Recent advancements and attacks on Zero-Knowledge Proofs

—

Kriptografik İspat Sistemlerinin ve Saldırıların Gelişim Serüveni

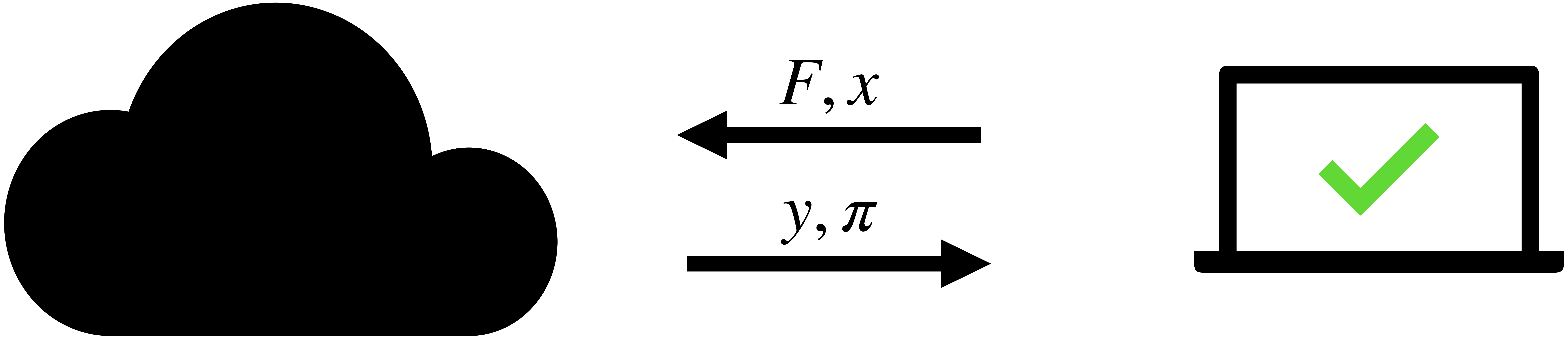
EPFL

Abdullah Talayhan
@talayhan_a
abdullah.talayhan@epfl.ch

R1CS
PLONK
Aurora
STARK
HyperPlonk
TurboPLONK
cq
Pinocchio
Nova
Sangria
Breakdown
FRI
Caulk
AIR
Groth16
HyperNova
Baloo
CCS
Halo2
SuperNova
Bulletproofs
KZG
Caulk+
ProtoStar

General Purpose Verifiable Computation

Task: Compute $F(x)$



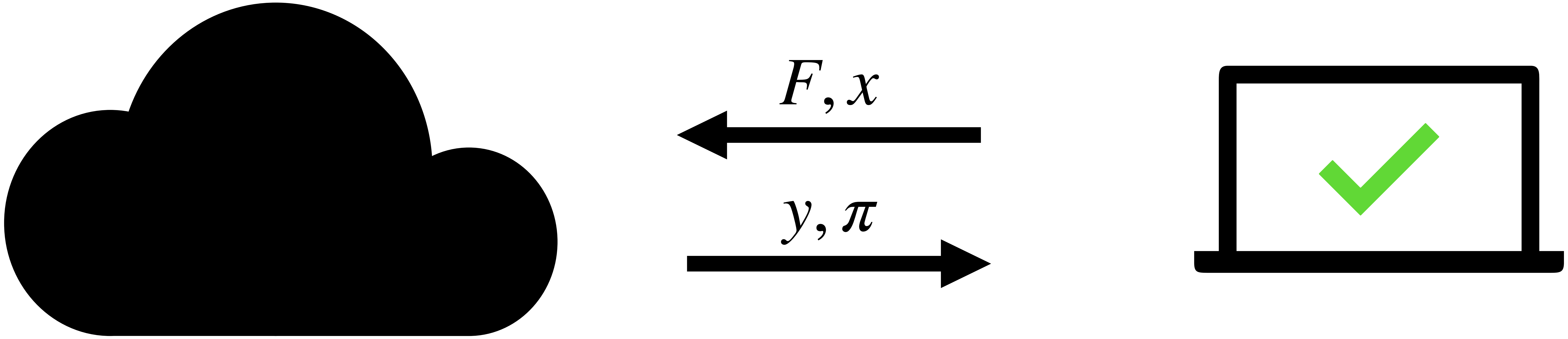
$F(x) \rightarrow y$

$Prove(F, x, y) \rightarrow \pi$

$Verify(F, x, y, \pi) \rightarrow 0/1$

General Purpose Verifiable Computation

Task: Compute $F(x, w)$

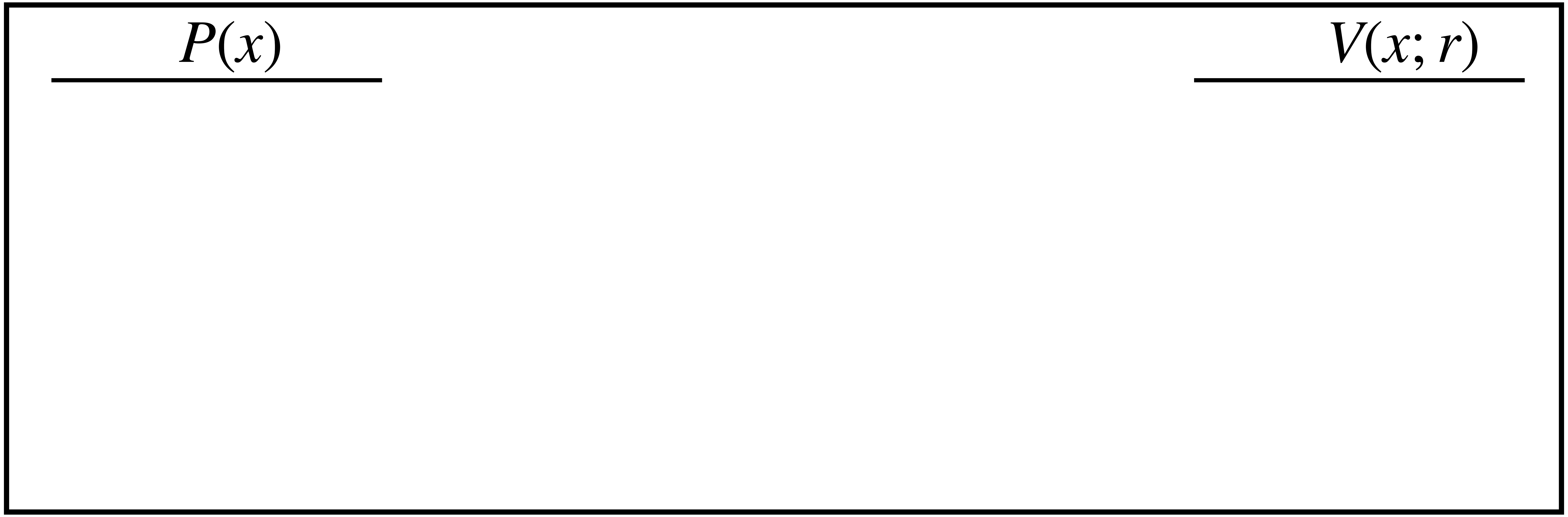


$F(x, w) \rightarrow y$

$Prove(F, x, y) \rightarrow \pi$

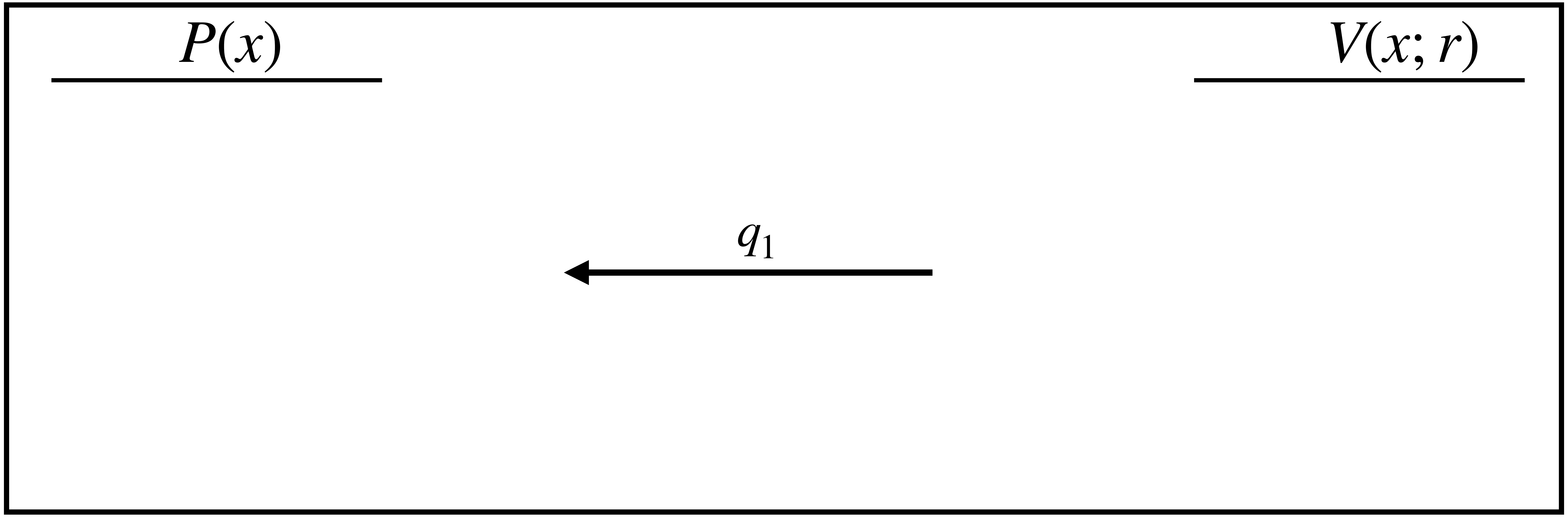
$Verify(F, x, y, \pi) \rightarrow 0/1$

Interactive Proof



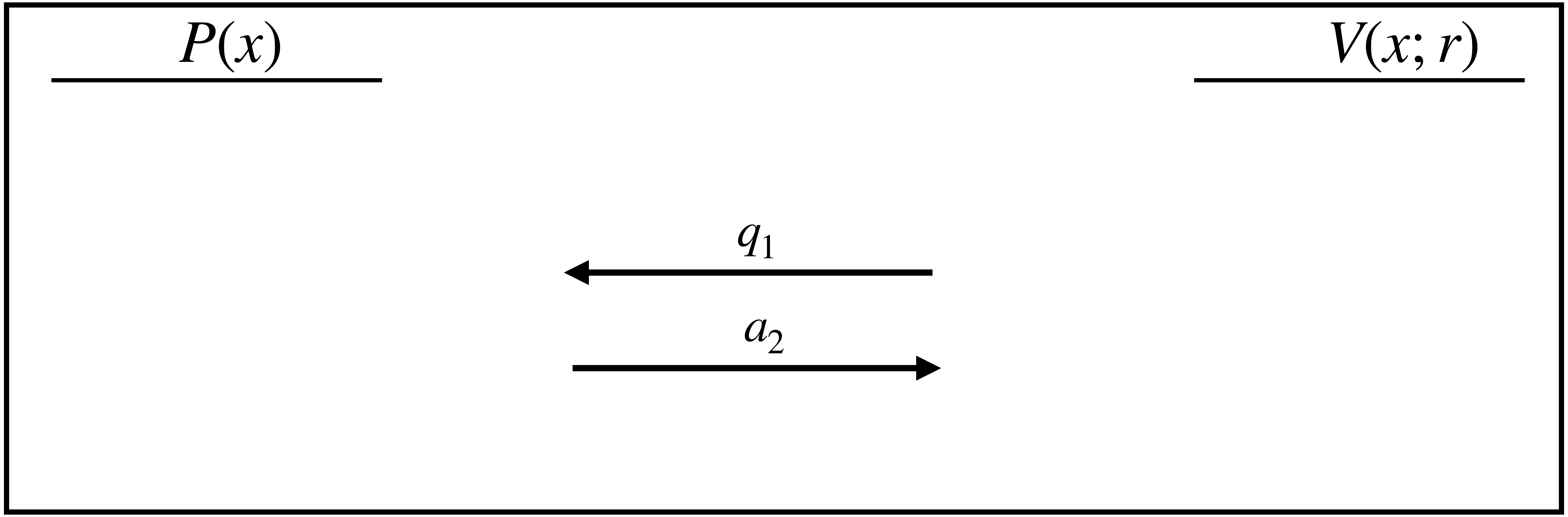
- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x; r)\rangle = 1] = 1$
- **Soundness:** $\forall x \notin L \quad \forall P^* \quad \Pr_r[\langle P^*(x), V(x; r)\rangle = 1] \leq 1/2$

Interactive Proof



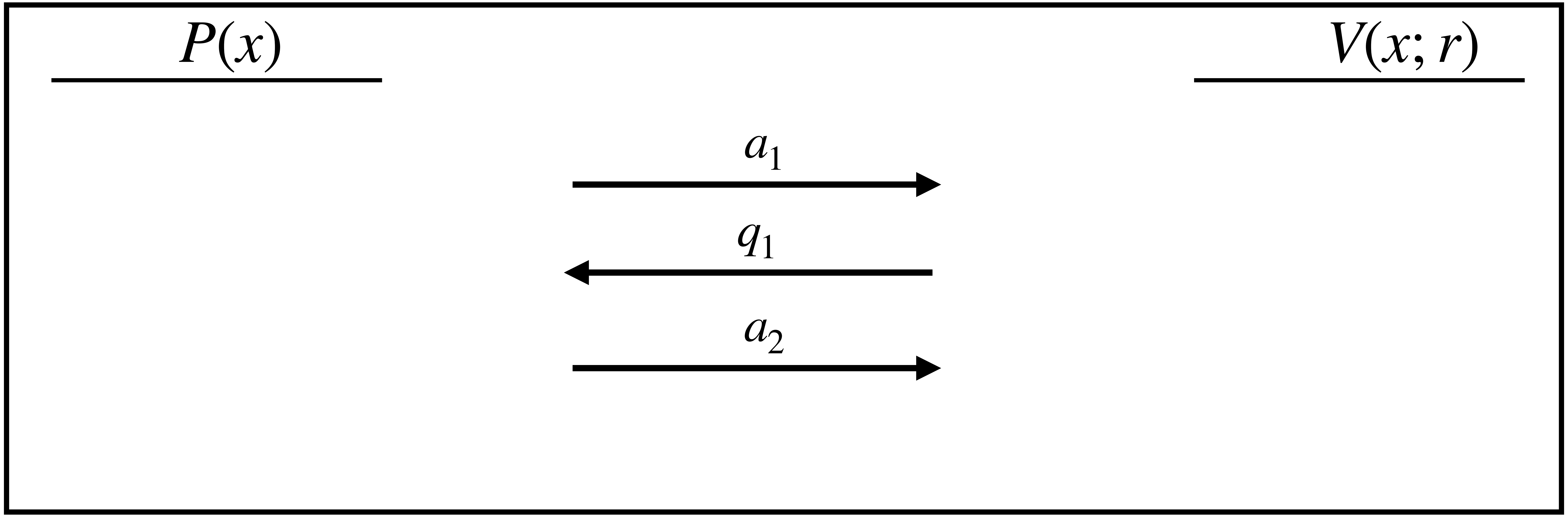
- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x;r)\rangle = 1] = 1$
- **Soundness:** $\forall x \notin L \quad \forall P^* \quad \Pr_r[\langle P^*(x), V(x;r)\rangle = 1] \leq 1/2$

Interactive Proof



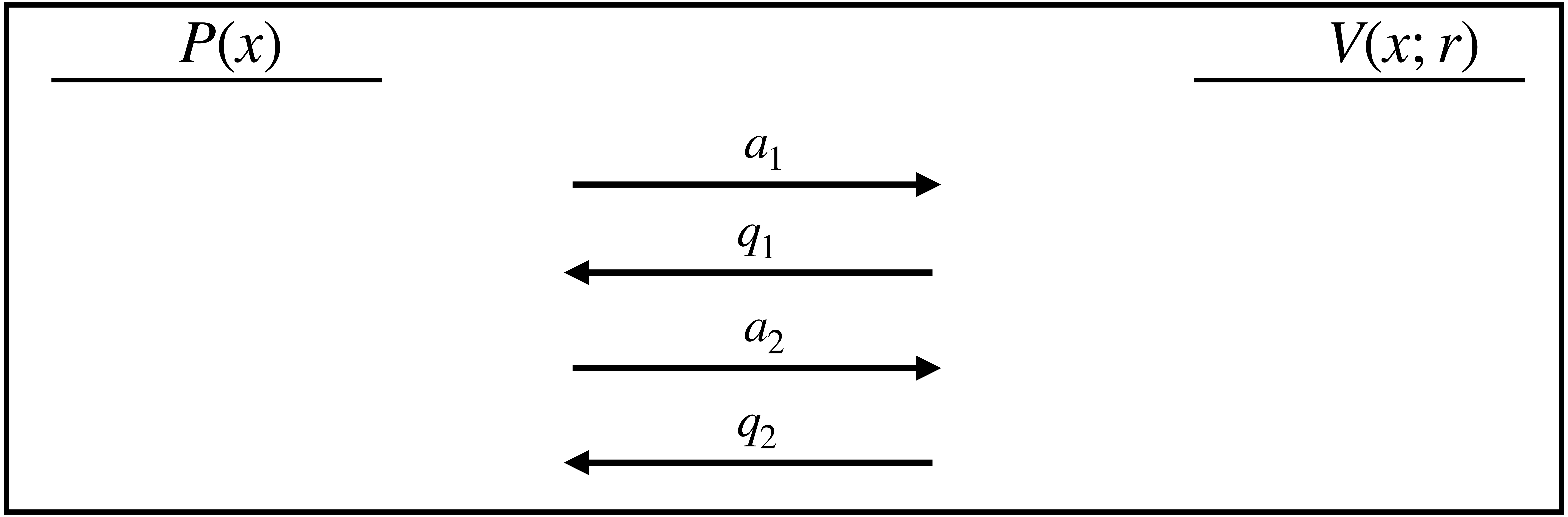
- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x;r)\rangle = 1] = 1$
- **Soundness:** $\forall x \notin L \quad \forall P^* \quad \Pr_r[\langle P^*(x), V(x;r)\rangle = 1] \leq 1/2$

Interactive Proof



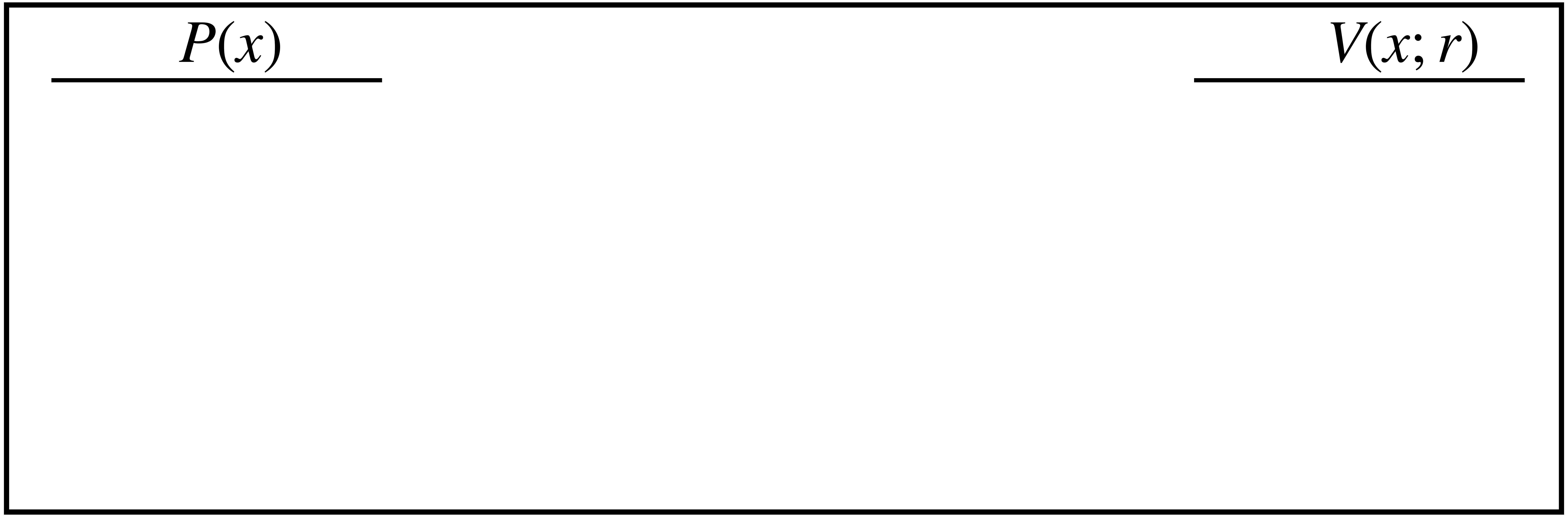
- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x;r)\rangle = 1] = 1$
- **Soundness:** $\forall x \notin L \quad \forall P^* \quad \Pr_r[\langle P^*(x), V(x;r)\rangle = 1] \leq 1/2$

Interactive Proof



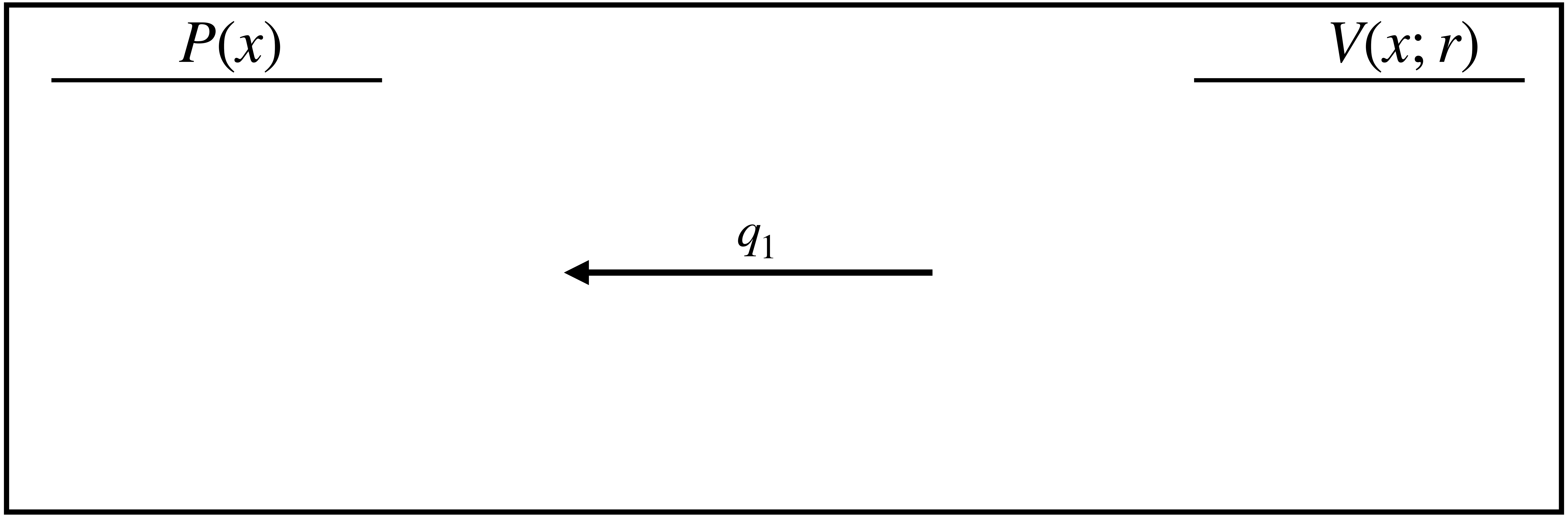
- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x; r)\rangle = 1] = 1$
- **Soundness:** $\forall x \notin L \quad \forall P^* \quad \Pr_r[\langle P^*(x), V(x; r)\rangle = 1] \leq 1/2$

Interactive Argument



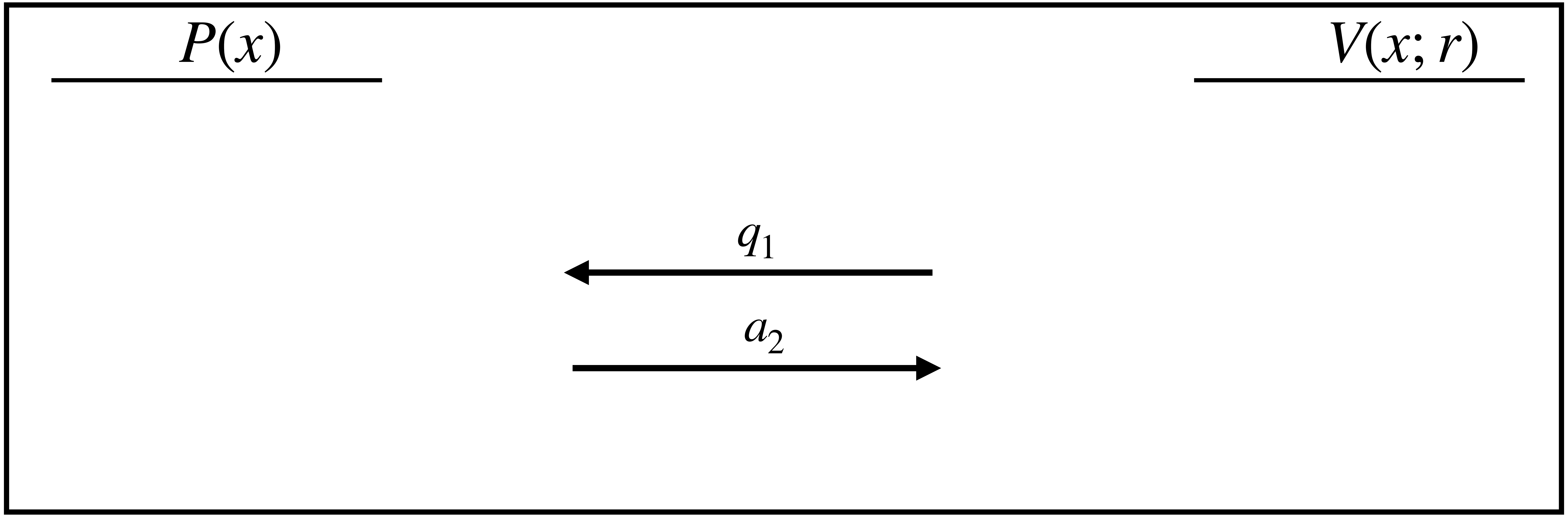
- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x;r) \rangle = 1] = 1$
- **Soundness:** $\forall x \notin L$ $\forall$ PPT $P^* \quad \Pr_r[\langle P^*(x), V(x;r) \rangle = 1] \leq 1/2$

Interactive Argument



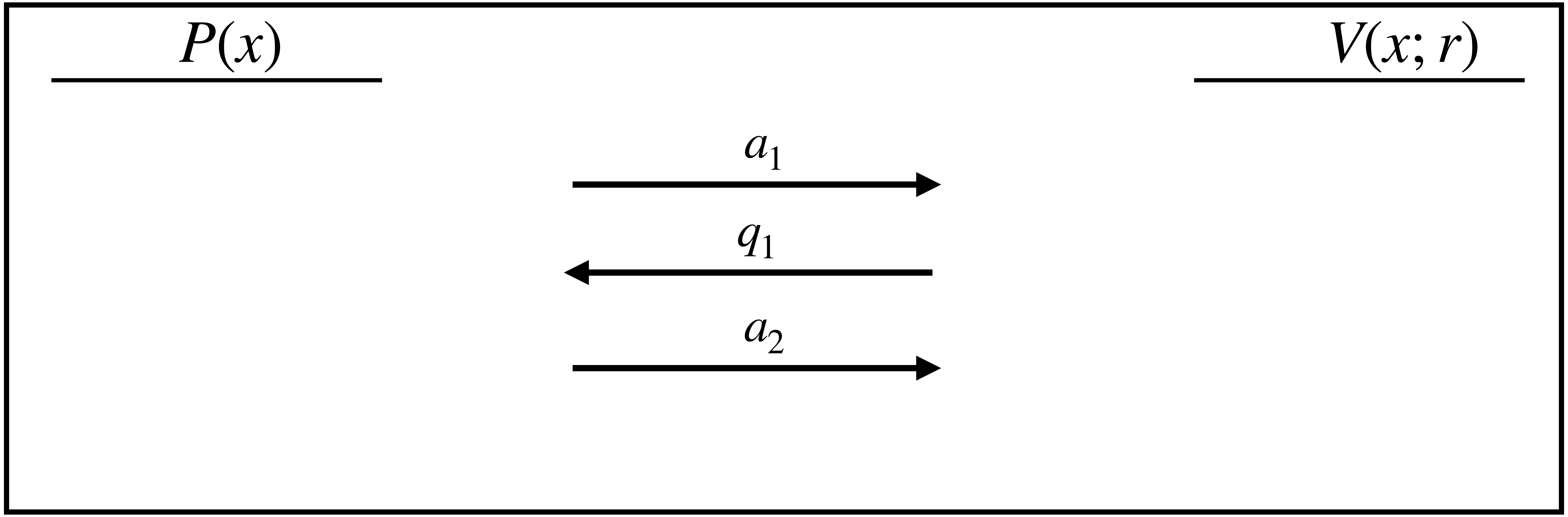
- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x; r)\rangle = 1] = 1$
- **Soundness:** $\forall x \notin L$ $\forall$ PPT $P^* \quad \Pr_r[\langle P^*(x), V(x; r)\rangle = 1] \leq 1/2$

Interactive Argument



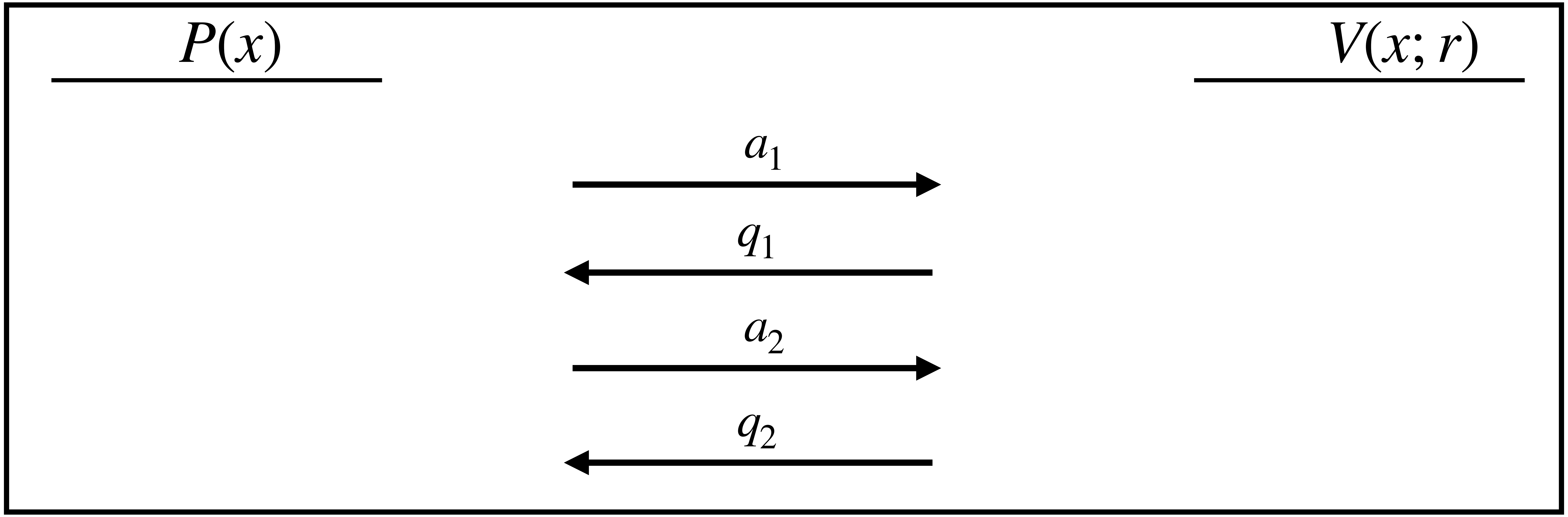
- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x;r)\rangle = 1] = 1$
- **Soundness:** $\forall x \notin L$ $\forall$ PPT $P^* \quad \Pr_r[\langle P^*(x), V(x;r)\rangle = 1] \leq 1/2$

Interactive Argument



- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x;r)\rangle = 1] = 1$
- **Soundness:** $\forall x \notin L$ $\forall$ PPT $P^* \quad \Pr_r[\langle P^*(x), V(x;r)\rangle = 1] \leq 1/2$

Interactive Argument

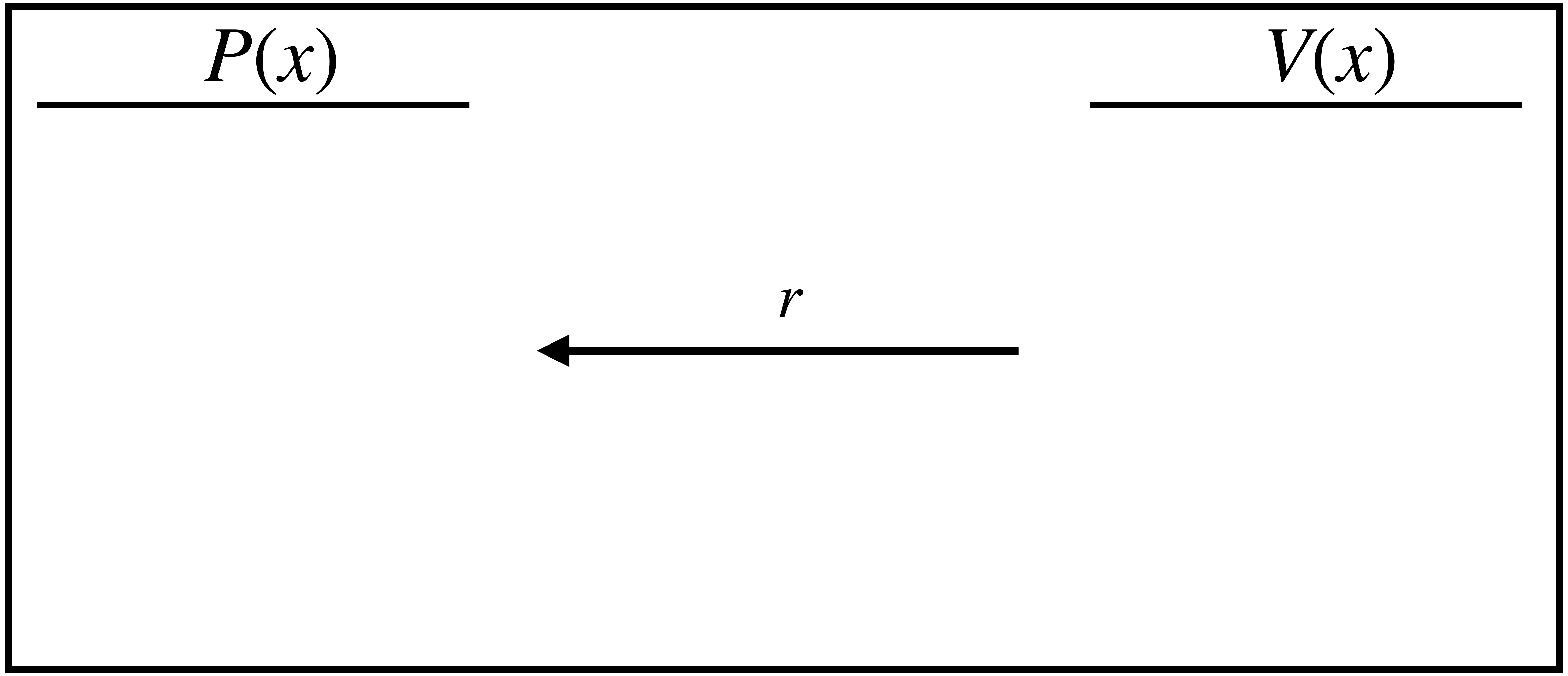


- **Completeness:** $\forall x \in L \quad \Pr_r[\langle P(x), V(x; r)\rangle = 1] = 1$
- **Soundness:** $\forall x \notin L$ $\forall$ PPT $P^* \quad \Pr_r[\langle P^*(x), V(x; r)\rangle = 1] \leq 1/2$

