cheap cheap lah ~

Low Cost Laser Fault Target

Jakub Breier, Chien-Ning Chen, Wei He,
Alexander Herrmann, Marc Stöttinger

Physical Analysis and Cryptographic Engineering
Nanyang Technological University, Singapore

“Is it a theoretical attack”

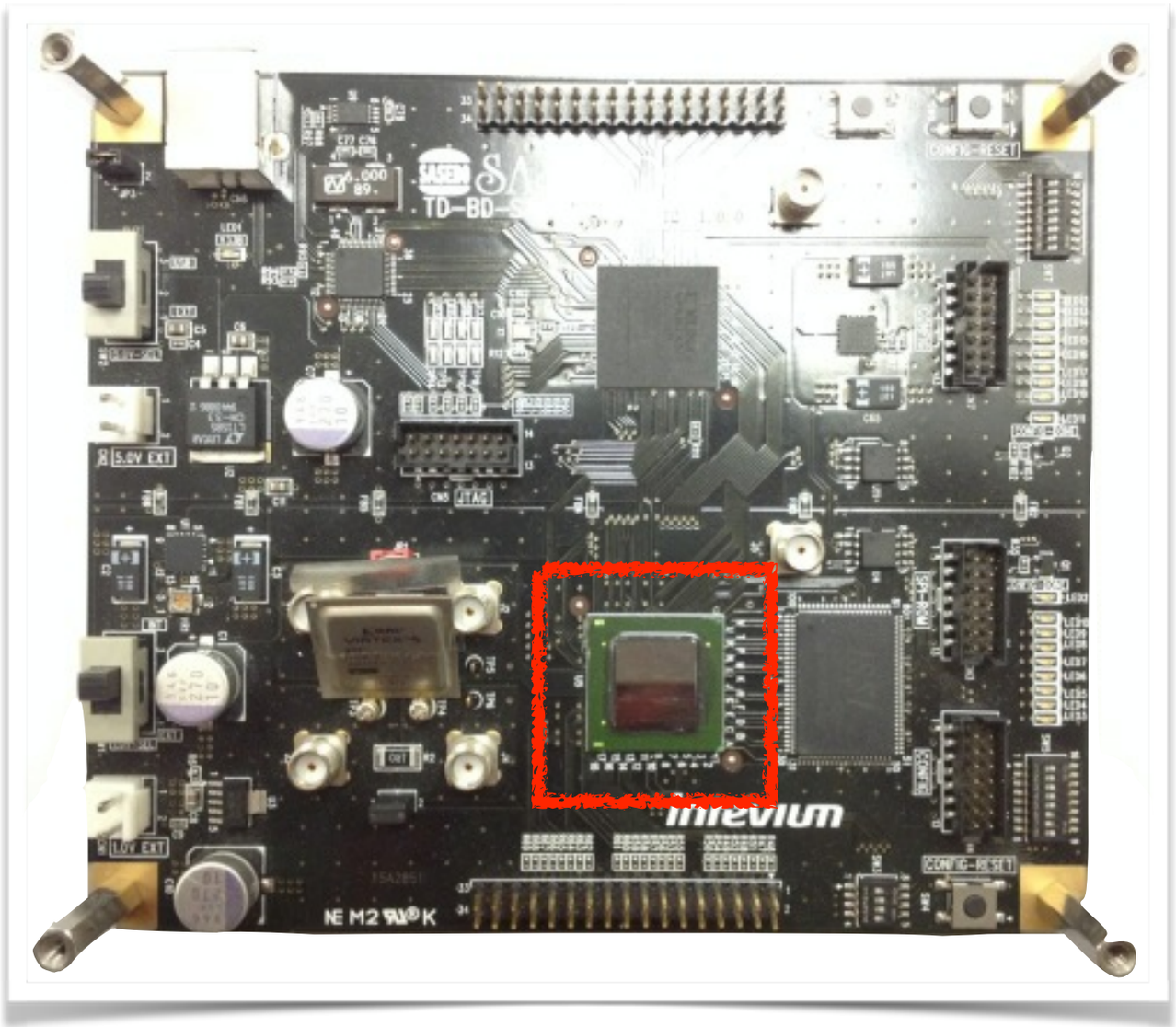
“The authors should provide experimental results”

–Anonymous Reviewers

Need real experiment!

