Random Oracles in a Quantum World

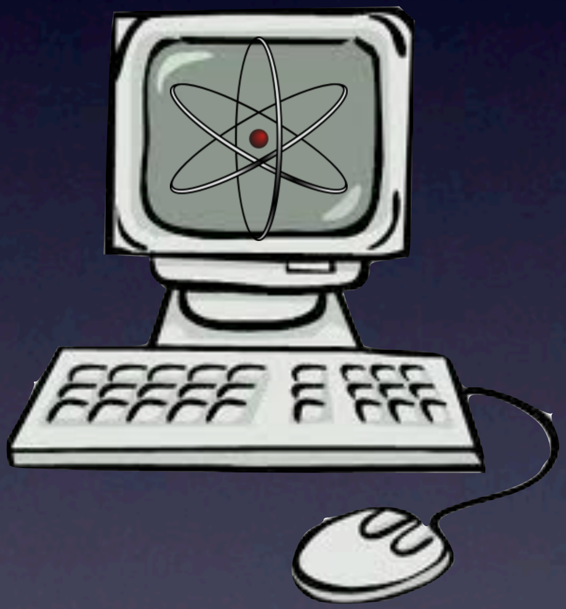
Dan Boneh, Mark Zhandry (Stanford)
Özgür Dagdelen, Marc Fischlin (TU Darmstadt)
Anja Lehmann (IBM Zürich)
Christian Schaffner (University of Amsterdam & CWI)

CWI

Séminaire de Crypto de l'ENS
Paris, 27 février 2012
(based on slides by Özgür and Mark)

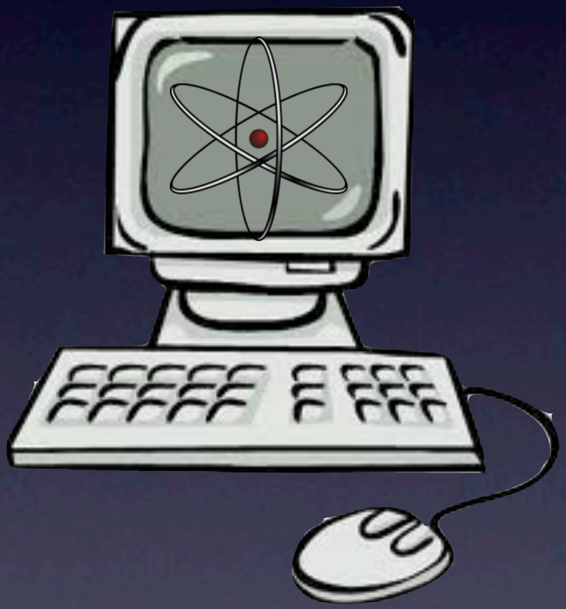
Nederlandse Organisatie voor Wetenschappelijk Onderzoek

Post-Quantum Crypto



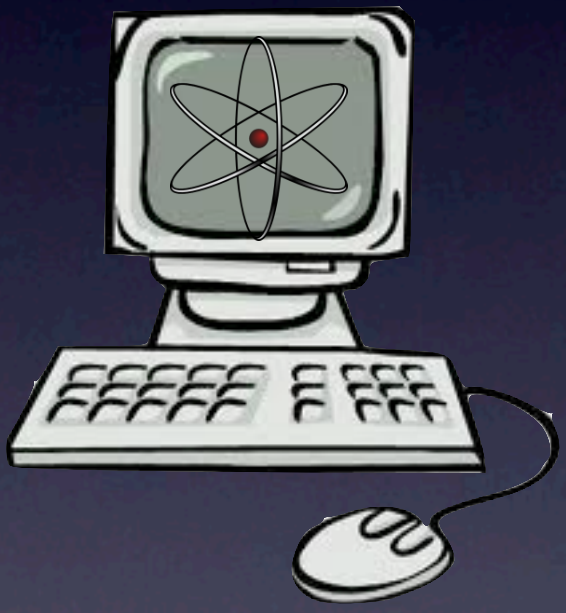
Post-Quantum Crypto

- Cryptosystems based on the hardness of factoring or discrete logarithms are broken by quantum computers



Post-Quantum Crypto

- Cryptosystems based on the hardness of factoring or discrete logarithms are broken by quantum computers
- Remaining assumptions:
  - lattices (e.g. NTRU)
  - codes (e.g. McEliece, Niederreiter)
  - hashes (Merkle's hash-tree signatures)
  - multi-variate polynomials



Post-Quantum Crypto and the Random-Oracle Model (ROM)

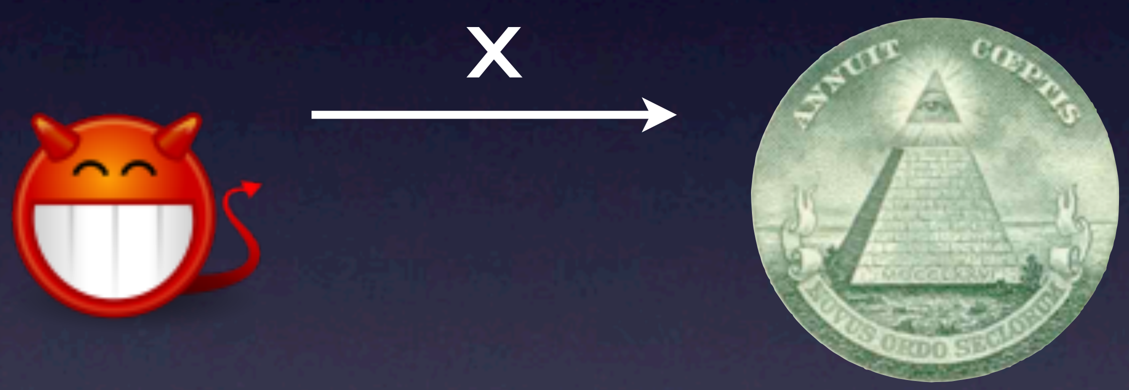
- Several lattice-based schemes have been proven secure in the classical ROM:
  - Signatures [GPV08, GKV10, BF11]
  - Encryption [GPV08]
  - Identification [CLRS10]
- Are they really secure in the quantum world?

Quantum-Accessible Random Oracles

classical

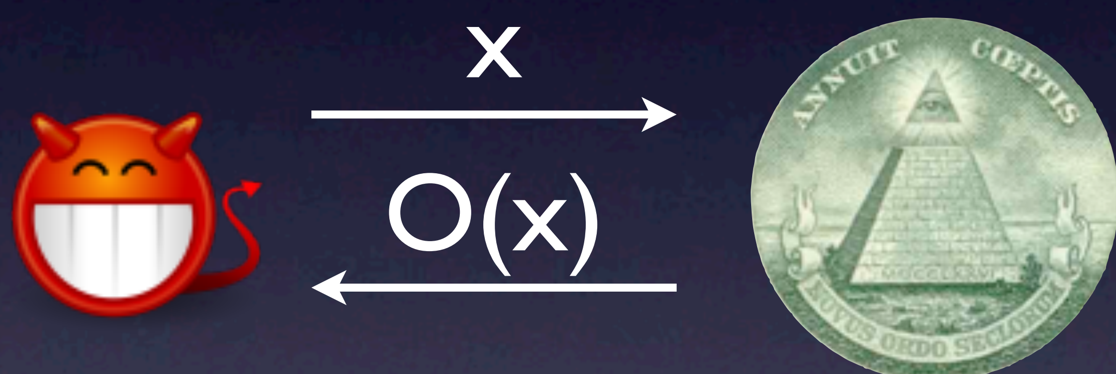
Quantum-Accessible Random Oracles

classical



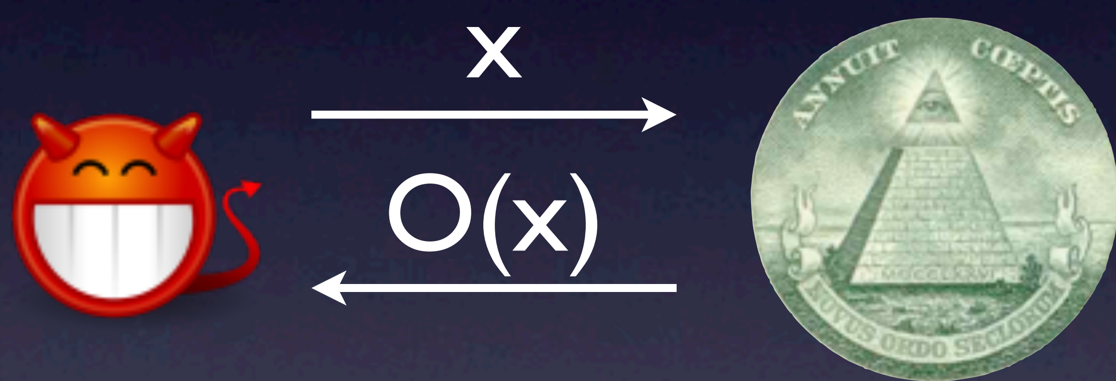
Quantum-Accessible Random Oracles

classical



Quantum-Accessible Random Oracles

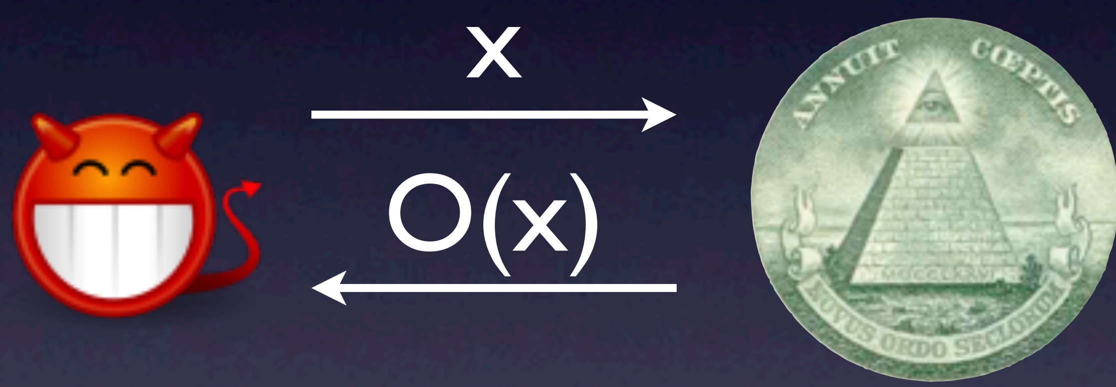
classical



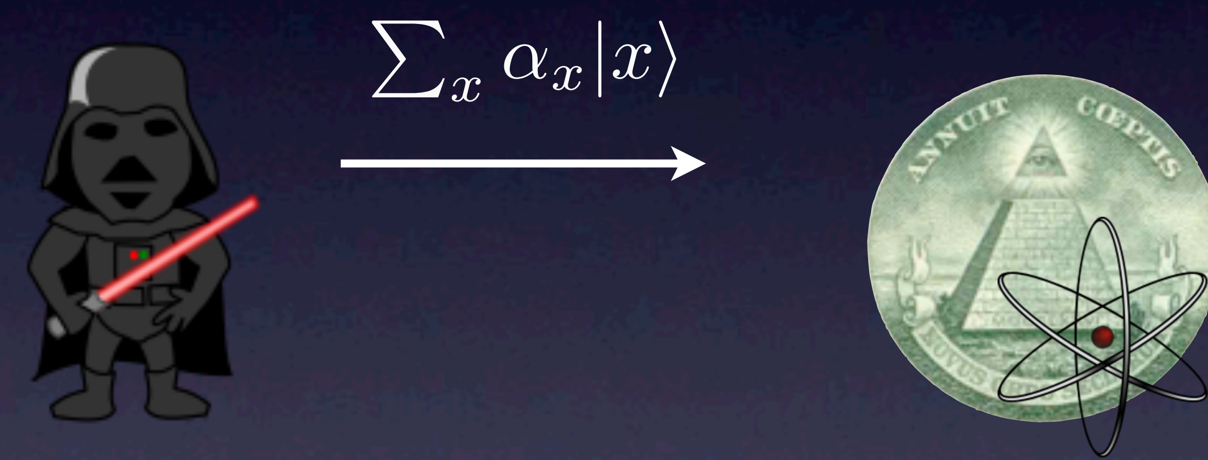
quantum

Quantum-Accessible Random Oracles

classical

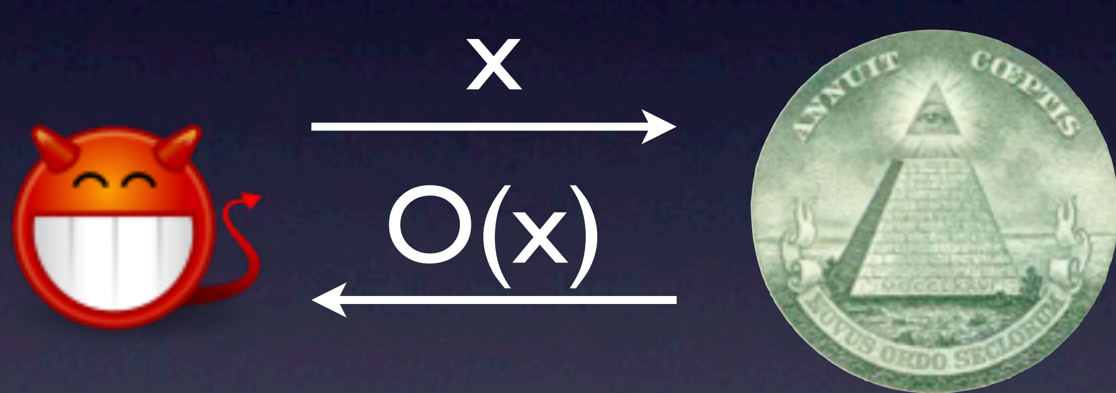


quantum

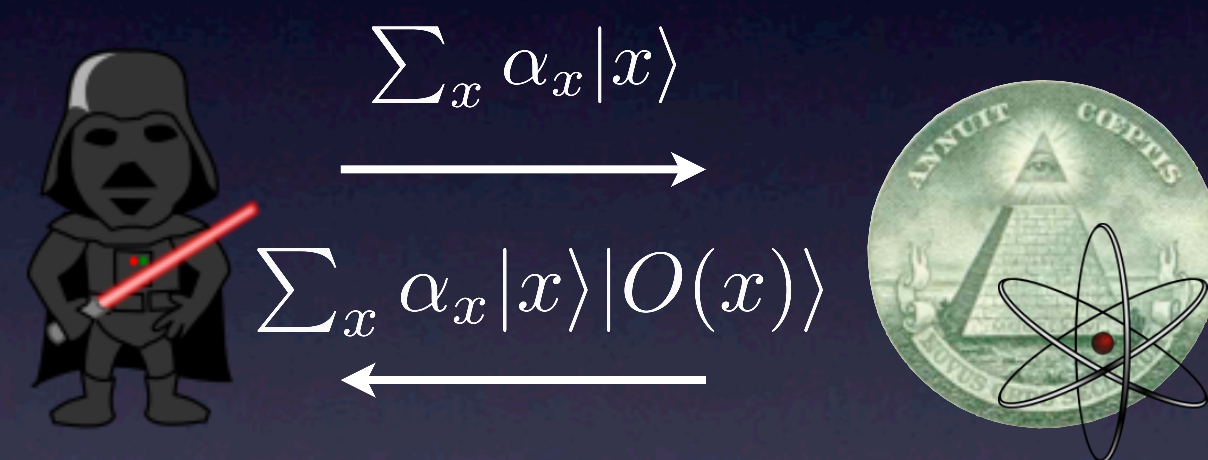


Quantum-Accessible Random Oracles

classical



quantum



Quantum-Accessible Random Oracles

classical

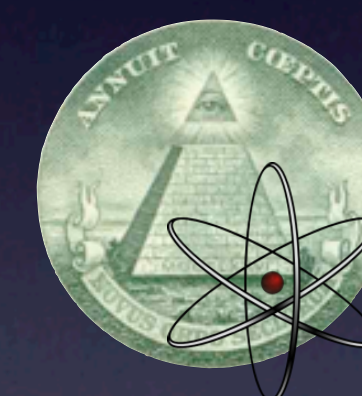
$\xrightarrow{\text{x}}$

$\xleftarrow{\text{O(x)}}$

quantum

$\xrightarrow{\sum_x \alpha_x |x\rangle}$

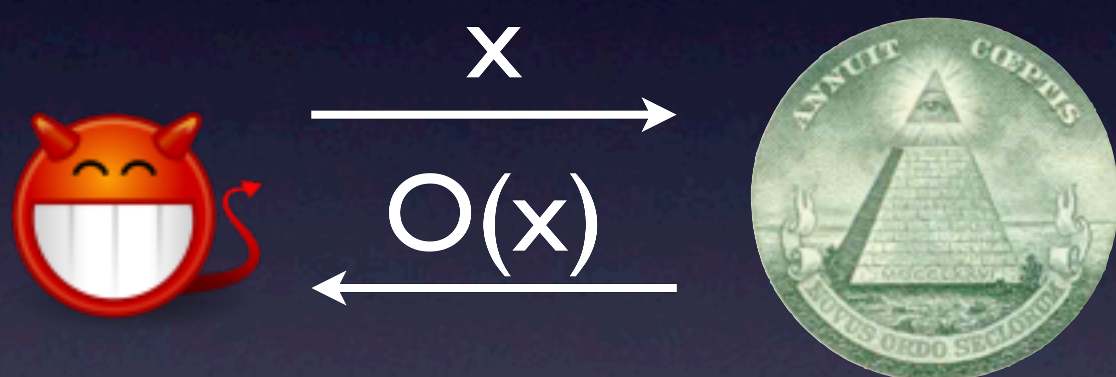
$\xleftarrow{\sum_x \alpha_x |x\rangle |O(x)\rangle}$



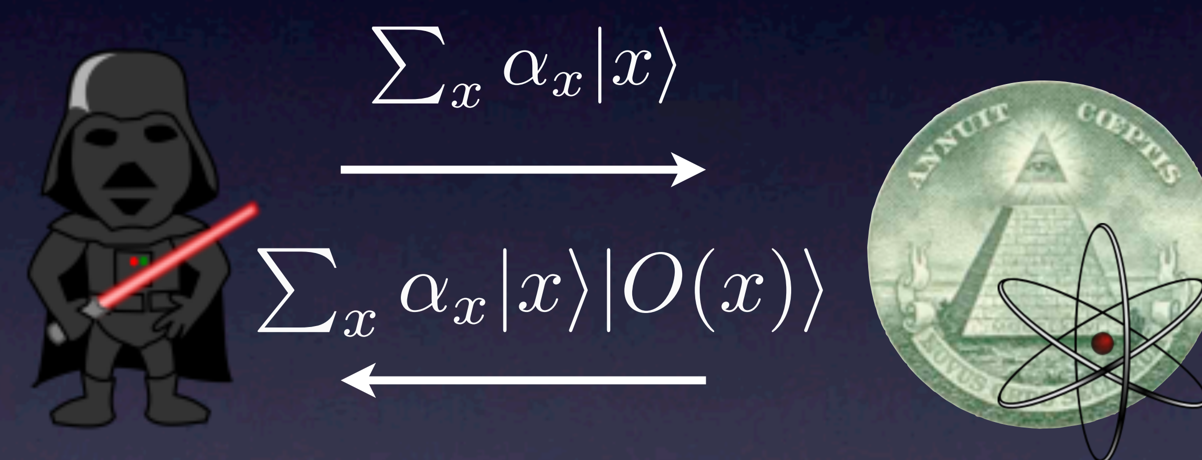
"quantum adversary may query RO in superposition"

Quantum-Accessible Random Oracles

classical



quantum

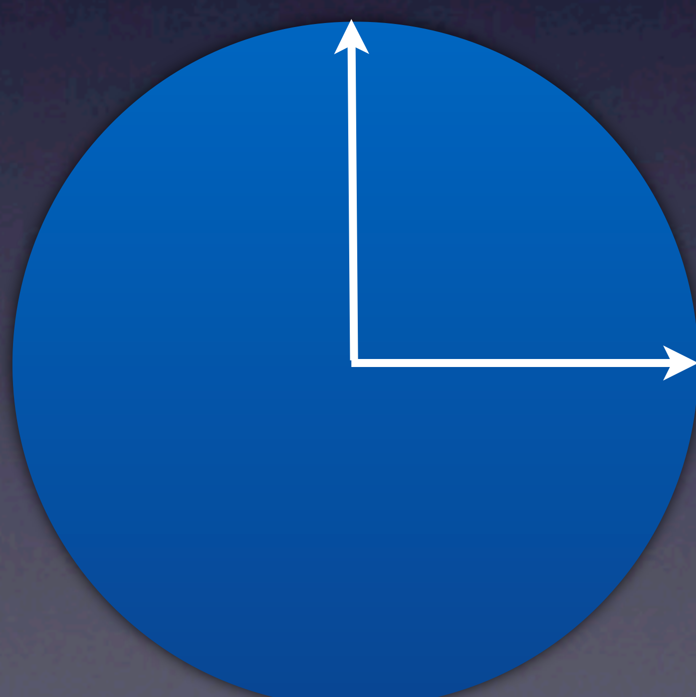


"quantum adversary may query RO in superposition"

- Does security in CROM imply security in QROM ?

One Quantum Bit

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

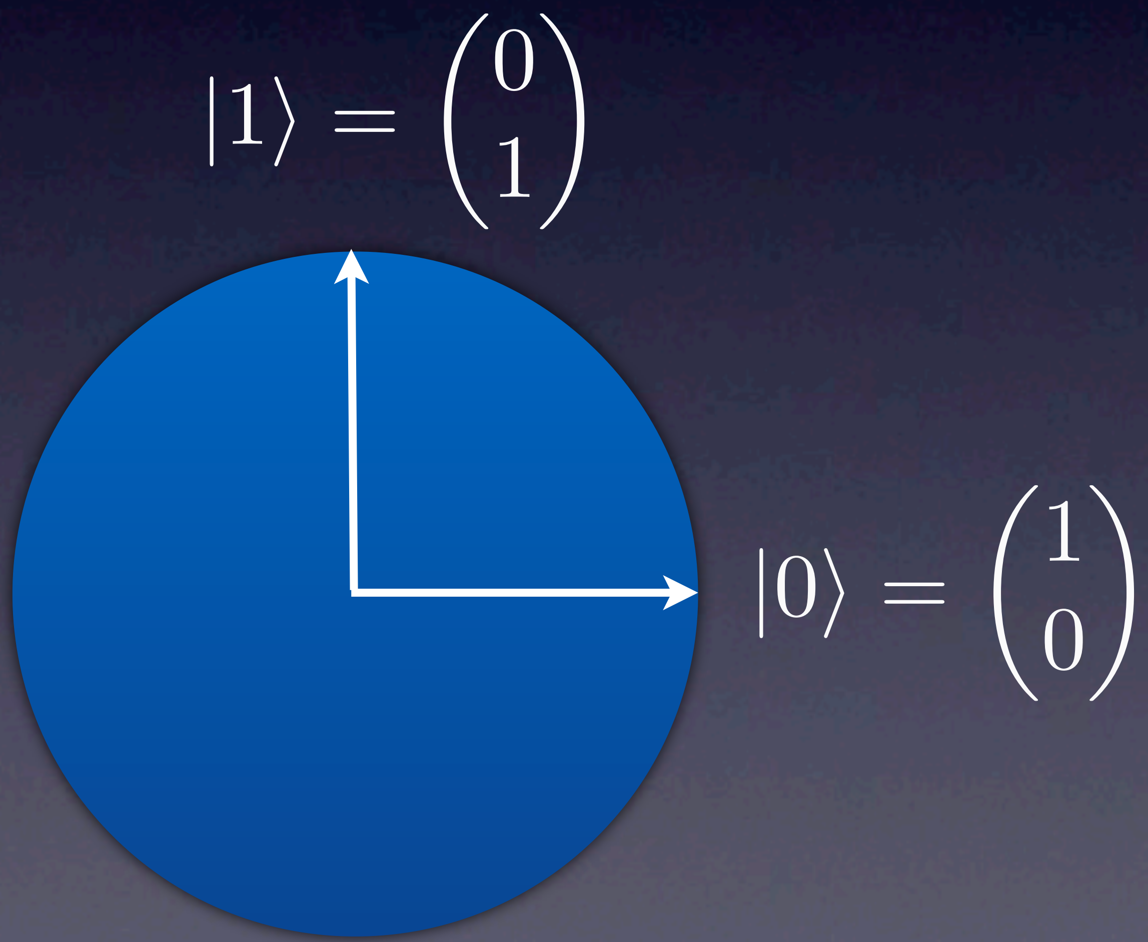


$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

One Quantum Bit

classical bits: 0 / 1

quantum state:

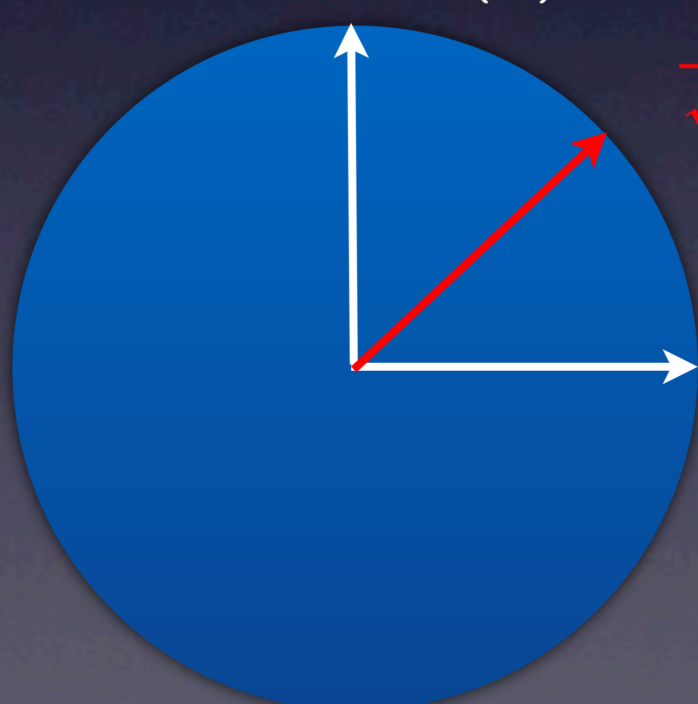


One Quantum Bit

classical bits: 0 / 1

quantum state:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$



$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

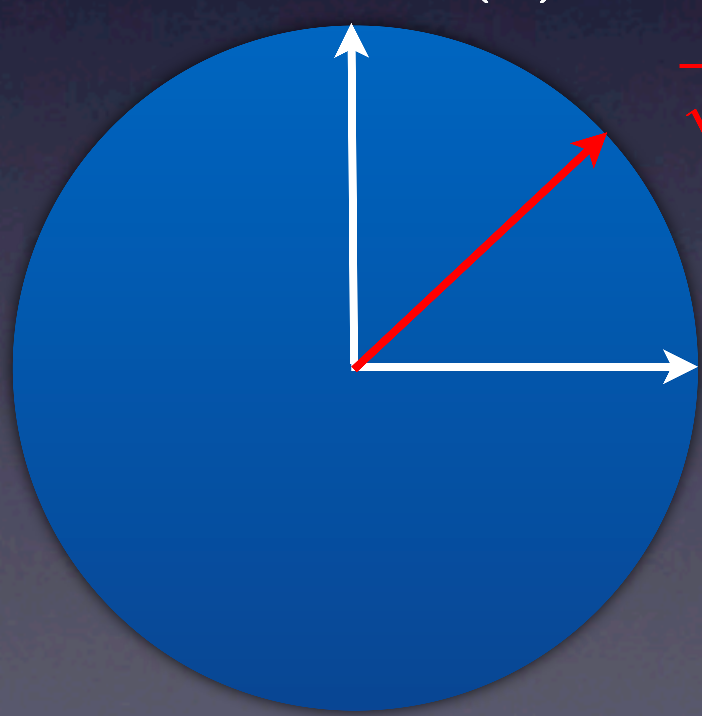
One Quantum Bit

classical bits: 0 / 1

quantum state: $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$



$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

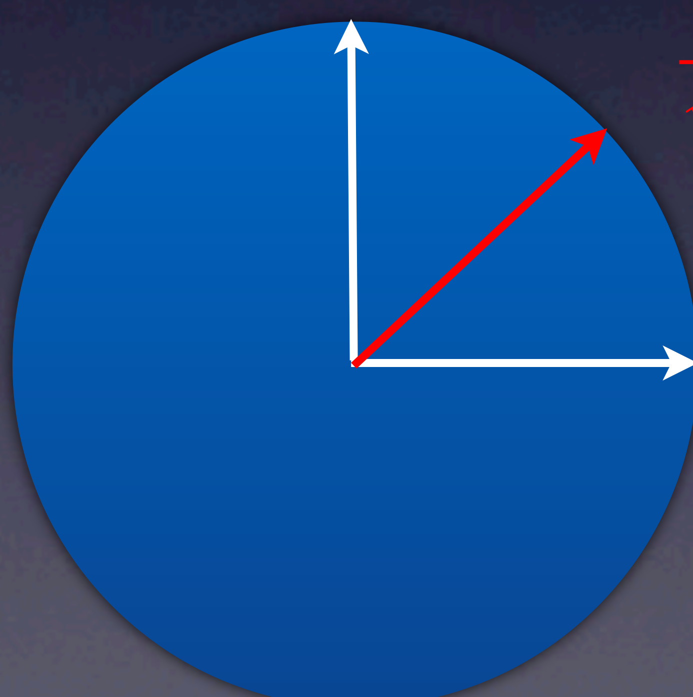
One Quantum Bit

classical bits: 0 / 1

quantum state: $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} \in \mathbb{C}^2$

complex amplitudes: $\alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$

$$|1\rangle = \begin{pmatrix}0 \\ 1\end{pmatrix}$$



$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 \\ 1\end{pmatrix}$$

$$|0\rangle = \begin{pmatrix}1 \\ 0\end{pmatrix}$$

Two Qubits

$$|\varphi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$$

Two Qubits

two classical bits: 00 , 01, 10, 11

quantum state: $|\varphi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$

Two Qubits

two classical bits: 00 , 01, 10, 11

quantum state: $|\varphi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$

$$|\varphi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \in \mathbb{C}^4$$

Two Qubits

two classical bits: 00 , 01, 10, 11

quantum state: $|\varphi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$

$$|\varphi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \in \mathbb{C}^4$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Two Qubits

two classical bits: 00 , 01, 10, 11

quantum state: $|\varphi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$

complex amplitudes: $\alpha_x \in \mathbb{C}, \quad \sum_{x\in\{00,01,10,11\}} |\alpha_x|^2 = 1$

$$|\varphi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \in \mathbb{C}^4$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

n-Qubit States

classical n-bit strings: $x \in \{0,1\}^n$

n-qubit state: $|\varphi\rangle = \sum_x \alpha_x |x\rangle \in \mathbb{C}^{2^n}$

complex amplitudes: $\alpha_x \in \mathbb{C}, \quad \sum_x |\alpha_x|^2 = 1$

$$|x\rangle = |x_1 x_2 \dots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle$$

Quantum Operations

linear unitary transformations on n qubits: U

- 2^n x 2^n dimensional matrix
- $U^* \cdot U$ = id, i.e. rows and columns of U form orthonormal bases
- U preserves inner products

$$U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$$

$$|x\rangle \mapsto U|x\rangle$$

Quantum Oracles

classical RO: $$O : \{0,1\}^n \to \{0,1\}^n$$
$$x \mapsto O(x)$$

Quantum Oracles

classical RO: $O : \{0,1\}^n \to \{0,1\}^n$

$$x \mapsto O(x)$$

quantum-accessible RO:

$$U : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus O(x)\rangle$$

Quantum Oracles

classical RO: $O : \{0,1\}^n \to \{0,1\}^n$

$$x \mapsto O(x)$$

quantum-accessible RO:

$$U : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus O(x)\rangle$$

$$U \sum_x \alpha_x |x\rangle|0^n\rangle = \sum_x \alpha_x |x\rangle|O(x)\rangle$$

Quantum Oracles

classical RO: $$O : \{0,1\}^n \to \{0,1\}^n$$
$$x \mapsto O(x)$$

quantum-accessible RO:

$$U : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus O(x)\rangle$$

$$U \sum_x \alpha_x |x\rangle|0^n\rangle = \sum_x \alpha_x |x\rangle|O(x)\rangle$$

- oracle can be accessed “in superposition”

Quantum Oracles

classical RO: $$O : \{0,1\}^n \to \{0,1\}^n$$
$$x \mapsto O(x)$$

quantum-accessible RO:

$$U : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus O(x)\rangle$$

$$U \sum_x \alpha_x |x\rangle|0^n\rangle = \sum_x \alpha_x |x\rangle|O(x)\rangle$$

- oracle can be accessed "in superposition"
- a single quantum query can involve O(x) for all x

Quantum Measurements

- quantum states need to be measured to extract classical information from them

Quantum Measurements

- quantum states need to be measured to extract classical information from them
- outcome is probabilistic

Quantum Measurements

- quantum states need to be measured to extract classical information from them
- outcome is probabilistic
- example: measuring $\sum_x \alpha_x |x\rangle|O(x)\rangle$ (in the computational basis) gives outcome *x* with probability $|\alpha_x|^2$

Quantum Measurements

- quantum states need to be measured to extract classical information from them
- outcome is probabilistic
- example: measuring $\sum_x \alpha_x |x\rangle|O(x)\rangle$ (in the computational basis) gives outcome *x* with probability $|\alpha_x|^2$
- quantum computers can not perform exponentially many classical computations in parallel!

Results in Quantum Information Processing

- Factoring: Given N, find its prime factors
  - classical: General Number Field Sieve: $e^{(O((\log N)^{1/3}(\log\log N)^{2/3})}$
  - quantum: Shor's algorithm: $O((\log N)^3)$

Results in Quantum Information Processing

- Factoring: Given N, find its prime factors
  - classical: General Number Field Sieve: $e^{(O((\log N)^{1/3}(\log\log N)^{2/3})}$
  - quantum: Shor's algorithm: $O((\log N)^3)$
- Search in unstructured database with N entries
  - classical: brute force, requires Ω(N) lookups
  - quantum: Grover's algorithm: $O(\sqrt{N})$ lookups

Results in Quantum Information Processing

- Factoring: Given N, find its prime factors
  - classical: General Number Field Sieve: $e^{(O((\log N)^{1/3}(\log\log N)^{2/3})}$
  - quantum: Shor's algorithm: $O((\log N)^3)$
- Search in unstructured database with N entries
  - classical: brute force, requires Ω(N) lookups
  - quantum: Grover's algorithm: $O(\sqrt{N})$ lookups
- Collision search for an r-to-1 function f with domain size N
  - classical: requires $\Theta(\sqrt{N/r})$ evaluations of f
  - quantum: Brassard et al: $O(\sqrt[3]{N/r})$ evaluations

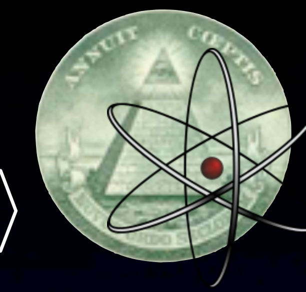
Roadmap

- What's the problem?
- Separation of QROM from CROM
- Secure Schemes in the QROM
- Open Problems

Potential Problems in QROM

$$\sum_x \alpha_x |x\rangle \longrightarrow$$

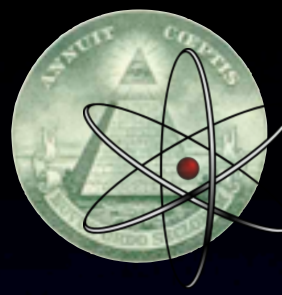
$$\sum_x \alpha_x |x\rangle |O(x)\rangle \longleftarrow$$



Potential Problems in QROM

$\sum_x \alpha_x |x\rangle$

$\sum_x \alpha_x |x\rangle |O(x)\rangle$

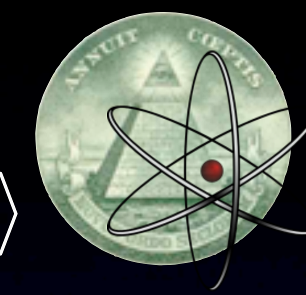


- Adaptive Programmability
  - quantum adversary can query oracle on exponentially values right at the beginning

Potential Problems in QROM

$$\sum_x \alpha_x |x\rangle$$

$$\sum_x \alpha_x |x\rangle |O(x)\rangle$$

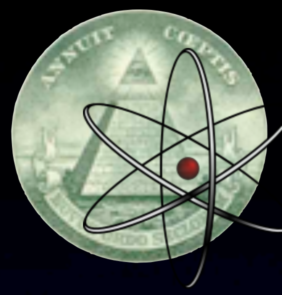


- Adaptive Programmability
  - quantum adversary can query oracle on exponentially values right at the beginning
- Extractability / Preimage Awareness
  - classical simulator learns exact pre-images which interest the adversary

Potential Problems in QROM

$\sum_x \alpha_x |x\rangle \longrightarrow$

$\longleftarrow \sum_x \alpha_x |x\rangle |O(x)\rangle$

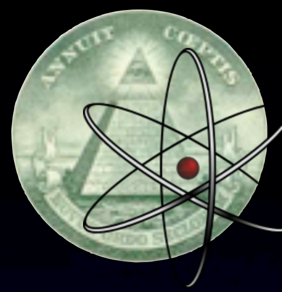


- Adaptive Programmability
  - quantum adversary can query oracle on exponentially values right at the beginning
- Extractability / Preimage Awareness
  - classical simulator learns exact pre-images which interest the adversary
- Efficient Simulation
  - lazy-sampling does not carry over

Potential Problems in QROM

$$\xrightarrow{\sum_x \alpha_x |x\rangle}$$

$$\xleftarrow{\sum_x \alpha_x |x\rangle |O(x)\rangle}$$



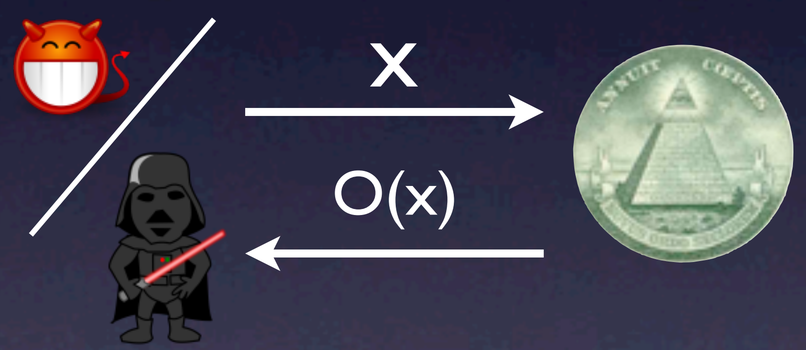
- Adaptive Programmability
  - quantum adversary can query oracle on exponentially values right at the beginning
- Extractability / Preimage Awareness
  - classical simulator learns exact pre-images which interest the adversary
- Efficient Simulation
  - lazy-sampling does not carry over
- Rewinding / Partial Consistency
  - unnoticed changing of hash values is difficult

QROM vs CROM

- Are these two models different? Yes!

