RUB

RUHR-UNIVERSITÄT BOCHUM

On the Impossibility of Obfuscating Programs

UbiCrypt Seminar & Lecture Series, 18.02.2016

Felix Heuer
Horst Görtz Institute for IT Security
Ruhr University Bochum

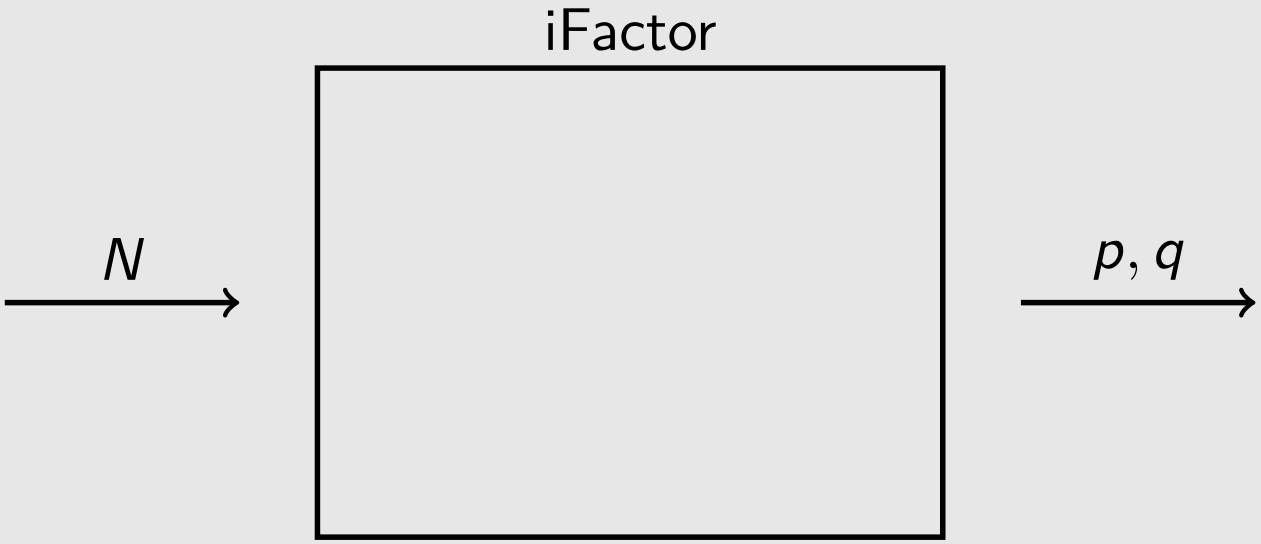
hgi
Horst Görtz Institut
für IT-Sicherheit

On the Impossibility of Obfuscating Programs

- *On the (Im)possibility of Obfuscating Programs*, CRYPTO'01
  Barak, Goldreich, Impagliazzo, Rudich, Sahai, Vadhan, Yang

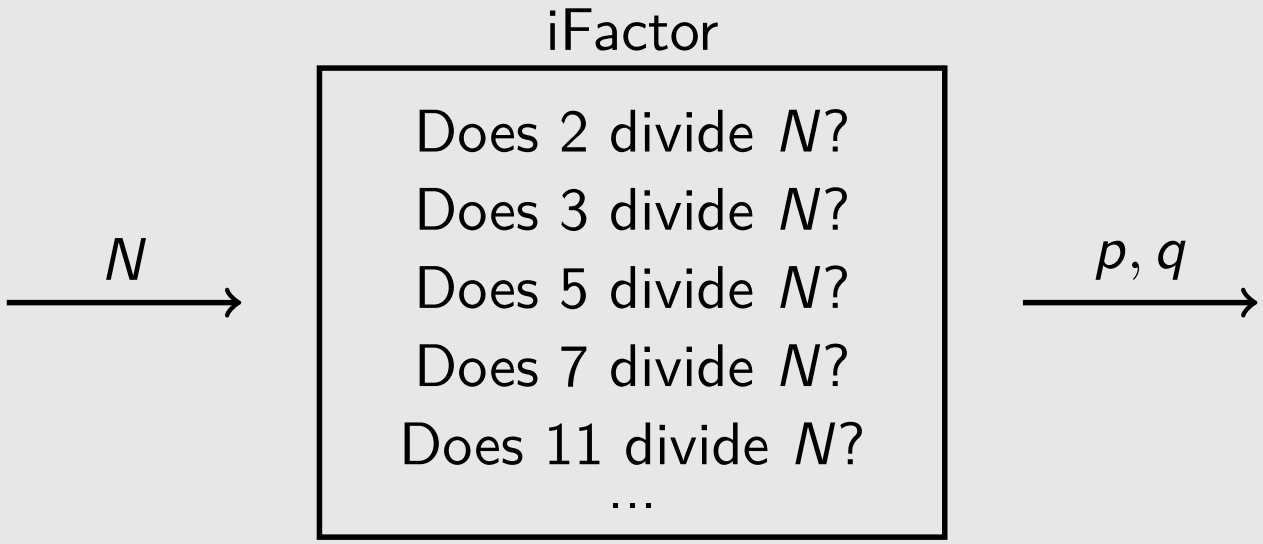
Virtual Blackbox Obfuscation does not exist.

