On Statistically Secure Obfuscation with Approximate Correctness

Zvika Brakerski[1] Christina Brzuska[2] **Nils Fleischhacker**[3]

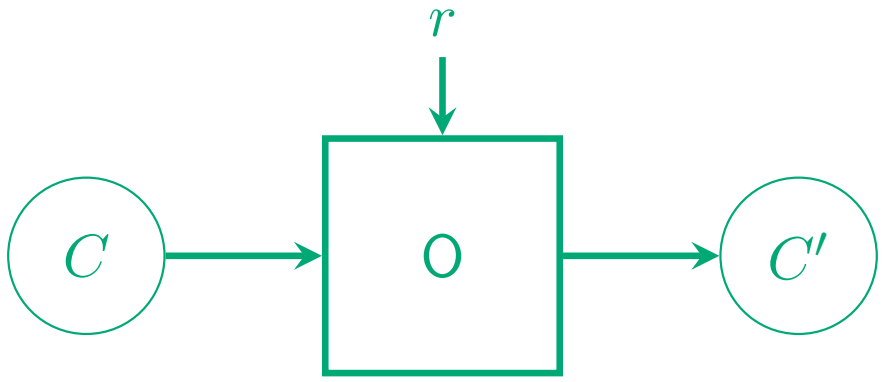
[1]Weizmann Institute of Science

[2]Technical University Hamburg

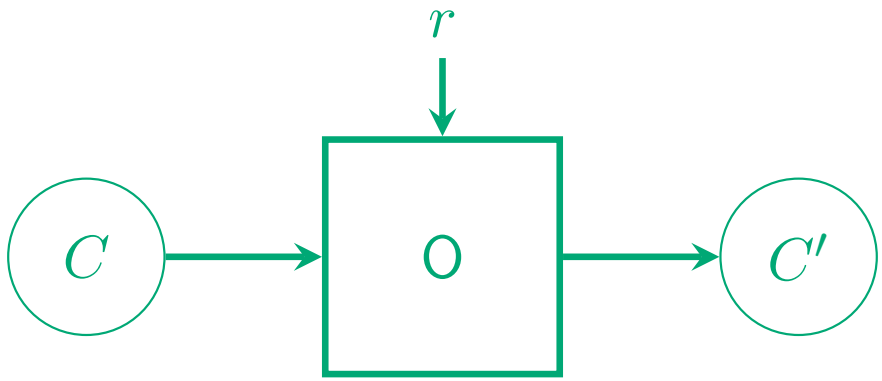
[3]Saarland University

August 15, 2016

Statistically Secure Obfuscation



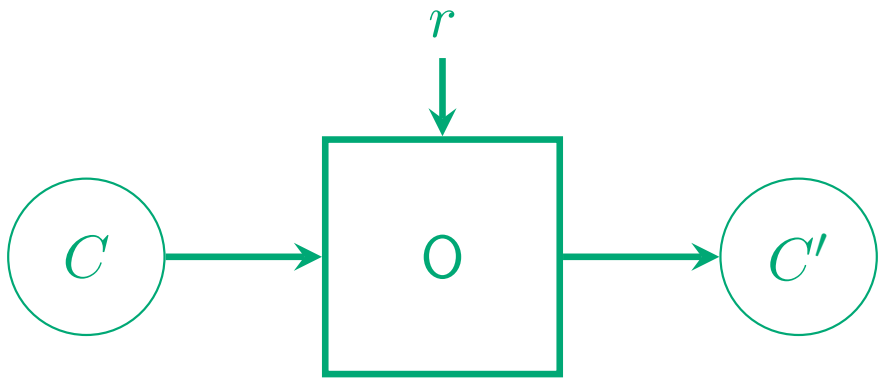
Statistically Secure Obfuscation



- **Perfect Correctness:** For any circuit C

$$\forall x : C'(x) = C(x)$$

Statistically Secure Obfuscation



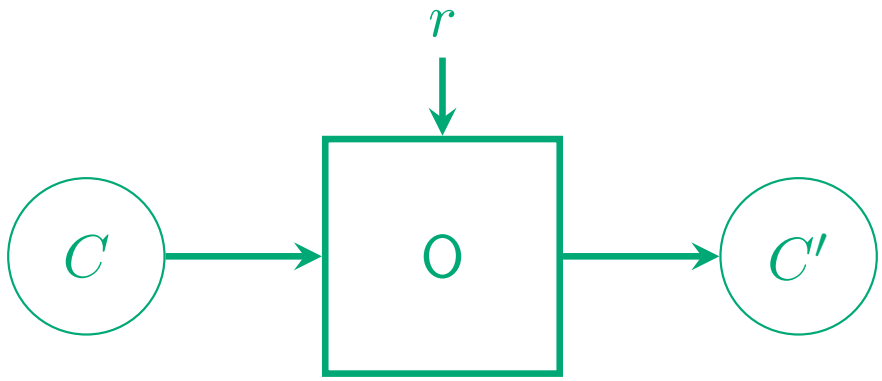
- **Perfect Correctness:** For any circuit C

$$\forall x : C'(x) = C(x)$$

- $(1-\epsilon)$-**Approximate Correctness:** For any circuit C,

$$\Pr_{r,x}\left[C'(x) = C(x)\right] \geq 1 - \epsilon(n)$$

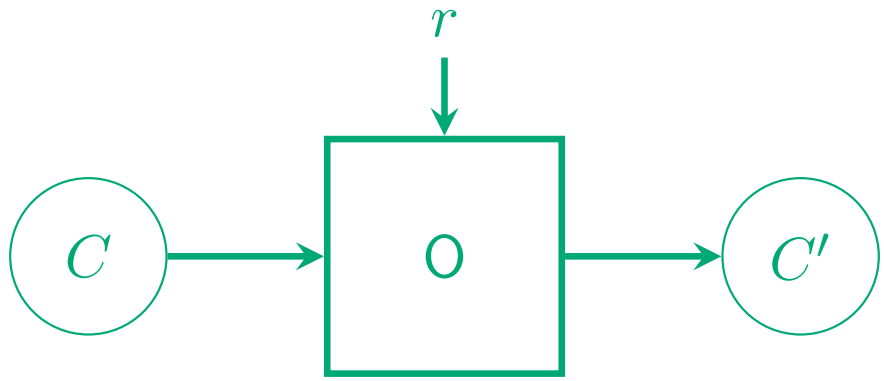
Statistically Secure Obfuscation



- **Indistinguishability Obfuscator:** For any pair of circuits, such that $C_1 \equiv C_2$ and $|C_1| = |C_2|$

$$\mathsf{SD}(\mathsf{O}(C_1), \mathsf{O}(C_2)) \leq \mathsf{negl}(n)$$

Statistically Secure Obfuscation



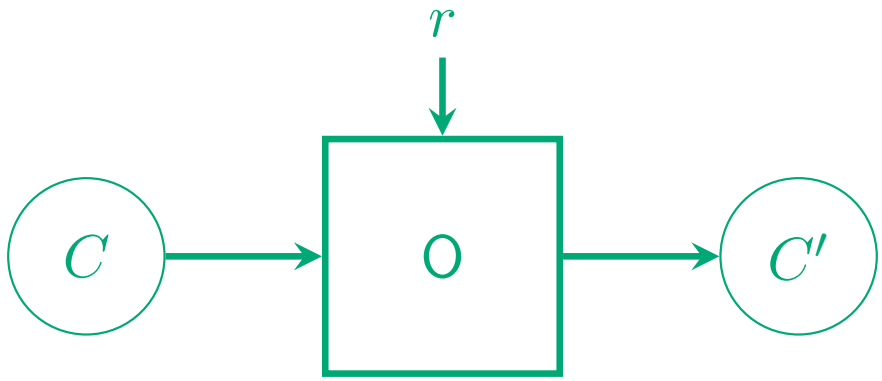
- **Indistinguishability Obfuscator:** For any pair of circuits, such that $C_1 \equiv C_2$ and $|C_1| = |C_2|$

$$\mathsf{SD}(\mathsf{O}(C_1), \mathsf{O}(C_2)) \leq \mathsf{negl}(n)$$

- $(1-\delta)$-**Correlation Obfuscator:** For any pair of circuits, such that $C_1 \equiv C_2$ and $|C_1| = |C_2|$

$$\mathsf{SD}(\mathsf{O}(C_1), \mathsf{O}(C_2)) \leq \delta(n)$$

Statistically Secure Obfuscation



- **Indistinguishability Obfuscator:** For any pair of circuits, such that $C_1 \equiv C_2$ and $|C_1| = |C_2|$

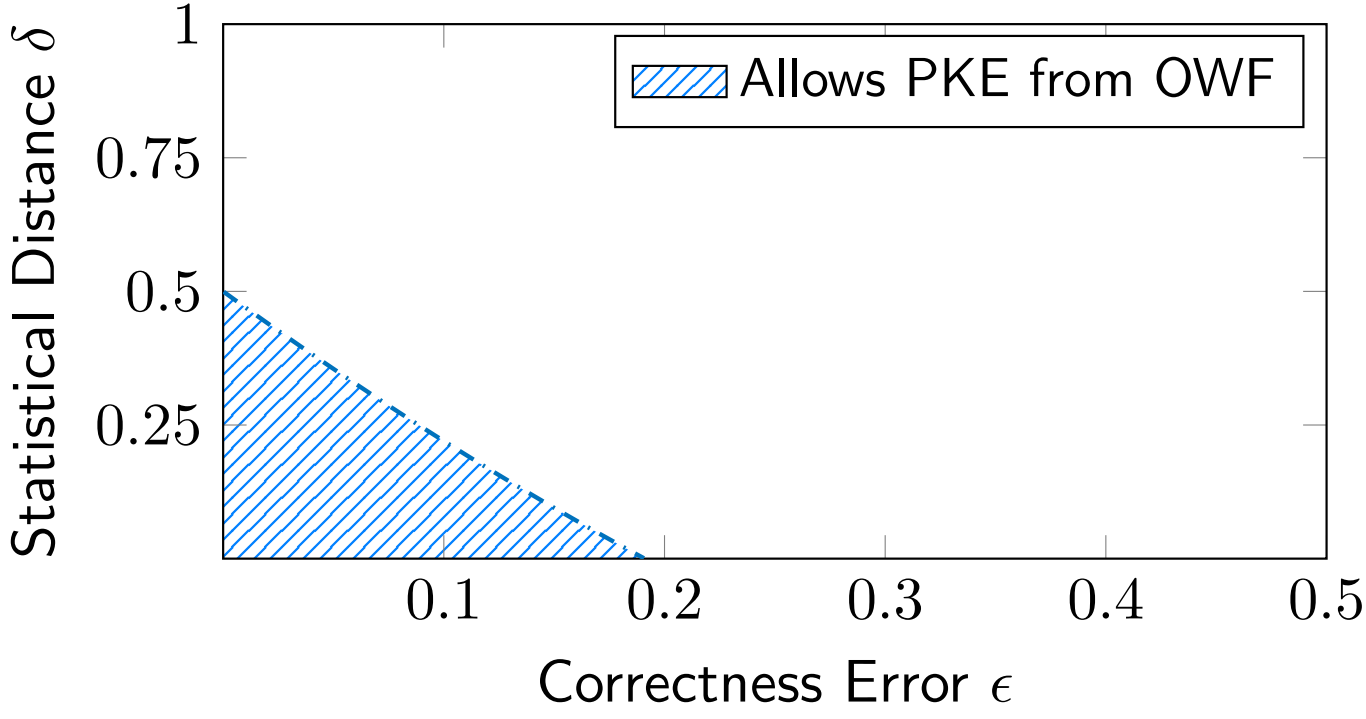
$$\mathsf{SD}(\mathsf{O}(C_1), \mathsf{O}(C_2)) \leq \mathsf{negl}(n)$$