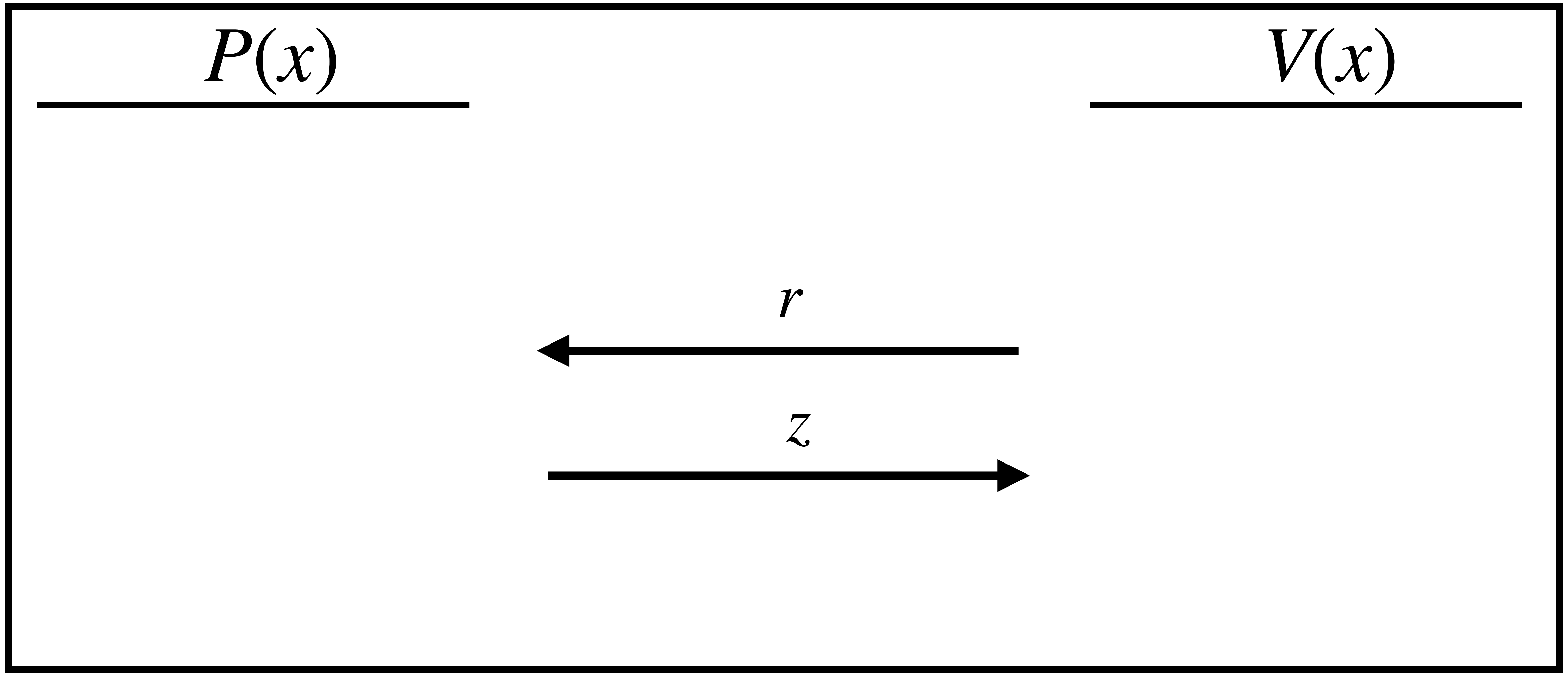
Sigma Protocol

$P(x)$		$V(x)$

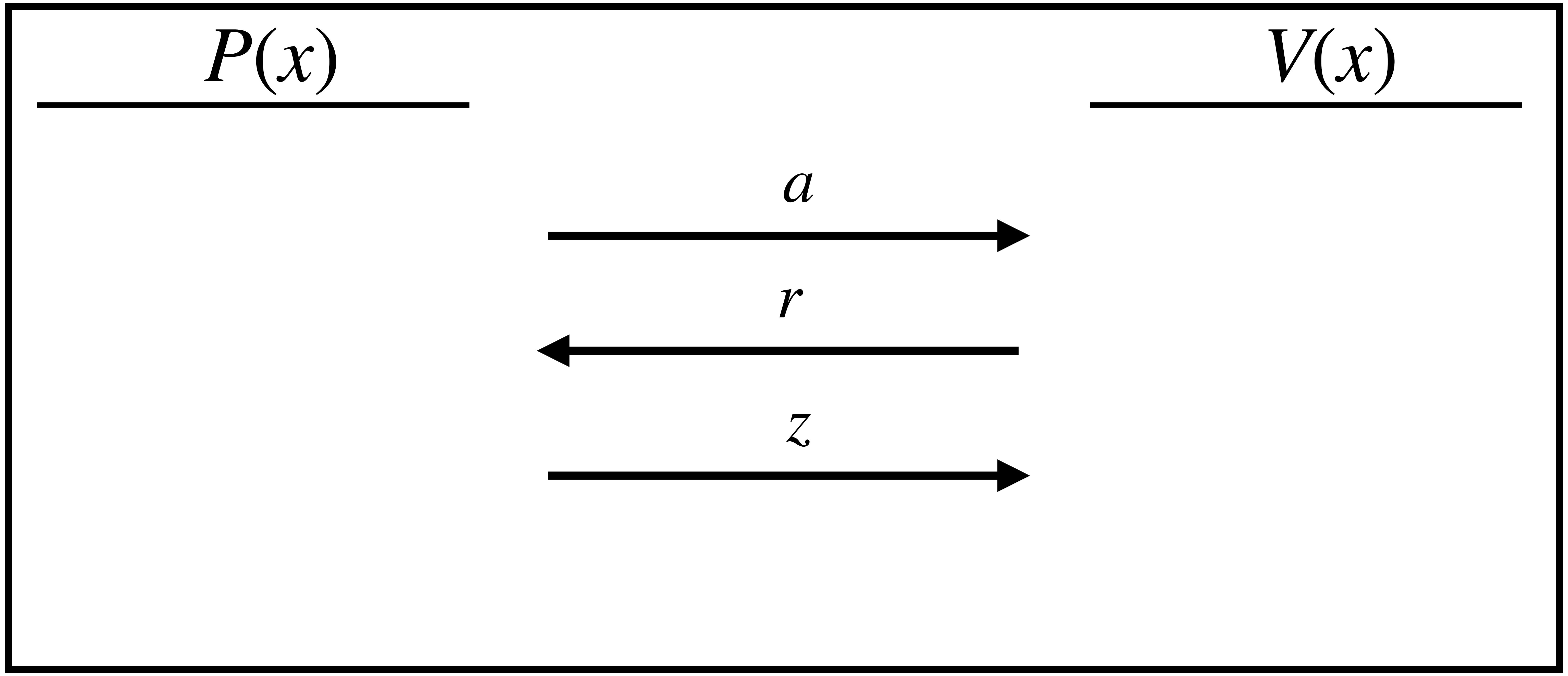
Sigma Protocol



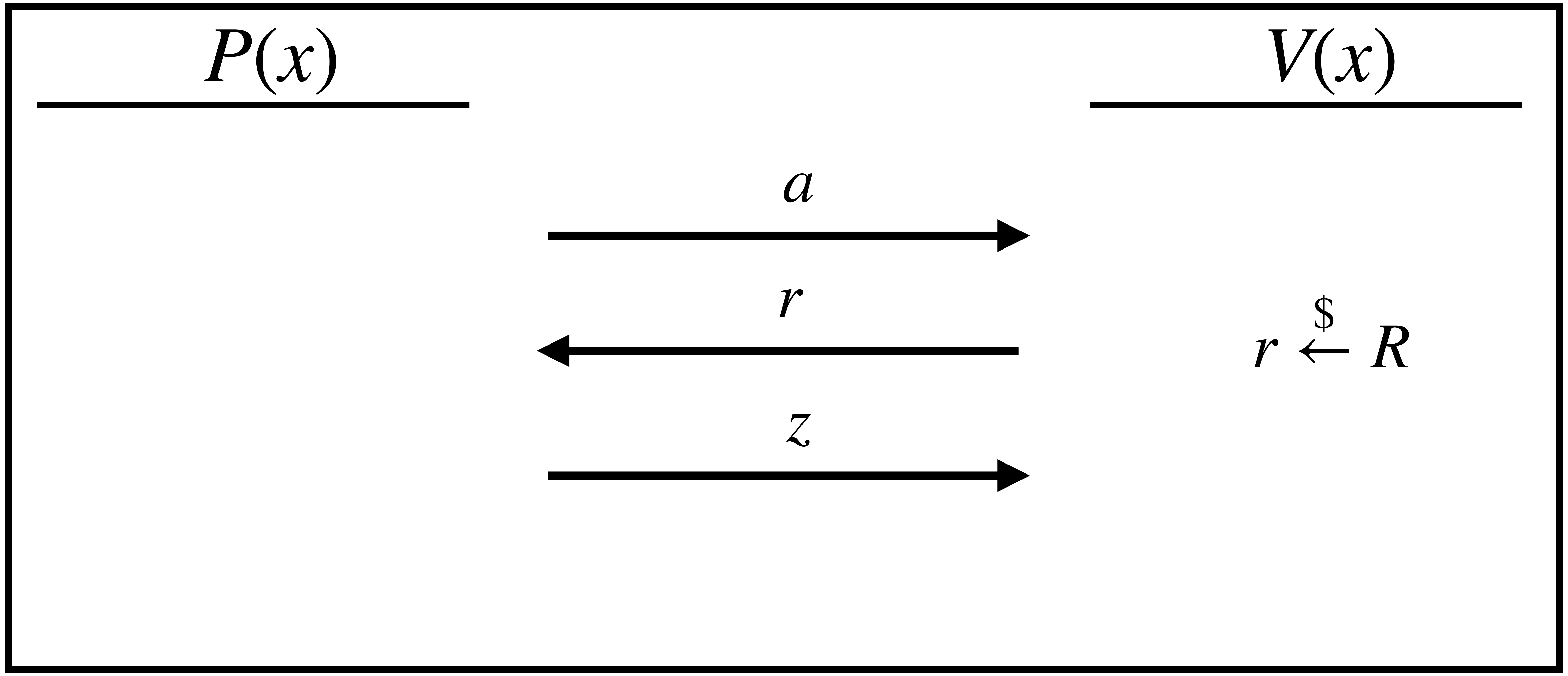
Sigma Protocol



Sigma Protocol



Sigma Protocol



Sigma Protocol
DLOG

Let g be the generator of a subgroup of large prime order q modulo p .

Prover: I know w such that $Y = g^w \mod p$

Sigma Protocol

Schnorr DLOG

$P(w)$	g, q, p, Y	$V()$
$k \xleftarrow{\$} Z_p^*$		
$a \leftarrow g^k$	a $\longrightarrow$	
	r $\longleftarrow$	$r \xleftarrow{\$} Z_p^*$
$z \leftarrow r \cdot w + k$	z $\longrightarrow$	$g^z \stackrel{?}{=} Y^r \cdot a$

Sigma Protocol

Schnorr DLOG

$P(w)$	g, q, p, Y	$V()$
$k \stackrel{\$}{\leftarrow} Z_p^*$ $a \leftarrow g^k$	$\xrightarrow{a}$	
	$\xleftarrow{r}$	$r \stackrel{\$}{\leftarrow} Z_p^*$
$z \leftarrow r \cdot w + k$	$\xrightarrow{z}$	$g^z \stackrel{?}{=} Y^r \cdot a$

- **Completeness**
- **Knowledge Soundness**
- **HV Zero-Knowledge**

Sigma Protocol

DLOG

$P(w)$	g, q, p, Y	$V()$
$k \xleftarrow{\$} Z_p^*$ $a \leftarrow g^k$	a →	
	← r	$r \xleftarrow{\$} Z_p^*$
$z \leftarrow r \cdot w + k$	z →	$g^z \stackrel{?}{=} Y^r \cdot a$

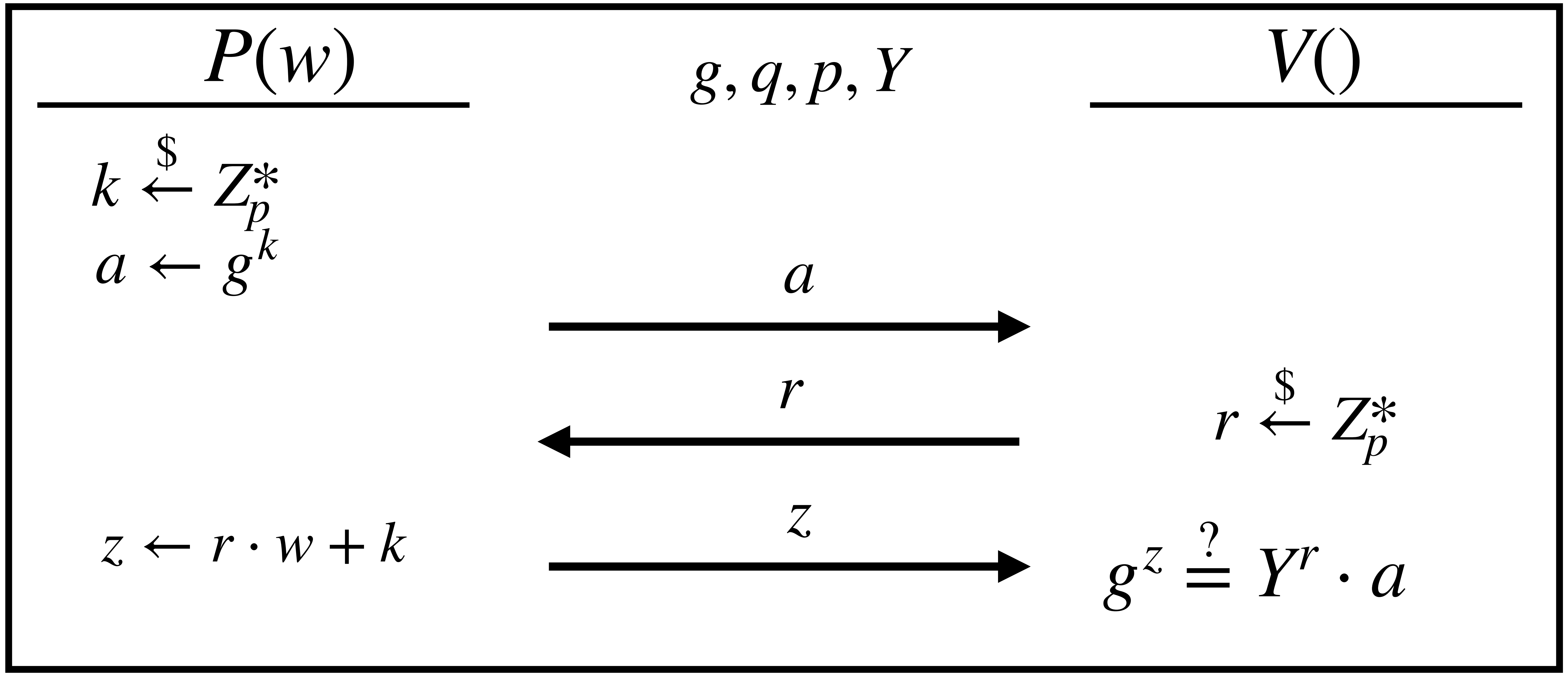
- **Completeness:**

$$g^z \stackrel{?}{=} Y^r \cdot a$$

$$g^{(r \cdot w + k)} \stackrel{?}{=} (g^w)^r \cdot g^k$$

$$g^{r \cdot w + k} = g^{w \cdot r + k}$$

Sigma Protocol
DLOG



- **Knowledge Soundness**

Given (a, r, z) and (a, r', z')

as valid transcripts.

Extract w in poly time.

$$g^z = Y^r \cdot a$$

$$g^{z'} = Y^{r'} \cdot a$$

Sigma Protocol

DLOG

$P(w)$	g, q, p, Y	$V()$
$k \xleftarrow{\$} Z_p^*$ $a \leftarrow g^k$	$a \longrightarrow$	
	$\longleftarrow r$	$r \xleftarrow{\$} Z_p^*$
$z \leftarrow r \cdot w + k$	$z \longrightarrow$	$g^z \stackrel{?}{=} Y^r \cdot a$

- **Knowledge Soundness**

Given (a, r, z) and (a, r', z')

as valid transcripts.

Extract w in poly time.

$$g^z = Y^r \cdot a$$
$$g^{z'} = Y^{r'} \cdot a$$
$$\implies g^{(z-z')} = Y^{(r-r')}$$

Sigma Protocol

DLOG

$P(w)$	g, q, p, Y	$V()$
$k \xleftarrow{\$} Z_p^*$ $a \leftarrow g^k$	$\xrightarrow{\quad a \quad}$	
	$\xleftarrow{\quad r \quad}$	$r \xleftarrow{\$} Z_p^*$
$z \leftarrow r \cdot w + k$	$\xrightarrow{\quad z \quad}$	$g^z \stackrel{?}{=} Y^r \cdot a$

- **Knowledge Soundness**

Given (a, r, z) and (a, r', z')

as valid transcripts.

Extract w in poly time.

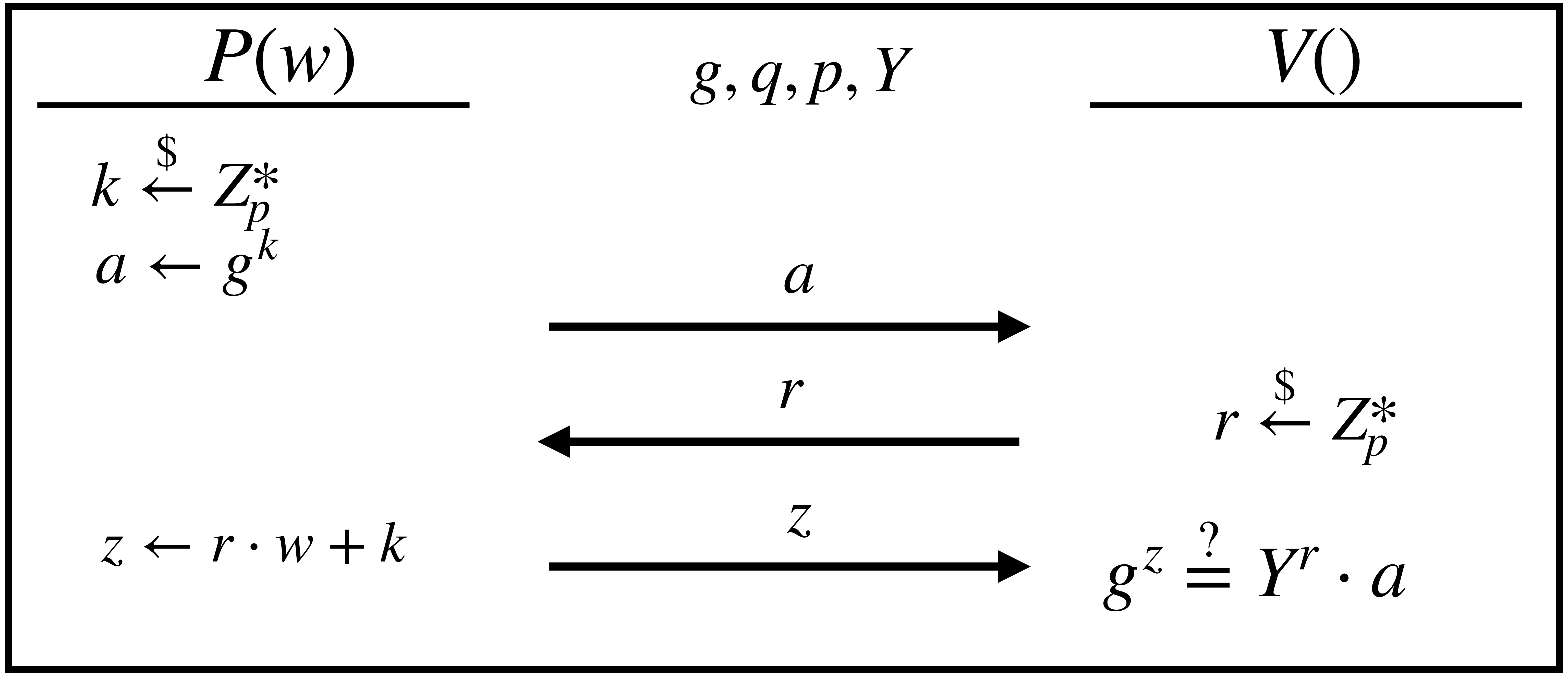
$$g^z = Y^r \cdot a$$
$$g^{z'} = Y^{r'} \cdot a$$

$$\implies g^{(z-z')} = Y^{(r-r')} \implies g^{(z-z')/(r-r'))} = Y$$

$$\implies w = (z - z')/(r - r')$$

Sigma Protocol

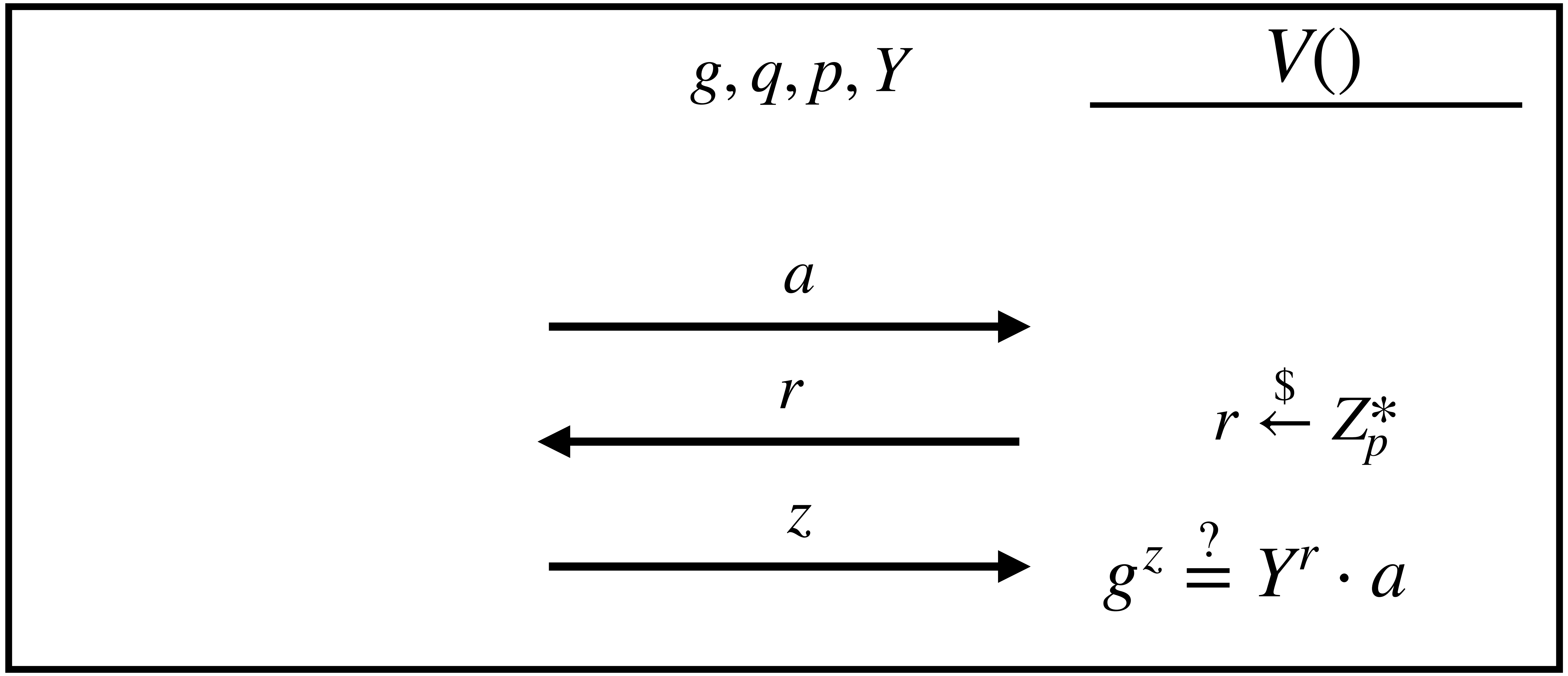
DLOG



- **HV Zero-Knowledge**

A valid transcript can be efficiently simulated.

Sigma Protocol
DLOG



- **HV Zero-Knowledge**

A valid transcript can be efficiently simulated.

Sigma Protocol

DLOG

$S()$	g, q, p, Y	$V()$
$z, r \xleftarrow{\$} Z_p^*$		
$a \leftarrow g^z \cdot Y^{-r}$	(a, r, z)	$g^z \stackrel{?}{=} Y^r \cdot a$

- **HV Zero-Knowledge**

A valid transcript can be efficiently simulated.

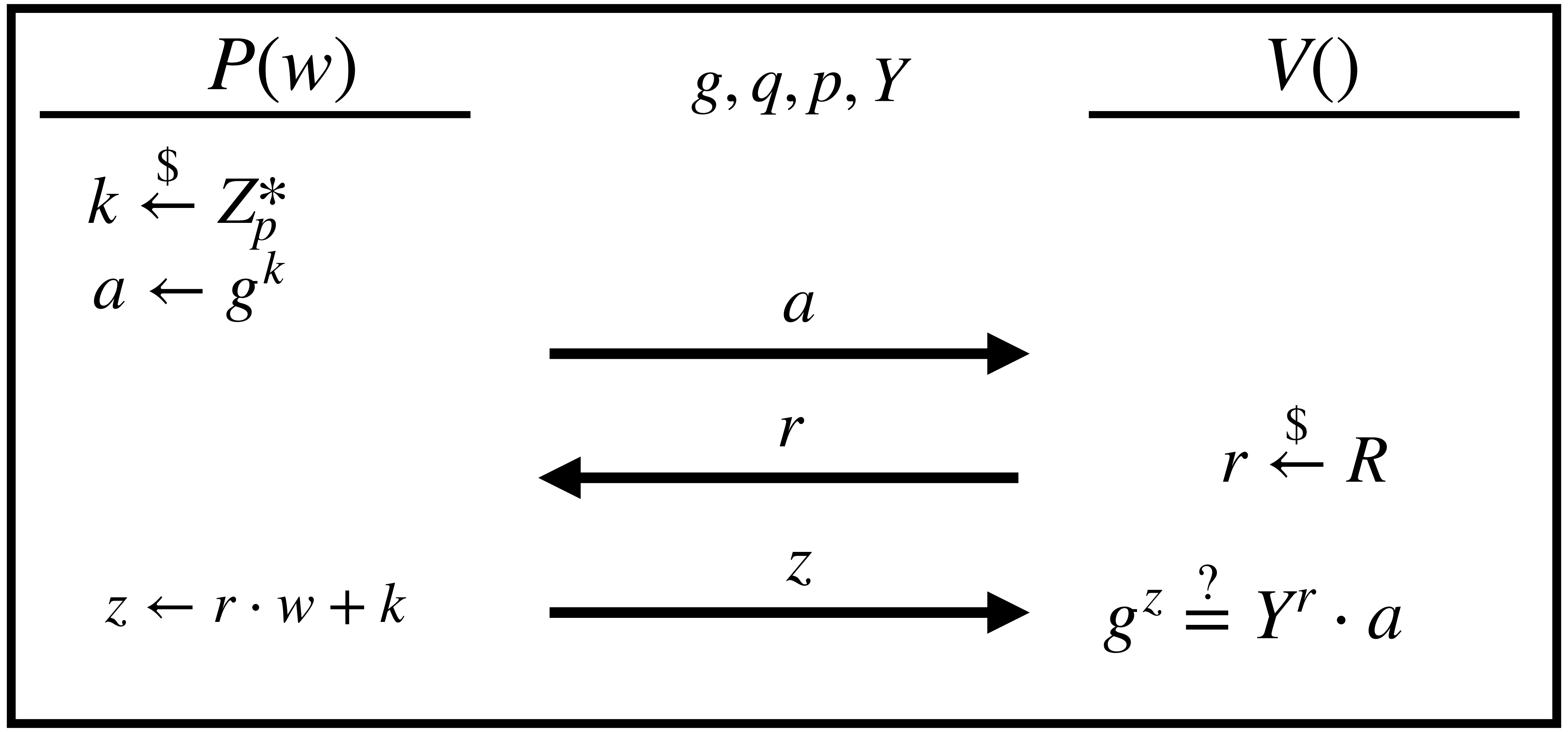
Sigma Protocol
ROM

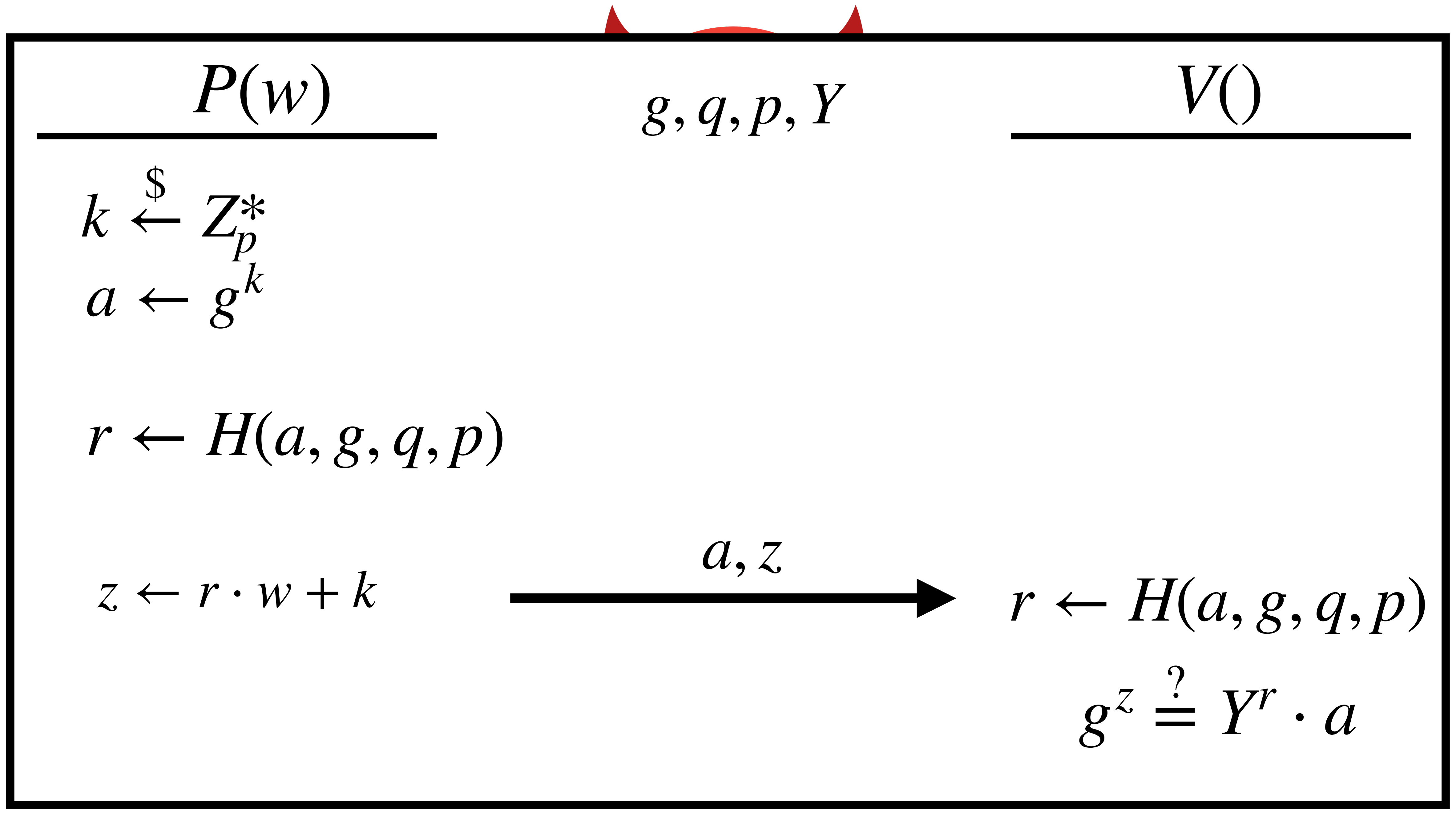
Blackbox oracle $H(\,.\,)$ that returns consistent but uniformly random values.

Realized using a hash function e.g. SHA256

Sigma Protocol

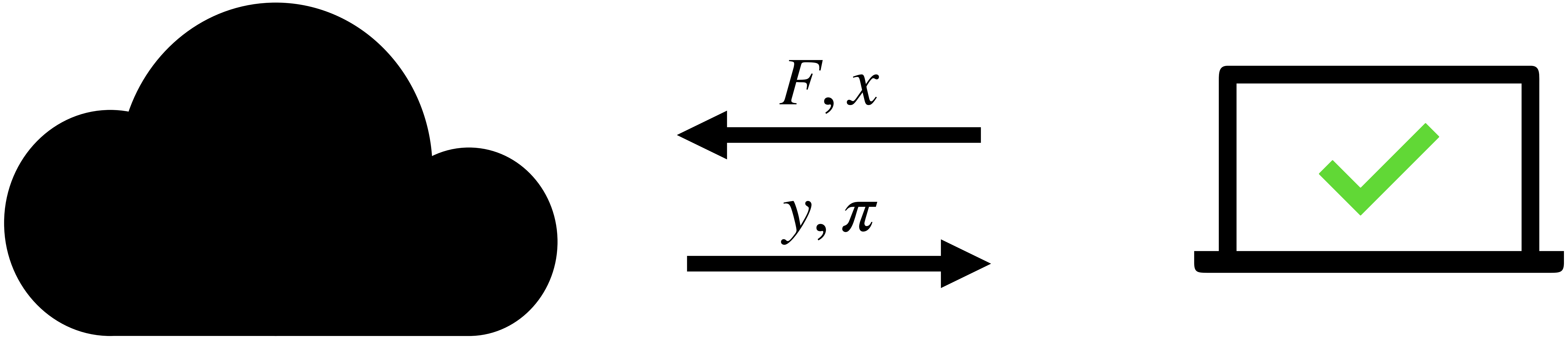
Non-interactivity via Fiat Shamir Heuristic





General Purpose Verifiable Computation

Task: Compute $F(x)$



$F(x) \rightarrow y$

$Prove(F, x, y) \rightarrow \pi$

$Verify(F, x, y, \pi) \rightarrow 0/1$

General Purpose Verifiable Computation

Succinct **N**on-interactive **ARG**ument

Soundness: There exists w such that $F(x, w) = y$

General Purpose Verifiable Computation

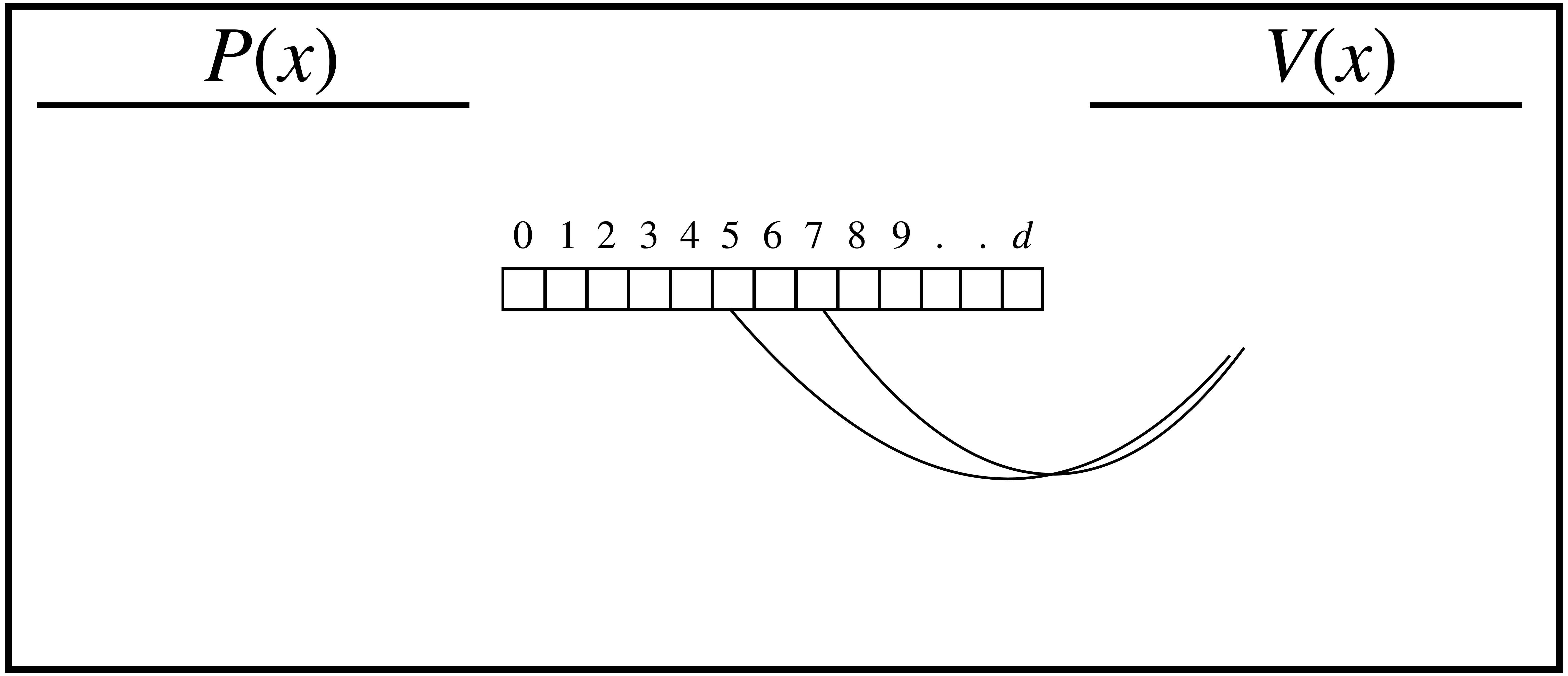
Succinct **N**on-interactive **AR**gument of **K**nowledge

Knowledge Soundness:

There exists w **known by the prover** such that $F(x, w) = y$

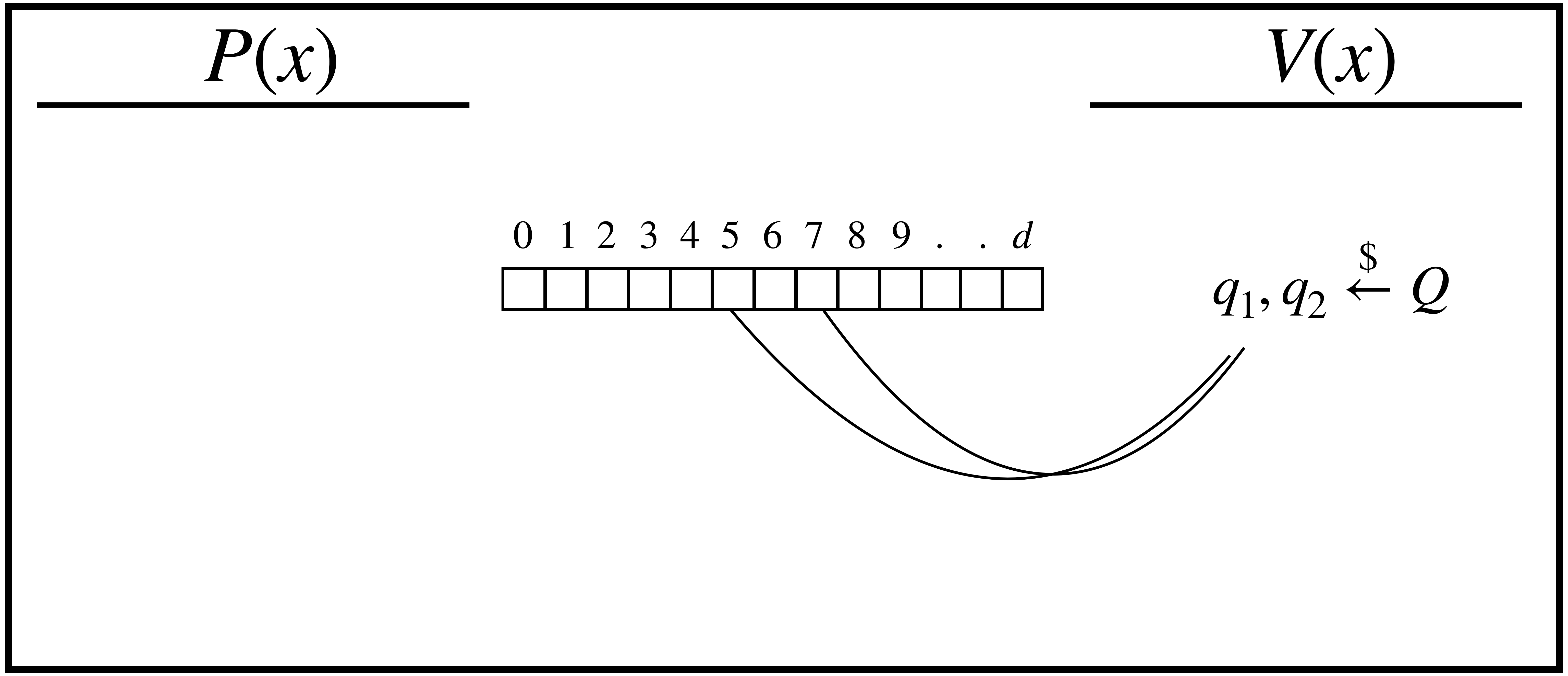
PCP

[BFLS'91]



"In this setup, a single reliable PC can monitor the operation of a herd of supercomputers working with possibly extremely powerful but unreliable software and untested hardware."

