Fast and Secure Updatable Encryption

Colin Boyd [1] Gareth T. Davies [2] Kristian Gjøsteen [1] Yao Jiang [1]

August 10, 2020

[1]Norwegian University of Science and Technology (NTNU), Norway
[2]Bergische Universität Wuppertal, Germany

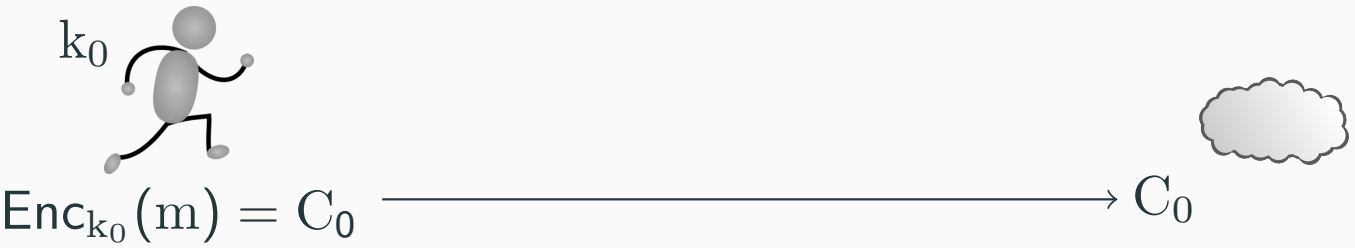
NTNU
Norwegian University of Science and Technology

BERGISCHE UNIVERSITÄT WUPPERTAL

Table of contents

Updatable Encryption

Problem Motivation: Outsourcing

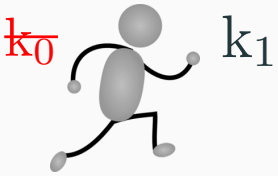


Problem Motivation: Outsourcing

$$\mathsf{Dec}_{k_0}(C_0) = m_0$$

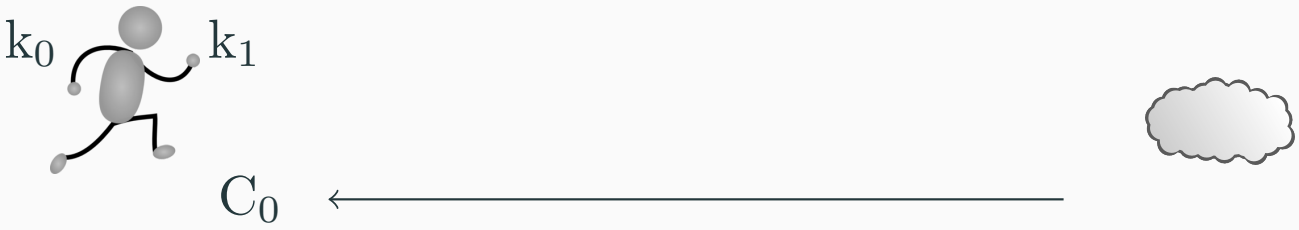
- Threats: Key compromise

Problem Motivation: Outsourcing



- Threats: Key compromise
- Solution: Key rotation

Key Rotation: a standard approach



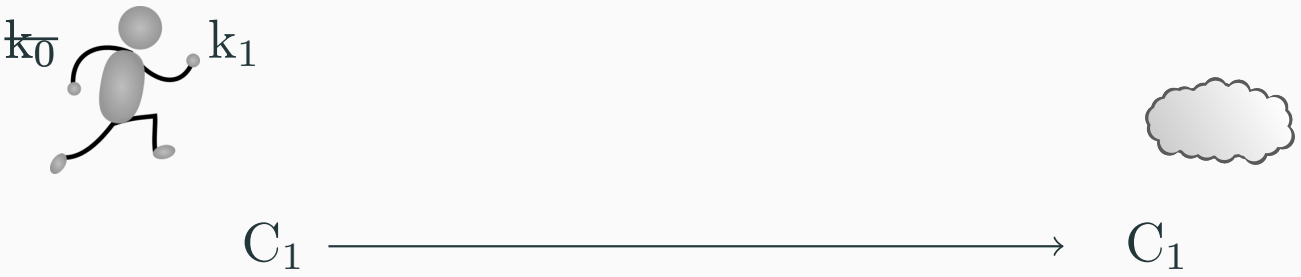
Key Rotation: a standard approach

$$m = \mathsf{Dec}_{k_0}(C_0)$$

Key Rotation: a standard approach

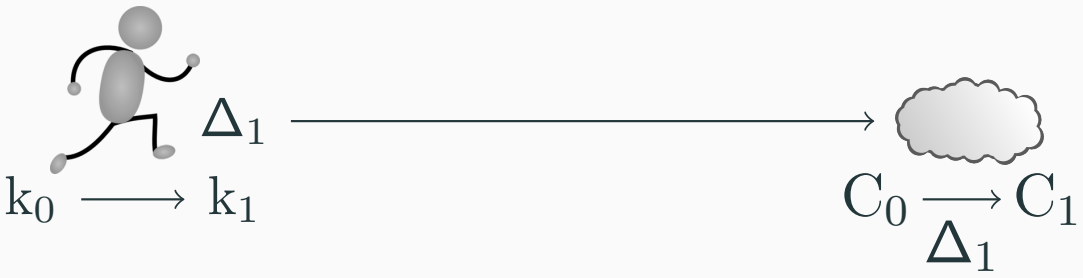
$\mathsf{Enc}_{k_1}(m) = C_1$

Key Rotation: a standard approach



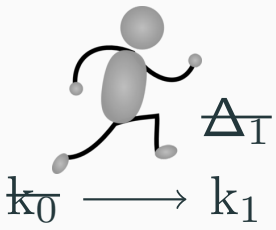
- Download and re-upload is infeasible
  even for moderate storage requirements

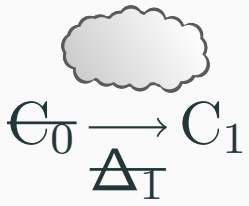
Key Rotation: Updatable Encryption (UE)



- **Key Homomorphic PRFs and their Applications**
  Boneh, Lewi, Montgomery, Raghunathan; CRYPTO '13 (+ ePrint 2015/220)

Key Rotation: Updatable Encryption (UE)





- Client only ever needs to store one key
- fresh encryptions, updated ciphertexts and tokens should all reveal nothing about plaintext

- **Key Homomorphic PRFs and their Applications**
  Boneh, Lewi, Montgomery, Raghunathan; CRYPTO '13 (+ ePrint 2015/220)

What Is Realistic?