- $(1-\delta)$-**Correlation Obfuscator:** For any pair of circuits, such that $C_1 \equiv C_2$ and $|C_1| = |C_2|$

$$\mathsf{SD}(\mathsf{O}(C_1), \mathsf{O}(C_2)) \leq \delta(n)$$

Why Do We Even Care About Approximate Correctness?

Because approximate obfuscation is useful!
[MMNPs16,SW14,Hol06]



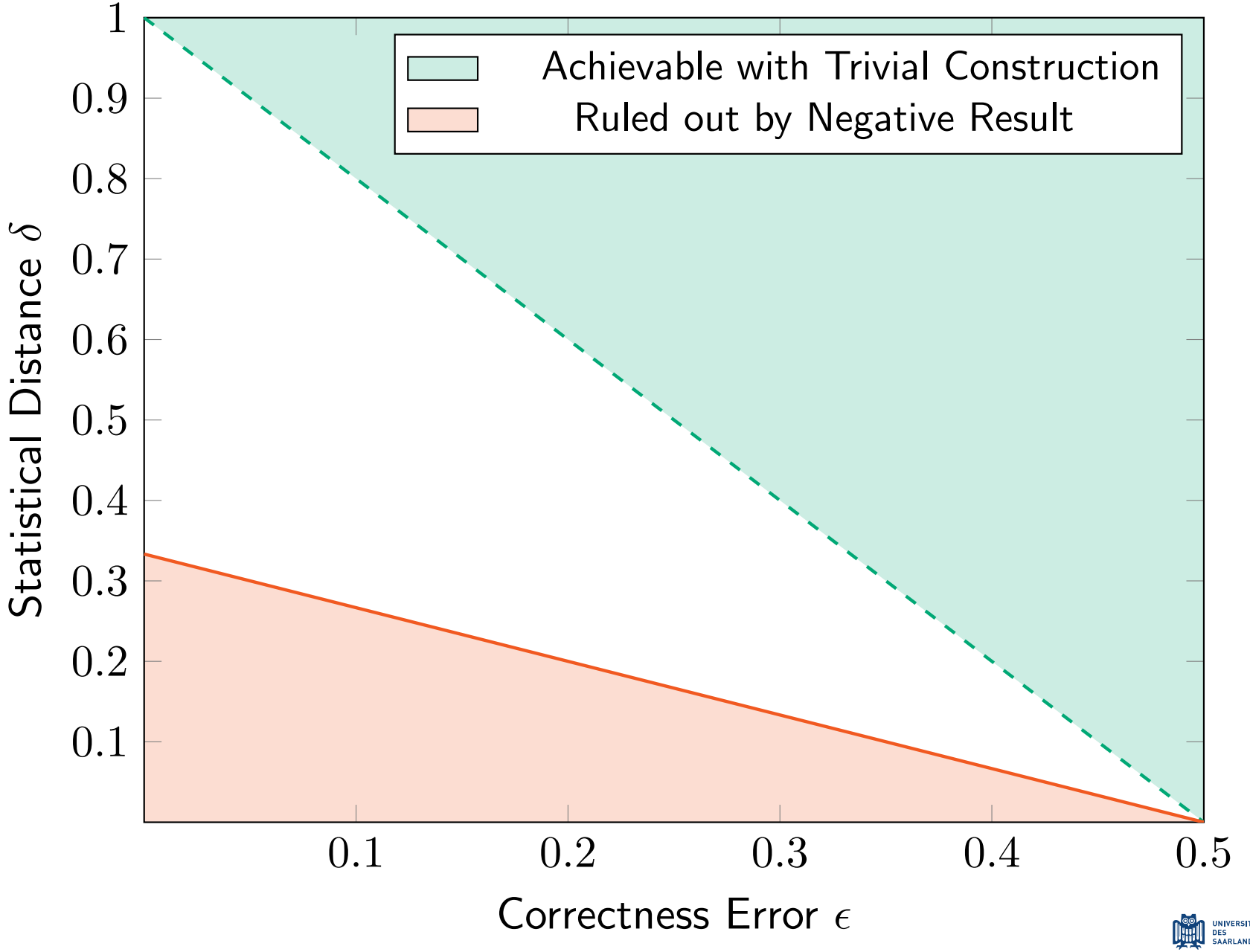
Main Result

- If statistically secure, approximately correct iO (saiO) exists, then either one-way functions do not exist, or NP $\subseteq$ AM $\cap$ coAM.

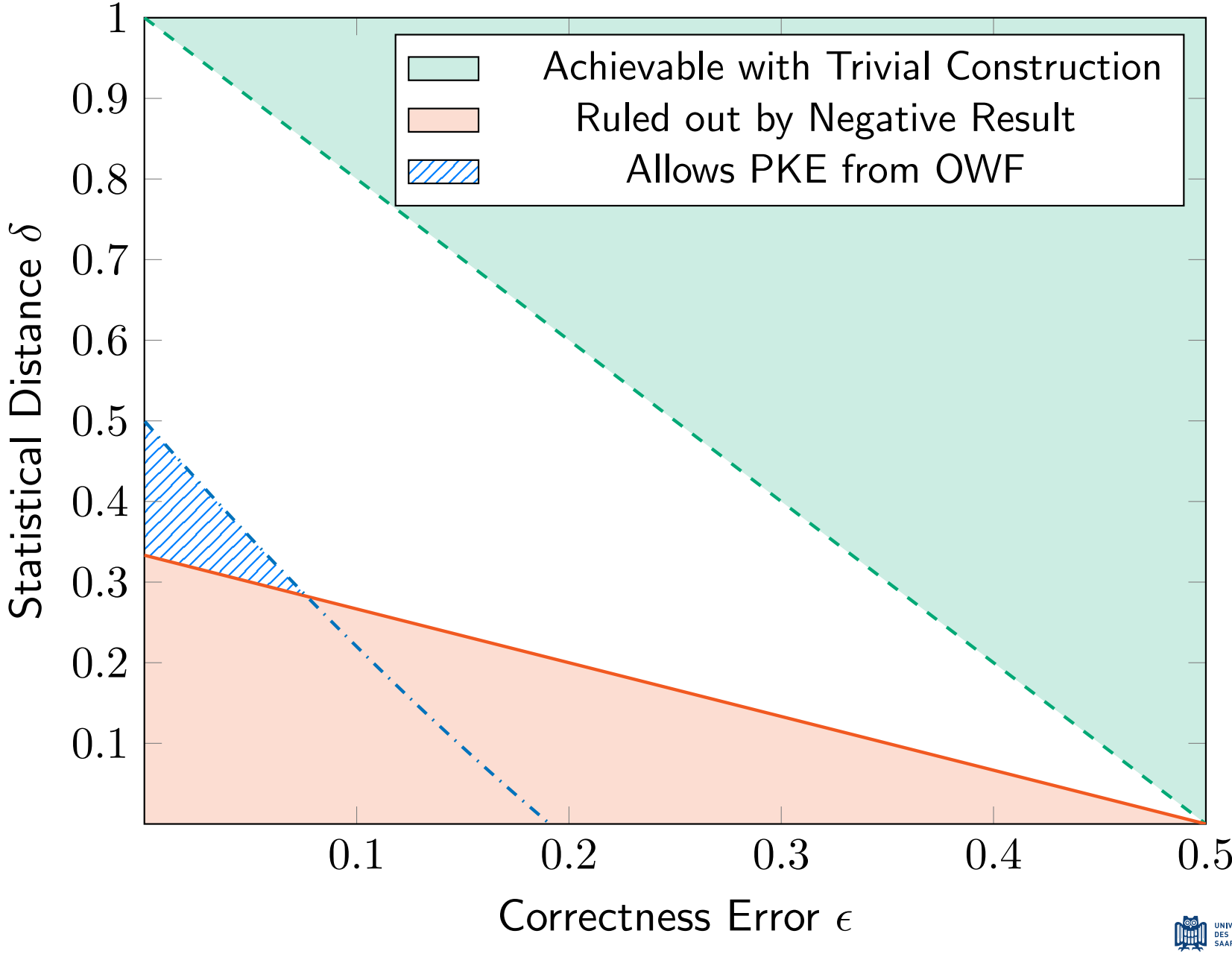
- **More Generally:** If $(1-\delta)$-statistically secure, $(1-\epsilon)$-approximately correct correlation obfuscation (sacO) exists with $\delta(n) \leq \frac{1}{3} - \frac{2}{3}\epsilon(n) - \frac{1}{\mathsf{poly}(n)}$, then either one-way functions do not exist, or NP $\subseteq$ AM $\cap$ coAM.

- For very weak parameters, a trivial construction of sacO exists with $\delta(n) = 2\epsilon(n)$.

