Black-box Laser Fault Injection on a Secure Memory

Olivier Hériveaux

Ledger

Secret protection in embedded systems

Microcontrollers

FLASH memory, basic readout protection fuses
Low-cost
Low resistance against hardware attacks

Secure Elements

Physical attacks counter-measures
Evaluated by accredited labs
Restricted access (JCVM, NDA, ...)

Microchip ATECC508A

Secure memory
IoT applications
Easy access, no NDA
Is this secure ?

Coldcard Wallet

Bitcoin hardware wallet

Version Mk2 studied

STM32L4 Microcontroller

Main firmware

⇅

ATECC508A

Stores the "Seed" (private key)
Protected with authentication

ATECC508A

Reduced software attack surface

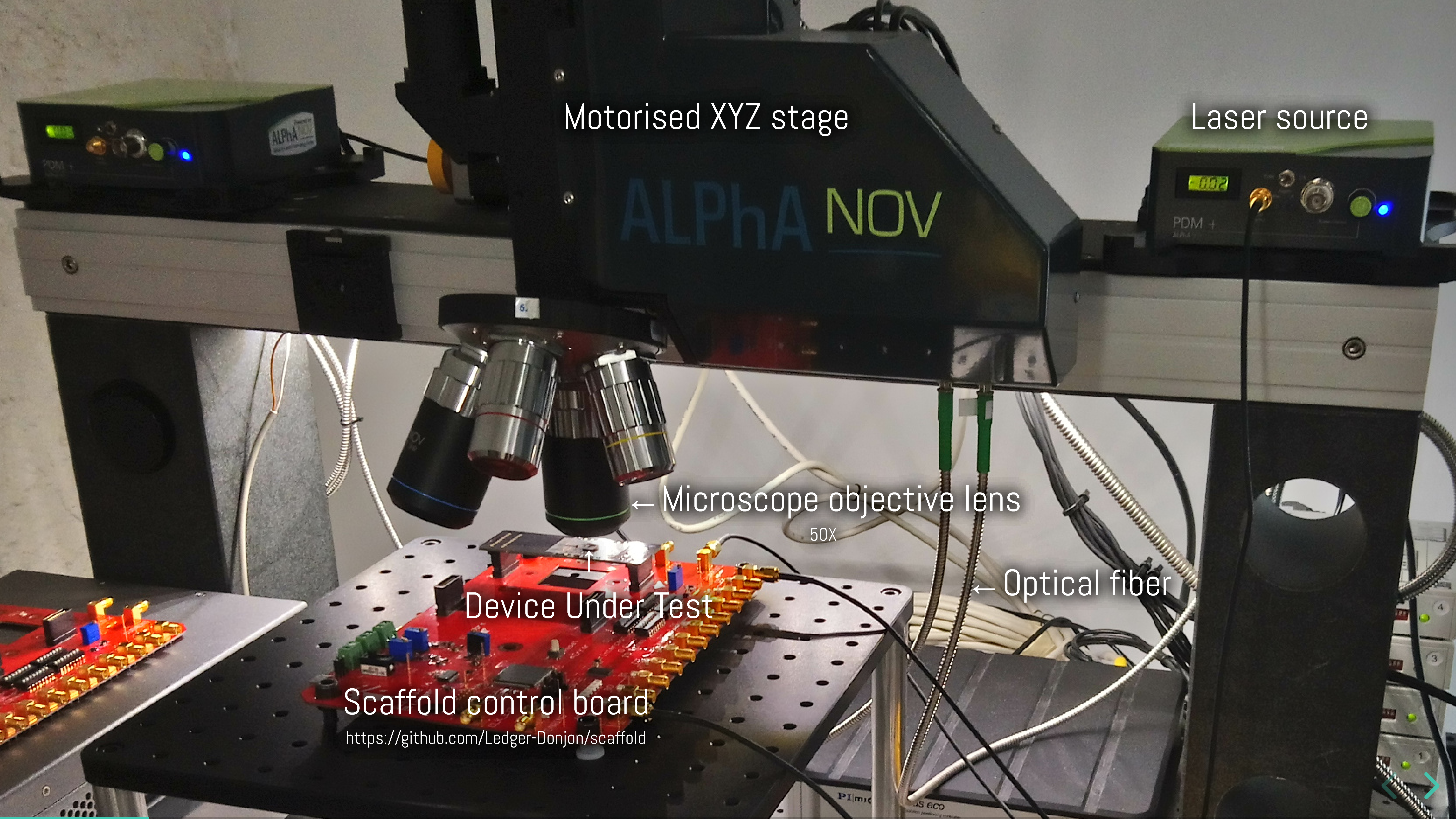
Confidential firmware

Voltage glitch sensors

Top-metal shield

Internal clock generator

No laser counter-measures


Motorised XYZ stage
Laser source
ALPhA NOV
PDM +
← Microscope objective lens
50X
← Optical fiber
Device Under Test
Scaffold control board
https://github.com/Ledger-Donjon/scaffold

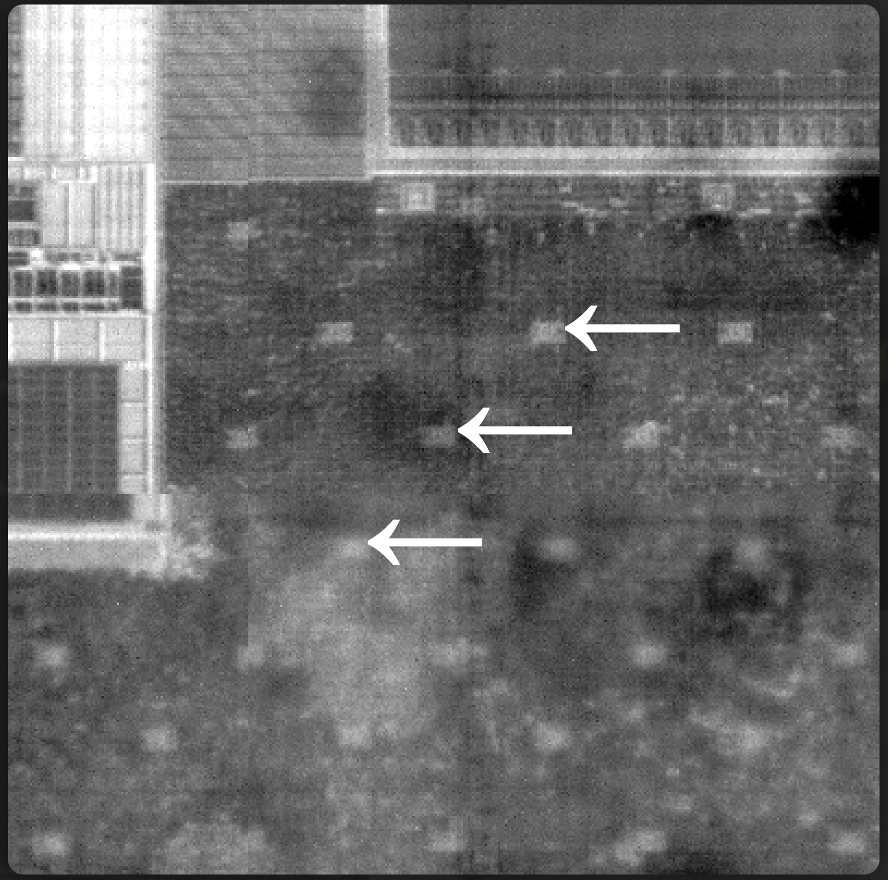
Silicon is transparent to infra-red light

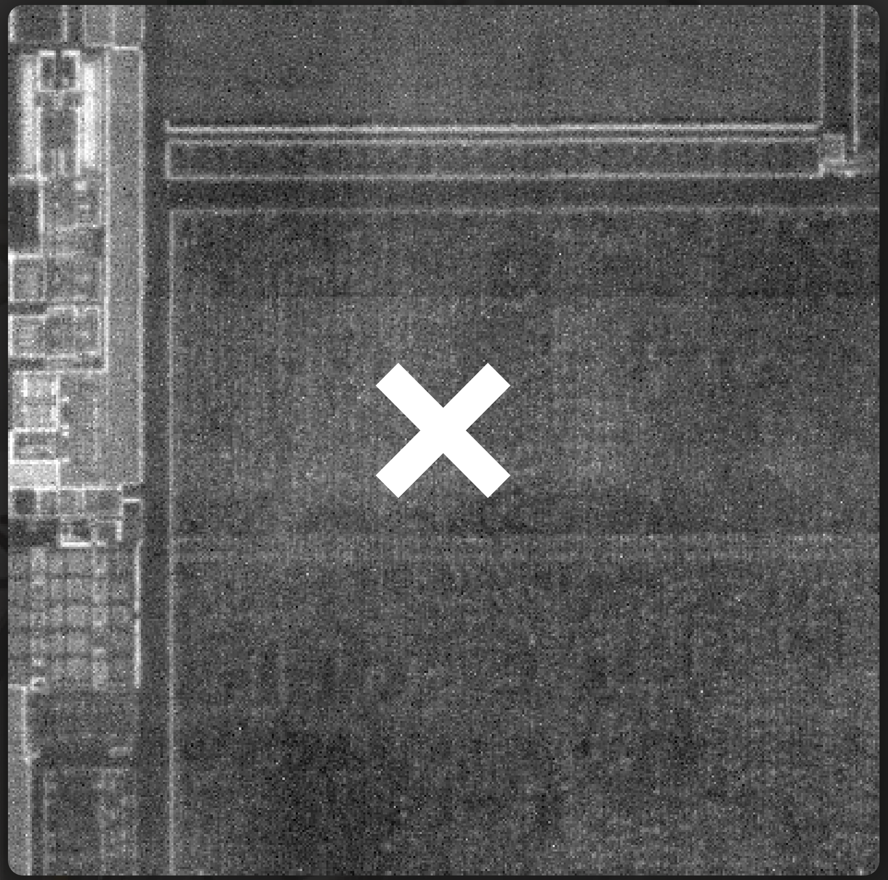
Integrated circuits are photosensitive

Light can enable transistors conduction…

… hence introducing computation errors!

Laser is a powerful and semi-invasive tool





What's the plan?

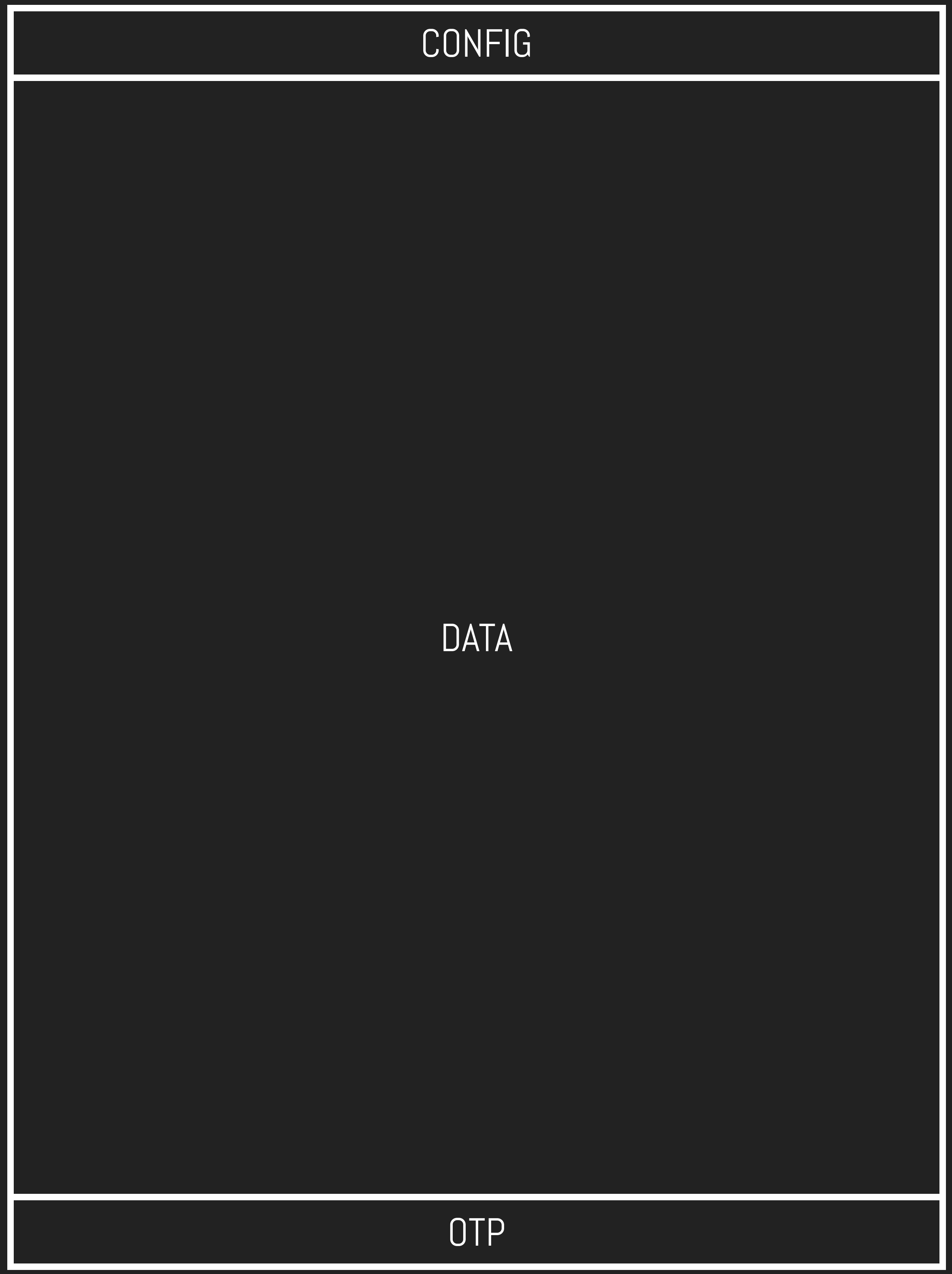
Identify assets and seek an attack path

Prepare and instrument the sample

Target

Test

ATECC508A Memory Layout



ATECC508A Memory Layout

CONFIG	
#0 - 36 bytes	#1 - 36 bytes
#2 - 36 bytes	#3 - 36 bytes
#4 - 36 bytes	#5 - 36 bytes
#6 - 36 bytes	#7 - 36 bytes
#8 - 416 bytes	
#9 - 72 bytes	
#10 - 72 bytes	
#11 - 72 bytes	
#12 - 72 bytes	
#13 - 72 bytes	
#14 - 72 bytes	
#15 - 72 bytes	
OTP	

ATECC508A Memory Layout

CONFIG	
Unused	Pairing secret
Anti-phishing	PIN1 hash
PIN2	PIN1 try counter
PIN2 try counter	PIN3
PIN4	
Seed1	
Seed2	
Seed3	
Seed4	
BrickMe	
Firmware hash	
Unused	
OTP	

Accessing data slots

ReadMemory command:

03	07	02	82	1800	0a78
Command	Length	OpCode Read Memory	DATA zone + Length	Adresse	CRC

Response when access granted:

23	303132333435363738396162636465666768696a6b6c6d6e6f70717273747576	384a
Length	Data (32 bytes)	CRC

Accessing data slots

ReadMemory command:

03	07	02	82	1800	0a78
Command	Length	OpCode Read Memory	DATA zone + Length	Adresse	CRC

Response when access denied:

1	10	384a
Length	Error code EXECUTION_ERROR	CRC

PIN1 data slot configuration

Raw	0x8f43
Write config	Encrypt
Write key	3
Read key	15
Is secret	Yes
Encrypt read	No
Limited use	No
No MAC	No

PIN1 data slot configuration

Raw	0x8f43
Write config	Encrypt
Write key	3
Read key	15
Is secret	Yes No
Encrypt read	No
Limited use	No
No MAC	No

Code hypothesis

```
config_address = get_config_address(slot);
config = eeprom_read(config_address);

if (!config.is_secret){
    data_address = get_data_address(slot);
    data = eeprom_read(data_address);

    if (config.encrypt_read)
        encrypt(data);

    i2c_send(data);
} else {
    i2c_send(EXECUTION_ERROR);
}
```

Code hypothesis

```
config_address = get_config_address(slot);
config = eeprom_read(config_address);

if (!config.is_secret){
    data_address = get_data_address(slot);
    data = eeprom_read(data_address);

    if (config.encrypt_read)
        encrypt(data);

    i2c_send(data);
} else {
    i2c_send(EXECUTION_ERROR);
}
```

Code hypothesis

```
config_address = get_config_address(slot);
config = eeprom_read(config_address);

if (!config.is_secret){
    data_address = get_data_address(slot);
    data = eeprom_read(data_address);

    if (config.encrypt_read)
        encrypt(data);

    i2c_send(data);
} else {
    i2c_send(EXECUTION_ERROR);
}
```

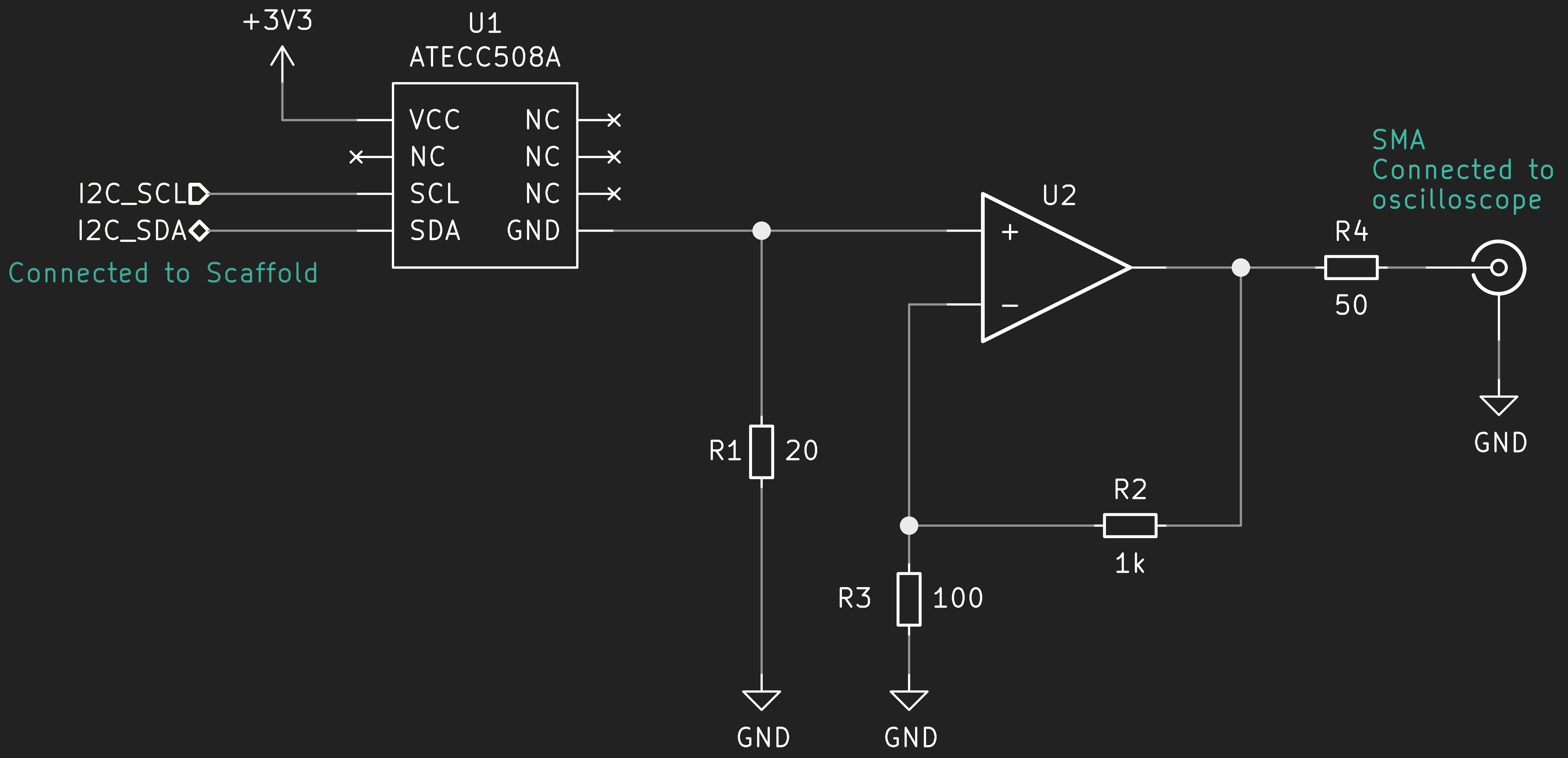
Code hypothesis

```
config_address = get_config_address(slot);
config = eeprom_read(config_address);

if (!config.is_secret){
    data_address = get_data_address(slot);
    data = eeprom_read(data_address);

    if (config.encrypt_read)
        encrypt(data);

    i2c_send(data);
} else {
    i2c_send(EXECUTION_ERROR);
}
```

When?

