Indistinguishability Obfuscation versus Multi-Bit Point Obfuscation with Auxiliary Input

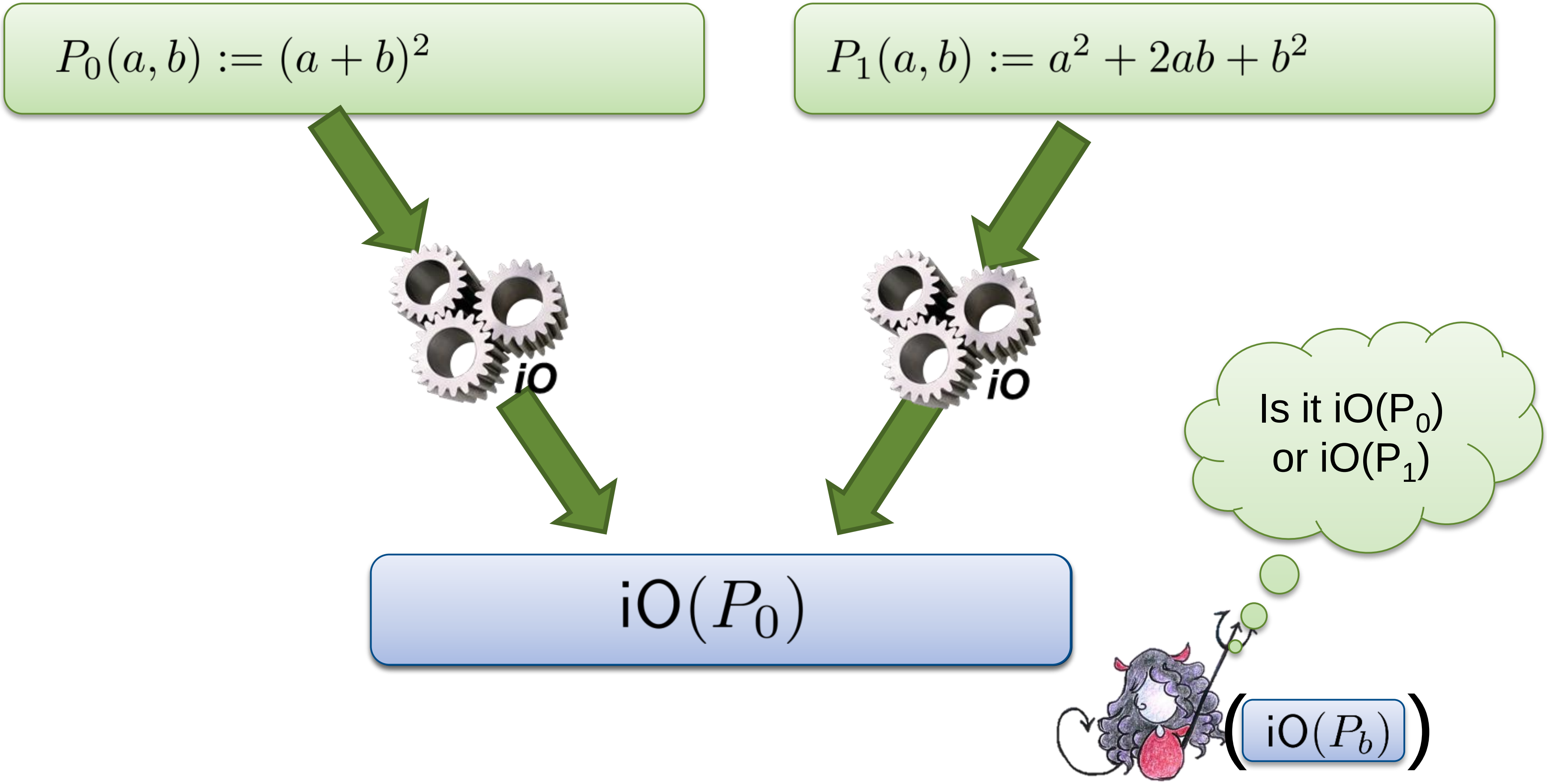
TECHNISCHE UNIVERSITÄT DARMSTADT

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

ASIACRYPT, Dec 10th, 2014

Christina Brzuska
Arno Mittelbach

Indistinguishability Obfuscation (iO)



