Detailed Explanation of SAWScript for Verifying the `encKeySchedule` Function

Introduction

This document provides a detailed explanation of the SAWScript used to verify the `encKeySchedule` function written in C against its Cryptol specification. Each line of the script is explained in great detail to ensure a thorough understanding of the verification process.

SAWScript

Explanation

Line 1: This line includes the common helper functions defined in the `helpers.saw` file. These helper functions provide basic functionalities such as memory allocation and initialization, which are reused across different SAWScript files.

Line 2: This line imports the Cryptol specification for the `encKeySchedule` function from the `HIGHT.cry` file. The imported module contains the Cryptol definition of the function that will be used for verification.

Line 4: This command loads the Cryptol module `HIGHT.cry` into the SAW environment, making its functions and definitions available for use in the script.

Lines 6-10: This block defines a helper function `ptr_to_fresh`, which allocates a fresh variable `x` of type `ty` with a given name `n`, initializes a pointer `p` to this variable, and returns a tuple containing `x` and `p`.

Line 12: This line begins the definition of the `encKeySchedule_setup` function, which sets up the verification environment for the `encKeySchedule` function.

Lines 13-15: These lines allocate fresh variables and pointers for the arrays `enc_WK`, `enc_SK`, and `MK`. The `ptr_to_fresh` function is used for writable arrays, while `ptr_to_fresh_readonly` is used for the read-only master key array.

Line 17: This command executes the `encKeySchedule` function with the allocated pointers as arguments. The function operates on the memory locations pointed to by these pointers.

Line 19: This line evaluates the Cryptol specification of `encKeySchedule` with the allocated arrays `enc_WK`, `enc_SK`, and `MK`, and stores the result.

Lines 20-21: These lines assert that the memory locations pointed to by `p_enc_WK` and `p_enc_SK` should contain the values produced by the Cryptol specification of `encKeySchedule`.

Line 24: This line begins the definition of the `main` function, which is the entry point for the SAWScript execution.

Line 25: This command loads the LLVM bitcode module for the C implementation of `encKeySchedule` from the file `tests/hight.bc`.

Line 28: This line runs the verification of the `encKeySchedule` function. It compares the results of the C implementation with the Cryptol specification using the Z3 solver. The `encKeySchedule_setup` function is used to set up the verification environment.

Line 31: This command prints the result of the verification process.

Line 34: This line runs the `main` function, starting the verification process.