# GPU implementation of RC6 cryptographic algorithm

Ke Jiang
ESLAB, IDA

# Questions

1. Give at least two methods or technologies to make computer systems more secure.

2. RC6 is a _____–key cryptography. Please name another algorithm belonged to the same category.

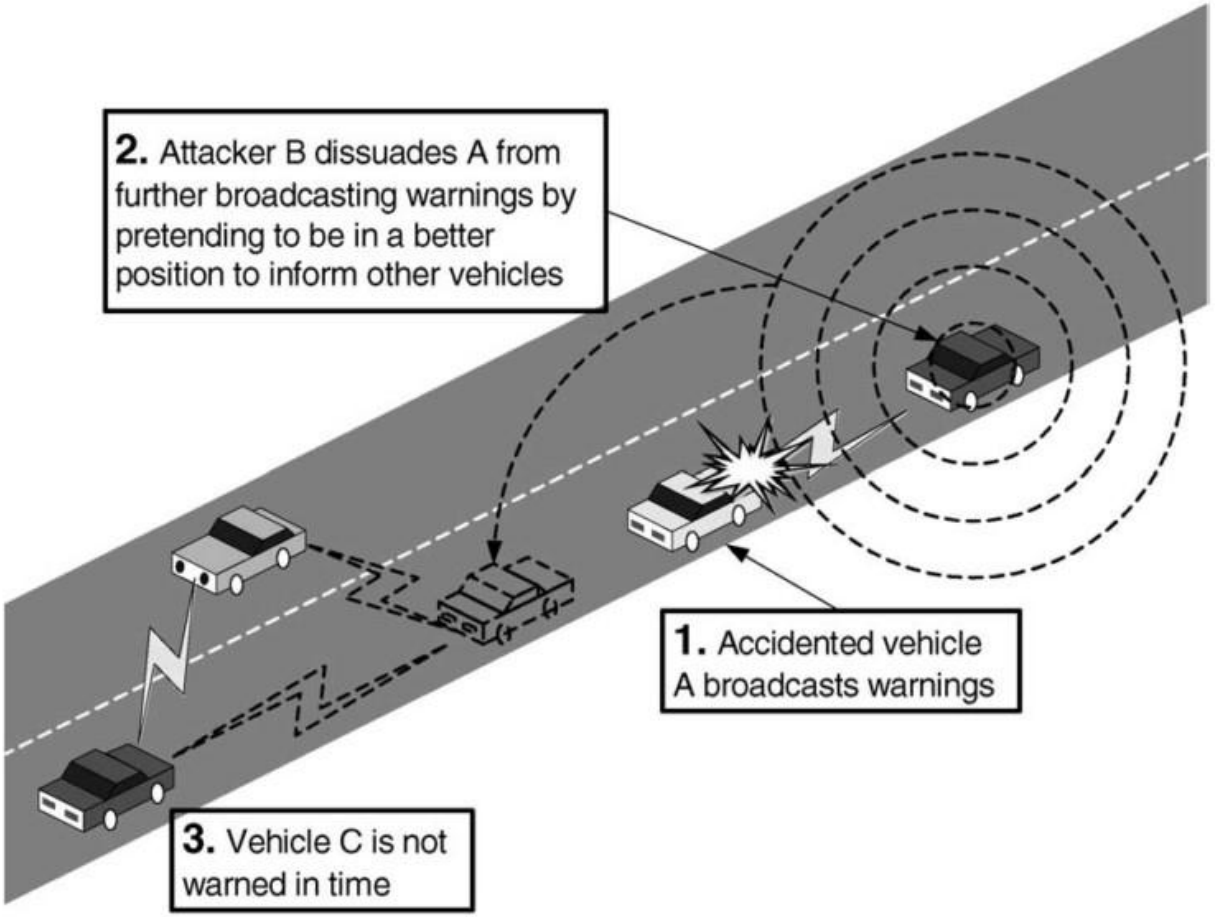
3. Can we do parallel computation within each encryption/decryption process? If yes, please state how we can do that. If no, please explain the reason briefly.

# 1. Why Security?

- Brief history
  - Julius Caesar invented Caesar Cipher around 30 B.C.
  - World War II (Allies v.s. Axis)
  - Internet
  - Automobiles?
    - IT systems in automobiles
    - Systems are becoming more and more complex
    - Privacy of the driver
    - Sensitive information
    - Vehicles are being connected

# 1. Why Security?

- Automobile attack example 1



# 1. Why Security?

- Automobile attack example 2


# 2. How to be more secure?

- Methods
  - Security level classification
  - Authentication
  - Access control
  - Information confusion and diffusion
  - ...
- Techniques
  - Cryptography – A fundamental step
  - Digital signature
  - Message digest
  - ...

