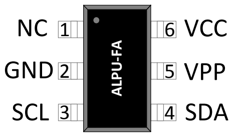
Features

- User programmable copy protection IC
- 32 Kbits EEPROM, Retention(10 years)
- Erase/Write Endurance: 100K
- Standard AES-128 encryption and decryption
- SHA-256/AES-128 Authentication
- User ID, User Serial, MIDR, RVC
- 3.3V Operation Voltage, I2C I/F
- Built- in Power on Reset and 8 MHz OSC.
- Active, Sleep Power Mode

Applications

- Print cartridge, GPS, Navigation
- Mobile Device, IPC, CCTV, DVD
- Set-Top Boxes (STBs), Etc.

Pin Configuration



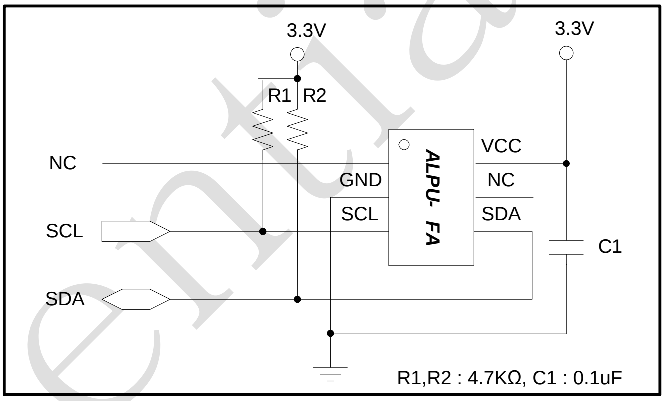
<SOT-23-6L Package>

- SOP8, TDFN2x3 packages will be available.

General Description

The ALPU-FA is the high-end IC among the ALPU series. The ALPU-FA has 32 Kbits EEPROM. A configuration data and user data can be saved at the EEPROM. The data is protected by password and encryption. The ALPU has SHA-256 core. SHA-256 is used for a authentication. ALPU-FA encryption core is based on Rijndeal AES-128 with programmable parameters. It is a slave device that always operates with MCU through the serial bus. The ALPU has internal 8 MHz clock. When MCU does not access the ALPU for a defined time, The ALPU goes to sleep mode. The 8MHz OSC does not oscillate for sleep mode.

Typical Operation Circuit



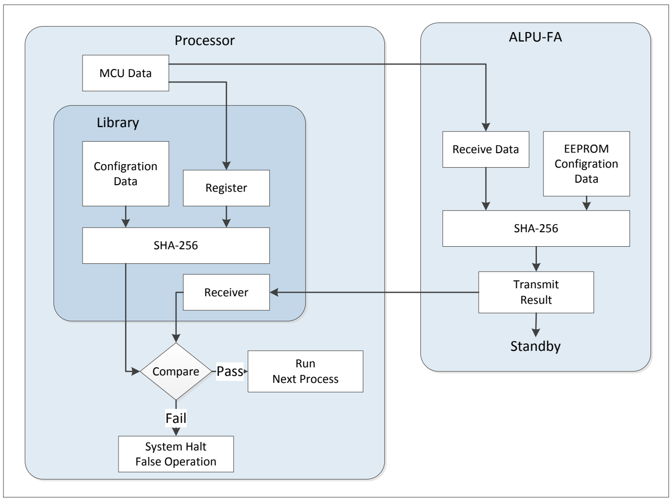
< SOT-23-6L Package Type >

SCL and SDA is open drain. SDA is bi-directional port.

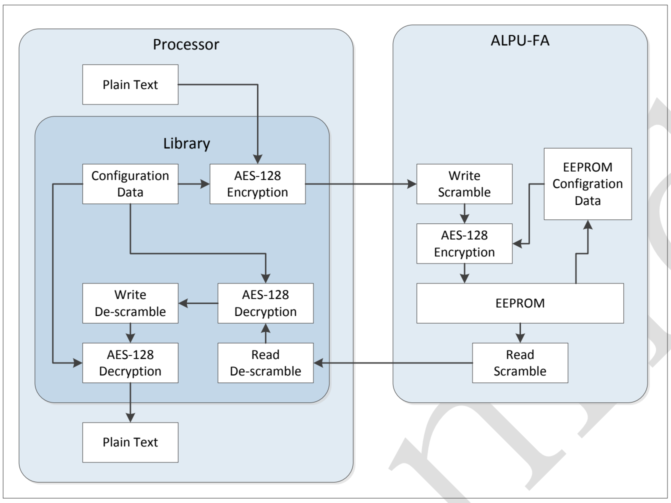
EEPROM

- Data Retention : 10 years
- Erase/Write Endurance: 100K@25℃
- Internally Synchronous read and read access time of 250ns.
- Low standby power consumption

