PALISADE

Introducing PALISADE

Kurt Rohloff

krohloff@DualityTech.com

contact@palisade-crypto.org

Welcome to the PALISADE Webinar Series!

- This is the first in a series of webinars.
- Focus on:
  - Lattice Crypto
  - Homomorphic Encryption
  - Implementation
  - Application
- We plan on offering this seminar monthly.
  - Email contact@palisade-crypto.org and we'll add you to our mailing list.
- Next webinar – August 28th
  - Reach out if you have requests for future webinars
- We're recording and will post to Youtube.
  - Link and slides on PALISADE website this weekend.

What is PALISADE For?

- PALISADE is an open-source project.
- Provides efficient implementations of:
  - Lattice cryptography building blocks
  - Leading homomorphic encryption (FHE) schemes.

- PALISADE is designed for
  - Usability, providing simpler APIs,
  - Modularity,
  - Cross-platform support
  - Integration of hardware accelerators.

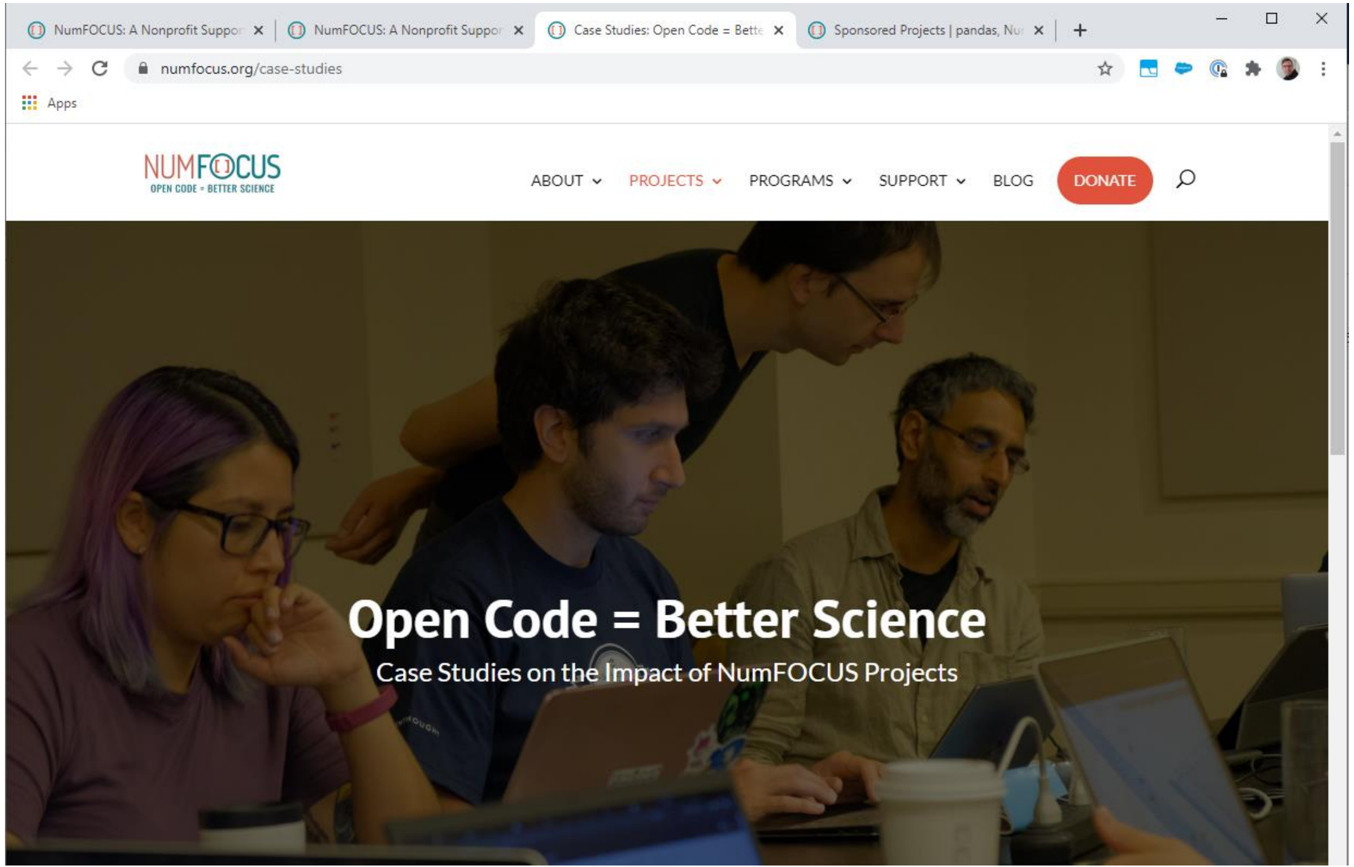
PALISADE Community

- PALISADE is Fiscally Sponsored Project of NumFOCUS
  - NumFOCUS promotes open practices in research, data and scientific computing
  - Aligned objectives to promote innovation via open source software.

- As a project, we take community growth and engagement seriously.
  - PALISADE is available for all

- Governance and Code of Conduct
  - We adopted NumFOCUS best practices for governance and code of conduct
  - We take our code of conduct very seriously!

- NumFOCUS has been a great fit for PALISADE
  - You can submit donations to PALISADE via NumFOCUS


NumFOCUS: A Nonprofit Suppor
NumFOCUS: A Nonprofit Suppor
Case Studies: Open Code = Bette
Sponsored Projects | pandas, Nu
numfocus.org/case-studies
Apps
NUMFOCUS
OPEN CODE = BETTER SCIENCE
ABOUT
PROJECTS
PROGRAMS
SUPPORT
BLOG
DONATE
Open Code = Better Science