The Landscape of Correlation Obfuscation



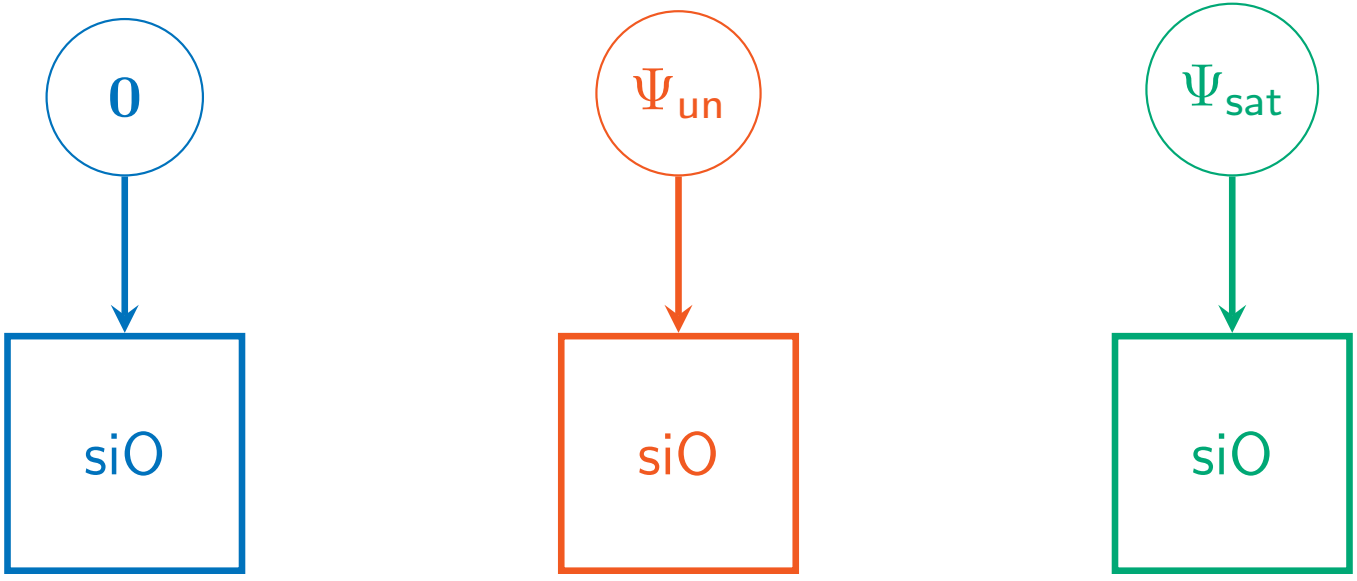
The Landscape of Correlation Obfuscation



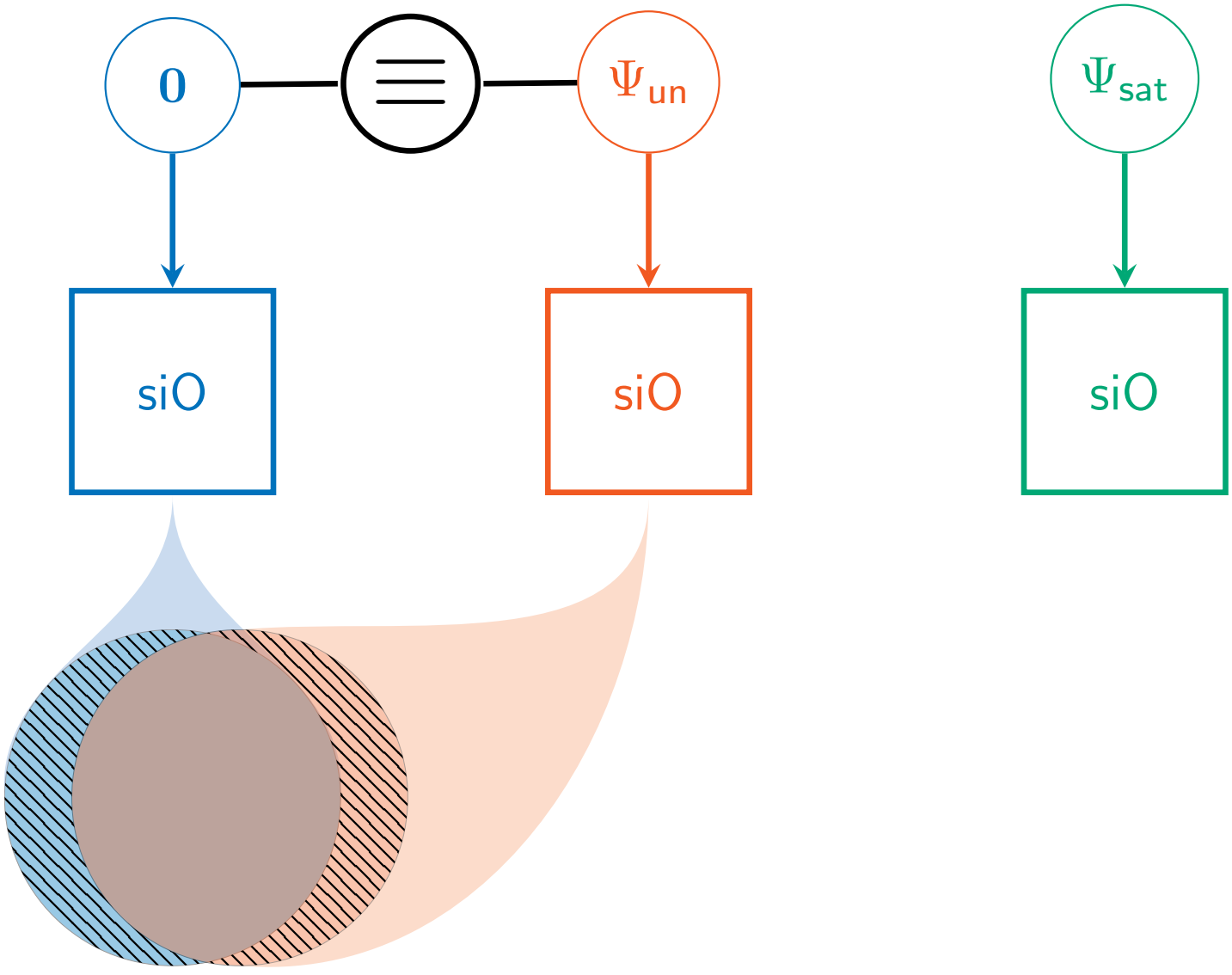
Impossibility of Perfect Correctness [GR07]

Impossibility of Perfect Correctness [GR07]

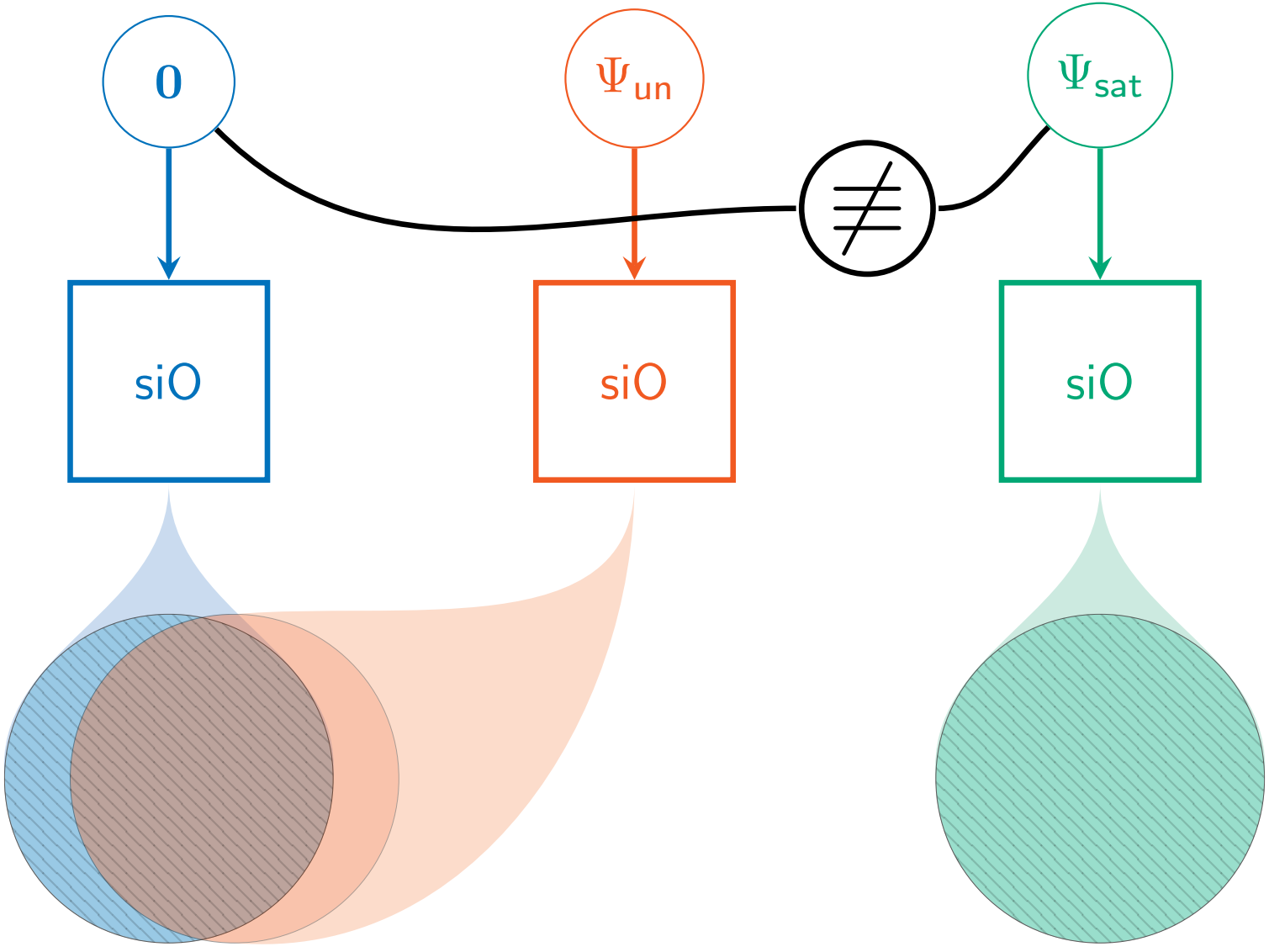
Impossibility of Perfect Correctness [GR07]



