PALISADE Lattice Cryptography Library User Manual (v1.3.0)

Yuriy Polyakov[1], Kurt Rohloff[1], and Gerard W. Ryan[1]

[1]Cybersecurity Research Center, New Jersey Institute of Technology (NJIT), Newark, NJ, 07102, USA.
{polyakov,rohloff,gwryan}@njit.edu

October 17, 2018

Abstract

This document is the manual for the PALISADE lattice cryptography library. This manual provides an introduction to the library by describing the library architecture and cataloging its capabilities. We focus on the PALISADE library's ability to support public-key homomorphic encryption capabilities to evaluate arithmetic operations on data while encrypted. We do not explicitly provide an introduction to lattice cryptography, but we provide an overview of notation and terminology necessary to use the PALISADE library. In addition to providing code samples for the use of the PALISADE library, we also discuss the library programming style for developers who wish to read library code or even add to the library. We also provide an overview of common pitfalls in the use of PALISADE.

Contents

Listings

1 Document Overview

This manuscript is a working document to introduce users to the PALISADE lattice cryptography library. The most recent copy of this document is available for download from the PALISADE library website. This document will be updated as the public version of the PALISADE library repo is updated. Copies of this document may be available for download from PALISADE contributors' websites, but the version available for download on the PALISADE library website should be considered authoritative.

The manual is organized as follows.

- An introduction to the library is provided in Section 2.
- Section 3 provides a basic introduction to lattice cryptography.
- The library architecture is discussed in Section 4.
- The library capabilities are discussed in Section 5.
- Section 6 provides an overview of the PALISADE library directory structure.
- Section 7 provides an overview of notation and terminology used in the library and this manual.
- This document is intended to be driven by code samples which show the library being used for specific needs.
- Section 8 provides these code samples, with a focus on homomorphic encryption applications.
- Section 9 describes how the library can be built in a generic Linux environment.
- Section 10 describes the programming style we maintain in the library for those users who wish to contribute code to the library.

In addition to the primary manual content discussed above, we provide the following appendices.

- Appendix A reproduces the library's BSD 2-clause license.
- Contributors to the PALISADE library are listed in Appendix B.
- The PALISADE library has been made possible by the generous support of our sponsors. A listing of the PALISADE library sponsors can been seen in Appendix C.

The public version of the PALISADE Lattice Cryptography library can be found on The PALISADE Git Repo.

The listed authors of this document are the current primary maintainers of the PALISADE library repo.

2 Introduction

Lattice cryptography has received considerable attention because of its capability to support both post-quantum public-key encryption and the ability to compute on data while encrypted via homomorphic encryption. Lattice cryptography also provides other powerful capabilities such as proxy re-encryption and attribute-based encryption. The PALISADE library provides implementations of the building blocks for lattice cryptography capabilities along with end-to-end implementations of advanced lattice cryptography protocols for public-key encryption, proxy re-encryption, homomorphic encryption and others. PALISADE provides both an experimental platform for researchers to design and evaluate new lattice cryptography capabilities, while at the same time providing implementations of known protocols that can be integrated into applications. In this manual we describe PALISADE and discuss how it can be used.

The PALISADE library is designed to address the following inherent challenges of lattice cryptography implementation:

- The complexity of algebraic constructions makes it hard for non-experts to leverage, let alone implement, algebraic constructions used as the building blocks of lattice cryptography.
- Lattice cryptography implementations are often purpose-built. Rapid deployment on new hardware systems is difficult to support with these existing implementations.
- Parameter selection for security and performance takes very sophisticated understanding, and this is nontrivial even for experts - up to a dozen parameters may be needed to be set for some schemes.
- Security assumptions are evolving, and it has been difficult to adapt prior implementations. See for example the recent subfield lattice attacks against LTV which required re-design of libraries that previously used this scheme.
- Application integration has been challenging, without easy methods to efficiently perform operations on non-trivial data types, such as rationals, complex numbers, etc.

As a result of these identified challenges, we design PALISADE to achieve the following design goals:

- *Create an extendible and adaptable library for lattice cryptography.* Lattice crypto uses few computational primitives. We allow for new protocols that mix-and-match these primitives to avoid the need for expert low-level knowledge. This has been a major advance in the PALISADE library, and we are still refining these features of PALISADE as we support more capabilities.

- *Provide a modular structure to mix and match components.* This allows for system-optimized arithmetic and lattice "backends"/plugins. We currently support multiple math backends which can be selected at compile time. The PALISADE library is thus designed to be highly portable into commodity computing and hardware environments, including Windows, Linux, MacOS and Android environments. The ability to support multiple hardware accelerators is a work in progress in PALISADE.

- *Offer (semi-)automated parameter selection.* This reduces the need to tune an overwhelming number of parameters. This is still a major research topic and is a work in progress in PALISADE.

- *Develop common crypto APIs.* Common crypto APIs across multiple schemes and backends "hide" complex details of lattice constructions / parameterization from application developers, allowing developers to focus on their areas of interest while integrating and replacing components to maintain security and performance. This is another major feature of PALISADE that we continue to refine.

- *Deliver good software engineering with focus on usability.* This permits standards-based design and style. Unit tests and benchmarking environments are supported for evaluation and tuning of integrated applications. We aim to provide documentation, clean code and code samples that reduce effort for new developers.

Our identification of these goals in PALISADE is informed by industry experience integrating PALISADE into multi-organizational large software engineering projects. As a result of these identified challenges and the resulting engineering goals we set for ourselves in the design of PALISADE, we design PALISADE to be highly modular, with a core library of lattice cryptography primitives that support multiple protocols for public-key encryption, homomorphic encryption, digital signature schemes, proxy re-encryption and program obfuscation.

3 A Brief Overview of Lattice Cryptography

At a high intuitive level, encryption is a computational process wherein **Data** is **Encoded** as **Plaintext** and then encrypted into **Ciphertext** according to some **Encryption** algorithm. Conversely, decryption is a corresponding computational process wherein the **Plaintext** can be recovered from the **Ciphertext** through the use of a correspoding **Decryption** algorithm.

These algorithms use cryptographic **Keys** to perform the **Encryption** and **Decryption** operations. Intuitively, an encryption scheme is secure if it prevents an adversary from recovering **Plaintext** (or information about a **Plaintext**) from **Ciphertext** when the adversary does not have the corresponding decryption key.

A "symmetric key" protocol uses the same key to perform both encryption and decryption. A "public key" or "assymmetric" protocol uses a pair of **Public** and **Secret** keys, respectively, for encryption and decryption. A **Secret** key is sometimes called a **Private** key.

In practice symmetric keys and secret keys are kept secret because they can be used to access protected information. Public keys are often widely distributed and often published on the open Internet. The intended use of a public key is that one can encrypt data with a downloaded public key corresponding to an intended recipient, encrypt sensitive information for the recipient with the public key, and send that encrypted sensitive information to the recipient. The recipient can use her secret key to decrypt and recover the protected information encoded in the plaintext.

Cryptographic algorithms are designed around computational hardness assumptions so that the difficulty of recovering information about plaintext is at least as hard as some computationally hard problem. Thus, it is theoretically possible to break such a system, but it is assumed infeasible to do so by any known practical means. Different computationally hard problems define different classes of encryption systems. PALISADE focuses on lattice-based cryptography. The security of lattice cryptography is based on the hardness of variants of the Shortest Vector Problem (SVP), Learning With Errors (LWE), and other hard problems. Lattice cryptography has both symmetric and public key variants, but we generally focus on the public key lattice cryptography variants in this manual and in the PALISADE library.

