CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Lockable Obfuscation from Circularly Insecure Fully Homomorphic Encryption

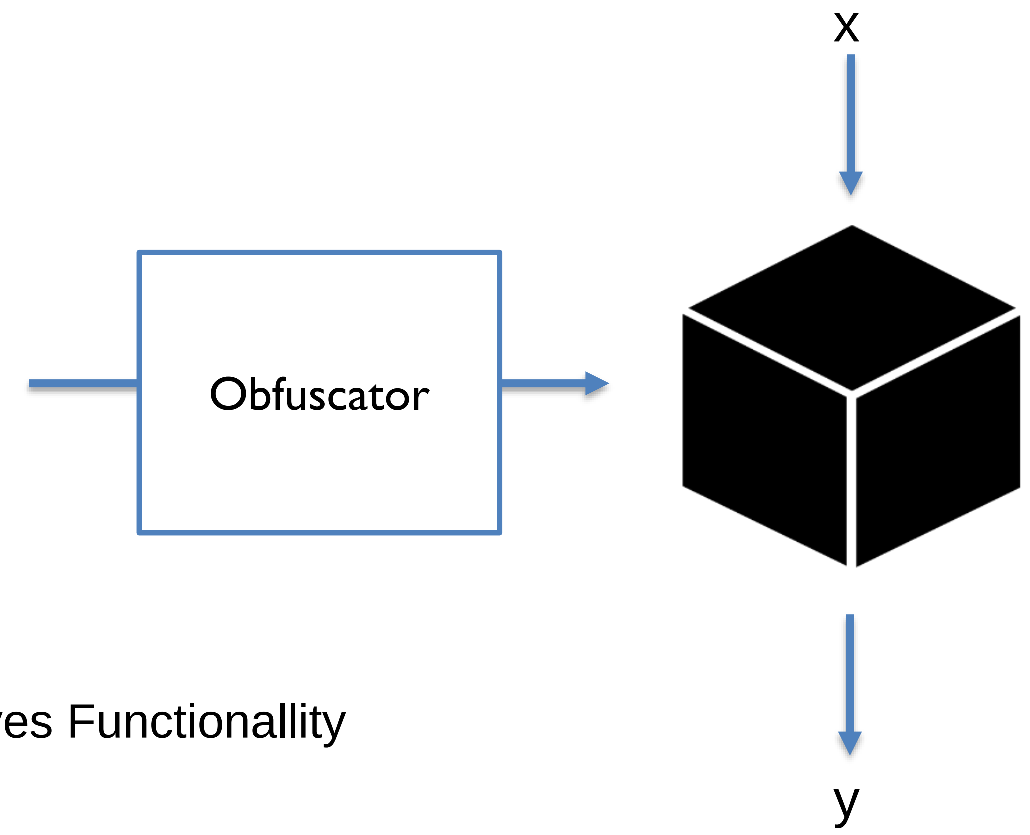
Lockable Obfuscation from Circularly Insecure Fully Homomorphic Encryption

Kamil Kluczniak

Stanford University, CISPA Helmholtz Center For Information Security

Obfuscation

```
int fun(int x){
    int y = (x + 5) % 11;
    return y;
}
```



- Preserves Functionallity

- Polynomial Slowdown

- Virtual Black-Box Secuity

What functions can we obfuscate from Standard Assumptions?

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Point Functions

$$\mathrm{PF}[\alpha](x) = \begin{cases} 1 & \text{if } \; x = \alpha \\ 0 & \text{otherwise} \end{cases}$$

