汎用的結合可能性と数理的技法への期待

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

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。
- 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。

計算論的アプローチ

計算論的アプローチで、安全性がいかに定式化されてきたか？

- 攻撃ベース定式化： 攻撃者とチャレンジャー間のゲームとして定式化。最近、ゲームを徐々に変換して作るゲーム列を解析することで、安全性を証明する手法が発展しつつある。

  公開鍵暗号、ディジタル署名、….

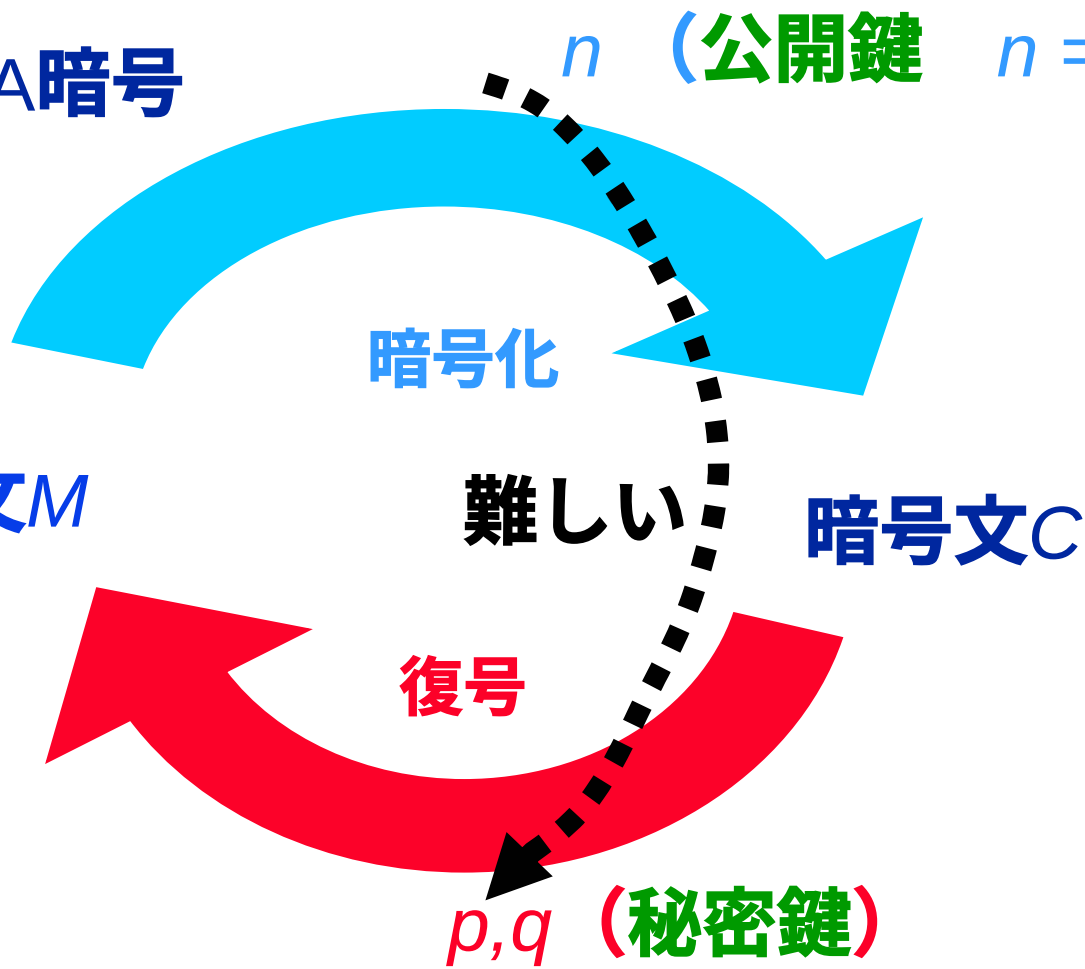
- シミュレーションベース定式化： 実際の方式（現実モデル）と、理想的な機能を使って現実をシミュレーションした方式（理想モデル）との間のギャップにより定式化。暗号におけるすべての対象に対する統一的定式化を可能とする。

  汎用的結合可能性（Universal composability)、...

公開鍵暗号の安全性：攻撃ベース定式化の典型例

公開鍵暗号の原理

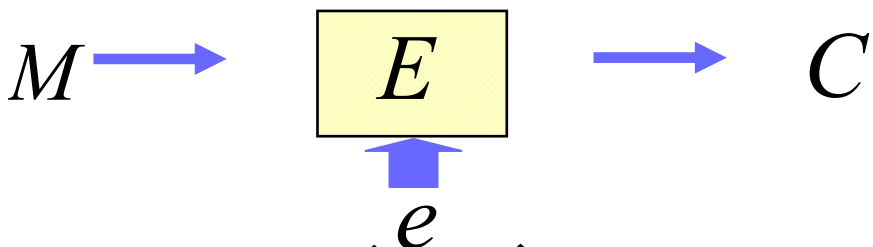
例：RSA暗号



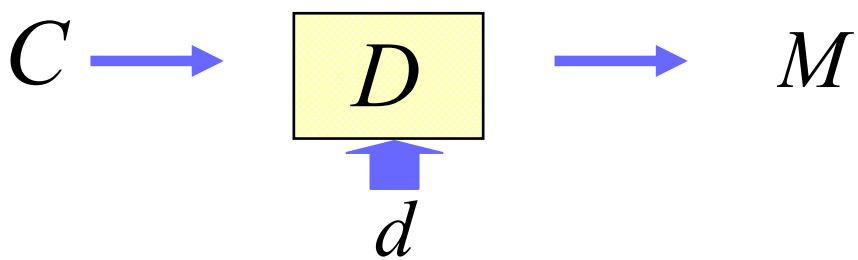
公開鍵暗号(G, E, D)