$P_0(a,b) := (a+b)^2$

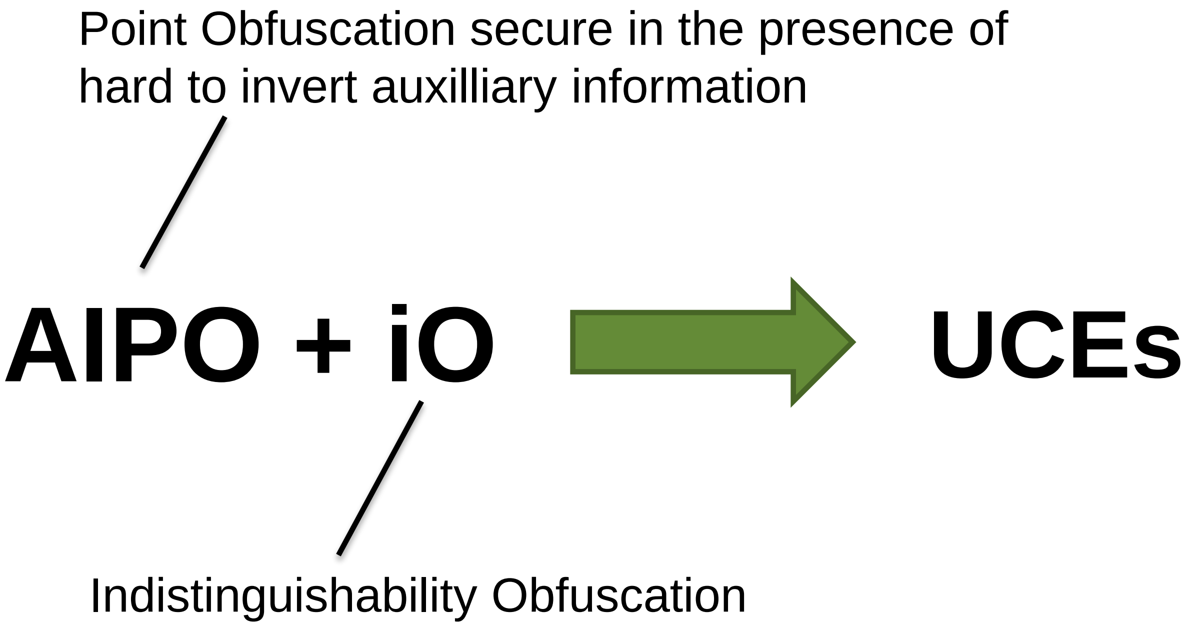
$P_1(a,b) := a^2 + 2ab + b^2$

iO(P_0)

Is it iO(P$_0$) or iO(P$_1$)

(iO(P_b))

The Last Talk



Point Obfuscation secure in the presence of hard to invert auxilliary information

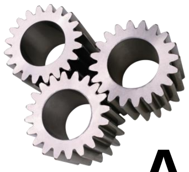
AIPO + iO

UCEs

Indistinguishability Obfuscation

AIPO (Point Obfuscation with Auxiliary Input)

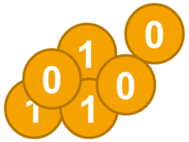
$$p_x(x') := \begin{cases} 1 & \text{if } x = x' \\ 0 & \text{othwerwise} \end{cases}$$

$p \longleftarrow$  $_{\textbf{AIPO}}(x)$

p hides x even in the presence of hard-to-invert auxiliary information about x.

AIPO (Point Obfuscation with Auxiliary Input)

$(\alpha_0, z) \leftarrow$

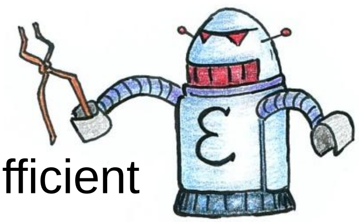
$\alpha_1 \leftarrow$ 

$b \leftarrow$

$p \leftarrow$ **AIPO** (α_b)

$b' \leftarrow$ (p, z)

z hides α_0 computationally

efficient 

$$\xcancel{(z) \downarrow \alpha_0}$$

The Last Talk

Point Obfuscation secure in the presence of hard to invert auxilliary information

Is AIPO a good assumption?

Is AIPO a good assumption?

Indistinguishability Obfuscation

AI

AIPO

[BCPR14]

For all circuits

Just for Point Functions

Candidates exist under non-standard assumptions

Candidates exist under non-standard assumptions

This Talk

is not about AIPOs.

It is about MB-AIPOs.

(And a bit on AIPOs.)

AIPO

$$p_\alpha(x) := \begin{cases} 1 & \text{if } x = \alpha \\ 0 & \text{othwerwise} \end{cases}$$

MB-AIPO

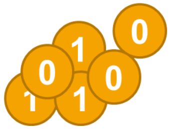
$$p_{\alpha,\beta}(x) := \begin{cases} \beta & \text{if } x = \alpha \\ 0 & \text{othwerwise} \end{cases}$$

Multi-Bit Output

MB-AIPO

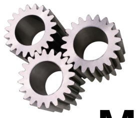
$(\alpha, \beta_0, z) \longleftarrow$

$\beta_1 \longleftarrow$



$b \longleftarrow$

$p \longleftarrow$



(α, β_b)

