ストランド空間

ストランド空間モデル

- ストランド空間モデル
  - Guttman, *et al.*（1998）
  - ストランド（個々の主体の実行トレース）
  - バンドル（因果関係について閉じたストランドの集合）
  - 後ろ向き推論 によるバンドルの網羅
- 攻撃者のストランド

  攻撃者によるあらゆる攻撃を想定。

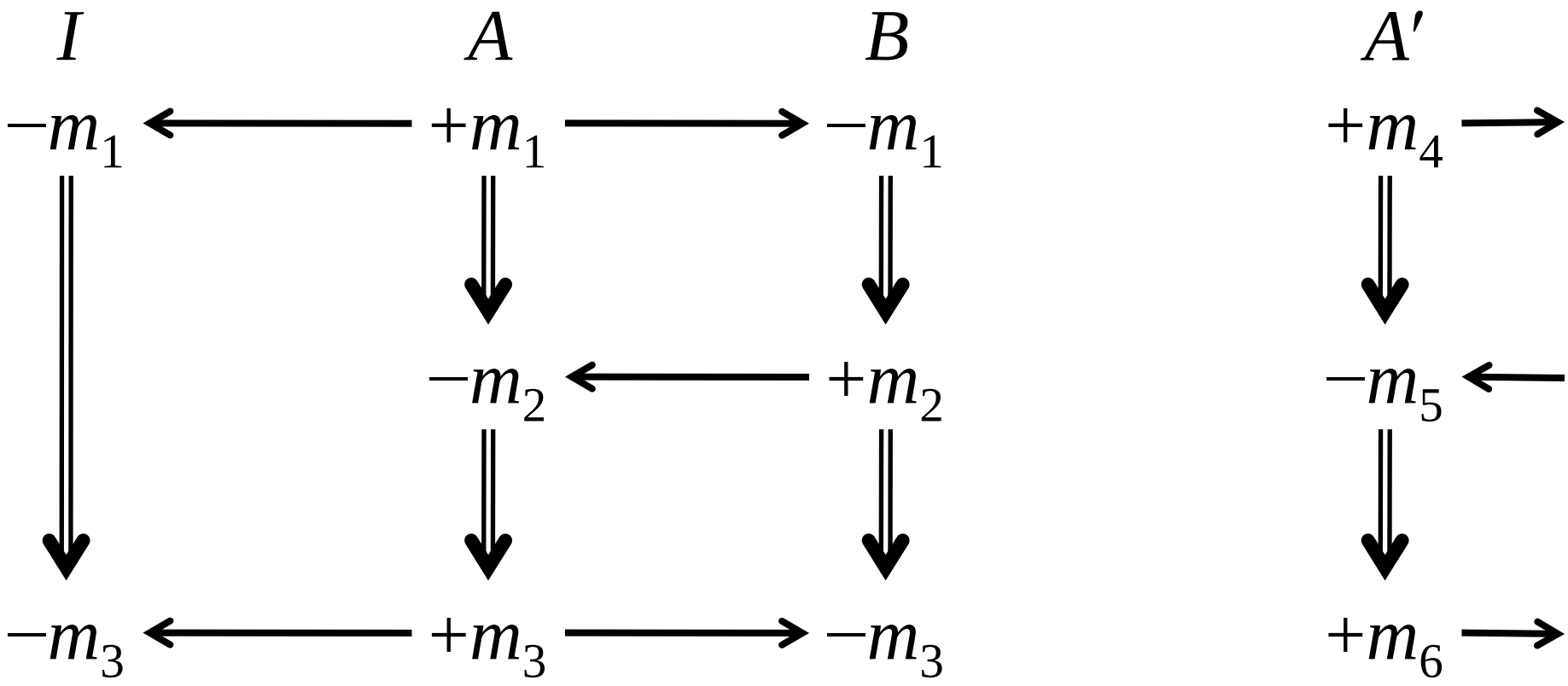
問題と提案手法

- セキュリティ・プロトコルとその実行をどのようにモデルかするか？
- 以下のことが可能なフレームワーク
  - セキュリティに関連した性質の形式的仕様
  - プロトコルの正しさの証明
  - プロトコルに依存しない推論
    - 前提が明確になる
- 提案手法：ストランド空間

