EXPLIOT
www.expliot.io

Attacking Hardware

Introduction to I2C Protocol

Copyright © 2021 EXPLIoT - www.expliot.io

I2C Protocol

- It stands for inter integrated circuit and requires only two wires connecting all peripherals to microcontroller. i.e. SDA (serial data line) and SCL (serial clock line).
- Multiple master, multiple slaves
- It’s a master to slave type communication having unique addresses for each slaves.
- I2C is synchronous and bidirectional communication.
- Developed by Philips Semiconductor(now NXP Semiconductors)
- Half-duplex

Copyright © 2021 EXPLIoT - www.expliot.io

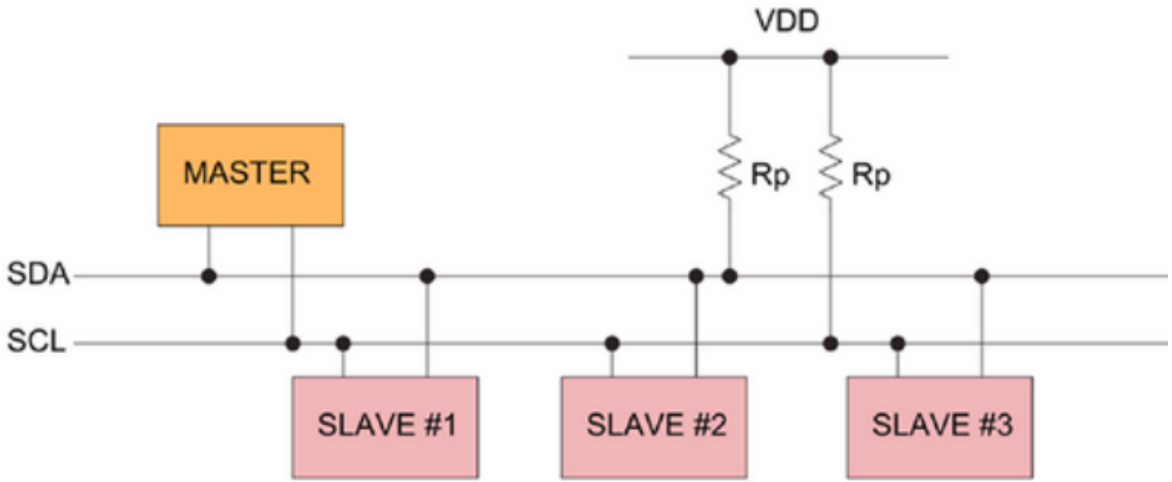
I2C Protocol

- Bidirectional open-collector lines pulled up with resistors
- Crosstalk takes place between SDA and SCL and can be prevented by increasing the serial resistors Rs and termination Rp. Or by keeping short interconnections.
- Supported speed : 100 kbit/s standard mode, 400 kbit/s fast mode, 1 Mbit/s fast mode plus, 3.4 Mbit/s high-speed mode, and unidirectional 5 Mbit/s ultra fast-mode

Copyright © 2021 EXPLIoT - www.expliot.io

I2C Protocol

- Master nodes
- Slave nodes

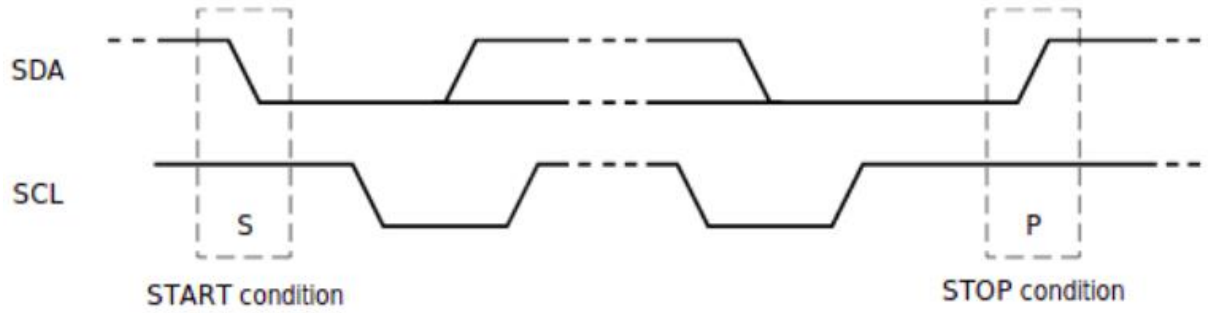


Source - https://www.analog.com/en/technical-articles/i2c-primer-what-is-i2c-part-1.html#

