Bounded Functional Encryption for Turing Machines: Adaptive Security from General Assumptions

Shweta Agrawal

Anuja Modi

Shota Yamada

Fuyuki Kitagawa

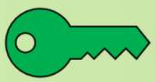
Ryo Nishimaki

Takashi Yamakawa

Ciphertext Policy Functional Encryption (CPFE) [SW05, BSW11]

Q – (bounded) polynomial collusion bound

Setup$(1^\lambda, |f|, 1^Q) \rightarrow$ mpk, msk



Encrypt$(mpk, f) \rightarrow ct$

KeyGen$(msk, m) \rightarrow sk_m$

Decrypt$(sk_m, ct) = f(m)$

Correctness

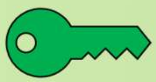
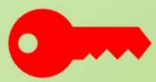
Decrypt$\big(sk_m, \text{Encrypt}(mpk, f)\big) = f(m)$

Simulation Security

$$ct \leftarrow Enc(mpk, m)$$
$$\approx$$
$$ct \leftarrow SIMEnc(mpk, \{sk_{m_i}, f(m_i)\}, 1^{|f|})$$

Key Policy Functional Encryption (KPFE) [SW05, BSW11]

$\text{Setup}(1^{\lambda}, |f|, 1^{Q}) \rightarrow mpk, msk$

$\text{Encrypt}(mpk, m) \rightarrow ct$

$\text{KeyGen}(msk, f) \rightarrow sk_f$

$\text{Decrypt}(sk_f, ct) = f(m)$

Dynamic Bounded Collusion Model

- Q is chosen per ct by encryptor
- Setup, KeyGen are independent of Q.
- $|ct|$ grows linearly with Q, Encrypt$(mpk, f, 1^Q)$

Setup$(1^\lambda, |f|) \to mpk, msk$

Encrypt$(mpk, m, 1^Q) \to ct$

KeyGen$(msk, f) \to sk_f$

Decrypt$(sk_f, ct, 1^Q) = f(m)$

Simulation Security for CPFE

AD-SIM security

Real

$$(mpk, msk) \leftarrow Setup(1^{\lambda}, prm)$$

$$(f, 1^{Q}) \leftarrow A^{Keygen(msk,.)}(mpk)$$

$$ct \leftarrow Encrypt(mpk, f, 1^{Q})$$

$$b \leftarrow A^{Keygen(msk,.)}(mpk, ct)$$

Output b

$$\approx$$

Ideal

$$(mpk, msk) \leftarrow Setup(1^{\lambda}, prm)$$

$$(f, 1^{Q}) \leftarrow A^{Keygen(msk,.)}(mpk)$$

$$(ct, st) \leftarrow SimEnc\left(mpk, \{sk_{m_i}, f(m_i)\}, 1^{|f|}, 1^{Q}\right)$$

$$b \leftarrow A^{SIMKG(st,msk,.)}(mpk, ct)$$

Output b

Simulation Security for CPFE

NA-SIM security

Real

$(mpk, msk) \leftarrow Setup(1^{\lambda}, prm)$

$(f, 1^Q) \leftarrow A^{Keygen(msk,.)}(mpk)$

$ct \leftarrow Encrypt(mpk, f, 1^Q)$

$b \leftarrow A^{Keygen(msk,.)}(mpk, ct)$

Output b

$\approx$

Ideal

$(mpk, msk) \leftarrow Setup(1^{\lambda}, prm)$

$(f, 1^Q) \leftarrow A^{Keygen(msk,.)}(mpk)$

$(ct, st) \leftarrow SimEnc\left(mpk, \{sk_{m_i}, f(m_i)\}, 1^{|f|}, 1^Q\right)$

$b \leftarrow A^{SIMKG(st,msk,.)}(mpk, ct)$

Output b

Sel-SIM security

A outputs f at the start of the game.

Dynamic Bounded Collusion Model

Related Work (without obfustopia assumptions)

	FE/ABE	Class	Security	Assumption
[AMVY21]	FE	TM	NA-SIM	(sub-exp, sub-exp)-LWE

Dynamic Bounded Collusion Model

Related Work (without obfustopia assumptions)

	FE/ABE	Class	Security	Assumption
[AMVY21]	FE	TM	NA-SIM	(sub-exp, sub-exp)-LWE
[AMVY21]	FE	NL	AD-SIM	(sub-exp, sub-exp)-LWE

Dynamic Bounded Collusion Model

Related Work (without obfustopia assumptions)

	FE/ABE	Class	Security	Assumption
[AMVY21]	FE	TM	NA-SIM	(sub-exp, sub-exp)-LWE
[AMVY21]	FE	NL	AD-SIM	(sub-exp, sub-exp)-LWE
[GSW21]	ABE	TM	AD-IND	IBE (ROM)

Dynamic Bounded Collusion Model

Related Work (without obfustopia assumptions)

	FE/ABE	Class	Security	Assumption
[AMVY21]	FE	TM	NA-SIM	(sub-exp, sub-exp)-LWE
[AMVY21]	FE	NL	AD-SIM	(sub-exp, sub-exp)-LWE
[GSW21]	ABE	TM	AD-IND	IBE (ROM)

Note: Encryption time for TM **depends** on the running time of computation.

Dynamic Bounded Collusion Model

Related Work and Our Results

	FE/ABE	Class	Security	Assumption
[AMVY21]	FE	TM	NA-SIM	(sub-exp, sub-exp)-LWE
[AMVY21]	FE	NL	AD-SIM	(sub-exp, sub-exp)-LWE
[GSW21]	ABE	TM	AD-IND	IBE (ROM)
[This]	FE	TM	AD-SIM	LOT, ABE for NC1 & PIR

Dynamic Bounded Collusion Model

Related Work and Our Results

	FE/ABE	Class	Security	Assumption
[AMVY21]	FE	TM	NA-SIM	(sub-exp, sub-exp)-LWE
[AMVY21]	FE	NL	AD-SIM	(sub-exp, sub-exp)-LWE
[GSW21]	ABE	TM	AD-IND	IBE (ROM)
[This]	FE	TM	AD-SIM	LOT, ABE for NC1 & PIR 1. (poly, quasi-poly)-LWE

Dynamic Bounded Collusion Model

Related Work and Our Results

	FE/ABE	Class	Security	Assumption
[AMVY21]	FE	TM	NA-SIM	(sub-exp, sub-exp)-LWE
[AMVY21]	FE	NL	AD-SIM	(sub-exp, sub-exp)-LWE
[GSW21]	ABE	TM	AD-IND	IBE (ROM)
[This]	FE	TM	AD-SIM	LOT, ABE for NC1 & PIR 1. (poly, quasi-poly)-LWE 2. DDH & DBDH

Dynamic Bounded Collusion Model

Related Work and Our Results

	FE/ABE	Class	Security	Assumption
[AMVY21]	FE	TM	NA-SIM	(sub-exp, sub-exp)-LWE
[AMVY21]	FE	NL	AD-SIM	(sub-exp, sub-exp)-LWE
[GSW21]	ABE	TM	AD-IND	IBE (ROM)
[This]	FE	TM	AD-SIM	LOT, ABE for NC1 & PIR 1. (poly, quasi-poly)-LWE 2. DDH & DBDH 3. QR & DBDH

