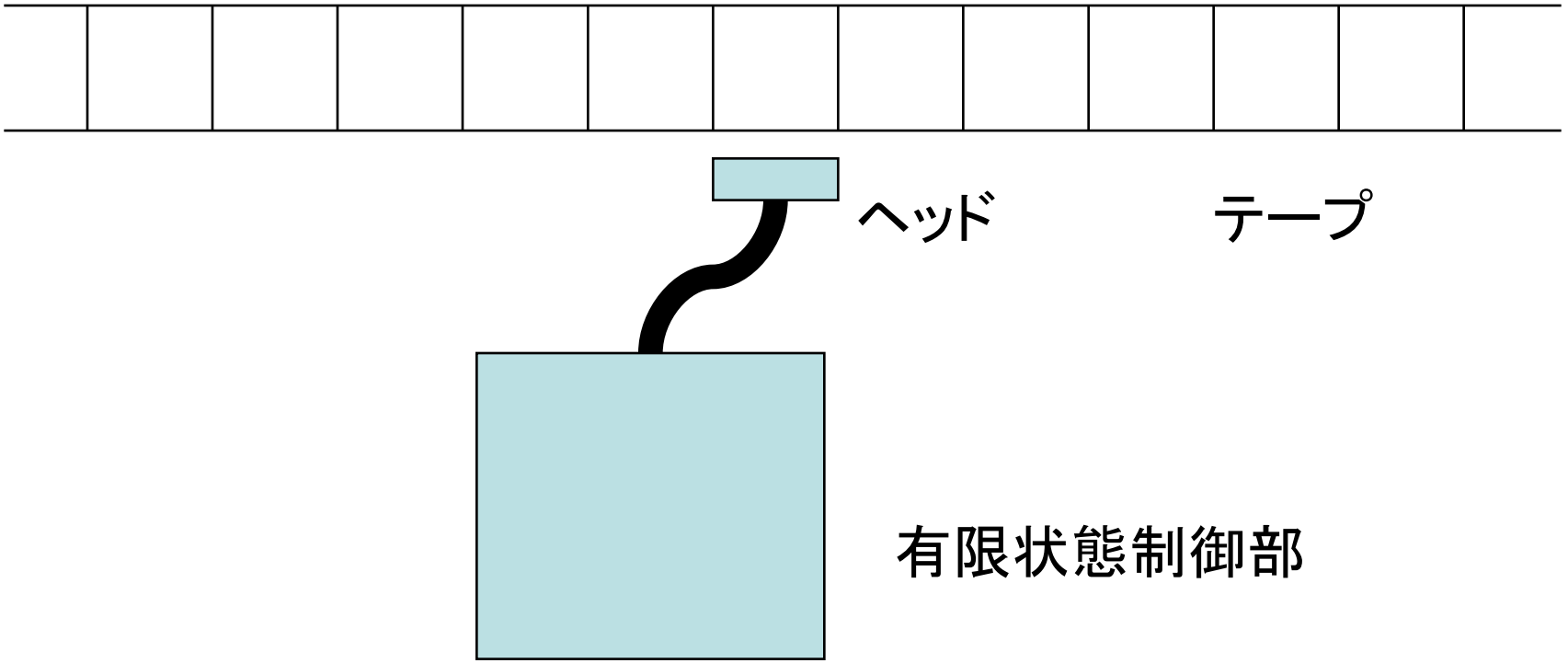
暗号化スキームとプロトコルの安全性

あらまし

- 確率的多項式時間チューリング機械
- 暗号化スキームの安全性
  - IND-CPA 安全性
    - Negligible とは？
  - IND-CCA 安全性
- Needham-Schroeder の安全性
  (レスポンダになりすますことはできない)
  - Needham-Schroeder 再び
  - イニシエータが1人だけいる場合 --- IND-CPA を仮定
  - レスポンダも1人だけいる場合 --- IND-CCA2 を仮定

チューリング機械



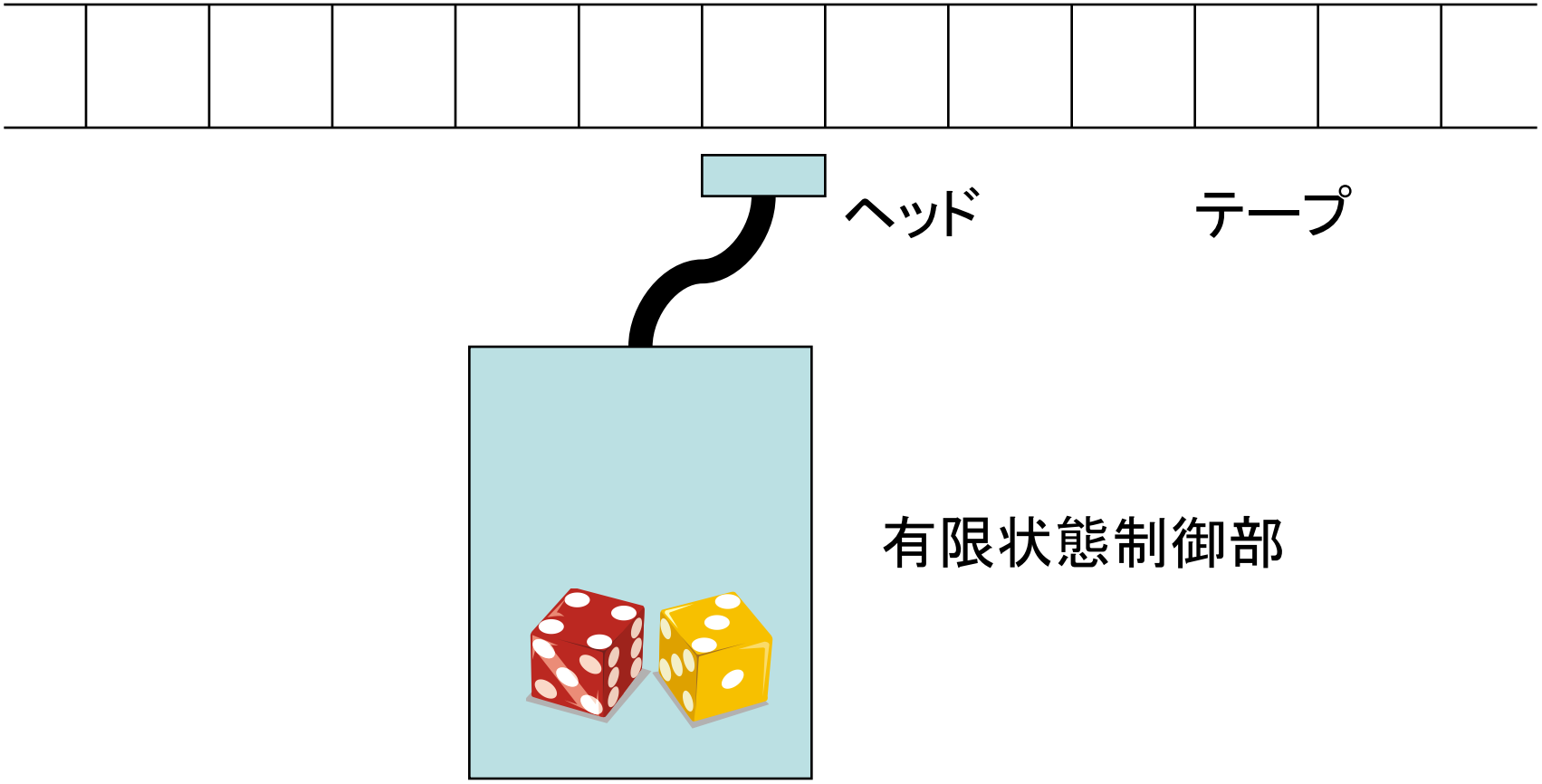
チューリング機械の遷移:

