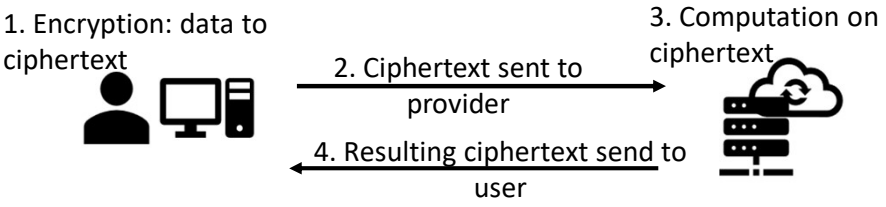
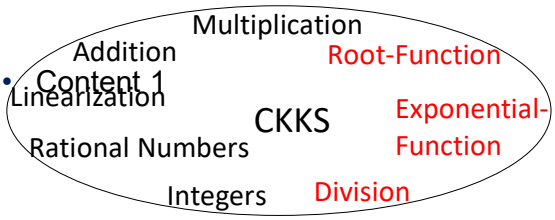
Title

Maximilian Krug - University of Würzburg, Germany

Background



Idea



- Content 1

Results

- Content 1

Problem

- Content 1

[1] Reference 1

Title

Maximilian Krug - University of Würzburg, Germany

Background

- Content 1

Idea

- Content 1

Results

- Content 1

Conclusion

- Content 1

[1] Reference 1

Title

Maximilian Krug - University of Würzburg, Germany

Background

- Content 1

Idea

- Content 1

Results

- Content 1

Conclusion

- Content 1

[1] Reference 1

Title

Maximilian Krug - University of Würzburg, Germany

Background

- Content 1

Idea

- Content 1

Results

- Content 1

Conclusion

- Content 1

[1] Reference 1

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Conference

Descartes research

Extension of the Homomorphic Cryptosystem BGV by Fixed-Point Number Arithmetic: Insights and Pitfalls

Maximilian Krug - University of Würzburg, Germany

Background

1. Encryption: data to ciphertext

2. Ciphertext sent to provider

3. Computation on ciphertext

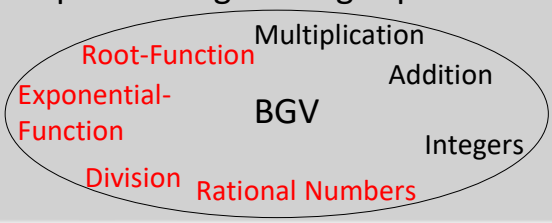
4. Resulting ciphertext send to user

1. What are the capabilities of step 3?
2. Are there different approaches to step 3?
3. How performend is step 3?

- Library: OpenFHE
- Implements: **BGV**, BFV and **CKKS** scheme
- **BGV** limited: rational numbers, division …

Idea

1. Implementing missing capabilities

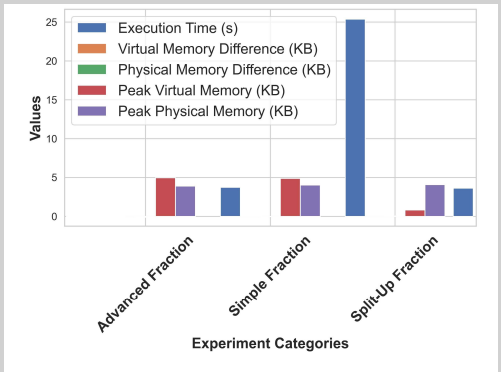


2. Testing performance and compare

Test Cases:
Multiple number representation, every function

Test Subject:
Completion time, Accuracy, RAM-/CPU usage

Preliminary Results



I will be aswell

I will contain much information

Conclusion

Here we see that much information and even more intel was gathered for a detailed and important conclusion.
From the last section we can conclude that this section is very much smart and gives us knowledge.
Furthermore we are going to say that more details will be needed for a deeper insight on the much good work.
But more test need to be conducted. Here would be space for your adverts.
This is just a mock up test to show how this could look like.

