Relativized Succinct Arguments in the ROM Do Not Exist

Annalisa Barbara, Alessandro Chiesa, Ziyi Guan

Bocconi EPFL

https://eprint.iacr.org/2024/728

Succinct non-interactive arguments

SNARGs in the ROM

Succinct non-interactive arguments

SNARGs in the ROM

Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

Succinct non-interactive arguments

SNARGs in the ROM

Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions $f\colon \{0,1\}^* \to \{0,1\}^\ell$

Succinct non-interactive arguments

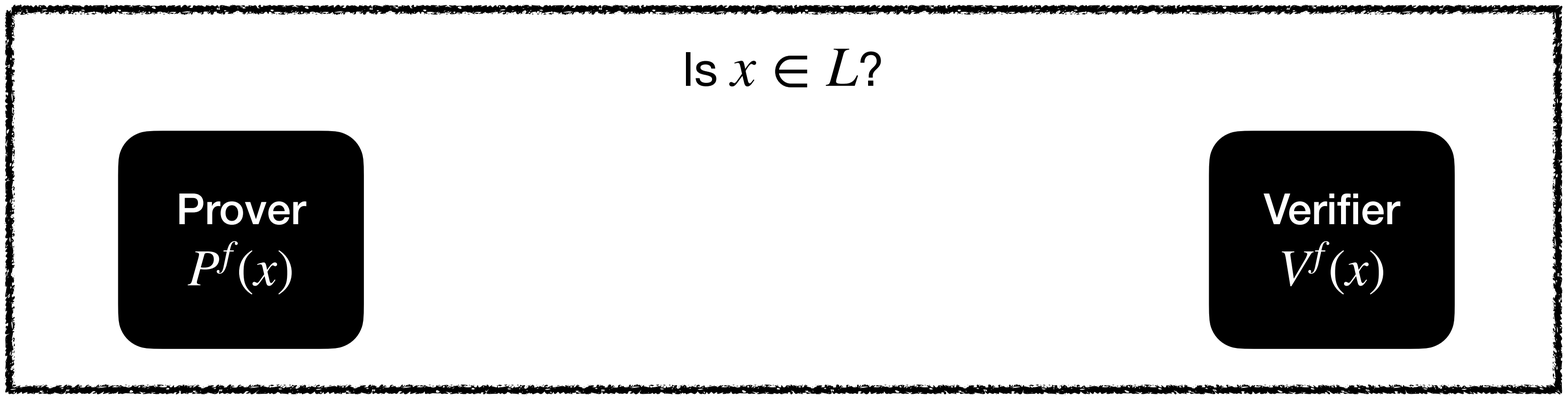
SNARGs in the ROM

Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions $f\colon \{0,1\}^* \to \{0,1\}^\ell$

Succinct non-interactive arguments

SNARGs in the ROM

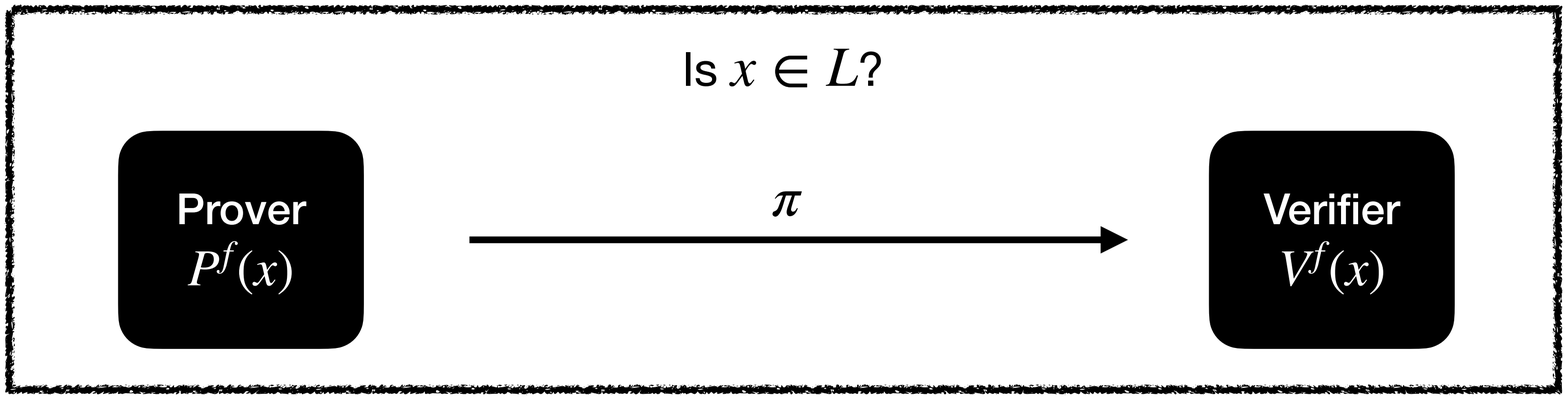


Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions $f\colon \{0,1\}^* \to \{0,1\}^\ell$

Succinct non-interactive arguments

SNARGs in the ROM

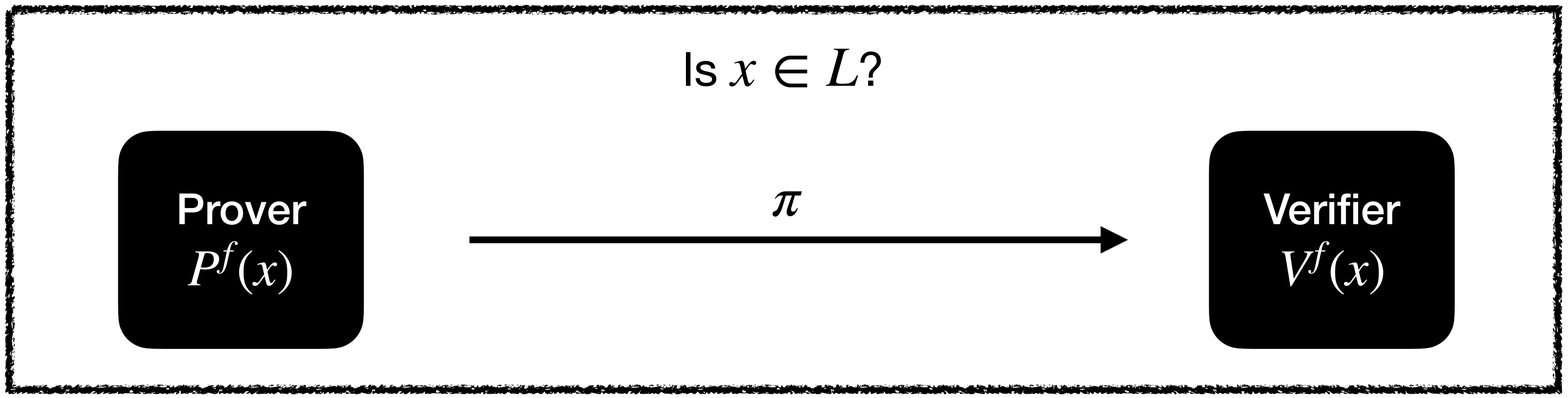


Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions $f\colon \{0,1\}^* \to \{0,1\}^\ell$

Succinct non-interactive arguments

SNARGs in the ROM



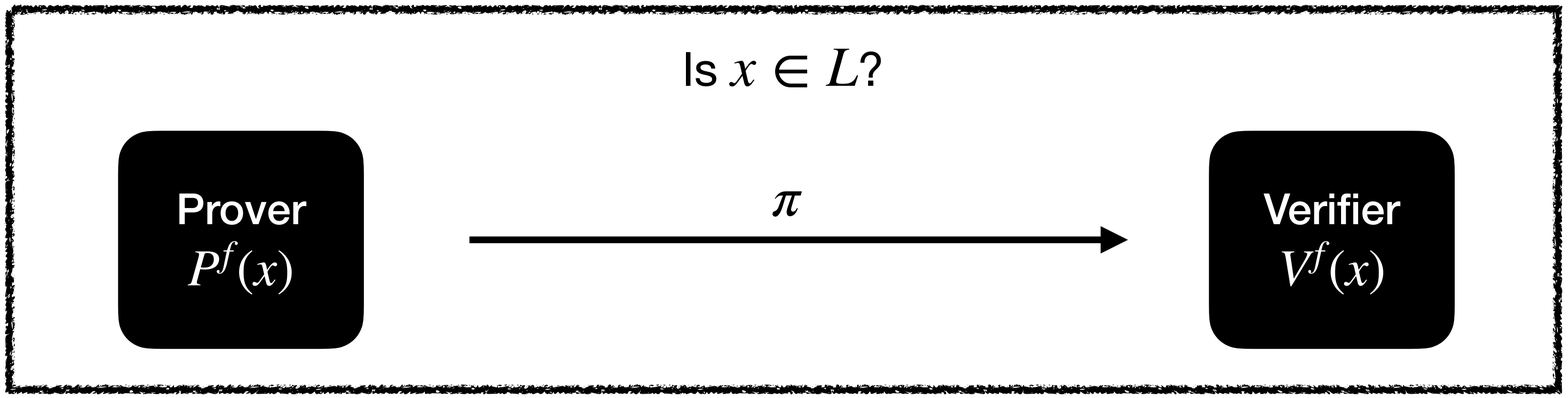
Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

