Schnorr 署名の標準モデルでの証明不可能性

川合 豊（東京大学）

証明不可能性

ある暗号プリミティブXが(ある仮定の下では)
安全性を必ず達成不可能なことを証明すること。

- 学術的な興味
- 暗号を設計する上での指針

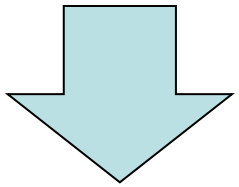
etc…

オラクルセパレーションを用いた証明技法

メタ帰着技法を用いた証明技法

本研究の(大きな)目的

ランダムオラクルモデルで安全な方式が標準モデルで安全かを様々な仮定で検証する



Schnorr署名がCDH問題で証明可能かの一考察を行う

Schnorr署名

後に複数人ユーザを考えるため

鍵生成アルゴリズム: (param,sk,pk)←Gen(k)
署名アルゴリズム: σ←Sig(param.sk,m)
検証アルゴリズム: 1/0←Ver(param,pk,σ,m)

ハッシュ関数H:{0,1}*→Zq

Gen: param=(p,G,g,H), $sk=x\in Z_q$, $pk=y(=g^x)$

Sig: $r\leftarrow Z_q$, $s=r+cx$ where $c=H(pk,m,g^r)$
$\sigma=(s,c)$

Ver: $k:=g^s y^{-c}$, $c'=H(pk,m,k)$, check $c=c'$

Schnorr署名の安全性

- ランダムオラクルモデル（ハッシュ関数Hを理想化したモデル）の上では、離散対数問題においてEUF-CMA安全が証明可能
- 標準モデルでは、離散対数問題に基づいてのEUF-CMA安全は（ある限られた帰着の方法では）証明不可能