[1] Reference 1

Extension of the Homomorphic Cryptosystem BGV by Fixed-Point Number Arithmetic: Insights and Pitfalls

Maximilian Krug - University of Würzburg, Germany

Background

1. Encryption: data to ciphertext

2. Ciphertext sent to provider

3. Computation on ciphertext

4. Resulting ciphertext send to user

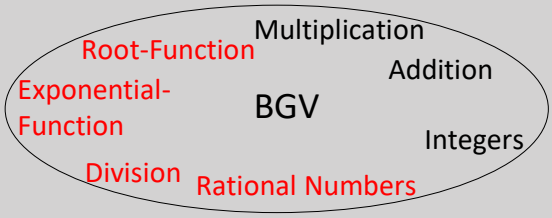
[1]

1. What are the capabilities of step 3?
2. Are there different approaches to step 3?
3. How performend is step 3?

- Library: OpenFHE
- Implements: **BGV**, BFV and **CKKS** scheme
- **BGV** limited: rational numbers, division …

Idea

1. Implementing missing capabilities



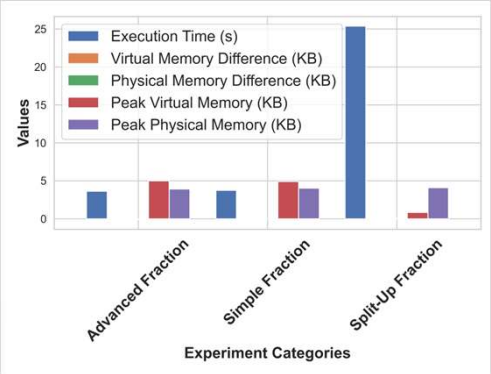
[2]

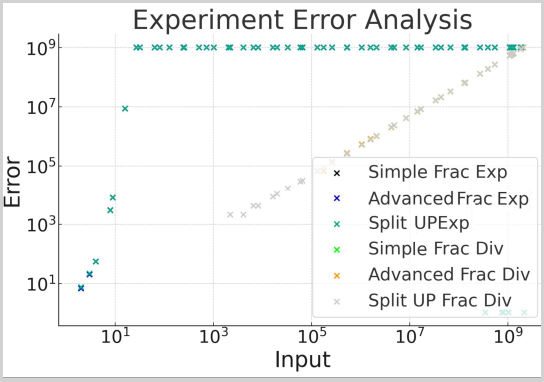
2. Testing performance and compare

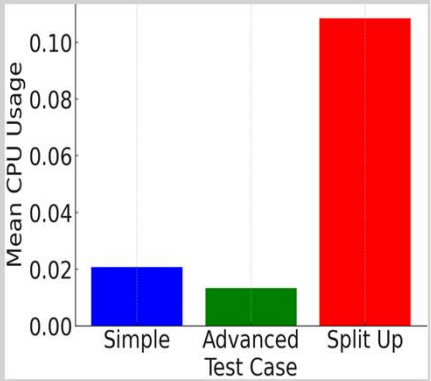
Test Cases:
Multiple number representation, every function

Test Subject:
Completion time, Accuracy, RAM-/CPU usage

Preliminary Results







Preliminary Conclusion

Here we see that much information and even more intel was gathered for a detailed and important conclusion.
From the last section we can conclude that this section is very much smart and gives us knowledge.
Furthermore we are going to say that more details will be needed for a deeper insight on the much good work.
But more test need to be conducted. Here would be space for your adverts.
This is just a mock up test to show how this could look like.

[3]

[1] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pp. 113–124, 2011.
[2] A. Al Badawi, J. Bates, F. Bergamaschi, D. B. Cousins, S. Erabelli, N. Genise, S. Halevi, H. Hunt, A. Kim, Y. Lee, et al., "Openfhe: Open-source fully homomorphic encryption library," in Proceedings of the 10th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, pp. 53–63, 2022
[3] T. Prantl, L. Horn, S. Engel, L. Iffländer, L. Beierlieb, C. Krupitzer, A. Bauer, M. Sakarvadia, I. Foster, and S. Kounev, "De bello homomorphico: Investigation of the extensibility of the openfhe library with basic mathematical functions by means of common approaches using the example of the ckks cryptosystem," International

