汎用的結合可能性(UC)について

岡本龍明
NTT

暗号とは

- 基本機能
  - 秘匿（暗号、鍵配送）
  - 認証（署名）
- 複合（応用）機能
  - 電子投票
  - 電子決済
  - 電子契約
  - 電子ゲーム

総　称 → 暗号プロトコル

理論的に一般化 → マルチパーティプロトコル

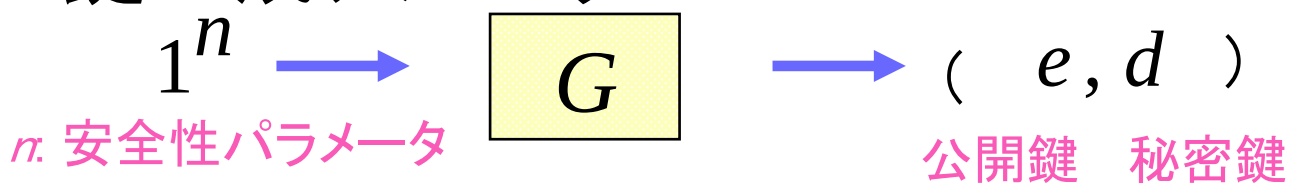
これら各種暗号機能に対してその安全性がいかに定式化されてきたか？

従来は、アドホックに定式化されてきた.

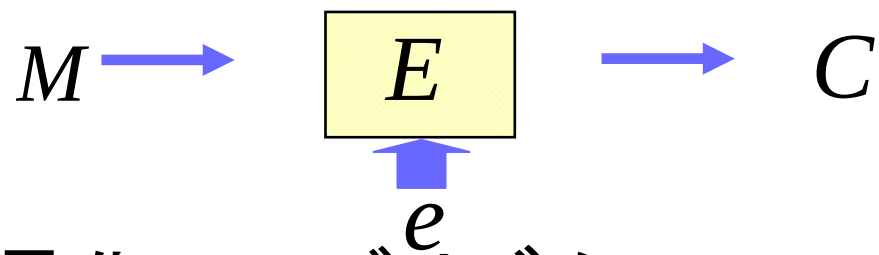
- それぞれの暗号機能の安全性は、個別に定式化.
- それらはしばしば不適切に定式化されたり、最終的に満足のいく定式化に至るまでに非常に時間がかる場合があった。
- 従来、これら各種安全性の定式化を統一的に扱う手法はなかった。

公開鍵暗号(G, E, D)

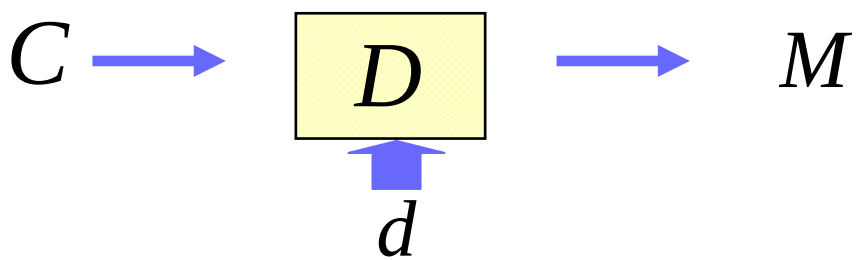
- G: 鍵生成アルゴリズム



- E: 暗号化アルゴリズム



- D: 復号化アルゴリズム



公開鍵暗号の安全性

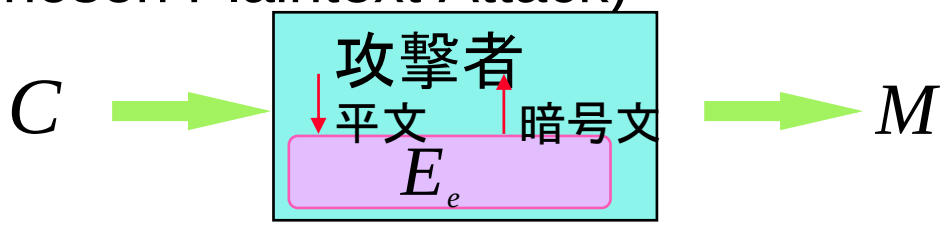
- 達成度
  - 秘匿性
    - 一方向性（OW） $c=E_{pk}(m) \xrightarrow{\text{困難}} m$
    - 強秘匿性（IND） $c=E_{pk}(m)$ より m のいかなる部分情報も解読困難
  - 頑強性（NM） ・・・ $c=E_{pk}(m) \xrightarrow{\text{困難}} c'=E_{pk}(m')$

    ある関係 R に関して $R(m, m')$
- 攻撃法
  - 受動的攻撃・・・選択平文攻撃（CPA）
  - 能動的攻撃・・・選択暗号攻撃（CCA）

安全性の各種定義(攻撃法に関して)

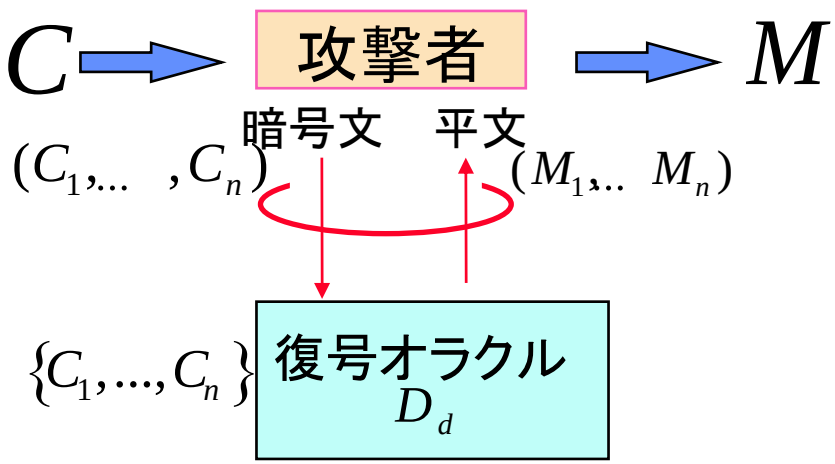
- 暗号文攻撃(選択平文攻撃)

  (CPA：Chosen Plaintext Attack)