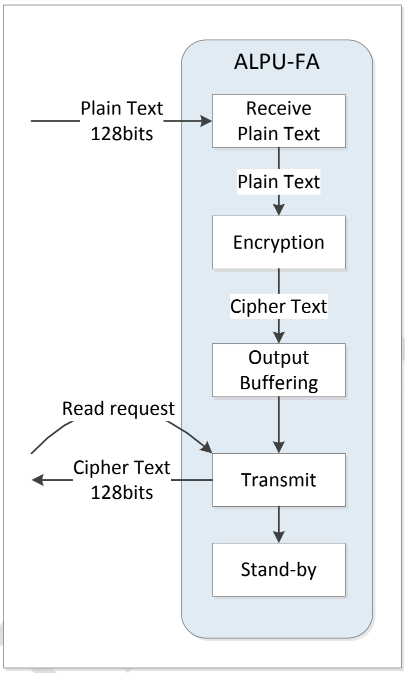
SHA-256 Encryption Flow



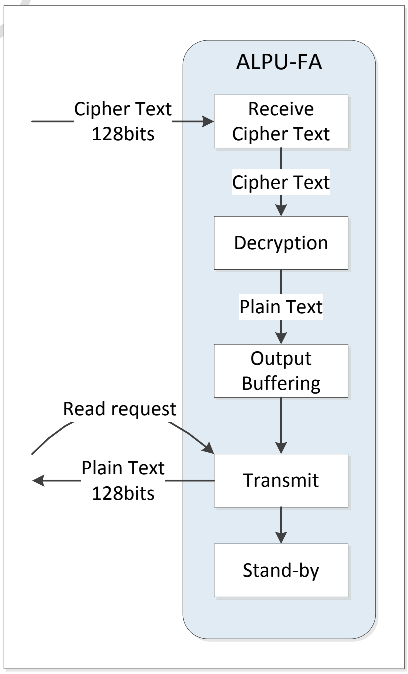
EEPROM Write/Read Flow



AES-128 Encryption Flow



AES-128 Decryption Flow



Contents

1. Overview

The ALPU-FA is the high-end IC among the ALPU series. The ALPU-FA has 32 Kbits EEPROM. A configuration data and user data can be saved at the EEPROM. The data is protected by password and encryption. The ALPU has SHA-256 core. SHA-256 is used for a authentication. ALPU-FA encryption core is based on Rijndeal AES-128 with programmable parameters. It is a slave device that always operates with MCU through the serial bus. The ALPU has internal 8 MHz clock. When MCU does not access the ALPU for a defined time, The ALPU goes to sleep mode. The 8MHz OSC does not oscillate for sleep mode.

1.1. Features

1.1.1 Security

- User programmable copy protection IC
- 32 Kbits EEPROM, Retention(10 years)
- Erase/Write Endurance: 100K
- Standard AES-128 encryption and decryption
- SHA-256/AES-128 Authentication
- User ID, User Serial, MIDR, RVC
- 3.3V Operation Voltage, I2C I/F
- Built- in Power on Reset and 8 MHz OSC.
- Active, Sleep Power Mode

1.1.2 Memories

- 32 Kbits EEPROM
- Configuration Data Region : 2.56 Kbits
- User Data Region : 30.208 Kbits

1.1.3 Peripheral Features

- IIC serial interface, Supporting up to 400 kbps

1.1.4 Special Features

- Built in Power-on-Reset
- Built in 8MHz selectable OSC
- Two Power Modes: Active, Sleep

