Hardware security multidimensional attack and defense tool set

Jie Fu

Kunzhe Chai

Mingchuang Qin

From—360 Hacker Research Institute, 360 Security Technology

HACKNOWN

BUILD LEGENDS FOR THE FUTURE

Abstract

- Hardware attack and defense tools.
- Master and implement a variety of hardware attack methods.
- Includes ultrasonic attacks, RFID attacks, power side channel attacks, and radio defense etc.
- Design idea, design concept

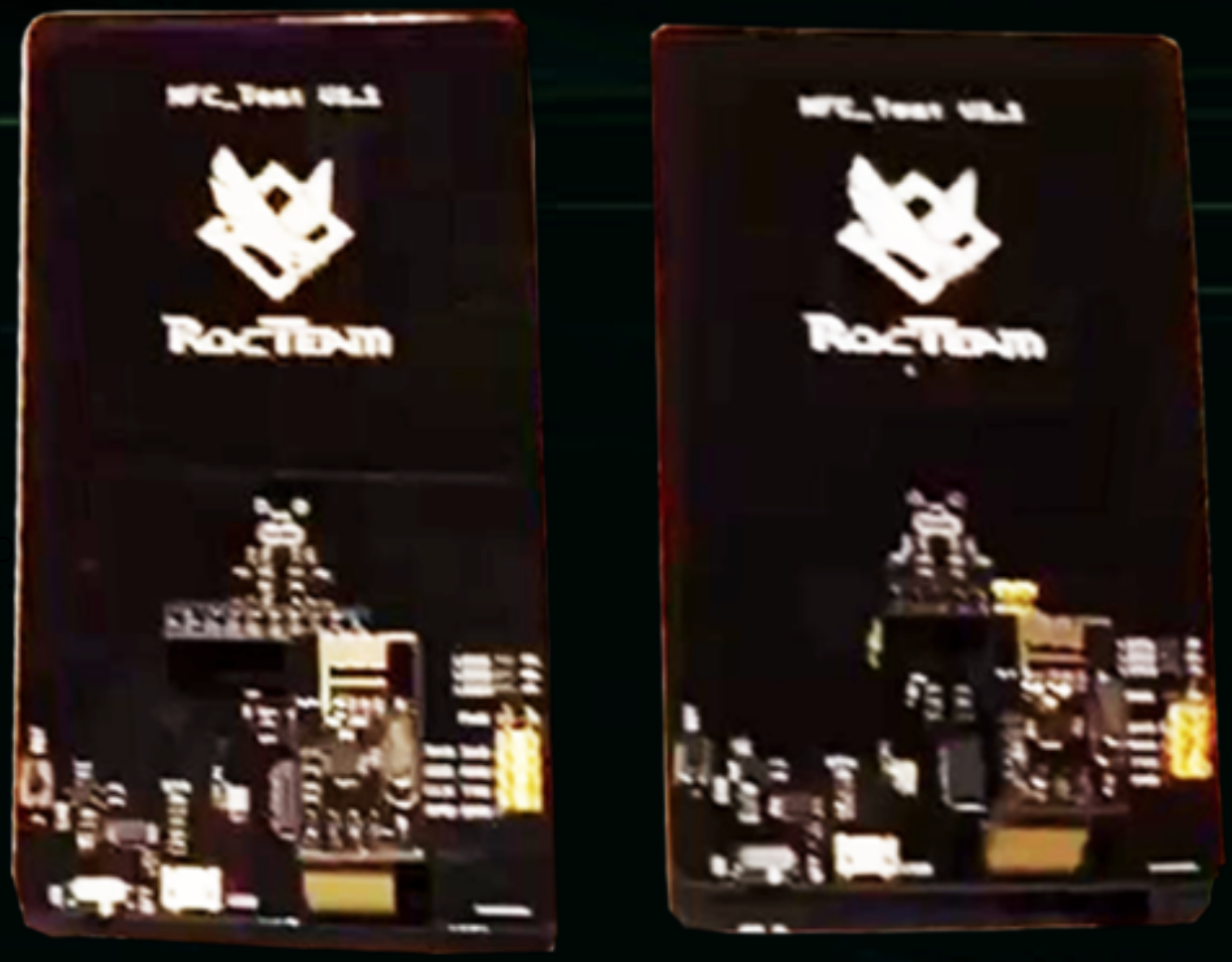
High frequency card reader and high frequency simulator

- proxmark3
- ChameleonMini
- HackNFC — designed by 360 Unicornteam


360UNICORNTEAM
RocTeam
RocTeam
3

HACKNFC

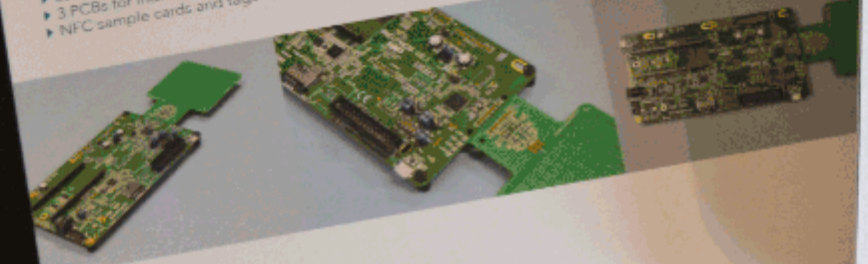
- Man in the NFC
- Chip — PN7462
- Protocol—14443A
- NRF24L01



PN7462 Controller Development Kit
OM27462CDK

PN7462 is the **first all-in-one full NFC controller solution.**
The respective development kit (OM27462CDK) contains:

- PNEV7462B with standard 65x65mm antenna
- 30x50mm antenna with matching components
- 3 PCBs for individual antenna matching
- NFC sample cards and tags
- 2 USB cables (A to mini and micro)
- 10 PN7462 samples
- Quick start guide
- OM13054 LPC-Link2 debug adapter



nfc everywhere
CONTROLLER SOLUTIONS

PN7462 Controller Development Kit
OM27462CDK Quick Start Guide

NXP

This kit ensures an easy and quick development of NFC applications running on the PN7462, PN7362, or PN7360. It contains:

- PNEV7462B with standard 65x65mm antenna
- 30x50mm antenna with matching components
- 3 PCBs for individual antenna matching
- NFC sample cards and tags
- 2 USB cables
- 10 PN7462 samples
- 7.5 VDC power supply
- OM13054 LPC-Link2 debug adapter

This kit is part of an extensive product support package. It demonstrate all functionalities of the PN7462 family and eases the development of customized applications as well as the antenna design.
All documentation, video tutorials and software libraries can be downloaded from the product page:

www.nxp.com/products/PN7462AUHN

1. Setting up the development board

The *UM10883 PN7462 Quick Start Guide - Customer Board* provides instructions on:

- How to connect the development board
- How to download the LPX Expresso environment
- How to manage various projects and examples in the development environment

2. Executing software examples

A collection of software examples shows how to integrate the NFC, contact card and USB interface for the PN7462 family:

- PC CCID reader: working with NFC, CT and USB *UM10915 PN7462 PC CCID Reader User Manual*
- Access reader: working with DESFire and MIFARE, with or without a SAM *UM10957 PN7462 Door Access User Manual*

3. Starting custom development

The *UM10913 - PN7462 Software User Manual* describes the software architecture and all components to successfully create fully customized projects.