Homomorphic Encryption (HE) or Fully Homomorphic Encryption (FHE) refer to a class of encryption methods envisioned by Rivest, Adleman, and Dertouzos in 1978. Homomorphic encryption differs from basic encryption methods in that it allows computation to be performed directly on encrypted data without requiring access to a secret key. The result of such a computation remains in an encrypted form, and can at a later point be revealed by the owner of the secret key by decrypting the result.

In 2009 Craig Gentry showed the existence of lattice-based FHE capabilities. Since this initial discovery of a lattice-based FHE protocol, there has been a Renaissance in lattice cryptography, with the discovery of several other increasingly practical homomorphic encryption schemes and variations of ho-

momorphic encryption protocols. Some of the common homomorphic encryption schemes include the Brakerski-Fan-Vercauteren (BFV)[1], Brakerski-Gentry-Vaikuntanathan (BGV), Lopez-Alt–Tramer–Vaikuntanathan (LTV) [2] and Stehle-Steinfeld (StSt) schemes. Other related protocols include:

- Proxy Re-Encryption (PRE), which permits delegation of ciphertext decryption, thus allowing a host to delegate access to encrypted data.
- Somewhat Homomomorphic Encryption (SHE), which permits a limited amount of computation on encrypted data.
- Leveled Somewhat Homomorphic Encryption (Leveled SHE), which permits at least a fixed depth of computation to be performed on encrypted data by using a decreasing ladder of ciphertext moduli.
- Multiparty Homomorphic Encryption, which enables multiple participants to contribute data to a joint computation, without sharing access to the actual data.

The public version of PALISADE supports all of the protocols discussed above, and we are in the process of adding support for more protocols and schemes.

An inherent property of encrypted computing technologies, including the various protocols supported by PALISADE, is that computing on encrypted data is significantly slower and more compute intensive than computing on plaintext data. As such, debugging the applications of encrypted computing technologies can be a frustrating, slow process. To aid developers in integrating PALISADE implementations of encrypted computing technoligies, we also provide in PALISADE a "Null" scheme which supports the same API as the BFV, BGV, LTV and StSt implementations, but which does not encrypt data and performs all operations on unencrypted plaintext. The Null scheme implementation operates as a light-duty no-security equivalent of the encrypted computing protocols supported by PALISADE. Thus, we provide the Null scheme so developers can test their PALISADE integrations more easily without the overhead or frustration of testing operations with slower more compute-intensive workloads engendered by encrypted computing capabilities.

[1] This scheme is also frequently denoted as the FV scheme, but we choose to call it the BFV scheme.

[2] Note that we include LTV in PALISADE for historical purposes. This scheme is no longer considered fully secure. We developed an initial implementation of this scheme before the later discovery of subfield lattice attacks.

4 Library Architecture

The PALISADE library implements lattice cryptography in C++. The objects that are created by and manipulated within PALISADE are instances of C++ classes.

PALISADE is designed as a layered architecture where each layer provides a set of services to the layer "above" it in the stack, and makes use of services in the layer "below" it in the stack. The interfaces between each of the layers are designed to implement a common API. This permits substituting multiple implementations at any layer for experimental purposes.

The high-level architecture of PALISADE is illustrated in Figure 1.

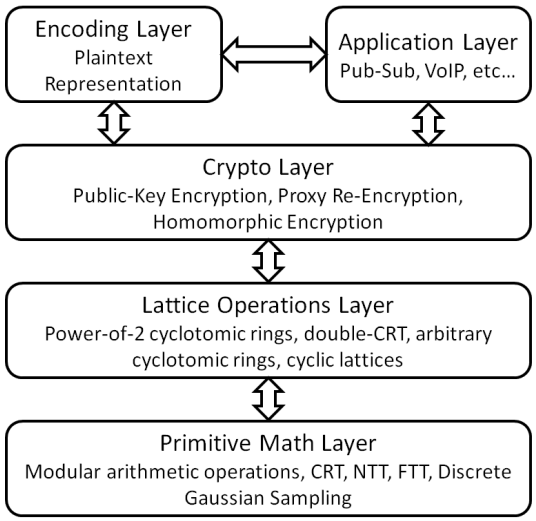

Figure 1: High-level PALISADE architecture

The layers in PALISADE are as follows:

1. **Application**: All programs that call the PALISADE library services are in this layer.
2. **Encoding**: All implementations of methods to encode data are at this layer.
3. **Crypto**: All implementation of cryptographic protocols are at this layer.
4. **Lattice Operations**: All higher-level lattice-crypto mathematical building blocks are in this layer.
5. **Primitive Math**: All low-level generic mathematical operations, such as multi-precision arithmetic implementations, are at this layer.

4.1 Application Layer

All programs that make use of the PALISADE library are said to be in the Application layer.

All programs at the Application layer make calls to services exposed in the PALISADE Crypto layer to gain access to PALISADE lattice cryptography functionality. The Application layer also makes use of service at the Encoding layer.

4.2 Encoding Layer

The Encoding layer contains all classes needed to provide for the encoding of any supported raw plaintext message data into a **Plaintext** object, and for decoding back to raw plaintext messages whenever necessary.

The Encoding layer is used to create **Plaintext** objects. These objects are sometimes created at the request of the Application layer, in which case Crypto layer methods act as a proxy for the Application layer, sometimes at the request of the Crypto layer itself. The interface for Encoding functionality is C++ methods provided by **Plaintext**.

4.3 Crypto Layer

The Crypto layer contains all classes needed to provide all available lattice cryptography functionality for specific cryptographic protocols such as public-key encryption, PRE and SHE schemes, and all included methods such as encryption and decryption, proxy re-encryption and container classes for parameters specific to those schemes.

The interface for Crypto functionality is C++ methods provided by **CryptoContext**. Therefore the Crypto layer provides various factory methods for creating a **CryptoContext** along with the context itself. The Crypto layer manipulates **Plaintext** and **Ciphertext** objects that are passed to it by the Application layer, and returns the appropriate **Plaintext** and **Ciphertext** objects to the Application. Operations on a **Matrix** of such objects is also provided.

The Crypto layer makes use of services provided by the Lattice Operations layer.

4.4 Lattice Operations Layer

The Lattice Operations layer provides support for all lattice constructs, including power-of-two cyclotomic rings and arbitrary cyclotomic rings. The Double Chinese Remainder Theorem (Double-CRT) representation of cyclotomic rings is also implemented in the Lattice layer.

The Lattice layer is used to provide an implementation of the various **Poly** classes, including **Poly**, **NativePoly**, and **DCRTPoly**. These objects are used as building blocks in **Plaintext** and **Ciphertext**. The interface for Lattice functionality is the C++ methods provided by the **Poly** classes.

The Lattice layer performs lattice operations by decomposing operations into primitive arithmetic operations on integers, vectors, and matrices. The Lattice layer makes use of the Primitive Math layer to perform these operations.

4.5 Primitive Math Layer

The Primitive Math layer provides support for basic modular arithmetic operations, including multi-precision arithmetic. This layer also includes efficient algorithms for Number-Theoretic Transform (NTT), Fermat-Theoretic Transform (FTT), and discrete Gaussian samplers, among others. The interface for Math functionality is the C++ methods provided by both custom multi-precision libraries, and external imported libraries such as NTL.

