Wave

Generated by Doxygen 1.9.1

Chapter 1

Data Structure Index

1.1 Data Structures

Here are the data structures with brief descriptions:

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

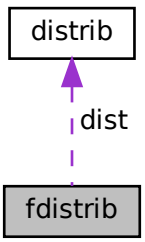
Definition at line 6 of file sample.c.

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

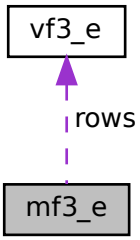
Definition at line 11 of file sample.c.

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

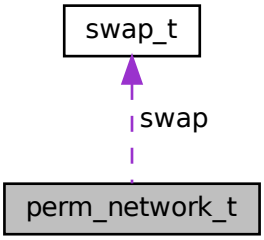
Definition at line 14 of file gen_trit_comp.py.

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

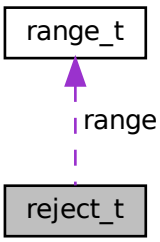
Definition at line 3 of file reject.c.

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

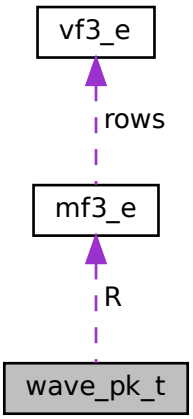
Definition at line 15 of file arith_f3.h.

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

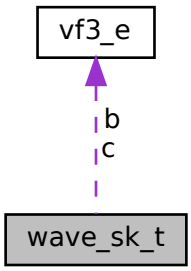
Definition at line 28 of file config.h.

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