Collusion Resistant Watermarking Schemes for Cryptographic Functionalities

Rupeng Yang, Man Ho Au, Junzuo Lai,
Qiuliang Xu, and Zuoxia Yu

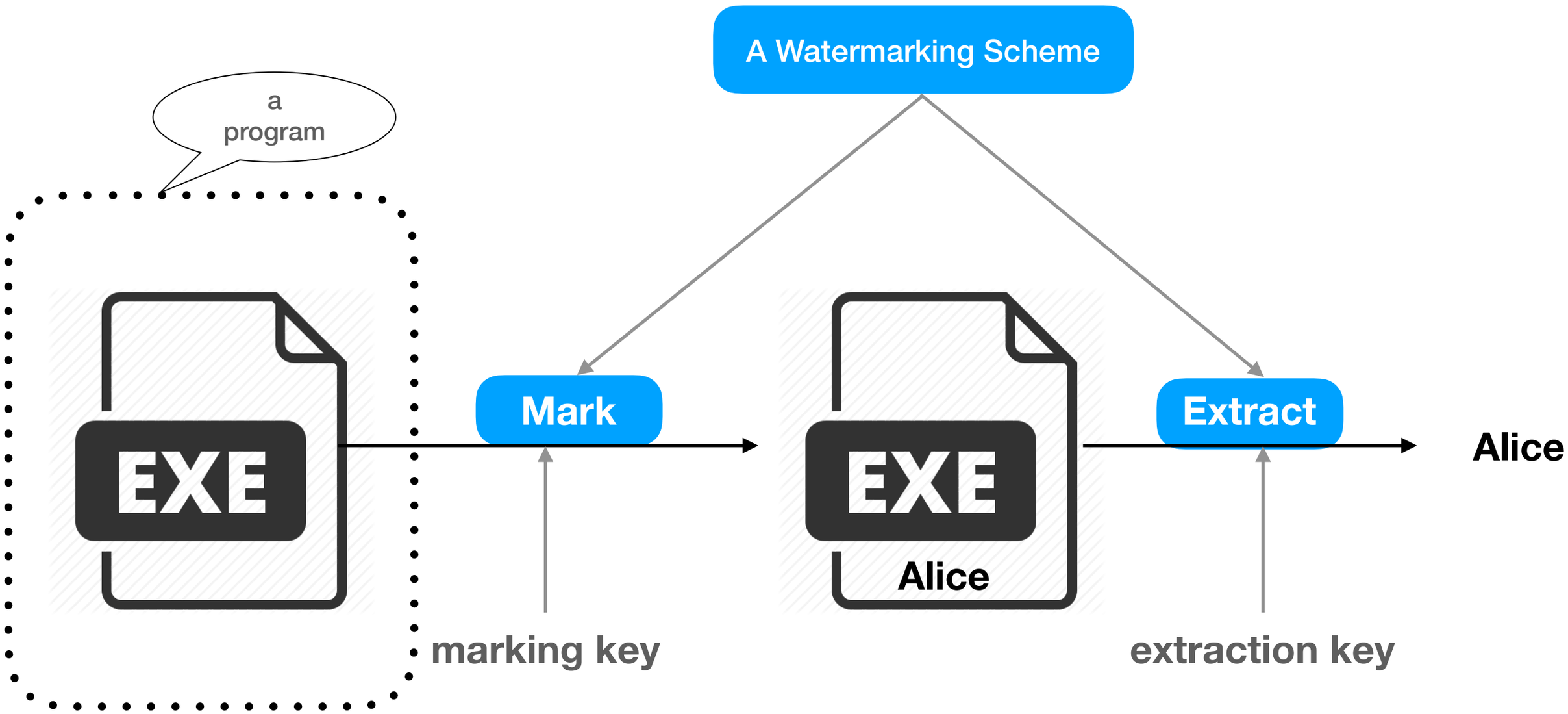
Outline

- Background☞
- The Problem
- Our Result

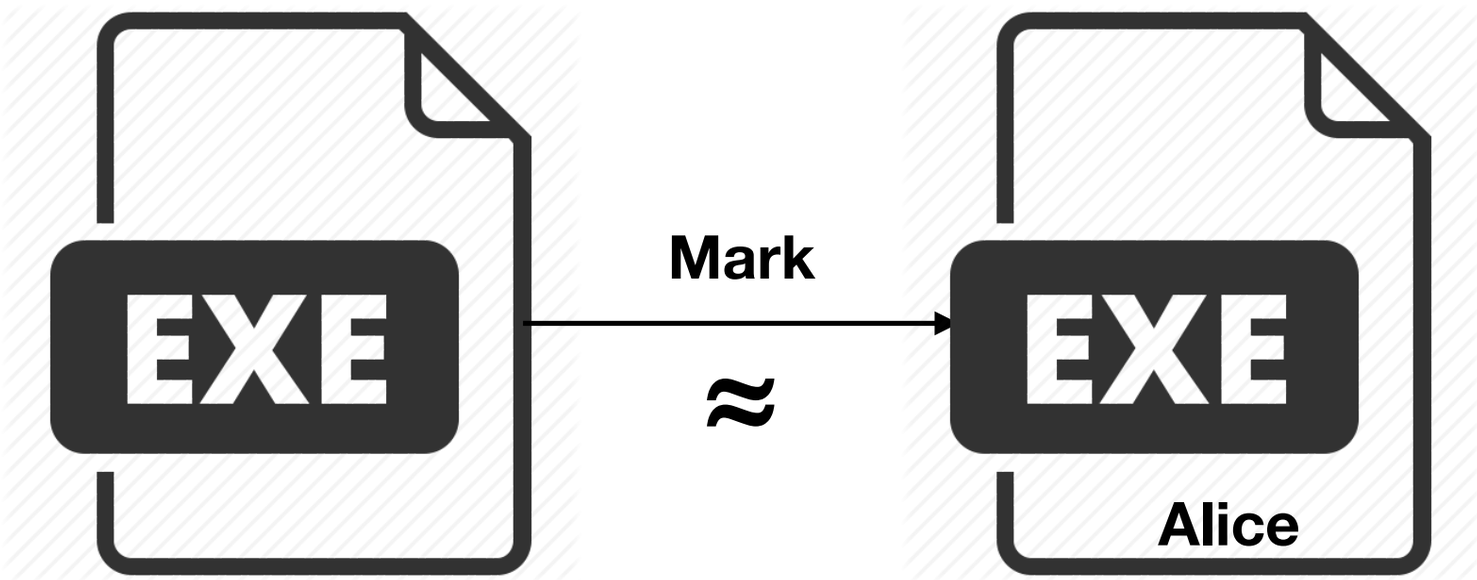
Watermarking A Cryptographic Program

Watermarking A Cryptographic Program

Watermarking A Cryptographic Program

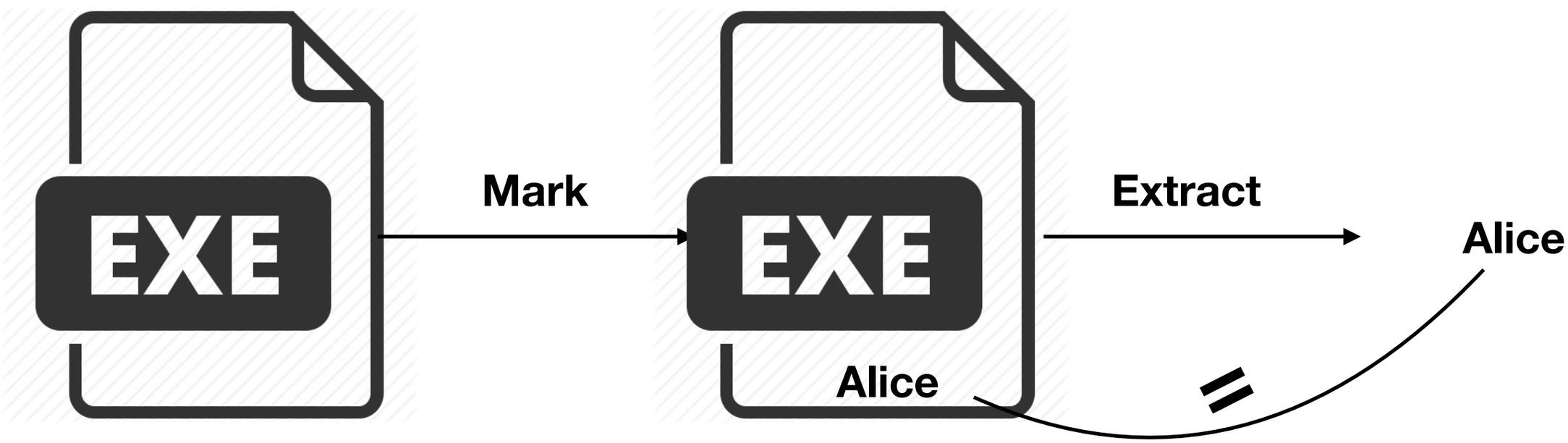


Watermarking A Cryptographic Program



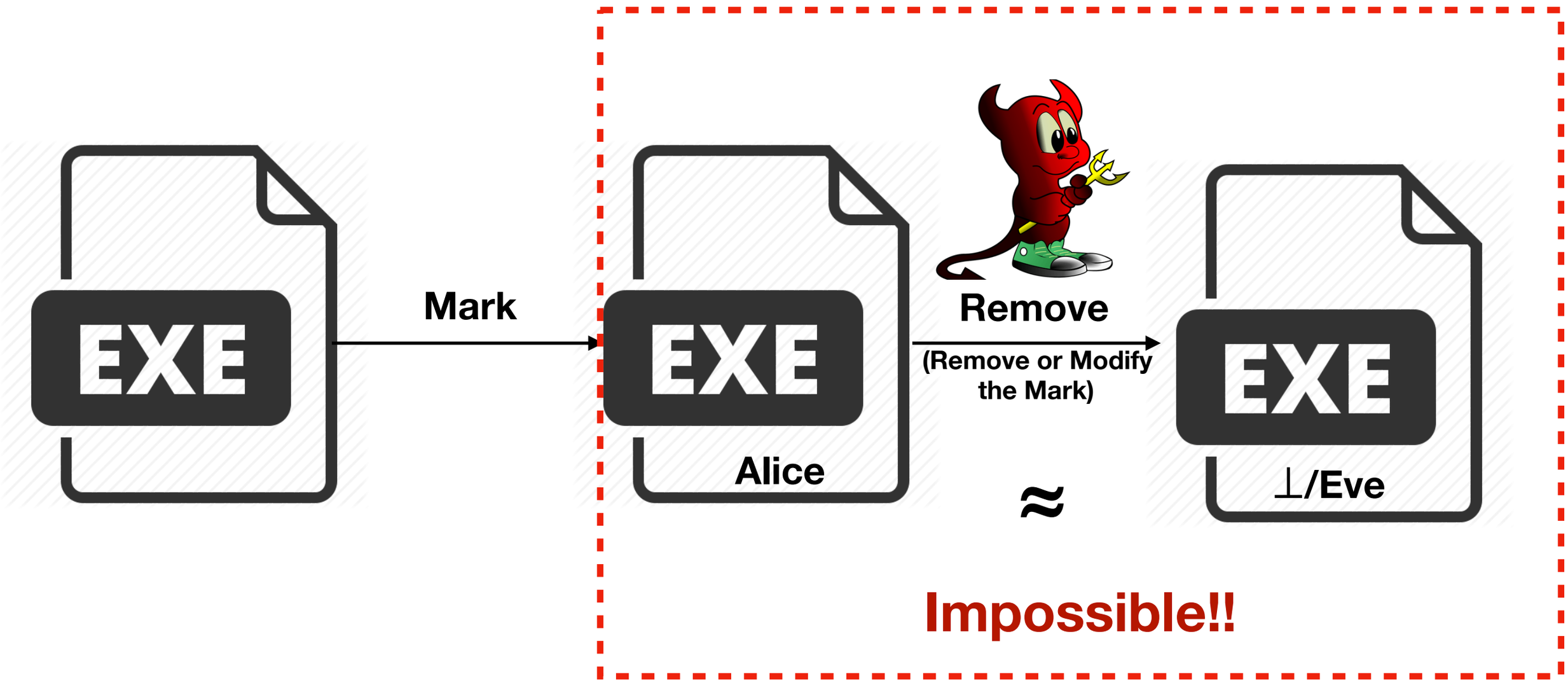
Correctness Requirement： Functionality Preserving