(現在の状態, ヘッドが読む文字) →
(次の状態, ヘッドが書く文字, ヘッドの移動方向)

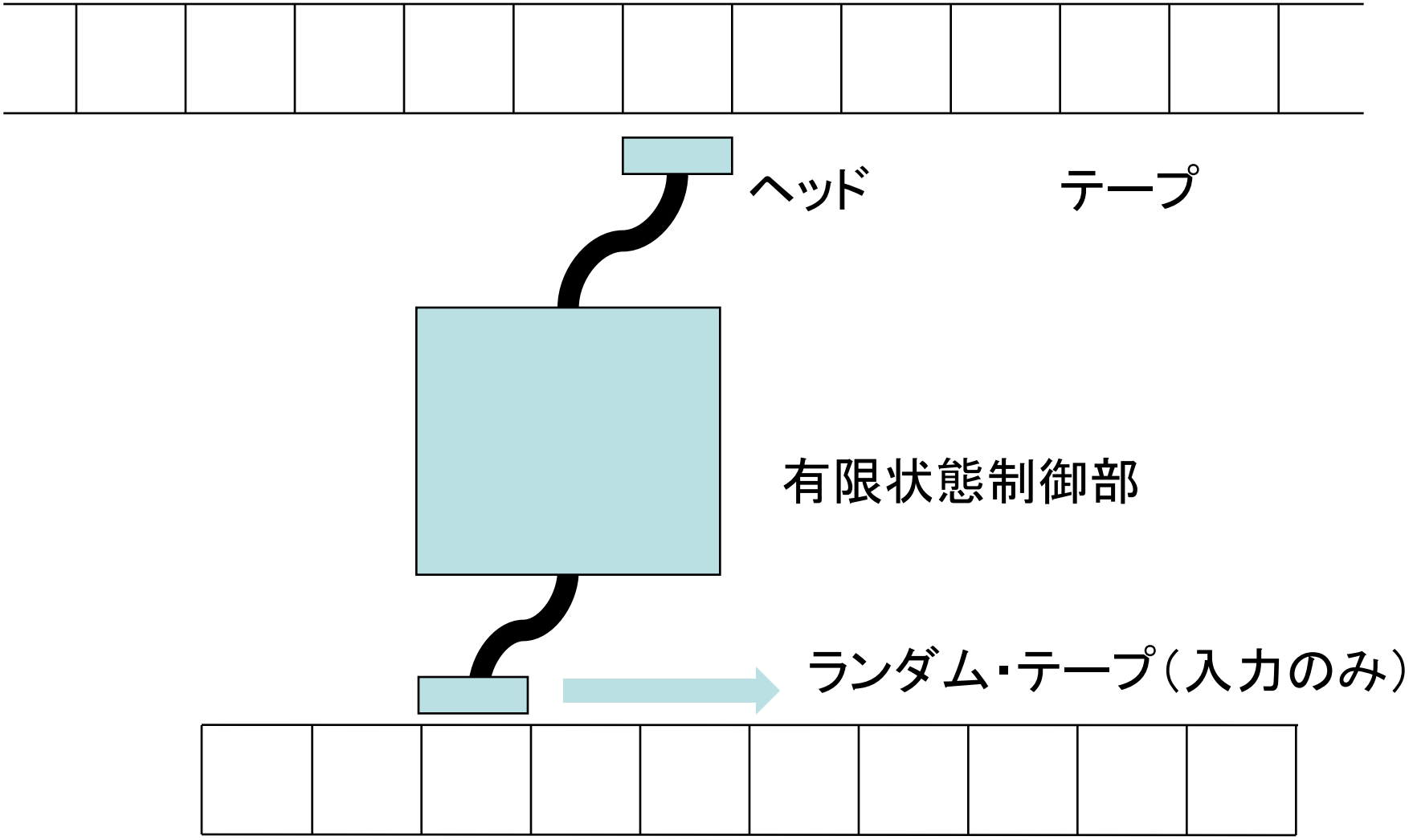
決定性 vs. 非決定性 vs. 確率的

- 決定性
  - 個々の対 (現在の状態, ヘッドが読む文字) に対して、遷移 (次の状態, ヘッドが書く文字, ヘッドの移動方向) が一意的。
- 非決定性
  - 遷移が必ずしも一意的でない。
- 確率的
  - いくつかの遷移の選択肢の中から、サイコロを振って決める。