MB-AIPO

$b' \longleftarrow$

(p, z)

$$(\alpha, \beta_0) \quad \text{vs.} \quad (\alpha, \beta_1)$$

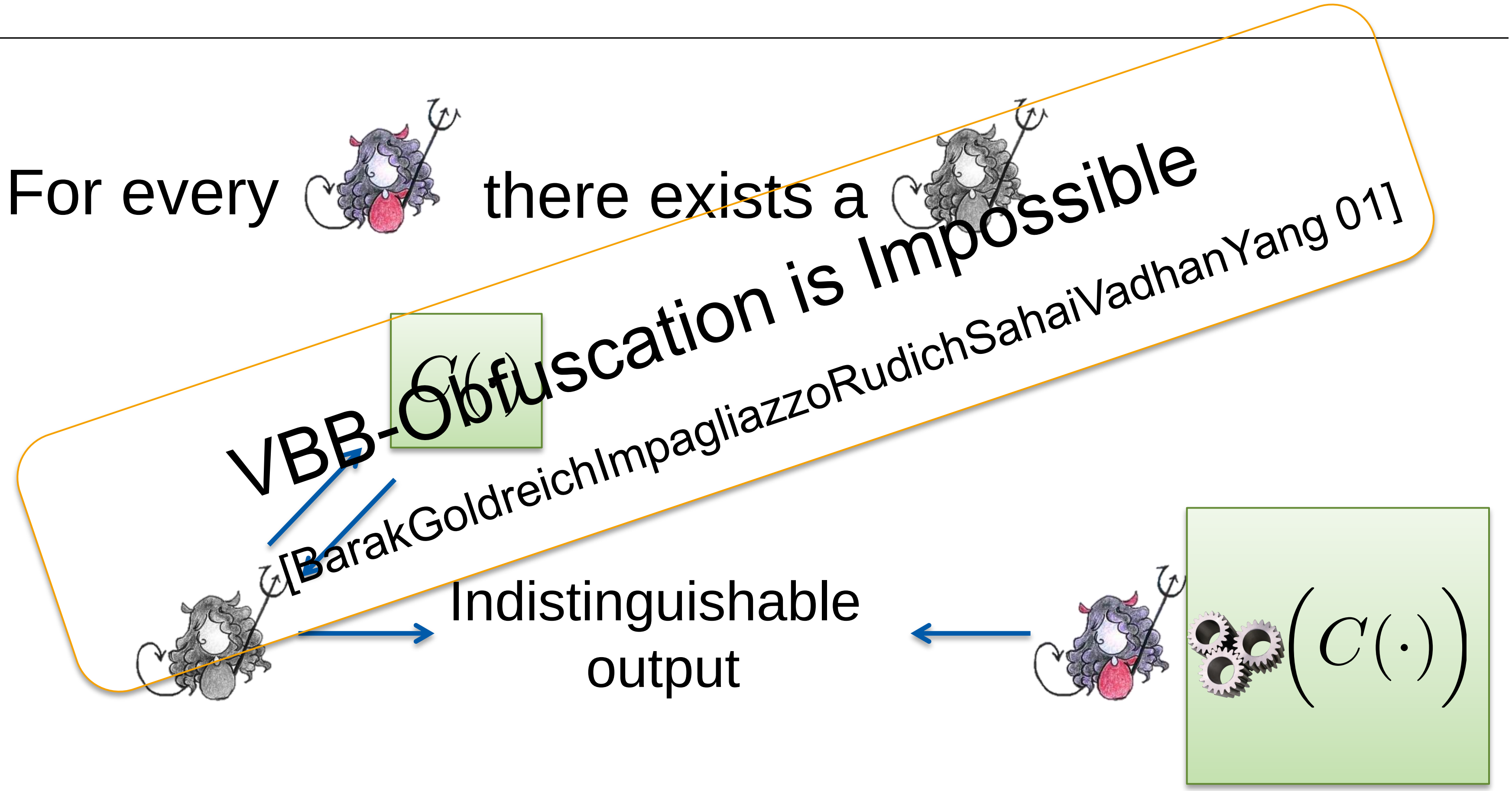
$$(\alpha_0, \beta_0) \quad \text{vs.} \quad (\alpha_1, \beta_1)$$

$$(\alpha_0, \beta) \quad \text{vs.} \quad (\alpha_1, \beta)$$

MB-AIPO vs. Indistinguishability Obfuscation

Theorem: If *Indistinguishability Obfuscation* exists, then MB-AIPO does not exist.

Virtual Black-Box Obfuscation



For every there exists a

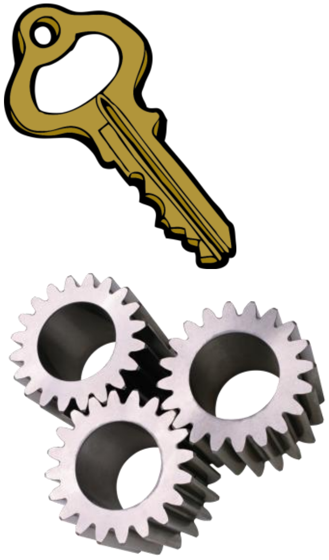
$C(\cdot)$

Indistinguishable output

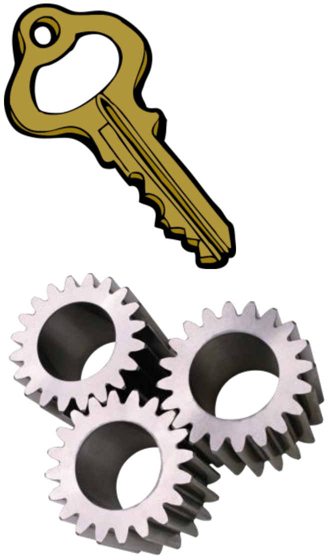
$\left(C(\cdot)\right)$

VBB-Obfuscation is Impossible

[BarakGoldreichImpagliazzoRudichSahaiVadhanYang 01]



