

The Need for Intrinsic Hardware Security below 65nm

Mathias Wagner
Chief Security Technologist
Business Unit Security & Connectivity



SECURE CONNECTIONS
FOR A SMARTER WORLD

Content

- **Introduction & Overview**
- **Security landscape:**
 - What are the business cases of today?
 - What level of security do they need?
 - What technology is available?
- **What happens to attack vectors as technology moves to 65nm and below**
- **Conclusion**



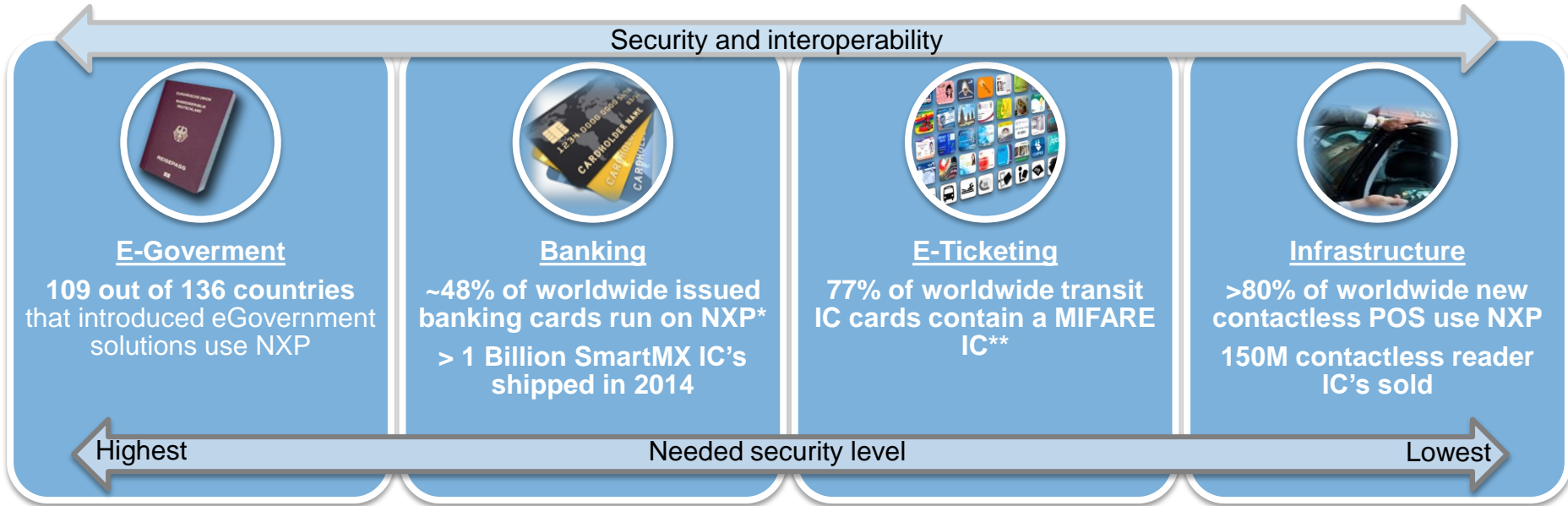
A close-up, microscopic view of a circuit board component, possibly a microchip or connector, with several pins and a blue cable attached. The background is dark and out of focus, suggesting a laboratory or industrial setting.

