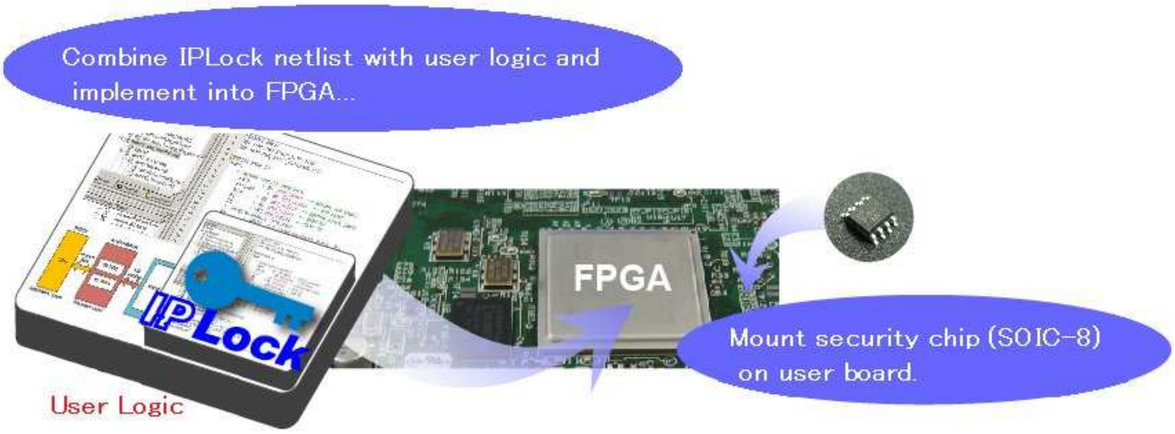
IP Lock

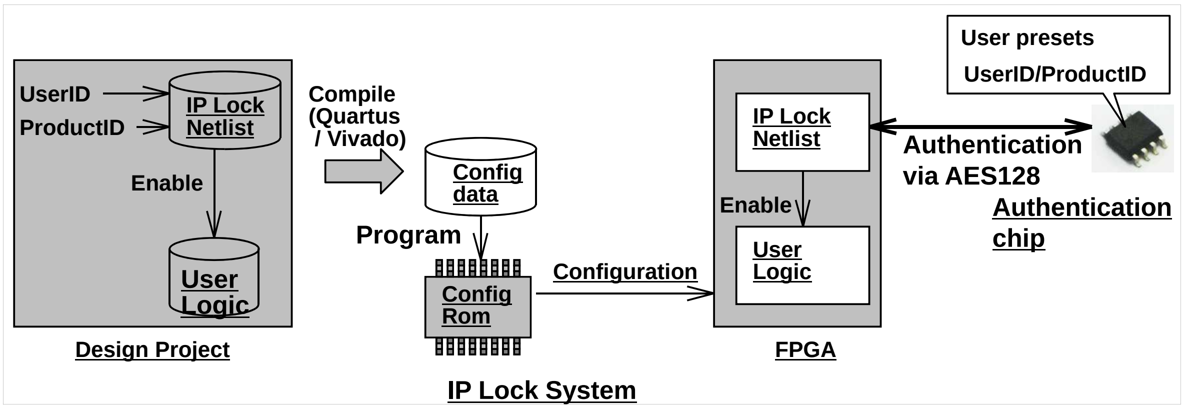
V1.3E


Combine IPLock netlist with user logic and implement into FPGA...
FPGA
IP Lock
User Logic
Mount security chip (SOIC-8) on user board.

Protect FPGA data from unauthorized copying

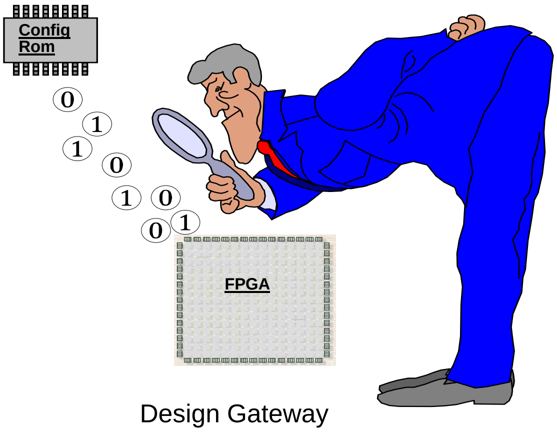
What is "IP Lock" ?