Can97

CRV10

LPS04

GKPV10

DKL09

BS16

CD08

Wee05

KY18

Conjunctions

$$f(x_1, \ldots, x_n) = \neg x_3 \wedge x_5 \wedge \neg x_9 \wedge x_n$$

BR13

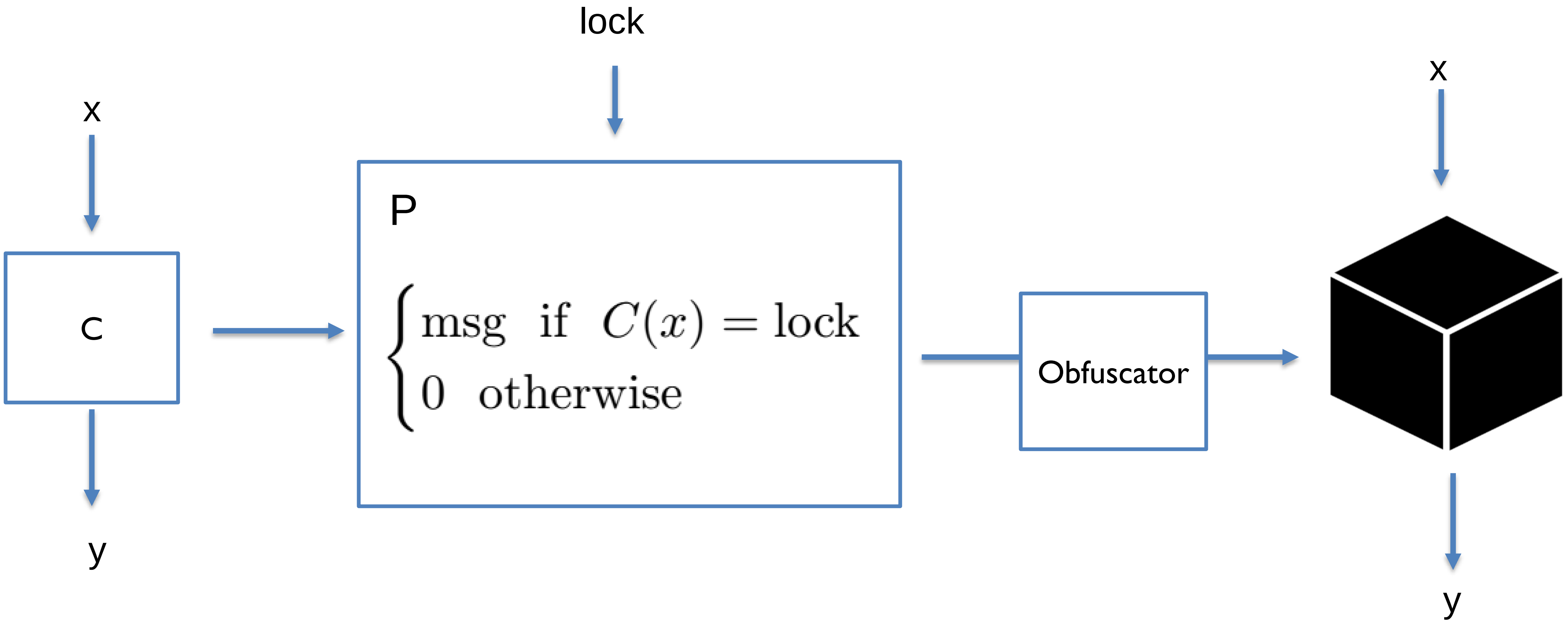
BKM+18

BVWW16

