

CONSORTIUM COMMUNICATION ASSET



AERO Project - Press Release

AXHEL Library

Headline	AERO Accelerates Homomorphic Encryption on Arm with AXHEL
Date	18 September 2026
Location	Pisa, Italy
Lead organisation(s)	University of Pisa (UNIPi)
Primary contact	Massimiliano Donati, Daniele Rossi, Sergio Saponara

The AERO project announces AXHEL (ARM aXceleration for Homomorphic Encryption Library), an open-source C++ library developed by the University of Pisa to accelerate the low-level arithmetic used by Homomorphic Encryption (HE) workloads on AArch64 processors.

AXHEL exploits the Arm Scalable Vector Extension (SVE) to accelerate key modular-arithmetic and polynomial-transform operations used by Microsoft SEAL. These computational kernels are common to many Homomorphic Encryption libraries and can potentially be reused beyond SEAL, while its integration remains transparent to existing SEAL applications.

Technological Advancements in AERO

Accelerating Homomorphic Encryption Computation on Arm Processors

AXHEL reduces the computational overhead of Homomorphic Encryption by applying architecture-aware SIMD vectorization based on the Arm Scalable Vector Extension (SVE) to modular and polynomial arithmetic.

Key features include:

- SVE-vectorized modular addition, subtraction, multiplication, reduction, and fused multiply-add.
- SVE-accelerated Number Theoretic Transform (NTT) and inverse NTT kernels.
- Vector-length-agnostic AArch64 implementation with portable scalar fallbacks.
- Integration with Microsoft SEAL without application-level code changes.

“AXHEL brings architecture-aware acceleration for Homomorphic Encryption to Arm Neoverse processors, achieving speedups of around 1.5× on key arithmetic kernels. It integrates transparently with Microsoft SEAL while targeting computational building blocks common to other HE libraries.”

Massimiliano Donati | Researcher, University of Pisa | AERO Consortium Partner

About the AERO project

AERO is a Horizon Europe research and innovation project focused on advancing next-generation computing systems with improved performance, scalability, and energy efficiency.

About AXHEL

AXHEL (ARM aXceleration for Homomorphic Encryption Library) is an open-source C++ acceleration library developed within AERO to accelerate Homomorphic Encryption workloads on Arm Neoverse processors.

Source code: <https://github.com/AERO-Project-EU/AXHEL>

Impact / Closing statement

AXHEL contributes to making Homomorphic Encryption more efficient on Arm-based computing platforms by accelerating its core computational kernels. This can support the broader adoption of privacy-preserving applications in HPC and cloud environments.