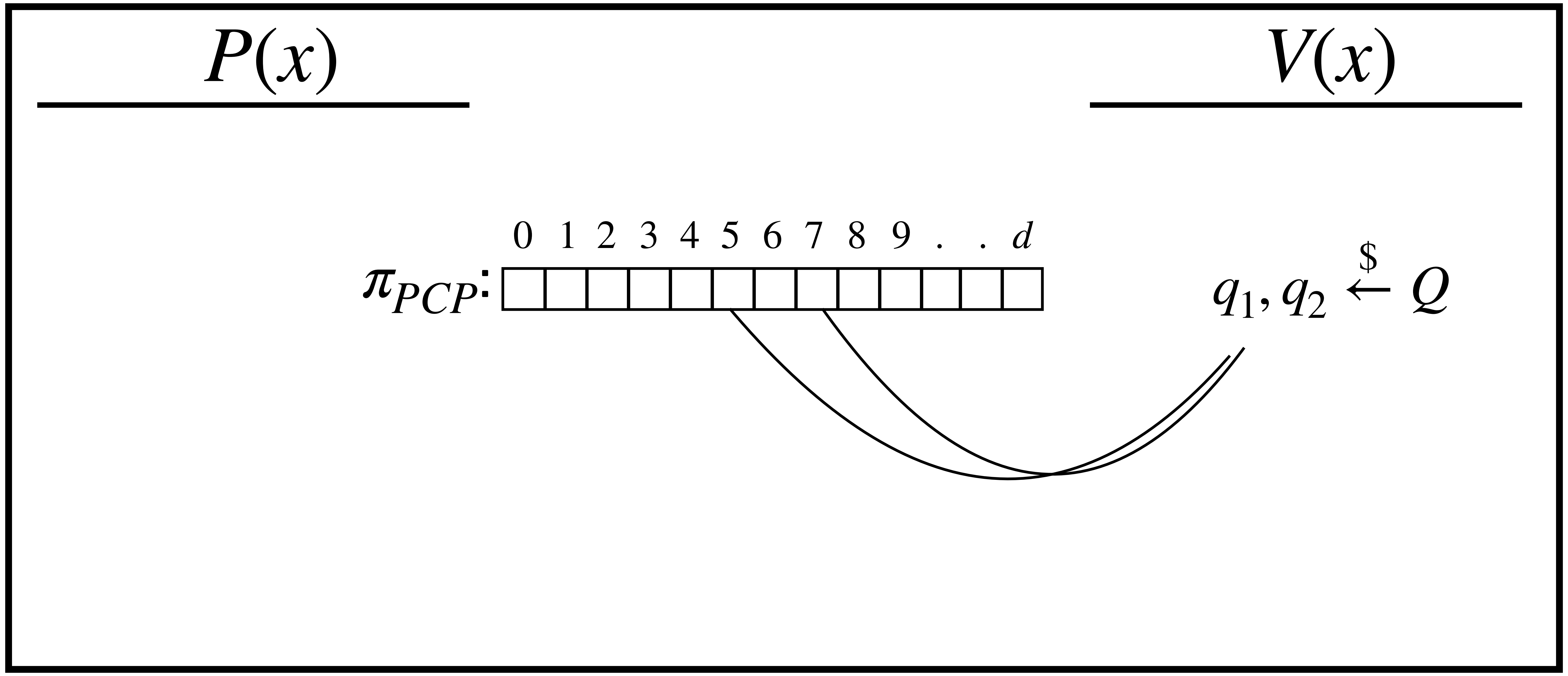
PCP
[BFLS'91]



"In this setup, a single reliable PC can monitor the operation of a herd of supercomputers working with possibly extremely powerful but unreliable software and untested hardware."

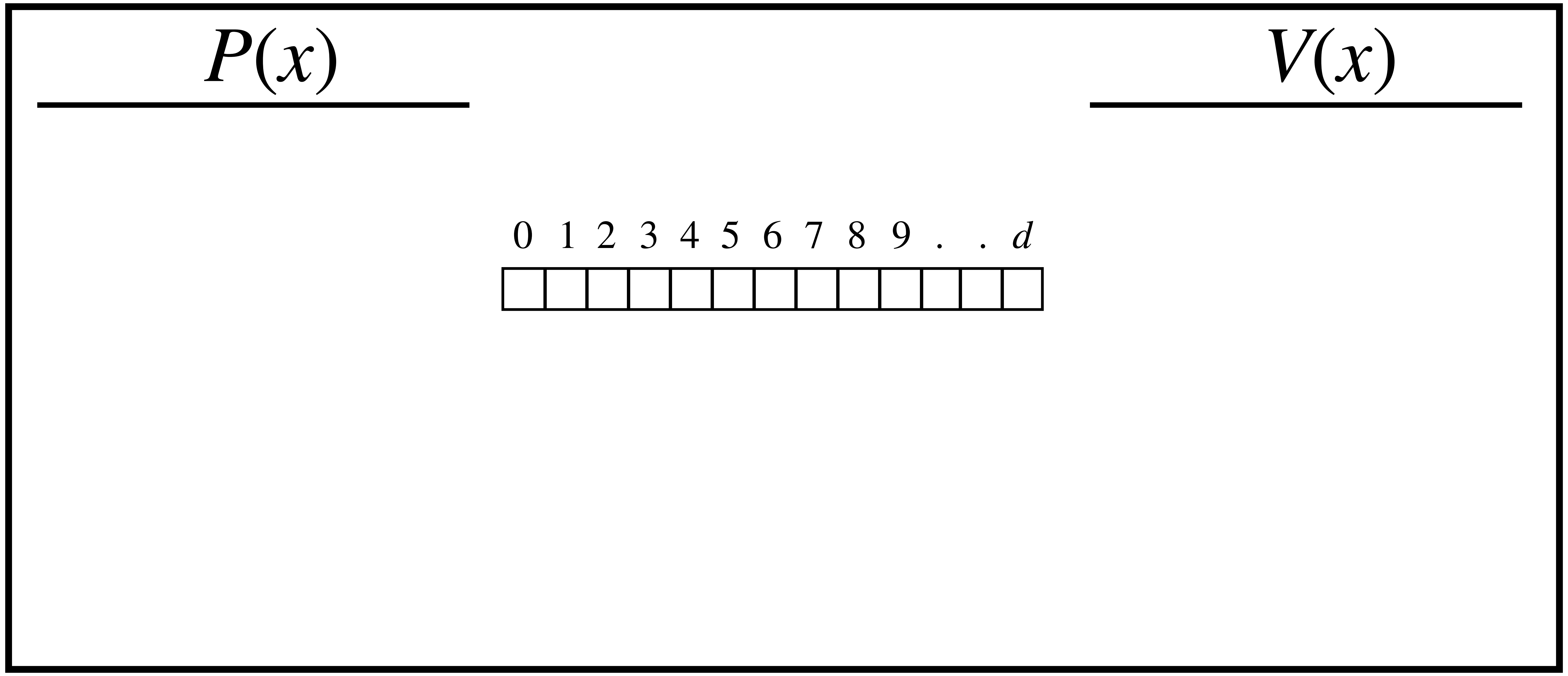
PCP

[BFLS'91]



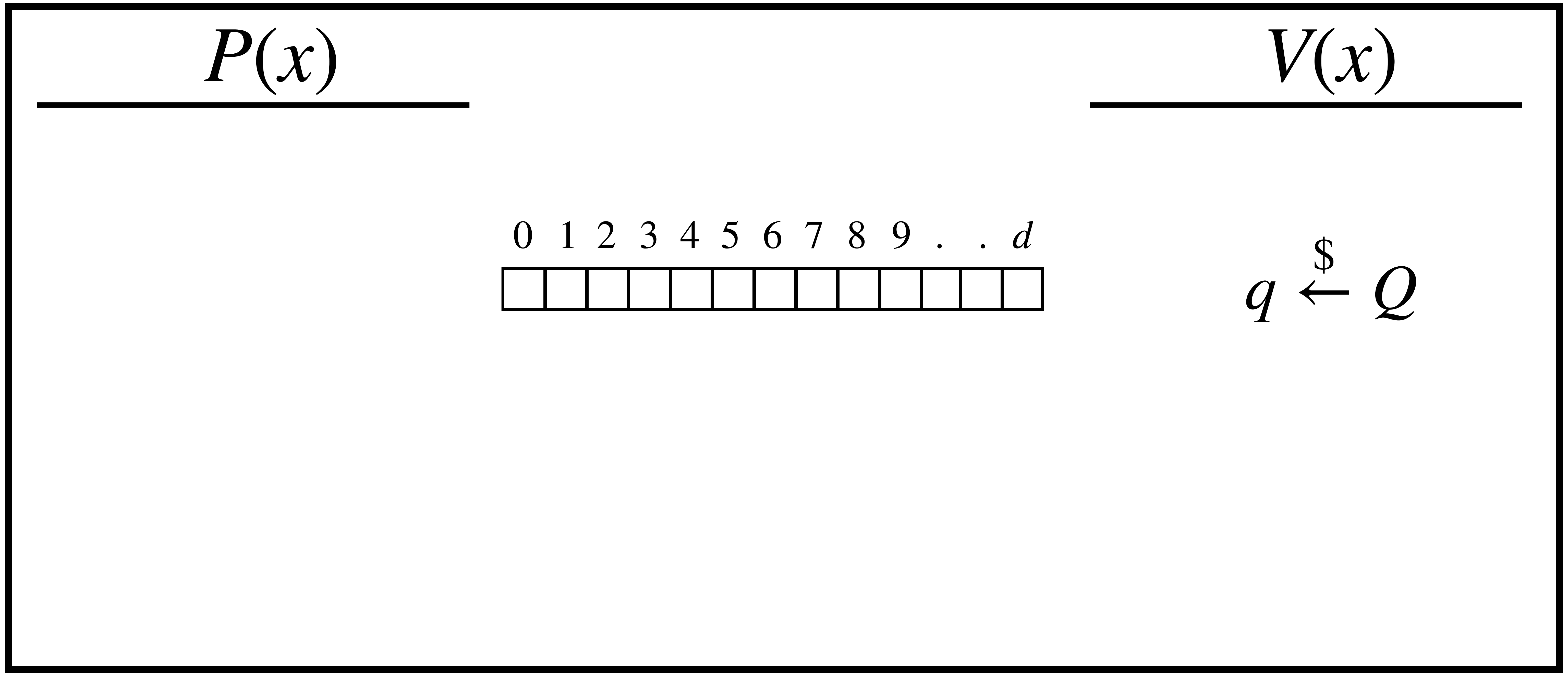
"In this setup, a single reliable PC can monitor the operation of a herd of supercomputers working with possibly extremely powerful but unreliable software and untested hardware."

PCP
[Killian'92]

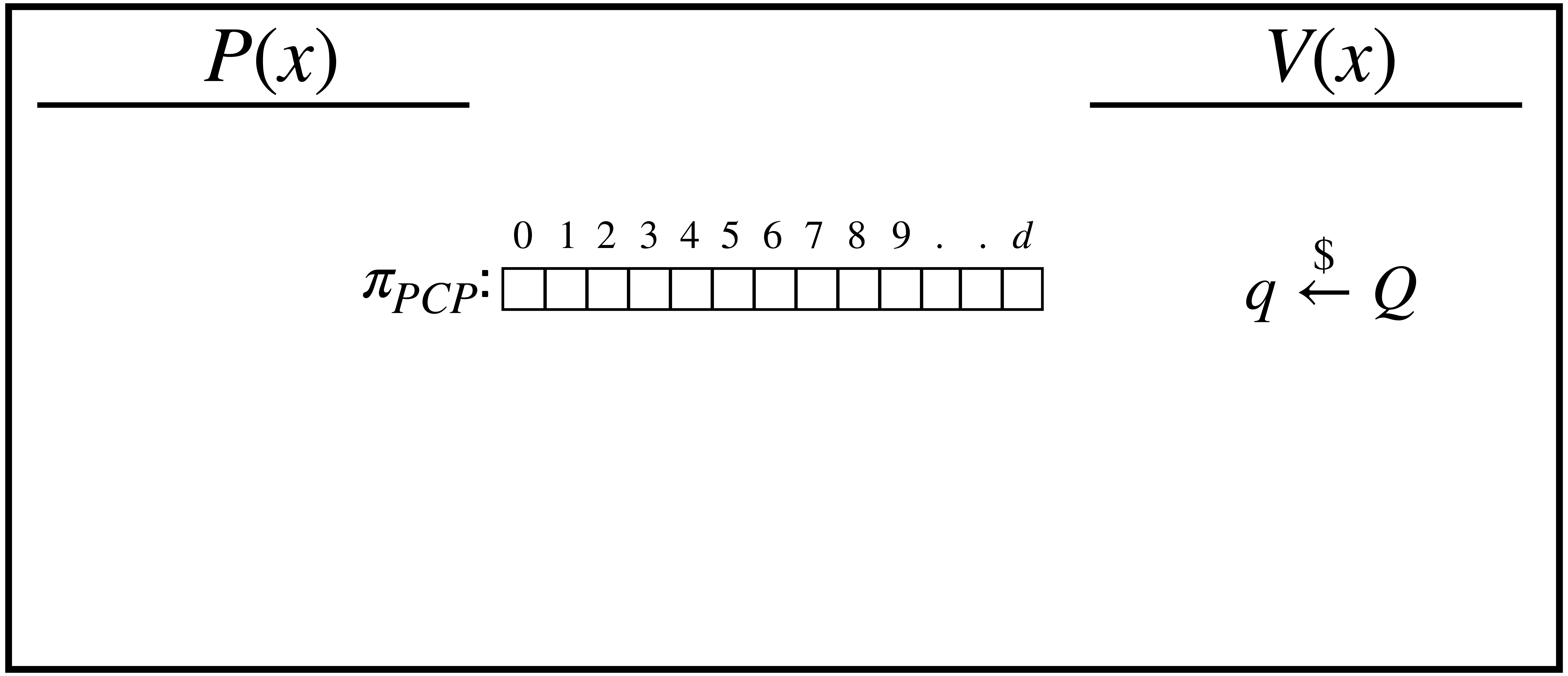


PCP

[Killian'92]



PCP
[Killian'92]

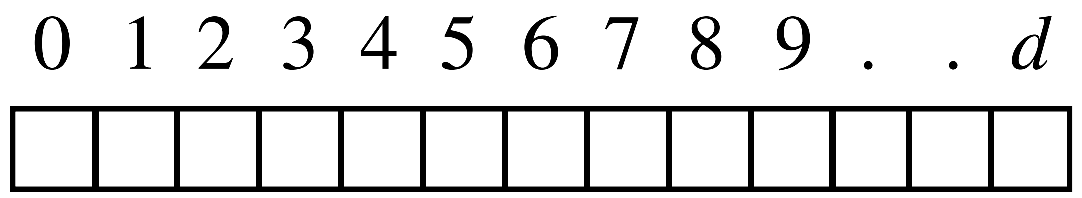


PCP

[Killian'92]

$P(x)$

$V(x)$



PCP

[Killian'92]

$P(x)$

$V(x)$

0 1 2 3 4 5 6 7 8 9 . . d

$q \xleftarrow{\$} Q$

PCP
[Killian'92]

$P(x)$ | $V(x)$

π: 0 1 2 3 4 5 6 7 8 9 . . d

$q \xleftarrow{\$} Q$

PCP

[Killian'92]

$P(x)$

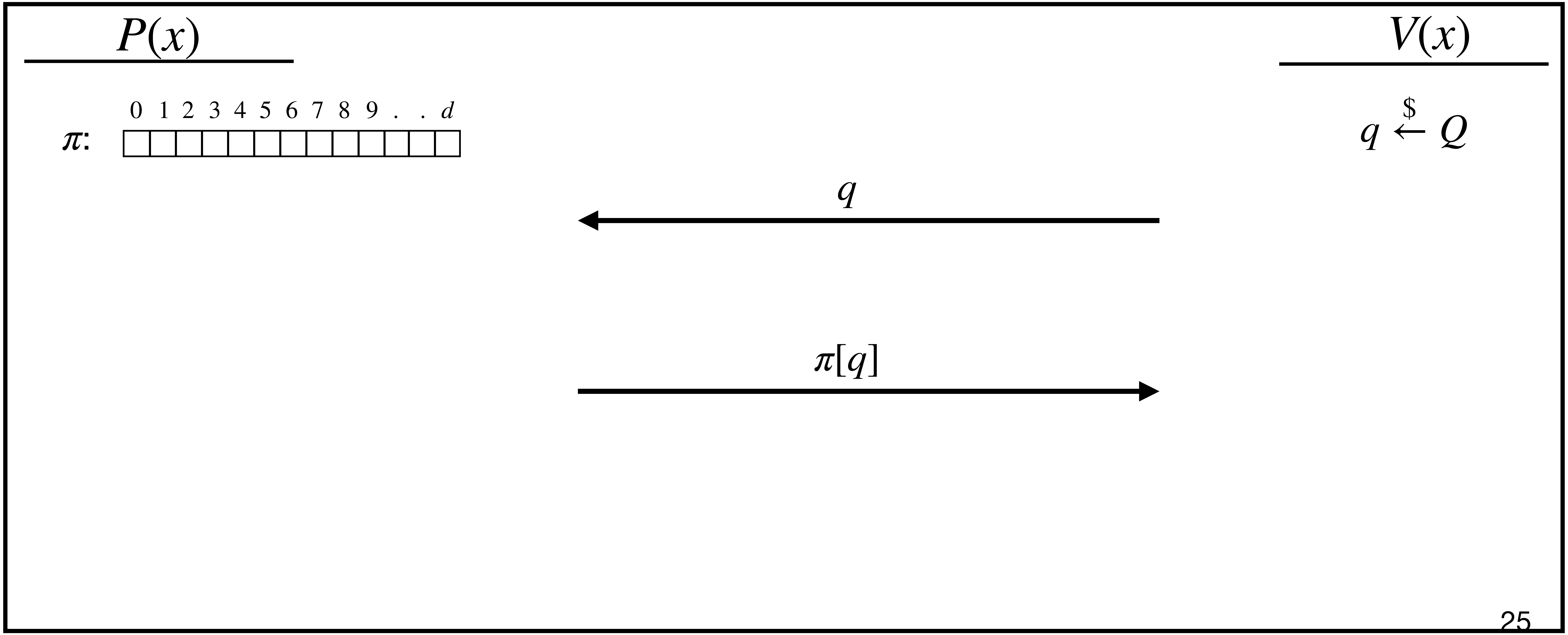
$V(x)$

π: 0 1 2 3 4 5 6 7 8 9 . . d

$q \xleftarrow{\$} Q$

q

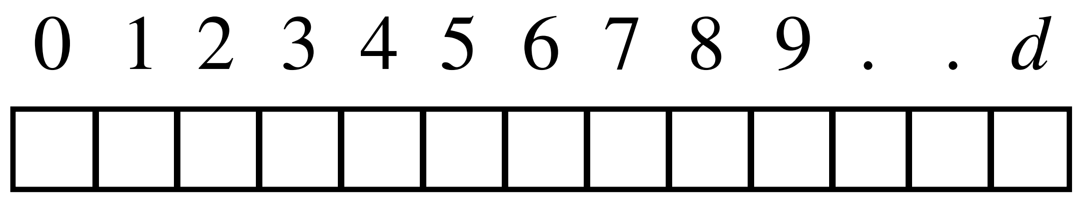
PCP
[Killian'92]



PCP
[Killian'92]

$P(x)$

$V(x)$



PCP

[Killian'92]

$P(x)$	$V(x)$

0 1 2 3 4 5 6 7 8 9 . . d

$q \xleftarrow{\$} Q$

PCP

[Killian'92]

$P(x)$	$V(x)$

π: $0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ .\ .\ d$

$$q \xleftarrow{\$} Q$$

PCP

[Killian'92]

$P(x)$

$V(x)$

0 1 2 3 4 5 6 7 8 9 . . d

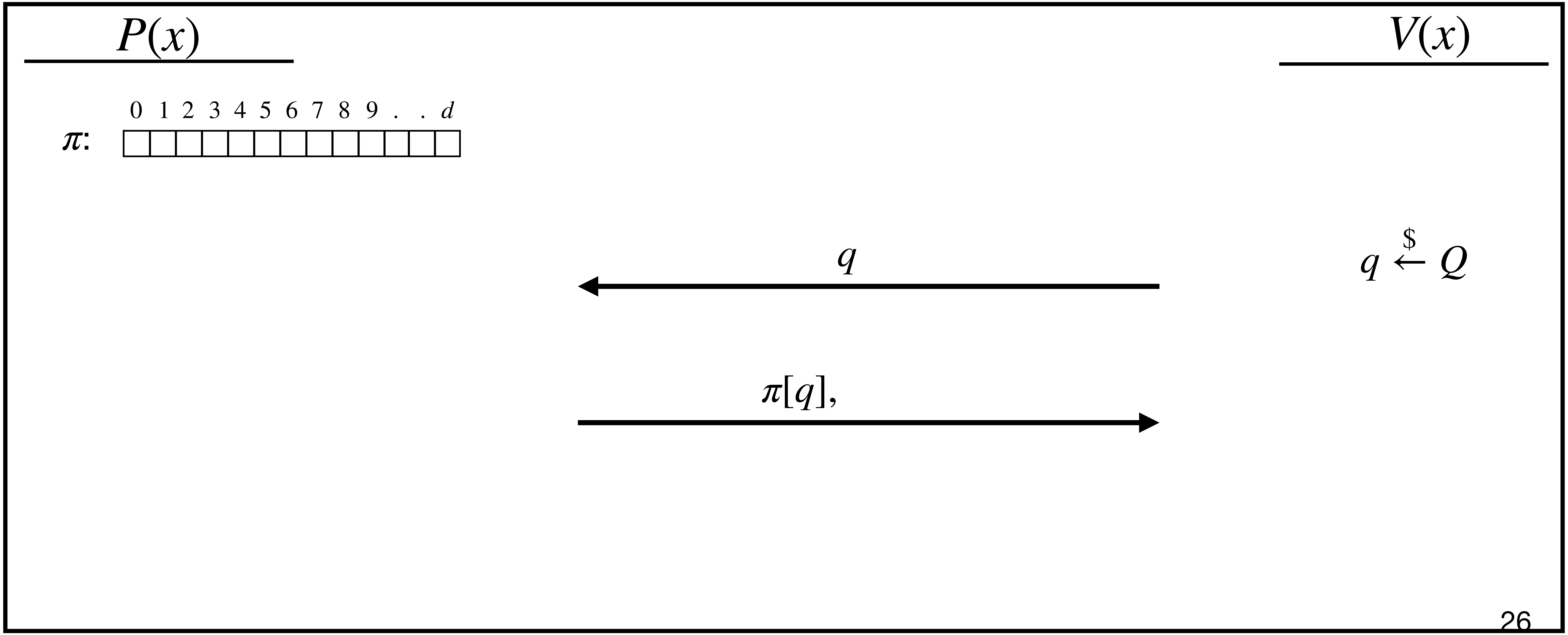
π:

$q \xleftarrow{\$} Q$

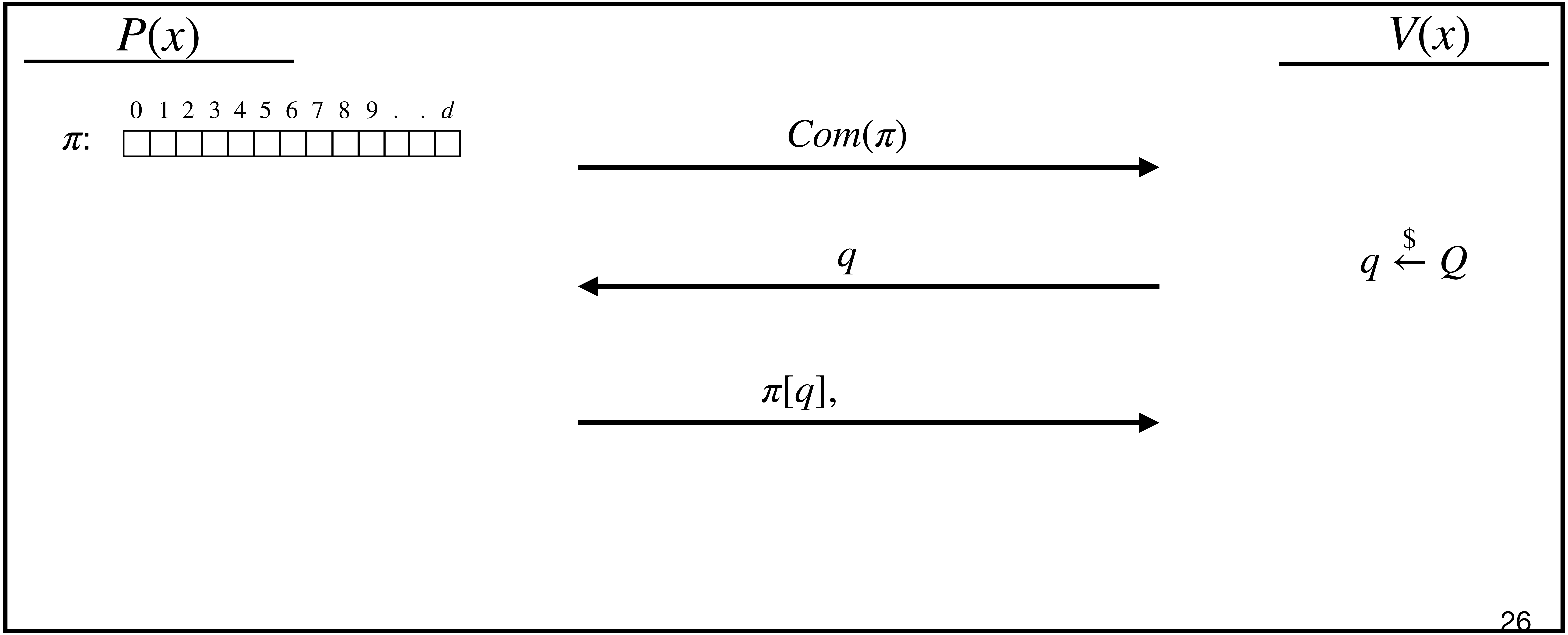
q ←

PCP

[Killian'92]

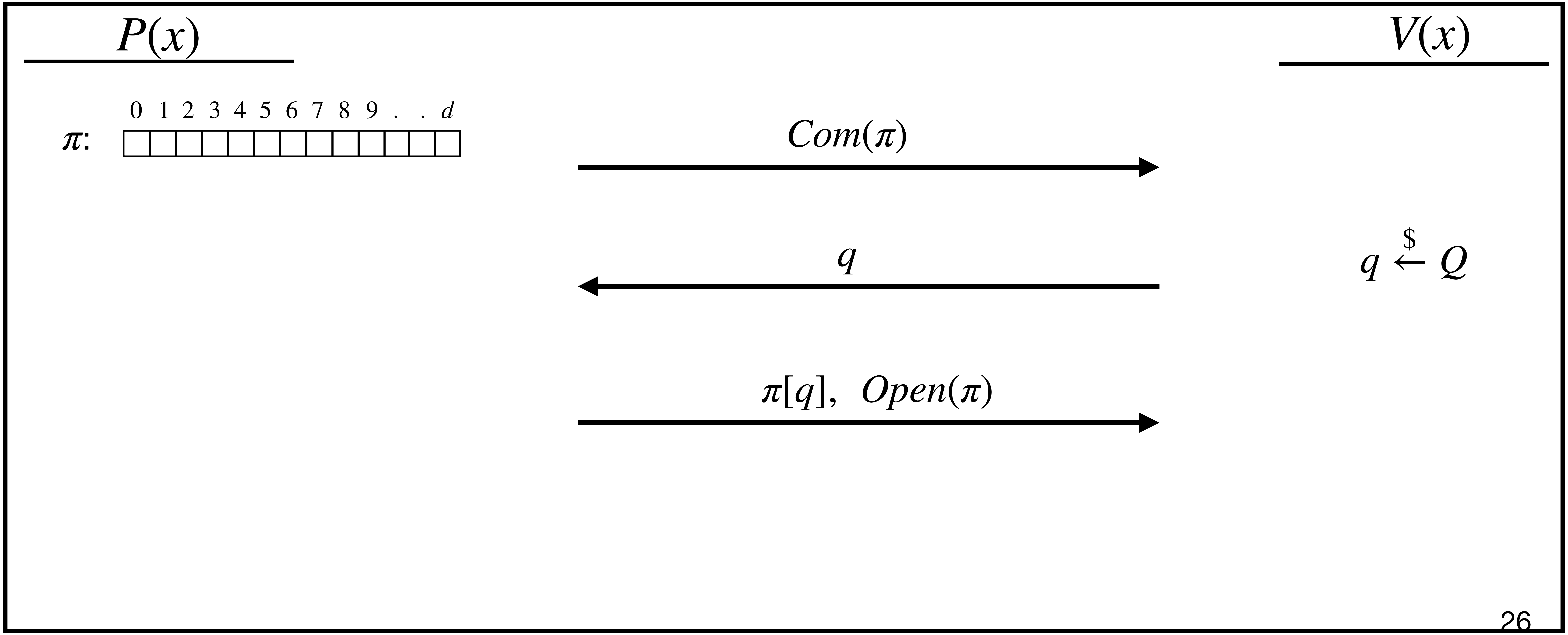


PCP
[Killian'92]



PCP

[Killian'92]