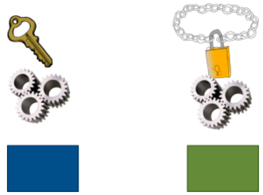
If

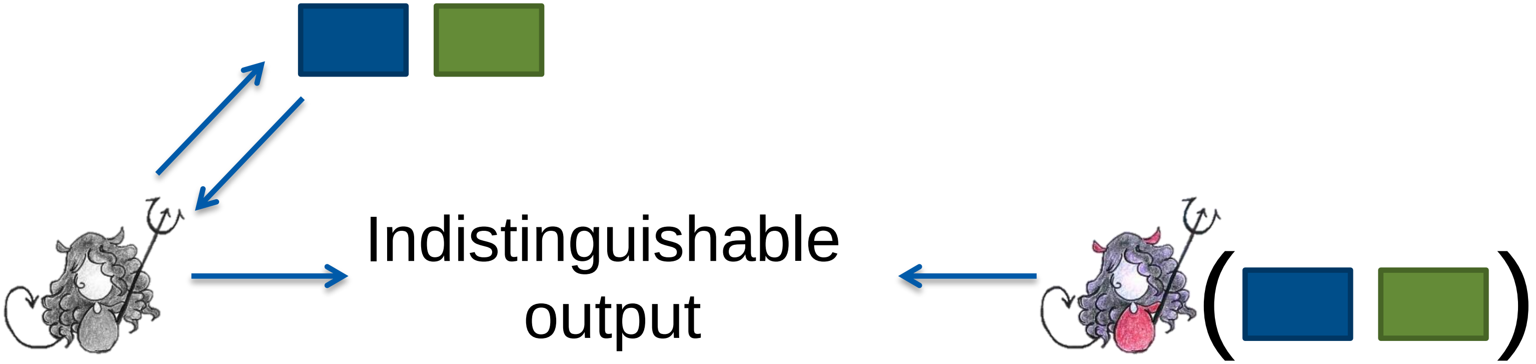


opens

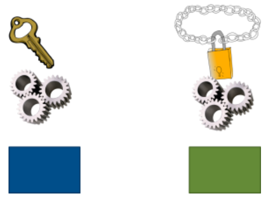
Then

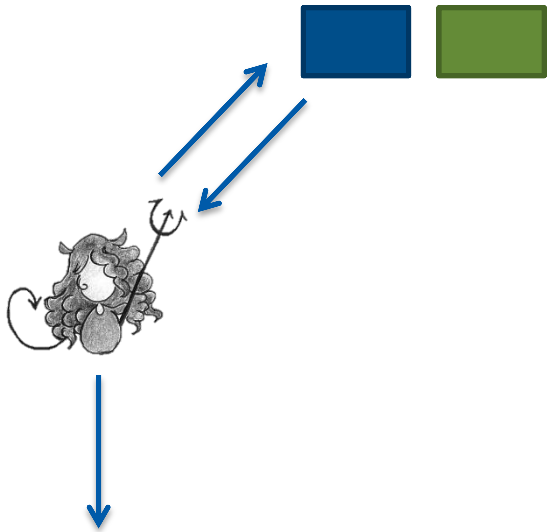
🟦 opens 🟩



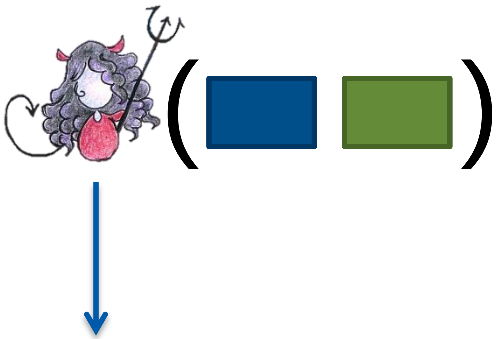


Indistinguishable output





?



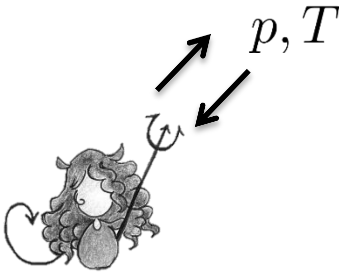
Output 1 if 🟦 fits into 🟩

VBB Obfuscation is Impossible

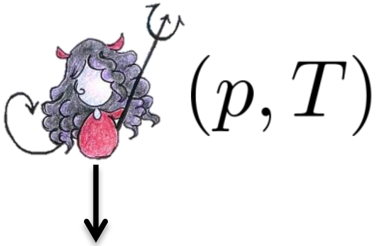
[BGI+ 01]

$$p_{\alpha,\beta}(x) := \begin{cases} \beta & \text{if } x = \alpha \\ 0 & \text{otherwise} \end{cases}$$

$$T_{\alpha,\beta}(C) := \begin{cases} 1 & \text{if } C(\alpha) = \beta \\ 0 & \text{otherwise} \end{cases}$$



p, T



(p, T)

