数理的技法による
セキュリティプロトコルの検証

萩谷　昌己
東大情報理工 & NTT CS研

目次

- 背景
  - 計算論的アプローチ
  - 記号論的アプローチ
  - 融合の試み
- 記号論的アプローチの事例
- 計算論的な安全性
- 計算論的な安全性に対する数理的技法
  - 受動的な判別不能性
  - 能動的な攻撃
  - 汎用的結合可能性に向かって
  - その他

計算論的アプローチ

- 暗号の脆弱性を考慮。
  - IND-CPA
  - IND-CCA
- 確率的多項式時間チューリング機械
  - 攻撃者のモデル化
  - 現実的な解析
    - guessing attack
- 煩雑
  - 機械化も容易でない。
  - 多くの証明間違いの報告

記号論的アプローチ

- 完璧に安全な暗号を仮定。
  - Dolev-Yaoモデル
    - メッセージを項によって表現（メッセージ代数）
- 数理的技法の駆使
  - モデル化
    - 状態遷移系
    - プロセス計算（汎用・専用）
    - ストランド空間
  - 自動検証
    - モデル検査系
    - 専用の検証系

融合の試み

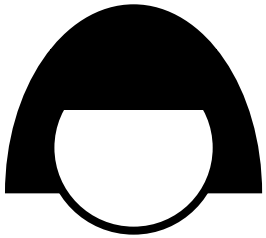
- 世界的な動向
  - IEEE Computer Security Foundations Workshop
  - Theory of Cryptography Conference
  - ICALP Track C
  - Formal and Computational Cryptography
- 直接的方法
  - 計算論的解析をそのまま形式化。
  - 自動検証
- 間接的方法
  - 記号論的推論に計算論的解釈を付与。
    「記号論的に正しければ計算論的に正しい。」

