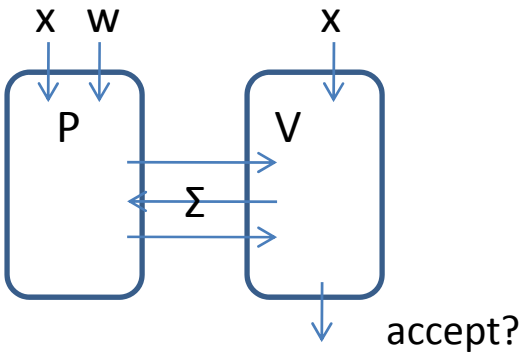
Σプロトコル入門

08.04.21

IISEC 有田 正剛

はじめに

- Σプロトコルとは？
  ある問題xの答えwを知っていることを証明するためのプロトコル。
  ただし、答えwそのものを教えたくない。



- Σプロトコル を用いて
  認証プロトコル、署名スキーム、コミットメントプロトコル
  その他が構成できる。

準備

- **PPTとEPT**
  - PPT: Probabilistic Polynomial Time, "効率的"
  - EPT: Expected Polynomial Time, "平均的には効率的"

- **関係R**
  - $R = \{(x,w)\} \subset \{0,1\}^* \times \{0,1\}^*$, x:問題, w:答え
  - あるPPTアルゴリズムRで $(x,w) \in^? R$ を判定可能
  - あるPPTアルゴリズムGがあってサンプル可能
    $(x, w) \leftarrow G(k), |x|=k, R(x,w)=1$

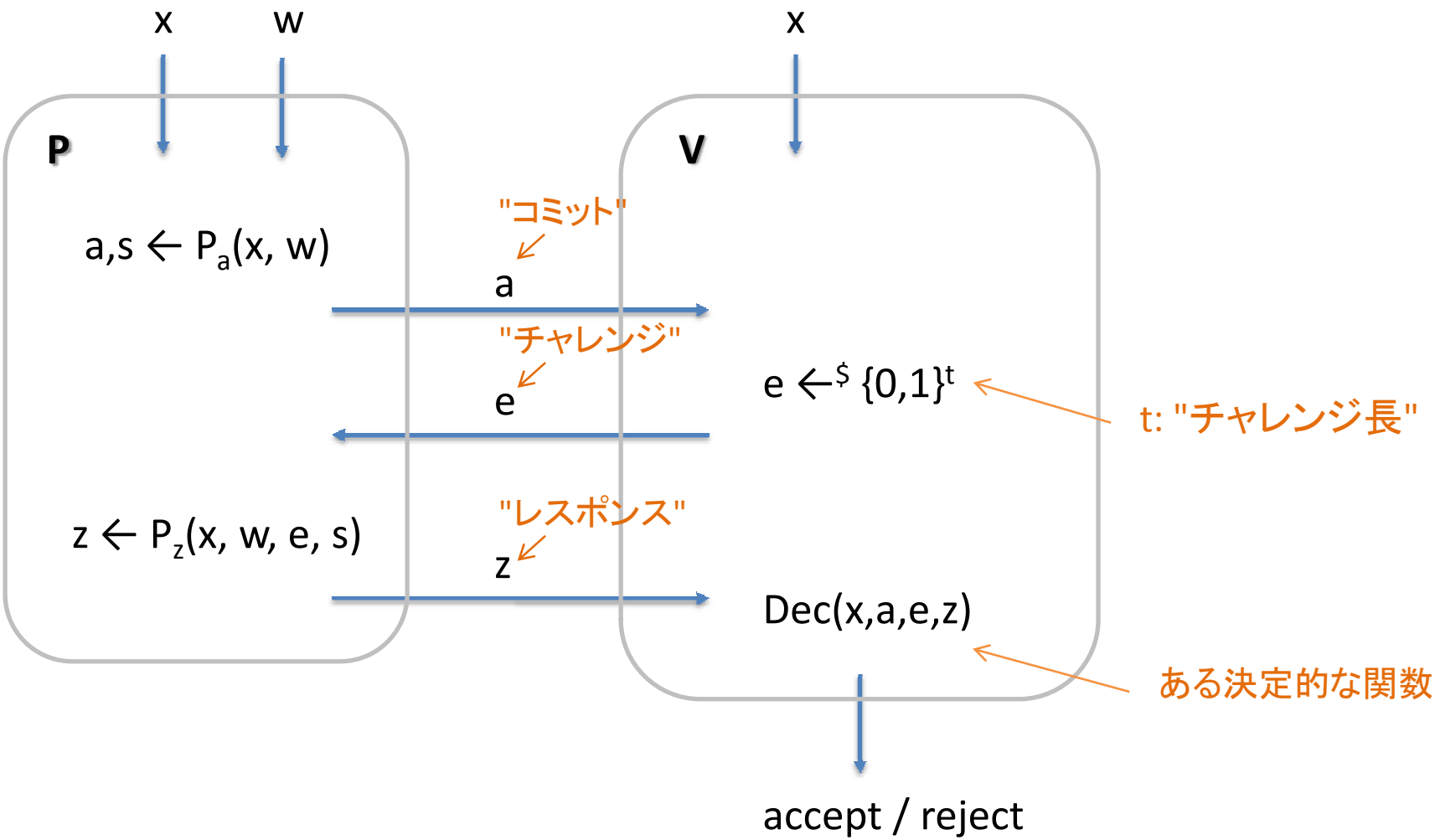
例:

- $R = GI = \{(x, w) \mid x = (G_0=(V_0,E_0), G_1=(V_1,E_1)),\ w: G_0 \rightarrow G_1$:同型$\}$
- $R = DL = \{(x, w) \mid x = g^w \bmod p\}$
- $R = \{(x, w) \mid x = w^q \bmod n\}$

1. Σプロトコルの定義と例

Σプロトコル：形

$R \subset \{0,1\}^* \times \{0,1\}^*$: 関係
$(x, w) \in R$ (ただし、$|w| \leqq p(|x|)$, $\exists p$: 多項式)



Σプロトコル：定義

先の形のプロトコル（P, V) が関係Rの**Σプロトコル**であるとは：

[完全性 (Completeness)]
　　正しい入力について(P, V)がプロトコルに従えば、Vは必ずaccept。

[特殊健全性(Special Soundness)]
以下のような効率的なアルゴリズム**E** (“エクストラクタ”)が存在：
　　入力：x , (a, e, z), (a, e', z') ただし, e ≠ e'
　　出力：w