What is Virtual Blackbox Obfuscation?



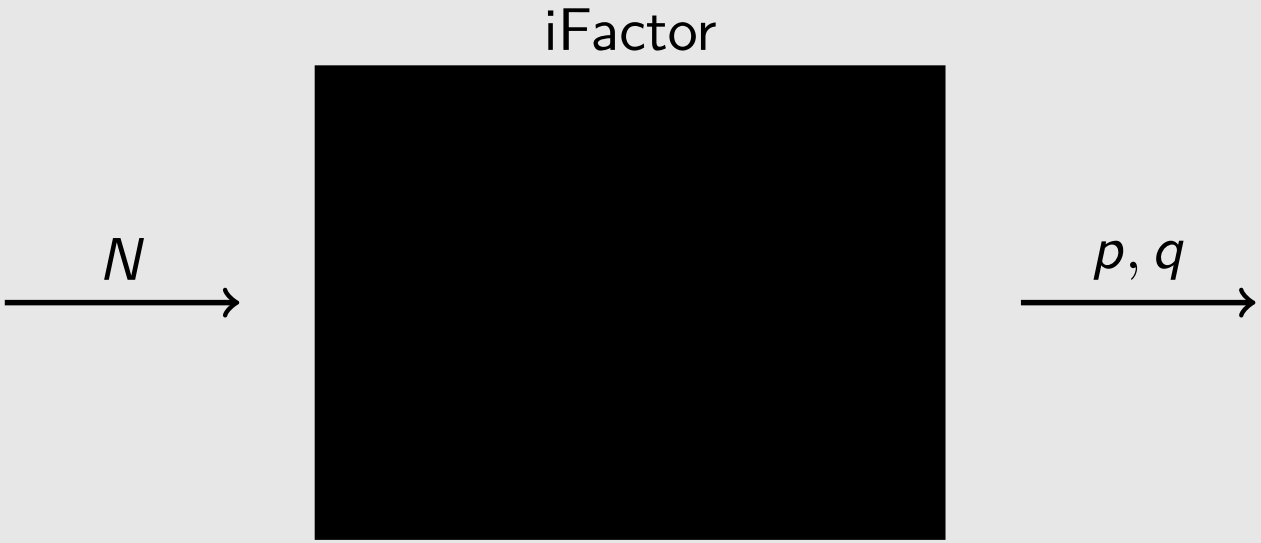
Suppose, you came up with a really clever algorithm for factoring. You want to sell it without revealing your code.

What is Virtual Blackbox Obfuscation?