Security landscape

Where are we today

USE CASES

NXP in established security markets



* H1 2014 acc. ABI

** ABI 2014

Embedded secure elements



Wallet

Payment



Transit



Access



Security

Authentication



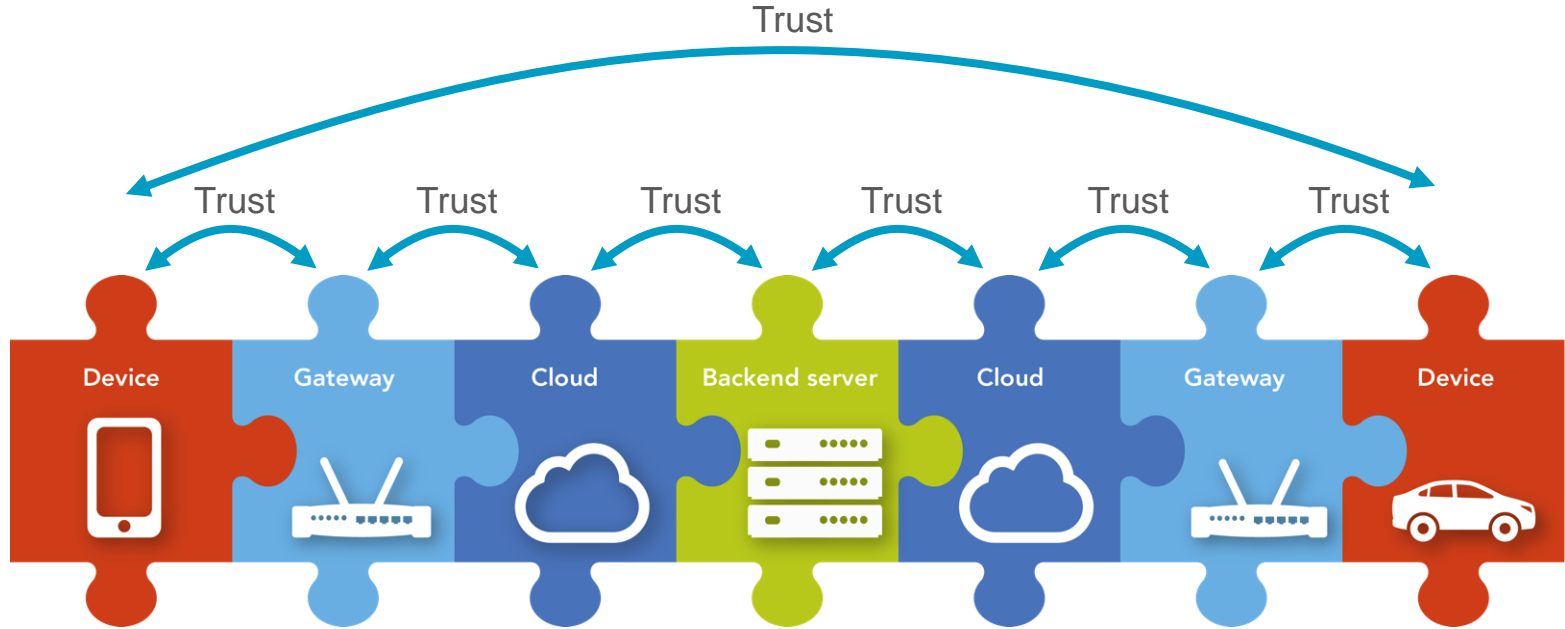
Cloud authentication



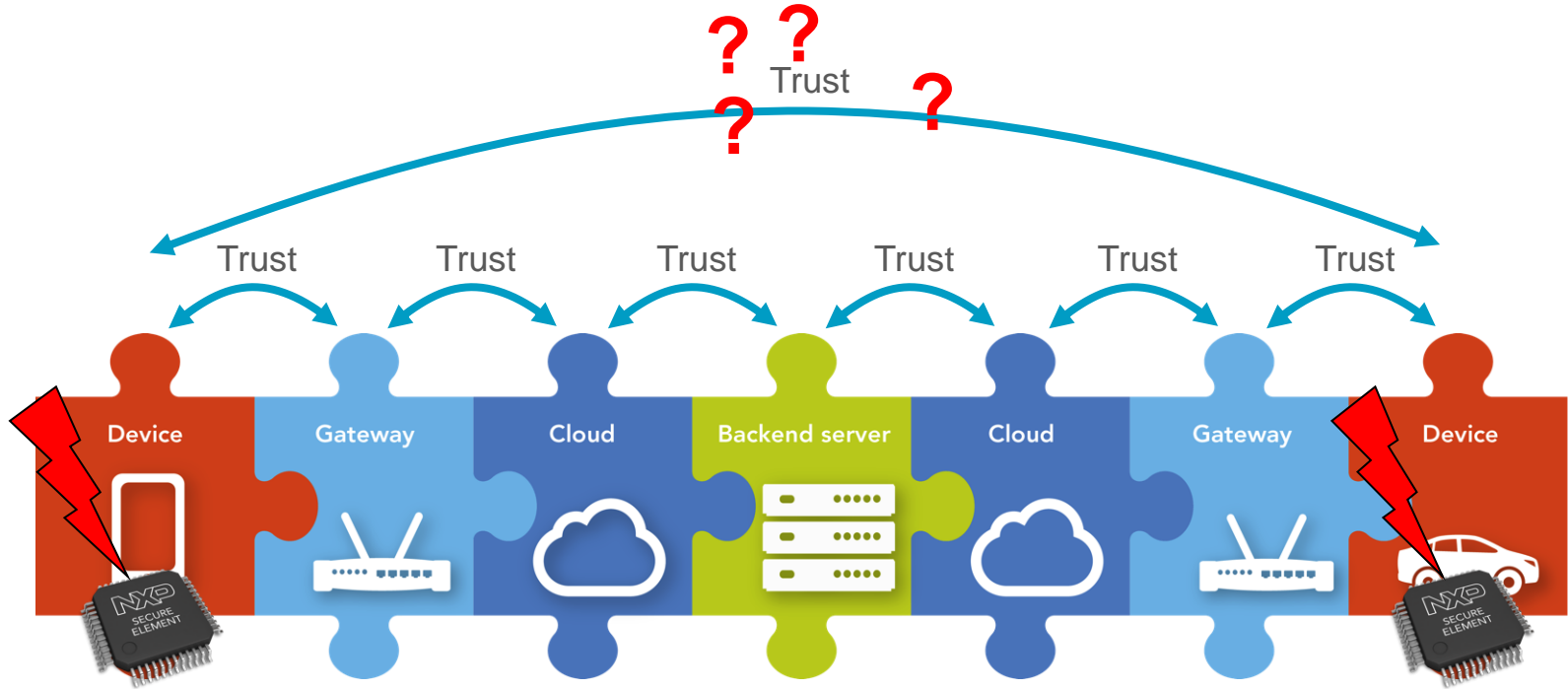
Secure Email



End to end security



The root of trust



NEED FOR HW SECURITY



Why is a secure element needed for security?

Reduce Impact of SW bugs

- Java SW averages ~1 bug every 80 lines of code.
