

# HYBRID COST-EFFECTIVE DECAPSULATION OF CHIPS FOR SUCCESSFUL LASER FAULT INJECTION



**Furkan BEKAR**

Informatics and Information Security  
Research Center (BILGEM)  
The Scientific and Technological  
Research Council of Turkiye (TUBITAK)  
Istanbul, Turkiye  
[f.bekar2023@gtu.edu.tr](mailto:f.bekar2023@gtu.edu.tr)



**Alp Arslan BAYRAKÇI**

Department of Computer Engineering  
Gebze Technical University  
Kocaeli, Turkiye  
[abayrakci@gtu.edu.tr](mailto:abayrakci@gtu.edu.tr)

**ISC Turkiye 2024 | 17 Ekim 2024**

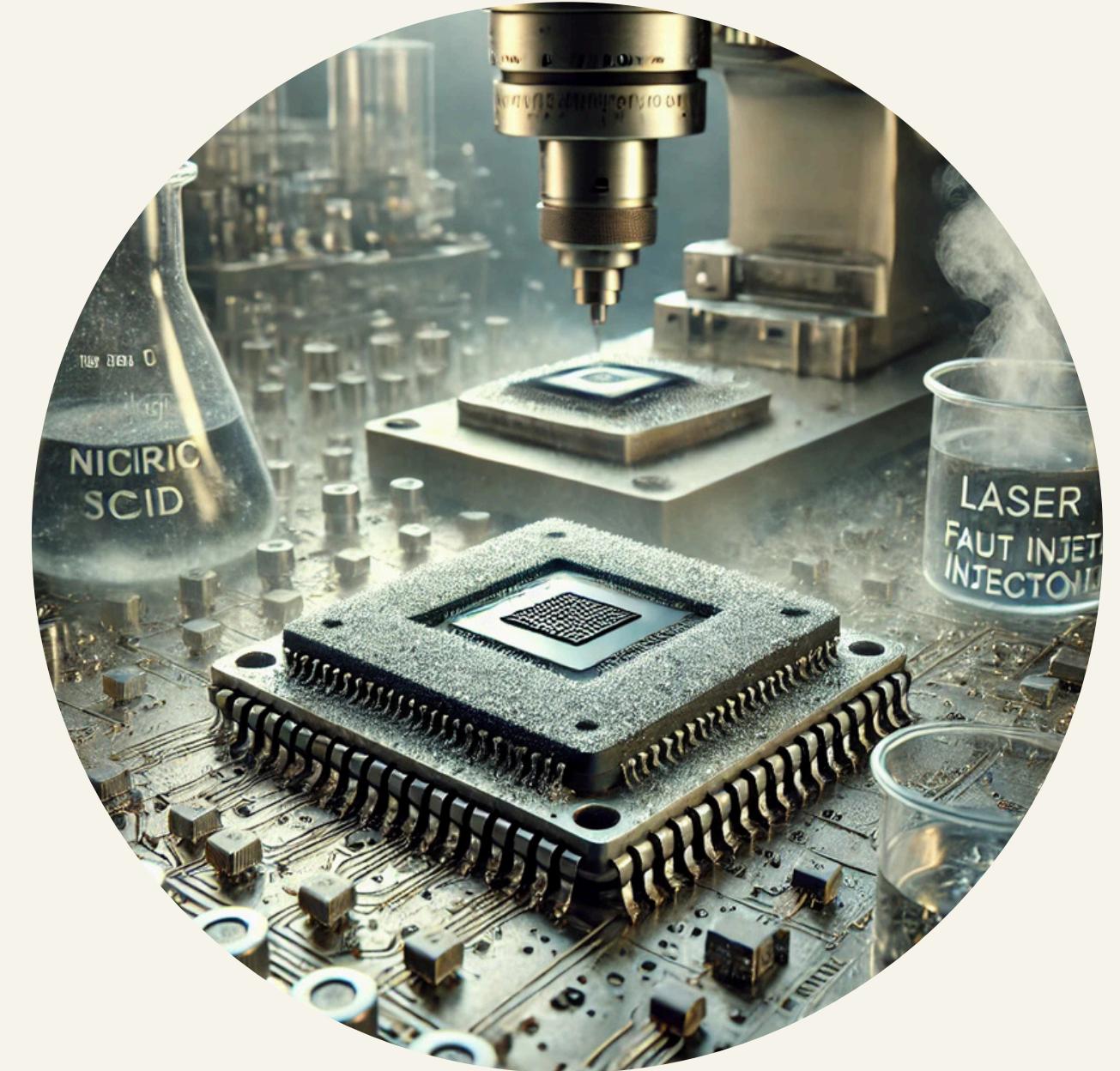
# AGENDA OUTLINE

- 1 Problem
- 2 Decapsulation Methods
- 3 Hybrid Decapsulation
- 4 Application on the ATmega328P
- 5 Results (Decapsulation and LFI)