- 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

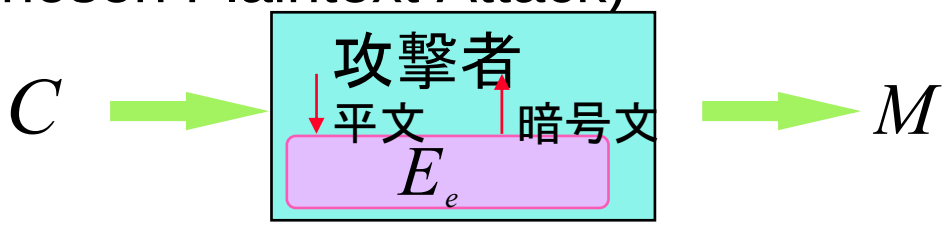
- 達成度
  - 秘匿性
    - 一方向性（OW）　$c=E_{pk}(m)$ →(困難) m
    - 強秘匿性（IND）　$c=E_{pk}(m)$ より m のいかなる部分情報も解読困難
  - 頑強性（NM）　・・・ $c=E_{pk}(m)$ →(困難) $c'=E_{pk}(m')$

    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)

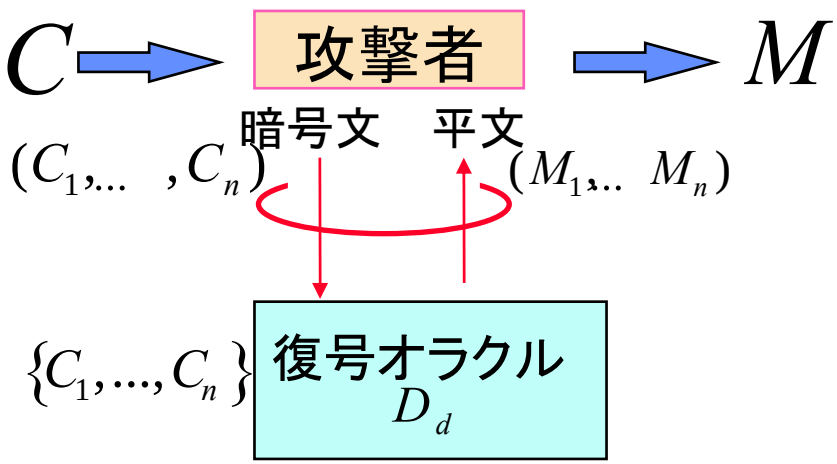
- 暗号文攻撃(選択平文攻撃)

  (CPA：Chosen Plaintext Attack)



- 選択暗号文攻撃

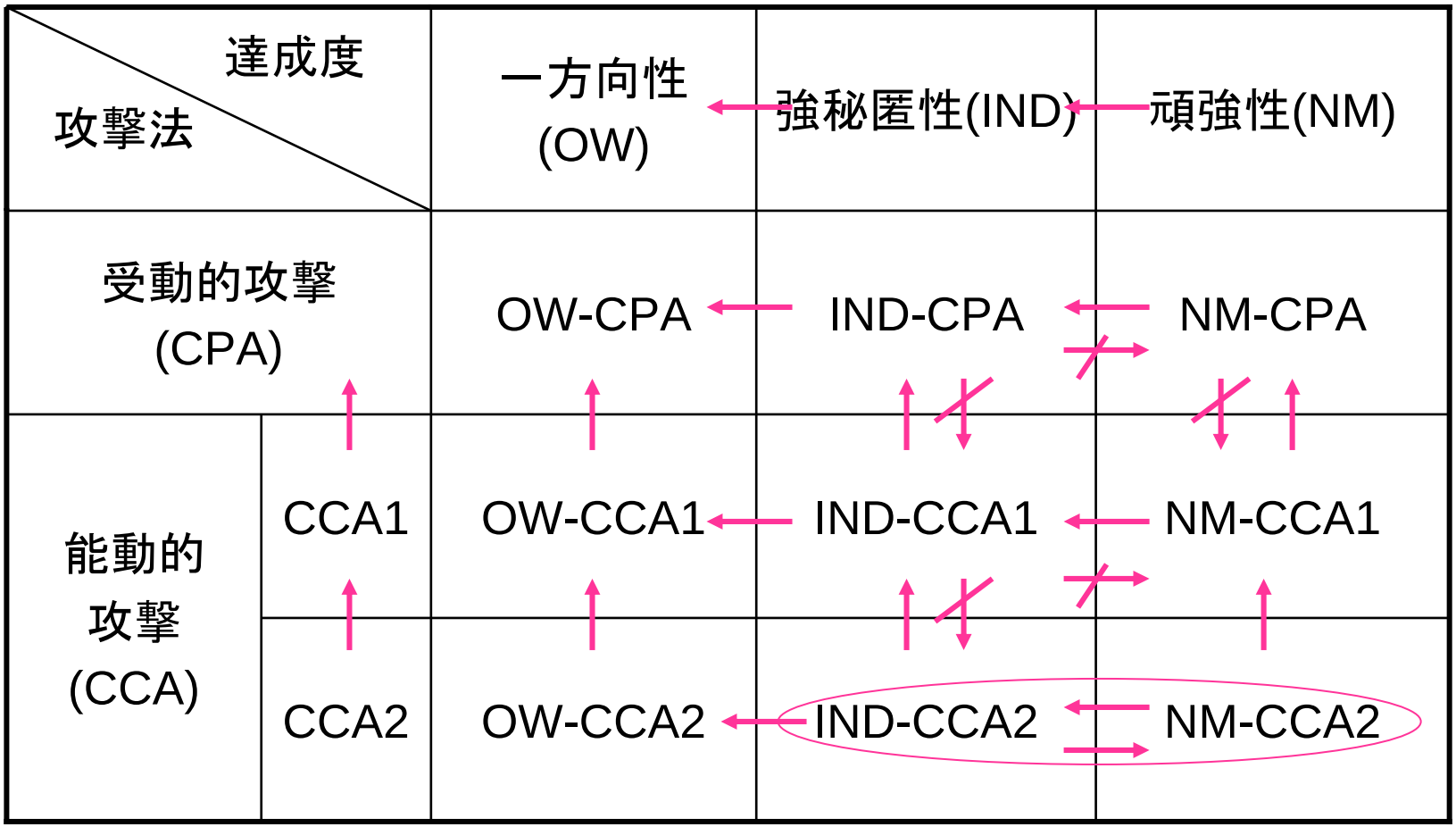
  (CCA：Chosen Ciphertext Attack)



