OK301

USB

Cloud Keyboard Security Controller

Specification

Version 1.1

November 8, 2012

oTHE Technology Inc.

Update History		
Version	**Date**	**Description**
0.9	August 8, 2011	Preliminary version.
1.0	May 2, 2012	Formal Release Version.
1.1	November 8, 2012	Update Chapter 10 - Application Circuit

Chapter Content Page

1. General Description

The OK301 Cloud Keyboard Security(CKS) Controller is a single chip implementation of CKS for USB keyboard. Cloud Keyboard Security is a method to resist keylogger for the Personal Computer in the Cloud Computing Internet. The OK301 embedded FIPS certificated AES engine for CKS. By the method of OK301 CKS controller, the Keylogger can't steal user's keystrokes with right meanings, so that the online applications are safe for any critical business transaction.

The OK301 built in an oTHE 8-bit single instruction RISC CPU with 8KByte Flash only. It provides USB 2.0 interface and supports USB 1.1 protocol. Meanwhile, OK301 embedded a non-conflict key-scan architecture that allows user press over 12 keys at the same time. It resolved a long time problem that USB keyboard can not press over 6 keys at the same time. This key-scan architecture also includes auto key scan change detection and ghost key cancellation.

The OK301 supports LQFP-48Pin package for standard USB keyboard. It is a best cost-effective keyboard controller, and high security keyboard encryptor for anti-keylogger solutions.

2. Features

- Single instruction RISC architecture(TSIR)
- Embedded 256 Bytes RAM, 8Kbytes Flash
- USB V2.0 low speed and V1.1 protocol
- Supports two SPI chip select for serial EEPROM
- Supports 8 x 18 keyboard scan matrix
- Hardware auto key scan change detection and ghost key cancellation
- Allow press over 12 keys at the same time
- Make / break generation keys without buffer size limitation
- AES security engine (US NIST FIPS certificated #1576)
- Hardware Random Number Generator
- Phantom key detection
- Supports Windows 98/ 2000/ NT/ XP/ Vista/ 7
- Support Multi-media or other special application keyboard encoder
- Internal pull-up resistor
- Compatible with carbon wire application
- Full duplex UART for TX and RX operation
- Built-in power management
- Internal oscillator
- Embedded 5V to 3.3V convertor
- Watchdog Timer
- Operating voltage: 4.5~5.5V
- Package: LQFP-48 pin

3. Block Diagram

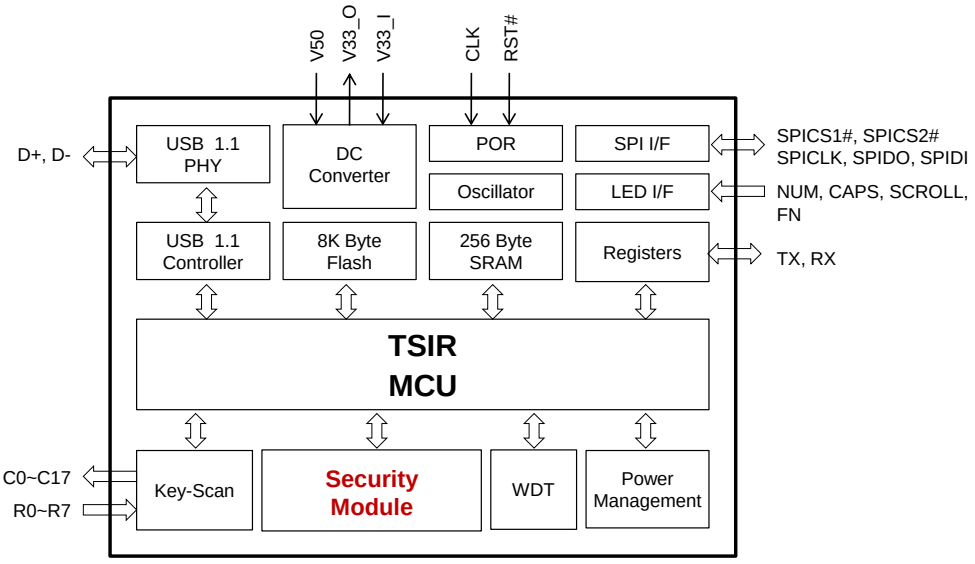


Figure 3-1: OK301 Block Diagram

4. Pin Configuration

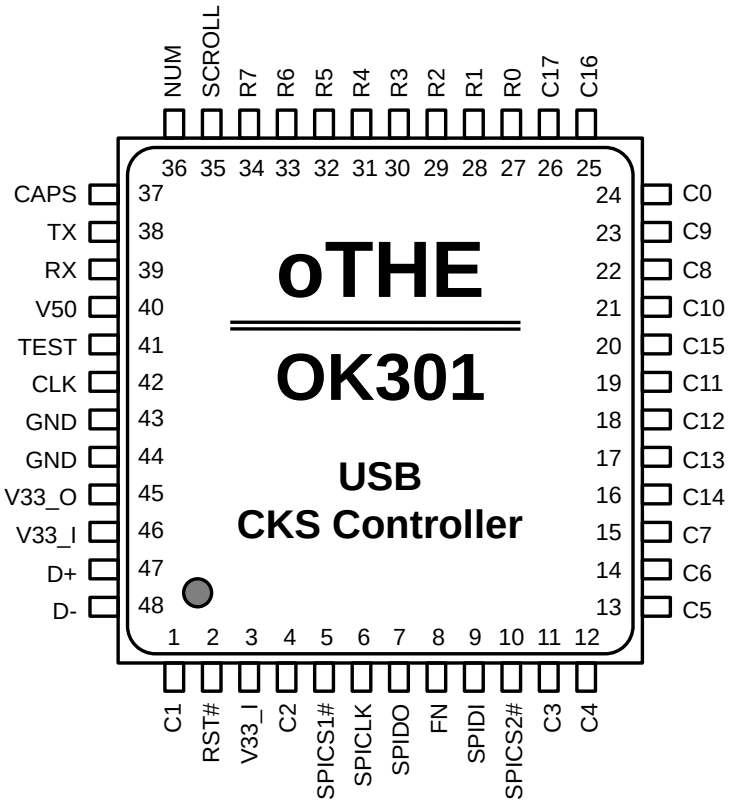


Figure 4-1: OK301-LQ48 (LQFP-48pin)

