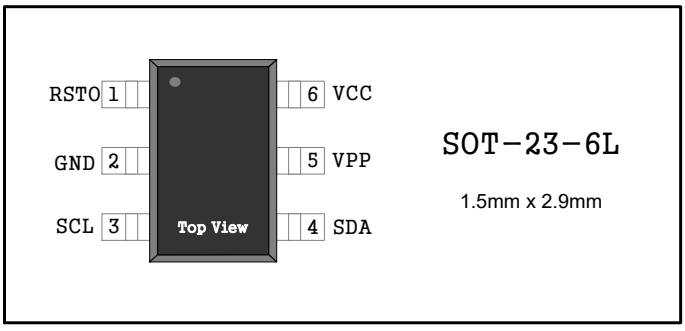
Features

- High performance illegal copy protection IC
- 128bits encryption and decryption applied with AES-128
- 128bits OTP cells for user serial code
- IIC Serial Interface, Supporting up to 400 Kbps
- 3.3V/1.8V Operation Voltage
- Built- in Power on Reset / 16MHz OSC
- Two Power Mode (Active, Sleep)
- Reset Output(open drain output)
  - Reset delay time on power up. Fixed(Factory programmed) reset out time : 8ms to 1s

Applications

- DMB, Navigation
- Mobile Phone, PMP, MP3
- DVR(PVR), DVDP
- Set-Top Boxes (STBs)
- Etc.(Most of electronic system using u-Processor)

Pin Configuration



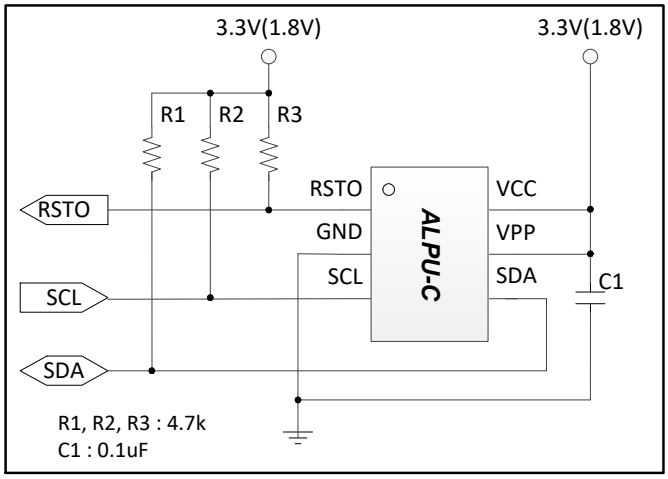
Ordering Information

Part	Operation Voltage	Package Type
ALPU-C	3.3V	SOT-23-6L
ALPU-CL	1.8V	SOT-23-6L

General Description

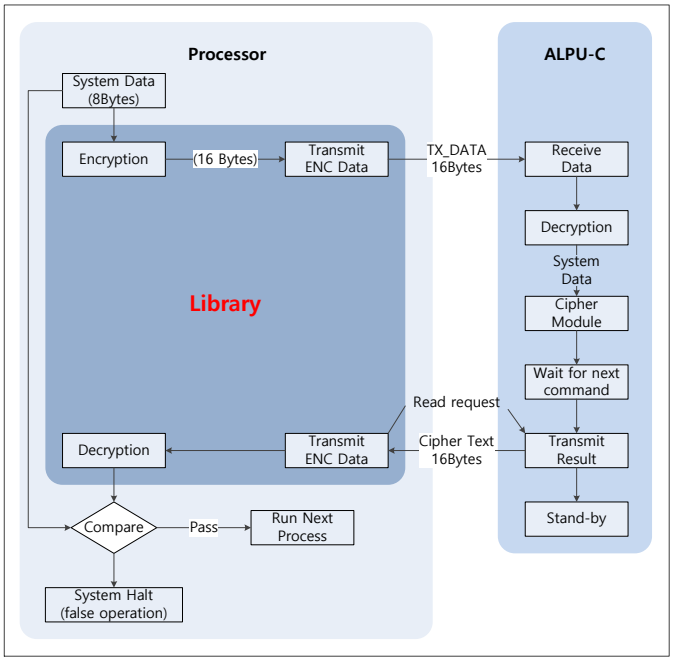
The ALPU-C is the high-end IC among the ALPU series. Its encryption core is based on Rijndeal AES-128 with 192-bits programmable parameters. It is a slave device that always operates with MCU through the serial bus.

Typical Operation Circuit



< SOT-23-6L Package Type >

Encryption Flow



Contents

1. Overview ---------- 3
2. I/O Port ---------- 5
3. Clock Management ---------- 7
4. Power Mode ---------- 7
5. Initialization ---------- 8
6. Encryption ---------- 9
7. One Time Programmable ROM ---------- 13
8. Reset Output ---------- 14
9. Communication Interface ---------- 16
10. Electrical Characteristic ---------- 18
11. Typical Operation Circuit ---------- 21
12. Package Information ---------- 22
13. Datasheet Revision History ---------- 23

1. Overview

ALPU-C is the high-end IC among the ALPU series. Its encryption core is based on Rijndael AES-128 with 192-bit programmable parameters. It is a slave device that always operates with MCU through the serial bus.

1.1. Features

1.1.1 Security

- High performance illegal copy protection IC
- 128 bit encryption applied with AES-128