Completeness: $\forall$ instance-generating adversary A,

Succinct non-interactive arguments

SNARGs in the ROM



Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

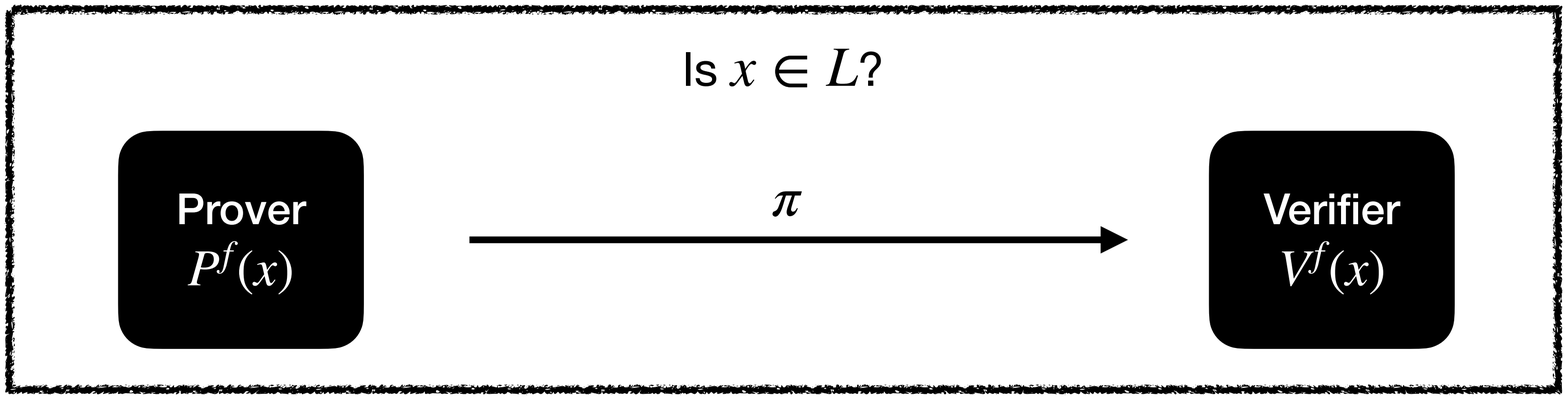
uniform distribution over all functions $f\colon \{0,1\}^* \to \{0,1\}^\ell$

Completeness: $\forall$ instance-generating adversary A,

$$\Pr\left[x \in L \wedge V^f(x,\pi) = 1 \;\middle|\; \begin{array}{l} f \leftarrow \mathcal{O} \\ x \leftarrow A^f \\ \pi \leftarrow P^f(x) \end{array}\right] = 1.$$

Succinct non-interactive arguments

SNARGs in the ROM



Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions $f\colon \{0,1\}^* \to \{0,1\}^\ell$

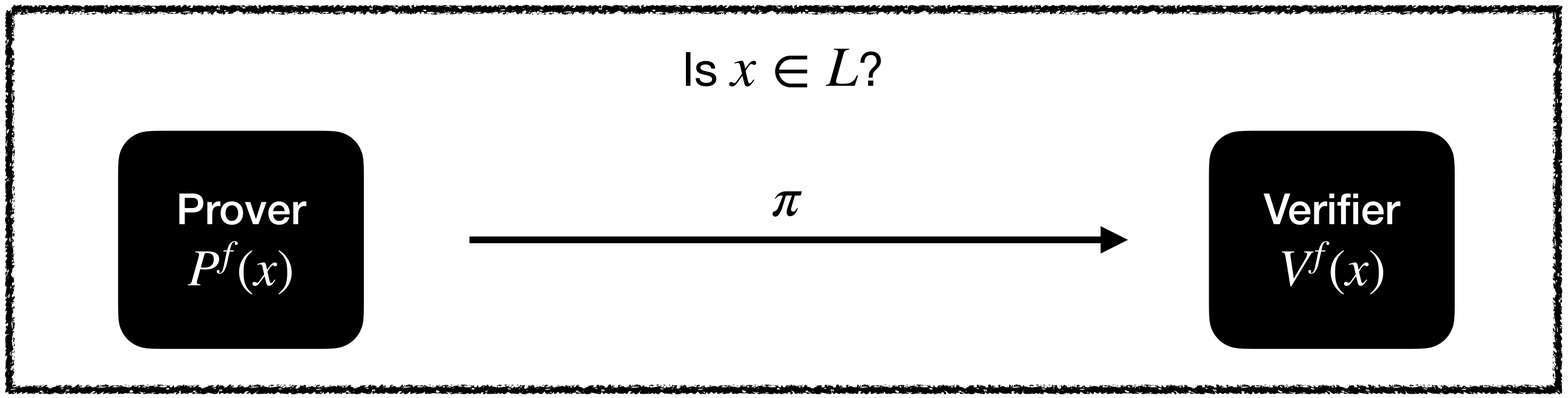
Completeness: ∀ instance-generating adversary A,

$$\Pr\left[\, x \in L \wedge V^f(x,\pi) = 1 \;\middle|\; \begin{array}{l} f \leftarrow \mathcal{O} \\ x \leftarrow A^f \\ \pi \leftarrow P^f(x) \end{array} \right] = 1.$$

Soundness: ∀ query-bounded and time-bounded adversary $\tilde{P}$,

Succinct non-interactive arguments

SNARGs in the ROM



Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

Completeness: ∀ instance-generating adversary A,

$$\Pr\left[x \in L \wedge V^f(x,\pi) = 1 \;\middle|\; \begin{array}{l} f \leftarrow \mathcal{O} \\ x \leftarrow A^f \\ \pi \leftarrow P^f(x) \end{array}\right] = 1.$$

Soundness: ∀ query-bounded and time-bounded adversary $\tilde{P}$,

$$\Pr\left[x \notin L \wedge V^f(x,\tilde{\pi}) = 1 \;\middle|\; \begin{array}{l} f \leftarrow \mathcal{O} \\ (x,\tilde{\pi}) \leftarrow \tilde{P}^f \end{array}\right] \leq \epsilon.$$

What is a relativized argument in the ROM?

Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions $f\colon \{0,1\}^* \to \{0,1\}^\ell$

What is a relativized argument in the ROM?

Relativization: The language L is relativized, $L = \{L_f : f \in \mathcal{O}\}$.

Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

What is a relativized argument in the ROM?

Relativization: The language L is relativized, $L = \{L_f : f \in \mathcal{O}\}$. e.g. $L_f := \{(x, y) : y = f(x)\}$

Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

What is a relativized argument in the ROM?

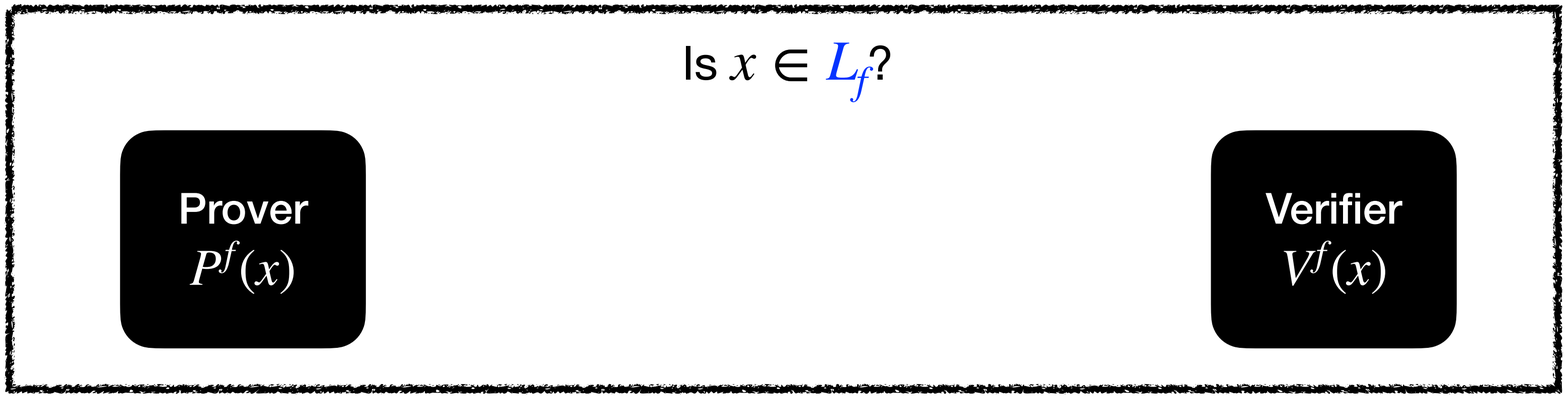
Relativization: The language L is relativized, $L = \{L_f : f \in \mathcal{O}\}$. e.g. $L_f := \{(x, y) : y = f(x)\}$

Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

What is a relativized argument in the ROM?

Relativization: The language L is relativized, $L = \{L_f : f \in \mathcal{O}\}$. e.g. $L_f := \{(x, y) : y = f(x)\}$

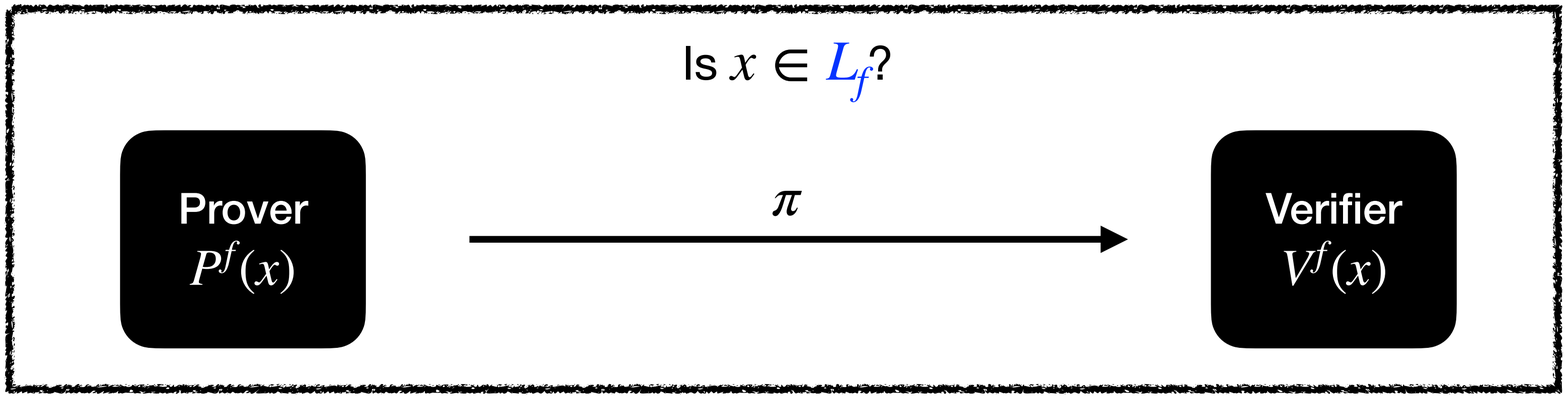


Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

What is a relativized argument in the ROM?