QROM vs CROM

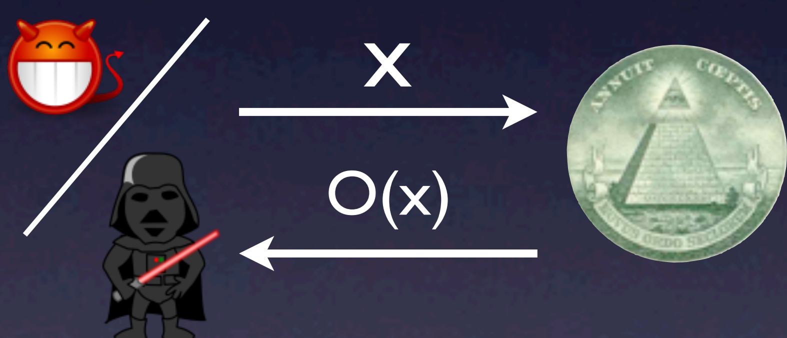
- Are these two models different? Yes!
- We present an identification scheme which is

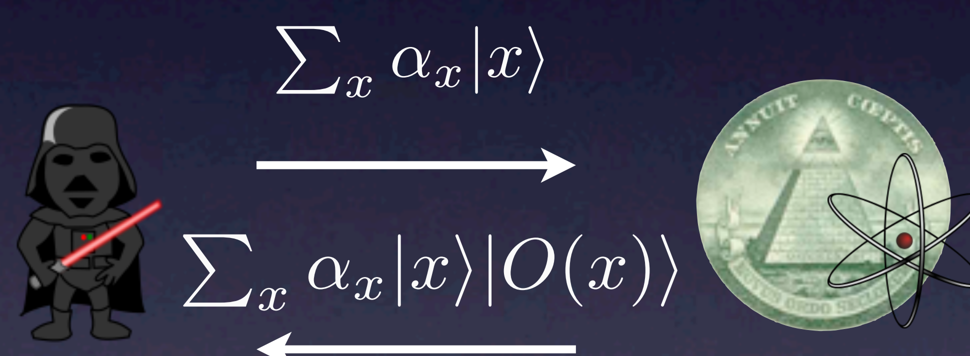


secure
in the
classical ROM

QROM vs CROM

- Are these two models different? Yes!
- We present an identification scheme which is



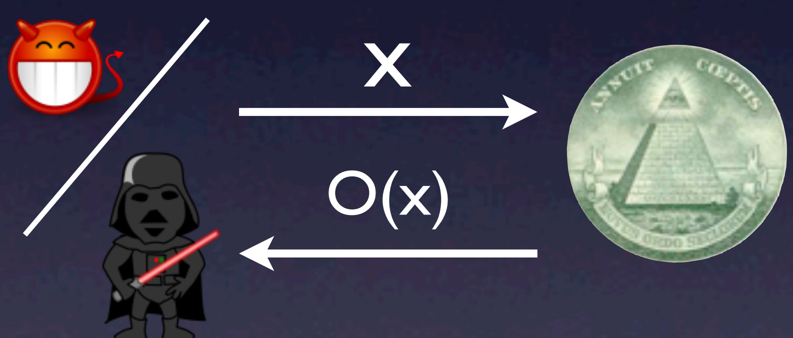


secure
in the
classical ROM

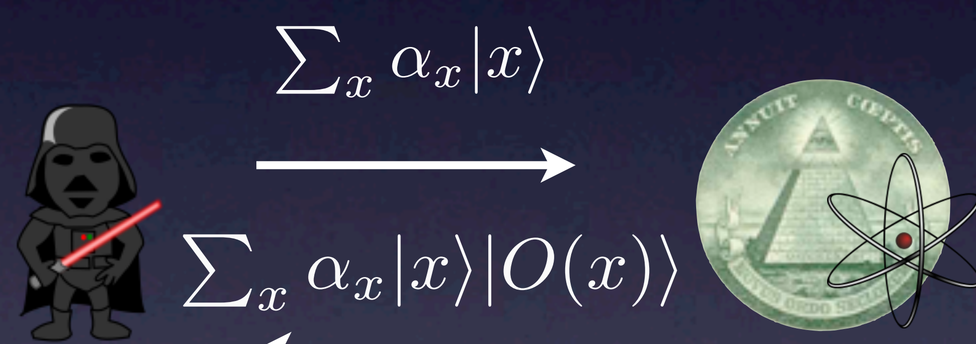
insecure
in the
quantum ROM

QROM vs CROM

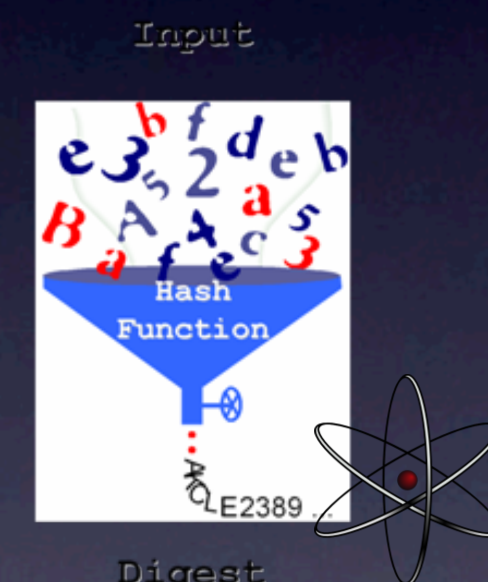
- Are these two models different? Yes!
- We present an identification scheme which is



secure
in the
classical ROM



insecure
in the
quantum ROM



insecure
under any
instantiation

Identification Protocol

Verifier
pk

Prover
(pk,sk)

Identification Protocol

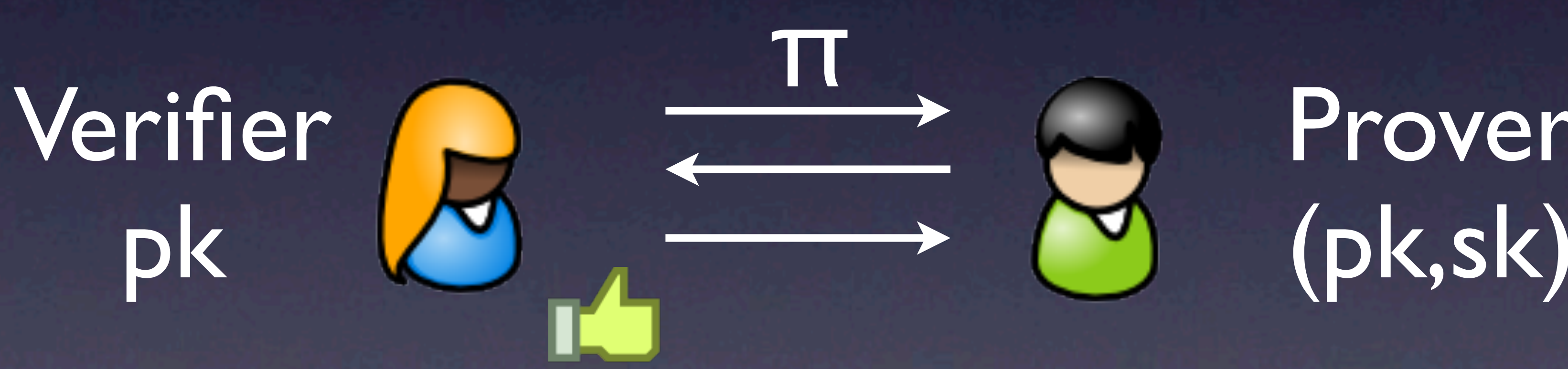
- (Public-Key) Identification Protocol between Prover P and Verifier V

Verifier
pk

Prover
(pk,sk)

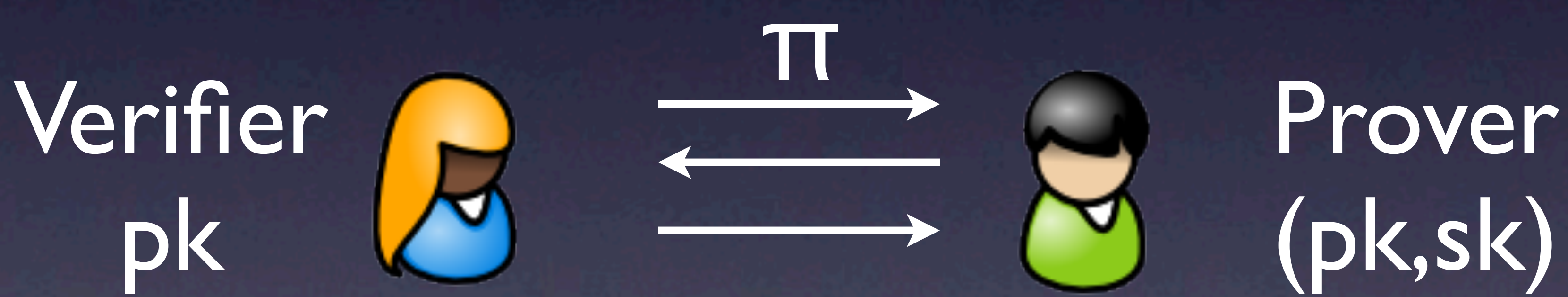
Identification Protocol

- (Public-Key) Identification Protocol between Prover P and Verifier V
- P and V perform protocol π. Then, V accepts or rejects.



Identification Protocol

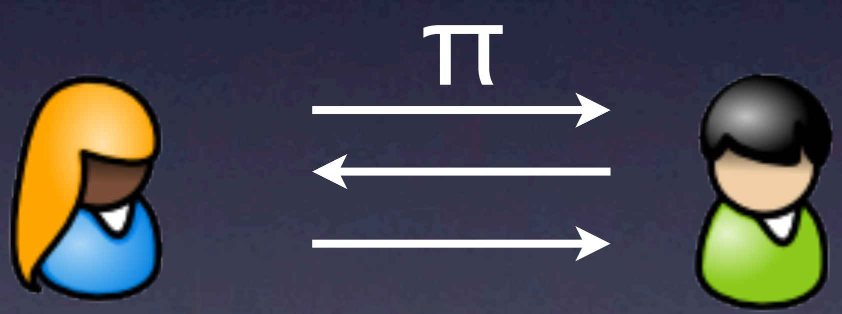
- (Public-Key) Identification Protocol between Prover P and Verifier V
- P and V perform protocol π. Then, V accepts or rejects.
- Security: No adversary who first interacts with the real prover can later make the verifier accept with non-negligible probability.



Identification Protocol

- (Public-Key) Identification Protocol between Prover P and Verifier V
- P and V perform protocol π. Then, V accepts or rejects.
- Security: No adversary who first interacts with the real prover can later make the verifier accept with non-negligible probability.

Verifier
pk

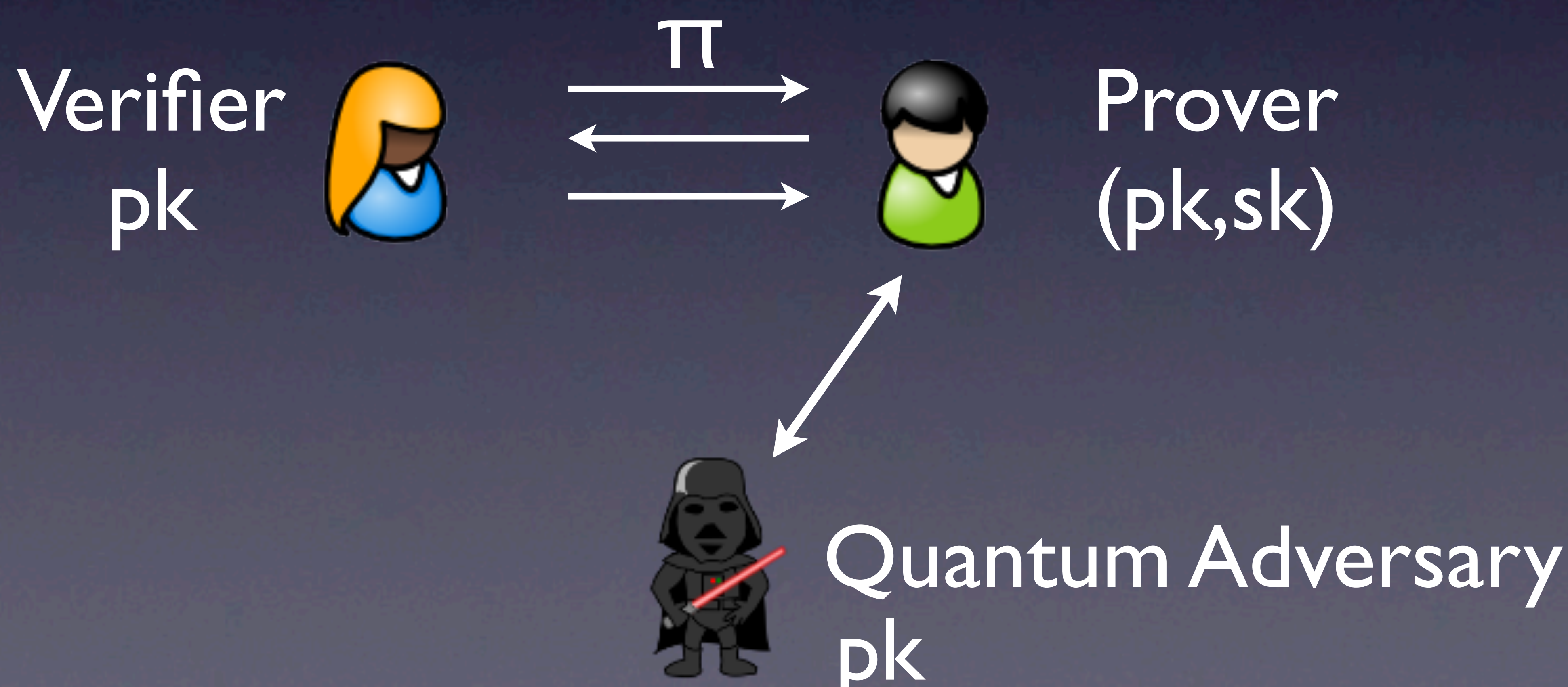


Prover
(pk,sk)

Quantum Adversary
pk

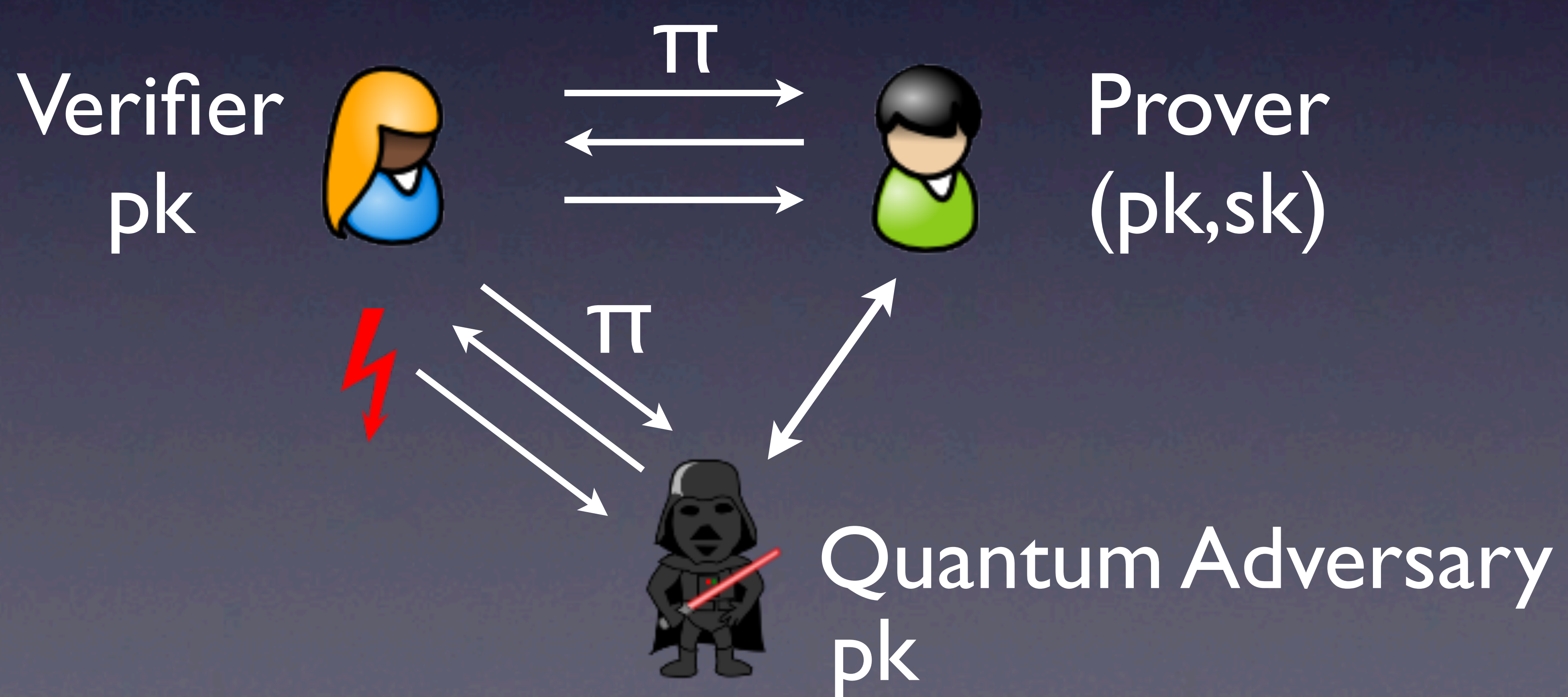
Identification Protocol

- (Public-Key) Identification Protocol between Prover P and Verifier V
- P and V perform protocol π. Then, V accepts or rejects.
- Security: No adversary who first interacts with the real prover can later make the verifier accept with non-negligible probability.

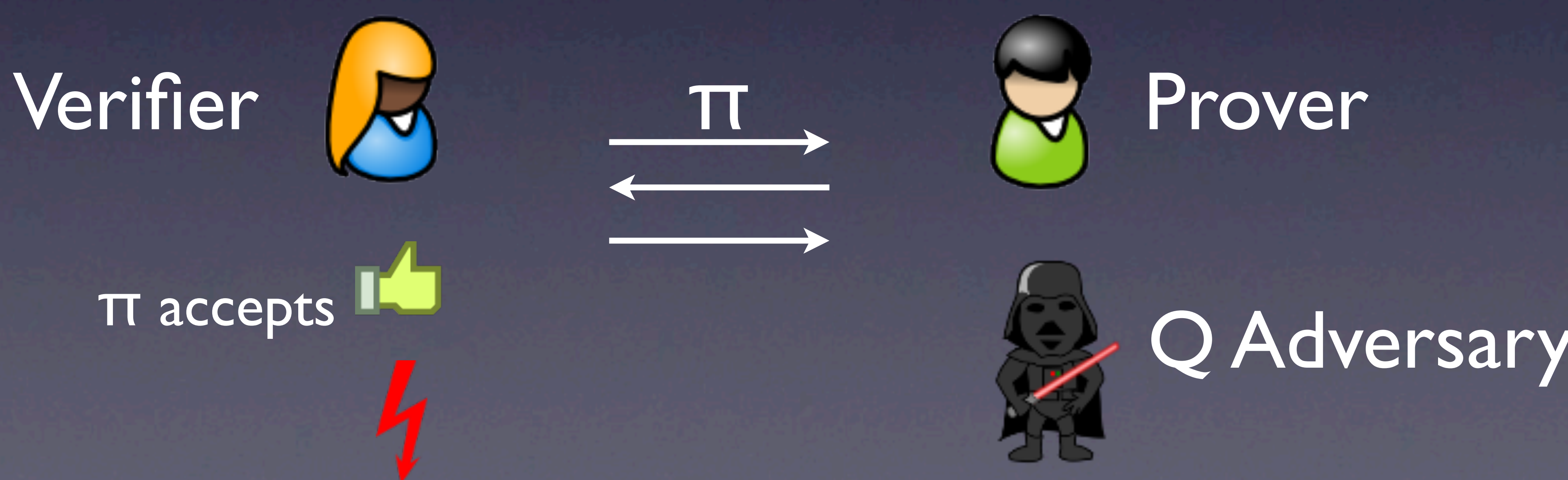


Identification Protocol

- (Public-Key) Identification Protocol between Prover P and Verifier V
- P and V perform protocol π. Then, V accepts or rejects.
- Security: No adversary who first interacts with the real prover can later make the verifier accept with non-negligible probability.

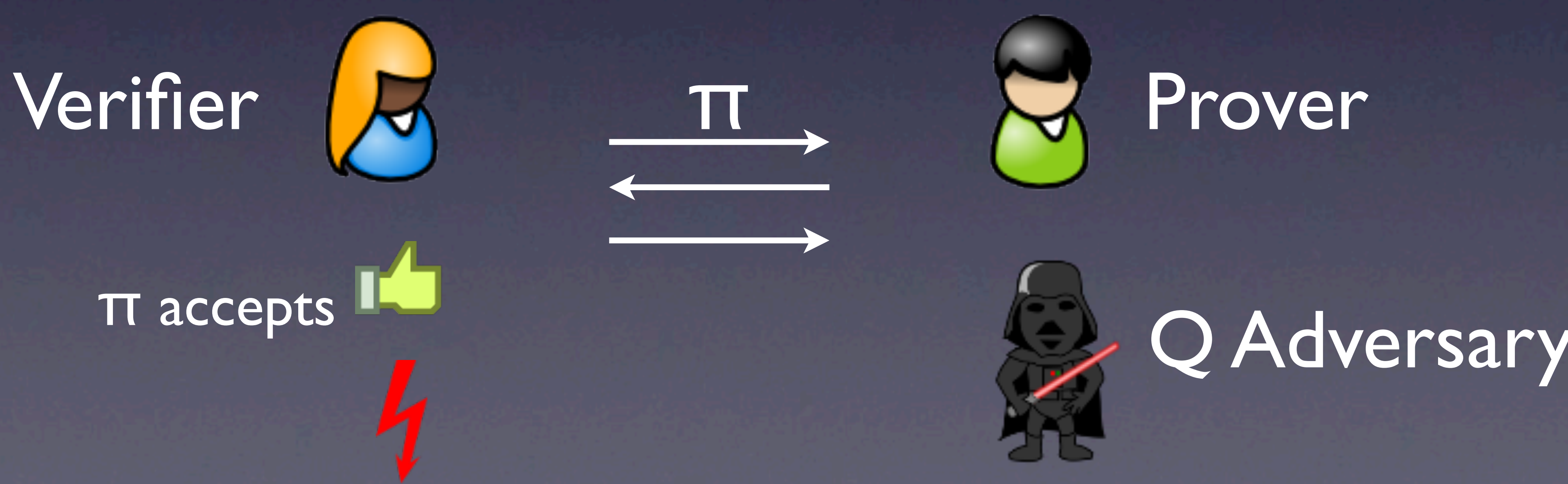


Separating QROM from CROM



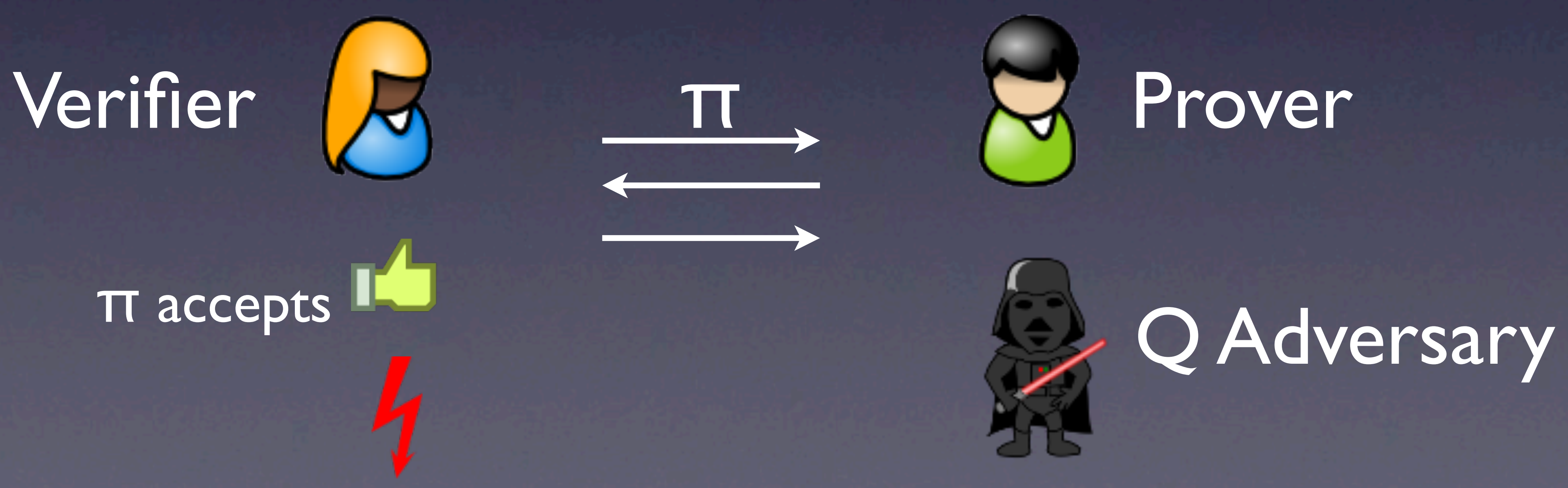
Separating QROM from CROM

- Idea: exploit the quantum speedup in collision finding



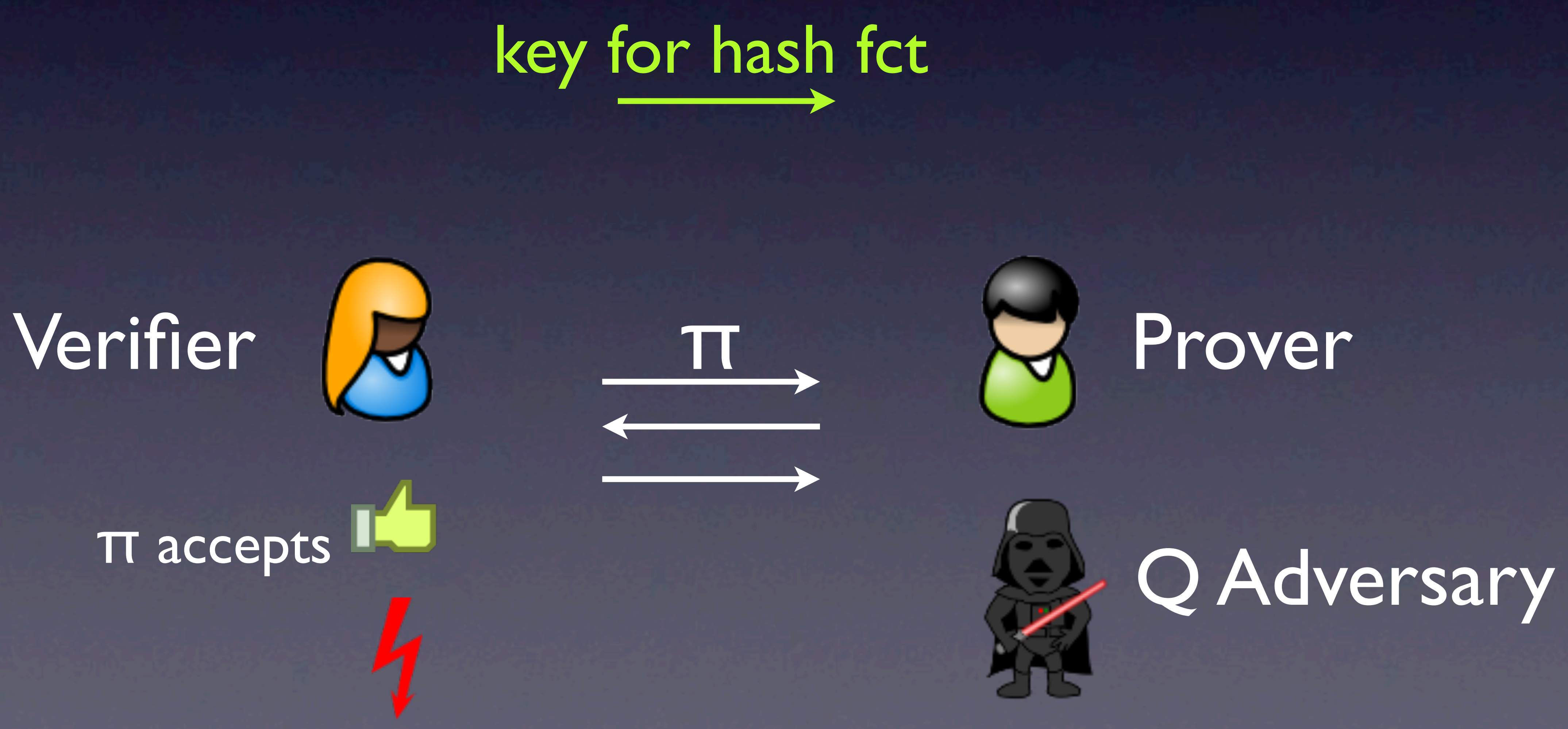
Separating QROM from CROM

- Idea: exploit the quantum speedup in collision finding
- "prepend" a collision-finding stage to a quantum-secure identification scheme π



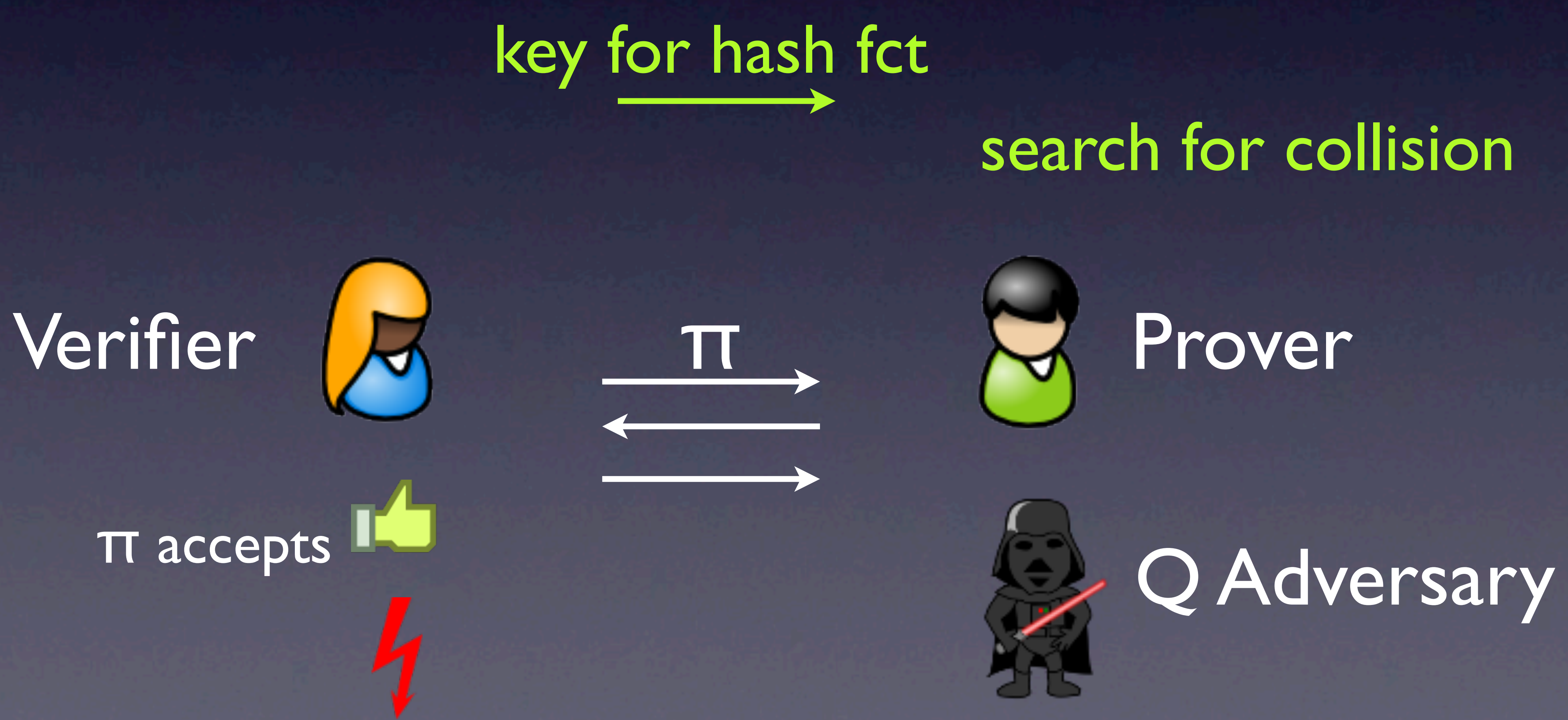
Separating QROM from CROM

- Idea: exploit the quantum speedup in collision finding
- "prepend" a collision-finding stage to a quantum-secure identification scheme π



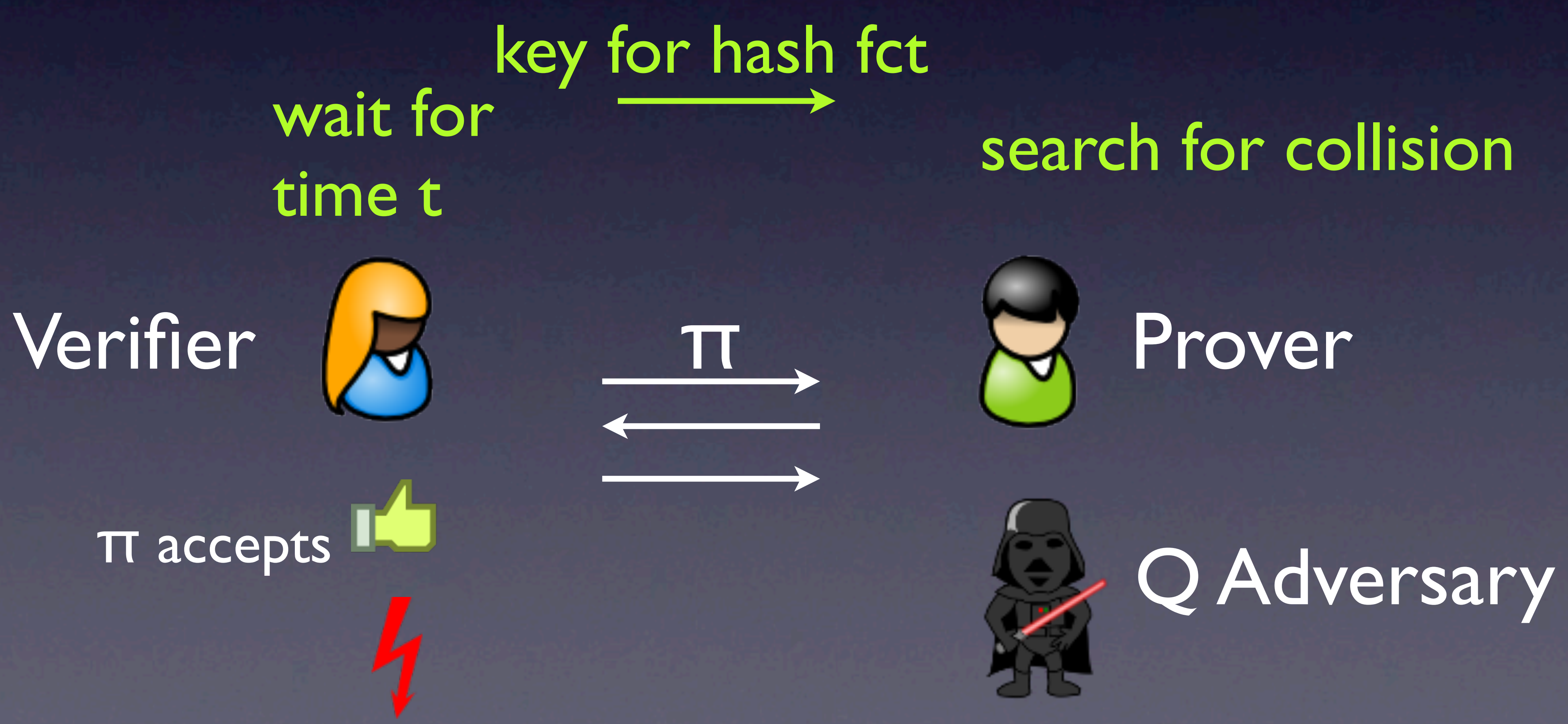
Separating QROM from CROM

- Idea: exploit the quantum speedup in collision finding
- “prepend” a collision-finding stage to a quantum-secure identification scheme π



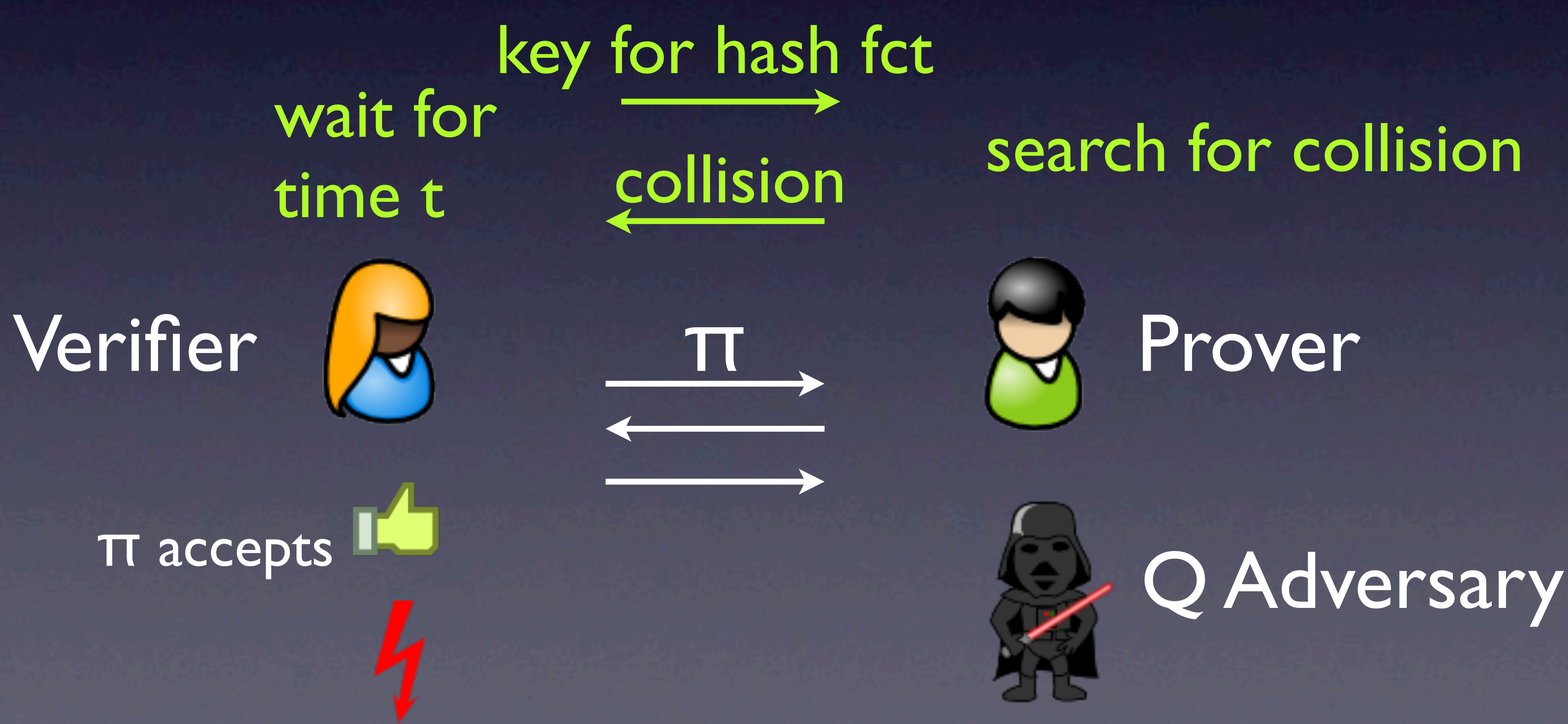
Separating QROM from CROM

- Idea: exploit the quantum speedup in collision finding
- "prepend" a collision-finding stage to a quantum-secure identification scheme π



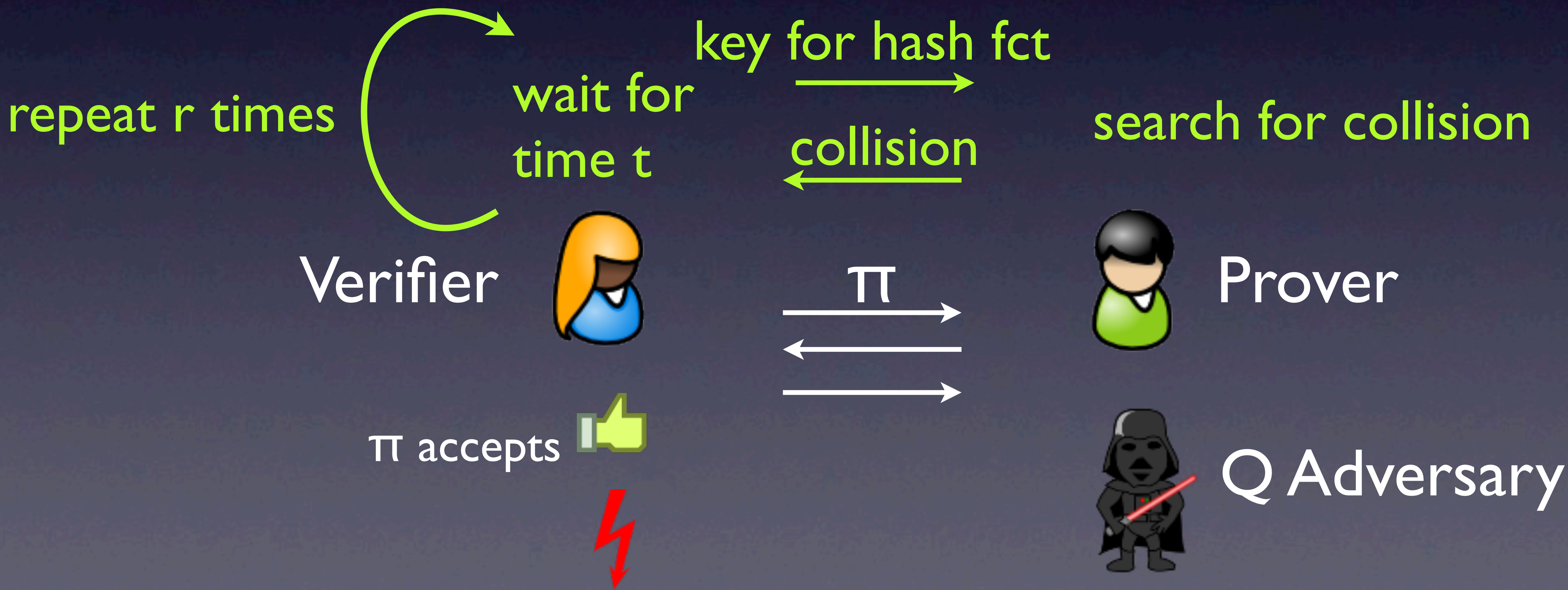
Separating QROM from CROM

- Idea: exploit the quantum speedup in collision finding
- "prepend" a collision-finding stage to a quantum-secure identification scheme π



