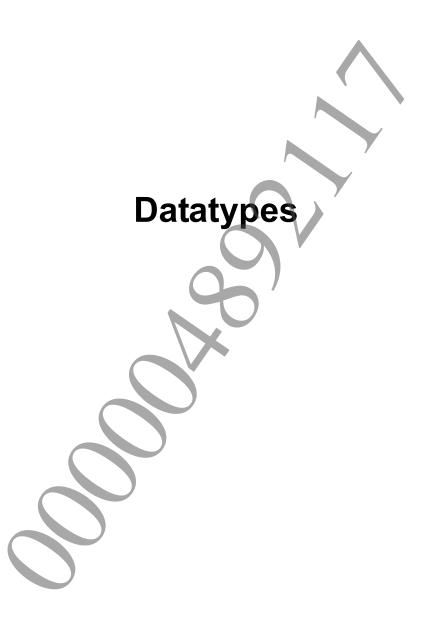


© 2011 Sony Computer Entertainment Inc. All Rights Reserved. SCE Confidential

# **Table of Contents**

Datatyp	es	3
	SceSha224Context	
Digest F	Function (Comprehensive)	
•	sceSha224Digest	
Digest F	Functions (Divided)sceSha224BlockInit	7
	sceSha224BlockUpdate	g
	sceSha224BlockResult	



# SceSha224Context

Context information for SHA-224 digest value computation

#### **Definition**

#### **Members**

h Work area

pad Padding for adjusting alignment

usRemains Less than 64 bytes of remaining data, which was temporarily copied within the

SceSha224Context structure

usComputed Digest value computed flag
ullTotalLen Total data size (bytes)

buf Temporary copy of less than 64 bytes of data

result Temporary copy of the digest value computation result

pad2 Padding for adjusting alignment

## **Description**

This structure is used as a work area when computation of the SHA-224 digest value is divided up. Since the sceSha224BlockInit(), sceSha224BlockUpdate(), and sceSha224BlockResult() functions use this structure as a work area, an application must not directly access the members of this structure.

#### See Also

sceSha224BlockInit(), sceSha224BlockUpdate(), sceSha224BlockResult()



# sceSha224Digest

# Compute SHA-224 digest

#### **Definition**

```
#include <libsha224.h>
SceInt32 sceSha224Digest(
        const void *plain,
        SceUInt32 len,
        SceUChar8 *digest
);
```

# **Calling Conditions**

Multithread safe

## **Arguments**

Pointer to plaintext data for which digest value is to be computed. plain len Data size (bytes) of plaintext data for which digest value is to be computed. digest Returns computed digest value (28 bytes).

### **Return Values**

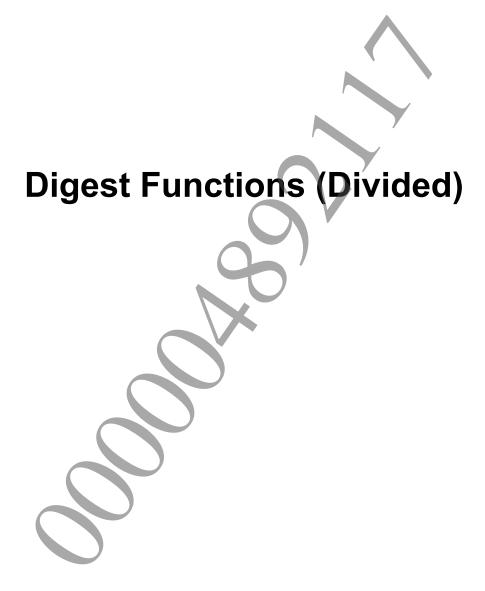
If an error occurs, a negative value is returned.

Value	
SCE OK	Normal termination

## **Description**

This function computes the SHA-224 digest value.

This function is used when all data of the plaintext for which the digest value is to be computed has been expanded in memory



# sceSha224BlockInit

Initialize digest value computation work area

#### **Definition**

```
#include <libsha224.h>
SceInt32 sceSha224BlockInit(
        SceSha224Context *pContext
);
```

## **Calling Conditions**

Multithread safe

## **Arguments**

pContext Address of digest value computation work area.

## **Return Values**

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA224_ERROR_INVALID_POINTER	Invalid pContext address

## **Description**

This function initializes the work area that is used to compute the SHA-224 digest value. It should be called before sceSha224BlockUpdate() function.

### See Also

SceSha224Context, sceSha224BlockUpdate(), sceSha224BlockResult()



# sceSha224BlockUpdate

# SHA-224 digest value computation processing

### **Definition**

# **Calling Conditions**

Multithread safe

### **Arguments**

pContext Address of digest value computation work area.

plain Pointer to plaintext data for which digest value is to be computed.

len Data size (bytes) of plaintext data for which digest value is to be computed.

#### **Return Values**

If an error occurs, a negative value is returned.

Value	Result	
SCE_OK	Normal termination	
SCE_SHA224_ERROR_INVALID_POINT	ER Invalid pContext or plain address	;

### **Description**

This function uses the plaintext specified by <code>plain</code> and <code>len</code> to update the work area within the <code>SceSha224Context</code> structure. By dividing the computation into multiple steps, the <code>sceSha224BlockUpdate()</code> function, which can be called any number of times between the <code>sceSha224BlockInit()</code> and <code>sceSha224BlockResult()</code> functions, enables the digest value to be computed even for a large amount of data that cannot fit in memory.

### See Also

SceSha224Context, sceSha224BlockInit(), sceSha224BlockResult()

# sceSha224BlockResult

## Get computed SHA-224 digest

#### **Definition**

## **Calling Conditions**

Multithread safe

## **Arguments**

pContext Address of digest value computation work area.

digest Returns the computed digest value (28 bytes).

#### **Return Values**

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA224_ERROR_INVALID_P	POINTER Invalid pContext or digest address

## **Description**

This function retrieves the computed digest value from the SceSha224Context structure. The SHA-224 algorithm computes a digest value in increments of 64 bytes, so a remaining amount less than 64 bytes may have been temporarily copied within the SceSha224Context structure by the sceSha224BlockUpdate() function. If this remaining data exists, the final digest value can be obtained by calling the sceSha224BlockResult() function. Always use the sceSha224BlockResult() function to obtain the digest value.

The digest value of the SceSha224Context structure is valid until the next time sceSha224BlockInit() function or sceSha224BlockUpdate() function is called.

### See Also

SceSha224Context, sceSha224BlockInit(), sceSha224BlockUpdate()