SASEBO – G2

- Easy to decapsulate, but discontinued lah!



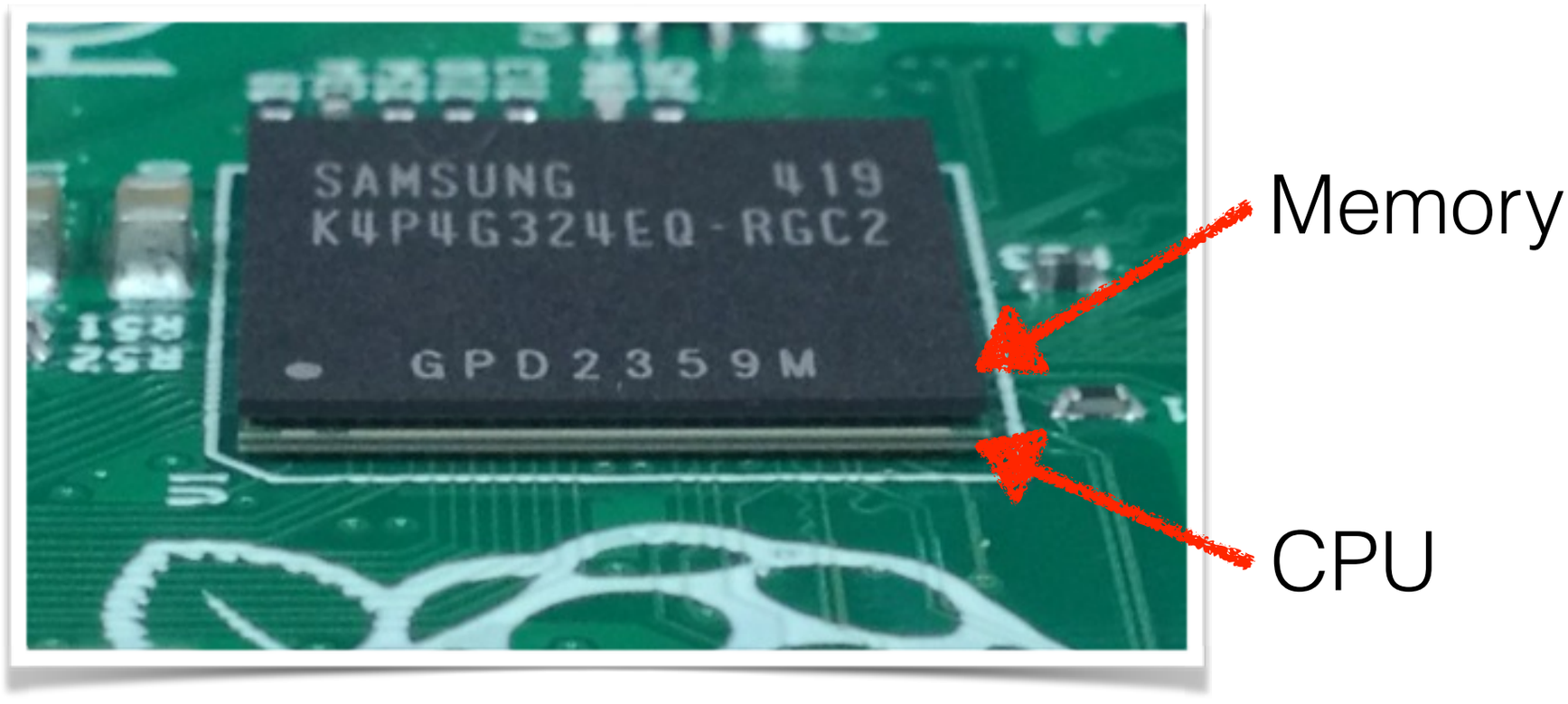
SAKURA – X/G

- SAKURA – X, JP¥ 370,000 (2.700 €)
  SAKURA – G, JP¥ 160,000 (1.168 €)

- where is your bonding wire?
  - $Cu + 4\ HNO_3 \rightarrow Cu(NO_3)_2 + 2\ NO_2 + 2H_2O$

