GenericCryptanalyzer

Generated by Doxygen 1.9.1

Chapter 1

Hierarchical Index

1.1 Class Hierarchy

This inheritance list is sorted roughly, but not completely, alphabetically:

Chapter 2

Class Index

2.1 Class List

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

Chapter 3

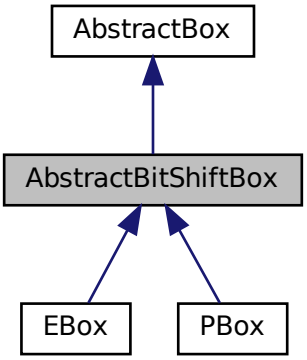
Class Documentation

3.1 AbstractBitShiftBox Class Reference

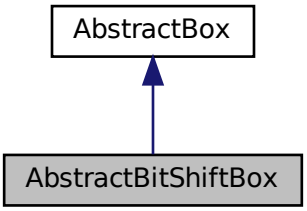
An AbstractBitShiftBox represents a generic box that transforms input in output by shifting bits around.

`#include <abstractbitshiftbox.h>`

Inheritance diagram for AbstractBitShiftBox:



Collaboration diagram for AbstractBitShiftBox:



Public Member Functions

- AbstractBitShiftBox (size_t in_size, size_t out_size, const vector< pair< AbstractBoxPtr, Connection >> &dst_boxes, const vector< size_t > &bit_src)
- AbstractBitShiftBox (size_t in_size, size_t out_size, const vector< size_t > &bit_src)

  similar to the previous constructor, but leaves `dst_boxes` *empty*
- void determine_next () override

  since apply_transformation is a linear deterministic transformations, this will set `is_det` *to* `true` *and* `prob` *to* `1`

Protected Member Functions

- void apply_transformation ()

  computes value of `out_bits` *from* `in_bits` *and* `bit_src`

Protected Attributes

- vector< size_t > bit_src

  an array which describes what bit from the input corresponds to each bit from the output

3.1.1 Detailed Description

An AbstractBitShiftBox represents a generic box that transforms input in output by shifting bits around.

More precisely, it takes a `vector<size_t> bit_src` as input and computes `out_bits[i] = in_↩ bits[bit_src[i]]`

This class is an abstraction that encapsulates the functionality of both PBox and EBox.

See also

PBox

EBox

@inherits AbstractBox

3.1.2 Constructor & Destructor Documentation

3.1.2.1 AbstractBitShiftBox() [1/2]

```
AbstractBitShiftBox::AbstractBitShiftBox (
            size_t in_size,
            size_t out_size,
            const vector< pair< AbstractBoxPtr, Connection >> & dst_boxes,
            const vector< size_t > & bit_src )
```

Parameters

in_size	size of the input bits of this box
out_size	size of the output bits of this box
dst_boxes	output flow connections to following boxes
bit_src	an array used to compute `out_bits` from `in_bits`

Precondition

bit_source.size() == output_size

3.1.2.2 AbstractBitShiftBox() [2/2]

```
AbstractBitShiftBox::AbstractBitShiftBox (
            size_t in_size,
            size_t out_size,
            const vector< size_t > & bit_src )
```

similar to the previous constructor, but leaves `dst_boxes` empty

Parameters

in_size	size of the input bits of this box
out_size	size of the output bits of this box
bit_src	an array used to compute `out_bits` from `in_bits`

Precondition

bit_source.size() == output_size

The documentation for this class was generated from the following files:

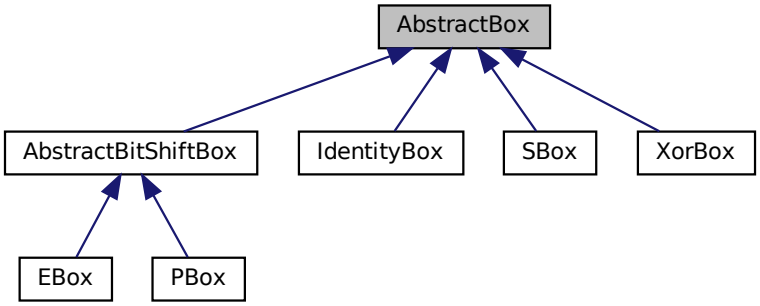
- src/box/abstractbitshiftbox.h
- src/box/abstractbitshiftbox.cpp

3.2 AbstractBox Class Reference

An AbstractBox represents an abstract idea of a block cipher component such as a Pbox, Sbox, Xor, Addition, etc. A cipher is composed of multiple such `boxes` that communicate with each other through connections.