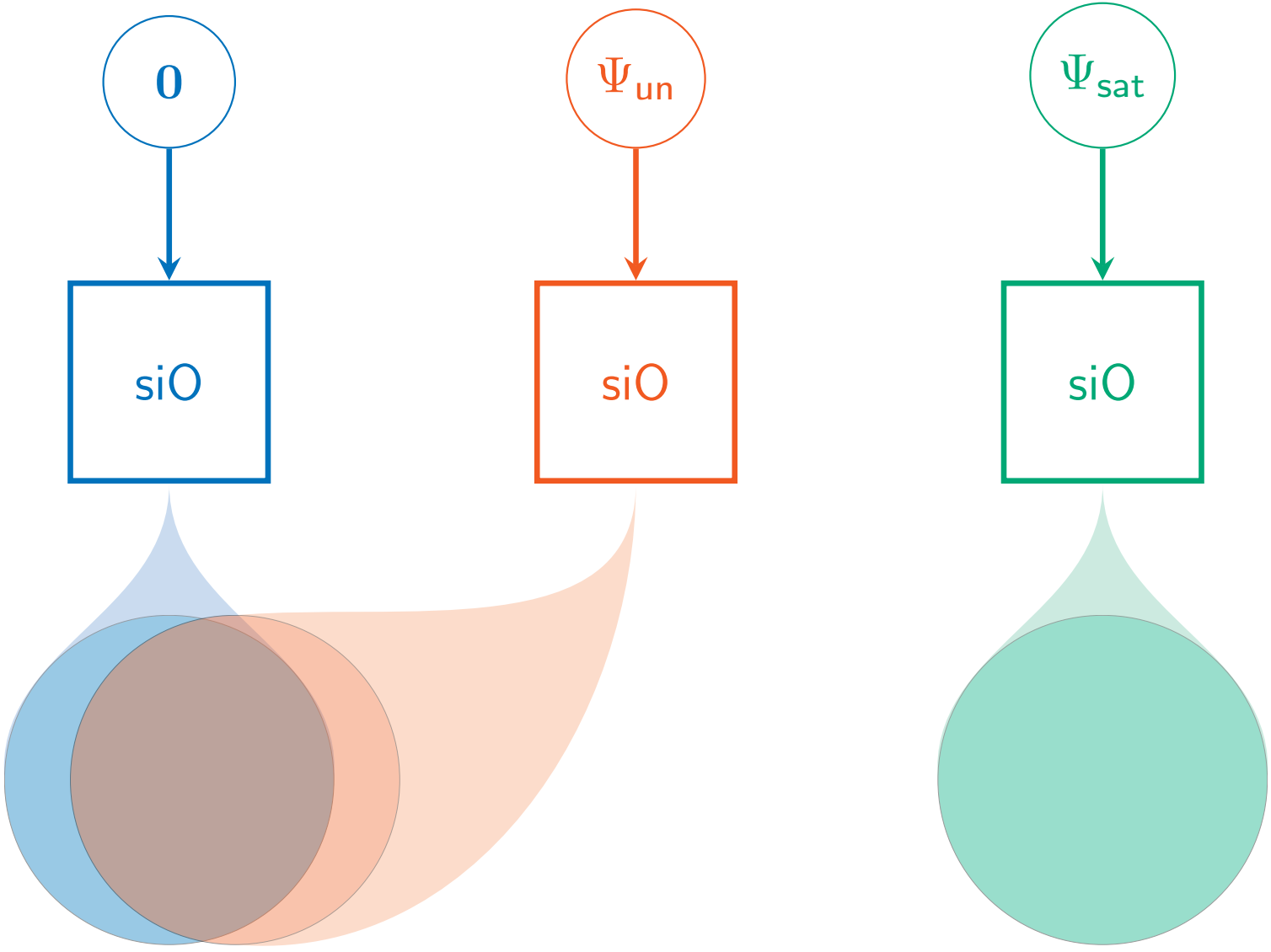
Impossibility of Perfect Correctness [GR07]



Impossibility of Perfect Correctness [GR07]

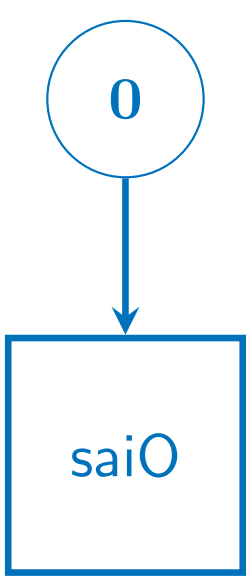


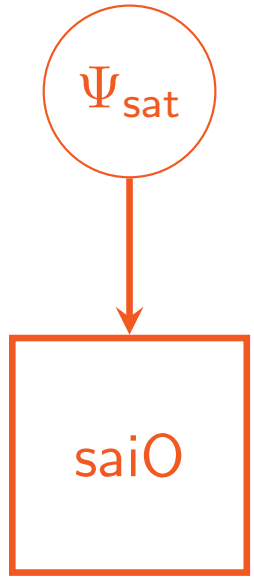
Impossibility of Perfect Correctness [GR07]



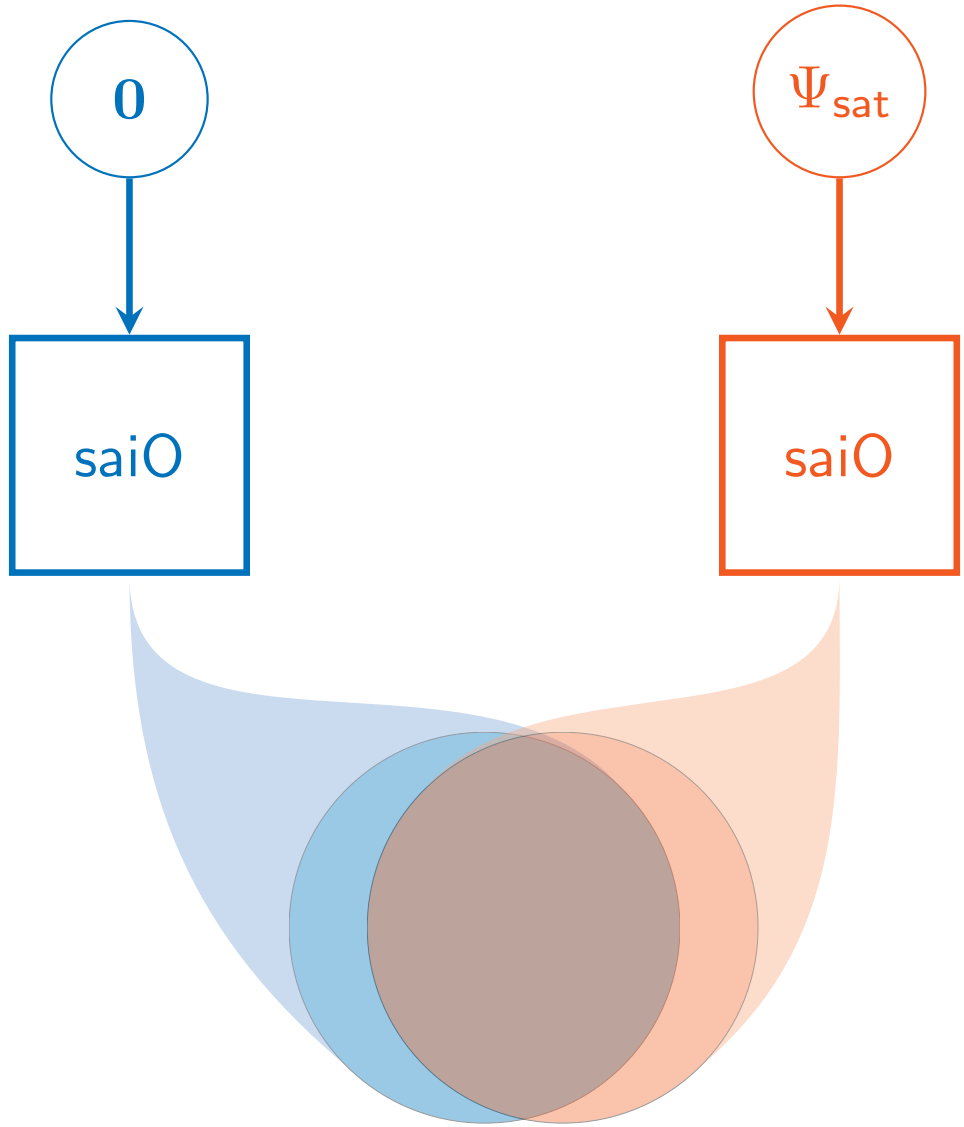
$$\text{GapSD} \in \text{AM} \cap \text{coAM} \implies \text{NP} \subseteq \text{AM} \cap \text{coAM}$$

Why Does the Approach Fail in the Approximate Case?

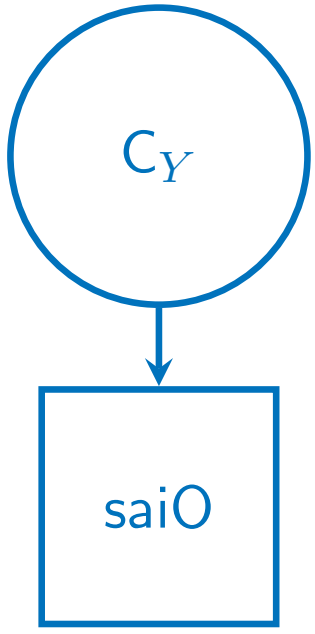


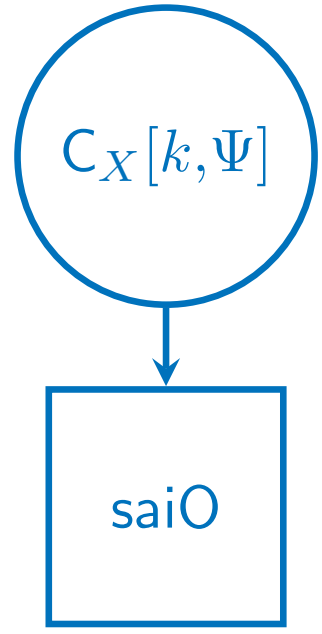


Why Does the Approach Fail in the Approximate Case?