- 選択暗号文攻撃

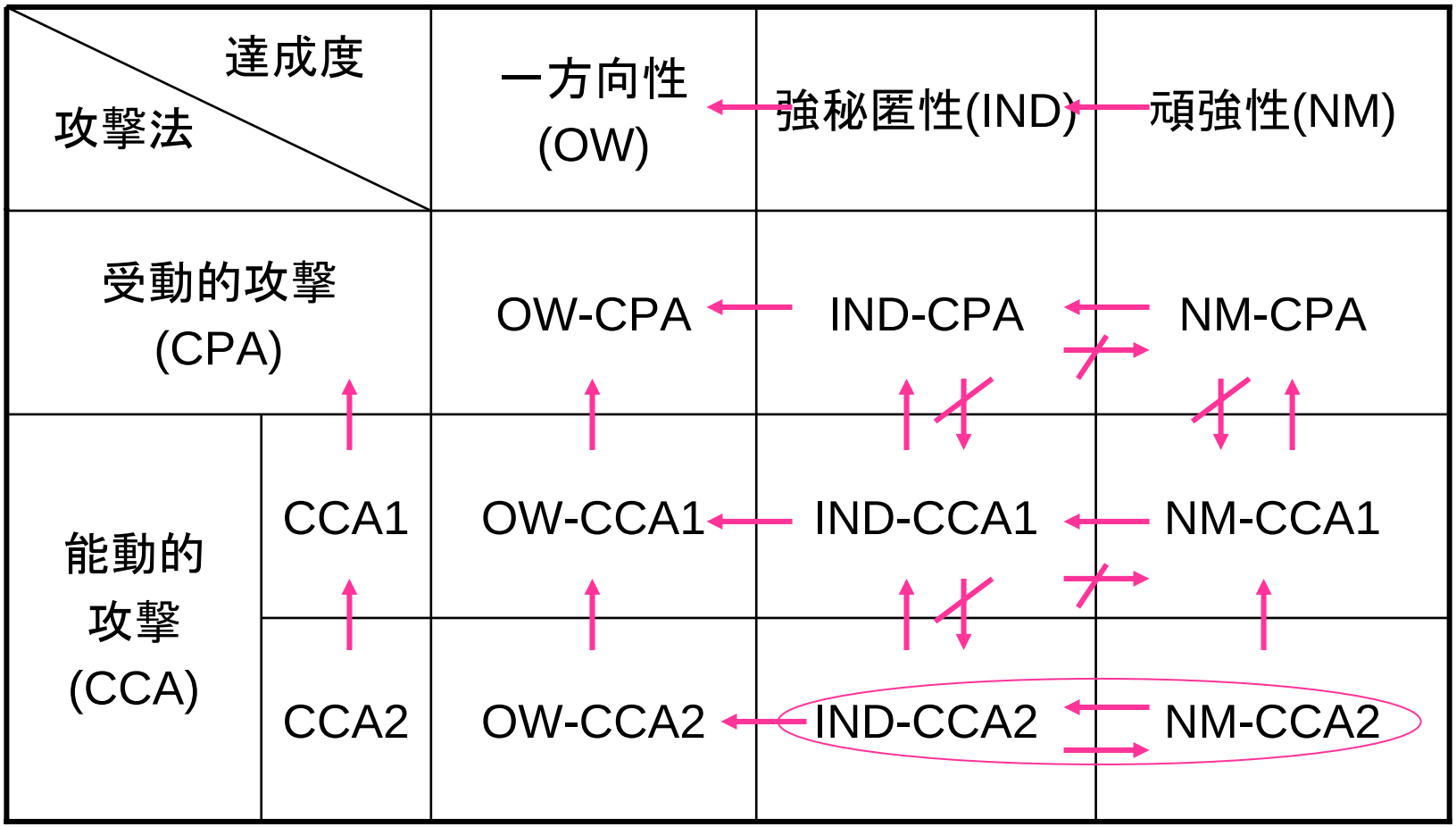
  （CCA：Chosen Ciphertext Attack)



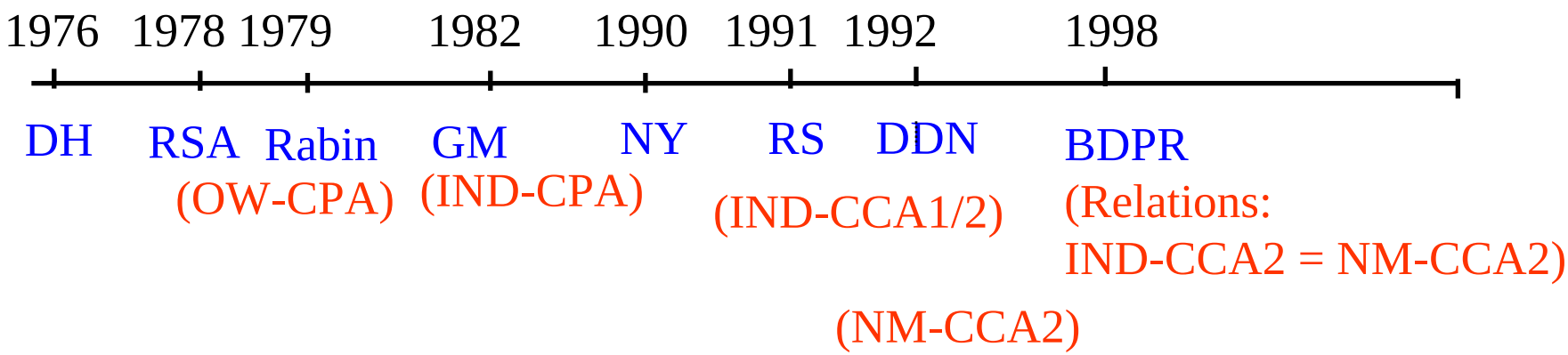
（但し, $C \notin \{C_1,\ldots,C_n\}$

CCA1・・Cを受け取る前にCCAを行う。
CCA2・・Cを受け取った後にCCAを行う。
（CCA2はCCA1より強力な攻撃法）

安全性定義間の関係

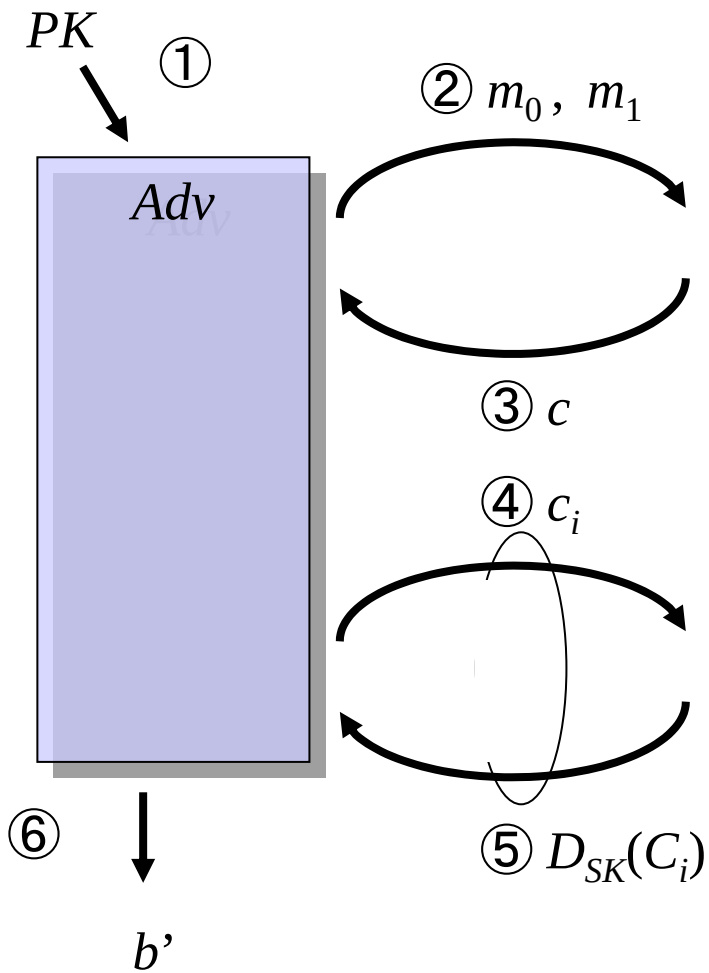

達成度
攻撃法
一方向性
(OW)
強秘匿性(IND)
頑強性(NM)
受動的攻撃
(CPA)
OW-CPA
IND-CPA
NM-CPA
能動的
攻撃
(CCA)
CCA1
OW-CCA1
IND-CCA1
NM-CCA1
CCA2
OW-CCA2
IND-CCA2
NM-CCA2

公開鍵暗号の安全性の定式化の歴史



公開鍵暗号の安全性(IND-CCA2)

[Rackoff-Simon'91, Dolev-Dwork-Naor'91,…]



EO(暗号オラクル)
(*PK*)

$b \in_R \{0,1\}$

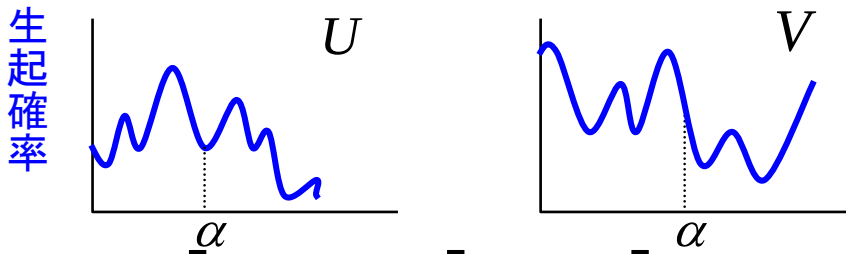
$c = E_{PK}(m_b)$

DO(復号オラクル)
(*SK*)

$$\Pr[b = b'] < \frac{1}{2} + \mu(n)$$

確率変数の識別不可能性 (Indistinguishability)

