$P \mid Q$	composition
$(\nu n)P$	restriciton
$!P$	replication
$[M\ is\ N]P$	match
0	nil
$case\ M\ of\ \{x\}_n\ in\ P$	decryption

各プロセスはそれぞれ次の意味を持つ．

- $\overline{M}\langle N\rangle.P$ はチャネル M 上で N を出力する．
- $M(x).P$ はチャネル M 上で出力された項を入力する．
- $P \mid Q$ は P と Q が並行に実行する．
- $(\nu n)P$ は新しい名前 n を作成し，P 内で束縛する．
- $!P$ は任意個数の P を複製する．
- $[M\ is\ N]P$ は M と N が一致すれば P を実行し，一致しなければ何もしない．
- 0 は何もしない．
- $case\ M\ of\ \{x\}_n\ in\ P$ は M が鍵 n の暗号文であれば，復号化し P を実行する．鍵が一致しなければ，何もしない．

また，$fn(M)$ と $fn(P)$ をそれぞれ項 M とプロセス P の自由な名前の集合とし，以下のように定義する．

$$
\begin{aligned}
fn(n) &= n \\
fn(x) &= \emptyset \\
fn(\{M\}_n) &= \{n\} \cup fn(M) \\
fn(\overline{M}\langle N\rangle.P) &= fn(M) \cup fn(N) \cup fn(P) \\
fn(M(x).P) &= fn(M) \cup fn(P) \\
fn(P \mid Q) &= fn(P) \cup fn(Q) \\
fn((\nu n)P) &= fn(P) - \{n\} \\
fn(!P) &= fn(P) \\
fn([M\ is\ N]P) &= fn(M) \cup fn(N) \cup fn(P) \\
fn(0) &= \emptyset \\
fn(case\ M\ of\ \{x\}_n\ in\ P) &= fn(M) \cup \{n\} \cup fn(P)
\end{aligned}
$$

次に，意味論を与える．最初に，簡約化関係 $>$ を与える．

$$
!P > P \mid !P
$$

$$
[M\ is\ M]P > P
$$

$$
case\ \{M\}_n\ of\ \{x\}_n\ in\ P > P[M/x]
$$

$!P > P \mid !P$ はプロセスの複製を実現する．$[M\ is\ M]P > P$ は M の照合を実現する．$case\ \{M\}_n\ of\ \{x\}_n\ in\ P > P$ は鍵 n の照合，復号化を実現する．

次に，等価関係 $\equiv$ を与える．

$$
\begin{aligned}
P \mid 0 &\equiv P \\
P \mid Q &\equiv Q \mid P \\
P \mid (Q \mid R) &\equiv (P \mid Q) \mid R \\
(\nu m)(\nu n)P &\equiv (\nu n)(\nu m)P \\
(\nu n)0 &\equiv 0 \\
(\nu n)(P \mid Q) &\equiv P \mid (\nu n)Q \quad \text{if } n \notin fn(P)
\end{aligned}
$$

$$
\frac{P > Q}{P \equiv Q} \qquad \frac{}{P \equiv P} \qquad \frac{P \equiv Q}{Q \equiv P}
$$

$$
\frac{P \equiv Q \qquad Q \equiv R}{P \equiv R} \qquad \frac{P \equiv P'}{P \mid Q \equiv P' \mid Q} \qquad \frac{P \equiv P'}{(\nu n)P \equiv (\nu n)P'}
$$

spi 計算での計算の基本となる遷移関係 $\rightarrow$ を与える．

$$
\overline{n}\langle N\rangle.P | n(x).Q \rightarrow P | Q[N/x]
$$

同チャネルで出力と入力を行うプロセスが隣接していれば，出力された項を入力側で受け取り，プロセスを実行する．

隣接していないプロセスの遷移を可能にするために以下の遷移関係を与える．

$$
\frac{P \equiv P' \qquad P' \rightarrow Q' \qquad Q' \equiv Q}{P \rightarrow Q}
$$

残りの遷移関係は以下のように与える．

$$
\frac{P \rightarrow P'}{P \mid Q \rightarrow P' \mid Q} \qquad \frac{P \rightarrow P'}{(\nu n)P \rightarrow (\nu n)P'}
$$

3. 機密性の定式化

spi 計算の機密性を定義する．機密性とは秘密の情報を守ることを意味するセキュリティ仕様の一つである．本稿では，文献 [3] の概念を用いて定義する．文献 [3] の拡張として，等価関係が成立するプロセスにラベル遷移関係を与える $\xrightarrow{\alpha}\equiv$ を新たに加える．また，関係 $\mathcal{R}$ のステップ数を明確にし，$\mathcal{R}^i$ と表記する．機密性の定義に必要な諸定義を与える．