- Security properties: confidentiality and integrity
  - What an attacker can possibly do?
  - What is the right security notion for UE?
- Users do encryption, then server(s) update ciphertexts for millions of users
  - Encryption and update must be efficient

- **Updatable Encryption with Post-Compromise Security**
  Lehmann, Tackmann; Eurocrypt '18

Security Properties

Epoch-based Corruptions

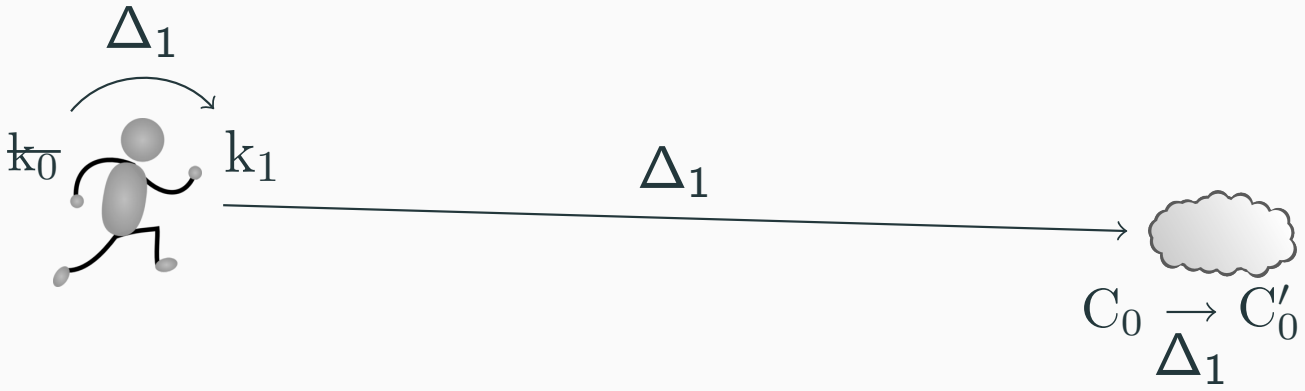
0	1	2	3	4	5	6	7	...	n
	Δ_1	Δ_2	Δ_3	Δ_4	Δ_5	Δ_6	Δ_7	...	
k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	...	k_n
C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	...	C_n

- Directly obtained information:
  - Adversary adaptively corrupts keys and tokens
  - Adversary can asks for ciphertexts
- Inferred information (Assume bi-directionality):
  - C_{i+1} and Δ_{i+1} is enough to compute C_i
  - k_{i+1} and Δ_{i+1} is enough to compute k_i
  - k_i and k_{i+1} is enough to compute Δ_{i+1}
- Adversary can use this information to trivially win a security game!

