libsfmt11213 Reference

Table of Contents

SCE CONFIDENTIAL

- 3 -

Constants

SCE_SFMT11213_ARRAY_SIZE

Array size for SFMT11213 pseudo random number calculation

Definition

```
#include <libsfmt11213.h>
#define SCE_SFMT11213_ARRAY_SIZE   88      /* (11213 / 128) + 1 */
```
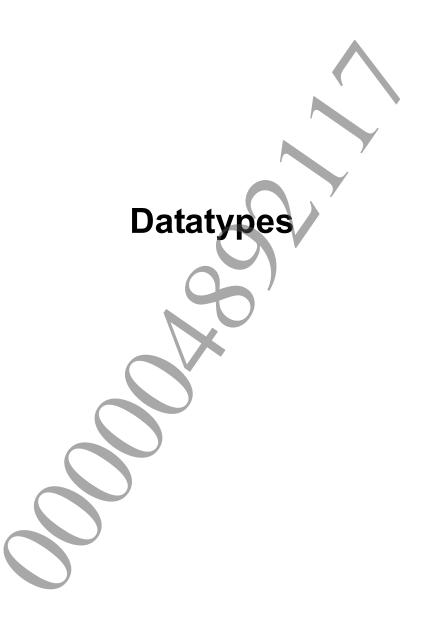
Description

This constant defines the array size for pseudo random numbers in conformance with SFMT11213.

In addition to indicating the array size that is maintained as state in the SceSfmt11213Context structure, this constant is also used by the sceSfmt11213FillArray32() and sceSfmt11213FillArray64() functions to indicate the minimum size for generating random numbers.

See Also

SceSfmt11213Context, sceSfmt11213FillArray32(), sceSfmt11213FillArray64()

SCE CONFIDENTIAL

- 5 -

Datatypes

SceSfmt11213Context

Context information for SFMT11213 pseudo random number calculation

Definition

```
#include <libsfmt11213.h>
typedef struct SceSfmt11213Context {
        unsigned int idx;
        unsigned int sfmt[SCE_SFMT11213_ARRAY_SIZE][4];
} SceSfmt11213Context;
```
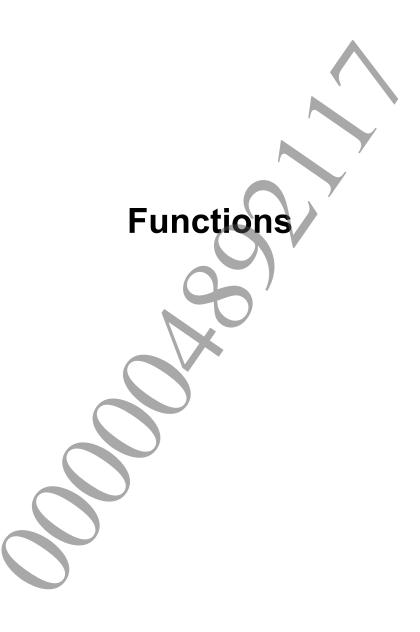
Description

This structure is a work area for calculating pseudo random numbers in conformance with SFMT11213.

One instance of this work area must be prepared for each random number sequence.

See Also

SCE_SFMT11213_ARRAY_SIZE,sceSfmt11213InitGenRand(),sceSfmt11213InitByArray()

- 7 -

Functions

sceSfmt11213InitGenRand

Initialize SFMT11213 pseudo random number work area

Definition

```
#include <libsfmt11213.h>
SceInt32 sceSfmt11213InitGenRand (
        SceSfmt11213Context *pCtx,
        SceUInt32 seed
);
```

Calling Conditions

Multithread safe

Arguments

pCtx   Pointer to an SceSfmt11213Context structure, which represents a random number
       sequence as a context.
seed   Specifies a random number sequence.

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function uses a 32-bit seed to initialize an SFMT11213 random number sequence, which is
represented by the SceSfmt11213Context structure. This function must be executed before the
sceSfmt11213GenRand32(), sceSfmt11213GenRand64(), sceSfmt11213FillArray32(),
and sceSfmt11213FillArray64() functions.

Since only the SceSfmt11213Context structure indicated by pCtx is initialized, multiple random
number sequences can be handled simultaneously by having multiple SceSfmt11213Context
structures.

See Also

SceSfmt11213Context, sceSfmt11213InitByArray()

sceSfmt11213InitByArray

Initialize SFMT11213 pseudo random number work area

Definition

```
#include <libsfmt11213.h>
SceInt32 sceSfmt11213InitByArray (
        SceSfmt11213Context *pCtx,
        const SceUInt32 initkey[],
        SceUInt32 keylength
);
```

Calling Conditions

Multithread safe

Arguments

pCtx	Pointer to an SceSfmt11213Context structure, which represents a random number sequence as a context.
initkey	Specifies the array to be used for initializing.
keylength	Number of elements in *initkey*.

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function uses an array of 32-bit seeds to initialize an SFMT11213 random number sequence, which is represented by the SceSfmt11213Context structure. This function must be executed before the sceSfmt11213GenRand32(), sceSfmt11213GenRand64(), sceSfmt11213FillArray32(), and sceSfmt11213FillArray64() functions.

Since only the SceSfmt11213Context structure indicated by *pCtx* is initialized, multiple random number sequences can be handled simultaneously by having multiple SceSfmt11213Context structures.