Relativization: The language L is relativized, $L = \{L_f : f \in \mathcal{O}\}$. e.g. $L_f := \{(x, y) : y = f(x)\}$

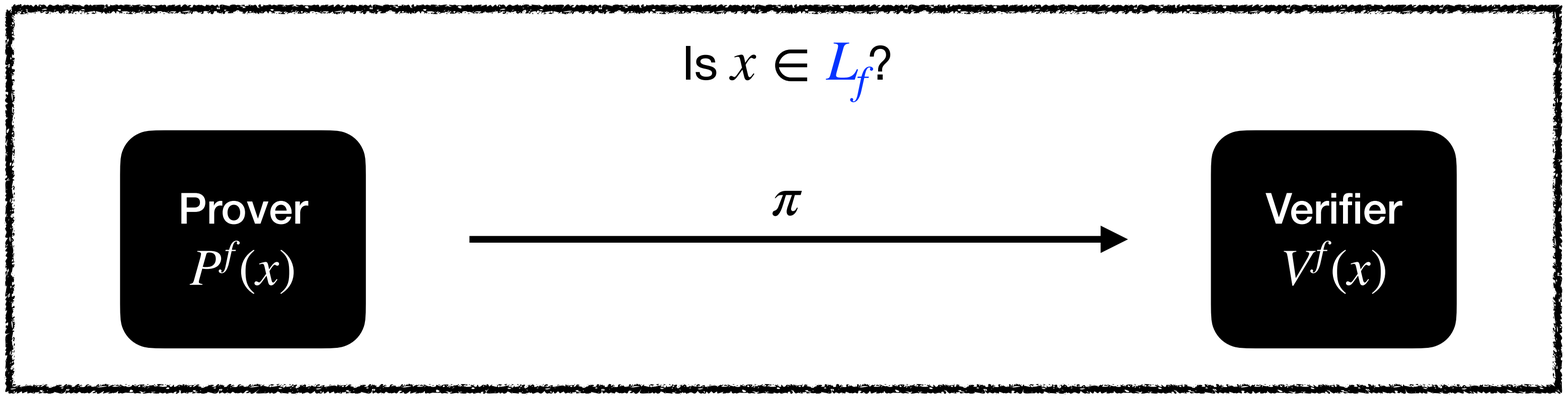


Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

What is a relativized argument in the ROM?

Relativization: The language L is relativized, $L = \{L_f : f \in \mathcal{O}\}$. e.g. $L_f := \{(x, y) : y = f(x)\}$



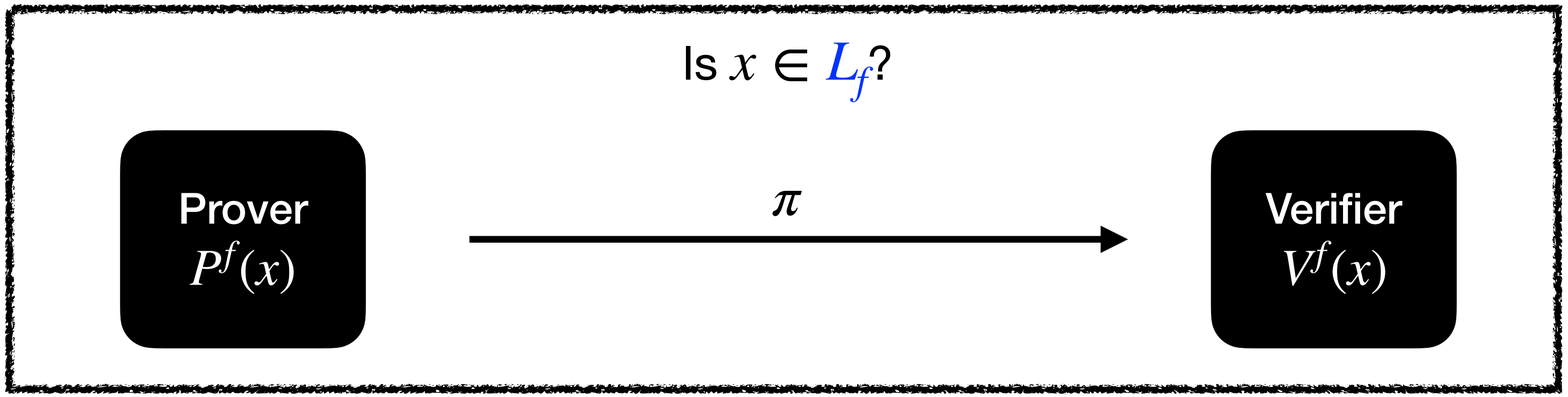
Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

Completeness: ∀ instance-generating adversary A,

What is a relativized argument in the ROM?

Relativization: The language L is relativized, $L = \{L_f : f \in \mathcal{O}\}$. e.g. $L_f := \{(x, y) : y = f(x)\}$



Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

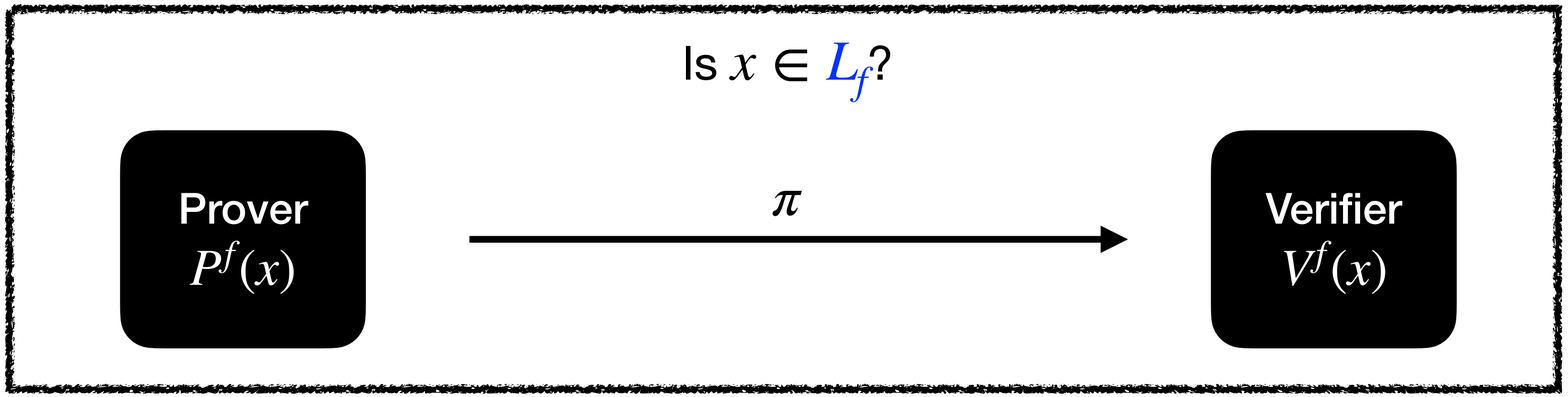
uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

Completeness: $\forall$ instance-generating adversary A,

$$\Pr\left[\, x \in L_f \wedge V^f(x, \pi) = 1 \;\middle|\; \begin{array}{l} f \leftarrow \mathcal{O} \\ x \leftarrow A^f \\ \pi \leftarrow P^f(x) \end{array} \right] = 1.$$

What is a relativized argument in the ROM?

Relativization: The language L is relativized, $L = \{L_f : f \in \mathcal{O}\}$. e.g. $L_f := \{(x, y) : y = f(x)\}$



Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

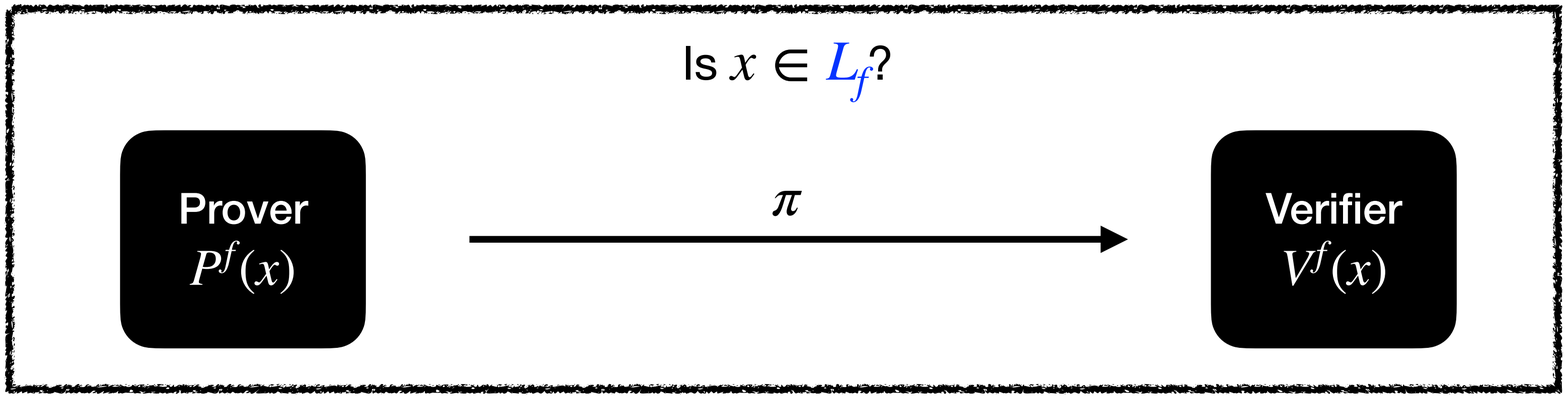
Completeness: ∀ instance-generating adversary A,

$$\Pr\left[x \in L_f \wedge V^f(x, \pi) = 1 \;\middle|\; \begin{array}{l} f \leftarrow \mathcal{O} \\ x \leftarrow A^f \\ \pi \leftarrow P^f(x) \end{array}\right] = 1.$$

Soundness: ∀ query-bounded and time-bounded adversary $\tilde{P}$,

What is a relativized argument in the ROM?

Relativization: The language L is relativized, $L = \{L_f : f \in \mathcal{O}\}$. e.g. $L_f := \{(x, y) : y = f(x)\}$



Random oracle $\mathcal{O} := \{\mathcal{O}_\ell\}_{\ell \in \mathbb{N}}$

uniform distribution over all functions f: $\{0,1\}^* \to \{0,1\}^\ell$

Completeness: ∀ instance-generating adversary A,

$$\Pr\left[x \in L_f \wedge V^f(x, \pi) = 1 \;\middle|\; \begin{array}{l} f \leftarrow \mathcal{O} \\ x \leftarrow A^f \\ \pi \leftarrow P^f(x) \end{array}\right] = 1.$$

Soundness: ∀ query-bounded and time-bounded adversary $\tilde{P}$,

$$\Pr\left[x \notin L_f \wedge V^f(x, \tilde{\pi}) = 1 \;\middle|\; \begin{array}{l} f \leftarrow \mathcal{O} \\ (x, \tilde{\pi}) \leftarrow \tilde{P}^f \end{array}\right] \leq \epsilon.$$

Why study relativized arguments?

Why study relativized arguments?

e.g. Verifiable distributed computation

Why study relativized arguments?

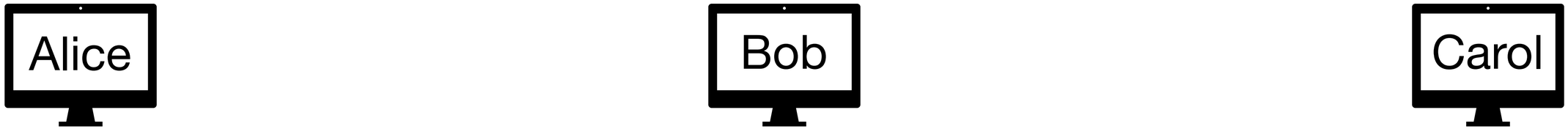
e.g. Verifiable distributed computation

Why study relativized arguments?

e.g. Verifiable distributed computation

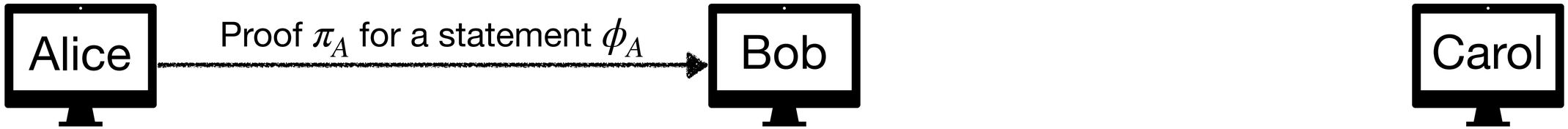
Why study relativized arguments?

e.g. Verifiable distributed computation



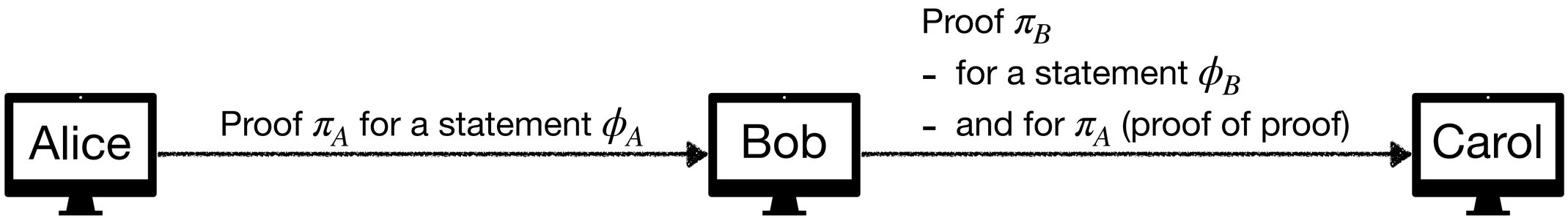
Why study relativized arguments?

e.g. Verifiable distributed computation



Why study relativized arguments?

e.g. Verifiable distributed computation



Why study relativized arguments?

e.g. Verifiable distributed computation

Distributed computation, blockchains, etc.
(Incrementally verifiable computation, Proof-carrying data)

Why study relativized arguments?

e.g. Verifiable distributed computation

Distributed computation, blockchains, etc.
(Incrementally verifiable computation, Proof-carrying data)

How does Bob produce π_B?

Why study relativized arguments?

e.g. Verifiable distributed computation

Distributed computation, blockchains, etc.
(Incrementally verifiable computation, Proof-carrying data)

How does Bob produce π_B?

Let ARG $= (P, V)$ be a SNARG for relativized CSAT:

Why study relativized arguments?

e.g. Verifiable distributed computation

Distributed computation, blockchains, etc.
(Incrementally verifiable computation, Proof-carrying data)

$\mathsf{CSAT}_f := \{(C, x) : \exists w, C^f(x, w) = 1\}$

How does Bob produce π_B?

Let $\mathsf{ARG} = (P, V)$ be a SNARG for relativized CSAT:

Why study relativized arguments?

e.g. Verifiable distributed computation

Distributed computation, blockchains, etc.
(Incrementally verifiable computation, Proof-carrying data)

$\mathsf{CSAT}_f := \{(C, x) : \exists w, C^f(x, w) = 1\}$

How does Bob produce π_B?

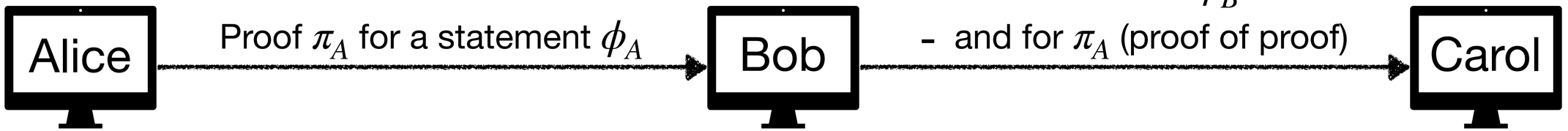
Let ARG $= (P, V)$ be a SNARG for relativized CSAT:

Oracle recursive circuit $\mathscr{C}^f(\phi_B, (\phi_A, \pi_A))$

Why study relativized arguments?

e.g. Verifiable distributed computation

Distributed computation, blockchains, etc.
(Incrementally verifiable computation, Proof-carrying data)



$\mathsf{CSAT}_f := \{(C, x) : \exists w, C^f(x, w) = 1\}$

How does Bob produce π_B?

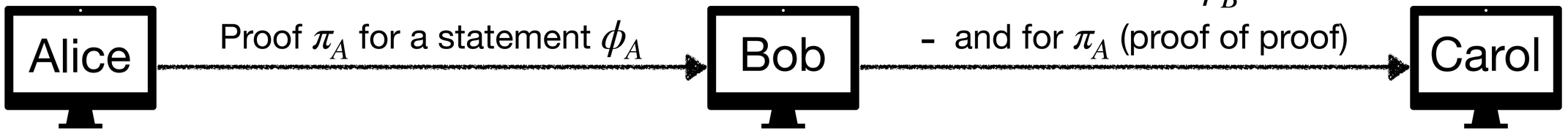
Let ARG $= (P, V)$ be a SNARG for relativized CSAT:

Oracle recursive circuit $\mathscr{C}^f(\phi_B, (\phi_A, \pi_A))$
- Check that ϕ_B is correct;

Why study relativized arguments?

e.g. Verifiable distributed computation

Distributed computation, blockchains, etc.
(Incrementally verifiable computation, Proof-carrying data)



$\mathsf{CSAT}_f := \{(C, x) : \exists w, C^f(x, w) = 1\}$

How does Bob produce π_B?

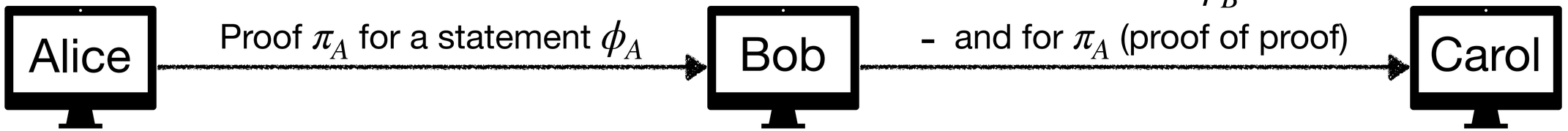
Let $\mathsf{ARG} = (P, V)$ be a SNARG for relativized CSAT:

Oracle recursive circuit $\mathscr{C}^f(\phi_B, (\phi_A, \pi_A))$
- Check that ϕ_B is correct;
- Check that $V^f(\mathscr{C}, \phi_A, \pi_A) = 1$.

Why study relativized arguments?

e.g. Verifiable distributed computation

Distributed computation, blockchains, etc.
(Incrementally verifiable computation, Proof-carrying data)



$\mathsf{CSAT}_f := \{(C, x) : \exists w, C^f(x, w) = 1\}$

How does Bob produce π_B?