U, V：確率変数



- **完全識別不可能**

  $U = V$

  つまりすべての α に対して $\Pr[U \to \alpha] = \Pr[V \to \alpha]$

- **統計的識別不可能**

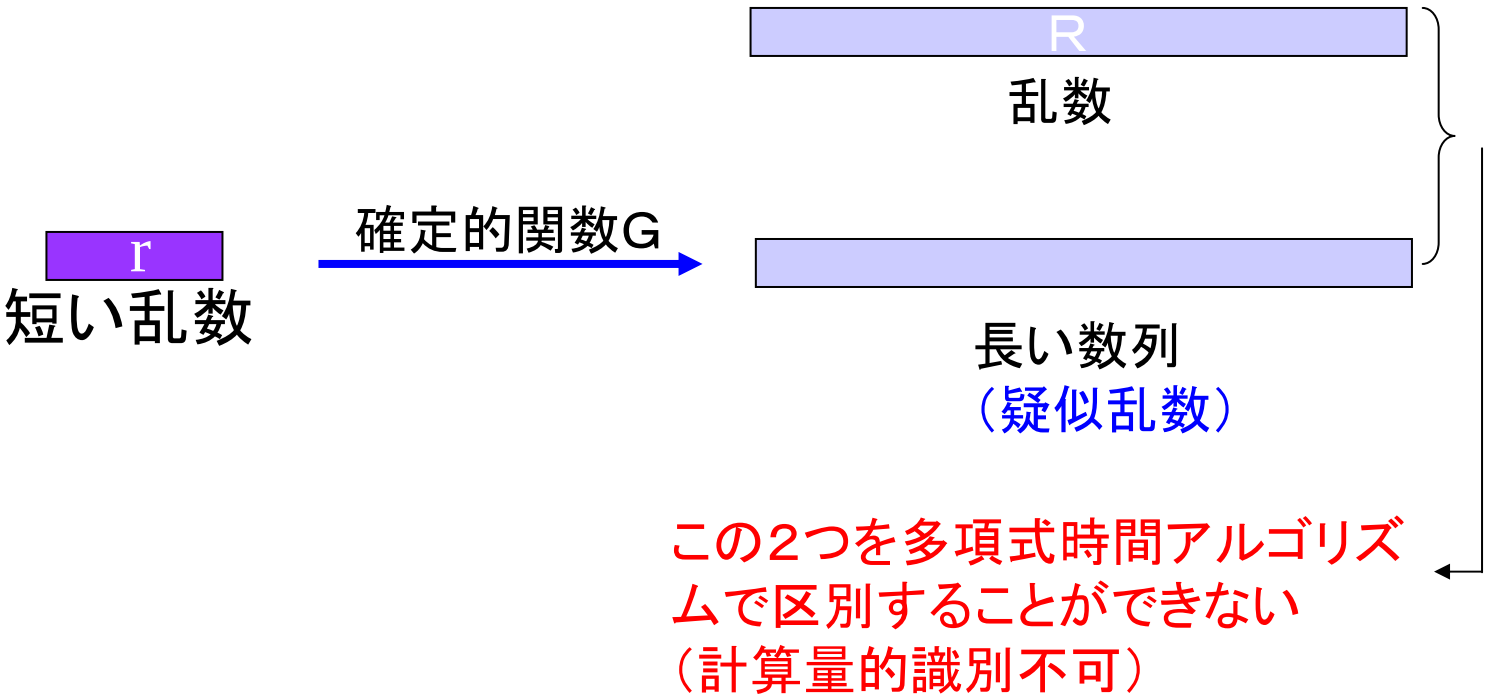
$$\sum_{\alpha \in \{0,1\}^*} \left| \Pr[U \to \alpha] - \Pr[V \to \alpha] \right| < \varepsilon$$

- **計算量的識別不可能 (Yao'82)**

  どのような多項式時間識別器 D に対しても

$$\left| \Pr[D(U) = 1] - \Pr[D[V] = 1] \right| < \varepsilon$$

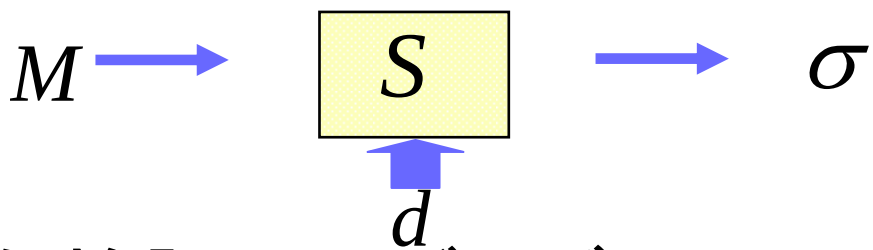
疑似乱数 (BM'82, Yao'82)



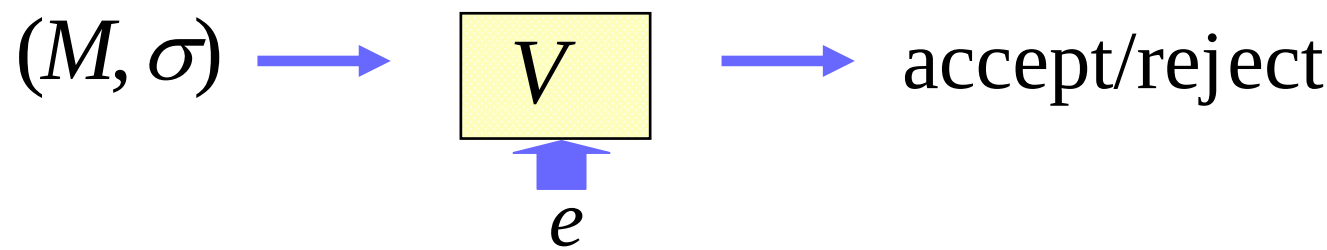
ディジタル署名 (G, S, V)

