Simulation Security in the Random Oracle Model

Jérémi Do Dinh

Master’s thesis supervised by Alessandro Chiesa and Giacomo Fenzi

Overview

- Motivation
- Preliminaries
- Results
- Construction:
  Encryption Scheme in the ROM

Overview

- ▸ **Motivation**
- Preliminaries
- Results
- Construction:
  Encryption Scheme in the ROM

Non-interactive ARGuments in the ROM

Motivation

Non-interactive ARGuments in the ROM

Motivation

- Simple setting.

Non-interactive ARGuments in the ROM

Motivation

- Simple setting.
- Heuristically instantiation with hash functions.

Non-interactive ARGuments in the ROM

Motivation

- Simple setting.
- Heuristically instantiation with hash functions.
- Can have a transparent setup.

Non-interactive ARGuments in the ROM

Simulation security

Non-interactive ARGuments in the ROM

Simulation security

- Classical security: isolated adversary.

Non-interactive ARGuments in the ROM

Simulation security

- Classical security: isolated adversary.
- NARGs in stronger adversarial settings:

Non-interactive ARGuments in the ROM

Simulation security

- Classical security: isolated adversary.
- NARGs in <u>stronger adversarial</u> settings:
  - Soundness when protocols can be observed.

Non-interactive ARGuments in the ROM

Simulation security

- Classical security: isolated adversary.
- NARGs in stronger adversarial settings:
  - Soundness when protocols can be observed.
- *Concrete security* formalizations are required.

Concrete Security

Concrete Security

- Limitations of asymptotic security.

Concrete Security

- Limitations of asymptotic security.
- Internal parameters affecting security.

Concrete Security

- Limitations of asymptotic security.
- Internal parameters affecting security.
- Concrete security: parameterized error bounds.

Concrete Security

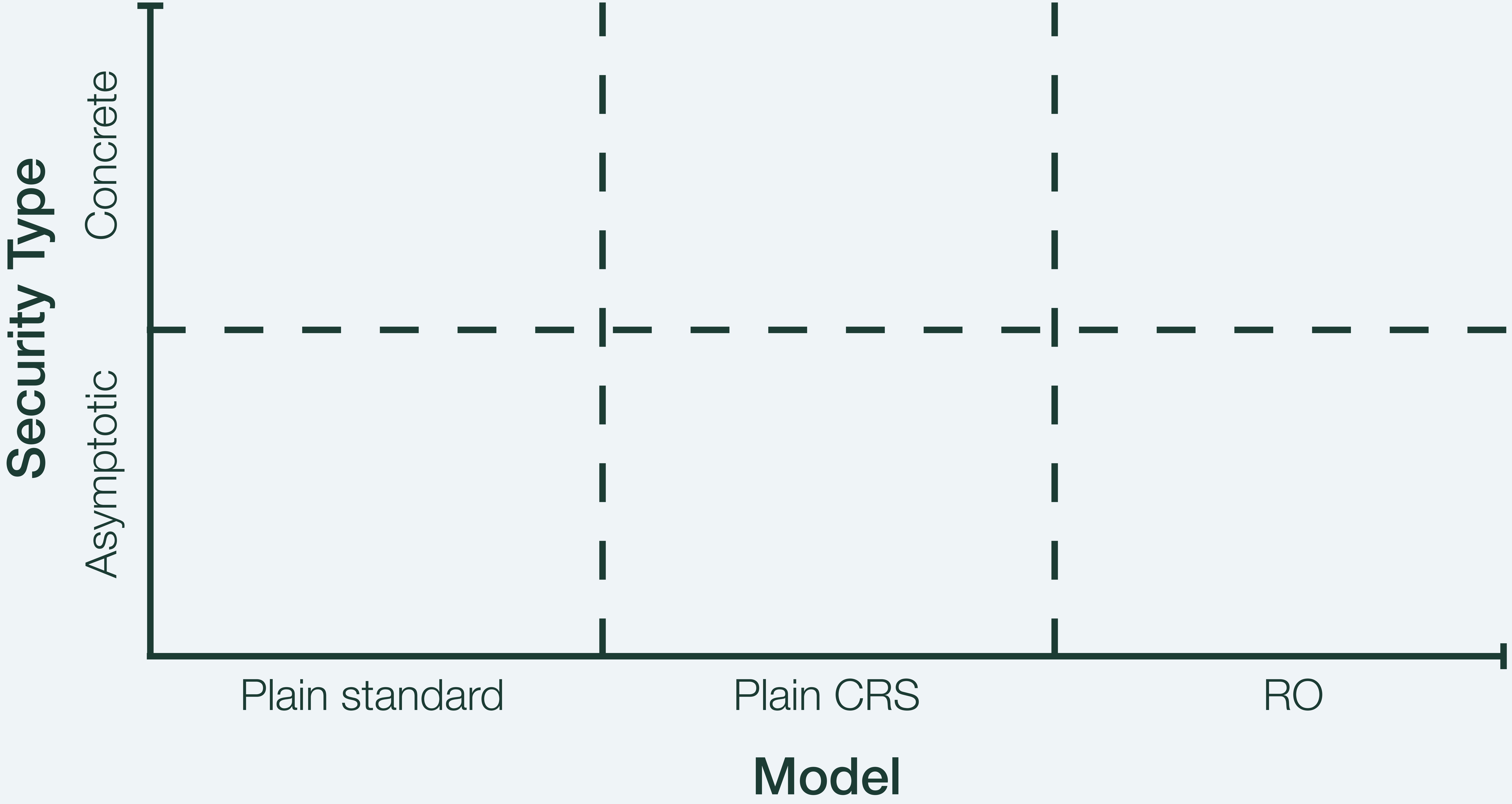
- Limitations of asymptotic security.
- Internal parameters affecting security.
- Concrete security: parameterized error bounds.
- Security reductions and resource overhead.

Concrete Security

- Limitations of asymptotic security.
- Internal parameters affecting security.
- Concrete security: parameterized error bounds.
- Security reductions and resource overhead.
- Practical protocol instantiation.

Simulation Security

Landscape



Simulation Security

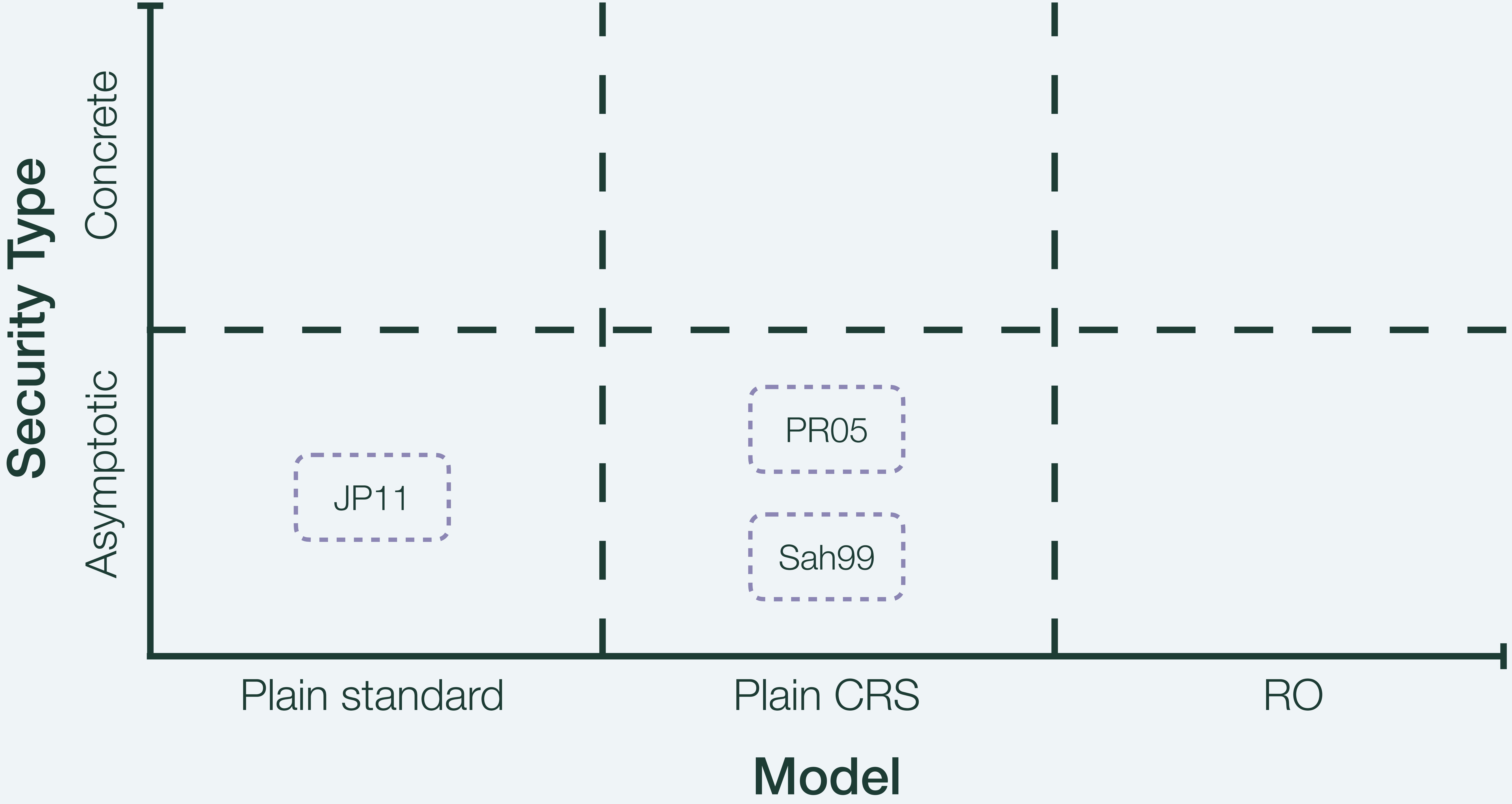
Landscape

Simulation Security

Landscape

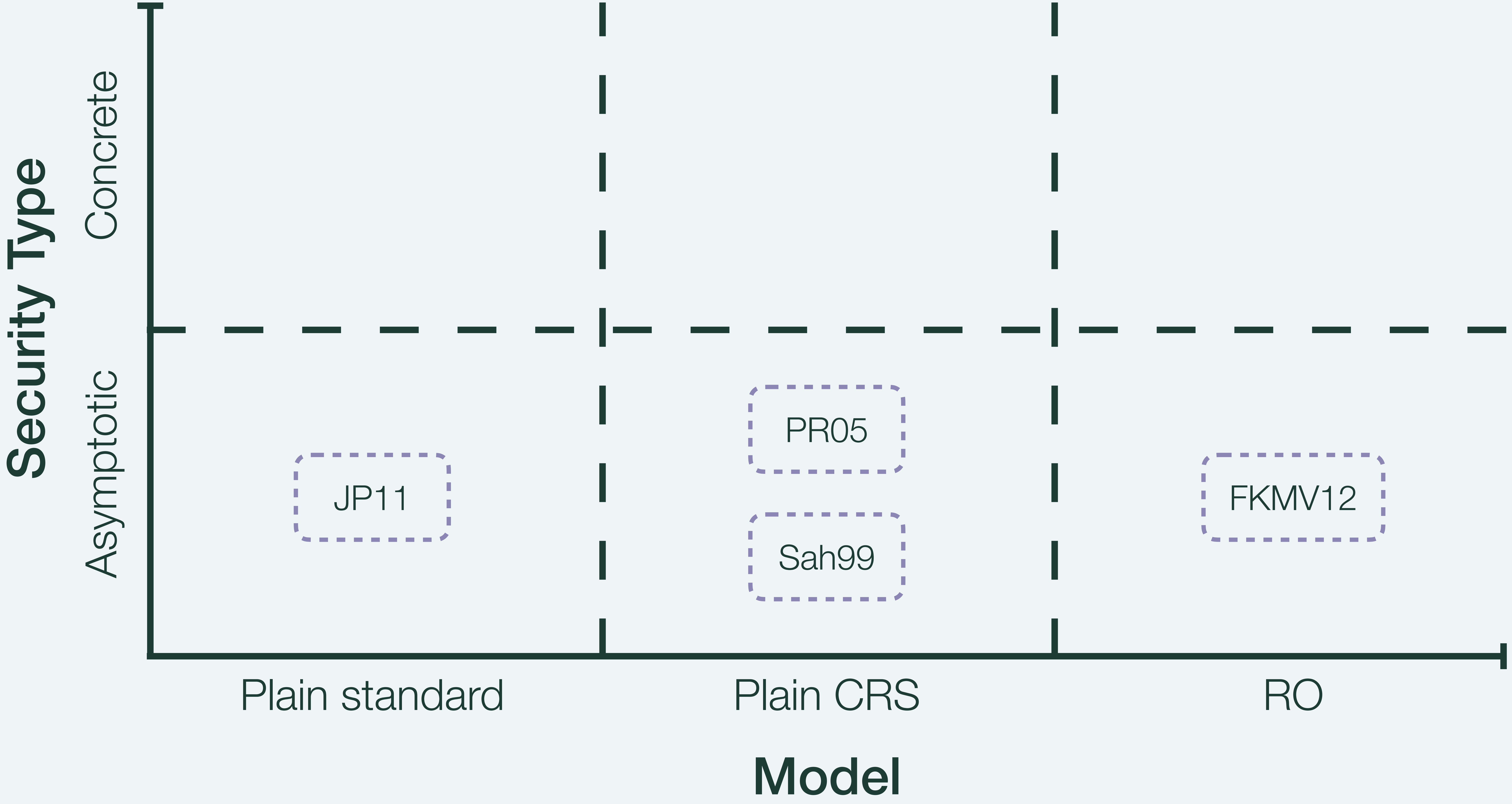
Simulation Security

Landscape



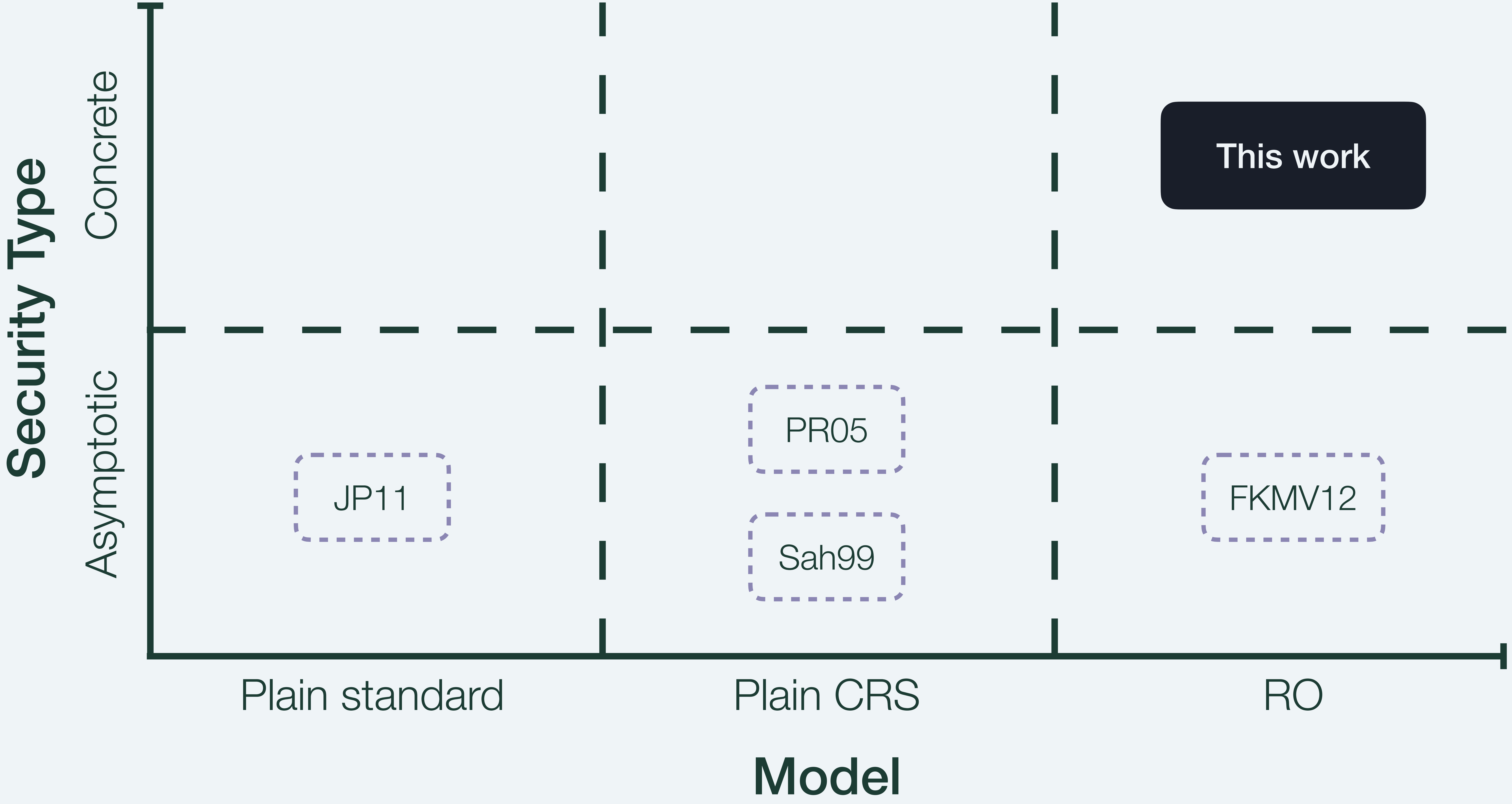
Simulation Security

Landscape



Simulation Security

Landscape



Overview

- Motivation
- ▸ Preliminaries
- Results
- Construction:
  Encryption Scheme in the ROM

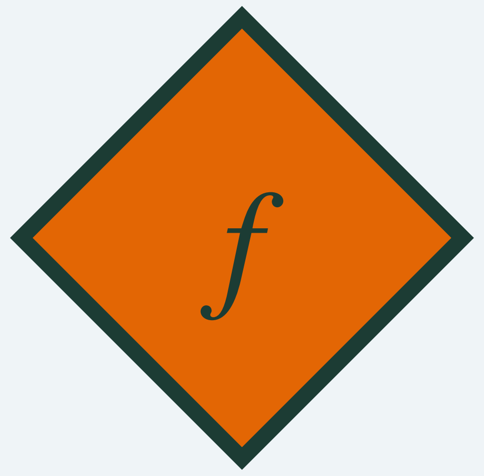
The Random Oracle Model (ROM)

The Random Oracle Model (ROM)

Security parameter $\sigma \in \mathbb{N}$

$f : \{0,1\}^* \rightarrow \{0,1\}^\sigma$

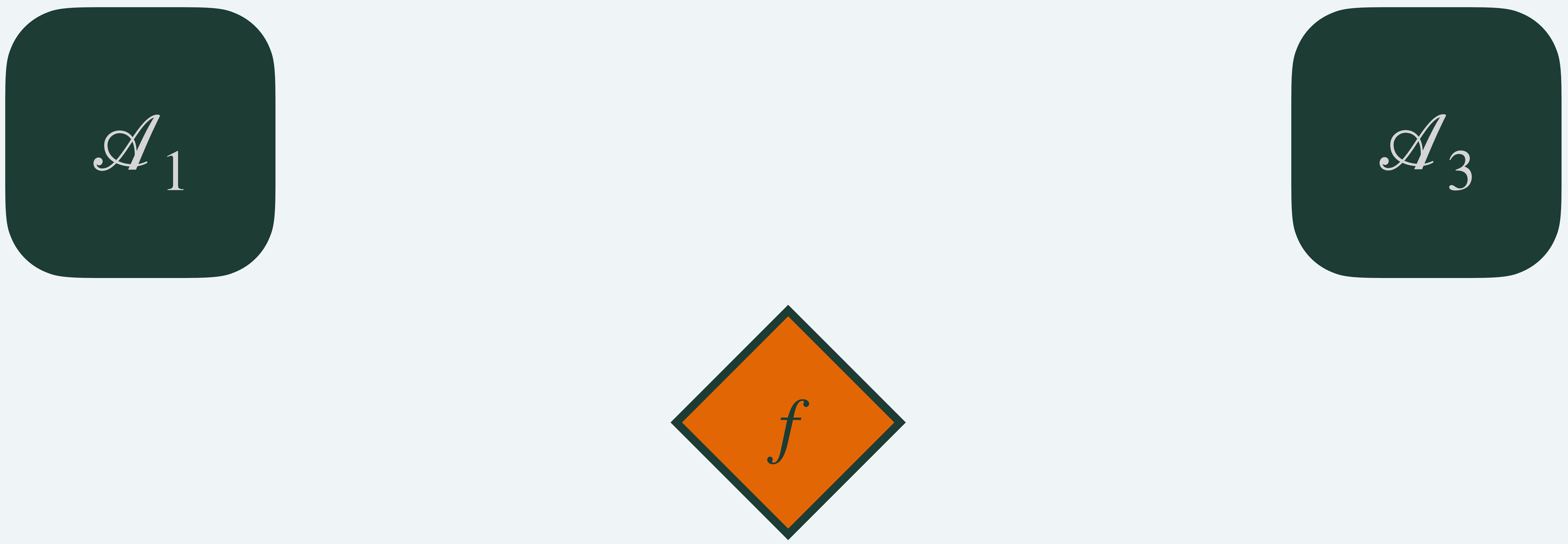
The Random Oracle Model (ROM)



Security parameter $\sigma \in \mathbb{N}$

$f: \{0,1\}^* \rightarrow \{0,1\}^\sigma$

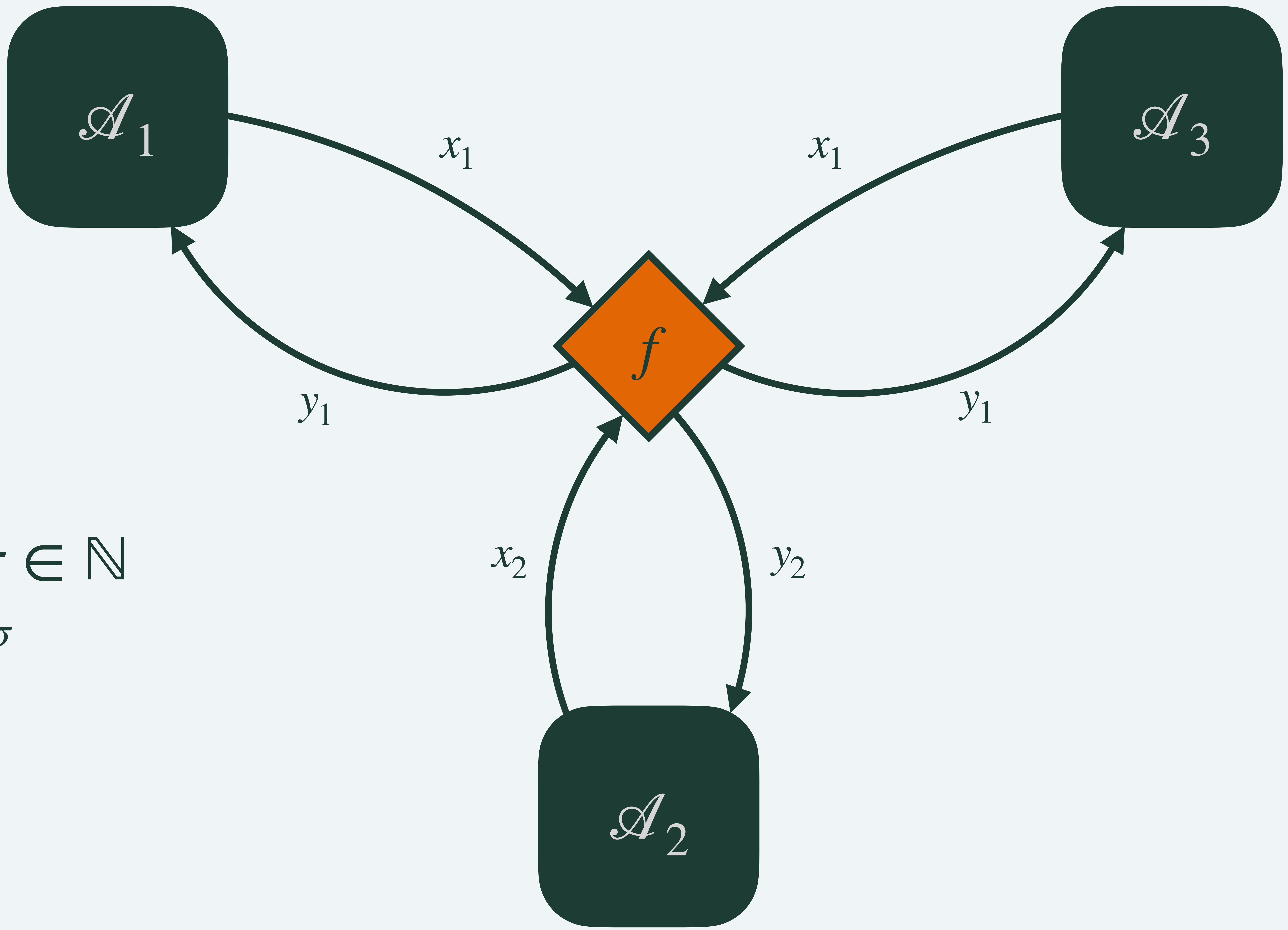
The Random Oracle Model (ROM)



Security parameter $\sigma \in \mathbb{N}$

$f : \{0,1\}^* \rightarrow \{0,1\}^\sigma$

The Random Oracle Model (ROM)



Security parameter $\sigma \in \mathbb{N}$

$f : \{0,1\}^* \rightarrow \{0,1\}^\sigma$

NARGs

Non-interactive ARGuments (in the ROM)

NARGs

Non-interactive ARGuments (in the ROM)

NARGs

Non-interactive ARGuments (in the ROM)

Relation $\mathscr{R} \subseteq \{0,1\}^* \times \{0,1\}^*$

NARGs

Non-interactive ARGuments (in the ROM)

Relation $\mathscr{R} \subseteq \{0,1\}^* \times \{0,1\}^*$

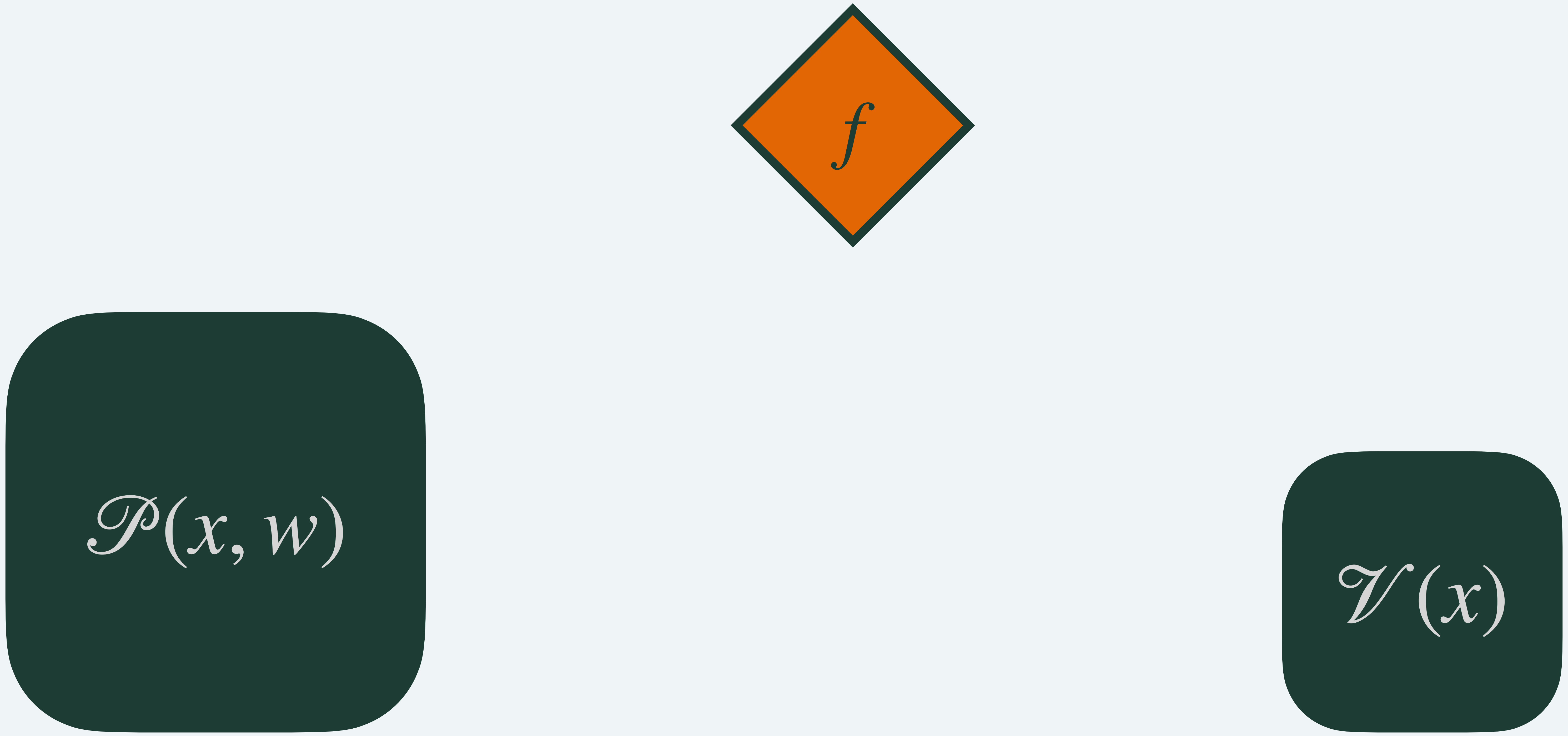
NARG $= (\mathscr{P}, \mathscr{V})$

NARGs

Non-interactive ARGuments (in the ROM)

Relation $\mathscr{R} \subseteq \{0,1\}^* \times \{0,1\}^*$

NARG $= (\mathscr{P}, \mathscr{V})$

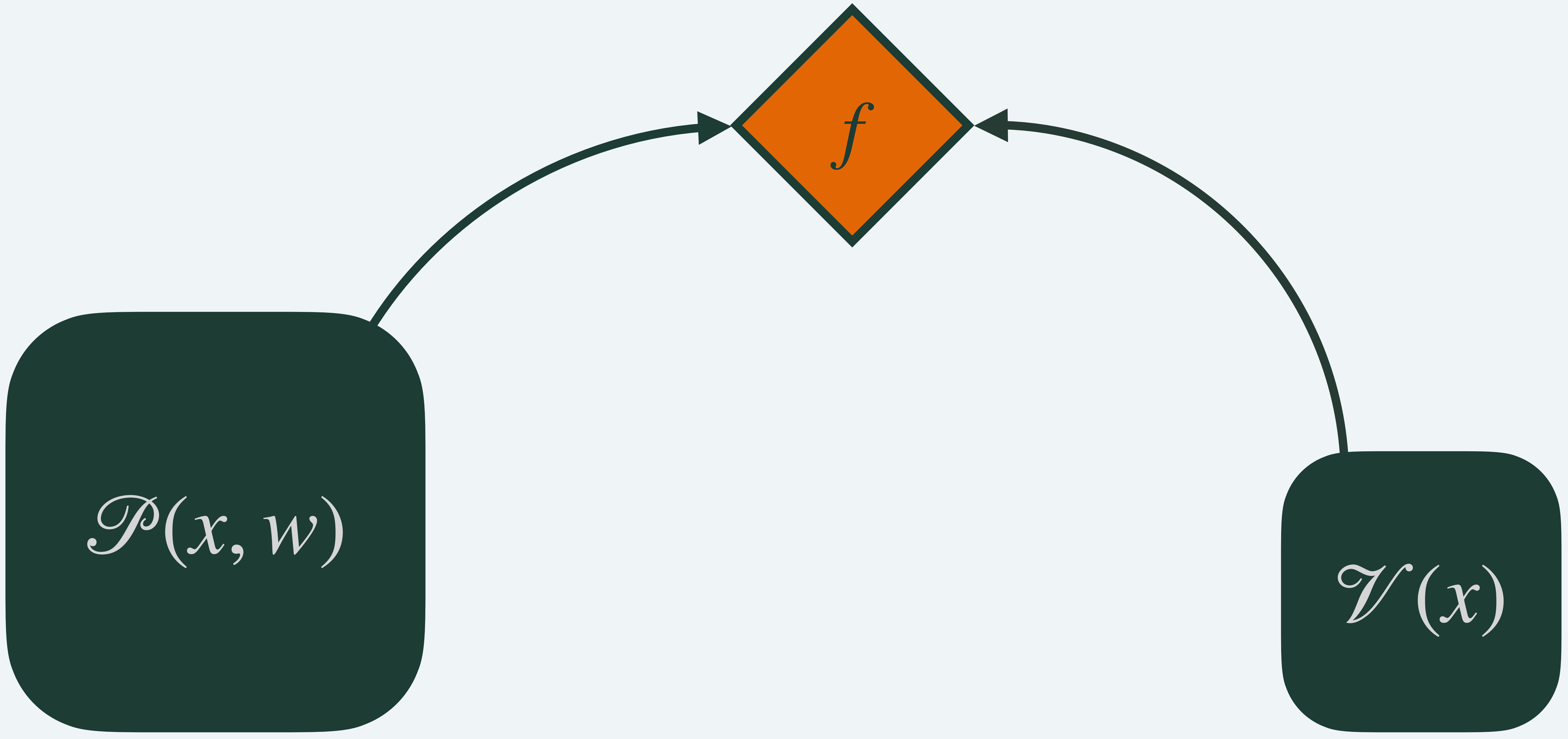


NARGs

Non-interactive ARGuments (in the ROM)