- With intense review ~1 bug in 500 lines of code
- This rate goes up again as code size and thus complexity increases.

Reduce Complexity

- The complexity caused by all devices connected with each other multiplied by their functionality keeps increasing dramatically.

Reduce Attack Surface

- A small, compact design with a few well-defined APIs has a much smaller attack surface to get worried about.

Why is a secure element needed for security?

Provide End-2-End Security

- E-2-E Security is needed to “tunnel” through hostile territory.
- Example: Payment with phone \leftrightarrow back end

Provide Secure Key Storage

- At the root of any cryptography are secret keys.
- Keeping secret keys secret is the essence of strong crypto.

Certification

- Independent 3rd party verification of security promise!

CERTIFICATION



Security Evaluation



FIPS 140-2

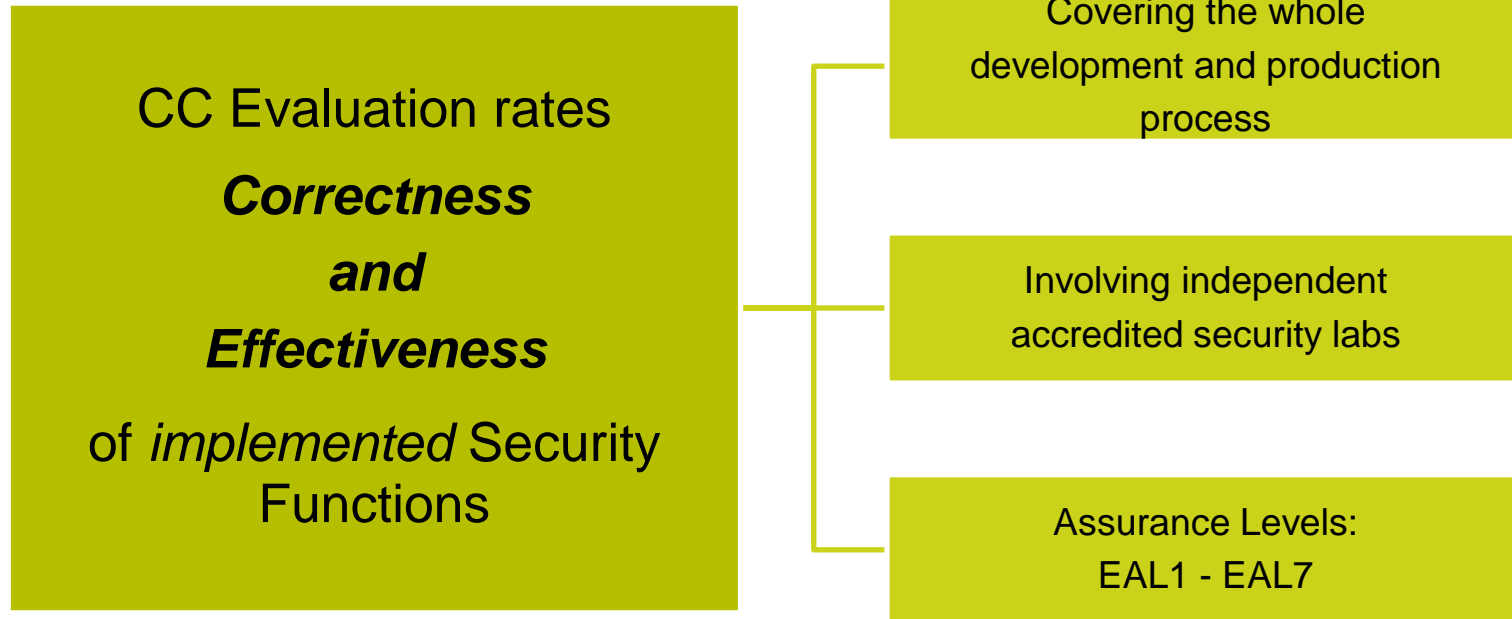
- Levels 1 – 4
- Not dedicated to smart cards, so it may also describe the physical security of a secure letter box...
- Based on Do's and Don'ts
- Based on **Checklists**



