

Rate One-third Non-malleable Codes

STOC 2022

Sruthi Sekar



Divesh
Aggarwal



Bhavana
Kanukurthi



Sai Lakshmi Bhavana
Obbattu

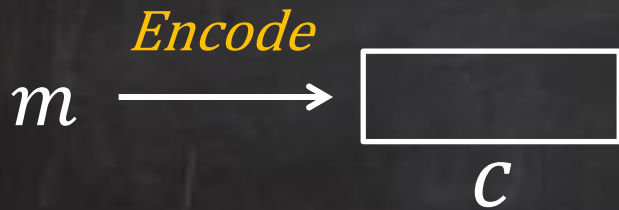


Maciej
Obremski



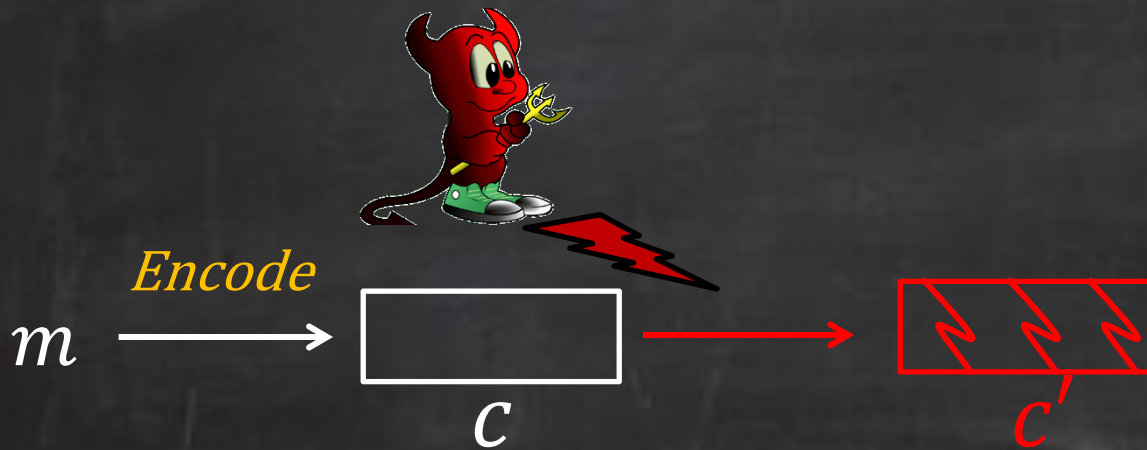
Non-malleable Codes

Dziembowski, Pietrzak, Wichs (ITCS 2010)



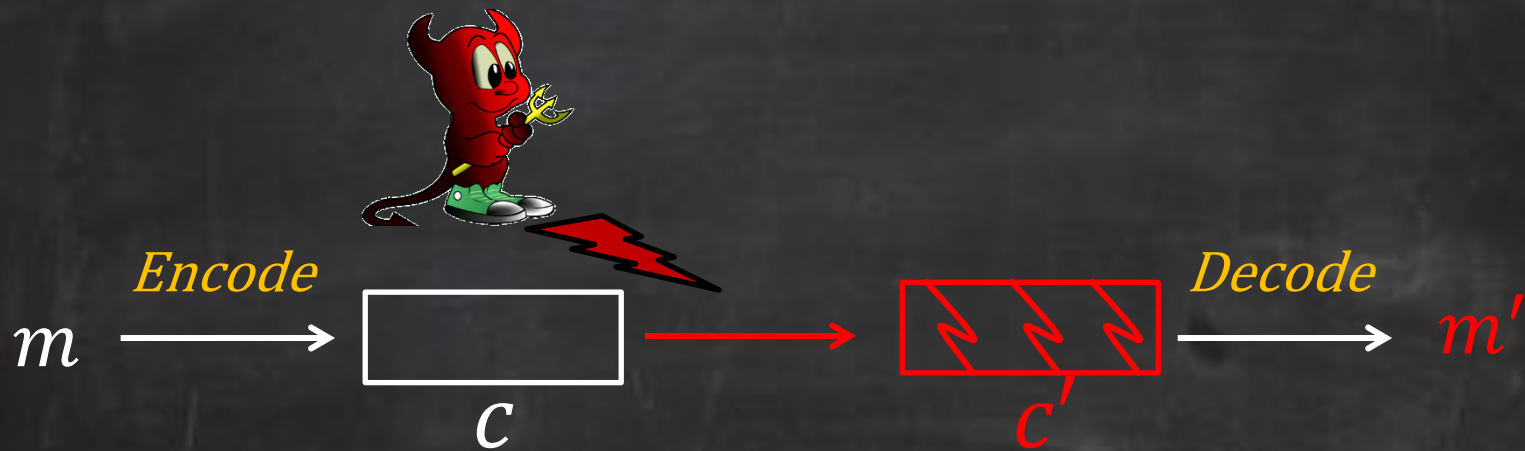
Non-malleable Codes

Dziembowski, Pietrzak, Wichs (ITCS 2010)



