セキュリティプロトコルの略式記法からspi計算への変換

住井 英二郎 （ペンシルバニア大学）
立沢 秀晃　米澤 明憲 （東京大学）

背景1: セキュリティプロトコルの略式記法

- 例: ISO対称鍵2パス一方向認証プロトコル [ISO/IEC 1993]

$$
\begin{array}{lcll}
1. & B & \rightarrow & A : N_B \\
2. & A & \rightarrow & B : \{N_B, B\}_{K_{AB}}
\end{array}
$$

1. BはAにN_Bを送信する。
2. AはN_BとBのペアをK_{AB}で暗号化し、Bに送信する。

問題: 正確な解釈が自明でない

- 例:ISO対称鍵2パス一方向認証プロトコル [ISO/IEC 1993]

$$
\begin{array}{lllll}
1. & B & \rightarrow & A & : \quad N_B \\
2. & A & \rightarrow & B & : \quad \{N_B, B\}_{K_{AB}}
\end{array}
$$

1. 参加者BはノンスN_Bを新規に生成し、参加者Aに送信する。
2. AはそのノンスN_Bと参加者Bの名前とのペアを共有鍵K_{AB}で暗号化し、Bに送信する。
   Bはそれを復号化し、受信したノンスがN_Bであること、受信した名前がBであることを確認する。

背景2: spi計算[Abadi/Gordon 97]

π計算[Milner他 92] + 完全な暗号

メッセージ M, N ::=

変数	v
暗号文	$\{M_1, ..., M_n\}_N$

プロセス P, Q ::=

送信	$\bar{v}\langle M_1, ..., M_n\rangle.P$
受信	$v(v_1, ..., v_n).P$
並列実行	$P \mid Q$
比較	**if M = N then P**
復号化	**case M of** $\{v_1, ..., v_n\}_N$ **in P**
鍵生成	$\nu v.\ P$

問題: 面倒くさい

- 先のプロトコルをspi計算で表すと...

$$
\begin{array}{ll}
 & \mathtt{chan}_A(x).\,\overline{\mathtt{chan}_B}\langle\{x, B\}_{K_{AB}}\rangle.\,\mathtt{After}_A \\
\mid & \nu N_B.\,\overline{\mathtt{chan}_A}\langle N_B\rangle. \\
 & \mathtt{chan}_B(y).\,\mathtt{case}\ y\ \mathtt{of}\ \{z_1, z_2\}_{K_{AB}}\ \mathtt{in} \\
 & \mathtt{if}\ z_1 = N_B\ \mathtt{then}\ \mathtt{if}\ z_2 = B\ \mathtt{then}\ \mathtt{After}_B
\end{array}
$$

今回の研究

- 略式記法からspi計算への変換を定義
  - プロトコルの各時点における参加者の「知識」によって動作を決める
  - 初期知識は人間が与える

⇓

略式記法の簡単さを享受しつつ、
spi計算の様々な研究が利用可能に

発表の構成

- 序論
- 変換の基本方針
- 例題
  - 単純なプロトコル
  - 公開鍵暗号を使用するプロトコル
  - 算術演算を使用するプロトコル
  - 暗号文を転送するプロトコル
- 鍵データベースによる拡張
- 結論: 関連研究と今後の課題

基本方針

1. 知識にない値を送信する（ことになっている）ときは、新規に生成し、知識に追加する
2. 知識にない値を受信したときは、知識に追加する
3. 知識にある値を受信したときは、知識にある値と受信した値が一致していることを確認する（一致していなかったら停止する）
4. 鍵が知識にある（はずの）暗号文を受信したときは、復号化して、再帰的に平文を処理する

例1: ISO認証プロトコル

$$
\begin{array}{llcll}
1. & B & \rightarrow & A & : \quad N_B \\
2. & A & \rightarrow & B & : \quad \{N_B, B\}_{K_{AB}}
\end{array}
$$

例1: ISO認証プロトコル

$$
\begin{array}{llcll}
1. & B & \rightarrow & A & : \quad N_B \\
2. & A & \rightarrow & B & : \quad \{N_B, B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	{A, B, K_{AB}}	{A, B, K_{AB}}

例1: ISO認証プロトコル

1. $B \rightarrow A : N_B$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$

例1: ISO認証プロトコル

$$1.\quad B \rightarrow A : N_B$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後		$\{A, B, K_{AB}, N_B\}$

$$\mid \quad \nu N_B.\, \overline{\mathtt{chan}_A}\langle N_B\rangle.$$

例1: ISO認証プロトコル

$$1.\quad B \rightarrow A : N_B$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{A, B, K_{AB}, N_B \mapsto x\}$	$\{A, B, K_{AB}, N_B\}$

$$\begin{array}{ll} & \mathtt{chan}_A(x). \\ | & \nu N_B.\, \overline{\mathtt{chan}_A}\langle N_B \rangle. \end{array}$$

例1: ISO認証プロトコル

$$
\begin{array}{lcccl}
1. & B & \rightarrow & A & : N_B \\
2. & A & \rightarrow & B & : \{N_B, B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	{A, B, K_{AB}}	{A, B, K_{AB}}
1.の後	{A, B, K_{AB}, $N_B \mapsto x$}	{A, B, K_{AB}, N_B}

$$
\begin{array}{ll}
 & \mathtt{chan}_A(x). \\
| & \nu N_B.\, \overline{\mathtt{chan}_A}\langle N_B \rangle.
\end{array}
$$