(但し, $C \notin \{C_1,\ldots,C_n\}$)

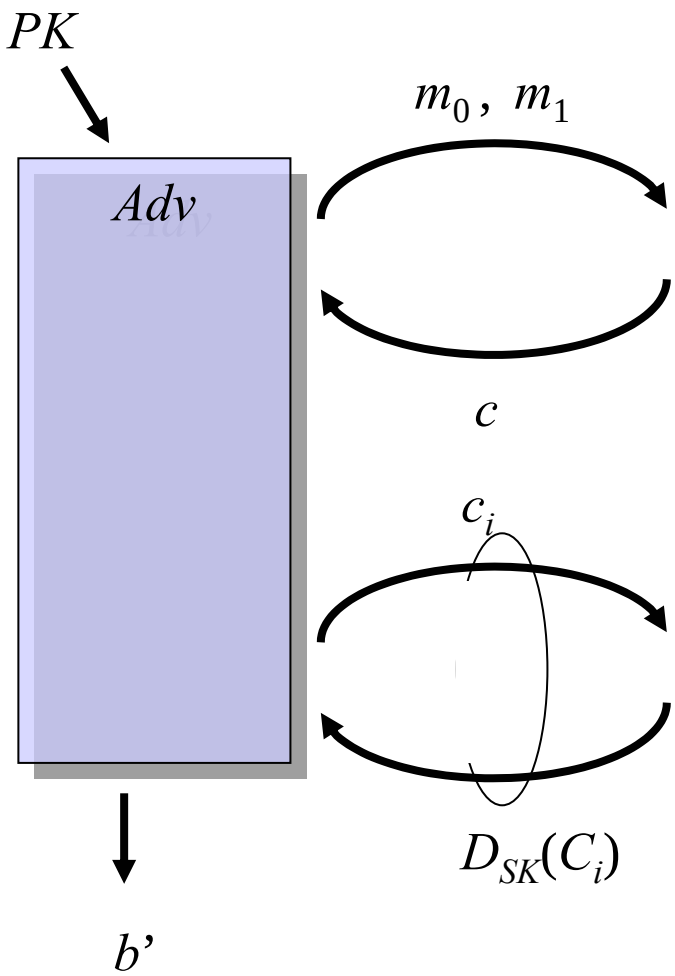
CCA1・・Cを受け取る前にCCAを行う。
CCA2・・Cを受け取った後にCCAを行う。
(CCA2はCCA1より強力な攻撃法)

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(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*)

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

ゲーム列による安全性証明の例

Cramer-Shoup 暗号

$$\mathrm{SK} \leftarrow (x_1, x_2, y_1, y_2, z_1, z_2) \in \mathsf{Z}_q^{\,6}$$

$$e \leftarrow g^{x_1}\hat{g}^{x_2},\ f \leftarrow g^{y_1}\hat{g}^{y_2},\ h \leftarrow g^{z_1}\hat{g}^{z_2}$$

$$\mathrm{PK} \leftarrow (\Gamma[G, \hat{G}, g, q], hk, \hat{g}, e, f, h) \quad (g \in G, \hat{g} \in \hat{G})$$

平文 m →

暗号化 (PK)

$E1: u \leftarrow_{\cup} \mathsf{Z}_q$

$E2: a \leftarrow g^u$

$E3: \hat{a} \leftarrow \hat{g}^u$

$E4: b \leftarrow h^u$

$E5: c \leftarrow b \cdot m$

$E6: v \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a^*, \hat{a}^*, c^*)$

$E7: d \leftarrow e^u f^{uv}$

暗号文 $(a, \hat{a}, c, d)$ →

復号化 (SK)

D1: Check the form.

D2: $a, \hat{a}, c \overset{?}{\in} G$

D3: $v \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a, \hat{a}, c)$

D4: $d \overset{?}{=} a^{x_1 + y_1 v}\, \hat{a}^{x_2 + y_2 v}$

D5: $b \leftarrow a^{z_1}\hat{a}^{z_2}$

D6: $m \leftarrow c \cdot b^{-1}$

→ m

Game0: IND-CCA2 Game

$$(\Gamma[G, \hat{G}, g, q], hk, \hat{g}, e, f, h)$$

Decryption Oracle

D1: Check the form.