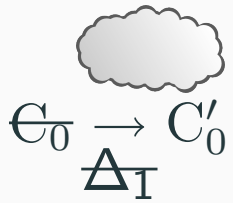
Confidentiality: a motivating example

$\mathsf{Enc}_{k_0}(\mathit{Contact\ A}) = C_0$ ⟶  C_0

Confidentiality: a motivating example



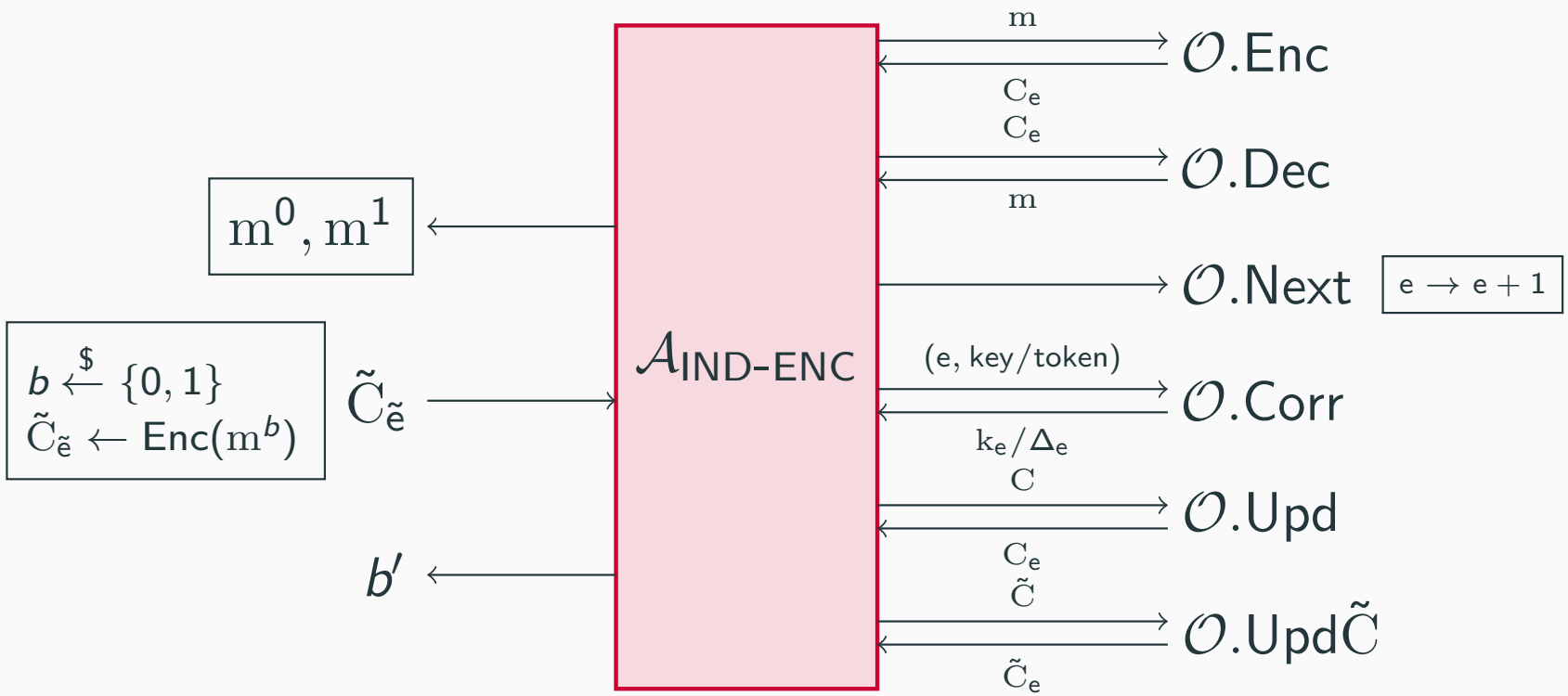
Confidentiality: a motivating example



Confidentiality: a motivating example

- Which ciphertext is the newest?
- How many ciphertexts are recently added?

Prior notions: Indistinguishability of Encryptions (IND-ENC)

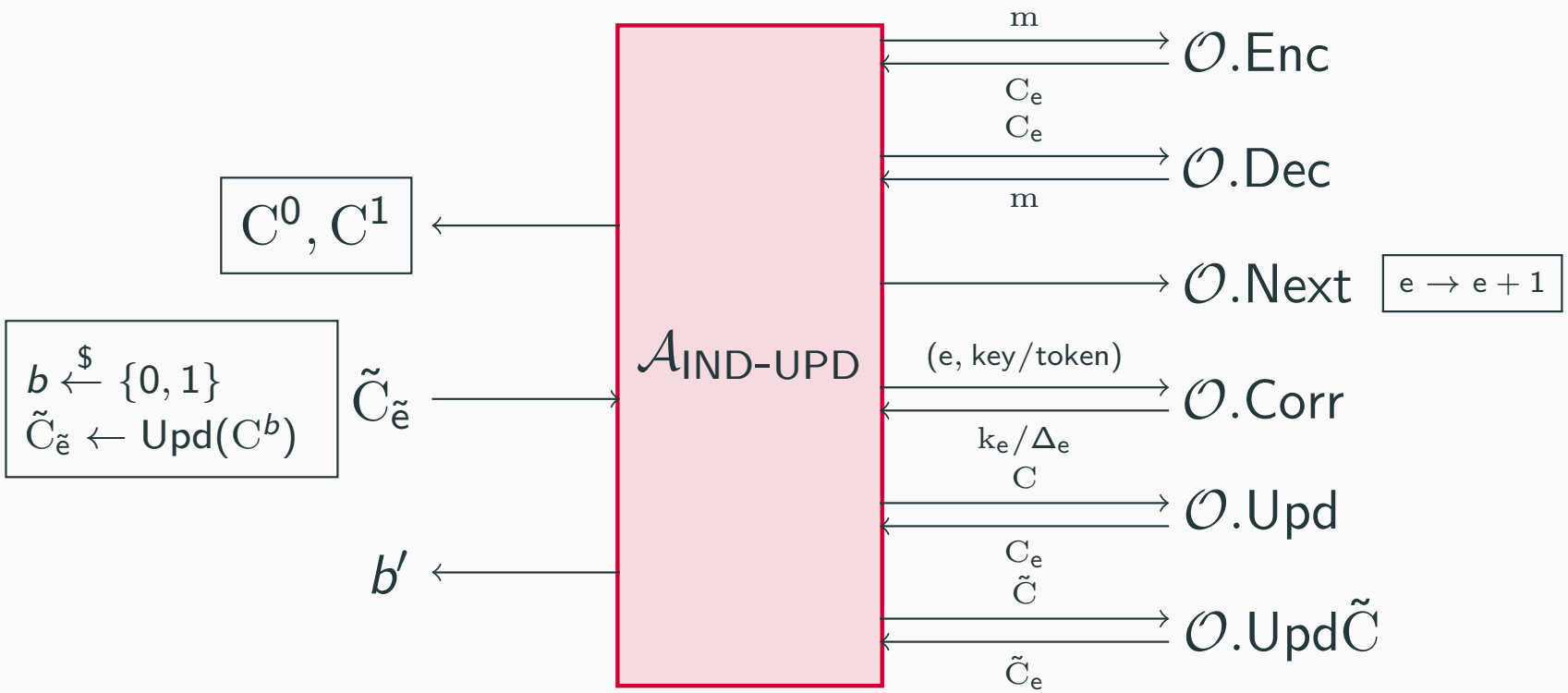


- Challenger checks for trivial wins

Only in CCA games does an adversary have access to $\mathcal{O}$.Dec

- **Updatable Encryption with Post-Compromise Security**
  Lehmann, Tackmann; Eurocrypt '18

Prior notions: Indistinguishability of Updates (IND-UPD)