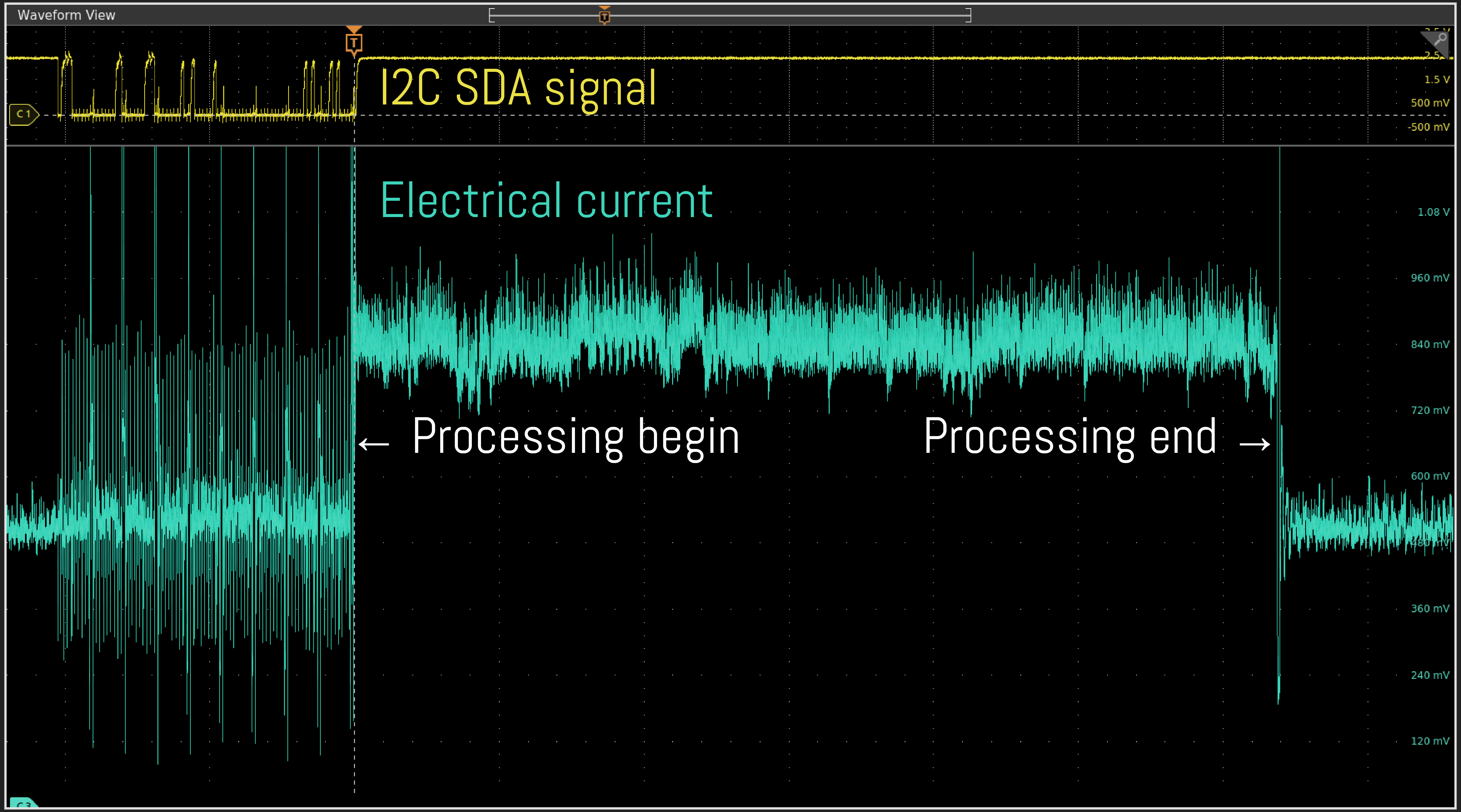
Power analysis

Circuit processing activity can be observed on the power trace



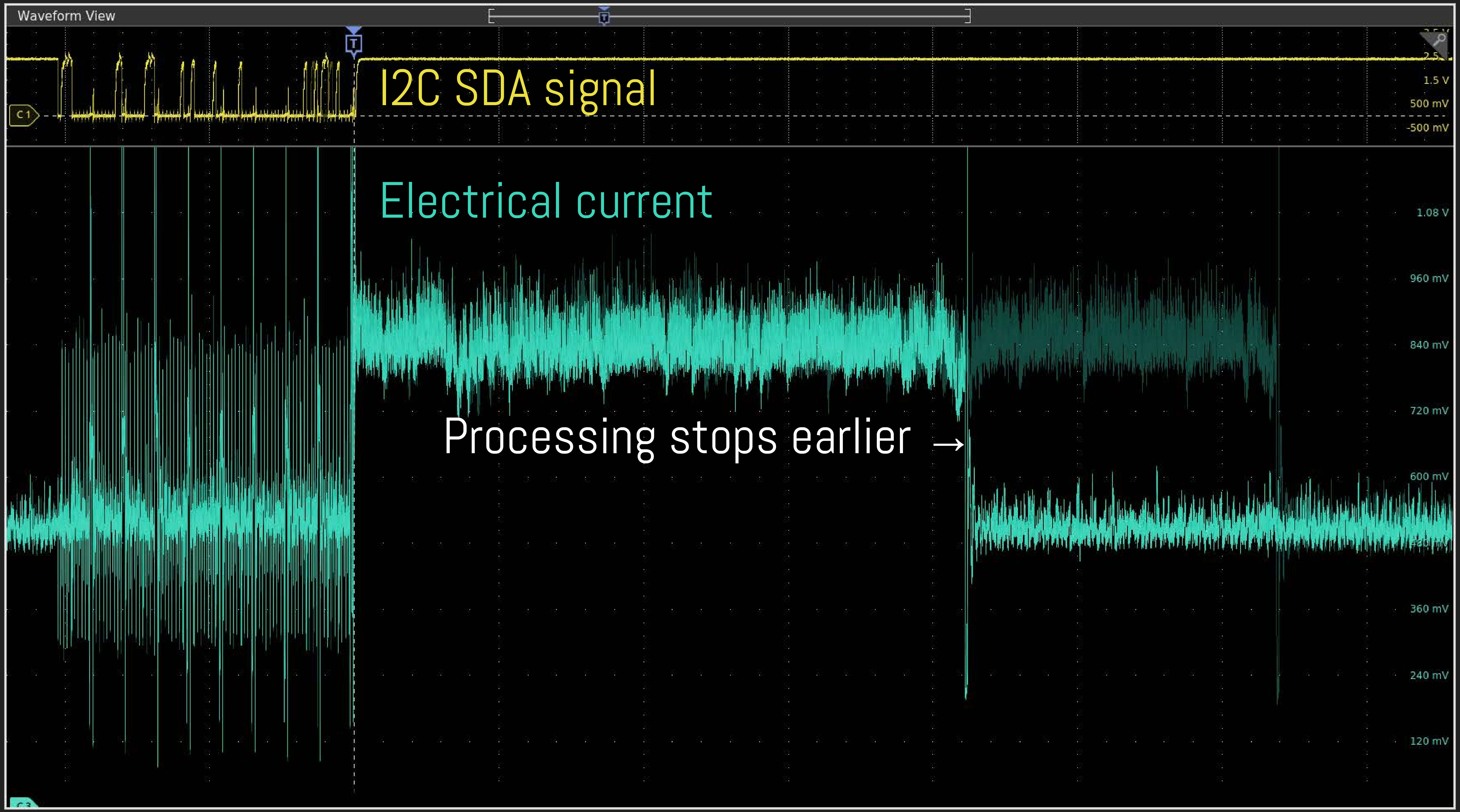
Power analysis

Reading a granted data slot



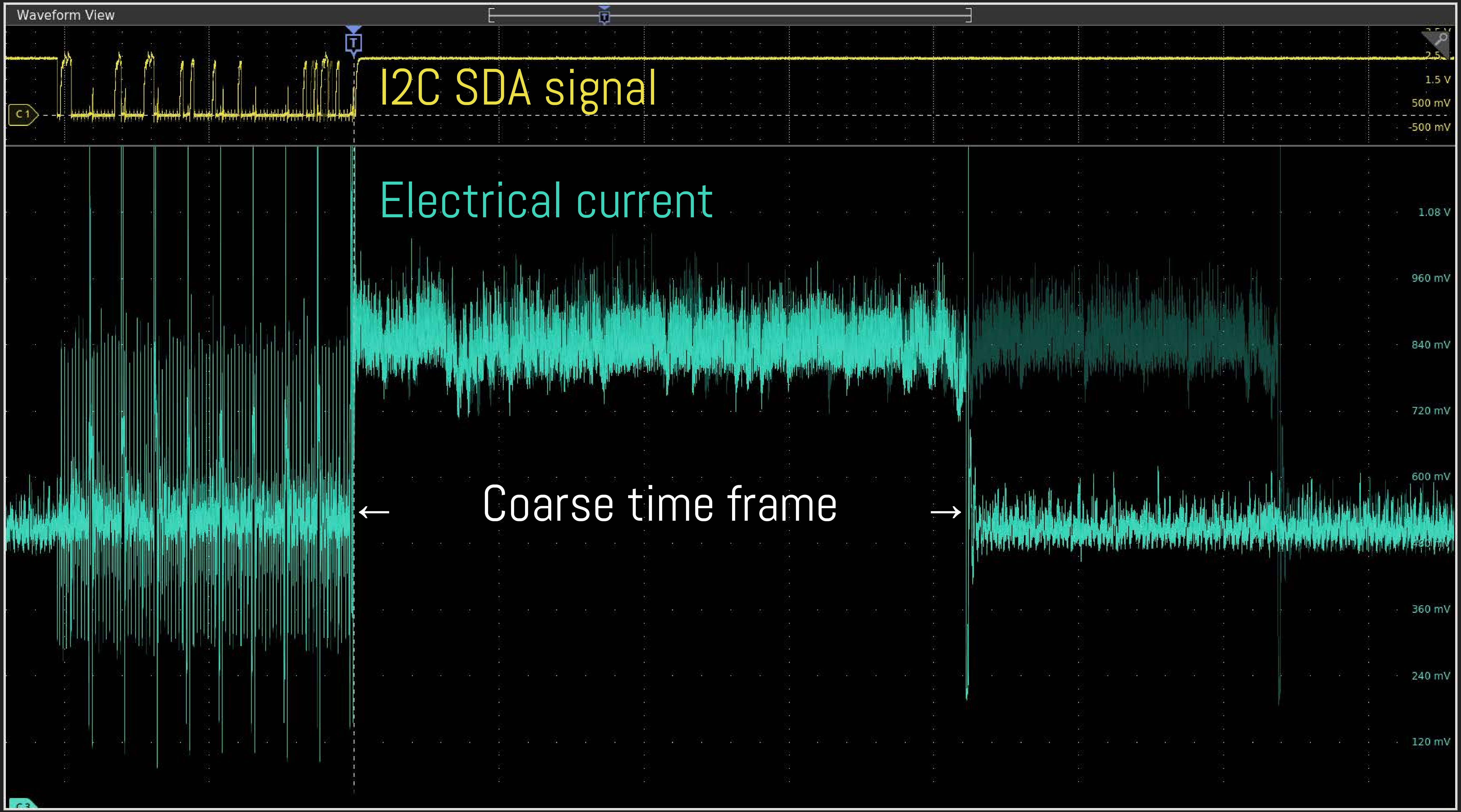
Power analysis

Reading a denied data slot



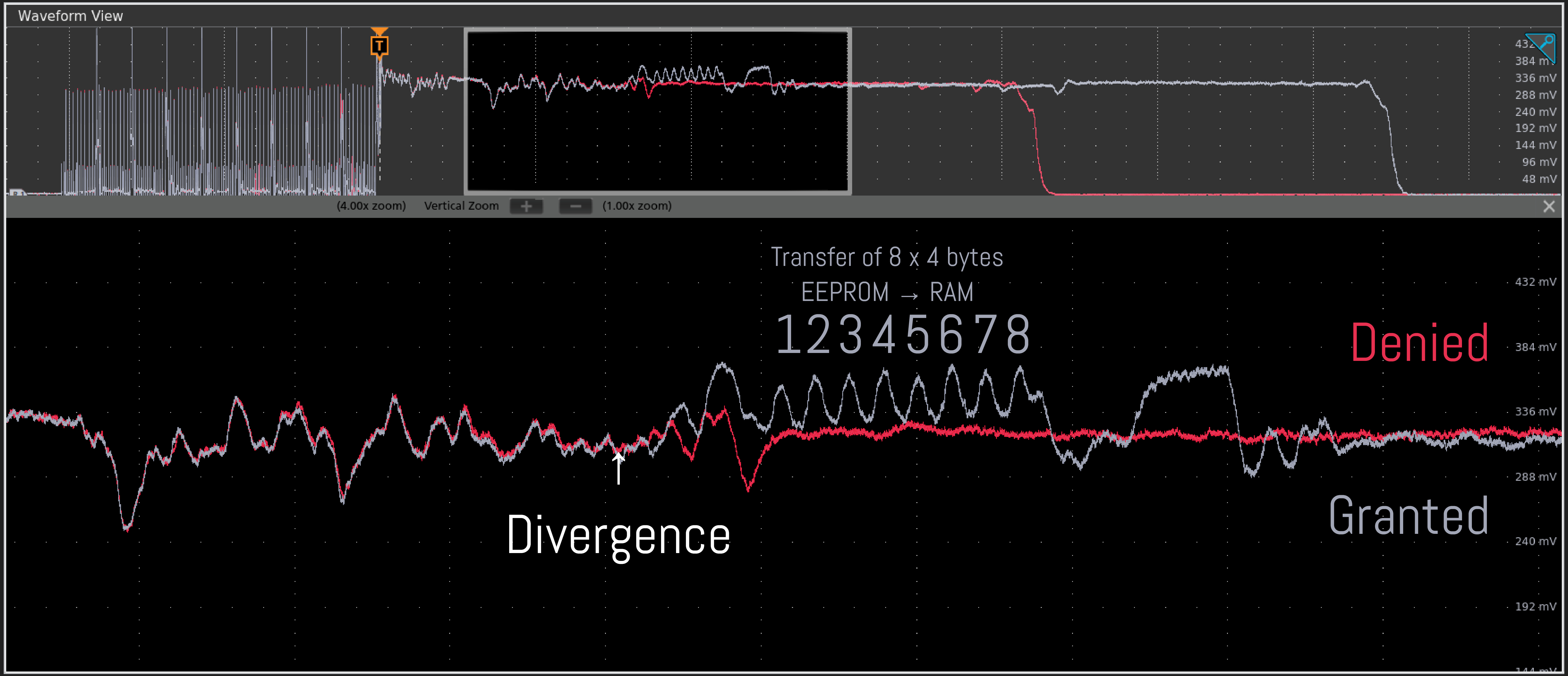
Power analysis

Reading a denied data slot



Power analysis

Comparison of averaged traces

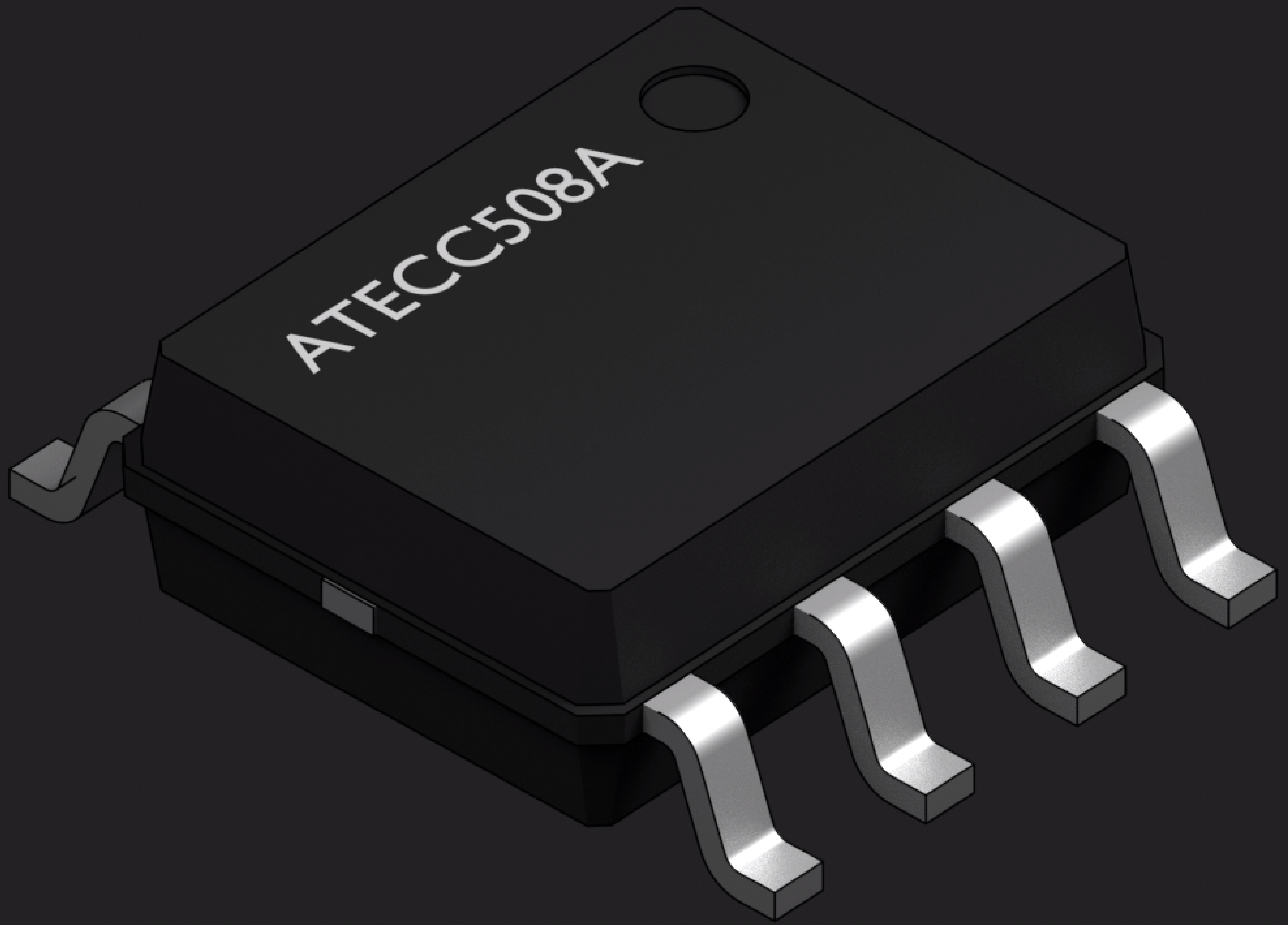


Power analysis

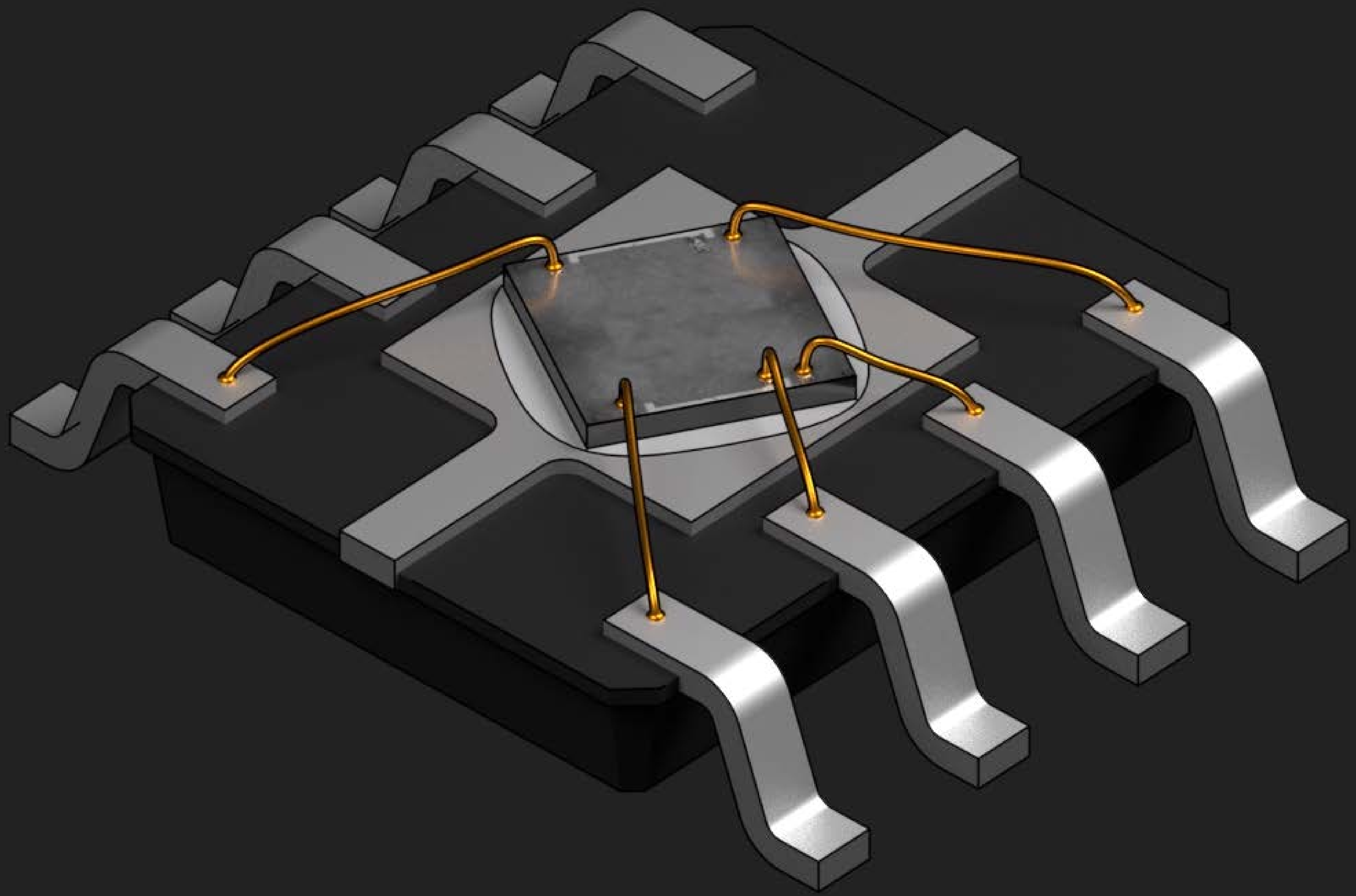
Comparison of averaged traces

Where?