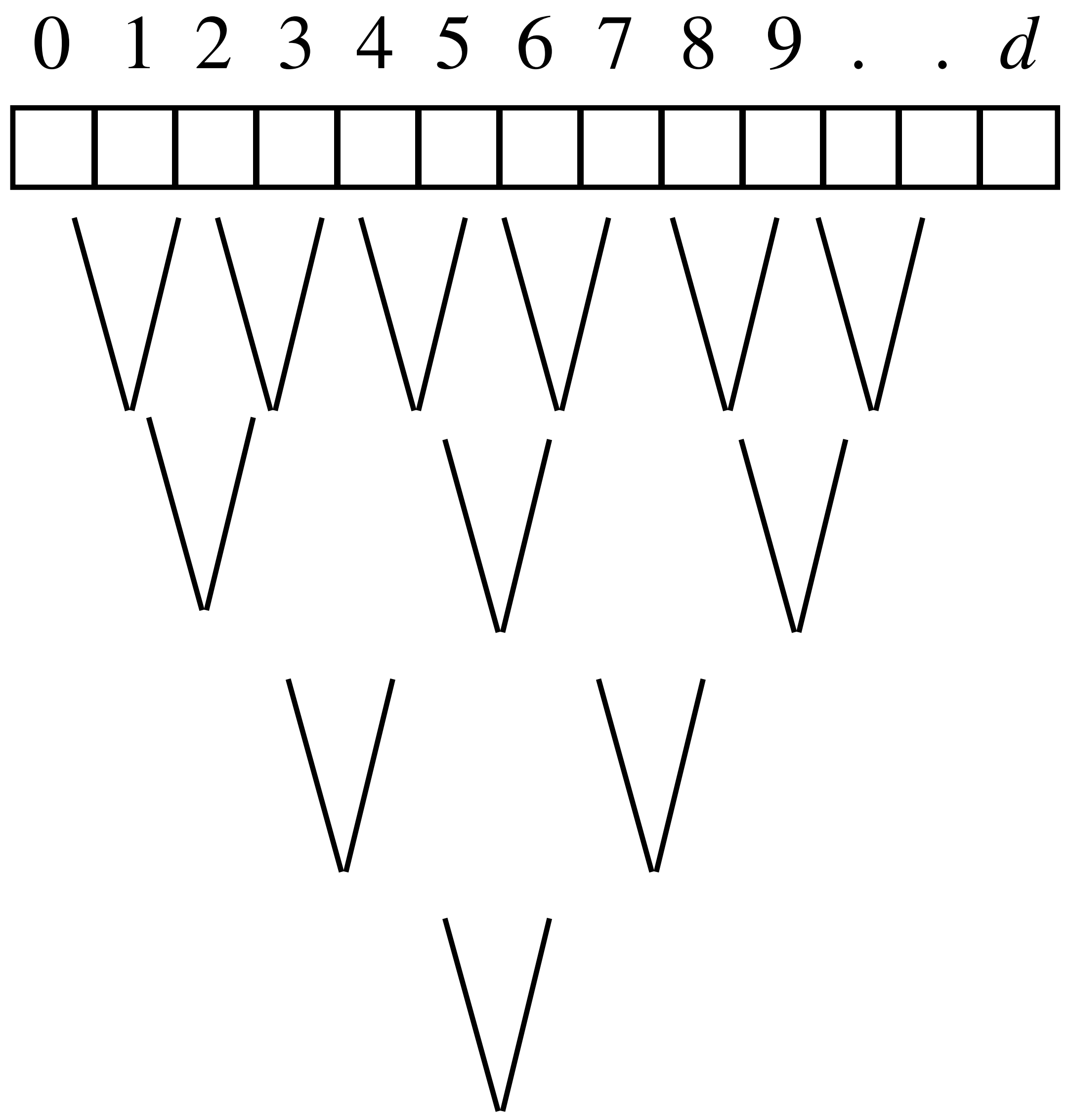


PCP

[Killian'92] Use a Vector Commitment to π

$P(x)$

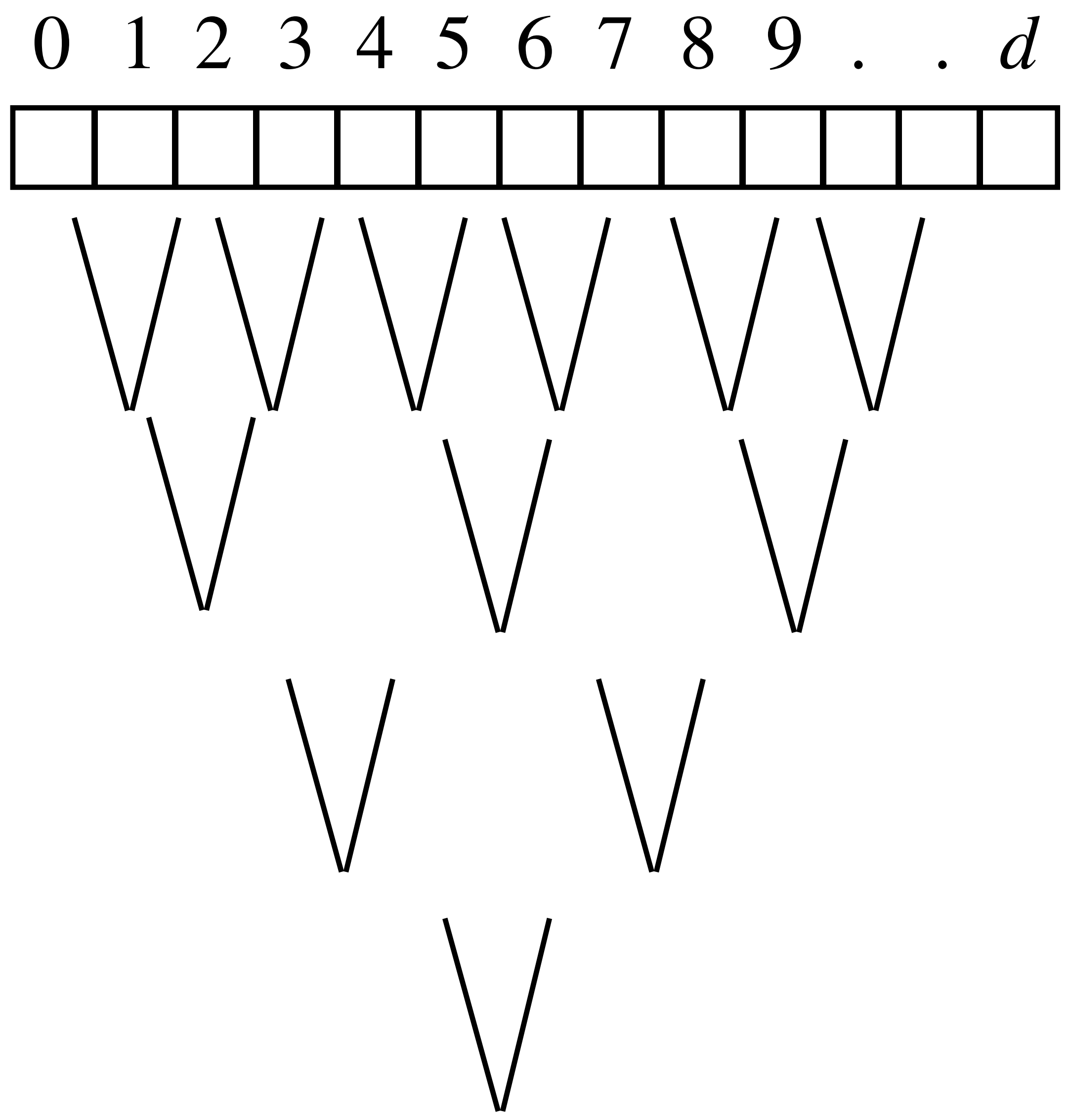
$V(x)$



PCP

[Killian'92] Use a Vector Commitment to π

$P(x)$



$V(x)$

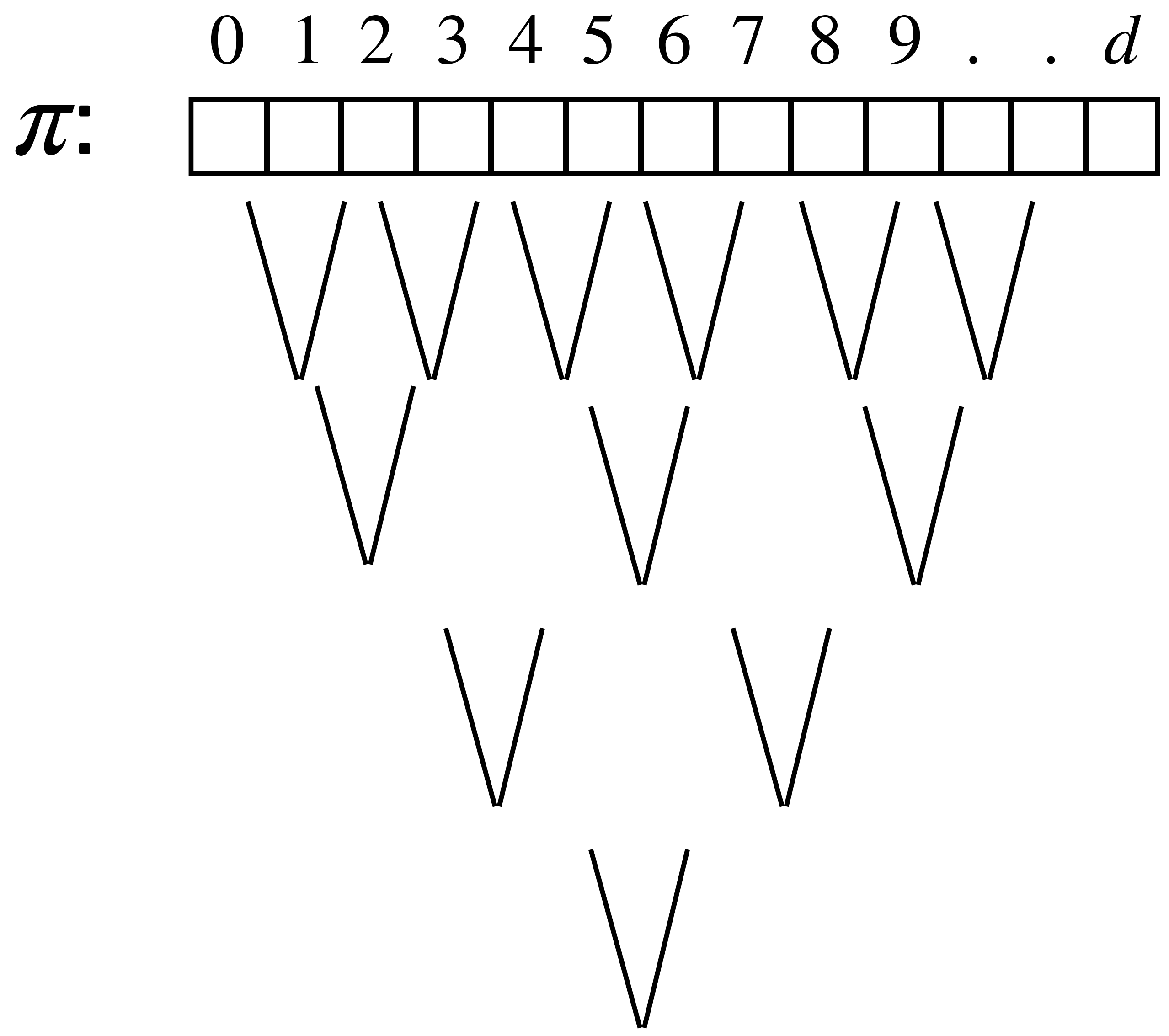
$q \xleftarrow{\$} Q$

PCP

[Killian'92] Use a Vector Commitment to π

$P(x)$

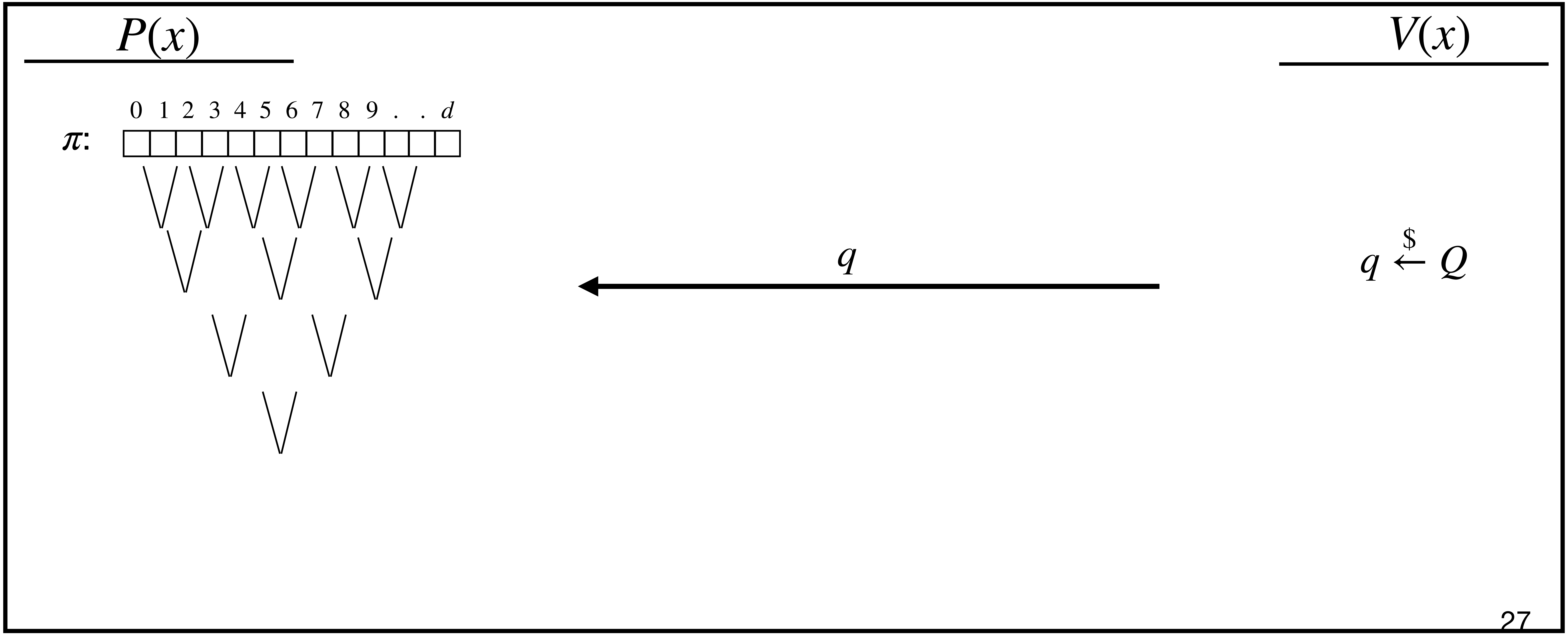
$V(x)$



$q \xleftarrow{\$} Q$

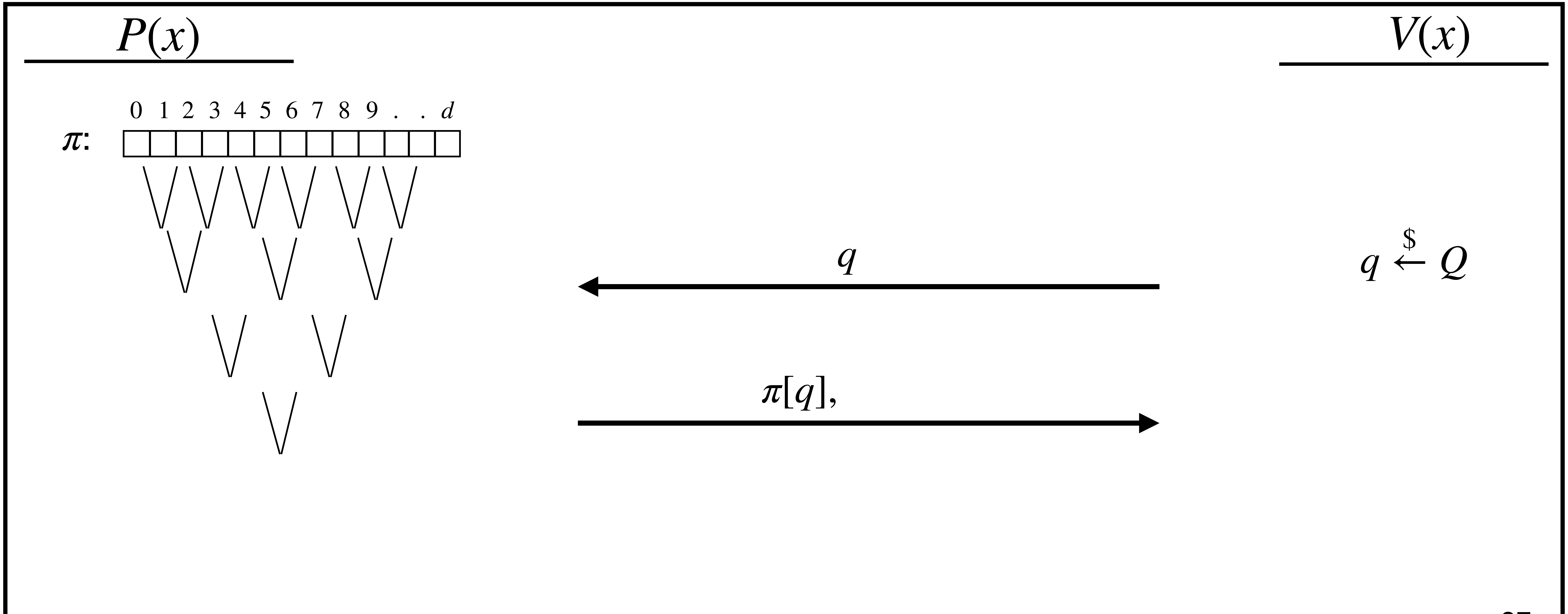
PCP

[Killian'92] Use a Vector Commitment to π



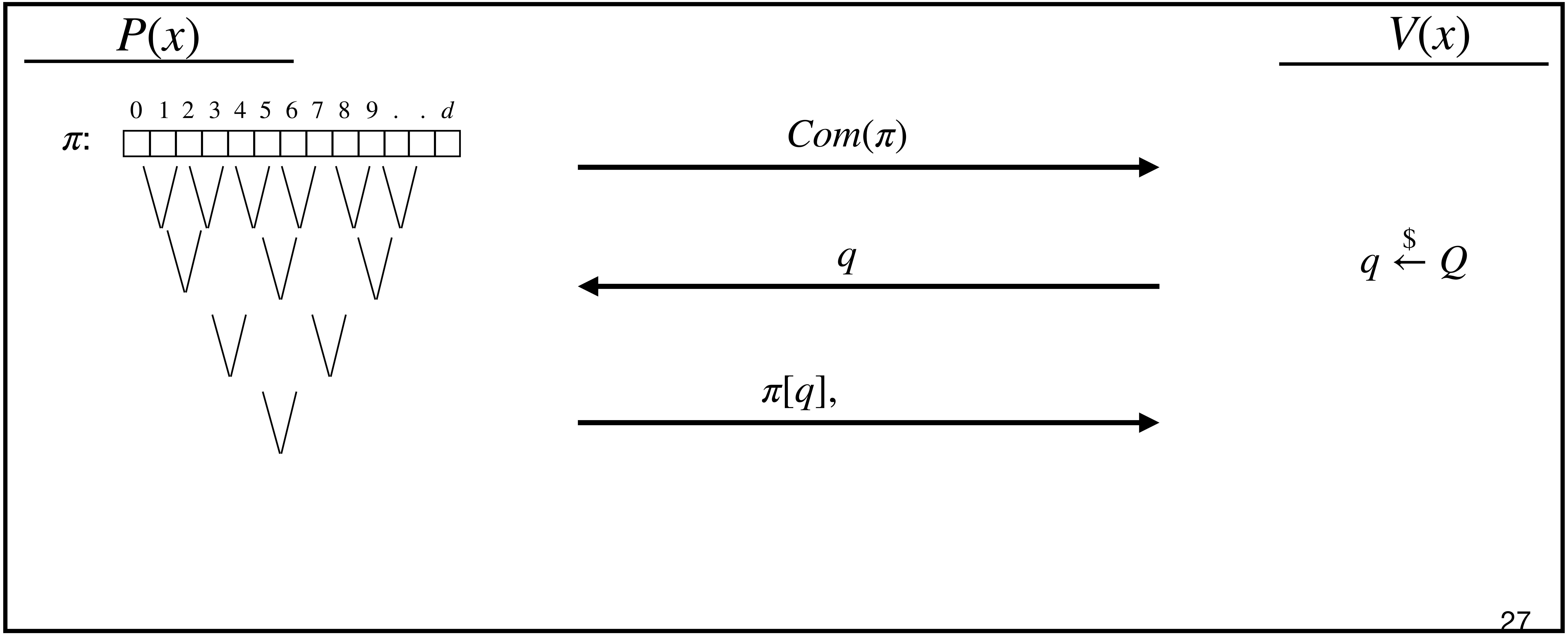
PCP

[Killian'92] Use a Vector Commitment to π



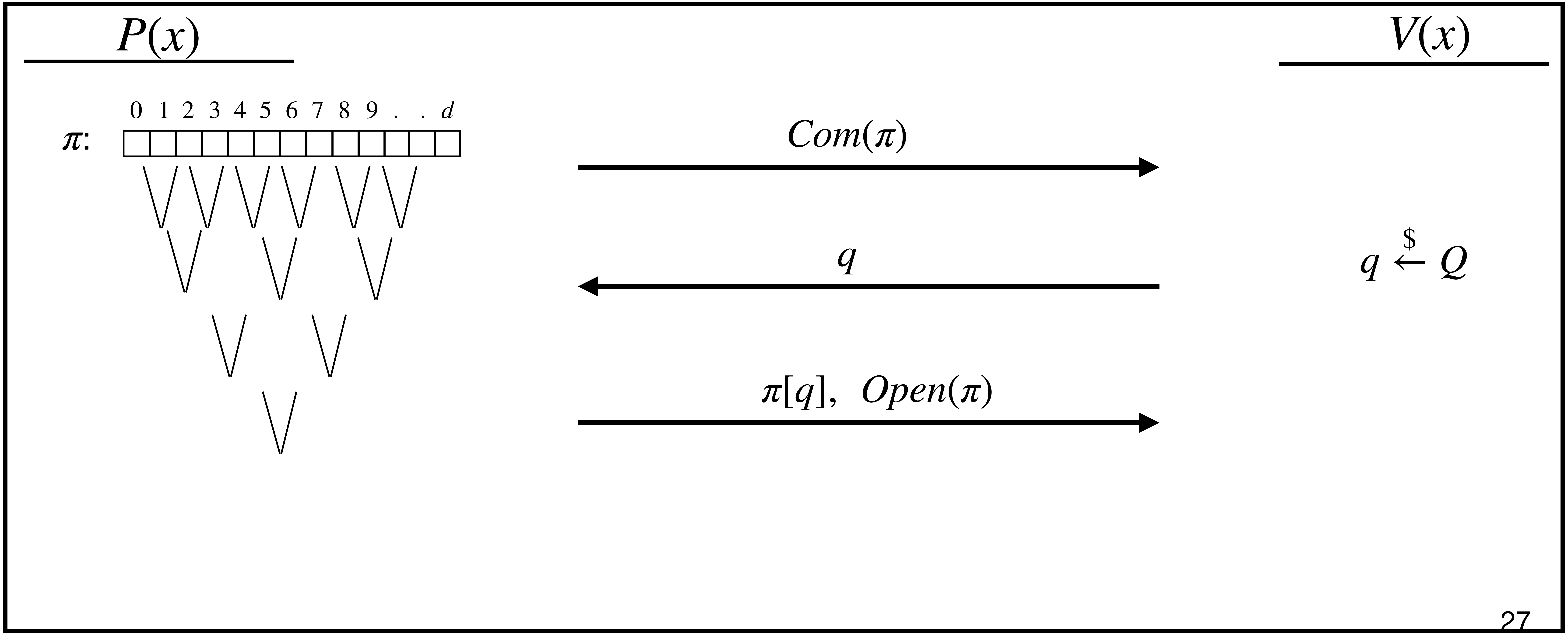
PCP

[Killian'92] Use a Vector Commitment to π



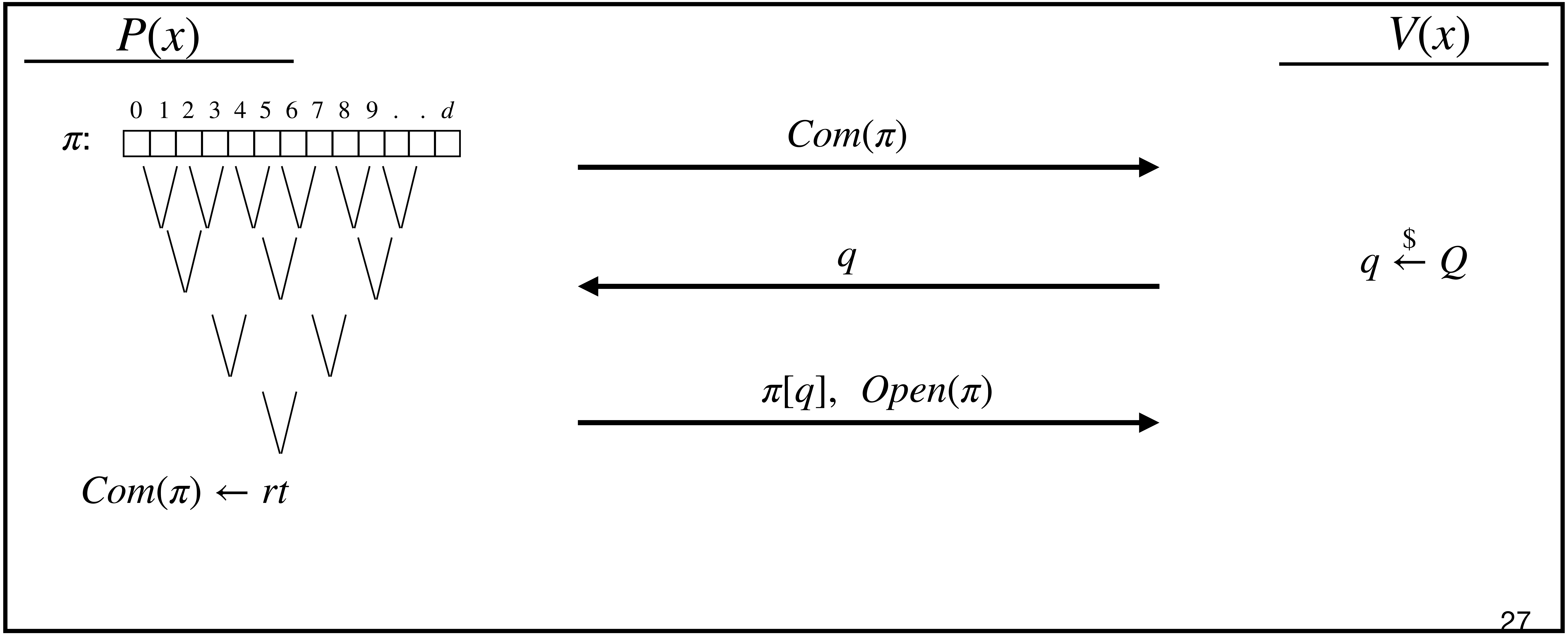
PCP

[Killian’92] Use a Vector Commitment to π



PCP

[Killian'92] Use a Vector Commitment to π

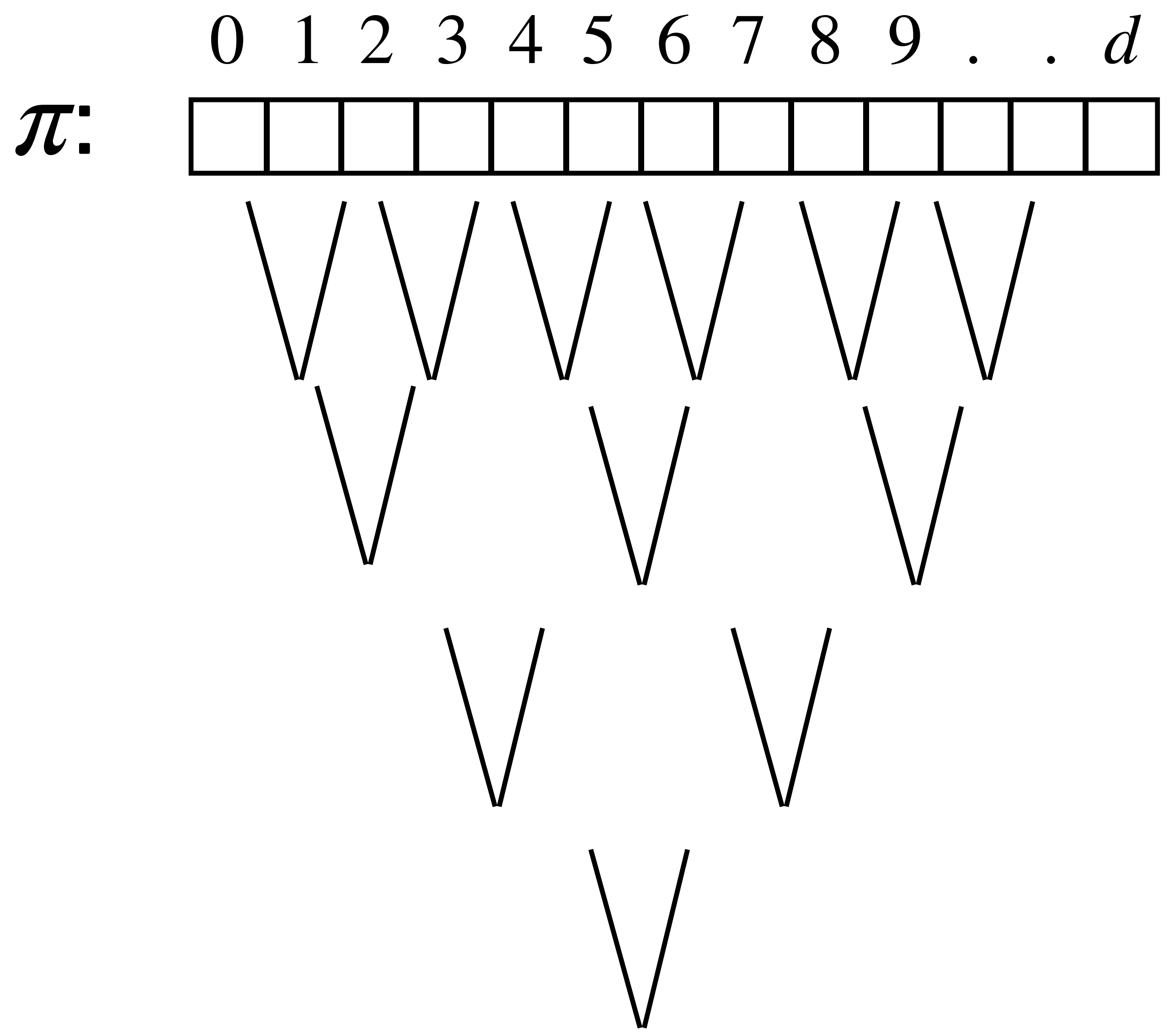


PCP

[Killian'92] Use a Vector Commitment to π

$P(x)$

$V(x)$



$Com(\pi)$ →

$q \xleftarrow{\$} Q$

← q

$\pi[q],\ Open(\pi)$ →

$Com(\pi) \leftarrow rt$

$Open(q, \pi)$: Authentication path of q in π

PCP

Polynomial Commitment

P		V
$p(x) = x^d + \ldots + x^5 + 1$		

PCP

Polynomial Commitment

P | V

$p(x) = x^d + \ldots + x^5 + 1$

PCP

Polynomial Commitment

P V

$p(x) = x^d + \ldots + x^5 + 1$

$Com(p(x))$

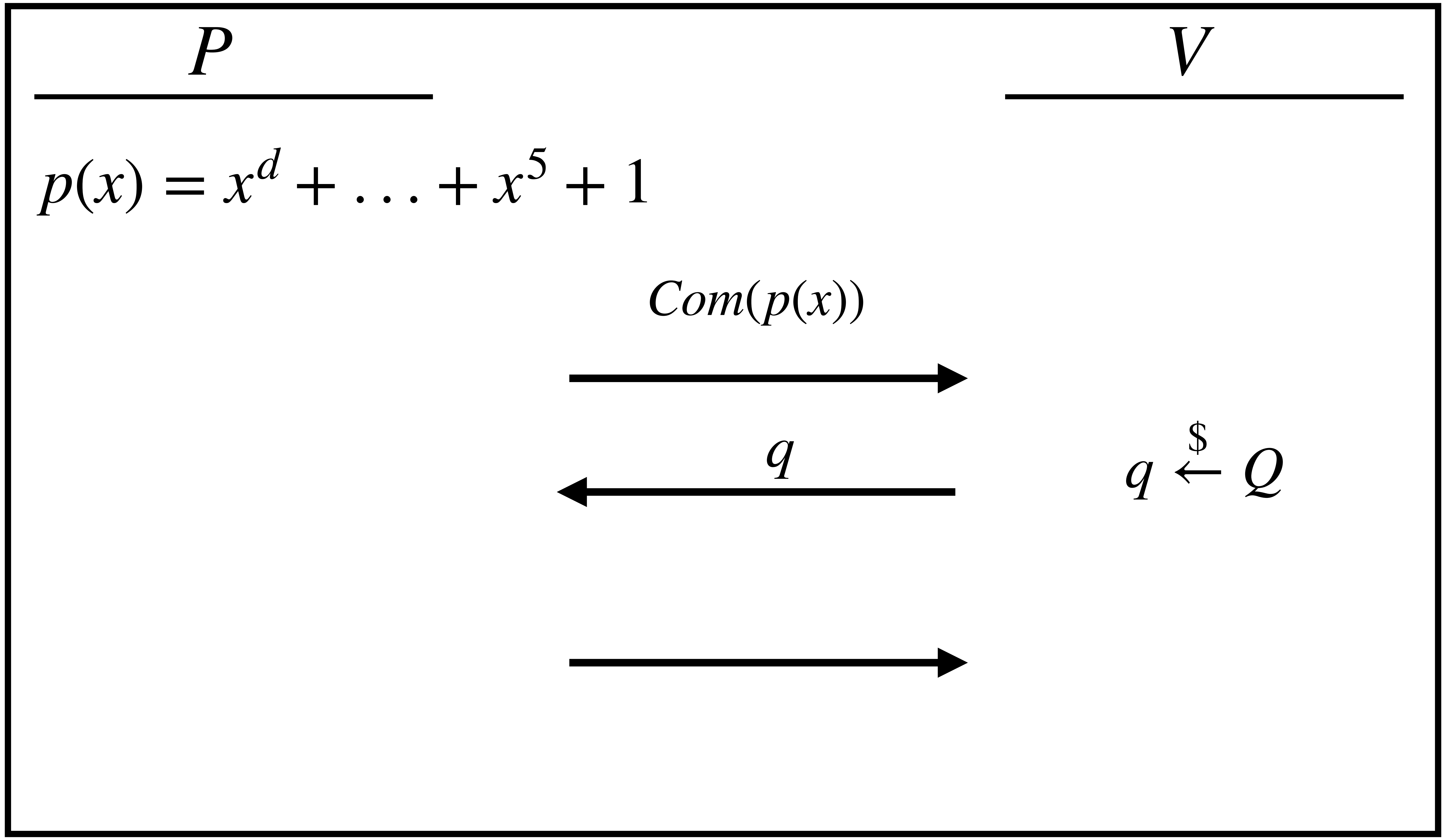
PCP

Polynomial Commitment

P		V
$p(x) = x^d + \ldots + x^5 + 1$		
	$Com(p(x))$ $\longrightarrow$	
		$q \xleftarrow{\$} Q$

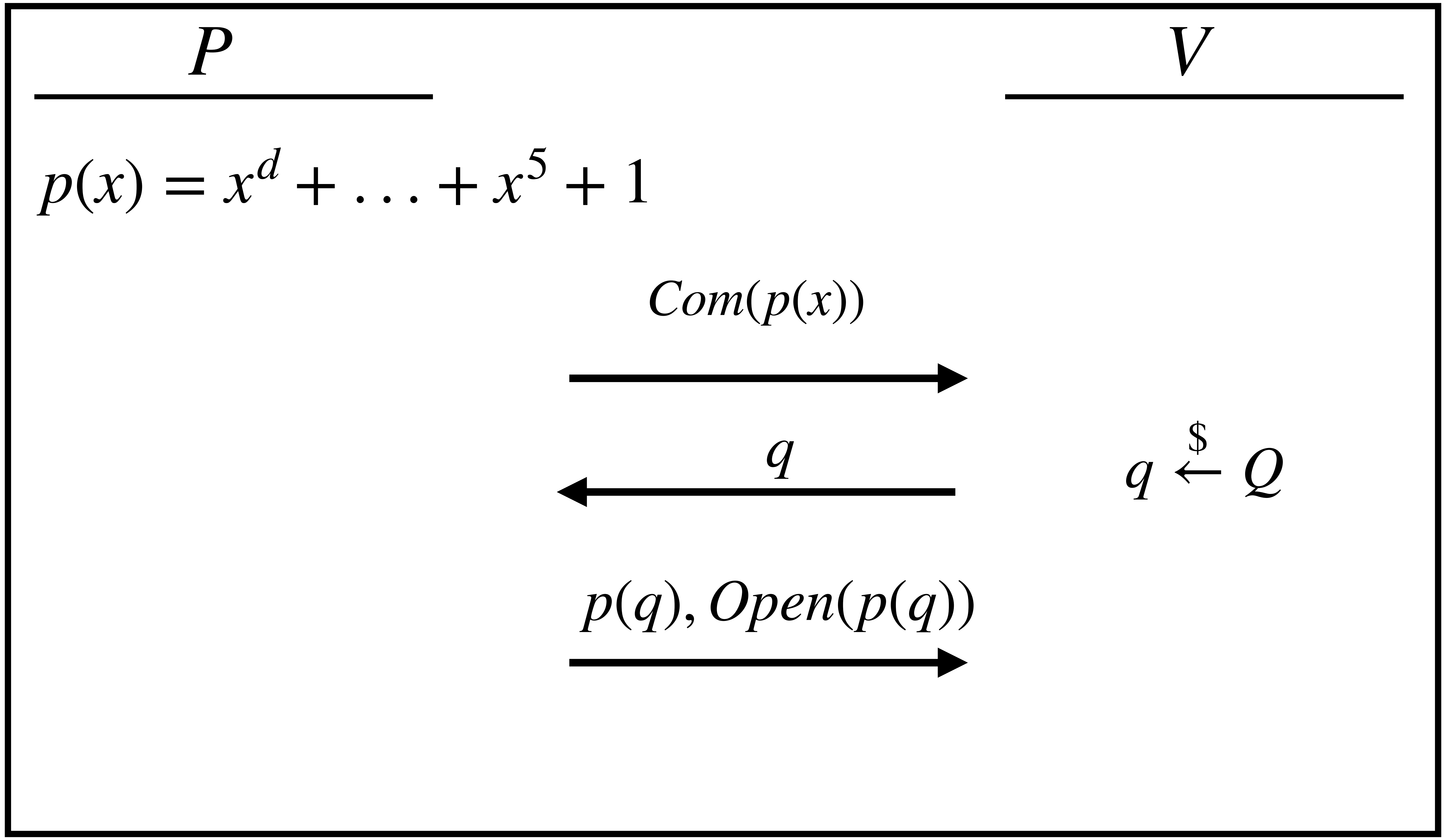
PCP

Polynomial Commitment

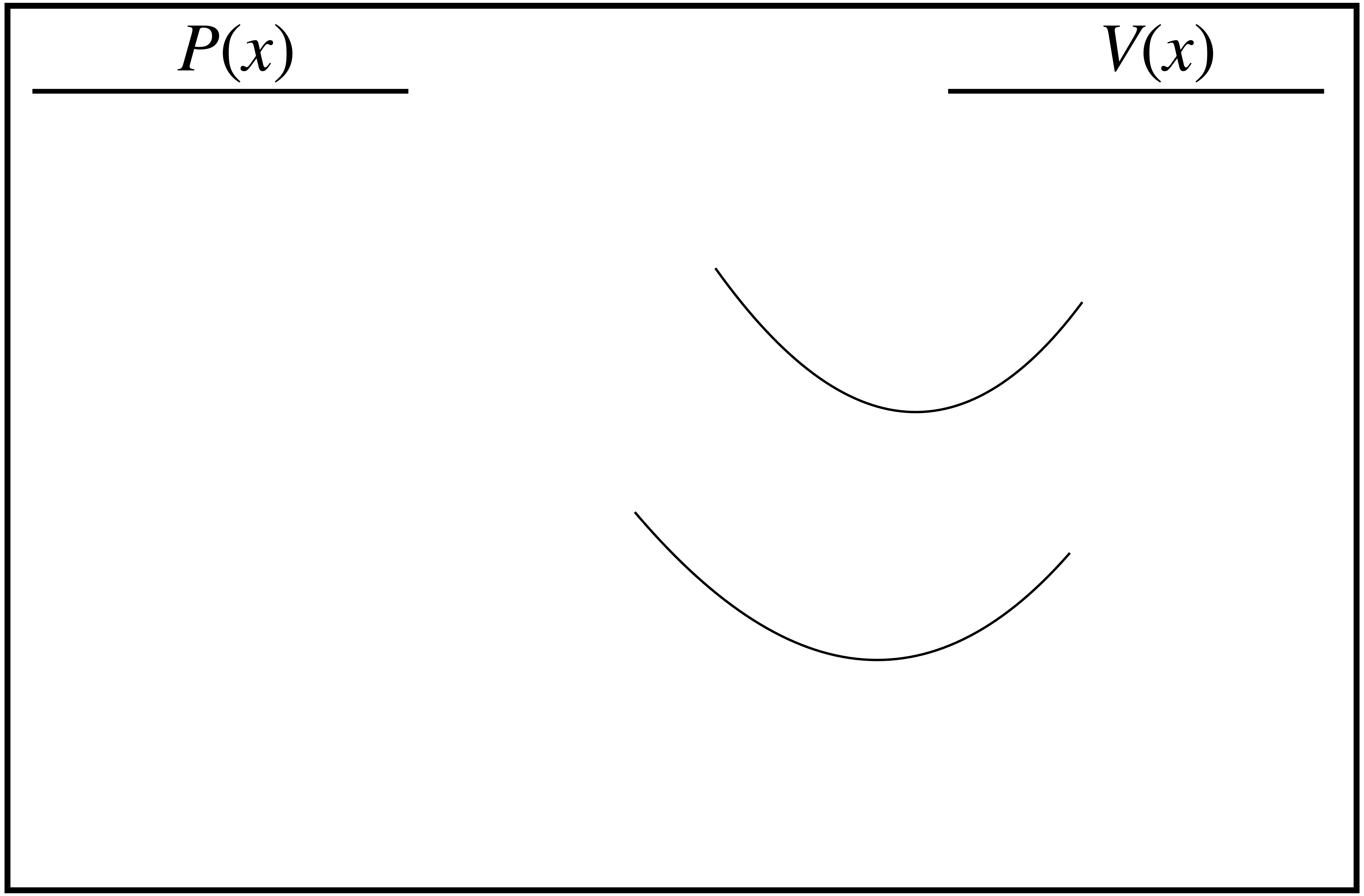


PCP

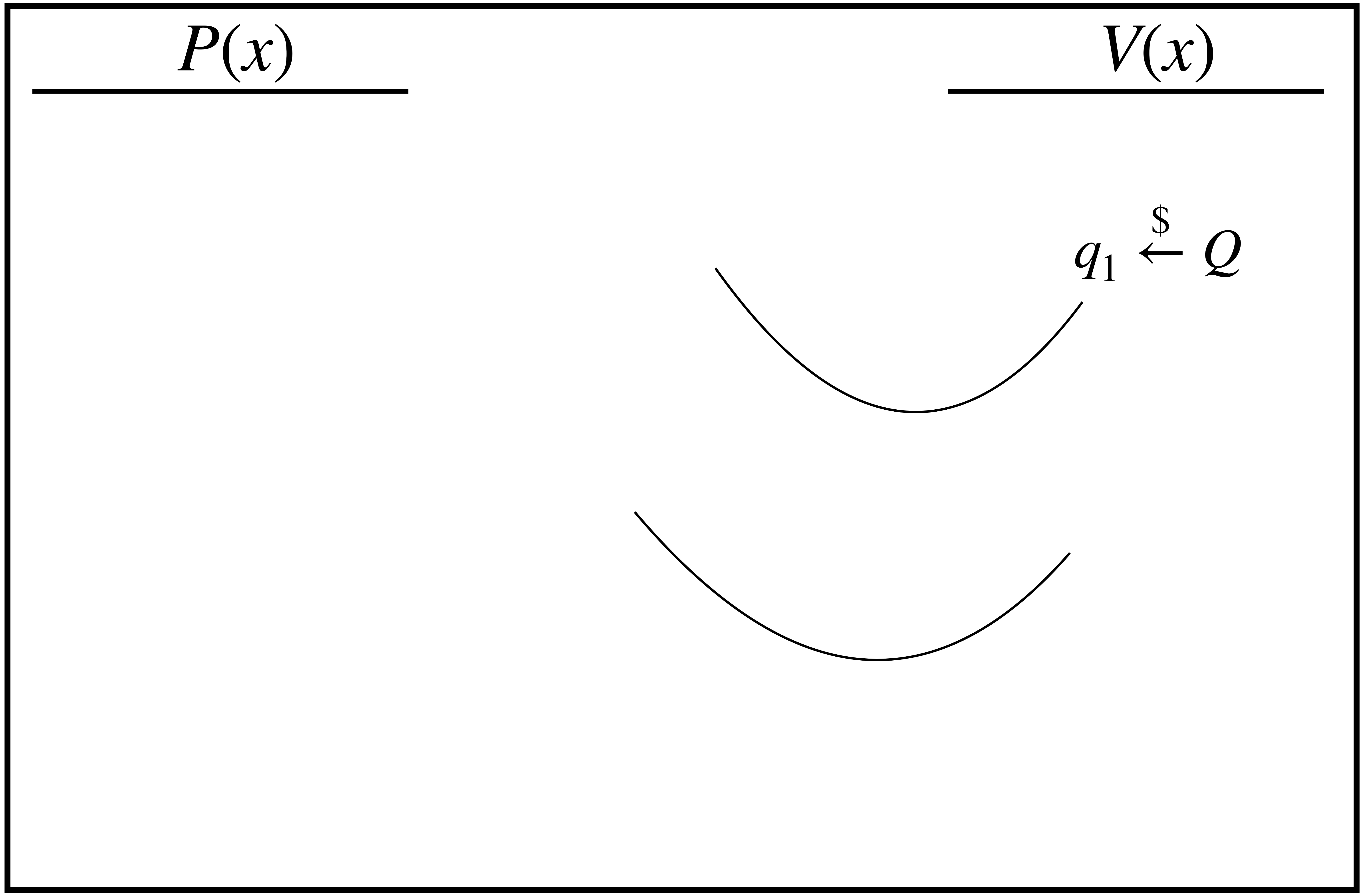
Polynomial Commitment



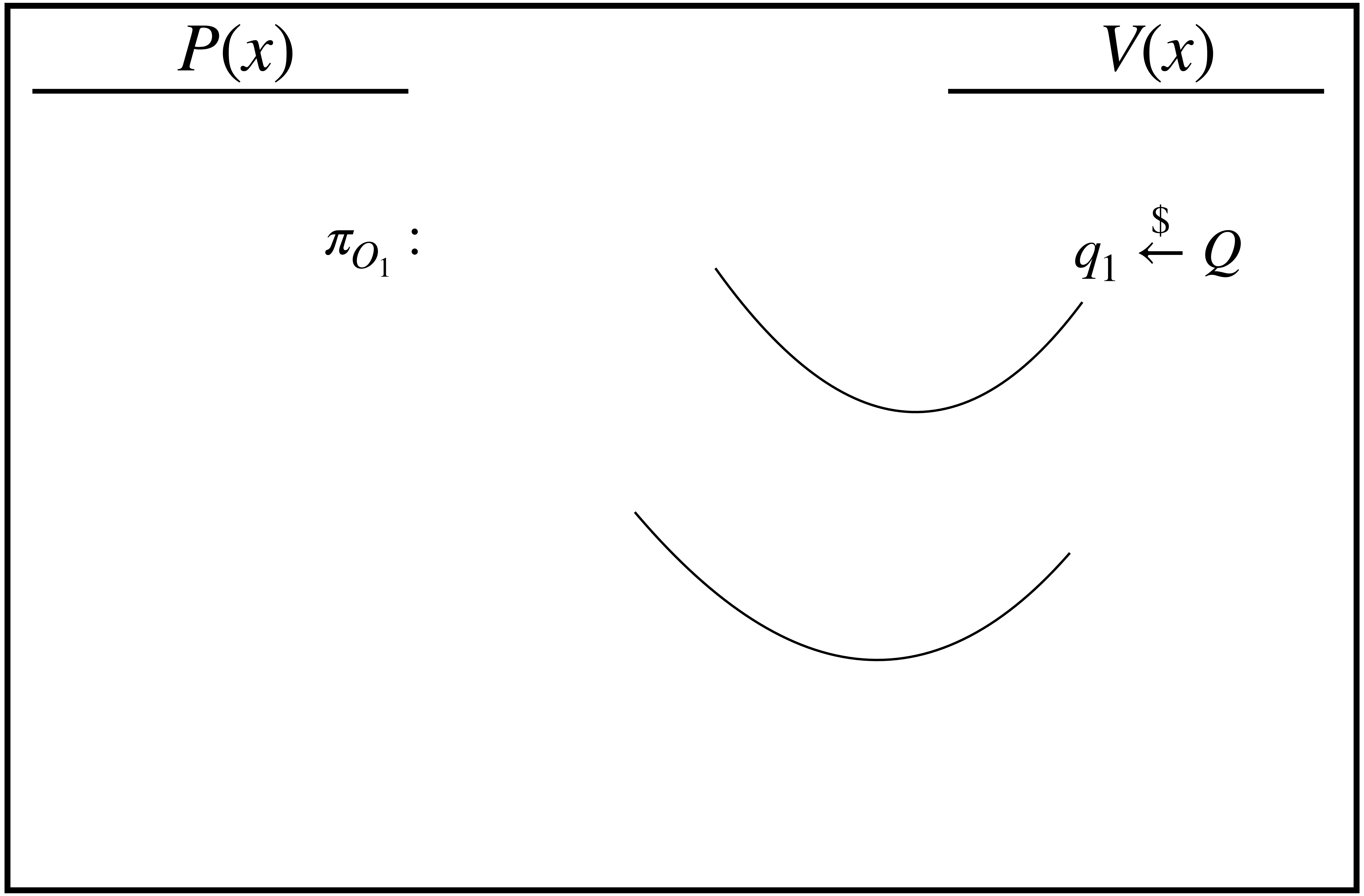
IOP
[BCS'16]