Watermarking A Cryptographic Program



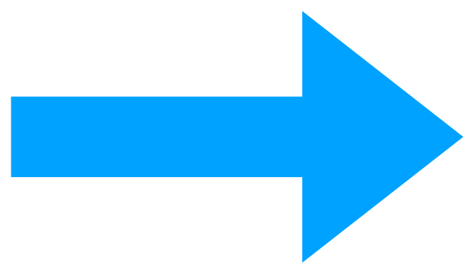
Correctness Requirement： Extraction Correctness

Watermarking A Cryptographic Program



Security Requirement： Unremovability

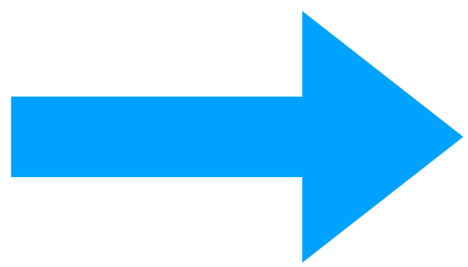
Watermarking A Cryptographic Program



PRF Evaluation
Decryption
Signing
⋮

It is *impossible* to watermark a learnable functionality.

Watermarking A Cryptographic Program



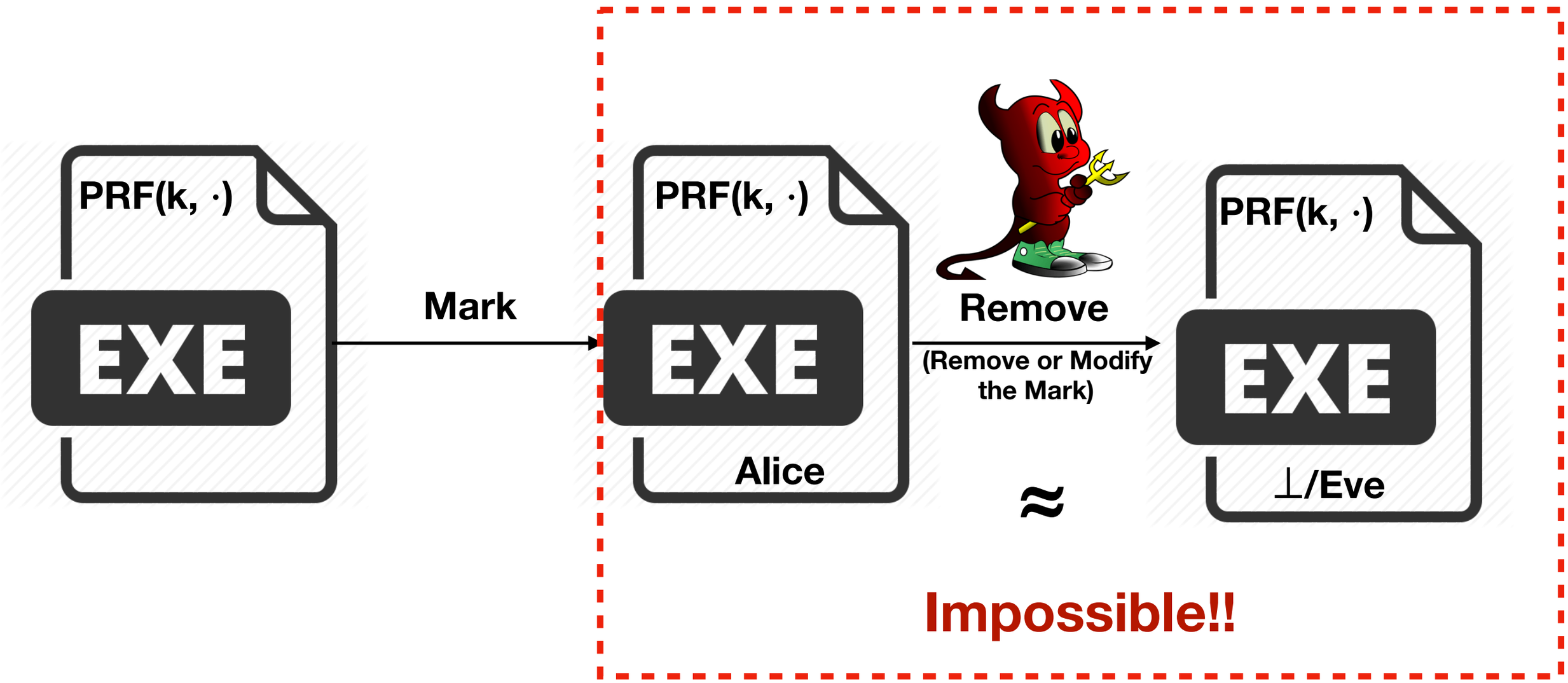
PRF Evaluation
Decryption
Signing
⋮

It is *impossible* to watermark a learnable functionality.