$\text{Output: } T(p)$

Towards MB-AIPO

$$p_{\alpha,\beta}(x) := \begin{cases} \beta & \text{if } x = \alpha \\ 0 & \text{otherwise} \end{cases}$$

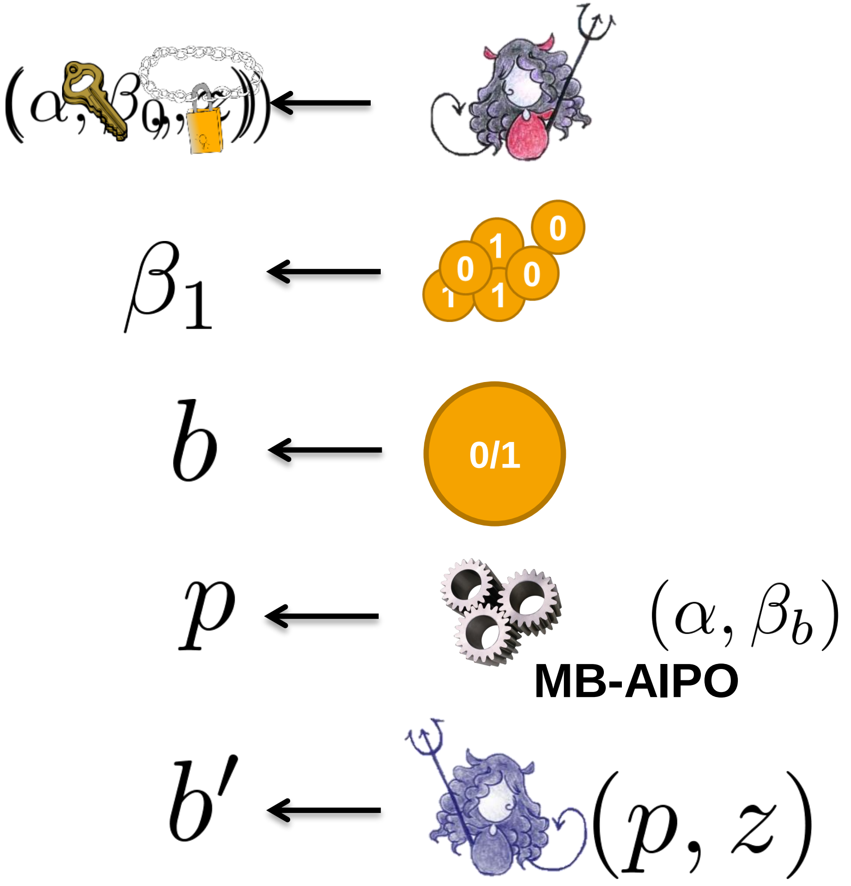
MB-PF

$$T_{\alpha,\beta}(C) := \begin{cases} 1 & \text{if } C(\alpha) = \beta \\ 0 & \text{otherwise} \end{cases}$$

AI

Can we approximate $T_{\alpha,\beta}$ such that the circuit hides α?

MB-AIPO



$(\alpha, \beta_0, z) \leftarrow$

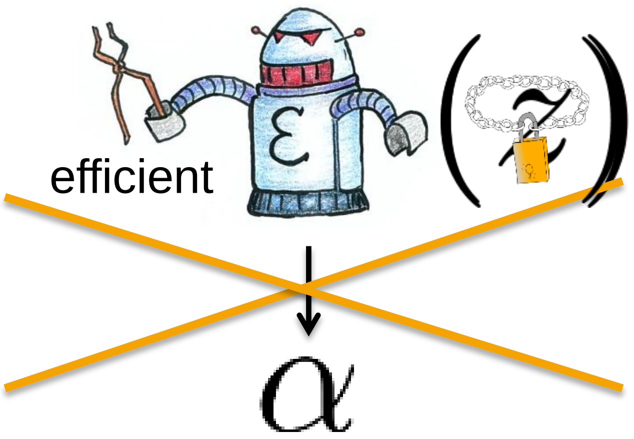
$\beta_1 \leftarrow$

$b \leftarrow$

$p \leftarrow$ (α, β_b)

$b' \leftarrow$ (p, z)

z hides α computationally



$$p_{\alpha,\beta}(x) := \begin{cases} \beta & \text{if } x = \alpha \\ 0 & \text{otherwise} \end{cases}$$

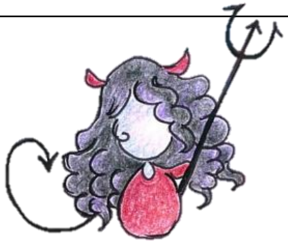
$$T_{\alpha,\beta}(C) := \begin{cases} 1 & \text{if } C(\alpha) = \beta \\ 0 & \text{otherwise} \end{cases}$$

First idea

Obfuscate T_{α,β_0} with an indistinguishability obfuscator.

