Massachusetts Institute of Technology

HATSOPOULOS MICROFLUIDS LABORATORY

Robust and Small Key-Size Image Encryption and Decryption Using Time Reversible Stokes Flow

2.29 Numerical Fluid Mechanics Course Project

Jianyi Du

Living in A Transparent World

- Privacy violation in the world
  - Facebook
  - Equifax
  - PRISM
- Can pure digital encryption fully protest us?

venturebeat.com

Scytale in the ancient Greeks. westfieldnj.com.

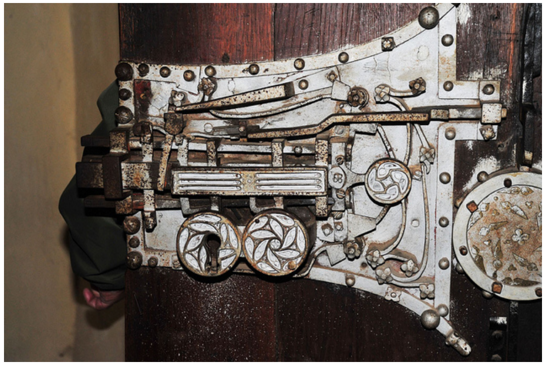
Enigma I. cryptomuseum.com.

democraticunderground.com

Bitcoins. forbes.com

Elements of Cryptography

- A complete encryption/decryption process: enciphering, key, and deciphering
- An analogy to a door:



Complex lock. flickrs.com

Enciphering:
a complex lock structure

illustrationsource.com.

Key:
space to save the method

Rbaofli.com.

Deciphering:
efforts to open with or without (violation) keys

A high safety encryption can be a trade-off of:

- Complex enciphering: stream cipher, quantum ciphering
- Large key-size: methods with perfect secrecy
- Deciphering: efficiency or safety (brute-force)

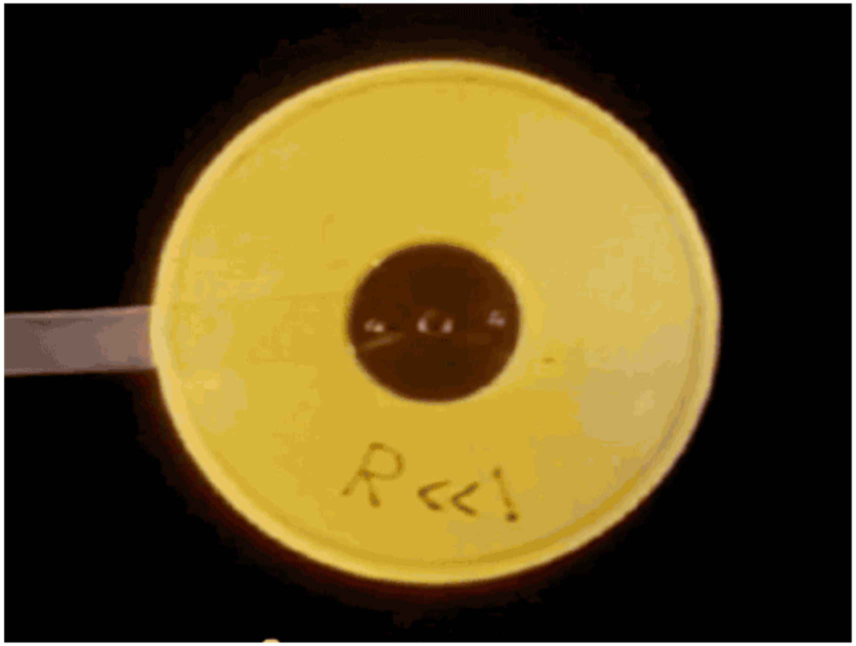
Patel, Komal D., and Sonal Belani. 2011.

Can Nature Help with Enciphering?

- We need a reversible process that cannot be easily broken by brute-force attack, or with a huge number of possible states, at the same time easy to perform the encryption and decryption
- **Ask Nature!**

Stokes flow of Newtonian fluids with time reversibility!

- Inspired to be used for en-/deciphering: image pixels as particle tracers



reddit.com.