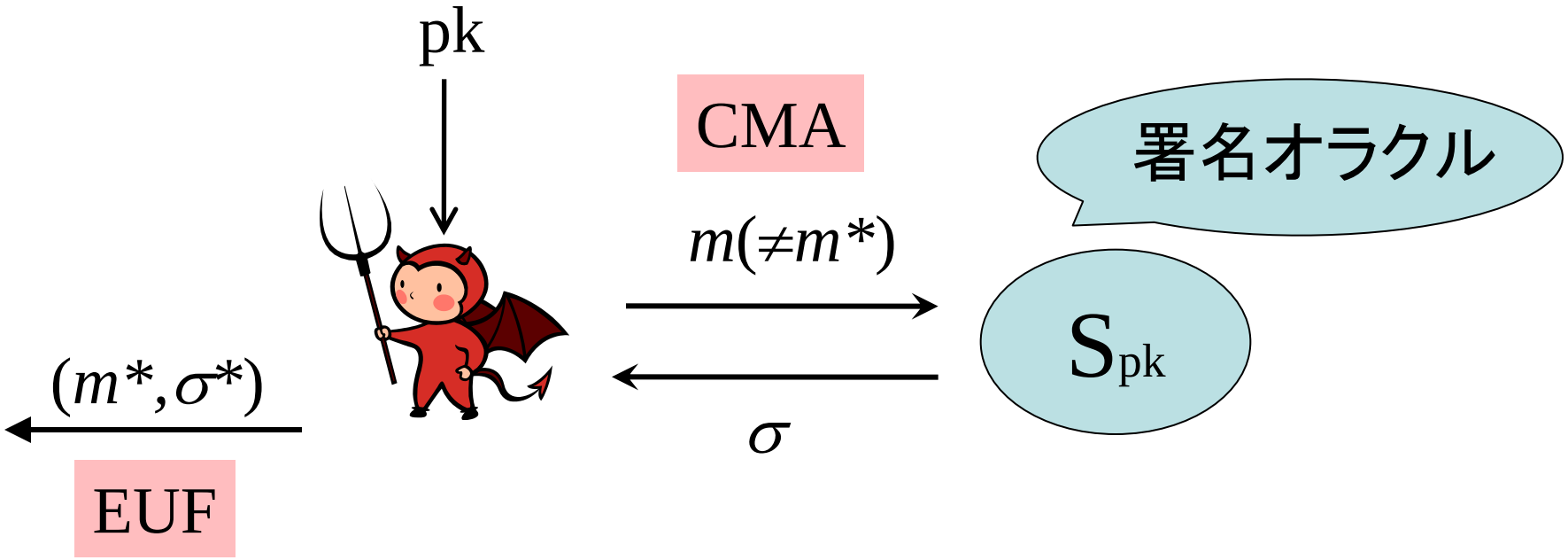
- 標準モデルで、離散対数よりも強い仮定では証明可能なのか？

CDH問題

- 群G上の離散対数問題 (DL)問題
  - 入力: g, g^x
  - 出力: x

- 群G上Computational Diffie-Hellman (CDH)問題
  - 入力: g, g^x, g^y
  - 出力: g^{xy}

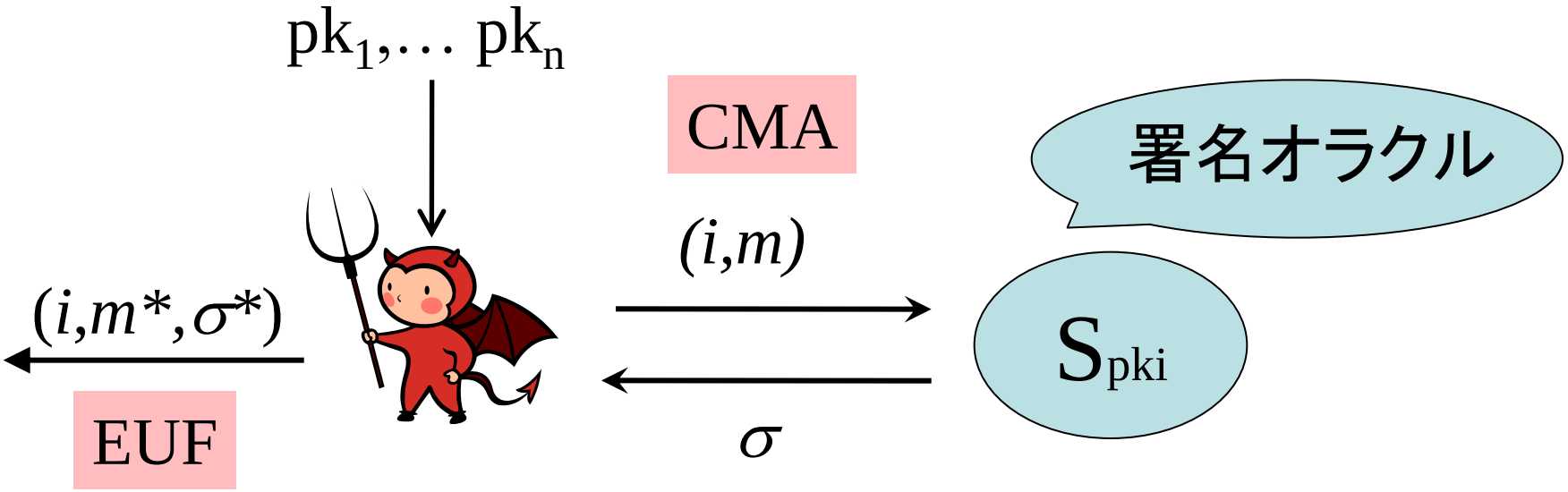
EUF-CMA攻撃者



$A^1_{\text{EUF-CMA}}$ と表記する

単一ユーザに対する安全性

n-EUF-CMA攻撃者



$A^n_{EUF\text{-}CMA}$ と表記する

複数ユーザに対する安全性

そもそもEUF-CMA安全が証明できるとは…