- G: 鍵生成アルゴリズム

- S: 署名生成アルゴリズム

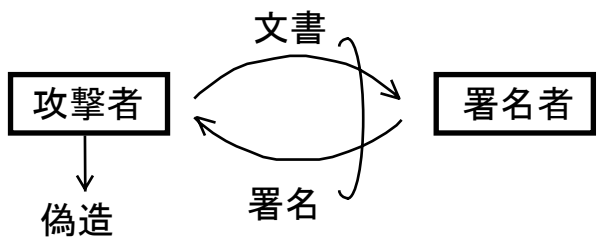


- V: 署名検証アルゴリズム



デジタル署名の安全性

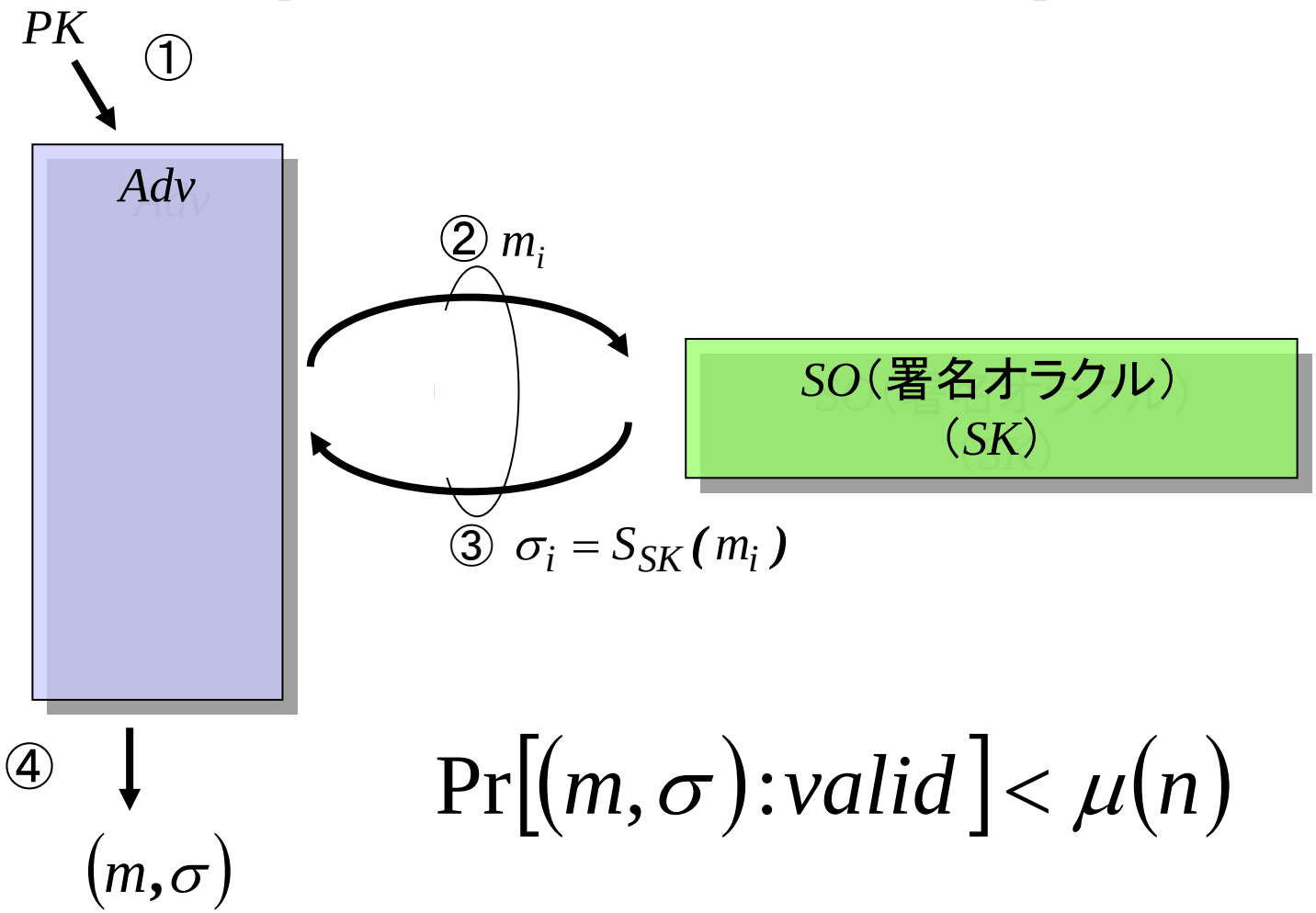
- 偽造困難性
  - 一般的偽造不可(ある文書に対して、署名偽造不可)
  - 選択的偽造不可
  - 存在的偽造不可(いかなる文書-署名対も偽造不可)
- 攻撃法
  - 受動的攻撃
  - 一般選択文書攻撃
  - 適応的選択文書攻撃



安全な署名とは・・・適応的選択文書攻撃の下で存在的偽造不可

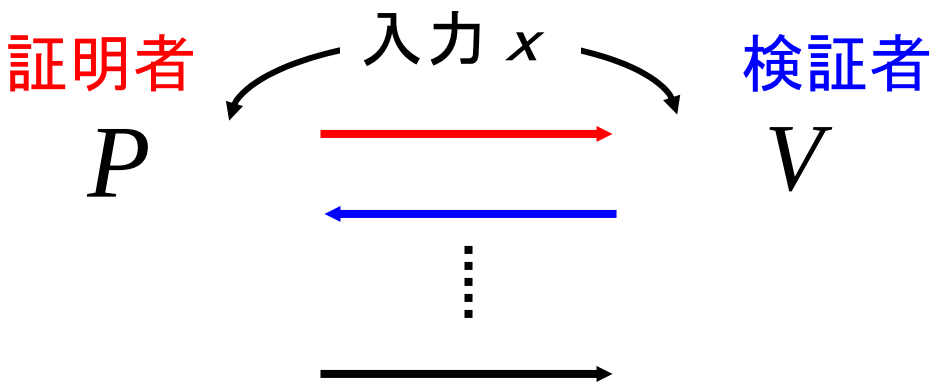
ディジタル署名の安全性(EUF-CMA)

[Goldwasser-Micali-Rivest'88]



$$\Pr[(m,\sigma):valid] < \mu(n)$$

ゼロ知識証明(GMR'85)



$View_V(x)$: V が見ることの出来るすべての情報

(P,V) が(完全に/統計的に/計算量的に)ゼロ知識 .....

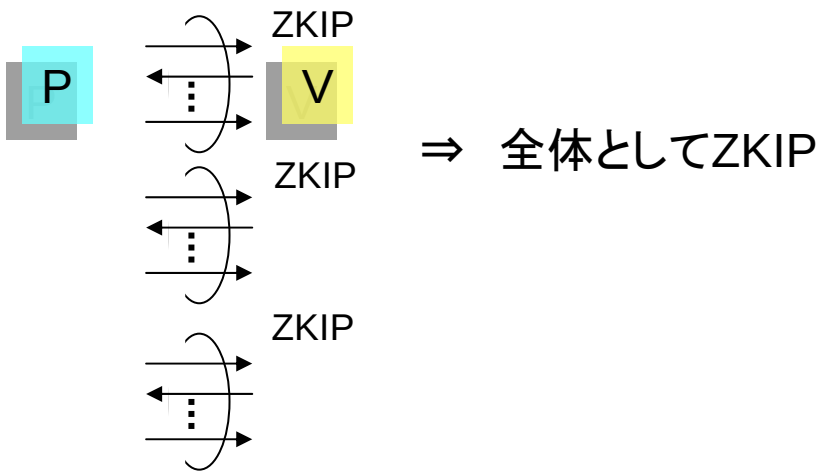
どのような x 、どのような V に対しても、シュミレータ(多項式時間アルゴリズム)M_Vが存在して

$$M_V(x) \approx View_V(x)$$

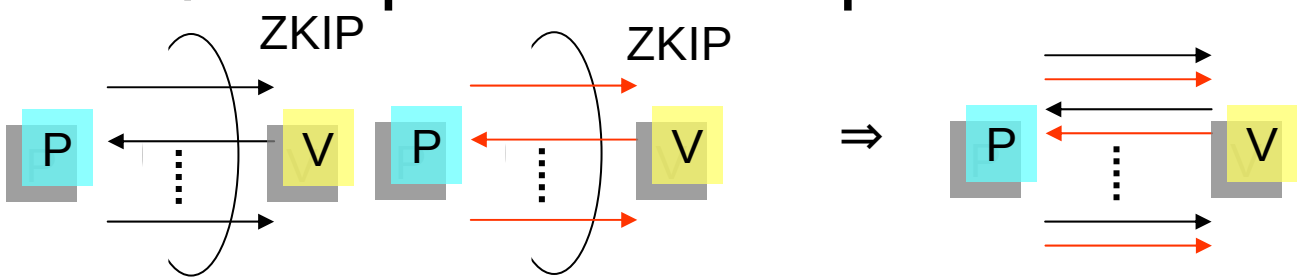
(完全/統計的/計算量的)識別不可

ゼロ知識証明の結合

- 逐次的結合（sequential composition）



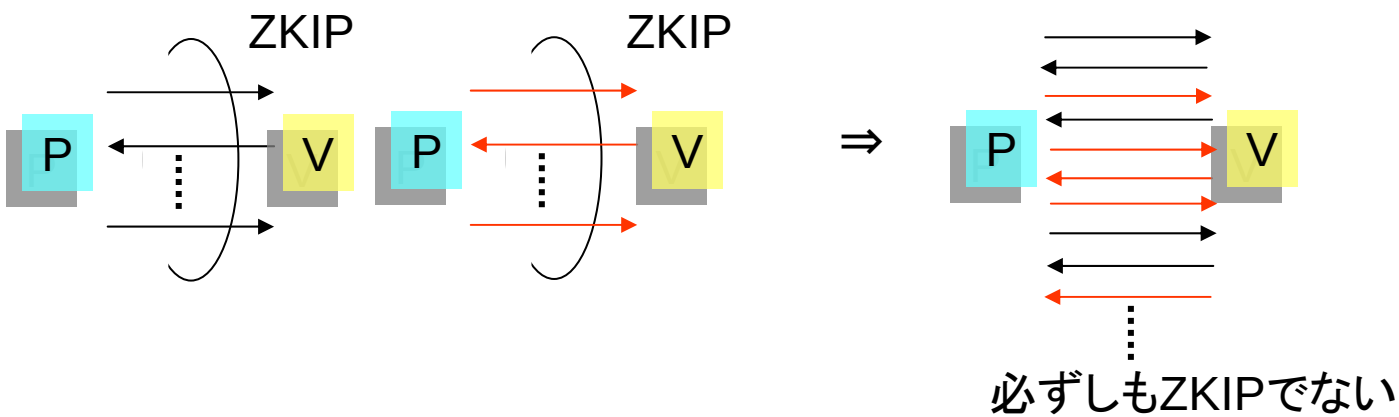
- 並列的結合（parallel composition）



必ずしもZKIPでない

Concurrent ZKIP

- 非同期並列結合（最も一般的な結合）

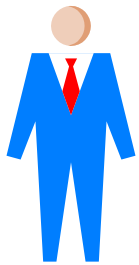


⇒ どのような種類のZKIPがconcurrent結合で閉じているか？
（従来のZKIPの定義では、閉じていない）

⇒ より強い安全性を保証する新しいZKIPの定義が必要

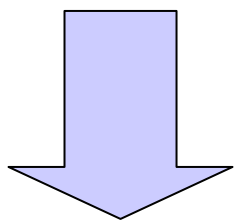
マルチパーティプロトコル（１）

参加者２
(x_2)



