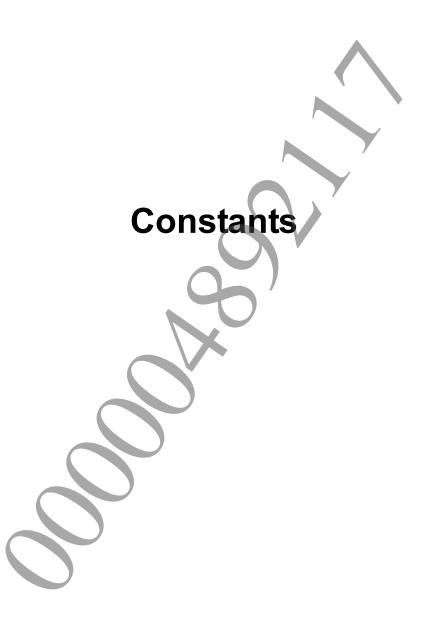


© 2011 Sony Computer Entertainment Inc. All Rights Reserved. SCE Confidential

Table of Contents

Constants	
SCE_SFMT2281_ARRAY_SIZE	
Datatypes	
SceSfmt2281Context	
Functions	
sceSfmt2281InitGenRand	8
sceSfmt2281InitByArray	
sceSfmt2281GenRand32	10
sceSfmt2281GenRand64	1′
sceSfmt2281FillArray32	12
sceSfmt2281FillArray64	13



SCE_SFMT2281_ARRAY_SIZE

Array size for SFMT2281 pseudo random number calculation

Definition

#include <libsfmt2281.h>
#define SCE SFMT2281 ARRAY SIZE 18 /* (2281 / 128) + 1 */

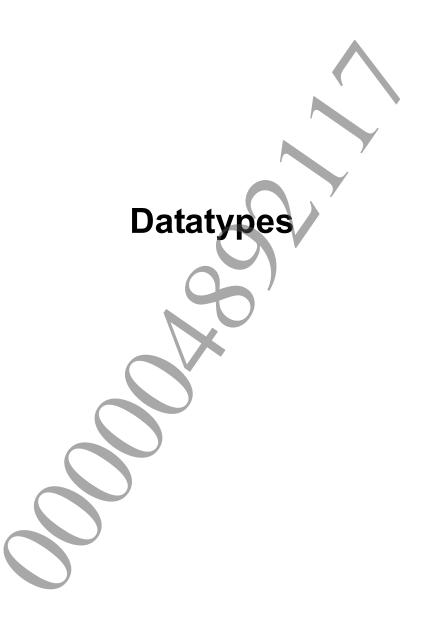
Description

This constant defines the array size for pseudo random numbers in conformance with SFMT2281. In addition to indicating the array size that is maintained as state in the SceSfmt2281Context structure, this constant is also used by the sceSfmt2281FillArray32() and sceSfmt2281FillArray64() functions to indicate the minimum size for generating random numbers.

See Also

SceSfmt2281Context, sceSfmt2281FillArray32(), sceSfmt2281FillArray64()





SceSfmt2281Context

Context information for SFMT2281 pseudo random number calculation

Definition

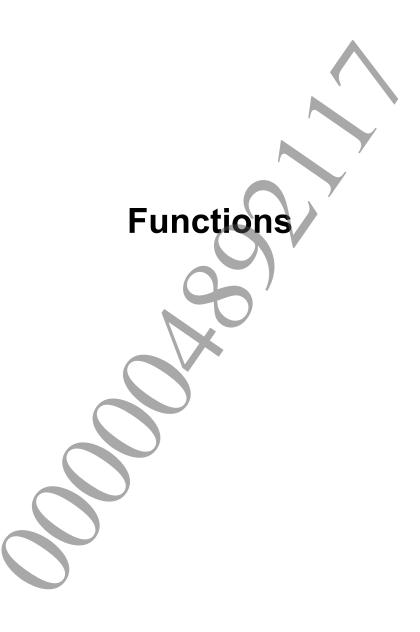
```
#include <libsfmt2281.h>
typedef struct SceSfmt2281Context {
          unsigned int idx;
          unsigned int sfmt[SCE_SFMT2281_ARRAY_SIZE][4];
} SceSfmt2281Context;
```

Description

This structure is a work area for calculating pseudo random numbers in conformance with SFMT2281. One instance of this work area must be prepared for each random number sequence.

See Also

SCE SFMT2281 ARRAY SIZE, sceSfmt2281InitGenRand(), sceSfmt2281InitByArray()



sceSfmt2281InitGenRand

Initialize SFMT2281 pseudo random number work area

Definition

Calling Conditions

Multithread safe

Arguments

Pointer to an SceSfmt2281Context 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	
SCE OK	Normal completion

Description

This function uses a 32-bit seed to initialize an SFMT2281 random number sequence, which is represented by the SceSfmt2281Context structure. This function must be executed before the sceSfmt2281GenRand32 (), sceSfmt2281GenRand34 (), sceSfmt2281FillArray32 (), and sceSfmt2281FillArray34 () functions.