Dynamic Bounded Collusion Model

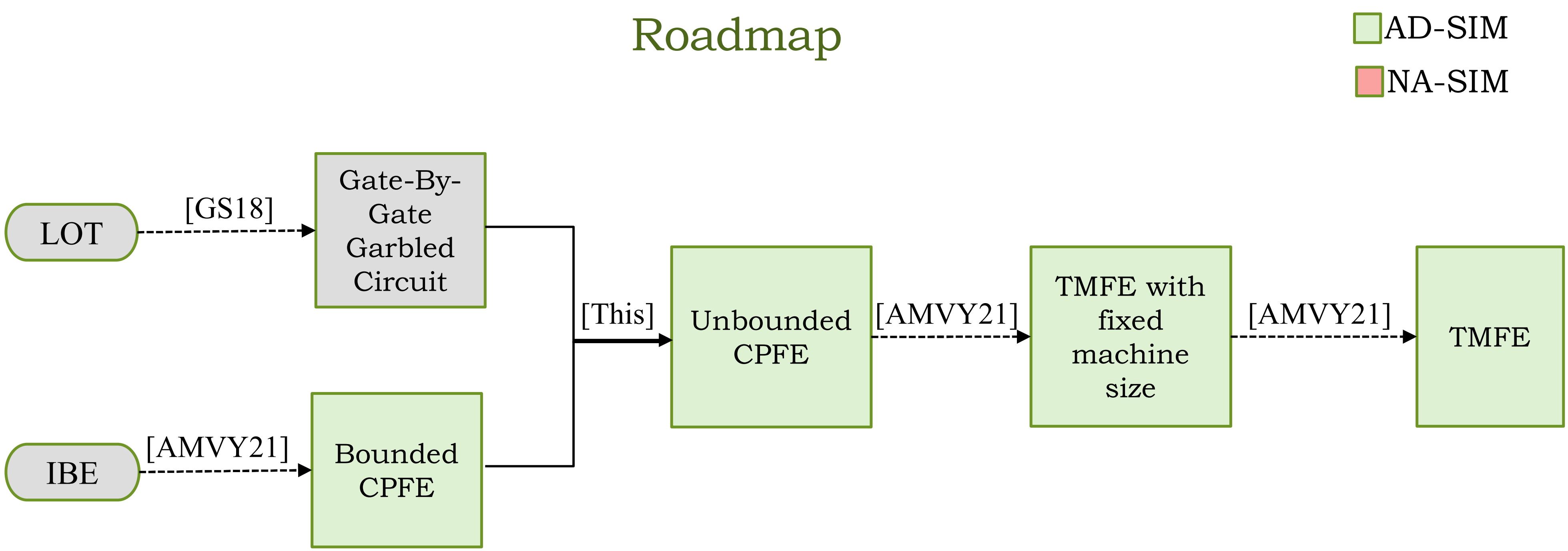
Related Work and Our Results

	FE/ABE	Class	Security	Assumption
[AMVY21]	FE	TM	NA-SIM	(sub-exp, sub-exp)-LWE
[AMVY21]	FE	NL	AD-SIM	(sub-exp, sub-exp)-LWE
[GSW21]	ABE	TM	AD-IND	IBE (ROM)
[This]	FE	TM	AD-SIM	LOT, ABE for NC1 & PIR 1. (poly, quasi-poly)-LWE 2. DDH & DBDH 3. QR & DBDH
[This]	ABE	TM	AD-IND	IBE & LOT

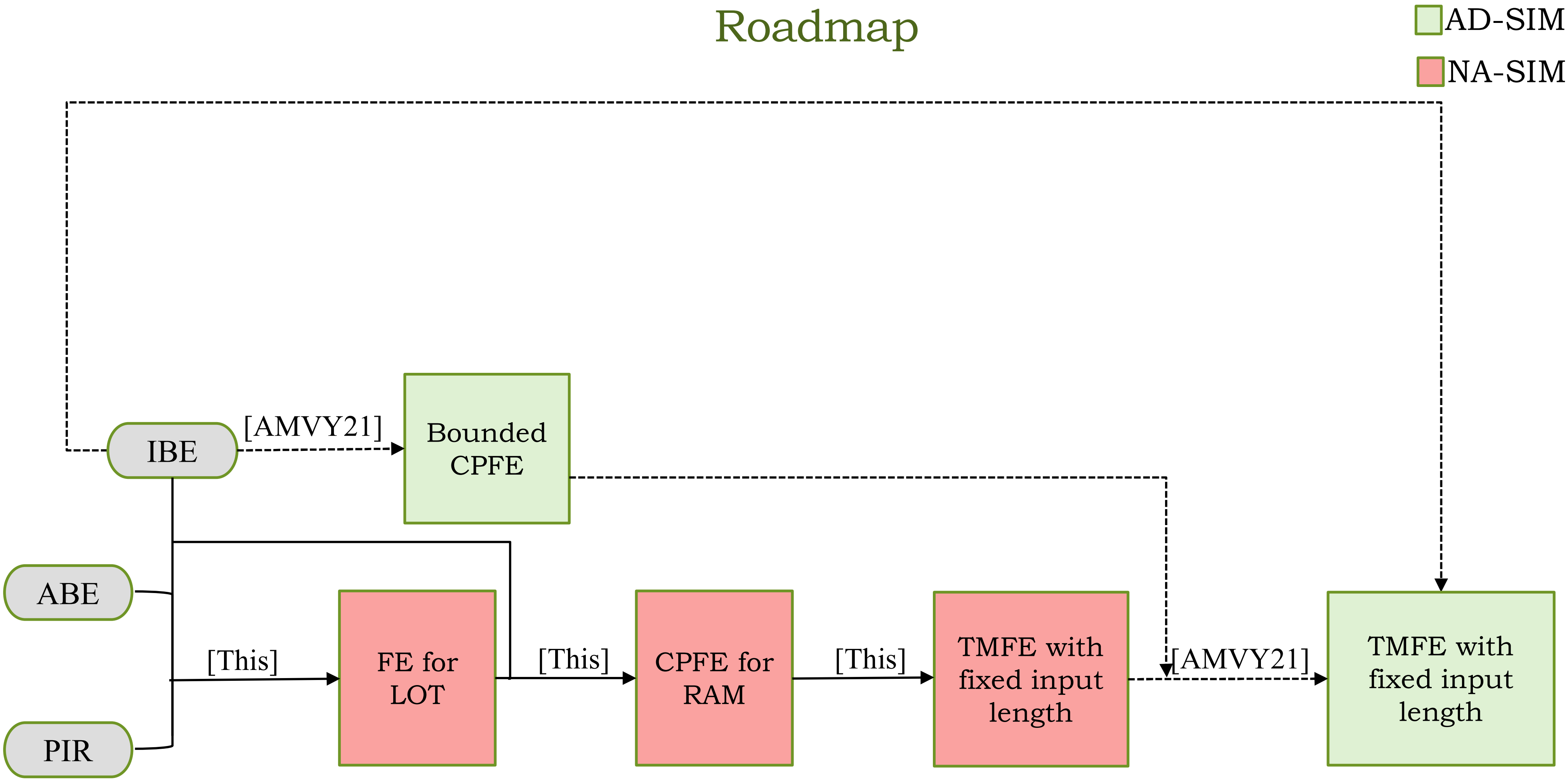
Simpler construction:

AD-SIM CPFE for circuits (unbounded size and depth), dynamic model from IBE and LOT.