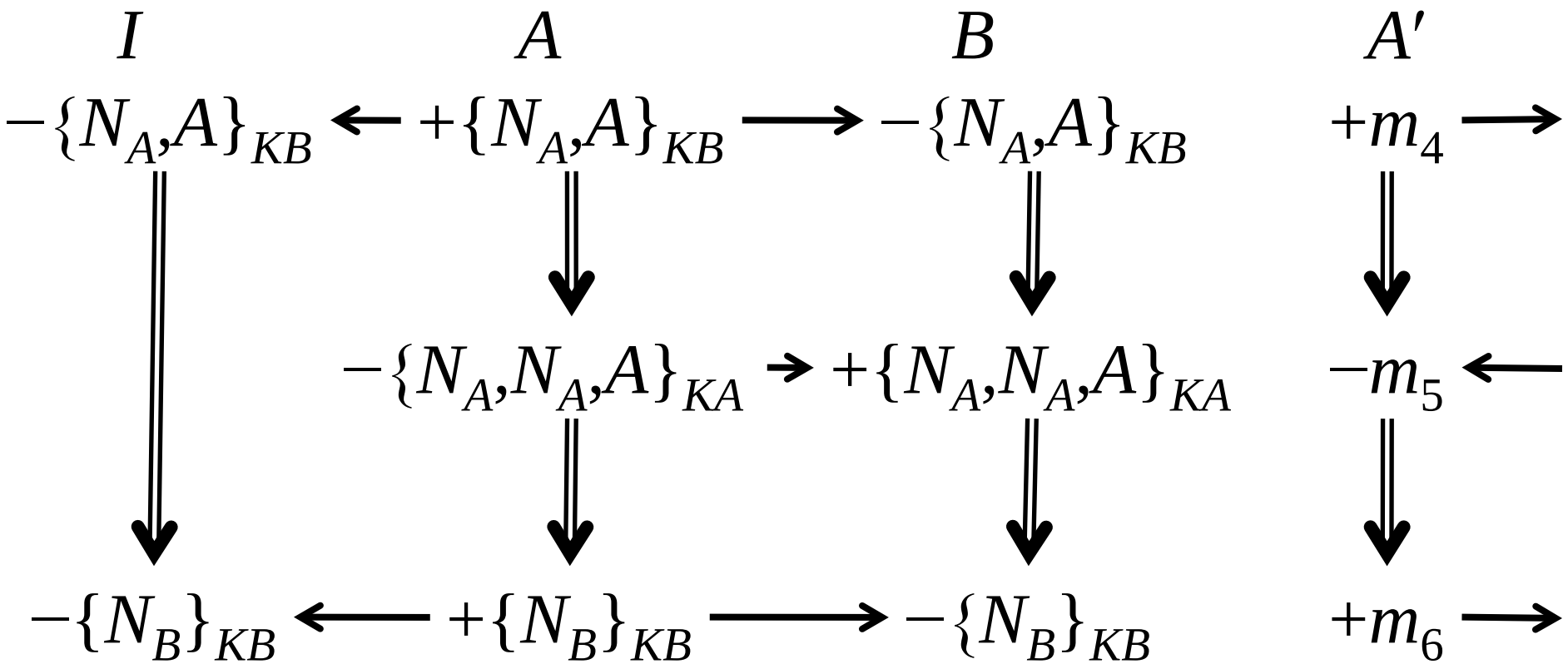
ストランド空間の定義

- メッセージ空間 $\boldsymbol{M}$
- 符号
  - 送信 ＋
  - 受信 －
- ストランド空間 (tr, Σ)
  - $tr : \Sigma \to (\pm M)^*$
- ストランド $s \in \Sigma$
  - $s \longmapsto tr(s) = \langle +m_1, -m_2, +m_3 \rangle$

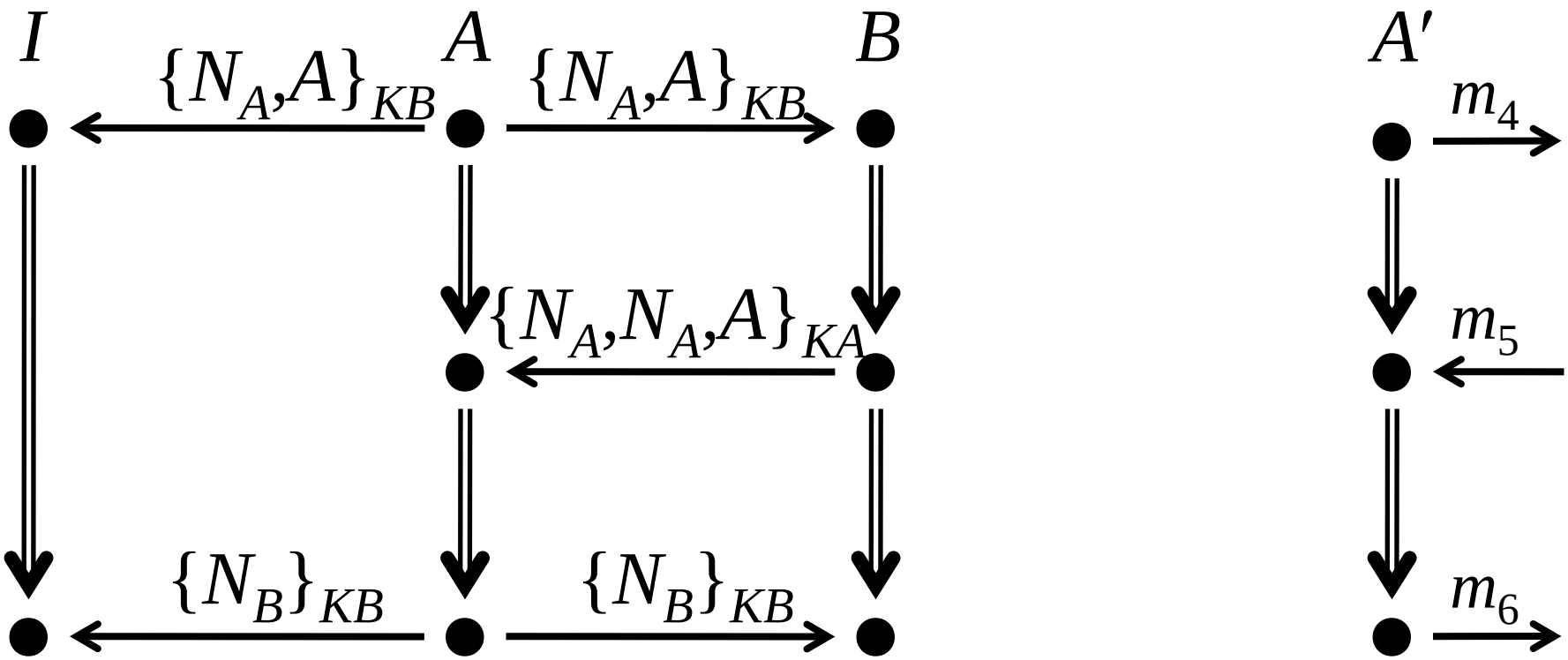
- $\Sigma = \{A, B, I, A'\}$
- $tr(A) = \langle +m_1, -m_2, +m_3 \rangle$
- $tr(B) = \langle -m_1, +m_2, -m_3 \rangle$
- $tr(I) = \langle -m_1, -m_3 \rangle$
- $tr(A') = \langle +m_4, -m_5, +m_6 \rangle$