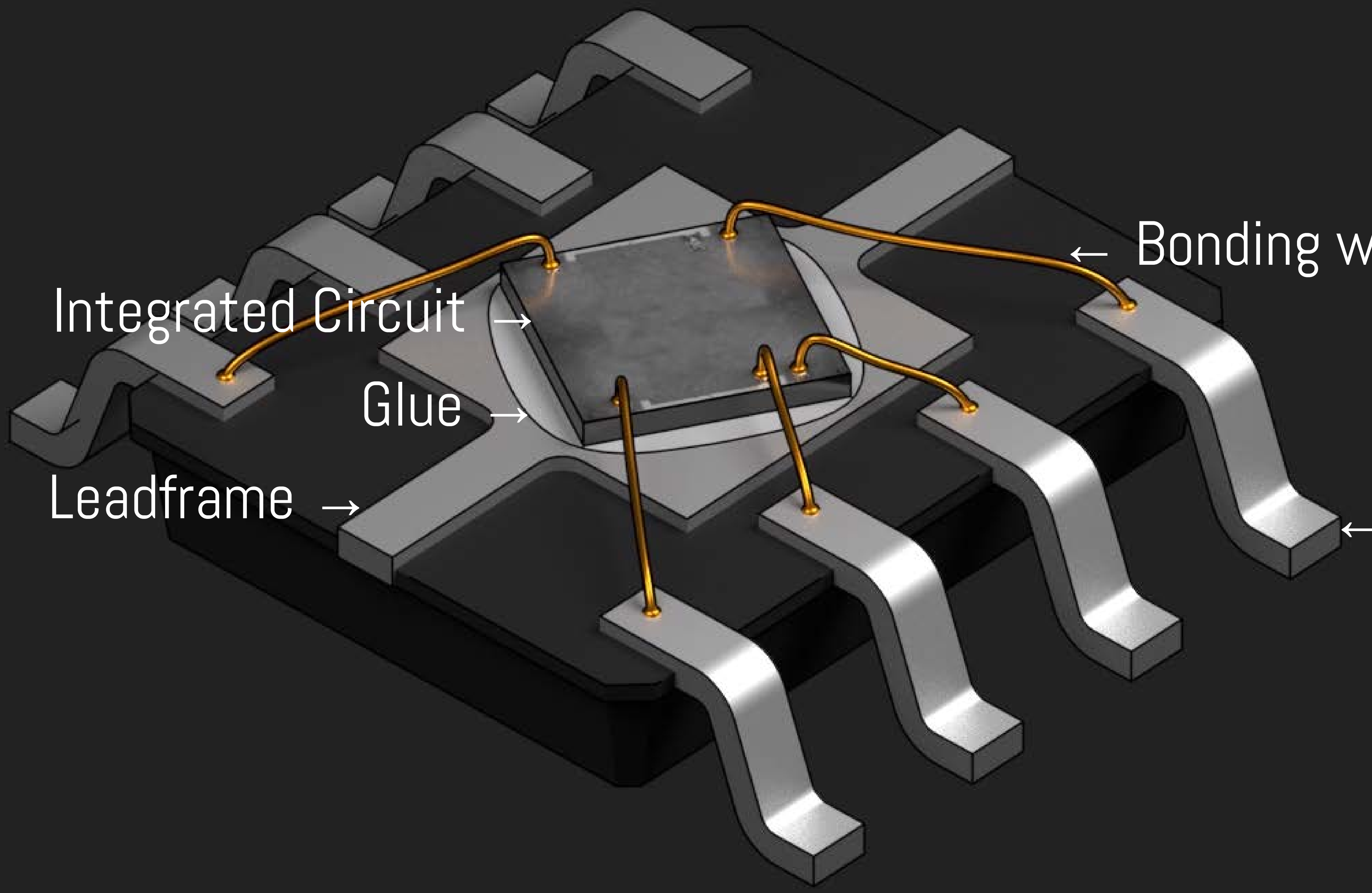
Circuit Dissection



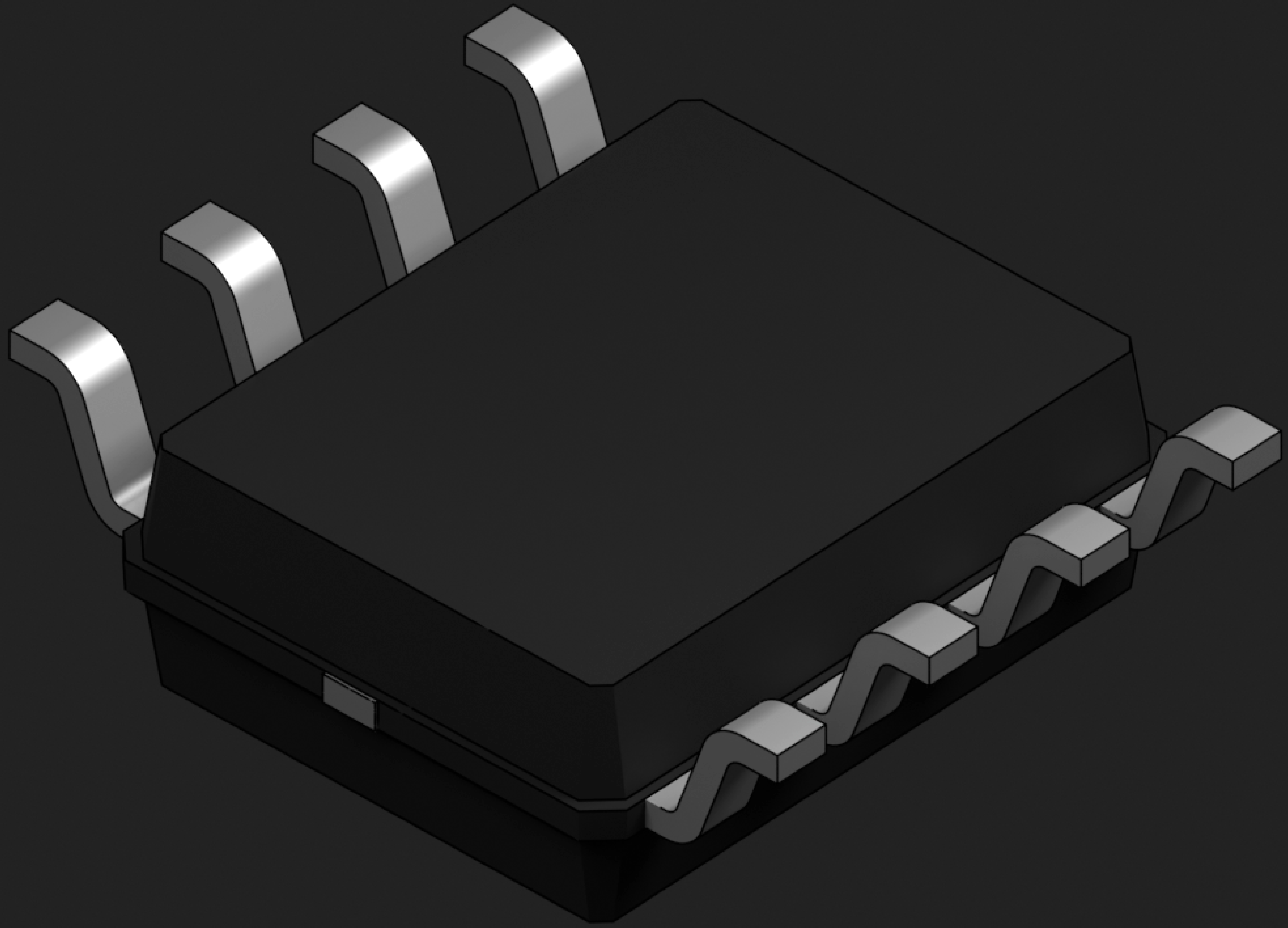
Circuit Dissection



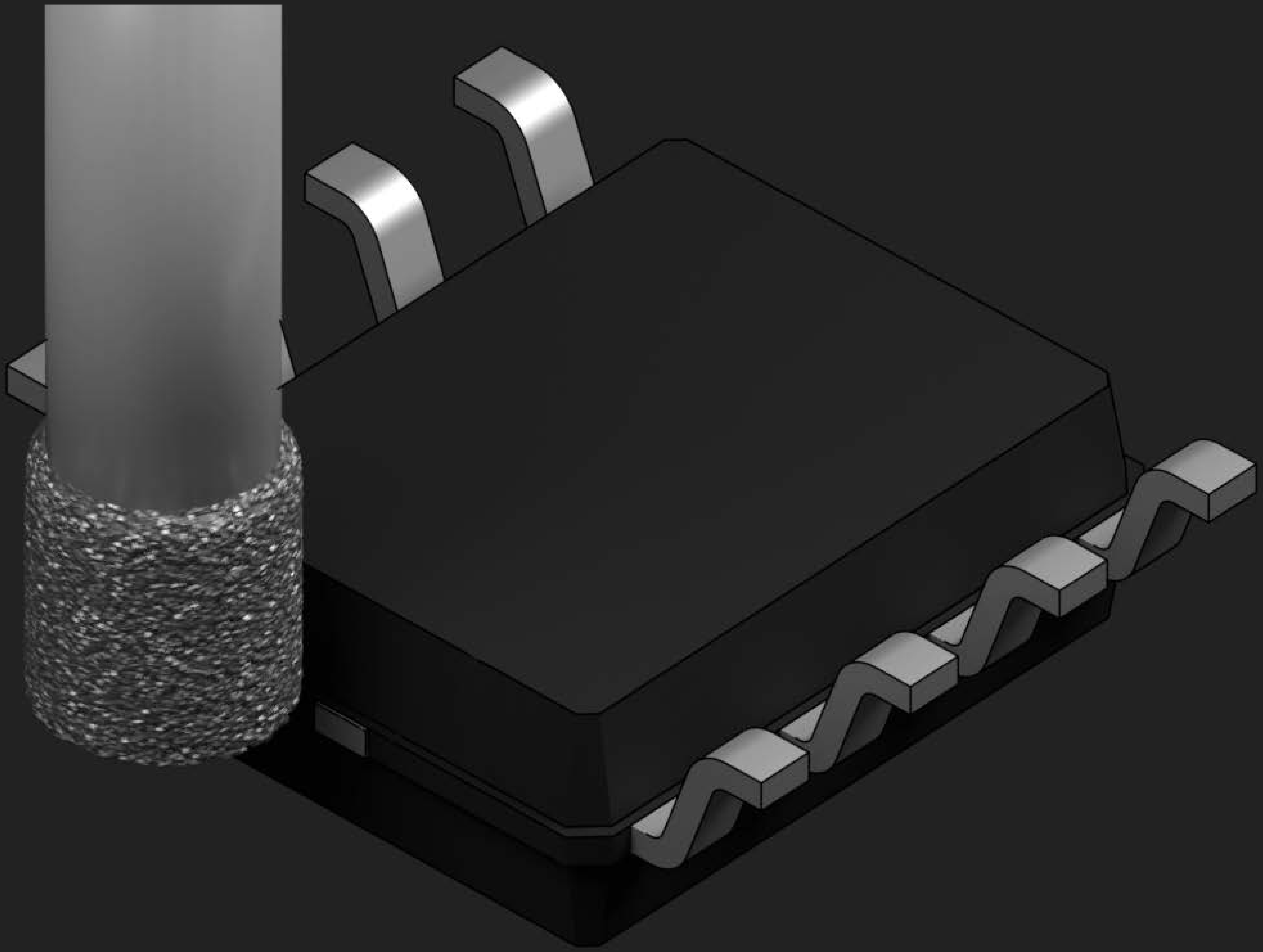
Circuit Dissection



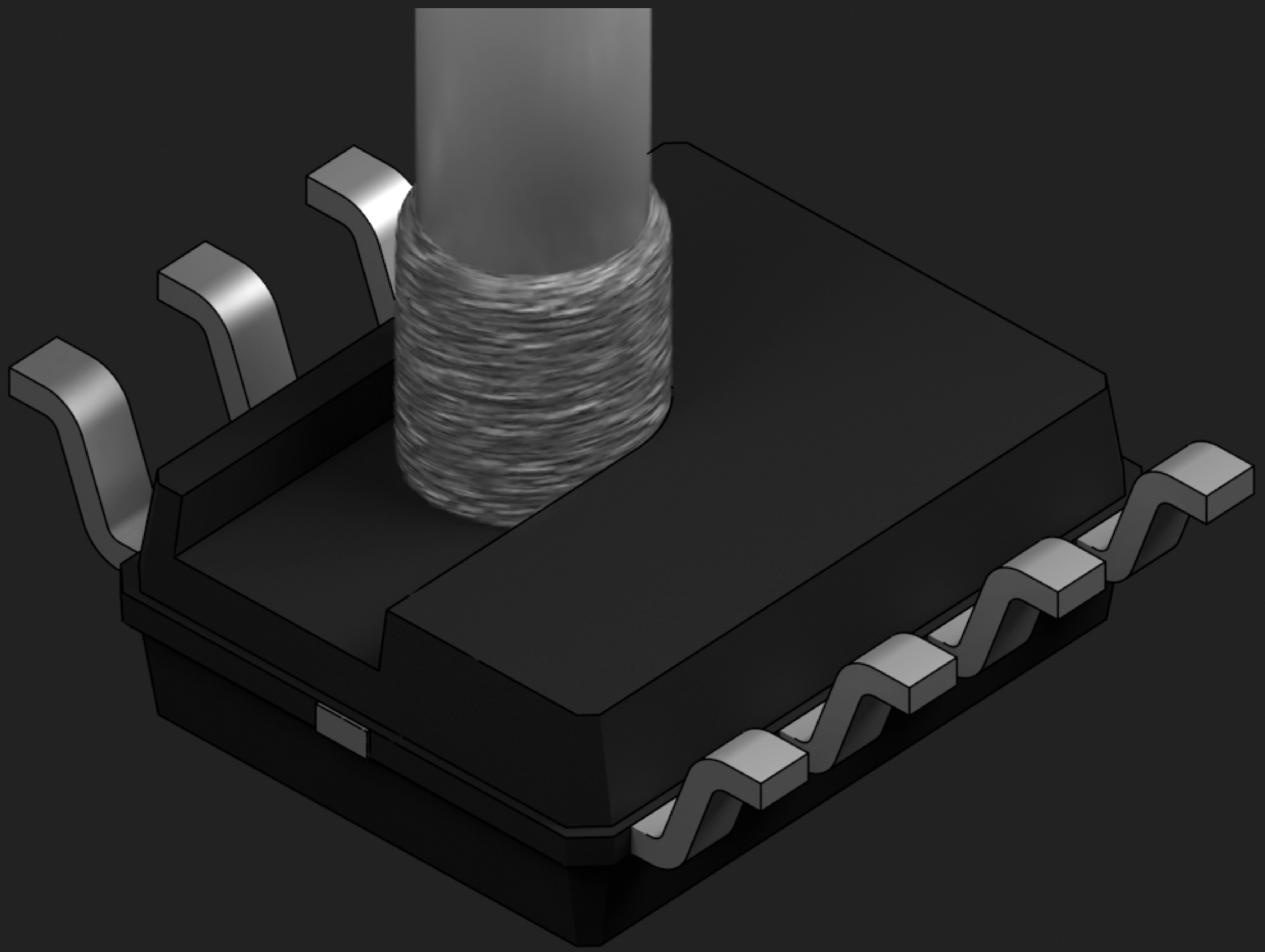
Backside decapsulation



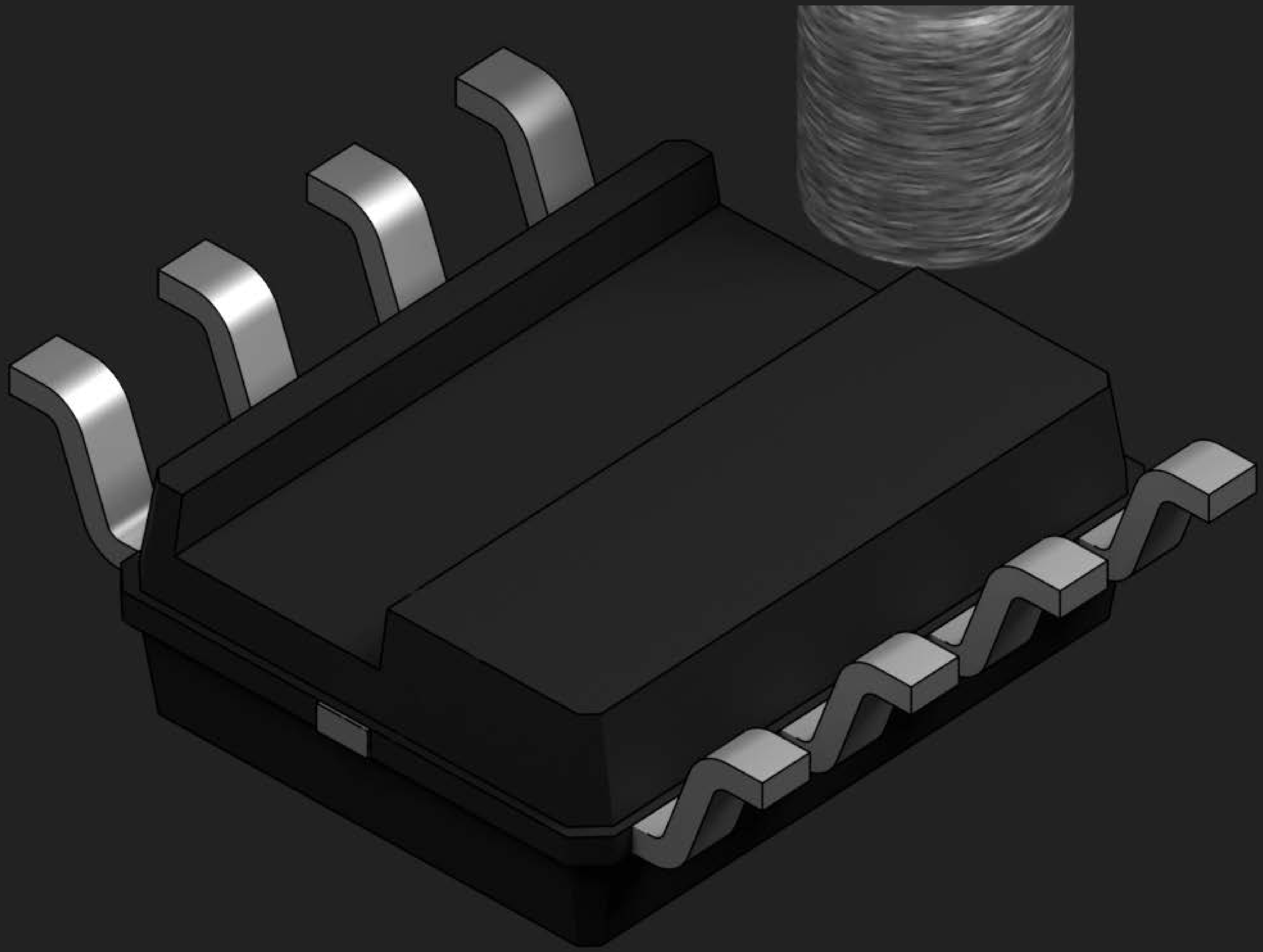
Backside decapsulation



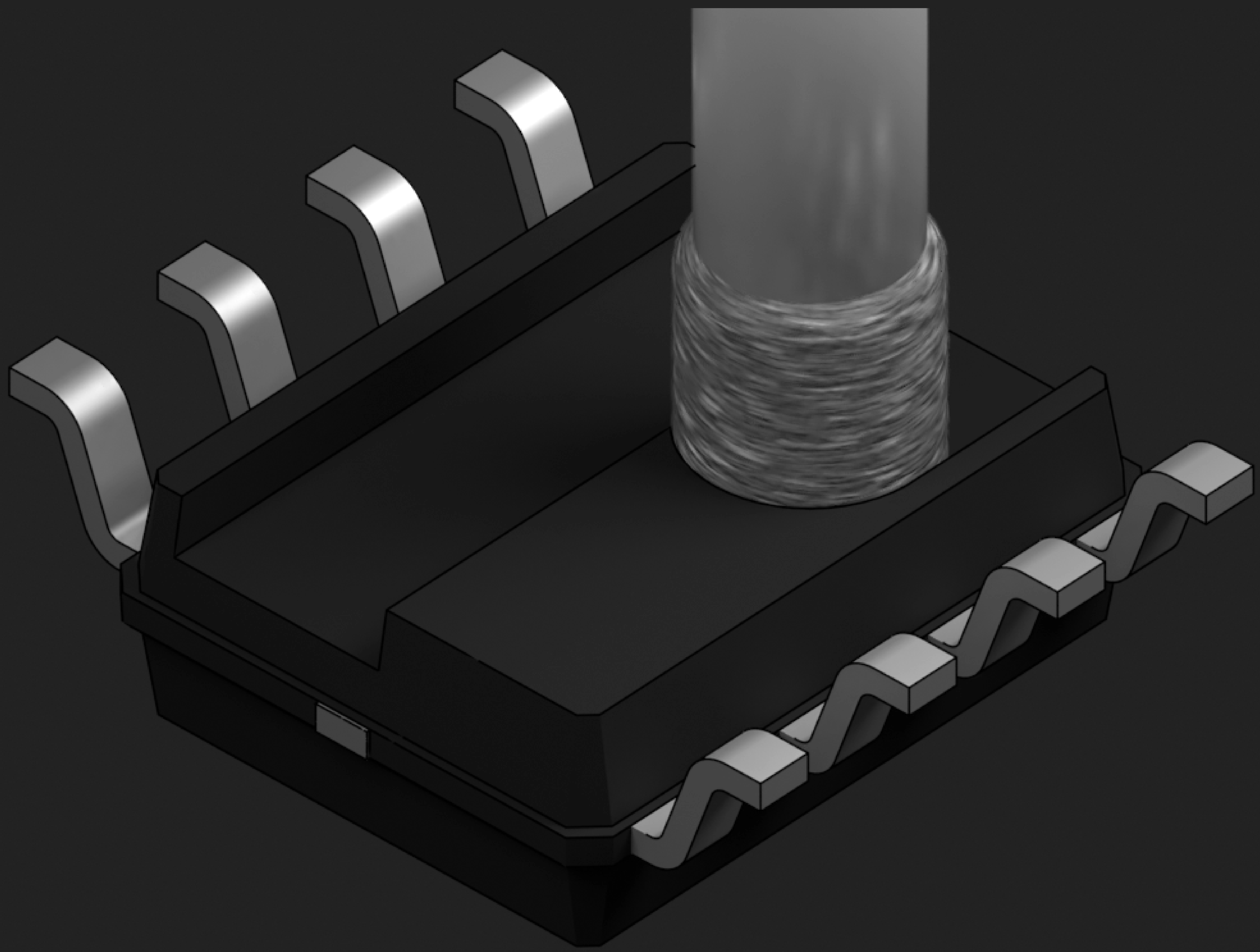
Backside decapsulation