Algorithm Overview

- Enciphering: analogy to **Lid Cavity Problem** with Stokes flow

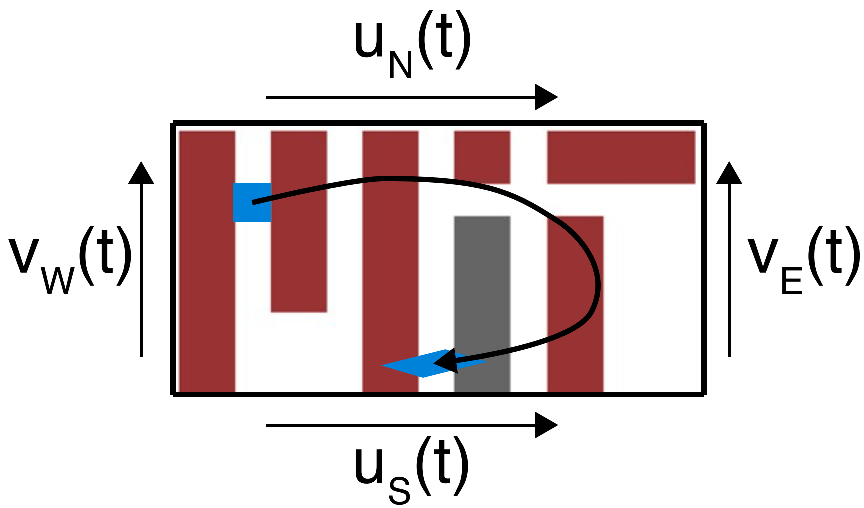
Governing equation: $$0 = -\boldsymbol{\nabla} p + \mu \nabla^2 \boldsymbol{v}$$

Particle tracing: $$\frac{D\phi(x,y)}{Dt} = \boldsymbol{\nabla} \cdot (\phi \boldsymbol{v}) = 0$$

- ϕ: pixel information of the image, can be either a number between 0 and 1 (grayscale) or a 3-value array (RGB/HSV).

Enciphering

$$\mathbf{v_e(0<t<T)} = \begin{bmatrix} u_N(t) \\ u_E(t) \\ v_S(t) \\ v_W(t) \end{bmatrix}$$



Deciphering

$$\mathbf{v_d(t) = -v_e(T-t)}$$

Stage 1: Solving Governing Equation

- With the NS solver provided in 2.29 class
- **Project methods**:

<u>Non-incremental form</u>

$$\left[\frac{I}{\Delta t} - \nu\nabla^2\right]\tilde{\boldsymbol{u}}^{k+1} = \frac{\boldsymbol{u}^k}{\Delta t} + \boldsymbol{F}^{k+1}$$

where $\boldsymbol{F}^{k+1} = -\boldsymbol{\nabla}\cdot(\boldsymbol{u}\boldsymbol{u})^{k+1} + \boldsymbol{\nabla}\cdot\boldsymbol{\tau}^{k+1}$

$$\nabla^2 P^{k+1} = \frac{1}{\Delta t}\boldsymbol{\nabla}\cdot\tilde{\boldsymbol{u}}^{k+1}$$

$$\boldsymbol{u}^{k+1} = \tilde{\boldsymbol{u}}^{k+1} - \Delta t\boldsymbol{\nabla}P^{k+1}$$

<u>Incremental form</u>

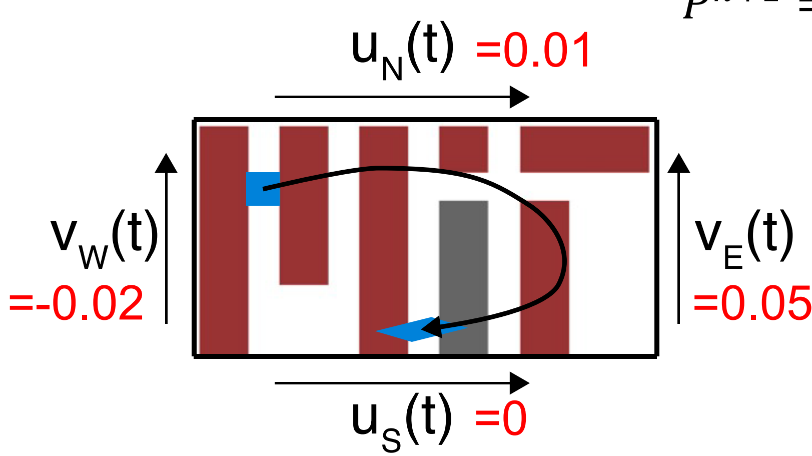
$$\left[\frac{I}{\Delta t} - \nu\nabla^2\right]\tilde{\boldsymbol{u}}^{k+1} = \frac{\boldsymbol{u}^k}{\Delta t} - \boldsymbol{\nabla}P^k + \boldsymbol{F}^{k+1}$$

where $\boldsymbol{F}^{k+1} = -\boldsymbol{u}^k\cdot\boldsymbol{\nabla}\boldsymbol{u}^k$

$$\nabla^2\left(q^{k+1}\right) = \frac{1}{\Delta t}\boldsymbol{\nabla}\cdot\tilde{\boldsymbol{u}}^{k+1}$$

$$\boldsymbol{u}^{k+1} = \tilde{\boldsymbol{u}}^{k+1} - \Delta t\boldsymbol{\nabla}q^{k+1}$$

