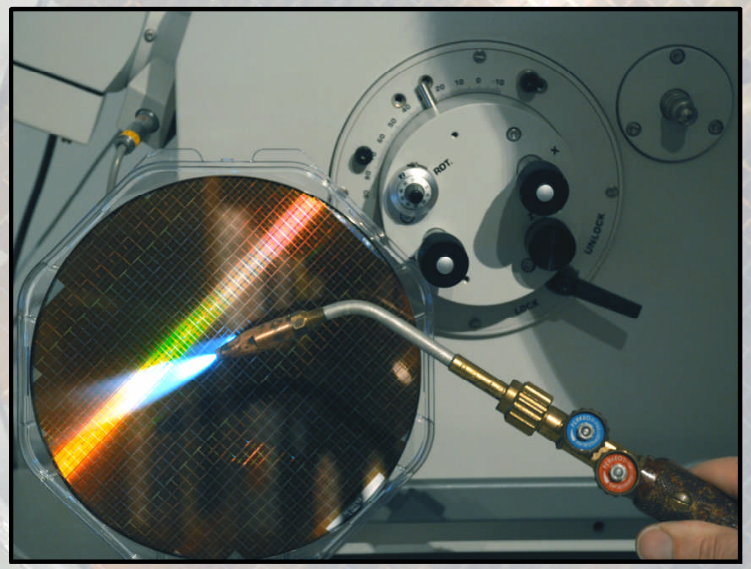
Uncaging Microchips

Techniques for Chip Preparation



Peter Laackmann
Marcus Janke

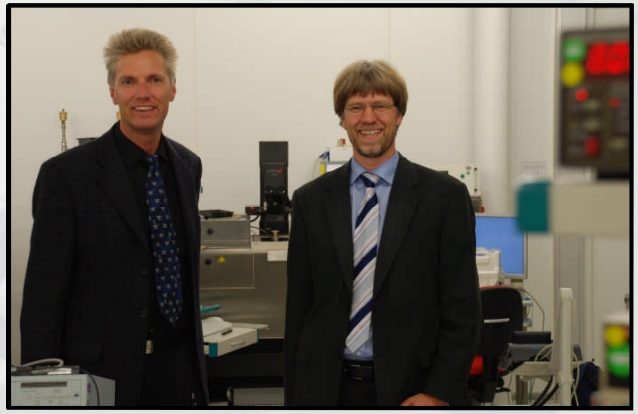
1989

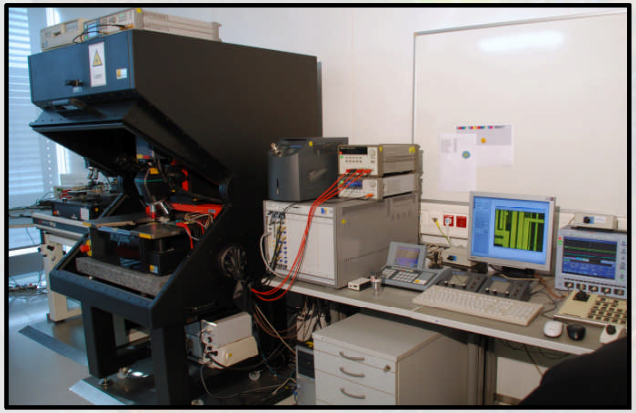
- Since 1989: Smart Card Research
- Brunsbüttel, Kiel, Hamburg
- Reverse Engineering
- Authors & Columnists during our study
- Consultancy for Data Protection/Privacy
- Privacy/Security weaknesses revealed:
  Health insurance card, ec-card, …
- Contacted by headhunter in 1999

Pictures: Private Archive M.Janke, P.Laackmann

2014

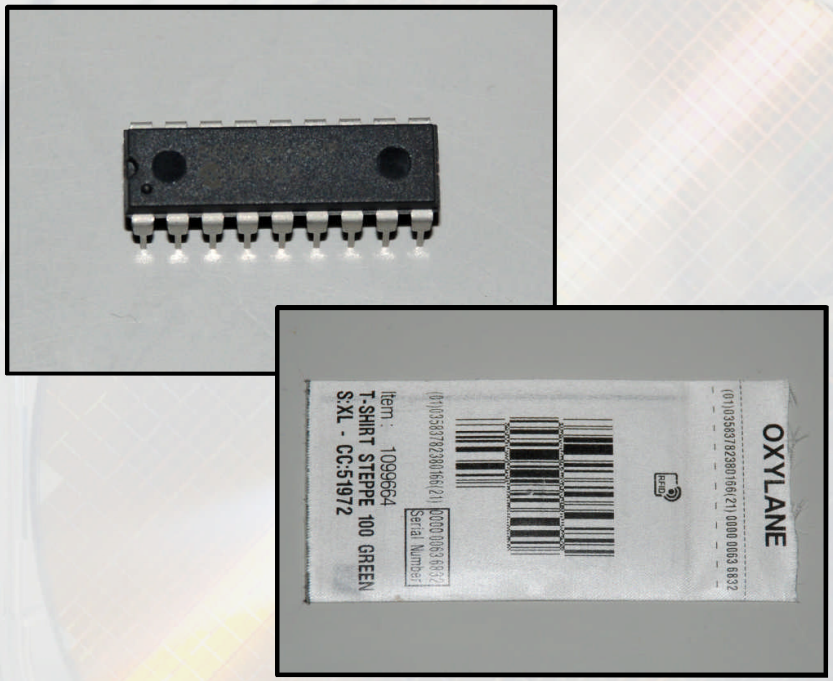
- Since 1999: Working with Infineon
- Munich
- Chip Security (Operational&Strategic)
- Leading the internal „hacker“ group
- Development of new attacks for threat anticipation
- Amateur attack projection
- Private security research ongoing…





Pictures: M.Janke/P.Laackmann (Infineon)

Why Should We Open Microchip Packages ?