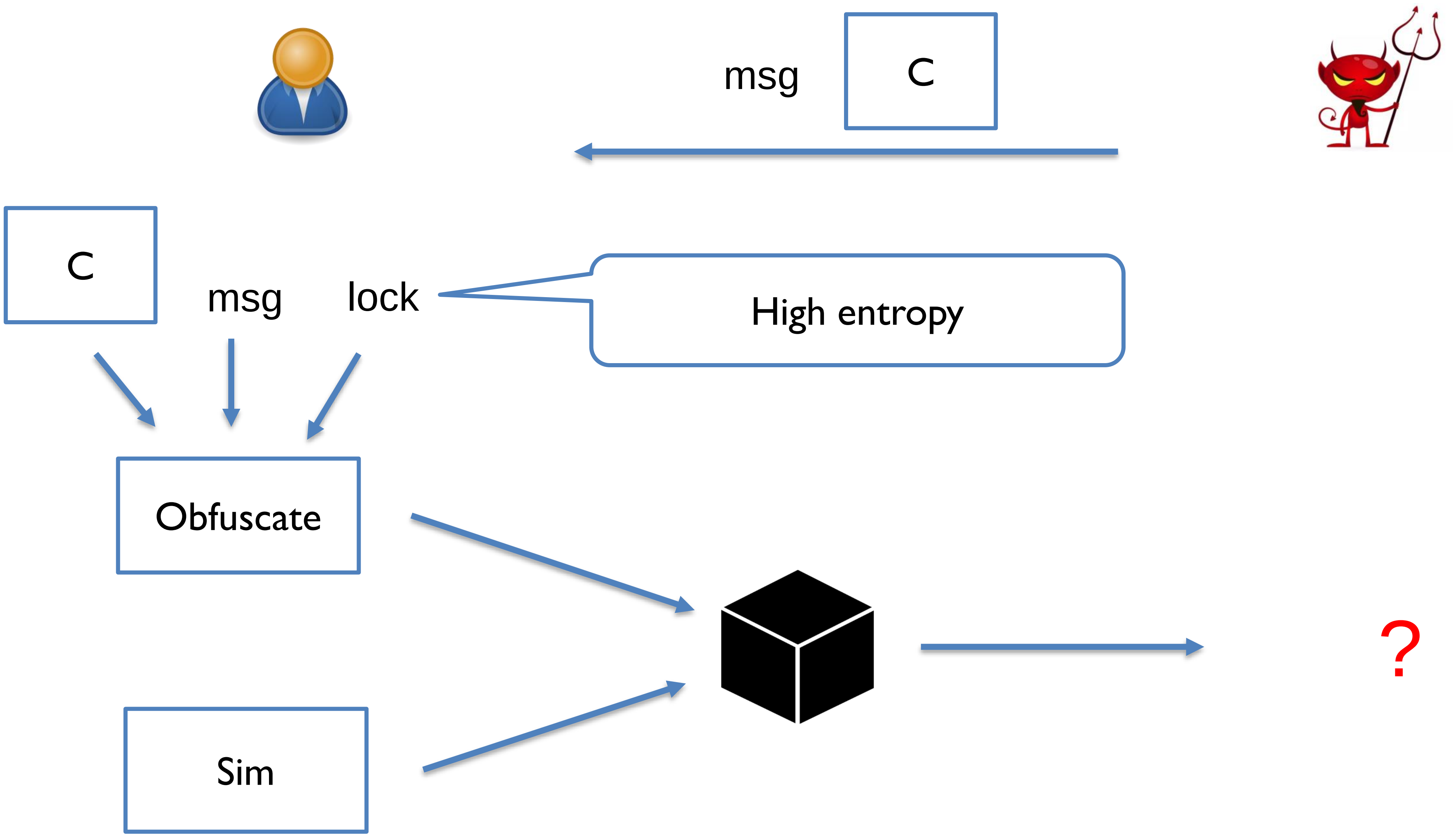
BW19

BLMZ19

Lockable Obfuscation: Obfuscating Compute-and-Compare Programs



Distributional Virtual Black-Box Security



Applications of Lockable Obfuscation

- Implications

