Beyond Birthday Bound Length Doubling

Yu Long Chen[1] Bart Mennink[2] Mridul Nandi[3]

imec-COSIC, KU Leuven

Digital Security Group, Radboud University, Nijmegen

Indian Statistical Institute, Kolkata

November 13, 2018

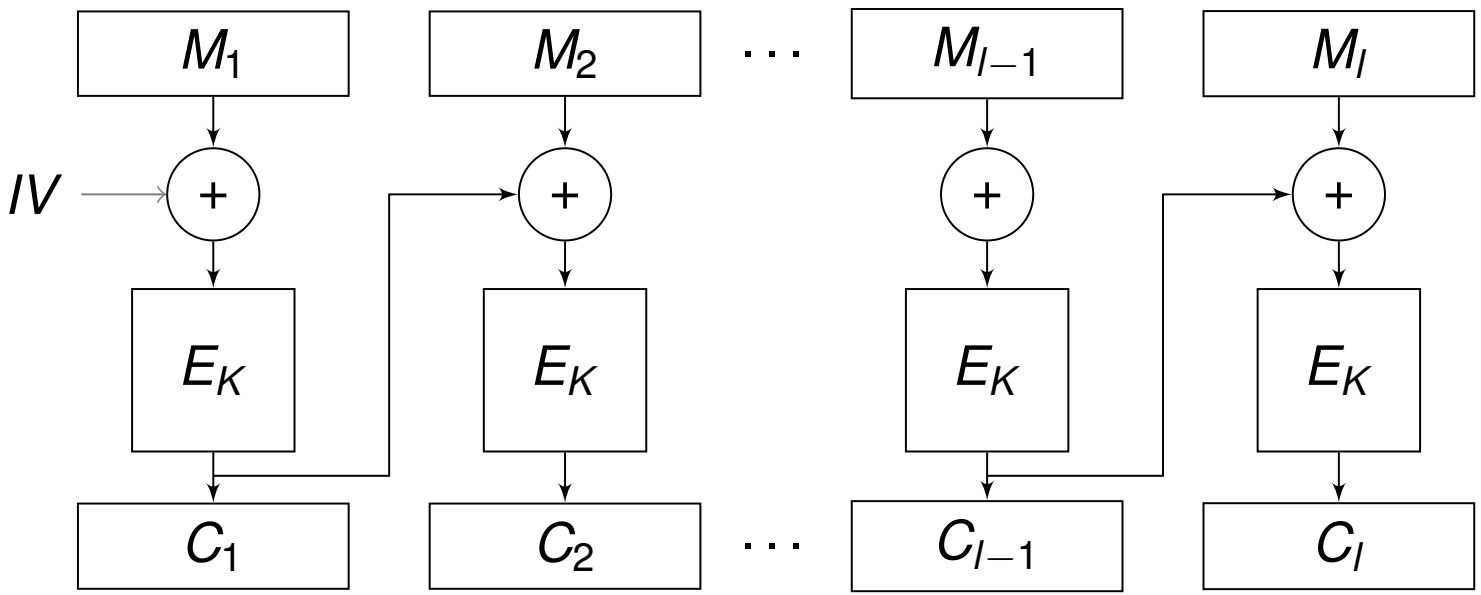
Modes of Operation

- Block cipher: fixed-input-length (FIL)

Modes of Operation

- Block cipher: fixed-input-length (FIL)
- Apply block cipher iteratively

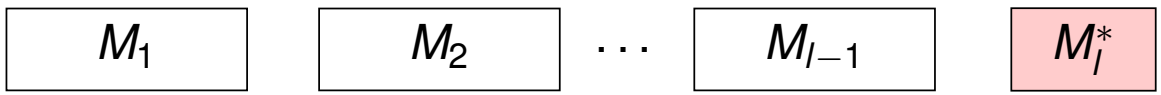
CBC mode



Modes of Operation

Fractional data $\Longrightarrow$ padding

CBC+padding



Modes of Operation

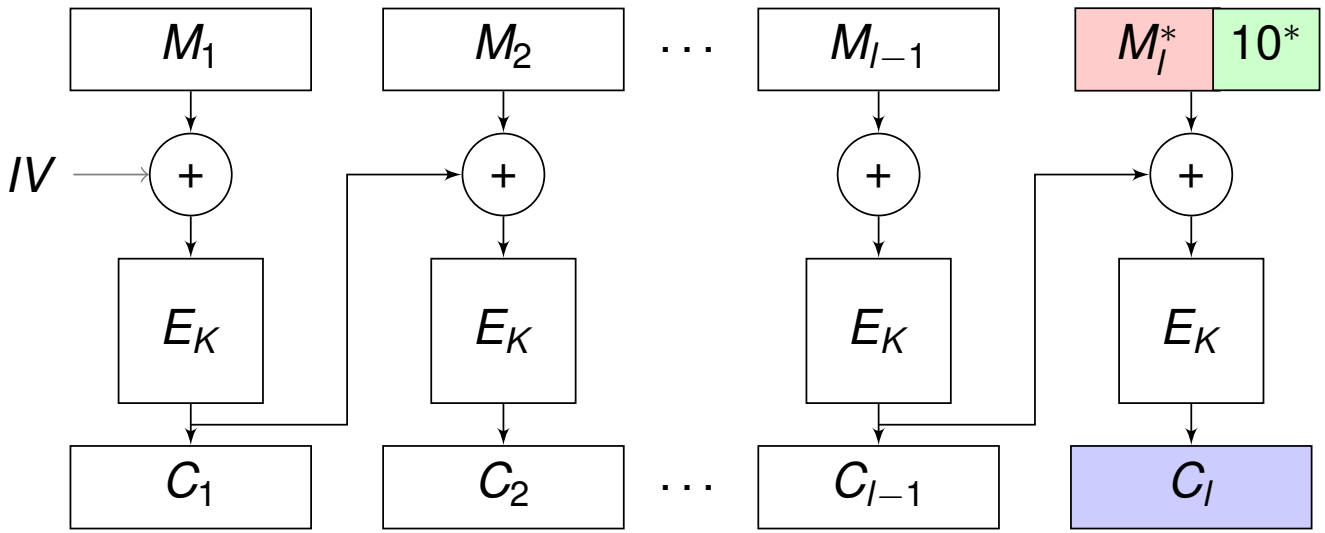
Fractional data $\Longrightarrow$ padding

CBC+padding

Modes of Operation

Fractional data $\Longrightarrow$ padding

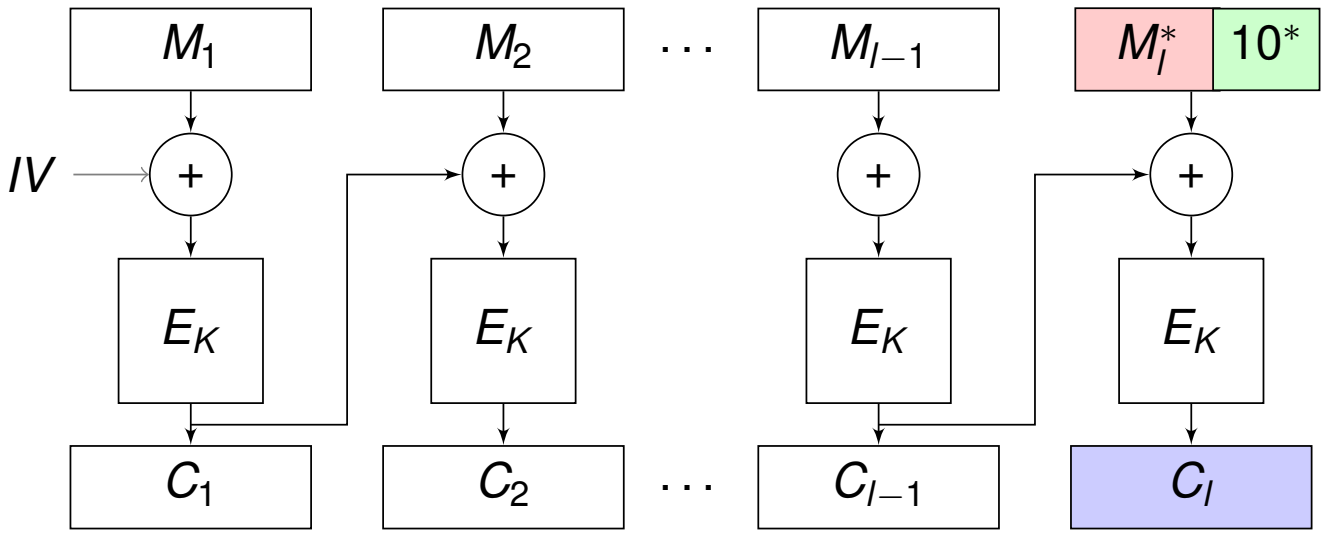
CBC+padding



Modes of Operation

Fractional data $\Longrightarrow$ padding

CBC+padding



Ciphertext expansion: $|C| > |M|$

Avoiding Ciphertext Expansion

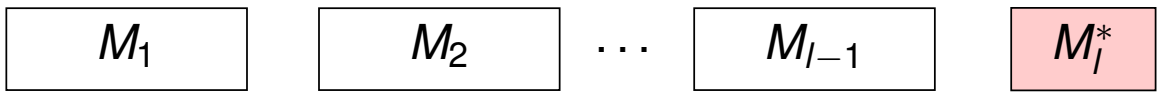
1. CTR: turns block cipher into stream cipher
   $\Longrightarrow$ not suitable for some applications

Avoiding Ciphertext Expansion

1. CTR: turns block cipher into stream cipher
   $\Longrightarrow$ not suitable for some applications
2. Non-generic methods: EME, TET, HEH, HCTR, HCH, XCB

Avoiding Ciphertext Expansion

1. CTR: turns block cipher into stream cipher
   $\Longrightarrow$ not suitable for some applications
2. Non-generic methods: EME, TET, HEH, HCTR, HCH, XCB
3. Ciphertext stealing:

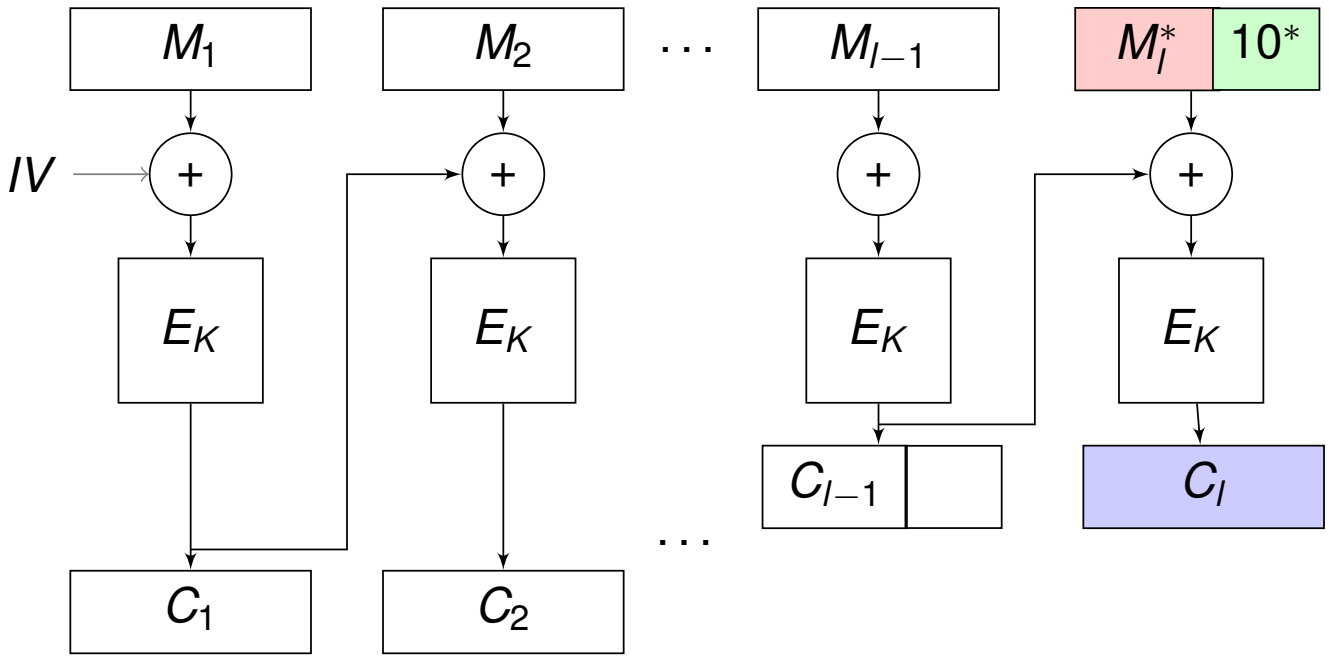


Avoiding Ciphertext Expansion

1. CTR: turns block cipher into stream cipher
   $\Longrightarrow$ not suitable for some applications
2. Non-generic methods: EME, TET, HEH, HCTR, HCH, XCB
3. Ciphertext stealing:

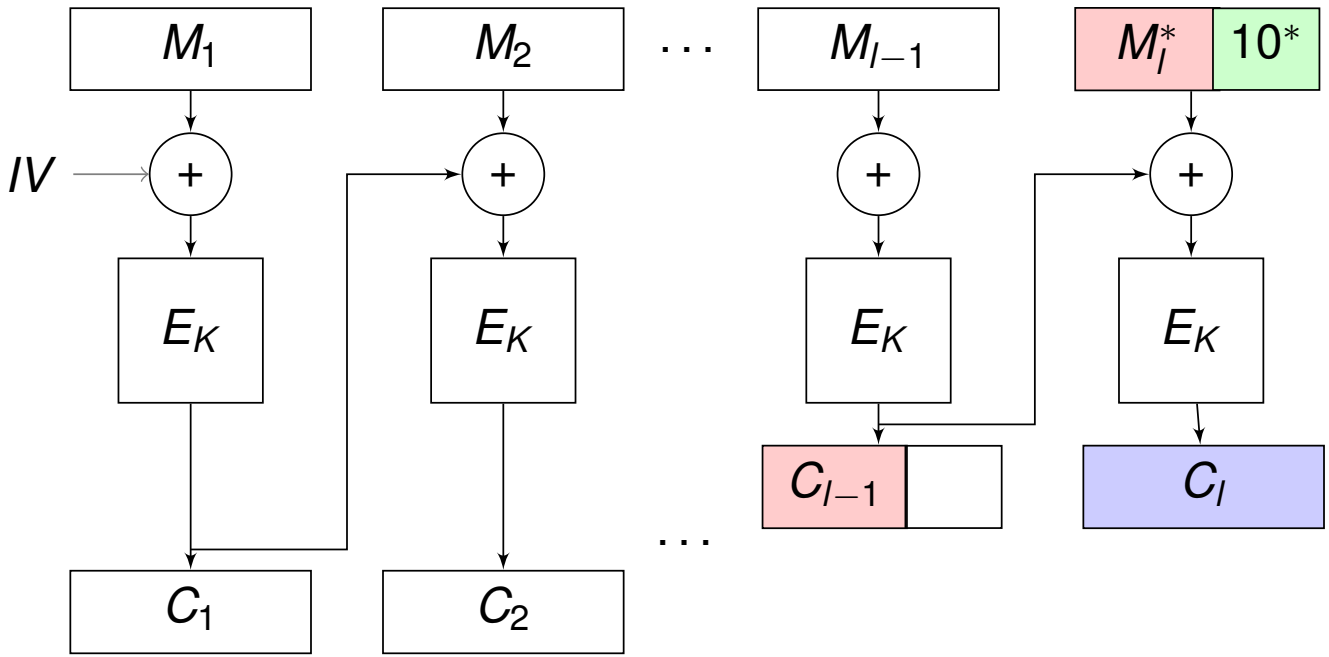
Avoiding Ciphertext Expansion

1. CTR: turns block cipher into stream cipher
   $\Longrightarrow$ not suitable for some applications
2. Non-generic methods: EME, TET, HEH, HCTR, HCH, XCB
3. Ciphertext stealing:



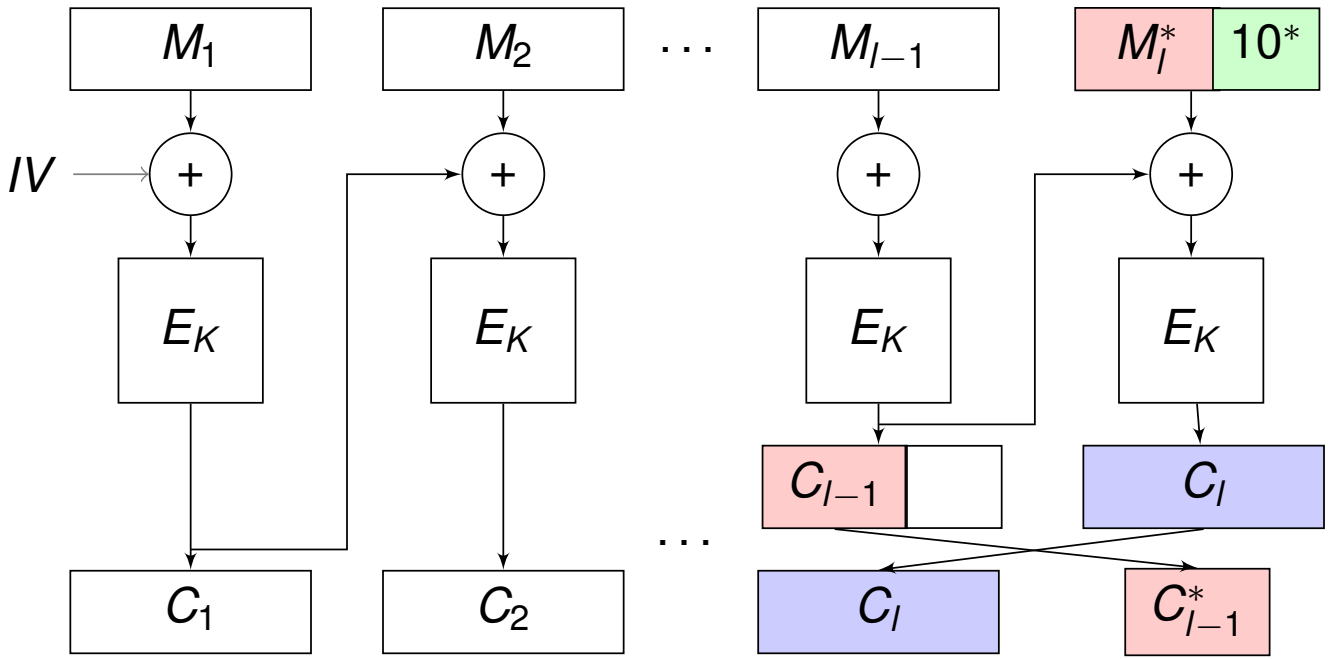
Avoiding Ciphertext Expansion

1. CTR: turns block cipher into stream cipher
   $\Longrightarrow$ not suitable for some applications
2. Non-generic methods: EME, TET, HEH, HCTR, HCH, XCB
3. Ciphertext stealing:



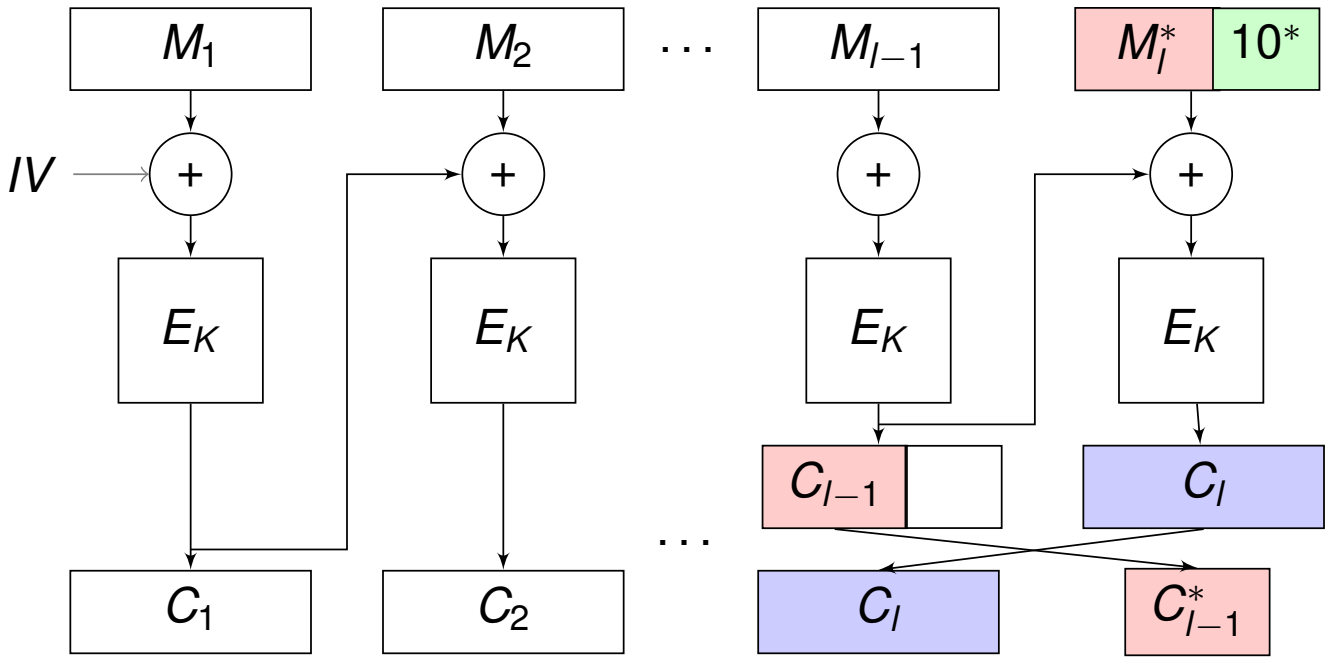
Avoiding Ciphertext Expansion

1. CTR: turns block cipher into stream cipher
   $\Longrightarrow$ not suitable for some applications
2. Non-generic methods: EME, TET, HEH, HCTR, HCH, XCB
3. Ciphertext stealing:



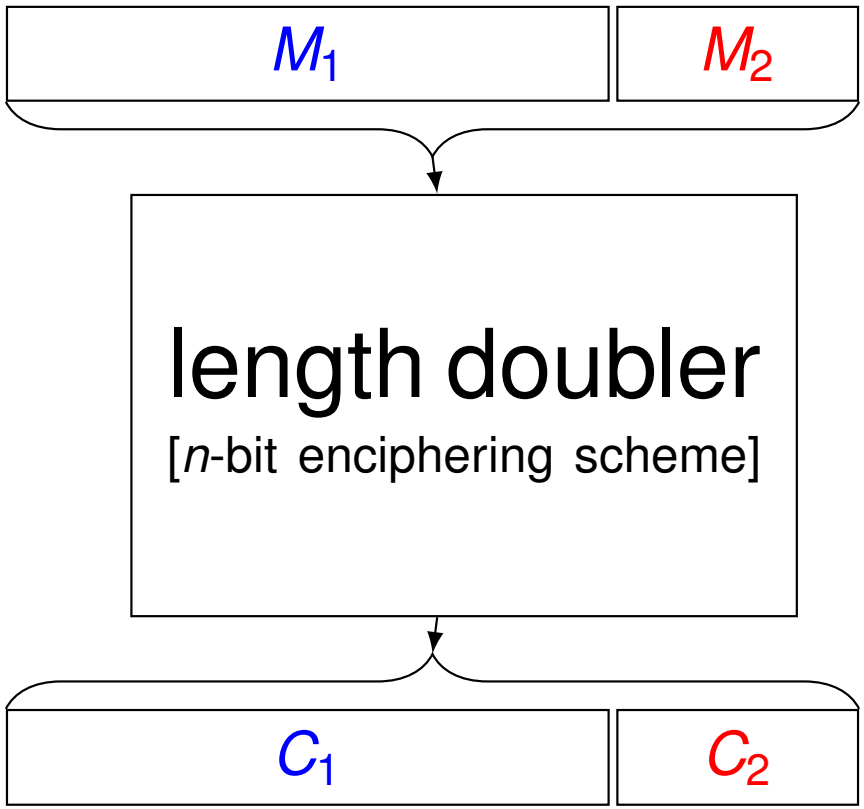
Avoiding Ciphertext Expansion

1. CTR: turns block cipher into stream cipher
   $\Longrightarrow$ not suitable for some applications
2. Non-generic methods: EME, TET, HEH, HCTR, HCH, XCB
3. Ciphertext stealing:



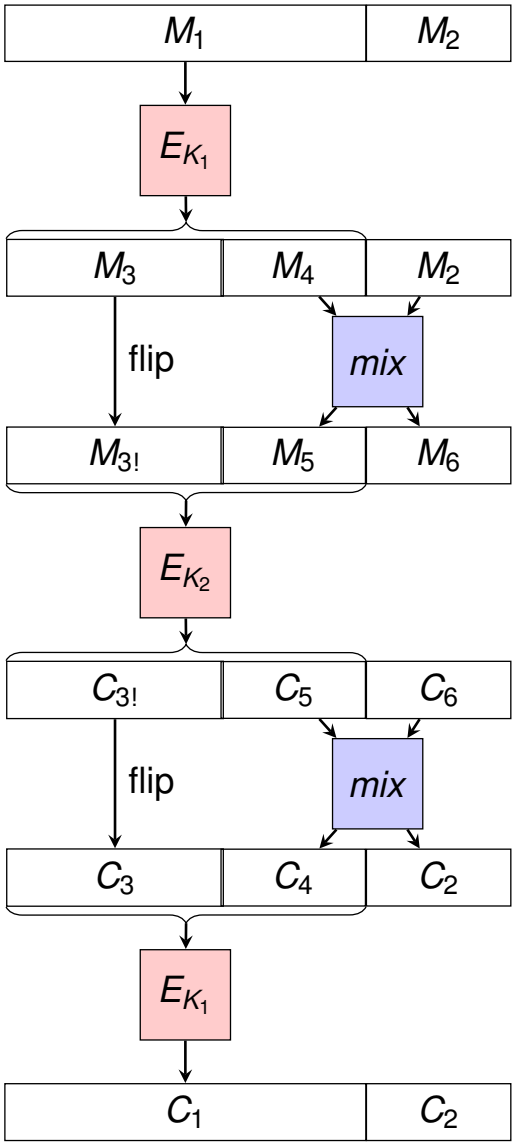
- Condition: C_i's need to be decrypted independently

Length Doublers



- $|M_1| = |C_1| = n =$ block size
- $|M_2| = |C_2| \in [0, n-1]$

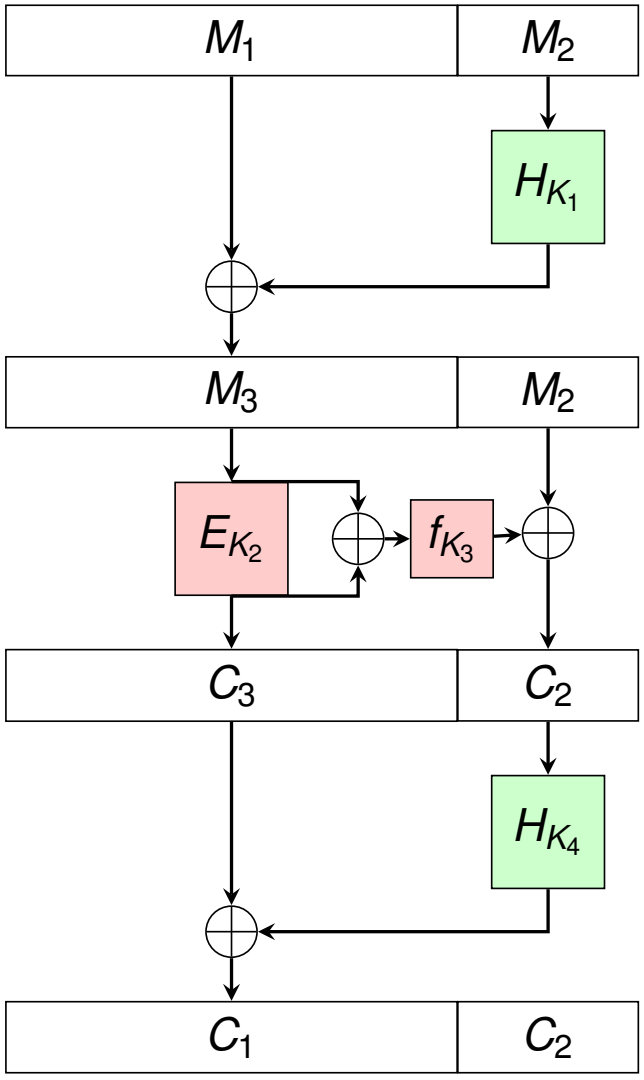
XLS



Ristenpart and Rogaway (2007)

