PALISADE

PALISADE is an open-source project that provides efficient cross-platform implementations of leading homomorphic encryption schemes and other post-quantum lattice cryptography protocols. Homomorphic encryption (HE) allows performing secure computations over encrypted sensitive data without ever decrypting them, and complies with the HomomorphicEncryption.org security standards for HE.

PALISADE is the only open-source software library that implements all major HE schemes. It also supports multi-party extensions of HE allowing shared computation over encrypted data. PALISADE uses a two-clause BSD open-source license, making it easier to wrap and redistribute PALISADE in products.

For more information, visit https://palisade-crypto.org/

APPLICATIONS

PALISADE is being used by academic researchers and commercial companies to develop new approaches to the problem of efficient computing on encrypted data to preserve the privacy using post-quantum cryptography. The open source nature of PALISADE is essential for commercial customers who need to be able to evaluate the security of critical software applications.

Example applications using PALISADE are cooperative secure training of machine learning models, network-based secure information distribution including re-encryption by proxies between security zones, distributed measurement and control of secure systems, identity and attribute-b

A range of tutorial applications are provided including for example, secure string search in encrypted text, secure emulation of encrypted digital circuits, and networked processes cooperating on joint encrypted computations or proxy re-encryptions.

PLANNED FEATURES

+ PALISADE is designed for usability. Future plans include streamlining APIs, increasing system modularity and cross-platform support including various embedded systems, integration of various hardware accelerators, and increasing the library of sample applications.

PROJECT NEEDS

Development of PALISADE Webinar Series	$10,000
Development of an IOS port of PALISADE	$25,000
Development of a fully-featured Python port of PALISADE	$30,000
Development of a matrix library component of PALISADE	$50,000

PALISADE

For more information on PALISADE, including our governance structure and project roadmap, please visit:

https://palisade-crypto.org/

PALISADE is a Sponsored Project of NumFOCUS, a US 501(c)(3) public charity.

NumFOCUS Sponsored Projects rely on the generous support of corporate sponsors, institutional partners, and individual donors.

NUMFOCUS
OPEN CODE = BETTER SCIENCE

For more information:
info@numfocus.org | +1 (512) 831-2870