- $\Sigma = \{A, B, I, A'\}$
- $tr(A) = \langle +\{N_A,A\}_{KB}, -\{N_A,N_A,A\}_{KA}, +\{N_B\}_{KB} \rangle$
- $tr(B) = \langle -\{N_A,A\}_{KB}, -\{N_A,N_A,A\}_{KA}, -\{N_B\}_{KB} \rangle$
- $tr(I) = \langle -\{N_A,A\}_{KB}, -\{N_B\}_{KB} \rangle$
- $tr(A') = \langle +m_4, -m_5, +m_6 \rangle$

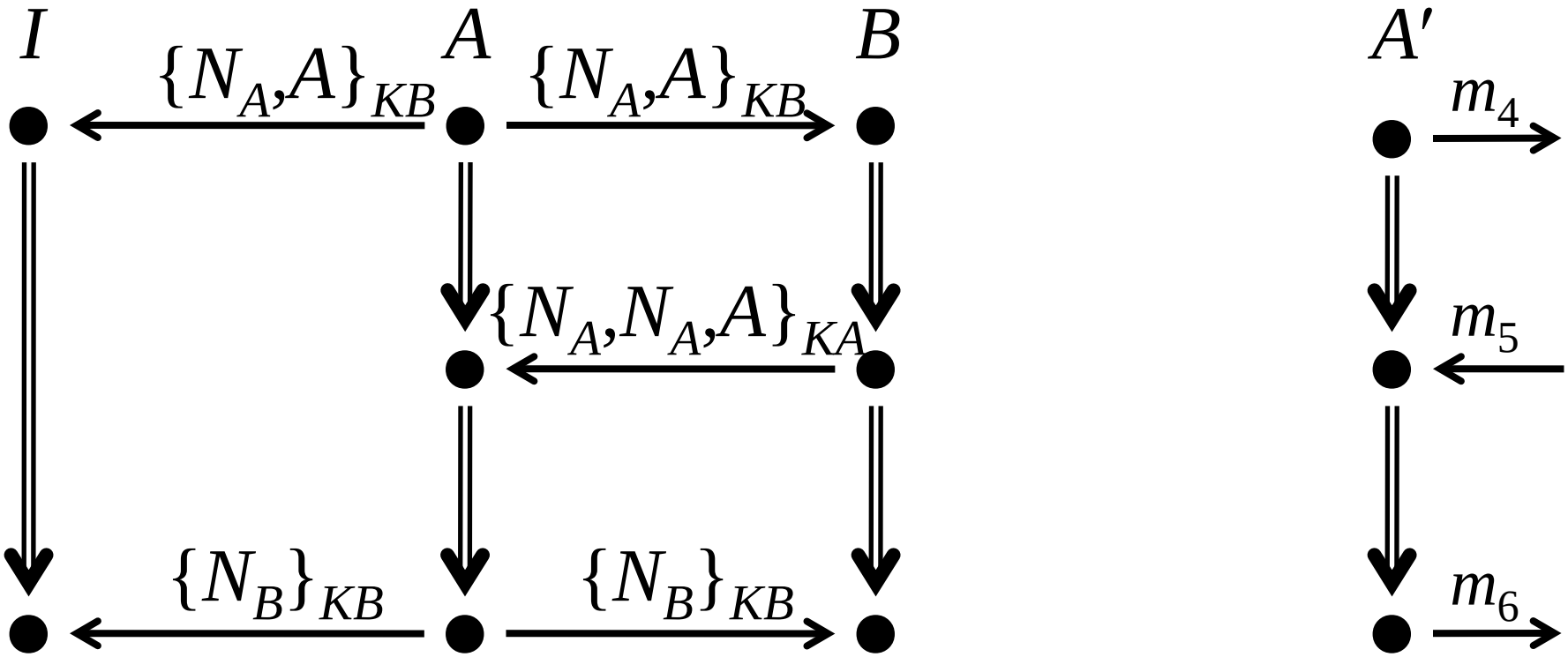


- $\Sigma = \{A, B, I, A'\}$
- $tr(A) = \langle +\{N_A,A\}_{KB}, -\{N_A,N_A,A\}_{KA}, +\{N_B\}_{KB} \rangle$
- $tr(B) = \langle -\{N_A,A\}_{KB}, -\{N_A,N_A,A\}_{KA}, -\{N_B\}_{KB} \rangle$
- $tr(I) = \langle -\{N_A,A\}_{KB}, -\{N_B\}_{KB} \rangle$
- $tr(A') = \langle +m_4, -m_5, +m_6 \rangle$



