Efficient Length Doubling From Tweakable Block Ciphers

Yu Long Chen[1] Atul Luykx[2] Bart Mennink[3]
Bart Preneel[1]

imec-COSIC, KU Leuven

Visa Research

Digital Security Group, Radboud University, Nijmegen

March 6, 2018

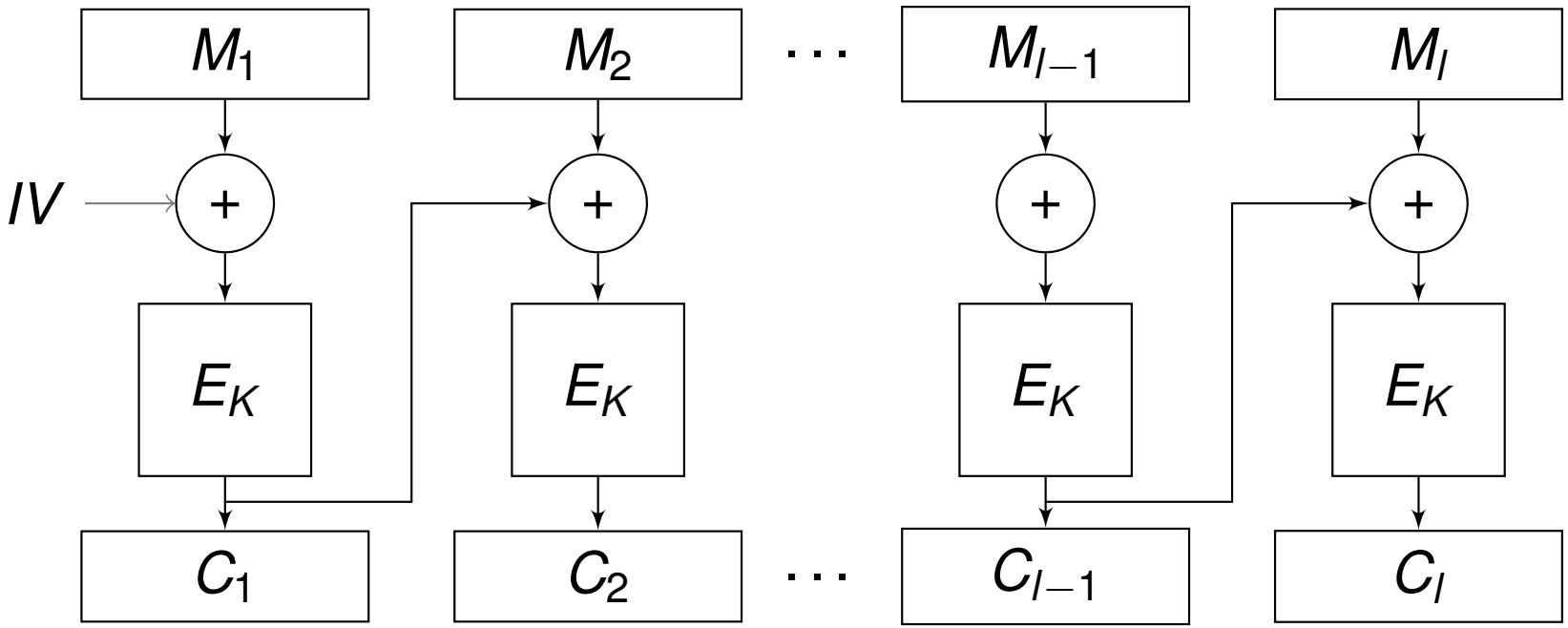
Modes of operation

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

Modes of operation

- block cipher: fixed-input-length (FIL)
- apply block cipher iteratively

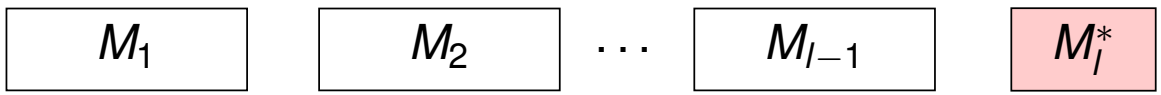
CBC mode



Modes of operation

fractional data $\Longrightarrow$ padding

CBC+padding



Modes of operation

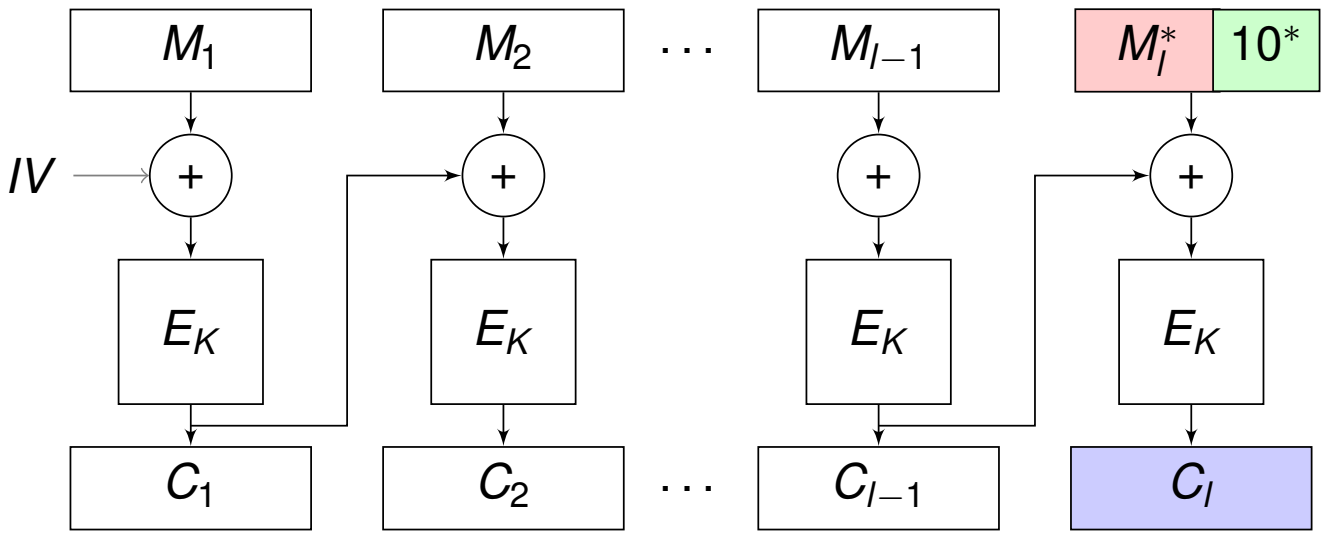
fractional data $\Longrightarrow$ padding

CBC+padding

Modes of operation

fractional data $\Longrightarrow$ padding

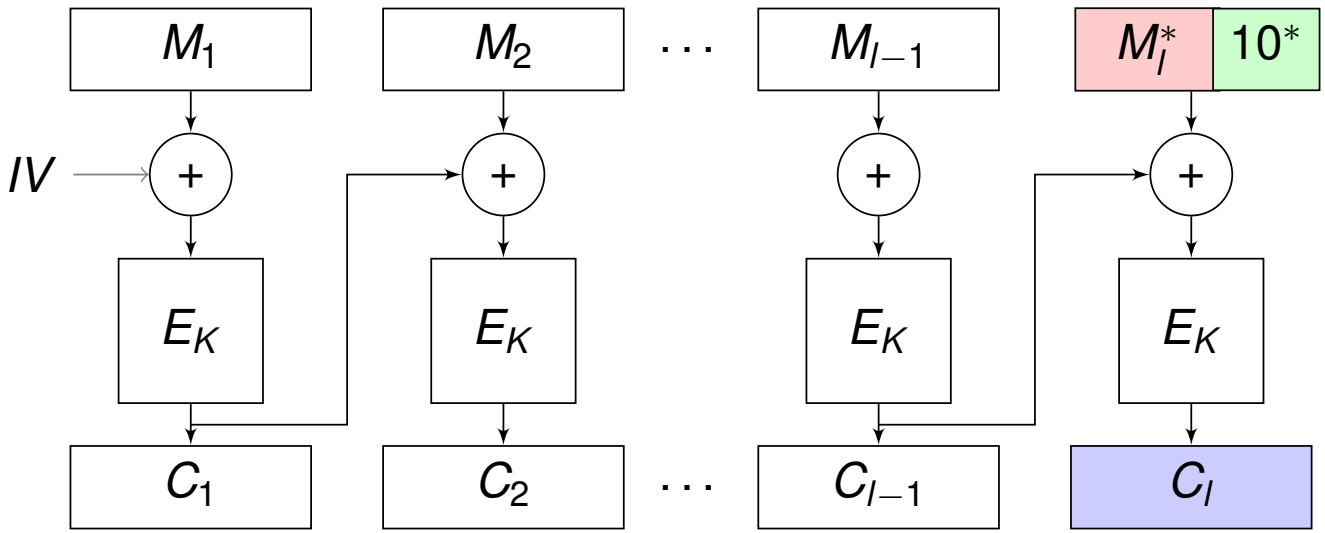
CBC+padding



Modes of operation

fractional data $\Longrightarrow$ padding

CBC+padding



ciphertext expansion: $|C| > |M|$

Avoiding ciphertext expansion

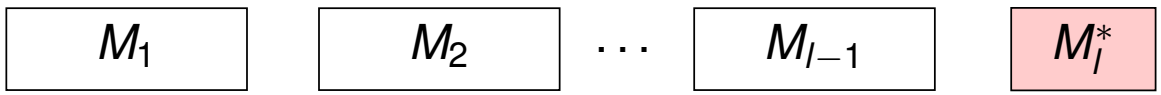
1. CTR: turns block cipher into stream cipher
   $\Longrightarrow$ not suitable for some applications

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:

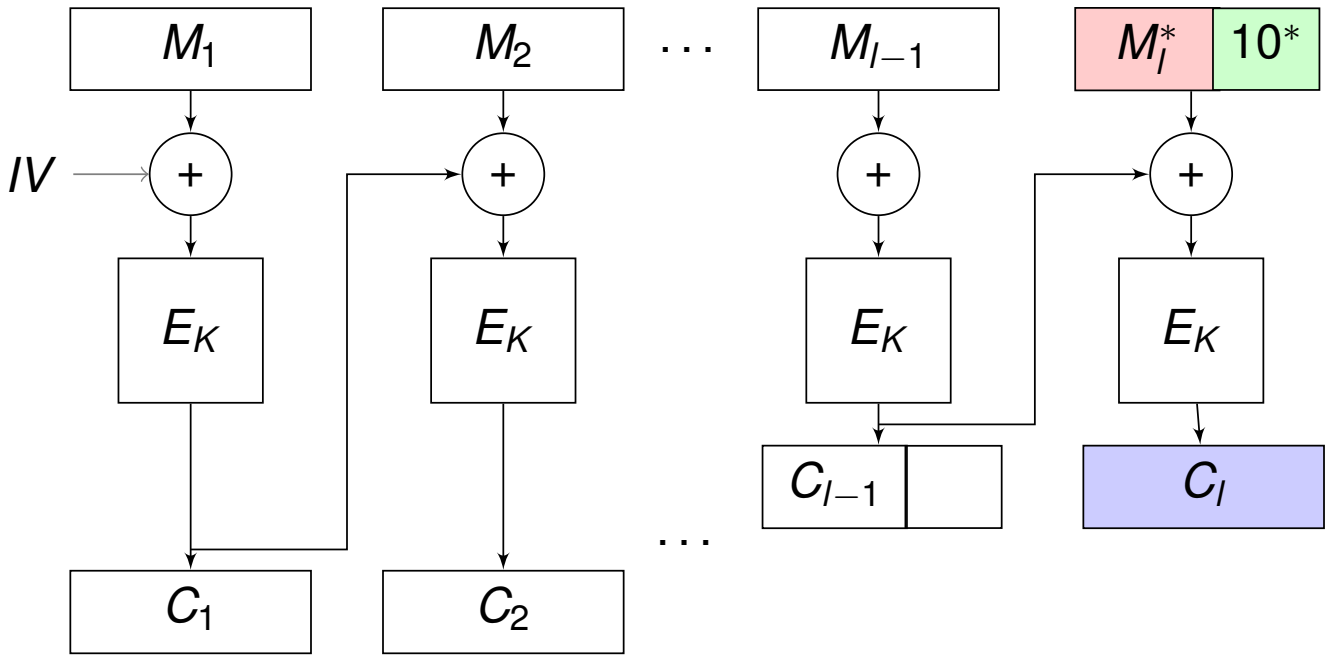


Avoiding ciphertext expansion

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:

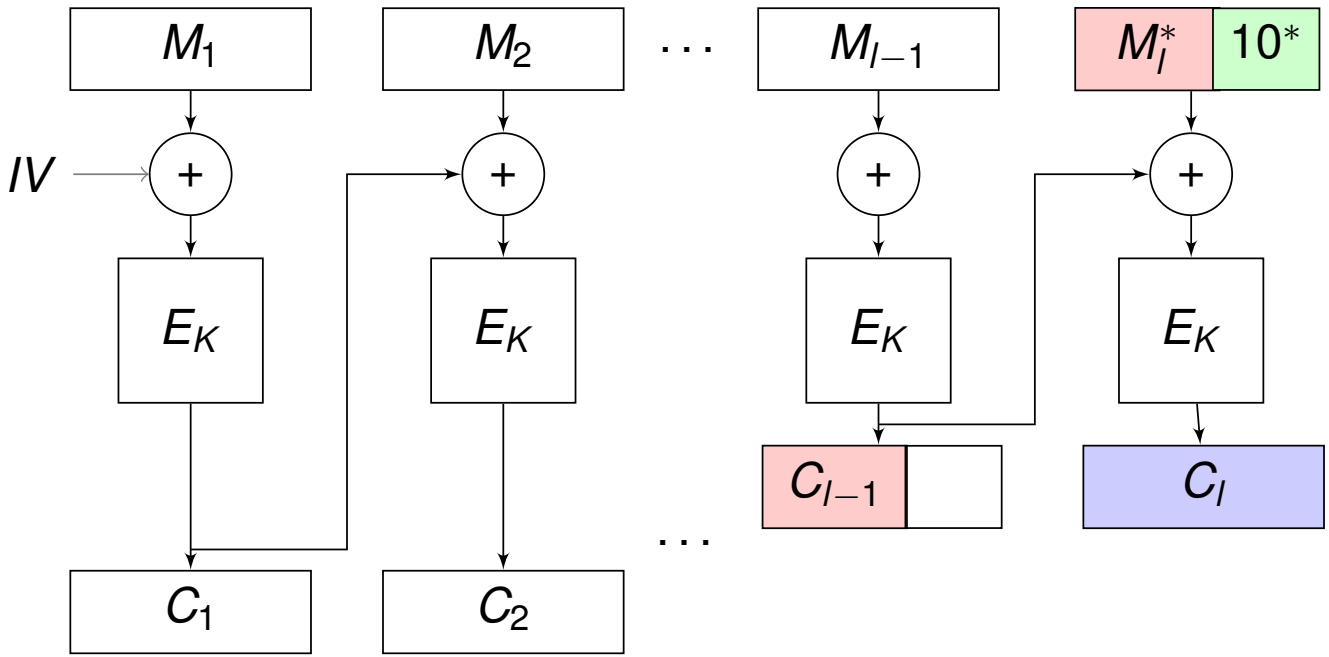
Avoiding ciphertext expansion

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:



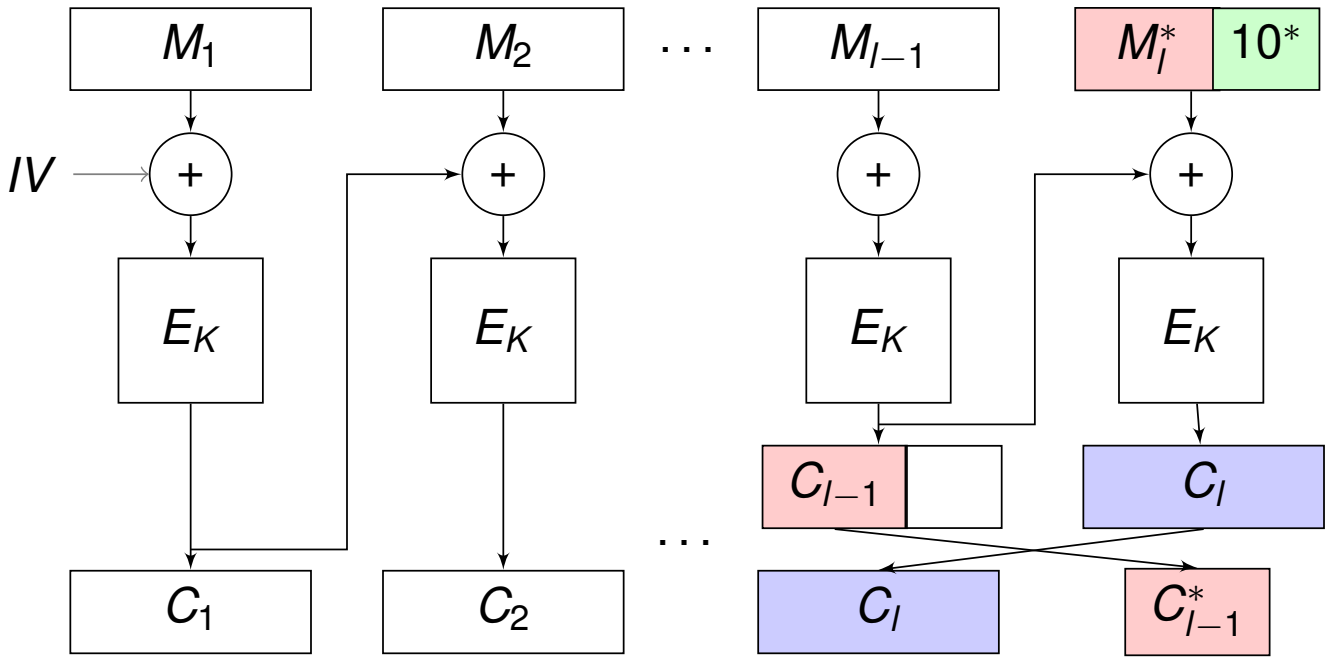
Avoiding ciphertext expansion

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:



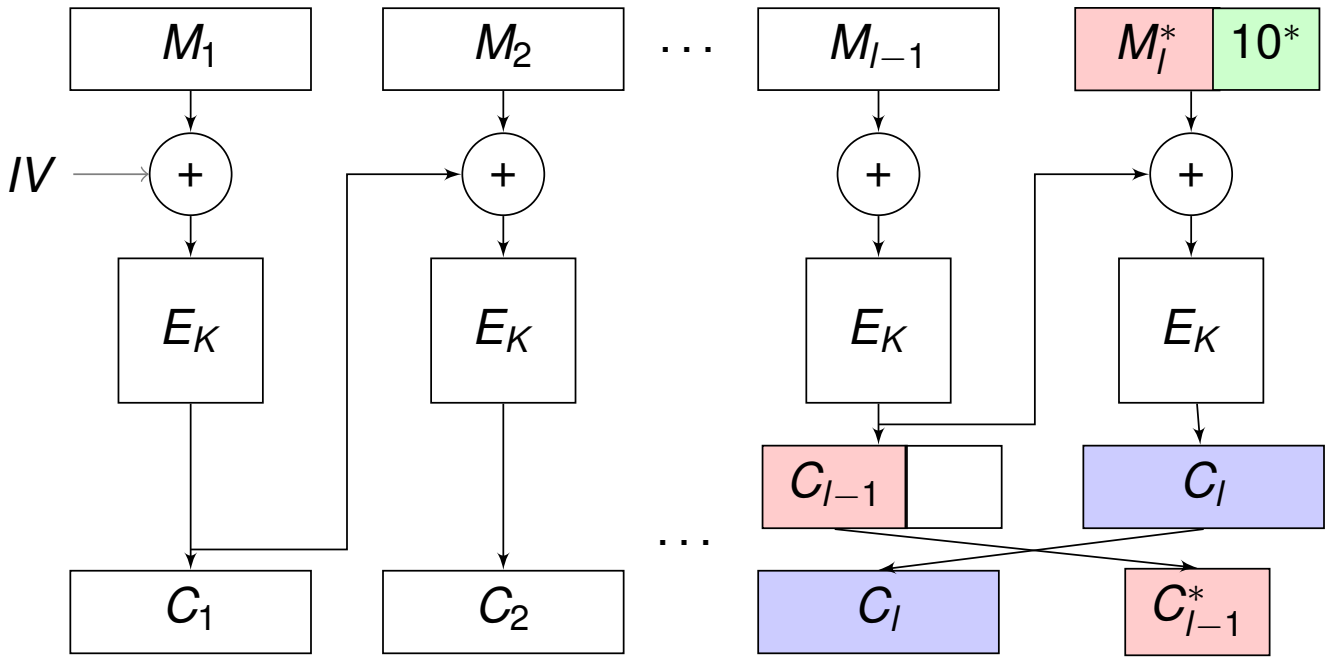
Avoiding ciphertext expansion

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:



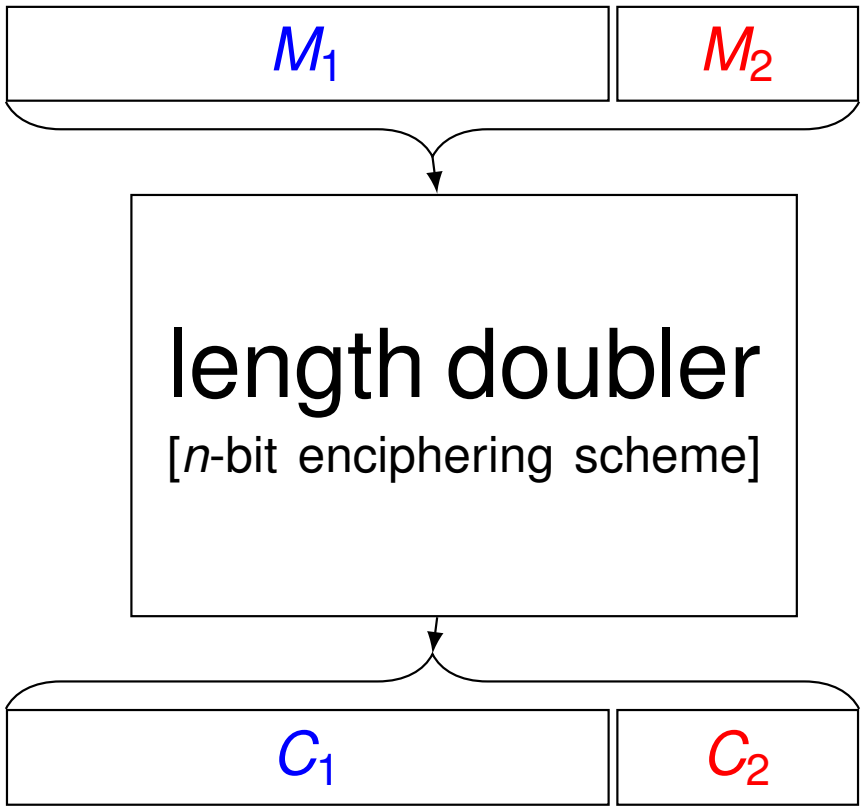
Avoiding ciphertext expansion

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:



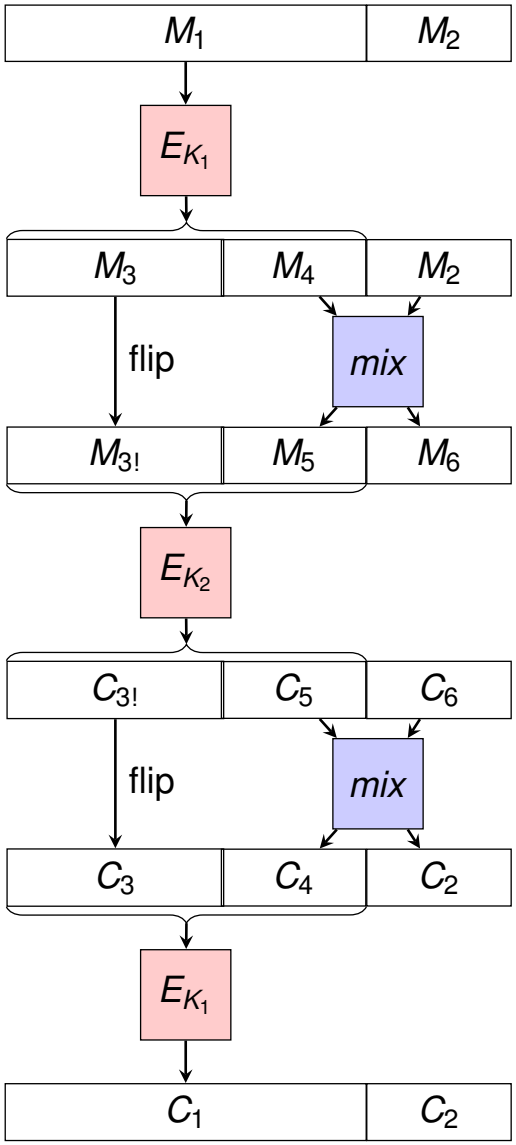
- condition: C_i's need to be decrypted independently

Length doublers



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

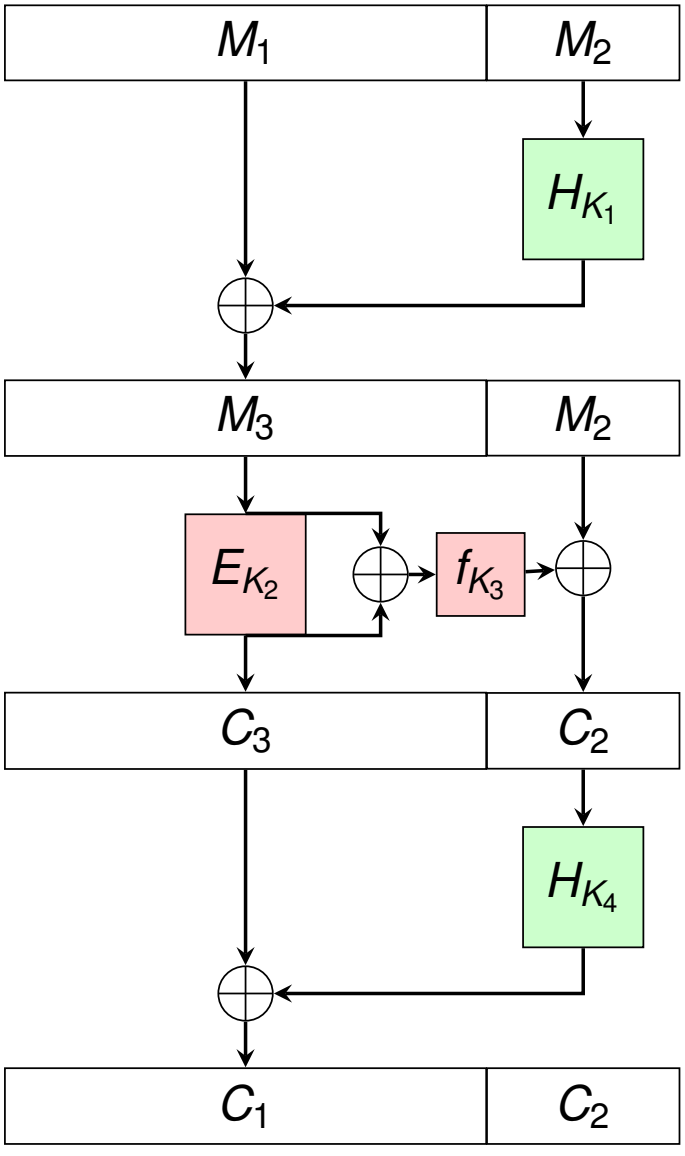
XLS



Ristenpart and Rogaway (2007)

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

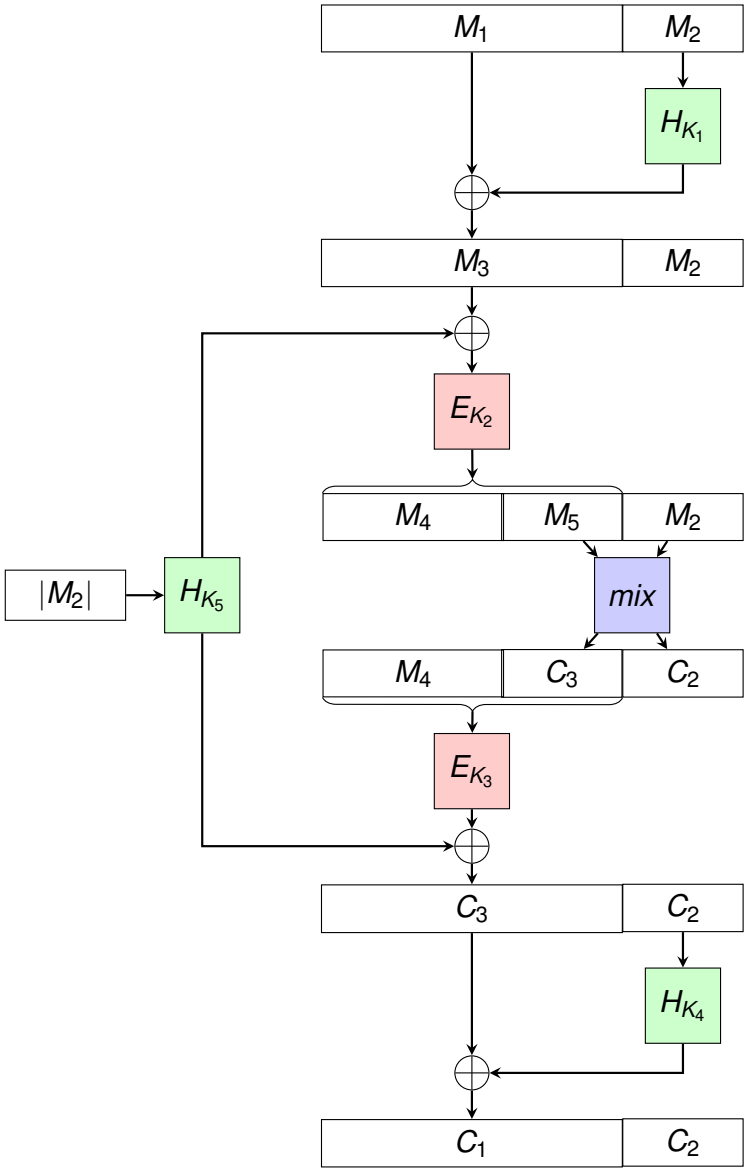
DE



Nandi (2009)

- four cryptographic primitive calls

HEM



Zhang (2012)