1.1.2 Memories

- 128-bit OTP cells for user serial code

1.1.3 Peripheral Features

- IIC serial interface, Supporting up to 400 kbps
- Support RSTO

1.1.4 Special Features

- Built in Power-on-Reset
- Built in 16MHz OSC
- Two Power Modes : Active, Sleep

1.1.5 Operating Voltages

- 3.3V / 1.8V Operation Voltage
- 6.5 V to VPP pin for OTP Writing Voltage

1.1.6 Package

- 6L-SOT23

1.2. Block Diagram

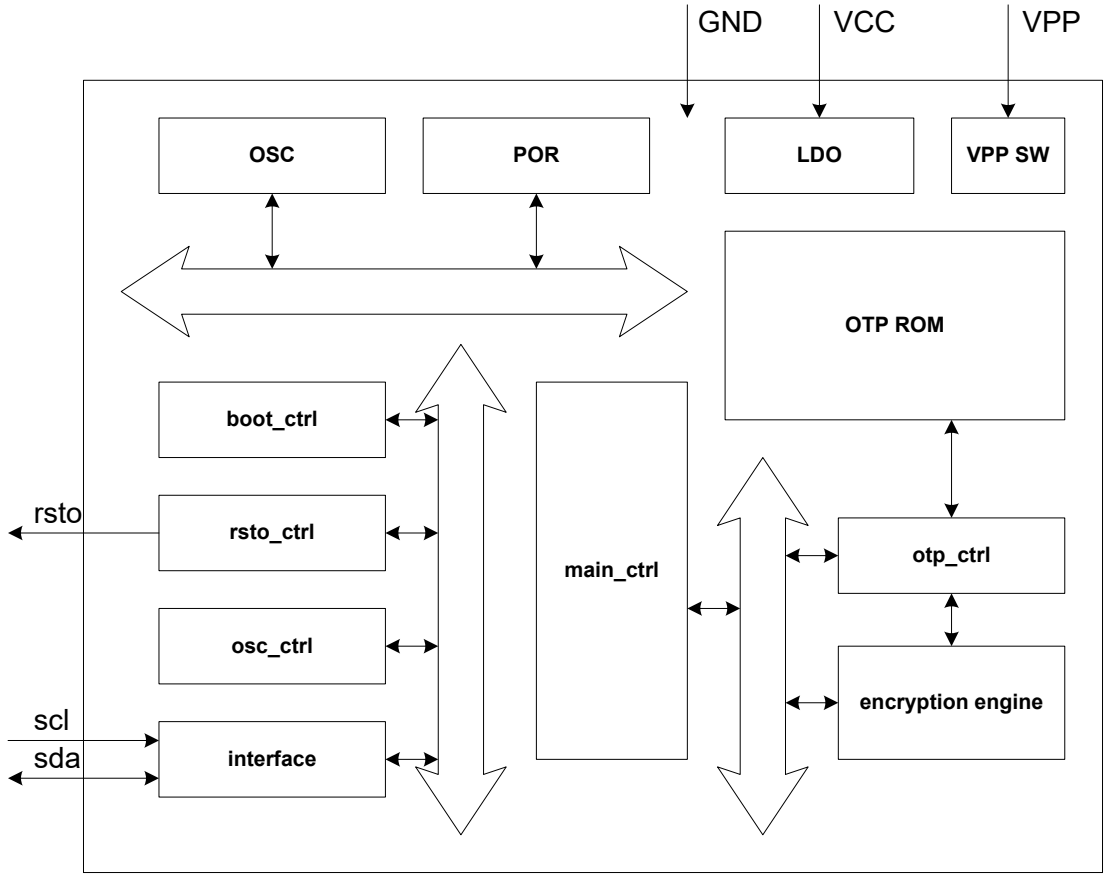


Figure 1-1. Block Diagram

ALPU-C consists of analog blocks (OSC, POR and LDO) and a memory block and digital logic ones. The boot control block manages the signals of analog blocks. And the main control block manages the communications between the digital blocks through two buses.

1.3. Pin Configurations

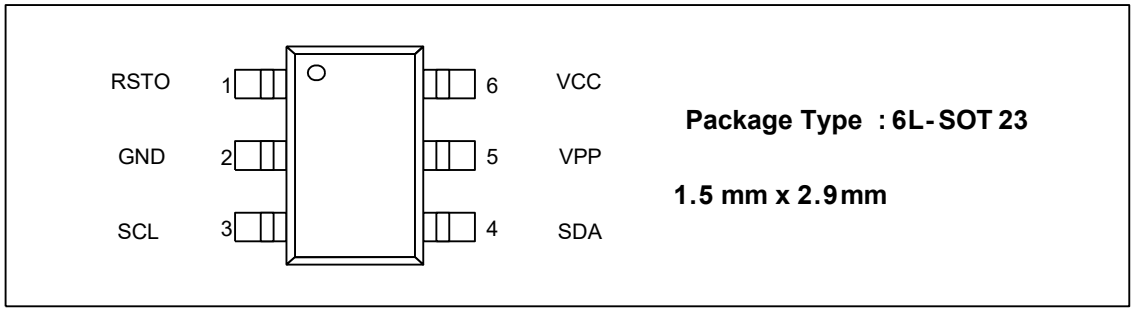


Figure 1-2. ALPU-C Pin Configuration

1.4. Pin Descriptions

Table 1-1. ALPU-C Pin Description

Pin Num	Pin Name	Description	Remark
1	RSTO	Reset Output(Low Active), Open-drain output	
2	GND	Ground	
3	SCL	IIC Serial Clock input pin. CMOS Input	
4	SDA	IIC Serial Data, CMOS Input / Open-Drain Output bi-directional I/O	
5	VPP	6.5V supply voltage for programming OTP cells.	
6	VCC (1)	Digital supply voltage	

Note (1) The ALPU-C operation voltage is supported by the two types, 1.8V or 3.3V

2. I/O Port

2.1 ESD protection circuit

ESD protection circuit for the whole chip is achieved as shown in Figure2-1. It can be protected the chip against two widely used industry standard ESD test models: Human Body Model (HBM) and Machine Model (MM). Both of these models test each pin against every other pin and/or a power/ground supply using a positive and a negative pulse.

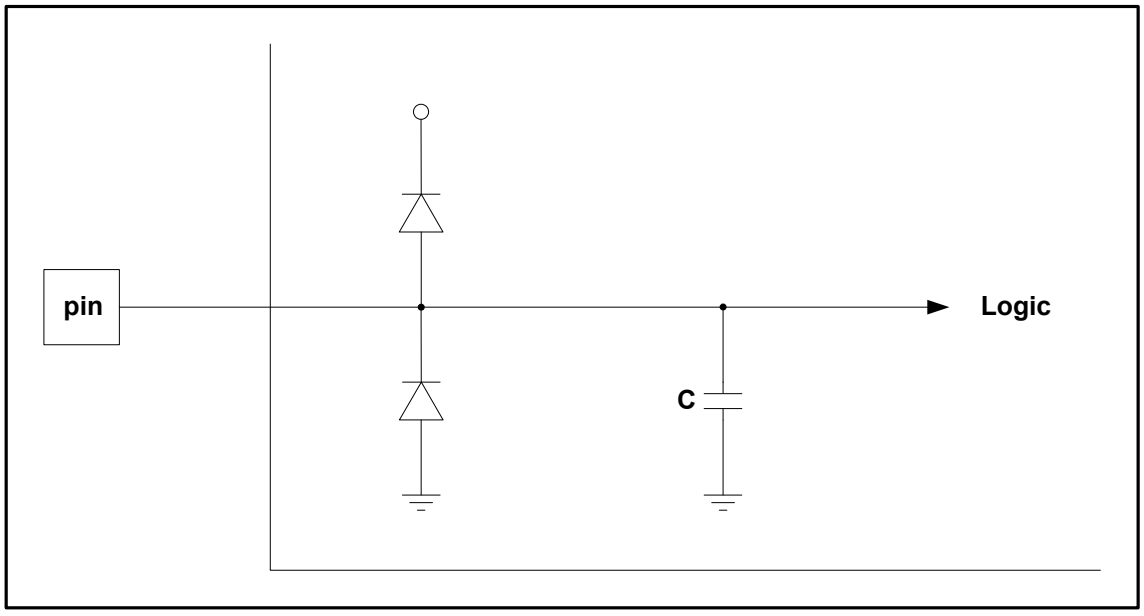


Figure 2-1. ESD protection circuit

2.2 I/O type

ALPU-C has I/O types as shown in Table2-1.

Table 2-1. I/O Types

Direction	Name	Description
Power	VPP	6.5V supply voltage for programming OTP cells
	VCC	Digital supply voltage
	GND	Ground
Bi-direction Port	SDA	IIC Serial Data bi-direction pin
Input Port	SCL	IIC Serial Clock input pin

2.2.1 Input Port (SCL)

The Input cell is an input buffer with CMOS input.