4.6 Utilities

PALISADE also provides a cross-cutting Utilities module for common utility functions used by all the layers. The primary use of this layer is for serialization and deserialization of objects, and for creation of exceptions.

5 Capabilities

One of the goals of PALISADE is to provide straightforward mechanisms to select 1) an encryption protocol, 2) an encryption scheme to support that protocol, 3) encoding mechanisms to represent data with that scheme, 4) a math back-end to support computational operations over that data for the scheme and 5) configuration parameters for that protocol, encoding mecahnisms and math back-end. PALISADE provides a broad set of selections for each of these choices, and provides the user with the ability to add their own schemes, encodings, operations, etc. Furthermore, the user of PALISADE can select from multiple lattice layer implementations and math layer implementations, can easily mix-and-match, and can even provide their own implementations at different layers. In this section we describe these choices we make available in PALISADE.

At the highest level, the PALISADE library groups encryption protocols into a set of capabilities that can be selectively enabled by the user at run time. Table 1 shows which functions are supported by which capabilities. Enabling a particular capability turns on several functions in support that capability. Some capabilities implies other capabilities, such as how SHE for example implies PKE capabilities. Thus, in these scenarioes, some capabilities are turned "on" automatically.

Capabilities currently supported PALISADE are listed in Table 1.

Once an encryption protocol is selected, a user of PALISADE can select from one of multiple schemes, each of which supports some or all of the above protocols

- BFV variants
  - BFV : "textbook" Fan-Vercauteren variant of Brakerski's scale invariant scheme [2, 4, 7]
  - BFVrns : Halevi-Polyakov-Shoup RNS variant of the BFV scheme [6]
  - BFVrnsB : Bajard-Eynard-Hasan-Zucca RNS variant of the BFV scheme [1]
- BGV : Brakerski-Gentry-Vaikuntanathan scheme [3, 5]
- LTV : Lopez-Alt–Tromer–Vaikuntanathan scheme [8]
- StSt : Stehele-Steinfeld scheme [9]
- Null

Table 2 maps which schemes support which capabilities.

After the selection of the scheme, a user can then select how to represent polynomials, among the following polynomial types:

- **Poly**, which corresponds to representing polynomial coefficients in a multiprecision integer format.

Table 1: PALISADE Capabilities and Functions

Capability	Description	Functions Supported	Also Enabled
ENCRYPTION	Public-Key Encryption	KeyGen Encrypt Decrypt	
PRE	Proxy Re-Encryption	ReKeyGen ReEncrypt	PKE
SHE	Somewhat Homomorphic Encryption	EvalAdd EvalMult EvalSub EvalNegate EvalAutomorphism EvalAtIndex EvalMerge EvalMultMany EvalSum EvalInnerProduct EvalLinRegression EvalLinRegressBatched EvalCrossCorrelation EvalRightShift ——— KeySwitch KeySwitchGen EvalMultKeyGen EvalAutomorphismKeyGen EvalAtIndexKeyGen EvalSumKeyGen	PKE
LeveledSHE	Leveled SHE using Modulus Switching	ModReduce RingReduce LevelReduce ComposedEvalMult	PKE SHE
Multiparty	Multiparty Capabilities	MultipartyKeyGen MultiPartyDecrypt	PKE

Table 2: PALISADE Implemented Capabilities Matrix

Function/Scheme	LTV	StSt	BGV	BFV*	Null
ENCRYPTION	Y	Y	Y	Y	Y
PRE	Y	Up to 2 Hops	Y	Y	Y
SHE	Y	Y	Y	Y	Y
LeveledSHE	Y		Y		Y
Multiparty	Y	Y	Y	Y	Y

- **DCRTPoly**, which corresponds to representing polynomial coefficients in a Residue Number System (RNS), a.k.a. Chinese Remainder Theorem (CRT), format using single-precision integers.
- **NativePoly**, which corresponds to representing polynomial coefficents in a single-precision format (only works up to the word size of 64 bits).

We generally recommend using the **DCRTPoly** representation of polynomials for performance on commodity computing environments, although we include the multiprecision polynomial representation **Poly** for advanced users and implementers of new schemes who which to initially implement using the simpler **Poly** representation.

Similar to the polynomial representations, PALISADE also supports multiple math back-ends. The current implementation of PALISADE selects the math back end at compile time. Supported multi-precision math backends include:

- Multi-precision with fixed sizing (BACKEND 2) supporting bit widths up to 1,500 by default (this value can be changed)
- Multi-precision with variable sizing (BACKEND 4)
- NTL (BACKEND 6)

Native data types are always available, and we require that native 64-bit operations be supported in order to use PALISADE.

6 PALISADE Directory Structure

The directory structure of the PALISADE source code is shown in Table 3

Table 3: PALISADE Library File Structure

Directory	Description
benchmark	Code for benchmarking PALISADE library components.
bin	Executables built by the make process.
doc	Documentation of library components, including doxygen.
google	Google unit test library components.
src	Library source code.
test	Google unit test code.
third-party	Code provided by an external third party.

Within the PALISADE library: the src/core/lib directory contains subdirectories for the Math, Lattice, Encoding and Utils layers; and the src/pke/lib directory contains the Crypto layer source code.

Both src/core and src/pke contain a subdirectory for unit tests as well as a subdirectory for demo applications that exercise the capabilities of PALISADE.

7 Terminology and Notation

In this section we provide a glossary of terminology that we use in PALISADE.

PALISADE provides a framework for using lattice cryptography.

If a **Scheme** supports the ENCRYPTION **Capability**, encrypt and decrypt methods are available for use. The encrypt and decrypt methods are provided as part of the implementation of the ENCRYPTION **Capability** in the **Scheme** being used. A **Plaintext** can be encrypted into a **Ciphertext** through the use of an encrypt method. A **Ciphertext** can be used to generate a **Plaintext** through the use of a decrypt method. The library supports several formats of **Plaintext** and methods to create a **Plaintext** for use in PALISADE.

If a **Scheme** supports the PRE **Capability**, a re-encrypt method is available.

If a **Scheme** supports the SHE and/or LeveledSHE **Capability**, then there is support for homomorphic operations on pairs of **Ciphertext** as well as mixed-mode operations between a **Ciphertext** and a **Plaintext**. These operations are supported by using C++ operator overloading. For example, multiplication of two instances of a **Ciphertext**, A and B, can be simply written as A * B.

PALISADE also includes support for several **Matrix** operations. It is possible to create several **Matrix** of **Plaintext**, encrypt them, perform operations on them, and then decrypt back into a **Matrix** of **Plaintext**.

7.1 Typing

All PALISADE operations are strongly typed. A **Plaintext** that is passed to encrypt will create a **Ciphertext** that is aware of the underlying format of the **Plaintext**, as well as the particular key that was used to encrypt the **Plaintext**. The decrypt operation will fail in cases where an improper key is used. A successful decrypt will produce a new **Plaintext** whose underlying format matches the initial **Plaintext** that was passed to encrypt. Homomorphic operations between **Ciphertext**, and mixed-mode operations between a **Ciphertext** and a **Plaintext** will only be permitted for operands with formats and keys that match.

The underlying data inside of PALISADE is an **Element** in lattice space. Within PALISADE, all **Plaintext** are encoded into an **Element**. Every **Ciphertext** contains one or more **Element** objects, and all operations are mathematical operations on these **Elements**.