まず，ラベル遷移関係 $\xrightarrow{\alpha}$ を以下のように定義する．

$$
\frac{}{n(x).P \xrightarrow{n} (x)P} \qquad \frac{}{\overline{n}\langle M\rangle.P \xrightarrow{\overline{n}} \langle M\rangle P}
$$

$$
\frac{n(x).P \xrightarrow{n} (x)P \qquad \overline{n}\langle M\rangle.P' \xrightarrow{\overline{n}} \langle M\rangle P'}{n(x).P \mid \overline{n}\langle M\rangle.P' \xrightarrow{\tau} P[M/x] \mid P'}
$$

$$
\frac{\overline{n}\langle M\rangle.P \xrightarrow{\overline{n}} \langle M\rangle P \qquad n(x).P' \xrightarrow{n} (x)P'}{\overline{n}\langle M\rangle.P \mid n(x).P' \xrightarrow{\tau} P \mid P'[M/x]}
$$

$$
\frac{P \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} A \mid Q} \qquad \frac{Q \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} P \mid A}
$$

$$
\frac{P \xrightarrow{\alpha} A \qquad \alpha \notin \{n, \overline{n}\}}{(\nu n)P \xrightarrow{\alpha} (\nu n)A} \qquad \frac{P > Q \qquad Q \xrightarrow{\alpha} A}{P \xrightarrow{\alpha} A}
$$

α と A はそれぞれ $\tau, n, \overline{n}$ と $P, (x)P, \langle M\rangle P$ のいずれかを表す．$P \xrightarrow{\tau} Q$ は P が 1 ステップで Q に遷移することを意味する．$P \xrightarrow{n} (x)Q$ は P がチャネル n で入力可能な状態で，入力後 Q を実行することを意味する．$P \xrightarrow{\overline{n}} \langle M\rangle Q$ は P がチャネル n に出力可能な状態で，出力後 Q を実行することを意味する．

また，$\xrightarrow{\alpha}\equiv$ を以下のようにそれぞれ定義する．

$\xrightarrow{\tau}\equiv$ の定義

- $P \xrightarrow{\tau} R$ かつ $R \equiv Q$ ならば，$P \xrightarrow{\tau}\equiv Q$.
- $P \equiv R$ かつ $R \xrightarrow{\tau} Q$ ならば，$P \xrightarrow{\tau}\equiv Q$.

$\xrightarrow{n}\equiv$ の定義

- $P \xrightarrow{n} (x)R$ かつ $R \equiv Q$ ならば，$P \xrightarrow{n}\equiv (x)Q$.
- $P \equiv R$ かつ $R \xrightarrow{n} (x)Q$ ならば，$P \xrightarrow{n}\equiv (x)Q$.

$\xrightarrow{\overline{n}}\equiv$ の定義

- $P \xrightarrow{\overline{n}} (\nu z_1, \cdots, z_m)\langle M\rangle R$ かつ $R \equiv Q$ ならば，
  $P \xrightarrow{\overline{n}}\equiv (\nu z_1, \cdots, z_m)\langle M\rangle Q$.
- $P \equiv R$ かつ $R \xrightarrow{\overline{n}} (\nu z_1, \cdots, z_m)\langle M\rangle Q$ ならば，
  $P \xrightarrow{\overline{n}}\equiv (\nu z_1, \cdots, z_m)\langle M\rangle Q$.

外部の知識状態を項の集合 O で表し，O の項から計算可能な全ての項の集合 $C(O)$ を定義する．$C(O)$ の計算規則は暗号化と復号化に関するものである．以下のように与える．

（1） $O \subseteq C(O)$

（2） $C(C(O)) = C(O)$

（3） $M \in C(O)$ かつ $n \in C(O)$ ならば，$\{M\}_n \in C(O)$

（4） $\{M\}_n \in C(O)$ かつ $n \in C(O)$ ならば，$M \in C(O)$

(3) が暗号化，(4) が復号化を表す規則である．

関係 $\mathcal{R}^i$ の定義を与える．

（1） $(P, O)\mathcal{R}^0(P, O)$

（2） $(P, O)\mathcal{R}^i(P', O')$ かつ $P' \xrightarrow{\tau}\equiv P''$ ならば，
$(P, O)\mathcal{R}^{i+1}(P'', O')$

