

Batch merge and merge path sort

BAUCHER Achille & MOURSLI Najwa

Polytech Sorbonne

December 13, 2020

KEY

- MODELLING & SIMULATION
- MULTISCALE & MEDICAL
- SECURITY
- ENVIRONMENT
- ENGINEERING MATERIALS & MANUFACTURING

- 1 Introduction
- 2 Merge Path and Sort
- 3 Batch merge
- 4 Application in Cryptanalysis

a	b	c	c	e	f	f	g	l	m	m	n	o	r	s	u	w	w	y	z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

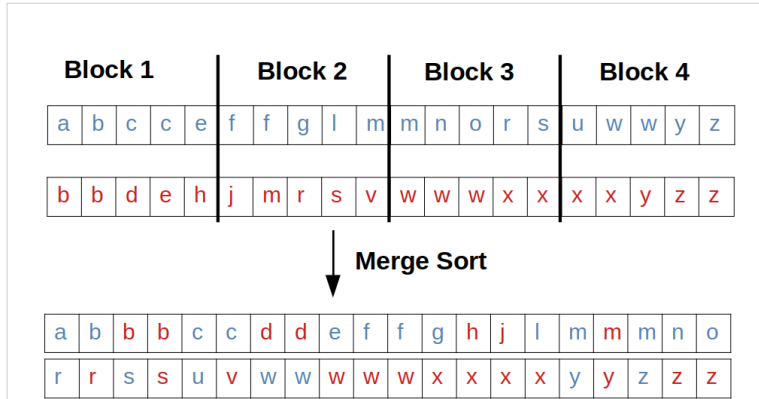
b	b	d	e	h	j	m	r	s	v	w	w	w	x	x	x	x	y	z	z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

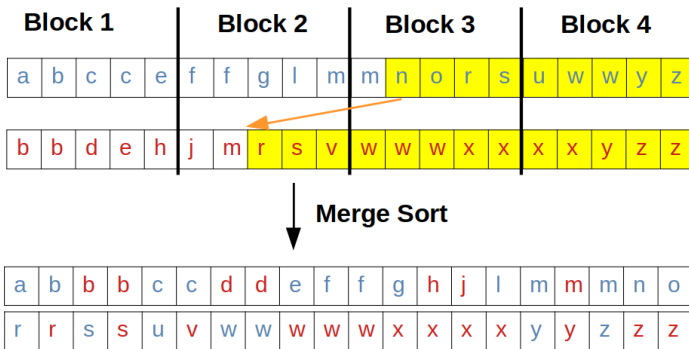


Merge Sort

a	b	b	b	c	c	d	d	e	f	f	g	h	j	l	m	m	m	n	o
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

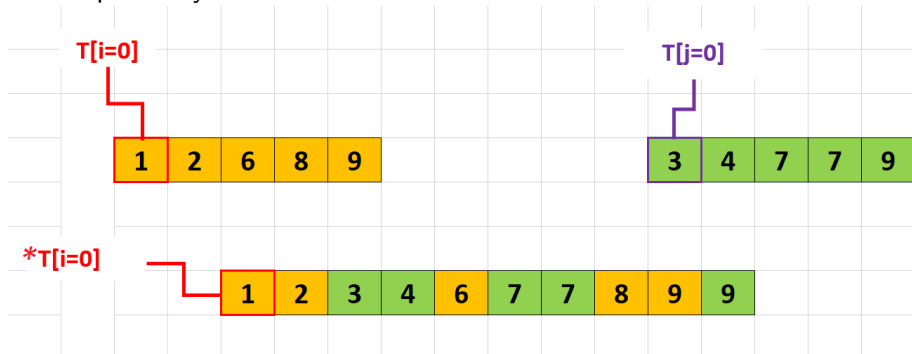
r	r	s	s	u	v	w	w	w	w	w	x	x	x	x	y	y	z	z	z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

