Injection de faute par laser en boîte-noire sur mémoire sécurisée

Olivier Hériveaux

Protection de secrets en embarqué

Microcontrôleurs

Mémoire FLASH, fusible contre la relecture
Peu coûteux
Faible résistance face aux attaques physiques

Secure Elements

Contre-mesures aux attaques physiques
Evalués par des laboratoires spécialisés
Accès limité (JCVM, NDA, ...)

Microchip ATECC508A

Mémoire sécurisée
Applications IoT
Utilisation ouverte
Quel niveau de sécurité ?

Wallet Coldcard

Bitcoin hardware wallet

Version Mk2 étudiée

Microcontrôleur STM32L4

Firmware applicatif

⇅

ATECC508A

Stocke la "Seed" (clef privée)

Protection par authentification

ATECC508A

Surface d'attaque logicielle réduite

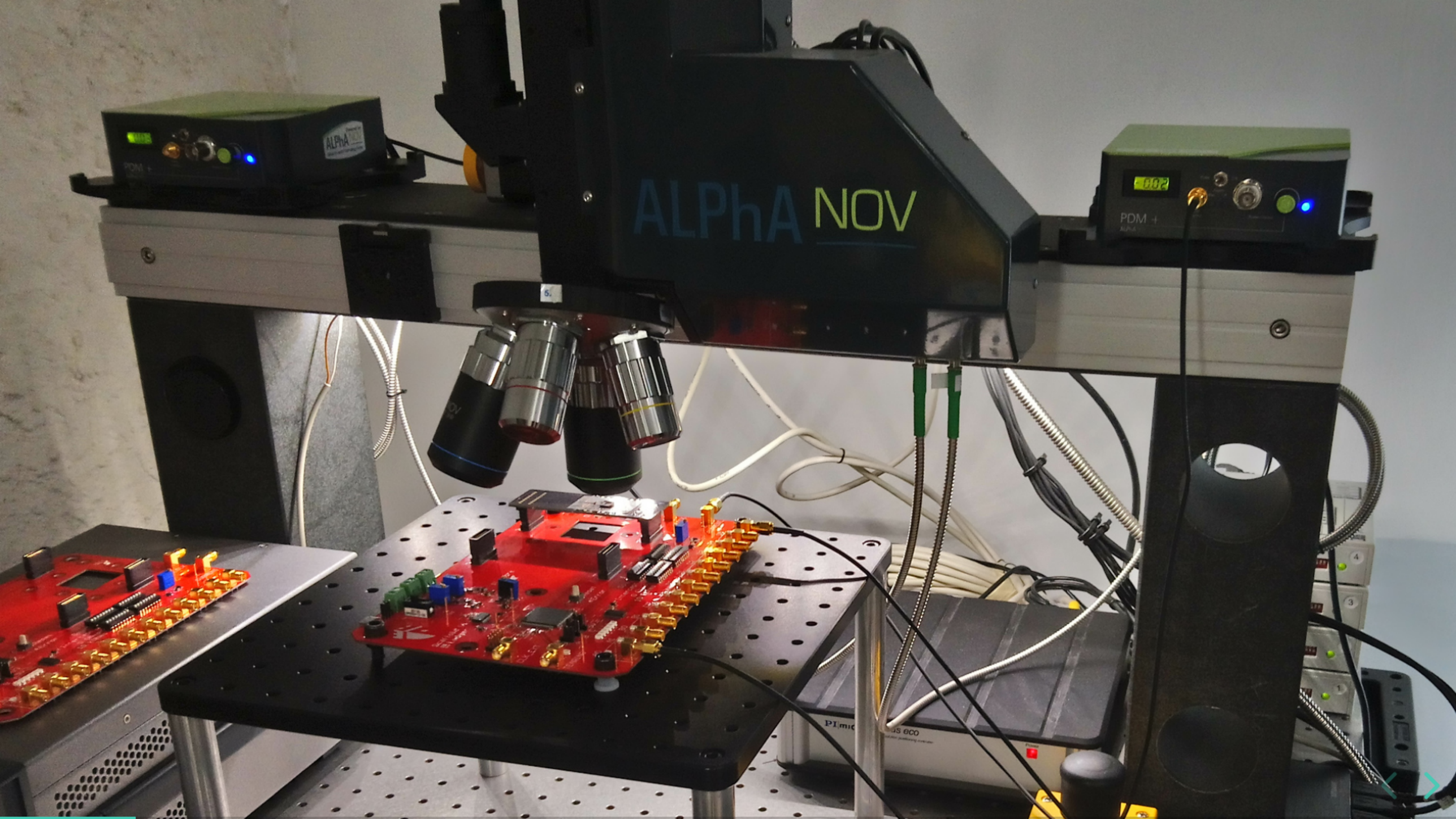
Firmware secret

Détecteur de glitchs en tension

Bouclier métallique en surface

Horloge générée en interne

Pas de protection contre les lasers


ALPhA NOV
PDM +

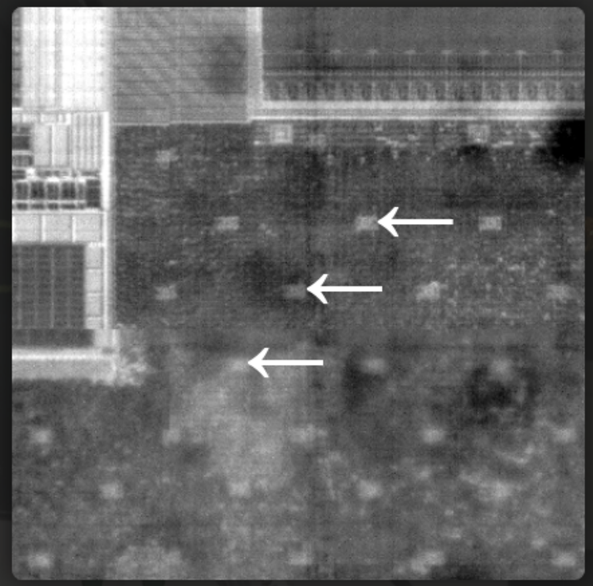
Le silicium est transparent
aux infra-rouges

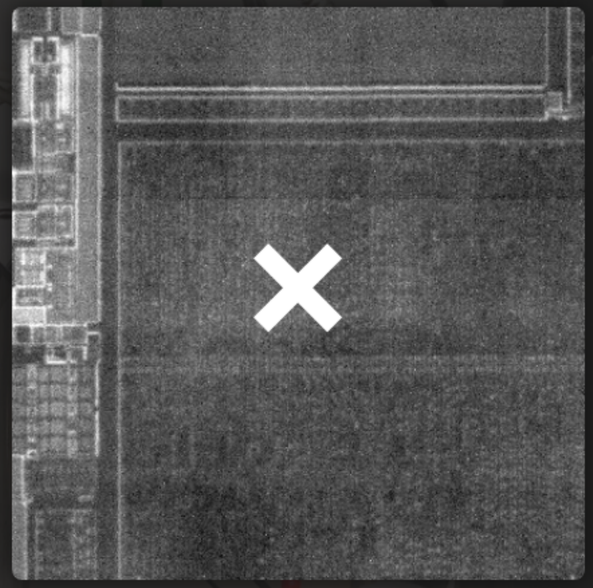
Les circuits intégrés sont photosensibles

Eclairer un transistor peut le rendre
conducteur...

... et introduire des erreurs de calcul !

Le laser est outil redoutable et peu invasif





Quel est le plan ?

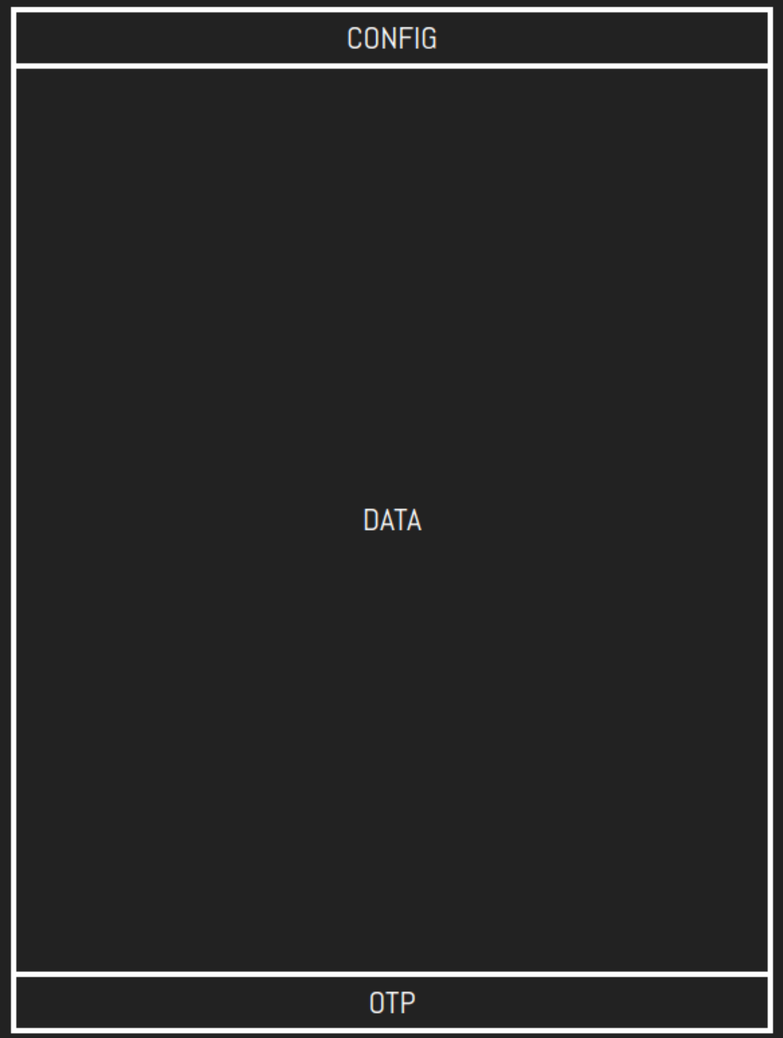
Identifier et établir un chemin d'attaque

Préparer et instrumenter

Cibler

Tester

Plan mémoire ATECC508A



Plan mémoire ATECC508A

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

Plan mémoire ATECC508A

CONFIG	
Non utilisé	Clef d'appairage
Aléa anti-phishing	Hash PIN1
PIN2	Compteur PIN1
Compteur PIN2	PIN3
PIN4	
Seed1	
Seed2	
Seed3	
Seed4	
BrickMe	
Hash firmware	
Non utilisé	
OTP	

Accès aux fichiers

Commande *ReadMemory* :

03	07	02	82	1800	0a78
Commande	Longueur	OpCode Read Memory	Zone DATA + Longueur	Adresse	CRC

Réponse :

23	303132333435363738396162636465666768696a6b6c6d6e6f70717273747576	384a
Longueur	Données (32 octets)	CRC

Configuration fichier PIN1

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

Configuration fichier PIN1

Code hypothétique

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

Code hypothétique

```
1  config_address = get_config_address(slot);
2  config = eeprom_read(config_address);
3
4      (!config.is_secret){
5      data_address = get_data_address(slot);
6      data = eeprom_read(data_address);
7
8      if (config.encrypt_read)
9          encrypt(data);
10
11     i2c_send(OK + data);
12 } else {
13     i2c_send(EXECUTION_ERROR);
14 }
```

Code hypothétique

```
1  config_address = get_config_address(slot);
2  config = eeprom_read(config_address);
3
4  if (!config.is_secret){
5      data_address = get_data_address(slot);
6      data = eeprom_read(data_address);
7
8      if (config.encrypt_read)
9          encrypt(data);
10
11     i2c_send(OK + data);
12 } else {
13     i2c_send(EXECUTION_ERROR);
14 }
```

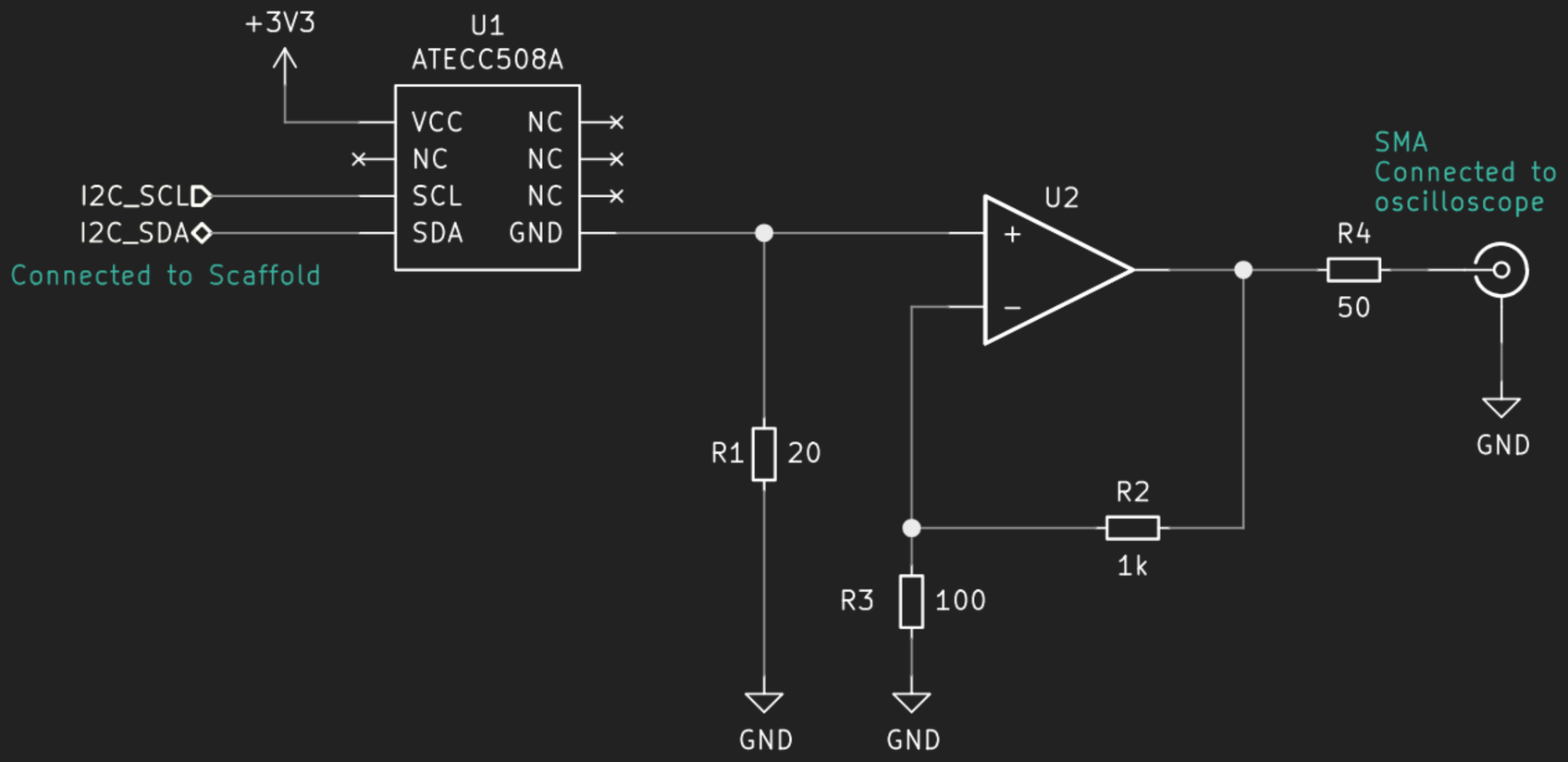
Code hypothétique

```
1  config_address = get_config_address(slot);
2  config = eeprom_read(config_address);
3
4  if (!config.is_secret){
5      data_address = get_data_address(slot);
6      data = eeprom_read(data_address);
7
8      if (config.encrypt_read)
9          encrypt(data);
10
11     i2c_send(OK + data);
12 } else {
13     i2c_send(EXECUTION_ERROR);
14 }
```

Quand ?