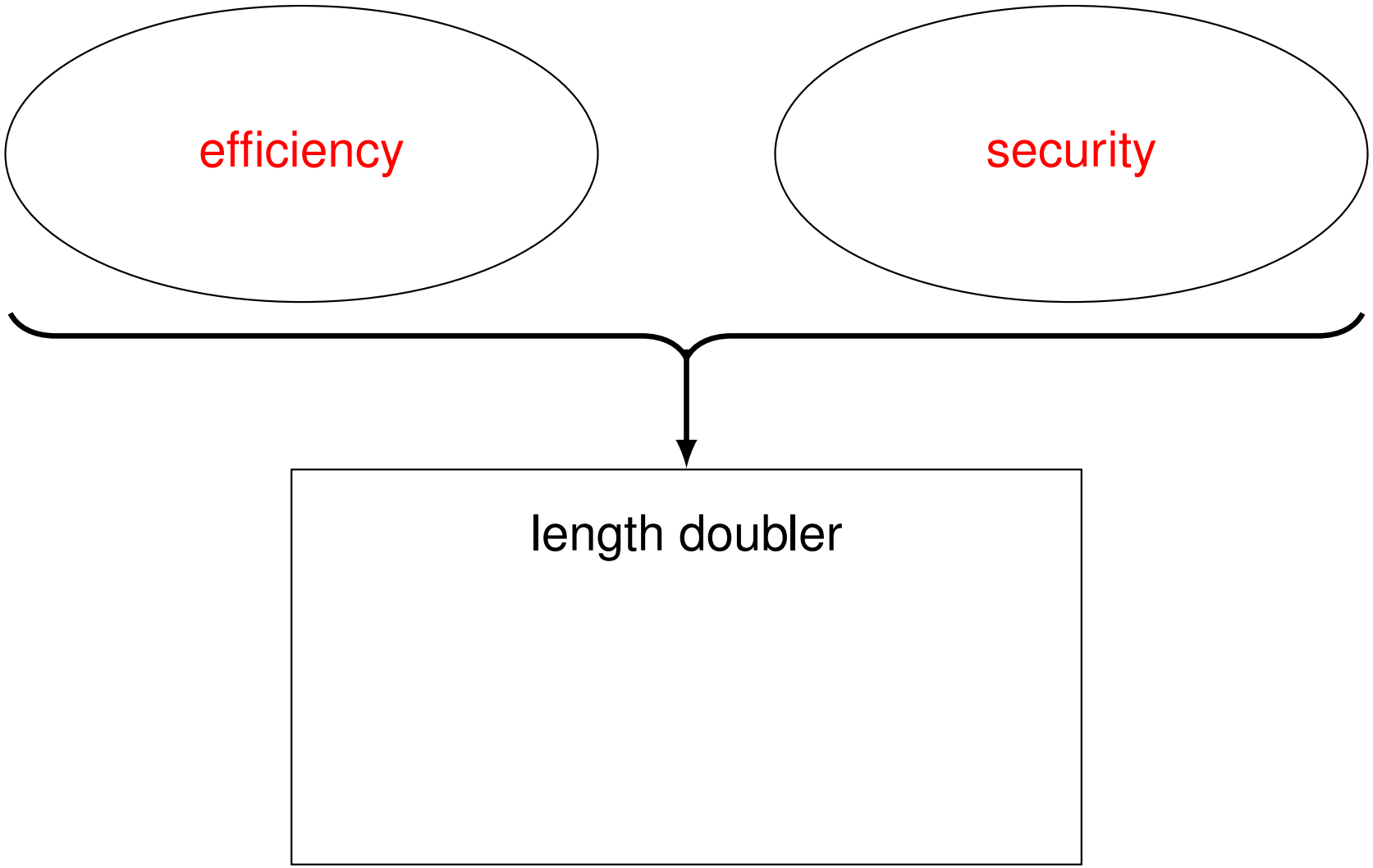
- five cryptographic primitive calls
- ϵ-good mixing function

State of the art

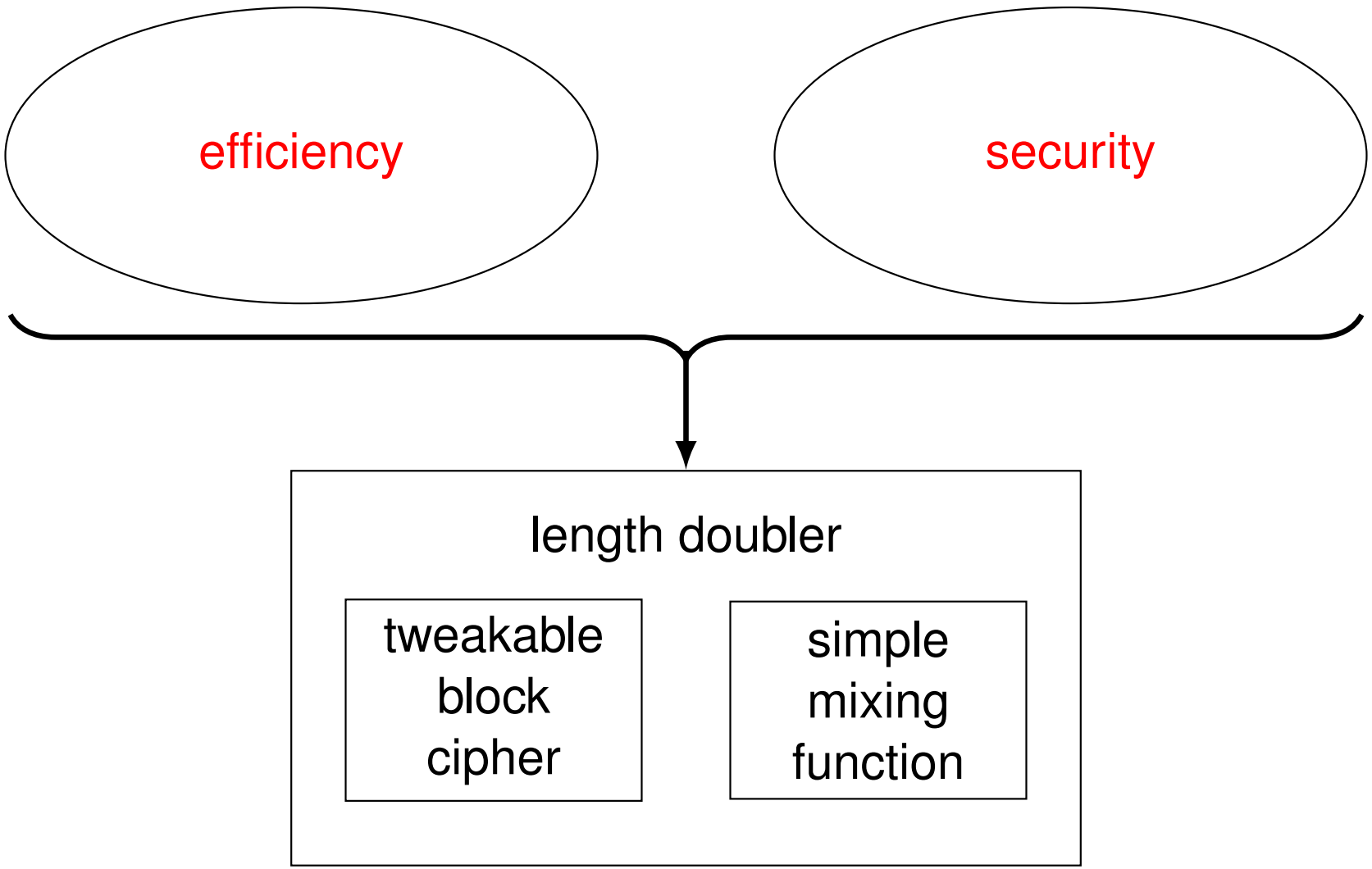
length doubler	security ($\log_2$)	key length	cryptographic primitive calls	mixing function
XLS	$n/2$	$2n$	3 BC	ϵ-good
DE	$n/2$	$5n$	4 hash+BC	-
HEM	$n/2$	$3n$	4 hash+BC	ϵ-good

- at least 4 cryptographic primitive calls needed?
- beyond $2^{n/2}$ security?