（3） $(P, O)\mathcal{R}^i(P', O')$ かつ $P' \xrightarrow{n}\equiv (x)P''$ かつ
$n \in C(O')$ かつ $M \in C(O')$ ならば，
$(P, O)\mathcal{R}^{i+1}(P''[M/x], O')$

（4） $(P, O)\mathcal{R}^i(P', O')$ かつ $P' \xrightarrow{\overline{n}}\equiv (\nu z_1, \cdots, z_m)\langle M\rangle P''$
かつ $n \in C(O')$ かつ $\{z_1, \cdots, z_m\} \cap (O' \cup fn(P)) = \emptyset$
ならば，$(P, O)\mathcal{R}^{i+1}(P'', O' \cup \{M\})$

$(P, O)\mathcal{R}^i(P_i, O_i)$ は外部の知識状態 O で P を i ステップ遷移すると，プロセス，外部の知識状態がそれぞれ P_i, O_i となることを表す．上記の $\mathcal{R}^i$ のそれぞれの意味は以下の通りである．

（1） 0 ステップでは遷移がなく，そのもの自身でのみ関係が成立する．

（2） $\xrightarrow{\tau}$ で遷移すれば，1 ステップ進んだ関係が成立する．外部状態は変化しない．

（3） $\xrightarrow{n}$ で遷移し，外部が n, M を知り得ることができれば，1 ステップ進んだ関係が成立し，P に出現する x に M を代入する．外部状態は変化しない．

（4） $\xrightarrow{\overline{n}}$ で遷移し，外部が n を知り得ることができ，$z_1, \cdots, z_m$ が新しい名前であれば，1 ステップ進んだ関係が成立し，外部が新たに M を知る．

(4) のみ外部の知識が増える．

全ての i の関係を含む $\mathcal{R}^\infty$ を以下のように定義する．

$$\mathcal{R}^\infty = \bigcup_{i \in \{0,1,2,\cdots\}} \mathcal{R}^i$$

これらを用いて，spi 計算の機密性を定義する．

［定義 1］ P, P' をプロセス，O, O' を項の集合，n を名前とする．全ての P', O' に対して，$(P, O)\mathcal{R}^\infty(P', O')$ かつ $n \in fn(P)$ かつ $n \notin C(O)$ ならば $n \notin C(O')$ である場合，P は O から n の機密性を守る．

P に出現する秘密にしたい情報 n が外部 O に知られていない状態で，P を実行しても外部が知ることができなければ，n の機密性は守られているといえる．

［例 1］ $P = \overline{p}\langle\{n\}_k\rangle.0, O = \{p\}, n = n$ のとき，P が O から n の機密性を守るか考える．p, k は名前である．

$n \in fn(P), n \notin C(O)$ であることは明らかである．$\mathcal{R}^\infty$ が成立する場合を考える．

- $i = 0$ のとき，$(P, O)\mathcal{R}^0(P, O)$ 成立．$n \notin C(O)$ は明らか．
- $i = 1$ のとき，$\mathcal{R}^i$ の定義の (4) が成立するときのみ $(P, O)\mathcal{R}^1(P', O')$ が成立する P', O' が存在する．

$\overline{p}\langle\{n\}_k\rangle.0 \xrightarrow{\overline{p}} \langle\{n\}_k\rangle 0, 0 \equiv 0$ より，$\overline{p}\langle\{n\}_k\rangle.0 \xrightarrow{\overline{p}}\equiv \langle\{n\}_k\rangle 0$.
$(P, O)\mathcal{R}^0(P, O), p \in C(O)$ より，$(P, O)\mathcal{R}^1(0, O \cup \{n\}_k)$.
このとき，$n \notin C(O \cup \{n\}_k)$.

- $i \geqq 2$ のとき，$(P, O)\mathcal{R}^i(P', O')$ が成立する P', O' が存在しない．

以上より，P は O から n の機密性を守る． □

［例 2］ $P = \overline{p}\langle\{n\}_k\rangle.0, O = \{p, k\}, n = n$ のとき，P が O から n の機密性を守るか考える．

例 1 と同様に，$(P, O)\mathcal{R}^1(0, O \cup \{n\}_k)$ が成立する．$O = \{p, k\}$ より，$C(O \cup \{n\}_k) = \{p, k, \{n\}_k, n\}$．よって，$n \in C(O \cup \{n\}_k)$．$P$ は O から n の機密性を守らない． □