あるCDH問題で**安全性証明できたとする**

Rを構成すること

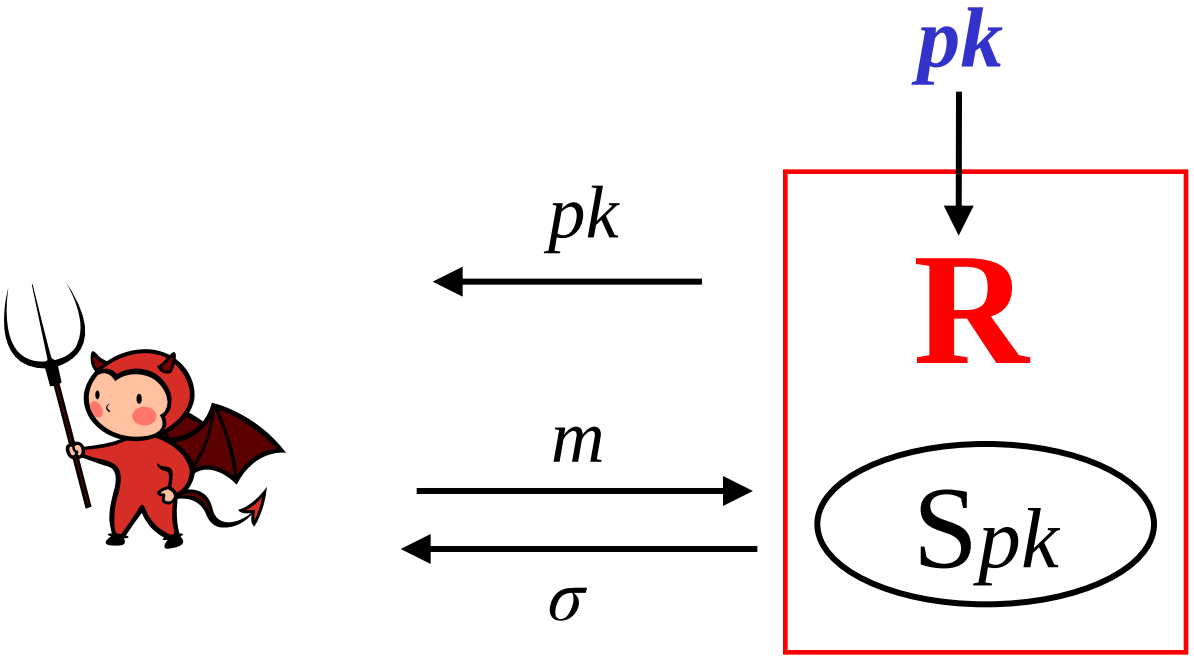
帰着 : R

CDH ⇐ $A_{\text{EUF-CMA}}$

CDH問題をを解く解読者　　EUF-CMA攻撃者

Key Preserving Black Box Reduction

入力された鍵と同じ鍵で攻撃者を動作させる

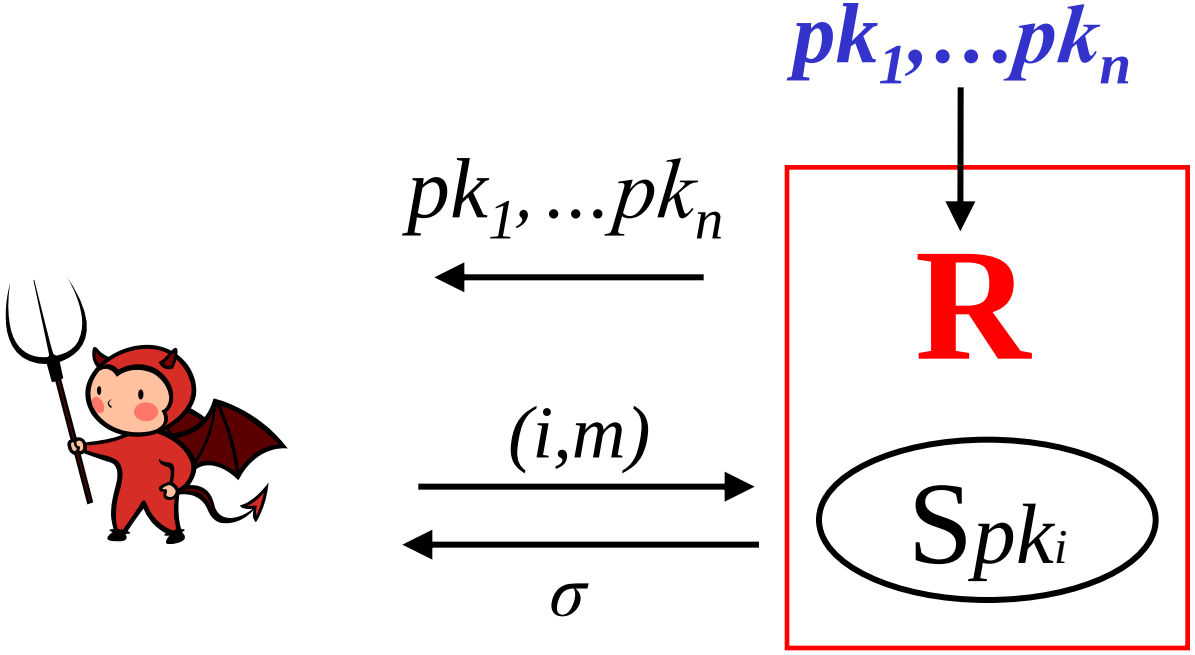


Rが解くべき問題：素因数分解
公開鍵pk=n（合成数）

このようなケースで考えられる

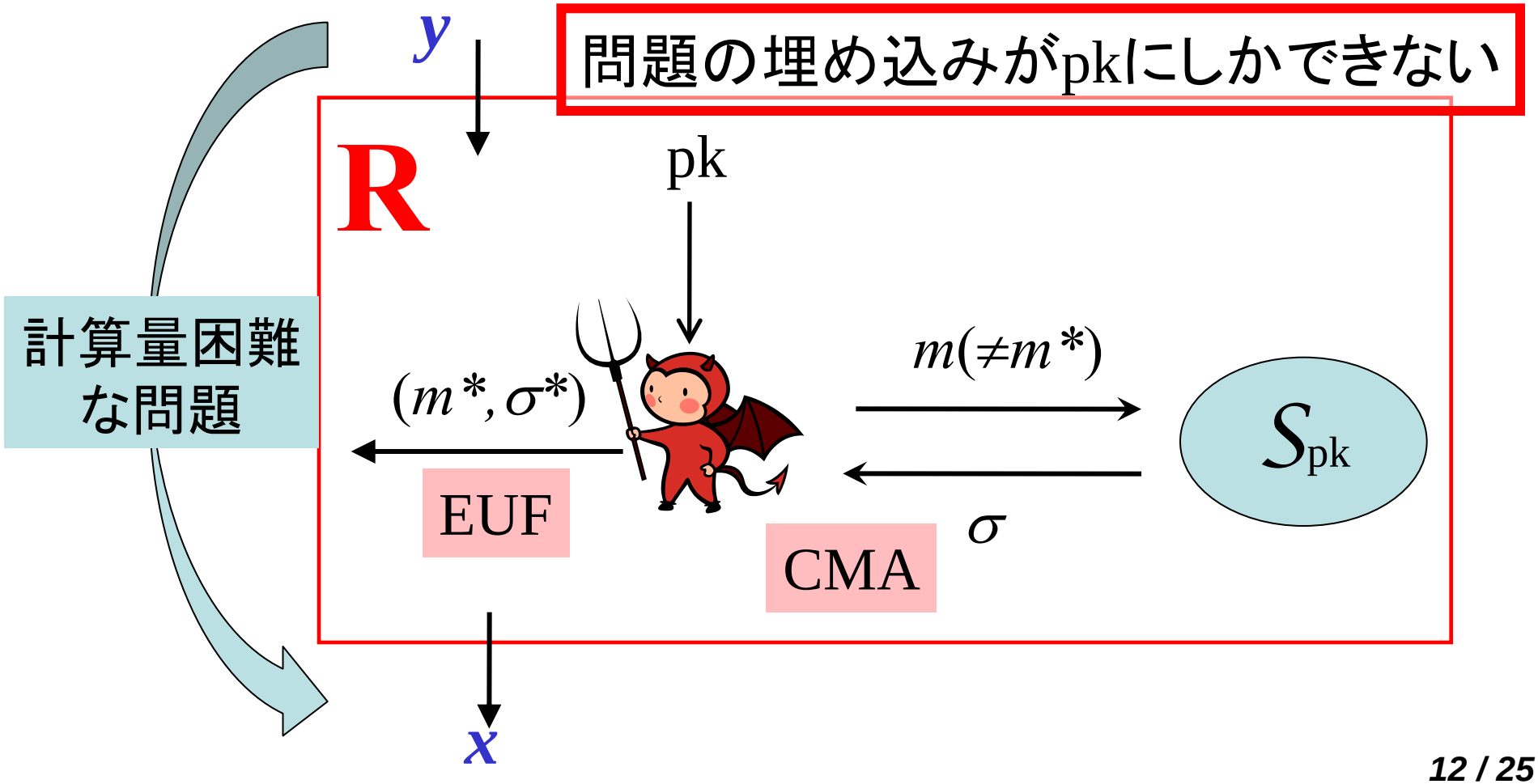
Multi-Key Preserving Black Box Reduction