1.1.5 Operating Voltages

- 3.3V Operation Voltage

1.1.6 Package

- SOT23-6L

1.2. Block Diagram

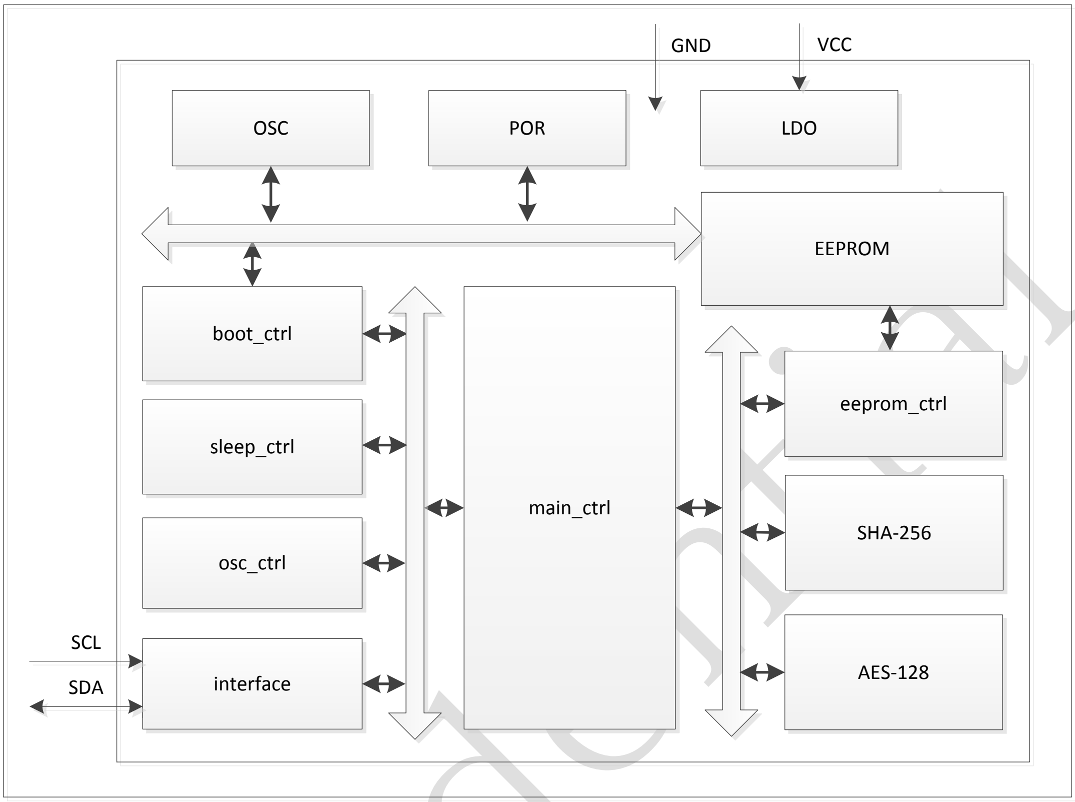


Figure 1-1. Block Diagram

ALPU-FA 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

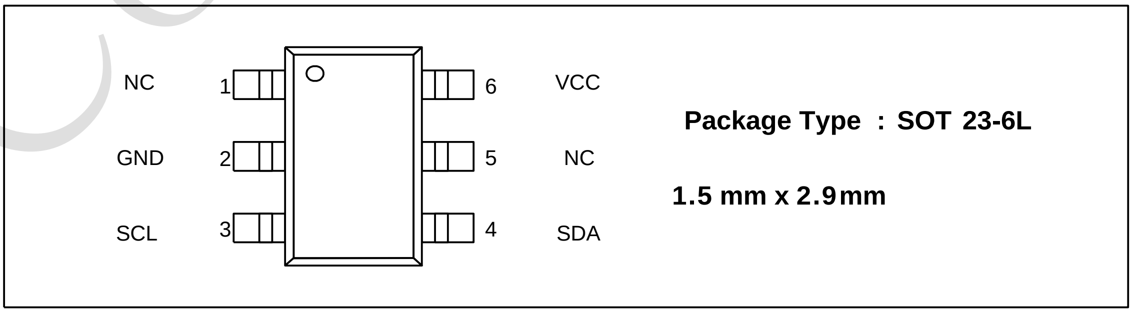


Figure 1-2. ALPU-FA Pin Configuration of SOT23-6L

1.4. Pin Descriptions

Table 1-1. ALPU-FA Pin Description of SOT-23-6L

Pin Num	Pin Name	Description	Remark
1	NC	None Connected	
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	NC	None Connected	
6	VCC [1]	Digital supply voltage	

Note [1] The ALPU-FA operation voltage is supported by 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.

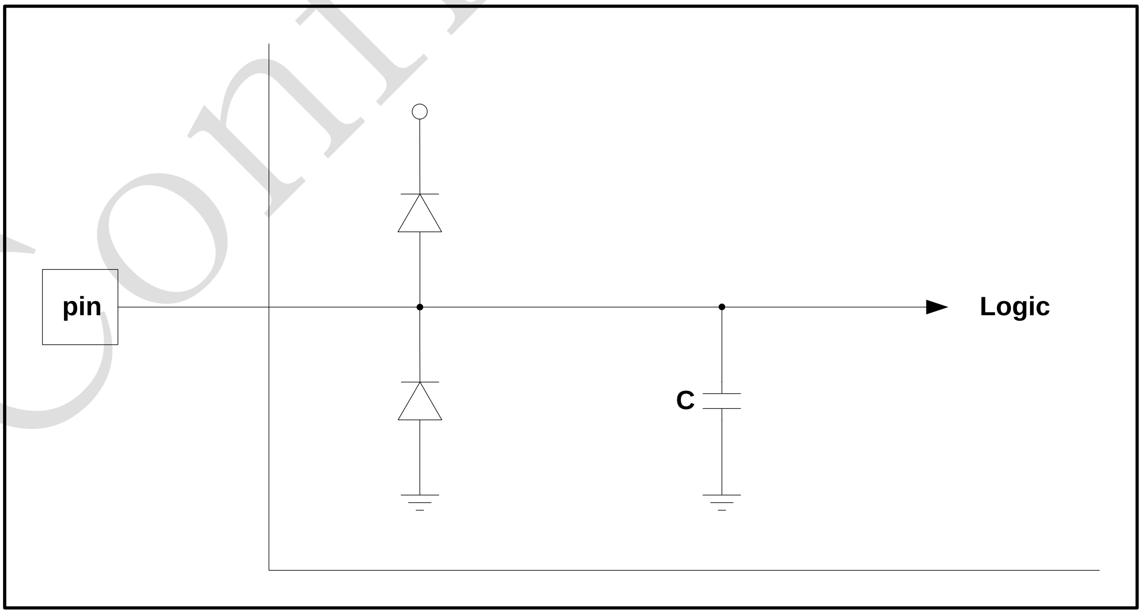


Figure 2-1. ESD protection circuit

2.2 I/O type

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

Table 2-1. I/O Types

Direction	Name	Description
	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.