There are several formats of **Element** available: a **Poly**, which represents the encoded **Plaintext** as a polynomial; a **NativePoly**, which uses a polynomial with coefficients with a maximum size of 64 bits; and a **DCRTPoly**, which represents the encoded **Plaintext** as a stack of decomposed **MativePoly** polynomials using the Double Chinese Remainder Transform.

7.2 CryptoContext

A **CryptoContext** in PALISADE is the class that provides all PALISADE encryption functionality. All objects used in a PALISADE implementation are created by a **CryptoContext** and can be considered to "belong to" the **CryptoContext** that they were created with.

Any and all operations on PALISADE objects must be on objects that belong to the same **CryptoContext**. The high-level use of the **CryptoContext** to encrypt a **Plaintext** to generate a **Ciphertext** is as follows:

1. Choose a set of **ElementParams** to define parameters for the **Element** to be used.
2. Choose a set of **EncodingParams** to define parameters for encoding.
3. Select a **Scheme** that you wish to use for lattice cryptography.
4. Construct a **CryptoContext** for your selected scheme, **ElementParams** and **EncodingParams**, in which all operations shall take place. The construction of a **CryptoContext** involves selecting parameters for security and performance. There are potentially multiple mechanisms to generate the Scheme parameters needed for this construction.
5. Select which **Capability** are used with the **CryptoContext**. Note that not every **Scheme** will support every possible **Capability**.
6. Use CryptoContext methods to create **Keys**.
7. The user may also perform homomorphic operations on **Ciphertext** and **Plaintext** objects if that **Capability** has been enabled and if the **Scheme** supports the operations.
8. Encrypt a **Plaintext** into a **Ciphertext**.
9. Decrypt a **Ciphertext** back to a **Plaintext**.

Each **CryptoContext** is uniquely identified by its **Scheme**, **Element** type, **ElementParams** and **EncodingParams**. When we say that an object "belongs to" a **CryptoContext**, we are actually saying that it is associated with a **CryptoContext** with a particular **Scheme**, **Element** type, **ElementParams** and **EncodingParams**.

PALISADE incorporates the standard security tables developed during the Homomorphic Encryption standardization process described at `http://homomorphicencryption.org`. Users of the library can construct a **CryptoContext** by specifying the parameter sets defined in the standard.

It follows that if one creates a **CryptoContext** on two different computers, each with the same **Scheme**, **Element** type, **ElementParams** and **EncodingParams**, then those two **CryptoContext**s are the same, and objects created on one machine can be transferred to and used on the other machine.

7.3 Plaintext

A **Plaintext** is used in PALISADE to represent something that has not been encrypted. It is actually the base class for each of the possible plaintext encodings that are supported in PALISADE:

- ScalarEncoding
- IntegerEncoding
- FractionalEncoding
- PackedEncoding
- CoefPackedEncoding
- StringEncoding

A **Plaintext** is created by invoking the appropriate **CryptoContext** method, passing it the unencrypted information as a parameter.

Once created, a **Plaintext** can be encrypted into a **Ciphertext** using the **CryptoContext** Encrypt routine.

A **Plaintext** can also be used as a parameter to several of the **CryptoContext** homomorphic operations.

When a **Ciphertext** is decrypted, the decryption method creates a new **Plaintext** to contain the decryption.

The **Plaintext** has several methods that provide access to the information in the **Plaintext**, as shown in listing 1:

```
const std::string&       GetStringValue();
const int64_t            GetIntegerValue();
const int64_t            GetScalarValue();
const vector<int64_t>&   GetCoefPackedValue();
const vector<uint64_t>&  GetPackedValue();
```

Listing 1: Values in Plaintext

Note that the only one of these **Plaintext** methods that will return a value is the one that corresponds to the actual type of the **Plaintext**. For example, GetStringValue() will return a std::string if the **Plaintext** is actually a **StringEncoding**, and will throw an exception otherwise.

7.4 Ciphertext

A **Ciphertext** is used in PALISADE to represent encrypted information. A **Ciphertext** is created from a **Plaintext** by an encrypt method, and is converted back to a **Plaintext** by a decrypt method. The encrypt and decrypt methods also require **Keys** that have been generated by the **CryptoContext**.

Homomorphic operations between pairs of **Ciphertext**, or between a **Ciphertext** and a **Plaintext**, are supported, provided that the encodings of the operands match, and provided that those encodings support homomorphic operations (for example, homomorphic operations are not supported for string encodings, and will be rejected if attempted).

7.5 Keys

Many PALISADE functions make use of **Keys**. These objects are created using **CryptoContext** methods.

Encryption and decryption functionality requires a public key/private key pair. The **CryptoContext** KeyGen method generates this key pair and returns it to the caller.

Re-Encryption requires an Evaluation key. This key is generated using the ReKeyGen method.

Certain homomorphic operations may require the applyication of evaluation keys to complete the operation. The **CryptoContext** EvalMultKeyGen and EvalAddKeyGen methods are used to generate the requisite keys needed for the EvalMult and EvalAdd operations, respectively.

7.6 Capability

A **Capability** refers to sets of **CryptoContext** methods that must be enabled before they can be used. A **Capability** must be enabled by calling the **CryptoContext** Enable method and passing it the name of the **Capability** as an argument. Multiple values for **Capability** can be or-ed together and passed as a single argument to Enable.

Table 1 lists the available choices for **Capability**, and the functionality enabled when a particular **Capability** is Enabled.

7.7 Scheme

A **Scheme** is the algorithms used for key generation, encryption/decryption, and homomorphic operations.

Table 2 outlines the different supported schemes in PALISADE.

In order to use a particular **Scheme**, its configuration parameters must be specified. The particular configuration parameters for each scheme are stored in a CryptoParameters class that is particular for that scheme. The classes for CryptoParameters for each scheme are unique, but they all share several characteristics:

1. Each CryptoParameter class has a constructor that allows for the specification of all configuration parameters.

2. The CryptoParameter may have a ParamsGen feature that generates a full set of configuration parameters from a small specification as to how many homomorphic operations will be performed.

3. The CryptoParameter class is part of the CryptoContext

7.8 Element

The math layer performs operations on different kinds of **Element**. This is a representation of a vector in lattice space.

7.8.1 Poly

A **Poly** is a vector of polynomial coefficients. The coefficients are whatever the BigInteger is for the selected math backend, and the vector is simply a vector of these BigInteger, and an associated modulus. All operations on a Poly are done modulo the modulus.

7.8.2 NativePoly

A **NativePoly** is a vector of polynomial coefficients where each of the coefficients is at most a 64-bit unsigned integer. The NativePoly also has a modulus of at most 64 bits, and all operations are done modulo the modulus.

7.8.3 DCRTPoly

A **DCRTPoly** implements a large Poly decomposed into a tower of **NativePoly** elements.

7.9 ElementParams

An **ElementParams** is a container for the configuration parameters of whatever Element is being used. The configuration parameters include the ring dimension, cyclotomic order, and primitive root of unity.

7.10 EncodingParams

An **EncodingParams** is a container for all of the parameters needed to encode a **Plaintext**. In most cases, this consists solely of a plaintext modulus; however, some encodings require more detailed parameters.