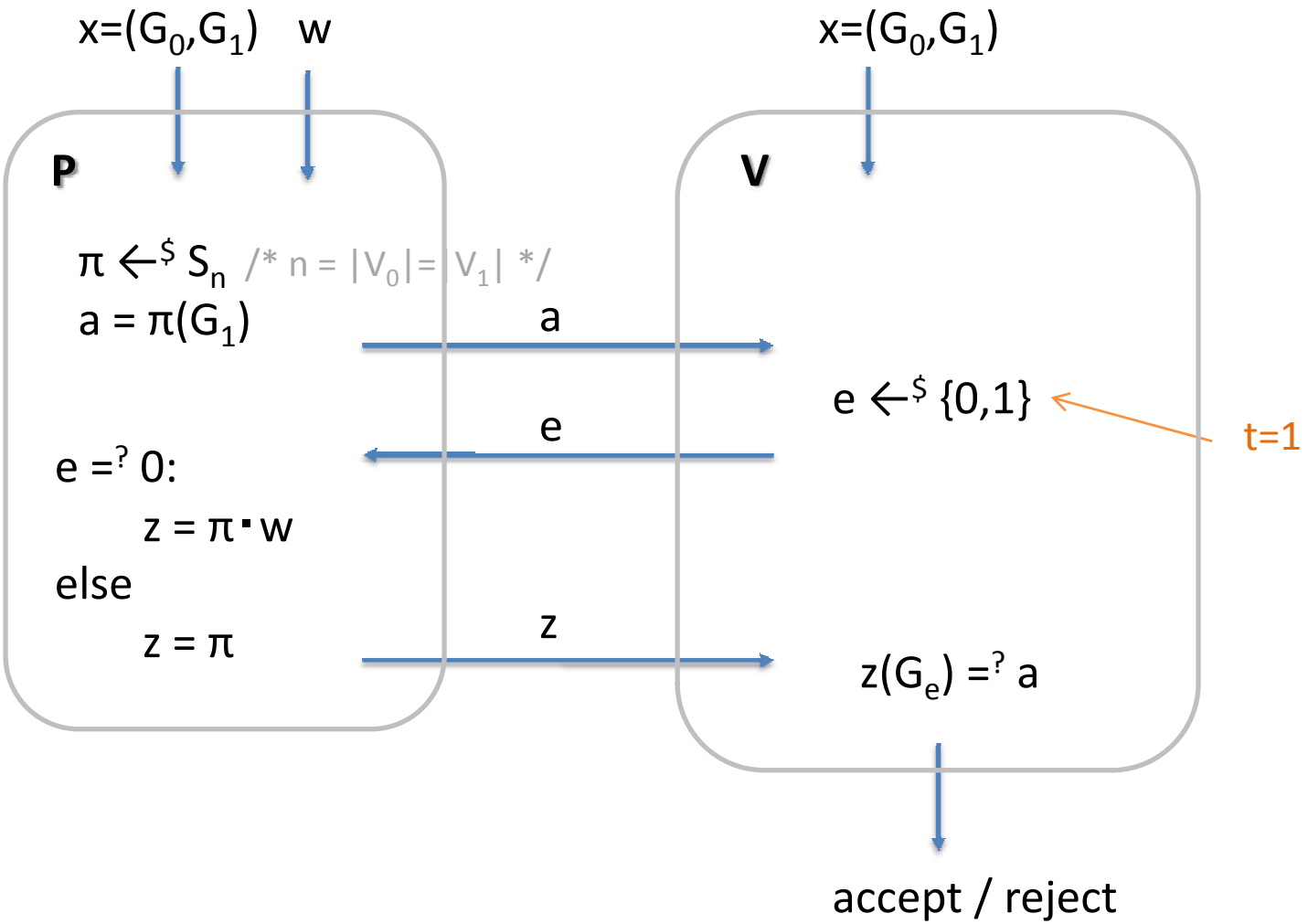
入力xに対する、同じaをもつ、２つの説得的なトランスクリプト

[特殊オネスト検証者ゼロ知識性 (Special Honest Verifier Zero Knowledge)]
以下のような効率的なアルゴリズム**M** (“シミュレータ”)が存在：
　　入力：x , e
　　出力：ランダムな説得的トランスクリプト (a,e,z)