Copyright © 2021 EXPLIoT - www.expliot.io

I2C Protocol

- Each slave has unique address
- No. of nodes depends on address space (7-bit or 10-bit) and bus capacitance (400 pF)
- START and STOP bits apart from data bits

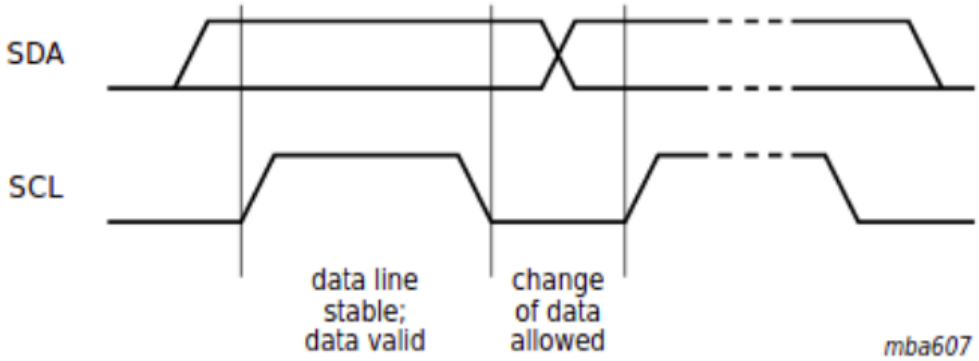


Source : https://www.nxp.com/docs/en/user-guide/UM10204.pdf

Copyright © 2021 EXPLIoT - www.expliot.io

I2C Protocol

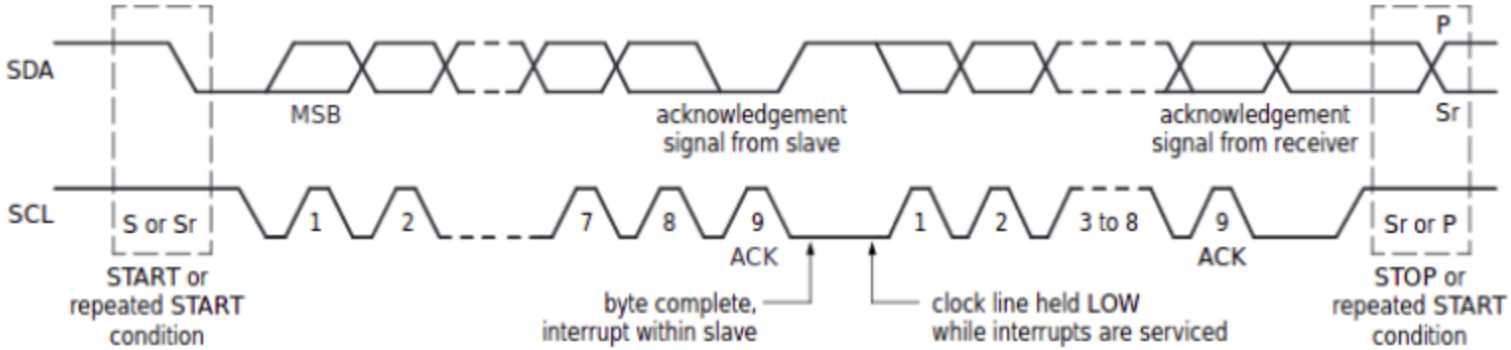
- The size of transmitted data frame - 8 bits
- During transferring, the data is put on the SDA line after SCL is pulled low



Source : https://www.nxp.com/docs/en/user-guide/UM10204.pdf

Copyright © 2021 EXPLIoT - www.expliot.io

I2C Protocol



Source : https://www.nxp.com/docs/en/user-guide/UM10204.pdf

Copyright © 2021 EXPLIoT - www.expliot.io

I2C Protocol

- Clock synchronization and arbitration
- Clock stretching

Source : https://www.nxp.com/docs/en/user-guide/UM10204.pdf

Copyright © 2021 EXPLIoT - www.expliot.io

I2C - Possible Attacks

- Signal sniffing
- Signal manipulation
- Data extraction
- Data manipulation
- Clock glitching (Research:

  https://www.researchgate.net/publication/314629854_Hardware_Attacks_on_Mobile_Robots_I2C_Clock_Attacking)

Copyright © 2021 EXPLIoT - www.expliot.io

I2C - Tools/Framework

- EXPLIoT Nano - https://expliot.io/products/expliot-nano
- Bus Pirate - http://dangerousprototypes.com/docs/Bus_Pirate
- Shikra - https://int3.cc/products/the-shikra
- CH341A - https://www.onetransistor.eu/2017/08/ch341a-mini-programmer-schematic.html
- EXPLIoT Framework - https://gitlab.com/expliot_framework/expliot
- Pyi2cflash - https://github.com/eblot/pyi2cflash
- Logic Analyzer
- RaspberryPi or Beaglebone can also be used.