`#include <abstractbox.h>`

Inheritance diagram for AbstractBox:



Public Member Functions

- AbstractBox (size_t in_size, size_t out_size, const vector< pair< AbstractBoxPtr, Connection >> &dst_boxes)
- AbstractBox (size_t in_size, size_t out_size)

  similar to the previous constructor, but leaves `dst_boxes` empty
- void add_dest (AbstractBoxPtr dst_box, BitsRange out_range, BitsRange in_range)

  add_dest adds a new destination box for the output of the box to flow to
- const dynamic_bitset & get_input ()

  getter for `in_bits`
- const dynamic_bitset & get_output ()

  getter for `out_bits`
- size_t input_size ()

  getter for the size of `in_bits`
- size_t output_size ()

  getter for the size of `out_bits`
- bool is_determined ()

  getter for `is_det`
- virtual void set_input (dynamic_bitset<> bits, const BitsRange &rng)

  sets a subrange `rng` of the input to the value of `bits`
- void notify_all ()

  notifies all the destination boxes after the output of the box is determined
- virtual void determine_next ()=0

  method to determine the next best output sorted by probabilities, if all possible outputs have been determined, `is_det` will be set to `true`
- virtual void reset_determination ()

  set the process to be undetermined by setting `is_det` to `false`
- double get_probability ()

  get the probability of the current characteristic

Protected Attributes

- dynamic_bitset in_bits

  the bits that flow into the box
- dynamic_bitset out_bits

  the bits that flow out of the box
- vector< pair< AbstractBoxPtr, Connection > > dst_boxes

  describes how the `out_bits` flow from this box to other following boxes
- bool is_det

  a boolean value that should be true if and only if at least one out of all possible outputs has been determined and returned
- double prob

  the probability of the box to output the currently determined state

Friends

- class **RoundFunction**

3.2.1 Detailed Description

An AbstractBox represents an abstract idea of a block cipher component such as a Pbox, Sbox, Xor, Addition, etc. A cipher is composed of multiple such `boxes` that communicate with each other through connections.

3.2.2 Constructor & Destructor Documentation

3.2.2.1 AbstractBox() [1/2]

```
AbstractBox::AbstractBox (
            size_t in_size,
            size_t out_size,
            const vector< pair< AbstractBoxPtr, Connection >> & dst_boxes )
```

Parameters

in_size	size of the input bits of this box
out_size	size of the output bits of this box
dst_boxes	output flow connections to following boxes

Precondition

for (auto &dst_box : dst_boxes) { dst_box.first != nullptr && dst_box.second.first.start + dst_box.second.↩ first.len <= out_bits.size() && dst_box.second.first.len == dst_box.second.second.len && dst_box.second.↩ second.start + dst_box.second.second.len <= dst_box.first->input_size(); }

3.2.2.2 AbstractBox() [2/2]

```
AbstractBox::AbstractBox (
            size_t in_size,
            size_t out_size )
```

similar to the previous constructor, but leaves `dst_boxes` empty

Parameters

in_size	size of the input bits of this box
out_size	size of the output bits of this box

Precondition

dst_box != nullptr && out_rng.start + out_rng.len <= out_bits.size() && in_rng.start + in_rng.len <= dst_box->in_bits.size();

3.2.3 Member Function Documentation

3.2.3.1 add_dest()

```
void AbstractBox::add_dest (
            AbstractBoxPtr dst_box,
            BitsRange out_range,
            BitsRange in_range )
```

add_dest adds a new destination box for the output of the box to flow to

Parameters

dst_box	a pointer to the destination box
out_range	a subrange of `out_bits` from this box that will flow to `dst_box`
in_range	a subrange of `in_bit` from `dst_box` into which the bits will flow