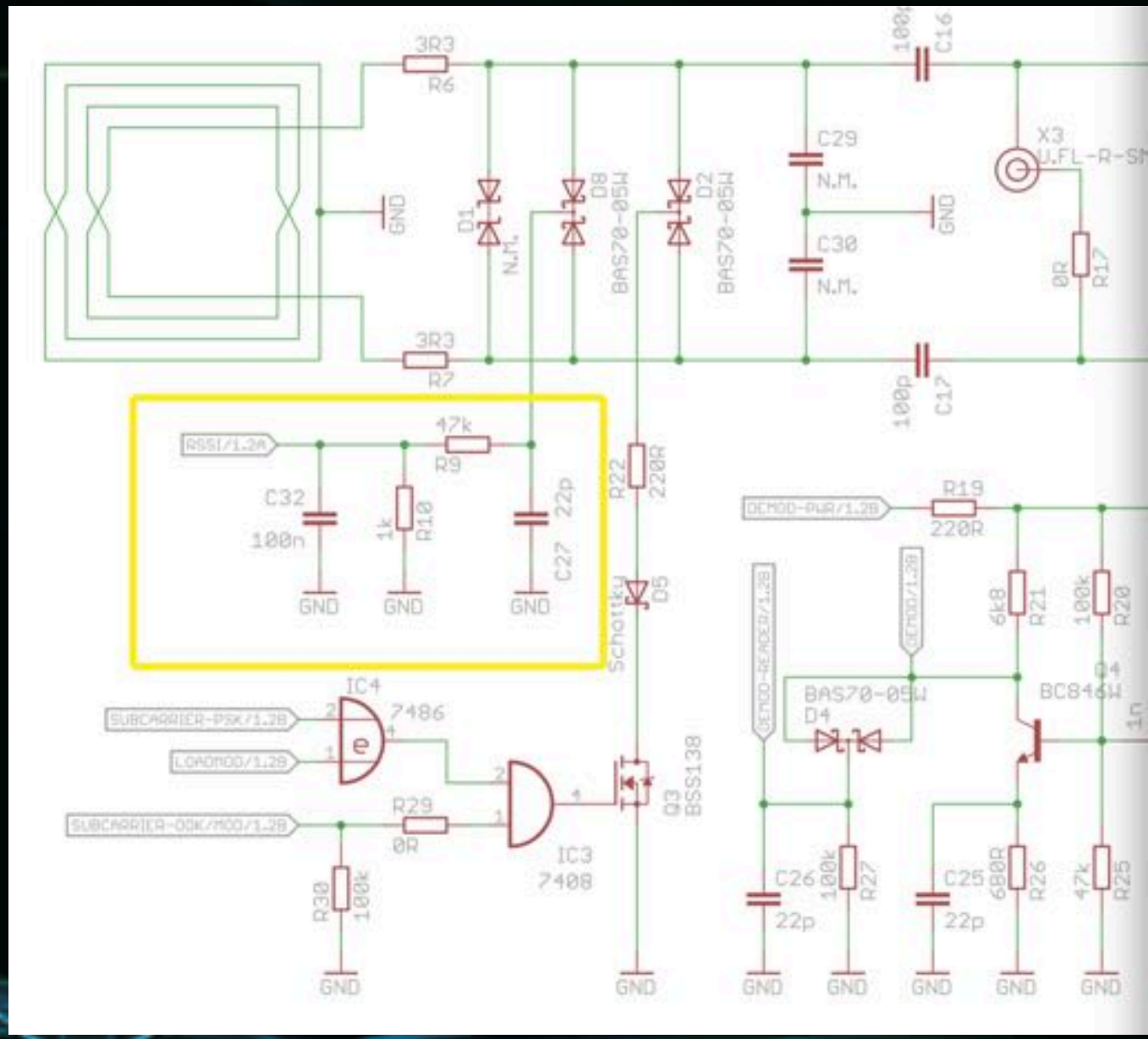
nfc everywhere
CONTROLLER SOLUTIONS

For additional information please visit: www.nxp.com/demoboard/OM27462CDK

ChameleonMini — how to emulate a mifare card

Why there is an error in the original SCH?

- Hardware Bug?
- Parameter adjustment
- The values in yellow are wrong



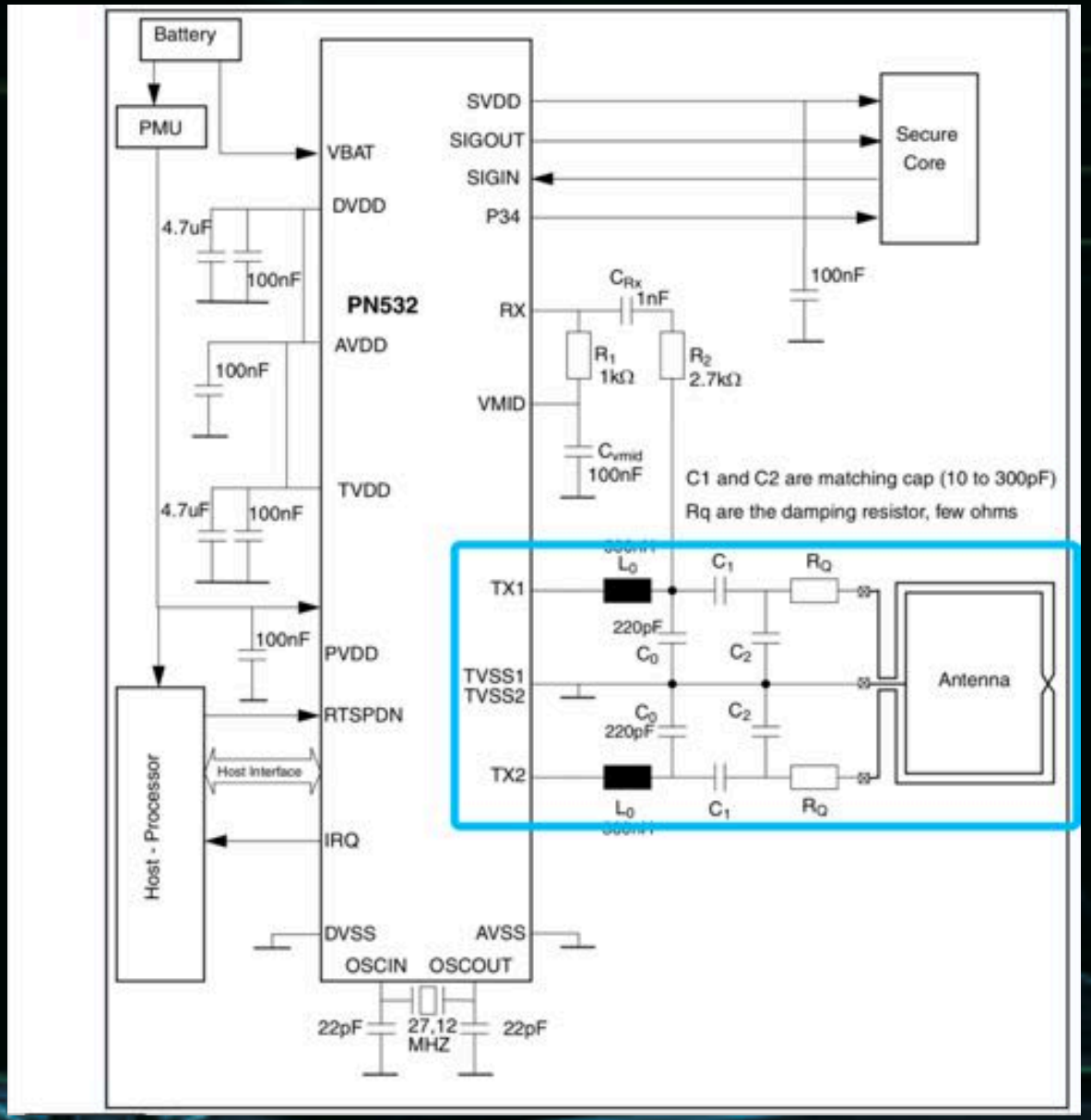
How to design a NFC hack tool ?

- How to design more concealed
- How to get a long distance
- What features do you want


秒拍
RocTeam

How to achieve a long reading distance?

- PN532
- Demodulation circuit



How to achieve a long reading distance?

- MFRC522
- Demodulation circuit

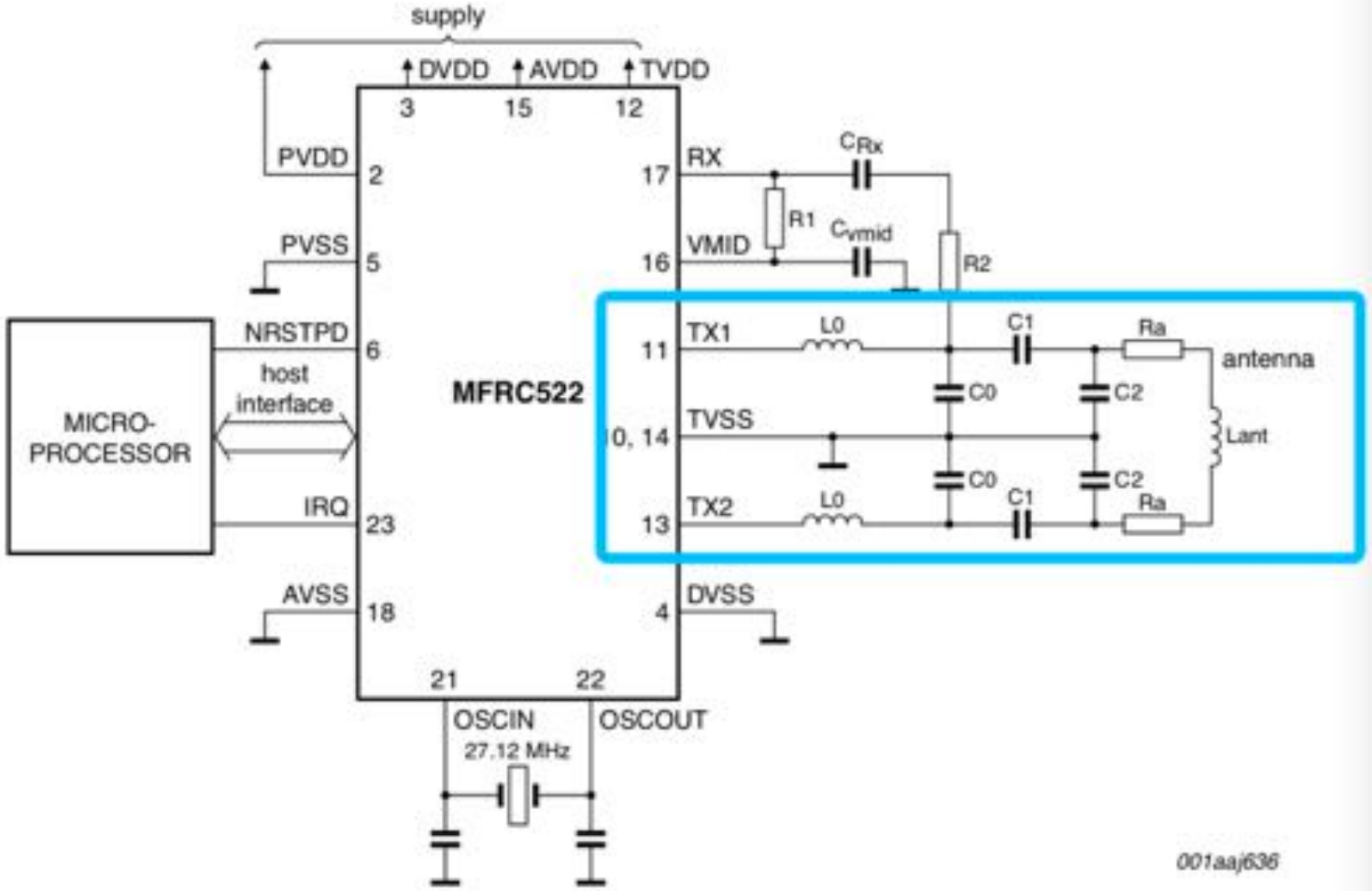


Fig 27. Typical application diagram

How to achieve a long reading distance?

- Chip — CLRC663
- General method
- Current monitoring

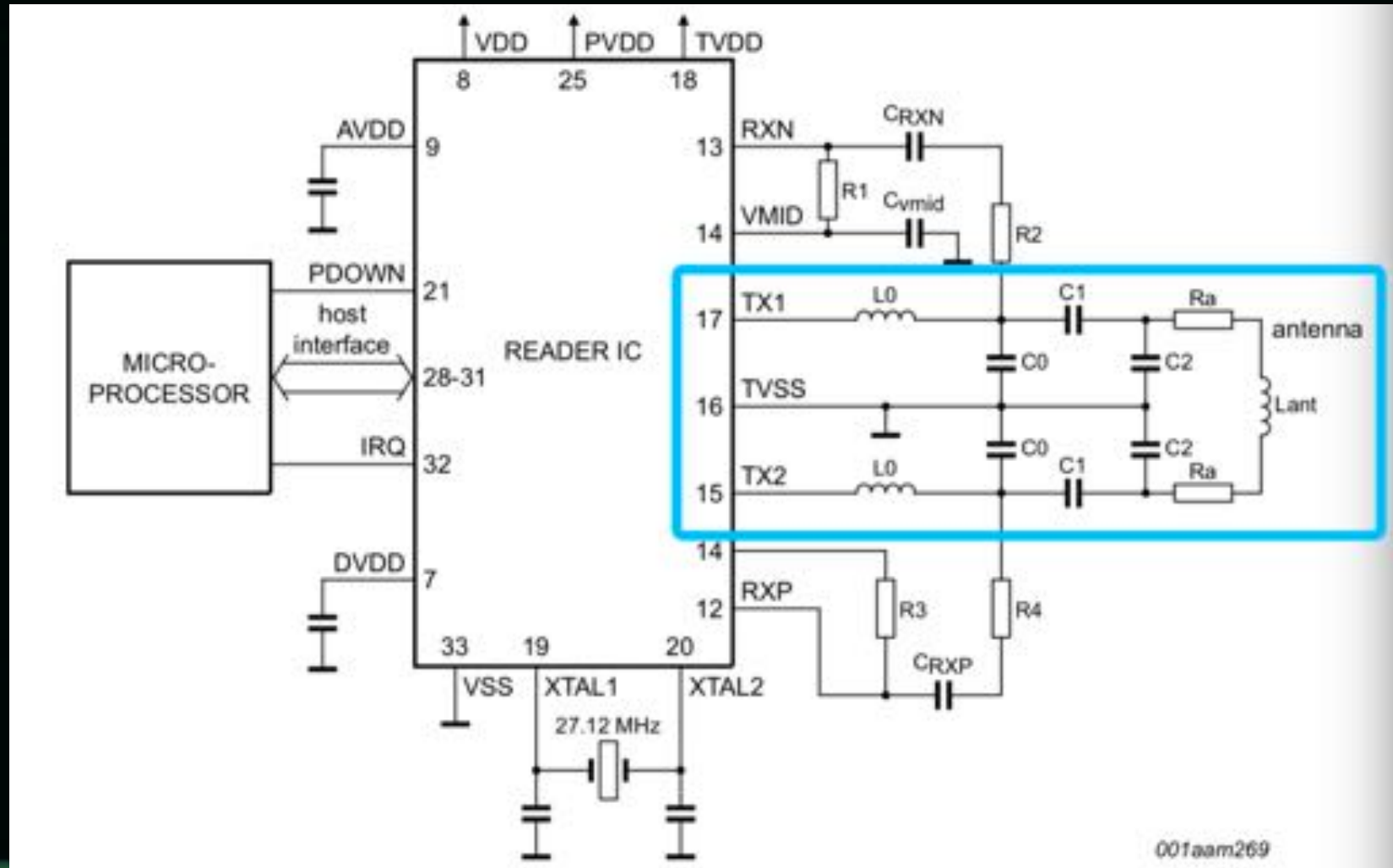


Figure 36. Typical application antenna circuit diagram

How to achieve a long reading distance?

