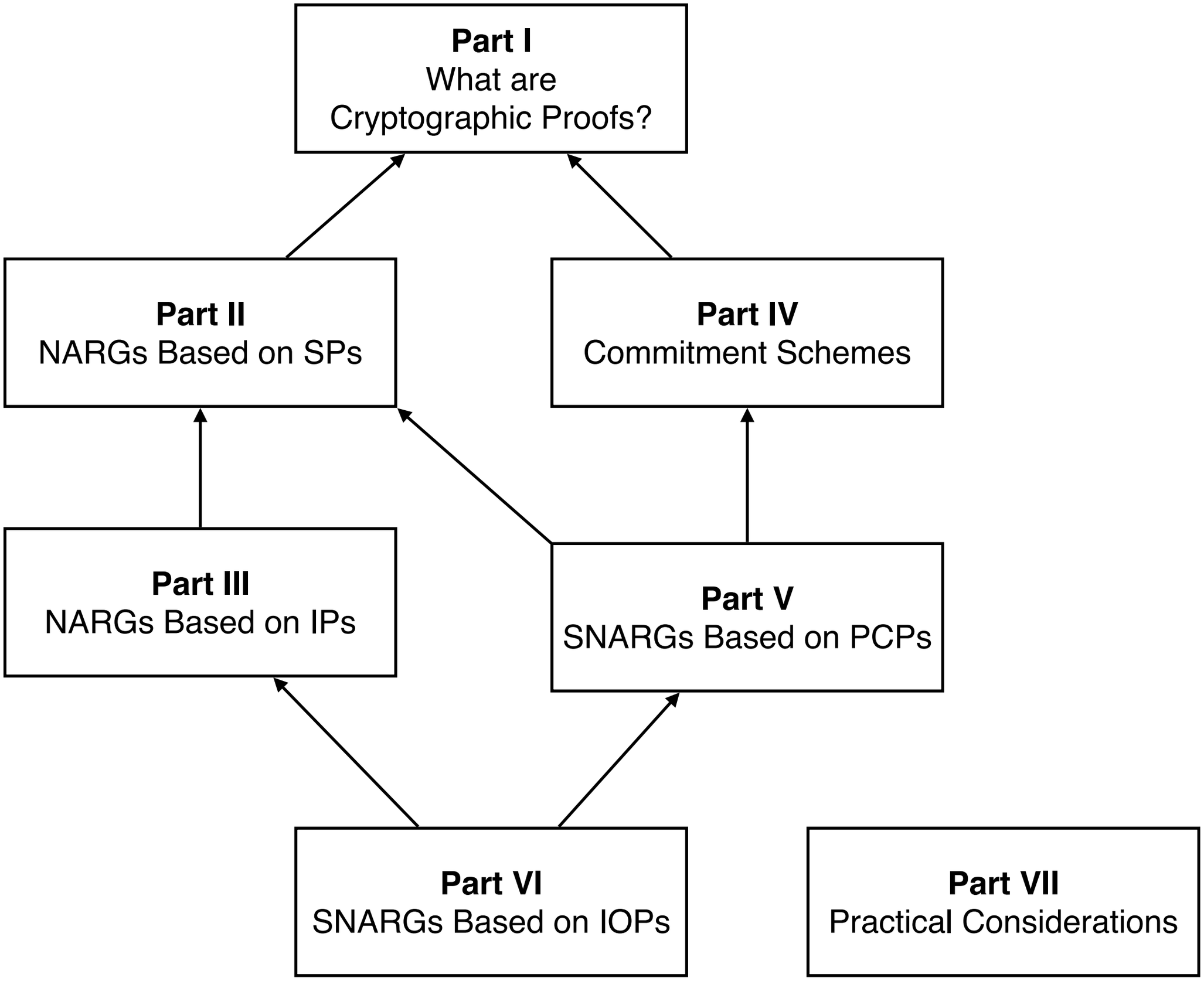
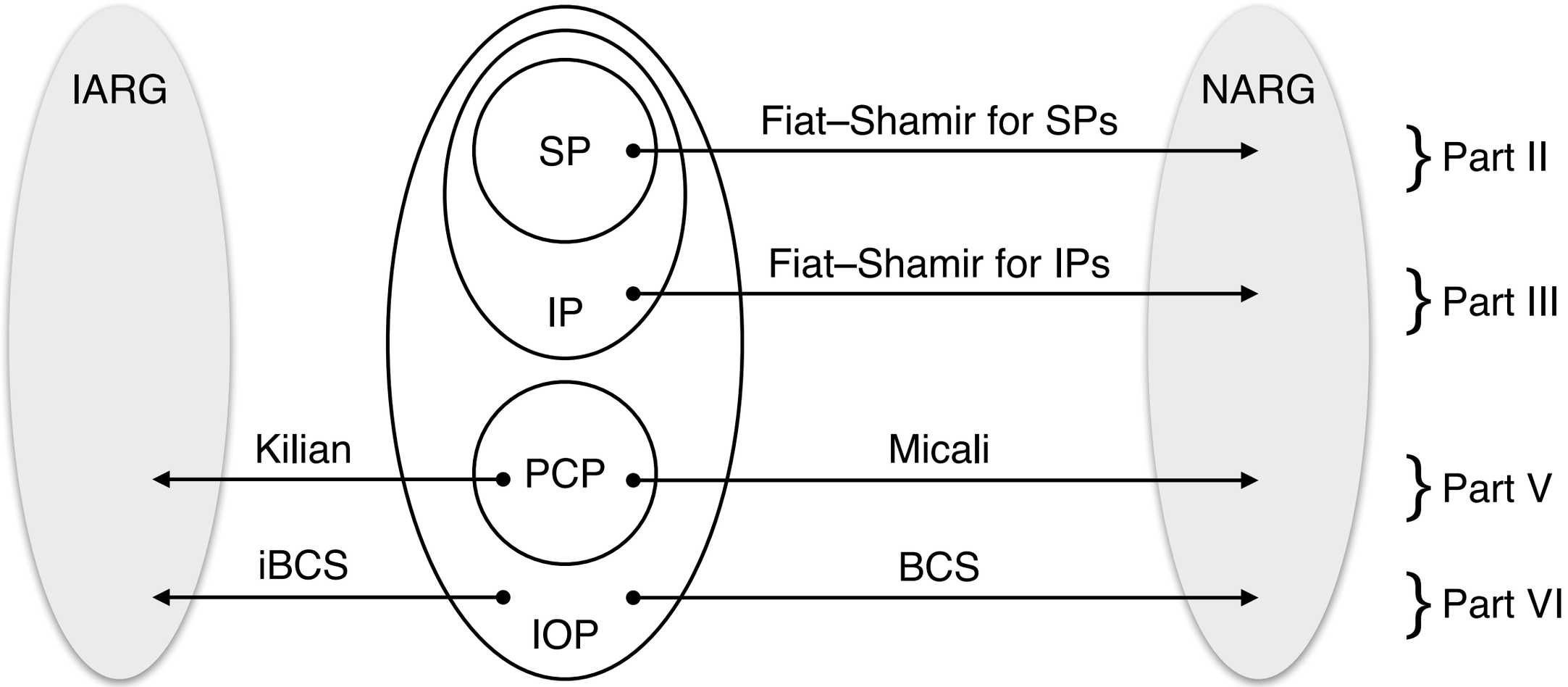
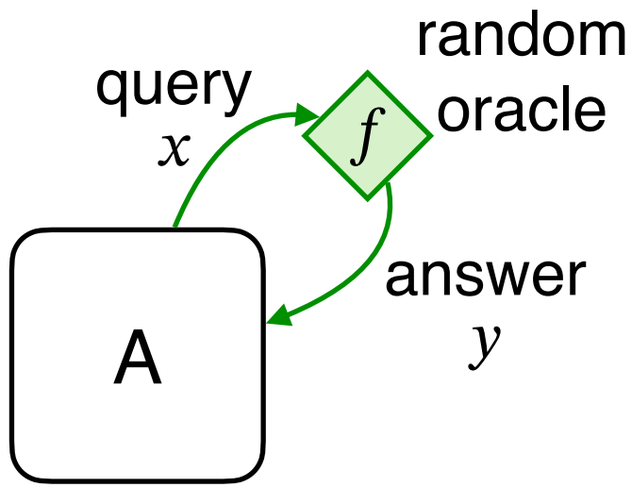
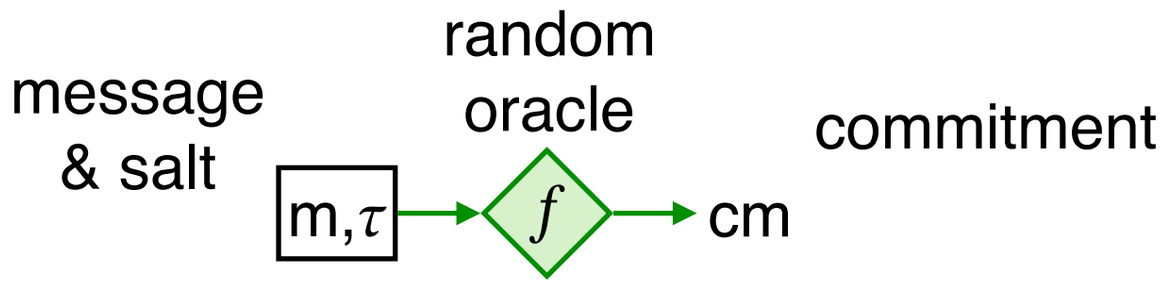
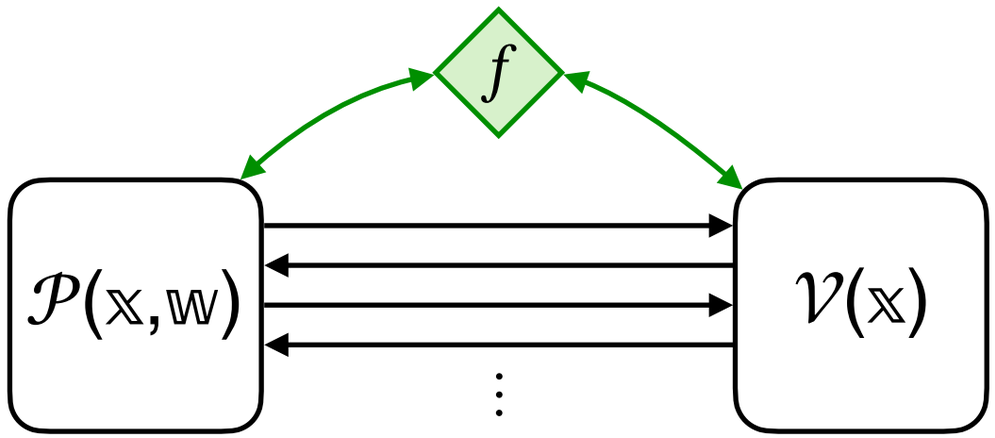
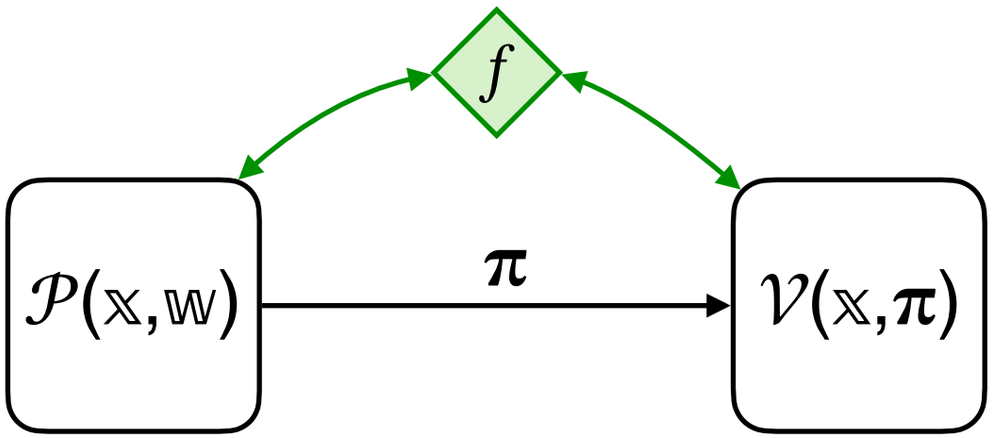

Part I
What are
Cryptographic Proofs?
Part II
NARGs Based on SPs
Part IV
Commitment Schemes
Part III
NARGs Based on IPs
Part V
SNARGs Based on PCPs
Part VI
SNARGs Based on IOPs
Part VII
Practical Considerations

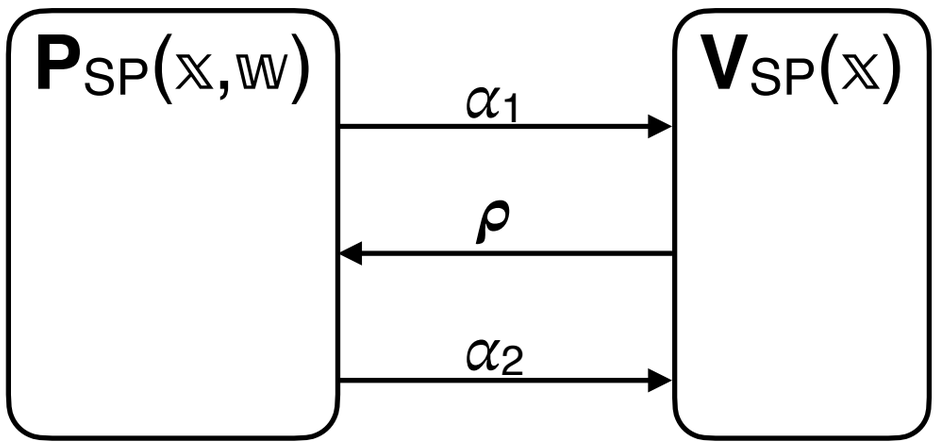

IARG
NARG
SP
IP
PCP
IOP
Fiat–Shamir for SPs
Fiat–Shamir for IPs
Kilian
Micali
iBCS
BCS
Part II
Part III
Part V
Part VI