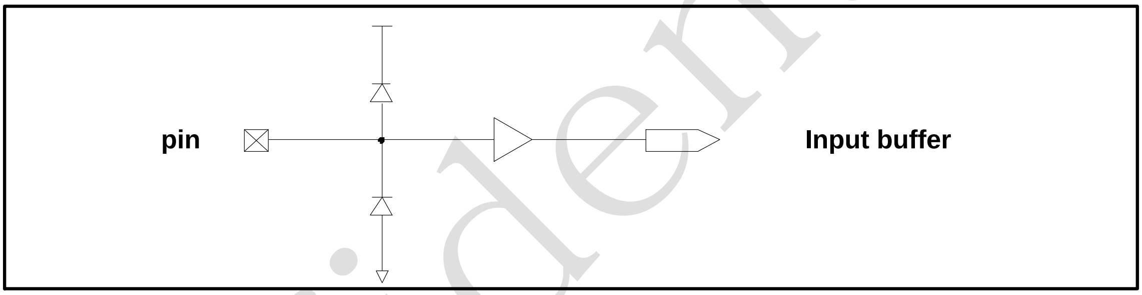


Figure 2-2. Input port Schematic

2.2.3 Bi-direction Port (SDA)

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

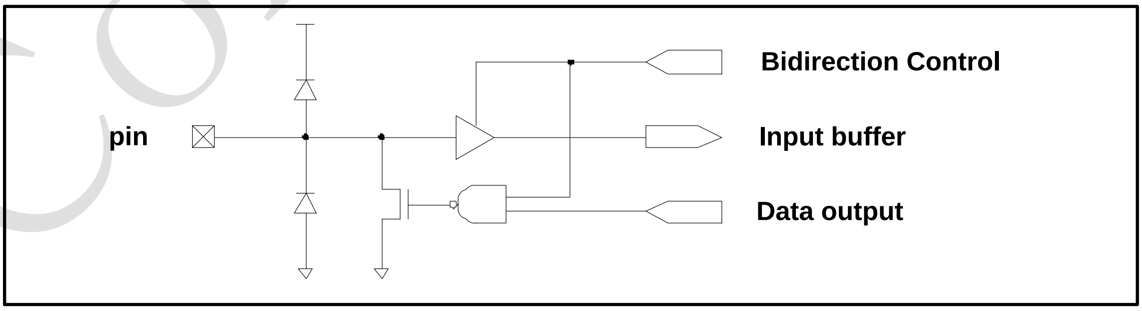


Figure 2-4. Bi-direction port Schematic

3. Clock Management

3.1 Internal clock

All Inner blocks use internal OSC clock. EEPROM can select OSC clock between 4MHz and 8MHz. Internal OSC clock is approximately 8MHz shown in Table3-1.

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

PARAMETER	SYMBOL	CONDITION	Min	Typ	Max	Unit
Frequency	f8m		7	8	9	MHz
Frequency Variation	Δf8m	-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-FA 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 specific time duration. This time can be from 4.096ms to 33 seconds in a 4.096ms time step. MCU can change this time duration with changing related register values. When the conditions above are not met it wakes up to active-mode. (Refer to chapter 4. Power Mode)

4. Power Mode

ALPU-FA 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 specific time duration. This time can be from 4.096ms to 33 seconds in a 4.096ms time step. MCU can change this time duration with changing related register values. (Refer to Figure 4-1)

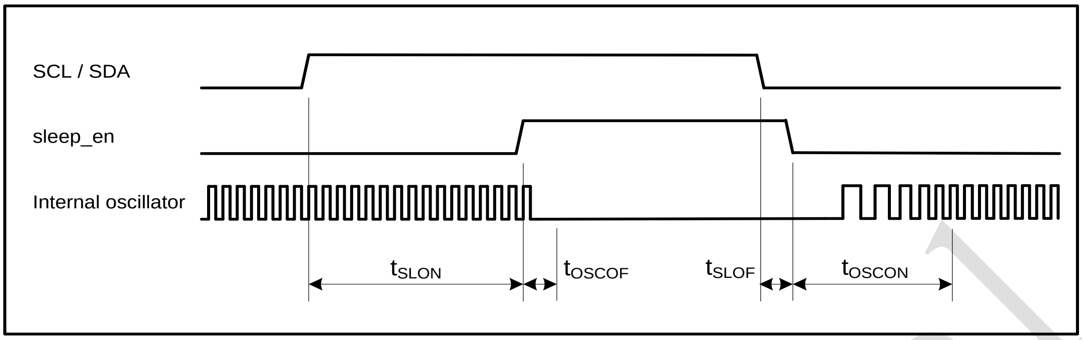


Figure 4-1. Sleep-mode Waveform

SCL/SDA : IIC signal

sleep_en : internal sleep-enable signal

Internal oscillator : 8MHz oscillator for internal logic

Table 4-1. Sleep-mode Waveform Parameters

Parameter	Symbol	MIN	TYP	MAX	Unit
Sleep-mode On Time	t_{SLON}	4.096		33000	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-FA has an internal POR (Power-on-Reset) circuit. When system power turns on ALPU-FA's POR resets its own system. During reset time, all internal registers of ALPU-FA are configured as their initial values. (Refer to chapter 9. Electrical Characteristic)

5.1 Start-up Waveform

After RESET, internal registers in ALPU-FA need $t_{INITIAL}$ time period to initialize all registers. After $t_{INITIAL}$ time period ALPU-FA's sleep time value can be changed by MCU. After Power On RESET the sleep time value is 33 seconds.

