Non-malleable Reductions and Applications

Divesh Aggarwal *
Yevgeniy Dodis *
Tomasz Kazana **
Maciej Obremski **

* New York University
** University of Warsaw

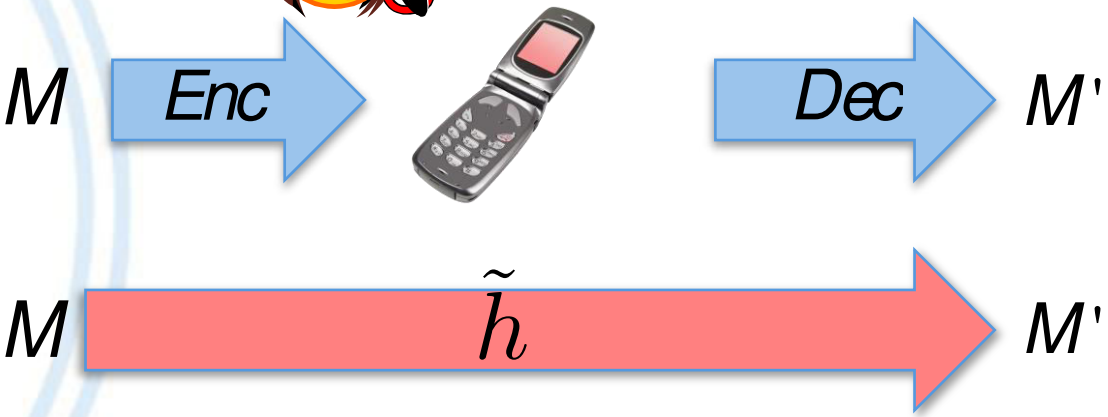
Plan

- Introduction to Non-Malleable Codes

- Split-state Model and Recent Results
- Non-malleable Reductions

Definition of Non-Malleable Codes

$h \in H$



Scheme is **non-malleable with respect to family H** if **h** can be represented as a **probabilistic combination**

- **constant** functions
- **identity** function

We have to limit class H

$$h(x) = Enc(1 + Dec(x))$$

$$h(Enc(M)) = Enc(1 + Dec(Enc(M))) = Enc(M + 1)$$

$\tilde{h}(x) = x + 1$ can not be represented as combination of constant functions and identity

Existential Result

Non-Malleable Codes (ICS 2010)

S.Dziembowski, K.Pietrzak and D.Wichs

- Existence of codes for small enough manipulation families via probabilistic argument