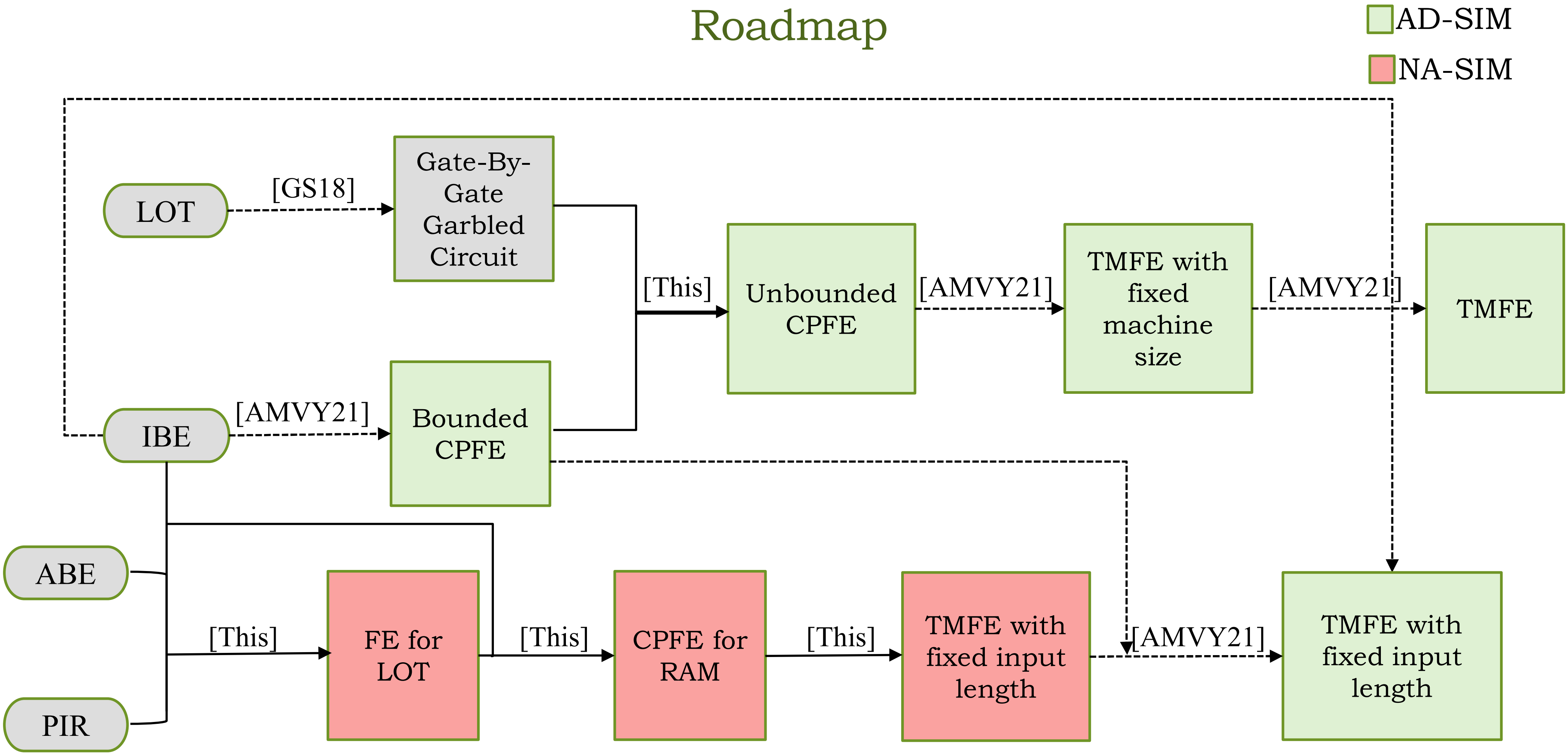
Roadmap


AD-SIM
NA-SIM
LOT
[GS18]
Gate-By-Gate Garbled Circuit
IBE
[AMVY21]
Bounded CPFE
[This]
Unbounded CPFE
[AMVY21]
TMFE with fixed machine size
[AMVY21]
TMFE