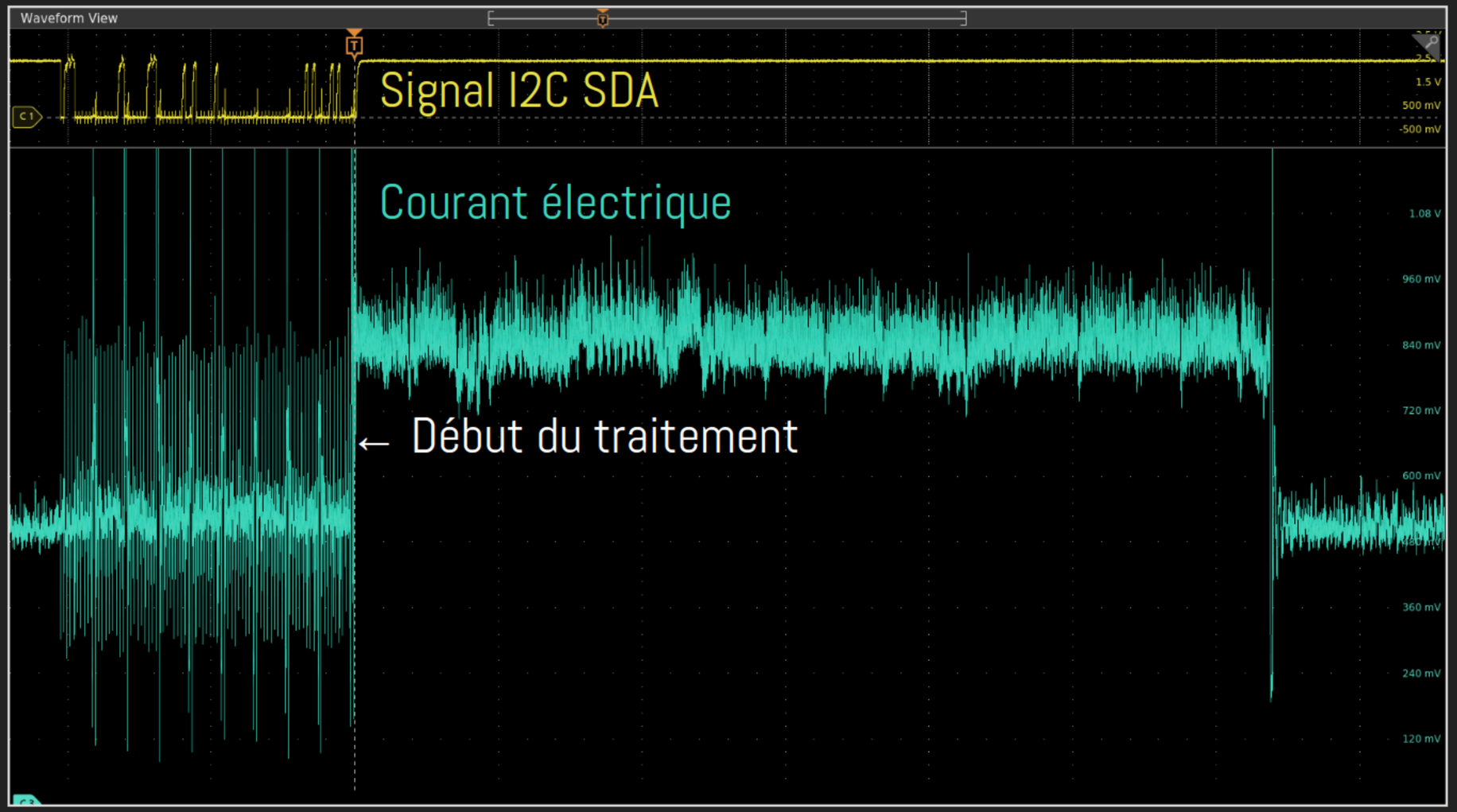
Instrumentation

La consommation électrique d'un circuit trahit son activité



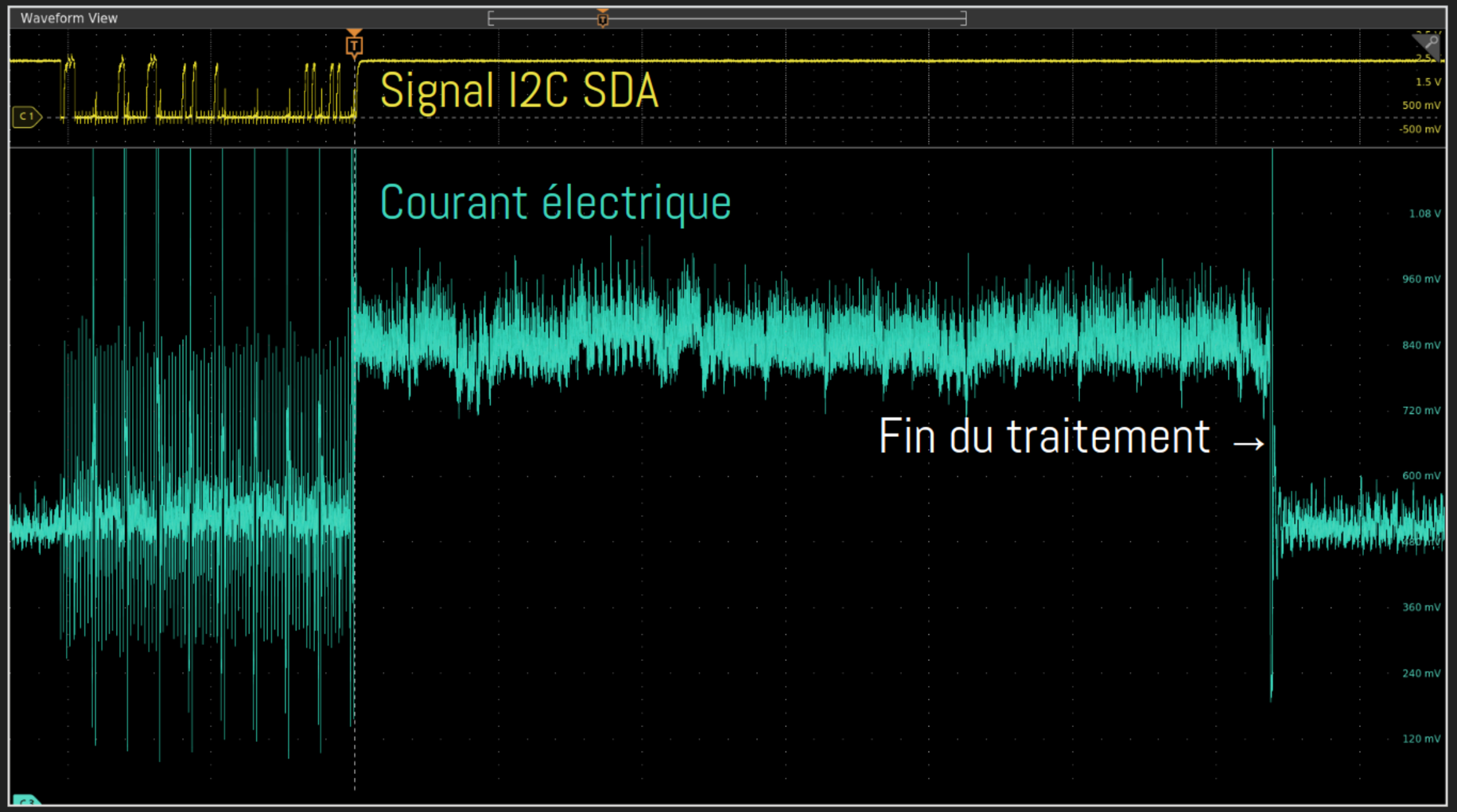
Instrumentation

Lecture autorisée d'un fichier



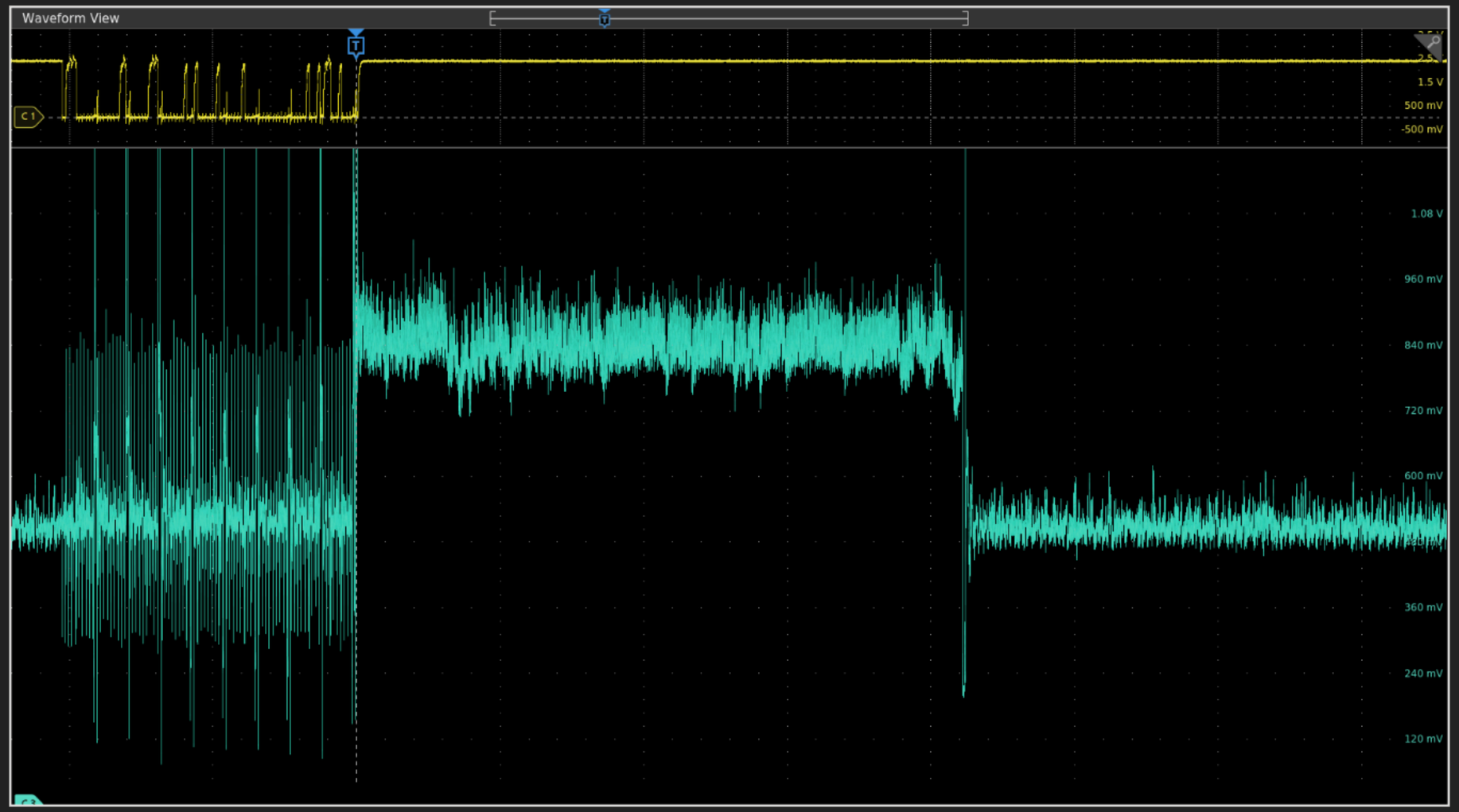
Instrumentation

Lecture autorisée d'un fichier