$$\log(\log(|H|)) < n$$

Where n is a size of codeword

$$\log(\log(|H_{\text{all}}|)) = n + \log(n)$$

Plan

- Introduction to Non-Malleable Codes

DONE

- Split-state Model and Recent Results

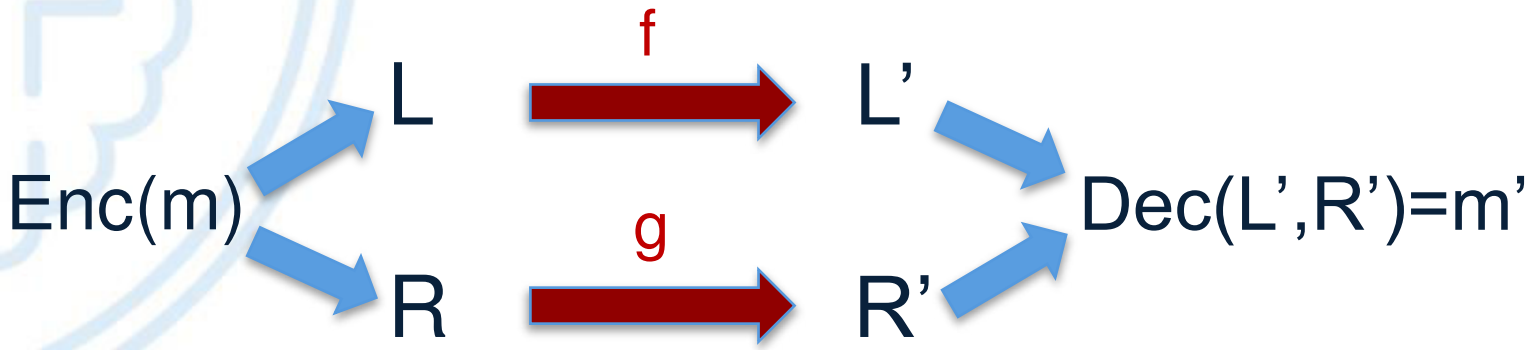
- Non-malleable Reductions

2-Split State Model

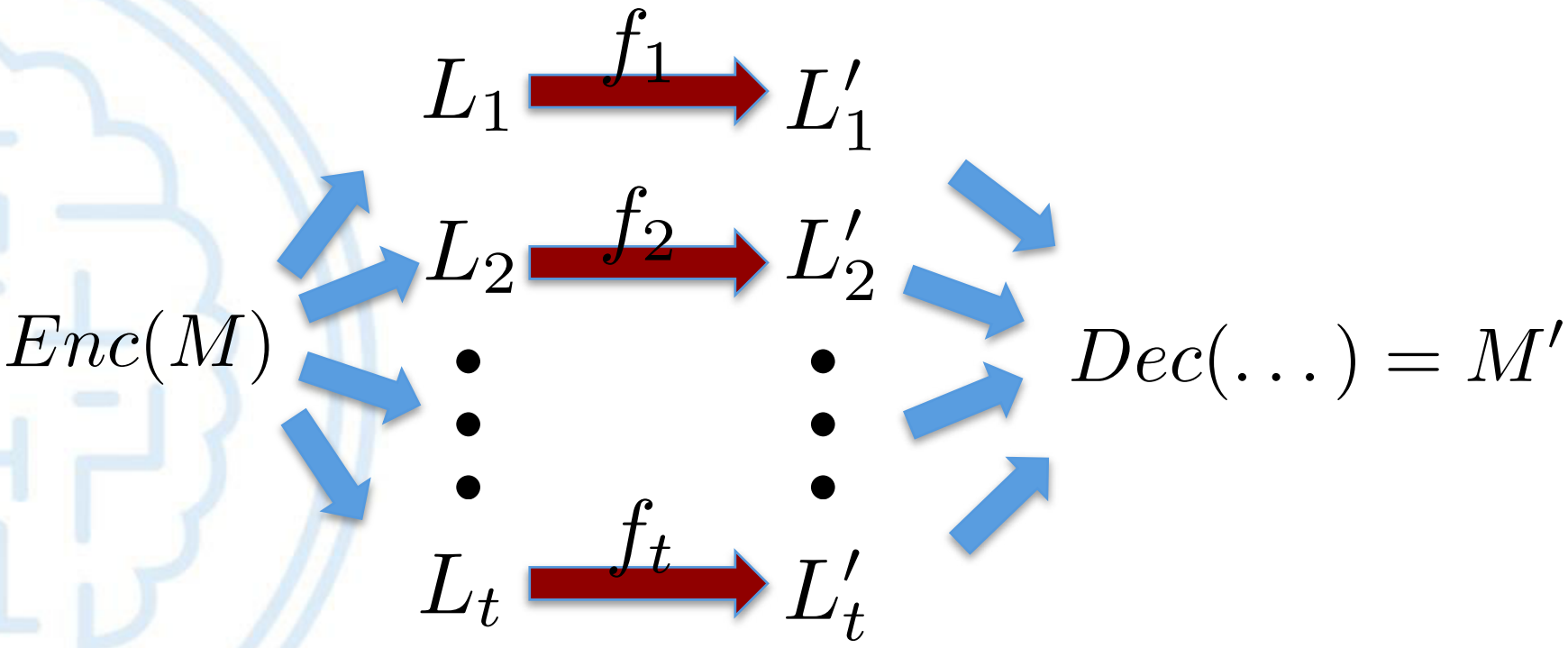
Enc(m)= L , R

Manipulation functions ***(f,g)*** are any arbitrary functions,

f,g are applied separately to ***L*** and ***R*** :



t-Split State Model



Recent Results

Non-malleable Codes from Two-source Extractors (Crypto'13)

S.Dziembowski (UW), T.Kazana (UW), M.Obremski (UW)

Non-malleable coding against bit-wise and split-state tampering (TCC'14)

M.Cheraghchi (MIT), V.Guruswami (CMU)

Non-malleable Codes from Additive Combinatorics (STOC'14)

D.Aggarwal (NYU), Y.Dodis (NYU), S.Lovett (UCSD)

Non-malleable Codes in the Constant Split-state Model (FOCS'14)

E.Chattopadhyay (U.Texas), D. Zuckerman (U.Texas)

Recent Results

	Number of states	Codeword length
[ADL'14]	2	$\mathcal{O}(n^7)$
[u.m.]	5	$\mathcal{O}(n^2)$
[CZ'14]	9	$\mathcal{O}(n)$

n- length of message

The more parts the easier it gets..