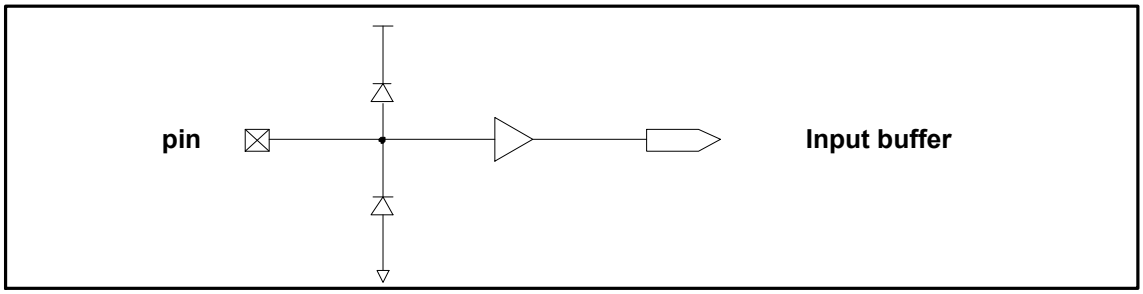


Figure 2-2. Input port Schematic

2.2.2 Output Port (RSTO)

The output cell is an output buffer with 2mA direct output.

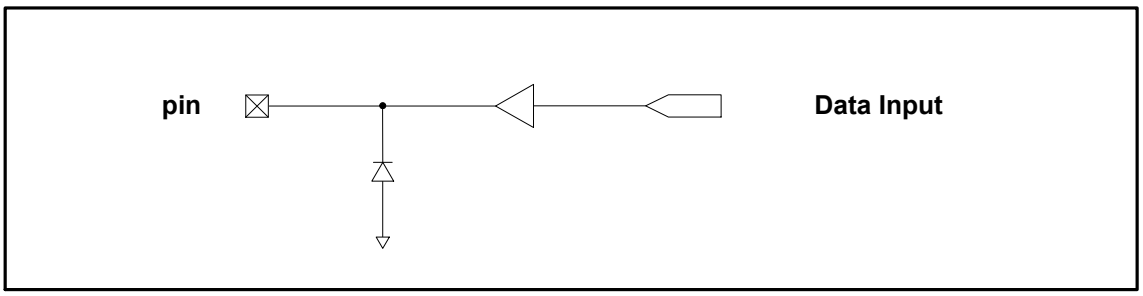


Figure 2-2. Output port Schematic

2.2.3 Bi-direction Port (SDA)

This cell is a bidirectional buffer with CMOS input and 2mA n-channel open drain output.

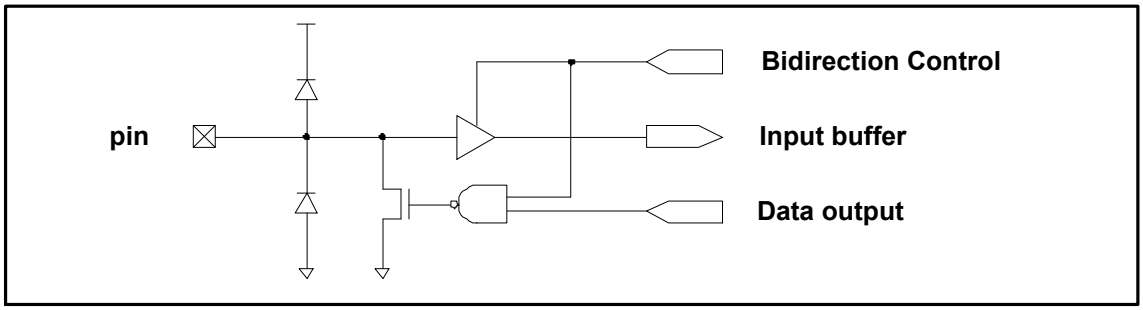


Figure 2-4. Bi-direction port Schematic

3. Clock Management

3.1 Internal clock

All Inner blocks use internal OSC clock. Internal OSC clock is approximately 16MHz shown in Table3-1.

Table 3-1. Internal OSC parameters (Ta = 25°C)

PARAMETER	SYMBOL	CONDITION	Min	Typ	Max	Unit
Frequency	f16m		14	16	18	MHz
Frequency Variation	Δf16m	-40≤Ta≤80°C	-	-	±10	%
Duty Cycle	Dmax		48	50	52	%

3.1.1 Clock on/off

Internal OSC clock can be turned on or off. If ALPU-C is in the condition of Sleep-mode, then internal OSC clock is turned off to save the power.

Here is the condition to enter the Sleep-mode. SCL and SDA pins both stay high and all functions are disabled for more than 2 seconds. When the conditions above are not met it wakes up to active-mode. (Refer to chapter 4. Power Mode)

4. Power Mode

ALPU-C supports the power saving mode called Sleep-mode in which internal oscillator is off.

4.1 Condition of entering Sleep-mode

Here is the condition to enter the Sleep-mode. SCL and SDA pins both stay high and all functions are disabled for more than 2 seconds. (Refer to Figure 4-1)

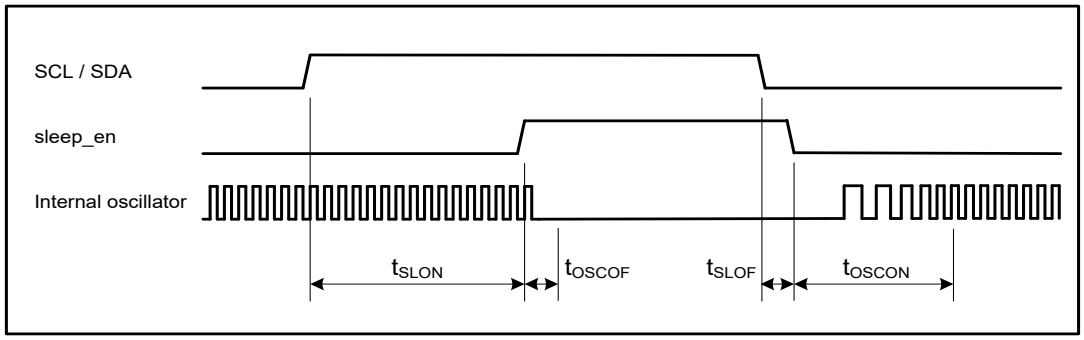


Figure 4-1. Sleep-mode Waveform

SCL/SDA : IIC signal

sleep_en : internal sleep-enable signal

Internal oscillator : 16MHz oscillator for internal logic

Table 4-1. Sleep-mode Waveform Parameters

Parameter	Symbol	MIN	TYP	MAX	Unit
Sleep-mode On Time	t_{SLON}	2000			ms
Sleep-mode Off Time	t_{SLOF}			10	ns
OSC On Time	t_{OSCON}			5	us
OSC Off Time	t_{OSCOF}			10	ns

4.2 Condition of exiting Sleep-mode

When the conditions are not met it wakes up to active-mode; Either SCL or SDA line goes down to low.