- **Security system for FPGA design data**
- **Communicate authentication chip via FPGA IO pin**
- **Combine user logic and cryptographic module (IP Lock netlist) then compile**
- **Cryptographic module detects authentication chip**



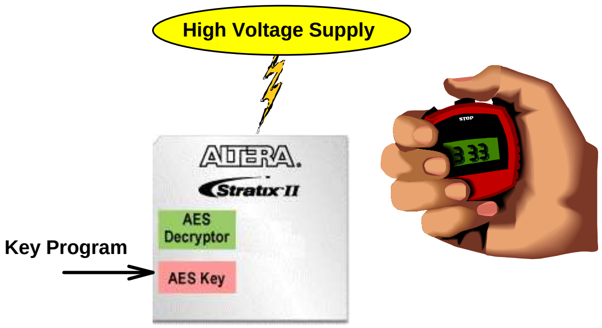
Background of IP Lock system

- Importance of IP protection
  - Development cost and time is increasing significantly in proportion to FPGA scale.
  - Serious damage if circuit design is illegally copied.
- Configuration data is observable from outside
  - Observation of Configuration data cannot be prevented.



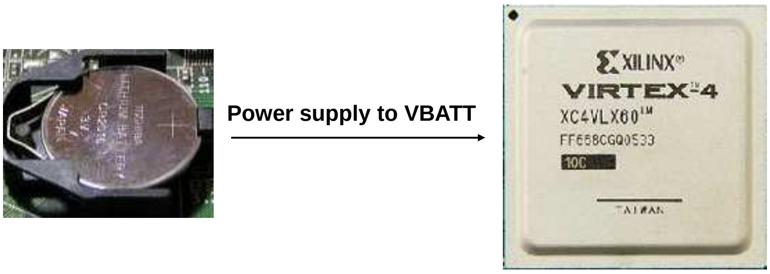
Legacy IP protection (Intel case)

- Protection method of Intel FPGA
  - Program AES key into non-volatile area of FPGA.
- Demerit
  - Needs special high-voltage power supply.
  - Power supply duration is limited, possible to damage if excess.



Legacy IP protection (Xilinx case)

- Protection method of Xilinx FPGA
  - Store AES key into internal SRAM memory.
- Demerit
  - Needs external battery to supply VBATT.
  - Product life is limited by battery life.



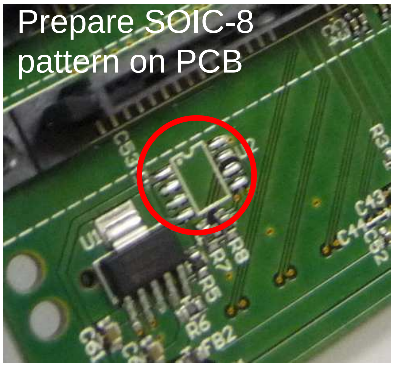
IP Lock Merit

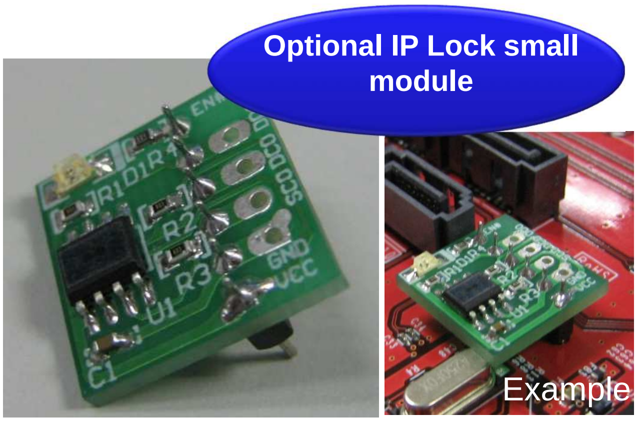
- Applicable to any FPGA without encrypted configuration feature
  - Further improve security even for encrypted configuration device.

- IP Lock can operate with 1.8/2.5/3.3V power supply
  - No extra high-voltage/battery power supply necessary.
- Periodic random seed update
  - Protect from signal generation emulation

IP Lock Merit (Cont'd)

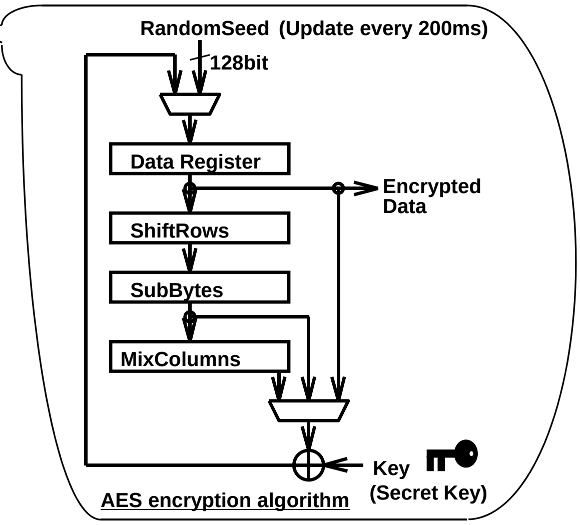
- **Individual Product ID setting.**
  - Can set different ID in IP Lock for different product protection.
- **Easy mounting on PCB**
  - Requires only two general purpose IO pin of FPGA
  - Small package (SOIC-8)