Case Studies on the Impact of NumFOCUS Projects

PALISADE

PALISADE Community

- Extensive External Financial Support
  - DARPA
    - PALISADE grew from PROCEED / SafeWare / YFA / CSL / etc…
  - IARPA
    - Support on RAMPARTS & HECTOR
  - Foundations
    - Sloan Foundation, Simons
  - Corporate / Private
    - Duality, LGS Innovations (CACI), etc…
  - University Contributions
    - MIT, WPI, Sabanci

PALISADE Community

- Extensive user community
  - DoD / Defense Industry
  - Financial Services
  - Healthcare
  - Academia / Research
  - Civil Government

Contributors

- Extensive Contributor Community
  - Duality, NJIT, MIT, UCSD, KU Leuven, TwoSix Labs, Raytheon, CACI, etc…
- We’re always welcoming of new community members!

PALISADE Supports Lattice-based encryption

- Lattice schemes form a “new” family of encryption.
  - Built on lattice mathematics.
    - Lattices are integer vectors.
  - They are resistant to quantum computing attacks.

- Not many lattice schemes have been implemented publicly.
  - This is starting to change.
    - PALISADE supports a general lattice crypto “toolbox”

- PALISADE is an investment in implementation to transition “revolutionary” encryption schemes to widespread production use.
  - See RSA, Elliptic Key, etc…

Lattice Capabilities supported in PALISADE

- Public Key Encryption - PKE
- Proxy Re-Encryption - PRE

- Lattice-based Trapdoors
- Lattice-based IBE / CP-ABE / KP-ABE

- Homomorphic Encryption
  - SHE, FHE, etc…
  - HE schemes supported include BGV, CKKS, BFV, FHEW

- We have a few other functionalities in pre-release.
  - Reach out if you have feature requests!

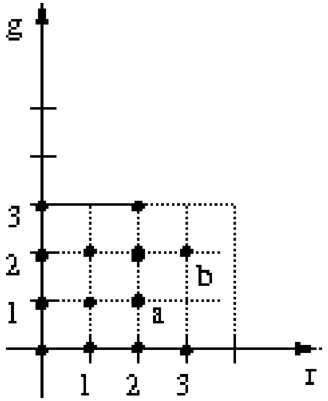
Post-Quantum

- Quantum attacks:
  - Shor showed quantum algorithms for factoring.
  - Grover showed a quadratic speedup relative to search algorithms.