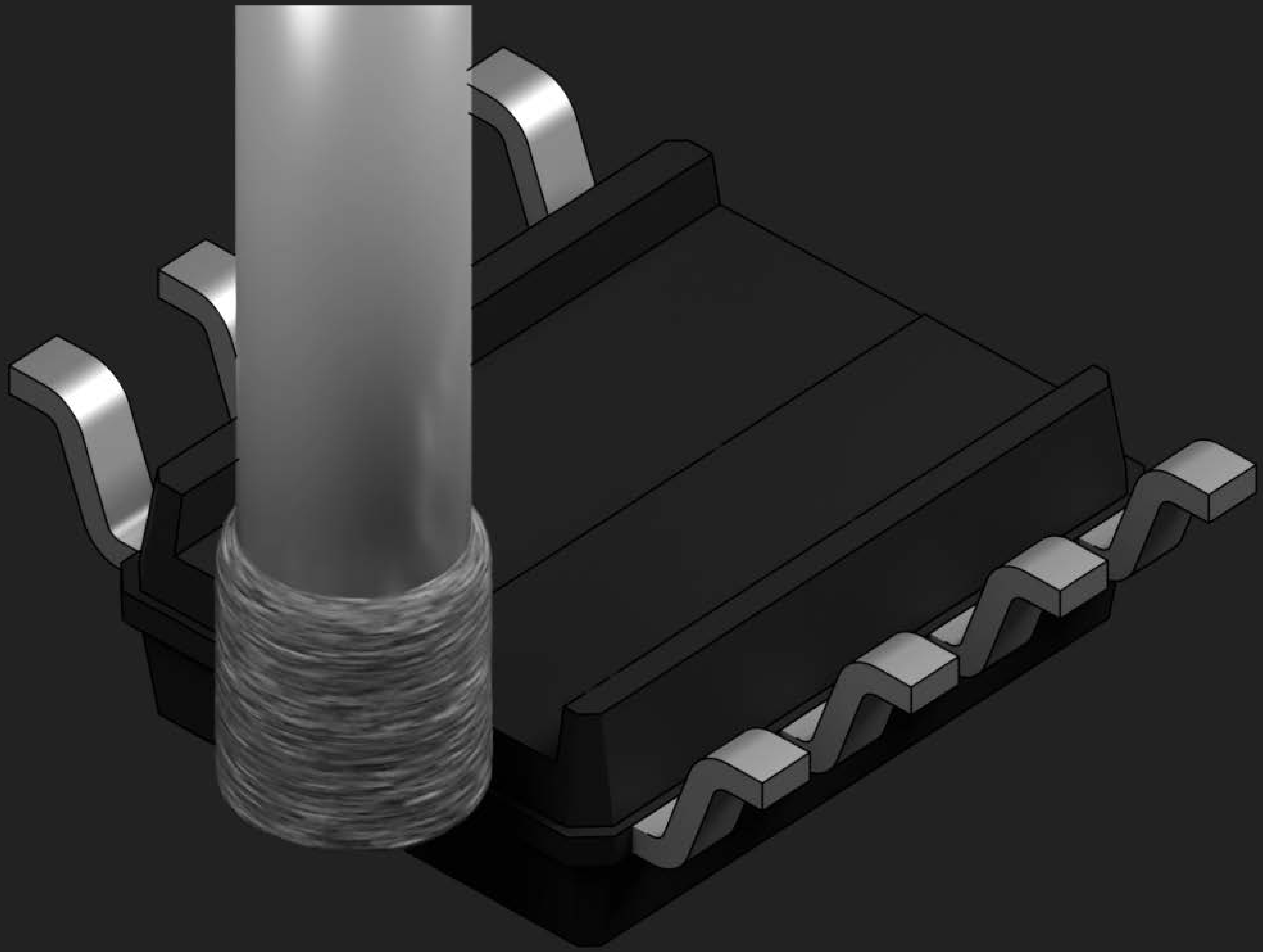
Backside decapsulation



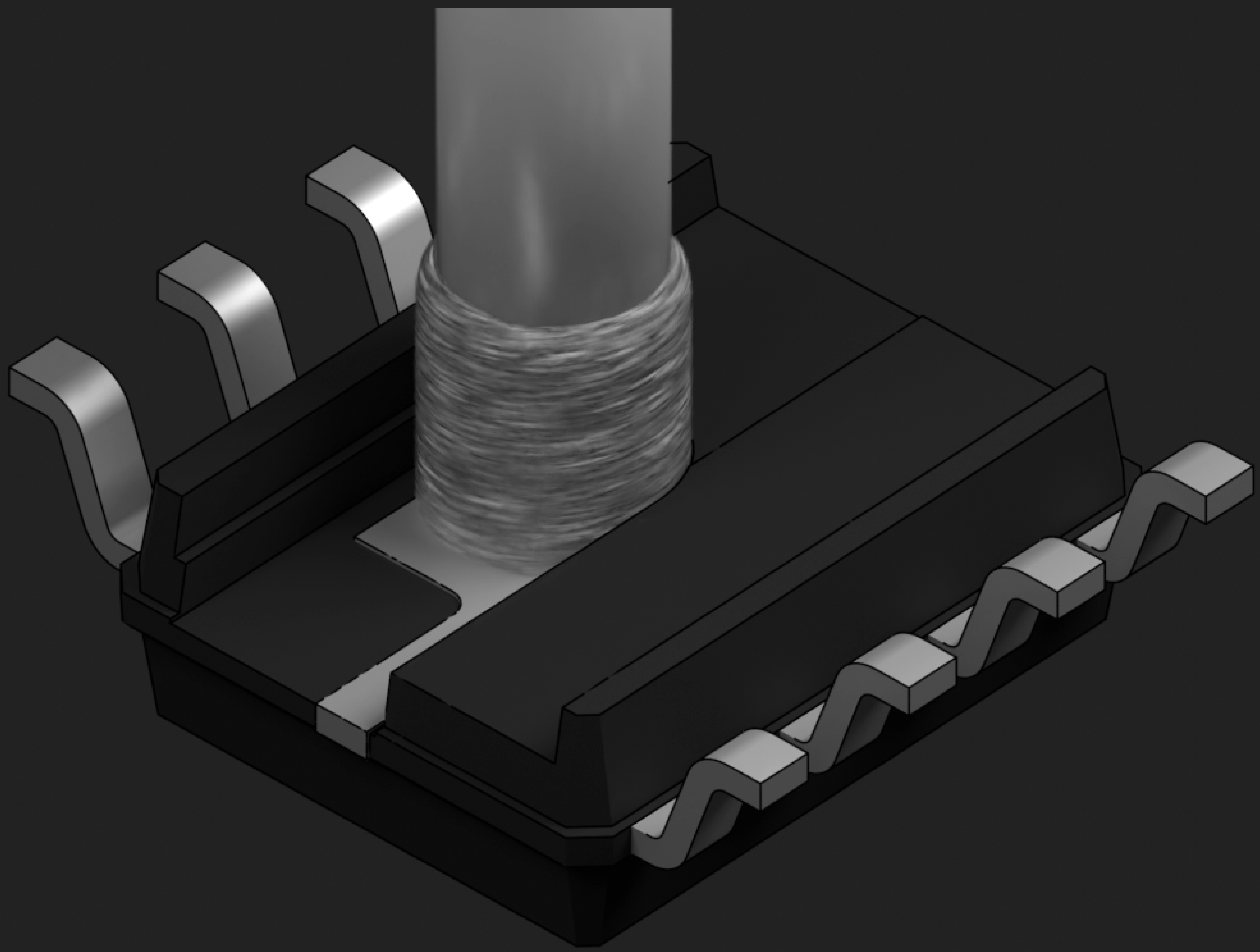
Backside decapsulation



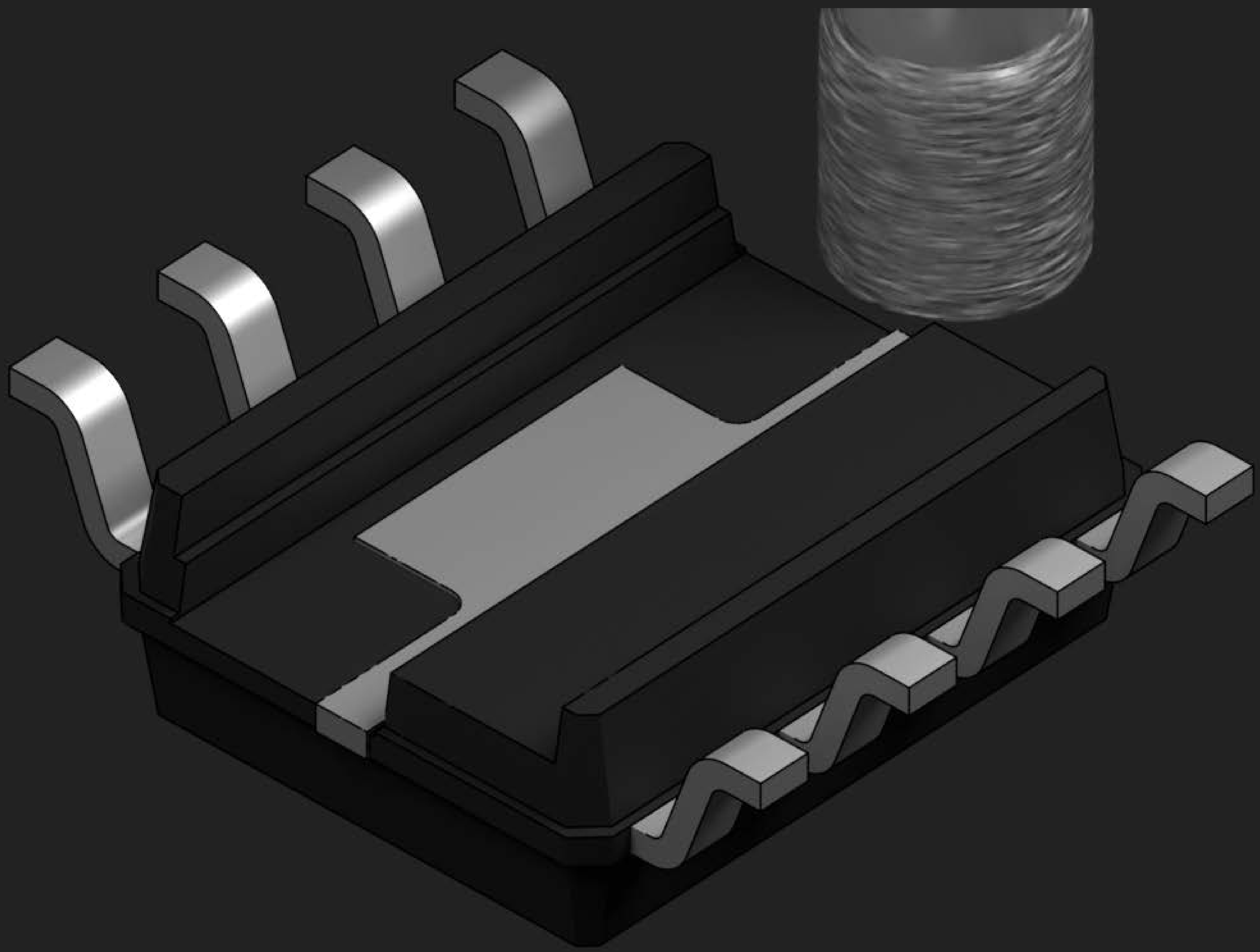
Backside decapsulation



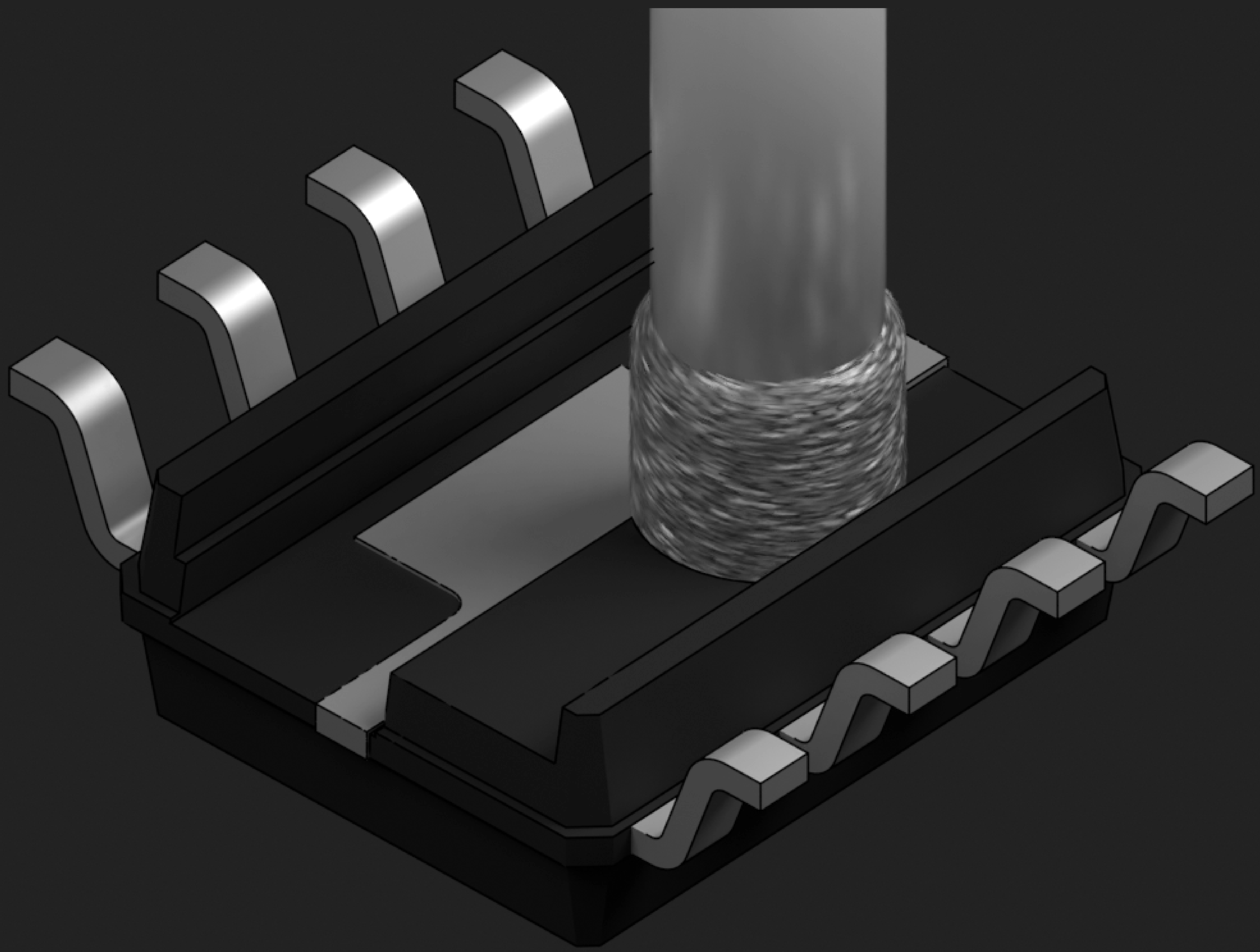
Backside decapsulation



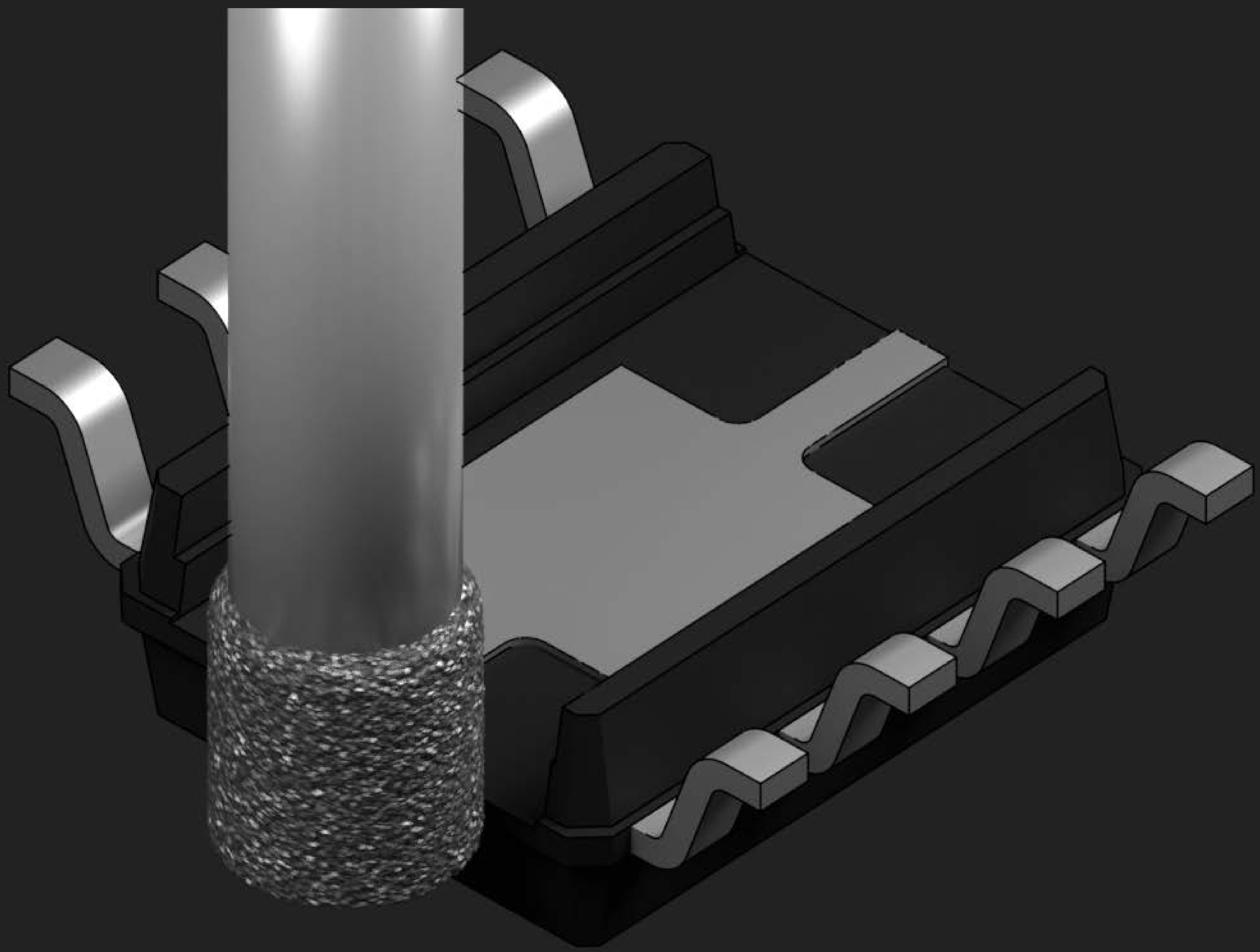
Backside decapsulation



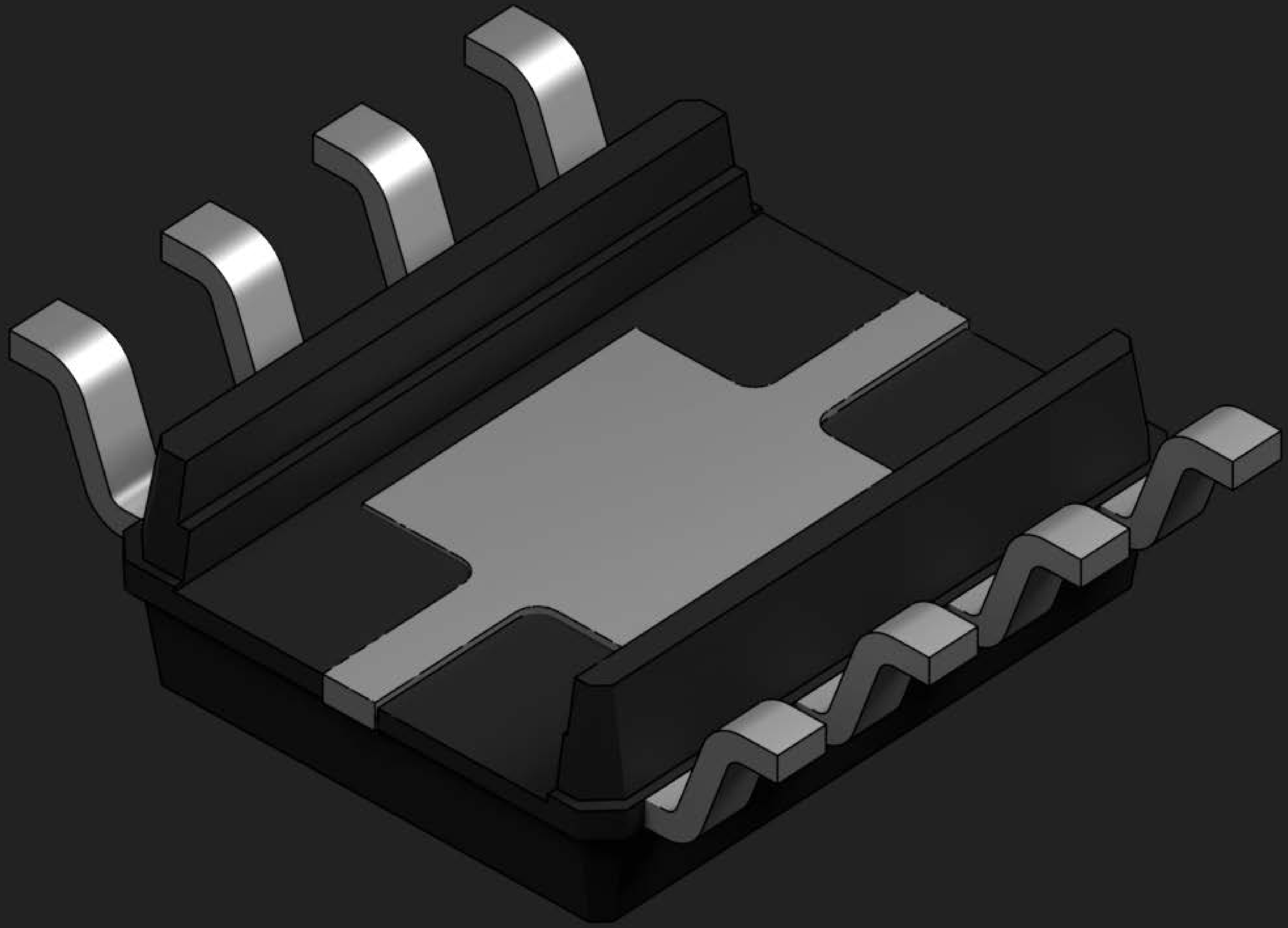
Backside decapsulation



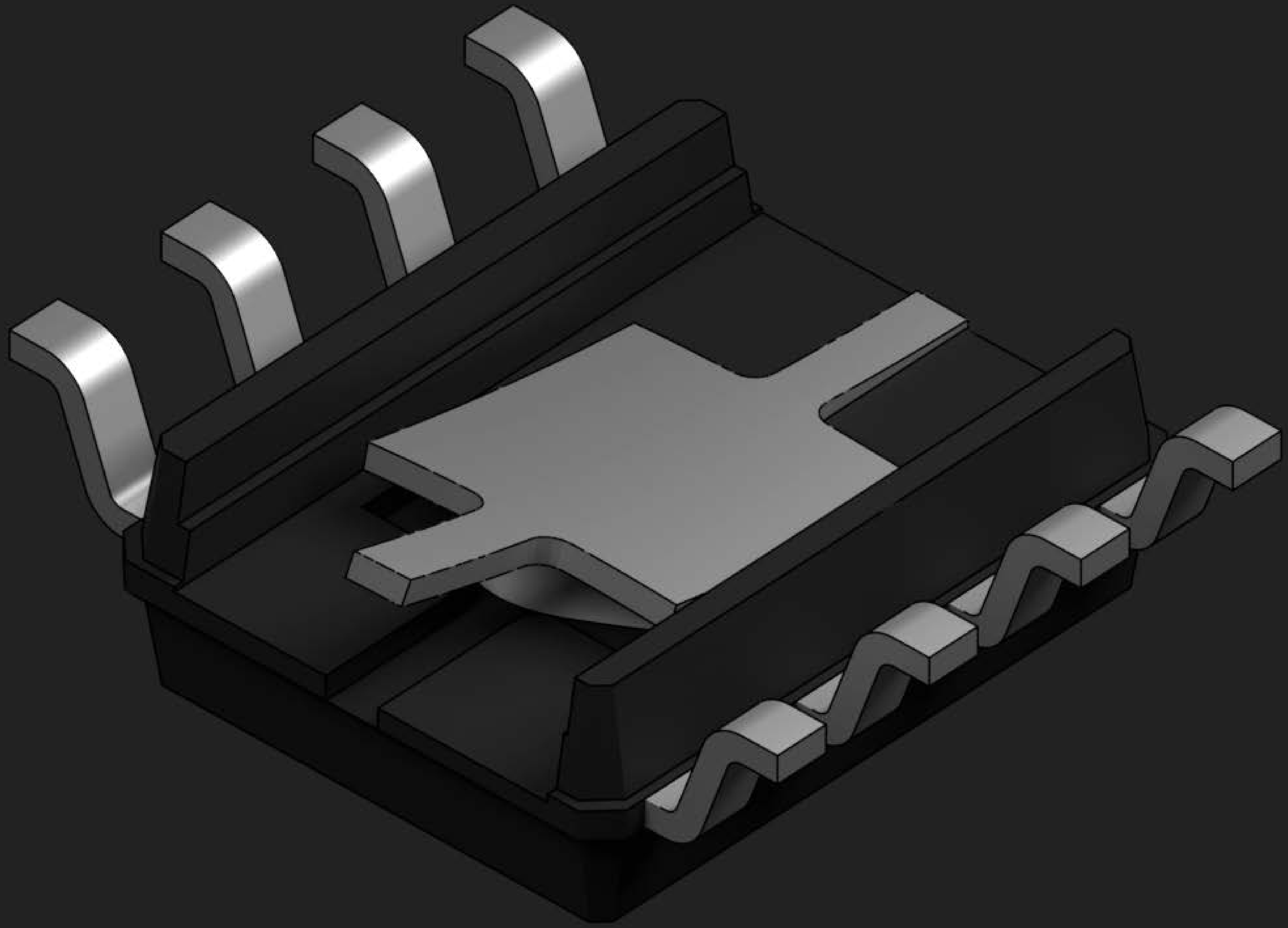