ストランド空間グラフ

- ノードの全体 N
- ストランド内の因果関係
- ストランド間の因果関係



バンドル

- ストランド空間グラフの部分グラフ
  - $C = \langle N_C, \rightarrow_C, \Rightarrow_C \rangle$
- 唯一の送信者が存在する。
  - 任意のノード $n \in N_C$ に対して、n が負ならば、唯一つの送信ノード $n' \in N_C$ が存在して $n' \rightarrow_C n$
- ストランド内の因果関係について閉じている。
  - $n \in N_C$ かつ $n' \Rightarrow n$ ならば $n' \in N_C$
- 有限かつサイクルを含まない。

バンドルの性質

- $\leqq$: $\rightarrow_C$ と $\Rightarrow_C$ の合併の反射推移閉包
  - $n \leqq n'$ とは、n から n' へ $\rightarrow_C$ または $\Rightarrow_C$ を繰り返して到達できること。
  - N_C 上の半順序
- 任意の空でない C の部分集合 S は、$\leqq$ に関する極小元を持つ。
  - もちろん、そのような極小元は S の元。
- C 自身の $\leqq$ に関する極小元の符号は正。

メッセージ空間

- 以下のようにして作られる自由代数 $\boldsymbol{M}$
  - $\boldsymbol{T} \subseteq \boldsymbol{M}$: テキスト
  - $\boldsymbol{K} \subseteq \boldsymbol{M}$: 鍵（$\boldsymbol{T} \cap \boldsymbol{K} = \emptyset$）
    - 攻撃者が持っている鍵の集合を $\boldsymbol{K}_I$ とおく。
  - 組 : $m_1 \in M$ かつ $m_2 \in M$ ならば $\langle m_1, m_2 \rangle \in \boldsymbol{M}$
  - 暗号化 : $K \in \boldsymbol{K}$ かつ $m \in M$ ならば $\{m\}_K \in \boldsymbol{M}$
  - 常に新規に記号を作ることが可能。
- 部分項
  - $m_1 \subset m_2$ **iff** m_1 は m_2 の部分項（$m_1 = m_2$ も含む）
  - $m \subset \{m\}_K$ は成り立つが、$K \subset m$ でない限り $K \subset \{m\}_K$ は成り立たない。

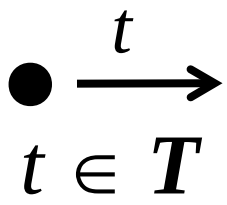
起源

- メッセージ m がノード $n \in N$ を起源とするとは、
  - n の符号は正（送信）
  - $m \sqsubset \mathrm{message}(n)$
    - $\mathrm{message}(n)$ は n の送受信する（符号なし）メッセージ。
  - n と同じストランド内で先行するノード p に対して、$m \sqsubset \mathrm{message}(p)$ でない。
- m の起源が唯一ならば、m はノンスと考えられる。

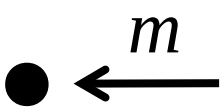
攻撃者のストランド

Dolev-Yao
モデル

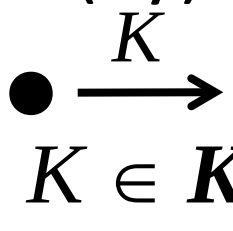
M(essage)



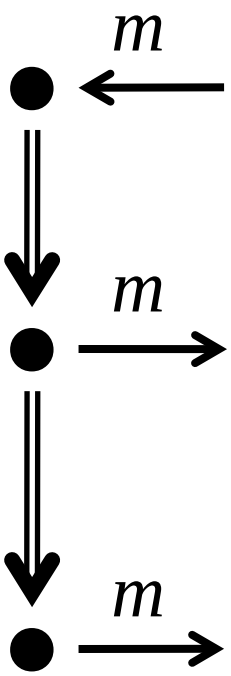
F(lushing)



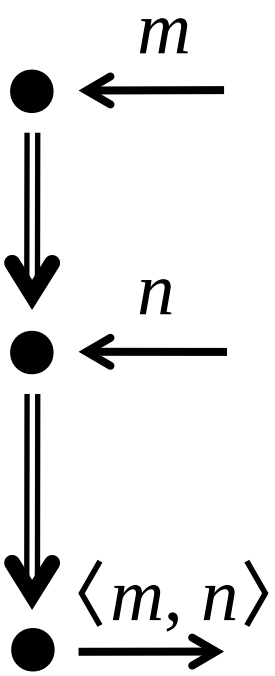
K(ey)