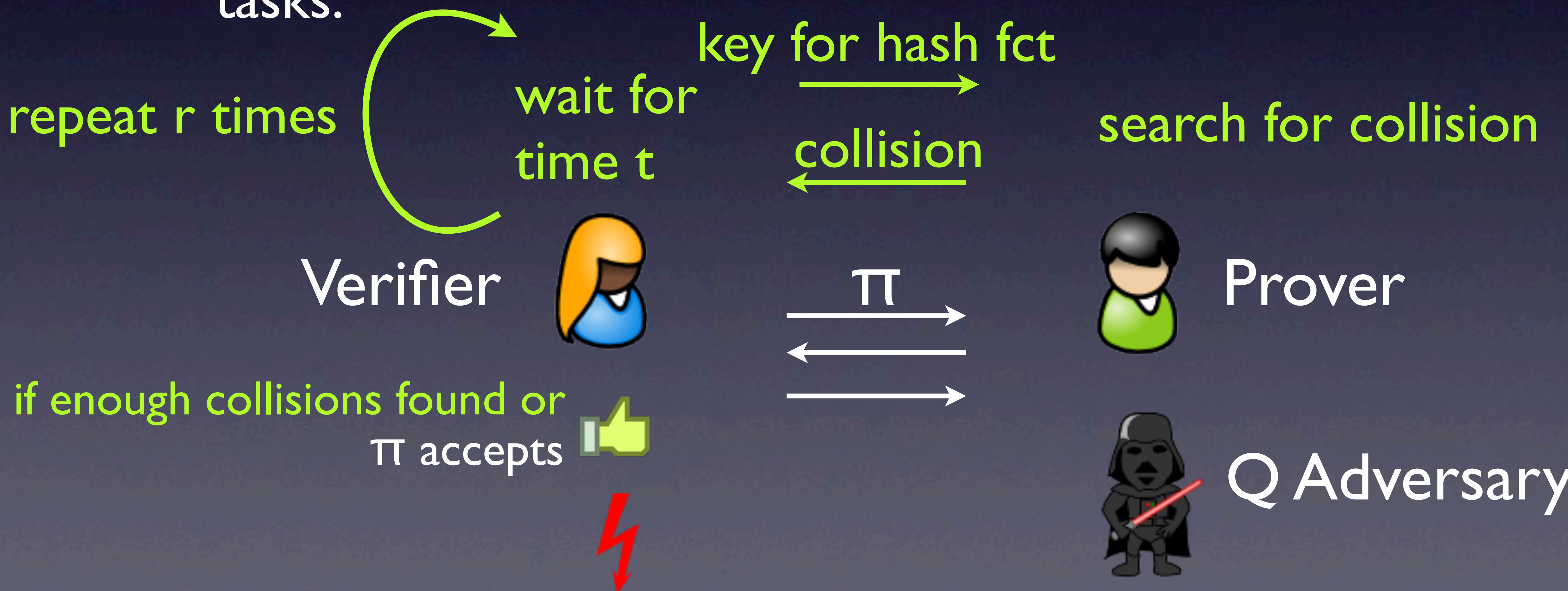
Separating QROM from CROM

- Idea: exploit the quantum speedup in collision finding
- “prepend” a collision-finding stage to a quantum-secure identification scheme π

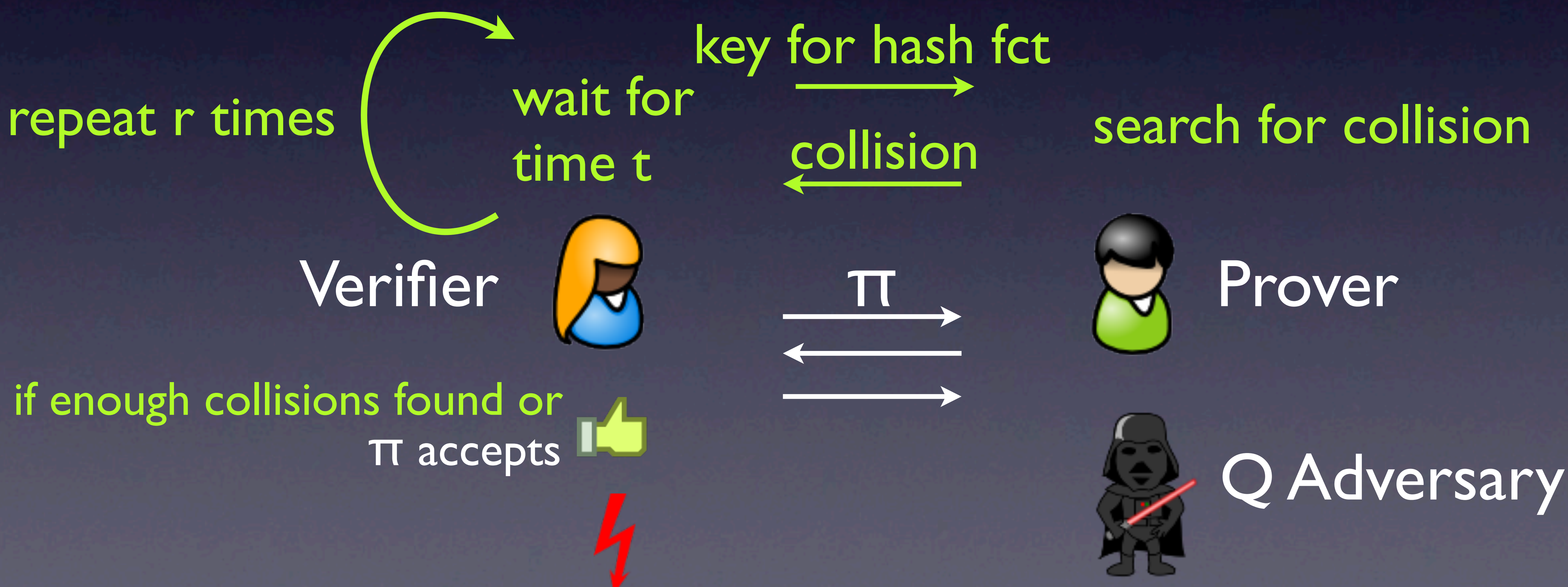


Separating QROM from CROM

- Idea: exploit the quantum speedup in collision finding
- "prepend" a collision-finding stage to a quantum-secure identification scheme π
- verifier accepts if prover succeeds in one of the two tasks.

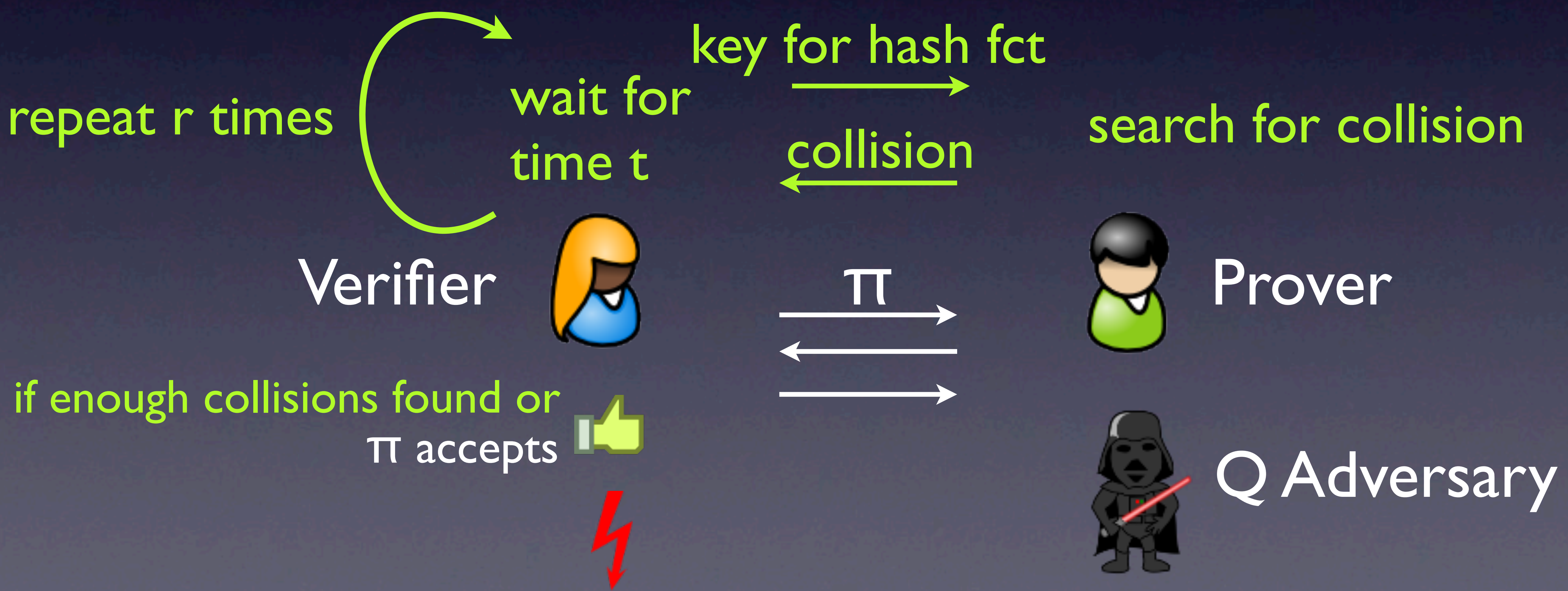


Separating QROM from CROM



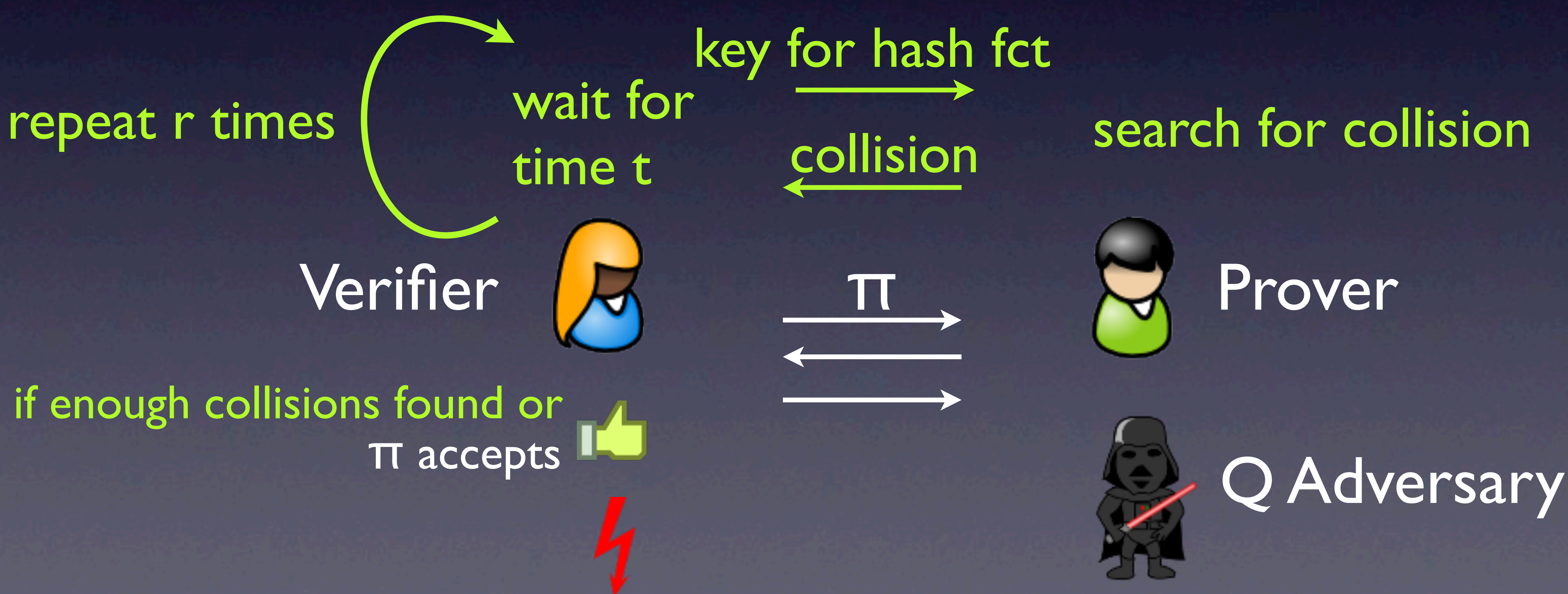
Separating QROM from CROM

- choose t such that collision-searcher with quantum access succeeds, but one with classical black-box access fails



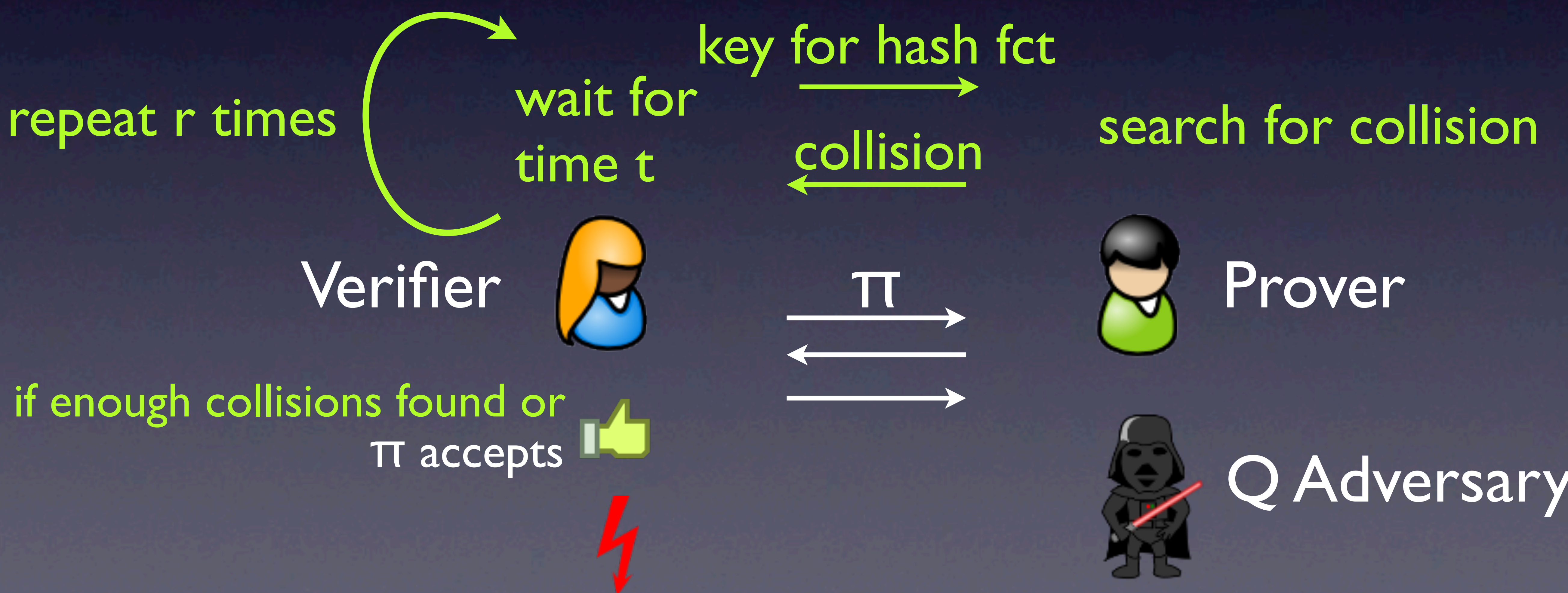
Separating QROM from CROM

- choose t such that collision-searcher with quantum access succeeds, but one with classical black-box access fails
- secure in classical ROM



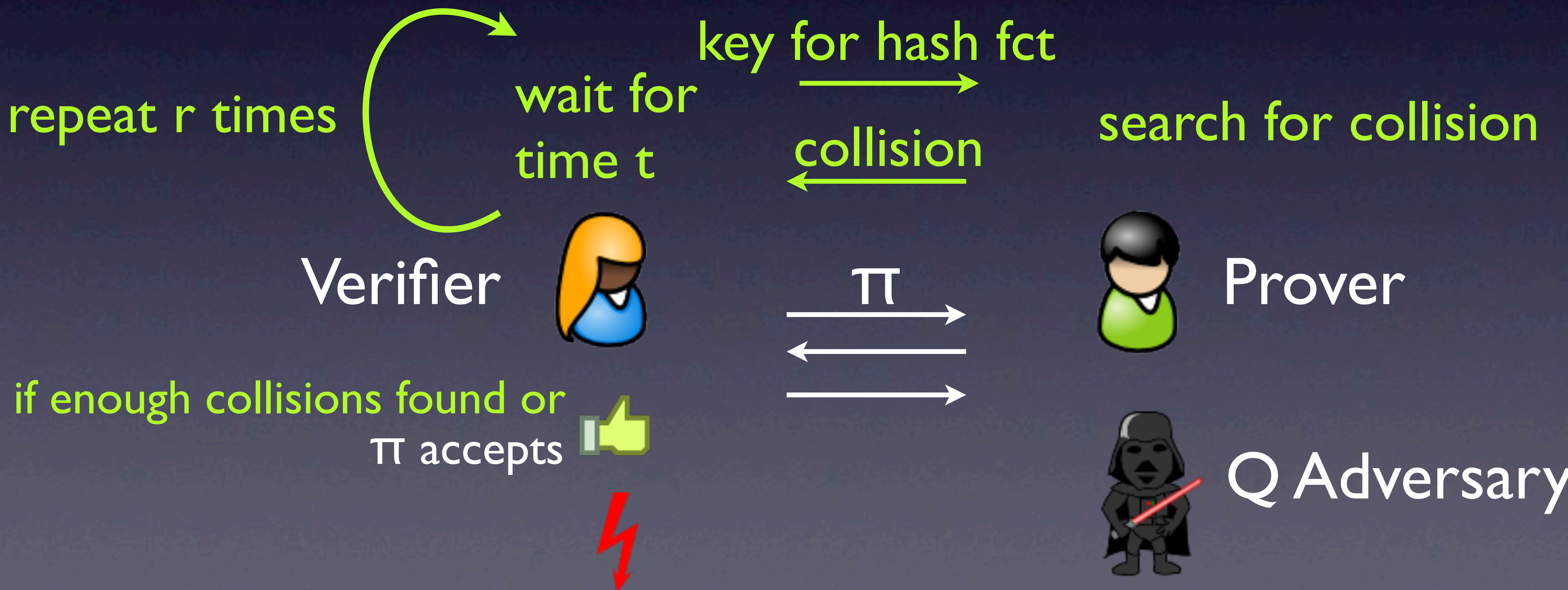
Separating QROM from CROM

- choose t such that collision-searcher with quantum access succeeds, but one with classical black-box access fails
- secure in classical ROM
- insecure in quantum ROM



Separating QROM from CROM

- choose t such that collision-searcher with quantum access succeeds, but one with classical black-box access fails
- secure in classical ROM
- insecure in quantum ROM
- insecure under any instantiation



Consequence

- All Post-Quantum cryptosystems proven in the RO model need to be revisited

Consequence

- All Post-Quantum cryptosystems proven in the RO model need to be revisited

Consequence

- All Post-Quantum cryptosystems proven in the RO model need to be revisited

- Good news:
    - Digital Signatures Schemes with "history-free" reductions are secure in the QROM
    - Encryption Schemes: CPA security of [BR93] and CCA security of hybrid encryption [BR93]

 $\Rightarrow$ 

Roadmap

- ✓ What’s the problem?
- ✓ Separation of QROM and CROM
- Secure Schemes in the QROM
- Open Problems

[GPV08] signatures

- Hash-and-sign principle:
- $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$
- $\mathrm{Vrfy}_{pk}(m,\sigma)$ accepts if and only if $f_{pk}(\sigma)=H(m)$

[GPV08] signatures

- Hash-and-sign principle:
- $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$
- $\mathrm{Vrfy}_{pk}(m,\sigma)$ accepts if and only if $f_{pk}(\sigma)=H(m)$

Theorem: Suppose (G,f,f^{-1}) is a quantum-secure preimage-sampleable function and quantum-accessible PRFs exist, then GPV signatures are secure in the QROM.

Preimage Sampleable Trapdoor Functions (PSF)

- Key Generation: $G(1^n) = (sk,pk)$
- $f_{pk}(x)$ is efficiently computable
  and uniformly distributed for random x

Preimage Sampleable Trapdoor Functions (PSF)

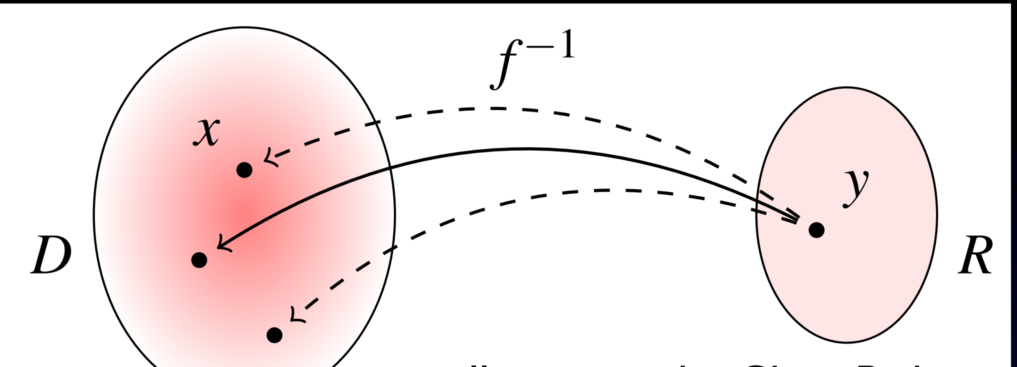
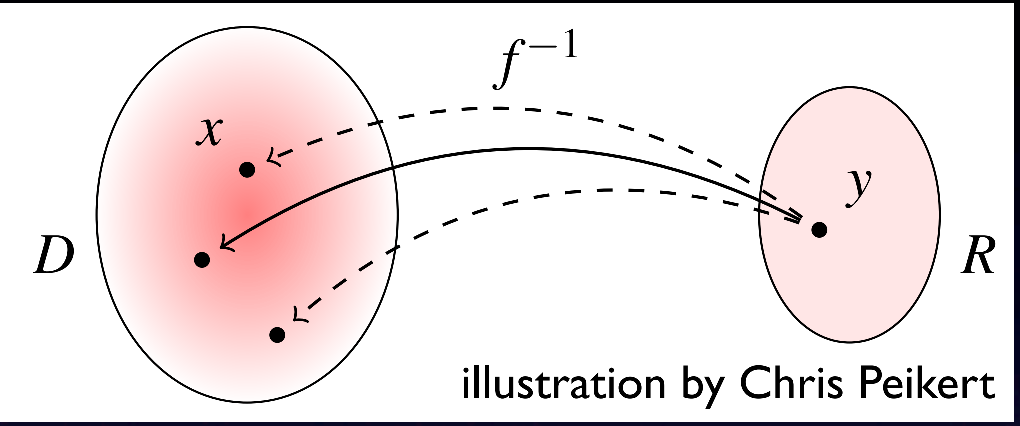


illustration by Chris Peikert

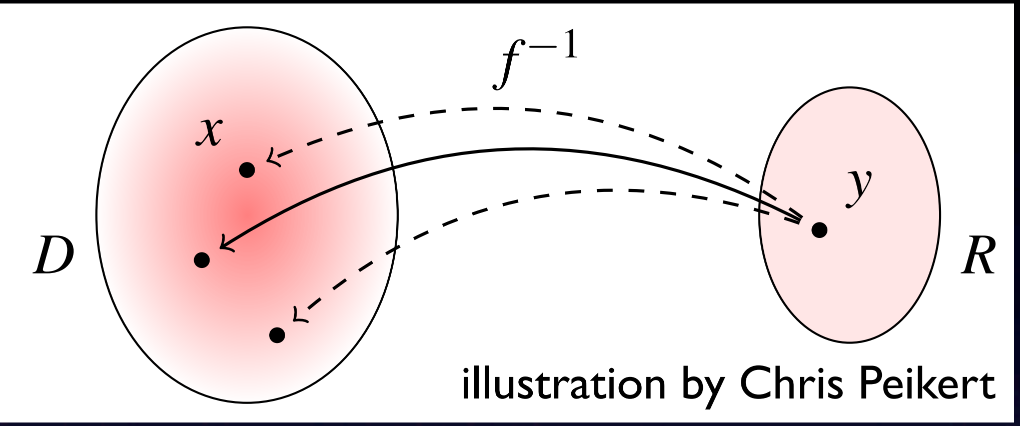
- Key Generation: $G(1^n) = (sk,pk)$
- $f_{pk}(x)$ is efficiently computable and uniformly distributed for random x
- $f^{-1}_{sk}(y)$ samples randomly from those x with $f_{pk}(x)=y$

Preimage Sampleable Trapdoor Functions (PSF)



- Key Generation: $G(1^n) = (sk,pk)$
- $f_{pk}(x)$ is efficiently computable and uniformly distributed for random x
- $f^{-1}_{sk}(y)$ samples randomly from those x with $f_{pk}(x)=y$
- (G,f,f^{-1}) is secure if it is one-way, collision-resistant and has high preimage min-entropy

Preimage Sampleable Trapdoor Functions (PSF)



- Key Generation: $G(1^n) = (sk,pk)$
- $f_{pk}(x)$ is efficiently computable and uniformly distributed for random x
- $f^{-1}{}_{sk}(y)$ samples randomly from those x with $f_{pk}(x)=y$
- (G,f,f^{-1}) is secure if it is one-way, collision-resistant and has high preimage min-entropy
- secure construction from lattices [GPV08]

Quantum-Accessible PseudoRandom Functions (PRF)

- efficiently computable function family such that for all efficient quantum distinguishers D:

$$\left| \Pr[D^{PRF(k,\cdot)}(1^n) = 1] - \Pr[D^{O(\cdot)}(1^n) = 1] \right|$$

is negligible.

However, currently no constructions are known

Quantum-Accessible PseudoRandom Functions (PRF)

- efficiently computable function family such that for all efficient quantum distinguishers D:

$$\left| \Pr[D^{PRF(k,\cdot)}(1^n) = 1] - \Pr[D^{O(\cdot)}(1^n) = 1] \right|$$

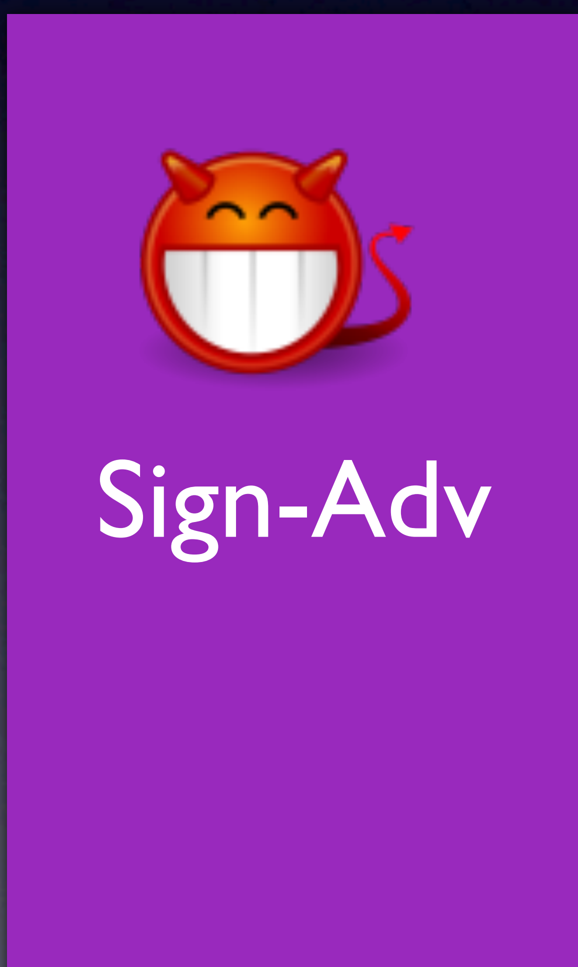
is negligible.

quantum access

However, currently no constructions are known

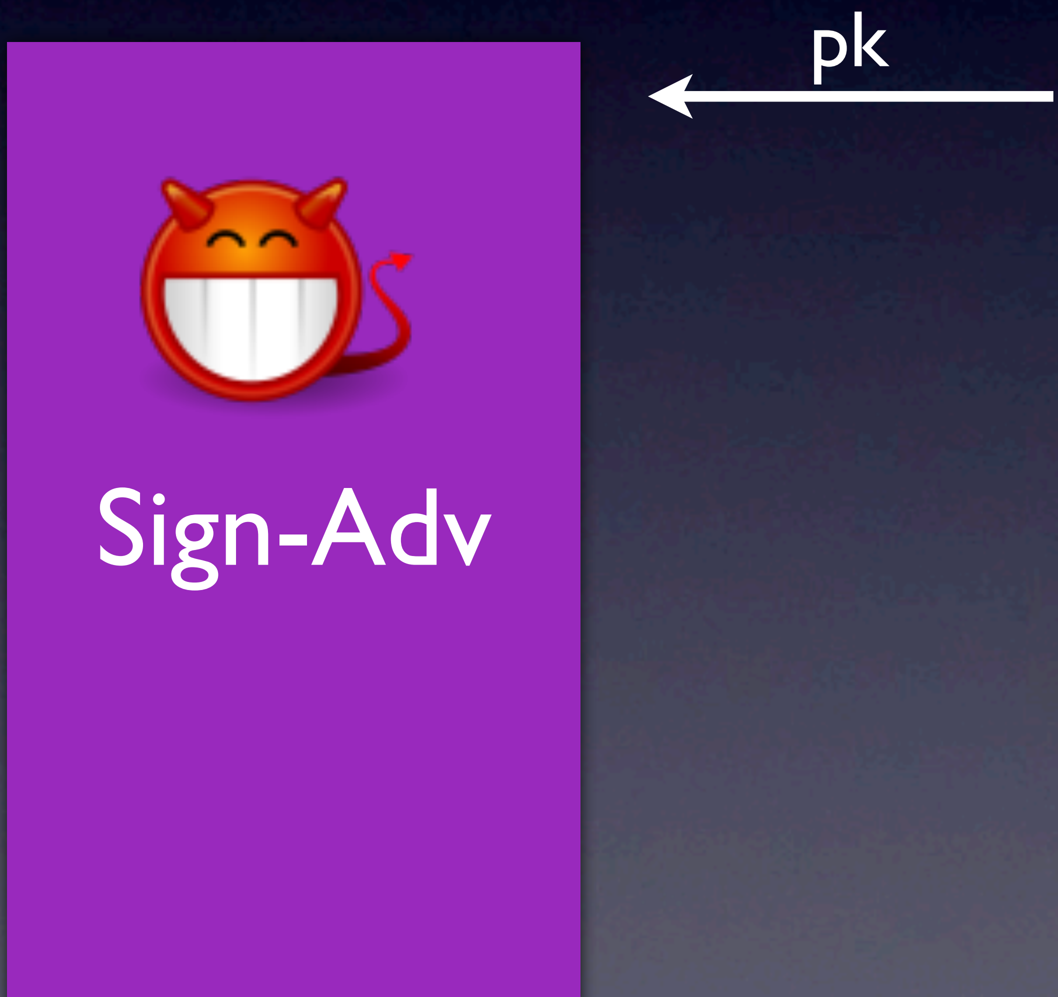
Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



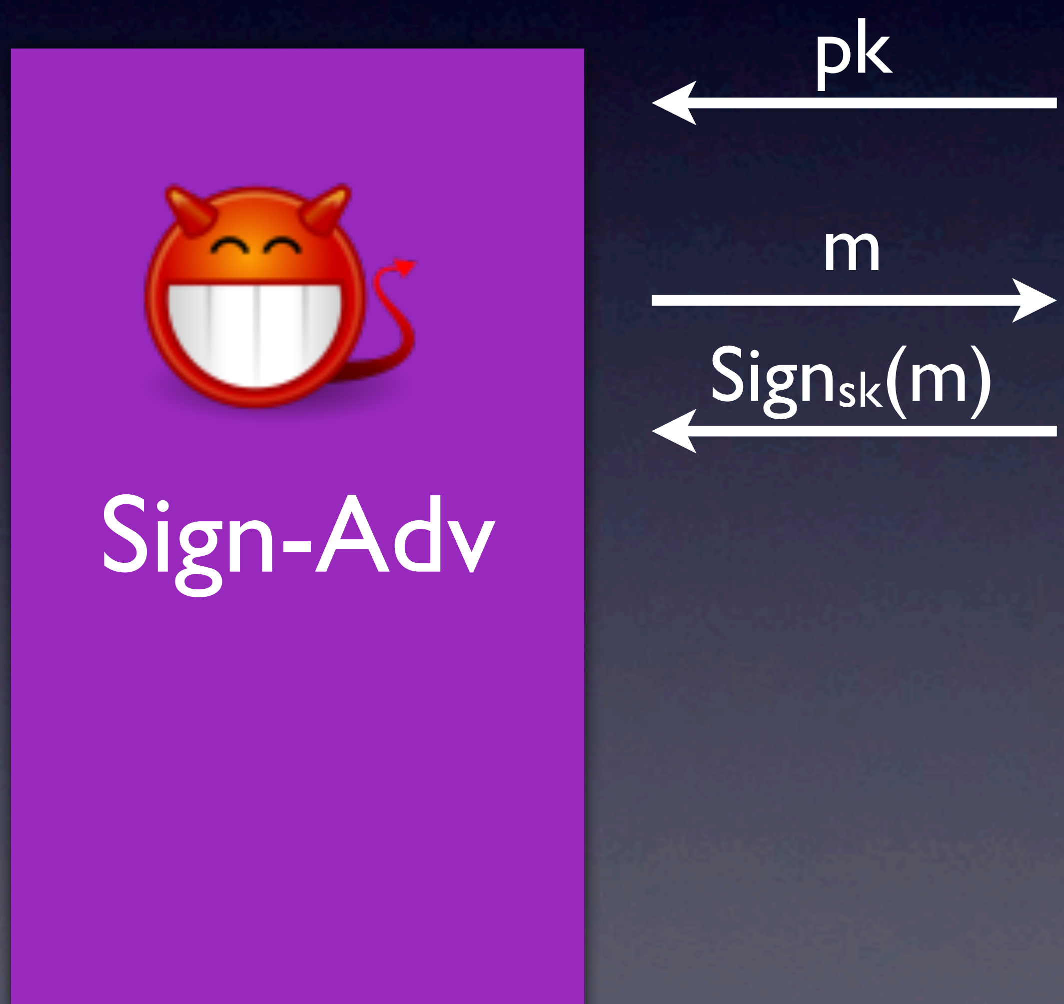
Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



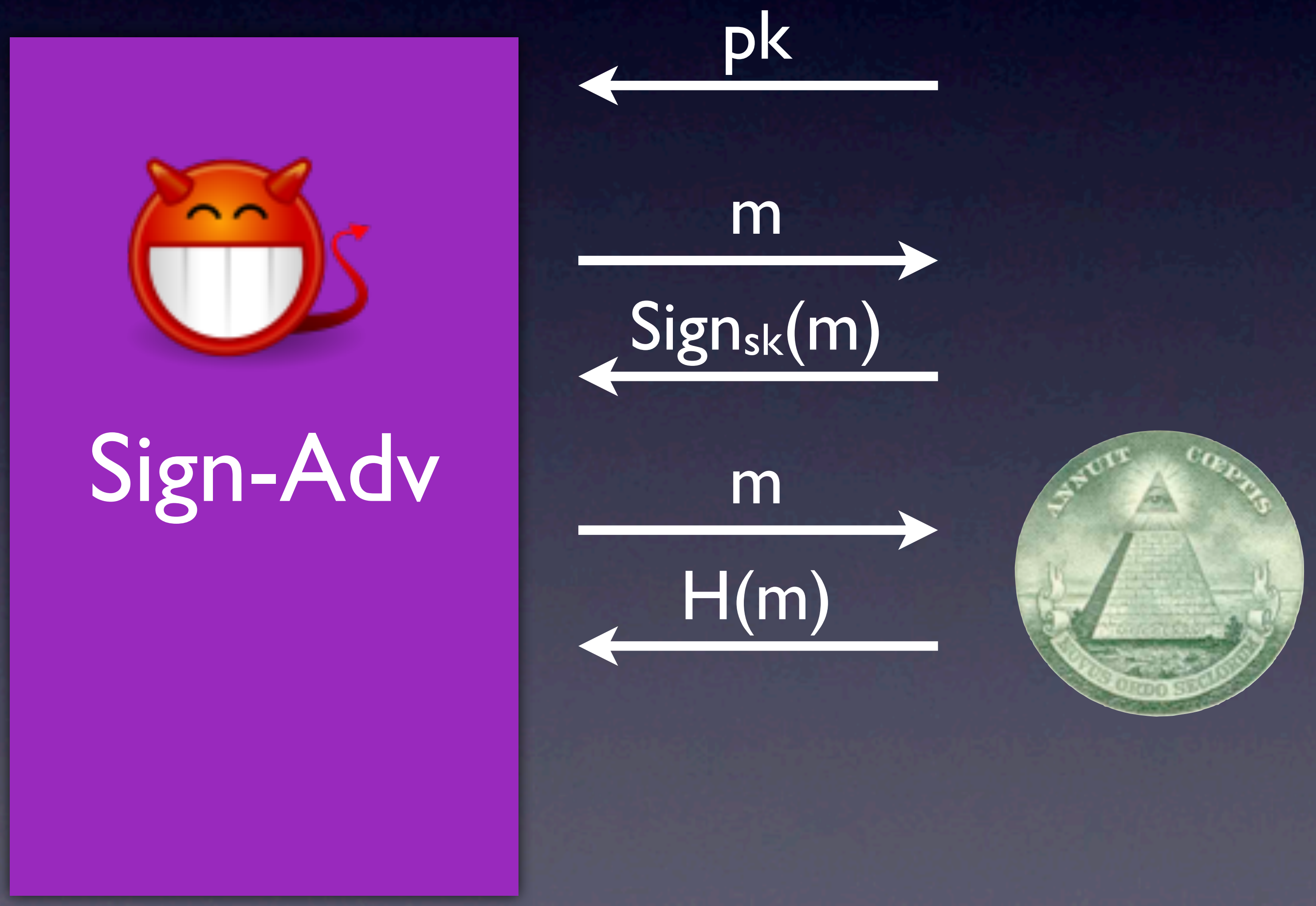
Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