Let ARG $= (P, V)$ be a SNARG for relativized CSAT:

Oracle recursive circuit $\mathscr{C}^f(\phi_B, (\phi_A, \pi_A))$
- Check that ϕ_B is correct;
- Check that $V^f(\mathscr{C}, \phi_A, \pi_A) = 1$.

$$\pi_B \leftarrow P^f(\mathscr{C}, \phi_B, (\phi_A, \pi_A))$$

Existing relativized SNARGs

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]
- Low-degree random oracle (LDROM) [CCS22]

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]
- Low-degree random oracle (LDROM) [CCS22]
- Arithmetized random oracle model (AROM) [CCGOS23]

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]
- Low-degree random oracle (LDROM) [CCS22]
- Arithmetized random oracle model (AROM) [CCGOS23]

Hard to instantiate!

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]
- Low-degree random oracle (LDROM) [CCS22]
- Arithmetized random oracle model (AROM) [CCGOS23]

Hard to instantiate!

How about the random oracle model?

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]
- Low-degree random oracle (LDROM) [CCS22]
- Arithmetized random oracle model (AROM) [CCGOS23]

Hard to instantiate!

How about the random oracle model?

Popular belief: No.

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]
- Low-degree random oracle (LDROM) [CCS22]
- Arithmetized random oracle model (AROM) [CCGOS23]

Hard to instantiate!

How about the random oracle model?

Popular belief: No.
Popular intuition: Relativized PCPs/IOPs do not exist in the ROM [CL20].

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]
- Low-degree random oracle (LDROM) [CCS22]
- Arithmetized random oracle model (AROM) [CCGOS23]

Hard to instantiate!

How about the random oracle model?

Popular belief: No.
Popular intuition: Relativized PCPs/IOPs do not exist in the ROM [CL20].
Counterexample to popular belief:

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]
- Low-degree random oracle (LDROM) [CCS22]
- Arithmetized random oracle model (AROM) [CCGOS23]

Hard to instantiate!

How about the random oracle model?

Popular belief: No.
Popular intuition: Relativized PCPs/IOPs do not exist in the ROM [CL20].
Counterexample to popular belief:
- Relativized PCPs/IOPs do not exist in the LDROM [CL20].

Existing relativized SNARGs

Relativized SNARGs exist in some oracle models:
- Signed random oracle model (SROM) [CT10]
- Low-degree random oracle (LDROM) [CCS22]
- Arithmetized random oracle model (AROM) [CCGOS23]

Hard to instantiate!

How about the random oracle model?

Popular belief: No.
Popular intuition: Relativized PCPs/IOPs do not exist in the ROM [CL20].
Counterexample to popular belief:
- Relativized PCPs/IOPs do not exist in the LDROM [CL20].
- Relativized SNARGs exist in the LDROM [CCS22].

Our results

Our results

Relativized arguments in the random oracle model do not exist.

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathsf{DTIME}^{\mathcal{O}}[t] \subseteq \mathsf{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$.

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathsf{DTIME}^{\mathcal{O}}[t] \subseteq \mathsf{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$.

Verifier computes everything itself.

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathrm{vq} = t]$.

Verifier computes everything itself.

Theorem 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathrm{vq} = o(t)]$.

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$.

Verifier computes everything itself.

Theorem 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = o(t)]$.

argument proof size

Trivial Baseline 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = t]$.

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$.

Verifier computes everything itself.

Theorem 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = o(t)]$.

argument proof size

Trivial Baseline 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = t]$.

Prover sends the entire witness.

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$.

Verifier computes everything itself.

Theorem 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = o(t)]$.

argument proof size

Trivial Baseline 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = t]$.

Prover sends the entire witness.

Theorem 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = o(t)]$.

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$. Verifier computes everything itself.

Theorem 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = o(t)]$.

argument proof size

Trivial Baseline 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = t]$. Prover sends the entire witness.

Theorem 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = o(t)]$.

Corollary. Relativized IVC/PCD does not exist in the ROM!

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$.

Verifier computes everything itself.

Theorem 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = o(t)]$.

argument proof size

Trivial Baseline 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = t]$.

Prover sends the entire witness.

Theorem 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = o(t)]$.

Existence of IVC/PCD in the ROM still remains open.

Corollary. Relativized IVC/PCD does not exist in the ROM!

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$.

Verifier computes everything itself.

Theorem 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = o(t)]$.

argument proof size

Trivial Baseline 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = t]$.

Prover sends the entire witness.

Theorem 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = o(t)]$.

Existence of IVC/PCD in the ROM still remains open.

Corollary. Relativized IVC/PCD does not exist in the ROM!

Note.

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$. Verifier computes everything itself.

Theorem 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = o(t)]$.

argument proof size

Trivial Baseline 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = t]$. Prover sends the entire witness.

Theorem 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = o(t)]$.

Existence of IVC/PCD in the ROM still remains open.

Corollary. Relativized IVC/PCD does not exist in the ROM!

Note.
- The results hold for SNARGs secure against query-bounded and time-bounded adversaries.

Our results

Relativized arguments in the random oracle model do not exist.

verifier query complexity to the RO

Trivial Baseline 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = t]$.

Verifier computes everything itself.

Theorem 1. $\mathrm{DTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{vq} = o(t)]$.

argument proof size

Trivial Baseline 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = t]$.

Prover sends the entire witness.

Theorem 2. $\mathrm{NTIME}^{\mathcal{O}}[t] \not\subseteq \mathrm{ARG}^{\mathcal{O}}[\mathsf{as} = o(t)]$.

Existence of IVC/PCD in the ROM still remains open.

Corollary. Relativized IVC/PCD does not exist in the ROM!

Note.
- The results hold for SNARGs secure against query-bounded and time-bounded adversaries.
- Similar results hold for interactive arguments.

Open problem: Characterization

Open problem: Characterization

Easy to learn/predict

Hard to learn/predict

Open problem: Characterization

Easy to learn/predict

Structured Oracle

Hard to learn/predict

Open problem: Characterization

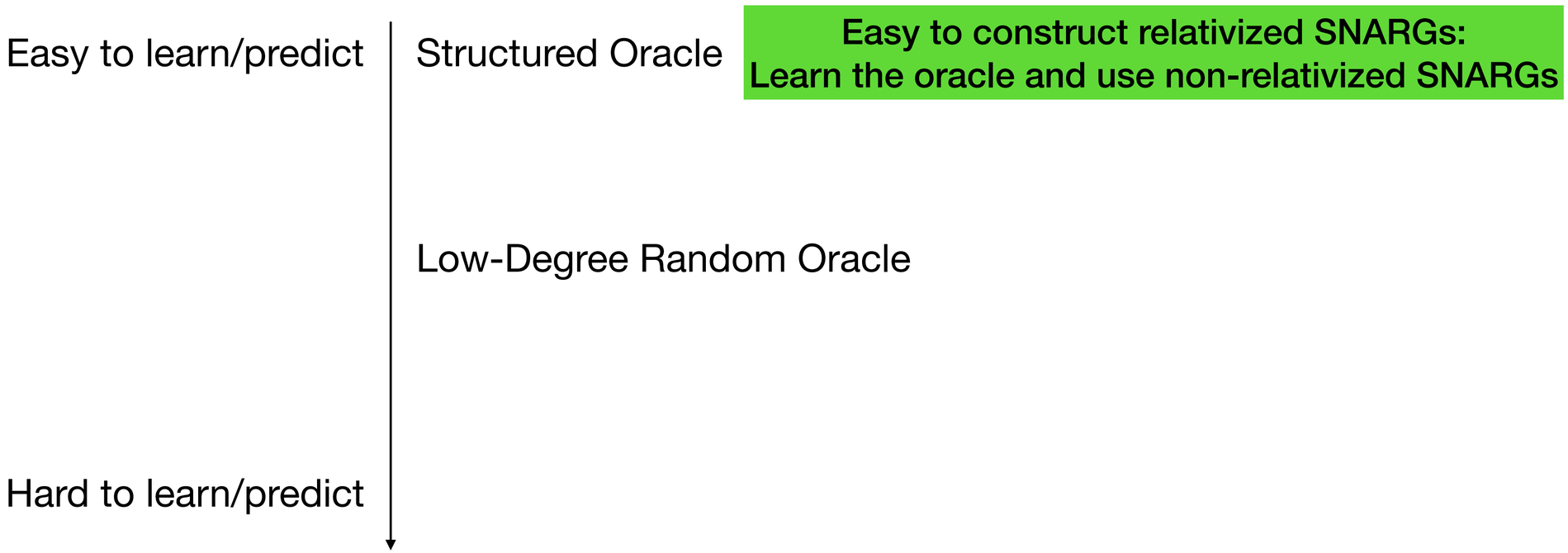
Easy to learn/predict

Hard to learn/predict

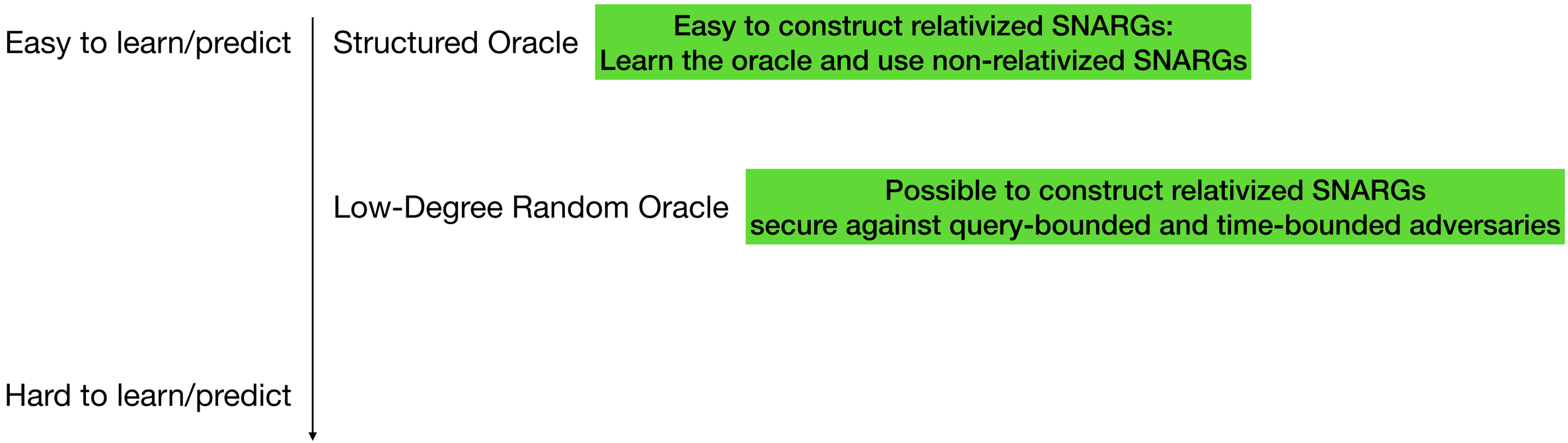
Structured Oracle

Easy to construct relativized SNARGs:
Learn the oracle and use non-relativized SNARGs

