

Wave

Generated by Doxygen 1.9.1



|   |          |
|---|----------|
| <b>1 Data Structure Index</b>                         | <b>1</b> |
| 1.1 Data Structures . . . . .                         | 1        |
| <b>2 Data Structure Documentation</b>                 | <b>3</b> |
| 2.1 AES256_CTR_DRBG_struct Struct Reference . . . . . | 3        |
| 2.1.1 Detailed Description . . . . .                  | 3        |
| 2.2 AES_XOF_struct Struct Reference . . . . .         | 3        |
| 2.2.1 Detailed Description . . . . .                  | 3        |
| 2.3 bitstream_t Struct Reference . . . . .            | 4        |
| 2.3.1 Detailed Description . . . . .                  | 4        |
| 2.4 distrib Struct Reference . . . . .                | 4        |
| 2.4.1 Detailed Description . . . . .                  | 4        |
| 2.5 fdistrib Struct Reference . . . . .               | 4        |
| 2.5.1 Detailed Description . . . . .                  | 5        |
| 2.6 mf3_e Struct Reference . . . . .                  | 5        |
| 2.6.1 Detailed Description . . . . .                  | 5        |
| 2.7 Node Class Reference . . . . .                    | 6        |
| 2.7.1 Detailed Description . . . . .                  | 6        |
| 2.8 perm_network_t Struct Reference . . . . .         | 6        |
| 2.8.1 Detailed Description . . . . .                  | 6        |
| 2.9 range_t Struct Reference . . . . .                | 6        |
| 2.9.1 Detailed Description . . . . .                  | 7        |
| 2.10 reject_t Struct Reference . . . . .              | 7        |
| 2.10.1 Detailed Description . . . . .                 | 7        |
| 2.11 sha3_256incctx Struct Reference . . . . .        | 7        |
| 2.11.1 Detailed Description . . . . .                 | 8        |
| 2.12 sha3_384incctx Struct Reference . . . . .        | 8        |
| 2.12.1 Detailed Description . . . . .                 | 8        |
| 2.13 sha3_512incctx Struct Reference . . . . .        | 8        |
| 2.13.1 Detailed Description . . . . .                 | 8        |
| 2.14 shake128ctx Struct Reference . . . . .           | 8        |
| 2.14.1 Detailed Description . . . . .                 | 9        |
| 2.15 shake128incctx Struct Reference . . . . .        | 9        |
| 2.15.1 Detailed Description . . . . .                 | 9        |
| 2.16 shake256ctx Struct Reference . . . . .           | 9        |
| 2.16.1 Detailed Description . . . . .                 | 9        |
| 2.17 shake256incctx Struct Reference . . . . .        | 9        |
| 2.17.1 Detailed Description . . . . .                 | 10       |
| 2.18 swap_t Struct Reference . . . . .                | 10       |
| 2.18.1 Detailed Description . . . . .                 | 10       |
| 2.19 tritstream_t Struct Reference . . . . .          | 10       |
| 2.19.1 Detailed Description . . . . .                 | 10       |

|   |           |
|---|-----------|
| 2.20 vf2_e Struct Reference . . . . .     | 10        |
| 2.20.1 Detailed Description . . . . .     | 11        |
| 2.21 vf3_e Struct Reference . . . . .     | 11        |
| 2.21.1 Detailed Description . . . . .     | 11        |
| 2.22 wave_pk_t Struct Reference . . . . . | 11        |
| 2.22.1 Detailed Description . . . . .     | 12        |
| 2.23 wave_sk_t Struct Reference . . . . . | 12        |
| 2.23.1 Detailed Description . . . . .     | 12        |
| <b>Index</b>                              | <b>13</b> |

# Chapter 1

## Data Structure Index

### 1.1 Data Structures

Here are the data structures with brief descriptions:

