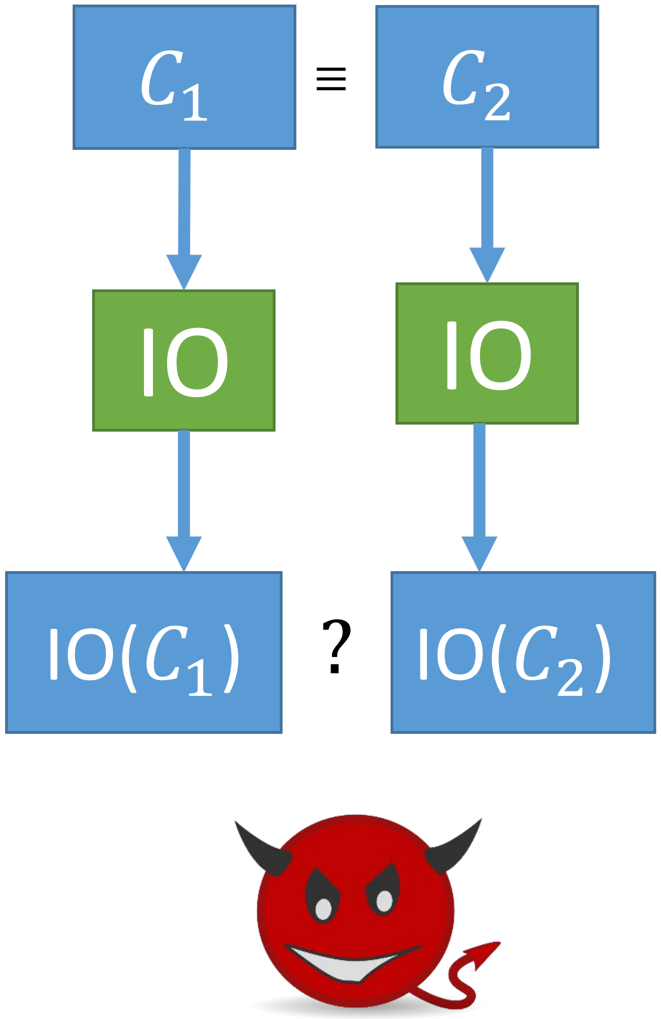
Black-box and Non-black-box Lower Bounds on Assumptions behind IO

Sanjam Garg (Berkeley)

Mohammad Mahmoody (Univ. of Virginia)

Ameer Mohammed (Univ. of Virginia)

Indistinguishability Obfuscation (IO) [BGIRSVY01, GGHRSW13]



What primitive do you want ?

IO

Functional Encryption: [Garg-Gentry-Halevi-Raykova-Sahai-Waters 2013]
Witness Encryption: [Garg-Gentry-Sahai-Waters 2013]
2-round MPC: [Garg-Gentry-Halevi-Raykova 2013]
Re-using garbled circuits: [Gentry–Halevi–Raykova-Wichs 2014]
Deniable Encryption, KEM, Oblivious Transfer,…: [Sahai-Waters 2014]
Random oracle instantiation: [Hohenberger-Sahai-Waters 2014]
Secret sharing: [Komargodski-Naor 2014]
2-round adaptively-secure MPC: [Garg-Polychroniadou 2015]
Multi-input Functional Encryption: [Goldwasser-Gordon-Goyal-Jain-Katz-Liu-Sahai-Shi-Zhao 2015] ……….

What assumptions give us IO?

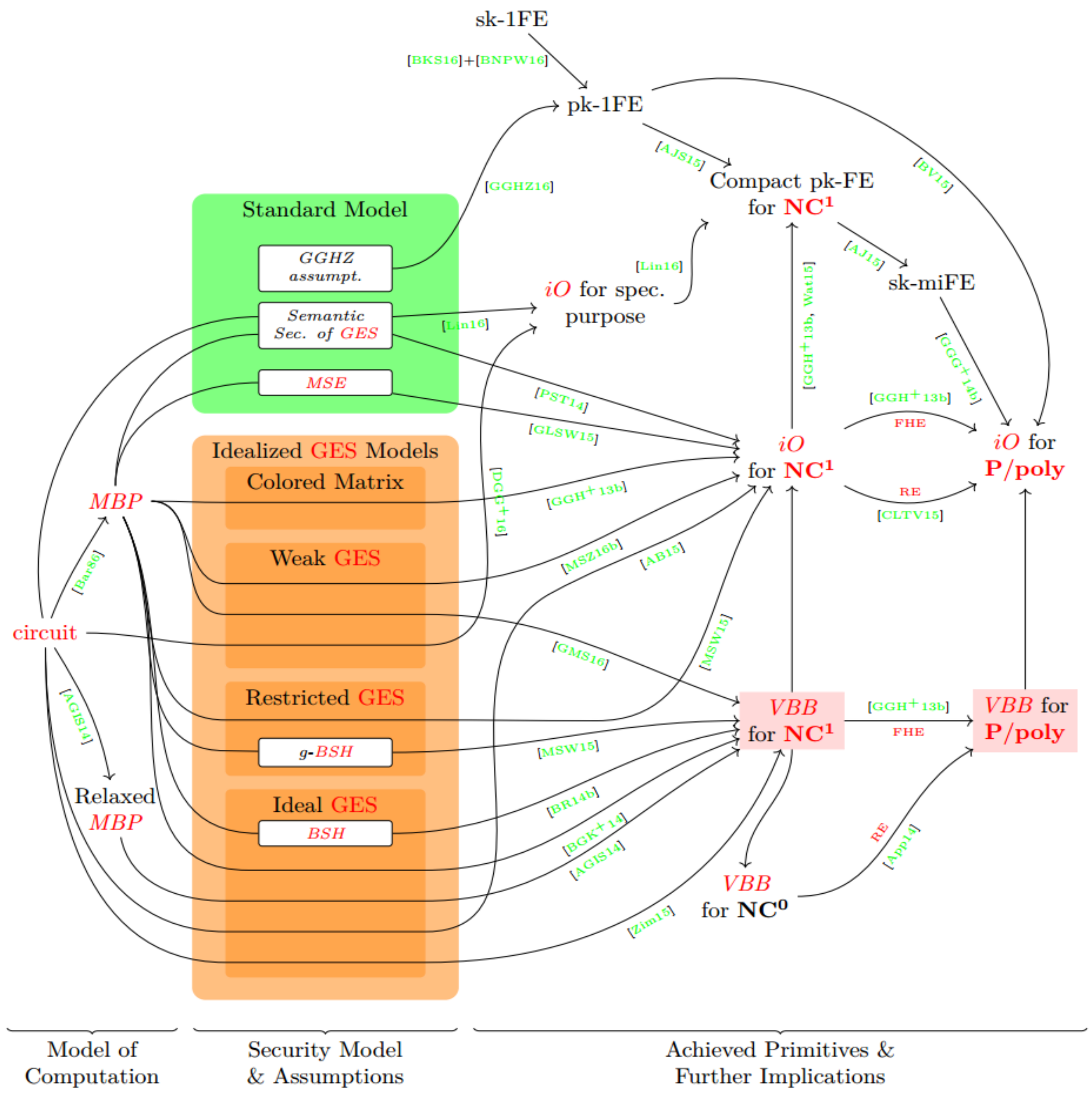
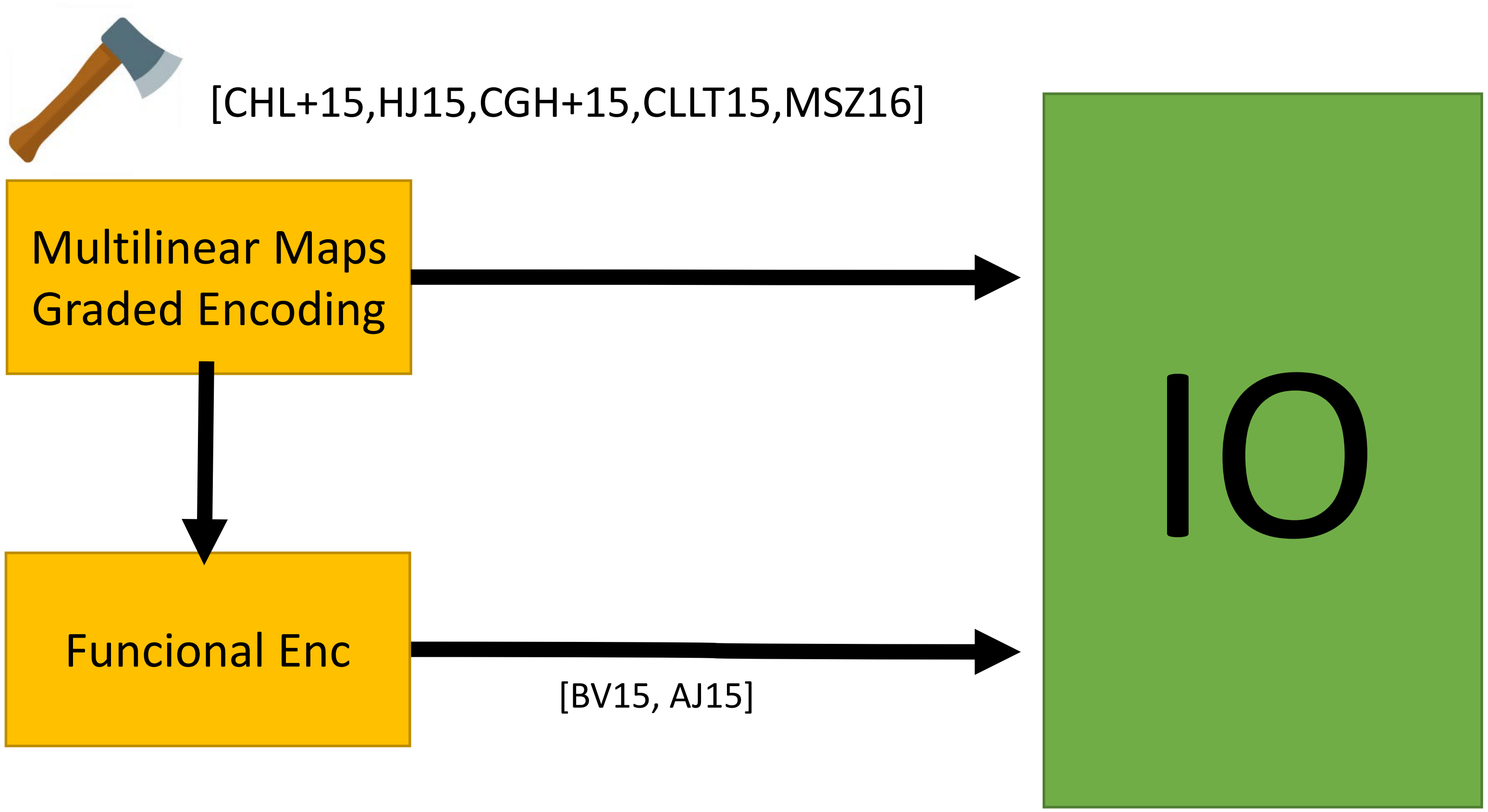