Backside decapsulation



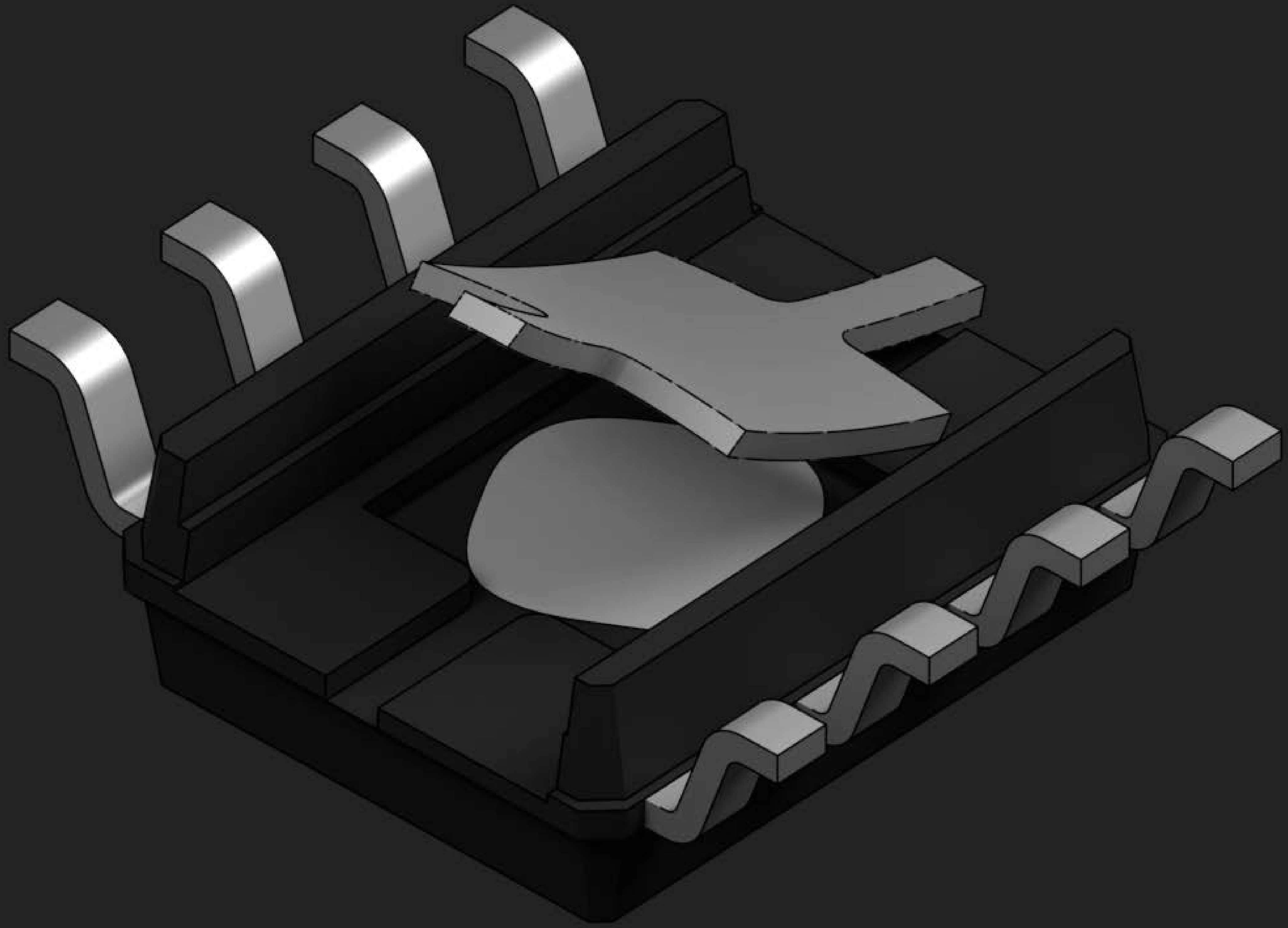
Backside decapsulation



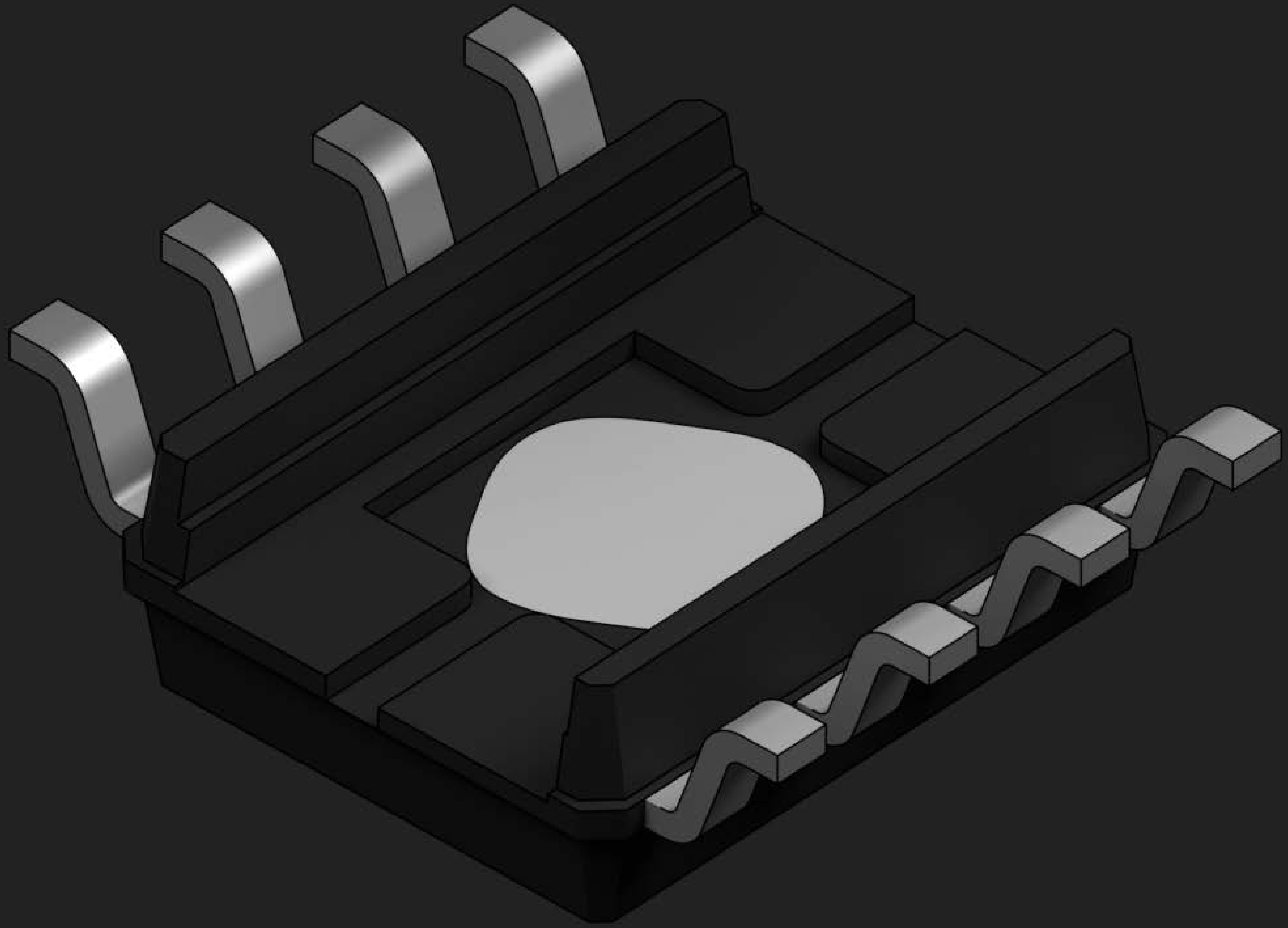
Backside decapsulation



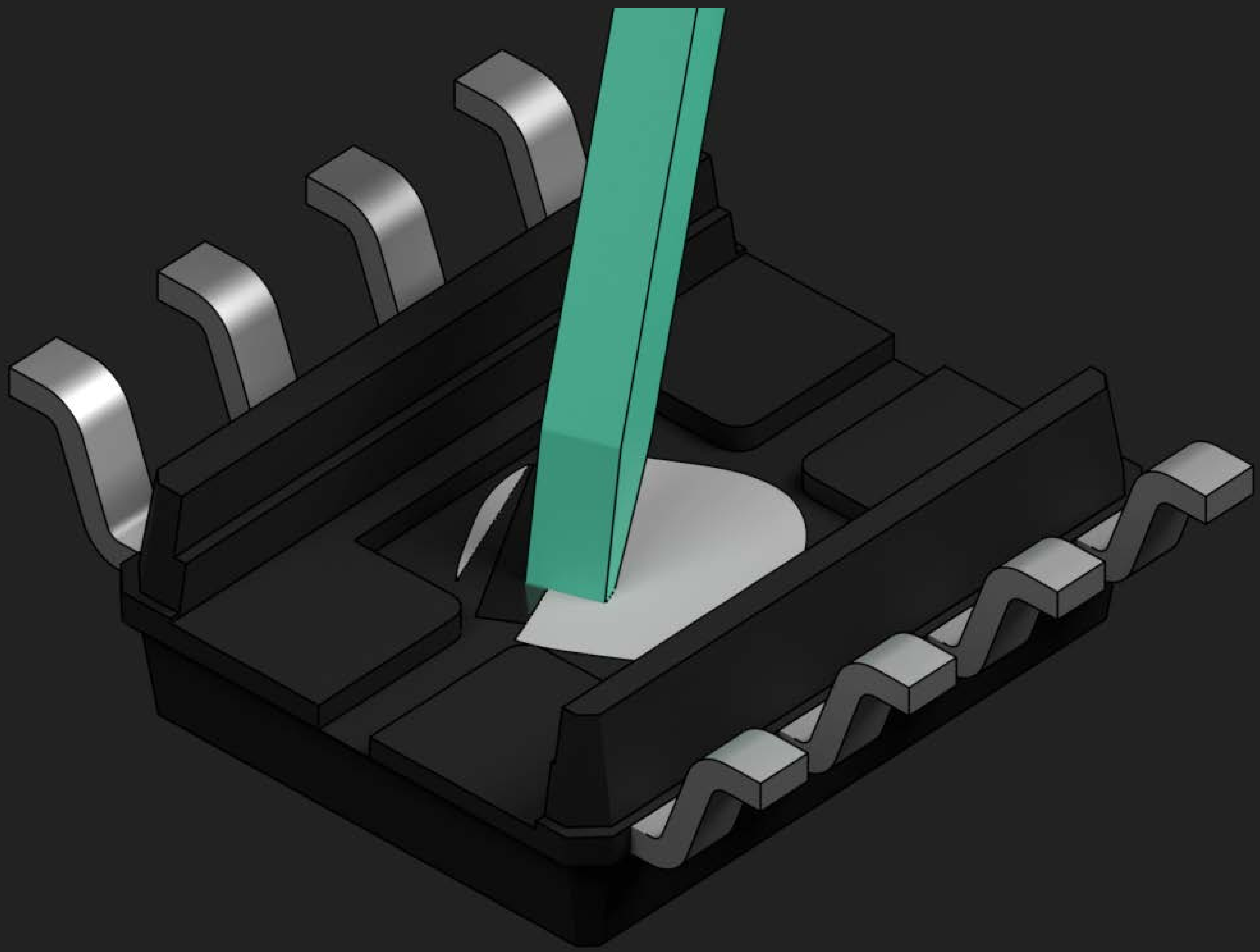
Backside decapsulation



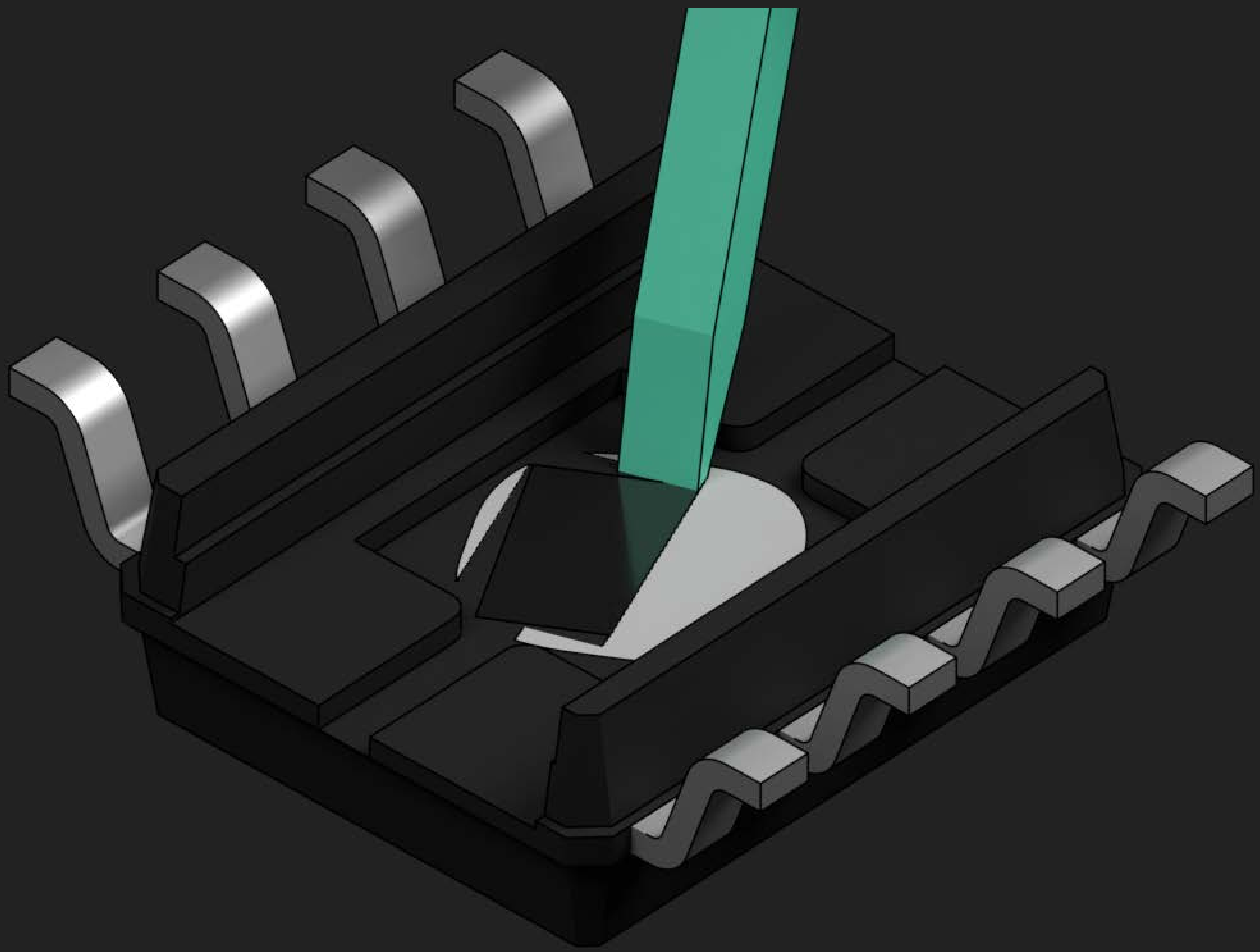
Backside decapsulation



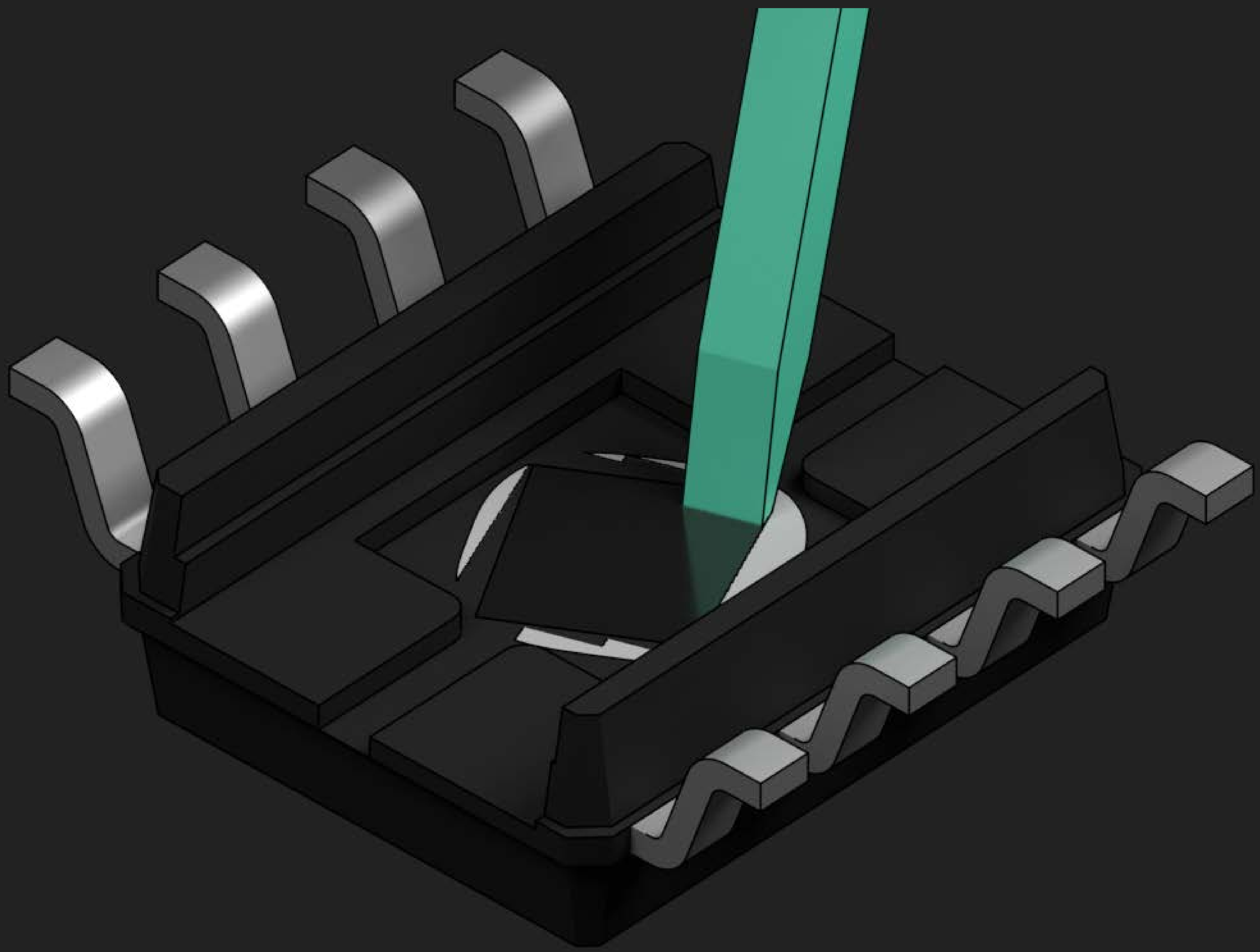
Backside decapsulation



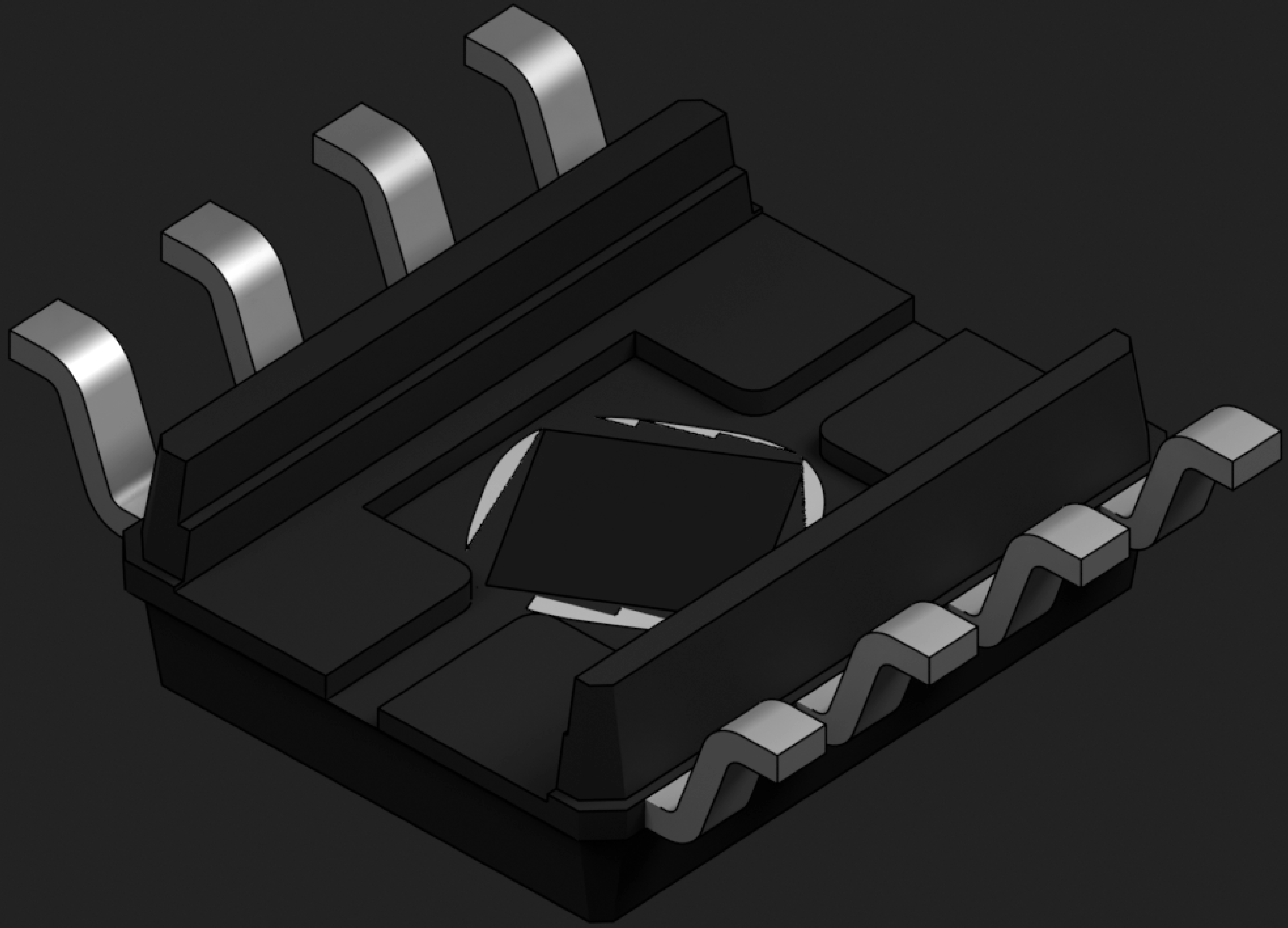