3.2.3.2 get_input()

```
const dynamic_bitset & AbstractBox::get_input ( )
```

getter for `in_bits`

Returns

`in_bits`

3.2.3.3 get_output()

```
const dynamic_bitset & AbstractBox::get_output ( )
```

getter for `out_bits`

Returns

`out_bits`

3.2.3.4 get_probability()

```
double AbstractBox::get_probability ( )
```

get the probability of the current characteristic

Returns

`prob`

3.2.3.5 input_size()

```
size_t AbstractBox::input_size ( )
```

getter for the size of `in_bits`

Returns

`in_bits.size()`

3.2.3.6 is_determined()

```
bool AbstractBox::is_determined ( )
```

getter for `is_det`

Returns

`is_det`

3.2.3.7 output_size()

```
size_t AbstractBox::output_size ( )
```

getter for the size of `out_bits`

Returns

`out_bits.size()`

3.2.3.8 set_input()

```
void AbstractBox::set_input (
            dynamic_bitset<> bits,
            const BitsRange & rng )  [virtual]
```

sets a subrange `rng` of the input to the value of `bits`

Parameters

bits	the bits that will be put in `in_bits`
rng	the subrange in which bits will be put in `in_bits`

Reimplemented in SBox.

The documentation for this class was generated from the following files:

- src/box/abstractbox.h
- src/box/abstractbox.cpp

3.3 BitsRange Struct Reference

Public Attributes

- size_t **start**
- size_t **len**

The documentation for this struct was generated from the following file:

- src/helpers/helpers.h

3.4 CipherAnalyzer Class Reference

Public Member Functions

- **CipherAnalyzer** (vector< RoundFunctionPtr > rounds, size_t input_max_hamming_weight, double global↩ _thresh, vector< double > opt_probs)
- **CipherAnalyzer** (vector< RoundFunctionPtr > rounds, size_t input_max_hamming_weight, double global↩ _thresh)
- ProbEntry **get_next_entry** ()
- void **set_input** (const dynamic_bitset<> &bits, BitsRange rng)

Protected Member Functions

- bool **advance_state** ()

Protected Attributes

- double **global_thresh**
- vector< double > **opt_probs**
- vector< double > **round_probs**
- vector< RoundFunctionPtr > **rounds**
- size_t **curr_idx**

The documentation for this class was generated from the following files:

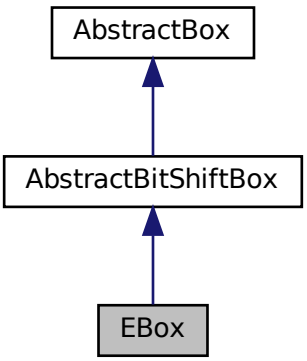
- src/cipheranalyzer.h
- src/cipheranalyzer.cpp

3.5 EBox Class Reference

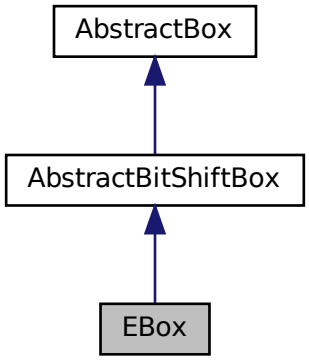
An EBox is a box that takes the input bits and expands them to the output by using some of multiple times.

`#include <ebox.h>`

Inheritance diagram for EBox:



Collaboration diagram for EBox:



Public Member Functions

- EBox (size_t in_size, size_t out_size, const vector< pair< AbstractBoxPtr, Connection >> &dst_boxes, const vector< size_t > &bit_expansion)
- EBox (size_t in_size, size_t out_size, const vector< size_t > &bit_expansion)

  similar to the previous constructor, but leaves `dst_boxes` empty

Additional Inherited Members

3.5.1 Detailed Description

An EBox is a box that takes the input bits and expands them to the output by using some of multiple times.