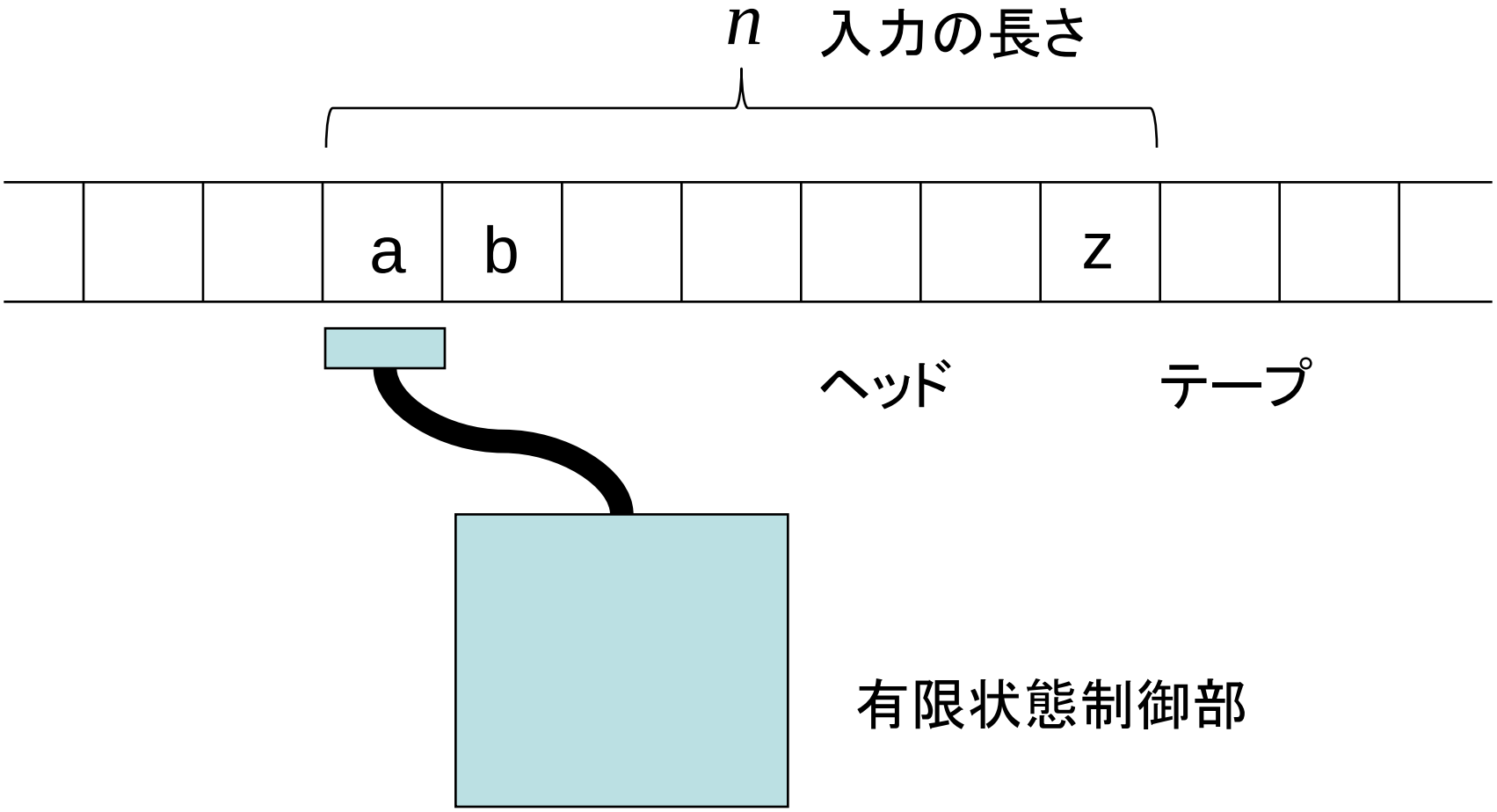
確率的チューリング機械



確率的チューリング機械

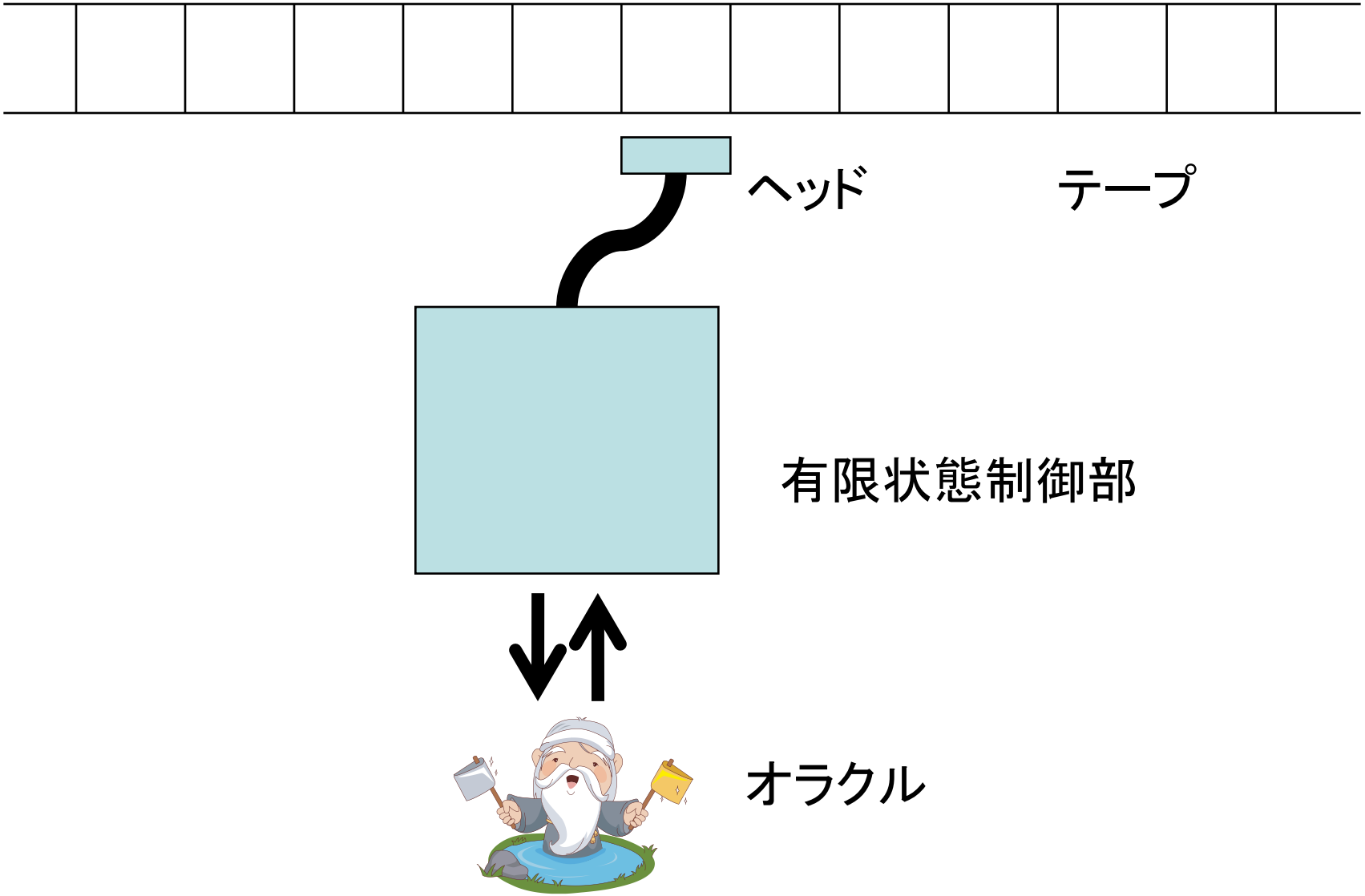


多項式時間チューリング機械

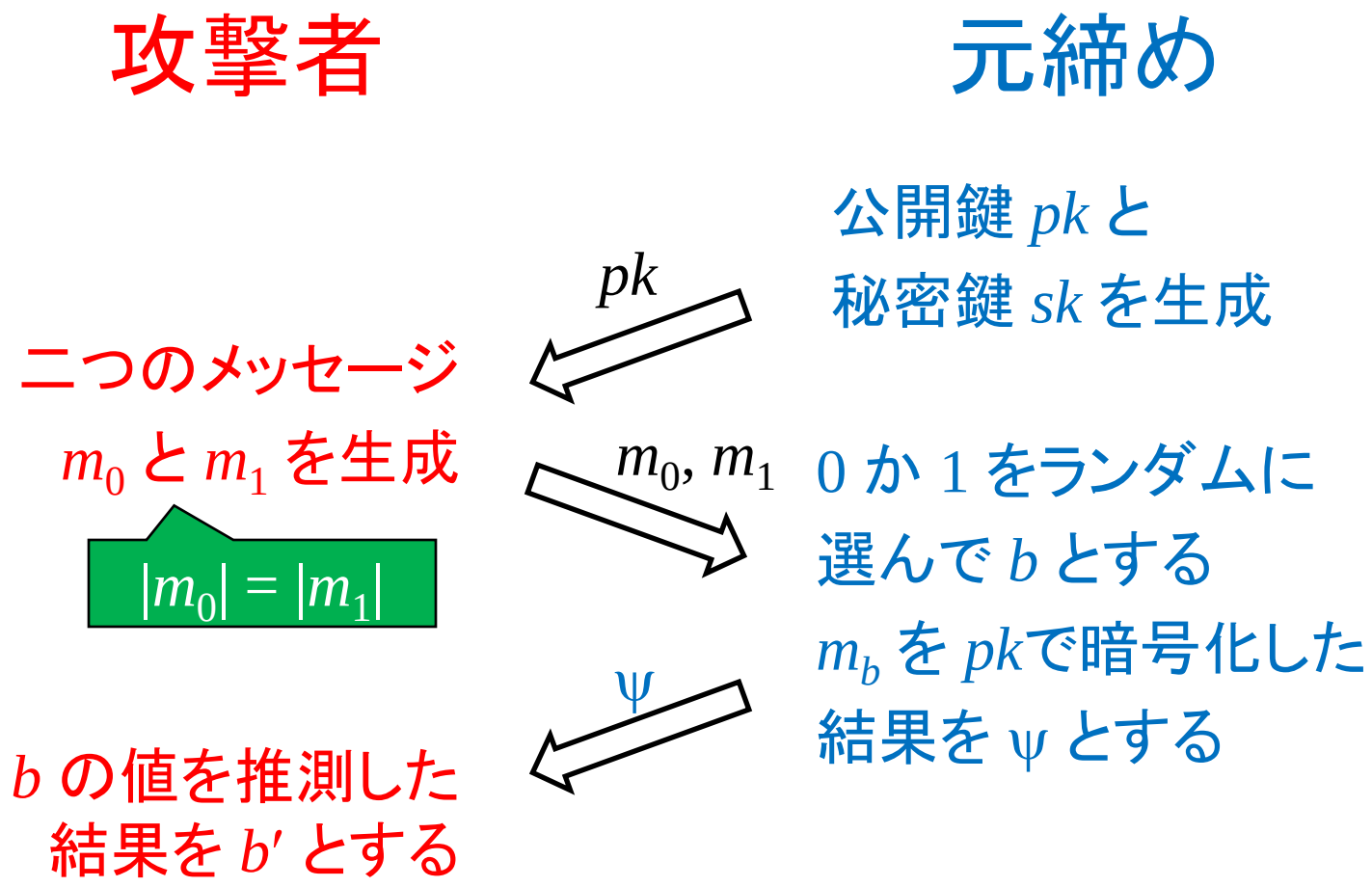


$p(n)$ ステップで終了 --- $p(n)$ は n の多項式

オラクル付きチューリング機械

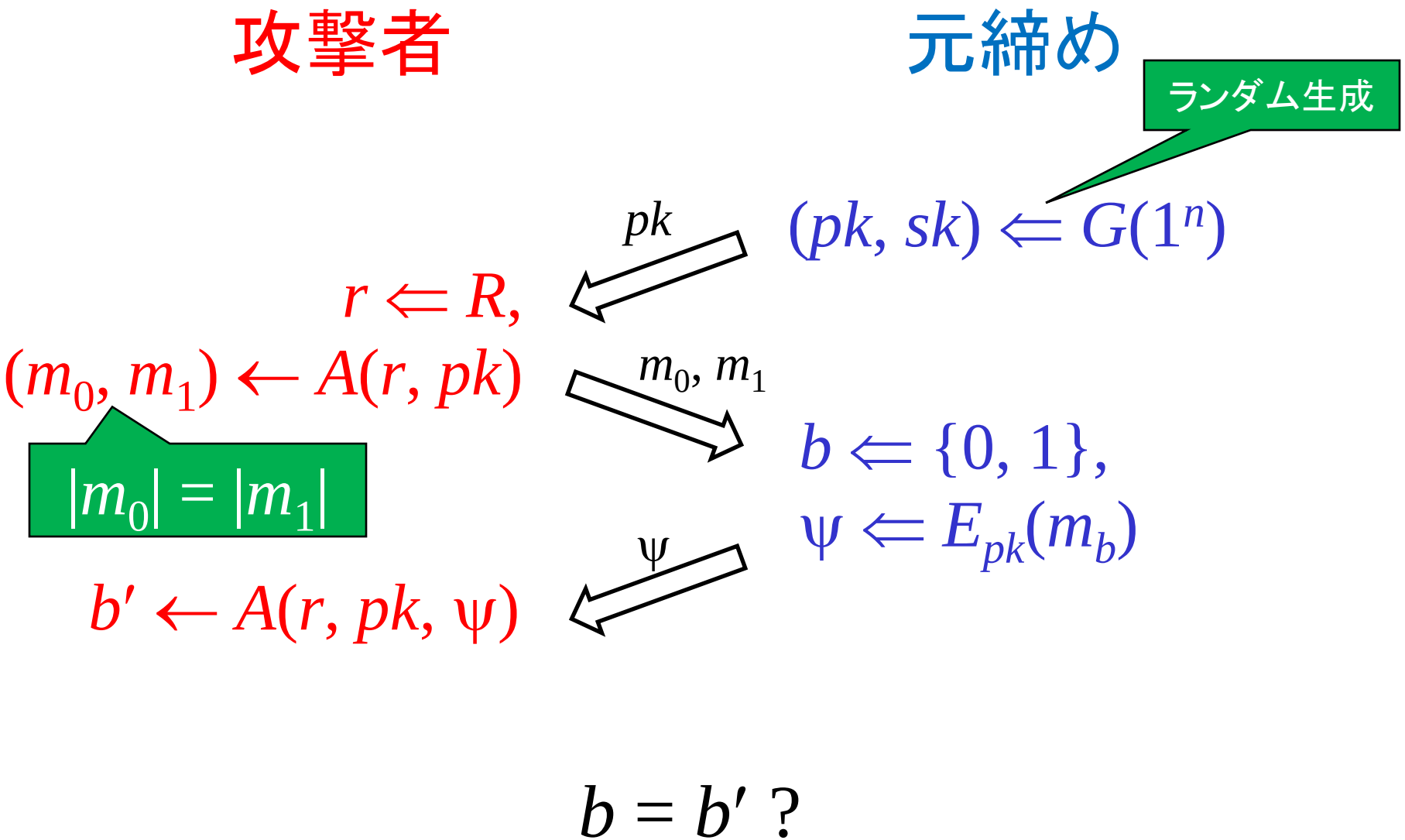


IND-CPA ゲーム



$$b = b' \ ?$$

IND-CPA ゲーム



$b = b'$?

IND-CPA ゲーム

攻撃者

$r \Leftarrow R,$

r はランダム・テープ

$(m_0, m_1) \leftarrow A(r, pk)$

A は pk を入力とし、
r をランダム・テープとする
確率的多項式時間チューリング機械

$|m_0| = |m_1|$

$b' \leftarrow A(r, pk, \psi)$

同じく A と書いてあるが、
別の確率的多項式時間チューリング機械で
b' を出力

IND-CPA ゲーム

- 元締め : $(pk, sk) \Leftarrow G(1^n)$
- 攻撃者 : $r \Leftarrow R,\ (m_0, m_1) \leftarrow A(r, pk)$
- 元締め : $b \Leftarrow \{0, 1\},\ \psi \Leftarrow E_{pk}(m_b)$
- 攻撃者 : $b' \leftarrow A(r, pk, \psi)$

$|m_0| = |m_1|$

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

Negligible とは？

- 関数 $\nu(n)$ が negligible であるとは、任意の多項式 $p(n)$ に対して、ある N が存在して、$n > N$ ならば $\nu(n) < 1/p(n)$ となること。
  - 十分大きな n に対して（for all sufficiently large n）、$\nu(n) < 1/p(n)$
- n はセキュリティ・パラメタ。たとえば、鍵の長さ。

