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

Bachelor Proposal Presentation

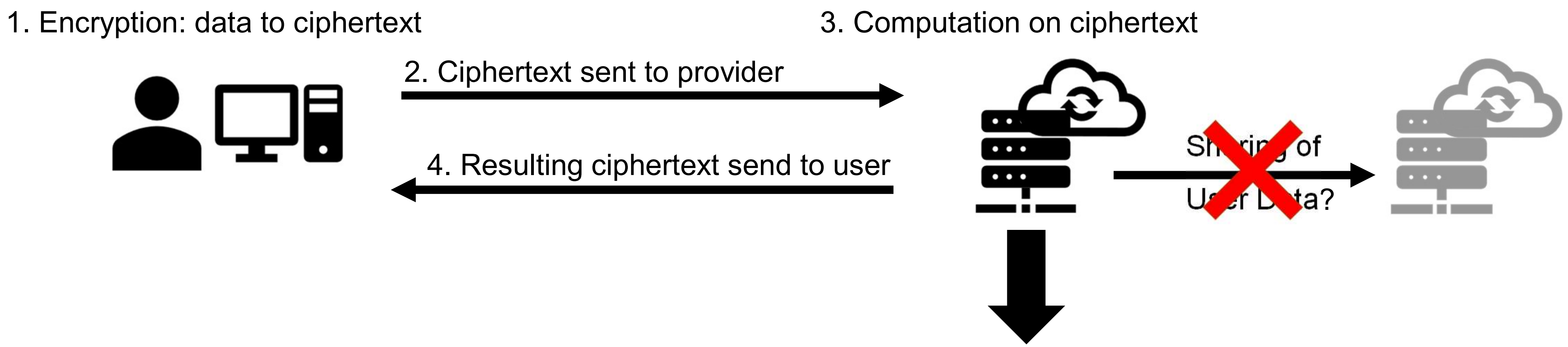
Author: Maximilian Krug

Advisors: Thomas Prantl and Simon Engel

01.02.2024

https://se.informatik.uni-wuerzburg.de

Overview



1. Encryption: data to ciphertext

2. Ciphertext sent to provider

3. Computation on ciphertext

4. Resulting ciphertext send to user

~~Sharing of User Data?~~

- Library: OpenFHE
- Implements: BGV, BFV and CKKS scheme
- Different support for each scheme

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

Answers from related work

Theoretical Capabilities?

- Features of the scheme
- Choice of parameters
- Mathematical boundries
- Mathematical capabilities

=> no mention of real world performance and difference

=> comparison of features or types only (FHE, SWHE)

[2,3,4,7]

Different Approaches?

- Comparison of multiple self implemented schemes
- Multitude of languages
- Limited capabilities

=> evaluation difficult

=> niche usecases

[5,6,9,10,11]

Performance?

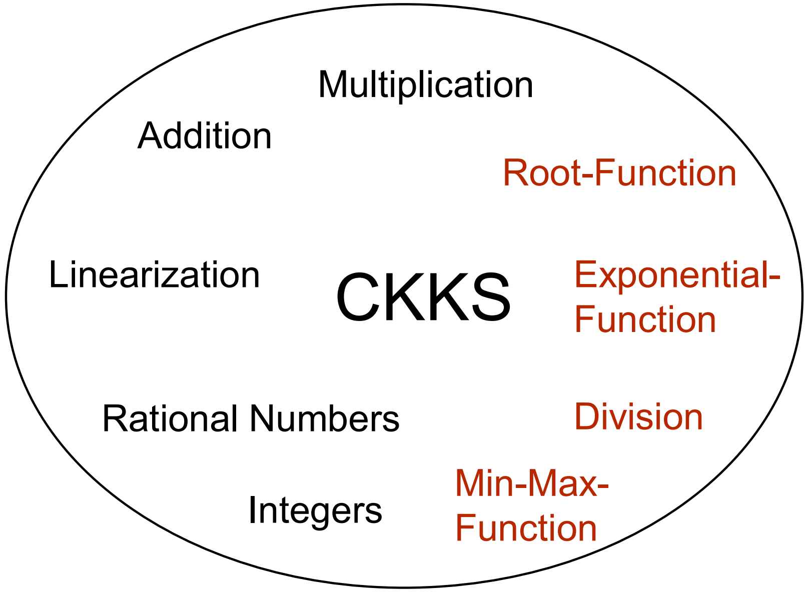
- Mostly built-in functions
- Measurement of completion time only
- Different libraries