ANALYSIS

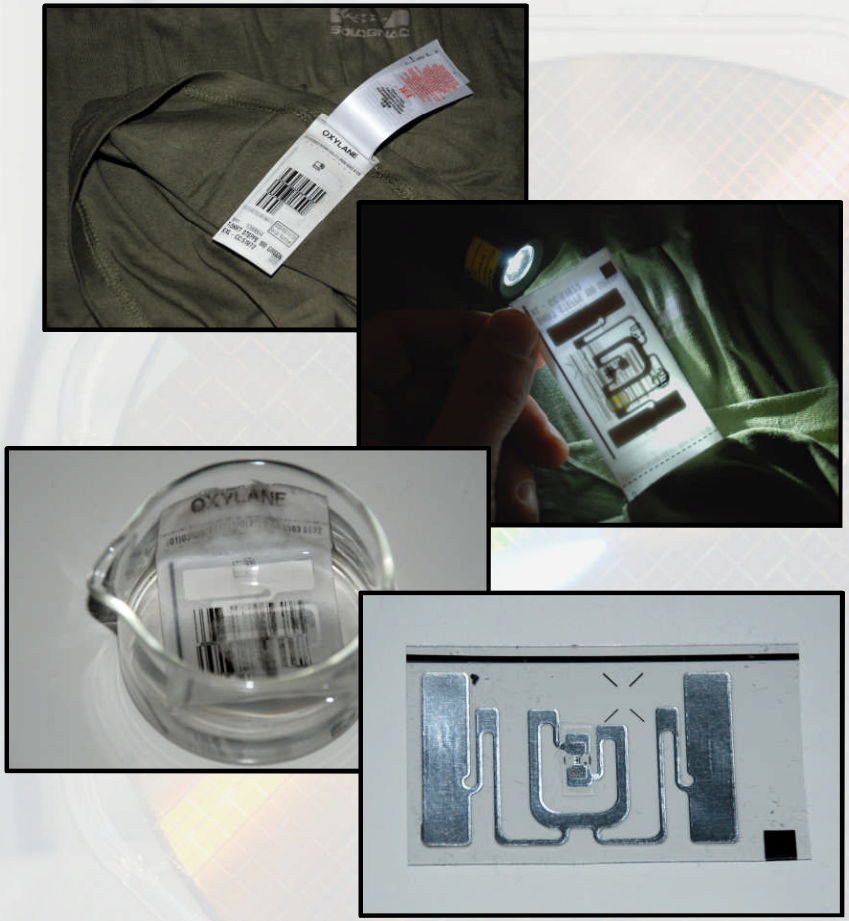
- Is there a chip in the package, anyhow ?
- Check chip functionality – what's the chip's task ?
- Determine the chip type – are literature, tools available ?
- Identify its technology generation – how old is the chip ?
- What is the value of the chip's function for the system ?

ATTACK PREPARATION

- For further reverse engineering tasks
- For laser fault injection attacks
- For UV fuse bit (code protection) erasing
- For permanent manipulations (e.g. FIB, Lasercutter)
- For alpha radiation fault injection attacks
- For photon emission side-channel analysis
- For local electromagnetic attacks

Pictures: Private Archive M.Janke, P.Laackmann

Why Should We Open Microchip Packages ?



CASE “TShirt” (2014)

- Attached to the shirt, an unusually bulky label was found
- Inspection with flashlight revealed hidden antenna
- Is an RFID chip with memory and ID present ?
- Or is it just a simple theft prevention mechanism ?

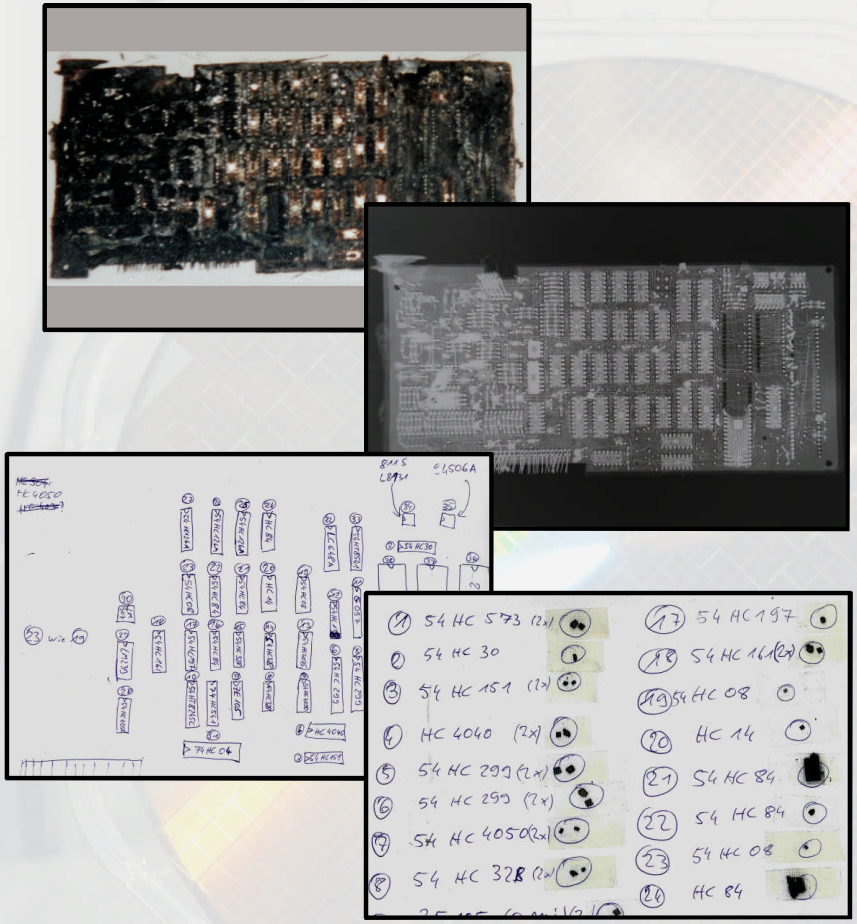
ANALYSIS

- Complete label is treated with acetone
- Carrier with chip and antenna could be extracted
- The microscope reveals a dark spot inside the antenna
- The chip is an RFID, communicating in UHF range

→Prepared for further analysis

Pictures: Private Archive M.Janke, P.Laackmann

Why Should We Open Microchip Packages ?



CASE "Cardphone (Kartentelefon)" (1990)

- Circuit board from burnt-down cardphone was found
- Chip's markings were destroyed and not readable
- Two chips were desoldered as an impact of fire
- Majority of conducting paths were still intact
- What were the tasks of this circuit board ?

ANALYSIS

- X-ray for reconstruction of printed wiring connections
- All chips were opened mechanically
- Chip markings on silicon were read under a microscope
- Schematics on module level were reconstructed

→ Main functions were resolved

Pictures: Private Archive M.Janke, P.Laackmann

Why Should We Open Microchip Packages ?

CASE “DOTWIN” (2001)

- 50 Mio pieces distributed for price competition
- Cardboard circles, must be attached to TV screen
- Dedicated shows were mandatory to watch
- Afterwards, circles had to be sent back
- Internet rumour: “Spy chip inside !”

> wird der Benutzer aufgefordert, den Dotwin während einer bestimmten Sendung an die Oberfläche seines Fernsehbildschirms zu kleben. Durch das Licht aus der Bildröhre wird ein elektronischer Chip im Innern des Dotwins aktiviert, der von diesem Augenblick bis zum Ende der Sendung Unmengen von Informationen sammelt. Gesteuert wird der Dotwin von einem CC128-A4 Controller, entwickelt von der

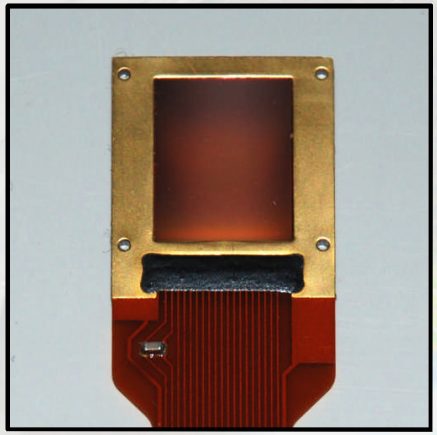
ANALYSIS

- No chip inside
- Light-sensitive film layer behind dot mask
- “Mandatory” shows displayed bright dots on TV screen

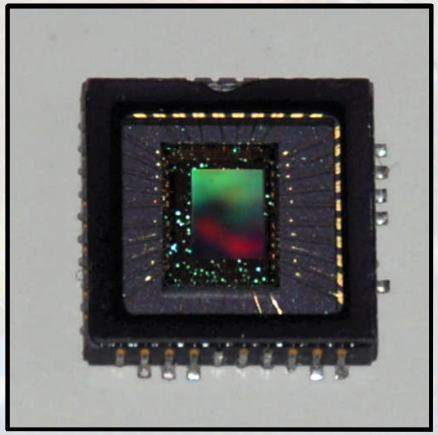
→ Spy-chip rumours were identified as “hoax”

Pictures: Private Archive M.Janke, P.Laackmann

Chip-Packages: From “Open” to “Armored” (1)



Fingerprint Sensor
The chip surface is directly touched with a finger.