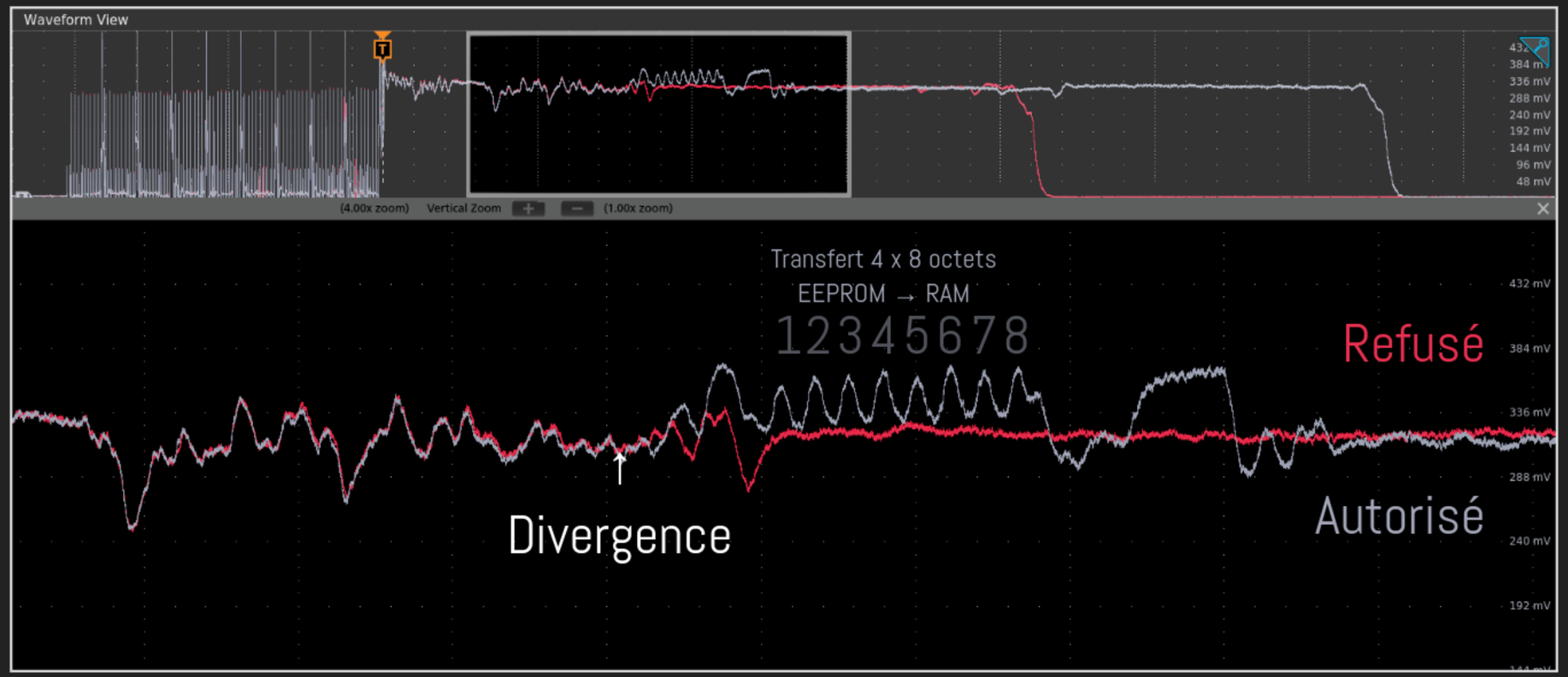
Instrumentation

Lecture refusée d'un fichier



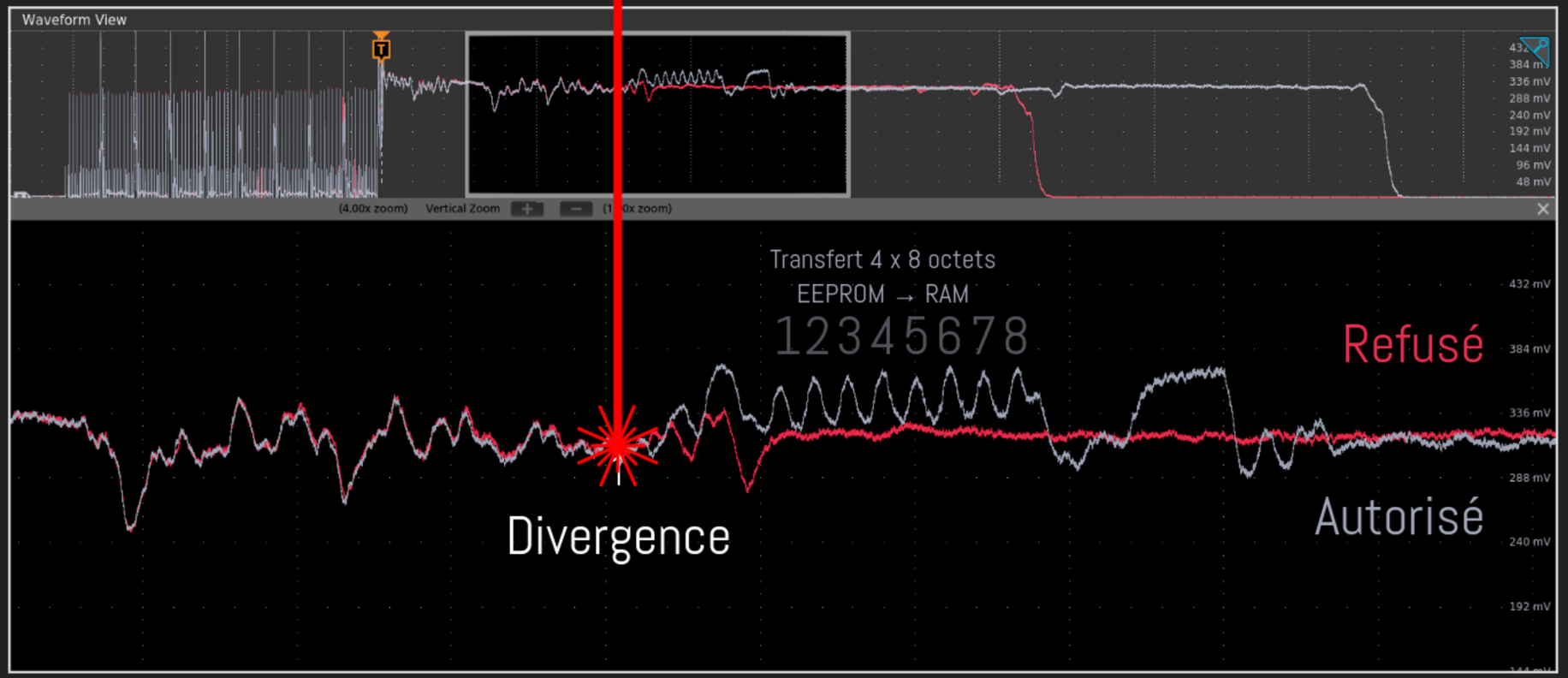
Instrumentation

Comparaison avec moyennage



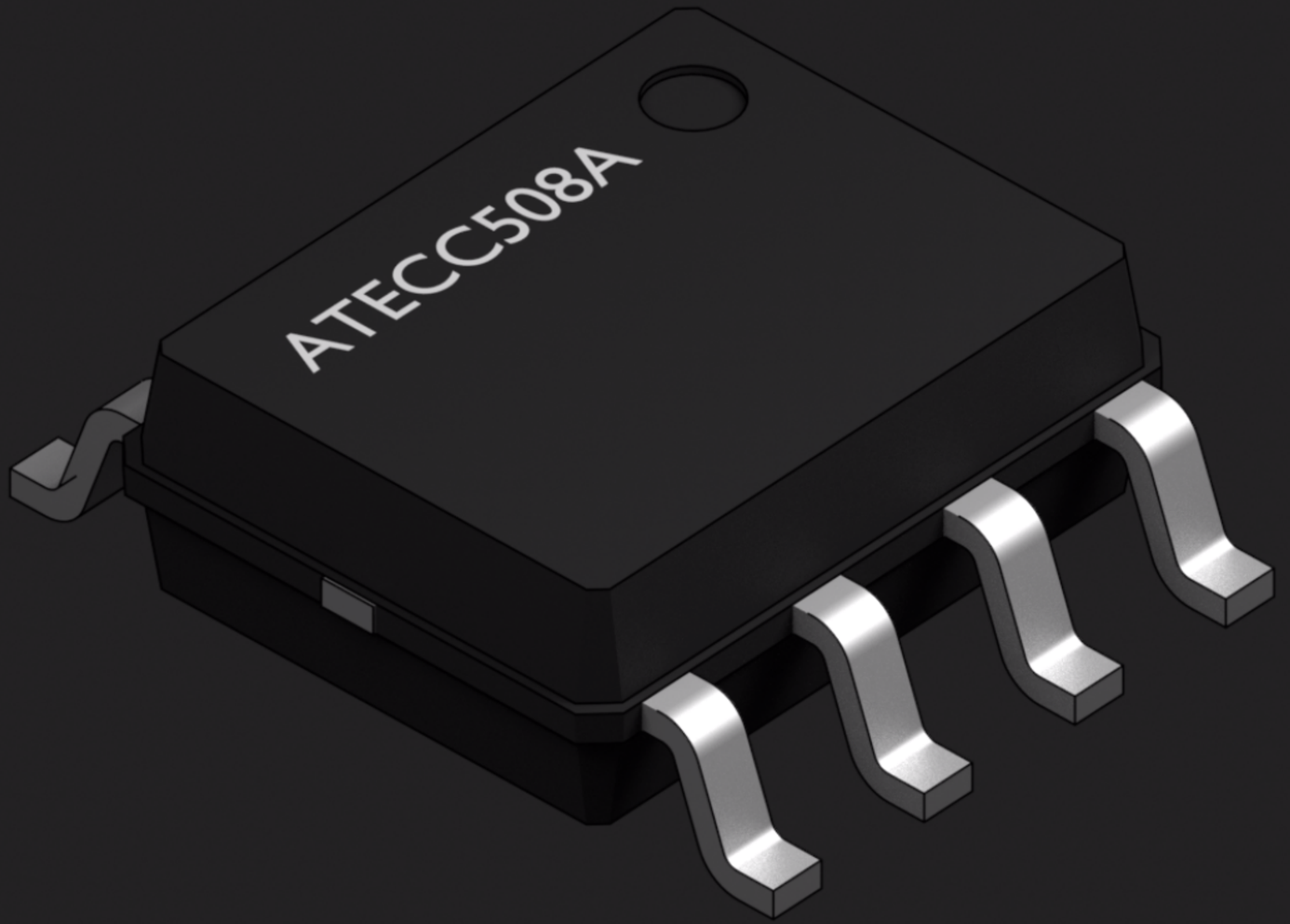
Instrumentation

Comparaison avec moyennage

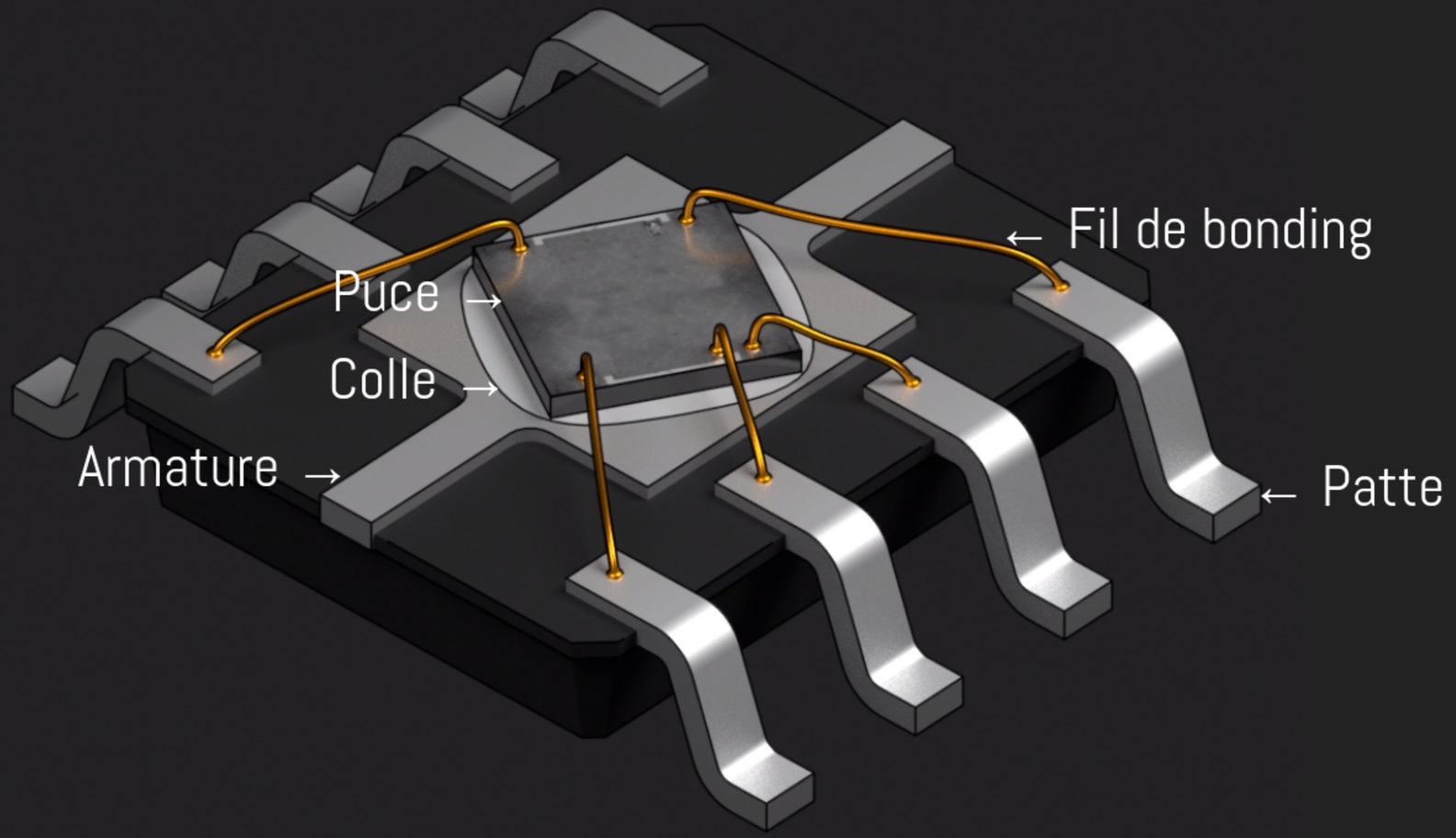


Où ?