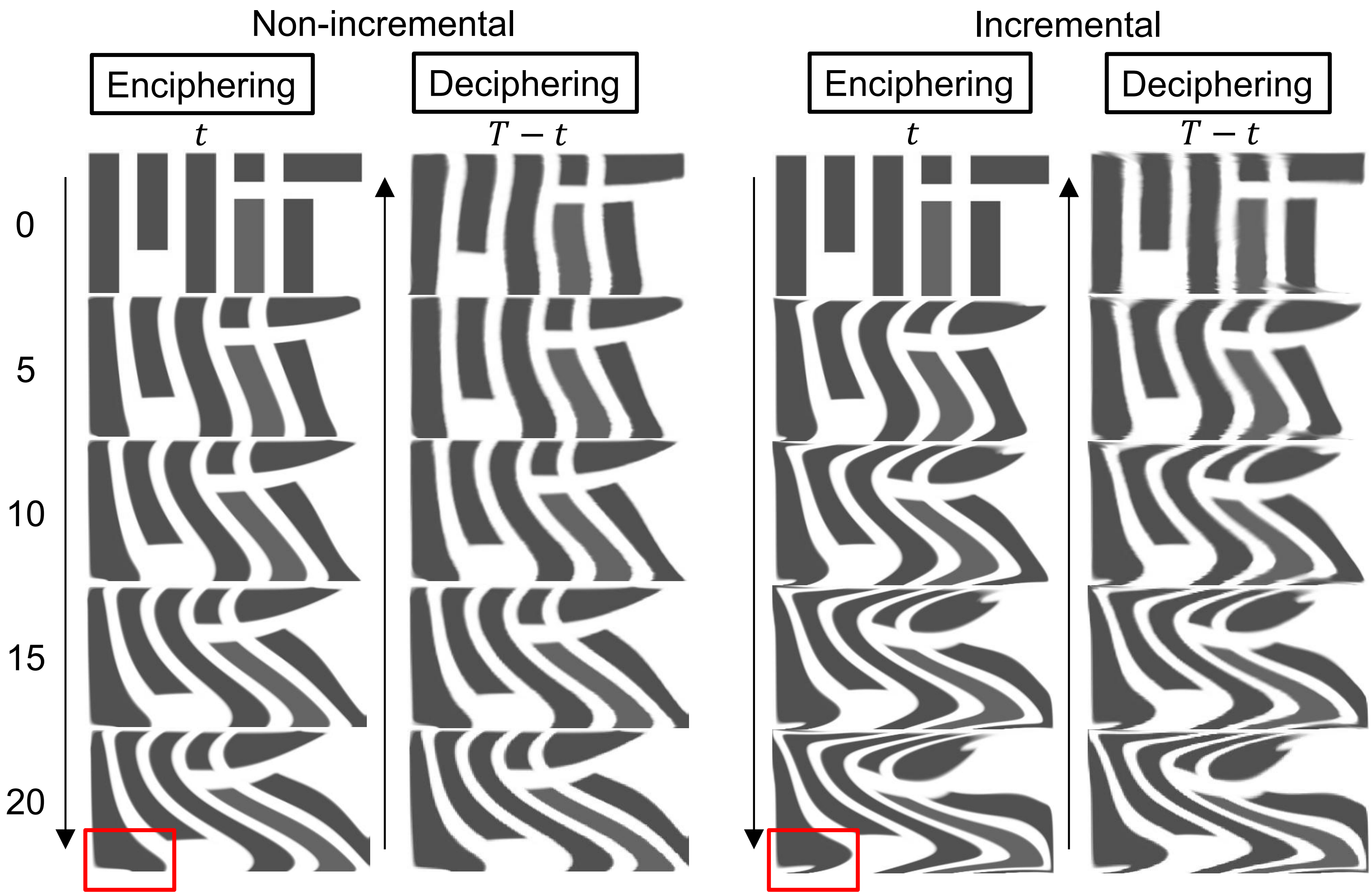
$$P^{k+1} = q^{k+1} + P^k - \nu\boldsymbol{\nabla}\cdot\tilde{\boldsymbol{u}}^{k+1}$$



$$\Delta t = 0.02,\ T = 20$$

Guermond and Minev. 2006.