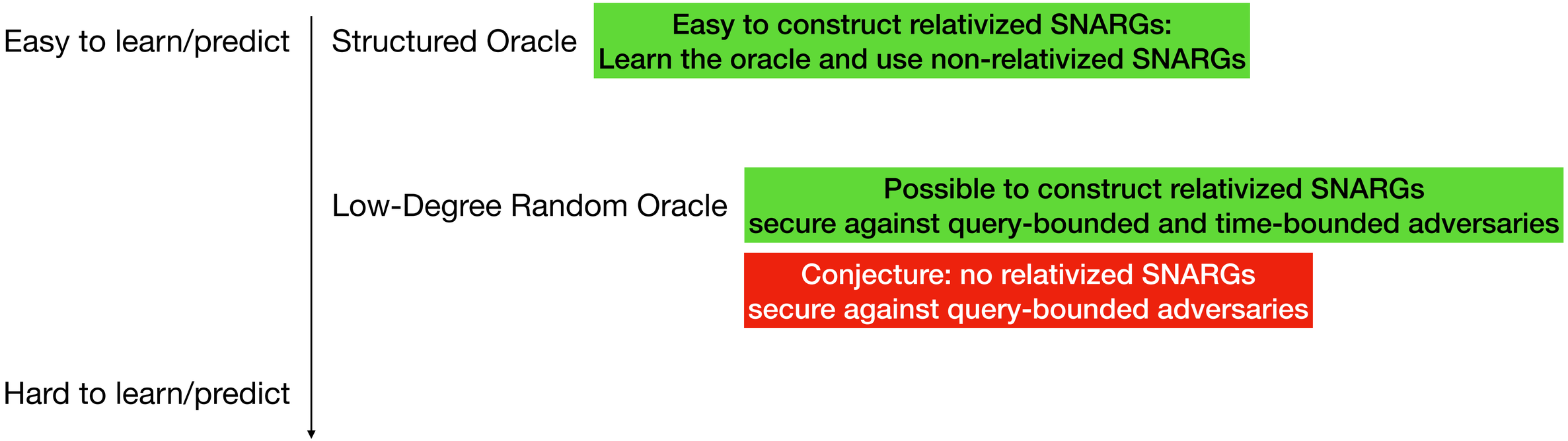
Open problem: Characterization



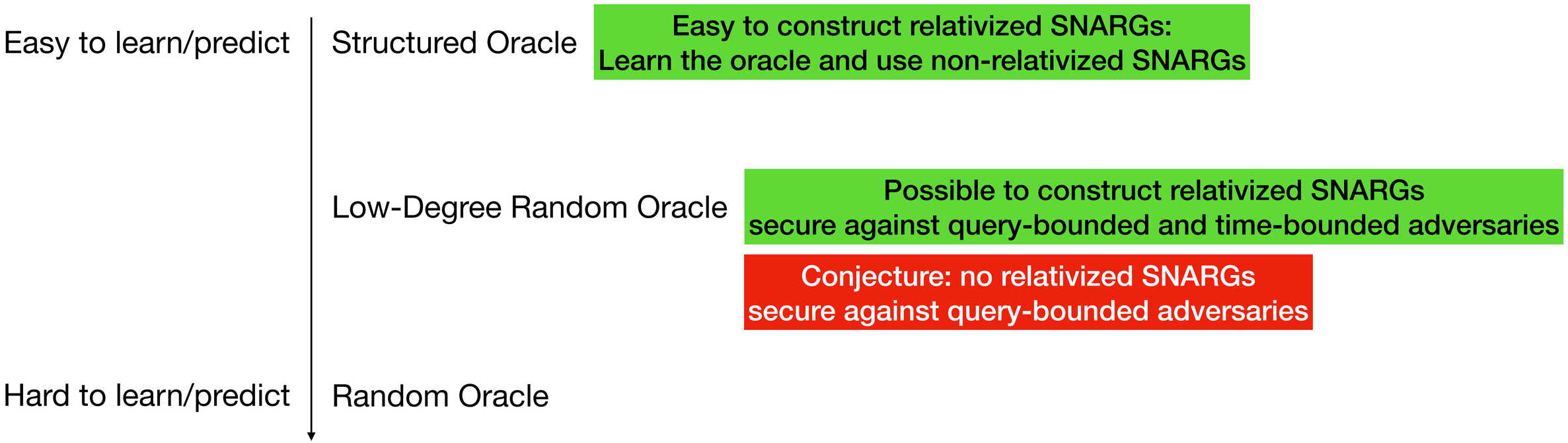
Open problem: Characterization



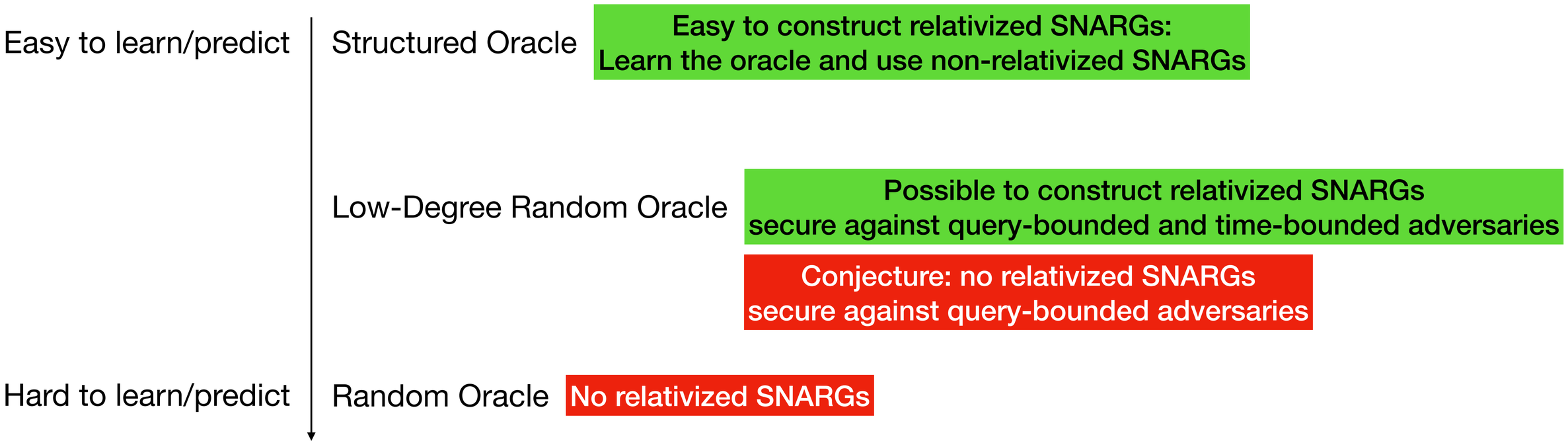
Open problem: Characterization



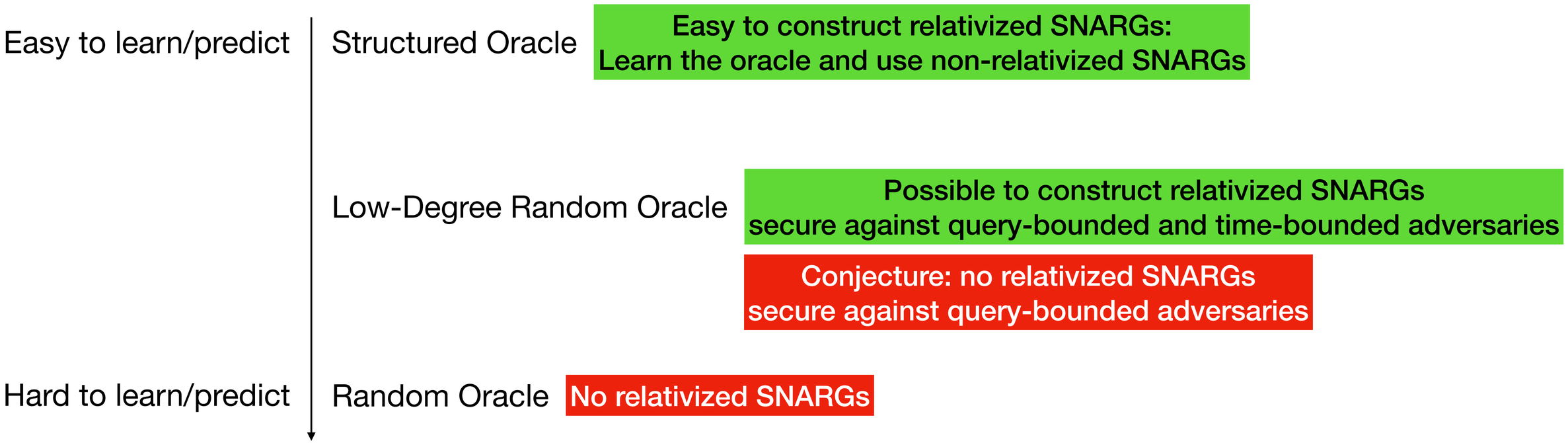
Open problem: Characterization



Open problem: Characterization



Open problem: Characterization



Open problem.