$\mathcal{R}^i$ に従った機密性検証 [2], [3] は $\mathcal{R}^i$ の成立条件が複数あり，各成立条件の判定に手間がかかる．

4. 項正規表現を用いた機密性検証

spi 計算の項を正規表現とし，機密性検証を行う手法について述べる．

まず，spi 計算の項を正規表現として表す．これを項正規表現と呼ぶ．

$E, F ::=$	term regular expression
n	name
x	variable
$\{E\}_n$	encription
$\square$	box
$E + F$	union

また，$|E|$ を以下のように定義する．

$$
\begin{aligned}
&|n| = \{n\}\\
&|x| = \{x\}\\
&|\{E\}_n| = \{\{e\}_n \mid e \in |E|\}\\
&|\Box| = \text{全ての項の集合}\\
&|E + F| = |E| \cup |F|
\end{aligned}
$$

P が $|E|$ から n の機密性を守る条件について述べる．P の実行後，E が知り得る情報の中に n が含まれていなければ，P は $|E|$ から n の機密性を守るといえる．P の実行後，新たに E が知る情報は E が知っているチャネル上で出力される情報である．その情報を計算する関数を $G(P, E)$ とし，以下のように定義する．

$$
\begin{aligned}
G(0, E) &= E\\
G(\overline{M}\langle N\rangle.P, E) &= \begin{cases} N + G(P, E) & \text{if } M \in C(|E|)\\ G(P, E) & \text{otherwise}\end{cases}\\
G(M(x).P, E) &= \begin{cases} G(P[\Box/x], E) & \text{if } M \in C(|E|)\\ G(P, E) & \text{otherwise}\end{cases}\\
G(P \mid Q, E) &= G(P, G(Q, E)) + G(Q, G(P, E))\\
G((\nu n)P, E) &= G(P, E)\\
G(!P, E) &= G(P, E)\\
G([M\ is\ N]P, E) &= \begin{cases} G(P, E) & \text{if } M = N\\ E & \text{otherwise}\end{cases}\\
G(case\ M\ of\ \{x\}_n\ in\ P, E) &= \begin{cases} G(P[L/x], E) & \text{if } M = \{L\}_n\\ E & \text{otherwise}\end{cases}
\end{aligned}
$$

$C(|G(P, E)|)$ は P の実行後，E が知り得る最大の情報である．$n \notin C(|G(P, E)|)$ が成立すれば，P は $|E|$ から n の機密性を守るといえる．しかし，P に入力プロセスが含まれる場合，$G(M(x).P, E) = G(P[\Box/x], E)$ であり，$\Box$ は任意の項を表すので，計算不可能である．よって，$n \notin C(|G(P, E)|)$ か判定不可能な場合が存在する．

この問題を解決するため，述語 $known(E, F)$ を与える．$known(E, F)$ は $|E|$ が $C(|F|)$ の部分集合であるかを判定する．よって，$C(O)$ の規則を考慮し，定義する．

- $E = n$ の場合
- $F = n'$ の場合，$known(n, n')$ は真 $\Leftrightarrow n = n'$
- $F = x$ の場合，$known(n, x)$ は偽
- $F = \{E'\}_{n'}$ の場合，$known(n, \{E'\}_{n'})$ は偽
- $F = \Box$ の場合，$known(n, \Box)$ は真
- $F = E' + F'$ の場合，
  $known(n, E' + F')$ は真
  $\Leftrightarrow known(n, E')$ は真，又は
  $known(n, F')$ は真，又は
  $known(\{n\}_{n'}, E')$ は真かつ $known(n', F')$ は真，又は
  $known(n', E')$ は真かつ $known(\{n\}_{n'}, F')$ は真

$F = E' + F'$ の場合において，$known(\{n\}_{n'}, E')$ は真かつ $known(n', F')$ は真の場合と $known(n', E')$ は真かつ $known(\{n\}_{n'}, F')$ は真の場合，$known(n, E' + F')$ は真であるのは $C(O)$ の復号化の規則に対応しているためである．

