GOST 28147-89
IP Core

Author: Kirill Fomichev
fanatid@ya.ru

Revision 0.2
March 31, 2014

Revision History

Rev.	Date	Author	Description
0.1	March 10, 2014	Kirill Fomichev	Initial Release
0.2	March 31, 2014	Kirill Fomichev	Add bidirectional ECB and CFB modules

Contents

1 Introduction

1.1 About GOST 28147-89

The *GOST block cipher*, defined in standard *GOST 28147-89*, is a Soviet and Russian government standard symmetric key block cipher. Developed in the 1970s, the standard has been marked "Top Secret" and the downgraded to "Secret" in 1990. Shortly after the dissolution of the USSR, it was declassified and it was released to the public in 1994.

GOST have a 64-bit block size and a key length of 256 bits. It's S-Boxes can be secret, and they contain about $354(log_2(16!^8))$ bits of secret information, so the effective key size can be increased to 610 bits; however, a chosen-key attack can recover the contents of the S-Boxes in approximately 2^{32} encryptions.

1.2 This roject

This project has implements *GOST block cipher* in three modes: electronic codebook (ECB), cipher feedback (CFB) and message authentication code (MAC).

All files licensed under *BSD license*.

2 Interface

ECB mode

Signal name	Width	In/Out	Description
clk	1	In	Clock
reset	1	In	Terminate current encryption/decryption process
mode	1	In	Decryption when mode equal 1, otherwise encryption
load_data	1	In	Start of encryption/decryption
sbox	512	In	S-Box
key	256	In	Key
in	64	In	Plain text/Cipher text
out	64	Out	Cipher text/Plain text. Results available after 34 clock cycles.
busy	1	Out	Status flag, triggered to zero after finished encryption/decryption

ECB mode with pipeline

Signal name	Width	In/Out	Description
clk	1	In	Clock
sbox	512	In	S-Box
key	256	In	Key
in	64	In	Plain text/Cipher text
out	64	Out	Cipher text/Plain text. Results available after 32 clock cycles.

CFB mode

Signal name	Width	In/Out	Description
clk	1	In	Clock
reset	1	In	Terminate current encryption/decryption process and load gamma from *in*
mode	1	In	Decryption when mode equal 1, otherwise encryption
load_data	1	In	Start of encryption/decryption
sbox	512	In	S-Box
key	256	In	Key
in	64	In	Gamma/Plain text/Cipher text
out	64	Out	Cipher text/Plain text. Results available after 35 clock cycles.
busy	1	Out	Status flag, triggered to zero after finished encryption/decryption

MAC mode

Signal name	Width	In/Out	Description
clk	1	In	Clock
reset	1	In	Drop current mac
load_data	1	In	Start calculate mac
sbox	512	In	S-Box
key	256	In	Key
in	64	In	Plain text
out	32	Out	MAC, available after 18 clock cycles.
busy	1	Out	Status flag, triggered to zero after finished processing

3 Testbench

Makefile run simulation using Icarus Verilog in testbench folder. You can see simulation results in GTKWave.

File name	*The module being tested*
gost89_ecb_tb.v	ECB encryption and decryption
gost89_pipelined_ecb_tb.v	Pipelined ECB encryption and decryption
gost89_cfb_tb.v	CFB encryption and decryption
gost89_mac_tb.v	MAC mode

4 References

1. GOST block cipher,
   http://en.wikipedia.org/wiki/GOST_(block_cipher)

2. RFC 4357: Additional Cryptographic Algorithms for Use with GOST
   http://tools.ietf.org/html/rfc4357

3. RFC 5830: GOST 28147-89 encryption, decryption and MAC algorithms
   http://tools.ietf.org/html/rfc5830

4. Schneier, Bruce (1996). Applied cryptography: protocols, algorithms, and source code in C