**安全IP软件**

**操作使用说明书**

[1 引言 - 2 -](#_Toc4770134)

[1.1 标示 - 2 -](#_Toc4770135)

[1.2 软件概述 - 2 -](#_Toc4770136)

[1.3 文档概述 - 2 -](#_Toc4770137)

[2 引用文件 - 2 -](#_Toc4770138)

[3 软件平台综述 - 2 -](#_Toc4770139)

[3.1 软件应用案例 - 2 -](#_Toc4770140)

[3.2软件环境 - 3 -](#_Toc4770141)

[4 平台搭建 - 3 -](#_Toc4770142)

[4.1 整体架构 - 3 -](#_Toc4770143)

[4.2 硬件设置 - 3 -](#_Toc4770144)

[4.3 软件安装 - 3 -](#_Toc4770145)

[5 软件使用指南 - 3 -](#_Toc4770146)

[5.1概况 - 3 -](#_Toc4770147)

[5.2软件使用 - 4 -](#_Toc4770148)

[5.3 屏幕输出 - 4 -](#_Toc4770149)

[5.4 波形输出 - 4 -](#_Toc4770150)

# 1 引言

## 1.1 标示

1. 本文档是安全IP软件的详细说明性文档。
2. 本文档中安全IP软件都用简称SISC\_Security代替。

## 1.2 软件概述

SISC\_Security软件是安全算法的C代码，其中包含了以下的算法：AES加解密，DES加解密，M1加解密，M2加解密，M4加解密，HASH加解密，ZUC加解密。

各种加解密算法不仅包含了算法的C代码，还包含了算法的测试代码示例程序，用户可根据自己的需求编写自己的测试代码。

## 1.3 文档概述

本文档详细描述了系统尤其是软件系统的操作流程及规范，方便实际使用者上手操作和运行使用，初次使用本操作系统者请详细阅读。

# 2 引用文件

1. GB/T 8567-2006《计算机软件文档编制规范》

# 3 软件平台综述

## 3.1 软件应用案例

SISC\_Security在linux服务器上运行，运行信息和结果在屏幕上显示，也可以生dump文件，可以查看波形。

## 3.2软件环境

SISC\_Security运行所需的环境如下：

**硬件平台**：

Linux服务器

**软件平台**：

Gcc编译器

Verilator软件

# 4 平台搭建

## 4.1 整体架构

整个C代码程序，包含相应的算法程序，以及相关的测试代码。

## 4.2 硬件设置

## 4.3 软件安装

SISC\_Security软件以C代码的方式交付，不需要安装。

# 5 软件使用指南

## 5.1概况

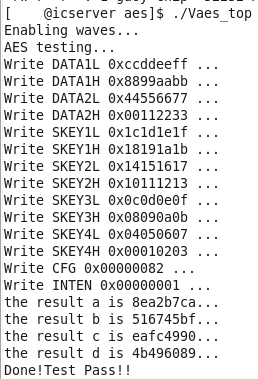
SISC\_Security软件通过C代码实现了加解密的算法，用户通过调用加解密算法的C代码，可以验证算法以及和用户代码的联调。

## 5.2软件使用

在提交的文件中包含了相应的测试make文件。可以使用命令make –f test.mk来生成可执行的测试文件。生成的可执行文件格式为V算法\_top。比如aes算法生成的可执行文件为Vaes\_top。直接运行此文件即可。

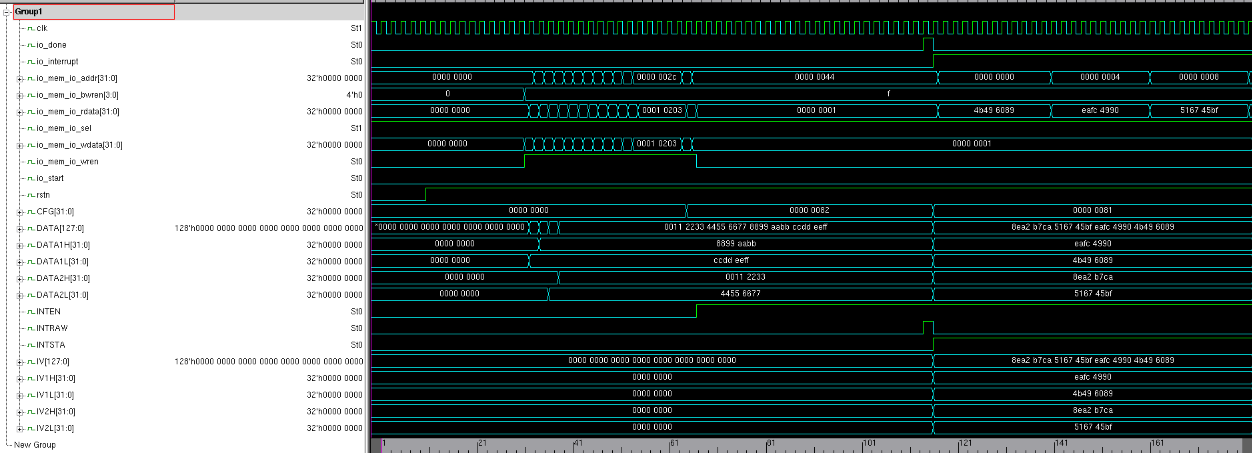
## 5.3 屏幕输出

同样，使用AES算法的例子，测试程序的屏幕输出：



## 5.4 波形输出

测试程序运行完后会输出波形文件dump.vcd。可以打开看波形。下面是AES的示例波形图：



《完》