Copyright © 2021 EXPLIoT - www.expliot.io

Labs

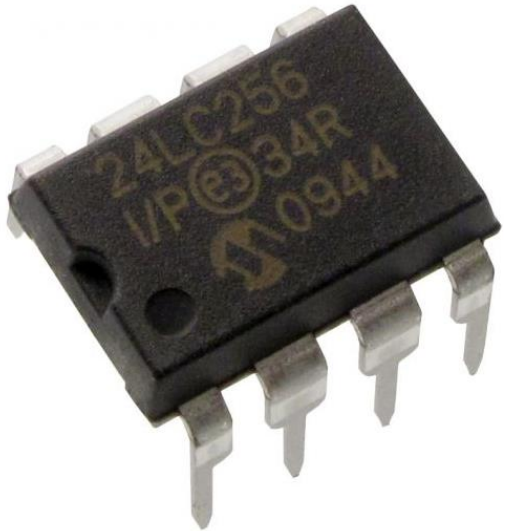
Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 1 – I2C chip recon

Objective: To perform reconnaissance on Microchip 24LC256 EEPROM using datasheet

Location: <course-dir>/labs/device-i2c-lab-1

Datasheet can be found in this directory

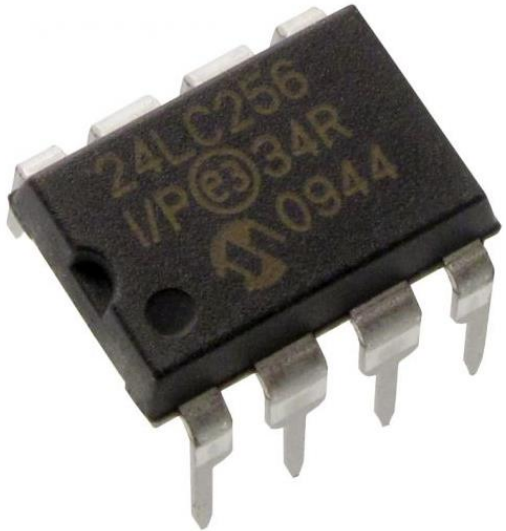


Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 1 – I2C chip recon

Steps

- Identify the size
- Identify the clock frequency
- Identify the Pin specifications
- Identify the slave address
- Understand the commands



Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 1 – I2C chip recon

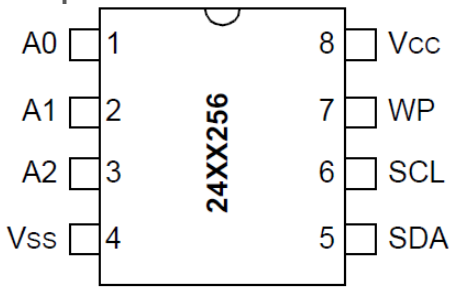
- The address input pins, A0, A1, and A2, are for multiple device operation
- There are 3 address, which means there can be a total of 8 EEPROM
- devices connected together to a microcontroller
- The WP pin, pin 7, is the Write-Protect pin.
- If tied to HIGH or VCC, write operations are inhibited. Read operations,however, are not affected. If tied LOW or to VSS,

  write operations are enabled.

Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 1

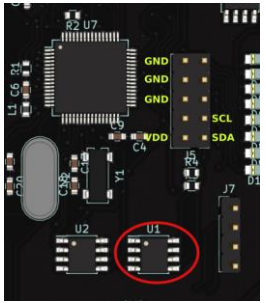
- Pin 6 is the serial clock line. The clock is used to synchronize data transfer to and from the device between the microcontroller and the EEPROM chip.
- Pin 5 is the serial data pin. This is the pin that transfers data between the micrcontroller and the EEPROM chip. It's bidirectional.



Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 2 – I2C communication sniffing to bypass authentication

- Objective – I2C communication sniffing using Logic analyzer to bypass auth
- Location: <course-dir>/labs/device-i2c-lab-1
- Datasheet can be found in this directory
- The circled one is I2C memory
- It’s a dual in-line package (DIP)



Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 2 – Contd.