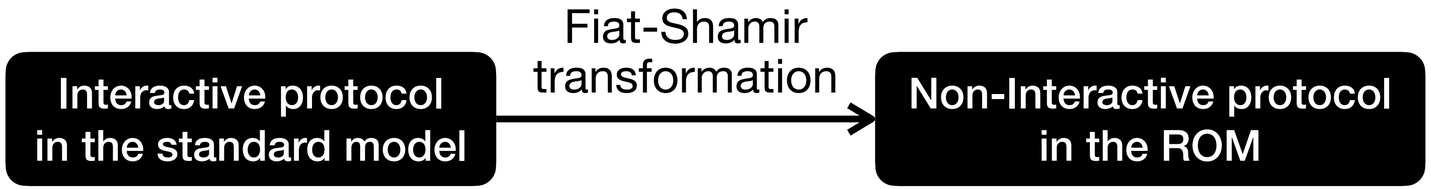
Give a sufficient and necessary condition for an oracle that separates DTIME/NTIME and relativized arguments.

Insights into Fiat-Shamir

Insights into Fiat-Shamir

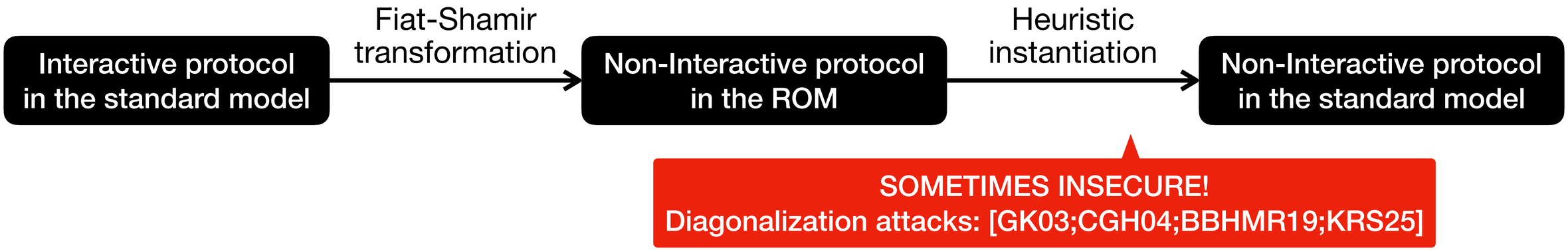
Interactive protocol
in the standard model

Insights into Fiat-Shamir

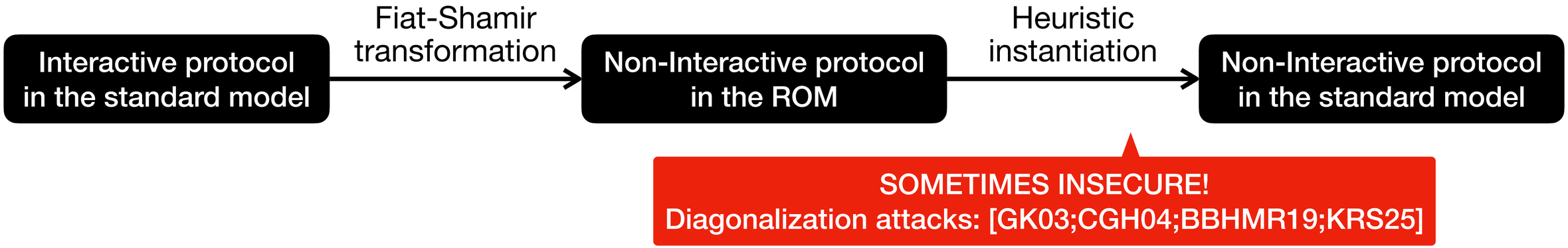


Insights into Fiat-Shamir

Insights into Fiat-Shamir

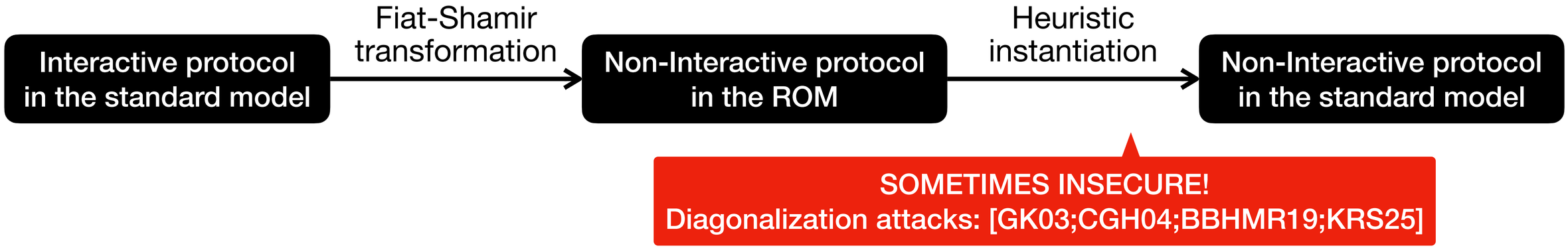


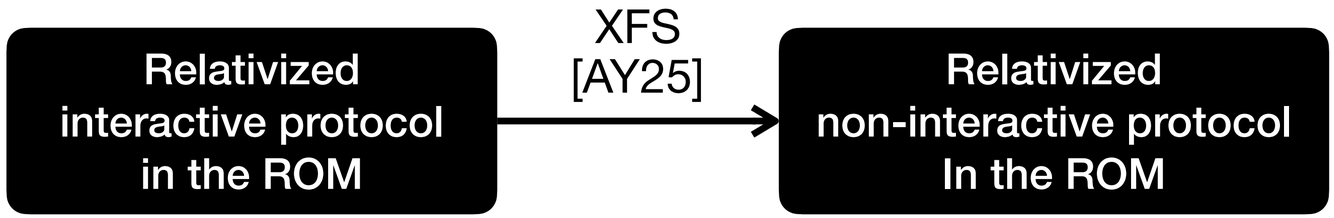
Insights into Fiat-Shamir



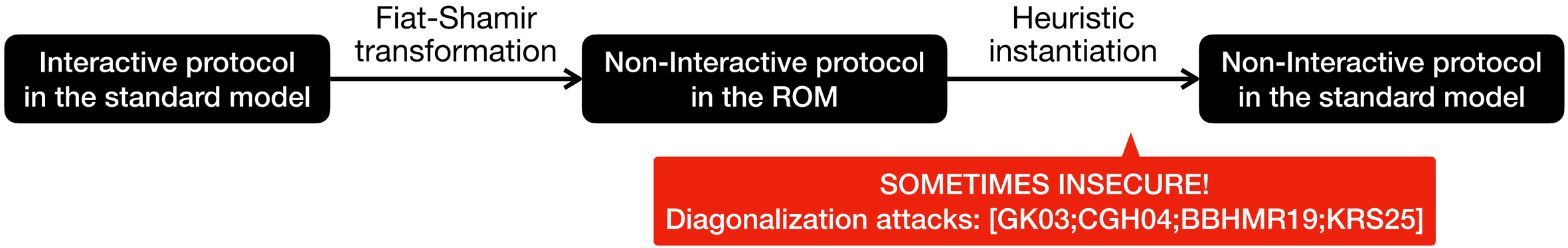
Relativized interactive protocol in the ROM