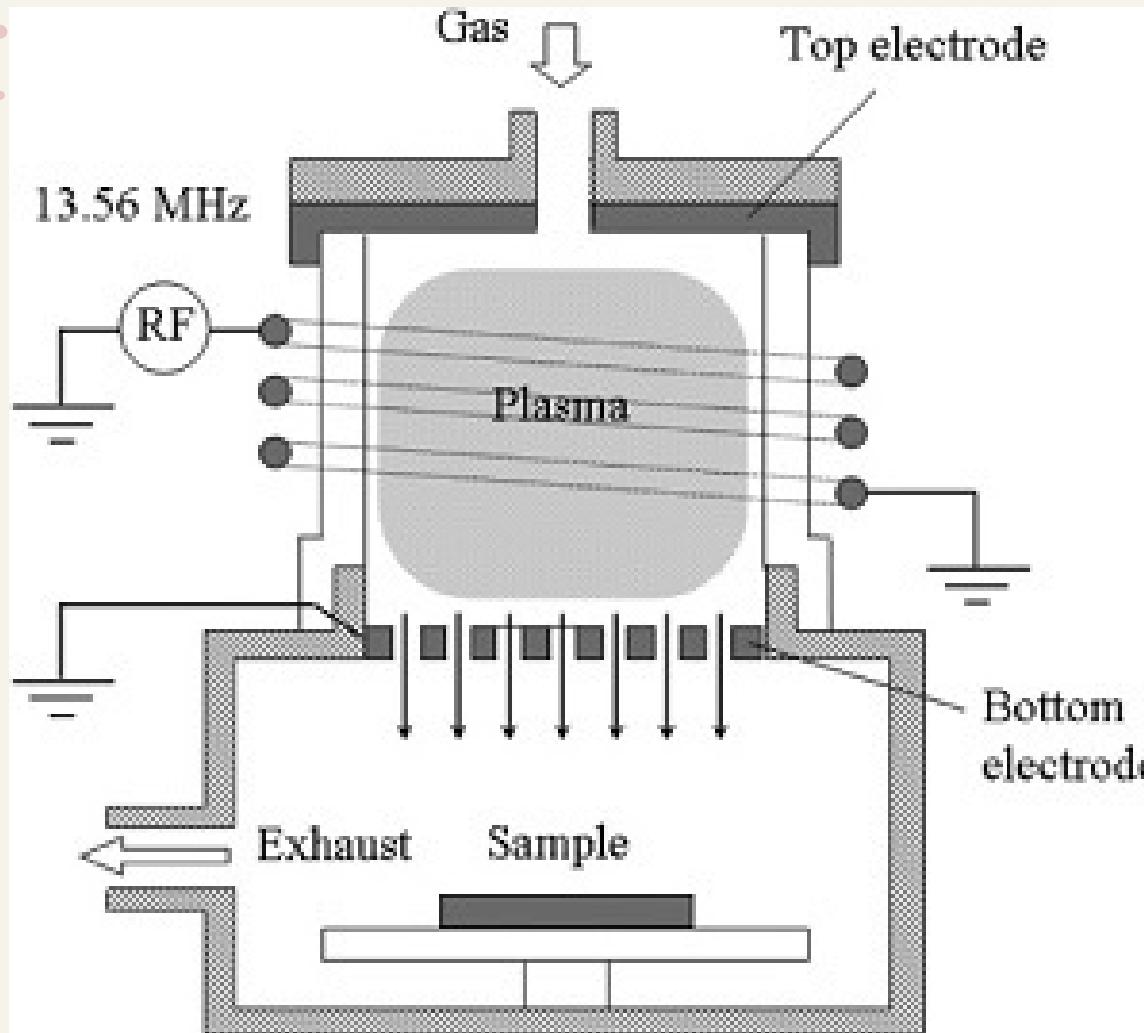
# PROBLEM

## CHIP DECAPSULATION

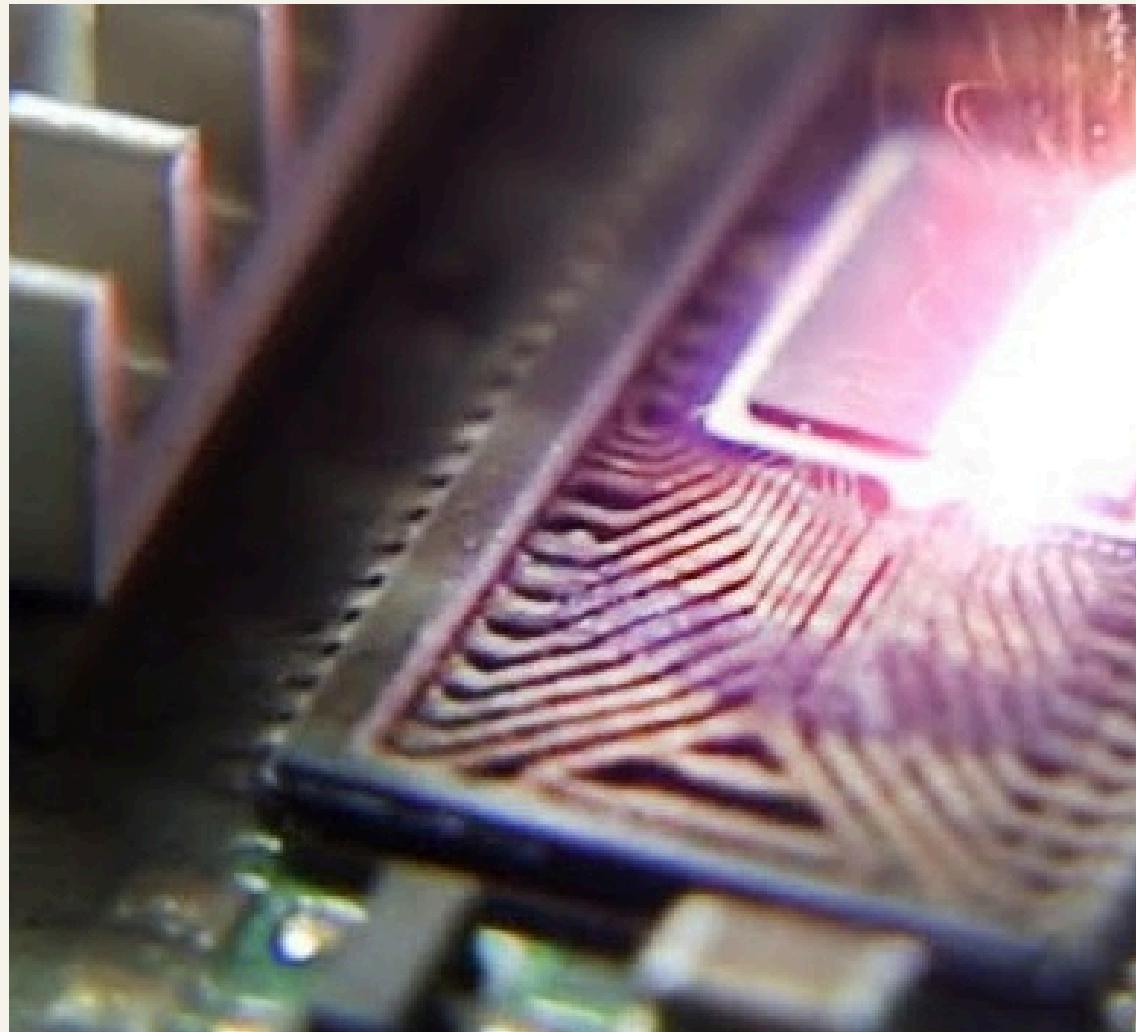
- Failure Analysis
- Reverse Engineering
- Counterfeit Product Detection
- Safety Audit
- Material Testing
- Product Development and Optimization



# DECAPSULATION METHODS



Plasma Etching



Laser Etching



Chemical Etching

# DECAPSULATION METHODS



## Chemical Etching:

- Low Success



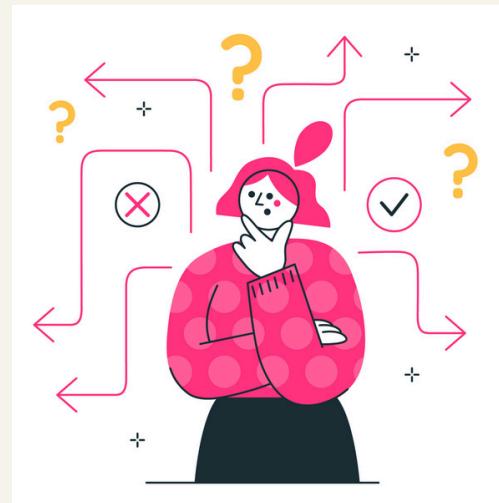
## Plasma Etching:

- 100,000s €

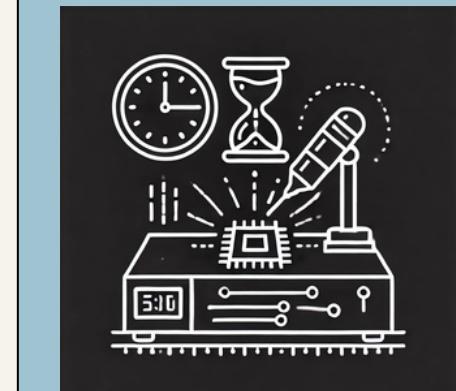


## Laser Etching:

- 10,000s €
- Low Selectivity



Disadvantages



## Plasma Etching:

- Slowly

# PROPOSED HYBRID METHOD

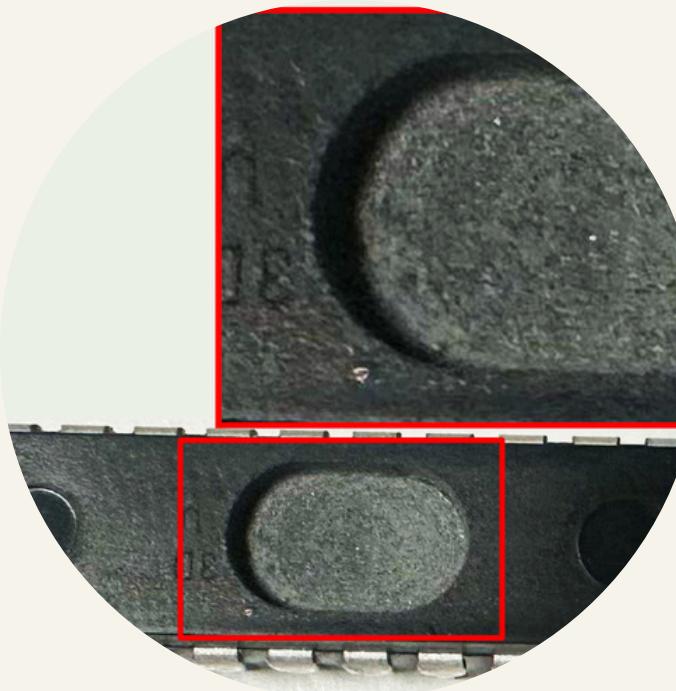
00

Preparation



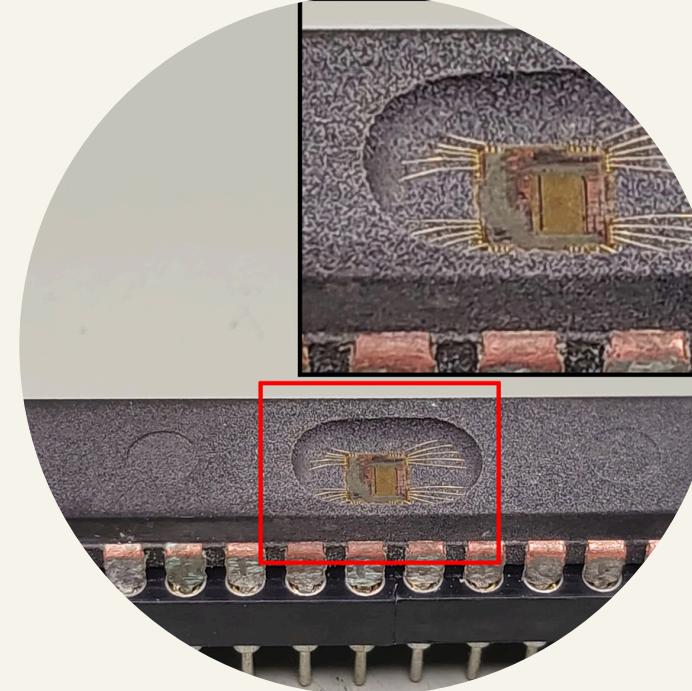
01

Mechanical Etching



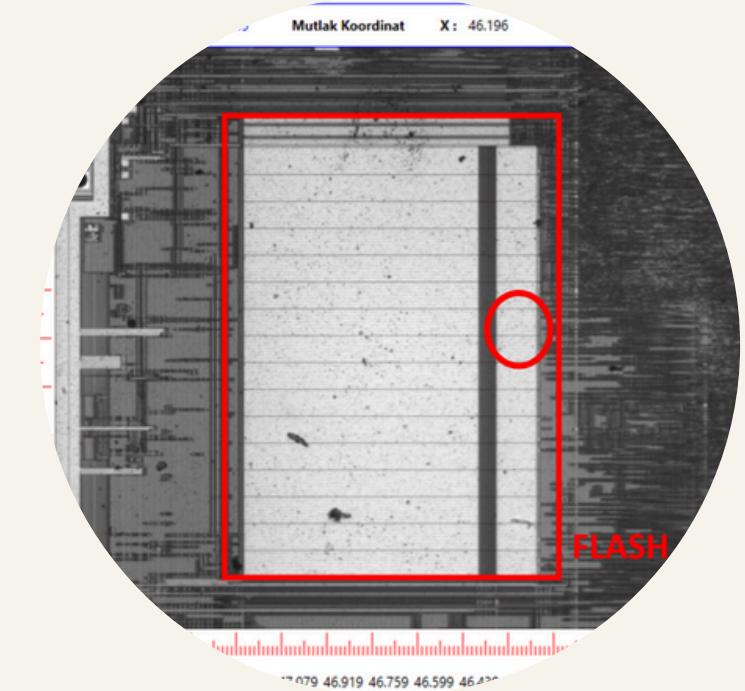
02

Chemical Etching

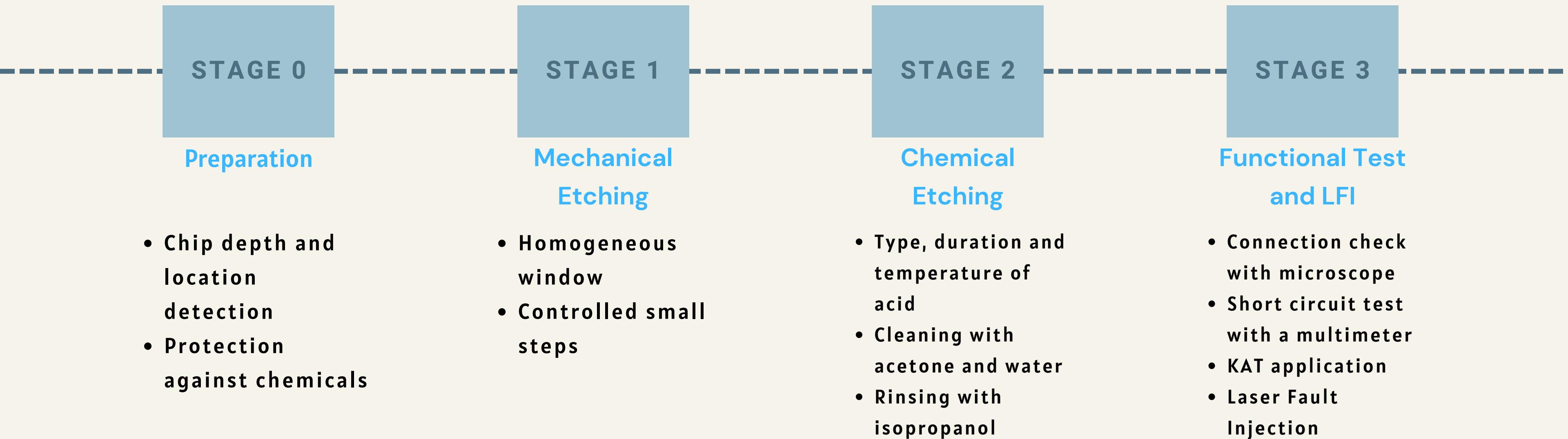


03

Functional Test and LFI



# PROPOSED HYBRID METHOD

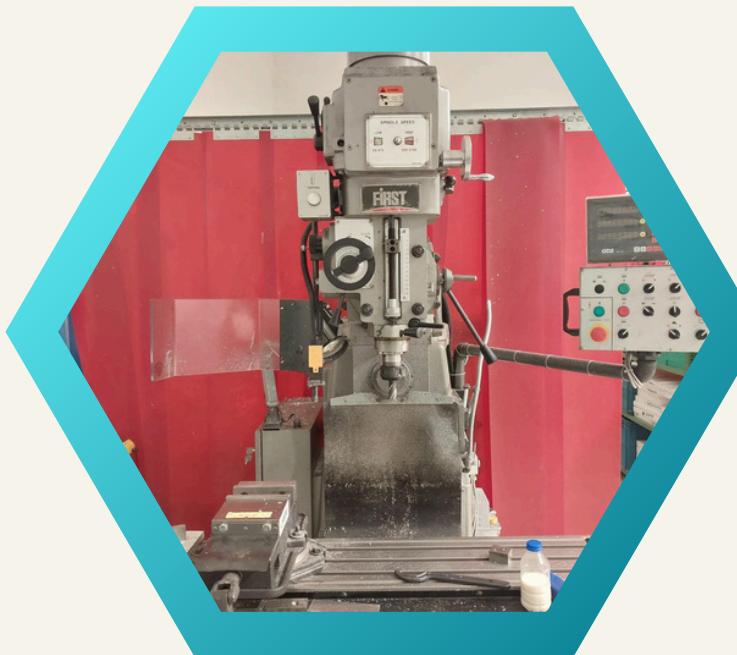


# EXPERIMENT: ATMEGA328P DECAPSULATION



**Preparation**

- Detecting location and depth by damaging the chip
- Aluminum tape for protection of the pins