本発表
これまでの
記号論的
解析を
活用可能。

記号論的アプローチの事例

- Needham-Schroeder の非対称鍵による認証プロトコル（1978）の本質的部分（アリス・ボブ記法）

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



アリス

乱数・ノンス
（作った人しか知り得ない）

$\{A, N_A\}_{KB}$

$\{$アリス, アリスの秘密$\}_{$ボブの公開鍵$}$

このとき、アリスの秘密は、
アリスとボブしか知り得ない。

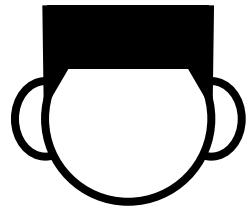
$\{N_A, N_B\}_{KA}$

$\{$アリスの秘密, ボブの秘密$\}_{$アリスの公開鍵$}$

アリスの秘密が帰って来たということは、
ボブが最初のメッセージを受信したはず。

$\{N_B\}_{KB}$

ボブ



$\{A, N_A\}_{KB}$

$\{$アリス, アリスの秘密$\}_{$ボブの公開鍵$}$

$\{N_A, N_B\}_{KA}$

$\{$アリスの秘密, ボブの秘密$\}_{$アリスの公開鍵$}$

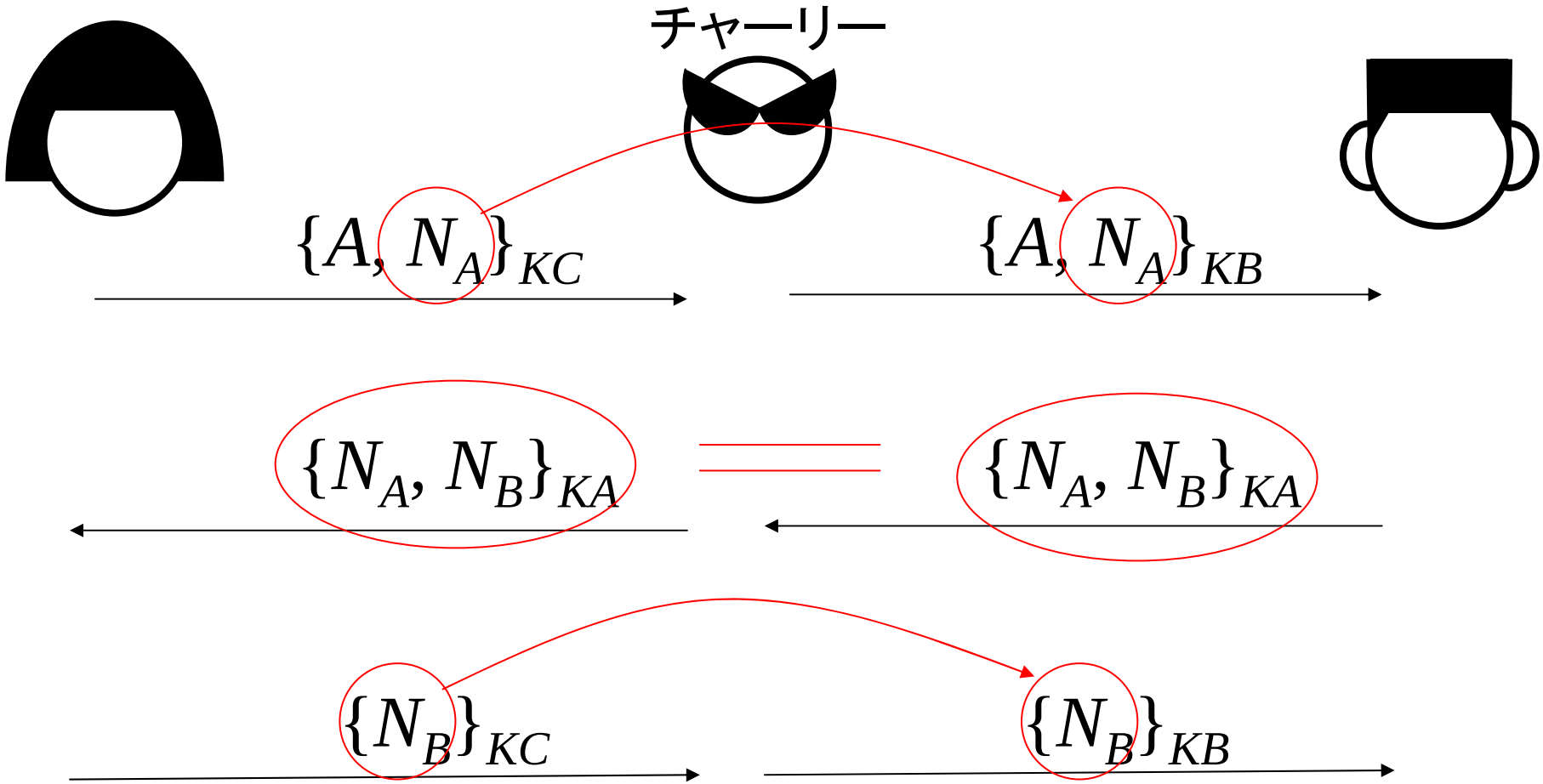
このとき、ボブの秘密は、
アリスとボブしか知り得ない？

$\{N_B\}_{KB}$

同様

Man-in-the-Middle攻撃

- Lowe が20年近くたってから発見（1995）
  - プロトコルの厳格なモデル化が一つの理由



修正されたプロトコル

- Needham-Schroeder-Lowe

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

ストランド空間とノンス解析

- 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
- ノンス解析
  - 萩谷他（2000）
  - ノンスの流れの解析
  - 前向き推論によるメッセージと状態の網羅
  - ノンス解析をストランドの解析の前処理として利用。

ノンス解析のためのフレームワーク

- (M, S) … システム全体の状態

  M … ネットワークを流れたメッセージの集合

  S … 主体と状態の組 $p{:}s$ の集合

- プロトコルのステップ … (M, S) の間の遷移

$$(M, S) \rightarrow (M \cup \{m'\}, (S - \{p{:}s\}) \cup \{p{:}s'\})$$

主体と状態の組 $p{:}s \in S$ を選び、
メッセージ $m \in M$ を受け取り、
必要なノンスを生成し、
メッセージ m' を送信し、
次状態 s' に遷移する。

Needham-Schroeder-Loweの場合

- メッセージ:

  $\{A, N_A\}_{KB}$

  $\{B, N_A, N_B\}_{KA}$

  $\{N_B\}_{KB}$

- 主体の状態:

  $s_0(B, N_A)$ ... $\{A, N_A\}_{KB}$ を送信した直後の A の状態

  $s_1(A, N_A, N_B)$ ... $\{B, N_A, N_B\}_{KA}$ を送信した直後の B の状態

  $s_2(B, N_A, N_B)$ ... $\{N_B\}_{KB}$ を送信した直後の A の状態

  $s_3(A, N_A, N_B)$ ... $\{N_B\}_{KB}$ を受信した B の状態

Lemma 1

このステップで作られたノンス

$(M, S) \rightarrow (M \cup \{\{B, N_A, N_B\}_{KA}\}, S \cup \{B{:}s_1(A, N_A, N_B)\})$

M_1 S_1

- もし $(M_1, S_1) \rightarrow_* (M', S')$ ならば、
  - もし $m \in M'$ かつ m が N_B を含むならば、
    - $m = \{B, N_A, N_B\}_{KA}$ または
    - $m = \{N_B\}_{KB}$.
  - もし $p{:}s \in S'$ かつ $p{:}s$ が N_B を含むならば、
    - $p{:}s = B{:}s_1(A, N_A, N_B)$ または
    - $p{:}s = A{:}s_2(B, N_A, N_B)$ または
    - $p{:}s = B{:}s_3(A, N_A, N_B)$.