Plan

- Introduction to Non-Malleable Codes — DONE
- Split-state Model and Recent Results — DONE
- Non-malleable Reductions 

Non-malleable Reductions

$f \in \mathcal{F}$

M Enc Dec M'

M M'

Identity and constant functions

$g \in \mathcal{G}$

(Enc,Dec) is reduction $\mathcal{F} \Rightarrow G$

Non-malleable Reductions

$\mathcal{F}$ is reduced to $\mathcal{G}$ (denote: $\mathcal{F} \Rightarrow \mathcal{G}$) if there exists encoding scheme (Enc,Dec), s.t.

$$\forall_{f \in \mathcal{F}} \, \mathrm{Dec}(f(\mathrm{Enc}(.))) \subseteq \mathrm{Conv}(\mathcal{G})$$

such encoding scheme is called *NM-Reduction*

Non-malleable Code as Reduction

Let NM denote set of trivial manipulation functions

if (Enc,Dec) is Non-malleable Code with respect to $\mathcal{F}$ then

$$\text{(Enc,Dec) is reduction } \mathcal{F} \Rightarrow \text{NM}$$

Composition

If (Enc,Dec) is reduction $\mathcal{F} \Rightarrow \mathcal{G}$

and (Enc',Dec') is reduction $\mathcal{G} \Rightarrow \mathcal{H}$

then

(Enc(Enc'),Dec'(Dec)) is reduction $\mathcal{F} \Rightarrow \mathcal{H}$

Remark

If $\mathcal{F} \Rightarrow \mathcal{G}$

and we know Non-malleable Code with respect to family $\mathcal{G}$

then $\mathcal{F} \Rightarrow \mathrm{NM}$

Codeword length

Assume (Enc,Dec) is reduction $\mathcal{F} \Rightarrow G$

Let n be length of message

Let $l(n)$ be length of codeword obtained from Enc

$r(n) = \dfrac{l(n)}{n}$ will be called the rate of reduction

$$\mathcal{F} \Rightarrow_{r(n)} \mathcal{G}$$

Composition v.2

$$\text{If } \mathcal{F} \Rightarrow_{r_1(n)} \mathcal{G}$$

$$\text{and } \mathcal{G} \Rightarrow_{r_2(n)} \mathcal{H}$$

$$\text{then } \mathcal{F} \Rightarrow_{r_1(n) \cdot r_2(n)} \mathcal{H}$$

Recent Results

	Number of states	Codeword length	
[ADL'14]	2	$\mathcal{O}(n^7)$	$\mathcal{S}_2 \Rightarrow_{\mathcal{O}(n^6)} \mathrm{NM}$
[u.m.]	5	$\mathcal{O}(n^2)$	$\mathcal{S}_5 \Rightarrow_{\mathcal{O}(n)} \mathrm{NM}$
[CZ'14]	9	$\mathcal{O}(n)$	$\mathcal{S}_9 \Rightarrow_{\mathrm{const.}} \mathrm{NM}$

n- length of message

Captain Obvious strikes again

$$S_t \Rightarrow_{\text{const.}} S_2$$

That does not give us much..

Our result

Non-malleable Reductions and Applications

D.Aggarwal, Y.Dodis, T.Kazana, M.Obremski

$$\mathcal{S}_2 \Rightarrow_{\text{const.}} \mathcal{S}_t$$

Which combined with [CZ'14] $(\mathcal{S}_9 \Rightarrow_{\text{const.}} \text{NM})$

Gives first constant rate (linear length codeword) Non-malleable Code construction in 2-split-state model

$$\mathcal{S}_2 \Rightarrow_{\text{const.}} \text{NM}$$

Thank You!