Lockable Obfuscation ⟹ Point Obfuscation

Lockable Obfuscation ⟹ Conjunction Obfuscation

- Compilers

PKE + Lockable Obfuscation ⟹ Anonymous PKE

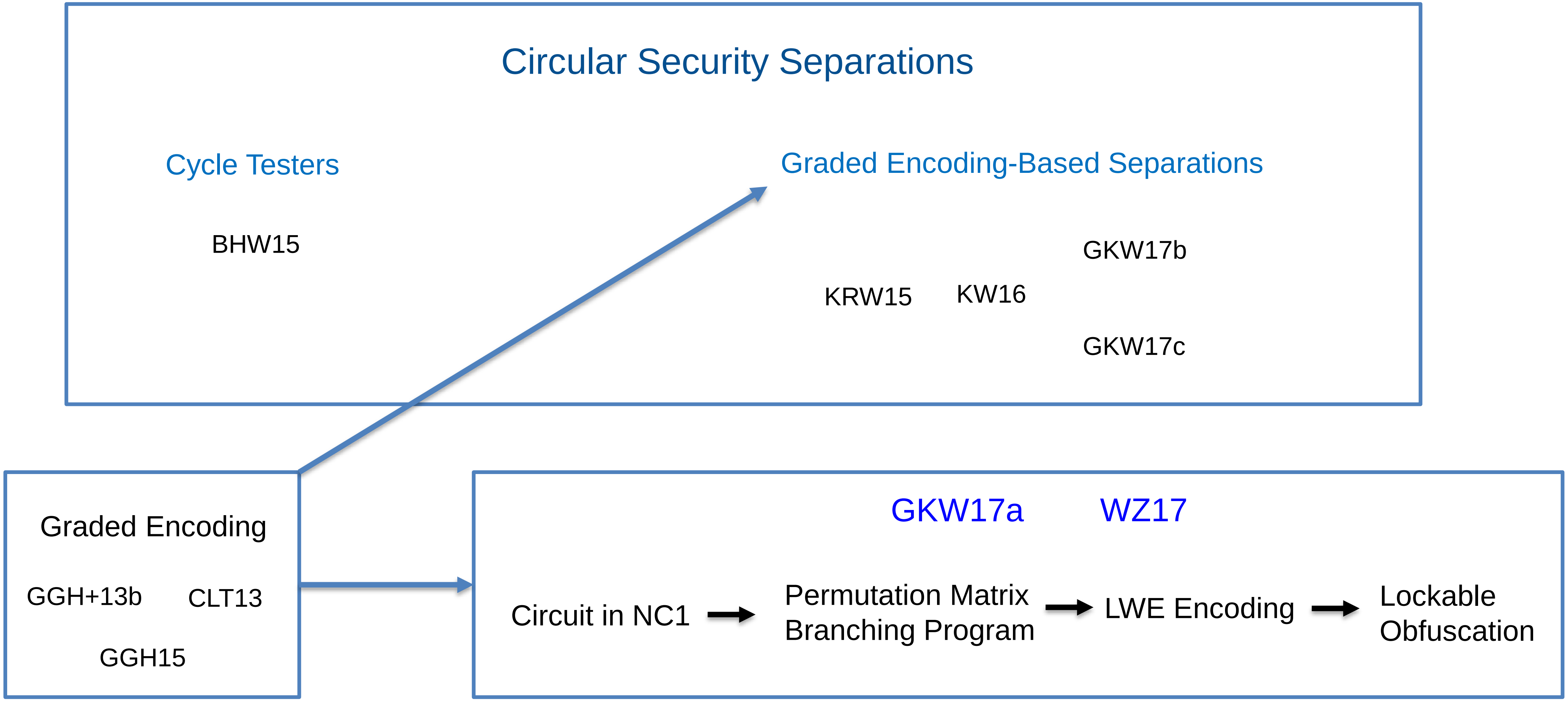
IBE + Lockable Obfuscation ⟹ Anonymous IBE