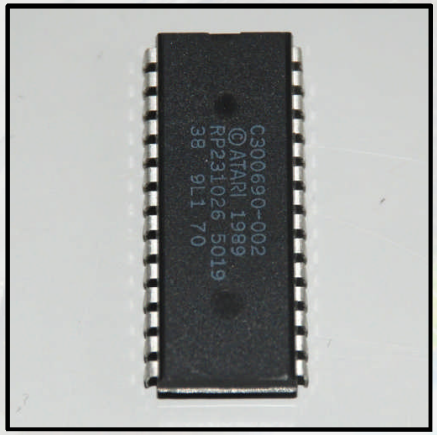
Webcam Chip
The chip surface is covered with thin optical glass.

EPROM
The chip is protected by a UV-transparent silica window.

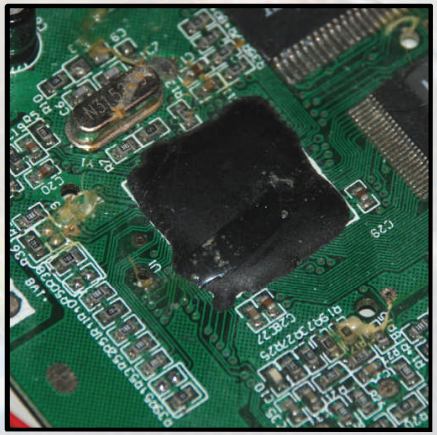
Amplifier Chip
The chip is covered and sealed with a metal lid, soldered to the package.

Pictures: Private Archive M.Janke, P.Laackmann

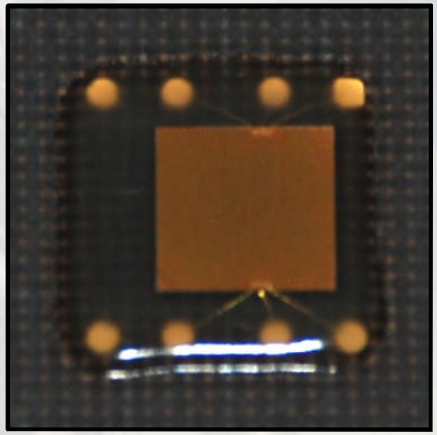
Chip-Packages: From “Open” to “Armored” (2)



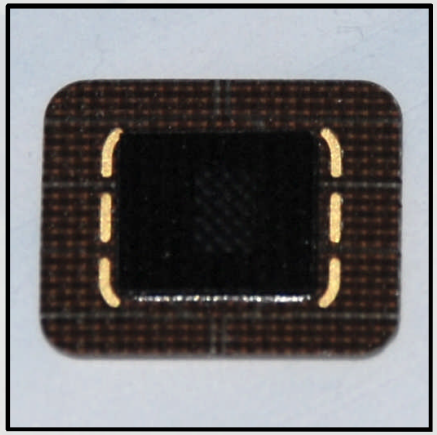
Plastic Package
The chip is fitted into an epoxy package.
Used very often today.



Glob-Top Package
The chip is covered with epoxy resin directly on the circuit board.



Smart Card Package
The chip is stabilized with a glass fibre mat and protected with epoxy.

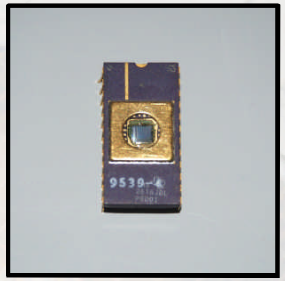


“Security” Package
The chip is encased using additional protective materials.

Pictures: Private Archive M.Janke, P.Laackmann

Close-Up Views – E(E)PROM

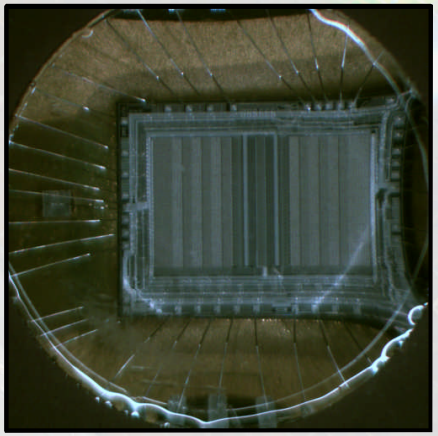
8755
2 kBit EPROM
with I/O Ports
(1976)

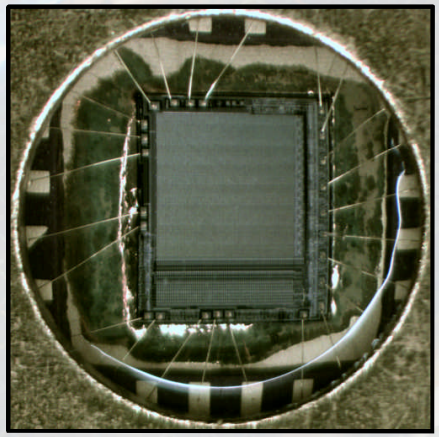


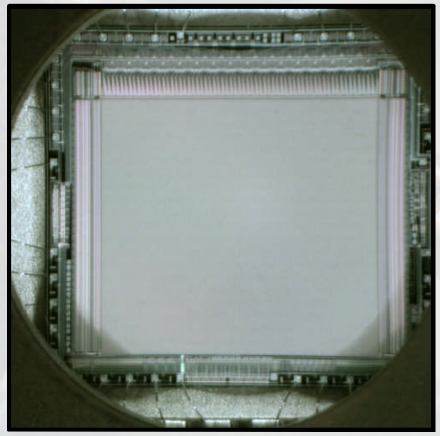
2516
16 kBit EPROM
Standalone
(1979)

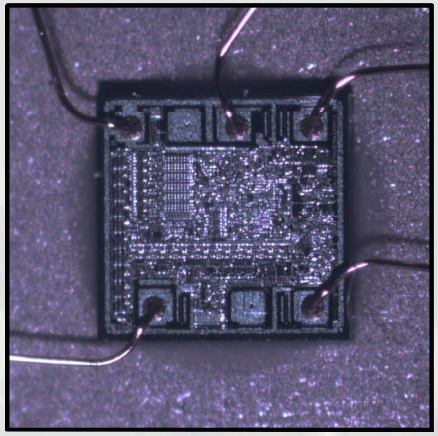
27C1024
1 MBit EPROM
Standalone
(1988)