**Mechanical Etching**

- 100 micron steps on a milling machine
- 4 mm milling bit
- 7x4 mm window



**Chemical Etching**

- 98% concentration of acid
- Application time 30 seconds
- Cleaning with acetone and water

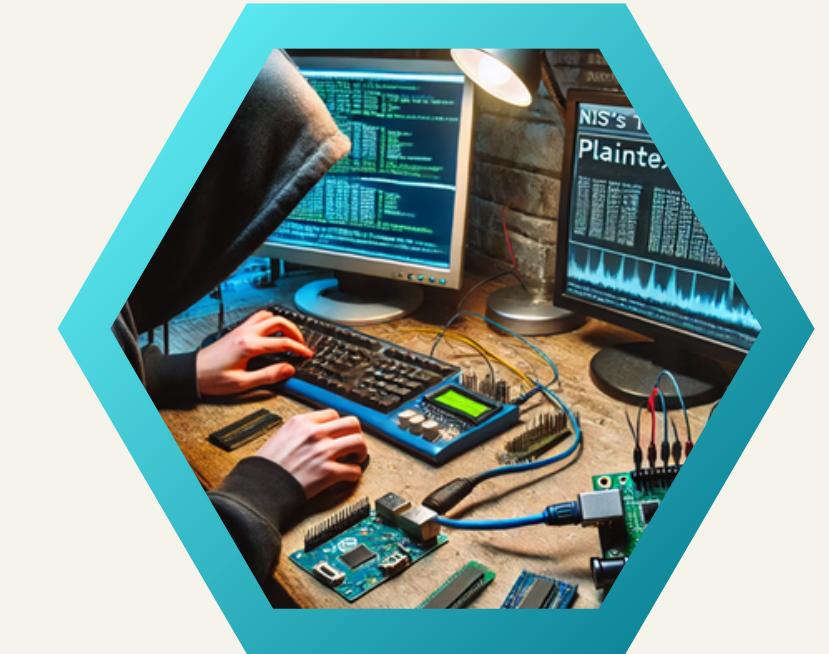
# EXPERIMENT: FUNCTIONAL VERIFICATION



- Connection check



- Short circuit check



- AESLib library
- NIST SP 800-38A

## F.1 ECB Example Vectors

### F.1.1 ECB-AES128.Encrypt

Key	2b7e151628aed2a6abf7158809cf4f3c
Block #1	
Plaintext	6bc1bee22e409f96e93d7e117393172a
Input Block	6bc1bee22e409f96e93d7e117393172a
Output Block	3ad77bb40d7a3660a89ecaf32466ef97
Ciphertext	3ad77bb40d7a3660a89ecaf32466ef97

```

1 #include <AESLib.h>
2 #include <string.h>

Serial Monitor ×

Message (Enter to send message to 'Arduino Uno' on 'COM3')
Key: 2B7E151628AED2A6ABF715889CF4F3C
Plaintext: 6BC1BEE22E409F96E93D7E117393172A
Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97