Relation $\mathscr{R} \subseteq \{0,1\}^* \times \{0,1\}^*$

NARG $= (\mathscr{P}, \mathscr{V})$



NARGs

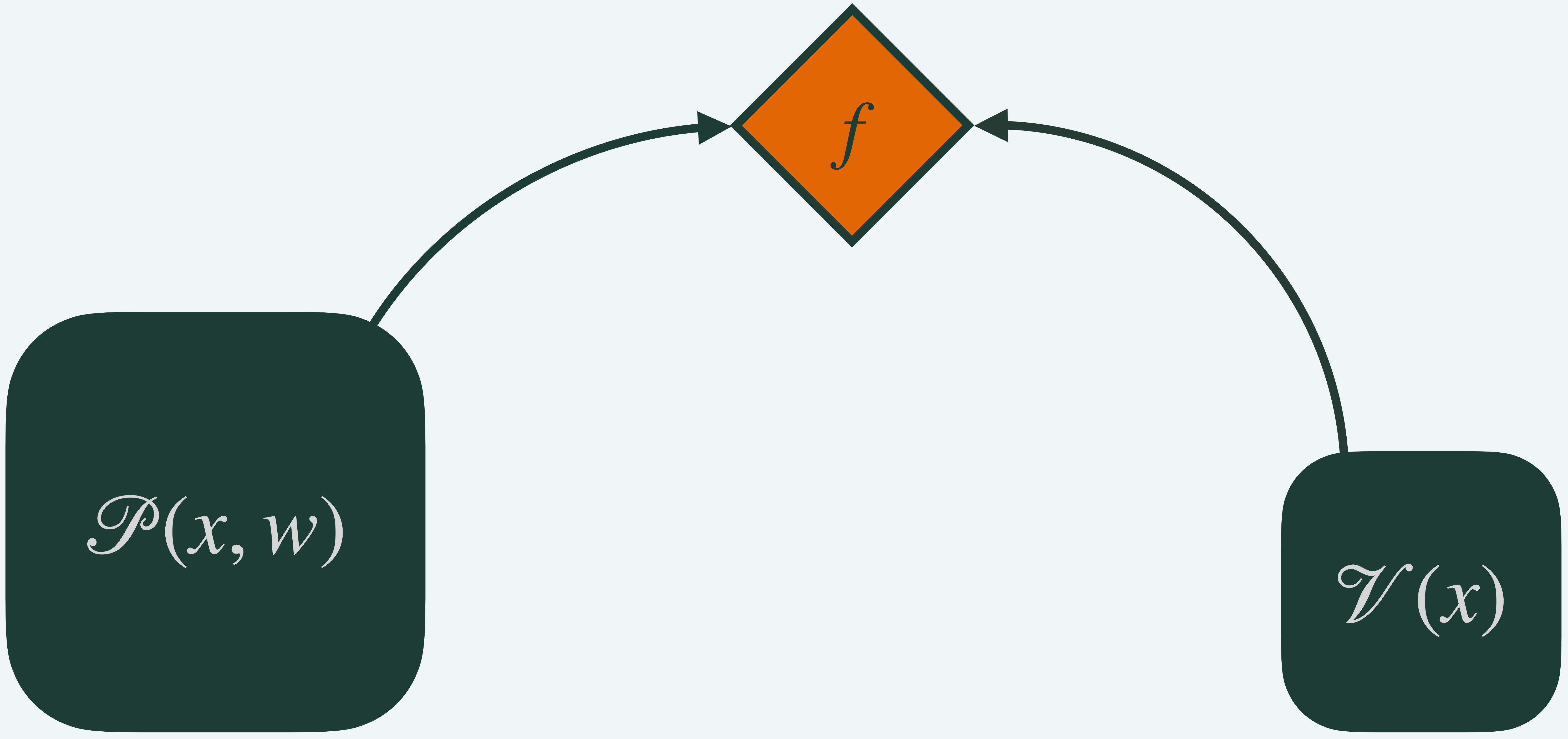
Non-interactive ARGuments (in the ROM)

Relation $\mathscr{R} \subseteq \{0,1\}^* \times \{0,1\}^*$

NARG $= (\mathscr{P}, \mathscr{V})$

Non-interactive:

The prover sends one message.



NARGs

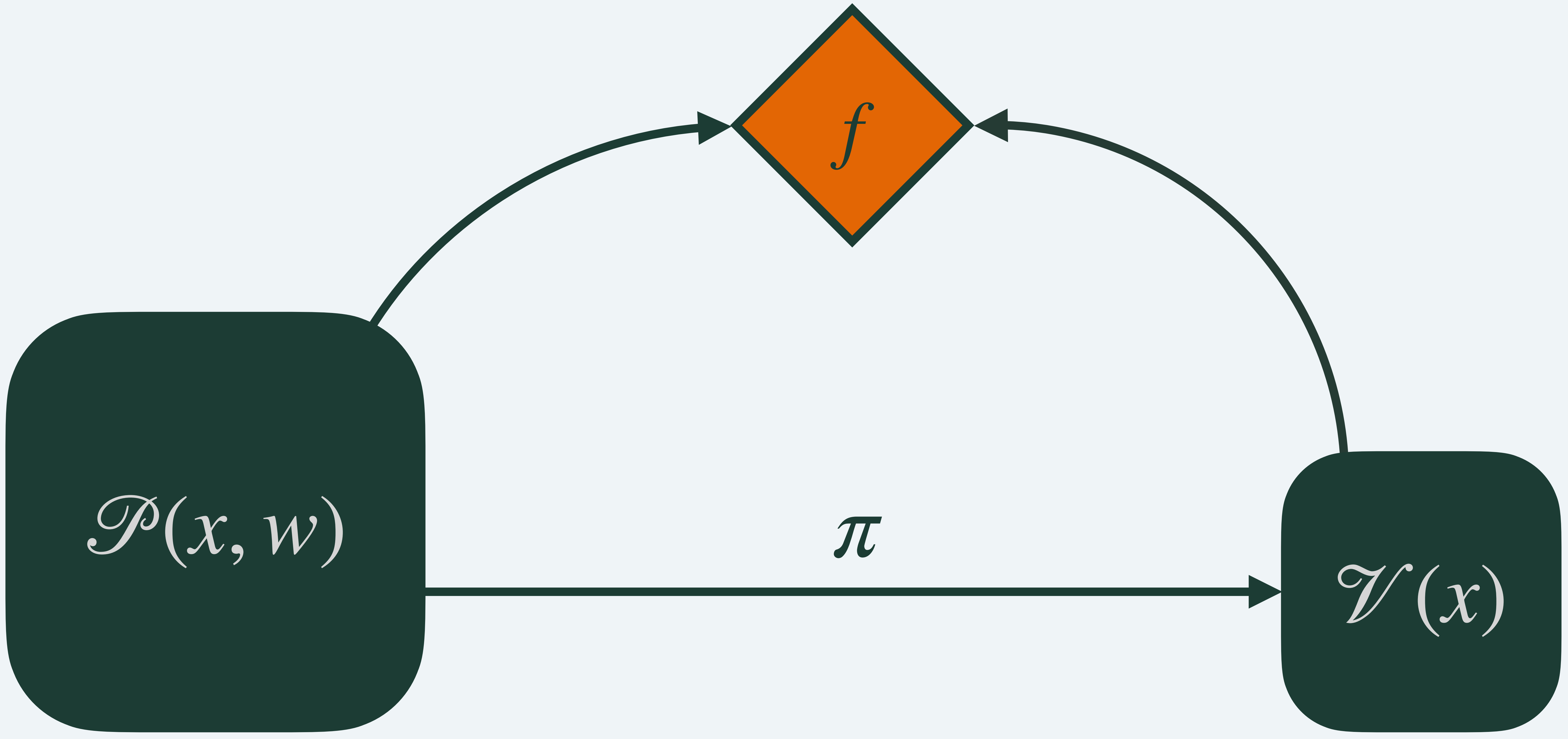
Non-interactive ARGuments (in the ROM)

Relation $\mathscr{R} \subseteq \{0,1\}^* \times \{0,1\}^*$

$\text{NARG} = (\mathscr{P}, \mathscr{V})$

Non-interactive:

The prover sends one message.



NARGs

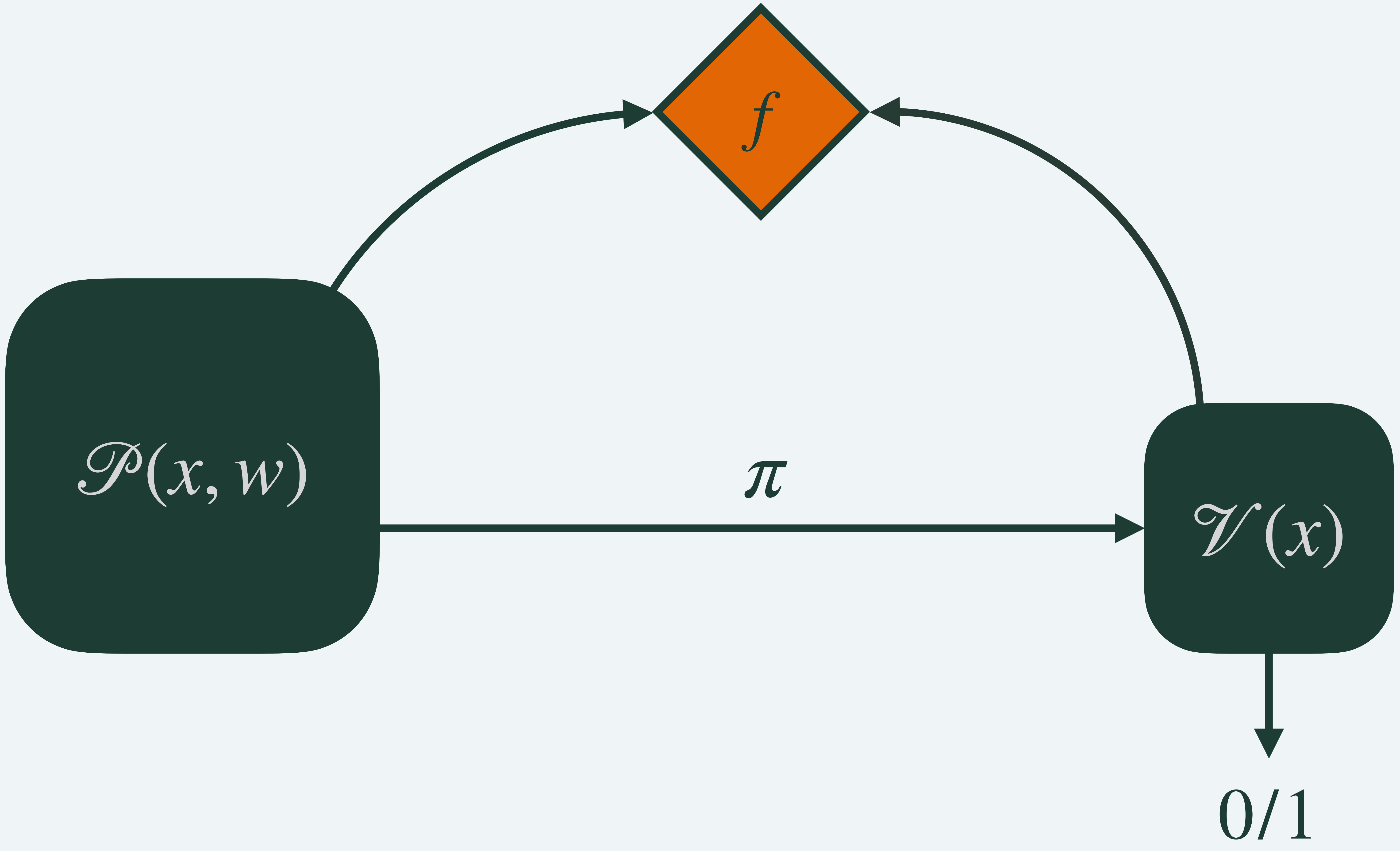
Non-interactive ARGuments (in the ROM)

Relation $\mathscr{R} \subseteq \{0,1\}^* \times \{0,1\}^*$

NARG $= (\mathscr{P}, \mathscr{V})$

Non-interactive:

The prover sends one message.



NARGs

Non-interactive ARGuments (in the ROM)

Relation $\mathscr{R} \subseteq \{0,1\}^* \times \{0,1\}^*$

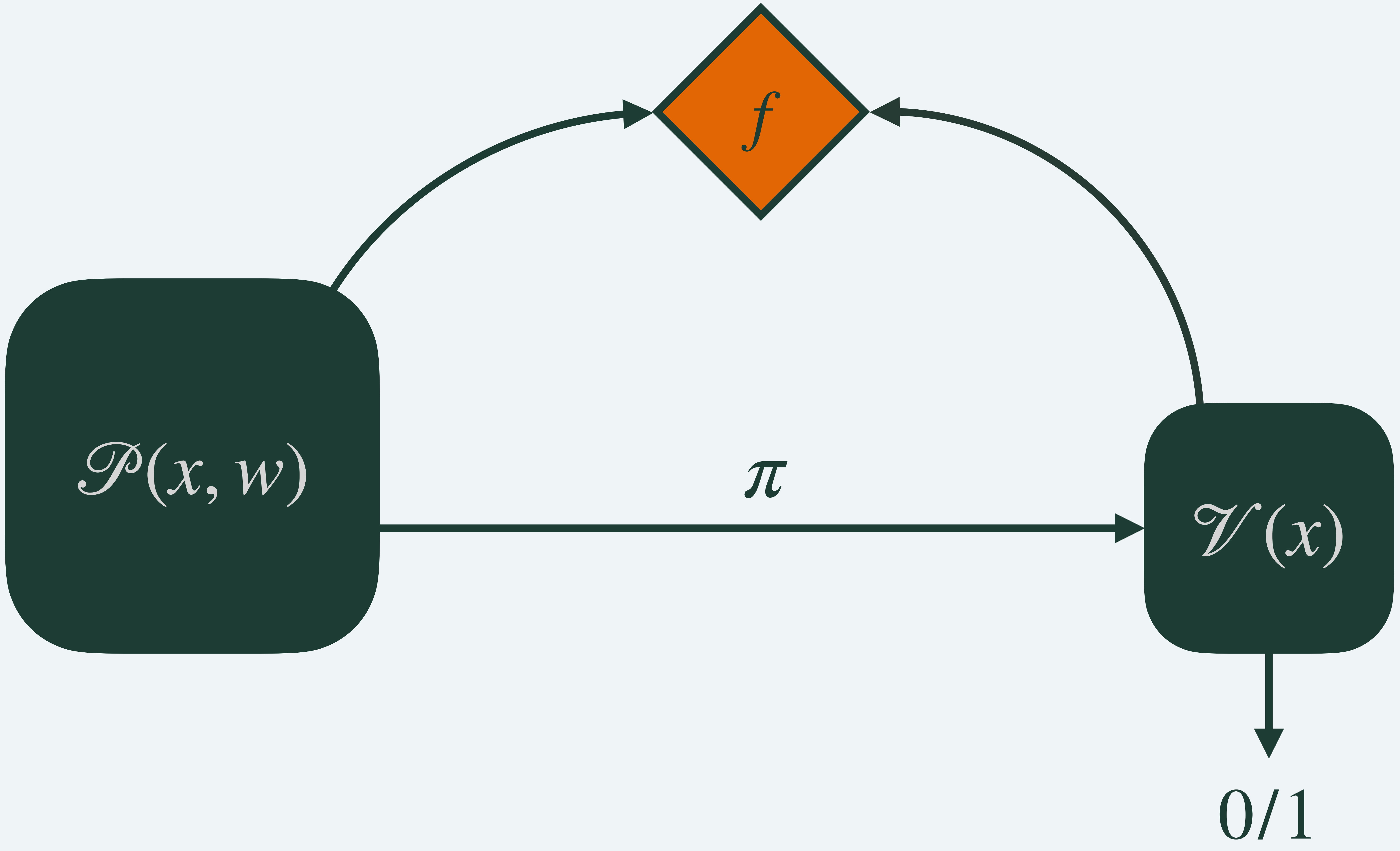
NARG $= (\mathscr{P}, \mathscr{V})$

Non-interactive:

The prover sends one message.

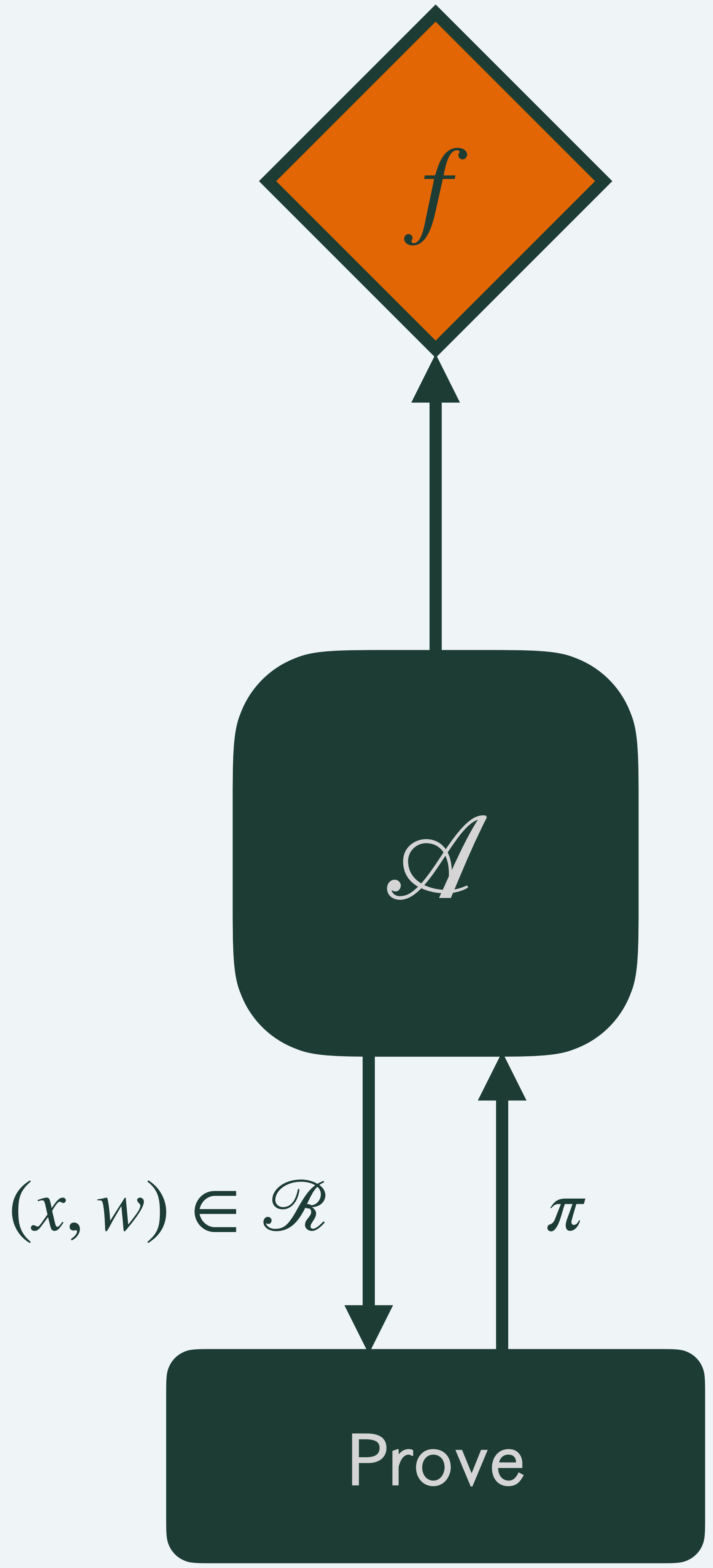
Complete:

If $(x, w) \in \mathscr{R}$, then $\mathscr{V}^f(x, \pi) = 1$.