Optional IP Lock small module

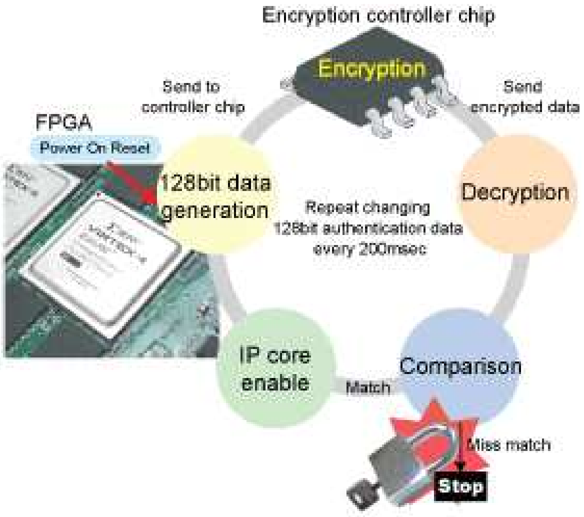
IP Lock technology 1: AES encryption

- **128bit-AES proven cryptographic strength**
  - Algorithm is open to the public
  - Keep encryption with key value only



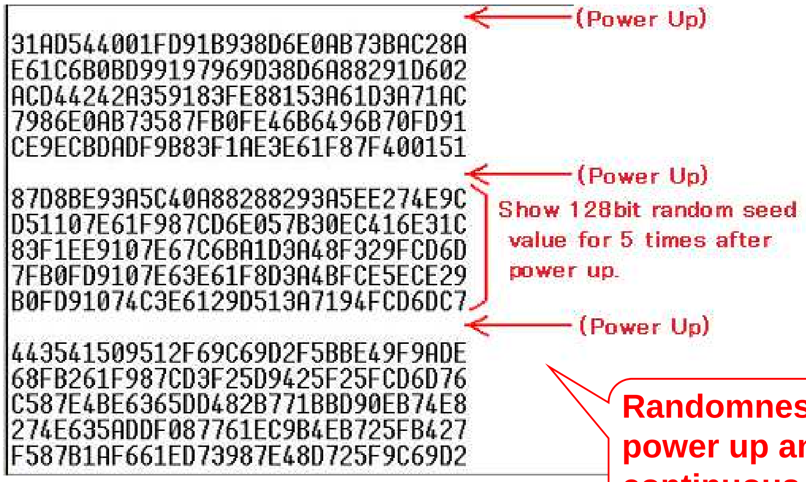
IP Lock technology 2: Real time authentication

- Change authentication data every about 200 ms
- Continuous authentication after power up
  - Immediately lock user logic if external IP Lock device is not detected



IP Lock technology 3: RNG

- Complete random seed generation function applying natural phenomena
  - Extremely strong resistance to attempts at deciphering



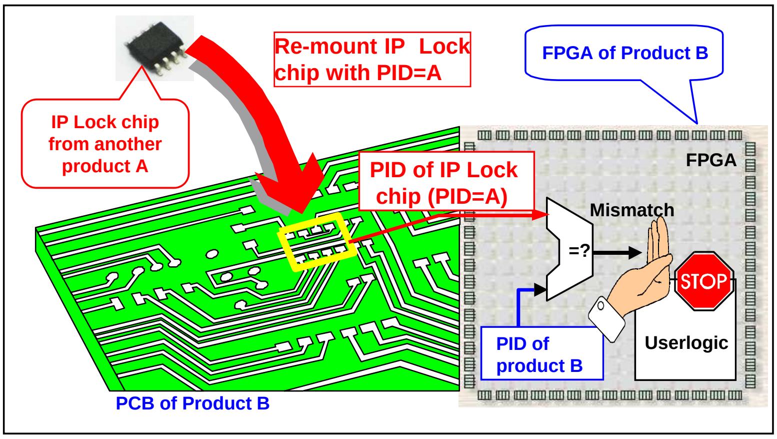
```
31AD544001FD91B938D6E0AB73BAC28A
E61C6B0BD99197969D38D6A88291D602
ACD44242A359183FE88153A61D3A71AC
7986E0AB73587FB0FE46B6496B70FD91
CE9ECBDADF9B83F1AE3E61F87F400151

87D8BE93A5C40A88288293A5EE274E9C
D51107E61F987CD6E057B30EC416E31C
83F1EE9107E67C6BA1D3A48F329FCD6D
7FB0FD9107E63E61F8D3A4BFCE5ECE29
B0FD91074C3E6129D513A7194FCD6DC7

443541509512F69C69D2F5BBE49F9ADE
68FB261F987CD3F25D9425F25FCD6D76
C587E4BE6365DD482B771BBD90EB74E8
274E635ADDF087761EC9B4EB725FB427
F587B1AF661ED73987E48D725F9C69D2
```