First idea

$(\alpha, \beta_0, \mathsf{iO}(C[\alpha, \beta_0])) \longleftarrow$



0

$$\mathsf{iO}(C[\alpha, \beta_0])(p_{\alpha,\beta_0}) = 1$$

$$\mathsf{iO}(C[\alpha, \beta_0])(p_{\alpha,\beta_1}) = 0$$

Adversary wins

```
$C[\alpha, \beta_0](\tilde{C})$
if $\tilde{C}(\alpha) = \beta_0$
    return 1
return 0
```

(α, β_b)

MB-AIPO

$1 - \mathsf{iO}(C[\alpha, \beta_0])(p) \longleftarrow$

$(p, \mathsf{iO}(C[\alpha, \beta_0]))$

Does $\mathsf{iO}(C[\alpha,\beta_0])$ hide α?

```
$C[\alpha,\beta_0](\tilde{C})$
if $\tilde{C}(\alpha)=\beta_0$
    return 1
return 0
```

VBB-obfuscation of $C[\alpha,\beta_0]$ hides α, but for indistinguishability obfuscation we don't know.

Can we tweak $C[\alpha,\beta_0]$ such that functionality is preserved while allowing us to hide α?

```
$\alpha \leftarrow \$\{0,1\}^\lambda$
$\beta_0 \leftarrow \$\{0,1\}^\lambda$

$- - - - --$

$C[\alpha, \beta_0](\tilde{C})$
if $\tilde{C}(\alpha) = \beta_0$
    return 1
return 0
```

```
$\alpha \leftarrow \$\{0,1\}^\lambda$
$\beta_0 \leftarrow \$\{0,1\}^\lambda$

$- - - - --$

$C_1[\alpha, \beta_0](\tilde{C})$
if $\mathsf{PRG}(\tilde{C}(\alpha)) = \mathsf{PRG}(\beta_0)$
    return 1
return 0
```

```
$\alpha \leftarrow \$\{0,1\}^\lambda$
$\beta_0 \leftarrow \$\{0,1\}^\lambda$
$y \leftarrow \mathsf{PRG}(\beta_0)$
$- - - - --$

$C_2[\alpha, y](\tilde{C})$
if $\mathsf{PRG}(\tilde{C}(\alpha)) = y$
    return 1
return 0
```

Precompute PRG(β$_0$)

iO($C_2[\alpha, \beta_0]$) hides α

```
$\alpha \leftarrow \$\{0,1\}^\lambda$
$\beta_0 \leftarrow \$\{($
$y \leftarrow$ PRG
$- - - - -$
$C_2[\alpha, y]](($
if PRG($\tilde{C}$
    return 1
return 0
```

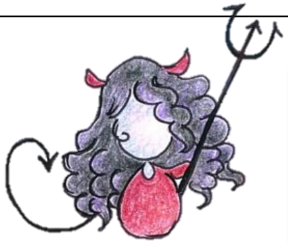
$$\text{iO}(C_2[\alpha, y]) \approx \text{iO}(\mathbf{0})$$

Constant zero circuit with high probability →

```
$\alpha \leftarrow \$\{0,1\}^\lambda$
$\{0,1\}^\lambda$
$0,1\}^{|\mathsf{PRG}(\beta_0)|}$
$--$
$](\tilde{C})$
$\tilde{C}(\alpha)) = y$
    return 1
return 0
```

Final Attack

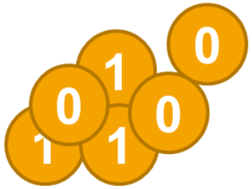
$(\alpha, \beta_0, \mathsf{iO}(C_2[\alpha, y])) \longleftarrow$



uniformly random

```
$C_2[\alpha, y \leftarrow \mathsf{PRG}(\beta_0)](\tilde{C})$
if $\mathsf{PRG}(\tilde{C}(\alpha)) = y$
    return 1
return 0
```

$\beta_1 \longleftarrow$



$b \longleftarrow$

$p \longleftarrow$

(α, β_b)