IOP
[BCS'16]

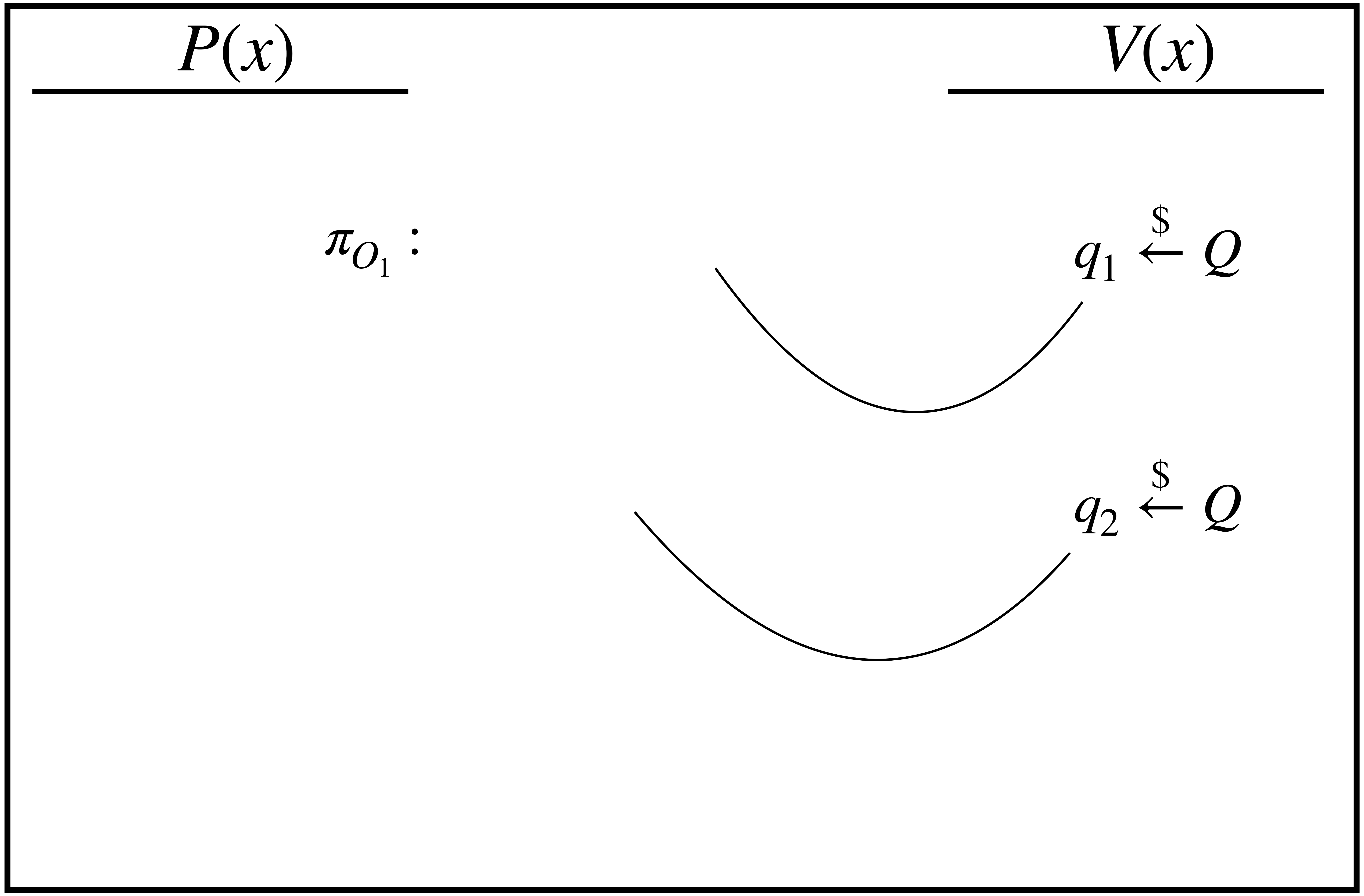


IOP
[BCS'16]

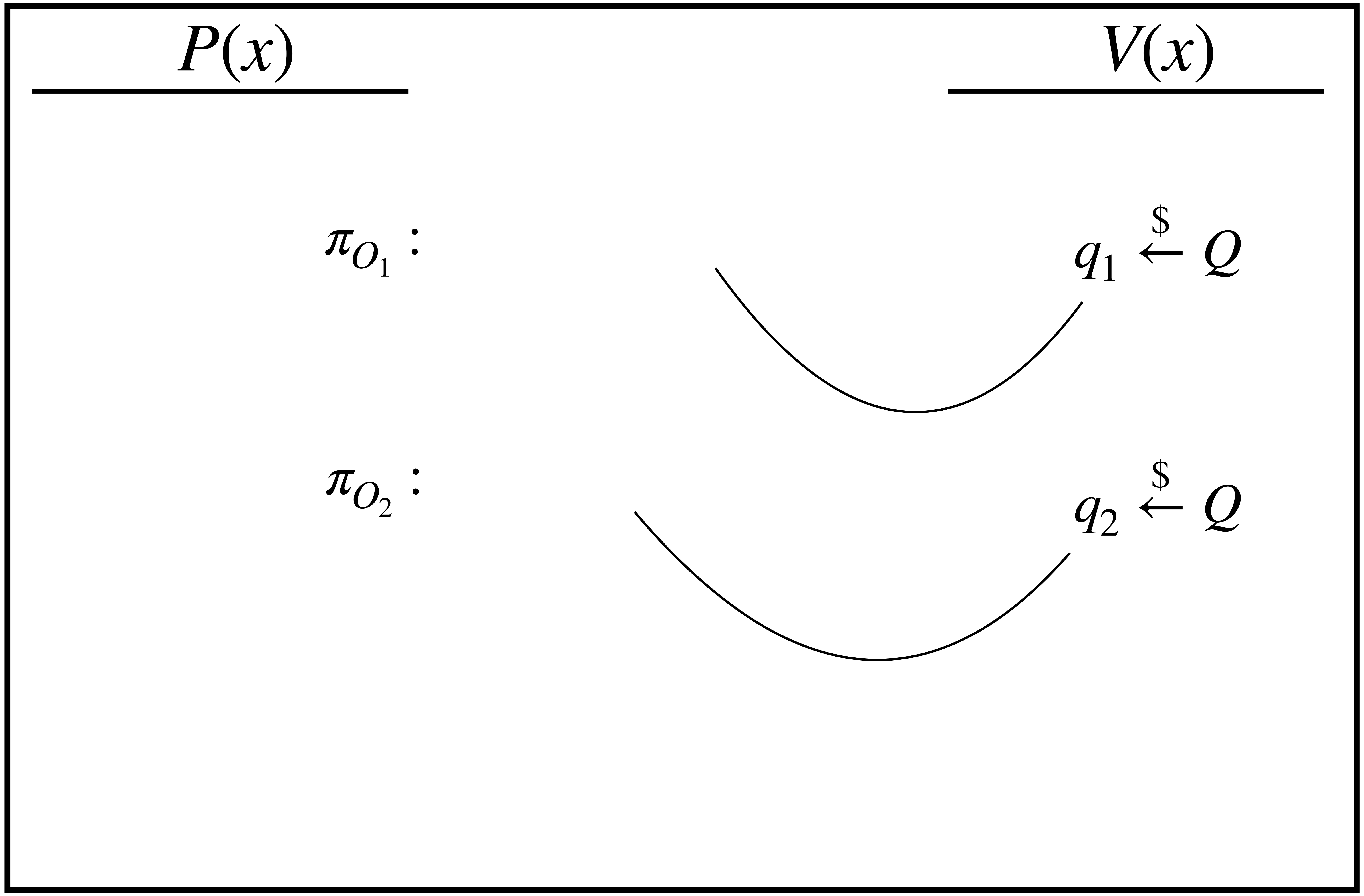


IOP

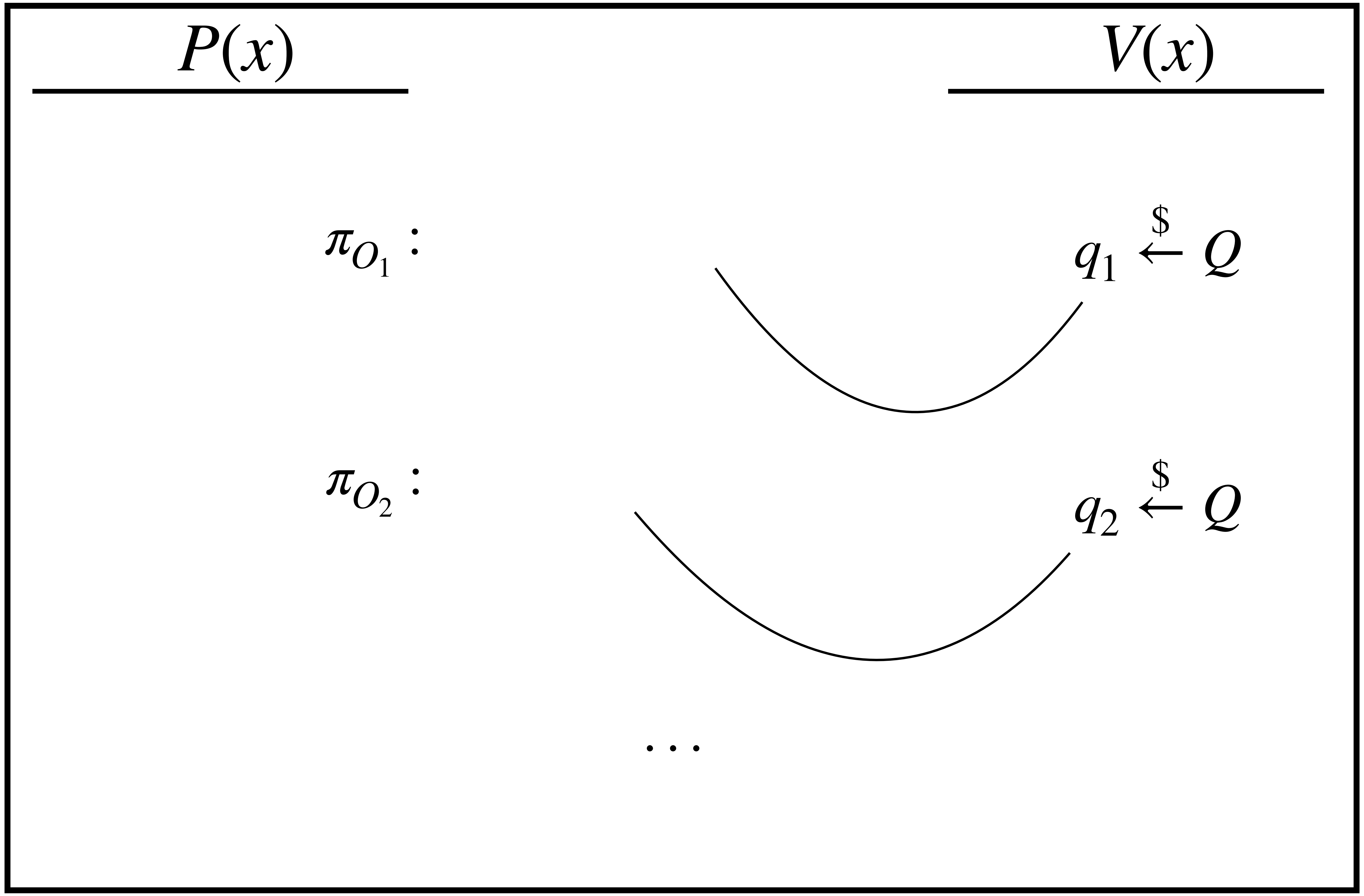
[BCS'16]



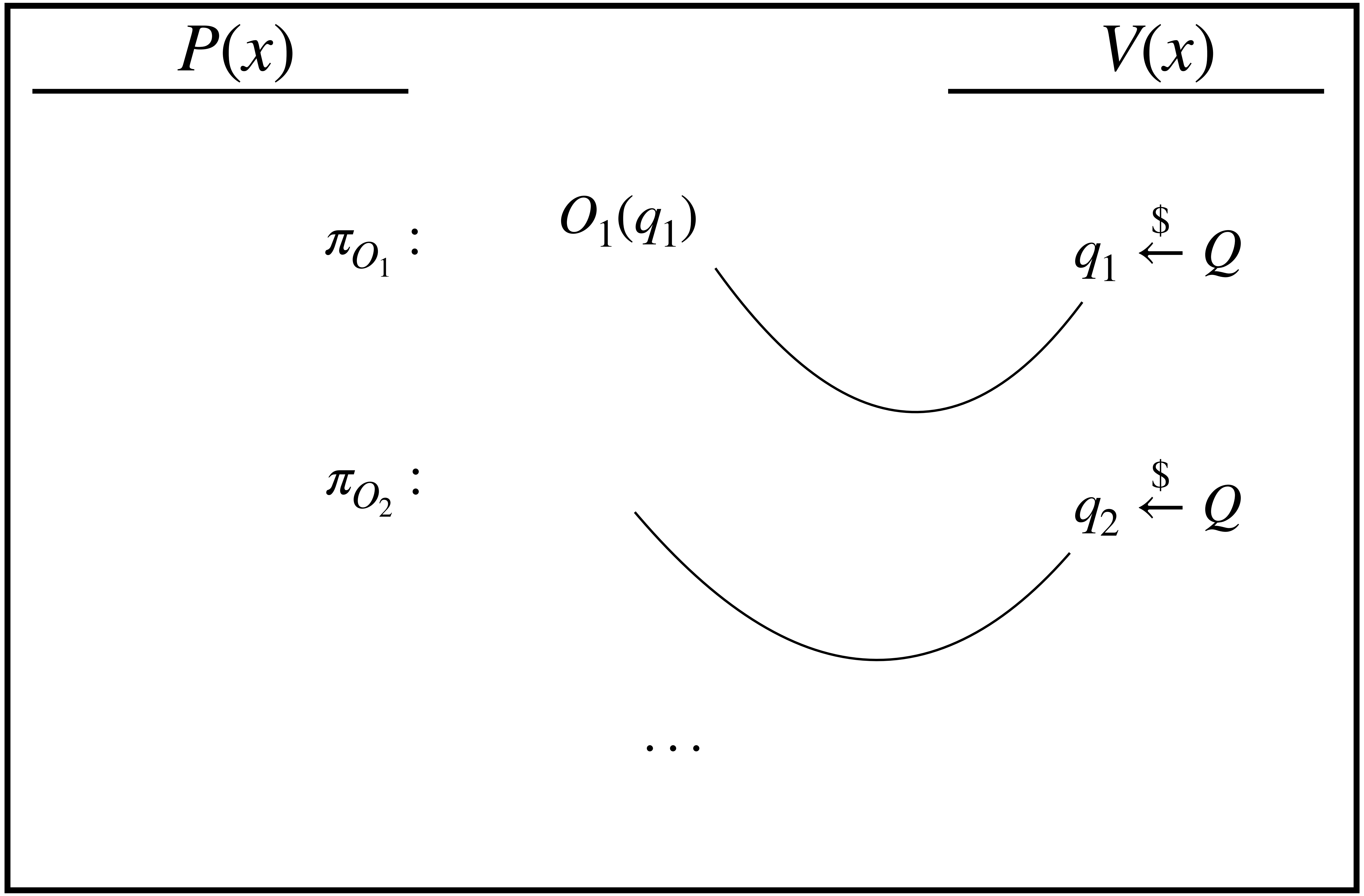
IOP
[BCS'16]



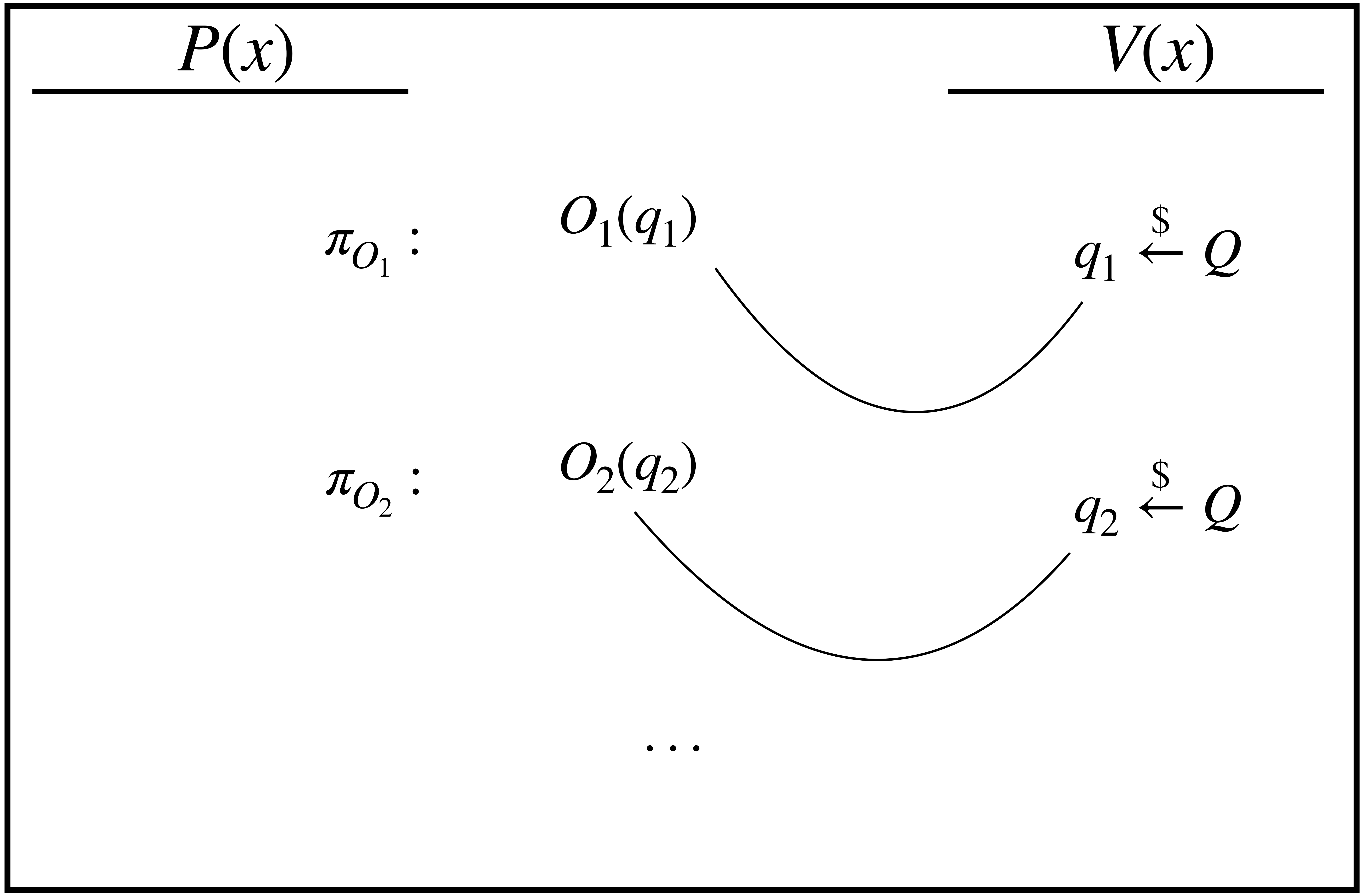
IOP
[BCS'16]



IOP
[BCS'16]

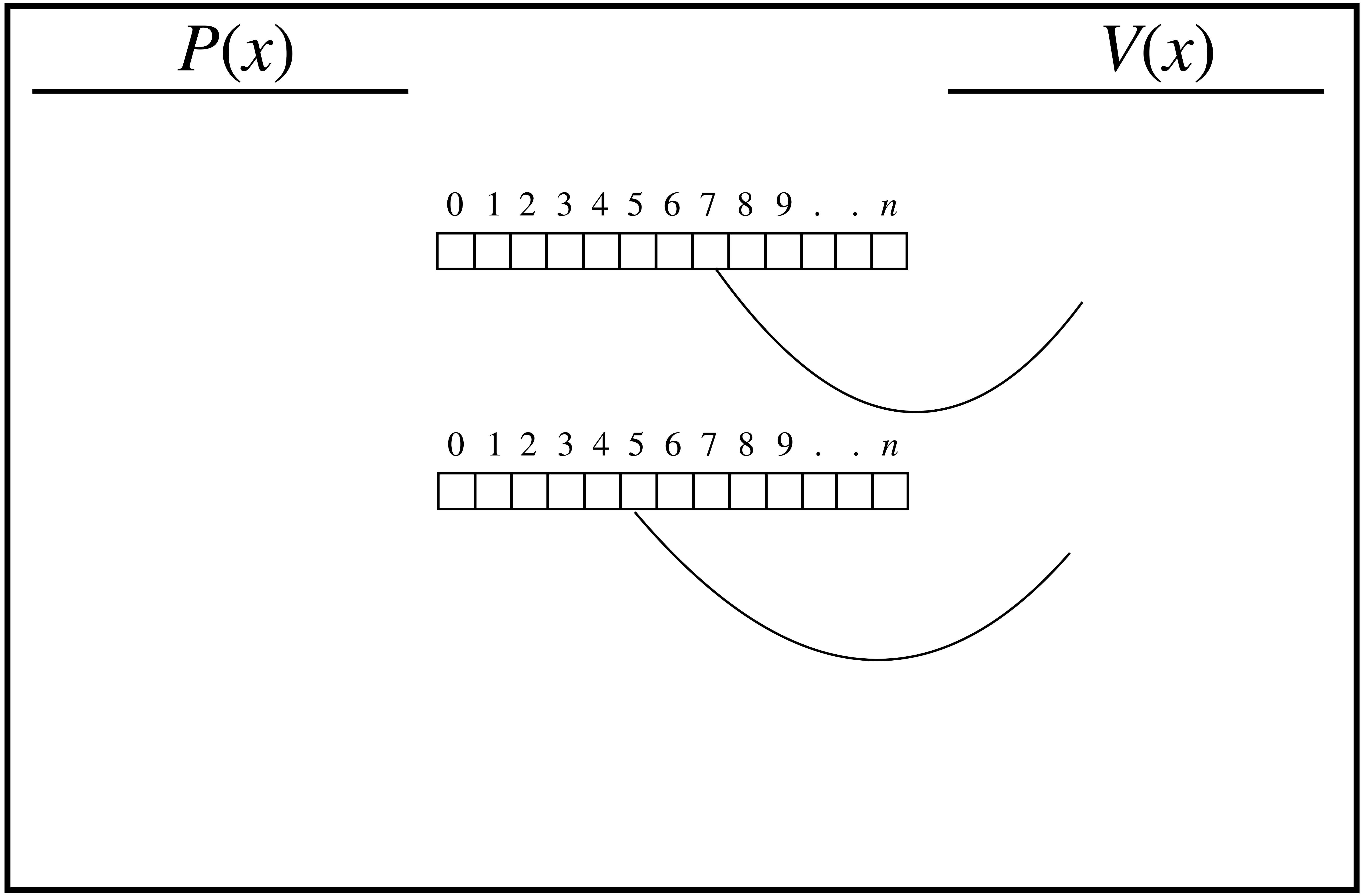


IOP
[BCS'16]


$P(x)$
$V(x)$
$\pi_{O_1}:$
$O_1(q_1)$
$q_1 \xleftarrow{\$} Q$
$\pi_{O_2}:$
$O_2(q_2)$
$q_2 \xleftarrow{\$} Q$
$\dots$

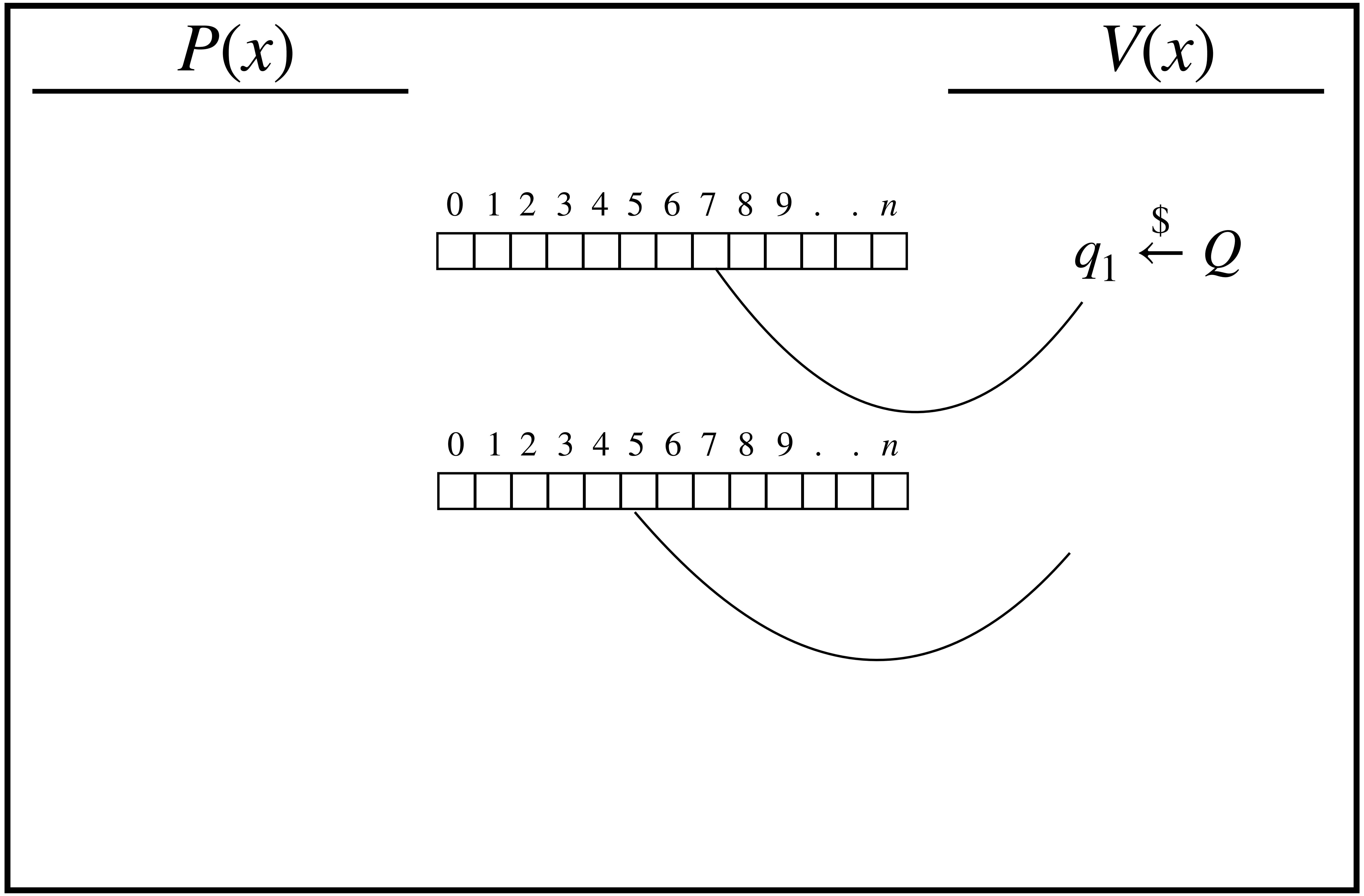
IOP

[BCS'16]



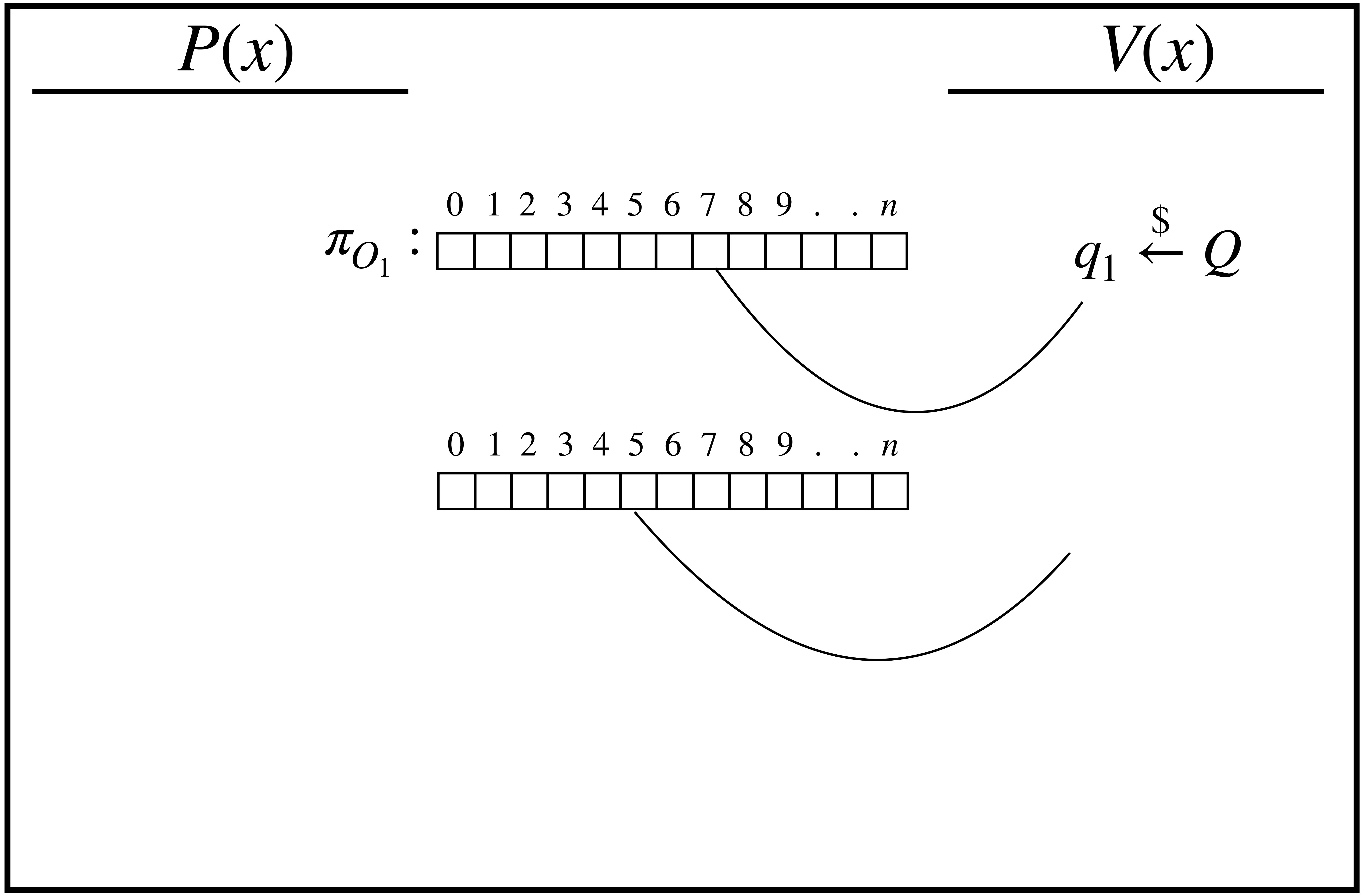
IOP

[BCS'16]



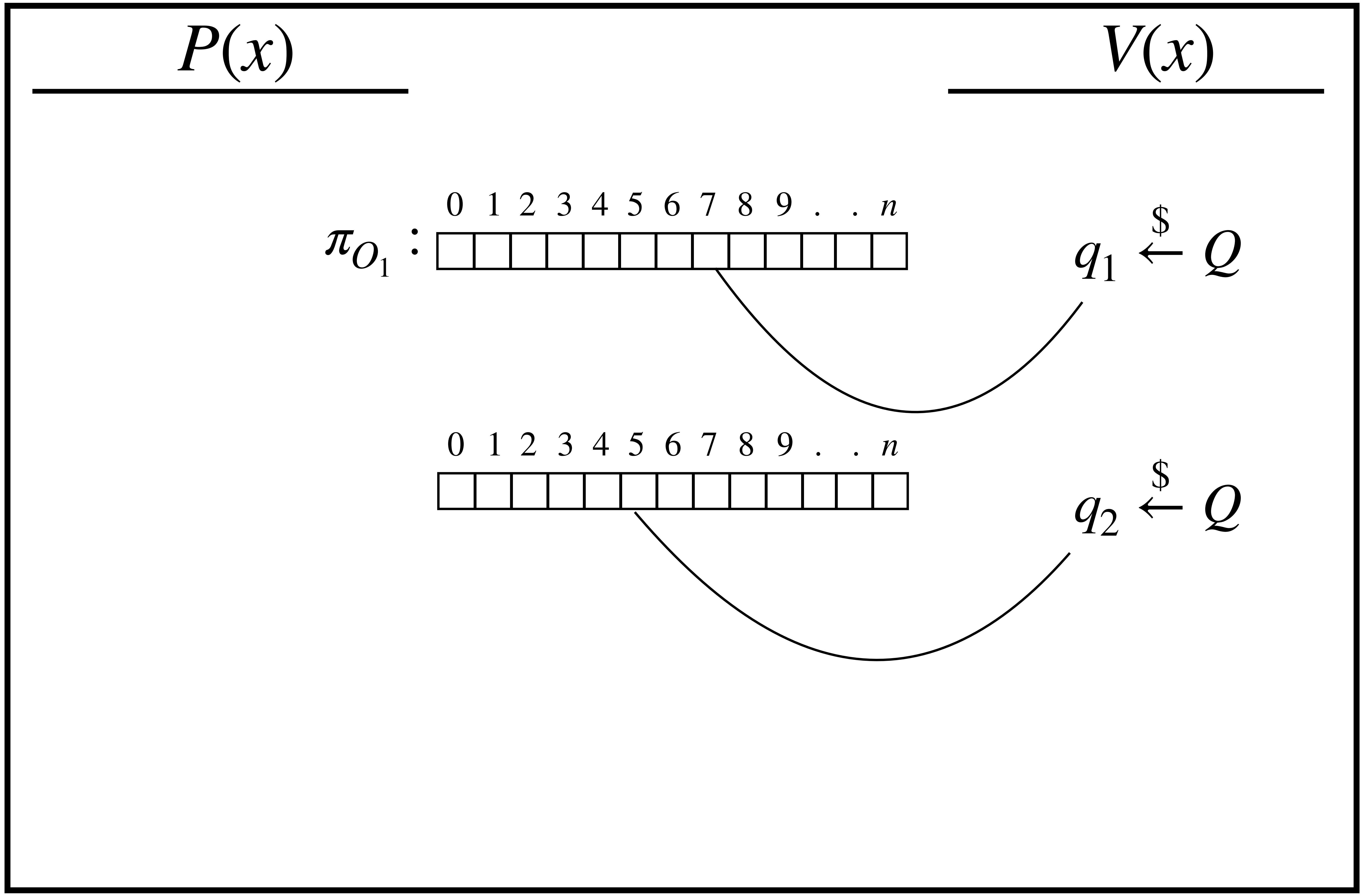
IOP

[BCS'16]



IOP

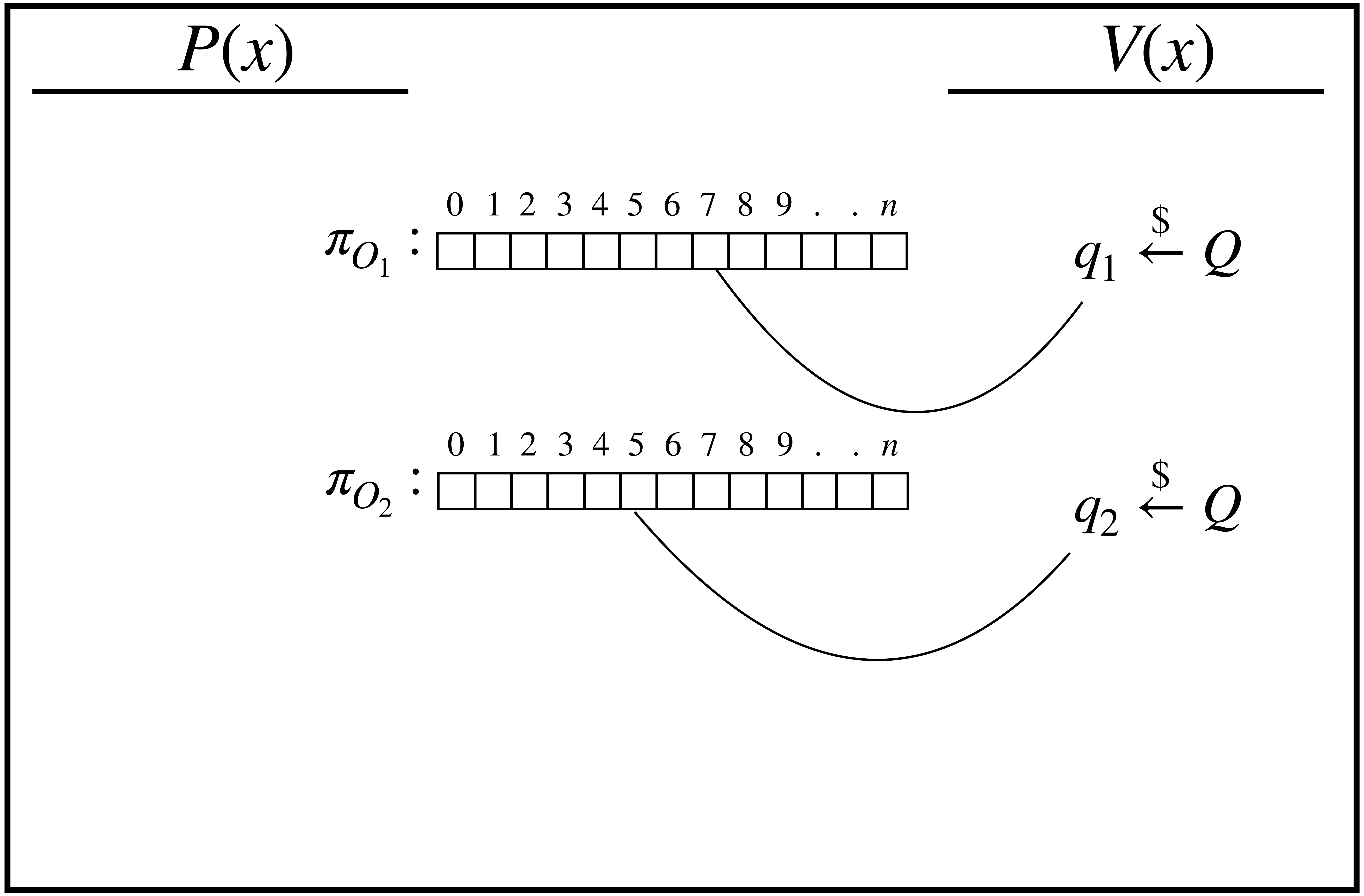
[BCS'16]