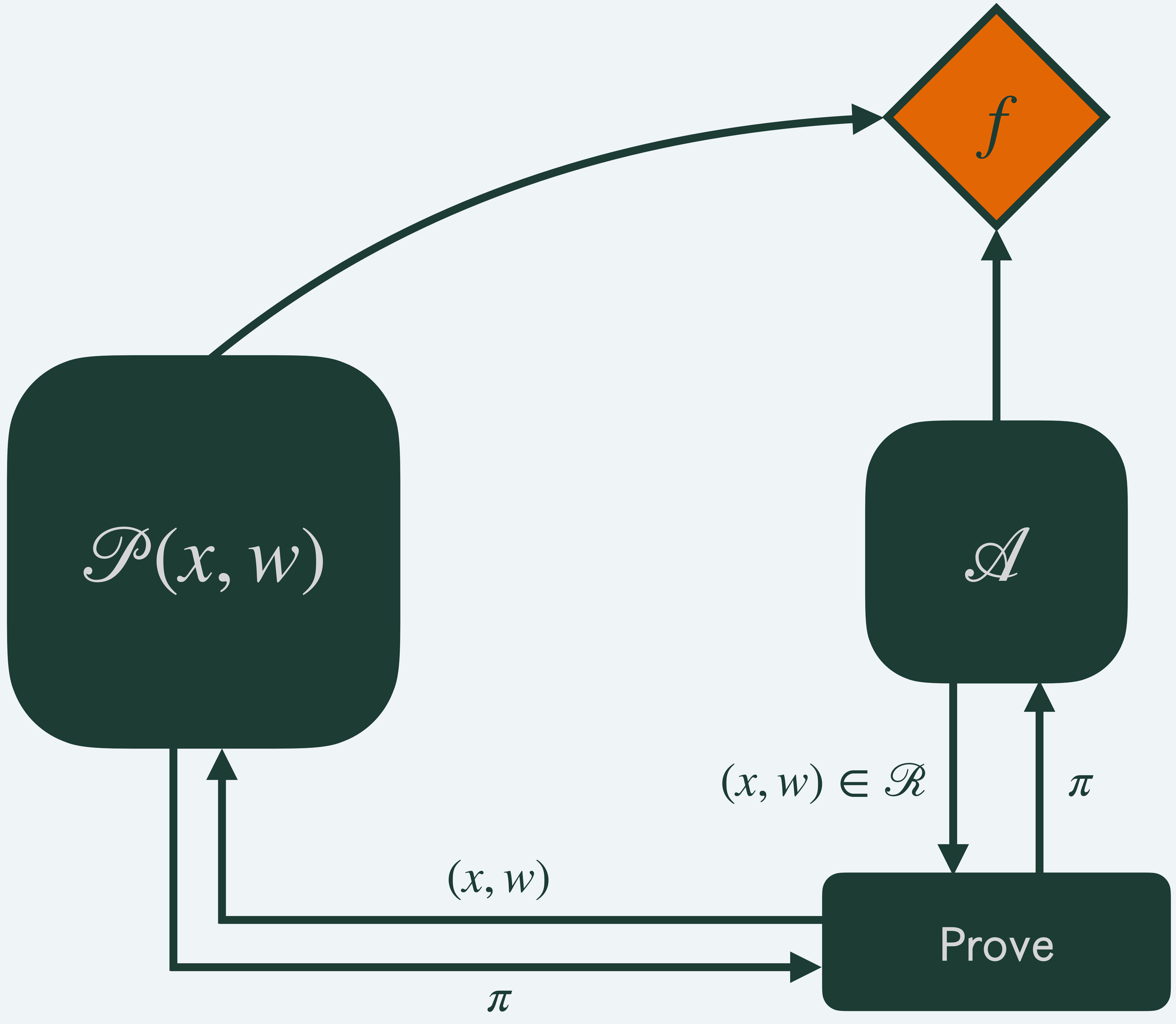


Zero-knowledge

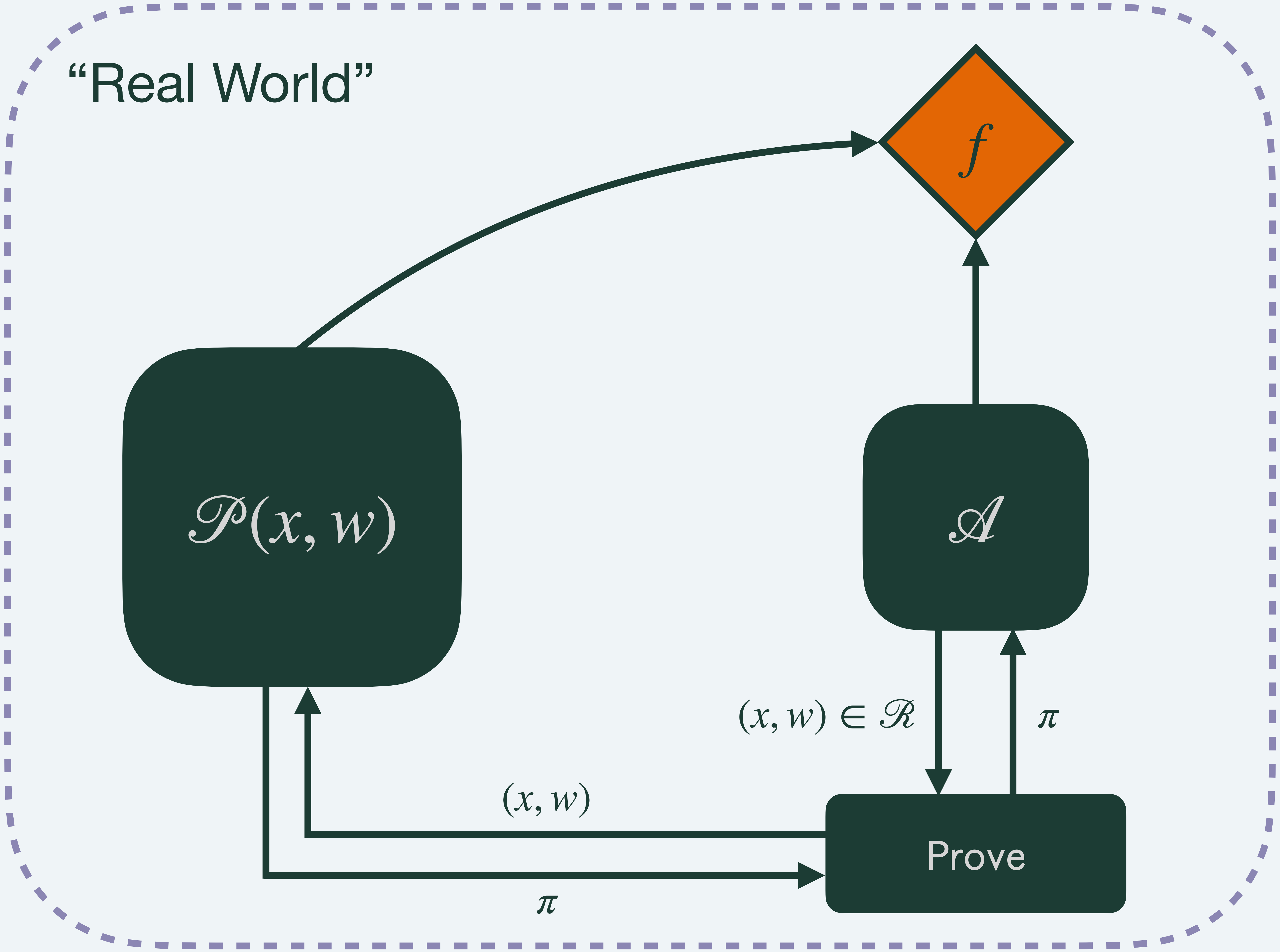
Zero-knowledge



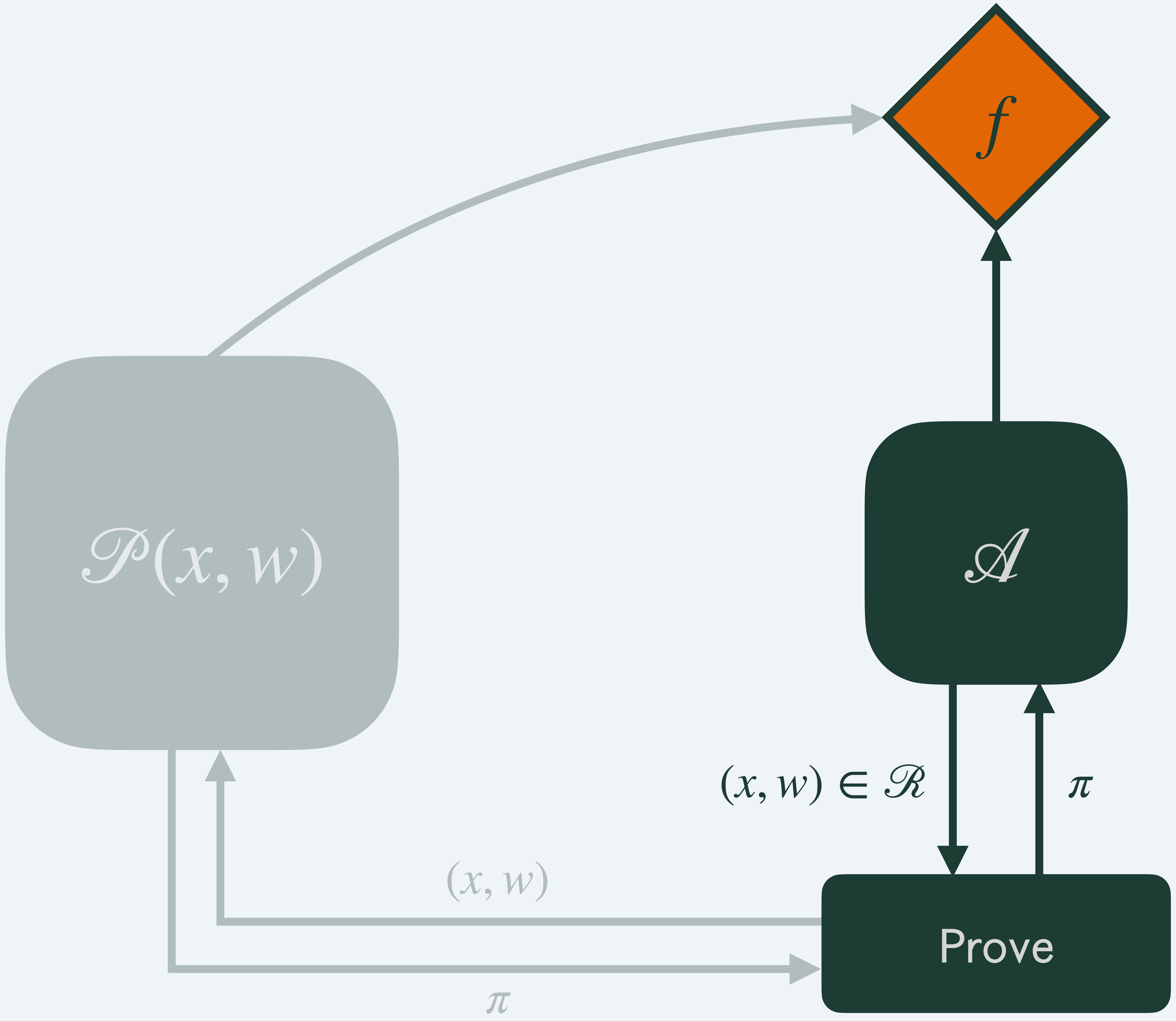
Zero-knowledge



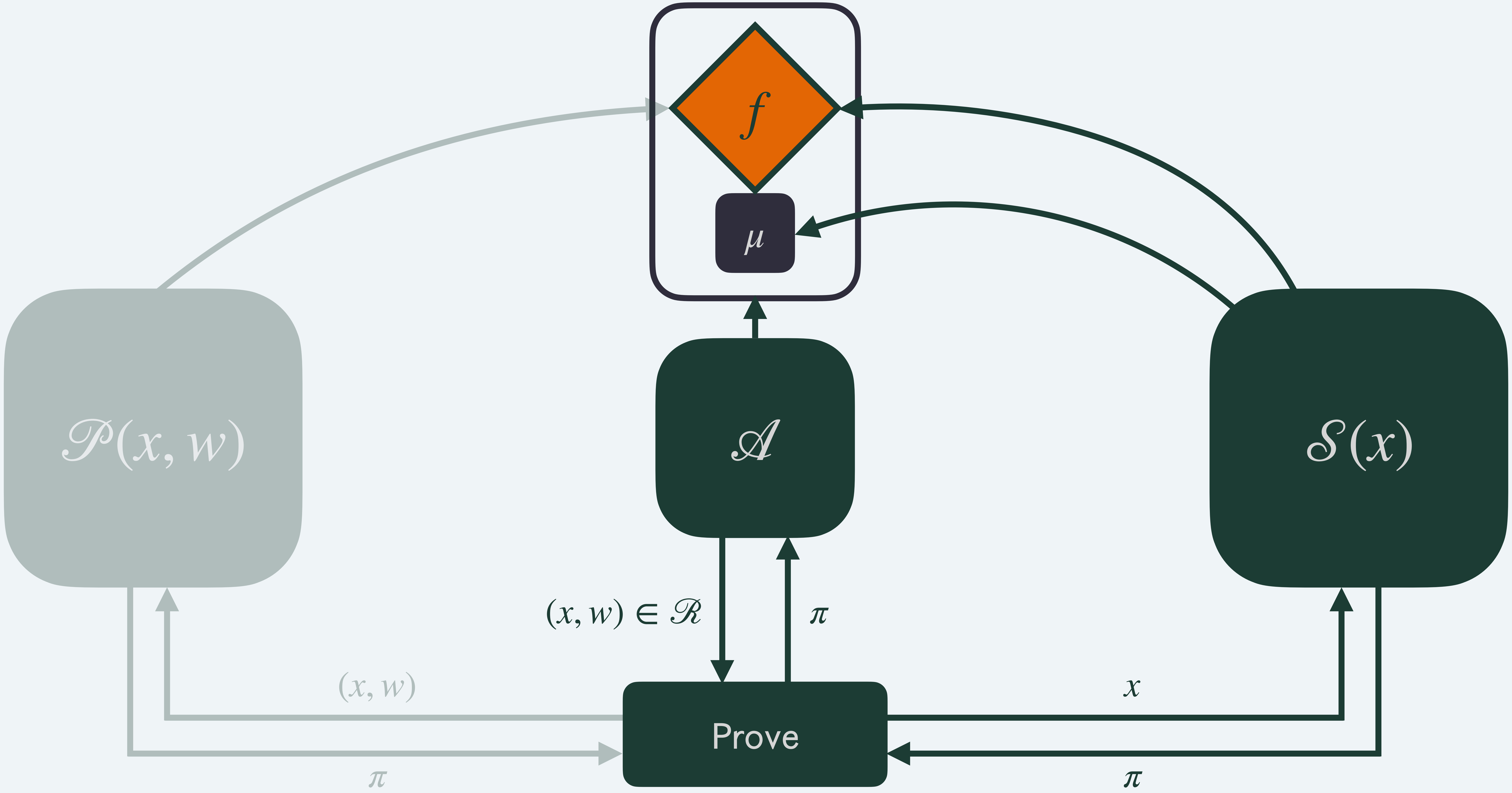
Zero-knowledge



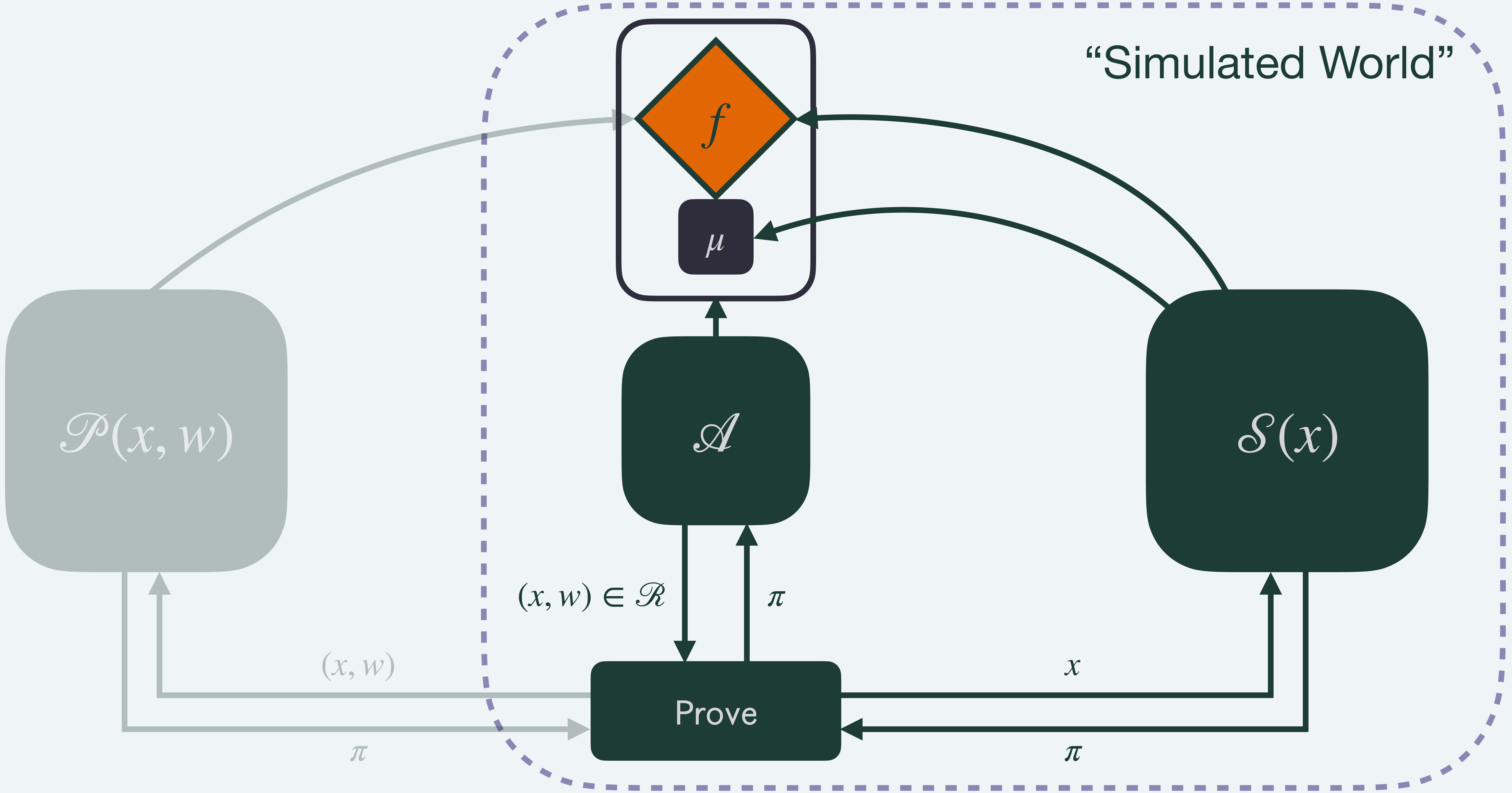
Zero-knowledge



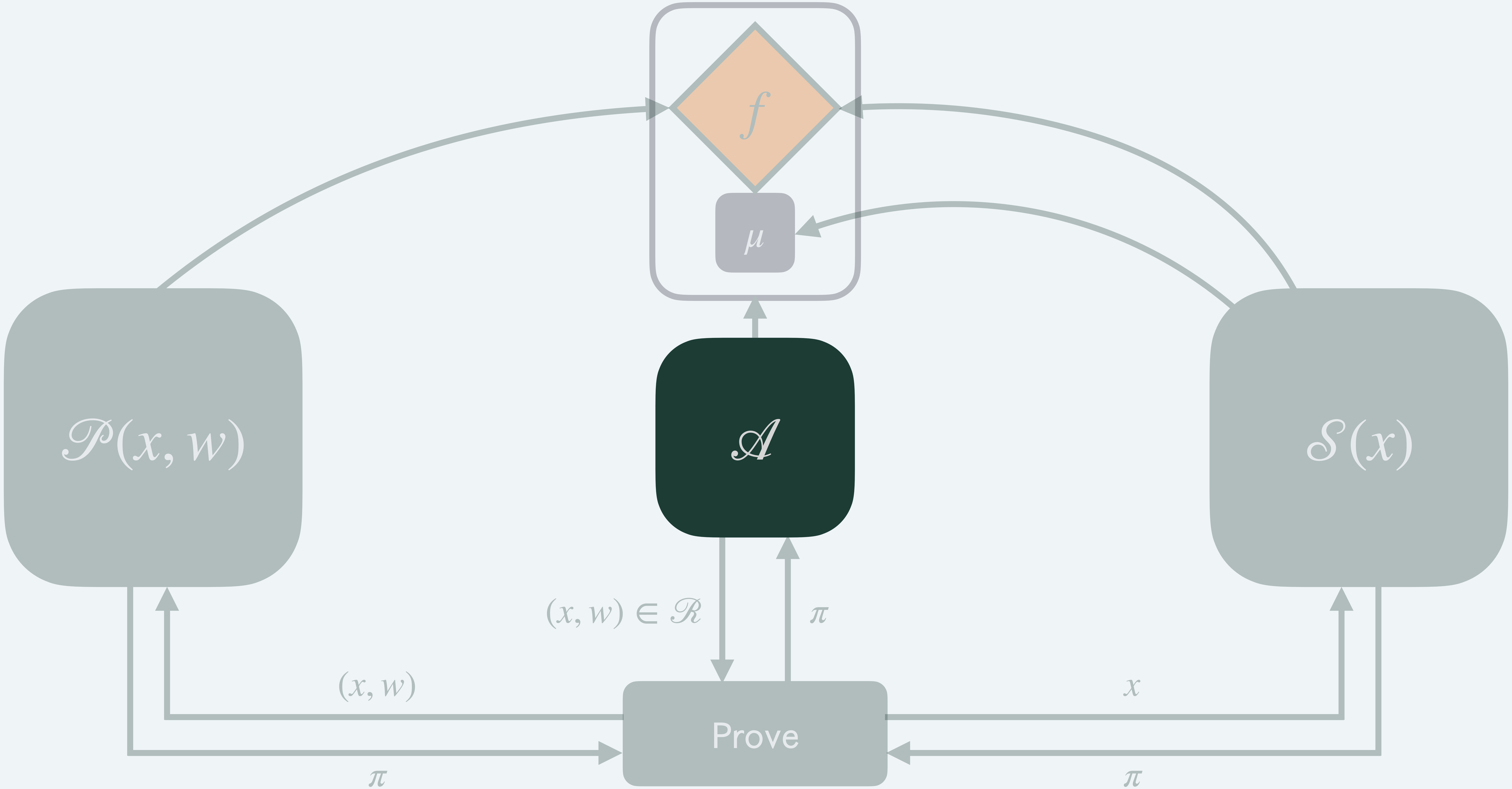
Zero-knowledge



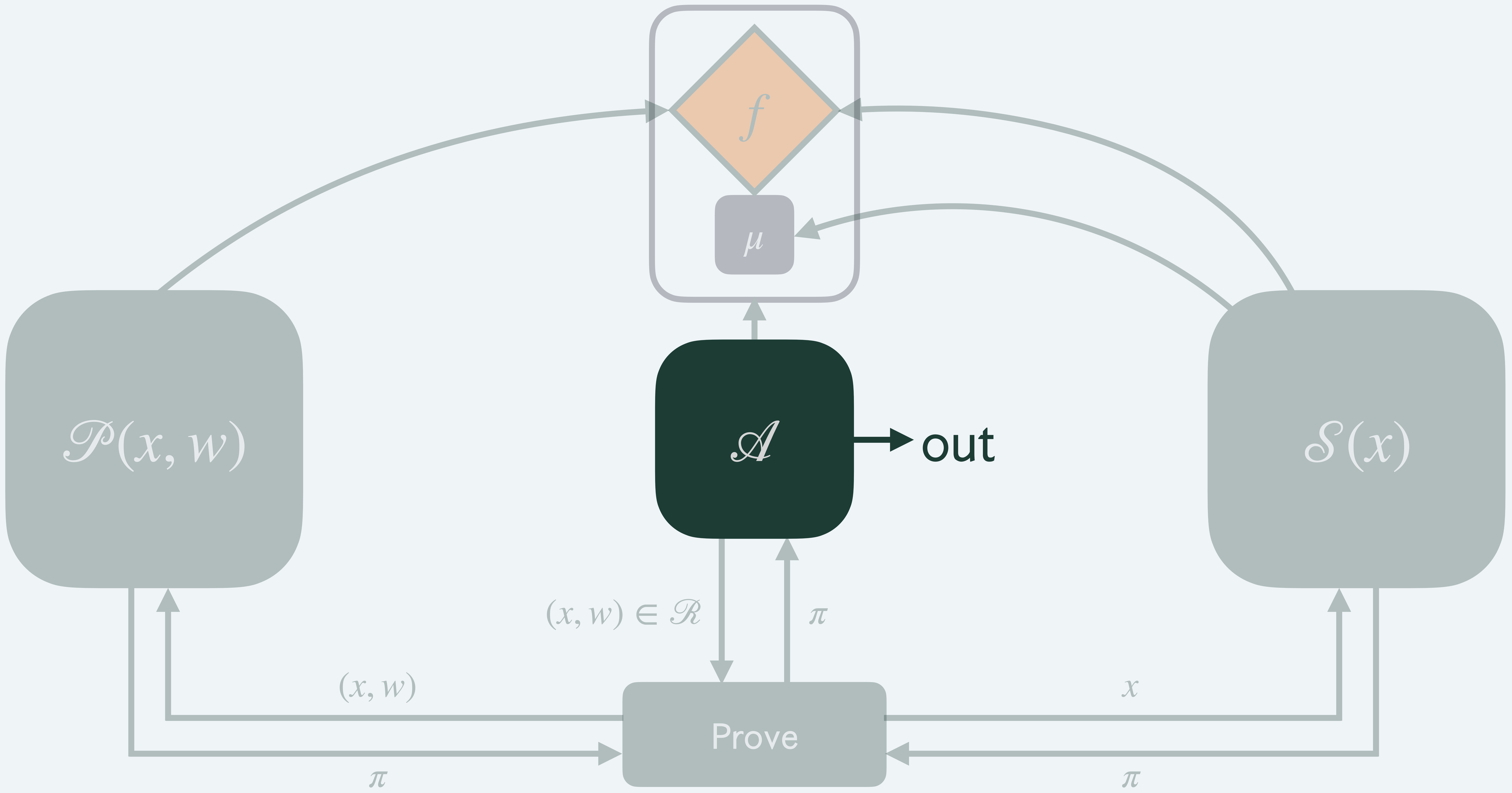
Zero-knowledge



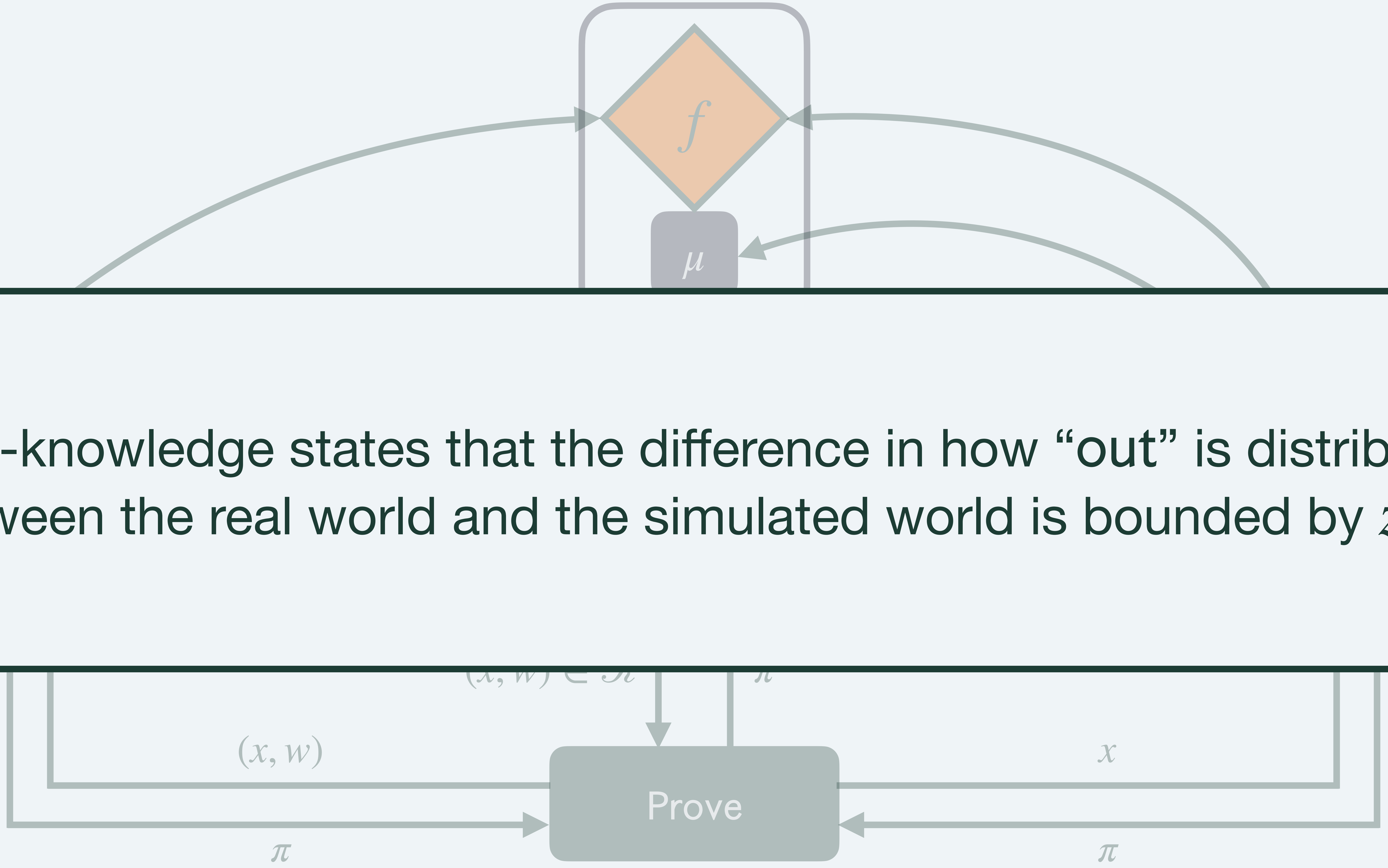
Zero-knowledge



Zero-knowledge



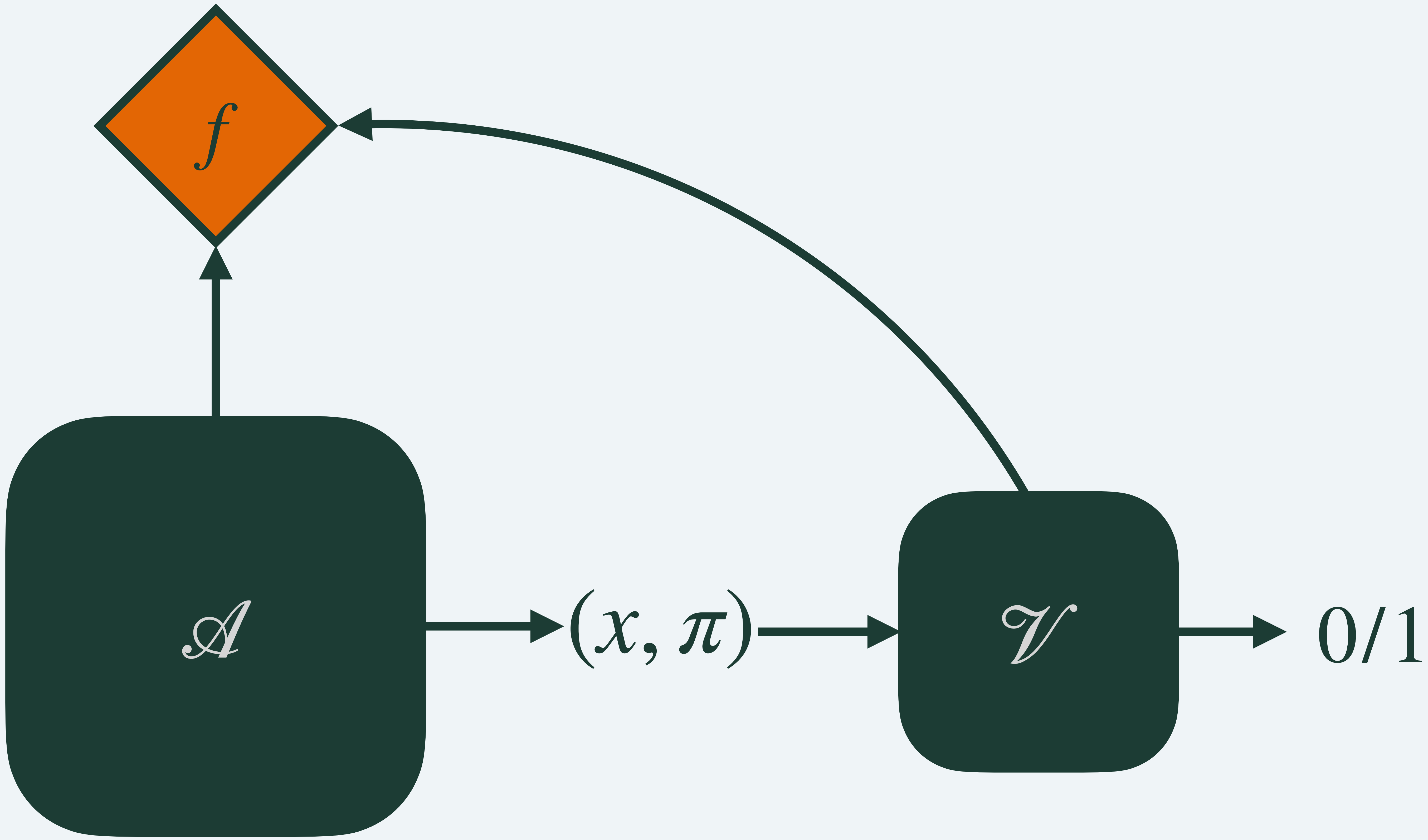
Zero-knowledge



Zero-knowledge states that the difference in how "out" is distributed between the real world and the simulated world is bounded by z_{ARG}.

Soundness Notions

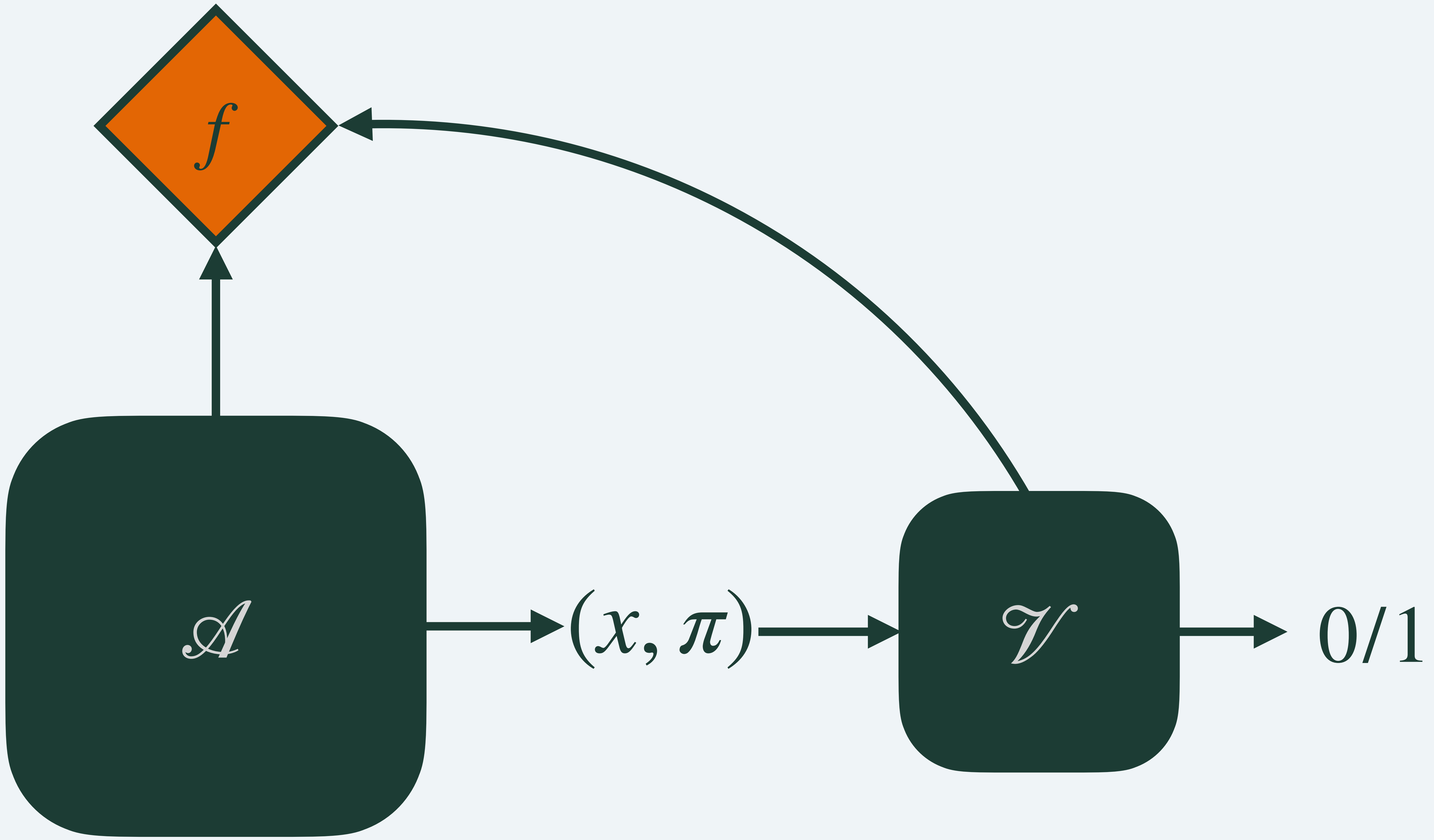
Soundness Notions



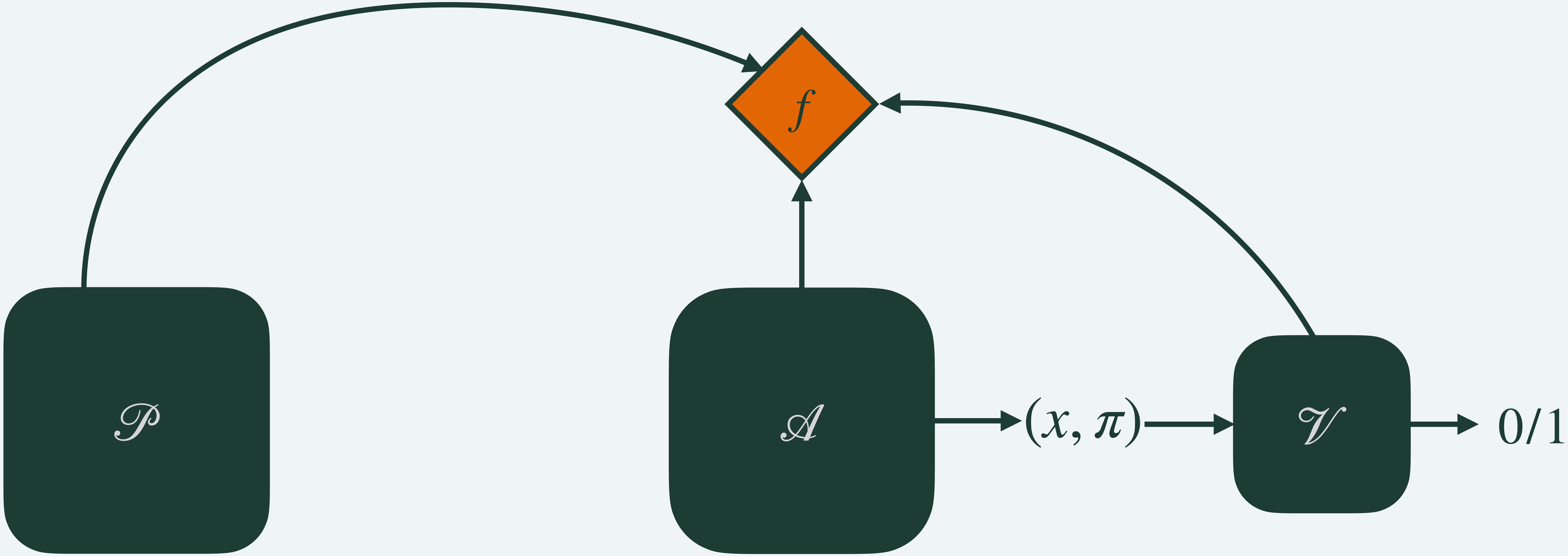
Soundness Notions

Knowledge Soundness:

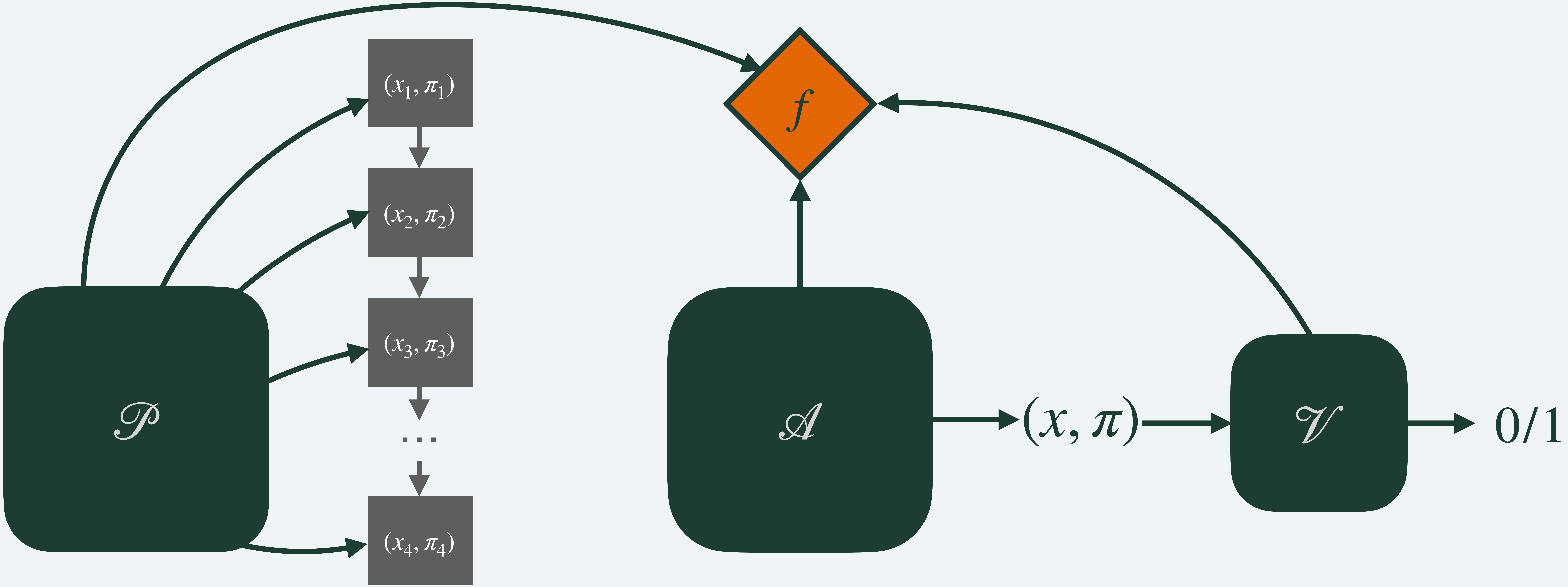
The probability $\mathscr{V}^f(x, \pi) = 1$ **and** we cannot extract a witness w s.t. $(x, w) \in \mathscr{R}$ is "small".



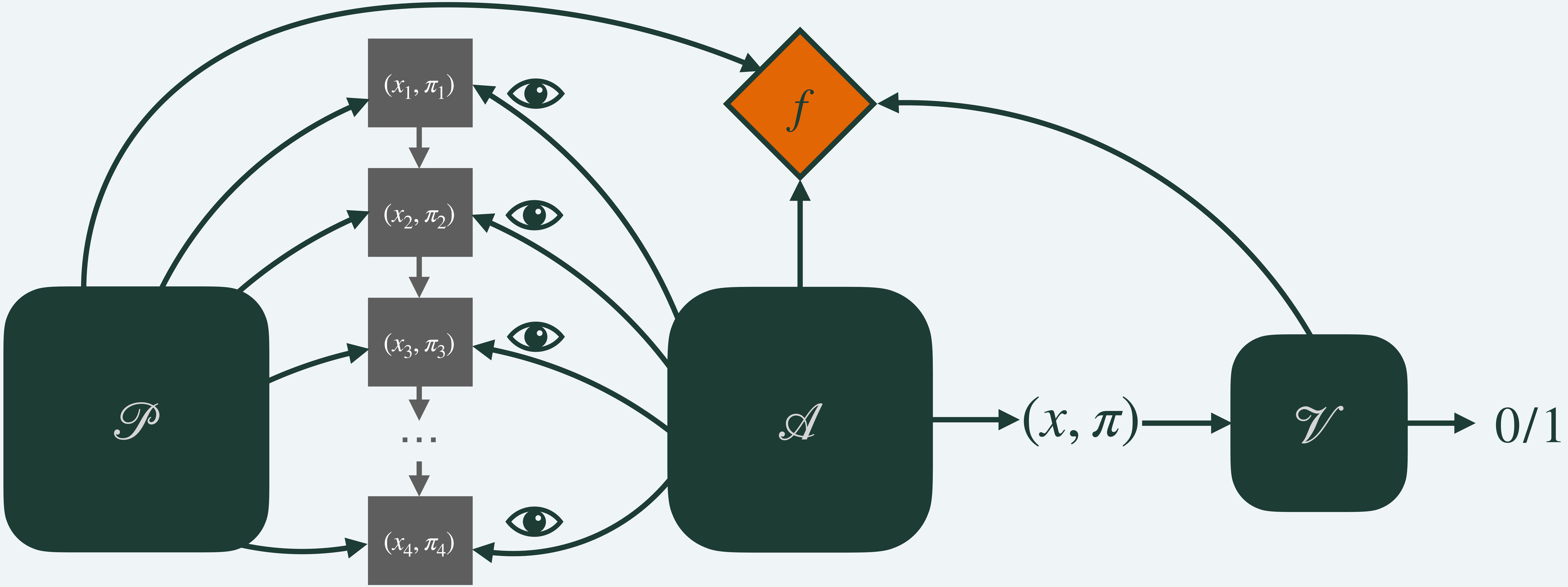
Soundness Notions



Soundness Notions



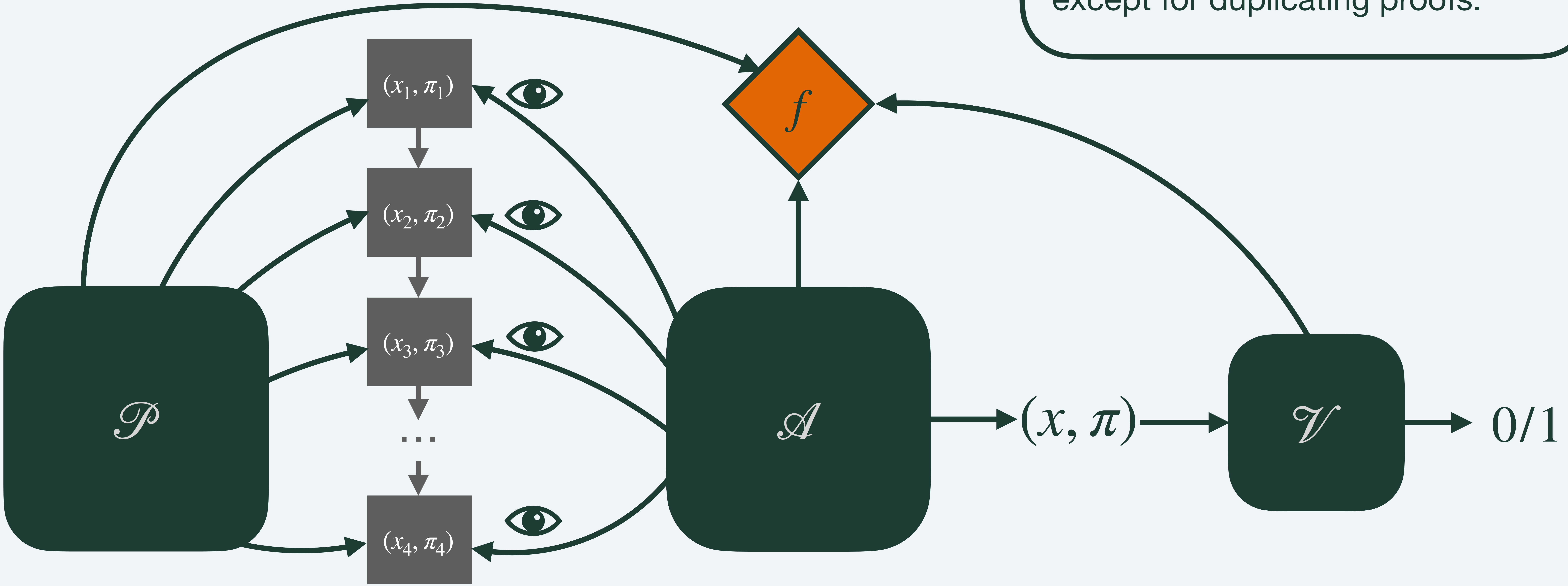
Soundness Notions



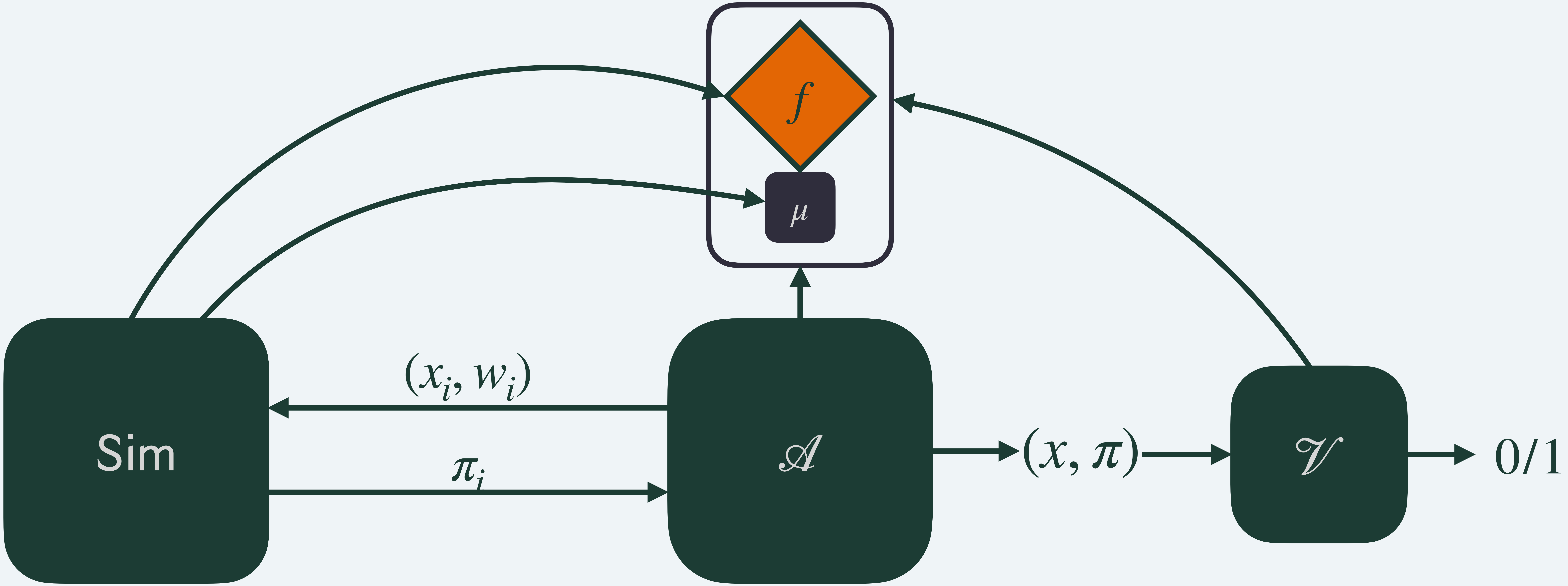
Soundness Notions

Non-malleability:

"Whatever one can compute after observing proofs, one could've computed before observing them, except for duplicating proofs."



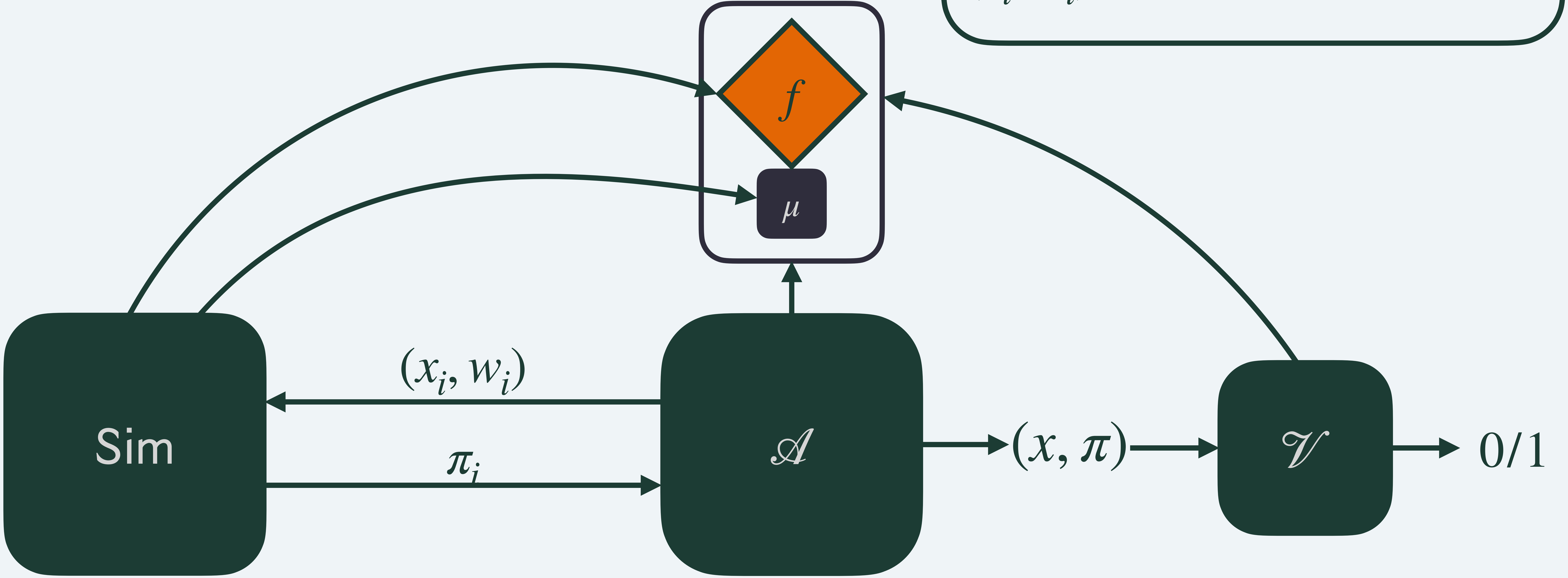
Simulation Security



Simulation Security

"True" Simulation Security:

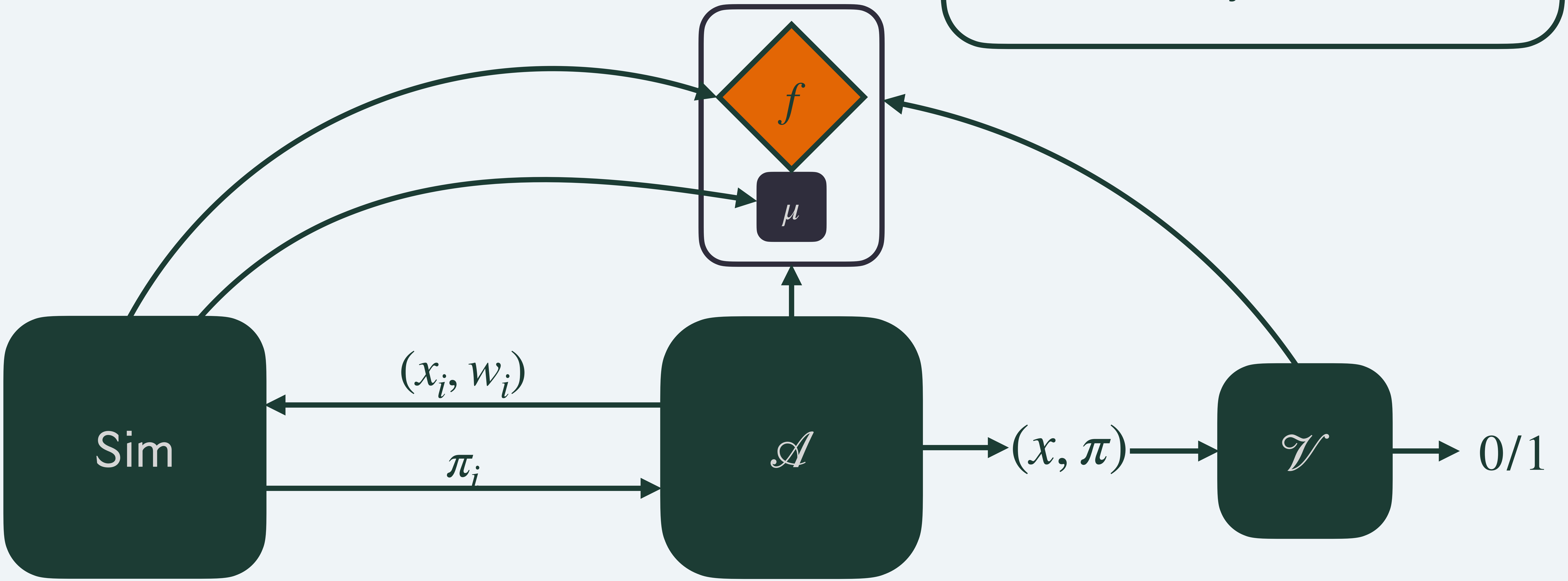
Sim answers with π_i only if $(x_i, w_i) \in \mathscr{R}$.



Simulation Security

“Any” Simulation Security:

Sim answers with π_i unconditionally

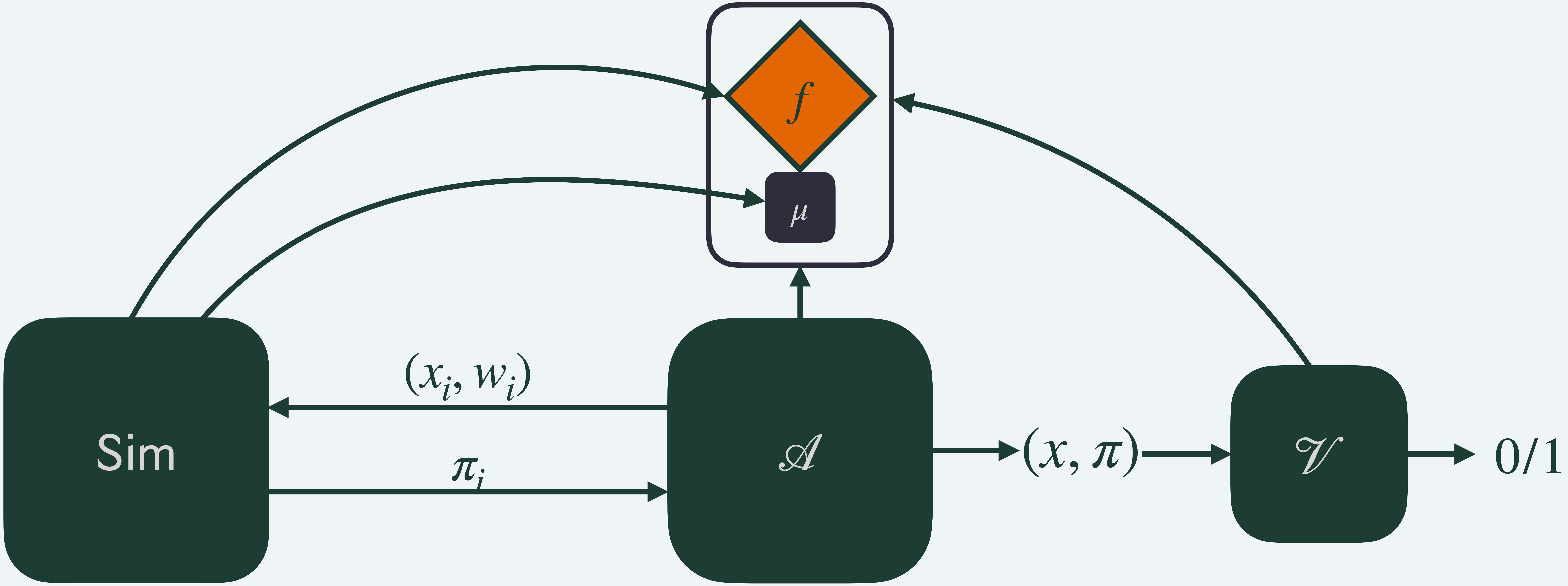


Overview

- Motivation
- Preliminaries
- ▸ **Results**
- Construction:
  Encryption Scheme in the ROM

Simulation Security

Definitions



Simulation Security

Definitions

Simulation Soundness

The probability that $\mathscr{A}$ outputs (x, π) s.t. $\mathscr{V}$ accepts, but $x \notin \mathscr{L}(\mathscr{R})$ is at most $\epsilon_{\text{ARG}}^{\text{SIM}}$.

Simulation Security

Definitions

Simulation Soundness

The probability that $\mathscr{A}$ outputs (x, π) s.t. $\mathscr{V}$ accepts, but $x \notin \mathscr{L}(\mathscr{R})$ is at most $\epsilon_{\mathrm{ARG}}^{\mathrm{SIM}}$.

Simulation Knowledge Soundness

The probability that $\mathscr{A}$ outputs (x, π) s.t. $\mathscr{V}$ accepts, but $\mathscr{A}$ does not know a witness w s.t. $(x, w) \in \mathscr{R}$ is at most $\kappa_{\mathrm{ARG}}^{\mathrm{SIM}}$.

Simulation Security

Definitions

Computational variants

Simulation Soundness

The probability that $\mathscr{A}$ outputs (x, π) s.t. $\mathscr{V}$ accepts, but $x \notin \mathscr{L}(\mathscr{R})$ is at most $\epsilon_{\mathrm{ARG}}^{\mathrm{SIM}}$.

Simulation Knowledge Soundness

The probability that $\mathscr{A}$ outputs (x, π) s.t. $\mathscr{V}$ accepts, but $\mathscr{A}$ does not know a witness w s.t. $(x, w) \in \mathscr{R}$ is at most $\kappa_{\mathrm{ARG}}^{\mathrm{SIM}}$.

Cryptographic primitives

Cryptographic primitives

We formalize:

Cryptographic primitives

We formalize:

(1) The notion of a signature scheme in the ROM; and

Cryptographic primitives

We formalize:

(1) The notion of a signature scheme in the ROM; and

(2) The notion of an encryption scheme in the ROM.

Cryptographic primitives

We formalize:

(1) The notion of a signature scheme in the ROM; and

(2) The notion of an encryption scheme in the ROM.

We construct:

Cryptographic primitives

We formalize:

(1) The notion of a signature scheme in the ROM; and

(2) The notion of an encryption scheme in the ROM.

We construct:

(1) An EUF-CMA secure signature scheme; and

Cryptographic primitives

We formalize:

(1) The notion of a signature scheme in the ROM; and

(2) The notion of an encryption scheme in the ROM.

We construct:

(1) An EUF-CMA secure signature scheme; and

(2) A CCA-2 secure encryption scheme.

Overview

- Motivation
- Preliminaries
- Results
- ▸ Construction:
  Encryption Scheme in the ROM

Encryption scheme in the ROM

Definition

$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$

Encryption scheme in the ROM

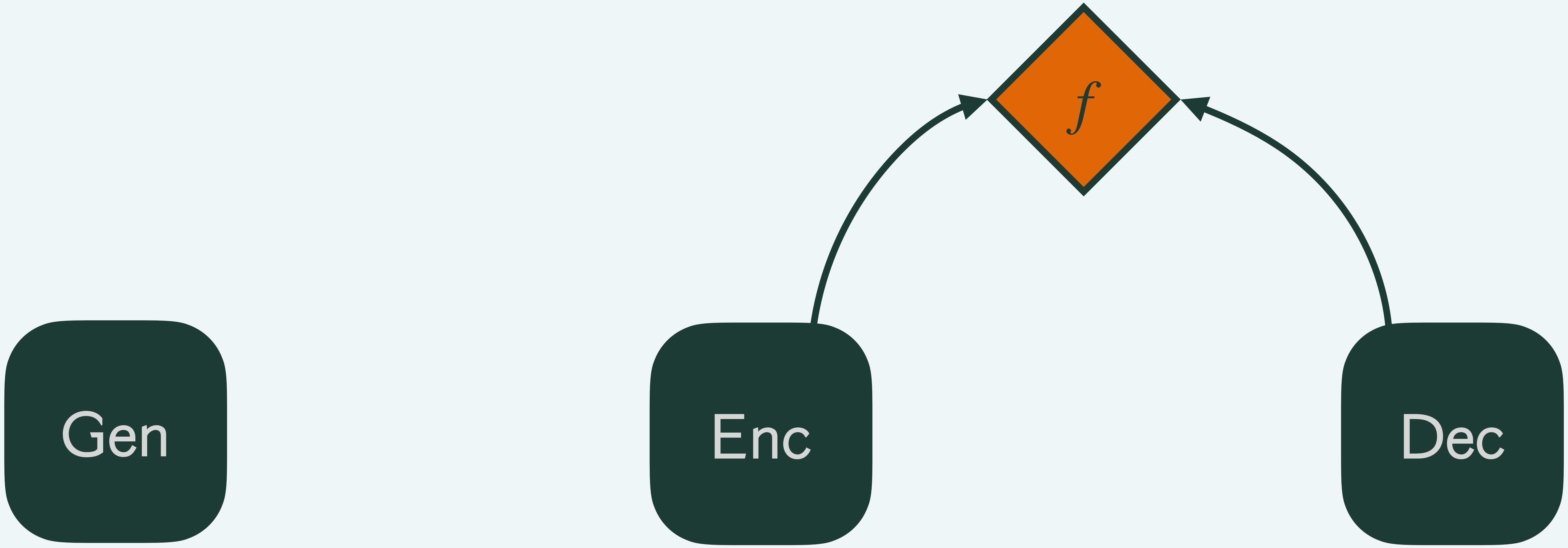
Definition

$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$

Encryption scheme in the ROM

Definition

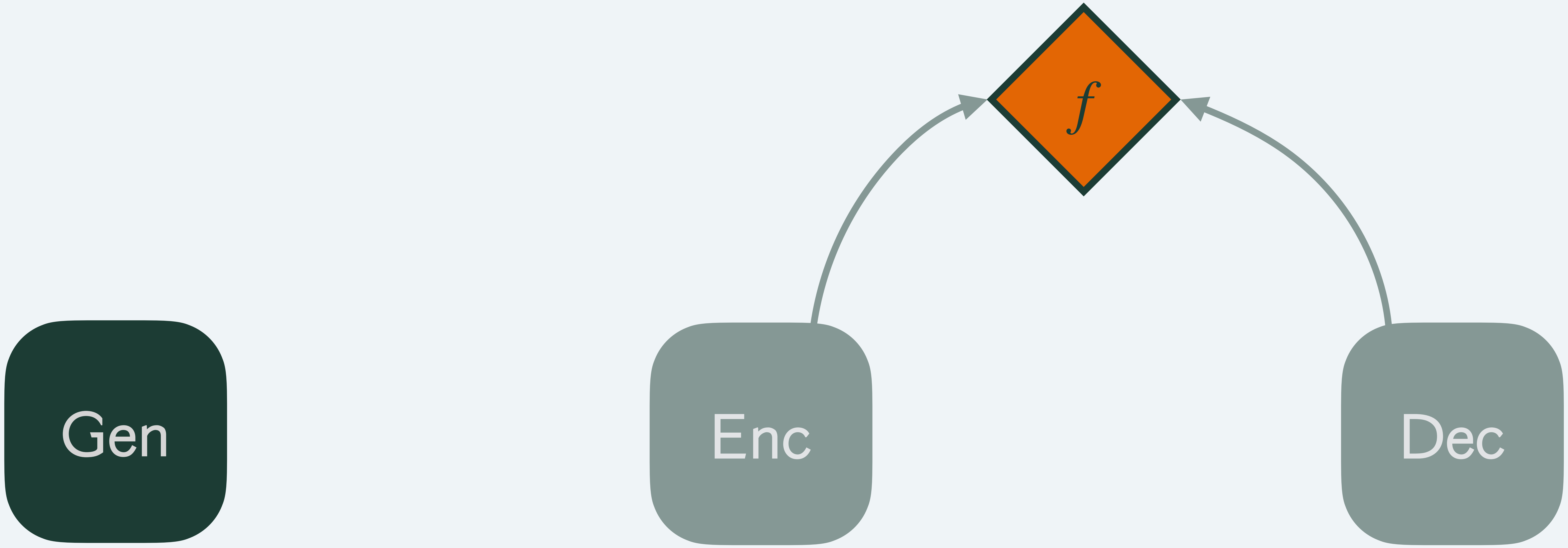
$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$



Encryption scheme in the ROM

Definition

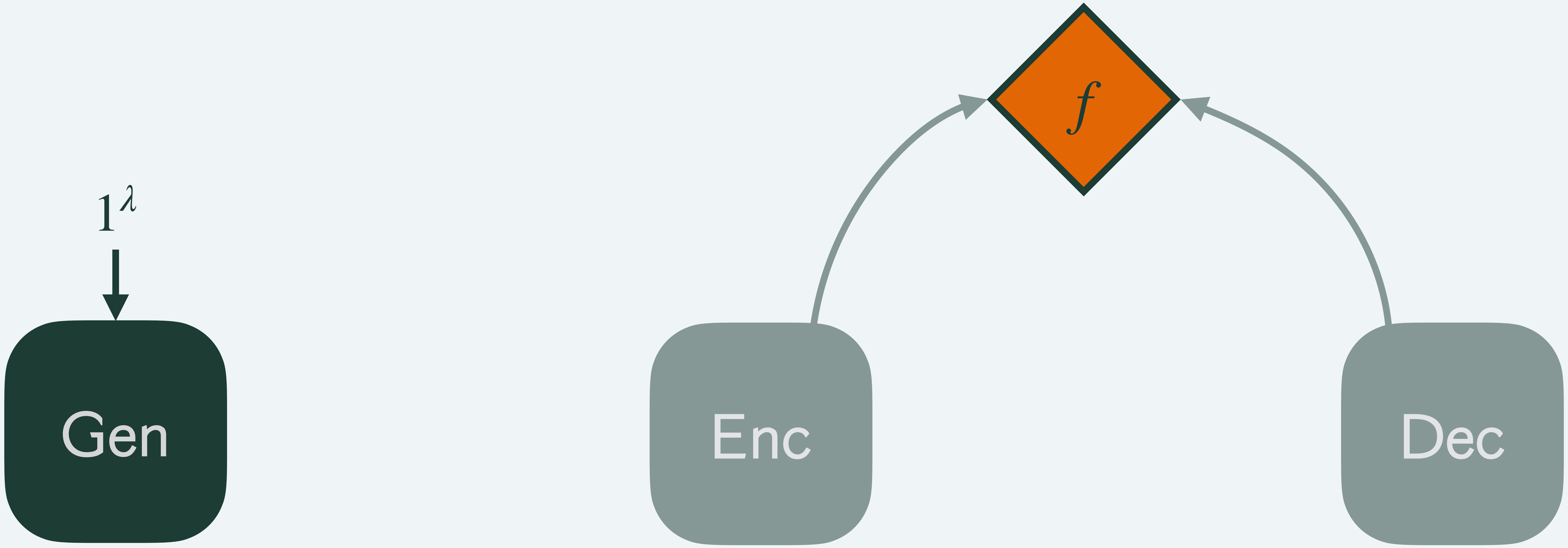
$\mathrm{ENC}[\lambda, \ell, \ell_c] = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$



Encryption scheme in the ROM

Definition

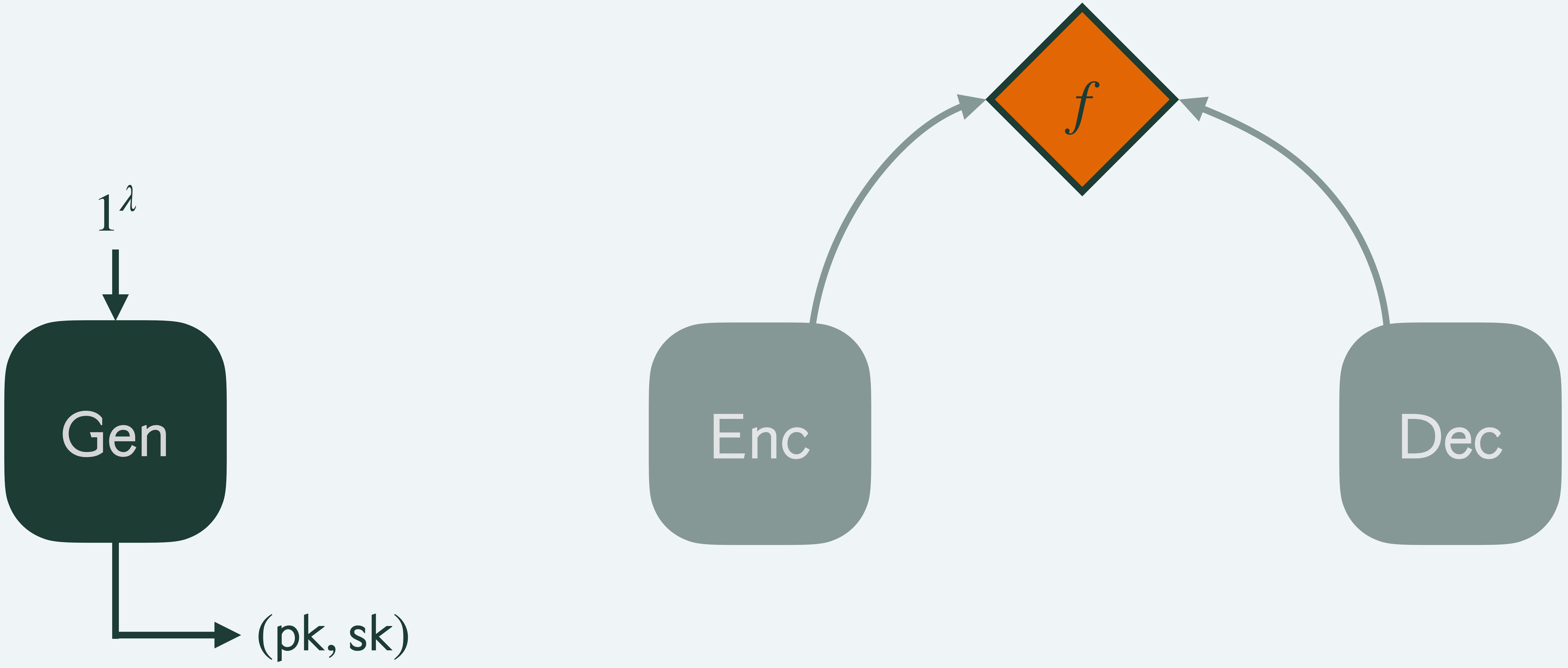
$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$