例1: ISO認証プロトコル

$$
\begin{array}{lcccl}
1. & B & \rightarrow & A & : N_B \\
2. & A & \rightarrow & B & : \{N_B, B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{A, B, K_{AB}, N_B \mapsto x\}$	$\{A, B, K_{AB}, N_B\}$

$$
\begin{array}{ll}
 & \mathtt{chan}_A(x).\,\overline{\mathtt{chan}_B}\langle\{x, B\}_{K_{AB}}\rangle. \\
| & \nu N_B.\,\overline{\mathtt{chan}_A}\langle N_B\rangle.
\end{array}
$$

例1: ISO認証プロトコル

$$
\begin{array}{llcll}
1. & B & \rightarrow & A & : N_B \\
2. & A & \rightarrow & B & : \{N_B, B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{A, B, K_{AB}, N_B \mapsto x\}$	$\{A, B, K_{AB}, N_B\}$

$$
\begin{array}{ll}
 & \mathtt{chan}_A(x).\,\overline{\mathtt{chan}_B}\langle\{x, B\}_{K_{AB}}\rangle. \\
| & \nu N_B.\,\overline{\mathtt{chan}_A}\langle N_B\rangle. \\
 & \mathtt{chan}_B(y).\,\mathtt{case}\ y\ \mathtt{of}\ \{z_1, z_2\}_{K_{AB}}\ \mathtt{in} \\
 & \mathtt{if}\ z_1 = N_B\ \mathtt{then}\ \mathtt{if}\ z_2 = B\ \mathtt{then}
\end{array}
$$

例1: ISO認証プロトコル

$$
\begin{array}{lcll}
1. & B & \rightarrow & A : N_B \\
2. & A & \rightarrow & B : \{N_B, B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{A, B, K_{AB}, N_B \mapsto x\}$	$\{A, B, K_{AB}, N_B\}$

$$
\begin{array}{ll}
 & \mathtt{chan}_A(x).\,\overline{\mathtt{chan}_B}\langle\{x, B\}_{K_{AB}}\rangle.\,\mathtt{After}_A^{N_B \mapsto x} \\
| & \nu N_B.\,\overline{\mathtt{chan}_A}\langle N_B\rangle. \\
 & \mathtt{chan}_B(y).\,\mathtt{case}\ y\ \mathtt{of}\ \{z_1, z_2\}_{K_{AB}}\ \mathtt{in} \\
 & \mathtt{if}\ z_1 = N_B\ \mathtt{then}\ \mathtt{if}\ z_2 = B\ \mathtt{then}\ \mathtt{After}_B^{\emptyset}
\end{array}
$$

例2: Needham-Schroederプロトコル[Needham/Schroeder 78]

$$
\begin{array}{lrcl}
1. & A & \rightarrow B & : \{N_A, A\}_{K_B^+} \\
2. & B & \rightarrow A & : \{N_A, N_B\}_{K_A^+} \\
3. & A & \rightarrow B & : \{N_B\}_{K_B^+}
\end{array}
$$

例2: Needham-Schroederプロトコル[Needham/Schroeder 78]

$$
\begin{array}{lcl}
1. \quad A \rightarrow B & : & \{N_A, A\}_{K_B^+} \\
2. \quad B \rightarrow A & : & \{N_A, N_B\}_{K_A^+} \\
3. \quad A \rightarrow B & : & \{N_B\}_{K_B^+}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_A^+, K_B^+, K_A^-\}$	$\{A, B, K_A^+, K_B^+, K_B^-\}$

例2: Needham-Schroederプロトコル[Needham/Schroeder 78]

1. $A \rightarrow B : \{N_A, A\}_{K_B^+}$

	Aの知識	Bの知識
初期	$\{A, B, K_A^+, K_B^+, K_A^-\}$	$\{A, B, K_A^+, K_B^+, K_B^-\}$

$$\nu N_A.\,\overline{\mathtt{chan}_B}\langle \{N_A, A\}_{K_B^+} \rangle.$$

$$\mid \quad \mathtt{chan}_B(x).\,\mathtt{case}\ x\ \mathtt{of}\ \{x_1, x_2\}_{K_B^-}\ \mathtt{in}$$

$$\mathtt{if}\ x_2 = A\ \mathtt{then}$$

例2: Needham-Schroederプロトコル[Needham/Schroeder 78]

$$1.\quad A \rightarrow B : \{N_A, A\}_{K_B^+}$$

	Aの知識	Bの知識
初期	$\{A, B, K_A^+, K_B^+, K_A^-\}$	$\{A, B, K_A^+, K_B^+, K_B^-\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_1\}$