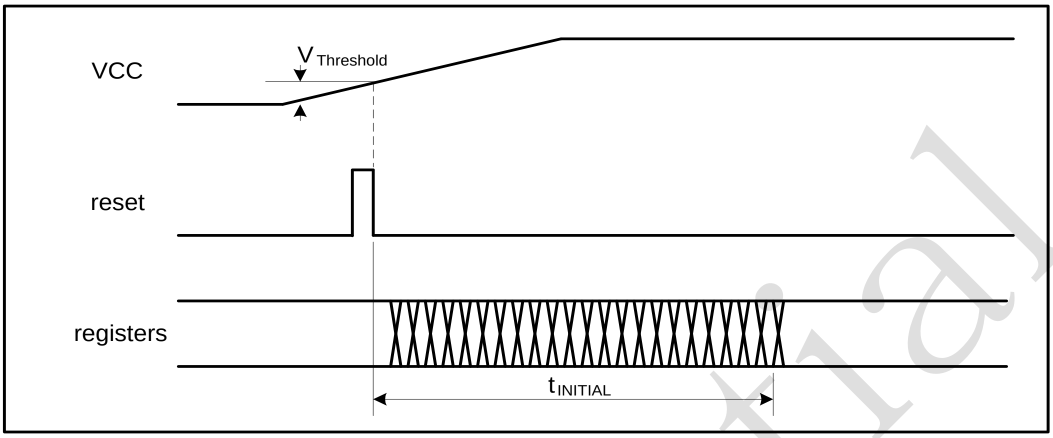


Figure 5-1. Start-up Waveform

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	$t_{INITIAL}$			14	ms

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

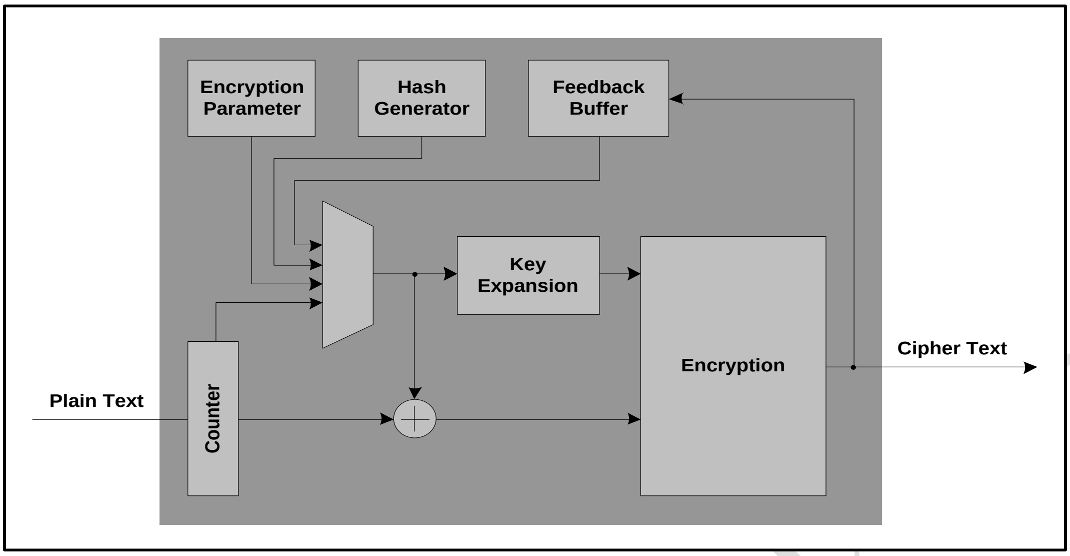


Figure 6-1. Encryption Core Block Diagram

ALPU-FA 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 AES-128 Encryption/Decryption

The ALPU-FA has 128-bit AES128 engine that accomplish encryption and decryption function. When AES128 encryption mode is selected, AES128 engine conducts cipher function with 128 bit key.

AES128 bit key and text input is applied to aes128 engine by external command from MCU through Host interface. AES128 encryption command invokes internal state machine and process aes128 encrypting operation.

The results of encryption, cipher text save to output buffer and assigned to read data buffer for read out through Host interface.

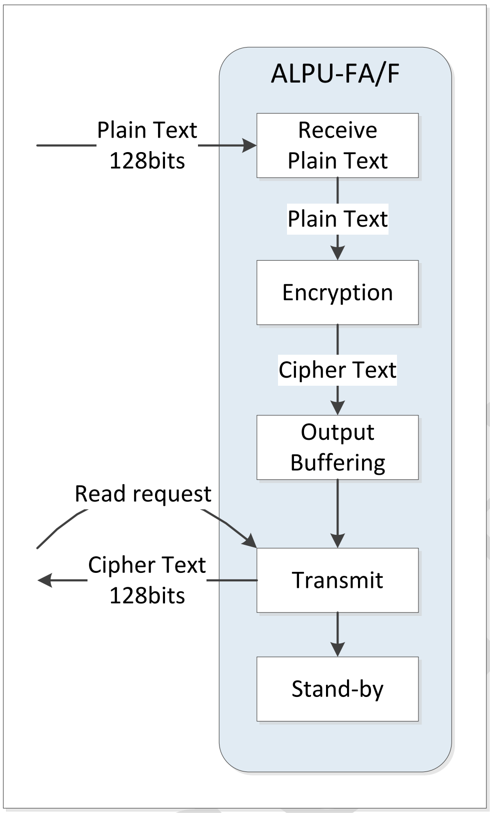


Figure 6-2. Encryption Core Block Diagram

The ALPU-FA has 128-bit AES128 engine that accomplish decryption function. When AES128 decryption is invoked, AES128 engine conducts decipher function with 128 bit key.

AES128 bit key and cipher text input is applied to aes128 engine by external command from MCU through Host interface. AES128 encryption command invokes internal state machine and process aes128 decrypting operation.

The results of encryption, decipher text save to output buffer and assigned to read data buffer for read out through Host interface.