7.11 Matrix

PALISADE supports general operations **Matrix** objects with elements of the types described above in this section, as well as operations on these matrices. A user can create a matrix of **Plaintext**, encrypt it into a matrix of **Ciphertext**, and perform operations on matrices.

In addition to homomorphic matrix multiplication, higher level statistical operations such as inner product and linear regression are available. Some operations result in a matrix of **RationalCiphertext**, where each entry in the matrix is a rational number such that the numerator and denominator of

the entry is a **Ciphertext**. For matrices of **RationalCiphertext**, separate decryption of the numerators and denominators of each entry are provided.

8 Sample Implementations

8.1 Creating a CryptoContext

All PALISADE operations are associated with a CryptoContext; therefore, the first step in using PALISADE is to acquire a CryptoContext. A CryptoContext can be created in a number of different ways through the use of static CryptoContextFactory methods. The factory methods return a shared_ptr to a CryptoContext.

It is useful to note that PALISADE keeps track all of the CryptoContexts that have been created, and will not create duplicate contexts. If a user requests that the factory create a context that already exists, the factory simply returns a shared_ptr to the existing context rather than creating a duplicate of that existing context.

A CryptoContext is uniquely identified by the parameters for the underlying lattice layer element that is to be used, the encoding parameters to be used with Plaintext, and the Scheme (and any associated configuration parameters for the Scheme).

The underlying lattice layer element is either a Poly, a NativePoly, or a DCRTPoly. These type names are used as template parameters with the CryptoContext and its methods. The lattice layer elements share a set of element parameters that are given to the CryptoContextFactory methods.

Encoding parameters may be a simple Plaintext modulus, or they may be a broader set of EncodingParms that are used. Encoding parameters are passed to the CryptoContextFactory methods.

Different Schemes have wildly different configuration parameters, and so the Scheme is selected by calling a CryptoContextFactory method for the desired Scheme.

Each Scheme actually has several factory methods:

- A method that accepts values for all configuration parameters for the scheme.
- A method that accepts some values for configuration parameters, and that invokes a scheme-specific parameter generation operation.

There are two other mechanisms available for creating a CryptoContext:

- Deserialize a previously serialized CryptoContext.
- Construct a CryptoContext from one of the set of predefined scheme parameters.

Once a CryptoContext has been created, the appropriate capabilities should be enabled. Once this is complete, the CryptoContext is ready for use.

Below are some code samples for creating contexts. Listing 2 demonstrates creating a CryptoContext by specifying all of the scheme's parameters.

Listing 3 demonstrates the use of the factory method that uses parameter generation.

```
/// Example showing creating an LTV CryptoContext
/// By specifying all Scheme parameters
/// Element is Poly with non power-of-two cyclotomics

usint m = 22;
PlaintextModulus p = 89;
BigInteger ptm(p);

BigInteger ctm("955263939794561");
BigInteger srr("941018665059848");
BigInteger bigmod("80899135611688102162227204937217");
BigInteger bigroot("77936753846653065954043047918387");

auto cycloPoly = GetCyclotomicPolynomial<BigVector,
    BigInteger>(m, ctm);
ChineseRemainderTransformArb<BigInteger, BigVector>::
    SetCylotomicPolynomial(cycloPoly, ctm);

float stdDev = 4;
usint bSize = 8;

shared_ptr<Poly::Params> params(new ILParams(m, ctm, srr,
     bigmod, bigroot));

EncodingParams ep(new EncodingParamsImpl(p,
    PackedEncoding::GetAutomorphismGenerator(p), bSize));

CryptoContext<Poly> cc = CryptoContextFactory<Poly>::
    genCryptoContextLTV(params, ep, bSize, stdDev);

cc->Enable(ENCRYPTION);
cc->Enable(SHE);
```

Listing 2: Creating a CryptoContext with parameters

```
/// Example showing creating an FV Cryptocontext
/// using parameter generation
/// Element is DCRTPoly (configured by ParamsGen)

int relWindow = 1;
PlaintextModulus ptm = 256;
double sigma = 4;
double rootHermiteFactor = 1.006;

//Set Crypto Parameters
CryptoContext<Poly> cryptoContext =
        CryptoContextFactory<Poly>::genCryptoContextFV(
                ptr, rootHermiteFactor, relWindow, sigma,
                    0, 5, 0, OPTIMIZED, 6);

// enable features that you wish to use
cryptoContext->Enable(ENCRYPTION);
cryptoContext->Enable(SHE);
```

Listing 3: Creating a CryptoContext with parameter generation

```
/// Example showing CryptoContext generation
// from a preconfigured parameter set

CryptoContext<Poly> cryptoContext =
        CryptoContextHelper::getNewContext("LTV3");

if( !cryptoContext ) {
        cout << "Error creating CryptoContext" << endl;
        return 0;
}

cryptoContext->Enable(ENCRYPTION);
```

Listing 4: Creating a preconfigured CryptoContext

```
/// Example showing CryptoContext generation
// using standard tables from the homomorphic encryption
    standardization project


PlaintextModulus ptm = 536903681;
double sigma = 3.2;
SecurityLevel securityLevel = HEStd_128_classic;

// support 7 multiplies (ciel(log2(7)))
usint nMults = 3;

// generate keys for s^2 and s^3
usint maxDepth = 3;

CryptoContext<DCRTPoly> cryptoContext =
     CryptoContextFactory<DCRTPoly>::
         genCryptoContextBFVrns(
           ptm, securityLevel, sigma, 0, nMults, 0,
               OPTIMIZED, maxDepth);

if( !cryptoContext ) {
        cout << "Error creating CryptoContext" << endl;
        return 0;
}

cryptoContext->Enable(ENCRYPTION);
```

Listing 5: Creating a CryptoContext using srandard oaranerers

Listing 4 shows the use of preconfigured parameter sets.

Listing 5 shows the use of parameter sets defined by the Homomorphic Encryption standardization process, as defined in `http://homomorphicencryption.org`.

Listing 6 shows creation from a serialization.

8.2 Creating A Plaintext

PALISADE users are able to convert integers, vectors of integers, and strings into Plaintext objects.

Plaintext objects can be used as input to Encryption, can be used as part of homomorphic operations, and are produced as a result of decryption.

All Plaintexts are created by static factory methods within the CryptoContext. Each style of Plaintext encoding has its own factory method.

The Plaintexts are all type safe. A Ciphertext knows the encoding used by

```
/// Example showing CryptoContext generation
/// from a serialization

Serialized serObj;
if( !SerializableHelper::
   ReadSerializationFromFile(FILENAME, &serObj) ) {
                return 1;
}

CryptoContext<DCRTPoly> cc =
   CryptoContextFactory<DCRTPoly>::
        DeserializeAndCreateContext(serObj);

if( cc == 0 ) {
        cout << "Unable to deserialize" << endl;
        return 1;
}

cc->Enable(ENCRYPTION | SHE | LEVELEDSHE);
```

Listing 6: Creating a CryptoContext from a serialization

the original Plaintext that it came from. Decryption creates a Plaintext with the proper encoding. All homomorphic operations check types before performing the operation, and will fail if either the encodings do not match, or if a particular encoding does not support homomorphic operations.