- ϵ-good mixing function
- Broken by Nandi in 2014

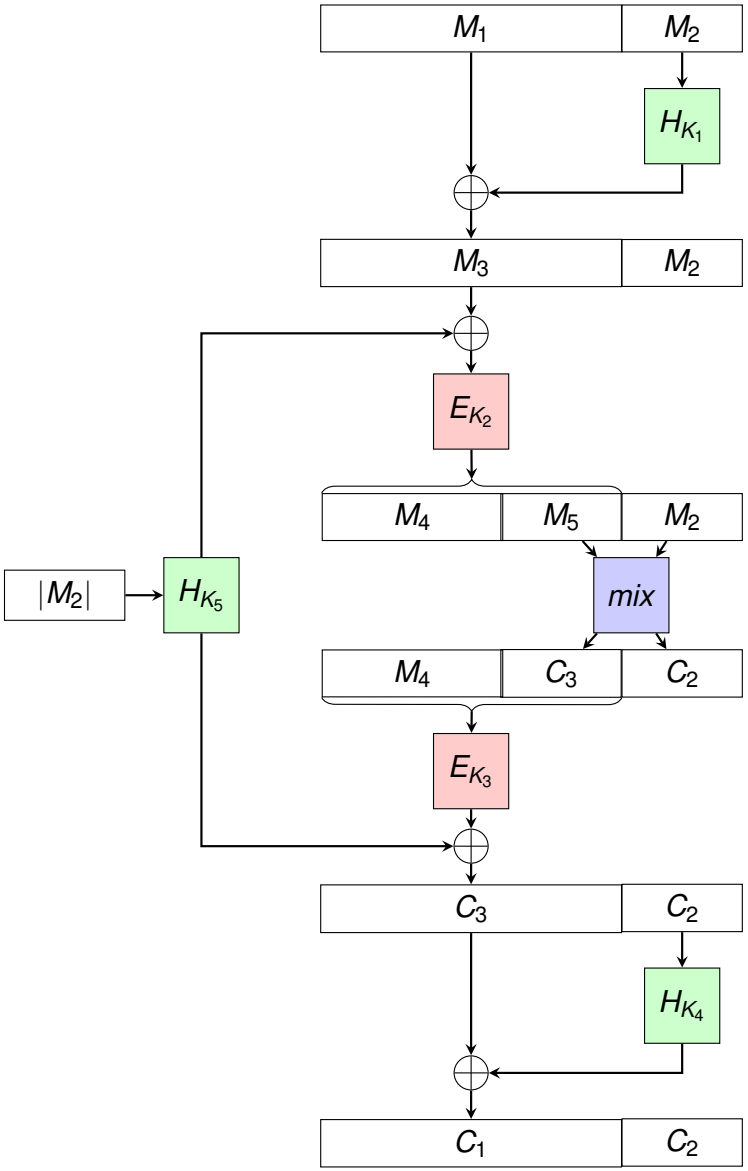
DE



Nandi (2009)

- Four cryptographic primitive calls

HEM



Zhang (2012)

- Five cryptographic primitive calls
- ϵ-good mixing function

State of the Art

length doubler	security ($\log_2$)	key length	cryptographic primitive calls	mixing function
XLS	$n/2$	$2n$	3 BC	ϵ-good
DE	$n/2$	$5n$	4 hash+BC	-
HEM	$n/2$	$3n$	4 hash+BC	ϵ-good

State of the Art

length doubler	security ($\log_2$)	key length	cryptographic primitive calls	mixing function
XLS	$n/2$	$2n$	3 BC	ϵ-good
DE	$n/2$	$5n$	4 hash+BC	-
HEM	$n/2$	$3n$	4 hash+BC	ϵ-good
LDT	$n/2$	$2n$	2 TBC	pure-good

State of the Art

length doubler	security ($\log_2$)	key length	cryptographic primitive calls	mixing function
XLS	$n/2$	$2n$	3 BC	ϵ-good
DE	$n/2$	$5n$	4 hash+BC	-
HEM	$n/2$	$3n$	4 hash+BC	ϵ-good
LDT	$n/2$	$2n$	2 TBC	pure-good

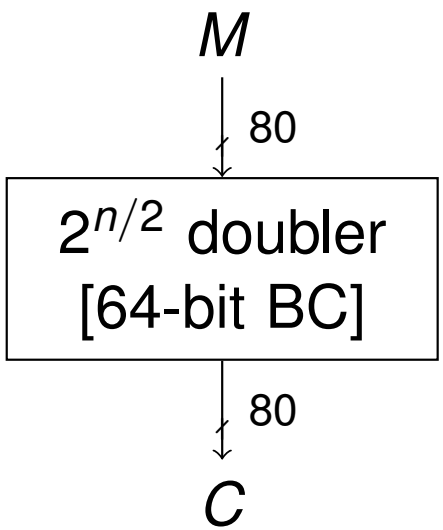
LDT: beyond $2^{n/2}$ security?

Beyond Birthday Bound Length Doubler

- Format-preserving encryption
- Electronic product code tag encryption

Beyond Birthday Bound Length Doubler

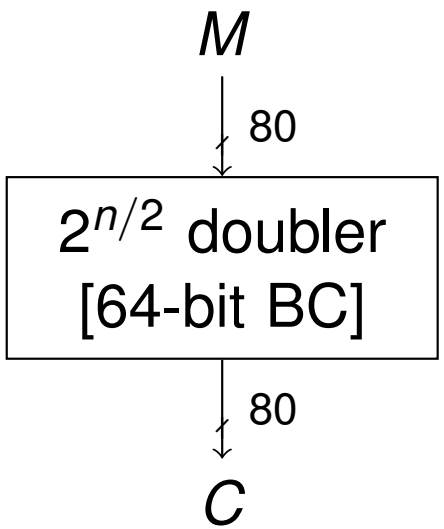
- Format-preserving encryption
- Electronic product code tag encryption



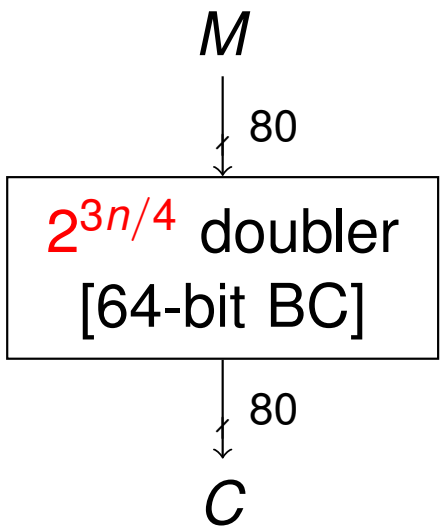
32-bits security

Beyond Birthday Bound Length Doubler

- Format-preserving encryption
- Electronic product code tag encryption

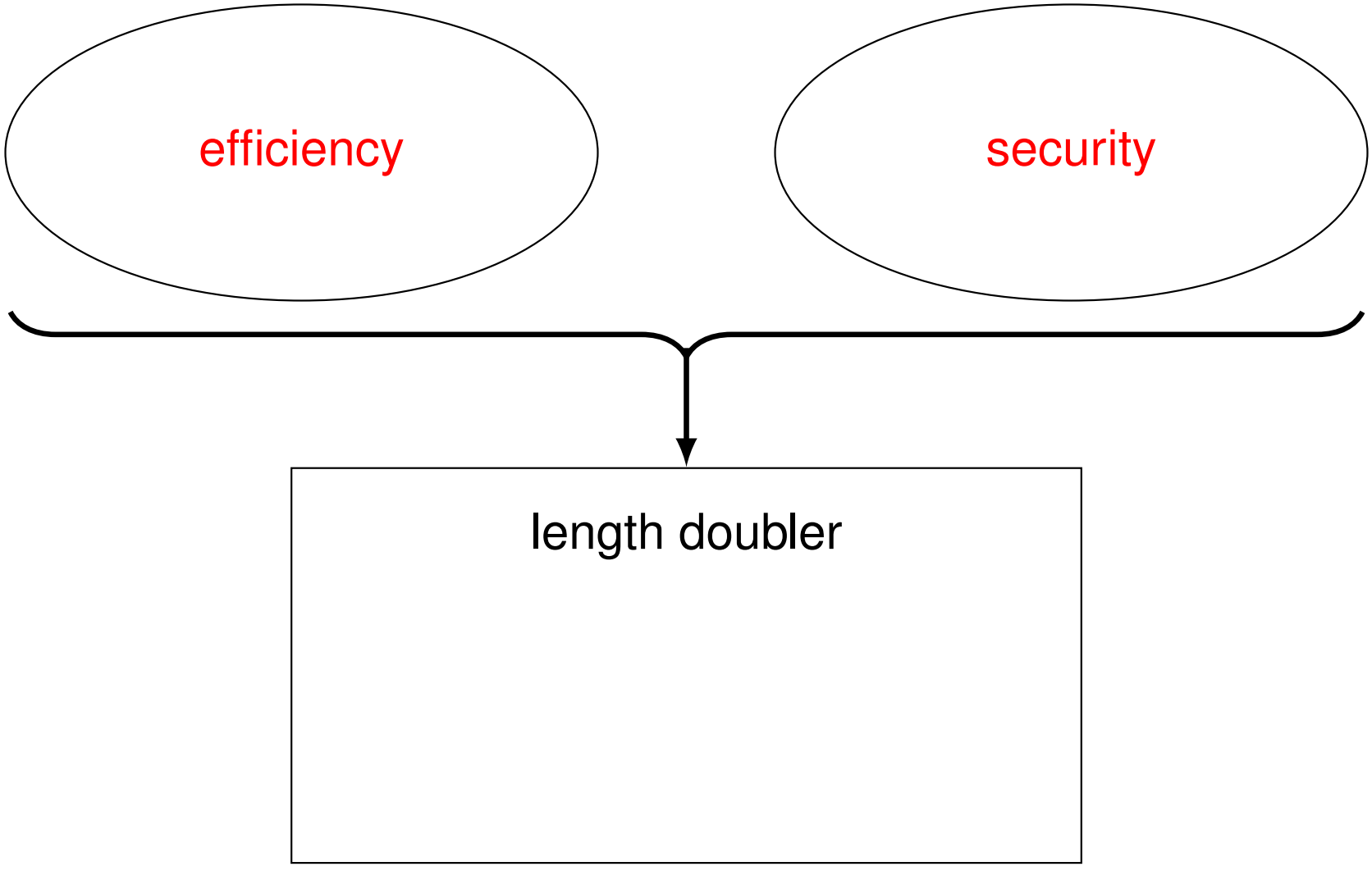


32-bits security

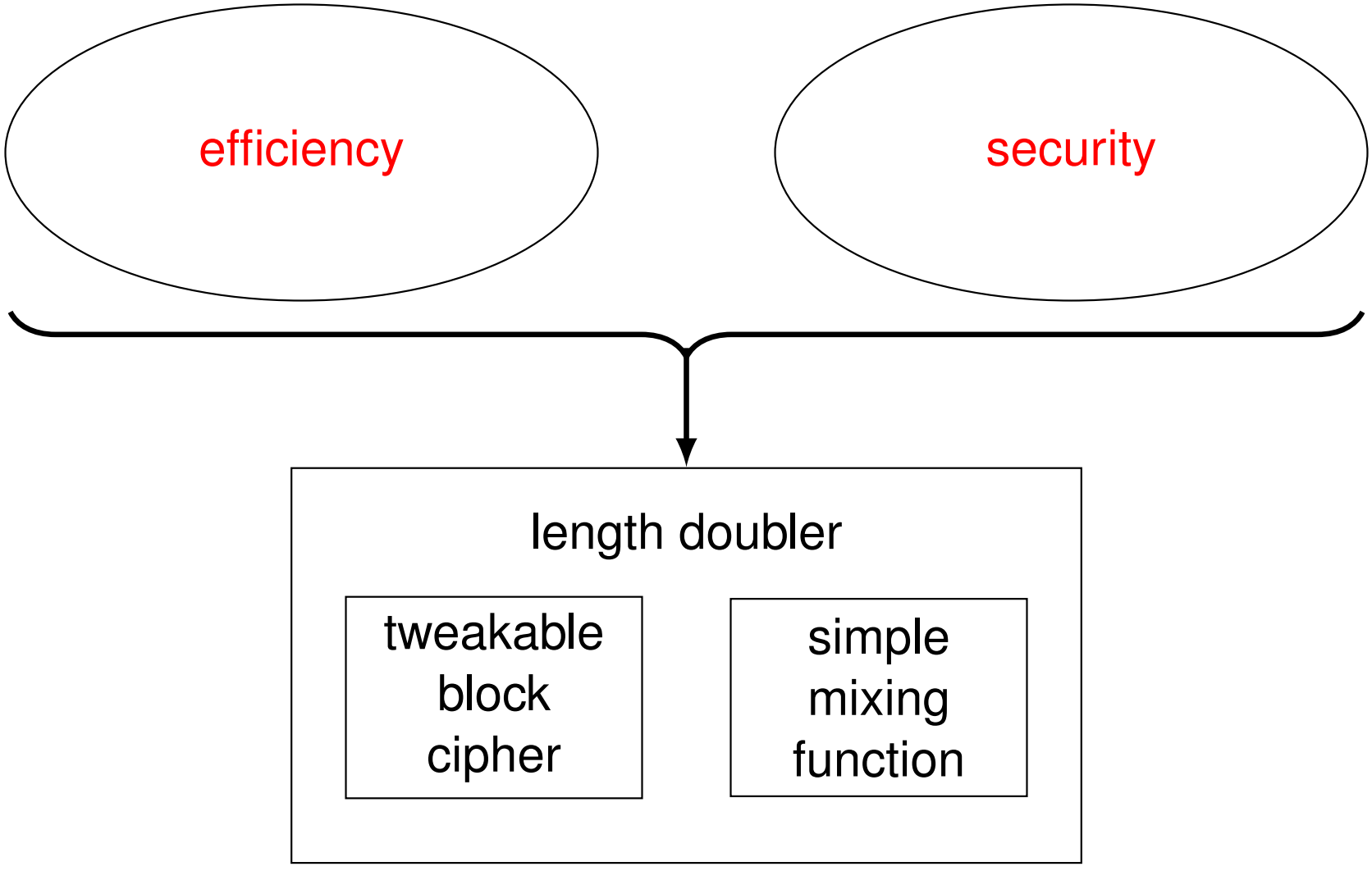


48-bits security

LDT Construction: Main Idea

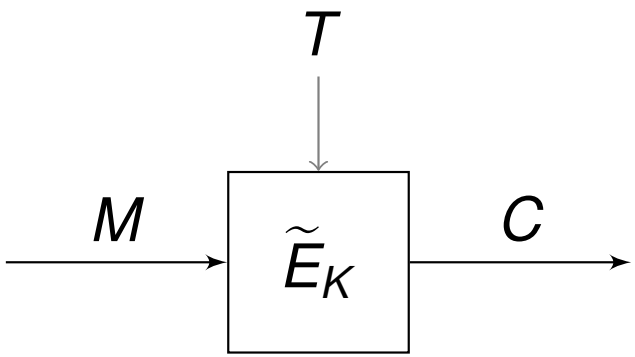


LDT Construction: Main Idea



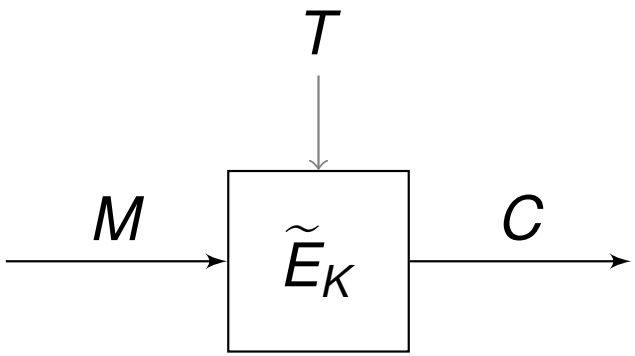
Tweakable Block Ciphers

- Extension of conventional block cipher
- Different tweak $T \longrightarrow$ independent permutation