KPBBを複数ユーザに拡張した帰着



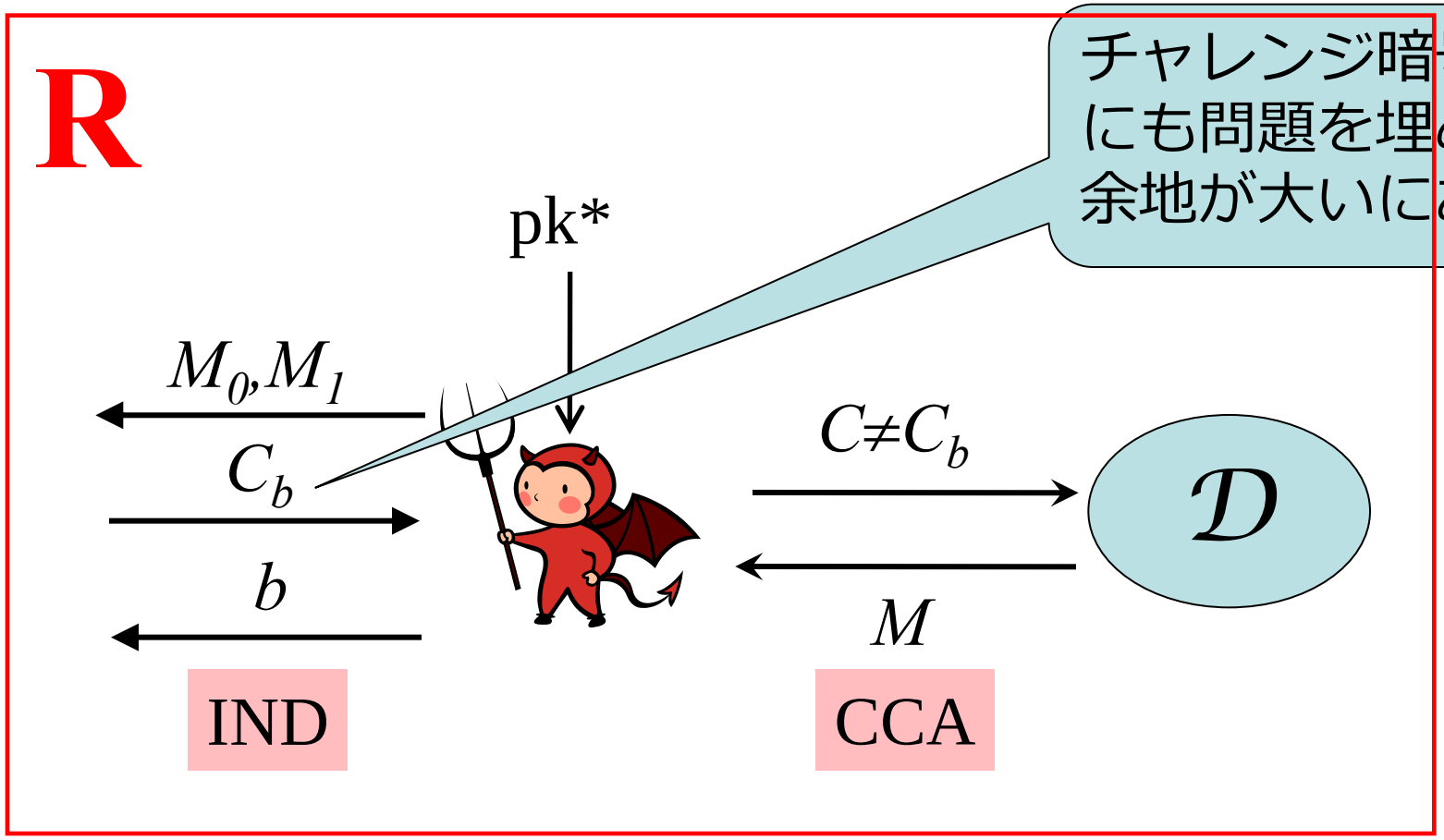
(M)KPBB Reductionの妥当性

署名系だと比較的妥当な仮定



(M)KPBB Reductionの妥当性

暗号系だとあまり妥当でない仮定



主定理

標準モデルにおいて、$\mathrm{CDH} \underset{R}{\Leftarrow} \mathrm{A}^{1}_{\text{EUF-CMA}}$