# 3. Cryptography

- Used everywhere around us now
- Classification
  - Symmetric-key cryptography
    - Block ciphers: DES, AES(Rijndael), RC6, ...
    - Stream ciphers: Vigenère cipher, RC4, …
  - Public-key cryptography
    - Integer factorization problem: RSA
    - Discrete logarithm problem: DSA(Digital Signature Algorithm)
    - Elliptic curves: ECC(Elliptic Curve Cryptography)
  - Cryptographic hash functions
    - MD5, SHA-1

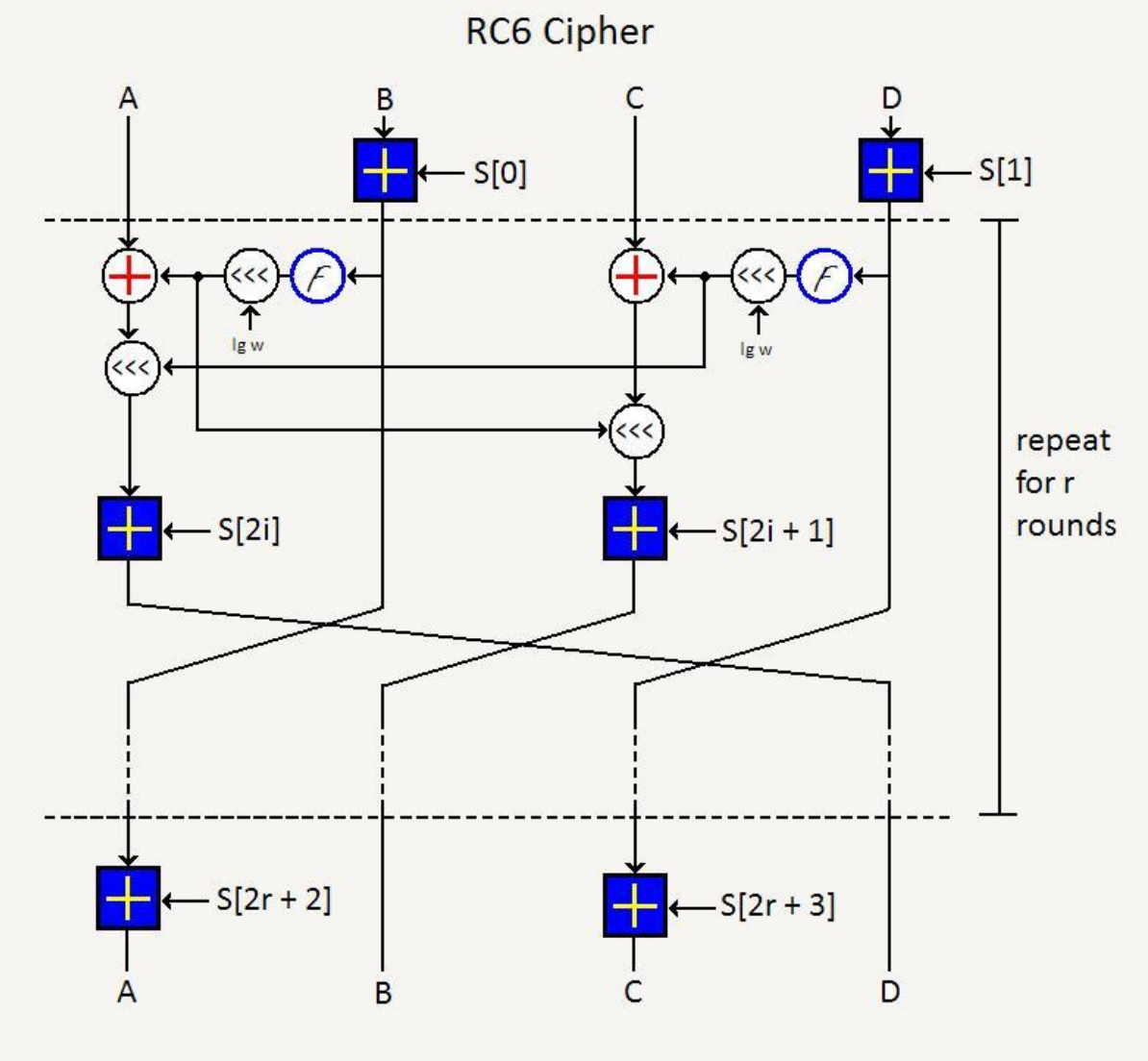
# 4. Why RC6 in automobiles?