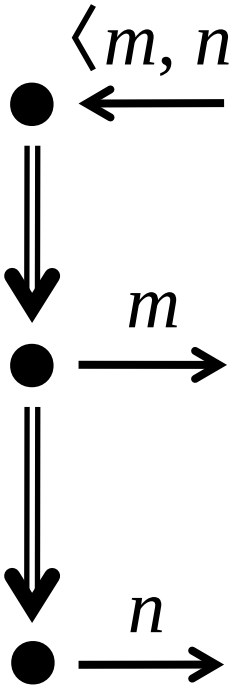
T(ee)



C(oncatenation)

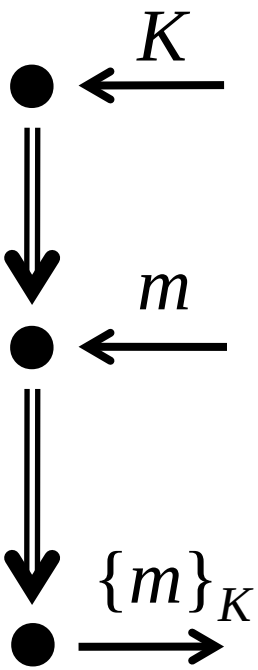


S(eparation)

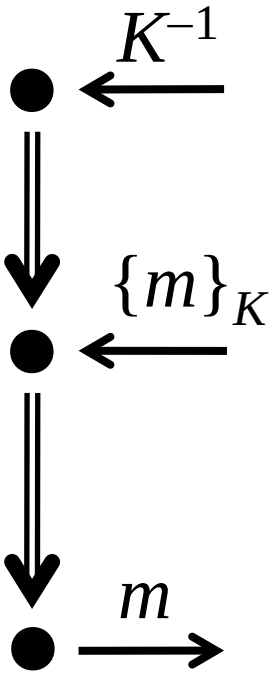


攻撃者のストランド

E(ncryption)



D(ecryption)



攻撃者の限界

- ストランドを、攻撃者のストランドと正規参加者のストランドに分ける。
  - 攻撃者のストランドのノードを攻撃者ノードという。
  - 正規参加者のストランドのノードを正規ノードという。
- 命題
  - C をバンドルとする。
  - $K \in \boldsymbol{K} \backslash \boldsymbol{K}_I$ とする。
  - K が正規ノードを起源としないならば、K は攻撃者ノードに部分項として現れない。