- Current monitoring : 70mA - 100mA

Table 1. Quick reference data CLRC66301HN and CLRC66302HN

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
V_{DD}	supply voltage			3.0	5.0	5.5	V
$V_{DD(PVDD)}$	PVDD supply voltage		[1]	3.0	5.0	V_{DD}	V
$V_{DD(TVDD)}$	TVDD supply voltage			3.0	5.0	5.5	V
I_{pd}	power-down current	PDOWN pin pulled HIGH	[2]	-	8	40	nA
I_{DD}	supply current			-	17	20	mA
$I_{DD(TVDD)}$	TVDD supply current			-	100	250	mA
T_{amb}	operating ambient temperature			-25	+25	+85	°C
T_{stg}	storage temperature	no supply voltage applied		-55	+25	+125	°C

[1] VDD(PVDD) must always be the same or lower voltage than VDD.
[2] I_{pd} is the sum of all supply currents

How to achieve a long reading distance?

- Chip — CLRC663
- General method
- Current monitoring
- Optimize parameters

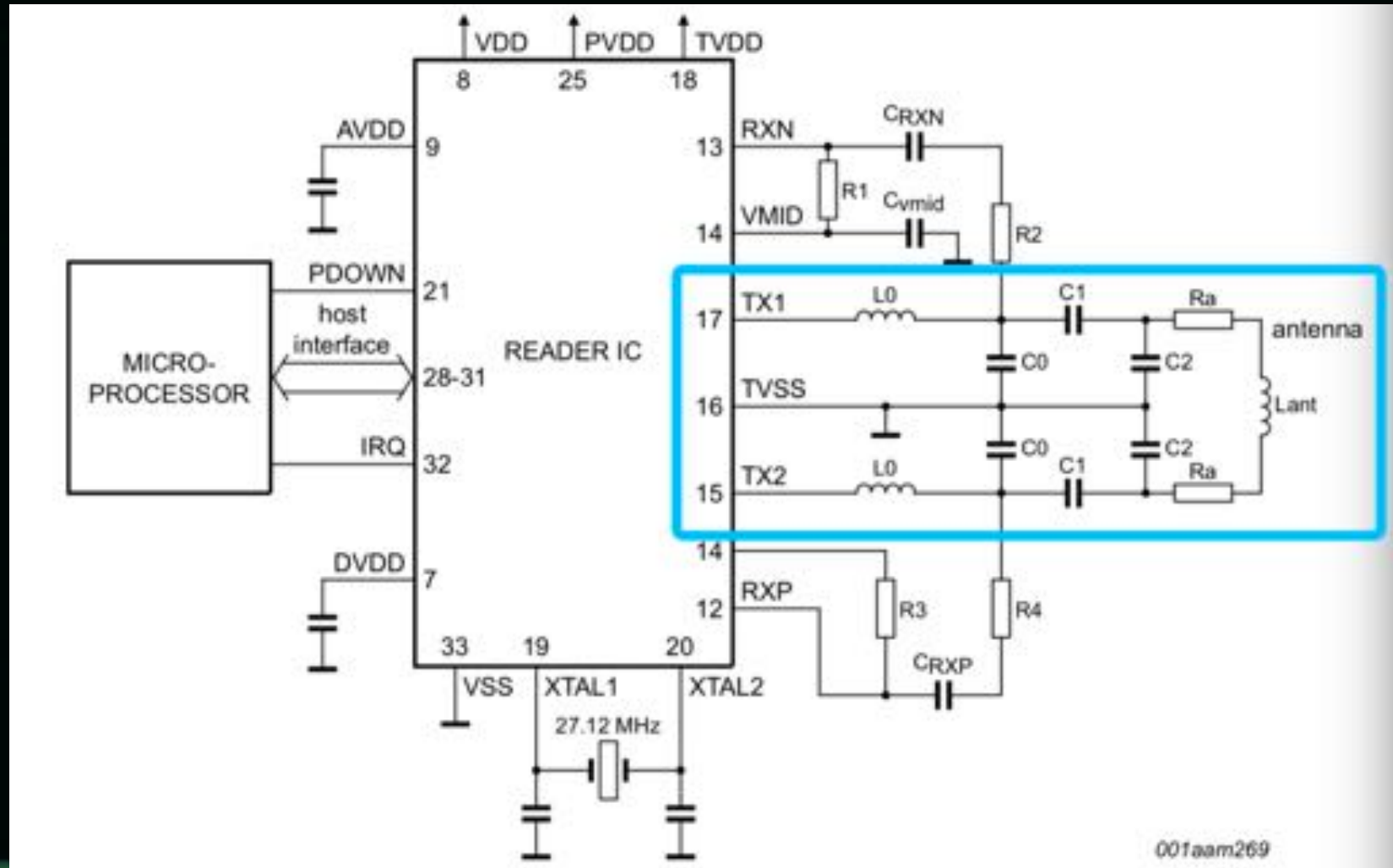
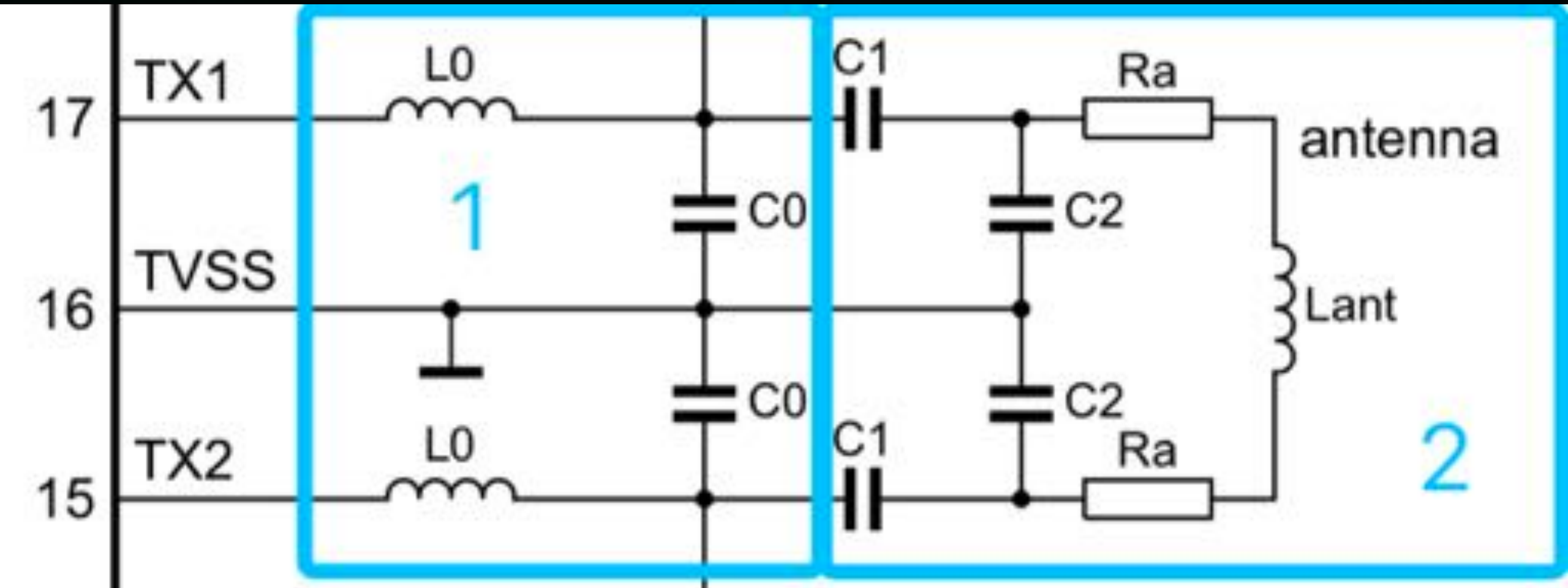