$P(x)$
$V(x)$
π_{O_1} :
0 1 2 3 4 5 6 7 8 9 . . n
$q_1 \xleftarrow{\$} Q$
0 1 2 3 4 5 6 7 8 9 . . n
$q_2 \xleftarrow{\$} Q$

IOP

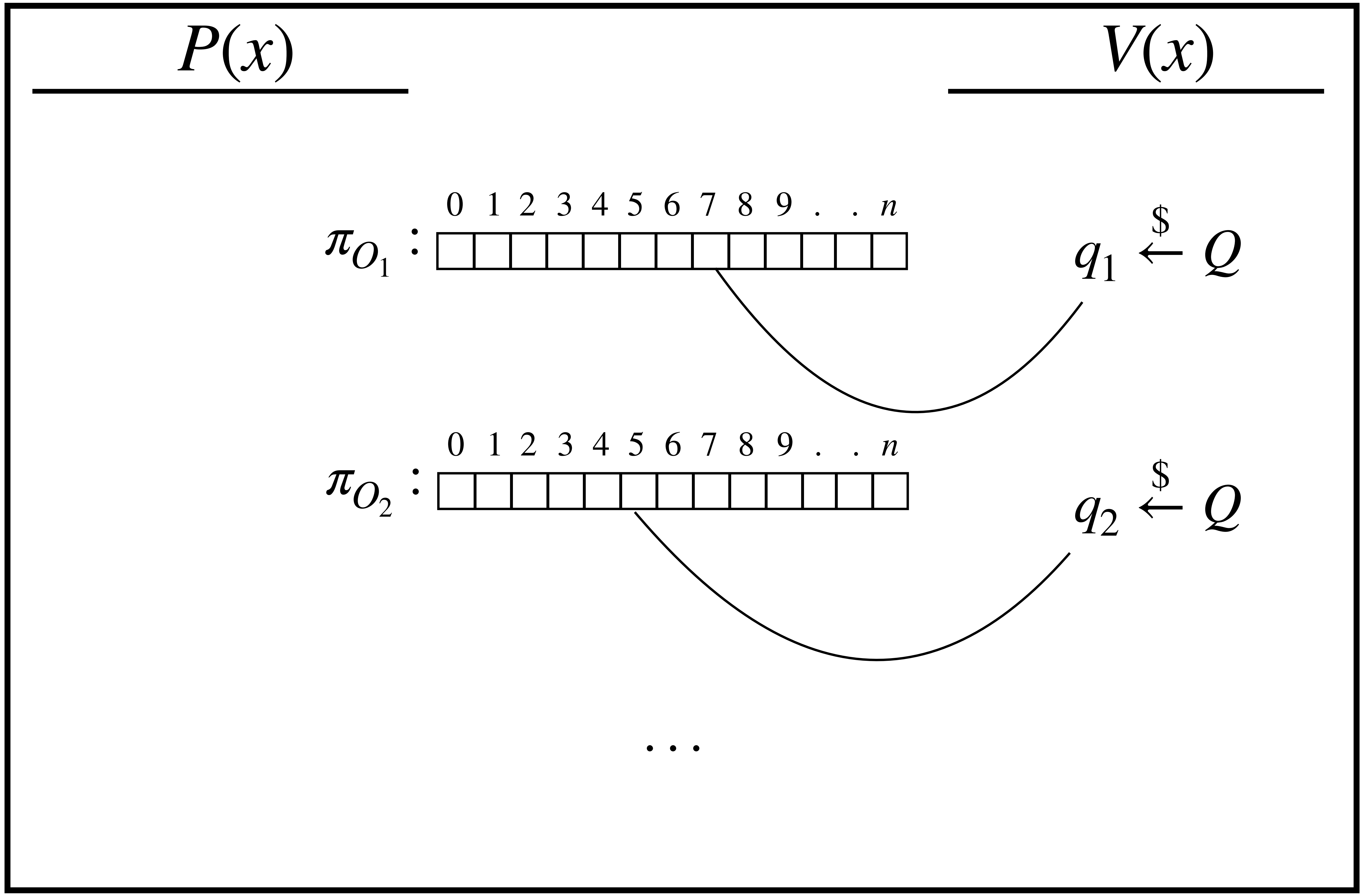
[BCS'16]



$P(x)$
$V(x)$
0 1 2 3 4 5 6 7 8 9 . . n
π_{O_1} :
$q_1 \xleftarrow{\$} Q$
0 1 2 3 4 5 6 7 8 9 . . n
π_{O_2} :
$q_2 \xleftarrow{\$} Q$

IOP

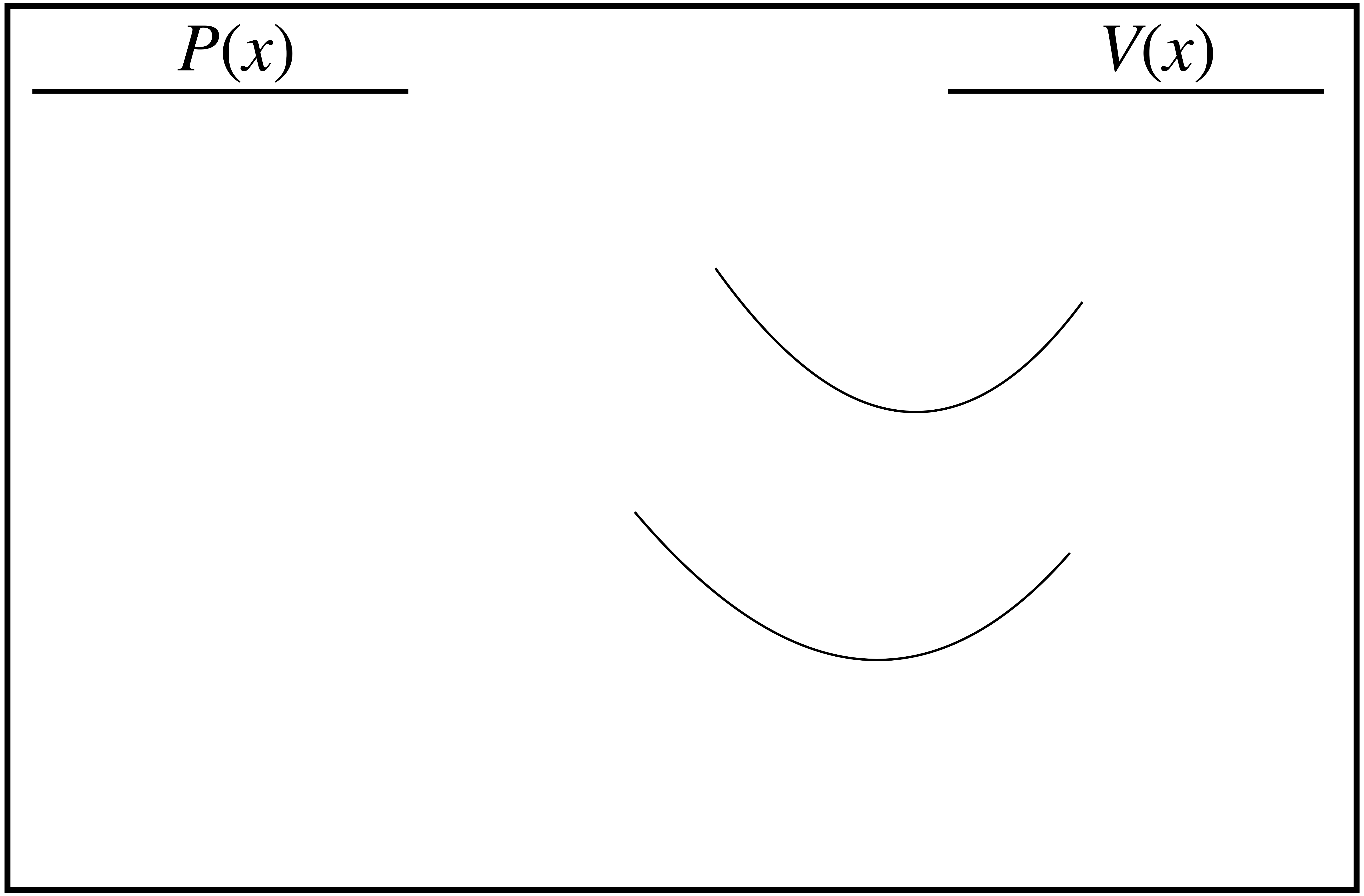
[BCS'16]



$P(x)$
$V(x)$
0 1 2 3 4 5 6 7 8 9 . . n
π_{O_1} :
$q_1 \xleftarrow{\$} Q$
0 1 2 3 4 5 6 7 8 9 . . n
π_{O_2} :
$q_2 \xleftarrow{\$} Q$
…

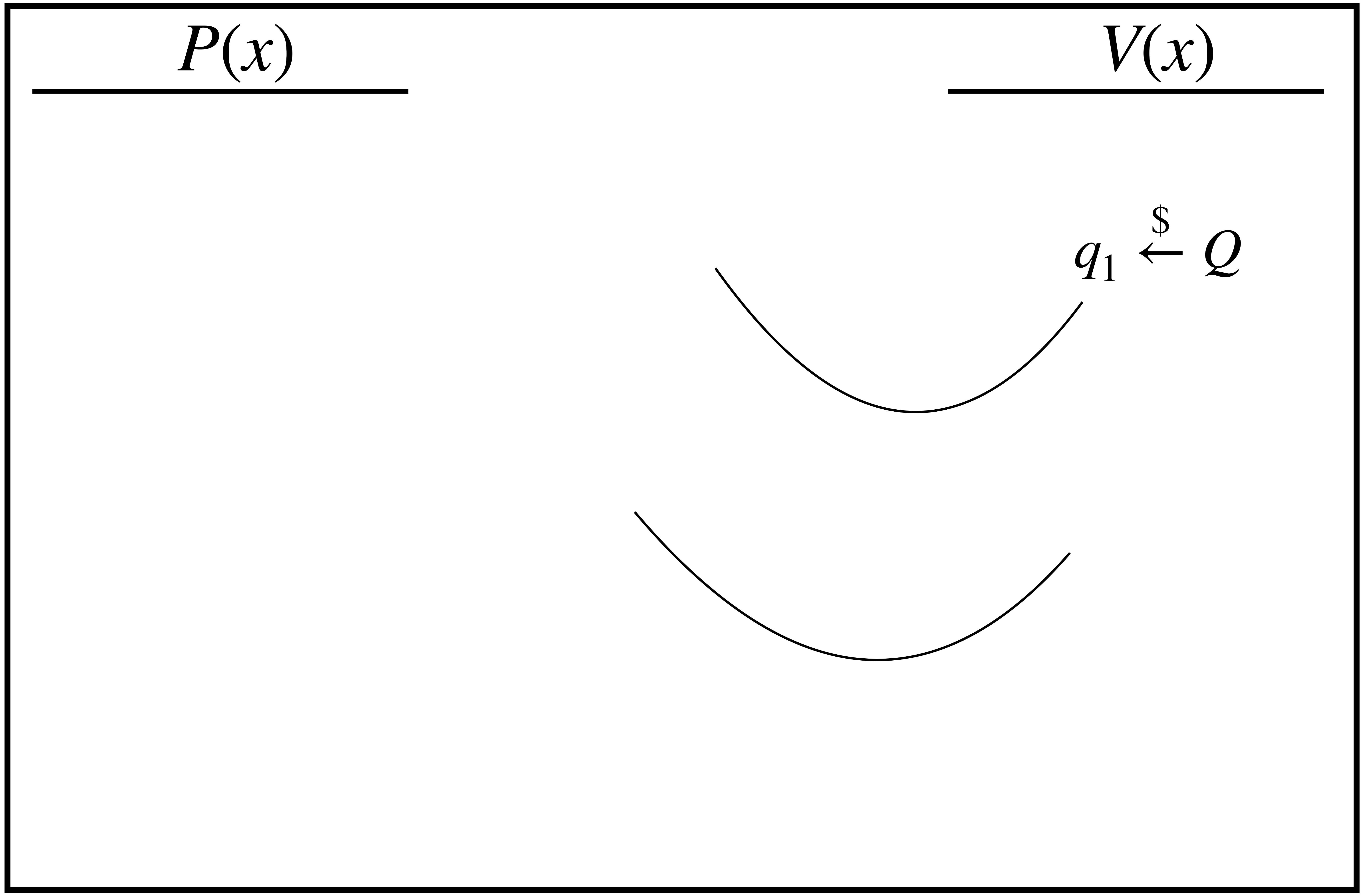
IOP

[BCS'16]



IOP

[BCS’16]



IOP
[BCS'16]

$P(x)$ | $V(x)$

$\pi_{O_1}:$ $q_1 \xleftarrow{\$} Q$

IOP

[BCS'16]

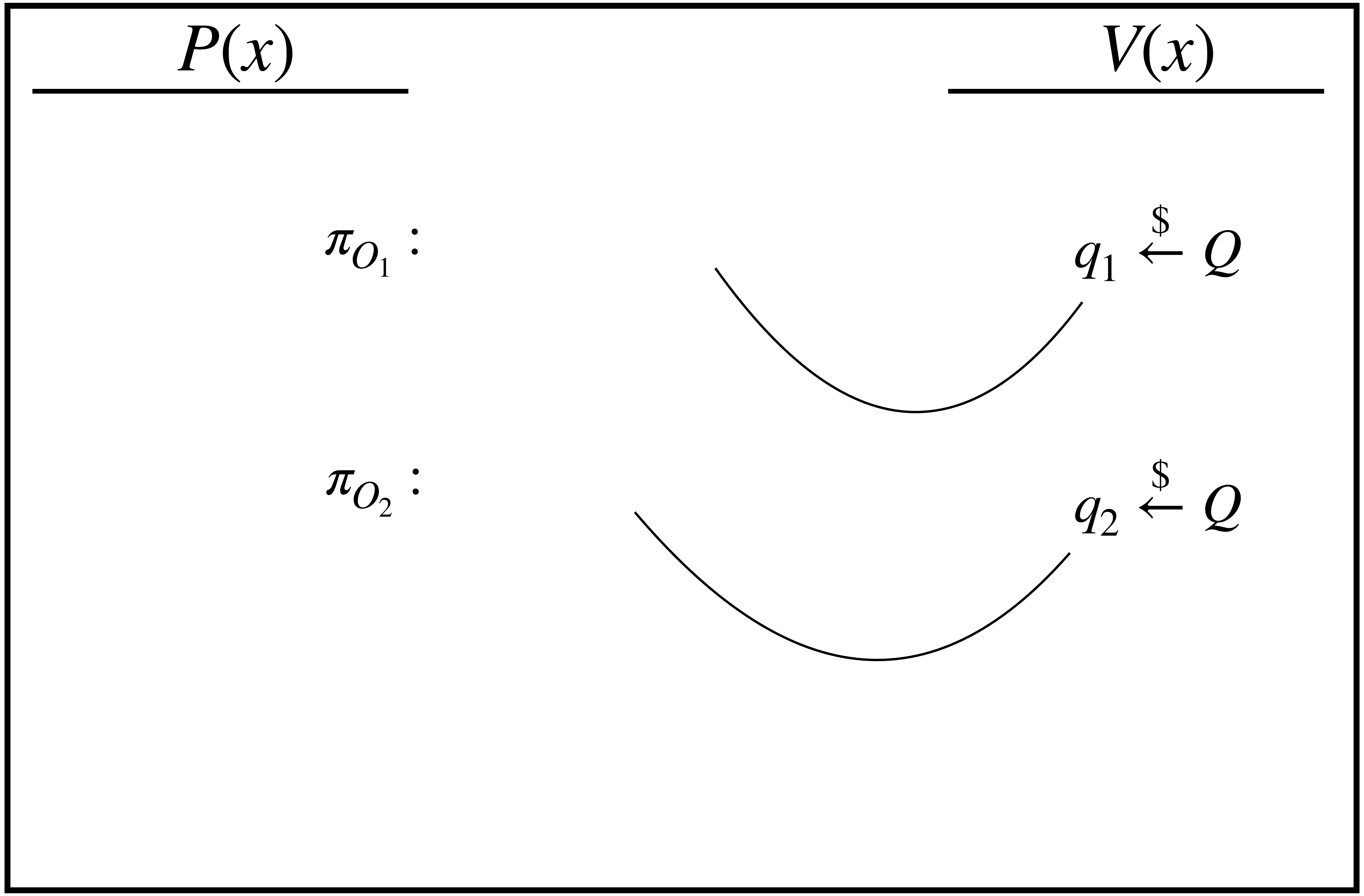
$P(x)$ | $V(x)$

$\pi_{O_1}:$

$q_1 \stackrel{\$}{\leftarrow} Q$

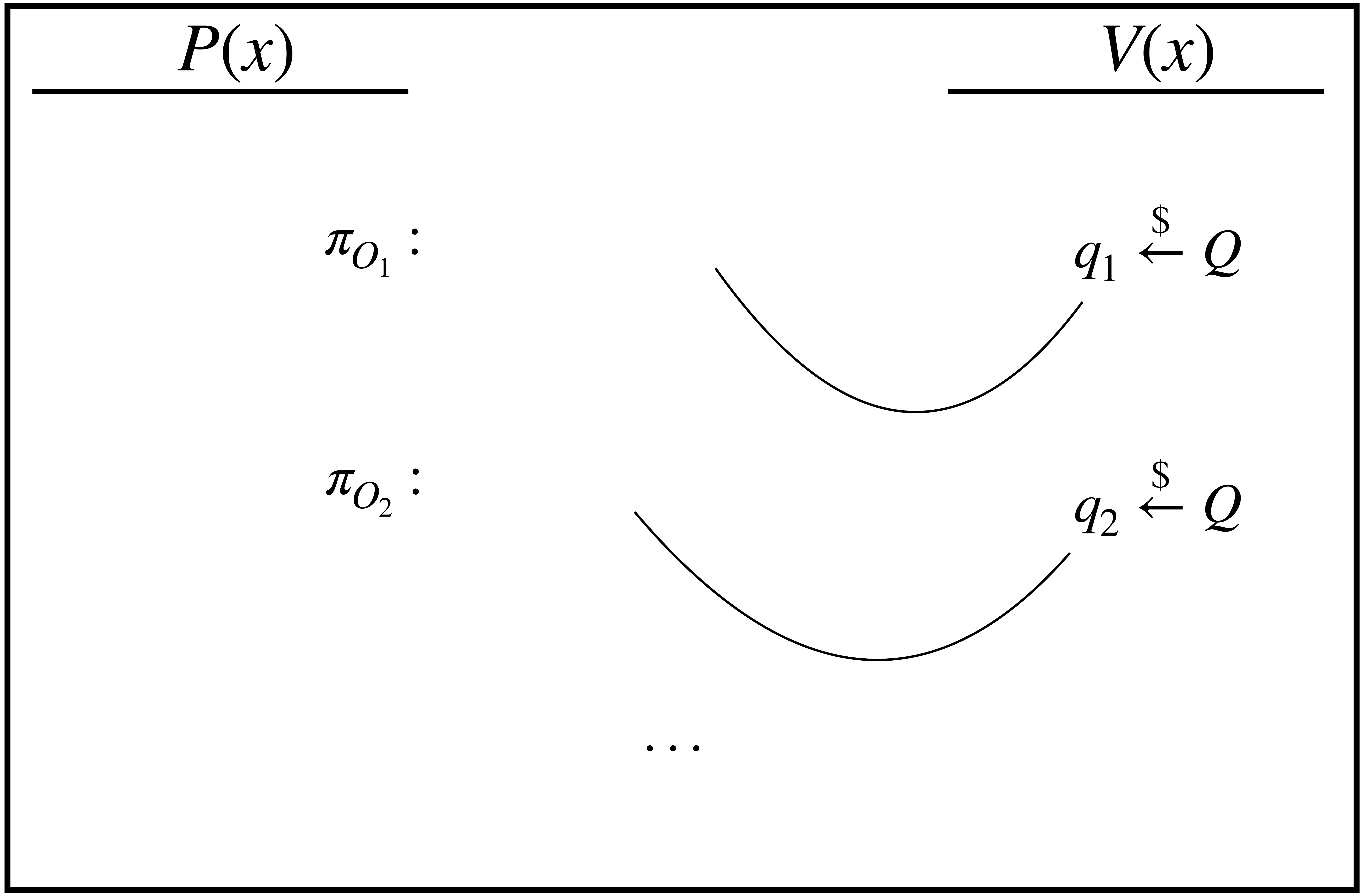
$q_2 \stackrel{\$}{\leftarrow} Q$

IOP
[BCS'16]

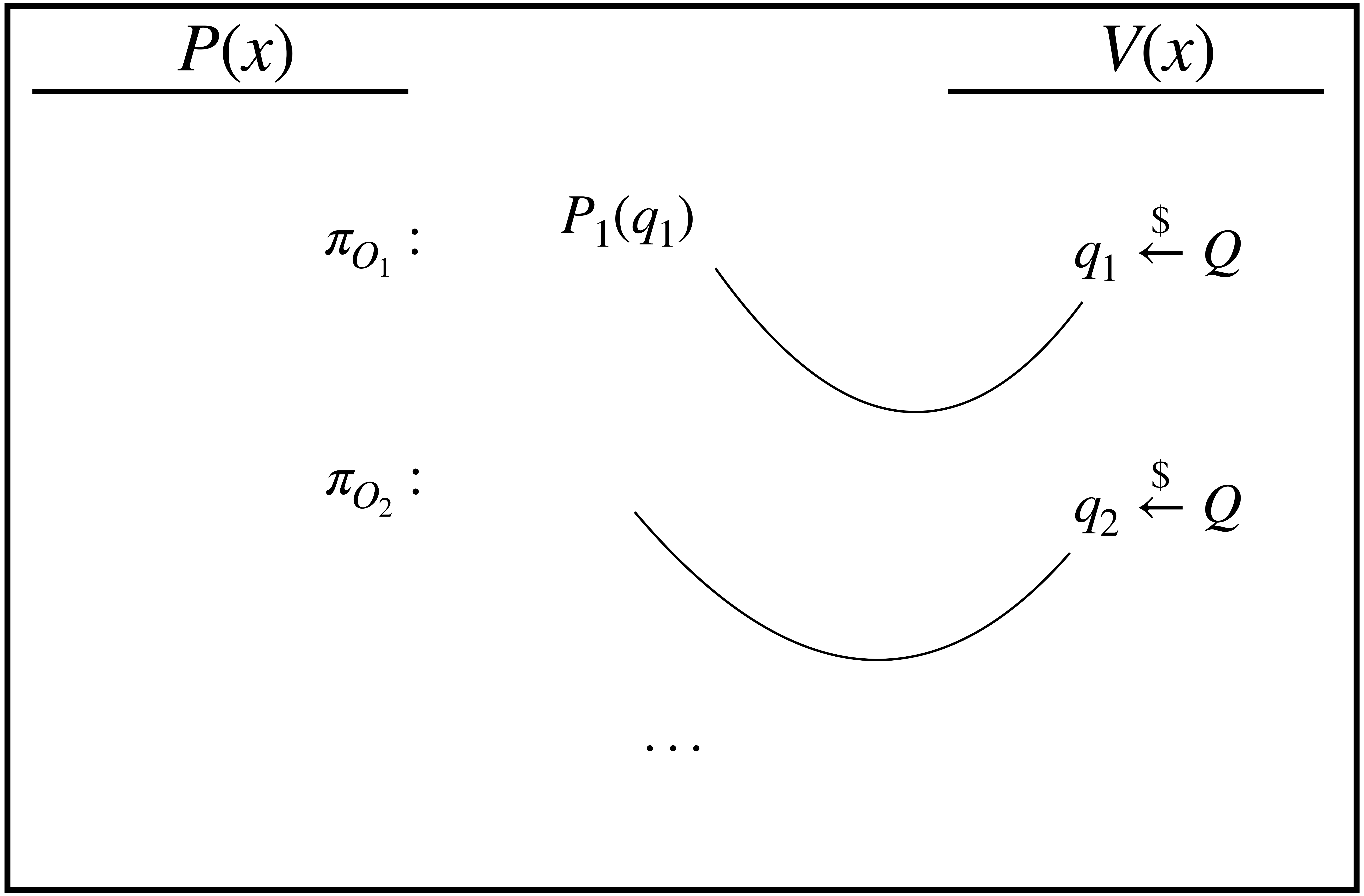

$P(x)$
$V(x)$
$\pi_{O_1}:$
$q_1 \stackrel{\$}{\leftarrow} Q$
$\pi_{O_2}:$
$q_2 \stackrel{\$}{\leftarrow} Q$

IOP

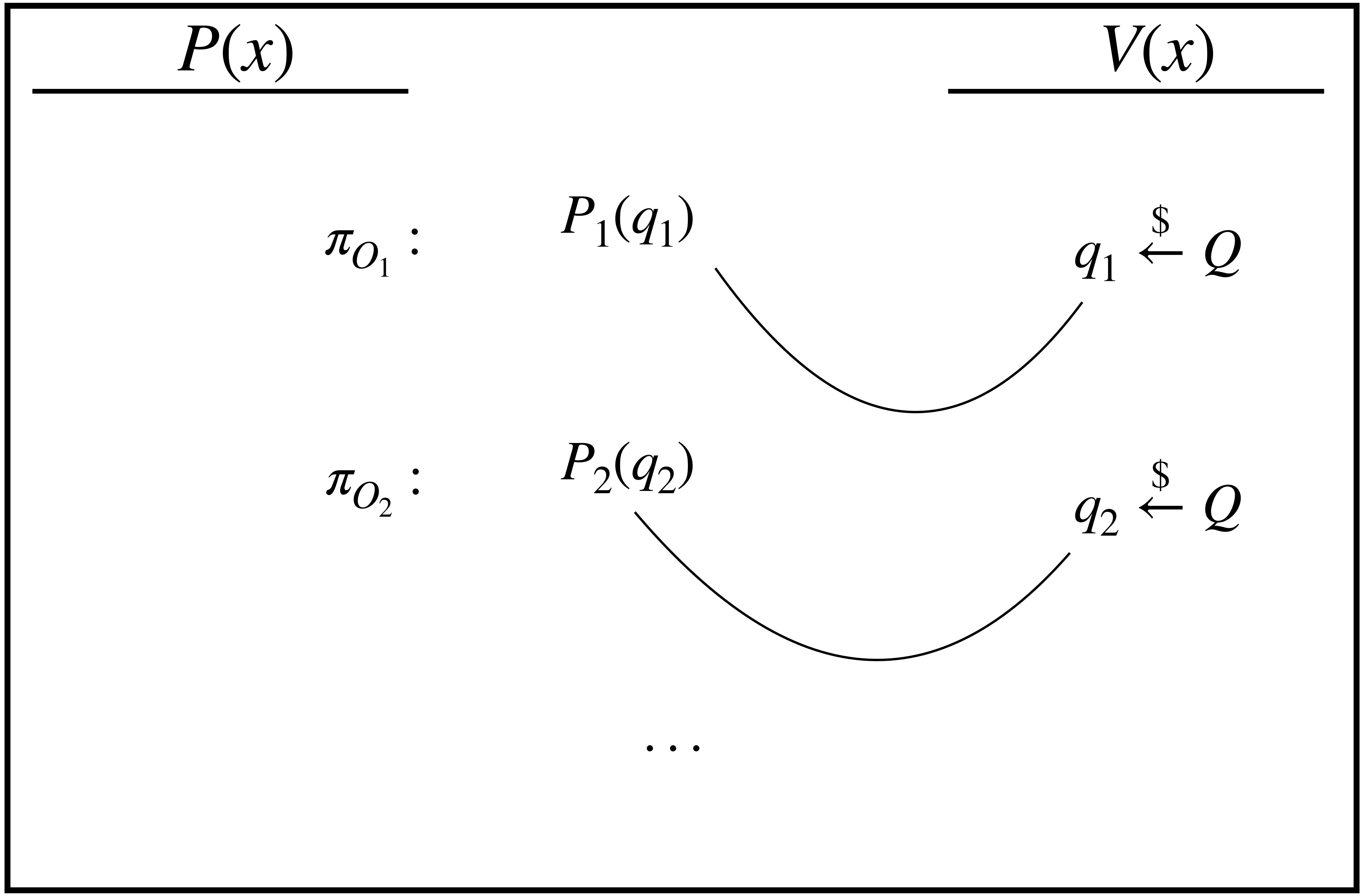
[BCS'16]



IOP
[BCS'16]



IOP
[BCS'16]


$P(x)$
$V(x)$
$\pi_{O_1}:$
$P_1(q_1)$
$q_1 \overset{\$}{\leftarrow} Q$
$\pi_{O_2}:$
$P_2(q_2)$
$q_2 \overset{\$}{\leftarrow} Q$
$\dots$

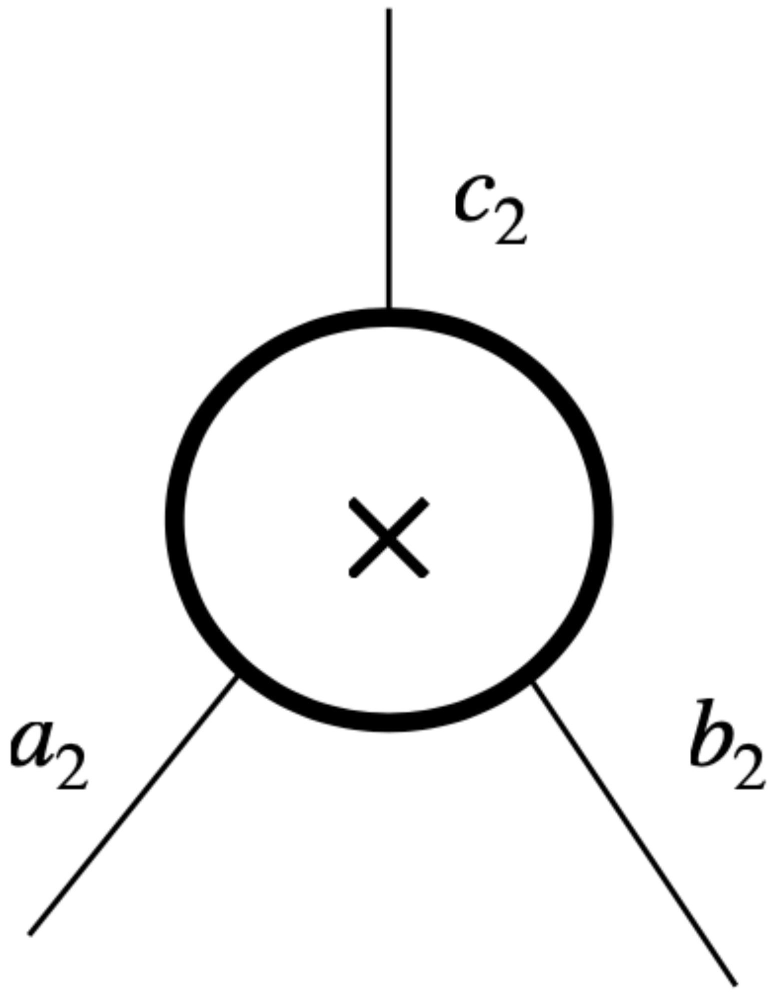
IOP Realization

- IOP + Commitment
- Most cryptographic properties inherited by the commitment scheme.
  - Trusted setup
  - Post-quantum security