トランスクリプト(a,e,z)には答えwの情報は漏れていない。

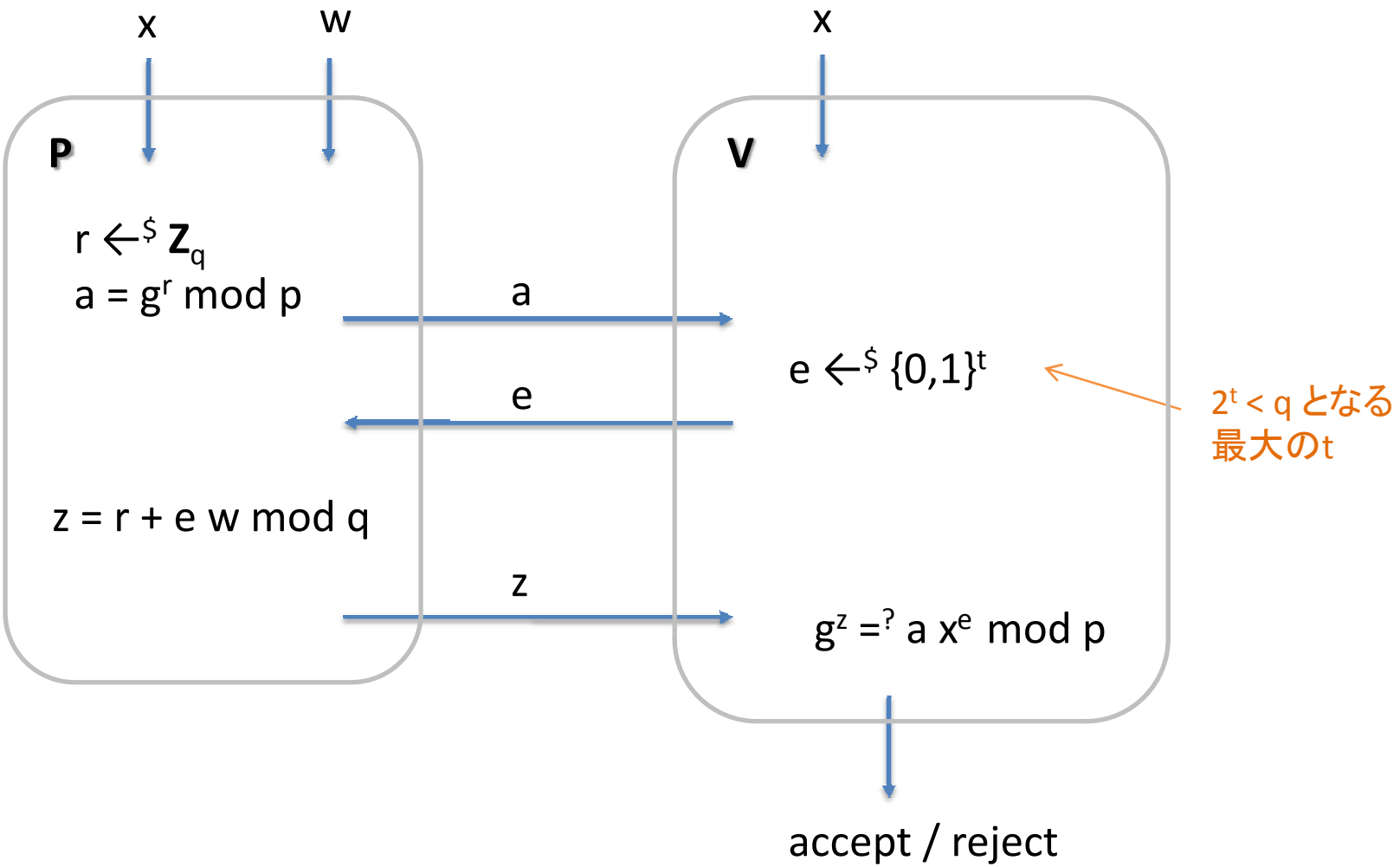
Σプロトコル1：グラフ同型問題

$R = GI = \{(x, w) \mid x = (G_0=(V_0,E_0), G_1=(V_1,E_1)),\ w: G_0 \to G_1 \text{:同型}\}$



