REMOTE CONTROL AND TESTING OF THE INTERACTIVE TV-DECODER

VLČEK, K.
Department of Electronics
Faculty of Electrical Engng. and Computer Science
VŠB-Technical University of Ostrava
708 33 Ostrava-Poruba
Czech Republic
e-mail: karel.vlcekvsb.cz

Abstract

The article deals with assembling and application of a complex sequential circuit VHDL (VHSIC (Very High-Speed Integrated Circuit) Hardware Description Language) model. The circuit model is a core of a cryptographic device for the signal encoding and decoding of discreet transmissions by TV-cable net. The cryptographic algorithm is changable according to the user's wishes. The principles of creation and example implementations are presented in the article. The behavioural model is used to minimize mistakes in the ASICs (Application Specific Integrated Circuits). The circuit implementation uses the FPGA (Field Programmable Gate Array) technology. The diagnostics of the circuit is based on remote testing by the IEEE Std 1149.1-1990. The VHDL model of diagnostic subsystem is created as an orthogonal model in relation to the cryptographic circuit VHDL model.

Keywords:

VHDL Behavioural Model. TV-interactive Decoder. Built-In Test. Boundary-Scan Test. Mixed Signal Test. FPGA. Cryptographic System.

1. Introduction

A sender wants to send a message to the user in such a way that an enemy with a wiretap on the channel will not be able to understand the message. The modern cryptosystems use error-correcting codes. The cryptography is typical very sensitive to noise. For this reason it is advisable to combine both the encryption and the error-correction codes. It is easier since encryption and decryption are usually quite demanding to apply data compression before encrypting. An error-correcting code [1] will be used as another application.

Before implementation, the modelling was used. The VHDL supports three distinct styles for the description of hardware architecture. The first and most general is the behavioural description in which the transformation is described in sequential programm statements that look lika a high level computer programming language. The second is data-flow description style of description embodied in register transfer language. The last one is a structural description. The architecture is expressed as a hierarchical arrangement of interconnected components.

2. Secret Key Encryption

One possibility of encryption is to use a secret key, which is greater or equal to the lenght of encrypted message. If the key is a random word, the encrypting method is completely secure. The method of using a random key is generating a linear feedback shift register (LFSR) sequence.

The weak point of this method is that the enemy, once deciding that this encryption was applied, can break the code whenever he learns a source message of a small length together with its encryption. In this sence, LFSR sequencers are insecure, and an application of non-linear elements is advisable.

3. Non-linear Element

The non-linear element can be implemented by a simple hardware. For an optimal bit choice, a specific method has been recommended. The method makes use of an array representation of the R-function into a two dimensional fied, the coordinates of which are the values of pseudorandom words. The pseudorandom sequences at least look random to the eye, whereas the corresponding arrays have a conspicuous non-random feature, having a nearly identical morphology.

Using the pseudorandom function R is given by expression R = (Pm) XOR (Pn) where Pm and Pn are selected bits of the remainder of multipliyng. This non-linear operation gives non-linear function and the pseudorandom function R is able to reach good results if the numbers m and n cannot be divided by a common divisor. If this condition is not fulfilled or the numbers are less then number four, the pseudorandom array gets more periodical.

This would be displayed as a dense retical of zero values of the rounding function R. When choosing big values m and n, a very coarsely structured pseudorandom array in the vinicity to zero values is generated.

4. Programmable Element

Another disadvantage of the pseudorandom function generated according to function R is its short periodicity, which is apparent in the vinicity to the zero values. For this reason the function has been generated out of three variables according to common sense.

Function $R' = (P_m)\ XOR\ (P_n)\ XOR\ (P_p)$. These pseudorandom fields are "finely grained". For final implementation, the function $R' = (P_2)\ XOR\ (P_3)\ XOR\ (P_1)$ has been chosen. It is carried out by the feedback when selecting the function mode. The nonlinear element is given by the arithmetic multiplication of the both constant and variable data words. The variable data can be changed if necessary [2].