Lemma 3

$(M, S) \rightarrow (M \cup \{\{B, N_A, N_B\}_{KA}\}, S \cup \{B{:}s_1(A, N_A, N_B)\})$

M_1 S_1

- もし $(M_1, S_1) \rightarrow_* (M', S')$ ならば、
  - もし $\{N_B\}_{KB} \in$ **closure**(M', S') ならば、
    - $\{N_B\}_{KB} \in M'$.
  - もし $\{B, N_A, N_B\}_{KA} \in$ **closure**(M', S') ならば、
    - $\{B, N_A, N_B\}_{KA} \in M'$.

攻撃者が作り出せるメッセージの集合

ストランド

- イニシエータ A のストランド

$$+\{A, N_A\}_{KB}$$

$$|$$

$$-\{B, N_A, N_B\}_{KA}$$

$$|$$

$$+\{N_B\}_{KB}$$

ストランド

- レスポンダ B のストランド

$$-\{A, N_A\}_{KB}$$

|

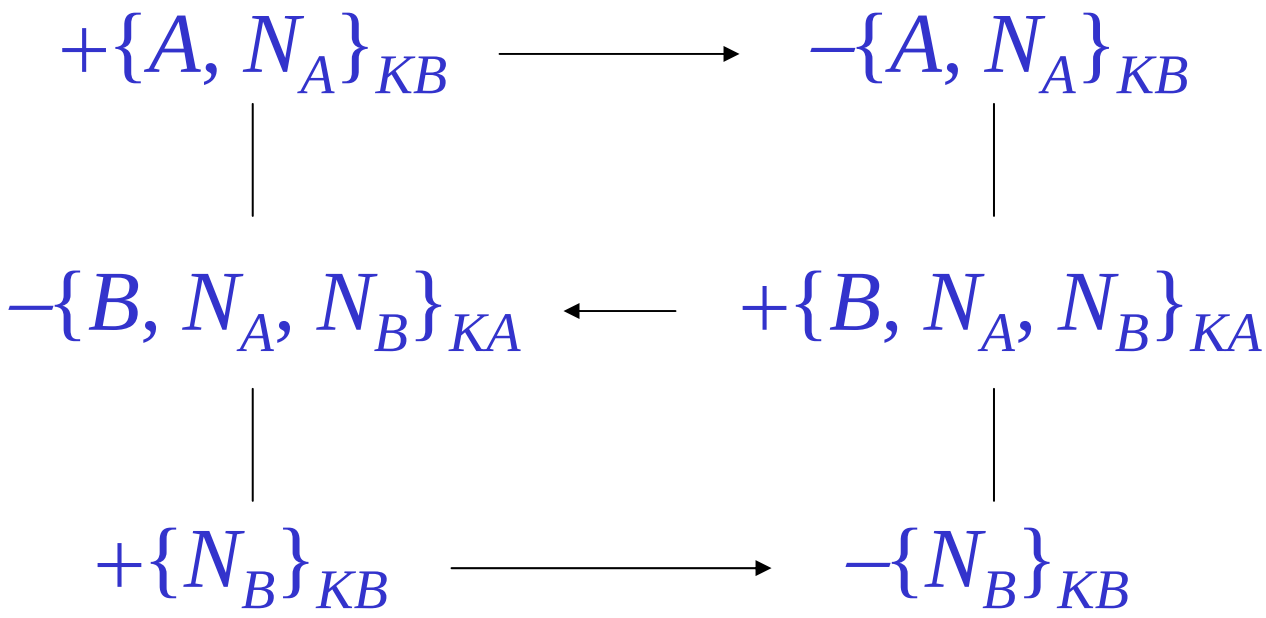
$$+\{B, N_A, N_B\}_{KA}$$

|

$$-\{N_B\}_{KB}$$

バンドル

- 因果関係について閉じたストランドの集合



ストランド空間モデル

- **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。

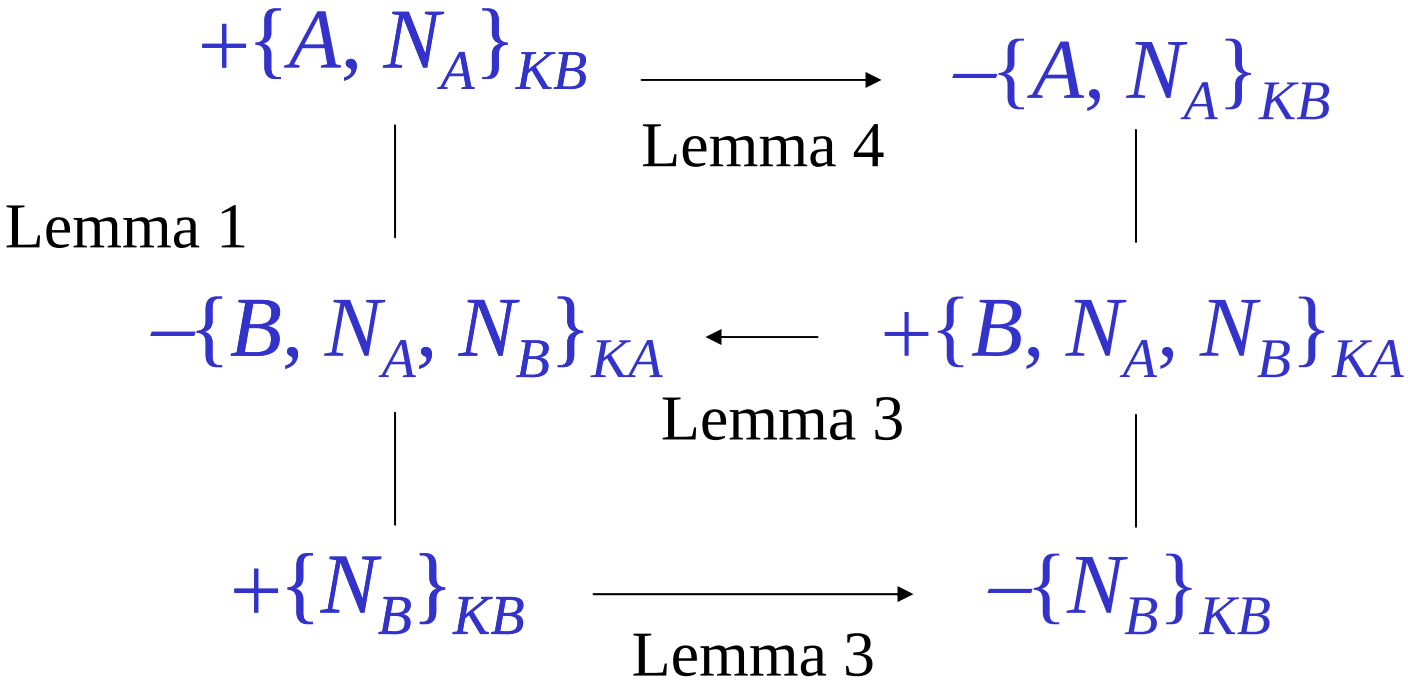
- 攻撃者のストランド

  攻撃者によるあらゆる攻撃を想定。

ここでは、攻撃者のストランドを考える代わりに、
ノンス解析の結果を活用。

ノンス解析とストランド空間モデル

- ノンス解析の結果をバンドルの構成に利用



計算論的な安全性

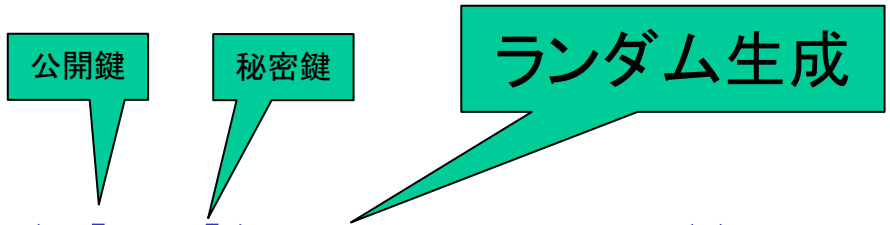
- ゲーム
- 汎用的結合可能性

ゲーム

- 例：非対称鍵
- チャレンジャ： $(pk, sk) \Leftarrow KeyGen(\ )$
- 攻撃者： $r \Leftarrow R,\ (m_0, m_1) \leftarrow A(r, pk)$