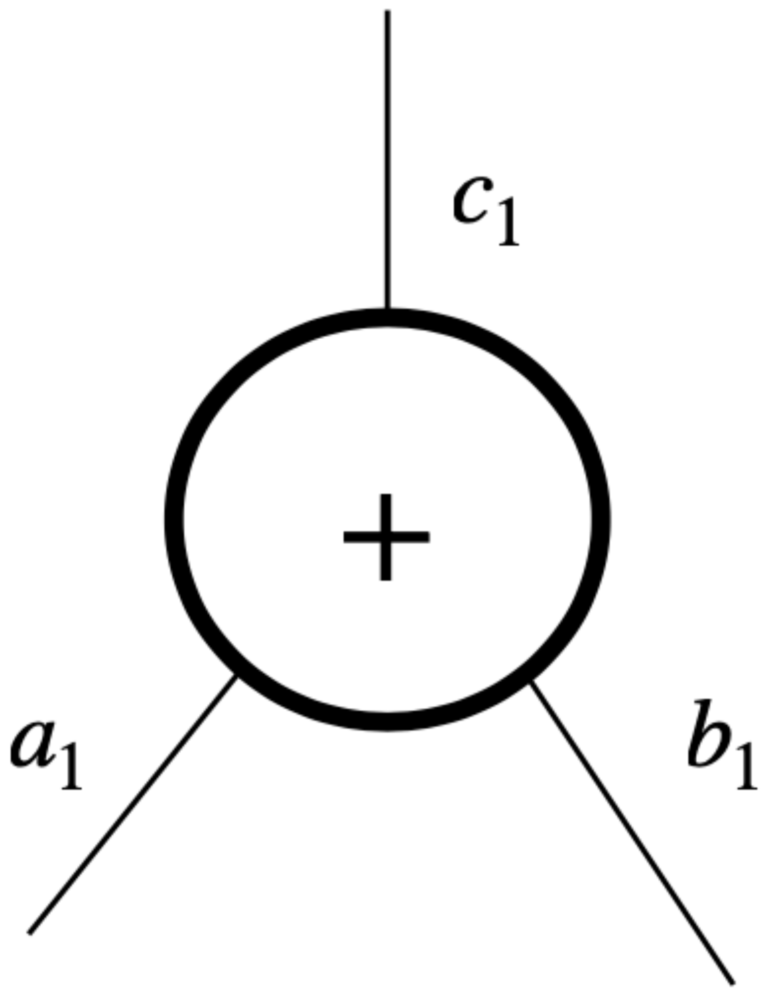
Arithmetization

Arithmetization

PLONKish



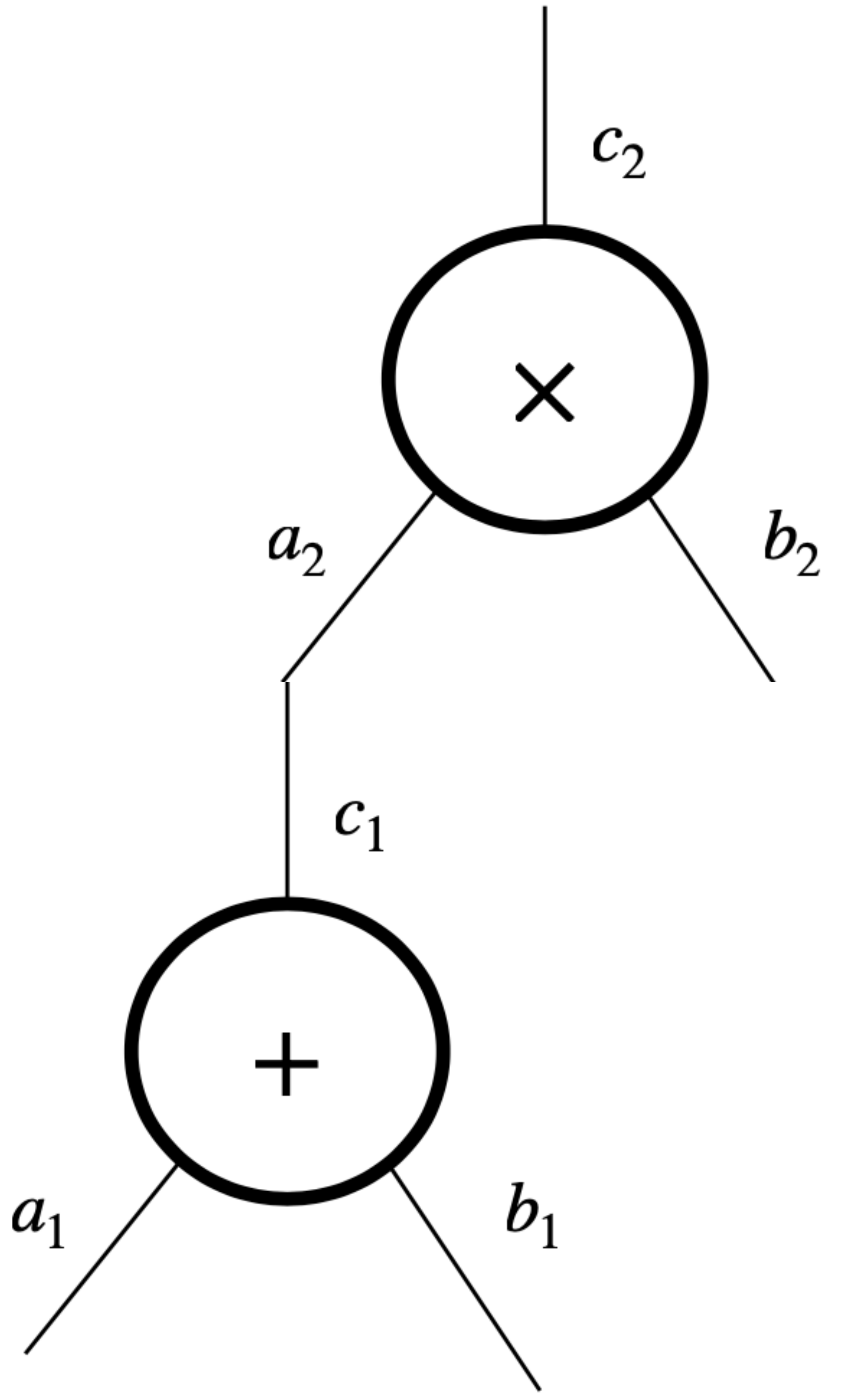
$$a_2 \cdot b_2 - c_2 = 0$$



$$a_1 + b_1 - c_1 = 0$$

Arithmetization

PLONKish



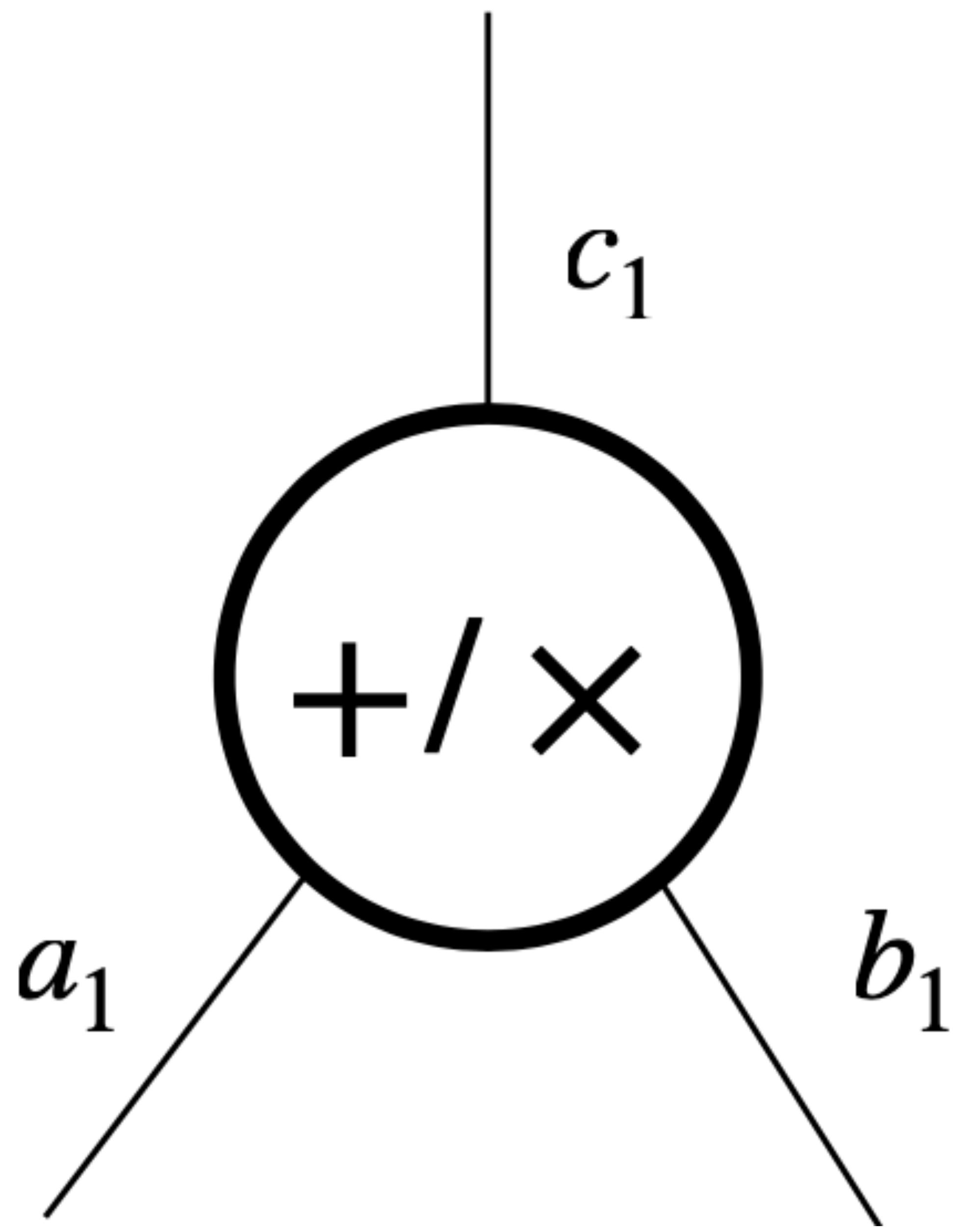
$$a_2 \cdot b_2 - c_2 = 0$$

$$a_1 + b_1 - c_1 = 0$$

$$c_1 = a_2 \text{ (Copy)}$$

Arithmetization

PLONKish



$S \in \{0,1\}$

$$S(a_1 + b_1) + (1 - S)(a_1 \cdot b_1) - c_1 = 0$$

Arithmetization

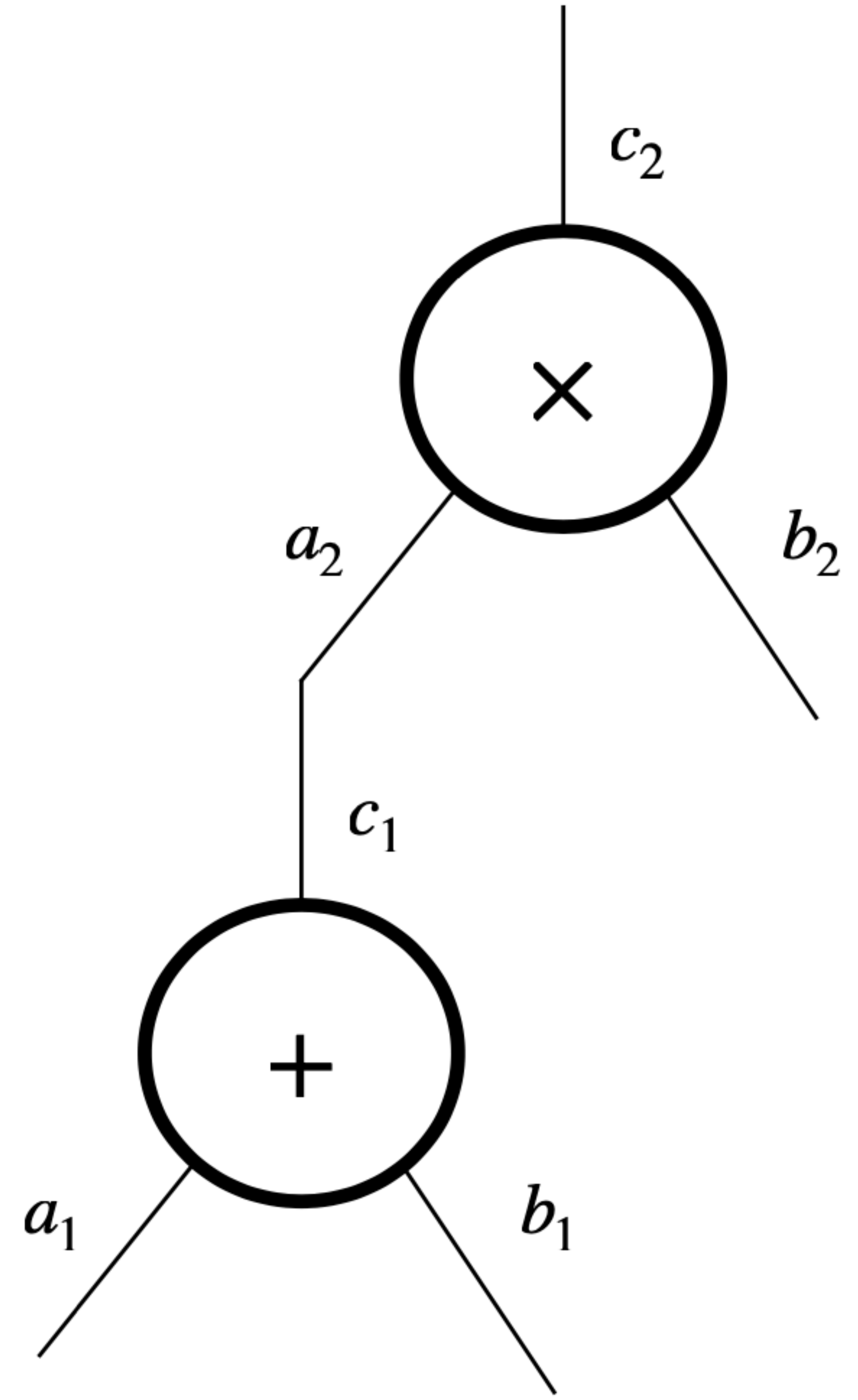
PLONKish

Computation: $(a_1 + b_1) \cdot b_2 = c_2 \mod 11$

Gate Constraints : $S_i(a_i + b_i) + (1 - S_i)(a_i \cdot b_i) - c_i = 0$

i	a_i	b_i	c_i	S_i
1	a_1	b_1	c_1	S_1
2	a_2	b_2	c_2	S_2

+ Copy



Arithmetization

PLONKish

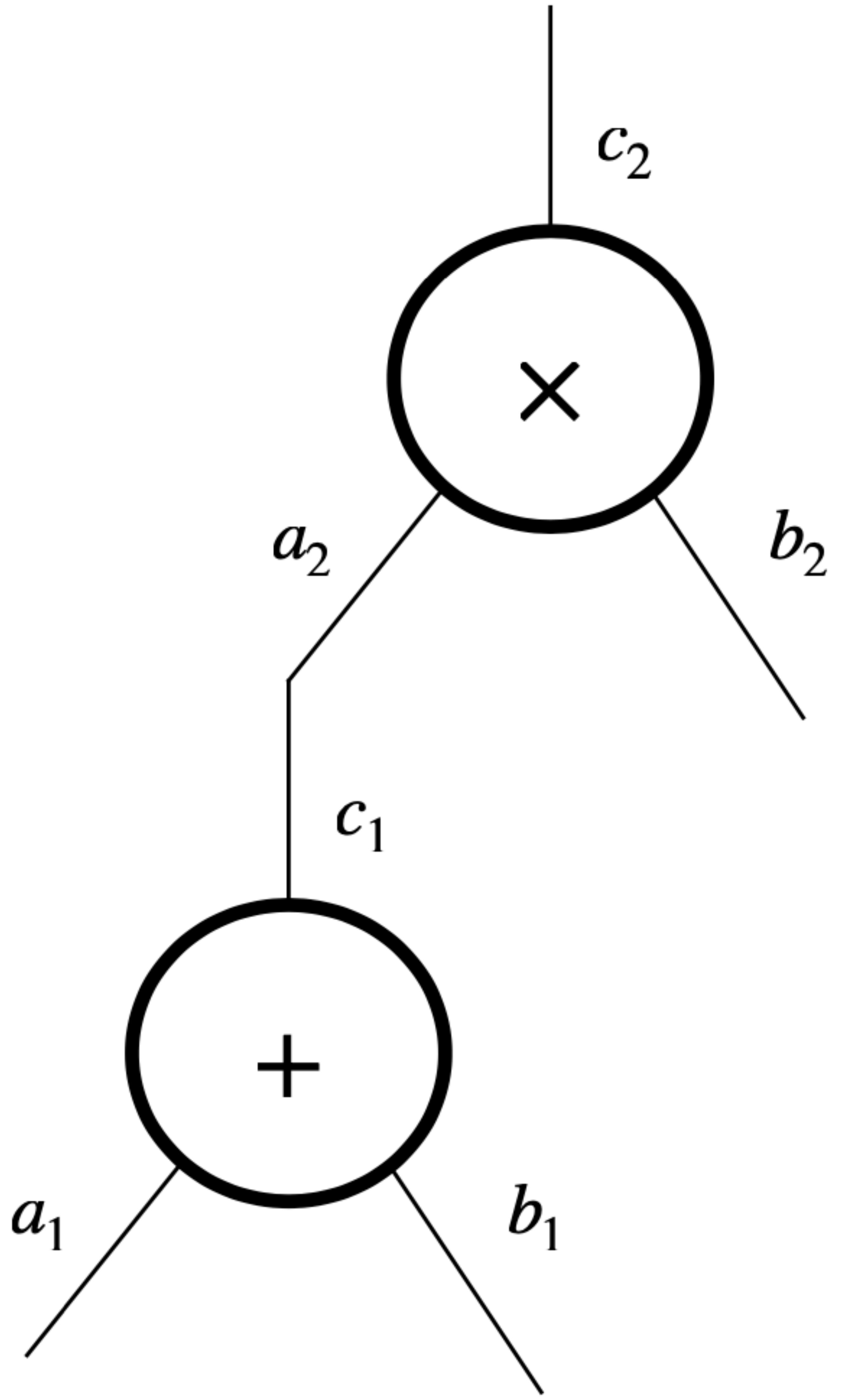
Computation: $(a_1 + b_1) \cdot b_2 = c_2 \mod 11$

Solution: $a_1 = 4$, $b_1 = 5$,$b_2 = 10$, $c_1 = 9$, $a_2 = 9$, $c_2 = 2$

Gate Constraints : $S_i(a_i + b_i) + (1 - S_i)(a_i \cdot b_i) - c_i = 0$

i	a_i	b_i	c_i	S_i
1	4	5	9	1
2	9	10	2	0

+ Copy



Arithmetization

PLONKish

Computation: $(a_1 + b_1) \cdot b_2 = c_2 \mod 11$

Solution: $a_1 = 4$, $b_1 = 5$,$b_2 = 10$, $c_1 = 9$, $a_2 = 9$, $c_2 = 2$

Gate Constraints : $S_i(a_i + b_i) + (1 - S_i)(a_i \cdot b_i) - c_i = 0$

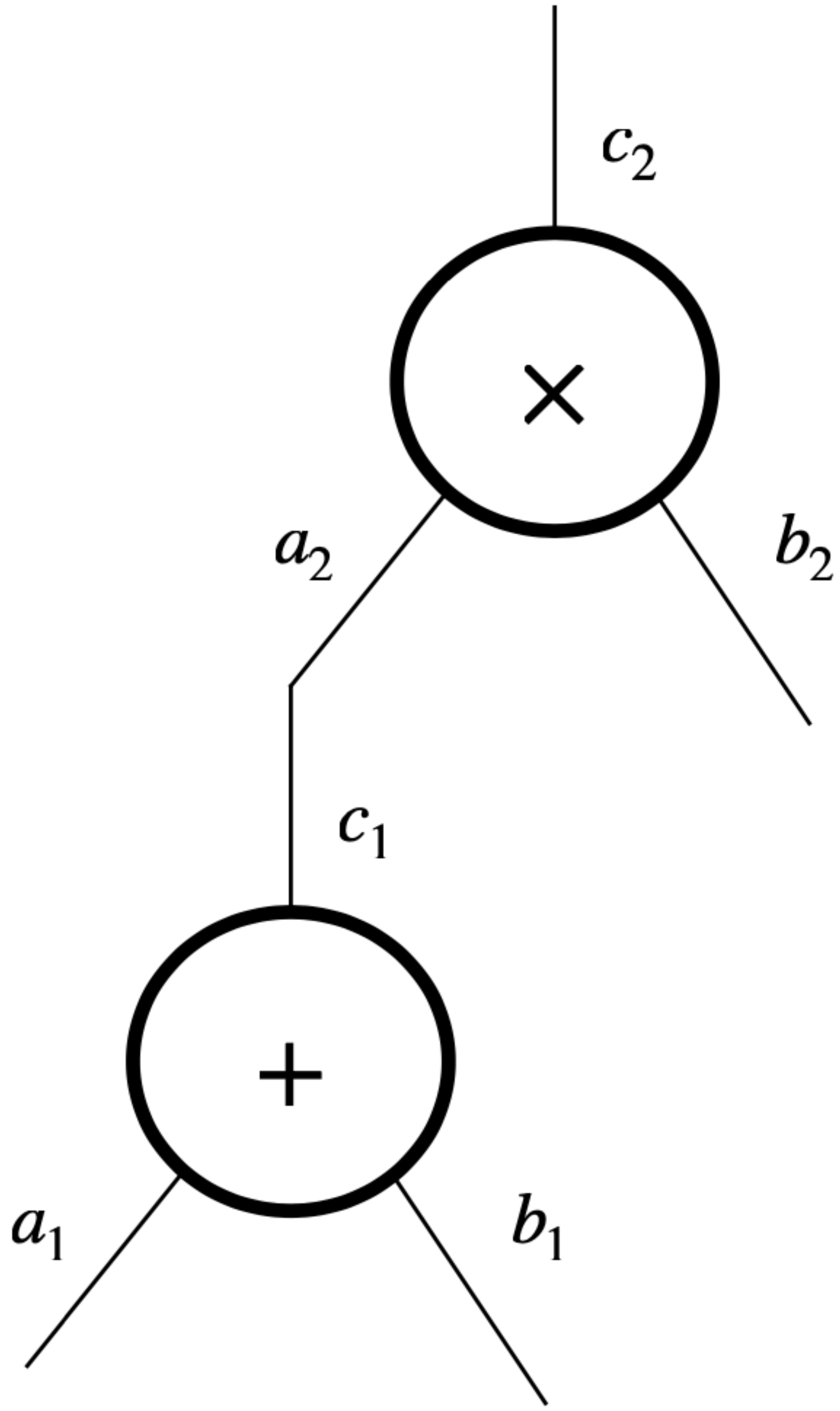
i	a_i	b_i	c_i	S_i
1	4	5	9	1
2	9	10	2	0

+ Copy

$A(x)$

$A(1) = 4$

$A(2) = 9$



Arithmetization

PLONKish

Computation: $(a_1 + b_1) \cdot b_2 = c_2 \mod 11$

Solution: $a_1 = 4$, $b_1 = 5$,$b_2 = 10$, $c_1 = 9$, $a_2 = 9$, $c_2 = 2$

Gate Constraints : $S_i(a_i + b_i) + (1 - S_i)(a_i \cdot b_i) - c_i = 0$

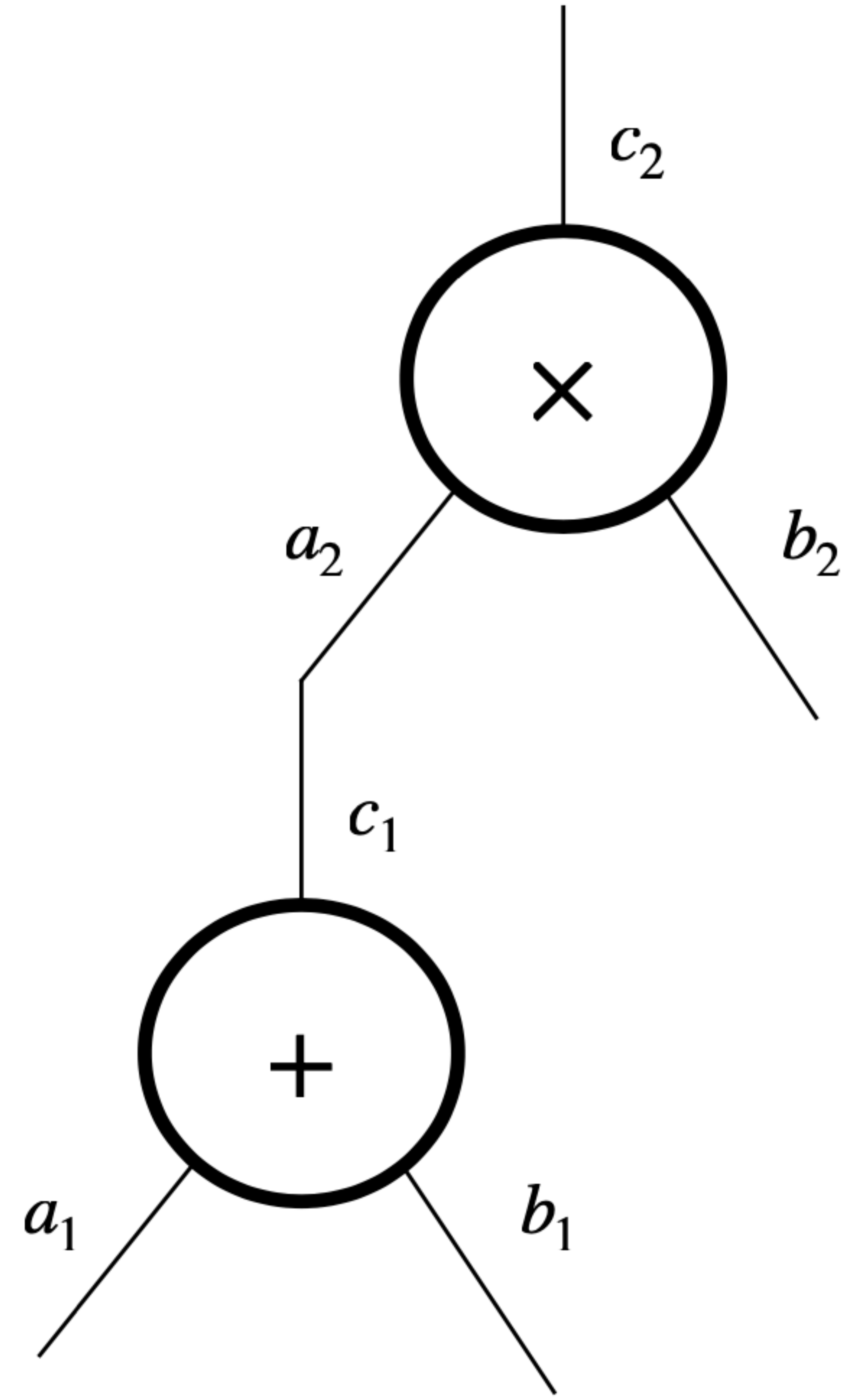
i	a_i	b_i	c_i	S_i
1	4	5	9	1
2	9	10	2	0

+ Copy

$A(x)$ $B(x)$

$A(1) = 4$ $B(1) = 5$

$A(2) = 9$ $B(2) = 10$



Arithmetization

PLONKish

Computation: $(a_1 + b_1) \cdot b_2 = c_2 \mod 11$

Solution: $a_1 = 4$, $b_1 = 5$, $b_2 = 10$, $c_1 = 9$, $a_2 = 9$, $c_2 = 2$

Gate Constraints : $S_i(a_i + b_i) + (1 - S_i)(a_i \cdot b_i) - c_i = 0$

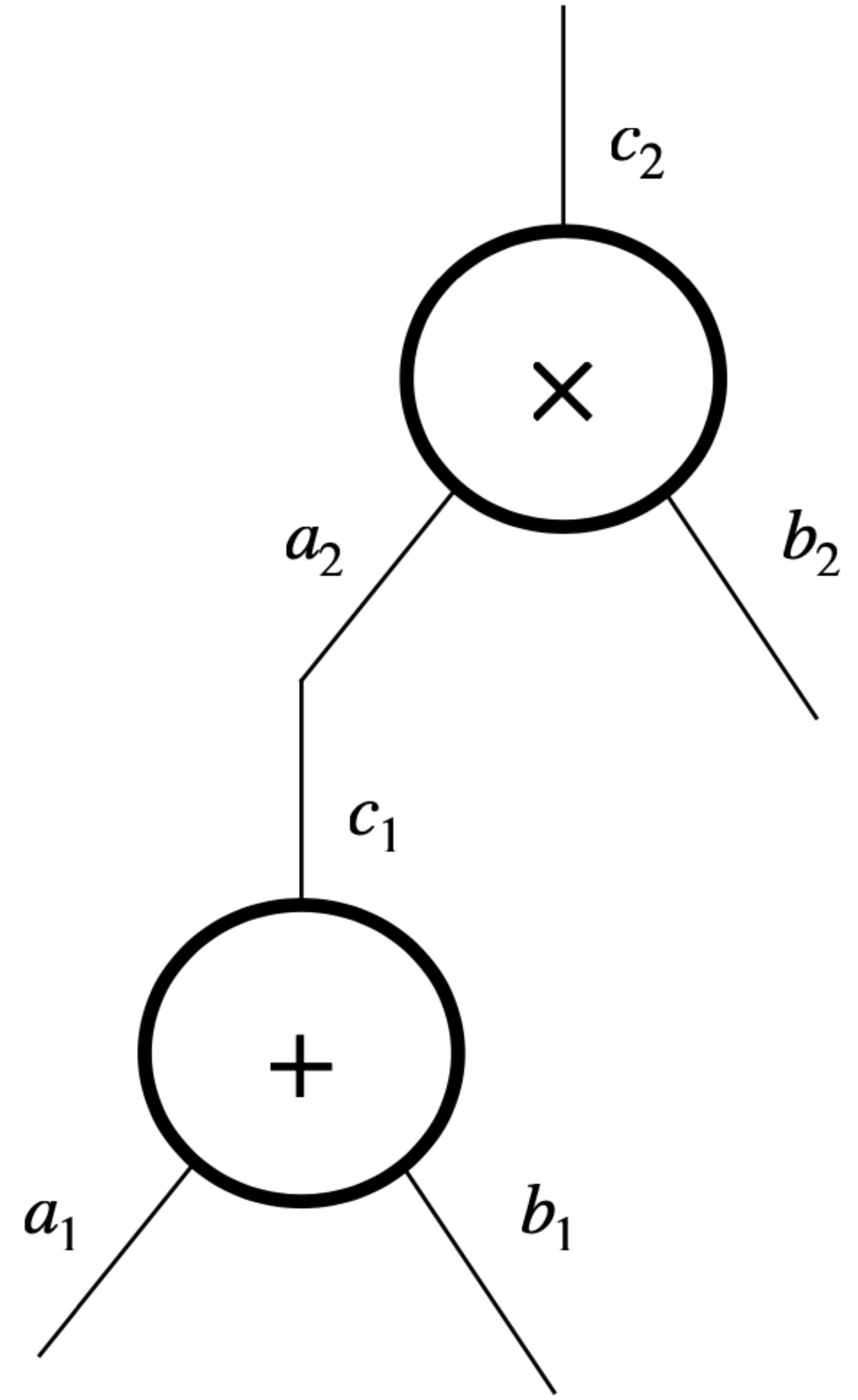
i	a_i	b_i	c_i	S_i
1	4	5	9	1
2	9	10	2	0

+ Copy

$A(x)$ $B(x)$

$A(1) = 4$ $B(1) = 5$

$A(2) = 9$ $B(2) = 10$



$$P(x) = S(x)(A(x) + B(x)) + (1 - S(x))(A(x)B(x)) - C(x)$$

Arithmetization

PLONKish

Computation: $(a_1 + b_1) \cdot b_2 = c_2 \mod 11$

Solution: $a_1 = 4$, $b_1 = 5$,$b_2 = 10$, $c_1 = 9$, $a_2 = 9$, $c_2 = 2$

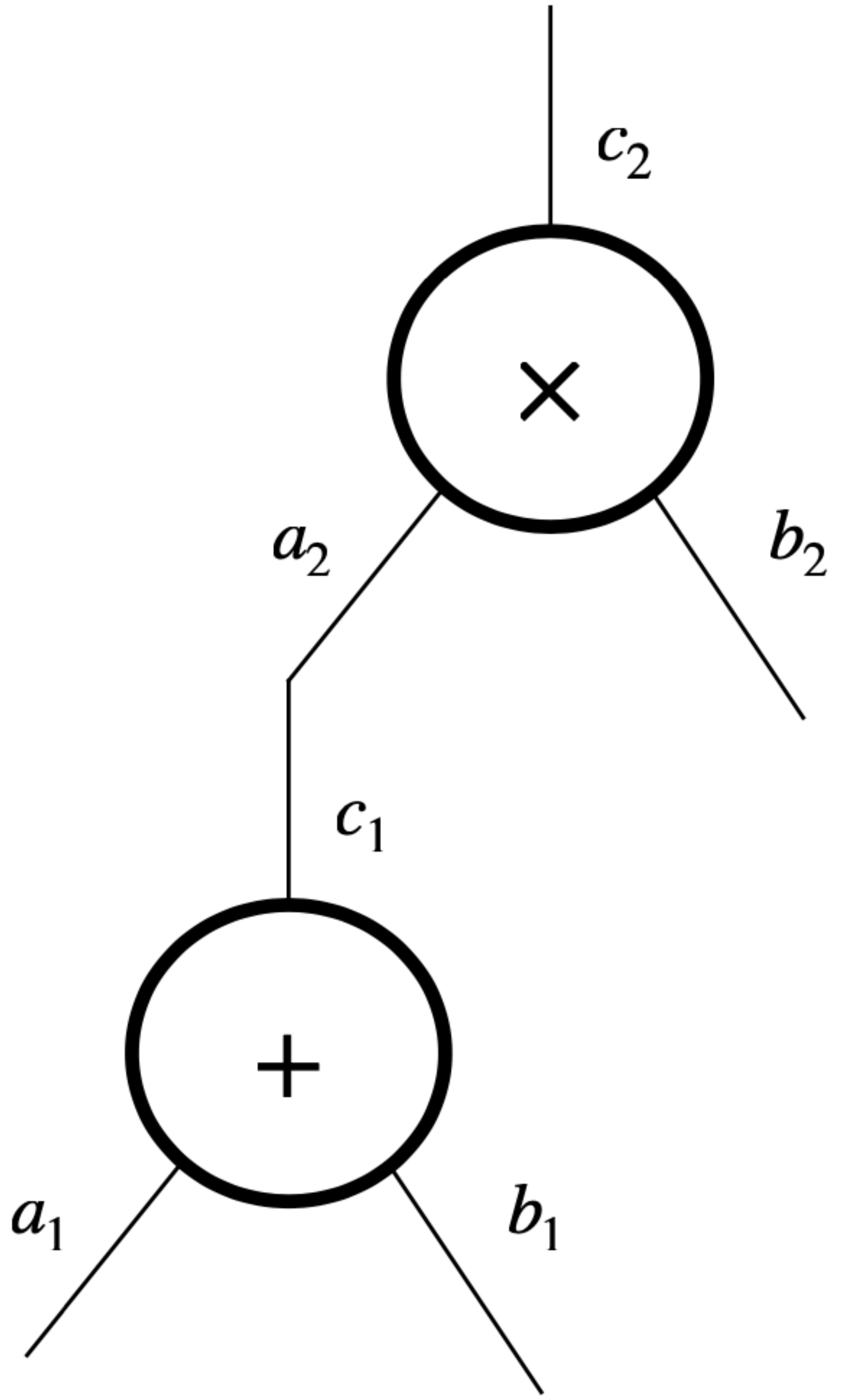
Gate Constraints : $S_i(a_i + b_i) + (1 - S_i)(a_i \cdot b_i) - c_i = 0$

i	a_i	b_i	c_i	S_i
1	4	5	9	1
2	9	10	2	0

+ Copy

$$P(x) = S(x)(A(x) + B(x)) + (1 - S(x))(A(x)B(x)) - C(x)$$

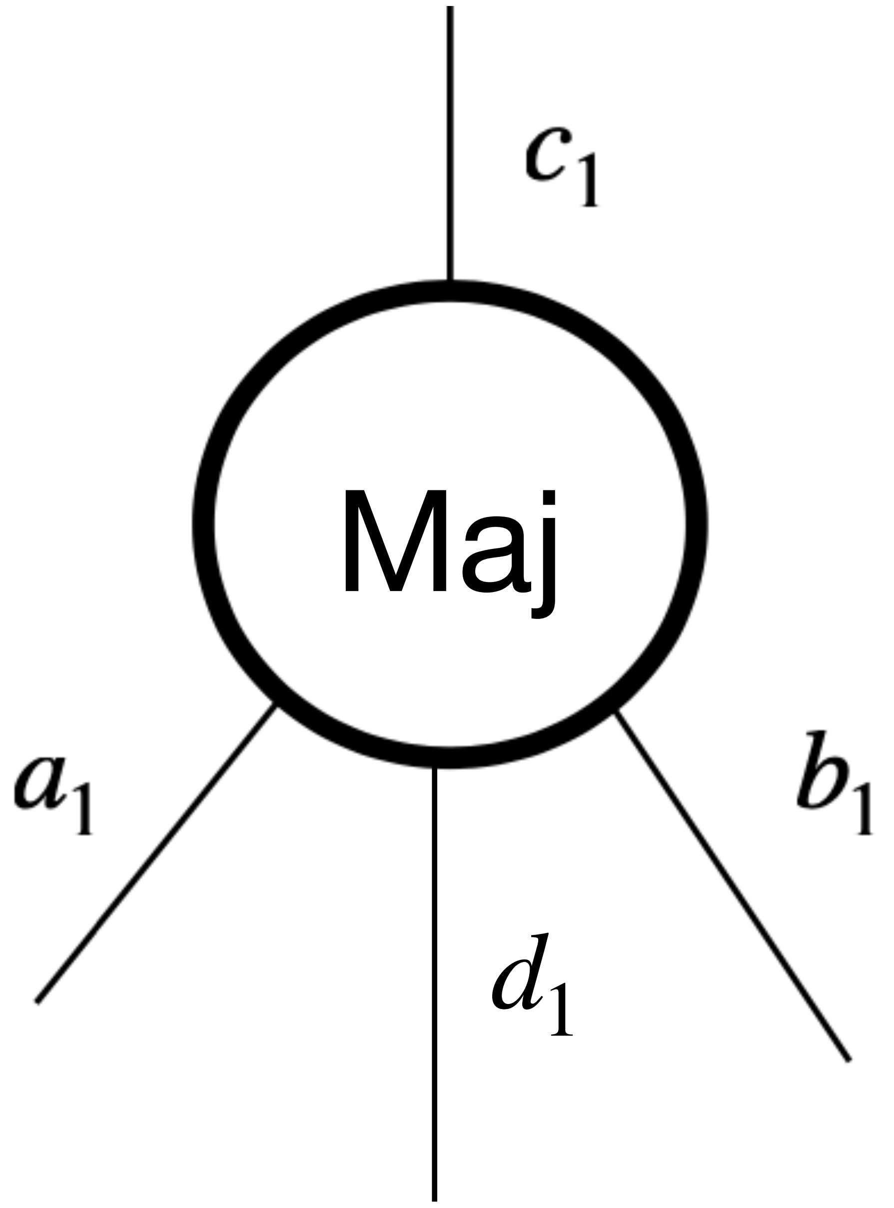
$P(1) = 0, \quad P(2) = 0 \implies (x-1)\cdot(x-2)$ **divides** $P(x)$



Arithmetization

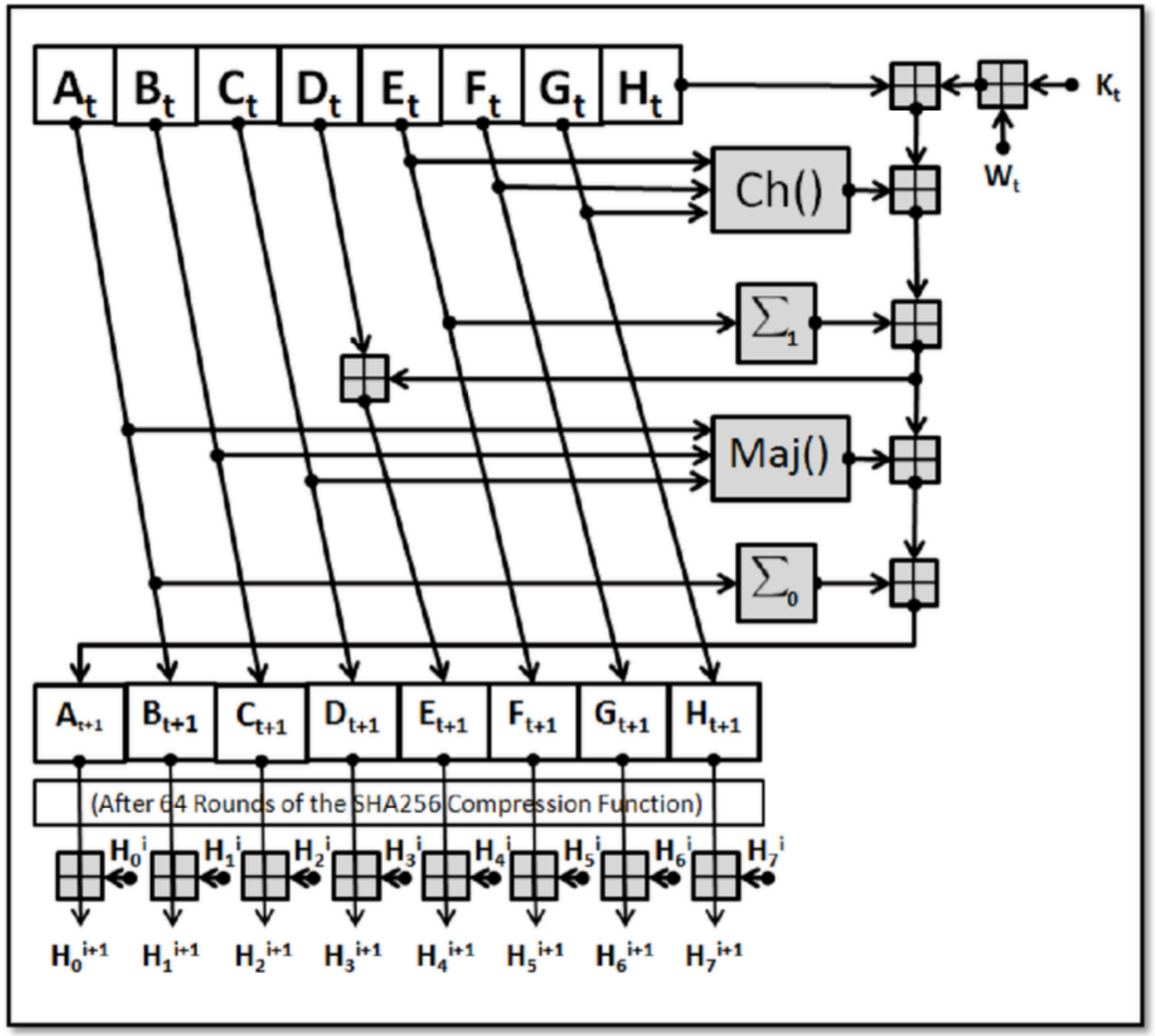
PLONKish - Custom Gates

$$S_1 \cdot (a_1 + b_1) + S_2 \cdot (a_1 \cdot b_1) + S_3 \cdot (Maj(a_1, d_1, b_1)) - c_1 = 0$$



Arithmetization

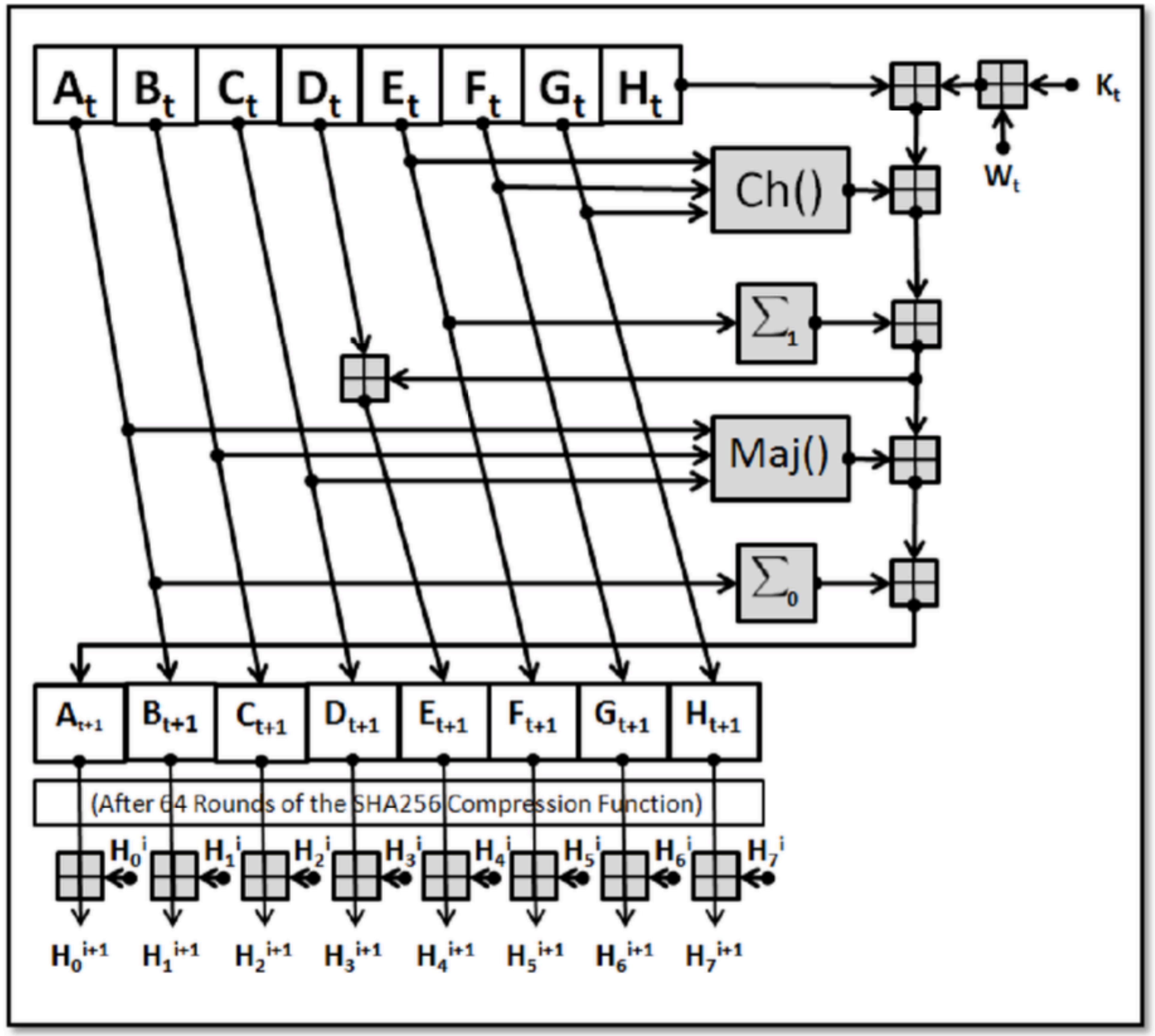
PLONKish



Alternative: Algebraic Hash Functions

Arithmetization

PLONKish - Lookup Arguments



Arithmetization

PLONKish - Lookup Arguments

a	b	c	Maj(a,b,c)
1	0	1	1

Arithmetization

PLONKish - Lookup Arguments

a	b	c	Maj(a,b,c)
1	0	1	1

a	b	c	Maj(a,b,c)
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Arithmetization

PLONKish - Lookup Arguments

a	b	c	Maj(a,b,c)
1	0	1	1

a	b	c	Maj(a,b,c)
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Arithmetization

PLONKish - Lookup Arguments

a	b	c	Maj(a,b,c)
[redacted]			

a	b	c	Maj(a,b,c)
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Arithmetization

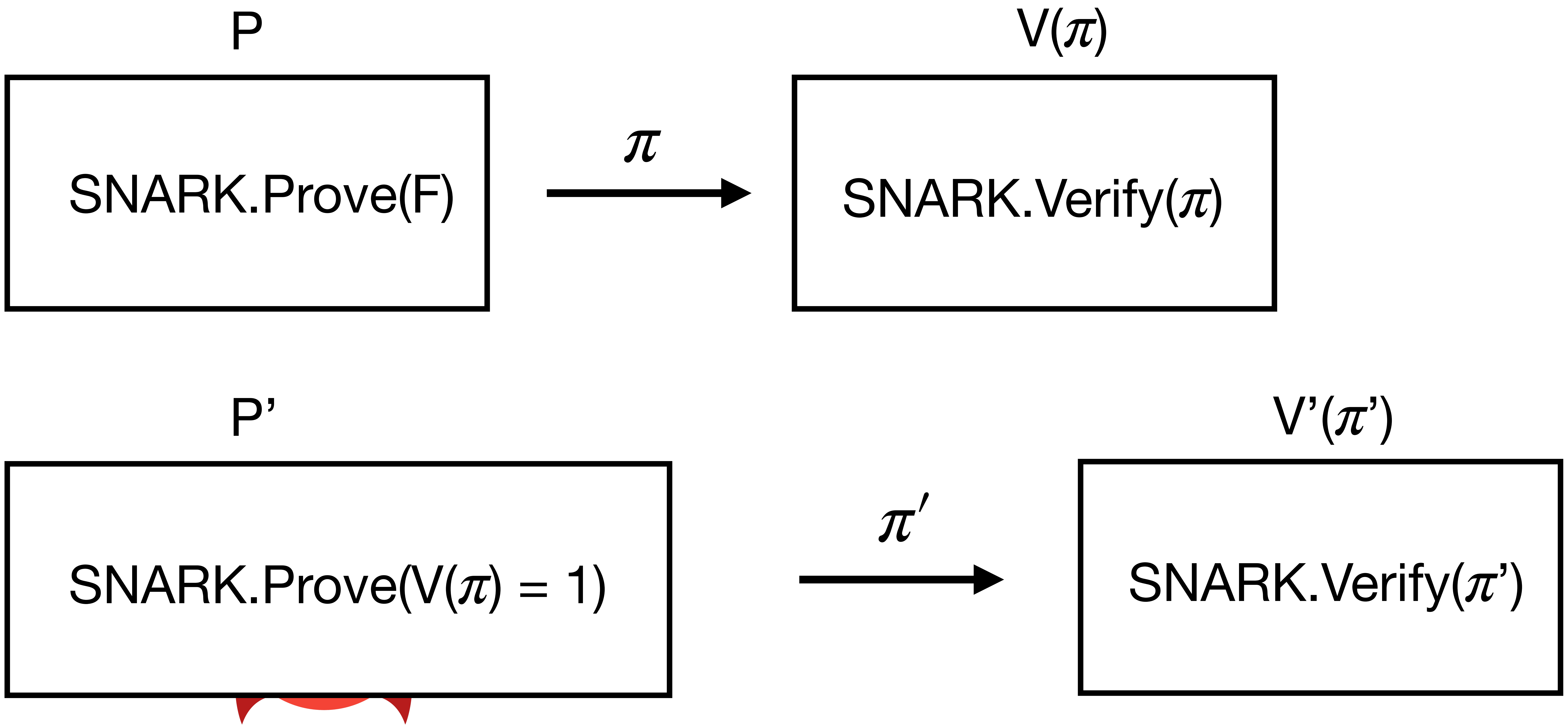
AIR - FRI

Step	R1	R2	R3
1	4	3	2
2	2	2	6
3	3	6	4
4	65	4	2

DSL

- HDL: Circom
- Zokrates, Noir, Cairo, Leo

Proof Composition



Doğru giden birçok şey var.