E が n 以外の場合においても，$F = E' + F'$ の場合，同様に $C(O)$ の復号化の規則に対応したものを定義する．

- $E = x$ の場合
- $F = n$ の場合，$known(x, n)$ は偽
- $F = x'$ の場合，$known(x, x')$ は真 $\Leftrightarrow x = x'$
- $F = \{E'\}_n$ の場合，$known(x, \{E'\}_n)$ は偽
- $F = \Box$ の場合，$known(x, \Box)$ は真
- $F = E' + F'$ の場合，
  $known(x, E' + F')$ は真
  $\Leftrightarrow known(x, E')$ は真，又は
  $known(x, F')$ は真，又は
  $known(\{x\}_n, E')$ は真 かつ $known(n, F')$ は真，又は
  $known(n, E')$ は真 かつ $known(\{x\}_n, F')$ は真
- $E = \{E'\}_n$ の場合
- $F = n'$ の場合，$known(\{E'\}_n, n')$ は偽
- $F = x$ の場合，$known(\{E'\}_n, x)$ は偽
- $F = \{E''\}_{n'}$ の場合，
  $known(\{E'\}_n, \{E''\}_{n'})$ は真
  $\Leftrightarrow known(E', E'')$ は真 かつ $known(n, n')$ は真
- $F = \Box$ の場合，$known(\{E'\}_n, \Box)$ は真
- $F = E'' + F''$ の場合，
  $known(\{E'\}_n, E'' + F'')$ は真
  $\Leftrightarrow known(\{E'\}_n, E'')$ は真，又は
  $known(\{E'\}_n, F'')$ は真，又は
  $known(\{\{E'\}_n\}_{n'}, E'')$ は真 かつ $known(n', F'')$ は真
  又は
  $known(n', E'')$ は真 かつ $known(\{\{E'\}_n\}_{n'}, F'')$ は真
  又は
  $known(n, E'')$ は真かつ $known(E', E'')$ は真，又は
  $known(E', E'')$ は真かつ $known(n, E'')$ は真

$C(O)$ の暗号化の規則に対応して，$E = \{E'\}_n, F = E'' + F''$ の場合において，$known(n, E'')$ は真かつ $known(E', E'')$ は真の場合と $known(E', E'')$ は真かつ $known(n, E'')$ は真の場合，$known(\{E'\}_n, E'' + F'')$ は真とする．

- $E = \Box$ の場合
- $F = n$ の場合，$known(\Box, n)$ は偽
- $F = x$ の場合，$known(\Box, x)$ は偽
- $F = \{E'\}_n$ の場合，$known(\Box, \{E'\}_n)$ は偽
- $F = \Box$ の場合，$known(\Box, \Box)$ は真
- $F = E' + F'$ の場合，
  $known(\Box, E' + F')$ は真
  $\Leftrightarrow known(\Box, E')$ は真，又は
  $known(\Box, F')$ は真，又は
  $known(\{\Box\}_n, E')$ は真 かつ $known(n, F')$ は真，又は
  $known(n, E')$ は真 かつ $known(\{\Box\}_n, F')$ は真

- $E = E' + F'$ の場合

– $F = n$ の場合，
$known(E' + F', n)$ は真
$\Leftrightarrow known(E', n)$ は真かつ $known(F', n)$ は真

– $F = x$ の場合，
$known(E' + F', x)$ は真
$\Leftrightarrow known(E', x)$ は真かつ $known(F', x)$ は真

– $F = \{E''\}_n$ の場合，
$known(E' + F', \{E''\}_n)$ は真
$\Leftrightarrow known(E', \{E''\}_n)$ は真 かつ $known(F', \{E''\}_n)$ は真

– $F = \Box$ の場合，$known(E' + F', \Box)$ は真

– $F = E'' + F''$ の場合，
$known(E' + F', E'' + F'')$ は真
$\Leftrightarrow known(E' + F', E'')$ は真，又は
$known(E' + F', F'')$ は真，又は
$known(\{E' + F'\}_n, E'')$ は真 かつ $known(n, F'')$ は真
又は
$known(n, E'')$ は真 かつ $known(\{E' + F'\}_n, F'')$ は真

$known(E, F)$ の真偽は判定可能であり，以下の定理が成立する．

［定理 1］ $known(E, F)$ が真かつ，そのときに限り $|E| \subseteqq C(|F|)$.

[証明] ($\Rightarrow$) E の構造に関する帰納法を用いる．

- $E = n$ の場合，F の構造に関する帰納法を用いる．

– $F = n'$ の場合，$known(n, n')$ が真であるのは $n = n'$ のときだけである．このとき，$|n| \subseteqq C(|n|)$ より，$|n| \subseteqq C(|n'|)$.

– $F = x$ の場合，$known(n, x)$ は偽.

– $F = \{E'\}_{n'}$ の場合，$known(n, \{E'\}_{n'})$ は偽.

– $F = \Box$ の場合，$known(n, \Box)$ は真．$|\Box|$ は全ての項の集合なので，$|n| \subseteqq C(|\Box|)$.