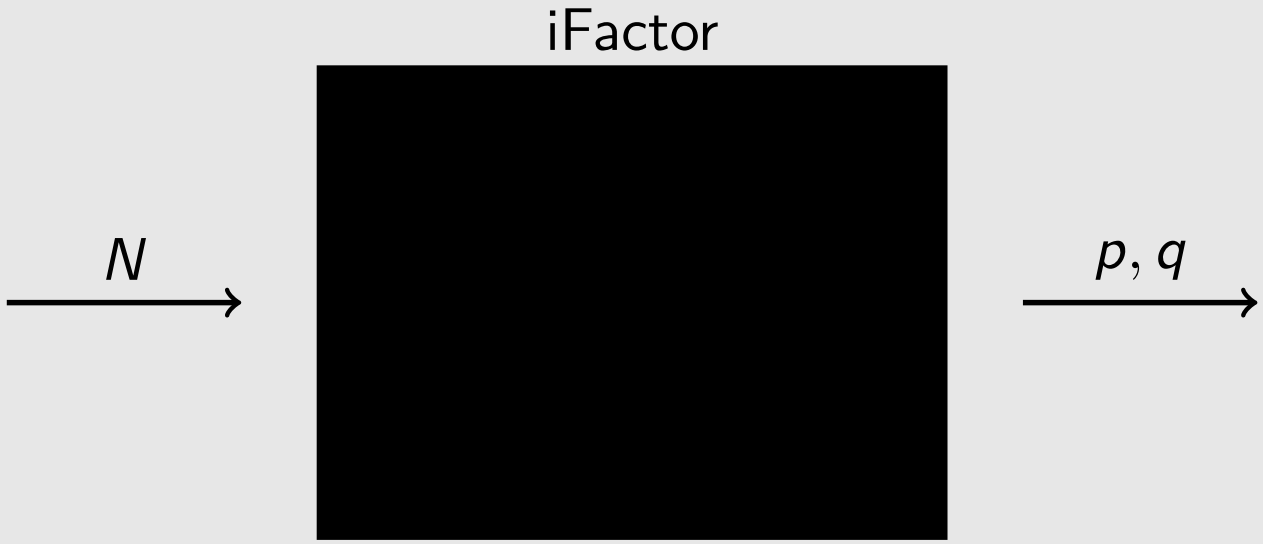
Suppose, you came up with a really clever algorithm for factoring. You want to sell it without revealing your code. (For instance, because it's actually stupid.)

What is Virtual Blackbox Obfuscation?



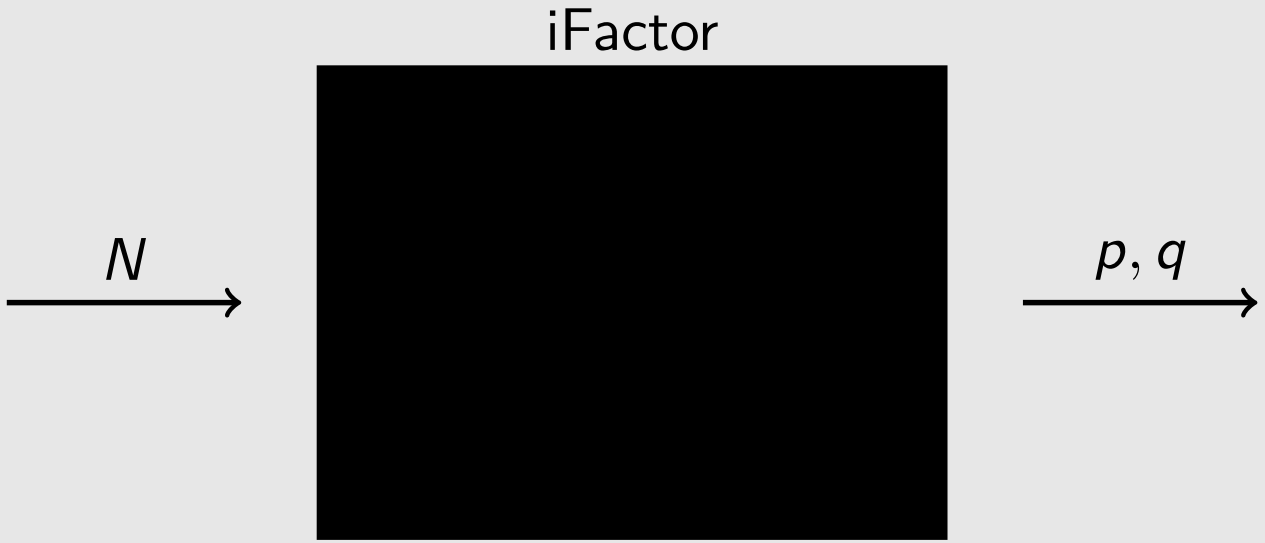
The obfuscated code should still compute the same function and should be roughly as efficient as the unobfuscated code.

What is Virtual Blackbox Obfuscation?