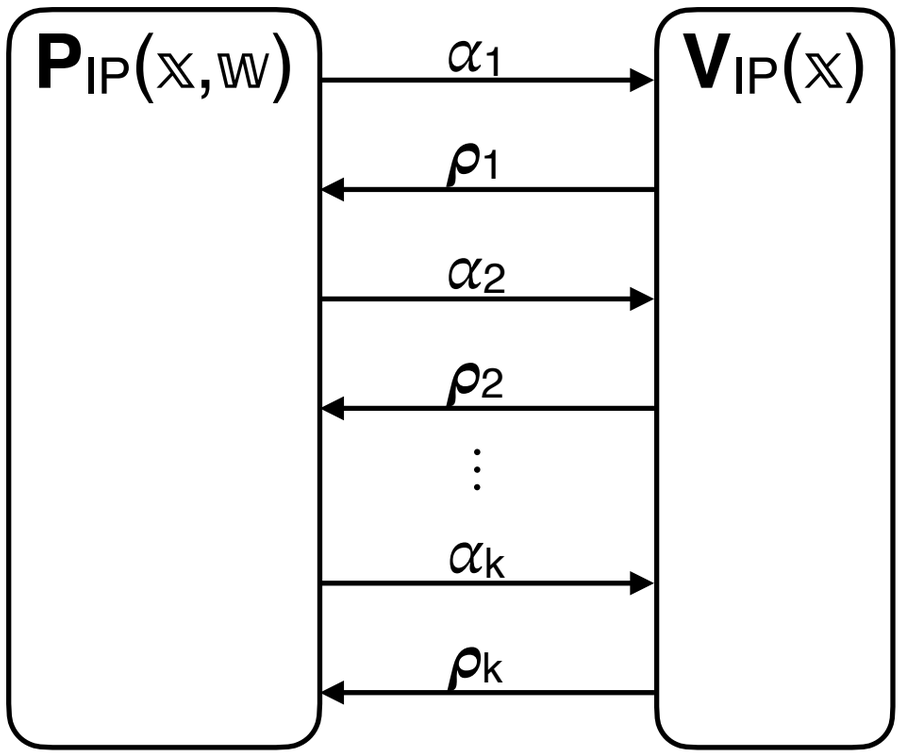

random
oracle
query
x
f
answer
y
A

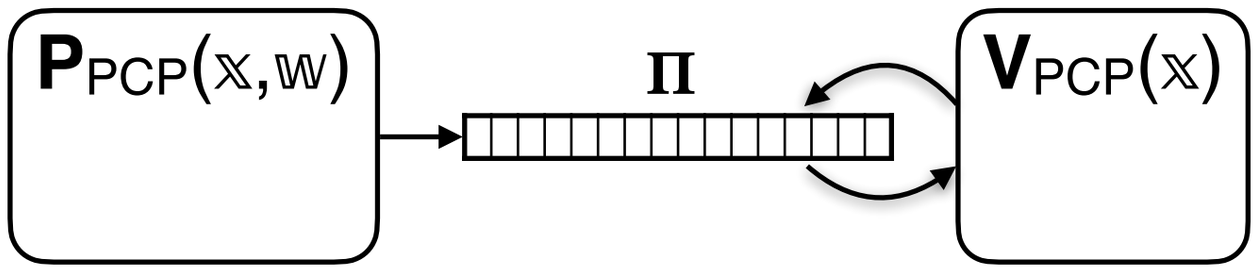

message
& salt
random
oracle
commitment
m,τ
f
cm

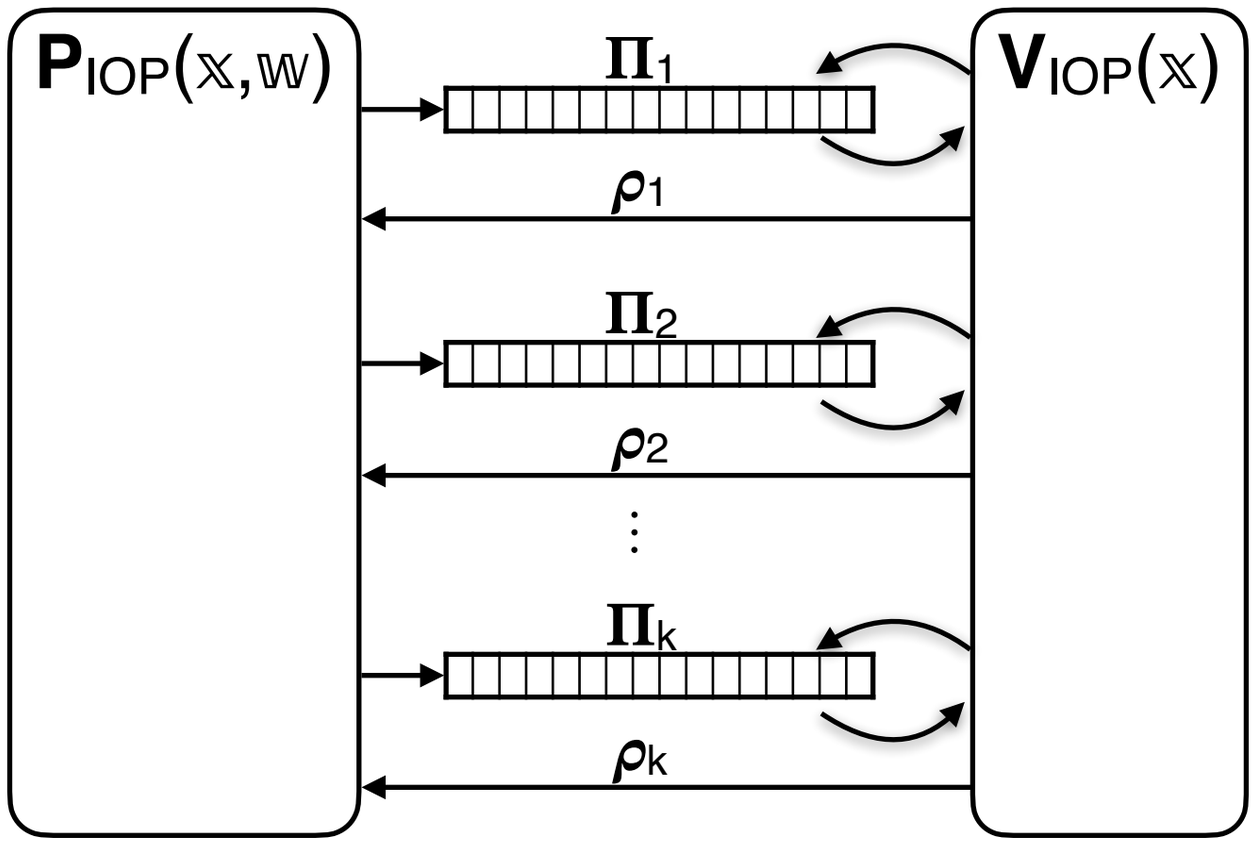

f
$\mathcal{P}(\mathbb{x},\mathbb{w})$
$\mathcal{V}(\mathbb{x})$

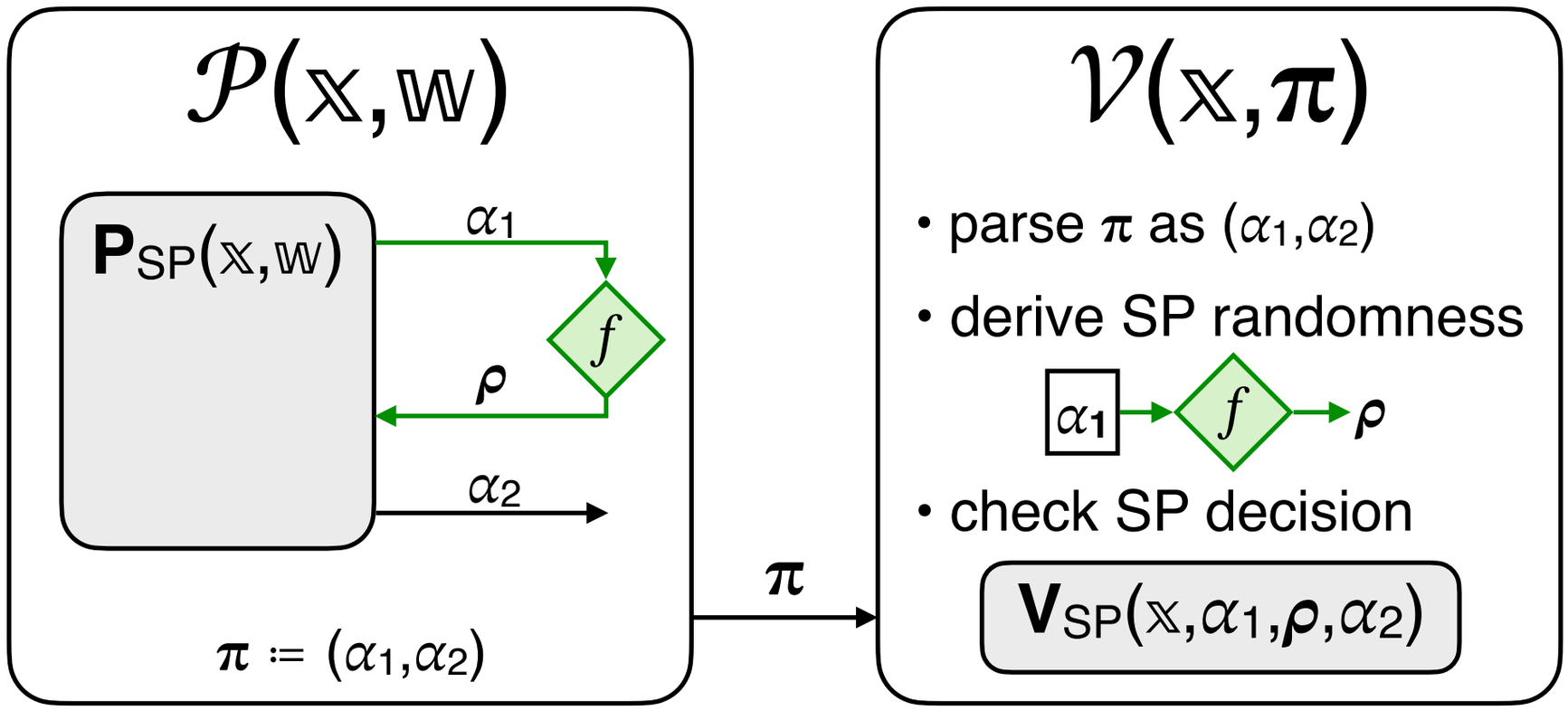

f
$\mathcal{P}(\mathbb{x},\mathbb{w})$
$\boldsymbol{\pi}$
$\mathcal{V}(\mathbb{x},\boldsymbol{\pi})$

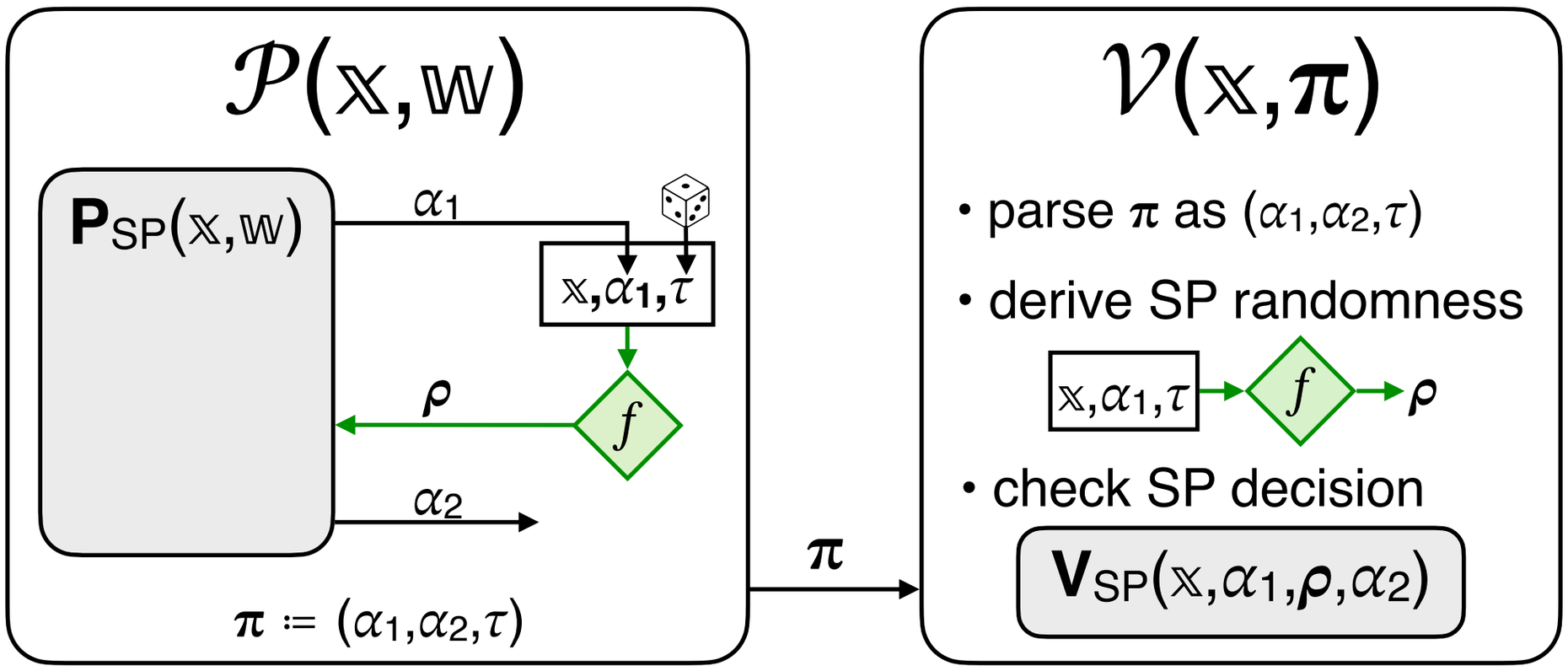

$\mathbf{P}_{SP}(\mathbb{x},\mathbb{w})$
$\mathbf{V}_{SP}(\mathbb{x})$
α_1
ρ
α_2


$\mathbf{P}_{\mathsf{IP}}(\mathbb{x},\mathbb{w})$
$\mathbf{V}_{\mathsf{IP}}(\mathbb{x})$
α_1
ρ_1
α_2
ρ_2
α_k
ρ_k

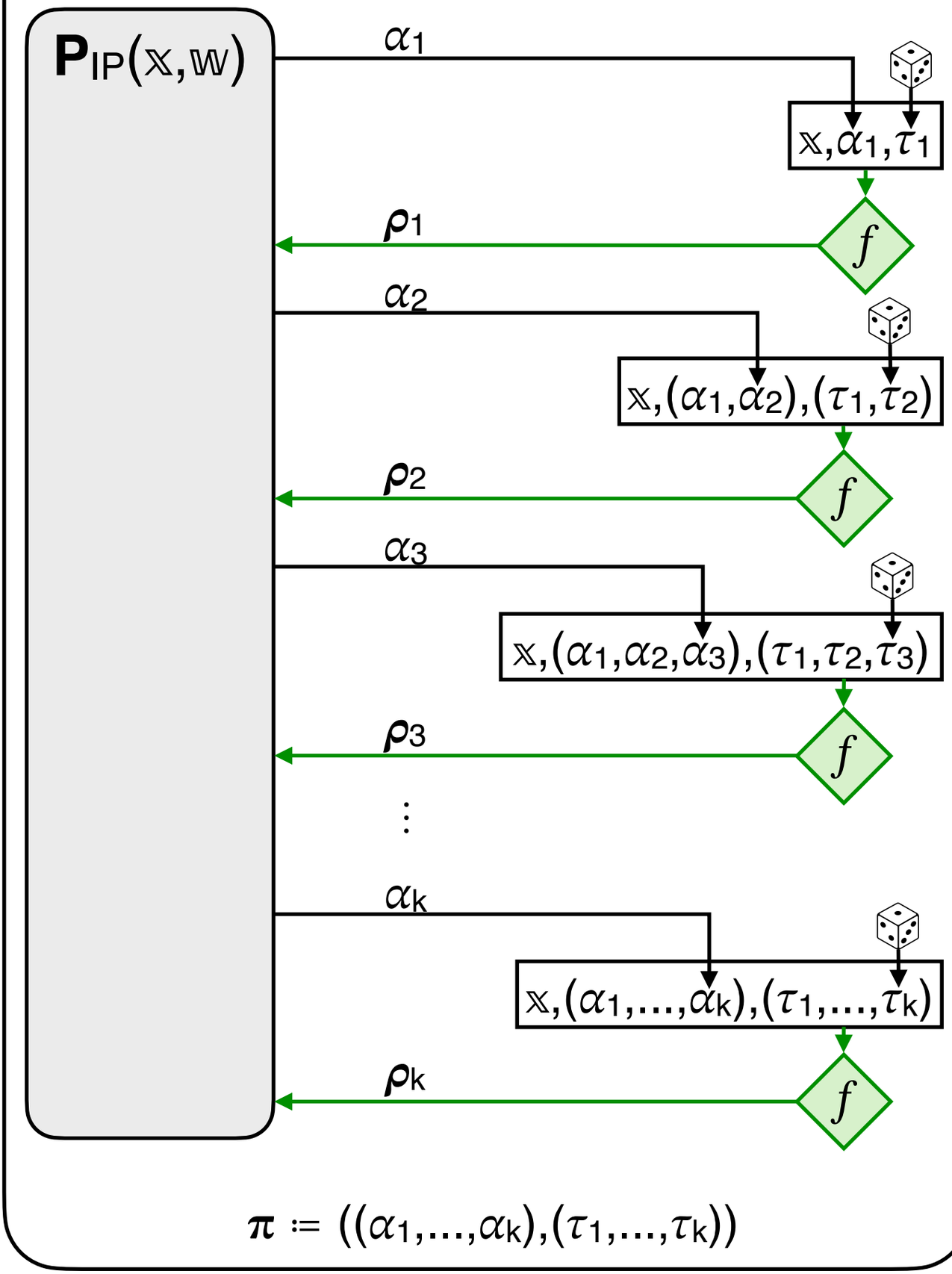

$\mathbf{P}_{\mathsf{PCP}}(\mathbb{x},\mathbb{w})$
$\boldsymbol{\Pi}$
$\mathbf{V}_{\mathsf{PCP}}(\mathbb{x})$