5. Ordering Information

Table 5-1: Part Number

Part Number	Package Descriptions
OK301-LQ48	LQFP-48pin

6. Pin Description

Table 6-1: Pin Description

Symbol	I/O	Description
R0~R7	I	Keyboard Scan Input
C0~C17	O	Keyboard Scan Output
SPICS1#	O	SPI Master Chip Select 1
SPICS2#	O	SPI Master Chip Select 2
SPICLK	O	SPI Master Clock Output
SPIDO	O	SPI Master Data Output
SPIDI	I	SPI Master Data Input
SCROLL	O	Scroll lock LED
NUM	O	Num Lock LED
CAPS	O	Caps Lock LED
FN	O	Fn Lock LED
TX	O	UART TX
RX	I	UART RX
D+	I/O	USB PHY I/F D+
D-	I/O	USB PHY I/F D-
CLK	I	External CLK (optional)
RST#	I	External Reset (optional)
TEST	I/O	Test Pin
V50	PWR	5V Power from USB Connector
V33_O	PWR	3.3V Regulator Output
V33_I	PWR	3.3V Regulator Input (2.0V~3.3V)
GND	PWR	Power Ground

7. Functional Description

7-1 USB Device Interface

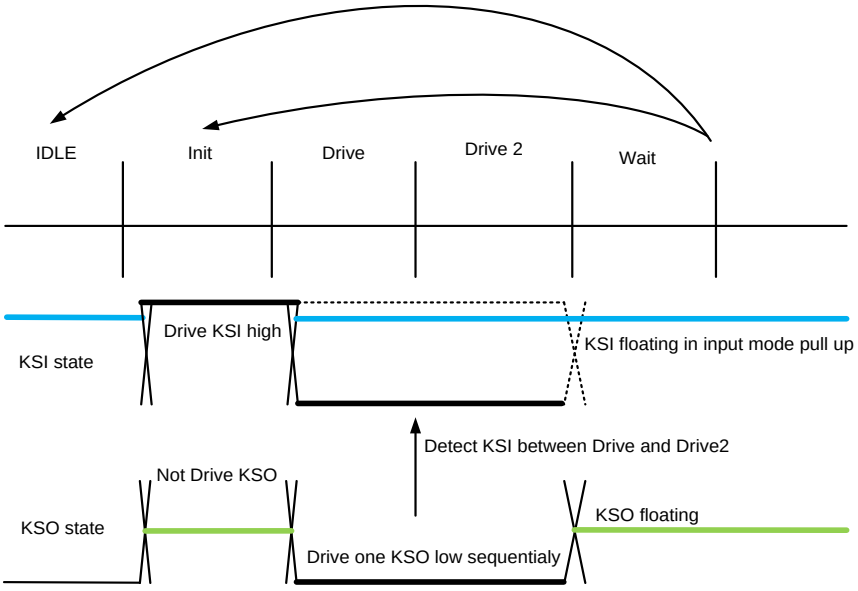
The module manipulates the transactions of USB Device, including Control and Interrupt transactions in 8 bytes format. There are two kinds of endpoint in the USB Device. They are Control pipe endpoint 0 and Interrupt endpoint = 1~14. The max data for a packet is 8 bytes. Setup OUT byte count always = 8 bytes. Interrupt endpoint 1~14 should have traffic control by firmware.

The USB Device Interface also includes a USB DLL (Delay Loop Lock). It enables OK301 to decode USB transaction in low speed clock (1.5Mhz), preventing from using higher speed clock (6 or 12Mhz) to over sampling. The methodology enables OK301 to run USB keyboard in very low power consumption.

7-2 Keyboard Scan Controller

OK301 includes a hardware scan keyboard controller. The firmware management is minimized. The ghost key cancellation are also done by hardware.

Fast keyboard scan controller scanning method



7-3 Keyboard Matrix

Table 7-1: Keyboard Matrix

	R0	R1	R2	R3	R4	R5	R6	R7
C0	Pause	Power	€	Sleep	Ctrl-R	Wake-up	Ctrl-L	F5
C1	Q	Tab	A	ESC	Z	N-CHG	` (~)	1 (!)
C2	W	CAP	S	K45	X	CHG	F1	2 (@)
C3	E	F3	D	F4	C	ROMA	F2	3 (#)
C4	R	T	F	G	V	B	5 (%)	4 ($)
C5	U	Y	J	H	M	N	6 (^)	7 (&)
C6	I	] (})	K	F6	, (<)	K56	= (+)	8 (*)
C7	O	F7	L	¥	. (>)	APP	F8	9 ('(')
C8	P	[({)	; (:)	' (")	K42	/ (?)	_ (-)	0 (')')
C9	Scroll		Fn	Alt-L	M/Mode	Alt-R		Print Scr
C10	K14	Back	\ (|)	F11	Enter-L	F12	F9	F10
C11	7 (Home)	4 (←)	1 (End)	Space	Num	↓	Del	Power
C12	8 (↑)	5	2 (↓)	0 (Ins)	/	→	Ins	Sleep
C13	9 (PgUp)	6 (→)	3 (PgDn)	. (Del)	*	-	Page Up	Page Dn
C14	+	K107	Enter-R	↑	Paly/Pause	←	Home	End
C15	Wake Up	Shift-L	Shift-R	Volume -	Volume +	NextTrack	PrevTrack	Media
C16	Mail	Win-L	WWW Forward	WWW Stop	WWW Back	WWW Refresh	Mute	WWW Search
C17	KC-L	WWW Favorites	Win-R	My Computer	Stop	Caculator	Web/Home	KC-R