Encryption scheme in the ROM

Definition

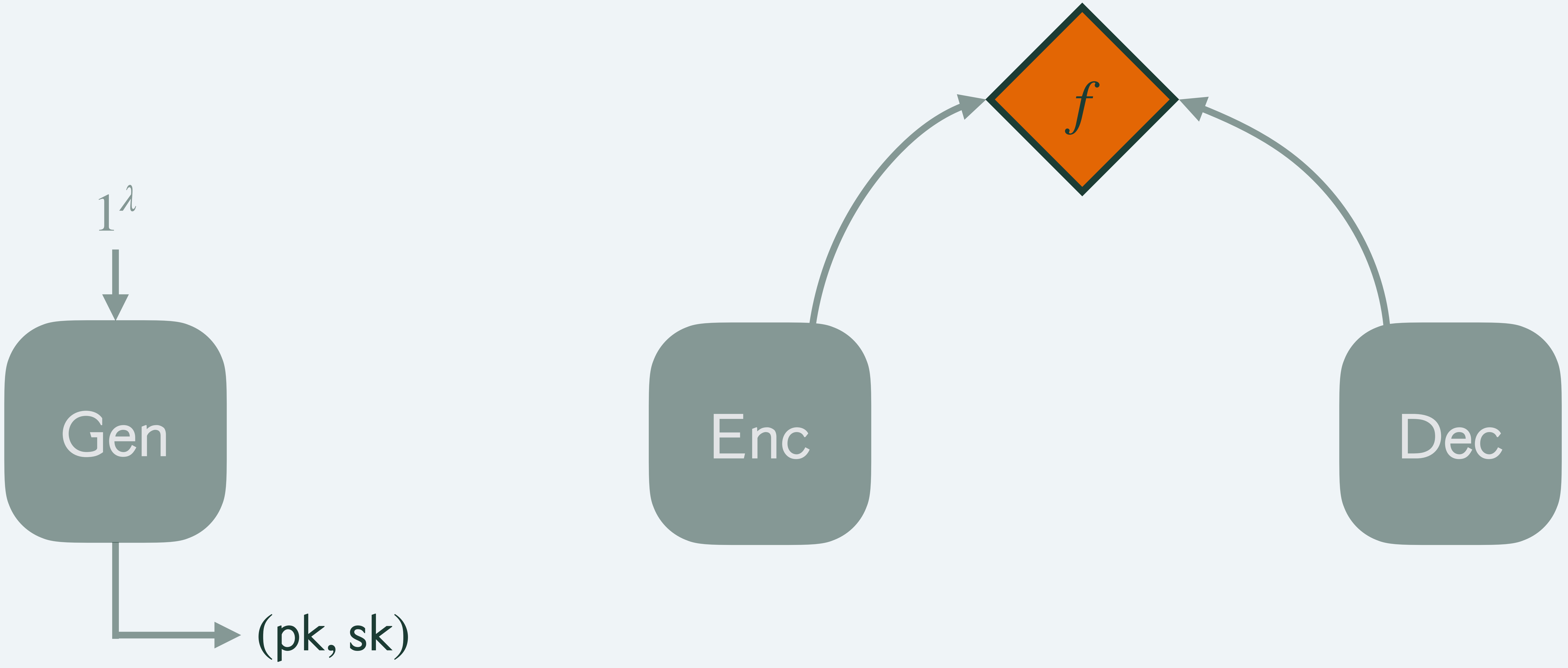
$\mathrm{ENC}[\lambda, \ell, \ell_c] = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$



Encryption scheme in the ROM

Definition

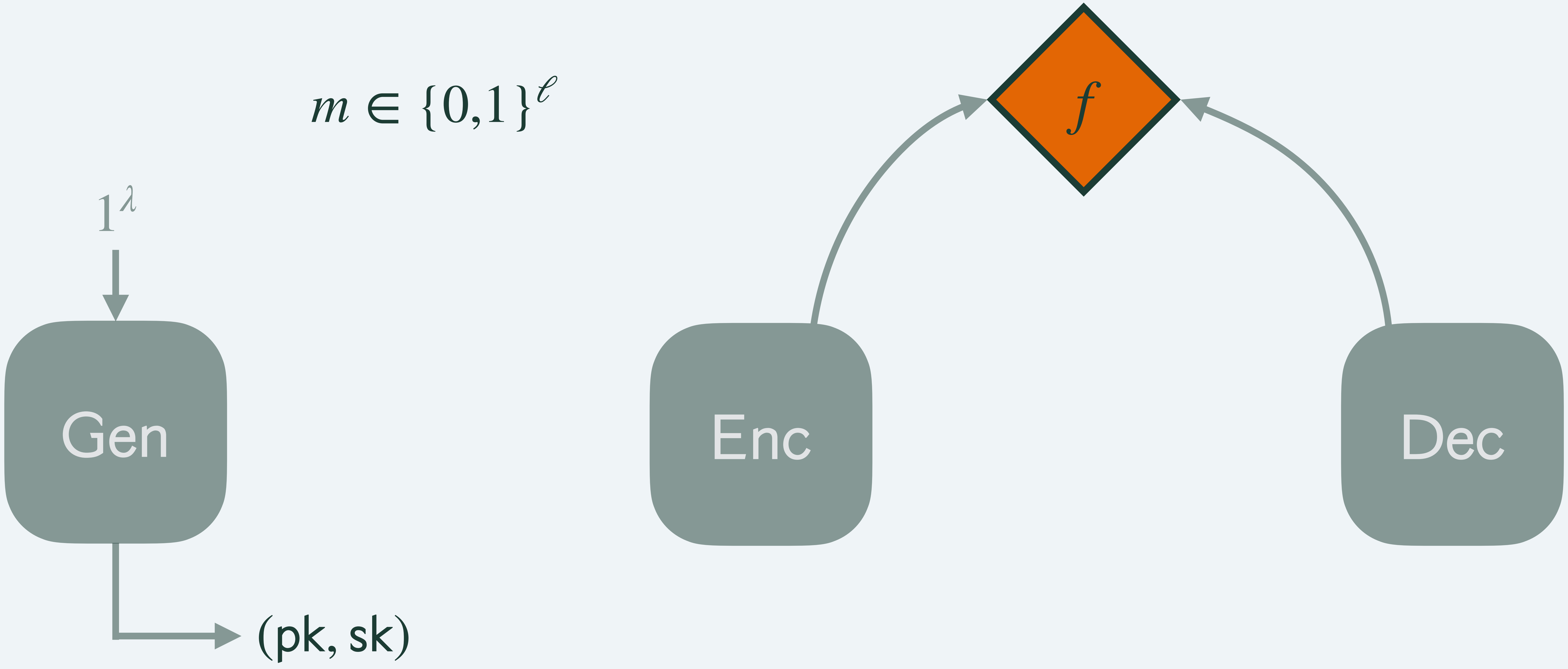
$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$



Encryption scheme in the ROM

Definition

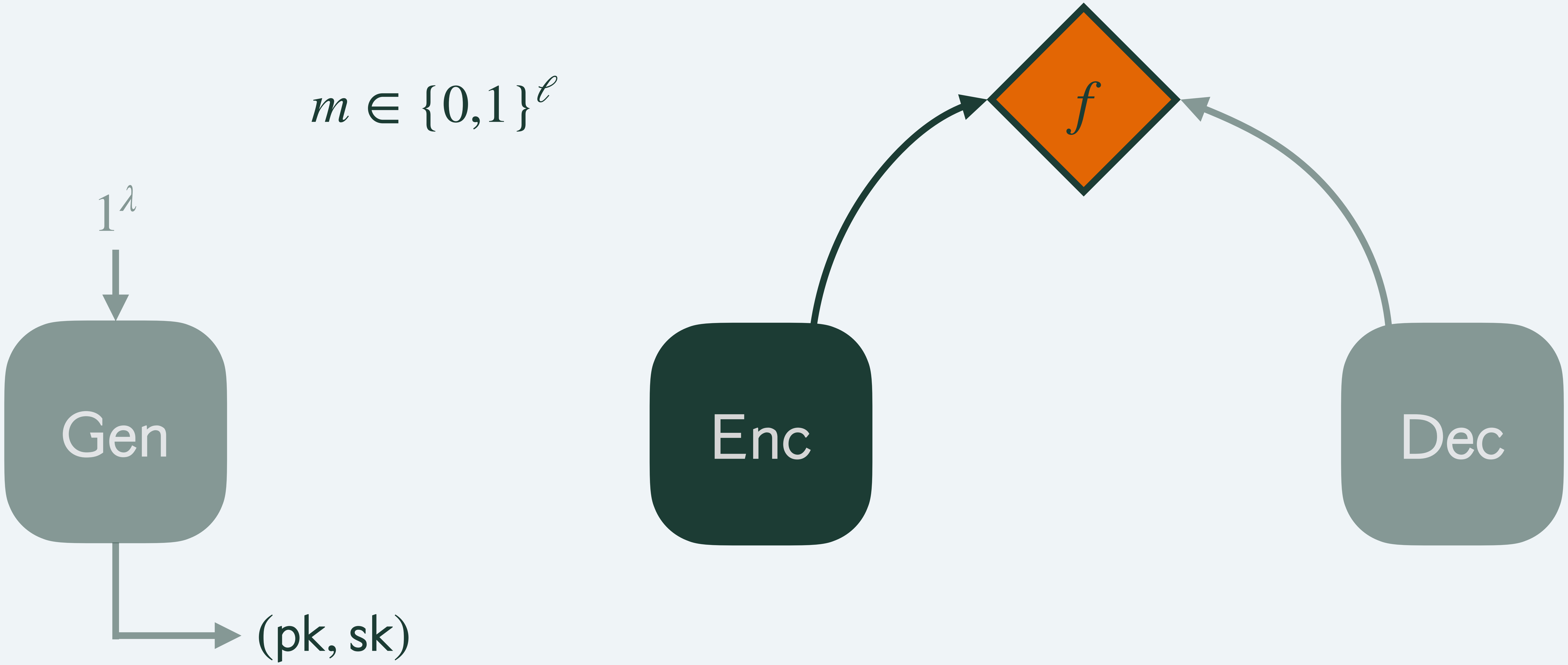
$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$



Encryption scheme in the ROM

Definition

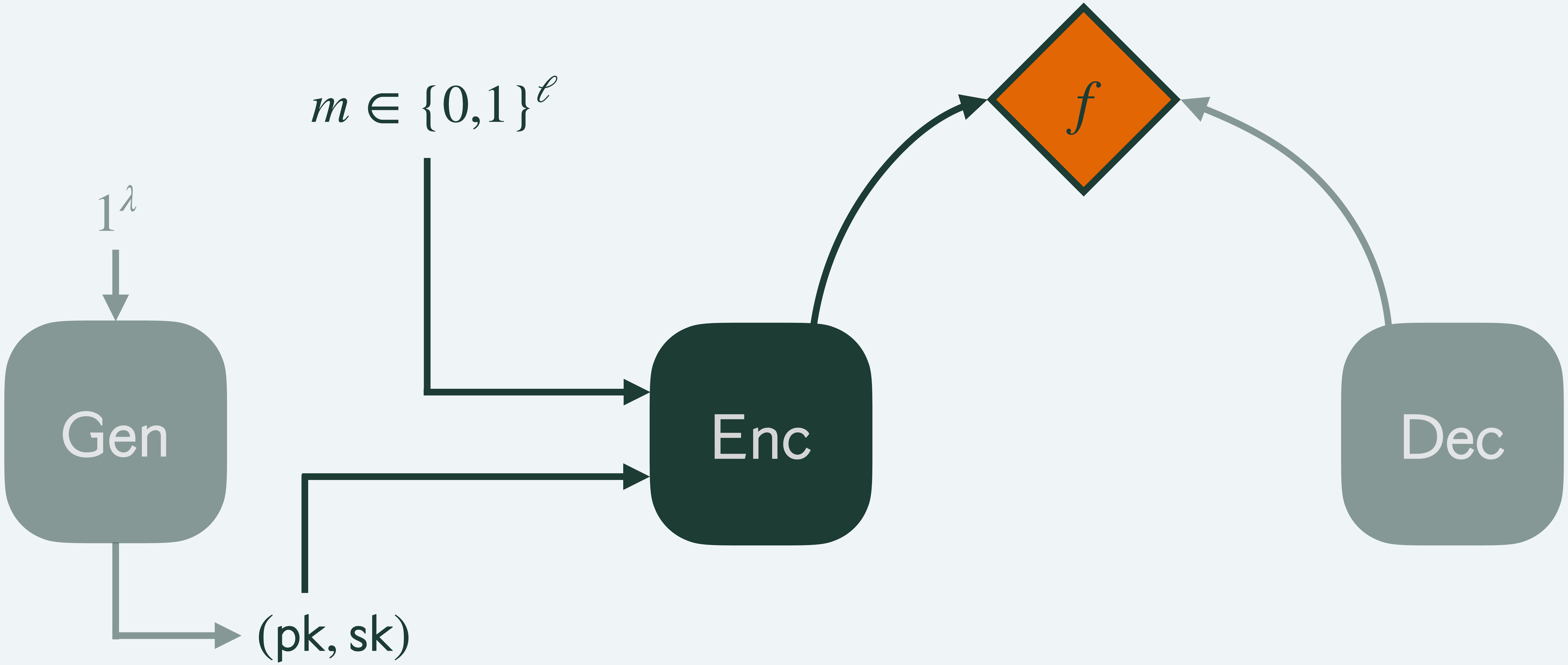
$\mathrm{ENC}[\lambda, \ell, \ell_c] = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$



Encryption scheme in the ROM

Definition

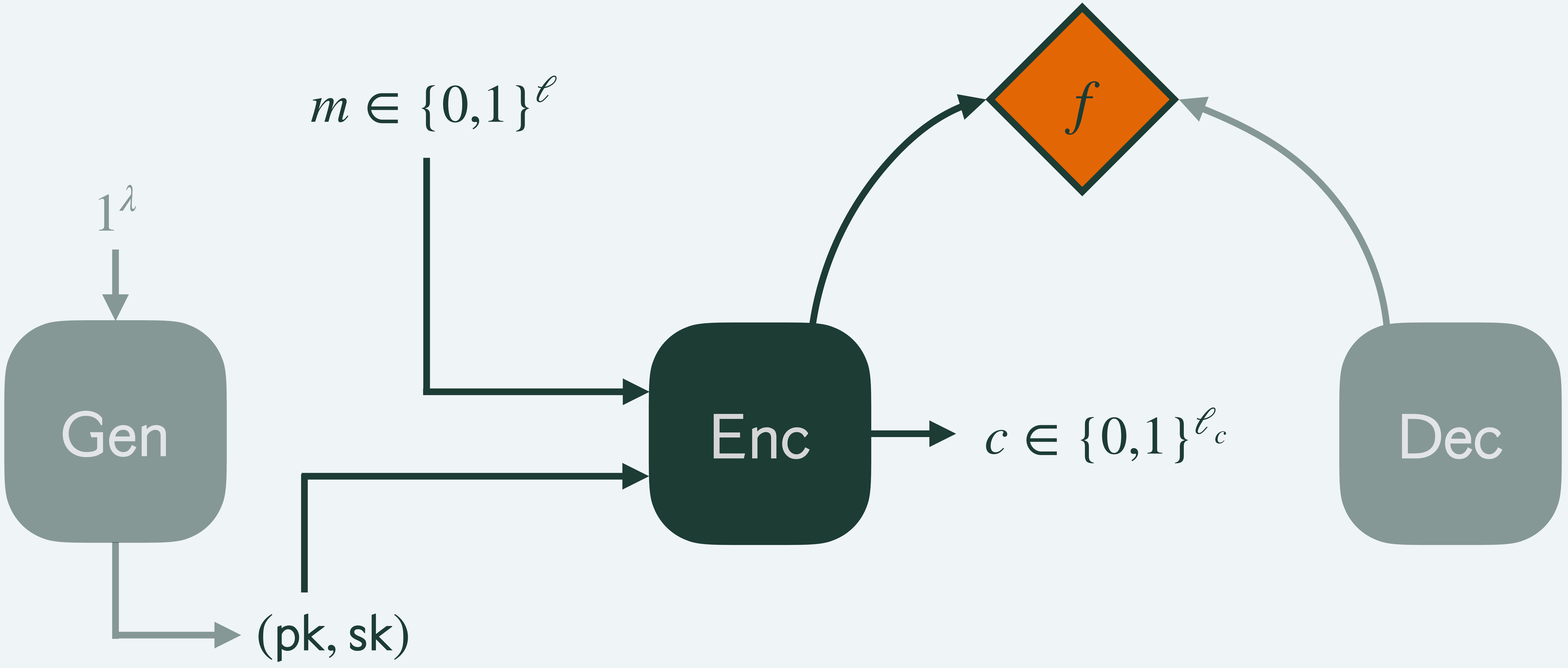
$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$



Encryption scheme in the ROM

Definition

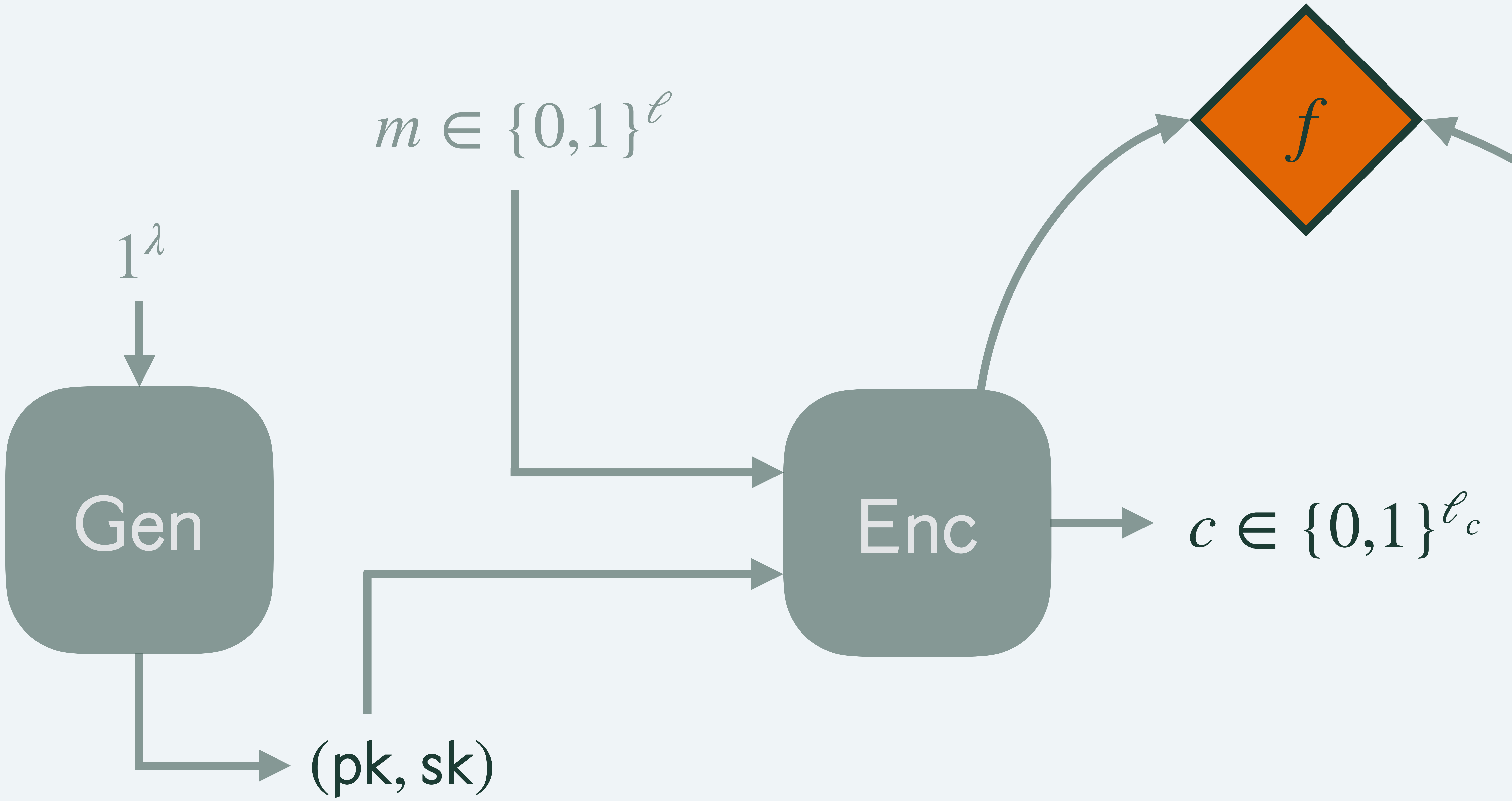
$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$



Encryption scheme in the ROM

Definition

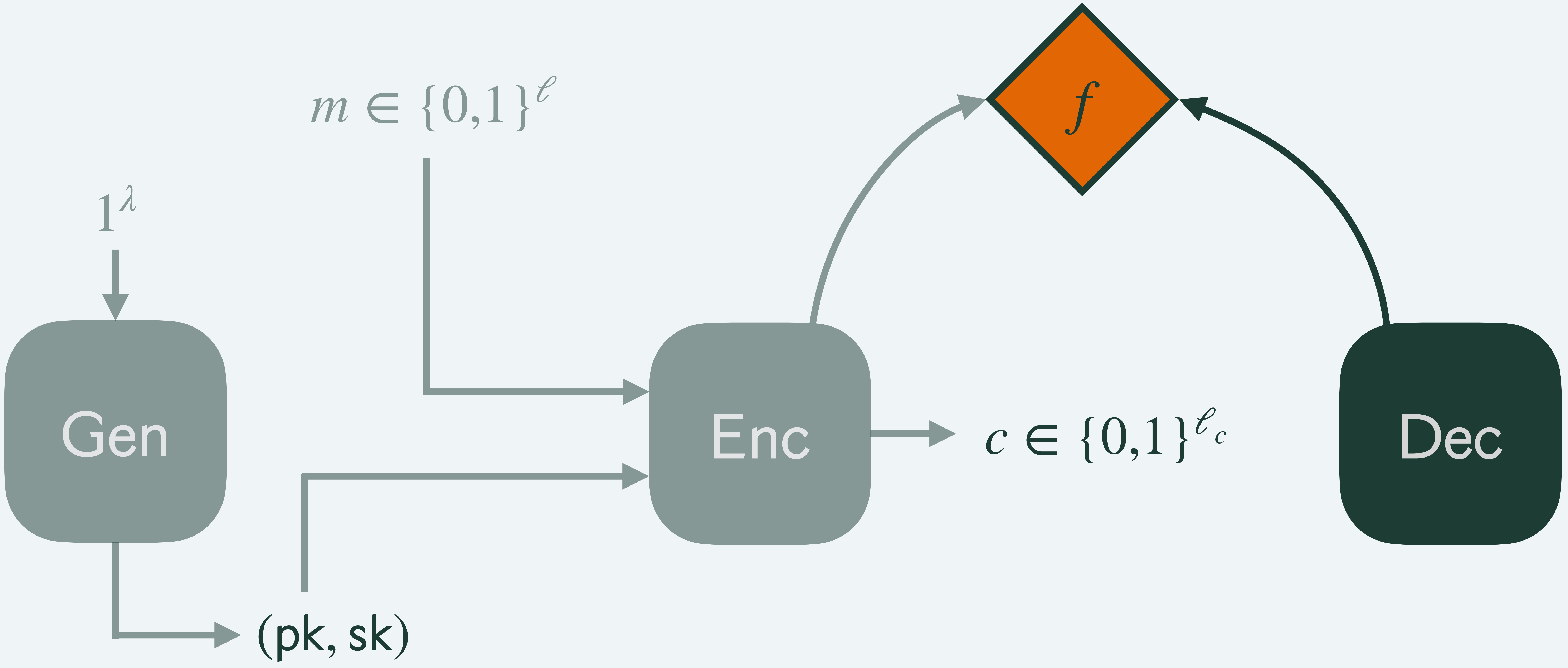
$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$



Encryption scheme in the ROM

Definition

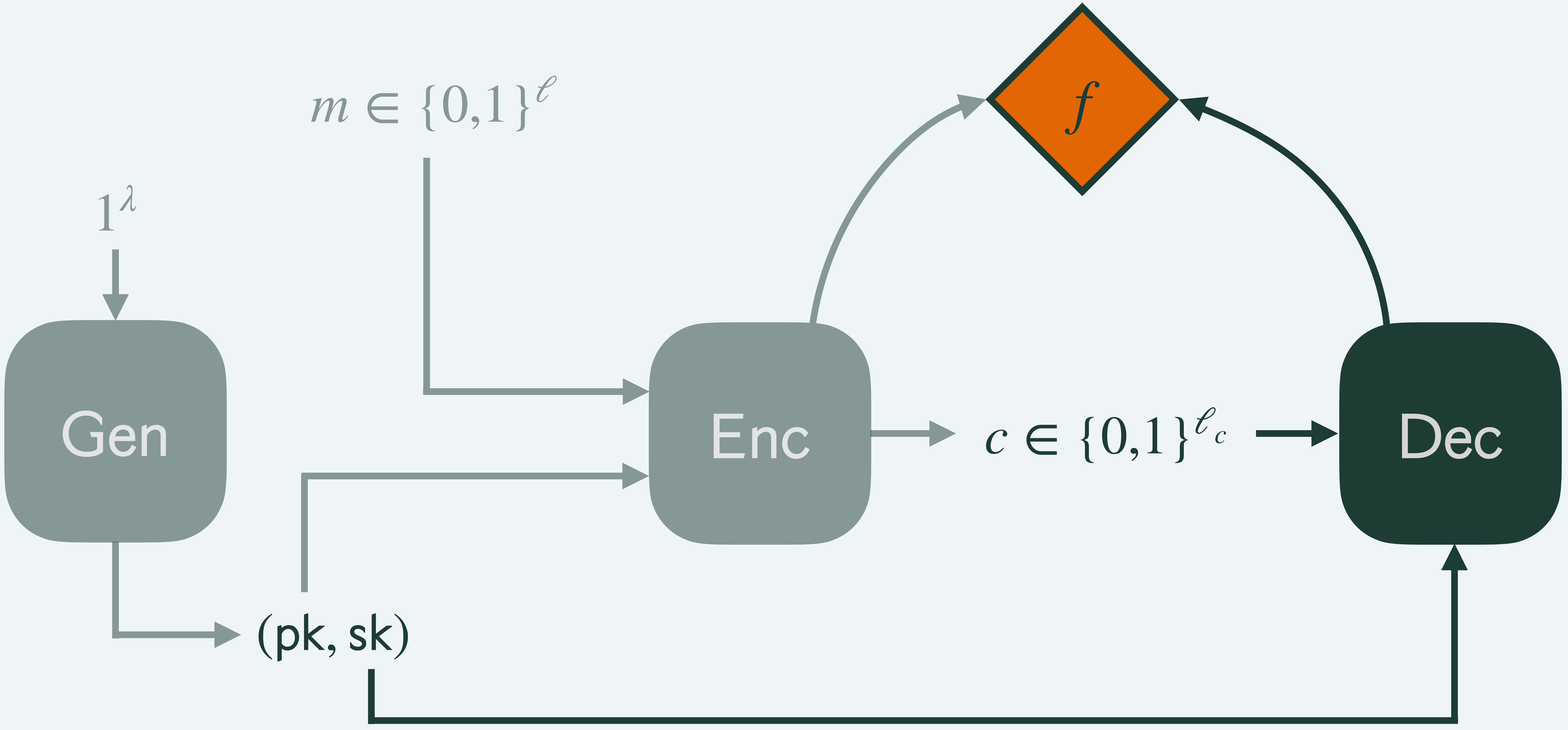
$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$



Encryption scheme in the ROM

Definition

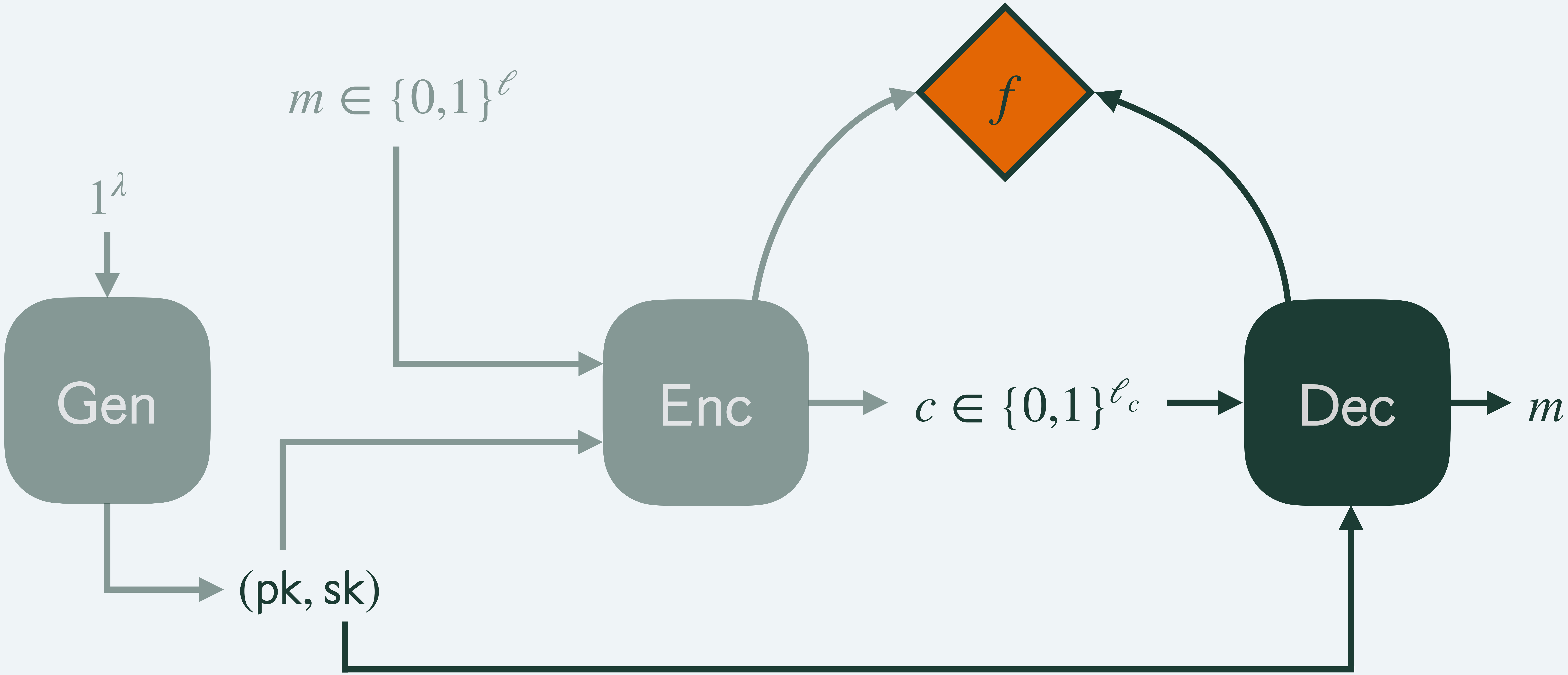
$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$



Encryption scheme in the ROM

Definition

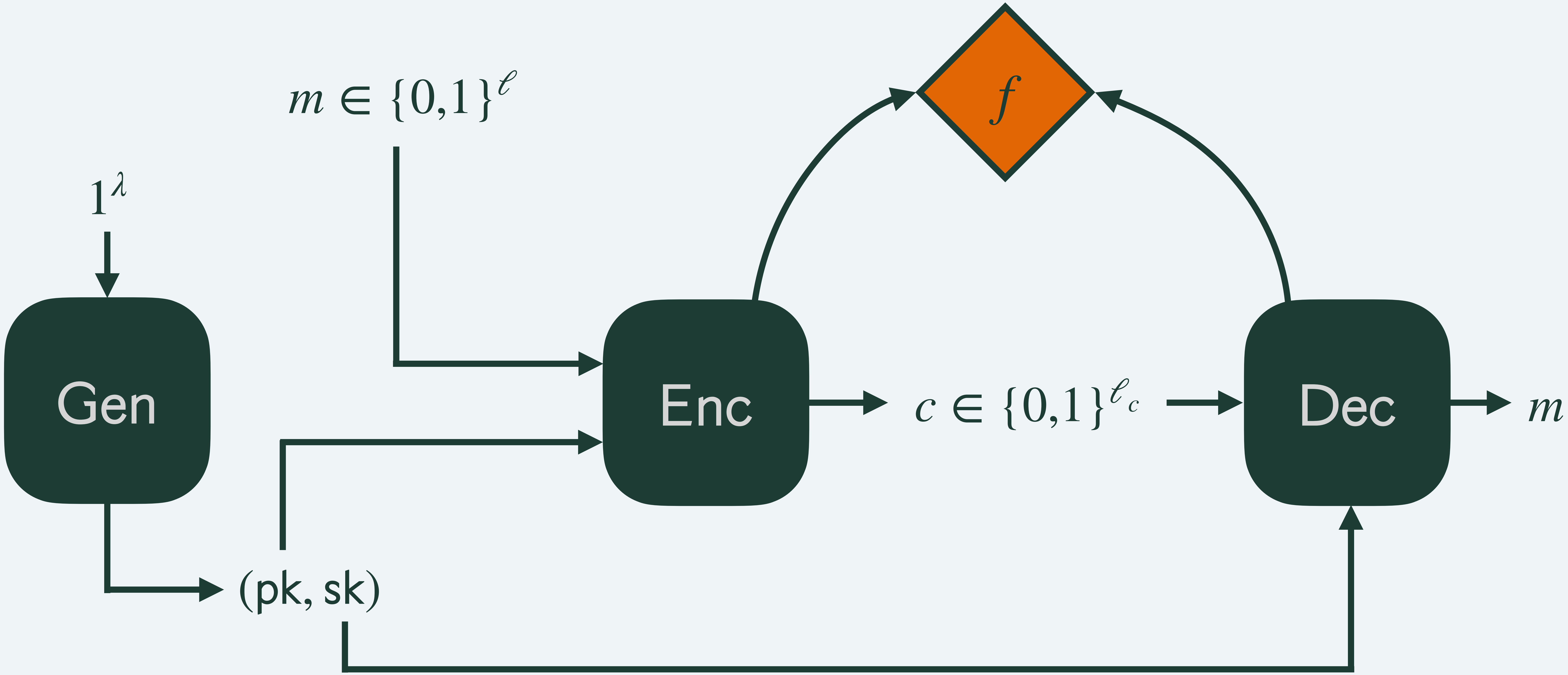
$\mathrm{ENC}[\lambda, \ell, \ell_c] = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$