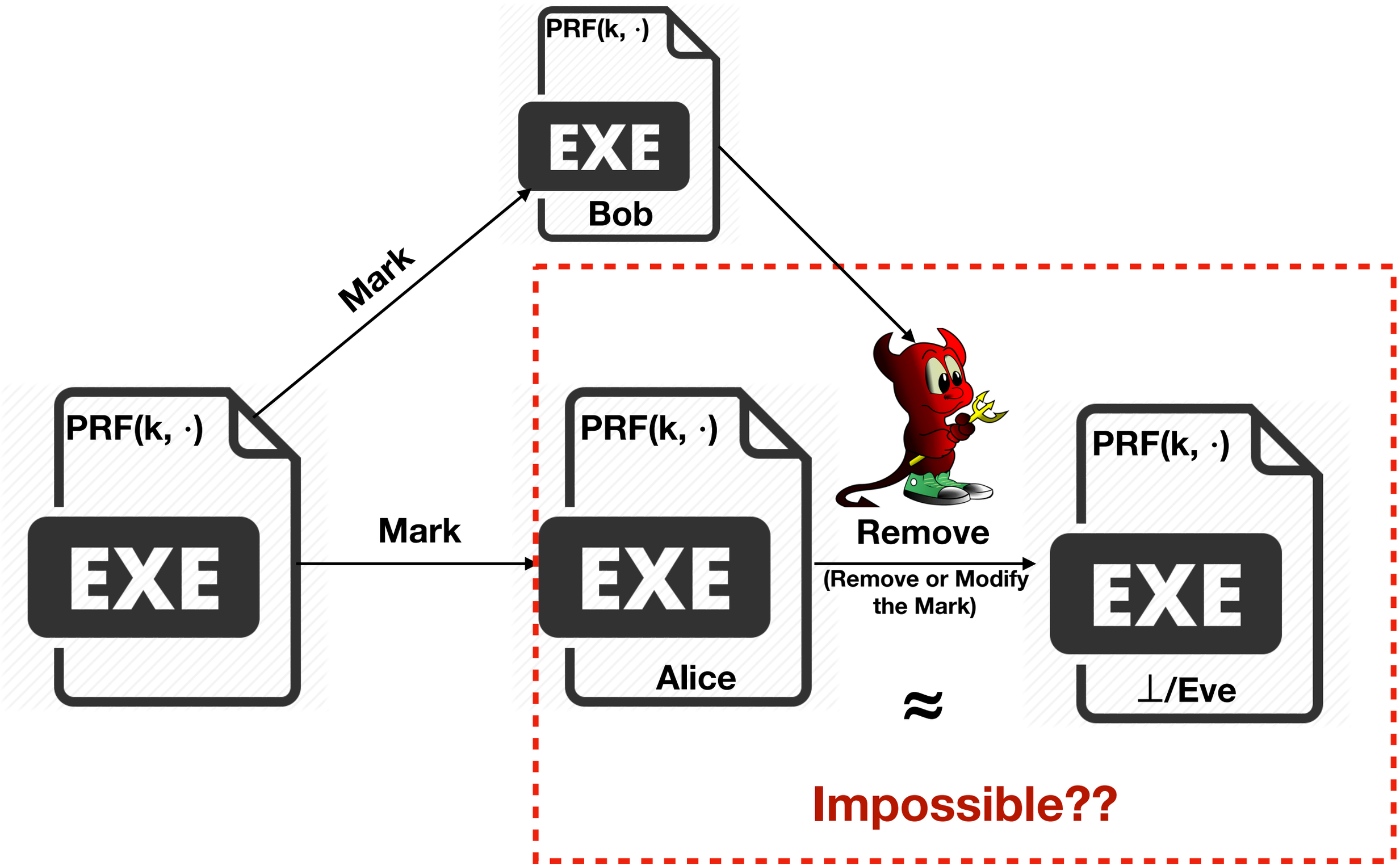
Outline

- Background
- The Problem☞
- Our Result

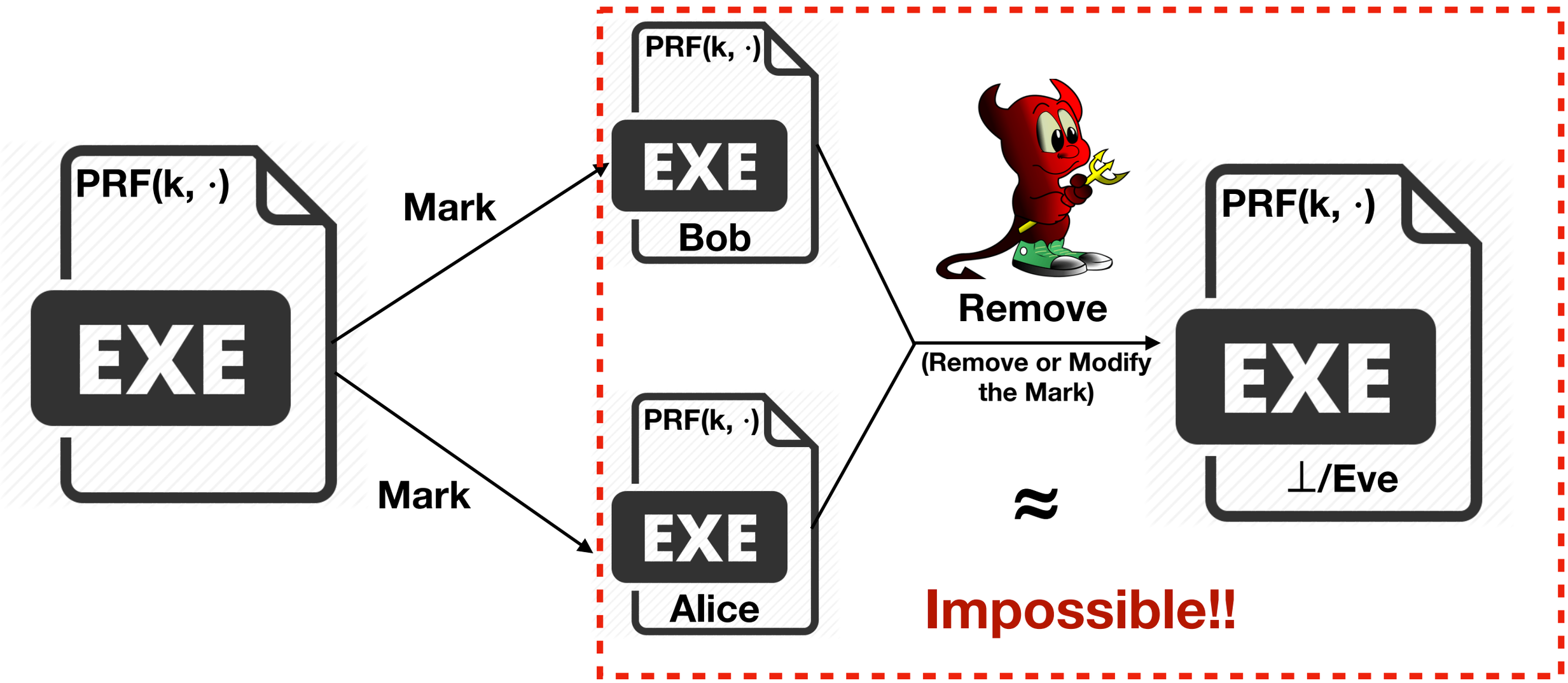
Unremovability, Revisited



Unremovability, Revisited



Collusion Resilient Watermarking

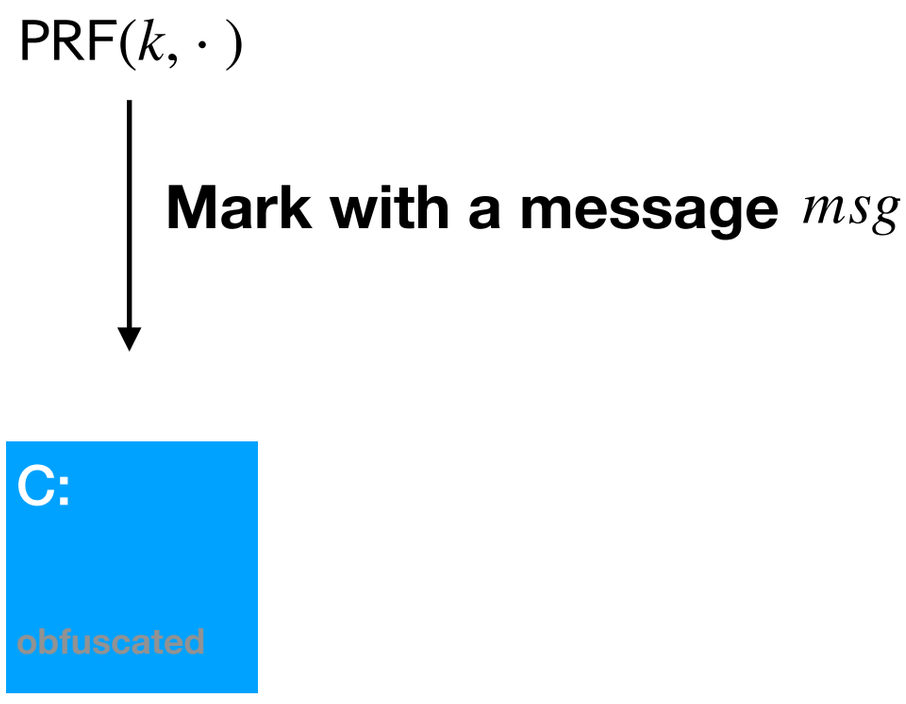


New Security Requirement： ***Collusion Resilient Unremovability***