See Also

SceSfmt11213Context, sceSfmt11213InitGenRand()

sceSfmt11213GenRand32

Generate an SFMT11213 32-bit pseudo random number

Definition

```
#include <libmt11213.h>
SceUInt32 sceSfmt11213GenRand32 (
        SceSfmt11213Context *pCtx
);
```

Calling Conditions

Multithread safe

Arguments

pCtx   Pointer to an SceSfmt11213Context structure, which represents a random number sequence as a context.

Return Values

32-bit pseudo random number

Description

This function generates a 32-bit pseudo random number that conforms to SFMT11213.

Before using this function, the SceSfmt11213Context structure must be initialized by calling the sceSfmt11213InitGenRand() or sceSfmt11213InitByArray() functions.

See Also

SceSfmt11213Context, sceSfmt11213InitGenRand(), sceSfmt11213InitByArray()

SCE CONFIDENTIAL

sceSfmt11213GenRand64

Generate an SFMT11213 64-bit pseudo random number

Definition

```
#include <libmt11213.h>
SceUInt64 sceSfmt11213GenRand64 (
        SceSfmt11213Context *pCtx
);
```

Calling Conditions

Multithread safe

Arguments

pCtx   Pointer to an SceSfmt11213Context structure, which represents a random number
sequence as a context.

Return Values

64-bit pseudo random number

Description

This function generates a 64-bit pseudo random number that conforms to SFMT11213.

Before using this function, the SceSfmt11213Context structure must be initialized by calling the
sceSfmt11213InitGenRand() or sceSfmt11213InitByArray() functions.

Note that if the sceSfmt11213GenRand32() and sceSfmt11213GenRand64() functions are used
together and the sceSfmt11213GenRand64() function is called after the
sceSfmt11213GenRand32() function has been called an odd number of times, a full 64-bit random
number will not be obtained. Instead, this function will return a 64-bit value in which the upper 32 bits
are zero.

See Also

SceSfmt11213Context, sceSfmt11213InitGenRand(), sceSfmt11213InitByArray()

sceSfmt11213FillArray32

Generate an array of SFMT11213 32-bit pseudo random numbers

Definition

```
#include <libmt11213.h>
SceInt32 sceSfmt11213FillArray32 (
        SceSfmt11213Context *pCtx,
        SceUInt32 array[],
        SceUInt32 size
);
```

Calling Conditions

Multithread safe

Arguments

pCtx	Pointer to an SceSfmt11213Context structure, which represents a random number sequence as a context.
array	Buffer for receiving the generated random numbers
size	Number of elements in *array* (multiple of 4 that is larger than SCE_SFMT11213_ARRAY_SIZE*4)

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function generates an arbitrary number of 32-bit pseudo random numbers that conform to SFMT11213. *size* specifies the number of elements in *array* and must be a multiple of 4 that is larger than (SCE_SFMT11213_ARRAY_SIZE * 4).

Before using this function, the SceSfmt11213Context structure must be initialized by calling the sceSfmt11213InitGenRand() or sceSfmt11213InitByArray() functions.

When the sceSfmt11213FillArray32() function is used together with the sceSfmt11213GenRand32() function, the sceSfmt11213FillArray32() function can be called only after the sceSfmt11213GenRand32() function has been called (SCE_SFMT11213_ARRAY_SIZE * 4) times.

When the sceSfmt11213FillArray32() function is used together with the sceSfmt11213GenRand64() function, the sceSfmt11213FillArray32() function can be called only after the sceSfmt11213GenRand64() function has been called (SCE_SFMT11213_ARRAY_SIZE * 2) times.

See Also

SceSfmt11213Context, sceSfmt11213InitGenRand(), sceSfmt11213InitByArray()

SCE CONFIDENTIAL

sceSfmt11213FillArray64

Generate an array of SFMT11213 64-bit pseudo random numbers

Definition

```
#include <libmt11213.h>
SceInt32 sceSfmt11213FillArray64 (
        SceSfmt11213Context *pCtx,
        SceUInt64 array[],
        SceUInt32 size
);
```

Calling Conditions

Multithread safe

Arguments

pCtx	Pointer to an `SceSfmt11213Context` structure, which represents a random number sequence as a context.
array	Buffer for receiving the generated random numbers
size	Number of elements in *array* (multiple of 2 that is larger than `SCE_SFMT11213_ARRAY_SIZE*2`)

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function generates an arbitrary number of 64-bit pseudo random numbers that conform to SFMT11213. *size* specifies the number of elements in *array* and must be a multiple of 2 that is larger than (`SCE_SFMT11213_ARRAY_SIZE * 2`).

Before using this function, the `SceSfmt11213Context` structure must be initialized by calling the `sceSfmt11213InitGenRand()` or `sceSfmt11213InitByArray()` functions.

When the `sceSfmt11213FillArray64()` function is used together with the `sceSfmt11213GenRand32()` function, the `sceSfmt11213FillArray64()` function can be called only after the `sceSfmt11213GenRand32()` function has been called (`SCE_SFMT11213_ARRAY_SIZE * 4`) times.

When the `sceSfmt11213FillArray64()` function is used together with the `sceSfmt11213GenRand64()` function, the `sceSfmt11213FillArray64()` function can be called only after the `sceSfmt11213GenRand64()` function has been called (`SCE_SFMT11213_ARRAY_SIZE * 2`) times.

See Also

SceSfmt11213Context, sceSfmt11213InitGenRand(), sceSfmt11213InitByArray()