- We'll have a future webinar on Lattice Crypto Security

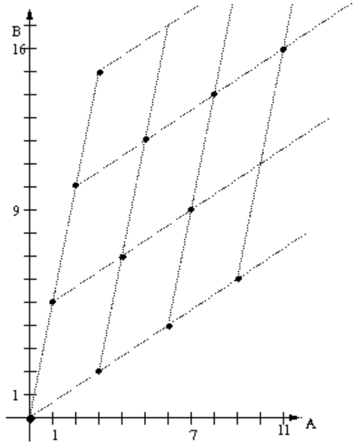
Lattice Encryption Intuition?

- Encryption, Decryption, etc… are primarily composed of linear transforms over large integer vectors.



Plaintext space

Linear transforms and add noise



Ciphertext space

- Plaintext are integer vectors, modulus small p.
- Ciphertext are integer vectors modulus very large q.

FHE?

- Discovery of a possible scheme in 2009
  - Craig Gentry from Stanford/IBM
  - Most important CS breakthrough of 21st century.
  - Very different computation model.

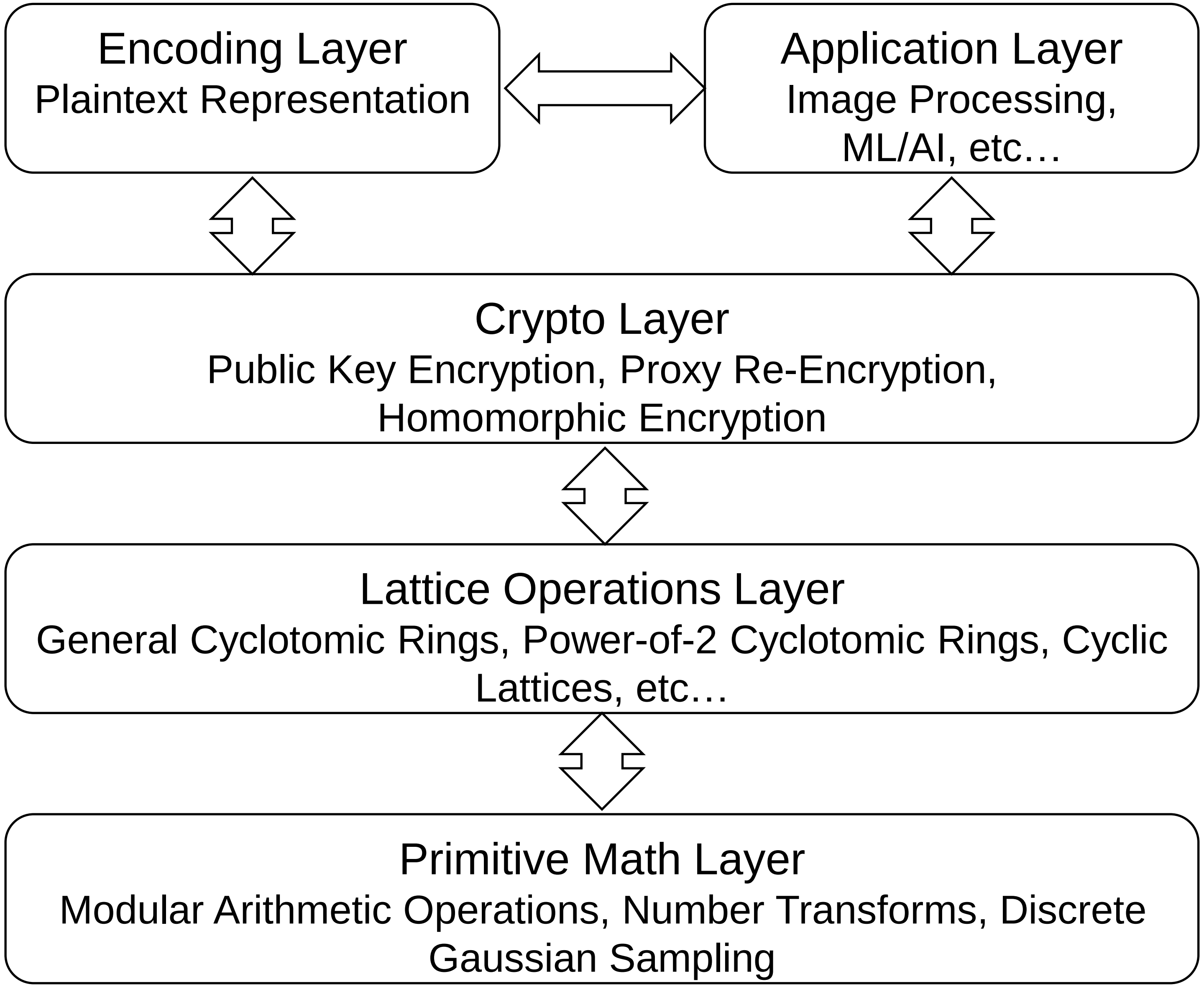
- There have been tremendous theoretical improvements since then.