5. Initialization

ALPU-C has an internal POR (Power-on-Reset) circuit. When system power turns on ALPU-C's POR resets its own system. During reset time, all internal registers of ALPU-C are configured as their initial values. After that, internal registers are set to the values in OTP memory. (Refer to chapter 9. Electrical Characteristic)

5.1 Start-up Waveform

After RESET, internal registers in ALPU-C need $t_{INITIAL}$ time period to initialize all registers. After $t_{INITIAL}$ time period ALPU-C enters the sleep mode.

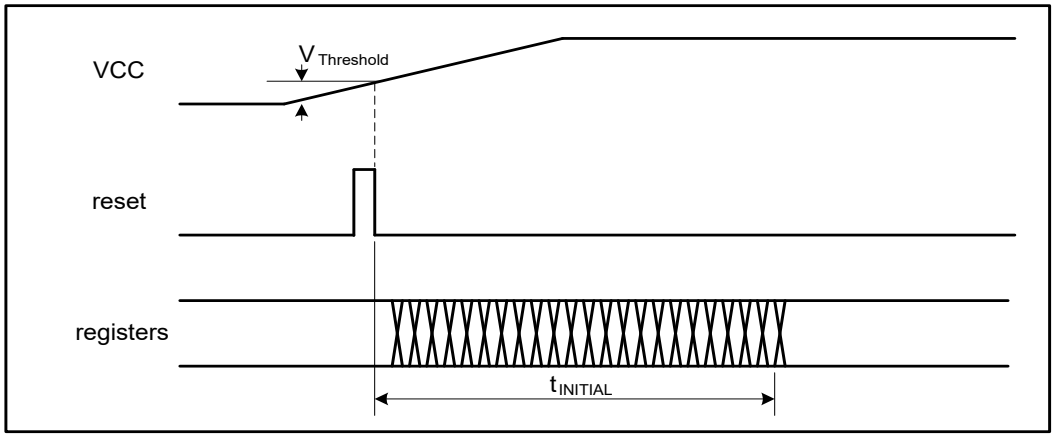


Figure 5-1. Start-up Waveform

VCC : 3.3V Supplied Power

reset : internal Power-on-Reset signal

registers : internal registers for initialization

Table 5-1. Start-up Timing Parameters

Parameter	Symbol	MIN	TYP	MAX	Unit
Threshold Voltage	$V_{Threshold}$	1.1	1.2	1.3	V
Initial Time	$t_{INITIAL}$			160	us

VCC information (Refer to chapter 10. Electrical Characteristic)

5.2 Internal Power-on-Reset

A Power-on-Reset (POR) pulse is generated by an On-chip detection circuit. The detection level is defined in Table5-1.The POR is activated whenever VCC is below the detection level (threshold voltage). The POR circuit ensures that the device is reset from Power-on. Reaching the POR threshold voltage invokes the delay counter, which determines how long the device is kept in RESET after VCC rise.

6. Encryption

6.1 Encryption Core Block Diagram

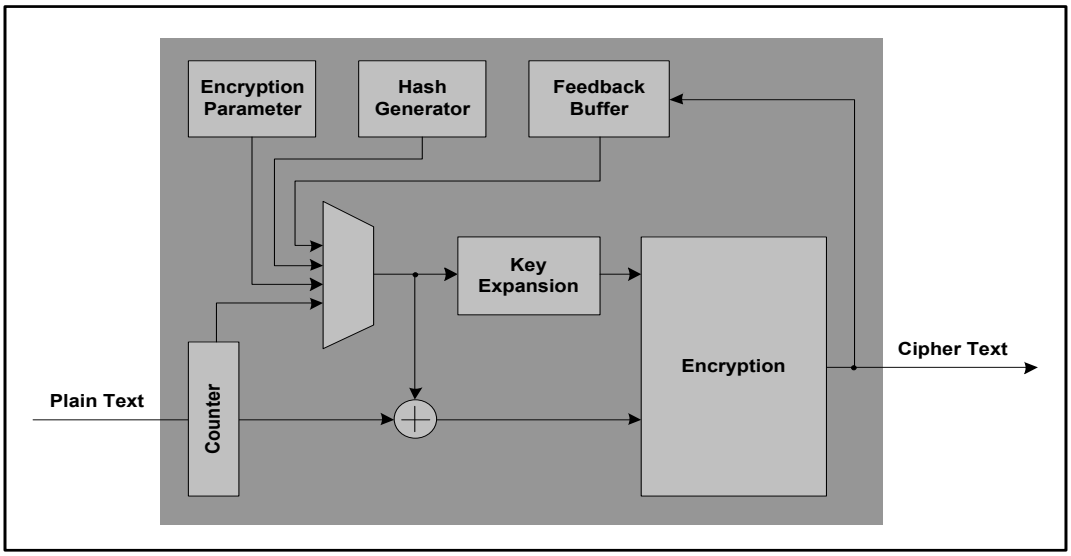


Figure 6-1. Encryption Core Block Diagram

ALPU-C has 128-bit encryption core applied with AES-128. The core consists of several blocks. They are Encryption Core, Random Generator, Feedback buffers and Encryption parameter.

6.2 Encryption configured with IIC sub address

Encryption Core is configured with sub addresses as shown in Figure 6-2. Each encryption bit can be overlapped.

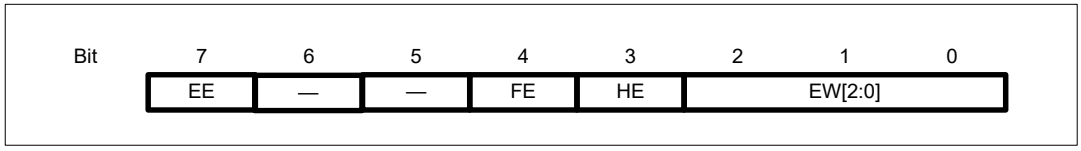


Figure 6-2. Sub Address Configuration

Bit 7: EE (Encryption Enable)

When EE bit is set 1, it is in Encryption Mode

Bit 6: Reserve

Bit 5: Reserve

Bit 4: FE (Feedback Enable)

When both EE and FE bits are set to 1, it is in Feedback Mode.

Bit 3: HE (Hash Enable)

When both EE and HE bits are set to 1, it is in Hash Generation Mode

Bit 2~0: EW (Encryption Width)

The EW bits are loop count numbers of the encryption algorithm. It is recommended that the bits are set with random numbers.

6.3 Encryption Mode

6.3.1 Bypass Mode

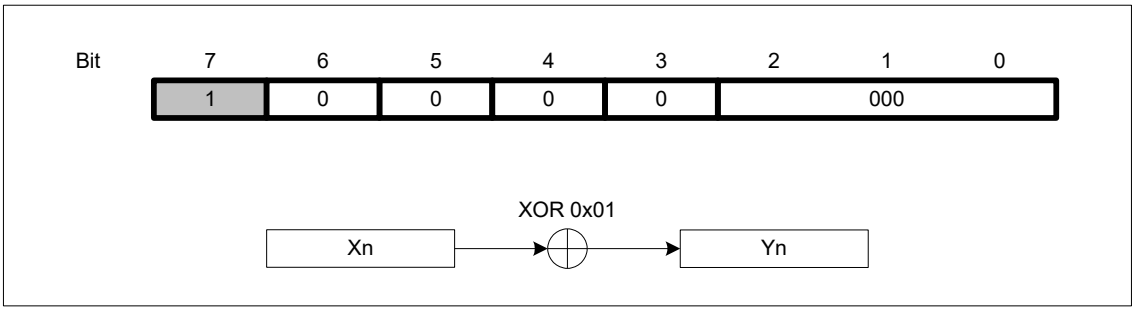


Figure 6-3. Bypass Mode Sub Address Construction

Bypass Mode is a mode to test the communication interface between CPU and ALPU-C. The data(Xn) from CPU will do Exclusive OR operation with 0x01 in ALPU-C.