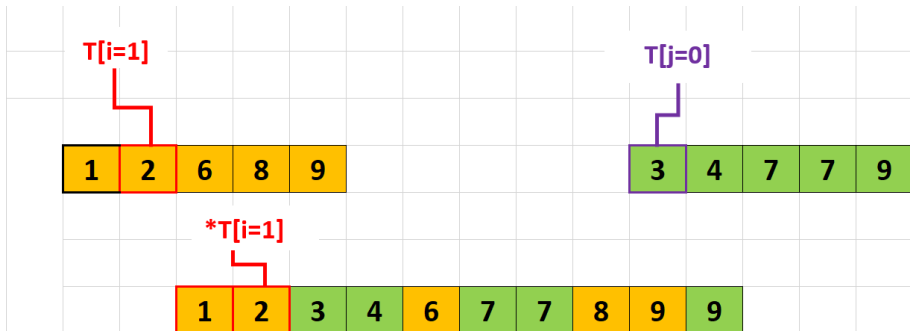


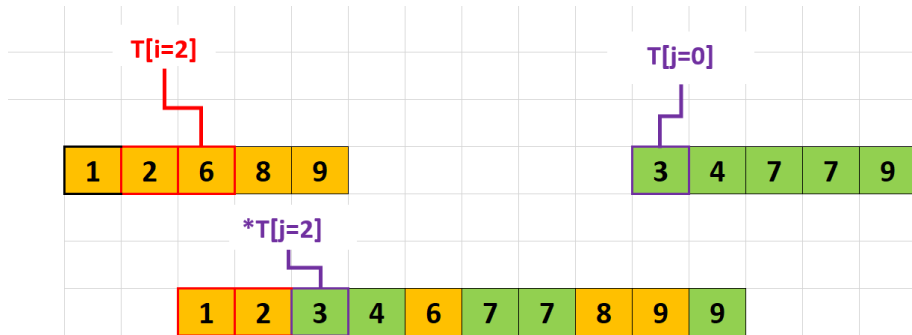


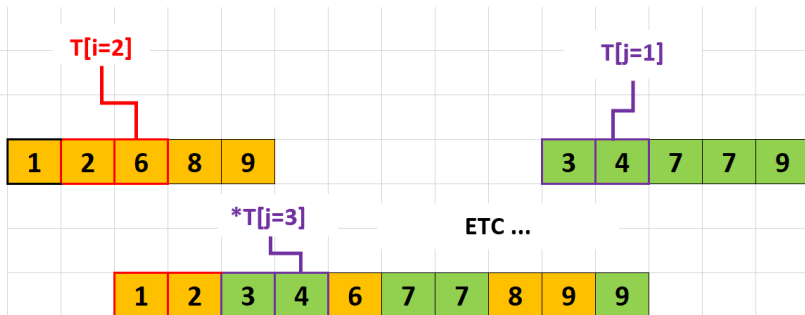
- 1 Introduction
- 2 Merge Path and Sort**
- 3 Batch merge
- 4 Application in Cryptanalysis

The most common idea is to use two pointers and increment one of them whenever it has the lowest value among both, while copying its value to the output array:







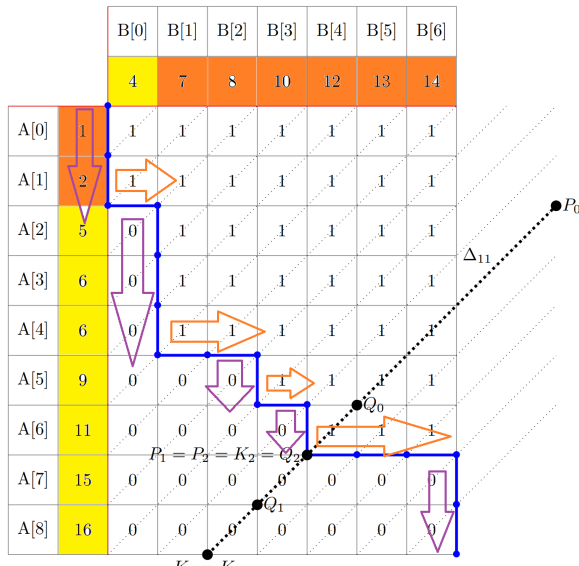


→ $A[i] < B[j]$

↓ $A[i] > B[j]$
 $A[i'] > B[j]$
 $i' \leq i$

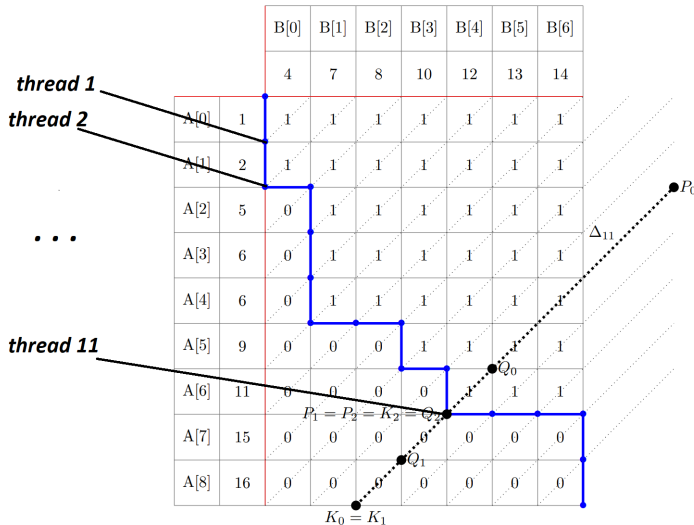
0 marked

1 marked



- It is simple to implement
- It has always the same linear complexity $\Theta(|A| + |B|)$: no bad surprise
- In its original form, it is impossible to parallelize the algorithm.
- An average linear complexity is not optimal

For one block :



■ Parallel Partition

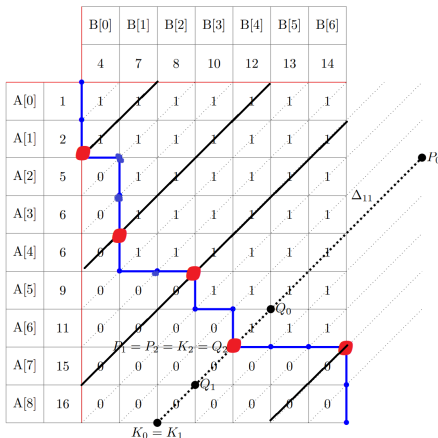
⇒ Map exactly the necessary inputs into each tile.

■ Merge Path

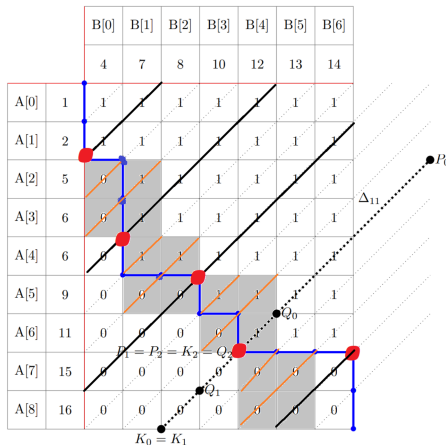
⇒ Cross diagonal binary search **GLOBAL MEMORY**

■ MergeSort of the Merge Path ⇒ Placing the Merge Path on the **SHARED MEMORY** ⇒ Blocksor

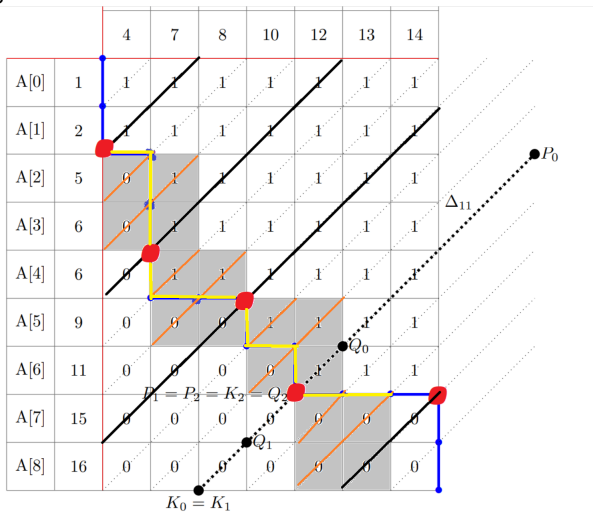
Diagonals divide the work among the blocks. Points of intersection using binary searches on the cross diagonals by comparing elements from A and B on **GLOBAL MEMORY**.



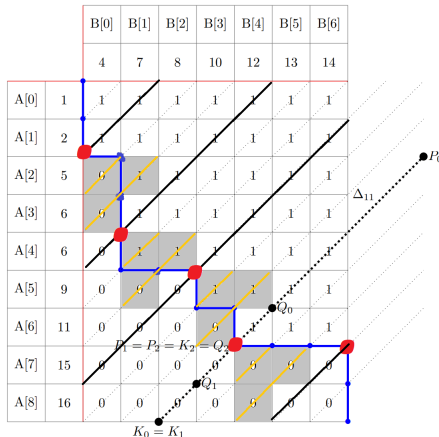
Take a window consisting of the Z largest elements of each of the partitions and place them in local **SHARED MEMORY**.



Write the Merge Path found on **GLOBAL MEMORY**.



Several cycles in parallel and Place the Merge Path on the **SHARED MEMORY** \Rightarrow MERGE.



3 different cases illustration:

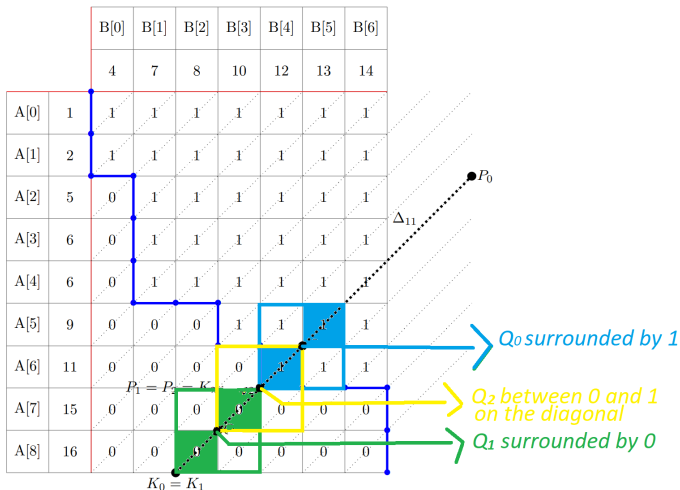
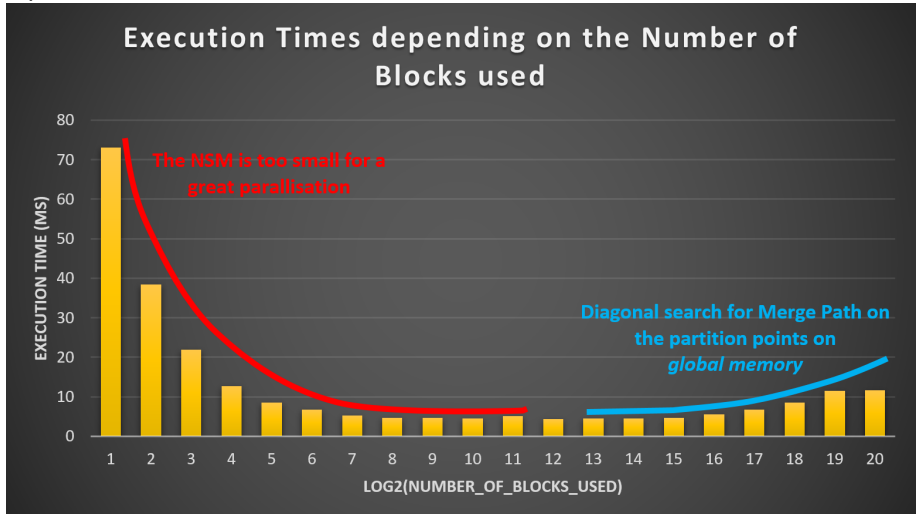
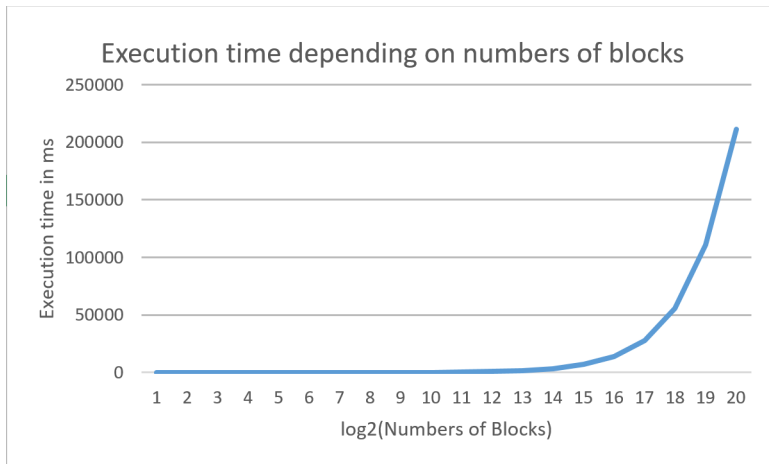
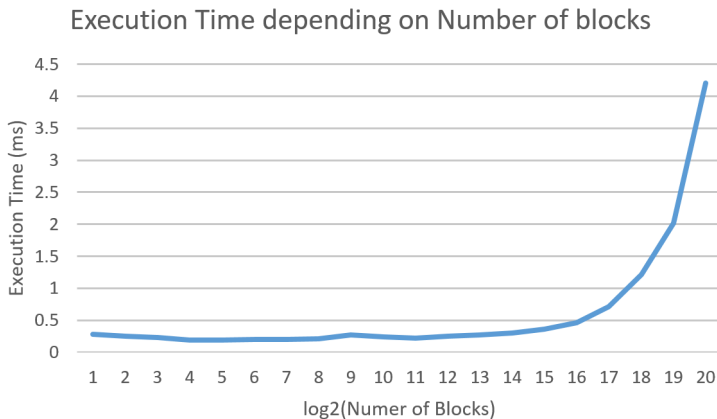


Figure 1: An example of Merge Path procedure

Optimal number of blocks







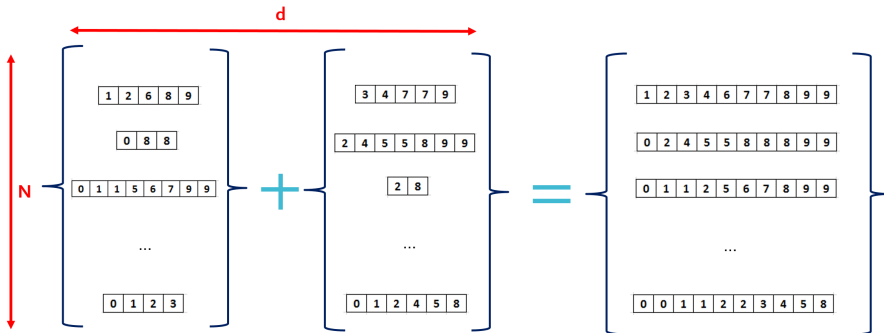
- We decided to compare the wall-clock time of merging randomly generated vectors of integers for the three algorithms. For the GPU algorithm, we also monitored the wall-clock time for sort initialization
⇒ **CUDA EVEN TIMER**
- Sanity check We implemented a sanity check (on CPU for the three versions) to check if the array is really sorted in the end of the program.

We ran 100 simulations of the three algorithms, gathering the average wall-clock time of the merge part only. The task consisted in merging $2^{20} = 1,048,576$ arrays of size 2

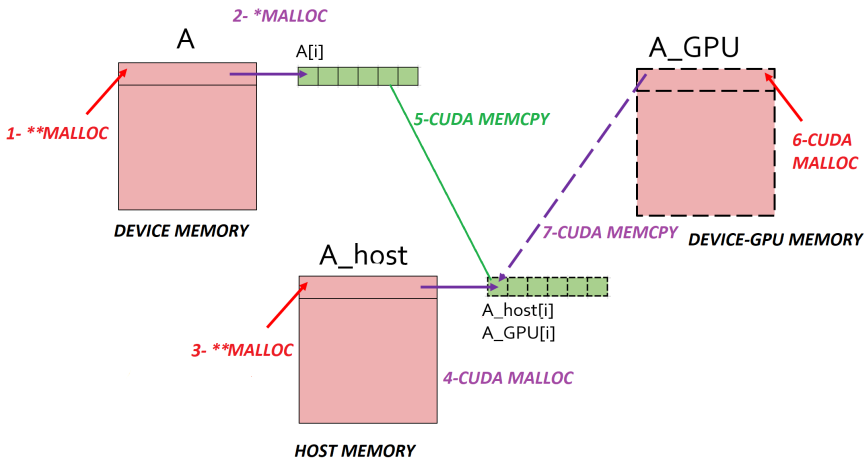
Algorithm	Wall-clock time (ms)
Merge path (CPU)	50 032
Sequential merge path	1 650
Merge path (GPU)	70

$\approx \times 20$

- 1 Introduction
- 2 Merge Path and Sort
- 3 Batch merge**
- 4 Application in Cryptanalysis



Procedure to allocate on the DEVICE an array of arrays:



d: number of elements in a pair of array

m: number of pairs of array mergesorted in a single block

- 1 $\text{int tid} = \text{threadIdx.x} \% d \Rightarrow$ Enumeration from 0 to d-1 of the elements of each of the m pairs of arrays which are going to be sorted in a single block
- 2 $\text{int Qt} = (\text{threadIdx.x} - \text{tid}) / d \Rightarrow$ Local enumeration from 0 to m-1 of the pairs of arrays in a single block
- 3 $\text{int gbx} = \text{Qt} + \text{blockIdx.x} * (\text{blockDim.x} / d) \Rightarrow$ Global enumeration from 0 to N-1 of the pairs of arrays in all the blocks

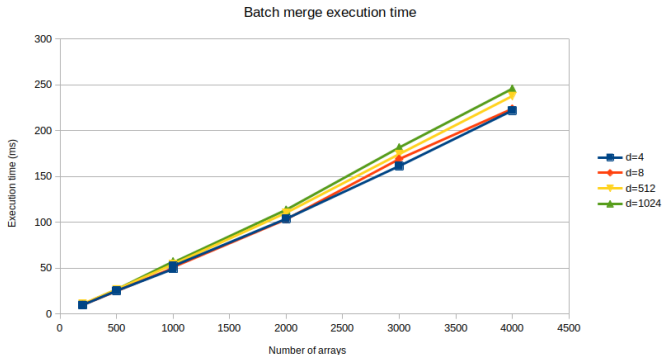


Figure: Batch merge execution times in function of N with various values of d

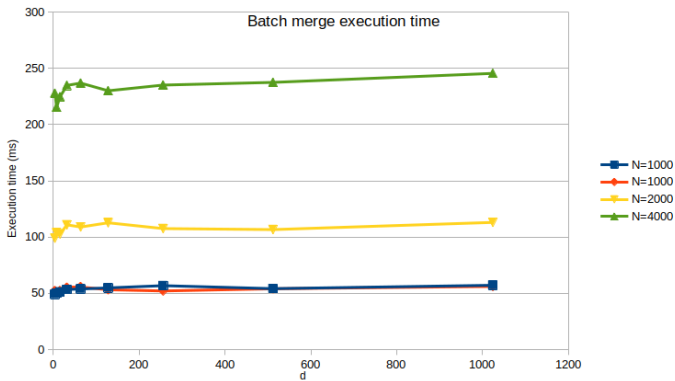


Figure: Batch merge execution times in function of d with various values of N

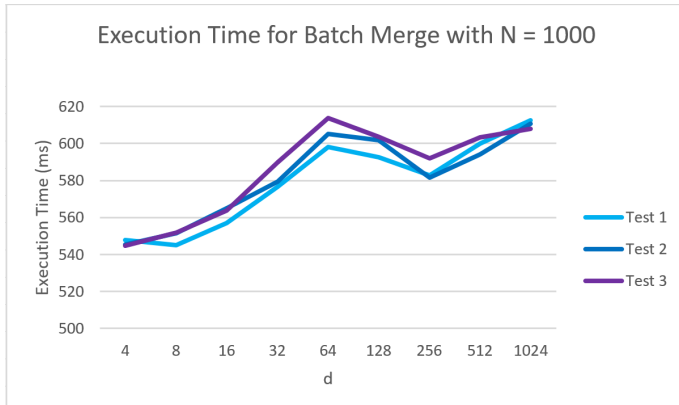


Figure: Batch merge execution times in function of $N = 10^4$ with various values of d

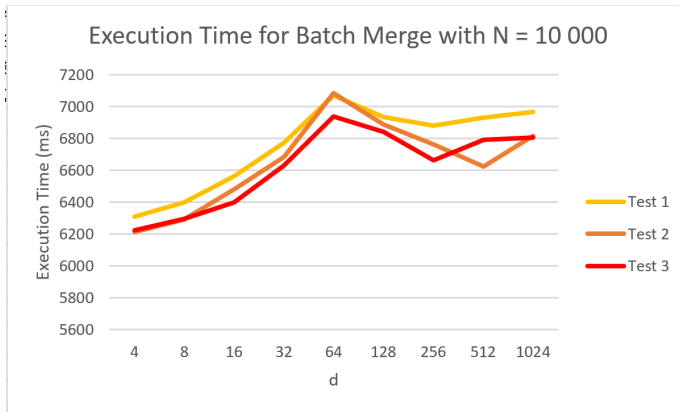


Figure: Batch merge execution times in function of $N = 10^5$ with various values of d

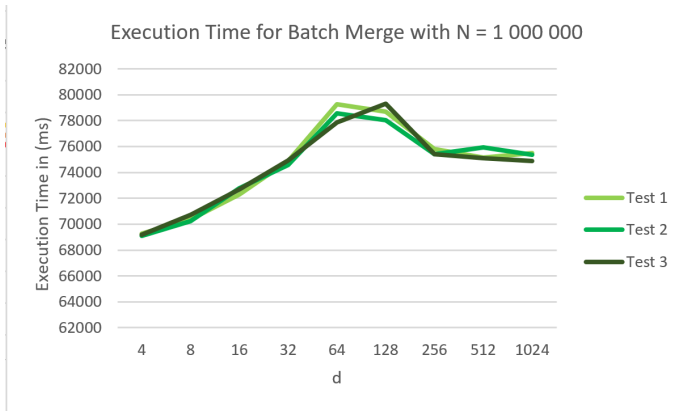


Figure: Batch merge execution times in function of $N = 10^6$ with various values of d

- 1 Introduction
- 2 Merge Path and Sort
- 3 Batch merge
- 4 Application in Cryptanalysis**