- チャレンジャ： $b \Leftarrow \{0, 1\},\ \psi \Leftarrow E(pk, m_b)$
- 攻撃者： $b' \leftarrow A(r, pk, \psi)$

$$\left| \Pr[b=b'] - 1/2 \right| : \text{negligible?}$$

- cf. IND-CPA



ElGamal Encryption

- プロトコル

  鍵生成: $x \Leftarrow \mathbf{Z}_q,\ \alpha \leftarrow \gamma^x,\ \ pk \leftarrow \alpha,\ sk \leftarrow x$

  暗号化: $y \Leftarrow \mathbf{Z}_q,\ \beta \leftarrow \gamma^y,\ \delta \leftarrow \alpha^y,\ \zeta \leftarrow \delta \cdot m,\ \psi \leftarrow (\beta, \zeta)$

  復号化: $m \leftarrow \zeta / \beta^x$

- ゲーム

  $x \Leftarrow \mathbf{Z}_q,\ \alpha \leftarrow \gamma^x$

  $r \Leftarrow R,\ (m_0, m_1) \leftarrow A(r, \alpha)$

  $b \Leftarrow \{0, 1\},\ y \Leftarrow \mathbf{Z}_q,\ \beta \leftarrow \gamma^y,\ \delta \leftarrow \alpha^y,\ \zeta \leftarrow \delta \cdot m_b$

  $b' \leftarrow A(r, \alpha, \beta, \zeta)$

ゲーム変換

- DDH-advantage

$$\left| \Pr[D(\gamma^x,\ \gamma^y,\ \gamma^{xy}) \mid x, y \Leftarrow \mathbf{Z}_q] - \Pr[D(\gamma^x,\ \gamma^y,\ \gamma^z) \mid x, y, z \Leftarrow \mathbf{Z}_q] \right|$$