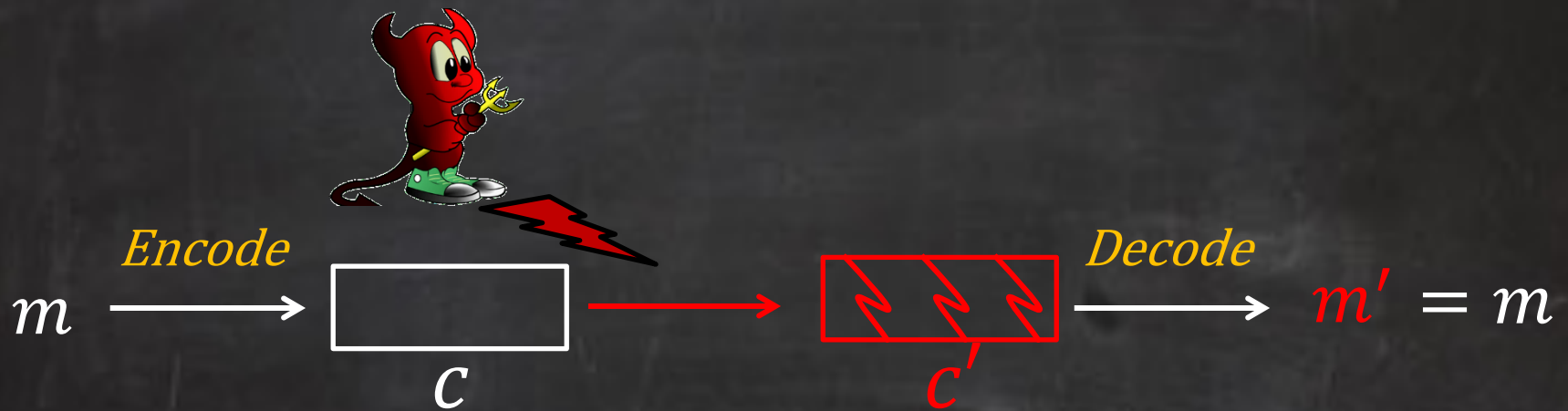
Non-malleable Codes

Dziembowski, Pietrzak, Wichs (ITCS 2010)



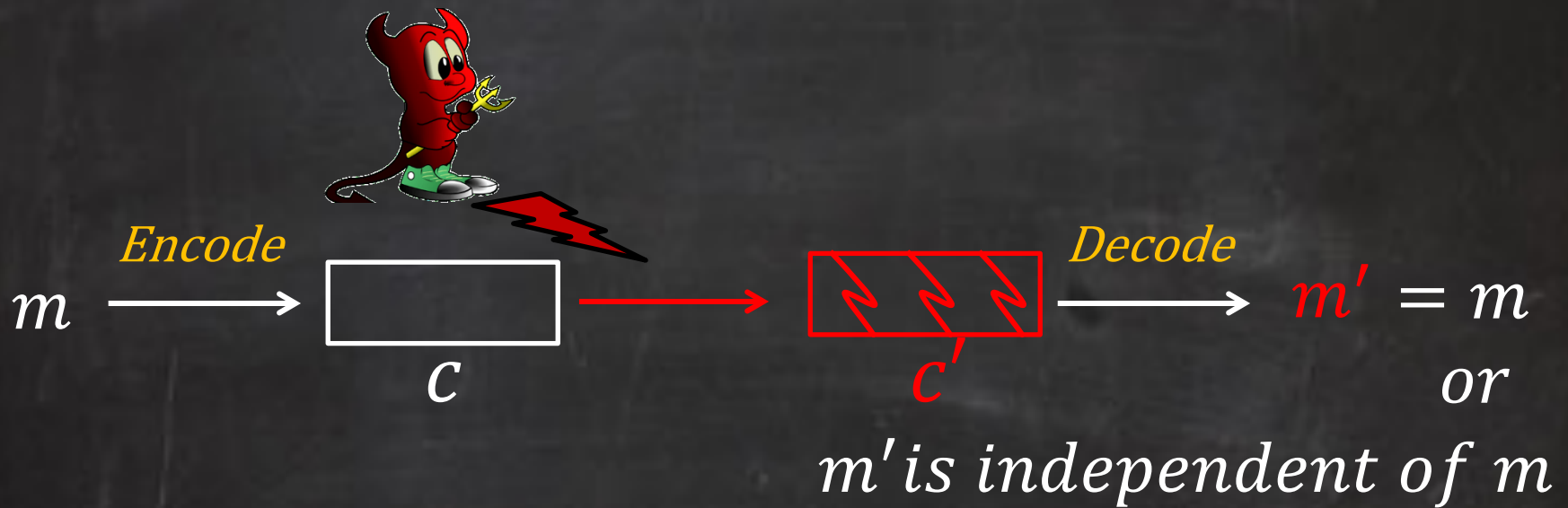
Non-malleable Codes

Dziembowski, Pietrzak, Wichs (ITCS 2010)



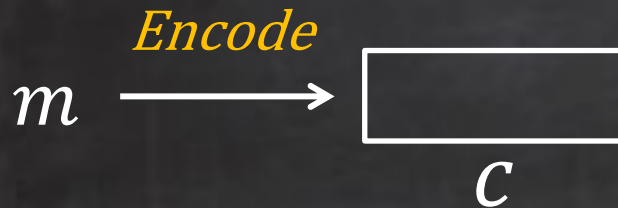
Non-malleable Codes

Dziembowski, Pietrzak, Wichs (ITCS 2010)



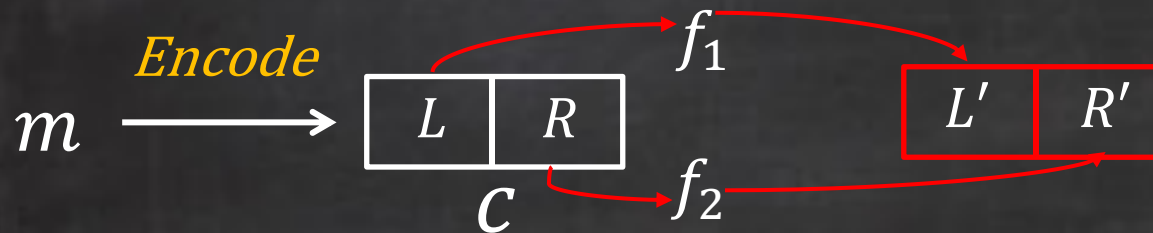
Non-malleable Codes

Formalizing Non-malleability



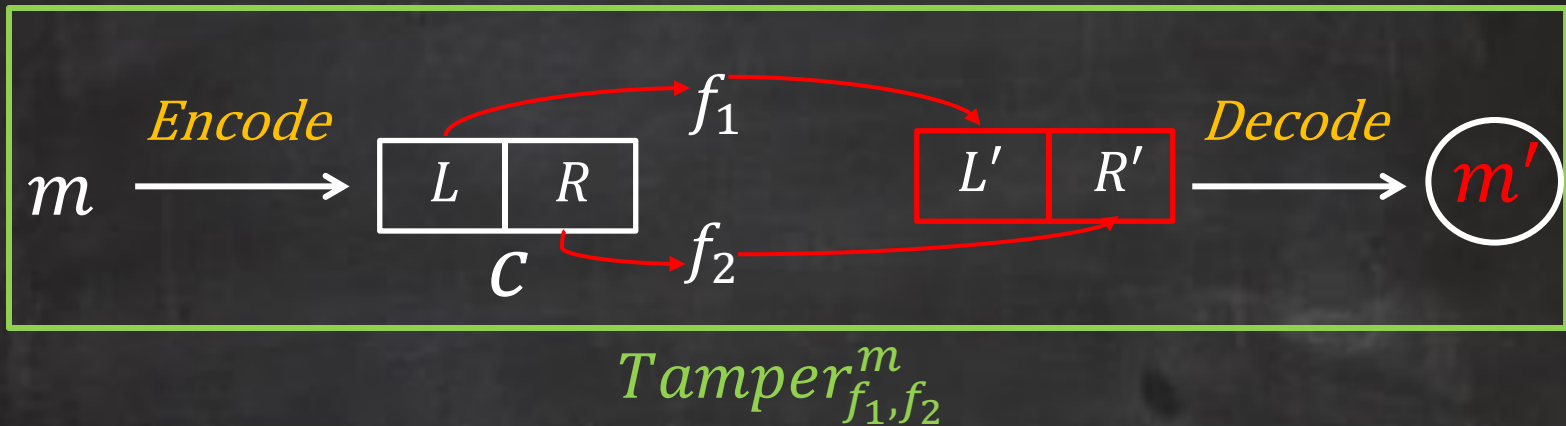
Non-malleable Codes

Formalizing Non-malleability



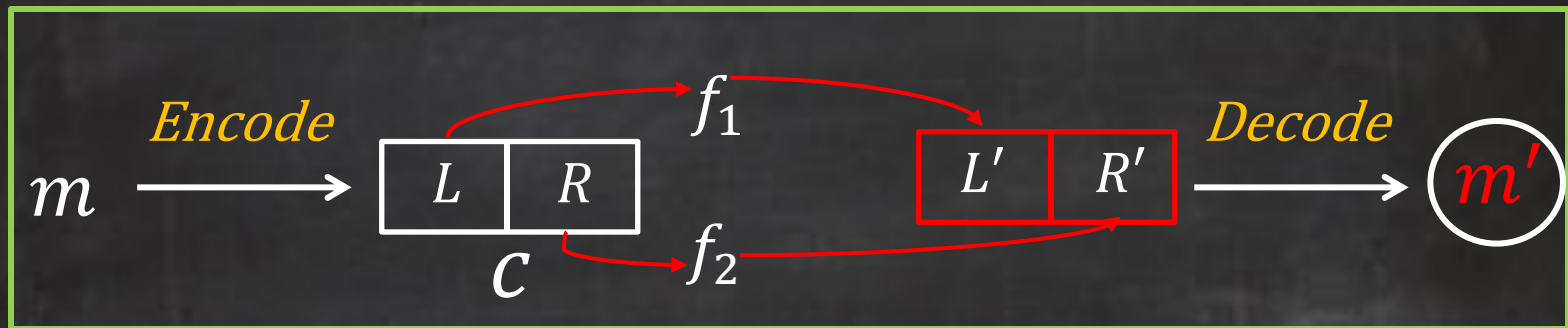
Non-malleable Codes

Formalizing Non-malleability



Non-malleable Codes

Formalizing Non-malleability

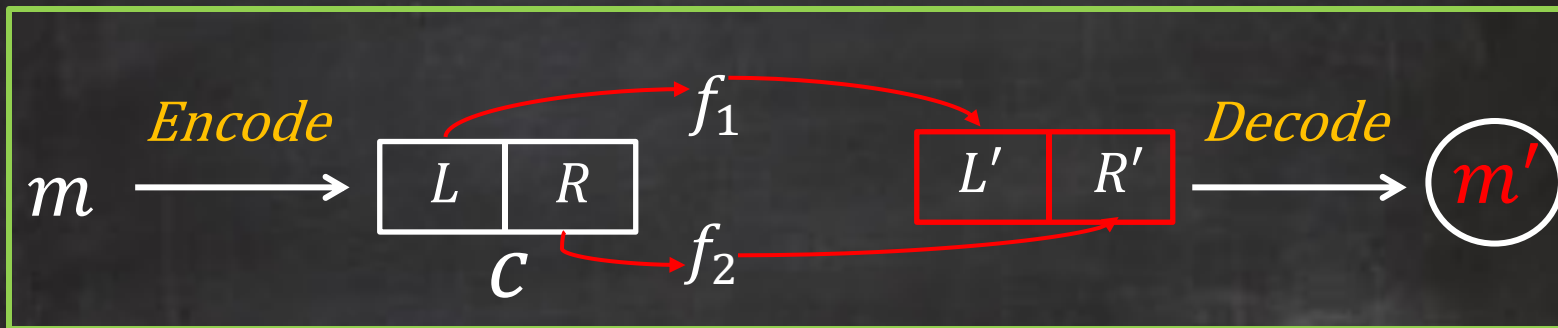


$Tamper_{f_1, f_2}^m$

$\exists Sim_{f_1, f_2}$ such that

Non-malleable Codes

Formalizing Non-malleability



$Tamper_{f_1, f_2}^m$

$\exists Sim_{f_1, f_2}$ such that
 $\forall m,$

$\approx$

Sim_{f_1, f_2}

Non-malleable Codes

Applications

- Non-malleable Commitments
[Goyal, Pandey, Richelson 2016]

Non-malleable Codes

Applications

- Non-malleable Commitments
[Goyal, Pandey, Richelson 2016]
- Non-malleable Secret Sharing
[Goyal, Kumar 2018]

Non-malleable Codes

Applications

- Non-malleable Commitments
[Goyal, Pandey, Richelson 2016]
- Non-malleable Secret Sharing
[Goyal, Kumar 2018]
- Domain Extension for Non-malleable Encryption
[Coretti, Maurer, Tackmann, Venturi 2014]

Non-malleable Codes

Applications

- Non-malleable Commitments
[Goyal, Pandey, Richelson 2016]
- Non-malleable Secret Sharing
[Goyal, Kumar 2018]
- Domain Extension for Non-malleable Encryption
[Coretti, Maurer, Tackmann, Venturi 2014]