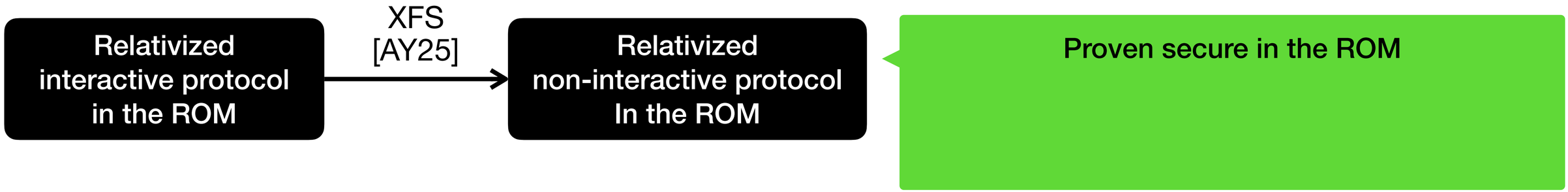
Insights into Fiat-Shamir



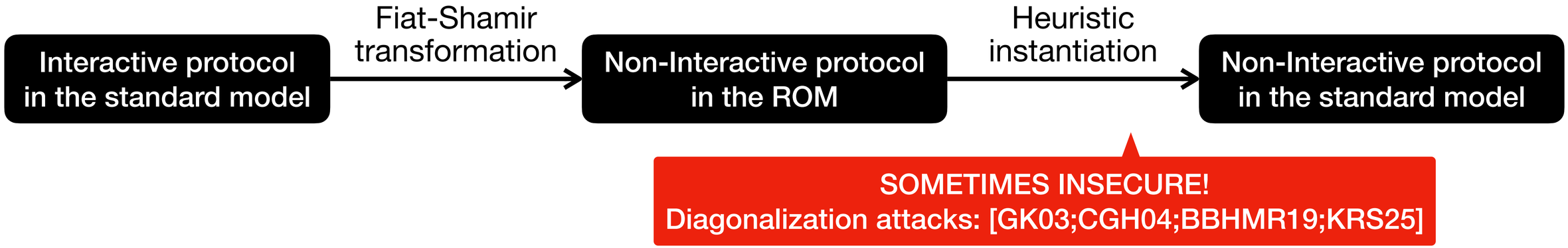


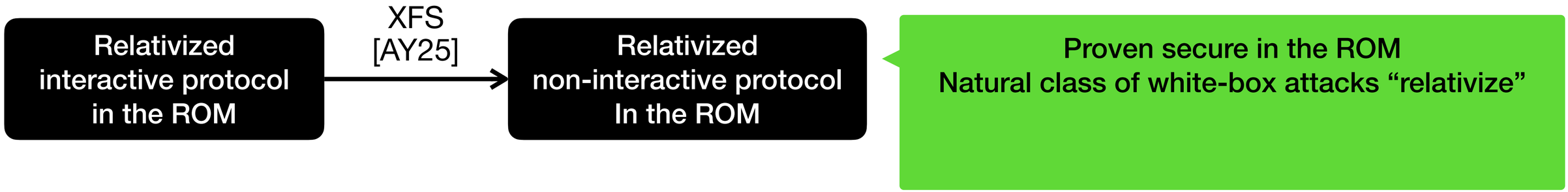
Insights into Fiat-Shamir



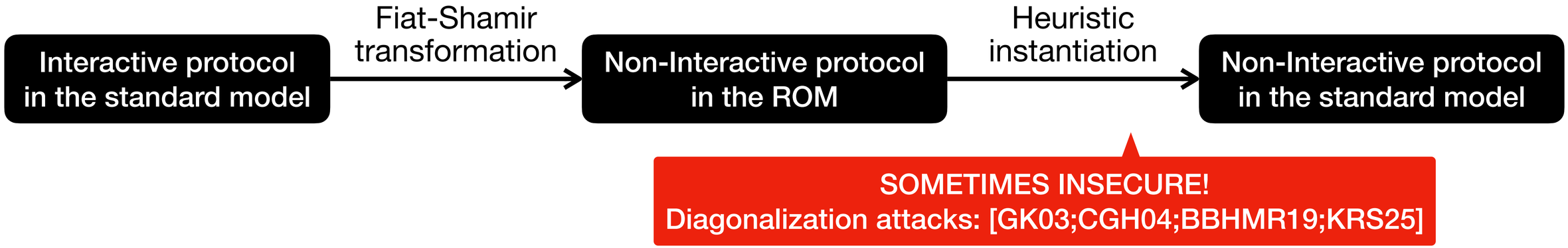


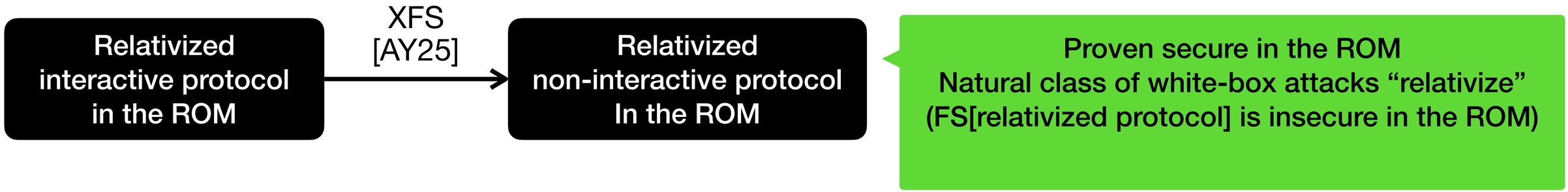
Insights into Fiat-Shamir



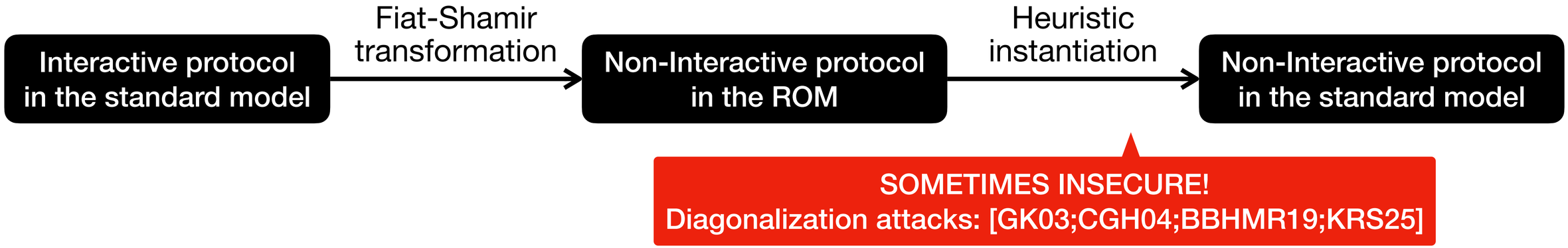


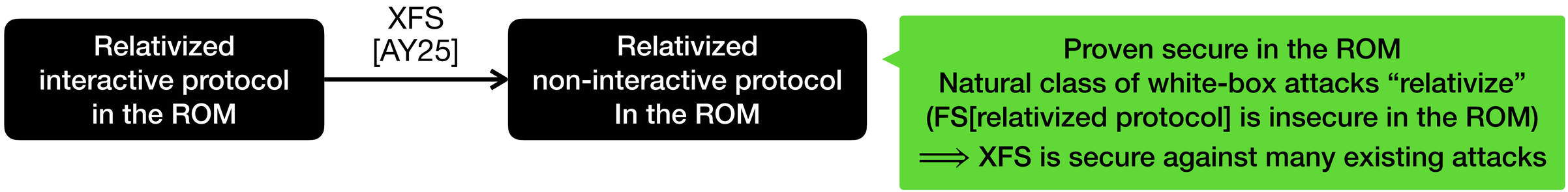
Insights into Fiat-Shamir



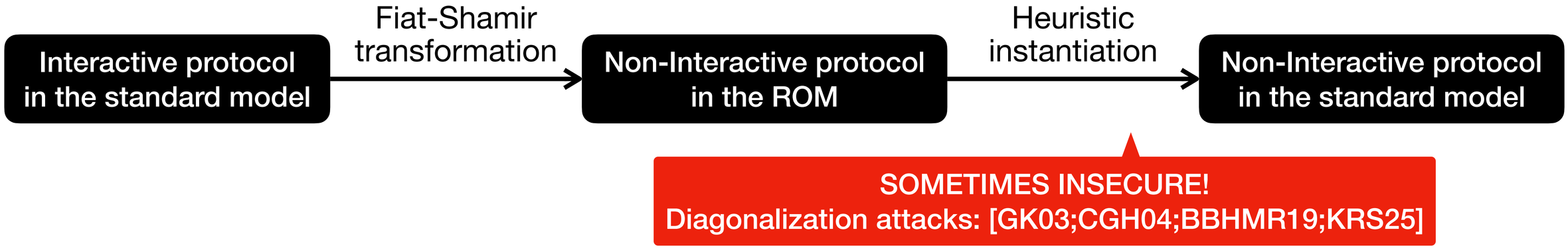


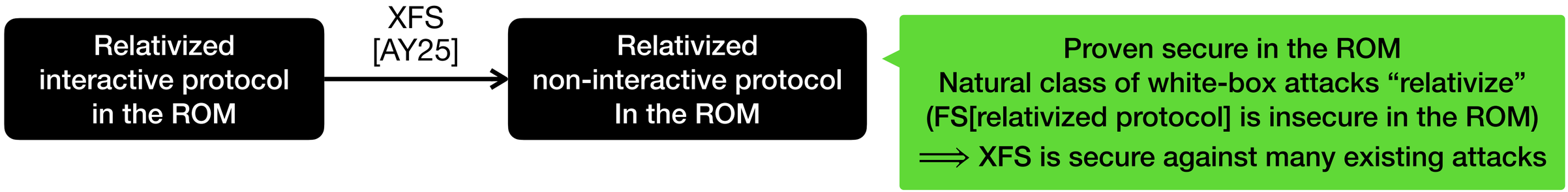
Insights into Fiat-Shamir





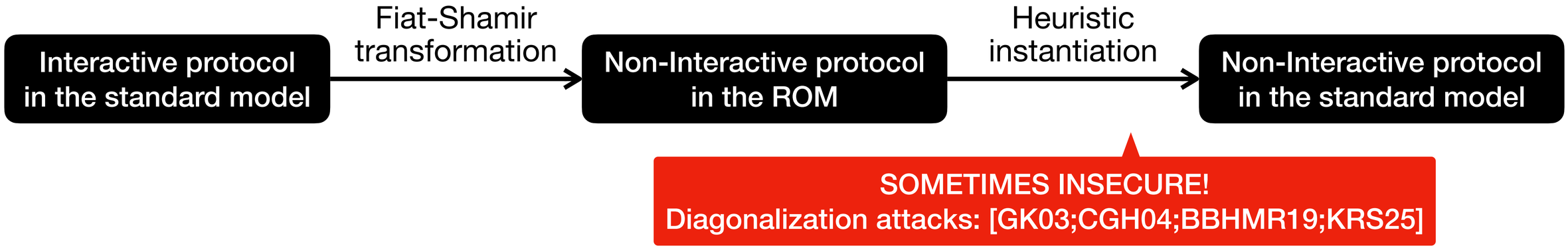
Insights into Fiat-Shamir

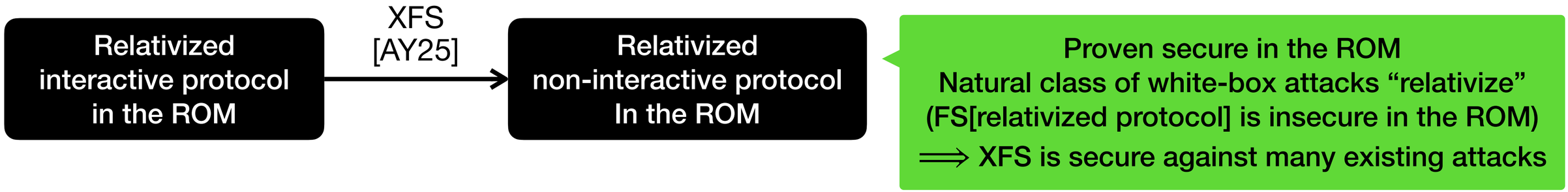




Is Fiat-Shamir transformation secure in other oracle models? LDROM? AROM?

Insights into Fiat-Shamir





Is Fiat-Shamir transformation secure in other oracle models? LDROM? AROM?

Thank you!