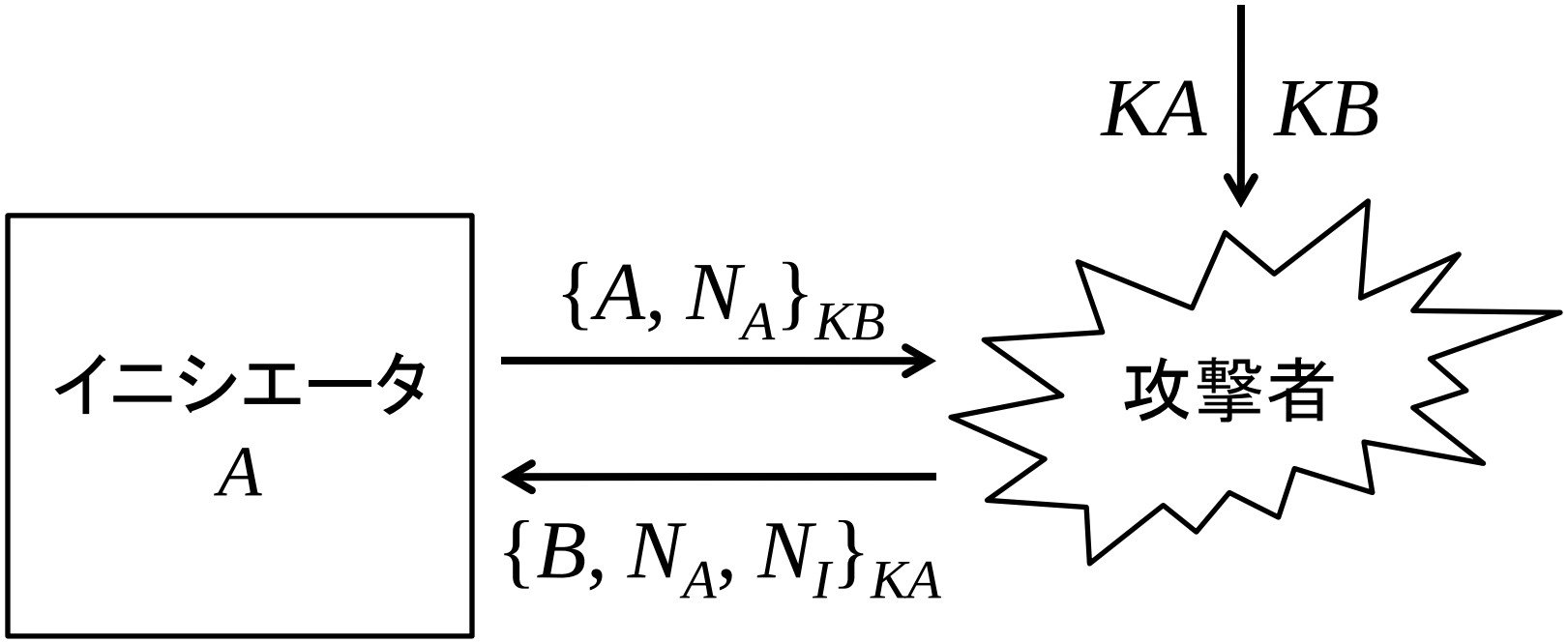
修正されたプロトコル

- Needham-Schroeder-Lowe

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

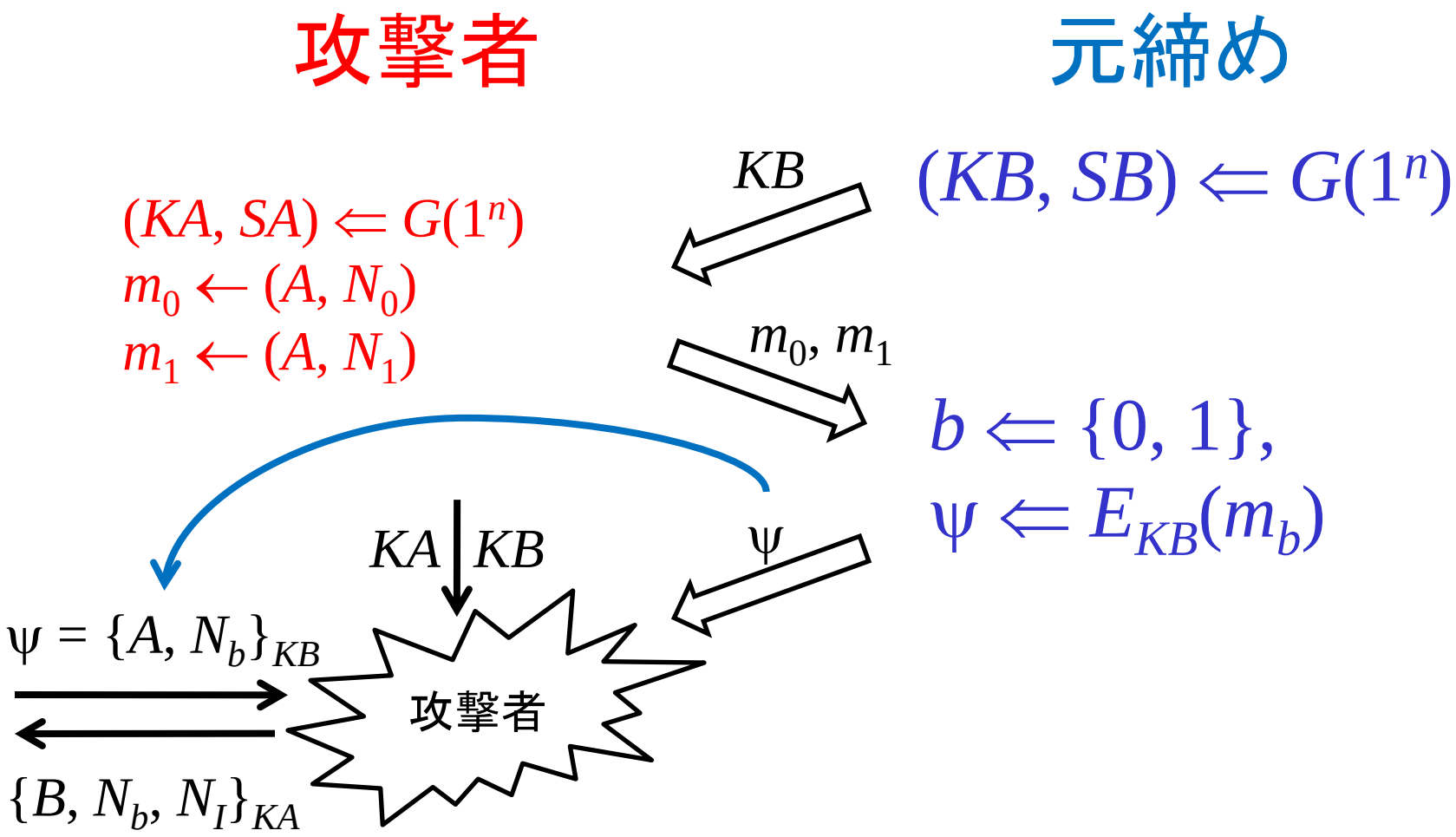
- レスポンダ B になりすませるか？

イニシエータが 1 人だけいる場合



レスポンダはいない

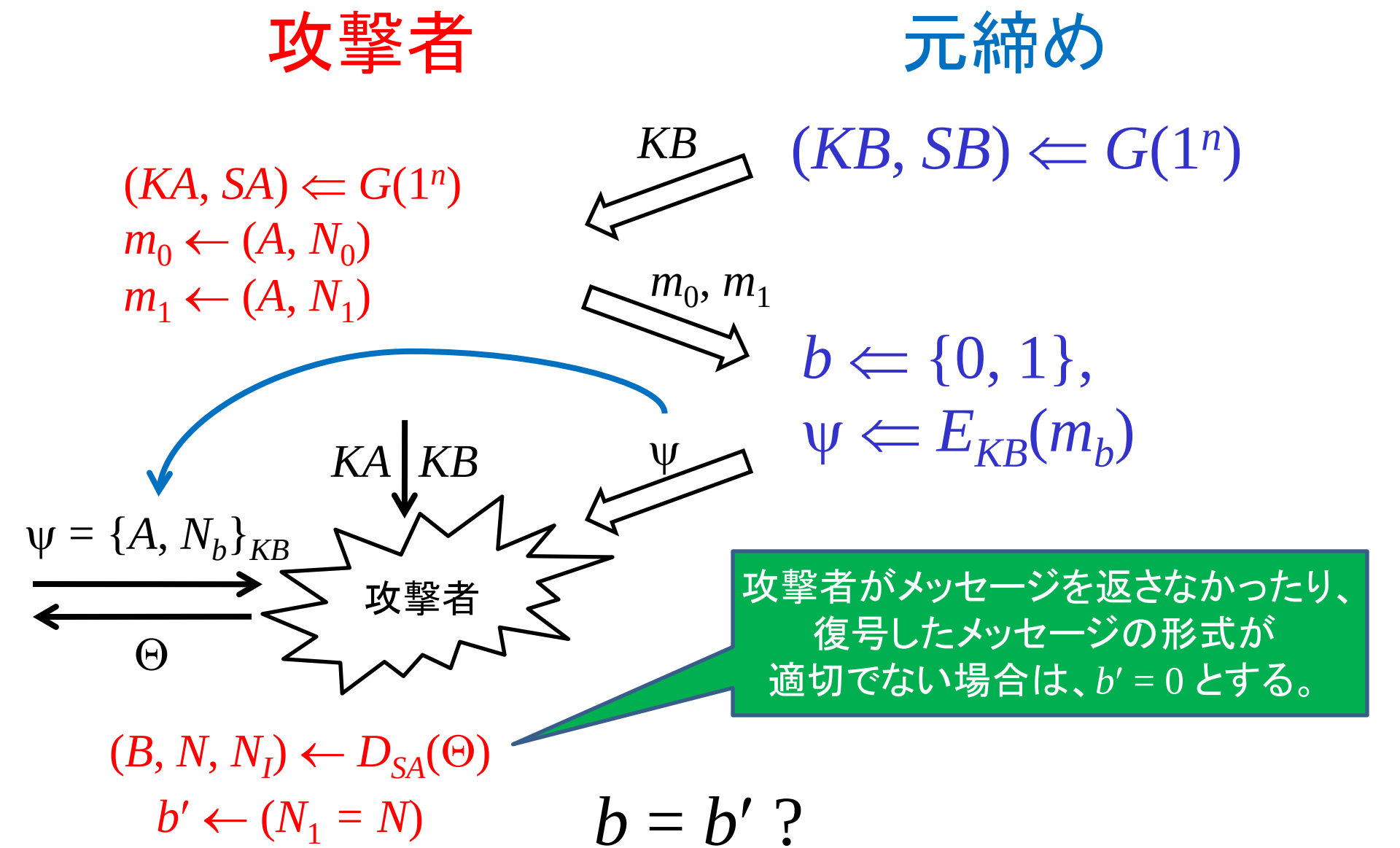
IND-CPA ゲーム


攻撃者
元締め
$(KA, SA) \Leftarrow G(1^n)$
$m_0 \leftarrow (A, N_0)$
$m_1 \leftarrow (A, N_1)$
KB
$(KB, SB) \Leftarrow G(1^n)$
m_0, m_1
$b \Leftarrow \{0, 1\},$
$\psi \Leftarrow E_{KB}(m_b)$
KA KB
ψ
$\psi = \{A, N_b\}_{KB}$
攻撃者
$\{B, N_b, N_I\}_{KA}$
$(B, N_b, N_I) \leftarrow D_{SA}(\{B, N_b, N_I\}_{KA})$
$b' \leftarrow (N_1 = N_b)$
$b = b'$?