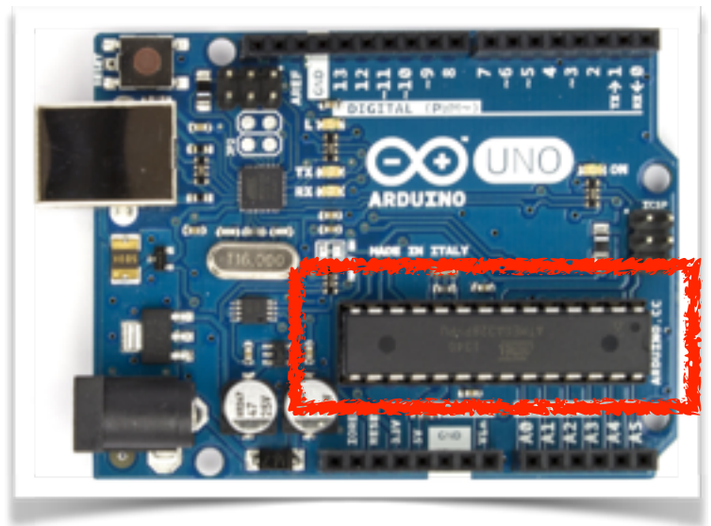
Raspberry Pi

- Cheap, 35 USD
- Fast, 700MHz ARMv6
- but …



Arduino UNO

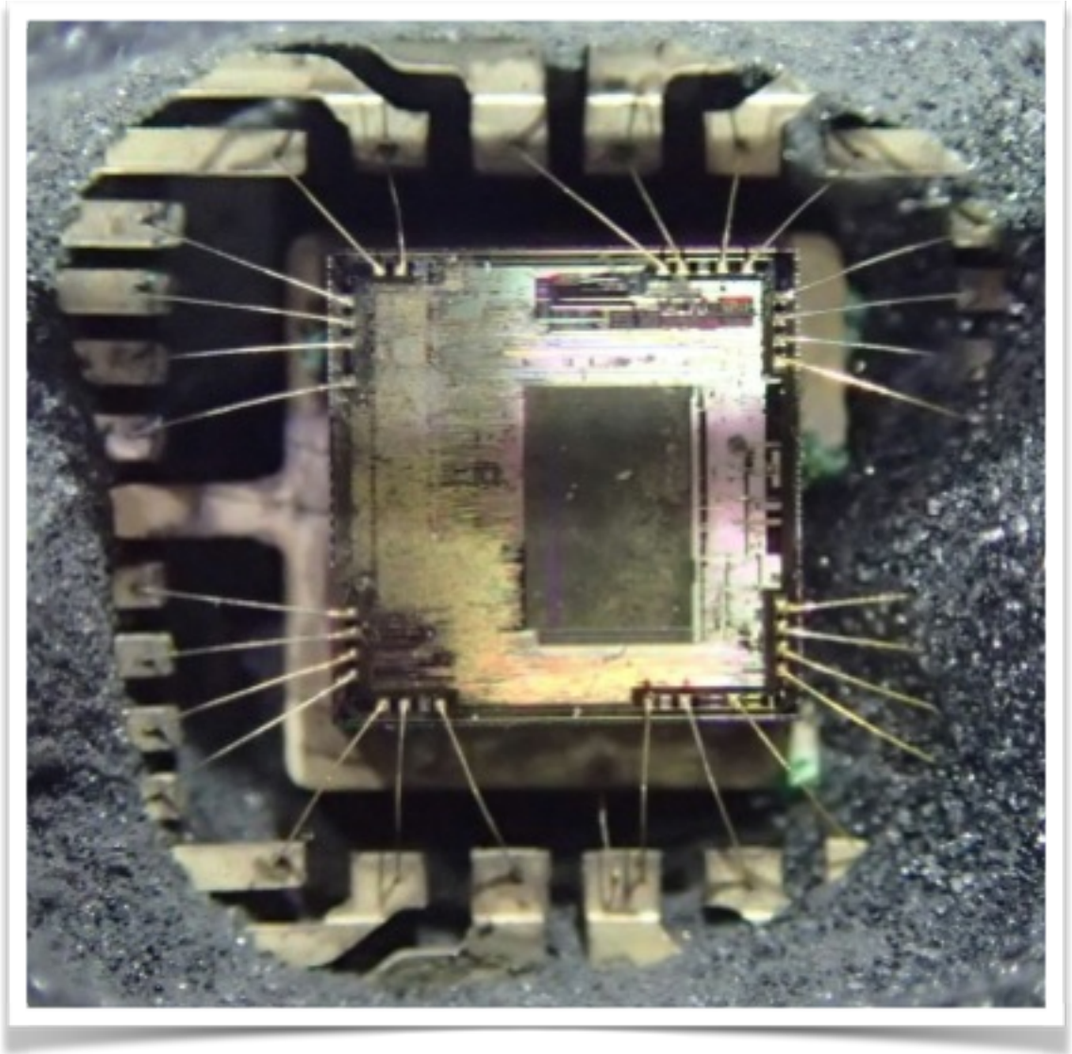
- Cheap, 20 € (25 USD)
- AVR ATmega328p, DIP, cheap, 2 €
- CPU, SRAM, Flash, EEPROM, …
- Simple development tools, support inline ASM, debug cable