8.2.1 ScalarEncoding

ScalarEncoding is used to encode a single integer by simply copying the integer into the polynomial starting at index 0 and zero-filling remaining unused indices of the polynomial. Listing 7 shows an example of creating a Scalar Plaintext.

```
int64_t val = 12;

Plaintext sPtx = ctx->MakeScalarPlaintext(val);

Plaintext sPtx2 = ctx->MakeScalarPlaintext(-val);
```

Listing 7: Creating a Scalar Plaintext

8.2.2 IntegerEncoding

IntegerEncoding is used to encode a single unsigned integer into a polynomial such that each bit (0 or 1) in the integer is copied into its corresponding slot in the polynomial. For example, the integer 14, which is binary 1110, is encoded by emplacing 1, 1, 1 and 0 into the first four positions of the polynomial. This is shown in listing 8.

```
Plaintext intPtx = ctx->MakeIntegerPlaintext(14);
```

Listing 8: Creating an Integer Plaintext

Important Note: IntegerEncoding encodes each bit of the integer into a separate coefficient of the polynomial. This implies that the ring dimension (degree of polynomial) should be large enough to store all bits, especially in scenarios where each homomorphic multiplication doubles the number of polynomial coefficients with each multiplication. This is typically a non-issue for secure schemes/settings (as the ring dimension is already large enough) but can be an issue for the Null scheme, where the cyclotomic order is provided as an input argument.

8.2.3 FractionalEncoding

FractionalEncoding is a generalization of IntegerEncoding that can encode both integers and fractions. Currently it is limited in its functionaly and is only used to add support for right shifting (moving least significant bits to the fractional part). Examples of FractionalEncoding for encoding an integer 3 and a fraction 1/8 are shown in listing 9.

```
Plaintext intPtx = ctx->MakeFractionalPlaintext(3);
Plaintext intPtx = ctx->MakeFractionalPlaintext(0,3);
```

Listing 9: Creating a Fractional Plaintext

Important Note: FractionalEncoding encodes each bit of the integer into a separate coefficient of the polynomial. This implies that the ring dimension (degree of polynomial) should be large enough to store all bits, especially in scenarios where each homomorphic multiplication doubles the number of polynomial coefficients with each multiplication. This is typically a non-issue for secure schemes/settings (as the ring dimension is already large enough) but can be an issue for the Null scheme, where the cyclotomic order is provided as an input argument.

8.2.4 CoefPackedEncoding

CoefPackedEncoding is used to encode a vector of integers, or an initializer list of integers, into a polynomial such that each integer is emplaced into a coefficient

of the polynomial. This is illustrated in listing 10.

```
std::vector<int64_t> inputs( { 2, 3, 5, 7} );

// construction from vector
Plaintext c1 = ctx->MakeCoefPackedPlaintext(inputs);

// construction from initializer list
Plaintext c2 = ctx->MakeCoefPackedPlaintext({-6,1,4,8});
```

Listing 10: Creating a CoefPackedEncoding Plaintext

8.2.5 PackedEncoding

PackedEncoding is an implementation of an efficient encoder packing multiple integers into a single plaintext polynomial (single ciphertext) that enables SIMD (Single Instruction, Mutiple Data) operations on these integers. Currently PALISADE supports addition, multiplication, and rotation capabilities for packed ciphertexts. The cyclotomic order m has to divide $p-1$, where p is the plaintext modulus. This is shown in listing 11.

```
std::vector<uint64_t> val( {37, 22, 18, 4, 3, 2, 1, 9} );

Plaintext packedPtx = ctx->MakePackedPlaintext(val);
```

Listing 11: Creating a PackedEncoding Plaintext

8.2.6 StringEncoding

StringEncoding is used to encode a string into a polynomial. For this encoding, each 8-bit character in the input is encoded directly into a coefficient of the polynomial. This encoding is constrained to only use 256 as a plaintext modulus. Listing 12 shows the use of this encoding.

Future implementations that support other character encodings, such as Unicode, are possible but are not currently supported.

Homomorphic operations will NOT work with this encoding.

```
string s("Here is my string!");

Plaintext stringPtx = ctx->MakeStringPlaintext(s);
```

Listing 12: Creating a String Plaintext

8.3 Encryption

In order to encrypt a Plaintext into a Ciphertext, create a CryptoContext and a Plaintext as illustrated above.

The code in listing 13 illustrates this. It assumes that you have created a CryptoContext named "cc" and have created a Plaintext named ptxt within cc.

Observe that the code uses the KeyGen method to create a key pair, and uses the publicKey portion of that key pair for the encryption. The encryption will fail if the keys were generated in a different CryptoContext than cc.

```
//////////////////////////////////////////////////////////
// Perform Key Generation Operation
//////////////////////////////////////////////////////////

LPKeyPair<Poly> keyPair = cc->KeyGen();

if( !keyPair.good() ) {
        cout << "Key generation failed!" << endl;
        exit(1);
}

//////////////////////////////////////////////////////////
// Encryption
//////////////////////////////////////////////////////////

Ciphertext<Poly> ciphertext;

ciphertext = cc->Encrypt(keyPair.publicKey, ptxt);
```

Listing 13: Encrypting

8.4 Decryption

In order to decrypt a Ciphertext into a Plaintext, a CryptoContext, Ciphertext and KeyPair must exist. The keys and the Ciphertext must have been created within the CryptoContext. An example is shown in listing 14.

8.5 Re-Encryption

Re-Encryption involves converting a Ciphertext that is decryptable with key "A" into a Ciphertext that is decryptable with key "B" by creating a re-encryption key and using it to re-encrypt the ciphertext.

The code sample in listing 15 illustrates this capability. It assumes a CryptoContext cc, an initial keypair A, and a Ciphertext cipher that has been created using A. We show the generation of key pair B, the generation of the

```
////////////////////////////////////////////////////////
//Decryption of Ciphertext
////////////////////////////////////////////////////////

Plaintext decrypted;

cc->Decrypt(keyPair.secretKey, ciphertext, &decrypted);
```

Listing 14: Decrypting

re-encryption key, the re-encryption operation, and the subsequent decryption of the re-encrypted Ciphertext with B's secret key.

Note that in order to use Re-Encryption, the PRE capability must be enabled for the CryptoContext.

8.6 Serialization and Deserialization

It is occasionally useful to be able to serialize objects in PALISADE into a string of characters, and to convert a string from a serialized object back into an object again.

PALISADE objects implement serialization through the use of RapidJSON (see http://rapidjson.org), Serialize and Deserialize methods, and a set of methods in the SerializableHelper class.

Serialize converts the object into a Serialized, which is a typedef for a RapidJSON Document. Deserialize converts from a Serialized back into an object.

The PALISADE library includes a number of SerializableHelper utility methods to

- convert a 'Serialized' to a JSON string
- convert a JSON string to a 'Serialized'
- write a 'Serialized' to an output stream
- read a 'Serialized' from an input stream
- write a 'Serialized' to a file, given a file name
- read a 'Serialized' from a file, given a file name

Many of the objects to be serialized are associated with a particular CryptoContext.

In order for such objects to be correctly serialized and deserialized, the serialization saves the CryptoContext that the object belongs to as part of the serialization, and the deserialization makes sure that the CryptoContext for the object being deserialized matches the CryptoContext in the serialization.