例2: Needham-Schroederプロトコル[Needham/Schroeder 78]

$$
\begin{array}{lllll}
1. & A & \rightarrow & B & : \quad \{N_A, A\}_{K_B^+} \\
2. & B & \rightarrow & A & : \quad \{N_A, N_B\}_{K_A^+}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_A^+, K_B^+, K_A^-\}$	$\{A, B, K_A^+, K_B^+, K_B^-\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_1\}$

$$\nu N_A.\,\overline{\mathtt{chan}_B}\langle \{N_A, A\}_{K_B^+} \rangle.$$
$$\mathtt{chan}_A(y).\,\mathtt{case}\ y\ \mathtt{of}\ \{y_1, y_2\}_{K_A^-}\ \mathtt{in}$$
$$\mathtt{if}\ y_1 = N_A\ \mathtt{then}$$

$$\mid\ \mathtt{chan}_B(x).\,\mathtt{case}\ x\ \mathtt{of}\ \{x_1, x_2\}_{K_B^-}\ \mathtt{in}$$
$$\mathtt{if}\ x_2 = A\ \mathtt{then}$$
$$\nu N_B.\,\overline{\mathtt{chan}_A}\langle \{x_1, N_B\}_{K_A^+} \rangle.$$

例2: Needham-Schroederプロトコル[Needham/Schroeder 78]

$$
\begin{array}{llllll}
1. & A & \rightarrow & B & : & \{N_A, A\}_{K_B^+} \\
2. & B & \rightarrow & A & : & \{N_A, N_B\}_{K_A^+}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_A^+, K_B^+, K_A^-\}$	$\{A, B, K_A^+, K_B^+, K_B^-\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_1\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$

例2: Needham-Schroederプロトコル[Needham/Schroeder 78]

$$
\begin{array}{lcl}
1. \quad A \rightarrow B & : & \{N_A, A\}_{K_B^+} \\
2. \quad B \rightarrow A & : & \{N_A, N_B\}_{K_A^+} \\
3. \quad A \rightarrow B & : & \{N_B\}_{K_B^+}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_A^+, K_B^+, K_A^-\}$	$\{A, B, K_A^+, K_B^+, K_B^-\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_1\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$

$\nu N_A.\, \overline{\mathtt{chan}_B}\langle \{N_A, A\}_{K_B^+} \rangle.$

$\mathtt{chan}_A(y).\, \mathtt{case}\ y\ \mathtt{of}\ \{y_1, y_2\}_{K_A^-}\ \mathtt{in}$

$\mathtt{if}\ y_1 = N_A\ \mathtt{then}$

$\overline{\mathtt{chan}_B}\langle \{y_2\}_{K_B^+} \rangle.$

$\mid\ \mathtt{chan}_B(x).\, \mathtt{case}\ x\ \mathtt{of}\ \{x_1, x_2\}_{K_B^-}\ \mathtt{in}$

$\mathtt{if}\ x_2 = A\ \mathtt{then}$

$\nu N_B.\, \overline{\mathtt{chan}_A}\langle \{x_1, N_B\}_{K_A^+} \rangle.$

$\mathtt{chan}_B(z).\, \mathtt{case}\ z\ \mathtt{of}\ \{z_1\}_{K_B^-}\ \mathtt{in}$

$\mathtt{if}\ z_1 = N_B\ \mathtt{then}$

$$\nu N_A.\,\overline{\mathtt{chan}_B}\langle \{N_A, A\}_{K_B^+}\rangle.$$
$$\mathtt{chan}_A(y).\,\mathtt{case}\ y\ \mathtt{of}\ \{y_1, y_2\}_{K_A^-}\ \mathtt{in}$$
$$\mathtt{if}\ y_1 = N_A\ \mathtt{then}$$
$$\overline{\mathtt{chan}_B}\langle \{y_2\}_{K_B^+}\rangle.\,\mathtt{After}_A^{N_B \mapsto y_2}$$
$$\mid\ \mathtt{chan}_B(x).\,\mathtt{case}\ x\ \mathtt{of}\ \{x_1, x_2\}_{K_B^-}\ \mathtt{in}$$
$$\mathtt{if}\ x_2 = A\ \mathtt{then}$$
$$\nu N_B.\,\overline{\mathtt{chan}_A}\langle \{x_1, N_B\}_{K_A^+}\rangle.$$
$$\mathtt{chan}_B(z).\,\mathtt{case}\ z\ \mathtt{of}\ \{z_1\}_{K_B^-}\ \mathtt{in}$$
$$\mathtt{if}\ z_1 = N_B\ \mathtt{then}\ \mathtt{After}_B^{N_A \mapsto x_1}$$

例3: Andrew Secure RPCプロトコル

$$
\begin{array}{llcll}
1. & A & \rightarrow & B & : \quad A, \{N_A\}_{K_{AB}} \\
2. & B & \rightarrow & A & : \quad \{succ(N_A), N_B\}_{K_{AB}} \\
3. & A & \rightarrow & B & : \quad \{succ(N_B)\}_{K_{AB}} \\
4. & B & \rightarrow & A & : \quad \{K'_{AB}, N'_B\}_{K_{AB}}
\end{array}
$$

例3: Andrew Secure RPCプロトコル

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \; A, \{N_A\}_{K_{AB}} \\
2. & B & \rightarrow & A & : \; \{succ(N_A), N_B\}_{K_{AB}} \\
3. & A & \rightarrow & B & : \; \{succ(N_B)\}_{K_{AB}} \\
4. & B & \rightarrow & A & : \; \{K'_{AB}, N'_B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$

例3: Andrew Secure RPCプロトコル

1. $A \rightarrow B : A, \{N_A\}_{K_{AB}}$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$

$\nu N_A.\, \overline{\mathtt{chan}_B}\langle A, \{N_A\}_{K_{AB}}\rangle.$

$\mid \quad \mathtt{chan}_B(x_1, x_2).\, \mathtt{if}\ x_1 = A\ \mathtt{then}$
$\mathtt{case}\ x_2\ \mathtt{of}\ \{x_3\}_{K_{AB}}\ \mathtt{in}$

