Somewhat homomorphic encryption schemes:

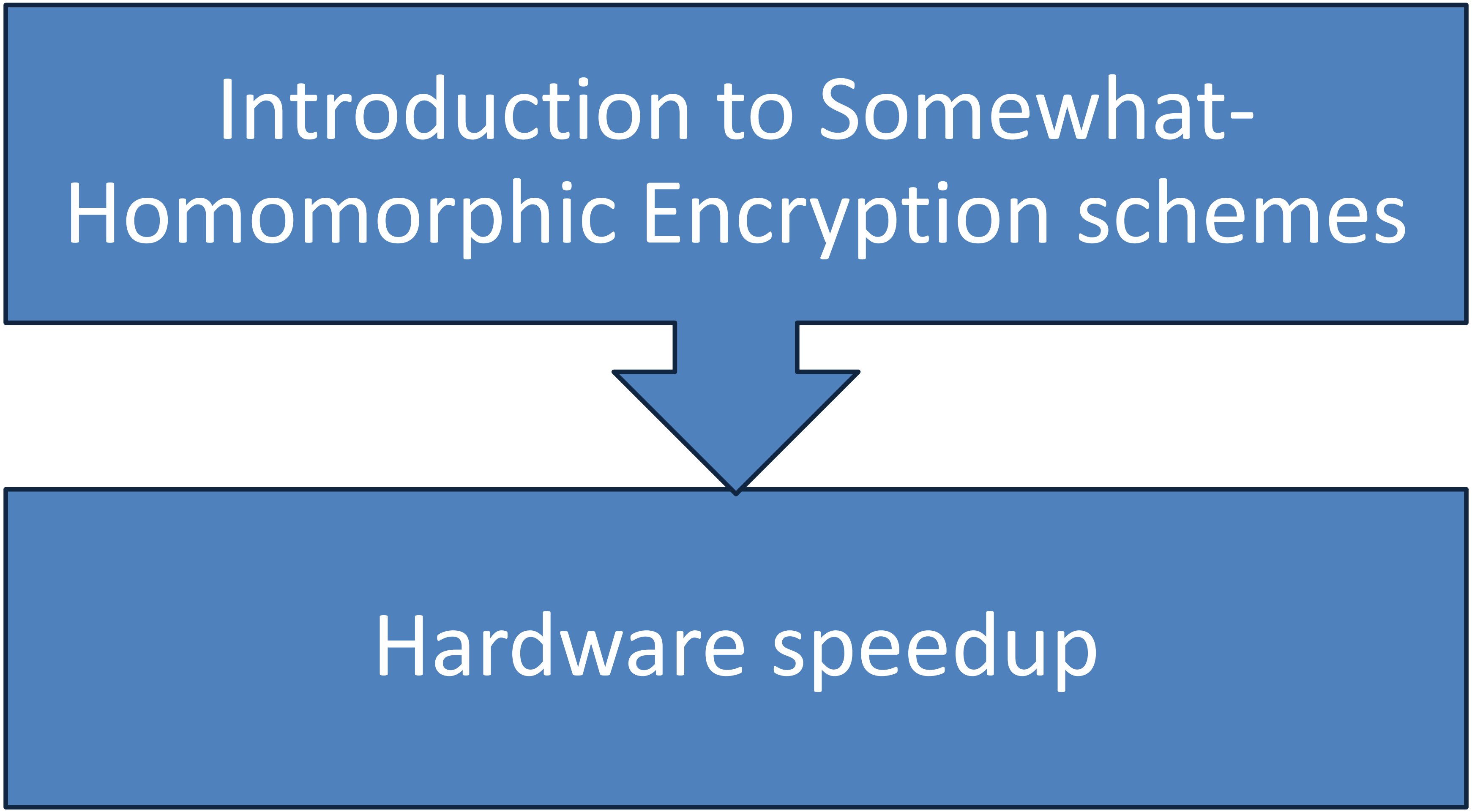
which candidates and which expectations to have with these encryption schemes?

Vincent MIGLIORE

June 29th, 2015

DGA Lab-STICC UMR IRISA

Plan



Introduction to Somewhat-Homomorphic Encryption schemes

Hardware speedup

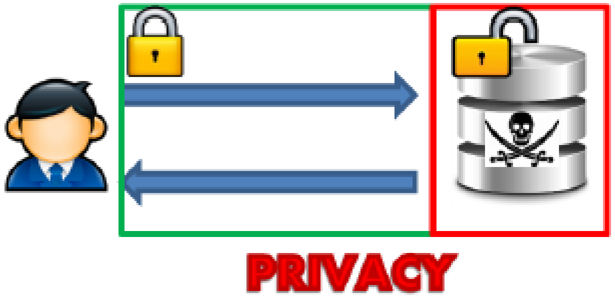
Definition of homomorphic encryption

Introduction to SHE schemes

- Definition and use case
- State of the art
- Technological barriers

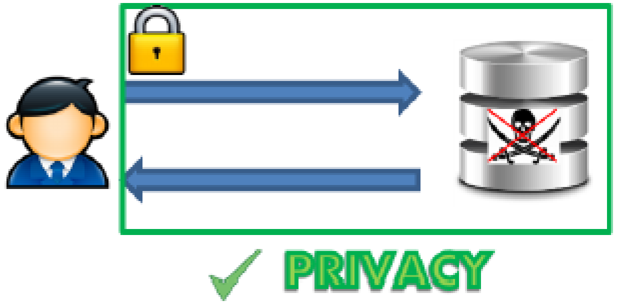
Speedup of Homomorphic multiplication

- Multiplication algorithms
- Co-processor architecture
- Expected speedup



Data are computed after decryption

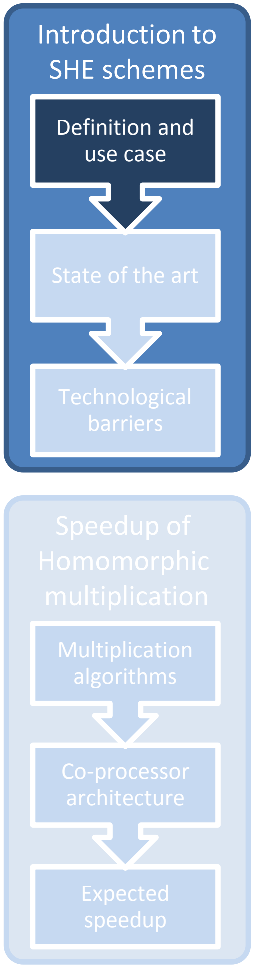
Classical cloud service



Data are computed in the cipher domain

Homomorphic encryption style cloud service

Use case


Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup

In the medical area:

Management of electronic medical records (EMR) to perform statistical analysis privatly.

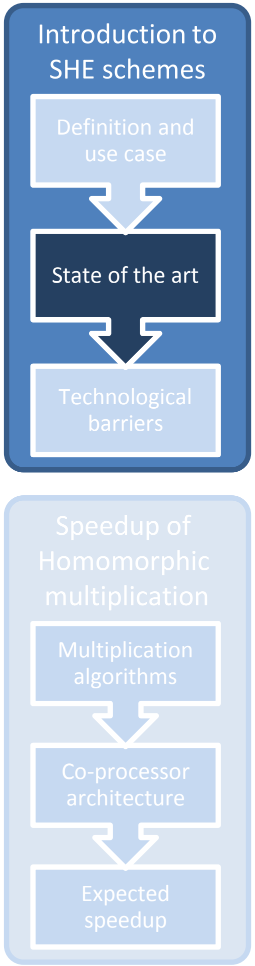
In the VOD services area:

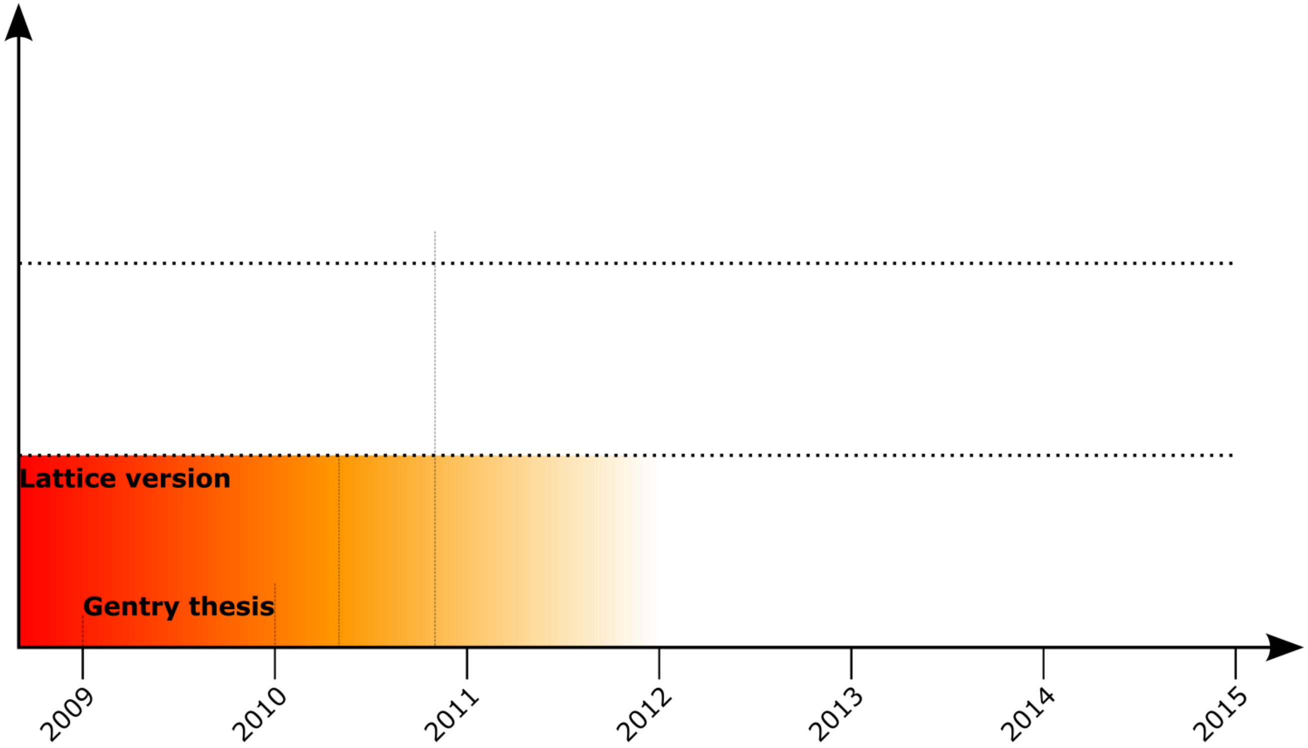
Hided search of a video link in a database.