Encryption scheme in the ROM

Security Properties: Completeness

$\mathsf{ENC}[\lambda, \ell, \ell_c] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$

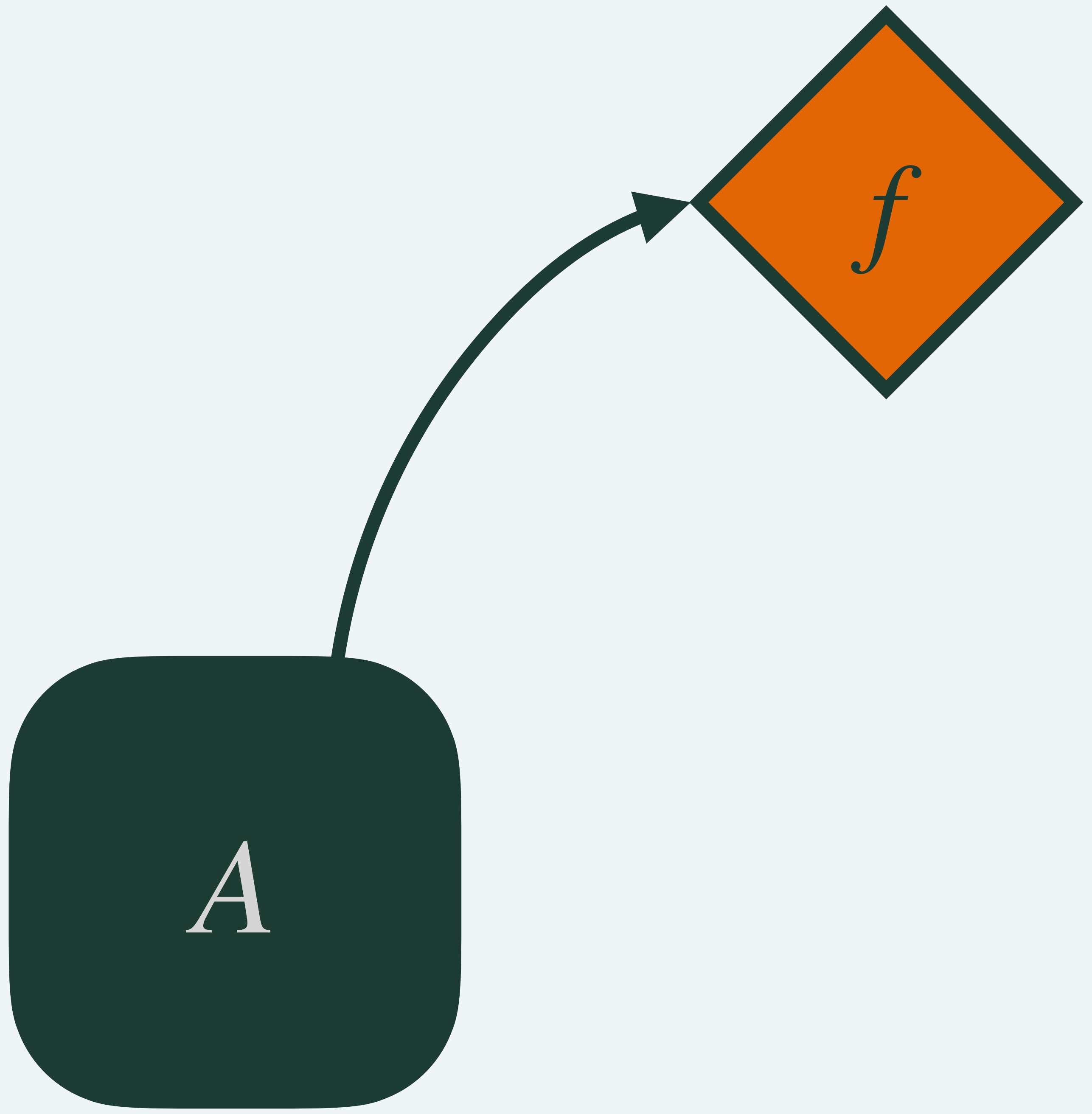


Encryption scheme in the ROM

Security Properties: CPA Security

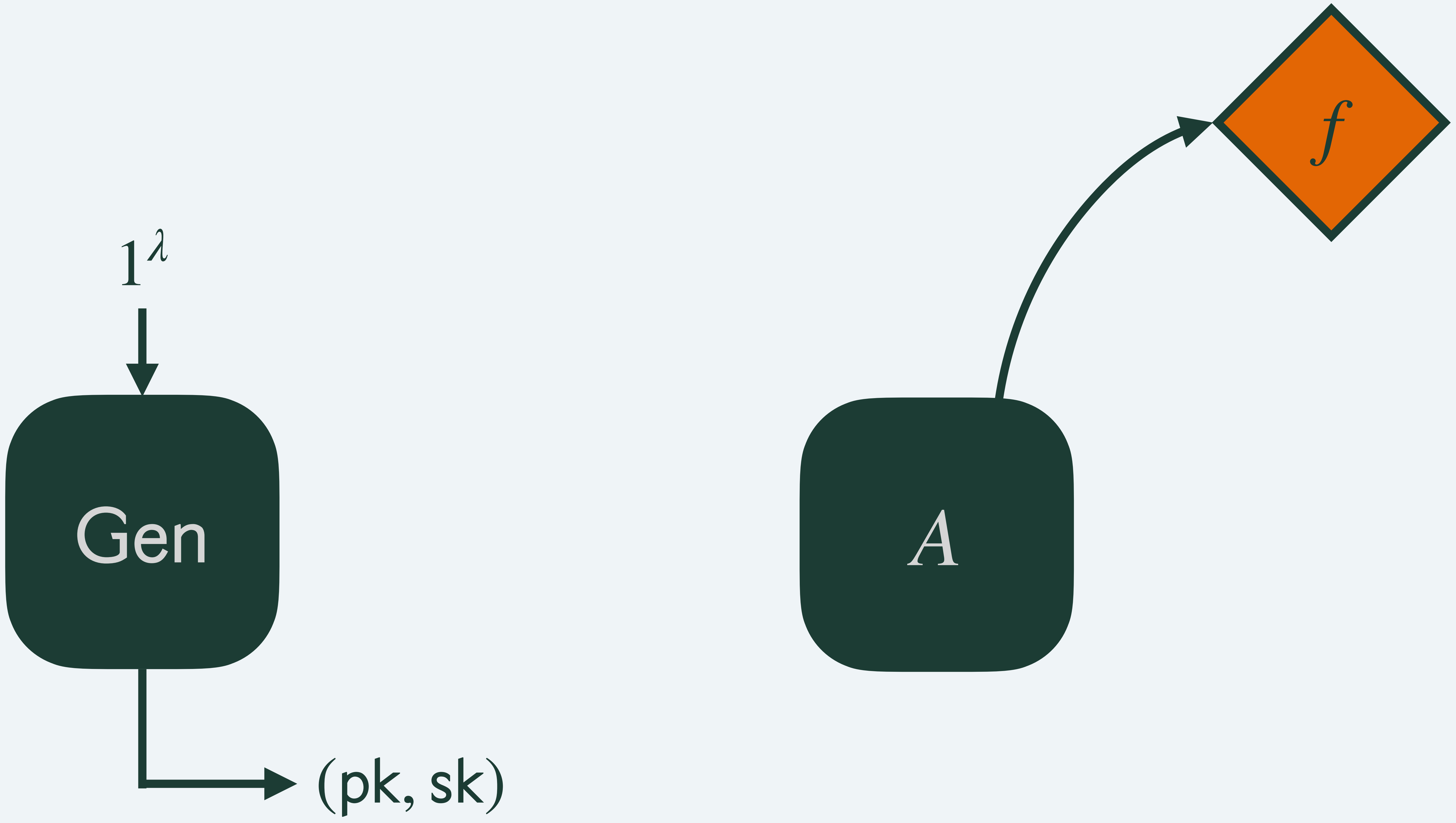
Encryption scheme in the ROM

Security Properties: CPA Security



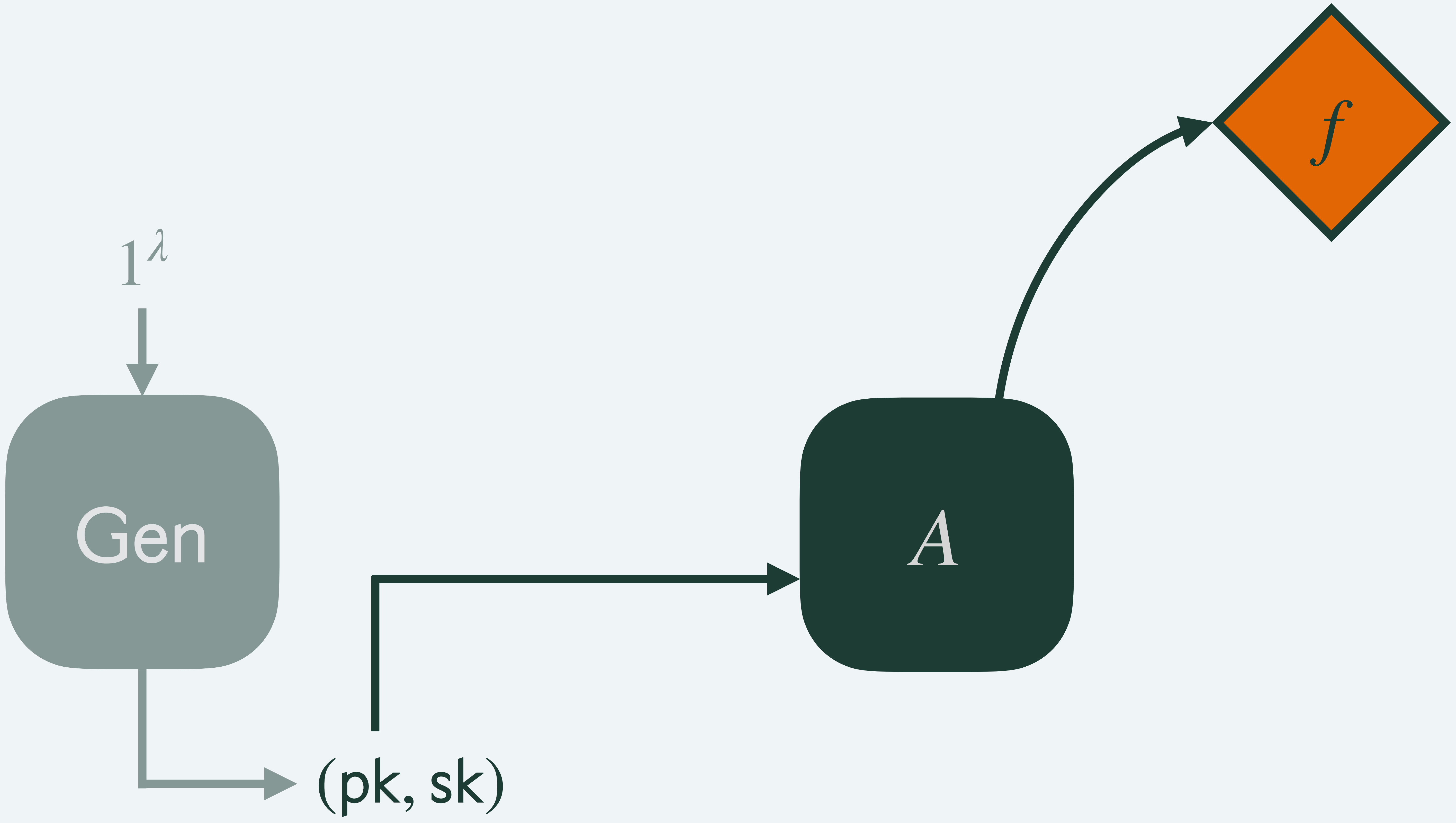
Encryption scheme in the ROM

Security Properties: CPA Security



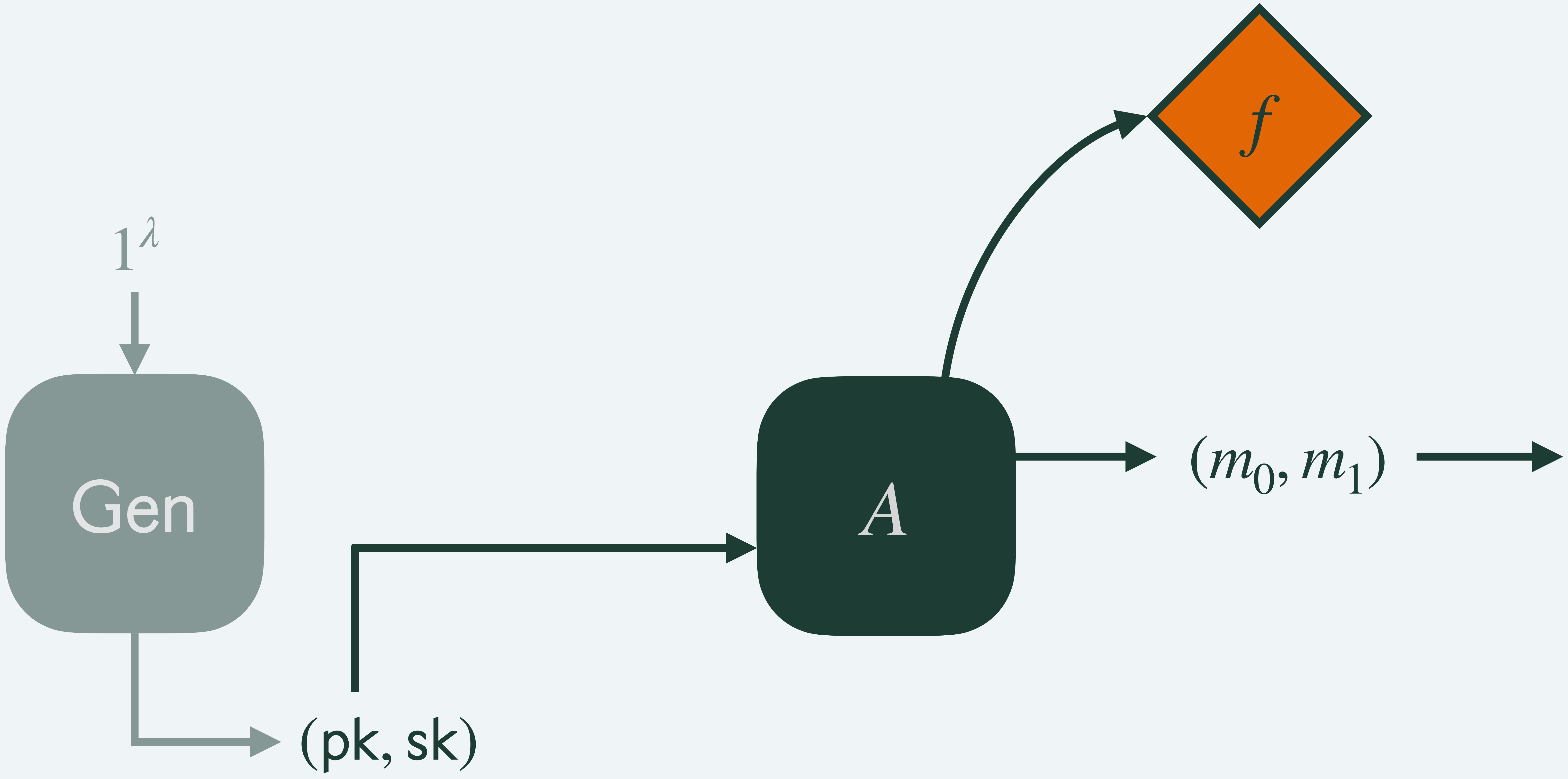
Encryption scheme in the ROM

Security Properties: CPA Security



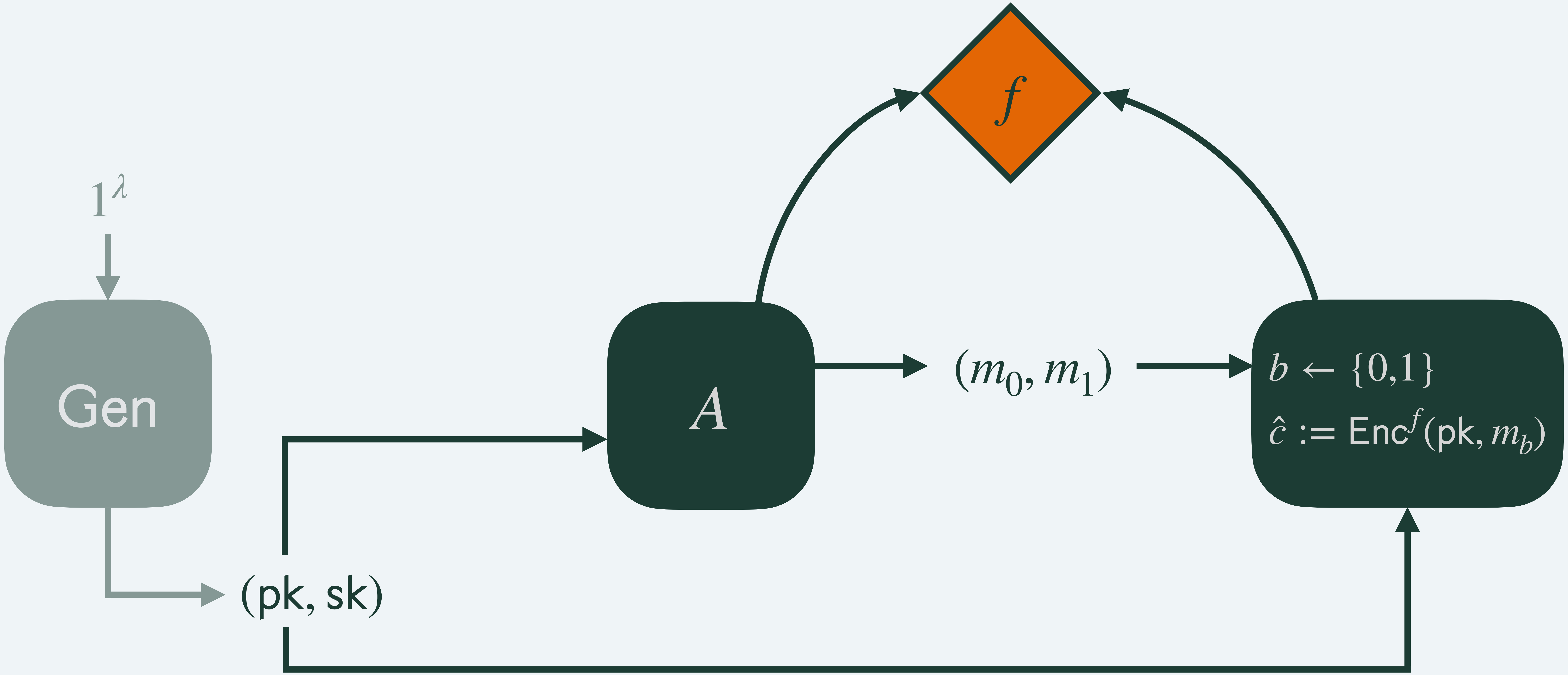
Encryption scheme in the ROM

Security Properties: CPA Security



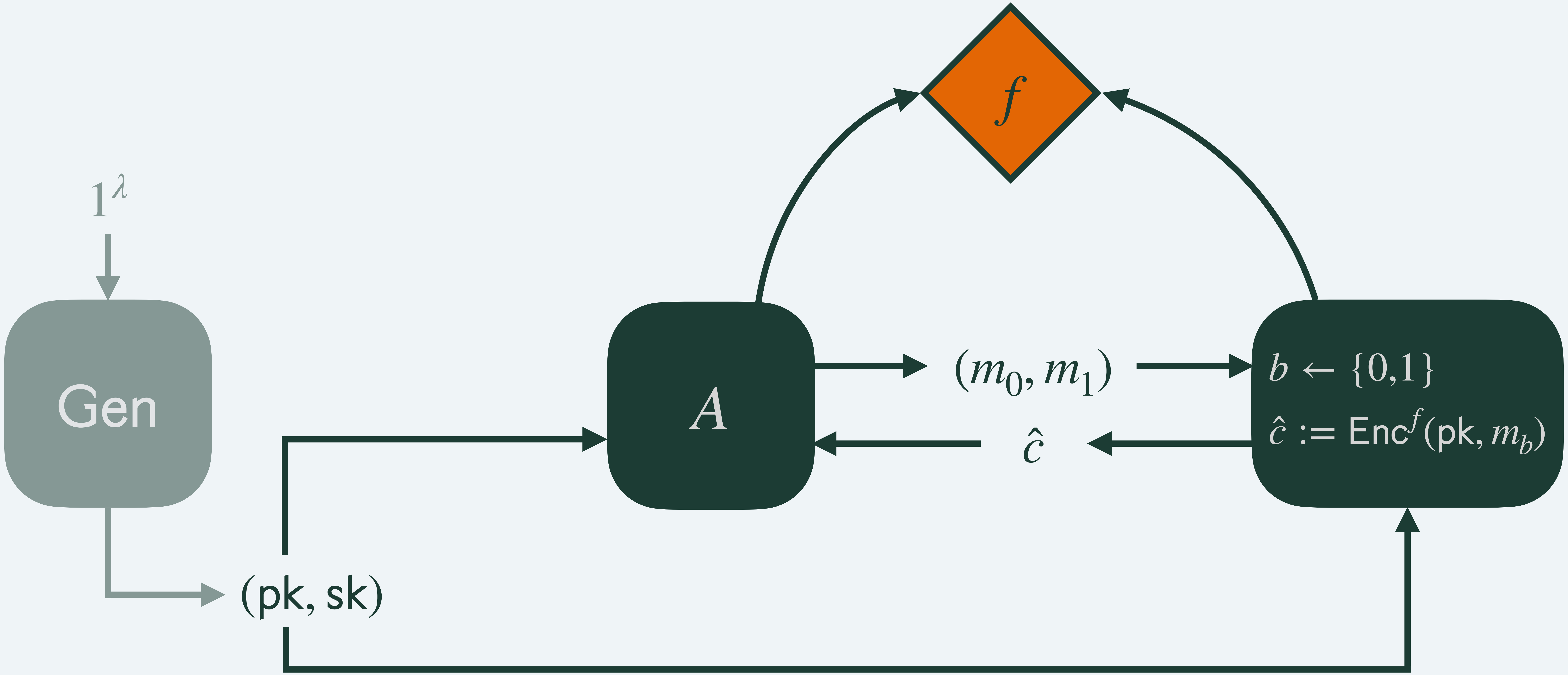
Encryption scheme in the ROM

Security Properties: CPA Security



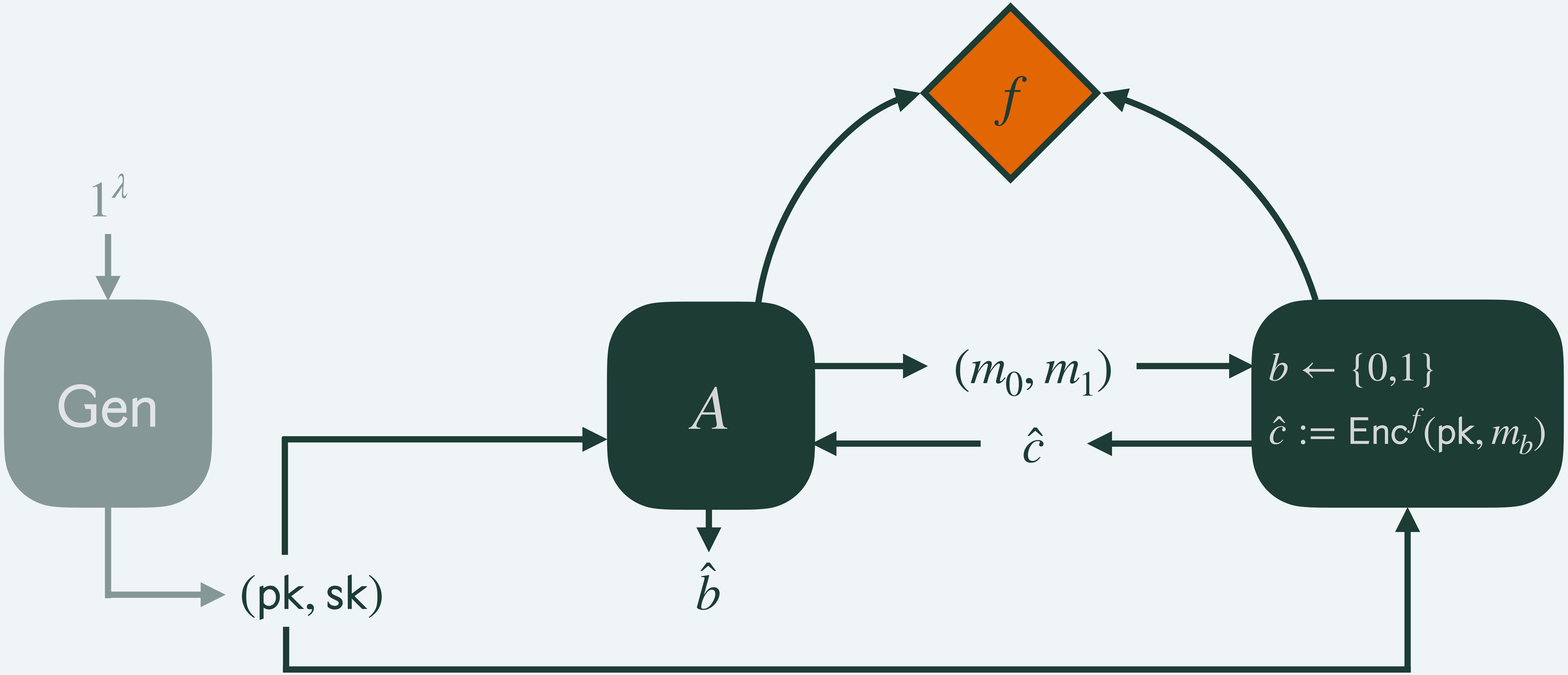
Encryption scheme in the ROM

Security Properties: CPA Security



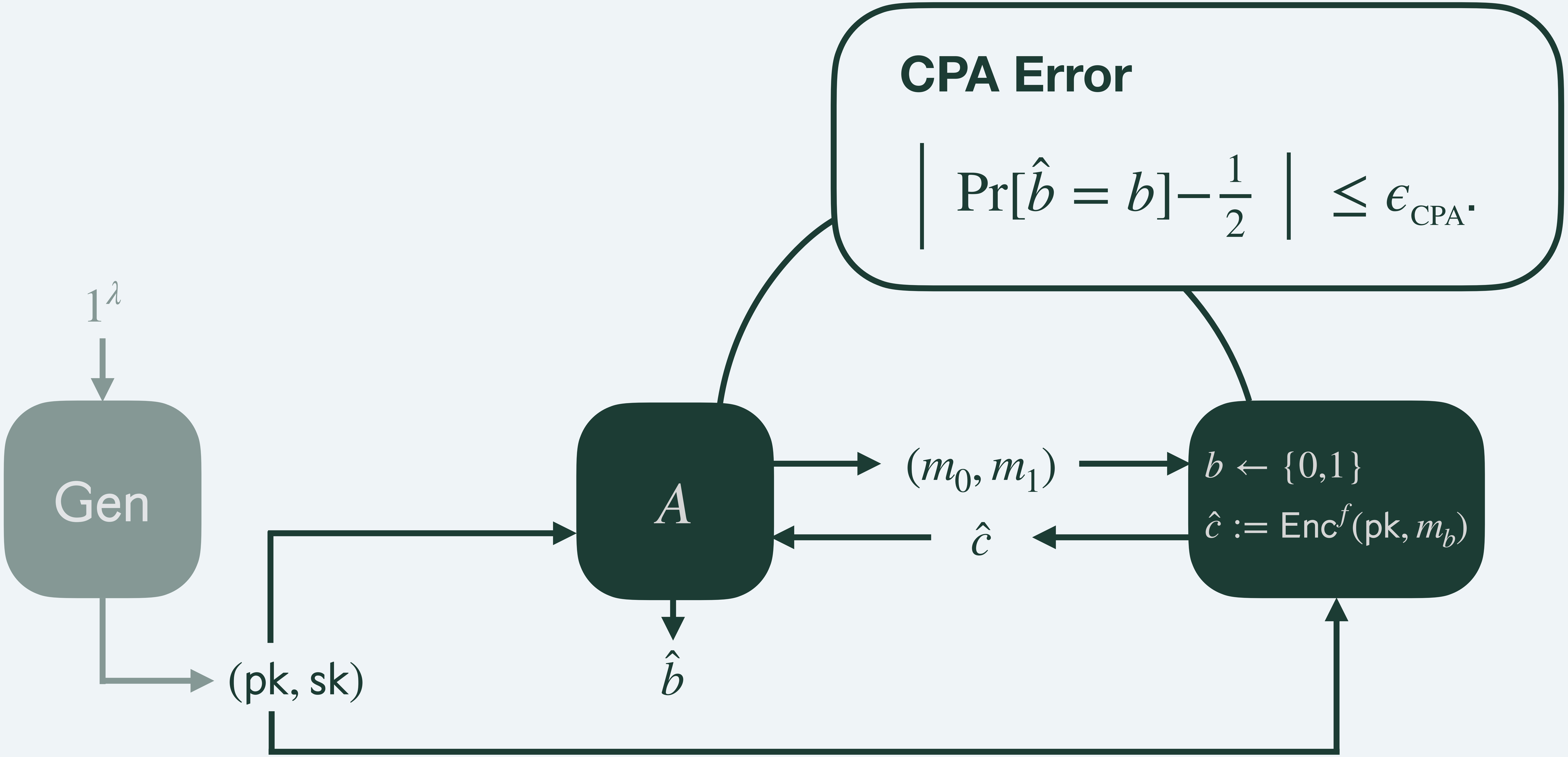
Encryption scheme in the ROM

Security Properties: CPA Security



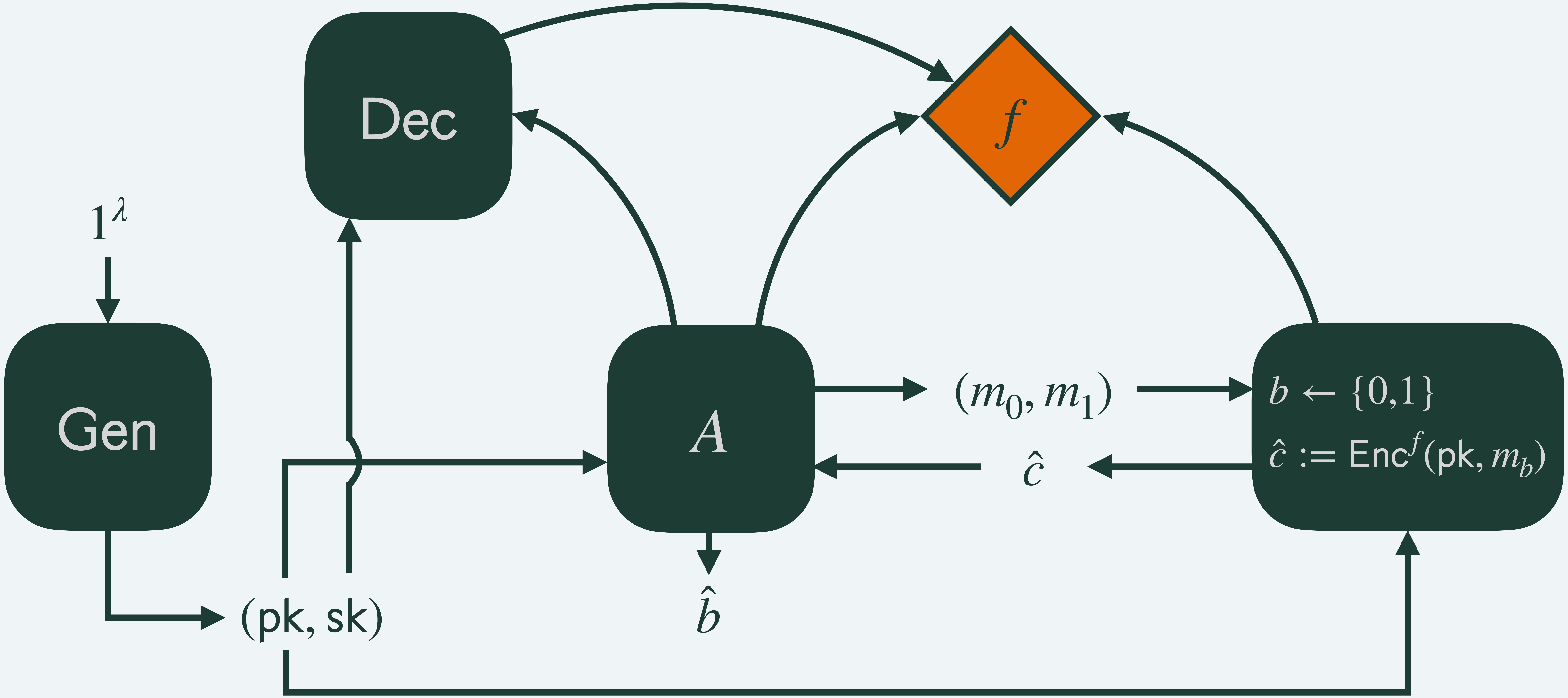
Encryption scheme in the ROM

Security Properties: CPA Security



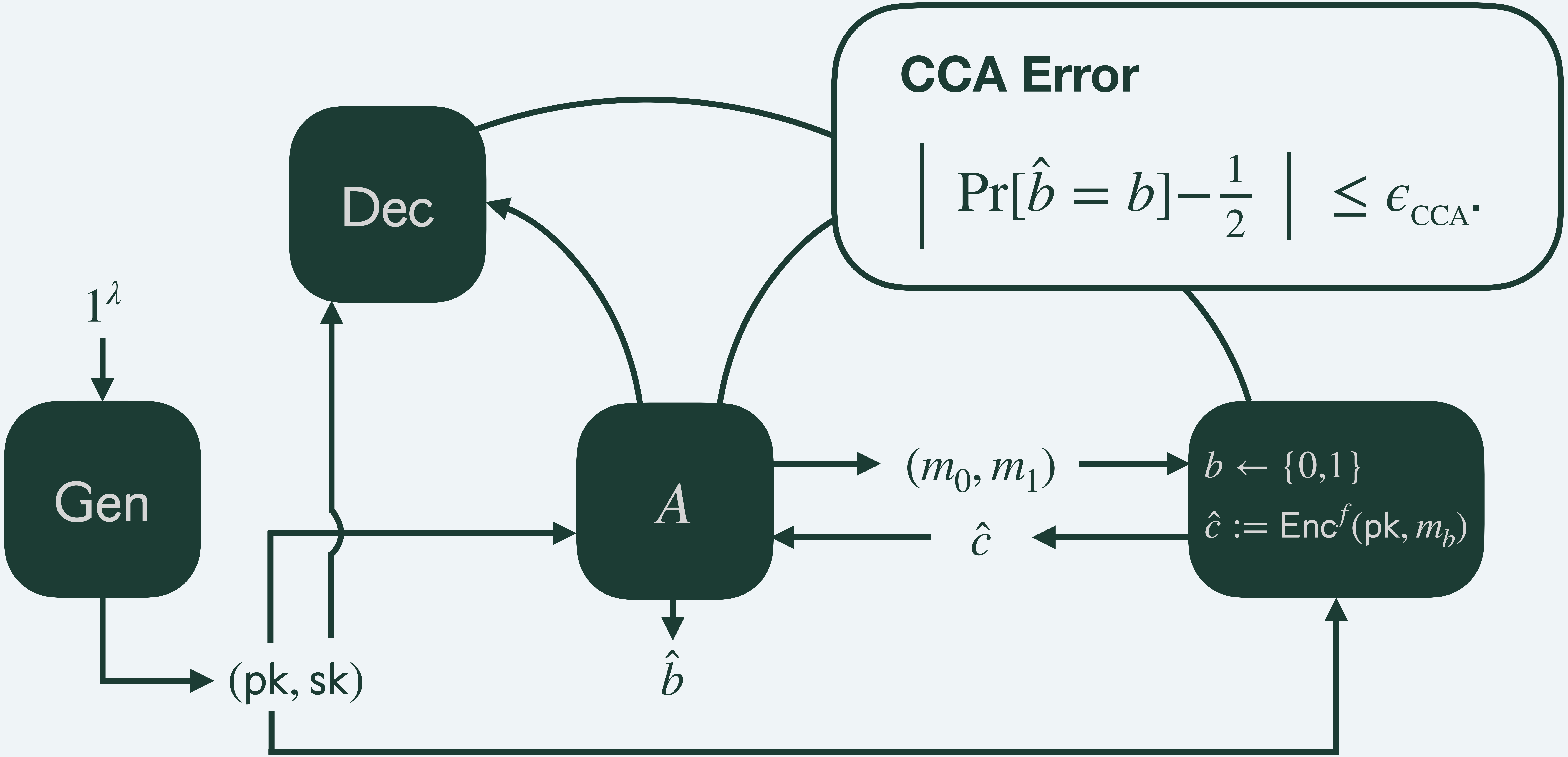
Encryption scheme in the ROM

Security Properties: CCA Security



Encryption scheme in the ROM

Security Properties: CCA Security



Encryption scheme in the ROM

Construction

Encryption scheme in the ROM

Construction

Ingredients:

Encryption scheme in the ROM

Construction

Ingredients:

- A CPA Secure Encryption Scheme; and

Encryption scheme in the ROM

Construction

Ingredients:

- A CPA Secure Encryption Scheme; and
- A NARG for the relation

Encryption scheme in the ROM

Construction

Ingredients:

- A CPA Secure Encryption Scheme; and
- A NARG for the relation

$$\mathcal{R}_\ell := \left\{ \big((\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1), (\rho_0, m_0, \rho_1, m_1)\big) \;\middle|\; \begin{array}{l} m_0, m_1 \in \{0,1\}^\ell \\ \wedge\, m_0 = m_1 \\ \wedge\, c_0 = \mathsf{ENC}.\mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_0, m_0; \rho_0) \\ \wedge\, c_1 = \mathsf{ENC}.\mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_1, m_1; \rho_1) \end{array} \right\}.$$

Encryption scheme in the ROM

Construction

NARG **needs to satisfy:**

$$\mathscr{R}_\ell := \left\{ \big((\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1), (\rho_0, m_0, \rho_1, m_1)\big) \;\middle|\; \begin{array}{l} m_0, m_1 \in \{0,1\}^\ell \\ \wedge\, m_0 = m_1 \\ \wedge\, c_0 = \mathsf{ENC}\,.\,\mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_0, m_0; \rho_0) \\ \wedge\, c_1 = \mathsf{ENC}\,.\,\mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_1, m_1; \rho_1) \end{array} \right\}.$$

Encryption scheme in the ROM

Construction

NARG **needs to satisfy**:

- Computational zero-knowledge; and