- ✓Attractive and clean simplicity
- ✓Extremely flexible
  - ✓Resource constraints
- ✓Very fast in software implementation
  - ✓We do not change the hardware of the automotive IT systems
- ✓Sufficient strength

# 5. RC6

- RC6-w/r/b
  - Word size is w(4 bytes)
  - Number of rounds is r (20 rounds as standard)
  - Length of the key is b bytes (16, 24, 32 bytes as standard)
- Basic operations
  - $a + b$
  - $a - b$
  - $a \oplus b$
  - $a \times b$
  - $a \lll b$
  - $a \ggg b$
- Procedure

# 5. RC6


RC6 Cipher
A
B
C
D
S[0]
S[1]
lg w
lg w
S[2i]
S[2i + 1]
repeat
for r
rounds
S[2r + 2]
S[2r + 3]
A
B
C
D

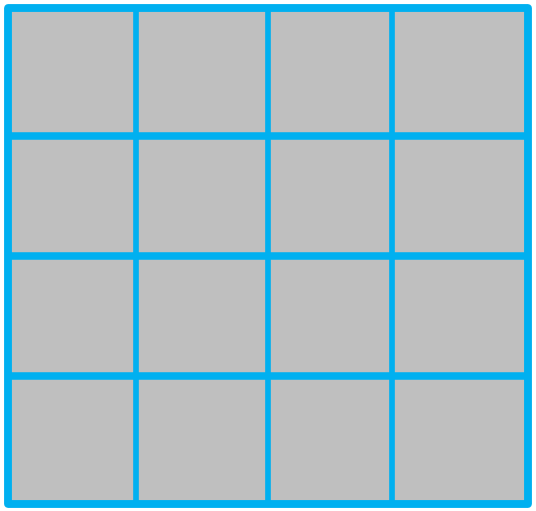
# 6. Platform

- CPU: Intel Xeon W3520, Quad-Cores, 2.66 GHz, 8 MB cache
- GPU: NIVDIA Quadro NVS 295, 8 cores, 256 MB
- Memory: 8 GB 1333 MHz DDR3
- OS: Ubuntu 9.10 x64
- CUDA Toolkit v2.3, 64-bit

# 7. Parallel computation

- What to parallel?
  - The encryption/decryption process?
  - The whole procedure?