Ne ters gidebilir?

Sigma Protocol

Non-interactivity via Fiat Shamir

Interactive protocol

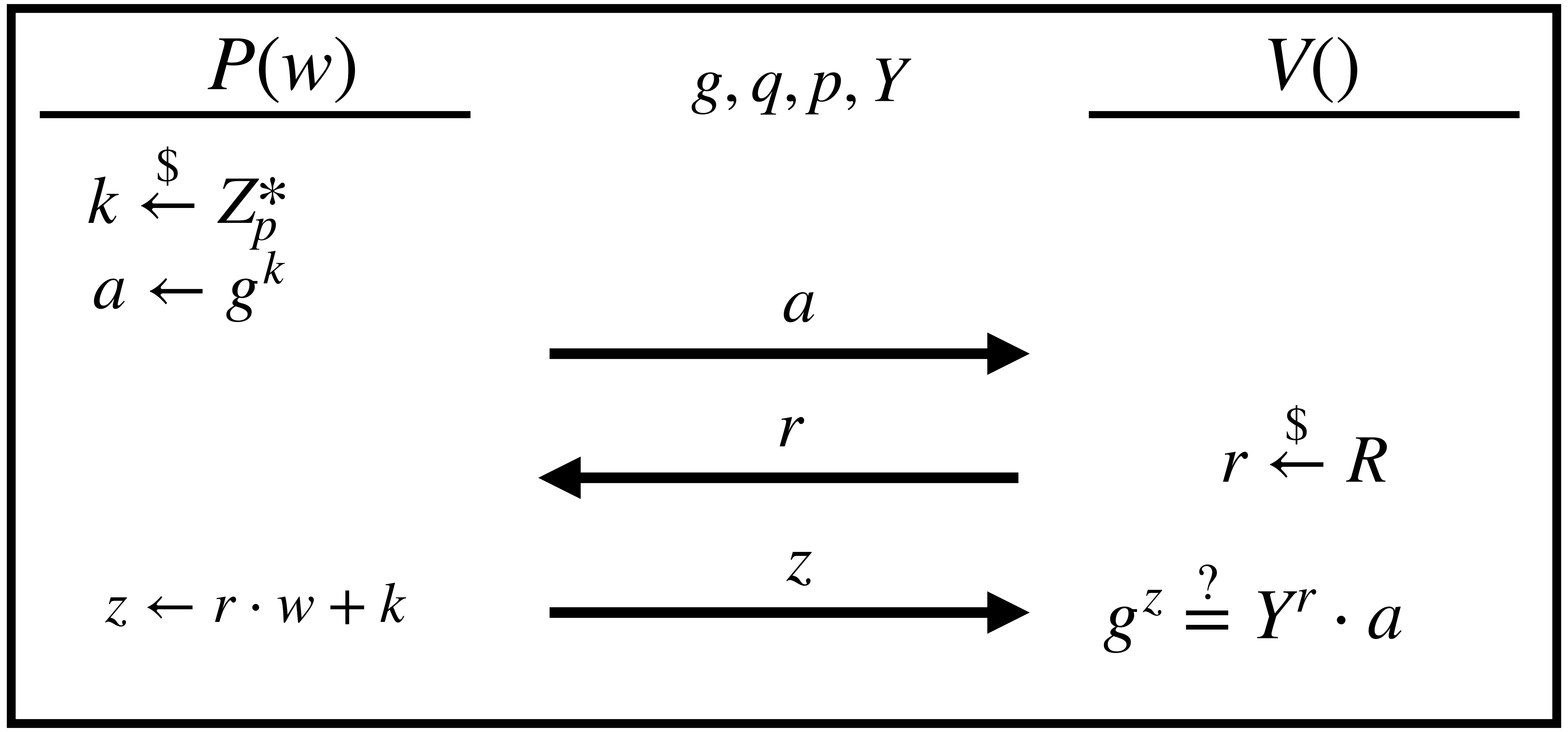
$P(w)$	g, q, p, Y	$V()$
$k \xleftarrow{\$} Z_p^*$		
$a \leftarrow g^k$	a →	
	← r	$r \xleftarrow{\$} R$
$z \leftarrow r \cdot w + k$	z →	$g^z \stackrel{?}{=} Y^r \cdot a$

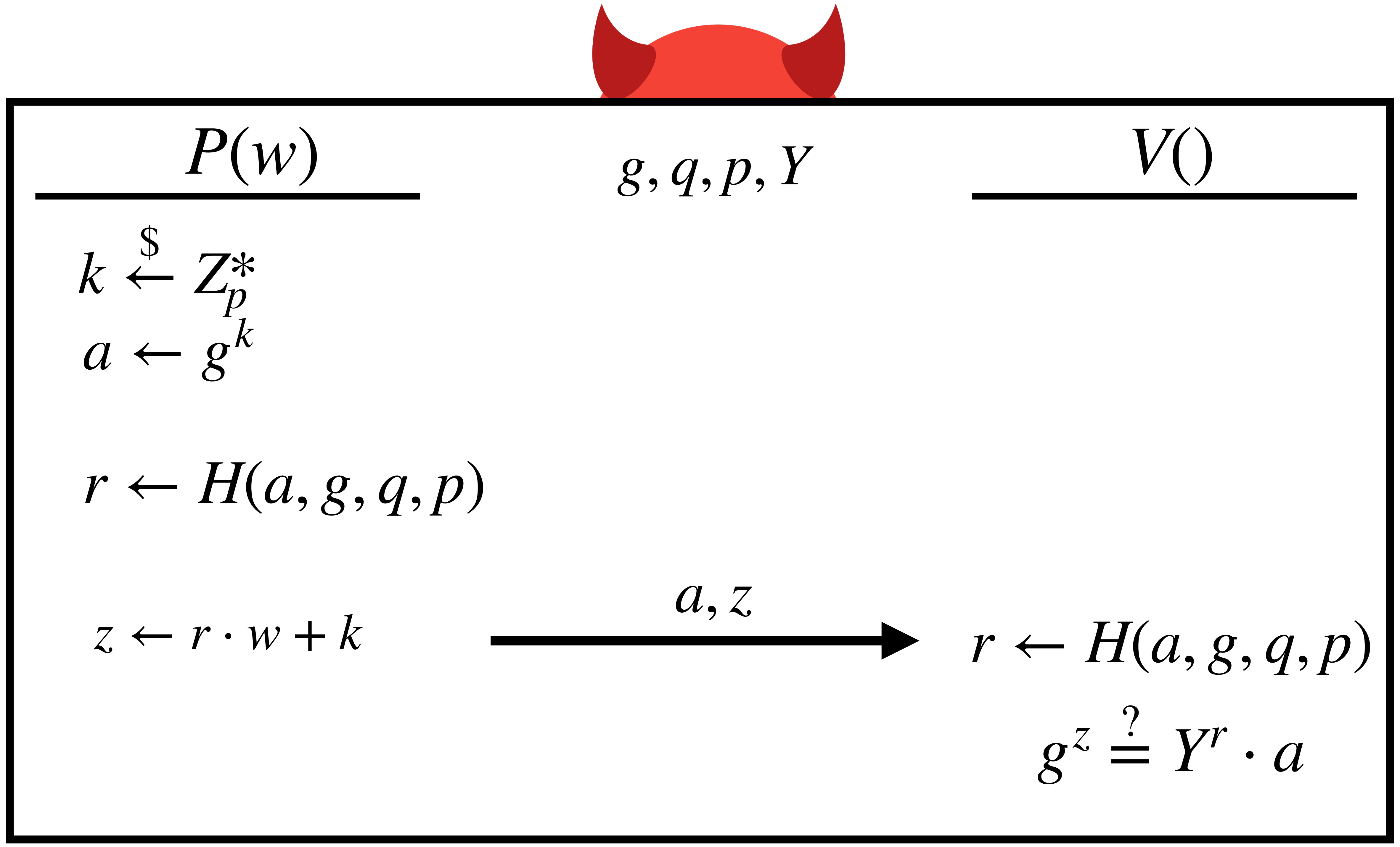
Non-interactive protocol

$P(w)$	g, q, p, Y	$V()$
$k \xleftarrow{\$} Z_p^*$		
$a \leftarrow g^k$		
$r \leftarrow H(a, g, q, p)$		
$z \leftarrow r \cdot w + k$	a, z →	$r \leftarrow H(a, g, q, p)$
		$g^z \stackrel{?}{=} Y^r \cdot a$

Sigma Protocol

Non-interactivity via Fiat Shamir





Sigma Protocol

Non-interactivity via Fiat Shamir

$P(w)$	g, q, p, Y	$V()$
$k \xleftarrow{\$} Z_p^*$		
$a \leftarrow g^k$	a →	
	← r	$r \xleftarrow{\$} R$
$z \leftarrow r \cdot w + k$	z →	$g^z \stackrel{?}{=} Y^r \cdot a$

$P(w)$	g, q, p, Y	$V()$
$k \xleftarrow{\$} Z_p^*$		
$a \leftarrow g^k$		
$r \leftarrow H(a, g, q, p)$		
$z \leftarrow r \cdot w + k$	a, z →	$r \leftarrow H(a, g, q, p)$
		$g^z \stackrel{?}{=} Y^r \cdot a$

Sigma Protocol

Non-interactivity via Fiat Shamir [BPW'16]

$P^*()$ $\qquad g, q, p, Y' \qquad$ $V()$

$a \leftarrow K$ random public key

$r \leftarrow H(a, g, q, p)$

$Y' \leftarrow (g^z / K)^{1/r}$

$\xrightarrow{a, z}$

$r \leftarrow H(a, g, q, p)$

$g^z \stackrel{?}{=} Y'^r \cdot a$

$P(w)$ $\qquad g, q, p, Y \qquad$ $V()$

$k \stackrel{\$}{\leftarrow} Z_p^*$

$a \leftarrow g^k$

$r \leftarrow H(a, g, q, p)$

$z \leftarrow r \cdot w + k$

$\xrightarrow{a, z}$

$r \leftarrow H(a, g, q, p)$

$g^z \stackrel{?}{=} Y^r \cdot a$

Sigma Protocol

Non-interactivity via Fiat Shamir [BPW'16]

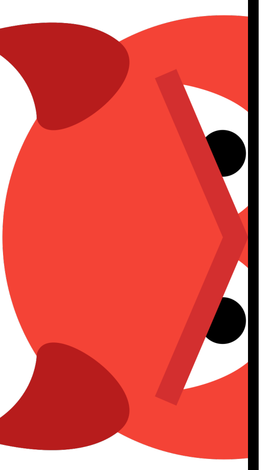
$P^*()$	g, q, p, Y'	$V()$
$a \leftarrow K$ random public key		
$z \xleftarrow{\$} Z_p^*$		
$r \leftarrow H(a, g, q, p)$		
$Y' \leftarrow (g^z/K)^{1/r}$	$\xrightarrow{a, z}$	$r \leftarrow H(a, g, q, p)$
		$g^z \stackrel{?}{=} Y'^r \cdot a$

$P(w)$	g, q, p, Y	$V()$
$k \xleftarrow{\$} Z_p^*$		
$a \leftarrow g^k$		
$r \leftarrow H(a, g, q, p)$		
$z \leftarrow r \cdot w + k$	$\xrightarrow{a, z}$	$r \leftarrow H(a, g, q, p)$
		$g^z \stackrel{?}{=} Y^r \cdot a$

IOP Realization

- IOP + Commitment
- Most cryptographic properties inherited by the commitment scheme.
  - Trusted setup
  - Post-quantum security

IOP Realization



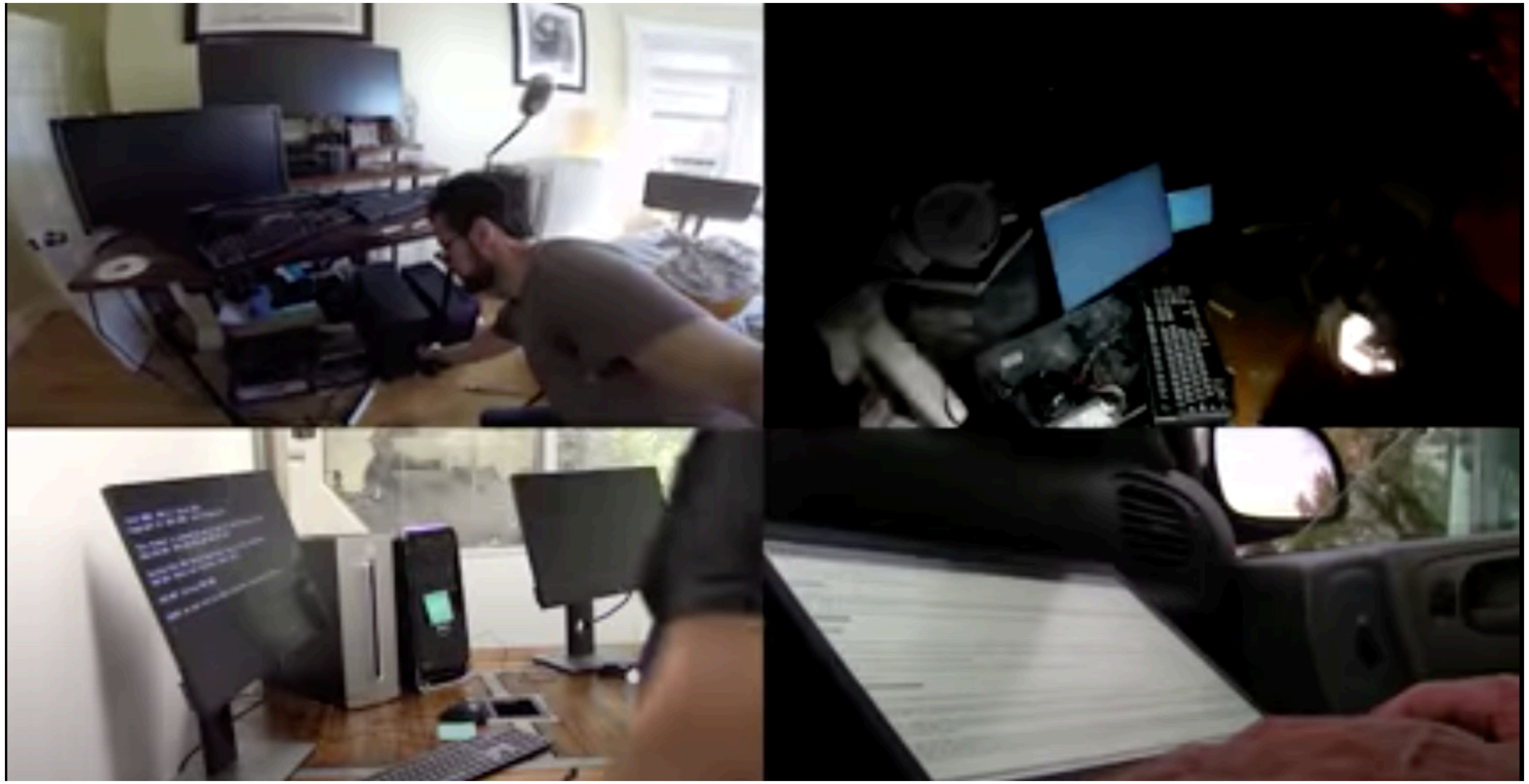
- IOP + Commitment
- Most cryptographic properties inherited by the commitment scheme.
    - Trusted setup
    - Post-quantum security

Infinite Inflation Bug

Zcash Trusted Setup (2017)

Infinite Inflation Bug

Zcash Trusted Setup (2017)



Infinite Inflation Bug

Zcash Trusted Setup (2017)

Infinite Inflation Bug

Zcash Trusted Setup (2017)

Zcash Counterfeiting Vulnerability Successfully Remediated

Josh Swihart, Benjamin Winston and Sean Bowe | February 5, 2019

Infinite Inflation Bug

Zcash Trusted Setup

BCTV'13

3. Set $\mathsf{pk} := (C, \mathsf{pk}_\mathsf{A}, \mathsf{pk}'_\mathsf{A}, \mathsf{pk}_\mathsf{B}, \mathsf{pk}'_\mathsf{B}, \mathsf{pk}_\mathsf{C}, \mathsf{pk}'_\mathsf{C}, \mathsf{pk}_\mathsf{K}, \mathsf{pk}_\mathsf{H})$ where for $i = 0,1,\ldots,m+3$:

$$\mathsf{pk}_{\mathsf{A},i} := A_i(\tau)\rho_\mathsf{A}\mathcal{P}_1\,, \quad \mathsf{pk}'_{\mathsf{A},i} := A_i(\tau)\alpha_\mathsf{A}\rho_\mathsf{A}\mathcal{P}_1\,,$$

$$\mathsf{pk}_{\mathsf{B},i} := B_i(\tau)\rho_\mathsf{B}\mathcal{P}_2\,, \quad \mathsf{pk}'_{\mathsf{B},i} := B_i(\tau)\alpha_\mathsf{B}\rho_\mathsf{B}\mathcal{P}_1\,,$$

$$\mathsf{pk}_{\mathsf{C},i} := C_i(\tau)\rho_\mathsf{A}\rho_\mathsf{B}\mathcal{P}_1\,, \mathsf{pk}'_{\mathsf{C},i} := C_i(\tau)\alpha_\mathsf{C}\rho_\mathsf{A}\rho_\mathsf{B}\mathcal{P}_1\,,$$

$$\mathsf{pk}_{\mathsf{K},i} := \beta\big(A_i(\tau)\rho_\mathsf{A} + B_i(\tau)\rho_\mathsf{B} + C_i(\tau)\rho_\mathsf{A}\rho_\mathsf{B}\big)\mathcal{P}_1\,,$$

Infinite Inflation Bug

Zcash Trusted Setup

BCTV'13

3. Set $\mathsf{pk} := (C, \mathsf{pk}_\mathsf{A}, \mathsf{pk}'_\mathsf{A}, \mathsf{pk}_\mathsf{B}, \mathsf{pk}'_\mathsf{B}, \mathsf{pk}_\mathsf{C}, \mathsf{pk}'_\mathsf{C}, \mathsf{pk}_\mathsf{K}, \mathsf{pk}_\mathsf{H})$ where for $i = 0,1,\ldots,m+3$:

$$\mathsf{pk}_{\mathsf{A},i} := A_i(\tau)\rho_\mathsf{A}\mathcal{P}_1\,, \quad \mathsf{pk}'_{\mathsf{A},i} := A_i(\tau)\alpha_\mathsf{A}\rho_\mathsf{A}\mathcal{P}_1\,,$$
$$\mathsf{pk}_{\mathsf{B},i} := B_i(\tau)\rho_\mathsf{B}\mathcal{P}_2\,, \quad \mathsf{pk}'_{\mathsf{B},i} := B_i(\tau)\alpha_\mathsf{B}\rho_\mathsf{B}\mathcal{P}_1\,,$$
$$\mathsf{pk}_{\mathsf{C},i} := C_i(\tau)\rho_\mathsf{A}\rho_\mathsf{B}\mathcal{P}_1\,, \mathsf{pk}'_{\mathsf{C},i} := C_i(\tau)\alpha_\mathsf{C}\rho_\mathsf{A}\rho_\mathsf{B}\mathcal{P}_1\,,$$
$$\mathsf{pk}_{\mathsf{K},i} := \beta\big(A_i(\tau)\rho_\mathsf{A} + B_i(\tau)\rho_\mathsf{B} + C_i(\tau)\rho_\mathsf{A}\rho_\mathsf{B}\big)\mathcal{P}_1\,,$$

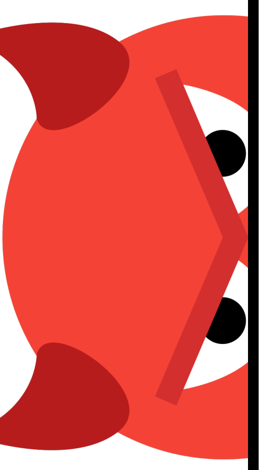
BCTV'19

3. Set $\mathsf{pk} := (C, \mathsf{pk}_\mathsf{A}, \mathsf{pk}'_\mathsf{A}, \mathsf{pk}_\mathsf{B}, \mathsf{pk}'_\mathsf{B}, \mathsf{pk}_\mathsf{C}, \mathsf{pk}'_\mathsf{C}, \mathsf{pk}_\mathsf{K}, \mathsf{pk}_\mathsf{H})$ where:

$$\mathsf{pk}_\mathsf{A} := \{A_i(\tau)\rho_\mathsf{A}\mathcal{P}_1\}_{i=0}^{m+3}\,, \quad \mathsf{pk}'_\mathsf{A} := \{A_i(\tau)\alpha_\mathsf{A}\rho_\mathsf{A}\mathcal{P}_1\}_{i=n+1}^{m+3}$$
$$\mathsf{pk}_\mathsf{B} := \{B_i(\tau)\rho_\mathsf{B}\mathcal{P}_2\}_{i=0}^{m+3}\,, \quad \mathsf{pk}'_\mathsf{B} := \{B_i(\tau)\alpha_\mathsf{B}\rho_\mathsf{B}\mathcal{P}_1\}_{i=0}^{m+3}\,,$$
$$\mathsf{pk}_\mathsf{C} := \{C_i(\tau)\rho_\mathsf{A}\rho_\mathsf{B}\mathcal{P}_1\}_{i=0}^{m+3}\,, \mathsf{pk}'_\mathsf{C} := \{C_i(\tau)\alpha_\mathsf{C}\rho_\mathsf{A}\rho_\mathsf{B}\mathcal{P}_1\}_{i=0}^{m+3}\,,$$
$$\mathsf{pk}_\mathsf{K} := \{\beta\big(A_i(\tau)\rho_\mathsf{A} + B_i(\tau)\rho_\mathsf{B} + C_i(\tau)\rho_\mathsf{A}\rho_\mathsf{B}\big)\mathcal{P}_1\}_{i=0}^{m+3}\,,$$

IOP Realization

- IOP + Commitment
- Most cryptographic properties inherited by the commitment scheme.
  - Trusted setup
  - Post-quantum security



Quantum Soundness

Quantum Rewinding [LWS'22]

P $\qquad\qquad\qquad\qquad\qquad\qquad$ V

$\xrightarrow{a}$

$\xleftarrow{r}$ $\qquad r \xleftarrow{\$} R$

$\xrightarrow{z}$

Quantum Soundness

Quantum Rewinding [LWS'22]

P

$\xrightarrow{a}$

V

Quantum Soundness

Quantum Rewinding [LWS'22]

P V

a →

r' ← $r' \xleftarrow{\$} R$

z' →

Quantum Soundness

Quantum Rewinding [LWS'22]

P V

Prover State: $|a\rangle$

measured $|a\rangle$ →

r ← $r \xleftarrow{\$} R$

z →

Quantum Soundness

Quantum Rewinding [LWS'22]

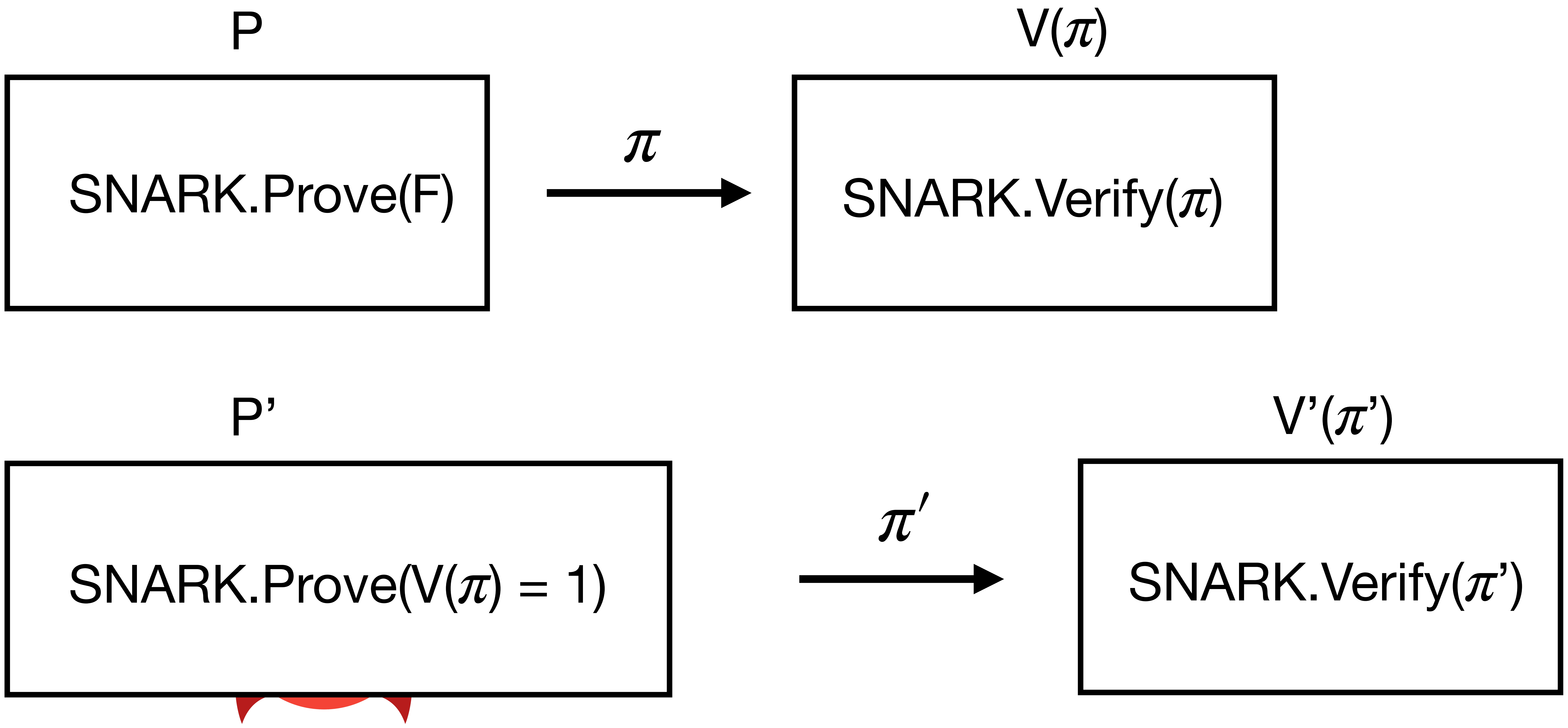
P

Prover State: $|$ ✗

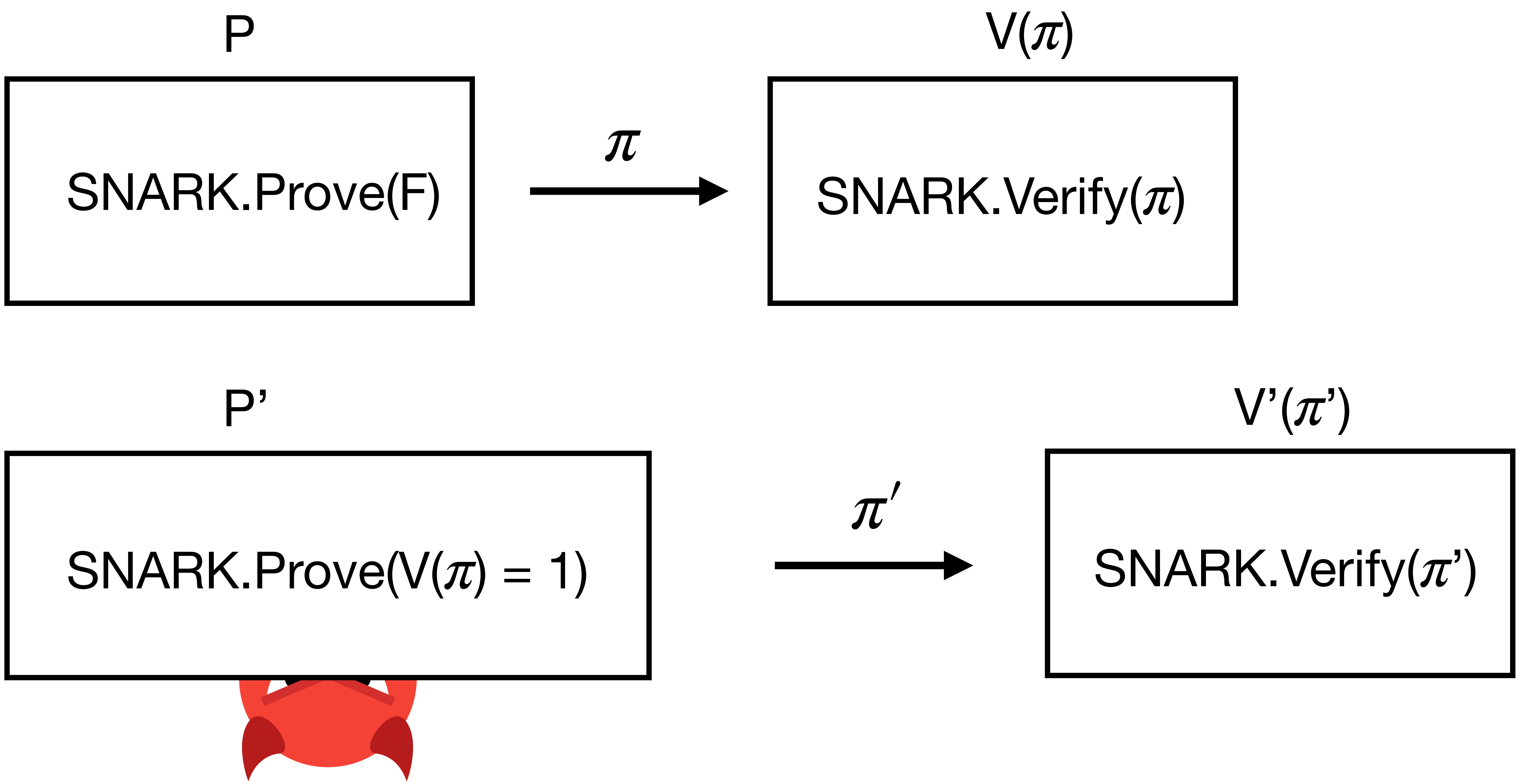
measured $|a\rangle$ →

V

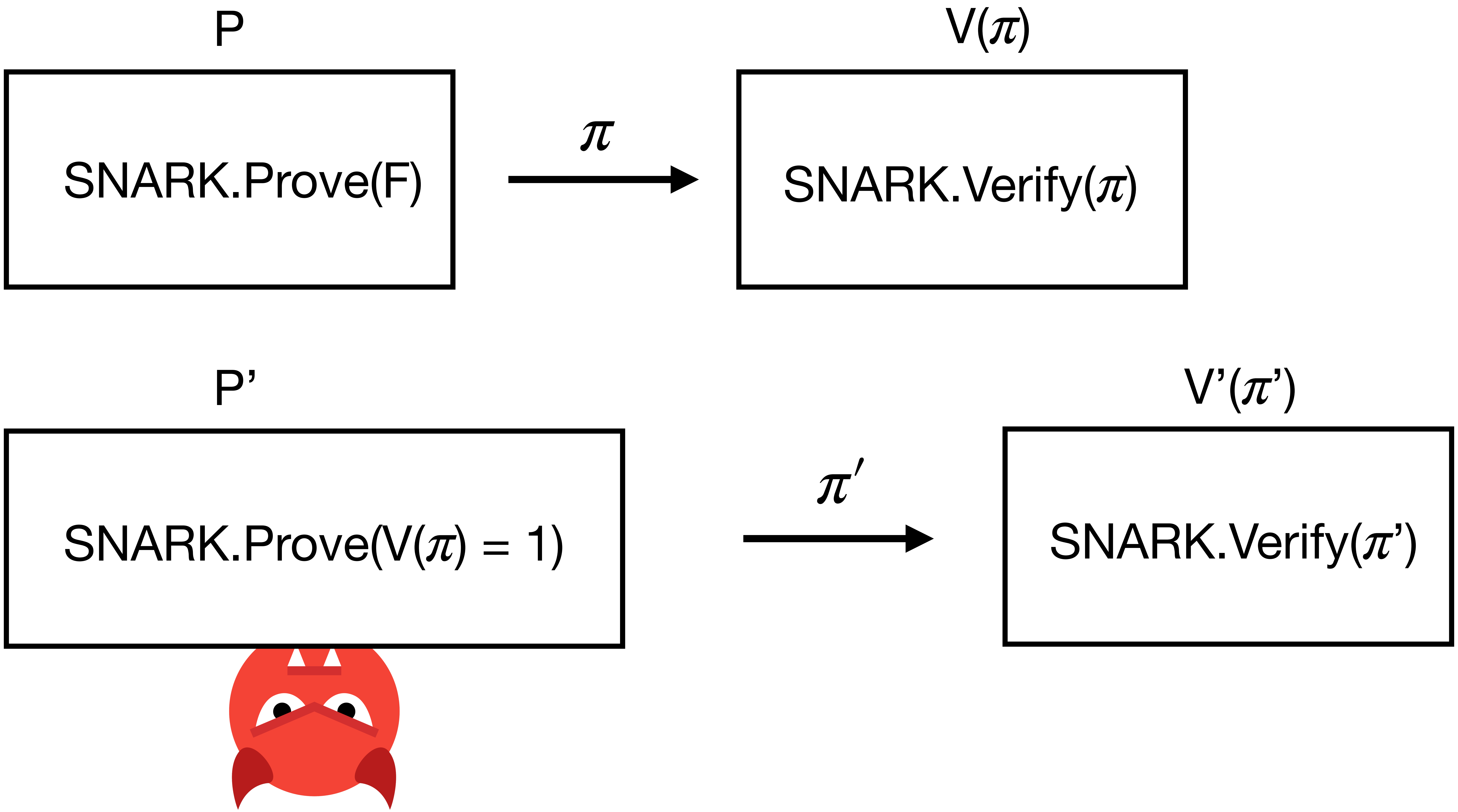
Proof Composition



Proof Composition



Proof Composition



Doğru giden birçok şey var

$$\wedge$$

Ters gidebilecek birçok şey var

$$\Longrightarrow$$

Birçok şey ters gidecek

Teşekkürler!

Abdullah Talayhan
@talayhan_a
abdullahtalayhan.com
abdullah.talayhan@epfl.ch