– $F = E' + F'$ の場合，
$known(n, E' + F')$ が真となるのは 4 通りある．

＊ $known(n, E')$ が真の場合，I.H. より成立.

＊ $known(n, F')$ が真の場合，I.H. より成立.

＊ $known(\{n\}_{n'}, E')$ が真かつ $known(n', F')$ が真の場合，I.H. より，$|\{n\}_{n'}| \subseteqq C(|E'|)$ かつ $|n'| \subseteqq C(|F'|)$.
よって，$|\{n\}_{n'}| \subseteqq C(|E' + F'|)$ かつ $|n'| \subseteqq C(|E' + F'|)$.
ゆえに，$\{n\}_{n'} \in C(|E' + F'|)$ かつ $n' \in C(|E' + F'|)$.
$C(O)$ の定義より，$n \in C(|E' + F'|)$．よって，$|n| \subseteqq C(|E' + F'|)$.

＊ $known(n', E')$ が真かつ $known(\{n\}_{n'}, F')$ が真の場合，$known(\{n\}'_n, E')$ が真かつ $known(n', F')$ が真の場合と同様に証明できる．

- $E = x, \{E'\}_n, \Box, E' + F'$ の場合も同様に F の構造に関する帰納法を用いて証明できる．

($\Leftarrow$) $\Rightarrow$ と同様に E, F の構造に関する帰納法を用いて証明できる． □

定理 1 より系 1 が得られる．

［系 1］ $known(n, E)$ が偽かつ，そのときに限り $n \notin C(|E|)$. □

このことより，$n \notin C(|G(P, E)|)$ も判定可能となる．

以降では，本稿の主定理である項正規表現に基づく十分条件による機密性検証に関する定理 (定理 2) を示す．その証明に必要な補題 1，2，3 を示し主定理を与える．

［補題 1］ $\mathcal{R}^{i+1} = \mathcal{R}^i \cdot \mathcal{R}^1$

[証明] ($\subseteqq$ の証明)
$(P, O)\mathcal{R}^{i+1}(P'', O'')$ が成立するのは次のいずれかの場合である．

（1） ある P' が存在して，$(P, O)\mathcal{R}^i(P', O'')$ かつ $P' \xrightarrow{\tau} \equiv P''$

（2） ある P', Q, n, M が存在して，$(P, O)\mathcal{R}^i(P', O'')$ かつ $P' \xrightarrow{n} \equiv (x)Q$ かつ $n \in C(O'')$ かつ $M \in C(O'')$ かつ $P'' = Q[M/x]$

（3） ある $P', O', n, \{z_1 \cdots z_m\}$ が存在して，
$(P, O)\mathcal{R}^i(P', O')$ かつ $P' \xrightarrow{\overline{n}} \equiv (\nu z_1 \cdots z_m)\langle M\rangle P''$ かつ $n \in C(O')$ かつ $\{z_1 \cdots z_m\} \cap (O' \cup fn(P)) = \emptyset$ かつ $O'' = O' \cup \{M\}$

また，$(P', O')\mathcal{R}^1(P'', O'')$ が成立するのは次のいずれかの場合である．

（1） $P' \xrightarrow{\tau} \equiv P''$ かつ $O'' = O'$

（2） ある Q, n, M が存在して，$P' \xrightarrow{n} \equiv (x)Q$ かつ $n \in C(O')$ かつ $M \in C(O')$ かつ $P'' = Q[M/x]$ かつ $O'' = O'$

（3） ある $n, \{z_1 \cdots z_m\}$ が存在して，
$P' \xrightarrow{\overline{n}} \equiv (\nu z_1 \cdots z_m)\langle M\rangle P''$ かつ $n \in C(O')$ かつ $\{z_1 \cdots z_m\} \cap (O' \cup fn(P')) = \emptyset$ かつ $O'' = O' \cup \{M\}$

$(P, O)\mathcal{R}^{i+1}(P'', O'')$ が成立すると仮定し，成立条件により場合分けして，$(P, O)\mathcal{R}^i(P', O')$ かつ $(P', O')\mathcal{R}^1(P'', O'')$ が成立することを示す．

（1） ある P' が存在して，$(P, O)\mathcal{R}^i(P', O'')$ かつ $P' \xrightarrow{\tau} \equiv P''$ が成立する場合，$P' \xrightarrow{\tau} \equiv P''$ より $(P', O'')\mathcal{R}^1(P'', O'')$ が成立する．