- Privacy Amplification
[Chattopadhyay, Kanukurthi, Obbattu, Sekar 2019]

Non-malleable Codes

Applications

- Non-malleable Commitments
[Goyal, Pandey, Richelson 2016]
- Non-malleable Secret Sharing
[Goyal, Kumar 2018]
- Domain Extension for Non-malleable Encryption
[Coretti, Maurer, Tackmann, Venturi 2014]
- Privacy Amplification
[Chattopadhyay, Kanukurthi, Obbattu, Sekar 2019]
- Black-box 4-round pairwise MPC in the plain model
[Ishai, Khurana, Sahai, Srinivasan 2021]

Non-malleable Codes

Parameters

- Tampering Family:

- Rate:

Non-malleable Codes

Parameters

- Tampering Family:



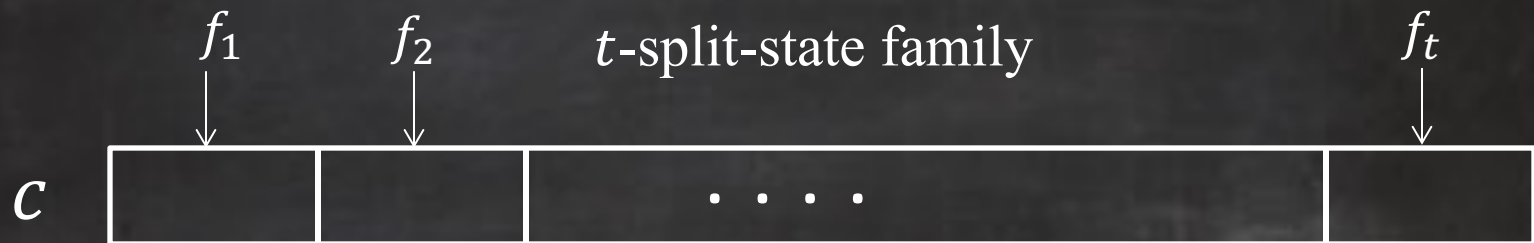
$$\mathcal{F}_t = \{(f_1, f_2, \dots, f_t): f_i: \{0,1\}^{\frac{n}{t}} \rightarrow \{0,1\}^{\frac{n}{t}} \text{ for each } i\}$$

- Rate:

Non-malleable Codes

Parameters

- Tampering Family:



Lower the value of $t \Rightarrow$ More powerful Adversary

- Rate:

Non-malleable Codes

Parameters

- Tampering Family:



Lower the value of $t \Rightarrow$ More powerful Adversary

- Rate: $= \frac{\text{message length}}{\text{codeword length}}$

Non-malleable Codes

Parameters

- Tampering Family:



Lower the value of $t \Rightarrow$ More powerful Adversary

- Rate: Higher Rate $\Rightarrow$ Lower Redundancy

Non-malleable Codes

Parameters

- Tampering Family:



Lower the value of $t \Rightarrow$ More powerful Adversary

- Rate: Higher Rate $\Rightarrow$ Lower Redundancy

Long-standing Open Problem: Build optimal rate NMCs for $\mathcal{F}_2$

Non-malleable Codes

Prior Works

[CG14a]

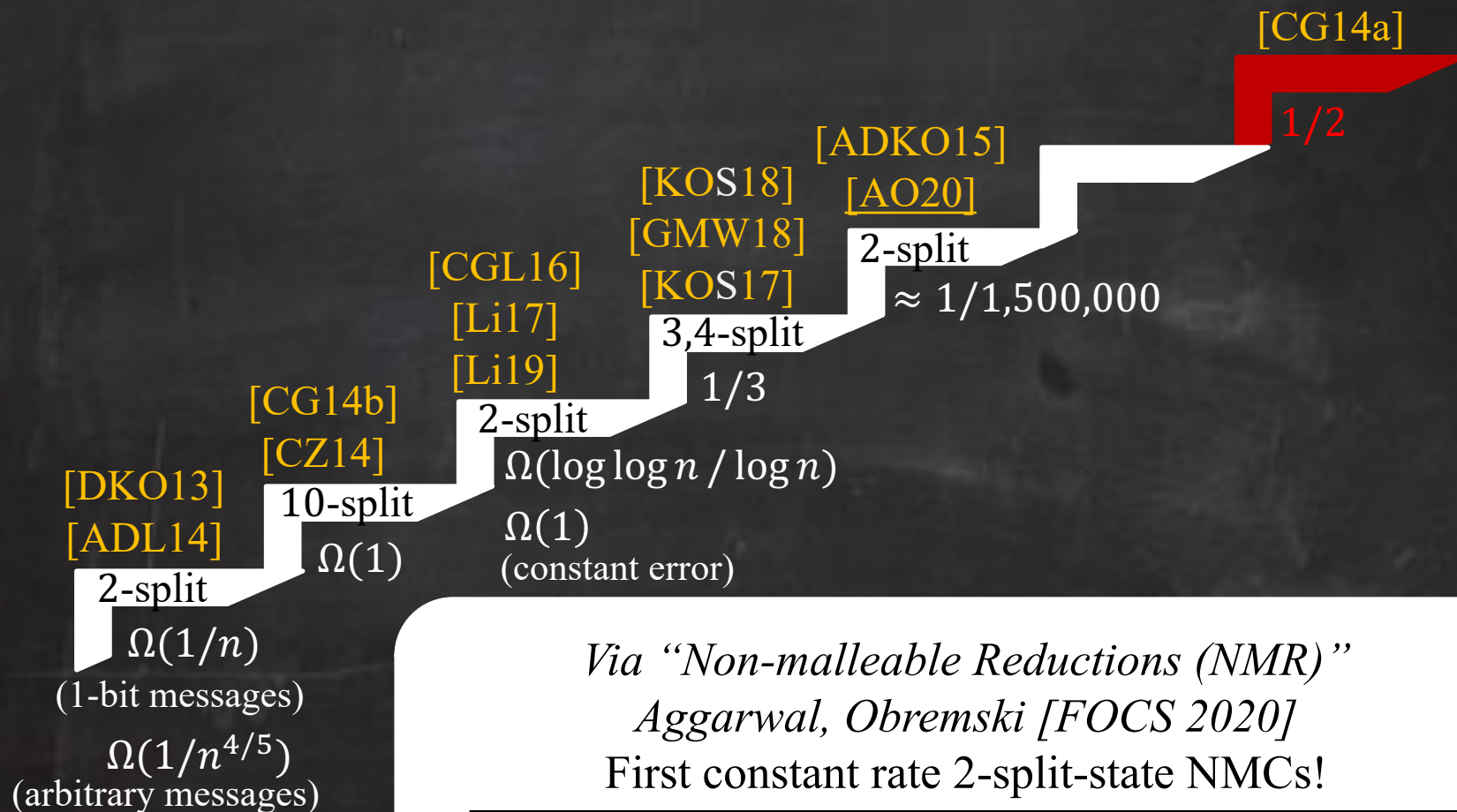
$1/2$

Cheraghchi and Guruswami [ITCS 2014]