|  |    |
|--|----|
| <a href="#">AES256_CTR_DRBG_struct</a> | 3  |
| <a href="#">AES_XOF_struct</a>         | 3  |
| <a href="#">bitstream_t</a>            | 4  |
| <a href="#">distrib</a>                | 4  |
| <a href="#">fdistrib</a>               | 4  |
| <a href="#">mf3_e</a>                  | 5  |
| <a href="#">Node</a>                   | 6  |
| <a href="#">perm_network_t</a>         | 6  |
| <a href="#">range_t</a>                | 6  |
| <a href="#">reject_t</a>               | 7  |
| <a href="#">sha3_256incctx</a>         | 7  |
| <a href="#">sha3_384incctx</a>         | 8  |
| <a href="#">sha3_512incctx</a>         | 8  |
| <a href="#">shake128ctx</a>            | 8  |
| <a href="#">shake128incctx</a>         | 9  |
| <a href="#">shake256ctx</a>            | 9  |
| <a href="#">shake256incctx</a>         | 9  |
| <a href="#">swap_t</a>                 | 10 |
| <a href="#">tritstream_t</a>           | 10 |
| <a href="#">vf2_e</a>                  | 10 |
| <a href="#">vf3_e</a>                  | 11 |
| <a href="#">wave_pk_t</a>              | 11 |
| <a href="#">wave_sk_t</a>              | 12 |



## Chapter 2

# Data Structure Documentation

## 2.1 AES256\_CTR\_DRBG\_struct Struct Reference

### Data Fields

- unsigned char **Key** [32]
- unsigned char **V** [16]
- int **reseed\_counter**

### 2.1.1 Detailed Description

Definition at line 27 of file rng.h.

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

- NIST-kat/rng.h

## 2.2 AES\_XOF\_struct Struct Reference

### Data Fields

- unsigned char **buffer** [16]
- int **buffer\_pos**
- unsigned long **length\_remaining**
- unsigned char **key** [32]
- unsigned char **ctr** [16]

### 2.2.1 Detailed Description

Definition at line 19 of file rng.h.

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

- NIST-kat/rng.h

## 2.3 bitstream\_t Struct Reference

### Data Fields

- uint8\_t \* **data**
- size\_t **buf\_len**
- uint32\_t **byte\_pos**
- uint32\_t **bit\_pos**

### 2.3.1 Detailed Description

Definition at line 7 of file bitstream.h.

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

- util/bitstream.h

## 2.4 distrib Struct Reference

### Data Fields

- int **prec**
- int **size**
- int **offset**
- uint64\_t \* **proba**

### 2.4.1 Detailed Description

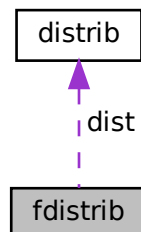
Definition at line 6 of file sample.c.

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

- wave/sample.c

## 2.5 fdistrib Struct Reference

Collaboration diagram for fdistrib:





## Data Fields

- int **size**
- int **offset**
- **distrib** \* **dist**

### 2.5.1 Detailed Description

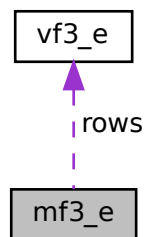
Definition at line 11 of file sample.c.

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

- wave/sample.c

## 2.6 mf3\_e Struct Reference

Collaboration diagram for mf3\_e:



## Data Fields

- **vf3\_e** \* **rows**
- size\_t **n\_row**
- size\_t **n\_col**

### 2.6.1 Detailed Description

Definition at line 21 of file arith\_f3.h.

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

- fq\_arithmetic/arith\_f3.h

## 2.7 Node Class Reference

### 2.7.1 Detailed Description

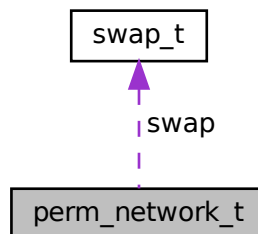
Definition at line 14 of file gen\_trit\_comp.py.

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

- gen\_trit\_comp.py

## 2.8 perm\_network\_t Struct Reference

Collaboration diagram for perm\_network\_t:



### Data Fields

- int **len**
- [swap\\_t](#) \* **swap**

### 2.8.1 Detailed Description

Definition at line 7 of file mf3permut.c.

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

- util/mf3permut.c

## 2.9 range\_t Struct Reference

### Data Fields

- int **min**
- int **max**

### 2.9.1 Detailed Description

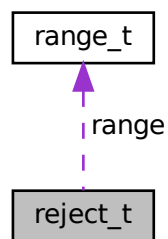
Definition at line 3 of file reject.c.

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

- wave/reject.c

## 2.10 reject\_t Struct Reference

Collaboration diagram for reject\_t:



### Data Fields

- int **size**
- int **offset**
- [range\\_t](#) \* **range**

#### 2.10.1 Detailed Description

Definition at line 7 of file reject.c.

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

- wave/reject.c

## 2.11 sha3\_256incctx Struct Reference

### Data Fields

- uint64\_t \* **ctx**

### 2.11.1 Detailed Description

Definition at line 38 of file fips202.h.