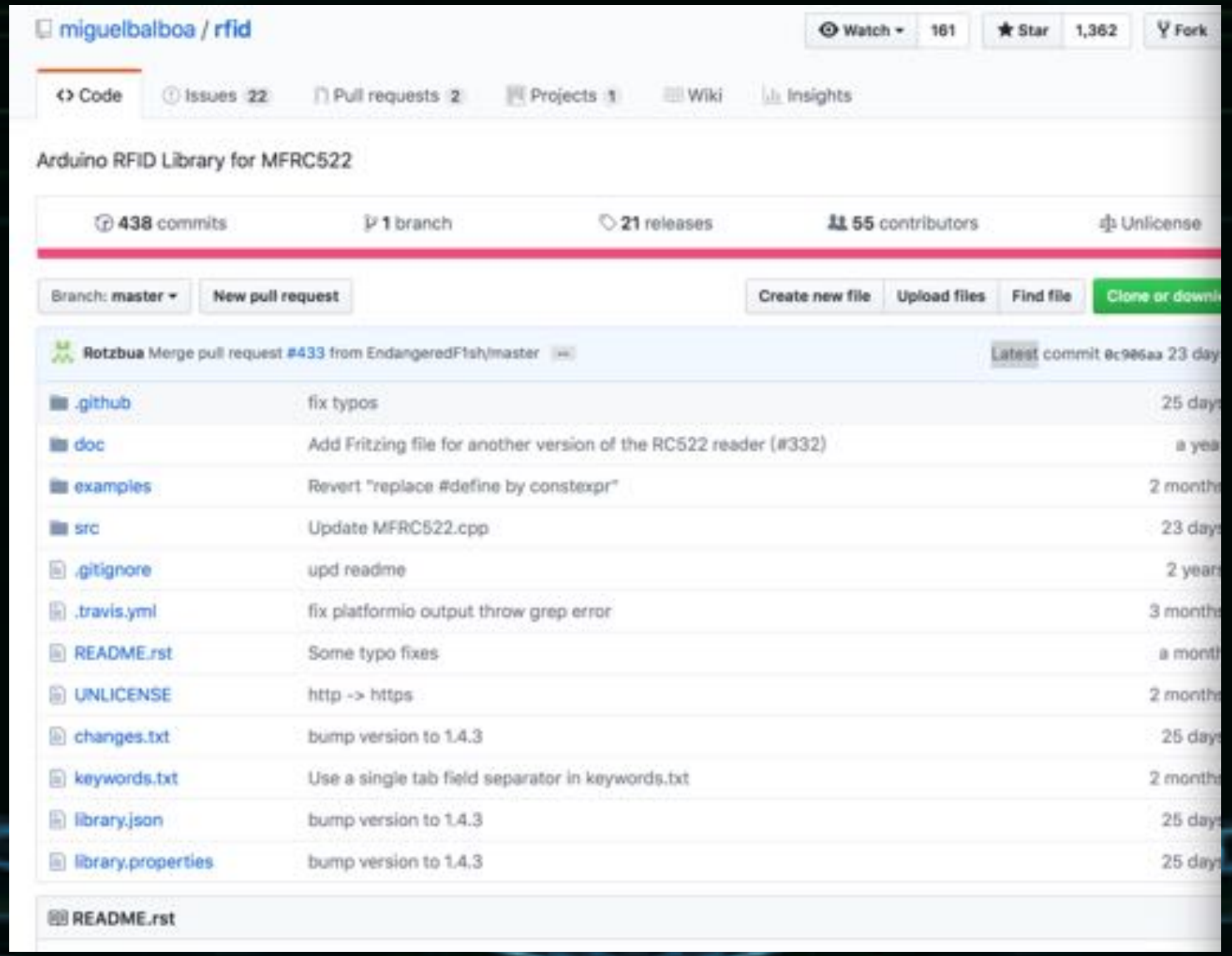
Figure 36. Typical application antenna circuit diagram

How to achieve a long reading distance?

- Remain L0, C0; Change C1, C2
- Antenna value 1uH - 2uH



Simple Arduino Reader



How to make the tool by yourself ?

- Electronic circuit design software ——EAGLE , Alitum Designer

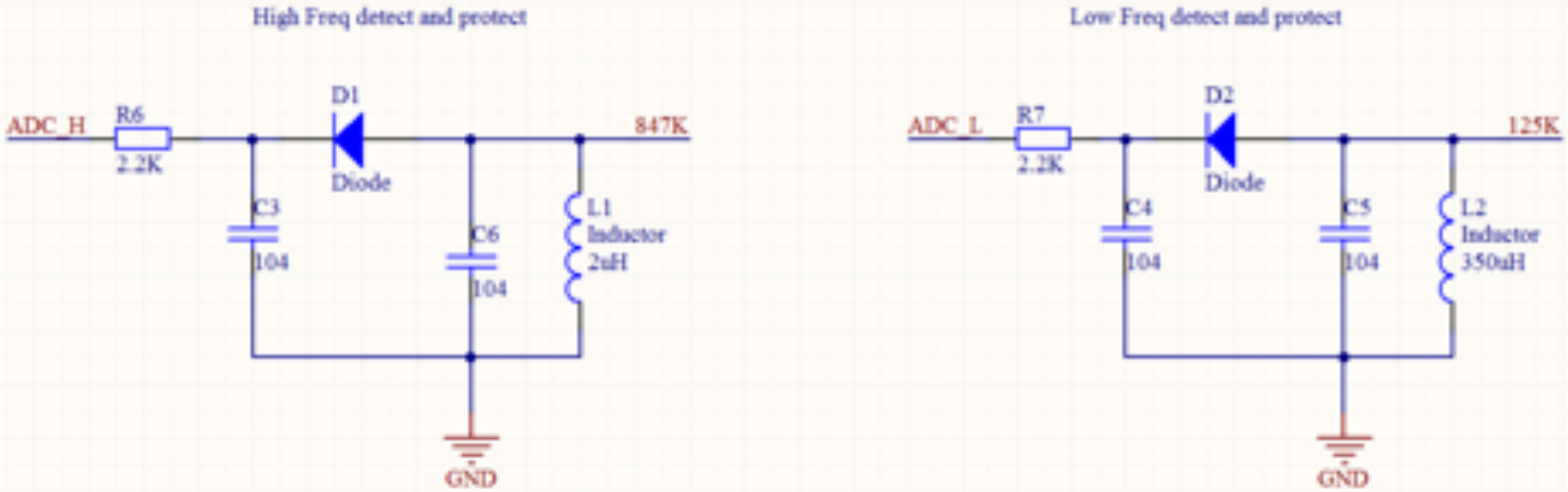
NFC defender and 125Khz defender

- How to block NFC communication


360卡防
NFC卡片信息防护
招商银行
CHINA MERCHANTS BANK
信用卡
Credit Card
http://www.8008205555.com