Tweakable Block Ciphers

- Extension of conventional block cipher
- Different tweak $T \longrightarrow$ independent permutation



Examples

- LRW, CRYPTO 2002
- XEX, ASIACRYPT 2004
- TWEAKEY, ASIACRYPT 2014
- SKINNY, CRYPTO 2016

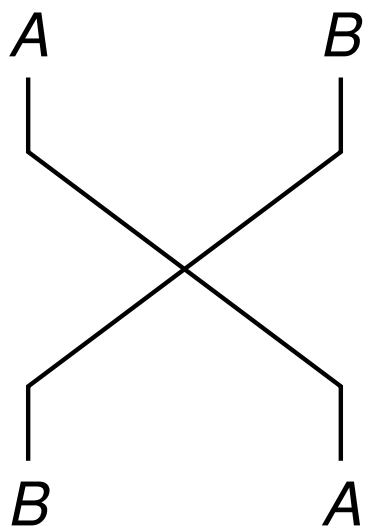
Pure Mixing Functions

- ϵ-good mixing functions: smaller ϵ is better
- ϵ-good mixing functions $\Longrightarrow$ pure mixing functions
- Easier to construct than ϵ-good mixing functions

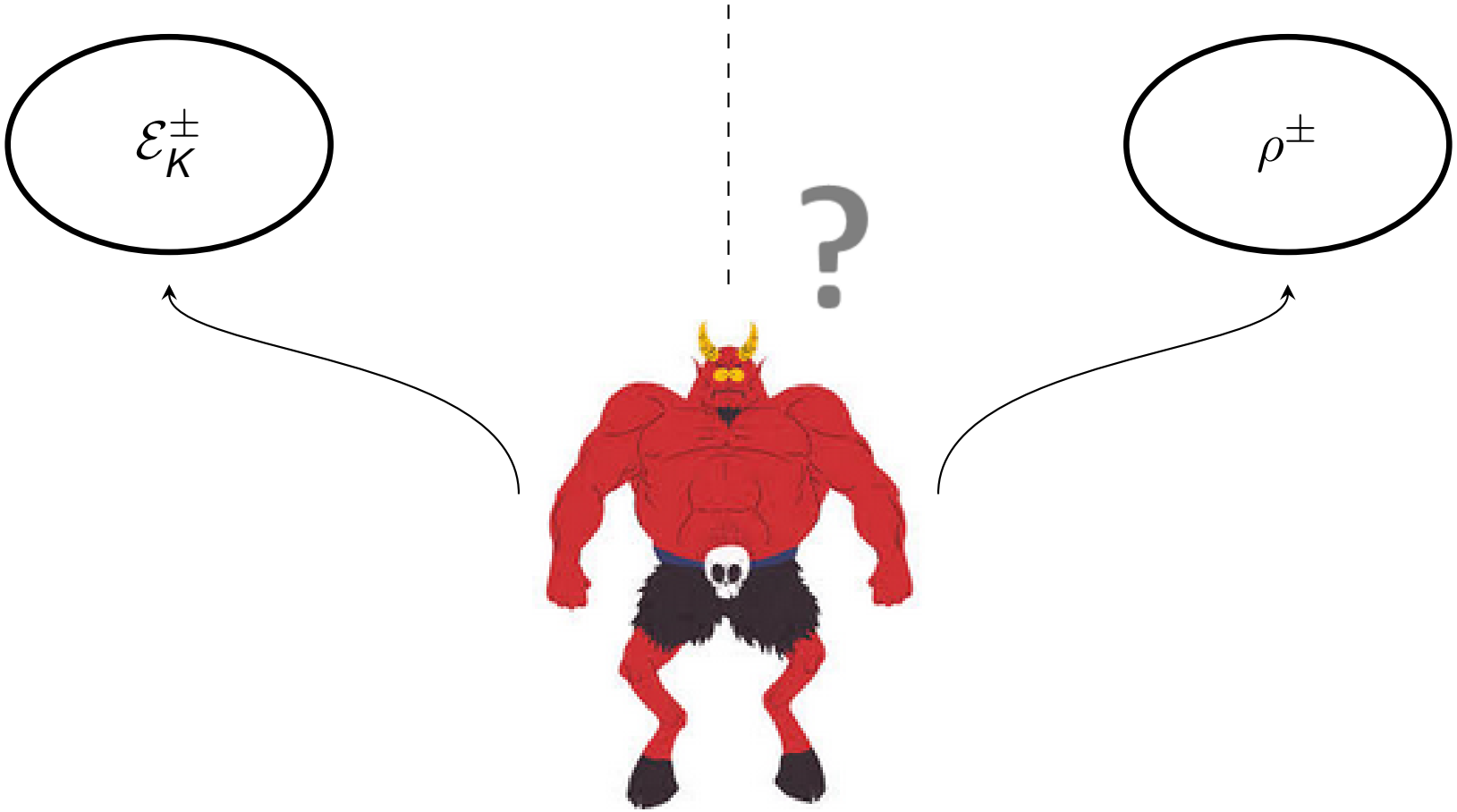
Pure Mixing Functions

- ϵ-good mixing functions: smaller ϵ is better
- ϵ-good mixing functions $\Longrightarrow$ pure mixing functions
- Easier to construct than ϵ-good mixing functions

Simplest example (not ϵ-good)



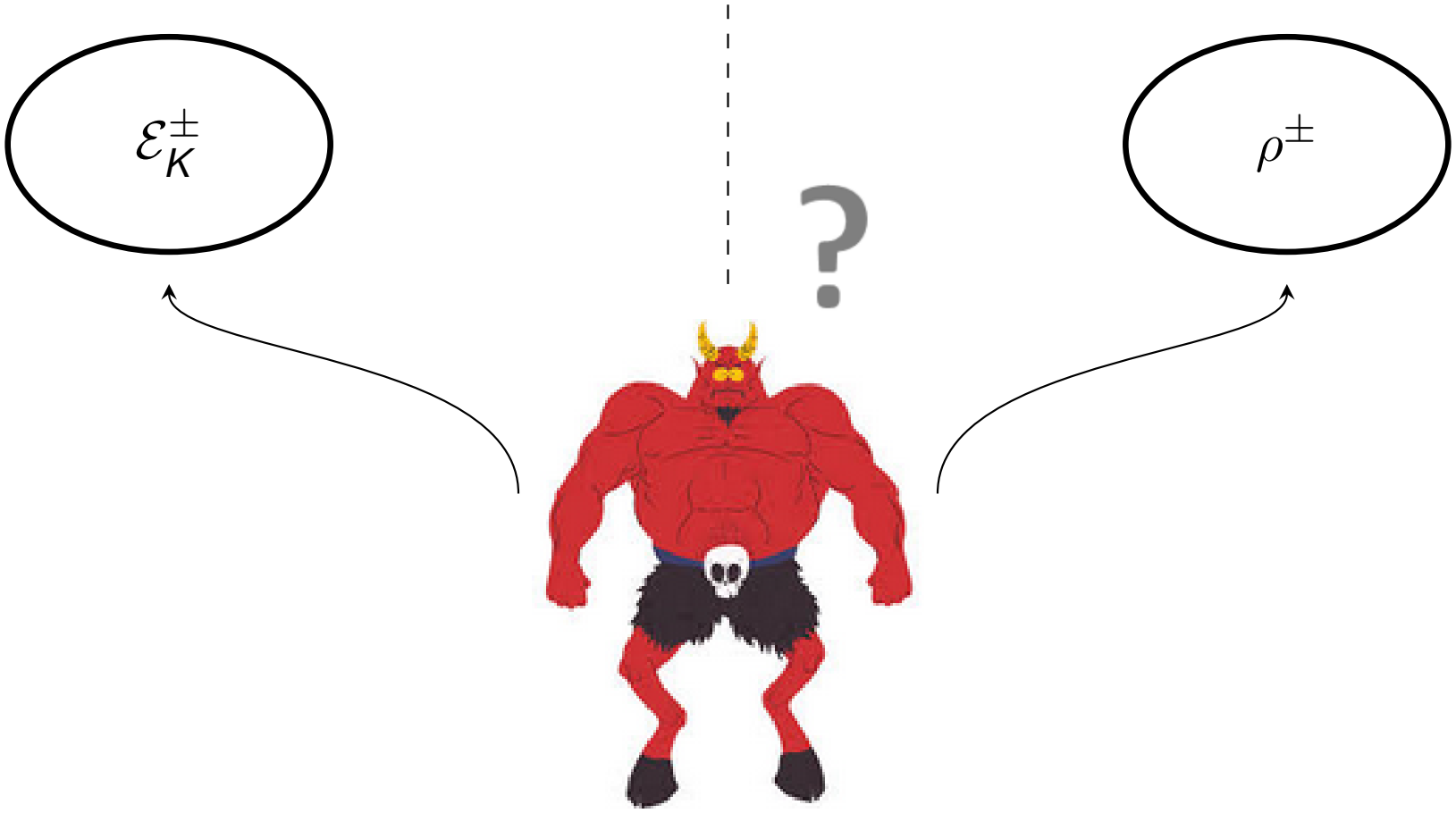
Security Definition



adversary $\mathcal{A}$

- Adversary $\mathcal{A}$ makes q queries to oracle ($\mathcal{E}_K$ or ρ)

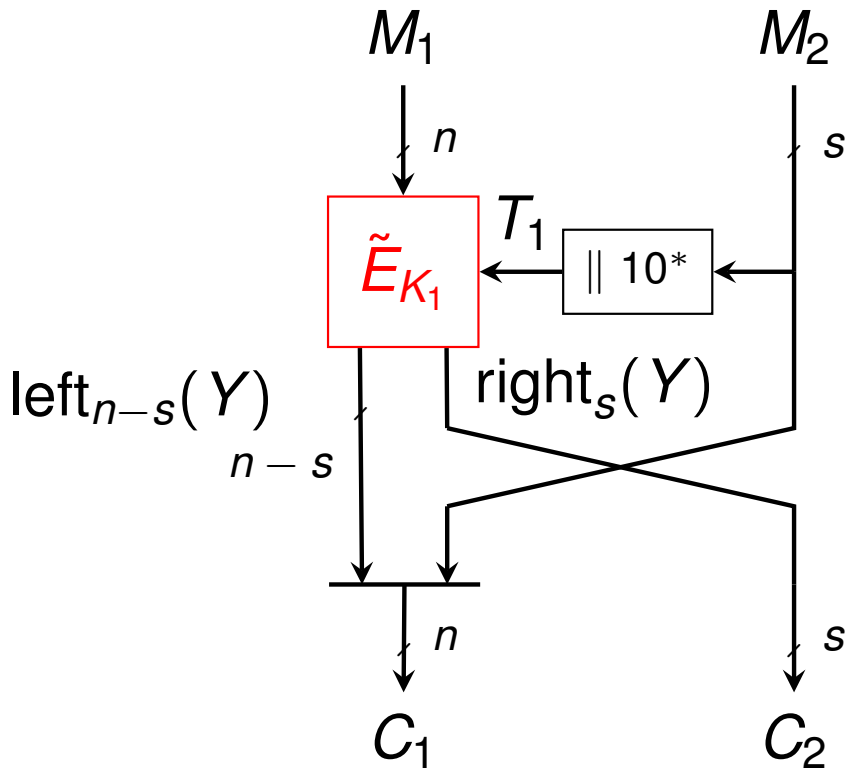
Security Definition



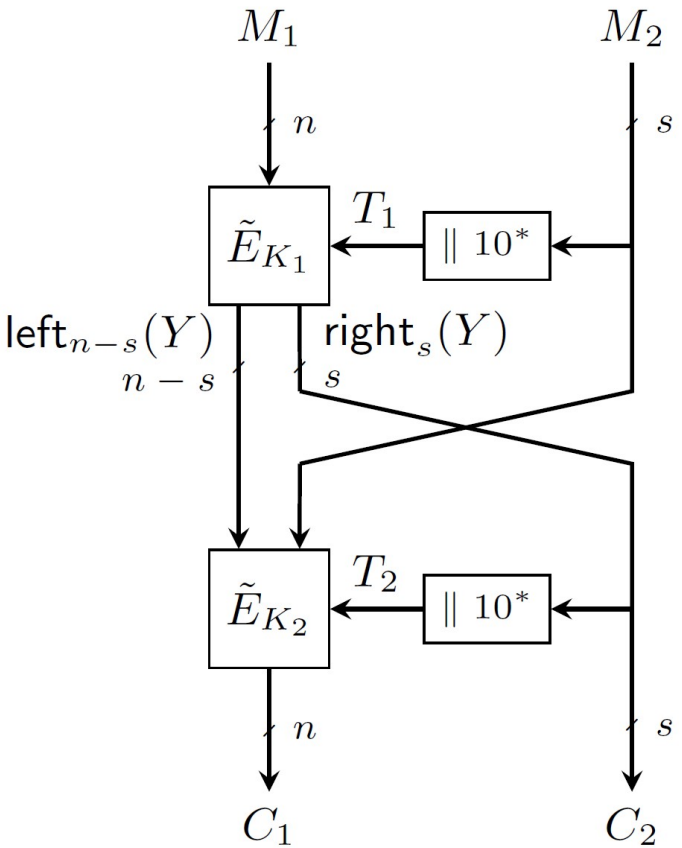
adversary $\mathcal{A}$

- Adversary $\mathcal{A}$ makes q queries to oracle ($\mathcal{E}_K$ or ρ)
- Strong length-preserving pseudorandom permutation
  $\iff$ $\mathcal{A}$ cannot determine which world it is interacting with