（2） ある P', Q, n, M が存在して，$(P, O)\mathcal{R}^i(P', O'')$ かつ $P' \xrightarrow{n} \equiv (x)Q$ かつ $n \in C(O'')$ かつ $M \in C(O'')$ かつ $P'' = Q[M/x]$ が成立する場合，$P' \xrightarrow{n} \equiv (x)Q$ かつ $n \in C(O'')$ かつ $M \in C(O'')$ かつ $P'' = Q[M/x]$ より，$(P', O'')\mathcal{R}^1(P'', O'')$ が成立する．

（3） ある $P', O', n, \{z_1 \cdots z_m\}$ が存在して，
$(P, O)\mathcal{R}^i(P', O')$ かつ $P' \xrightarrow{\overline{n}} \equiv (\nu z_1 \cdots z_m)\langle M\rangle P''$ かつ $n \in C(O')$ かつ $\{z_1 \cdots z_m\} \cap (O' \cup fn(P)) = \emptyset$ かつ $O'' = O' \cup \{M\}$ が成立する場合，$P' \xrightarrow{\overline{n}} \equiv (\nu z_1 \cdots z_m)\langle M\rangle P''$ かつ $n \in C(O')$ かつ $\{z_1 \cdots z_m\} \cap (O' \cup fn(P')) = \emptyset$ かつ $O'' = O' \cup \{M\}$ より，$(P', O')\mathcal{R}^1(P'', O'')$ が成立する．

($\supseteqq$ の証明)
$\mathcal{R}^{i+1}$ と $\mathcal{R}^1$ の成立条件より，明らかに成立する． □

［補題 2］ $\mathcal{R}^{i+1} = \mathcal{R}^1 \cdot \mathcal{R}^i$

[証明] i に関する帰納法を用いる．

- $i = 0$ の場合，$\mathcal{R}^1 = \mathcal{R}^1 \cdot \mathcal{R}^0$ は明らかに成立する．
- $i \geqq 1$ の場合，以下が成立する．

$$\begin{aligned}\mathcal{R}^{i+1} &= \mathcal{R}^i \cdot \mathcal{R}^1 \ (\because \text{補題 1}) \\ &= \mathcal{R}^1 \cdot \mathcal{R}^{i-1} \cdot \mathcal{R}^1 \ (\because \text{I.H.}) \\ &= \mathcal{R}^1 \cdot \mathcal{R}^i \ (\because \text{補題 1})\end{aligned}$$

□

［補題 3］ 全ての P, E において，$|E| \subseteqq |G(P,E)|$ である．

[証明] $G(0,E) = E$ より，明らかに成立する． □

［定理 2］ 全ての P, E, n において，$known(n, G(P,E))$ が偽ならば，P が $|E|$ から n の機密性を守る．

[証明] 全ての P', E' に対して，$(P,|E|)\mathcal{R}^i(P',|E'|)$ かつ $n \in fn(P)$ かつ $n \notin C(|E|)$ ならば $n \notin C(|E'|)$ であることを $\pi^i(P,|E|,n)$ とおくと，証明すべきことは以下のことである．

$\forall n.\forall i.\forall P.\forall E.(known(n, G(P,E))$ は偽 $\rightarrow \pi^i(P,|E|,n))$

n を任意の name とし，i に関する帰納法を用いて全ての i に対して，以下を示す．

$\forall P.\forall E.(known(n, G(P,E))$ は偽 $\rightarrow \pi^i(P,|E|,n))$

- $i = 0$ のとき，$(P,|E|)\mathcal{R}^0(P,|E|)$.

$known(n, G(P,E))$ は偽 と系 1 より，$n \notin C(|G(P,E)|)$.
補題 3 より，$n \notin C(|E|)$．よって，$\pi^0(P,|E|,n)$.

- $i \geqq 1$ のとき，P の構造に関する帰納法を用いる．
  - $P = 0$ の場合，$n \notin fn(0)$ より，$\pi^i(0,|E|,n)$.
  - $P = \overline{M}\langle N\rangle.P'$ の場合

$known(n, G(\overline{M}\langle N\rangle.P', |E|))$ は偽 とする．
さらに，$(\overline{M}\langle N\rangle.P', |E|)\mathcal{R}^i(P_i, |E_i|)$ かつ $n \in fn(\overline{M}\langle N\rangle.P')$ かつ $n \notin C(|E|)$ であると仮定したとき，$n \notin C(|E_i|)$ であることを示す．
補題 2 より，$\mathcal{R}^i = \mathcal{R}^1 \cdot \mathcal{R}^{i-1}$.
$(\overline{M}\langle N\rangle.P', |E|)\mathcal{R}^i(P_i, |E_i|)$ を $(\overline{M}\langle N\rangle.P', |E|)\mathcal{R}^1(P_1, |E_1|)$ かつ $(P_1, |E_1|)\mathcal{R}^{i-1}(P_i, |E_i|)$ とする，このとき，$\mathcal{R}^1$ が成立するのは $\mathcal{R}^i$ の定義の (4) のときだけである．