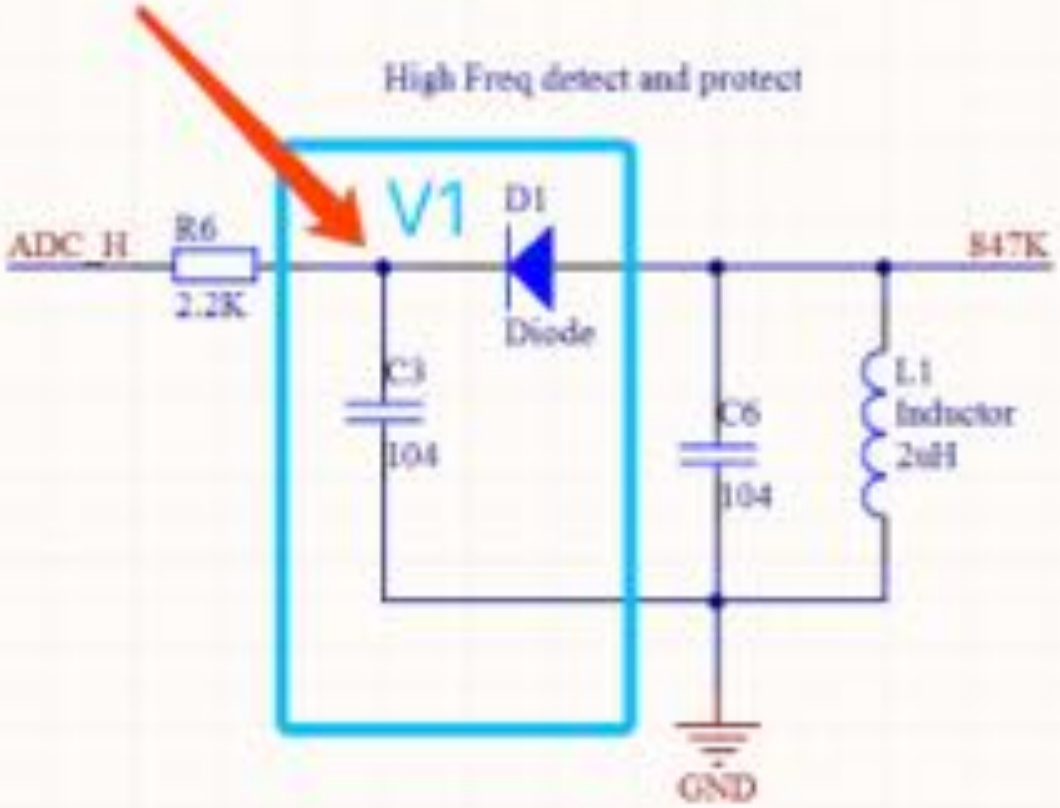
NFC defender and 125KHz defender

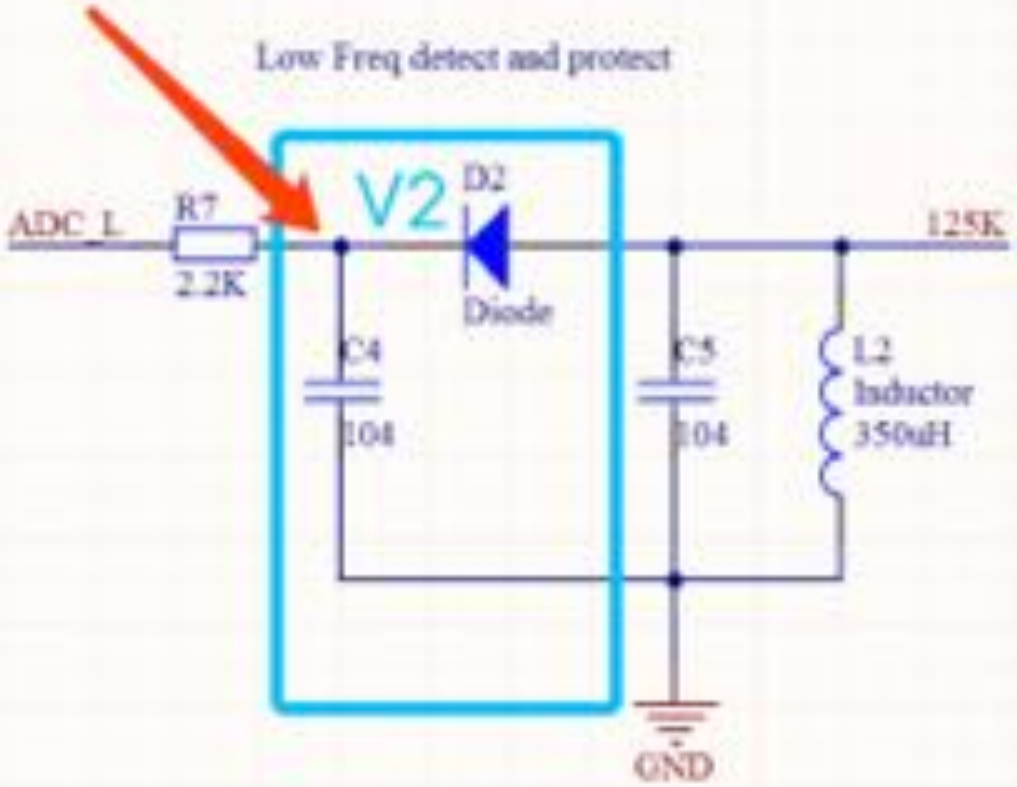
- Detect and protect



NFC defender and 125KHz defender

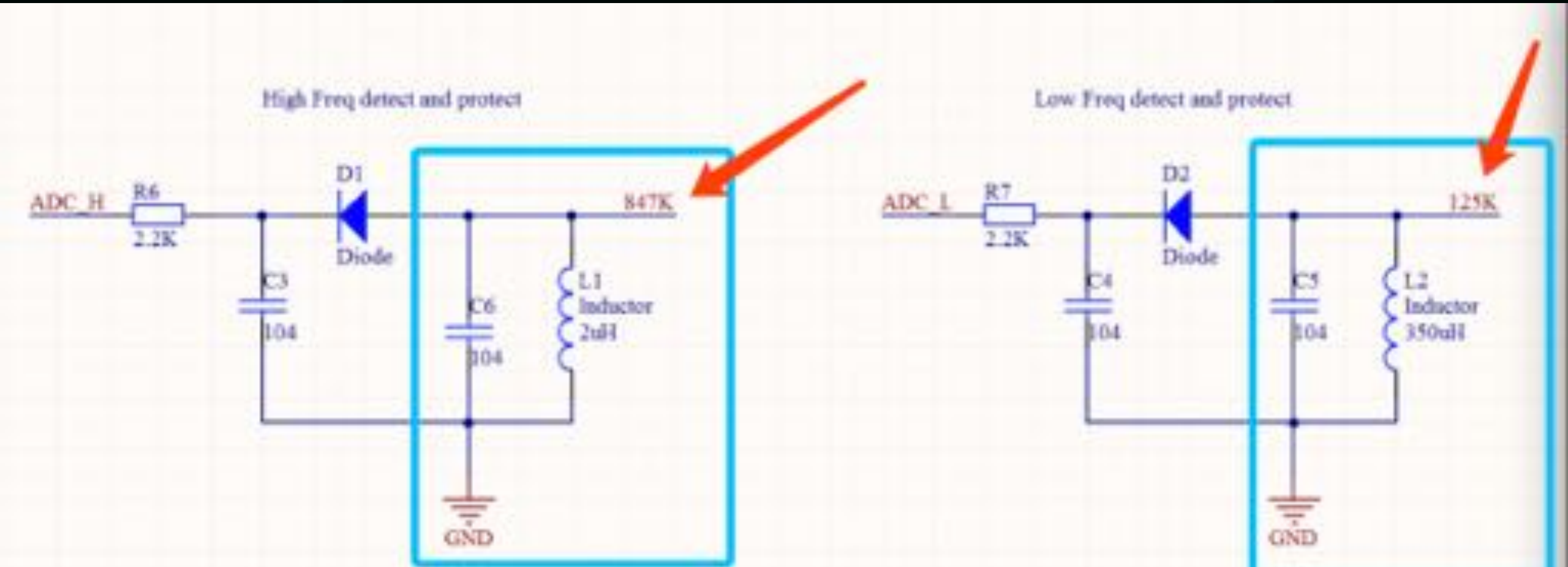
- Detect and protect





NFC defender and 125KHz defender

- Detect and protect



Ultrasound attacks smart hardware

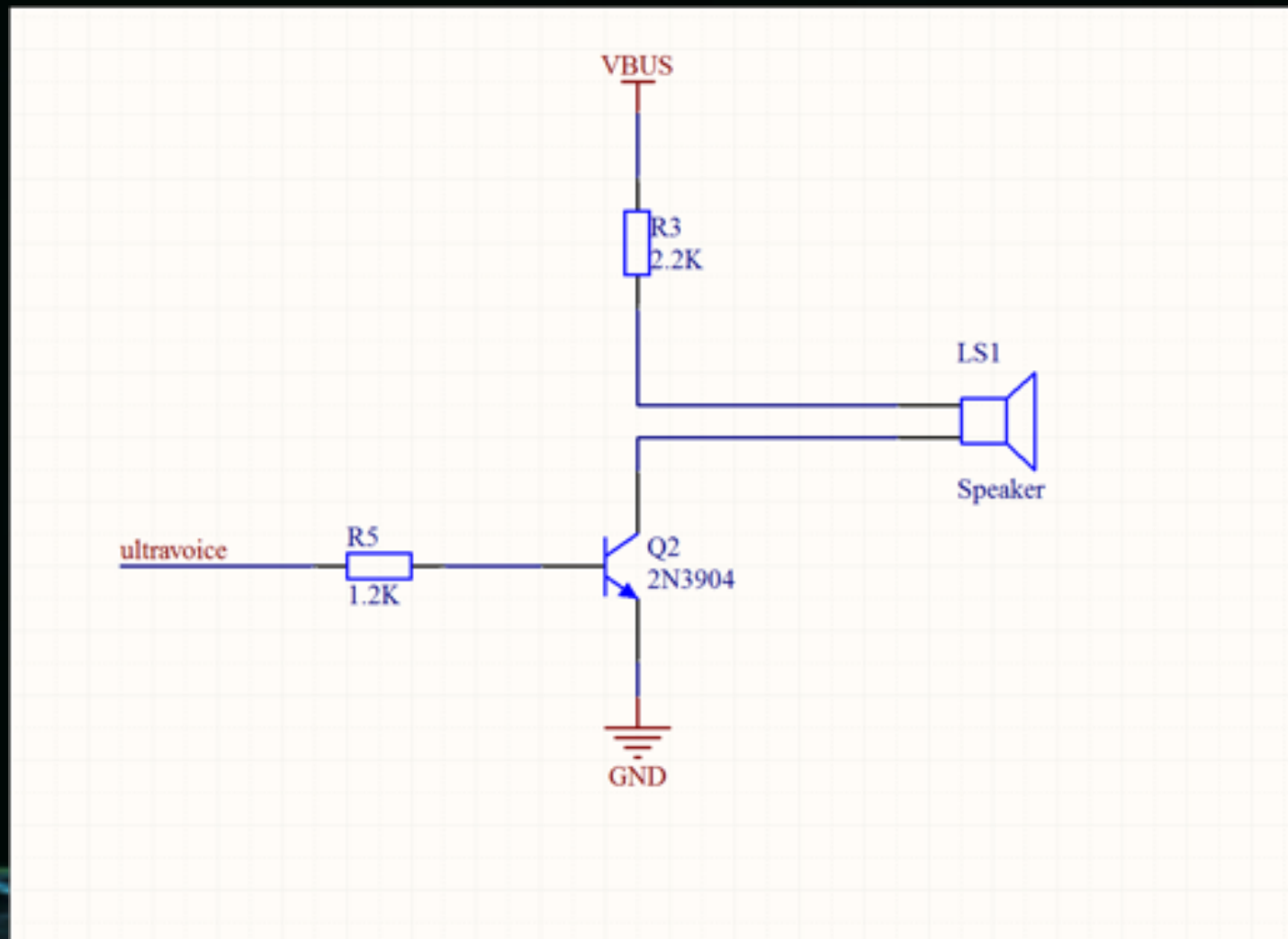
- What could voice do?

Ultrasound attacks smart hardware