Test numerical diffusion



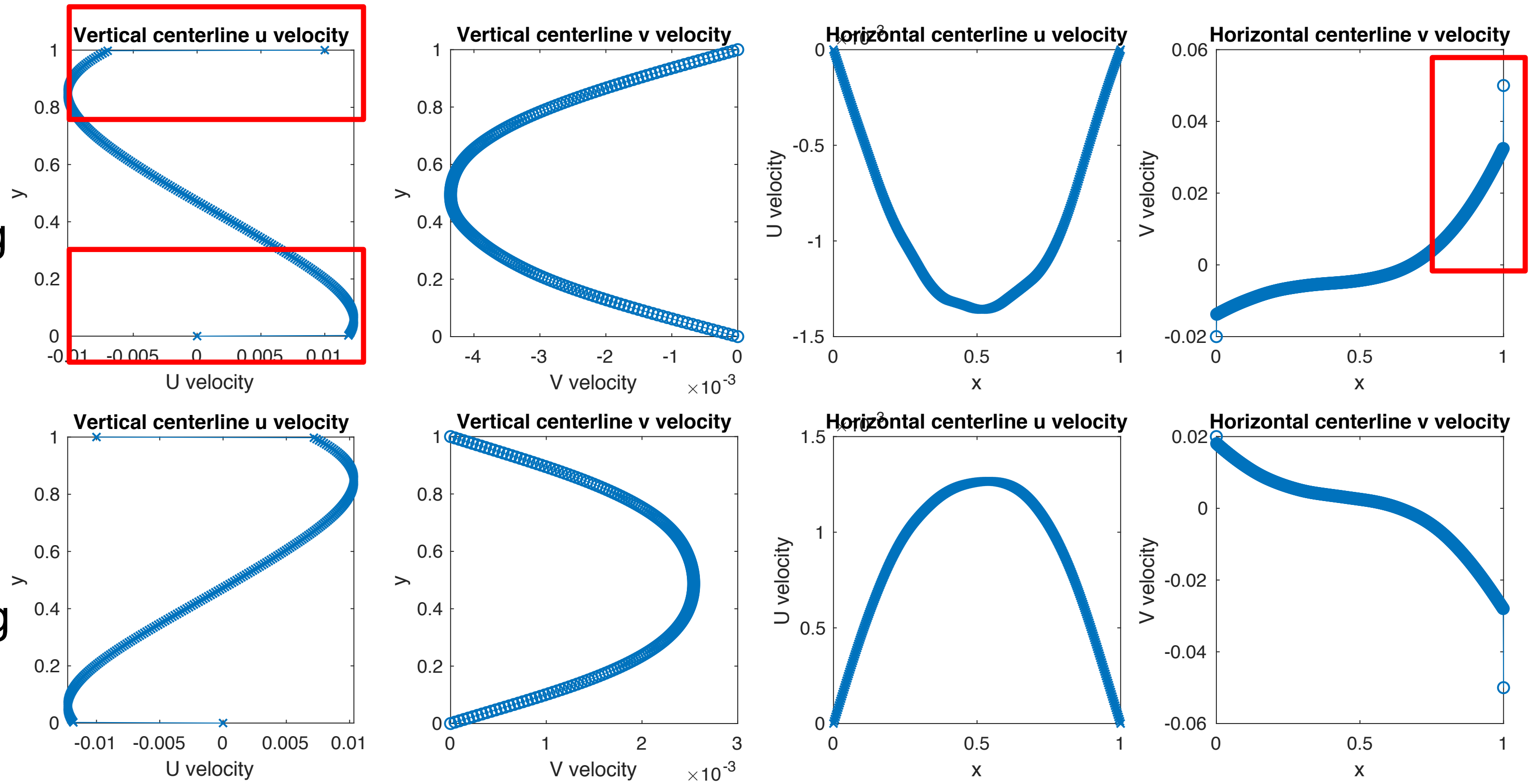
$\Delta t = 0.01,\ T = 20$

Incremental v. Non-Incremental

- Check the boundary conditions

t = 20 Enciphering

t = 20 Deciphering



Non-incremental

- Wall slip is observed, leading to less fidelity in velocity reversibility
  - No pressure term is used in momentum equation, which incorporates the boundary informations