MB-AIPO

$1 - \mathsf{iO}(C_2[\alpha, y])(p) \longleftarrow$

$(p, \mathsf{iO}(C_2[\alpha, y]))$

iO and MB-AIPO are mutually exclusive

Indistinguishability Obfuscation

MB-AIPO

AI

For all circuits

Just for Point Functions

Candidates exist under non-standard assumptions

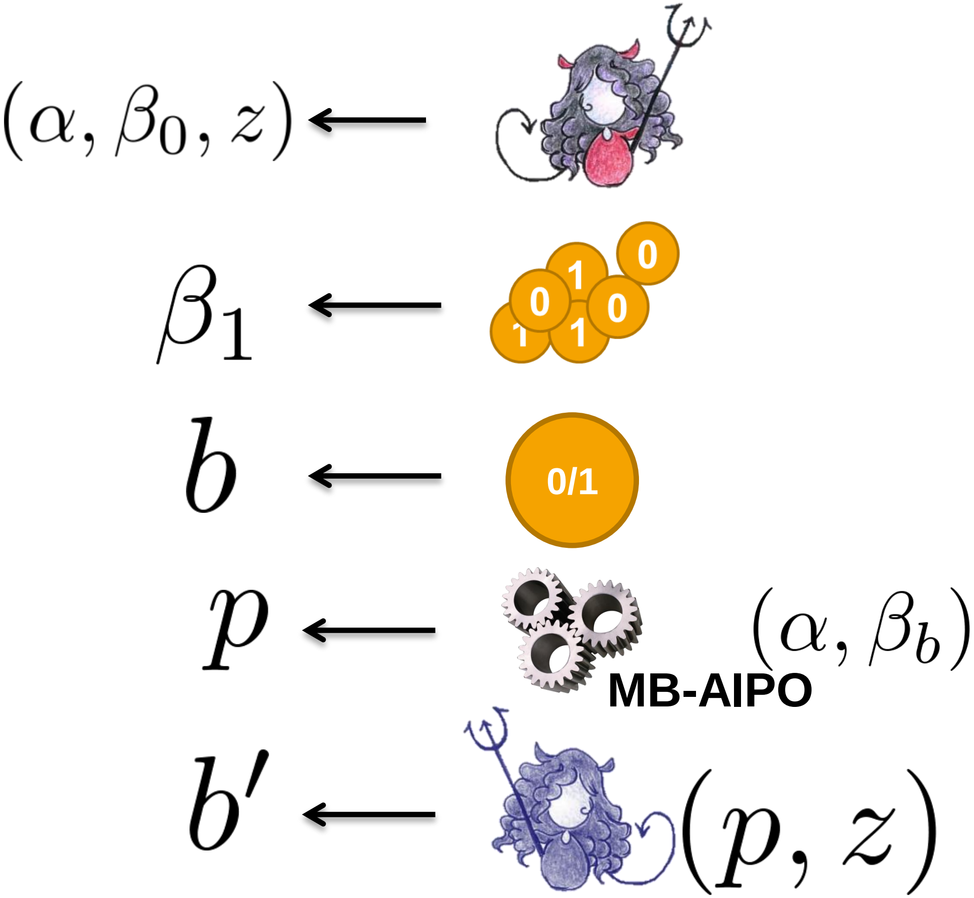
No candidate construction in the standard model

Can we bypass the impossibility?

Bypassing the Impossibility

- Restrict auxiliary information to be
  1. statistically hard-to-invert
  2. short
  3. hard-to-invert in the presence of beta (weak MB-AIPO)

Weak MB-AIPO



$(\alpha, \beta_0, z) \longleftarrow$

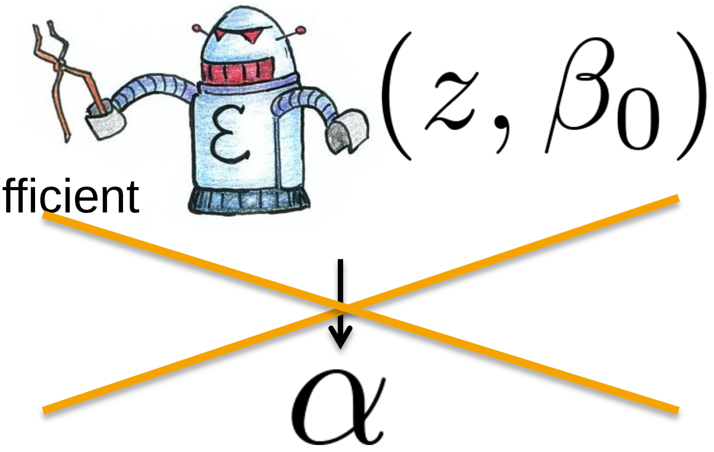
$\beta_1 \longleftarrow$

$b \longleftarrow$

$p \longleftarrow$ MB-AIPO (α, β_b)

$b' \longleftarrow$ (p, z)