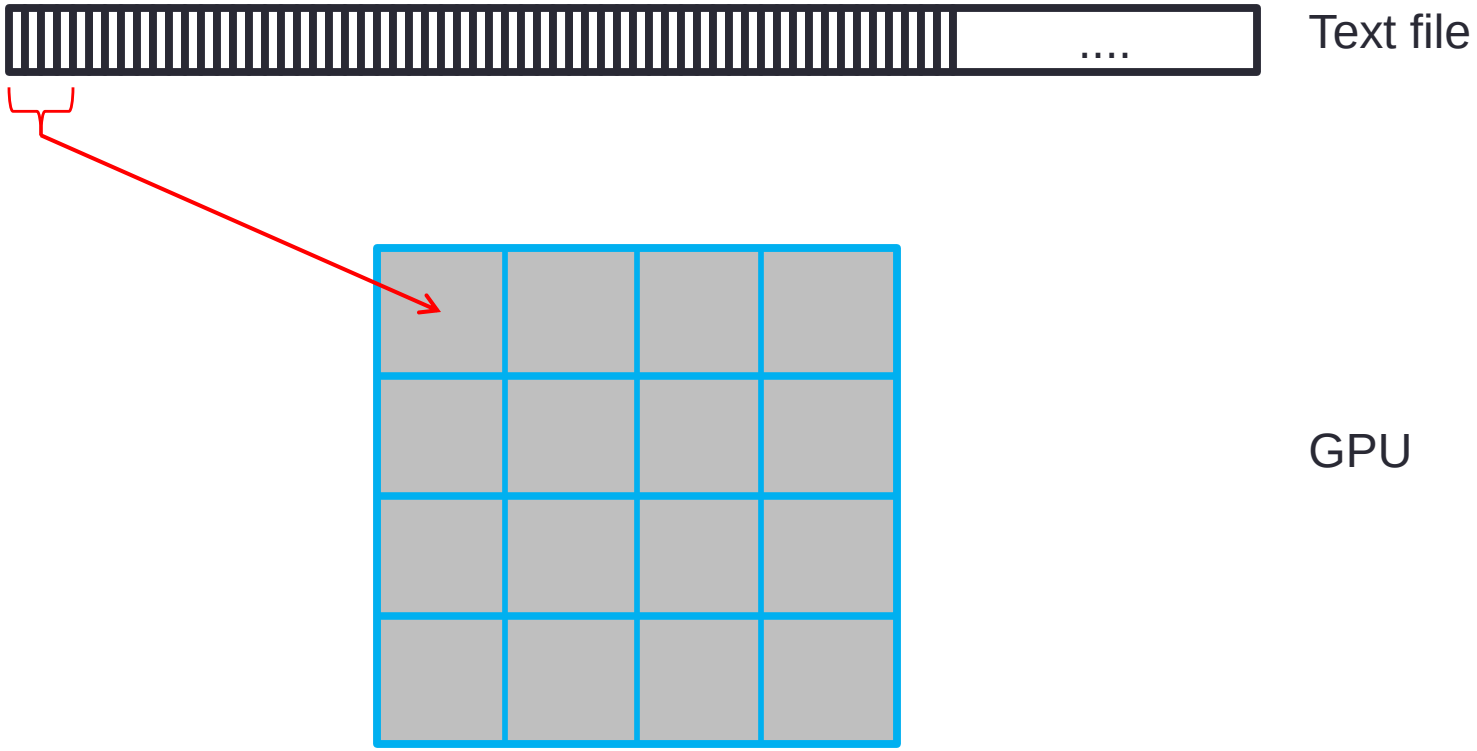

Text file



GPU

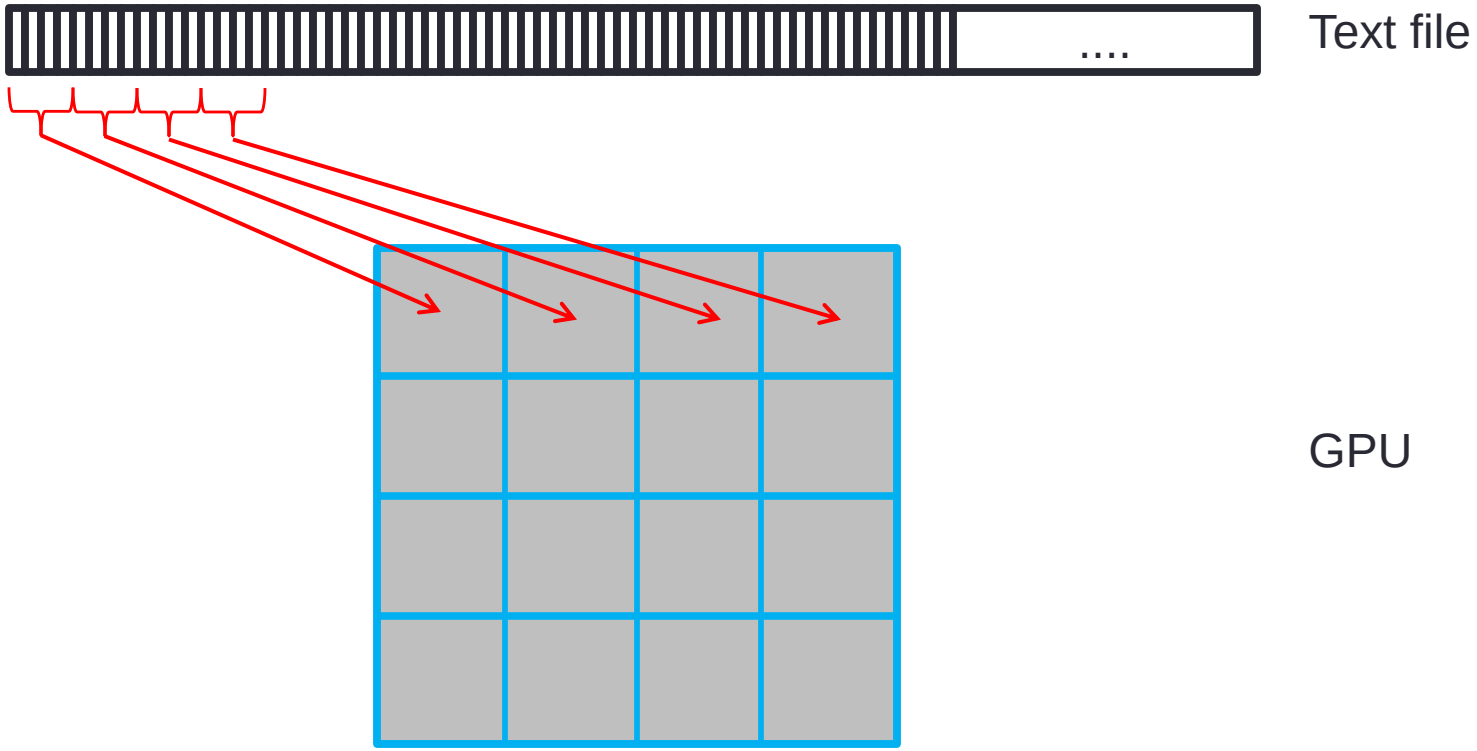
# 7. Parallel computation

- What to parallel?
  - The encryption/decryption process?