Figure 4: The map of different ways towards achieving iO for circuits in $\mathbf{P/poly}$ at the date of writing.

Picture by [Horváth, L Buttyán 16]



Can we use “standard assumptions” ?

Main Results - Informal

Thm: Assuming OWFs and that Poly-Hierarchy does not collapse, none of primitives below imply IO in a `**non-black-box**' way:

- Witness encryption
- Predicate encryption
- Fully hom encryption

[GMM Crypto 17]

- **`Short output' functional encryption** [GMM 17]

Previous Results: [MMNPS16]

Full black-box separation from OWF, CRH, IBE

Assuming OWFs and that Poly-Hierarchy does not collapse, none of primitives below imply IO in a `black-box' way:

- Witness encryption
- Predicate encryption
- Fully hom encryption

[GMM Crypto 17]

- **`Short output' functional encryption** [GMM 17]

- **Question**: Why is the result conditional?
- **Answer**: If $\mathrm{P} = \mathrm{NP}$ → **statistically secure IO** for P/poly
  → Black-box IO possible by ignoring primitive $\mathcal{P}$

Plan

1. Black-box model and its “non-bb extension”

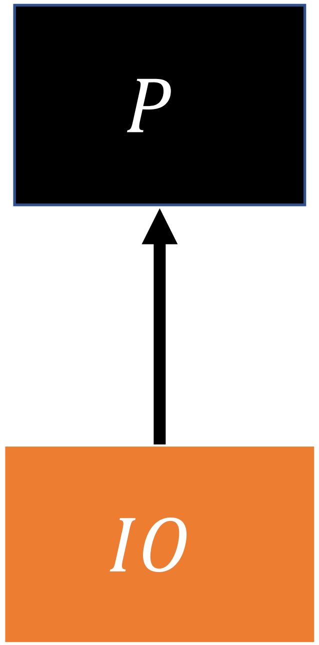
2. Recipe for lower bounds for IO.

3. Separating IO from “short output” FE

Plan

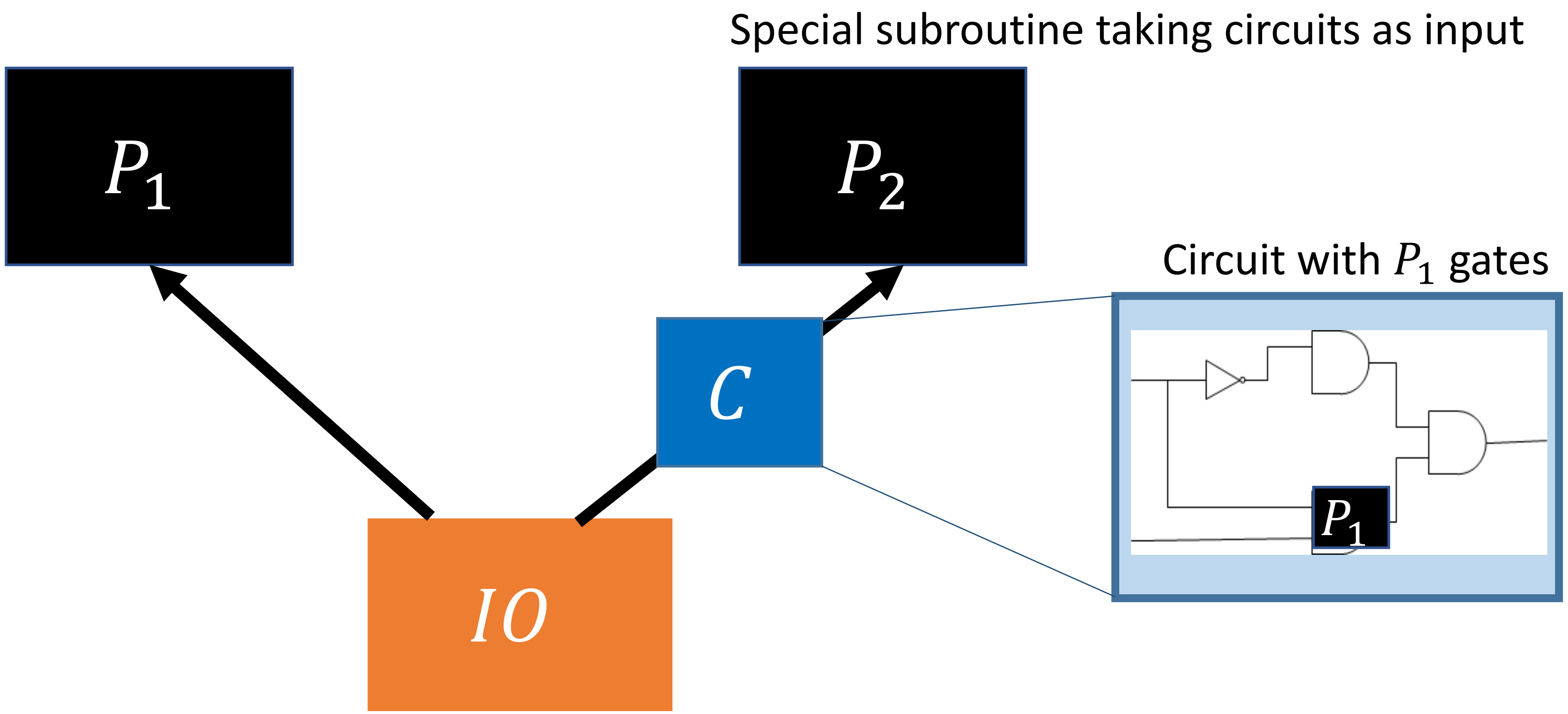
1. Black-box model and its “non-bb extension”
2. Recipe for lower bounds for IO.
3. Separating IO from “short output” FE