SLE4406
88 Bit EEPROM
with logic functions
(1999)







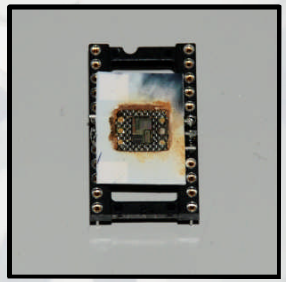


Pictures: Private Archive M.Janke, P.Laackmann

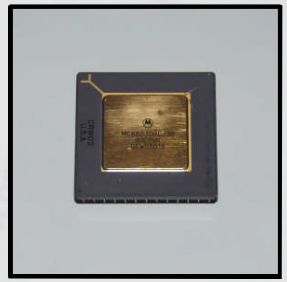
Close-Up Views – MCU (Microcontroller)

8748
8-Bit MCU
with 1 kB EPROM
(1976)

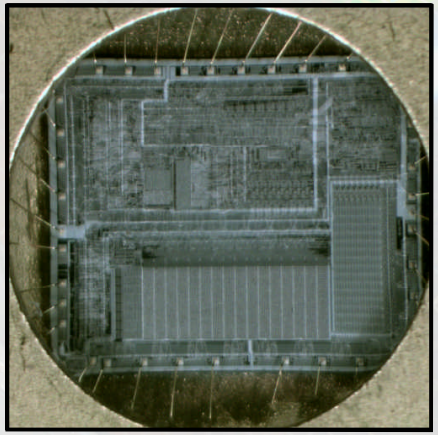
PIC16C55
8-Bit RISC MCU
with 512 Byte EPROM
(1988)

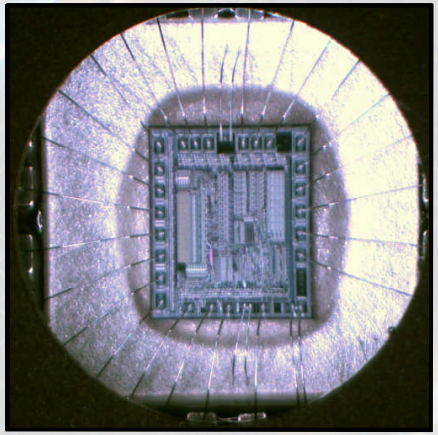


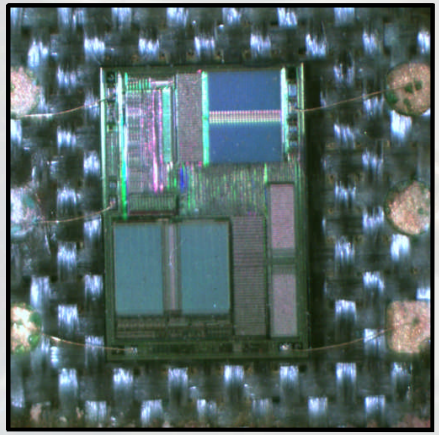
P83C855
8-Bit MCU
for Smart Cards
(1996)

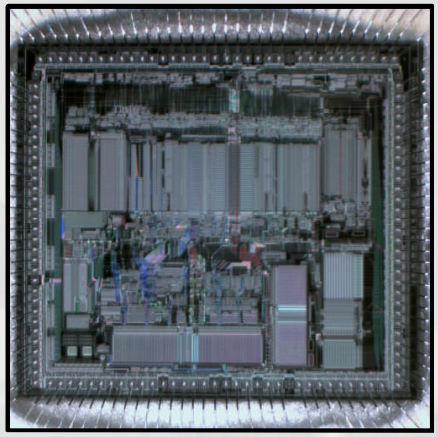


68030
32-Bit CPU
with 256 Byte Cache
(1987)



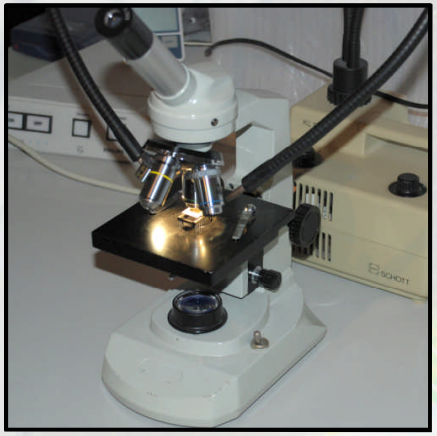






Pictures: Private Archive M.Janke, P.Laackmann

First Equipment Set-Up



Simple microscope
New: about 300 Euro
Used: from 50 Euro

Tools
New: about 20-50 Euro
Used: from 10 Euro

Ultrasonic cleaner
New: about 20-50 Euro
Used: from 10 Euro

Solvents
and glassware
New: about 20 Euro

Pictures: Private Archive M.Janke, P.Laackmann

Equipment Upgrade

Stereo microscope
New: about 1500 Euro
Used: from 250 Euro

Microscope camera
New: about 350 Euro
Used: from 150 Euro

Chemicals and glassware
New: about 50 Euro
Used: from 10 Euro

Lab coat, protective gear
New: about 50 Euro
Used: from 10 Euro

Pictures: Private Archive M.Janke, P.Laackmann

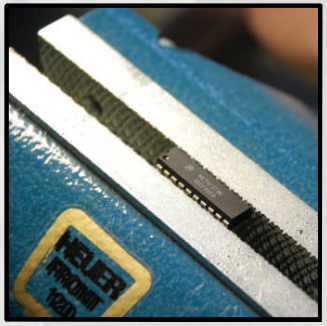
Package Opening Techniques – Overview

Physical
- Thermal release of the connection
- Thermal shock (use of thermal strain)
- Mechanical decapsulation (e.g. shear-off, milling, drilling)
- Laser material processing (ablation)

Chemical/Physical
- Disintegration by use of solvents
- Swelling (maceration) by diffusion of solvents into package
- Thermal decomposition of plastics

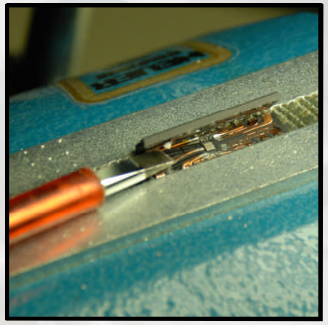
Chemical
- Material destruction with acids, lyes or oxidants
- Electrolytic methods

