libsfmt1279 Reference

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

Document serial number: 000004892117

Document serial number: 000004892117

Table of Contents

Constants

SCE_SFMT1279_ARRAY_SIZE

Array size for SFMT1279 pseudo random number calculation

Definition

```
#include <libsfmt1279.h>
#define SCE_SFMT1279_ARRAY_SIZE     10      /* (1279 / 128) + 1 */
```

Description

This constant defines the array size for pseudo random numbers in conformance with SFMT1279.

In addition to indicating the array size that is maintained as state in the `SceSfmt1279Context` structure, this constant is also used by the `sceSfmt1279FillArray32()` and `sceSfmt1279FillArray64()` functions to indicate the minimum size for generating random numbers.

See Also

`SceSfmt1279Context`, `sceSfmt1279FillArray32()`, `sceSfmt1279FillArray64()`

Datatypes

SceSfmt1279Context

Context information for SFMT1279 pseudo random number calculation

Definition

```
#include <libsfmt1279.h>
typedef struct SceSfmt1279Context {
        unsigned int idx;
        unsigned int sfmt[SCE_SFMT1279_ARRAY_SIZE][4];
} SceSfmt1279Context;
```

Description

This structure is a work area for calculating pseudo random numbers in conformance with SFMT1279. One instance of this work area must be prepared for each random number sequence.

See Also

SCE_SFMT1279_ARRAY_SIZE, sceSfmt1279InitGenRand(), sceSfmt1279InitByArray()

Functions

sceSfmt1279InitGenRand

Initialize SFMT1279 pseudo random number work area

Definition

```
#include <libsfmt1279.h>
SceInt32 sceSfmt1279InitGenRand (
        SceSfmt1279Context *pCtx,
        SceUInt32 seed
);
```

Calling Conditions

Multithread safe

Arguments

pCtx Pointer to an `SceSfmt1279Context` 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 SFMT1279 random number sequence, which is represented by the `SceSfmt1279Context` structure. This function must be executed before the `sceSfmt1279GenRand32()`, `sceSfmt1279GenRand64()`, `sceSfmt1279FillArray32()`, and `sceSfmt1279FillArray64()` functions.

Since only the `SceSfmt1279Context` structure indicated by *pCtx* is initialized, multiple random number sequences can be handled simultaneously by having multiple `SceSfmt1279Context` structures.

See Also

`SceSfmt1279Context`, `sceSfmt1279InitByArray()`

sceSfmt1279InitByArray

Initialize SFMT1279 pseudo random number work area

Definition

```
#include <libsfmt1279.h>
SceInt32 sceSfmt1279InitByArray (
        SceSfmt1279Context *pCtx,
        const SceUInt32 initkey[],
        SceUInt32 keylength
);
```

Calling Conditions

Multithread safe

Arguments

pCtx	Pointer to an `SceSfmt1279Context` 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 SFMT1279 random number sequence, which is represented by the `SceSfmt1279Context` structure. This function must be executed before the `sceSfmt1279GenRand32()`, `sceSfmt1279GenRand64()`, `sceSfmt1279FillArray32()`, and `sceSfmt1279FillArray64()` functions.

Since only the `SceSfmt1279Context` structure indicated by *pCtx* is initialized, multiple random number sequences can be handled simultaneously by having multiple `SceSfmt1279Context` structures.

See Also

`SceSfmt1279Context`, `sceSfmt1279InitGenRand()`

sceSfmt1279GenRand32

Generate an SFMT1279 32-bit pseudo random number

Definition

```
#include <libmt1279.h>
SceUInt32 sceSfmt1279GenRand32 (
        SceSfmt1279Context *pCtx
);
```

Calling Conditions

Multithread safe

Arguments

pCtx Pointer to an `SceSfmt1279Context` 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 SFMT1279.

Before using this function, the `SceSfmt1279Context` structure must be initialized by calling the `sceSfmt1279InitGenRand()` or `sceSfmt1279InitByArray()` functions.