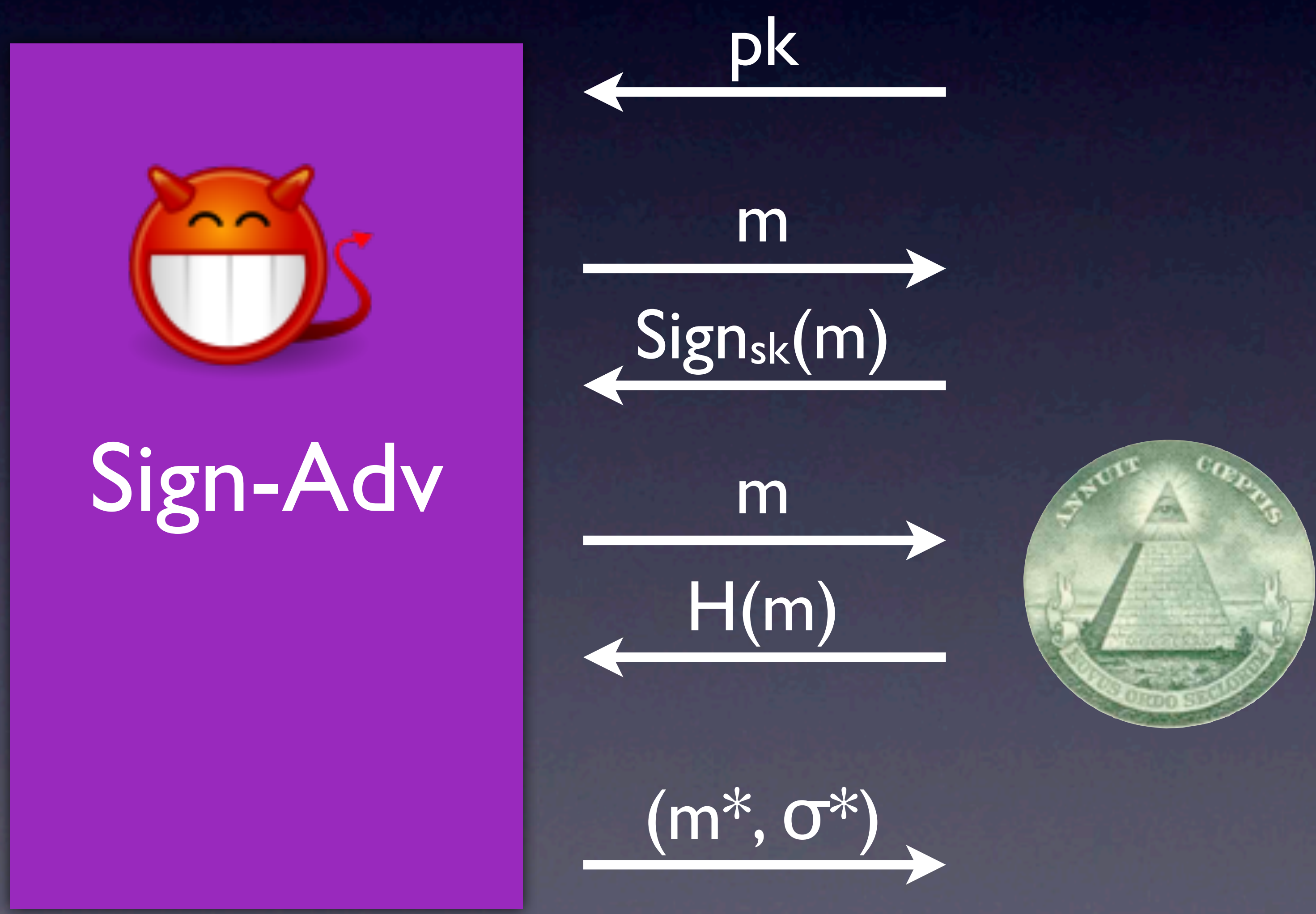
Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



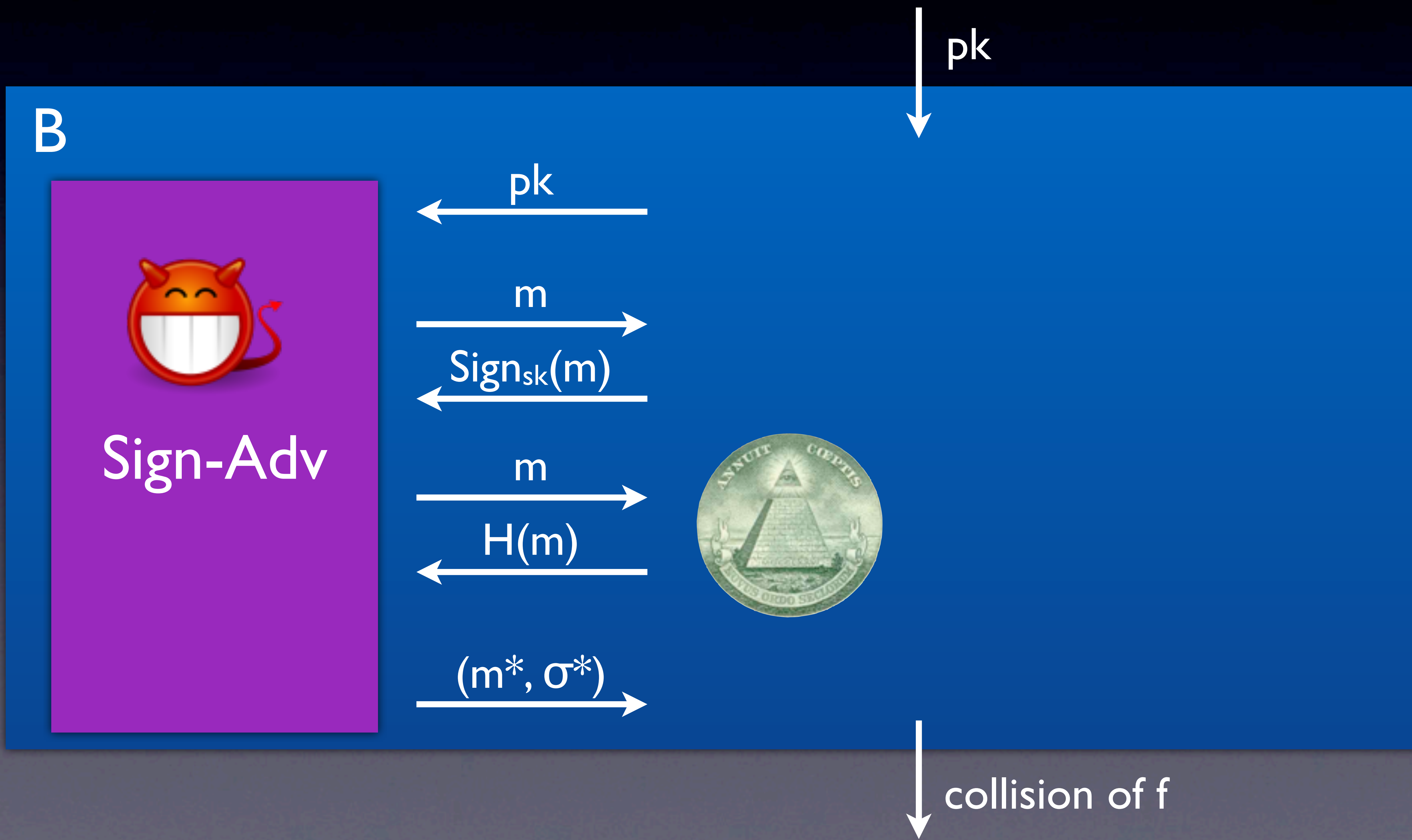
Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM

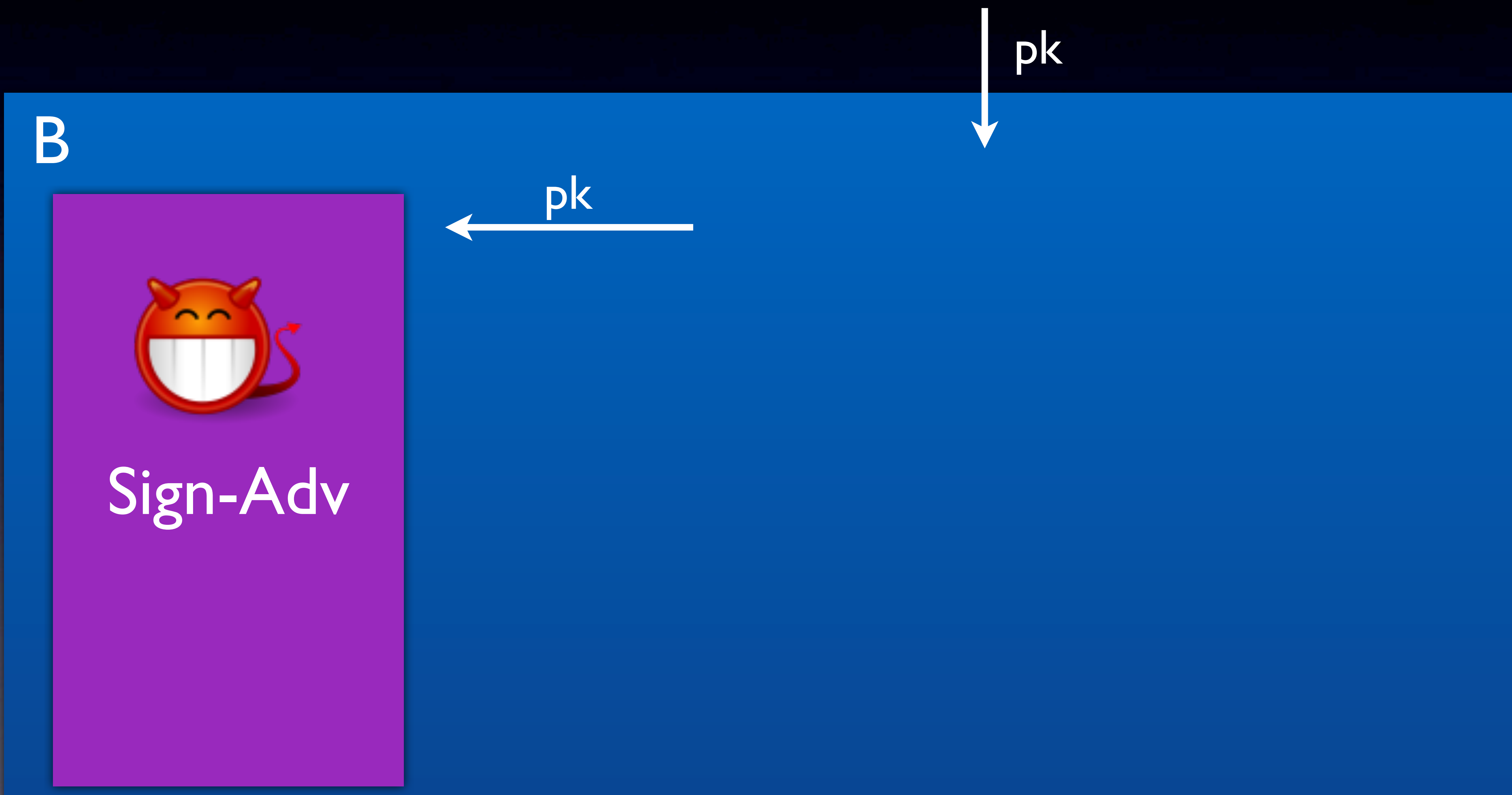


Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM

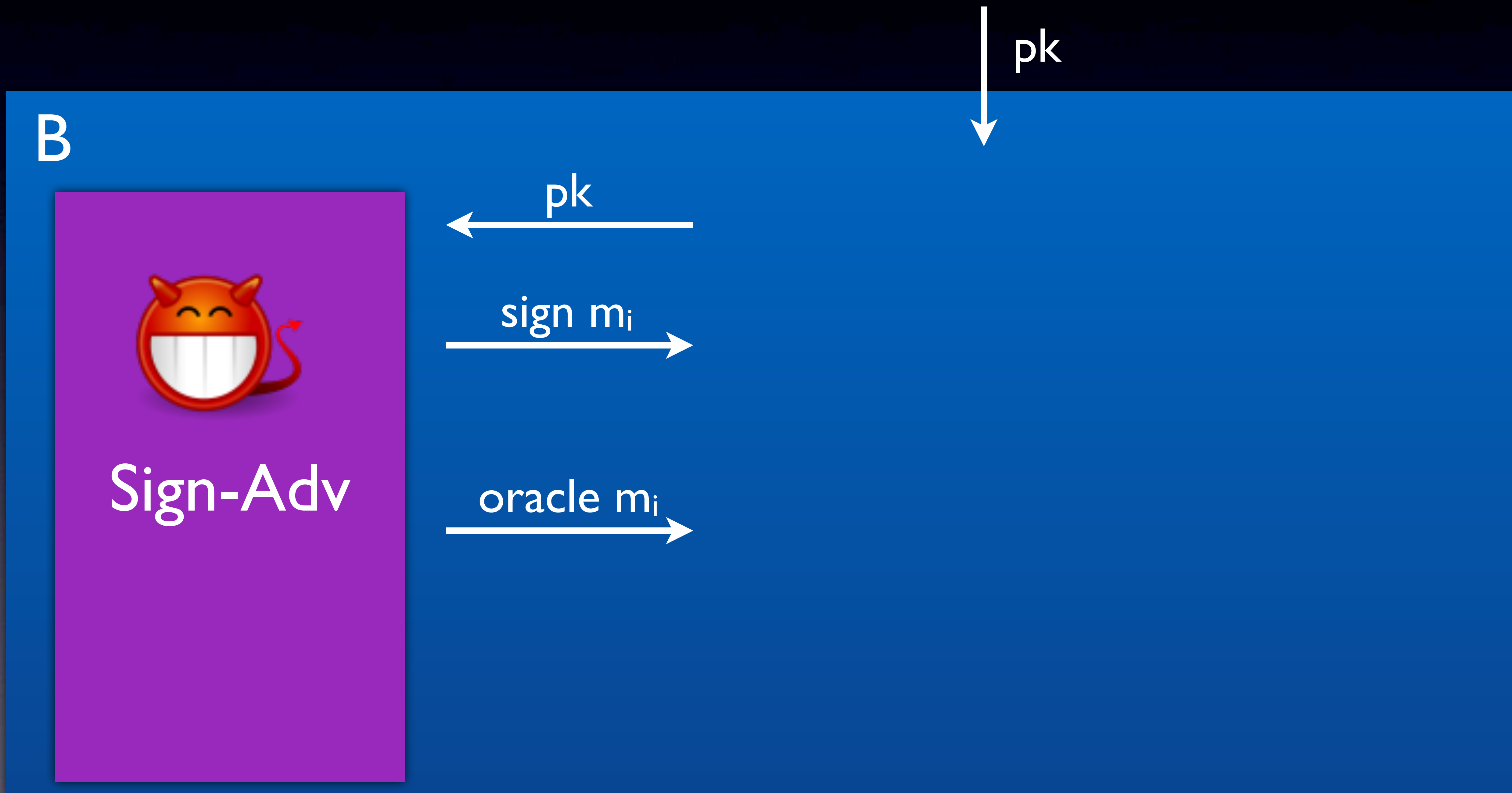
Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



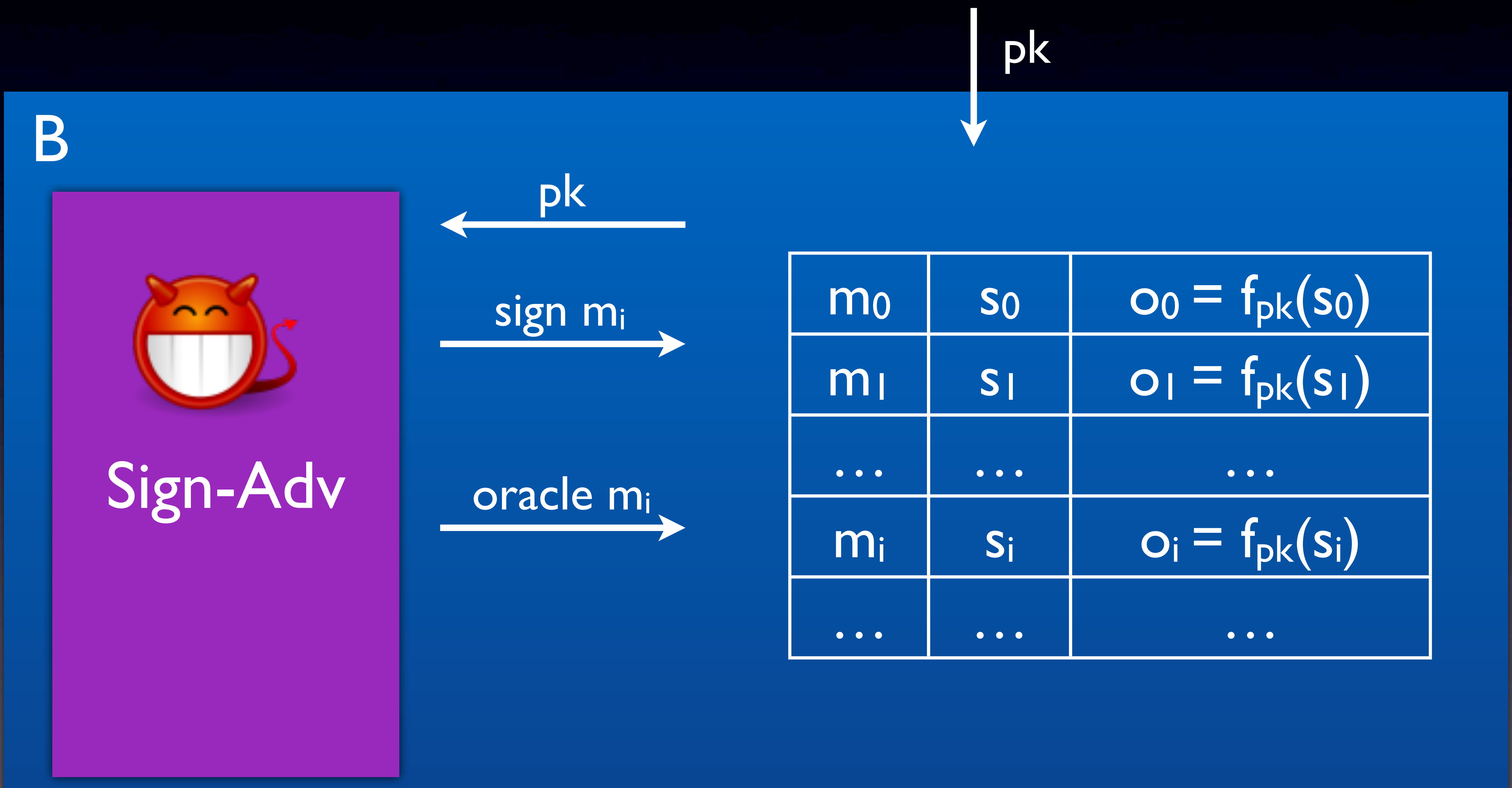
Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\text{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



Classical ROM Proof

Theorem: Suppose (G, f, f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



m_0	s_0	$o_0 = f_{pk}(s_0)$
m_1	s_1	$o_1 = f_{pk}(s_1)$
...	...	...
m_i	s_i	$o_i = f_{pk}(s_i)$
...	...	...

Classical ROM Proof

Theorem: Suppose (G, f, f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM

pk

B

Sign-Adv

pk

sign m_i

s_i

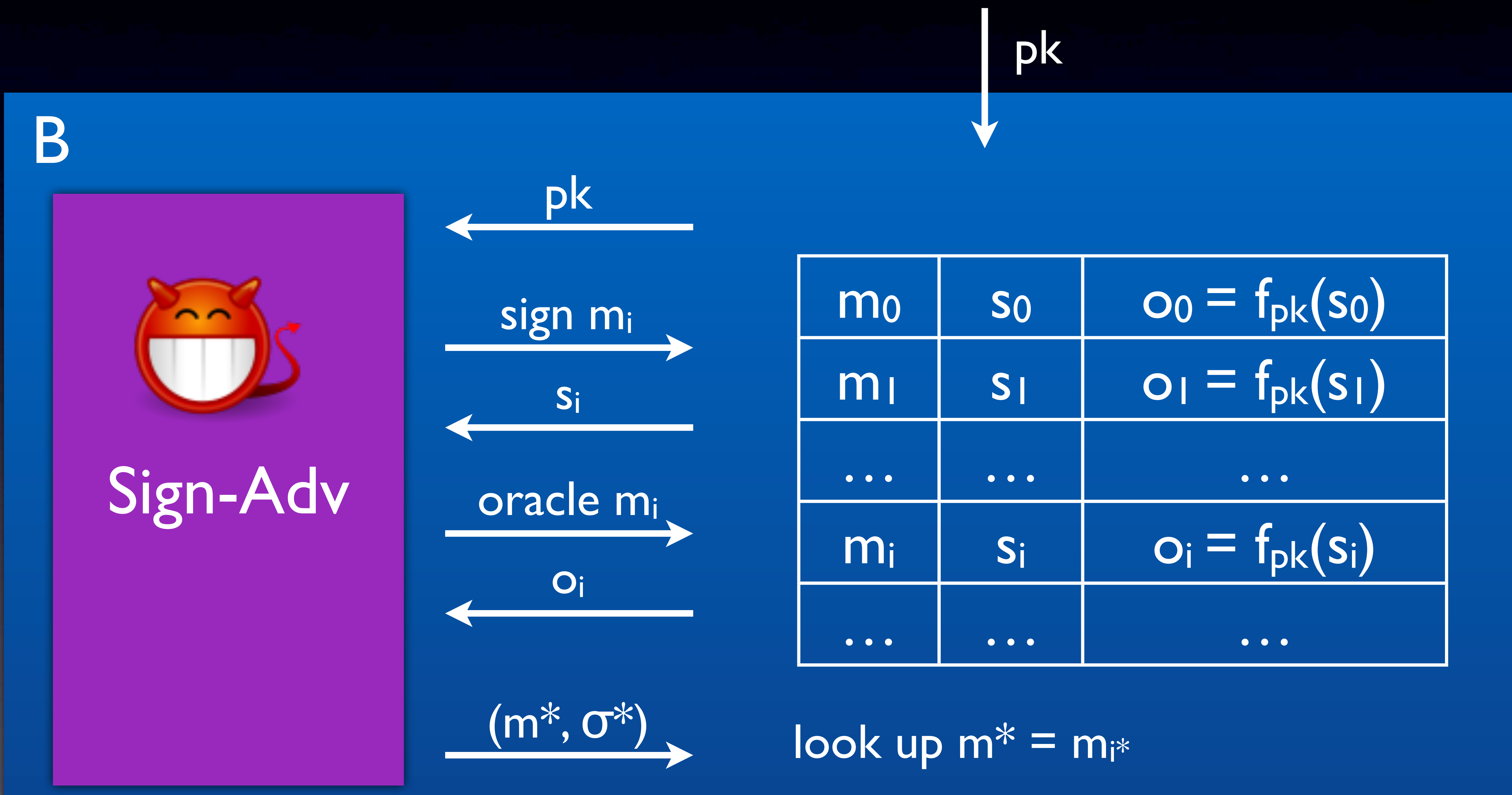
oracle m_i

o_i

m_0	s_0	$o_0 = f_{pk}(s_0)$
m_1	s_1	$o_1 = f_{pk}(s_1)$
…	…	…
m_i	s_i	$o_i = f_{pk}(s_i)$
…	…	…

Classical ROM Proof

Theorem: Suppose (G, f, f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



m_0	s_0	$o_0 = f_{pk}(s_0)$
m_1	s_1	$o_1 = f_{pk}(s_1)$
...	...	...
m_i	s_i	$o_i = f_{pk}(s_i)$
...	...	...

Classical ROM Proof

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM

pk

B

Sign-Adv

$\xleftarrow{\text{pk}}$

$\xrightarrow{\text{sign } m_i}$

$\xleftarrow{s_i}$

$\xrightarrow{\text{oracle } m_i}$

$\xleftarrow{o_i}$

m_0	s_0	$o_0 = f_{pk}(s_0)$
m_1	s_1	$o_1 = f_{pk}(s_1)$
...	...	...
m_i	s_i	$o_i = f_{pk}(s_i)$
...	...	...

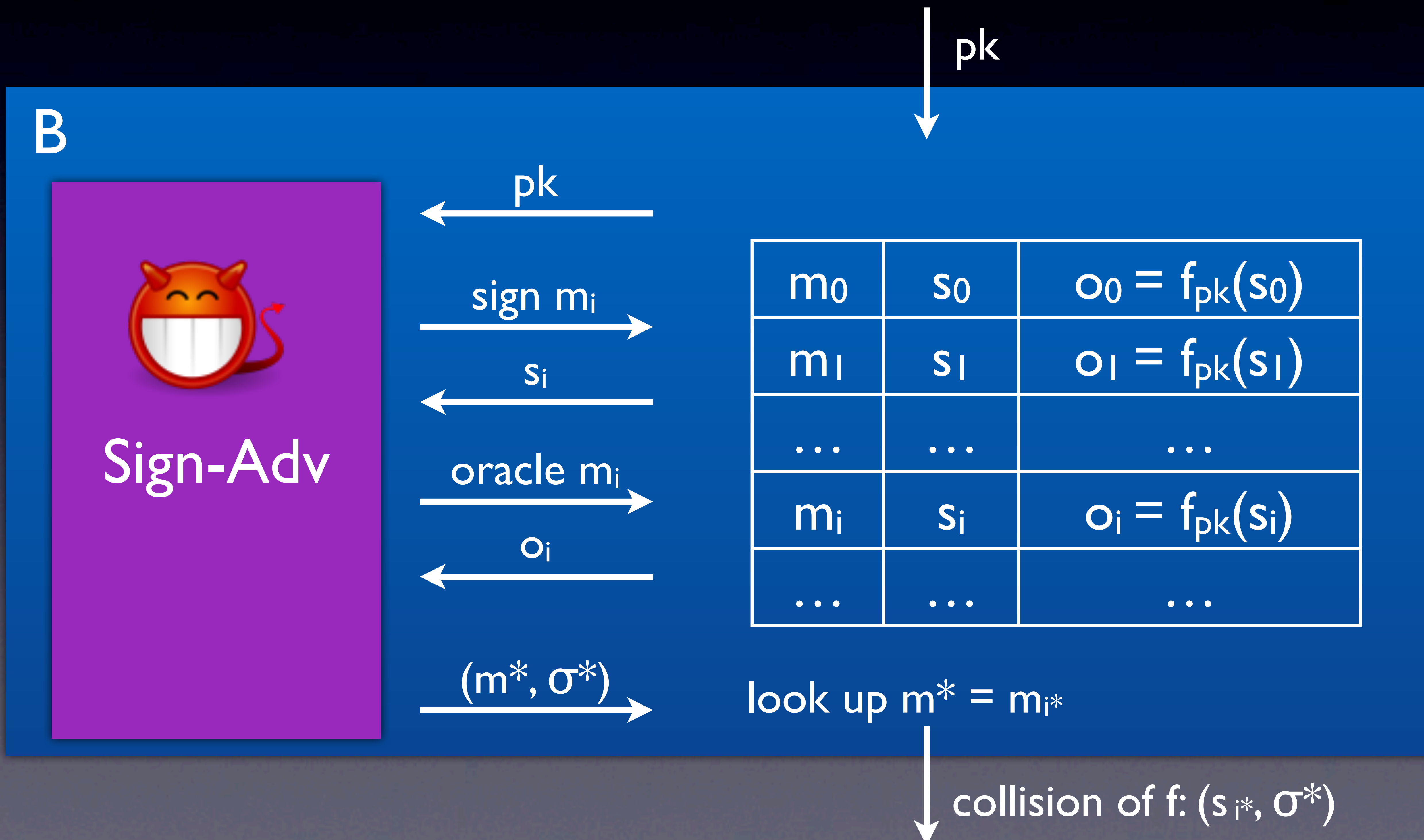
$\xrightarrow{(m^*, \sigma^*)}$

look up $m^* = m_{i^*}$

collision of f: (s_{i^*}, σ^*)

Classical ROM Proof

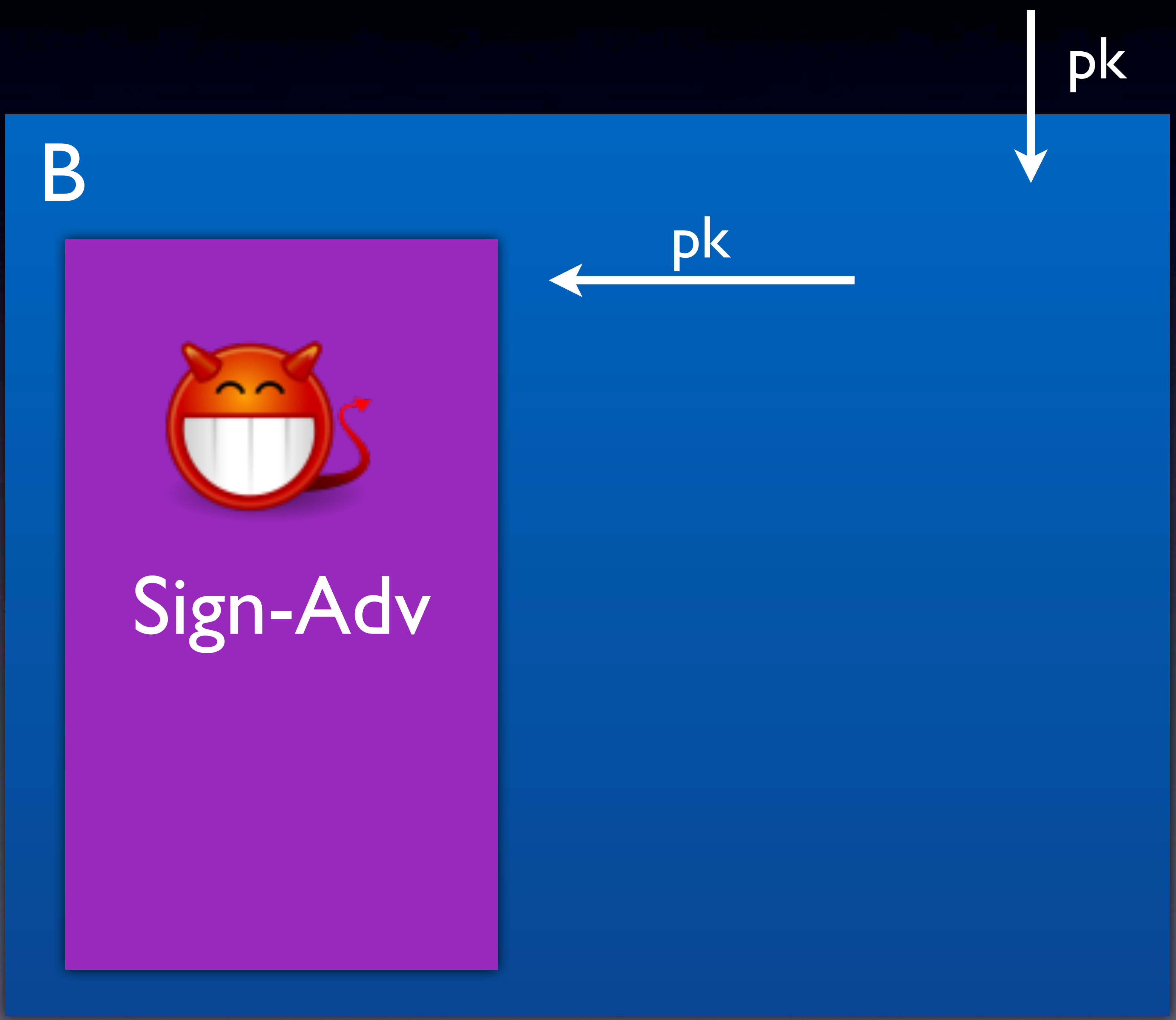
Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



$\blacksquare$

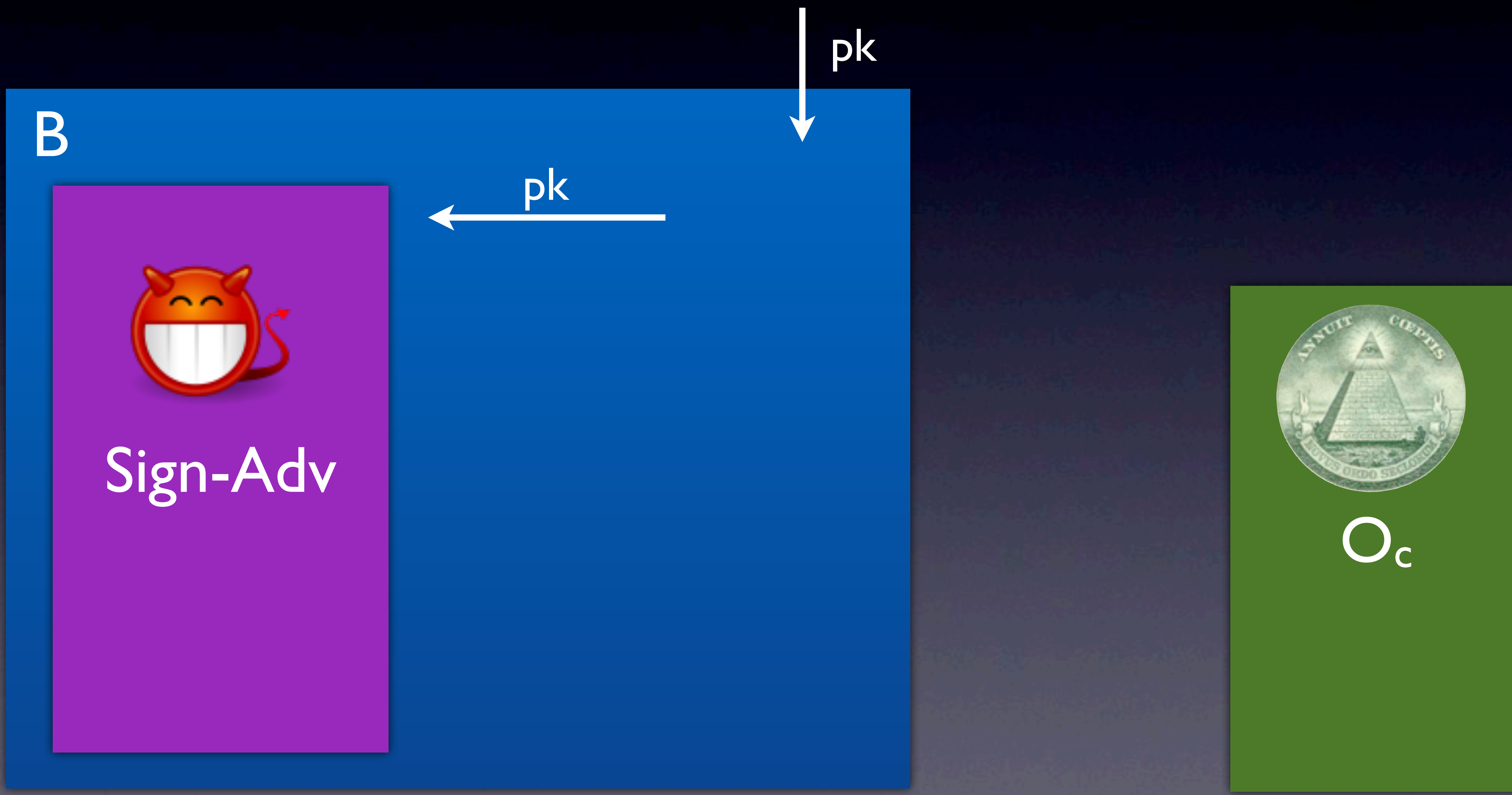
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



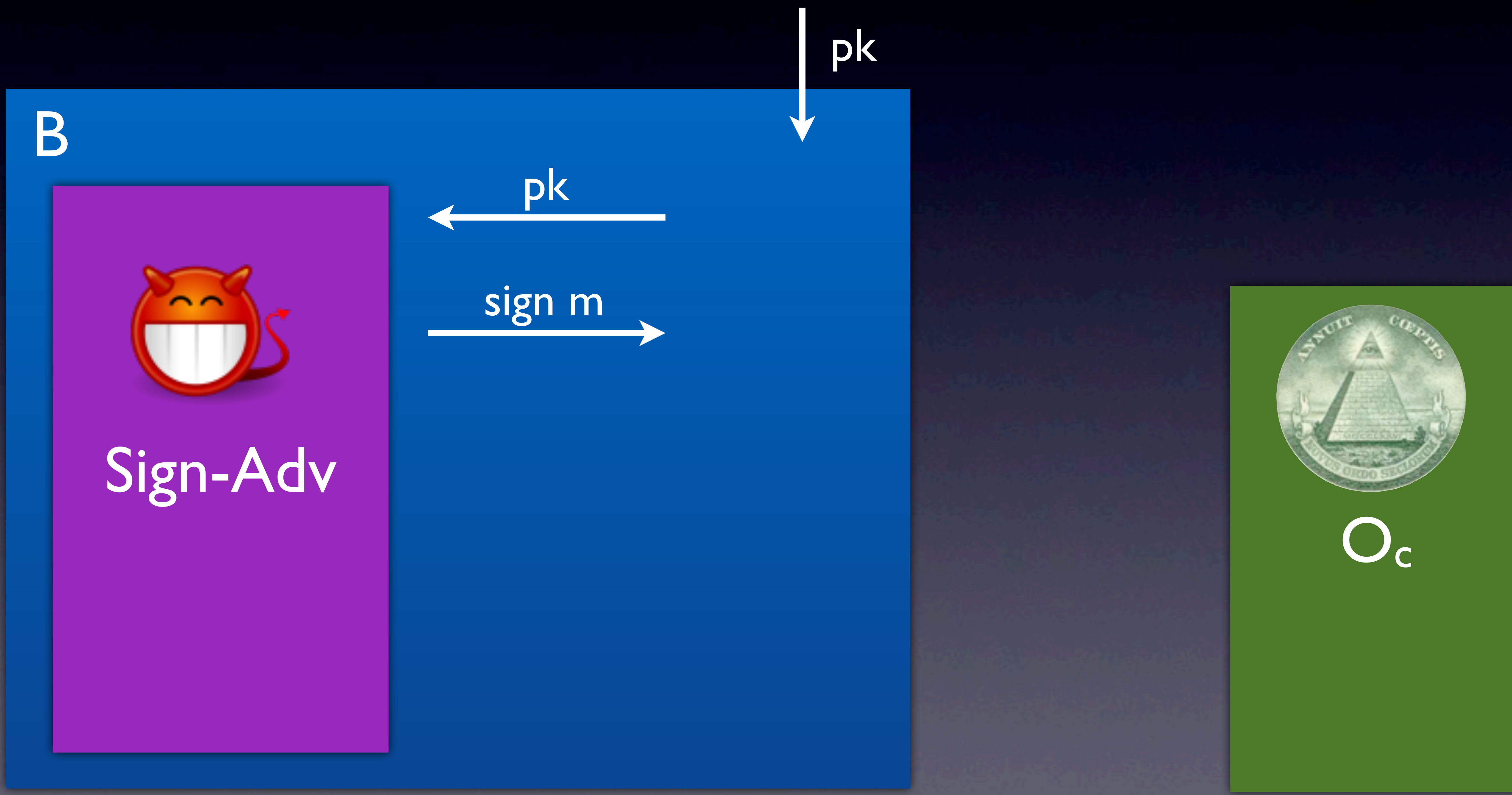
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



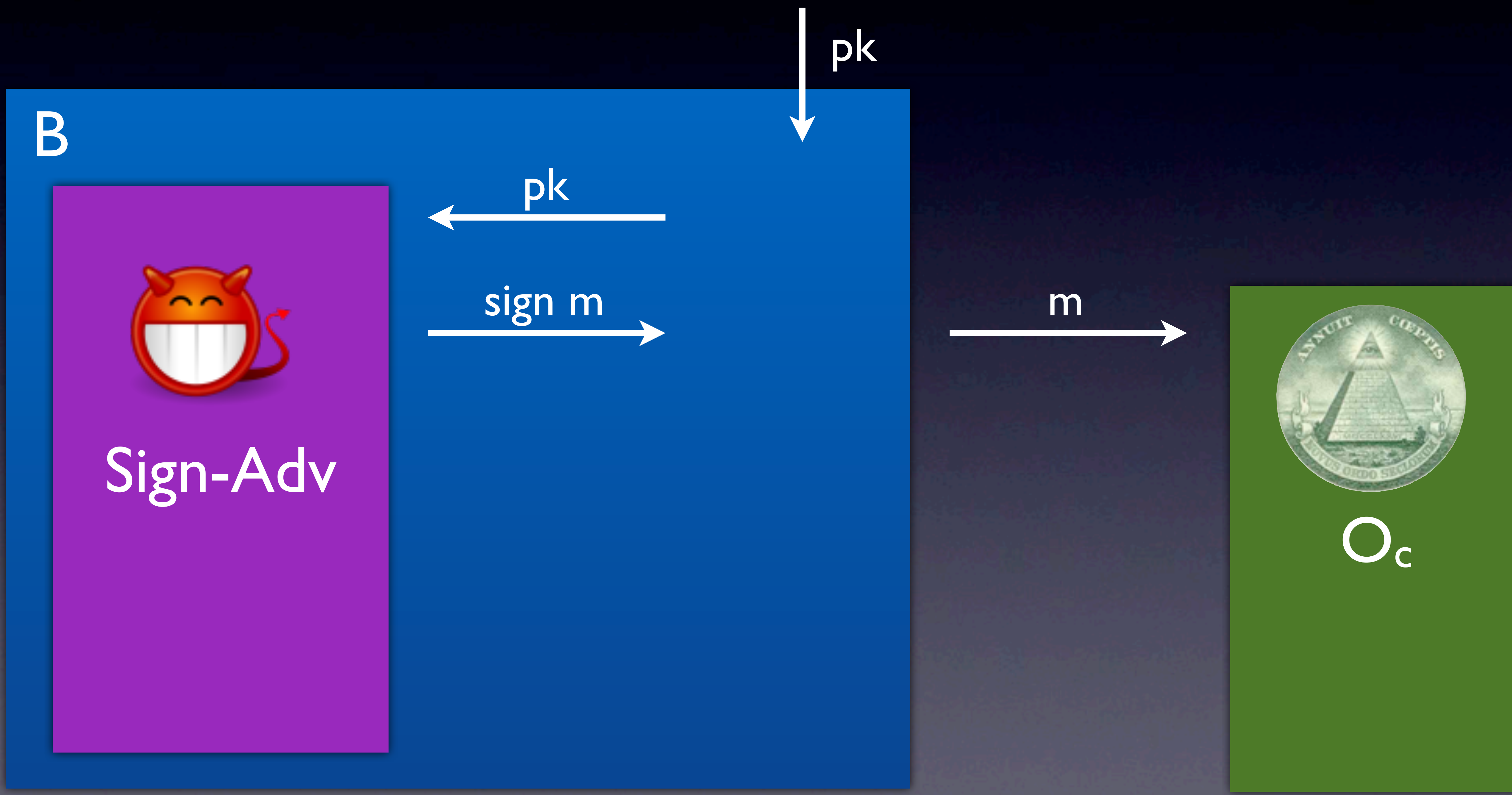
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