Since only the SceSfmt2281Context structure indicated by pCtx is initialized, multiple random number sequences can be handled simultaneously by having multiple SceSfmt2281Context structures.

See Also

SceSfmt2281Context, sceSfmt2281InitByArray()

sceSfmt2281InitByArray

Initialize SFMT2281 pseudo random number work area

Definition

Calling Conditions

Multithread safe

Arguments

Pointer to an SceSfmt2281Context 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	
SCE_OK	Normal completion

Description

This function uses an array of 32-bit seeds to initialize an SFMT2281 random number sequence, which is represented by the SceSfmt2281Context structure. This function must be executed before the sceSfmt2281GenRand32(), sceSfmt2281GenRand64(), sceSfmt2281FillArray32(), and sceSfmt2281FillArray64() functions.

Since only the SceSfmt2281Context structure indicated by pCtx is initialized, multiple random number sequences can be handled simultaneously by having multiple SceSfmt2281Context structures.

See Also

SceSfmt2281Context, sceSfmt2281InitGenRand()

Document serial number: 000004892117

sceSfmt2281GenRand32

Generate an SFMT2281 32-bit pseudo random number

Definition

Calling Conditions

Multithread safe

Arguments

pCtx Pointer to an SceSfmt2281Context 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 SFMT2281.

Before using this function, the SceSfmt2281Context structure must be initialized by calling the sceSfmt2281InitGenRand() or sceSfmt2281InitByArray() functions.

See Also

SceSfmt2281Context, sceSfmt2281InitGenRand(), sceSfmt2281InitByArray()

sceSfmt2281GenRand64

Generate an SFMT2281 64-bit pseudo random number

Definition

Calling Conditions

Multithread safe

Arguments

pCtx Pointer to an SceSfmt2281Context 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 SFMT2281.

Before using this function, the SceSfmt2281Context structure must be initialized by calling the sceSfmt2281InitGenRand() or sceSfmt2281InitByArray() functions.

Note that if the sceSfmt2281GenRand32() and sceSfmt2281GenRand64() functions are used together and the sceSfmt2281GenRand64() function is called after the sceSfmt2281GenRand32() 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

SceSfmt2281Context, sceSfmt2281InitGenRand(), sceSfmt2281InitByArray()

sceSfmt2281FillArray32

Generate an array of SFMT2281 32-bit pseudo random numbers

Definition

Calling Conditions

Multithread safe

Arguments

```
Pointer to an SceSfmt2281Context 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_SFMT2281_ARRAY_SIZE*4)
```

Return Values

If an error occurs, a negative value is returned.

Value	
SCE_OK	Normal completion

Description

This function generates an arbitrary number of 32-bit pseudo random numbers that conform to SFMT2281. size specifies the number of elements in array and must be a multiple of 4 that is larger than (SCE SFMT2281 ARRAY SIZE * 4).

Before using this function, the SceSfmt2281Context structure must be initialized by calling the sceSfmt2281InitGenRand() or sceSfmt2281InitByArray() functions.

When the sceSfmt2281FillArray32() function is used together with the sceSfmt2281GenRand32() function, the sceSfmt2281FillArray32() function can be called only after the sceSfmt2281GenRand32() function has been called (SCE_SFMT2281_ARRAY_SIZE * 4) times.

When the sceSfmt2281FillArray32() function is used together with the sceSfmt2281GenRand64() function, the sceSfmt2281FillArray32() function can be called only after the sceSfmt2281GenRand64() function has been called (SCE_SFMT2281_ARRAY_SIZE * 2) times.

See Also

SceSfmt2281Context, sceSfmt2281InitGenRand(), sceSfmt2281InitByArray()

sceSfmt2281FillArray64

Generate an array of SFMT2281 64-bit pseudo random numbers

Definition

Calling Conditions

Multithread safe

Arguments

```
Pointer to an SceSfmt2281Context 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_SFMT2281_ARRAY_SIZE*2)
```

Return Values

If an error occurs, a negative value is returned.

Value	
SCE_OK	Normal completion

Description

This function generates an arbitrary number of 64-bit pseudo random numbers that conform to SFMT2281. *size* specifies the number of elements in *array* and must be a multiple of 2 that is larger than (SCE SFMT2281 ARRAY SIZE * 2).

Before using this function, the SceSfmt2281Context structure must be initialized by calling the sceSfmt2281InitGenRand() or sceSfmt2281InitByArray() functions.

When the sceSfmt2281FillArray64() function is used together with the sceSfmt2281GenRand32() function, the sceSfmt2281FillArray64() function can be called only after the sceSfmt2281GenRand32() function has been called (SCE_SFMT2281_ARRAY_SIZE * 4) times.

When the sceSfmt2281FillArray64() function is used together with the sceSfmt2281GenRand64() function, the sceSfmt2281FillArray64() function can be called only after the sceSfmt2281GenRand64() function has been called (SCE_SFMT2281_ARRAY_SIZE * 2) times.

See Also

SceSfmt2281Context, sceSfmt2281InitGenRand(), sceSfmt2281InitByArray()