- PALISADE leverages the “best” in theory with “best” in implementation.

Design Considerations for Adaptability

- There is a tension between crypto-application-specific configurations vs. generic-math-library configurations
- Crypto-specific (These are specific to the crypto library)
  - Scheme selection
  - crypto parameters
- “Systems” interaction configuration (These are relevant across multiple math-intensive libraries)
  - lattice operations - ex: single-CRT vs. double-CRT
  - Parallelism
    - parallelism in math layer, and SIMD vs. multi-core
    - parallelism in lattice layer, and multi-core vs. multi-node
    - parallelism in circuit execution, such as what is scheduled when, especially in multi-core and multi-node operations to minimize runtime or overall memory usage, and what to cache to disk.

PALISADE Open-Source Library



Encoding Layer
Plaintext Representation

Application Layer
Image Processing, ML/AI, etc…

Crypto Layer
Public Key Encryption, Proxy Re-Encryption, Homomorphic Encryption

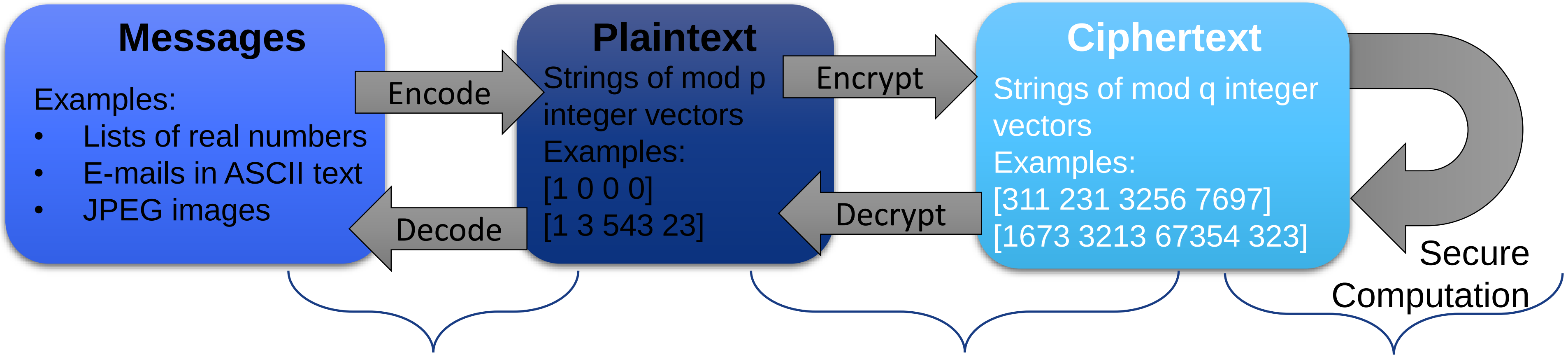
Lattice Operations Layer
General Cyclotomic Rings, Power-of-2 Cyclotomic Rings, Cyclic Lattices, etc…

Primitive Math Layer
Modular Arithmetic Operations, Number Transforms, Discrete Gaussian Sampling

An Encrypted Computing Ecosystem

- Applications
- Software Engineering
- Usability
- Schemes
- Configuration
    - Support for Standards – HomomorphicEncryption.org
- Computer Engineering / Hardware

Computing on Encrypted Data



- Message-Plaintext encodings determined by translation of program into EvalAdd, EvalMult operations.
- Coding is an open research topic and drastically impacts effective runtime.