6.3.2 Feedback Encryption Mode

It is not able to open this information

6.3.3 Hash Generator Mode

It is not able to open this information

6.4 Encryption Flow

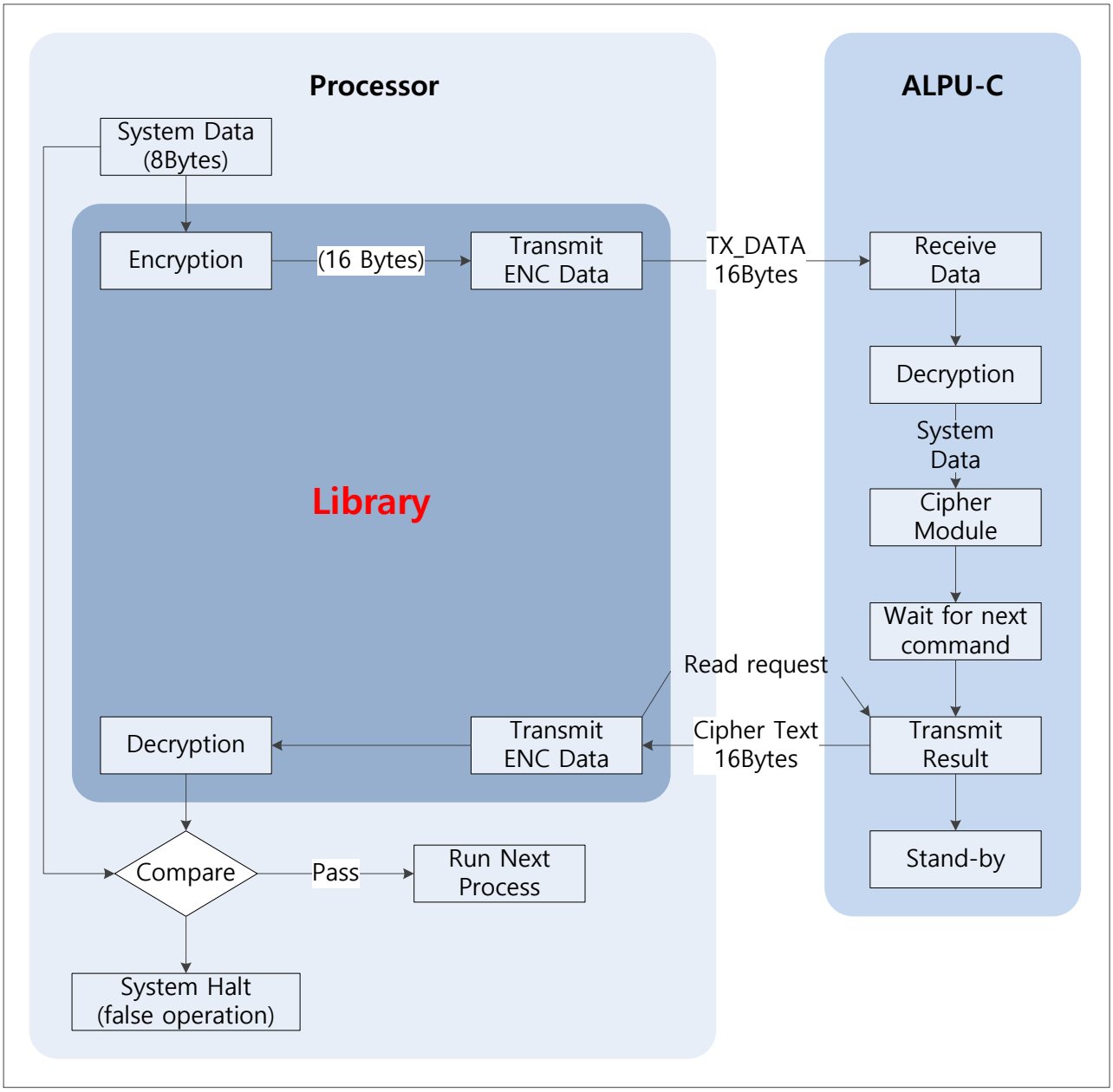


Figure 6-7. Encryption Flow

6.5 Communication Packet Structure

6.5.1 Write Packet Structure

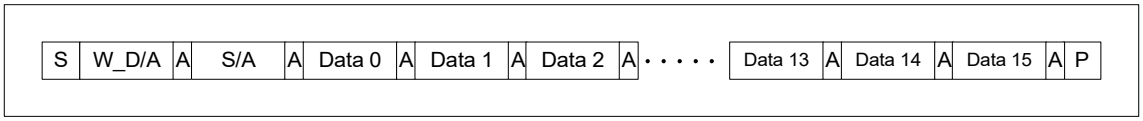


Figure 6-8. Write Packet Structure

S: Start

P: Stop

A : Acknowledge

W_D/A: Device Address (Write)

S/A: Sub Address

Data 0~15: 16byte Write Data (Initial Encryption Data)

6.5.2 Read Packet Structure

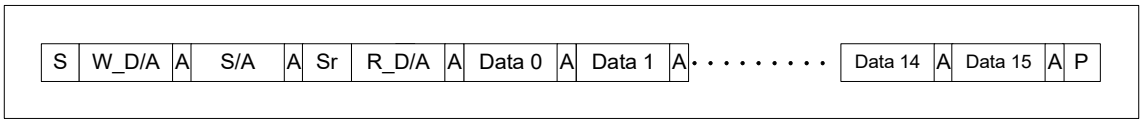


Figure 6-9. Read Packet Structure

S: Start

Sr: Repeated Start

P: Stop

A : Acknowledge

W_D/A: Device Address (Write)

R_D/A: Device Address (Read)

S/A: Sub Address

Data 0~15: 16byte Read Data (Result data)

6.6 Implementation

6.6.1 Bypass Mode

```
// Bypass Mode Set
sub_address = 0x80;

// Seed Generate
for ( i=0; i<8; i++) alpuc_tx_data[i] = rand();

// Write Seed Data to ALPU-C
_i2c_write(device_address, sub_address, alpuc_tx_data, 8);

// Read Result Data from ALPU-C
_i2c_read(device_address, sub_address, alpuc_rx_data, 8);

// XOR operation
for ( i=0; i<8; i++) alpuc_ex_data[i] = alpuc_tx_data[i] ^ 0x01;

// Compare the encoded data and received data
for (i=0; i<8; i++) {
        if (alpuc_rx_data[i] != alpuc_ex_data[i]) return 1; // Fail
}
return 0: // Pass
```

Figure 6-10. Bypass Mode example C code

1. Generate seed data(Plain Text) with the random data
2. Write seed data to ALPU-C
3. Read Result data from ALPU-C
4. Compare the encrypted data(Cipher Text) and received data

7. One Time Programmable ROM

ALPU-C has 128-bit OTP memory. To program OTP memory, DC 6.5V is applied to VPP pin. The memory write and read instructions are achieved through IIC interface. Refer to Application Notes

8. Reset Output

ALPU-C has Reset Out function that gives the reset signal to Reset pin of the external device. POR provides stabilized chip initialization.