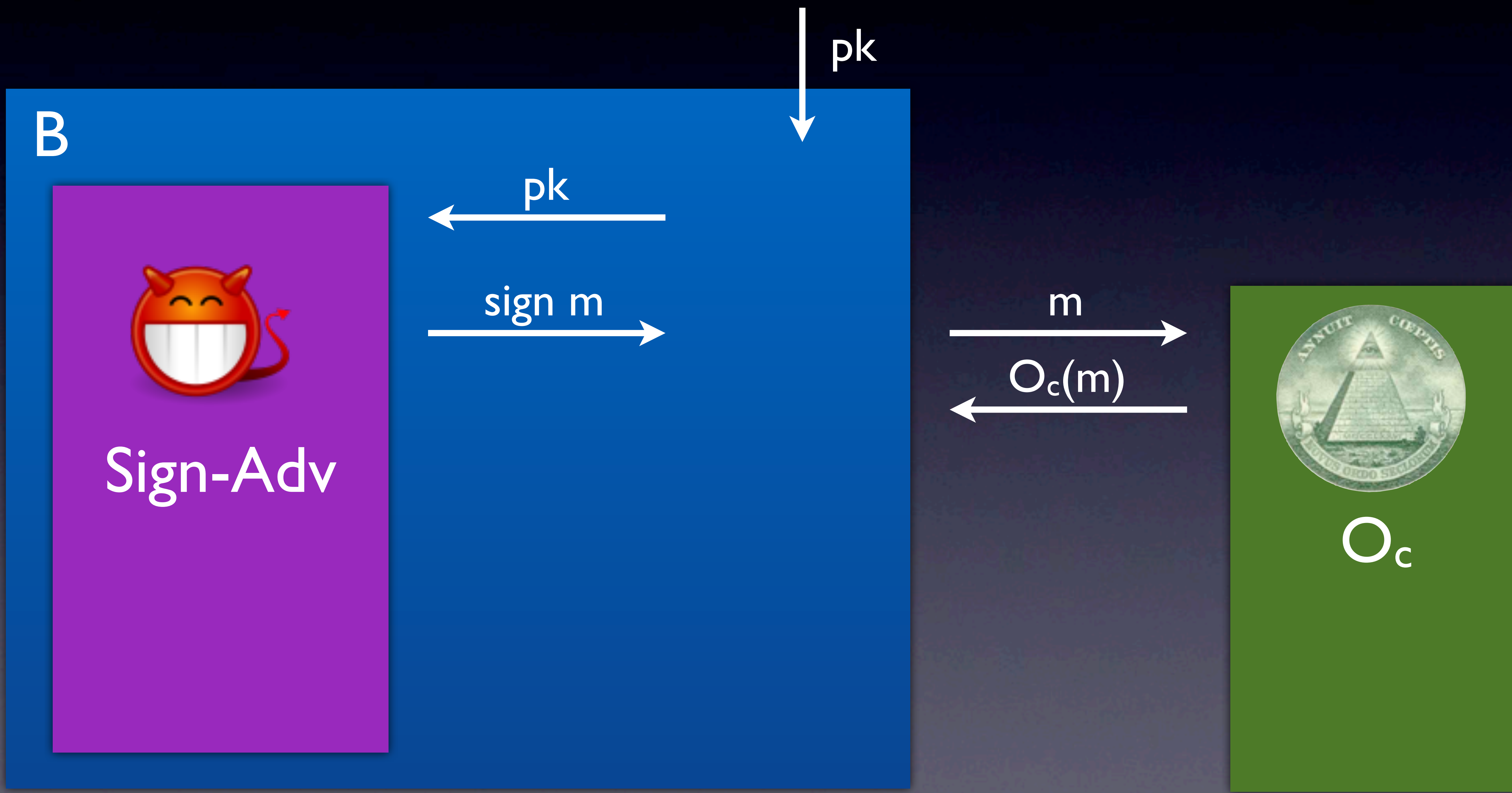
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



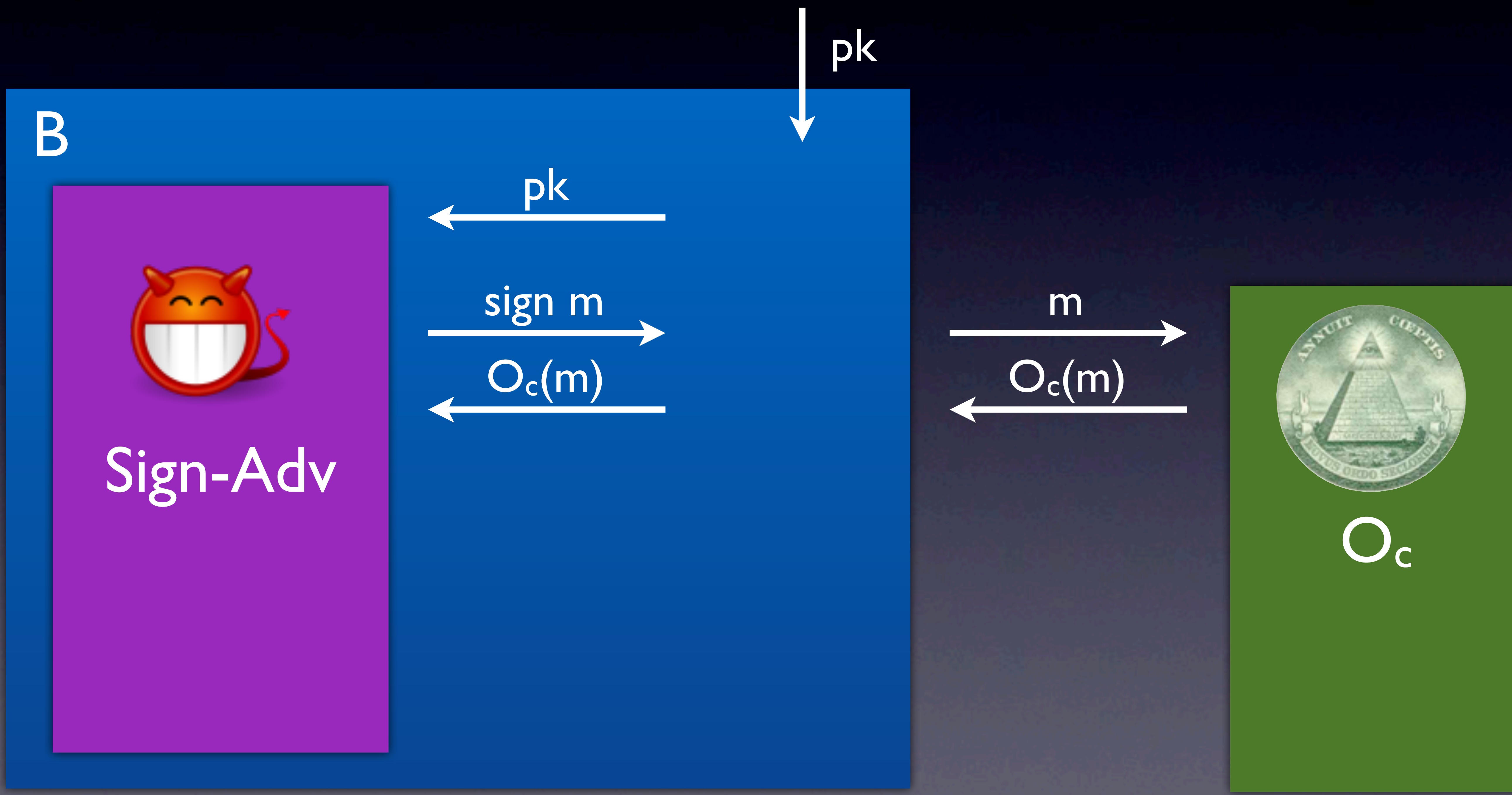
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



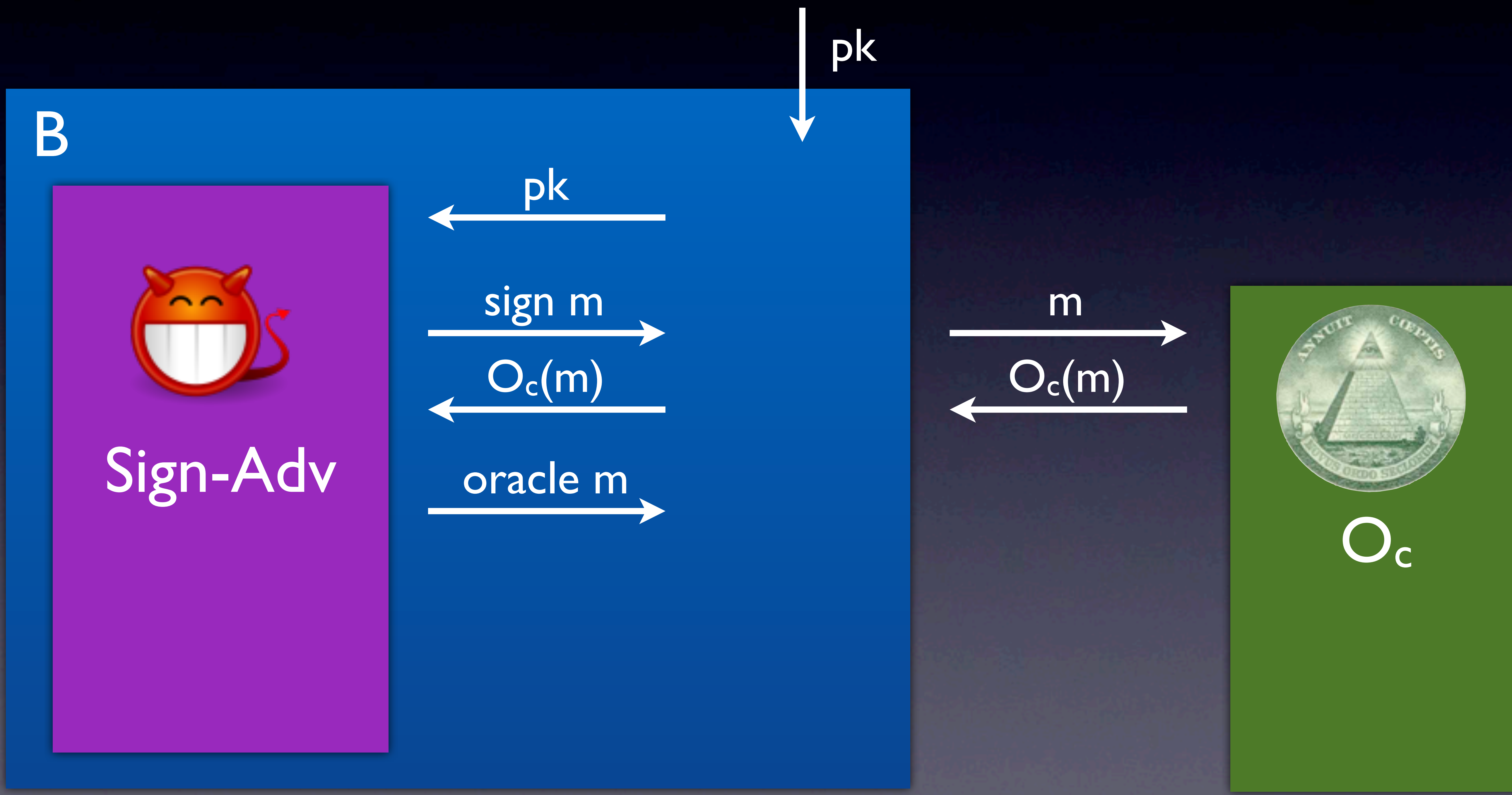
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



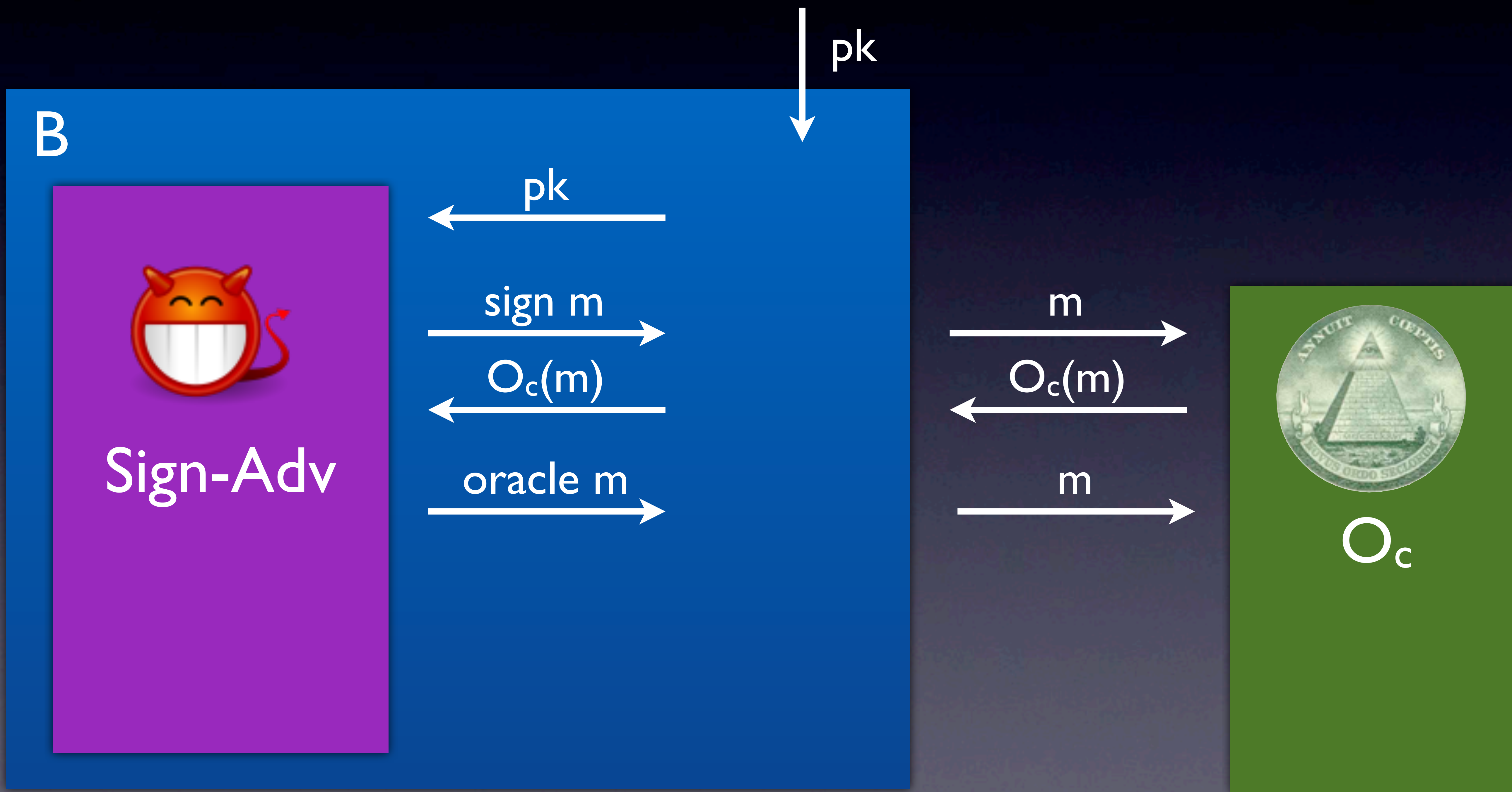
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



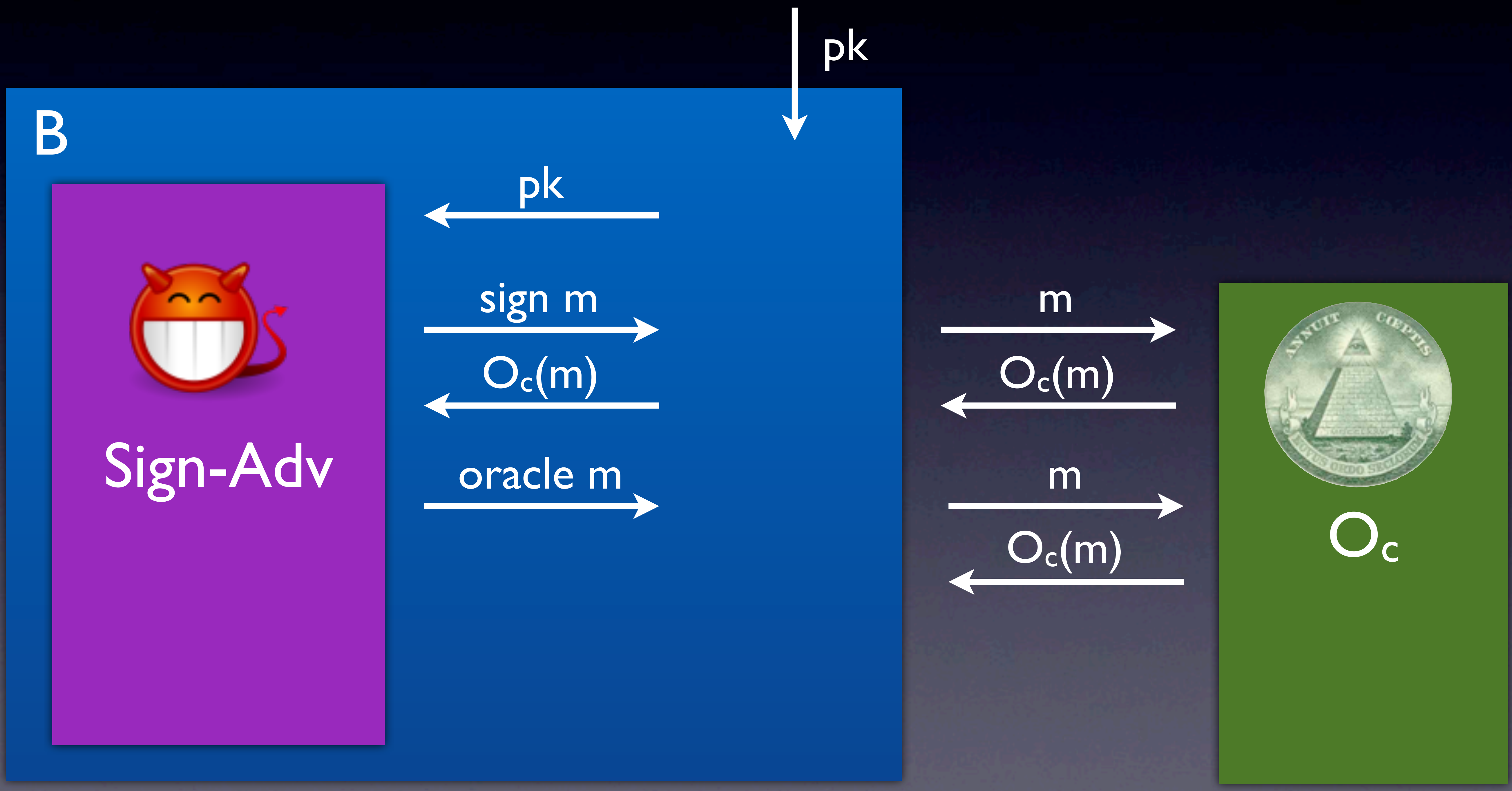
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



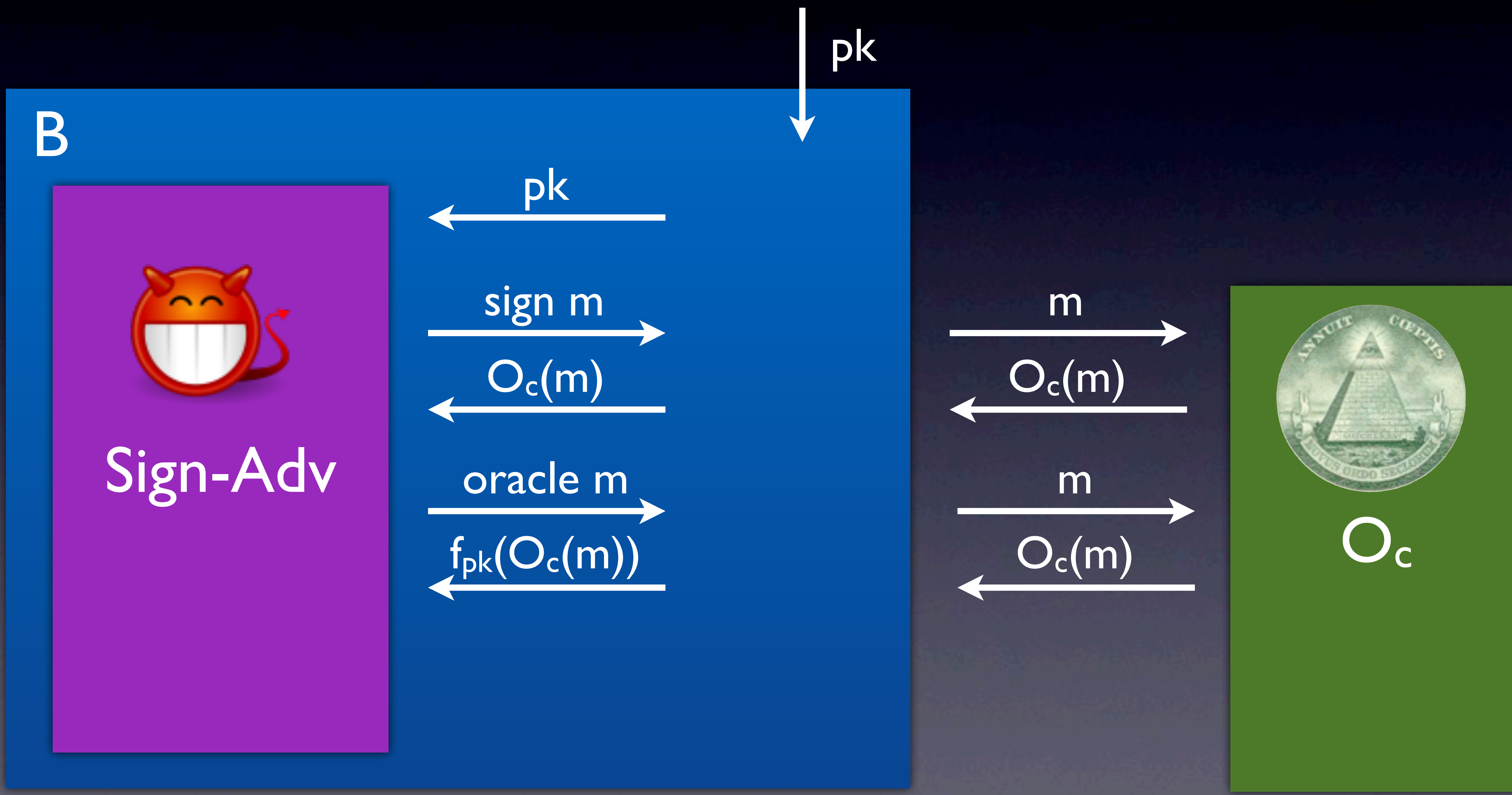
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



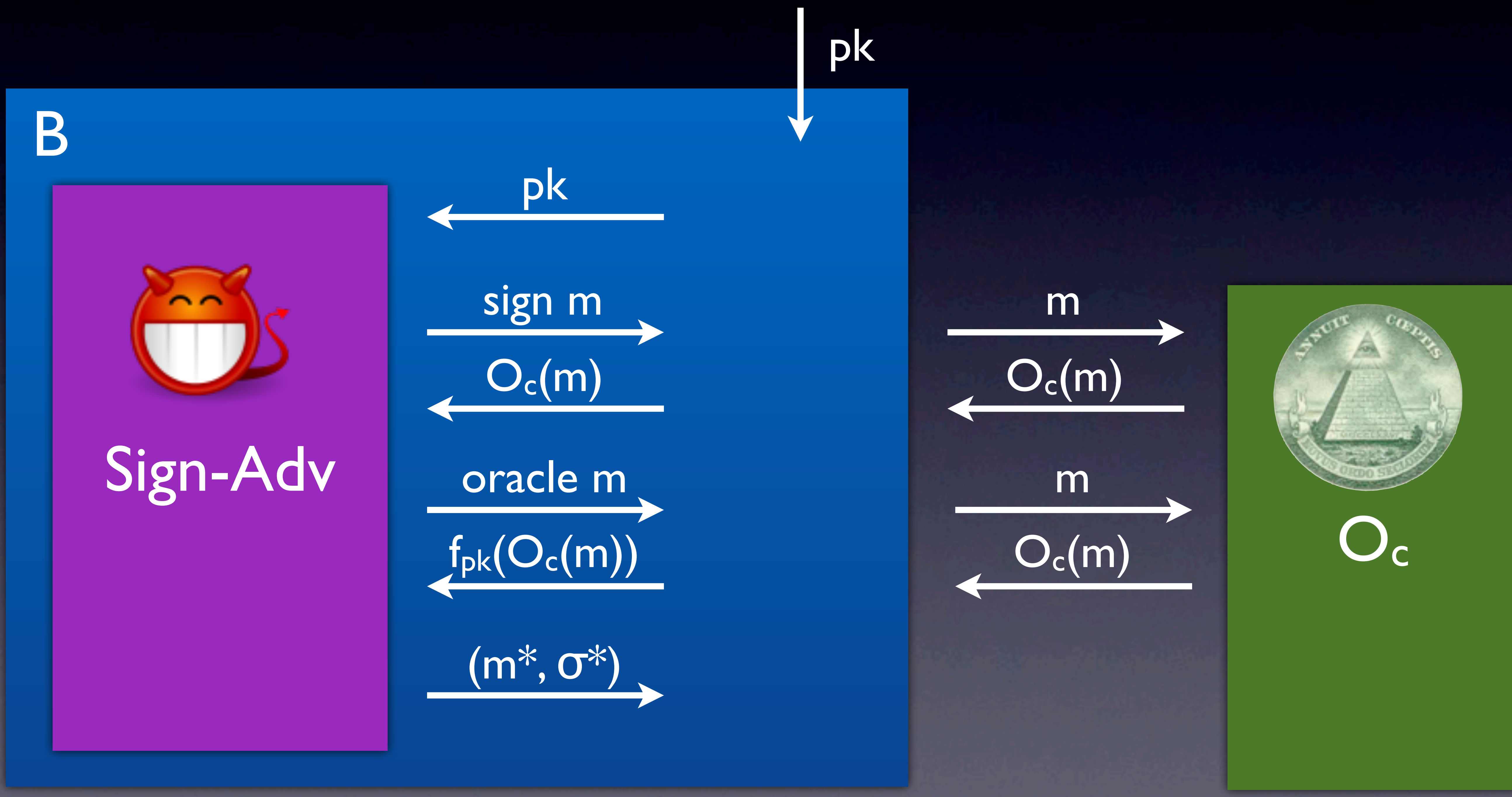
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



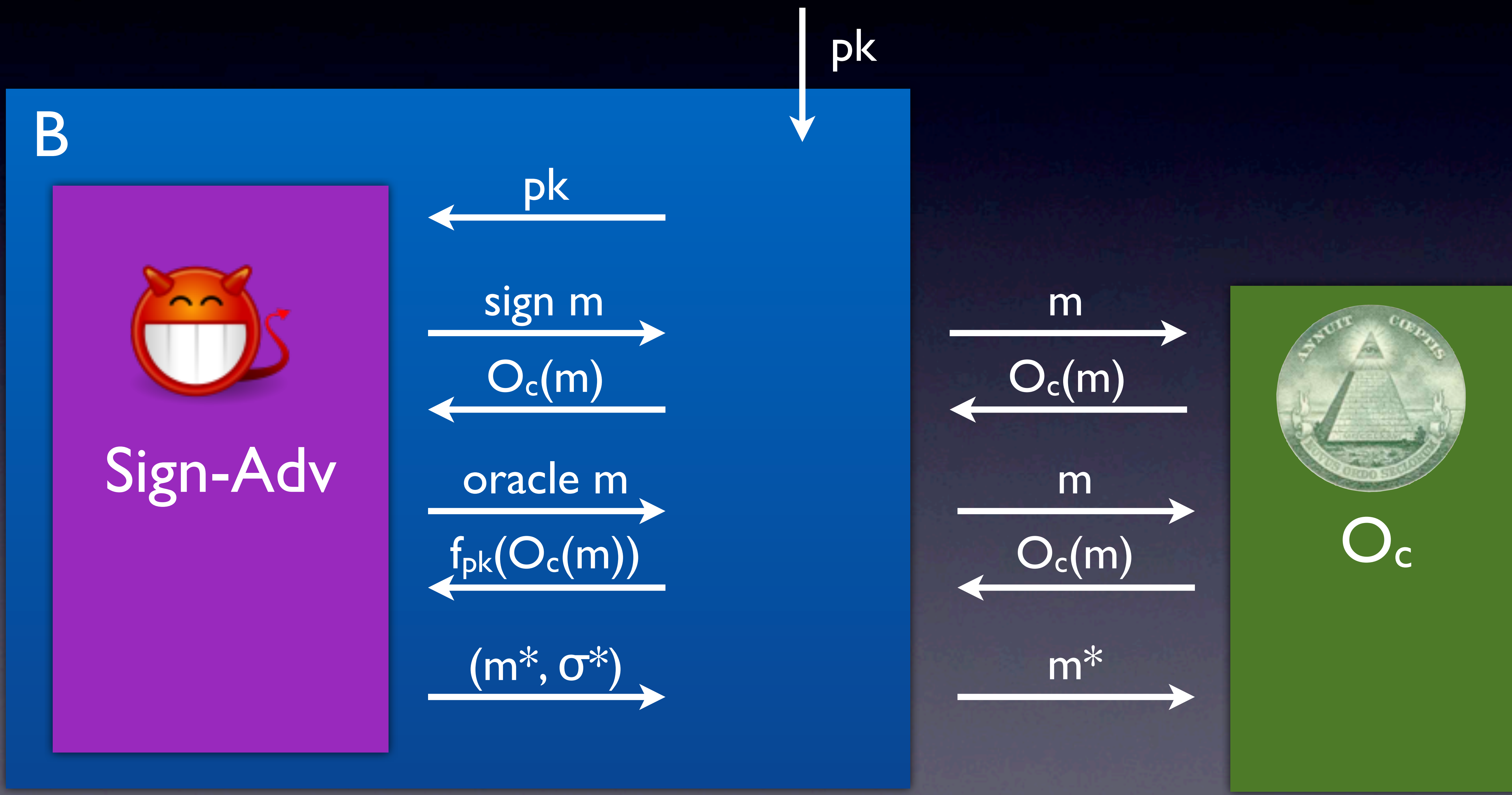
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



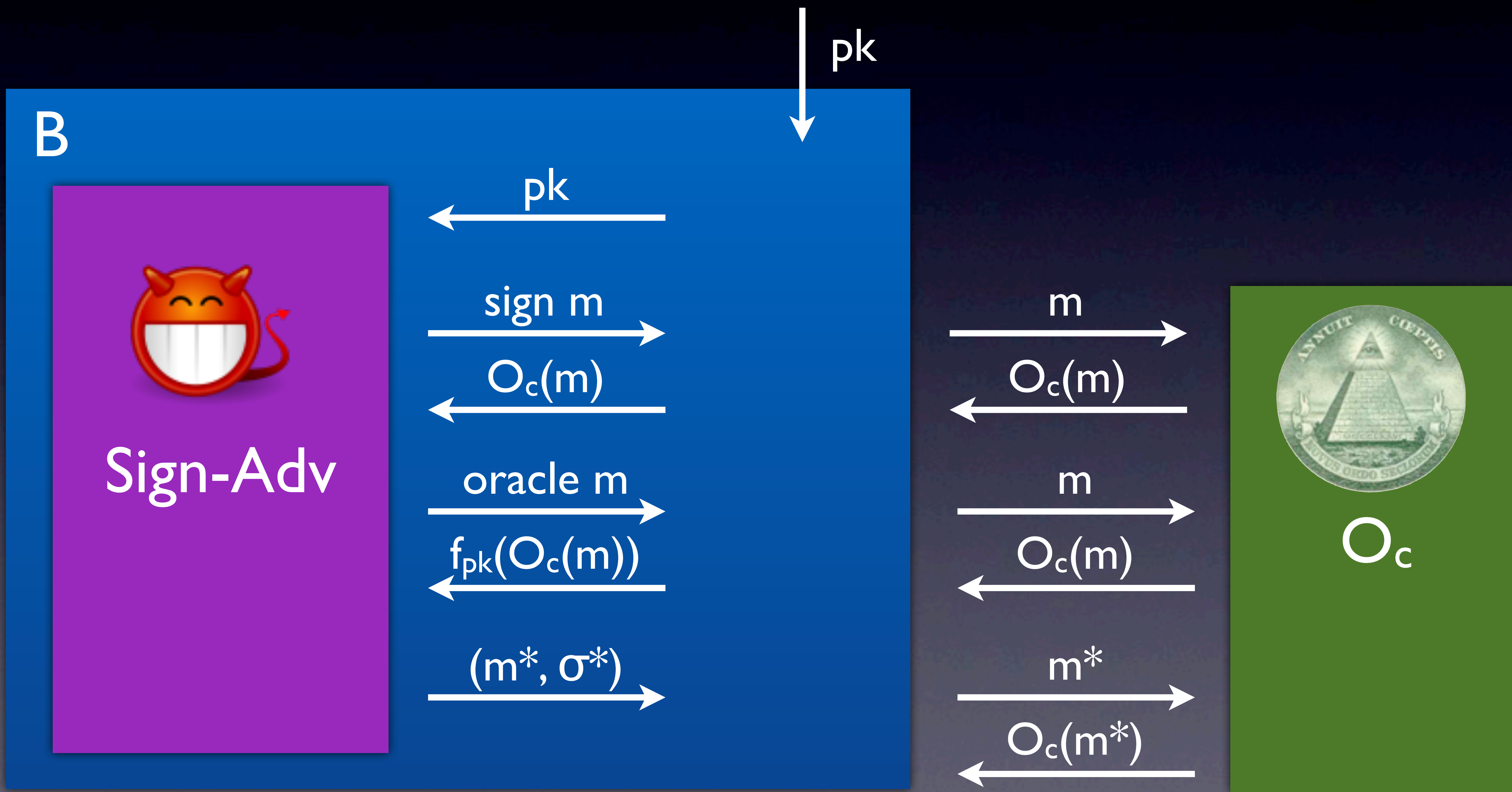
Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM



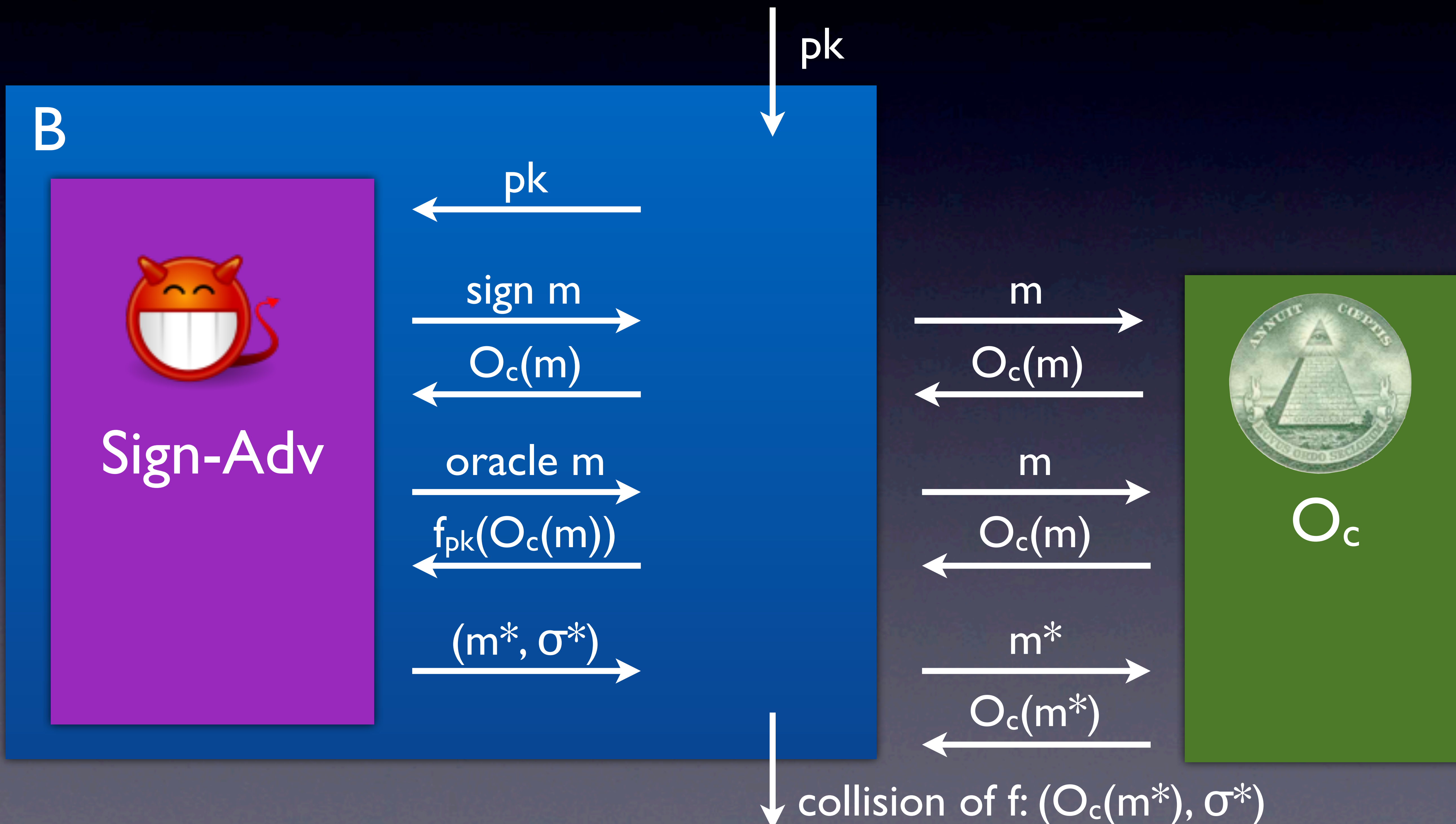
Modified GPV Reduction

Theorem: Suppose (G, f, f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM

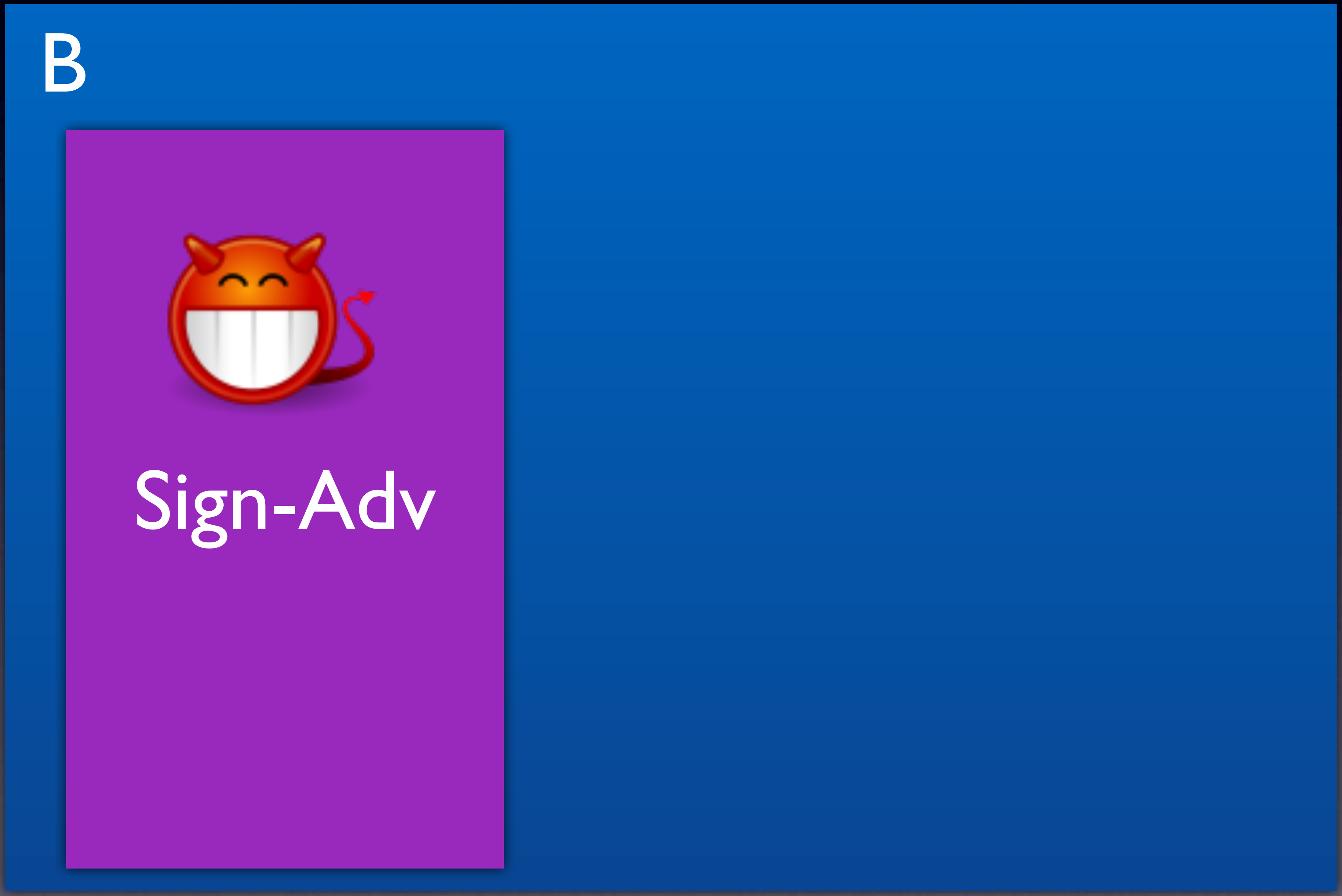


Modified GPV Reduction

Theorem: Suppose (G,f,f^{-1}) is a PSF, then $\mathrm{Sign}_{sk}(m) = f^{-1}_{sk}(H(m))$ is secure in the CROM