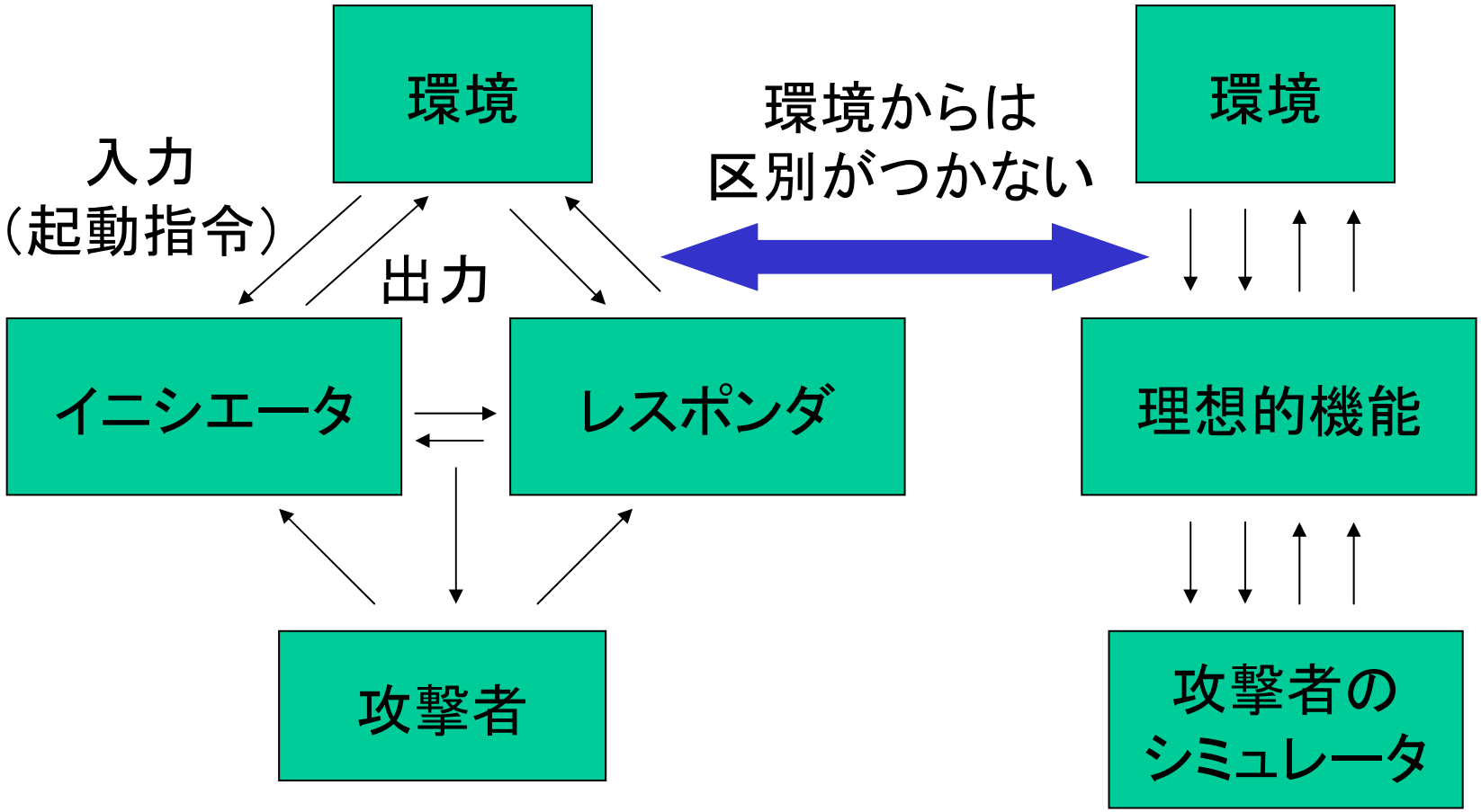
（D : 多項式時間述語）

- ElGamal Encryption ゲームの成功確率を DDH-advantage に変換。
- Blanchet-Pointcheval（2006）
  - プロセス計算の中でゲーム変換を形式化。