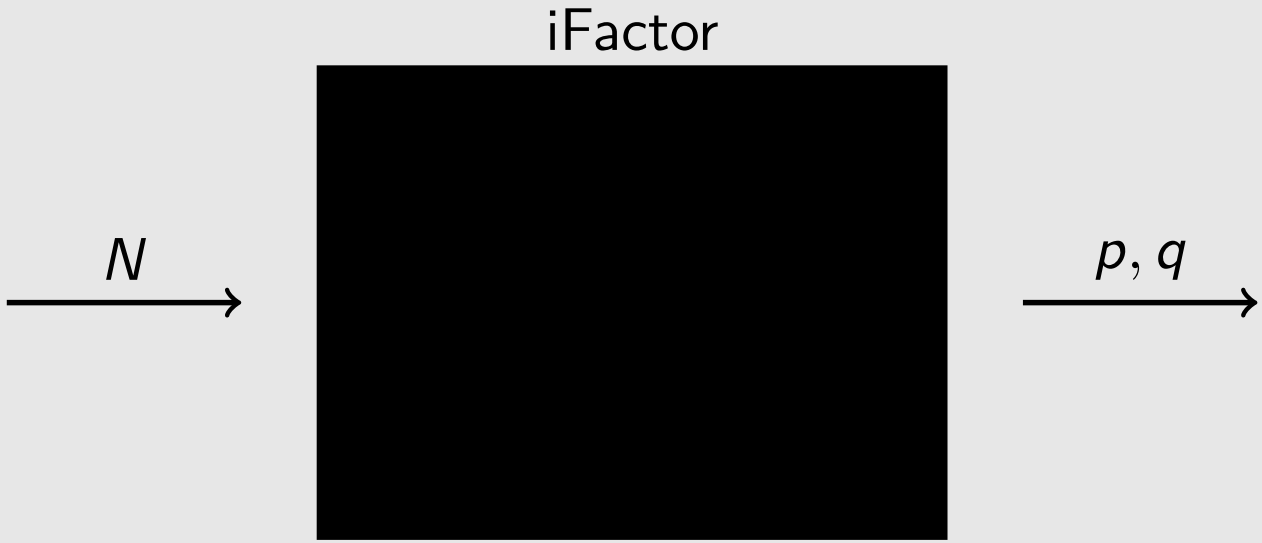
Ideally, the obfuscated code should behave like a black box, i.e. it should not leak any information beyond input/output behaviour.

What is Virtual Blackbox Obfuscation?



Ideally, the obfuscated code should behave like **an oracle** i.e. it should not leak any information beyond input/output behaviour.

What is Virtual Blackbox Obfuscation?



Ideally, the obfuscated code should behave like **an oracle** i.e. it should not leak any information beyond input/output behaviour.

For any efficient $\mathcal{A}$ there is an efficient $\mathcal{S}$ s.t. for all TM M:

$$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[\mathcal{S}^{M} = 1]$$

Why do we care about Obfuscation?

Why do we care about Obfuscation?

- Turn private key into public key cryptography

$$Enc_{pk}(\cdot) := \boxed{Enc_k(\cdot)}$$

Why do we care about Obfuscation?

- Turn private key into public key cryptography

$$Enc_{pk}(\cdot) := \boxed{Enc_k(\cdot)}$$

- Turn a MAC into a signature scheme

$$Vrfy_{pk}(\cdot,\cdot) := \boxed{Vrfy_k(\cdot,\cdot)}$$

Why do we care about Obfuscation?

- Turn private key into public key cryptography

$$Enc_{pk}(\cdot) := \boxed{Enc_k(\cdot)}$$

- Turn a MAC into a signature scheme

$$Vrfy_{pk}(\cdot,\cdot) := \boxed{Vrfy_k(\cdot,\cdot)}$$

- Interested in fully homomorphic encryption?

$$Enc_{pk}(\cdot) \star Enc_{pk}(\cdot) := \boxed{Enc_{pk}(Dec_{sk}(\cdot) \star Dec_{sk}(\cdot))}$$

Why do we care about Obfuscation?

- Turn private key into public key cryptography

$$Enc_{pk}(\cdot) := \boxed{Enc_k(\cdot)}$$

- Turn a MAC into a signature scheme

$$Vrfy_{pk}(\cdot,\cdot) := \boxed{Vrfy_k(\cdot,\cdot)}$$

- Interested in fully homomorphic encryption?

$$Enc_{pk}(\cdot) \star Enc_{pk}(\cdot) := \boxed{Enc_{pk}(Dec_{sk}(\cdot) \star Dec_{sk}(\cdot))}$$

- $\exists VBB \Rightarrow \exists OWFs \Rightarrow P \neq NP$.

Theorem: VBB O for TMs does not exist.

xkcd.com

Theorem: VBB O for TMs does not exist.

