# OpenFHE – Open-Source Fully Homomorphic Encryption Library

Ahmad Al Badawi[1], Jack Bates[1], Flavio Bergamaschi[2], David Bruce Cousins[1], Saroja Erabelli[1], Nicholas Genise[1], Shai Halevi[3], Hamish Hunt[2], Andrey Kim[4], Yongwoo Lee[4], Zeyu Liu[1], Daniele Micciancio[1,5], Ian Quah[1], Yuriy Polyakov[1], Saraswathy R.V. [1], Kurt Rohloff[1], Jonathan Saylor[1], Dmitriy Suponitsky[1], Matthew Triplett[1], Vinod Vaikuntanathan[1,6], Vincent Zucca[7,8]

[1]Duality Technologies, [2]Intel Corporation, [3]Algorand Foundation, [4]Samsung Advanced Institute of Technology, [5]University of California, San Diego, [6]Massachusets Institute of Technology, [7]DALI, Universit´e de Perpignan Via Domitia, [8]LIRMM, University of Montpellier

## Key Facts

OpenFHE, a new open-source C++17 FHE software library that incorporates selected design ideas from prior FHE projects, such as PALISADE, HElib, HEAAN, and FHEW, and includes several new design concepts and ideas [1].

The main new design features can be summarized as follows:

- We assume from the very beginning that all implemented FHE schemes will support bootstrapping and scheme switching;
- OpenFHE supports multiple hardware acceleration backends using a standard Hardware Abstraction Layer (HAL);
- OpenFHE includes both user-friendly modes, where all maintenance operations, such as modulus switching, key switching, and bootstrapping, are automatically invoked by the library, and compiler-friendly modes, where an external compiler makes these decisions.

OpenFHE includes efficient implementations of all common FHE schemes:

- ✓ Brakerski/Fan-Vercauteren (BFV) scheme for integer arithmetic
- ✓ Brakerski-Gentry-Vaikuntanathan (BGV) scheme for integer arithmetic
- ✓ Cheon-Kim-Kim-Song (CKKS) scheme for real-number arithmetic (includes approximate bootstrapping)
- ✓ Ducas-Micciancio (DM) and Chillotti-Gama-Georgieva-Izabachene (CGGI) schemes for Boolean circuit evaluation

OpenFHE also includes the following multiparty extensions of FHE:

- ✓ Threshold FHE for BGV, BFV, and CKKS schemes
- ✓ Proxy Re-Encryption for BGV, BFV, and CKKS schemes

OpenFHE complies with the HomomorphicEncryption.org post-quantum security standards for homomorphic encryption. We offer OpenFHE under the 2-clause BSD open-source license, making it easier to wrap and redistribute OpenFHE in products.

OpenFHE is generously supported by DARPA. OpenFHE is a community-driven open-source project developed by a diverse group of contributors from both industry and academia, including Duality, Samsung, Intel, MIT, UCSD, and others. Google Transpiler [2] uses OpenFHE as an FHE backend. OpenFHE is formally affiliated with the NumFocus stable of open-source software projects.

## New Features as Compared to PALISADE

Includes all prior FHE functionality of PALISADE.

Also includes the following new features:

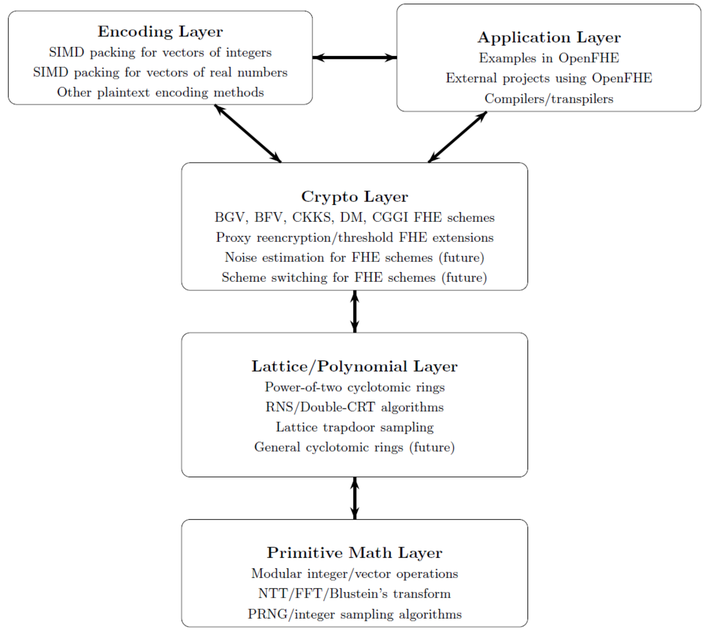
- ✓ Adds support for multiple hardware acceleration backends using a Hardware Abstraction Layer feature; includes a backend for Intel HEXL library [3]
- ✓ New BGV and BFV RNS variants proposed in [4]
- ✓ A new CKKS RNS variant proposed in [5]
- ✓ A full RNS implementation of CKKS bootstrapping
- ✓ Large-precision comparison and other algorithms proposed in [6]