See Also

`SceSfmt1279Context`, `sceSfmt1279InitGenRand()`, `sceSfmt1279InitByArray()`

sceSfmt1279GenRand64

Generate an SFMT1279 64-bit pseudo random number

Definition

```
#include <libmt1279.h>
SceUInt64 sceSfmt1279GenRand64 (
        SceSfmt1279Context *pCtx
);
```

Calling Conditions

Multithread safe

Arguments

pCtx Pointer to an `SceSfmt1279Context` 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 SFMT1279.

Before using this function, the `SceSfmt1279Context` structure must be initialized by calling the `sceSfmt1279InitGenRand()` or `sceSfmt1279InitByArray()` functions.

Note that if the `sceSfmt1279GenRand32()` and `sceSfmt1279GenRand64()` functions are used together and the `sceSfmt1279GenRand64()` function is called after the `sceSfmt1279GenRand32()` 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

`SceSfmt1279Context`, `sceSfmt1279InitGenRand()`, `sceSfmt1279InitByArray()`

sceSfmt1279FillArray32

Generate an array of SFMT1279 32-bit pseudo random numbers

Definition

```
#include <libmt1279.h>
SceInt32 sceSfmt1279FillArray32 (
        SceSfmt1279Context *pCtx,
        SceUInt32 array[],
        SceUInt32 size
);
```

Calling Conditions

Multithread safe

Arguments

pCtx	Pointer to an SceSfmt1279Context 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_SFMT1279_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 SFMT1279. *size* specifies the number of elements in *array* and must be a multiple of 4 that is larger than (SCE_SFMT1279_ARRAY_SIZE * 4).

Before using this function, the SceSfmt1279Context structure must be initialized by calling the sceSfmt1279InitGenRand() or sceSfmt1279InitByArray() functions.

When the sceSfmt1279FillArray32() function is used together with the sceSfmt1279GenRand32() function, the sceSfmt1279FillArray32() function can be called only after the sceSfmt1279GenRand32() function has been called (SCE_SFMT1279_ARRAY_SIZE * 4) times.

When the sceSfmt1279FillArray32() function is used together with the sceSfmt1279GenRand64() function, the sceSfmt1279FillArray32() function can be called only after the sceSfmt1279GenRand64() function has been called (SCE_SFMT1279_ARRAY_SIZE * 2) times.

See Also

SceSfmt1279Context, sceSfmt1279InitGenRand(), sceSfmt1279InitByArray()

sceSfmt1279FillArray64

Generate an array of SFMT1279 64-bit pseudo random numbers

Definition

```
#include <libmt1279.h>
SceInt32 sceSfmt1279FillArray64 (
        SceSfmt1279Context *pCtx,
        SceUInt64 array[],
        SceUInt32 size
);
```

Calling Conditions

Multithread safe

Arguments

pCtx	Pointer to an SceSfmt1279Context 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_SFMT1279_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 SFMT1279. *size* specifies the number of elements in *array* and must be a multiple of 2 that is larger than (SCE_SFMT1279_ARRAY_SIZE * 2).

Before using this function, the SceSfmt1279Context structure must be initialized by calling the sceSfmt1279InitGenRand() or sceSfmt1279InitByArray() functions.

When the sceSfmt1279FillArray64() function is used together with the sceSfmt1279GenRand32() function, the sceSfmt1279FillArray64() function can be called only after the sceSfmt1279GenRand32() function has been called (SCE_SFMT1279_ARRAY_SIZE * 4) times.

When the sceSfmt1279FillArray64() function is used together with the sceSfmt1279GenRand64() function, the sceSfmt1279FillArray64() function can be called only after the sceSfmt1279GenRand64() function has been called (SCE_SFMT1279_ARRAY_SIZE * 2) times.

See Also

SceSfmt1279Context, sceSfmt1279InitGenRand(), sceSfmt1279InitByArray()