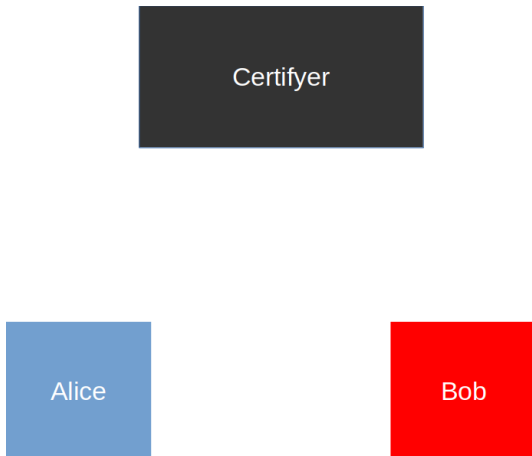


Figure: Alice and Bob want to get access to the certifier

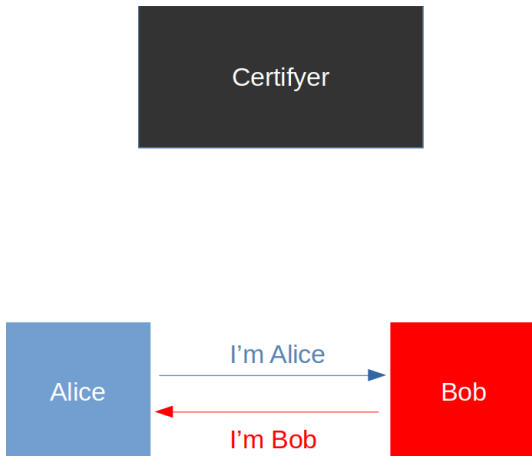


Figure: Alice and Bob recognise each other

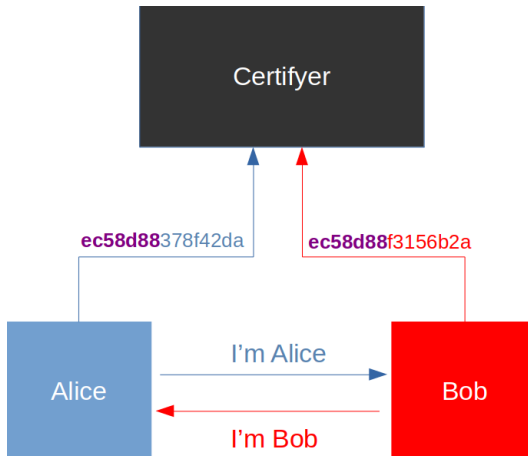


Figure: Alice and Bob send their hashed message

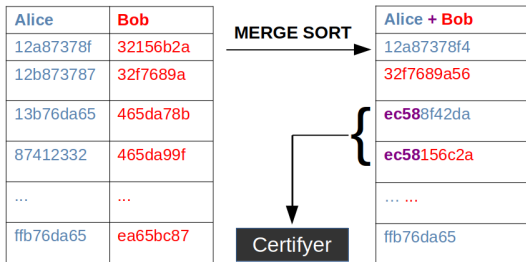


Figure: Merge sort and find keys to get access

```
./main
Initialize and sort every possible vectors ... Ok.

-----

Alice and bob arrive ! Merge sort Alice's and Bob's vectors
dim: 80000
-13507636 -13507255 -13506814 -13506804 -13506753 -13506653
End. Execution time: 0.760576 ms

-----n
Try to find 2 chains with the same first bits
Begining of the search... End of the search.
2 keys are:
ff36e7fe
ff36e707
```

Figure: Output

**THANK YOU
FOR
YOUR
ATTENTION!
ANY QUESTIONS?**

Reference: O. Green, R. McColl and D. A. Bader «GPU Merge Path, A GPU Merging Algorithm» 26th ACM International Conference on Supercomputing (ICS), San Servolo Island, Venice, Italy, June 25-29, 2012