Feasibility Result: For any t -split state
best rate achievable is $1 - 1/t$

Non-malleable Codes

Prior Works

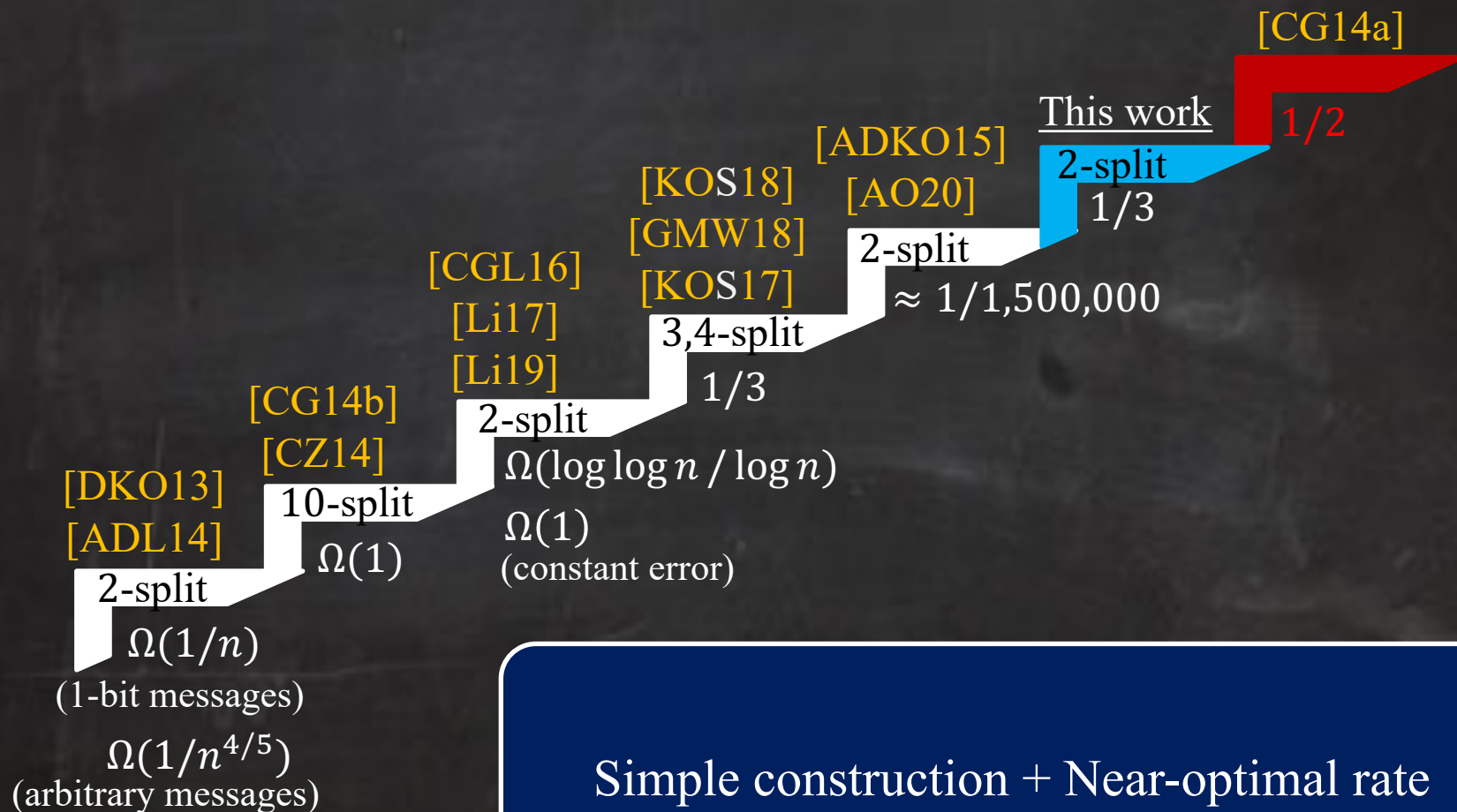


Via “Non-malleable Reductions (NMR)”
 Aggarwal, Obremski [FOCS 2020]
 First constant rate 2-split-state NMCs!

Caveat- Complex construction and proof, each step of NMR incurs unsalvageable parameter loss!