8.1 Waveform

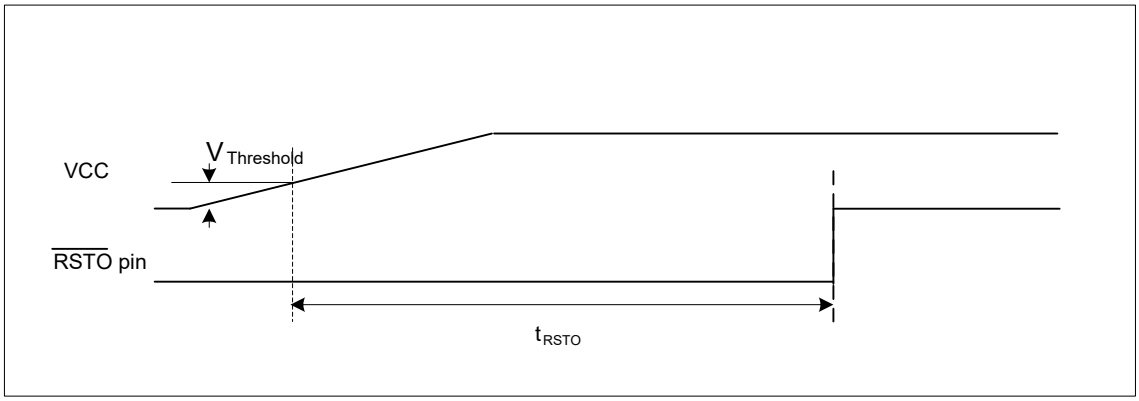


Figure 8-1. Start-up Waveform

VCC : Supplied Power

RSTO pin : Reset output signal

Figure8-1 shows the boot sequence of ALPU-C. When VCC is applied, the internal POR works as the figure of internal reset. After internal reset, a counter for Reset Out starts counting for $V_{Threshold}$ After that time, RSTO pin goes high.

Table 8-1. Start-up Timing parameters

Parameter	Symbol	MIN	TYP	MAX	Unit
Threshold Voltage	$V_{Threshold}$	1.1	1.2	1.3	V
Reset-Out Time (1)	t_{RSTO}	8		960	ms

Note (1)Refer to Table 8-2

Table 8-2. Selection mode of the Reset Out Time

Selection mode (1)	RSTO Time	Remarks
0	8ms	Default settings
1	16ms	
2	32ms	
3	64ms	
4	80ms	
5	160ms	

6	240ms	
7	320ms	
8	400ms	
9	480ms	
10	560ms	
11	640ms	
12	720ms	
13	800ms	
14	880ms	
15	960ms	

Note (1) The selection mode can be selected through the NEOWINE.

9. Communication Interface

9.1 IIC interface (Two Wire Interface)

The IIC Interface is ideally suited for typical microcontroller applications. The IIC protocol allows the systems designer to interconnect up to 128 different devices using only two bus lines, one for clock (SCL) and one for data (SDA). The only external hardware needed to implement the bus is a single pull-up resistor for each of the TWI bus lines. All devices connected to the bus have individual addresses.

ALPU-C operates as a slave device on the IIC bus. IIC interface on ALPU-C is compatible with Phillips Format, supporting up to 400 Kbps

9.1.1 Write Packet Structure

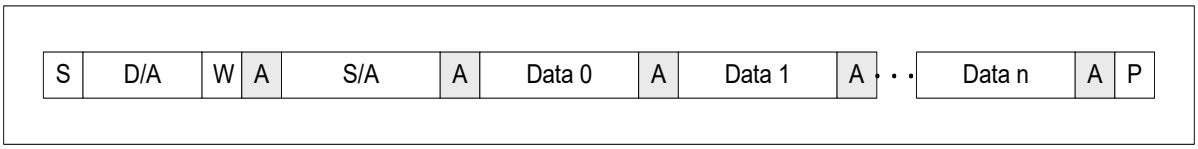


Figure 9-1. Write Packet Structure

S: Start

D/A: Device Address (Slave Address) 7bit

W: Device Address Write bit (0)

A: Acknowledge

S/A: Sub Address

Data 0~n: Write Data

P: Stop

9.1.2 Read Packet Structure

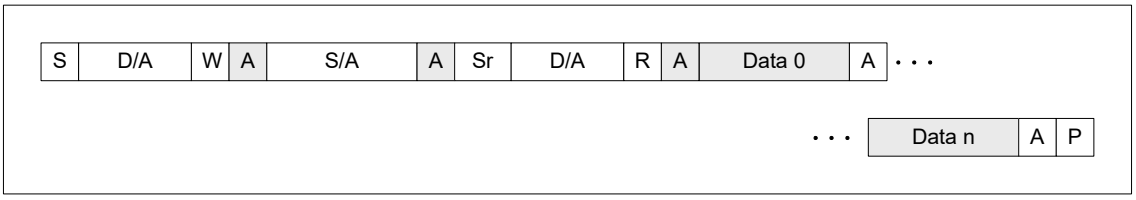


Figure 9-2. Read Packet Structure

S: Start

D/A: Device Address (Slave Address) 7bit

W: Device Address Write bit (0)

A: Acknowledge

S/A: Sub Address

Sr : Repeated Start (**Non-Stop**)

R: Device Address Read bit (1)