Round Function $F[\tilde{E}_K]$



2-LDT



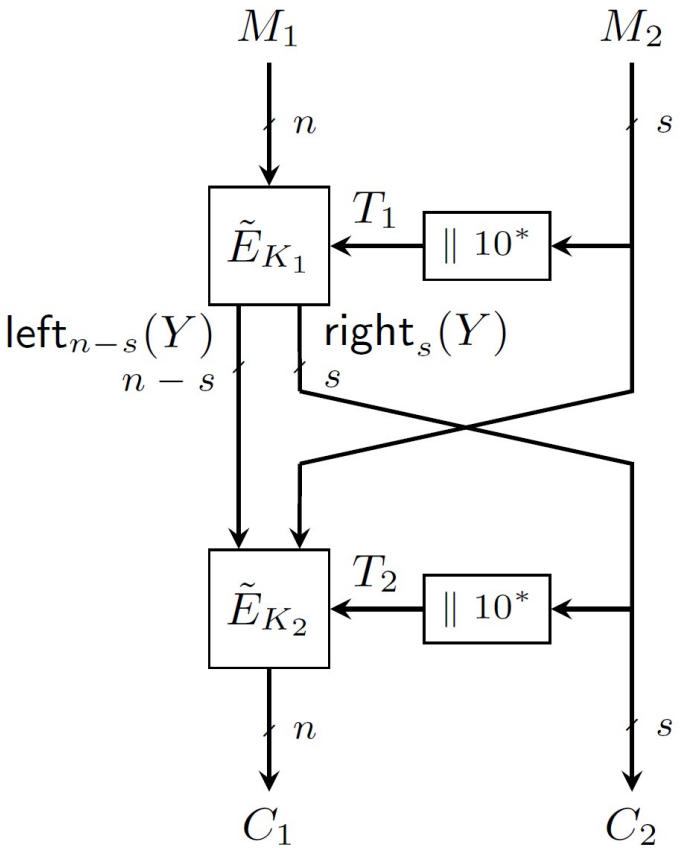
Security upper bound:

- $2^{n-(s/2)}$

Security lower bound

- $2^{n/2}$ (ToSC 2017(3))

2-LDT



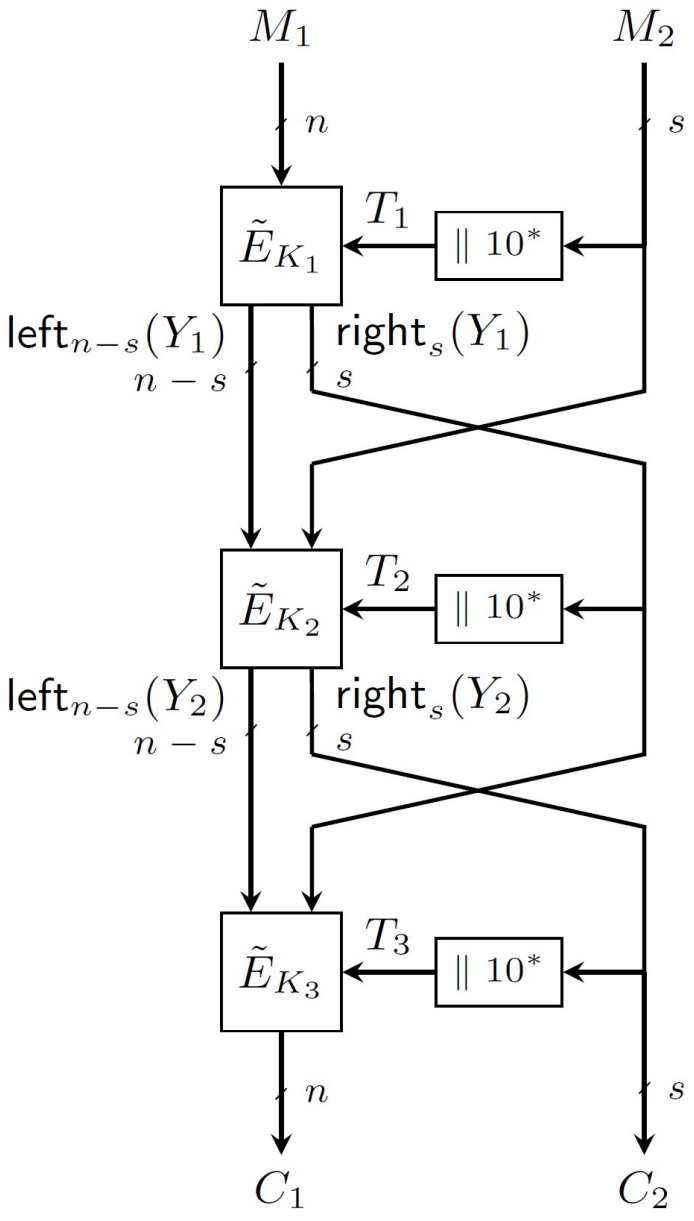
Security upper bound:

- $2^{n-(s/2)}$

Security lower bound

- ~~$2^{n/2}$ (ToSC 2017(3))~~
- "New bound"

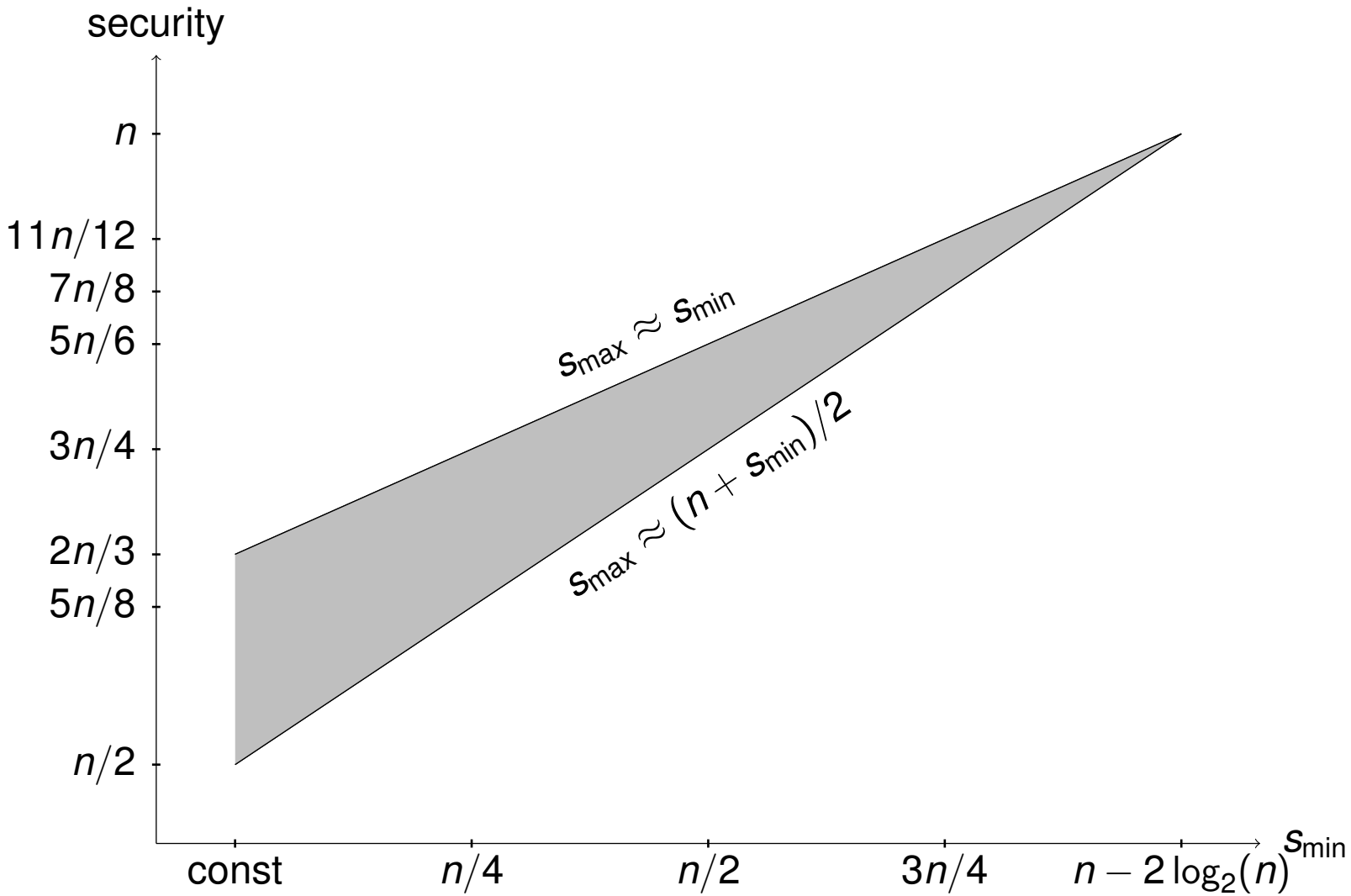
3-LDT



Security lower bound

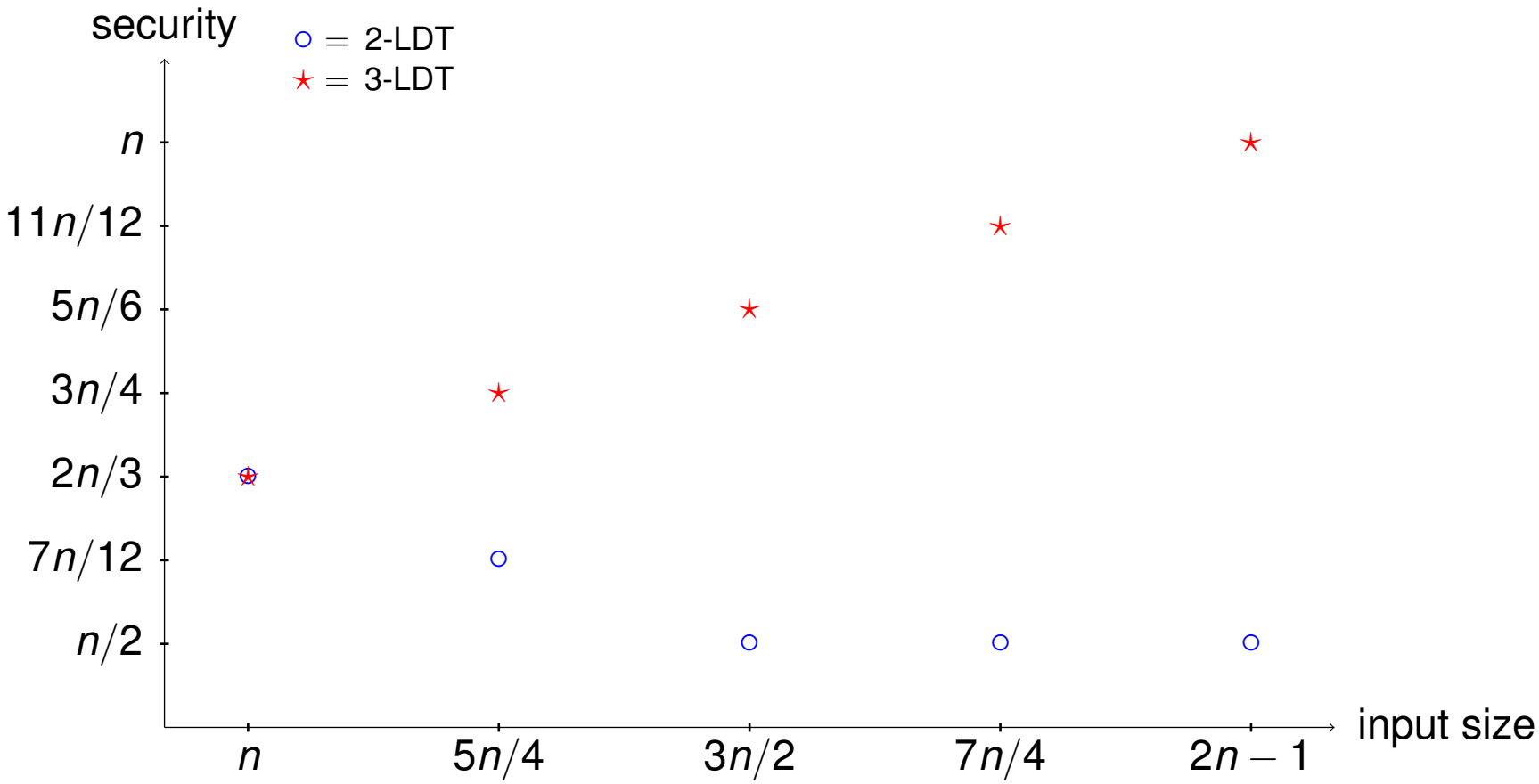
- "New bound"
- Better bound than 2-LDT

Security Analysis of 3-LDT



$$s_{min} \leq s_{max} \leq (n + s_{min})/2$$

Security Bound of 2-LDT and 3-LDT



Harmonic Permutation Primitives

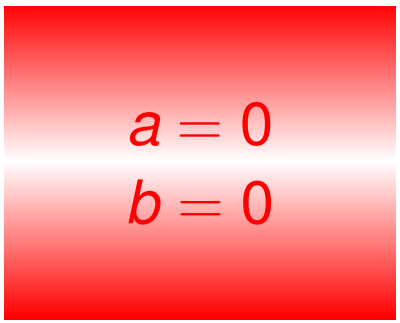
(Tweakable) pseudorandom permutation $G_{a,b}$ and $H_{a,b}$

- $a, b \in \{0, 1\}$
- $a =$ forward, $b =$ inverse
- $0 =$ random permutation, $1 =$ special

Harmonic Permutation Primitives

(Tweakable) pseudorandom permutation $G_{a,b}$ and $H_{a,b}$

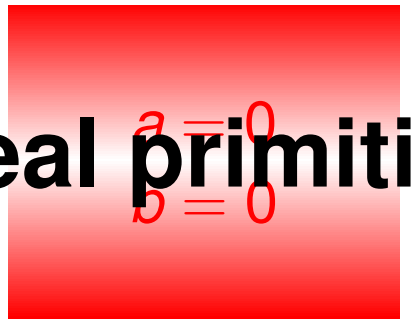
- $a, b \in \{0, 1\}$
- $a =$ forward, $b =$ inverse
- $0 =$ random permutation, $1 =$ special