Black-Box Framework [IR'89, RTV'04]



Natural when P : OWF or TDP

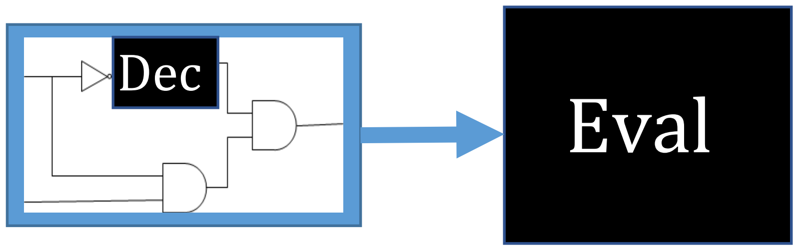
How about self-feeding P ?



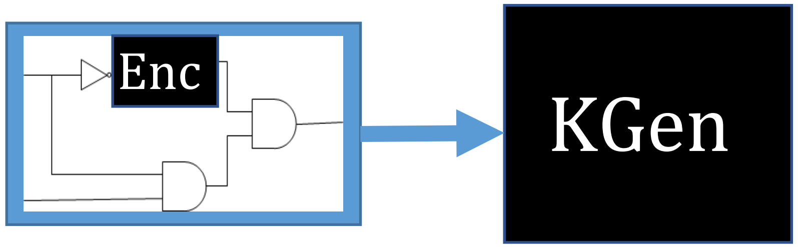
Not black-box according to [IR,RTV]
But we do this sometimes..

Examples of where this trick is used

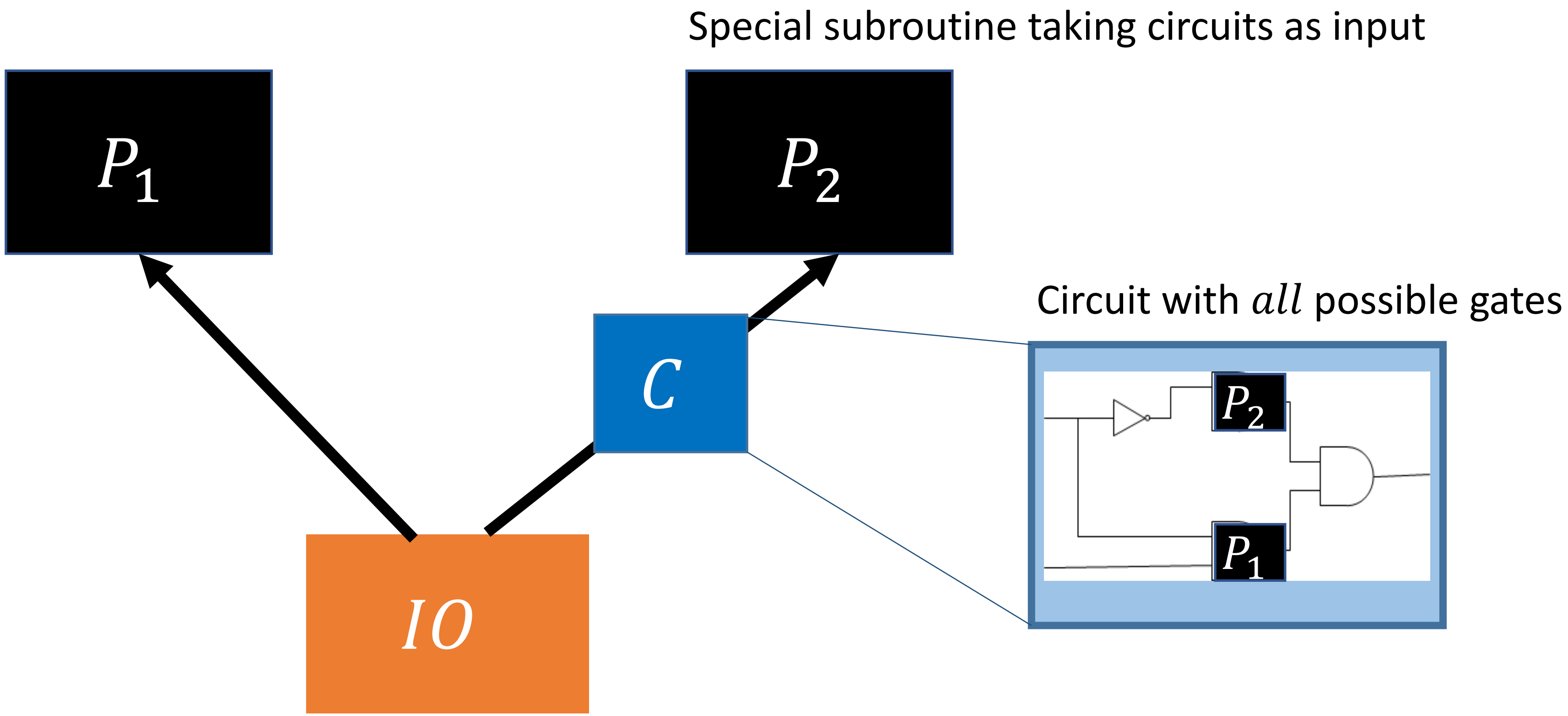
- FHE bootstrapping [Gentry'09]



- **FE → IO** [AJ'16,BV'16]