- Challenger checks for trivial wins

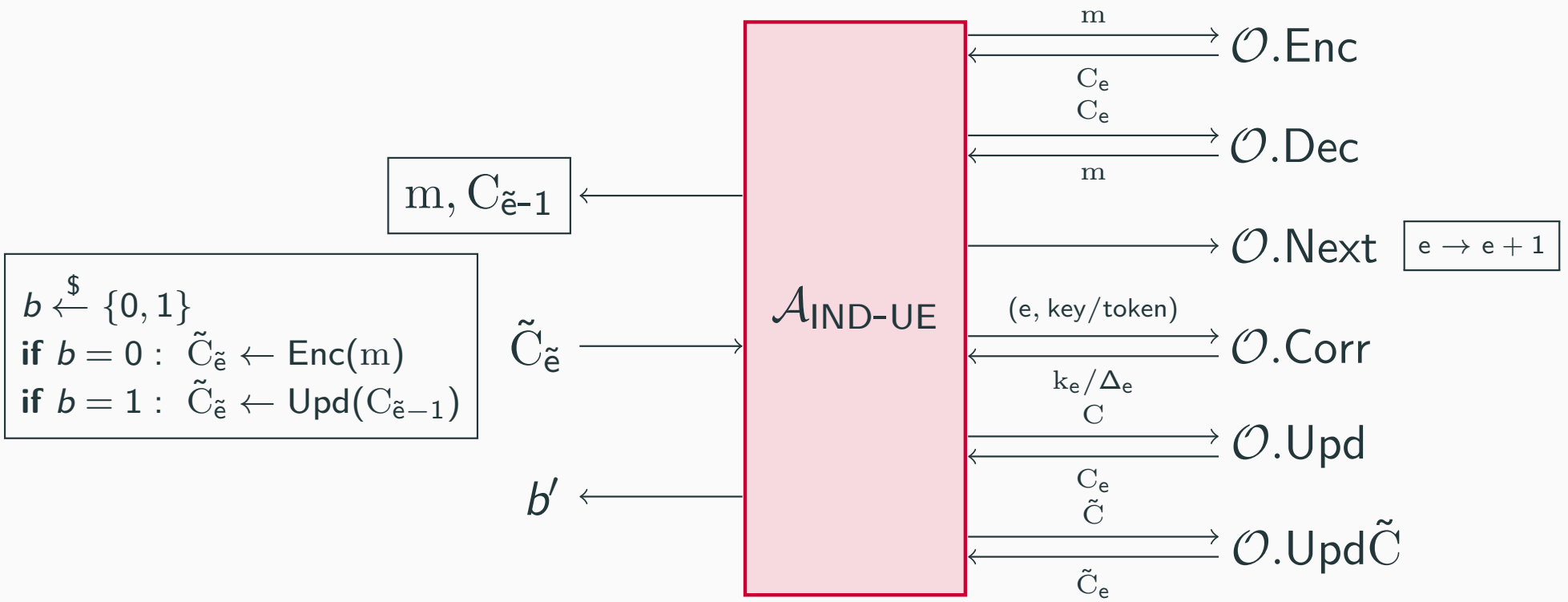
Only in CCA games does an adversary have access to $\mathcal{O}$.Dec

- **Updatable Encryption with Post-Compromise Security**
  Lehmann, Tackmann; Eurocrypt '18

What else do we want to achieve?

- None of the prior notions capture our journalist motivating example.
- Can we find a notion captures a ciphertext freshly created is indistinguishable from an updated ciphertext?

A New Notion for Updatable Encryption (IND-UE)



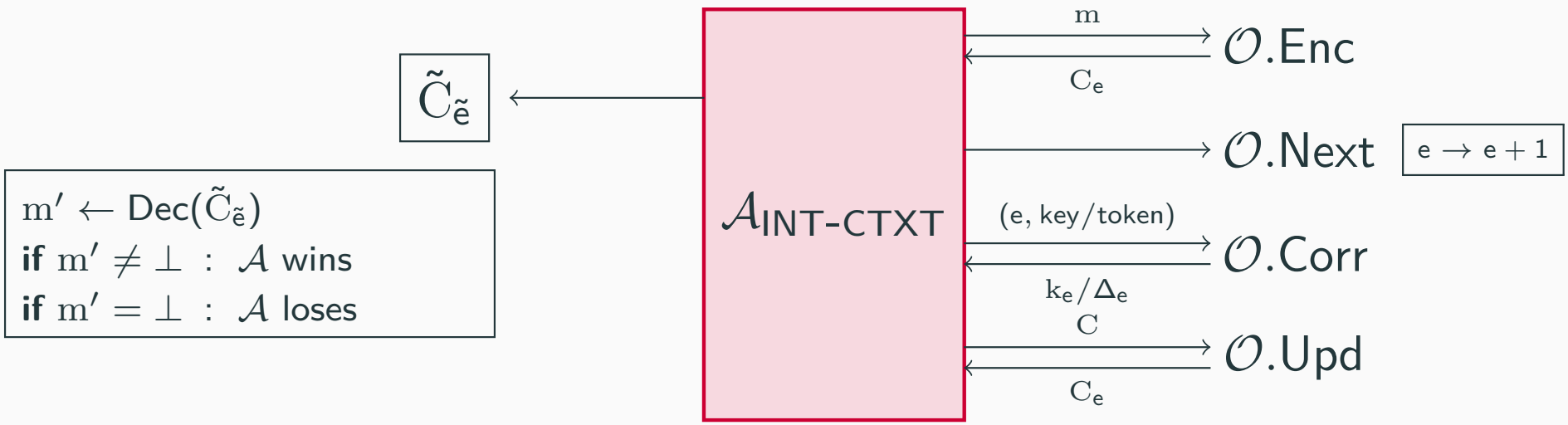
- Challenger checks for trivial wins

Only in CCA games does an adversary have access to $\mathcal{O}$.Dec

Scheme that leaks epoch number of original upload can be IND-ENC **and** IND-UPD **but not** IND-UE