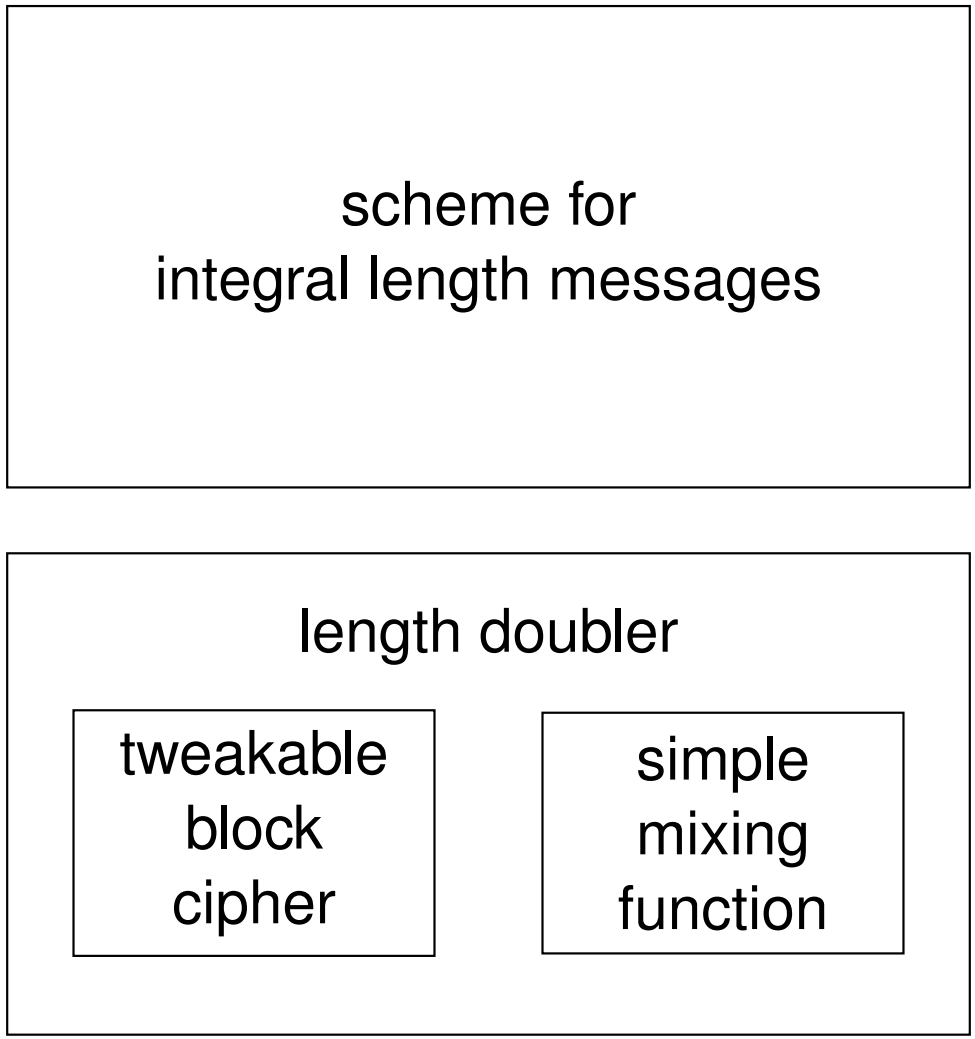
Our contribution



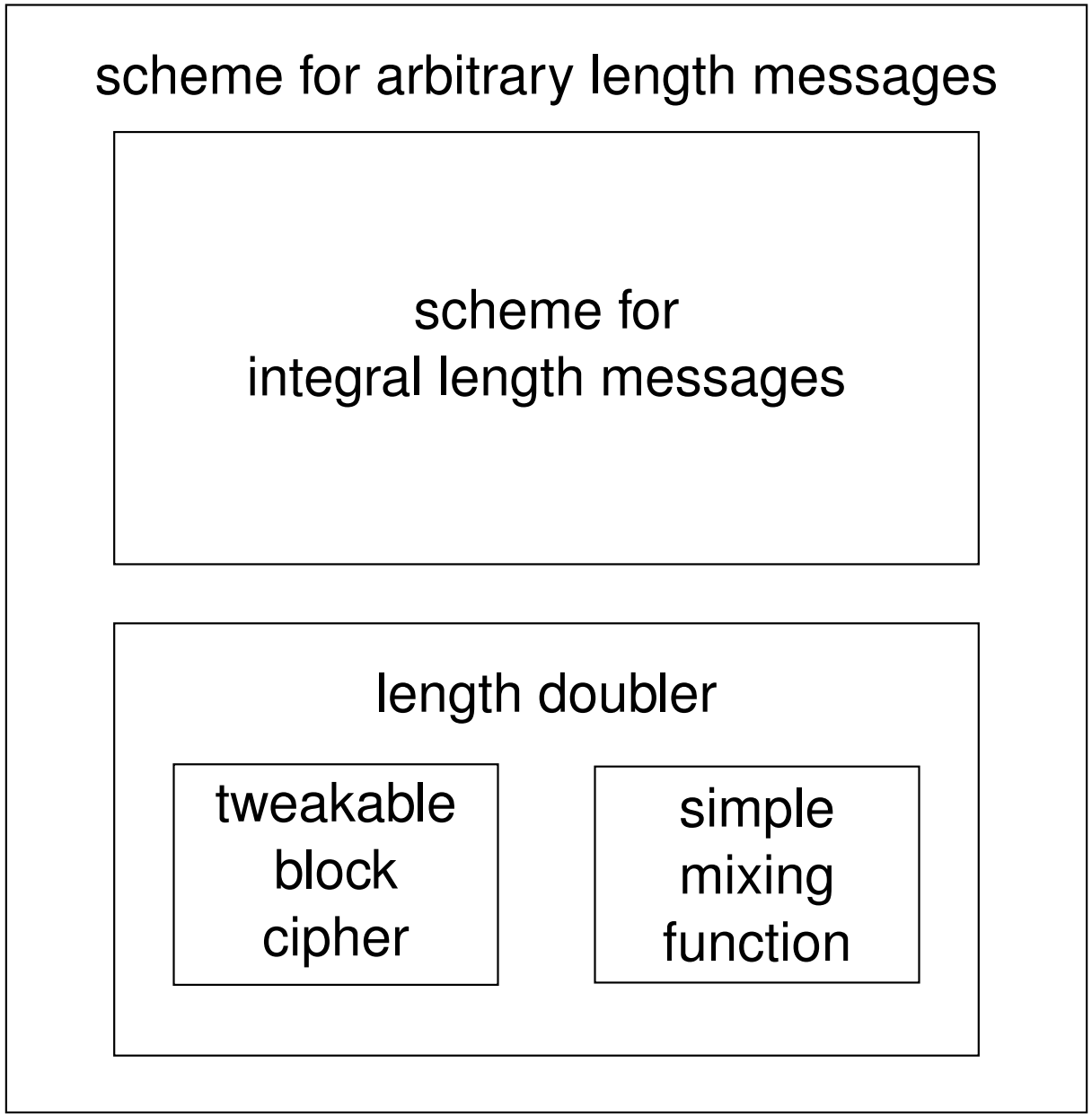
Our contribution



Our contribution

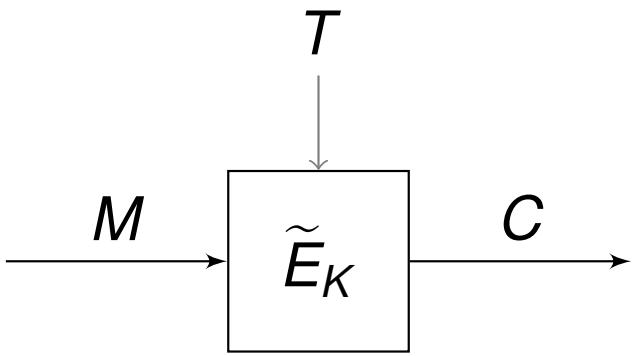


Our contribution



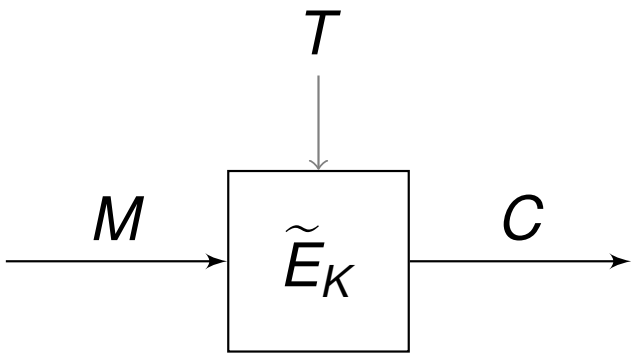
Tweakable block ciphers

- 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

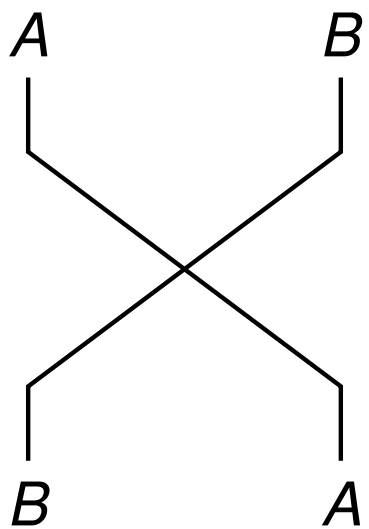
Pure mixing functions

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

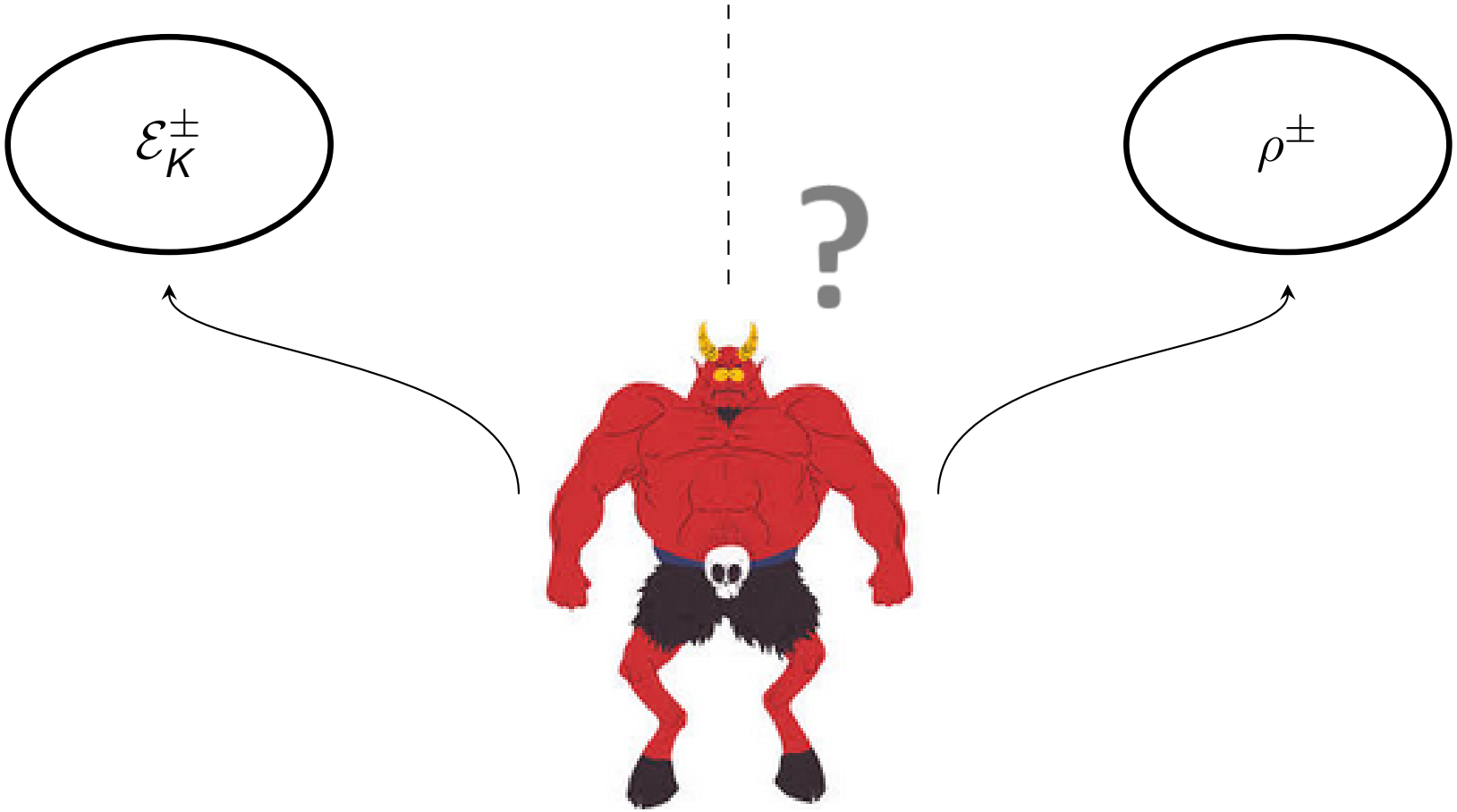
Pure mixing functions

- 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)