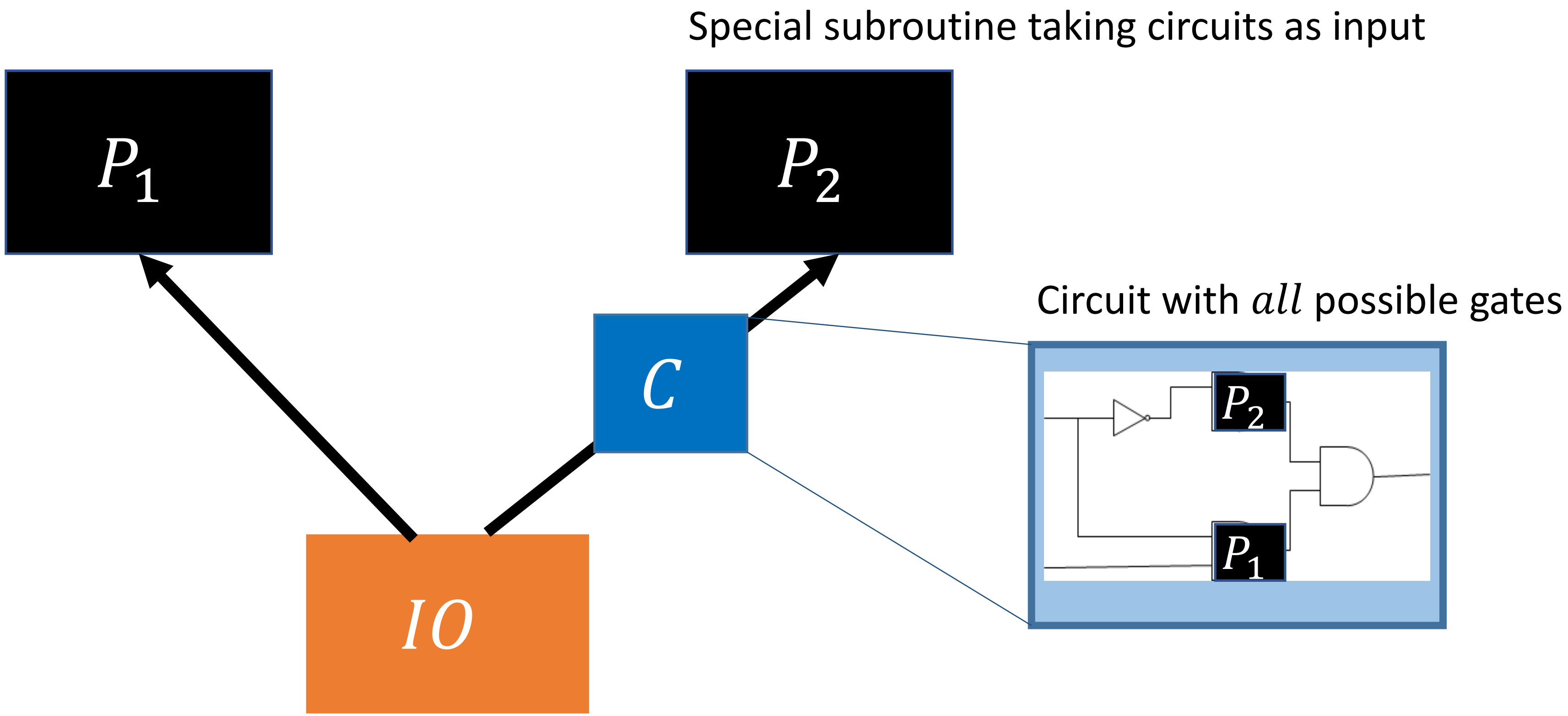


Let’s give it a name: **extended** black-box



- Inspired by [BKSY11, AS15, AS16] who allowed OWF gates
- Extended black-box : **all subroutines of primitive** are allowed

Relation to fully BB



- **Extended** black-box construction from P

- Fully black-box use of **extended** version of P

Main Results – Half Formal

Thm: Assuming OWFs and that Poly-Hierarchy does not collapse, none of primitives below imply IO in **extended** black-box way:

- Witness encryption
- Predicate encryption
- Fully hom encryption

[GMM Crypto 17]

- **`Short output' functional encryption** [GMM 17]

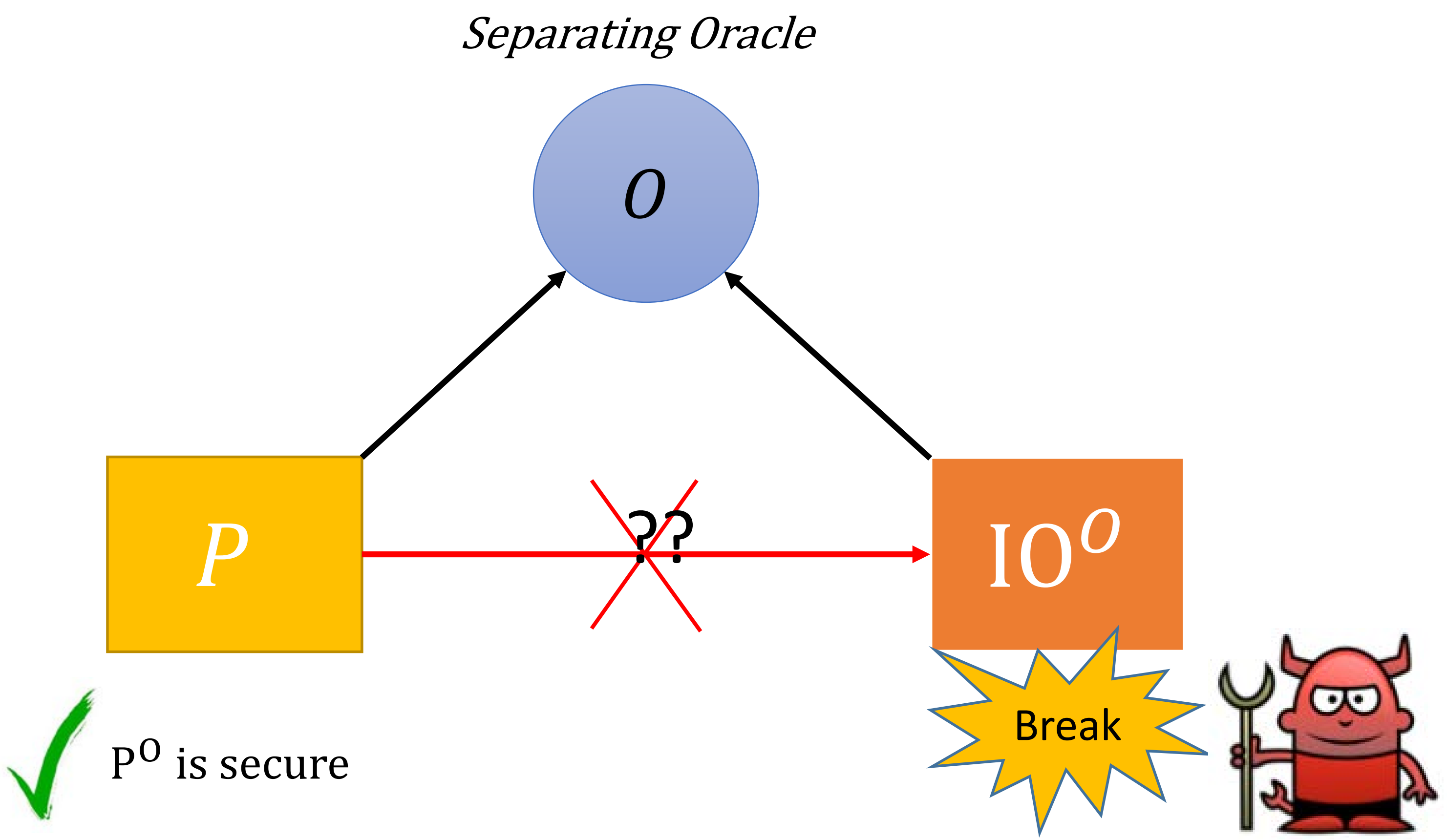
Plan

1. Black-box model and its “extensions”

2. Recipe for lower bounds for IO.

3. Separating IO from “short output” FE

General technique: oracle separation



Recipe of attacking $\mathrm{IO}^{\mathcal{P}}$ in idealized model $\mathcal{P}$

Only correct on 99% of inputs

1. [CKP'15] Compile out $\mathcal{P}$ from $\mathrm{IO}^{\mathcal{P}}$ → get **approx** IO

2. [BBF'16] there is always an unbounded attack to approx IO

3. Combine two steps above → poly-query attack to $\mathrm{IO}^{\mathcal{P}}$

Closer look at compiling out an oracle $\mathcal{P}$

We are here:

$\mathrm{IO}^{\mathcal{P}}$

IO in $\mathcal{P}$ Model

$$\mathrm{IO}^{\mathcal{P}} \longrightarrow \mathrm{IO}'$$

Our Goal is:

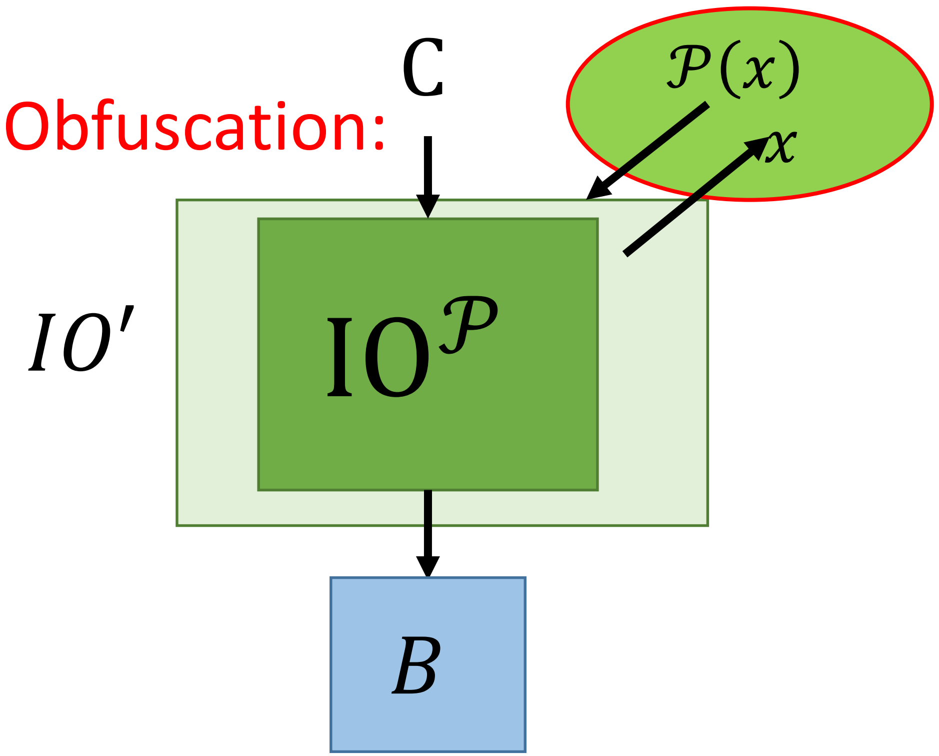
IO'

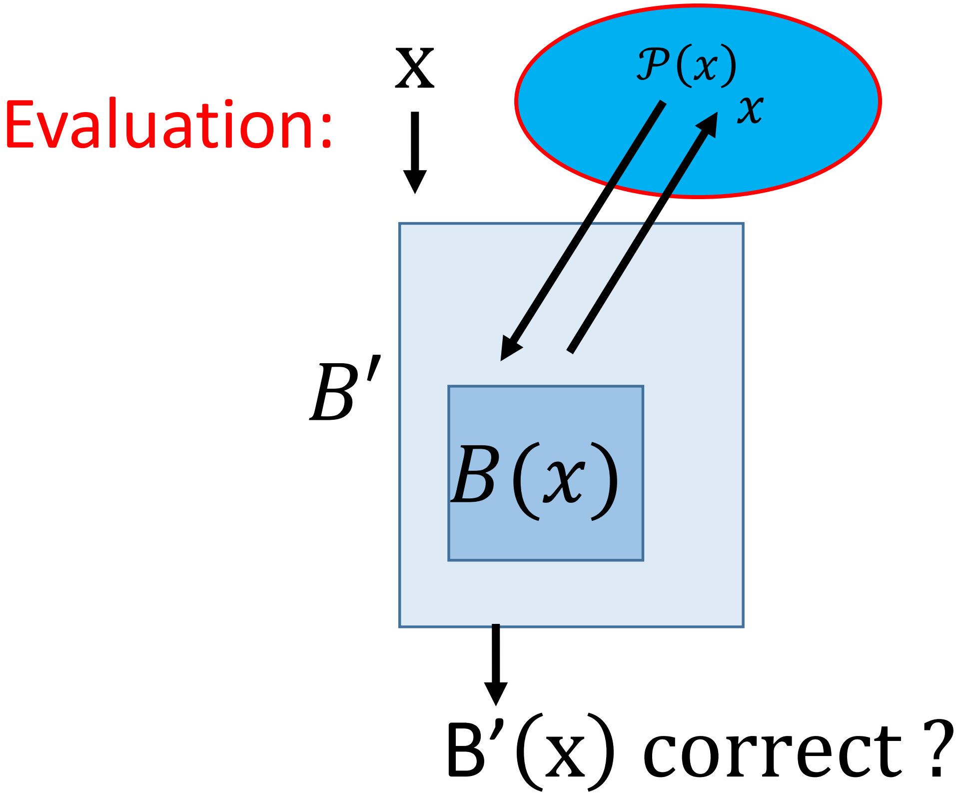
“approximate IO” in **plain** model

How to obfuscate?

How to evaluate?