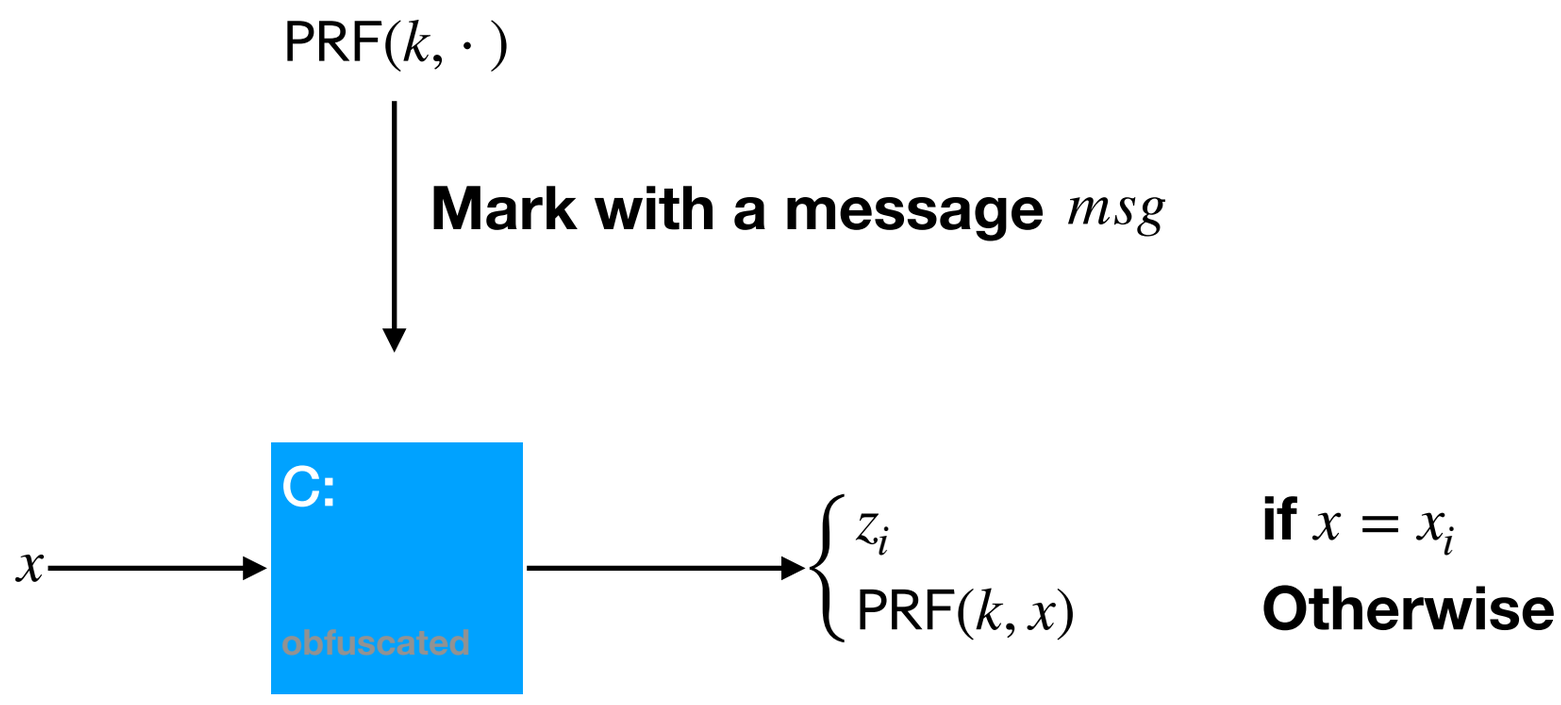
Outline

- Background
- The Problem
- Our Result☞

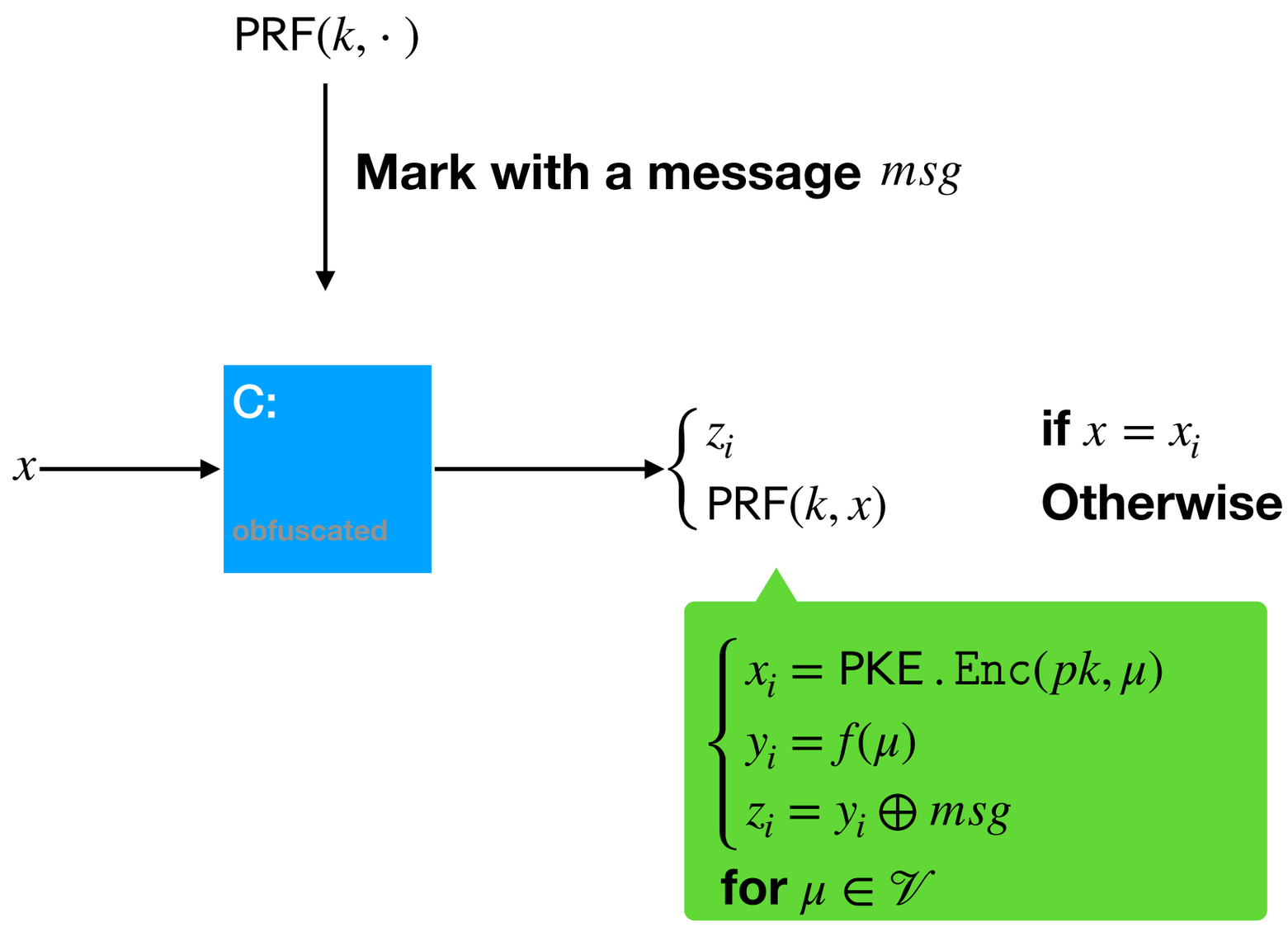
Warmup: The Watermarking Scheme in [CHN+ 16]



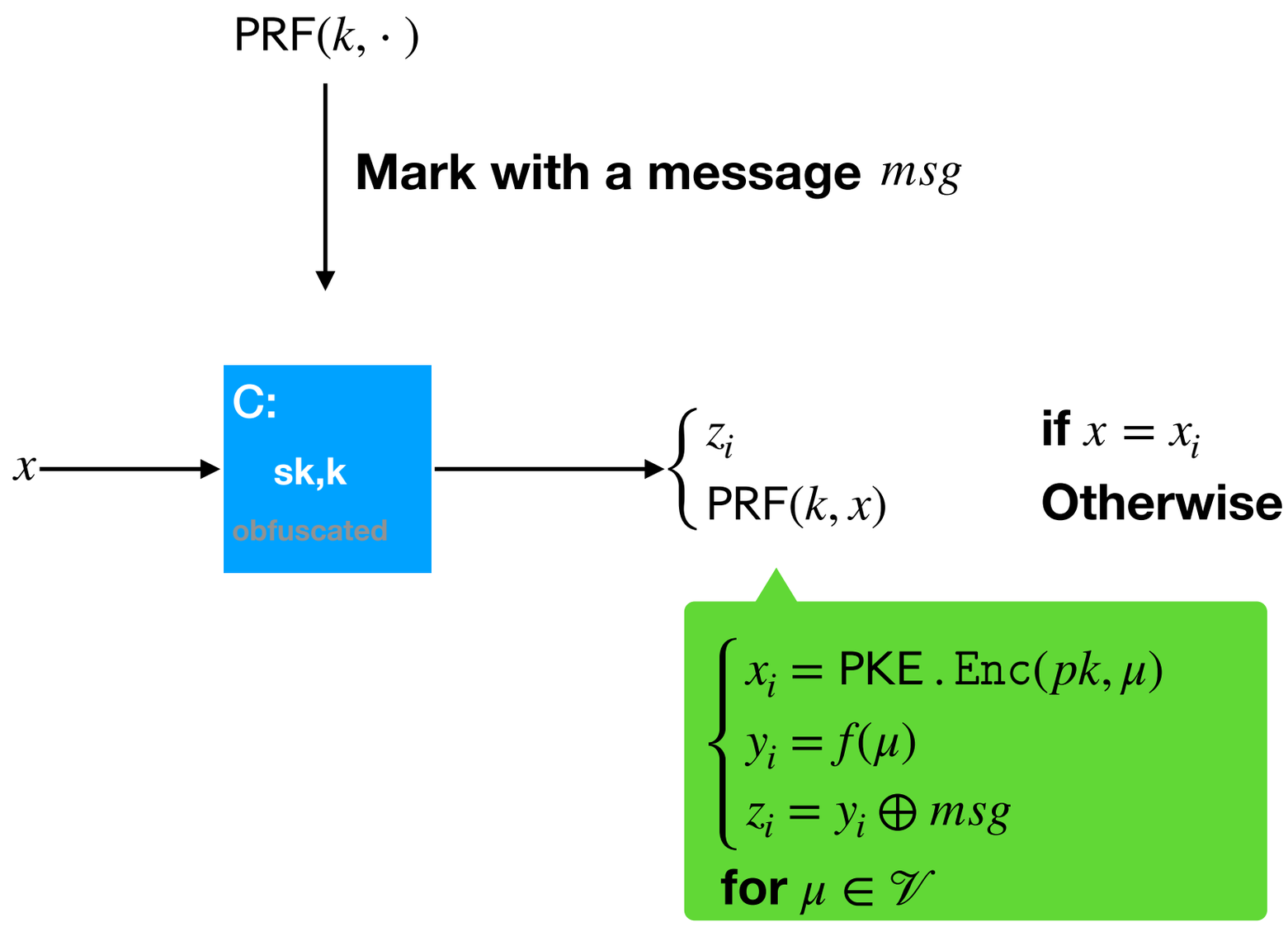
Warmup: The Watermarking Scheme in [CHN+ 16]



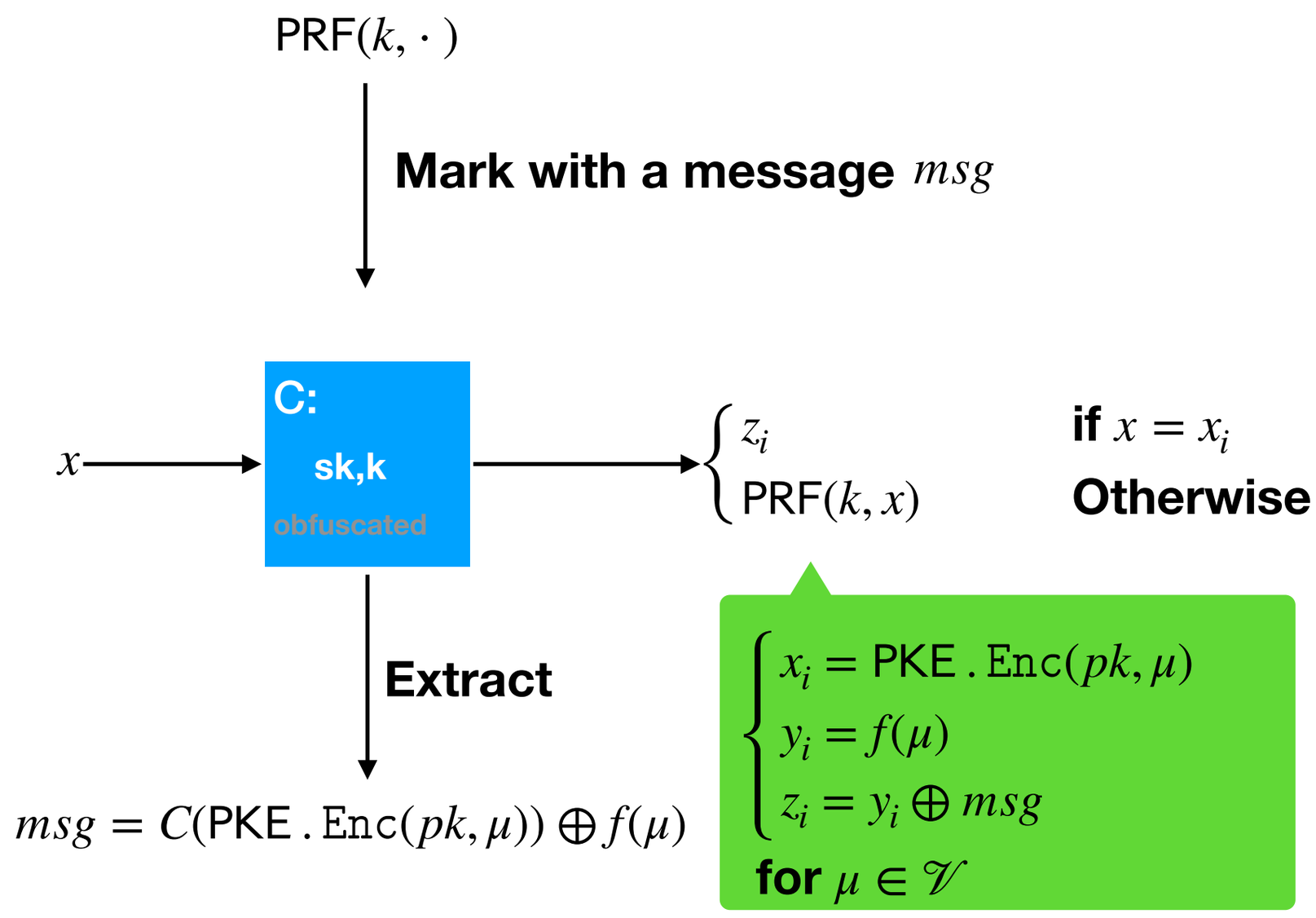
Warmup: The Watermarking Scheme in [CHN+ 16]