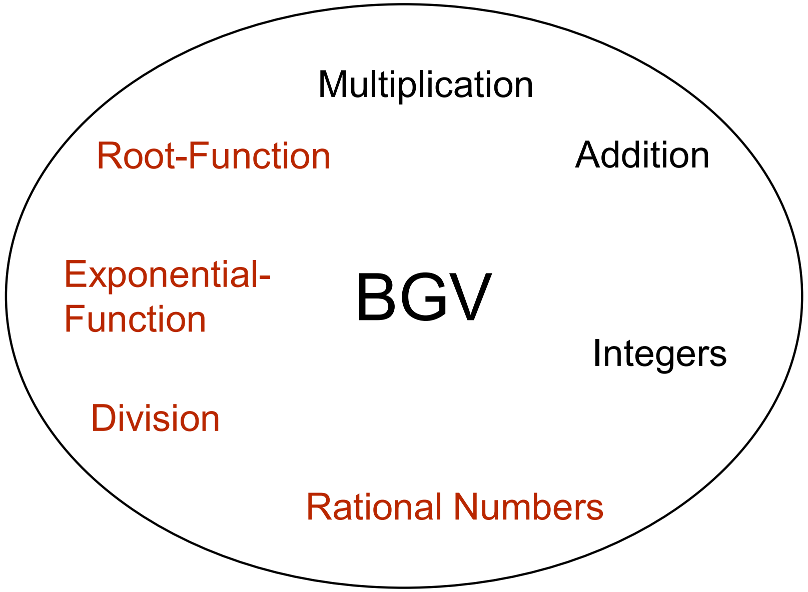
=> no high level functions using the capabilities

=> no depth in evaluation

[1,9]

Approach to Implementation





Performance Testing

Test Cases:

- Every number representation
- Every function (Division …)

Test Subject:

- Completion time
- Accuracy
- RAM usage
- CPU usage

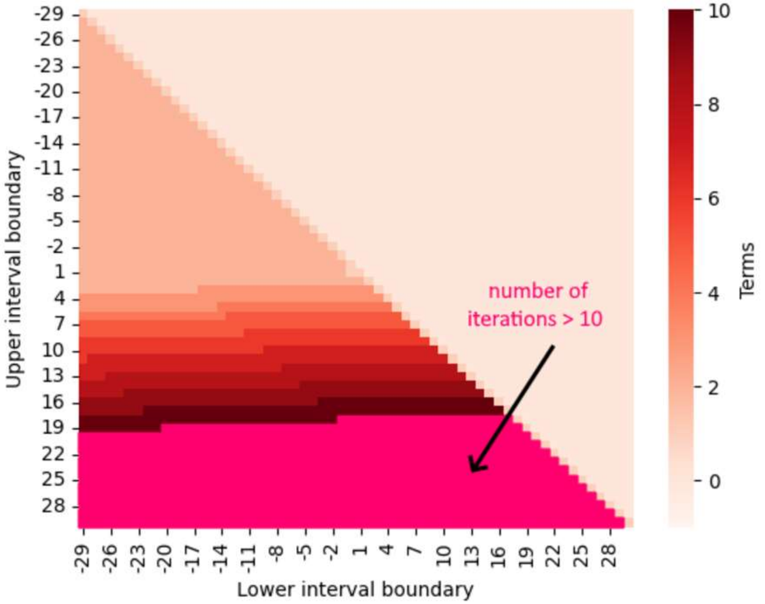
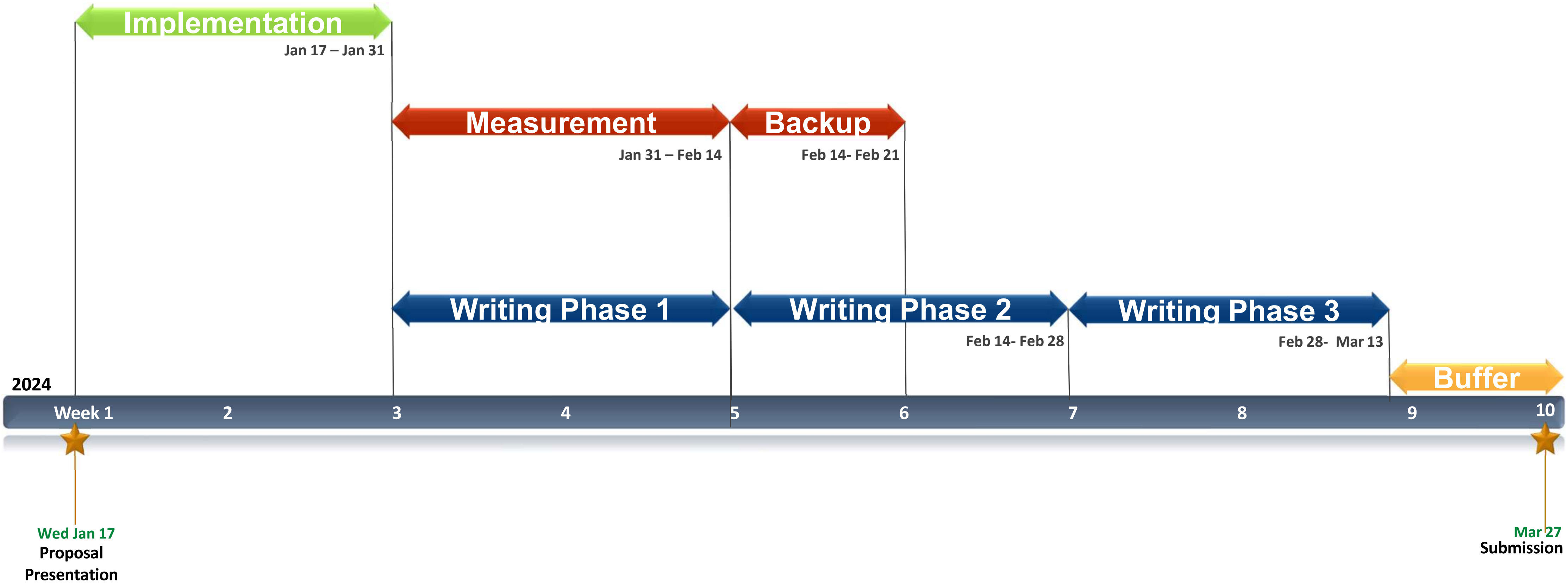