```

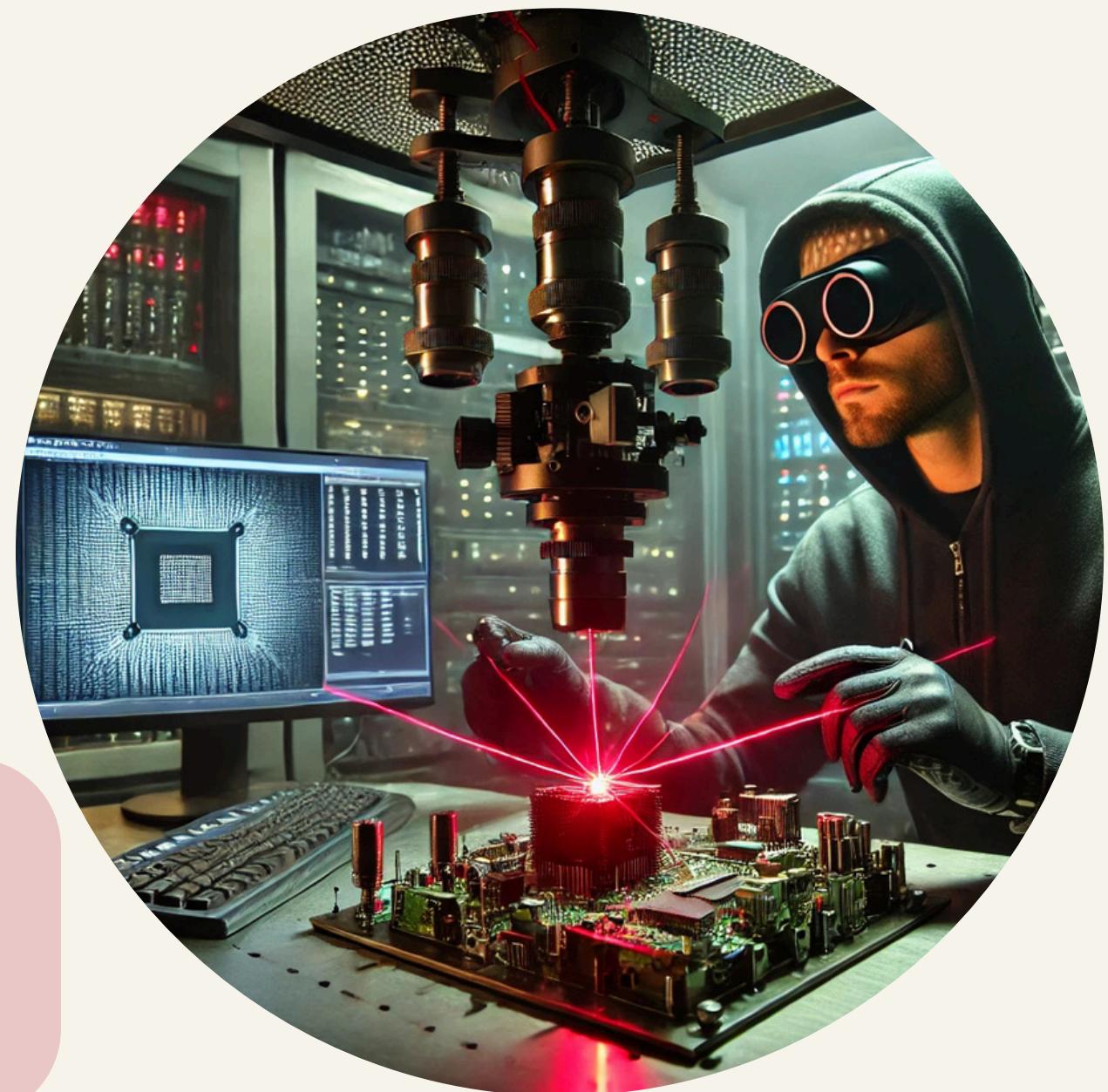
# EXPERIMENT: LFI

## Laser Station

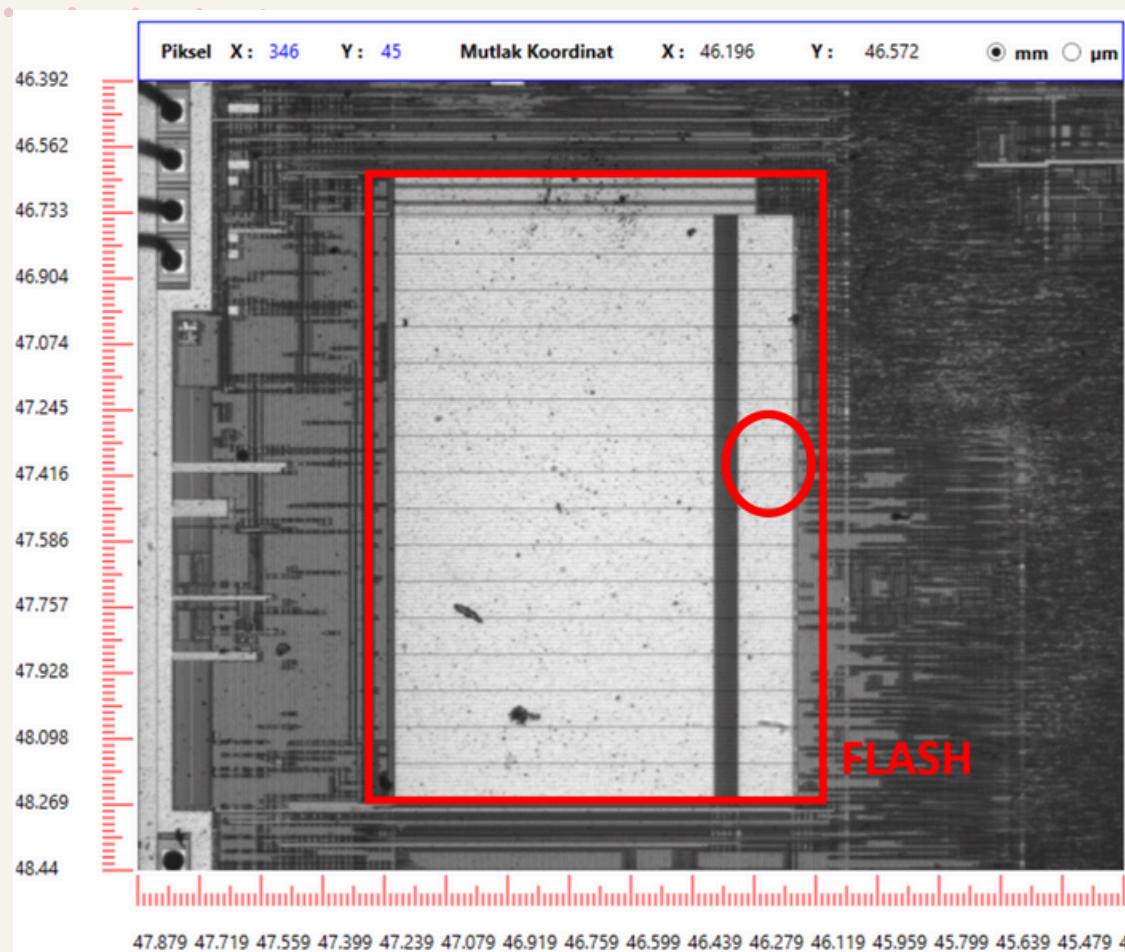
- 1064 nm laser source
- 150 ns pulse duration
- 1200 mA current
- 1.4 um laser spot size
- 5x objective

## LFI Method

- Trigger mechanism for laser pulse
- Fault sensitive region detection
- Scanned area: Flash memory
- 0.1 mm step size



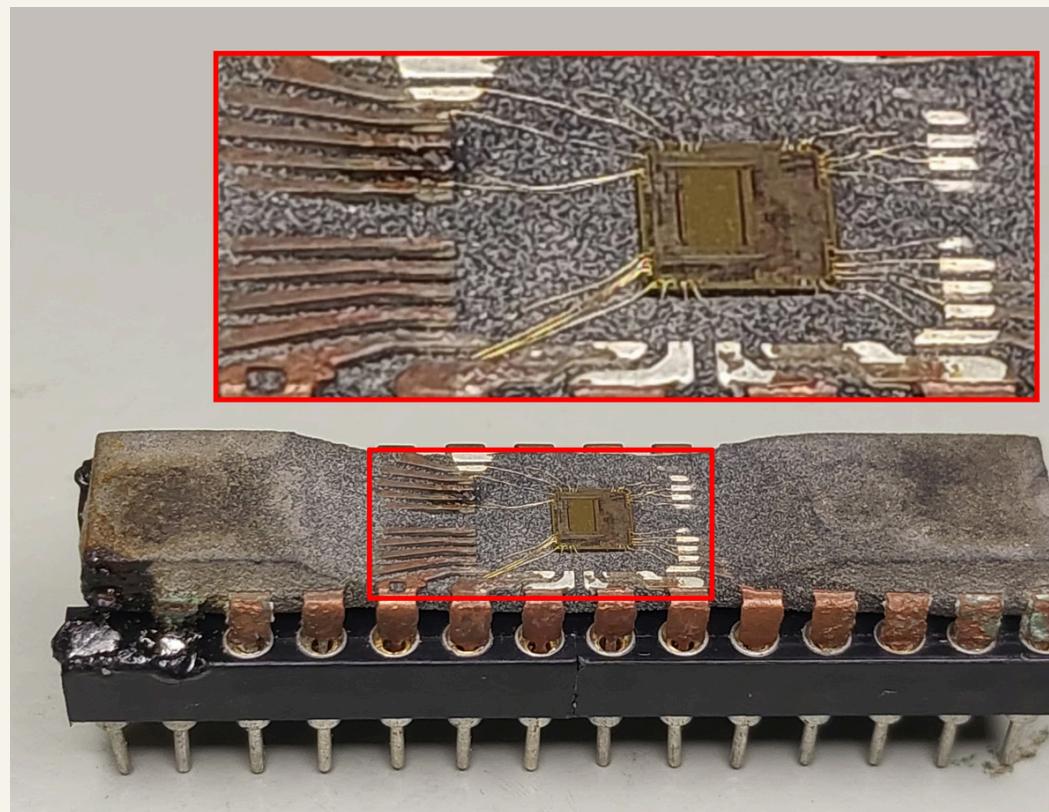
# LFI TEST RESULTS



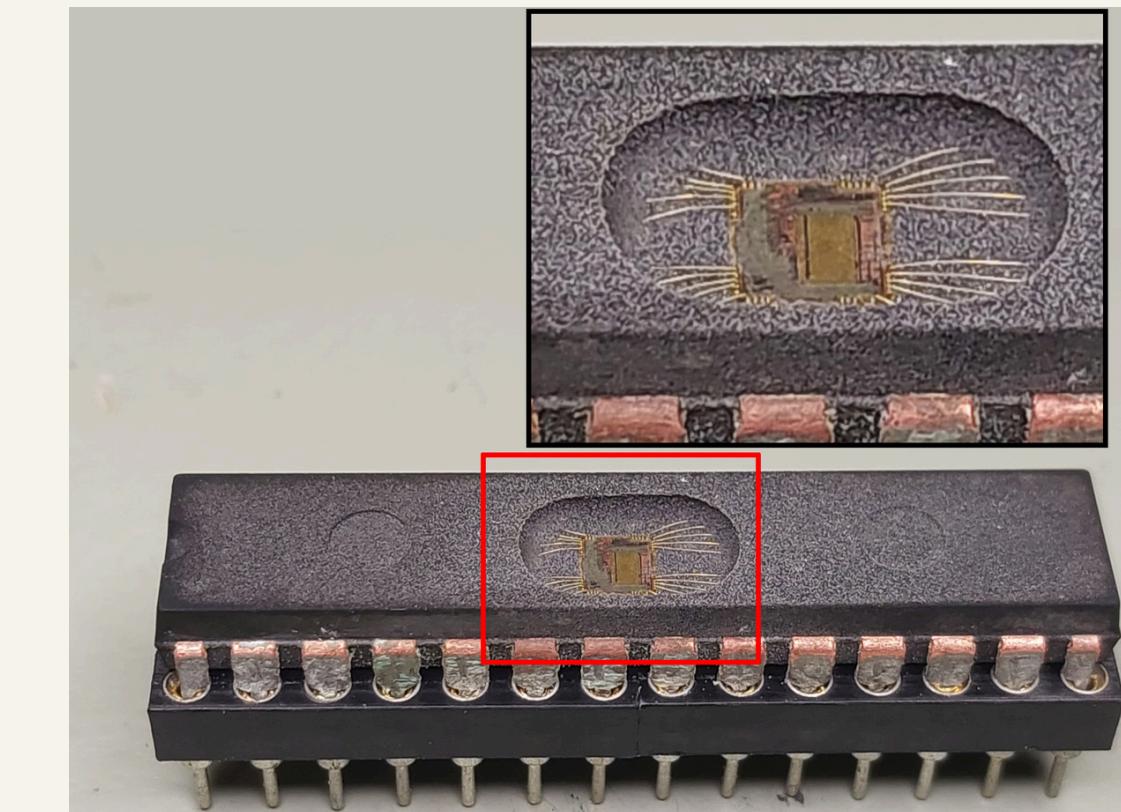
Expected Result	Return Value	X Coordinate	Y Coordinate
Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97	Key: 2B7E151628AED2A6ABF715889CF4F3C Encrypted:24 BE 83 91 FD AF 61 93 FA 0E EF A3 E8 DD 3A 87	45.937	47.473
Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97	Key: 2B7E151628AED2A6ABF715889CF4F3C	45.937	47.621
Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97	Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97	45.937	47.769