例3: Andrew Secure RPCプロトコル

1. $A \rightarrow B : A, \{N_A\}_{K_{AB}}$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_3\}$

例3: Andrew Secure RPCプロトコル

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \quad A, \{N_A\}_{K_{AB}} \\
2. & B & \rightarrow & A & : \quad \{succ(N_A), N_B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_3\}$

$\nu N_A.\,\overline{\mathtt{chan}_B}\langle A, \{N_A\}_{K_{AB}}\rangle.$
$\mathtt{chan}_A(y).\,\mathtt{case}\ y\ \mathtt{of}\ \{y_1, y_2\}_{K_{AB}}\ \mathtt{in}$
$\mathtt{if}\ y_1 = succ(N_A)\ \mathtt{then}$

$\mid\ \mathtt{chan}_B(x_1, x_2).\,\mathtt{if}\ x_1 = A\ \mathtt{then}$
$\mathtt{case}\ x_2\ \mathtt{of}\ \{x_3\}_{K_{AB}}\ \mathtt{in}$
$\nu N_B.\,\overline{\mathtt{chan}_A}\langle\{succ(x_3), N_B\}_{K_{AB}}\rangle.$

例3: Andrew Secure RPCプロトコル

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \quad A, \{N_A\}_{K_{AB}} \\
2. & B & \rightarrow & A & : \quad \{succ(N_A), N_B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_3\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$

例3: Andrew Secure RPCプロトコル

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \; A, \{N_A\}_{K_{AB}} \\
2. & B & \rightarrow & A & : \; \{succ(N_A), N_B\}_{K_{AB}} \\
3. & A & \rightarrow & B & : \; \{succ(N_B)\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_3\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$

$\nu N_A.\, \overline{\mathtt{chan}_B}\langle A, \{N_A\}_{K_{AB}}\rangle.$
$\mathtt{chan}_A(y).\, \mathtt{case}\ y\ \mathtt{of}\ \{y_1, y_2\}_{K_{AB}}\ \mathtt{in}$
$\mathtt{if}\ y_1 = succ(N_A)\ \mathtt{then}$
$\overline{\mathtt{chan}_B}\langle\{succ(y_2)\}_{K_{AB}}\rangle.$

$\mid\ \mathtt{chan}_B(x_1, x_2).\, \mathtt{if}\ x_1 = A\ \mathtt{then}$
$\mathtt{case}\ x_2\ \mathtt{of}\ \{x_3\}_{K_{AB}}\ \mathtt{in}$
$\nu N_B.\, \overline{\mathtt{chan}_A}\langle\{succ(x_3), N_B\}_{K_{AB}}\rangle.$
$\mathtt{chan}_B(z).\, \mathtt{case}\ z\ \mathtt{of}\ \{z_1\}_{K_{AB}}\ \mathtt{in}$
$\mathtt{if}\ z_1 = succ(N_B)\ \mathtt{then}$

例3: Andrew Secure RPCプロトコル

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \; A, \{N_A\}_{K_{AB}} \\
2. & B & \rightarrow & A & : \; \{succ(N_A), N_B\}_{K_{AB}} \\
3. & A & \rightarrow & B & : \; \{succ(N_B)\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_3\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$
3.の後	同上	同上

例3: Andrew Secure RPCプロトコル

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \; A, \{N_A\}_{K_{AB}} \\
2. & B & \rightarrow & A & : \; \{succ(N_A), N_B\}_{K_{AB}} \\
3. & A & \rightarrow & B & : \; \{succ(N_B)\}_{K_{AB}} \\
4. & B & \rightarrow & A & : \; \{K'_{AB}, N'_B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_3\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$
3.の後	同上	同上

$\nu N_A.\,\overline{\mathtt{chan}_B}\langle A, \{N_A\}_{K_{AB}}\rangle.$
$\mathtt{chan}_A(y).\,\mathtt{case}\ y\ \mathtt{of}\ \{y_1, y_2\}_{K_{AB}}\ \mathtt{in}$
$\mathtt{if}\ y_1 = succ(N_A)\ \mathtt{then}$
$\overline{\mathtt{chan}_B}\langle\{succ(y_2)\}_{K_{AB}}\rangle.$
$C_A(w).\,\mathtt{case}\ w\ \mathtt{of}\ \{w_1, w_2\}_{K_{AB}}\ \mathtt{in}$

$\mid\ \mathtt{chan}_B(x_1, x_2).\,\mathtt{if}\ x_1 = A\ \mathtt{then}$
$\mathtt{case}\ x_2\ \mathtt{of}\ \{x_3\}_{K_{AB}}\ \mathtt{in}$
$\nu N_B.\,\overline{\mathtt{chan}_A}\langle\{succ(x_3), N_B\}_{K_{AB}}\rangle.$
$\mathtt{chan}_B(z).\,\mathtt{case}\ z\ \mathtt{of}\ \{z_1\}_{K_{AB}}\ \mathtt{in}$
$\mathtt{if}\ z_1 = succ(N_B)\ \mathtt{then}$
$\nu K'_{AB}.\,\nu N'_B.\,\overline{\mathtt{chan}_A}\langle\{K'_{AB}, N'_B\}_{K_{AB}}\rangle.$