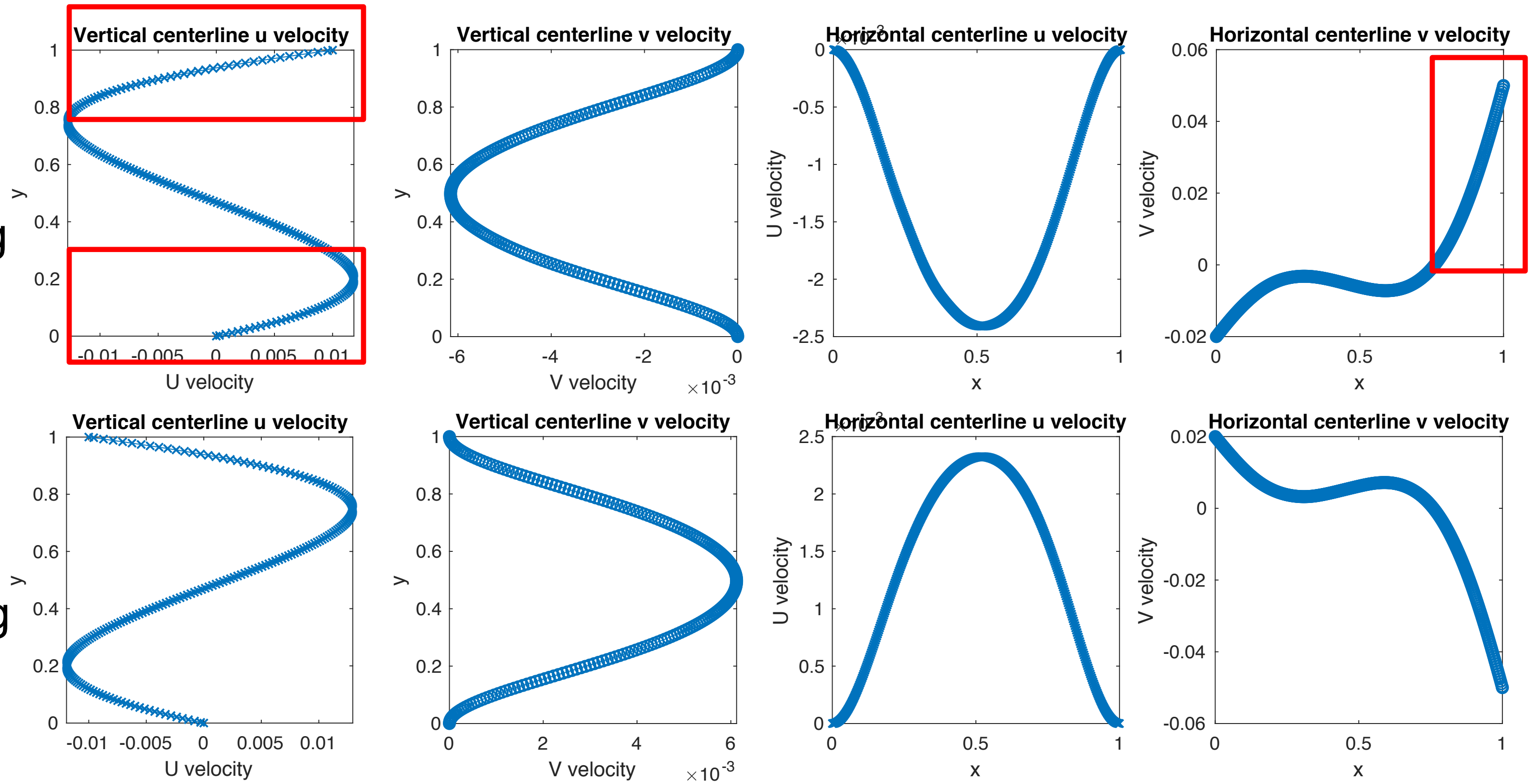
Massachusetts Institute of Technology

Incremental v. Non-Incremental

HATSOPOULOS MICROFLUIDS LABORATORY

t = 20
Enciphering

t = 20
Deciphering



Incremental

- Incremental scheme leads to well control ed boundary conditions since the momentum equation contains pressure term
  - Pressure is further corrected by the velocity

Stage 2: Advection Scheme

- New Advection method needed
  - LeVeque 1996: 2D flux-limited advection method

Step 1: Upwind scheme

$$F^{UW}_{i-\frac{1}{2},j} = U_{i-\frac{1}{2},j}\phi_U$$

Step 2: Upwind scheme with transverse propagation (CTU method)

- Pink region should not belong to the flux

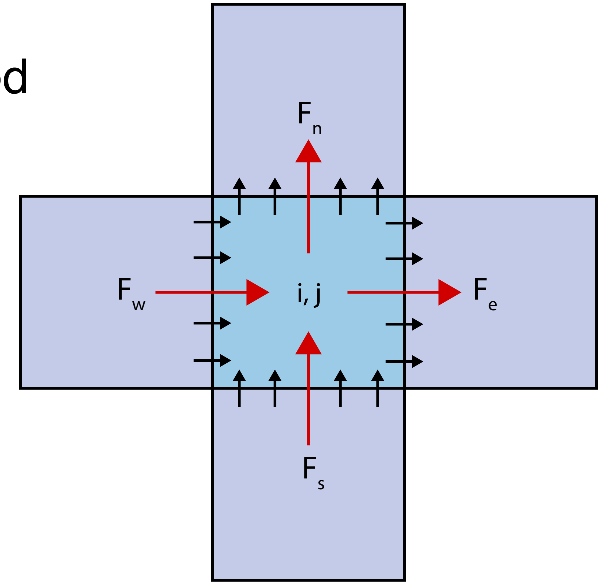
$$F^{CTU}_{i,j+\frac{1}{2}} = F^{UW}_{i,j+\frac{1}{2}} - \frac{\Delta t}{2\Delta x}uv(\phi_{i,j} - \phi_{i-1,j})$$