参加者１
(x_1)

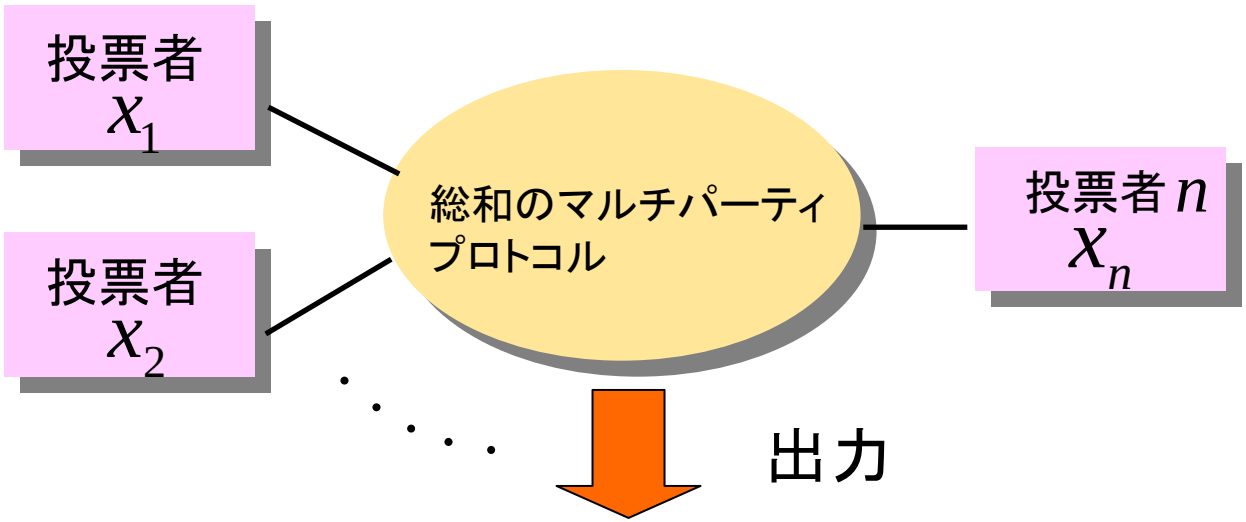
参加者n
(x_n)



$f(x_1,\ldots,x_n)$

$x_1, x_2,\ldots, x_n$は秘密にしたまま
与えられた関数 f に対して
$f(x_1,\ldots,x_n)$を計算する

マルチパーティプロトコル（2）

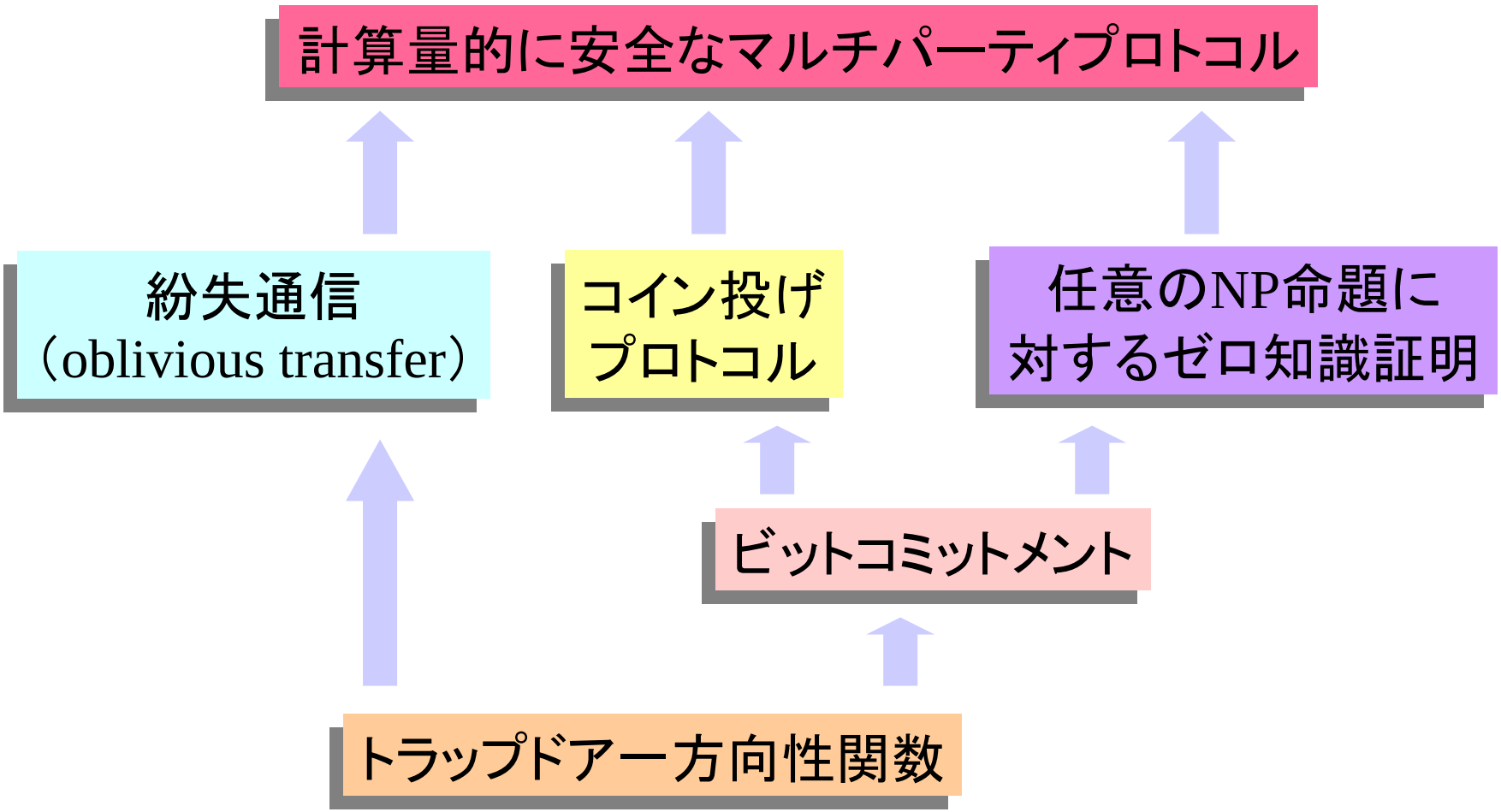


$$f(x_1, x_2, \cdots, x_n) = x_1 + x_2 + \cdots + x_n$$

投票内容： $x_i \in \{0, 1\}$

反対　賛成

計算量的に安全な
マルチパーティプロトコル（1）



計算量的に安全なマルチパーティプロトコル(2)

- 完全性定理

  (Goldreich-Micali-Wigderson 1987)

  - トラップドア一方向性関数(公開鍵暗号)が存在すると仮定

  ➡ 任意の関数 f に対して、任意の数 $t < n$ の不正者がいても計算量的に安全なマルチパーティプロトコルが実現可

  しかし、モデルは限定的(同期通信 、非適応的攻撃、非結合的 etc.)