7-4 Security Module

The module includes security control logic. The internal functions include AES, DES, RNG, RSA. The firmware can combine the functions to do process the critical data. OK301 series chip only includes AES and RNG modules for reducing the cost. There are 3 registers for security operations: AS, CS, DS.

AS : 128 bits (16 bytes): AES data for encryption or decryption. ASW0~3 are four 32 bits word of AS.

CS : 128 bits (16 bytes):AES key for encryption or decryption.

DS : 32 bits (4 bytes): AES key generation temp storage.

AS, CS, DS are accessed by programming SEC_INDEX and SEC_DIO registers. The data input/output are only accessible by AS. The CS register can be accessed by A x C exchange operation through SEC_CSR operations.

The AES encryption and decryption are done by sequential of data(SEC_INDEX/SEC_DIO) and SEC_CSR programming.

AES Encryption Pseudo Code

1. AddRoundKey(AS, CS), AS = AS ^ CS, round 1
2. Repeat 3~7 for 1~9 rounds:
3. *Expension AES key in CS, round 1~9*
4. *SubByte(AS)*
5. *ShiftRow(AS)*
6. *MixColumn(AS)*
7. *AddRoundKey(AS, CS), AS = AS ^ CS*
8. Expension AES key(round 10) in CS
9. SubByte(AS)
10. ShiftRow(AS)
11. AddRoundKey(AS, CS), AS = AS ^ CS

AES Decryption Pseudo Code

1. Expension AES key in CS
2. AddRoundKey(AS, CS), AS = AS ^ CS, round 10
3. Repeat 4~8 for 10~2 rounds
4. Expension AES key in CS
5. ShiftRow(AS)
6. InvSubByte(AS)
7. InvMixColumn(AS)
8. AddRoundKey(AS, CS), AS = AS ^ CS
9. Expension AES key in CS,round 0
10. InvSubByte(AS)
11. InvShiftRow(AS)
12. AddRoundKey(AS, CS), AS = AS ^ CS, round 1

7-5 Power Management

The module collects clock and distributed control registers not listed in other modules. The chip includes two power states for saving power consumption by programming: **IDLE** and **STOP**.

CPU IDLE State

CPU is in idle for low power mode to stop the instruction execution of CPU. The interrupt event will exit the IDLE state. The IDLE state is active by CPU IDLE instruction. The interrupt flag can be used to know the source of wakeup from IDLE state. There are 3 instructions for supporting IDLE state:

IDLE Enter IDLE state if IDLE_ON already set enable IDLE flag
IDLE_ON Enable CPU enter IDLE state (execute when device state machine is going to IDLE)
IDLE_OFF Disable CPU enter IDLE state (execute in a interrupt service routine)

Clock STOP State

In the Clock STOP State, the clock source is stop for low power mode to stop logic clock, except the clock control logic is not stop. The GPI async. event will wake up the STOP clock state. The STOP state is active by programming the Enable STOP Clock control register in ***Chip Configuration (CLK_CFG.0)***, then let CPU execute IDLE instruction. If there is no hardware not in idle state, the chip will stop clock immediately. If there is some hardware not in idle state, the stop clock logic will wait until the hardware state machine going to idle. The clock wakeup event should eventually generate an interrupt to CPU, so that the firmware can use the interrupt to know the wakeup source of Clock STOP State.

To enter Clock STOP State, the ***Enable Stop Clock*** in ***CLK_CFG*** should be enabled before CPU entering CPU IDLE State by IDLE instruction.

Table 7-2: Power Control Mode

Power Level	Oscillator	MCU Clock	USB SIE Clock	Clock Control	Active By
CPU IDLE	ON	ON	OFF	ON	CPU IDLE
MCU Clock Stop	ON	OFF	OFF	ON	CPU IDLE
USB Transaction	ON/OFF	ON/OFF	ON	ON	Auto Control
Oscillator Stop	OFF	OFF	OFF	OFF	CPU IDLE

8. Electrical Characteristics

8-1 Absolute Maximum Ratings

Table 8-1: Absolute Maximum Ratings

Parameter	Symbol	Value	Unit
Supply Voltage on V50 Relative to GND	V_{DD}	-0.5V~+6.5V	V
Supply Voltage on V33_I Relative to GND	V_{33_I}	-0.5V~+4.0V	V
Input Voltage Range	V_{IN}	-0.3 to V_{DD}+0.3	V
Power Dissipation	P_D	≦300	mW
Operation Temperature Range	T_{OPR}	-0 to +70	℃
Storage Temperature	T_{ST}	-45 to +150	℃
Soldering Temperature (10 seconds, Note 2)	T_{SOLDER}	260	℃

Notes:

1. These are stress ratings only. Stresses exceeding the range specified under ”Absolute Maximum Ratings” may cause substantial damage to the device. Functional operation of this device at other conditions beyond those listed in the specification is not implied and prolonged exposure to extreme conditions may affect device reliability.