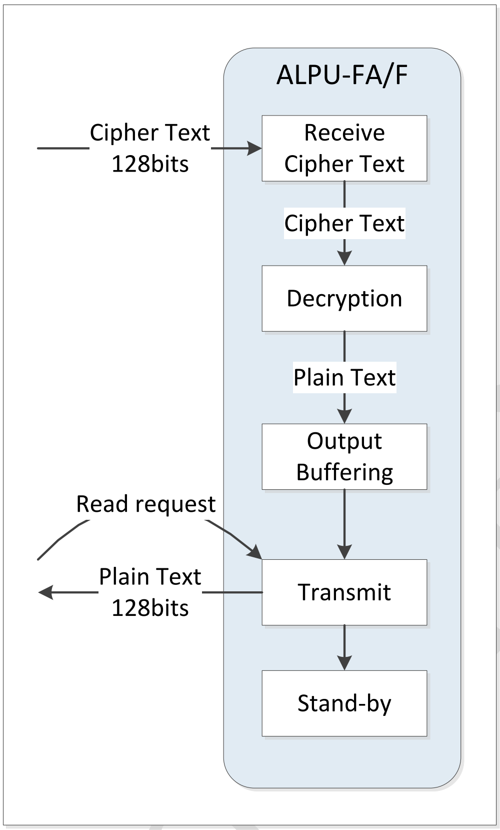


Figure 6-3. Decryption Core Block Diagram

6.3 Encryption Mode

6.3.1 Bypass Mode

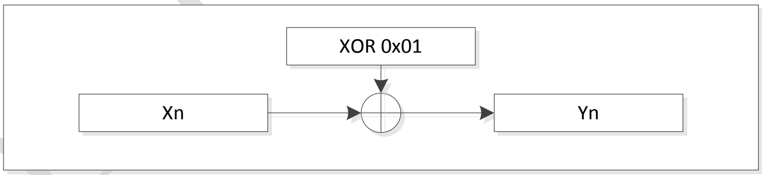


Figure 6-3. Bypass Mode Construction

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

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

6.5 Communication Packet Structure

6.5.1 Write Packet Structure

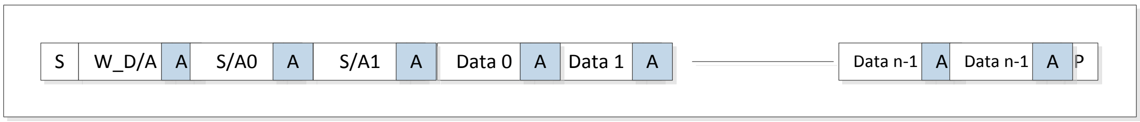


Figure 6-8. Write Packet Structure

S: Start

P: Stop

A : Acknowledge

W_D/A: Device Address (Write)

S/A0, S/A1: Sub Address

Data 0 ~ n-1: n byte Write Data (Can be 16 Byte Encryption Data)

6.5.2 Read Packet Structure

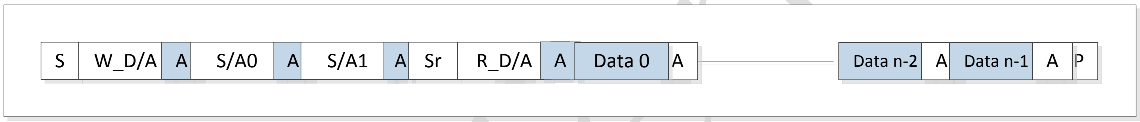


Figure 6-9. Read Packet Structure

S: Start

Sr: Repeated Start

P: Stop

A : Acknowledge

W_D/A: Device Address (Write)

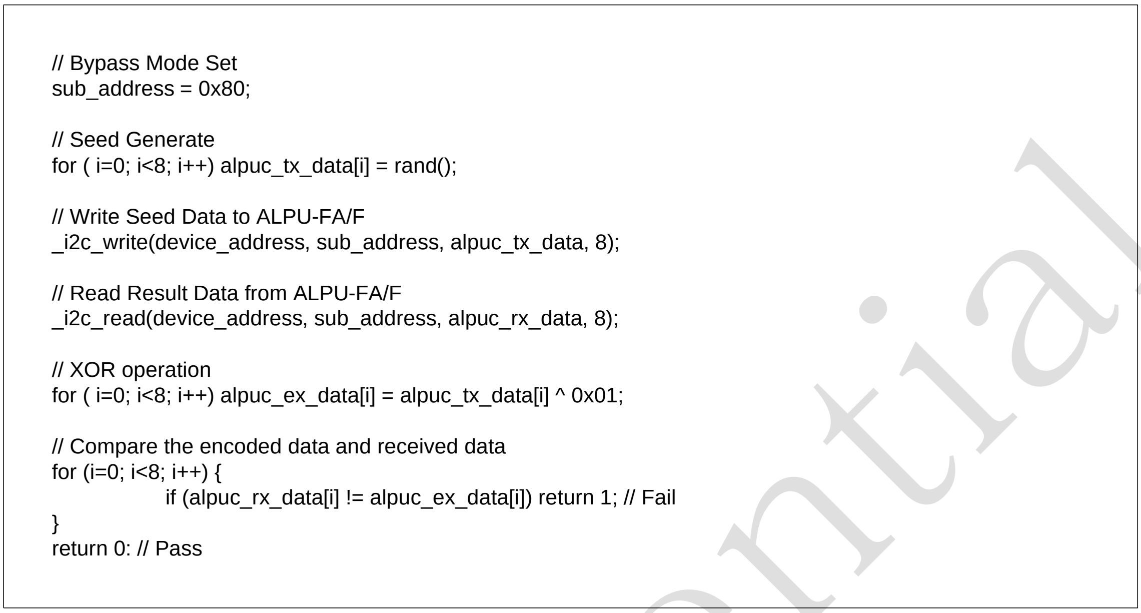
R_D/A: Device Address (Read)

S/A0, S/A1: Sub Address

Data 0 ~ n-1: n byte Read Data (Can be 16 Byte AES-128 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-FA/F
_i2c_write(device_address, sub_address, alpuc_tx_data, 8);

// Read Result Data from ALPU-FA/F
_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-FA
3. Read Result data from ALPU-FA
4. Compare the encrypted data (Cipher Text) and received data

7. EEPROM

ALPU-FA has 32 Kbits EEPROM memory. The memory write and read instructions are achieved through IIC interface. Refer to Application Notes

8. Communication Interface

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

8.1.1 Write Packet Structure

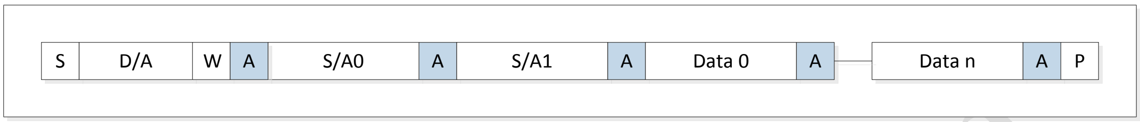


Figure 8-1. Write Packet Structure

S: Start

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

W: Device Address Write bit (0)

A: Acknowledge

S/A0, S/A1: Sub Address, S/A0(MSB 8bits of 16bits Address), S/A1(LSB 8bits of 16bits Address)