Package Opening Techniques – Physical

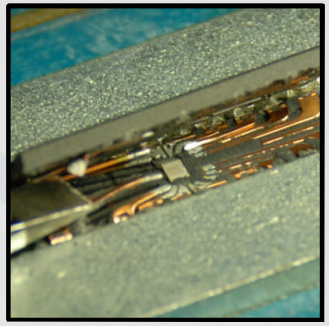


Lower part of chip
fixed in vise

Deformation, until
upper part is sheared off



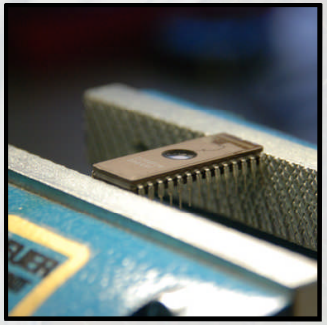
Plastic lid
is carefully removed



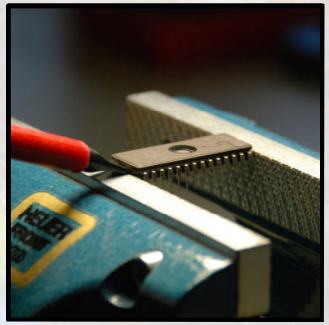
Open chip
with “Leadframe”

Pictures: Private Archive M.Janke, P.Laackmann

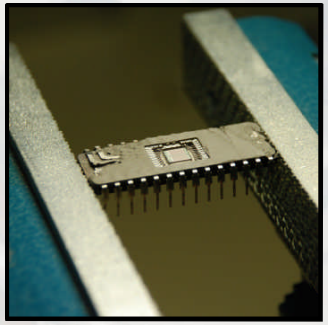
Package Opening Techniques – Physical



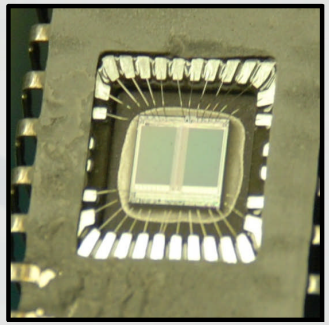
Lower part of chip fixed in vise



Screwdriver is set to middle of chip's package



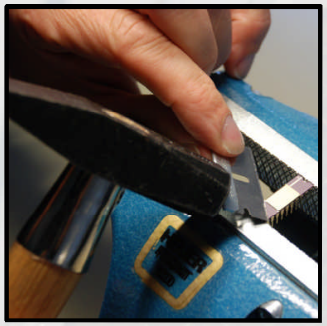
Upper part of the package is knocked off



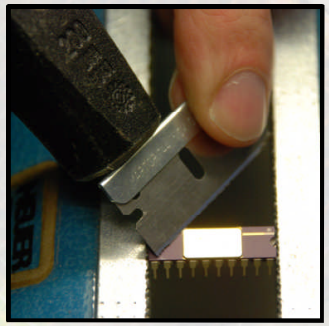
Open chip showing parts of "Leadframe"

Pictures: Private Archive M.Janke, P.Laackmann

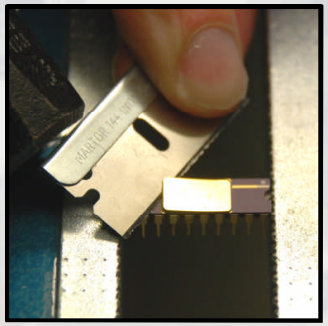
Package Opening Techniques – Physical



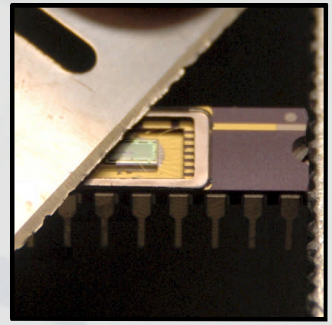
Blade is set to corner of chip's metal lid