2. The humidity resistance of the flat package may be reduced if the package is immersed in solder. Use a soldering technique that does not heat stress the package.

3. All supply voltages are referenced to GND = 0V.

8-2 DC Electrical Characteristics

Table 8-2: DC Electrical Characteristics

Symbol	Description	Condition	Min.	Typ.	Max.	Unit
V_{50}	Supply Power	USB 5V	4.5	5	5.5	V
V_{IH1}	R0~R7 Input High	Voltage Schmitt-trigger is built-in	1.9		VDD+0.3	V
V_{IL1}	R0~R7 Input Low	Voltage Schmitt-trigger is built-in	-0.3		1.6	V
V_{IH2}	Input High	Voltage Schmitt-trigger is built-in	2.4		VDD+0.3	V
V_{IL2}	Input Low	Voltage Schmitt-trigger is built-in	-0.3		1.7	V
V_{OH}	Output High	Voltage I_{OH} = -2mA		V33_I - 0.3		V
V_{OL}	Output Low	Voltage I_{OL} = 2mA		0		V
I_{DS}	Drive/Sink Current for LED	V_{OL} = 0.2V (R=220 ohm)		8		mA
I_{IN}	Input Leakage Current	V33_I = 3.3V	-1		1	μA
R_{P1}	Pull up Resistance		60	80	100	KΩ
R_{P2}	Pull up Resistance	For Carbon wire	1.5	1.8	2.1	MΩ
I_{OP1}	Chip Operating Current	USB connected, continuous key pressed		2		mA
I_{OP2}	Chip Operating Current	USB connected,		2		mA
I_{SB1}	Chip Standby Current	USB Connected. Int OSC disable		2		mA
I_{SB2}	Chip Standby Current	non-WDT standby		270		μA
V_{33_O}	3.3V Regulator Output	VDD= 5V, 30mA (100Ω load)	3	3.3	3.6	V
F_{OSC}	System Clock	V33_I=3.3V, USB connected.	-1.5%	1.5	+1.5%	MHz
PWR_OK			2	2.05	2.1	V
USB Interface						
V_{ON}	Static Output High	15K ± 5% Ohm to GND	2.8		3.6	V
V_{OFF}	Static Output Low	RUP is enabled			0.3	V
V_{DI}	Differential Input Sensitivity		0.2			V
V_{CM}	Differential Input Common Mode Range		0.8		2.5	V
V_{SE}	Single Ended Receiver Threshold		0.8		2	V
C_{IN}	Transceiver Capacitance				20	pF
I_{IO}	Hi-Z State Data Line Leakage	0V < V_{IN} < 3.3V	-10		10	mA

8-3 AC Electrical Characteristics

Table 8-3: AC Electrical Characteristics

Symbol	Description	Conditions	Min	Typ.	Max.	Unit
USB Driver						
T_{R1}	Transition Rise Time	CLOAD = 200 pF	75			ns
T_{R2}	Transition Rise Time	CLOAD = 600 pF			300	ns
T_{F1}	Transition Fall Time	CLOAD = 200 pF	75			ns
T_{F2}	Transition Fall Time	CLOAD = 600 pF			300	ns
T_R	Rise/Fall Time Matching		80		125	%
V_{CRS}	Output Signal Crossover Voltage		1.3		2.0	V
USB Data Timing						
T_{DRATE}	Low-speed Data Rate	Ave. Bit Rate (1.5 Mbps ± 1.5%)	1.4775		1.5225	Mbps
T_{DJR1}	Receiver Data Jitter Tolerance	To next transition	-75		75	ns
T_{DJR2}	Receiver Data Jitter Tolerance	To pair transition	-45		45	ns
T_{DEOP}	Differential to EOP Transition Skew		-40		100	ns
T_{EOPR1}	EOP Width at Receiver	Rejects as EOP			330	ns
T_{EOPR2}	EOP Width at Receiver	Accept as EOP	675			ns
T_{EOPT}	Source EOP Width		1.25		1.5	µs
T_{EOPT}	Source EOP Width		1.25		1.5	µs
T_{UDJ1}	Differential Driver Jitter	To next transition	-95		95	ns
T_{UDJ2}	Differential Driver Jitter	To pair transition	-95		95	ns
T_{LST}	Width of SE0 during Diff. Transition				210	ns