Common Criteria

- In practice levels EAL 3 – 6+
- Levels 6 & 7 require formal modeling and proofs
- Variant dedicated to smart cards available
- Based on **Assets** that need to be protected like secret keys, user data, user SW

Common Criteria – Mission Statement



„EAL“ Assurance Levels

EAL 7: formally verified designed & tested

EAL 6: semi-formally verified designed & tested

EAL 5: semi-formally designed & tested

EAL 4: methodically designed, tested & reviewed

EAL 3: methodically tested & checked

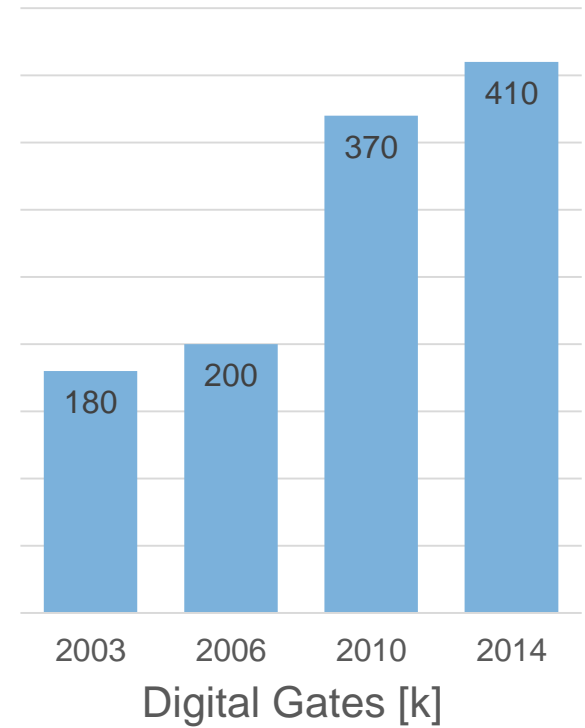
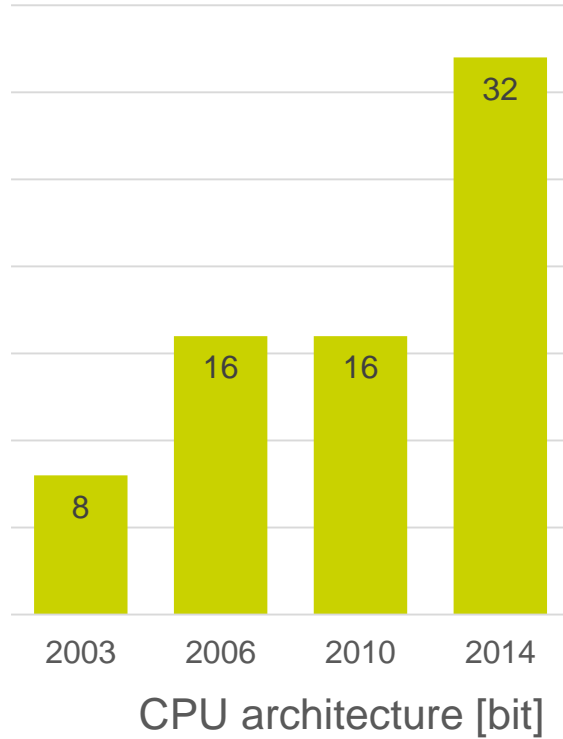
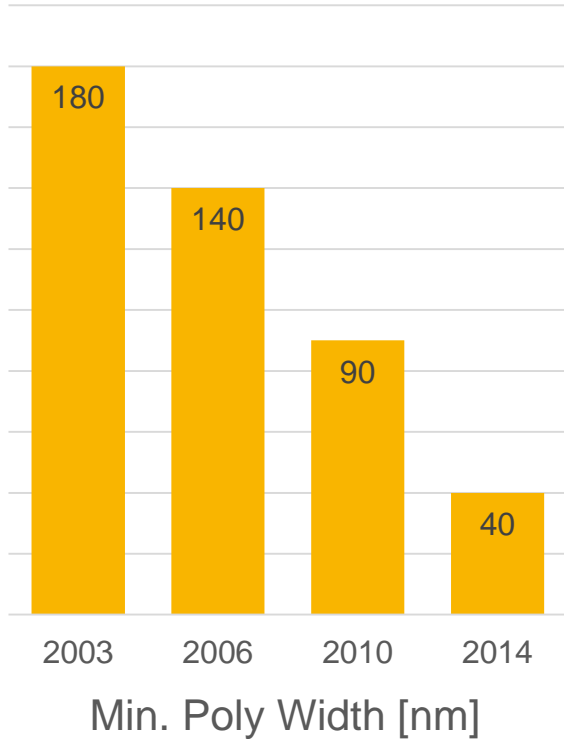
EAL 2: structurally tested