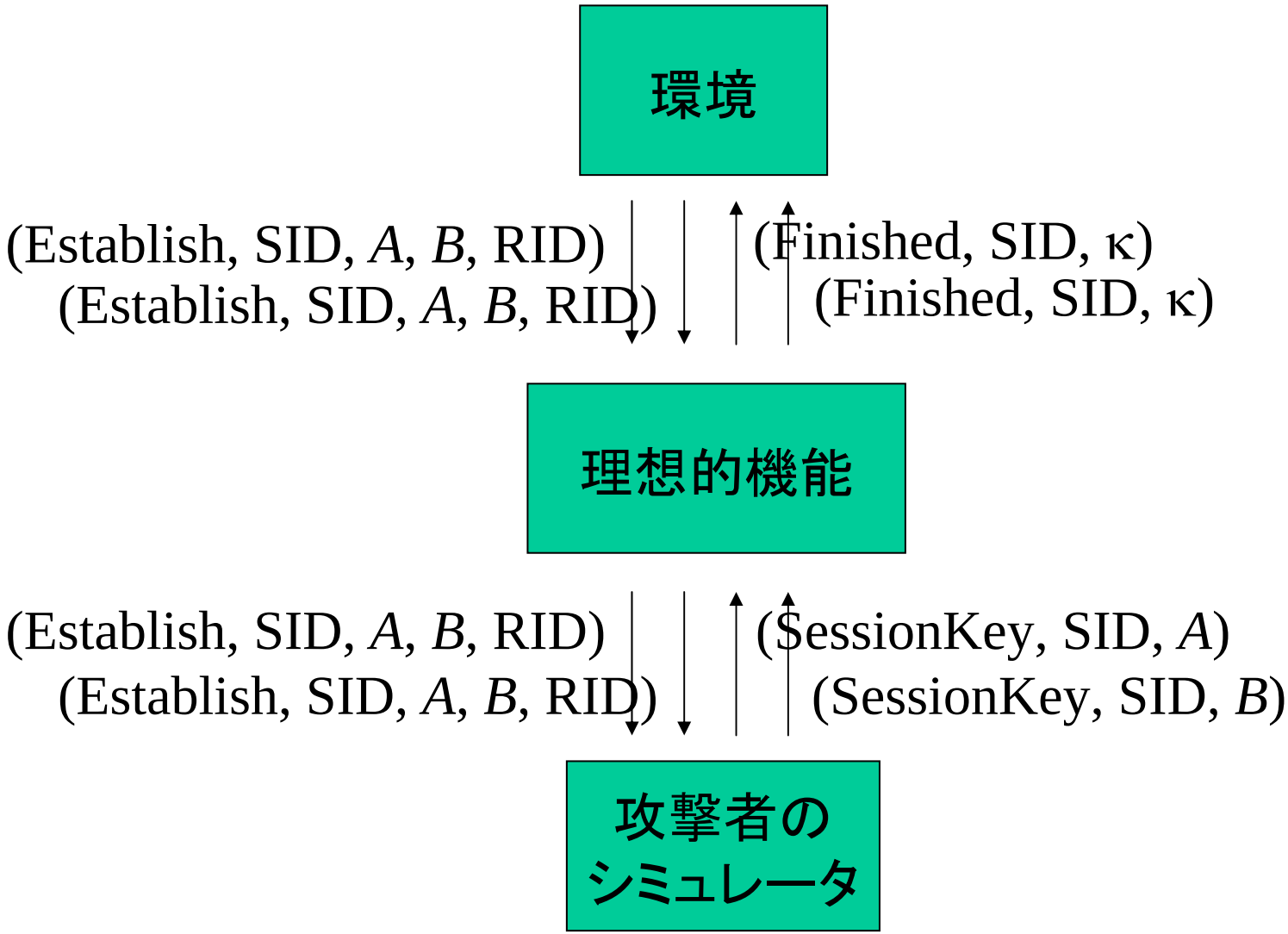
汎用的結合可能性

- 鍵交換プロトコルの場合

任意の攻撃者に対して
そのシミュレータが存在して、



鍵交換の理想的機能


環境
(Establish, SID, A, B, RID)
(Establish, SID, A, B, RID)
(Finished, SID, κ)
(Finished, SID, κ)
理想的機能
(Establish, SID, A, B, RID)
(Establish, SID, A, B, RID)
(SessionKey, SID, A)
(SessionKey, SID, B)
攻撃者の
シミュレータ

入力と出力の追加

- Needham-Schroeder-Lowe
  （鍵交換プロトコルとして）

A and B receive (Establish, SID, A, B, RID)

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

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

A outputs (Finished, SID, N_A)

$A \rightarrow B : \{N_B\}_{KB}$

B outputs (Finished, SID, N_A)

計算論的な安全性に対する数理的技法

- 受動的な判別可能性
- 能動的な攻撃
- 汎用的結合可能性に向かって
- その他

受動的な判別可能性

- Abadi-Rogaway（2000, 2002）
  - 間接的方法のパイオニア
  - 対称鍵
- Dolev-Yaoモデルに基づいて、
  メッセージを表す項の間の等価性を定義。

$$(K_1, (\{m_1\}_{K_1}, \{m_2\}_{K_2}))$$
$$\approx (K_1, (\{m_1\}_{K_1}, \{m_3\}_{K_2}))$$
$$\not\approx (K_1, (\{m_4\}_{K_1}, \{m_3\}_{K_2}))$$