$\mathbf{P}_{\mathsf{IOP}}(\mathbb{x},\mathbb{w})$
$\mathbf{V}_{\mathsf{IOP}}(\mathbb{x})$
Π_1
ρ_1
Π_2
ρ_2
Π_k
ρ_k


$\mathcal{P}(\mathbb{x},\mathbb{w})$
$\mathbf{P}_{SP}(\mathbb{x},\mathbb{w})$
α_1
f
ρ
α_2
$\boldsymbol{\pi} := (\alpha_1,\alpha_2)$
$\boldsymbol{\pi}$
$\mathcal{V}(\mathbb{x},\boldsymbol{\pi})$
• parse $\boldsymbol{\pi}$ as (α_1,α_2)
• derive SP randomness
α_1
f
ρ
• check SP decision
$\mathbf{V}_{SP}(\mathbb{x},\alpha_1,\boldsymbol{\rho},\alpha_2)$


$\mathcal{P}(\mathbb{x},\mathbb{W})$
$\mathbf{P}_{SP}(\mathbb{x},\mathbb{W})$
α_1
$\mathbb{x},\alpha_1,\tau$
f
ρ
α_2
$\pi := (\alpha_1,\alpha_2,\tau)$
π
$\mathcal{V}(\mathbb{x},\pi)$
• parse π as (α_1,α_2,τ)
• derive SP randomness
$\mathbb{x},\alpha_1,\tau$
f
ρ
• check SP decision
$\mathbf{V}_{SP}(\mathbb{x},\alpha_1,\rho,\alpha_2)$

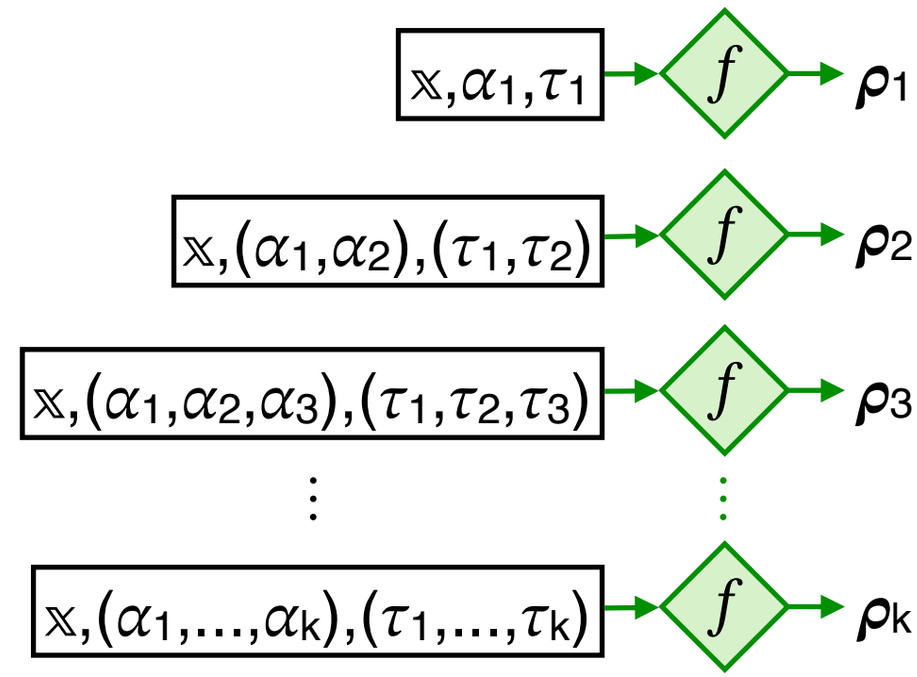
$\mathcal{P}(\mathbb{x},\mathbb{w})$



π

$\mathcal{V}(\mathbb{x},\pi)$

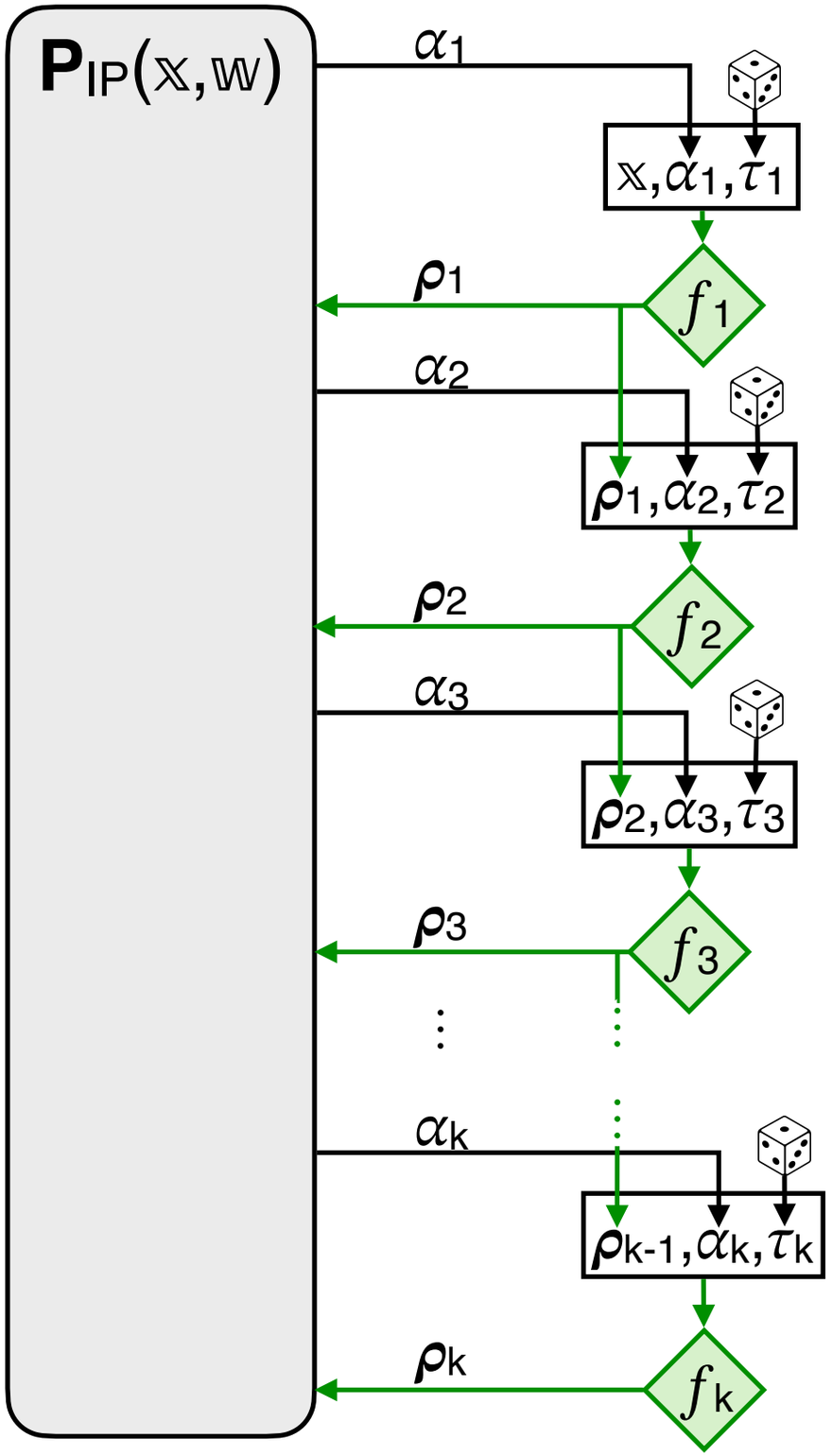
- parse π as $((\alpha_1,\ldots,\alpha_k),(\tau_1,\ldots,\tau_k))$
- derive IP randomness



- check IP decision

$\mathbf{V}_{\mathrm{IP}}(\mathbb{x},(\alpha_1,\ldots,\alpha_k),(\rho_1,\ldots,\rho_k))$

$\mathcal{P}(\mathbb{x},\mathbb{W})$

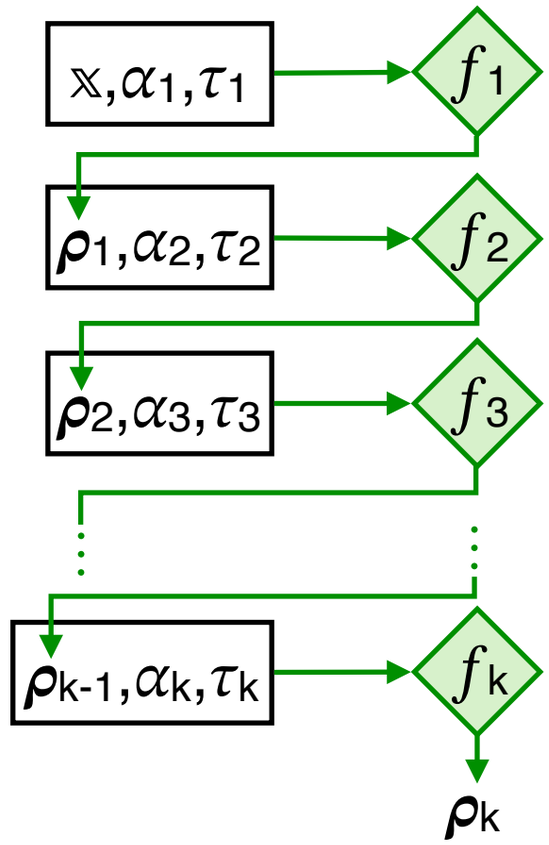


$\pi := ((\alpha_1,\ldots,\alpha_k),(\tau_1,\ldots,\tau_k))$

π

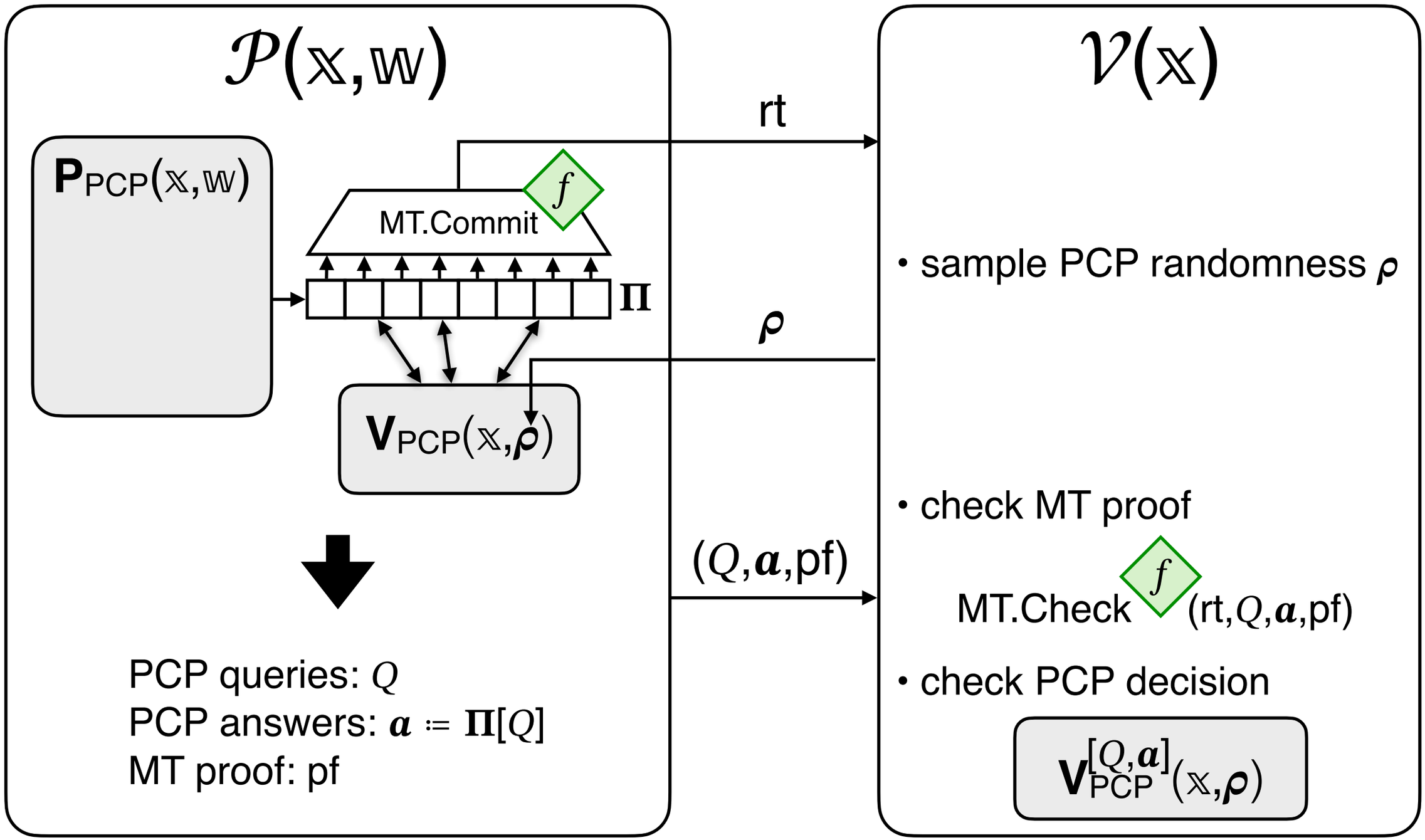
$\mathcal{V}(\mathbb{x},\pi)$

- parse π as $((\alpha_1,\ldots,\alpha_k),(\tau_1,\ldots,\tau_k))$
- derive IP randomness