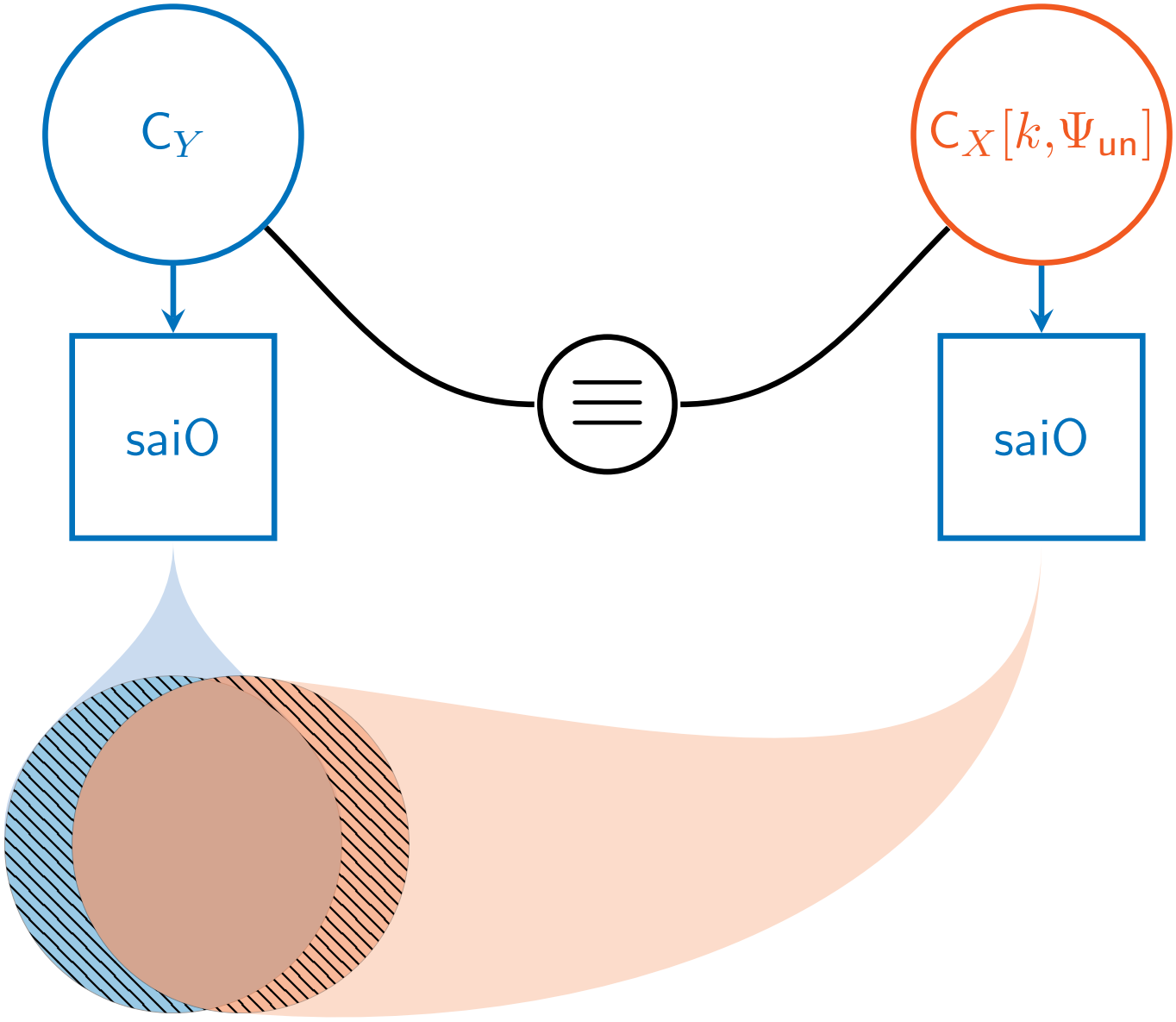


Overview of Our Approach

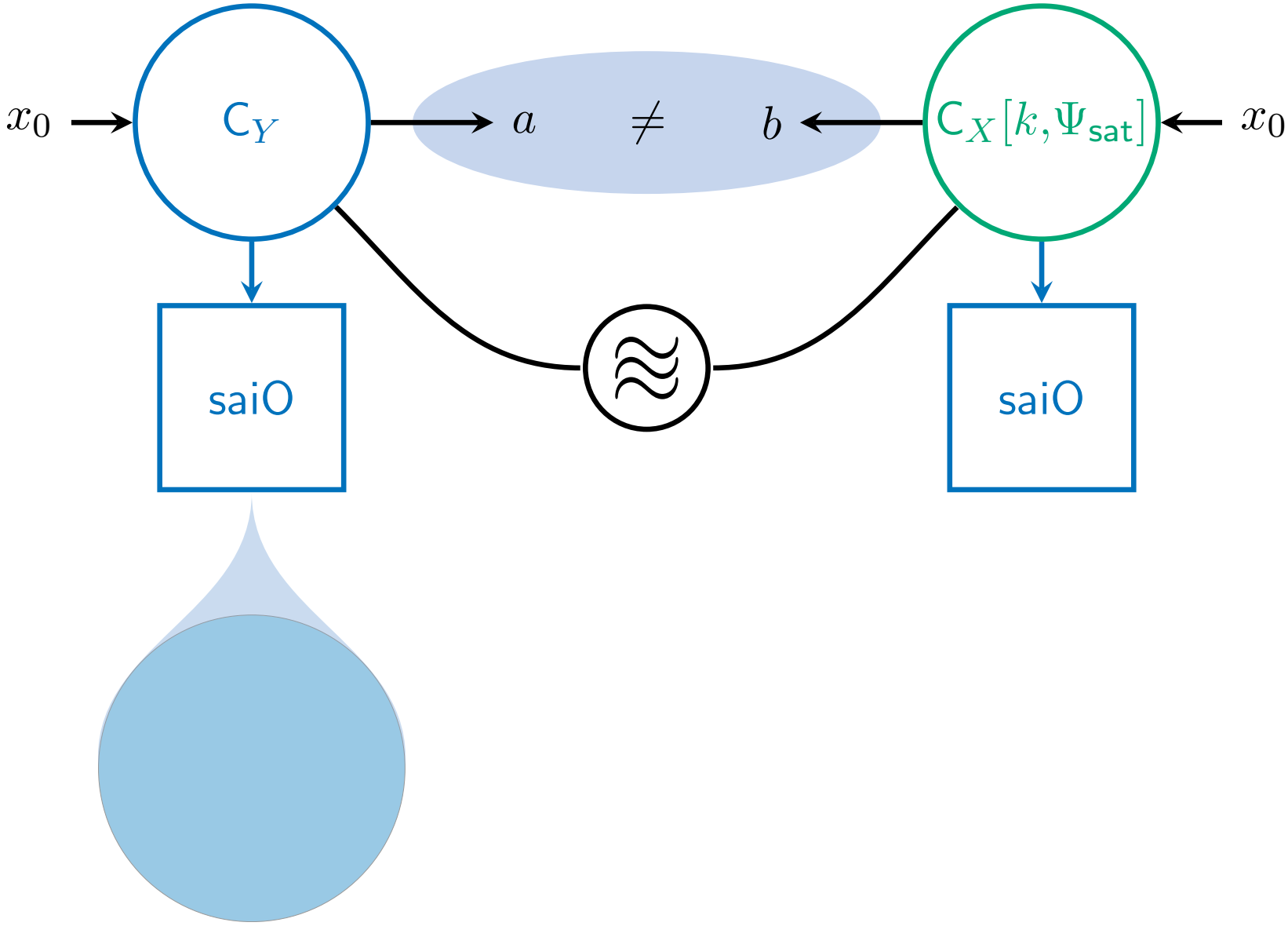




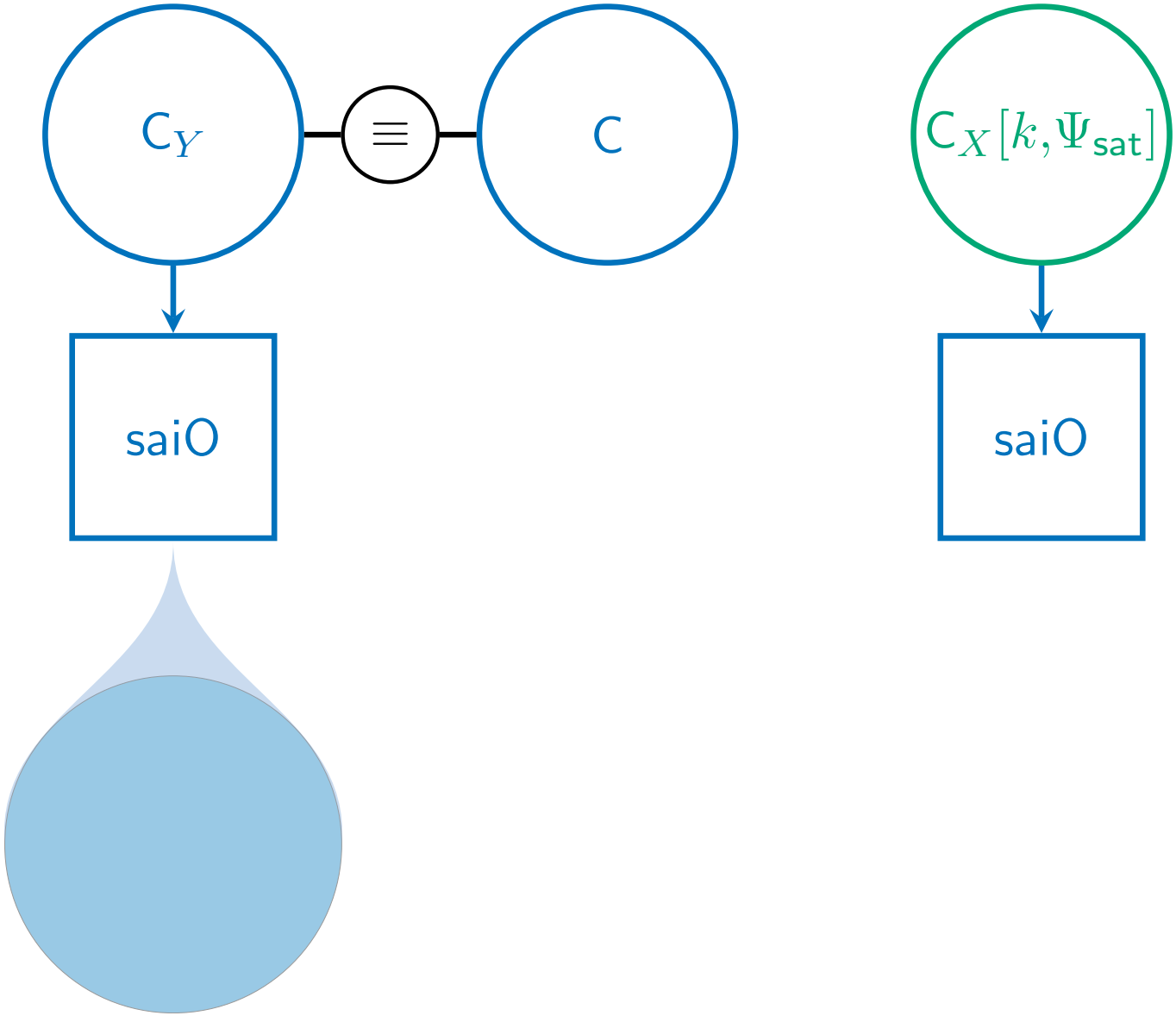
Overview of Our Approach



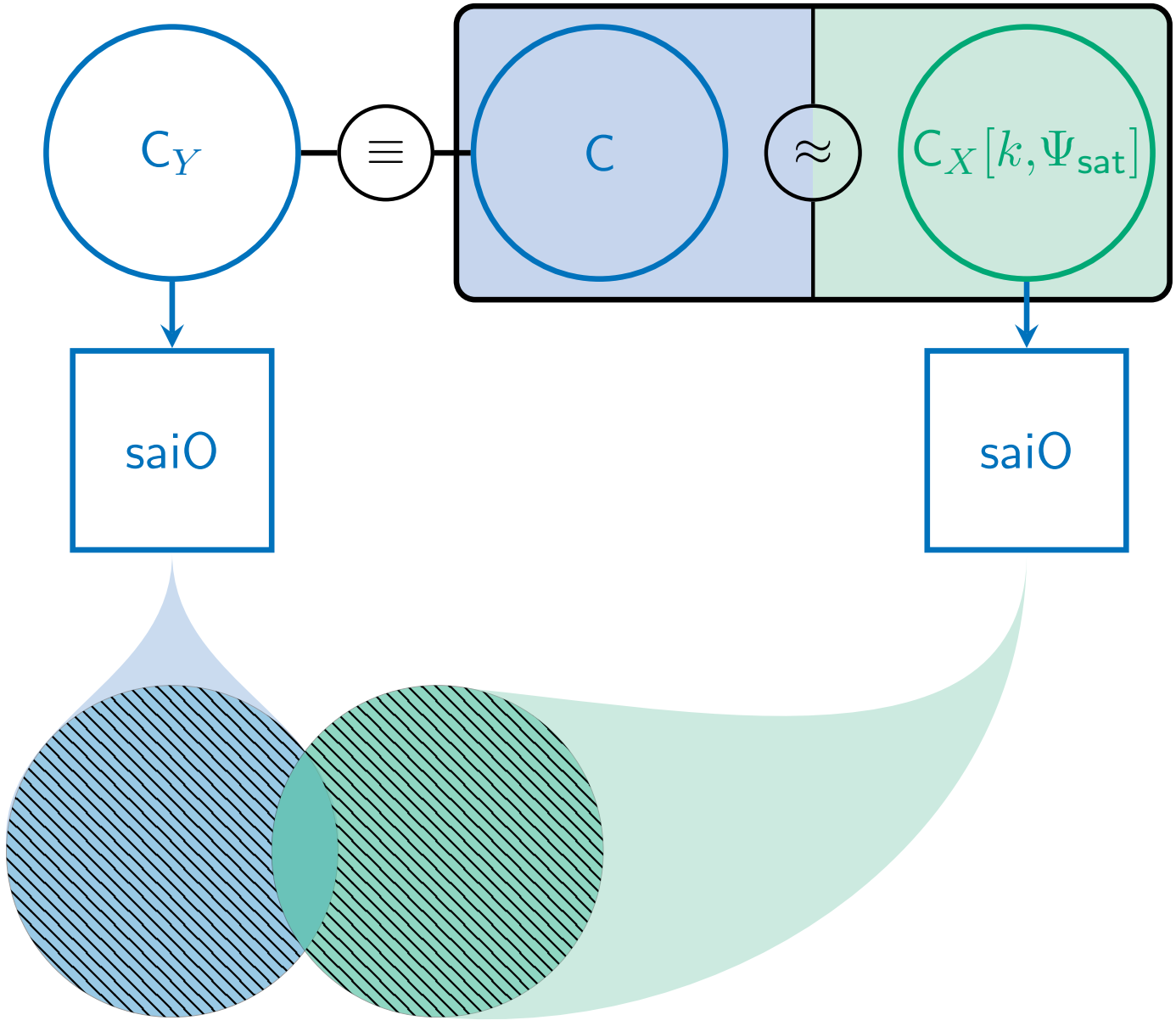
Overview of Our Approach



Overview of Our Approach



Overview of Our Approach



Puncturable Pseudorandom Functions [BW13,BGI14,KPTZ13]

$b \leftarrow \mathsf{PRF}(k, x) \qquad k^* \leftarrow \mathsf{Puncture}(k, x_0)$

Puncturable Pseudorandom Functions [BW13,BGI14,KPTZ13]

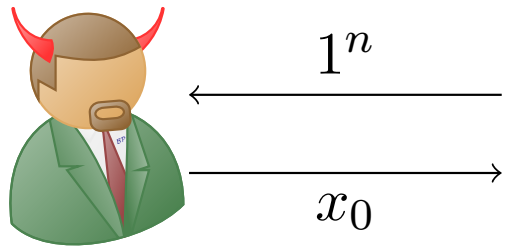
$$b \leftarrow \mathsf{PRF}(k, x) \qquad k^* \leftarrow \mathsf{Puncture}(k, x_0)$$

- **Functionality Preserved Under Puncturing:**
  For all $x \neq x_0$, $\mathsf{PRF}(k^*, x) = \mathsf{PRF}(k, x)$

Puncturable Pseudorandom Functions [BW13,BGI14,KPTZ13]