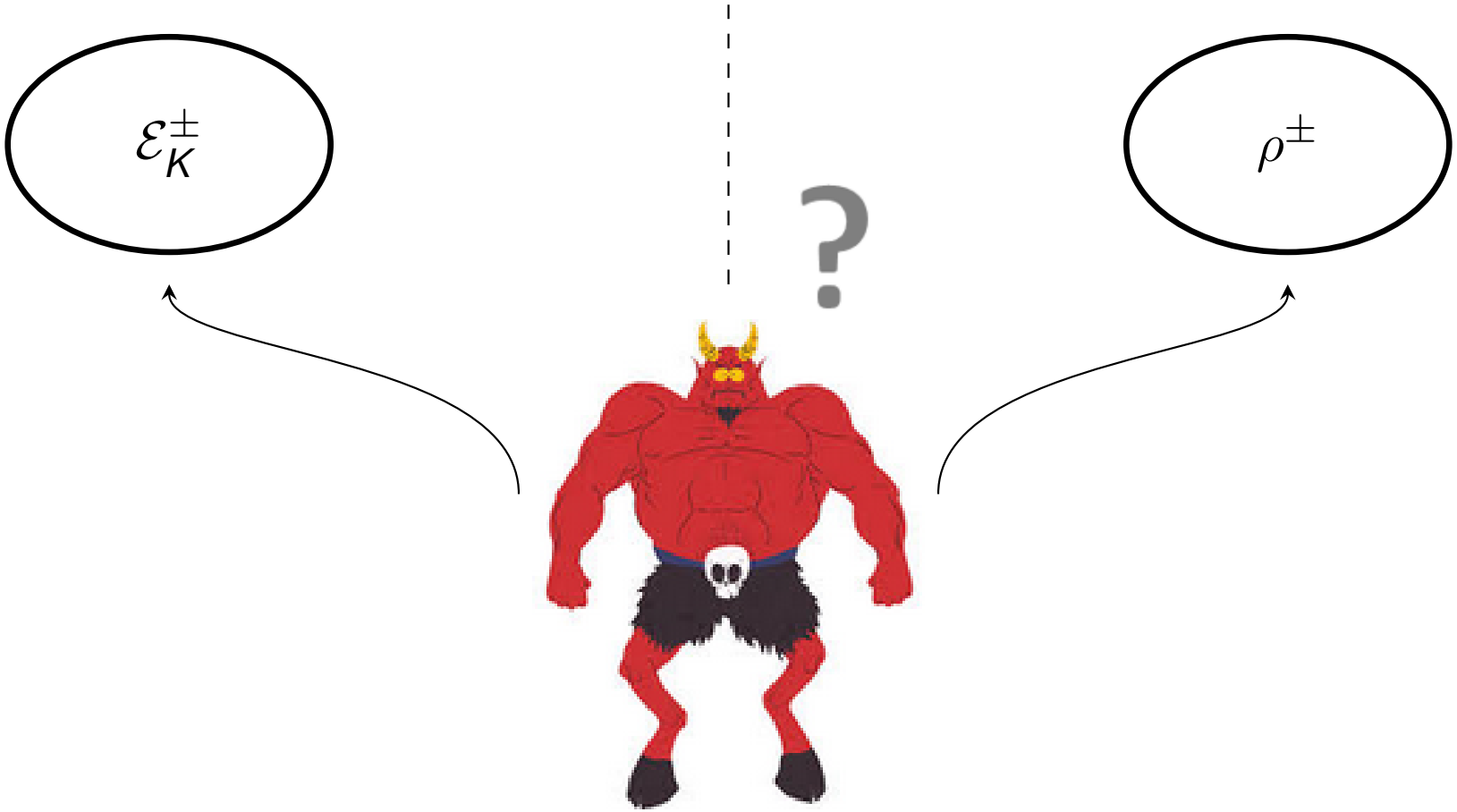
Security definition



adversary $\mathcal{A}$

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

Security definition



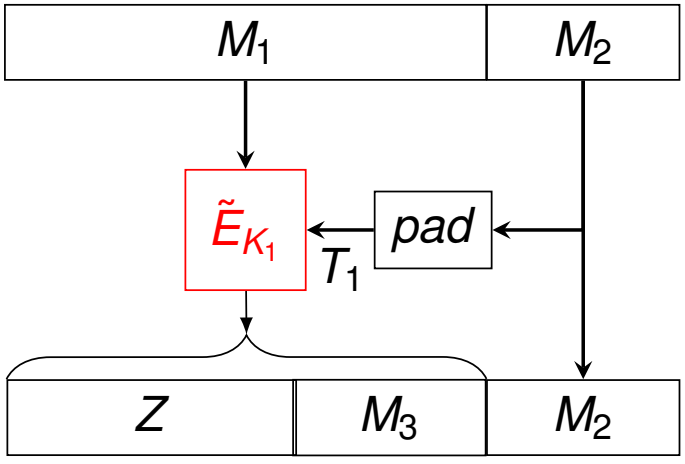
adversary $\mathcal{A}$

- 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

Our length doubler **LDT**

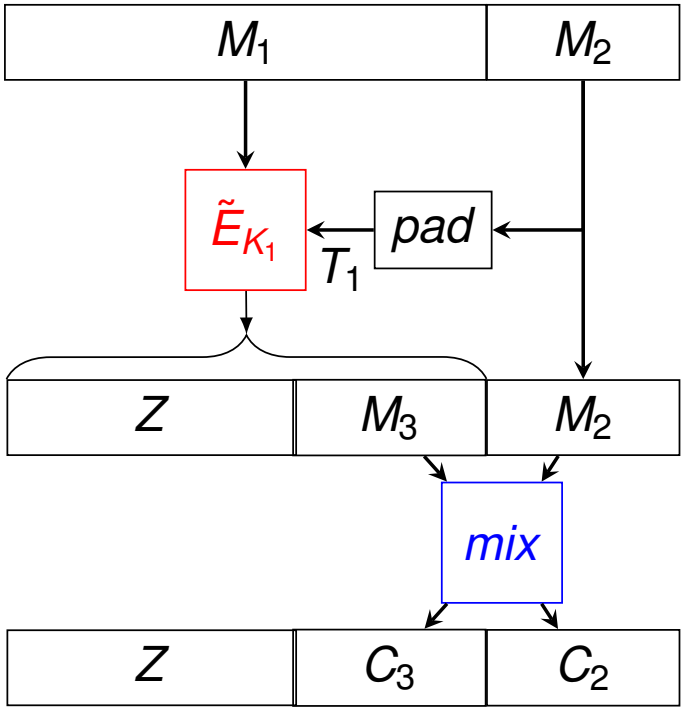
- 2 tweakable block cipher calls
- pure mixing function
- decryption function similar to encryption function

Our length doubler **LDT**



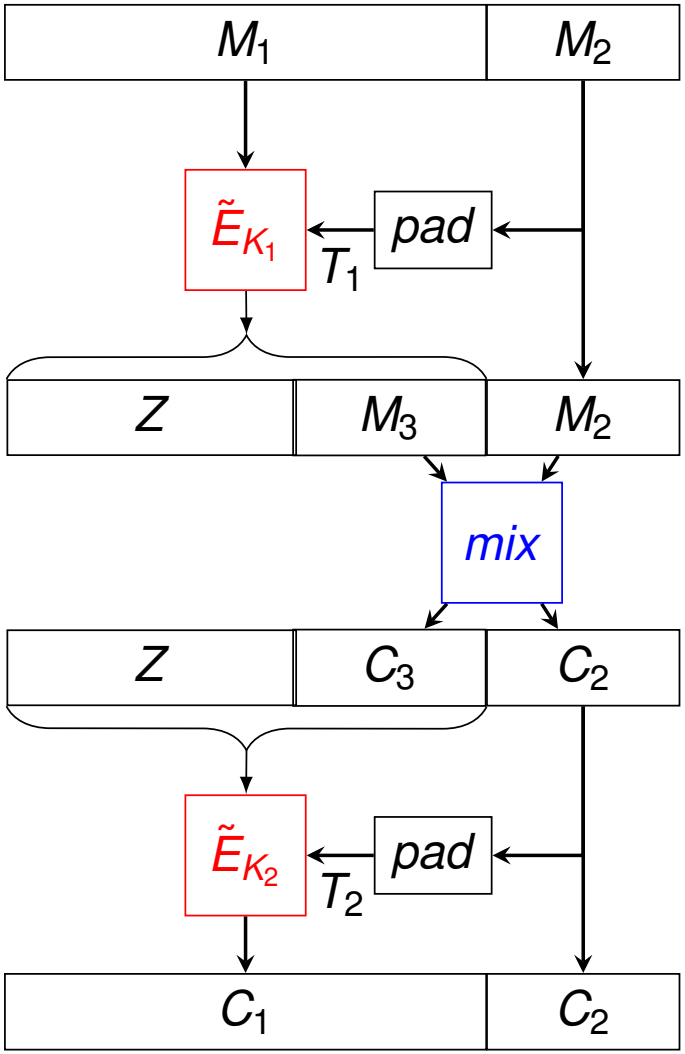
- 2 tweakable block cipher calls
- pure mixing function
- decryption function similar to encryption function