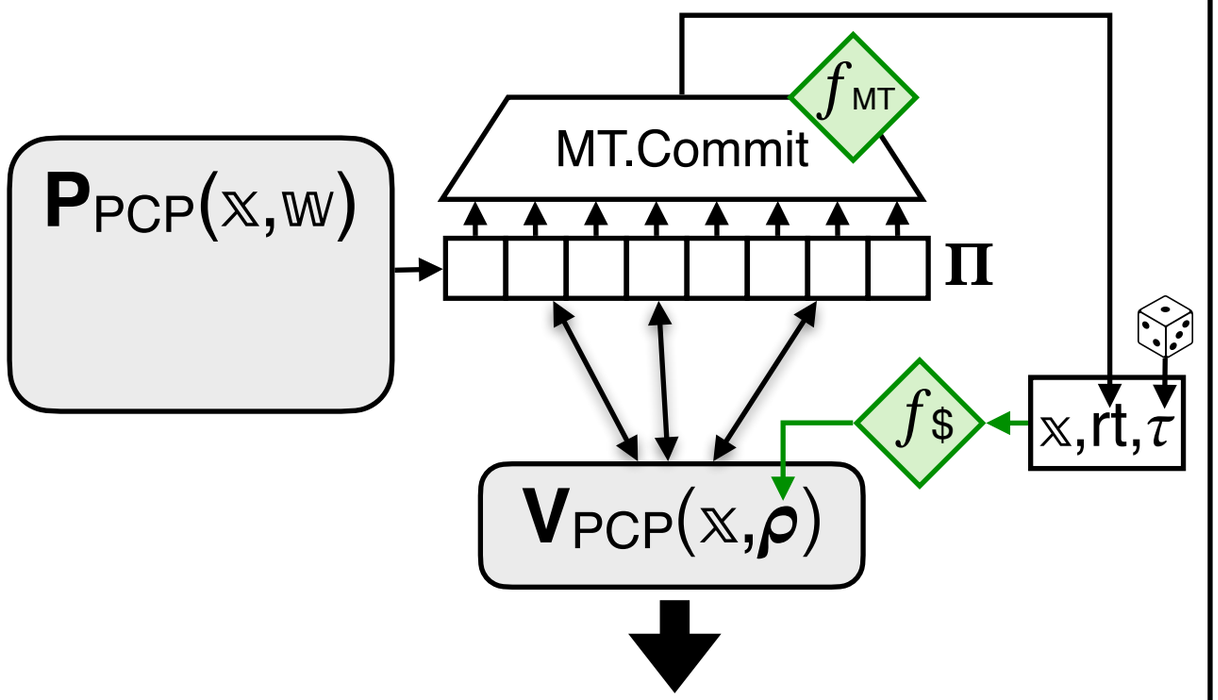


- check IP decision

$\mathbf{V}_{IP}(\mathbb{x},(\alpha_1,\ldots,\alpha_k),(\rho_1,\ldots,\rho_k))$


$\mathcal{P}(\mathbb{x},\mathbb{w})$
$\mathcal{V}(\mathbb{x})$
$\mathbf{P}_{\mathrm{PCP}}(\mathbb{x},\mathbb{w})$
f
MT.Commit
$\boldsymbol{\Pi}$
rt
$\boldsymbol{\rho}$
$\mathbf{V}_{\mathrm{PCP}}(\mathbb{x},\boldsymbol{\rho})$
PCP queries: Q
PCP answers: $\boldsymbol{a} \coloneqq \boldsymbol{\Pi}[Q]$
MT proof: pf
$(Q,\boldsymbol{a},\mathrm{pf})$
• sample PCP randomness $\boldsymbol{\rho}$
• check MT proof
MT.Check f (rt,Q,$\boldsymbol{a}$,pf)
• check PCP decision
$\mathbf{V}_{\mathrm{PCP}}^{[Q,\boldsymbol{a}]}(\mathbb{x},\boldsymbol{\rho})$

$\mathcal{P}(\mathbb{x},\mathbb{w})$



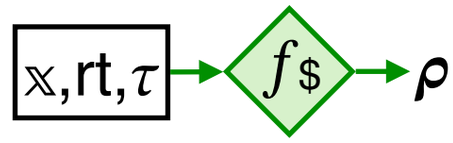
PCP queries: Q
PCP answers: $\boldsymbol{a} \coloneqq \boldsymbol{\Pi}[Q]$
MT proof: pf

$\boldsymbol{\pi} \coloneqq$ (rt,Q,$\boldsymbol{a}$,pf,τ)

$\boldsymbol{\pi}$

$\mathcal{V}(\mathbb{x},\boldsymbol{\pi})$

- parse $\boldsymbol{\pi}$ as (rt,Q,$\boldsymbol{a}$,pf,τ)
- derive PCP randomness



- check MT proof

MT.Check f_{MT} (rt,Q,$\boldsymbol{a}$,pf)

- check PCP decision

$\mathbf{V}_{\text{PCP}}^{[Q,\boldsymbol{a}]}(\mathbb{x},\boldsymbol{\rho})$

$\mathcal{P}(\mathbb{x},\mathbb{W})$

$\mathcal{V}(\mathbb{x})$

$\mathbf{P}_{\mathsf{IOP}}(\mathbb{x},\mathbb{W})$

rt_1

MT.Commit f

$\boldsymbol{\Pi}_1$

$\boldsymbol{\rho}_1$

- sample IOP randomness $\boldsymbol{\rho}_1$

rt_2

MT.Commit f

$\boldsymbol{\Pi}_2$

$\boldsymbol{\rho}_2$

- sample IOP randomness $\boldsymbol{\rho}_2$

rt_k

MT.Commit f

$\boldsymbol{\Pi}_k$

$\boldsymbol{\rho}_k$

- sample IOP randomness $\boldsymbol{\rho}_k$
- check MT proofs

$\wedge_{i\in[k]}$ MT.Check$^{f}(\mathsf{rt}_i,Q_i,\boldsymbol{a}_i,\mathsf{pf}_i)$

- check IOP decision

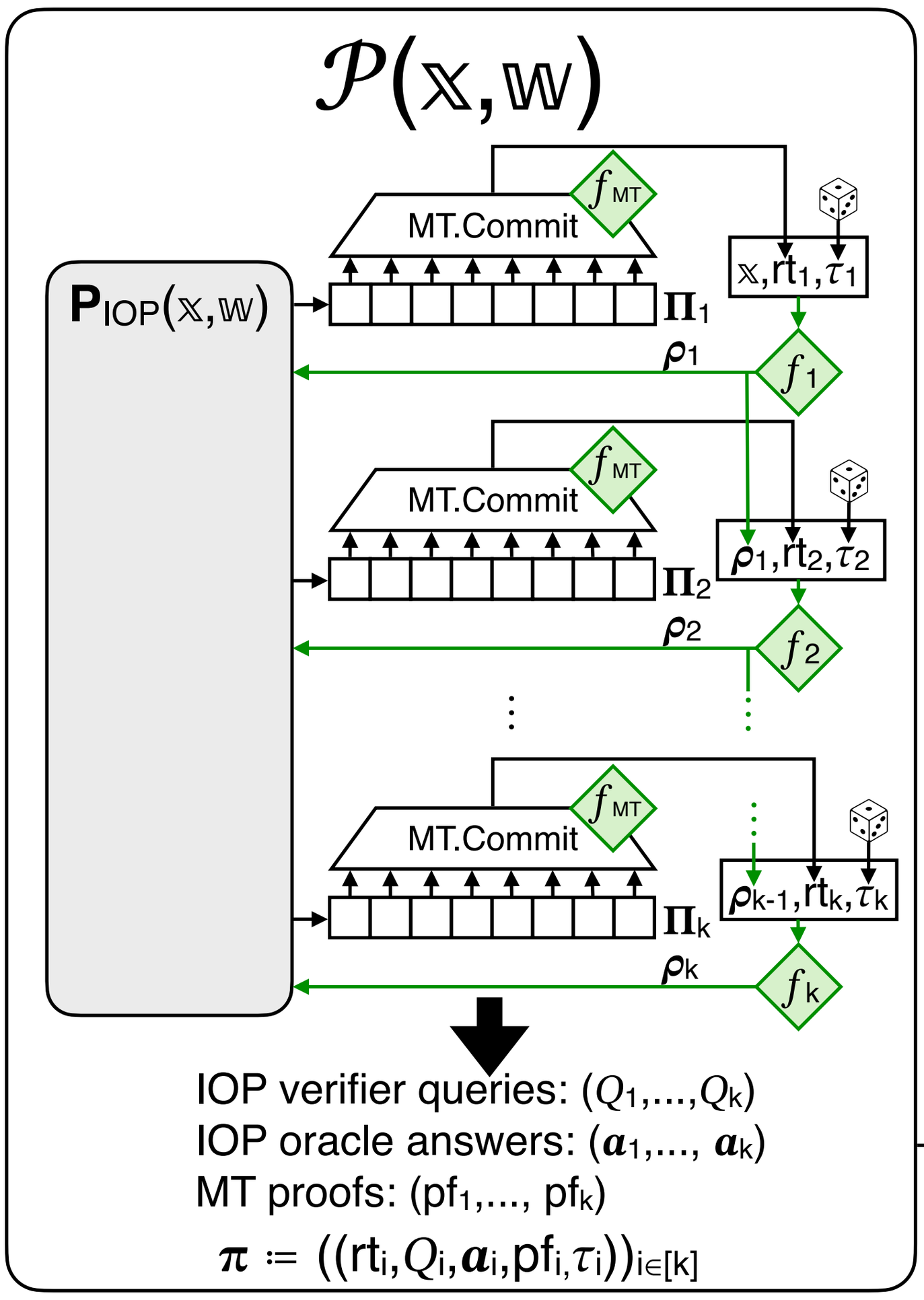
$((Q_i,\boldsymbol{a}_i,\mathsf{pf}_i))_{i\in[k]}$

IOP verifier queries: $(Q_1,...,Q_k)$

IOP oracle answers: $(\boldsymbol{a}_1,...,\boldsymbol{a}_k)$

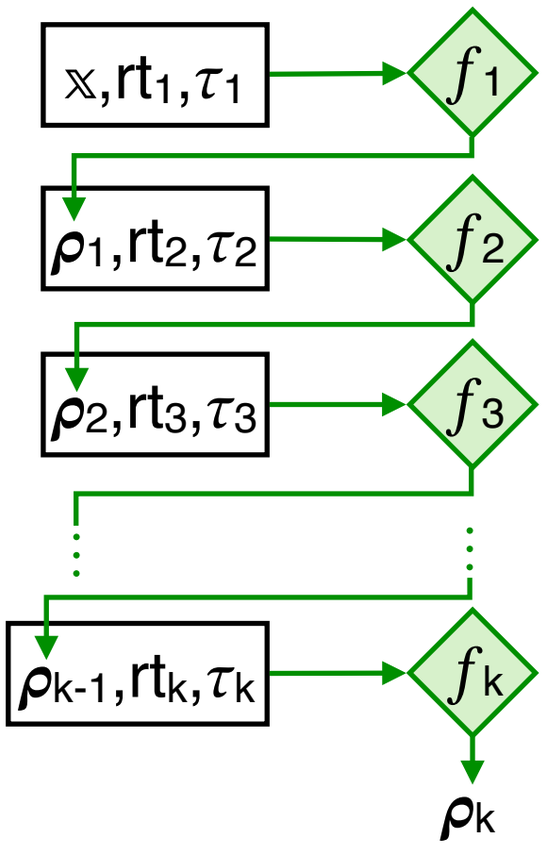
MT proofs: $(\mathsf{pf}_1,...,\mathsf{pf}_k)$

$\mathbf{V}_{\mathsf{IOP}}^{[Q_i,\boldsymbol{a}_i]_{i\in[k]}}(\mathbb{x},(\boldsymbol{\rho}_1,\ldots,\boldsymbol{\rho}_k))$



$\mathcal{V}(\mathbb{x},\boldsymbol{\pi})$

- parse $\boldsymbol{\pi}$ as $((\mathsf{rt}_i,Q_i,\boldsymbol{a}_i,\mathsf{pf}_i,\tau_i))_{i\in[k]}$
- derive IOP randomness

