HElib

Implementing Homomorphic Encryption

Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

AltCRT	Alternative implementation of integer polynomials
AltCRTHelper	A helper class to enforce consistency within an **AltCRTHelper** object
BipartitleGraph	A bipartite flow graph
Cmodulus	
ColPerm	Permuting a single dimension (column) of a hypercube
ConstCubeSlice	A constant lower-dimension slice of a hypercube
Ctxt	A **Ctxt** object holds a single cipehrtext
CtxtPart	One entry in a ciphertext vector
Cube	Indexing into a hypercube
CubeSignature	Holds a vector of dimensions for a hypercube and some additional data
CubeSlice	A lower-dimension slice of a hypercube
deep_clone	Deep copy: initialize with clone
DoubleCRT	Implementatigs polynomials (elements in the ring R_Q) in double-CRT form
DoubleCRTHelper	A helper class to enforce consistency within an **DoubleCRTHelper** object
DynamicCtxtPowers	Store powers of X, compute them synamically as needed
EncryptedArray	A simple wrapper for a smart pointer to an **EncryptedArrayBase**. This is the interface that higher-level code should use
EncryptedArrayBase	Virtual class for data-movement operations on arrays of slots
EncryptedArrayDerived	Derived concrete implementation of **EncryptedArrayBase**

EvalMap	Class that provides the functionality for the linear transforms used in boostrapping. The constructor is invoked with three arguments:
FHEcontext	Maintaining the parameters
FHEPubKey	The public key
FHESecKey	The secret key
FHEtimer	A simple class to accumulate time
FlowEdge	An edge in a flow graph
FullBinaryTree	A simple implementation of full binary trees (each non-leaf has 2 children)
GenDescriptor	A minimal description of a generator for the purpose of building tree
GeneralBenesNetwork	Implementation of generalized Benes Permutation Network
GeneratorTrees	A vector of generator trees, one per generator in Zm*/(p)
HyperCube	A multi-dimensional cube
IndexMap	IndexMap<T> implements a generic map indexed by a dynamic index set
IndexMapInit	Initializing elements in an **IndexMap**
IndexSet	A dynamic set of non-negative integers
KeySwitch	Key-switching matrices
LabeledEdge	A generic directed edge in a graph with some labels
LabeledVertex	A generic node in a graph with some labels
MappingData	Auxilliary structure to support encoding/decoding slots
PAlgebra	The structure of (Z/mZ)* /(p)
PAlgebraMod	The structure of Z[X]/(Phi_m(X), p)
PAlgebraModBase	Virtual base class for **PAlgebraMod**
PAlgebraModDerived	A concrete instantiation of the virtual class
PermNetLayer	The information needed to apply one layer of a permutation network
PermNetwork	A full permutation network
PlaintextArray	A simple wrapper for a pointer to

	a **PlaintextArrayBase**. This is the interface that higher-level code should use
PlaintextArrayBase	Virtual class for array of slots, not encrypted
PlaintextArrayDerived	Derived concrete implementation of **PlaintextArrayBase**
PlaintextBlockMatrixBaseInterface	An abstract interface for linear transformations
PlaintextBlockMatrixInterface	A somewhat less abstract interface for linear transformations
PlaintextMatrixBaseInterface	An abstract interface for linear transformations
PlaintextMatrixInterface	A somewhat less abstract interface for linear transformations
PowerfulConversion	Conversion between powerful representation in R_m/(q) and zz_pX
PowerfulDCRT	Conversion between powerful representation, **DoubleCRT**, and ZZX
PowerfulTranslationIndexes	Holds index tables for translation between powerful and zz_pX
RandomState	Facility for "restoring" the NTL PRG state
RecryptData	A structure to hold recryption-related data inside the **FHEcontext**
ReplicateHandler	A virtual class to handle call-backs to get the output of replicate
shallow_clone	Shallow copy: initialize with copy constructor
SKHandle	A handle, describing the secret-key element that "matches" a part, of the form s^r(X^t)
SubDimension	A node in a tree relative to some generator
TreeNode	A node in a full binary tree
zz_pXModulus1	Auxiliary classes to facillitiate faster reduction mod Phi_m(X) when the input has degree less than m
ZZ_pXModulus1	Placeholder for pXModulus ...no optimizations