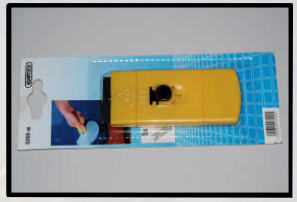
Hammer drives blade under metal lid

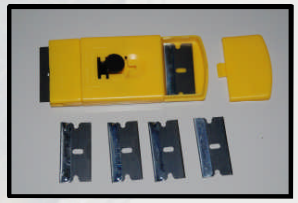


The lid is carefully lifted using blade



Chip has been completely opened



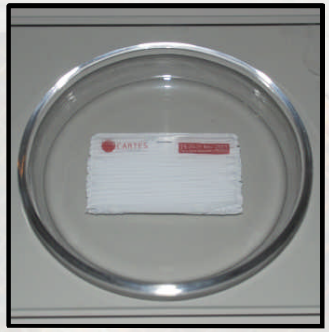


Source for blades: Cleaner for glass ceramic

Pictures: Private Archive M.Janke, P.Laackmann

Package Opening Techniques – Physical/Chemical

Smart card is covered with 50ml of acetone



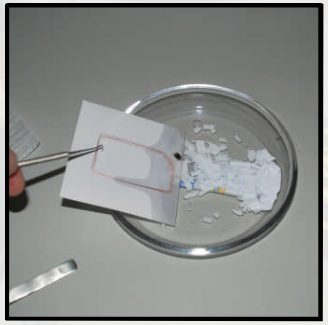
After 5 minutes: Card package swells

After 15 minutes: Structure fully decayed

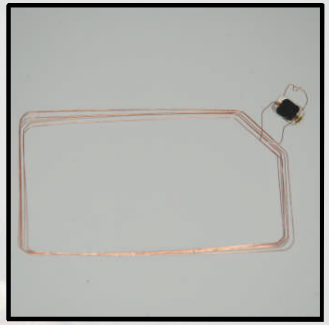
Plastic particles float around

Manual removal of particles

Chip and antenna are revealed



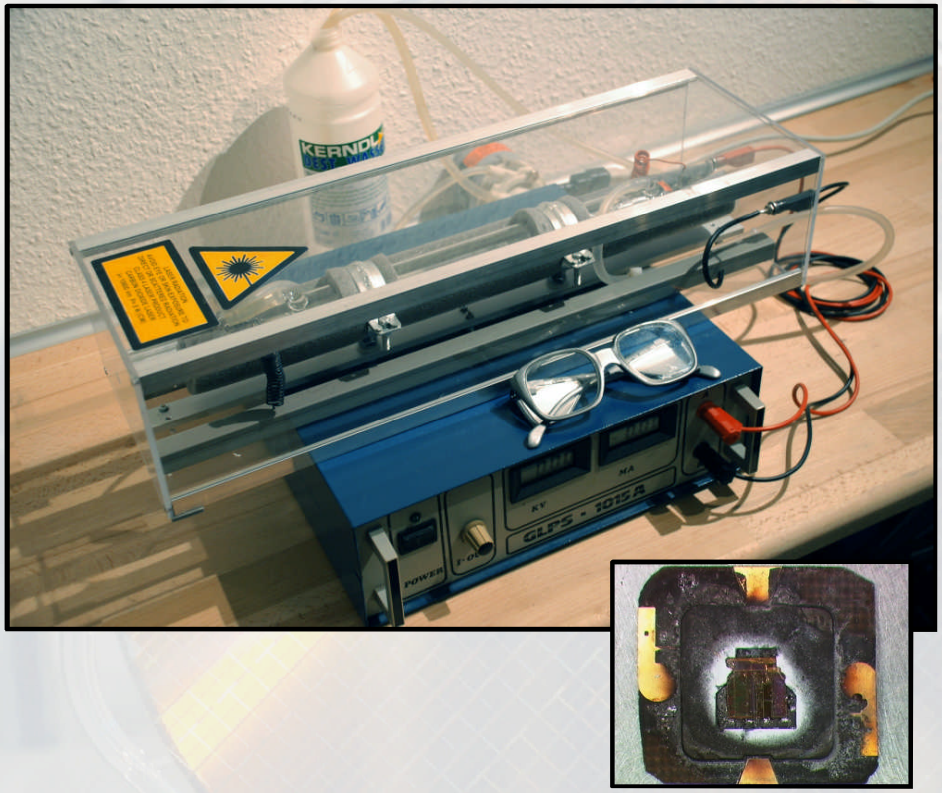
Chip with antenna extracted on paper



Chip with antenna completely dismantled

Pictures: Private Archive M.Janke, P.Laackmann

Package Opening Techniques – Physical/Chemical

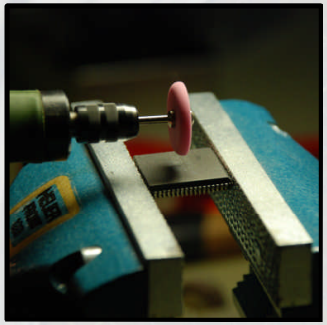


- CO_2 Laser tube (mass production in China)
- Infrared radiation 10600nm (10,6µm) wavelength
- Silicon is transparent, will not be heated up
- Package absorbs laser radiation and is decomposed
- For special targets (“Secure” Packages)

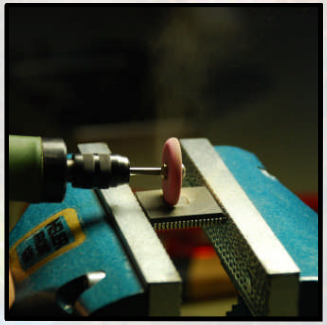
- Heat effects can destroy the chip inside
- Laser effects are not easy to control
- Local irradiation may cause severe thermal strain
- Invisible laser radiation is very dangerous

Pictures: Private Archive M.Janke, P.Laackmann

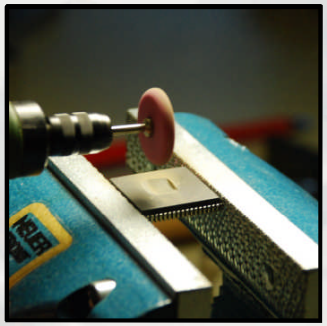
Package Opening Techniques – Preparation for Chemicals



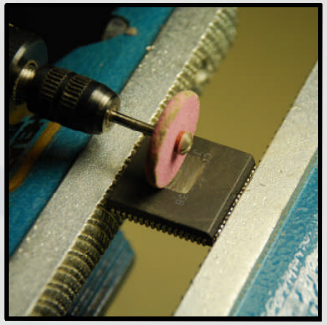
Chip has been fixed in vise



Grinding disk is positioned



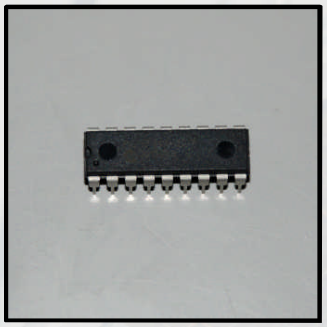
Parallel movement to create recess



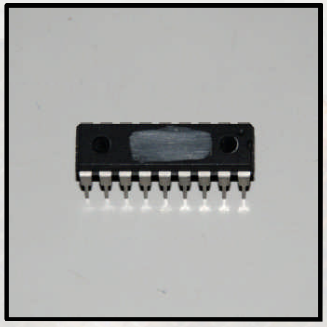
Finished recess ready for chemical treatment

Pictures: Private Archive M.Janke, P.Laackmann

Package Opening Techniques – Chemical



Chip in plastic package (PDIP)



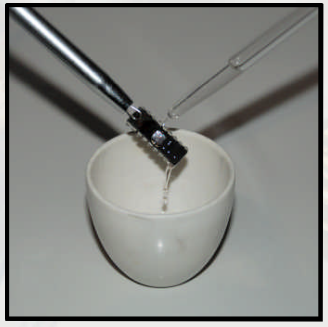
Recess is ground into chip

Chip is placed in heated laboratory sand bath

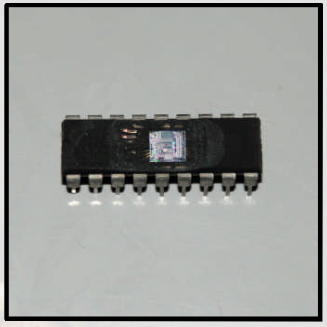
Nitric acid is dropped on chip at 50-90°C

Remains of acid are removed with acetone

Ultrasonic cleaner removes particles



Acetone treatment for rapid drying

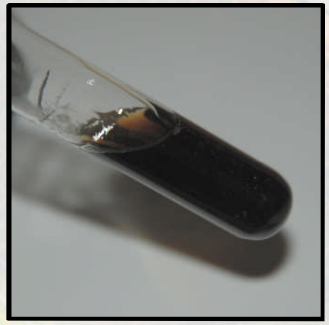


Chip is completely exposed

Pictures: Private Archive M.Janke, P.Laackmann

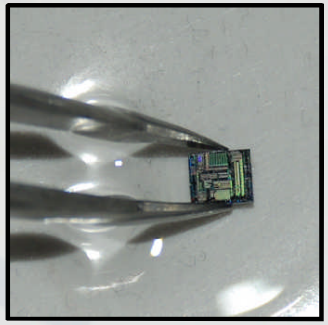
Package Opening Techniques – Chemical

Colophony is heated near to boiling point (250-350°C)



Chip package dissolves in heated liquid (5-20 min)

Chip is cleaned with acetone (40°C)



Extracted chip showing no acid damage

Colophony (German: Kolophonium) and Heatgun

Pictures: Private Archive M.Janke, P.Laackmann

Chemicals from Household Products

Chemicals	Use case	German name	Trivial name
Acetone	Dissolving Polystyrene, Polycarbonate	Aceton	Acetone (Aceton technisch)
(Cleaning-) Benzine	Dissolving glues and degreasing of surfaces	(Wasch-) Benzin	White Spirit (Wasch- oder Reinigungsbenzin)
Ethanol	Universal cleaning agent and solvent	Ethanol	Methylated Spirit (Brennspiritus)
Ethylene Glycol	Selective solvent e.g. to open paper tickets	Ethylenglykol	Antifreeze (Kühler-Frostschutzmittel)
Hydrofluoric Acid	Selective etching of chip-structures (depassivation)	Flußsäure	Rust Remover (Rostentferner)
Perchloroethylene	Dissolving/swelling of various plastics	Perchlorethylen	Stain remover (Fleckentferner)
Sodium Bicarbonate	Neutralization of acid remains and spills	Natriumhydrogen-Carbonat	Baking Soda (Natron)
Sodium Hydroxide	Dissolving paper glues, dissolving aluminum antennas	Natriumhydroxid	Drain pipe cleaner (Abflussreiniger „Ätznatron“)
Tensides	Ultrasonic cleaning (surface tension removal)	Tenside	Dishwashing agent (Spülmittel)
Tetrahydrofurane	Dissolving Polyvinylchloride (PVC) and other plastics	Tetrahydrofuran	PVC pipe/sheet adhesive and solvent (PVC-Schweißmittel/Anlöser)
Water Demineralized	For general rinsing, acid removal, ultrasonic cleaning	Wasser entmineralisiert	Distilled Water (Destilliertes Wasser)