Predicate Encryption + Lockable Obfuscation ⟹ PE with One-Sided Privacy

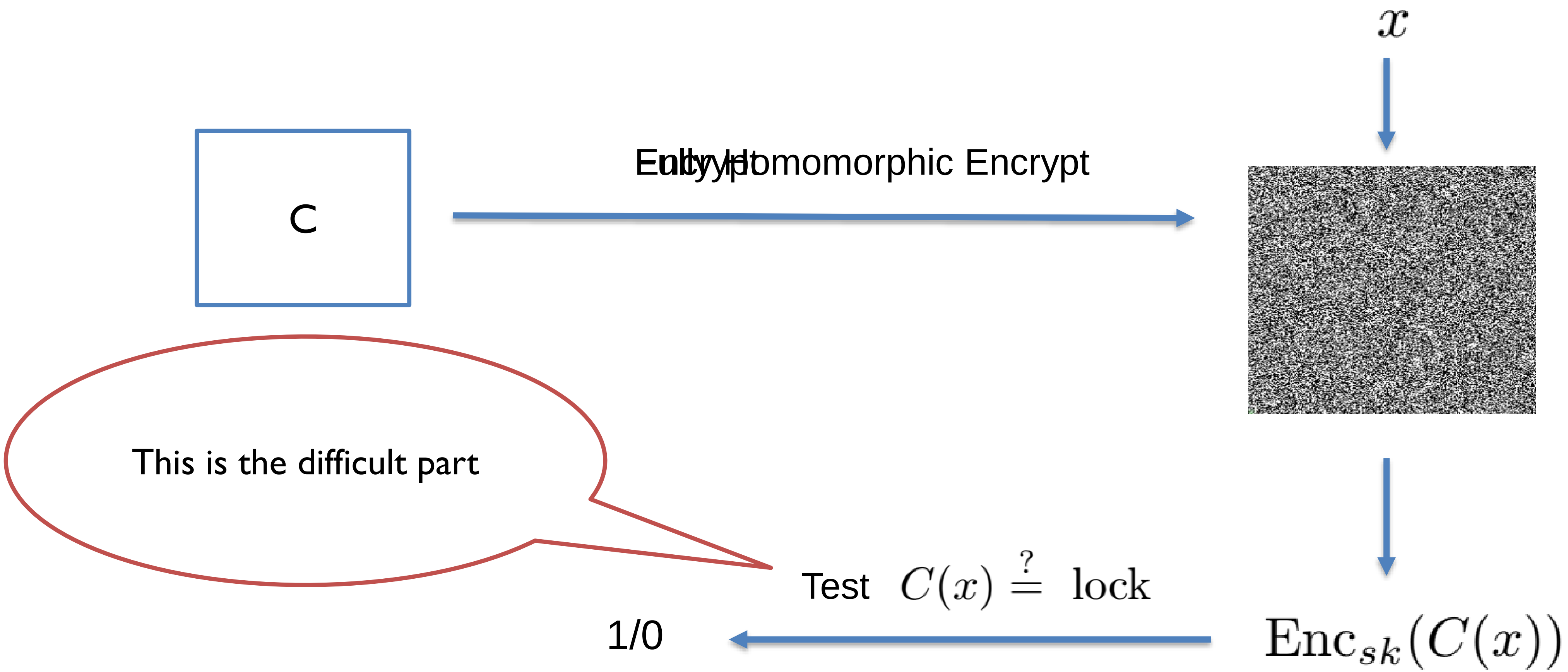
Broadcast Encryption + Lockable Obfuscation ⟹ Anonymous Broadcast Encryption

WE + Lockable Obfuscation ⟹ Indistinguishability Obfuscation for Rejecting Programs

Previous Construtions of Lockable Obfuscation



Intuitively: What is a Lockable Obfuscation?



Our base construction: Testing the Lock

Given $\mathrm{Enc}_{sk}(C(x))$ test $C(x) \stackrel{?}{=} \mathrm{lock}$

Idea: Use a fully homomorphic encryption scheme that is circularly insecure

(Equiped with a cycle tester)

Cycle Testers

$$\mathrm{Enc}_{sk_1}(sk_2), \ldots, \mathrm{Enc}_{sk_n}(sk_1) \not\approx \mathrm{Enc}_{sk_1}(0), \ldots, \mathrm{Enc}_{sk_n}(0)$$

$$\mathrm{Enc}_{sk}(sk) \not\approx \mathrm{Enc}_{sk}(0)$$

Our base construction: Putting Things Together

$$c \leftarrow \mathrm{Enc}_{sk}(C)$$

$$a \leftarrow \mathrm{Enc}_{\mathrm{lock}}(sk)$$

Evaluation

$$\mathrm{Eval}(U_x, c) \quad = \mathrm{Enc}_{sk}(C(x)) \quad = d$$

$$\mathrm{Eval}(\mathrm{Dec}(d, .), a) \quad = \mathrm{Enc}_{sk}(\mathrm{Dec}(C(x), \mathrm{Enc}_{\mathrm{lock}}(sk))) \quad = e$$