## OpenFHE Scheme Support Matrix

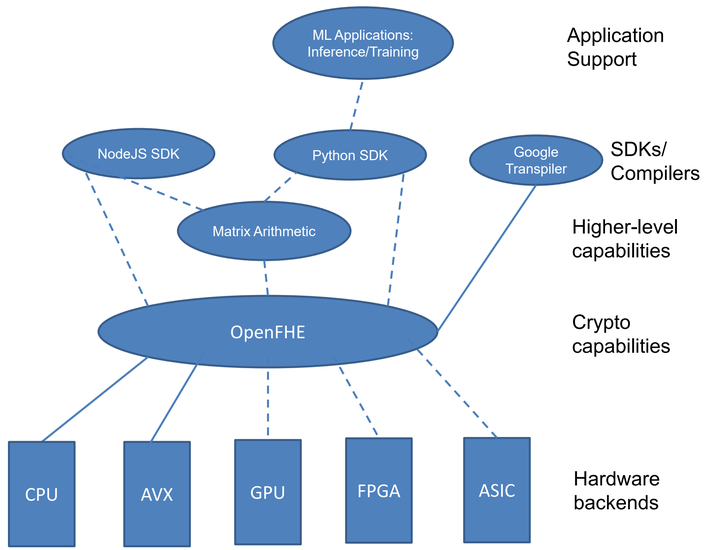
| Library/ Scheme or Extension | BGV | BGV Bootstr. | BFV | CKKS | CKKS Bootstr. | DM | CGGI | Threshold FHE (MP) | PRE (MP) |
|---|---|---|---|---|---|---|---|---|---|
| Concrete | | | | | | | ✓ | | |
| **FHEW** | | | | | | ✓ | | | |
| **HEAAN** | | | | ✓ | ✓ | | | | |
| **HELib** | ✓ | ✓ | | ✓ | | | | | |
| Lattigo | | | ✓ | ✓ | ✓ | | | ✓ | |
| **OpenFHE** | ✓ | * | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **PALISADE** | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| SEAL | ✓ | | ✓ | ✓ | | | | | |
| TFHE | | | | | | | ✓ | | |

* - prototype exists, but not part of release

## Layers in OpenFHE (Contributor View)




## Broader OpenFHE Community (User View)




## Further Information

Main resources and links for OpenFHE:

- ✓ OpenFHE design paper: https://eprint.iacr.org/2022/915
- ✓ OpenFHE website: https://openfhe.org
- ✓ ReadTheDocs documentation for OpenFHE: https://openfhe-development.readthedocs.io/en/latest/
- ✓ OpenFHE development repository: https://github.com/openfheorg/openfhe-development
- ✓ OpenFHE github organization where various OpenFHE-dependent projects are housed: https://github.com/openfheorg
- ✓ Community Forum for OpenFHE: https://openfhe.discourse.group/

## Contact

Yuriy Polyakov
Email: ypolyakov@openfhe.org
Website: https://openfhe.org/

## References

1. Ahmad Al Badawi and Jack Bates and Flavio Bergamaschi and David Bruce Cousins and Saroja Erabelli and Nicholas Genise and Shai Halevi and Hamish Hunt and Andrey Kim and Yongwoo Lee and Zeyu Liu and Daniele Micciancio and Ian Quah and Yuriy Polyakov and Saraswathy R.V. and Kurt Rohloff and Jonathan Saylor and Dmitriy Suponitsky and Matthew Triplett and Vinod Vaikuntanathan and Vincent Zucca, OpenFHE: Open-Source Fully Homomorphic Encryption Library, Cryptology ePrint Archive, Paper 2022/915, 2022.
2. Shruthi Gorantala and Rob Springer and Sean Purser-Haskell and William Lam and Royce Wilson and Asra Ali and Eric P. Astor and Itai Zukerman and Sam Ruth and Christoph Dibak and Phillipp Schoppmann and Sasha Kulankhina and Alain Forget and David Marn and Cameron Tew and Rafael Misoczki and Bernat Guillen and Xinyu Ye and Dennis Kraft and Damien Desfontaines and Aishe Krishnamurthy and Miguel Guevara and Irippuge Milinda Perera and Yurii Sushko and Bryant Gipson, A General Purpose Transpiler for Fully Homomorphic Encryption, Cryptology ePrint Archive, Paper 2021/811, 2021.
3. Fabian Boemer and Sejun Kim and Gelila Seifu and Fillipe D. M. de Souza and Vinodh Gopal, Intel HEXL: Accelerating Homomorphic Encryption with Intel AVX512-IFMA52, Cryptology ePrint Archive, Paper 2021/420, 2021.
4. Andrey Kim and Yuriy Polyakov and Vincent Zucca, Revisiting Homomorphic Encryption Schemes for Finite Fields, ASIACRYPT 2021.
5. Andrey Kim and Antonis Papadimitriou and Yuriy Polyakov, Approximate Homomorphic Encryption with Reduced Approximation Error, CT-RSA 2022.
6. Zeyu Liu and Daniele Micciancio and Yuriy Polyakov, Large-Precision Homomorphic Sign Evaluation using FHEW/TFHE Bootstrapping, Cryptology ePrint Archive, Paper 2021/1337, 2021.