D2: $a, \hat{a}, c \overset{?}{\in} G$

D3: $v \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a,\hat{a},c)$

D4: $d \overset{?}{=} a^{x_1 + y_1 v}\, \hat{a}^{x_2 + y_2 v}$

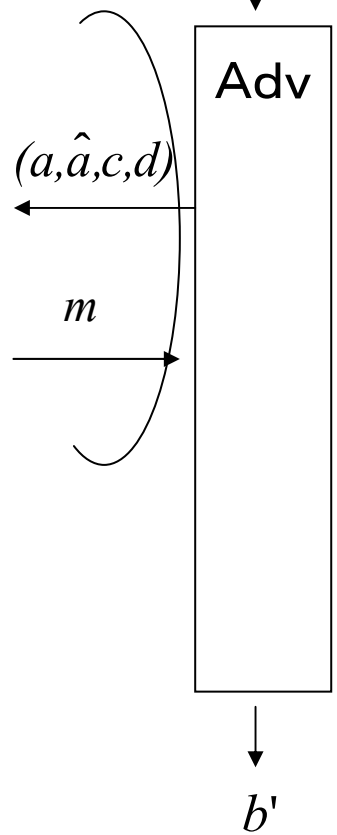
D5: $b \leftarrow a^{z_1} \hat{a}^{z_2}$

D6: $m \leftarrow c \cdot b^{-1}$

$\mathsf{SK} \leftarrow (x_1, x_2, y_1, y_2, z_1, z_2)$

$e \leftarrow g^{x_1} \hat{g}^{x_2}$, $f \leftarrow g^{y_1} \hat{g}^{y_2}$,

$h \leftarrow g^{z_1} \hat{g}^{z_2}$



Encryption Oracle

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

E1: $u \leftarrow_U Z_q$

E2: $a^* \leftarrow g^u$

E3: $\hat{a}^* \leftarrow \hat{g}^u$

E4: $b^* \leftarrow h^u$

E5: $c^* \leftarrow b^* \cdot m_b$

E6: $v^* \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a^*,\hat{a}^*,c^*)$

E7: $d^* \leftarrow e^u f^{uv^*}$

$$\text{Advantage} = \left| \Pr[b = b'] - \frac{1}{2} \right|$$

Game1

$(\Gamma[G, \hat{G}, g, q], hk, \hat{g}, e, f, h)$

Decryption Oracle

D1: Check the form.

D2: $a, \hat{a}, c \overset{?}{\in} G$

D3: $v \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a,\hat{a},c)$

D4: $d \overset{?}{=} a^{x_1 + y_1 v}\, \hat{a}^{x_2 + y_2 v}$

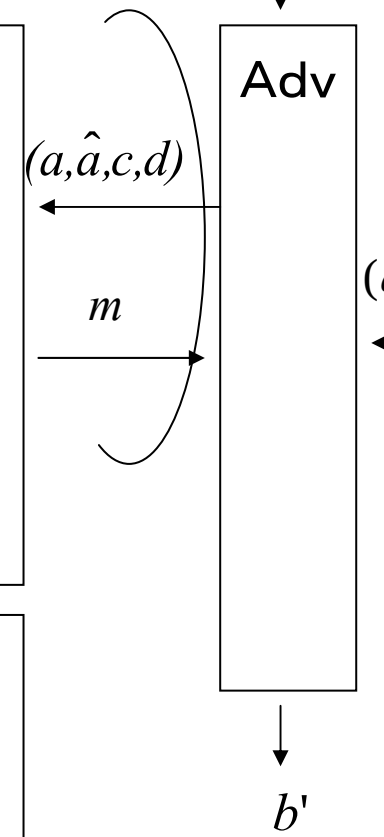
D5: $b \leftarrow a^{z_1} \hat{a}^{z_2}$

D6: $m \leftarrow c \cdot b^{-1}$

$\mathsf{SK} \leftarrow (x_1, x_2, y_1, y_2, z_1, z_2)$

$e \leftarrow g^{x_1} \hat{g}^{x_2}$, $f \leftarrow g^{y_1} \hat{g}^{y_2}$,

$h \leftarrow g^{z_1} \hat{g}^{z_2}$



Encryption Oracle

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

E1: $u \leftarrow_U Z_q$

E2: $a^* \leftarrow g^u$

E3: $\hat{a}^* \leftarrow \hat{g}^u$

E4': $b^* \leftarrow a^{z_1} \hat{a}^{z_2}$

E5: $c^* \leftarrow b^* \cdot m_b$

E6: $v^* \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a^*,\hat{a}^*,c^*)$

E7': $d^* \leftarrow a^{*x_1 + y_1 v} \cdot \hat{a}^{*x_2 + y_2 v^*}$

$$\text{Advantage} = \left| \Pr[b = b'] - \frac{1}{2} \right|$$

Game2

$(\Gamma[G, \hat{G}, g, q], hk, \hat{g}, e, f, h)$

Decryption Oracle

D1: Check the form.

D2: $a, \hat{a}, c \overset{?}{\in} G$

D3: $v \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a,\hat{a},c)$

D4: $d \overset{?}{=} a^{x_1+y_1 v}\,\hat{a}^{x_2+y_2 v}$

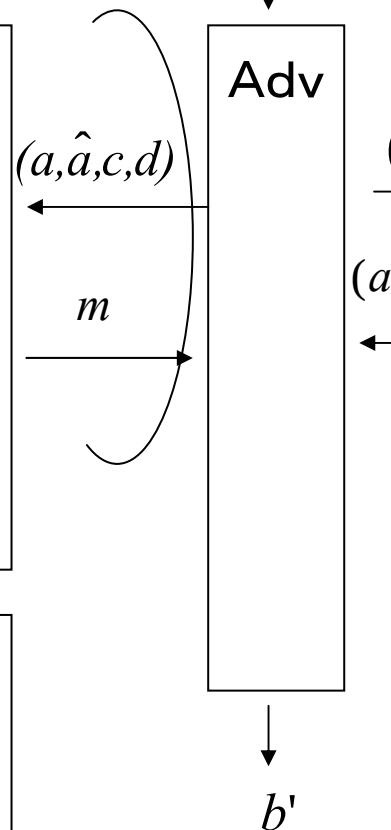
D5: $b \leftarrow a^{z_1}\hat{a}^{z_2}$

D6: $m \leftarrow c \cdot b^{-1}$

$\mathsf{SK} \leftarrow (x_1, x_2, y_1, y_2, z_1, z_2)$

$e \leftarrow g^{x_1}\hat{g}^{x_2}$, $f \leftarrow g^{y_1}\hat{g}^{y_2}$,

$h \leftarrow g^{z_1}\hat{g}^{z_2}$



Encryption Oracle

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

E1: $u \leftarrow_U Z_q$

E2: $d^* \leftarrow g^u$

E3': $\hat{a}^* \leftarrow \hat{g}^{\hat{u}}$, $\hat{u} \leftarrow_U Z_q \setminus \{u\}$