One realisation of this element can be reached by the shift register equipped with more than only one feedback and by the nonlinear elementary operation [3]. This element is easily implemented by programmable logic devices. The circuit of encryptor and decryptor is implemented by the FPGA integrated circuit. This application is streamed to bi-directional transmissions in private cable nets.

5. Variety of Models

The results of the research can be divided into three areas. The first area is the source code of the sequential circuit which is programmable by the customer. A wide variety of changes of the basic algorithm of system is the crucial property of the main circuit cryptographic function.

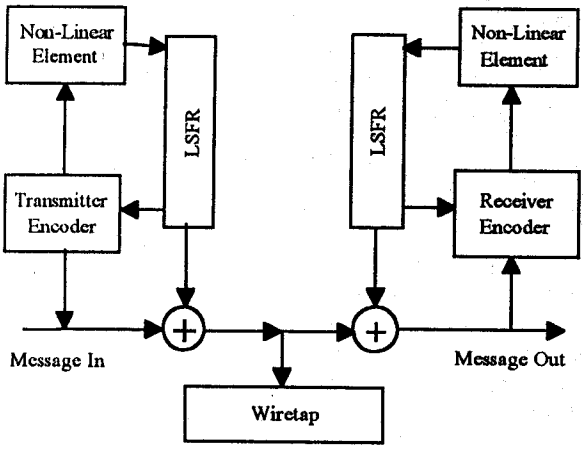

Figure 1: The non-linear secret-key generator

The second area is the resulting code translatable into the lower level of behavioural VHDL model: the register-transfer language model. This model gives the simulation of the time response in a very good approximation. The time response is important for the high speed of transmission by the TV-cable in both the synchronous and asynchronous modes.

6. Behavioural Description

An interactive decoder circuitry for secret TV signal decoding is designed and implemented as an order for a private TV company. The decoder properties are specified to reach a minimum attendance during TV watching. The interventions are necessary required only for the rejection of a chosen TV program. The testing of both the analog and the digital signals is the typical diagnostic problem of mixed signal test techniques.

The input circuit of the TV-interactive decoder is implemented by a TV receiver, an analog signal detector and an analog-signal-to-binary-code converter. This converter output digital signal is synchronized by the phase lock. With respect to the multiplex of received signals the TV image digital signal must be very tightly synchronized. In consequence the circuit for the time watch interval provides the signalization about the beginning of the payed TV operation. The circuit must be locked in the payed position. It must be proof to re-choosing the payed channel in a short time interval.

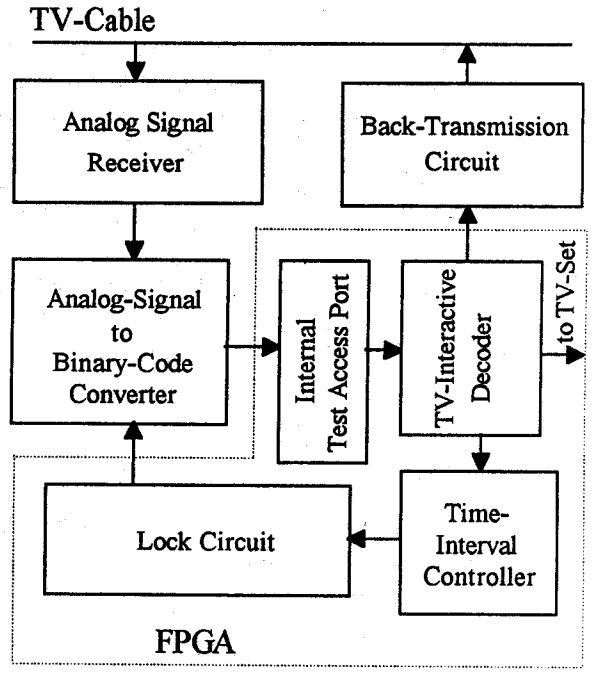

Figure 2: The block diagram of TV-interactive decoder

The TV-interactive decoder is completed by the circuit of the back-transmission of the TV-viewer address

to the programm-transmission station. The core of an identification circuit is a digital decoder and a time interval controller. The built-in diagnostic circuitry familiarly known as boundary-scan testing means is implemented by an integrated circuit packaged together with the above mentioned circuits. The test access port (TAP) is compatible with recomendations of IEEE Std 1149.1.