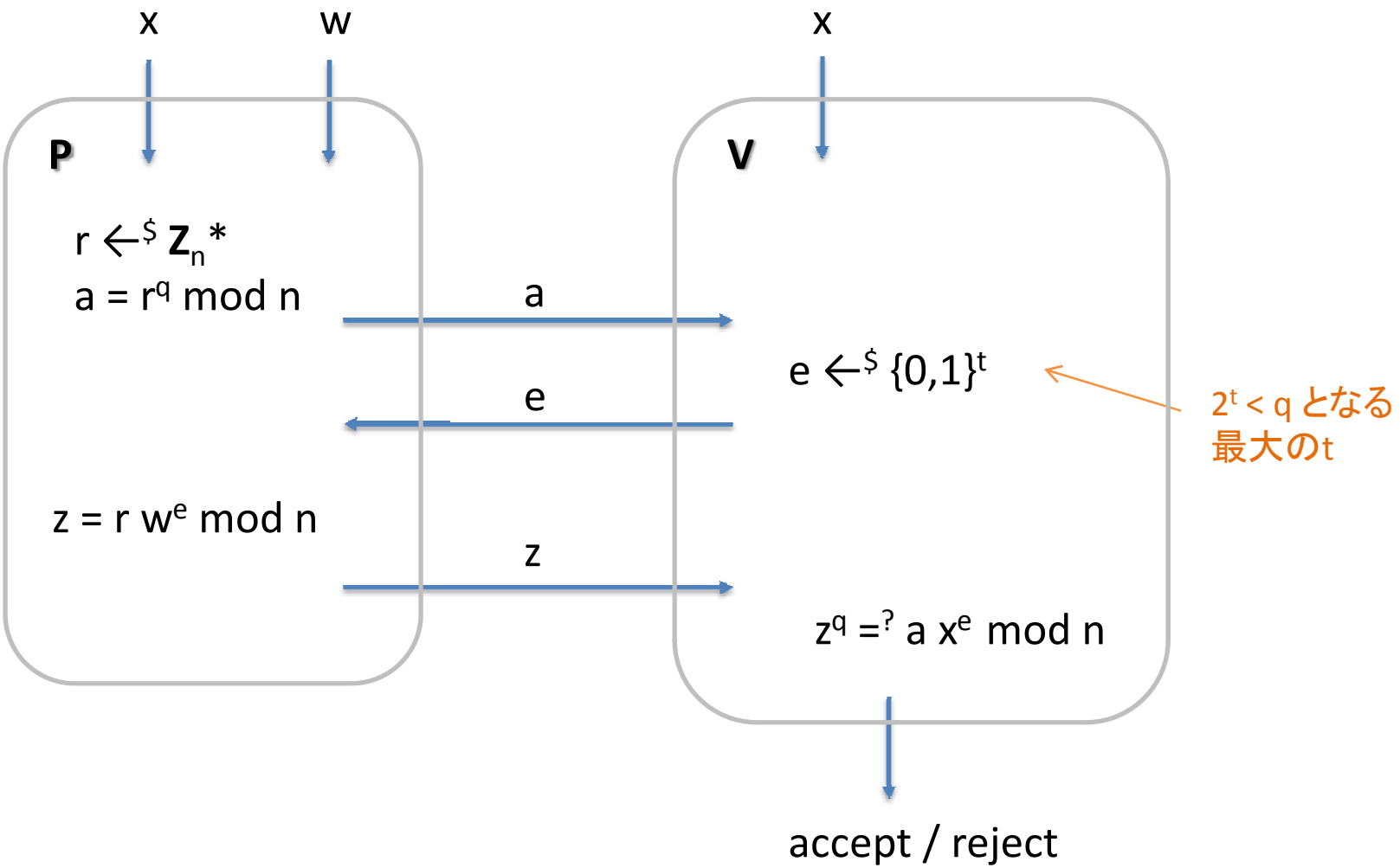
Σプロトコル2：離散対数問題

$R = DL = \{(x, w) \mid x = g^w \bmod p\}$



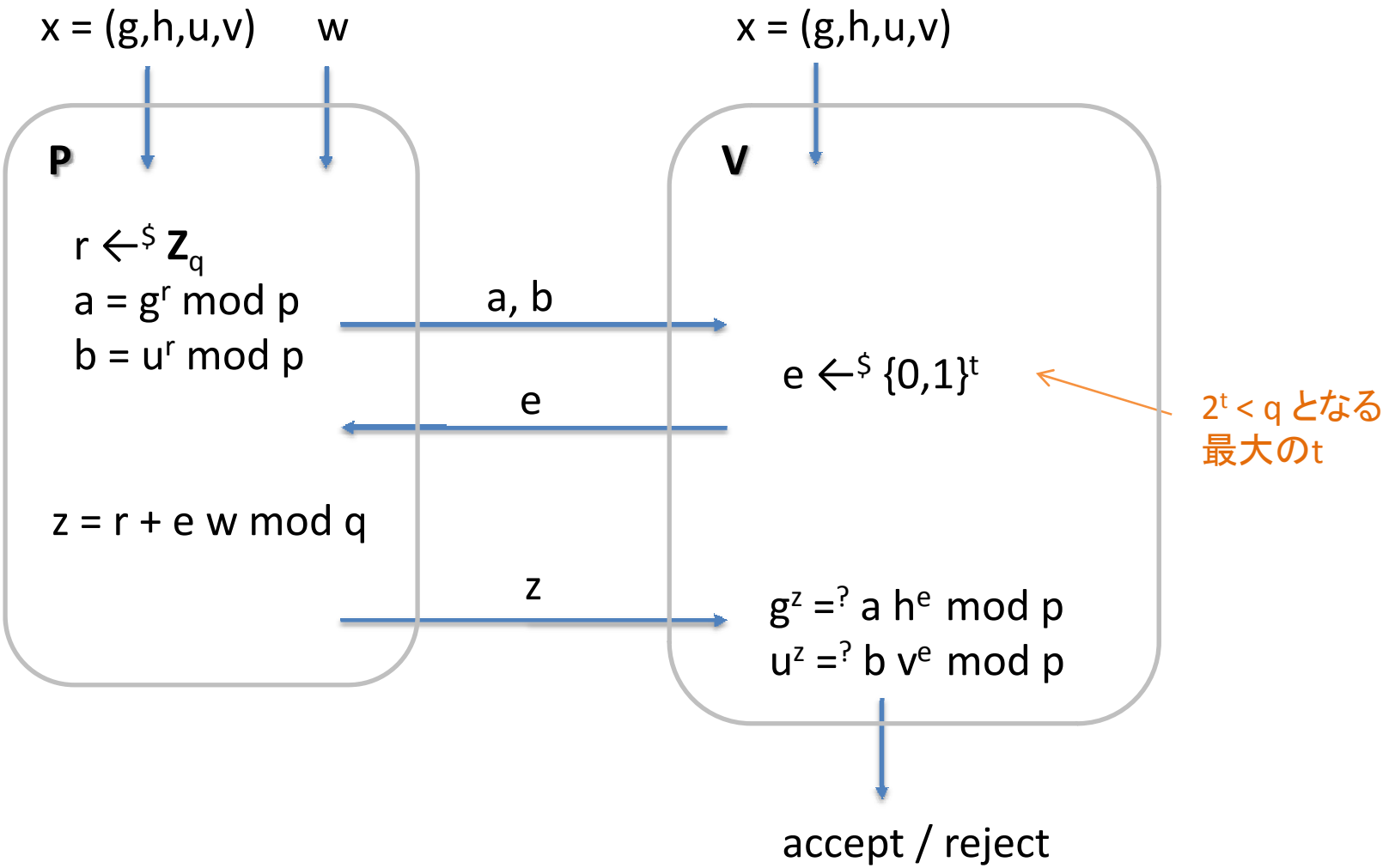
Σプロトコル3 : RSA問題

$R = \{(x, w) \mid x = w^q \bmod n\}$, q: prime, n : RSA modulus



Σプロトコル4：DH問題

$R = DH = \{(x, w) \mid x = (g,h,u,v), h=g^w \bmod p, v=u^w \bmod p\}$



2. Σプロトコルの基本的性質

知識証明プロトコル

κ: {0,1}* → [0..1]: 関数

プロトコル(P, V) が知識エラー κ をもつ、関係Rの**知識証明プロトコル**であるとは

[完全性] $\forall (x,w) \in R,\ \Pr[\ \langle P(w), V\rangle(x) = \text{accept}\ ] = 1$

[知識健全性]
以下のようなEPTアルゴリズム**KE** (”知識エクストラクタ”)が存在 :
$\forall\ x,\ \forall P^*,\ p^* := \Pr[\ \langle P^*, V\rangle(x) = \text{accept}\ ]$に対して

$$\Pr[\mathbf{KE}^{P^*}(x) = w\ ] \geqq p^* - \kappa(x)$$

検証者Vを納得させることのできるP*は
確かに答えwを知っている。

Σプロトコルは知識証明プロトコル

定理1

(P, V): チャレンジ長tをもつ関係RのΣプロトコル
⇒
(P, V): 知識エラー2^{-t}をもつ関係Rの知識証明プロトコル

チャレンジ長 t が健全性を支配

チャレンジ長を大きくするには？

定理2

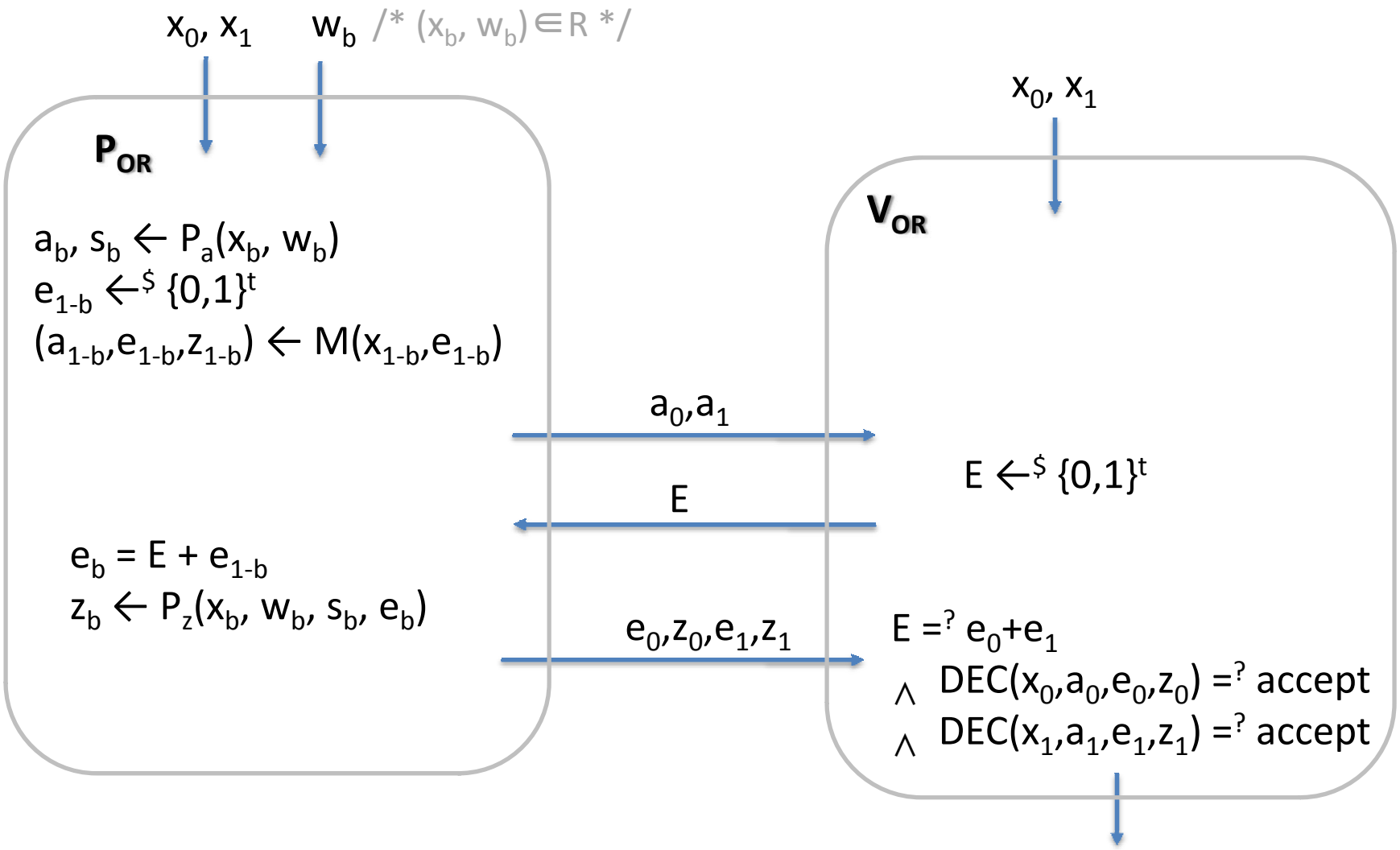
チャレンジ長t_0をもつ関係RのΣプロトコル(P_0,V_0)が存在するならば、
任意のチャレンジ長 t をもつ、関係RのΣプロトコルが存在する。