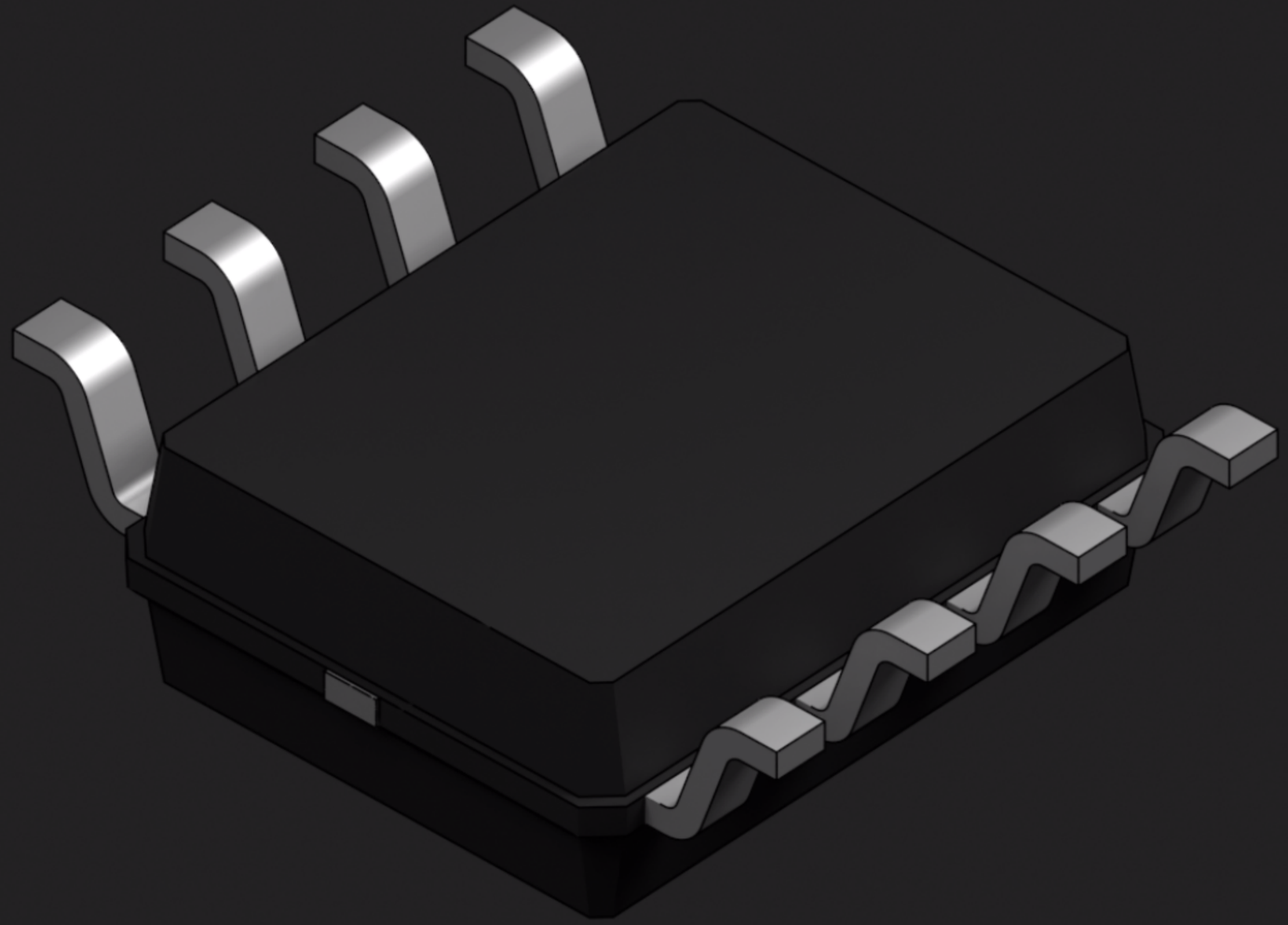
Dissection



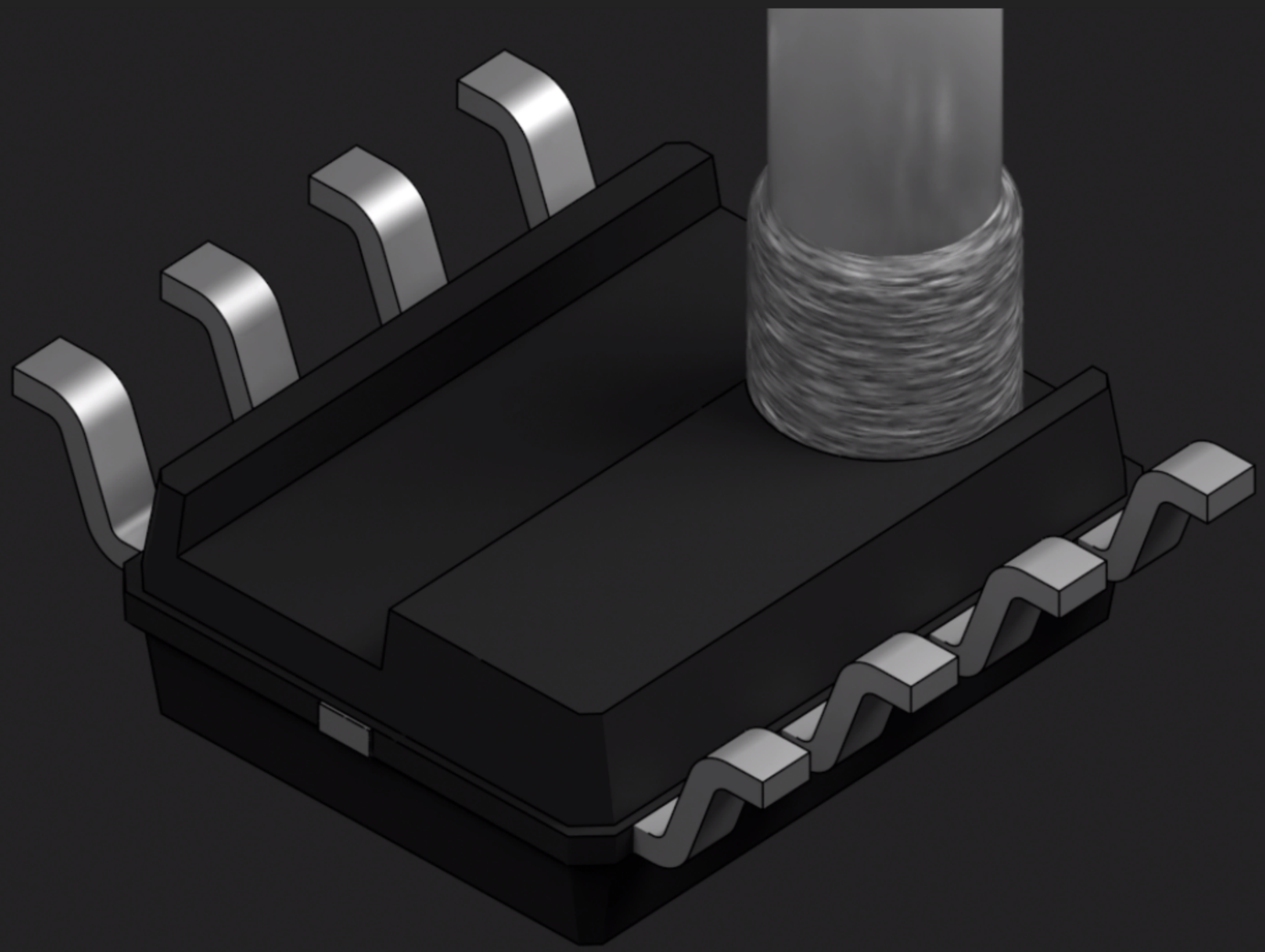
Dissection



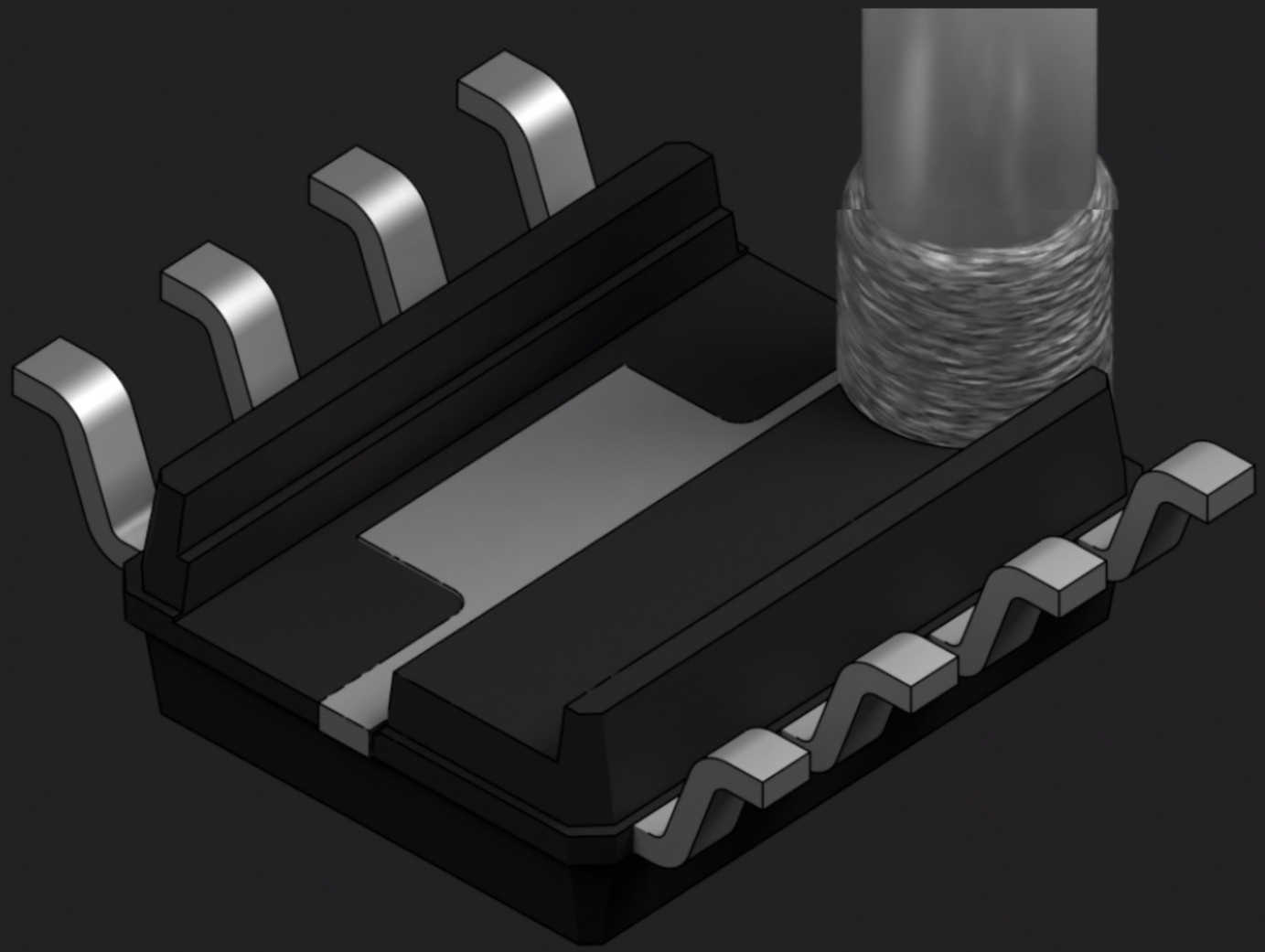
Ouverture face-arrière



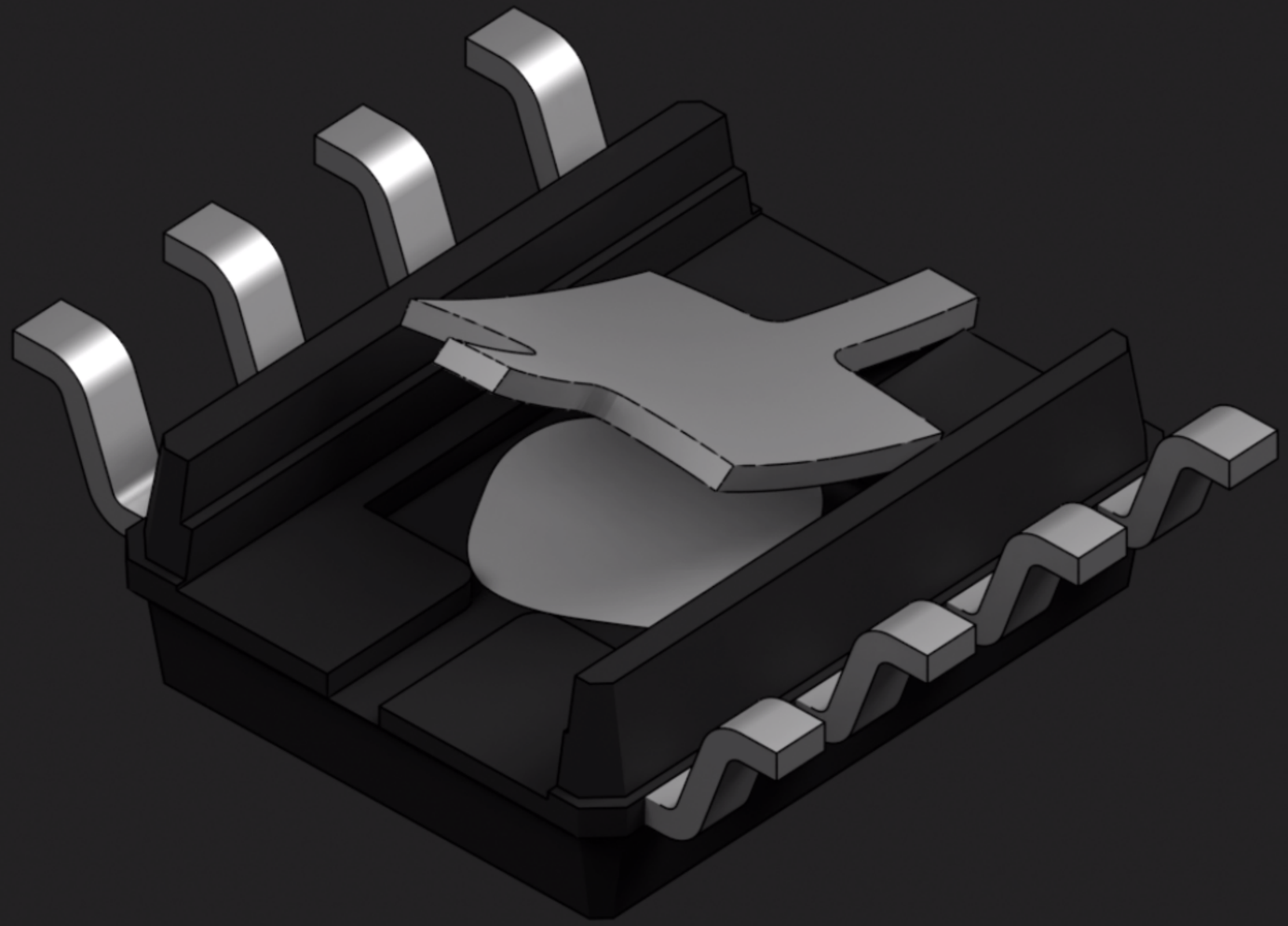
Ouverture face-arrière



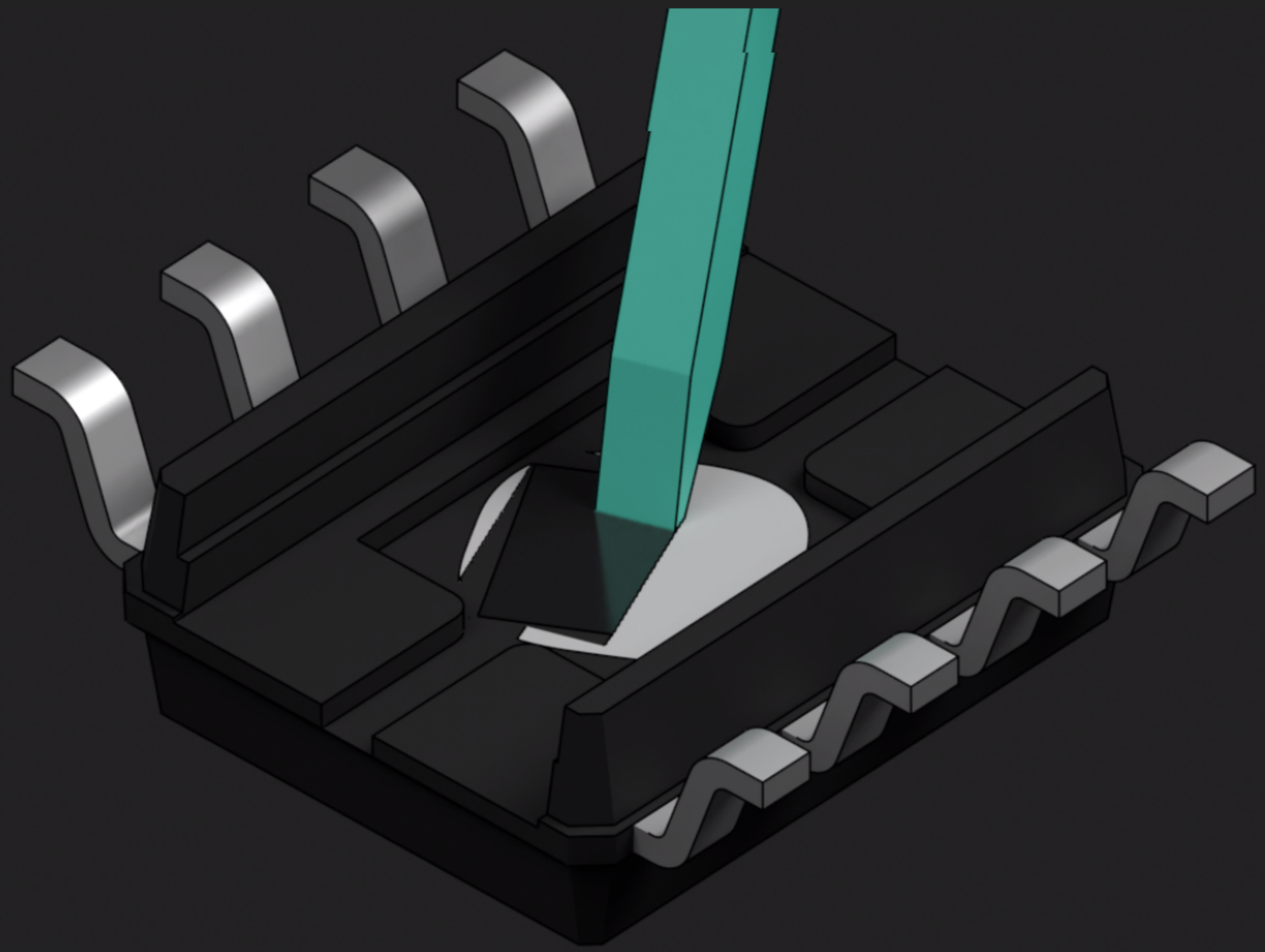
Ouverture face-arrière



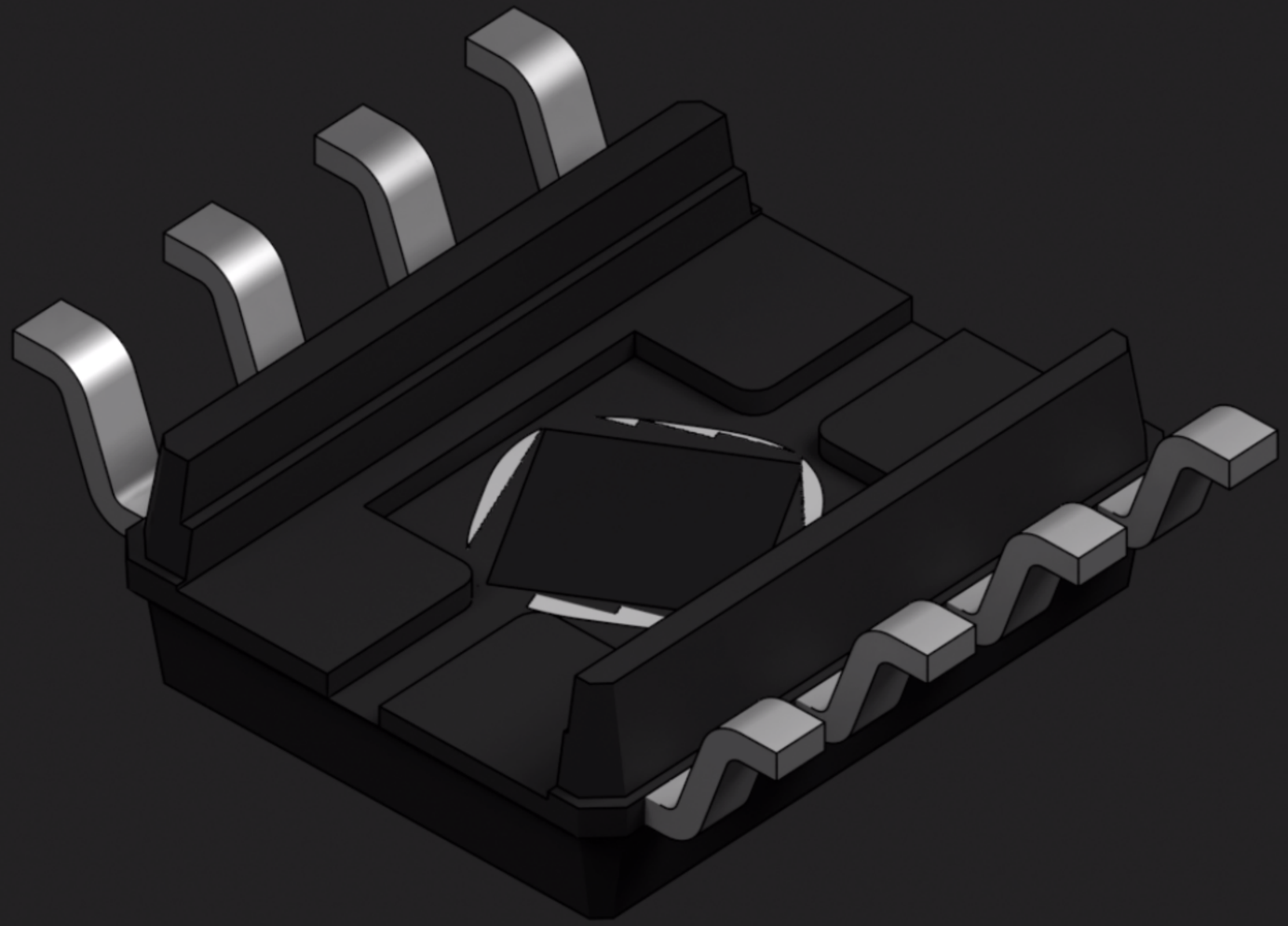
Ouverture face-arrière



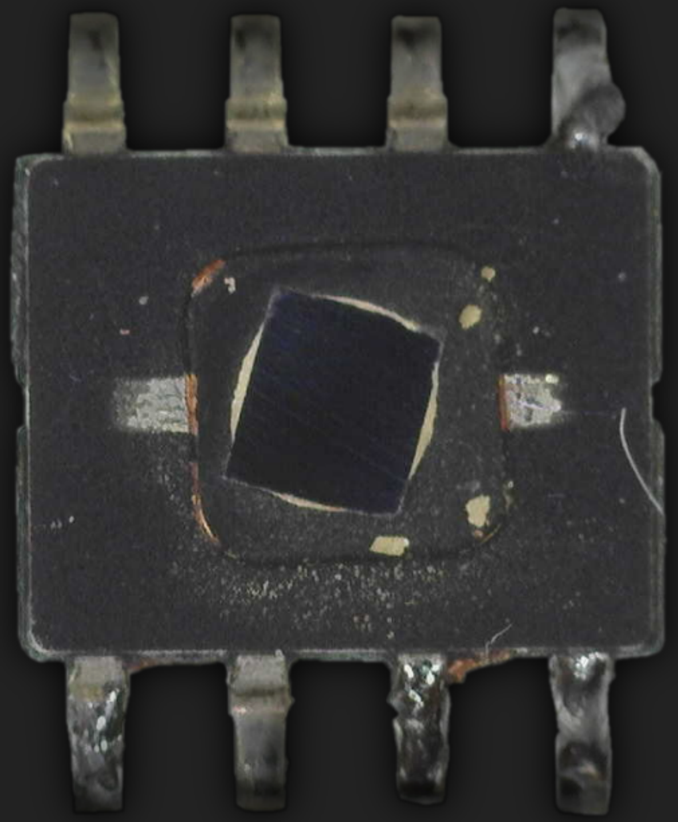
Ouverture face-arrière



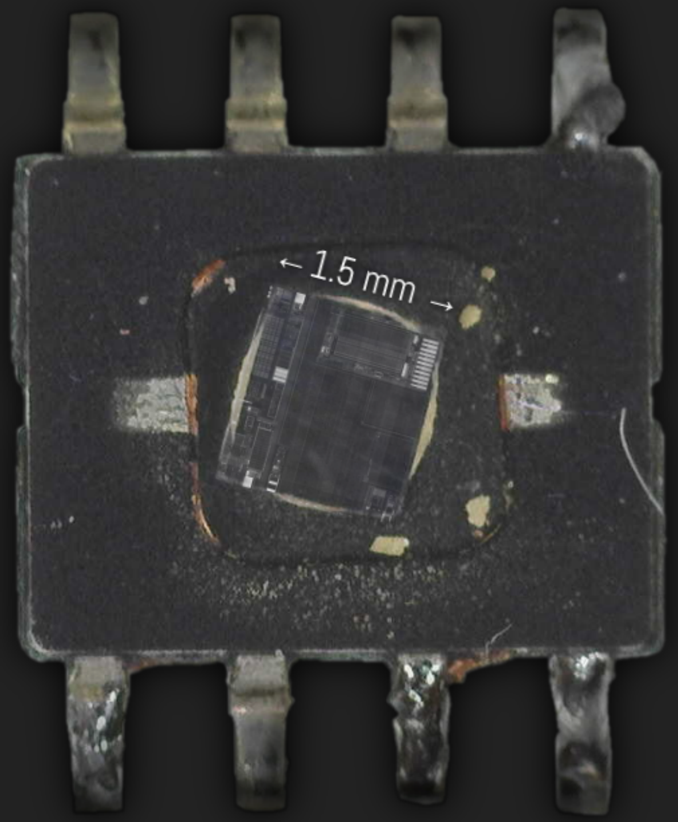
Ouverture face-arrière



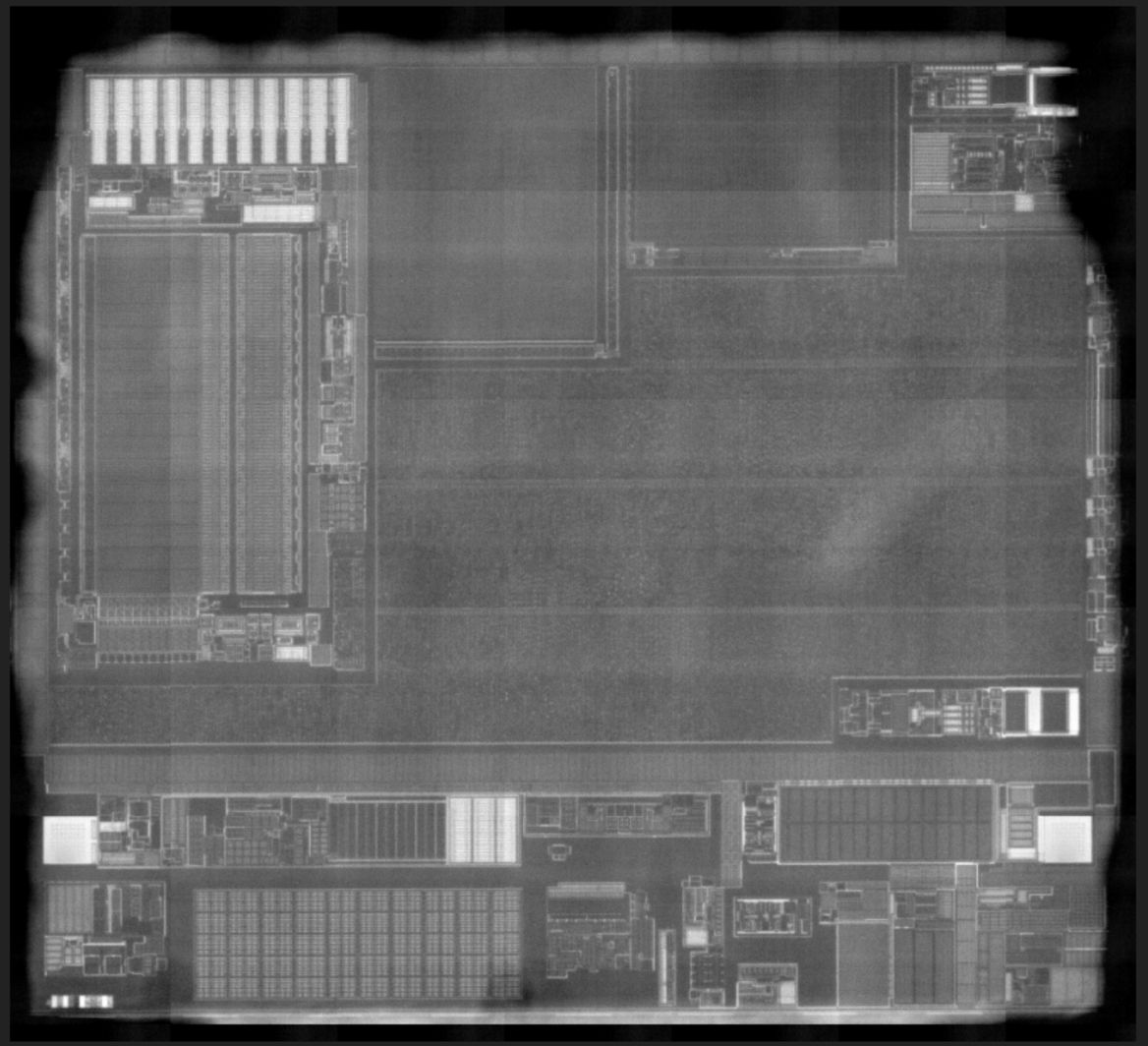
Ouverture face-arrière



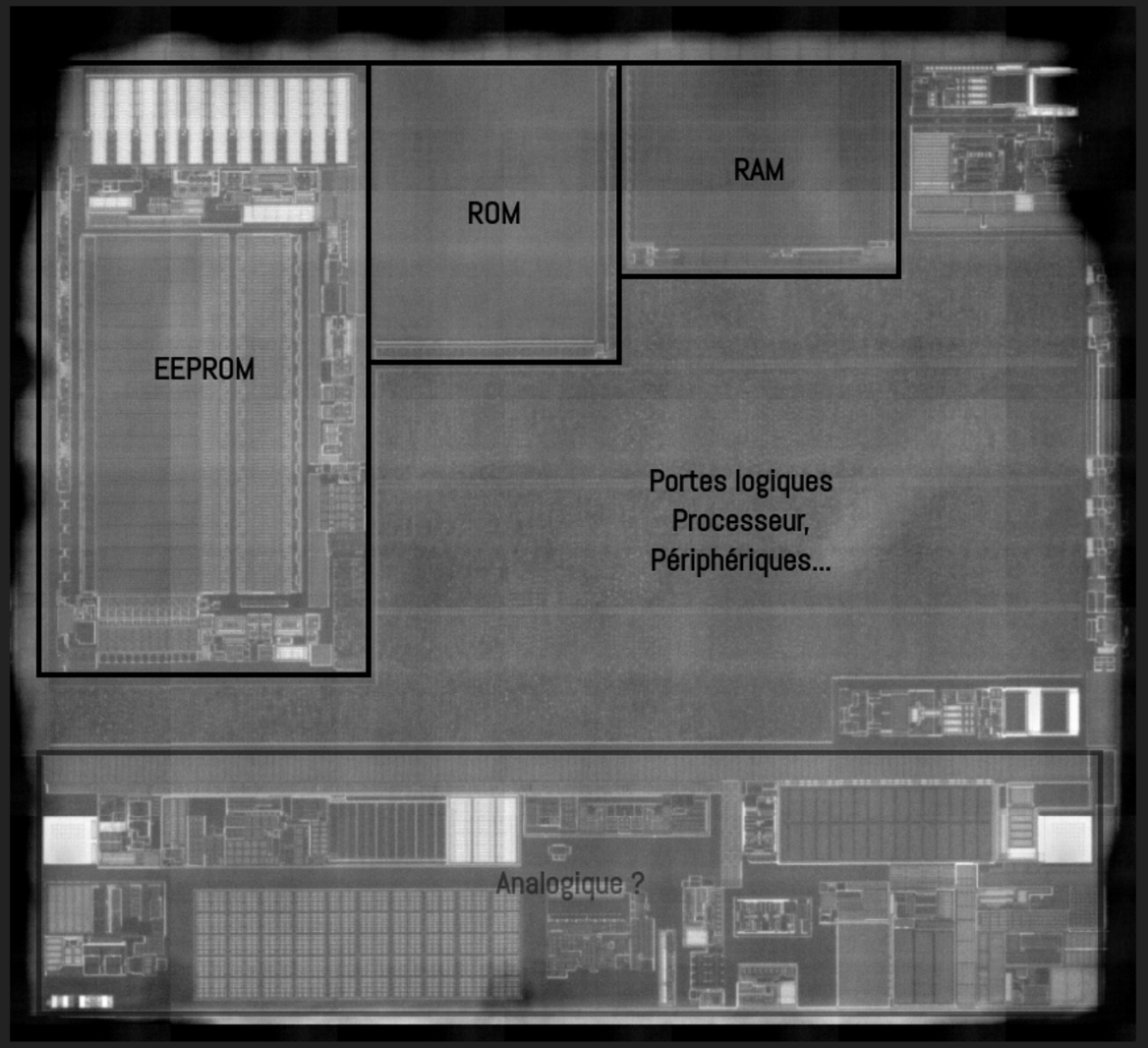
Ouverture face-arrière



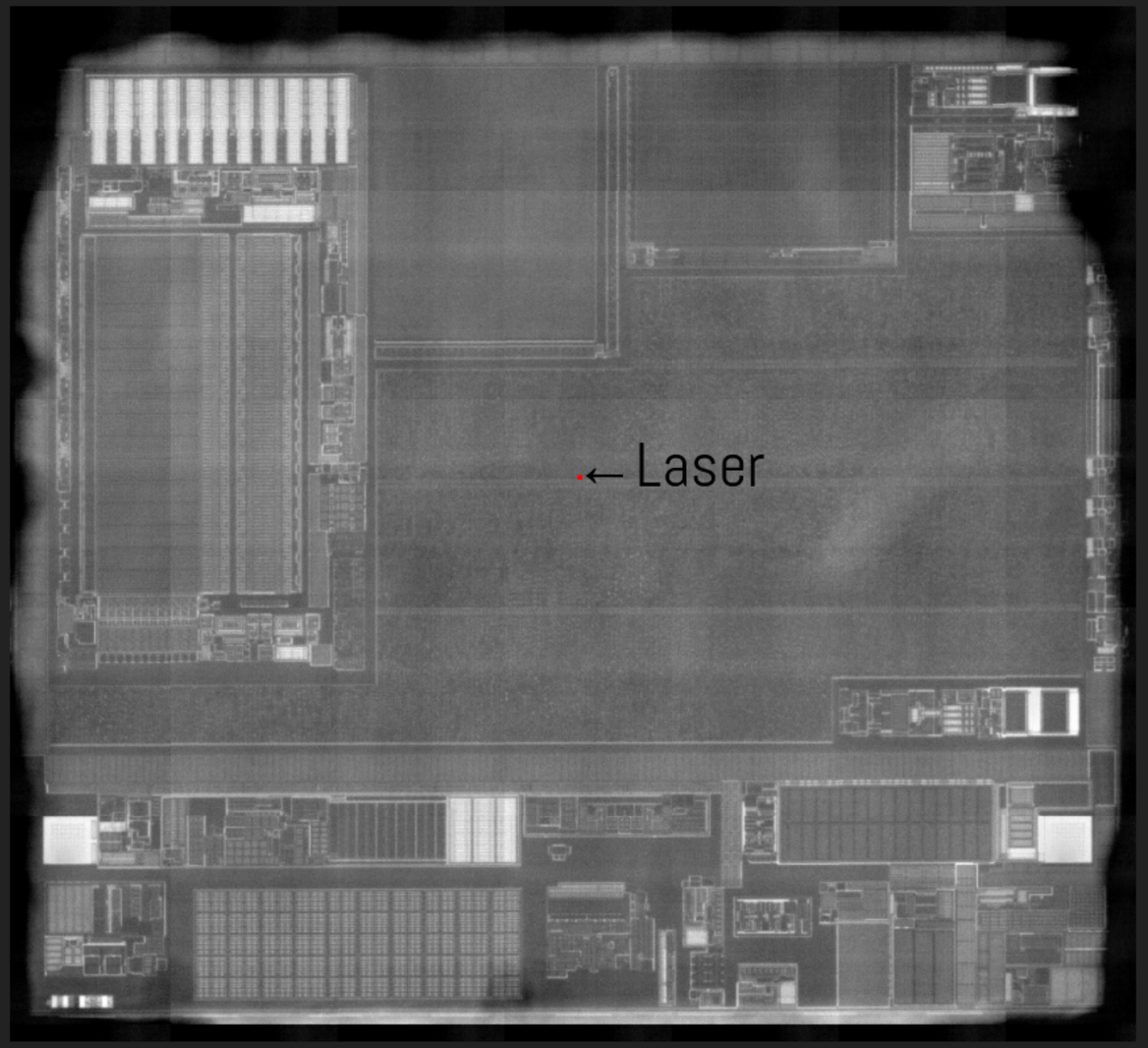
