Hacking iButtons

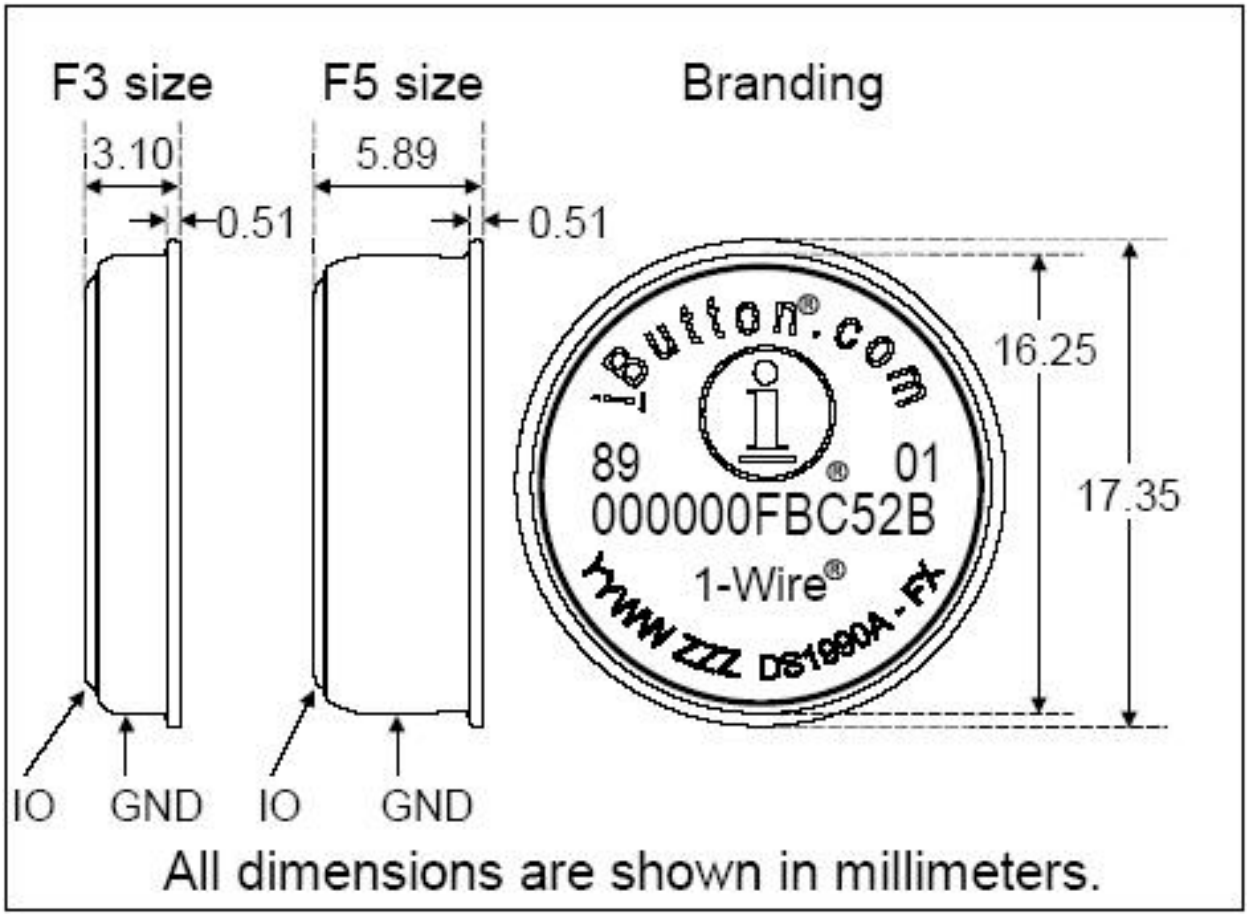
Christian Brandt

2011-04-23

Übersicht

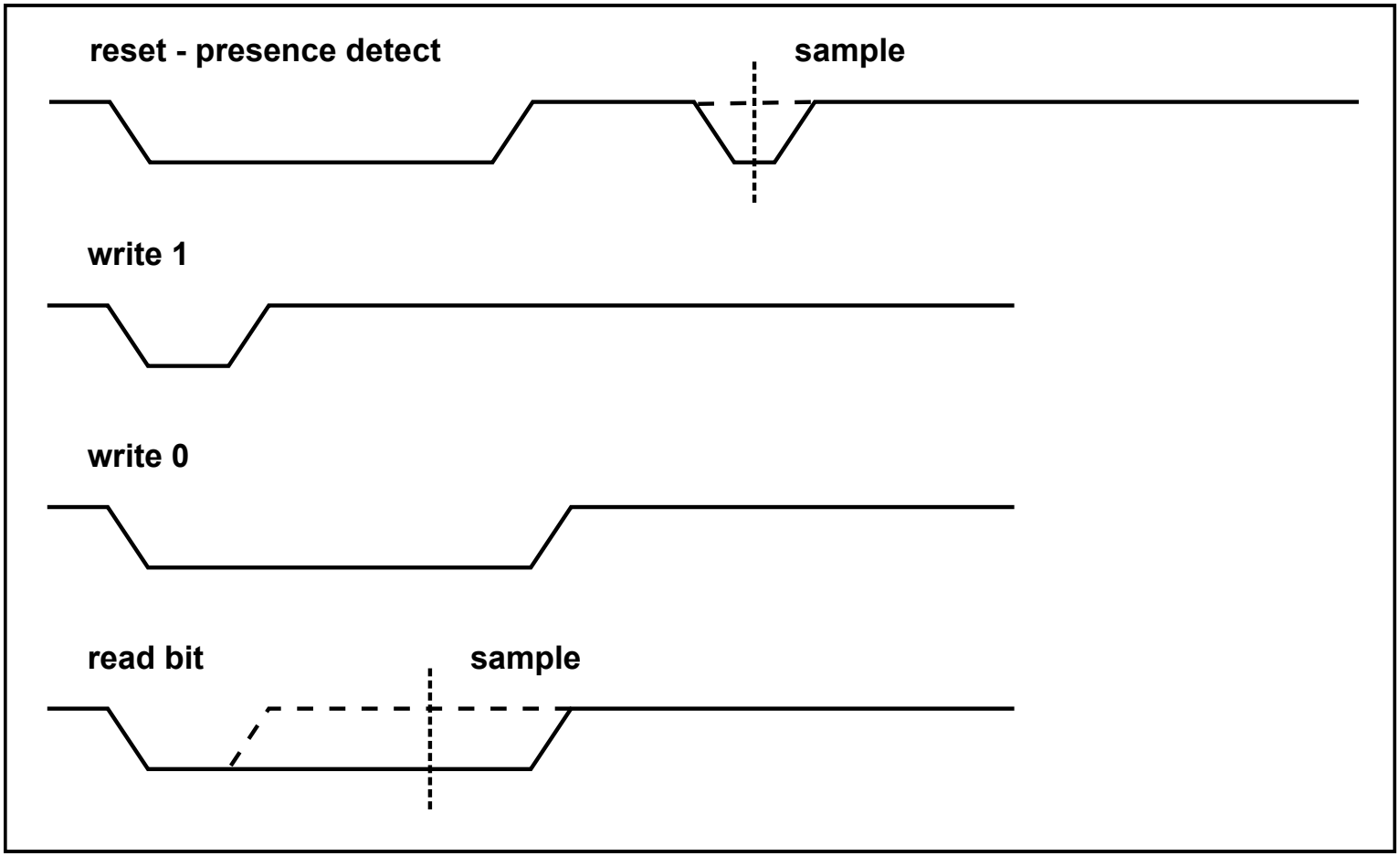
- iButtons ohne Crypto
  - iButton Spezifikation
  - 1-Wire Protokoll
  - Sicherheit durch Seriennummern
- iButtons mit Crypto
  - Soft Feature Management
  - Wahlcomputer
  - Bezahlsysteme
  - Angriff auf DS1963S iButton

iButton Spezifikation

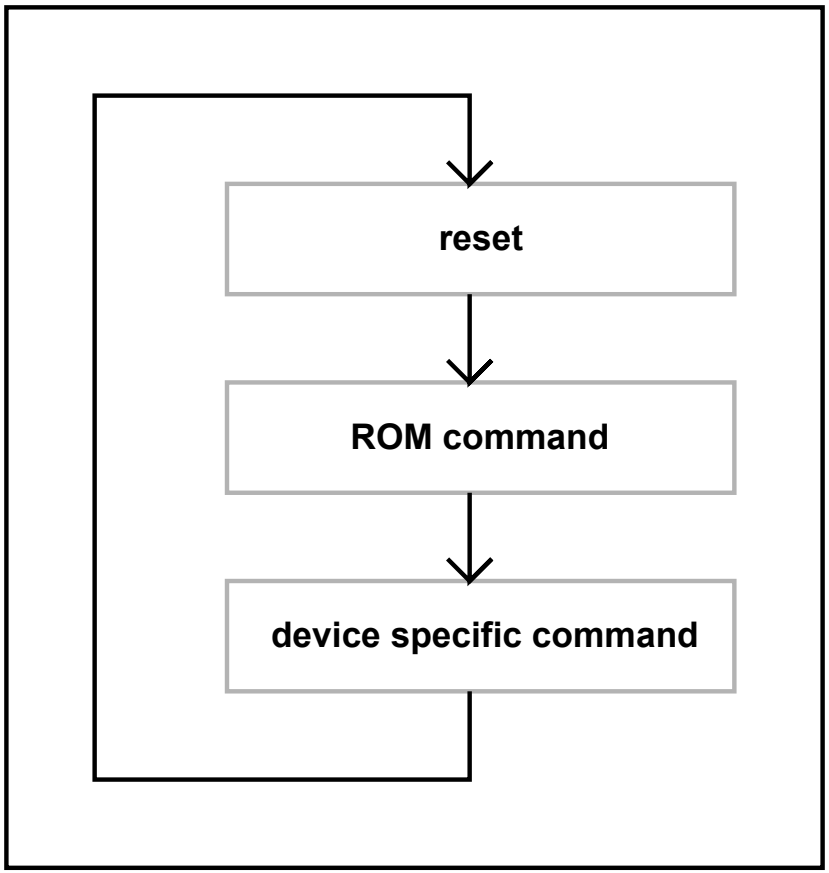


iButton Key Fob

1-Wire Bitübertragung



1-Wire Kommunikationsprinzip



1-Wire Devices

- Temperatursensoren / -logger
- Feuchtigkeitssensoren / -logger
- ADC
- RTC
- Akku-Controller
- EEPROM / SRAM Speicher
- Seriennummern

1-Wire Seriennummer

3F0000004A323F18

- bei Herstellung per Laser gesetzt
- einmalig
- unveränderbar
- theoretisch 64bit groß


Starter-Package:
e-primo-cylinder
+
media kit
EVVA
e primo


EVVA

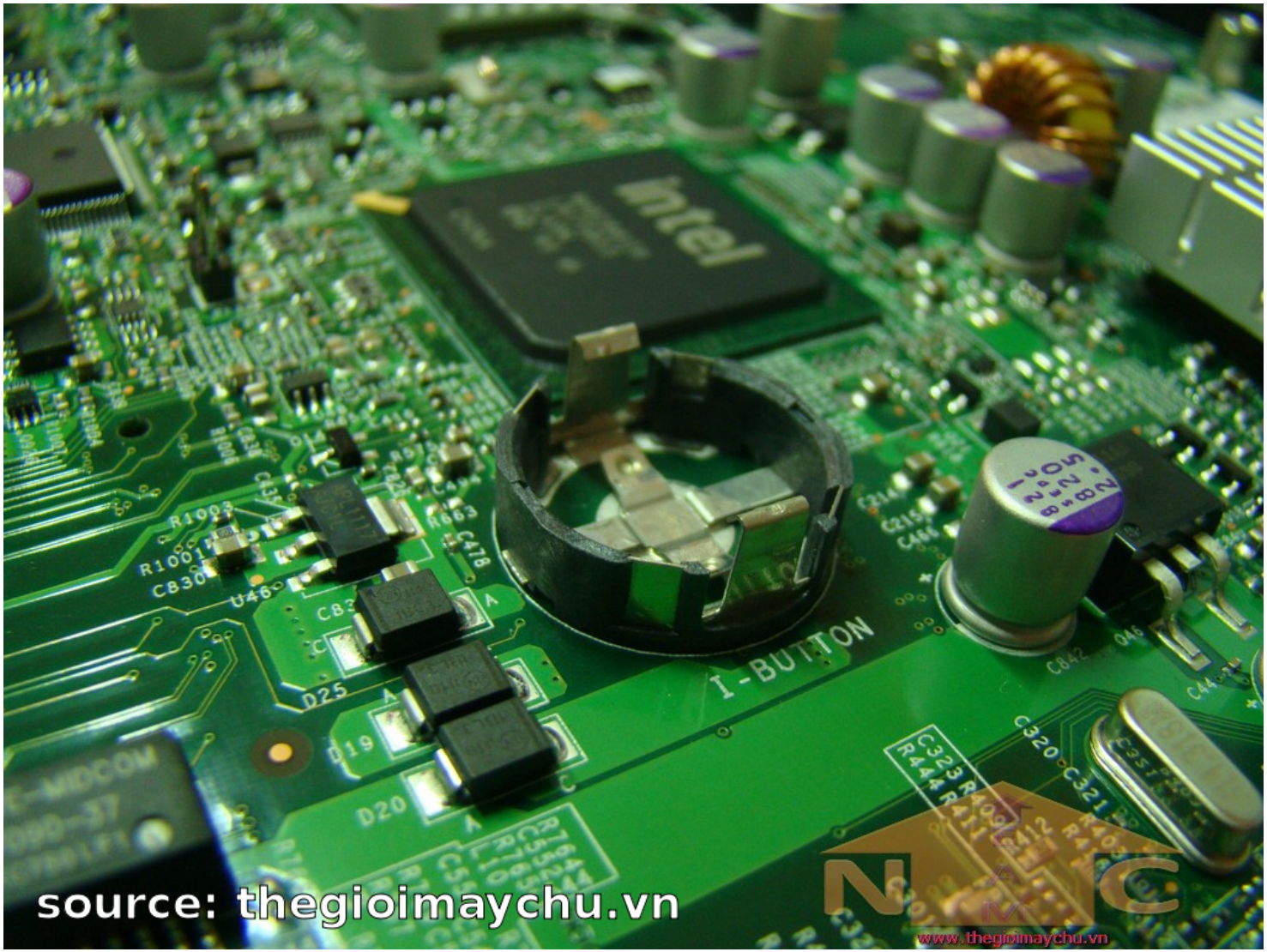
Hier fehlt leider was ...


Fahrausweise
Tickets

SHA-1 iButtons

- DS1961S
  - 128 Byte EEPROM
  - 1 Secret/Key (64 Bit)
  - User Token
- DS1963S (SRAM Version)
  - 512 Byte SRAM
  - 8 Secrets/Keys (je 64 Bit)
  - interne Lithium-Zelle
  - User Token und Coproc
- “World-Class Security for Access Control and eCash Applications”

Soft Feature Management - RAID KEY




Cancel
Return


Security Key

The system utilizes the SHA (secure hash algorithm) iButton ([redacted]) security keys with factory-lasered [redacted] address that is unalterable and unique. These security tokens have an integrated [redacted] cryptographic processor with the ability to perform [redacted] transformations and to securely store and protect secrets within its NVRAM (Non-volatile RAM) memory. The token has sixteen 32-byte memory pages in addition to the storage for [redacted] [redacted] secrets. In addition, the token has lithium power source inside its stainless steel container. [redacted] is non-reversible, collision-resistant, and has a good avalanche effect. The SHA series of hashes are currently the only FIPS-approved method and are specified in ISO/IEC 10118-3.