$$b \leftarrow \mathsf{PRF}(k, x) \qquad k^* \leftarrow \mathsf{Puncture}(k, x_0)$$

- **Functionality Preserved Under Puncturing:**
  For all $x \neq x_0$, $\mathsf{PRF}(k^*, x) = \mathsf{PRF}(k, x)$
- **Security:**

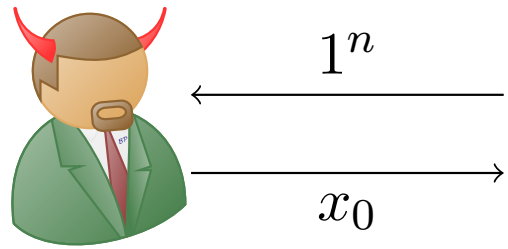


$$k \leftarrow_{\$} \{0,1\}^n, k^* = \mathsf{Puncture}(k, x_0)$$

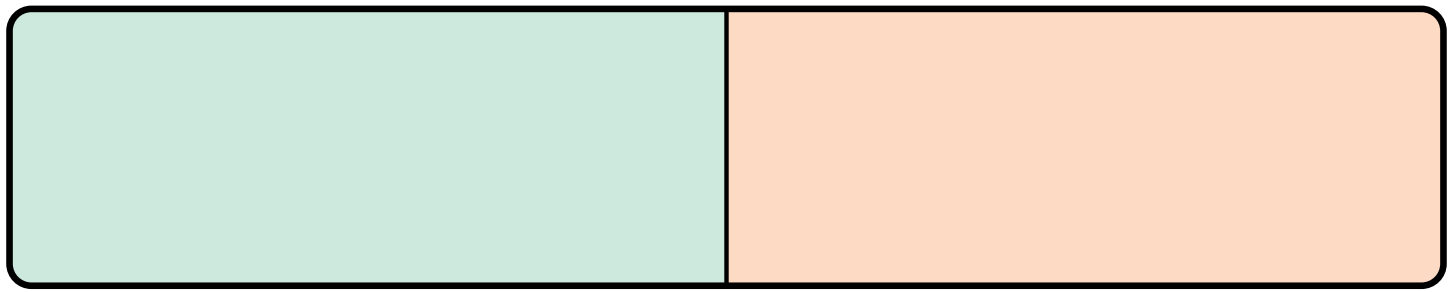
Puncturable Pseudorandom Functions [BW13,BGI14,KPTZ13]

$$b \leftarrow \mathsf{PRF}(k, x) \qquad k^* \leftarrow \mathsf{Puncture}(k, x_0)$$

- **Functionality Preserved Under Puncturing:**
  For all $x \neq x_0$, $\mathsf{PRF}(k^*, x) = \mathsf{PRF}(k, x)$
- **Security:**



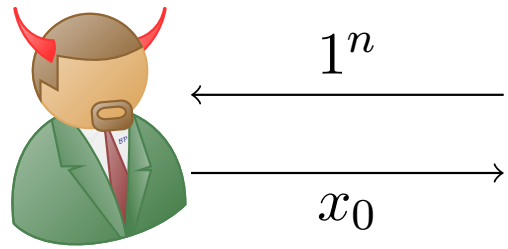
$$k \leftarrow_{\$} \{0,1\}^n, k^* = \mathsf{Puncture}(k, x_0)$$