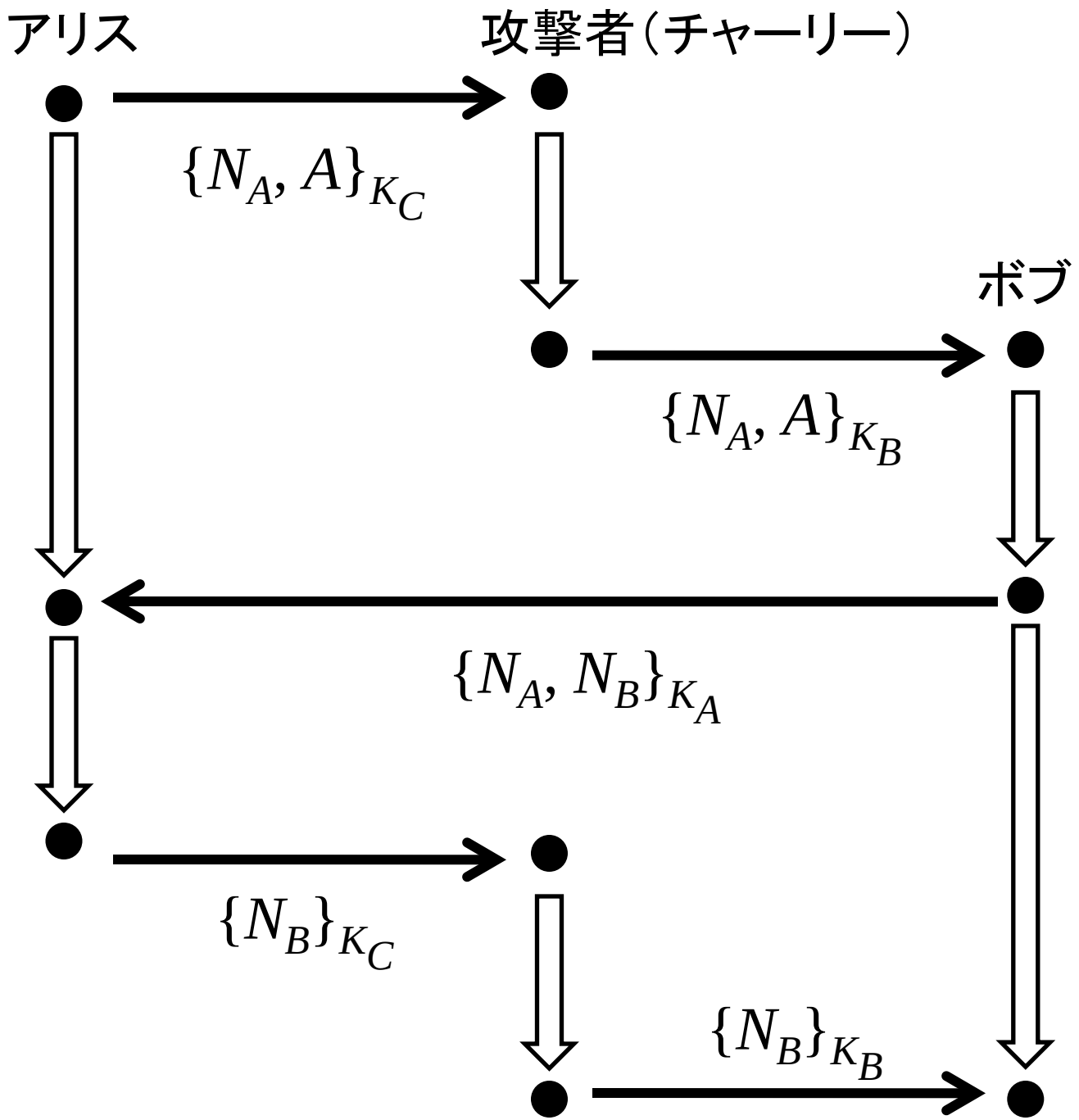
証明スケッチ

- $S = \{n \in C \mid K \subset \text{message}(n)\}$ は空でないと仮定する。
- S の任意の極小元は、K の起源である。
  - 負のノードとすると、その送信者（正のノード）も S に入るはずなので、極小にはならない。
  - 同じストランド内で先行するノードに K が含まれるとすると、やはり極小にならない。
- 仮定より攻撃者ノード。矛盾を導く。
  - 攻撃者ストランド（M, F, T, ...）に関する場合分け。
    - たとえば、S: $-\langle g, h\rangle$, $+g$, $+h$ における $+g$ が S に入るとすると、$-\langle g, h\rangle$ も S に入るので、やはり $+g$ は極小にはならない。

修正されたプロトコル

- Needham-Schroeder-Lowe

$$A \rightarrow B : \{A, N_A\}_{KB}$$
$$B \rightarrow A : \{B, N_A, N_B\}_{KA}$$
$$A \rightarrow B : \{N_B\}_{KB}$$


アリス
攻撃者（チャーリー）
ボブ
$\{N_A, A\}_{K_C}$
$\{N_A, A\}_{K_B}$
$\{N_A, N_B\}_{K_A}$
$\{N_B\}_{K_C}$
$\{N_B\}_{K_B}$