汎用的結合可能性:
Universal Composability （UC)

汎用的結合可能性：Universal Composability (UC)

- 2001年にRan Canetti により提唱された新しいパラダイム。それ以降、Canetti 他多くの研究者により急速に進展している。
- 従来定式化されてきたいずれの安全性概念よりも強い安全性を保証。つまり、単体として保証された安全が、どのような結合／利用環境でも保持される。
- 全ての暗号機能（公開鍵暗号、署名、ビットコミット、ゼロ知識証明、マルチパーティプロトコルなど）の安全性を統一的に定式化するフレームワークを提供する。
- UC は、いまでの暗号安全性理論を集大成／統合したものであり、これからの暗号理論の基盤となる体系である。

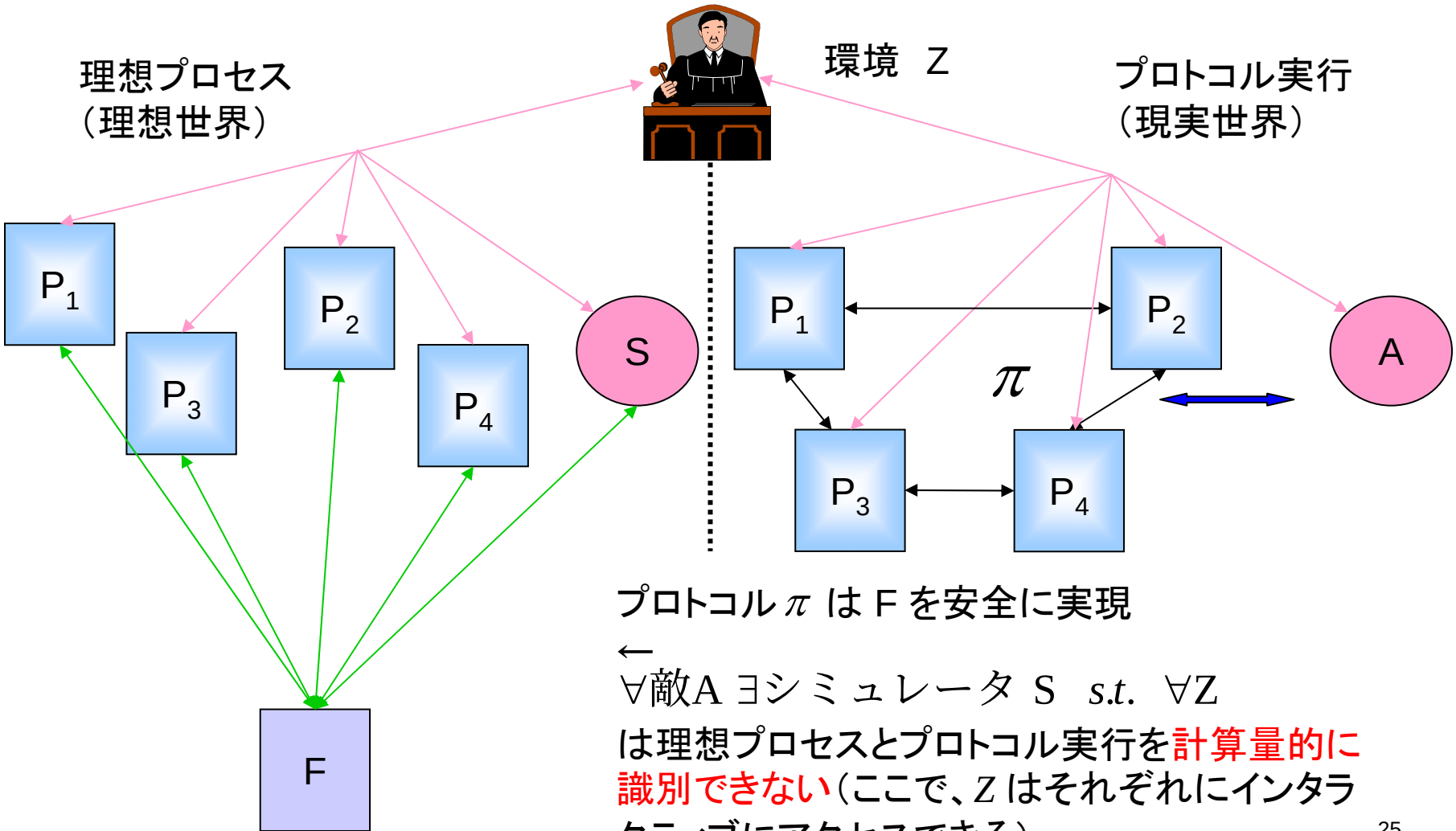
いかに安全性を定義するか（1）

実現したい理想機能 (functionality) F を記述

F は理想的な信頼できるサービスの記述

F は、正当性（correctness）と 秘匿性（secrecy）の両条件を同時にとらえる

いかに安全性を定義するか(2)