E4': $b^* \leftarrow a^{z_1}\hat{a}^{z_2}$

E5: $c^* \leftarrow b^* \cdot m_b$

E6: $v^* \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a^*,\hat{a}^*,c^*)$

E7': $d^* \leftarrow a^{*x_1+y_1 v} \cdot \hat{a}^{*x_2+y_2 v^*}$

$$\text{Advantage} = \left| \Pr[b = b'] - \frac{1}{2} \right|$$

Game3

$(\Gamma[G, \hat{G}, g, q], hk, \hat{g}, e, f, h)$

Decryption Oracle

D1: Check the form.

D2: $a, \hat{a}, c \overset{?}{\in} G$

D3: $v \leftarrow \mathrm{HF}_{hk}^{\lambda,\Gamma}(a,\hat{a},c)$

D4': $\hat{a} \overset{?}{=} a^{w}, d \overset{?}{=} a^{x+yv}, \mathrm{v} \overset{?}{\neq} \mathrm{v}^*$

D5': $b \leftarrow a^{z}$

D6: $m \leftarrow c \cdot b^{-1}$

$\mathrm{SK} \leftarrow (x_1, x_2, y_1, y_2, z_1, z_2)$

$e \leftarrow g^{x_1}\hat{g}^{x_2} = g^{x}$, $f \leftarrow g^{y_1}\hat{g}^{y_2} = g^{y}$,

$h \leftarrow g^{z_1}\hat{g}^{z_2} = g^{z}$

$(a,\hat{a},c,d)$

m

Adv

b'

(m_0, m_1)

$(a^*, \hat{a}^*, c^*, d^*)$

Encryption Oracle

$b \leftarrow_{\mathrm{U}} \{0,1\}$

E1: $u \leftarrow_{\mathrm{U}} Z_q$

E2: $d^* \leftarrow g^{u}$

E3': $\hat{a}^* \leftarrow \hat{g}^{\hat{u}}$, $\hat{u} \leftarrow_{\mathrm{U}} Z_q \setminus \{u\}$

E4': $b^* \leftarrow a^{z_1}\hat{a}^{z_2}$

E5: $c^* \leftarrow b^* \cdot m_b$

E6: $v^* \leftarrow \mathrm{HF}_{hk}^{\lambda,\Gamma}(a^*,\hat{a}^*,c^*)$

E7': $d^* \leftarrow a^{*x_1+y_1v} \cdot \hat{a}^{*x_2+y_2v^*}$

$$\text{Advantage} = \left| \Pr[b = b'] - \frac{1}{2} \right|$$

Game4

$(\Gamma[G, \hat{G}, g, q], hk, \hat{g}, e, f, h)$

Decryption Oracle

D1: Check the form.

D2: $a, \hat{a}, c \overset{?}{\in} G$

D3: $v \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a,\hat{a},c)$

D4': $\hat{a} \overset{?}{=} a^{w}, d \overset{?}{=} a^{x+yv}, \mathrm{v} \overset{?}{\neq} \mathrm{v}^*$

D5': $b \leftarrow a^{z}$

D6: $m \leftarrow c \cdot b^{-1}$

$\mathsf{SK} \leftarrow (x_1, x_2, y_1, y_2, z_1, z_2)$

$e \leftarrow g^{x_1}\hat{g}^{x_2} = g^{x}$, $f \leftarrow g^{y_1}\hat{g}^{y_2} = g^{y}$,

$h \leftarrow g^{z_1}\hat{g}^{z_2} = g^{z}$

$(a,\hat{a},c,d)$

m

Adv

b'

(m_0, m_1)

$(a^*, \hat{a}^*, c^*, d^*)$

Encryption Oracle

$b \leftarrow_{\cup} \{0,1\}$

E1: $u \leftarrow_{\cup} Z_q$

E2: $a^* \leftarrow g^{u}$

E3': $\hat{a}^* \leftarrow \hat{g}^{\hat{u}}$, $\hat{u} \leftarrow_{\cup} Z_q \setminus \{u\}$