Harmonic Permutation Primitives

(Tweakable) pseudorandom permutation $G_{a,b}$ and $H_{a,b}$

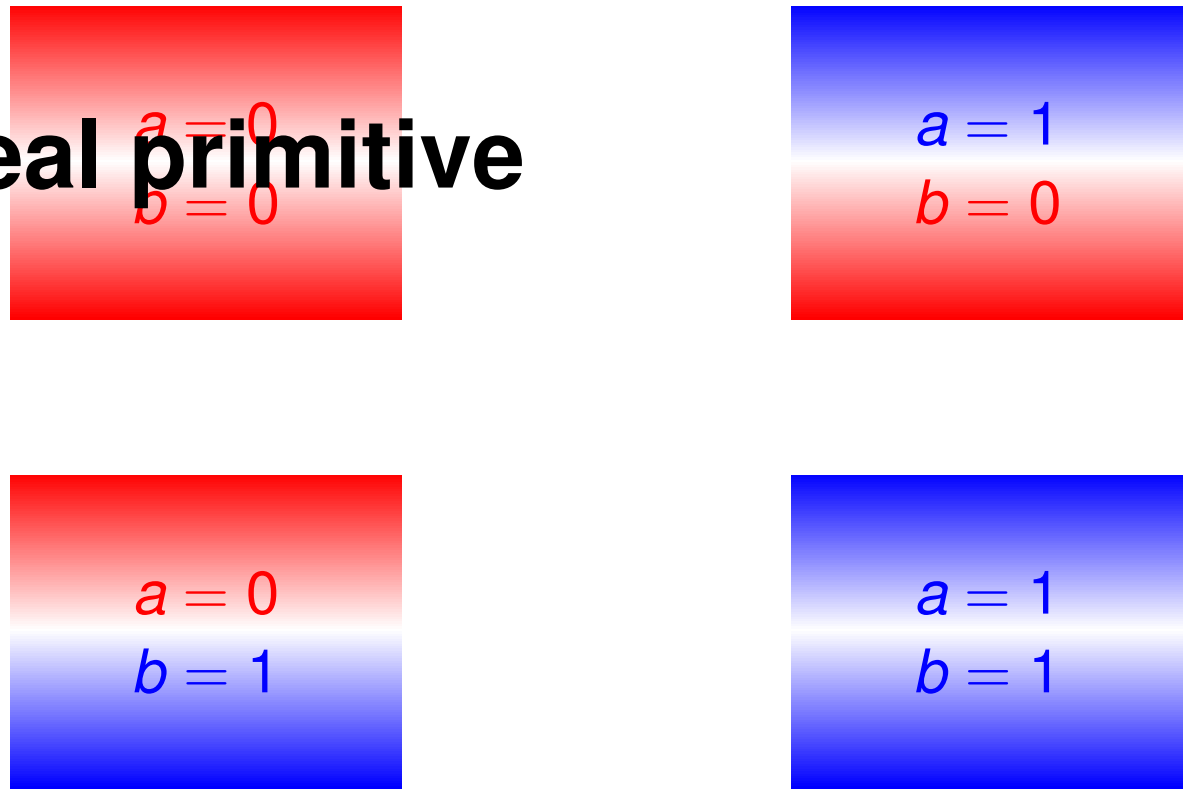
- $a, b \in \{0, 1\}$
- $a =$ forward, $b =$ inverse
- $0 =$ random permutation, $1 =$ special



Harmonic Permutation Primitives

(Tweakable) pseudorandom permutation $G_{a,b}$ and $H_{a,b}$

- $a, b \in \{0, 1\}$
- $a =$ forward, $b =$ inverse
- $0 =$ random permutation, $1 =$ special

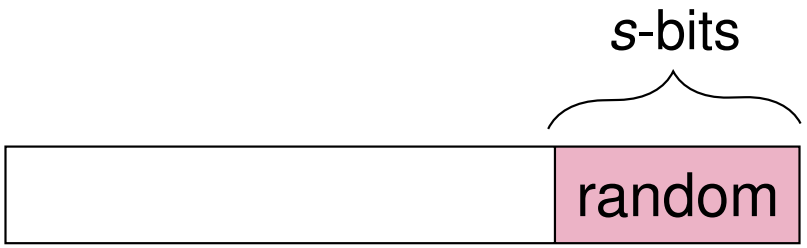


Harmonic Permutation Primitives

If $a = 1$ or $b = 1$, then

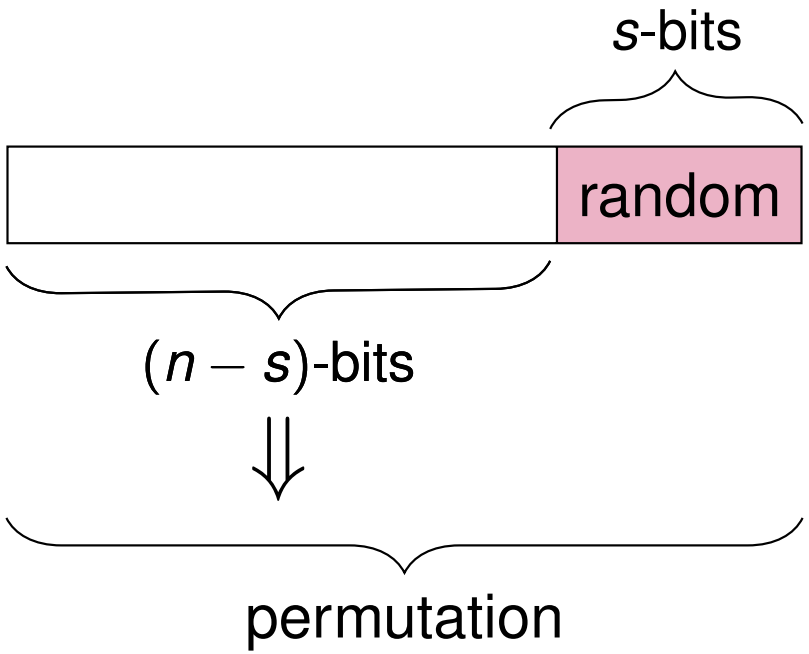
Harmonic Permutation Primitives

If $a = 1$ or $b = 1$, then



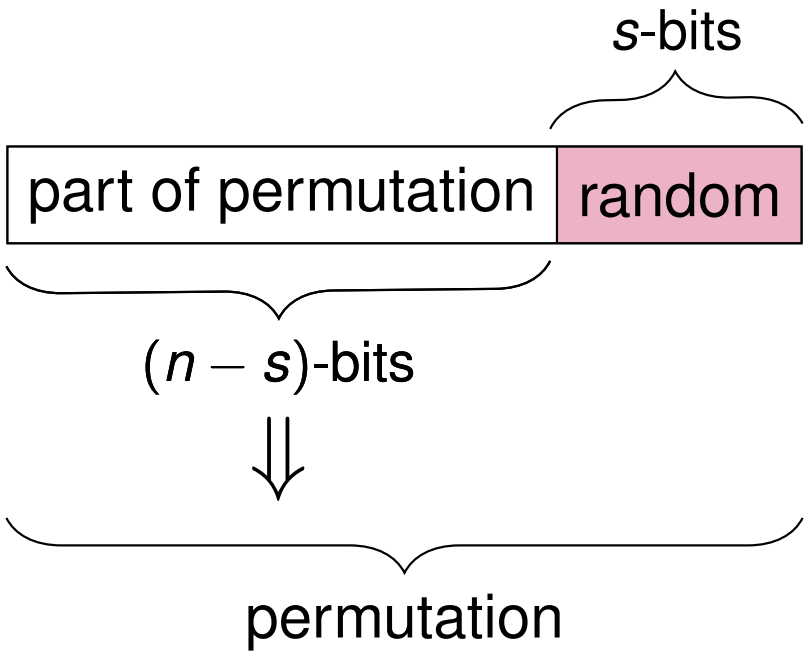
Harmonic Permutation Primitives

If $a = 1$ or $b = 1$, then

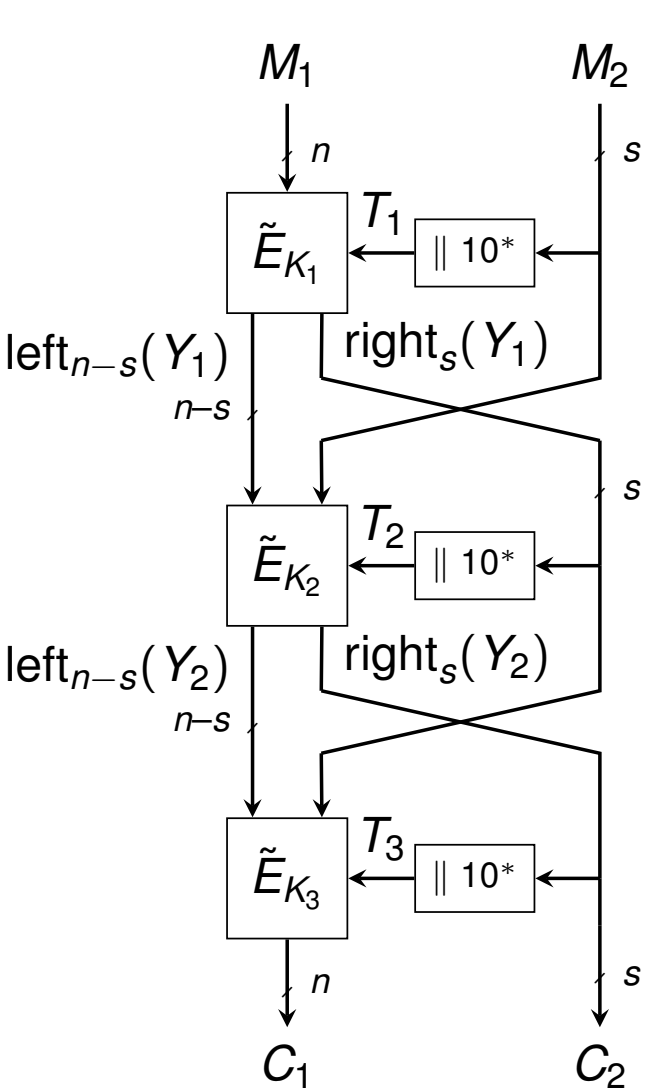


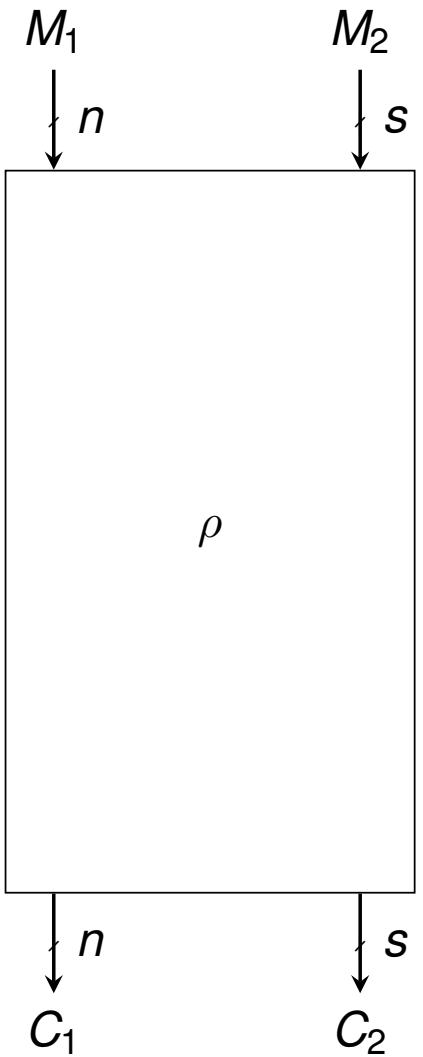
Harmonic Permutation Primitives

If $a = 1$ or $b = 1$, then

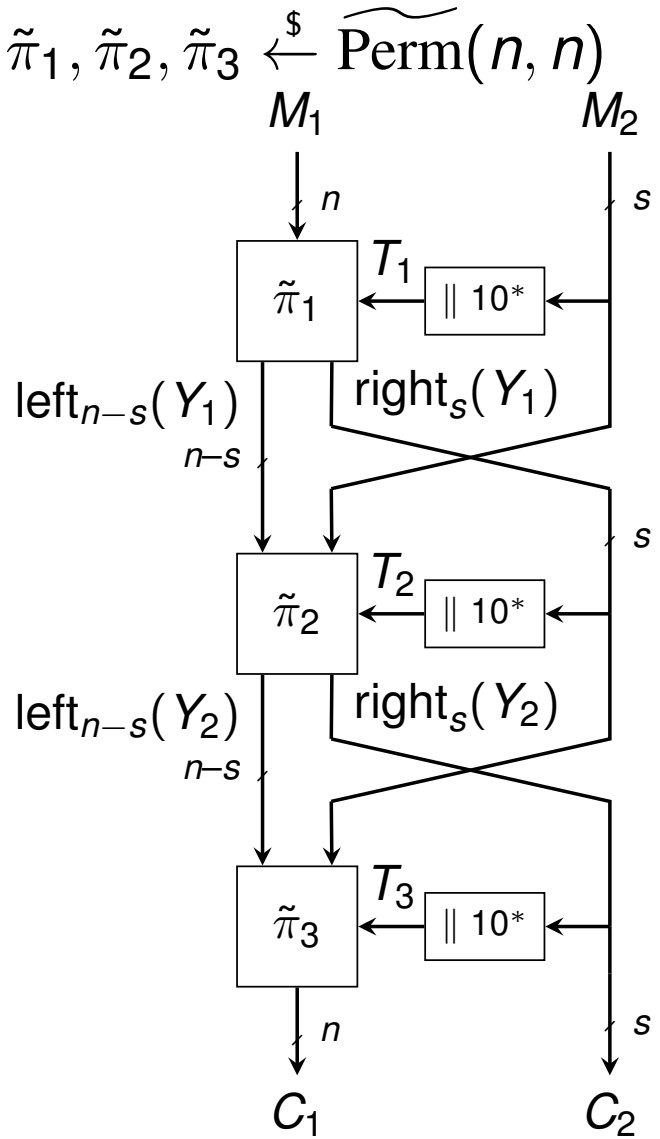


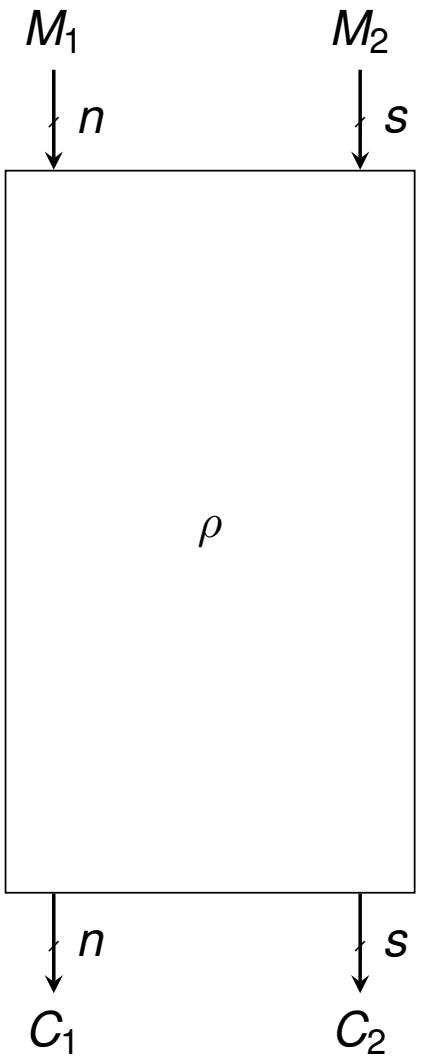
Proof Idea


M_1
M_2
n
s
$\tilde{E}_{K_1}$
T_1
$\| 10^*$
$\text{left}_{n-s}(Y_1)$
$n-s$
$\text{right}_s(Y_1)$
s
$\tilde{E}_{K_2}$
T_2
$\| 10^*$
$\text{left}_{n-s}(Y_2)$
$n-s$
$\text{right}_s(Y_2)$
$\tilde{E}_{K_3}$
T_3
$\| 10^*$
n
s
C_1
C_2