The inicialization test is controlled by the RUNBIST instruction. It reads some signature characteristics of fault-free run. The special boundary-scan testing may be done by specific input-test patterns. This is the way how to identify and prove the origin of the TV-interactive decoder circuit. This special remote testing is controlled by the instruction INTEST. This control mode tests also the function of the transmitter of the TV-set.

The philosophy of TV-interactive decoder is based on the following: a television viewer pays for the watched program only. If he is watching more TV-channels, the decoding installation records the short intervals of the payed programms consequently. Complex coupling of the boundary-scan testing and the mixed signal testing makes easier the identification of the television viewer address by proposal 1149.4. The advantage is the protocol compatibility and the recommended measurement conditions of the both standards.

The article provides the view of the global technical schematics of a TV-interactive decoder. The stress is imposed on the compatibility between the standards 1149.1 and 1149.4.

7. The FPGA Implementation

The important result is defined by the used implementation technology. The C-MOS Anti-Fuse FPGA was used owing to the high reliability. Low power consumption and the resistance to power failures were the prior properties of the application. The advantage of the high-speed FPGA logic elements is very favourable in this application.

The experimental results are encouraging for the continuing application research. The last but not least result is the remote testing of the circuit. Thanks to Boundary-Scan Architecture according to IEEE Std 1149.1-1990, the diagnostic function is very effective and simple: both Test Data Input (TDI) and Test Data Output (TDO) are used in serial mode.

8. Listing "Pseudorandom Array"

```
program PseudoArray;
uses crt;
var x,y,a: integer;
  b1,b2,b3: word;
  w,w1,w2,w3: boolean;


procedure pixel(x,y:word; col:byte);
var adr: word;
begin
 adr:=x*320+y;
 asm
  mov ax,sega000
  mov es,ax
  mov bx,adr
  mov al,col
  mov es:[bx],al
 end
end;


procedure vloz(var bit:word);
var i,j:word;
begin
 repeat
 readln(j)
 until (j<16);
 bit:=1;
 for i:=1 to j do bit:=bit*2
end;


procedure vga256; assembler;


asm
 mov ax,13h
 int 10h
end;
procedure no256; assembler;
asm
 mov ax,3
 int 10h
end;


begin
 writeln('Vloz postupne tri cisla (0-15): ');
 vloz(b1); vloz(b2); vloz(b3);
 vga256;
 for x:=-64 to 128 do
  for y:=-128 to 128 do
   begin
   a:=x*y; w1:=false; w2:=false; w3:=false;
   if (a and b1)>0 then w1:=true;
   if (a and b2)>0 then w2:=true;
   if (a and b3)>0 then w3:=true;
   w:=(w1 xor w2 xor w3);
   if not w then pixel(129-x,y+149,15)
   end;
 readkey;
 no256;
end.
```

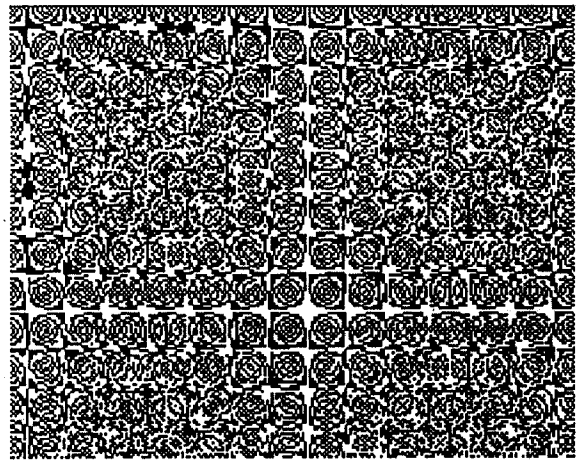

Figure 3: Array of function R' = (P7) XOR (P3).