EAL 1: functionally tested

TECHNOLOGY



Technology progress





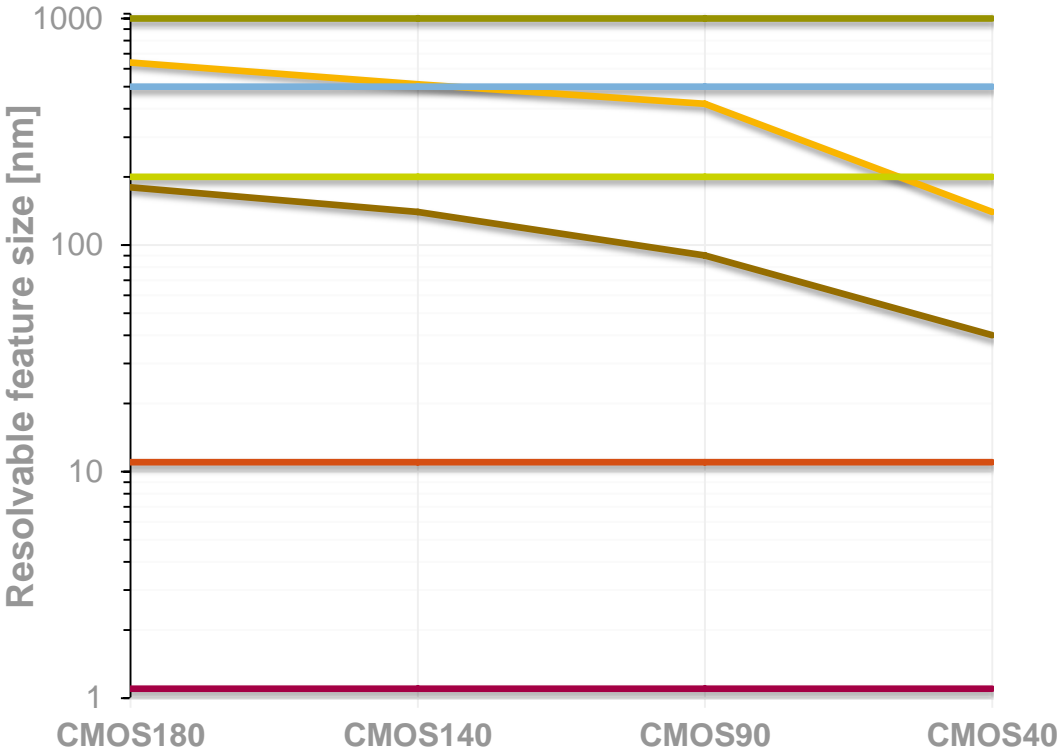
Attack vectors

Below 65 nm

INVASIVE



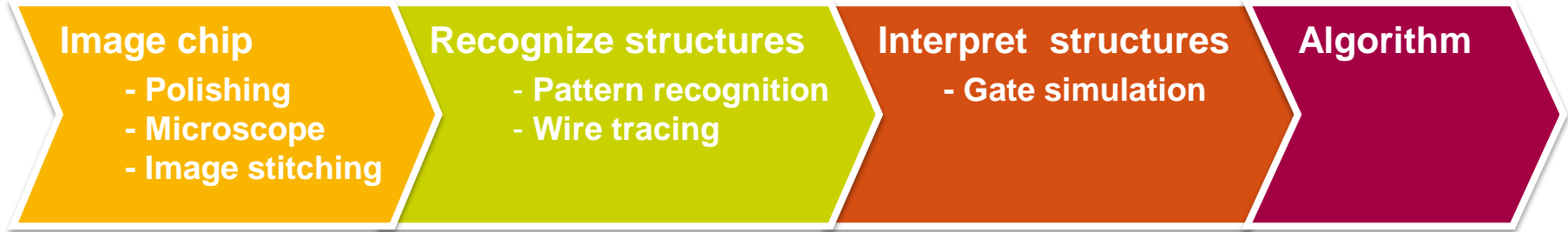
Invasive attacks complexity



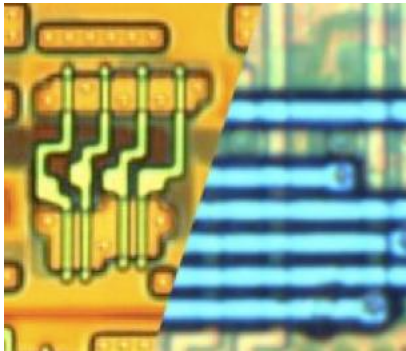
Resolutions



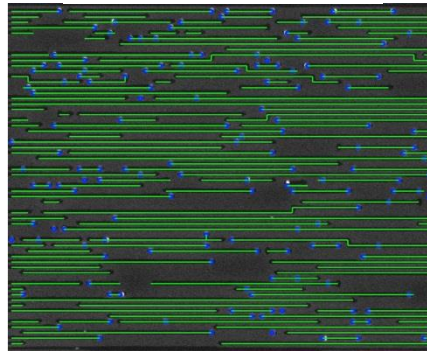
HW Reverse engineering



Chip image



Wires

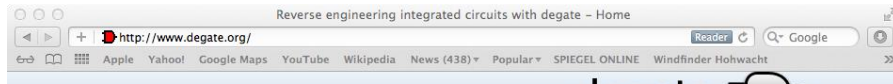


Netlist

```
<?xml version="1.0"
<gate-library>
  <gate description=
    <ports>
      <port id="0" nam
      <port id="1" nam
```

Annotated netlist

Open source tool



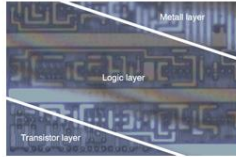
degate

Home Status Documentation Screenshots Download Contact

Welcome to the Degate Project Website.

About Degate

Degates' purpose is to aid in [VLSI reverse engineering](#) of [digital logic](#) in [integrated circuits \(ICs\)](#). Degate helps you to explore images from ICs. It matches [standard cells](#) on the imagery given by graphical templates and to some degree [vias](#) and wires. Degate assists you in tracing circuit paths and in reconstructing the netlist.



Degate is not a completely automatic analyzing tool. Degate helps you with some automation in your manual reverse engineering process.

Supported Platforms

Degate is developed under Ubuntu and OS X. The GUI is based on [gtkmm](#). So Degate should run on any unixoid platform, where gtkmm was ported to.