The system utilizes the SHA (secure hash algorithm) iButton (DS1963S) security keys with factory-lasered 64-bit address that is unalterable and unique. These security tokens have an integrated SHA-1 cryptographic processor with the ability to perform SHA-1 transformations and to securely store and protect secrets within its NVRAM (Non-volatile RAM) memory. The token has sixteen 32-byte memory pages in addition to the storage for eight separate SHA-1 secrets. In addition, the token has lithium power source inside its stainless steel container. SHA-1 is non-reversible, collision-resistant, and has a good avalanche effect. The SHA series of hashes are currently the only FIPS-approved method and are specified in ISO/IEC 10118-3.

eCash: Monetary iButtons

- Micropayment
- keine Verbindung zu Backend
- Geldbetrag nur im iButton hinterlegt
- Missbrauch nur über Transaktionslogs feststellbar
- primär im öffentlichen Personennahverkehr verwendet
- Sicherheit stark abhängig von
  - Ticketautomaten
  - Abbuchungsautomaten
  - User Token
- größtes System: Akbil (Türkei)

Akbil - Bus


26-08-2008
Salı
source:
http://www.gundemcafe.com/tag/yeni-akbiller-nasil-olacak/

Akbil - Straßenbahn

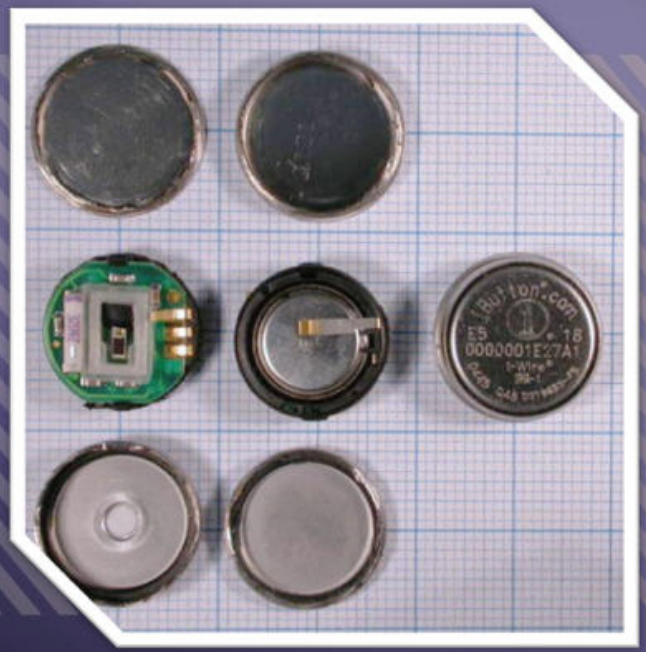
Akbil - Ticketautomat

Akbil - Eckdaten

- 5,5 Millionen Nutzer
- 2 Millionen Debit-Transaktionen pro Tag
- 600.000 (kostenfreie) Umstiege pro Tag
- Aufladen der Tokens an
  - 145 Fahrkartenschalter
  - 58 Fahrkartenautomaten
  - 203 POS Automaten
- verwendete iButtons
  - zuerst DS1991 (passwortgeschütztes EEPROM)
  - danach DS1963S

İstanbul Büyükşehir Belediyesi
Belbim A.Ş

AKBİL'İNİZ BOZULDUĞUNDA

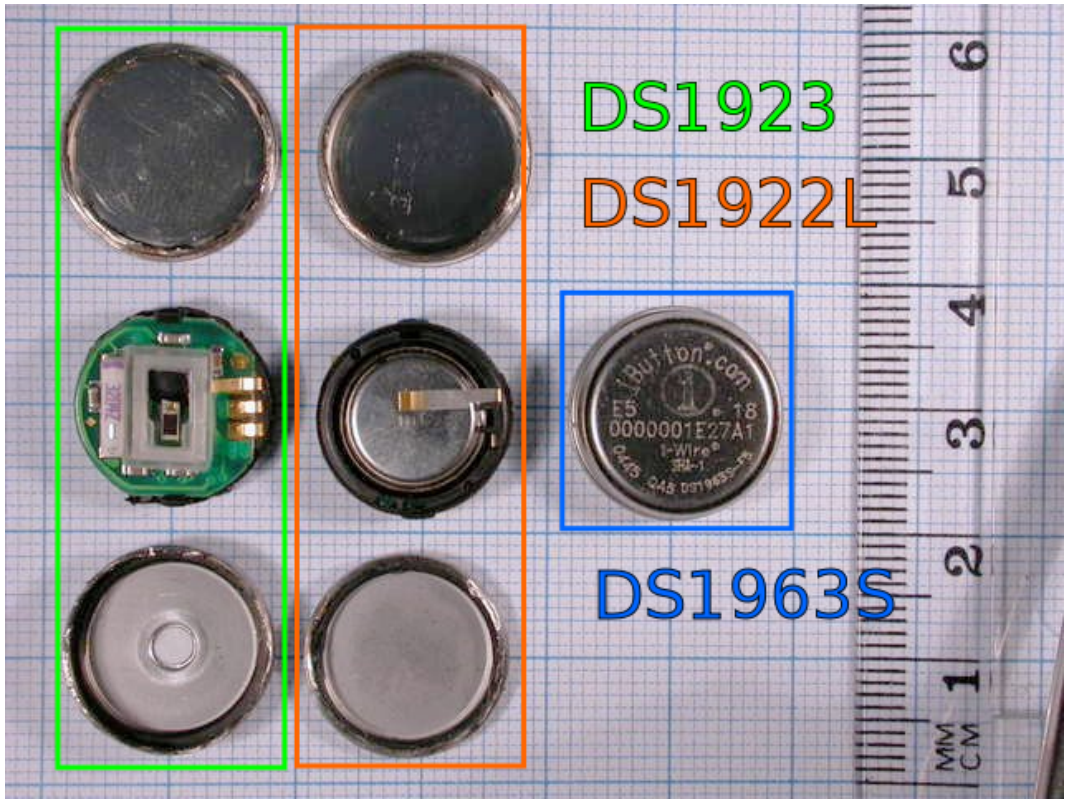


Üstün teknolojilerle donatılmış AKBİL'iniz, ender rastlanabilecek bazı nedenlerden dolayı işlevini gerçekleştirmeyebilir.

Bu durumda AKBİL'iniz;

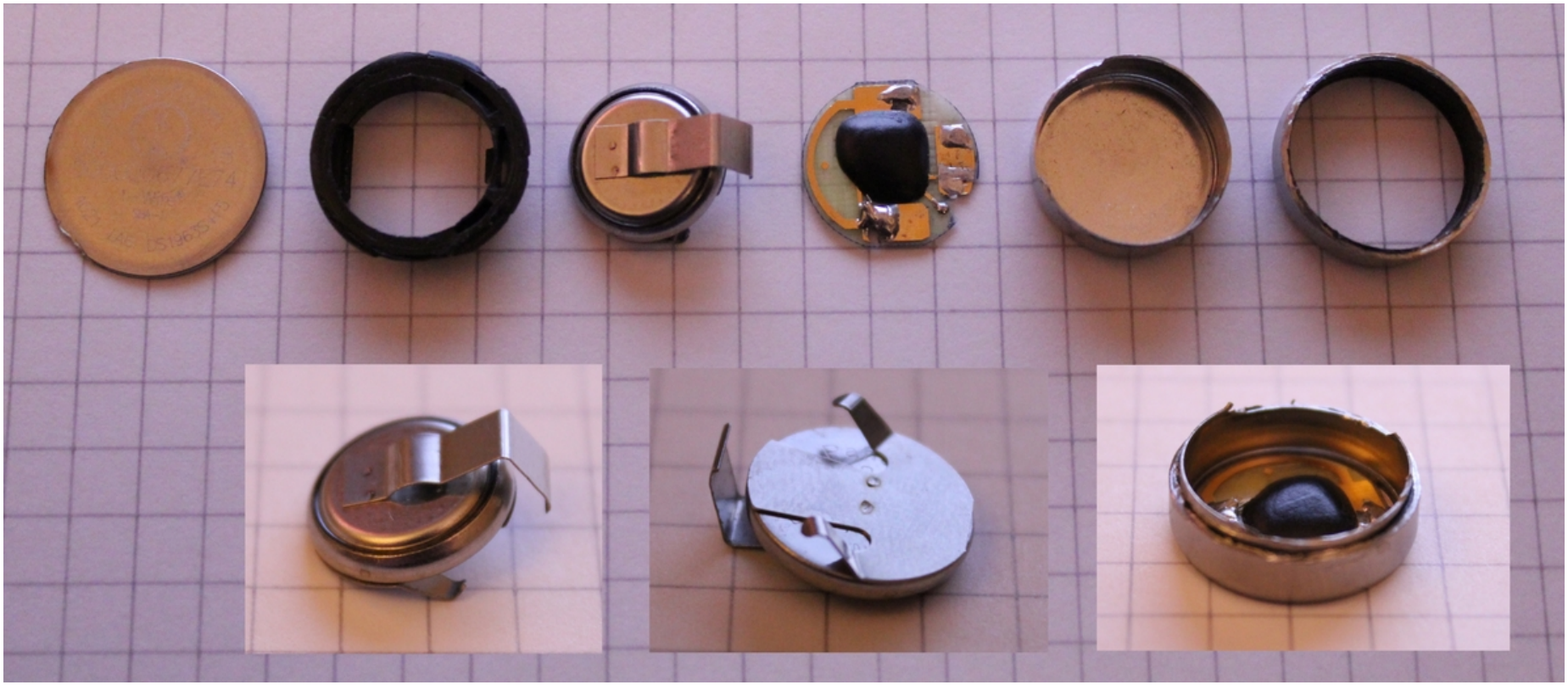
* Kullanım dışı, geçersizdir
* Yenilenmeli gişeye götürün
* AKBİL hatalı mesajları vermektedir.

source: http://www.flickr.com/photos/sunumer/2326577288/



source: http://www.cl.cam.ac.uk/~sjm217/projects/ibutton/

DS1963S zerlegt



Security by Obscurity

- “World-Class Security in Stainless Steel Case for Access Control and eCash Applications”
- “Request Full Data Sheet”
  - “This product is designed for a highly specific application. The detailed data sheet contains information about proprietary technology, and is only available to customers whose requirements closely match this application. To request the data sheet, please complete the following information detailing your requirements.”
  - “Unfortunately we are unable to respond to requests that do not meet our qualification criteria. If you do not receive a response within two business days, please select another part. Technical support for this product is NOT available from our normal Tech Support desk.”
- datasheetarchive.com

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	C0F4E2925E70A713	C0055BEE19E3C519	1B1D9FBBA3F8AE89	B85B29B2806011B1
01	00	20	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
09	01	20	E053017B691B3383	C05AB12A924BACB4	0E9A321A6B9A75A4	32117BD19F84826A
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	8000000031000000	70000000B9000000	FA00000000000000	0000000000000000
14	02	80	00000000B7120000	FAD82000BA210000	0000000000000000	0000000000000000
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	**C0F4E2925E70A713**	**C0055BEE19E3C519**	**1B1D9FBBA3F8AE89**	**B85B29B2806011B1**
01	00	20	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
02	00	40	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
03	00	60	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
04	00	80	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
05	00	A0	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
06	00	C0	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
07	00	E0	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
08	01	00	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
09	01	20	E053017B691B3383	C05AB12A924BACB4	0E9A321A6B9A75A4	32117BD19F84826A
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	8000000031000000	70000000B9000000	FA00000000000000	0000000000000000
14	02	80	00000000B7120000	FAD82000BA210000	0000000000000000	0000000000000000
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	C0F4E2925E70A713	C0055BEE19E3C519	1B1D9FBBA3F8AE89	B85B29B2806011B1
01	00	20	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
09	01	20	**E053017B691B3383**	**C05AB12A924BACB4**	**0E9A321A6B9A75A4**	**32117BD19F84826A**
0A	01	40	**823FA69EC3EF2B10**	**953527D2772F516E**	**17E17471693CF118**	**D1116BBB0E13301B**
0B	01	60	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
0C	01	80	**0BD76674FF2AC13B**	**211F570DDBC17647**	**F24ED91E9A7C345E**	**B95FBA5D3C015419**
0D	01	A0	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
0E	01	C0	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
0F	01	E0	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
10	02	00	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	8000000031000000	70000000B9000000	FA00000000000000	0000000000000000
14	02	80	00000000B7120000	FAD82000BA210000	0000000000000000	0000000000000000
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	C0F4E2925E70A713	C0055BEE19E3C519	1B1D9FBBA3F8AE89	B85B29B2806011B1
01	00	20	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
09	01	20	E053017B691B3383	C05AB12A924BACB4	0E9A321A6B9A75A4	32117BD19F84826A
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	**FFFFFFFFFFFFFFFF**	**FFFFFFFFFFFFFFFF**	**FFFFFFFFFFFFFFFF**	**FFFFFFFFFFFFFFFF**
11	02	20	**FFFFFFFFFFFFFFFF**	**FFFFFFFFFFFFFFFF**	**FFFFFFFFFFFFFFFF**	**FFFFFFFFFFFFFFFF**
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	8000000031000000	70000000B9000000	FA00000000000000	0000000000000000
14	02	80	00000000B7120000	FAD82000BA210000	0000000000000000	0000000000000000
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	C0F4E2925E70A713	C0055BEE19E3C519	1B1D9FBBA3F8AE89	B85B29B2806011B1
01	00	20	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
09	01	20	E053017B691B3383	C05AB12A924BACB4	0E9A321A6B9A75A4	32117BD19F84826A
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	**FFFFFFFFFFFFFFFF**	**870EC0E9FAD19213**	**153DCF5B06F6AD68**	**75CA8403FFFFFFFF**
13	02	60	8000000031000000	70000000B9000000	FA00000000000000	0000000000000000
14	02	80	00000000B7120000	FAD82000BA210000	0000000000000000	0000000000000000
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	C0F4E2925E70A713	C0055BEE19E3C519	1B1D9FBBA3F8AE89	B85B29B2806011B1
01	00	20	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
09	01	20	E053017B691B3383	C05AB12A924BACB4	0E9A321A6B9A75A4	32117BD19F84826A
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	**8000000031000000**	**70000000B9000000**	**FA00000000000000**	**0000000000000000**
14	02	80	00000000B7120000	FAD82000BA210000	0000000000000000	0000000000000000
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	C0F4E2925E70A713	C0055BEE19E3C519	1B1D9FBBA3F8AE89	B85B29B2806011B1
01	00	20	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
09	01	20	E053017B691B3383	C05AB12A924BACB4	0E9A321A6B9A75A4	32117BD19F84826A
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	8000000031000000	70000000B9000000	FA00000000000000	0000000000000000
14	02	80	**00000000B7120000**	**FAD82000BA210000**	**0000000000000000**	**0000000000000000**
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	C0F4E2925E70A713	C0055BEE19E3C519	1B1D9FBBA3F8AE89	B85B29B2806011B1
01	00	20	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
09	01	20	E053017B691B3383	C05AB12A924BACB4	0E9A321A6B9A75A4	32117BD19F84826A
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	8000000031000000	70000000B9000000	FA00000000000000	0000000000000000
14	02	80	00000000B7120000	FAD82000BA210000	0000000000000000	0000000000000000
15	02	A0	**CF18000000000000**	**0000000000000000**	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	**C0F4E2925E70A713**	**C0055BEE19E3C519**	**1B1D9FBBA3F8AE89**	**B85B29B2806011B1**
01	00	20	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
09	01	20	E053017B691B3383	C05AB12A924BACB4	0E9A321A6B9A75A4	32117BD19F84826A
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	**FFFFFFFFFFFFFFFF**	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	**80000000**31000000	70000000B9000000	FA00000000000000	0000000000000000
14	02	80	**00000000**B7120000	FAD82000BA210000	0000000000000000	0000000000000000
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	C0F4E2925E70A713	C0055BEE19E3C519	1B1D9FBBA3F8AE89	B85B29B2806011B1
01	00	20	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
09	01	20	**E053017B691B3383**	**C05AB12A924BACB4**	**0E9A321A6B9A75A4**	**32117BD19F84826A**
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	FFFFFFFFFFFFFFFF	**FFFFFFFFFFFFFFFF**	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	80000000**31000000**	70000000B9000000	FA00000000000000	0000000000000000
14	02	80	00000000**B7120000**	FAD82000BA210000	0000000000000000	0000000000000000
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