Warmup: The Watermarking Scheme in [CHN+ 16]

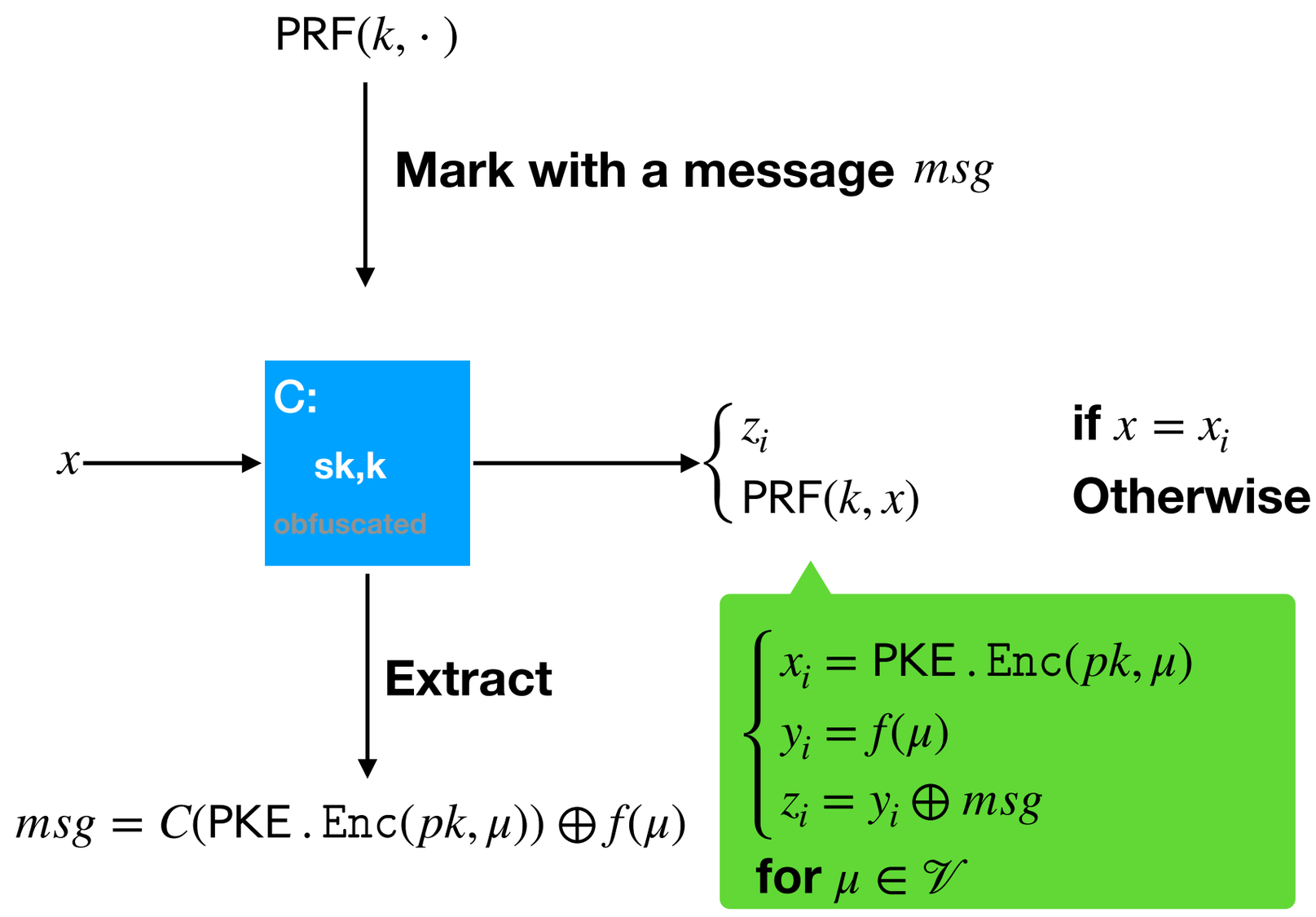


Warmup: The Watermarking Scheme in [CHN+ 16]



Warmup: The Watermarking Scheme in [CHN+ 16]

Security comes from hidden of x_i



Warmup: The Watermarking Scheme in [CHN+ 16]

Security comes from hidden of x_i

1. **Security of Obfuscation**
2. **Security of PKE**

$\mathsf{PRF}(k, \cdot)$

Mark with a message msg

x → **C:** **sk,k** **obfuscated** →

$$\begin{cases} z_i & \textbf{if } x = x_i \\ \mathsf{PRF}(k, x) & \textbf{Otherwise} \end{cases}$$

Extract

$$msg = C(\mathsf{PKE}.\mathtt{Enc}(pk, \mu)) \oplus f(\mu)$$

$$\begin{cases} x_i = \mathsf{PKE}.\mathtt{Enc}(pk, \mu) \\ y_i = f(\mu) \\ z_i = y_i \oplus msg \end{cases}$$

for $\mu \in \mathscr{V}$

Warmup: The Watermarking Scheme in [CHN+ 16]

~~Security comes from hidden of x_i~~

Collusion Attacks

1. **Security of Obfuscation**
2. **Security of PKE**

$\mathsf{PRF}(k, \cdot)$

Mark with a message msg

x → **C:** **sk,k** obfuscated → $\begin{cases} z_i & \textbf{if } x = x_i \\ \mathsf{PRF}(k, x) & \textbf{Otherwise} \end{cases}$

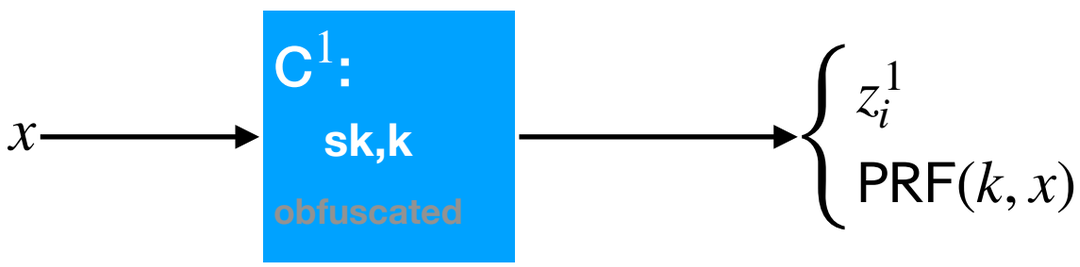
Extract

$$msg = C(\mathsf{PKE}.\mathtt{Enc}(pk, \mu)) \oplus f(\mu)$$

$$\begin{cases} x_i = \mathsf{PKE}.\mathtt{Enc}(pk, \mu) \\ y_i = f(\mu) \\ z_i = y_i \oplus msg \end{cases}$$

for $\mu \in \mathscr{V}$

A Collusion Attack

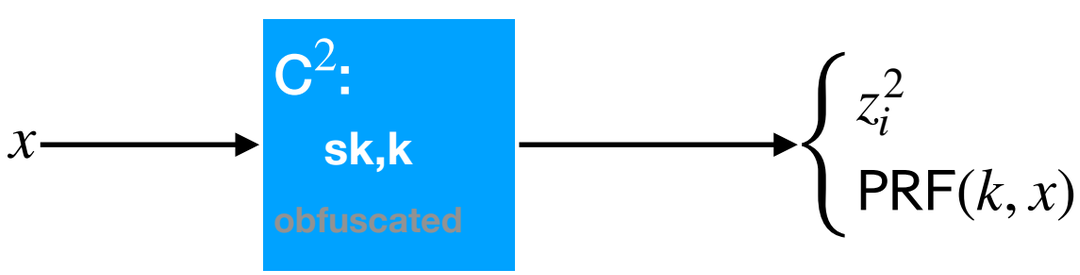


if $x = x_i$

Otherwise

$$\begin{cases} x_i = \text{PKE}.\texttt{Enc}(pk, \mu) \\ y_i = f(\mu) \\ z_i^1 = y_i \oplus msg^1 \end{cases}$$

for $\mu \in \mathscr{V}$



if $x = x_i$

Otherwise

$$\begin{cases} x_i = \text{PKE}.\texttt{Enc}(pk, \mu) \\ y_i = f(\mu) \\ z_i^2 = y_i \oplus msg^2 \end{cases}$$

for $\mu \in \mathscr{V}$

A Collusion Attack

$x \longrightarrow$ **C^1:** **sk,k** obfuscated $\longrightarrow \begin{cases} z_i^1 & \textbf{if } x = x_i \\ \mathsf{PRF}(k, x) & \textbf{Otherwise} \end{cases}$

$$\begin{cases} x_i = \mathsf{PKE}.\mathtt{Enc}(pk, \mu) \\ y_i = f(\mu) \\ z_i^1 = y_i \oplus msg^1 \end{cases}$$

for $\mu \in \mathscr{V}$

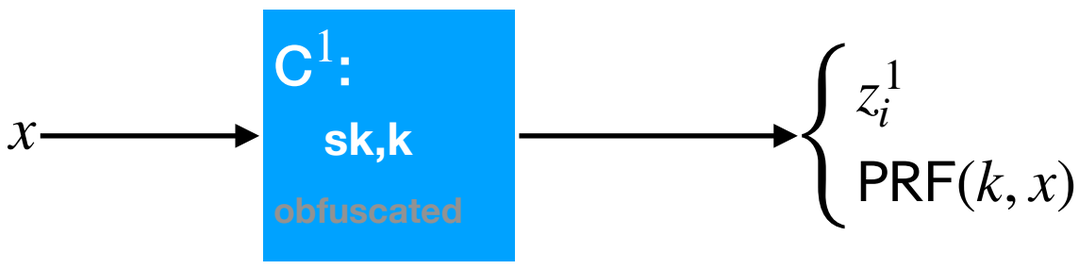
$$\begin{cases} \mathbf{C}^1(x) \neq \mathbf{C}^2(x) & \textbf{if } x = x_i \\ \mathbf{C}^1(x) = \mathbf{C}^2(x) & \textbf{Otherwise} \end{cases}$$