$$\mathscr{R}_\ell := \left\{ \big((\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1), (\rho_0, m_0, \rho_1, m_1)\big) \;\middle|\; \begin{array}{l} m_0, m_1 \in \{0,1\}^\ell \\ \wedge\, m_0 = m_1 \\ \wedge\, c_0 = \mathsf{ENC}\,.\,\mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_0, m_0; \rho_0) \\ \wedge\, c_1 = \mathsf{ENC}\,.\,\mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_1, m_1; \rho_1) \end{array} \right\}.$$

Encryption scheme in the ROM

Construction

NARG **needs to satisfy**:

- Computational zero-knowledge; and
- Computational “true”-simulation soundness.

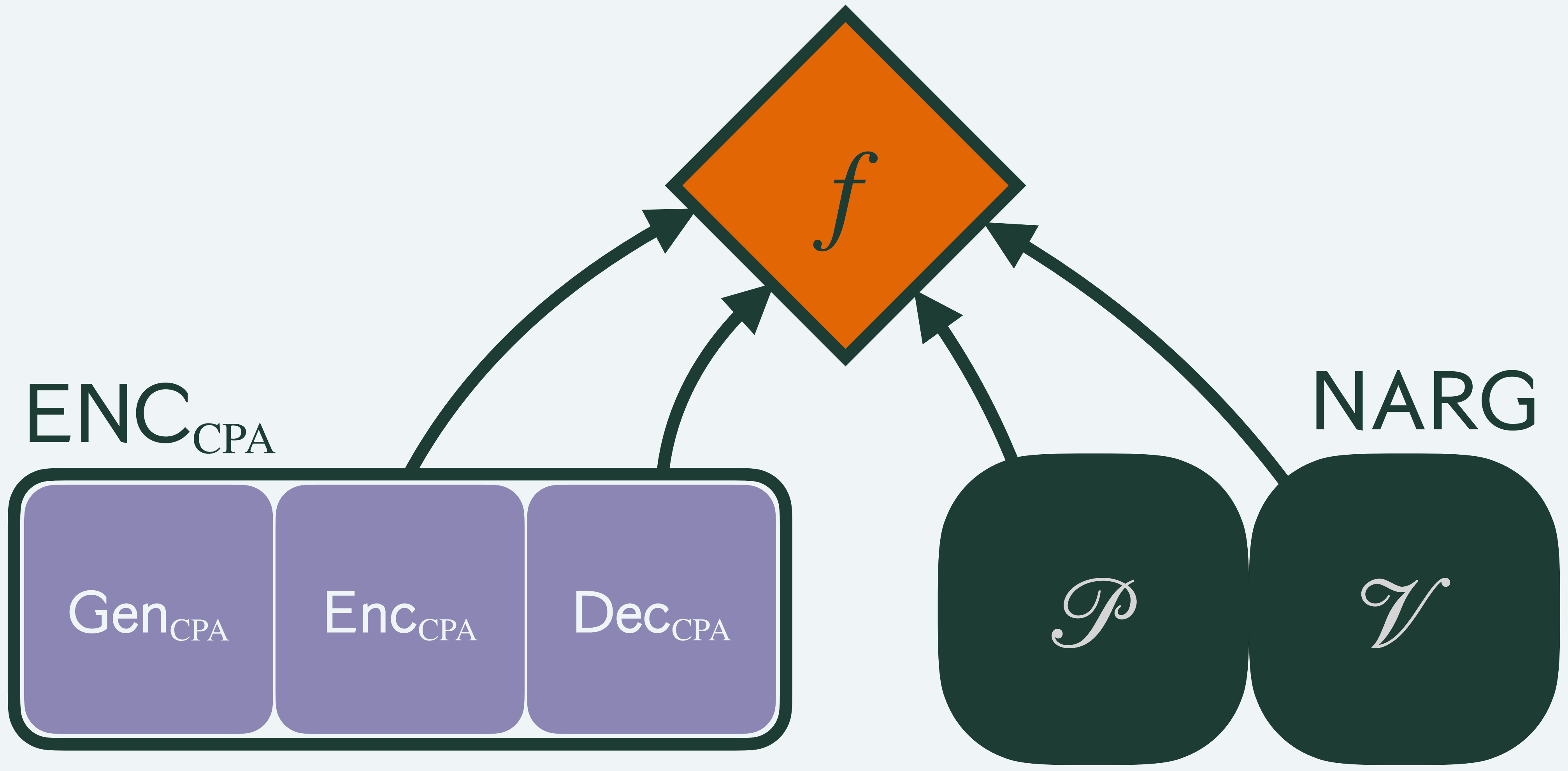
$$\mathscr{R}_\ell := \left\{ \big((\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1), (\rho_0, m_0, \rho_1, m_1)\big) \;\middle|\; \begin{array}{l} m_0, m_1 \in \{0,1\}^\ell \\ \wedge\ m_0 = m_1 \\ \wedge\ c_0 = \mathsf{ENC}\,.\,\mathsf{Enc}^f_{\text{CPA}}(\mathsf{pk}_0, m_0; \rho_0) \\ \wedge\ c_1 = \mathsf{ENC}\,.\,\mathsf{Enc}^f_{\text{CPA}}(\mathsf{pk}_1, m_1; \rho_1) \end{array} \right\}.$$

Encryption scheme in the ROM

Construction

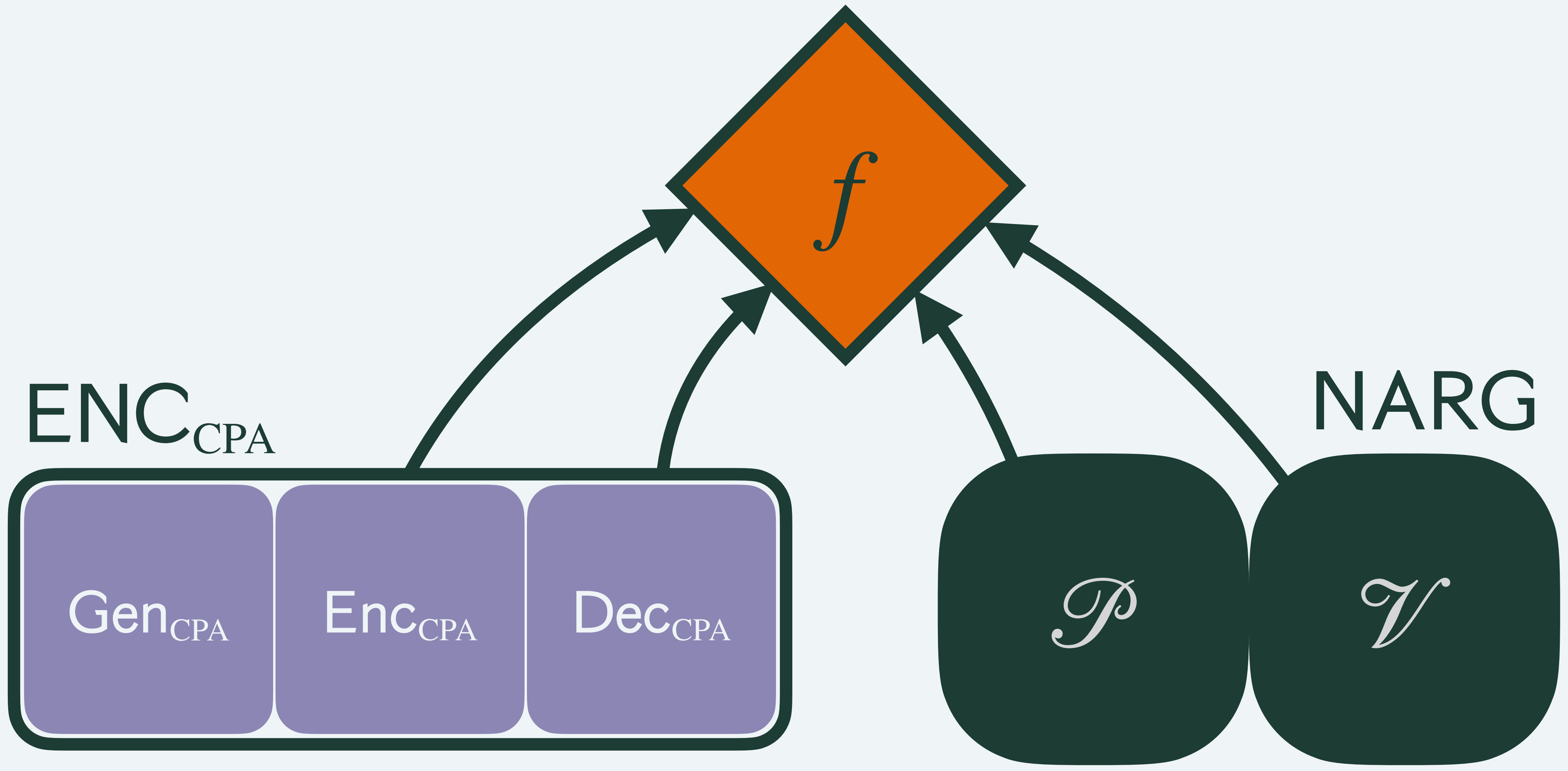
Encryption scheme in the ROM

Construction



Encryption scheme in the ROM

Construction



$\underline{\mathsf{Gen}(1^\lambda)}$

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{Gen}_{\mathrm{CPA}}(1^\lambda)$

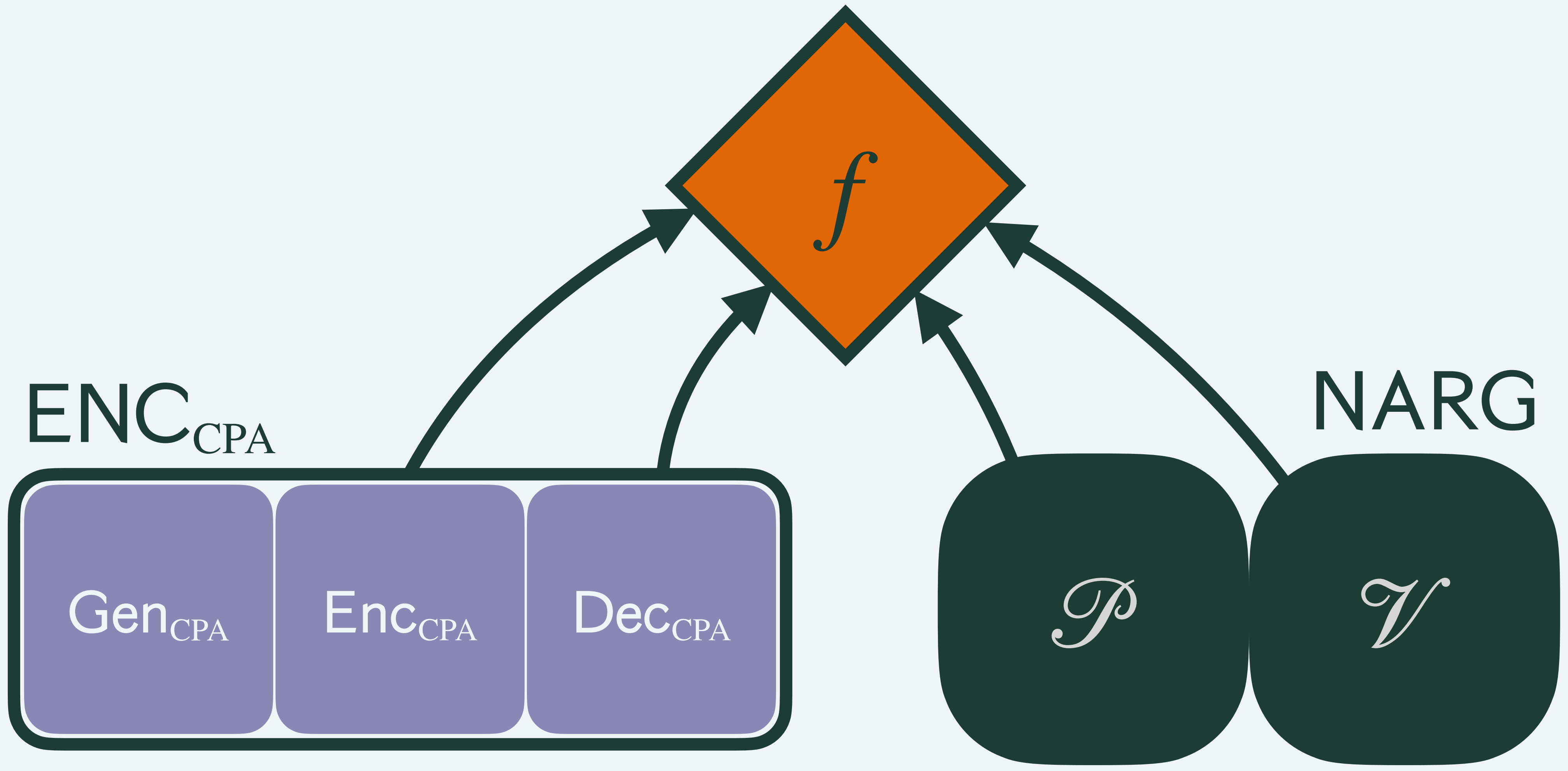
$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{Gen}_{\mathrm{CPA}}(1^\lambda)$

$\mathsf{pk} = (\mathsf{pk}_0, \mathsf{pk}_1)$

$\mathsf{sk} = (\mathsf{pk}_0, \mathsf{pk}_1, \mathsf{sk}_0, \mathsf{sk}_1)$

Encryption scheme in the ROM

Construction



<u>$\text{Gen}(1^\lambda)$</u>

$(\text{pk}_0, \text{sk}_0) \leftarrow \text{Gen}_{\text{CPA}}(1^\lambda)$

$(\text{pk}_1, \text{sk}_1) \leftarrow \text{Gen}_{\text{CPA}}(1^\lambda)$

$\text{pk} = (\text{pk}_0, \text{pk}_1)$

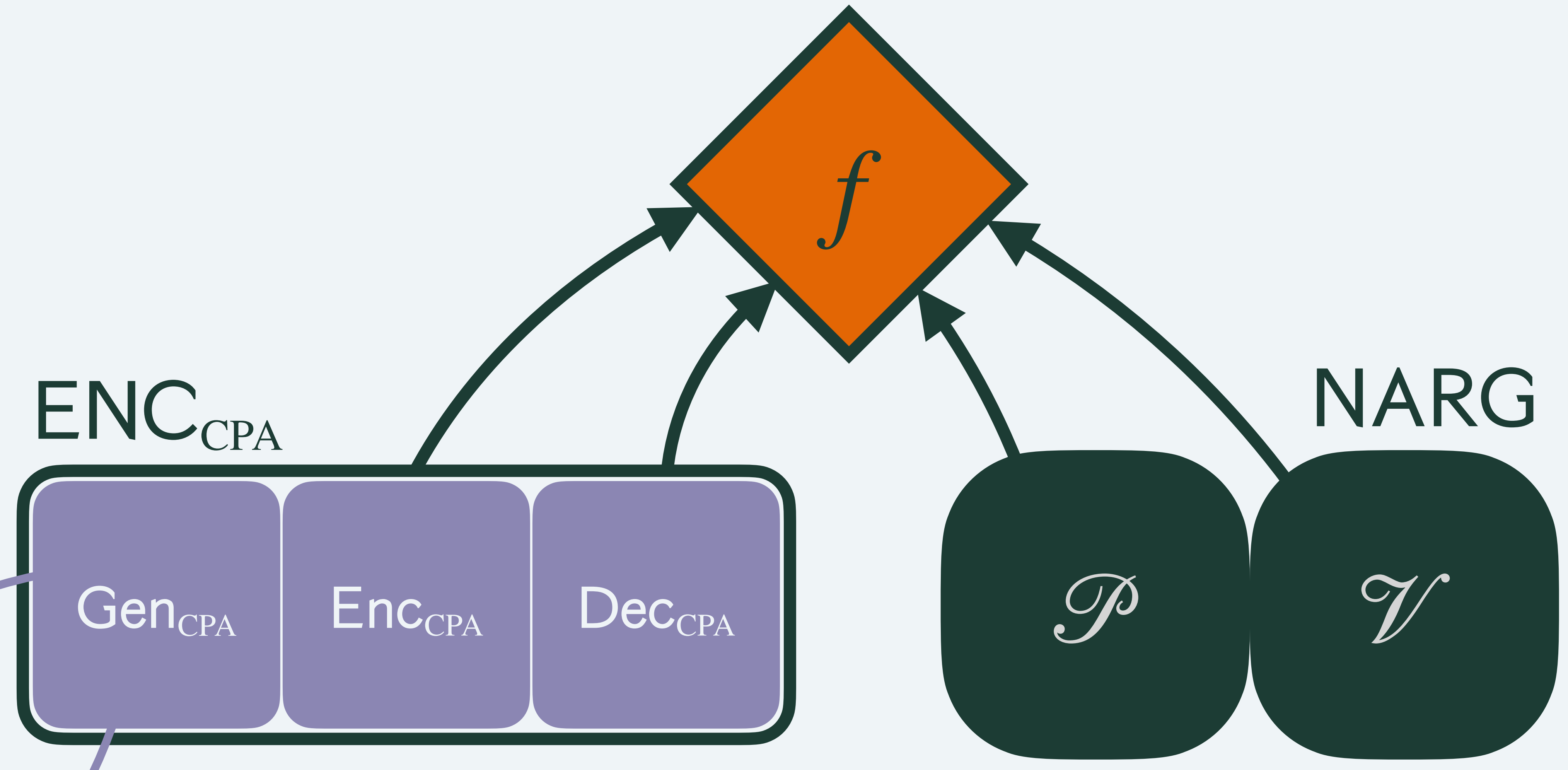
$\text{sk} = (\text{pk}_0, \text{pk}_1, \text{sk}_0, \text{sk}_1)$

$\downarrow$

(pk, sk)

Encryption scheme in the ROM

Construction



<u>$\mathsf{Gen}(1^\lambda)$</u>

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{Gen}_{\text{CPA}}(1^\lambda)$

$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{Gen}_{\text{CPA}}(1^\lambda)$

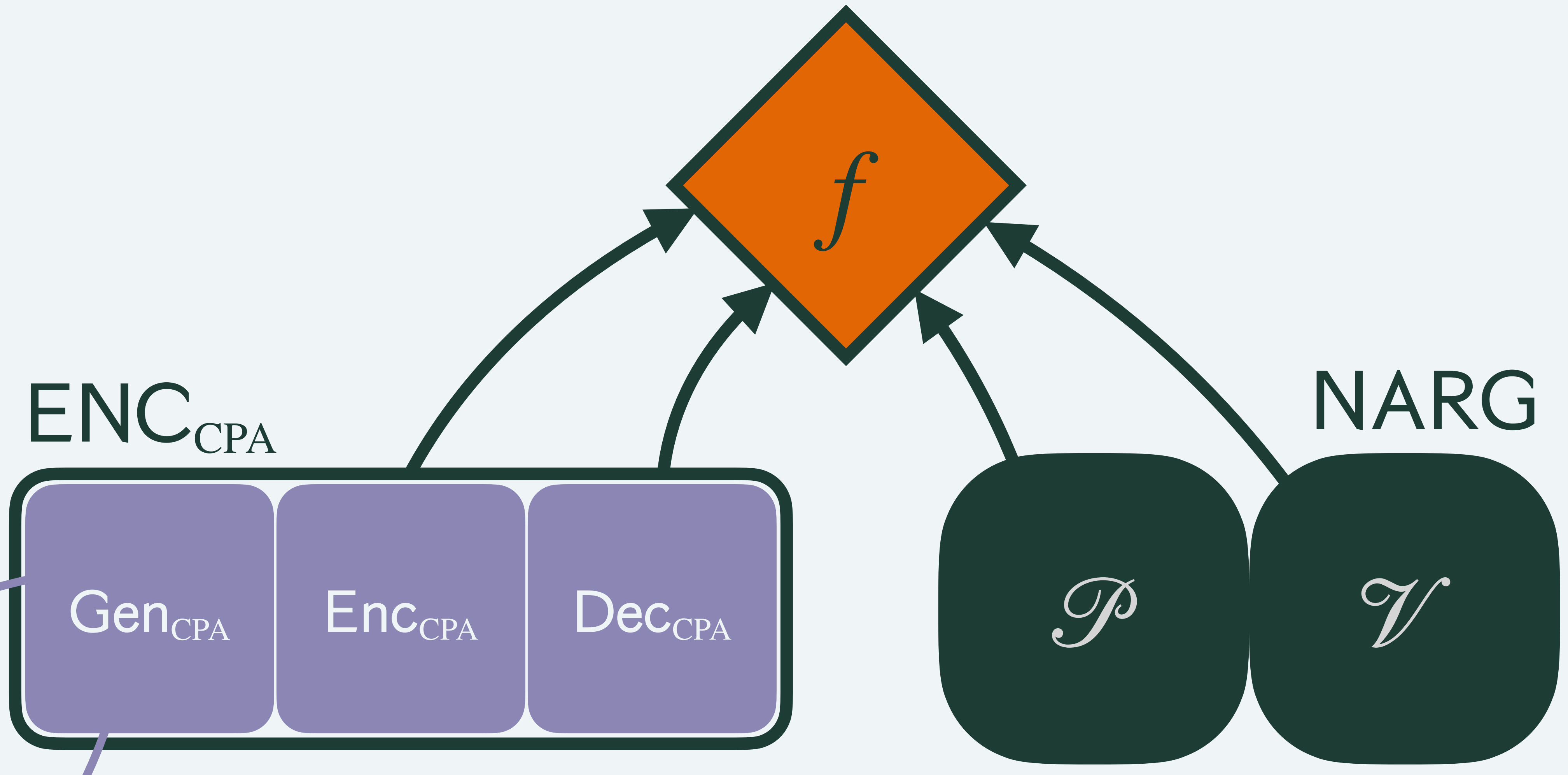
$\mathsf{pk} = (\mathsf{pk}_0, \mathsf{pk}_1)$

$\mathsf{sk} = (\mathsf{pk}_0, \mathsf{pk}_1, \mathsf{sk}_0, \mathsf{sk}_1)$

$(\mathsf{pk}, \mathsf{sk})$

Encryption scheme in the ROM

Construction



<u>$\mathsf{Gen}(1^\lambda)$</u>

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{Gen}_{\mathrm{CPA}}(1^\lambda)$

$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{Gen}_{\mathrm{CPA}}(1^\lambda)$

$\mathsf{pk} = (\mathsf{pk}_0, \mathsf{pk}_1)$

$\mathsf{sk} = (\mathsf{pk}_0, \mathsf{pk}_1, \mathsf{sk}_0, \mathsf{sk}_1)$

$(\mathsf{pk}, \mathsf{sk})$

<u>$\mathsf{Enc}^f(\mathsf{pk}, m)$</u>

$c_0 \leftarrow \mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_0, m; \rho_0)$

$c_1 \leftarrow \mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_1, m; \rho_1)$

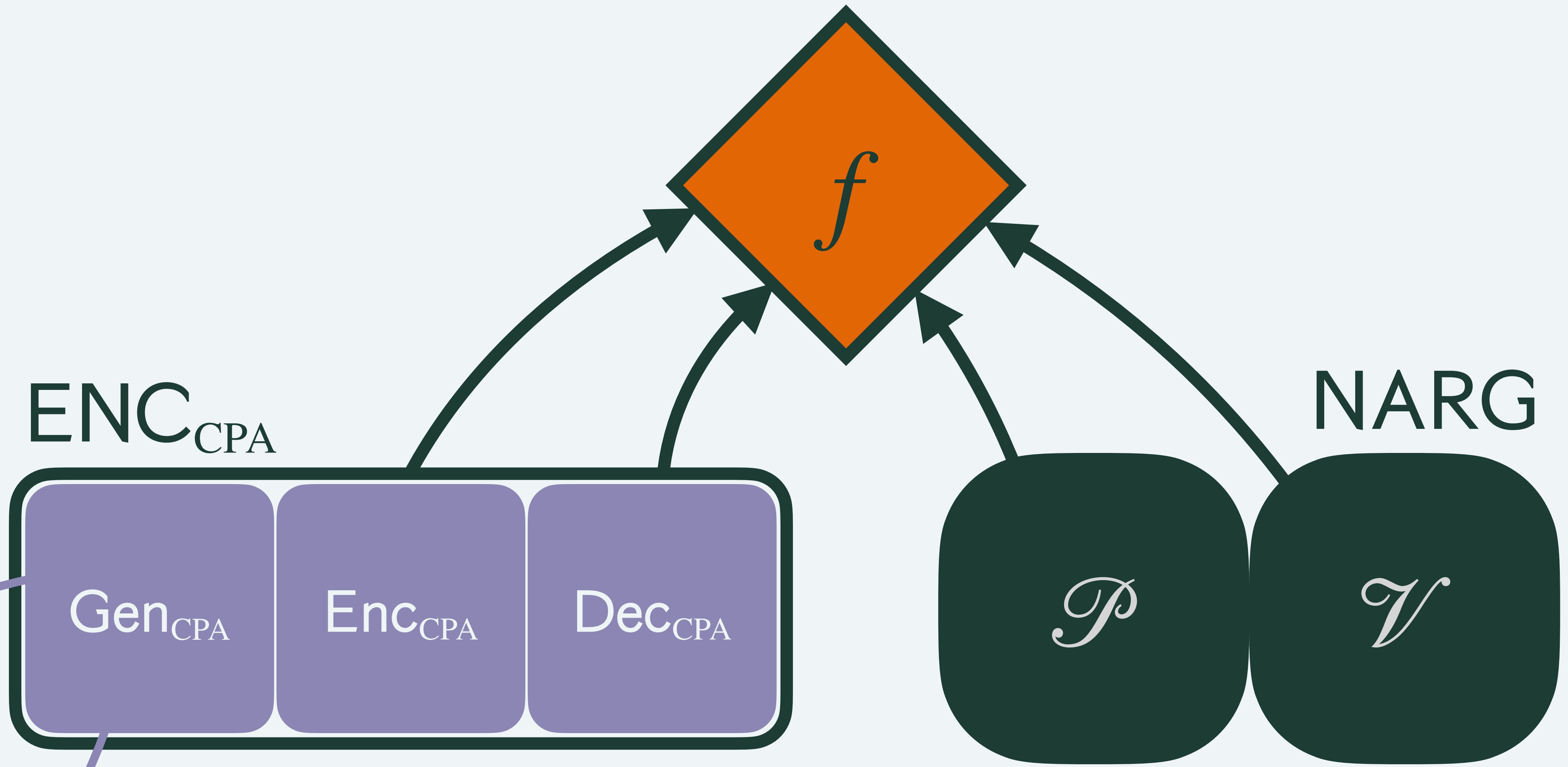
$x := (\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1)$