例3: Andrew Secure RPCプロトコル

$$
\begin{array}{llcll}
1. & A & \rightarrow & B & : A, \{N_A\}_{K_{AB}} \\
2. & B & \rightarrow & A & : \{succ(N_A), N_B\}_{K_{AB}} \\
3. & A & \rightarrow & B & : \{succ(N_B)\}_{K_{AB}} \\
4. & B & \rightarrow & A & : \{K'_{AB}, N'_B\}_{K_{AB}}
\end{array}
$$

	Aの知識	Bの知識
初期	$\{A, B, K_{AB}\}$	$\{A, B, K_{AB}\}$
1.の後	$\{..., N_A\}$	$\{..., N_A \mapsto x_3\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$
4.の後	$\{..., K'_{AB} \mapsto w_1, N'_B \mapsto w_2\}$	$\{..., K'_{AB}, N'_B\}$

$$\nu N_A.\,\overline{\mathtt{chan}_B}\langle A, \{N_A\}_{K_{AB}}\rangle.$$
$$\mathtt{chan}_A(y).\,\mathtt{case}\ y\ \mathtt{of}\ \{y_1, y_2\}_{K_{AB}}\ \mathtt{in}$$
$$\mathtt{if}\ y_1 = succ(N_A)\ \mathtt{then}$$
$$\overline{\mathtt{chan}_B}\langle\{succ(y_2)\}_{K_{AB}}\rangle.$$
$$C_A(w).\,\mathtt{case}\ w\ \mathtt{of}\ \{w_1, w_2\}_{K_{AB}}\ \mathtt{in}$$
$$\mathtt{After}_A^{N_B \mapsto y_2, K'_{AB} \mapsto w_1, N'_B \mapsto w_2}$$
$$\mid\ \mathtt{chan}_B(x_1, x_2).\,\mathtt{if}\ x_1 = A\ \mathtt{then}$$
$$\mathtt{case}\ x_2\ \mathtt{of}\ \{x_3\}_{K_{AB}}\ \mathtt{in}$$
$$\nu N_B.\,\overline{\mathtt{chan}_A}\langle\{succ(x_3), N_B\}_{K_{AB}}\rangle.$$
$$\mathtt{chan}_B(z).\,\mathtt{case}\ z\ \mathtt{of}\ \{z_1\}_{K_{AB}}\ \mathtt{in}$$
$$\mathtt{if}\ z_1 = succ(N_B)\ \mathtt{then}$$
$$\nu K'_{AB}.\,\nu N'_B.\,\overline{\mathtt{chan}_A}\langle\{K'_{AB}, N'_B\}_{K_{AB}}\rangle.$$
$$\mathtt{After}_B^{N_A \mapsto z_1}$$

例4: WooとLamの認証プロトコル Π [Woo/Lam 94]

$$
\begin{array}{lrcl}
1. & A & \rightarrow B & : A \\
2. & B & \rightarrow A & : N_B \\
3. & A & \rightarrow B & : \{N_B\}_{K_{AS}} \\
4. & B & \rightarrow S & : \{A, \{N_B\}_{K_{AS}}\}_{K_{BS}} \\
5. & S & \rightarrow B & : \{N_B\}_{K_{BS}}
\end{array}
$$

例4: WooとLamの認証プロトコル∏ [Woo/Lam 94]

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \; A \\
2. & B & \rightarrow & A & : \; N_B \\
3. & A & \rightarrow & B & : \; \{N_B\}_{K_{AS}} \\
4. & B & \rightarrow & S & : \; \{A, \{N_B\}_{K_{AS}}\}_{K_{BS}} \\
5. & S & \rightarrow & B & : \; \{N_B\}_{K_{BS}}
\end{array}
$$

	Aの知識	Bの知識	Sの知識
初期	{A, B, S, K_{AS}}	{A, B, S, K_{BS}}	{A, B, S, K_{AS}, K_{BS}}

例4: WooとLamの認証プロトコル∏ [Woo/Lam 94]

1. $A \rightarrow B : A$

	Aの知識	Bの知識	Sの知識
初期	{A, B, S, K_{AS}}	{A, B, S, K_{BS}}	{A, B, S, K_{AS}, K_{BS}}

$\overline{\texttt{chan}_B}\langle A \rangle.$

$\mid \quad \texttt{chan}_B(x).\,\texttt{if}\ x = A\ \texttt{then}$

$\mid$

例4: WooとLamの認証プロトコル∏ [Woo/Lam 94]

1. $A \rightarrow B : A$
2. $B \rightarrow A : N_B$

	Aの知識	Bの知識	Sの知識
初期	$\{A, B, S, K_{AS}\}$	$\{A, B, S, K_{BS}\}$	$\{A, B, S, K_{AS}, K_{BS}\}$

$$\overline{\mathtt{chan}_B}\langle A\rangle.$$

$$\mathtt{chan}_A(y).$$

$$\mid \mathtt{chan}_B(x).\,\mathtt{if}\ x = A\ \mathtt{then}\ \nu N_B.\,\overline{\mathtt{chan}_A}\langle N_B\rangle.$$

$$\mid$$

例4: WooとLamの認証プロトコル∏ [Woo/Lam 94]