$x \longrightarrow$ **C^2:** **sk,k** obfuscated $\longrightarrow \begin{cases} z_i^2 & \textbf{if } x = x_i \\ \mathsf{PRF}(k, x) & \textbf{Otherwise} \end{cases}$

$$\begin{cases} x_i = \mathsf{PKE}.\mathtt{Enc}(pk, \mu) \\ y_i = f(\mu) \\ z_i^2 = y_i \oplus msg^2 \end{cases}$$

for $\mu \in \mathscr{V}$

A Collusion Attack

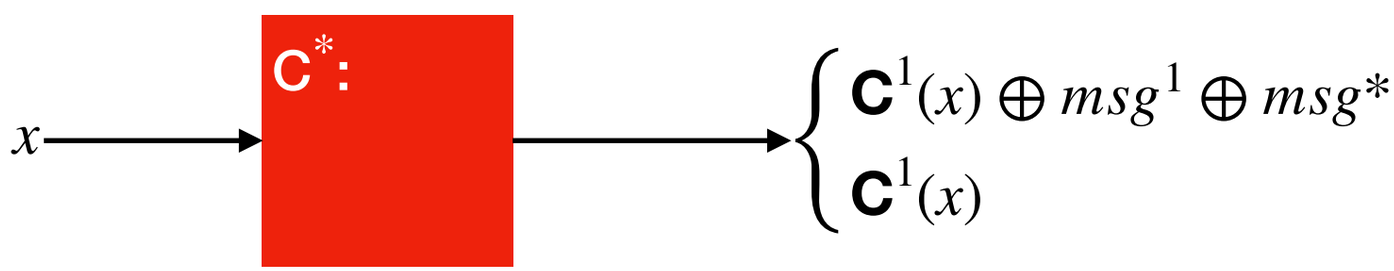


if $x = x_i$

Otherwise

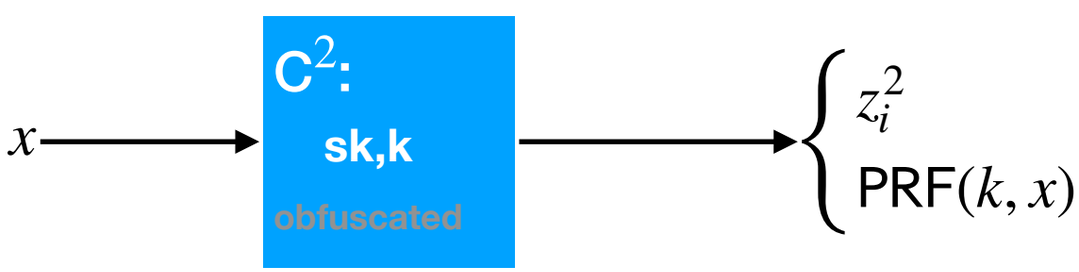
$$\begin{cases} x_i = \text{PKE}.\texttt{Enc}(pk, \mu) \\ y_i = f(\mu) \\ z_i^1 = y_i \oplus msg^1 \end{cases}$$

for $\mu \in \mathscr{V}$



if $\mathbf{C}^1(x) \neq \mathbf{C}^2(x)$

Otherwise



if $x = x_i$

Otherwise

$$\begin{cases} x_i = \text{PKE}.\texttt{Enc}(pk, \mu) \\ y_i = f(\mu) \\ z_i^2 = y_i \oplus msg^2 \end{cases}$$

for $\mu \in \mathscr{V}$

A Collusion Attack

The attack strategy works for all previous watermarkable PRFs.
[CHN+16, BLW17, KW17, PS18, YAL+18, QWZ18, KW19]

A Collusion Attack

Q: Why the collusion attack works?

A: The collusion attacker is able to:

1. locate some/all punctured points;
2. modify/remove the embedded message via resetting outputs on located punctured points.

The attack strategy works for all previous watermarkable PRFs.
[CHN+16, BLW17, KW17, PS18, YAL+18, QWZ18, KW19]

A Collusion Attack

Q: Why the collusion attack works?

A: The collusion attacker is able to:

1. locate some/all punctured points;
2. modify/remove the embedded message via resetting outputs on located punctured points.

Unavoidable if black-box extraction is required.

We need a robust way for message embedding to prevent this.

Our Solution

$\mathsf{PRF}(k, \cdot)$

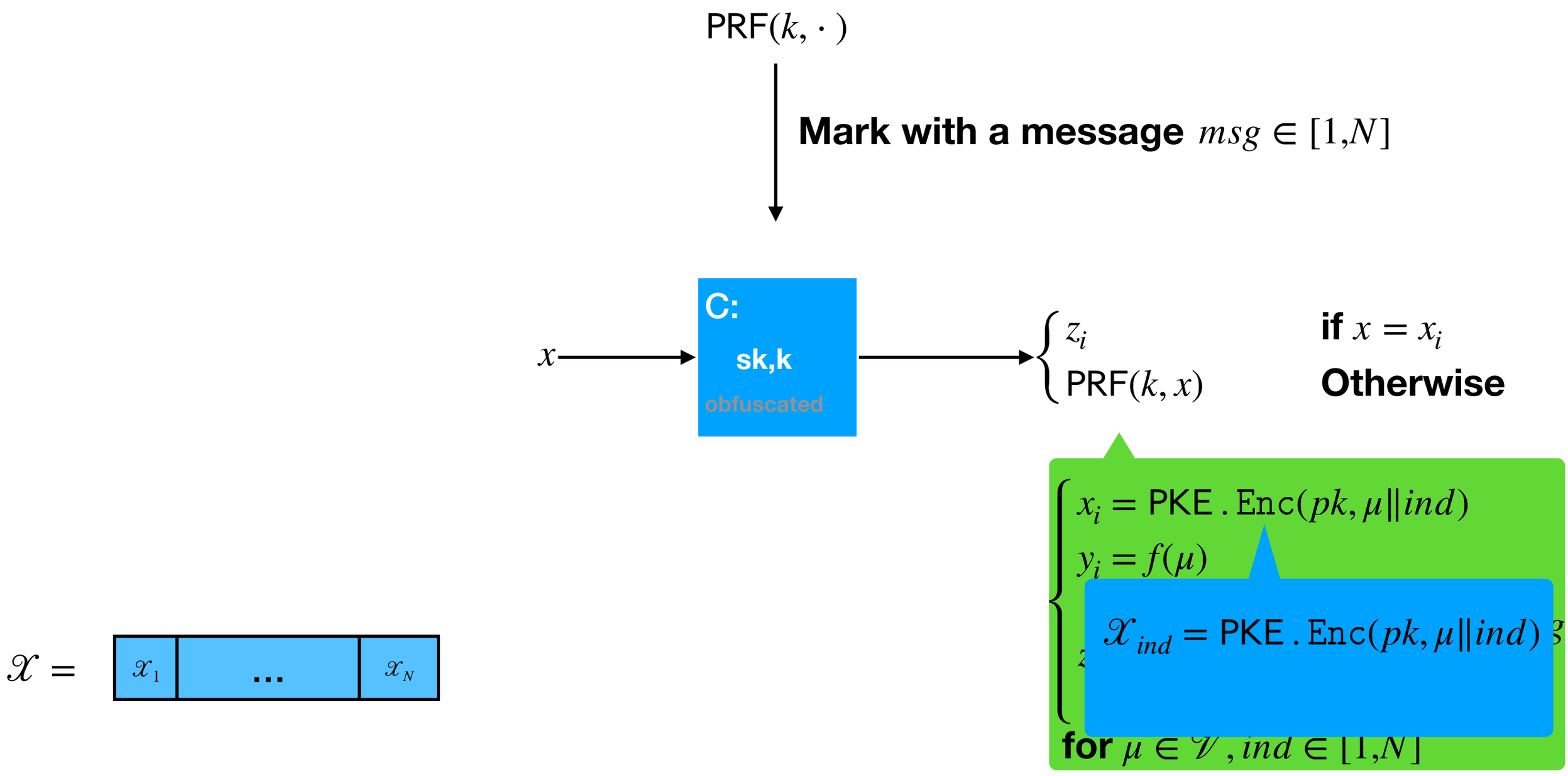
Mark with a message $msg \in [1,N]$

$x \longrightarrow$ **C:** **sk,k** **obfuscated** $\longrightarrow \begin{cases} z_i & \textbf{if } x = x_i \\ \mathsf{PRF}(k, x) & \textbf{Otherwise} \end{cases}$

$$\begin{cases} x_i = \mathsf{PKE}.\mathtt{Enc}(pk, \mu \| ind) \\ y_i = f(\mu) \\ z_i = \begin{cases} y_i & \textbf{if } ind \leq msg \\ \mathsf{PRF}(k, x_i) & \textbf{Otherwise} \end{cases} \end{cases}$$

for $\mu \in \mathscr{V}, ind \in [1,N]$

Our Solution



Our Solution

$\mathsf{PRF}(k, \cdot)$

Mark with a message $msg \in [1,N]$

$x \longrightarrow$ **C:** **sk,k** **obfuscated** $\longrightarrow \begin{cases} z_i & \textbf{if } x = x_i \\ \mathsf{PRF}(k, x) & \textbf{Otherwise} \end{cases}$

$$\begin{cases} x_i = \mathsf{PKE}.\mathtt{Enc}(pk, \mu \| ind) \\ y_i = f(\mu) \\ z_i = \begin{cases} y_i & \textbf{if } ind \leq msg \\ \mathsf{PRF}(k, x_i) & \textbf{Otherwise} \end{cases} \end{cases}$$

for $\mu \in \mathscr{V}, ind \in [1,N]$

$\mathscr{X} =$

$\mathscr{X}_1$	...	$\mathscr{X}_{msg}$	...	$\mathscr{X}_N$

Reprogrammed Unreprogrammed

Our Solution

$\mathsf{PRF}(k, \cdot)$

Mark with a message $msg \in [1,N]$

x → **C:** **sk,k** obfuscated → $\begin{cases} z_i & \textbf{if } x = x_i \\ \mathsf{PRF}(k, x) & \textbf{Otherwise} \end{cases}$