First try: emulate $\mathcal{P}$ on demand

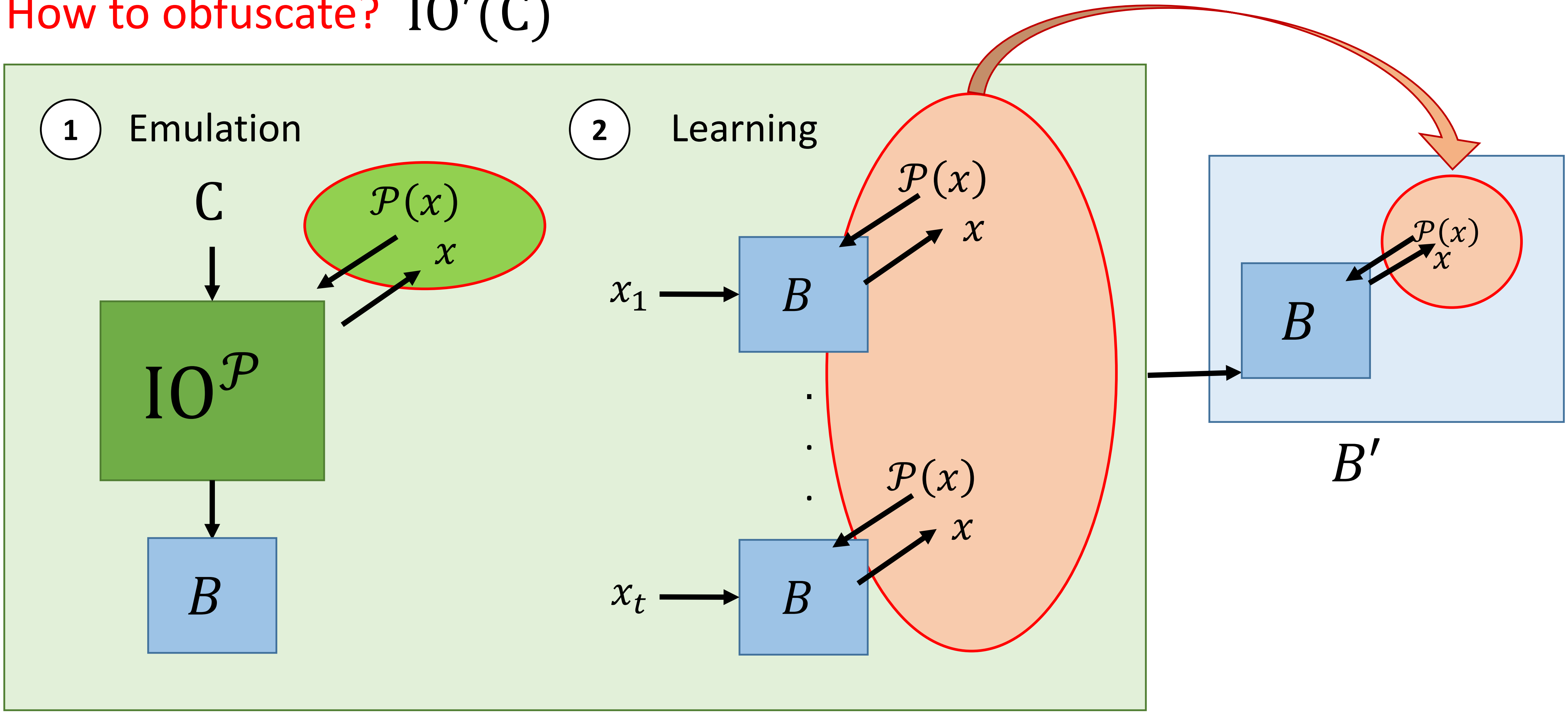




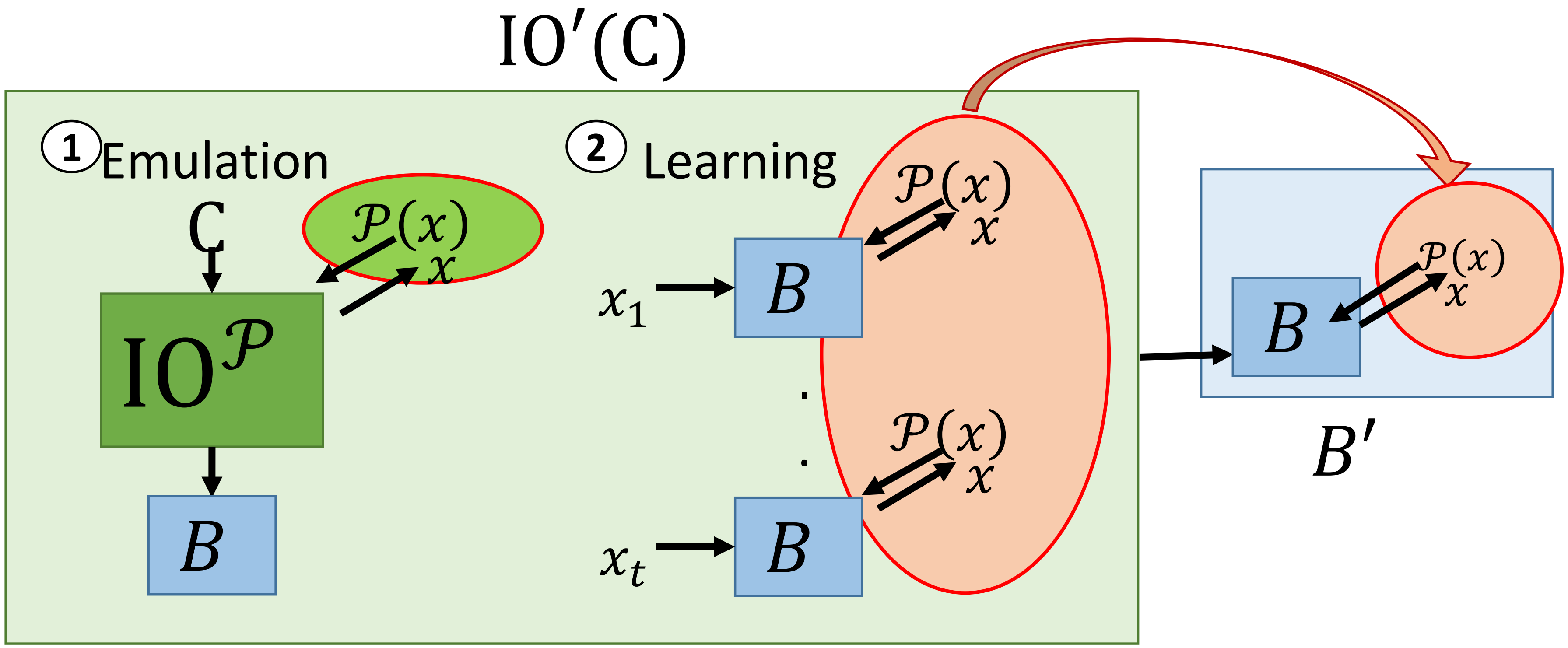
- It is "secure" but $\mathcal{P}(x)$ x and $\mathcal{P}(x)$ x might be inconsistent.
- If we reveal $\mathcal{P}(x)$ x to B' for correctness → breaks security.

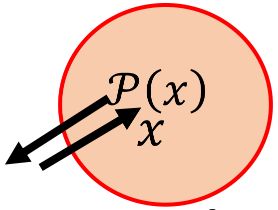
[CKP'15]: revealing useful `simulatable' queries

How to obfuscate? $\mathrm{IO}'(\mathrm{C})$



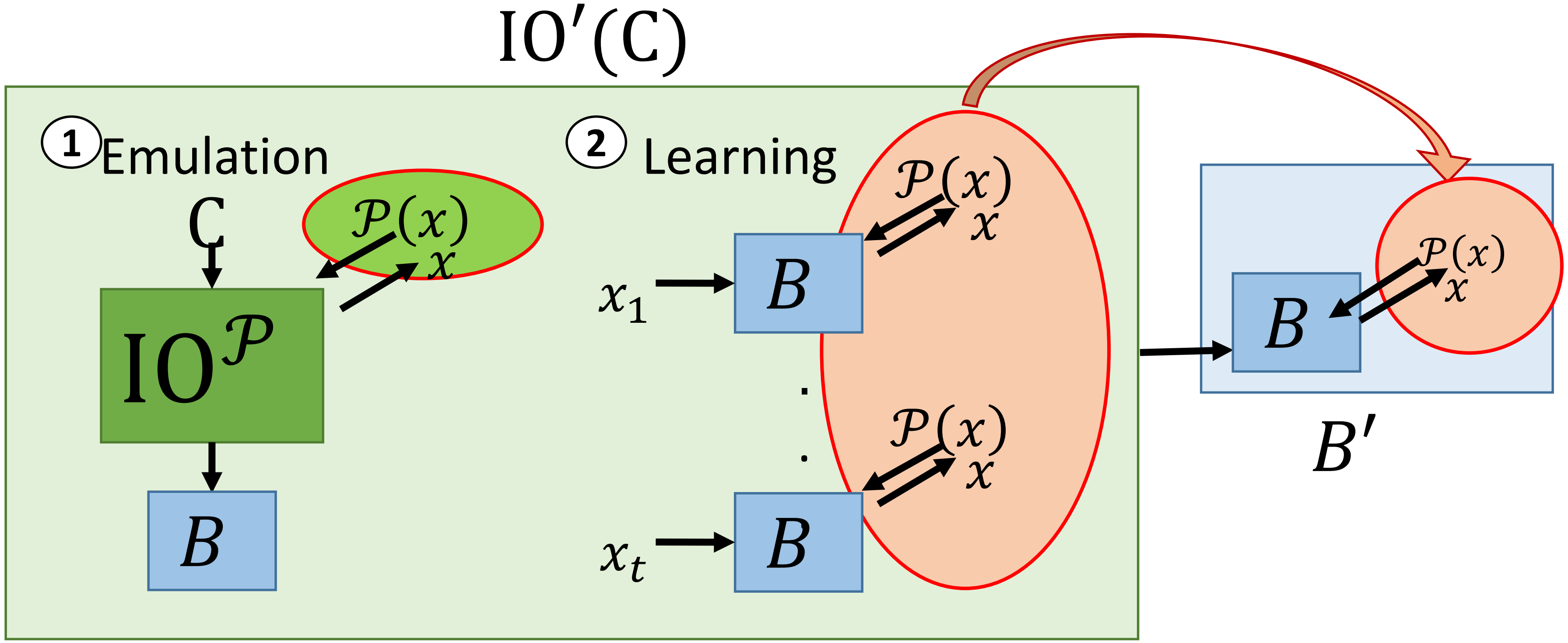
What is the challenge ?