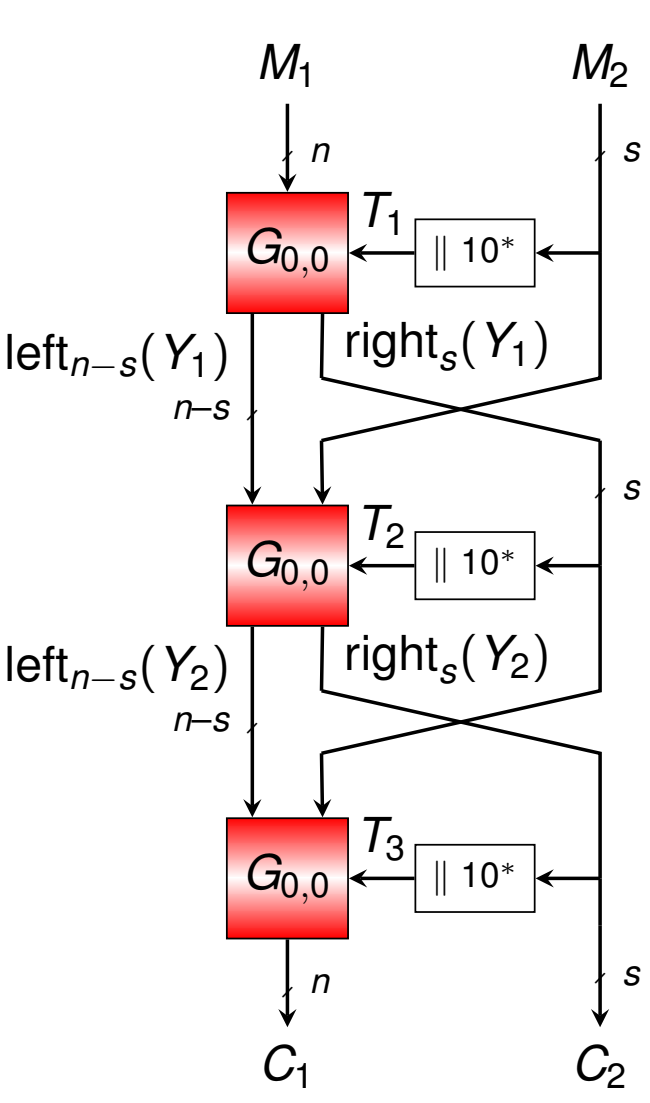

M_1
M_2
n
s
ρ
n
s
C_1
C_2

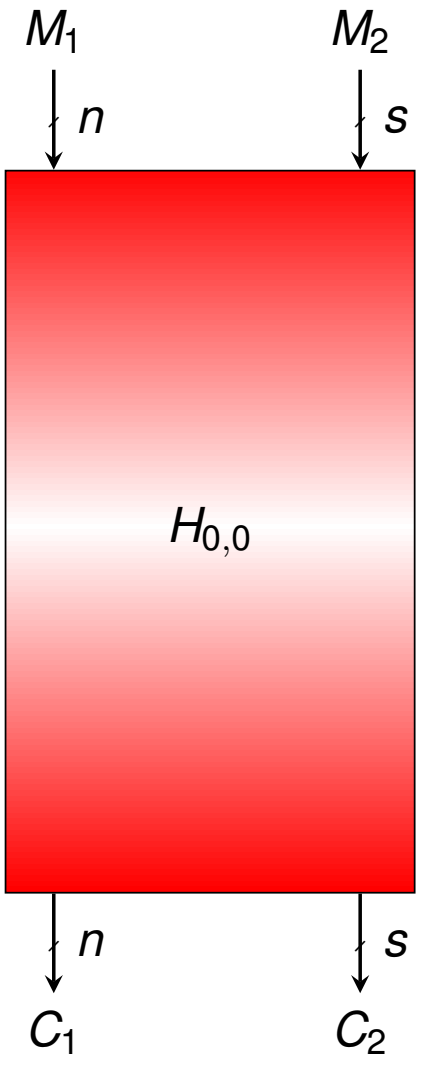
Proof Idea


$\tilde{\pi}_1, \tilde{\pi}_2, \tilde{\pi}_3 \xleftarrow{\$} \widetilde{\mathrm{Perm}}(n, n)$
M_1
M_2
n
s
$\tilde{\pi}_1$
T_1
$\| 10^*$
$\mathrm{left}_{n-s}(Y_1)$
$n-s$
$\mathrm{right}_s(Y_1)$
s
$\tilde{\pi}_2$
T_2
$\| 10^*$
$\mathrm{left}_{n-s}(Y_2)$
$n-s$
$\mathrm{right}_s(Y_2)$
$\tilde{\pi}_3$
T_3
$\| 10^*$
n
s
C_1
C_2

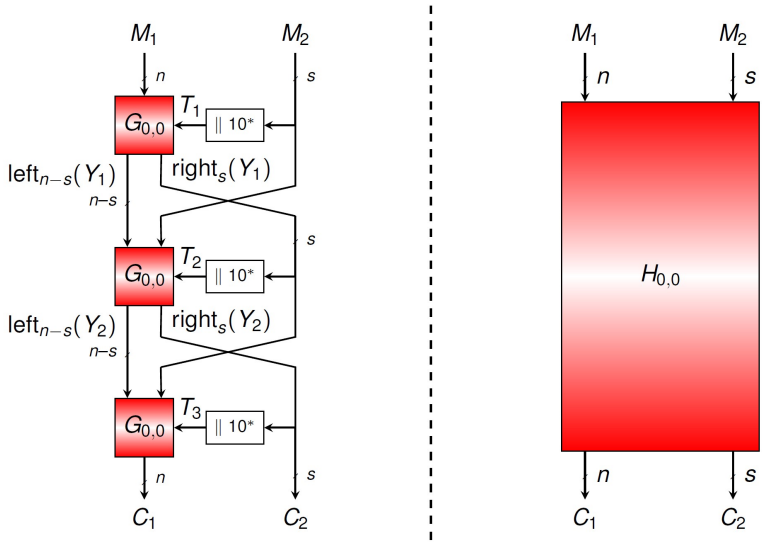

M_1
M_2
n
s
ρ
n
s
C_1
C_2

Proof Idea

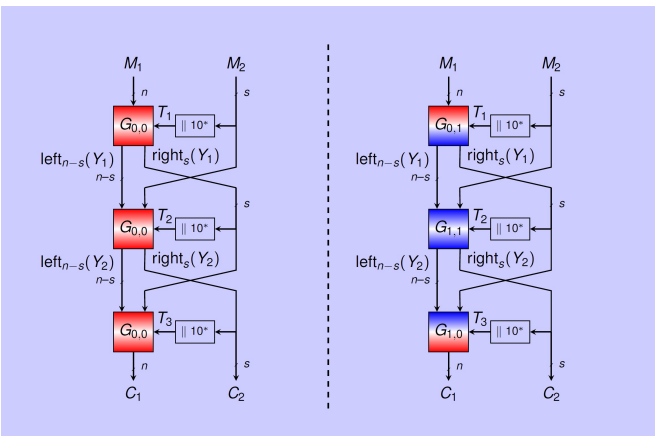

M_1
M_2
n
s
T_1
$G_{0,0}$
$\| 10^*$
$\text{left}_{n-s}(Y_1)$
$n-s$
$\text{right}_s(Y_1)$
s
T_2
$G_{0,0}$
$\| 10^*$
$\text{left}_{n-s}(Y_2)$
$n-s$
$\text{right}_s(Y_2)$
T_3
$G_{0,0}$
$\| 10^*$
n
s
C_1
C_2

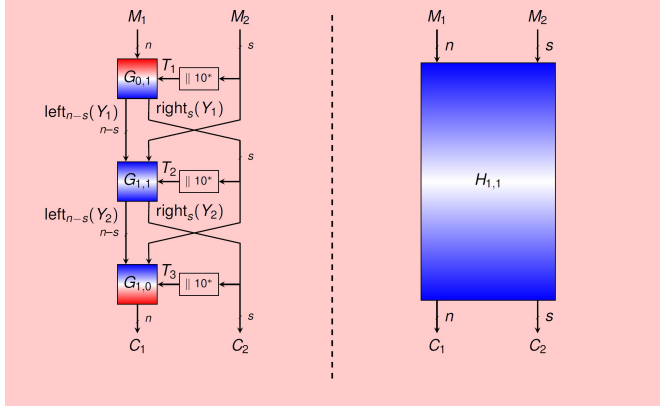

M_1
M_2
n
s
$H_{0,0}$
n
s
C_1
C_2

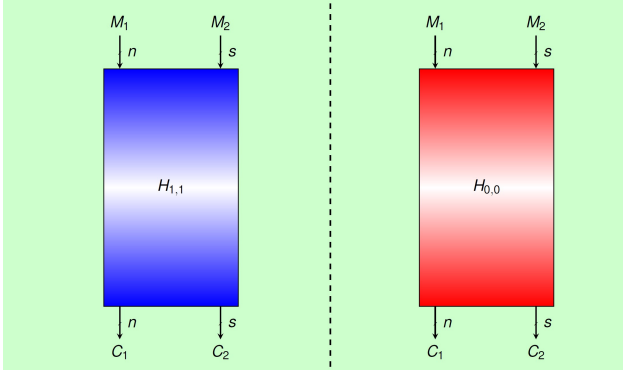
Proof Idea [Reduction]