Expected Result	Return Value	
Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97	Key: 2B7E151628AED2A6ABF715889CF4F3C	
Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97	Encrypted:24 BE 83 91 FD AF 61 93 FA 0E EF A3 E8 DD 3A 87	
Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97	Key: 2B7E151628AED2A6ABF715889CF4F3C	
Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97	Encrypted:3A D7 7B B4 0D 7A 36 60 A8 9E CA F3 24 66 EF 97	

# RESULTS (MECHANICAL ETCHING)

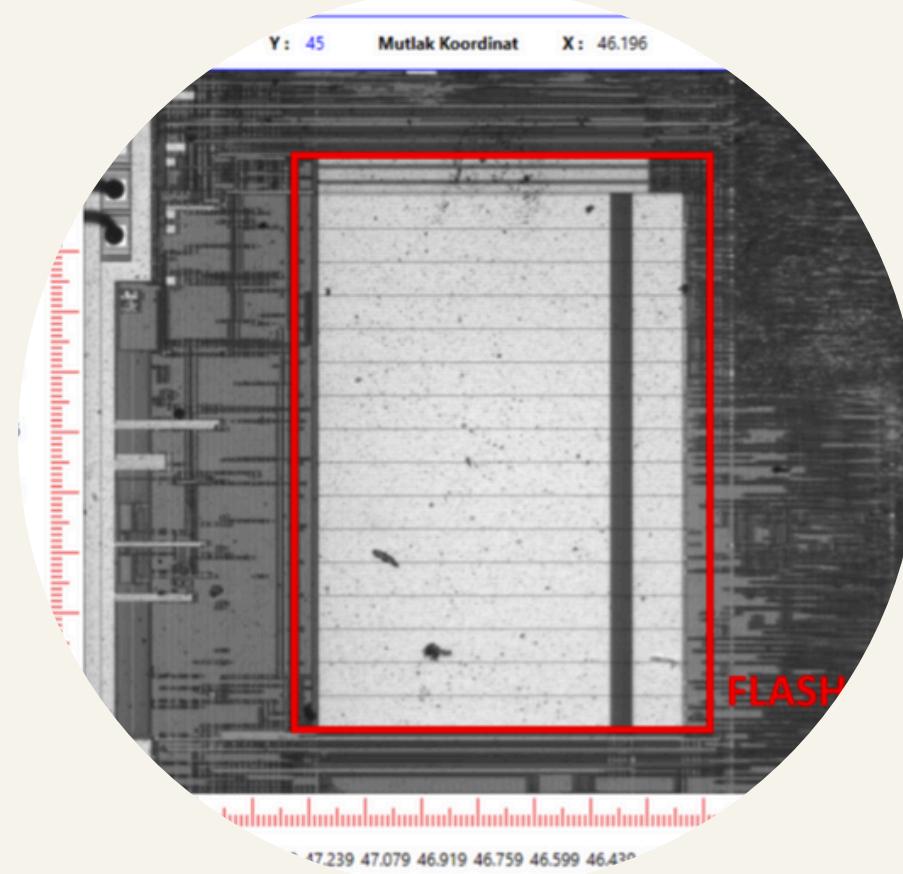