In the financial area:

Constant verification of financial data to prevent financial crisis without compromising privacy of investors and financial players.

State of the art


Introduction to SHE schemes
Definition and use case
State of the art
Technological barriers
Speedup of Homomorphic multiplication
Multiplication algorithms
Co-processor architecture
Expected speedup



State of the art

Introduction to SHE schemes

Definition and use case

State of the art

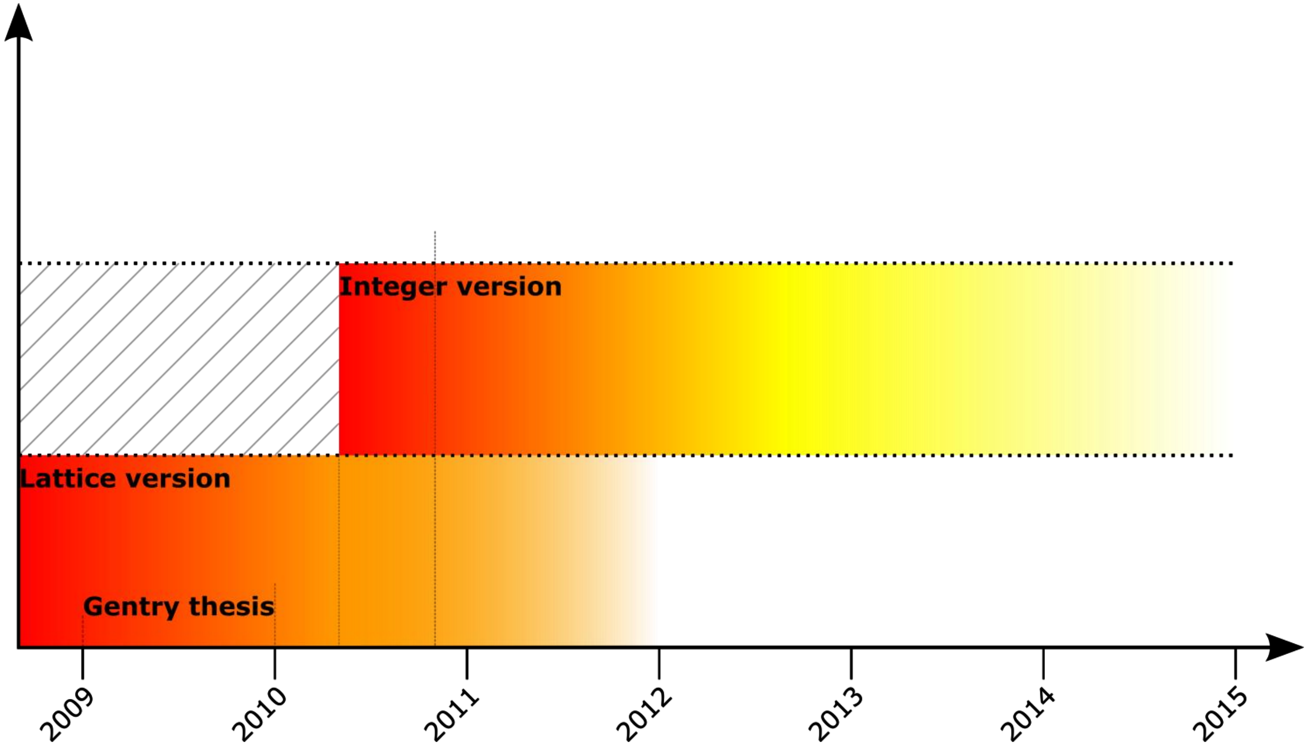
Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup



State of the art

Introduction to SHE schemes

Definition and use case

State of the art

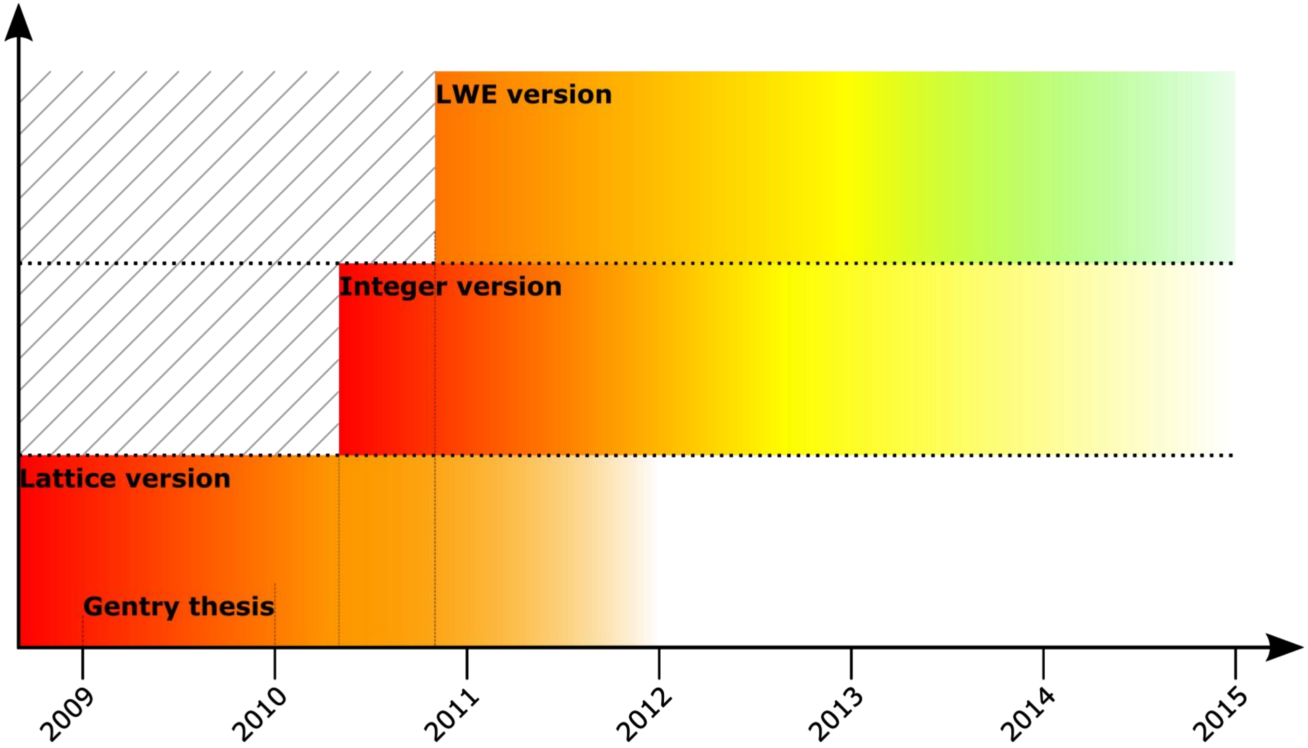
Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup



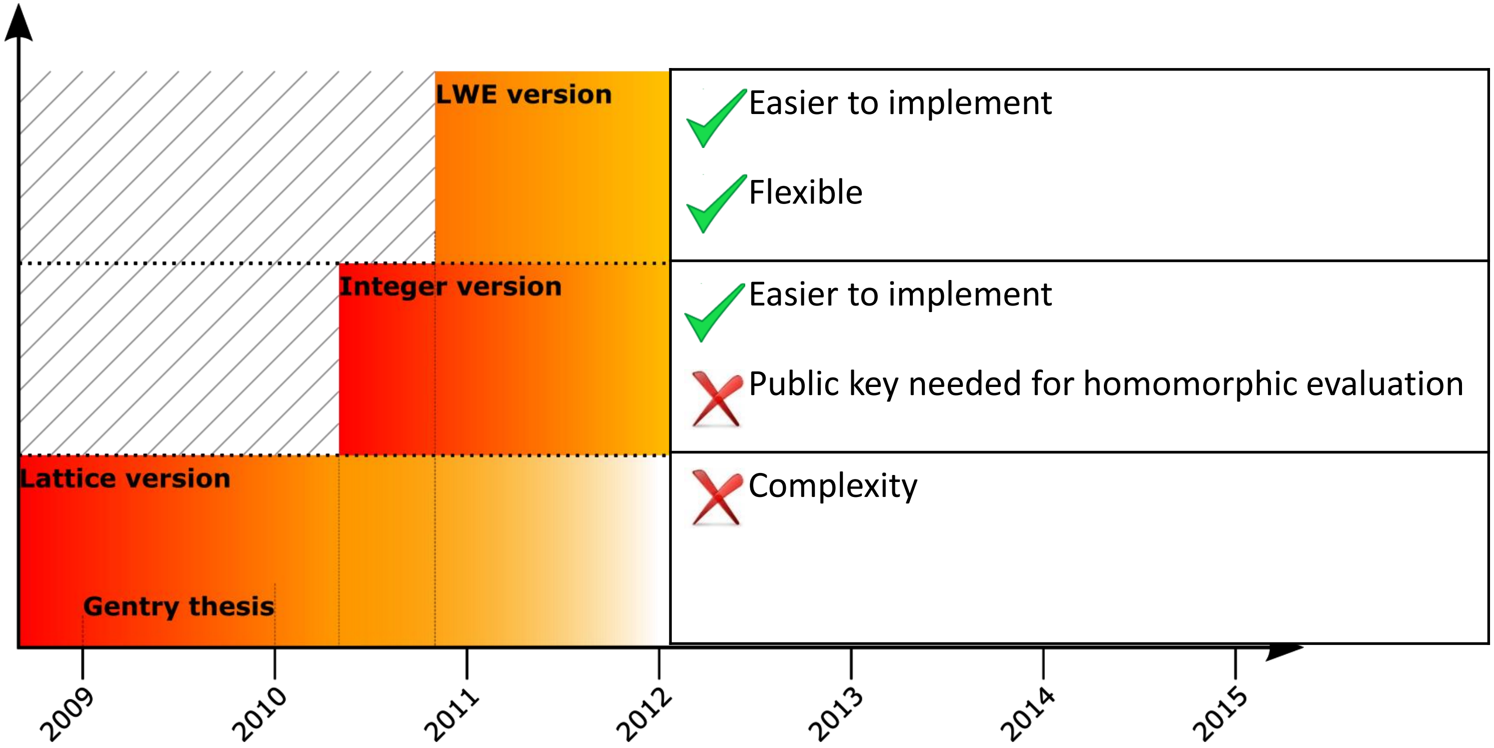
State of the art

Introduction to SHE schemes

- Definition and use case
- State of the art
- Technological barriers

Speedup of Homomorphic multiplication

- Multiplication algorithms
- Co-processor architecture
- Expected speedup



✓ Easier to implement

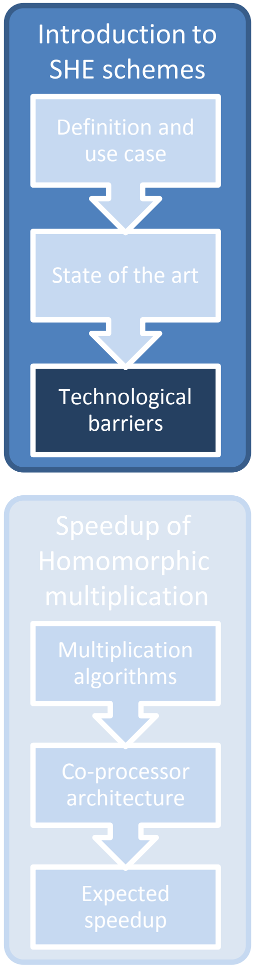
✓ Flexible

✓ Easier to implement

✗ Public key needed for homomorphic evaluation

✗ Complexity

Technological barriers



Introduction to SHE schemes

Definition and use case

State of the art

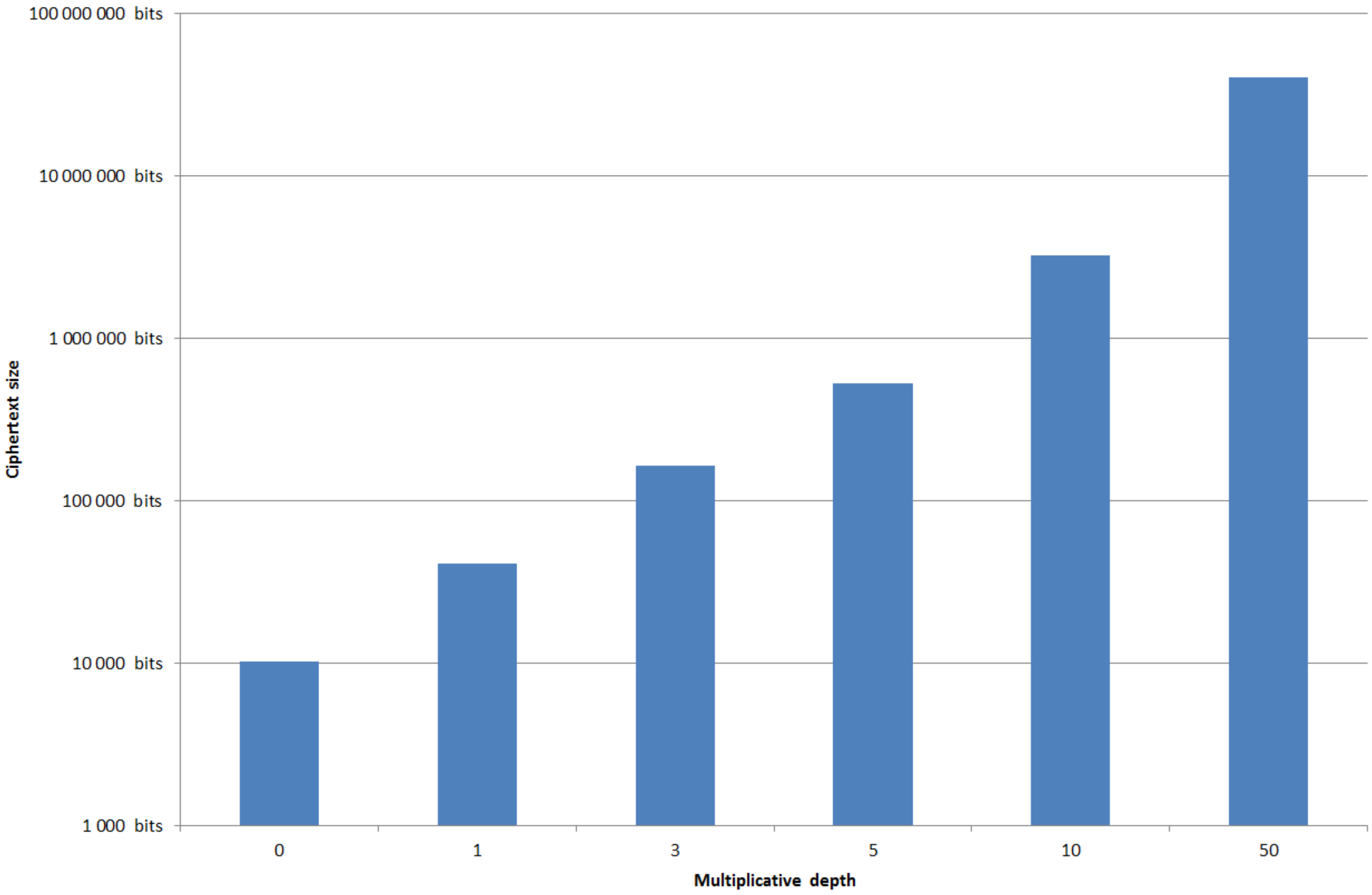
Technological barriers

Speedup of Homomorphic multiplication

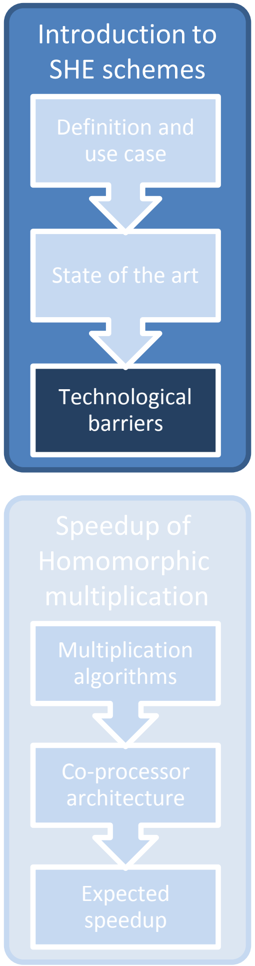
Multiplication algorithms

Co-processor architecture

Expected speedup



Technological barriers



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup

- $C \in Z_q[X]/f(X);$
  - $f(X) = X^n + 1$

L	$log_2(q)$	n
0	20	512
1	40	1024
3	80	2048
5	128	4096
10	392	8192
50	1225	32768

Technological barriers

Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

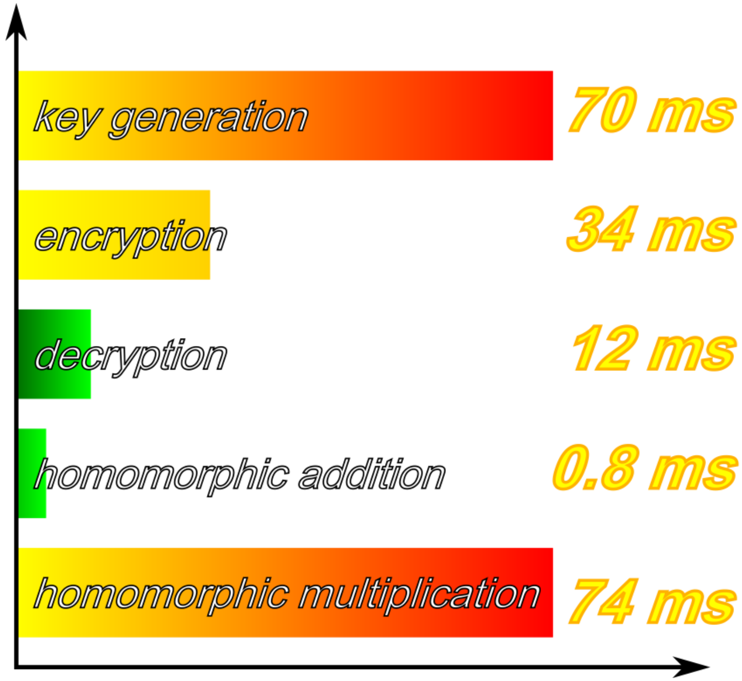
Multiplication algorithms

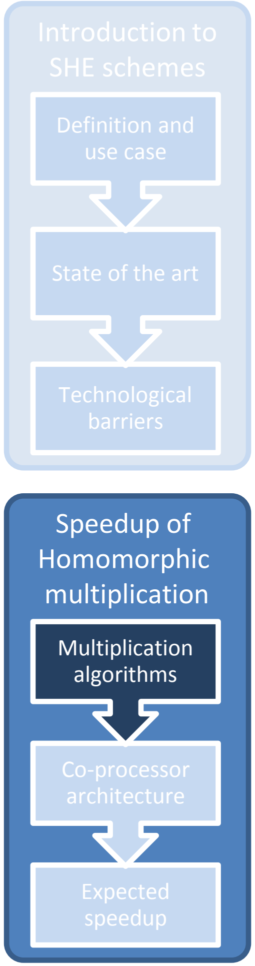
Co-processor architecture

Expected speedup

- $C \in Z_q[X]/f(X);$
  - $f(X) = X^n + 1$

L	$log_2(q)$	n
0	20	512
1	40	1024
3	80	2048
5	128	4096
10	392	8192
50	1225	32768





Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

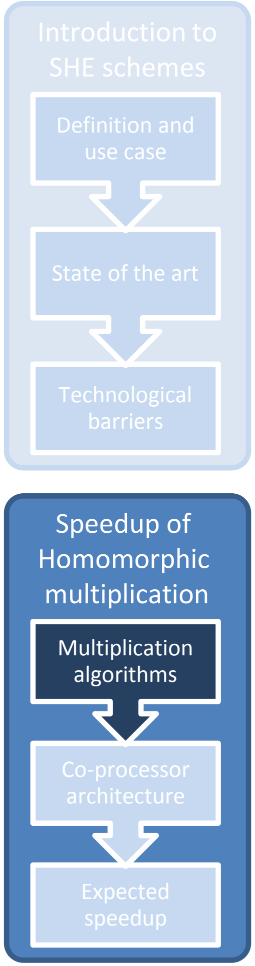
Multiplication algorithms

Co-processor architecture

Expected speedup

Speedup the Homomorphic multiplication

Multiplication algorithms



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup

- **Classical multiplication (naive)**
  - *Complexity:* $O(n^2)$
- **Karatsuba multiplication**
  - *Complexity:* $O(n^{1.58})$
- **FFT multiplication**
  - *Complexity:* $O(n.log_2(n))$

First architecture

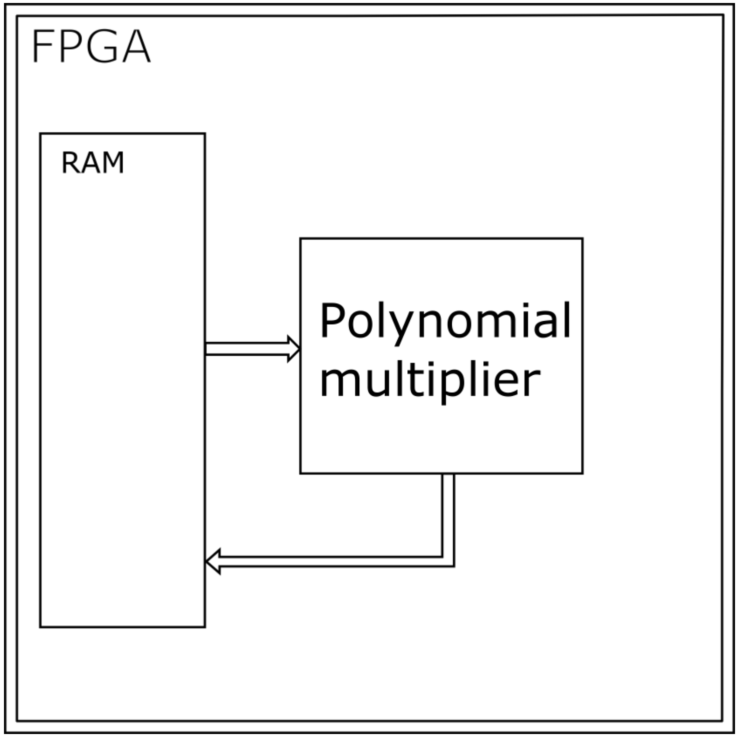
Introduction to SHE schemes

- Definition and use case
- State of the art
- Technological barriers

Speedup of Homomorphic multiplication

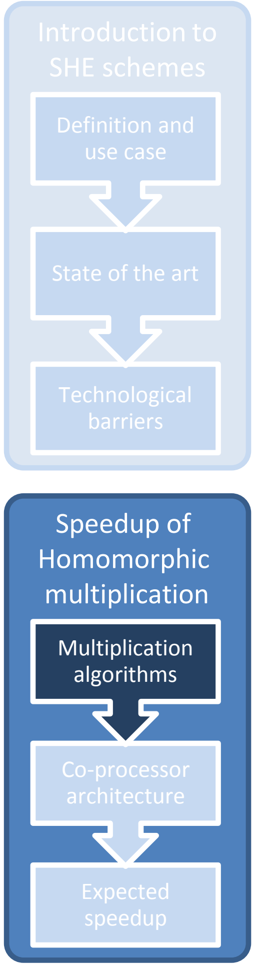
- Multiplication algorithms
- Co-processor architecture
- Expected speedup

- Classical architecture:



- Limited RAM reads/writes
- Limited hardware ressources

Karatsuba algorithm



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup

$$A(x) = A_0(x) + A_1(x)x^{\lceil n/2 \rceil}; B(x) = B_0(x) + B_1(x)x^{\lceil n/2 \rceil};$$

$$C(x) = A(x).B(x)$$

Karatsuba algorithm

Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

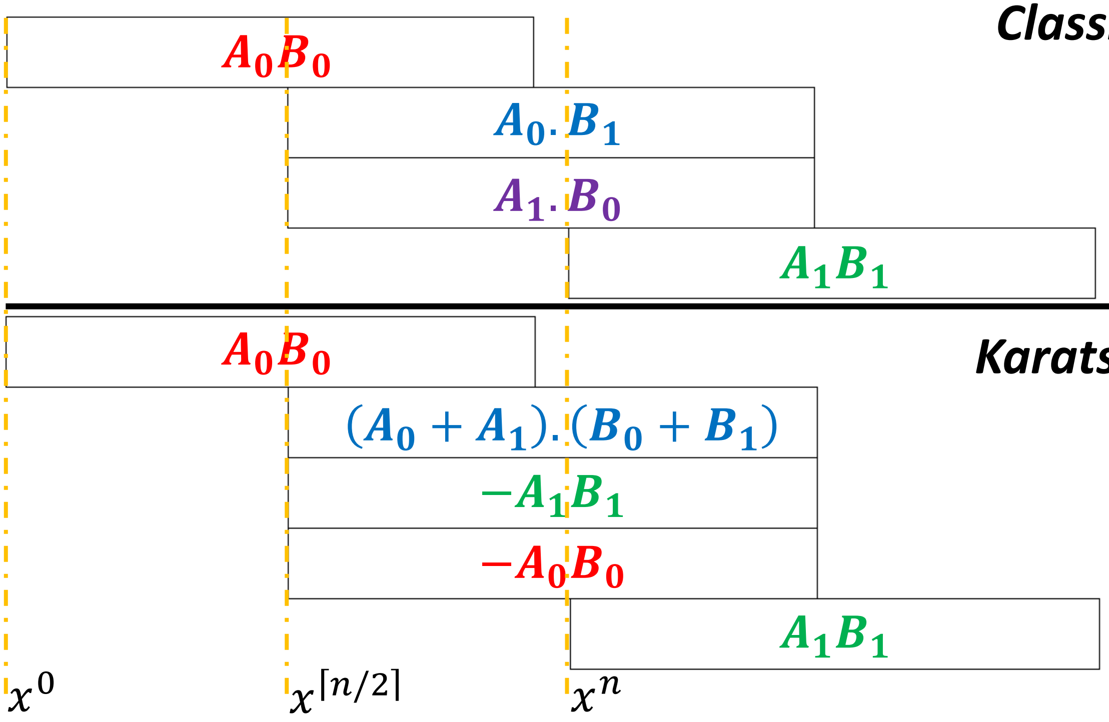
Multiplication algorithms

Co-processor architecture

Expected speedup

$$A(x) = A_0(x) + A_1(x)x^{\lceil n/2 \rceil}; B(x) = B_0(x) + B_1(x)x^{\lceil n/2 \rceil};$$

$$C(x) = A(x).B(x)$$



Classical multiplier

4 multiplications

1 addition

Karatsuba multiplier

3 multiplications

4 additions

Karatsuba algorithm

Introduction to SHE schemes

Definition and use case

State of the art

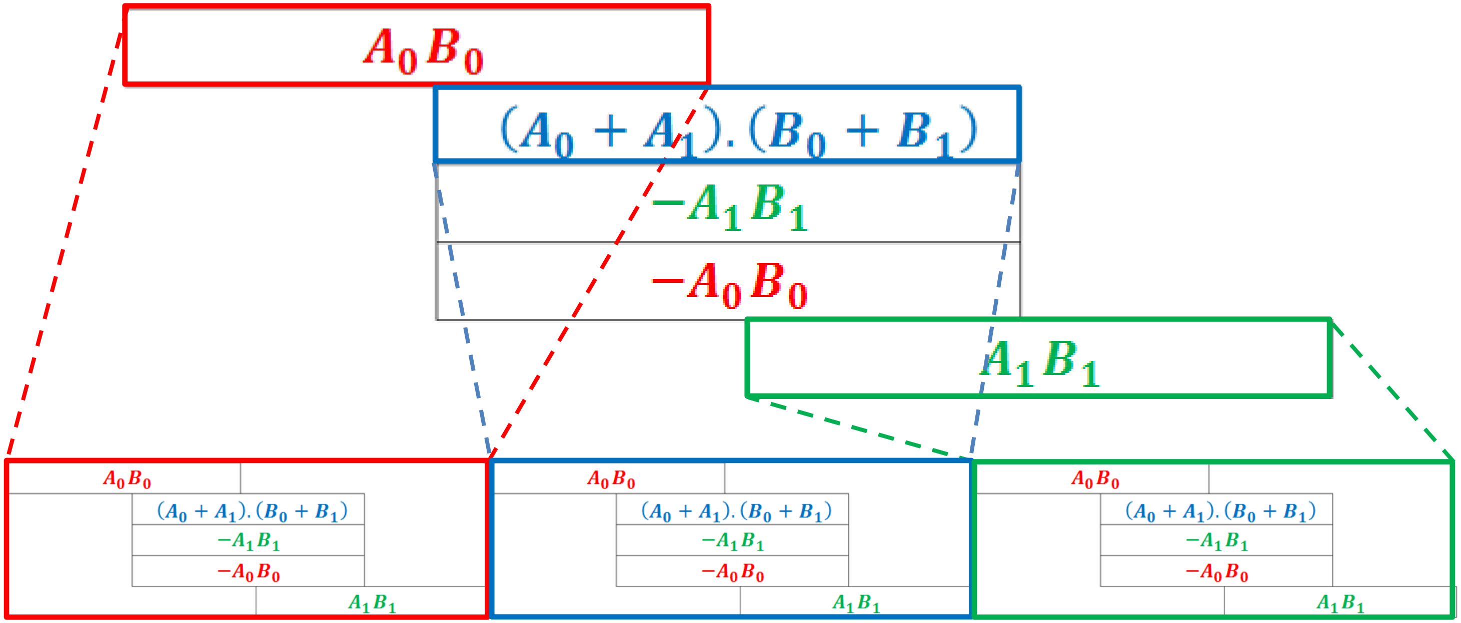
Technological barriers

Speedup of Homomorphic multiplication

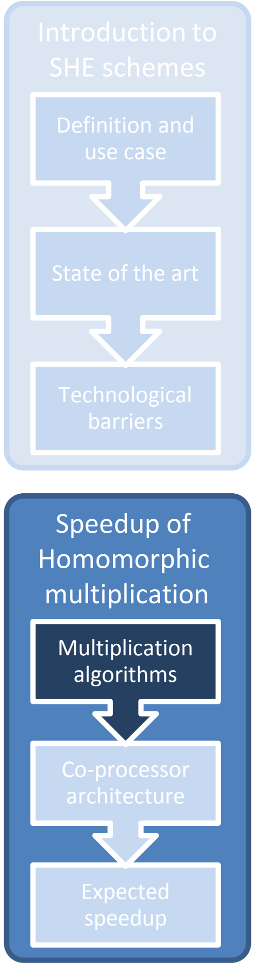
Multiplication algorithms

Co-processor architecture

Expected speedup



Karatsuba algorithm



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

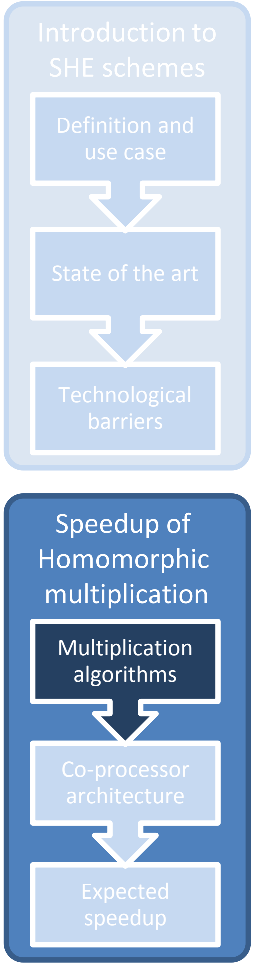
Multiplication algorithms

Co-processor architecture

Expected speedup

- Number of operations:
  - $\underbrace{3^{\log_2(n)}}_{\text{Total of products}} / \underbrace{3^{\log_2\left(\frac{m}{2}\right)}}_{\text{Total of products calculated with m coefficients}}$

FFT algorithm


Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

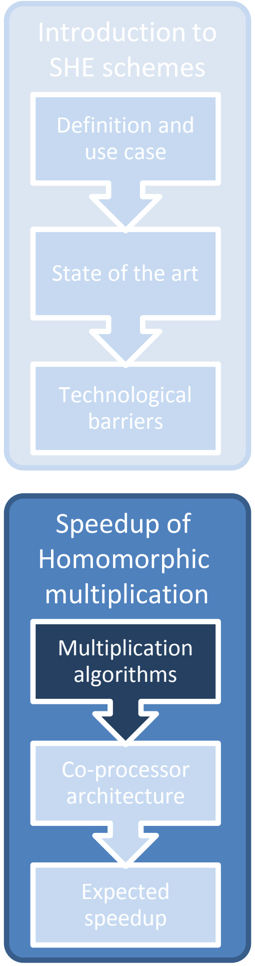
Multiplication algorithms

Co-processor architecture

Expected speedup

- 2 types of FFT:

FFT algorithm



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

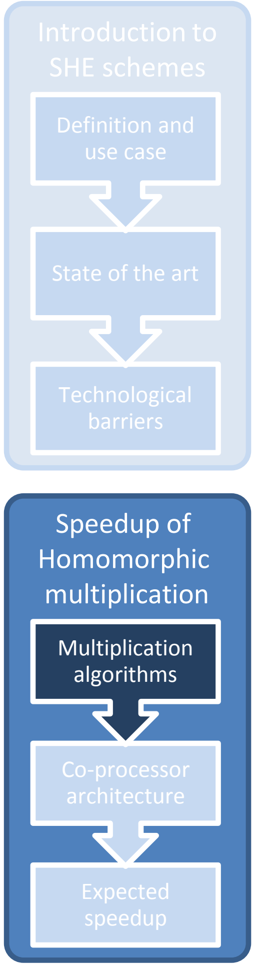
Multiplication algorithms

Co-processor architecture

Expected speedup

- 2 types of FFT:
  - Classical FFT
    - Need to fill with zeros $n \rightarrow 2.n$

FFT algorithm



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup

- 2 types of FFT:
  - Classical FFT
    - Need to fill with zeros $n \rightarrow 2.n$
  - Negative Wrapped Convolution (NWC)
    - Reduction by $X^n + 1$
    - No need to fill with zero

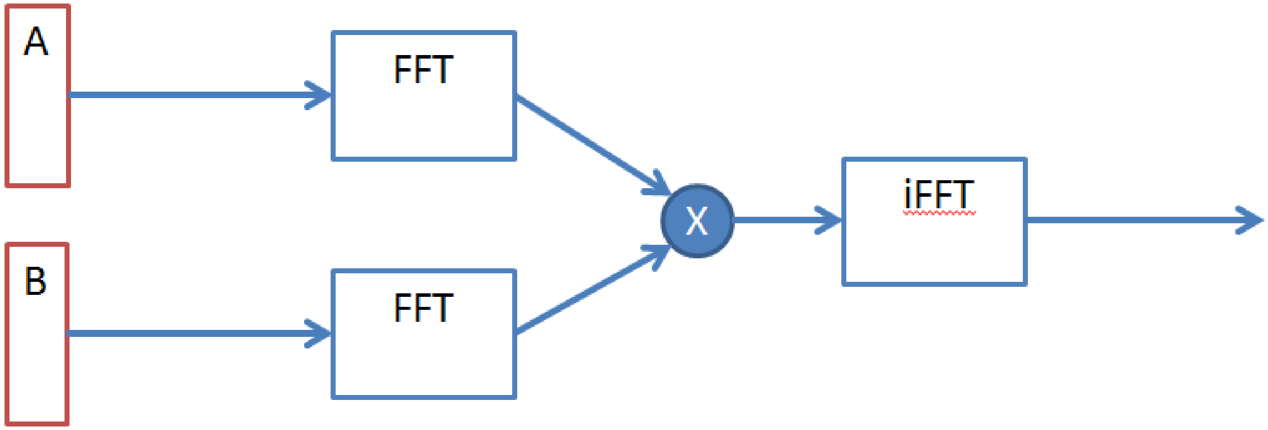
FFT algorithm

Introduction to SHE schemes

- Definition and use case
- State of the art
- Technological barriers

Speedup of Homomorphic multiplication

- Multiplication algorithms
- Co-processor architecture
- Expected speedup

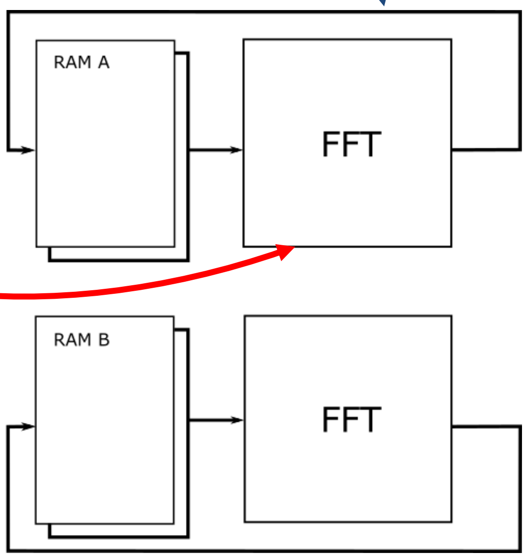


FFT algorithm

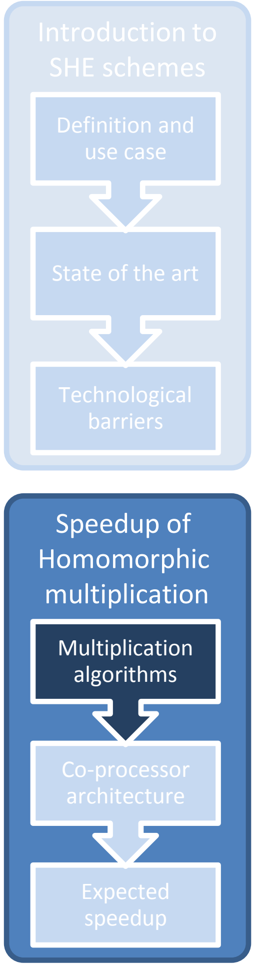
Introduction to SHE schemes
Definition and use case
State of the art
Technological barriers
Speedup of Homomorphic multiplication
Multiplication algorithms
Co-processor architecture
Expected speedup

```
$a = reverse\_order(a)$
for $i = 0$ to $log_2(n) - 1$ do
    for $j = 0$ to $n/2 - 1$ do
        $P_{i,j} = \lfloor \frac{j}{2^{log_2(n-1-i)}} \rfloor . 2^{log_2(n-1-i)}$
        $A_j = a_{2j} + a_{2j+1}\omega^{P_{i,j}} \bmod p$
        $A_{j+\frac{n}{2}} = a_{2j} - a_{2j+1}\omega^{P_{i,j}} \bmod p$
    end for
    if $i \neq log_2(n) - 1$ then
        $a = A$
    end if
end for
```

$log_2(n)$ $rounds$



FFT algorithm



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

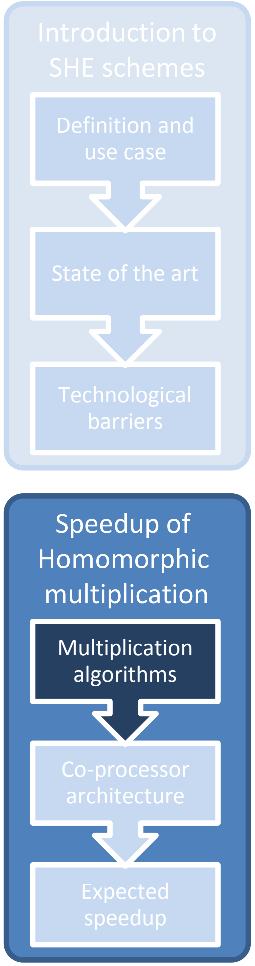
Multiplication algorithms

Co-processor architecture

Expected speedup

- Operations:
  - $\underbrace{\frac{n}{2}log_2(n)}_{\text{2xFFT}}+\underbrace{\frac{n}{4}}_{\substack{\text{Pointwise}\\\text{multiplication}}}+\underbrace{\frac{n}{4}log_2(n)}_{\text{iFFT}}$

FFT algorithm


Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

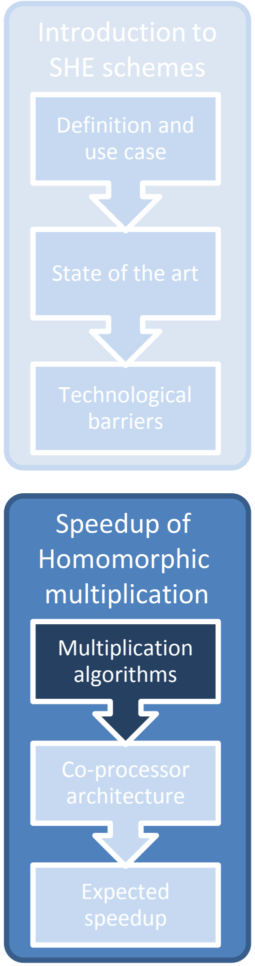
Co-processor architecture

Expected speedup

- Operations:
  - $\underbrace{\frac{n}{2}log_2(n)}_{\text{2xFFT}} + \underbrace{\frac{n}{4}}_{\text{Pointwise multiplication}} + \underbrace{\frac{n}{4}log_2(n)}_{\text{iFFT}}$

- General case:
  - $\frac{n}{m}log_2(n) + \frac{n}{m} + \frac{n}{2m}log_2(n)$
  - $\frac{3n}{2m}log_2(n) + \frac{n}{m}$

FFT / Karatsuba comparison



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

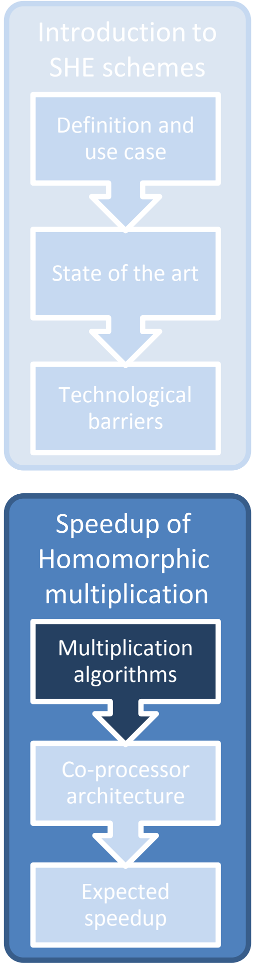
Multiplication algorithms

Co-processor architecture

Expected speedup

Coefficients per operation	Karatsuba	FFT NWC	FFT
4	19683	7936	17408
8	6561	3968	8704
16	2187	1984	4352
32	729	992	2176
64	243	496	1088
128	81	248	544
256	27	124	272
512	9	62	136
1024	3	31	68

FFT / Karatsuba comparison



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

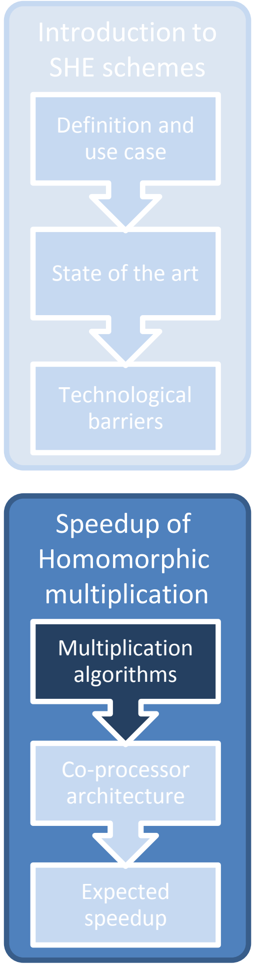
Multiplication algorithms

Co-processor architecture

Expected speedup

Coefficients per operation	Karatsuba	FFT NWC	FFT
4	19683	7936	17408
8	6561	3968	8704
16	2187	1984	4352
32	729	992	2176
64	243	496	1088
128	81	248	544
256	27	124	272
512	9	62	136
1024	3	31	68

FFT / Karatsuba comparison


Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

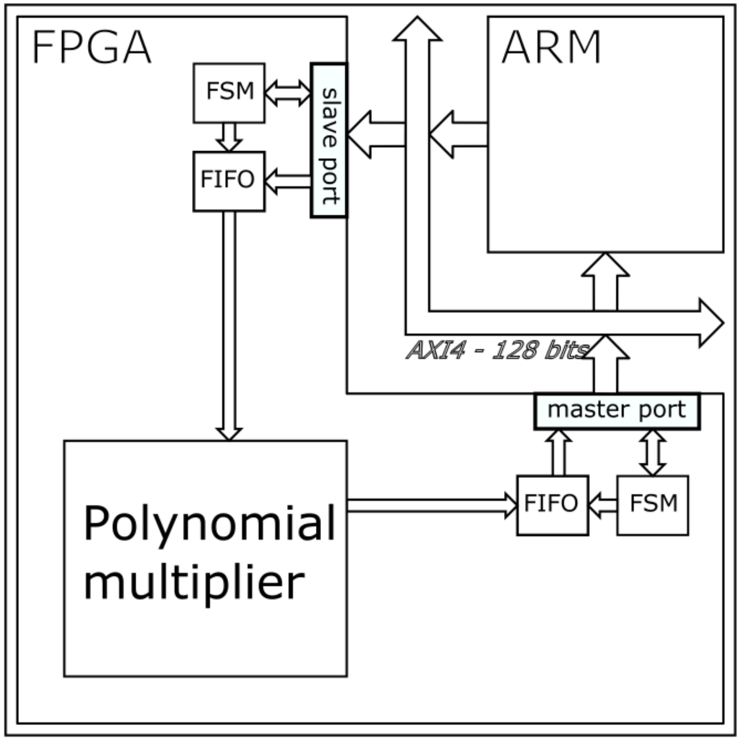
Co-processor architecture

Expected speedup

Coefficients per operation	Karatsuba	FFT NWC	FFT
4	19683	7936	17408
8	6561	3968	8704
16	2187	1984	4352
32	729	992	2176
64	243	496	1088
128	81	248	544
256	27	124	272
512	9	62	136
1024	3	31	68

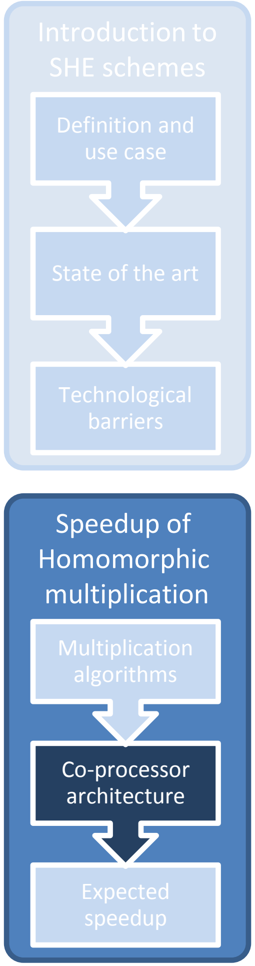
Second architecture

- Co-processor architecture:



- Limited bandwidth
- Limited hardware ressources

Impact on the FFT



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

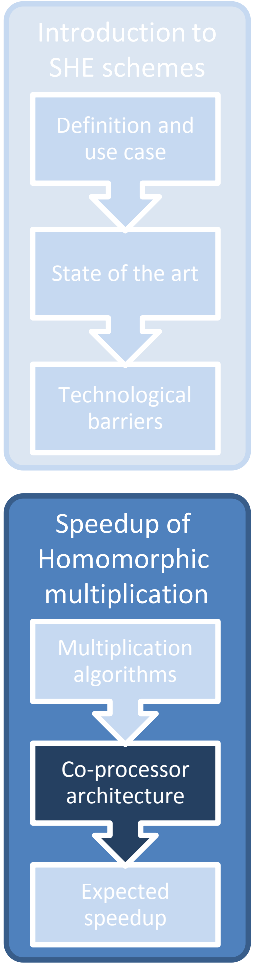
Expected speedup

- The first round of the FFT can be performed completely only if both polynomials are sent to the FPGA

- $$\frac{3n}{2m}log_2(n)+\frac{n}{m}$$

$$\rightarrow \frac{3n}{2m}(log_2(n)-1)+\frac{n}{m}+3n$$

Impact on the Karatsuba



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup

- Output coefficients can be pipelined.
- Scheduling of input/output coefficients.

FFT / Karatsuba comparison

Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

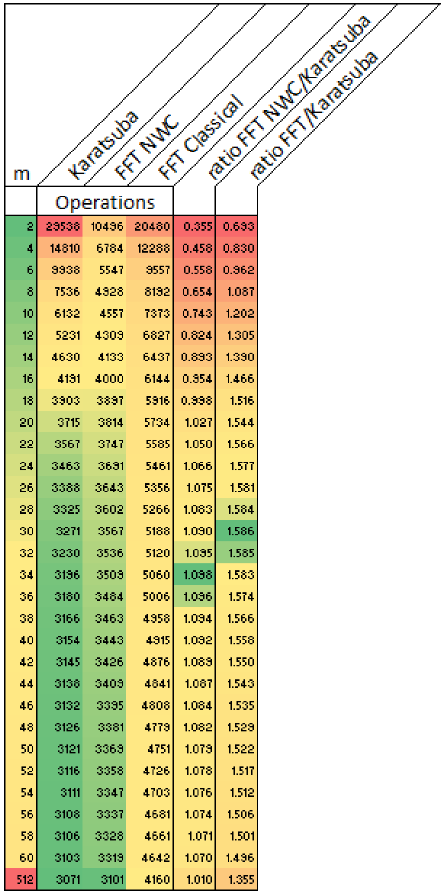
Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup

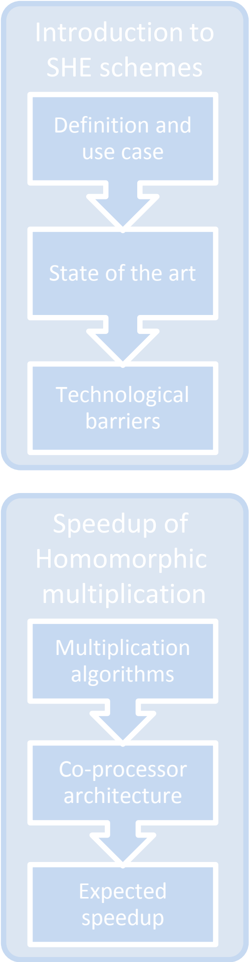
- $n = 1024 \quad ; \quad log_2(q) = 40$

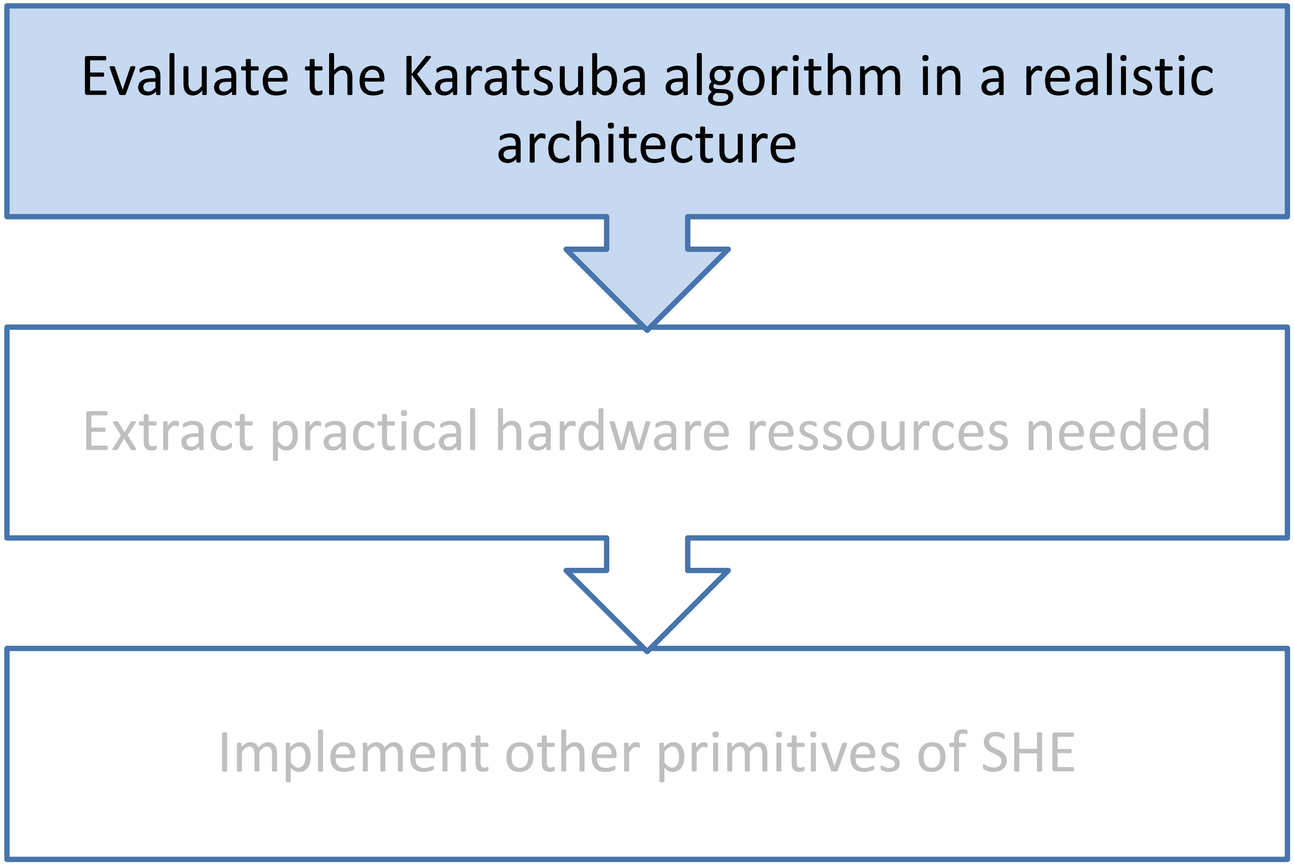


m	Karatsuba	FFT NWC	FFT Classical	ratio FFT NWC/Karatsuba	ratio FFT/Karatsuba
	Operations				
2	29538	10496	20480	0.355	0.693
4	14810	6784	12288	0.458	0.830
6	9938	5547	9557	0.558	0.962
8	7536	4928	8192	0.654	1.087
10	6132	4557	7373	0.743	1.202
12	5231	4309	6827	0.824	1.305
14	4630	4133	6437	0.893	1.390
16	4191	4000	6144	0.954	1.466
18	3903	3897	5916	0.998	1.516
20	3715	3814	5734	1.027	1.544
22	3567	3747	5585	1.050	1.566
24	3463	3691	5461	1.066	1.577
26	3388	3643	5356	1.075	1.581
28	3325	3602	5266	1.083	1.584
30	3271	3567	5188	1.090	1.586
32	3230	3536	5120	1.095	1.585
34	3196	3509	5060	1.098	1.583
36	3180	3484	5006	1.096	1.574
38	3166	3463	4958	1.094	1.566
40	3154	3443	4915	1.092	1.558
42	3145	3426	4876	1.089	1.550
44	3138	3409	4841	1.087	1.543
46	3132	3395	4808	1.084	1.535
48	3126	3381	4779	1.082	1.529
50	3121	3369	4751	1.079	1.522
52	3116	3358	4726	1.078	1.517
54	3111	3347	4703	1.076	1.512
56	3108	3337	4681	1.074	1.506
58	3106	3328	4661	1.071	1.501
60	3103	3319	4642	1.070	1.496
512	3071	3101	4160	1.010	1.355

Multipliers	Karatsuba	FFT NWC	Classical FFT
$\rightarrow 0$	✗	✓ ★★★★★	✗
≈ 30	✓ ★★★★★	✓ ★★★★	✓ ★★★
$\rightarrow \infty$	≈	✓ ★★	✓ ★★

Future Work


Introduction to SHE schemes
Definition and use case
State of the art
Technological barriers
Speedup of Homomorphic multiplication
Multiplication algorithms
Co-processor architecture
Expected speedup

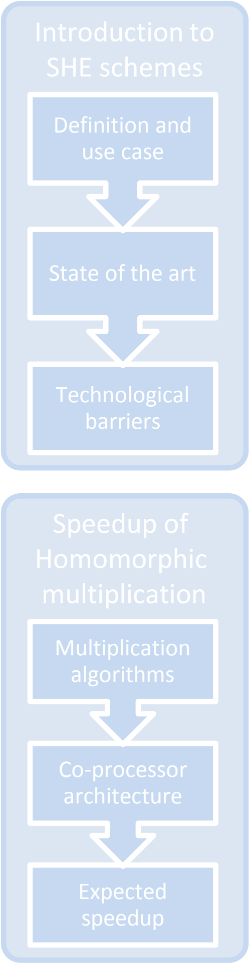


Evaluate the Karatsuba algorithm in a realistic architecture

Extract practical hardware ressources needed

Implement other primitives of SHE

Future Work



Introduction to SHE schemes

Definition and use case

State of the art

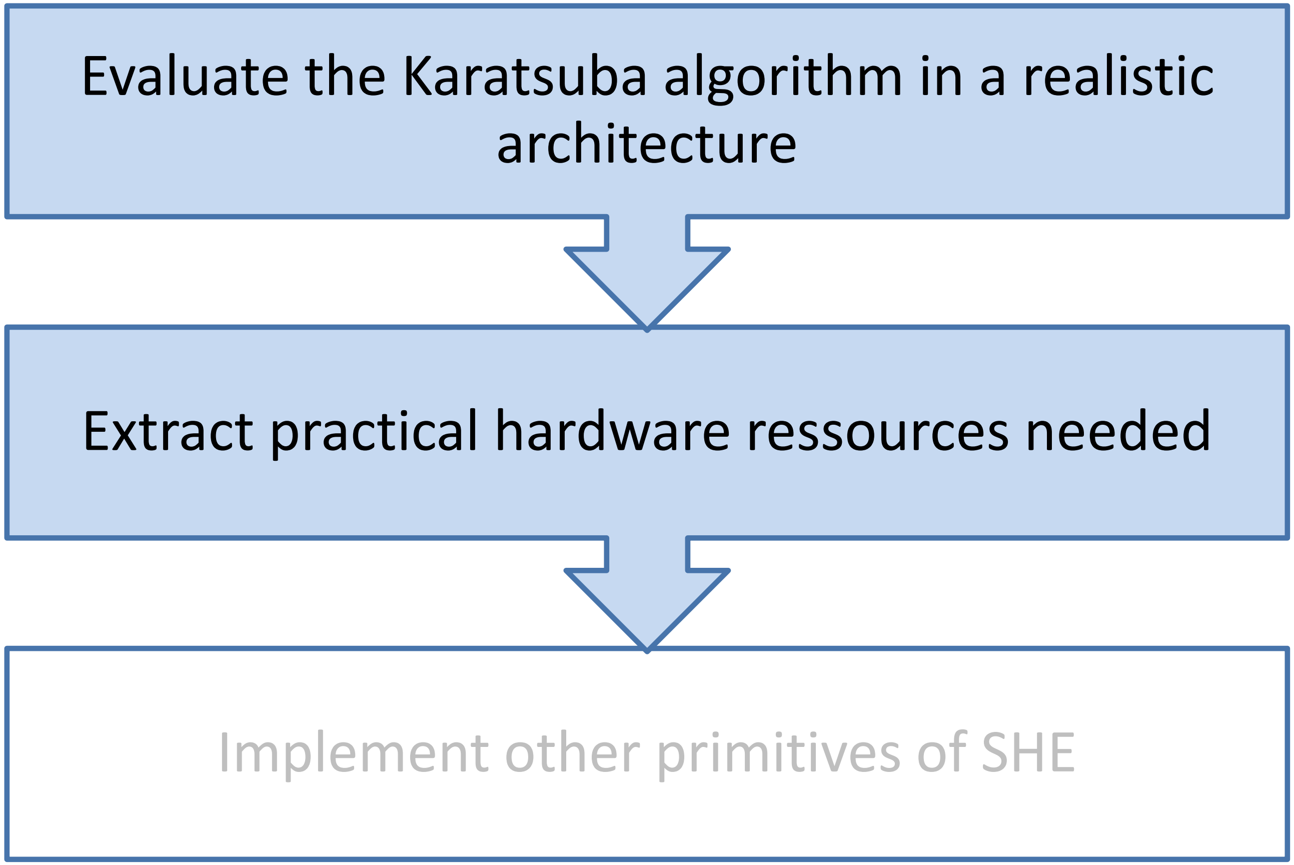
Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup

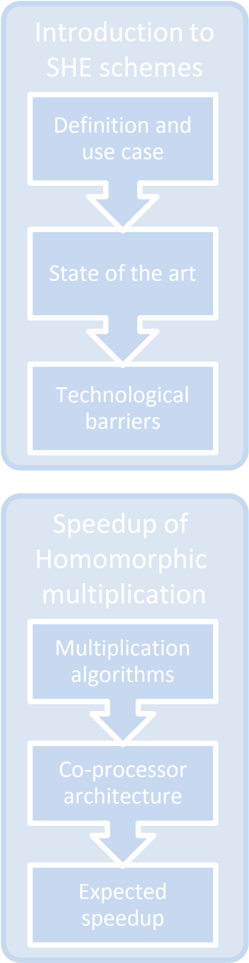


Evaluate the Karatsuba algorithm in a realistic architecture

Extract practical hardware ressources needed

Implement other primitives of SHE

Future Work



Introduction to SHE schemes

Definition and use case

State of the art

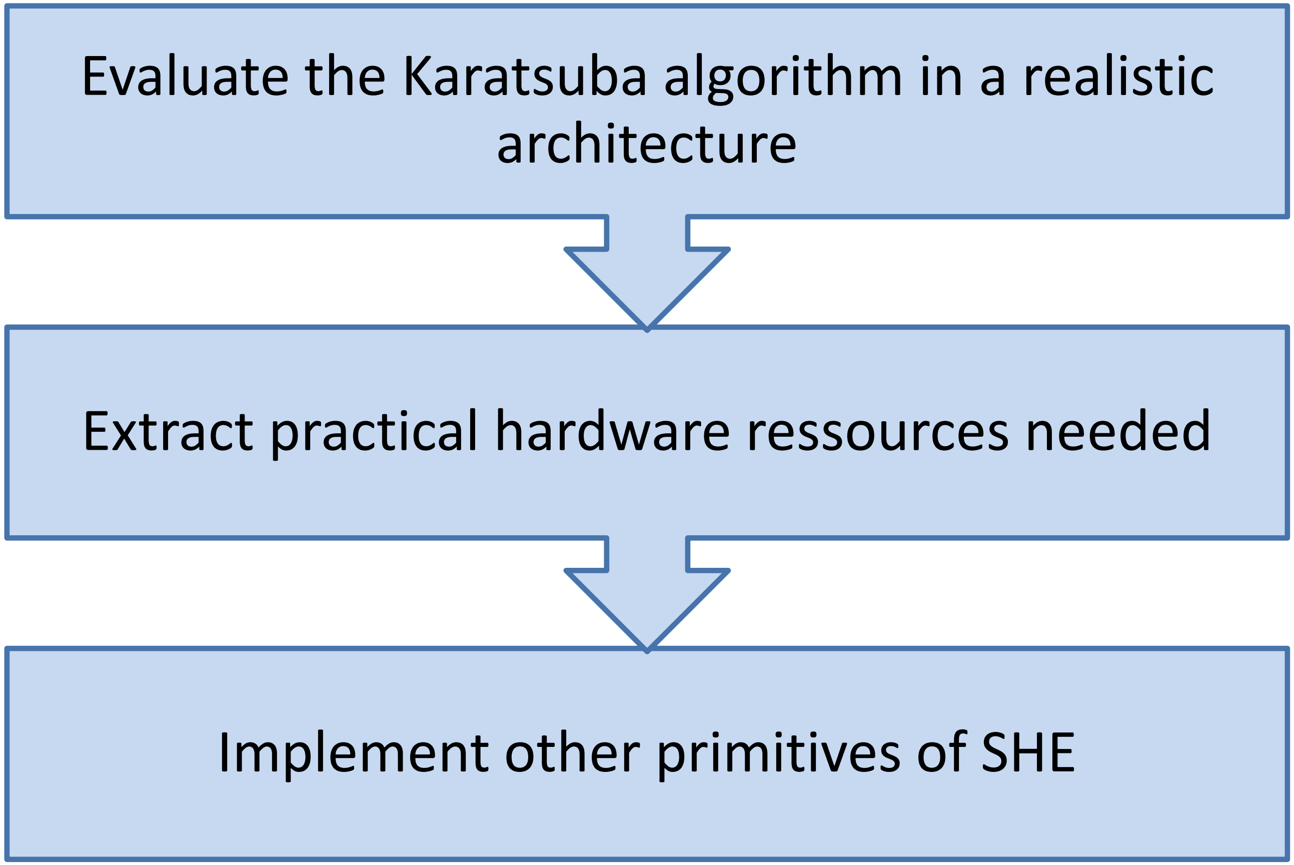
Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

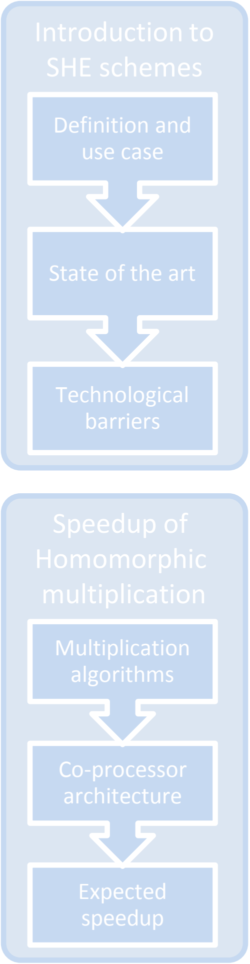
Expected speedup



Evaluate the Karatsuba algorithm in a realistic architecture

Extract practical hardware ressources needed

Implement other primitives of SHE



Introduction to SHE schemes

Definition and use case

State of the art

Technological barriers

Speedup of Homomorphic multiplication

Multiplication algorithms

Co-processor architecture

Expected speedup

Many thanks for your attention!