IND-ENC + IND-UPD $\not\Rightarrow$ IND-UE

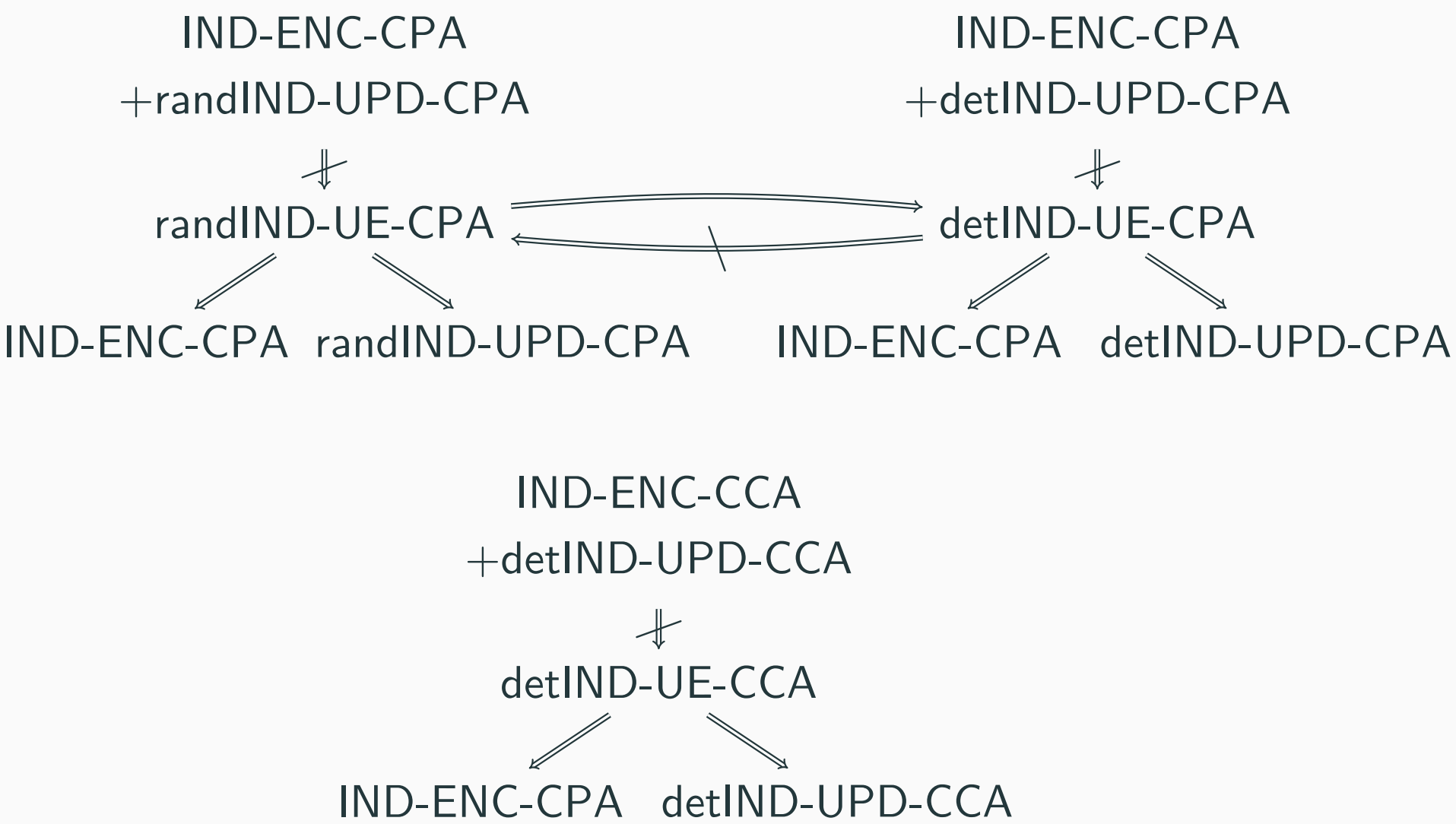
Ciphertext integrity



- Challenger checks for trivial wins*
- CPA + CTXT $\implies$ CCA?
  - **(R)CCA secure updatable encryption with integrity protection**
    Klooß, Lehmann and Rupp; Eurocrypt '19

Relations

Relations among IND-ENC, IND-UPD and IND-UE



Relations among CPA, CTXT and CCA

$\mathsf{CPA} + \mathsf{CTXT} \implies \mathsf{CCA}$ **for UE**

$\mathsf{IND\text{-}ENC\text{-}CPA} + \mathsf{INT\text{-}CTXT} \implies \mathsf{IND\text{-}ENC\text{-}CCA}$

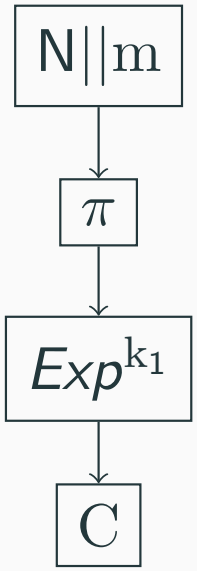
$\det \mathsf{IND\text{-}UPD\text{-}CPA} + \mathsf{INT\text{-}CTXT} \implies \det \mathsf{IND\text{-}UPD\text{-}CCA}$

$\det \mathsf{IND\text{-}UE\text{-}CPA} + \mathsf{INT\text{-}CTXT} \implies \det \mathsf{IND\text{-}UE\text{-}CCA}$

UE Constructions

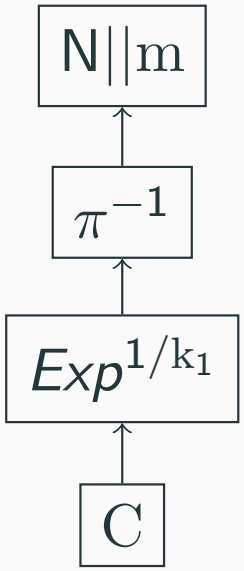
Secure Homomorphic Ideal-cipher Nonce-based Encryption (SHINE)

SHINE.Enc :