- Opened with a hand motor

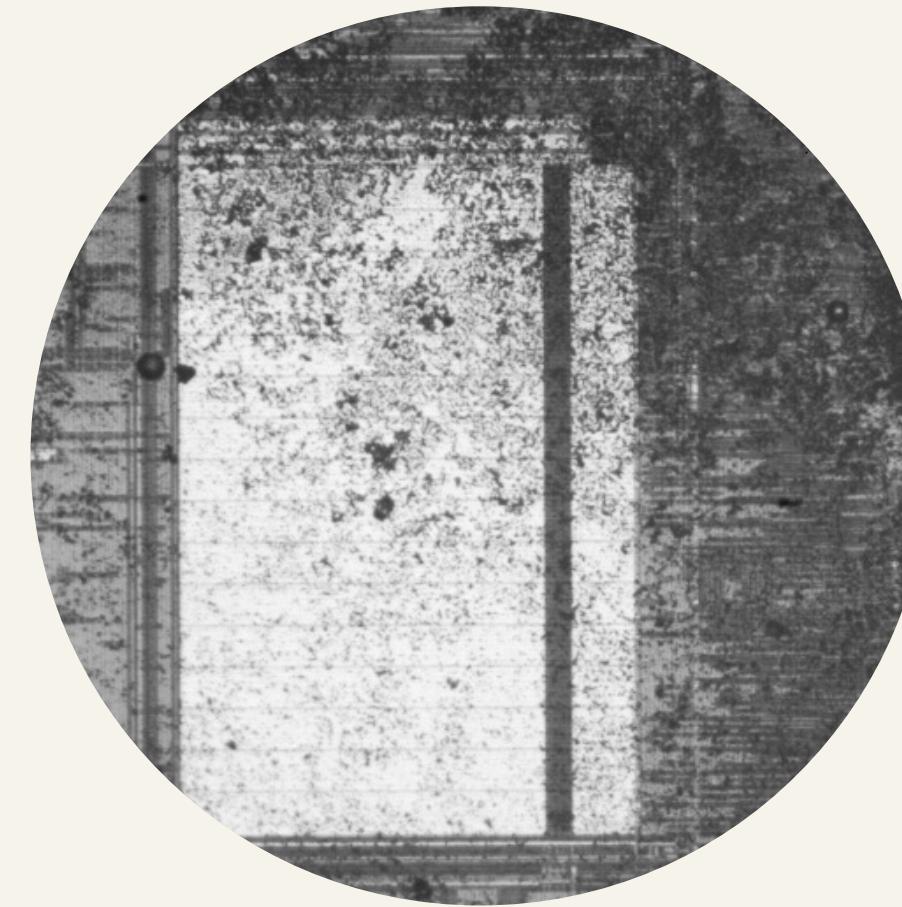


- Opened with a milling machine

# RESULTS (WATER - ACETONE)

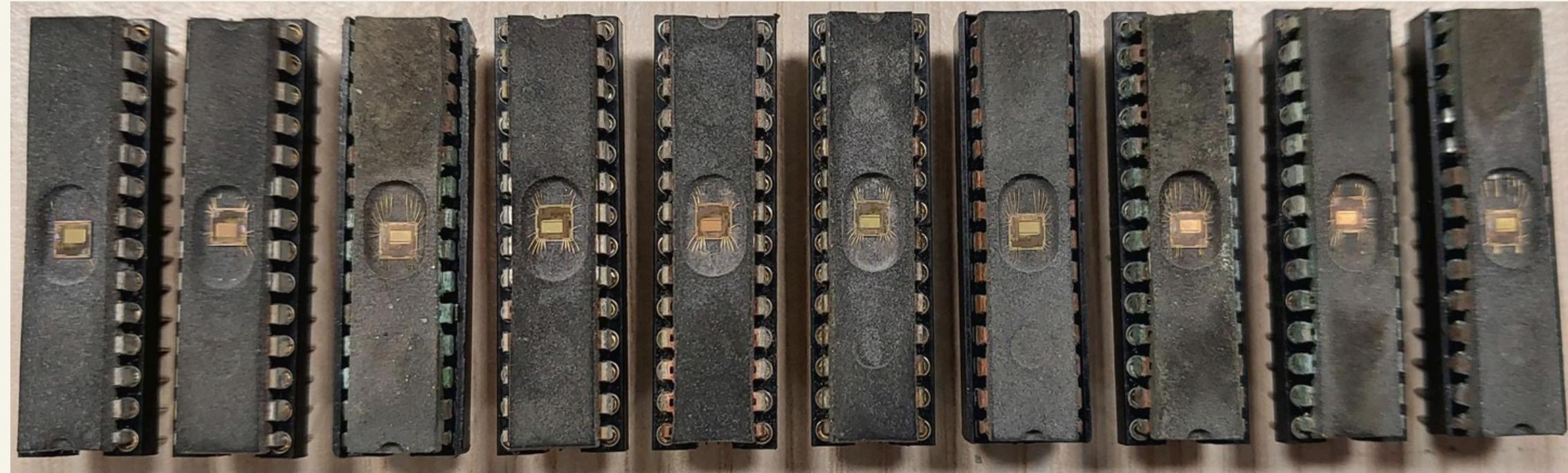


- Cleaning with water and acetone



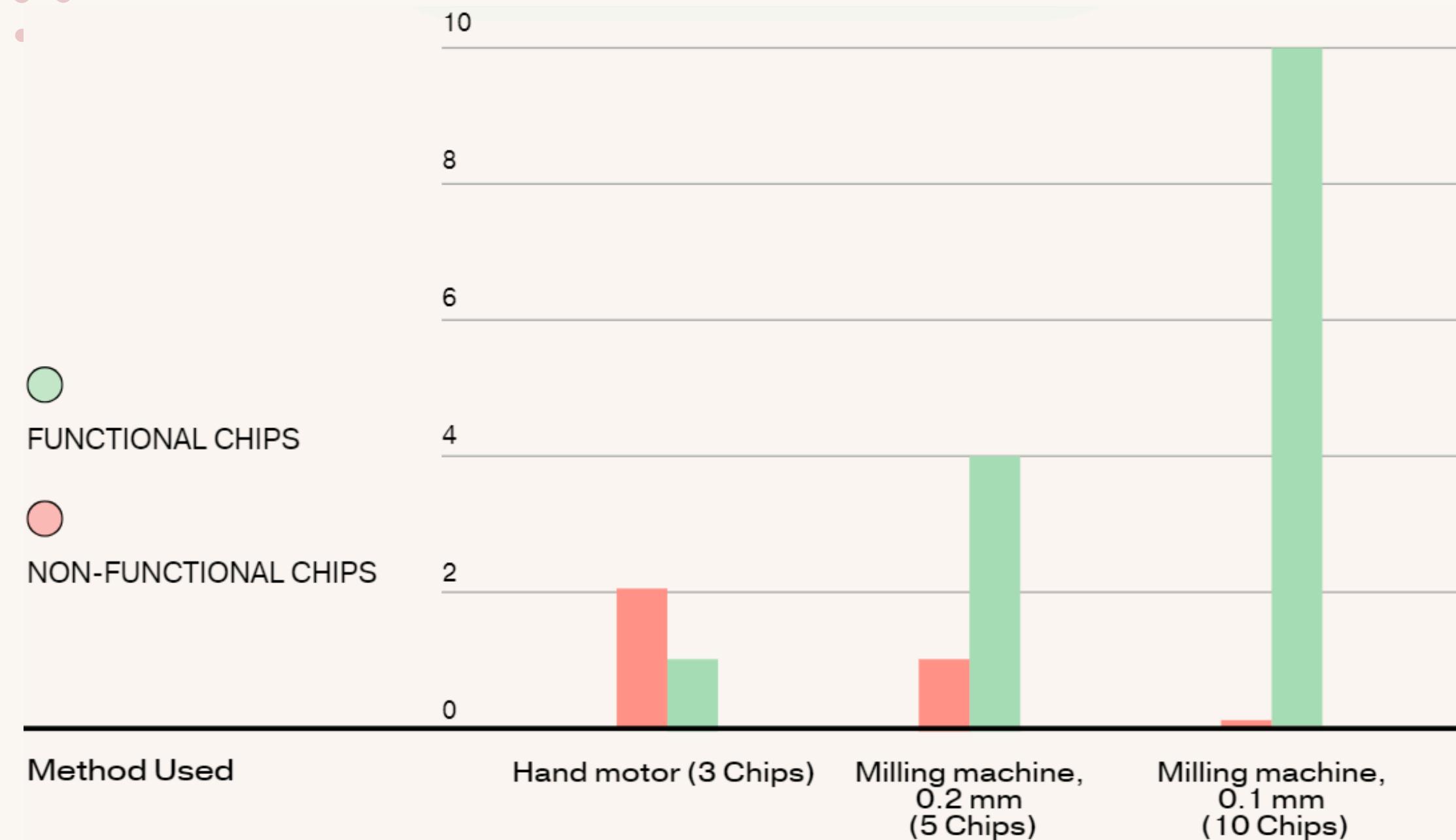
- Cleaning with water only

# RESULTS (PROPOSED METHOD)



- Chips opened with the proposed method

# DECAPSULATION SUCCESS

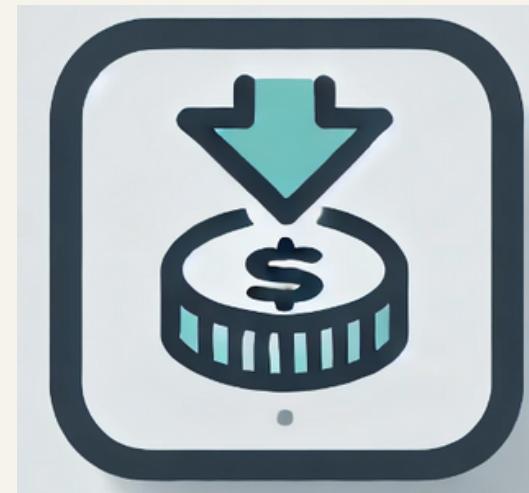


# RESULTS (COST EFFICIENCY)

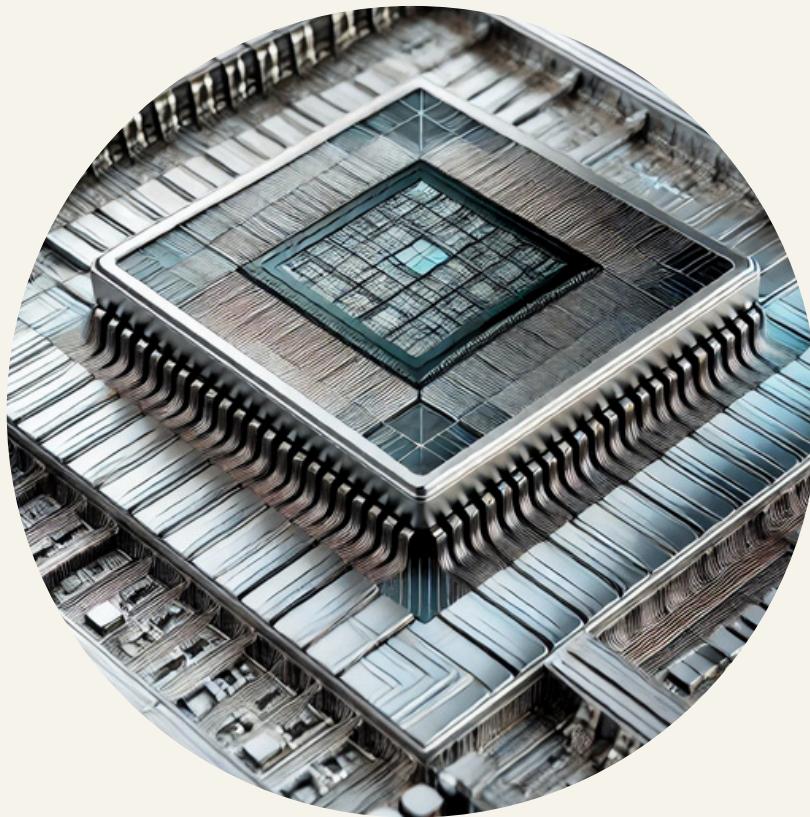