$w := (\rho_0, m, \rho_1, m)$

$\pi \leftarrow \mathscr{P}^f(x, w)$

Encryption scheme in the ROM

Construction



<u>$\mathsf{Gen}(1^\lambda)$</u>

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{Gen}_{\text{CPA}}(1^\lambda)$

$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{Gen}_{\text{CPA}}(1^\lambda)$

$\mathsf{pk} = (\mathsf{pk}_0, \mathsf{pk}_1)$

$\mathsf{sk} = (\mathsf{pk}_0, \mathsf{pk}_1, \mathsf{sk}_0, \mathsf{sk}_1)$

$(\mathsf{pk}, \mathsf{sk})$

<u>$\mathsf{Enc}^f(\mathsf{pk}, m)$</u>

$c_0 \leftarrow \mathsf{Enc}^f_{\text{CPA}}(\mathsf{pk}_0, m; \rho_0)$

$c_1 \leftarrow \mathsf{Enc}^f_{\text{CPA}}(\mathsf{pk}_1, m; \rho_1)$

$x := (\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1)$

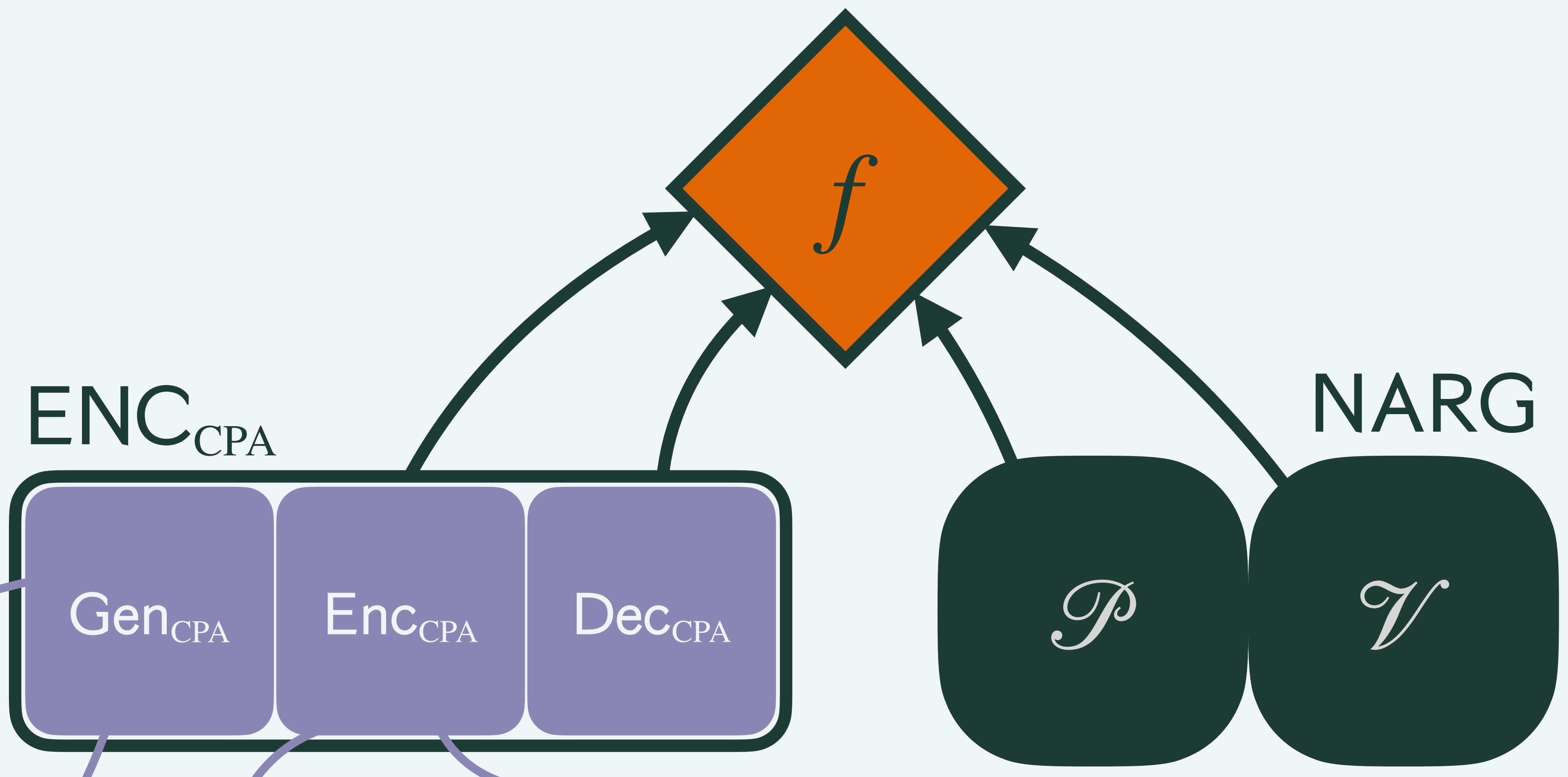
$w := (\rho_0, m, \rho_1, m)$

$\pi \leftarrow \mathcal{P}^f(x, w)$

(c_0, c_1, π)

Encryption scheme in the ROM

Construction



<u>Gen(1^λ)</u>

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{Gen}_{\text{CPA}}(1^\lambda)$

$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{Gen}_{\text{CPA}}(1^\lambda)$

$\mathsf{pk} = (\mathsf{pk}_0, \mathsf{pk}_1)$

$\mathsf{sk} = (\mathsf{pk}_0, \mathsf{pk}_1, \mathsf{sk}_0, \mathsf{sk}_1)$

$(\mathsf{pk}, \mathsf{sk})$

<u>Enc$^f(\mathsf{pk}, m)$</u>

$c_0 \leftarrow \mathsf{Enc}^f_{\text{CPA}}(\mathsf{pk}_0, m; \rho_0)$

$c_1 \leftarrow \mathsf{Enc}^f_{\text{CPA}}(\mathsf{pk}_1, m; \rho_1)$

$x := (\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1)$

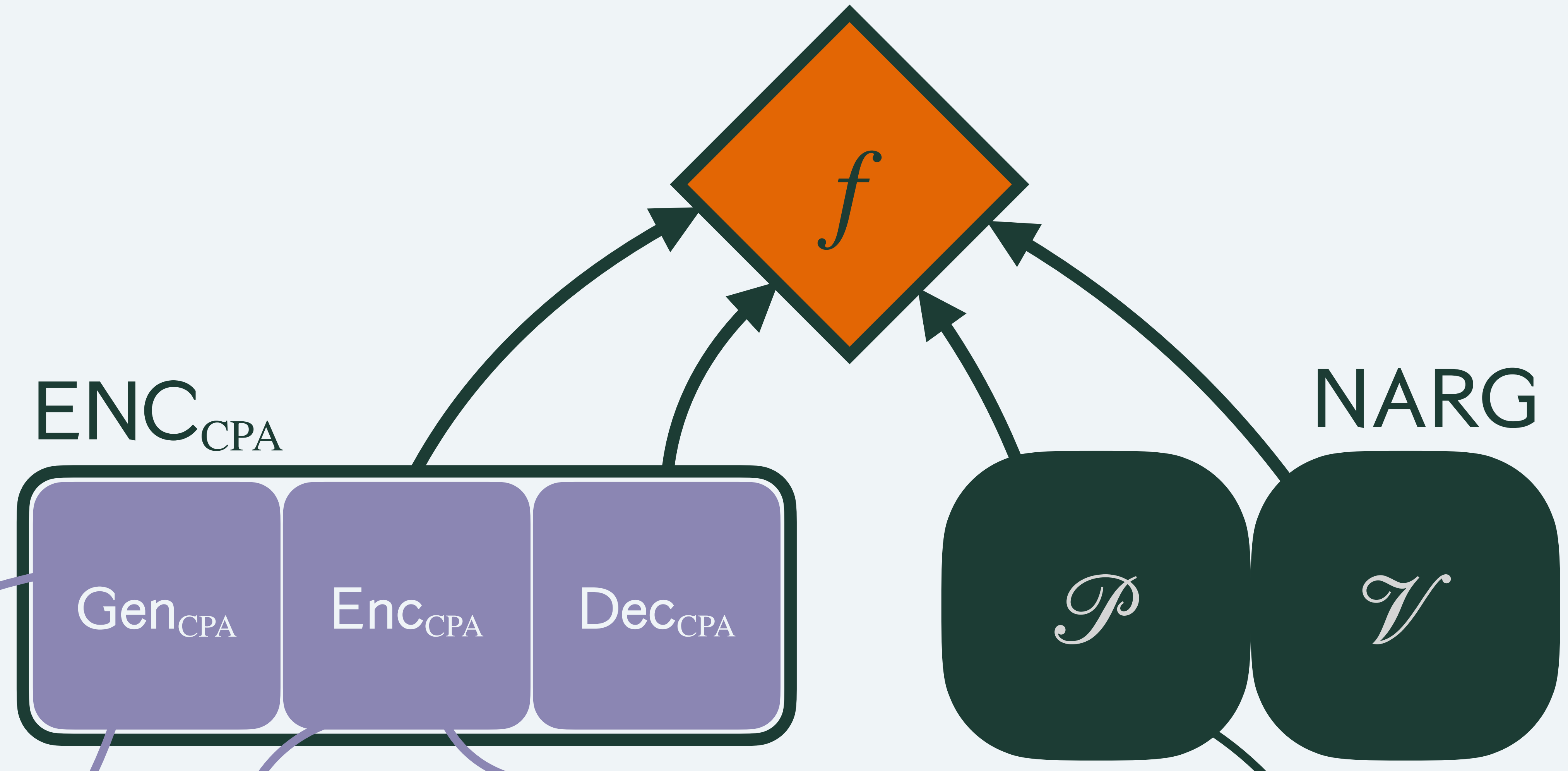
$w := (\rho_0, m, \rho_1, m)$

$\pi \leftarrow \mathscr{P}^f(x, w)$

(c_0, c_1, π)

Encryption scheme in the ROM

Construction



<u>Gen(1^λ)</u>

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{Gen}_{\mathrm{CPA}}(1^\lambda)$

$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{Gen}_{\mathrm{CPA}}(1^\lambda)$

$\mathsf{pk} = (\mathsf{pk}_0, \mathsf{pk}_1)$

$\mathsf{sk} = (\mathsf{pk}_0, \mathsf{pk}_1, \mathsf{sk}_0, \mathsf{sk}_1)$

$(\mathsf{pk}, \mathsf{sk})$

<u>Enc^f(pk, m)</u>

$c_0 \leftarrow \mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_0, m; \rho_0)$

$c_1 \leftarrow \mathsf{Enc}^f_{\mathrm{CPA}}(\mathsf{pk}_1, m; \rho_1)$

$x := (\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1)$

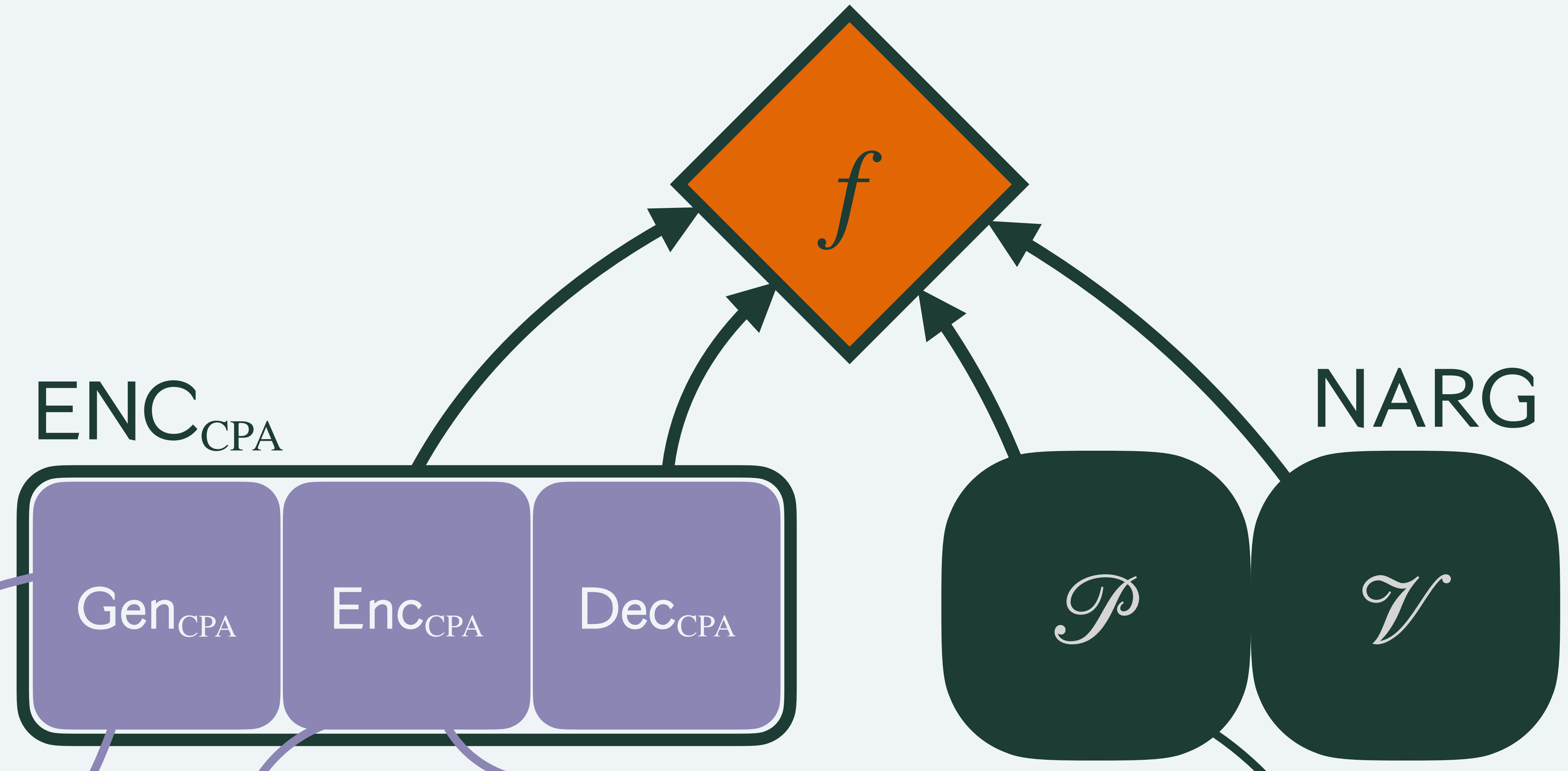
$w := (\rho_0, m, \rho_1, m)$

$\pi \leftarrow \mathcal{P}^f(x, w)$

(c_0, c_1, π)

Encryption scheme in the ROM

Construction



<u>$\mathsf{Gen}(1^\lambda)$</u>

$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{Gen}_{\text{CPA}}(1^\lambda)$

$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{Gen}_{\text{CPA}}(1^\lambda)$

$\mathsf{pk} = (\mathsf{pk}_0, \mathsf{pk}_1)$

$\mathsf{sk} = (\mathsf{pk}_0, \mathsf{pk}_1, \mathsf{sk}_0, \mathsf{sk}_1)$

$(\mathsf{pk}, \mathsf{sk})$

<u>$\mathsf{Enc}^f(\mathsf{pk}, m)$</u>

$c_0 \leftarrow \mathsf{Enc}^f_{\text{CPA}}(\mathsf{pk}_0, m; \rho_0)$

$c_1 \leftarrow \mathsf{Enc}^f_{\text{CPA}}(\mathsf{pk}_1, m; \rho_1)$

$x := (\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1)$

$w := (\rho_0, m, \rho_1, m)$

$\pi \leftarrow \mathscr{P}^f(x, w)$

(c_0, c_1, π)

<u>$\mathsf{Dec}^f(\mathsf{sk}, c)$</u>

$x := (\mathsf{pk}_0, c_0, \mathsf{pk}_1, c_1)$

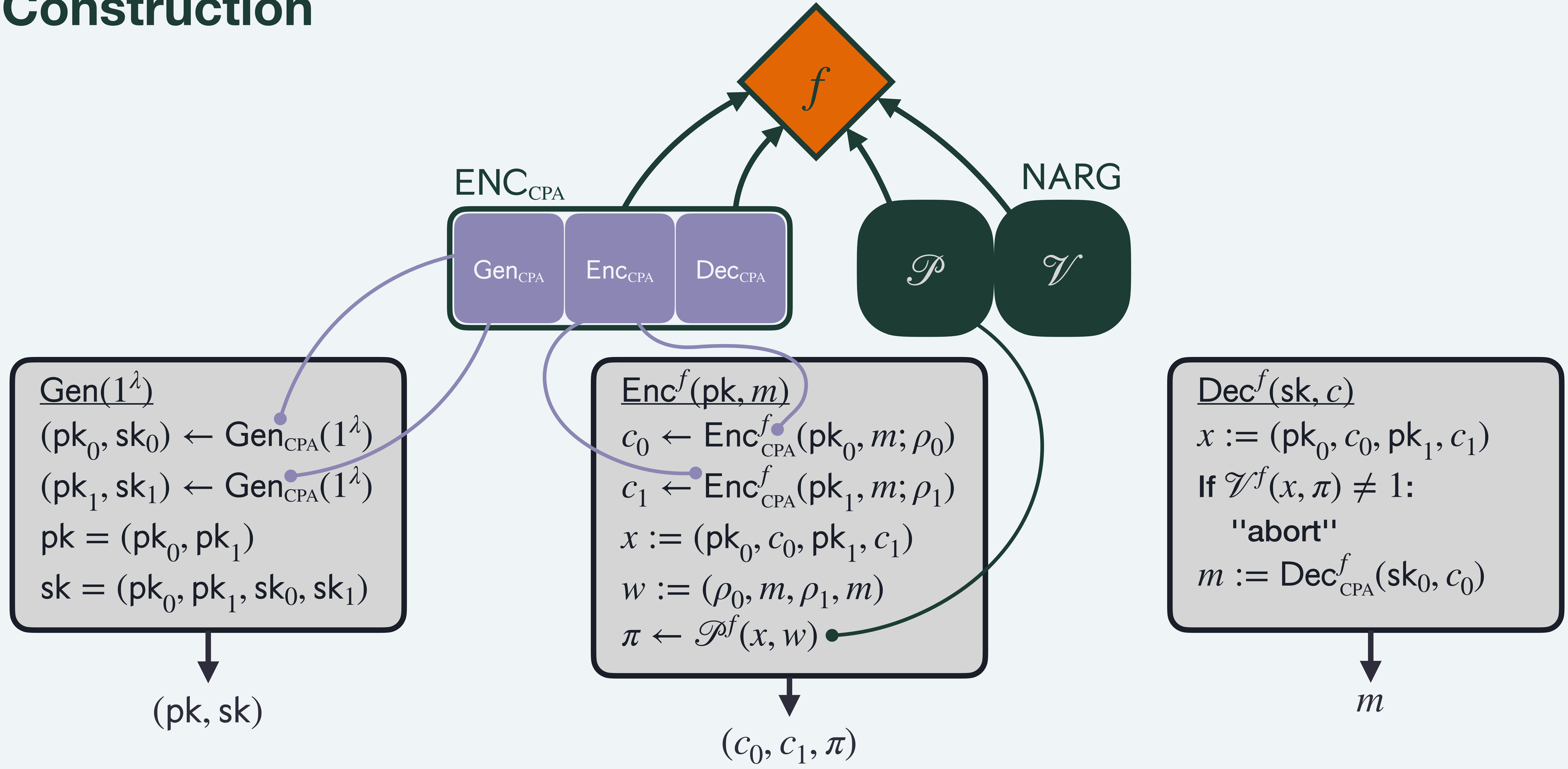
If $\mathscr{V}^f(x, \pi) \neq 1$:

"abort"

$m := \mathsf{Dec}^f_{\text{CPA}}(\mathsf{sk}_0, c_0)$

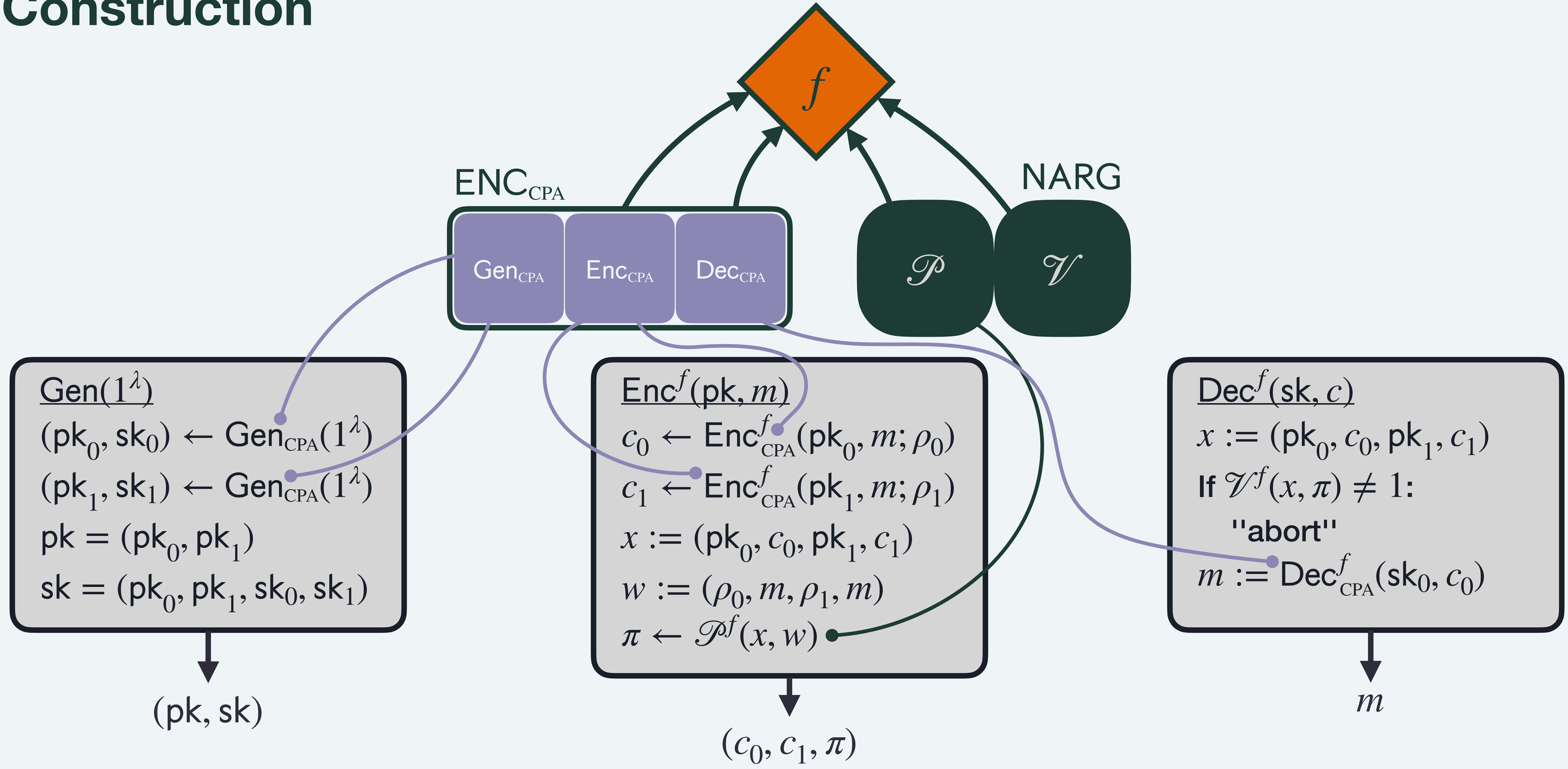
Encryption scheme in the ROM

Construction



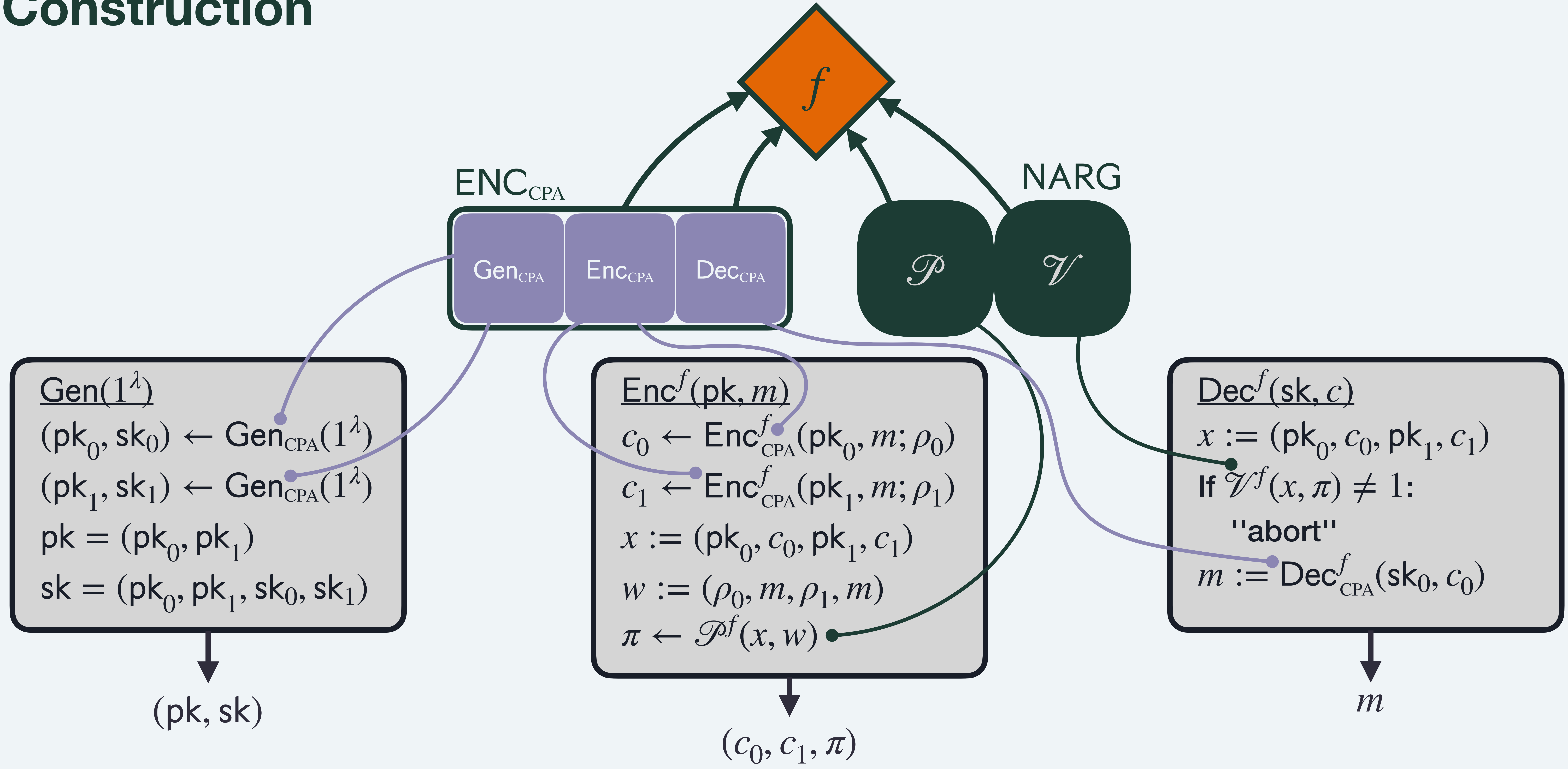
Encryption scheme in the ROM

Construction



Encryption scheme in the ROM

Construction



Encryption scheme in the ROM

Theorem 5.4

Encryption scheme in the ROM

Theorem 5.4

If:

Encryption scheme in the ROM

Theorem 5.4

If:

- ENC_{CPA} has CPA error ϵ_{CPA}; and

Encryption scheme in the ROM

Theorem 5.4

If:

- $\mathsf{ENC}_{\mathrm{CPA}}$ has CPA error ϵ_{CPA}; and
- NARG has computational zero-knowledge error z_{ARG} and computational *true*-simulation soundness error $\epsilon_{\mathrm{ARG}}^{\mathrm{SIM}}$,

Encryption scheme in the ROM

Theorem 5.4

If:

- ENC$_{\text{CPA}}$ has CPA error ϵ_{CPA}; and
- NARG has computational zero-knowledge error z_{ARG} and computational *true*-simulation soundness error $\epsilon_{\text{ARG}}^{\text{SIM}}$,

then for any adversary size bound $s \in \mathbb{N}$, random oracle query bound $t \in \mathbb{N}$, decryption oracle query bound $t_{\text{DEC}} \in \mathbb{N}$ and (t, t_{DEC})-query admissible adversary A of size at most s, ENC $:=$ ENC$[\lambda, \ell, \ell_c]$ is perfectly complete has CCA error such that:

Encryption scheme in the ROM

Theorem 5.4

If:

- $\mathsf{ENC}_{\mathrm{CPA}}$ has CPA error ϵ_{CPA}; and
- NARG has computational zero-knowledge error z_{ARG} and computational *true*-simulation soundness error $\epsilon_{\mathrm{ARG}}^{\mathrm{SIM}}$,

then for any adversary size bound $s \in \mathbb{N}$, random oracle query bound $t \in \mathbb{N}$, decryption oracle query bound $t_{\mathrm{DEC}} \in \mathbb{N}$ and (t, t_{DEC})-query admissible adversary A of size at most s, $\mathsf{ENC} := \mathsf{ENC}[\lambda, \ell, \ell_c]$ is perfectly complete has CCA error such that:

$$
\begin{aligned}
&\epsilon_{\mathrm{CCA}}(\lambda, \ell, t, t_{\mathrm{DEC}}, s) \leqslant \\
&\qquad z_{\mathrm{ARG}}(\lambda, t + t_{\mathrm{DEC}} \cdot (t_{\mathrm{RO},\mathcal{V}} + t^{\mathrm{CPA}}_{\mathrm{RO},\mathsf{Dec}}) + 2t^{\mathrm{CPA}}_{\mathrm{RO},\mathsf{Enc}}, 1, 2\ell_{\mathsf{key},\mathrm{CPA}} + 2\ell_{c,\mathrm{CPA}}, s + \mathsf{poly}(\lambda, \ell, t, t_{\mathrm{DEC}})) \\
&\qquad + \epsilon^{\mathrm{SIM}}_{\mathrm{ARG}}(\lambda, t + t_{\mathrm{DEC}} \cdot (t_{\mathrm{RO},\mathcal{V}} + 2t^{\mathrm{CPA}}_{\mathrm{RO},\mathsf{Dec}}) + 2t^{\mathrm{CPA}}_{\mathrm{RO},\mathsf{Enc}}, 1, 2\ell_{\mathsf{key},\mathrm{CPA}} + 2\ell_{c,\mathrm{CPA}}, s + \mathsf{poly}(\lambda, \ell, t, t_{\mathrm{DEC}})) \\
&\qquad + \epsilon_{\mathrm{CPA}}(\lambda, \ell, t + t_{\mathrm{DEC}} \cdot (t_{\mathrm{RO},\mathcal{V}} + t^{\mathrm{CPA}}_{\mathrm{RO},\mathsf{Dec}}) + 2t^{\mathrm{CPA}}_{\mathrm{RO},\mathsf{Enc}} + t_{\mathrm{RO},\mathcal{S}}, s + \mathsf{poly}(\lambda, \ell, t, t_{\mathrm{DEC}})) \quad .
\end{aligned}
$$

Thank you

Questions