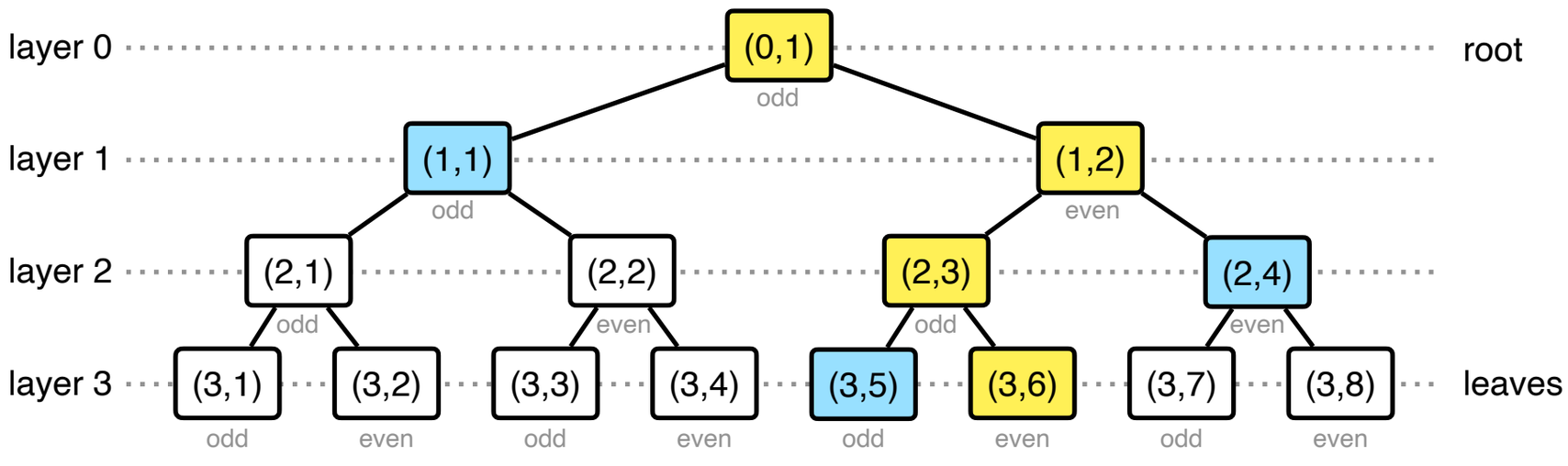


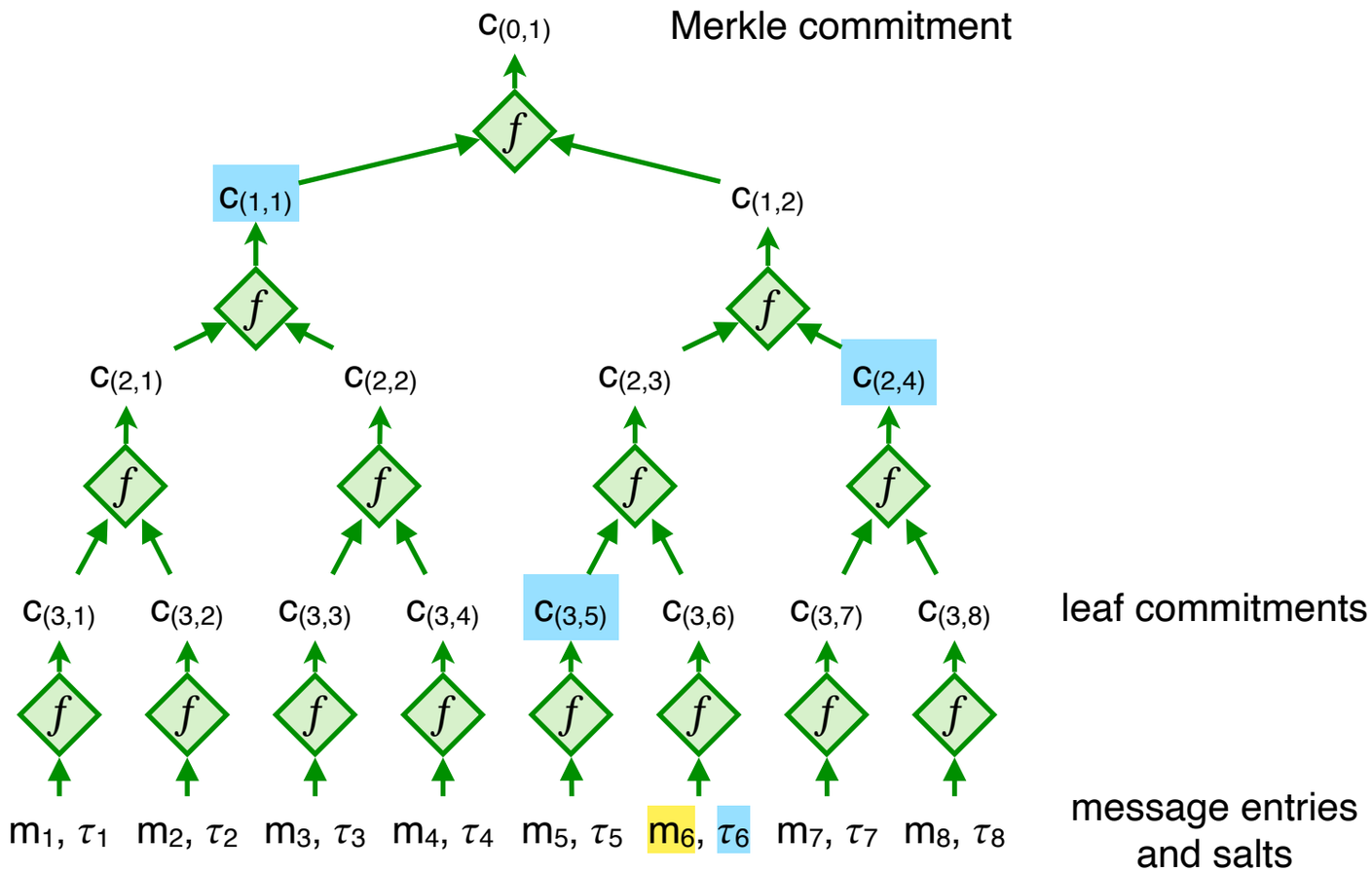
- check MT proofs

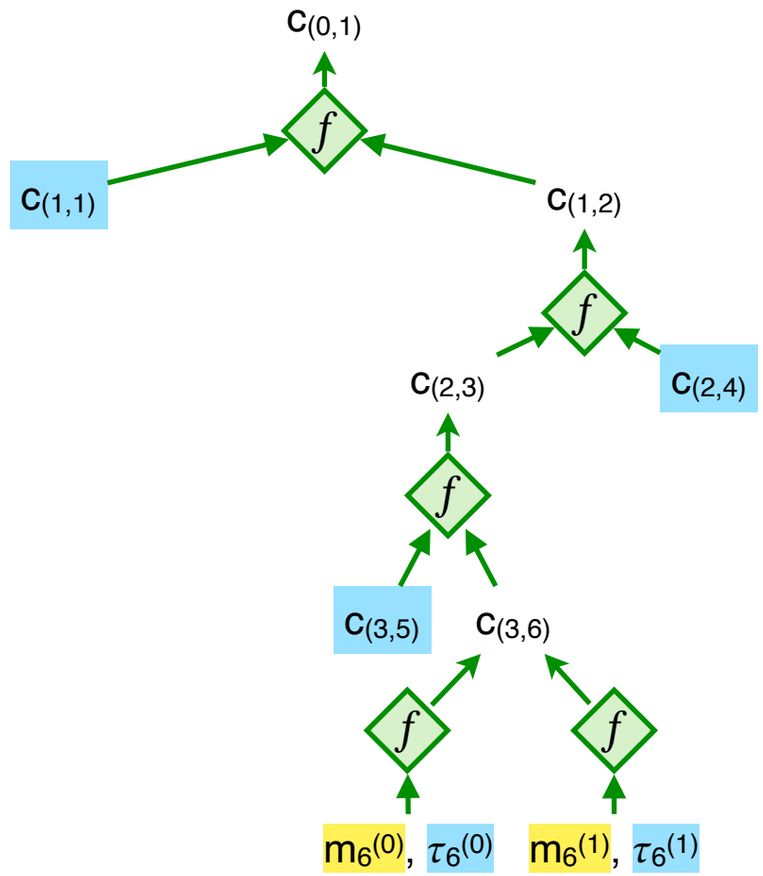
$\wedge_{i\in[k]}$ MT.Check$^{f_{\mathsf{MT}}}(\mathsf{rt}_i,Q_i,\boldsymbol{a}_i,\mathsf{pf}_i)$

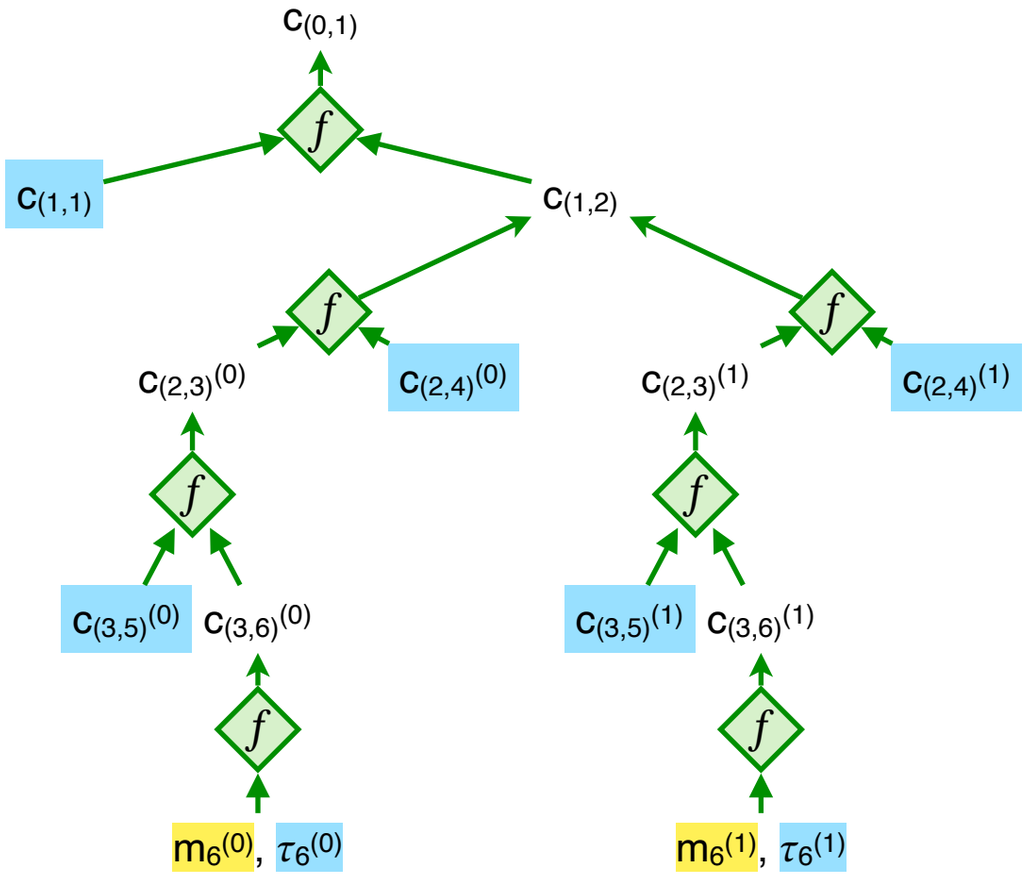
- check IOP decision

$\mathbf{V}_{\mathsf{IOP}}^{[Q_i,\boldsymbol{a}_i]_{i\in[k]}}(\mathbb{x},(\boldsymbol{\rho}_1,\ldots,\boldsymbol{\rho}_k))$

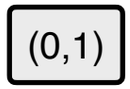

layer 0
layer 1
layer 2
layer 3
root
leaves
(0,1)
odd
(1,1)
odd
(1,2)
even
(2,1)
odd
(2,2)
even
(2,3)
odd
(2,4)
even
(3,1)
odd
(3,2)
even
(3,3)
odd
(3,4)
even
(3,5)
odd
(3,6)
even
(3,7)
odd
(3,8)
even


$c_{(0,1)}$
Merkle commitment
$c_{(1,1)}$
$c_{(1,2)}$
$c_{(2,1)}$
$c_{(2,2)}$
$c_{(2,3)}$
$c_{(2,4)}$
$c_{(3,1)}$
$c_{(3,2)}$
$c_{(3,3)}$
$c_{(3,4)}$
$c_{(3,5)}$
$c_{(3,6)}$
$c_{(3,7)}$
$c_{(3,8)}$
leaf commitments
m_1, τ_1
m_2, τ_2
m_3, τ_3
m_4, τ_4
m_5, τ_5
m_6, τ_6
m_7, τ_7
m_8, τ_8
message entries
and salts

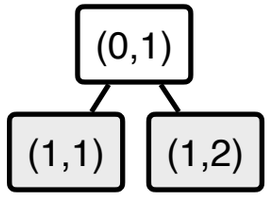

C(0,1)
f
C(1,1)
C(1,2)
f
C(2,3)
C(2,4)
f
C(3,5)
C(3,6)
f
f
m6(0), τ6(0)
m6(1), τ6(1)


C(0,1)
f
C(1,1)
C(1,2)
f
f
C(2,3)(0)
C(2,4)(0)
C(2,3)(1)
C(2,4)(1)
f
f
C(3,5)(0)
C(3,6)(0)
C(3,5)(1)
C(3,6)(1)
f
f
m6(0), τ6(0)
m6(1), τ6(1)