E4': $b^* \leftarrow a^{z_1}\hat{a}^{z_2}$

E5': $c^* \leftarrow g^{r}, r \leftarrow_{\cup} Z_q$

E6: $v^* \leftarrow \mathsf{HF}_{hk}^{\lambda,\Gamma}(a^*,\hat{a}^*,c^*)$

E7': $d^* \leftarrow a^{*x_1+y_1v} \cdot \hat{a}^{*x_2+y_2v^*}$

$$\text{Advantage} = \left| \Pr[b = b'] - \frac{1}{2} \right|$$

汎用的結合可能性（Universal Composability：UC）：シミュレーションベース定式化

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。

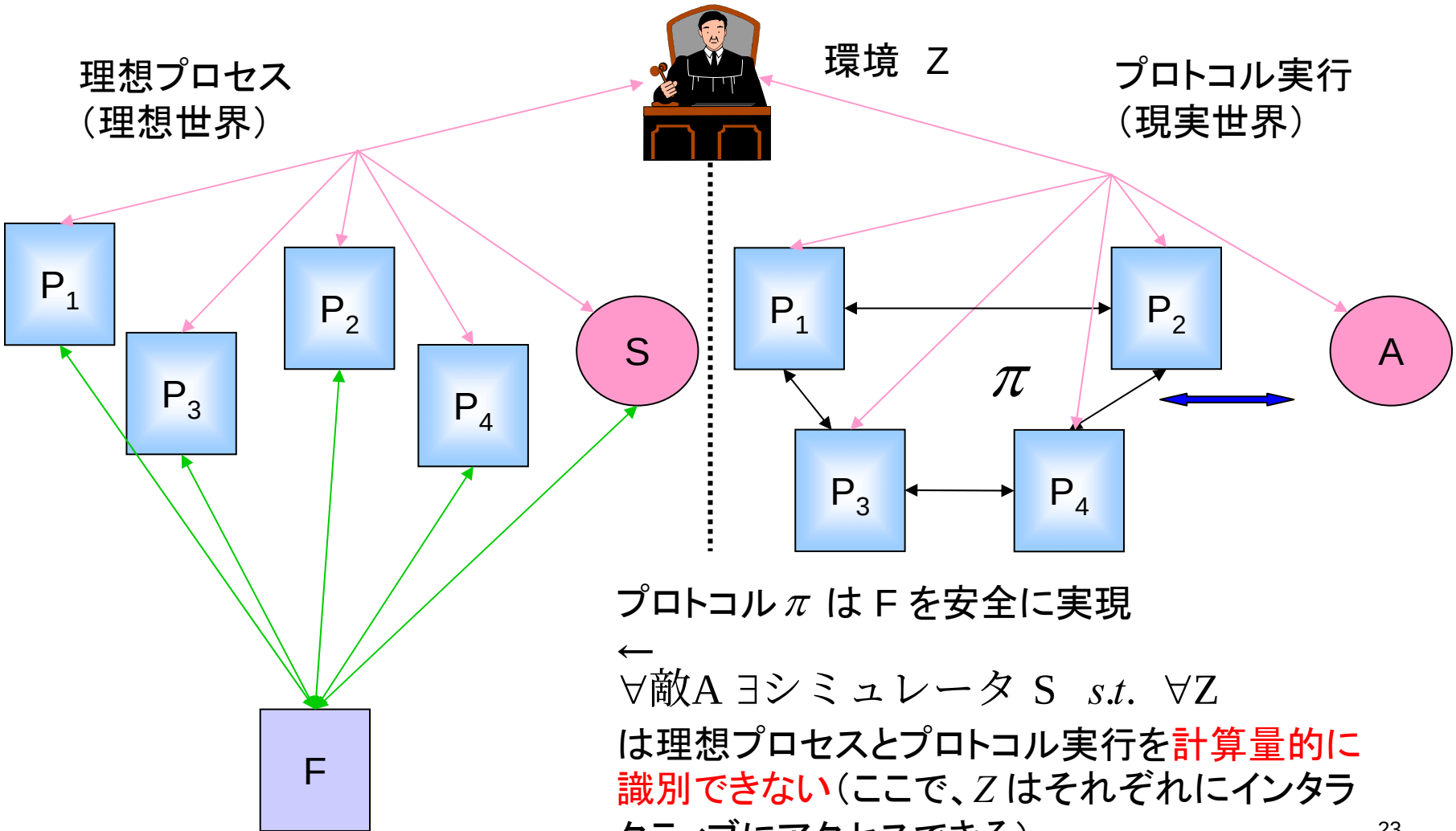
いかに安全性を定義するか（1）

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)