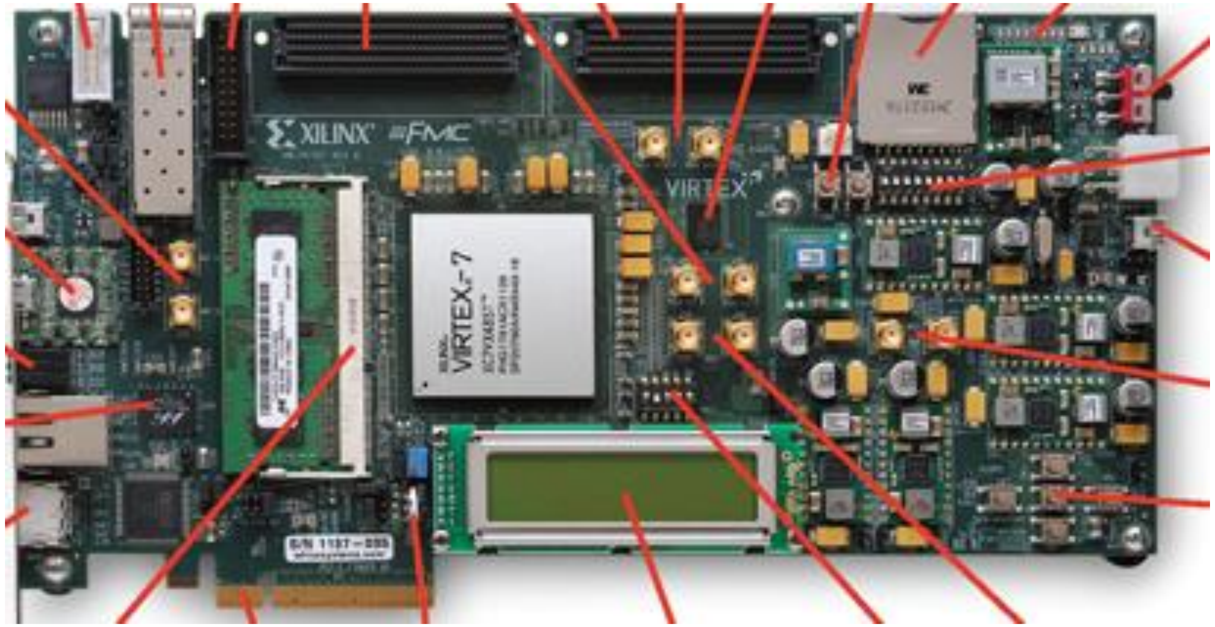
- Plaintext-Ciphertext encryption/decryption defined by FHE scheme.

- EvalAdd and EvalMult operations on ciphertexts

Hardware Acceleration

- Supports Hardware co-processors (FHE Processing Unit - FHEPU) for fast execution of FHE operations.

- Capability for subroutine calls to GPU / FGPA accelerators to execute FHE primitives



PALISADE Community?

- Website:
  - https://palisade-crypto.org/
  - Everything below is linked from the PALISADE site, along with links to publications.

PALISADE Community?

- Google Group:
  - https://groups.google.com/a/palisade-crypto.org/d/forum/announcements
  - Please subscribe

- Documentation / PALISADE Manual:
  - https://gitlab.com/palisade/palisade-release/blob/master/doc/palisade_manual.pdf

- GitLab Repo:
  - Official Release: https://gitlab.com/palisade/palisade-release
  - Development Preview: https://gitlab.com/palisade/palisade-development

- Reach out!
  - contact@palisade-crypto.org

THANK YOU

contact@palisade-crypto.org
krohloff@palisade-crypto.org