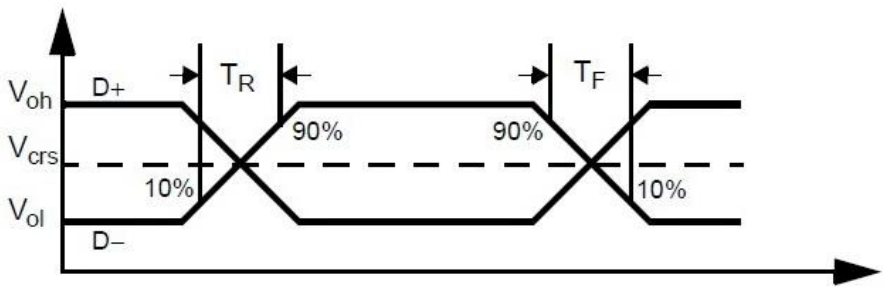


Figure 8-1: USB Data Signal Timing

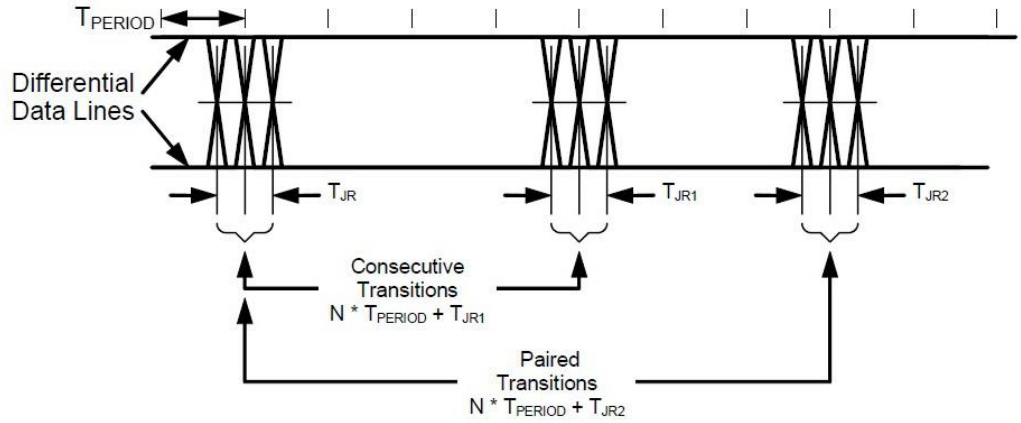


Figure 8-2: Receiver Jitter Tolerance

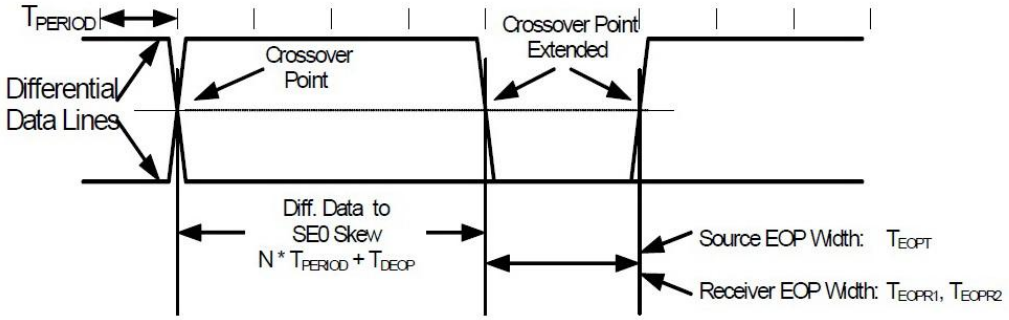


Figure 8-3: Differential to EOP Transition Skew and EOP Width

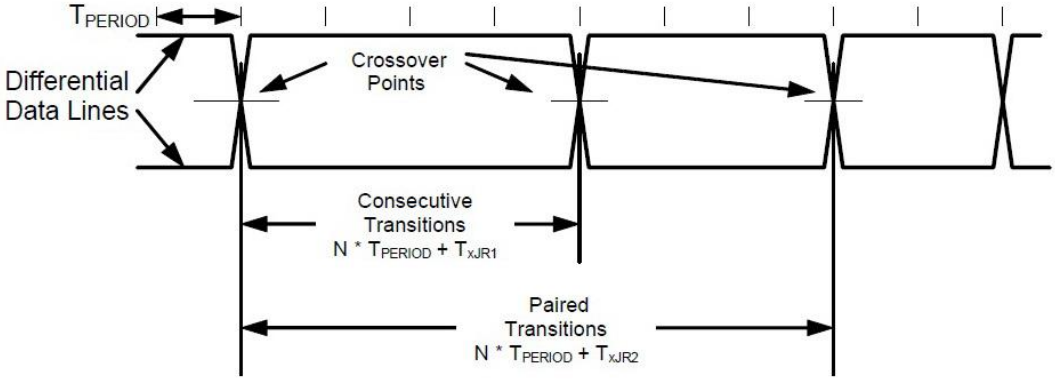


