New Tool Release

PySEAL: A Python wrapper implementation of the SEAL homomorphic encryption library

Alexander J. Titus 1,2,4, Shashwat Kishore3,4, Todd Stavish3, Stephanie M. Rogers1, and Karl Ni3,*

1B.Next, IQT Labs, Arlington, VA, 22201, USA
2Quantitative Biomedical Sciences, Dartmouth School of Graduate and Advanced Studies, Hanover, NH, 03755, USA
3Lab41, IQT Labs, Menlo Park, CA, 94025, USA
4Authors contributed equally
*To whom correspondence should be addressed.

Primary Authors: AJ Titus & S Kishore
Published on March 05, 2018

Abstract

Motivation: The ability to perform operations on encrypted data has a growing number of applications in bioinformatics, with implications for data privacy in health care and biosecurity. The SEAL library is a popular implementation of fully homomorphic encryption developed in C++ by Microsoft Research. Despite the advantages of C++, Python is a flexible and dominant programming language that enables rapid prototyping of bioinformatics pipelines.

Results: In an effort to make homomorphic encryption accessible to a broader range of bioinformatics scientists and applications, we present a Python binding implementation of the popular homomorphic encryption library, SEAL, using pybind11. The software contains a Docker image to facilitate easy installation and execution of the SEAL build process.

Availability: All code is publicly available at https://github.com/Lab41/PySEAL

Contact: lab41@iqt.org

Supplementary information: Supplementary information is available on the Lab41 GitHub.

1 Introduction

The volume of available genomic data is growing rapidly as the cost of sequencing continues to decline. Biomedical research advances can greatly benefit from this wealth of data, but the sensitive nature of such information demands that privacy and security concerns be given full attention. For example, recent work has demonstrated an ability to re-identify individuals using their genomic data (Gymrek et al., 2013; Lippert et al., 2017). Furthermore, many analyses, such as the Genome Wide Association Studies (GWAS), require large sample sizes that are often difficult to collect at a single clinical site, which highlights the challenge of maintaining the security of sensitive data being collected and shared among multiple platforms at multiple geographic locations.

In 2010, the Center for Integrating Data for Analysis, Anonymization and SHaring (iDASH) was founded at the University of California, San Diego to address privacy challenges to research progress. At the annual iDASH Privacy & Security Workshop, teams from around the world develop novel methods for private and secure computation on health data, and extend the applications of homomorphic encryption into the areas of biological data storage, transport, and computation (Kim and Lauter, 2015).

Homomorphic Encryption offers a promising approach to addressing privacy and security concerns in the handling of sensitive genomic data, because it allows data to remain encrypted even during use, and it offers a security method to enable comparisons across disparate hardware and geographic distances. Under a fully homomorphic encryption cryptoscheme (Gentry, 2009), any arbitrary set of operations that take place on the ciphertext (encrypted space) are mirrored in unencrypted space (Figure 1).

Here, we present a Python binding of the Simple Encrypted Arithmetic Library (SEAL) homomorphic encryption library (Chen and Laine, 2017). SEAL is maintained by the Cryptography Research Group at Microsoft Research and implements a fully homomorphic encryption scheme in C++. The software has strong applications in bioinformatics (Dowlin et al., 2017). While C++ is appropriate for software engineering and developed
Therefore, we present PySEAL, a Python wrapper implementation of the SEAL library using pybind11. The PySEAL package implements SEALv2.3 and the package is under active maintenance.

2 Methods

PySEAL is a Python wrapper for the Simple Encrypted Arithmetic Library (SEAL) homomorphic encryption library. The PySEAL software is implemented using pybind11 and is released as a Docker container, a C++ SEAL example build, and a Python wrapper build. The software also includes bash scripts to build the Docker container and execute a series of examples using PySEAL functions.

The PySEAL code is released on the Lab41 Github page (https://github.com/Lab41/PySEAL) and is under active maintenance. The README includes an overview description of the steps to instantiate and use the homomorphic encryption scheme.

Briefly, the first step to using the library for basic encryption tasks is to instantiate a new EncryptionParameters object and set its modulus attributes. These parameters are stored in a SEALContext object which checks the validity of the parameters. Once validated, these parameters are used to create encryption keys and Encryptor and Decryptor objects.