Data 0~n: Write Data

P: Stop

8.1.2 Read Packet Structure

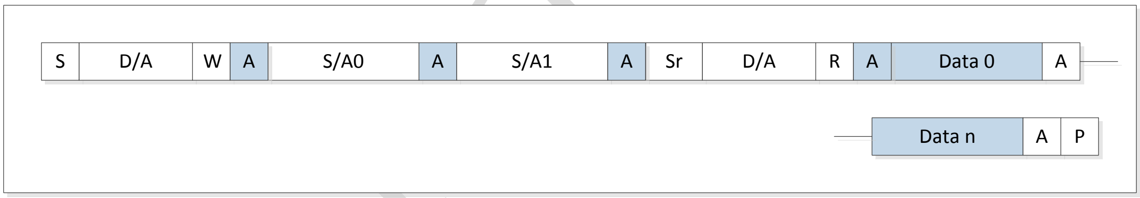


Figure 8-2. Read Packet Structure

S: Start

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

W: Device Address Write bit (0)

A: Acknowledge

S/A0,S/A1: Sub Address, S/A0(MSB 8bits of 16bits Address), S/A1(LSB 8bits of 16bits Address)

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

R: Device Address Read bit (1)

Data 0~n: Read Data

P: Stop

8.1.3 Waveform

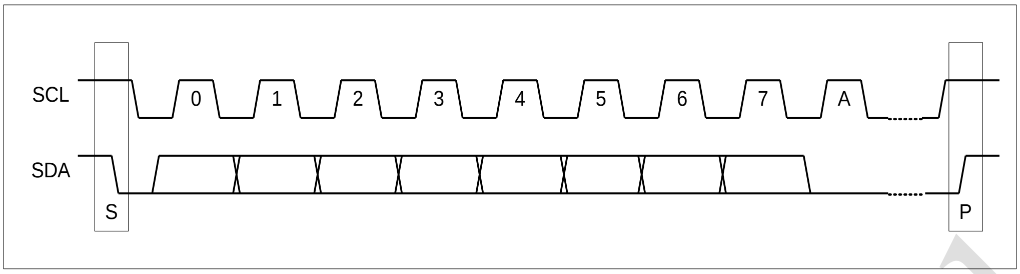


Figure 8-3. IIC waveform

8.1.4 Definition of timing

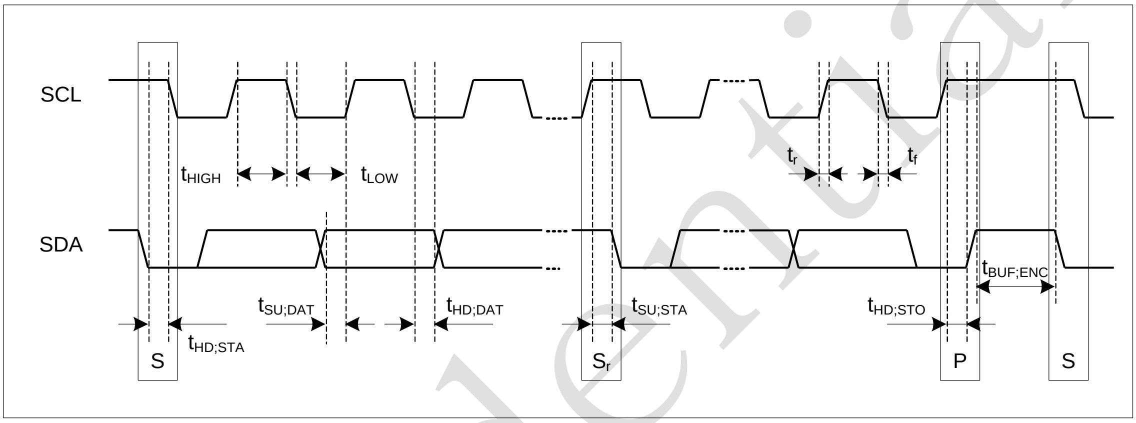


Figure 8-4. Definition of timing

Table 8-1. 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	t_r	-	1000	20	300	ns

SCL signals						
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.

9. Electrical Characteristic

9.1 Absolute Maximum Ratings

Table 9-1. Absolute Maximum Ratings

Parameter	Min	Max	Units
Supply Voltage	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.

9.2 Recommended Operating Conditions

Table 9-2. Recommended Operation Conditions

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

9.3 DC Characteristics

Table 9-3. 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 9-4. Supply Current

Symbol	Parameter	Condition	Min	Typ	Max
I_{VCC}	VCC Supply Current	Active 8MHz, VCC=3.3V		500uA(1)	

		Sleep mode		90uA[2]	

Note [1] TBD.

[2] TBD.

9.4 Internal IP

Table 9-5. Internal Oscillator (Ta = 25°C)

Symbol	Parameter	Condition	Min	Typ	Max
fOSC	Switching Frequency		7MHz	8MHz	9MHz
Δf_{OSC}	Frequency Variation	$-40 \leq Ta \leq 80°C$	-		±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 9-6. 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 9-7. EEPROM 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.