Randomness in both power up and continuous RNG update

RNG evaluation example using real IP Lock

IP Lock technology 4: Product ID

- User can specify Product ID (PID) for each product
  - Not unlock if 32bit PID value does not match
  - Protect from swapping authentication chip


Re-mount IP Lock chip with PID=A
FPGA of Product B
IP Lock chip from another product A
PID of IP Lock chip (PID=A)
FPGA
Mismatch
=?
STOP
PID of product B
Userlogic
PCB of Product B

<u>Protect IP Lock chip swapping by PID value verification</u>

Supported FPGA and resource usage

- For Intel
  - Support 5 series and 10 series FPGA (*)
  - Logic usage: About 1280LE
  - Memory usage: 24,576 memory bit

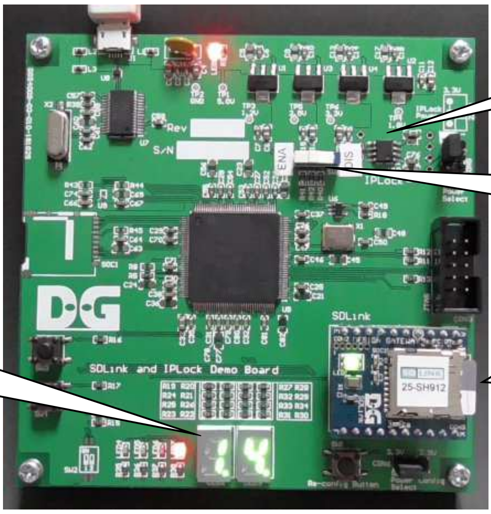
- For Xilinx
  - Support 7 series and UltraScale(+) series (*)
  - Slice usage: About 350Slice
  - Memory usage: 2 BlockRAM

(*) Refer to the support list for the latest information.

URL : https://dgway.com/products/IPLock/IPL-LIST.pdf

Evaluation Board

- IP Lock evaluation board (combination Eval. board of SDLink and IP Lock）
  - User can check real time authentication by connection ON/OFF switch.



IPL-CHP (Authentication chip)

Connection ON/OFF switch

LED illumination pattern change by authentication result

(SDLink from DesignGateway)

IPLock evaluation board

Product line up (authentication chip)

- Low voltage support version
  - Product name：IPL-CHP1.8V
  - Operation voltage：1.8V, 2.5V, 3.3V
  - Suitable for 1.8V I/O
- Standard version
  - Product name：IPL-CHP
  - Operation voltage：2.5V, 3.3V
  - Lower cost than IPL-CHP1.8V

Product line up (package)

- **Package for prototype (Laboratories Pack)**
  - Pre-programmed Product ID for each package, better for small volume usage.
  - Authentication chip 10pcs/30pcs package.
    - Product name: IPL-010L (10pcs) / IPL-030L (30pcs)
- **Package for mass production**
  - IP Lock Writer(IPL-003WR) and Blank chip (IPL-CHP/IPL-CHP1.8V)
  - User can program unique Product ID into authentication chip via IP Lock writer, better for mass production.

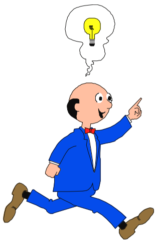
IP Lock Writer: IPL-003WR

Conclusion: Merit for user

- **Secure protection for valuable user design assets**
  - Strong security with 128bit-AES application
  - Protect from signal emulation by constant authentication
- **Easy for use**
  - Can apply to even without security feature FPGA
  - No extra power supply required
  - Minimum space occupation on PCB（SOIC-8 with two signals connection)

Inquiry

- **Detailed documents on website**
  - https://www.dgway.com/IPLock_E.html
- **Contact:**
  - **URL:** http://www.design-gateway.com/aboutus.html
  - **E-mail : info@dgway.com**



"IP Lock" AES Encryption IP Security System

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

Revision History

Rev.	Date	Description
1.0J	15-Jul-2010	1st Japanese version
1.3E	3-Jun-2019	English version with IPL-CHP1.8V new line up