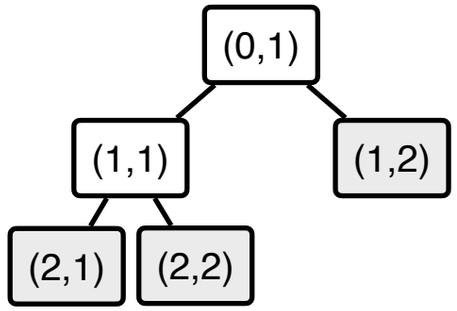
T_1



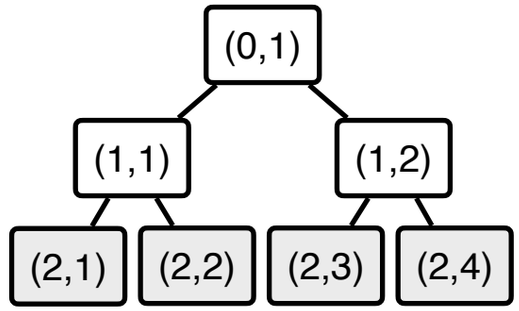
T_2



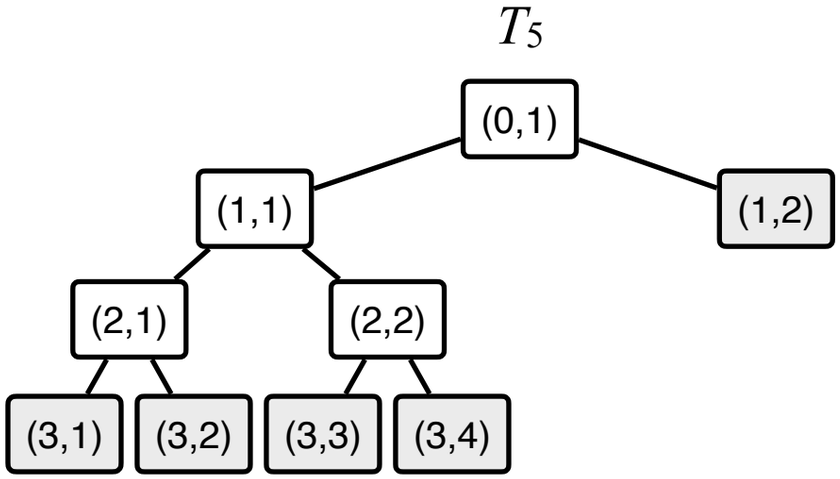
T_3



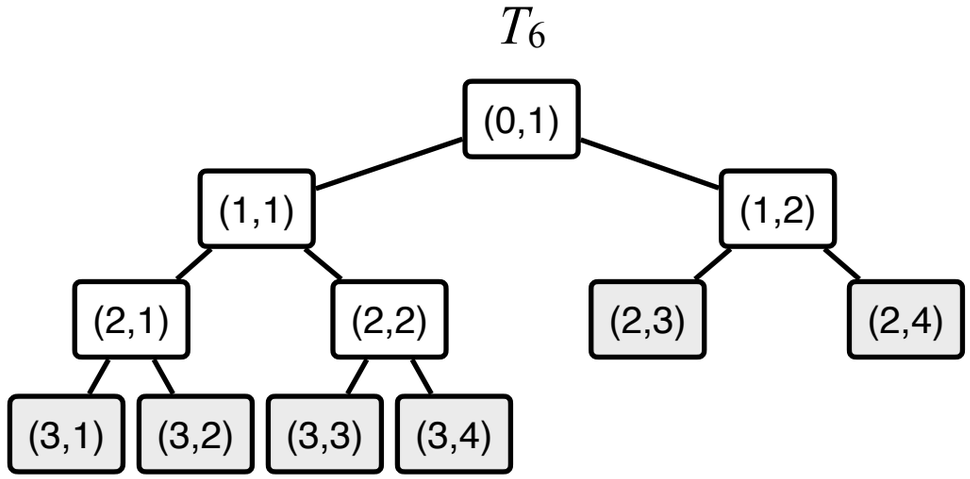
T_4



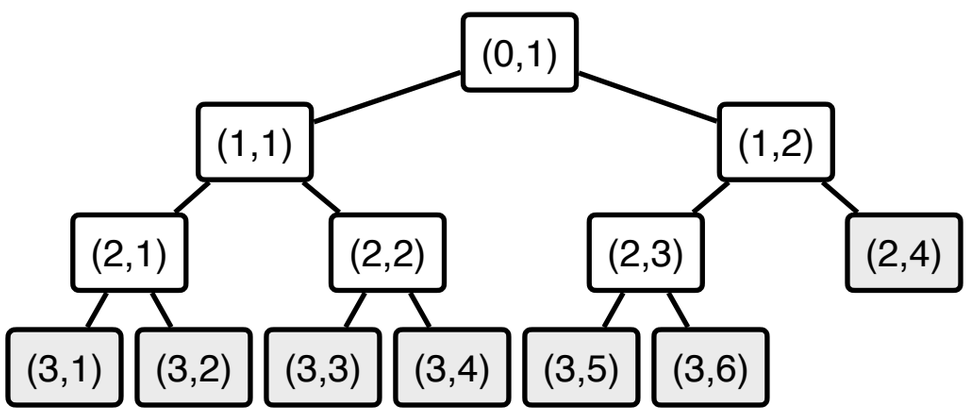
T_5



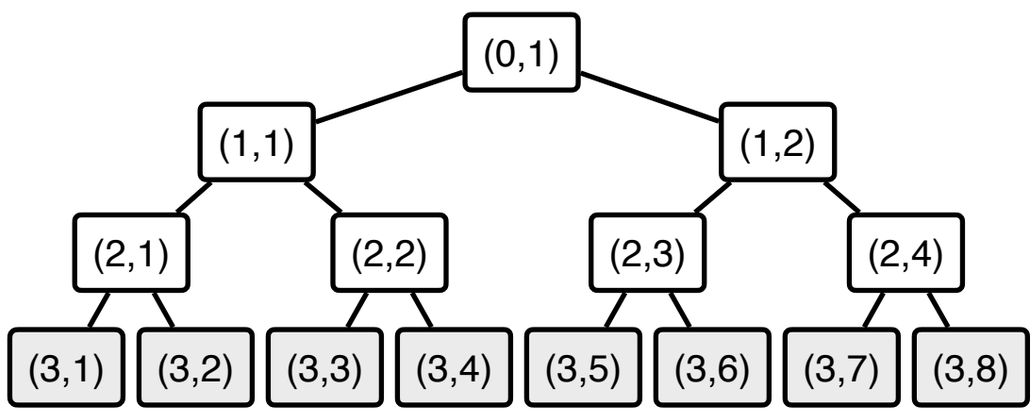
T_6

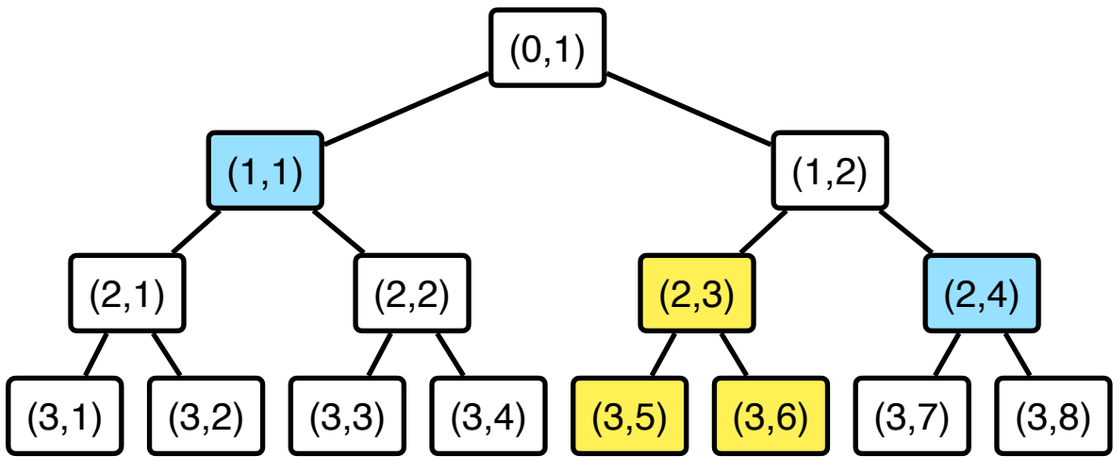


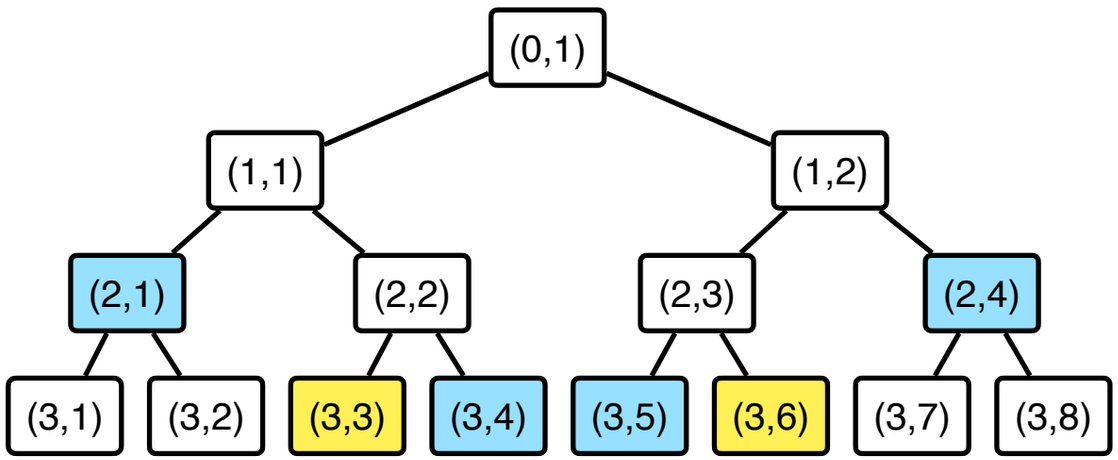
T_7

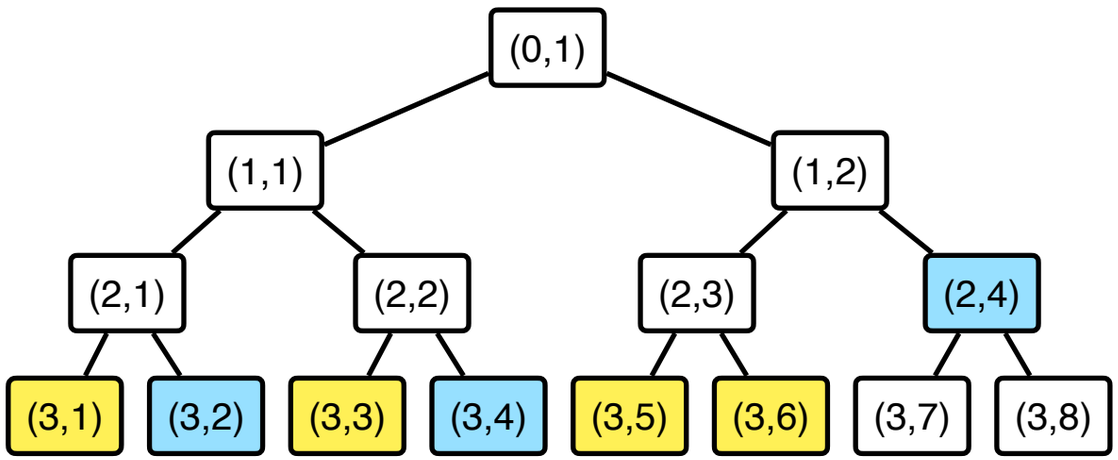


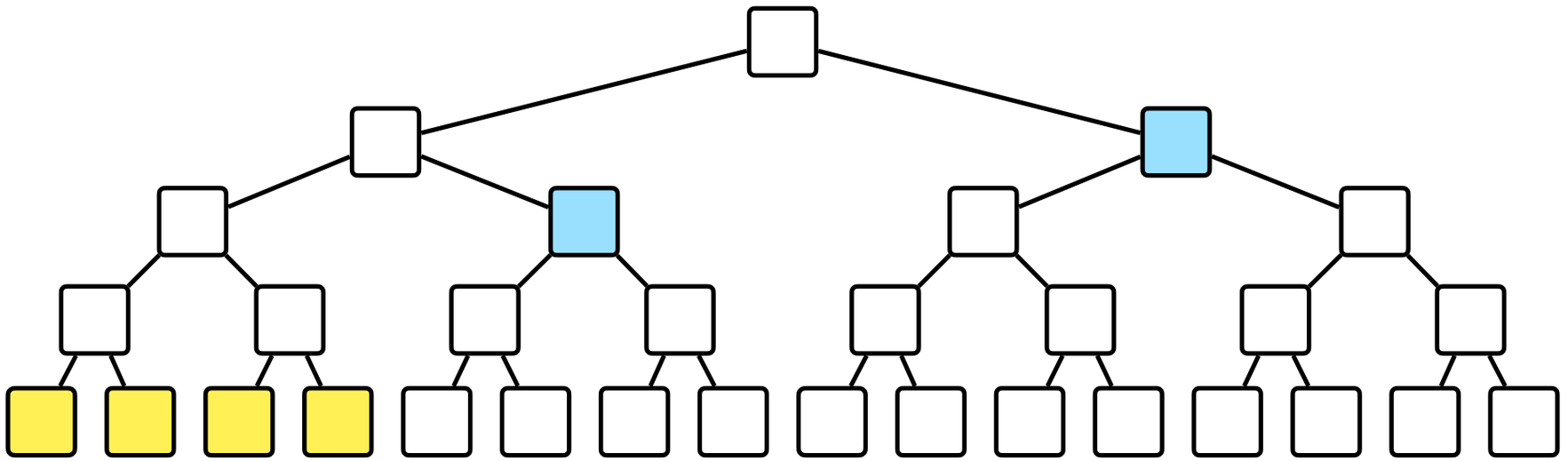
T_8

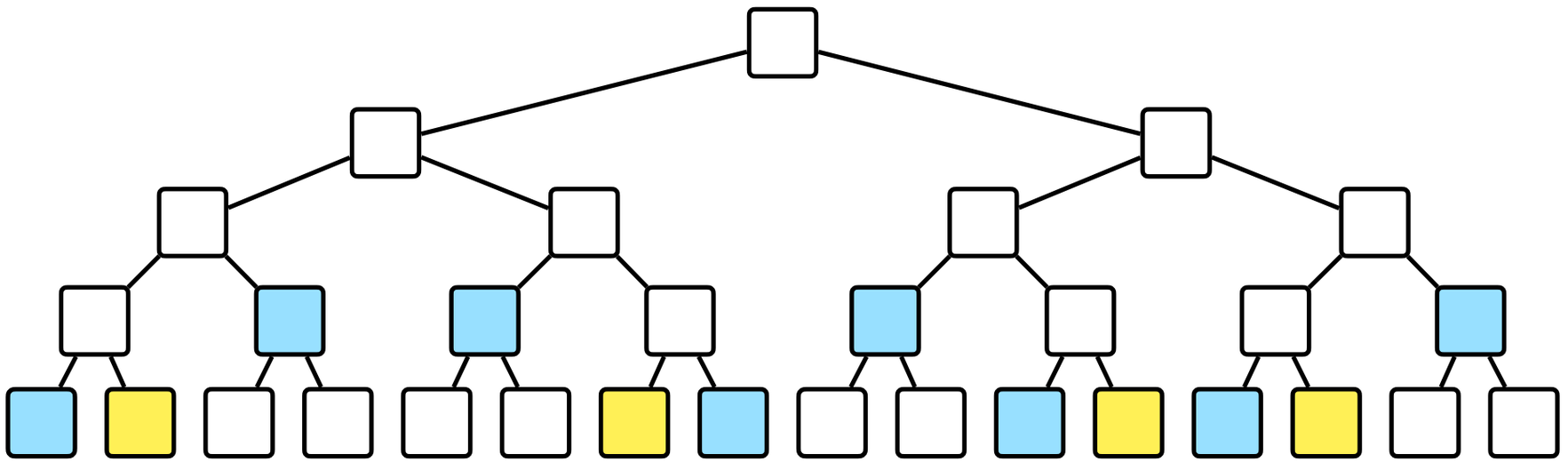


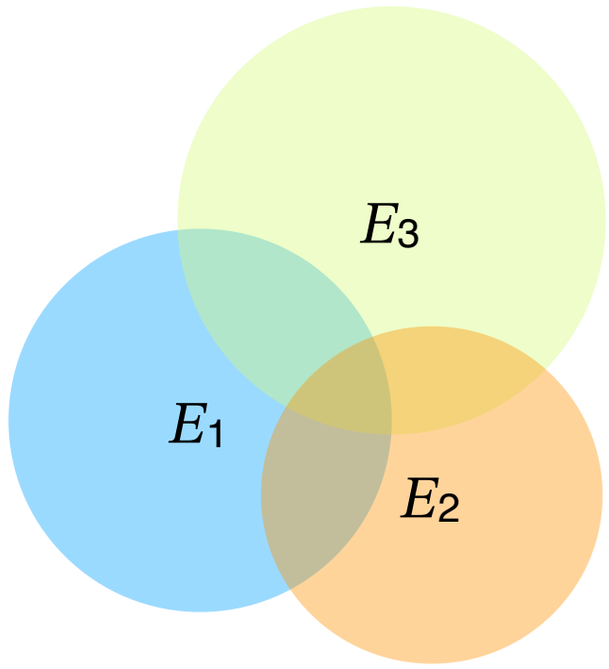

(0,1)
(1,1)
(1,2)
(2,1)
(2,2)
(2,3)
(2,4)
(3,1)
(3,2)
(3,3)
(3,4)
(3,5)
(3,6)
(3,7)
(3,8)

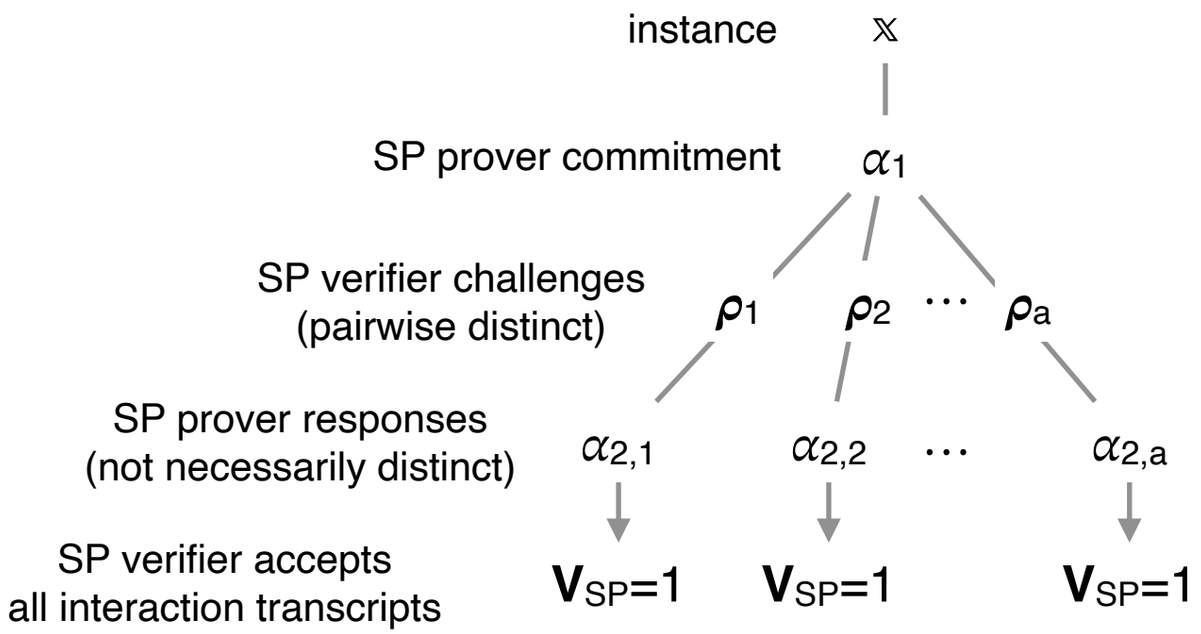

(0,1)
(1,1)
(1,2)
(2,1)
(2,2)
(2,3)
(2,4)
(3,1)
(3,2)
(3,3)
(3,4)
(3,5)
(3,6)
(3,7)
(3,8)

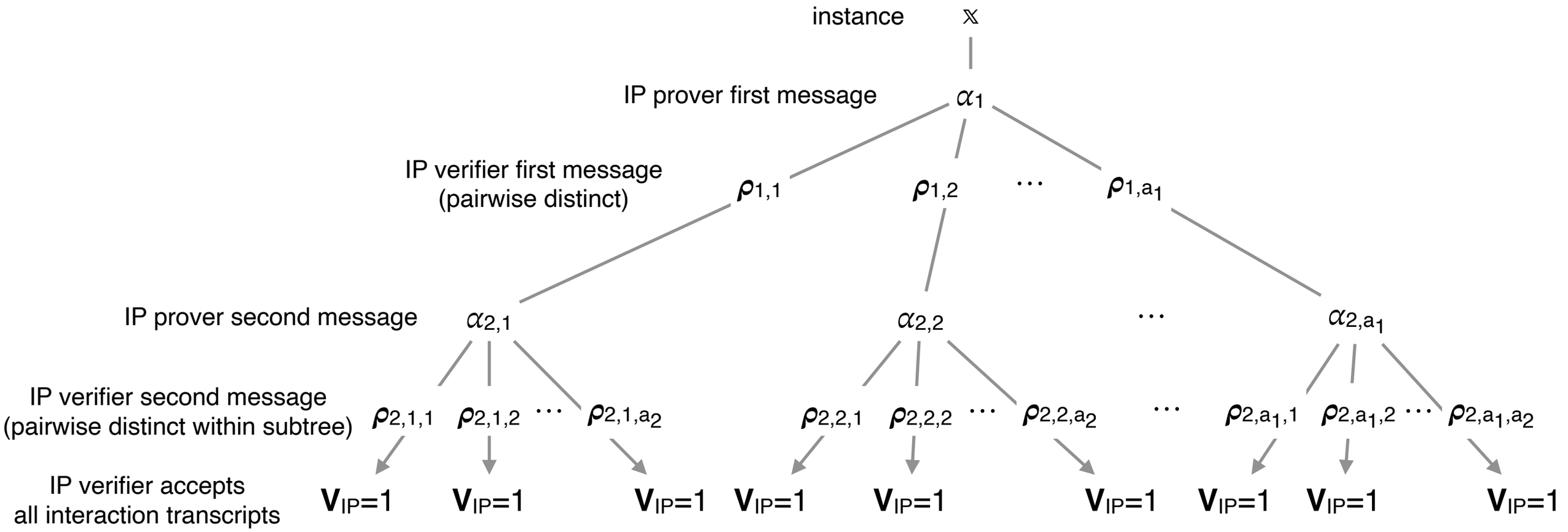

(0,1)
(1,1)
(1,2)
(2,1)
(2,2)
(2,3)
(2,4)
(3,1)
(3,2)
(3,3)
(3,4)
(3,5)
(3,6)
(3,7)
(3,8)

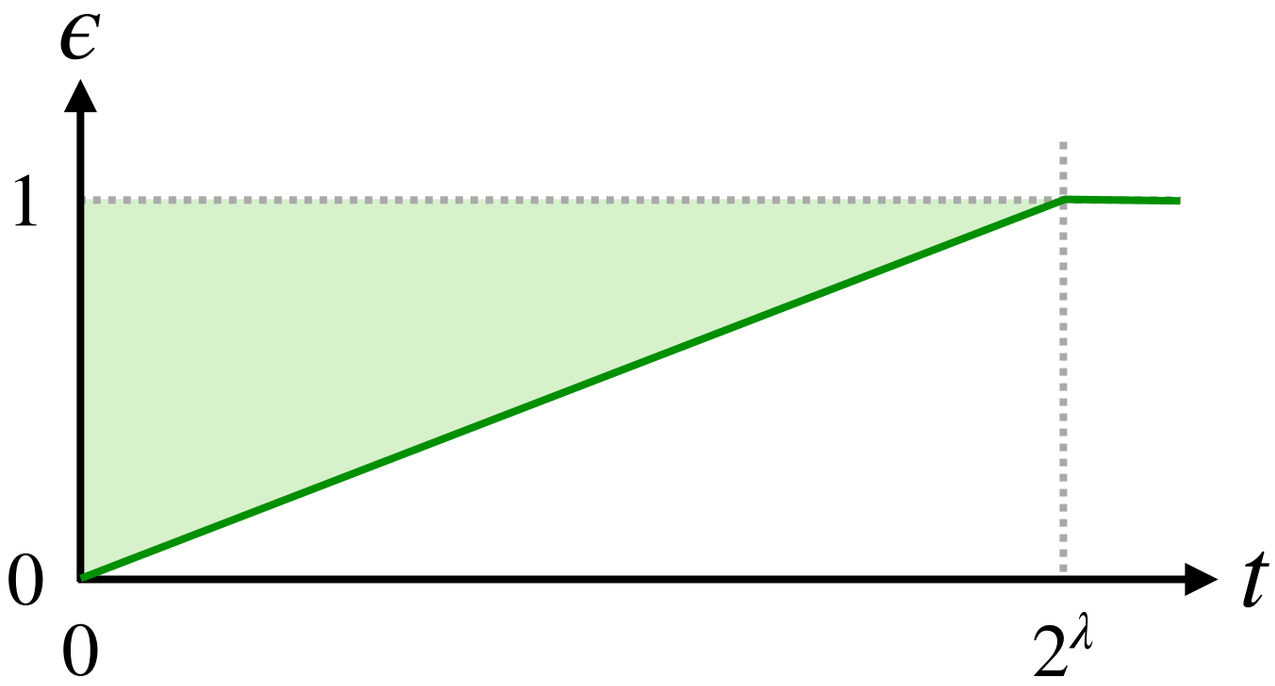


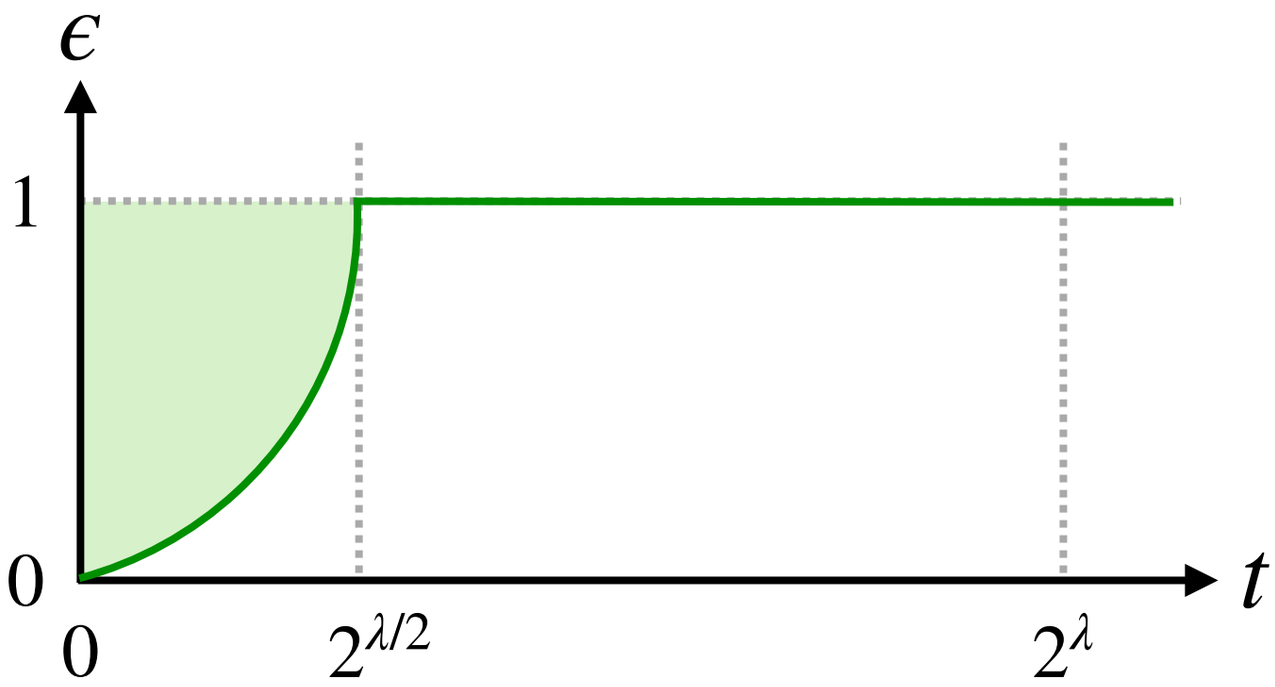


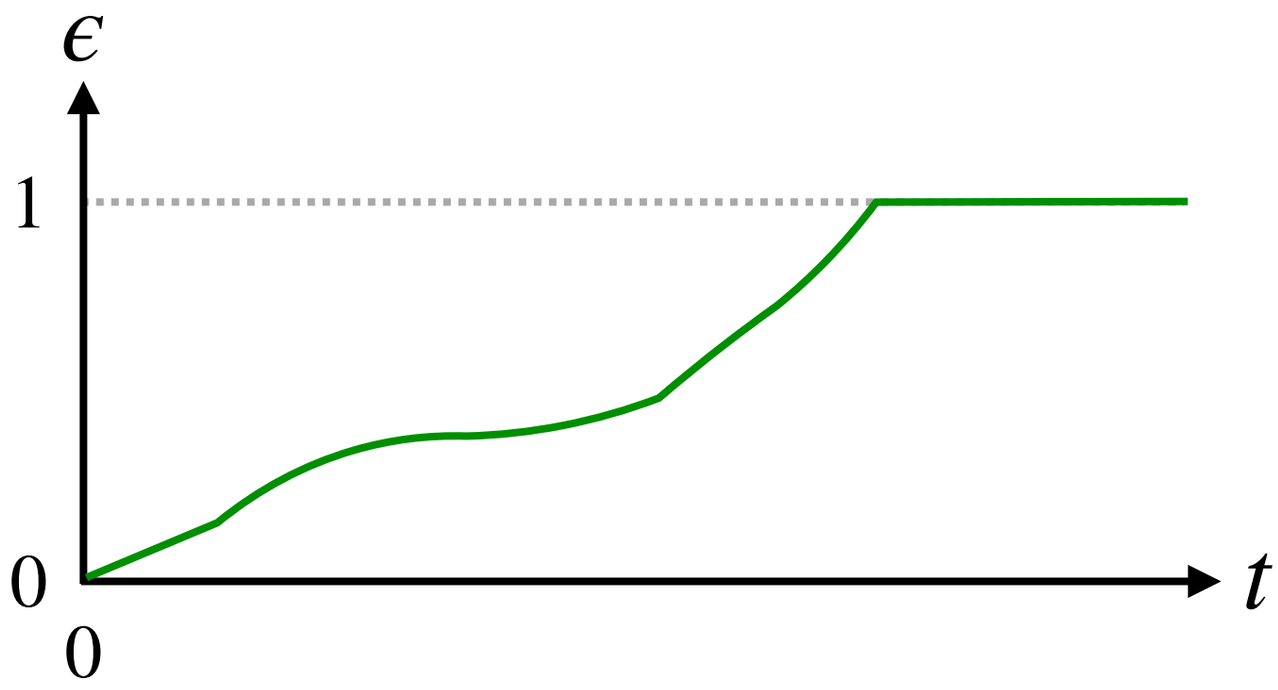

E_3
E_1
E_2

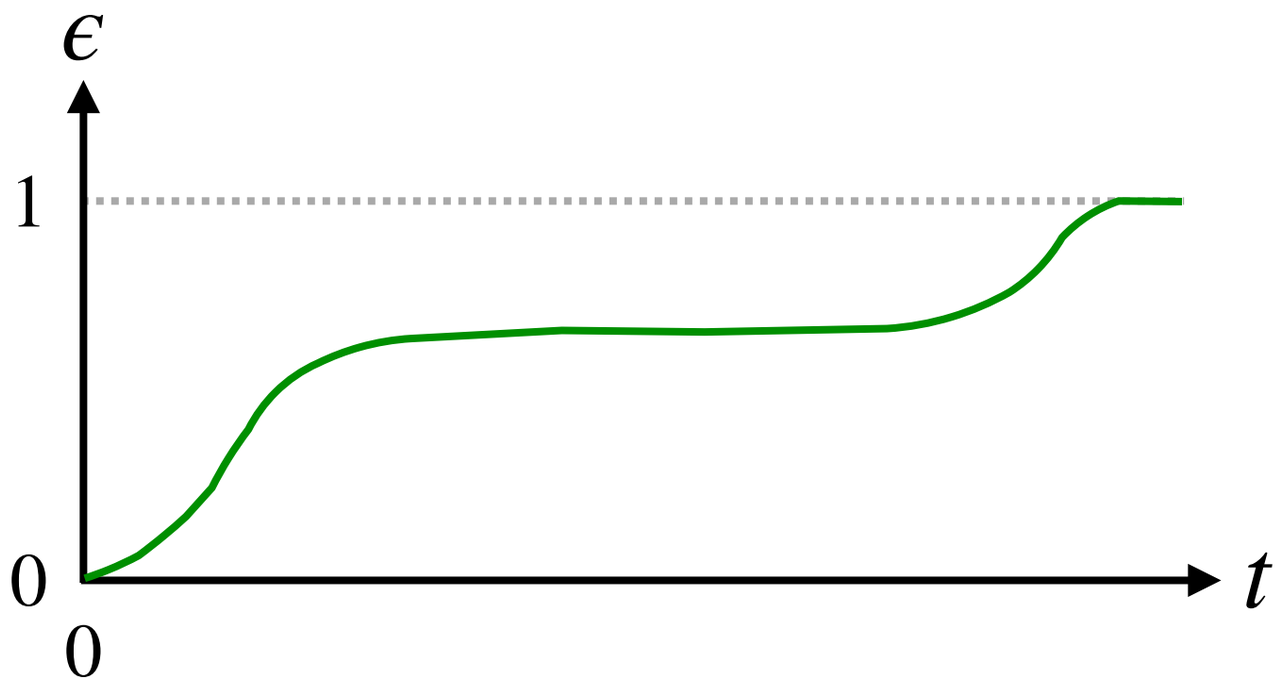

instance
𝕏
SP prover commitment
α_1
SP verifier challenges
(pairwise distinct)
ρ_1
ρ_2
$\cdots$
ρ_a
SP prover responses
(not necessarily distinct)
$\alpha_{2,1}$
$\alpha_{2,2}$
$\cdots$
$\alpha_{2,a}$
SP verifier accepts
all interaction transcripts
$\mathbf{V}_{SP}=1$
$\mathbf{V}_{SP}=1$
$\mathbf{V}_{SP}=1$

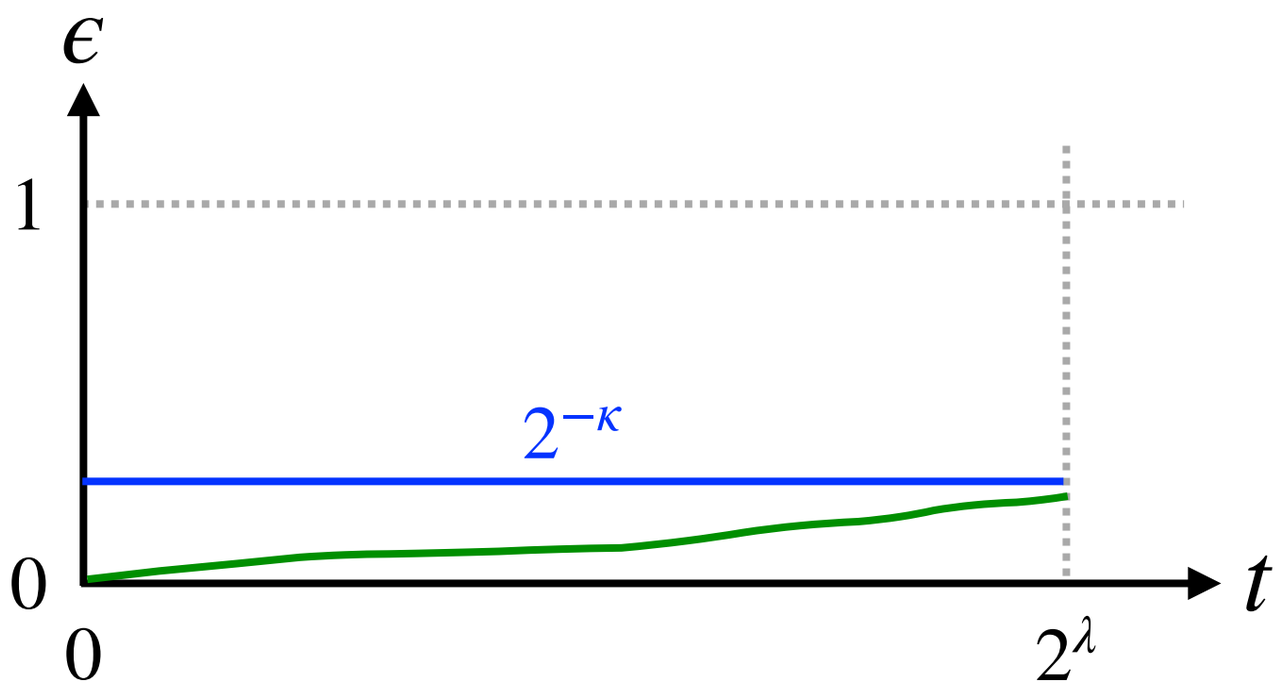

instance
$\mathbb{x}$
IP prover first message
α_1
IP verifier first message
(pairwise distinct)
$\rho_{1,1}$
$\rho_{1,2}$
$\cdots$
ρ_{1,a_1}
IP prover second message
$\alpha_{2,1}$
$\alpha_{2,2}$
$\cdots$
α_{2,a_1}
IP verifier second message
(pairwise distinct within subtree)
$\rho_{2,1,1}$
$\rho_{2,1,2}$
$\cdots$
$\rho_{2,1,a_2}$
$\rho_{2,2,1}$
$\rho_{2,2,2}$
$\cdots$
$\rho_{2,2,a_2}$
$\cdots$
$\rho_{2,a_1,1}$
$\rho_{2,a_1,2}$
$\cdots$
ρ_{2,a_1,a_2}
IP verifier accepts
all interaction transcripts
$\mathbf{V}_{IP}=1$
$\mathbf{V}_{IP}=1$
$\mathbf{V}_{IP}=1$
$\mathbf{V}_{IP}=1$
$\mathbf{V}_{IP}=1$
$\mathbf{V}_{IP}=1$
$\mathbf{V}_{IP}=1$
$\mathbf{V}_{IP}=1$
$\mathbf{V}_{IP}=1$

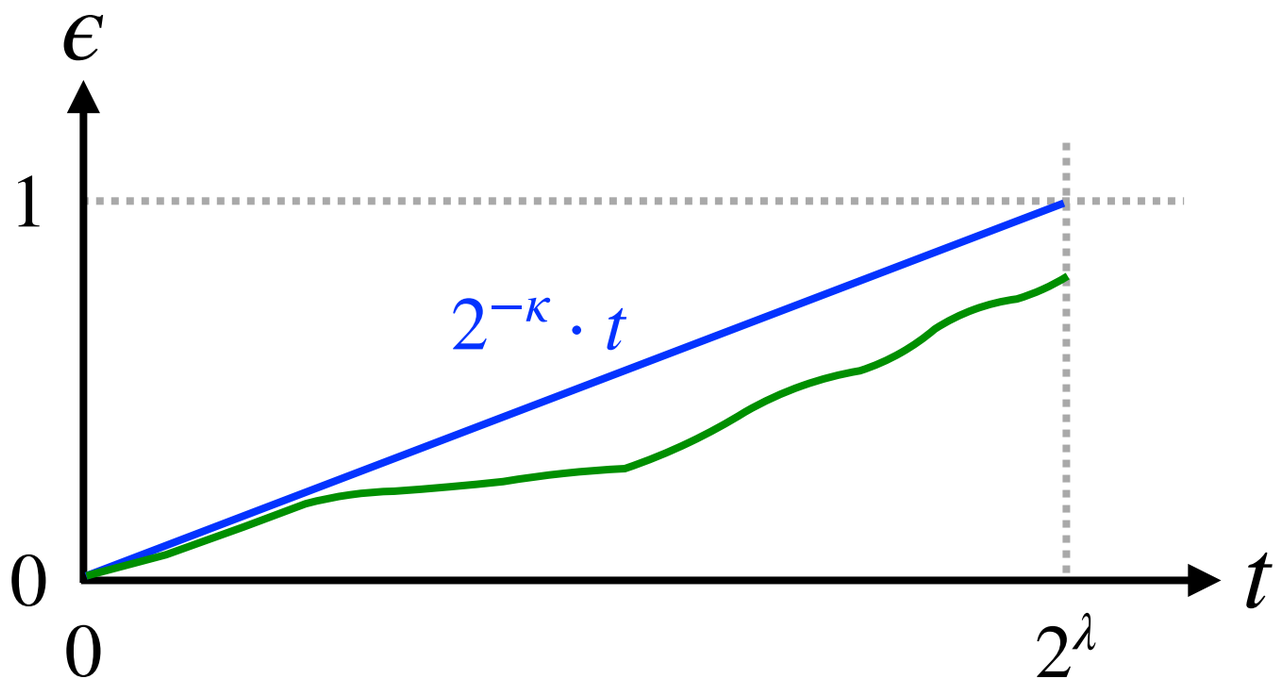

ϵ
1
0
0
2^{λ}
t

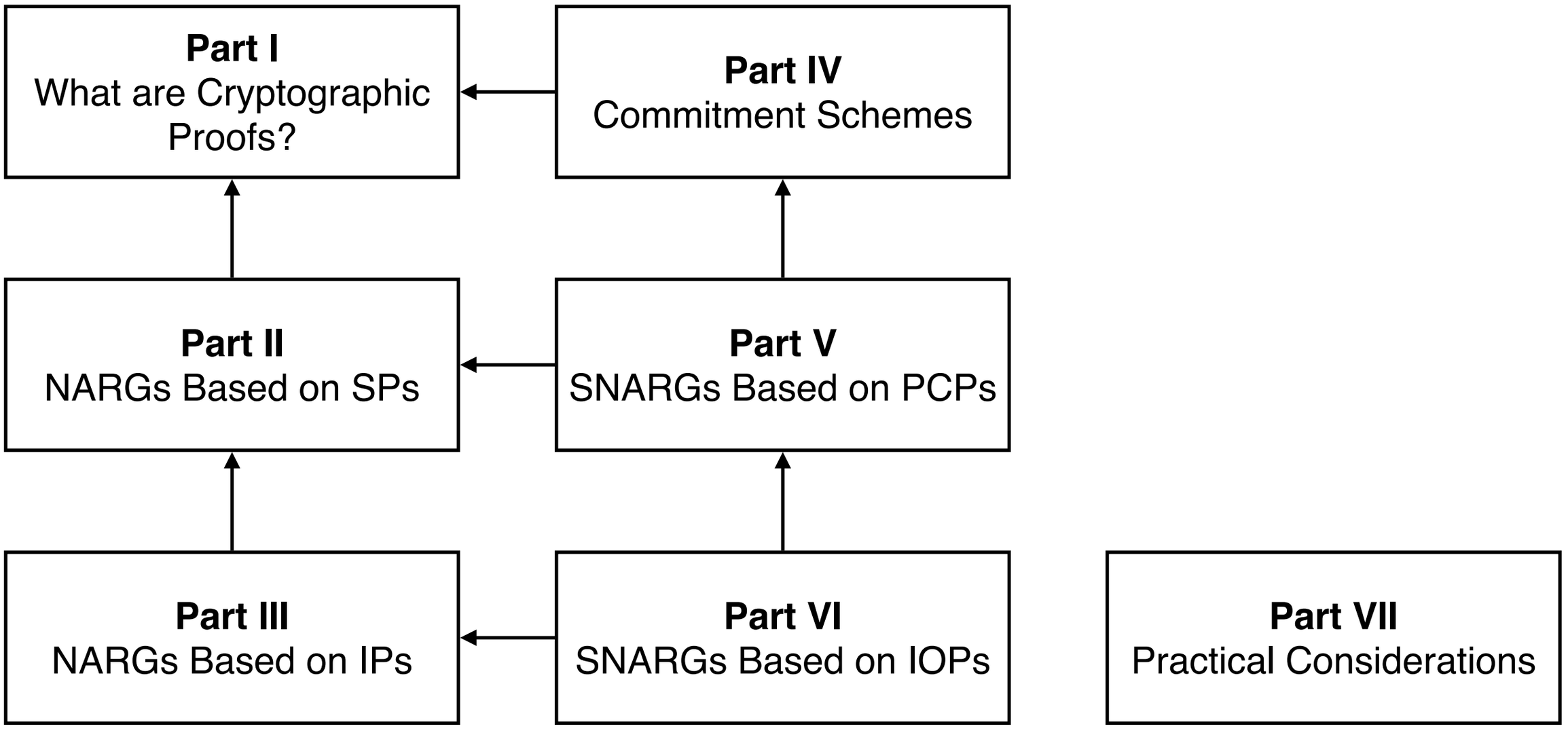

ϵ
1
0
0
$2^{\lambda/2}$
2^{λ}
t


ϵ
1
0
0
t


ϵ
1
0
0
t


ϵ
1
$2^{-\kappa}$
0
0
2^{λ}
t

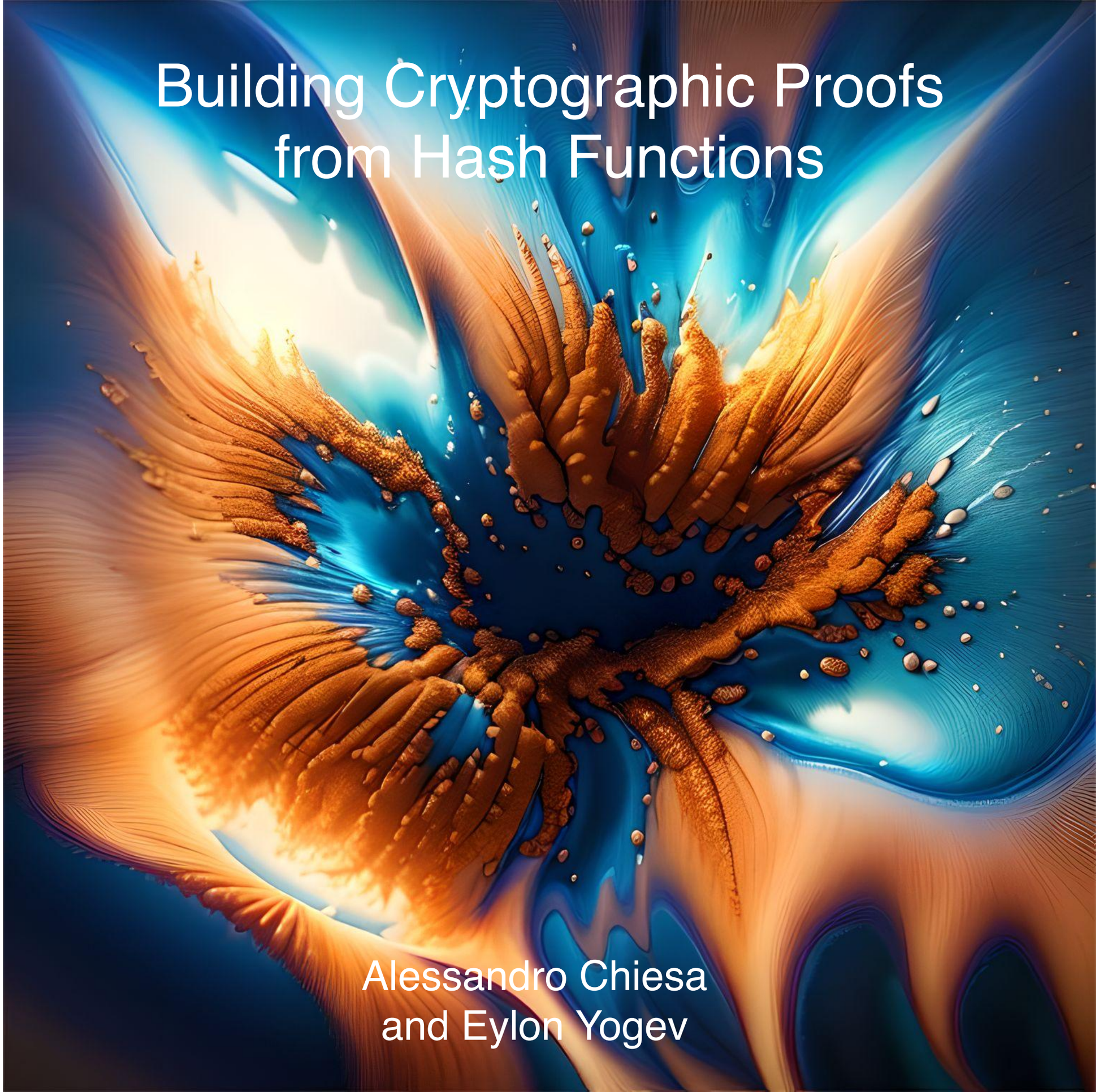

ϵ
1
$2^{-\kappa} \cdot t$
0
0
t
2^{λ}


Part I
What are Cryptographic Proofs?
Part IV
Commitment Schemes
Part II
NARGs Based on SPs
Part V
SNARGs Based on PCPs
Part III
NARGs Based on IPs
Part VI
SNARGs Based on IOPs
Part VII
Practical Considerations

Building Cryptographic Proofs from Hash Functions

Alessandro Chiesa
and Eylon Yogev

Building Cryptographic Proofs from Hash Functions



Alessandro Chiesa
and Eylon Yogev