http://arduino.cc/en/uploads/Main/ArduinoUno_R3_Front.jpg

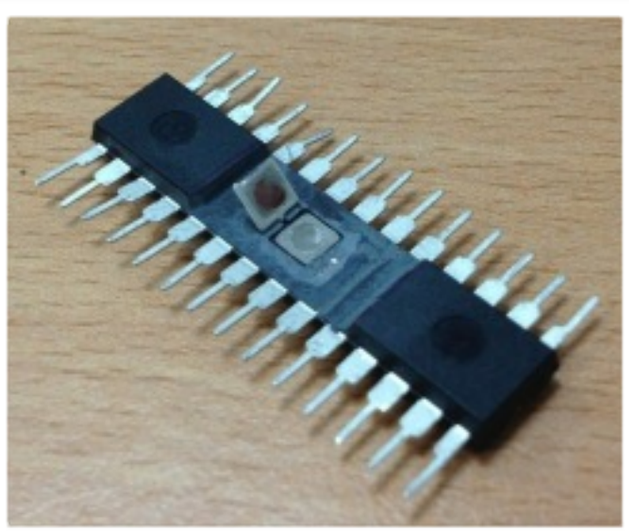
Front-Side Decapsulation

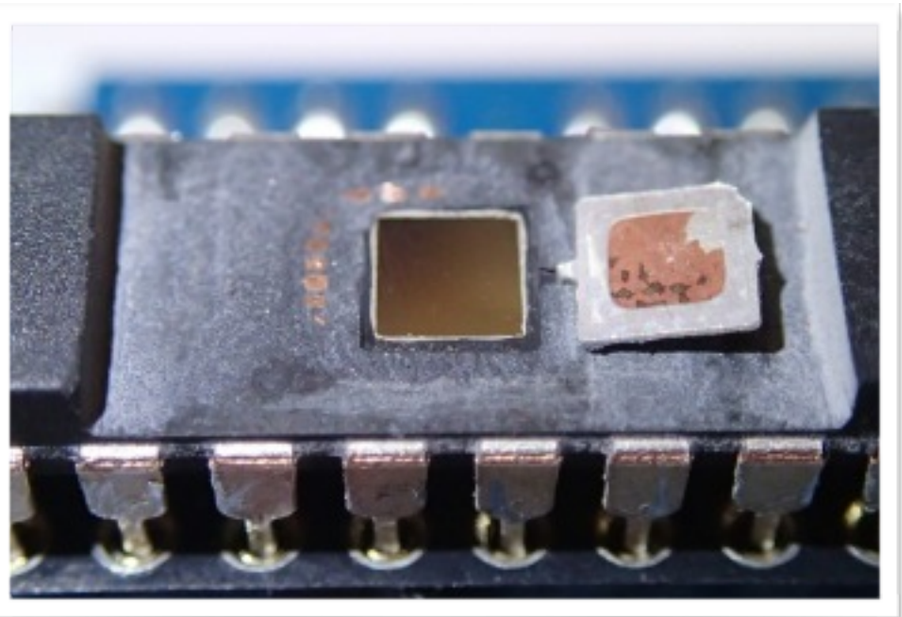