PNR	TA2	TA1	MEMORY PAGE DATA			
00	00	00	C0F4E2925E70A713	C0055BEE19E3C519	1B1D9FBBA3F8AE89	B85B29B2806011B1
01	00	20	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
02	00	40	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
03	00	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
04	00	80	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
05	00	A0	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
06	00	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
07	00	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
08	01	00	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
09	01	20	E053017B691B3383	C05AB12A924BACB4	0E9A321A6B9A75A4	32117BD19F84826A
0A	01	40	823FA69EC3EF2B10	953527D2772F516E	17E17471693CF118	D1116BBB0E13301B
0B	01	60	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0C	01	80	0BD76674FF2AC13B	211F570DDBC17647	F24ED91E9A7C345E	B95FBA5D3C015419
0D	01	A0	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**	**AAAAAAAAAAAAAAAA**
0E	01	C0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
0F	01	E0	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAA
10	02	00	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
11	02	20	FFFFFFFFFFFFFFFF	**FFFFFFFFFFFFFFFF**	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF
12	02	40	FFFFFFFFFFFFFFFF	870EC0E9FAD19213	153DCF5B06F6AD68	75CA8403FFFFFFFF
13	02	60	8000000031000000	70000000B9000000	FA000000**00000000**	0000000000000000
14	02	80	00000000B7120000	FAD82000BA210000	00000000**00000000**	0000000000000000
15	02	A0	CF18000000000000	0000000000000000	FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF

```
1   h[0] = 0x67452301;
    h[1] = 0xEFCDAB89;
    h[2] = 0x98BADCFE;
    h[3] = 0x10325476;
    h[4] = 0xC3D2E1F0;
6
    for(int i = 16; i < 80; i++)
        w[i] = LROT(w[i-3] ^ w[i-8] ^ w[i-14] ^ w[i-16], 1);

    for(int i = 0; i < 80; i++) {
11      uint32_t f, k, tmp;
        if(i < 20) {
            f = (h[1] & h[2]) | ((~h[1]) & h[3]);
            k = 0x5A827999;
        } else if(i < 40) {
16          f = h[1] ^ h[2] ^ h[3];
            k = 0x6ED9EBA1;
        } else if(i < 60) {
            f = (h[1] & h[2]) | (h[1] & h[3]) | (h[2] & h[3]);
            k = 0x8F1BBCDC;
21      } else {
            f = h[1] ^ h[2] ^ h[3];
            k = 0xCA62C1D6;
        }

26      tmp = LROT(h[0], 5) + f + h[4] + k + w[i];
        h[4] = h[3];
        h[3] = h[2];
        h[2] = LROT(h[1], 30);
        h[1] = h[0];
31      h[0] = tmp;
    }
```

Beispiel: Read Authenticated Page

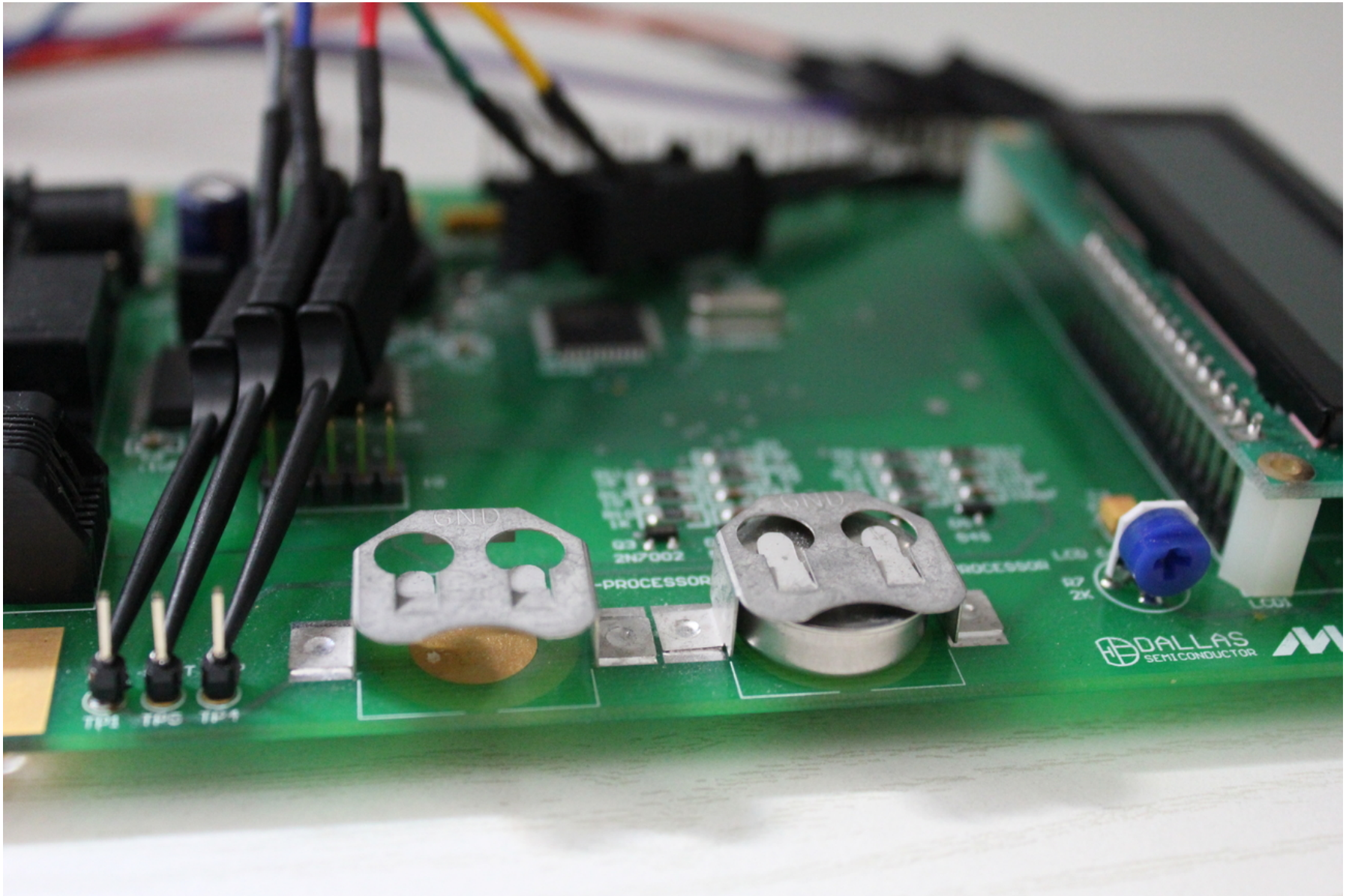
```
...
 09  01  20  E053017B691B3383 C05AB12A924BACB4 0E9A321A6B9A75A4 32117BD19F84826A
...
 10  02  00  FFFFFFFFFFFFFFFF XXXXXXXXXXXXXXXX FFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFF
...
 12  02  40  YYYYYYYYYYYYYYYY YYYYYYYYYYYYYYYY YYYYYYYY112233YY YYYYYYYYYYYYYYYY
...
 14  02  80  00000000B7120000 FAD82000BA210000 0000000000000000 0000000000000000
...
```

```
 0   XX XX XX XX  E0 53 01 7B  69 1B 33 83  C0 5A B1 2A
 4   92 4B AC B4  0E 9A 32 1A  6B 9A 75 A4  32 11 7B D1
 8   9F 84 82 6A  B7 12 00 00  Z9 18 DD 8E  67 00 00 00
12   XX XX XX XX  11 22 33 80  00 00 00 00  00 00 01 B8
```

Z = M X 0 0

eCash Szenario (1)

- Tokens
  - User Token
  - Coproc Token
- Secrets
  - Master Secret
  - Master Signing Secret
  - Custom User Secret


GND
GND
2N7002
-PROCESSOR
DALLAS
SEMICONDUCTOR

eCash Szenario (2)

- Validierung des Tokens
  - Coprozessor: generiert Challenge
  - User Token: Read Auth. Page CMD
  - Coprozessor berechnet User Secret
  - Coprozessor: Read Auth. Page CMD
  - Ergebnisse werden verglichen
- eMoney besteht aus
  - Geldbetrag
  - Counter
  - Signatur

Bruteforce

- MMAC/s = Million Message Authentication Codes per second
- 64 Bit Schlüsselgröße unzureichend
- Maxim: schneller Computer schafft 1 MMAC/s
- Maxim: realistisch nur mit Supercomputer
- mit CUDA / OpenCL
  - nVidia GTS250: 240 MMAC/s (80 EUR)
  - nVidia GTX275: 310 MMAC/s
  - Fermi Dual GPU + CPU: $>$ 1.000 MMAC/s
  - FPGA-Ansatz etwa genauso schnell
- Distributed Computing

Kryptanalyse

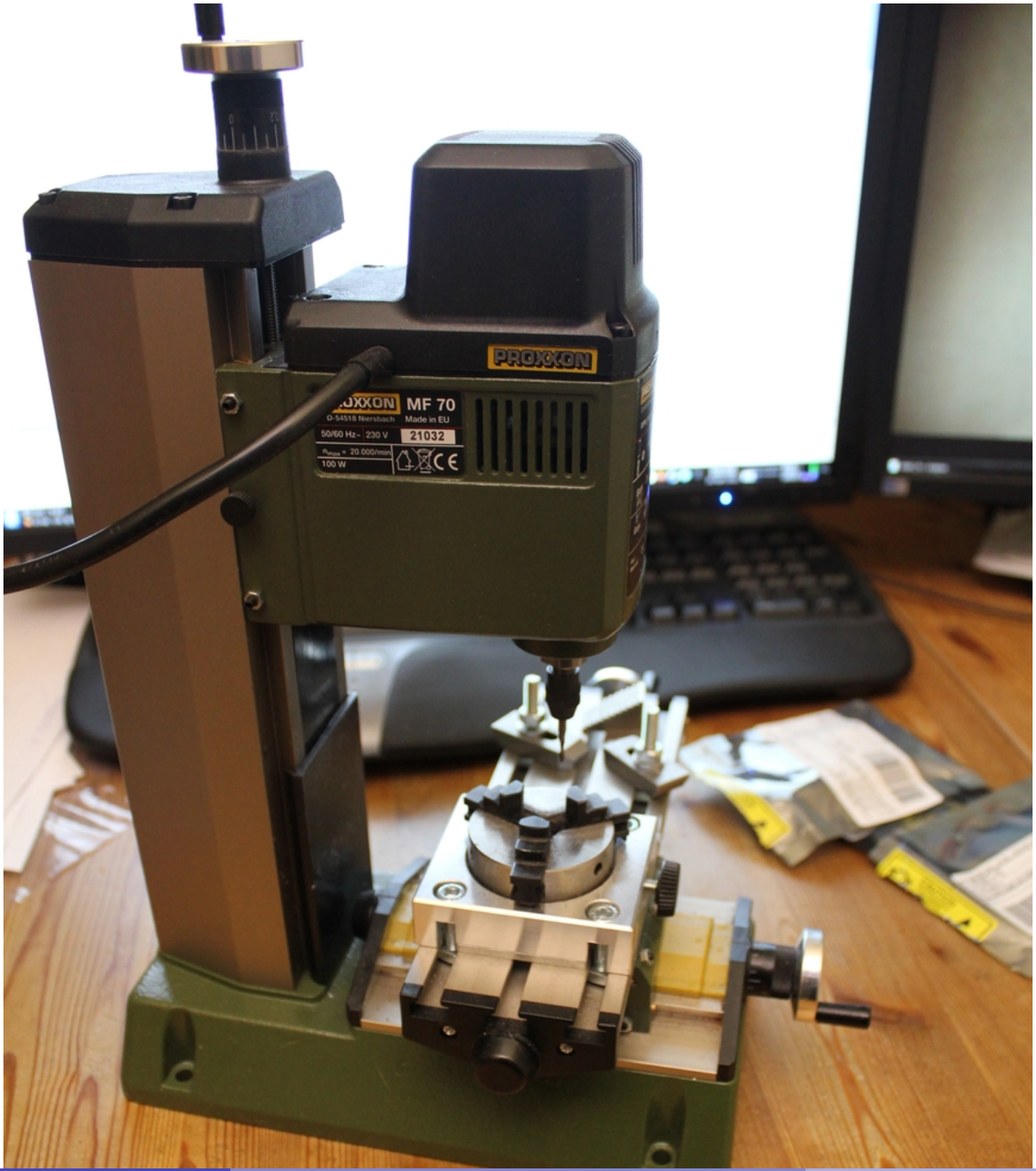
- einige Angriffsmöglichkeiten gefunden
  - Time-Memory Trade-Off
  - Algebraic Attack
  - Side-Channel Attack
  - Fault Attack
- beste gefundene Methode
  - Fault Attack
  - Zeitaufwand insgesamt: 10-15 Minuten

Fault Attack

- Fehler provozieren
- SRAM Data Remanence
- drei Phasen
  1. Präparation
  2. Angriff
  3. Analyse
- Angriffsvektor: SRAM Versorgungsleitung
- iButton muss geöffnet werden
- zuverlässiges, reproduzierbares Verfahren notwendig

Fault Attack - Phase 1

- Benötigte Materialien
  - kleine 3-achsige Fräse
  - Teilapparat (4. Achse)
  - Schaftfräser, Kegelfräser, Bohrer
  - Backup-Batterie 3,3V
- perfekt reproduzierbar
- 100% Erfolgsquote
- Materialkosten unter 350 EUR


PROXXON
MF 70
Made in EU
50/60 Hz~ 230 V
21032
100 W


07 18
1021 LA6 DS1963S+F5

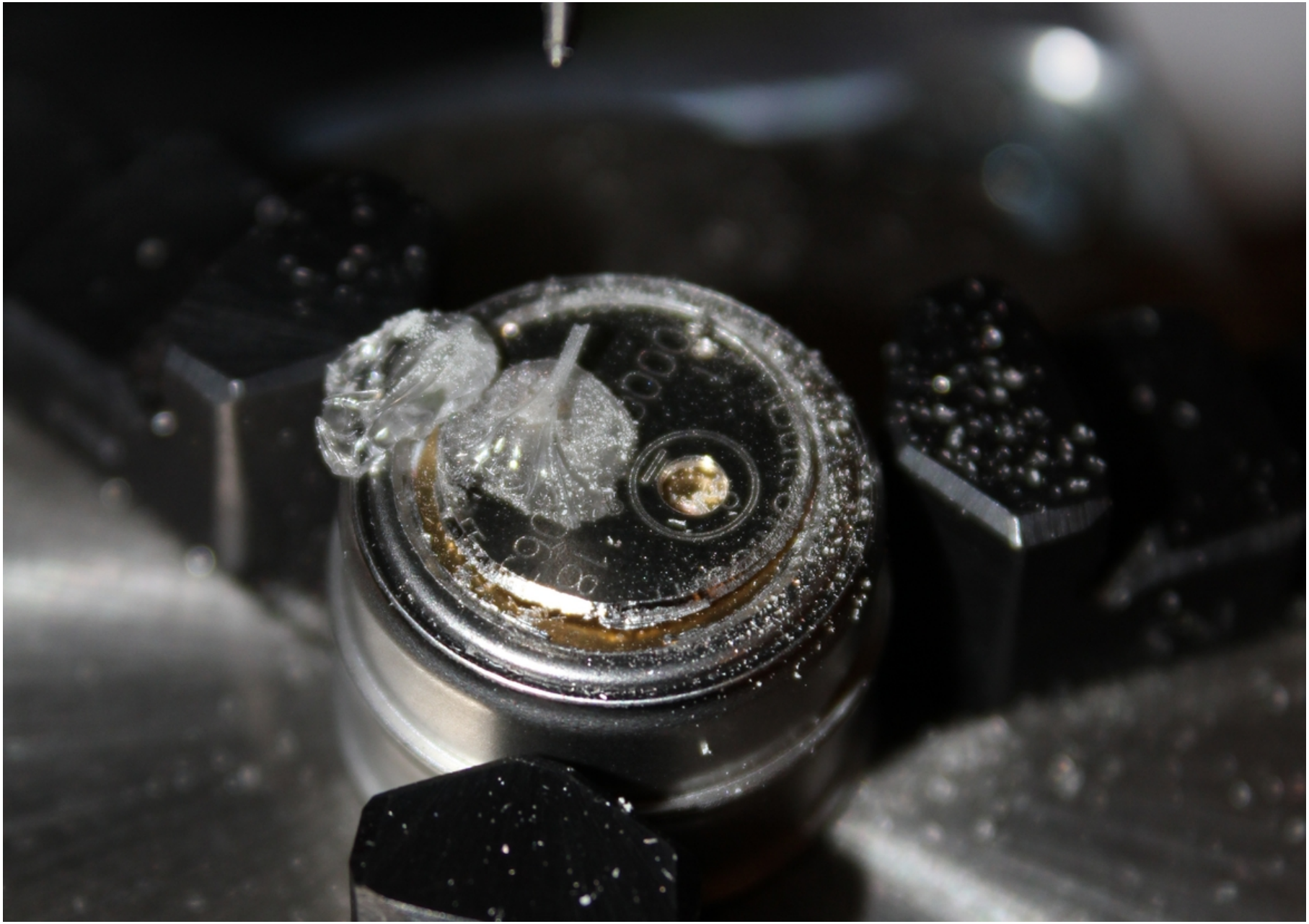

iButton.com
07 18
000000675792
1-Wire
SHA-1
1021 LA6 DS1963S+F5

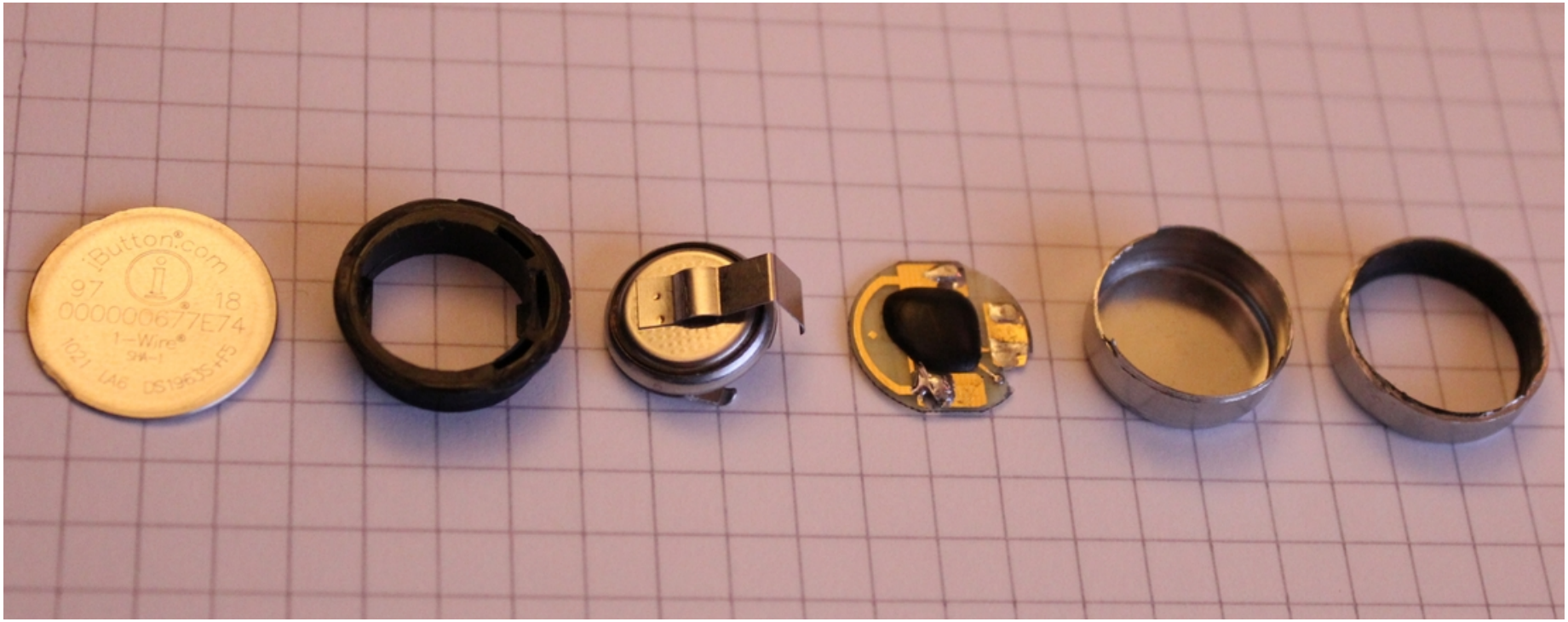

iButton.com
07
18
0000000675792
1-Wire®
SHA-1
1021
LA6
DS1963S-F5

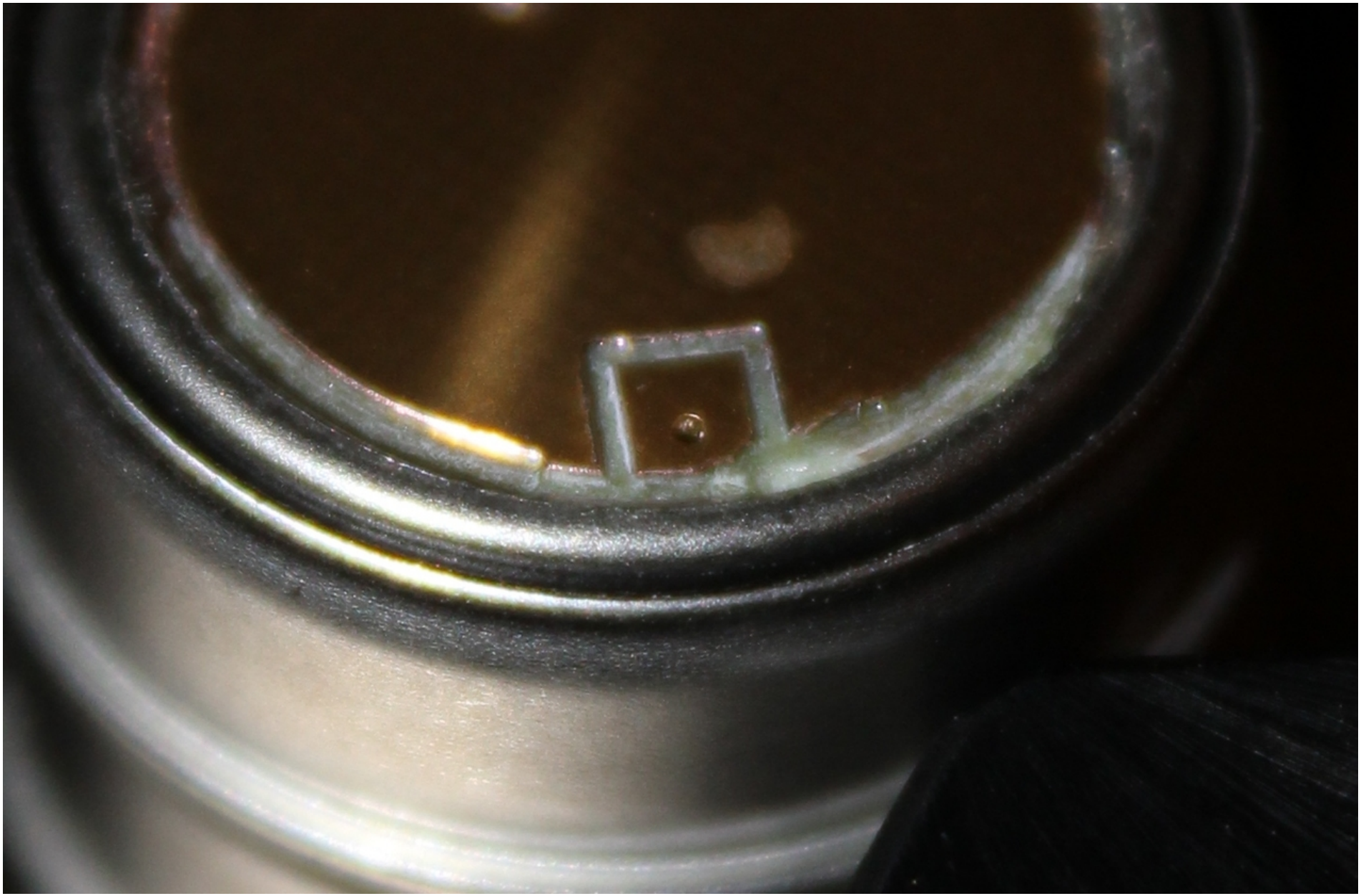

iButton.com
07 18
0000000675792
1-Wire®
SHA-1
1021 LA6 DS1963S-F5

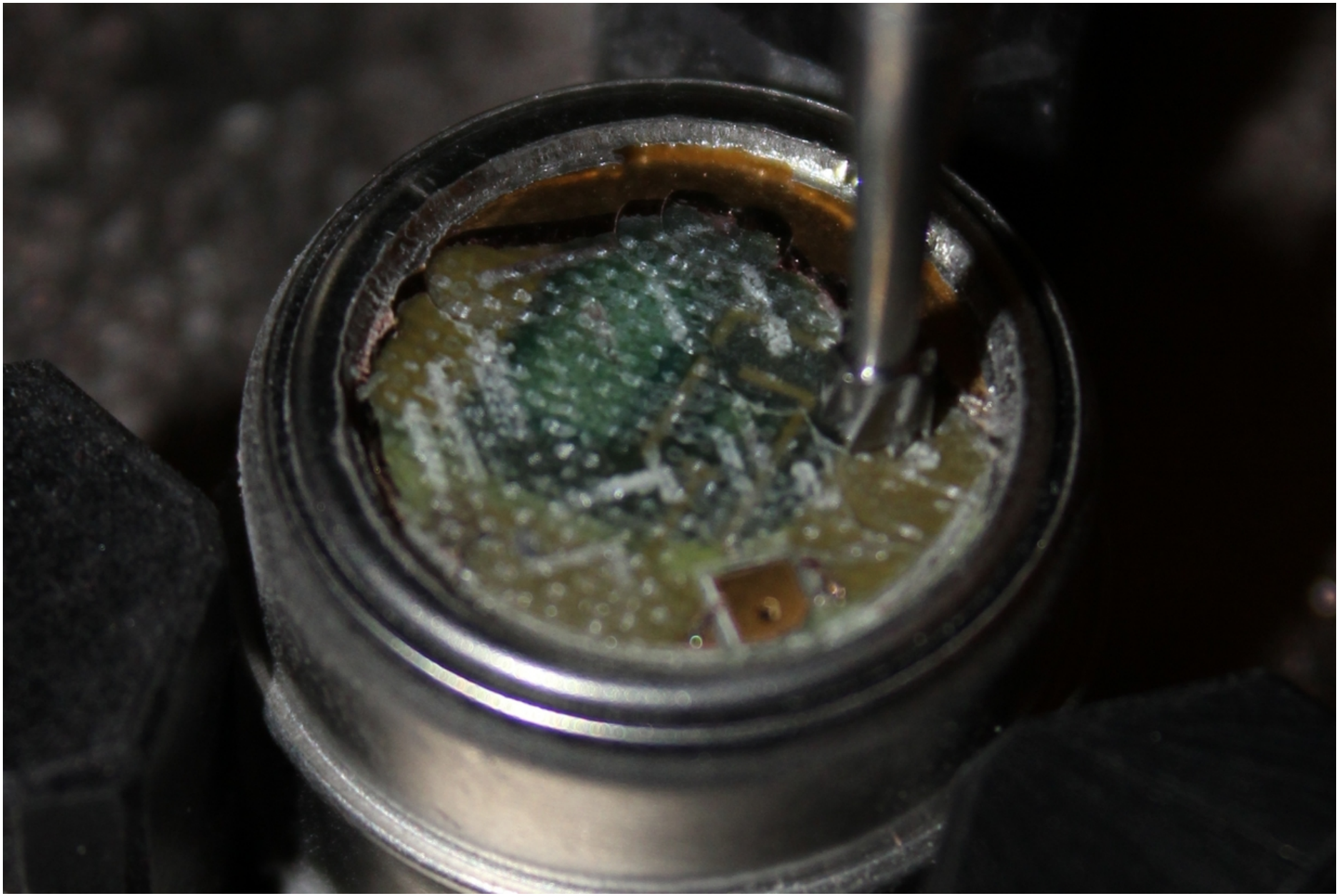

iButton.com
07
18
792
DS1963S

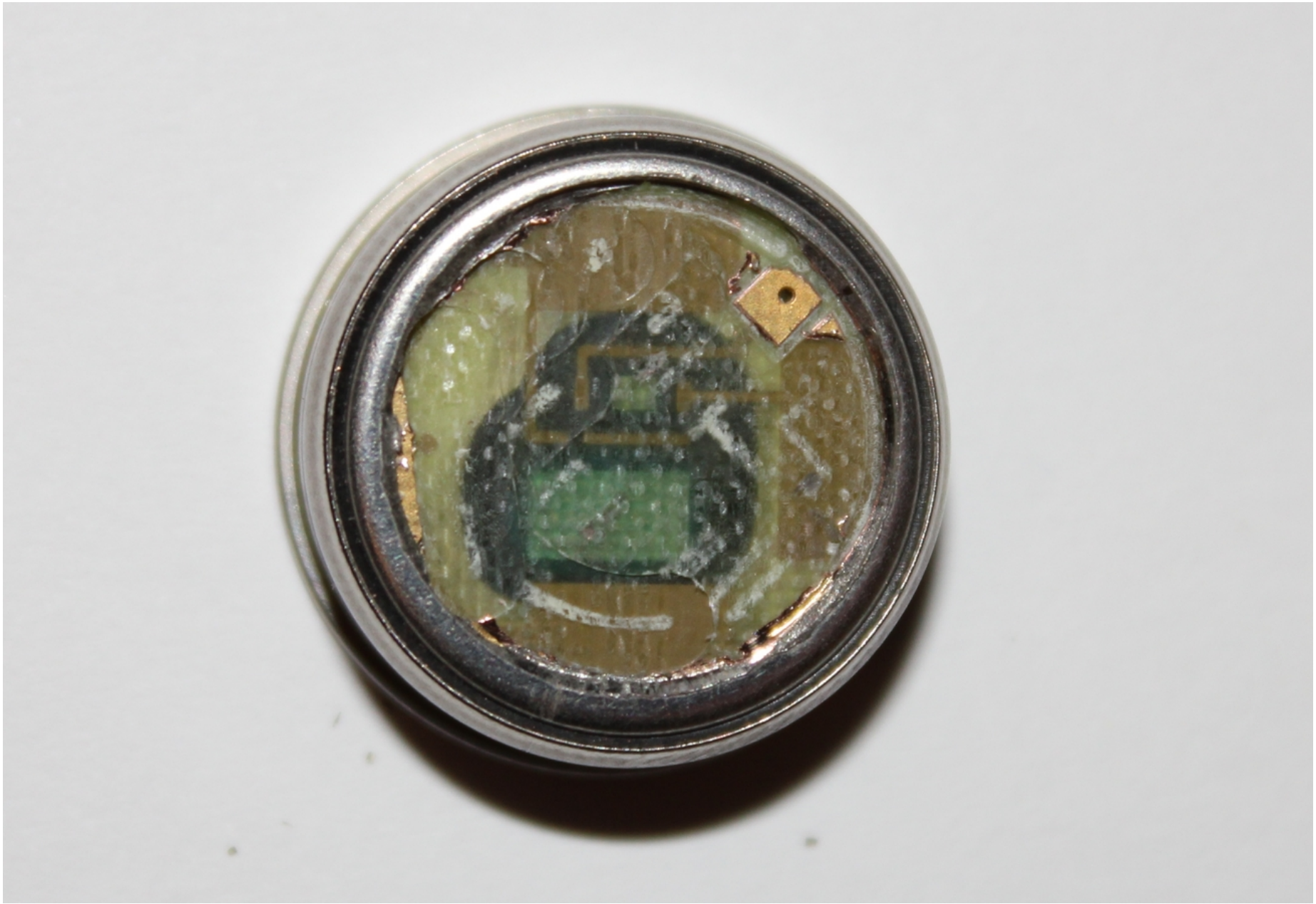

iButton.com

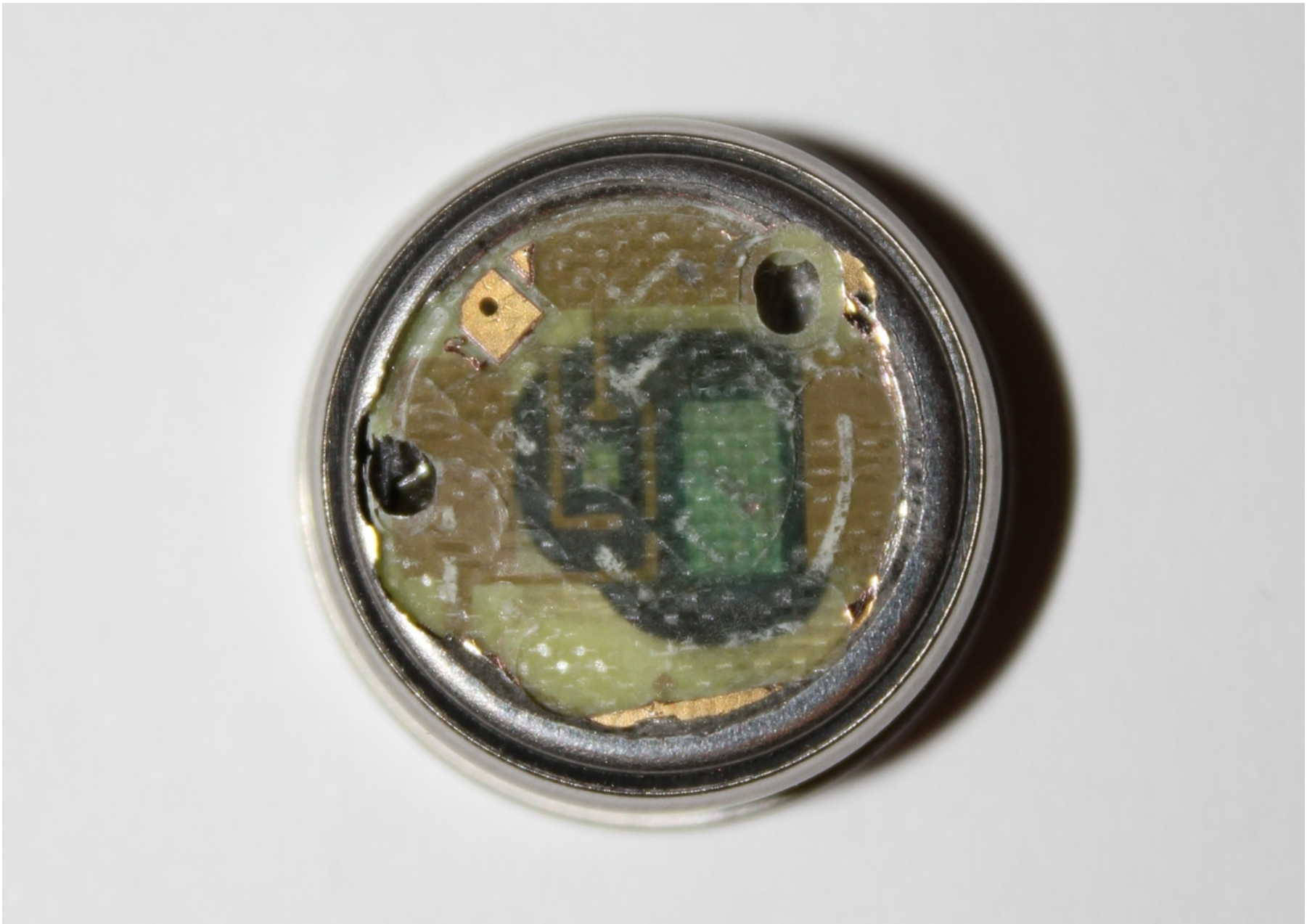


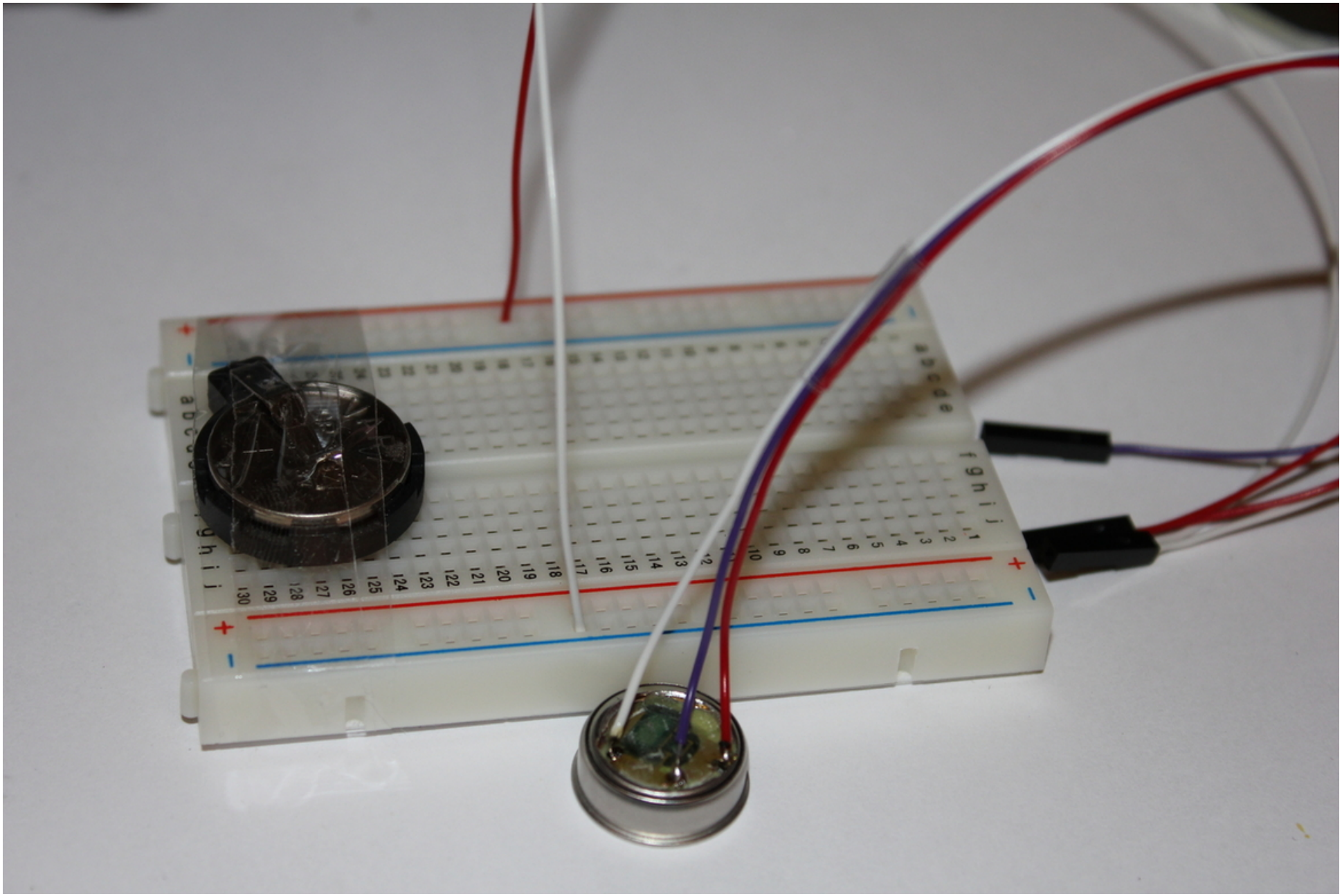

iButton.com
97 18
000000677E74
1-Wire

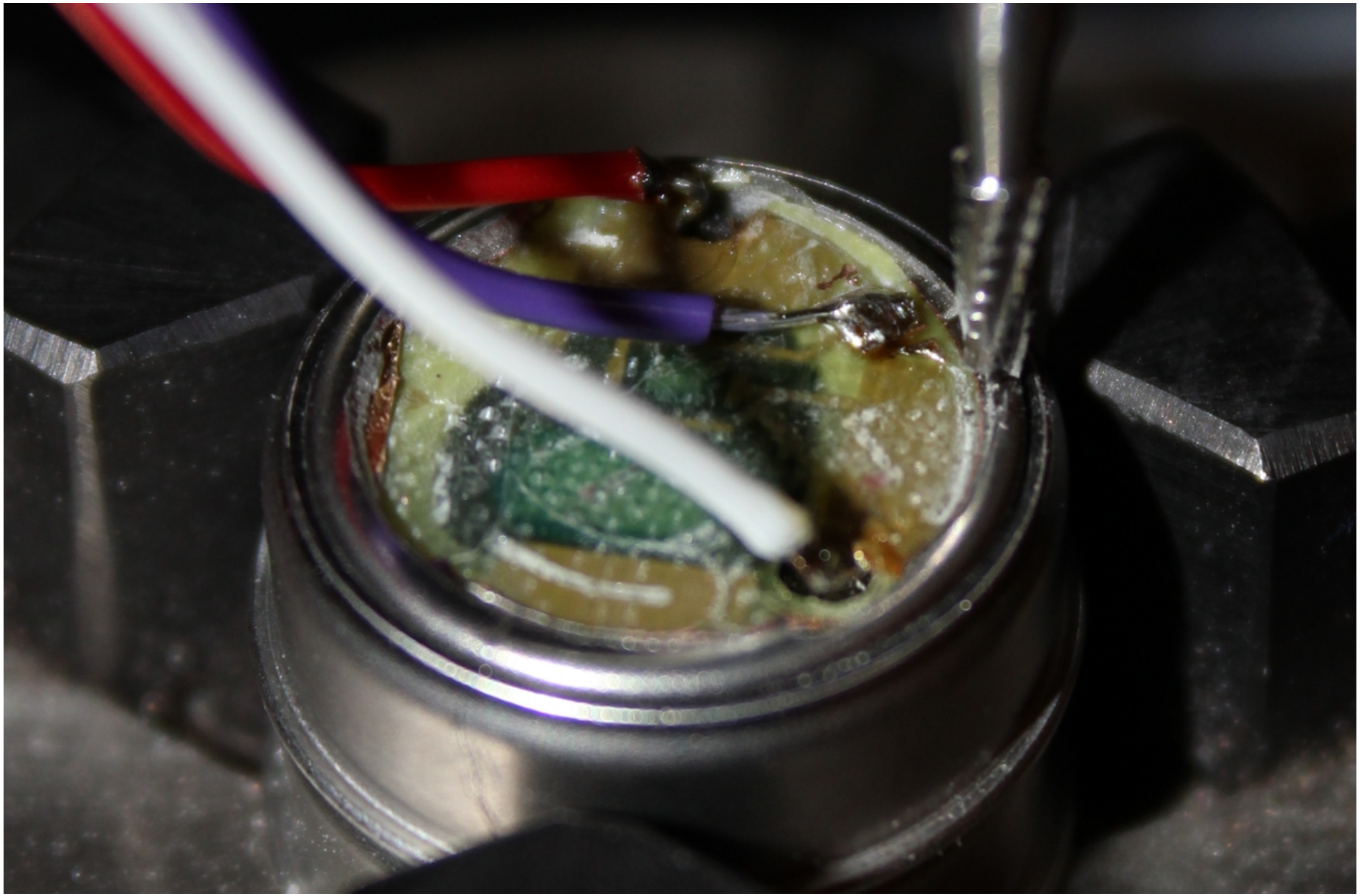


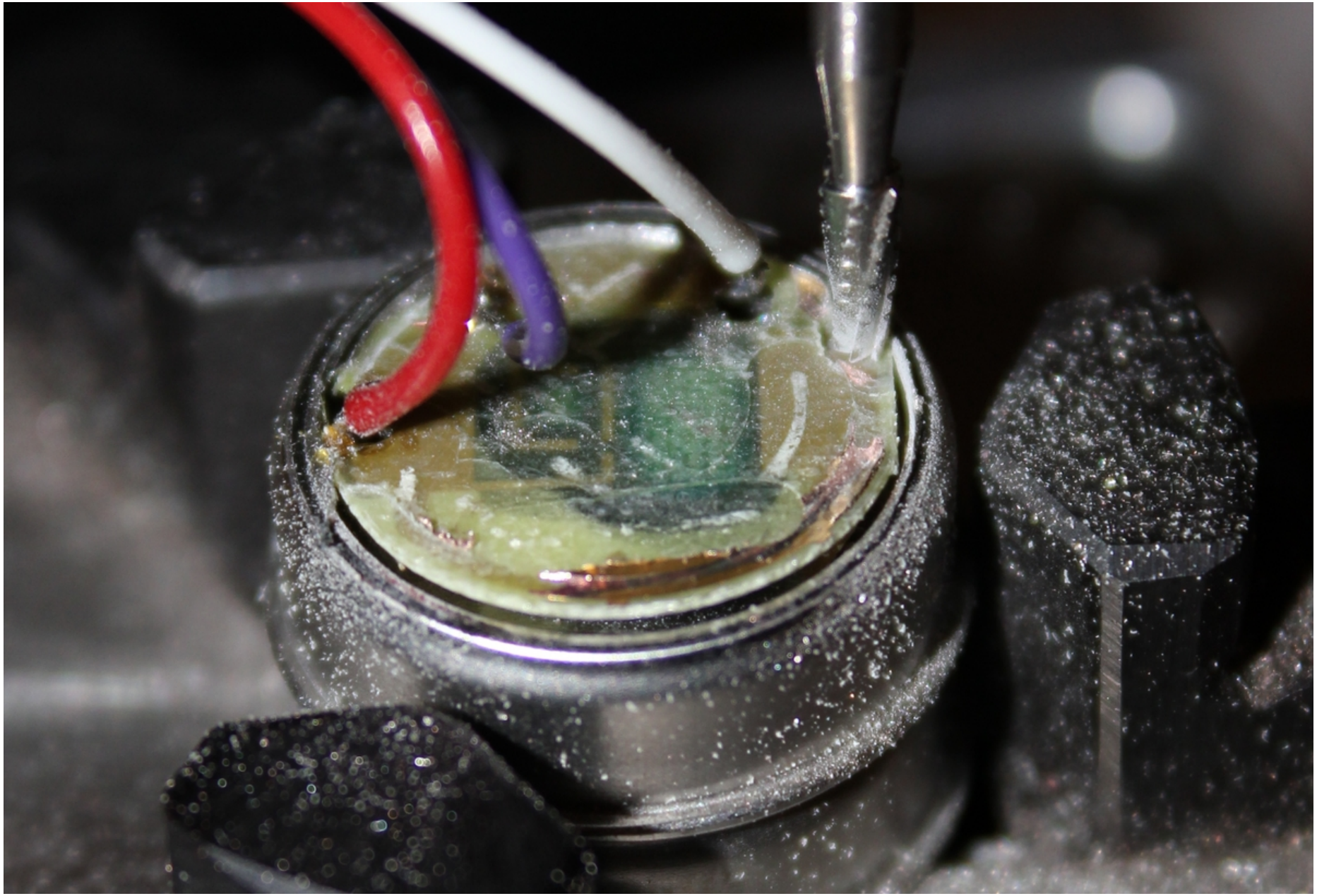


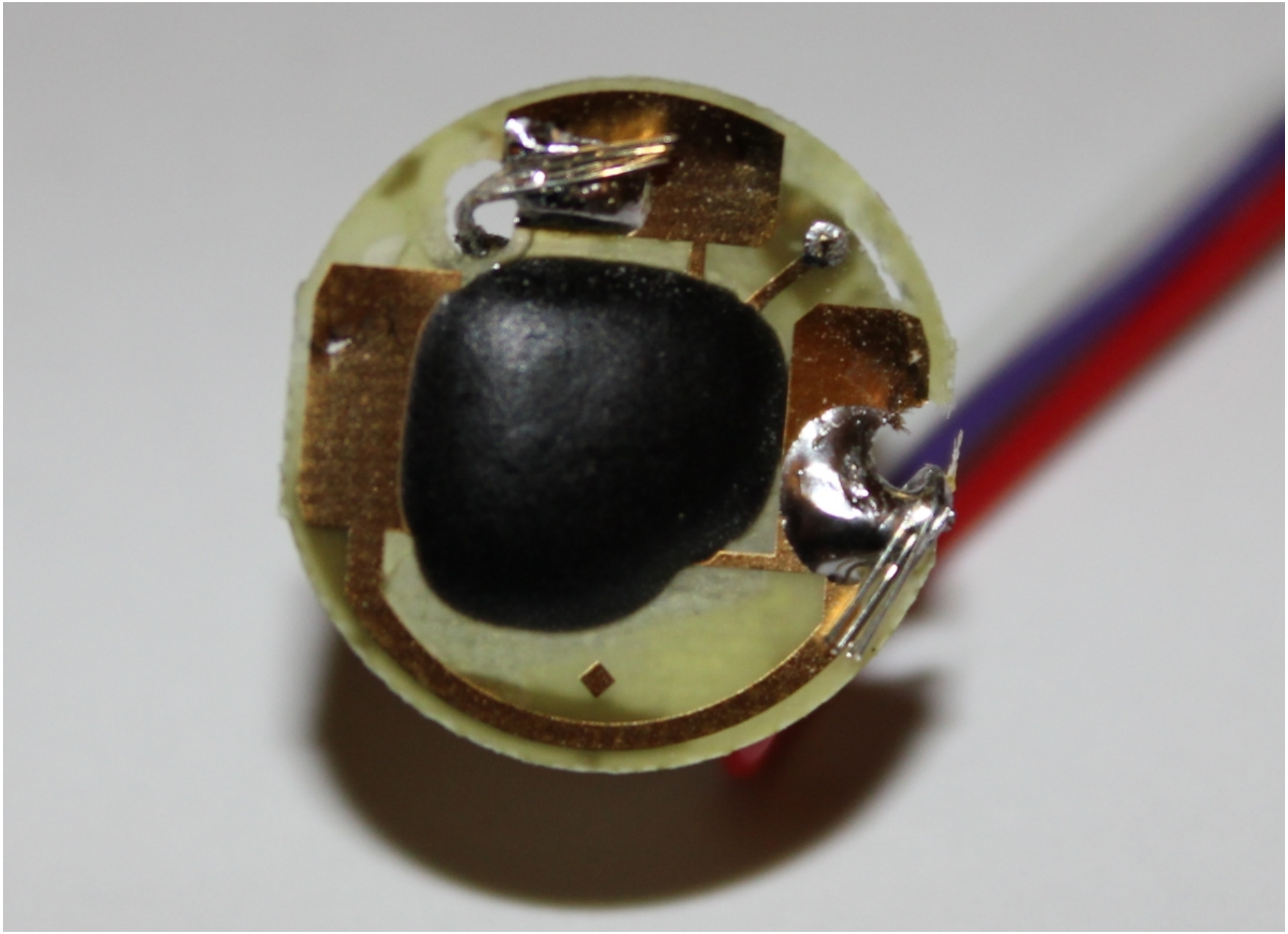


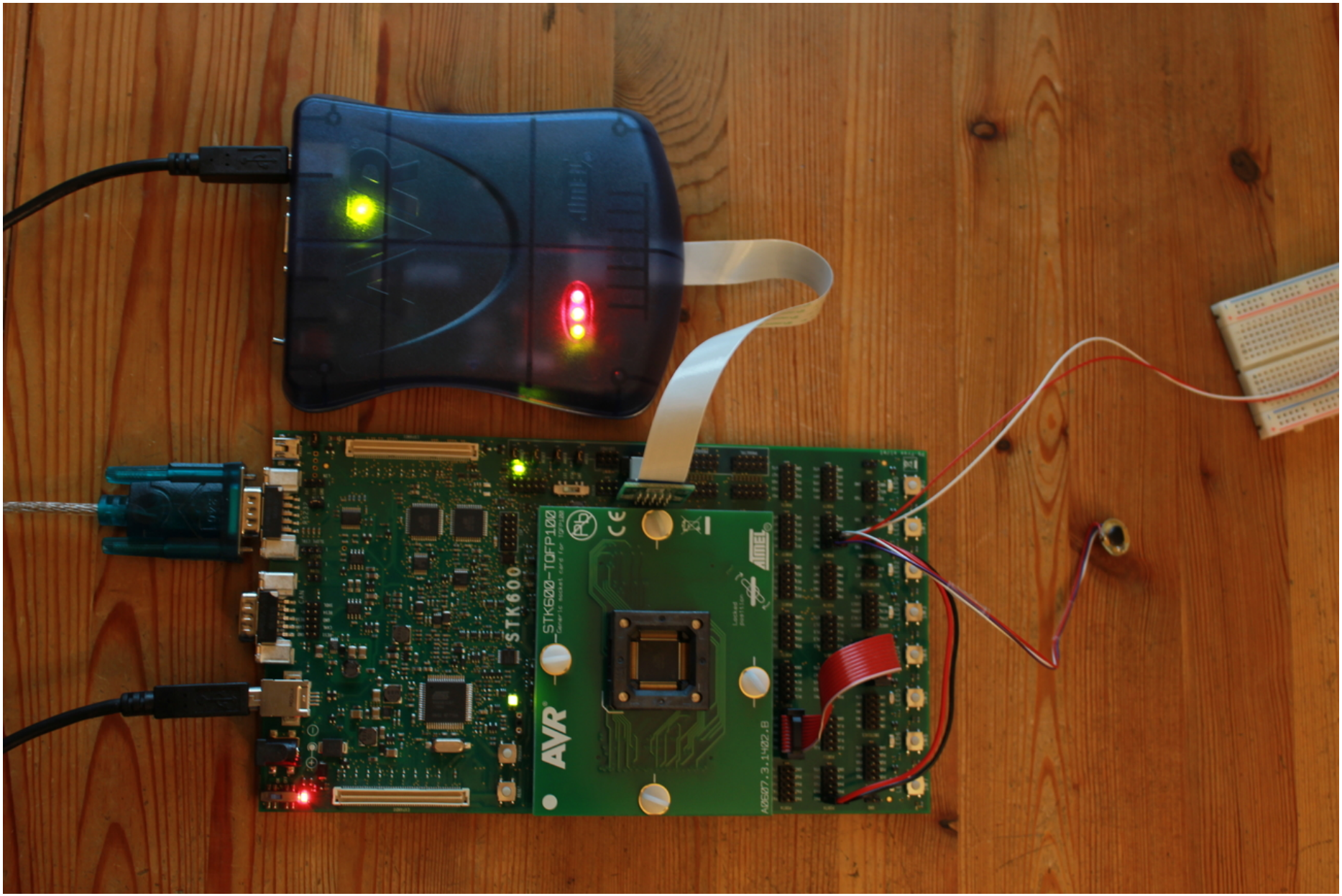











STK600
STK600-TQFP100
AVR
ATMEL

Fault Attack - Phase 2 (1)

- parasitäre Versorgung
- interne Versorgung: SRAM, Copy Scratchpad CMD
  - Speicherseiten 0-15: Zielbereich frei wählbar
  - Speicherseiten 16-17: Zielbereich fest vorgegeben
  - atomare Operation
- Idee:
  - Störung dieser atomaren Operation
  - Aushebeln der festen Vorgabe des Zielbereichs

Fault Attack - Phase 2 (2)

- SRAM benötigt ca. 3V
- interessante Eigenschaft:
  - Verlust der I/O Fähigkeit unterhalb 1,07V $\pm$ 0,01V
  - Daten bleiben erhalten
  - Schreibbefehle werden nicht mehr durchgeführt
  - Lesebefehle liefern ausschließlich 0xFF
- Problem:
  - schlecht reproduzierbar
  - Spannung muss möglichst schnell fallen
- Lösung:
  - Chip auf -5 deg C kühlen
  - Data Remanence Effekt
  - Kurzschluss zwischen SRAM POWER und GND
  - mögliche Kurzschlussdauer 500 ms und länger

Fault Attack - Phase 2 (3)

- Durchführung einer einzelnen Attacke:
  - neuen Schlüssel generieren, Parameter merken
  - Kopiervorgang vorbereiten, letztes Bit (esx) zurückhalten
  - abhängig von esx Bus für 6 μs bzw. 60 μs auf GND ziehen
  - mit steigender Flanke Timer auslösen
  - nach Ablauf des Timers SRAM kurzschließen
  - nach 5 μs SRAM Kurzschluss aufheben
  - 5 ms Pause, 1-wire Reset durchführen, 2 ms Pause
  - mindestens ein Bit vom Bus lesen

Was haben wir erreicht?

```
BK   = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00110011

K    = 01101100 11100000 10101011 11001110 01100100 10000011 10111110 00000011

K'1 = 10100100 11100000 10101011 11001110 01100100 10000011 10111110 00000011
K'2 = 10100111 11111100 10101011 11001110 01100100 10000011 10111110 00000011
K'3 = 10100111 11111101 01000111 11001110 01100100 10000011 10111110 00000011
K'4 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00000011
K'5 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00110011
```

Was haben wir erreicht?

```
BK   = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00110011

K    = 01101100 11100000 10101011 11001110 01100100 10000011 10111110 00000011

K'1 = 10100100 11100000 10101011 11001110 01100100 10000011 10111110 00000011
K'2 = 10100111 11111100 10101011 11001110 01100100 10000011 10111110 00000011
K'3 = 10100111 11111101 01000111 11001110 01100100 10000011 10111110 00000011
K'4 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00000011
K'5 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00110011

K    = 01101100 11100000 10101011 11001110 01100100 10000011 10111110 00000011
K'1 = 10100111 11100000 10101011 11001110 01100100 10000011 10111110 00000011
K'2 = 10100111 11111101 10101011 11001110 01100100 10000011 10111110 00000011
K'3 = 10100111 11111101 01000111 11001110 01100100 10000011 10111110 00000011
K'4 = 10100111 11111101 01000111 01001011 01100100 10000011 10111110 00000011
K'5 = 10100111 11111101 01000111 01001011 01010100 10000011 10111110 00000011
K'6 = 10100111 11111101 01000111 01001011 01010100 10011000 10111110 00000011
K'7 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00000011
K'8 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00110011
```

Fault Attack - Phase 2 (4)

- Durchführung eines vollständigen Angriffs:
  - ROM auslesen und speichern
  - Read Authenticated Page
  - alle Daten und MAC speichern
  - Timer Limit auf 0x0040 setzen (4 μs)
  - solange Timer Limit $<$ 0x0118 (17,5 μ)
    - einzelne Attacke durchführen
    - Read Authenticated Page
    - alle Daten und MAC speichern
    - Timer Limit um 4 erhöhen (+250 ns)

Fault Attack - Phase 2 (5)

- 36 Angriffe
- Dauer: ca. 8 Sekunden
- für alle 8 Keys/Secrets ca. 64 Sekunden
- Angriff wird vollständig und autonom von μC durchgeführt
- gesammelte Daten über USB an PC

Daten aus Phase 2

```
$ cat /dev/ttyUSB2 | tee -a attack.log
O 1846316700000092
...
R 0108 00 40 AAA....AAA 0...0 89000000 4507 000000 6D8C67342DF51313BD8A348619535C5EA9E29C59
R 0110 00 40 AAA....AAA 0...0 8A000000 4543 000000 6D8C67342DF51313BD8A348619535C5EA9E29C59
E
S 3
B 923CBE2F84774B50
R 0000 00 60 AAA....AAA 0...0 6F000000 D3D0 000000 CE9085788236E8131FA312CFC0E7CEFA0082AD7B
R 0040 00 60 AAA....AAA 0...0 70000000 D404 000000 CE9085788236E8131FA312CFC0E7CEFA0082AD7B
R 0048 00 60 AAA....AAA 0...0 71000000 D5F8 000000 CE9085788236E8131FA312CFC0E7CEFA0082AD7B
R 0050 00 60 AAA....AAA 0...0 72000000 D5BC 000000 CE9085788236E8131FA312CFC0E7CEFA0082AD7B
R 0058 00 60 AAA....AAA 0...0 73000000 D440 000000 CE9085788236E8131FA312CFC0E7CEFA0082AD7B
R 0060 00 60 AAA....AAA 0...0 74000000 D534 000000 CE9085788236E8131FA312CFC0E7CEFA0082AD7B
R 0068 00 60 AAA....AAA 0...0 75000000 D4C8 000000 2A49D0F218F41C4F85CAF1862E2A2A9AF60E0C41
R 0070 00 60 AAA....AAA 0...0 76000000 D48C 000000 2A49D0F218F41C4F85CAF1862E2A2A9AF60E0C41
R 0078 00 60 AAA....AAA 0...0 77000000 D570 000000 2A49D0F218F41C4F85CAF1862E2A2A9AF60E0C41
R 0080 00 60 AAA....AAA 0...0 78000000 D664 000000 7F8D2EF5B7274DF97AD902EC3FACEC96023B54BC
R 0088 00 60 AAA....AAA 0...0 79000000 D798 000000 7F8D2EF5B7274DF97AD902EC3FACEC96023B54BC
R 0090 00 60 AAA....AAA 0...0 7A000000 D7DC 000000 7F8D2EF5B7274DF97AD902EC3FACEC96023B54BC
R 0098 00 60 AAA....AAA 0...0 7B000000 D620 000000 2CA8539432E929AD8B219364814601D4CD830031
R 00A0 00 60 AAA....AAA 0...0 7C000000 D754 000000 2CA8539432E929AD8B219364814601D4CD830031
...
```

Fault Attack - Phase 3 (1)

- bisher nur Idealfall betrachtet
- Ausnutzen von Verhalten außerhalb der Spezifikation
- Fehler treten häufig auf
- Daten müssen gefiltert werden
  - iCRC16 prüfen
  - Stetigkeitsfilter
  - die 9 größten MAC Sets verwenden
- wir erhalten
  - 1x ROM
  - je Key
    - 1 BaseKey
    - 9 Read Authenticated Page Data Sets
    - 9 Message Authentication Codes

Fault Attack - Phase 3 (2)

- Wie kommen wir jetzt an die Keys/Secrets?
- angenommen
  - K' ist bekannt
  - M'' basiert auf K''
  - für K' gilt $BK \preccurlyeq_n K'$
  - für K'' gilt $BK \preccurlyeq_m K''$
  - und n $>$ m
- dann lässt sich K" durch M" mit 2^{n-m-1} SHA-1 MAC Berechnungen ermitteln
- zu jeder M_n gehört K_n mit $K_8 \preccurlyeq_{n*8} K_n$
- mit K_n und M_{n-1} können wir also K_{n-1} mit

$$2^{n*8-(n-1)*8-1} = 2^7$$

  SHA-1 MAC Berechnungen finden
- mit insgesamt 8 solchen Schritten und damit einem Aufwand von $8 * 2^7 = 1024$ gelangen wir von K_8 zu K_0

aus Phase 2

```
BK   = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00110011

K    = 01101100 11100000 10101011 11001110 01100100 10000011 10111110 00000011

K'0 = 01101100 11100000 10101011 11001110 01100100 10000011 10111110 00000011
K'1 = 10100111 11100000 10101011 11001110 01100100 10000011 10111110 00000011
K'2 = 10100111 11111101 10101011 11001110 01100100 10000011 10111110 00000011
K'3 = 10100111 11111101 01000111 11001110 01100100 10000011 10111110 00000011
K'4 = 10100111 11111101 01000111 01001011 01100100 10000011 10111110 00000011
K'5 = 10100111 11111101 01000111 01001011 01010100 10000011 10111110 00000011
K'6 = 10100111 11111101 01000111 01001011 01010100 10011000 10111110 00000011
K'7 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00000011
K'8 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00110011
```

rückwärts auflösen

```
K'8 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00110011
K'7 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 xxxxxxxx
K'7 = 10100111 11111101 01000111 01001011 01010100 10011000 11001010 00000011
K'6 = 10100111 11111101 01000111 01001011 01010100 10011000 xxxxxxxx 00000011
K'6 = 10100111 11111101 01000111 01001011 01010100 10011000 10111110 00000011
K'5 = 10100111 11111101 01000111 01001011 01010100 xxxxxxxx 10111110 00000011
K'5 = 10100111 11111101 01000111 01001011 01010100 10011000 10111110 00000011
K'4 = 10100111 11111101 01000111 01001011 xxxxxxxx 10000011 10111110 00000011
K'4 = 10100111 11111101 01000111 01001011 01010100 10000011 10111110 00000011
K'3 = 10100111 11111101 01000111 xxxxxxxx 01100100 10000011 10111110 00000011
K'3 = 10100111 11111101 01000111 01001011 01100100 10000011 10111110 00000011
K'2 = 10100111 11111101 xxxxxxxx 11001110 01100100 10000011 10111110 00000011
K'2 = 10100111 11111101 01000111 11001110 01100100 10000011 10111110 00000011
K'1 = 10100111 xxxxxxxx 10101011 11001110 01100100 10000011 10111110 00000011
K'1 = 10100111 11111101 10101011 11001110 01100100 10000011 10111110 00000011
K'0 = xxxxxxxx 11100000 10101011 11001110 01100100 10000011 10111110 00000011
K'0 = 01101100 11100000 10101011 11001110 01100100 10000011 10111110 00000011
```

real durchgeführt

```
$ time ./fa_resolve_key attack.log

SECRET 0: F6464F60FAFD145E  [1108]  (VALID)
SECRET 1: ACDDAF04A550363A  [ 929]  (VALID)
SECRET 2: 79C0ED28C4053F46  [ 924]  (VALID)
SECRET 3: 568CCD45CE6CB6F3  [1239]  (VALID)
SECRET 4: B5EDF140D8938E9F  [1387]  (VALID)
SECRET 5: DE7C444EEDBE6B52  [1108]  (VALID)
SECRET 6: AB99710A33BFE5FF  [1173]  (VALID)
SECRET 7: CF26940A68C6F52E  [ 996]  (VALID)

DONE

real    0m0.015s
user    0m0.016s
sys     0m0.000s
```

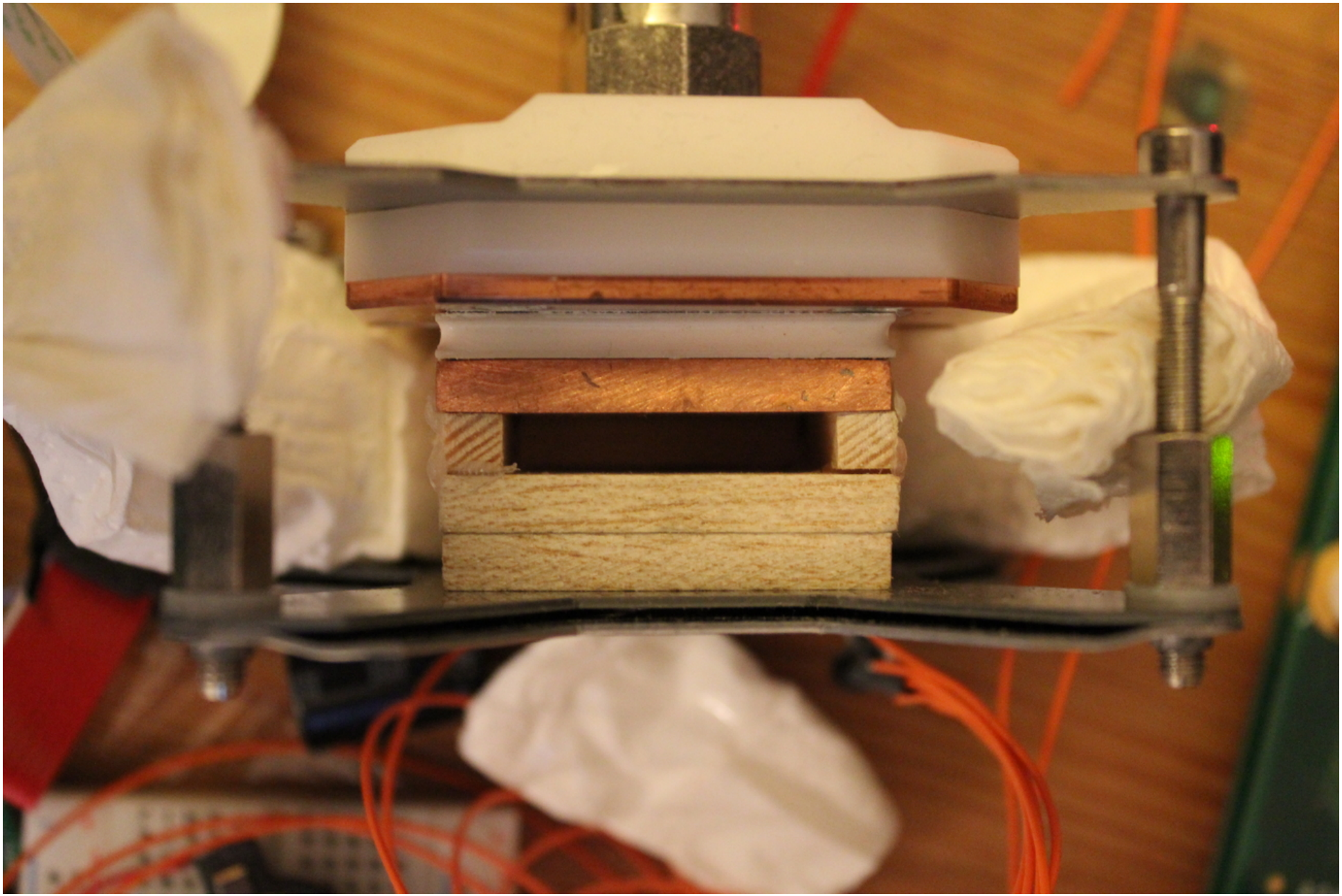
nochmal zurück: Fault Attack - Phase 2 (3)

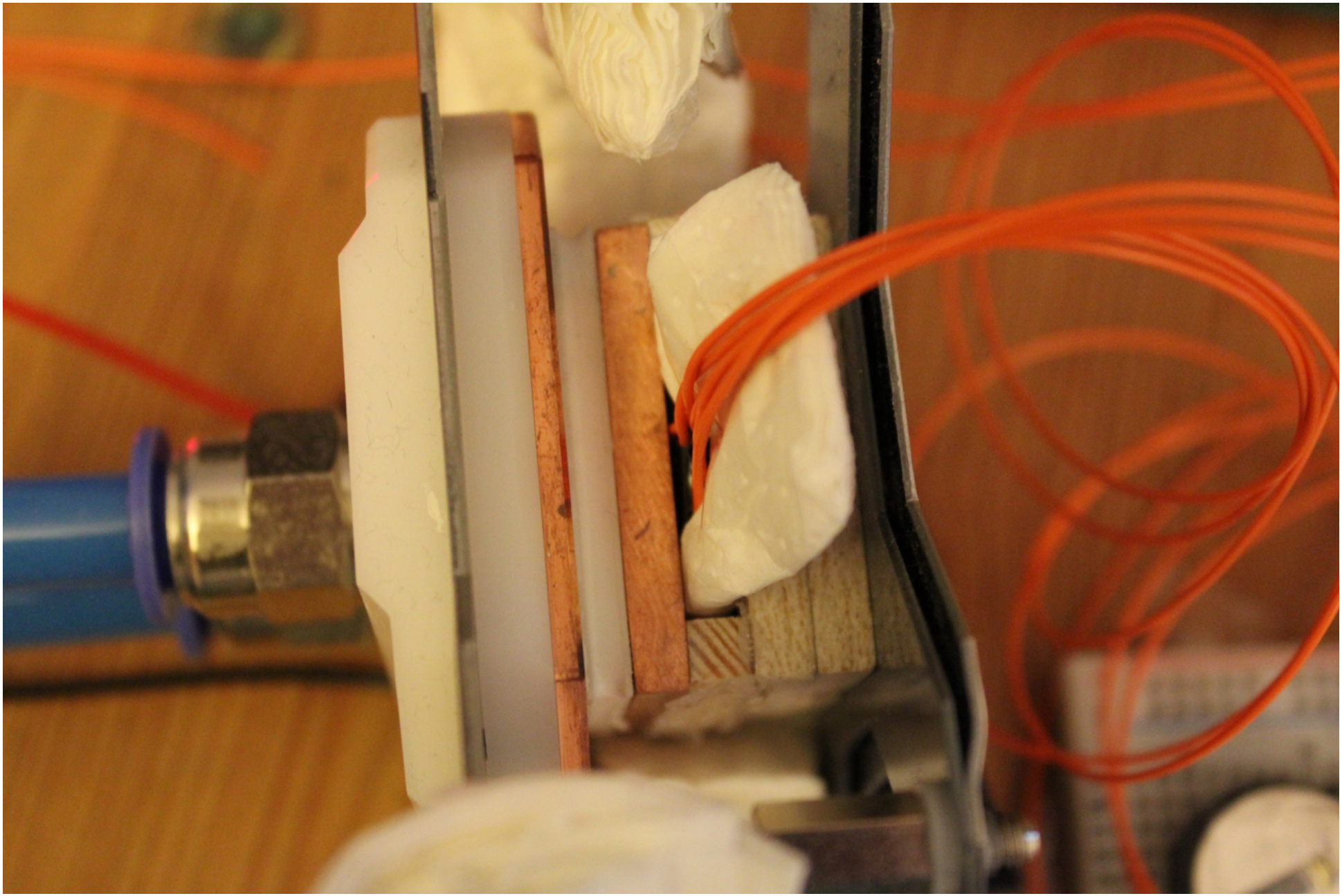
- Durchführung einer einzelnen Attacke:
  - neuen Schlüssel generieren, Parameter merken
  - Kopiervorgang vorbereiten, letztes Bit (esx) zurückhalten
  - abhängig von esx Bus für 6 μs bzw. 60 μs auf GND ziehen
  - mit steigender Flanke Timer auslösen
  - nach Ablauf des Timers SRAM kurzschließen
  - nach 5 μs SRAM Kurzschluss aufheben
  - 5 ms Pause, 1-wire Reset durchführen, 2 ms Pause
  - mindestens ein Bit vom Bus lesen

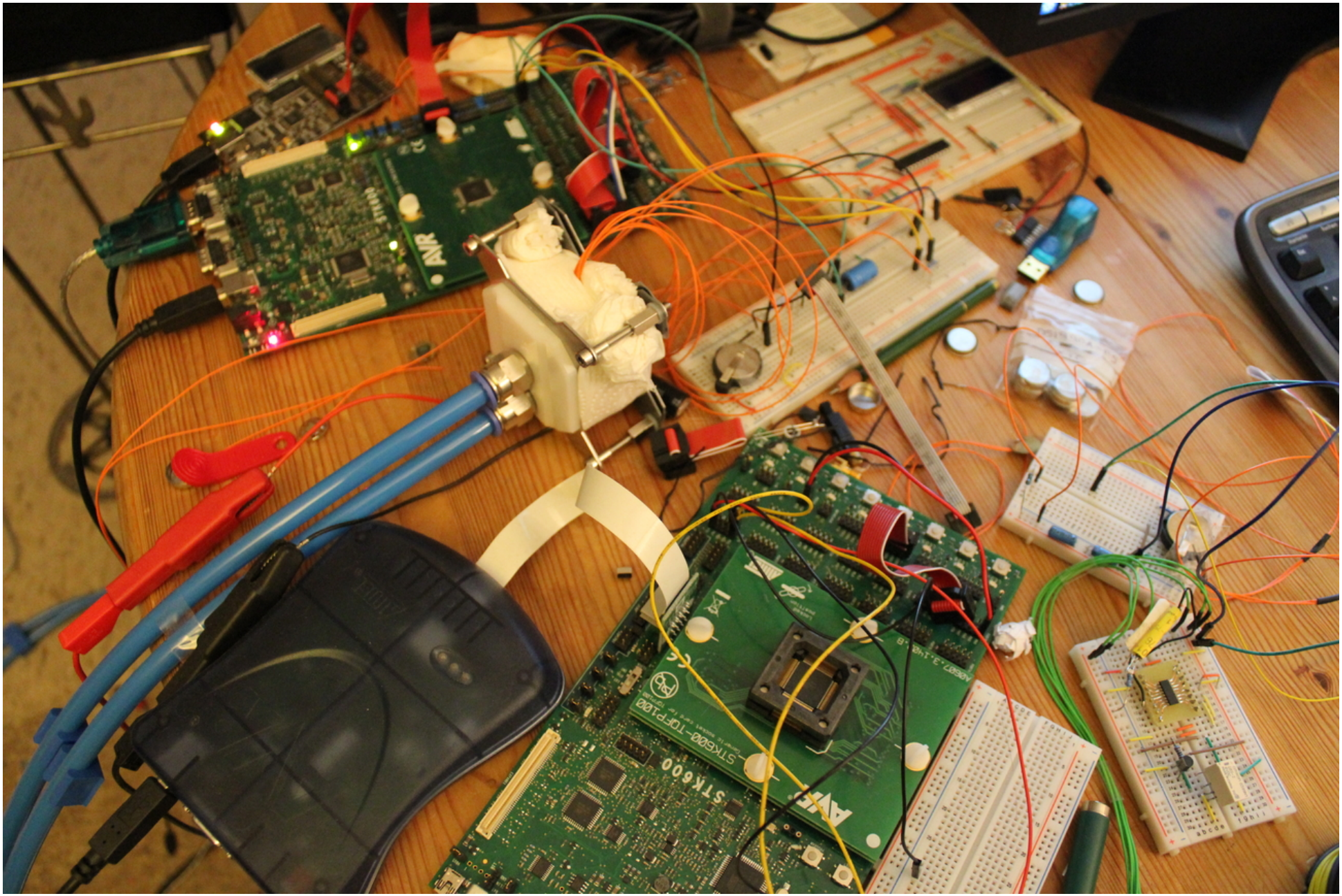

KÄLTE
75
Ergiebiges
Kältespray
Kühlt bis -52°C
KONTAKT CHEMIE
DEKRA - GEPRÜ
KONTAKT CHEMIE Kälte 75

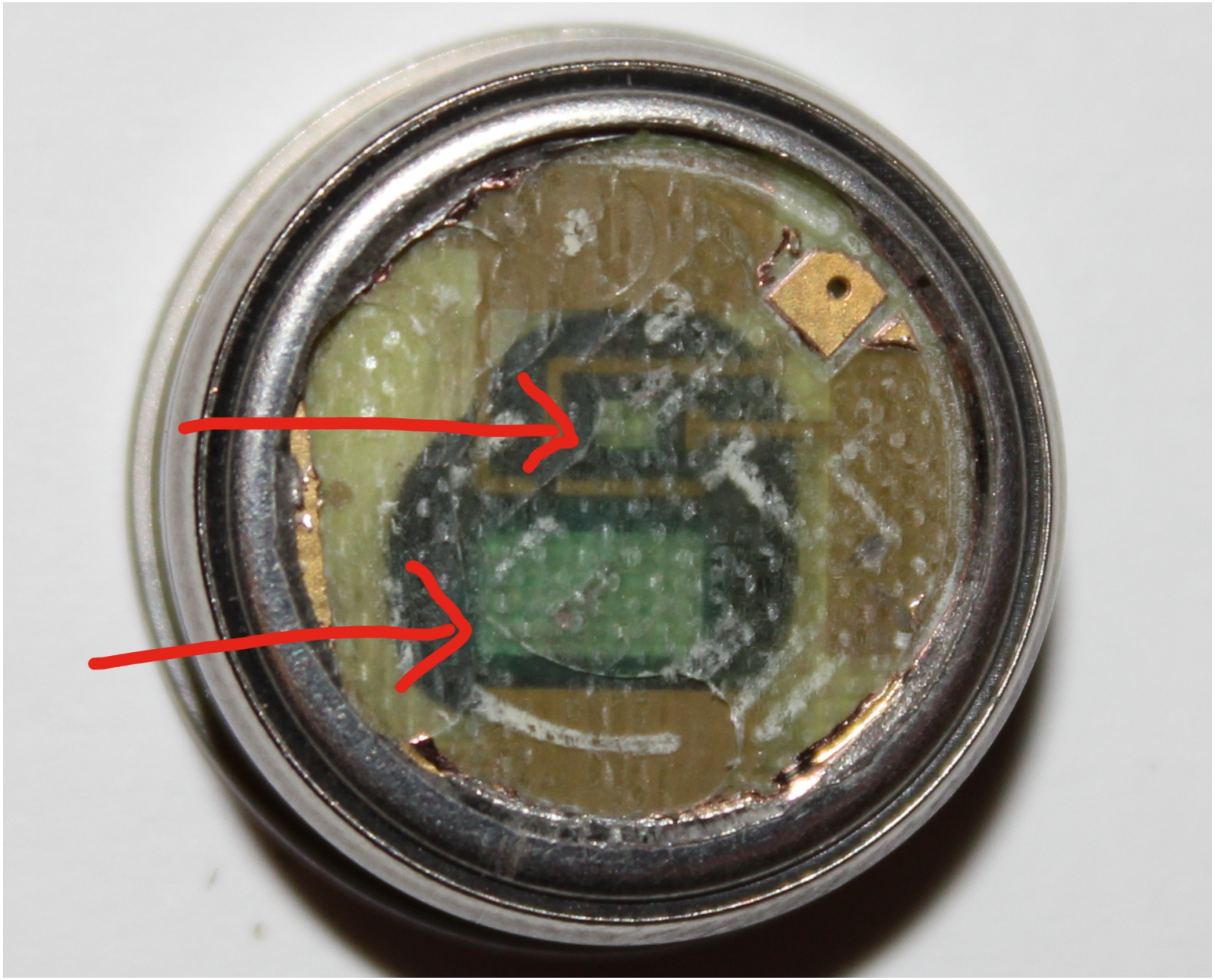

Ultracain®
setzt den Standard in der
zahnärztlichen Lokalanästhesie
Aventis
VOLTCRAFT
VC150
-007°C
POWER
HOLD
NCV
hFE
200m
2000m
20M
200k
20k
2000
200
20 V
200
250
250
V~
200
10
200m
20m
2000µ
°C
A
V
CAT III 250V
FUSED
10A/250V
MAX10sec
EACH15min
10A
COM
FUSED
200mA/250V
mAΩ

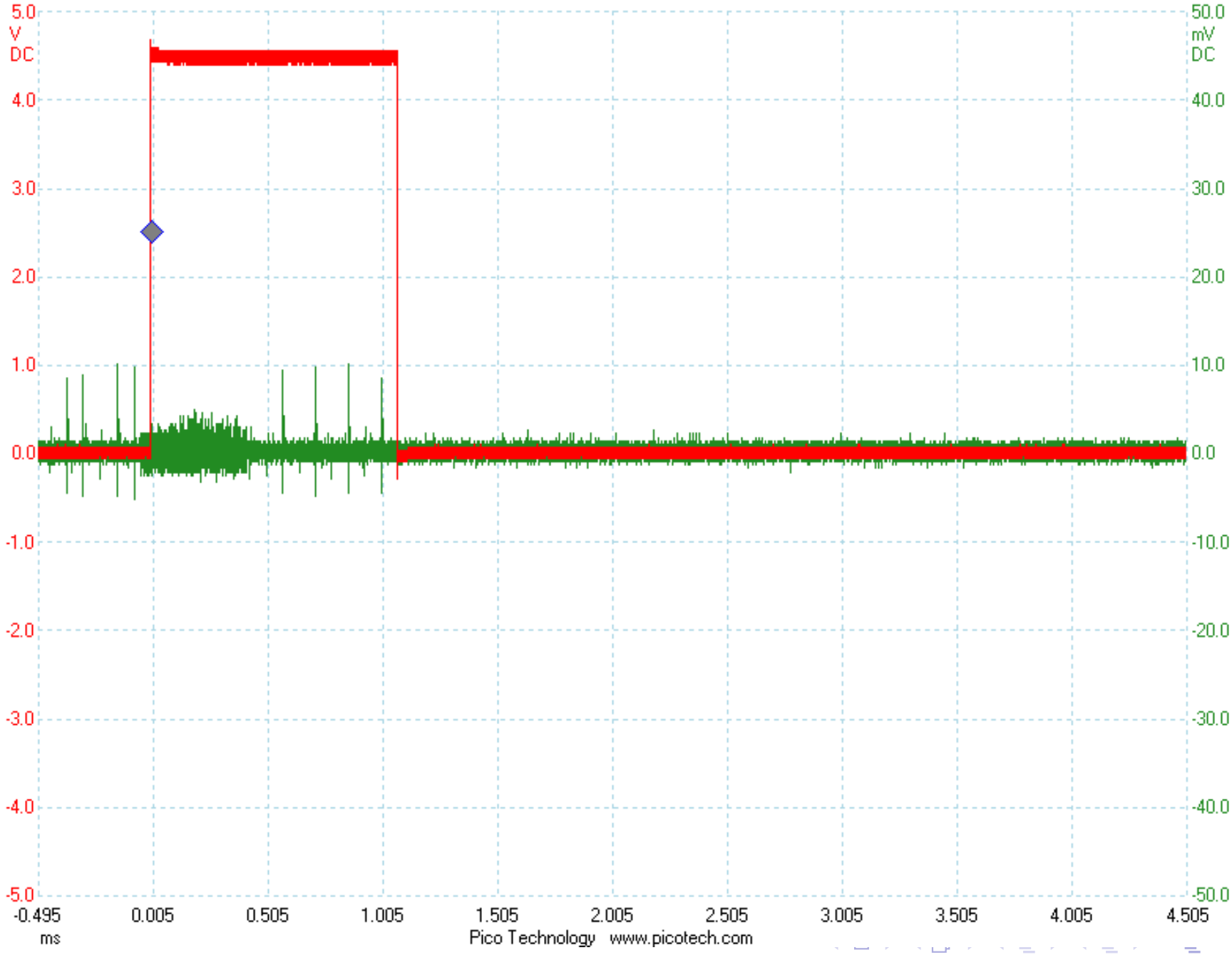

NB-BlackSilentPRO
developed in Germany
NB-BlackSilentPRO
developed in Germany

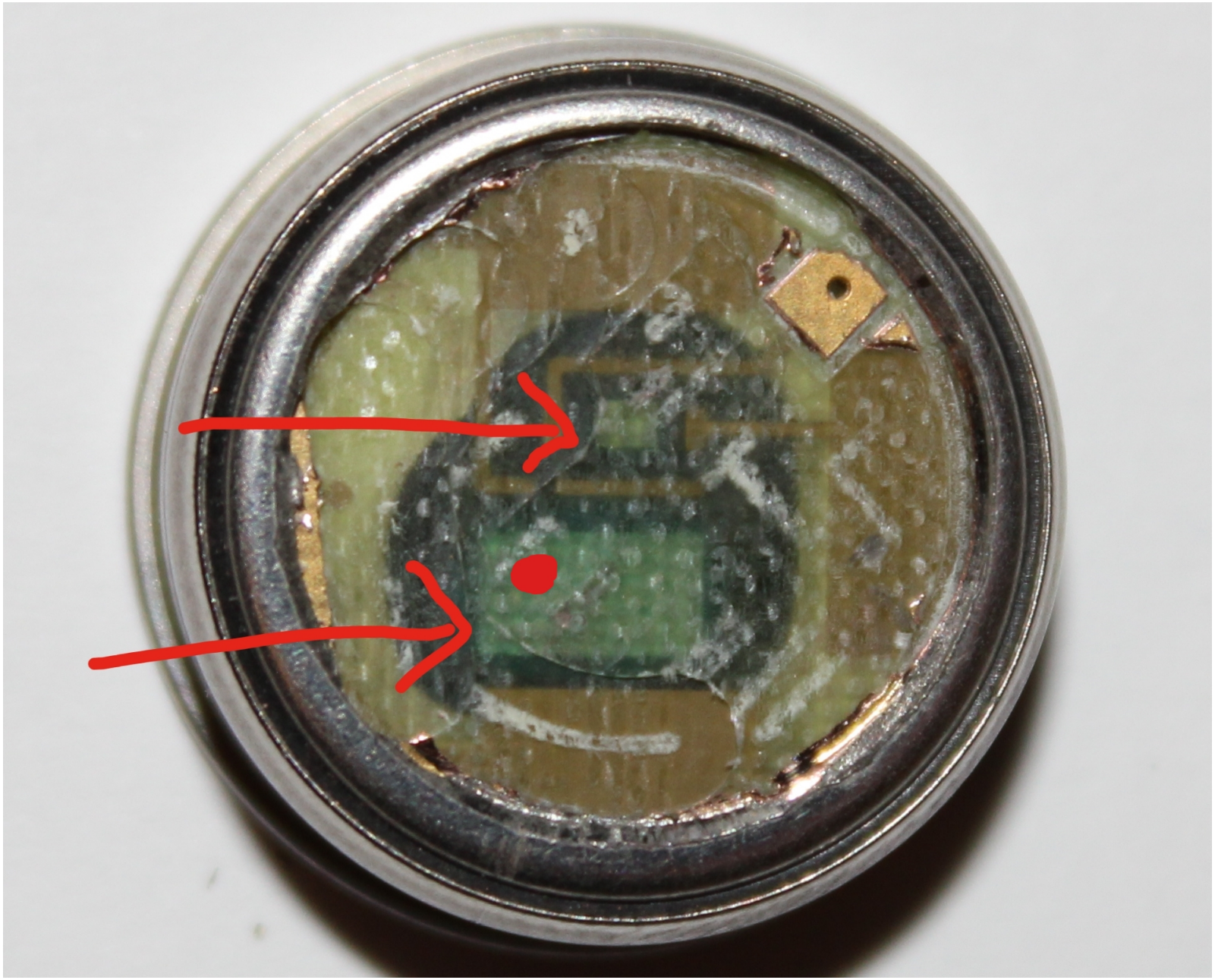





AVR
STK600-TQFP100
STK600




5.0
V
DC
4.0
3.0
2.0
1.0
0.0
-1.0
-2.0
-3.0
-4.0
-5.0
50.0
mV
DC
40.0
30.0
20.0
10.0
0.0
-10.0
-20.0
-30.0
-40.0
-50.0
-0.495
ms
0.005
0.505
1.005
1.505
2.005
2.505
3.005
3.505
4.005
4.505
Pico Technology www.picotech.com



und jetzt?

- was noch fehlt
  - Emulator
  - Angriffe auf eCash-Systeme
- viele weitere Hacks
  - weitere Faultattacken
  - und Seitenkanalangriffe
  - und vieles mehr ... später

DANKE FÜR'S ZUHÖREN