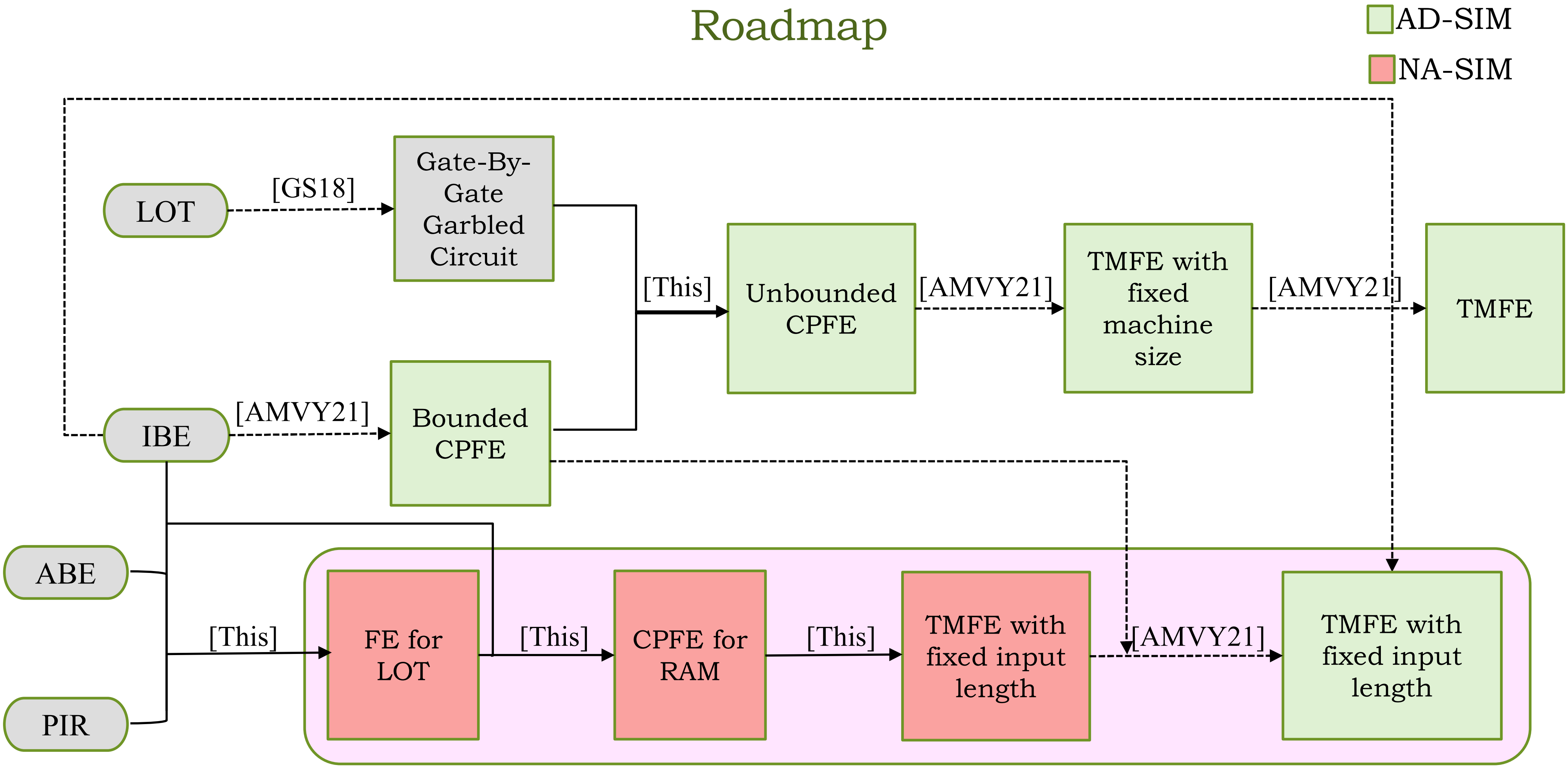
Roadmap


AD-SIM
NA-SIM
IBE
[AMVY21]
Bounded CPFE
ABE
PIR
[This]
FE for LOT
[This]
CPFE for RAM
[This]
TMFE with fixed input length
[AMVY21]
TMFE with fixed input length

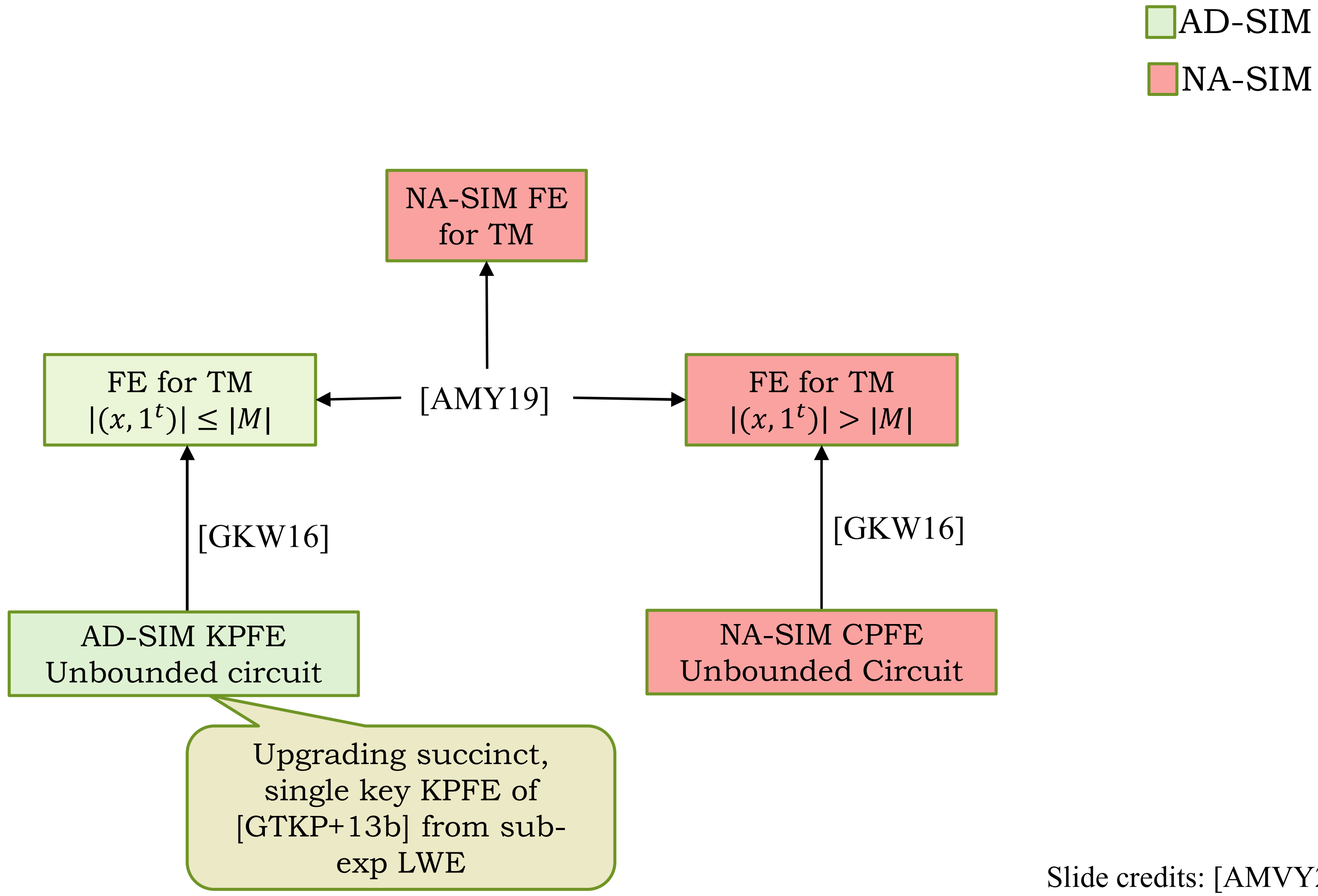
Roadmap


AD-SIM
NA-SIM
LOT
[GS18]
Gate-By-Gate Garbled Circuit
[This]
Unbounded CPFE
[AMVY21]
TMFE with fixed machine size
[AMVY21]
TMFE
IBE
[AMVY21]
Bounded CPFE
ABE
PIR
[This]
FE for LOT
[This]
CPFE for RAM
[This]
TMFE with fixed input length
[AMVY21]
TMFE with fixed input length