- Golden bonding wires, few pins



Back-Side Decapsulation

- Good equipment

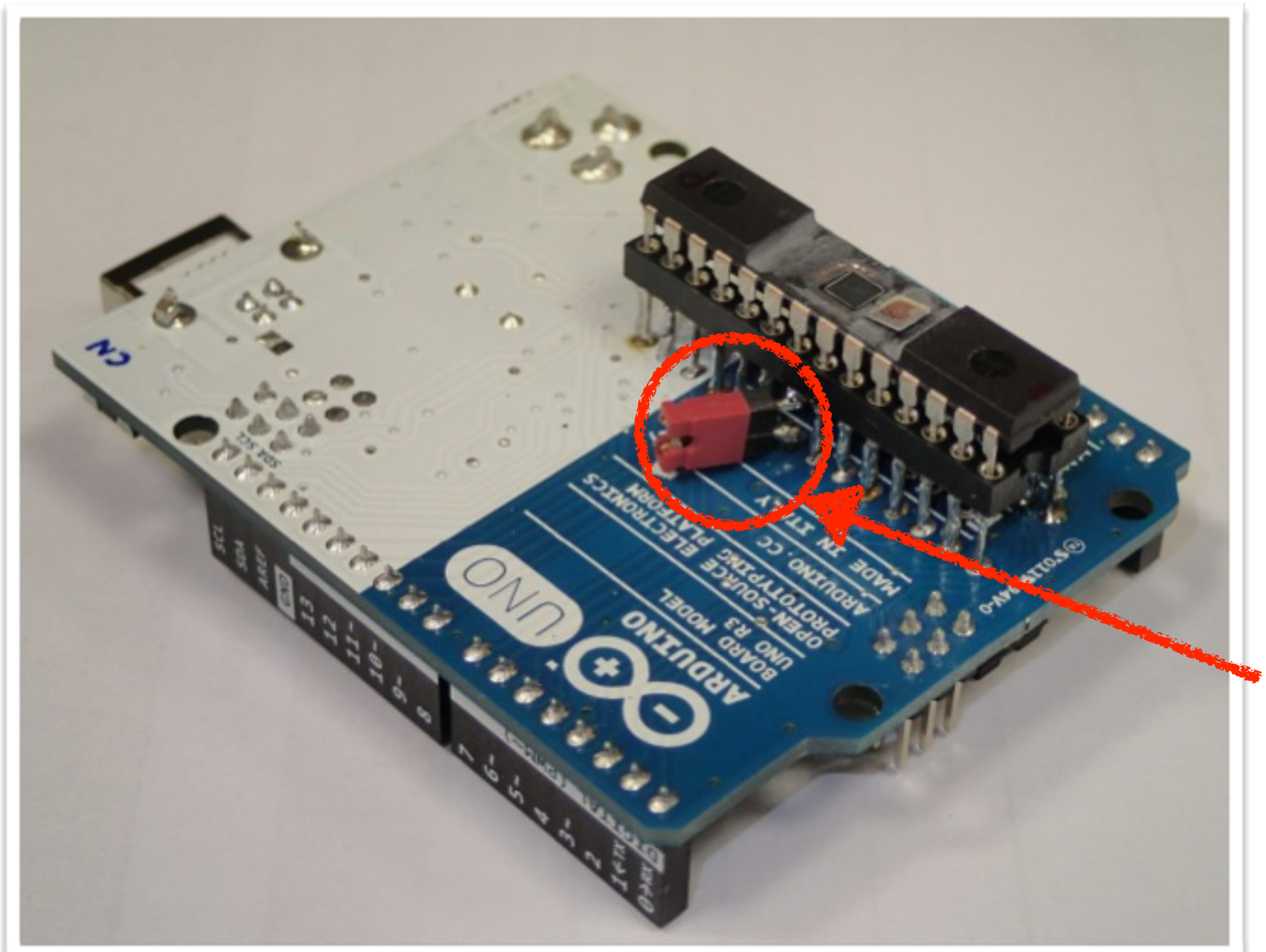




- Cheap equipment

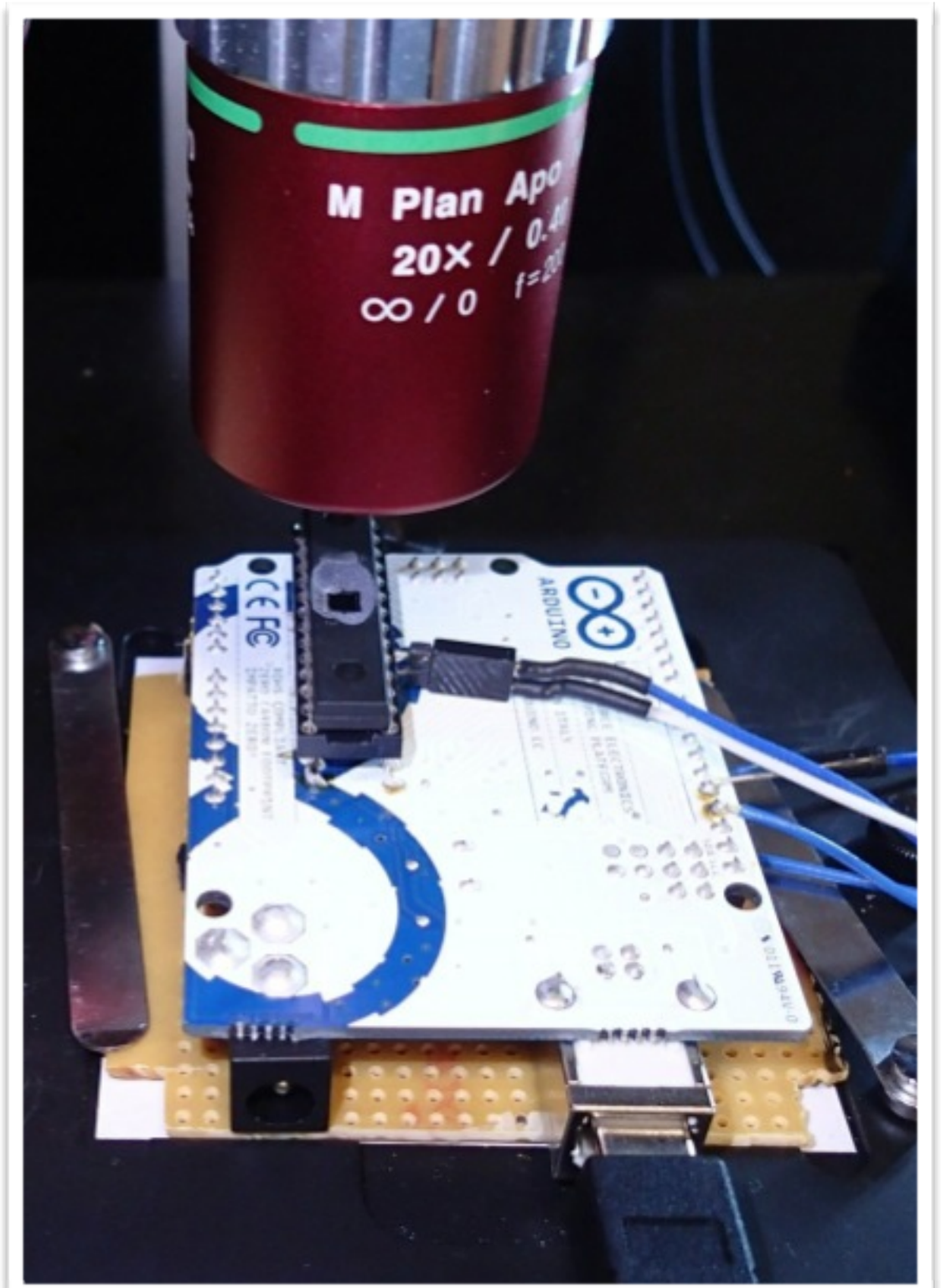
http://img.diytrade.com/cdimg/351847/1464632/0/1123656775.jpg

Arduino ОПП



Laser Fault Injection

20 mW IR laser can cause something wrong!



Thank you.