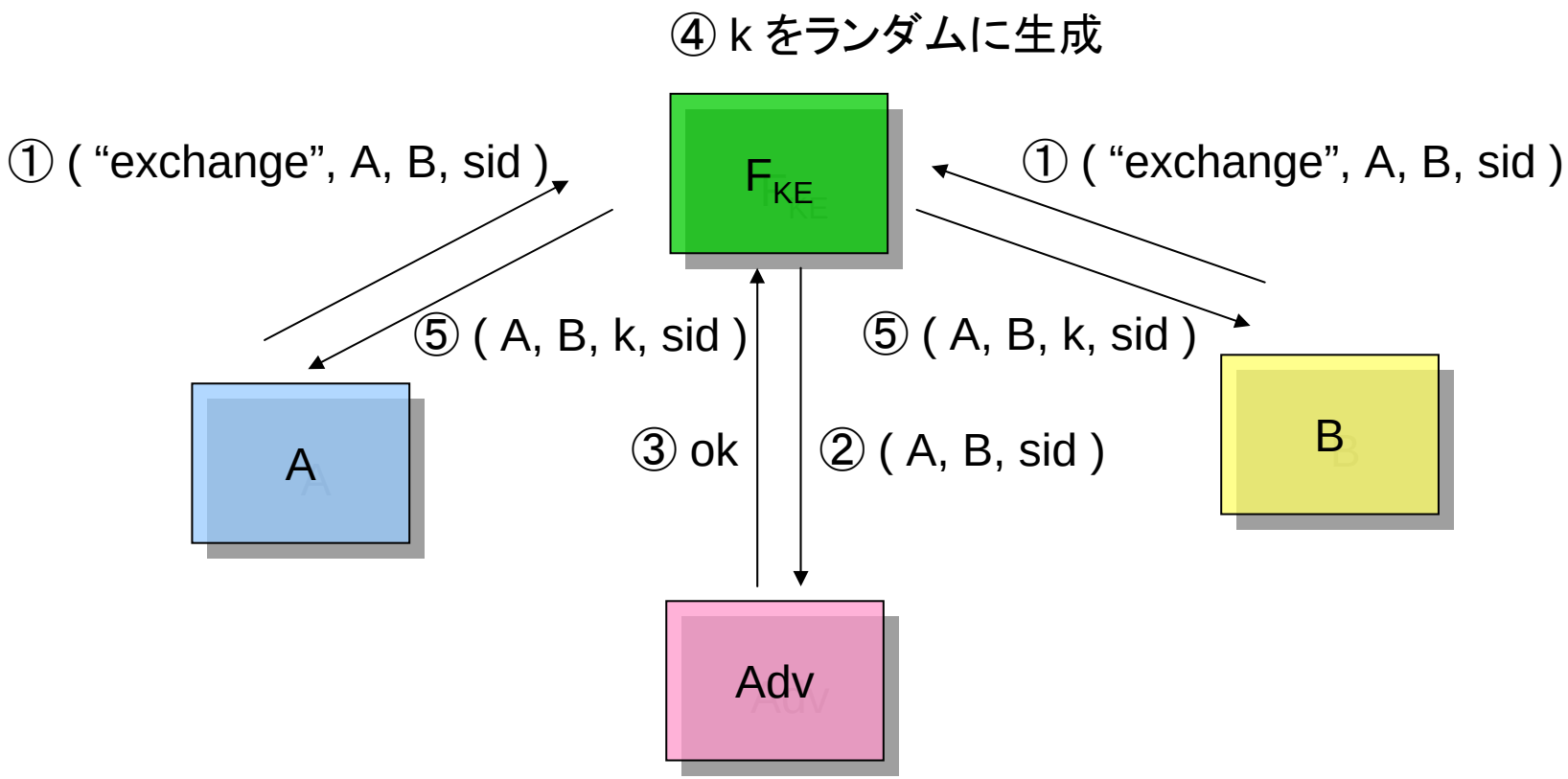
プロトコル π は F を安全に実現

←

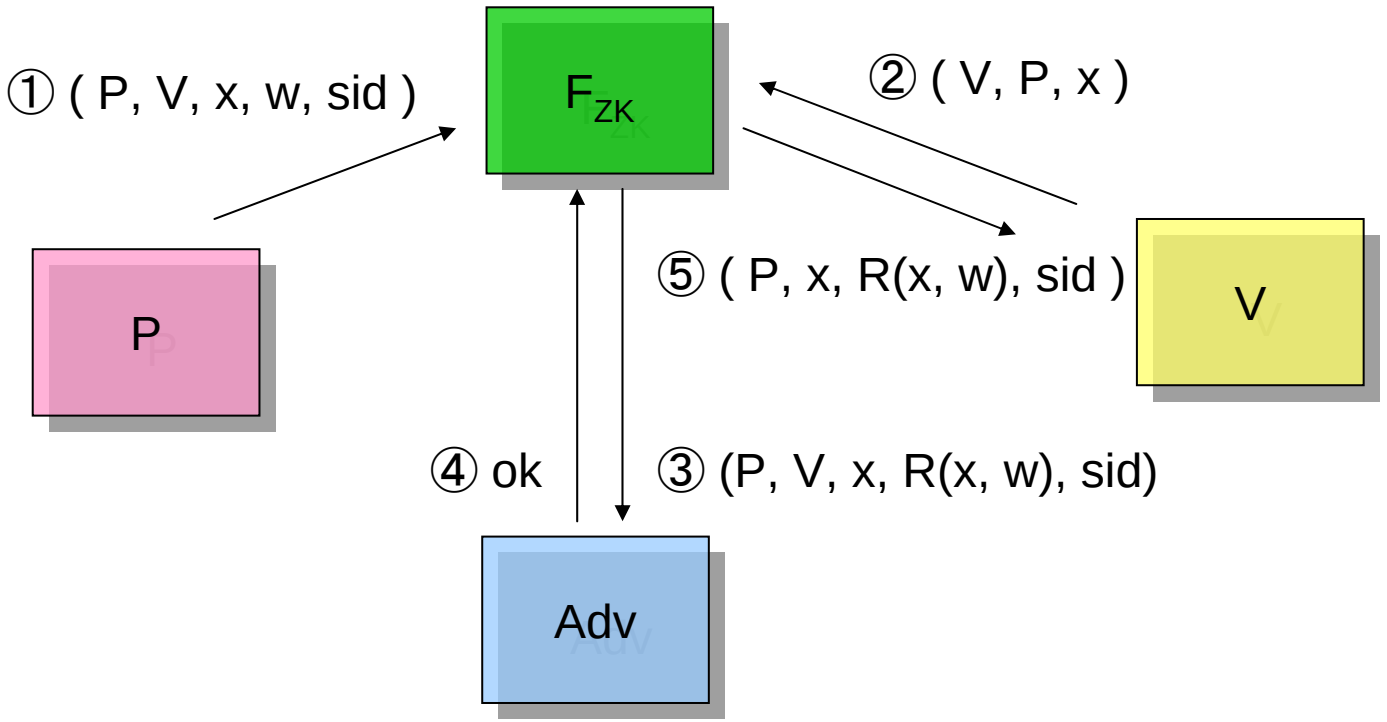
$\forall$敵A $\exists$シミュレータ S *s.t.* $\forall$Z

は理想プロセスとプロトコル実行を計算量的に識別できない(ここで、Z はそれぞれにインタラクティブにアクセスできる)

例：機能F_{KE}：鍵交換


④ k をランダムに生成
① (“exchange”, A, B, sid)
F_{KE}
① (“exchange”, A, B, sid)
⑤ (A, B, k, sid)
⑤ (A, B, k, sid)
A
③ ok
② (A, B, sid)
B
Adv

例：機能F_{ZK}：ゼロ知識証明（関係Rに対して）



注：●V は x を受理 ⇔ R(x, w)＝1（完全性/健全性）
●V は R(x, w) 以外の情報を得ない（ゼロ知識性）

汎用的結合可能性（Universal Composability）

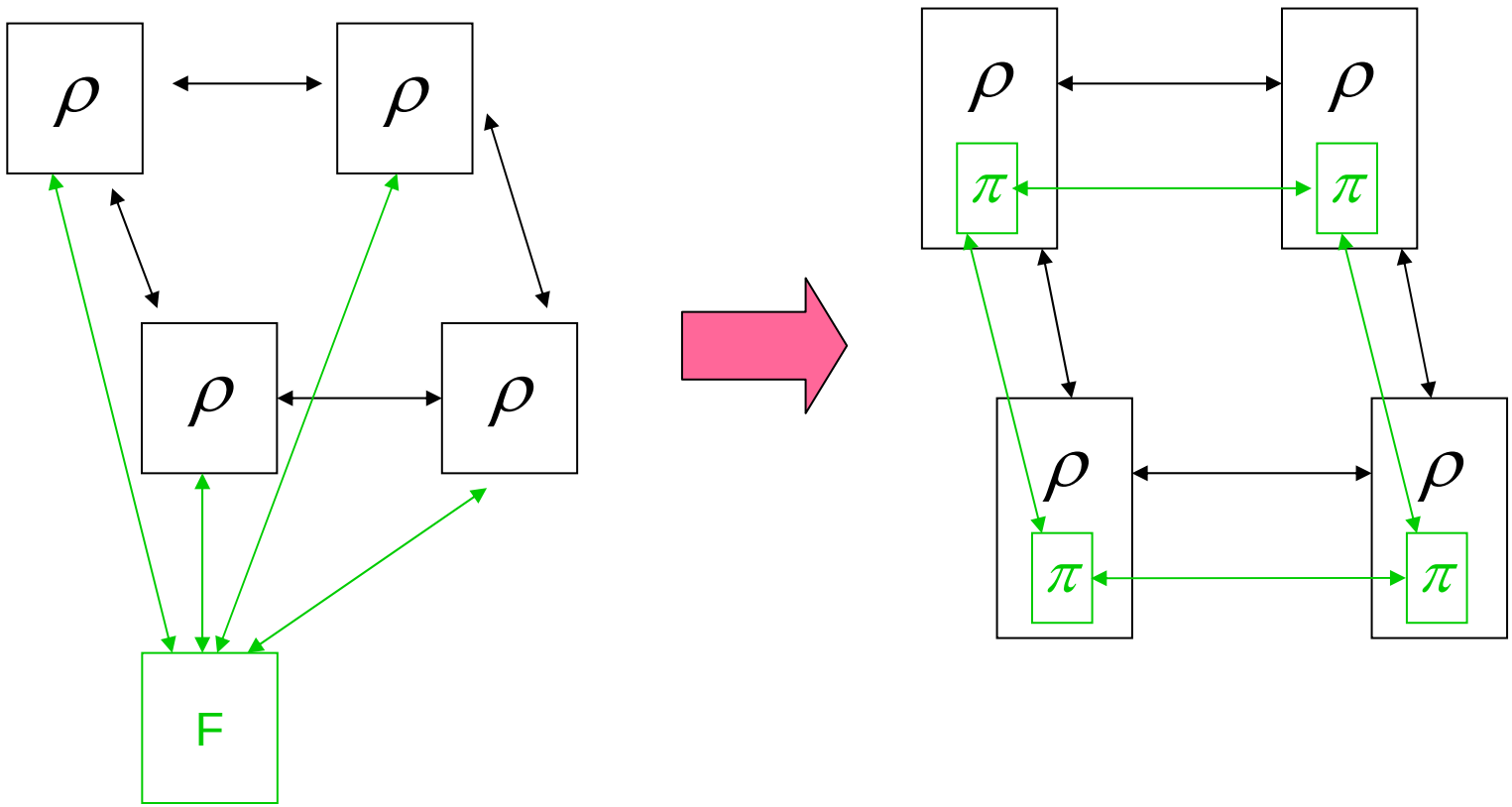
- 単体の機能として実現したプリミティブ/プロトコルが、どのような組合せの中で部品として使われても、単体のときの安全性/機能を保存する。