  - The whole procedure?



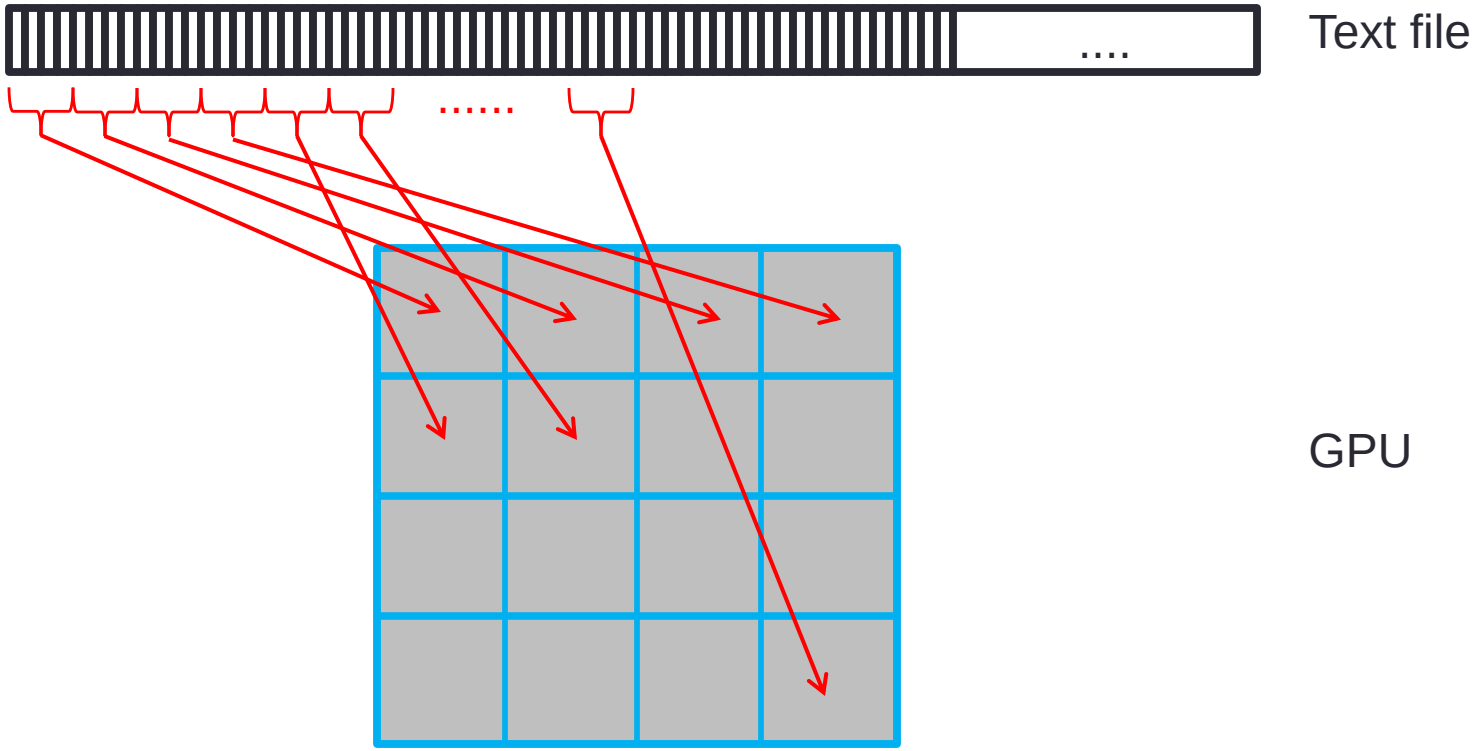
# 7. Parallel computation

- What to parallel?
  - The encryption/decryption process?
  - The whole procedure?