Data 0~n: Read Data

P: Stop

9.1.3 Waveform

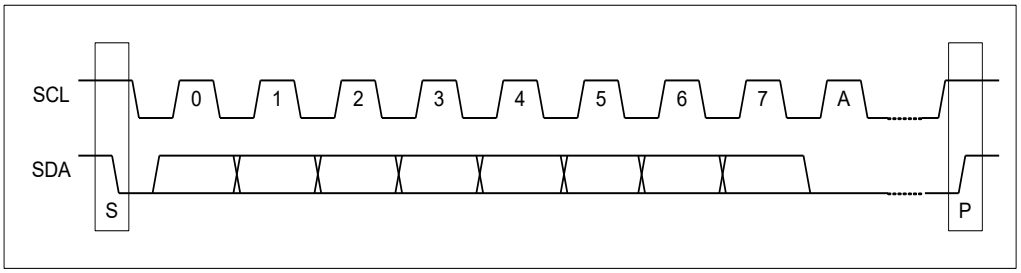


Figure 9-3. IIC waveform

9.1.4 Definition of timing

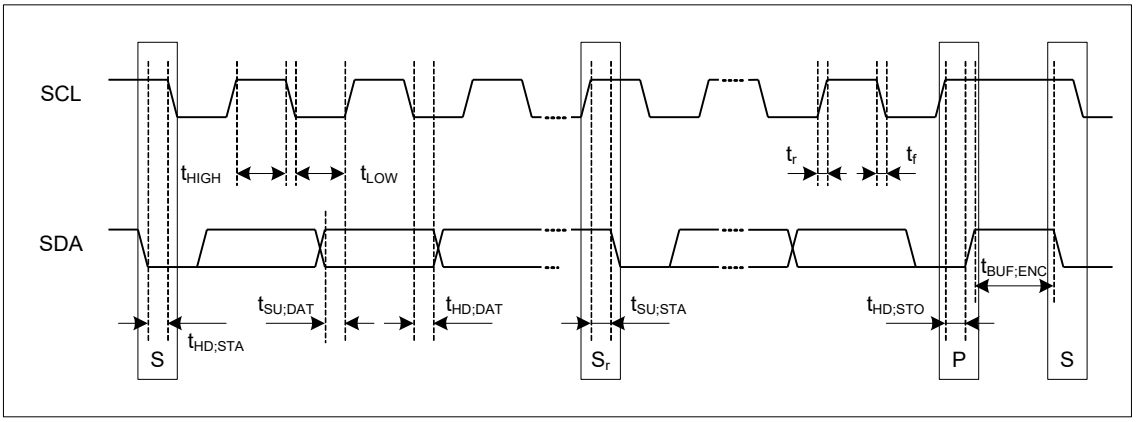


Figure 9-4. Definition of timing

Table 9-1. IIC Timing Parameters

Parameter	Symbol	Standard-Mode		Fast-Mode		Unit
		MIN	MAX	MIN	MAX	
SCL clock frequency	f_{SCL}	0	100	0	400	KHz
Hold time (repeated) START condition.	$t_{HD;STA}$	4.0	-	0.6	-	us
LOW period of the SCL clock	t_{LOW}	4.7	-	1.3	-	us
HIGH period of the SCL clock	t_{HIGH}	4.0	-	0.6	-	us
Setup time for repeated START condition	$t_{SU;STA}$	4.7	-	0.6	-	us
Data hold time	$t_{HD;DAT}$	5.0	-	-	-	us
Data setup time	$t_{SU;DAT}$	250	-	100	-	ns
Rising time of both SDA and SCL signals	t_r	-	1000	20	300	ns
Falling time of both SDA and SCL signals	t_f	-	300	20	300	ns
Setup time of STOP condition	$t_{SU;STO}$	4.0	-	0.6	-	us
Bus free time between STOP and START condition	$t_{BUF;ENC}$ (1)	1	-	1	-	ms

Note (1) It need for encryption processing time.

10. Electrical Characteristic

10.1 Absolute Maximum Ratings

Table 10-1. Absolute Maximum Ratings

Parameter	Min	Max	Units
Supply Voltage (1)	2.7	6.0	V
Storage Temperature	-35	120	℃
ESD Susceptibility	2000		V
DC Current VCC and GND		3	mA

Note. Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or other conditions beyond those indicated in the operational sections of this specification is not implied.

Note (1) In case of low voltage operation type, have the range of 1.4 ~ 3.8V.

10.2 Recommended Operating Conditions

Table 10-2. Recommended Operation Conditions

Parameter	Min	Max	Units
Operating Temperature	-30	80	℃
Operating Voltage (1)	3.0	3.6	V

Note (1) In case of low voltage operation type, have the range of 1.6 ~ 2.2V.

10.3 DC Characteristics

Table 10-3. DC Specifications 3.3V I/O

Symbol	Parameter	Condition	Min	Typ	Max
V_{IL}	Input Low Voltage				0.8V
V_{IH}	Input High Voltage		2.0V		
I_I	Input Leakage Current	VCC = MIN V_{IN}=GND or 3.6V			1uA
V_{OL}	Output Low Voltage	I_{OL} = 2mA			0.4V
V_{OH}	Output High Voltage	I_{OH} = 2mA	2.4V		3.6V

Table 10-4. Supply Current

Symbol	Parameter	Condition	Min	Typ	Max
I_{VCC}	VCC Supply Current	Active 16MHz, VCC=3.3V		200uA(1)	
		Sleep mode		55uA(2)	
Ivpp	VPP Supply Current	At OTP Write, VPP=6.5V		5mA	

Note (1) In case of 1.8V operation type, has under 130uA.

(2) In case of 1.8V operation type, has under 5uA.

10.4 Internal IP

Table 10-5. Internal Oscillator (Ta = 25°C)

Symbol	Parameter	Condition	Min	Typ	Max
fOSC	Switching Frequency		14MHz	16MHz	18MHz
Δf_{OSC}	Frequency Variation	-40≤Ta≤80°C	-		±10 %
Dmax	Duty Cycle		48%	50%	52%

Note (1) When the ring voltage is 3.3V (typical), CMOS voltage level and LVTTL voltage level are the same.

Table 10-6. Power-on-Reset

Symbol	Parameter	Condition	Min	Typ	Max
Vt	Threshold Voltage		1.1 V	1.2V	1.3V
t_{RINIT}	Register Initial time				160 us

Table 10-7. OTP cell

Symbol	Parameter	Condition	Min	Typ	Max
I_{VDD_R}	Read Current VDD				128uA (32bits)
I_{VPP_R}	Read Current VPP				704uA (32bits)
I_{VDD_P}	Program Current VDD				<1uA
I_{VPP_P}	Program Current VPP				600uA (for 1bit)
I_{VDD_SB}	Standby Current VDD				<1uA
I_{VPP_SB}	Standby Current VPP				<1uA
V_{PP}	Program VPP Voltage		6.25V	6.5V	6.75V

Note. No active current at sleep mode thus I_{VDD_SB} and I_{VPP_SB} is dependent on device leakage current.

Table 10-8. Regulator1 (1.8V for Logic, VCC=3.3V, Ta=25°)

Symbol	Parameter	Condition	Min	Typ	Max
VDD	Output Voltage	No load	1.7V	1.8V	1.9V
		0 < load < 3mA	1.6V	1.8V	2.0V
I_{max}	Peak Output Current			10mA	