Fig. 5: Visualization of the required iterations to compute the exponential function for values from different intervals with an accuracy of 0.1.
[9]

Time Management



Implementation

Jan 17 – Jan 31

Measurement

Jan 31 – Feb 14

Backup

Feb 14- Feb 21

Writing Phase 1

Writing Phase 2

Feb 14- Feb 28

Writing Phase 3

Feb 28- Mar 13

Buffer

2024

Week 1 2 3 4 5 6 7 8 9 10

Wed Jan 17
Proposal
Presentation

Mar 27
Submission

Risk Management

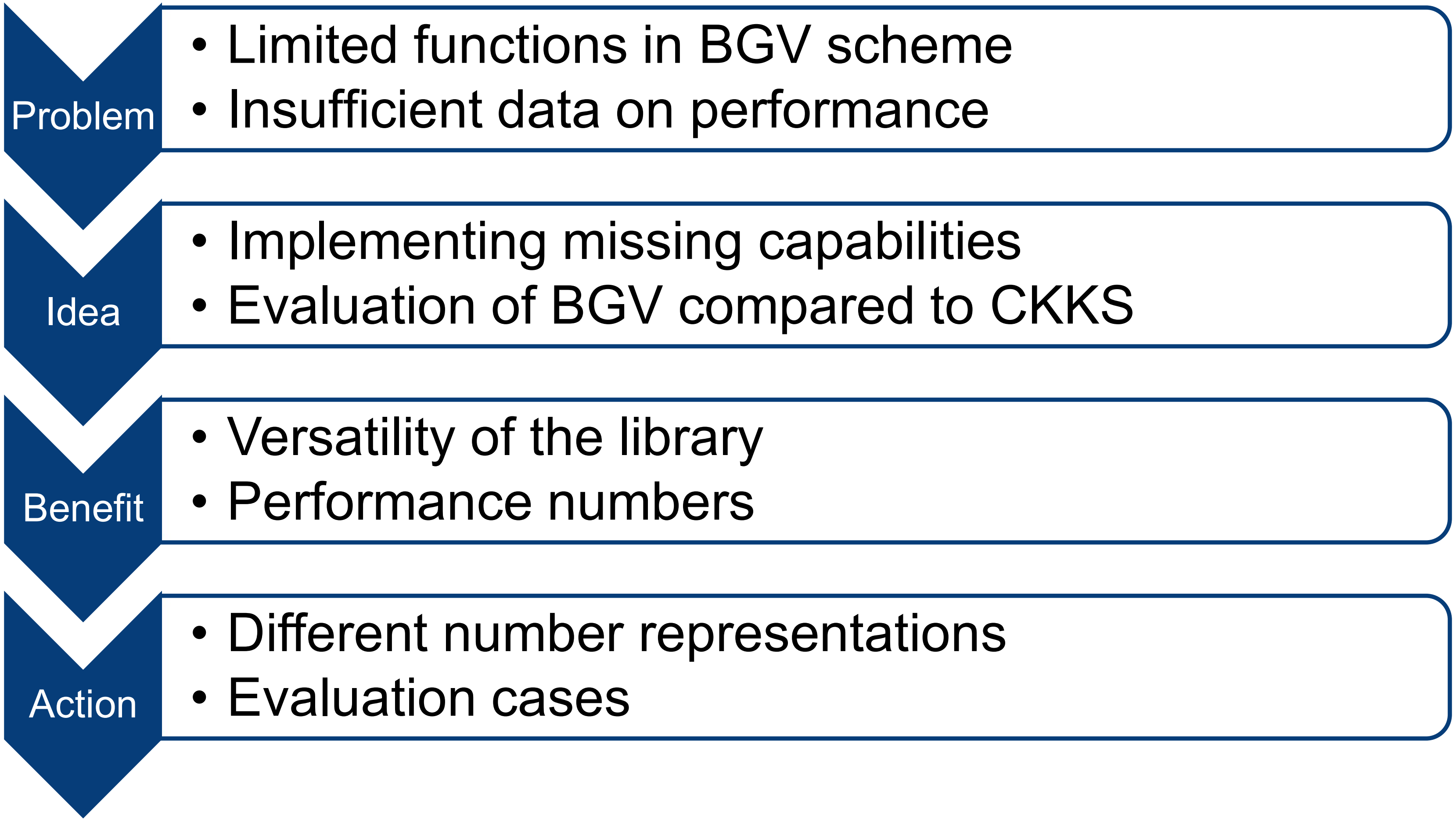
Risks:

- ➢ Mathematical bounds/ parameters
- ➢ Testing
  - Time for test suite
  - Values invalid
- ➢ Results inconclusive due to variance

Solutions:

- ➢ Evaluating with disclosed errors
- ➢ Multiple test cases
  - Reduced number of intervals
  - Multitute of parameters
- ➢ General information

Conclusion



Problem

- Limited functions in BGV scheme
- Insufficient data on performance

Idea

- Implementing missing capabilities
- Evaluation of BGV compared to CKKS

Benefit

- Versatility of the library
- Performance numbers

Action

- Different number representations
- Evaluation cases

Sources:

- [1] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, “A survey on homomorphic encryption schemes: Theory and implementation,” ACM Computing Surveys (Csur), vol. 51, no. 4, pp. 1–35, 2018.

- [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] 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.

- [4] J. Willmert, “Numerically computing the exponential function with polynomial approximations,” 2020. Last accessed on 07.12.2023.

- [5] M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, K. Lauter, et al., “Homomorphic encryption standard,” Protecting privacy through homomorphic encryption, pp. 31–62, 2021.

- [6] V. Rocha, J. L´opez, and V. F. Da Rocha, “An overview on homomorphic encryption algorithms,” UNICAMP Universidade Estadual de Campinas, Tech. Rep, 2018. 27 28 Bibliography

- [7] T. Lepoint and M. Naehrig, “A comparison of the homomorphic encryption schemes fv and yashe,” in Progress in Cryptology–AFRICACRYPT 2014: 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings 7, pp. 318–335, Springer, 2014.