Our length doubler **LDT**



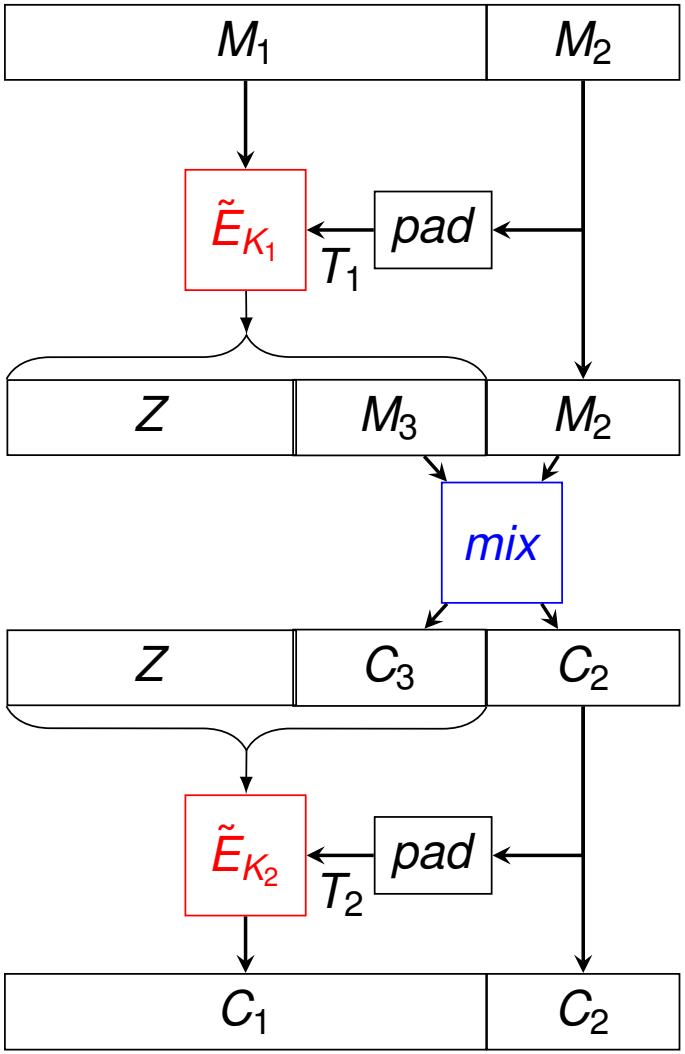
- 2 tweakable block cipher calls
- pure mixing function
- decryption function similar to encryption function

Our length doubler **LDT**



- 2 tweakable block cipher calls
- pure mixing function
- decryption function similar to encryption function

Our length doubler **LDT**



- 2 tweakable block cipher calls
- pure mixing function
- decryption function similar to encryption function

$2^{n/2}$ security

Security analysis

security lower bound: $2^{n/2}$

Security analysis

security lower bound: $2^{n/2}$

- Patarin's H-coefficient Technique

$$\frac{Pr(X_{\mathcal{O}} = \tau)}{Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

Security analysis

security lower bound: $2^{n/2}$

- Patarin's H-coefficient Technique

$$\frac{Pr(X_{\mathcal{O}} = \tau)}{Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

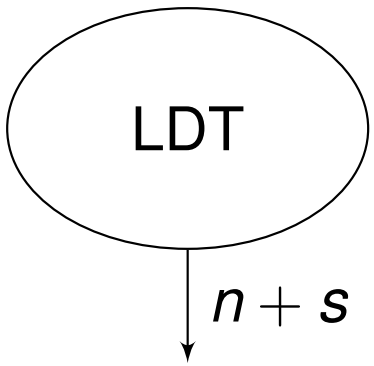
- our case: $Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}}) = 0$ and $\epsilon = q^2/2^n$