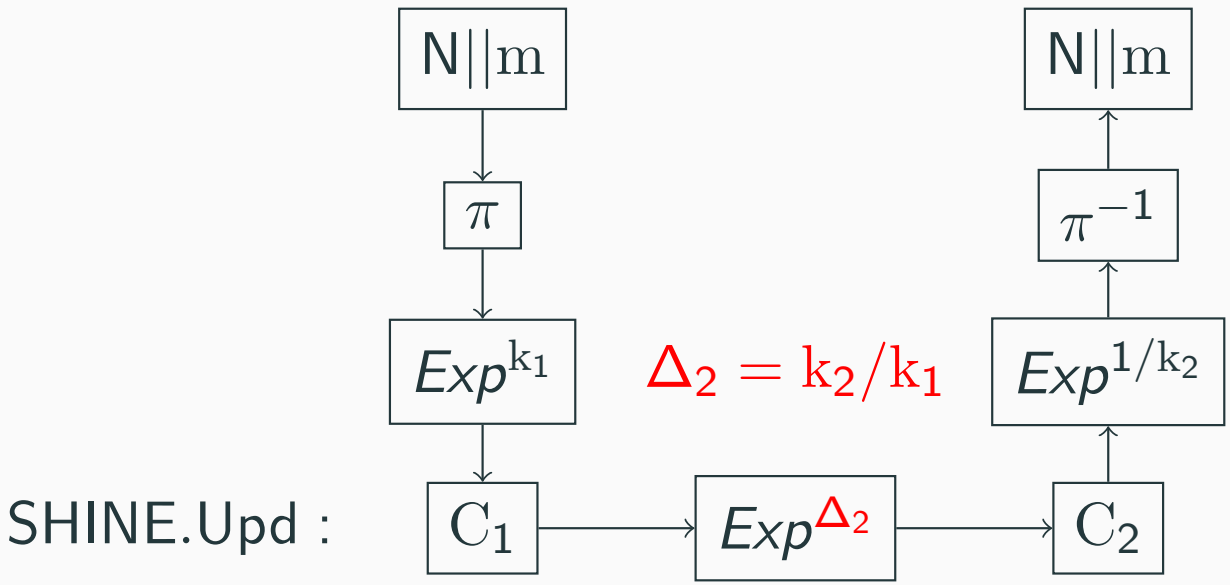
$$C = \pi(N||m)^{k_1}$$

SHINE.Dec :



$$N||m = \pi^{-1}(C^{1/k_1})$$

Secure Homomorphic Ideal-cipher Nonce-based Encryption (SHINE)



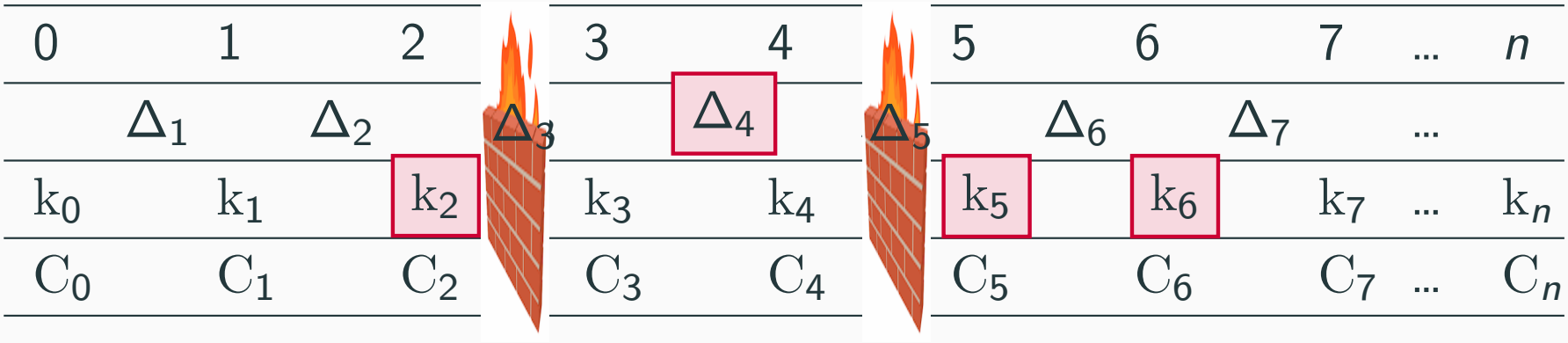
$$C_1 = \pi(N||m)^{k_1} \qquad C_2 = \pi(N||m)^{k_2}$$

OK, but is it secure?

- How can we embed the challenge, with deterministic updates and adaptive security?
- Partition epoch set into air-gapped segments ('firewalls')

- **Updatable Encryption with Post-Compromise Security**
  Lehmann, Tackmann; Eurocrypt '18
- **(R)CCA secure updatable encryption with integrity protection**
  Klooß, Lehmann and Rupp; Eurocrypt '19

Firewalls: cryptographic separation



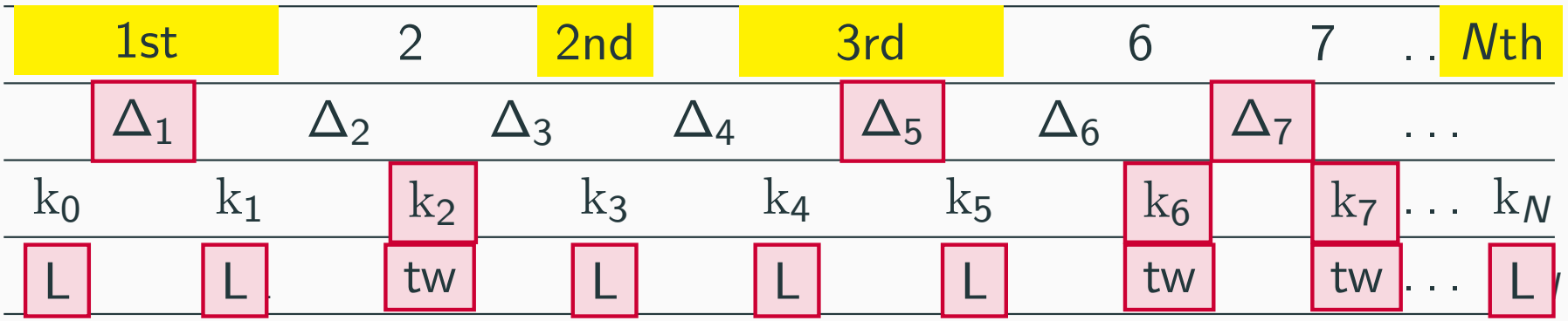
- Firewalls (insulated region) definition:
  - No key inside firewalls is corrupted
  - Tokens 'on' the firewalls are not corrupted
  - All tokens inside firewalls are corrupted
- Separate keys, tokens and ciphertexts using firewalls

OK, but is it secure?