This latter point creates a bit of a "chicken and egg" problem in the code.

```
////////////////////////////////////////////////////////
// Perform Key Generation Operation
////////////////////////////////////////////////////////

// Initialize Key Pair Containers
LPKeyPair<Poly> B = cc->KeyGen();

if( !B.good() ) {
        cout << "Key generation failed!" << endl;
        exit(1);
}

////////////////////////////////////////////////////////
//Perform Re-encryption key generation operation.
////////////////////////////////////////////////////////

LPEvalKey<Poly> rekey =
        cc->ReKeyGen(B.publicKey, A.secretKey);

////////////////////////////////////////////////////////
// Re-Encryption
////////////////////////////////////////////////////////

auto re_cipher = cc->ReEncrypt(rekey, cipher);

////////////////////////////////////////////////////////
//Decryption of Ciphertext
////////////////////////////////////////////////////////

Plaintext ptxt;

cc->Decrypt(B.secretKey, re_cipher, &ptxt);
```

Listing 15: Re-Encrypting

- When objects are created, they are created within a particular CryptoContext.
- Once an object is in a CryptoContext, it cannot be moved to another CryptoContext.
- To deserialize, you must first create an object so that you can call its 'Deserialize()' method.
- For that 'Deserialize()' to work properly, the object that you created has to be in the proper CryptoContext, but you don't know what the proper

CryptoContext is until you deserialize the object!

PALISADE addresses this problem by keeping track of all known CryptoContexts, and by providing static methods of CryptoContext that are used to deserialize objects that belong in that context. Each method takes a reference to a 'Serialized' and returns a fresh object; the functionality should be obvious from the name of the method:

- deserializePublicKey
- deserializeSecretKey
- deserializeCiphertext
- deserializeEvalKey

8.6.1 CryptoContexts

In the code sample in listing 16, we assume a CryptoContext named cc.

```
Serialized s;
ser.SetObject();
if( cc->Serialize(&s) == false ) {
        cout << "Serialization failed";
}

CryptoContext<Poly> cc2 = CryptoContextFactory<Poly>::
  DeserializeAndCreateContext(s);
```

Listing 16: Serializing and Deserializing a CryptoContext

8.6.2 Other Objects

In the code sample in listing 17, we assume a CryptoContext named cc.

```
LPKeyPair<Poly> kp = cc->KeyGen();

// serializing/deserializing key in a context
Serialized sK;
kp.publicKey->Serialize(&sK);
LPPublicKey<Poly> newPub = cc->deserializePublicKey(sK);

// creating context when deserializing key
CryptoContext<Poly> newcc = CryptoContextFactory<T>::
    DeserializeAndCreateContext(sK);

LPPublicKey<Poly> nPub = newcc->deserializePublicKey(sK);
```

Listing 17: Serializing and Deserializing Keys

The PALISADE library includes a number of SerializableHelper utility methods to

- convert a ‘Serialized‘ to a JSON string
- convert a JSON string to a ‘Serialized‘
- write a ‘Serialized‘ to an output stream
- read a ‘Serialized‘ from an input stream
- write a ‘Serialized‘ to a file, given a file name
- read a ‘Serialized‘ from a file, given a file name

8.7 Homomorphic Addition of Ciphertexts

Homomorphic addition of two **Ciphertext** is performed by invoking the EvalAdd method of the **CryptoContext**. Both of the operands to the EvalAdd must have been created in the same **CryptoContext**, encrypted with the same **Key**, and encoded in the same way for this operation to work.

The code sample in listing 18 illustrates how to encode two vectors of integers into **Plaintext**, encrypt them into **Ciphertext**, perform homomorphic addition, and decrypt the result back into a **Plaintext**.

This code assumes a **CryptoContext** named cc and a keypair named kp.

```
// Encode source data

std::vector<int64_t> v1 = {3,2,1,3,2,1,0,0,0,0,0,0};
std::vector<int64_t> v2 = {2,0,0,0,0,0,0,0,0,0,0,0};
std::vector<int64_t> v3 = {1,0,0,0,0,0,0,0,0,0,0,0};
Plaintext p1 = cc->MakeCoefPackedPlaintext(v1);
Plaintext p2 = cc->MakeCoefPackedPlaintext(v2);
Plaintext p3 = cc->MakeCoefPackedPlaintext(v3);

// Encryption

auto c1 = cc->Encrypt(kp.publicKey, p1);
auto c2 = cc->Encrypt(kp.publicKey, p2);
auto c3 = cc->Encrypt(kp.publicKey, p3);

// EvalAdd Operation

auto c12 = cc->EvalAdd(c1,c2);
auto csum = cc->EvalAdd(c12,c3);

//Decryption after Accumulation Operation

Plaintext plaintextAdd;

cc->Decrypt(kp.secretKey, csum, &plaintextAdd);

plaintextAdd->SetLength(p1->GetLength());

cout << "Original Plaintext:" << endl;
cout << p1 << endl;
cout << p2 << endl;
cout << p3 << endl;

cout << "Resulting Added Plaintext:" << endl;
cout << plaintextAdd << endl;
```

Listing 18: Adding Ciphertexts

8.8 Homomorphic Multiplication of Ciphertexts

Homomorphic multiplication of two **Ciphertext** is performed by invoking the EvalMult method of the **CryptoContext**. Both of the operands to the EvalMult must have been created in the same **CryptoContext**, encrypted with the same **Key**, and encoded in the same way for this operation to work.

The code sample in listing 19 illustrates how to encode two vectors of integers into **Plaintext**, encrypt them into **Ciphertext**, perform homomorphic multiplication, and decrypt the result back into a **Plaintext**.

This code assumes a **CryptoContext** named cc and a keypair named kp.

Note the creation of an EvalMult key using EvalMultKeyGen at the beginning of the sample.

```
cc->EvalMultKeyGen(kp.secretKey);

// Encode source data

std::vector<int64_t> v1 = {3,2,1,3,2,1,0,0,0,0,0,0};
std::vector<int64_t> v2 = {2,0,0,0,0,0,0,0,0,0,0,0};
std::vector<int64_t> v3 = {1,0,0,0,0,0,0,0,0,0,0,0};
Plaintext p1 = cc->MakeCoefPackedPlaintext(v1);
Plaintext p2 = cc->MakeCoefPackedPlaintext(v2);
Plaintext p3 = cc->MakeCoefPackedPlaintext(v3);

// Encryption

auto c1 = cc->Encrypt(kp.publicKey, p1);
auto c2 = cc->Encrypt(kp.publicKey, p2);
auto c3 = cc->Encrypt(kp.publicKey, p2);

// EvalMult Operation

auto m12 = cc->EvalMult(c1,c2);
auto cprod = cc->EvalMult(m12,c3);

//Decryption after Multiplication Operation

Plaintext plaintextMul;

cc->Decrypt(kp.secretKey, cprod, &plaintextMul);

plaintextMul->SetLength(p1->GetLength());

cout << "Original Plaintext:" << endl;
cout << p1 << endl;
cout << p2 << endl;
cout << p3 << endl;

cout << "Resulting Plaintext:" << endl;
cout << plaintextMul << endl;
```

Listing 19: Multiplying Ciphertexts

8.9 Matrix Operations

A large number of matrix operations are available in PALISADE.