Pictures: Private Archive M.Janke, P.Laackmann

Chemicals – Fuming Nitric Acid

Fuming Nitric Acid (HNO_3)

- Decomposition of all organic ingredients of the package by oxidation
- Water content of the acid must be as low as possible in order not to damage the chip
- Chemical trade: HNO_3 >99% for about 100-200 Euro / Litre (!)
- Alternative: DIY production under all protective measures

- Organic materials are destroyed within seconds
- Combustible materials can be inflamed at contact
- Fumes and reaction products can be highly toxic

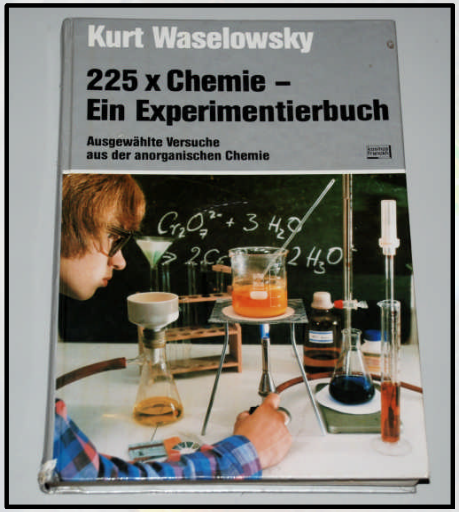
→Safety goggles/shield, appropriate (!) gloves, fume cabinet

Pictures: Private Archive M.Janke, P.Laackmann

Chemicals – Fuming Nitric Acid

DIY Production

- Reaction of potassium nitrate with concentrated sulfuric acid, then distillation
- Instruction can be found in older chemical science books for juveniles
- Typically, acid concentrations of >90% are reached, but not >99%



Science experiments book with instruction (1982)

Standard distillation apparatus

Micro distillation glassware

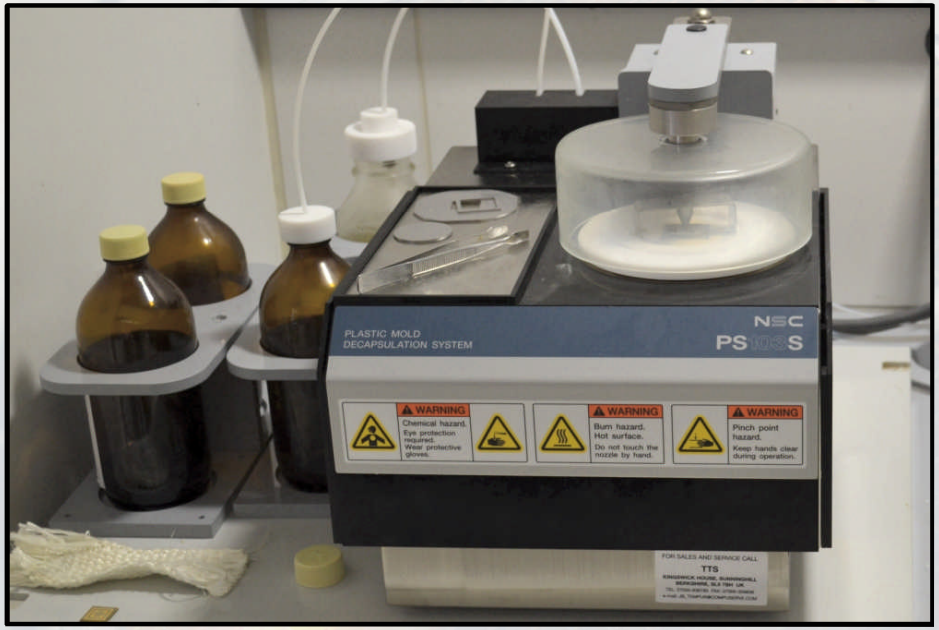
Pictures: Private Archive M.Janke, P.Laackmann

Chemicals from Professional Sources

Chemicals	Use case	German name	GHS hazard pictograms
Choline	Removal of silicones Cleaning agent for wafers, chips	Cholin	
Chloroform	Dissolving and swelling of epoxy compunds	Chloroform	
Colophony	Decomposition of epoxy package material (decapping)	Kolophonium	
Dimethyl formamide	Dissolving and swelling of epoxy compunds	Dimethylformamid	
Ethylene diamine	Removal of polyimides (chip protection layers)	Ethylendiamin	
Hydrazine hydrate	Removal of polyimides (chip protection layers)	Hydrazinhydrat	
Isopropyl alcohol	Water removal on chemically treated packages	Isopropanol	
Methylene chloride	Dissolving and swelling of epoxy compunds	Dichlormethan	
Nitric acid, fuming	Decomposition of plastic package material (decapping)	Salpetersäure rauchend	
Sulphuric acid conc.	Decomposition of plastic package material (decapping)	Schwefelsäure konzentriert	
Sulphuric acid „Oleum"	Decomposition of plastic package material (decapping)	Schwefelsäure „Oleum" rauchende Schwefelsäure	

Pictures: Private Archive M.Janke, P.Laackmann

Professional Methods – Chemical Decapsulator



- For decapsulation of plastic packages by etching
- Typically operated with fuming nitric acid
- Acid jetting method – acid is constantly renewed
- Chip structure is preserved, as reaction products like water and particles are immediately purged

- Consumption of acid is much higher than manual (dropping) method
- Waste acid must be disposed off properly (neutralized)
- Fumes must be neutralized or absorbed
- Operation costs can be quite high

Pictures: M.Janke/P.Laackmann (Infineon)

Professional Methods – CNC Milling Machine

- For pre-preparation of various packages, including ceramic housings
- Reproducible micrometer precision
- Standard CNC flows for standard packages available
- Machine can be programmed for special or new cases
- Ideal for complex situations (e.g. Multi-chip packages)

- Equipment is very expensive
- Operation is also expensive, if abrasive wear is high (e.g. with ceramic packages)
- Machine is very heavy !