となる帰着は存在しない（ただし、R^2を2-MKPBB帰着としたとき $R=R^2 \circ I$となるR）

補題1

標準モデルにおいて、CDH $\overset{R^2}{\Leftarrow}$ $A_{\text{EUF-CMA}}$

となる2-MKPBB帰着は存在しない

証明不可能性の(大雑把な)証明方法

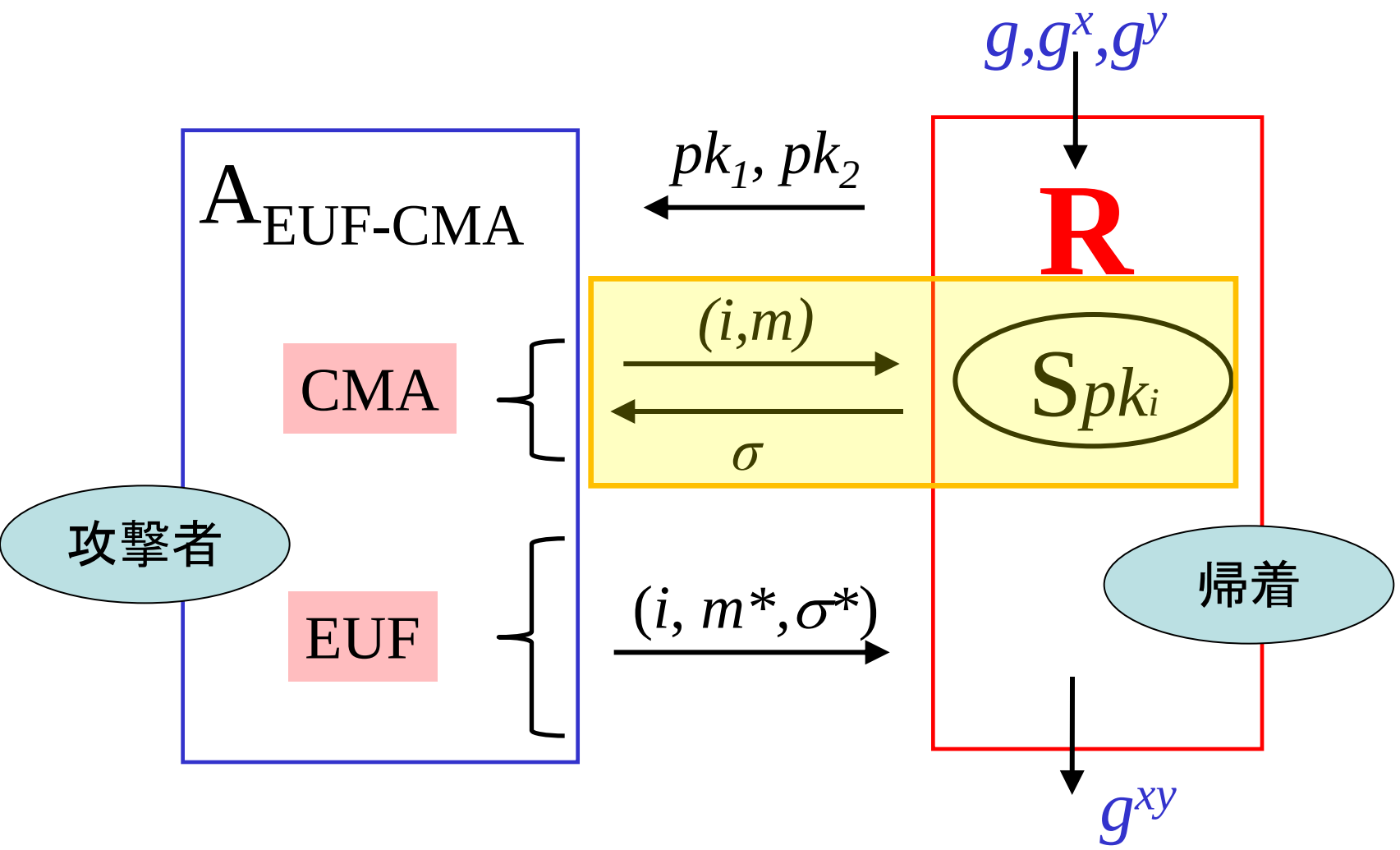
ある計算量仮定の下で**安全性証明できたとする**

⇩

矛盾がある！

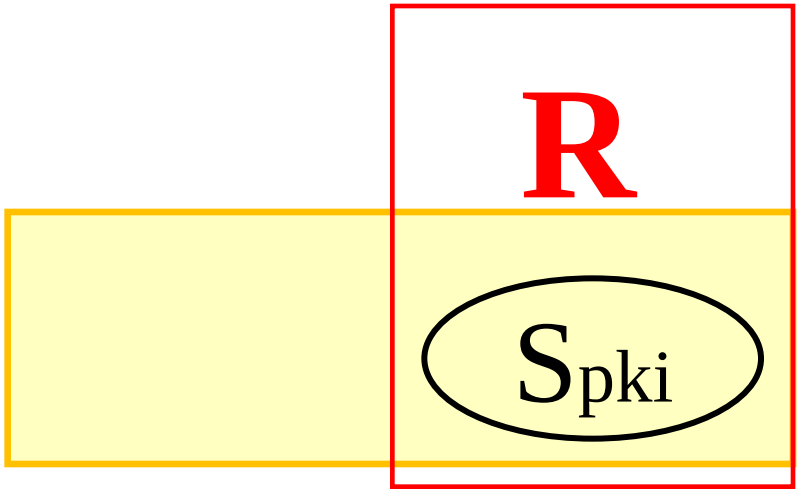
そもそもEUF-CMA安全が証明できるとは…