Figure 8-4: Differential Data Jitter

9. Package Dimensions

9-1 LQFP-48 Pin

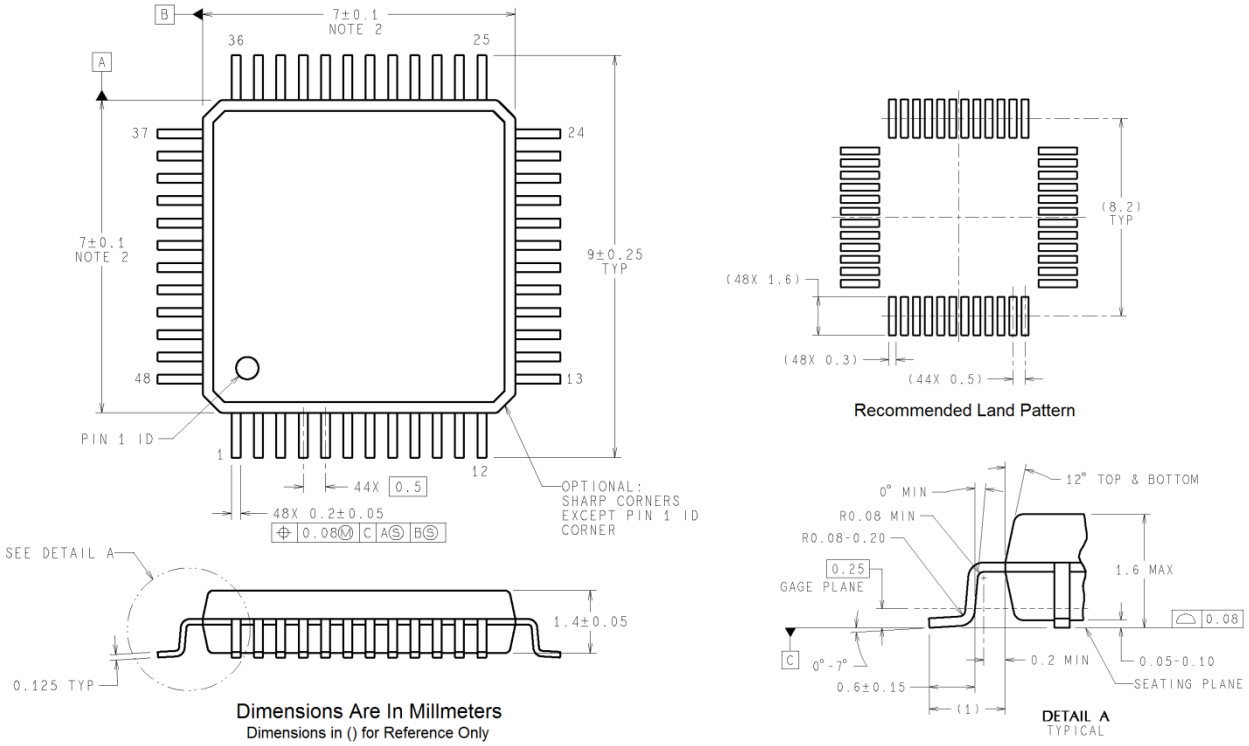


Figure 9-1: LQFP-48 Pin Package Dimension

Notes:

1. Dimenision does not include mold protrusion. Maximum allowable mold protrusion is 0.25mm per-side.
2. Reference JEDEC registration MS-026, variation BBC.