Pictures: M.Janke/P.Laackmann (Infineon)

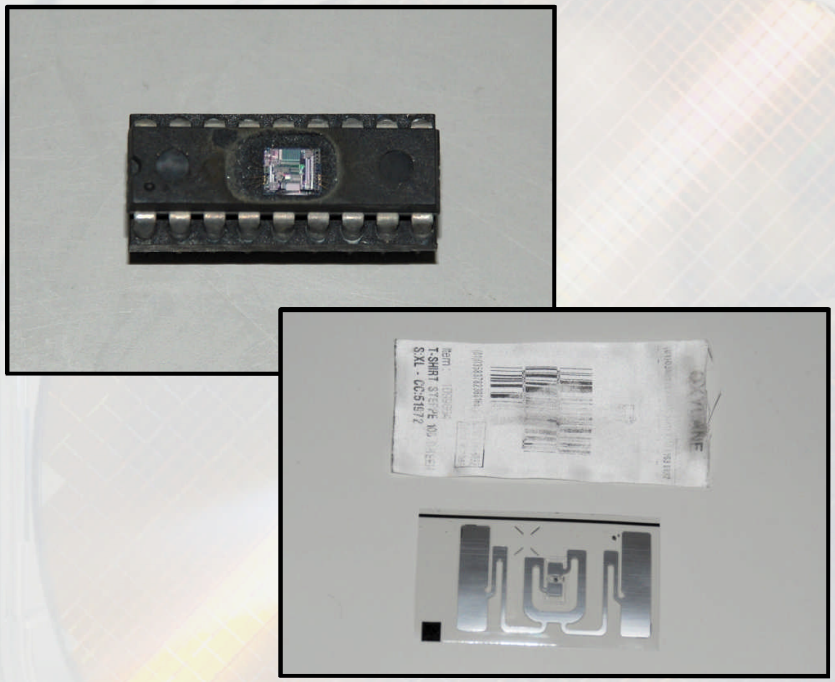
Professional Methods – Laser Decapsulator

- Laser for material processing, specialized for packages
- Mainly used for plastic packages
- Standard flows for standard packages available
- Machine can be programmed for special or new cases
- Optical control by integrated camera
- Internal fume hood

- Proper selection of ablation method is vital
- Thermal strain can destroy the chip in the package
- Typically used for pre-preparation, laser stops before reaching chip
- Chemical etching is then very efficient and fast

Pictures: M.Janke/P.Laackmann (Infineon)

From Analysis towards Attack Preparation



ANALYSIS

- Is there a chip in the package, anyhow ?
- Check chip functionality – what's the chip's task ?
- Determine the chip type – are literature, tools available ?
- Identify its technology generation – how old is the chip ?
- What is the value of the chip's function for the system ?

ATTACK PREPARATION

- For further reverse engineering tasks
- For laser fault injection attacks
- For UV fuse bit (code protection) erasing
- For permanent manipulations (e.g. FIB, Lasercutter)
- For alpha radiation fault injection attacks
- For photon emission side-channel analysis
- For local electromagnetic attacks

Pictures: Private Archive M.Janke, P.Laackmann

Literature

OVERVIEW:

Friedrich Beck (Siemens), "Integrated Circuit Failure Analysis – A Guide to Preparation Techniques", Wiley, 1998, ISBN 978-0-471-97401-7, 190 pages.

Friedrich Beck (Siemens), "Präparationstechniken für die Fehleranalyse an integrierten Halbleiterschaltungen", VCH Verlagsgesellschaft mbH, 1988, ISBN 3-527-26879-0 (German), 134 pages.

DECAPSULATION USING FUMING NITRIC ACID:

Valentin Kulikov, "Manual Chemical Decapsulation", ON Semiconductor, 2008, vvku.eu/cv/docs/decap.pdf (as of 27th Dec 2014)

DECAPSULATION USING COLOPHONIUM:

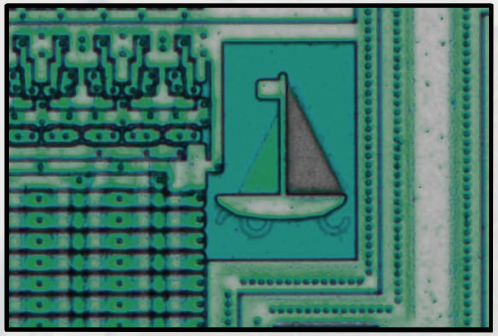
CCCB, "IC-Entkapselung mit Kolophonium" (German), berlin.ccc.de/wiki/Experiment:_IC-Entkapselung_mit_Kolophonium (as of 27th Dec 2014)
The Lab, "Die Kolophoniumkombüse" (German), runningserver.com/?page=runningserver.content.thelab.koko (as of 27th Dec 2014)

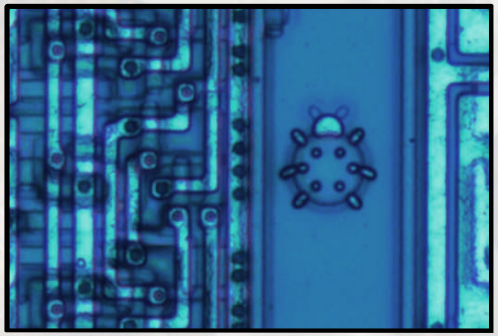
DECAPSULATION USING LASER:

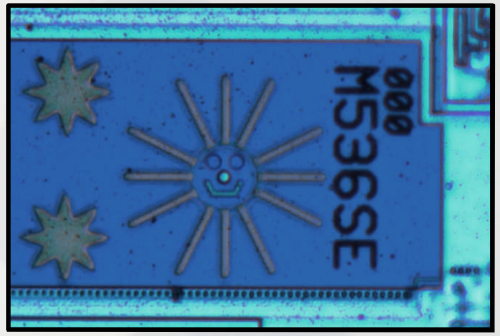
Francois Kerisit, "Laser Chip Access in 3D ICs and other Techniques", EUFANET 2011.

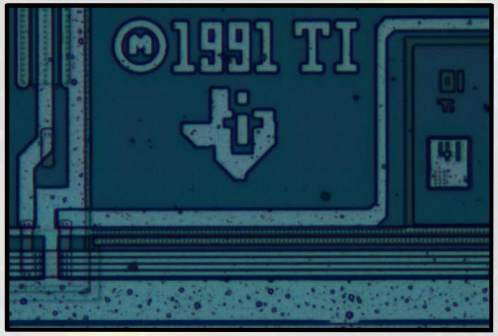
Pictures: Private Archive M.Janke, P.Laackmann

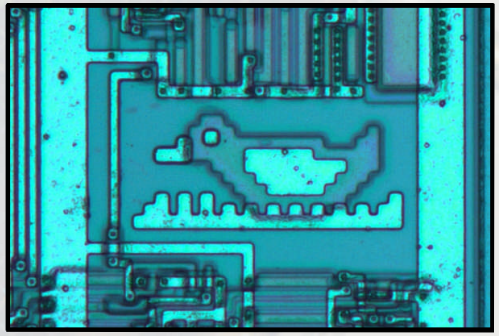
Have Fun Researching

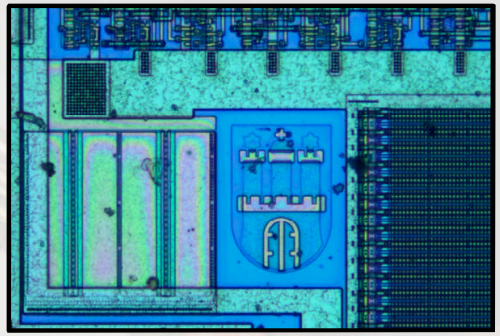












Pictures: Private Archive M.Janke, P.Laackmann