@inherits AbstractBitShiftBox

3.5.2 Constructor & Destructor Documentation

3.5.2.1 EBox() [1/2]

```
EBox::EBox (
            size_t in_size,
            size_t out_size,
            const vector< pair< AbstractBoxPtr, Connection >> & dst_boxes,
            const vector< size_t > & bit_expansion )
```

Parameters

in_size	size of the input bits of this box
out_size	size of the output bits of this box
dst_boxes	output flow connections to following boxes
bit_expansion	an array used to compute to describe the expansion process of the input bits

See also

AbstractShiftBox constructor

Precondition

in_size <= out_size

3.5.2.2 EBox() [2/2]

```
EBox::EBox (
            size_t in_size,
            size_t out_size,
            const vector< size_t > & bit_expansion )
```

similar to the previous constructor, but leaves `dst_boxes` empty

Parameters

in_size	size of the input bits of this box
out_size	size of the output bits of this box
bit_expansion	an array used to compute to describe the expansion process of the input bits

Precondition

in_size <= out_size

The documentation for this class was generated from the following files:

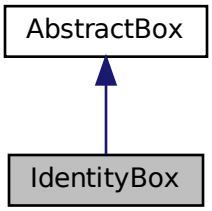
- src/box/ebox.h
- src/box/ebox.cpp

3.6 IdentityBox Class Reference

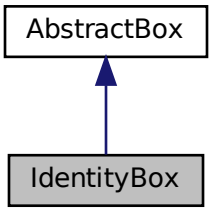
An IdentityBox is a box that represents the identity function `out_bits[i] = in_bits[i]`. An IdentityBox is useful as an accumulator for bits from multiple previous boxes which will then be sent to multiple following boxes.

`#include <identitybox.h>`

Inheritance diagram for IdentityBox:



Collaboration diagram for IdentityBox:



Public Member Functions

- IdentityBox (size_t data_size, const vector< pair< AbstractBoxPtr, Connection >> &dst_boxes)
- IdentityBox (size_t data_size)

  similar to the previous constructor, but leaves `dst_boxes` *empty*
- void determine_next () override

  since the identity function is a linear deterministic transformations, this will set `is_det` *to* `true` *and* `prob` *to* `1`

Additional Inherited Members

3.6.1 Detailed Description

An IdentityBox is a box that represents the identity function `out_bits[i] = in_bits[i]`. An IdentityBox is useful as an accumulator for bits from multiple previous boxes which will then be sent to multiple following boxes.

@inherits AbstractBox

3.6.2 Constructor & Destructor Documentation

3.6.2.1 IdentityBox() [1/2]

```
IdentityBox::IdentityBox (
            size_t data_size,
            const vector< pair< AbstractBoxPtr, Connection >> & dst_boxes )
```

Parameters

data_size	the size in bits of the input and the output
dst_boxes	output flow connections to following boxes

3.6.2.2 IdentityBox() [2/2]

```
IdentityBox::IdentityBox (
            size_t data_size )
```

similar to the previous constructor, but leaves `dst_boxes` empty

Parameters

data_size	the size in bits of the input and the output

The documentation for this class was generated from the following files:

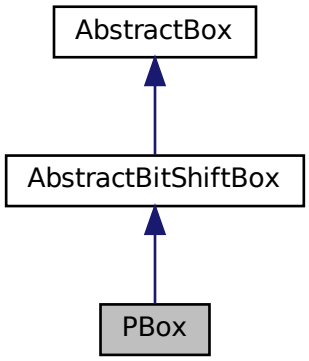
- src/box/identitybox.h
- src/box/identitybox.cpp

3.7 PBox Class Reference

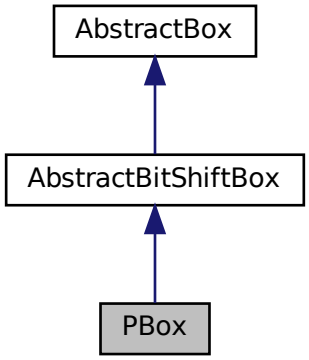
A PBox is a box that takes the input bits and permutes them to get the output.