1. $A \rightarrow B : A$
2. $B \rightarrow A : N_B$

	Aの知識	Bの知識	Sの知識
初期	$\{A, B, S, K_{AS}\}$	$\{A, B, S, K_{BS}\}$	$\{A, B, S, K_{AS}, K_{BS}\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$	同上

例4: WooとLamの認証プロトコル∏ [Woo/Lam 94]

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \quad A \\
2. & B & \rightarrow & A & : \quad N_B \\
3. & A & \rightarrow & B & : \quad \{N_B\}_{K_{AS}}
\end{array}
$$

	Aの知識	Bの知識	Sの知識
初期	$\{A, B, S, K_{AS}\}$	$\{A, B, S, K_{BS}\}$	$\{A, B, S, K_{AS}, K_{BS}\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$	同上

$$\overline{\texttt{chan}_B}\langle A\rangle.$$
$$\texttt{chan}_A(y).\,\overline{\texttt{chan}_B}\langle\{y\}_{K_{AS}}\rangle.$$
$$\mid\ \texttt{chan}_B(x).\,\texttt{if}\ x = A\ \texttt{then}\ \nu N_B.\,\overline{\texttt{chan}_A}\langle N_B\rangle.$$
$$\texttt{chan}_B(z).$$

$$\mid$$

例4: WooとLamの認証プロトコル∏ [Woo/Lam 94]

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \quad A \\
2. & B & \rightarrow & A & : \quad N_B \\
3. & A & \rightarrow & B & : \quad \{N_B\}_{K_{AS}}
\end{array}
$$

	Aの知識	Bの知識	Sの知識
初期	$\{A, B, S, K_{AS}\}$	$\{A, B, S, K_{BS}\}$	$\{A, B, S, K_{AS}, K_{BS}\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$	同上
3.の後	同上	$\{..., \{N_B\}_{KAS} \mapsto z\}$	同上

例4: WooとLamの認証プロトコル∏ [Woo/Lam 94]

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \; A \\
2. & B & \rightarrow & A & : \; N_B \\
3. & A & \rightarrow & B & : \; \{N_B\}_{K_{AS}} \\
4. & B & \rightarrow & S & : \; \{A, \{N_B\}_{K_{AS}}\}_{K_{BS}}
\end{array}
$$

	Aの知識	Bの知識	Sの知識
初期	$\{A, B, S, K_{AS}\}$	$\{A, B, S, K_{BS}\}$	$\{A, B, S, K_{AS}, K_{BS}\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$	同上
3.の後	同上	$\{..., \{N_B\}_{KAS} \mapsto z\}$	同上

$$\overline{\mathtt{chan}_B}\langle A\rangle.$$
$$\mathtt{chan}_A(y).\,\overline{\mathtt{chan}_B}\langle\{y\}_{K_{AS}}\rangle.$$
$$\mid\ \mathtt{chan}_B(x).\,\mathtt{if}\ x = A\ \mathtt{then}\ \nu N_B.\,\overline{\mathtt{chan}_A}\langle N_B\rangle.$$
$$\mathtt{chan}_B(z).\,\overline{\mathtt{chan}_S}\langle\{A, z\}_{K_{BS}}\rangle.$$

$$\mid\ \mathtt{chan}_S(w).\,\mathtt{case}\ w\ \mathtt{of}\ \{w_1, w_2\}_{K_{BS}}\ \mathtt{in}$$
$$\mathtt{if}\ w_1 = A\ \mathtt{then}\ \mathtt{case}\ w_2\ \mathtt{of}\ \{w_3\}_{K_{AS}}\ \mathtt{in}$$

例4: WooとLamの認証プロトコル∏ [Woo/Lam 94]

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \quad A \\
2. & B & \rightarrow & A & : \quad N_B \\
3. & A & \rightarrow & B & : \quad \{N_B\}_{K_{AS}} \\
4. & B & \rightarrow & S & : \quad \{A, \{N_B\}_{K_{AS}}\}_{K_{BS}}
\end{array}
$$

	Aの知識	Bの知識	Sの知識
初期	$\{A, B, S, K_{AS}\}$	$\{A, B, S, K_{BS}\}$	$\{A, B, S, K_{AS}, K_{BS}\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$	同上
3.の後	同上	$\{..., \{N_B\}_{KAS} \mapsto z\}$	同上
4.の後	同上	同上	$\{..., N_B \mapsto w_3\}$

例4: WooとLamの認証プロトコル∏ [Woo/Lam 94]

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : \; A \\
2. & B & \rightarrow & A & : \; N_B \\
3. & A & \rightarrow & B & : \; \{N_B\}_{K_{AS}} \\
4. & B & \rightarrow & S & : \; \{A, \{N_B\}_{K_{AS}}\}_{K_{BS}} \\
5. & S & \rightarrow & B & : \; \{N_B\}_{K_{BS}}
\end{array}
$$