Imagerie infra-rouge



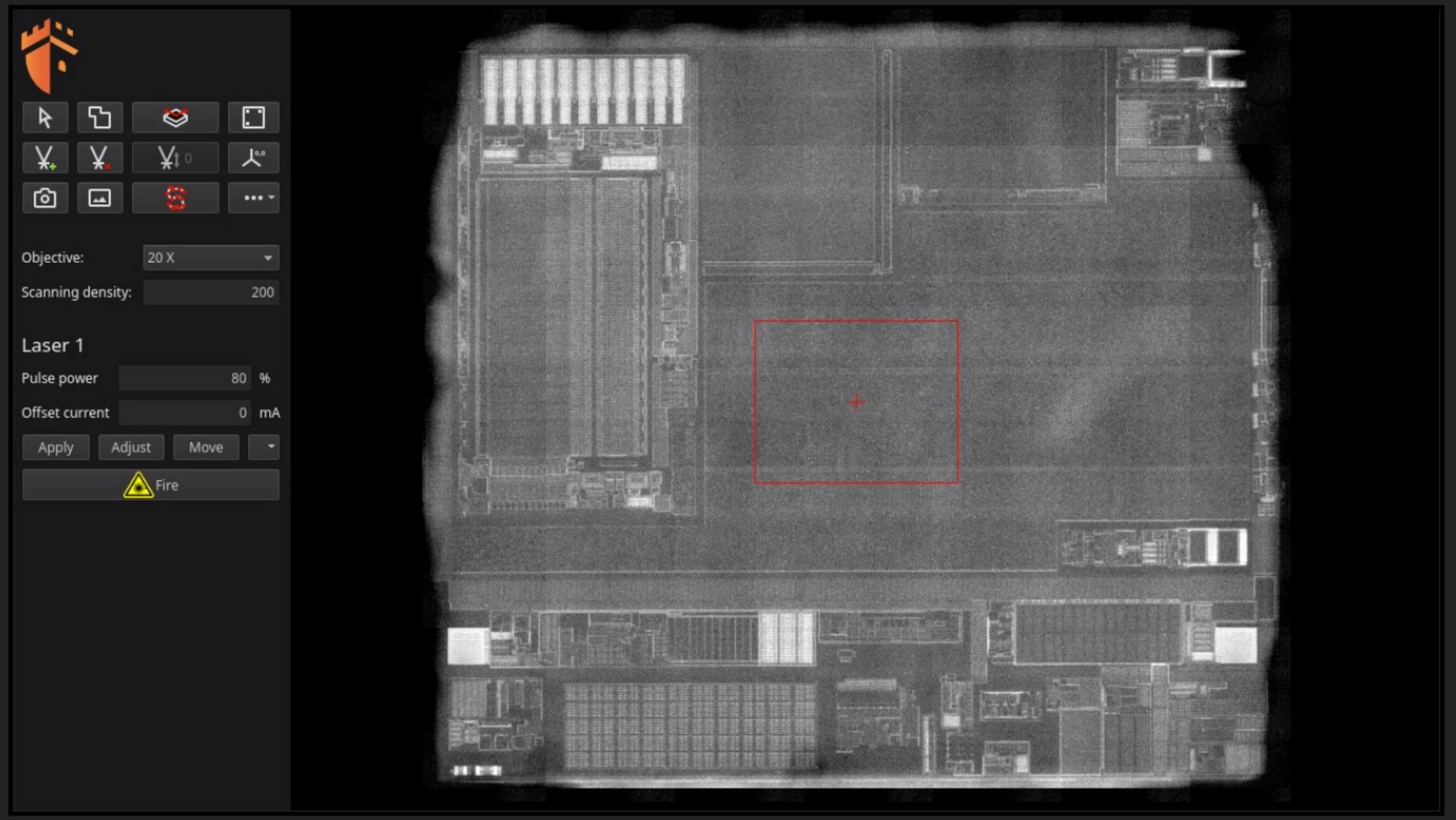
Imagerie infra-rouge



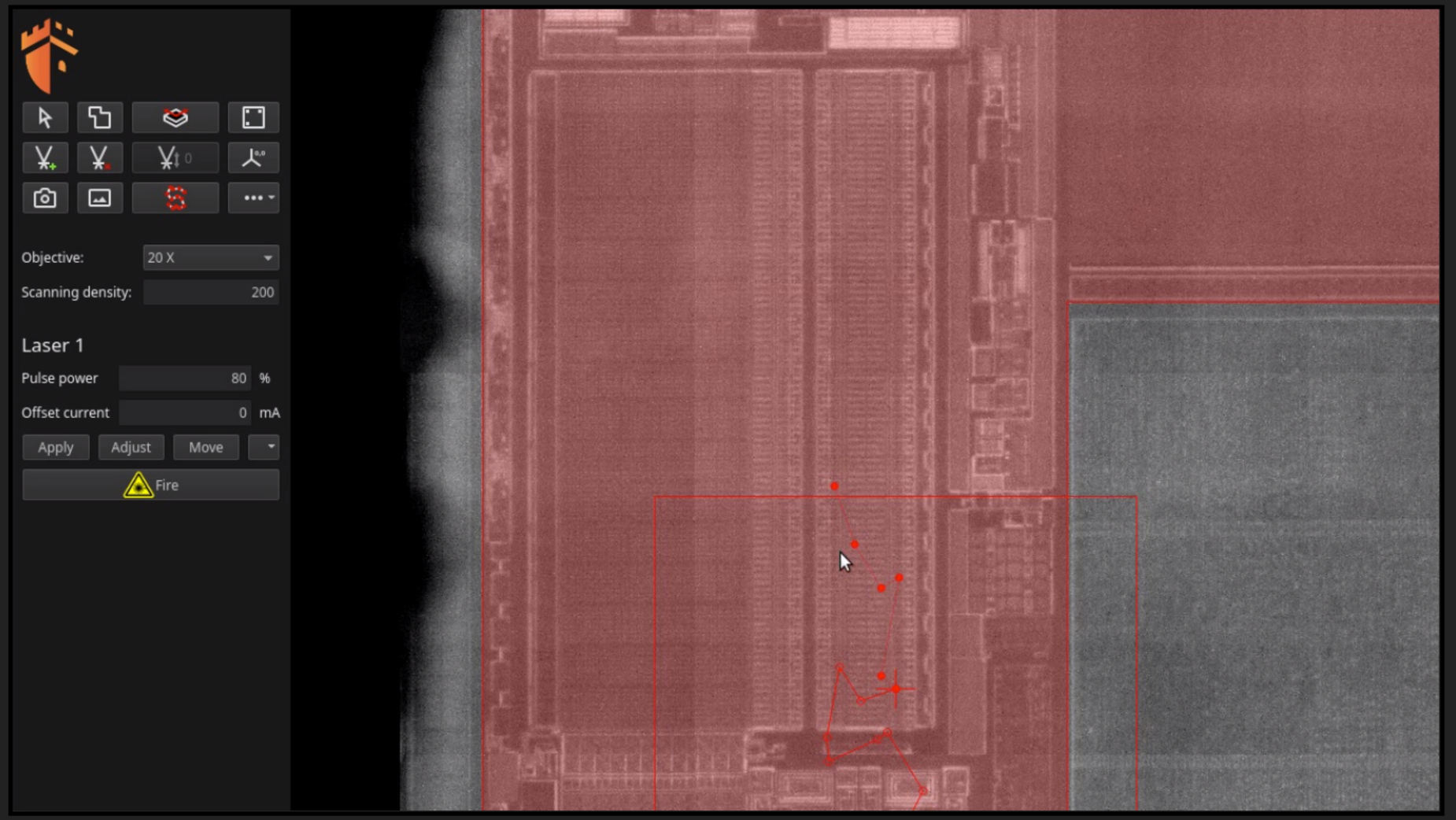
Imagerie infra-rouge



Ciblage


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

Ciblage


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

Campagne de test

Pour chaque test :

1. Réglage de l'instant de tir
2. Déplacement du laser
3. Mise sous tension
4. Initialisation
5. Activation du laser
6. Commande *ReadMemory* + tir laser
7. Désactivation du laser
8. Lecture réponse
9. Mise hors tension
10. Journalisation

Campagne de test

```
Test #1:
  EXECUTION_ERROR
Test #2:
  Timeout, no response received!
Test #3:
  PARSE_ERROR
Test #4:
  OK 09c842000000000000000000000000000000000000000000000000000000000000
Test #5:
  OK 41e0f633a019cd625920691b11400c9387009e68d0b13e53d73257216a4c0ce8
Test #6:
  UNKNOWN_ERROR 0xFF
Test #7:
  EXECUTION_ERROR
Test #8:
  OK
Test #9:
  OK 2ffef9424c7e67d31b519d3d4ea96444265a5189aadba8ab27624ca34c2fdf27
...
```

Campagne de test

343617

fautes injectées

Plusieurs jours de test

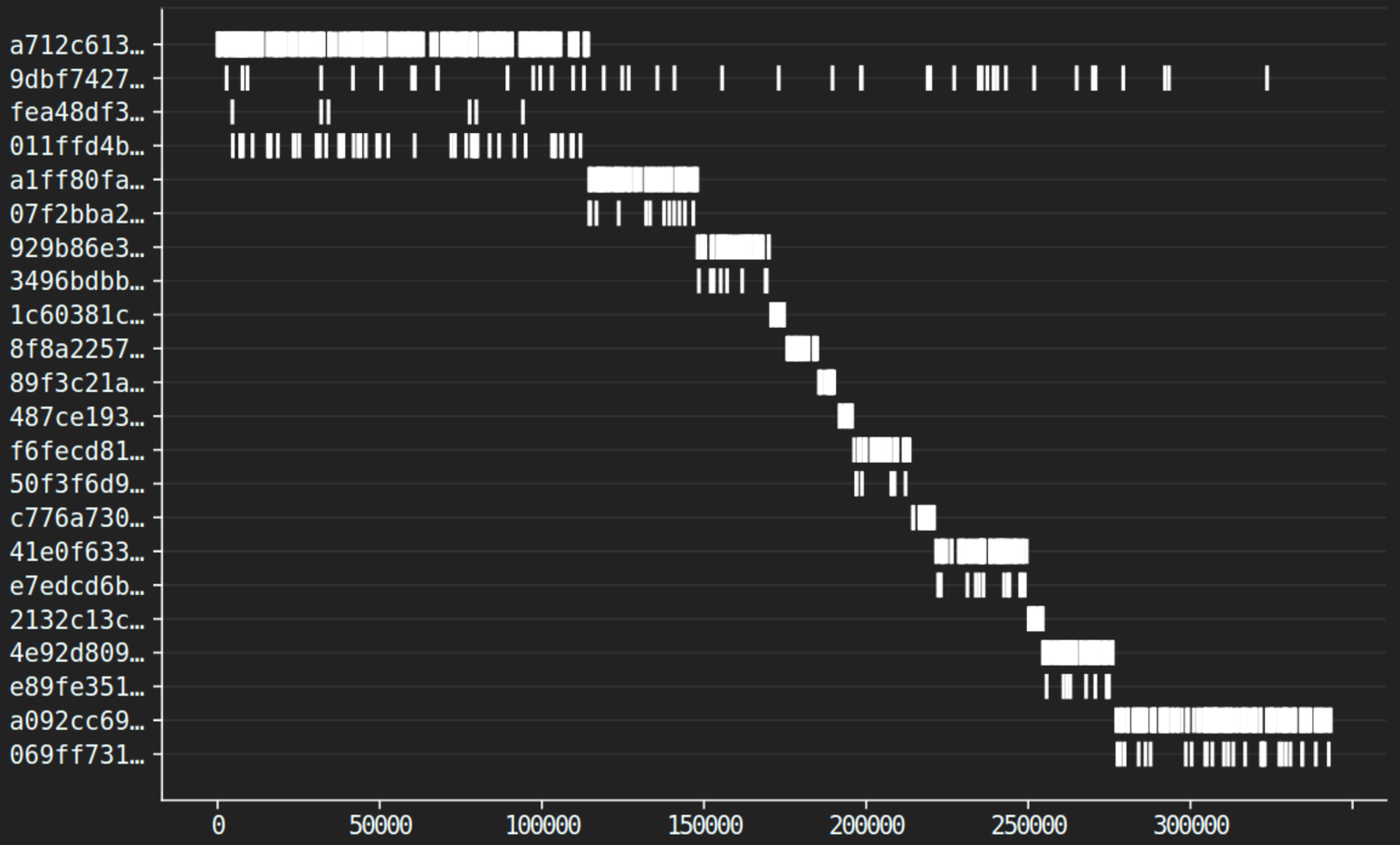
1546 réponses reçues

Pas de succès dans les journaux...

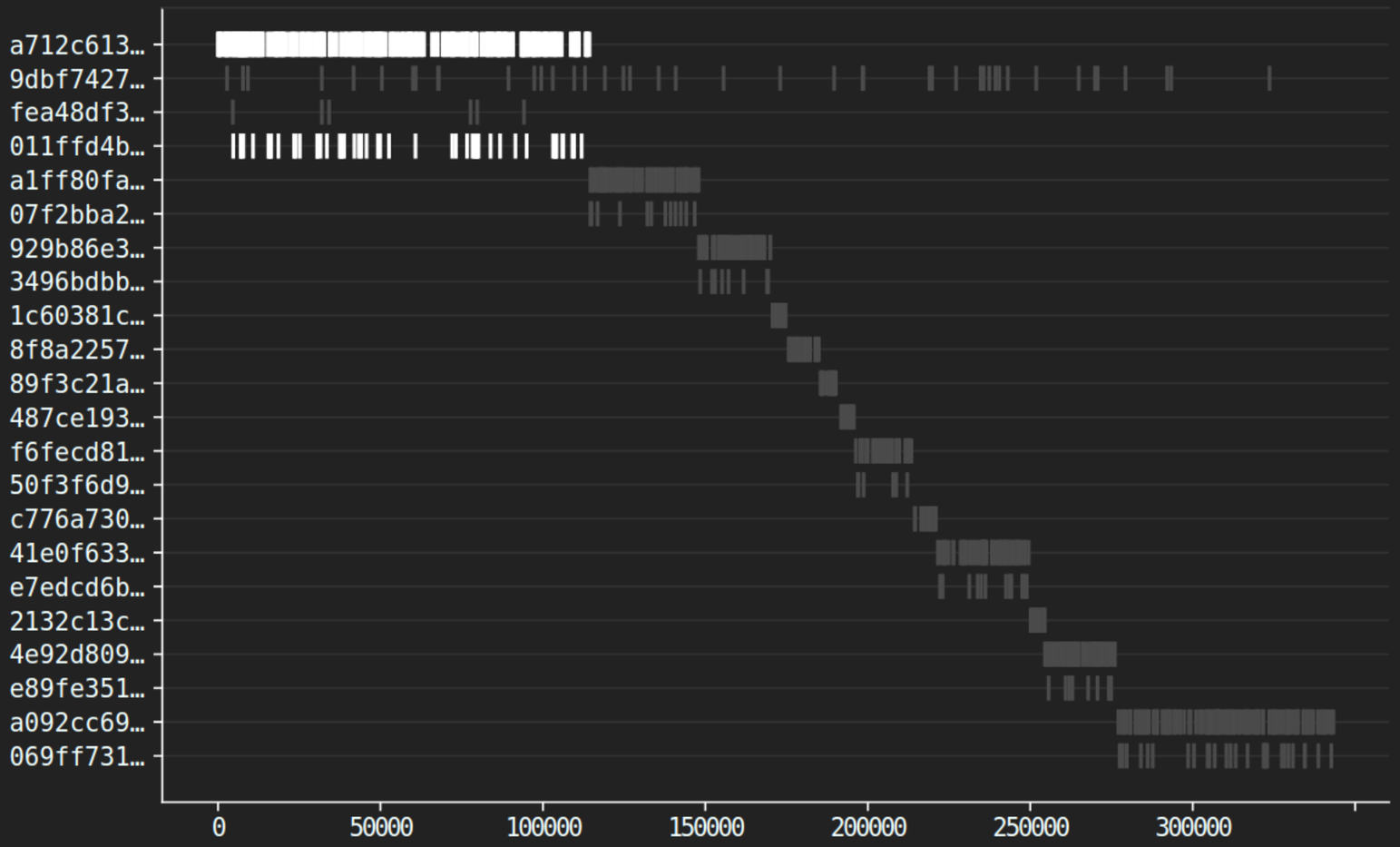
Top 20

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	09c842000000000000000000000000000000000000000000000000000000000000000...
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