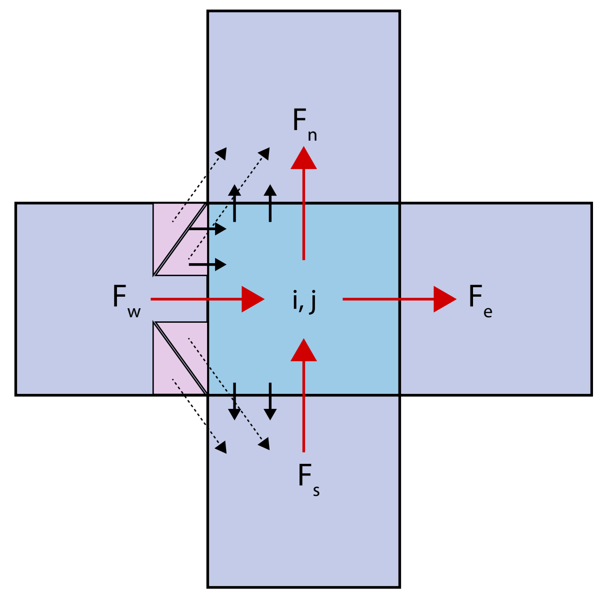
Step 3: Add Flux-Limiter

$$F^{FL}_{i+\frac{1}{2},j} = F^{CTU}_{i+\frac{1}{2},j} + \frac{|u|}{2}\left(1 - |u|\frac{\Delta t}{\Delta x}\right)C(r_{i-\frac{1}{2},j})R$$

where $R = \phi_{i,j} - \phi_{i-1,j}$

$$r_{i-\frac{1}{2},j} = (\phi_{i-1,j} - \phi_{i-2,j})/R$$

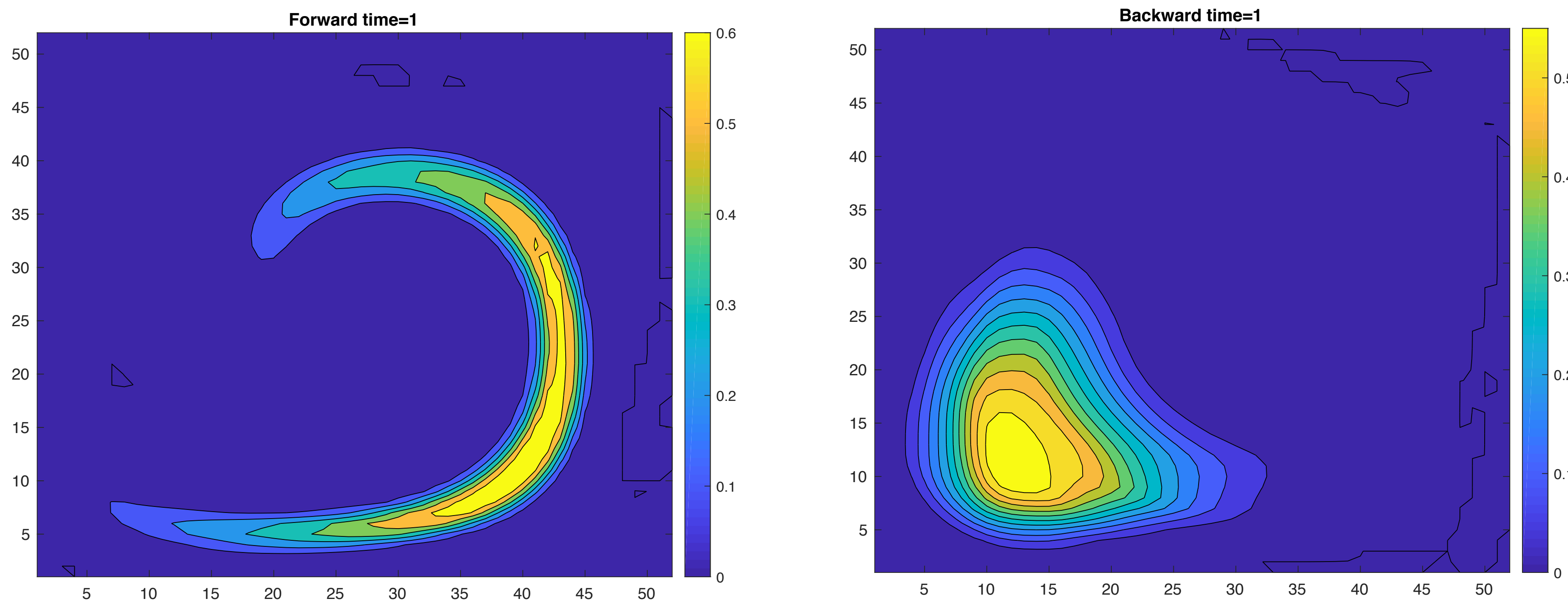




LeVeque. 1996.
Durran, Numerical Methods for Fluid Dynamics. 2nd ed.