Roadmap

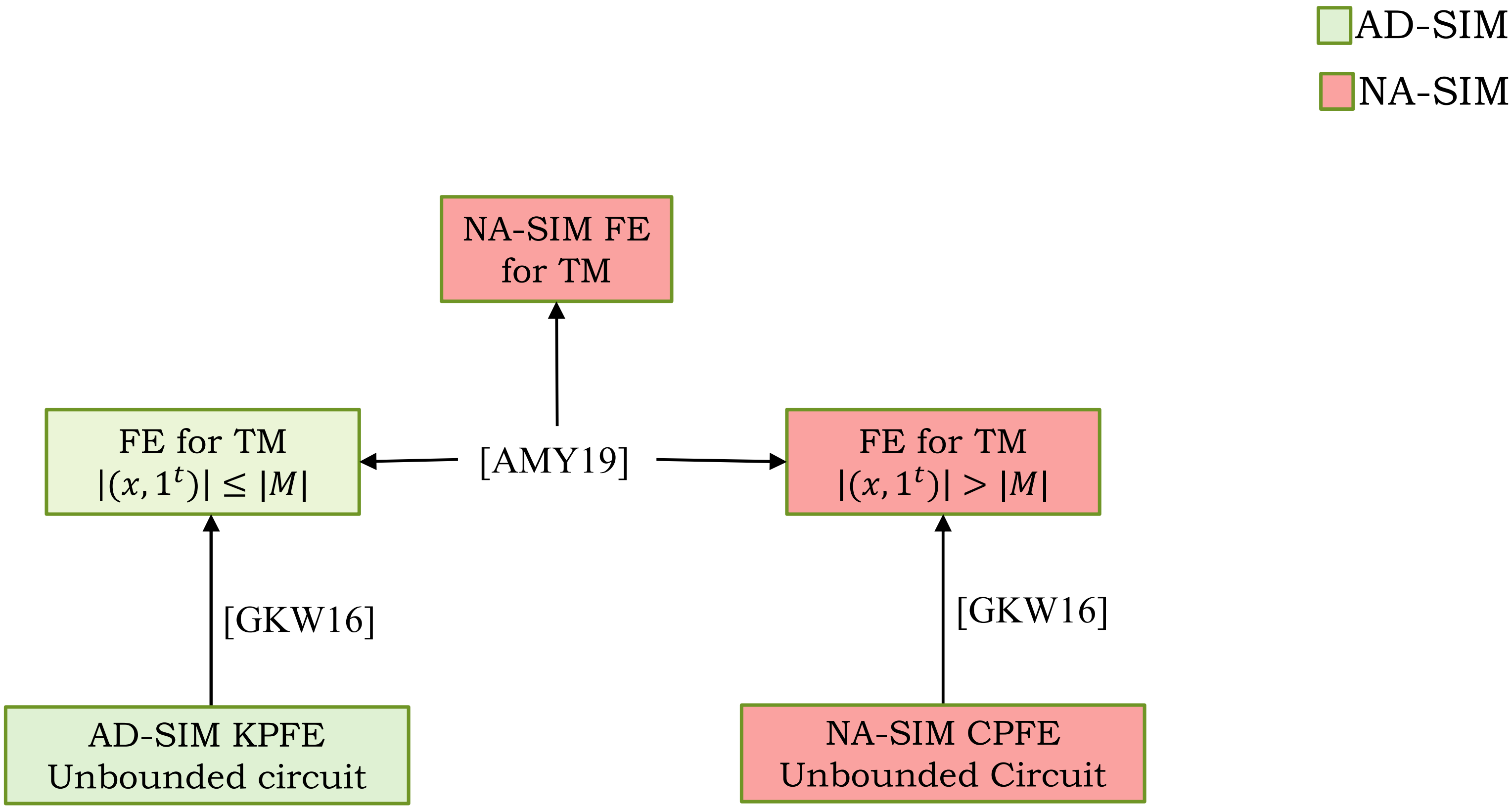

AD-SIM
NA-SIM
LOT
[GS18]
Gate-By-Gate Garbled Circuit
[This]
Unbounded CPFE
[AMVY21]
TMFE with fixed machine size
[AMVY21]
TMFE
IBE
[AMVY21]
Bounded CPFE
ABE
PIR
[This]
FE for LOT
[This]
CPFE for RAM
[This]
TMFE with fixed input length
[AMVY21]
TMFE with fixed input length

Recap of TMFE by [AMVY21]



Slide credits: [AMVY21]

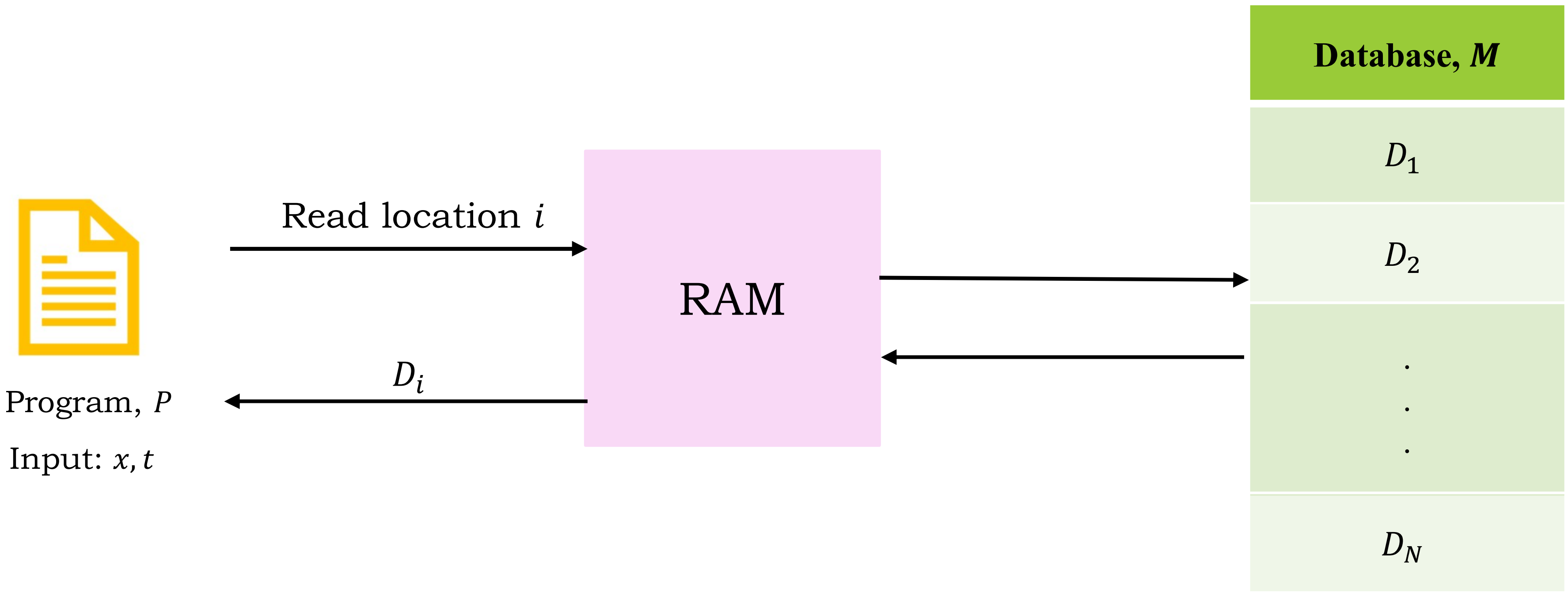
Recap of TMFE by [AMVY21]