- How can we embed the challenge, with deterministic updates and adaptive security?
- Partition epoch set into air-gapped segments ('firewalls')
- Hybrid argument across insulated regions
- Embed the challenge in the i-th insulated region.

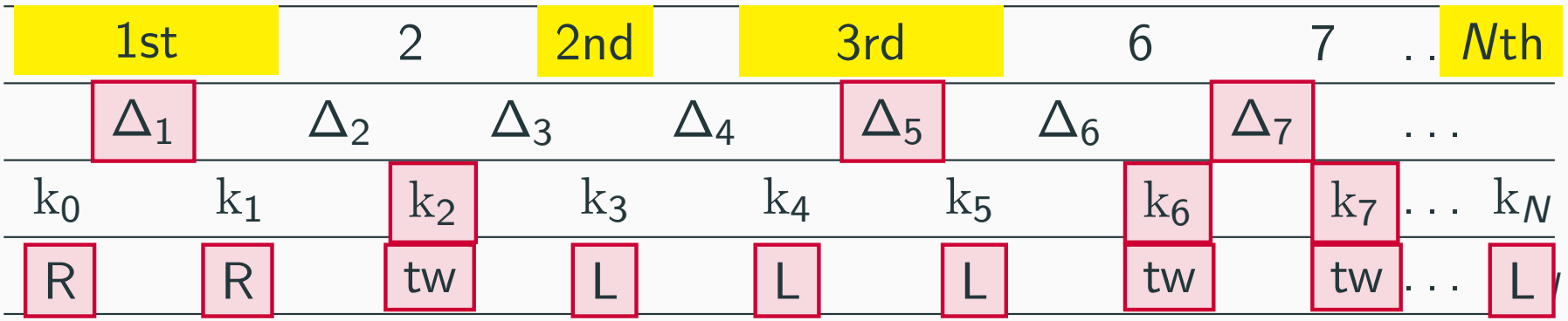
- **Updatable Encryption with Post-Compromise Security**
  Lehmann, Tackmann; Eurocrypt '18
- **(R)CCA secure updatable encryption with integrity protection**
  Klooß, Lehmann and Rupp; Eurocrypt '19