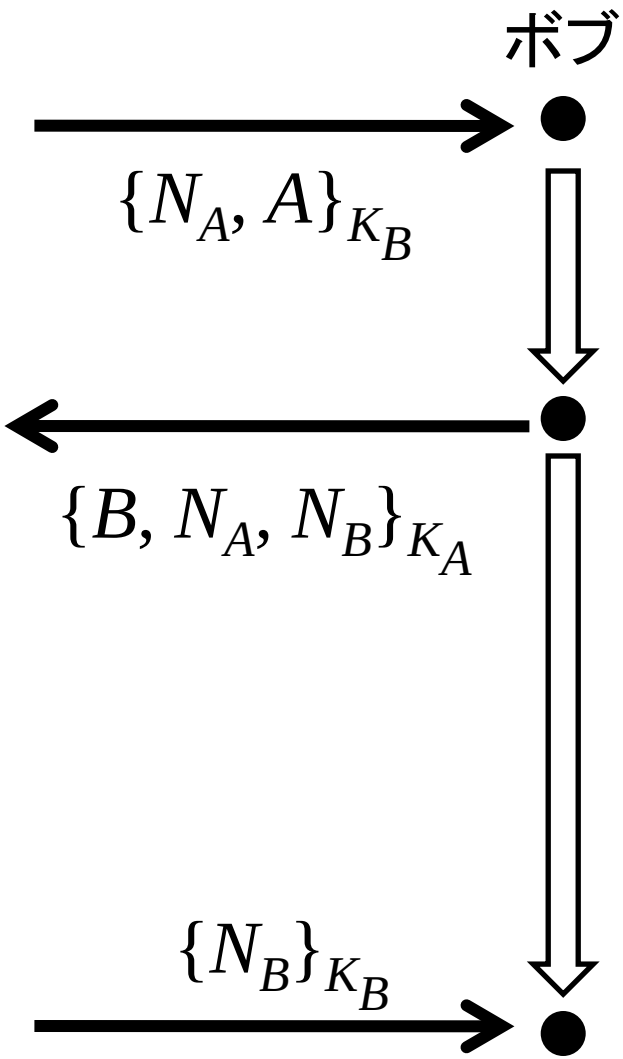
ストランド空間モデルによる検証

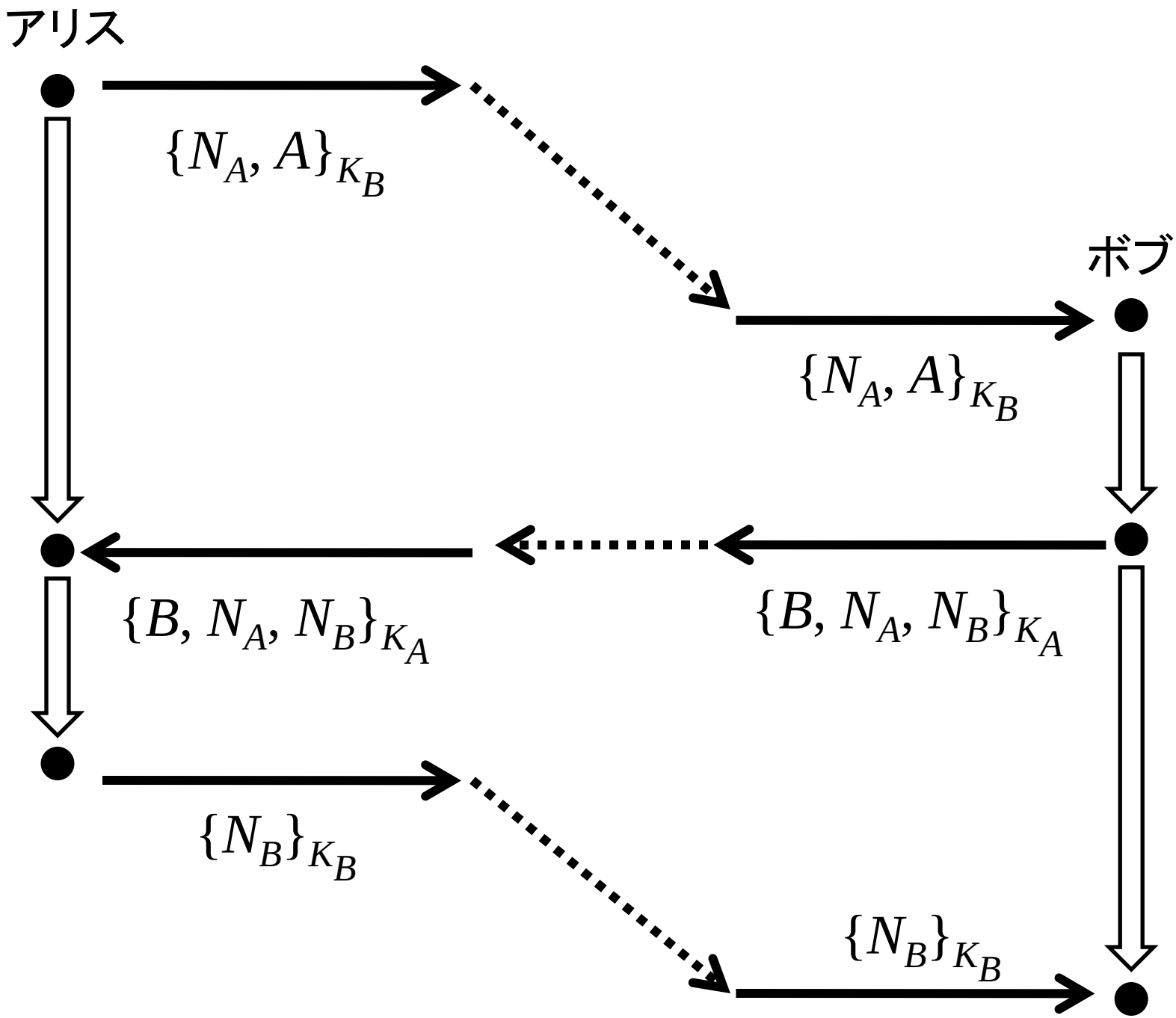
- **agreement** の検証

  ある主体のストランドを仮定して、
  それを含むバンドルを網羅し、
  対応する主体のストランドが必ずバンドルに
  含まれることを示す。
- 認証性（authenticity）
- 相互認証性（mutual authenticity）

レスポンダによるイニシエータの認証

- C は NSL ストランド空間のバンドルとする。
- s は C の中の A, B, N_A, N_B をパラメタとするレスポンダのストランドとする。
- $K_A^{-1} \notin \boldsymbol{K}_I$
- $N_A \neq N_B$
- N_B は唯一の起源を持つ。
- 以上が成り立つとき、C は A, B, N_A, N_B をパラメタとするイニシエータのストランドを含む。