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Descartes research

Extension of the Homomorphic Cryptosystem BGV by Fixed-Point Number Arithmetic: Insights and Pitfalls

Maximilian Krug - University of Würzburg, Germany

Background

1. Encryption: data to ciphertext

2. Ciphertext sent to provider

3. Computation on ciphertext

4. Resulting ciphertext send to user

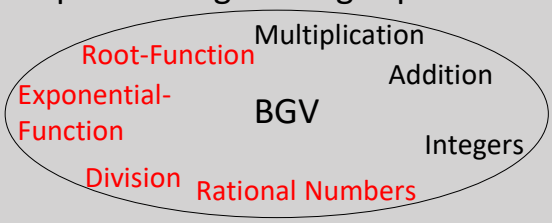
[1]

1. What are the capabilities of step 3?
2. Are there different approaches to step 3?
3. How performend is step 3?

- Library: OpenFHE
- Implements: **BGV**, BFV and **CKKS** scheme
- **BGV** limited: rational numbers, division …

Idea

1. Implementing missing capabilities



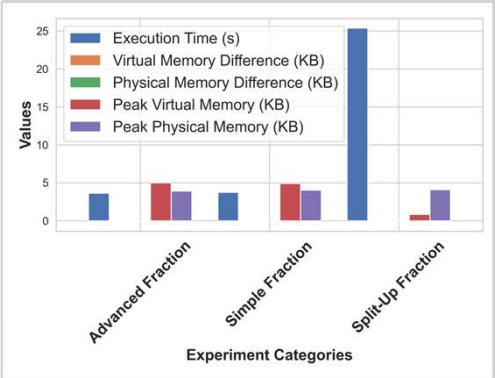
[2]

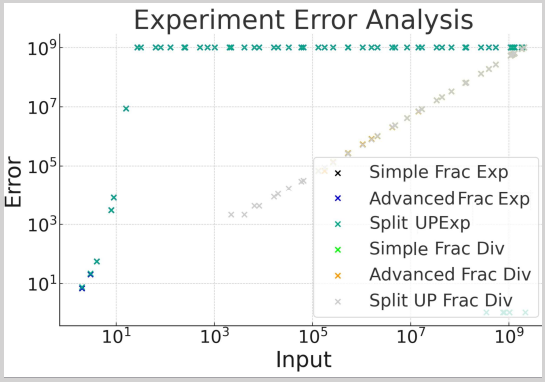
2. Testing performance and compare

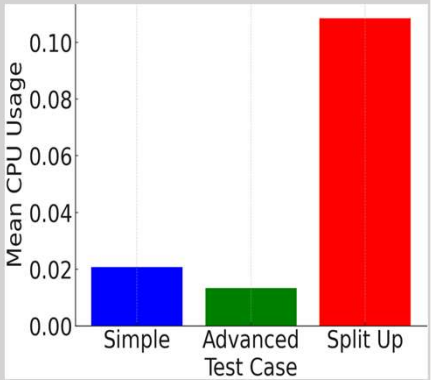
Test Cases:
Multiple number representation, every function

Test Subject:
Completion time, Accuracy, RAM-/CPU usage

Preliminary Results







Preliminary Conclusion

These are preliminary results, meaning that evaluation is not yet finalized, the current results conclude:

- Execution Time and CPU usage vary to most
- The Memory usage difference of less concern in terms of performance evaluation
- There is a trade-off between CPU usage and Accuracy to be made
- The accuracy of the functions especially exp() is highly depended on the input

[3]

References:
[1] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pp. 113–124, 2011.
[2] A. Al Badawi, J. Bates, F. Bergamaschi, D. B. Cousins, S. Erabelli, N. Genise, S. Halevi, H. Hunt, A. Kim, Y. Lee, et al., "Openfhe: Open-source fully homomorphic encryption library," in Proceedings of the 10th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, pp. 53–63, 2022
[3] T. Prantl, L. Horn, S. Engel, L. Iffländer, L. Beierlieb, C. Krupitzer, A. Bauer, M. Sakarvadia, I. Foster, and S. Kounev, "De bello homomorphico: Investigation of the extensibility of the openfhe library with basic mathematical functions by means