10. Application Circuits

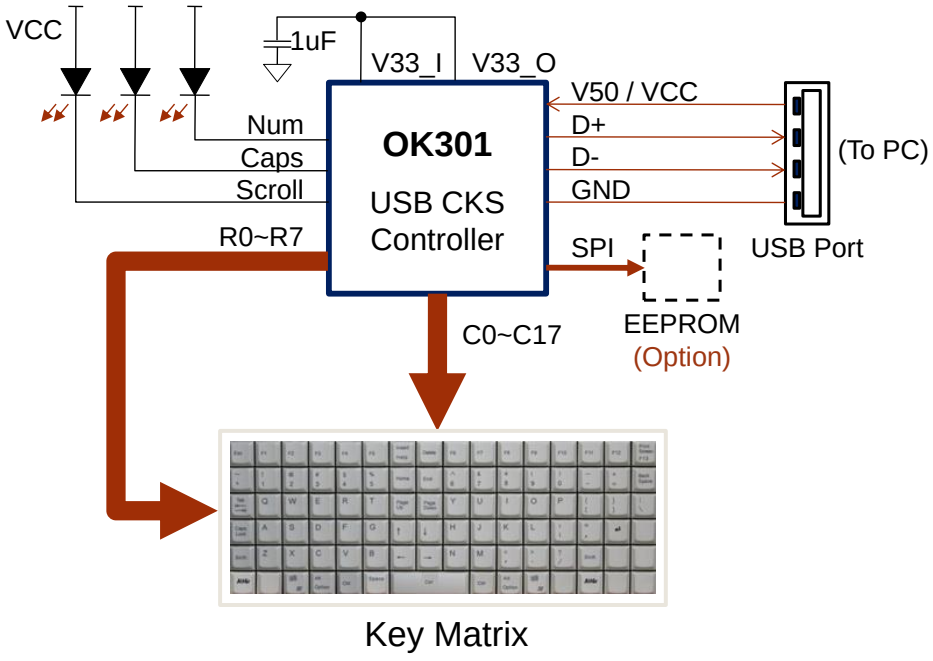


Figure 10-1: Application Block Diagram

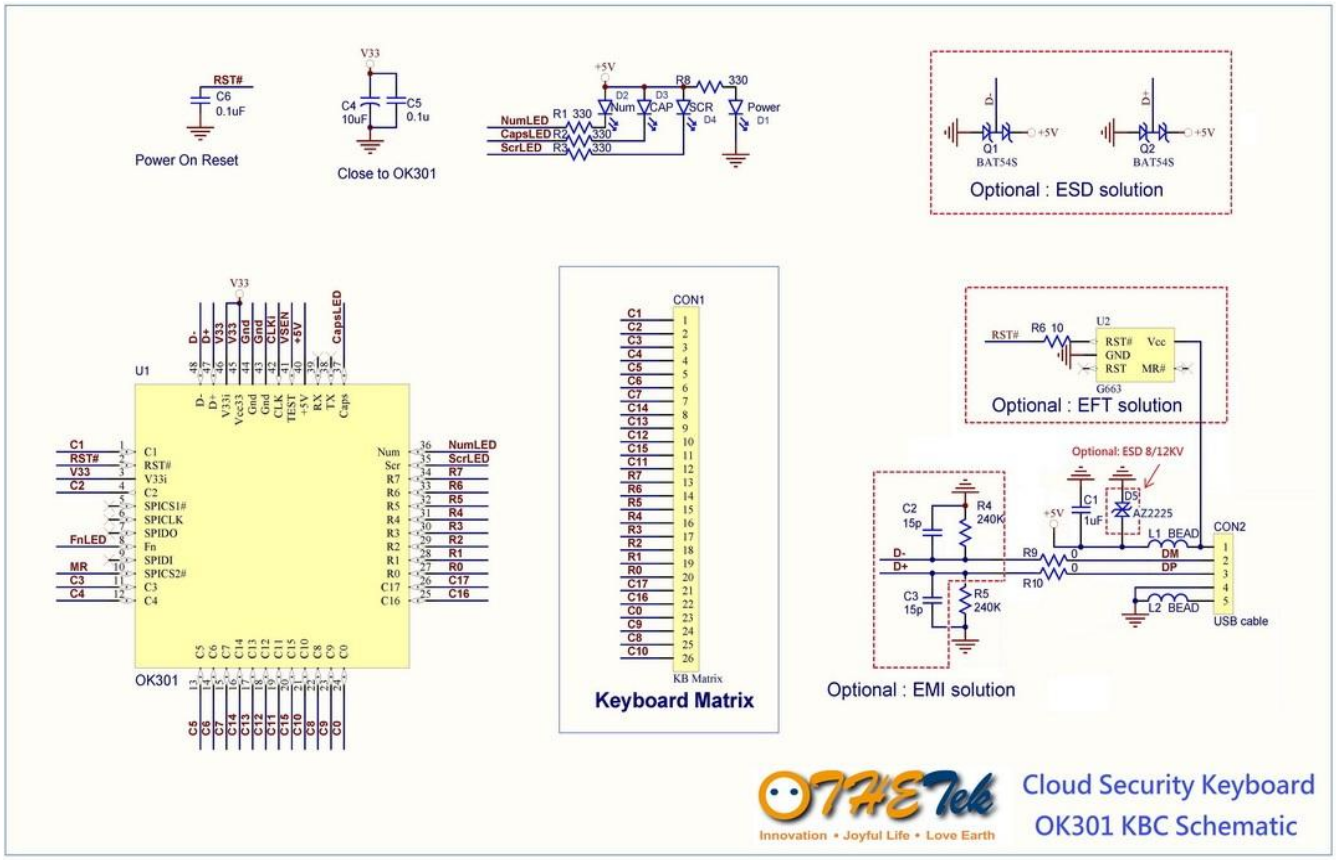


Figure 10-2: Application Circuit

Table 10-1: BOM List

	Part Type	Footprint	Description	Q'ty	Designator				
1	0Ω	RES 0603	0Ω SMD Resistor 0603±5%	2	R9	R10			
2	330Ω	RES 0603	330Ω SMD Resistor 0603±5%	3	R1	R2	R3	R8	
3	240KΩ	RES 0603	240KΩ SMD Resistor 0603±5%	1	R5				
4	0.1uF	CAP NPO 0603	0.1uF Capacitor 0603 NPO 50V	2	C5	C6			
5	1uF	CAP NPO 0603	1uF Capacitor 0603 NPO 50V	1	C1				
6	10uF	CAP NPO 0805	10uF Capacitor 0805 NPO 50V	1	C4				
7	FB 300	FB 300 Ω	Ferrite Bead 300Ω @ 100MHz 0805	2	L1	L2			
8	LED		Power, Num, Cap, Scr	4	D1	D2	D3	D4	
9	OK301	LQFP 48L	OK301 CKS Chip LQFP48L	1	U1				
EMI Options									
10	15P	CAP NPO 0603	15pF Capacitor 0603 NPO 50V	2	C2	C3			
11	240K	RES 0603	240KΩ SMD Resistor 0603±5%	1	R4				
ESD Options									
12	BAT54S			2	Q1	Q2			
13	AZ2225		(for ESD 8/12KV)	1	D5				
EFT Options									
14	10Ω	RES 0603	10Ω SMD Resistor 0603±5%	1	R6				
15	G663	SOT-23-5	Reset chip	1	U2				