3. Σプロトコルと OR証明

ORプロトコル

(P, V): 関係Rのσプロトコル

$R_{OR} = \{((x_0,x_1),w) \mid (x_0,w) \in R \text{ or } (x_1,w) \in R\}$



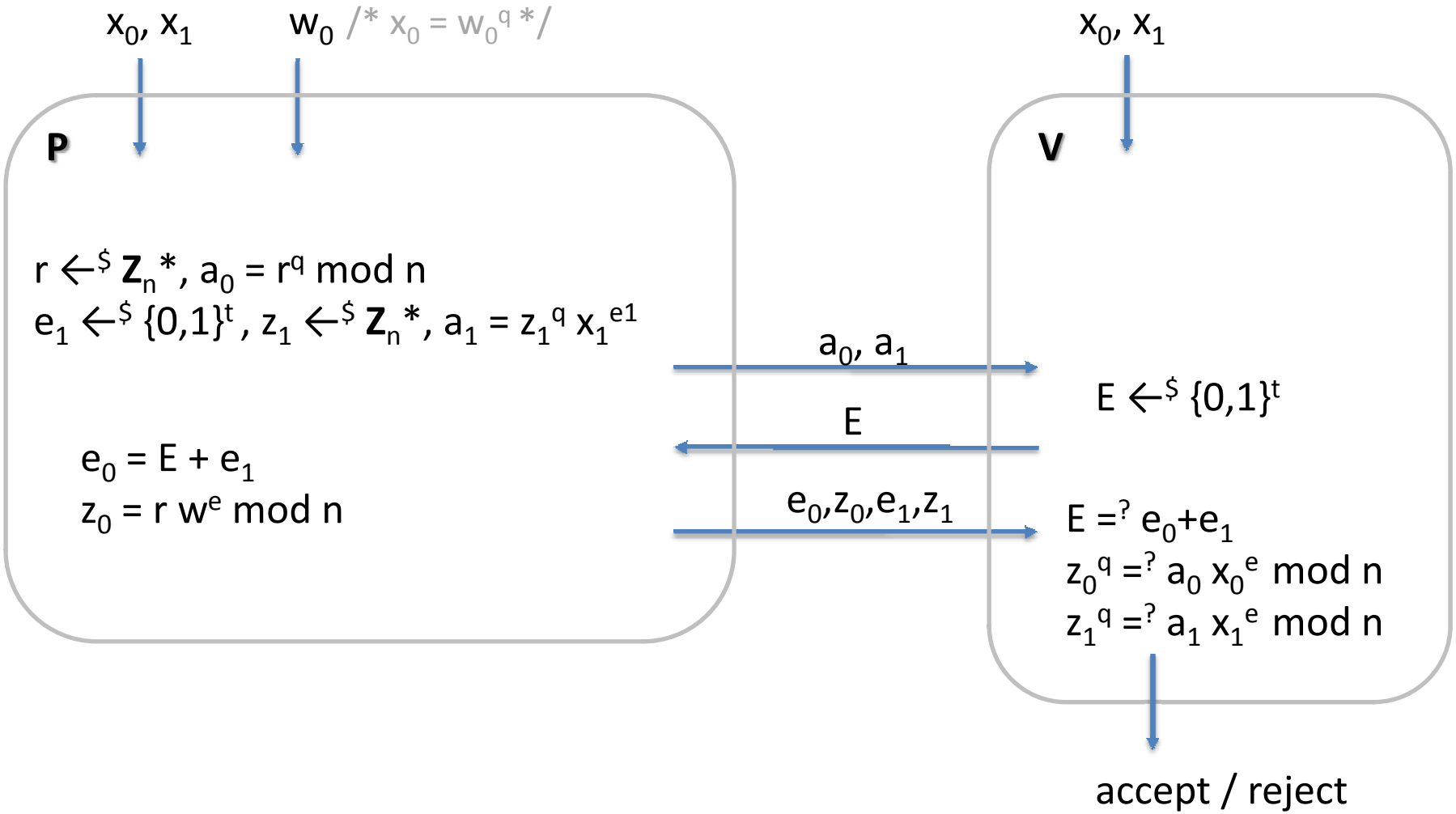
ORプロトコルは証拠識別不可能

定理3　[証拠識別不可能性(Witness Indistinguishable)]

ORプロトコル(P_{OR}, V_{OR})は関係R_{OR}のΣプロトコル。
さらに、任意のV* にとって、P_{OR}がx_0を証明しているのか、x_1を証明しているのか、識別不可能。

ORプロトコルの例

$R = \{((x_0,x_1), w) \mid x_0=w^q \bmod n \text{ or } x_1=w^q \bmod n\}$



困難な関係

関係Rが**困難**であるとは:

- ある効率的なアルゴリズムGがあって

$$(x, w) \leftarrow G(k),\ |x| = k,\ (x, w) \in R$$

- どのような効率的なアルゴリズムAに対しても

$$\Pr[\ (x, w) \leftarrow G(k),\ w_A \leftarrow A(x) : (x, w_A) \in R\ ]\ ;\ \text{negligible in } k$$

証拠秘匿性

関係R のΣプロトコル (P, V) が**証拠秘匿性**をもつ(Witness Hiding)とは:

- どのような効率的なアルゴリズムV*も以下のゲームに勝つ確率は negligible であること。

- ゲーム:

  (x, w) ← G(k)
  (P(w), V*)(x) を任意の多項式回数実行。
  w* ← V*　　/* V*のチャレンジeはランダムとは限らない。*/

  (x, w*) ∈ R ならばV*の勝ち。

ゼロ知識性: V* は P(w) から何も得ない。
証拠秘匿性: V* は P(w) から w を得ない。

証拠秘匿性をもつΣプロトコルの構成

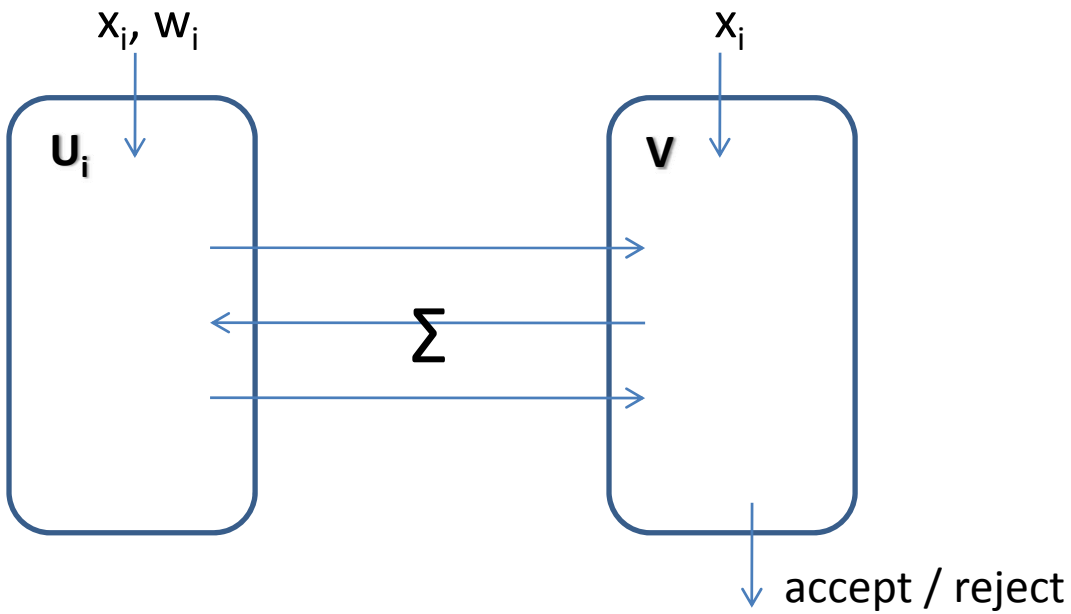
定理4
(P,V)を関係RのΣプロトコルとし、(P_{OR}, V_{OR})をそのORプロトコルとする。

このとき、関係Rが困難であるならば、ORプロトコル(P_{OR}, V_{OR})は関係R_{OR}について証拠秘匿性をもつ。

4. Σプロトコルの応用

Σプロトコルから認証プロトコル

1. (P,V)を関係Rに関するΣプロトコルとする。
2. 各利用者U_iについて
   $(x_i, w_i) \leftarrow G(k)$,
   x_iを公開し、w_iをU_iだけの秘密とする。
3. 利用者U_iはΣプロトコルを用いて自身の正当性を証明する。



認証プロトコルの安全性

□ 受動的攻撃に対する安全性

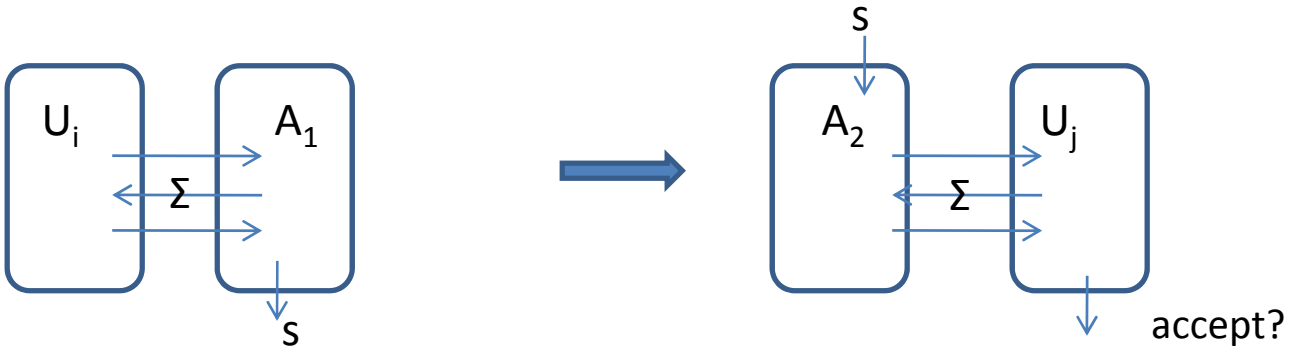
1. 攻撃者AはU$_i$とVとの間のやりとりを入手。
2. 攻撃者Aは上で得た知識をもとに、他の利用者U$_j$に対してU$_i$になりすまそうとする。

このようにしてもAがU$_i$になりすませないとき、
認証プロトコルは**受動的攻撃に対して安全**であるという。

□ 能動的攻撃に対する安全性

1. 攻撃者Aは検証者としてU$_i$との間ですきなだけIDプロトコルを実行。
2. 攻撃者Aは上で得た知識をもとに、他の利用者U$_j$に対してU$_i$になりすまそうとする。

このようにしてもAがU$_i$になりすませないとき、
認証プロトコルは**能動的攻撃に対して安全**であるという。



受動的攻撃に対して

定理5
(P,V)を関係Rのプロトコルとする。

チャレンジ長 t が（2^{-t}がnegligibleなくらい）十分大きく、関係Rが困難ならば、プロトコル(P,V) からつくられる認証プロトコルは受動的攻撃に対して安全である。

能動的攻撃に対して

定理6
(P,V)を関係Rのプロトコルとする。

チャレンジ長 t が（2^{-t}がnegligibleなくらい）十分大きく、証拠秘匿性をもつならば、(P,V)からつくられる認証プロトコルは能動的攻撃に対して安全である。