議論

- N_0 と N_1 はどちらもランダムに作られるので対称的。
- 攻撃者がなりすましに成功する確率を p とすると、N_b が N_0 に等しい確率は $p/2$、N_b が N_1 に等しい確率も $p/2$。どちらの場合も、$b = b'$ が成り立つ。この確率は p。
- どちらでもない場合、$N_1 = N_b$ は成り立たないので、$b' = 0$。このとき、$b = 0$ と $b = 1$ は等確率なので、$b = b'$ が成り立つ確率は $(1–p)/2$。
- 結局、$b = b'$ が成り立つ確率は $1/2 + p/2$。

IND-CPA ゲーム


攻撃者
元締め
$(KA, SA) \Leftarrow G(1^n)$
$m_0 \leftarrow (A, N_0)$
$m_1 \leftarrow (A, N_1)$
KB
$(KB, SB) \Leftarrow G(1^n)$
m_0, m_1
$b \Leftarrow \{0, 1\},$
$\psi \Leftarrow E_{KB}(m_b)$
KA KB
ψ
$\psi = \{A, N_b\}_{KB}$
攻撃者
Θ
攻撃者がメッセージを返さなかったり、
復号したメッセージの形式が
適切でない場合は、$b' = 0$ とする。
$(B, N, N_I) \leftarrow D_{SA}(\Theta)$
$b' \leftarrow (N_1 = N)$
$b = b'$?

レスポンダも１人だけいる場合

二つの場合：

1. 攻撃者は、$\{A, N_A\}_{KB}$ をそのままレスポンダに転送。
2. そうでない場合。

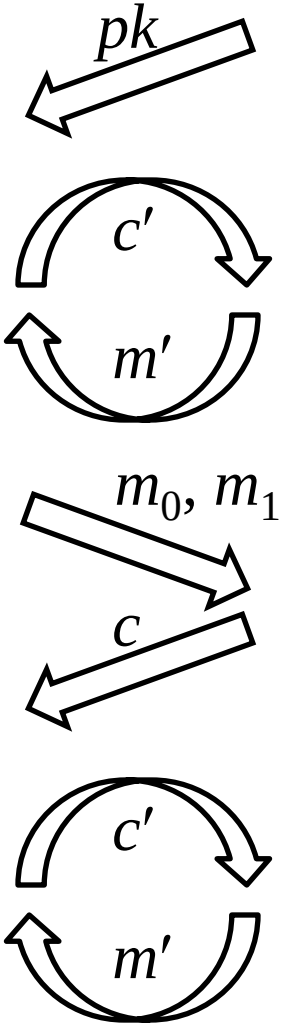
レスポンダも１人だけいる場合

- 元締めが二つの鍵対を生成するようなゲームを考えれば、どちらの場合にも対処できるが、ここでは、先の IND-CPA の例との類似から、二番目の場合のみ考える。

IND-CCA2 ゲーム

攻撃者

元締め



公開鍵 pk と
秘密鍵 sk を生成

c' を復号した結果
m' を送る

0 か 1 をランダムに
選んで b とする
m_b を pkで暗号化した
結果を c とする

c' を復号した結果
m' を送る

二つのメッセージ
m_0 と m_1 を生成

$|m_0| = |m_1|$

c 以外のメッセージ
c' を送る

b の値を推測した
結果を b' とする

$b = b'$?