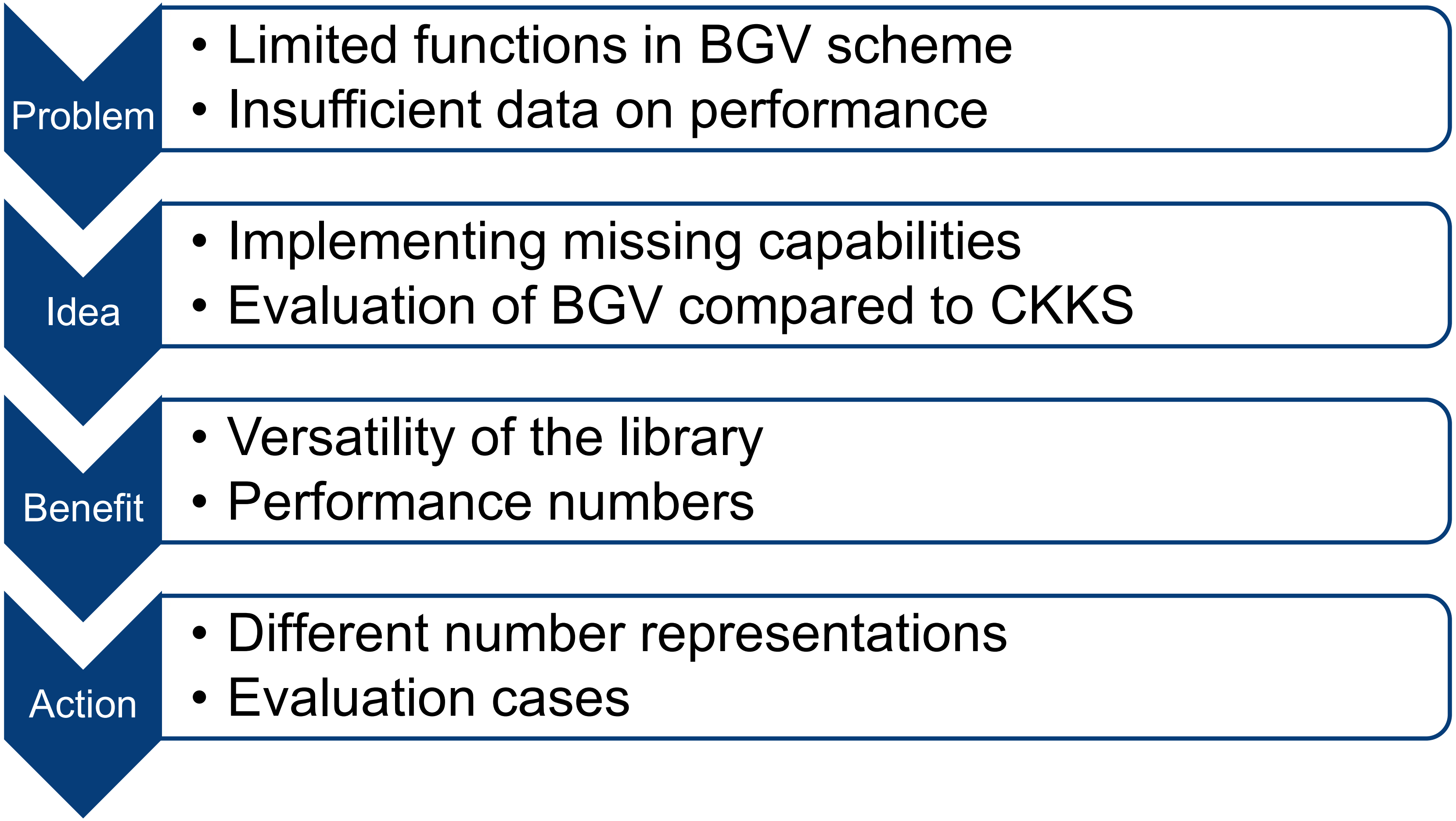
- [8] A. Kim, A. Papadimitriou, and Y. Polyakov, “Approximate homomorphic encryption with reduced approximation error,” in Cryptographers’ Track at the RSA Conference, pp. 120–144, Springer, 2022.

- [9] T. Prantl, L. Horn, S. Engel, L. Iffl ̈ander, 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 Journal of Information Security, pp. 1–21, 2023.

- [10] J.-W. Lee, H. Kang, Y. Lee, W. Choi, J. Eom, M. Deryabin, E. Lee, J. Lee, D. Yoo, Y.- S. Kim, and J.-S. No, “Privacy-preserving machine learning with fully homomorphic encryption for deep neural network,” IEEE Access, vol. 10, pp. 30039–30054, 2022.

- [11] W. Ao and V. N. Boddeti, “Autofhe: Automated adaption of cnns for efficient evaluation over fhe.” Cryptology ePrint Archive, Paper 2023/162, 2023.

Conclusion



Problem

- Limited functions in BGV scheme
- Insufficient data on performance

Idea

- Implementing missing capabilities
- Evaluation of BGV compared to CKKS

Benefit

- Versatility of the library
- Performance numbers

Action

- Different number representations
- Evaluation cases

Number Representation

- Example: 6.453
- 1. Expand to fraction with power of ten

$$6.453 = \frac{6.453 \times 1000}{1000} = \frac{6453}{1000}$$

- 2. Encode as vector

$$\begin{pmatrix} 6453 \\ 1000 \end{pmatrix}$$

- 3. Encrypt to ciphertext

- Example: 6.453 – but different
- What if the vector is extended?

$$\begin{pmatrix} 6453 \\ 1000 \\ 6453 \\ 0 \end{pmatrix}$$

- What if the nominator and denominator are different vectors?

$$\begin{pmatrix} 6 \\ 4 \\ 5 \\ 3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$