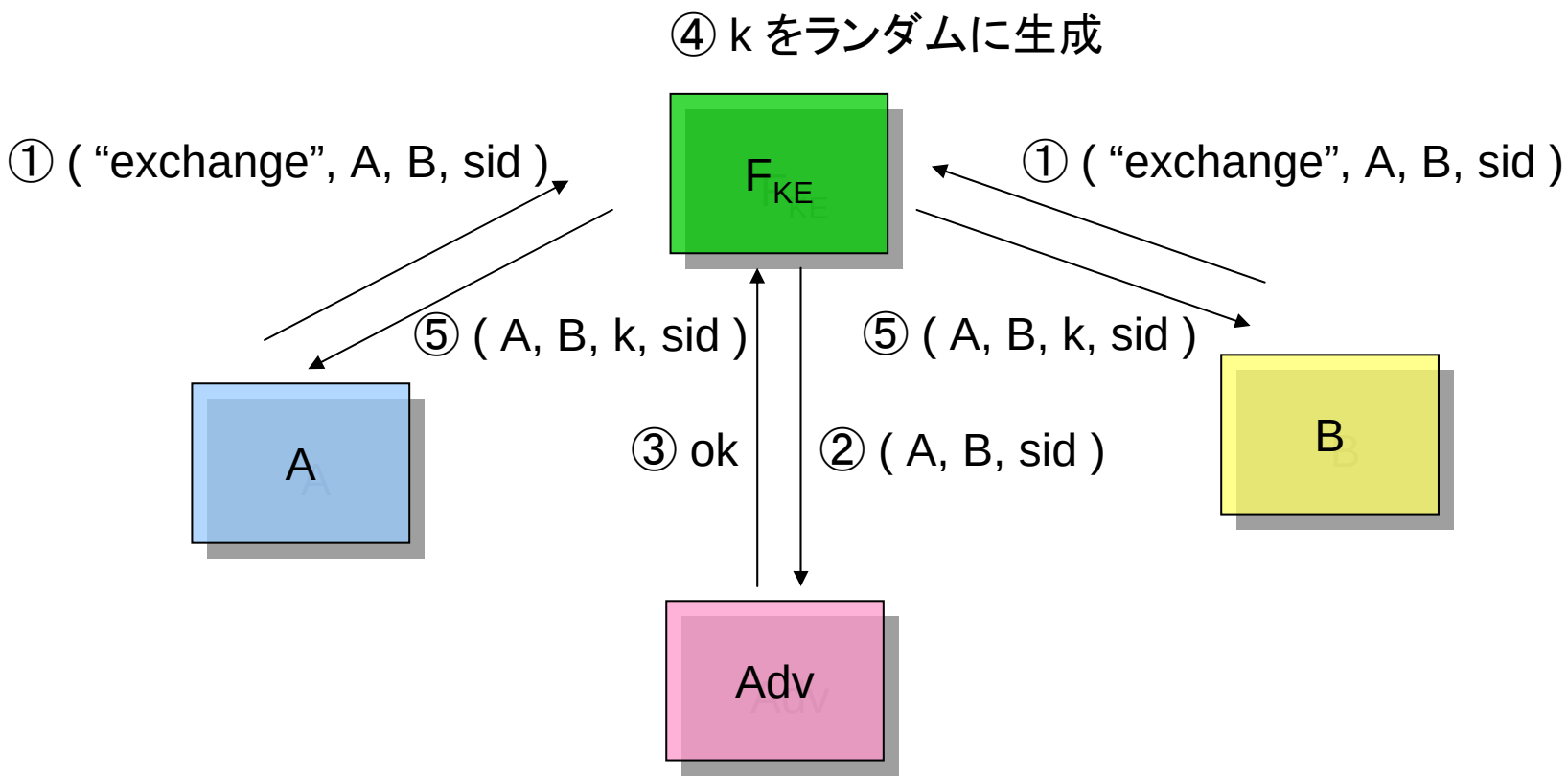
プロトコル π は F を安全に実現

←

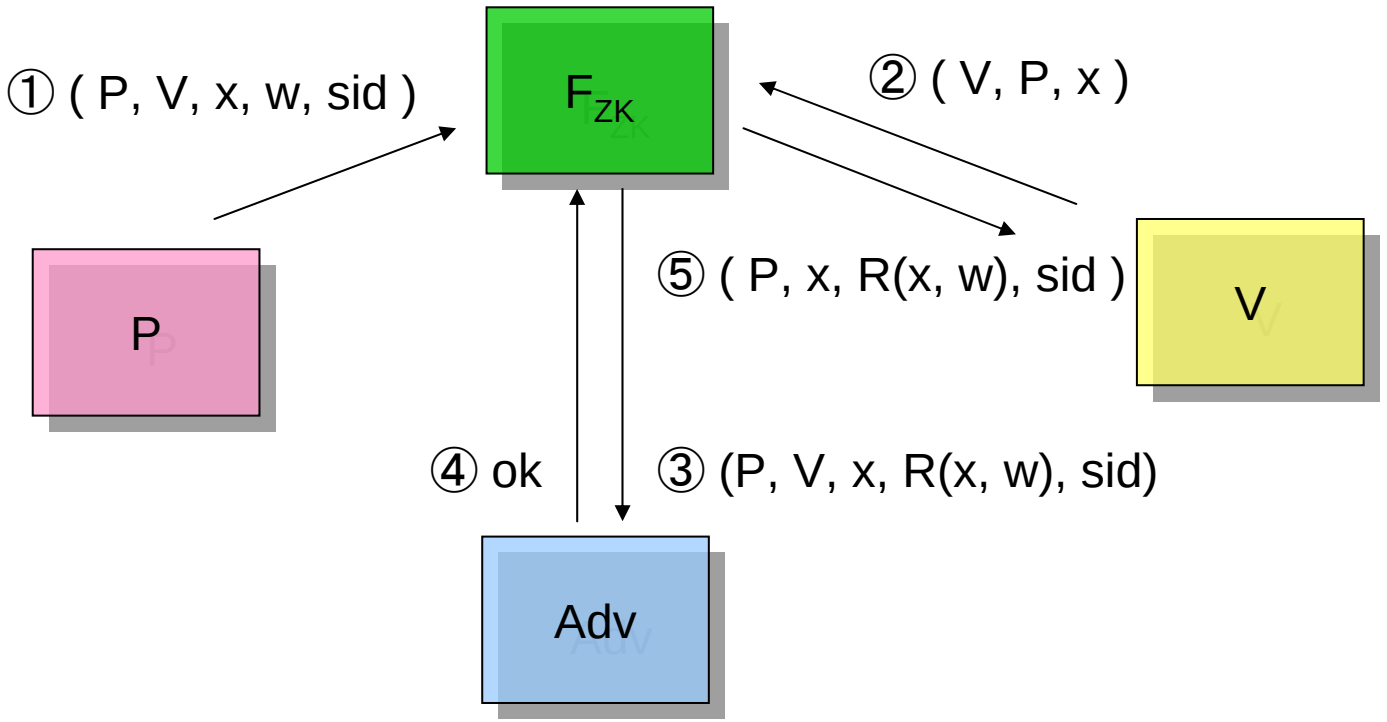
$\forall$敵A $\exists$シミュレータ S *s.t.* $\forall$Z