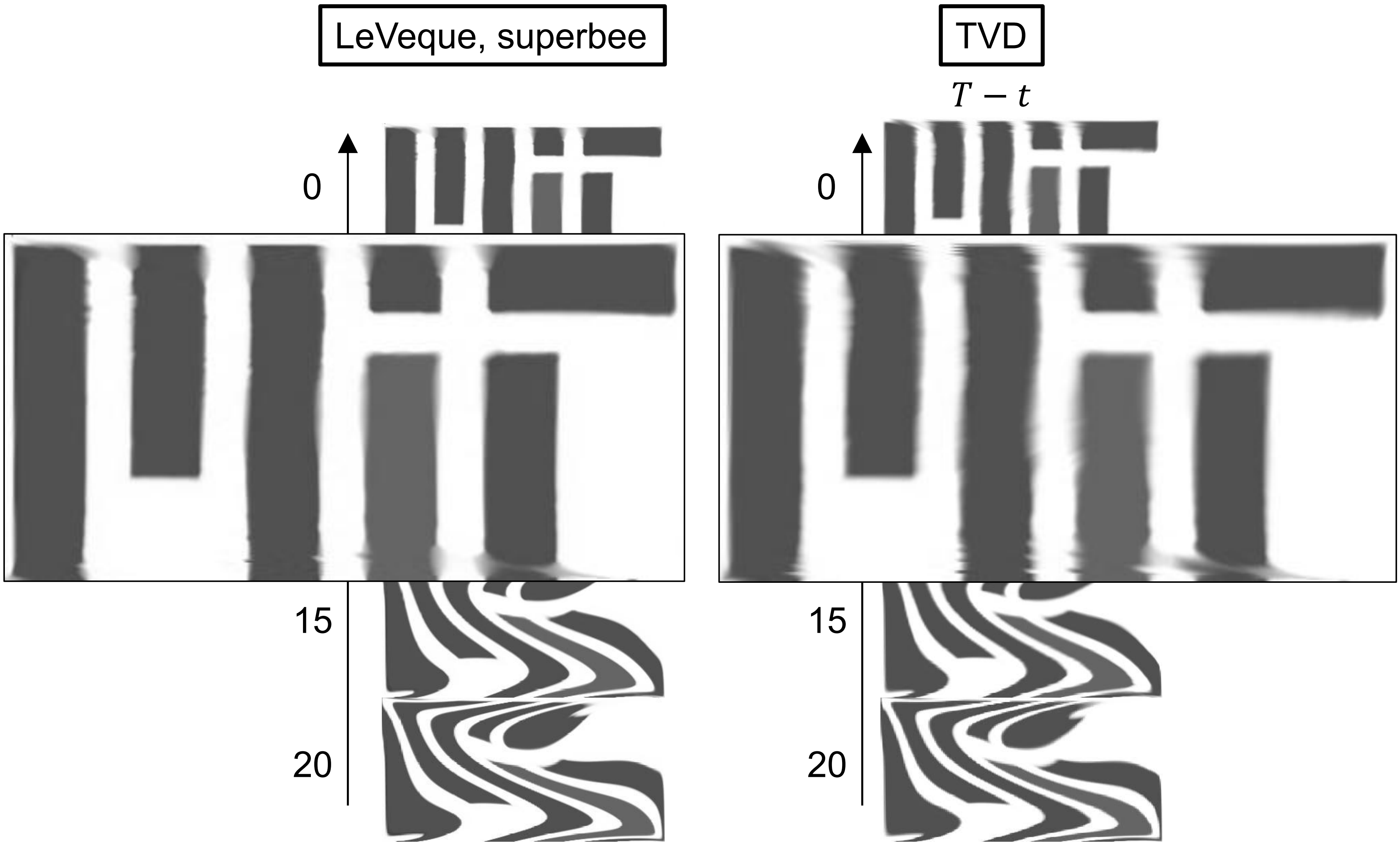
Swirling Test

- $C(r)$: scalar functions of flux limiter to keep the total variation diminishing
- Test the scheme with a proposed method
  - Lax-Wendroff: C(r)=1
  - Minmod: C(r)=max(0, min(1, r))
  - Superbee: C(r)=max(0, min(1, 2r), min(2, r))
  - Van Leer: C(r)=(r+|r|)/(1+|r|)



LeVeque. 1996.
Durran, Numerical Methods for Fluid Dynamics. 2nd ed.

Implementation on MIT



LeVeque. 2006.