(z,β$_0$) hides α computationally

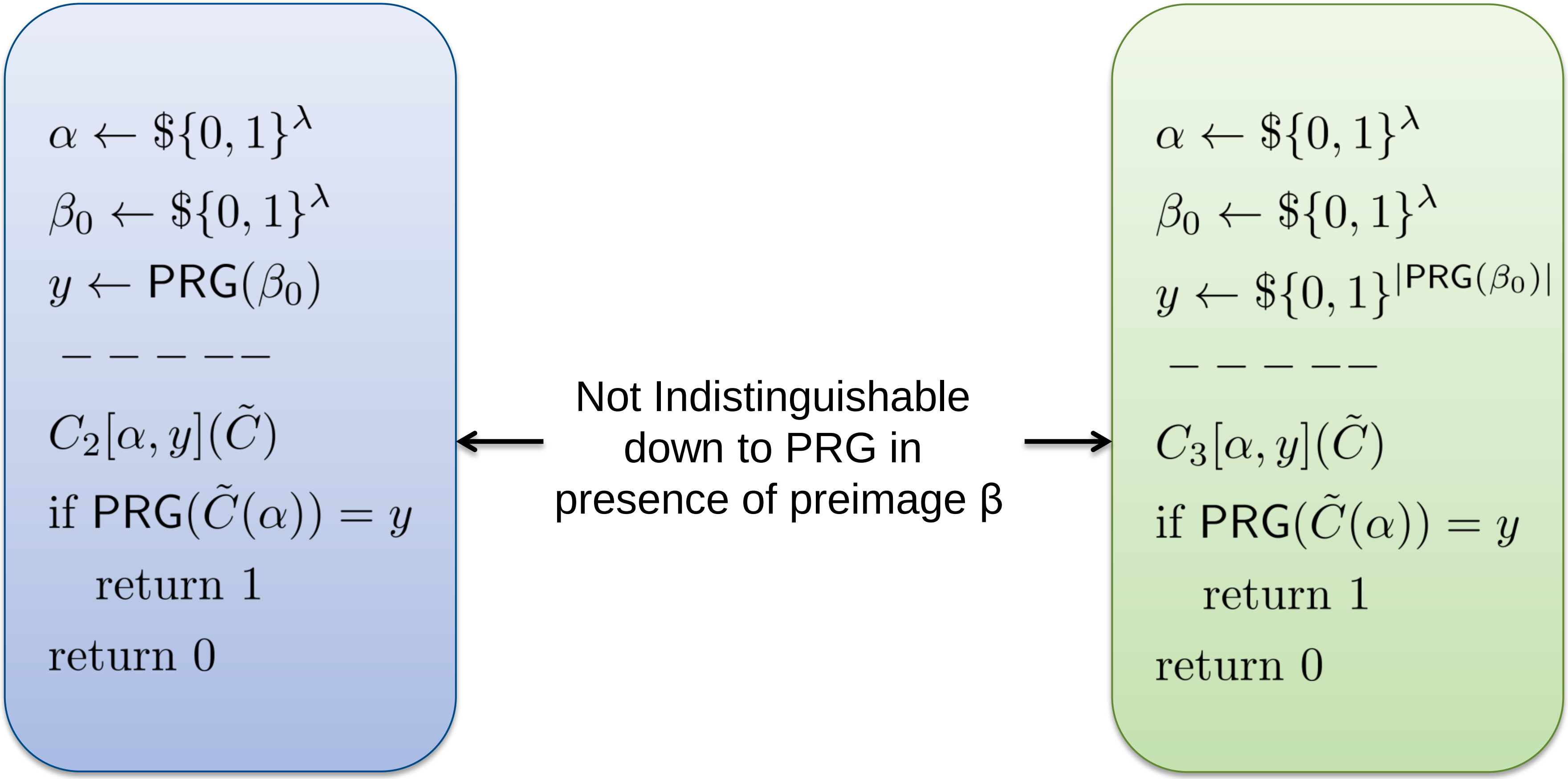


efficient

(z, β_0)

α

Attack fails

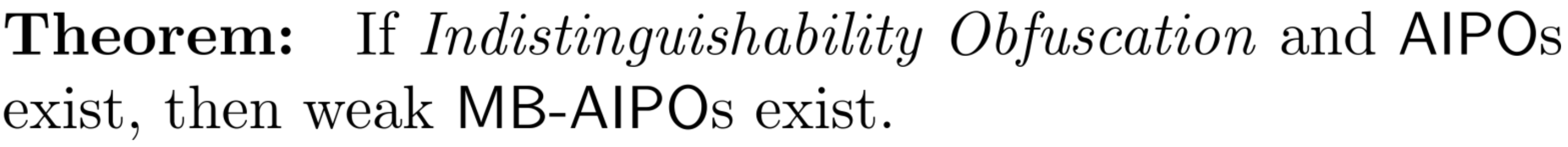


```
$\alpha \leftarrow \$\{0,1\}^{\lambda}$
$\beta_0 \leftarrow \$\{0,1\}^{\lambda}$
$y \leftarrow \mathsf{PRG}(\beta_0)$
$- - - - --$
$C_2[\alpha, y](\tilde{C})$
if $\mathsf{PRG}(\tilde{C}(\alpha)) = y$
    return 1
return 0
```

Not Indistinguishable
down to PRG in
presence of preimage β

```
$\alpha \leftarrow \$\{0,1\}^{\lambda}$
$\beta_0 \leftarrow \$\{0,1\}^{\lambda}$
$y \leftarrow \$\{0,1\}^{|\mathsf{PRG}(\beta_0)|}$
$- - - - --$
$C_3[\alpha, y](\tilde{C})$
if $\mathsf{PRG}(\tilde{C}(\alpha)) = y$
    return 1
return 0
```

Weak MB-AIPO from iO and AIPO



Theorem: If *Indistinguishability Obfuscation* and AIPOs exist, then weak MB-AIPOs exist.

Weak MB-AIPO implies leakage resilient PKE

Summary

- Indistinguishability Obfuscation and MB-AIPO are mutually exclusive.
- We can bypass the impossibility result by restricting the auxiliary information to be
  1. statistically hard-to-invert
  2. short
  3. hard-to-invert in the presence of beta (weak MB-AIPO)