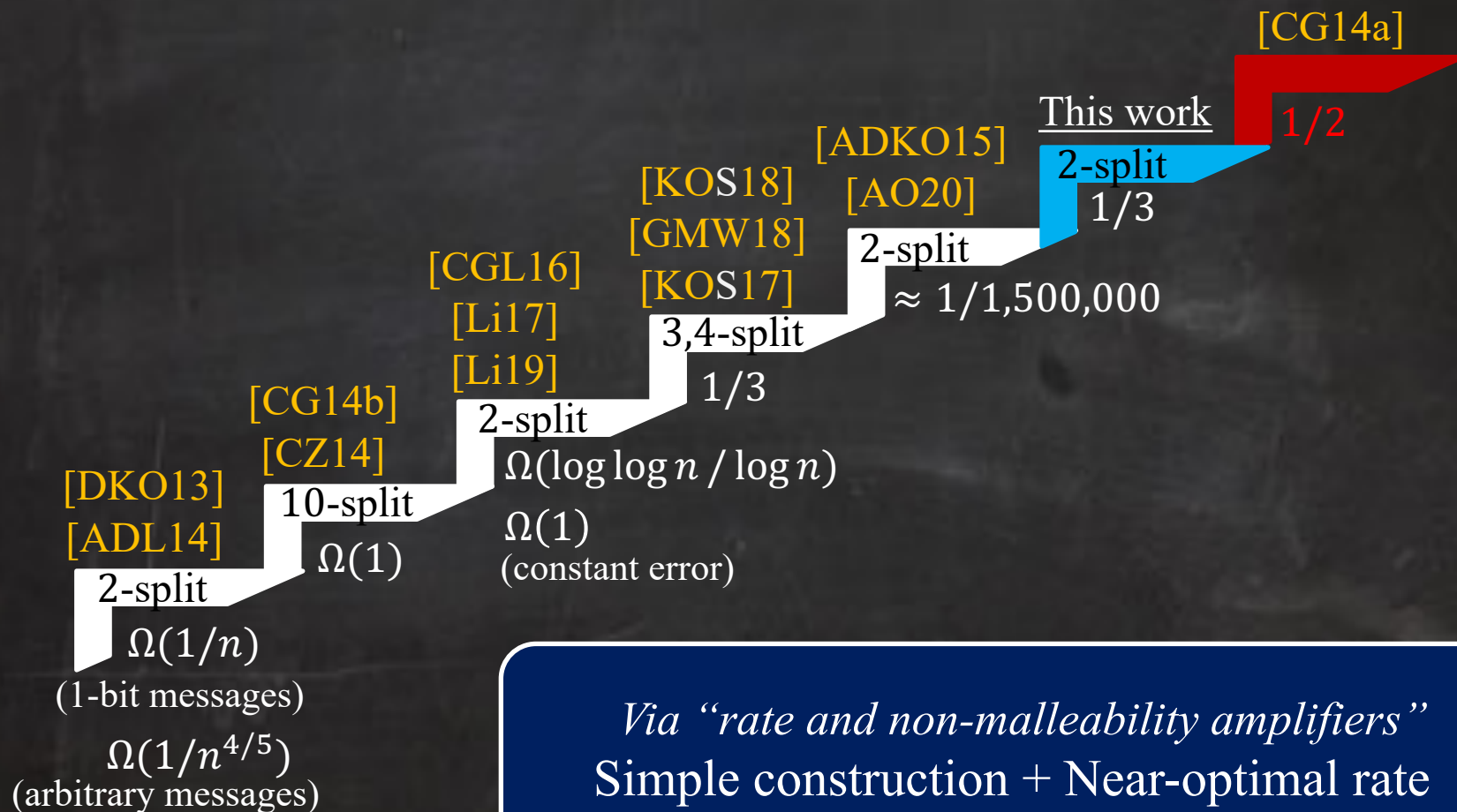
Non-malleable Codes

Prior Works



Non-malleable Codes

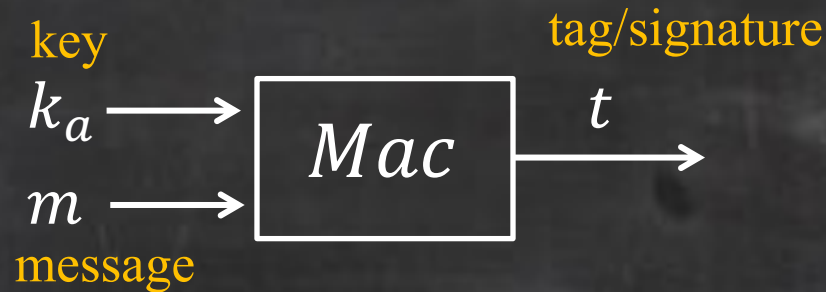
Prior Works



CONSTRUCTION

Building Blocks

I: Information-theoretic One time Message Authentication Code (MAC)



For any $m \neq m', t, t'$

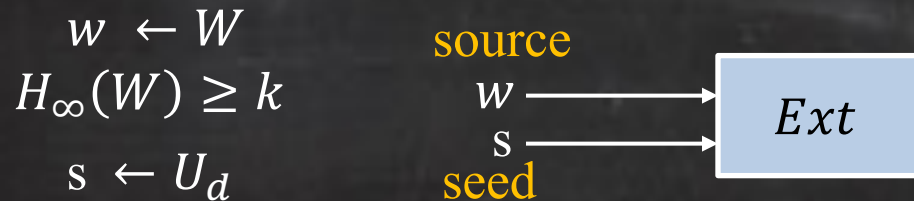
$$\Pr[Mac(k_a, m) = t \mid Mac(k_a, m') = t'] \leq \epsilon$$

Building Blocks

I: Information-theoretic One time Message Authentication Code (MAC)

II: Strong Randomness Extractors

[Nissan and Zuckerman, 1996]



Building Blocks

I: Information-theoretic One time Message Authentication Code (MAC)

II: Strong Randomness Extractors

[Nissan and Zuckerman, 1996]



$$Ext(W; U_d), f(W), U_d \approx U, f(W), U_d$$

Building Blocks

I: Information-theoretic One time Message Authentication Code (MAC)

II: Strong Randomness Extractors

III: Any 2-split-state non-malleable code.
(used to encode only “short messages”)

Our Construction

Encode(m):

$$m \oplus \text{Ext}(w; s)$$

$$w \leftarrow W$$

$$s \leftarrow U_d$$

Our Construction

Encode(m):

$$m \oplus \text{Ext}(w; s)$$

c



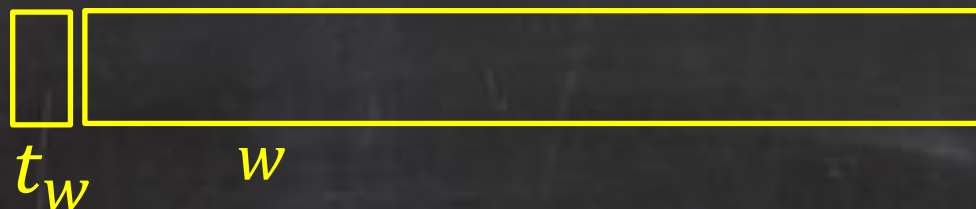
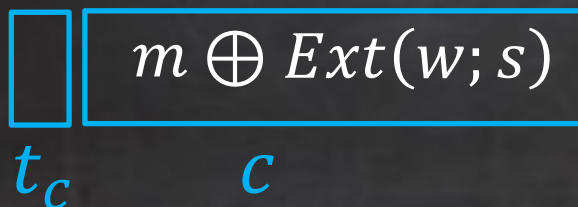
w

$$w \leftarrow W$$

$$s \leftarrow U_d$$

Our Construction

Encode(m):