Proof idea:

Conceptual difference:

- Hands-on access allows one to do computations *on a function's description*, no matter how obfuscated.
- Oracle access to a function rules that out, unless the function is efficiently learnable by queries.

$$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[S^M = 1]$$

VBB "security"

Theorem: VBB O for TMs does not exist.

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

Conceptual difference:

- Hands-on access allows one to do computations *on a function's description*, no matter how obfuscated.
- Oracle access to a function rules that out, unless the function is efficiently learnable by queries.

We will construct $\mathcal{A}$ and TMs, such that assuming the obfuscatability of the TMs leads to a contradiction for all $\mathcal{S}$.

$$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[\mathcal{S}^M = 1]$$

VBB "security"

Theorem: VBB O for TMs does not exist.

xkcd.com

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\alpha,\beta}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases}$$
$$\alpha, \beta \leftarrow_{\$} \{0,1\}^k$$

$$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[S^M = 1]$$

VBB "security"

Theorem: VBB O for TMs does not exist.

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\alpha,\beta}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases}$$
$$\alpha, \beta \leftarrow_{\$} \{0,1\}^k$$

Almost everywhere 0^k; hard to learn via queries.

$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[S^M = 1]$

VBB "security"

Theorem: VBB O for TMs does not exist.

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\substack{\alpha,\beta \leftarrow_{\$} \{0,1\}^k}}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Almost everywhere 0^k; hard to learn via queries.

$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[S^M = 1]$

VBB "security"

Theorem: VBB O for TMs does not exist.

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\substack{\alpha,\beta \leftarrow_{\$} \{0,1\}^k}}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Almost everywhere 0^k; hard to learn via queries.

Actually, not computable. Suffices to let it run for a while assuming that C terminates in reasonable time.

$$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[S^M = 1]$$

VBB "security"

Theorem: VBB O for TMs does not exist.

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\substack{\alpha,\beta \\ \alpha,\beta \leftarrow_{\$} \{0,1\}^k}}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Consider $\mathcal{A}$ that obtains two TMs C, D encoded as (one TM called) $C\#D$ and always outputs $\mathcal{A}(C\#D) := D(C)$.

$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[S^M = 1]$

VBB "security"

Theorem: VBB O for TMs does not exist.

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\substack{\alpha,\beta \leftarrow_{\$} \{0,1\}^k}}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Consider $\mathcal{A}$ that obtains two TMs C, D encoded as (one TM called) $C\#D$ and always outputs $\mathcal{A}(C\#D) := D(C)$.

$$\Pr[\mathcal{A}(\boxed{C_{\alpha,\beta}\#D_{\alpha,\beta}}) = 1] = 1$$

$$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[S^M = 1]$$

VBB "security"

Theorem: VBB O for TMs does not exist.

xkcd.com

hgi Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\substack{\alpha,\beta \\ \alpha,\beta \leftarrow_{\$} \{0,1\}^k}}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Consider $\mathcal{A}$ that obtains two TMs C, D encoded as (one TM called) $C\#D$ and always outputs $\mathcal{A}(C\#D) := D(C)$.

$$\Pr[\mathcal{A}(\boxed{C_{\alpha,\beta}\#D_{\alpha,\beta}}) = 1] = 1$$

Let Z_k be a TM that always outputs 0^k, then

$$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[S^M = 1]$$

VBB "security"

Theorem: VBB O for TMs does not exist.

xkcd.com

hgi Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\substack{\alpha,\beta \\ \alpha,\beta \leftarrow_{\$} \{0,1\}^k}}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Consider $\mathcal{A}$ that obtains two TMs C, D encoded as (one TM called) $C\#D$ and always outputs $\mathcal{A}(C\#D) := D(C)$.

$$\Pr[\mathcal{A}(\boxed{C_{\alpha,\beta}\#D_{\alpha,\beta}}) = 1] = 1$$

Let Z_k be a TM that always outputs 0^k, then

$$\Pr[\mathcal{S}^{C_{\alpha,\beta}\#D_{\alpha,\beta}} = 1] \approx \Pr[\mathcal{S}^{Z_k\#D_{\alpha,\beta}} = 1].$$

$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[\mathcal{S}^M = 1]$

VBB "security"

Theorem: VBB O for TMs does not exist.

xkcd.com

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\substack{\alpha,\beta \\ \alpha,\beta \leftarrow_\$ \{0,1\}^k}}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Consider $\mathcal{A}$ that obtains two TMs C, D encoded as (one TM called) $C\#D$ and always outputs $\mathcal{A}(C\#D) := D(C)$.