11. Typical Operation Circuit

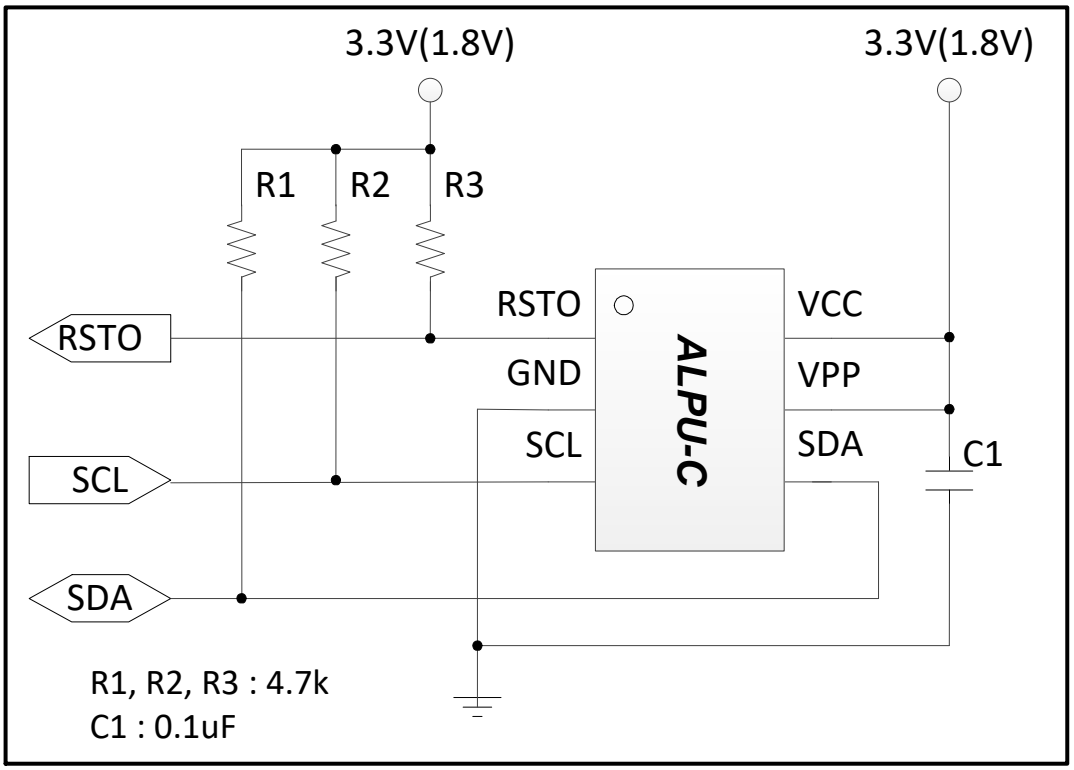


Figure 11-1. ALPU-C Operation Circuit

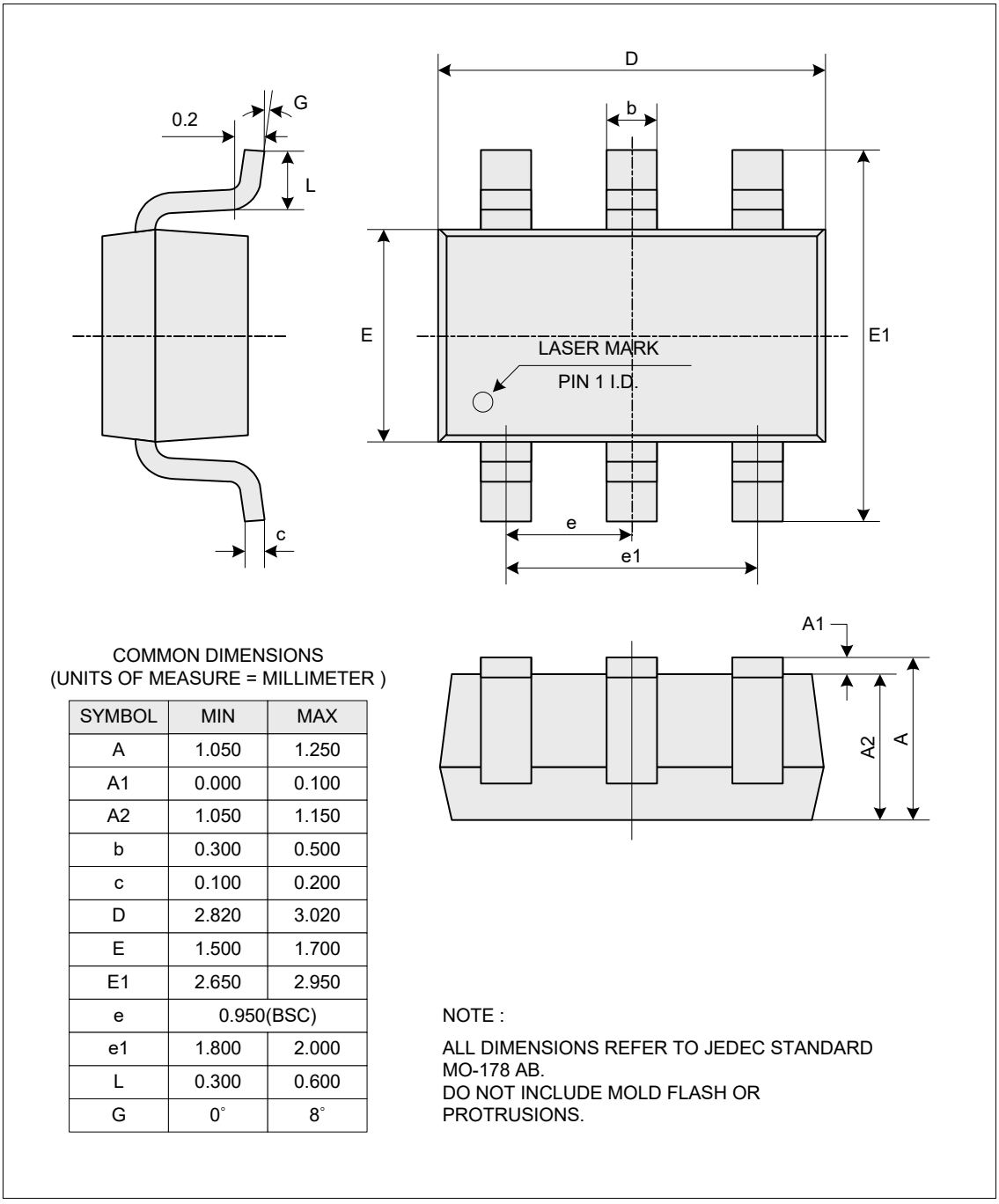
R1, R2 : 2K ~ 10K ohm (TYP. 4.7K ohm)

C1 : 0.1uF

Note (1) This can be changed to 1.8V Operation in case of low voltage type.

12. Package Information

12.1 POD - 6L-SOT23



COMMON DIMENSIONS
(UNITS OF MEASURE = MILLIMETER)

SYMBOL	MIN	MAX
A	1.050	1.250
A1	0.000	0.100
A2	1.050	1.150
b	0.300	0.500
c	0.100	0.200
D	2.820	3.020
E	1.500	1.700
E1	2.650	2.950
e	0.950(BSC)	
e1	1.800	2.000
L	0.300	0.600
G	0°	8°

NOTE :

ALL DIMENSIONS REFER TO JEDEC STANDARD MO-178 AB.
DO NOT INCLUDE MOLD FLASH OR PROTRUSIONS.

Figure 12-1. 6L-SOT23 Package Outline Dimension

13. Datasheet Revision History

13.1 Ver 1.0 (2013/02/15)

- Initial version release.

NEOWINE Co., Ltd.

http://www.neowine.com

Headquarters

BundangDowntown building #1206, 97, Baekhyeon-ro, Bundang-gu, Seongnam-city,
Gyeonggi-do, Republic of Korea
Zip code : 3595
Tel: 82-31-706-8484 Fax: 82-31-706-8485
contact@neowine.com

China Office (Shenzhen)

深圳市宝安区华丰国际商务大厦803
QQ : 2853578119
Tel: 13823560523