CDH⇐$A_{EUF\text{-}CMA}$と変換する**R**を構成すること！



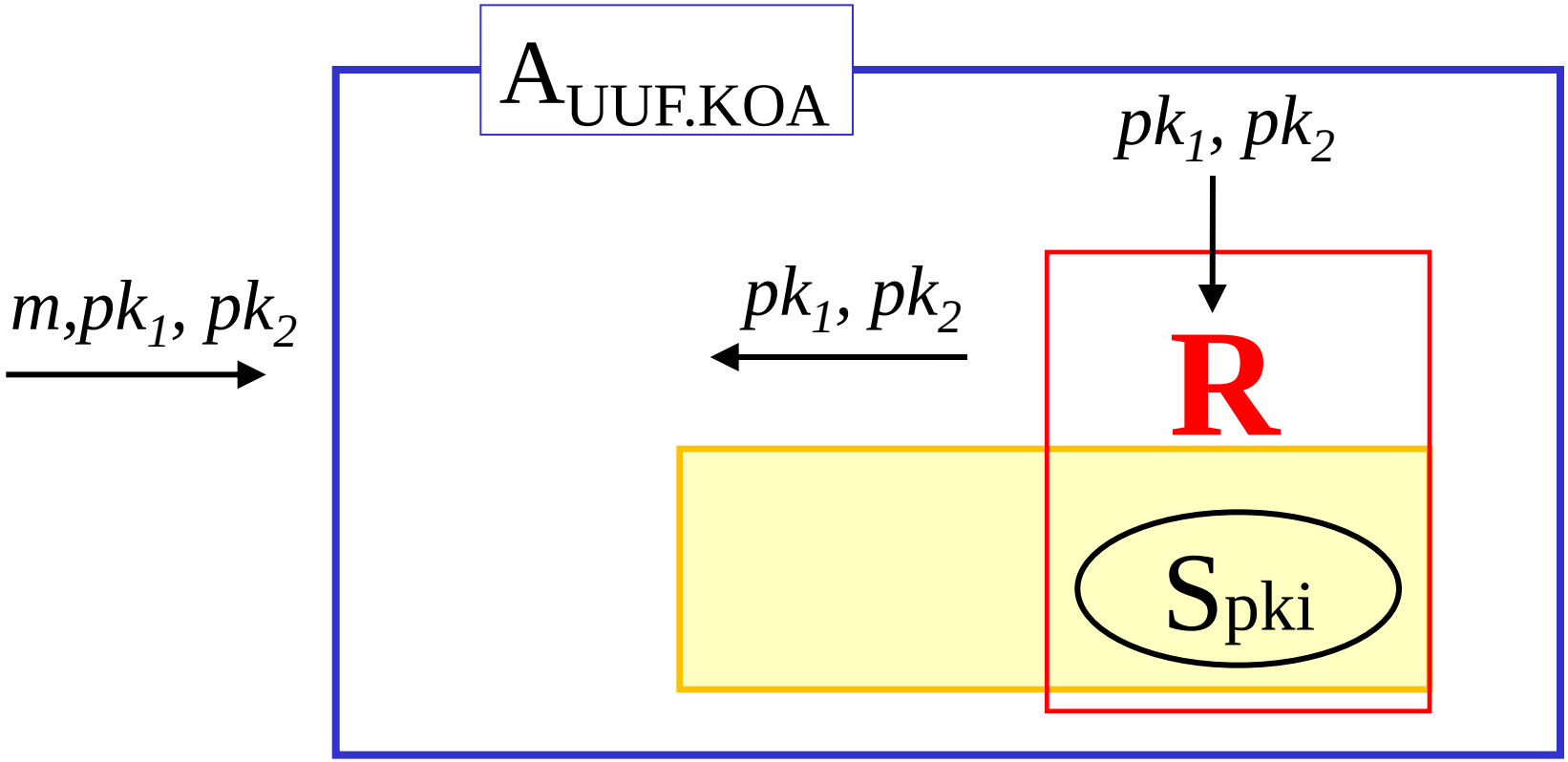
証明不可能性証明

$$\mathrm{CDH} \overset{\mathbf{R}^2}{\Leftarrow} \mathrm{A}_{\mathrm{EUF\text{-}CMA}}$$



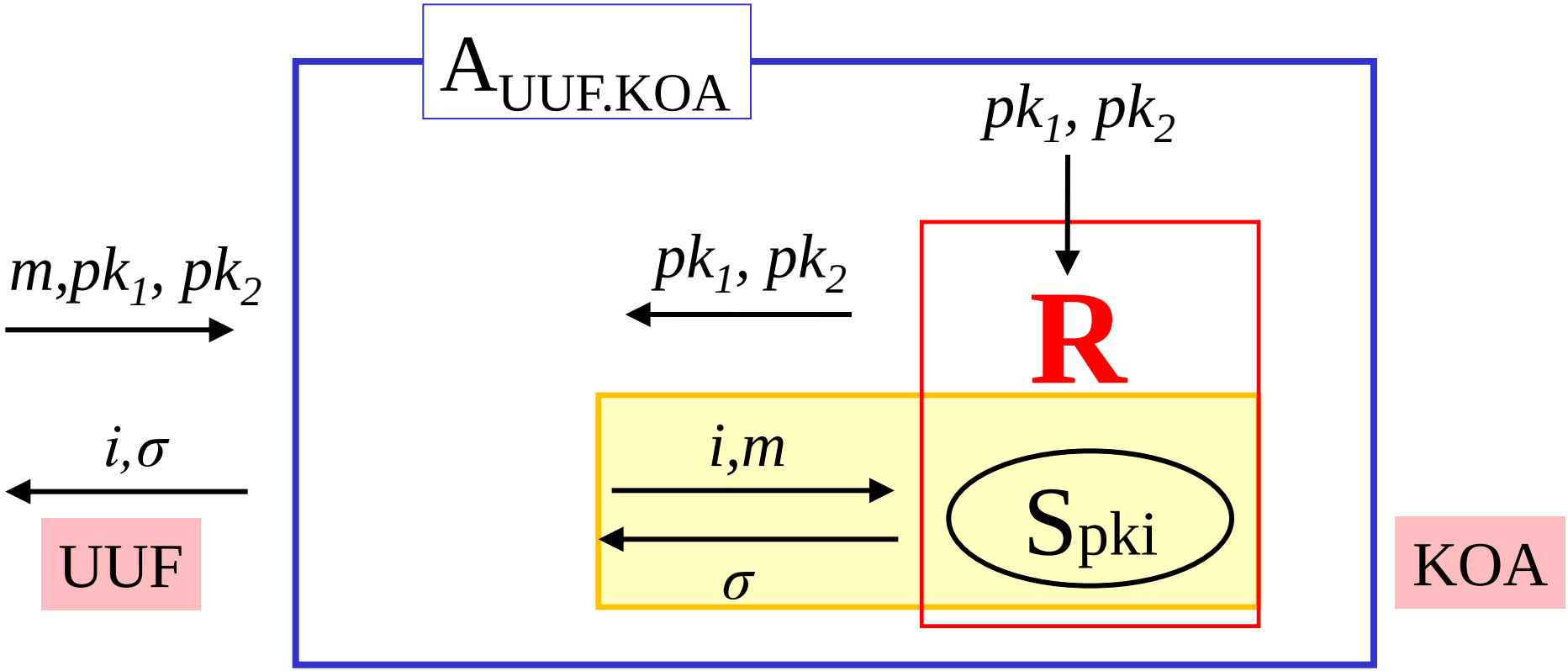
証明不可能性証明

$$\mathrm{CDH} \overset{\mathbf{R}^2}{\Leftarrow} \mathrm{A}_{\mathrm{EUF\text{-}CMA}}$$