Backside decapsulation



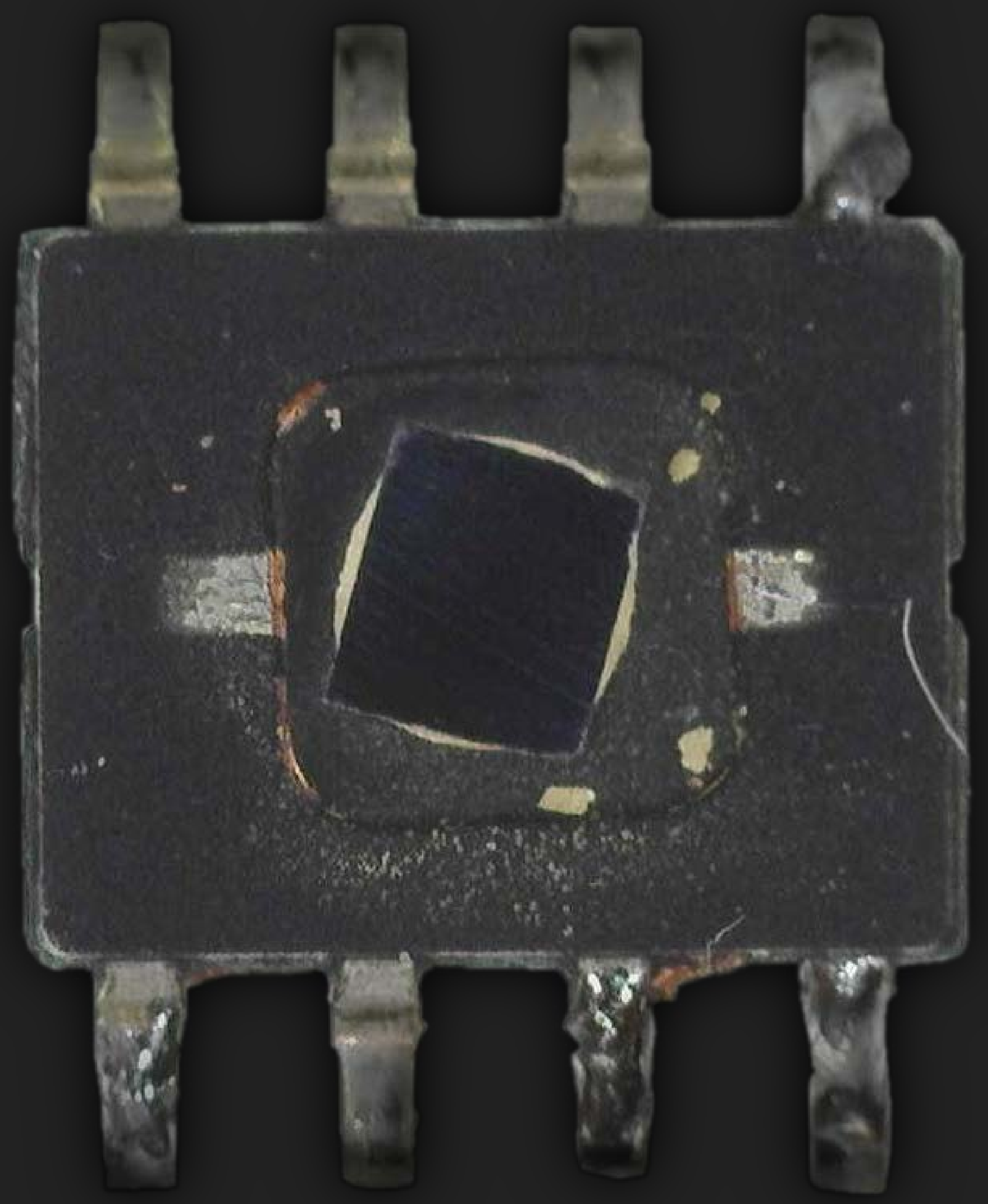
Backside decapsulation



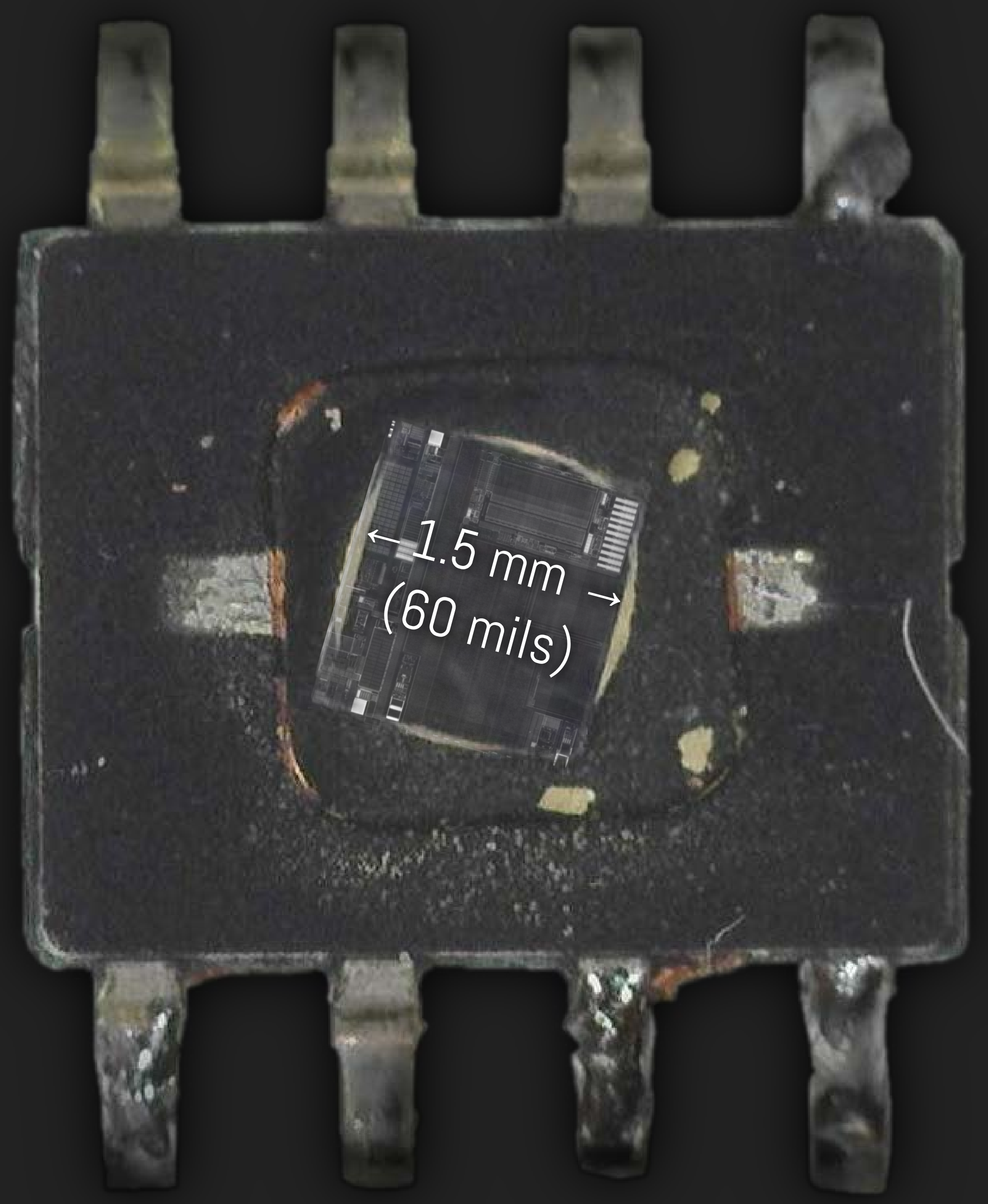
Backside decapsulation



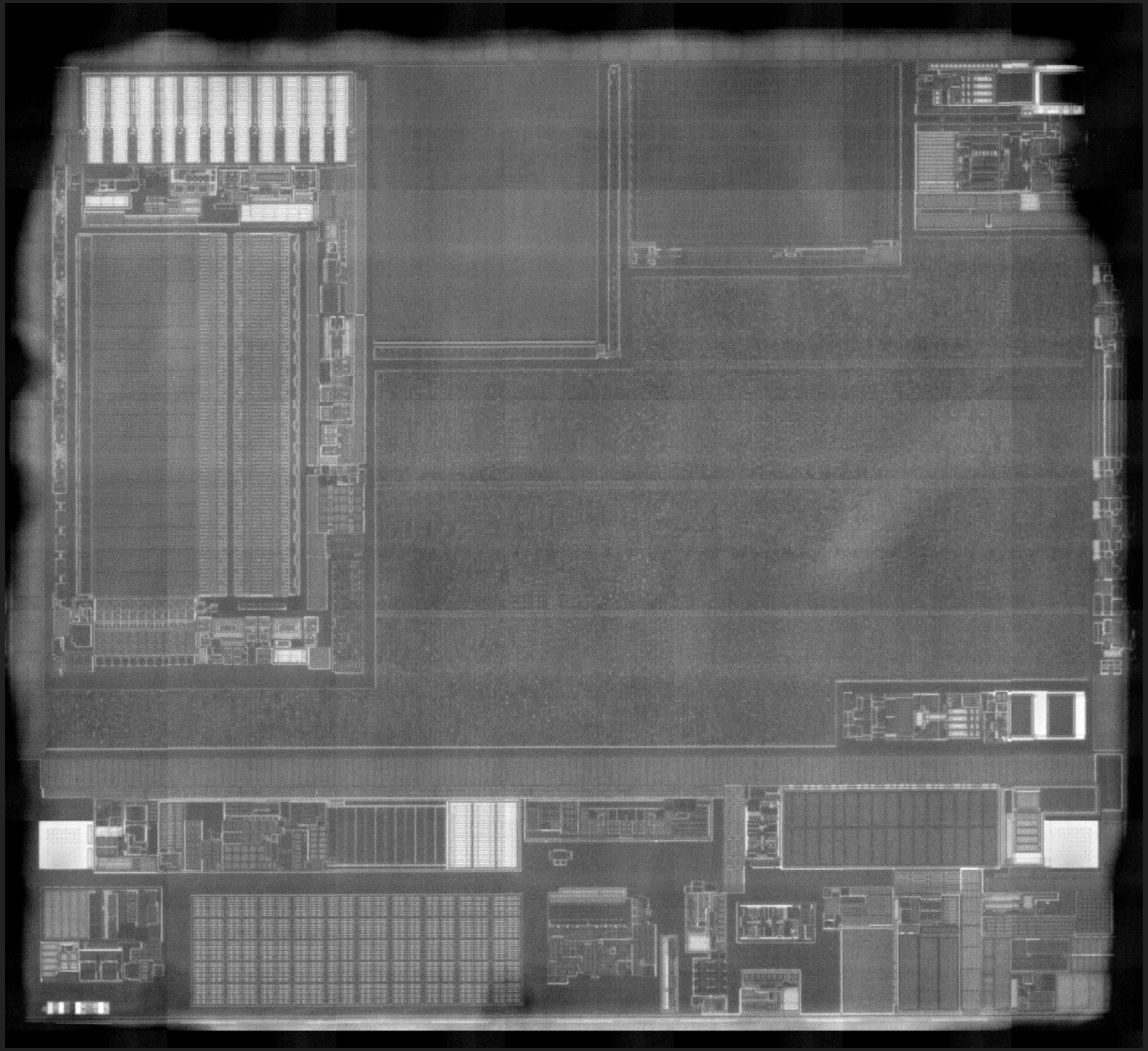
Backside decapsulation



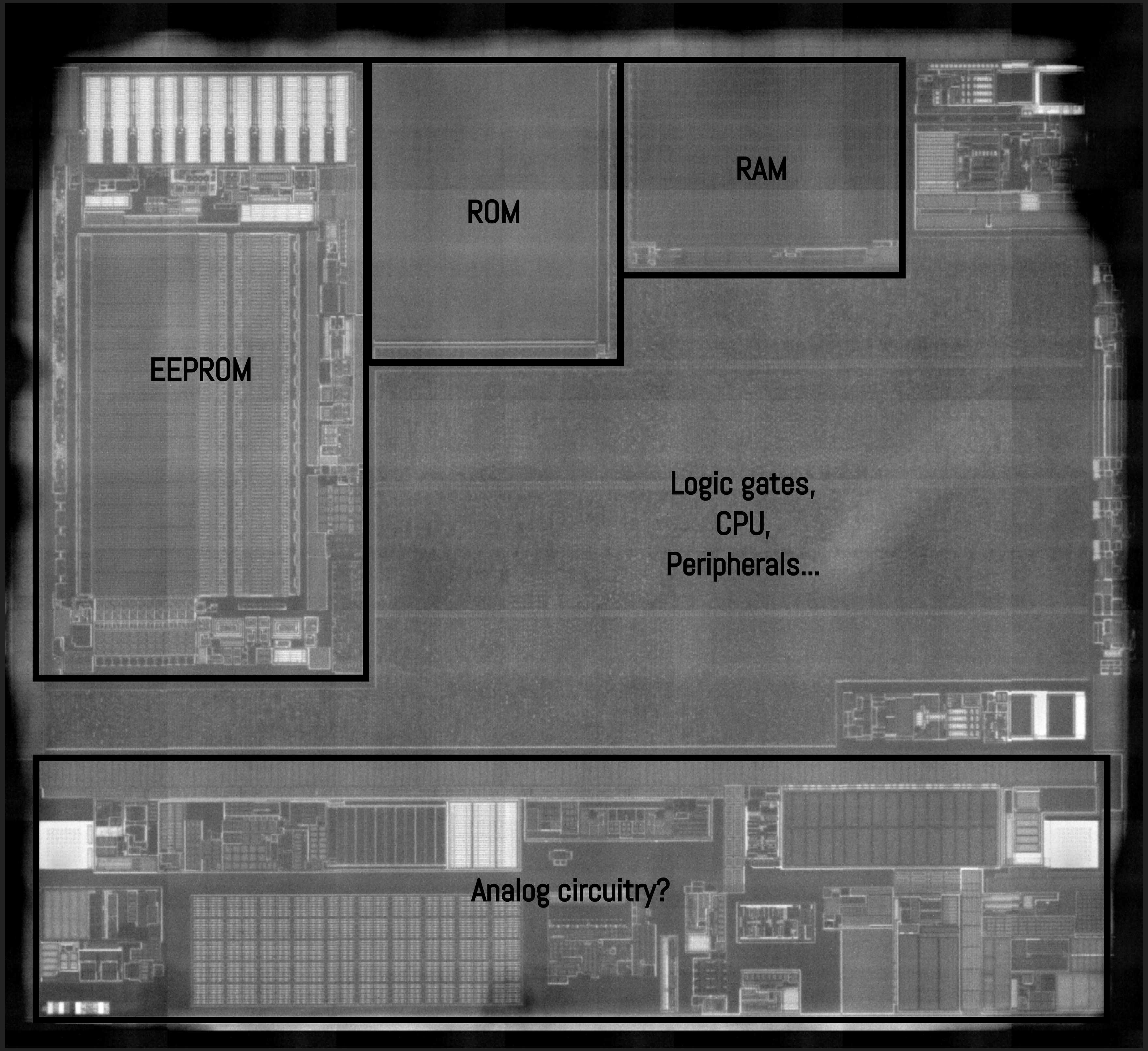
Backside decapsulation



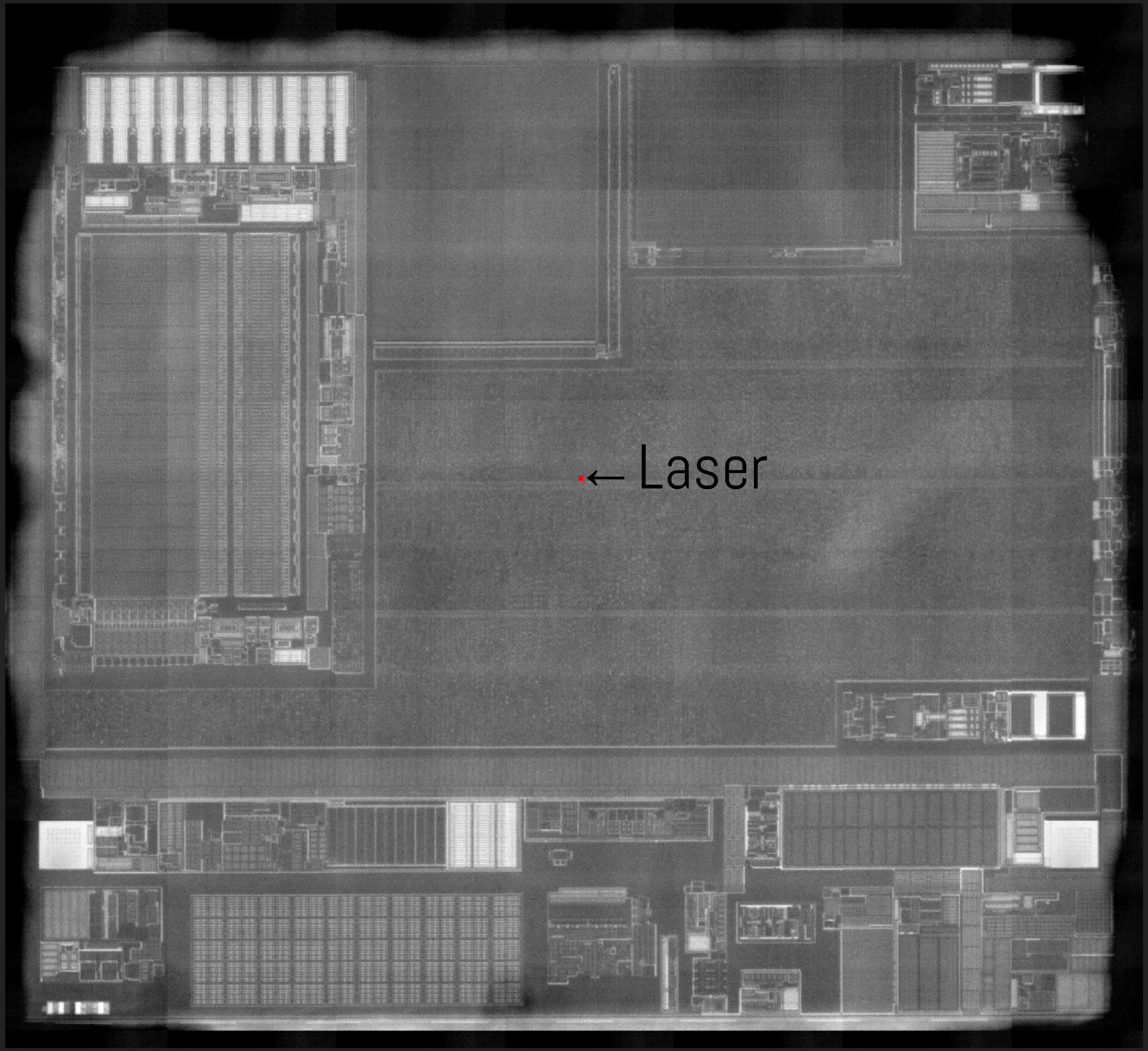
Infrared imaging



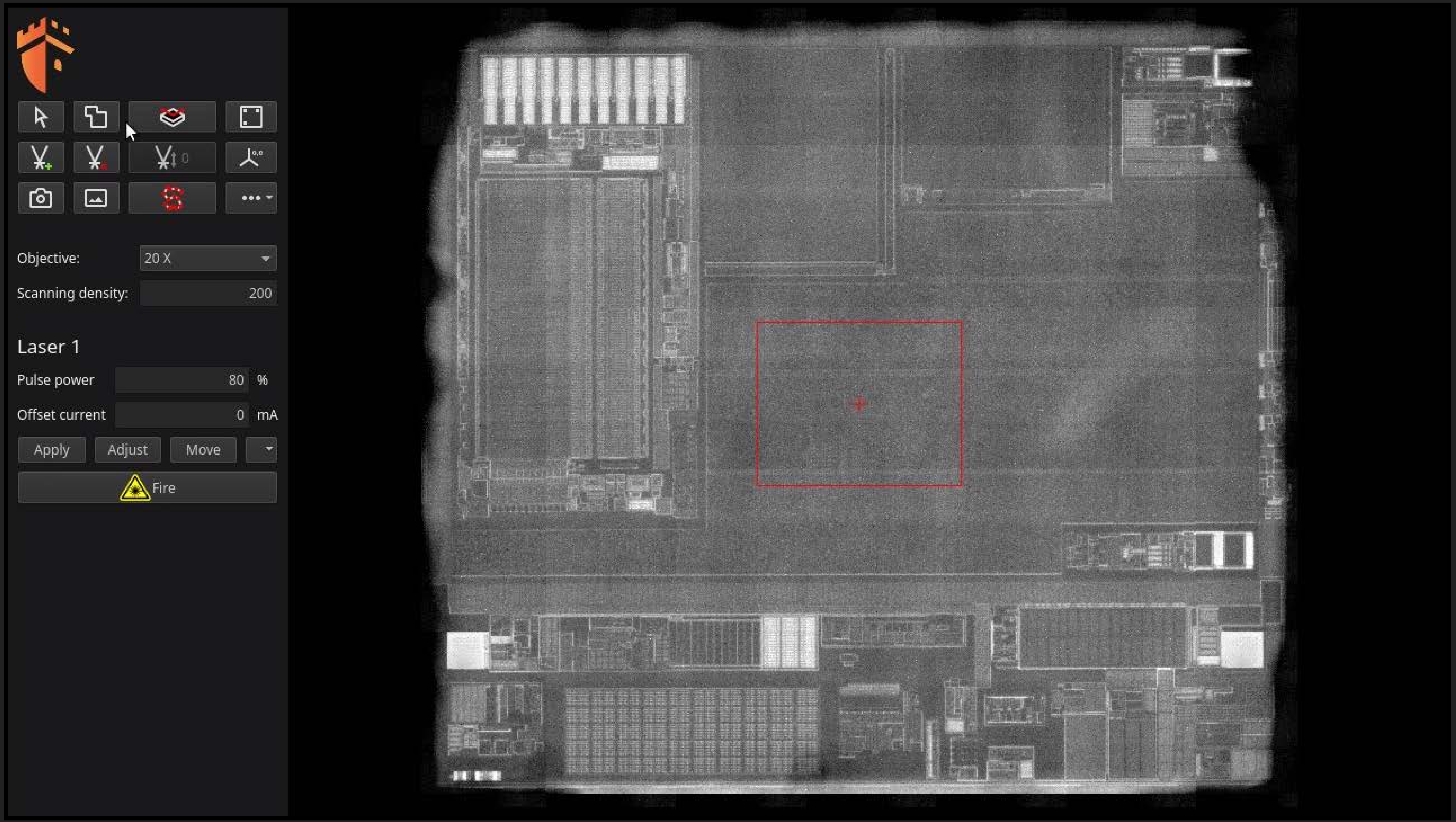