署名スキーム

SS = (Kg, Sgn, Vfy) が**署名スキーム**であるとは

[完全性] (pk,sk) ← Kg(k), σ ← Sgn(sk, m), Vfy(pk,m,σ) = valid

[存在的偽造不可能性]
どのような効率的なアルゴリズムFも以下のゲームに勝てない:

ゲーム:

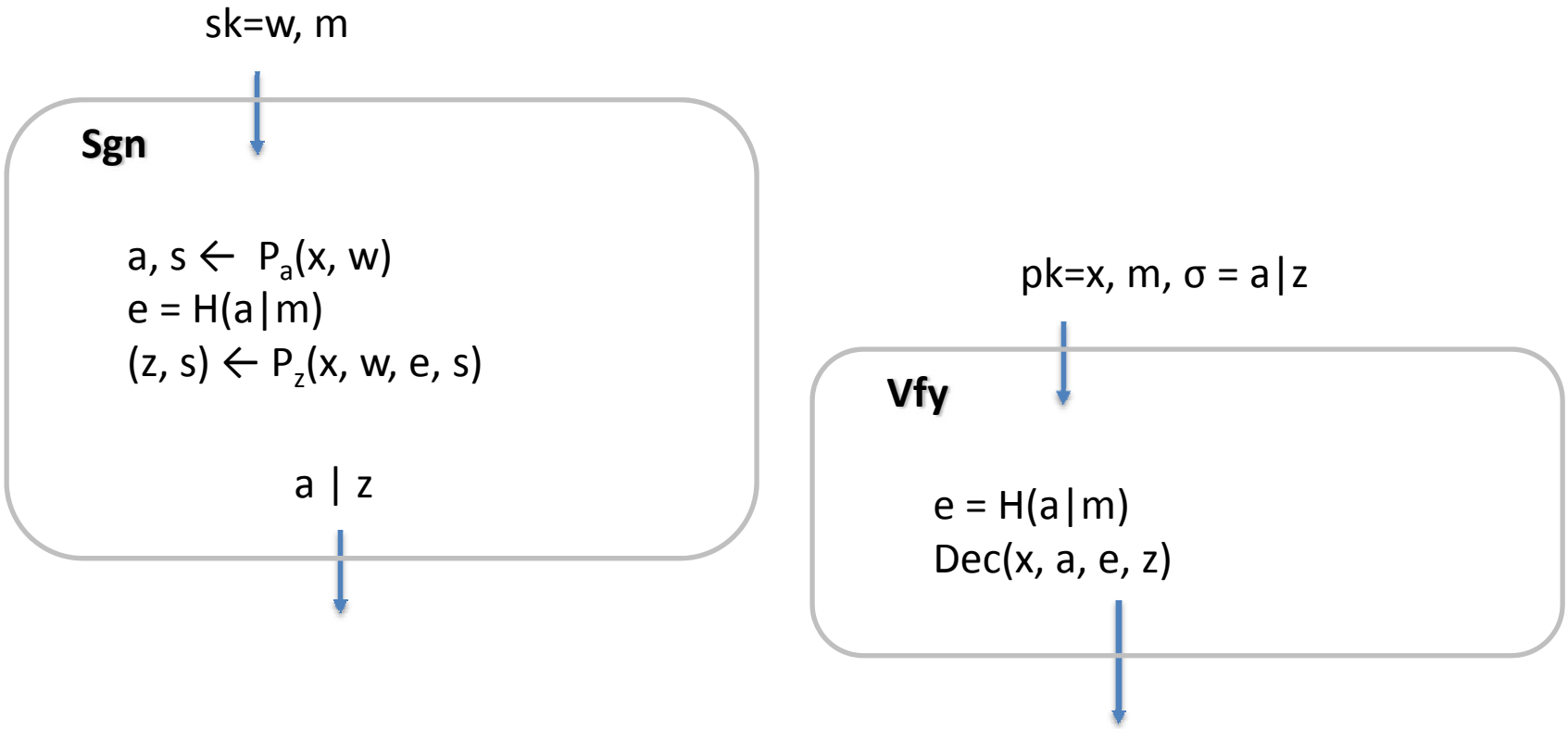
(pk, sk) ← Kg(k)
(m,σ) ← $F^{Sgn(sk,\cdot)}$(pk)

Vfy(pk,m,σ)=valid かつmはSgn(sk,・)に尋ねられていないならば、
Fの勝ち

FS変換

Σ=(P, V): 関係RのΣプロトコル、チャレンジ長 t
G : 関係Rのジェネレータ
H : {0,1}* → {0,1}^{t}: ハッシュ関数

SS = FS_H(Σ) = (G, Sgn, Vfy) :