結合処理（Composition operation）

- 前提
  - プロトコル ρ^F は F へアクセス
  - プロトコル π は F を安全に実現
- 結合プロトコル ρ^π を実現:
  - F へのアクセスを π へのサブルーチンコールに置き換え
  - π からのリターン値は F からの応答に対応させる
    - 注意: ρ^F において各パーティは F の複数のコピーにアクセス

    $\rightarrow \rho^\pi$ において π の複数のコピーは concurrent に実行

結合（プロトコル π をプロトコル ρ の中の部品として利用）



汎用的結合可能性定理： UC定理
(The Universal Composition Theorem:[Canetti01])

- プロトコル ρ^{π} がプロトコル ρ^{F} をエミュレート

  つまり $\forall A \exists A' \ s.t. \forall Z$ は、 ρ^{π} と ρ^{F} のいずれとインタラクションしたかを区別できない）
- 系：$\left(\rho^{F}, A'\right)$ が安全に機能Gを実現

  $\Rightarrow \left(\rho^{\pi}, A\right)$ も安全にGを実現

UC定理の意味づけ（1）

1. プロトコル設計のモジュラー化
   - 機能 T をよりシンプルなサブ機能 $T_1, \ldots, T_k$ に分割
   - 各 $T_1, \ldots, T_k$ を実現するプロトコルに構成
   - $T_1, \ldots, T_k$ に理想的にアクセスすると仮定してTを構成
   - UC定理に基づき T を実現するプロトコルを構成

UC定理の意味づけ(2)

2. プロトコル π が理想機能 F を実現すると仮定すると、π をどのように複数回組み合わせて利用しても、その安全性が保証

環境から見た場合、π の複数個のコピーにアクセスすることと、F の複数個のコピーにアクセスすることは同等

(例えば、UC-ZKを実現するプロトコルはconcurrentタイプなどすべての結合に対して安全(ZK))

問題

- 各種機能に対応する理想機能をいかに記述するか？
- 既知のプロトコルはUC-安全か？
- UC-安全なプロトコルをいかに設計するか？

既存の結果：正しく動作する者が過半数の場合

- 定理：正しく動作する者が過半数の場合は、どのような機能もUC-安全に実現可
  - (e.g. [BenOr-Goldwasser-Wigderson88, Rabin-BenOr89, Canetti-Feige-Goldreich-Naor96])

２者プロトコル

- 既存のプロトコルはUC-安全でない（リワインデンングを伴うブラックボックスシミュレーションが使えない）
- 多くの興味深い機能（コミットメント、ZK、コイン投げ　等）が標準的モデルでUC-安全に実現不可。
- 共通参照情報（CRS）モデルでは実現可。
  - UC コミットメント
  - UC ゼロ知識証明
  - 任意の２者プロトコル

  （一般のマルチパーティプロトコルに一般化可）

UC暗号とUC署名

- UC公開鍵暗号の条件は、[Rackoff-Simon91, Dolev-Dwork-Naor91,…]による“選択暗号文攻撃に対する強秘匿／頑強”(IND/NM-CCA2)と同じ
- UC署名の条件は、[Goldwasser-Micali-Rivest88]による“選択文書攻撃に対する存在的偽造不可”(EUF-CMA2)と同じ

UC 鍵交換[Canetti-Krawzcyk01,02]

- 既存のプロトコル (e.g. ISO 9798-3, IKE, SSL/TLS)が UC 鍵交換であることを証明

その他の結果

- UC コミットメントの改良
  - [Damgard-Nielsen02, Damgard-Groth03, Camenish-Shoup03]
- 自動検証における UC 暗号ライブラリ
  - [Backes-Pfitzemann-Waidner03]
- UC 定式化の最適性
  - [Lindell03]
- 標準モデルにおけるUCマルチパーティプロトコル
  - [Prabhakaran-Sahai04]

暗号(プロトコル)の安全性を証明する2つのアプローチ

1.計算論的アプローチ

- 確率的多項式時間(PPT)TMを敵のモデルとして捉え、いかなるPPT-TMに対しても安全である事を示す。(確率、時間限定TMの導入)

  BM'82、Yao'82、GM'82、・・・

- 暗号(プロトコル)の安全性定義として、暗号コミュニティーでは広く受け入れられている(その典型がUC)。
- 一般にその安全性証明は複雑で、間違った証明も多く見られる。

2.数理的(Formal method)アプローチ

- 対象とする暗号(プロトコル)を記号列で表現し、その記号列に対する論理的推論／書換規則などにより、安全性を示す。

  Dolev-Yao'82、BAN Logic、・・・

- Formal methodコミュニティーでは活発／多様な研究があるが、暗号コミュニティーには受け入れられてこなかった。
- 証明は明確で、(部分的)自動化も可能である。

２つのアプローチの融合:新しい動向

1.Abadi-Rogaway 2000

- 共通鍵暗号の単純なプロトコルに対して、数理的アプローチによる安全性が計算論的アプローチの安全性を保証することを示した(つまり、数理的アプローチの「健全性」を示した。ただし、その逆、「完全性」は必ずしもいえない）

2.Canetti-Herzog　2006

- Dolev-Yao流の数理的アプローチが（ハイブリッドモデルでの）UC安全性を保証する事を示した。また、既存の検査ツールを使って具体的鍵交換プロトコルのUC安全性を示した。

2つのアプローチの融合(2)

1.Abadi-Rogaway 2000

- 数理的アプローチにおける各種記号列の中に、(理想的)暗号機能を意味する記号$\{M\}_k$を導入
- 計算論的アプローチにおいて、強秘匿(IND)を強化した安全性を持つ暗号機能を (ブラックボックスとして)導入

  ⇒この暗号機能をfunctionalityと捉えてUCの枠組みの中で考えれば、Canetti-Herzogの結果と極めて類似する。

2.Canetti-Herzog 2006

- DY流数理的アプローチにおいて、(理想的)公開鍵暗号機能を意味する記号$\{M\}_{PK}$を導入
- UCにおいて、公開鍵暗号のfunctionality(理想機能)F_{CPKE}をハイブリッドモデルとして導入

  ⇒UCにおける functionality(理想機能)は、数理的アプローチにおける記号(ある種の理想機能)に対応する事ができる。

2つのアプローチの融合(3)

Canetti-Cheung-Kaynar-Liskov-Lynch-Pereira-Segala 2006

- 数理的アプローチとして、記号列／論理的推論の代わりに確率的I/Oオートマトン(PIOA)のモデルを導入し、PIOAにより表現した安全性が(弱いモデルでの)UC安全性を保証することを(OTの一実現例について)示した。

  ⇒UC安全性の証明をPIOAモデル(従来のDYモデルなどよりも強力なモデル)で(部分的に)機械化することへの一歩となる。

Announcement

日本応用数理学会に新しい研究部会発足予定

「数理的技法による情報セキュリティ」研究部会

（FAIS: Formal Approach to Information Security）

- 代表：　萩谷昌己（東大）
- 幹事：　赤間陽二（東北大）
  岡本龍明（NTT）
  竹内泉　（産総研）
  塚田恭章（NTT）　◎連絡窓口
  藤原融　（阪大）
- 当面の予定：　・7月末　informal meeting
  ・9月　応用数理学会年会(筑波大)：オーガナイズド
  セッション（この分野のチュートリアル予定）
- 研究部会には誰でも(会員である必要無)無料で参加／発表できます。
  多くの皆様の参加をお待ちしています！