Infrared imaging



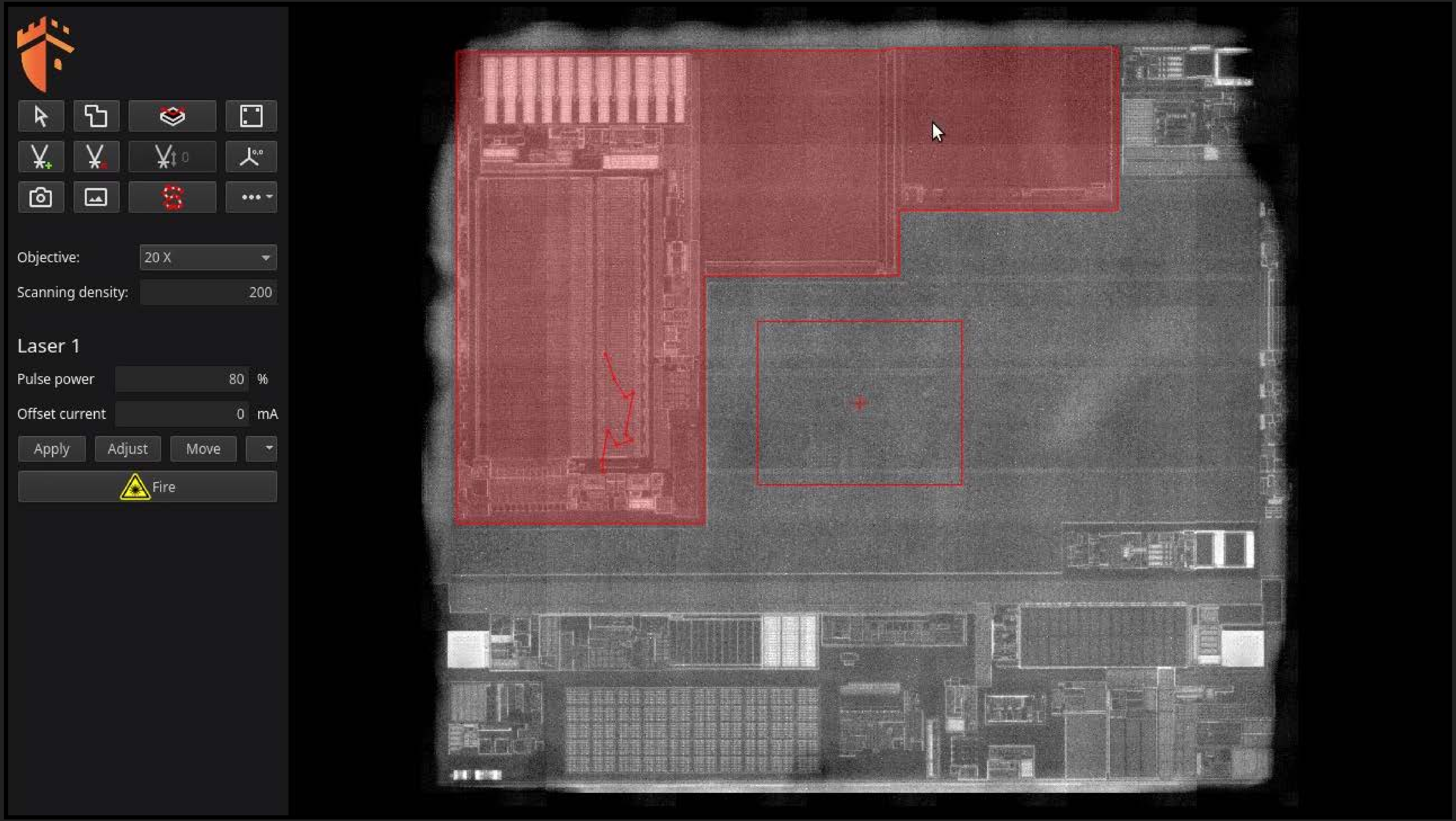
Infrared imaging



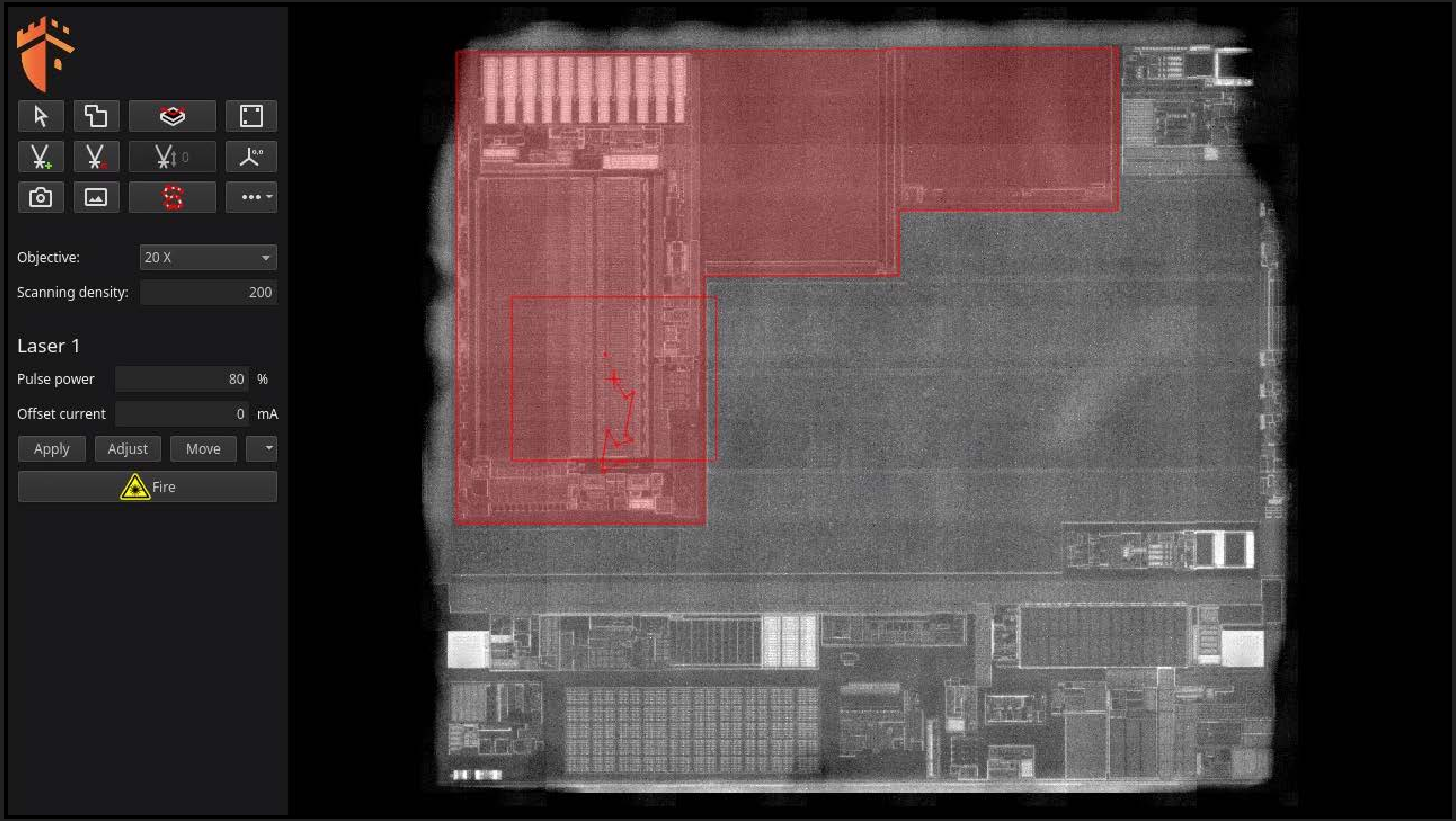
Targeting


Objective:
20 X
Scanning density:
200
Laser 1
Pulse power
80
%
Offset current
0
mA
Apply
Adjust
Move
Fire

Targeting

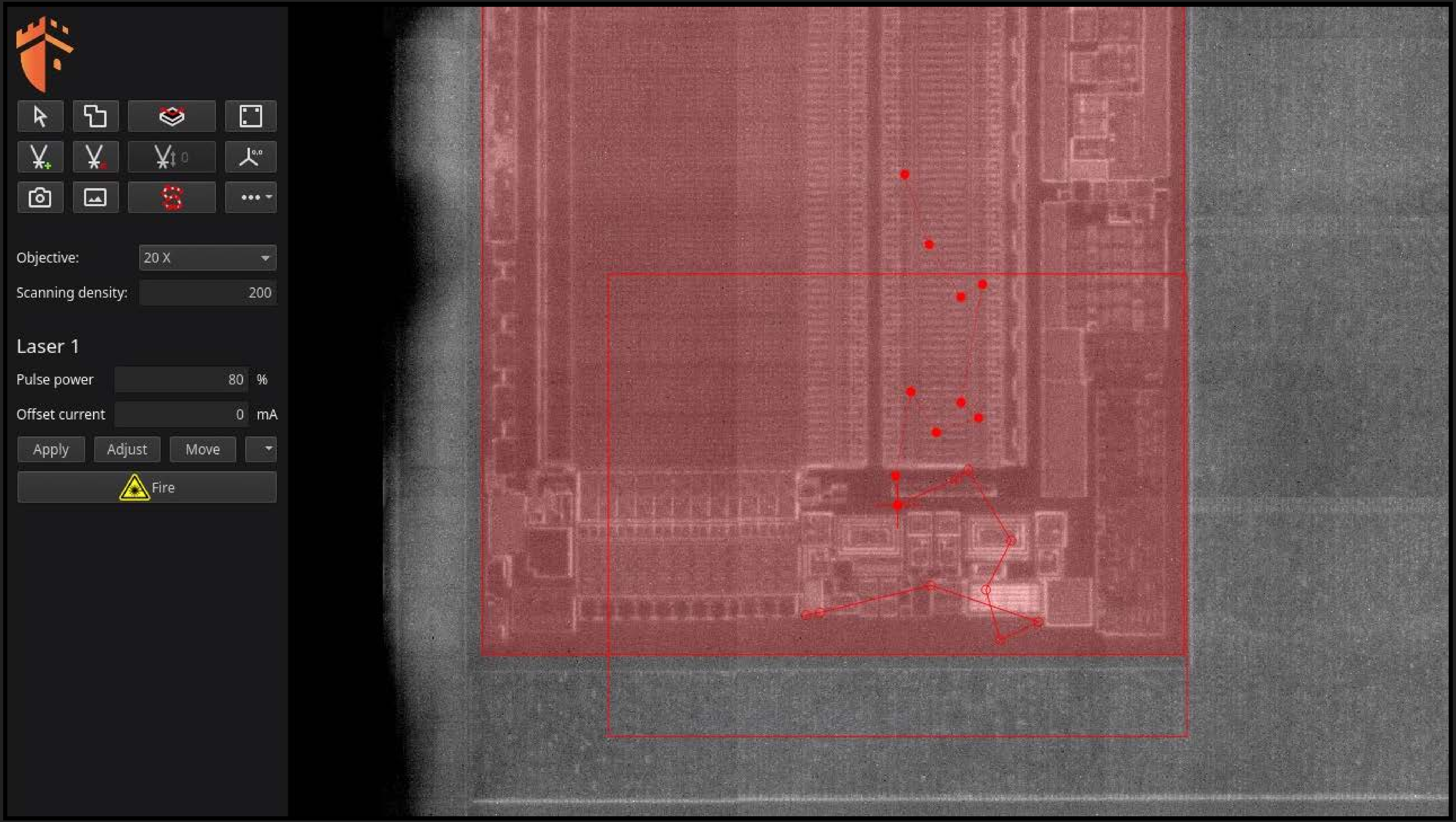

Objective:
20 X
Scanning density:
200
Laser 1
Pulse power
80
%
Offset current
0
mA
Apply
Adjust
Move
Fire