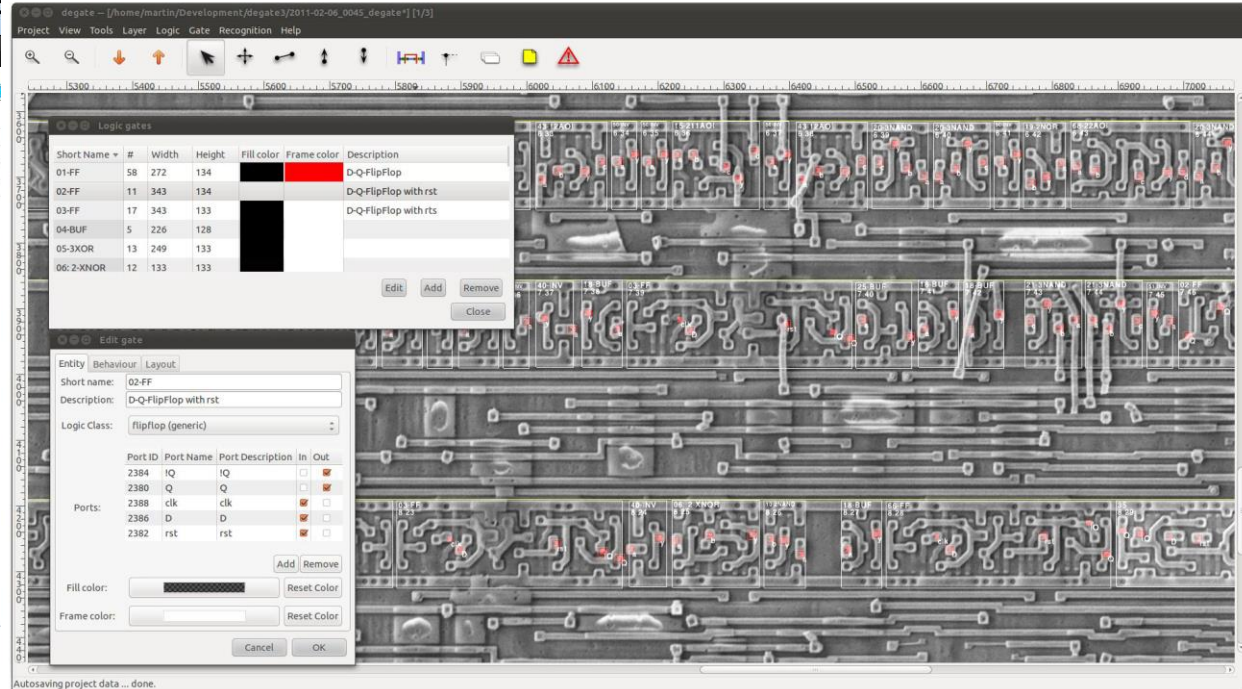
Status

Degate is a spare time project. It is still under development. Some project steps are already implemented other steps are not. Please have a look at the [status page](#) to see what is implemented until now. Degate is topic of my diploma thesis, which was [published](#) in June 2011.

Author and Licence

Degate is developed by [Martin Schobert](#). The software is open source. It is released under the [GNU General Public Licence Version 3](#).