Hybrid argument across insulated regions



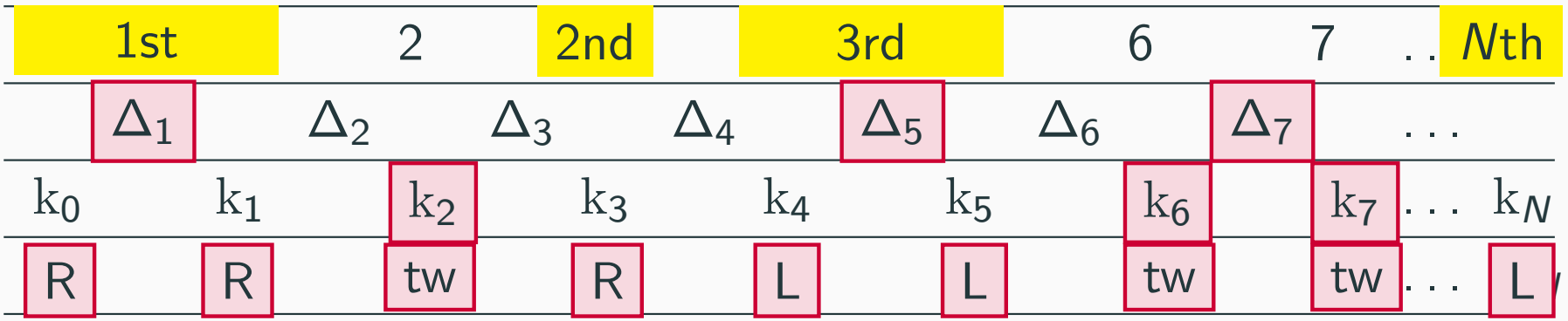
- Game 0

Hybrid argument across insulated regions



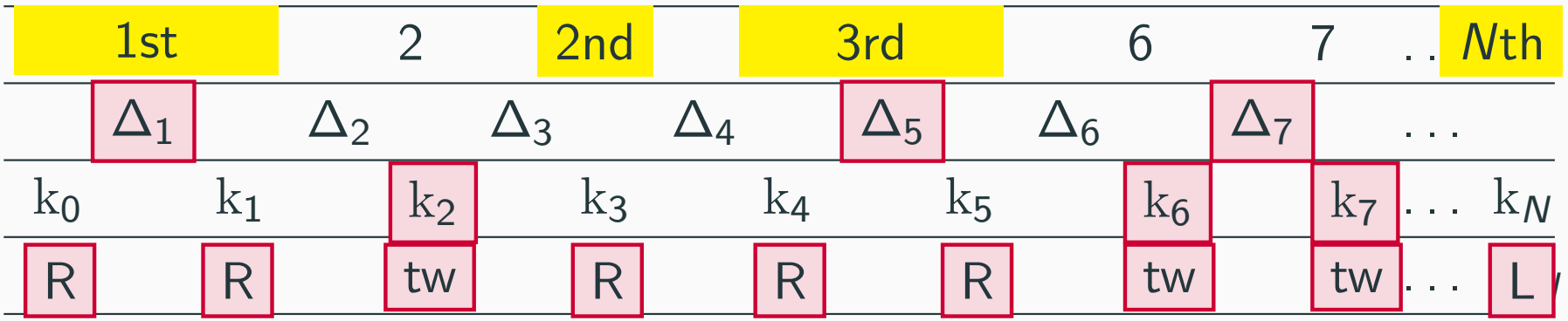
- Game 1

Hybrid argument across insulated regions



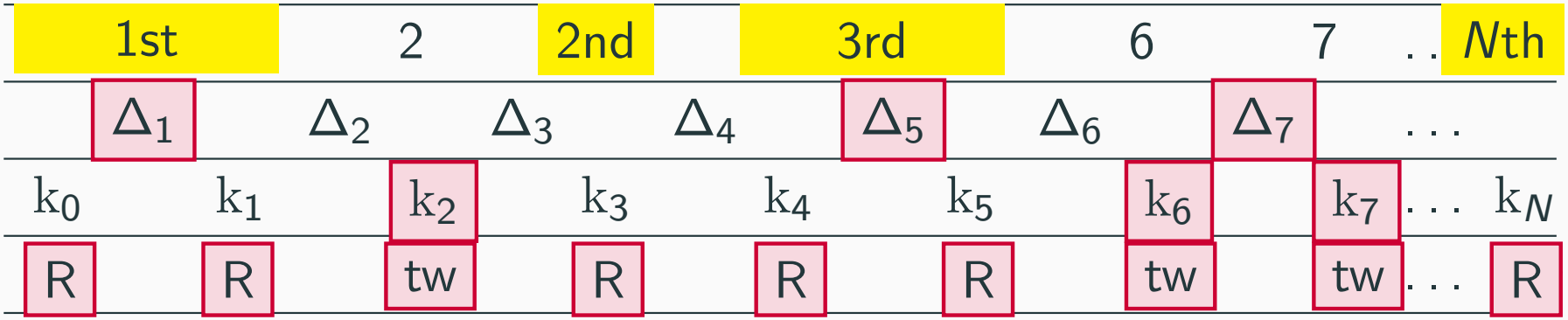
- Game 2

Hybrid argument across insulated regions



- Game 3

Hybrid argument across insulated regions



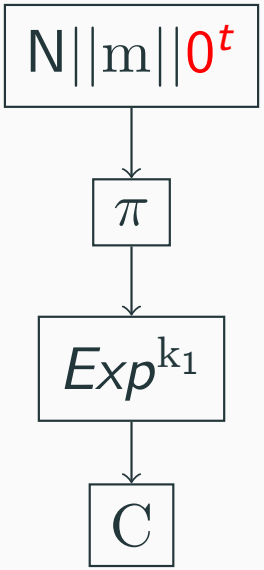
- Game N

OK, but is it secure?

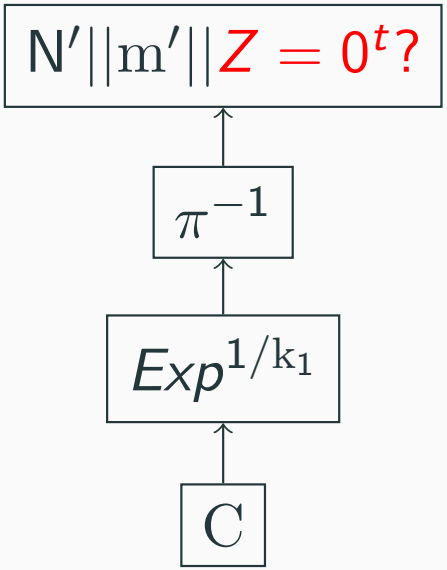
SHINE is det IND-UE-CPA Secure

Assuming DDH, and in the ideal cipher model

SHINE0.Enc :



SHINE0.Dec :



OK, but is it secure?

SHINE is det IND-UE-CPA Secure

Assuming DDH, and in the ideal cipher model

SHINE is INT-CTXT Secure

Assuming CDH, and in the ideal cipher model

SHINE is det IND-UE-CCA Secure

Assuming DDH and CDH, and in the ideal cipher model

OK, but is it secure?

	IND	INT
BLMR+	(weak,UE,CPA)	✘
RISE	(rand,UE,CPA)	✘
NYUAE	(rand, ENC, RCCA) (rand, UPD, RCCA)	PTXT
E&M	(det, ENC, CCA) (det, UPD, CCA)	CTXT
SHINE0	(det, UE, CCA)	CTXT
MirrorSHINE	(det, UE, CCA)	CTXT
OCBSHINE	(det, UE, CCA)	CTXT

(xx, yy, atk) represents the best possible xxIND-yy-atk notion that each scheme can achieve.

OK, but is it efficient?

	$\|M\|$	$\|C\|$	Enc (Upd)
BLMR+	$n\|G\|$	$(n+1)\|G\|$	nE
RISE	$1\|G\|$	$2\|G\|$	2E
NYUAE	$1\|G_1\|$	$(58\|G_1\|, 44\|G_2\|)$	(110E,90E)
E&M	$1\|G\|$	$3\|G\|$	3E
SHINE0[CPA]	$(1-\gamma)\|G\|$	$1\|G\|$	1E
SHINE0	$(1-2\gamma)\|G\|$	$3\|G\|$	3E
MirrorSHINE	$(1-\gamma)\|G\|$	$2\|G\|$	2E
OCBSHINE	$n\|G\|$	$(n+2)\|G\|$	$(n+2)$E

E = Exponentiation

γ represents the bit-size of the used nonce as a proportion of the group element bit-size.

BLMR+ and OCBSHINE support encryption of arbitrary size messages (of n blocks), with $|M| \approx n|G|$.

Summary

Summary

- New notion, IND-UE, that implies past notions
- Generic composition result
- New scheme, SHINE, that meets detIND-UE-CCA and INT-CTXT
- A greater understanding of the proof techniques
  - in particular in the context of deterministic updates

Thank you for your attention!

Questions?

The Research Council of Norway

NTNU
Norwegian University of Science and Technology

BERGISCHE UNIVERSITÄT WUPPERTAL