- Physical resonance
- An electronic device with adjustable frequency of sound wave
- Be patient — Looking for the frequency of resonance

Ultrasound attacks smart hardware

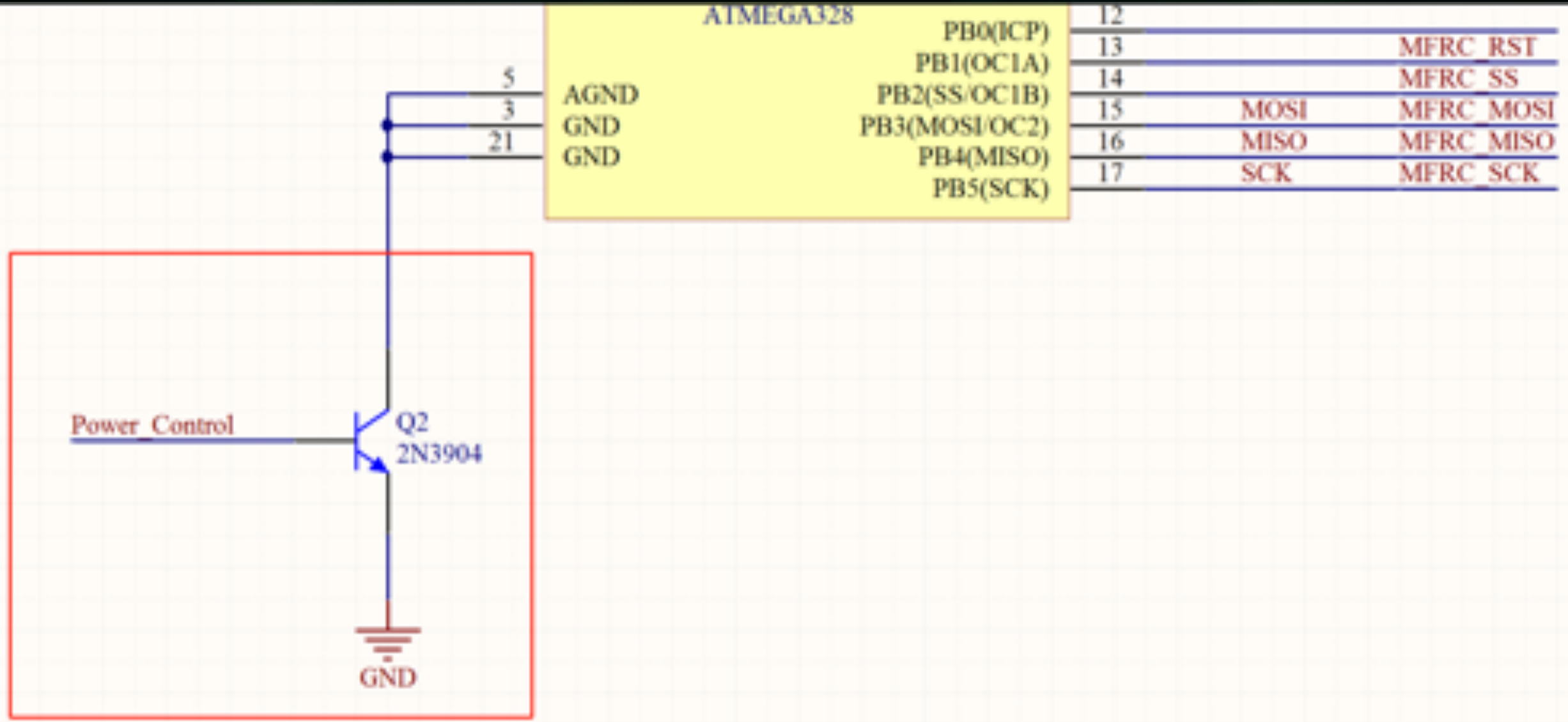
- Simplified —No Amplifier
- Speaker — Characteristic
- Microprocessor control



Hardware Power glitch attack

- Power fluctuation
- Clock disorder, program to run error
- Program bypass, decryption