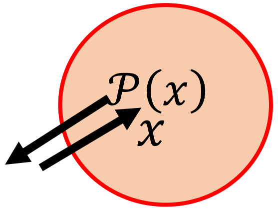
- **Security**:  can be simulated in ideal world of $IO^{\mathcal{P}}$ so revealing it does not hurt the security of IO

- **Challenge**: to prove approximate correctness of B’ in plain model

Example:
$\mathcal{P}$: ROM



- If we compile out random oracle $\mathcal{P}$ → get separation from OWF, CRH, etc.

- 

covers queries of IO^P likely to be asked by $B'(x)$ (with error < 0.01)

- Any other query could be answered at random!

Plan

1. Black-box model and its “extensions”
2. Recipe for lower bounds for IO. Case of OWFs
3. Separating IO from “short output” FE

Functional Encryption

- $\mathrm{Setup}(1^\kappa) \to (\mathrm{PK}, \mathrm{SK})$
- $\mathrm{Enc}(\mathrm{PK}, m) \to \mathrm{ct}$
- $\mathrm{KeyGen}(\mathrm{SK}, f) \to \mathrm{Key}_f$ **f is arbitrary circuit**
- $\mathrm{Dec}\left(\mathrm{ct}, \mathrm{Key}_f\right) = f(x)$
- **Security:** $f(m_0) = f(m_1) \rightarrow (\mathrm{PK}, \mathrm{Key}_f, \mathrm{ct}_0) \approx_{\mathrm{ind}} (\mathrm{PK}, \mathrm{Key}_f, \mathrm{ct}_0)$

Thm: Assuming OWFs and that Poly-Hierarchy does not collapse, none of primitives below imply IO in `**extended** black-box' way:

- **`Short output' functional encryption** [GMM 17]

- **Short output:** $|f(x)| < |\mathrm{ct}| - \omega(|m|)$
- LWE-based FE of [GKPVZ13] satisfies this condition
- Positive results of [BV,AJ'15] use long outputs $|f(x)| \approx 2 \cdot |\mathrm{ct}|$

Extended Functional Encryption

$$\mathrm{FE} = (\mathrm{Setup}, \mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$$

- **Extended** Black-Box use of Functional Encryption: Construction can use f^{FE} with all possible FE gates

- Equivalent to **fully black-box** use of **Extended_FE** where we allow issuing keys for f^{FE} with all possible FE gates

Recall the goal: compiling out an ideal ext-FE oracle from any IO construction

We are here:

Our Goal is:

$$\boxed{\mathrm{IO}^{FE}} \longrightarrow \boxed{\mathrm{IO}'}$$

IO : idealize FE Model
for extended Func Enc

“approximate IO” in **plain** model

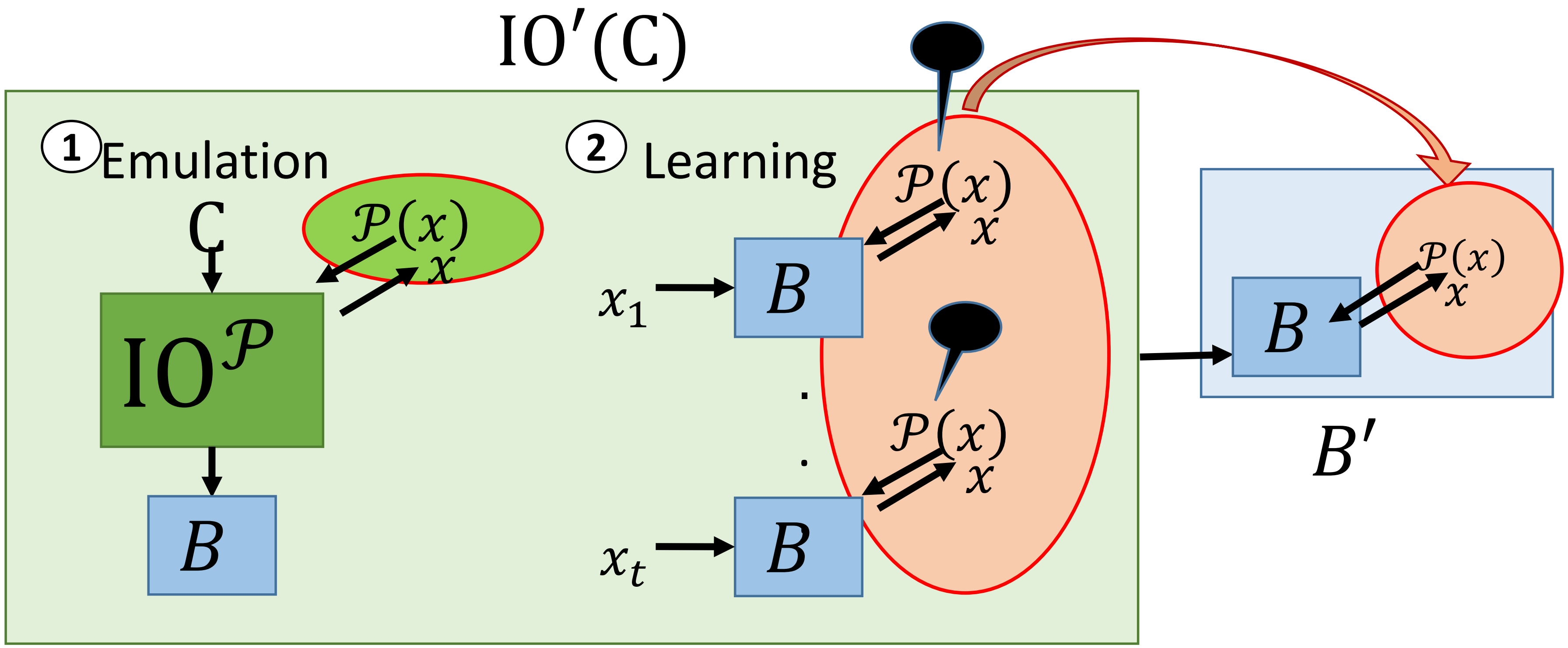
Enough to just compile out $\mathrm{Dec}(\cdot)$ queries:

- $\mathrm{Setup}(1^\kappa) \to (\mathrm{PK}, \mathrm{SK})$
- $\mathrm{Enc}(\mathrm{PK}, m) \to \mathrm{ct}$
- $\mathrm{KeyGen}(\mathrm{SK}, f) \to \mathrm{Key}_f$

Just a random oracle!