- On connecting Logic analyser and DIVA with proper input,this is how you screen should look like. Enter .h for help and .l to list the challenges, in the DIVA prompt

```
Diva 2.0
Enter ".l" for challenges ".h" for help
diva>.l
List of challenges
  1 LED
  2 I2C
  3 SPI
  4 UART
  5 ZigBee
  6 JTAG
  7 Hardcoded password
Choose the challenge number to run?
```

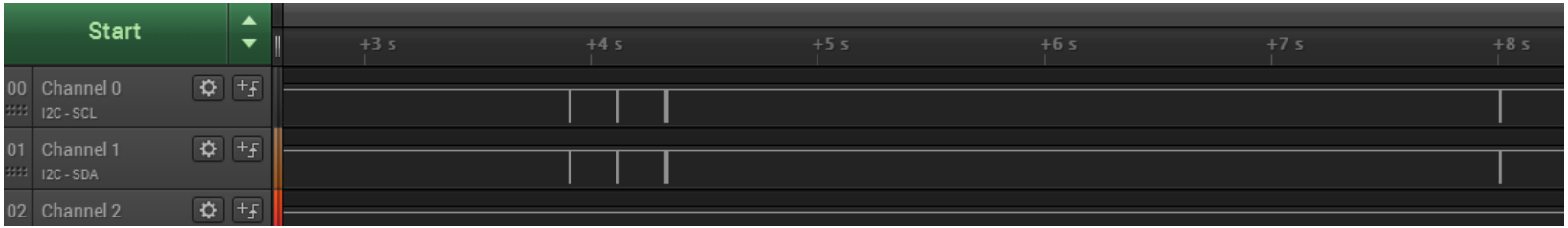

Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 2 – Contd.

- On the Logic software, click on analysers and set as I2C with correct channel, click on the double arrow and set speed as 24MS/s
- Click on start and go back to the serial monitor
- Press 2 (for I2C challenge) and type a random password when asked
- ‘Go back to logic software and click on **stop**
- Save the sniffed data by clicking on double arrow near capture

Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 2 – Contd.



Copyright © 2021 EXPLIoT - www.expliot.io

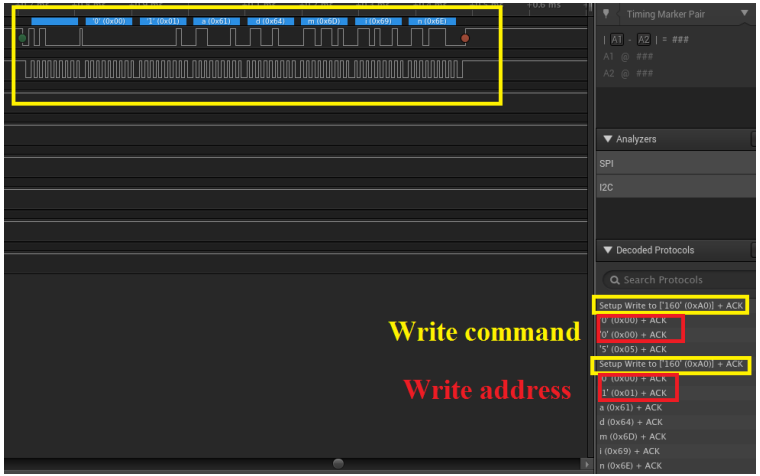
I2C Lab 2 – Contd.

```
Choose the challenge number to run?
diva>2
Welcome to I2C sniffing Lab

In this Lab you will sniff an I2C transaction

Please login
Enter the password
diva>>****
Access Denied :(
diva>
```


Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 2 – Contd.

- **Sniffed data**
- **Transferred during authentication process**
- Analyse the data and see if it helps you in any way



Copyright © 2021 EXPLIoT - www.expliot.io

I2C Lab 3 - I2C chip memory dumping

- **Objective** – I2C chip memory dump using Expliot Nano
- Find the I2C Line in the Diva board and connect it to expliot nano
- Open expliot framework
- To extract data from I2C eeprom, type following command run i2c.generic.readeeprom -c <chipname -w <filename>

```
ef> run i2c.generic.readeeprom -c 24AA256
[*] Test:         i2c.generic.readeeprom
[*] Author:       Aseem Jakhar
[*] Author Email: aseemjakhar@gmail.com
[*] Reference(s): ['https://github.com/eblot/pyi2cflash']
[*] Category:     Protocol=i2c|Interface=hardware|Action=analysis
[*] Target:       Name=generic|Version=generic|Vendor=generic
[*]
[*] Reading data from i2c eeprom at address(0) using device(ftdi:///1)
[+] (chip size=32768 bytes)
[?] Reading 32768 bytes from start address 0
Read @ 0x0000
[+] (data=['0x61', '0x64', '0x6d', '0x69', '0x6e', '0x0', '0xff', '0xff', '0xff',
f', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff
xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0x
'0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff', '0xff',
```


Copyright © 2021 EXPLIoT - www.expliot.io

The End

Copyright © 2021 EXPLIoT - www.expliot.io