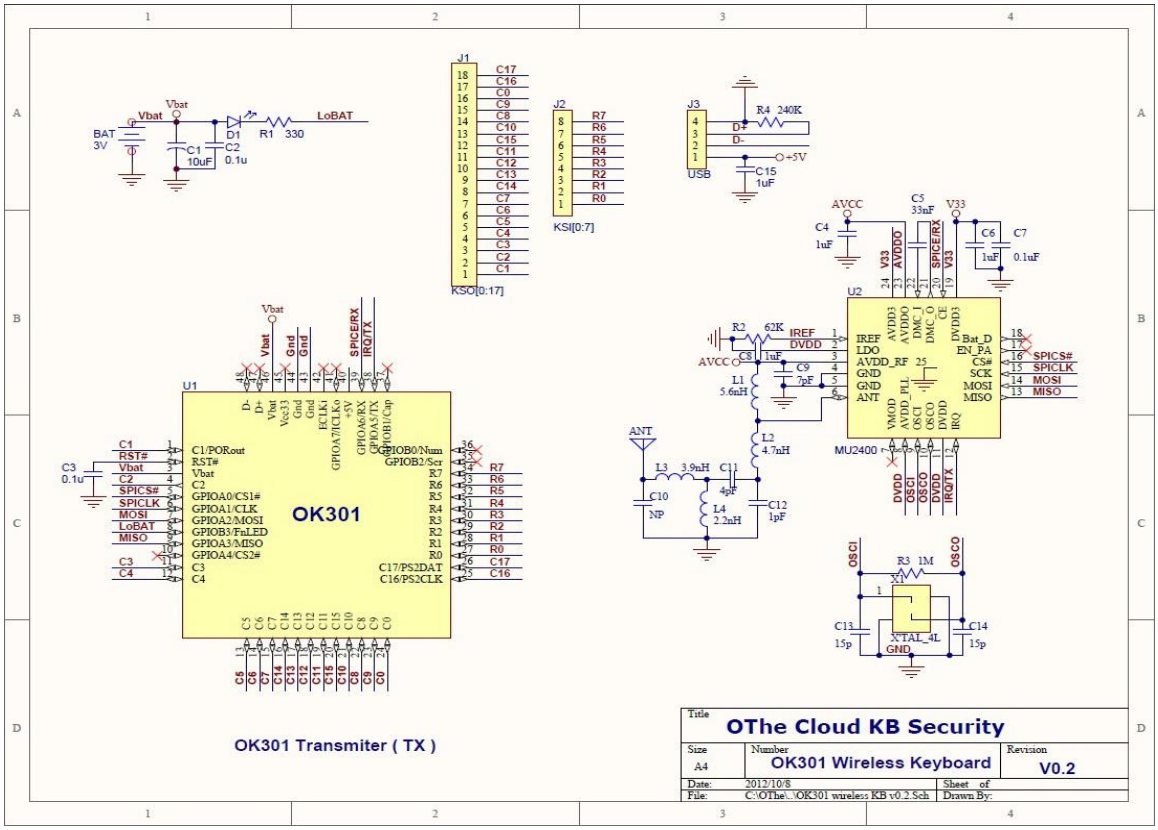


Figure 10-3 : RF Keyboard Application Circuit

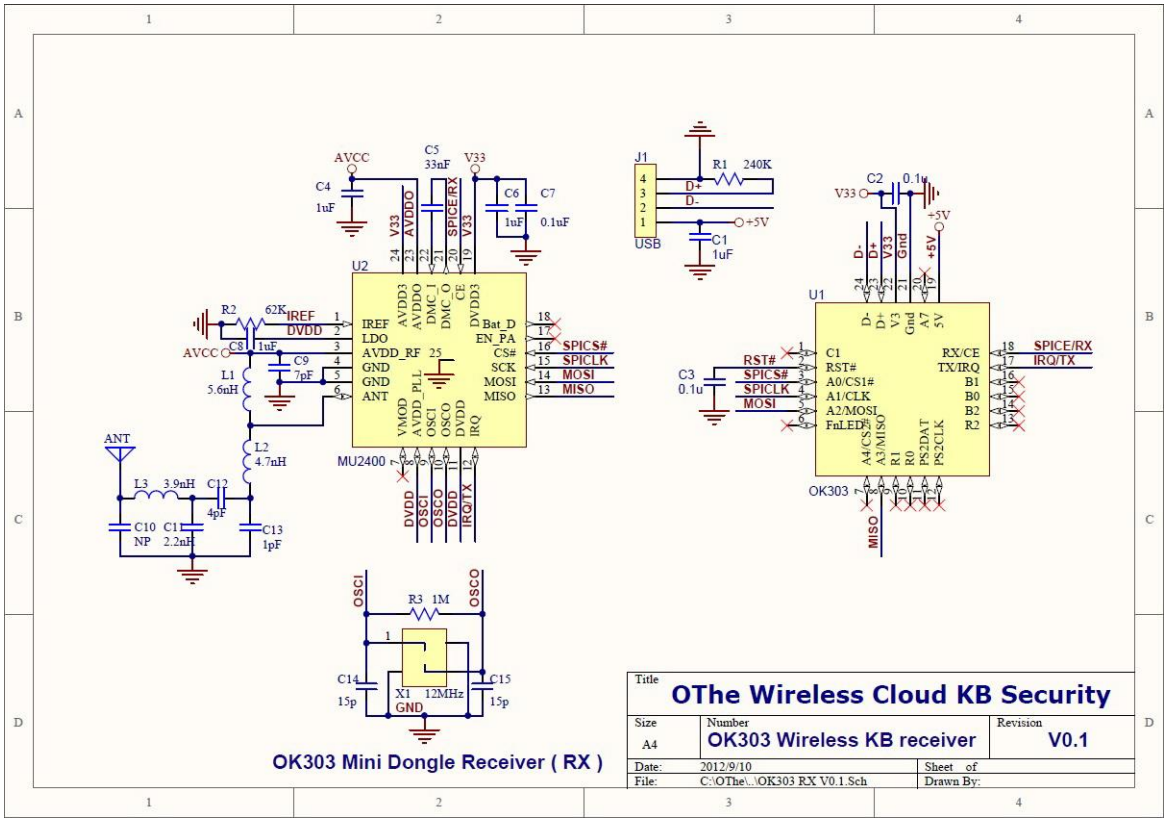


Figure 10-4 : RF Keyboard(Receiver) Application Circuit

About oTHE

oTHE Technology Inc. was founded on August of 2008 located in Hsinchu City, Taiwan by over 15 years experienced RD and Marketing team from Hsinchu Science Park. oTHE team had successful experience and related background specialized in the field of PC related chips. oTHE is a leading and professional IC design company which decided to provide high quality, high performance and high value products and services. oTHE has extensive experience developing computer industry component, especially in PC keyboard controller, keyboard security, security information system and optics.

oTHE's symbol is the smile face, and the core meaning is joy employee provide well service to customer and then create profit to company, and next the profitable enterprise contribute source to society. Our Company slogan: Innovation, Joyful Life, Love Earth. For further information about oTHE, please contact us at http://www.othe.com.tw.

Innovation • Joyful Life • Love Earth

OTHE TECHNOLOGY INC.

Headquarter:

4F., No.5, Xin'an Rd., Science Park., Hsinchu City 30076, Taiwan
Tel: +886-666-8690
http://www.othe.com.tw