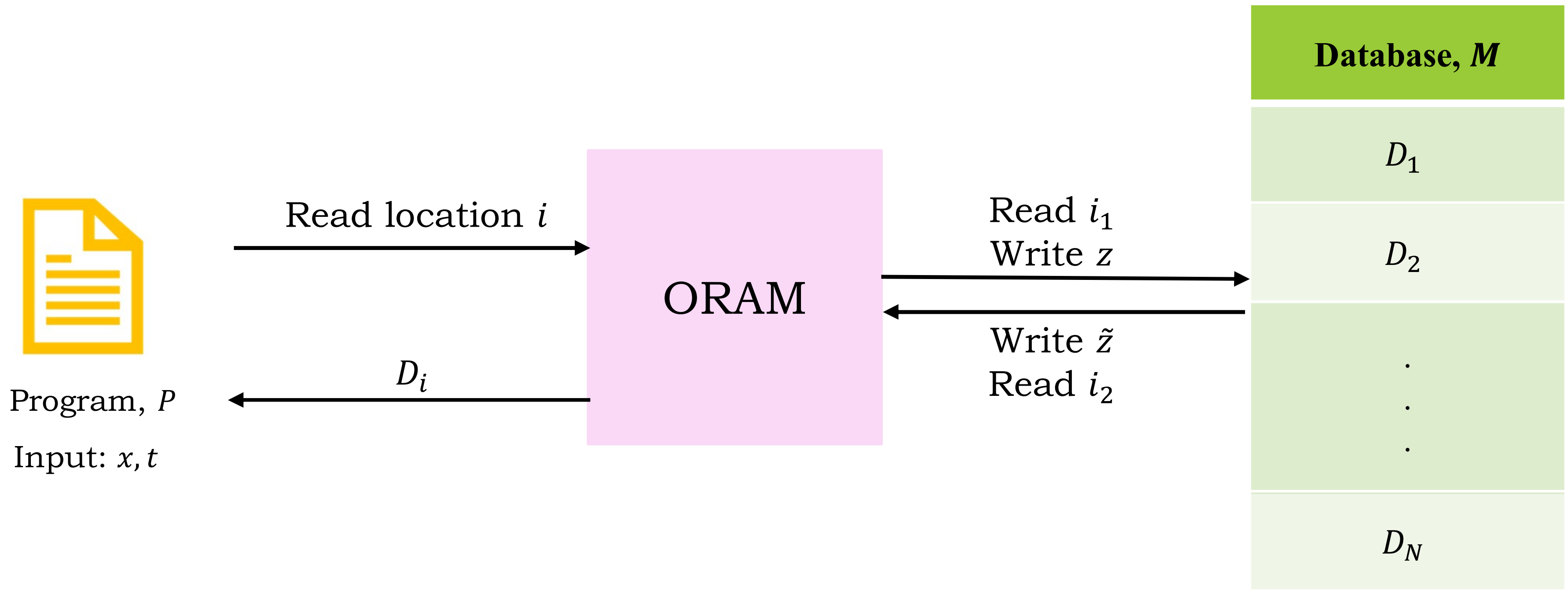
OUR GOAL:
Construct AD-SIM FE without relying on succinct KPFE.

Slide credits: [AMVY21]

Read Only Random Access Machine (RAM) Model of Computation



Oblivious RAM (ORAM) Model of computation

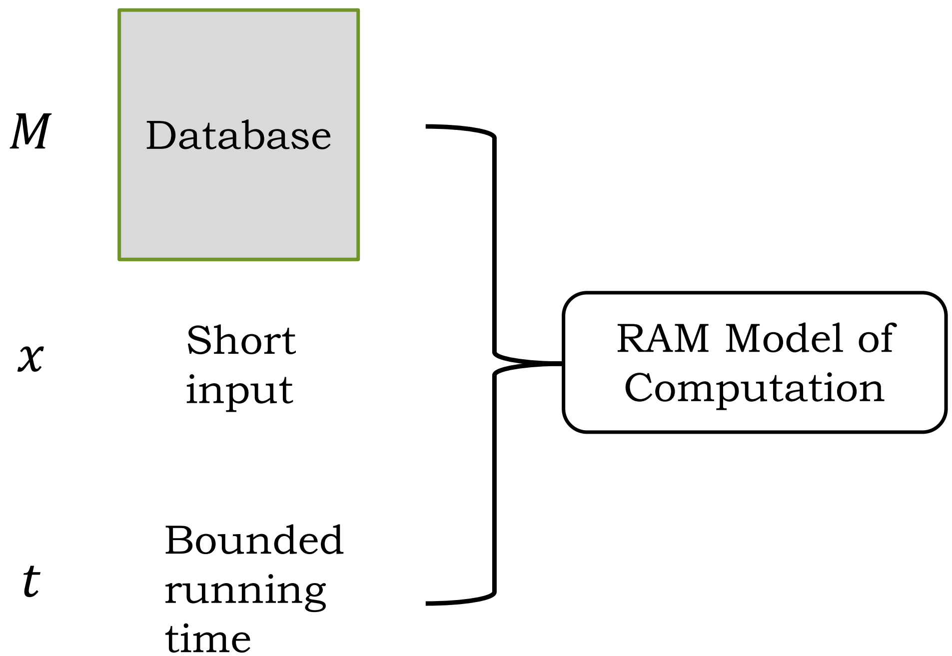


Security

ORAM hides the access location i.

Motivation for RAM model

FE for TM
$|(x, 1^t)| \leq |M|$

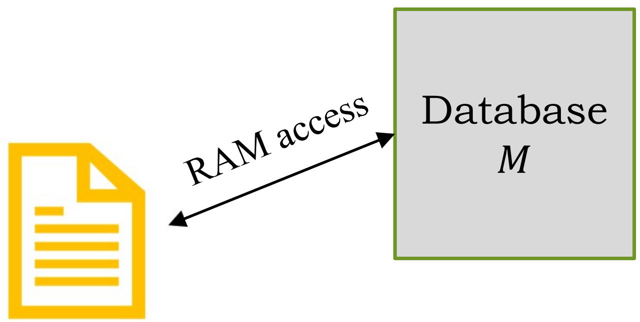


M is unbounded, $|x|, t$ is fixed.
Run M on x.
We will have

- Bounded number of lookups in the transition table
- Bounded number of steps

regardless of the size of M.