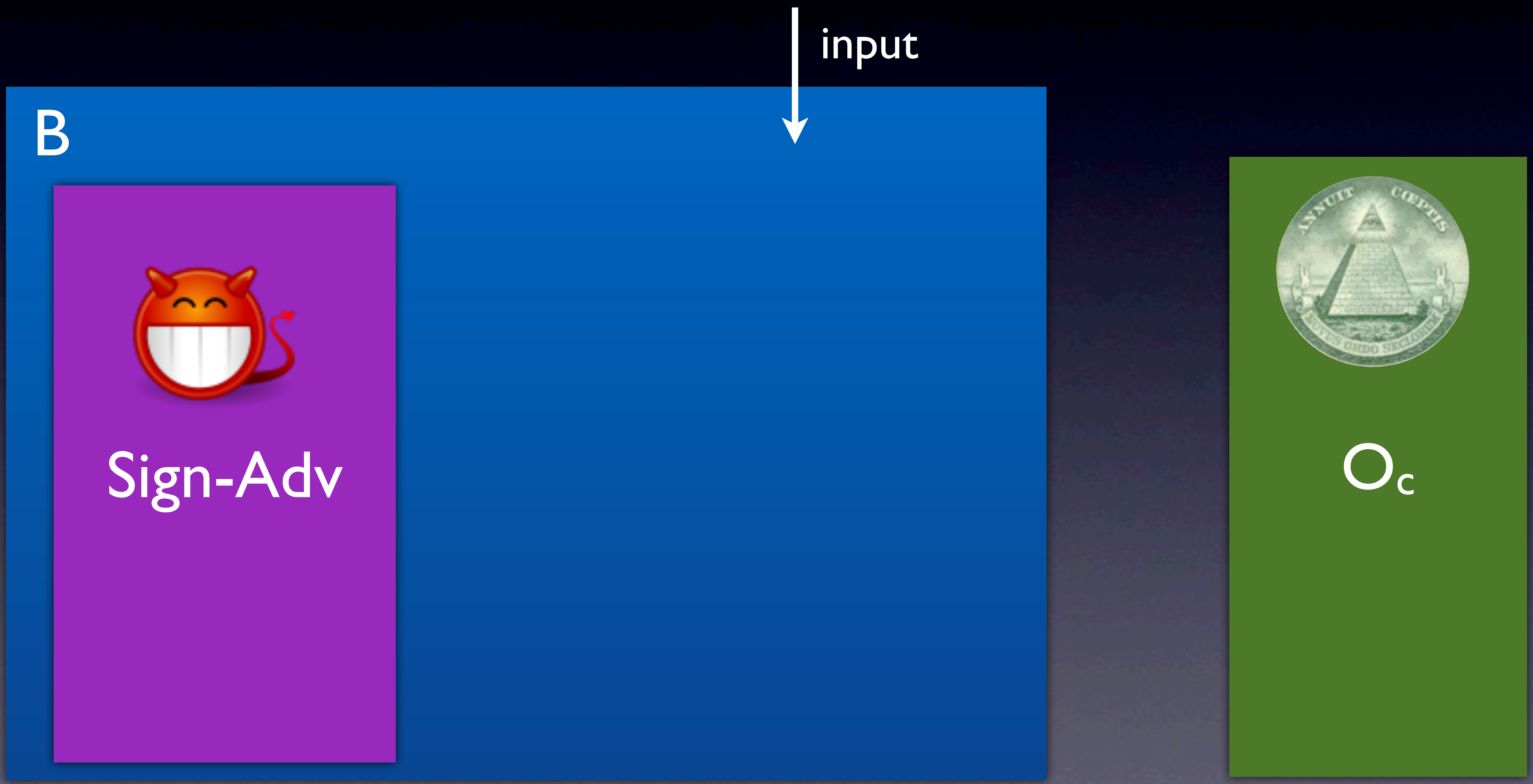


History-Free (Classical) Reduction

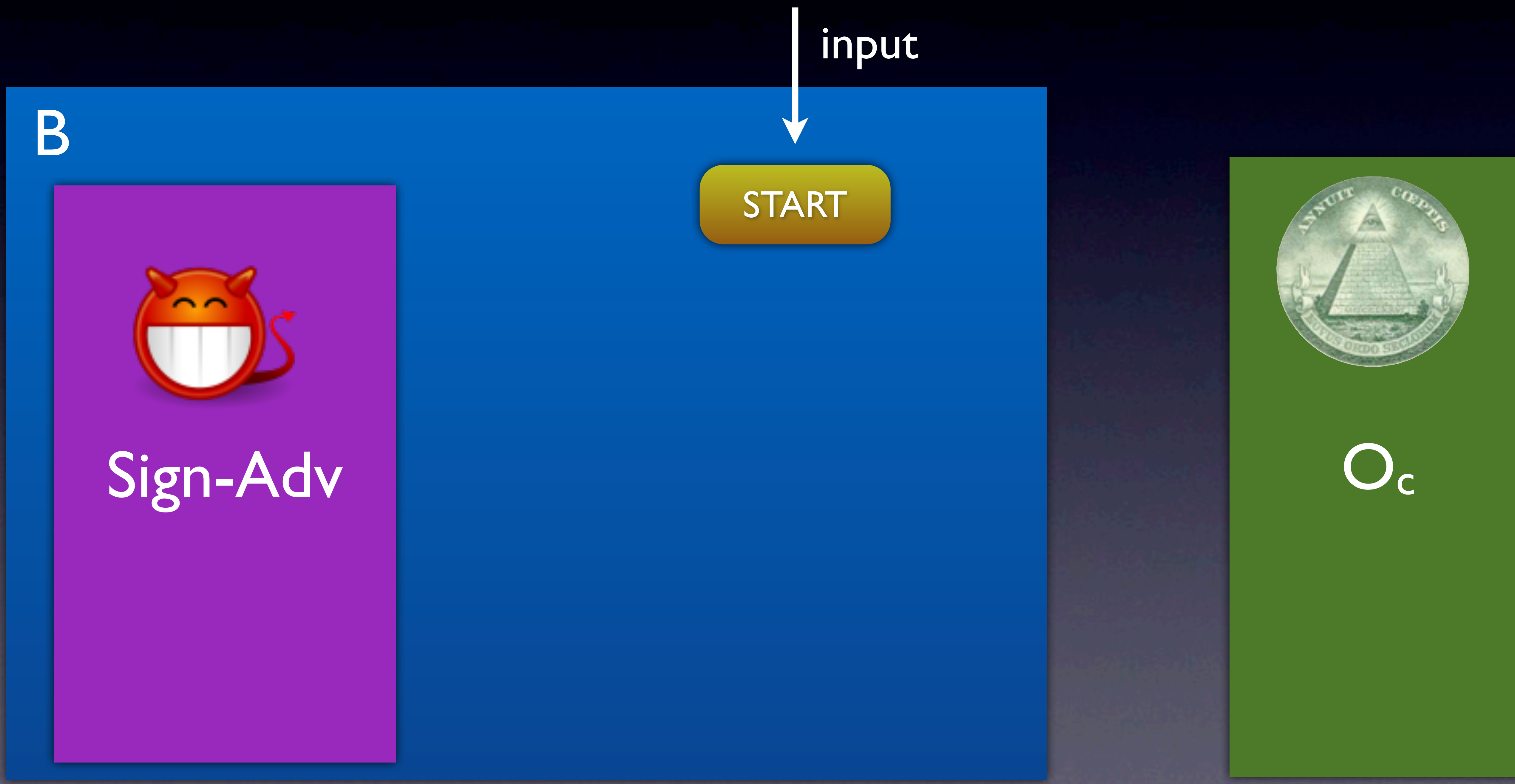


History-Free (Classical) Reduction

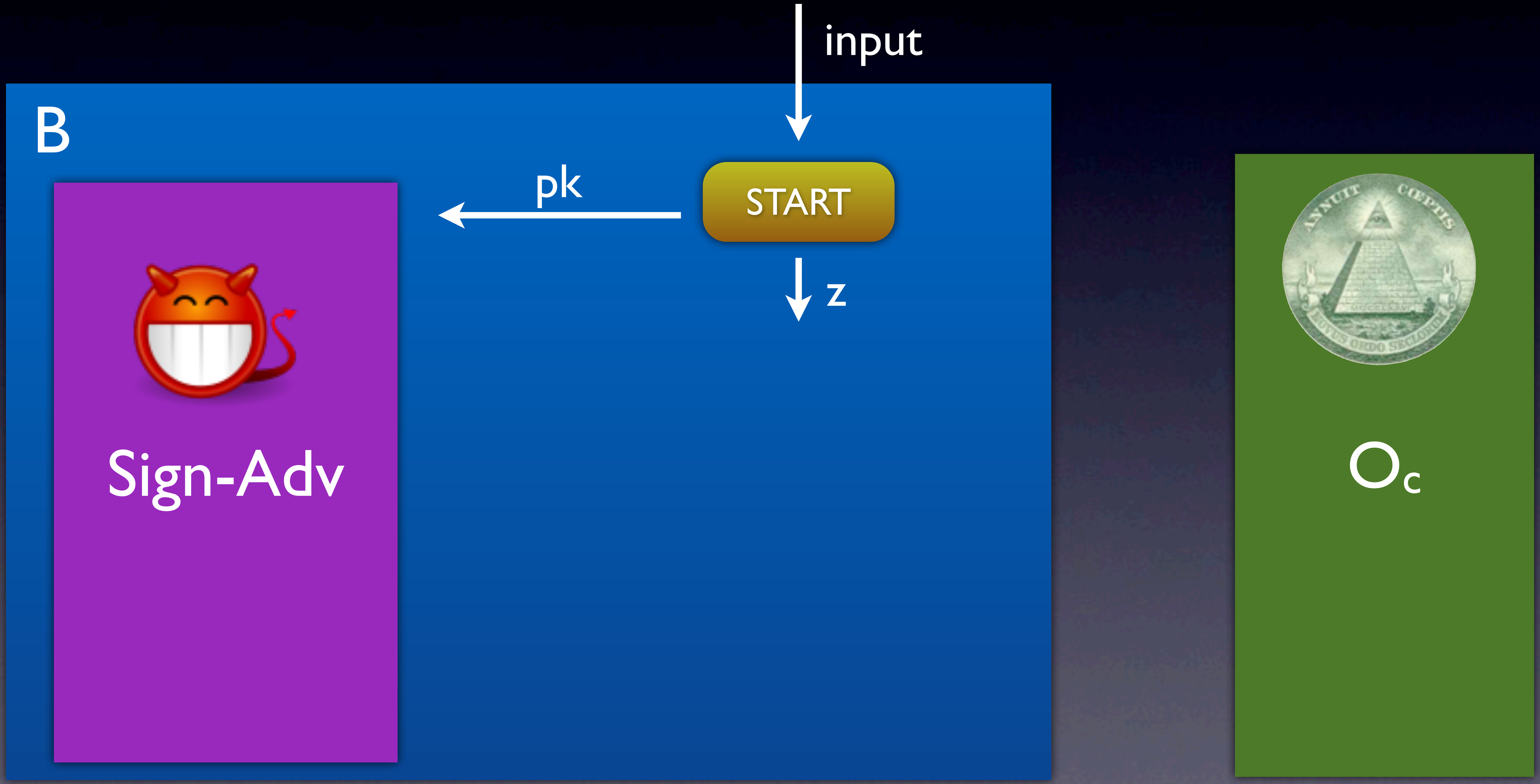
History-Free (Classical) Reduction



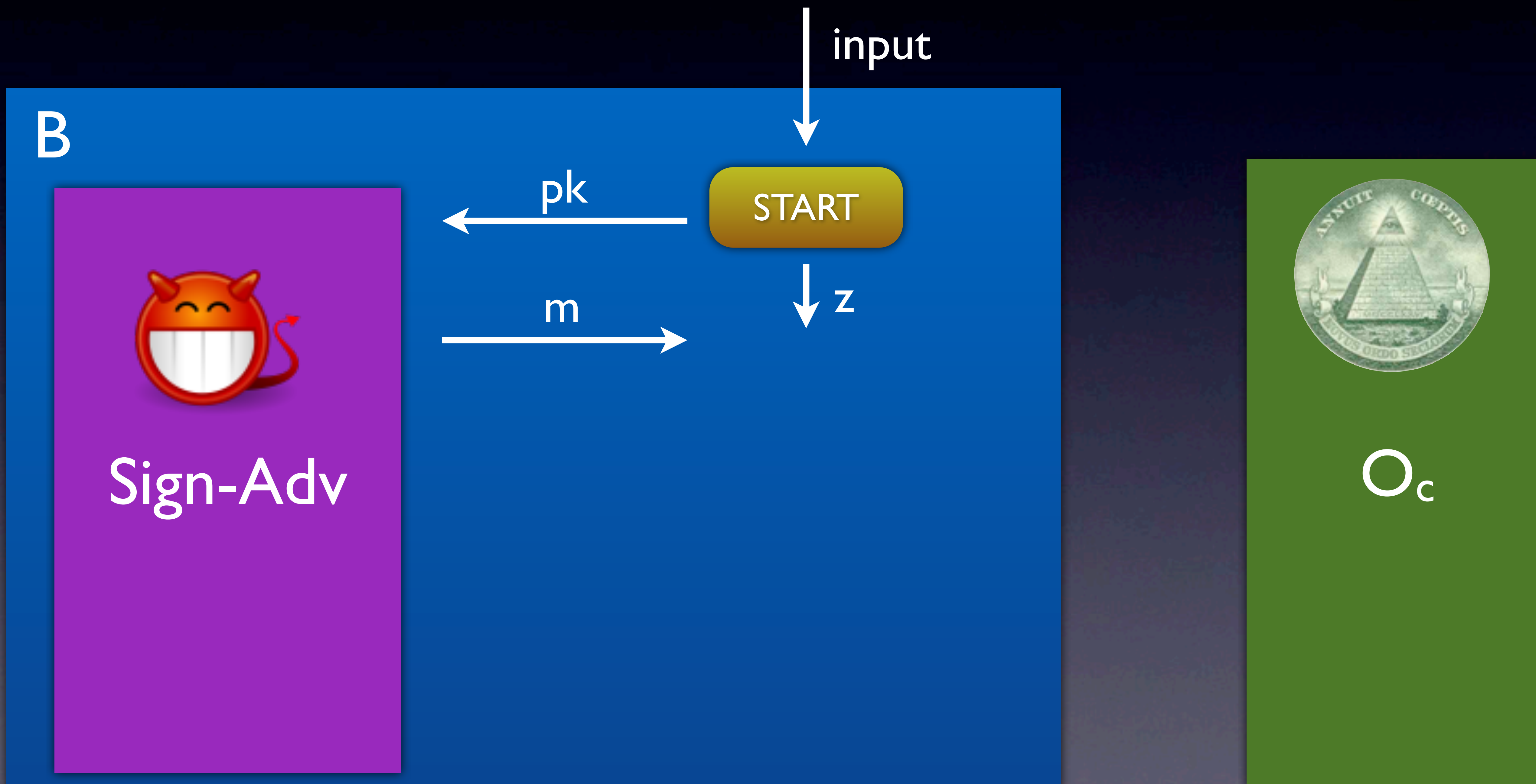
History-Free (Classical) Reduction



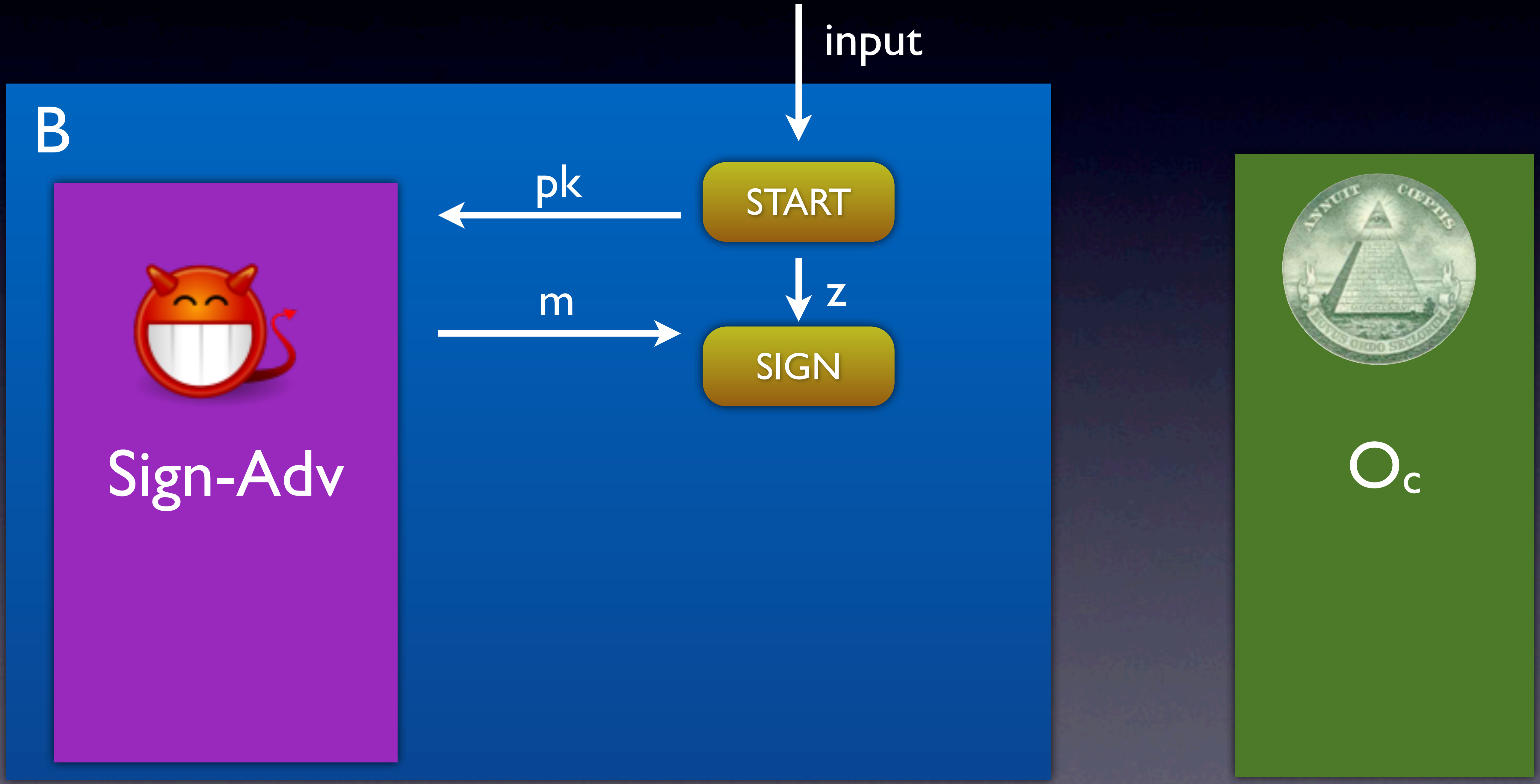
History-Free (Classical) Reduction



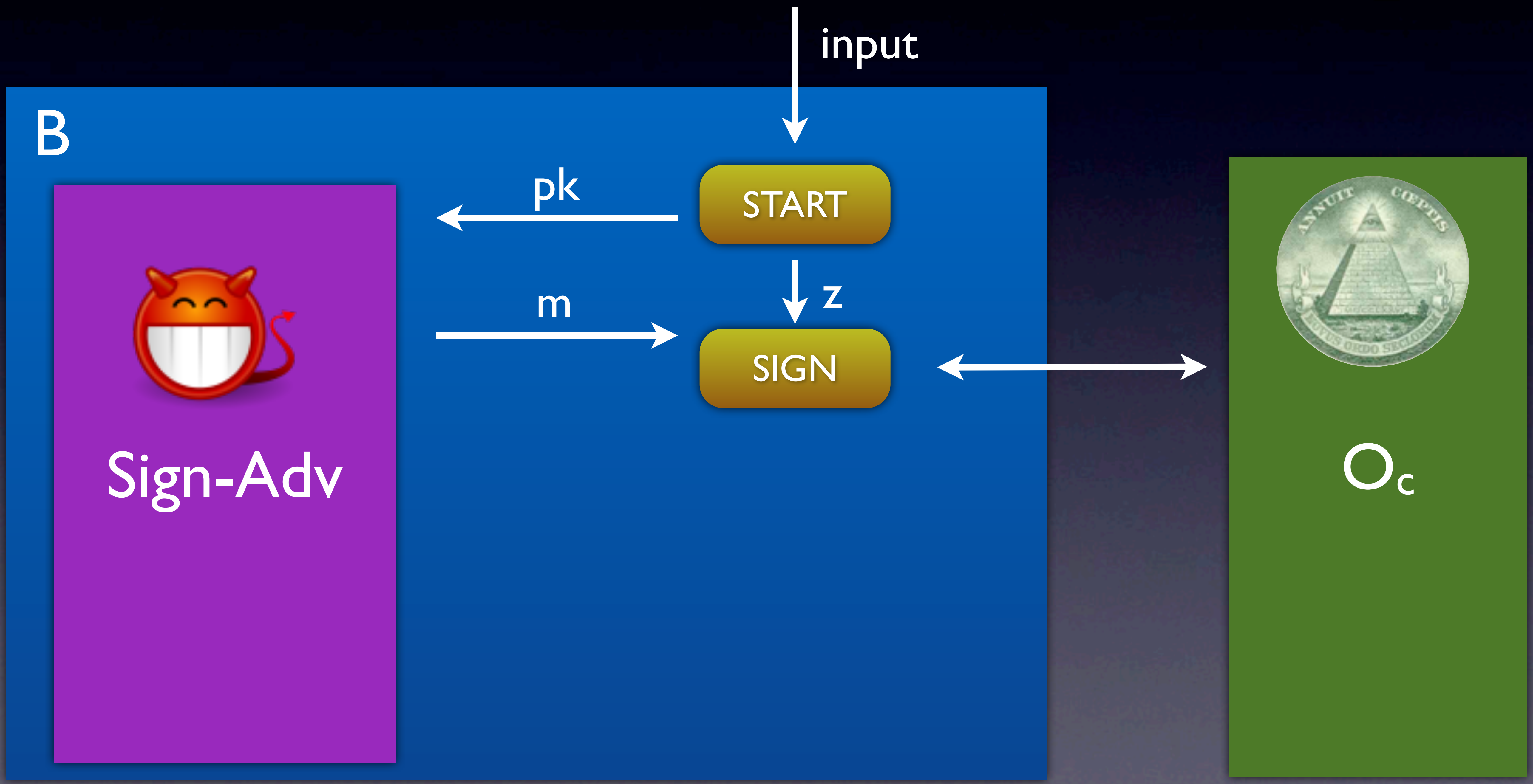
History-Free
(Classical) Reduction



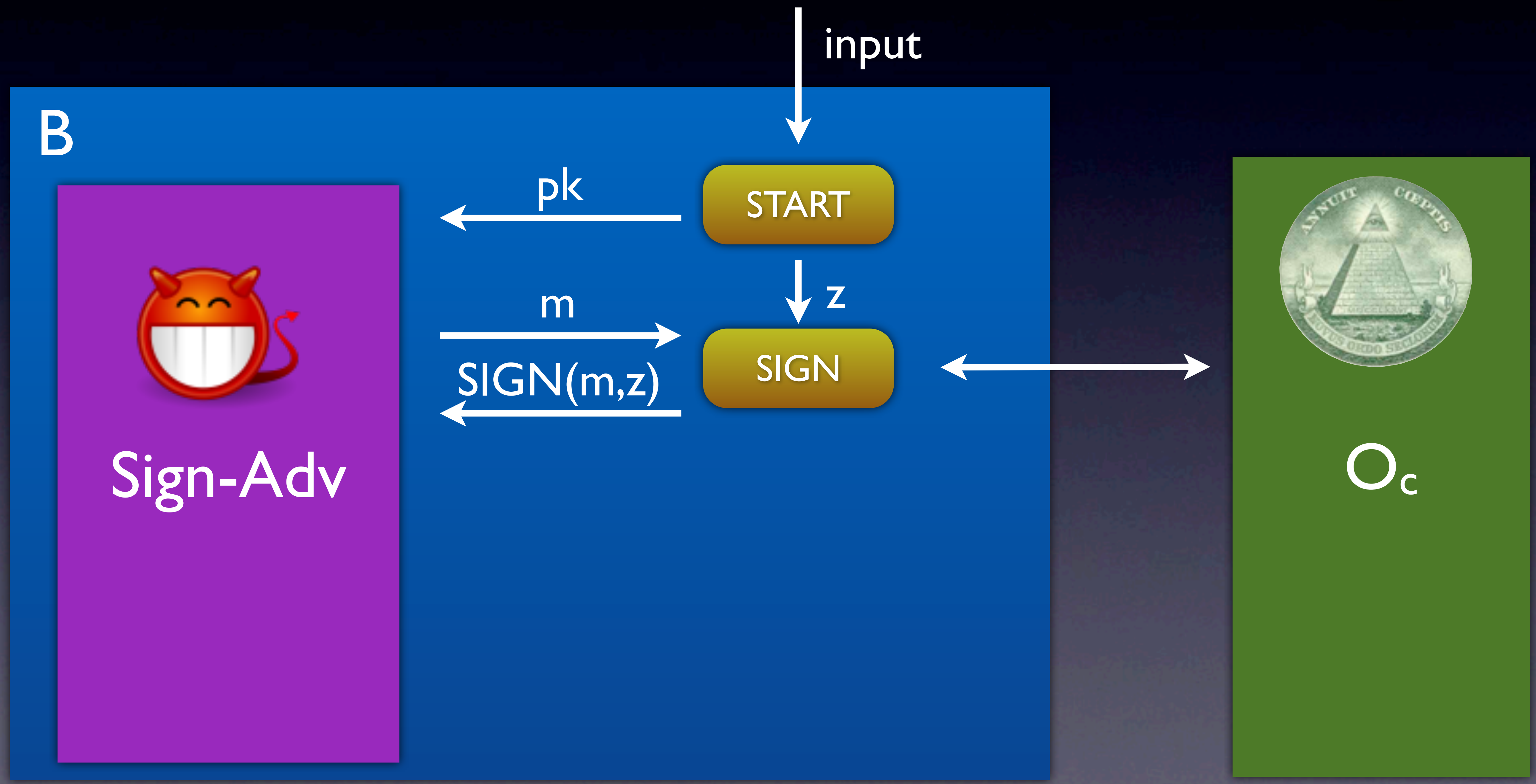
History-Free (Classical) Reduction



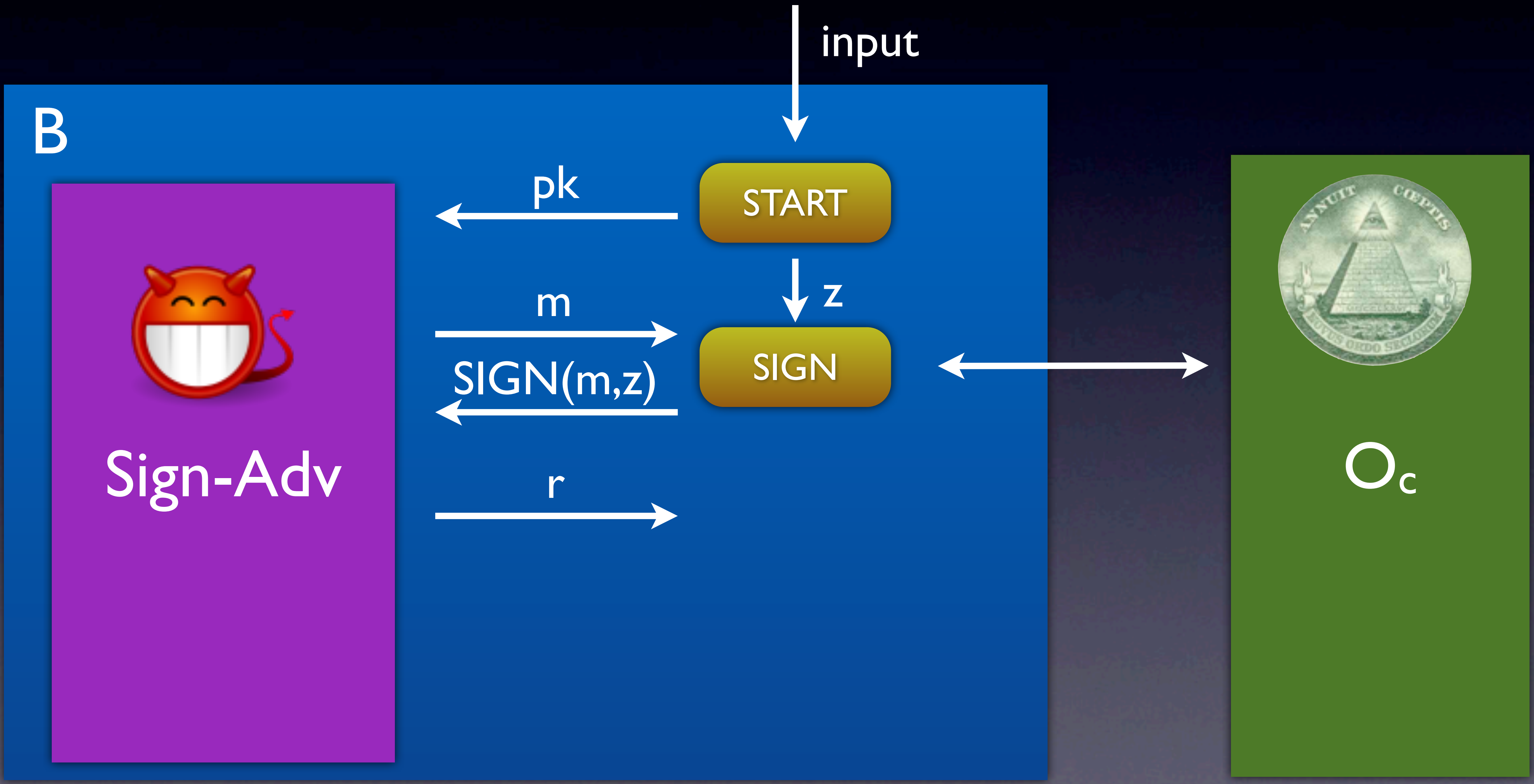
History-Free (Classical) Reduction



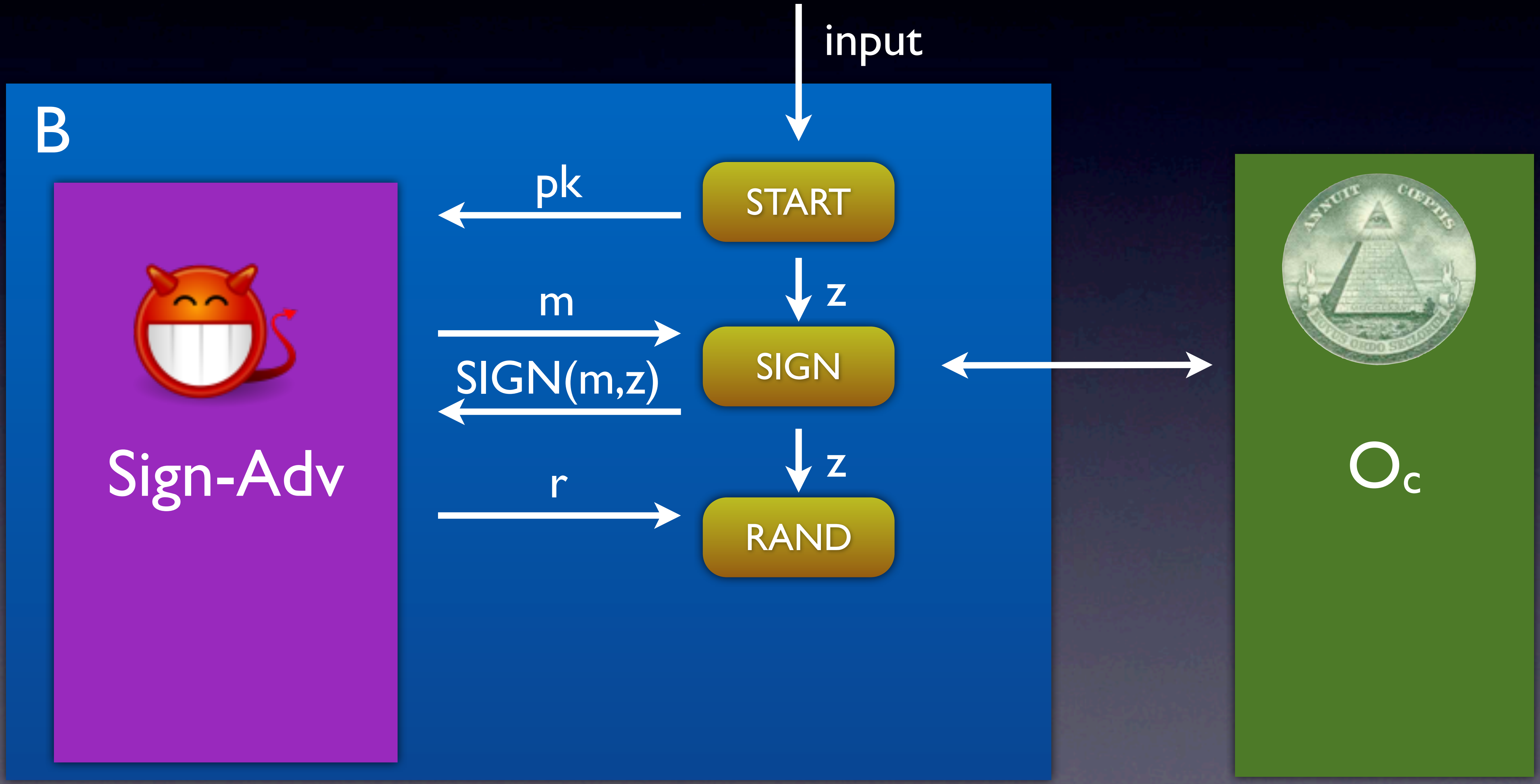
History-Free (Classical) Reduction



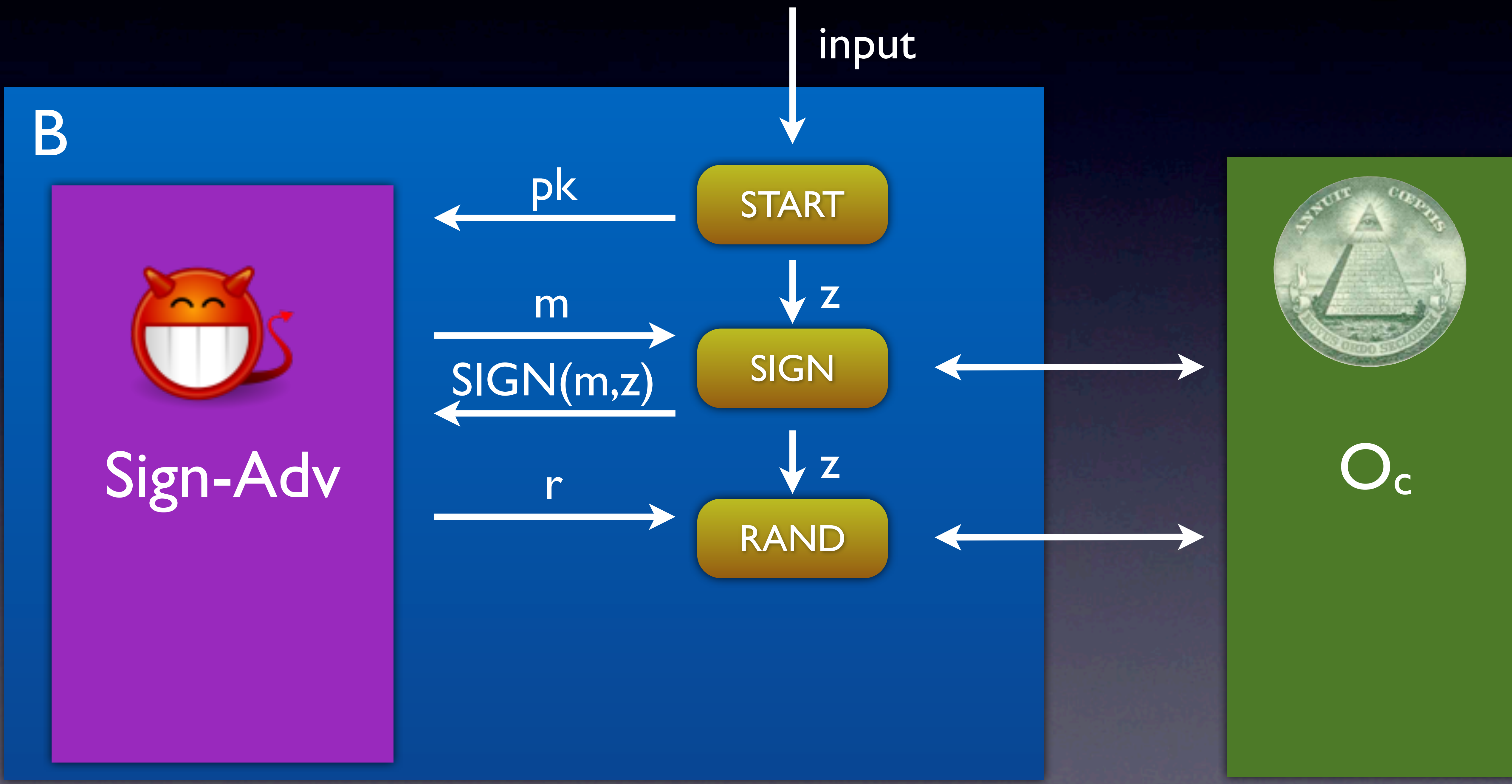
History-Free (Classical) Reduction



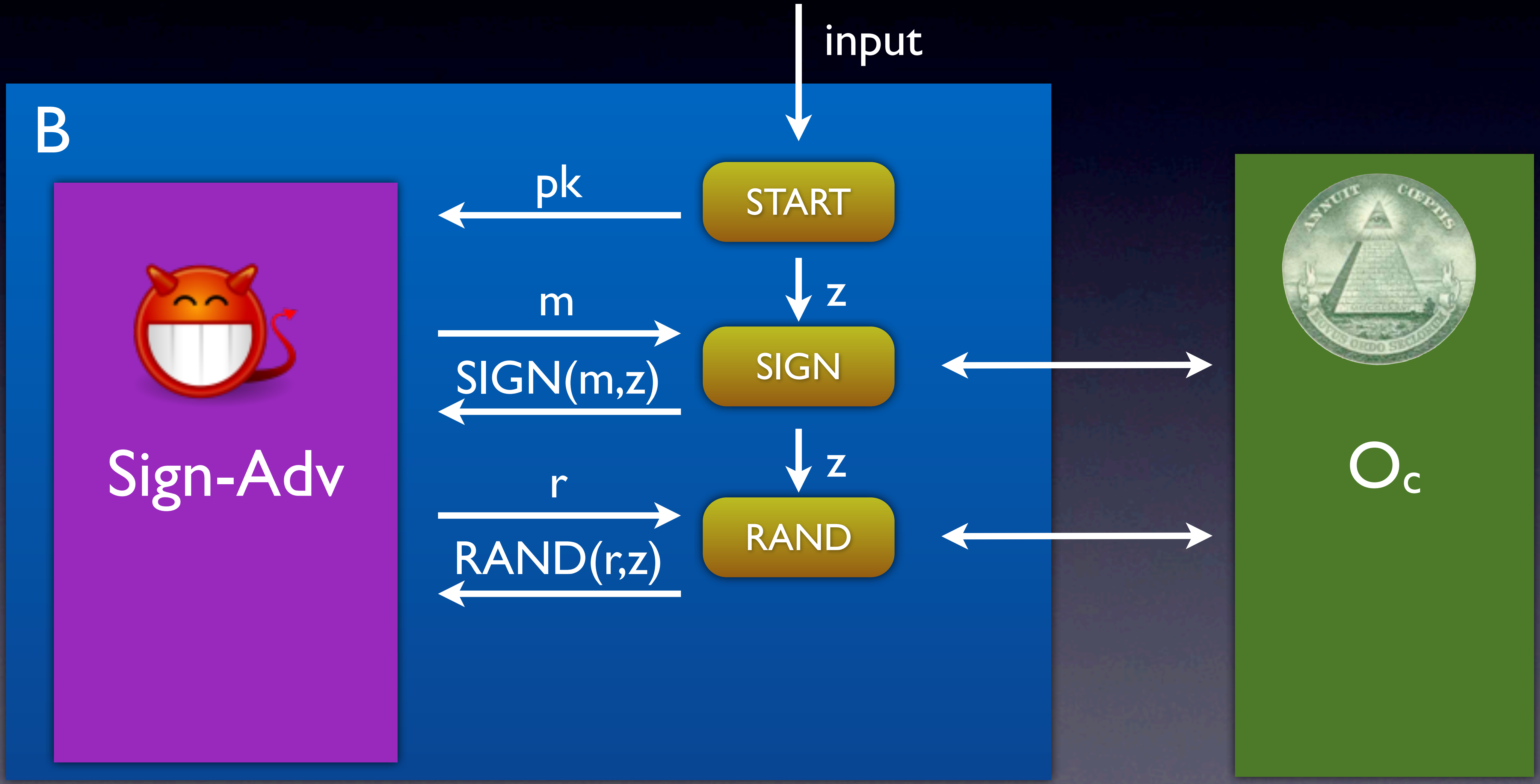
History-Free (Classical) Reduction



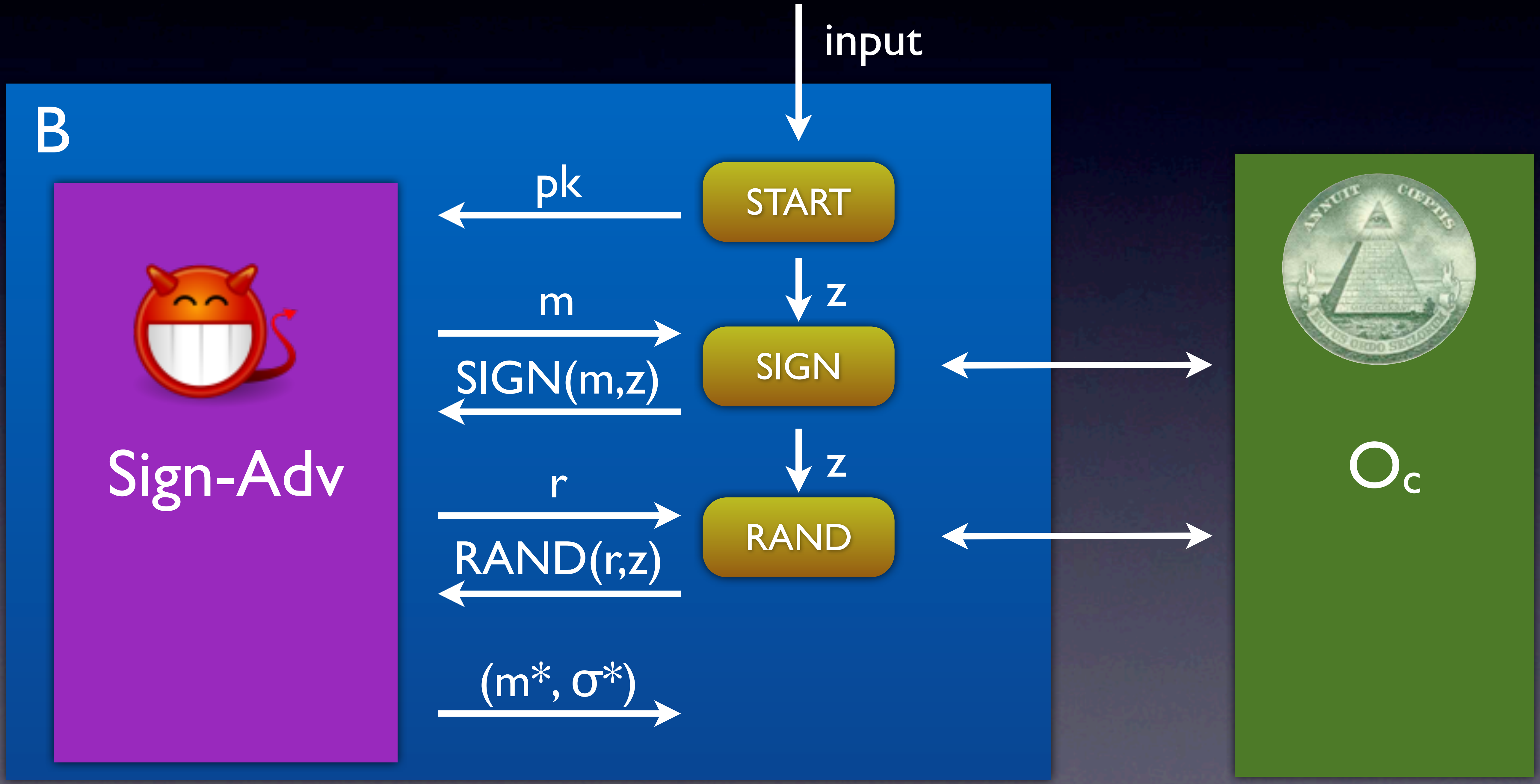
History-Free (Classical) Reduction