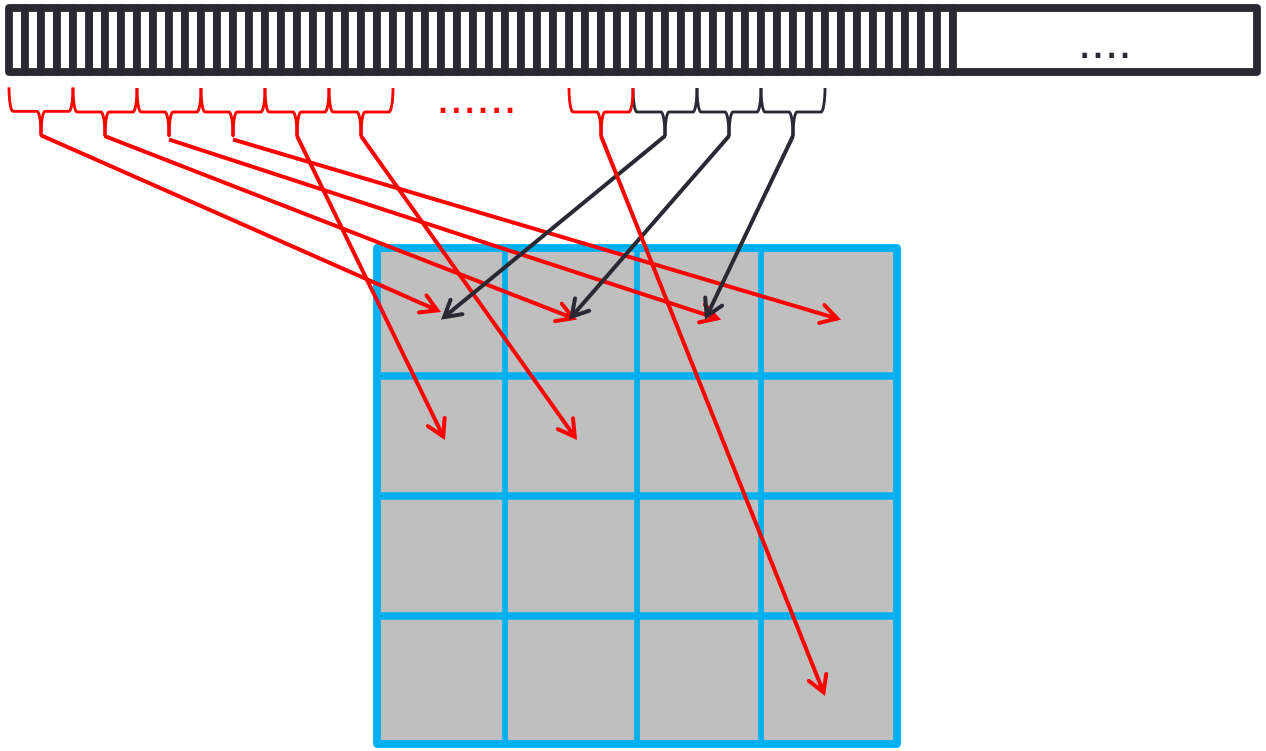
# 7. Parallel computation

- What to parallel?
  - The encryption/decryption process?
  - The whole procedure?



# 7. Parallel computation

- What to parallel?
  - The encryption/decryption process?
  - The whole procedure?



# 8. Results

| Size(KB)\Platform(us) | CPU | GPU |
|---|---|---|
| 0.3 | 49 | 679 |
| 0.6 | 97 | 708 |
| 1.2 | 192 | 779 |
| 2.4 | 397 | 919 |
| 4.8 | 770 | 1179 |
| 9.6 | 1541 | 1720 |
| 19 | 3130 | 2732 |
| 38 | 6261 | 4813 |
| 75 | 12617 | 9254 |
| 150 | 24971 | 17897 |
| 300 | 48888 | 34907 |
| 600 | 100532 | 69527 |