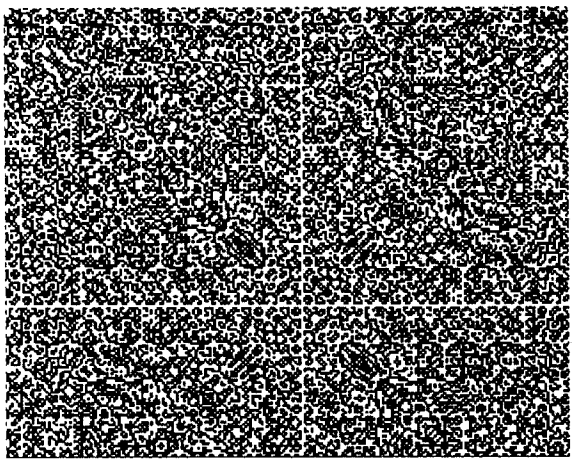

Figure 4: Array of Function R' = (P7) XOR (P3) XOR (P1).

9. The Behavioural Model of Main Part of LFSR

```
LIBRARY ieee;
USE ieee.std_ulogic_1164.all
ENTITY lfsr IS
PORT(parallel_in:IN std_ulogic_vector(0 TO 15);
serial_in:IN std_ulogic;
clk:IN std_ulogic;
xor_in:IN std_ulogic;
nul_in:IN
std_ulogic_vector(0 TO 15);
parallel_out:BUFFER std_ulogic_vector(0 TO 15);
ALIAS serial_out:std_ulogic IS parallel_out(0);
END lfsr;
ARCHITECTURE lfx OF lfsr IS
BEGIN
PROCESS (clk)
BEGIN
IF clk='1' AND clk'EVENT AND
clk'LAST_VALUE='0'
THEN IF xor_in = '1'
THEN parallel_out(1,3,7) <= NOT parallel_in(0,2,6);
ELSE parallel_out(15) <= serial_in;
parallel_out(0 to 14) <= parallel_out(0 TO 15);
END IF;
END IF;
END PROCESS;
END lfx;
```

References

[1] Adámek, J.: Foundations of Coding. John Wiley & Sons, Inc. (1991)

[2] Vlček, K.: Multiplier-Accumulator with Directed Data Flow. The 2-nd European Signal Processing Conf. EUSIPCO-83, Erlangen, Germany, Sept.12-16, 1983, (North-Holland, Amsterodam, 1983), pp. 833-836.

[3] Novák, O.: Pseudoexhaustive Test Sets Generated in LFSRs. Proc. IEE - ETC 91 Conference, Munchen, Germany, (1991), p. 485.

[4] IEEE Standard VHDL Language Ref. Manual. IEEE Std 1076-1987. IEEE Inc., NY 100017, USA. (March 31, 1988).

[5] Coelho, D. R.: The VHDL Handbook. Kluwer Acad. Publish. (1989).

[6] Dewey, A.: Design Automation. IBM Enterprise Systems. Czech Technical University Prague (March 8 - 11, 1993).

[7] IMEC: VHDL: Intensive Course. Leuven, Belgium, (August, 1993).

About author

Karel Vlček was born in Zlín in 1948. He received the MSc degree at Technical University of Brno and PhD. degree at Czech Technical University of Prague. At the time beeing, he is at the Dept of Electronics, Technical University of Ostrava. His main field of interests is investigated Digital Signal Processing, and Error Control Codig, Cryptography, Automation of Digital Circuits Design, and Design for Test.