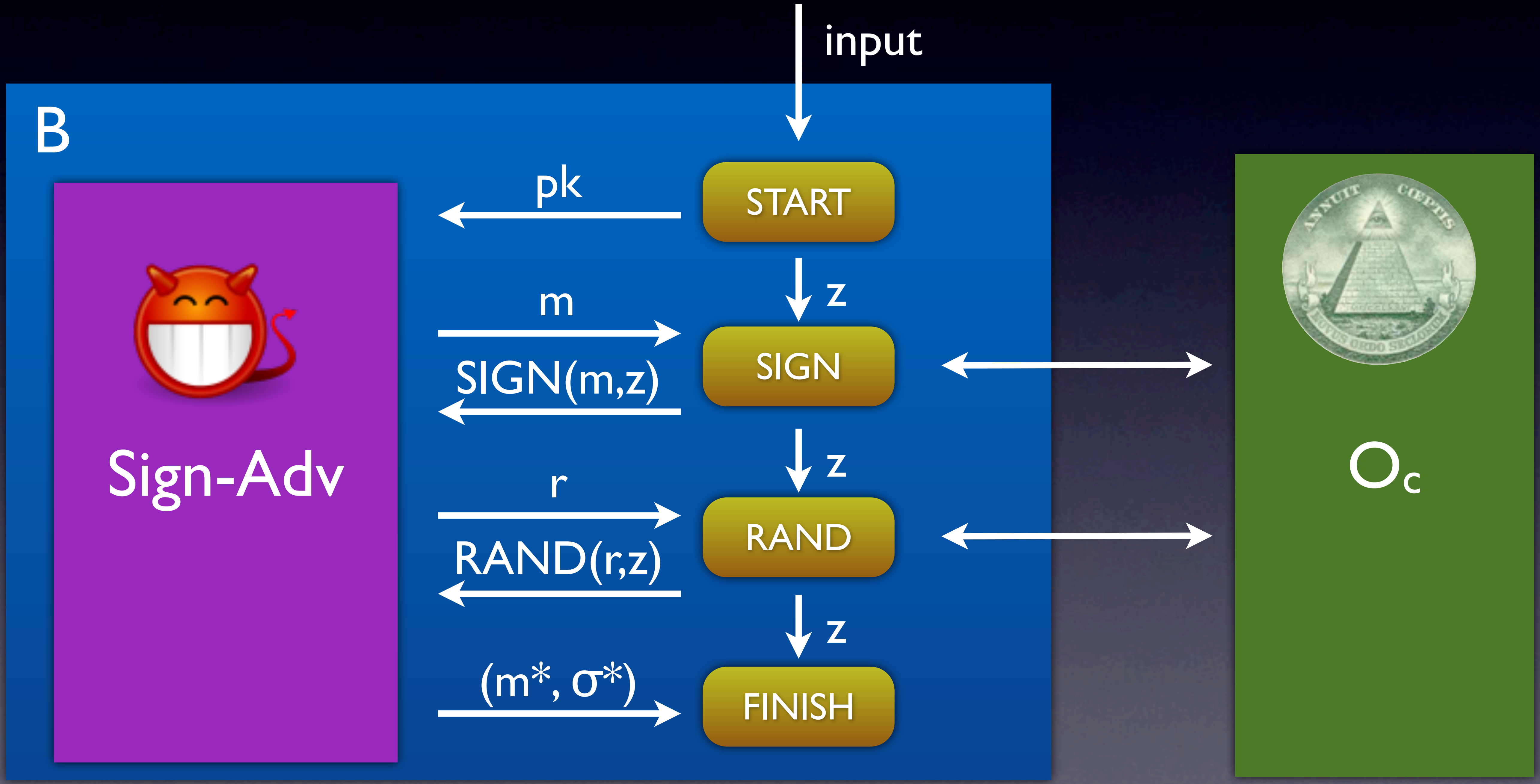
History-Free (Classical) Reduction



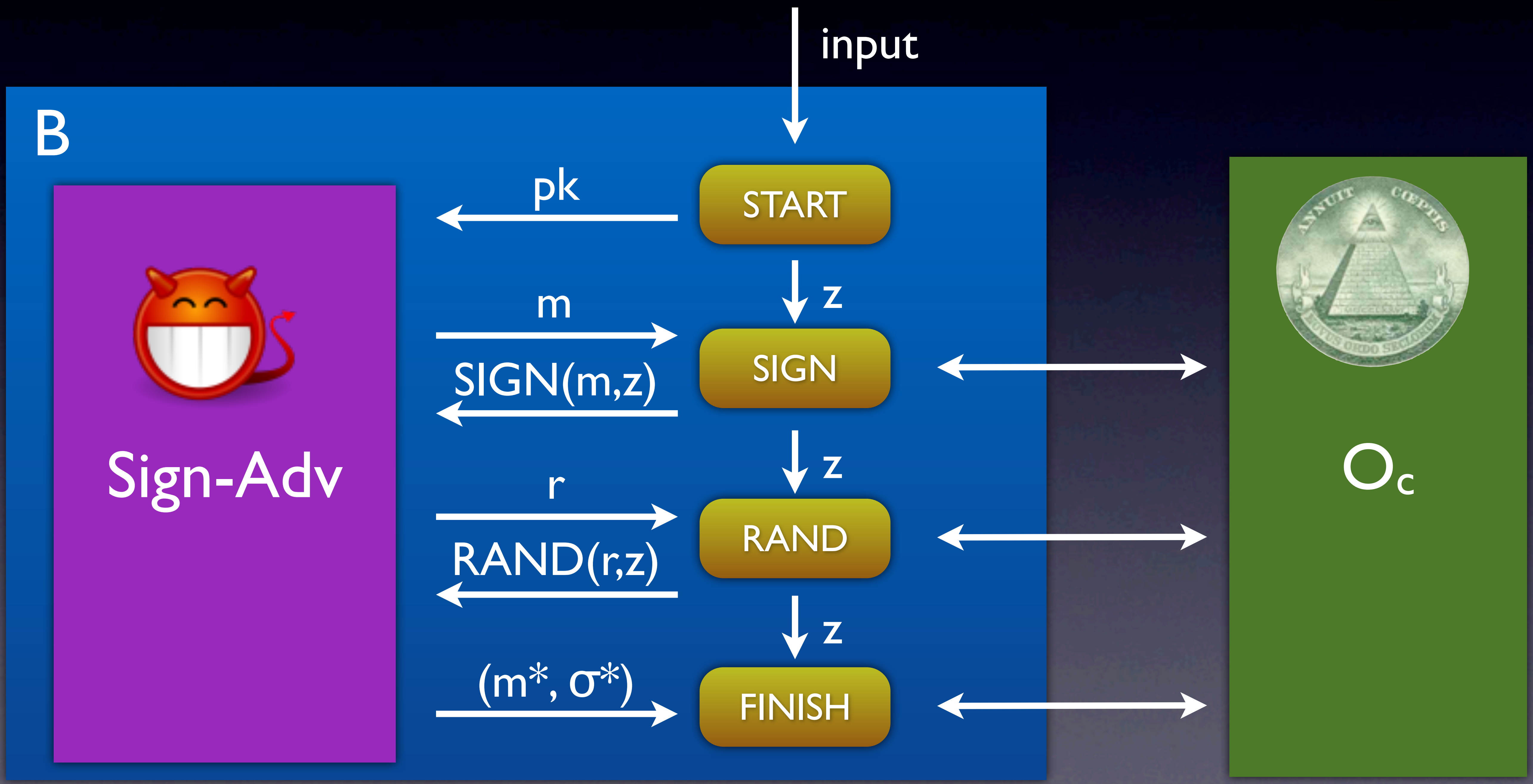
History-Free (Classical) Reduction



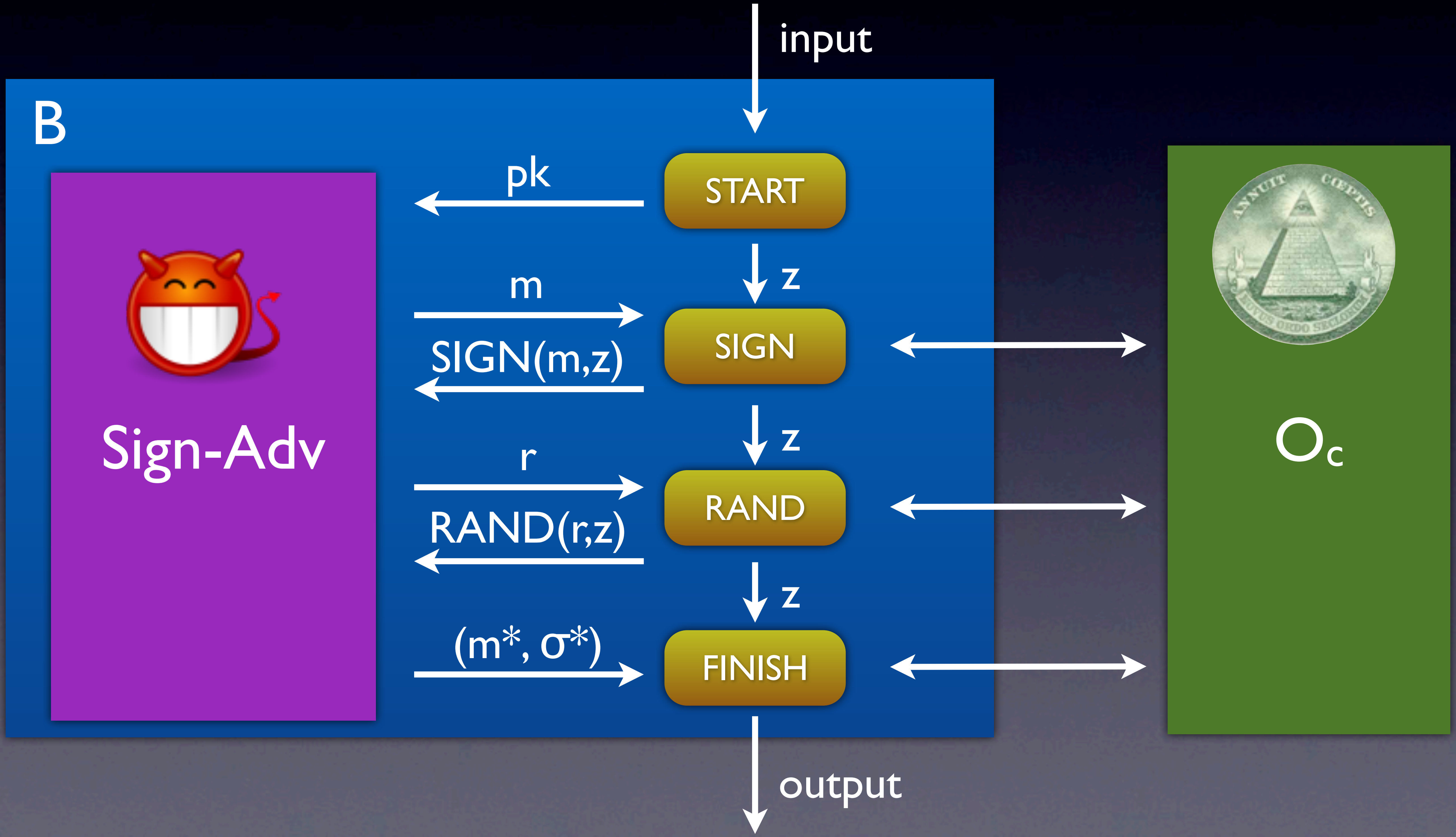
History-Free (Classical) Reduction



History-Free (Classical) Reduction

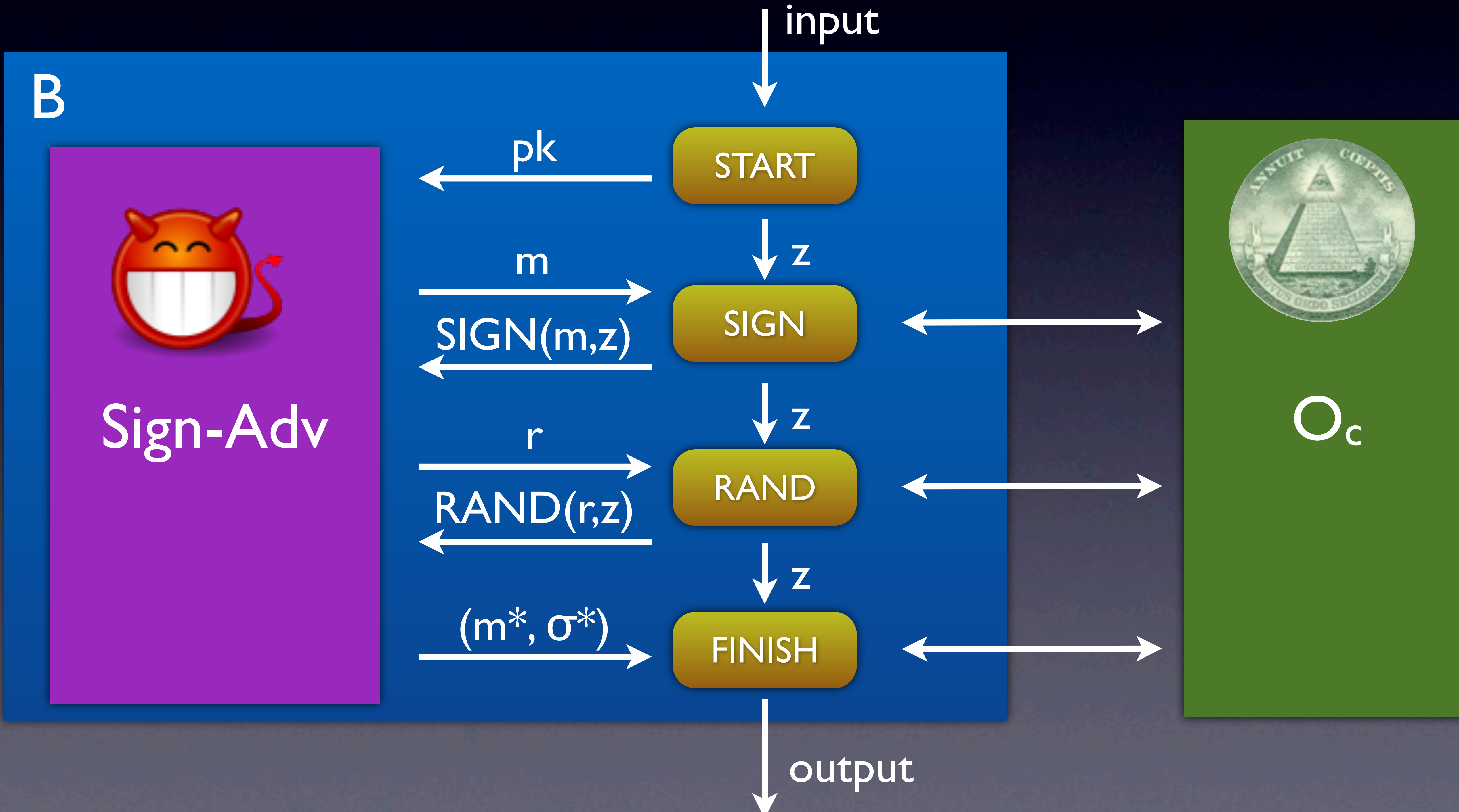


History-Free (Classical) Reduction



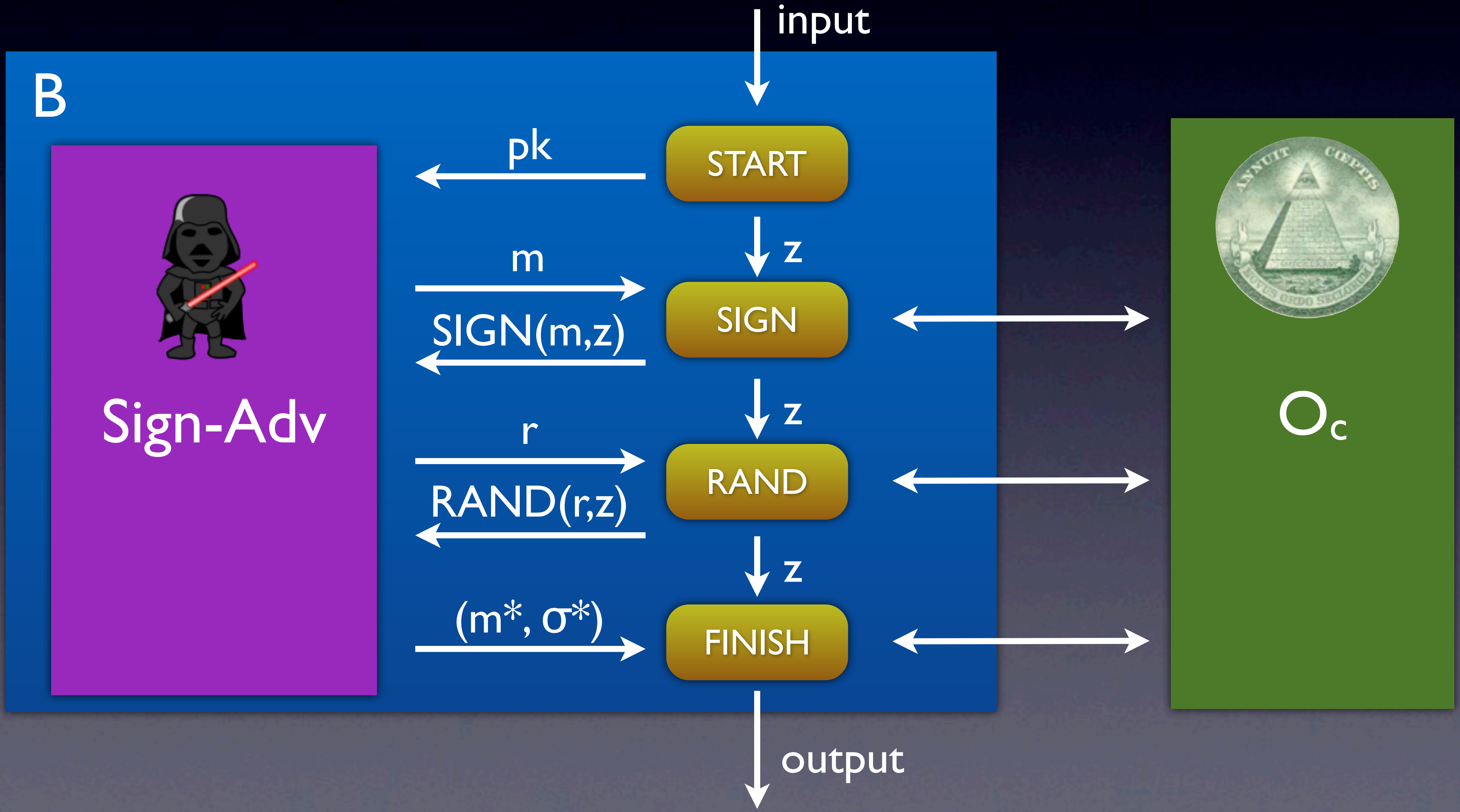
History-Free Security

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



History-Free Security

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.

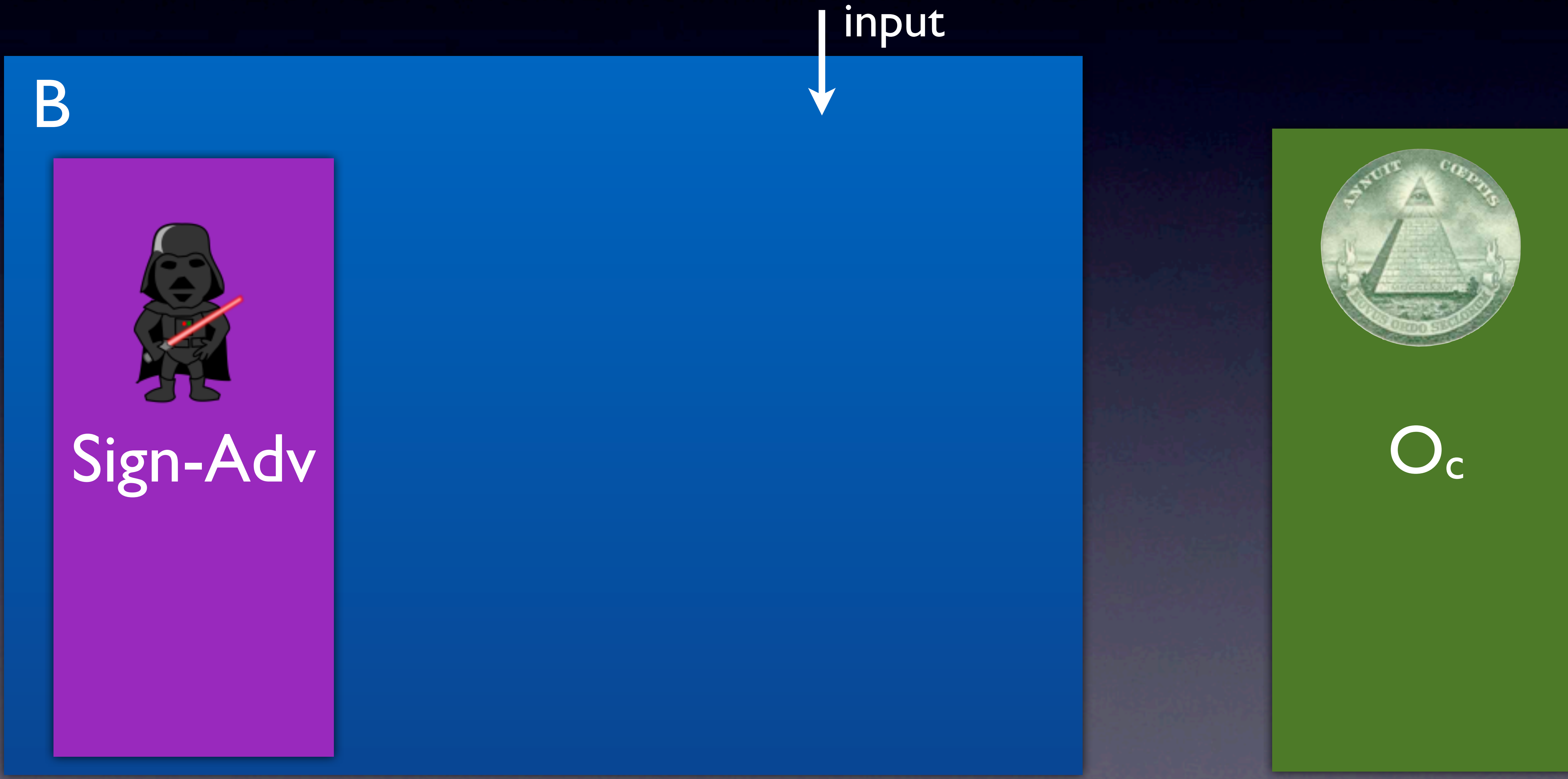


Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.

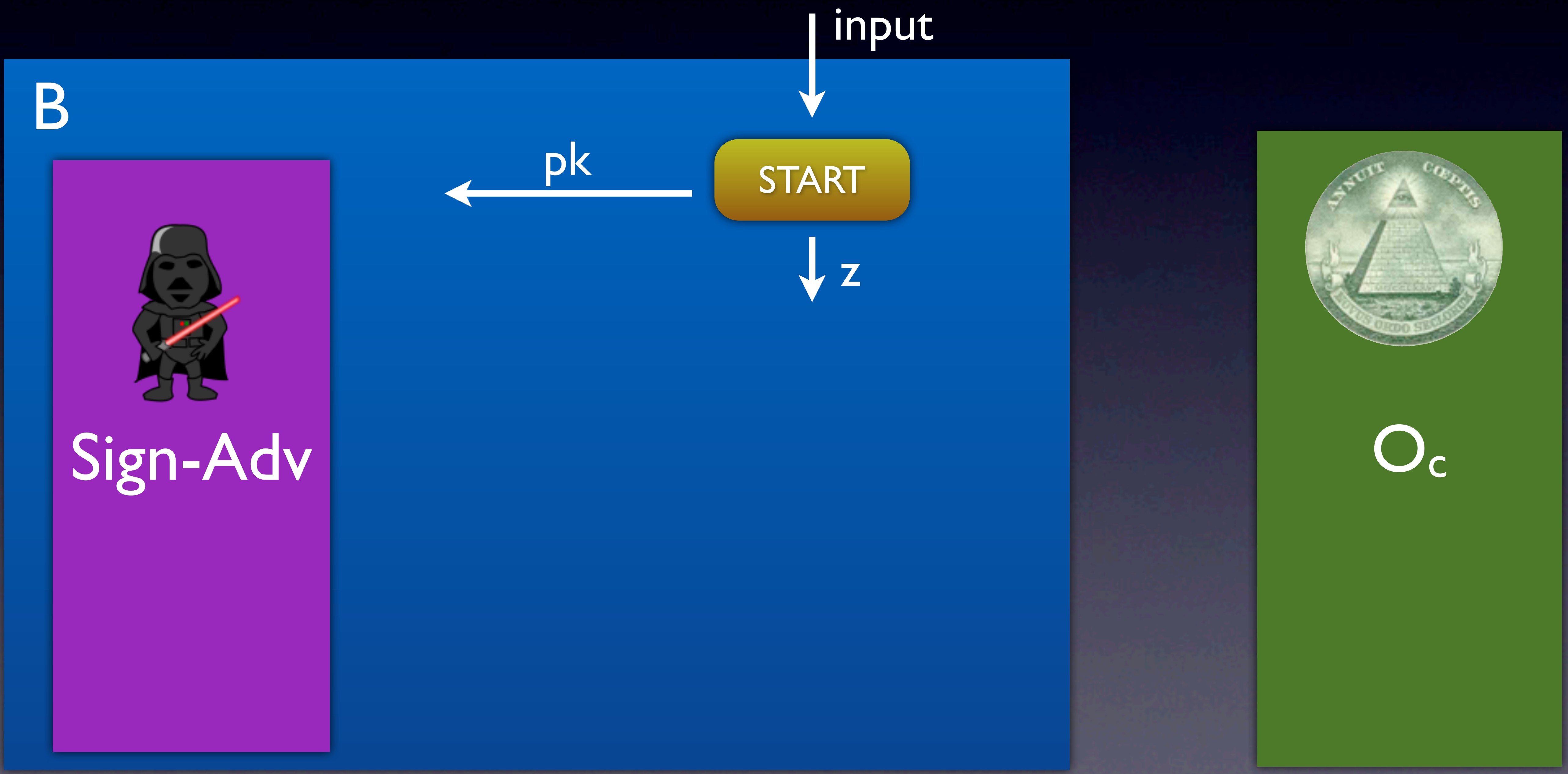
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



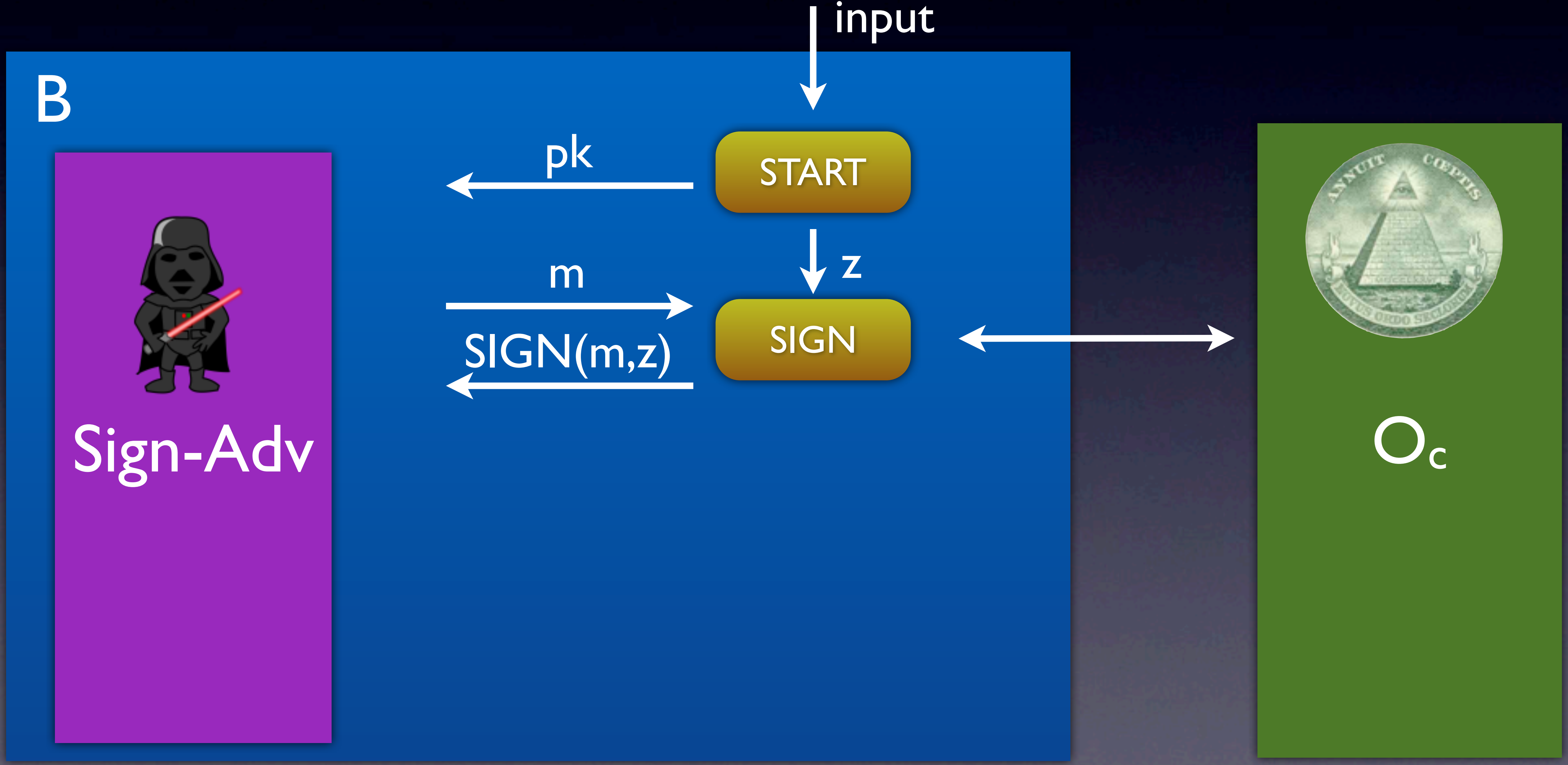
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



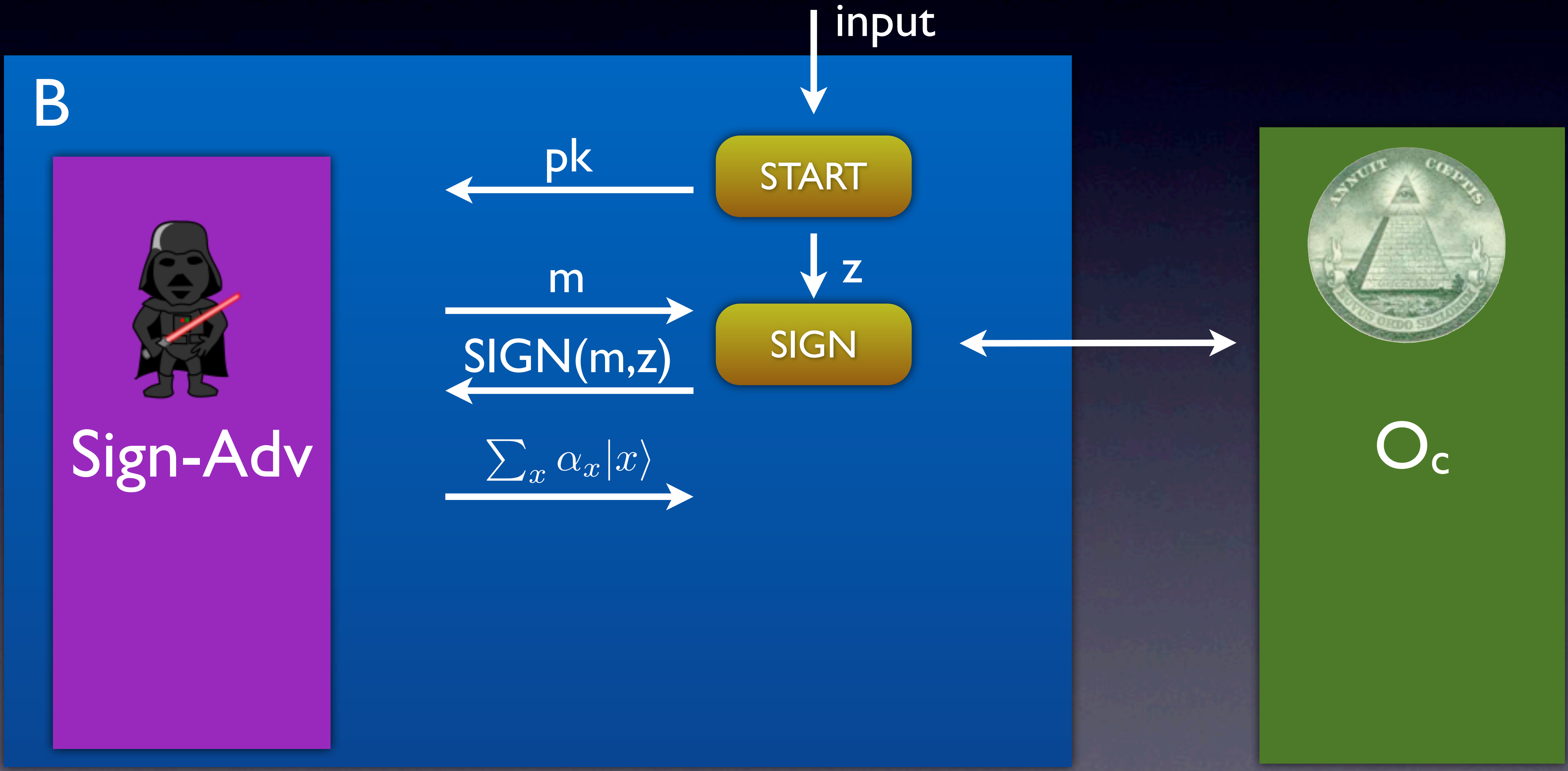
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