$$w \leftarrow W$$

$$s \leftarrow U_d$$

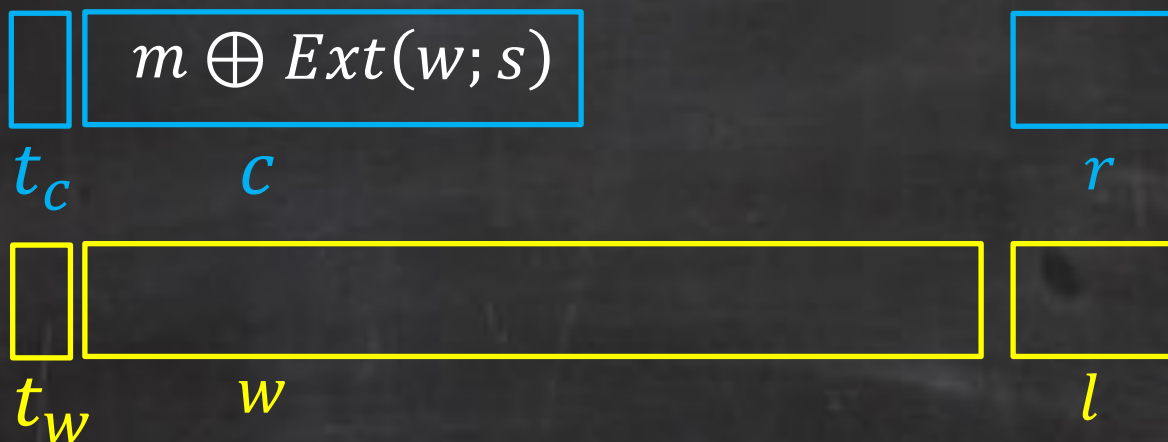
$$k_w, k_c \leftarrow \mathcal{K}$$

$$t_w \leftarrow \text{Mac}_{k_w}(w)$$

$$t_c \leftarrow \text{Mac}_{k_c}(c)$$

Our Construction

Encode(m):



$$w \leftarrow W$$

$$(l, r) \leftarrow \text{NMEnc}(s, k_w, k_c)$$

$$s \leftarrow U_d$$

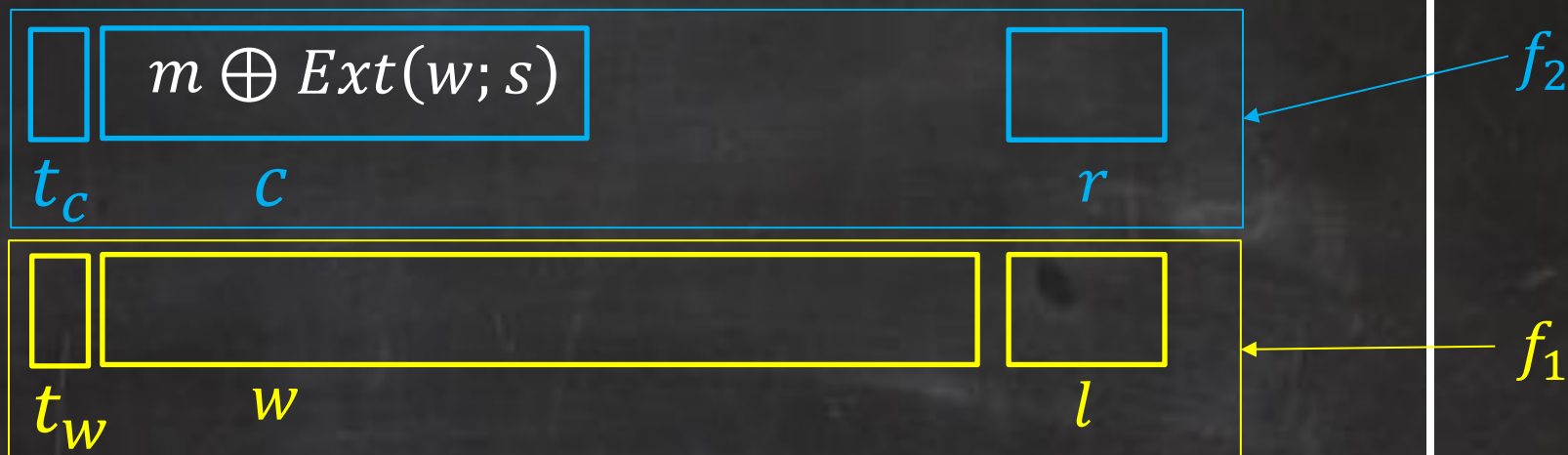
$$t_w \leftarrow \text{Mac}_{k_w}(w)$$

$$k_w, k_c \leftarrow \mathcal{K}$$

$$t_c \leftarrow \text{Mac}_{k_c}(c)$$

Our Construction

Encode(m):



$$w \leftarrow W$$

$$(l, r) \leftarrow \text{NMEnc}(s, k_w, k_c)$$

$$s \leftarrow U_d$$

$$t_w \leftarrow \text{Mac}_{k_w}(w)$$

$$k_w, k_c \leftarrow \mathcal{K}$$

$$t_c \leftarrow \text{Mac}_{k_c}(c)$$

Summary and Open Problems

- We build a 2-split-state NMC with rate $1/3$.
(improving prior known best rate of $\approx 1/1,500,000$).
- One of the simplest NMC constructions!
- OPEN: Can we get optimal rate for any split-state with t being a constant > 2 ?

THANK YOU
Questions?