$$\text{if} \quad C(x) = \text{lock} \quad e = \mathrm{Enc}_{sk}(sk)$$

$$\text{otherwise} \quad e \neq \mathrm{Enc}_{sk}(sk) \quad \text{w.h.p.}$$

?

Cycle Tester

Security Proof

$$c \leftarrow \mathrm{Enc}_{sk}(C) \qquad a \leftarrow \mathrm{Enc}_{\mathrm{lock}}(sk)$$

↓ IND-CPA

$$c \leftarrow \mathrm{Enc}_{sk}(C) \qquad a \leftarrow \mathrm{Enc}_{\mathrm{lock}}(0)$$

↓ Pseudorandom Ciphertexts

$$c \leftarrow \mathrm{Enc}_{sk}(C) \qquad a \leftarrow \text{uniform random}$$

↓ IND-CPA

$$c \leftarrow \mathrm{Enc}_{sk}(0) \qquad a \leftarrow \text{uniform random}$$

In the paper, we have a version without this assumption

Extension: Distributional Security

$c \leftarrow \mathrm{Enc}_{sk}(C) \qquad a \leftarrow \mathrm{Enc}_{\mathrm{lock}}(sk)$

IND-CPA → Enc may be CPA-secure with respect to key from other distributions (not necessarily uniform)

$c \leftarrow \mathrm{Enc}_{sk}(C) \qquad a \leftarrow \mathrm{Enc}_{\mathrm{lock}}(0)$

Unpredictable Distribution:

$(x, \mathsf{aux}) \leftarrow_{\mathsf{D}} D_\lambda$

$\mathsf{aux} \rightarrow$  $\rightarrow x$

DKL09 DGK+10 CKVW10

α-Pseudo Entropy Distribution:

$(x, \mathsf{aux}) \leftarrow_{\mathsf{D}} D_\lambda \qquad \mathbf{H}_{\mathsf{HILL}}(x|\mathsf{aux}) \geq \alpha(\lambda)$

AGV09 GKPV10 BLSV18 DP08

ADN+10 NS09 Pie09 Zha16

DHLW10 BG10 AKPW13

Extention: Multi-bit messages

$$c \leftarrow \mathrm{Enc}_{sk}(C) \qquad a \leftarrow \mathrm{Enc}_{\mathrm{lock}}(sk) \qquad f_1 \leftarrow \mathrm{Enc}_{sk}(m_1), \ldots, f_n \leftarrow \mathrm{Enc}_{sk}(m_n)$$

Evaluation

$$\mathrm{Eval}(U_x, c) = \mathrm{Enc}_{sk}(C(x)) = d$$

$$\mathrm{Eval}(\mathrm{Dec}(d, .), a) = \mathrm{Enc}_{sk}(\mathrm{Dec}(C(x), \mathrm{Enc}_{\mathrm{lock}}(sk))) = e$$

Suppose $C(x) = \text{lock}$ and $e = \mathrm{Enc}_{sk}(sk)$

$$f_1 \cdot e = \mathrm{Enc}_{sk}(m_1 \cdot sk)$$

$m_1 = 0$ → $\mathrm{Enc}_{sk}(0)$

$m_1 = 1$ → $\mathrm{Enc}_{sk}(sk)$

?

Cycle Tester

Summary

- Generic Construction of Lockable Obfuscation from FHE with Cycle Testers
- In the paper: the construction for arbitrary cycle lenght

Implications

Lockable Obfuscation + (FH)E ⟹ (FH)E with a Cycle Tester

FHE + Cycle Tester ⟹ Lockable Obfuscation

Thank You

https://eprint.iacr.org/2021/1324