10. Typical Operation Circuit

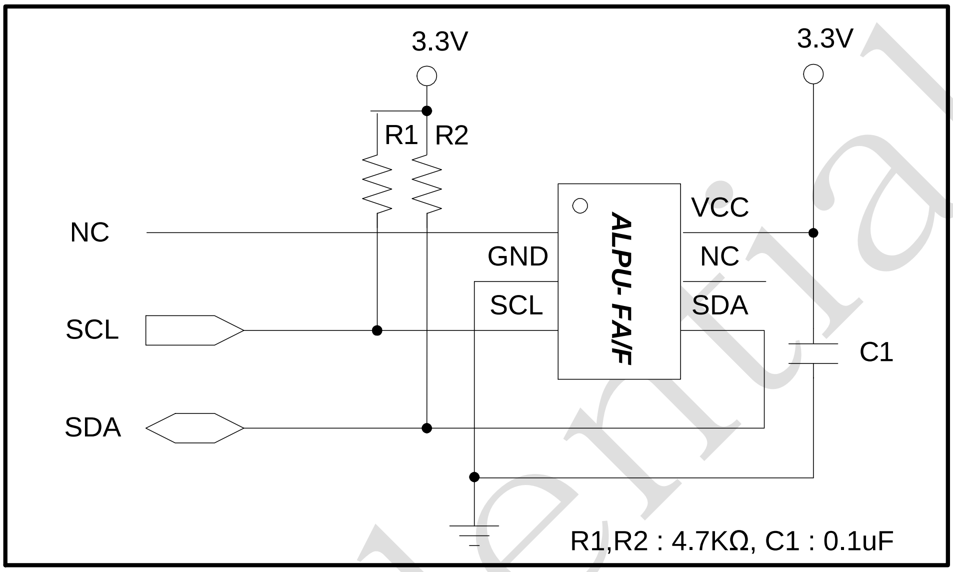


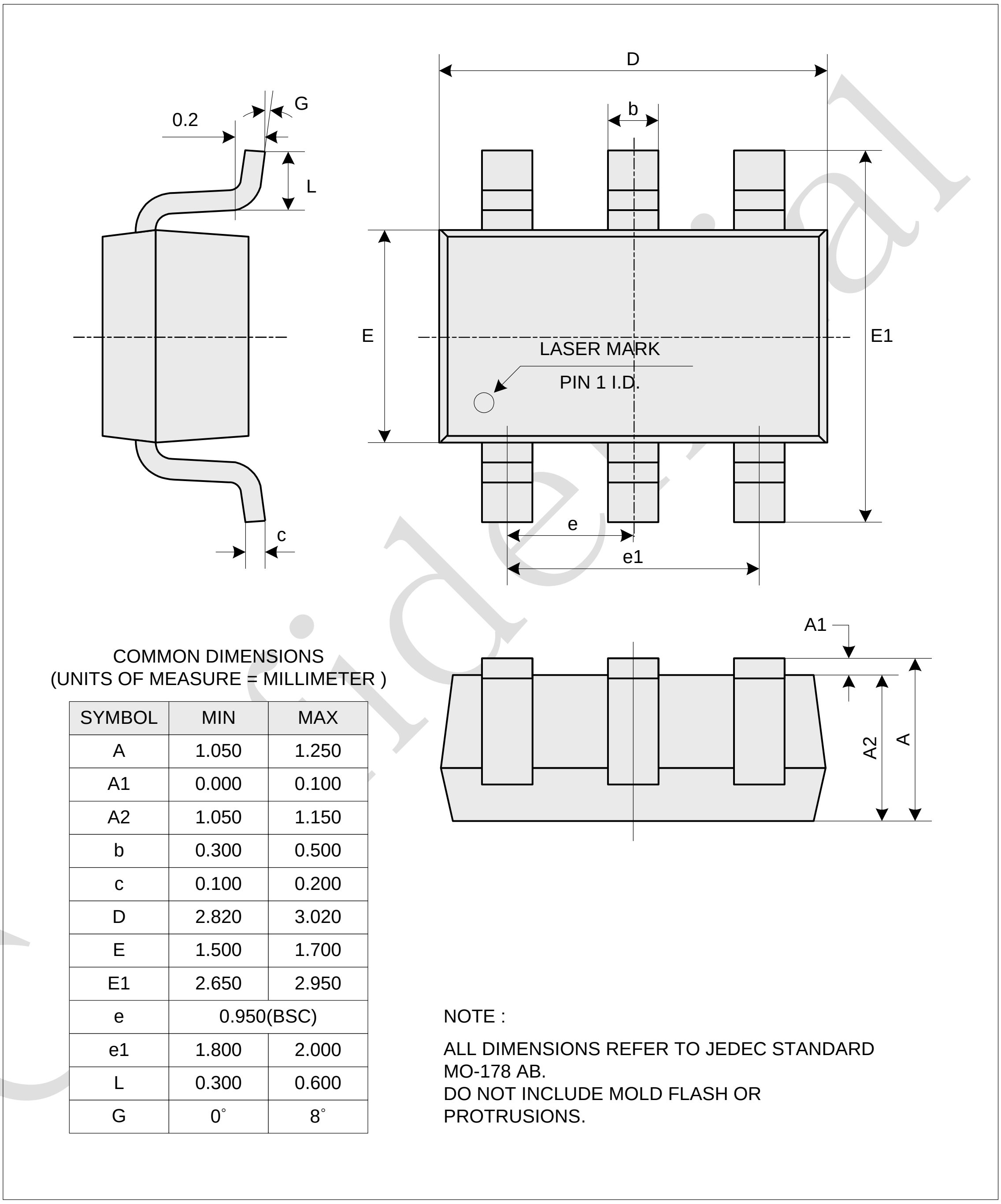
Figure 10-1. ALPU-FA Operation Circuit

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

C1 : 0.1uF

11. Package Information

11.1 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 11-1. 6L-SOT23 Package Outline Dimension

12. Datasheet Revision History

12.1 Ver 1.0 (2015/10/28)

- Initial version release.

NEOWINE Co., Ltd.

http://www.neowine.com

Headquarters
#401, 182, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do,
Korea 463-400
Tel: 82-31-706-8484   Fax: 82-31-706-8485
info@neowine.com

China Office (Shanghai)
A-2111 Oriental International Plaza, 85 LouShanGuan Rd, Changning District, Shanhai
China 200336
Tel: 86-21-6278-2288(ext 221)   Fax: 86-21-6278-3723
alpu-china@neowine.com