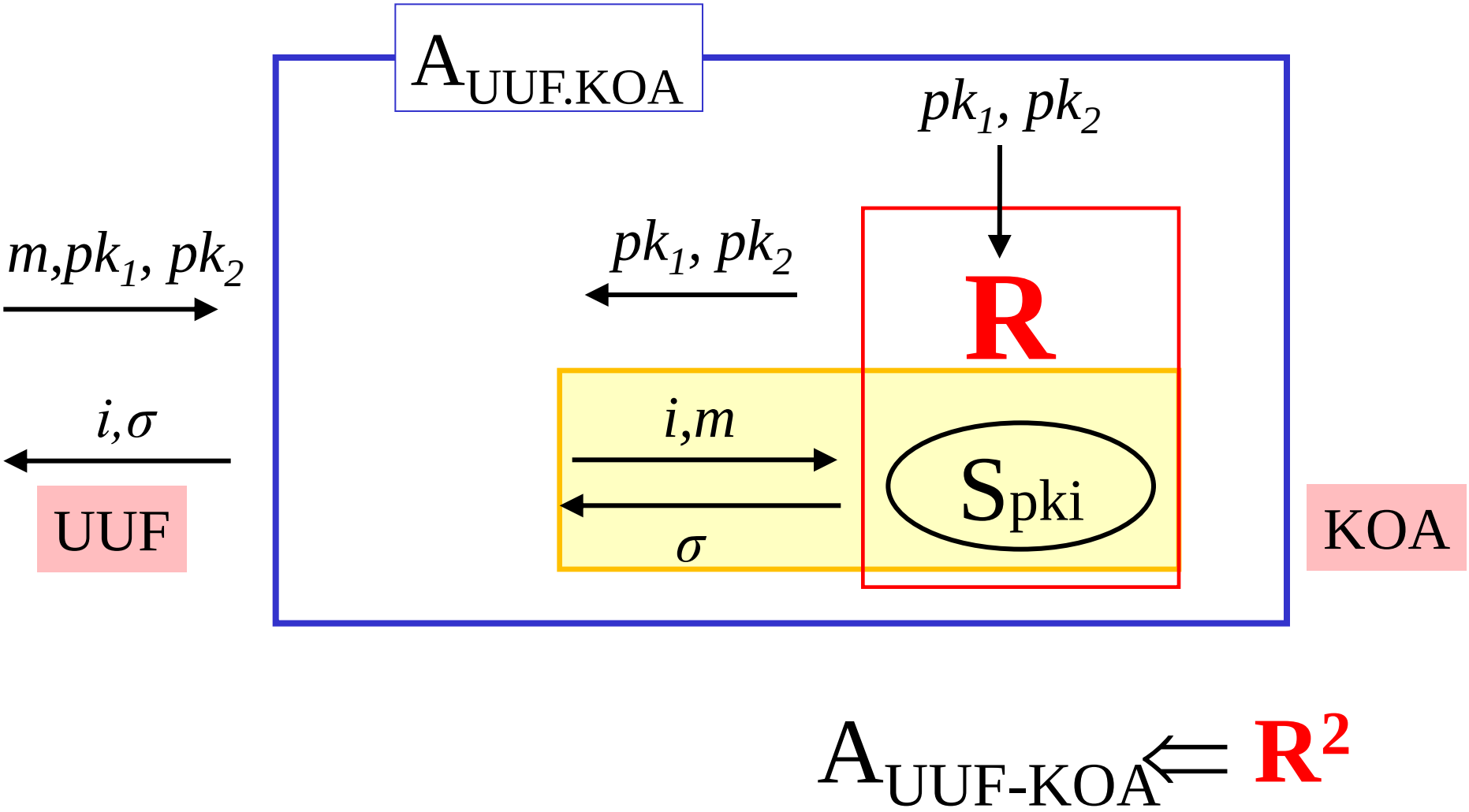
証明不可能性証明

$$\mathrm{CDH} \overset{R^2}{\Leftarrow} \mathrm{A}_{\mathrm{EUF\text{-}CMA}}$$



証明不可能性証明

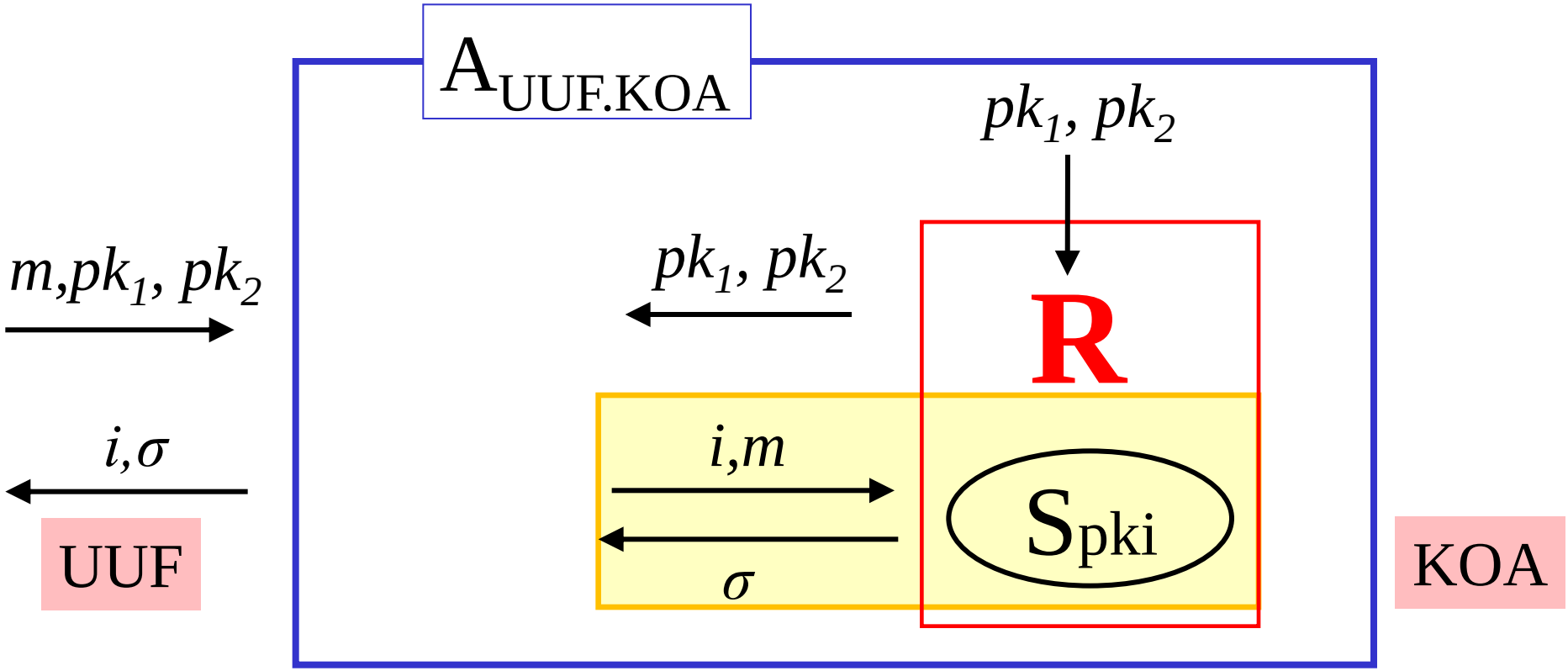
$\mathrm{CDH} \overset{\mathbf{R}^2}{\Leftarrow} \mathrm{A}_{\mathrm{EUF\text{-}CMA}}$



$\mathrm{A}_{\mathrm{UUF\text{-}KOA}} \Leftarrow \mathbf{R}^2$

証明不可能性証明

$$\mathrm{CDH} \overset{R^2}{\Leftarrow} \mathrm{A}_{\mathrm{EUF\text{-}CMA}}$$



$$\mathrm{CDH} \overset{R^2}{\Leftarrow} \mathrm{A}_{\mathrm{EUF\text{-}CMA}} \Leftarrow \mathrm{A}_{\mathrm{UUF\text{-}KOA}} \Leftarrow R^2$$

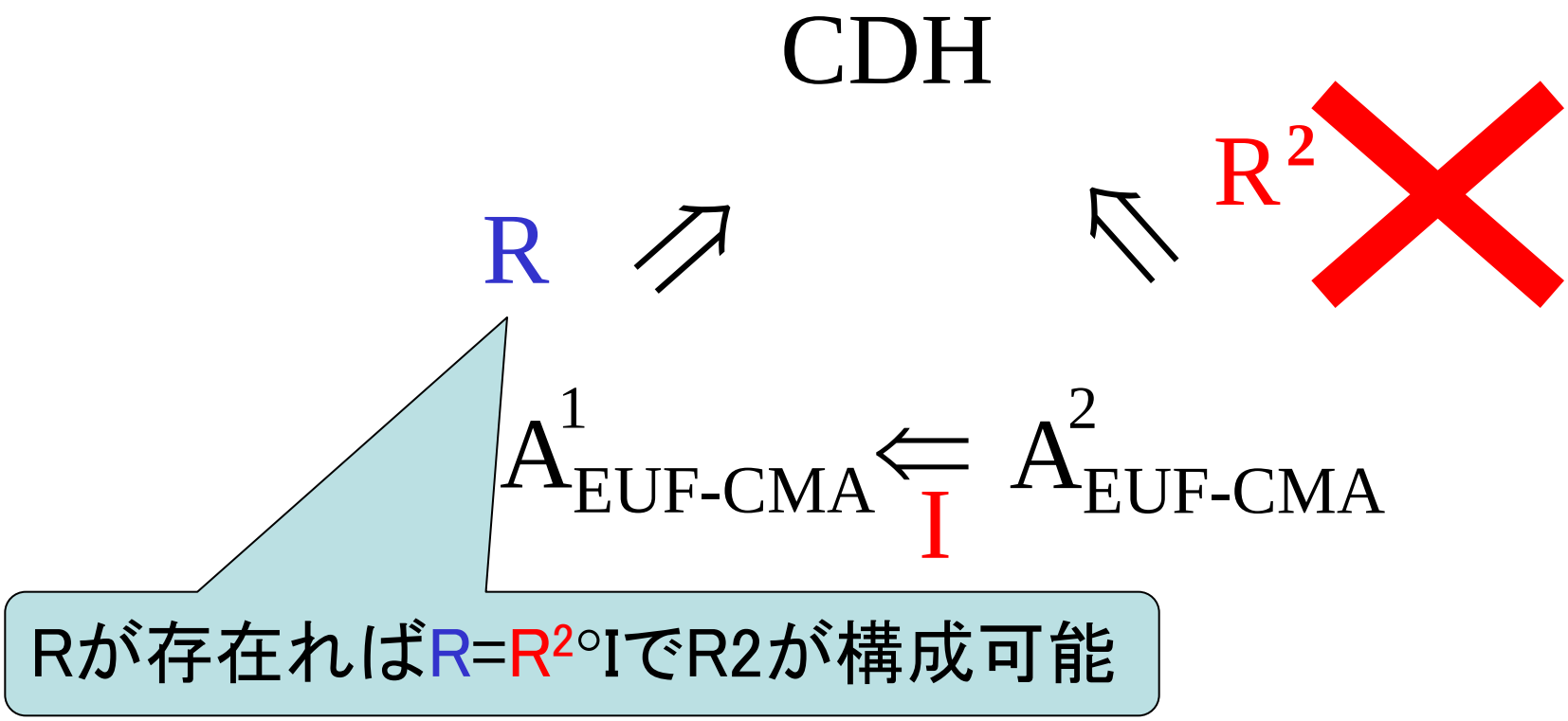
Rが存在するとCDHが解ける⇒**R**は存在しない！

補題2

$A^{1}_{\text{EUF-CMA}} \Leftarrow_{I} A^{2}_{\text{EUF-CMA}}$ となる帰着Iが存在する

一般的に存在する帰着
（個別の方式ではもっと効率のいい方法があるかもしれない）

証明不可能性



まとめと展望

- CDH仮定でのSchnorr署名の証明不可能性に関する一考察を行った
  - DDH, q-SDH, BDHなどにも適用可能
- 否定できる帰着Rに制限がある
  - Iの構成方法で変化する
  - 今のところ、Iはランダムにターゲットを選ぶ帰着のみ

今後の課題

- Key Preserving 以外のConceptで証明不可能性を示す
  - 帰着に何の制約も持たせない証明不可能性は示すのがかなり難しそう
  - 帰着の演算に制限を加えた帰着でCDH過程に対する証明不可能性を示す（DLはこれで成功している）
- 一般化したい
  - 対象とする問題を一般化したい
  - DDHはCDHのときと証明の仕方が異なるため、単純な一般化ができていない