CPFE for (read only) RAM



Program, P
Executes $M(x)$

Introduce new primitive CPFE for (read only) RAM

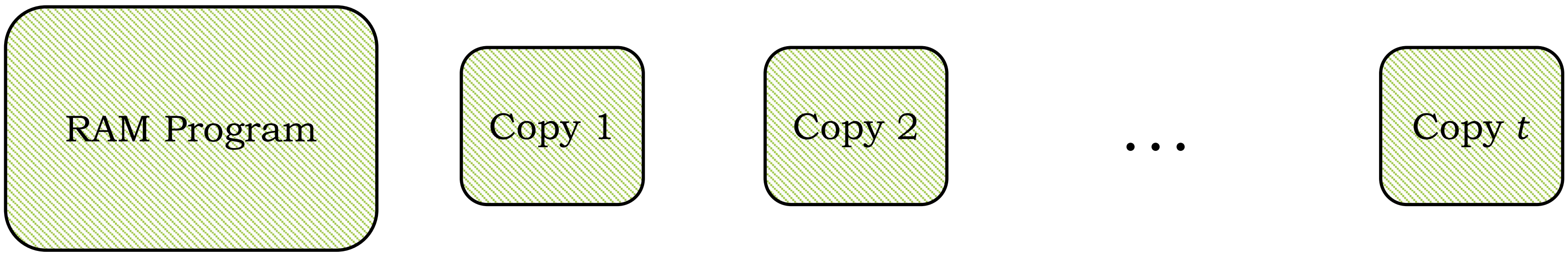
Encryptor
Encrypt
Program $P_{(x,1^t)}$

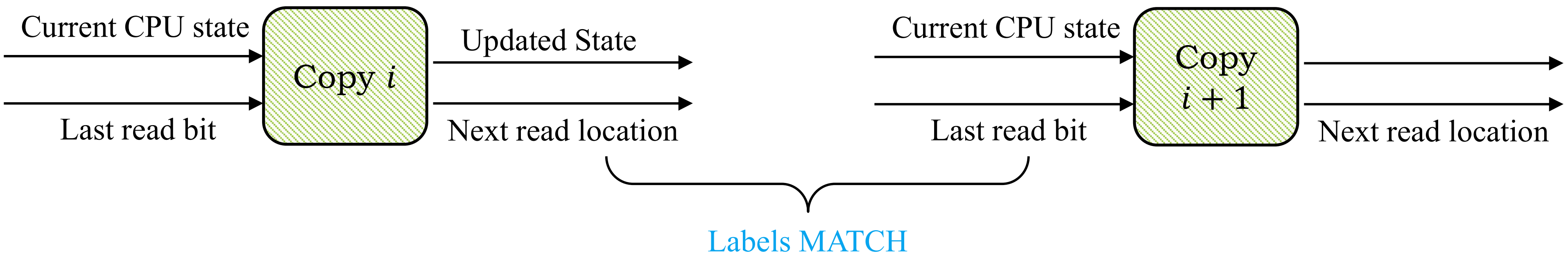
KeyGen
Provide key for M

Decryptor
Execute $P_{(x,1^t)}$ on x to give $M(x)$

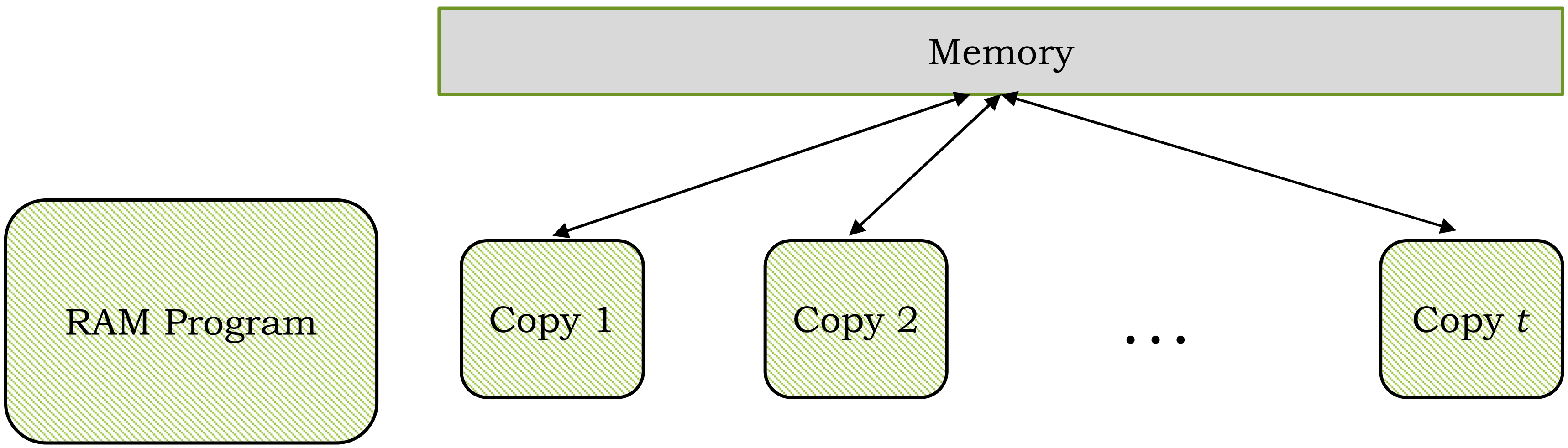
CPFE for (read only) RAM

Build upon ideas that were developed in the context of garbled RAM constructions [LO14].





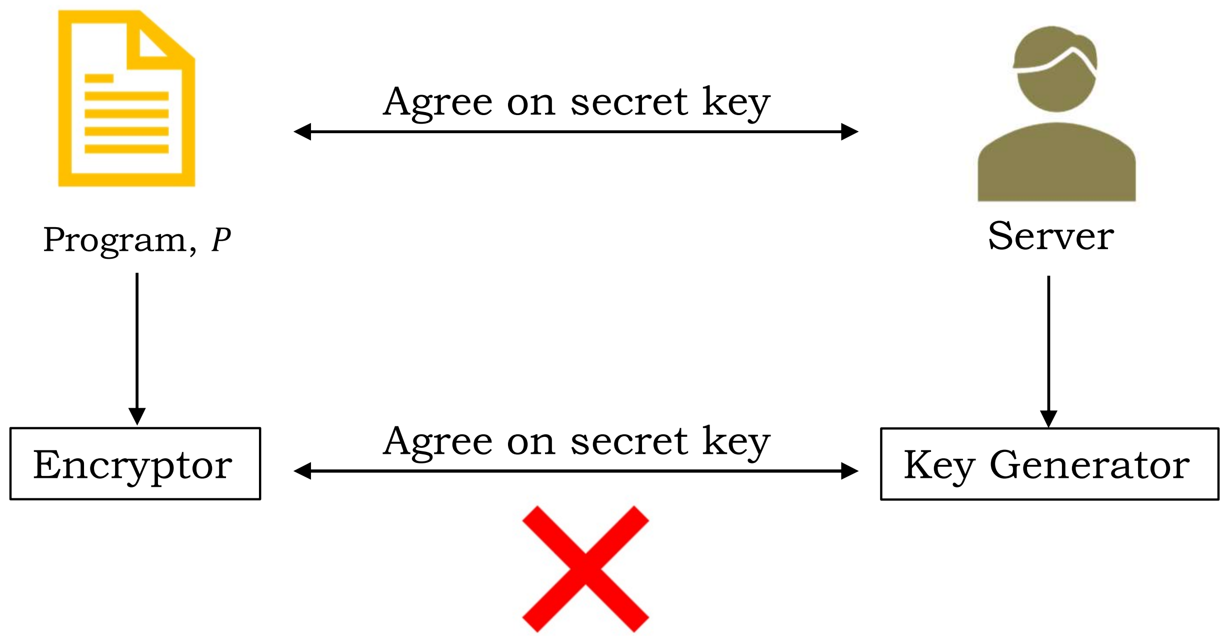
CPFE for (read only) RAM



To incorporate data from memory into computation, previous works used

IBE	Choose correct labels of GC
Oblivious RAM (ORAM)	Hide position read

Problem with ORAM



In our setting

Public Key Setting

Solution: Introduce FE for LOT (LOTFE)

FE for LOT (LOTFE)