	Aの知識	Bの知識	Sの知識
初期	$\{A, B, S, K_{AS}\}$	$\{A, B, S, K_{BS}\}$	$\{A, B, S, K_{AS}, K_{BS}\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$	同上
3.の後	同上	$\{..., \{N_B\}_{KAS} \mapsto z\}$	同上
4.の後	同上	同上	$\{..., N_B \mapsto w_3\}$

$$
\begin{array}{ll}
 & \overline{\mathtt{chan}_B}\langle A\rangle. \\
 & \mathtt{chan}_A(y).\,\overline{\mathtt{chan}_B}\langle\{y\}_{K_{AS}}\rangle. \\
\mid & \mathtt{chan}_B(x).\,\mathtt{if}\ x = A\ \mathtt{then}\ \nu N_B.\,\overline{\mathtt{chan}_A}\langle N_B\rangle. \\
 & \mathtt{chan}_B(z).\,\overline{\mathtt{chan}_S}\langle\{A, z\}_{K_{BS}}\rangle. \\
 & \mathtt{chan}_B(u).\,\mathtt{case}\ u\ \mathtt{of}\ \{u_1\}_{K_{BS}}\ \mathtt{in} \\
 & \\
 & \mathtt{if}\ u_1 = N_B\ \mathtt{then} \\
\mid & \mathtt{chan}_S(w).\,\mathtt{case}\ w\ \mathtt{of}\ \{w_1, w_2\}_{K_{BS}}\ \mathtt{in} \\
 & \mathtt{if}\ w_1 = A\ \mathtt{then}\ \mathtt{case}\ w_2\ \mathtt{of}\ \{w_3\}_{K_{AS}}\ \mathtt{in} \\
 & \overline{\mathtt{chan}_B}\langle\{w_3\}_{K_{BS}}\rangle.
\end{array}
$$

$$
\begin{array}{ll}
 & \overline{\mathtt{chan}_B}\langle A\rangle. \\
 & \mathtt{chan}_A(y).\,\overline{\mathtt{chan}_B}\langle\{y\}_{K_{AS}}\rangle.\,\mathtt{After}_A^{N_B\mapsto y} \\
| & \mathtt{chan}_B(x).\,\mathtt{if}\ x = A\ \mathtt{then}\ \nu N_B.\,\overline{\mathtt{chan}_A}\langle N_B\rangle. \\
 & \mathtt{chan}_B(z).\,\overline{\mathtt{chan}_S}\langle\{A,z\}_{K_{BS}}\rangle. \\
 & \mathtt{chan}_B(u).\,\mathtt{case}\ u\ \mathtt{of}\ \{u_1\}_{K_{BS}}\ \mathtt{in} \\
 & \mathtt{if}\ u_1 = N_B\ \mathtt{then}\ \mathtt{After}_B^{\{N_B\}_{K_{AS}}\mapsto z} \\
| & \mathtt{chan}_S(w).\,\mathtt{case}\ w\ \mathtt{of}\ \{w_1,w_2\}_{K_{BS}}\ \mathtt{in} \\
 & \mathtt{if}\ w_1 = A\ \mathtt{then}\ \mathtt{case}\ w_2\ \mathtt{of}\ \{w_3\}_{K_{AS}}\ \mathtt{in} \\
 & \overline{\mathtt{chan}_B}\langle\{w_3\}_{K_{BS}}\rangle.\,\mathtt{After}_S^{N_B\mapsto w_3}
\end{array}
$$

鍵データベースによる拡張: 例4の場合

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : A \\
2. & B & \rightarrow & A & : N_B \\
3. & A & \rightarrow & B & : \{N_B\}_{K_{AS}} \\
4. & B & \rightarrow & S & : \{A, \{N_B\}_{K_{AS}}\}_{K_{BS}} \\
5. & S & \rightarrow & B & : \{N_B\}_{K_{BS}}
\end{array}
$$

	Aの知識	Bの知識	Sの知識
初期	$\{A, B, S, K_{AS}\}$	$\{A, B, S, K_{BS}\}$	$\{A, B, S, K_{AS}, K_{BS}\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$	同上
3.の後	同上	$\{..., \{N_B\}_{KAS} \mapsto z\}$	同上
4.の後	同上	同上	$\{..., N_B \mapsto w_3\}$

鍵データベースによる拡張: 例4の場合

$$
\begin{array}{lcccl}
1. & A & \rightarrow & B & : A \\
2. & B & \rightarrow & A & : N_B \\
3. & A & \rightarrow & B & : \{N_B\}_{K_{AS}} \\
4. & B & \rightarrow & S & : \{A, \{N_B\}_{K_{AS}}\}_{K_{BS}} \\
5. & S & \rightarrow & B & : \{N_B\}_{K_{BS}}
\end{array}
$$

	Aの知識	Bの知識	Sの知識
初期	$\{A, B, S, K_{AS}\}$	$\{A, B, S, K_{BS}\}$	$\{A, B, S, K_{AS}, K_{BS}\}$
2.の後	$\{..., N_B \mapsto y_2\}$	$\{..., N_B\}$	同上
3.の後	同上	$\{..., \{N_B\}_{KAS} \mapsto z\}$	同上
4.の後	同上	同上	$\{..., N_B \mapsto w_3\}$

素朴に変換すると...