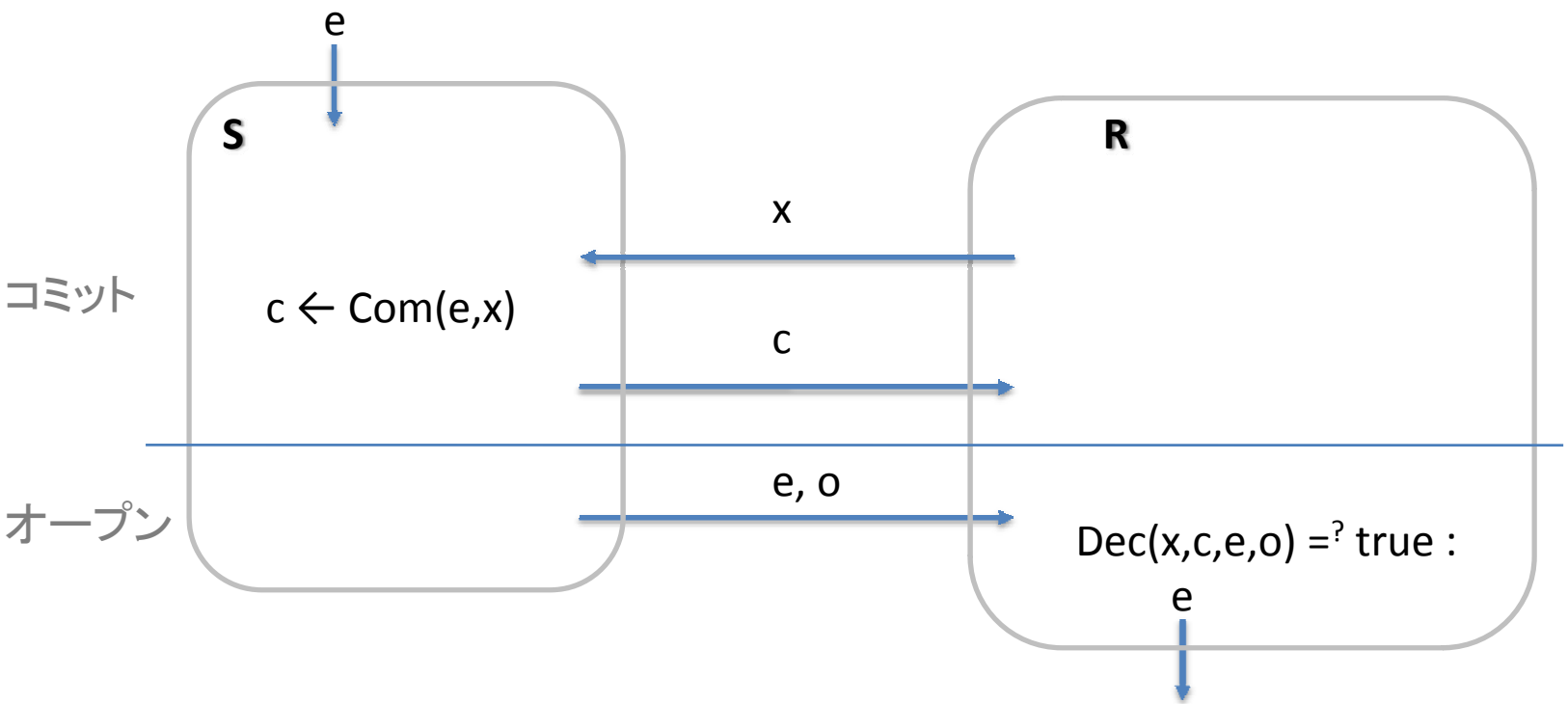
FS変換の安全性

定理7
(P,V)を関係Rのプロトコルとする。

関係Rが困難でコミットメント長もチャレンジ長も十分大きいならば、ランダムオラクルモデルのもとで、SS = $FS_H(\Sigma)$ は存在的偽造不可能な署名スキームである。

コミットメントプロトコル

コミットが2ムーブの場合



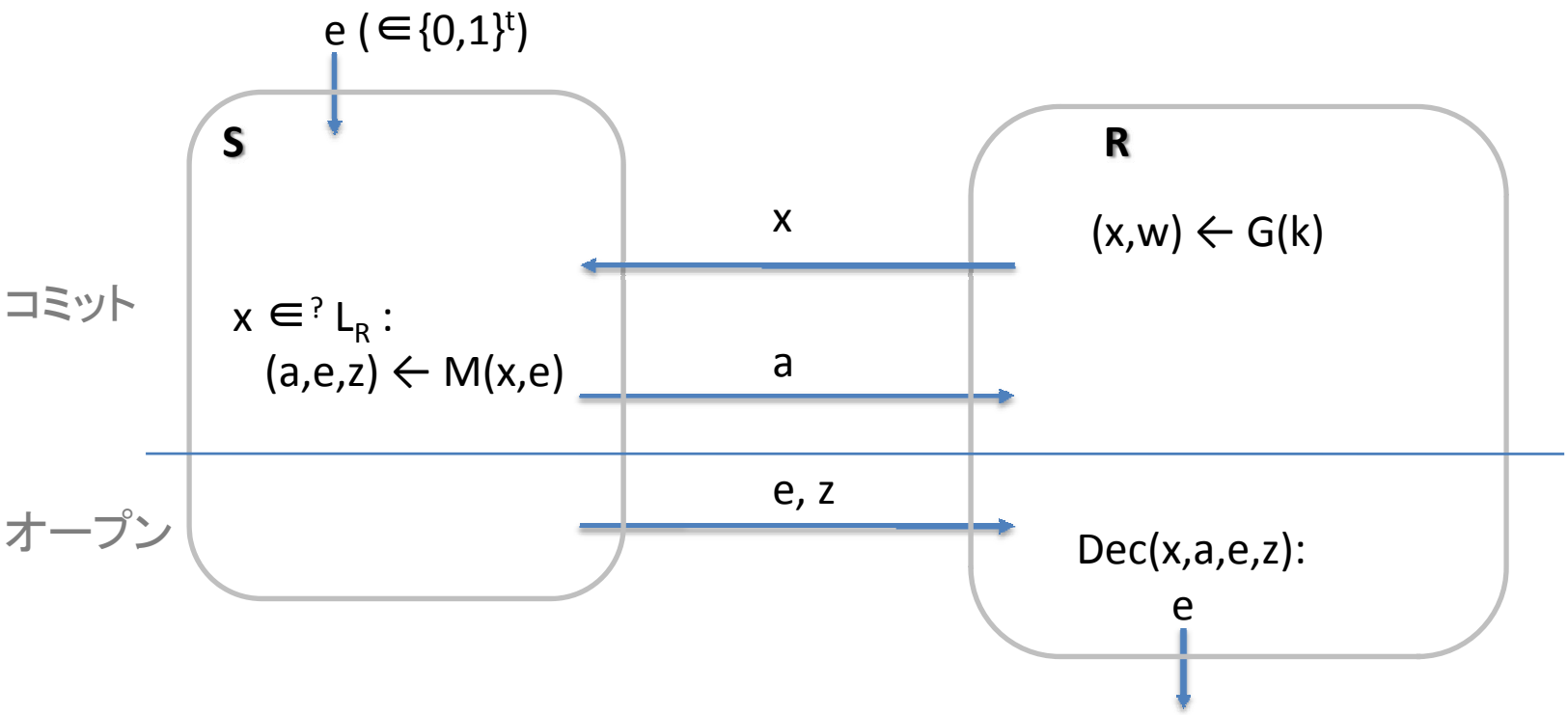
[秘匿性] コミットメントc からeは1ビットもわからない。

[束縛性] どのようなS*も、eにもe'にも(e≠e')オープンできるコミットメントc を作ることはできない。

Dec(x,c,e,o) = Dec(x,c,e',o') = true

Σプロトコルからコミットメントプロトコル

M : 関係RについてのΣプロトコル(P,V)のシミュレータ



関係Rが困難ならば、(S,R)はコミットメントプロトコル

参考文献

• Ivan Damgard, On Σ-protocols, CPT '05

• R. Cramer, I. Damgard, Secure Signatures from Interactive Protocols, CRYPTO '95

• M. Abdalla, J.H.An, M.Bellare, C. Namprempre,
From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security,
EUROCRYPT ‘02

• M. Bellare, C. Namprempre, G. Neven,
Security Proofs for Identity-Based Identification and Signature Schemes,
EUROCRYPT '04