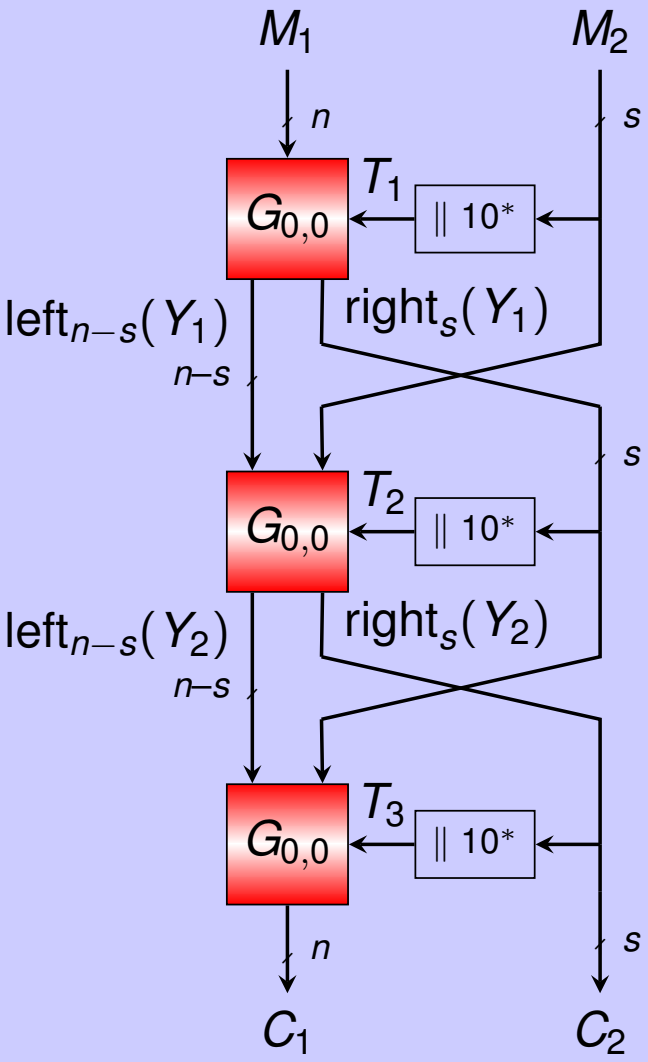
$\leq$

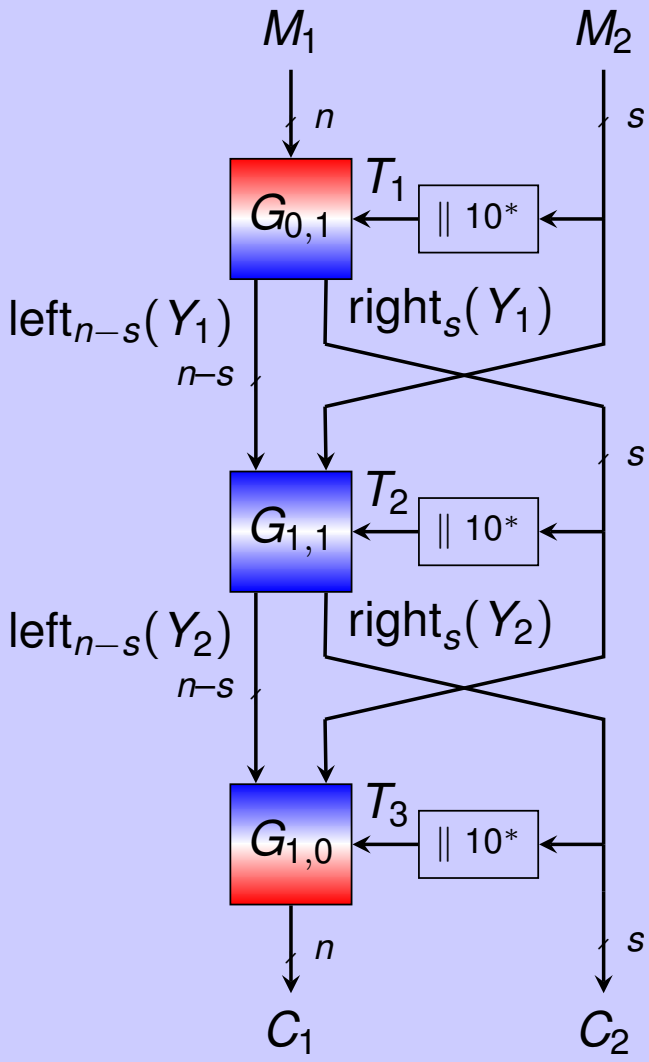




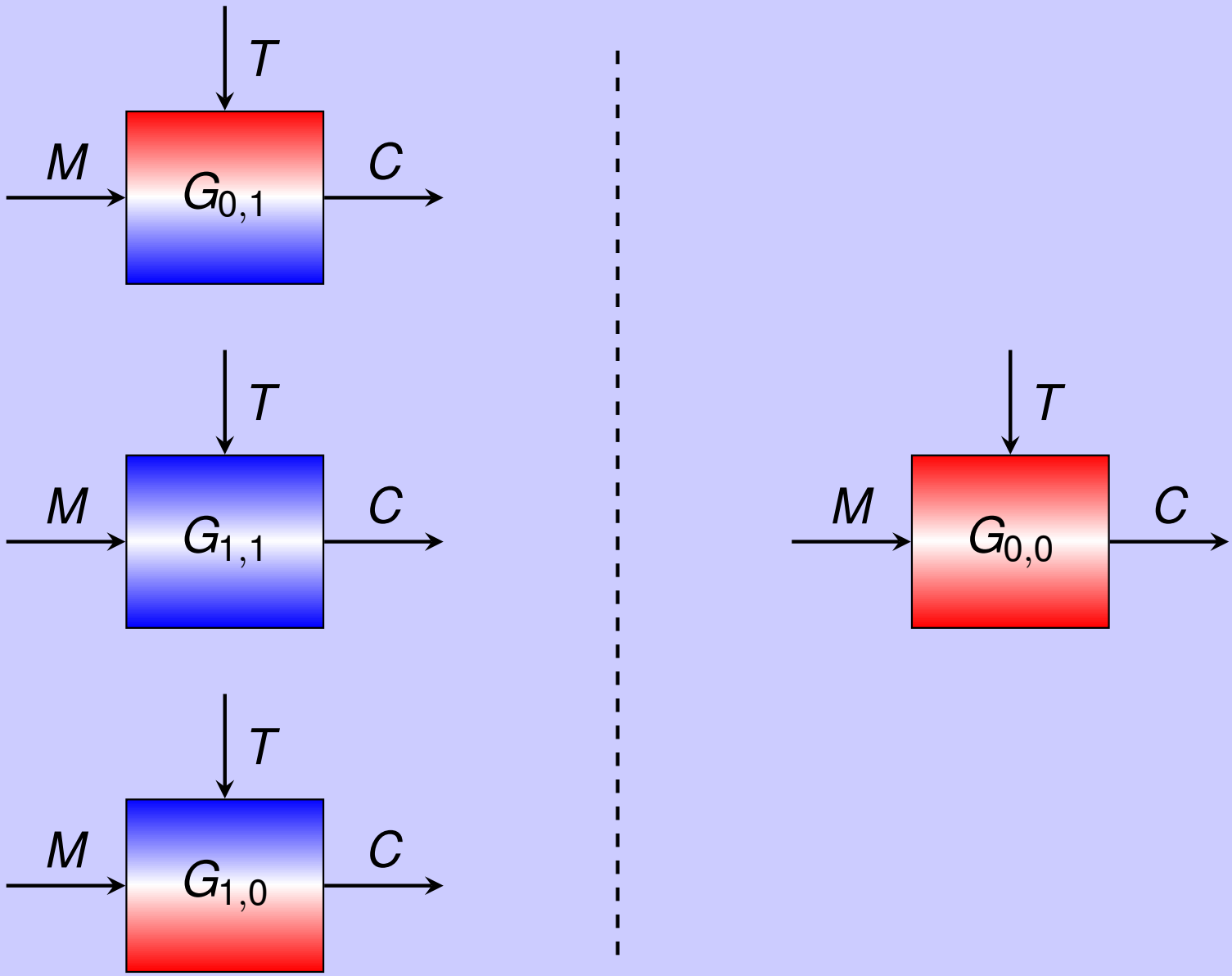


Proof Idea [Step 1]

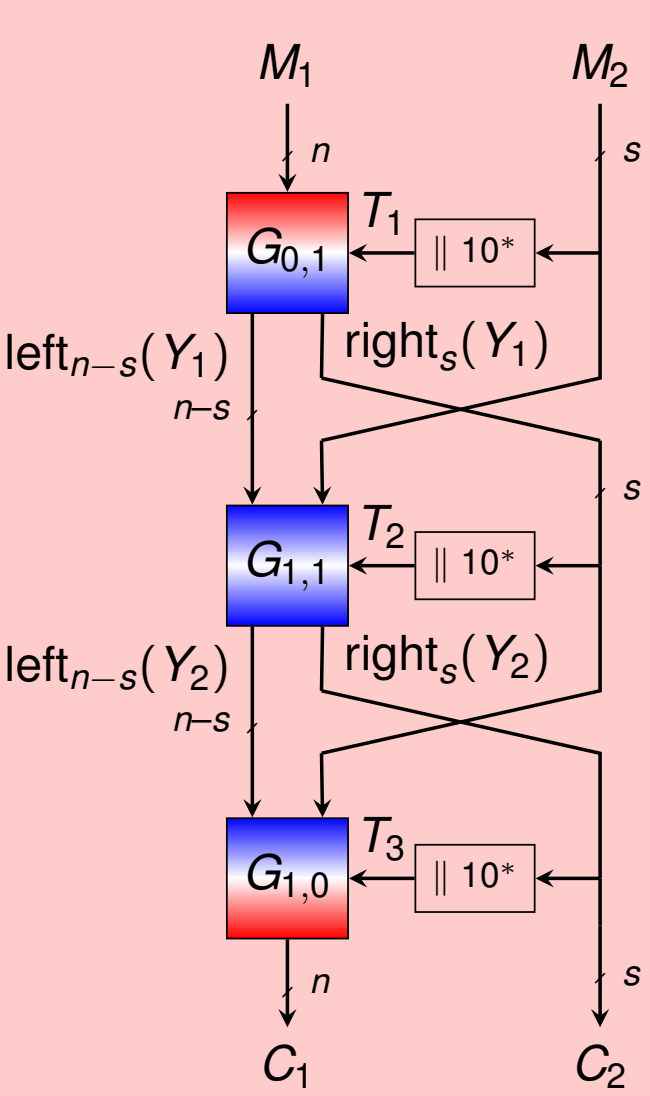


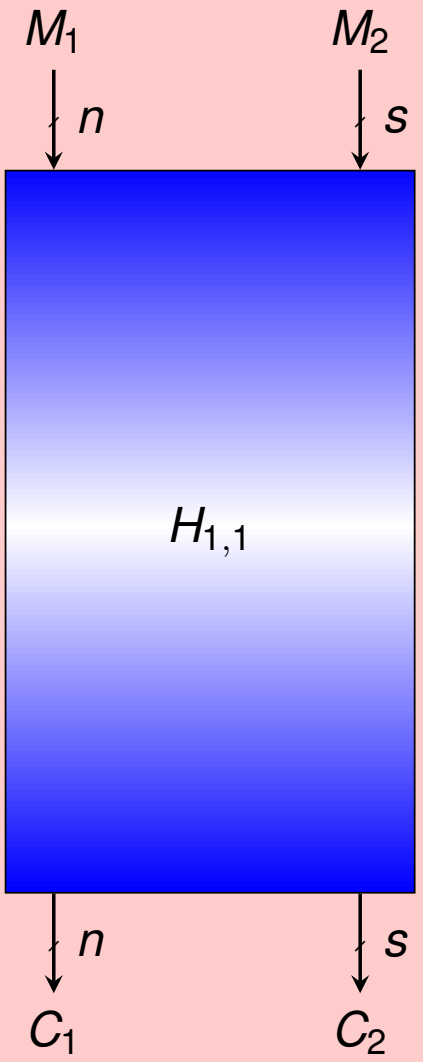


Proof Idea [Step 1]

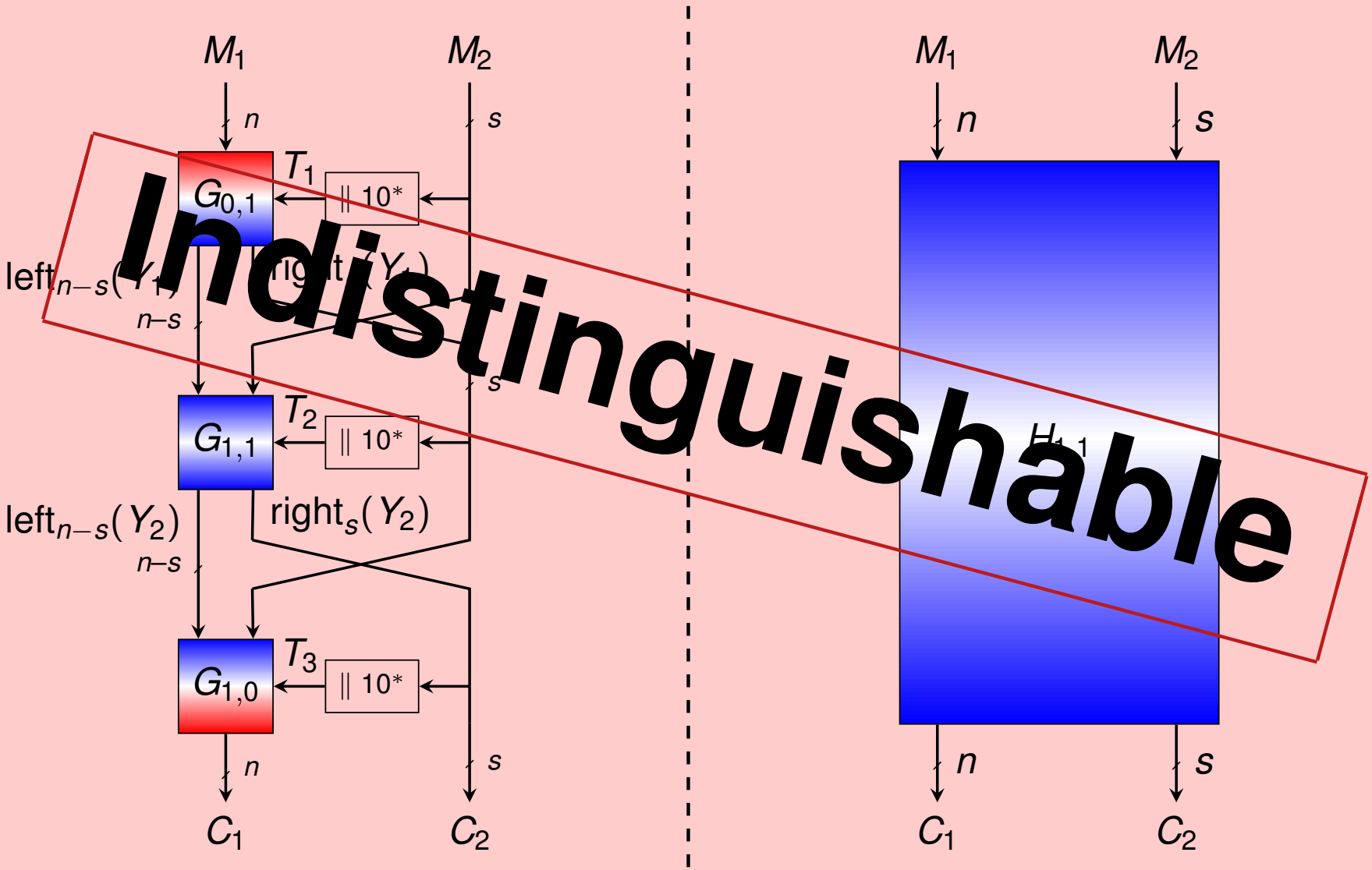


Proof Idea [Step 2]

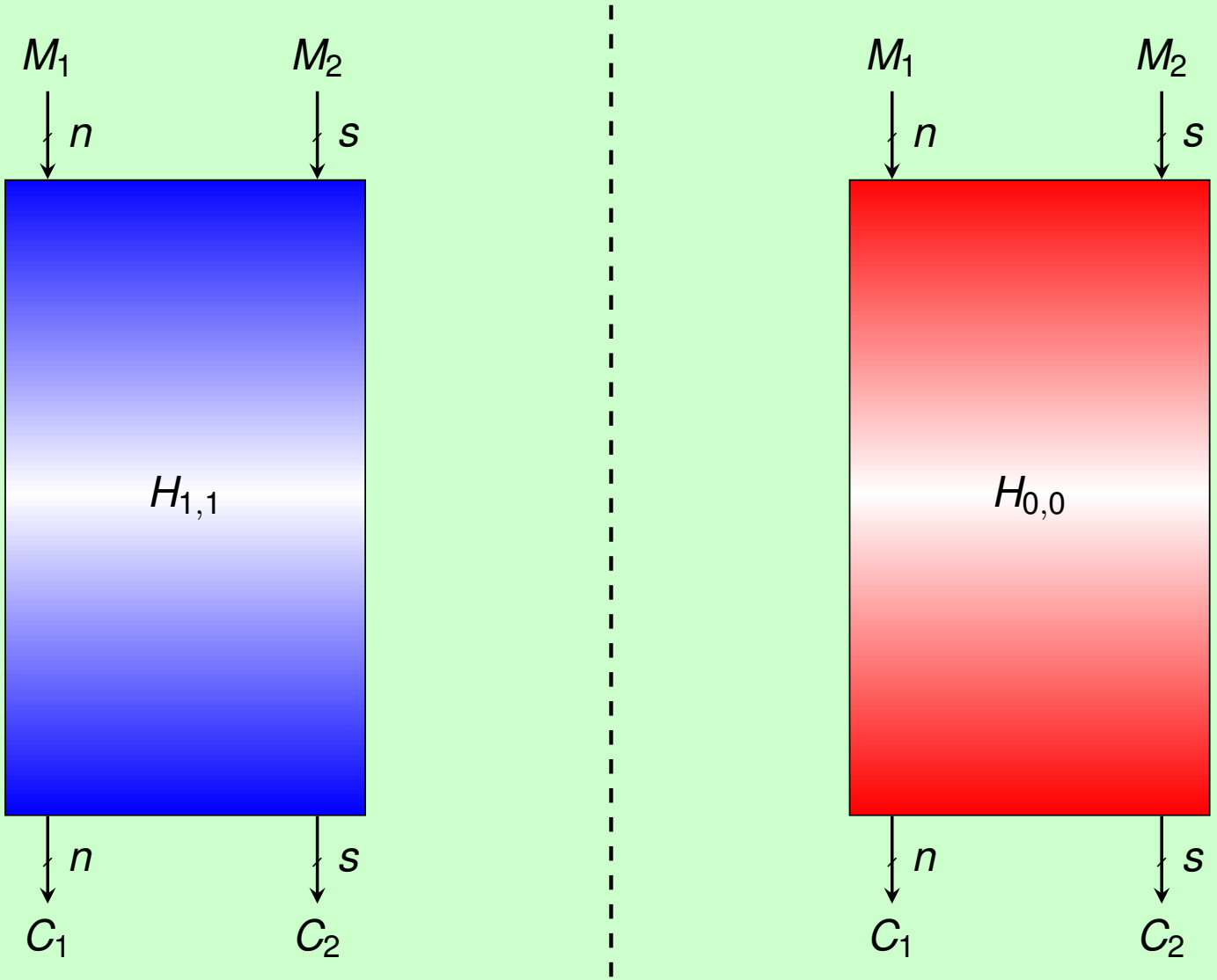




Proof Idea [Step 2]



Proof Idea [Step 3]



Conclusion

New results

- Harmonic primitives
- 2-LDT: beyond birthday bound
- 3-LDT: better bound

Conclusion

New results

- Harmonic primitives
- 2-LDT: beyond birthday bound
- 3-LDT: better bound

Further research

- 2-LDT and 3-LDT: tight bound?
- 3-LDT: optimal security?
- Harmonic primitives: tight bound and use for other constructions?

Conclusion

New results

- Harmonic primitives
- 2-LDT: beyond birthday bound
- 3-LDT: better bound

Further research

- 2-LDT and 3-LDT: tight bound?
- 3-LDT: optimal security?
- Harmonic primitives: tight bound and use for other constructions?

Thank you for your attention!