ボブ
$\{N_A, A\}_{K_B}$
$\{B, N_A, N_B\}_{K_A}$
$\{N_B\}_{K_B}$

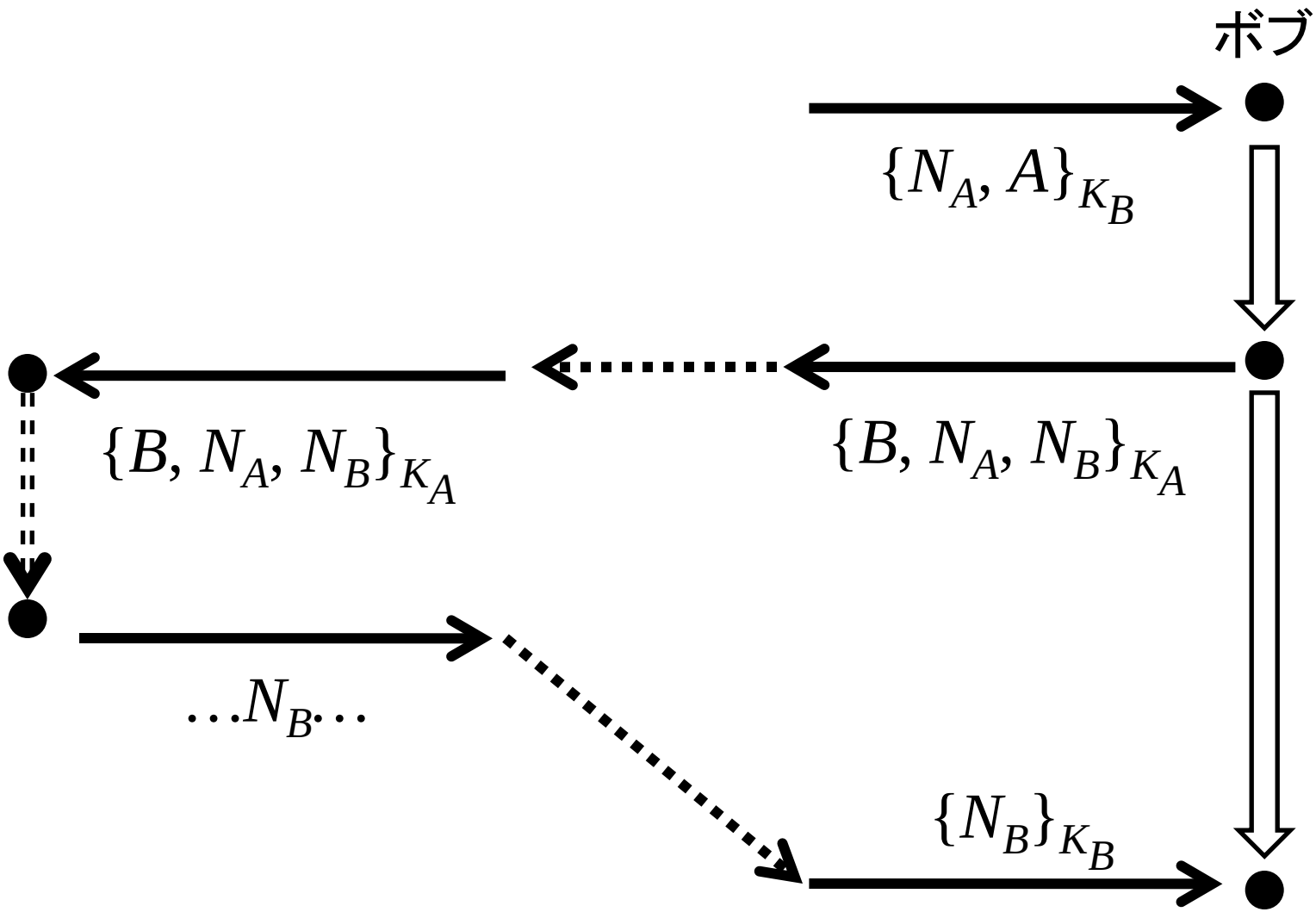

アリス
ボブ
$\{N_A, A\}_{K_B}$
$\{N_A, A\}_{K_B}$
$\{B, N_A, N_B\}_{K_A}$
$\{B, N_A, N_B\}_{K_A}$
$\{N_B\}_{K_B}$
$\{N_B\}_{K_B}$

補題

- N_B を含んでいるが、$\{B, N_A, N_B\}_{K_A}$ を含んでいないノードの全体を S とすると、S の極小元は正規ノードになる。
- 攻撃者ノードと仮定して矛盾を導く。
  - 攻撃者ストランド（M, F, T, …）に関する場合分け。
  - 極小性より、S: $-\langle g, h \rangle$, $+g$, $+h$ の場合のみ有り得る。
    - たとえば、$+g$ が極小元とすると、g は N_B を含んでいて、h は $\{B, N_A, N_B\}_{K_A}$ を含む。
  - $\langle g, h \rangle$ を含むノードの全体を T として、T の極小元を考える。
    - 結局、T または S における極小性に矛盾する。

証明の残り

- S の極小元である正規ノードの可能性を分析。
  - 特に、このノードと同じストランドにあって先行するノードが $\{B, N_A, N_B\}_{K_A}$ を含むことを示す。
    - このノードは仮定より N_B の起源ではない。(N_B は唯一の起源を持つので)
    - 先行するノードは S に含まれてはならないので、$\{B, N_A, N_B\}_{K_A}$ を含むはず。($\{B, N_A, N_B\}_{K_A}$ を含まないと S に入ってしまうので)


ボブ
$\{N_A, A\}_{K_B}$
$\{B, N_A, N_B\}_{K_A}$
$\{B, N_A, N_B\}_{K_A}$
$\ldots N_B \ldots$
$\{N_B\}_{K_B}$

イニシエータの唯一性

- さらに N_A の起源が唯一であると仮定すると、イニシエータのストランドの唯一性が成り立つ。

N_B の秘密性

- C は NSL ストランド空間のバンドルとする。
- s は C の中の A, B, N_A, N_B をパラメタとするレスポンダのストランドとする。
- $K_A^{-1} \notin \boldsymbol{K}_I\ ,\ K_B^{-1} \notin \boldsymbol{K}_I$
- $N_A \neq N_B$
- N_B は唯一の起源を持つ。
- 以上が成り立つとき、送受信されるメッセージで N_B を含むものは、$\{B, N_A, N_B\}_{K_A}$ もしくは $\{N_B\}_{K_B}$ に限られる。