`#include <pbox.h>`

Inheritance diagram for PBox:



Collaboration diagram for PBox:



Public Member Functions

- PBox (size_t data_size, const vector< pair< AbstractBoxPtr, Connection >> &dst_boxes, const vector< size_t > &bit_perm)
- PBox (size_t data_size, const vector< size_t > &bit_perm)

  PBox similar to the previous constructor, but leaves `dst_boxes` *empty.*

Additional Inherited Members

3.7.1 Detailed Description

A PBox is a box that takes the input bits and permutes them to get the output.

@inherits AbstractBitShiftBox

3.7.2 Constructor & Destructor Documentation

3.7.2.1 PBox() [1/2]

```
PBox::PBox (
            size_t data_size,
            const vector< pair< AbstractBoxPtr, Connection >> & dst_boxes,
            const vector< size_t > & bit_perm )
```

Parameters

data_size	the size in bits of the input and the output
dst_boxes	output flow connections to following boxes
bit_perm	a permutation used to shuffle the bits of the input to get the output

Precondition

bit_perm must be a permutation of [0, ..., bits_size - 1]

3.7.2.2 PBox() [2/2]

```
PBox::PBox (
            size_t data_size,
            const vector< size_t > & bit_perm )
```

PBox similar to the previous constructor, but leaves `dst_boxes` empty.

Parameters

data_size	the size in bits of the input and the output
bit_perm	a permutation used to shuffle the bits of the input to get the output

Precondition

bit_perm must be a permutation of [0, ..., bits_size - 1]

The documentation for this class was generated from the following files:

- src/box/pbox.h
- src/box/pbox.cpp

3.8 RoundFunction Class Reference

Public Member Functions

- **RoundFunction** (string src_id, string dst_id, map< string, AbstractBoxConstructor > constrs, map< string, vector< NamedConnection >> conns)
- bool **is_determined** ()
- ProbEntry **get_next_entry** ()
- void **set_input** (const dynamic_bitset<> bits, BitsRange rng)
- void **set_threshold** (double beta)

Protected Member Functions

- bool **advance_state** ()
- void **top_sort_boxes** (AbstractBoxPtr src, vector< AbstractBoxPtr > &top_sort, map< AbstractBoxPtr, bool > &is_visited)
- vector< AbstractBoxPtr > **sort_boxes** (AbstractBoxPtr src)

Protected Attributes

- AbstractBoxPtr **src**
- AbstractBoxPtr **dst**
- size_t **curr_box_idx**
- vector< AbstractBoxPtr > **boxes**
- vector< double > **partial_prob**
- double **beta_thresh**
- bool **is_det**

Friends

- class **CipherAnalyzer**

The documentation for this class was generated from the following files:

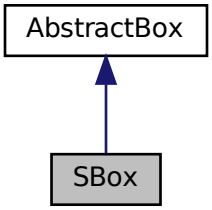
- src/roundfunction.h
- src/roundfunction.cpp

3.9 SBox Class Reference

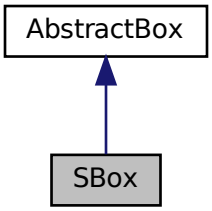
An SBox is a box that applies an arbitrary substitution on the input based on a substitution table. Since the actual value of the difference between pairs of inputs will change depending on the key bytes, this is a non-deterministic element in the cipher.

`#include <sbox.h>`

Inheritance diagram for SBox:



Collaboration diagram for SBox:



Public Member Functions

- SBox (size_t in_size, size_t out_size, const vector< pair< AbstractBoxPtr, Connection >> &dst_boxes, const ProbTable &prob_table)
- SBox (size_t in_size, size_t out_size, const ProbTable &prob_table)

  similar to the previous constructor, but leaves `dst_boxes` empty
- void determine_next () override

  determines the next best possible output for the given input, if all possible outputs have been determined, `is_det` is set to `true`
- void reset_determination () override

  sets `prob` to `0`, `is_det` to `false` and `table_idx` to `0`
- void set_input (dynamic_bitset<> bits, const BitsRange &rng) override

  sets a subrange `rng` of the input to the value of `bits`. Additionaly, `table_idx` to `0` and computes `table_entry` from `in_bits`

Protected Attributes

- ProbTable prob_table

  prob_table the probability table of the sbox
- size_t table_idx

  table_idx the current column in the row of the probability table. This is incremented each time `determine_next()` is called.
- size_t table_entry

  table_entry the row in the probability table corresponding to the value of `in_bits`

3.9.1 Detailed Description

An SBox is a box that applies an arbitrary substitution on the input based on a substitution table. Since the actual value of the difference between pairs of inputs will change depending on the key bytes, this is a non-deterministic element in the cipher.