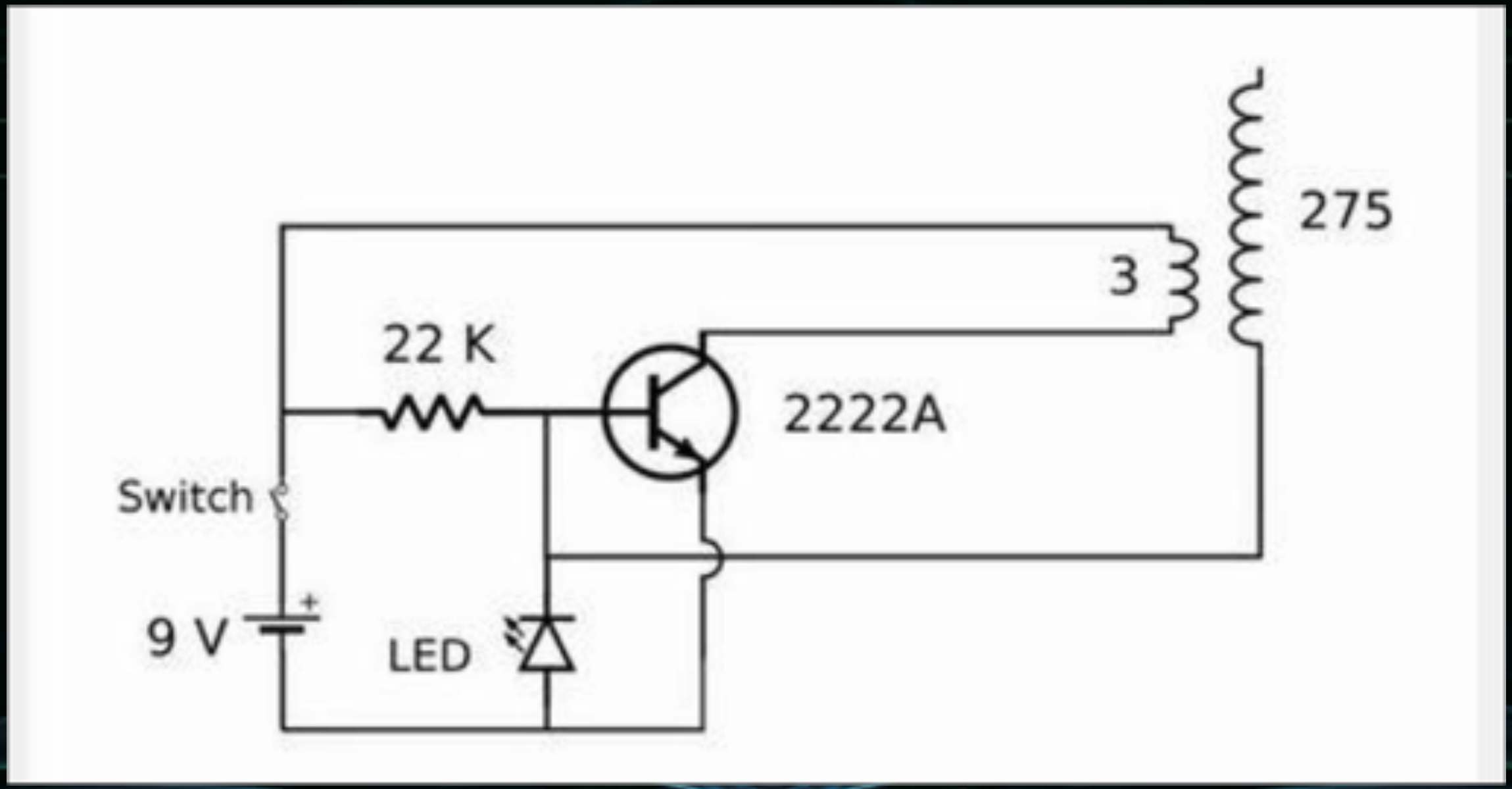
Hardware Power glitch attack



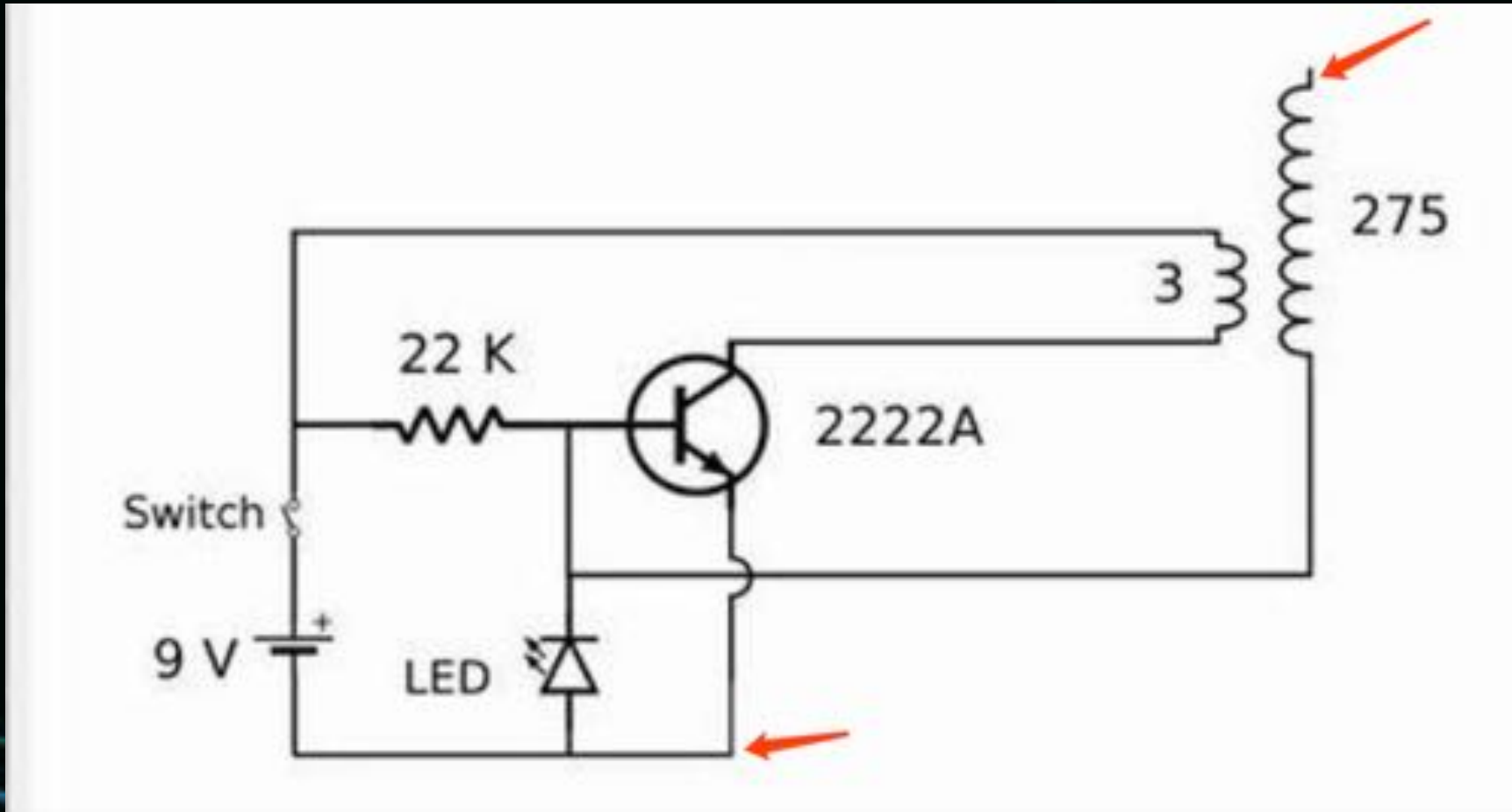
Ultra strong electromagnetic field circuit system breaker

- To attack a circuit system, such as an access control system, and c

Ultra strong electromagnetic field circuit system breaker



Make amazing artificial lightning



Hacker Research Institute

Thanks! && Any questions?

zhujiu1234@gmail.com