$$\Pr[\mathcal{A}(\boxed{C_{\alpha,\beta}\#D_{\alpha,\beta}}) = 1] = 1$$

Let Z_k be a TM that always outputs 0^k, then

$$\Pr[\mathcal{S}^{C_{\alpha,\beta}\#D_{\alpha,\beta}} = 1] \approx \Pr[\mathcal{S}^{Z_k\#D_{\alpha,\beta}} = 1].$$

$\mathcal{S}$ would have to query $C_{\alpha,\beta}$ (resp. Z_k) on β to tell the oracles apart.

$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[\mathcal{S}^M = 1]$ VBB "security"

Theorem: VBB O for TMs does not exist.

xkcd.com

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\substack{\alpha,\beta \\ \alpha,\beta \leftarrow_{\$} \{0,1\}^k}}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Consider $\mathcal{A}$ that obtains two TMs C, D encoded as (one TM called) $C\#D$ and always outputs $\mathcal{A}(C\#D) := D(C)$.

$$\Pr[\mathcal{A}(\boxed{C_{\alpha,\beta}\#D_{\alpha,\beta}}) = 1] = 1$$

Let Z_k be a TM that always outputs 0^k, then

$$\Pr[\mathcal{S}^{C_{\alpha,\beta}\#D_{\alpha,\beta}} = 1] \approx \Pr[\mathcal{S}^{Z_k\#D_{\alpha,\beta}} = 1].$$

On the other hand

$$\Pr[\mathcal{A}(\boxed{Z_k\#D_{\alpha,\beta}}) = 1] \leq \text{negl}.$$

$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[\mathcal{S}^M = 1]$ VBB "security"

Theorem: VBB O for TMs does not exist.

xkcd.com

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\alpha,\beta}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad \alpha, \beta \leftarrow_{\$} \{0,1\}^k$$

$$D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Consider $\mathcal{A}$ that obtains two TMs C, D encoded as (one TM called) $C\#D$ and always outputs $\mathcal{A}(C\#D) := D(C)$.

$$\Pr[\mathcal{A}(\boxed{C_{\alpha,\beta}\#D_{\alpha,\beta}}) = 1] = 1$$

Let Z_k be a TM that always outputs 0^k, then

$$\Pr[\mathcal{S}^{C_{\alpha,\beta}\#D_{\alpha,\beta}} = 1] \approx \Pr[\mathcal{S}^{Z_k\#D_{\alpha,\beta}} = 1].$$

On the other hand

$$\Pr[\mathcal{A}(\boxed{Z_k\#D_{\alpha,\beta}}) = 1] \leq \text{negl}.$$

$\mathcal{A}$ returns 0 unless $\beta = 0^k$.

$\Pr[\mathcal{A}(\boxed{M}) = 1] \approx \Pr[\mathcal{S}^M = 1]$

VBB "security"

Theorem: VBB O for TMs does not exist.

xkcd.com

Horst Görtz Institut für IT-Sicherheit

RUB

Proof idea:

$$C_{\substack{\alpha,\beta \\ \alpha,\beta \leftarrow_\$ \{0,1\}^k}}(x) := \begin{cases} \beta & x = \alpha \\ 0^k & \textit{otherwise} \end{cases} \qquad D_{\alpha,\beta}(C) := \begin{cases} 1 & C(\alpha) = \beta \\ 0 & \textit{otherwise} \end{cases}$$

Consider J … e TM called) $C\#D$ and

Let Z_k be

On the ot

Contradiction:

$$\Pr[\mathcal{A}(\boxed{C_{\alpha,\beta}\#D_{\alpha,\beta}}) = 1] = 1$$

$$\overset{\text{VBB}}{\approx}$$

$$\Pr[\mathcal{S}^{C_{\alpha,\beta}\#D_{\alpha,\beta}} = 1] \approx \Pr[\mathcal{S}^{Z_k\#D_{\alpha,\beta}} = 1].$$

$$\overset{\text{VBB}}{\approx}$$

$$\Pr[\mathcal{A}(\boxed{Z_k\#D_{\alpha,\beta}}) = 1] \leq \text{negl}.$$

$\Pr[\mathcal{A}(\boxed{\quad}) = 1] \approx \Pr[\mathcal{S}^M = 1]$

VBB "security"