Extract

$p_0 = 1, p_{N+1} = 0$

$\forall ind \in [1,N], p_{ind} = \dfrac{\|\{x_i : C(x_i) = y_i\}\|}{\|\mathcal{X}_{ind}\|}$

Out ind **s.t.** $p_{ind} - p_{ind+1}$ **is large**

$$\begin{cases} x_i = \mathsf{PKE}.\mathtt{Enc}(pk, \mu \| ind) \\ y_i = f(\mu) \\ z_i = \begin{cases} y_i & \textbf{if } ind \leq msg \\ \mathsf{PRF}(k, x_i) & \textbf{Otherwise} \end{cases} \end{cases}$$

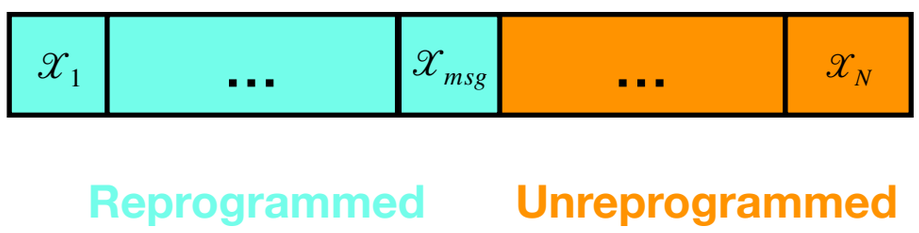
for $\mu \in \mathcal{V}, ind \in [1,N]$

Our Solution

$\mathsf{PRF}(k, \cdot)$

Mark with a message $msg \in [1,N]$

x → **C:** **sk,k** obfuscated → $\begin{cases} z_i & \textbf{if } x = x_i \\ \mathsf{PRF}(k, x) & \textbf{Otherwise} \end{cases}$



Extract

$$p_0 = 1, p_{N+1} = 0$$

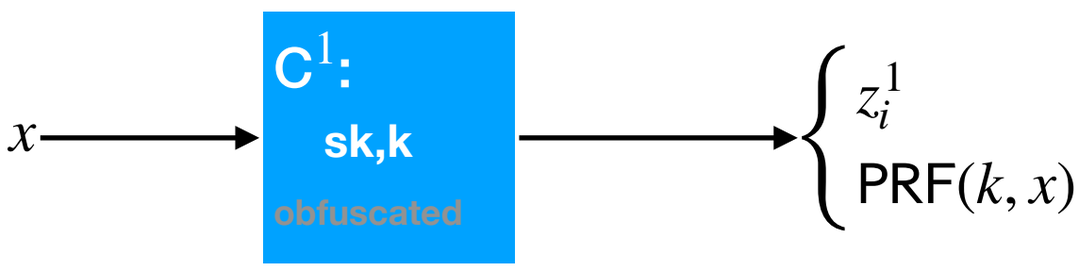
$$\forall ind \in [1,N], p_{ind} = \frac{\|\{x_i : C(x_i) = y_i\}\|}{\|\mathscr{X}_{ind}\|}$$

Out ind **s.t.** $p_{ind} - p_{ind+1}$ **is large**

$$\begin{cases} x_i = \mathsf{PKE}.\mathtt{Enc}(pk, \mu \| ind) \\ y_i = f(\mu) \\ z_i = \begin{cases} y_i & \textbf{if } ind \leq msg \\ \mathsf{PRF}(k, x_i) & \textbf{Otherwise} \end{cases} \end{cases}$$

for $\mu \in \mathscr{V}, ind \in [1,N]$

Security of Our Solution

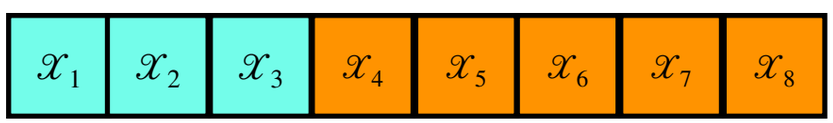


if $x = x_i$

Otherwise

$$\begin{cases} x_i = \text{PKE}.\texttt{Enc}(pk, \mu \| ind) \\ y_i = f(\mu) \\ z_i^1 = \begin{cases} y_i & \textbf{if } ind \leq 3 \\ \text{PRF}(k, x_i) & \textbf{Otherwise} \end{cases} \end{cases}$$

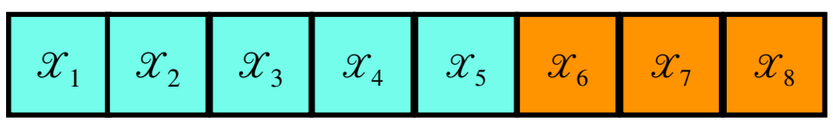
for $\mu \in \mathscr{V}, ind \in [1,N]$

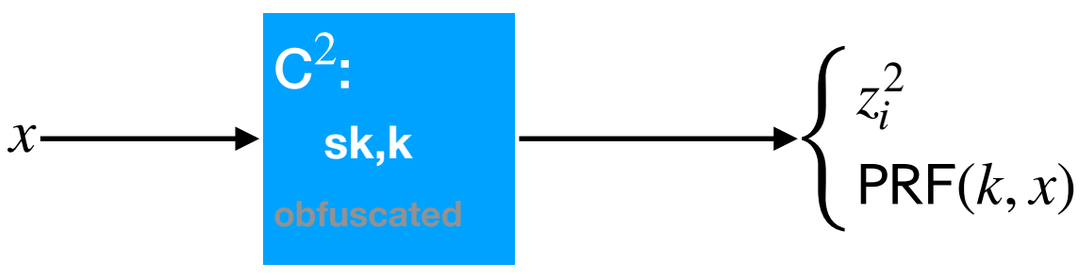


$N = 8$

$msg^1 = 3$

$msg^2 = 5$





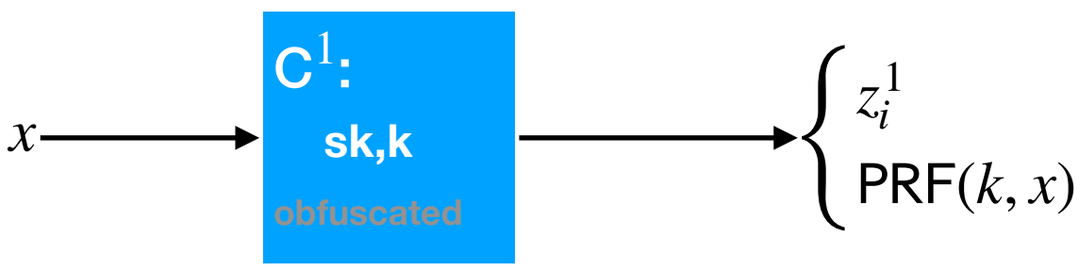
if $x = x_i$

Otherwise

$$\begin{cases} x_i = \text{PKE}.\texttt{Enc}(pk, \mu \| ind) \\ y_i = f(\mu) \\ z_i^2 = \begin{cases} y_i & \textbf{if } ind \leq 5 \\ \text{PRF}(k, x_i) & \textbf{Otherwise} \end{cases} \end{cases}$$

for $\mu \in \mathscr{V}, ind \in [1,N]$

Security of Our Solution

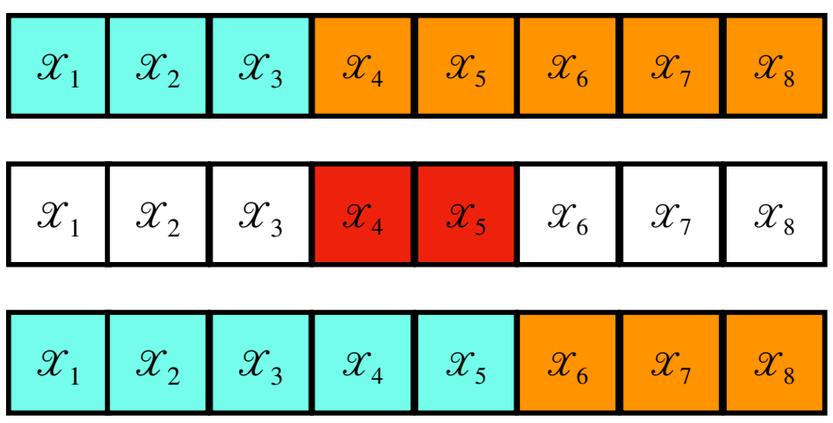


if $x = x_i$

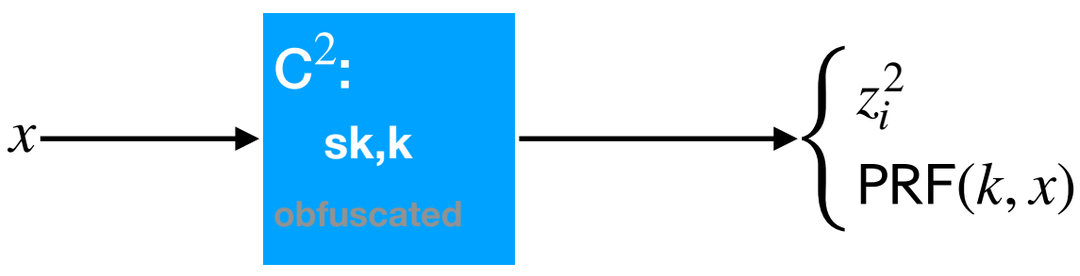
Otherwise

$$\begin{cases} x_i = \text{PKE}.\texttt{Enc}(pk, \mu \| ind) \\ y_i = f(\mu) \\ z_i^1 = \begin{cases} y_i & \textbf{if } ind \leq 3 \\ \text{PRF}(k, x_i) & \textbf{Otherwise} \end{cases} \end{cases}$$

for $\mu \in \mathscr{V}, ind \in [1,N]$



$$N = 8$$
$$msg^1 = 3$$
$$msg^2 = 5$$



if $x = x_i$

Otherwise

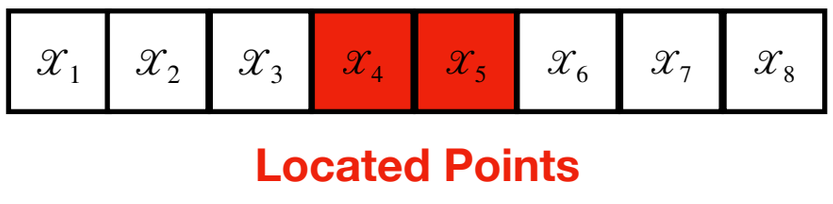
$$\begin{cases} x_i = \text{PKE}.\texttt{Enc}(pk, \mu \| ind) \\ y_i = f(\mu) \\ z_i^2 = \begin{cases} y_i & \textbf{if } ind \leq 5 \\ \text{PRF}(k, x_i) & \textbf{Otherwise} \end{cases} \end{cases}$$

