CHALMERS

Department of Computer Science and Engineering

2018-08-13

DAT093
Introduction to Electronic System Design

Using encrypted source files in QuestaSim

Introduction

Many companies use encrypted VHDL files to hide their designs. In this paper, we will look on how to create an encrypted VHDL source file and how to simulate the file using a test bench.

Example code

We will use the 1-bit full adder that we have been using before as an example. The original code looks like this

```
LIBRARY ieee;
USE ieee.std_logic_1164.ALL;

ENTITY full_adder IS
   PORT (a:IN STD_LOGIC;
         b:IN STD_LOGIC;
         cin:IN STD_LOGIC;
         s:OUT STD_LOGIC;
         cout:OUT STD_LOGIC);
END full_adder;

ARCHITECTURE arch_full_adder OF full_adder IS
BEGIN
   s<=(a XOR b) XOR cin;
   cout<=(a AND b) OR
         (a AND cin) OR
         (b AND cin);
END arch_full_adder;
```

To prepare the source code for encryption

Now we want to encrypt the implementation, that is the architecture. To do this we edit the source code and surround the architecture with

```
`protect begin
```

before the architecture that we like to encrypt and

```
`protect end
```

after the architecture.

Our edited source code looks like this

```
LIBRARY ieee;
USE ieee.std_logic_1164.ALL;

ENTITY full_adder IS
   PORT (a:IN STD_LOGIC;
         b:IN STD_LOGIC;
         cin:IN STD_LOGIC;
         s:OUT STD_LOGIC;
         cout:OUT STD_LOGIC);
END full_adder;

`protect begin
ARCHITECTURE arch_full_adder OF full_adder IS
BEGIN
   s<=(a XOR b) XOR cin;
   cout<=(a AND b) OR
         (a AND cin) OR
         (b AND cin);
END arch_full_adder;
`protect end
```

The additions are highlighted in red.

To create the encrypted source code

Start by creating a new QuestaSim project. Place the source file `full_adder.vhdl` in the project folder.

The compilation of the encrypted file cannot be done from the GUI but will have to be done by giving a command in the Transcript window. The syntax is

```
vcom +protect=<name of encrypted_file>.vhdp <name of source_file>.vhdl
```

so in our case it would be

```
vcom +protect=full_adder.vhdp full_adder.vhdl
```

When we run the command the encrypted file `full_adder.vhdp` will be created and it looks like this

```
LIBRARY ieee;
USE ieee.std_logic_1164.ALL;

ENTITY full_adder IS
   PORT (a:IN STD_LOGIC;
         b:IN STD_LOGIC;
         cin:IN STD_LOGIC;
         s:OUT STD_LOGIC;
         cout:OUT STD_LOGIC);
END full_adder;
`protect begin_protected
`protect version = 1
`protect encrypt_agent = "QuestaSim" , encrypt_agent_info = "10.6b"
`protect key_keyowner = "Mentor Graphics Corporation" , key_keyname = "MGC-
VERIF-SIM-RSA-2"
`protect key_method = "rsa"
`protect encoding = ( enctype = "base64" , line_length = 64 , bytes = 256 )
`protect key_block
JE3JL27meEIGrH3KS8PUukiDJE4KdWsdCiI16V2KXKWma5ghn8IEs/mKM7g3cfBk
qkHR8fGEDtZK217qbJmxB7SygN3IyXTpOkyaoI2rjLswvxFPrD9Q/8u4YNd4BCeO
DLFOwndCcGWOeH14JxSR6IsiMZpgO9oAGgX5X4TGROsjacHFsykjhPuroIaNRQSd
/qIEKR0xPXKOuwTOORy54yNIgIb3Xvw6ryYcqRLxFRED1BNMqHqCKptk4E+zAWC0
QBBdL5yGu/dTWfe72hrLpnPyCZVDf/e6OZtKlNZwLpxZU46yM1pkOoeqtYTej4Te
vtHeYMzlYTegdvGB6p5Lag==
`protect data_method = "aes128-cbc"
`protect encoding = ( enctype = "base64" , line_length = 64 , bytes = 192 )
`protect data_block
9RHDsJPbLbDmSyMp+hMcI/mS+vgSvzPOlyGzkt8OKO0HD5GASznTUJ+Wi5m655fF
UKK5BQuiF3vRtxkzRf6ZM9teUZTJEc0WQZgyTMonO8j0L1n1yQE4479gyGxmlM/b
```

```
R99S2yk3e1MnALmsHQWQiKZGi0MKjuZVOhKv10N32FSzWYO5KNQdhRTEmt3XVoVu
EYfl9+zh7zFaDKzPgTTDmcl78Az9UDHMzkWMhtZIPF30cQzvIVWhTvUNutgWXPEC
`protect end_protected
```

As we can see the entity is fully visible, but the architecture is not readable.

Setting up the project and simulating the design with a testbench

Now remove the source file `full_adder.vhdl` from the project and instead add the encrypted file `full_adder.vhdp`.

Finish the project by adding the testbench for the design and the do file to run the simulation.

Since the encrypted file haven´t been compiled from the GUI but from the Transcript windows command line it will still be shown with a question mark ? and not a check sign ✓ but this is OK.

The next step is to compile the testbench and that can be done from the GUI in the normal way. Since the enkrypted file shouldn´t be compiled again, as we said this can´t be done from the GUI, you should select Compile/Compile Selected and compile the testbench and any other source files that are not encrypted.

What´s left is to run the simulation in the normal way.

Using the encrypted file in another project

If you supply the encrypted file to someone for use in another project, then after creating the project the encrypted file must be compiled down to the projects work folder. You do this by running

```
vcom <name_of_encrypted_file>.vhdlp
```

from the command line in the Transcript window.

After this you proceed as above and compile the top-level design that uses the encrypted file and any other uncrypted files and do the simulation as usual.