$$
\begin{array}{ll}
 & \overline{\mathtt{chan}_B}\langle A\rangle. \\
 & \mathtt{chan}_A(y).\,\overline{\mathtt{chan}_B}\langle\{y\}_{K_{AS}}\rangle.\,\mathtt{After}_A^{N_B\mapsto y} \\
\mid & \mathtt{chan}_B(x).\,\nu N_B.\,\overline{\mathtt{chan}_A}\langle N_B\rangle. \\
 & \mathtt{chan}_B(z).\,\overline{\mathtt{chan}_S}\langle\{x,z\}_{K_{BS}}\rangle. \\
 & \mathtt{chan}_B(u).\,\mathtt{case}\ u\ \mathtt{of}\ \{u_1\}_{K_{BS}}\ \mathtt{in} \\
 & \mathtt{if}\ u_1 = N_B\ \mathtt{then}\ \mathtt{After}_B^{\{N_B\}_{K_{AS}}\mapsto z} \\
\mid & \mathtt{chan}_S(w).\,\mathtt{case}\ w\ \mathtt{of}\ \{w_1,w_2\}_{K_{BS}}\ \mathtt{in} \\
 & \mathtt{case}\ w_2\ \mathtt{of}\ \{w_3\}_{K_{AS}}\ \mathtt{in} \\
 & \overline{\mathtt{chan}_B}\langle\{w_3\}_{K_{BS}}\rangle.\,\mathtt{After}_S^{N_B\mapsto w_3}
\end{array}
$$

- やはり特定のAとしか通信できない

自明に「拡張」すると…

$$
\begin{array}{ll}
 & \overline{\mathtt{chan}_B}\langle A\rangle. \\
 & \mathtt{chan}_A(y).\,\overline{\mathtt{chan}_B}\langle\{y\}_{K_{AS}}\rangle.\,\mathtt{After}_A^{N_B\mapsto y} \\
\mid & \mathtt{chan}_B(x).\,\nu N_B.\,\overline{\mathtt{chan}_x}\langle N_B\rangle. \\
 & \mathtt{chan}_B(z).\,\overline{\mathtt{chan}_S}\langle\{x,z\}_{K_{BS}}\rangle. \\
 & \mathtt{chan}_B(u).\,\mathtt{case}\ u\ \mathtt{of}\ \{u_1\}_{K_{BS}}\ \mathtt{in} \\
 & \mathtt{if}\ u_1 = N_B\ \mathtt{then}\ \mathtt{After}_B^{\{N_B\}_{K_{AS}}\mapsto z} \\
\mid & \mathtt{chan}_S(w).\,\mathtt{case}\ w\ \mathtt{of}\ \{w_1,w_2\}_{K_{BS}}\ \mathtt{in} \\
 & \mathtt{case}\ w_2\ \mathtt{of}\ \{w_3\}_{K_{xS}}\ \mathtt{in} \\
 & \overline{\mathtt{chan}_B}\langle\{w_3\}_{K_{BS}}\rangle.\,\mathtt{After}_S^{N_B\mapsto w_3}
\end{array}
$$

- spi計算の操作的意味論を逸脱

解決: 動的な検索

$$
\begin{array}{l}
\quad \overline{\mathtt{chan}_B}\langle A\rangle. \\
\quad \mathtt{chan}_A(y).\, \overline{\mathtt{chan}_B}\langle \{y\}_{K_{AS}}\rangle.\, \mathtt{After}_A^{N_B \mapsto y} \\
\mid \quad \mathtt{chan}_B(x).\, \nu N_B.\, \boxed{\mathit{lookup}\ \mathtt{chan}_x\ \mathit{in}}\ \overline{\mathtt{chan}_x}\langle N_B\rangle. \\
\quad \mathtt{chan}_B(z).\, \overline{\mathtt{chan}_S}\langle \{x, z\}_{K_{BS}}\rangle. \\
\quad \mathtt{chan}_B(u).\, \mathtt{case}\ u\ \mathtt{of}\ \{u_1\}_{K_{BS}}\ \mathtt{in} \\
\quad \mathtt{if}\ u_1 = N_B\ \mathtt{then}\ \mathtt{After}_B^{\{N_B\}_{K_{AS}} \mapsto z} \\
\mid \quad \mathtt{chan}_S(w).\, \mathtt{case}\ w\ \mathtt{of}\ \{w_1, w_2\}_{K_{BS}}\ \mathtt{in} \\
\quad \boxed{\mathit{lookup}\ K_{xS}\ \mathit{in}}\ \mathtt{case}\ w_2\ \mathtt{of}\ \{w_3\}_{K_{xS}}\ \mathtt{in} \\
\quad \overline{\mathtt{chan}_B}\langle \{w_3\}_{K_{BS}}\rangle.\, \mathtt{After}_S^{N_B \mapsto w_3}
\end{array}
$$

- 実際には「*lookup ... in ...*」も通常のspi計算におけるプロセスの構文糖衣として実現

結論(1/2)

- セキュリティプロトコルの略式記法の意味を、spi計算への変換により定義
  - Objective Caml [Leroy他]で実装

    プレーンテキスト

    ⇒ 略式記法を表現するOCamlのデータ型

    ⇒ spi計算のプロセスを表現するOCamlのデータ型

    ⇒ TeX
  - 文献[Clark/Jacob 97]にある24個のプロトコルについて、変換の妥当さを目視で確認

結論(2/2)

- 関連研究:
  Casper [Lowe 97], CAPSL [Millen]
  - プロトコルの動作を記述する目的では我々の方法より面倒
- さらなる拡張
  - プロトコルの意図の記述
    - 秘密にしたいメッセージを指定(secrecy)
    - 対応表明[Woo/Lam 93]を挿入(authenticity)
  - 算術演算の性質の考慮
    - **A → B : (x + y) + z *as* x + (y + z)** のように指定