見えない部分は等価

等価⇒判別不能

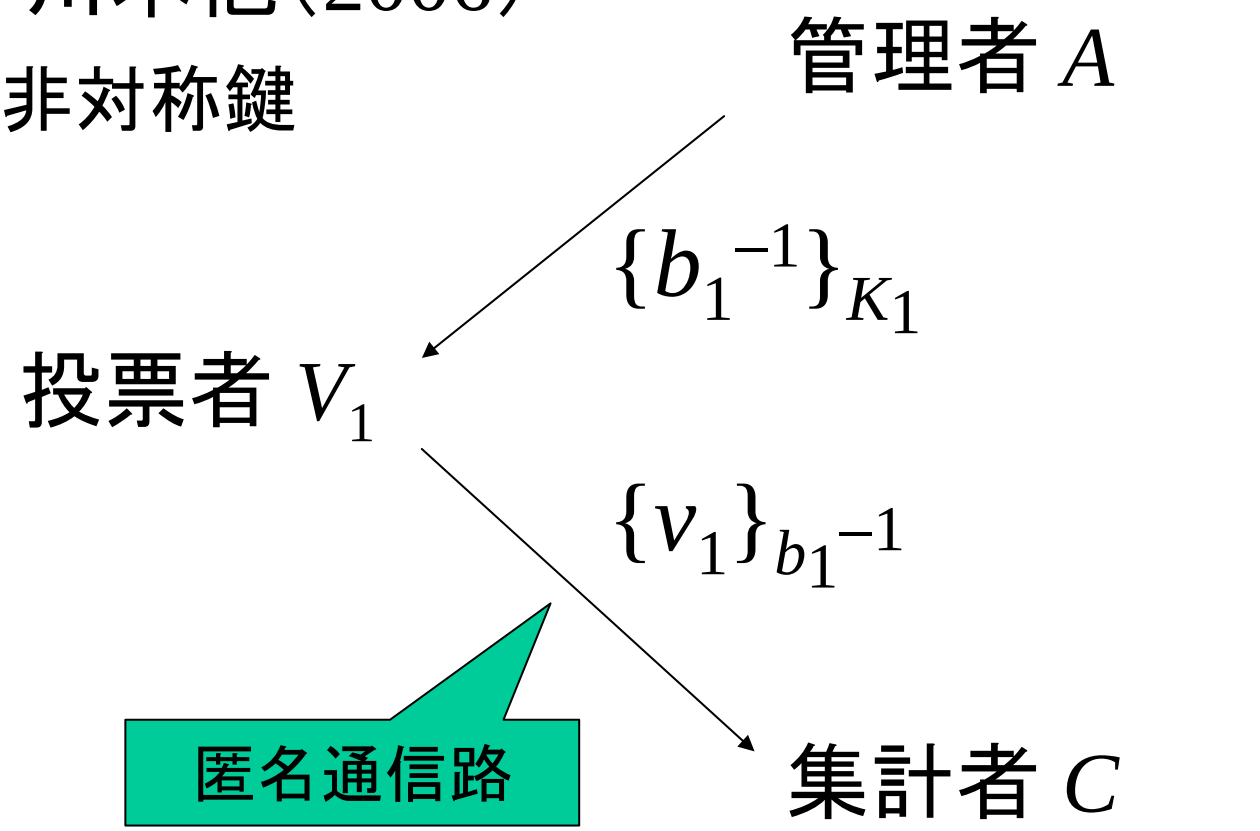
- $m_1 \approx m_2$ ならば、
  任意の確率多項式時間述語 D に対して、

$$\left| \Pr[D(x) \mid x \in [[m_1]]_\eta] - \Pr[D(x) \mid x \in [[m_2]]_\eta] \right|$$

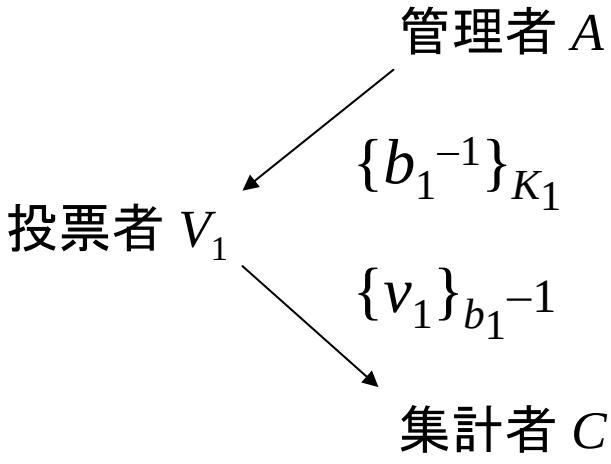
  は security parameter η に関して negligible
- 根底にある暗号の type-0 安全性に帰着。
  – ゲーム変換