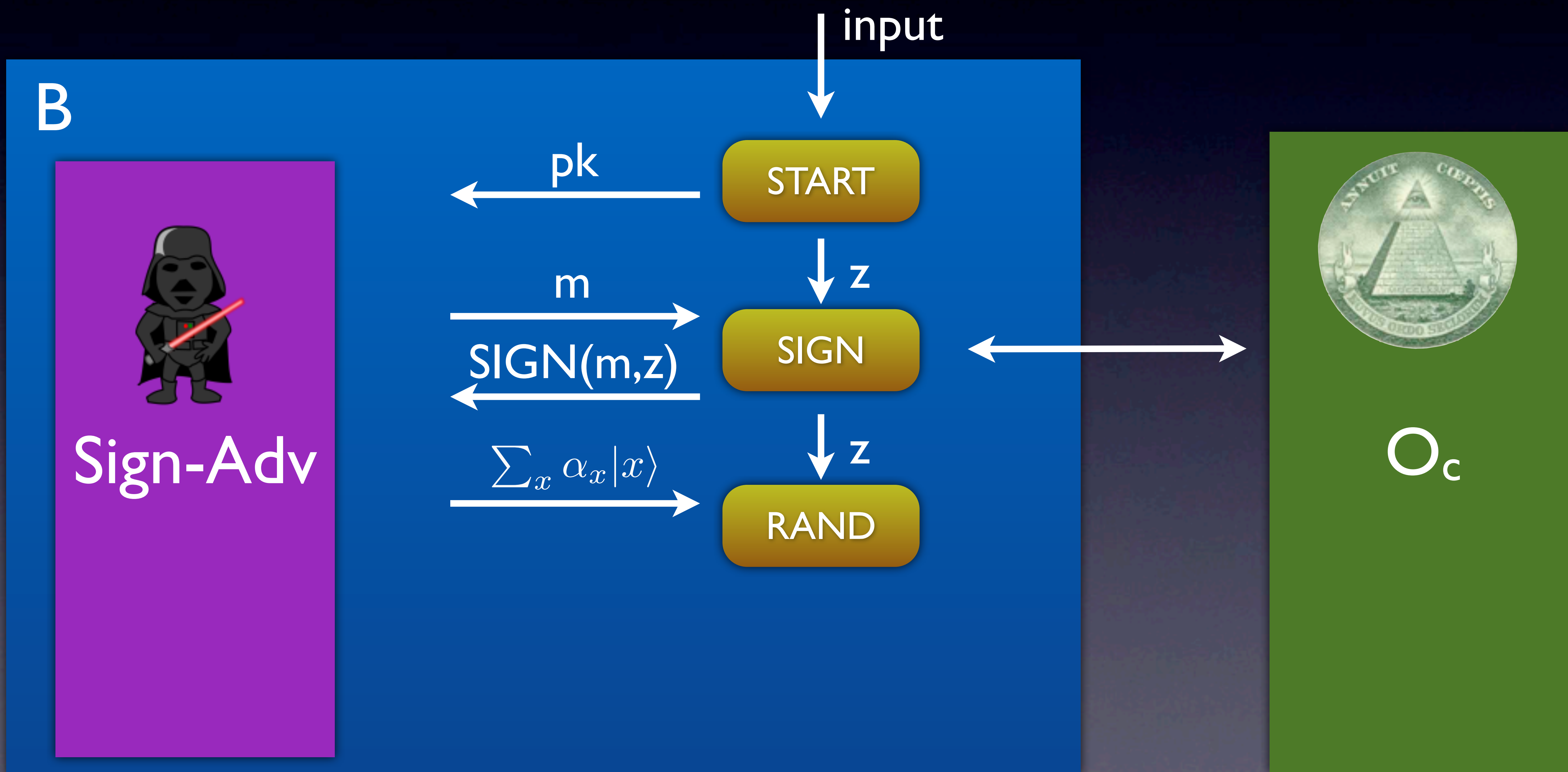
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



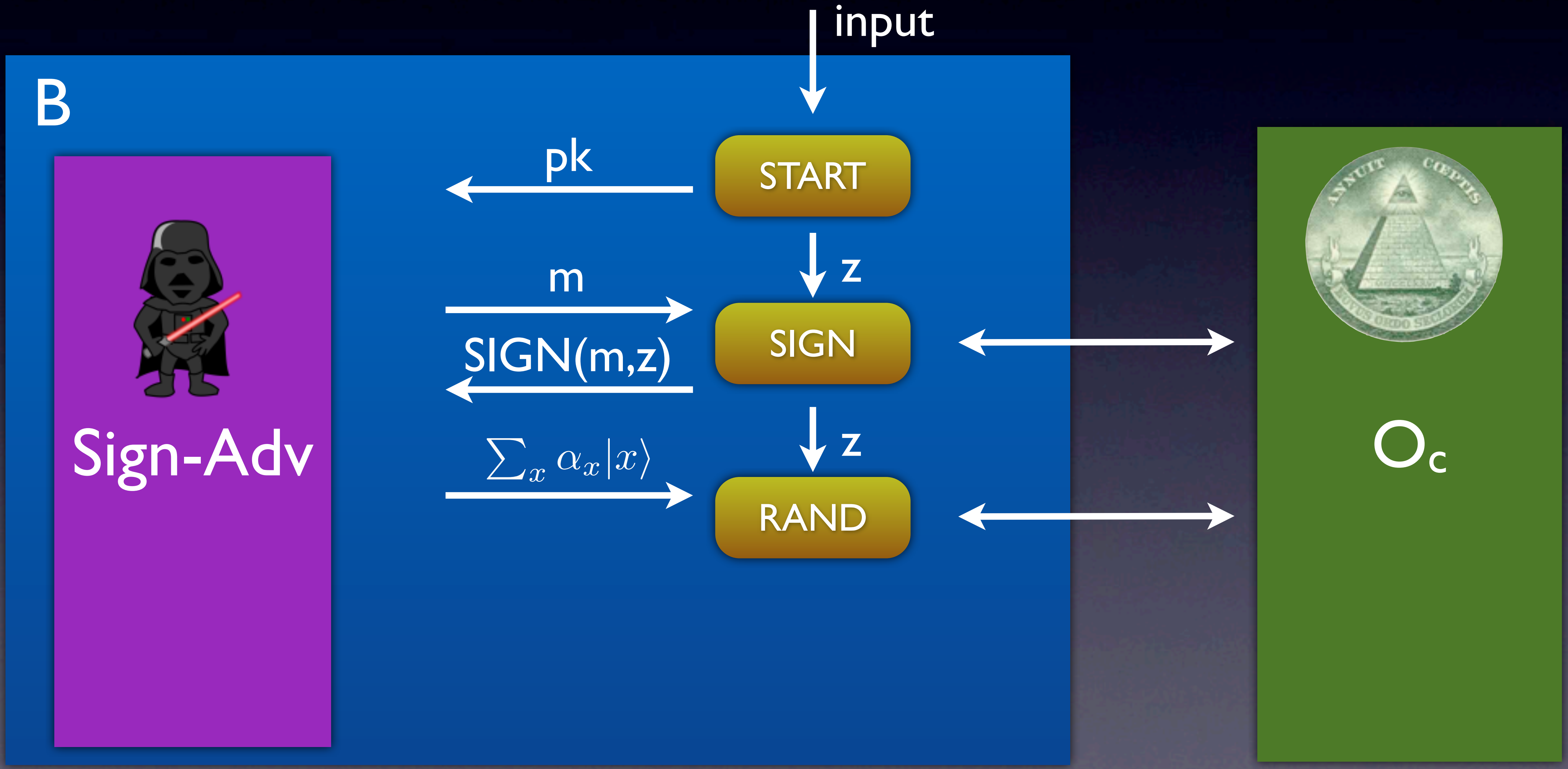
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



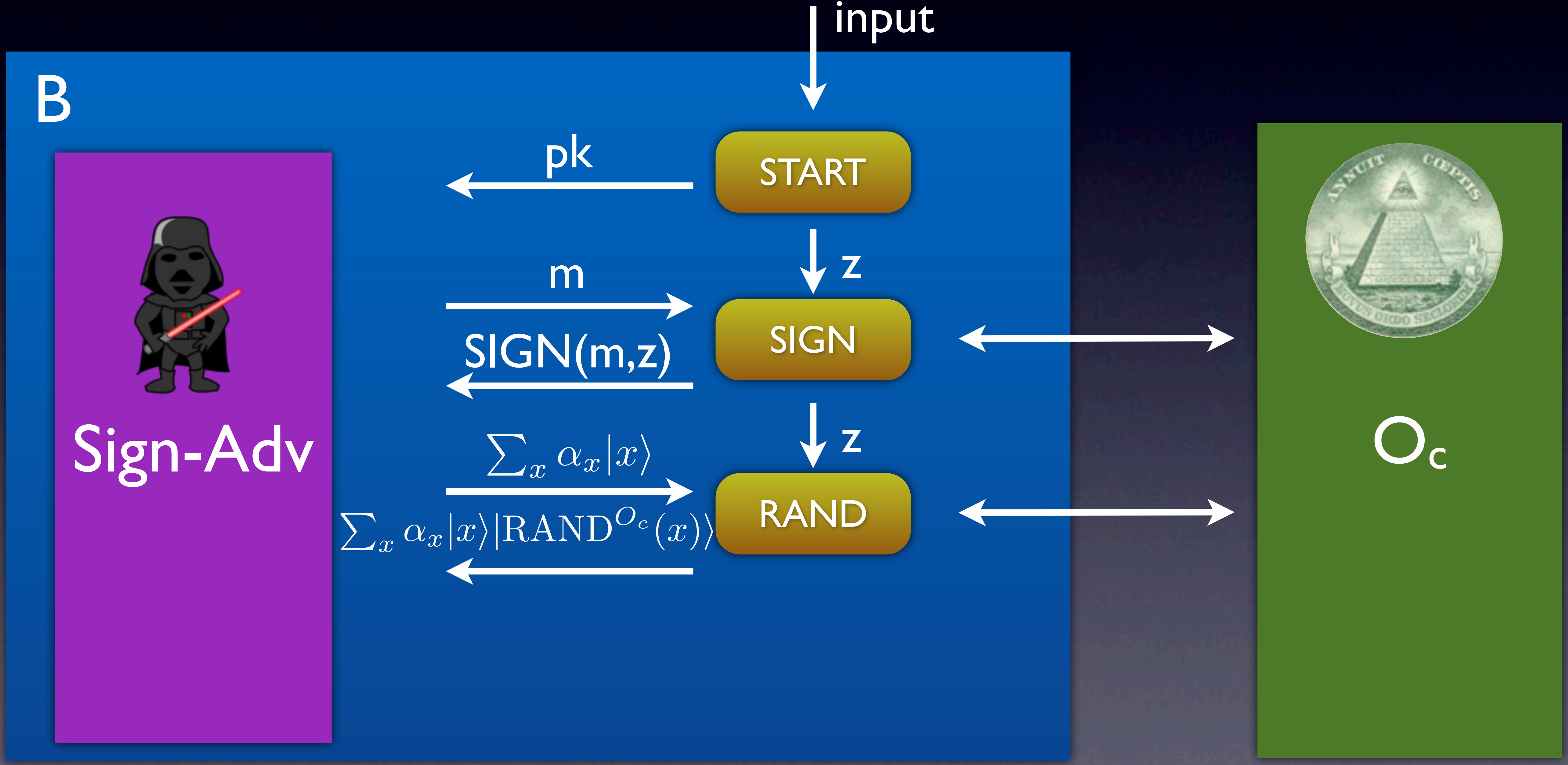
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



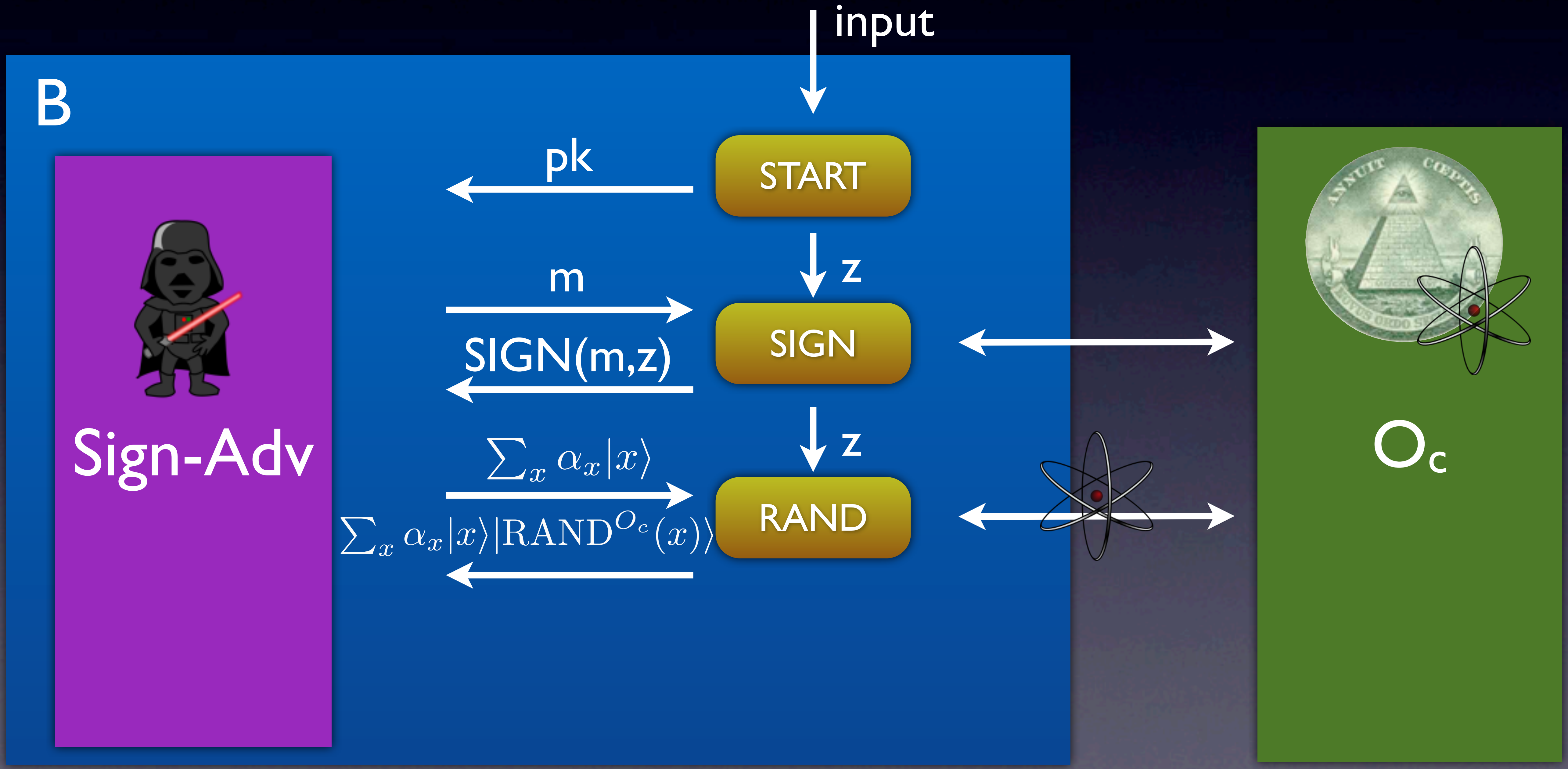
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



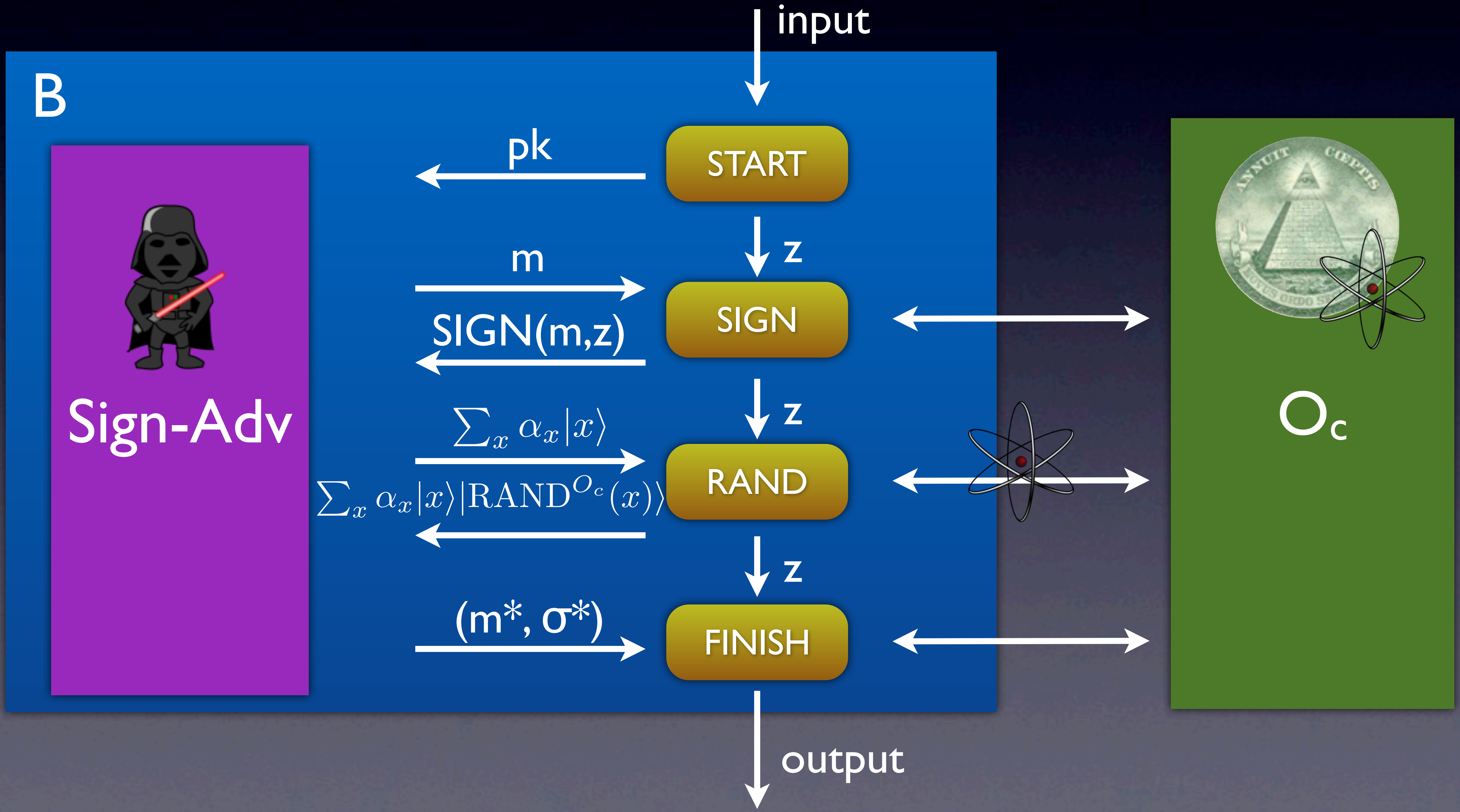
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



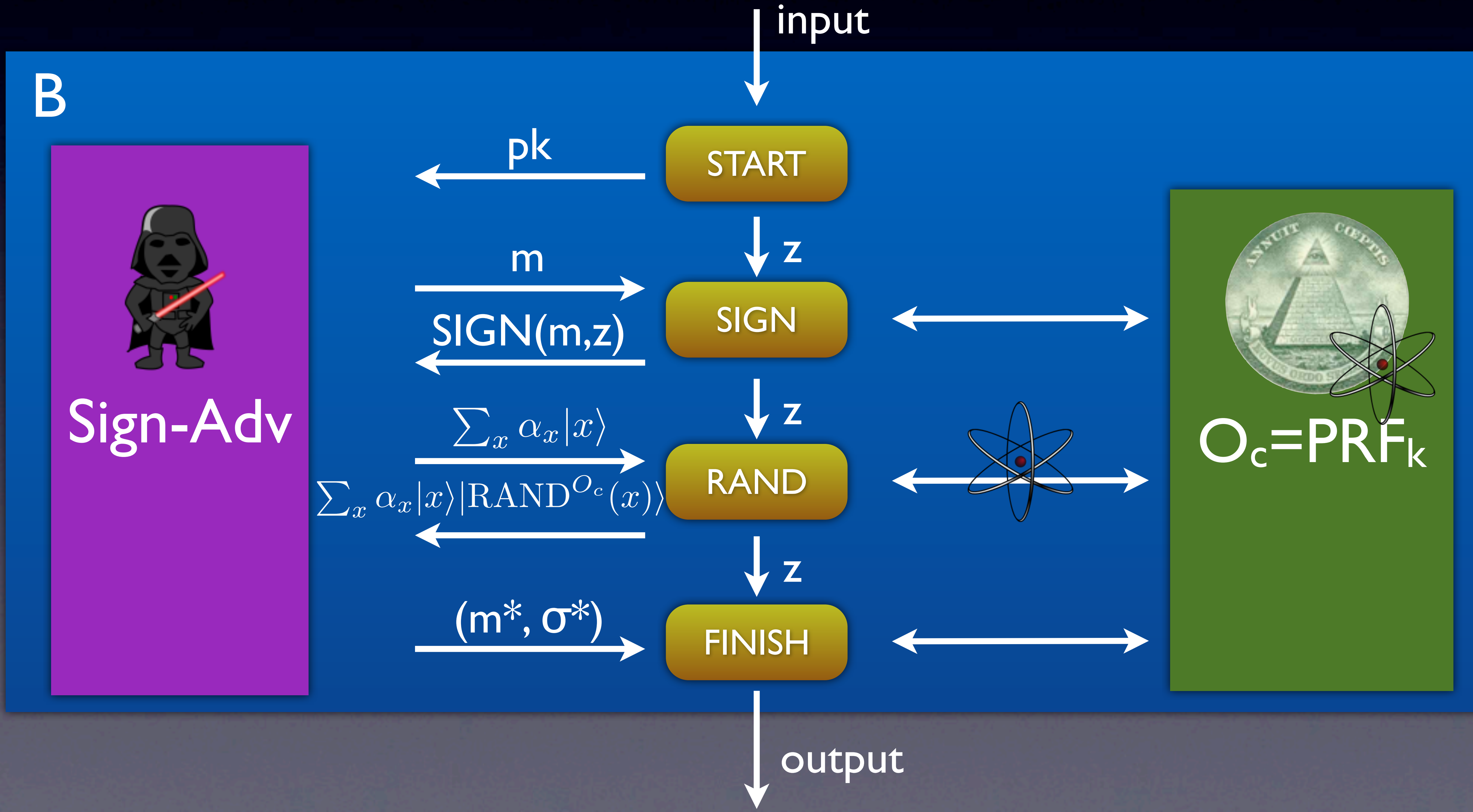
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



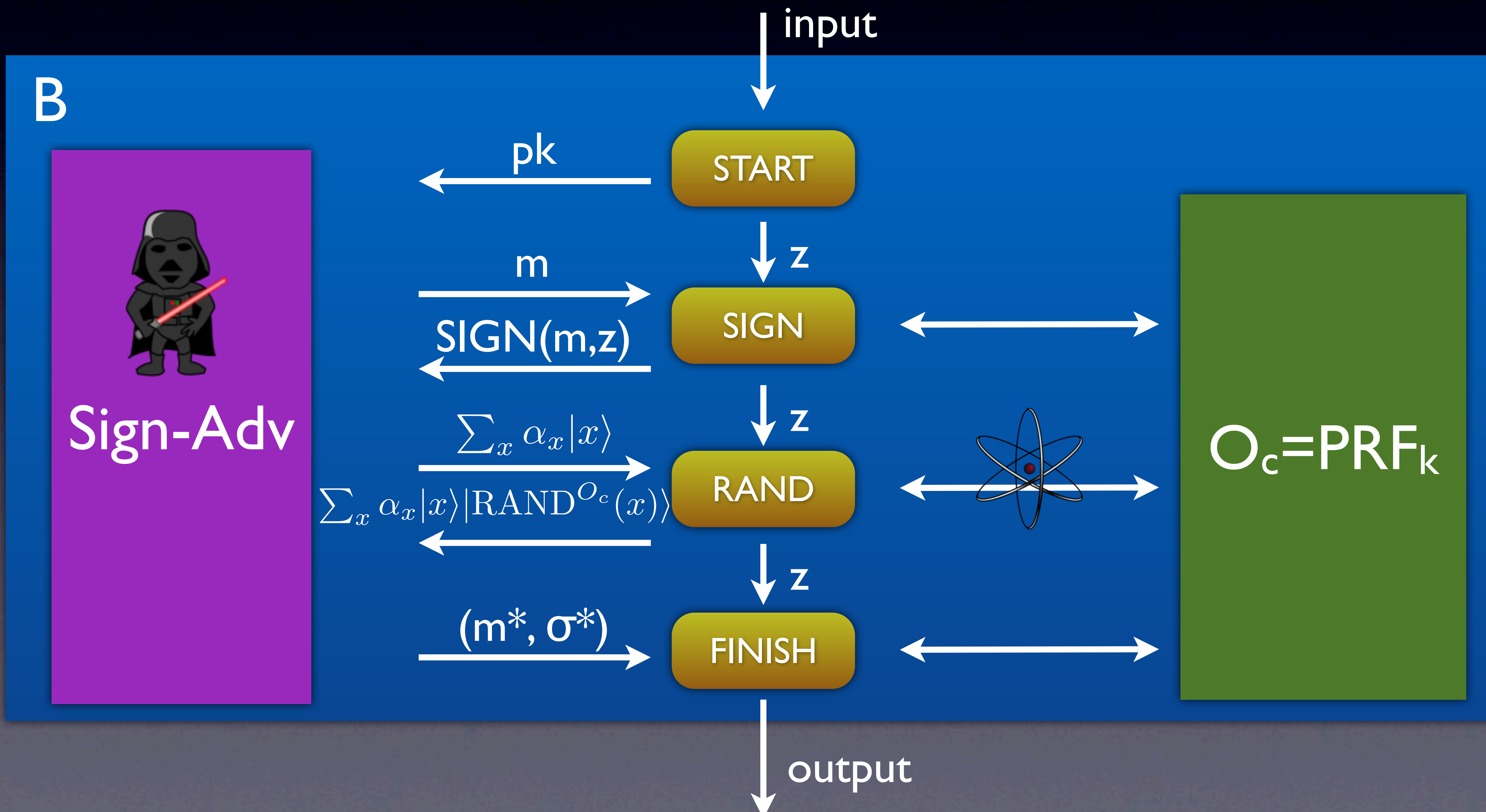
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



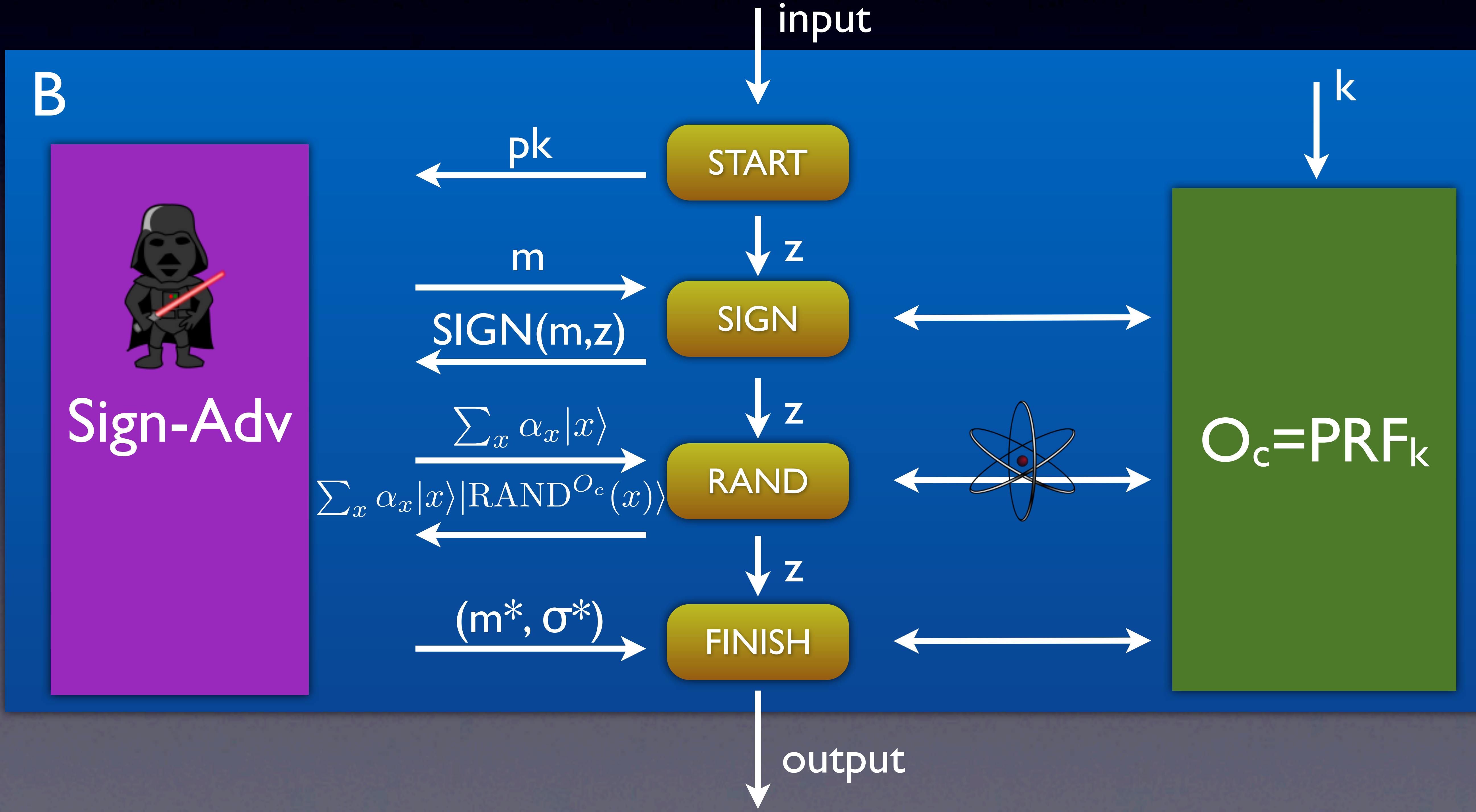
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



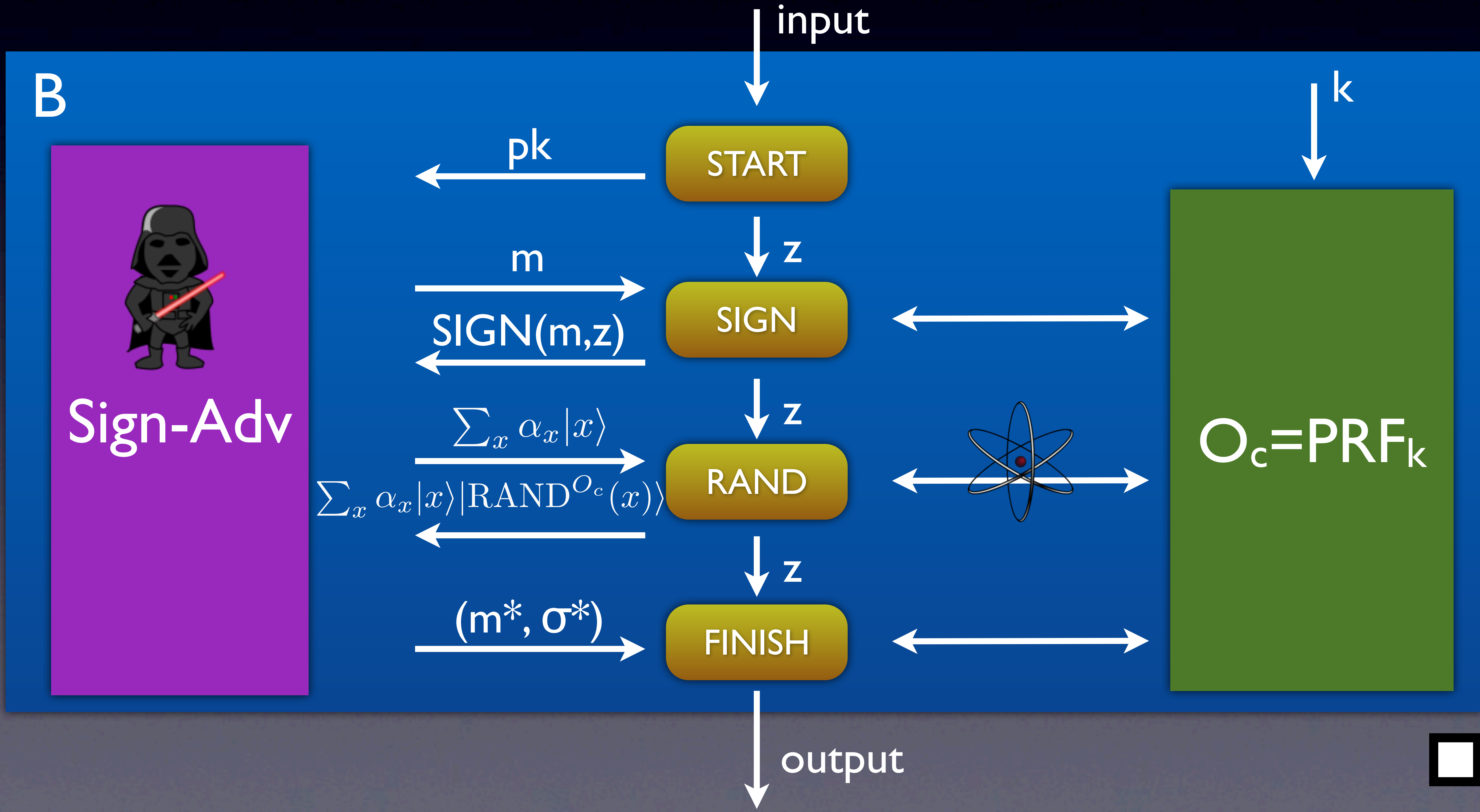
Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



Proof

Theorem: Assume that quantum-accessible PRFs exist, then a signature scheme with history-free reduction is secure in the QROM.



Other History-Free Reductions

- Signatures from claw-free permutations:
  - Full-Domain Hash [Coron00]
  - Katz-Wang Signatures [KW03]

Encryption

- history-freeness is complicated by the challenge query. Easier to prove security in QROM directly.

Encryption

- history-freeness is complicated by the challenge query. Easier to prove security in QROM directly.
- CPA-security of Bellare-Rogaway encryption [BR93]: $$E_{pk}(m) = f_{pk}(r) \,\|\, m \oplus O(r)$$

  where r random and f is a trapdoor permutation.

Encryption

- history-freeness is complicated by the challenge query. Easier to prove security in QROM directly.
- CPA-security of Bellare-Rogaway encryption [BR93]: $$E_{pk}(m) = f_{pk}(r) \,\|\, m \oplus O(r)$$ where r random and f is a trapdoor permutation.
- CCA-security of hybrid encryption scheme: $$E_{pk}(m) = f_{pk}(r) \,\|\, E^{\mathrm{sym}}_{O(r)}(m)$$ where f is a trapdoor permutation and E^{sym} is a CCA-secure private-key encryption

Summary

Summary

- Explanation of "querying oracles in superposition"

$$\sum_x \alpha_x |x\rangle \longrightarrow$$

$$\sum_x \alpha_x |x\rangle |O(x)\rangle \longleftarrow$$

Summary

- Explanation of "querying oracles in superposition"

$$\sum_x \alpha_x |x\rangle \longrightarrow$$

$$\sum_x \alpha_x |x\rangle |O(x)\rangle \longleftarrow$$

- In general, classical security reductions do not carry over to the quantum world

Summary

- Explanation of "querying oracles in superposition"

$$\sum_x \alpha_x |x\rangle \longrightarrow$$

$$\sum_x \alpha_x |x\rangle |O(x)\rangle \longleftarrow$$

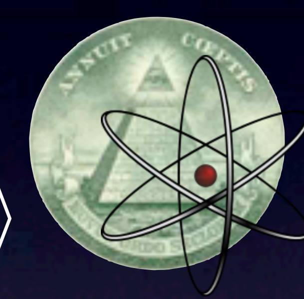
- In general, classical security reductions do not carry over to the quantum world
- Restricted classes of classical security proofs do imply quantum security

Summary

- Explanation of "querying oracles in superposition"

$$\sum_x \alpha_x |x\rangle \longrightarrow$$

$$\sum_x \alpha_x |x\rangle |O(x)\rangle \longleftarrow$$



- In general, classical security reductions do not carry over to the quantum world
- Restricted classes of classical security proofs do imply quantum security
- GPV signatures and BR encryption are secure in the QROM

Open Problems

- Generic Full-Domain Hash

Open Problems

- Generic Full-Domain Hash
- lattice-based identity-based encryption [GPV08]

Open Problems

- Generic Full-Domain Hash
- lattice-based identity-based encryption [GPV08]
- Signatures from Identification Protocols
  [Fiat Shamir 86]

Open Problems

- Generic Full-Domain Hash
- lattice-based identity-based encryption [GPV08]
- Signatures from Identification Protocols [Fiat Shamir 86]
- is history-freeness necessary?

Open Problems

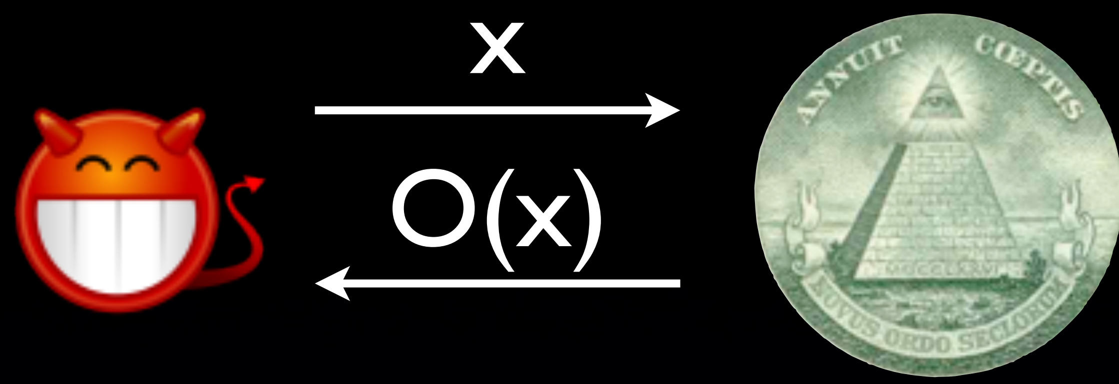
- Generic Full-Domain Hash
- lattice-based identity-based encryption [GPV08]
- Signatures from Identification Protocols [Fiat Shamir 86]
- is history-freeness necessary?
- CCA-security from weaker security notions [Fujisaki Okamoto 99]

Open Problems

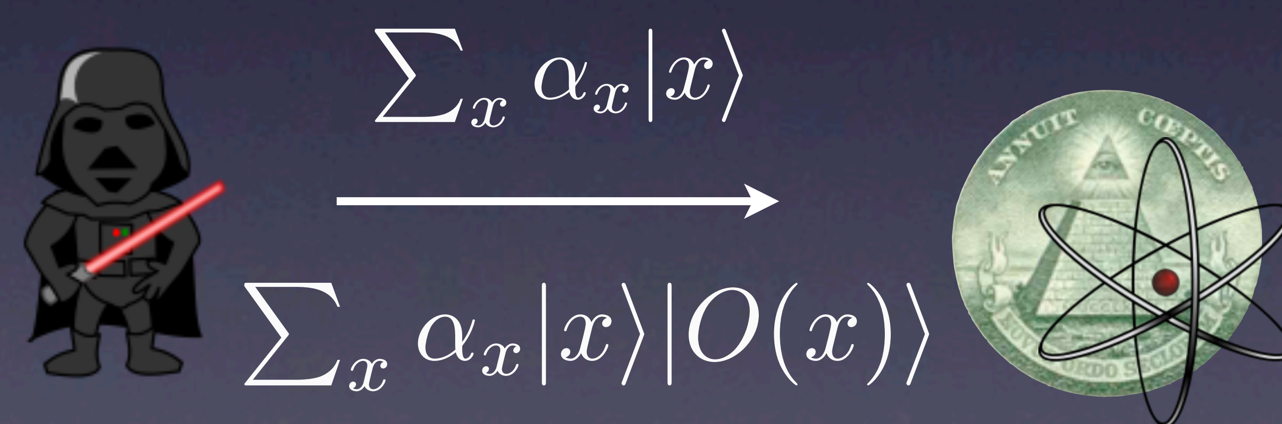
- Generic Full-Domain Hash
- lattice-based identity-based encryption [GPV08]
- Signatures from Identification Protocols [Fiat Shamir 86]
- is history-freeness necessary?
- CCA-security from weaker security notions [Fujisaki Okamoto 99]
- Quantum-accessible PRFs from one-way functions

Thank you!
Questions?

http://arxiv.org/abs/1008.0931
http://eprint.iacr.org/2010/428



Thank you!
Questions?



http://arxiv.org/abs/1008.0931
http://eprint.iacr.org/2010/428