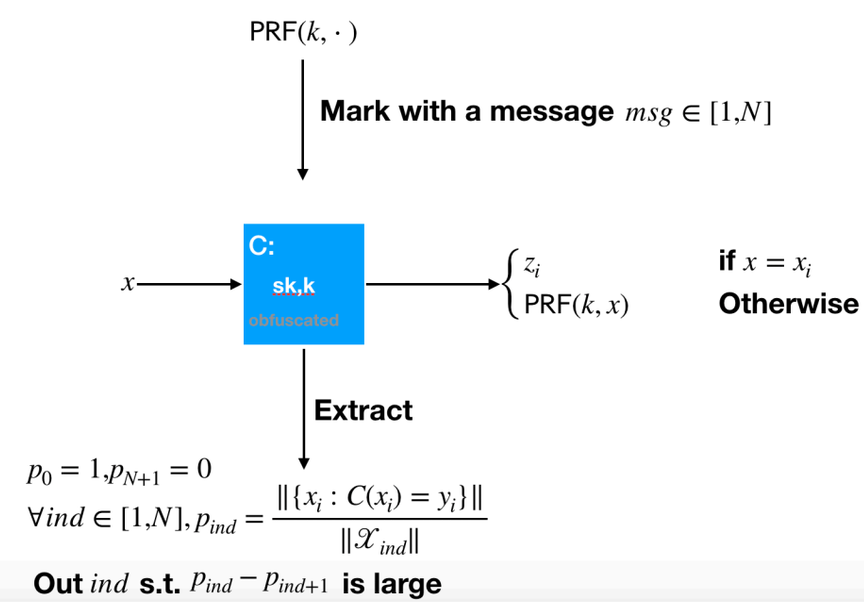
for $\mu \in \mathscr{V}, ind \in [1,N]$

Security of Our Solution

The adversary cannot reset outputs on an input x for $x \in \mathcal{X}_{ind}$, where $ind \notin [4,5]$.
($p_1, p_2, p_3 \approx 1, \;\; p_6, p_7, p_8 \approx 0$)

Security holds if the adversary cannot:
1. distinguish a point in $\mathcal{X}_{ind}$ and a random point for $ind \notin [4,5]$.





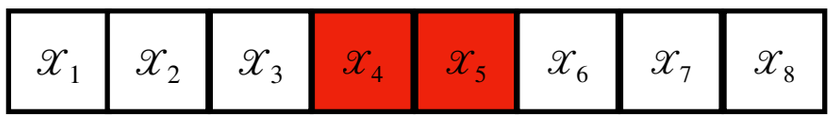
Security of Our Solution

The adversary cannot reset outputs on an input x for $x \in \mathcal{X}_{ind}$, where $ind \notin [4,5]$.
($p_1, p_2, p_3 \approx 1, \;\; p_6, p_7, p_8 \approx 0$)

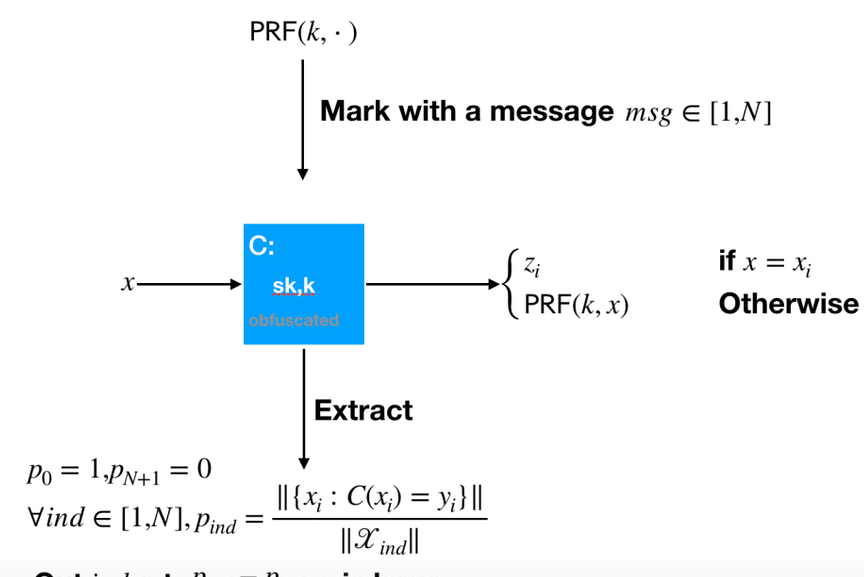
Security holds if the adversary cannot:

1. distinguish a point in $\mathcal{X}_{ind}$ and a random point for $ind \notin [4,5]$.
2. distinguish a point in $\mathcal{X}_4$ and that in $\mathcal{X}_5$.

$| \, p_4 - p_5 \, |$ is small.



Located Points



Security of Our Solution

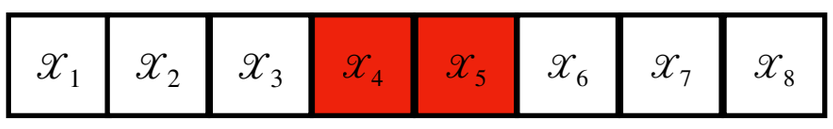
The adversary cannot reset outputs on an input x for $x \in \mathcal{X}_{ind}$, where $ind \notin [4,5]$.
($p_1, p_2, p_3 \approx 1, \;\; p_6, p_7, p_8 \approx 0$)

Security holds if the adversary cannot:

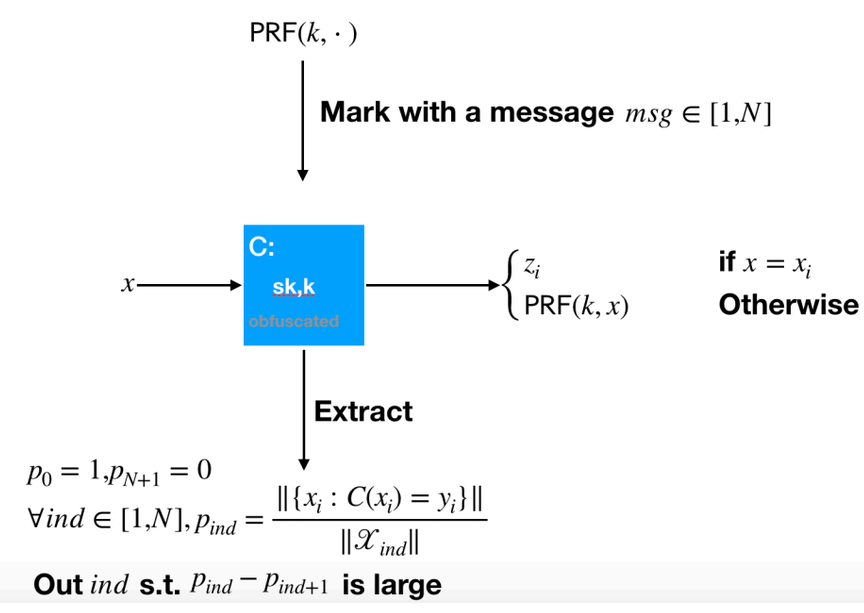
1. distinguish a point in $\mathcal{X}_{ind}$ and a random point for $ind \notin [4,5]$.
2. distinguish a point in $\mathcal{X}_4$ and that in $\mathcal{X}_5$.

$| p_3 - p_4 |$ is large or
$| p_5 - p_6 |$ is large or both

$| p_4 - p_5 |$ is small.



Located Points



Security of Our Solution

Security of Obfuscation and Security of PKE

Security holds if the adversary cannot:

1. distinguish a point in $\mathcal{X}_{ind}$ and a random point for $ind \notin [4,5]$.
2. distinguish a point in $\mathcal{X}_4$ and that in $\mathcal{X}_5$.

$\mathcal{X}_1$	$\mathcal{X}_2$	$\mathcal{X}_3$	$\mathcal{X}_4$	$\mathcal{X}_5$	$\mathcal{X}_6$	$\mathcal{X}_7$	$\mathcal{X}_8$

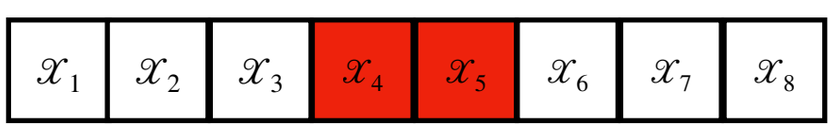
Located Points

Security of Our Solution

Security holds if the adversary cannot:

1. distinguish a point in $\mathscr{X}_{ind}$ and a random point for $ind \notin [4,5]$.
2. distinguish a point in $\mathscr{X}_4$ and that in $\mathscr{X}_5$.

Security of PKE is not enough, use Function Encryption instead (Actually, puncturable functional encryption presented in this work).
Security of Obfuscation is also needed.



Located Points

Conclusion

👎: All previous watermarkable PRF is not secure under collusion attacks.

👍: We present a new approach to embed messages in the watermarking setting and construct collusion resistant watermarkable PRF.

Conclusion

👎: All previous watermarkable PRF is not secure under collusion attacks.
👍: We present a new approach to embed messages in the watermarking setting and construct collusion resistant watermarkable PRF.

What is not covered in this talk:

1. How to deal with exponentially large message space.
2. How to construct puncturable functional encryption.
3. How to construct collusion resistant watermarking schemes for PKE and signature.

Please see our paper ia.cr/2017/1201

THANK YOU!