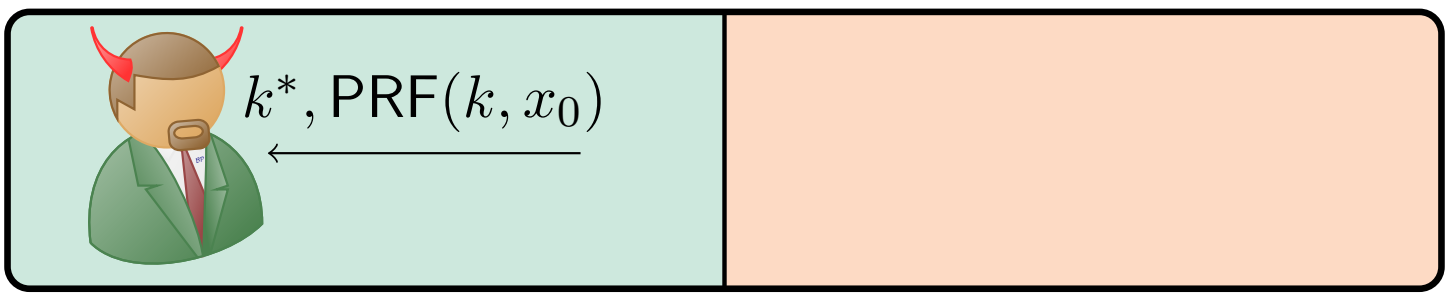
Puncturable Pseudorandom Functions [BW13,BGI14,KPTZ13]

$$b \leftarrow \mathsf{PRF}(k, x) \qquad k^* \leftarrow \mathsf{Puncture}(k, x_0)$$

- **Functionality Preserved Under Puncturing:**
  For all $x \neq x_0$, $\mathsf{PRF}(k^*, x) = \mathsf{PRF}(k, x)$
- **Security:**



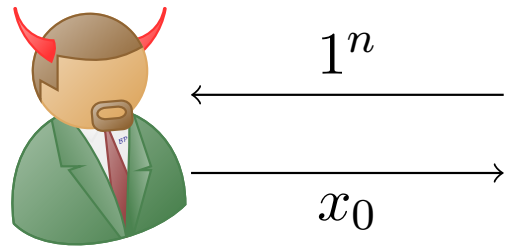
$$k \leftarrow_{\$} \{0,1\}^n, k^* = \mathsf{Puncture}(k, x_0)$$



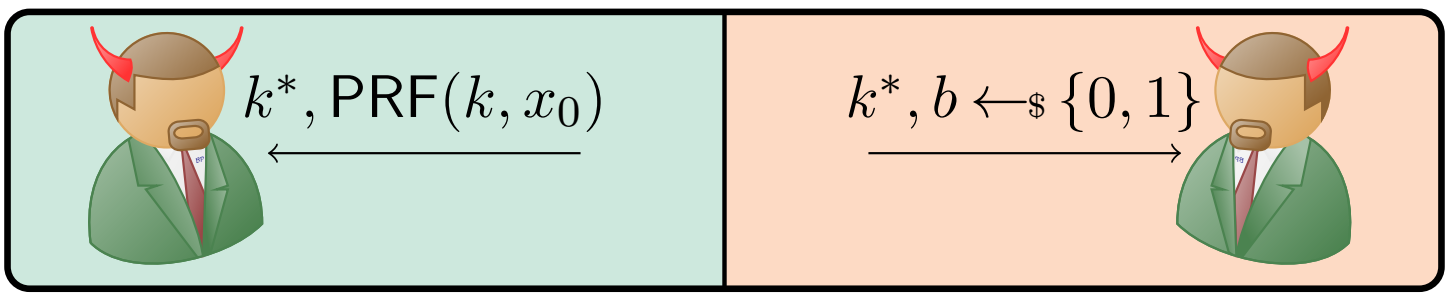
Puncturable Pseudorandom Functions [BW13,BGI14,KPTZ13]

$$b \leftarrow \mathsf{PRF}(k, x) \qquad k^* \leftarrow \mathsf{Puncture}(k, x_0)$$

- **Functionality Preserved Under Puncturing:**
  For all $x \neq x_0$, $\mathsf{PRF}(k^*, x) = \mathsf{PRF}(k, x)$
- **Security:**



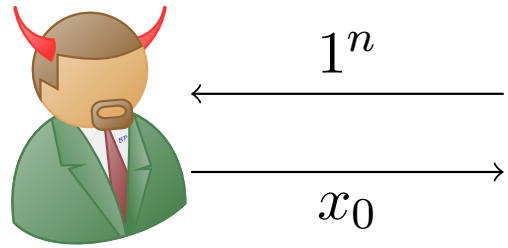
$$k \leftarrow_{\$} \{0,1\}^n, k^* = \mathsf{Puncture}(k, x_0)$$



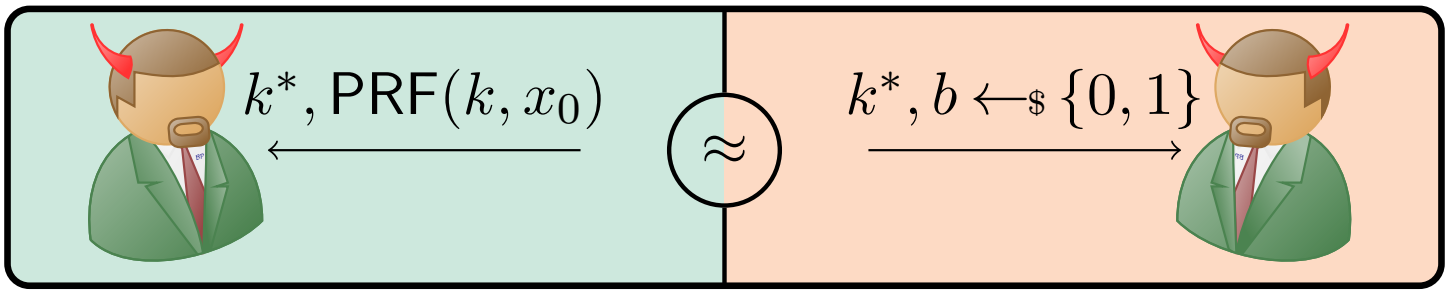
Puncturable Pseudorandom Functions [BW13,BGI14,KPTZ13]

$$b \leftarrow \mathsf{PRF}(k, x) \qquad k^* \leftarrow \mathsf{Puncture}(k, x_0)$$

- **Functionality Preserved Under Puncturing:**
  For all $x \neq x_0$, $\mathsf{PRF}(k^*, x) = \mathsf{PRF}(k, x)$
- **Security:**



$$k \leftarrow_{\$} \{0,1\}^n, k^* = \mathsf{Puncture}(k, x_0)$$



Enforcing Large Statistical Distance

$\mathsf{C}[k^*, x_0, b](x)$

---

if $x = x_0$
  return b
else
  return $\mathsf{PRF}(k^*, x)$

Let C' denote $\mathsf{saiO}(\mathsf{C}[k^*, x_0, b])$.

Enforcing Large Statistical Distance

$\mathsf{C}[k^*, x_0, b](x)$

---

if $x = x_0$

  return b

else

  return $\mathsf{PRF}(k^*, x)$

Let C' denote $\mathsf{saiO}(\mathsf{C}[k^*, x_0, b])$.

$b = \mathsf{PRF}(k, x_0) \oplus 1$

Enforcing Large Statistical Distance

$\mathsf{C}[k^*, x_0, b](x)$

---

if $x = x_0$
  return b
else
  return $\mathsf{PRF}(k^*, x)$

Let C' denote $\mathsf{saiO}(\mathsf{C}[k^*, x_0, b])$.

$b = \mathsf{PRF}(k, x_0) \oplus 1$	$b = \mathsf{PRF}(k, x_0)$

Enforcing Large Statistical Distance

$\mathsf{C}[k^*, x_0, b](x)$

if $x = x_0$
  return b
else
  return $\mathsf{PRF}(k^*, x)$

Let C' denote $\mathsf{saiO}(\mathsf{C}[k^*, x_0, b])$.

$b = \mathsf{PRF}(k, x_0) \oplus 1$	$b = \mathsf{PRF}(k, x_0)$ $\mathsf{C}[k^*, x_0, b] \equiv \mathsf{PRF}(k, \cdot)$

Enforcing Large Statistical Distance

$\mathsf{C}[k^*, x_0, b](x)$

if $x = x_0$
  return b
else
  return $\mathsf{PRF}(k^*, x)$

Let C' denote $\mathsf{saiO}(\mathsf{C}[k^*, x_0, b])$.

$b = \mathsf{PRF}(k, x_0) \oplus 1$

$\mathsf{C}_{\mathsf{PRF}} \leftarrow \mathsf{saiO}(\mathsf{PRF}(k, \cdot))$
$\Pr[\mathsf{C}_{\mathsf{PRF}}(x_0) = b] \geq 1 - \epsilon$

$b = \mathsf{PRF}(k, x_0)$

$\mathsf{C}[k^*, x_0, b] \equiv \mathsf{PRF}(k, \cdot)$

$\Downarrow$

$\Pr[\mathsf{C}'(x_0) = b] \gtrsim 1 - \epsilon$

Enforcing Large Statistical Distance

$\mathsf{C}[k^*, x_0, b](x)$

if $x = x_0$
  return b
else
  return $\mathsf{PRF}(k^*, x)$

Let C' denote $\mathsf{saiO}(\mathsf{C}[k^*, x_0, b])$.