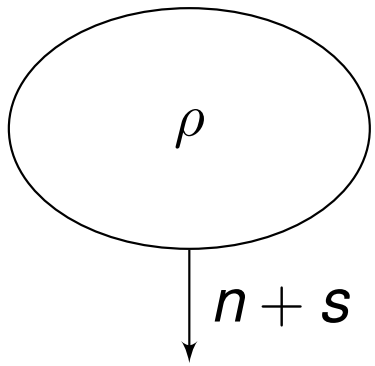
Security analysis

security upper bound: $2^{n-s/2}$

Security analysis

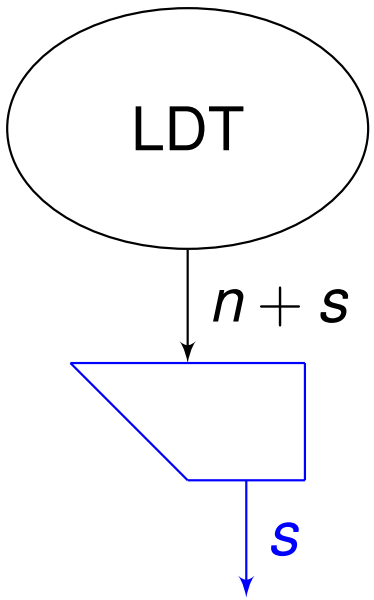
security upper bound: $2^{n-s/2}$

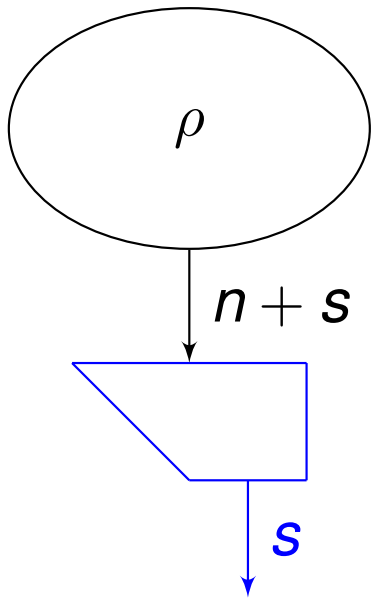




Security analysis

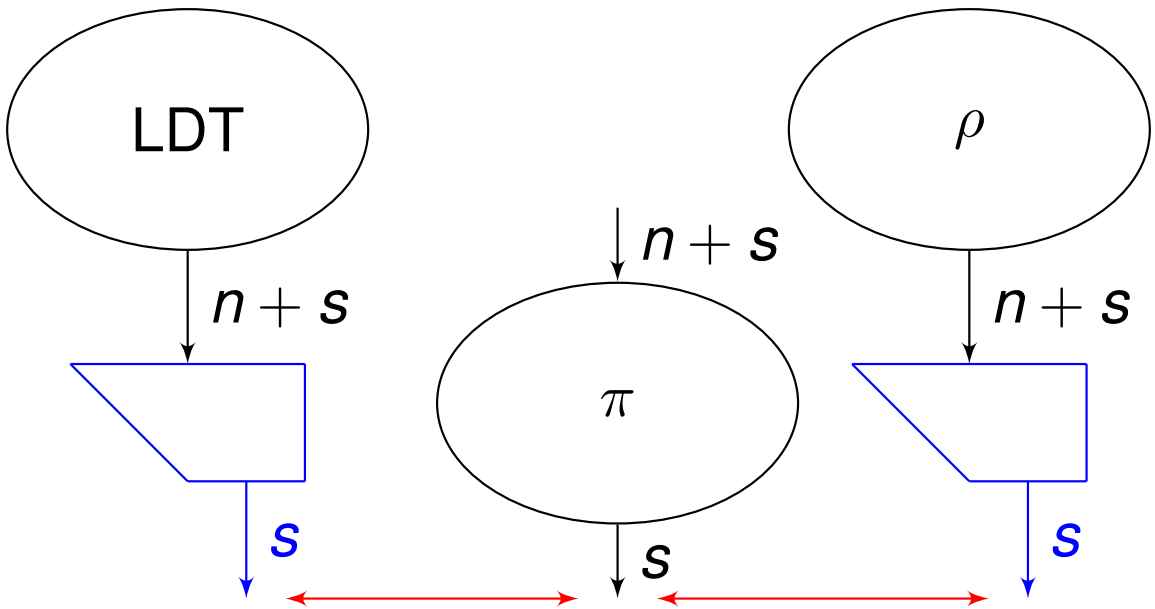
security upper bound: $2^{n-s/2}$





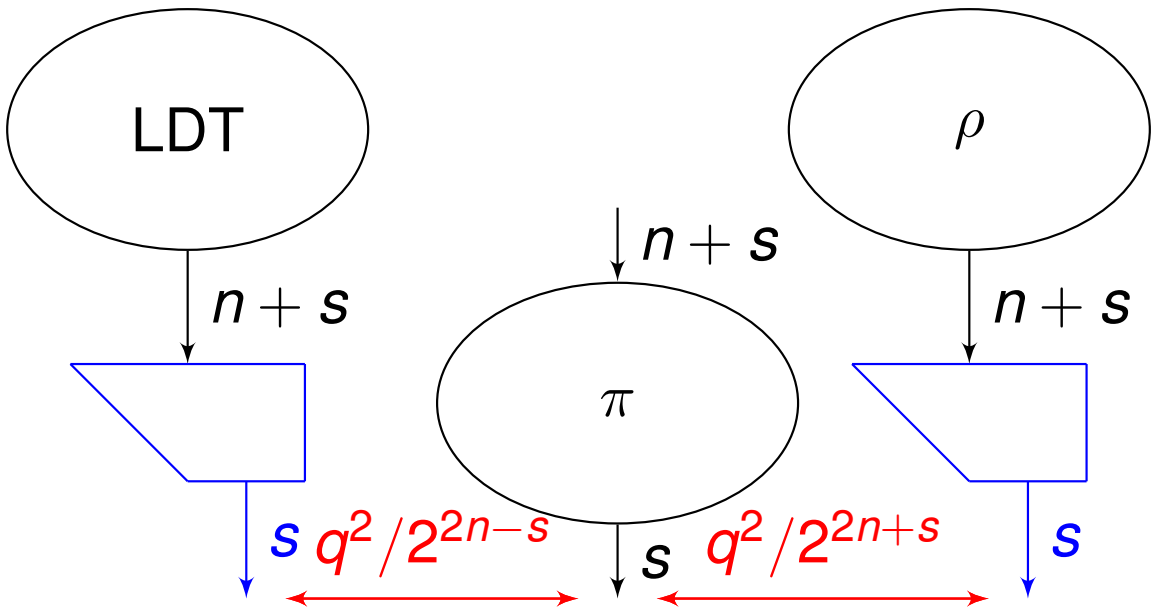
Security analysis

security upper bound: $2^{n-s/2}$



Security analysis

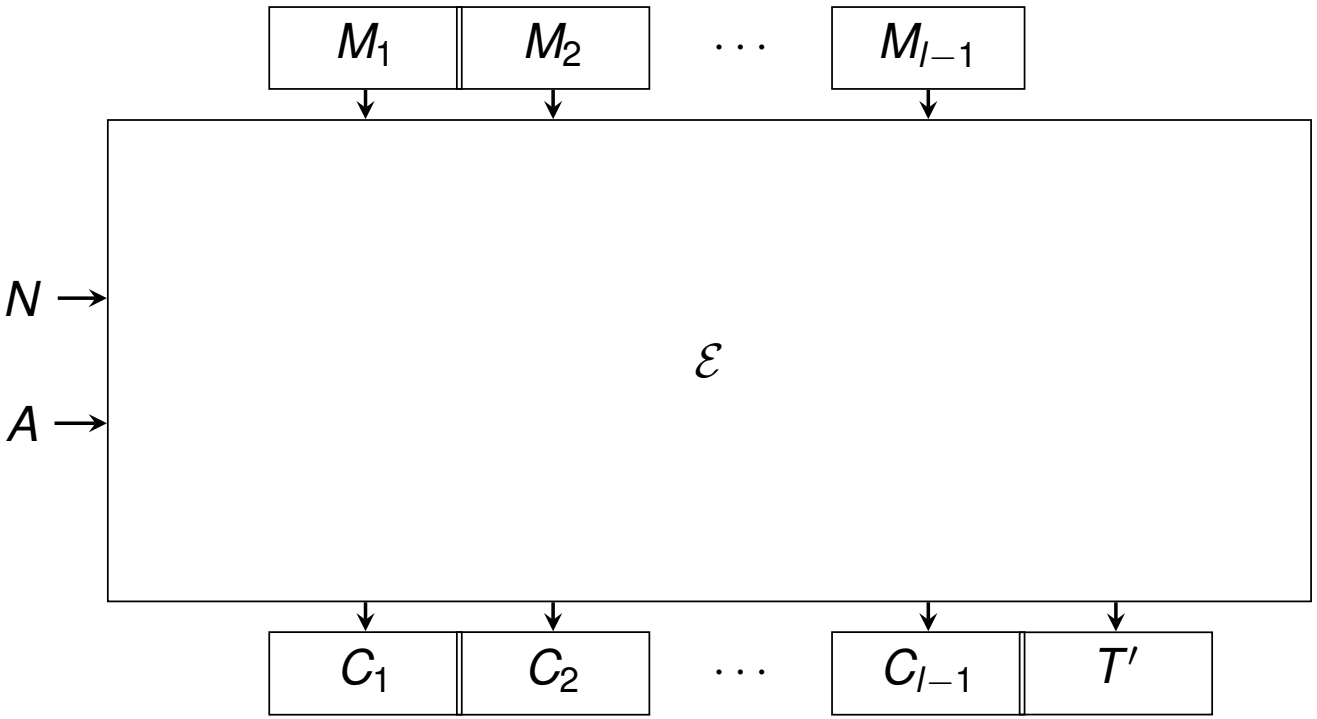
security upper bound: $2^{n-s/2}$



Comparison

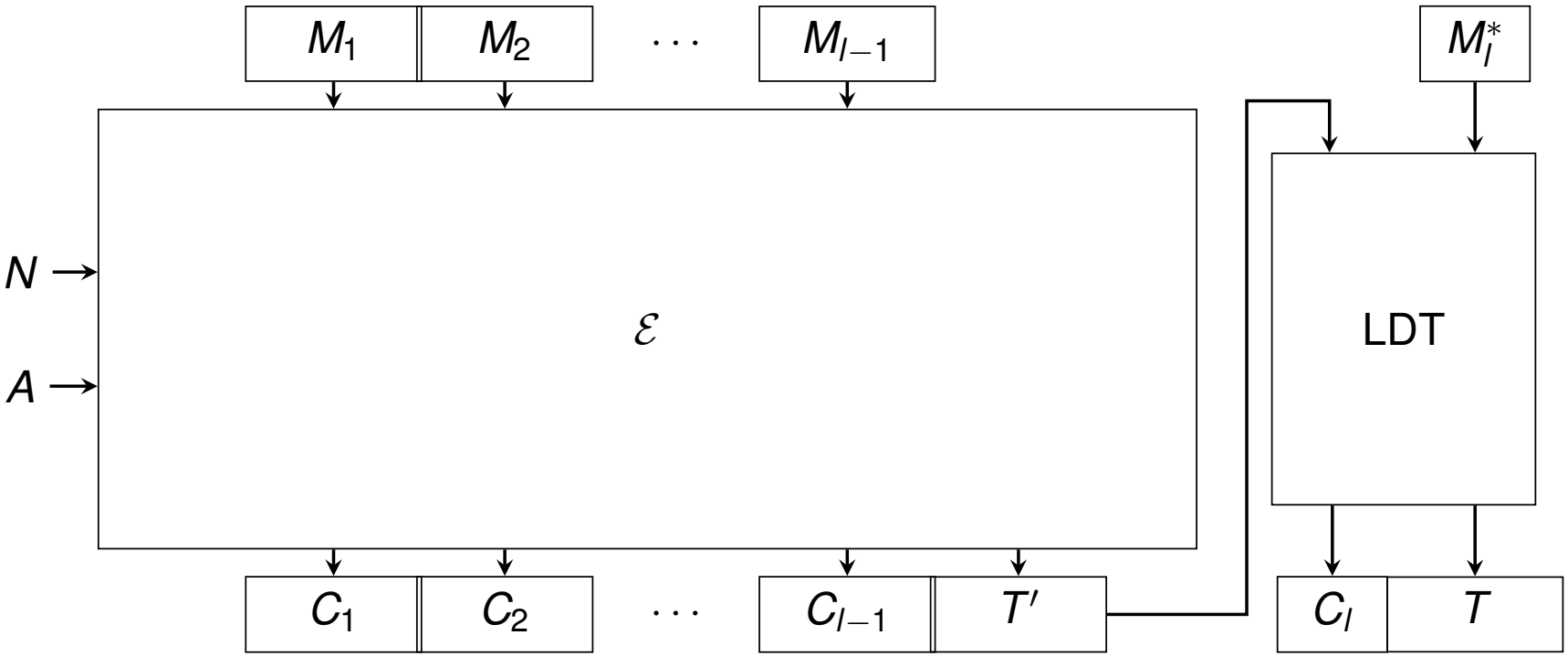
length doubler	security ($\log_2$)	key length	cryptographic primitive calls	mixing function
XLS	$n/2$	$2n$	3 BC	ϵ-good
DE	$n/2$	$5n$	4 hash+BC	-
HEM	$n/2$	$3n$	4 hash+BC	ϵ-good
LDT	$n/2$	$2n$	2 TBC	pure

Scheme for arbitrary data



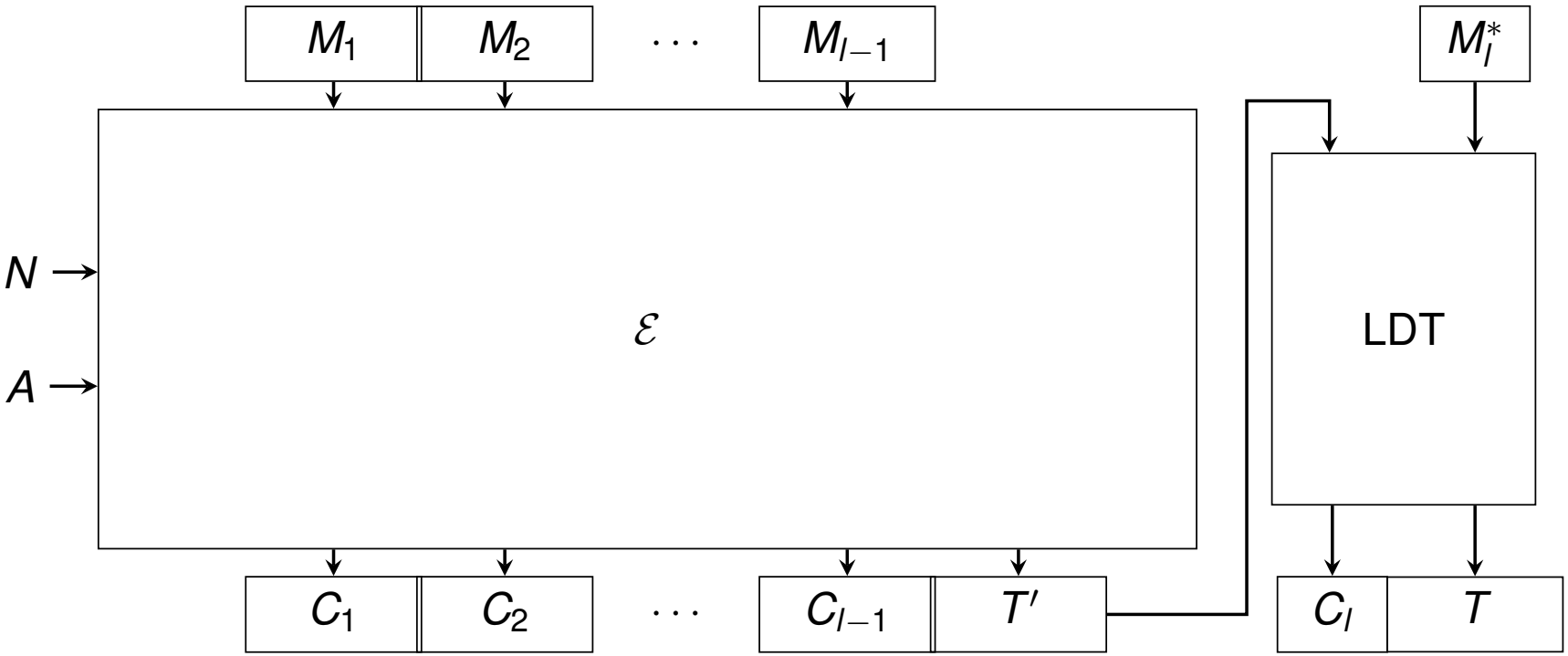
combine AE scheme for integral data + LDT

Scheme for arbitrary data



combine AE scheme for integral data + LDT

Scheme for arbitrary data



combine AE scheme for integral data + LDT

$2^{n/2}$ security

Conclusion

new results

- birthday bound length doubler
- 2 tweakable block cipher calls + pure mixing function
- AE scheme for arbitrary length data

Conclusion

new results

- birthday bound length doubler
- 2 tweakable block cipher calls + pure mixing function
- AE scheme for arbitrary length data

further research

- beyond birthday bound?
- multiple round?
- other optimizations?

Conclusion

new results

- birthday bound length doubler
- 2 tweakable block cipher calls + pure mixing function
- AE scheme for arbitrary length data

further research

- beyond birthday bound?
- multiple round?
- other optimizations?

Thank you for your attention!