For operations, IntegerEncoder and Evaluator objects are included to encrypt input data and perform operations on the ciphertext. SEALv2.3 includes functionality to compute operations between ciphertext and plaintext, allowing for runtime improvements due to reduced encryption overhead.

3 Applications

The combination of such operations has enabled encrypted mutation searching (Çetin et al. 2017) and encrypted bloom filter searching for sequence-to-sequence comparisons. Other recent bioinformatics applications of homomorphic encryption schemes include the computation of edit distances (Çetin et al. 2018), goodness of fit testing (Lauter et al. 2014), linkage disequilibrium measurement (Lauter et al. 2014), minor allele frequency computations (Kim and Lauter 2015), and chi-square statistic computations (Kim and Lauter 2015).

The homomorphic encryption package has many applications outside genomics as well. For example, homomorphic encryption has recently been used in conjunction with other methods to implement biometric authentication schemes (Karabat et al. 2015) and secure E-commerce recommendation systems (Ahila and Shunmuganathan 2015). In general, homomorphic encryption could potentially be used for any of a host of tasks that involve multiple parties sharing sensitive data.

4 Conclusion

Homomorphic encryption is a promising application for secure computation in biomedical research and clinical data applications. The C++ SEAL software from Microsoft Research is under active development for performance improvements, as homomorphic encryption algorithm runtime is a limiting factor to deploying homomorphic encryption in production systems. With PySEAL, we reduce the challenge of developing in C++ and provide the bioinformatics research community with a tool to quickly prototype and iterate on new methods, allowing performance and implementations to progress in parallel.

Acknowledgements

The authors thank Lisa Porter for her continued support and guidance. This work was supported in part by a Big Data to Knowledge (BD2K) training grant to AJT (T32LM012204).

References

Ahila, S. S. and Shunmuganathan, K. L. (2015). Role of agent technology in web usage mining: Homomorphic encryption based recommendation for e-commerce applications. Wireless Personal Communications.

Çetin, G. S.; Chen, H.; Lauer, K.; Lauter, K.; Rindal, P.; and Xia, Y. (2017). Private queries on encrypted genomic data. BMC Medical Genomics, 10(4), 45.

Chen, H. and Lauer, K. (2017). Simple Encrypted Arithmetic Library - SEAL v2.2. Technical report.

Cheor., J. H.; Kim, M., and Lauter, K. (2015). Homomorphic computation of edit distance. Financial Cryptography and Data Security.

Dowlin, N.; Gilad-Bachrach, R.; Lauer, K.; Lauter, K.; Naehrig, M.; and Werning, J. (2015). Manual for using homomorphic encryption for bioinformatics. Proceedings of the IEEE, 105(3), 552–567.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In STOC, volume 9, pages 697–708.

Gynmek, M.; McGuire, A. L.; Golan, D.; Halperin, E.; and Erelsh, Y. (2013). Identifying Personal Genomes by Same Name Inference. Science, 339(6147), 321–324.

Karabat, M.; Mehmet, S. K.; Erdoghan, G.; and Savas, E. (2015). Thrive: threshold homomorphic encryption based secure and privacy preserving biometric verification system. EURASIP Journal on Advances in Signal Processing.

Kim, M. and Lauter, K. (2015). Private genome analysis through homomorphic encryption. BMC medical informatics and decision making, 15(5), 83.

Lauter, K.; Lopez-Alt, A., and Naehrig, M. (2014). Private computation on encrypted genomic data. Progress in Cryptology.

Lippert, C.; Sabatini, R.; Måler, M. C.; Kang, E. Y.; Lee, S.; Atikan, O.; Harley, A.; Bernal, A.; Guri, P.; Lavenko, V.; Voucas, K.; Wong, Y.; Zhu, M.; Yang, W.-Y.; Chang, C.; Lu, T.; Lee, C. W. H.; Hicks, B.; Ramakrishnan, S.; Tang, H.; Xie, C.; Piper, J.; Bresson, S.; Tarpay, Y.; Telenti, A.; Rohy, R. K.; Och, F. J., and Venter, J. C. (2017). Identification of individuals by trait prediction using whole-genome sequencing data. Proceedings of the National Academy of Sciences, 114(38), 10166–10171.