## COST



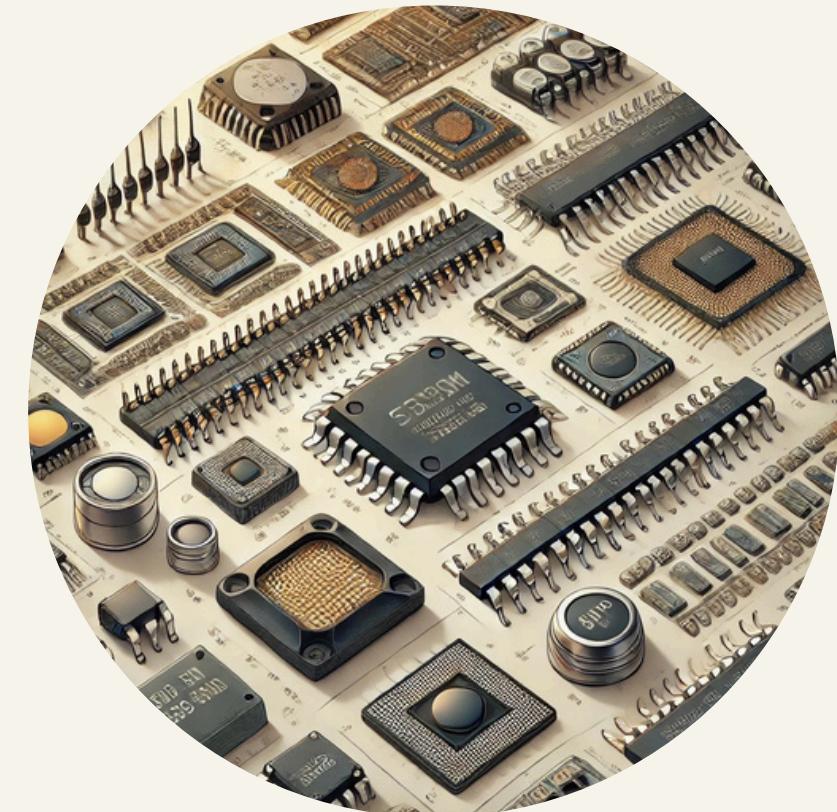
No	Necessary Material	Unit Price
1	Milling Machine	2500 Euro
2	Fuming Nitric Acid	200 Euro
3	Viton Gloves	100 Euro
4	Fume Hood	1400 Euro
5	Other Equipments	50 Euro
	<b>TOTAL</b>	<b>4250 Euro</b>



# FUTURE WORK



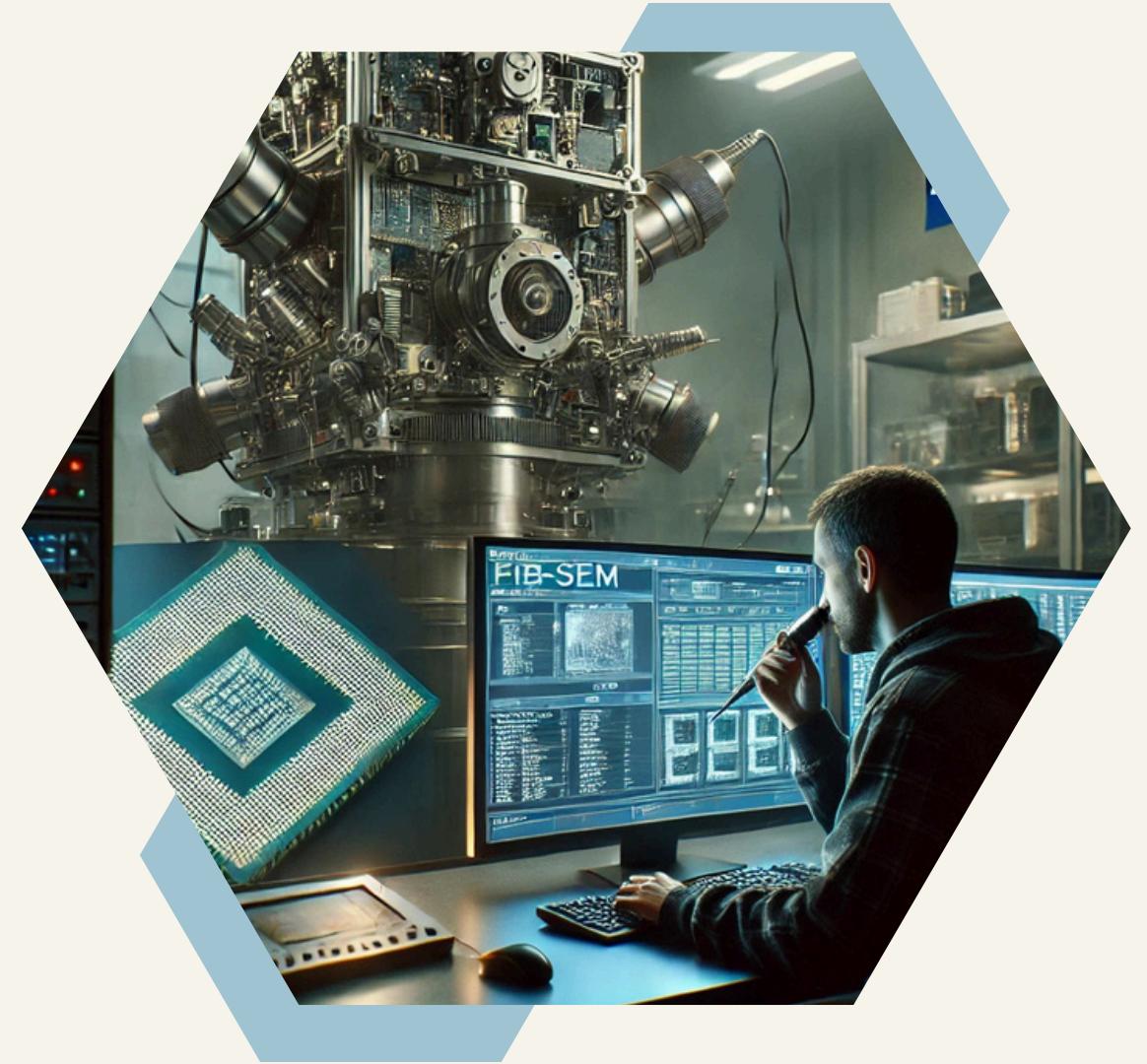
different wirebond types



different packaging types



# FIELDS OF RESEARCH



Side Channel Analysis

Laser Fault Injection

FIB-SEM

# ACKNOWLEDGMENT



# Q&A





ISC Türkiye 2024 | 17 Ekim 2024

**THANKS!**