- $\overline{M}\langle N\rangle.P' \overset{\overline{M}}{\rightarrow} \equiv \langle N\rangle P'$ かつ $M \in C(|E|)$ のとき

$(\overline{M}\langle N\rangle.P', |E|)\mathcal{R}^1(P', |E| \cup \{N\})$.
$G(\overline{M}\langle N\rangle.P', |E|) = N + G(P', |E|)$.
$known(n, G(\overline{M}\langle N\rangle.P', |E|))$ は偽 より，
$known(n, N + G(P', |E|))$ は偽.
補題 3 より，$known(n, N + |E|)$ は偽.
系 1 より，$n \notin C(|N + |E||) = C(|E_1|)$.
$known(n, G(\overline{M}\langle N\rangle.P', |E|))$ は偽 より，
$known(n, G(P', |E_1|))$ は偽.
よって，$(P', |E_1|)\mathcal{R}^{i-1}(P_i, |E_i|)$ と I.H. より，$n \notin C(|E_i|)$.

- P がその他の場合，P の $\overset{\overline{n}}{\rightarrow}$ で $\mathcal{R}^i$ の定義の (4) の関係がつかず成立． □

定理 2 の適用例を挙げる．

［例 3］ 定理 2 を用いて，例 1（$P = \overline{p}\langle\{n\}_k\rangle.0, E = p, n = n$）について考える．
$G(\overline{p}\langle\{n\}_k\rangle.0, p) = \{n\}_k + G(0,p) = \{n\}_k + p$. $known$ の定義に従うと，$known(n, G(\overline{p}\langle\{n\}_k\rangle.0, p))$ は偽．定理 2 より，P は $|E|$ から n の機密性を守る． □

［例 4］ 定理 2 を用いて，例 2（$P = \overline{p}\langle\{n\}_k\rangle.0, E = p+k, n = n$）について考える．
$G(\overline{p}\langle\{n\}_k\rangle.0, p + k) = \{n\}_k + G(0, p + k) = \{n\}_k + p + k$. $known(\{n\}_k, G(\overline{p}\langle\{n\}_k\rangle.0, p + k))$ が真かつ $known(k, G(\overline{p}\langle\{n\}_k\rangle.0, p + k))$ が真より，
$known(n, G(\overline{p}\langle\{n\}_k\rangle.0, p + k))$ は真.
定理 2 より，P は $|E|$ から n の機密性を守るとはいえない．
□

例 3 のような定理 2 の十分条件を満たす場合，例 1 と比較して簡単に検証が可能である．

一方，例 4 のような十分条件を満たさない場合，機密性の判定ができない．

5. おわりに

本稿では，spi 計算の下でプロセスの機密性を定式化し，その検証手法について検討した．具体的には，機密性を保証する十分条件を与え，項の正規表現に基づく判定手法を提案した．

本稿で提案した十分条件の計算はプロセスが出力した外部が知り得る全ての情報を網羅している．秘密情報に関わる情報のみ取得する計算手法を考案できれば，条件を緩和させることが可能である．また，機密性の決定可能性や本稿の機密性の定式化と文献 [3] の定式化との関係について議論する必要がある．

謝辞 本研究は一部，科研費#15500007，#16650005，#17700009 ならびに名古屋大学 21 世紀 COE プログラム（社会情報基盤のための音声・映像の知的統合）の補助を受けている．

文　献

[1] M. Abadi and A.D. Gordon : A calculus for cryptographic protocols: The spi calculus, Information and Computation, 148(1), pp.1–70, 1999.
[2] M. Abadi : Security protocols and specifications, In Foundations of Software Science and Computation Structures: Second International Conf., FOSSACS '99, pp.1–13, 1999.
[3] M. Abadi : Security protocols and their properties, Foundations of Secure Computation, NATO Science Series, IOS Press, pp.39–60, 2000.
[4] M. Abadi and B. Blanchet : Secrecy types for asymmetric communication, Theoretical Computer Science 298(3), pp.387–415, 2003.
[5] M. Abadi : Secrecy by typing in security protocols, Journal of the ACM, 46(5), pp.749–786, 1999.