Encryptor
Has two msg μ_0, μ_1 and DB location i

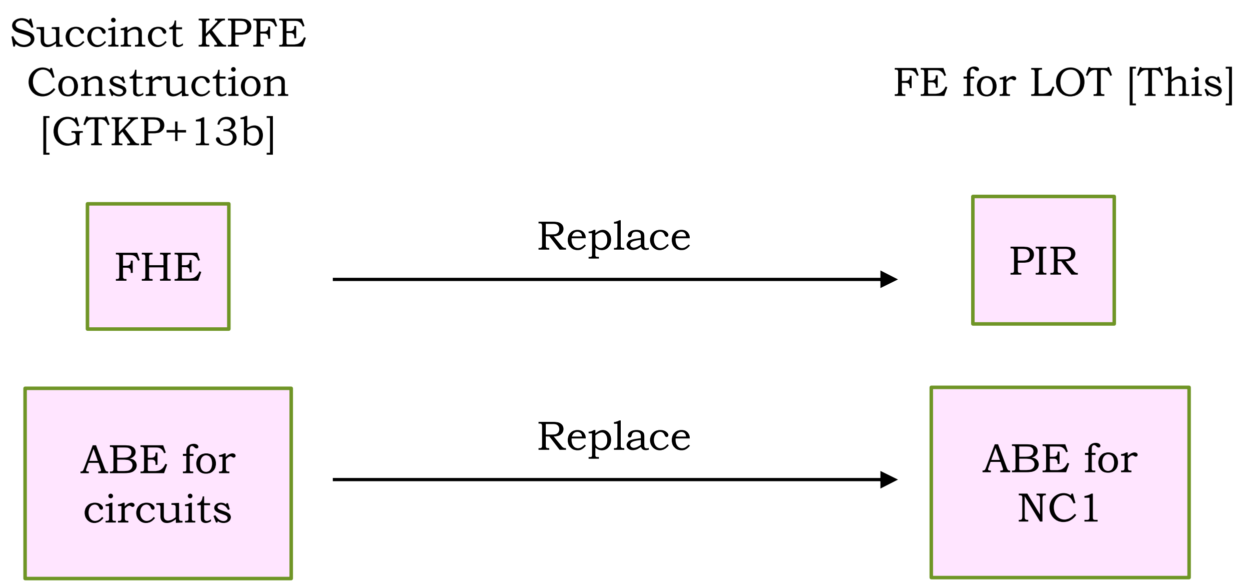
KeyGen
Input is DB, D

Decryptor
Allows to recover $\mu_{D[i]}$

Security: $\mu_{1-D[i]}$ and i are hidden

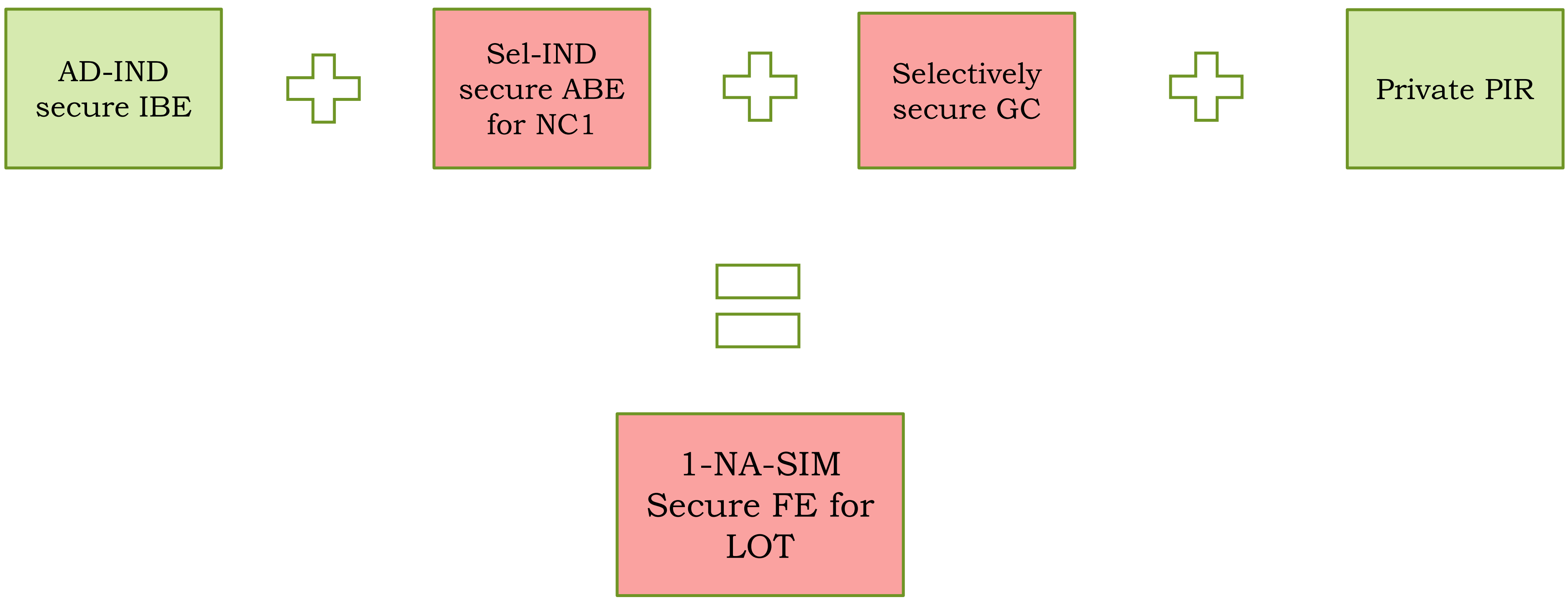
FE for LOT (LOTFE)

Need to support TABLE LOOKUP FUNCTIONALITY

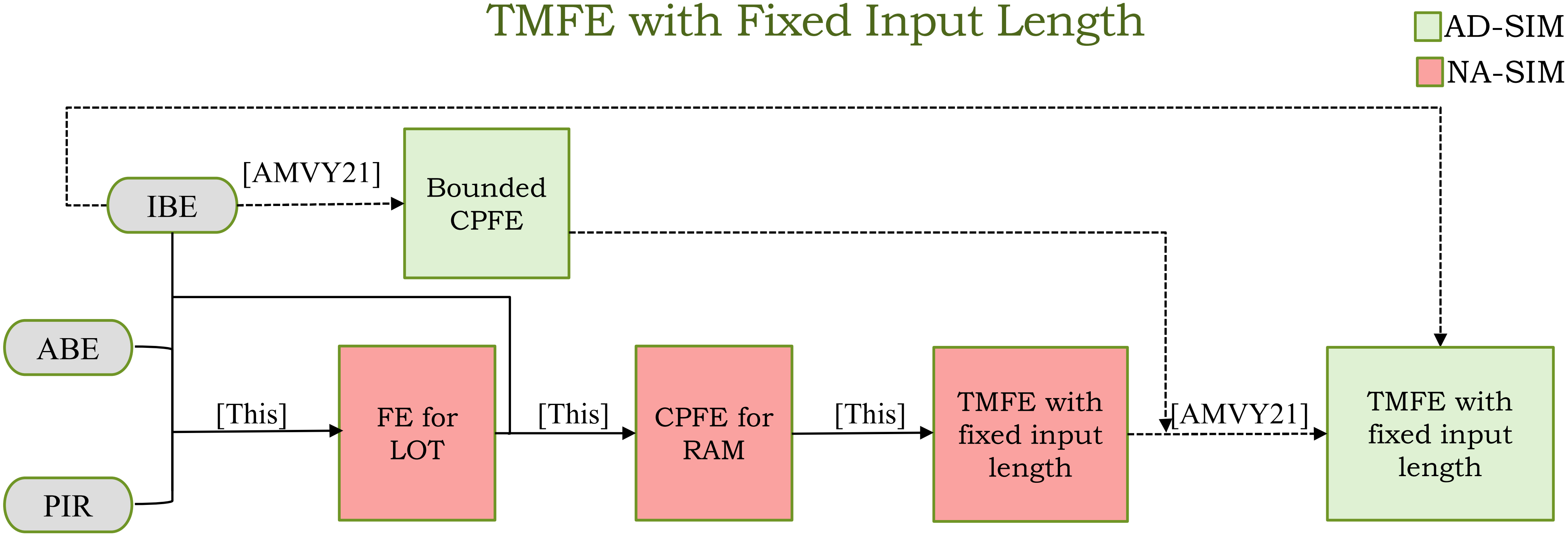


FE for LOT (LOTFE)

AD-SIM
NA-SIM



TMFE with Fixed Input Length



Thank you