$b = \mathsf{PRF}(k, x_0) \oplus 1$

$\Pr[\mathsf{C}'(x_0) = b] \gtrsim 1 - \epsilon$

PRF security $\Longleftarrow$

$b = \mathsf{PRF}(k, x_0)$

$\mathsf{C}[k^*, x_0, b] \equiv \mathsf{PRF}(k, \cdot)$

$\Downarrow$

$\Pr[\mathsf{C}'(x_0) = b] \gtrsim 1 - \epsilon$

Enforcing Large Statistical Distance

$\mathsf{C}[k^*, x_0, b](x)$

if $x = x_0$
  return b
else
  return $\mathsf{PRF}(k^*, x)$

Let C' denote $\mathsf{saiO}(\mathsf{C}[k^*, x_0, b])$.

b

$$\begin{aligned} & \Pr[\mathsf{C}_{\mathsf{PRF}}(x_0) = \mathsf{PRF}(k, x_0)] \geq 1 - \epsilon \\ \wedge \quad & \Pr[\mathsf{C}'(x_0) \neq \mathsf{PRF}(k, x_0)] \gtrsim 1 - \epsilon \\ \Longrightarrow \quad & \mathsf{SD}(\mathsf{C}_{\mathsf{PRF}}, C) \gtrsim 1 - 2\epsilon \end{aligned}$$

$, \cdot)$

Pr

$- \epsilon$

Restriction to Unique-SAT

- We restrict our attention to Unique-SAT (USAT)
- USAT is NP hard via a randomized reduction [VV85]
- Combining this with previous results [MX10,BL13] we show that

$$\text{USAT} \in \text{BPP}^{\text{GapSD}} \implies \text{SAT} \in \text{AM} \cap \text{coAM}$$

The Formula-Indexed Circuit

$\mathsf{C}_X[k, s, \Psi](x)$

---

if $\Psi(x \oplus s) = 1$

  return $\mathsf{PRF}(k, x) \oplus 1$

else

  return $\mathsf{PRF}(k, x)$

The Formula-Indexed Circuit

$\mathsf{C}_X[k, s, \Psi](x)$

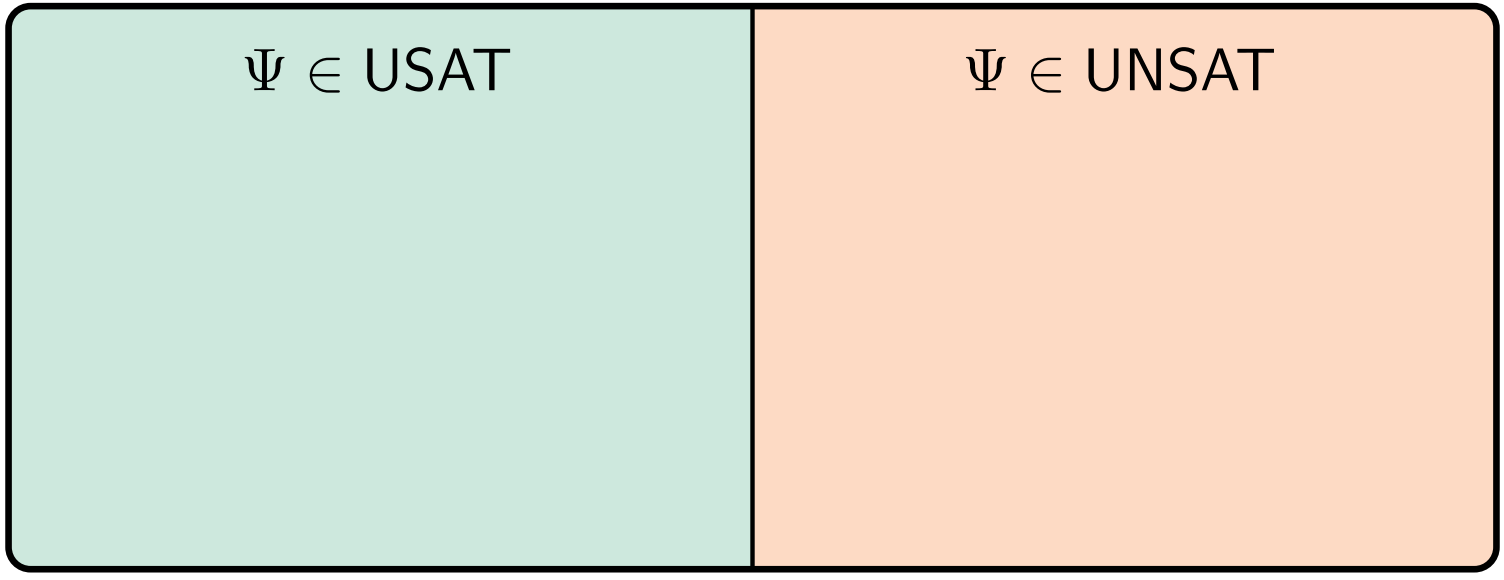
---

if $\Psi(x \oplus s) = 1$

  return $\mathsf{PRF}(k, x) \oplus 1$

else

  return $\mathsf{PRF}(k, x)$



The Formula-Indexed Circuit

$\mathsf{C}_X[k, s, \Psi](x)$

---

if $\Psi(x \oplus s) = 1$
  return $\mathsf{PRF}(k, x) \oplus 1$
else
  return $\mathsf{PRF}(k, x)$

$\Psi \in \mathsf{USAT}$	$\Psi \in \mathsf{UNSAT}$
	$\mathsf{C}_X[k, s, \Psi] \equiv \mathsf{PRF}(k, \cdot)$

The Formula-Indexed Circuit

$\mathsf{C}_X[k, s, \Psi](x)$

---

if $\Psi(x \oplus s) = 1$
  return $\mathsf{PRF}(k, x) \oplus 1$
else
  return $\mathsf{PRF}(k, x)$

$\Psi \in \mathsf{USAT}$	$\Psi \in \mathsf{UNSAT}$
$\mathsf{C}_X[k, s, \Psi] \equiv \mathsf{C}[k^*, x_0, b]$ for $x_0 = x_\psi \oplus s$, $b = \mathsf{PRF}(k, x_0) \oplus 1$	$\mathsf{C}_X[k, s, \Psi] \equiv \mathsf{PRF}(k, \cdot)$

Putting it All Together

$X[\Psi](1^n)$

$k \leftarrow\!\!\$\ \{0,1\}^n$

$s \leftarrow\!\!\$\ \{0,1\}^n$

$C := \mathsf{C}_X[k, s, \Psi]$

$C' \leftarrow\!\!\$\ \mathsf{O}(C)$

return (k, s, C')

$Y(1^n)$

$k \leftarrow\!\!\$\ \{0,1\}^n$

$s \leftarrow\!\!\$\ \{0,1\}^n$

$C := \mathsf{PRF}(k, \cdot)$

$C' \leftarrow\!\!\$\ \mathsf{O}(C)$

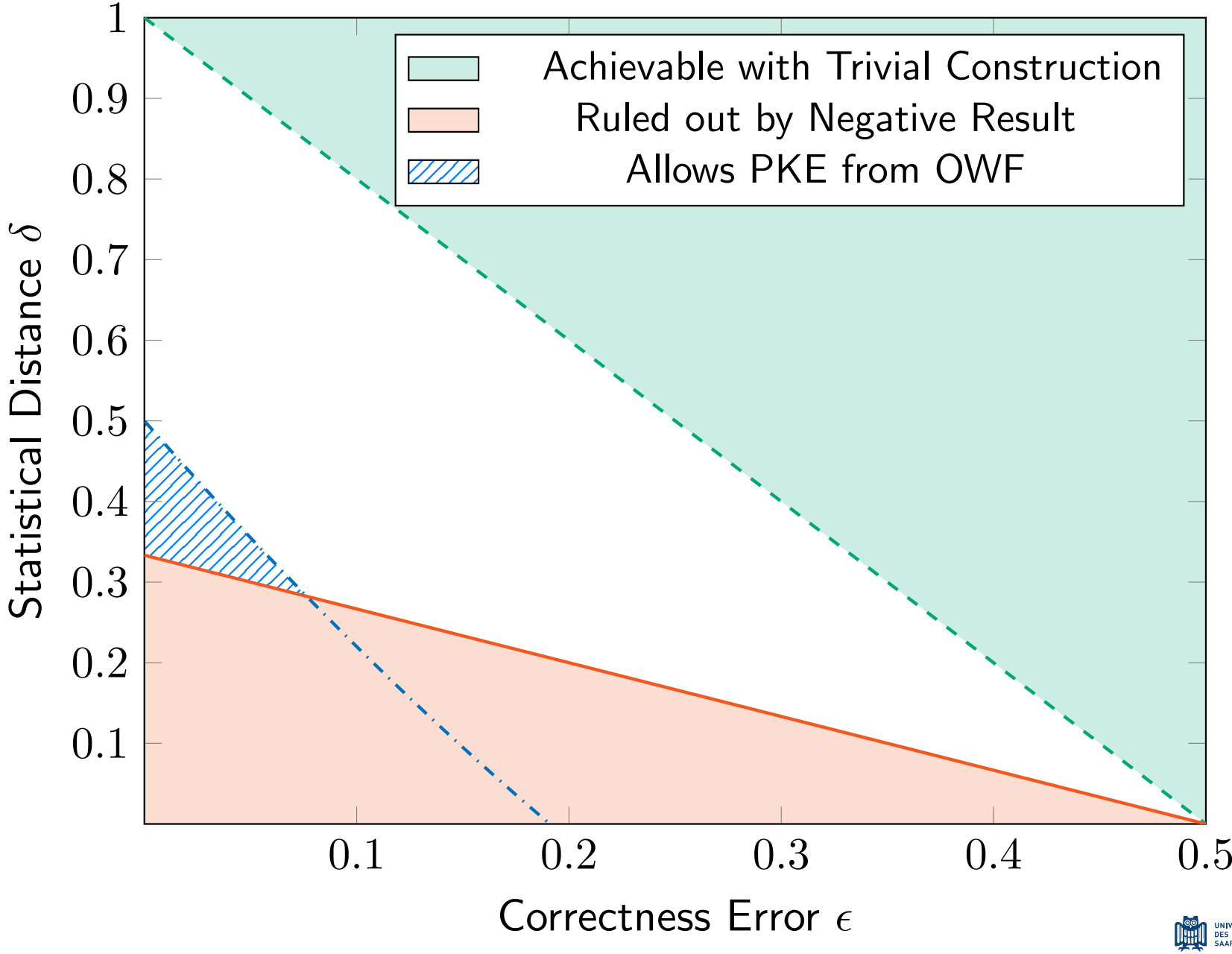
return (k, s, C')

$$\Psi \in \mathsf{UNSAT} \iff \mathsf{SD}(X[\Psi], Y) \leq \mathsf{negl}(n)$$

$$\Psi \in \mathsf{USAT} \iff \mathsf{SD}(X[\Psi], Y) \gtrsim 1 - 2\epsilon$$

- We can therefore decide USAT in $\mathsf{BPP}^{\mathsf{GapSD}}$.
- Thus, if saiO and one-way functions both exist, then $\mathsf{NP} \subseteq \mathsf{AM} \cap \mathsf{coAM}$ and the polynomial hierarchy collapses.

The Landscape of Correlation Obfuscation



Thank You!

Nils Fleischhacker
fleischhacker@cs.uni-saarland.de

I'm looking for a postdoc position.
If you're interested in hiring me, please send me an email.

Full Version: ia.cr/2016/226