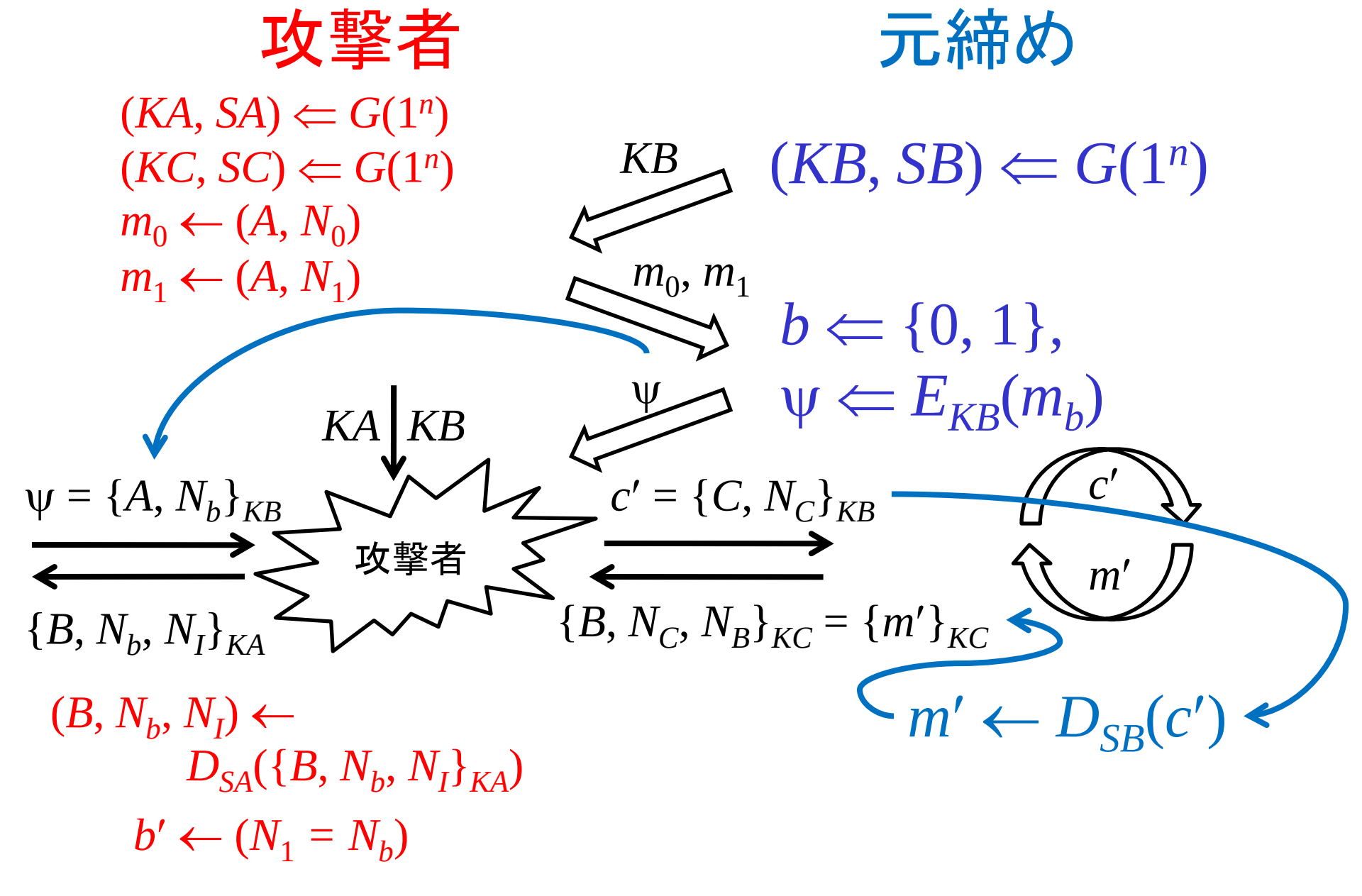
IND-CCA2 ゲーム

- 元締め : $(pk, sk) \Leftarrow G(1^n)$

  $D_{sk}(\cdot)$: 復号オラクル
- 攻撃者 : $r \Leftarrow R,\ (m_0, m_1) \leftarrow A^{D_{sk}}(r, pk)$ $|m_0| = |m_1|$
- 元締め : $b \Leftarrow \{0, 1\},\ \psi \Leftarrow E_{pk}(m_b)$
- 攻撃者 : $b' \leftarrow A^{D_{sk}}(r, pk, \psi)$

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

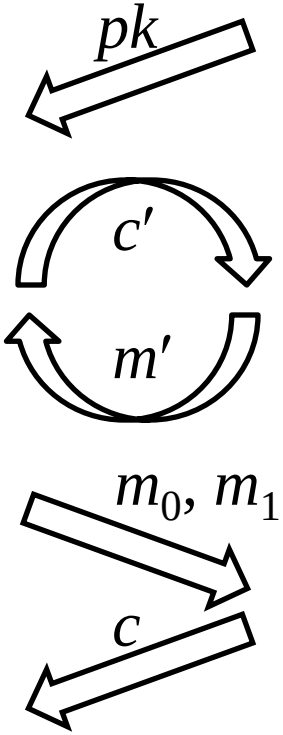
IND-CCA2 ゲーム


攻撃者
元締め
$(KA, SA) \Leftarrow G(1^n)$
$(KC, SC) \Leftarrow G(1^n)$
$m_0 \leftarrow (A, N_0)$
$m_1 \leftarrow (A, N_1)$
KB
$(KB, SB) \Leftarrow G(1^n)$
m_0, m_1
$b \Leftarrow \{0, 1\},$
$\psi \Leftarrow E_{KB}(m_b)$
ψ
KA KB
$\psi = \{A, N_b\}_{KB}$
$c' = \{C, N_C\}_{KB}$
c'
m'
攻撃者
$\{B, N_b, N_I\}_{KA}$
$\{B, N_C, N_B\}_{KC} = \{m'\}_{KC}$
$(B, N_b, N_I) \leftarrow$
$D_{SA}(\{B, N_b, N_I\}_{KA})$
$m' \leftarrow D_{SB}(c')$
$b' \leftarrow (N_1 = N_b)$

IND-CCA1 ゲーム

攻撃者

元締め



公開鍵 pk と
秘密鍵 sk を生成

c' を復号した結果
m' を送る

0 か 1 をランダムに
選んで b とする
m_b を pkで暗号化した
結果を c とする

二つのメッセージ
m_0 と m_1 を生成

$|m_0| = |m_1|$

b の値を推測した
結果を b' とする

$b = b'$?

IND-CCA1 ゲーム

- 元締め : $(pk, sk) \Leftarrow G(1^n)$

  $D_{sk}(\cdot)$: 復号オラクル
- 攻撃者 : $r \Leftarrow R,\ (m_0, m_1) \leftarrow A^{D_{sk}}(r, pk)$ $|m_0| = |m_1|$
- 元締め : $b \Leftarrow \{0, 1\},\ \psi \Leftarrow E_{pk}(m_b)$
- 攻撃者 : $b' \leftarrow A(r, pk, \psi)$

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

Private-Key の場合の IND-CPA ゲーム

- 元締め : $(pk, sk) \Leftarrow G(1^n)$

  $E_{pk}(\cdot)$: 暗号化オラクル
- 攻撃者 : $r \Leftarrow R,\ (m_0, m_1) \leftarrow A^{E_{pk}}(r, 1^n)$ $|m_0| = |m_1|$
- 元締め : $b \Leftarrow \{0, 1\},\ \psi \Leftarrow E_{pk}(m_b)$
- 攻撃者 : $b' \leftarrow A^{E_{pk}}(r, 1^n, \psi)$

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

Private-Key の場合の IND-CCA1 ゲーム

- 元締め : $(pk, sk) \Leftarrow G(1^n)$

  $E_{pk}(\cdot)$: 暗号化オラクル

  $D_{sk}(\cdot)$: 復号オラクル

  $|m_0| = |m_1|$

- 攻撃者 : $r \Leftarrow R,\ (m_0, m_1) \leftarrow A^{E_{pk}, D_{sk}}(r, 1^n)$
- 元締め : $b \Leftarrow \{0, 1\},\ \psi \Leftarrow E_{pk}(m_b)$
- 攻撃者 : $b' \leftarrow A^{E_{pk}}(r, 1^n, \psi)$

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

Private-Key の場合の IND-CCA2 ゲーム

- 元締め : $(pk, sk) \Leftarrow G(1^n)$

  $E_{pk}(\cdot)$: 暗号化オラクル

  $D_{sk}(\cdot)$: 復号オラクル

  $|m_0| = |m_1|$

- 攻撃者 : $r \Leftarrow R,\ (m_0, m_1) \leftarrow A^{E_{pk}, D_{sk}}(r, 1^n)$
- 元締め : $b \Leftarrow \{0, 1\},\ \psi \Leftarrow E_{pk}(m_b)$
- 攻撃者 : $b' \leftarrow A^{E_{pk}, D_{sk}}(r, 1^n, \psi)$

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