@inherits AbstractBox

3.9.2 Constructor & Destructor Documentation

3.9.2.1 SBox() [1/2]

```
SBox::SBox (
            size_t in_size,
            size_t out_size,
            const vector< pair< AbstractBoxPtr, Connection >> & dst_boxes,
            const ProbTable & prob_table )
```

Parameters

in_size	size of the input bits of this box
out_size	size of the output bits of this box
dst_boxes	output flow connections to following boxes
prob_table	the probability table of the sbox

3.9.2.2 SBox() [2/2]

```
SBox::SBox (
            size_t in_size,
            size_t out_size,
            const ProbTable & prob_table )
```

similar to the previous constructor, but leaves `dst_boxes` empty

Parameters

in_size	size of the input bits of this box
out_size	size of the output bits of this box
prob_table	the probability table of the sbox

3.9.3 Member Function Documentation

3.9.3.1 set_input()

```
void SBox::set_input (
            dynamic_bitset<> bits,
            const BitsRange & rng )  [override], [virtual]
```

sets a subrange `rng` of the input to the value of `bits`. Additionaly, `table_idx` to `0` and computes `table_entry` from `in_bits`

Parameters

bits	the bits that will be put in `in_bits`
rng	the subrange in which bits will be put in `in_bits`

Reimplemented from AbstractBox.

The documentation for this class was generated from the following files:

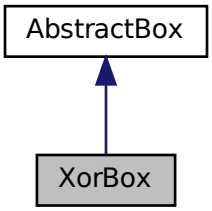
- src/box/sbox.h
- src/box/sbox.cpp

3.10 XorBox Class Reference

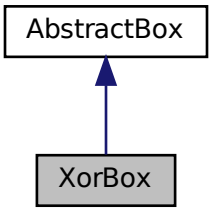
A XorBox is a box that computes the bitwise xor of two inputs. In order to simplify the implementation the the XorBox takes only one input `in_bits` but of size double of that of `out_bits`. the first half of `in_bits` represents the first of the two inputs, and the second half represents the last of the two inputs.

```
#include <xorbox.h>
```

Inheritance diagram for XorBox:



Collaboration diagram for XorBox:



Public Member Functions

- XorBox (size_t data_size, const vector< pair< AbstractBoxPtr, Connection >> &dst_boxes)
- XorBox (size_t data_size)

  similar to the previous constructor, but leaves `dst_boxes` *empty*
- void determine_next () override

  computes the xor between the first half and the second half of the `in_bits` *and stores it in* `out_bits`*. This is a linear and deterministic operation so* `is_det` *will be set to* `true` *and* `prob` *to* `1`

Additional Inherited Members

3.10.1 Detailed Description

A XorBox is a box that computes the bitwise xor of two inputs. In order to simplify the implementation the the XorBox takes only one input `in_bits` but of size double of that of `out_bits`. the first half of `in_bits` represents the first of the two inputs, and the second half represents the last of the two inputs.

@inherits AbstractBox

3.10.2 Constructor & Destructor Documentation

3.10.2.1 XorBox() [1/2]

```
XorBox::XorBox (
            size_t data_size,
            const vector< pair< AbstractBoxPtr, Connection >> & dst_boxes )
```

Parameters

data_size	the size in bits of the input and the output
dst_boxes	output flow connections to following boxes

3.10.2.2 XorBox() [2/2]

```
XorBox::XorBox (
            size_t data_size )
```

similar to the previous constructor, but leaves `dst_boxes` empty

Parameters

data_size	the size in bits of the input and the output

The documentation for this class was generated from the following files:

- src/box/xorbox.h
- src/box/xorbox.cpp

Index