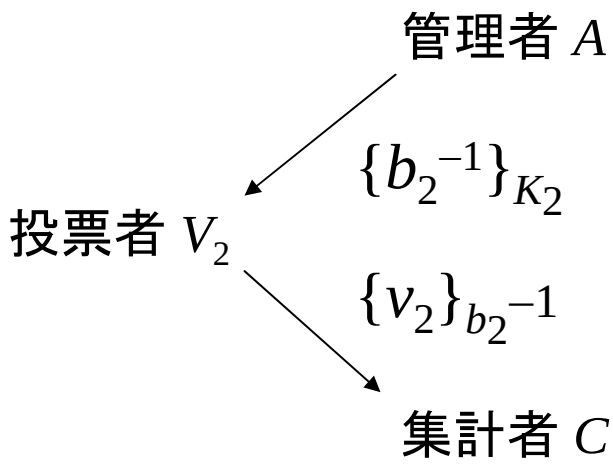
簡単な選挙プロトコル

- cf. 川本他(2006)
  - 非対称鍵

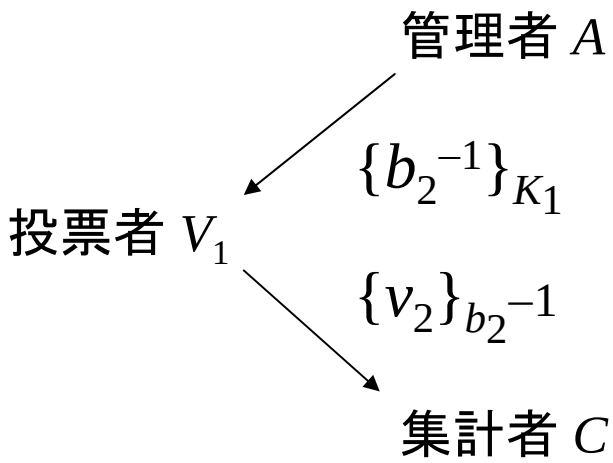


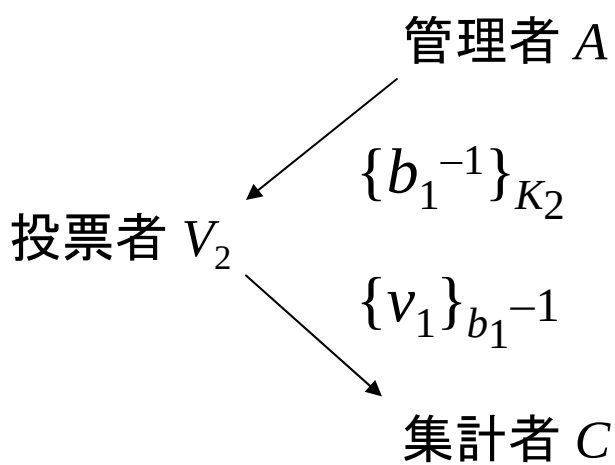
観測: $\{(V_1, \{b_1^{-1}\}_{K_1}), \{v_1\}_{b_1^{-1}}\}$





$$\{(V_1, \{b_1^{-1}\}_{K_1}), \{v_1\}_{b_1^{-1}}, (V_2, \{b_2^{-1}\}_{K_2}), \{v_2\}_{b_2^{-1}}\}$$





等価

$$\{V_1, \{b_2^{-1}\}_{K_1}), \{v_2\}_{b_2^{-1}}, ((V_2, \{b_1^{-1}\}_{K_2}), \{v_1\}_{b_1^{-1}}\}$$

能動的な攻撃

- Micciancio-Warinschi（2004）
- 例：Needham-Schroeder-Lowe
- 相互認証性（mutual authentication）

  イニシエータにおいても

  レスポンダにおいても **agreement** が成立。
- 記号論的に相互認証性が成り立つならば、計算論的にも相互認証性が成り立つ。
  - 相互認証性が成り立たない確率は negligible
  - 能動的な攻撃も含まれる。

Mapping Lemma

- negligible な確率を除いて、
  計算論的なトレース（実行過程）には、
  記号論的なトレースが対応する。
  - 記号論的なトレースに対応しないような
    計算論的なトレースの確率は negligible
  - 例えば guessing attack が成功する可能性は
    negligible
- IND-CCA2 を仮定。
  - 非対称鍵

汎用的結合可能性に向かって

- Canetti-Herzog（2006）
- 相互認証性と real-or-random secrecy から鍵交換の汎用的結合可能性が導かれる。
  - Mapping Lemma が本質的。
  - real-or-random secrecy が成り立たないと Rackoff 攻撃が可能。
  - NSL では N_B を返す場合
- real-or-random secrecy

  出力される鍵をランダムなものに置き換えても、攻撃者の攻撃パターンは影響を受けない。

個人的な意見だが...

- Mapping Lemma により、
  鍵交換プロトコルの正当性が導かれている。
- わざわざ汎用的結合可能性を示す必要は
  あるのか？
- Mapping Lemma の結合可能性が
  成り立てばよいのではないか？
- その条件は？

その他

- プロセス計算
  - 計算論的な解釈
  - ゲーム変換の形式化（直接的方法）
- 論理体系
  - 様相論理
  - 秘匿性・相互認証性などを推論規則を用いて導出。
  - 計算論的な解釈
- BPWモデル
  - 記号論的なライブラリと計算論的なライブラリを扱える統一的な意味モデル