Targeting



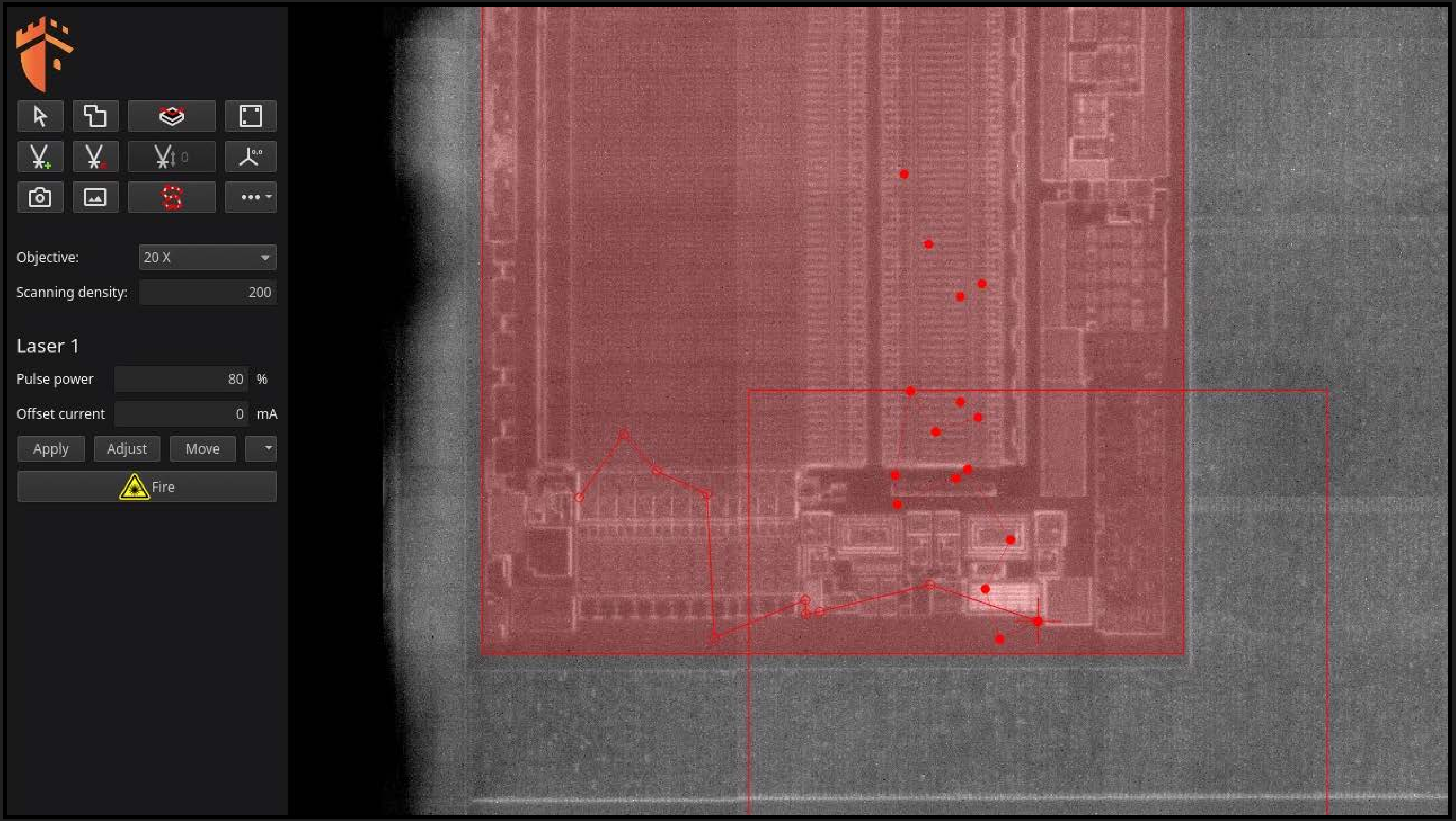
Objective:
20 X
Scanning density:
200
Laser 1
Pulse power
80
%
Offset current
0
mA
Apply
Adjust
Move
Fire

Targeting



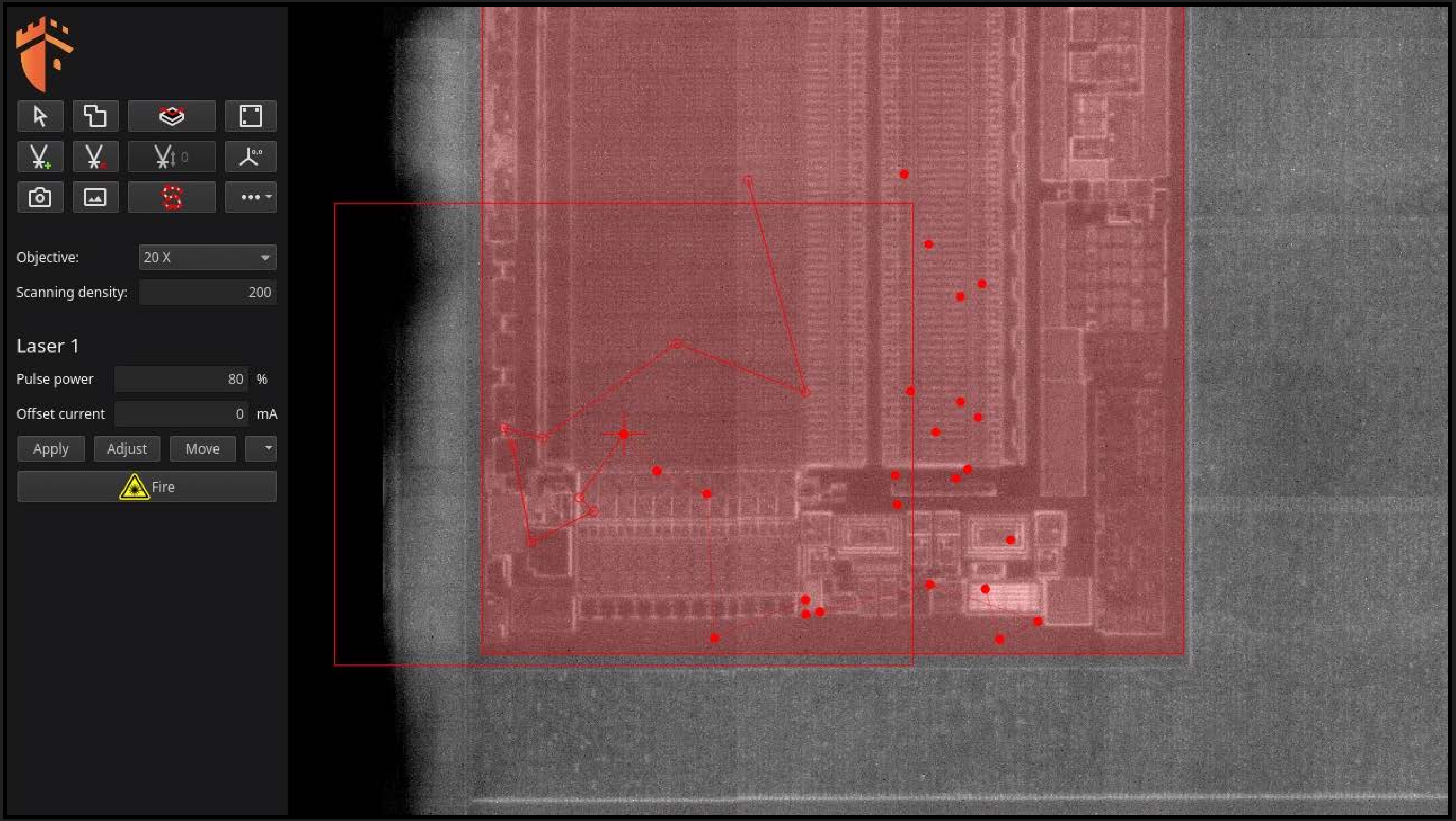
Objective:
20 X
Scanning density:
200
Laser 1
Pulse power
80
%
Offset current
0
mA
Apply
Adjust
Move
Fire

Targeting



Objective:
20 X
Scanning density:
200
Laser 1
Pulse power
80
%
Offset current
0
mA
Apply
Adjust
Move
Fire

Targeting



Objective:
20 X
Scanning density:
200
Laser 1
Pulse power
80
%
Offset current
0
mA
Apply
Adjust
Move
Fire

Testing campaign

Known data is loaded prior to testing:

303132333435363738396162636465666768696a6b6c6d6e6f70717273747576

Testing campaign

For each test:

1. Laser shooting time configuration
2. Laser beam displacement
3. Power-on
4. Initialization
5. Laser activation
6. *ReadMemory* command + Laser shoot
7. Laser deactivation
8. Response readout
9. Power-off
10. Result and parameters logging

Testing campaign

```
Test #1:
  EXECUTION_ERROR
Test #2:
  Timeout, no response received!
Test #3:
  PARSE_ERROR
Test #4:
  OK 09c8420000000000000000000000000000000000000000000000000000000000
Test #5:
  OK 41e0f633a019cd625920691b11400c9387009e68d0b13e53d73257216a4c0ce8
Test #6:
  UNKNOWN_ERROR 0xFE
Test #7:
  EXECUTION_ERROR
Test #8:
  OK
Test #9:
  OK 2ffef9424c7e67d31b519d3d4ea96444265a5189aadba8ab27624ca34c2fdf27
...
```

Testing campaign

343617

faults injected

Many days of testing

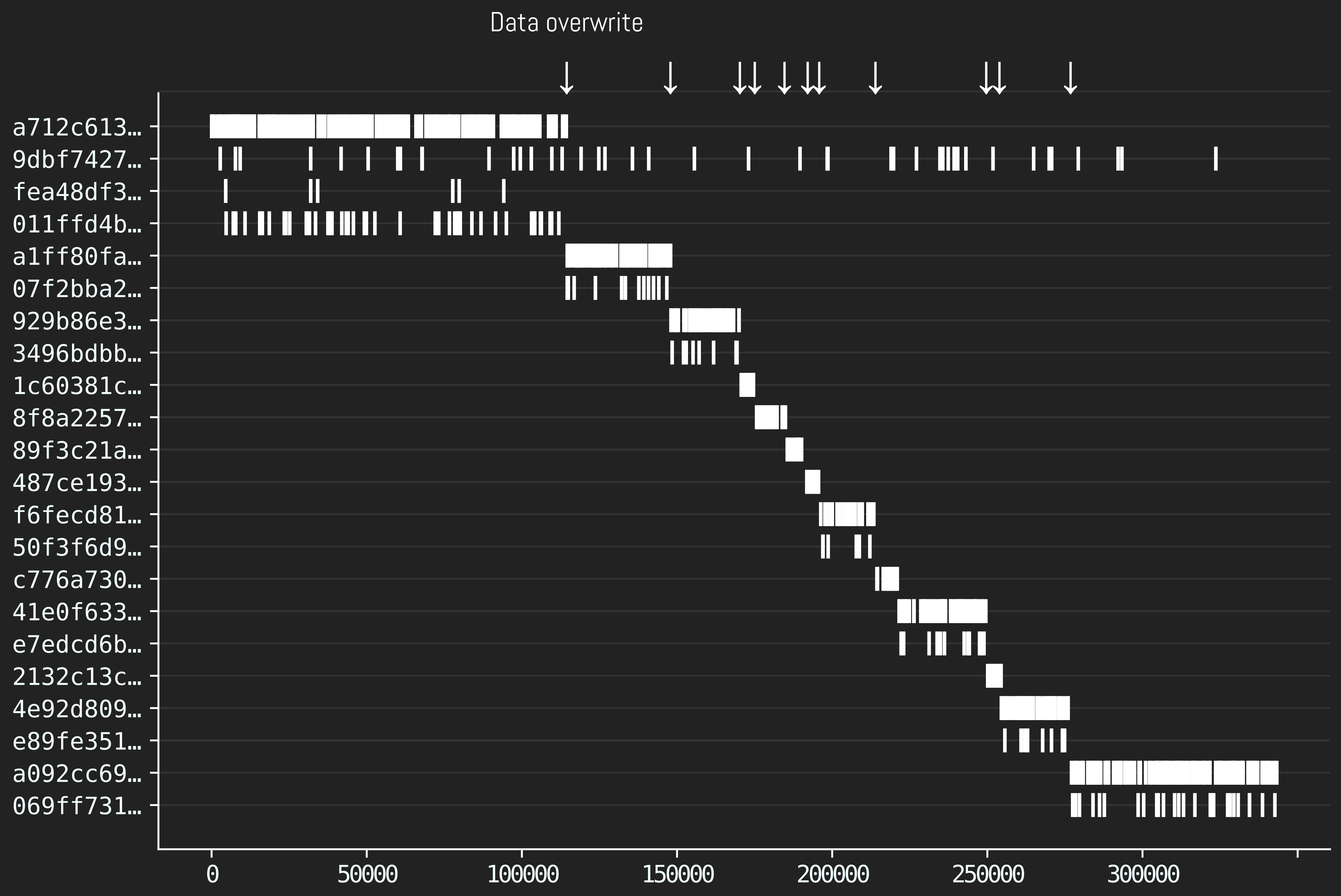
1546 responses received

No success observed...

Top 20

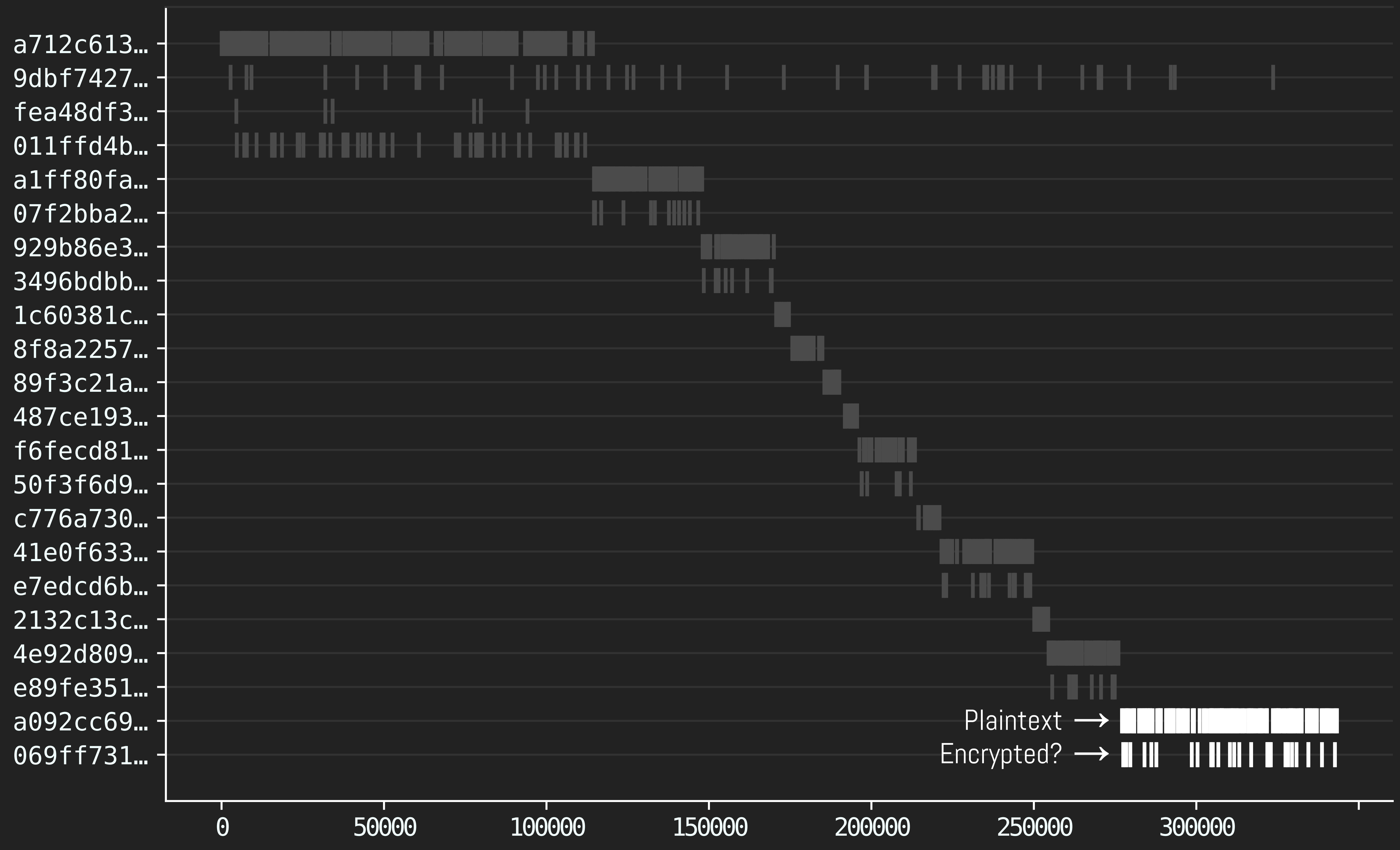
x 336	a712c6137b0b50b401d8deff8b0b3b8e5f2b01e0707d4eaeaeb6bbe589220274
x 152	a092cc6943e6c408bdd924e4ce90b8c895ddac03d2ada707088cace9d9cb803a
x 151	00000000
x 76	a1ff80fa7028066d4dcc023f23e2ec6b79864aa8b6e979e1d63cbf05277ebeb7
x 72	41e0f633a019cd625920691b11400c9387009e68d0b13e53d73257216a4c0ce8
x 58	929b86e3dff0ecb1d2318cf0c4bf5872b32d9db260cf012ae7c00d40cac19cc1
x 53	4e92d8096bfa78254581b9f5b987e60337e4f9860f92a2615581676e896854dd
x 51	011ffd4b459e81f8ab7f42cd2662fc6117cad15cb99155e72ed6b76211067e22
x 50	09c842000000000000000000000000000000000000000000000000000000000000000000...
x 43	9dbf7427f5098feb2c708174875896f7294629a30049f5aa825dffa05b7c3c29
x 37	f6fecd81f528d1ebfcf005b0d59ebfd84839dbcc0c1a9614be3a13351009b107
x 31	8f8a22572231abafd8035be7d84eece928e7754d966b054fa4f02e5d02599bc6
x 29	069ff7317d731544177eb8d663f97f27dd3c7cbf1b41bc4e88eca06e41effc6c
x 21	c776a730a55dd031685d2afc76672ba5d23187ca07ce42b66286888be89cac2d
x 20	01000000
x 15	89f3c21a72ebb69fb1f6010fe3c0a3ab6ebb81356337b3e2a7024024d40ba371
x 14	2132c13ce836eda1ab62fc3c9b07345da28616d792e0ebc3e7bae5864c0d9e80
x 12	07f2bba24ebdd721e76b9e0d8e8b2b8431679a147f0562a8565cb382bf5ac2e1
x 12	e7edcd6b9e8c1c2ef387f529bc29cb7ccfe14ed4195d251a57525ba6f26870be
x 11	1c60381c2111566e7b200149b12bc72ee416bd90d1db927d4fe0abc008d0349a

Analysis



Data overwrite
a712c613…
9dbf7427…
fea48df3…
011ffd4b…
a1ff80fa…
07f2bba2…
929b86e3…
3496bdbb…
1c60381c…
8f8a2257…
89f3c21a…
487ce193…
f6fecd81…
50f3f6d9…
c776a730…
41e0f633…
e7edcd6b…
2132c13c…
4e92d809…
e89fe351…
a092cc69…
069ff731…
0
50000
100000
150000
200000
250000
300000

Analysis


a712c613…
9dbf7427…
fea48df3…
011ffd4b…
a1ff80fa…
07f2bba2…
929b86e3…
3496bdbb…
1c60381c…
8f8a2257…
89f3c21a…
487ce193…
f6fecd81…
50f3f6d9…
c776a730…
41e0f633…
e7edcd6b…
2132c13c…
4e92d809…
e89fe351…
a092cc69…
069ff731…
Plaintext →
Encrypted? →
0
50000
100000
150000
200000
250000
300000

Oh wait!

The attack seems to work!

Can we do it without losing data?

Attack refinement

Optimal parameters identification

New sample preparation and programming

Test run

Success!

Two minutes of testing only

PIN1 and pairing secret data slots can be revealed
Grants access to Seed1 data slot

Coldcard Mk2 vulnerable

Realistic attack

Did we killed chips?

Yes!

Misconfiguration due to misunderstanding

Failed sample preparation

Data corruption with bad EEPROM write

Possible software mitigations

Double checking

Sensitive constants value

Kill-chip

Possible hardware mitigations

Light sensors for laser detection

Power trace jamming

CPU clock frequency randomization

Error-Detection-Codes on memories

Cost of mitigations

Implementing them correctly is difficult.

More counter-measures requires more silicon area.

Power and performance is impacted.

Counter-measures may be patent protected.

Security is expensive!

Conclusion

High potential attack
Very expensive equipment

Specific configuration
P-256 keys are not affected

Less resistant than a Secure Element

ATECC508A now deprecated
Superseeded by ATECC608A

Thank you!