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）

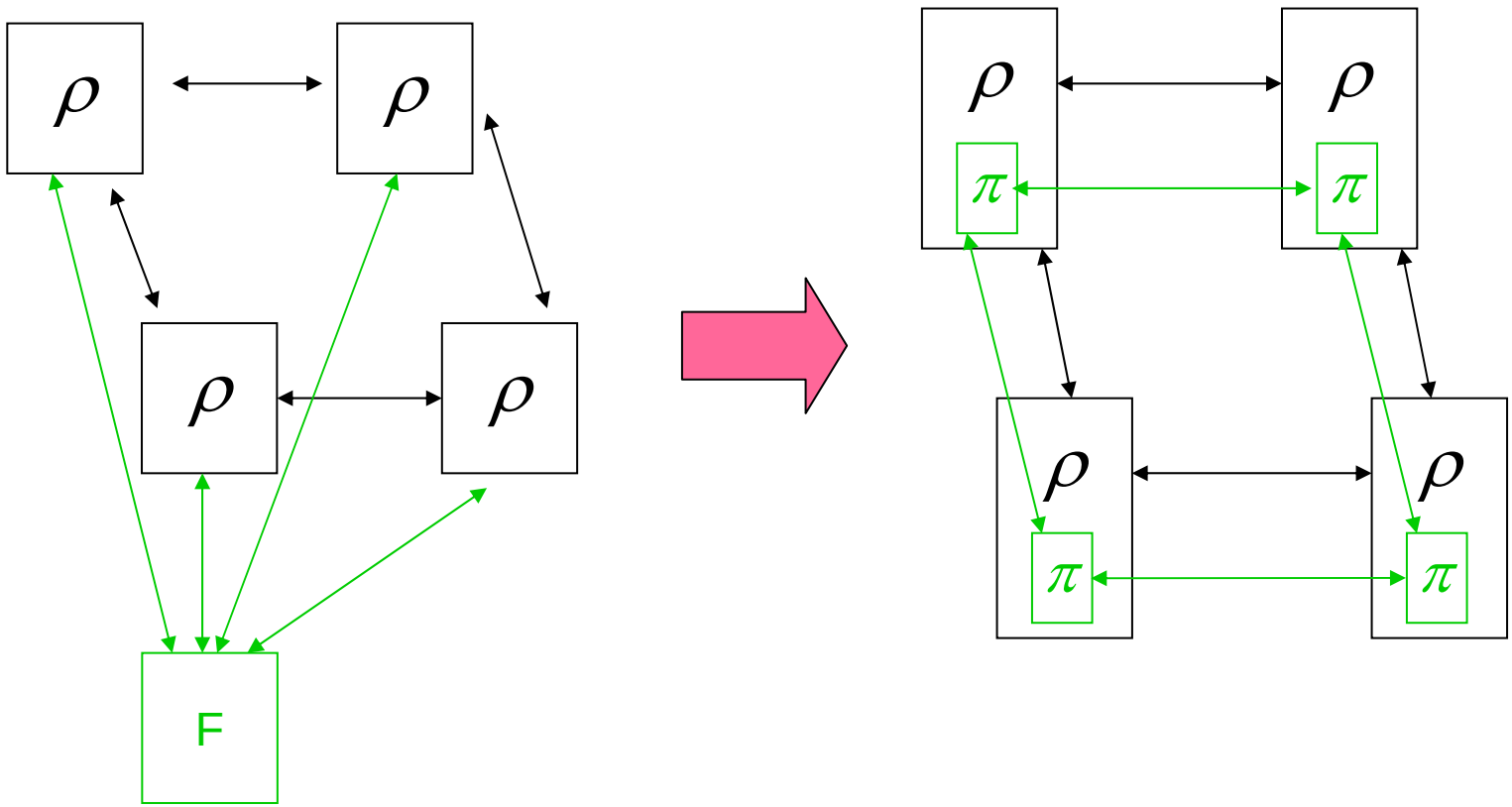
- 単体の機能として実現したプリミティブ/プロトコルが、どのような組合せの中で部品として使われても、単体のときの安全性/機能を保存する。

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))

数理的技法への期待

どこに数理的技法を適用するか

- 目的: 計算量的アプローチによる証明を簡明化／(部分)自動化したい
- 必要条件: 数理的技法による証明の健全性
- 適用可能な領域:

  (1)UCにおける理想機能の記述および理想機能を組み合わせたプロトコル(ハイブリッドモデル)の安全性証明

  (2)UCの理想機能を実現する基本方式の証明

  (3)ゲーム列による証明の形式化／自動化

UCの理想機能に基づくプロトコル（ハイブリッドモデル）の証明に数理的技法を適用

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。

UCの理想機能に基づくプロトコル（ハイブリッドモデル）の証明に数理的技法を適用

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。

UCの理想機能を実現する基本方式の証明

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。

ゲーム列による証明の形式化／自動化

Blanchet-Pointcheval 2006

- 他の融合のアプローチが、上位レベル（ある理想的な基本機能を仮定した上で、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す）だったのに対して、本研究は、下位レベル（理想的基本機能を仮定することなく、計算量的な仮定だけに基づき安全性を証明）において、2つのアプローチの融合を行う。
- 計算論的アプローチ（攻撃ベース定式化）で、最近流行している手法（ゲームの系列で安全性を証明）を数理的アプローチに適用。ゲームを変換するルールを抽出し、それをプロセス計算に適用することでゲーム系列を自動生成し証明する。

  ⇒具体的署名の安全性をプロセス計算ツールを用いて自動証明する。

まとめ

- 暗号安全性の研究には、計算論的アプローチ（主に暗号コミュニティで研究され、標準的な方法論と認知される）と数理的アプローチ（定理の自動証明やプロトコルの自動検証などを研究する数理証明技法コミュニティで研究される）がある。
- 計算論的アプローチの成熟により、数理的アプローチとの関係が明確になりつつある。その一つは、UC（汎用的結合可能性）の定式化であり、もうひとつは、ゲーム変換による証明手法の発展である。
- 両アプローチが融合することにより、暗号コミュニティで認知されている標準的安全性の証明が（半）自動化される可能性が高まっている。