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

- prng/fips202.h

## 2.12 sha3\_384incctx Struct Reference

### Data Fields

- uint64\_t \* ctx

### 2.12.1 Detailed Description

Definition at line 43 of file fips202.h.

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

- prng/fips202.h

## 2.13 sha3\_512incctx Struct Reference

### Data Fields

- uint64\_t \* ctx

### 2.13.1 Detailed Description

Definition at line 48 of file fips202.h.

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

- prng/fips202.h

## 2.14 shake128ctx Struct Reference

### Data Fields

- uint64\_t \* ctx

### 2.14.1 Detailed Description

Definition at line 23 of file fips202.h.

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

- prng/fips202.h

## 2.15 shake128incctx Struct Reference

### Data Fields

- uint64\_t \* ctx

### 2.15.1 Detailed Description

Definition at line 18 of file fips202.h.

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

- prng/fips202.h

## 2.16 shake256ctx Struct Reference

### Data Fields

- uint64\_t \* ctx

### 2.16.1 Detailed Description

Definition at line 33 of file fips202.h.

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

- prng/fips202.h

## 2.17 shake256incctx Struct Reference

### Data Fields

- uint64\_t ctx [26]

### 2.17.1 Detailed Description

Definition at line 28 of file fips202.h.

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

- prng/fips202.h

## 2.18 swap\_t Struct Reference

### Data Fields

- uint16\_t **min**
- uint16\_t **max**

### 2.18.1 Detailed Description

Definition at line 3 of file mf3permut.c.

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

- util/mf3permut.c

## 2.19 tritstream\_t Struct Reference

### Data Fields

- uint8\_t \* **data**
- size\_t **buf\_len**
- uint32\_t **byte\_pos**
- uint32\_t **factor**

### 2.19.1 Detailed Description

Definition at line 7 of file tritstream.h.

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

- util/tritstream.h

## 2.20 vf2\_e Struct Reference

### Data Fields

- wave\_word \* **x**
- size\_t **alloc**
- size\_t **size**

### 2.20.1 Detailed Description

Definition at line 10 of file arith\_f3.h.

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

- fq\_arithmetic/arith\_f3.h

## 2.21 vf3\_e Struct Reference

### Data Fields

- wave\_word \* **r0**
- wave\_word \* **r1**
- size\_t **alloc**
- size\_t **size**

### 2.21.1 Detailed Description

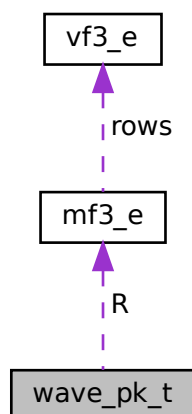
Definition at line 15 of file arith\_f3.h.

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

- fq\_arithmetic/arith\_f3.h

## 2.22 wave\_pk\_t Struct Reference

Collaboration diagram for wave\_pk\_t:



## Data Fields

- [mf3\\_e](#) \* **R**

### 2.22.1 Detailed Description

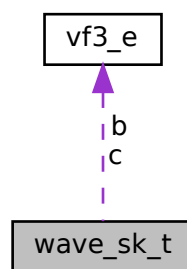
Definition at line 28 of file config.h.

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

- config.h

## 2.23 wave\_sk\_t Struct Reference

Collaboration diagram for wave\_sk\_t:



## Data Fields

- [vf3\\_e](#) \* **b**
- [vf3\\_e](#) \* **c**
- uint16\_t **perm** [N]
- uint8\_t **mk** [MK\_SIZE]

### 2.23.1 Detailed Description

Definition at line 22 of file config.h.

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

- config.h



# Index

AES256\_CTR\_DRBG\_struct, [3](#)

AES\_XOF\_struct, [3](#)

bitstream\_t, [4](#)

distrib, [4](#)

fdistrib, [4](#)

mf3\_e, [5](#)

Node, [6](#)

perm\_network\_t, [6](#)

range\_t, [6](#)

reject\_t, [7](#)

sha3\_256incctx, [7](#)

sha3\_384incctx, [8](#)

sha3\_512incctx, [8](#)

shake128ctx, [8](#)

shake128incctx, [9](#)

shake256ctx, [9](#)

shake256incctx, [9](#)

swap\_t, [10](#)

tritstream\_t, [10](#)

vf2\_e, [10](#)

vf3\_e, [11](#)

wave\_pk\_t, [11](#)

wave\_sk\_t, [12](#)