AES Encryption IP Security System

IP Lock

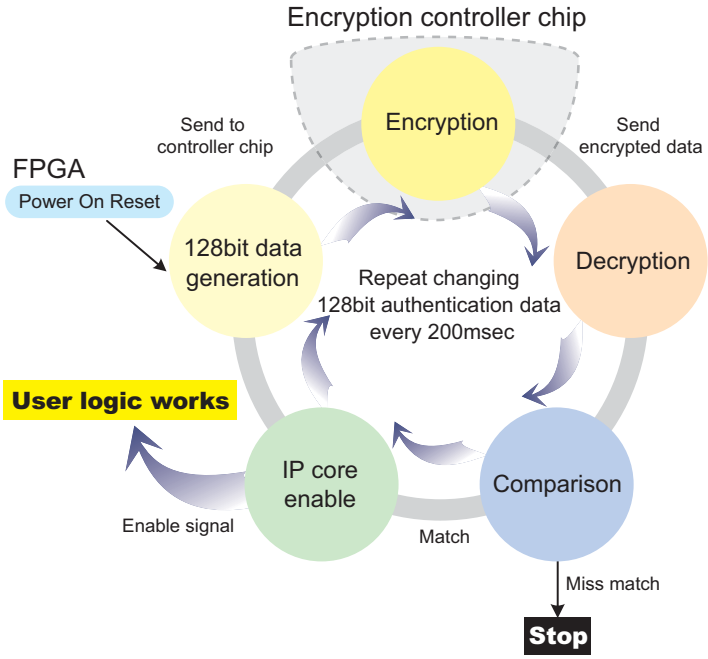
IP Lock is FPGA logic security system which used very reliable AES encryption technology. IP propaties in FPGA are protected from illegal copy by only including IP Lock in FPGA and connectiing with encryption controller chip.

Features

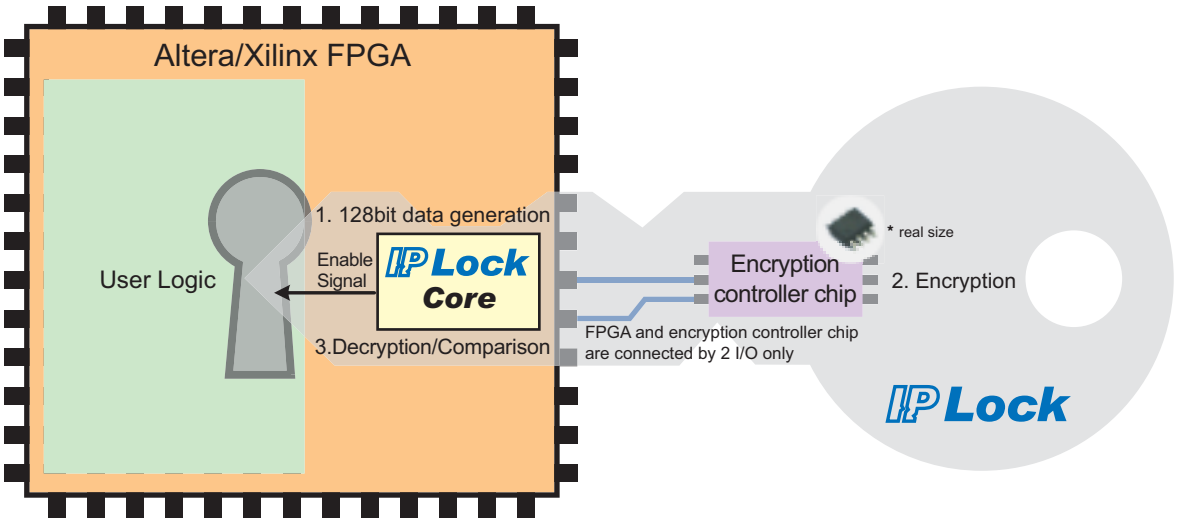
- Strong security by AES encryption
- Change & encrypt authentication data at about 200msec cycle
- Generate true random authentication data by natural random number generator
- Stop user logic when removing the chip
- Connecting I/O with FPGA are only 2 pins
- No need to input clock to IP Lock logic
- Provide easy laboratories pack and IP Lock writer + blank chip

AES Cryptosystem

AES(Advanced Encryption Standard) is common key cryptosystem chosen by NIST, US. Both encryption and decryption are high speed. And it is also stronger than triple DES. So it is noticed as encryption standard for next generation replaced with DES. Currently AES is adopted with security for financial system, LAN system and so on.



IP Lock encryption/decryption process flowchart



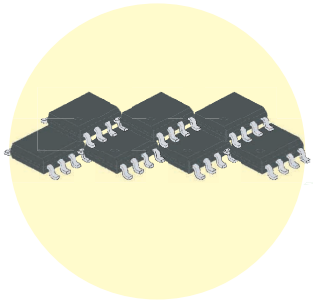
IP Lock block diagram

IP Lock

Usage

Laboratories pack

Laboratories pack containes encryption chips which are already written unique ID at shipment. It is for small usage.



Unique ID for each pack written by DesignGateway

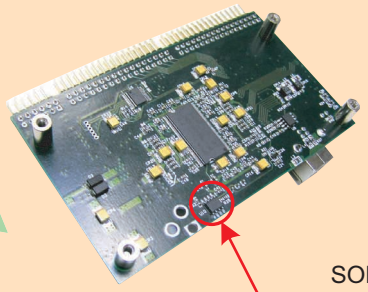
IP Lock writer + blank chip

IPL-CHP * real size

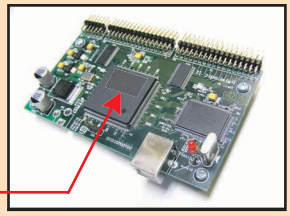
User can write any ID to blank chip by using IP Lock writer

Possible to write optional ID to blank chips by IP Lock writer. Because every IP Lock writer have different ID, even if a user write same key but using different IP Lock writer, written ID are also different. It is for mass production or using it for several products.

IP Lock implementation example



Step1:
SOP8 pin package mount encryption chip



Step2:
Implement IP Lock to FPGA

Specifications

■Production name	IP Lock
■Cryptosystem	AES-128 Cryptosystem
■Consumption resources of IP Lock core	about 1,200LE / about 24,500 memory bit (for Altera FPGA) about 400 slices / 2 blockRAM (for Xilinx FPGA)
■Encryption controller	SOP8 pin package 2 I/O for connecting with FPGA No need clock input
■Contents	● IP Lock encryption contrpller chip ● IP Lock core netlist ● User's manual ● ID writing software (for Windows, included in IP Lock writer IPL-003WR only)
■Part number	●IP Lock Laboratories pack IPL-010L IP core netlist + encryption controller chip 10pcs pack IPL-030L IP core netlist + encryption controller chip 30pcs pack ●IP Lock writer IPL-003WR IP Lock writer (with IPL-CHP 3pcs) IPL-CHP Blank chip for IP Lock writer (MOQ 100pcs)

DESIGN GATEWAY COMPANY LIMITED

54 BB Building 13th Floor, Room1302, Sukhumvit 21(Asoke),
Klongtoey-Nua, Wattana, Bangkok 10110 THAILAND

TEL : +66-(0)2-261-2277 www.design-gateway.com
FAX : +66-(0)2-261-2290 sales@design-gateway.com

Authorized Distributor: