Teardown and feasibility study of IronKey – the most secure USB Flash drive

Dr Sergei Skorobogatov

http://www.cst.cam.ac.uk/~sps32 *email: sps32@cam.ac.uk*

UNIVERSITY OF CAMBRIDGE
Dept of Computer Science and Technology

Introduction

- Senior Research Associate at the University of Cambridge
  - Hardware Security research (attack technologies) since 1995
  - test microcontrollers, smartcards, FPGAs and SoCs for security
  - knowledge: chemistry, electronics, physics (MSc), computer science (PhD)
- Research interests
  - finding real solutions to “impossible problems”
  - developing new attack methods and techniques
  - testing challenging hardware devices for vulnerabilities
- Problems found in the past (or created)

2002: discovery of optical fault injection attacks shook the industry

2005: prove of data remanence in EEPROM and Flash memory

2006: demonstrating combined attacks of fault injection with power analysis

2010: bumping attacks that can extract AES key and data from Flash memory

2012: hardware acceleration to power analysis for finding backdoor in military FPGA

2016: demonstration of “impossible” NAND mirroring attack on iPhone 5c

2016: direct SEM imaging of EEPROM and Flash memory contents

2020: NVM vulnerability and finding backdoors in ECC authentication device

Why the IronKey?

- Has strong security claims: “world’s most secure flash drive”
- FIPS 140-2 Level 3 certified: sold to military and government users
- Possible candidate for our students hardware security practical
  - old one was completely hacked (presented at Hardwear.IO, Virtual, October 2020)
- Was recently in the news when a legitimate user was unable to access files with cryptocurrency assets
- There are public evaluations on encrypted USB drives but not IronKey
- Good to compare IronKey with other secure USB Flash drives
- The results could help in mitigation of possible data losses in the future
- Maybe also evaluate secure chips found inside
- Just for the sake of curiosity and to have some fun
- Hence, we do reverse engineering or can call it teardown

IronKey evaluation

- Encrypted USB Flash drives were evaluated before
  - Master's thesis that outline possible attack vectors
  - presentation by Google researchers
  - none of IronKey devices were previously looked at
- Test a few devices to see what is inside and how different they are
  - started with an old IronKey device collecting dust in my desk
  - ordered more old devices from eBay
  - ordered latest models of IronKey
  - started looking at encrypted USB drives from other manufacturers
  - looked at other USB devices with security
- In total 26 different USB devices were teared down
  - 9 families of IronKey devices from very first model to the latest one
  - 15 encrypted USB drives from Kingston, iStorage, MXI, DataLocker, Integral, SafeXS
  - USB controllers and secure chips from many USB drives were looked at
  - security protection level of encrypted USB Flash drives was compared
  - also looked at 2 cryptowallet devices to compare with their hardware security level

IronKey history

- USB Flash drives emerged on the market from early 2000
  - compact devices with decent storage size
  - if they are lost anyone can access the files
- IronKey was released by IronKey Inc. in 2007
  - user data is always encrypted with using AES256 in CBC or XTS mode
  - AES key is encrypted with user password and never leaves the device
  - number of consecutive incorrect password attempts is limited to 10
  - user applications are stored on write-protected partition (mounted as CD-ROM)
  - encrypted USB communication to prevent eavesdropping
- Hardware features
  - robust metal case: tamper proof and waterproof
  - inner part is potted with epoxy compound making it hard to access the PCB
  - specialised USB controller with hardware AES256 encryption engine
  - secure way of AES key storage, password verification, max 10 password attempts
  - reliable Flash memory storage

IronKey history

- IronKey Inc. was an internet security and privacy company since 1996
- Development of tamper-resistant USB Flash drive 2005 – 2007
  - US government grant US$1.4 million and US$6 million from venture investors
  - aimed at military, government and corporate users with FIPS 140-2 Level 3
  - robust waterproof and tamper-resistant case
  - relied on secure chip for AES256 key storage and password protection
- First device IronKey D2 was released in 2007
  - certified to FIPS 140-2 Level 2
- Next revision IronKey D2 Rev.2 was released in 2008
  - more robust case and modified hardware
- Improved version of IronKey devices in 2009
  - S100, D200, S200: improved security and optimised hardware
  - certified to FIPS 140-2 Level 3
- In 2011 Imation Corp. bought the hardware business of IronKey Inc.
  - IronKey devices started to be sold under Imation name

IronKey history

- Imation Corp. was already a storage device manufacturer
- Has acquired MXI Security from Memory Experts International in 2011
  - added encrypted USB Flash drives: Defender F100 and Defender F150
- New IronKey devices F100 and F150
  - certified to FIPS 140-2 Level 3
- New IronKey device F200 with biometric fingerprint identification
  - IronKey devices started to be sold under Imation name
- Two new members of IronKey devices in 2013
  - D250, S250: improved characteristics
  - certified to FIPS 140-2 Level 3
- Budgetary version of IronKey D80 in 2014 (plastic case, no cert.)
- In 2015 first USB3.0 version of IronKey device S1000
  - the fastest USB Flash drive on the market with hardware AES256 encryptionn
- In 2016 the IronKey business split between DataLocker and Kingston

IronKey history

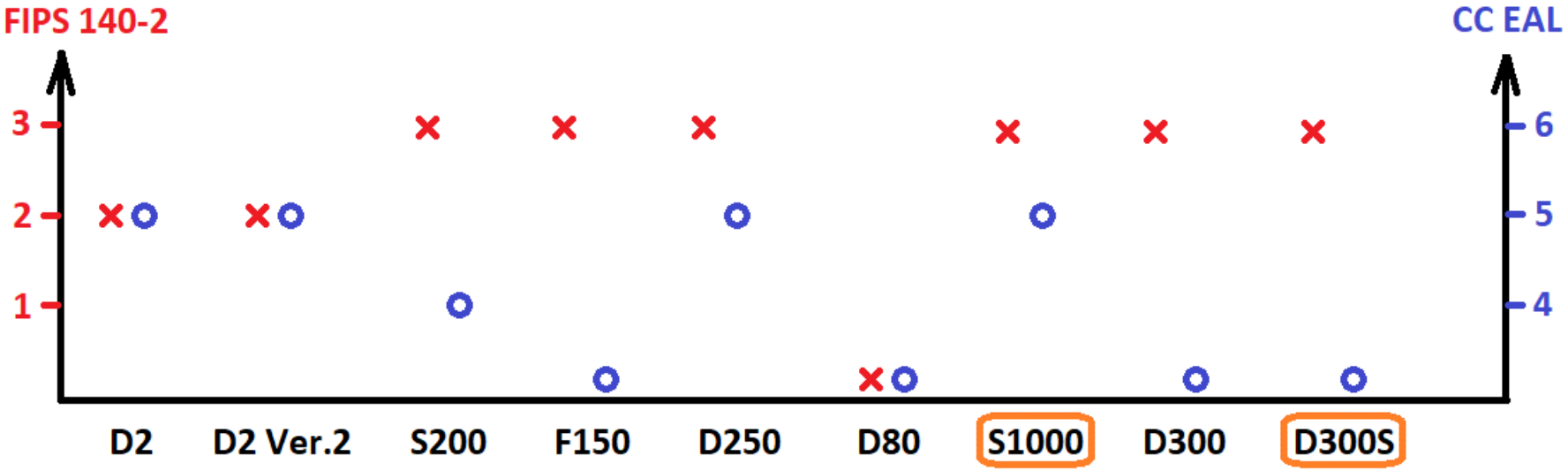
- Kingston Digital Inc. is manufacturer and distributor of memory products and part of Kingston Technology Corp.
- Kingston had its own line of encrypted USB Flash drives
  - DataTraveler Locker and DataTraveler Vault Privacy from 2010
  - DataTraveler 4000 with FIPS 140-2 Level 2 certification from 2011
  - USB3.0 devices: DataTraveler Locker+G3, Vault Privacy 3.0 (FIPS 197) from 2015
  - USB3.0 device DataTraveler DT4000G2 (FIPS 140-2 Level3) from 2015
- New IronKey device D300 in 2016
  - USB3.0, advanced security, certified to FIPS 140-2 Level 3 and approved by NATO
  - IronKey devices started to be sold under Kingston name
- In 2018 the latest model of IronKey device D300S
  - improved security features (serialisation and virtual keyboard)
  - certified to FIPS 140-2 Level 3
- At the moment only S1000 and D300S models are on the market

Other manufacturers

- DataLocker
  - USB2.0 and USB3.0 devices with FIPS 197 and FIPS 140-2 Level 2 and 3
- Integral
  - USB3.0 devices with FIPS 197 and FIPS 140-2 Level 2
- MXI Security
  - USB2.0 devices with FIPS 140-2 Level 3
- SafeXS
  - USB3.0 devices without certification
- iStorage
  - USB2.0 and USB3.0 devices with numerical keypad and battery inside
  - FIPS 140-2 Level 3 certified
- Other manufacturers: Verbatim, Corsair, Apricorn, Kanguru, Freecom, Elecom and others

Security certification

- FIPS (Federal Information Processing Standards) certification levels
  - FIPS 197: looks at hardware encryption algorithms
  - FIPS 140-2: more advanced with rigorous analysis of physical protection
- Common Criteria (CC) Evaluation Assurance Levels
  - EAL4: methodically designed, tested and reviewed
  - EAL5: semi-formally designed and tested
  - EAL6: semi-formally verified design and tested
  - EAL7: formally verified design and tested

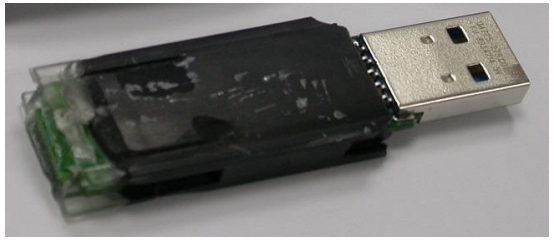


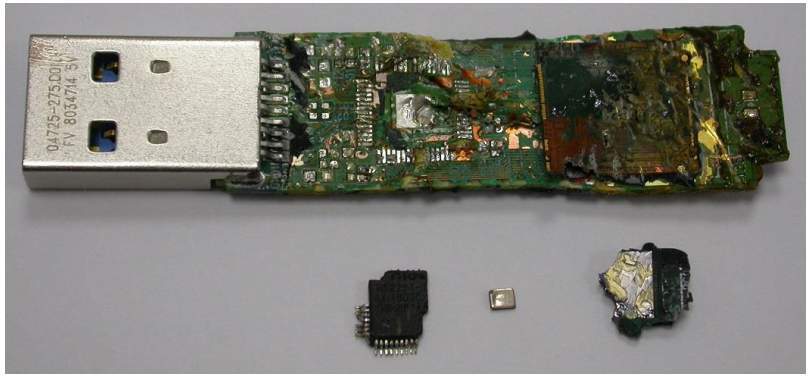
Opening robust metal case

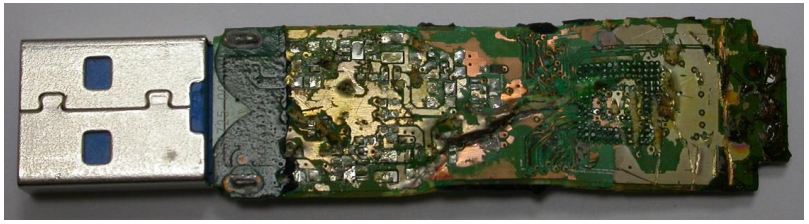
- Can be opened using mechanical tools (saw, blade, knife, chisel, CNC)
- This will leave tamper evidence

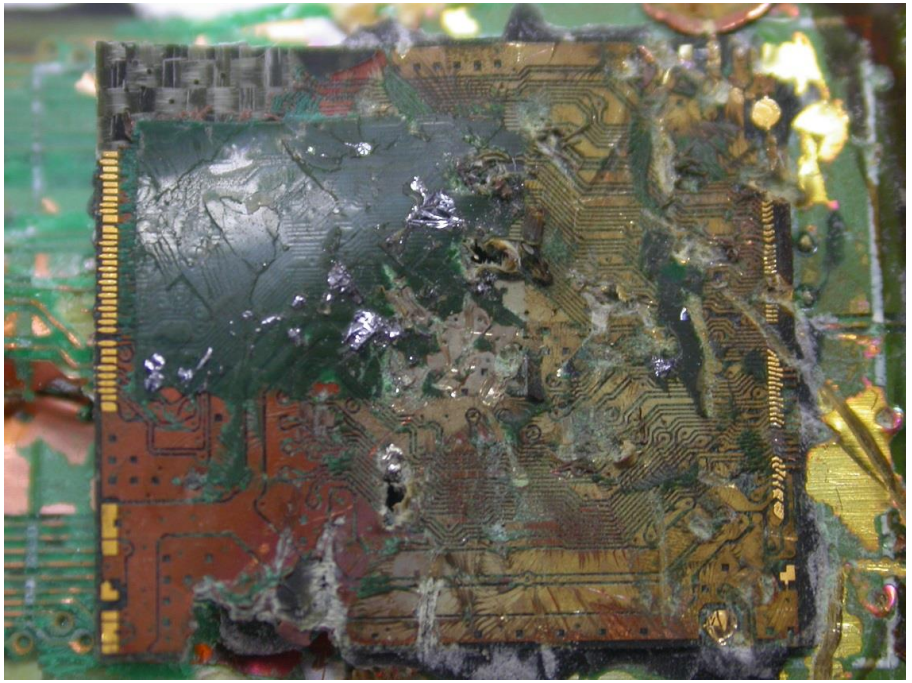
Removing epoxy compound

- Mechanical methods (hammer, drill, blade, knife, CNC)
  - danger of breaking PCB components (epoxy sticks better to IC than to PCB)



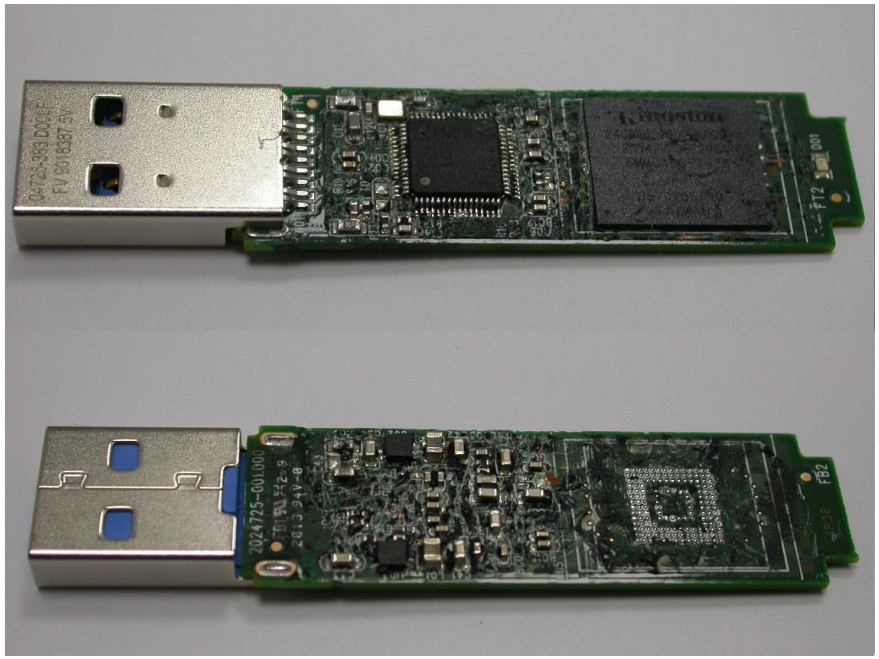






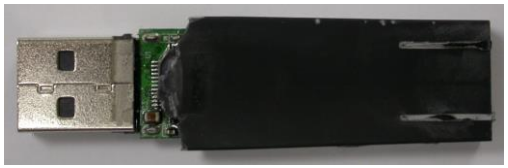
Removing epoxy compound

- Thermal methods: epoxy looses its strength above 150˚C (302˚F)
  - easier to remove with mechanical tools (knife, needle, tweezers)
  - danger of breaking or de-soldering PCB components
  - careful removal using solder iron tip (temperature and force control, mind the tip)



Removing epoxy compound

- Chemical methods: epoxy is not good for harsh environment
  - can be corroded by acids, alkalines, organic solvents and even water steam
  - can be combined with thermal and mechanical methods for better efficiency
  - danger of damaging components and PCB (IC packages and FR4 contain epoxy)



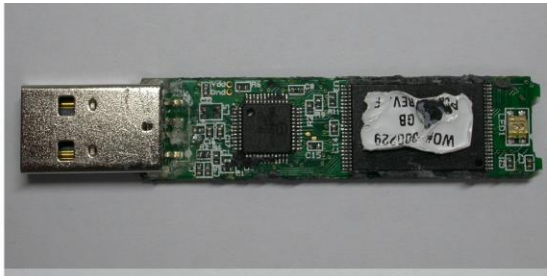
Removing epoxy compound

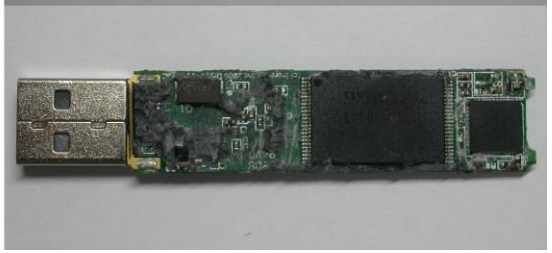
- Other methods
  - laser ablation (laser cutter)
  - plasma methods (microwave induced plasma (MIP) from Ar, O_2 or CF_4)
  - combined methods
    - mechanical tools followed by thermal methods
    - mechanical tools followed by chemical methods
    - chemical methods followed by thermal methods
    - chemical methods combined with thermal methods

IronKey D2 teardown

- Metal case was opened with pliers after removing the lid


- Epoxy was removed using thermal method

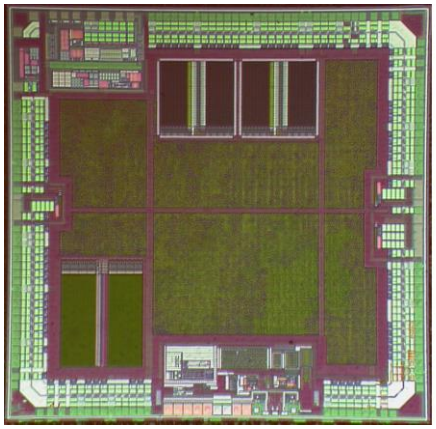
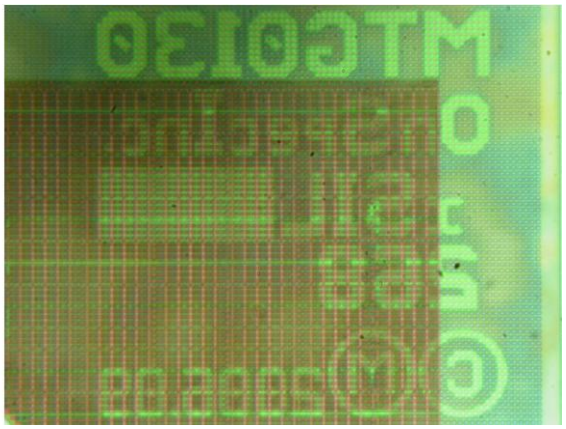





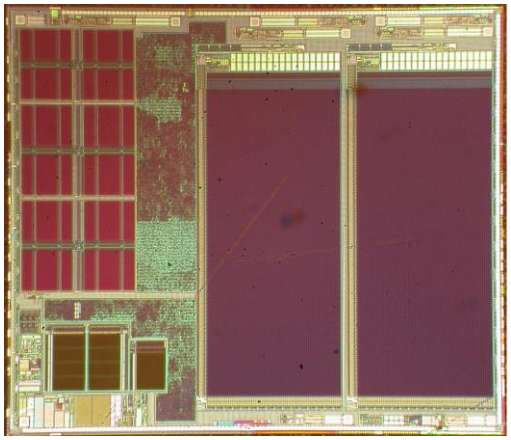
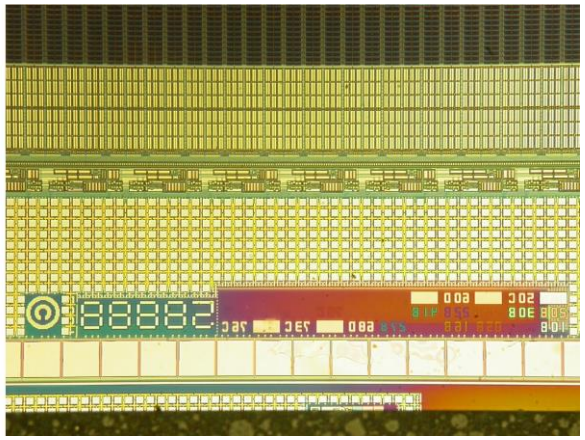
- IRONKEY 294.001, SAMSUNG K9K8G08U0A, ATMEL 98SC008CT

IronKey D2 teardown

- IRONKEY 294.001 die marking: On Spec Inc. MTG0130
  - Custom device with Mask ROM and SRAM

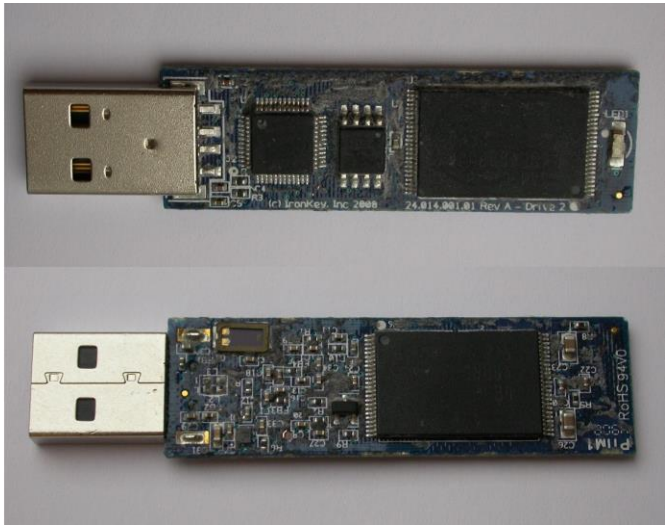
- ATMEL 98SC008CT die marking: 58888
  - Atmel Secure ASSP AT98SC008CT authentication device, EAL5+

IronKey D2 Ver.2 teardown

- Metal case was cut with mini saw

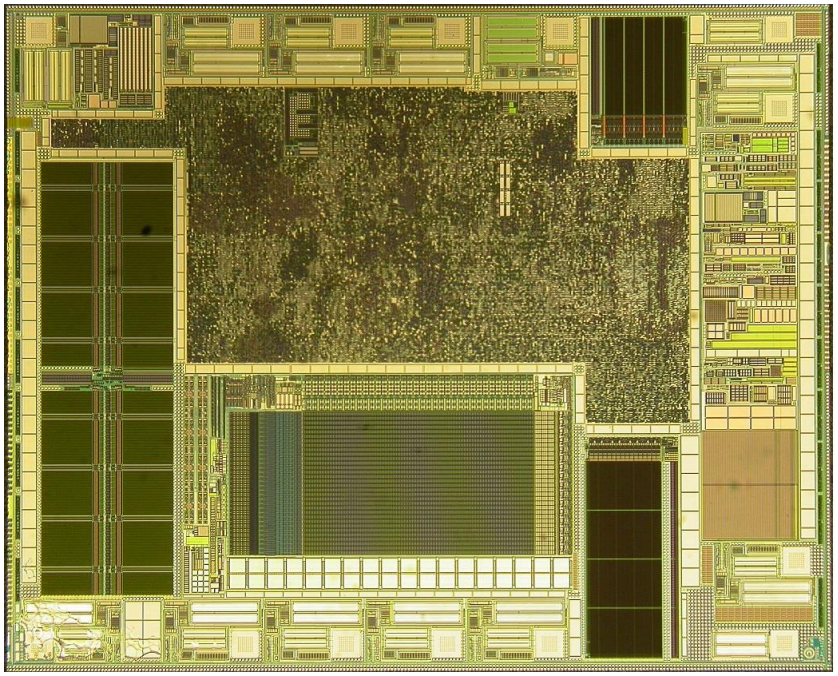
- Epoxy was removed using chemical method

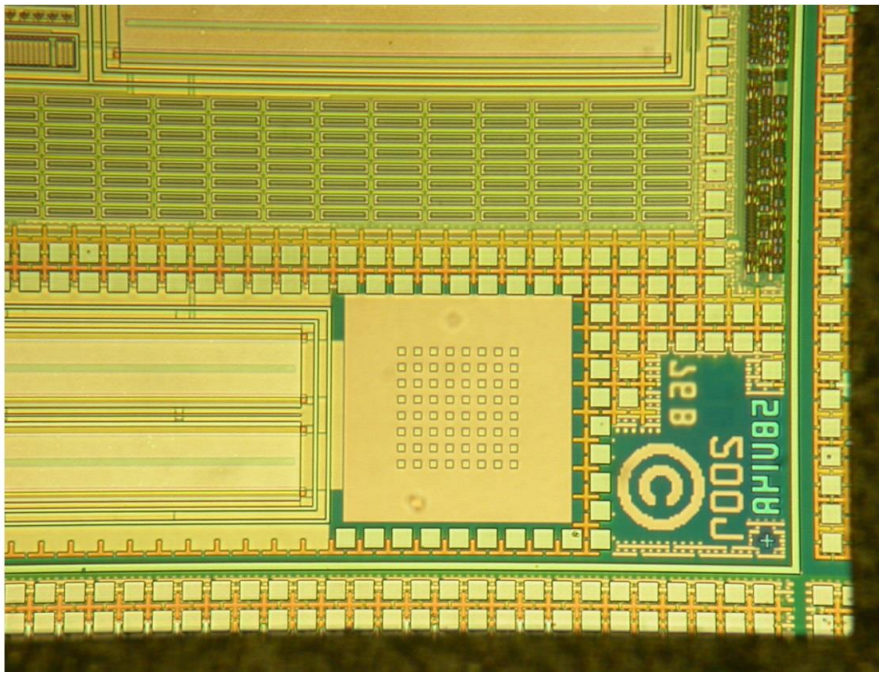


- IRONKEY 294.001, SAMSUNG K9F4G08U0A, ATMEL 016CU-R

IronKey D2 Ver.2 teardown

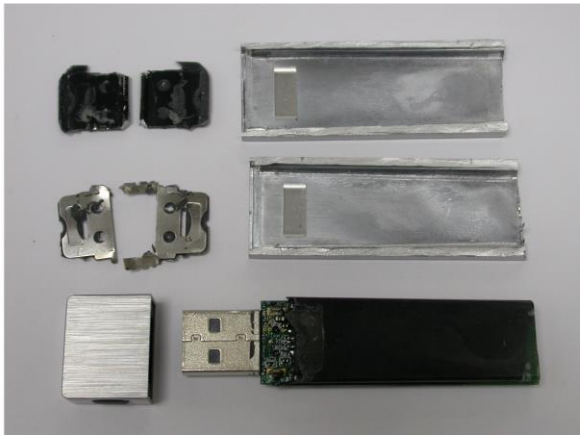
- ATMEL 016CU-R die marking: 58U14A
  - Atmel Secure ASSP AT98SC016CU authentication device, EAL4+



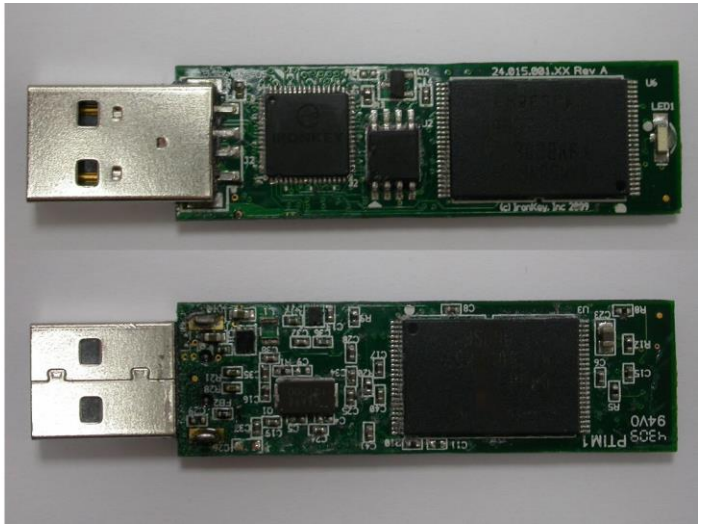


IronKey S200 teardown

- Metal case was cut with mini saw



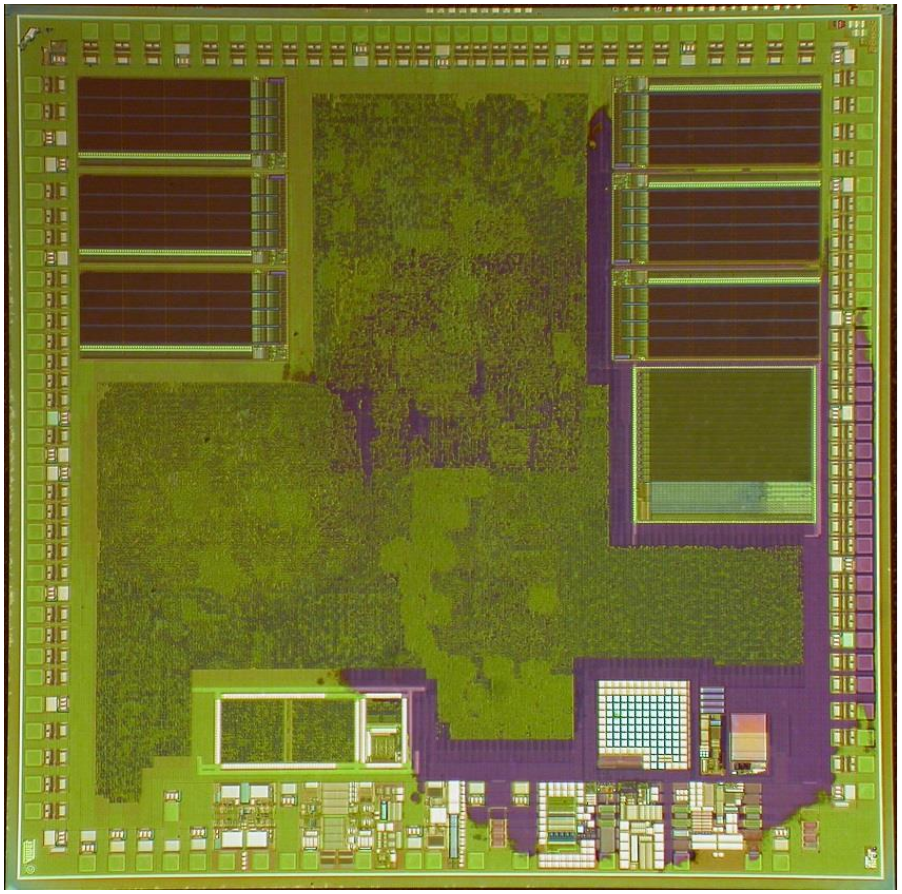
- Epoxy was removed using thermal method

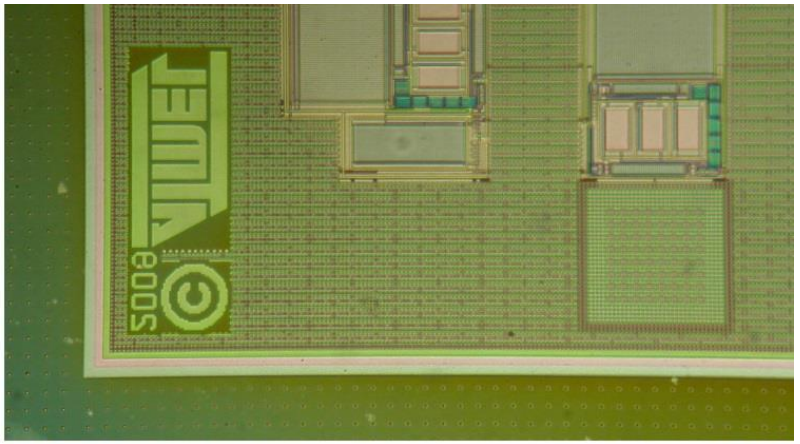


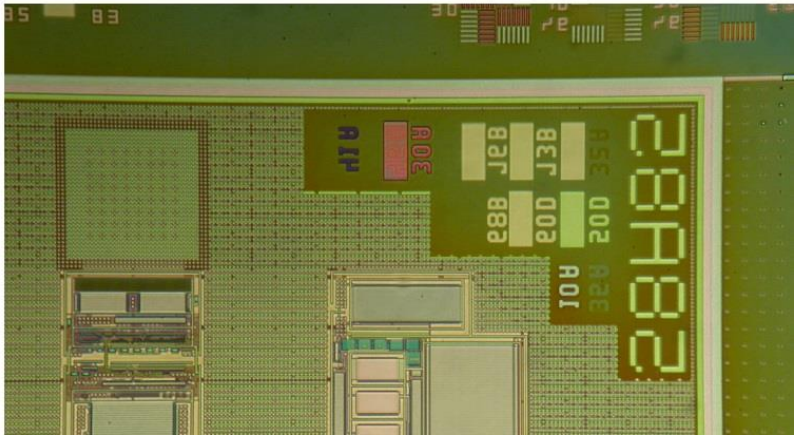
- IRONKEY 294.005, SAMSUNG K9WBG08U1M, ATMEL 016CU-R

IronKey S200 teardown

- IRONKEY 294.005 die marking: 58A85
  - Atmel custom device with Mask ROM and SRAM

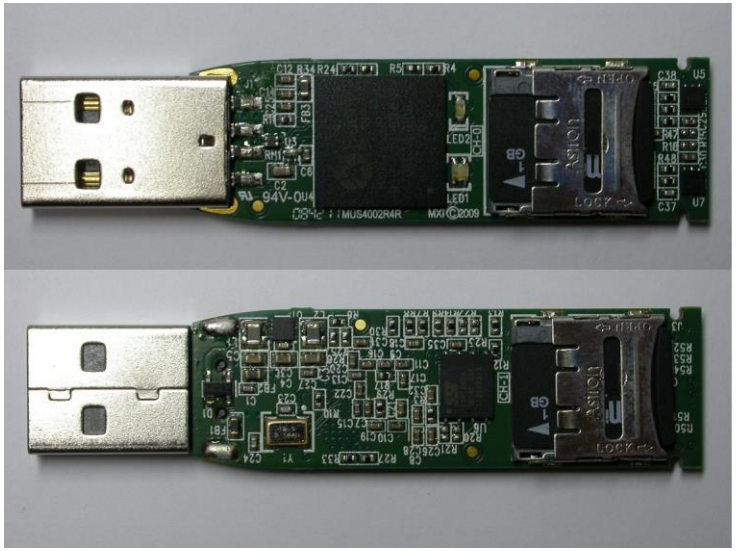






IronKey F150 teardown

- Plastic case is easy to open and no epoxy inside

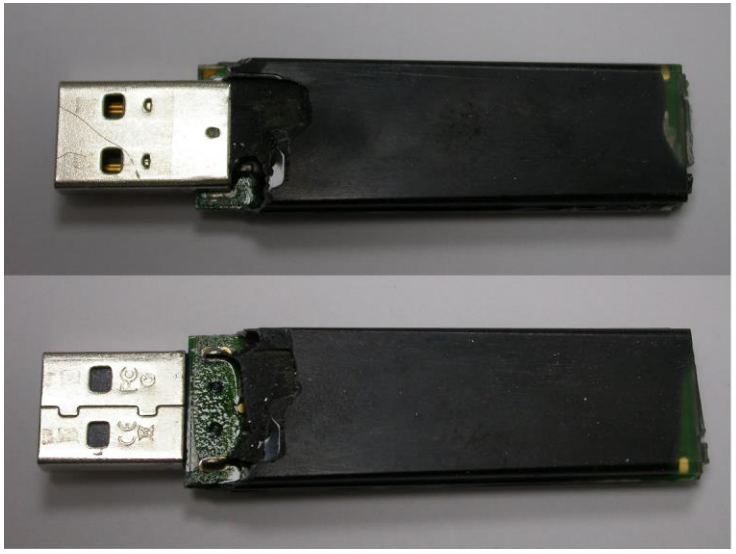


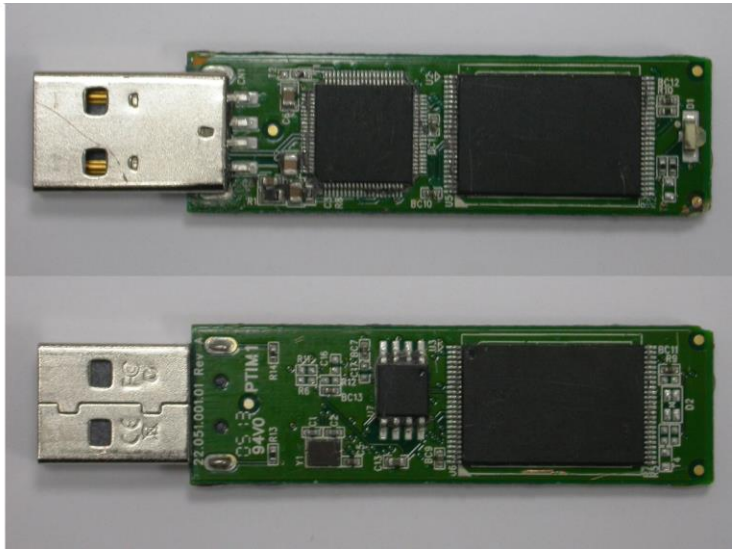
- Bluefly Processor 950 000 004 R, SST 25VF040B, microSD cards
  - exactly the same PCB and hardware components as MXI Security Stealth M200

IronKey D250 teardown

- Metal case was cut with mini saw

- Epoxy was removed using thermal method

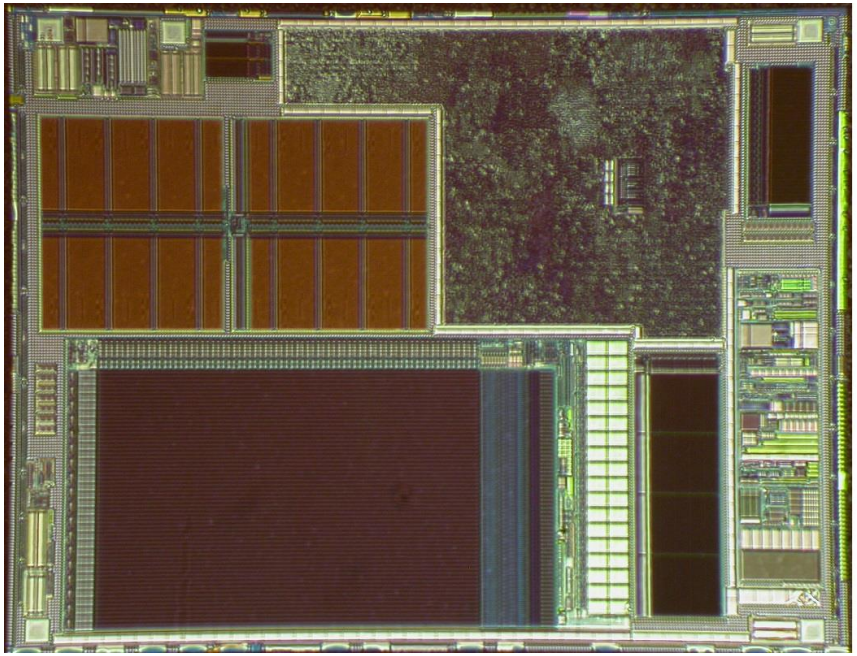


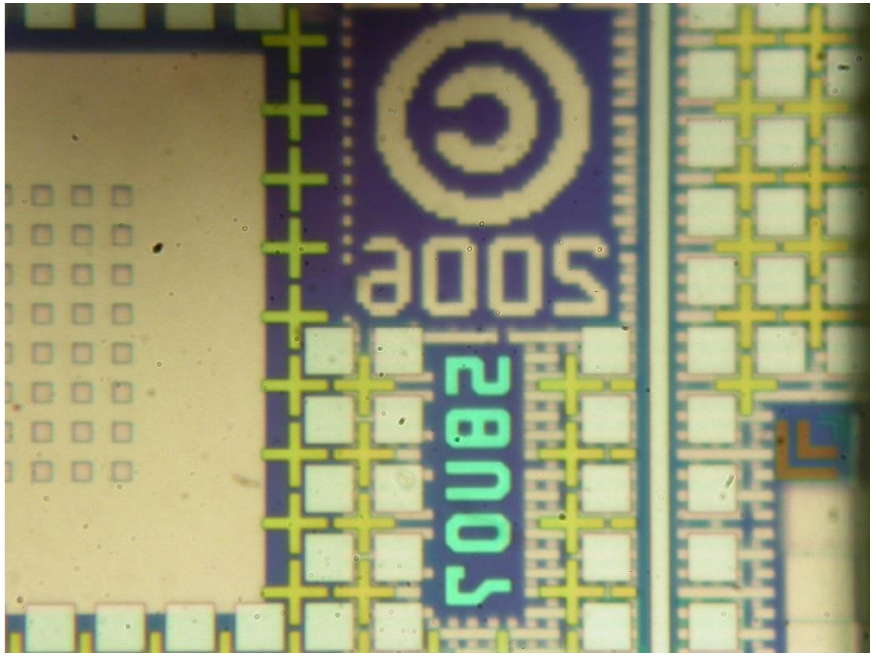


- PHISON PS2251-85-9, Micron 29F16G08CBACA, IRONKEY 31AV011

IronKey D250 teardown

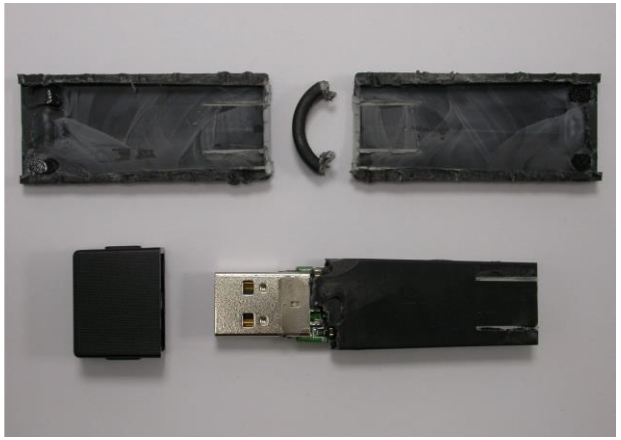
- IRONKEY 31AV011 die marking: 58U07
  - Atmel device





IronKey D80 teardown

- Plastic case was cut with mini saw

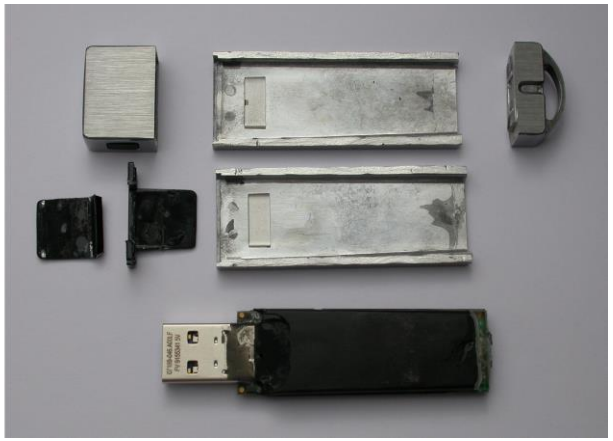


- Epoxy was removed using chemical method

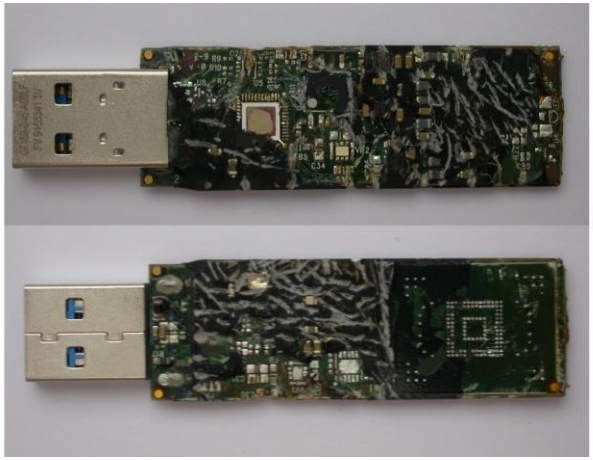
- PHISON PS2251-73-5, Micron 29F32G08CBACA

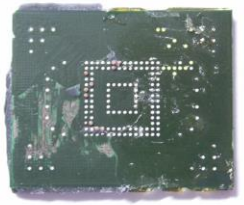
IronKey S1000 teardown

- Metal case was cut with mini saw



- Epoxy was removed using thermal method





- D720230K8, µSSD PHISON PSS5A311-16G, IRONKEY 31AV011
  - Renesas USB3.0 to SATAIII bridge, SATAIII SSD chip (6Gb/s), Atmel device

IronKey D300 and D300S teardown

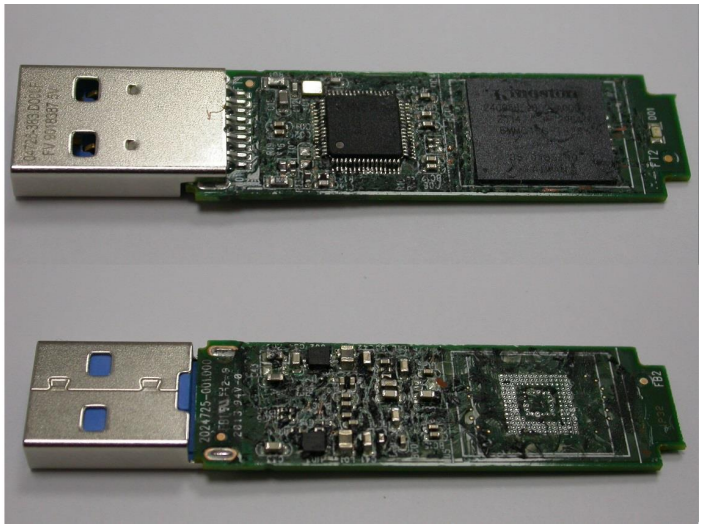
- Metal case was cut with mini saw
- Epoxy was removed using thermal method

- PHISON PS2251-15-Q, Kingston EMMC16G-TB28

Kingston DT4000G2 teardown

- Plastic case is easy to open

- Epoxy was removed using thermal method



- PHISON PS2251-15-Q, Kingston EMMC16G-TB28
  - exactly the same PCB revision and components as IronKey D300 and D300S

Kingston DT4000G2 teardown

- FIPS 140-2 certification documents (security policy)
  - IronKey D300 is the same except the names (even firmware version is the same)

2.4 Cryptographic Module Specification

The module is the Kingston Technology DataTraveler DT4000 G2 Series USB Flash Drive running Firmware Version 3.05 on Hardware part DT4000 Version 1.0 [4GB, 8GB, 16GB, 32GB, 64GB, 128GB or 256GB]. The module is classified as a multi-chip standalone cryptographic module, and the physical cryptographic boundary is drawn at the module's printed circuit board with USB connector and LED interface and includes all significant components within that boundary. The module's memory is logically partitioned; memory not executable by the module (Host-application 4.0.0 on CD-ROM partition) is considered excluded. The physical boundary is pictured in the image below:

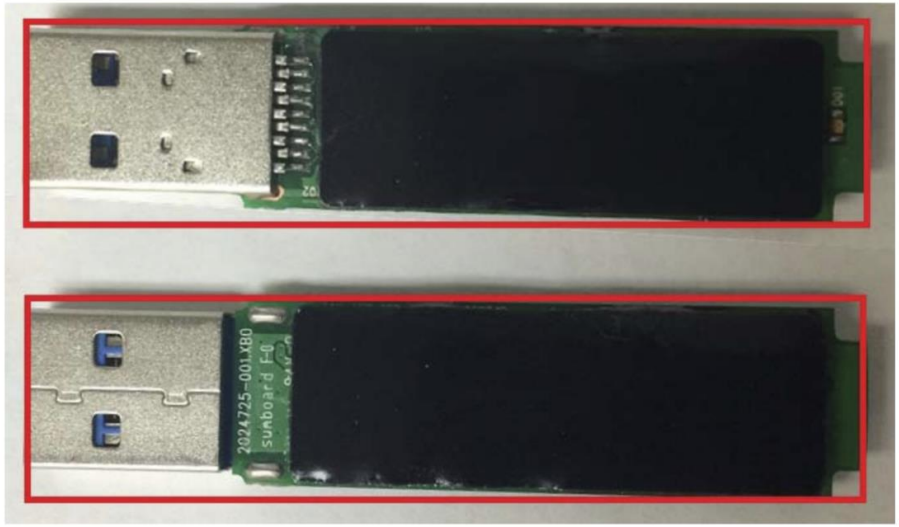


Figure 1 – Physical Boundary

2.4 Cryptographic Module Specification

The module is the Kingston Technology IronKey D300 Series USB Flash Drive running Firmware Version 3.05 on Hardware part IKD300 Version 1.0 [4GB, 8GB, 16GB, 32GB, 64GB, 128GB or 256GB]. The module is classified as a multi-chip standalone cryptographic module, and the physical cryptographic boundary is drawn at the module's printed circuit board with USB connector and LED interface and includes all significant components within that boundary. The module's memory is logically partitioned; memory not executable by the module (Host-application 4.0.0 on CD-ROM partition) is considered excluded. The physical boundary is pictured in the image below:

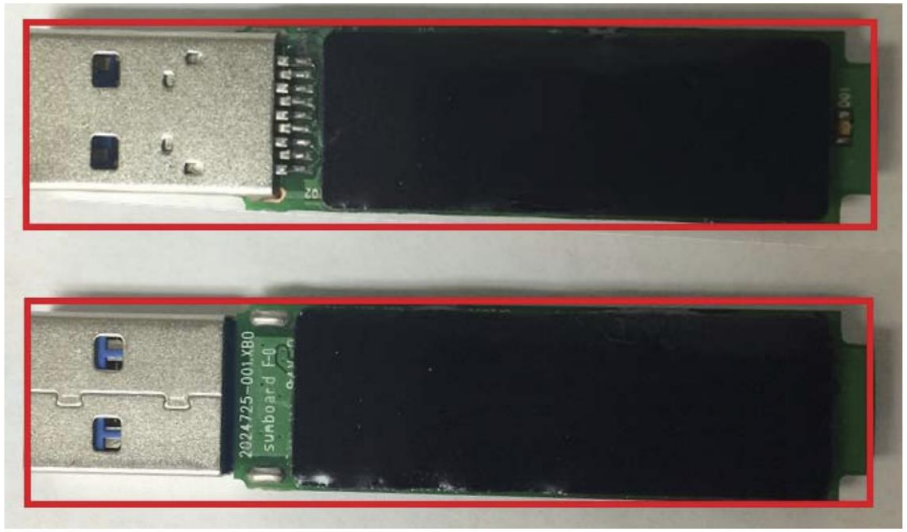
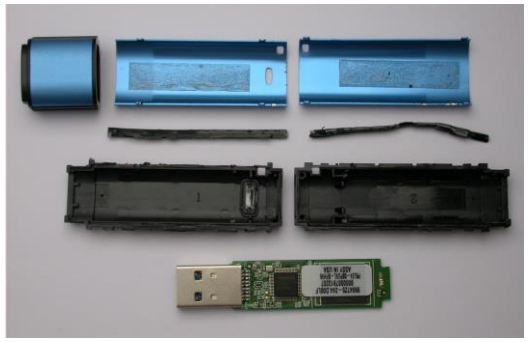
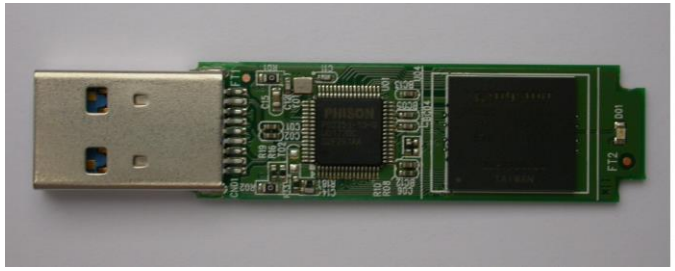


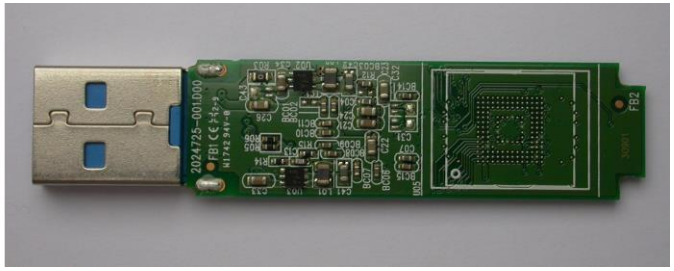
Figure 1 – Physical Boundary

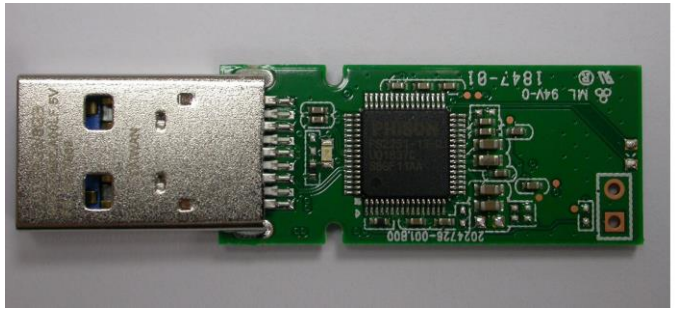
Kingston DTVP30 and DTLPG3 teardown

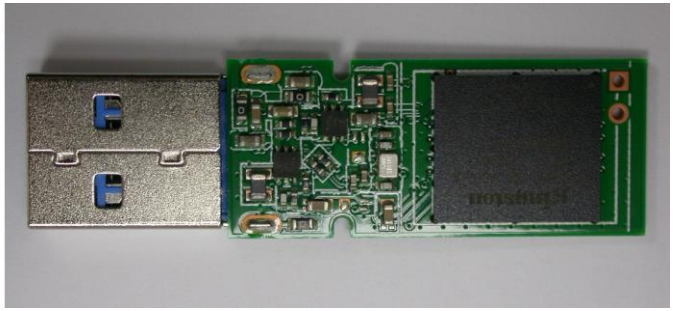
- Cases are easy to open and no epoxy inside







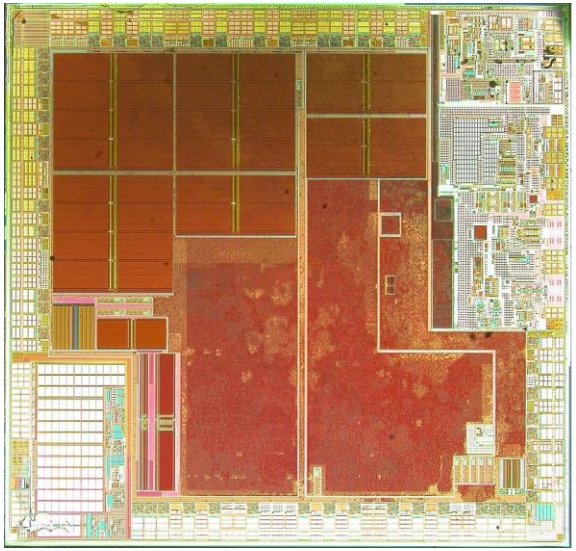
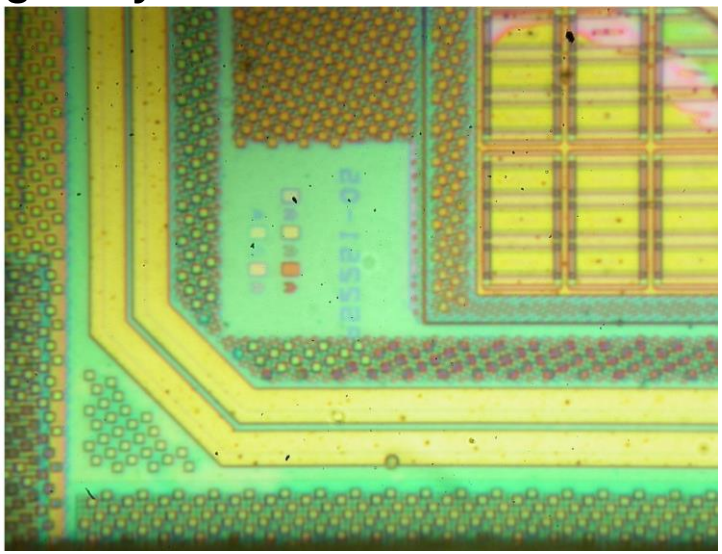
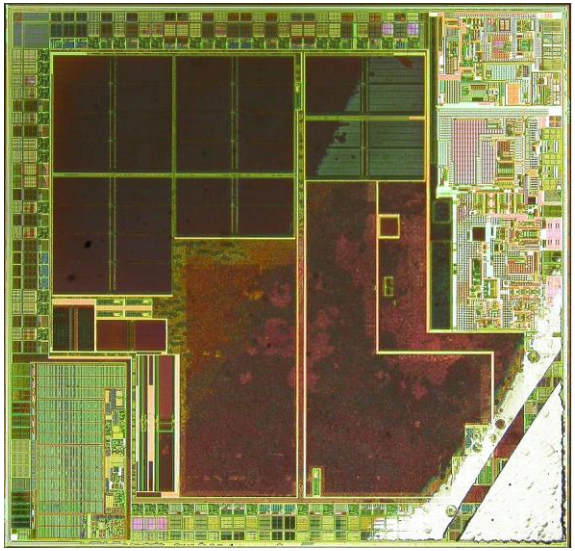
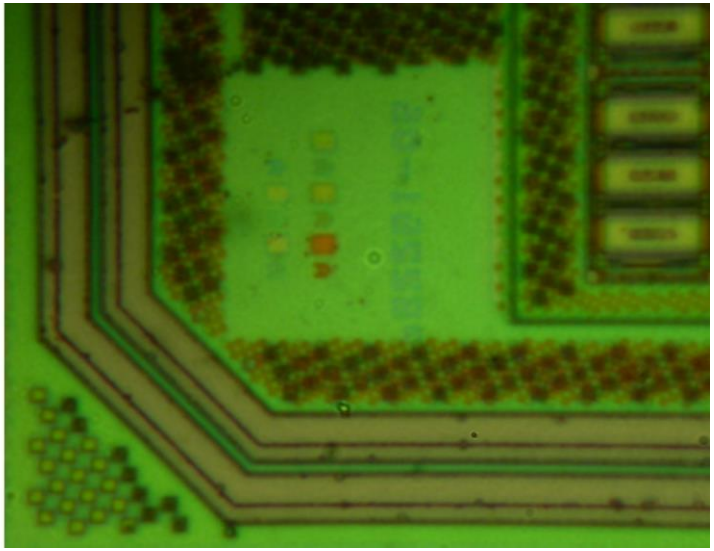




- PHISON PS2251-13-Q, Kingston EMMC04G-M627
- PHISON PS2251-13-Q, Kingston EMMC08G-M325

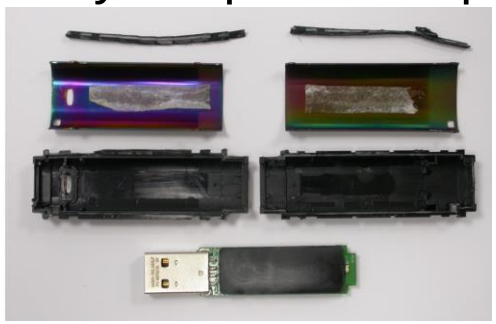
Phison PS2251-15-Q vs PS2251-13-Q

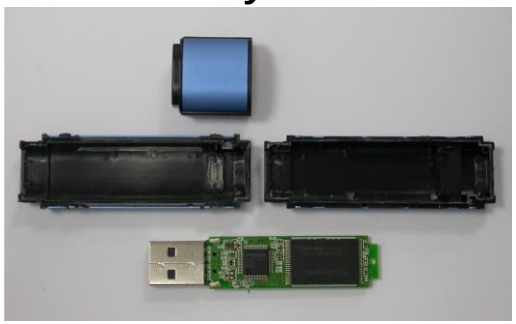
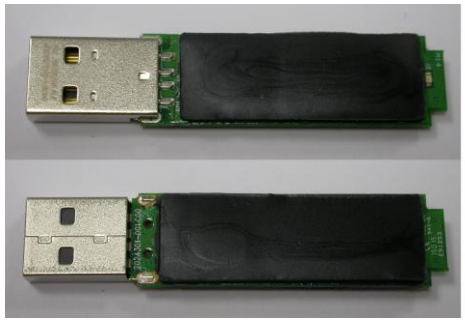
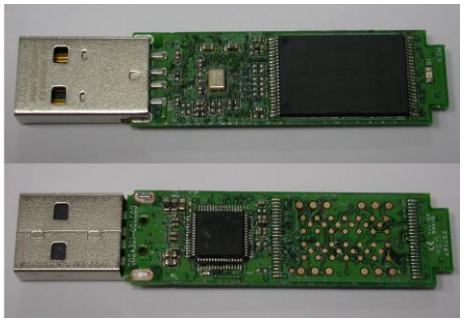
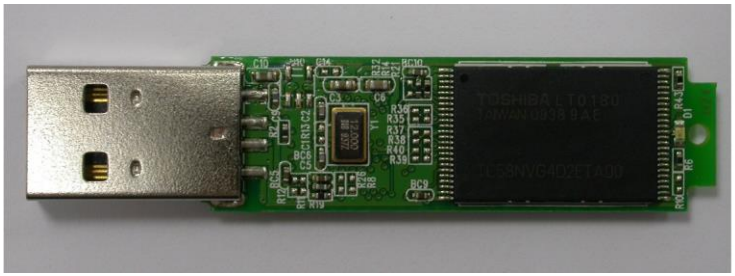
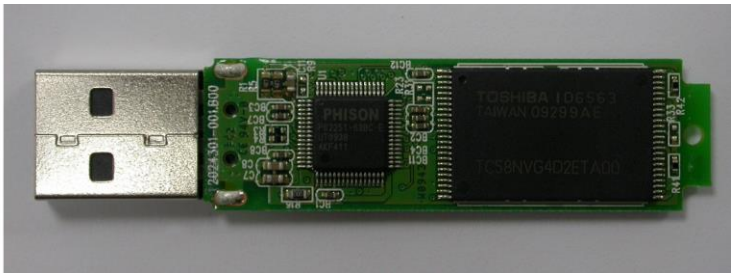
- Both have same die marking, only Mask ROM and SRAM: PS2251-05

Kingston DT4000 and DTVP teardown

- Cases are easy to open and epoxy in DT4000 was chemically removed

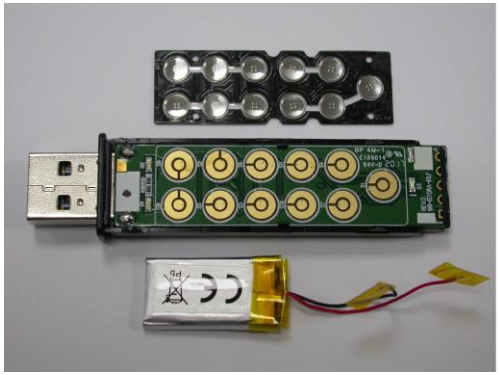
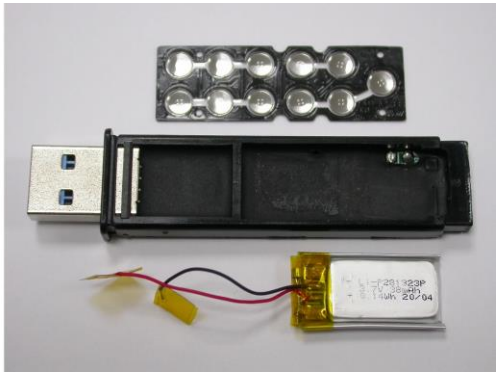


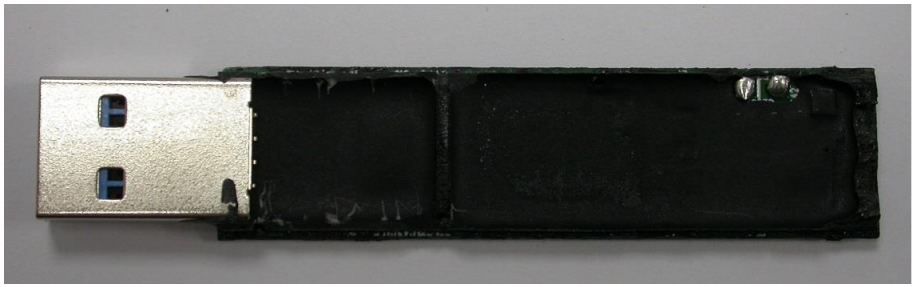
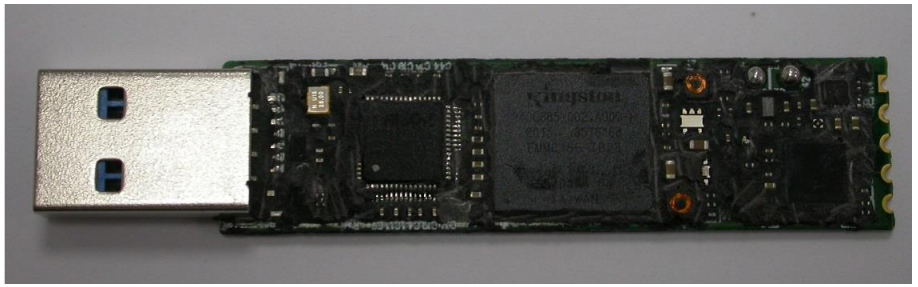
- PHISON PS2251-65-6, Micron 29F32G08CBACA
- PHISON PS2251-63BC-E, Toshiba TC58NVG4D2ETA00

Kingston DT2000 teardown

- Metal case is easy to open: remove the cap and slide

- Epoxy was removed using both chemical and thermal methods

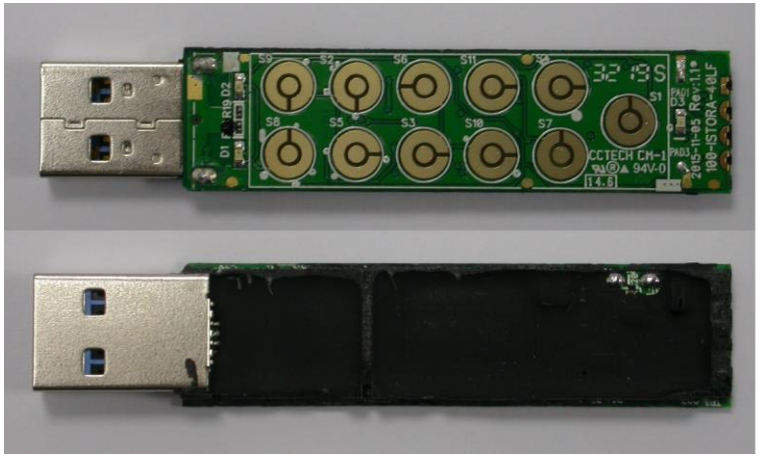



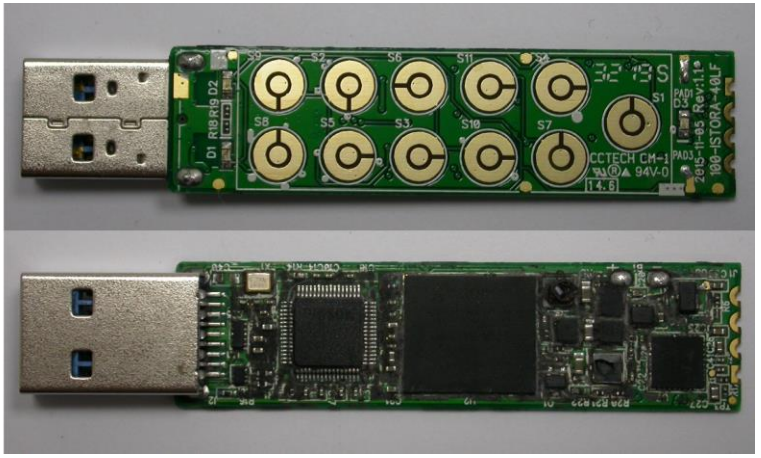
- PHISON PS2251-13-Q, Kingston EMMC16G-TB28, L051K6 (STM32)

iStorage Datashur Pro teardown

- Metal case is easy to open: remove the cap and slide

- Epoxy was removed using chemical method

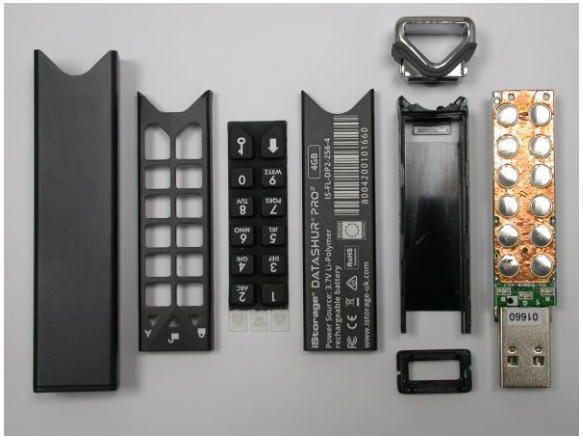




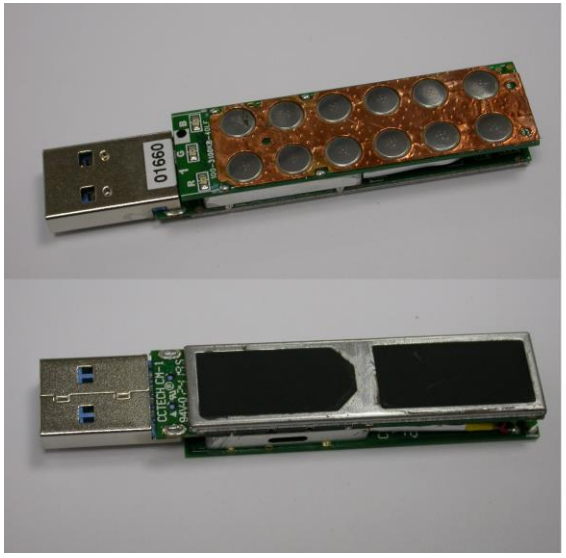
- PHISON PS2251-13-Q, Kingston EMMC04G-M627, L051K8 (STM32)

iStorage Datashur Pro2 teardown

- Metal case was cut with mini saw



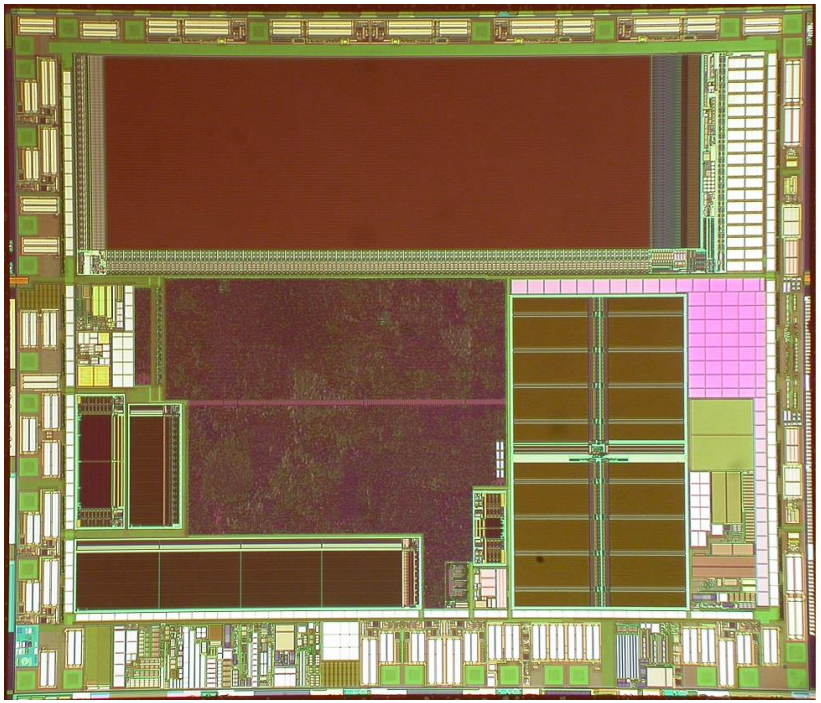
- Epoxy was removed using chemical method

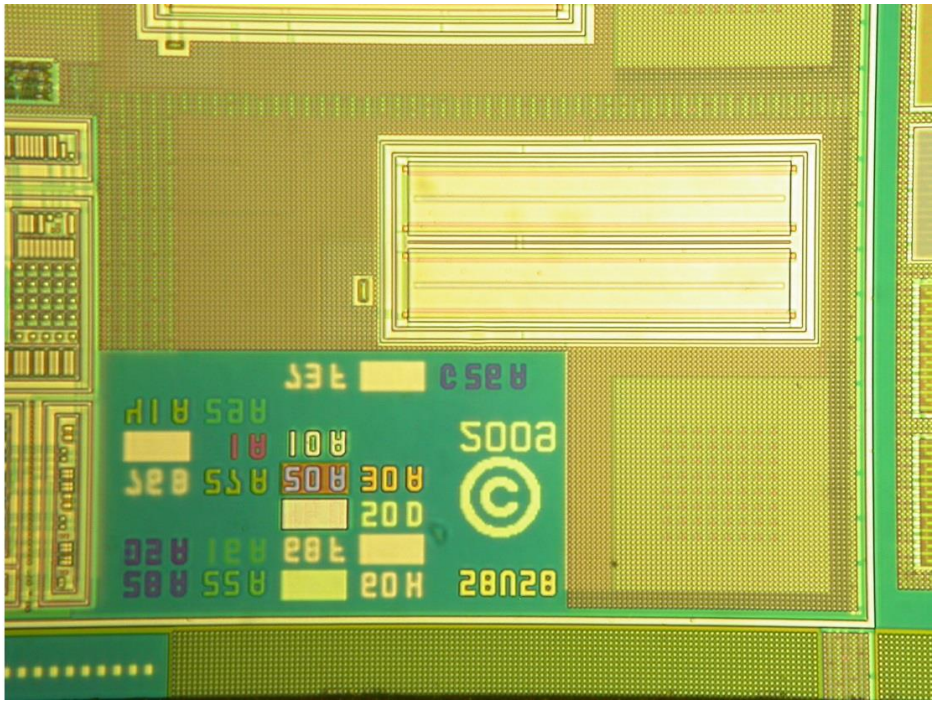


- initio INIC-3861EN, Kingston EMMC04G-M627, iStorage IST61273Q

iStorage Datashur Pro2 teardown

- iSTORAGE IST61273Q die marking: 58U58
  - Atmel device

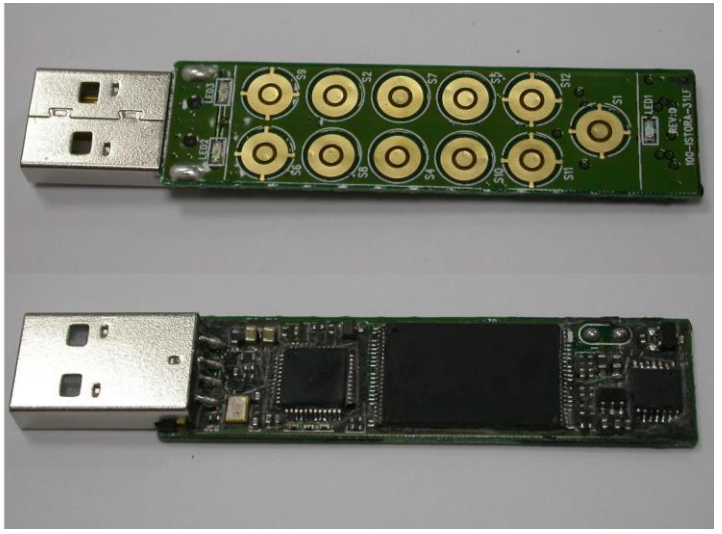




iStorage Datashur teardown

- Metal case is easy to open: remove the cap and slide

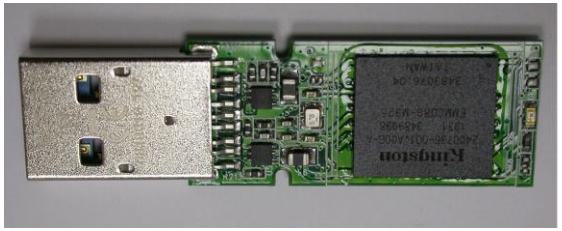

- Epoxy was removed using chemical method

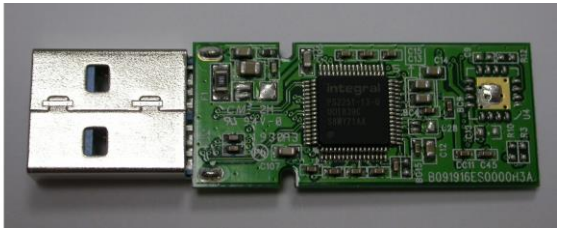



- initio INIC-1861L, Micron 29F32G08CBACA, L1825 (PIC16)

Integral Crypto and Courier teardown

- Cases are easy to open and epoxy in Crypto was chemically removed

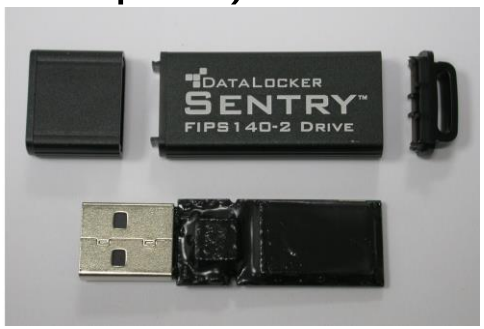


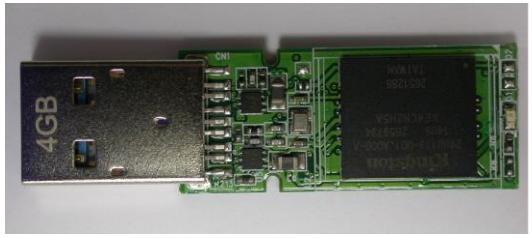


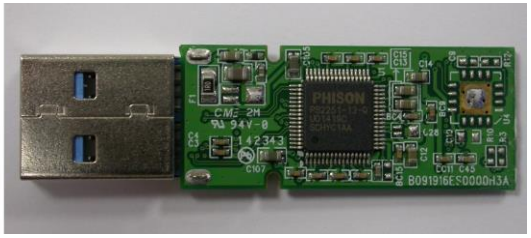
- PHISON PS2251-15-Q, Kingston EMMC08G-M325, space for QFN16
- PHISON PS2251-13-Q, Kingston EMMC08G-M325, space for QFN16

DataLocker Sentry 3.0 and Sentry teardown

- Cases are easy to open and fake epoxy in Sentry (black paint)



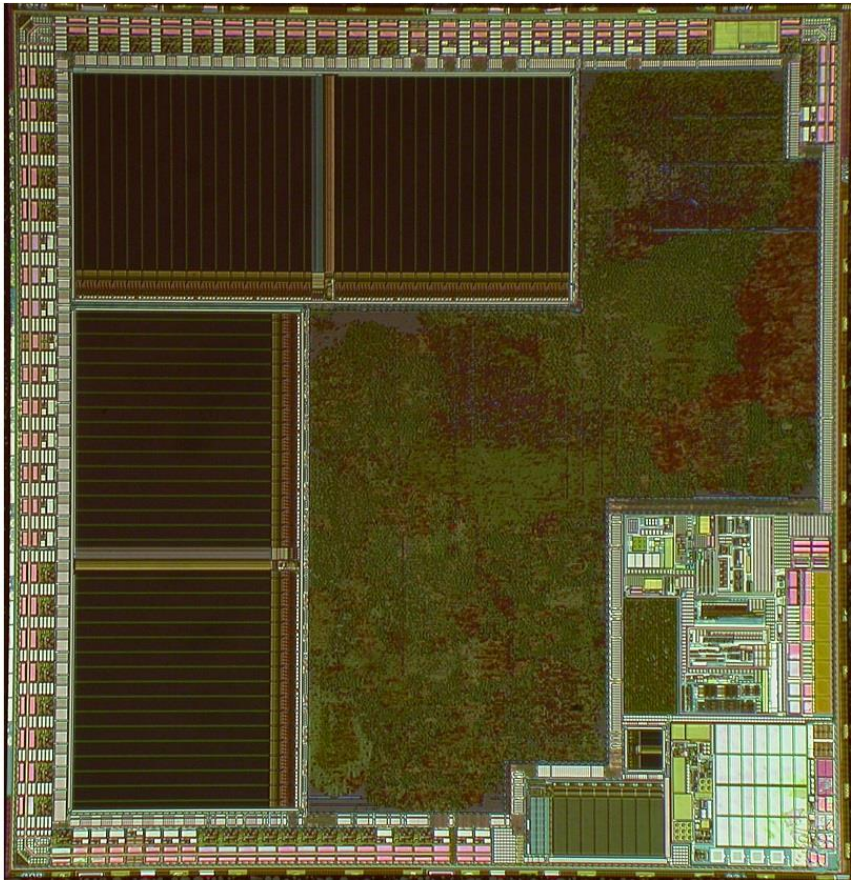




- PHISON PS2251-13-Q, Kingston KE4CN2H5A, space for QFN16
- BLOCKMASTER BM9931, TF15G2GAFA

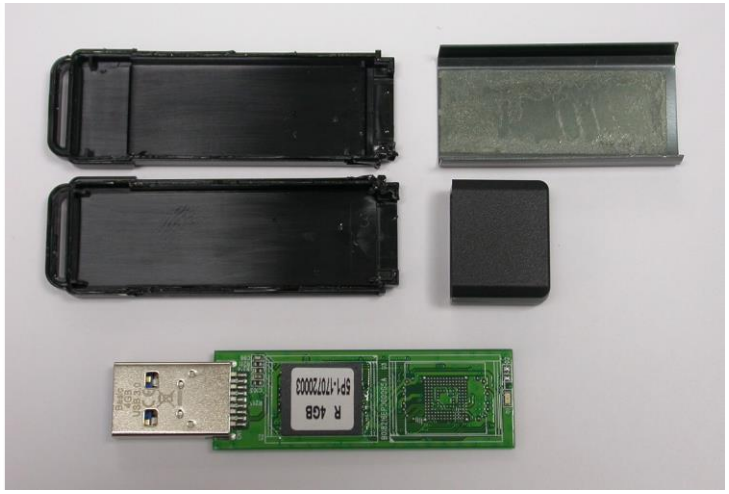
DataLocker Sentry 3.0 and Sentry teardown

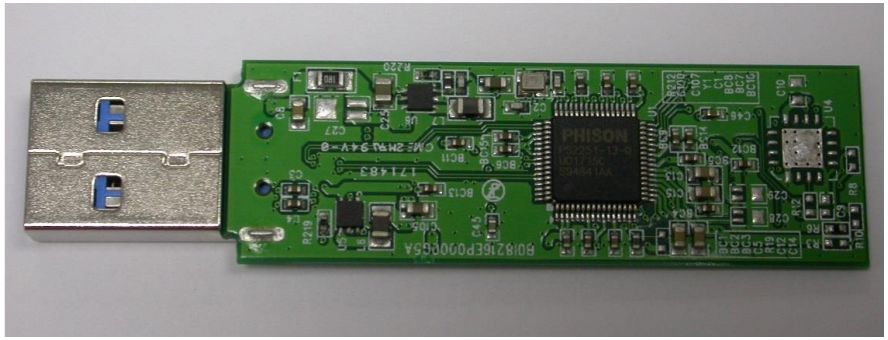
- BLOCKMASTER BM9931 has no die marking
  - custom device with Mask ROM and SRAM



SafeXS Protector teardown

- Case is easy to open and no epoxy inside

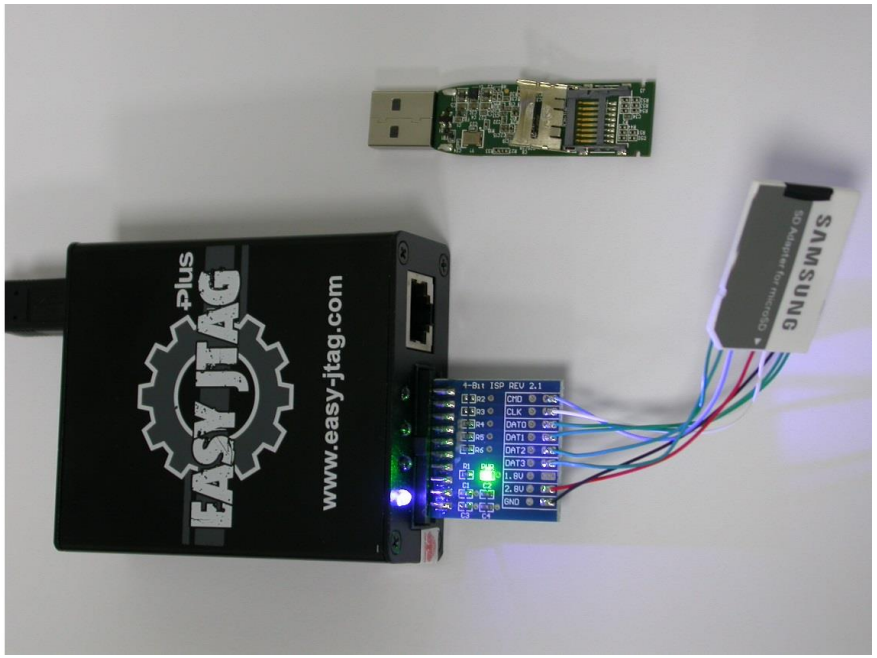




- PHISON PS2251-13-Q, Kingston EMMC04G-M627, space for QFN-16

IronKey F150 evaluation

- Two types of Flash storage: serial SST 25VF040B and microSD cards
  - no changes in serial Flash when incorrect passwords are entered
  - restoring the image of rear microSD card back reinstates the number of attempts
- IronKey F150 is vulnerable to NAND mirroring attacks

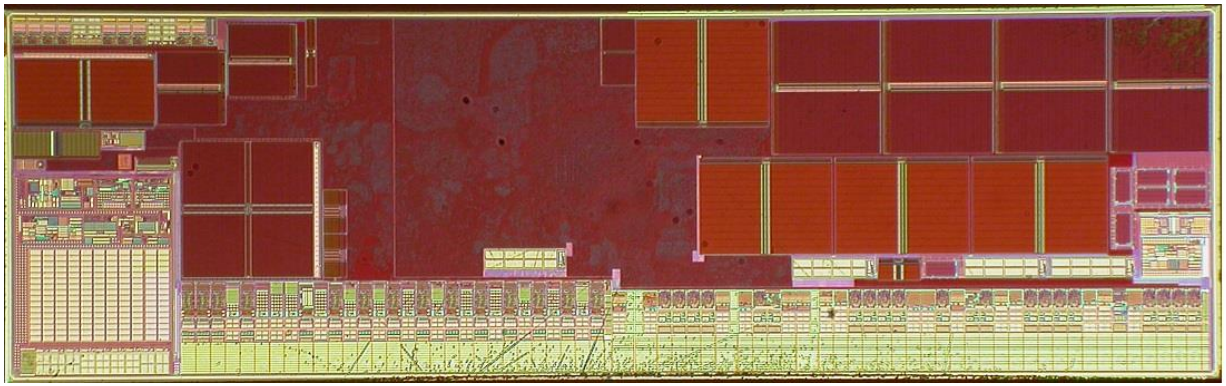


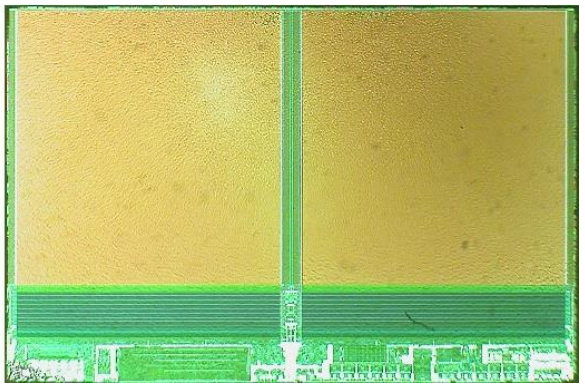
IronKey D80 evaluation

- Flash storage: Micron 29F32G08CBACA
  - restoring the image of NAND Flash back reinstates the number of attempts
- IronKey D80 is vulnerable to NAND mirroring attacks

eMMC evaluation

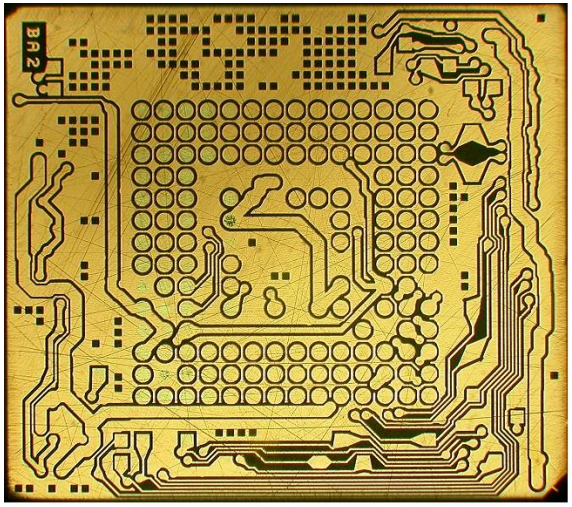
- eMMC chip has specialised controller and NAND Flash inside BGA
  - communication according to JEDEC standard
  - performs error correction and wear levelling
  - manages low level partitioning into multiple storage devices
- eMMC security
  - password protection
  - Replay Protected Memory Block (RPMB) partition
    - OTP symmetric authentication key with randomised challenge-response protocol
    - any write access increments dedicated write counter to prevent unauthorised overwriting

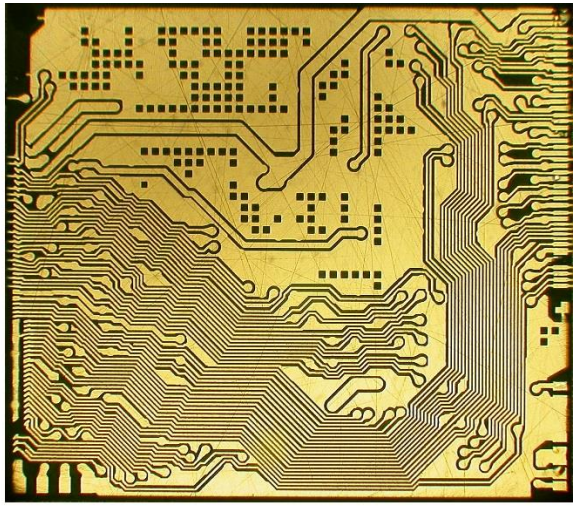


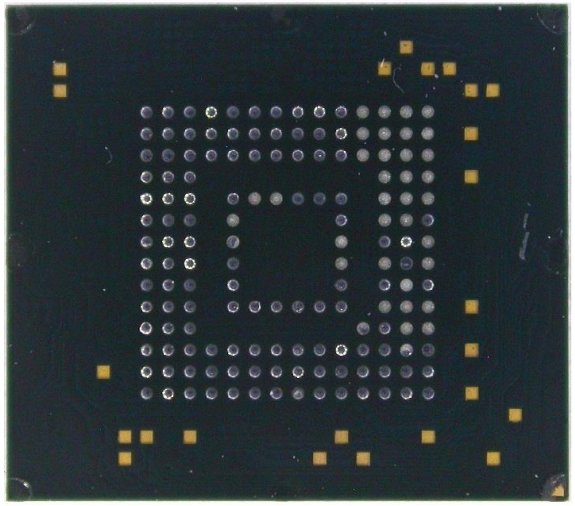


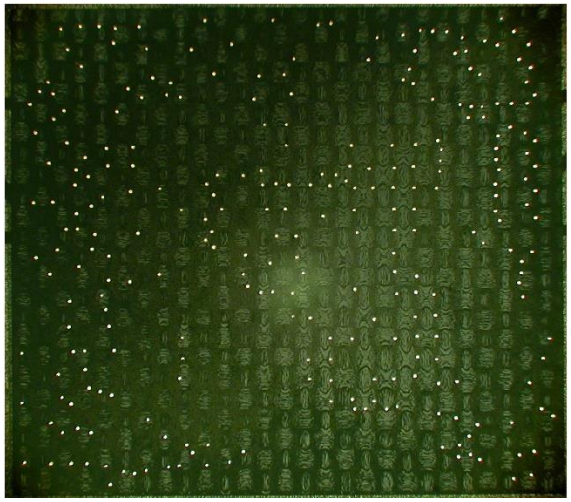
eMMC evaluation

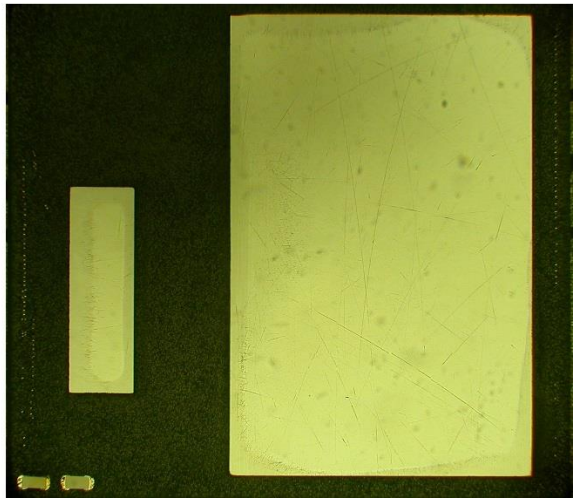
- eMMC layout





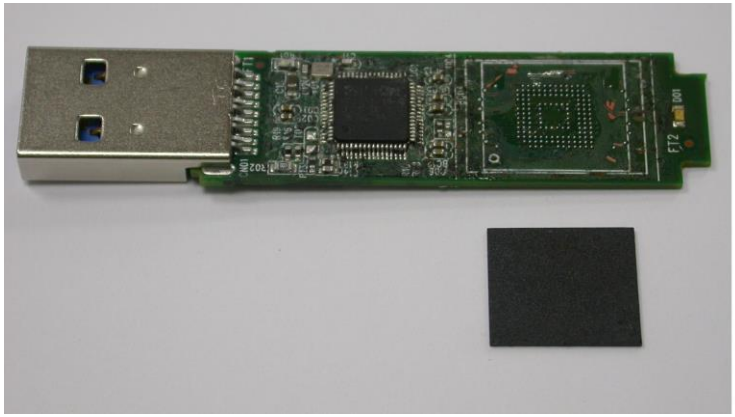
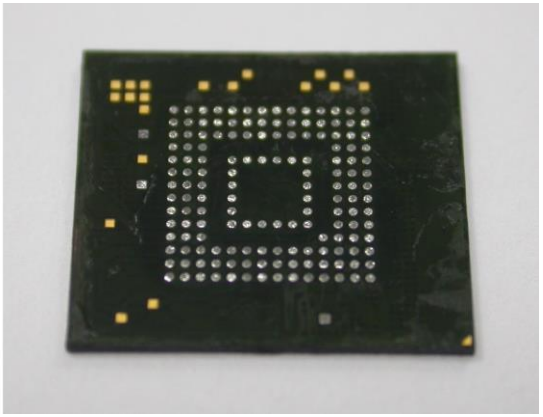
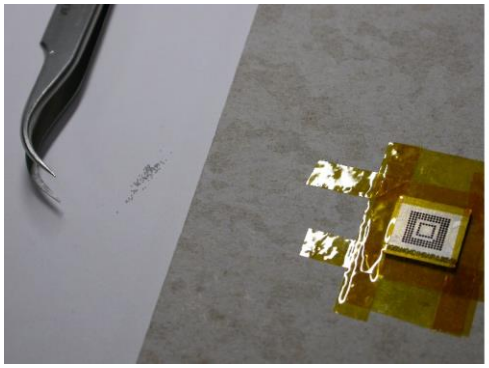
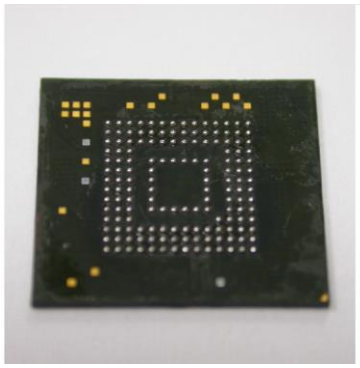
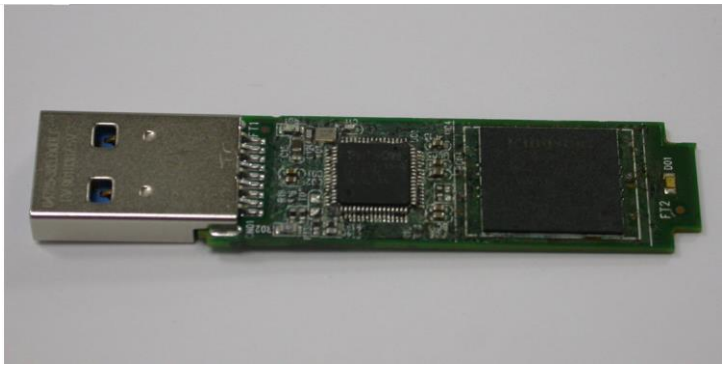






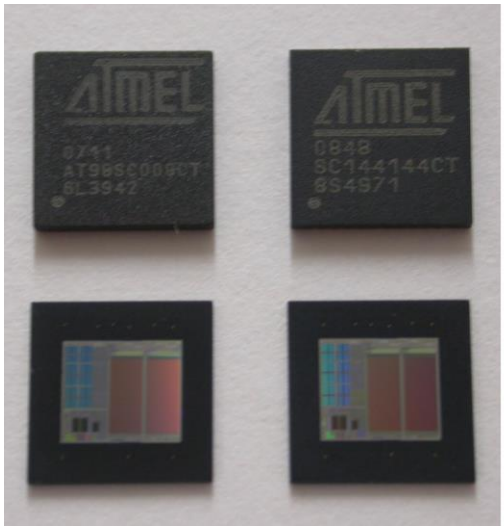
IronKey D300/D300S evaluation

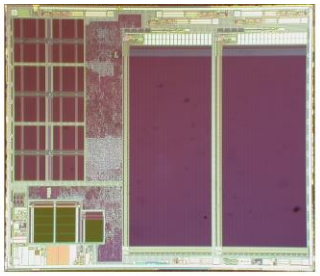
- eMMC chip: Kingston EMMC16G-TB28
  - de-soldered, re-balled and soldered back after reading/writing in EASYJTAGplus
- IronKey D300 and D300S are identical to Kingston DT4000G2 and vulnerable to NAND mirroring attacks

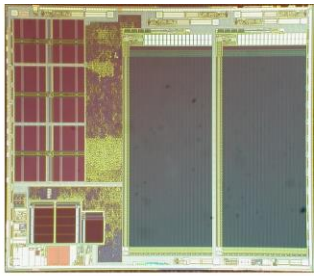






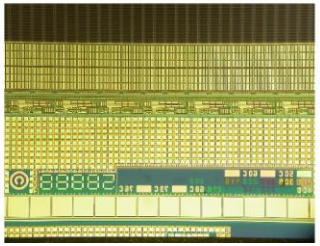
Atmel secure chips evaluation

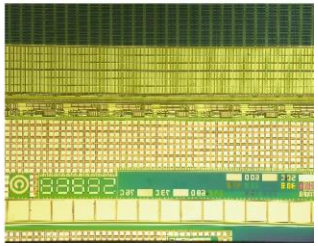
- AT98SC008CT die marking is the same as AT90SC144144CT: 58888
- AT98SC016CU die marking is the same as AT90SC12818RCU: 58U14

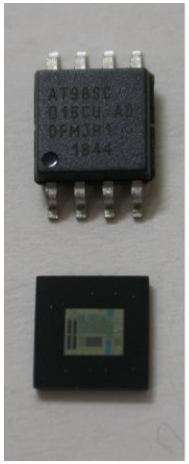


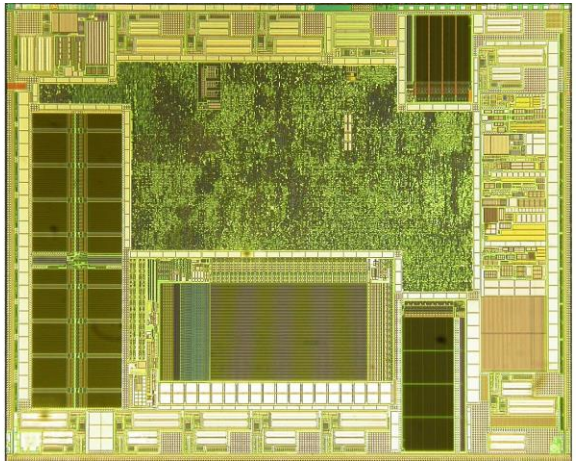


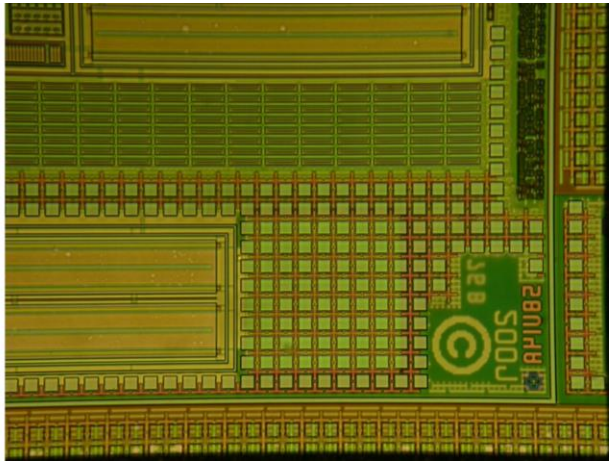






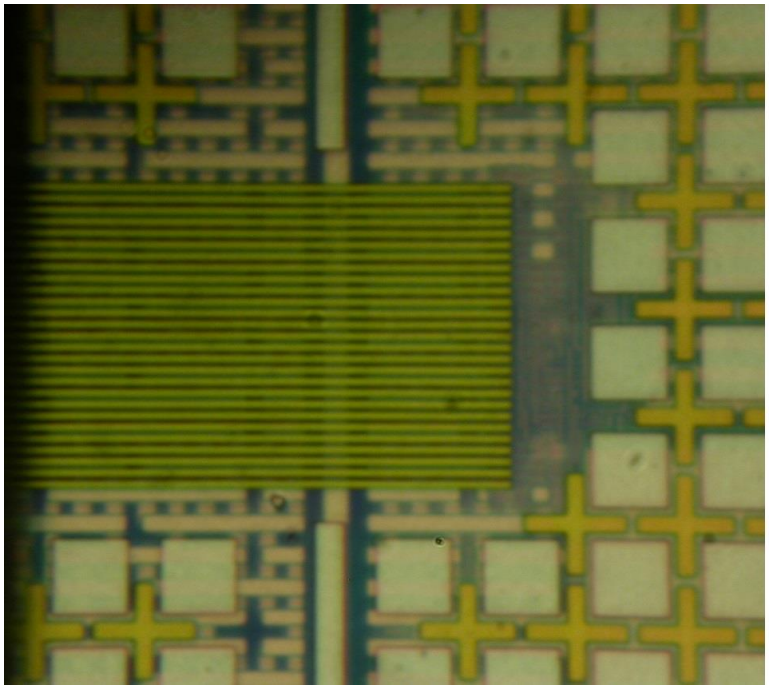


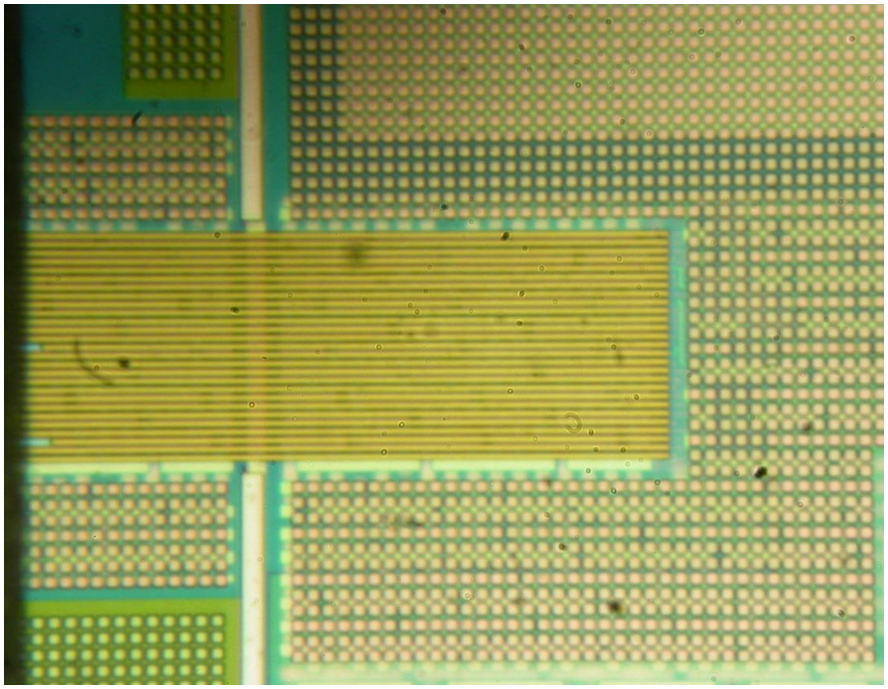




Atmel secure chips evaluation

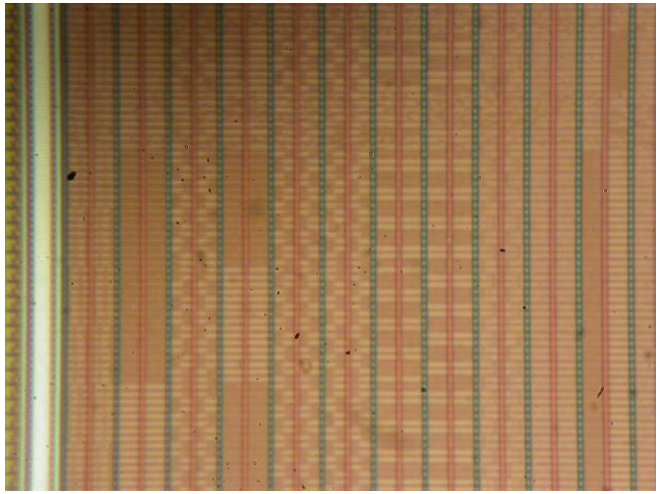
- Secure chip 31AV011 used in IronKey D250 and S1000
  - same die marking as AT90SC28872RCU: 58U07
- Secure chip iStorage IST61273Q used in Datashur Pro2
  - same die marking as AT90SO128: 58U58
- All AT90SC secure chips found in IronKey and iStorage
  - recognisable feature on the die – 27 wires going outside: factory debug (backdoor)

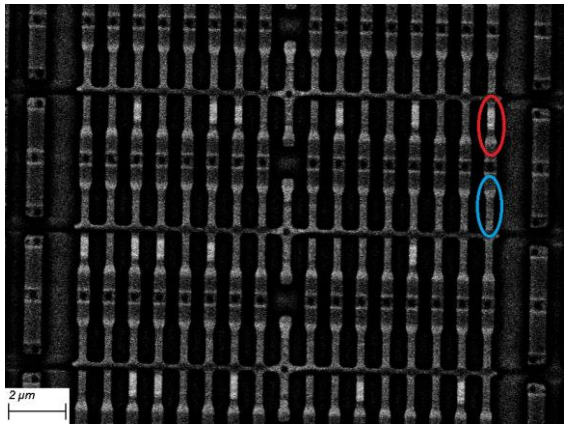


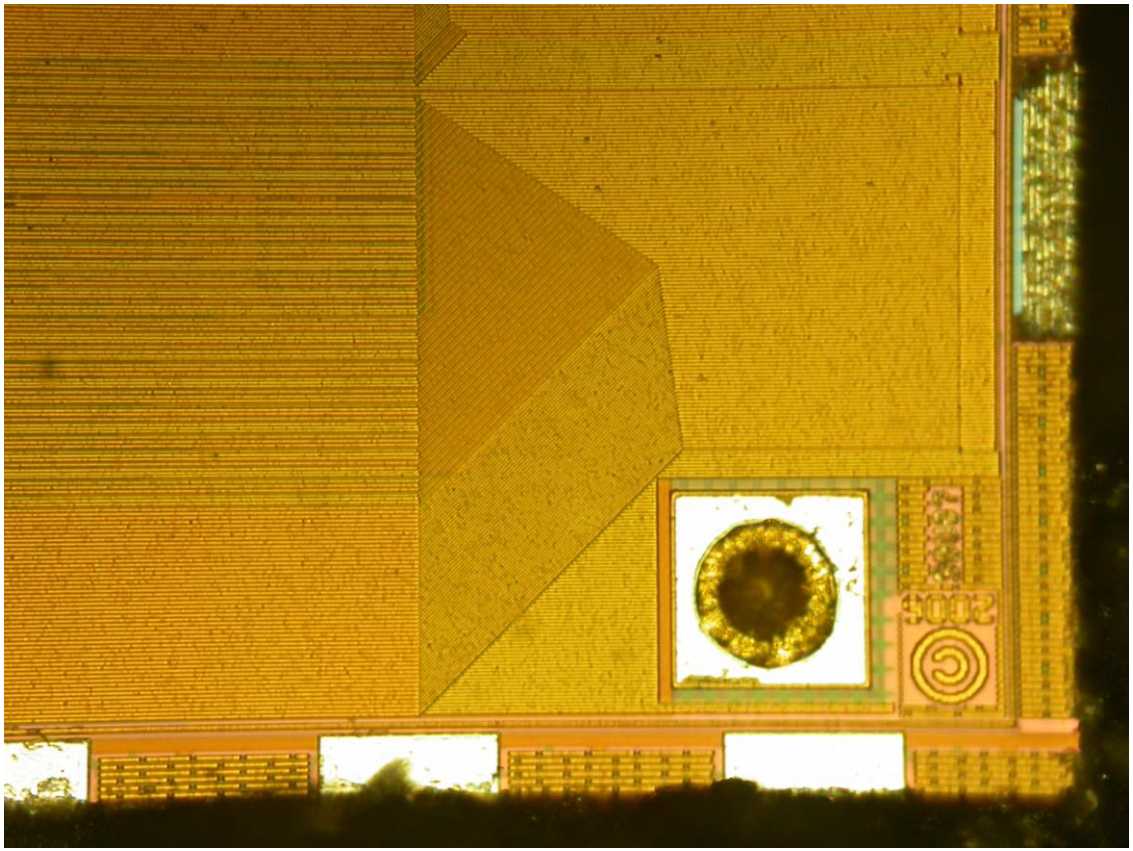


Atmel secure chips evaluation

- Mask ROM in many AT90SC devices is visible with optical microscope
- EEPROM can be extracted using SEM methods
- Top layer sensor mesh makes probing attacks more challenging

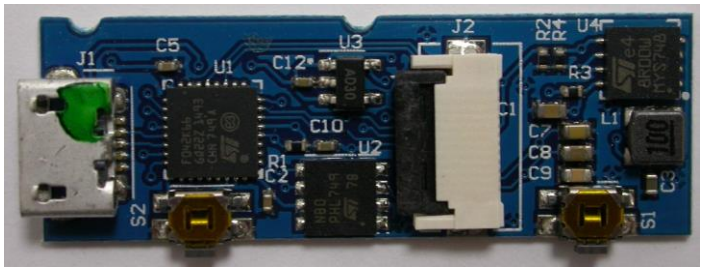


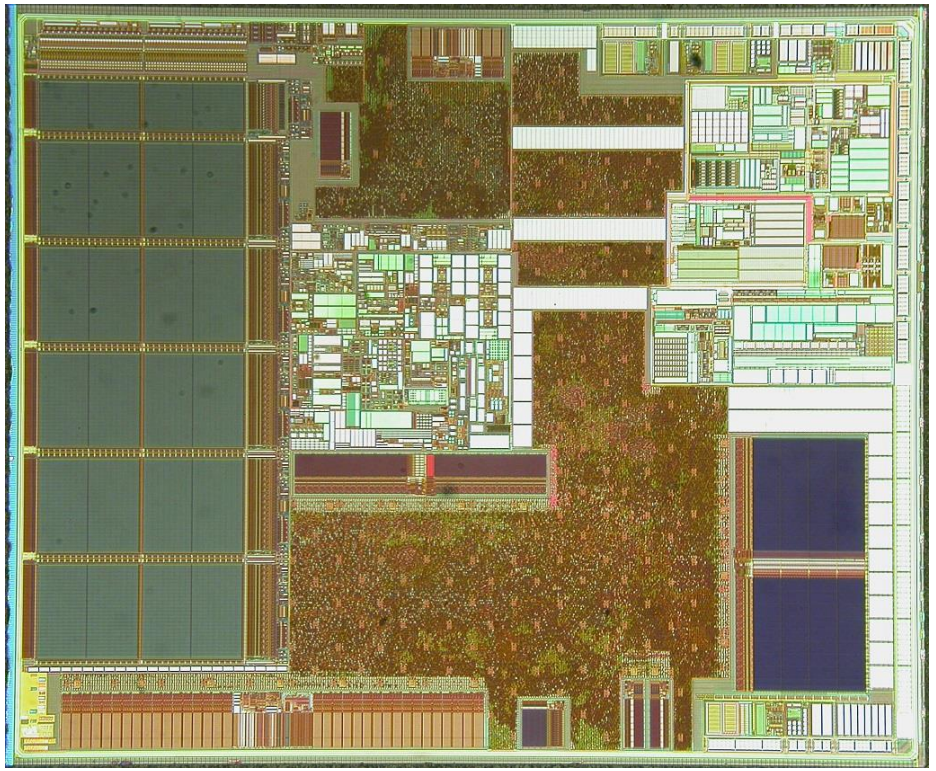




Ledger Nano S teardown

- Case is easy to open and no epoxy inside

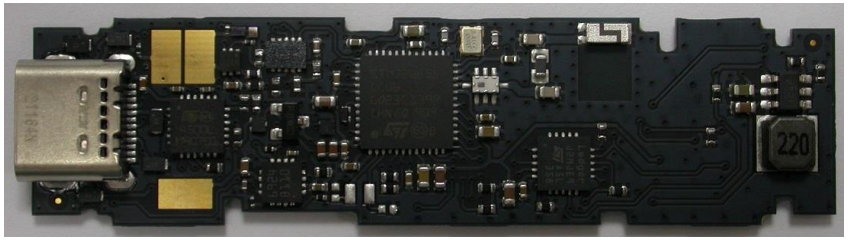


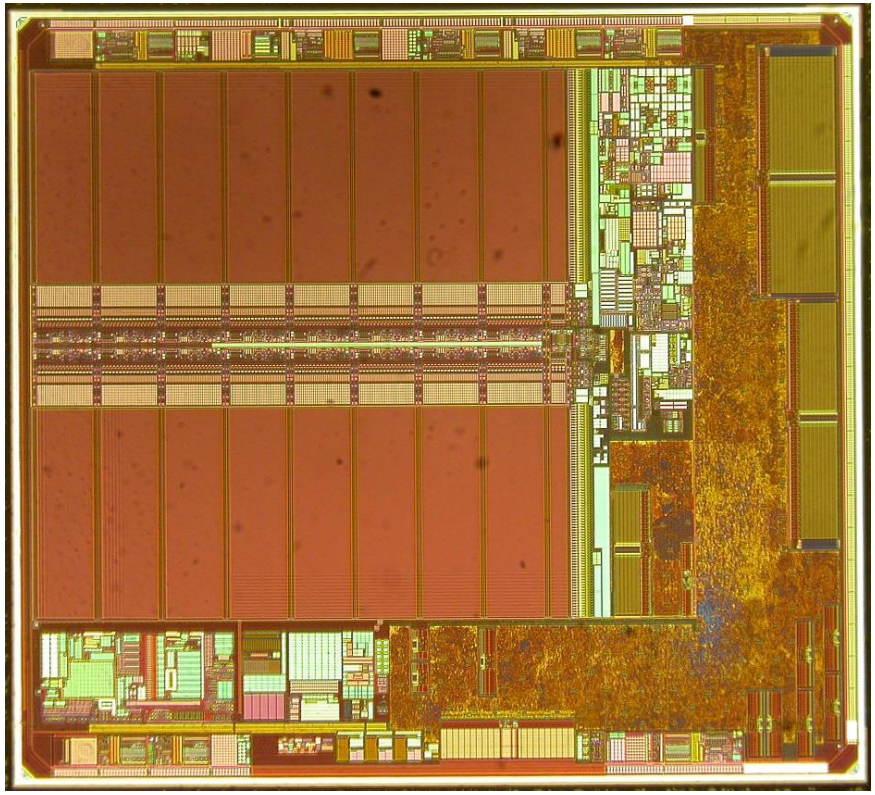


- Secure chip ST31H320, die marking: ST K8N0A 2014

Ledger Nano X teardown

- Case is easy to open and no epoxy inside





- Secure chip ST33J2M0, die marking: ST K500A 2015

Future Work

- Further details are in the paper: http://arxiv.org/abs/2110.14090
  - images of PCBs inside encrypted USB Flash drives
  - images of secure chips inside these devices
  - comparison table of encrypted USB Flash drives
- More research to be done for off-line password bruteforcing
  - understand how the AES key is encrypted with user password
  - understand how the number of password attempts are stored
  - emulate NAND or eMMC interface or simulate the controller operation
- If secure element is used for password and AES key protection
  - extract firmware from Mask ROM and descramble it
  - extract applications and data from EEPROM and descramble it
  - decompile the code and understand it
  - analyse backdoor interface on the die of AT90SC devices
  - perform various attacks on AT90SC devices

Conclusion

- Teardown process and results for 9 generations of IronKey devices
  - most devices have robust metal case filled with epoxy compound
  - secure chips were used in some old devices
  - latest models use eMMC Flash storage
  - 3 devices without secure chip are prone to NAND mirroring attack
- Teardown results on 15 encrypted USB Flash drives from 6 vendors
  - 7 devices have their PCB with epoxy filling, but none have full encapsulation
  - only 1 device have secure chip inside for AES key and password protection
  - some devices have battery but do not benefit from extra security (battery SRAM)
- FIPS 140-2 Level 3 certification does not guarantee hardware security
- None of the devices use inherited security features of eMMC Flash
- Atmel AT98SC family turned out to be programmed AT90SC chips
- AT90SC devices have silicon level factory debug interface (backdoor?)
- Cryptowallets are likely to have better hardware security than IronKey

Thank you!

Paper: http://arxiv.org/abs/2110.14090

URL: *http://www.cst.cam.ac.uk/~sps32*

email: *sps32@cam.ac.uk*