In the example in Listing 20, we illustrate performing a linear regression on two encrypted matrices. The code assumes a CryptoContext named cc.

```
auto zA = [=]() { return
make_unique<Plaintext>(cc->MakeCoefPackedPlaintext(
                    {int64_t(0)} ));
};

Matrix<Plaintext> xP = Matrix<Plaintext>(zA, 2, 2);
xP(0,0) = cc->MakeCoefPackedPlaintext({1,0,1,1,0,1,0,1});
xP(0,1) = cc->MakeCoefPackedPlaintext({1,1,0,1,0,1,1,0});
xP(1,0) = cc->MakeCoefPackedPlaintext({1,1,1,1,0,1,0,1});
xP(1,1) = cc->MakeCoefPackedPlaintext({1,0,0,1,0,1,1,0});

Matrix<Plaintext> yP = Matrix<Plaintext>(zA, 2, 1);
yP(0,0) = cc->MakeCoefPackedPlaintext({1,1,1,0,0,1,0,1});
yP(1,0) = cc->MakeCoefPackedPlaintext({1,0,0,1,0,1,1,0});

//Perform the key generation operations.
LPKeyPair<Poly> kp = cc->KeyGen();
cc->EvalMultKeyGen(kp.secretKey);

//Encryption
shared_ptr<Matrix<RationalCiphertext<Poly>>> x =
  cc->EncryptMatrix(kp.publicKey, xP);
shared_ptr<Matrix<RationalCiphertext<Poly>>> y =
  cc->EncryptMatrix(kp.publicKey, yP);

//Linear Regression
auto result = cc->EvalLinRegression(x, y);

//Decryption into num and denom matrices
shared_ptr<Matrix<Plaintext>> num;
shared_ptr<Matrix<Plaintext>> denom;
cc->DecryptMatrix(kp.secretKey, result, &num, &denom);
```

Listing 20: Calculating Linear Regression

9 Building and Installing PALISADE

PALISADE includes a wiki with detailed instructions on building and running PALISADE on various platforms.

PALISADE can be built and used in Windows, Linux and Macintosh environments.

The library requires a C++ compiler that implements the C++11 standard, support for the OpenMP library, and make.

While not required, it is also recommended that you install and use doxygen.

Users may run the configure.sh script to test if their build environment supports building and running PALISADE.

Running `make` builds the entirety of the library in the `bin` subdirectory. All unit tests, sample demos, and libraries are contained in bin.

A full suite of unit tests is available by running `make testall`.

Library users must ensure that the directories containing the library files, bin/lib and third-party/lib, are available to any executables wishing to dynamically link to the libraries.

10 Programming Style

PALISADE coding style is based on the official Google C++ coding style.
Of particular note on the documentation style:

- We use doxygen commenting style on classes, methods and constants.
- We given meaningful variable names to all variables.
- Every reused discrete block of code has its own method.
- Every discrete line or code or discrete group of code lines for each task has its own comment.

With regards to naming conventions:

- Variable names: camelCase.
- Class, struct, typedef, and enum names: CamelCase.
- Class data members: m_camelCase.
- Class accessor names: GetProperty() and SetProperty().
- Class method names: CamelCase.
- Global variable names: g_camelCase.
- Constant names and macros: UPPER_CASE_WITH_UNDERSCORES (example: BIT_LENGTH).
- Operator overloading is used for binary operations.

We also follow the additional design principles that:

- cout should never be used for exception handling and should never be used in committed code in the core PALISADE library.
- a set of PALISADE exceptions is defined in utils/exception.h. The library is being migrated to throw only these exceptions.

A PALISADE License

PALISADE is available under the following license:

Copyright (c) 2017, New Jersey Institute of Technology (NJIT)
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. *Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.*

2. *Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.*

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

B Contributors

We gratefully acknowledge intellectual and software contributions to the library from numerous individuals at Duality Technologies, Galois, Inc., IBM, TwoSix Labs, Lucent Government Systems (LGS Innovations), Massachussetts Institute of Technology (MIT), New Jersey Institute of Technology (NJIT), Raytheon BBN Technologies, Sabancı University (SU), University of California San Diego (UCSD), National University of Singapore (NUS), New York University (NYU), Worcester Polytechnic Institute (WPI) and Vencore Labs / Applied Communication Sciences (ACS).

Along with the authors of this manual, the following individuals have contributed code or algorithms to the PALISADE library:

- Ahmad Al Badawi (NUS)
- Lisa Bahler (ACS)
- Cheng Chen (MIT)
- Dave Cousins (Raytheon BBN)
- Yarkın Doröz (NJIT)
- Arnab Bobby Deb Gupta (NJIT)
- Shai Halevi (IBM)
- Nick Genise (UCSD)
- Kamil Doruk Gür (NJIT)
- Chiraag Juvekar (MIT)
- Kevin King (MIT)
- Alex Malozemoff (Galois)
- Daniele Micciancio (UCSD)
- Nishanth Pasham (NJIT)
- Thomas Petsche (NJIT)
- Gyana Sahu (NJIT)
- Hadi Sajjadpour (NJIT)
- Erkay Savaş (SU/NJIT)
- Victor Shoup (NYU)
- David Stott (LGS)
- Matthew Triplett (NJIT)
- Vinod Vaikuntanathan (MIT)
- Michael Walter (UCSD)

Note. We have attempted to make an as inclusive a list as possible to identify contributors, but we may of forgotten some important contributors. Any oversights are unintentional. If we neglected to identify your contribution, please let us know and we'll update our listing. If you are on the list of contributors and you'd prefer not to be, please let us know and we'll similarly update our list.

C Support

Support to develop and maintain the PALISADE lattice cryptography library has been generously provided by the following organizations:

- Defense Advanced Research Projects Agency (DARPA) and the Army Research Laboratory (ARL) under contract numbers W911NF-15-C-0226 and W911NF-15-C-0233.
- Defense Advanced Research Projects Agency (DARPA) and the SPAWAR System Center Pacific under contract number N66001-17-1-40403.
- National Security Agency under Grant H98230-15-1-0274.
- Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA).
- The Alfred P. Sloan Foundation.
- A Simons Investigator Award Agreement Dated 6-5-12.

The views expressed are those of the authors and do not necessarily reflect the official policy or position of the Department of Defense or the U.S. Government. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either express or implied, of ODNI, IARPA, or the U.S. Government.

The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.

References

[1] Jean-Claude Bajard, Julien Eynard, M Anwar Hasan, and Vincent Zucca. A full rns variant of fv like somewhat homomorphic encryption schemes. In *International Conference on Selected Areas in Cryptography*, pages 423–442. Springer, 2016.

[2] Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. In *Advances in Cryptology–CRYPTO 2012*, pages 868–886. Springer, 2012.

[3] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):13, 2014.

[4] Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. *IACR Cryptology ePrint Archive*, 2012:144, 2012.

[5] Craig Gentry, Shai Halevi, and Nigel P Smart. Homomorphic evaluation of the aes circuit. In *Advances in Cryptology–CRYPTO 2012*, pages 850–867. Springer, 2012.

[6] Shai Halevi, Yuriy Polyakov, and Victor Shoup. An improved rns variant of the bfv homomorphic encryption scheme. `https://eprint.iacr.org/2018/117`.

[7] Tancrede Lepoint and Michael Naehrig. A comparison of the homomorphic encryption schemes fv and yashe. In *International Conference on Cryptology in Africa*, pages 318–335. Springer, 2014.

[8] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. Multikey fully homomorphic encryption and on-the-fly multiparty computation. *IACR Cryptology ePrint Archive*, 2013:94, 2013. Full Version of the STOC 2012 paper with the same title.

[9] Damien Stehlé and Ron Steinfeld. Making ntru as secure as worst-case problems over ideal lattices. In KennethG. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 27–47. Springer Berlin Heidelberg, 2011.