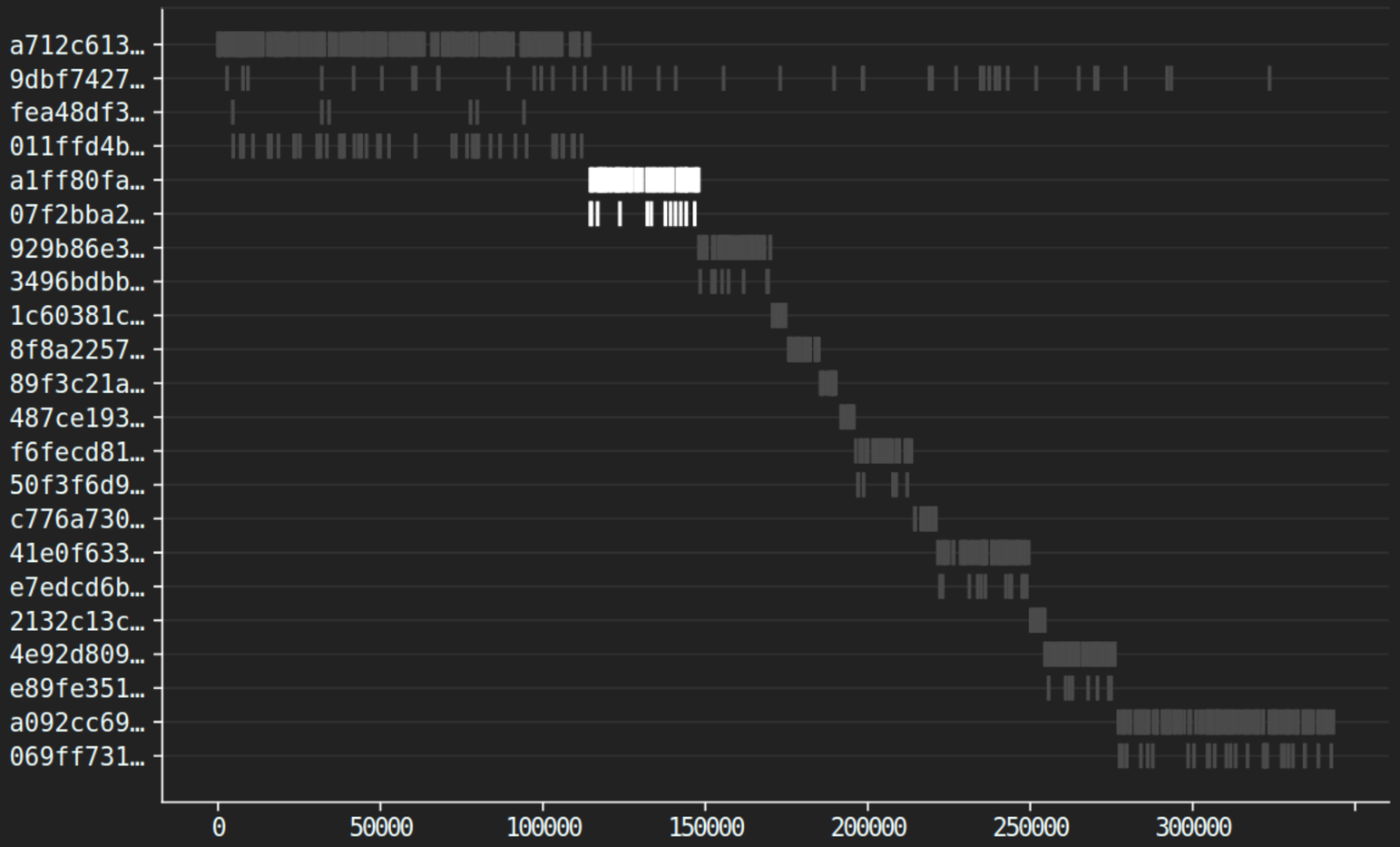
Analyse


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

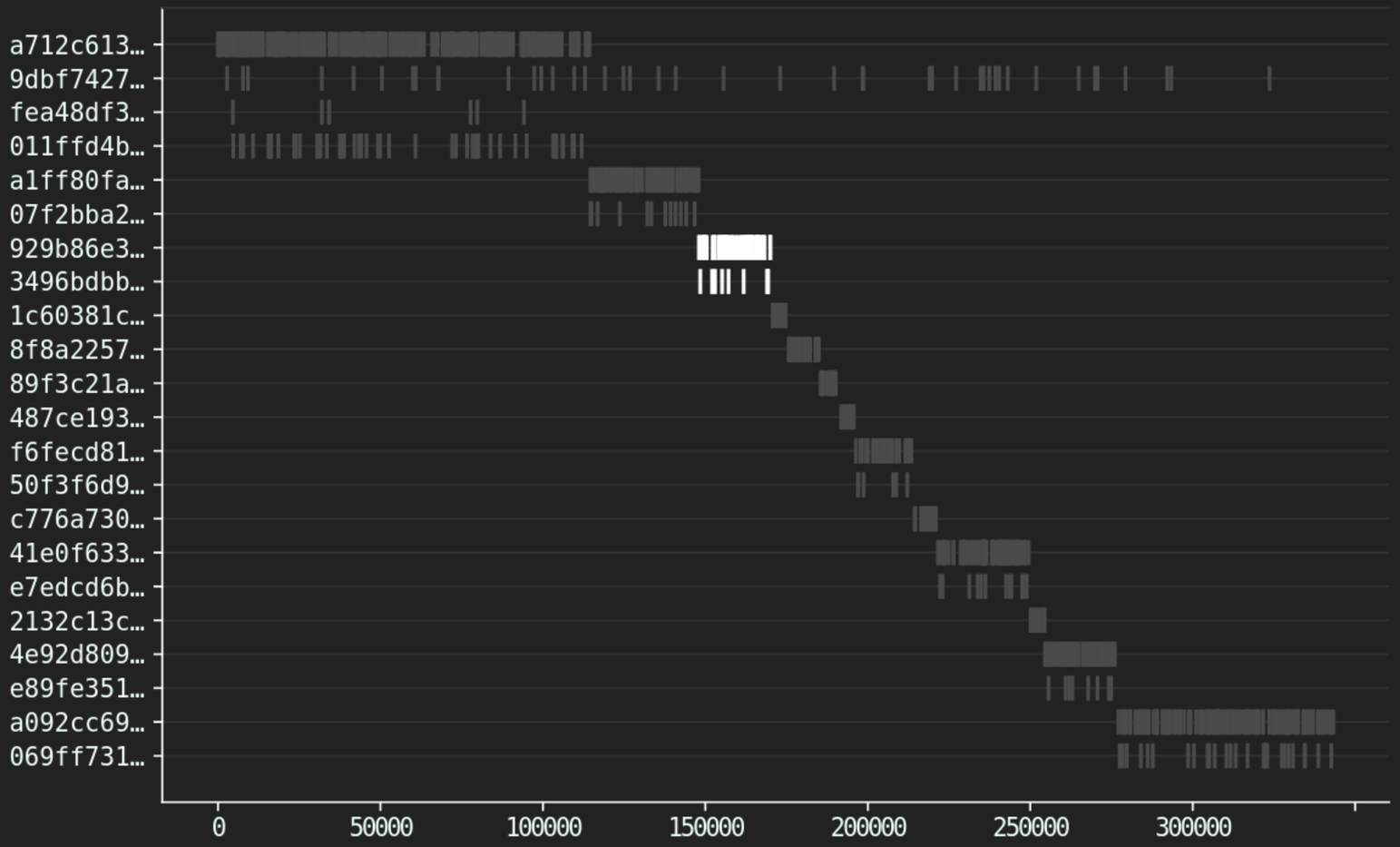
Analyse


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

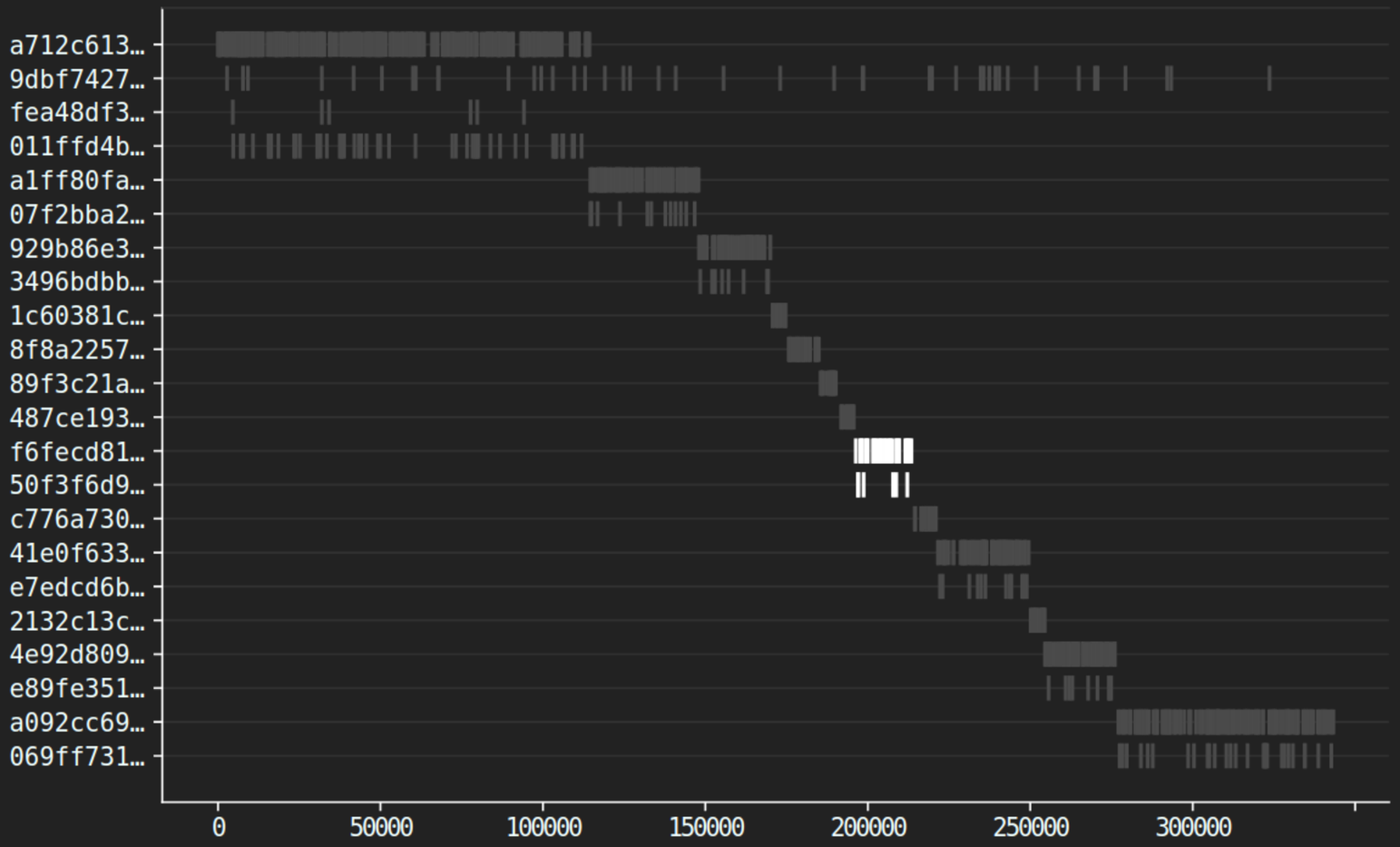
Analyse


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

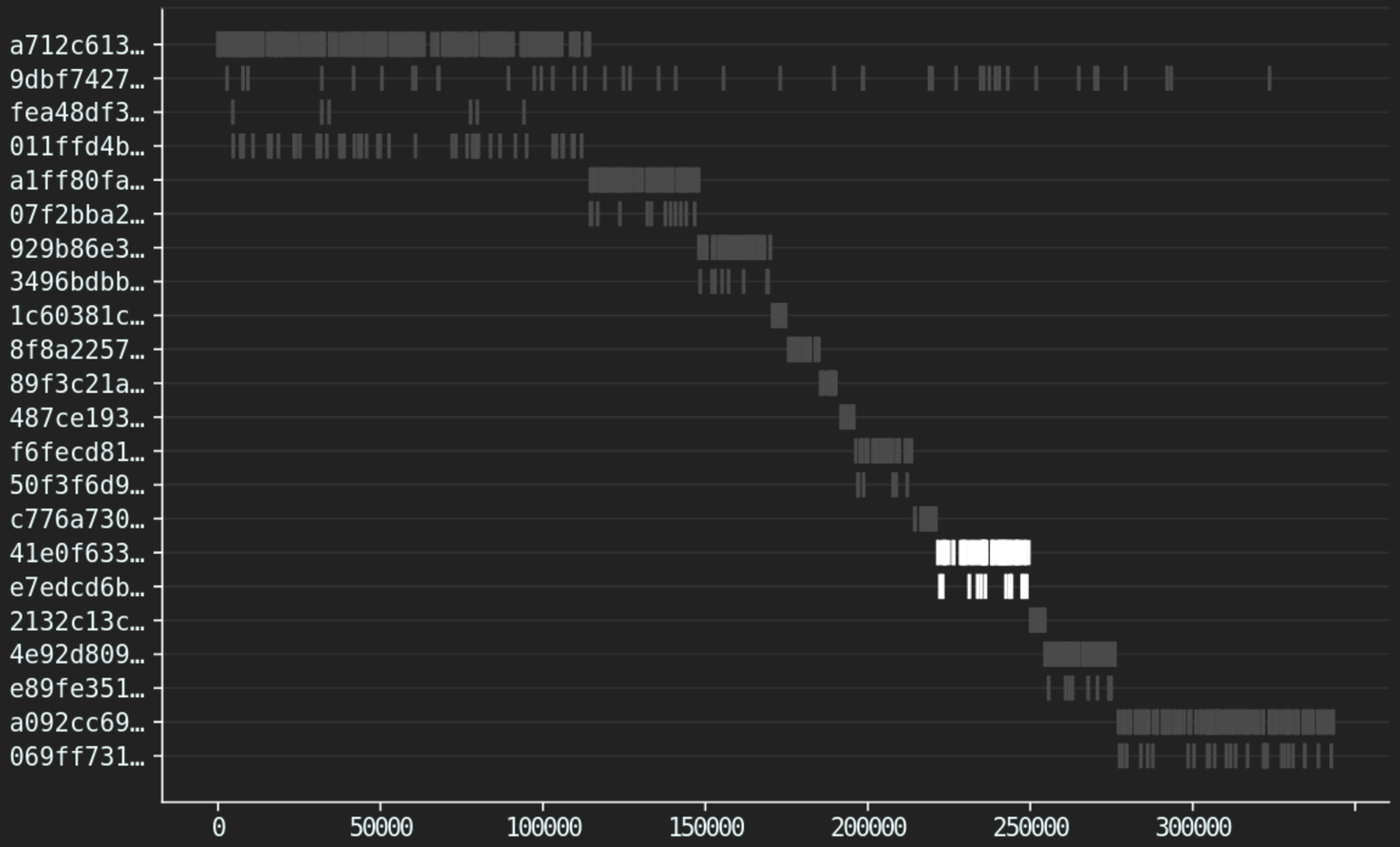
Analyse


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

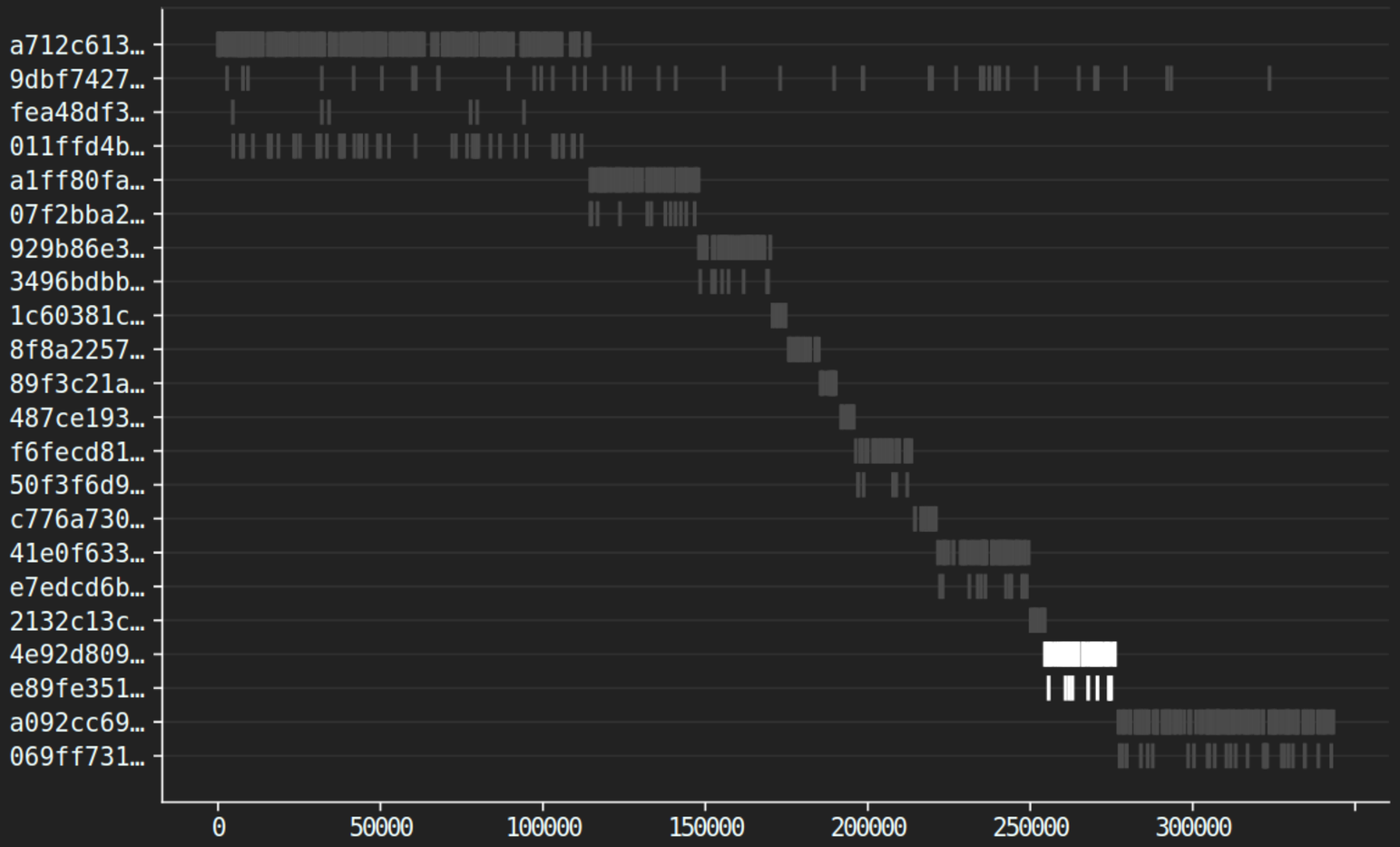
Analyse


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

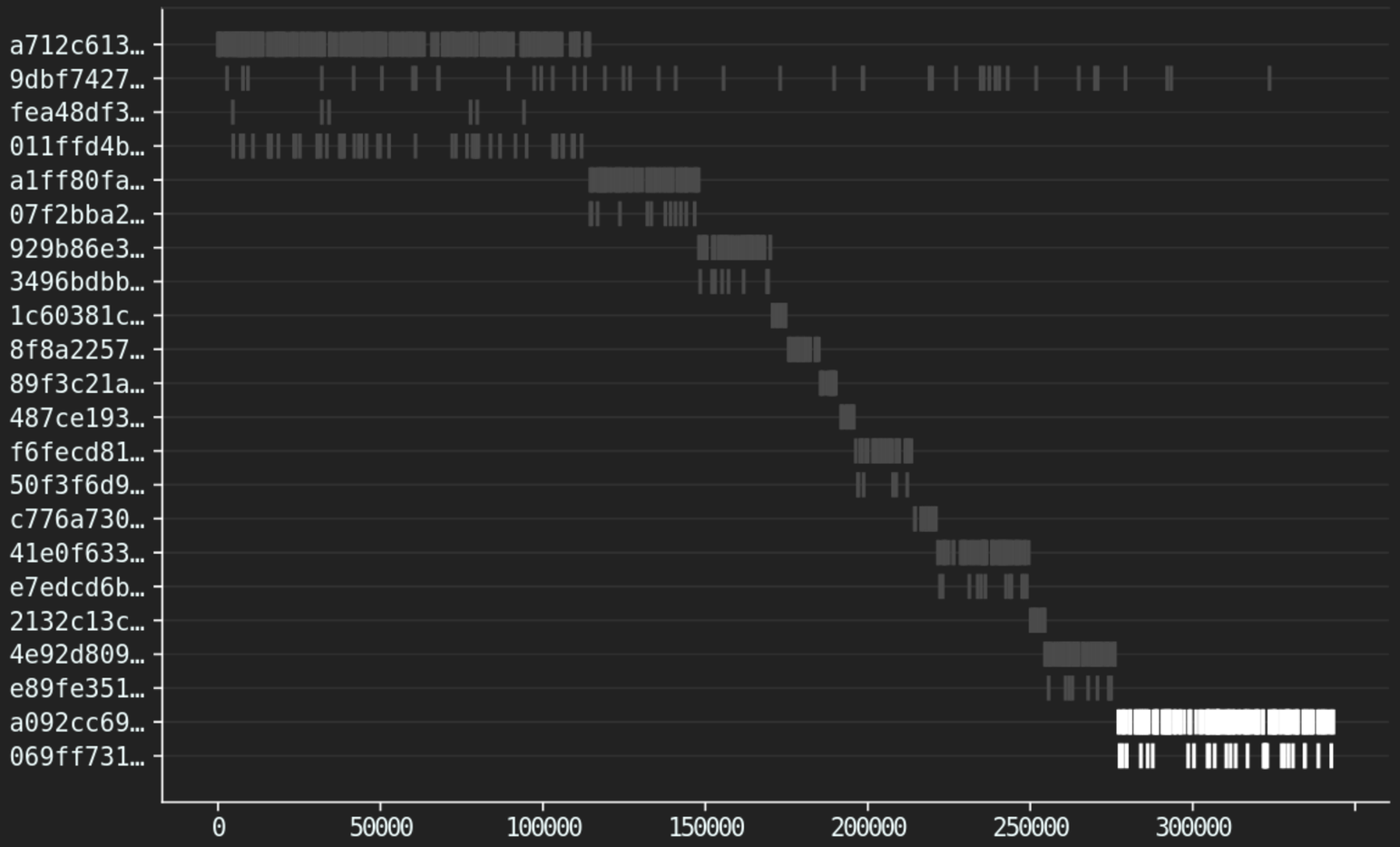
Analyse


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

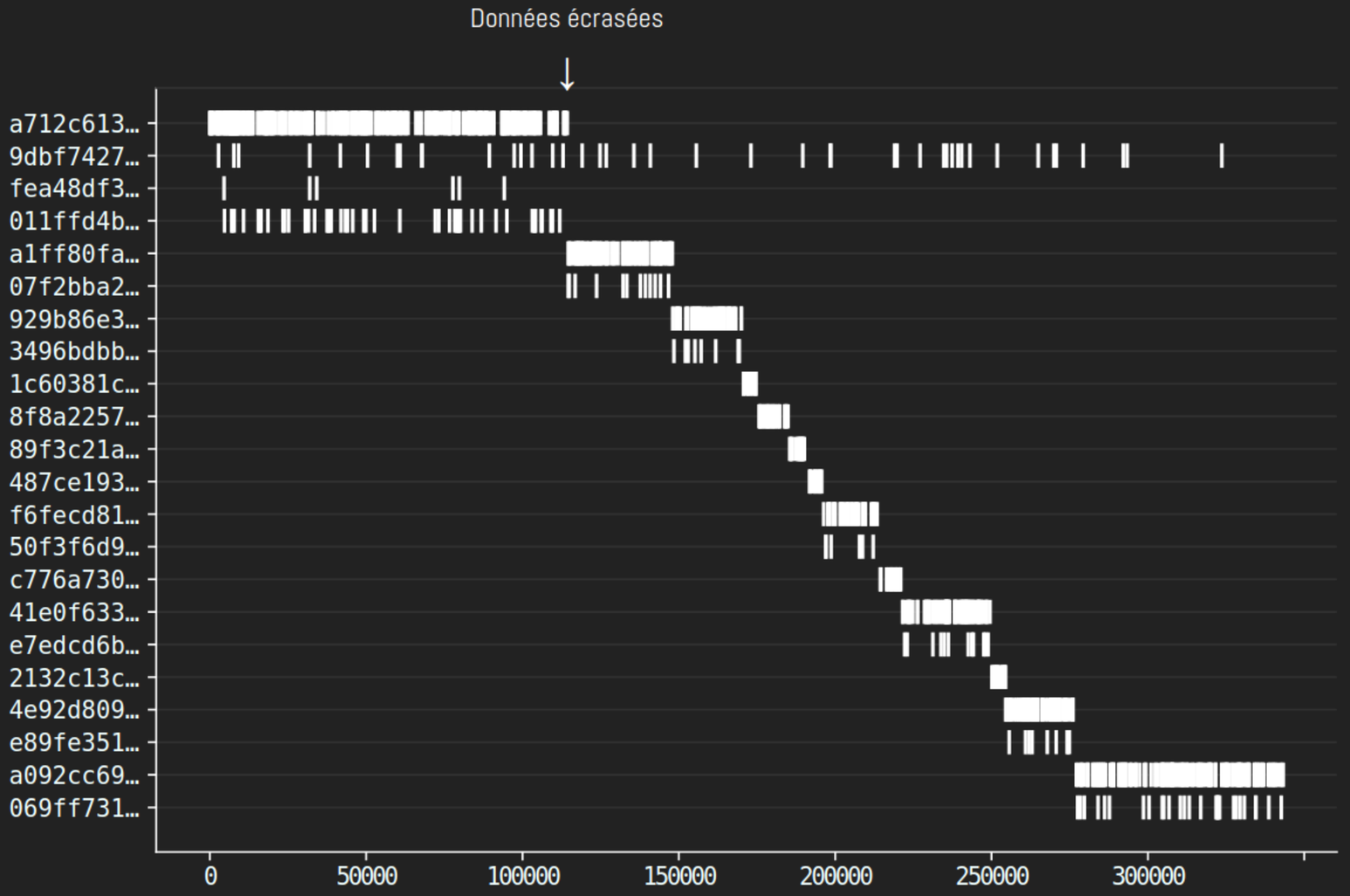
Analyse


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

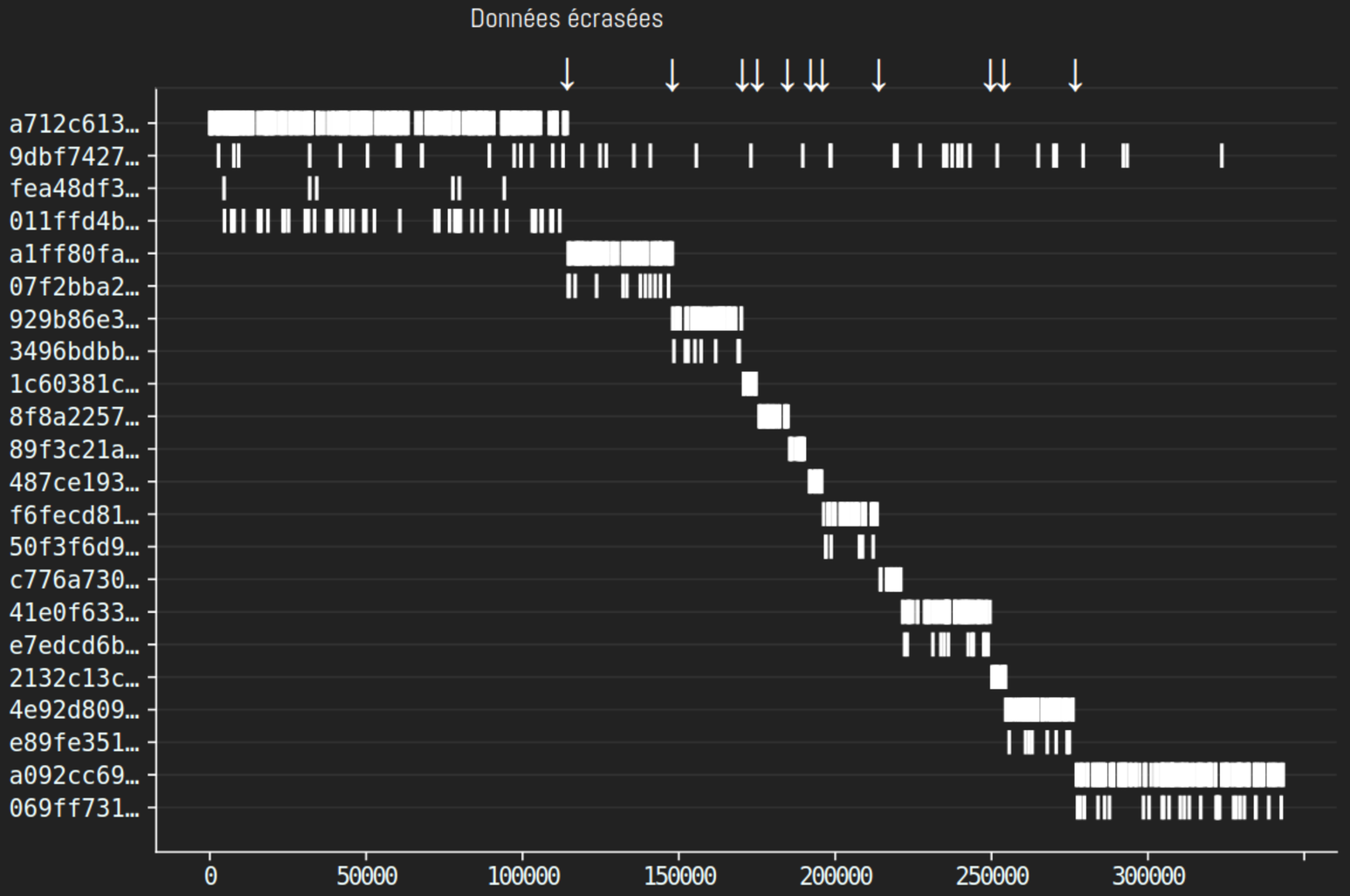
Analyse


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

Analyse


Données écrasées
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

Analyse


Données écrasées
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

On chauffe !

L'attaque semble fonctionner !

Peut-on y arriver sans perdre les données ?

Raffinement de l'attaque

Identification des paramètres optimaux de l'attaque

Préparation nouvel échantillon

Relancement des tests

Succès !

Deux minutes de test seulement

Fichiers secrets PIN1 et clef d'appairage extractibles
Permet l'accès au fichier Seed1

Coldcard Mk2 vulnérable

Attaque réaliste

Conclusion

Attaque de haut niveau
Matériel très onéreux

Configuration particulière
Clés P-256 non vulnérables

Moins résistant qu'un Secure Element

ATECC508A maintenant déprécié
Remplacé par l'ATECC608

Merci !