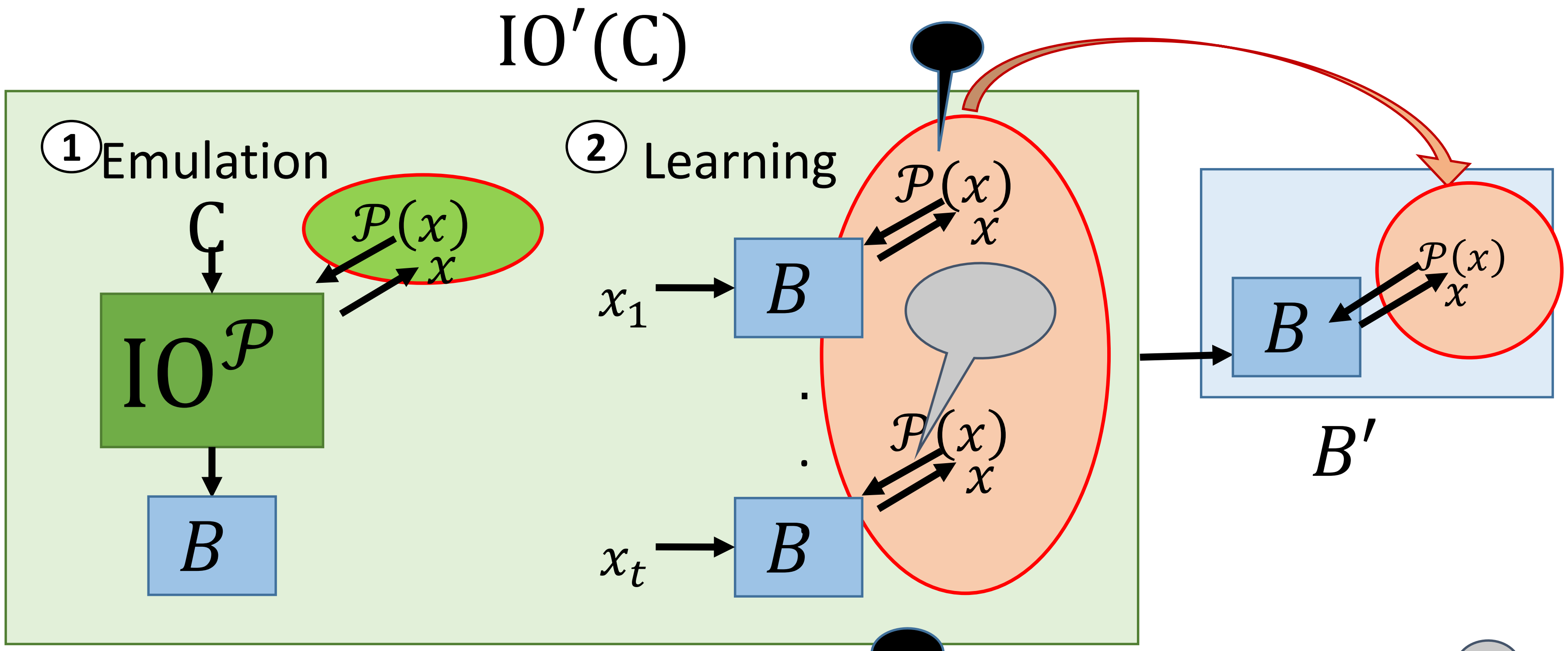
- $\cancel{\mathrm{Dec}\left(\mathrm{ct}, \mathrm{Key}_f\right) = f(x)}$

$\mathcal{P}$: ideal ex-FE
Goal: compiling out Dec queries



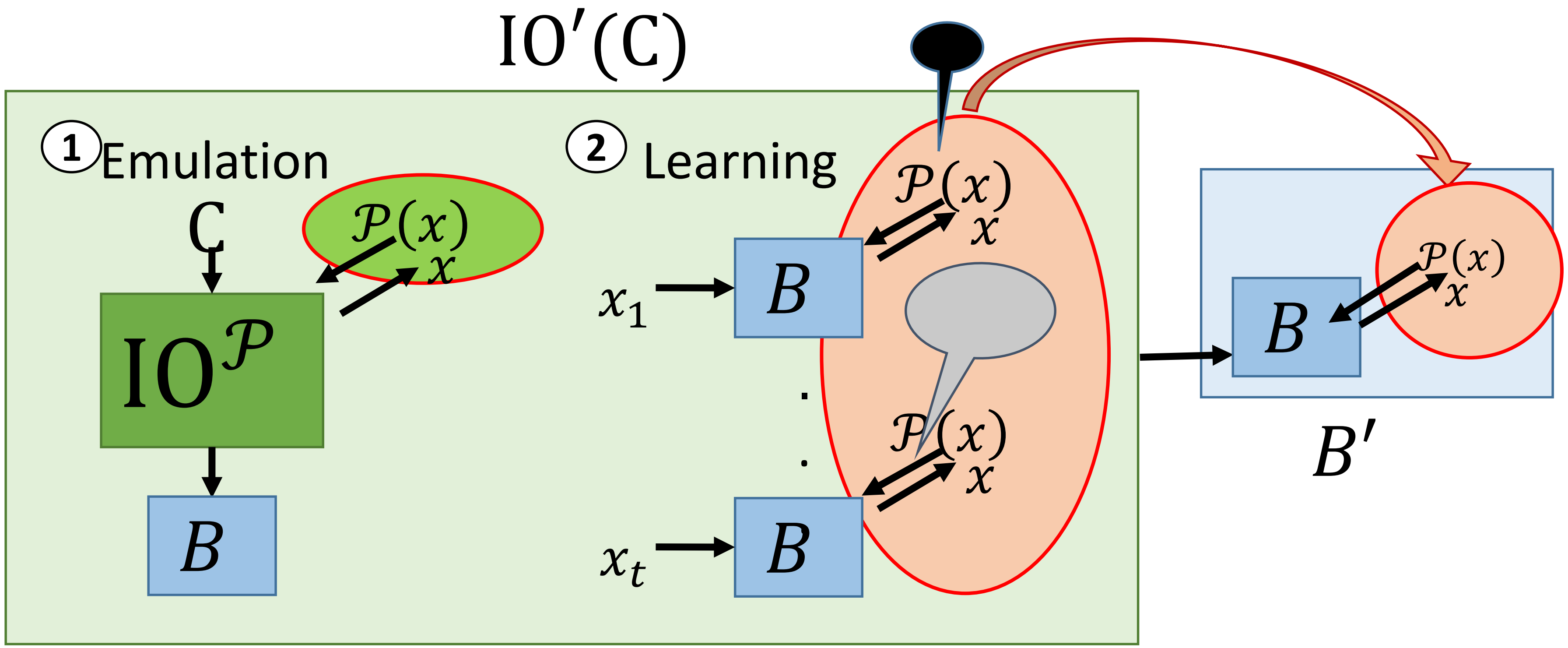
- **Challenge:**
- Any $\mathrm{Dec}(\mathrm{ct}, f)$ query has its own internal queries during $f^{\mathrm{FE}}(m)$
- queries are not simulatable → not OK to be passed to B’

$\mathcal{P}$: ideal ex-FE
Goal: compiling out Dec queries



- **Idea 1:** if we know m inside $\mathrm{ct} = \mathrm{Enc(m)}$ → $\mathrm{Dec}(\mathrm{ct}, f)$ turns into $\mathrm{Dec}(\mathrm{ct}, f)$ because we can run $f^{\mathrm{FE}}(m)$ instead
- **Idea 2:** we can assume every ct is decrypted at most **once**
- **Final goal:** show that $\mathrm{Dec}(\mathrm{ct}, f)$ **does not happen** during final exec B’

$\mathcal{P}$: ideal ex-FE
Goal: compiling out Dec queries



- **Final Idea (using short output of FE) :**
  learner sees a fixed polynomial number of $\mathrm{Dec}(\mathrm{ct}, f)$ queries

- By choosing t large enough → no "unknown" ciphertext during final exec

Short output → only poly new unknown ciphertexts

- Suppose $|f(x)| \ll |\mathrm{ct}| - |m|$
  where $\mathrm{ct} = \mathrm{Enc}(m)$ and $f(x) = \mathrm{Dec}(\mathrm{ct})$

- **Claim**: If we use random $enc : \{0,1\}^{|m|} \to \{0,1\}^{|\mathrm{ct}|}$, then any algorithm A with s bits of `advice' can hit only at most s "unknown" ciphertexts

- **Proof**:
  1. a string ct is a valid ciphertext with probability $2^{|\mathrm{m}|-|\mathrm{ct}|}$
  2. → "hitting" a valid ciphertext needs $\approx |\mathrm{ct}| - |m|$ bits of `advice'
  3. The answer $f(x)$ can only give back $|f(x)|$ bits of advice
  4. If $|f(x)| < |\mathrm{ct}| - |m|$ → after t steps we run out of advice bits!

Recap

Thm: Assuming OWFs and that Poly-Hierarchy does not collapse, none of primitives below imply IO in `**extended** black-box' way:

- Witness encryption
- Predicate encryption
- Fully hom encryption

[GMM Crypto 17]

- **Short output functional encryption** [GMM 17]

Future Directions?

- Tighter upper and lower bounds for output length of FE for IO?
- Long output FE from LWE?
- Revisiting classical separation results like OWF !→ PKE [IR’89] even more important in light of recent IBE from DDH [DG’17]

Thanks!