Evaluation of the Protocol

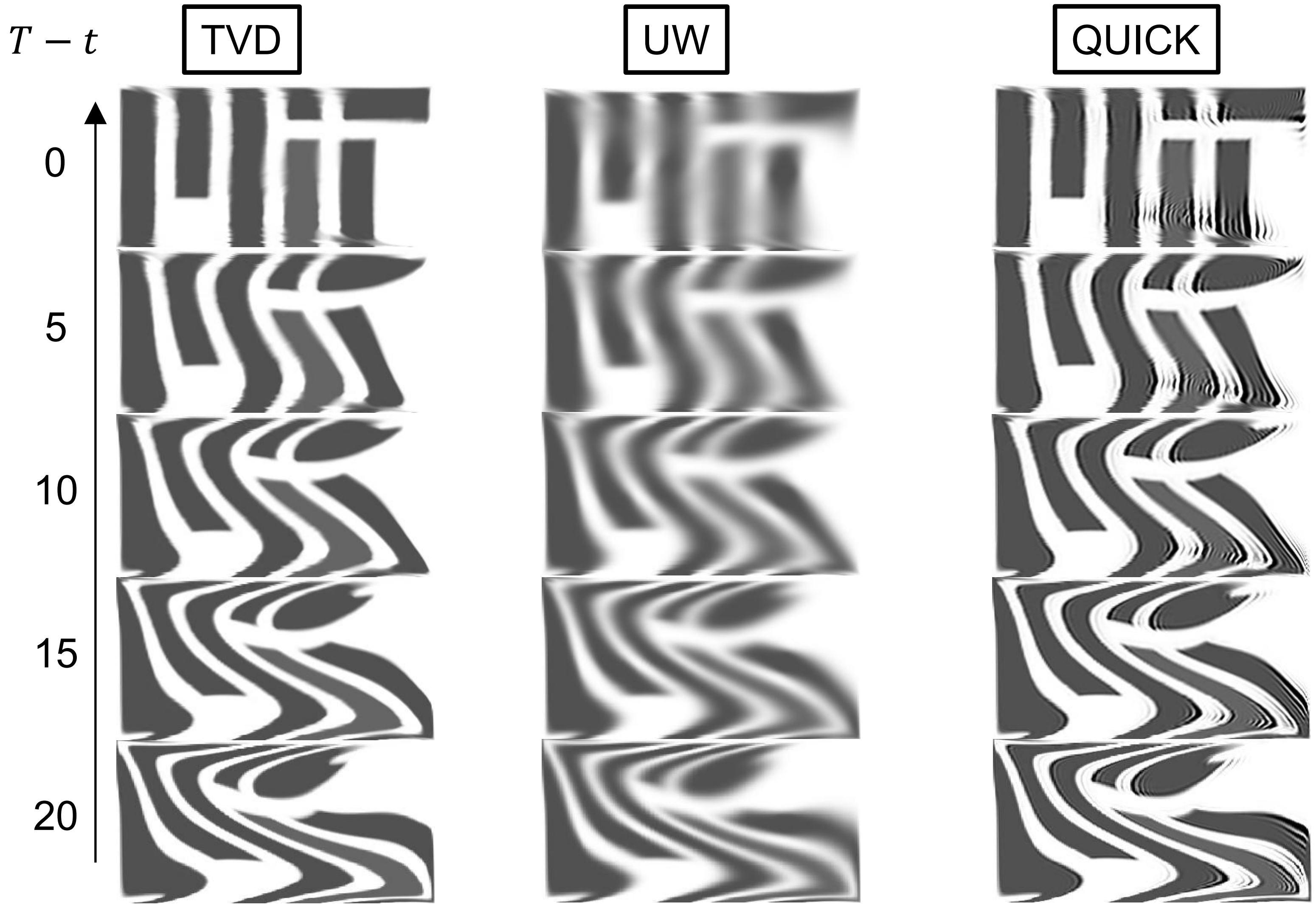
- The Stokes flow encryption has the following advantages:
  - Encryption from nature: Efficient enciphering or deciphering process with only solving the NS equation
    - Independent of the image information, so can be pre-calculated!
  - Key: small key size with only the boundary conditions
  - Safety:
    - Flow itself is rather a random process, introducing a large number of possible states by altering a little bit in boundary conditions
    - Easy to add complexity to the ciphering structure by just adding noise to the original image
- Limitations
  - Time of particle advection calculation scales up with image size:
    - A large image (1000 x 2000) can take about 20 mins to en-/decipher
  - Information is only repositioned, but not substituted (encoded)
  - Still room for accuracy

A Demo

- An RGB image: individual encryption of three layers

Thank you!

Advection Schemes



- Numerical diffusion is key to image resolution
  - A more accurate advection scheme is needed