Last page update: 2011-09-16



<http://www.degate.org/>

28. January 10, 2016

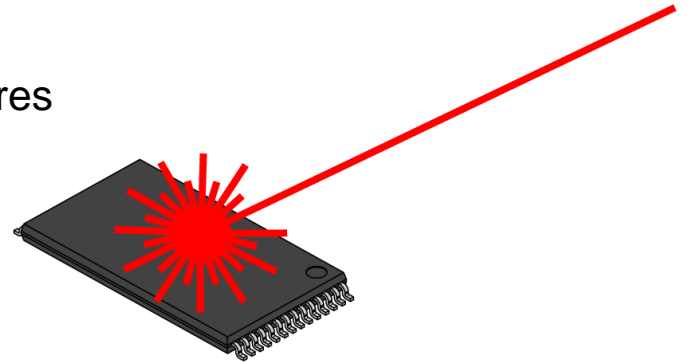


FAULT INJECTION

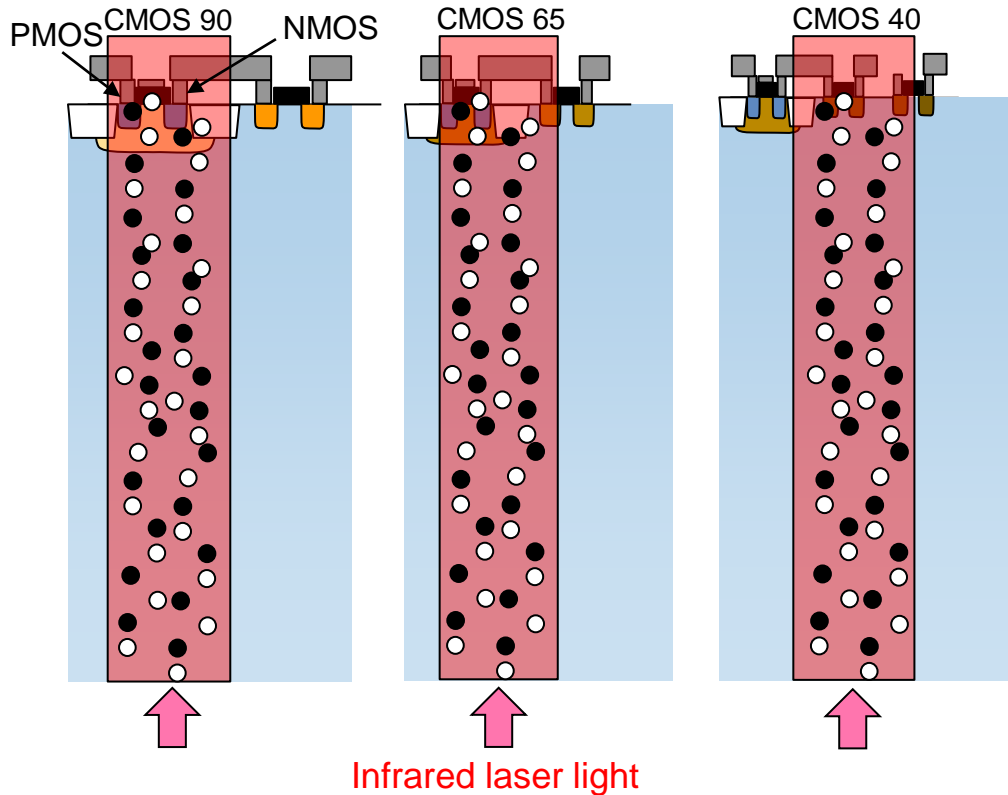


Laser fault injection

- **Question: Do small feature sizes make laser fault injection more difficult?**
- Critical aspects for a successful fault injection
 - Enough light to manipulate bits
 - Little enough light to avoid triggering countermeasures
 - Correct timing
 - Repeatability
 - Predictable impact on the IC operation



Charge generation by laser light



Determined by

- Wavelength
- Light Intensity
- Illuminated volume

Maintained for

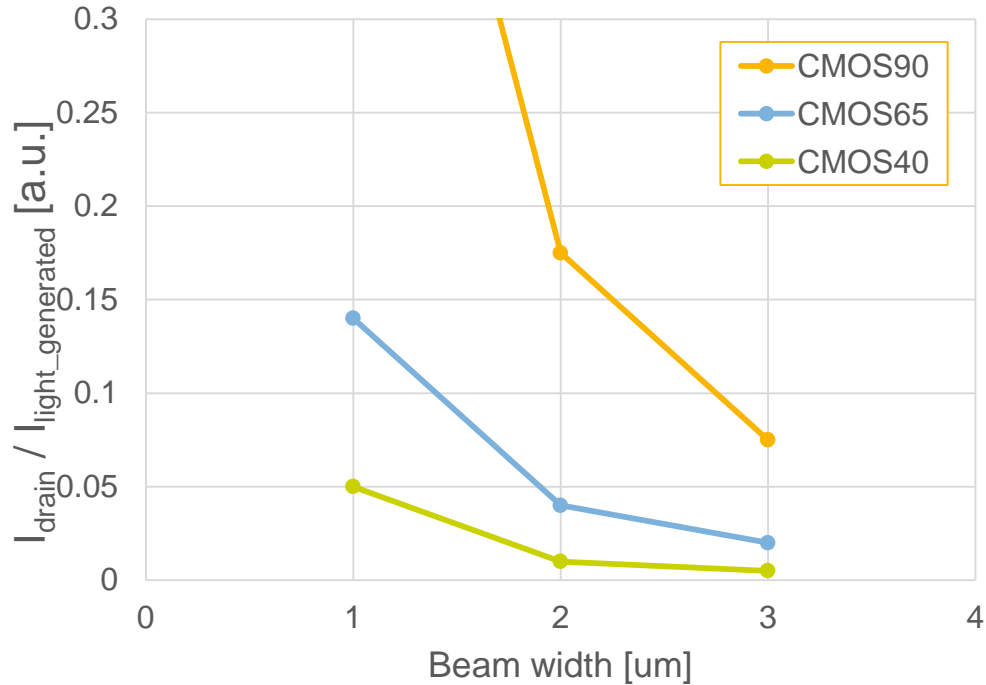
- All technology nodes equally
- Slight differences due to dopant concentrations

For newer technologies

- NIR laser spots always illuminate multiple cells
- Frontside illumination is blocked by metal layers

Charge diffusion / drift

Fraction of current collected by drain



Reaches more than one well

Determined by

- Temperature
- Substrate dopant level
- Electrical fields

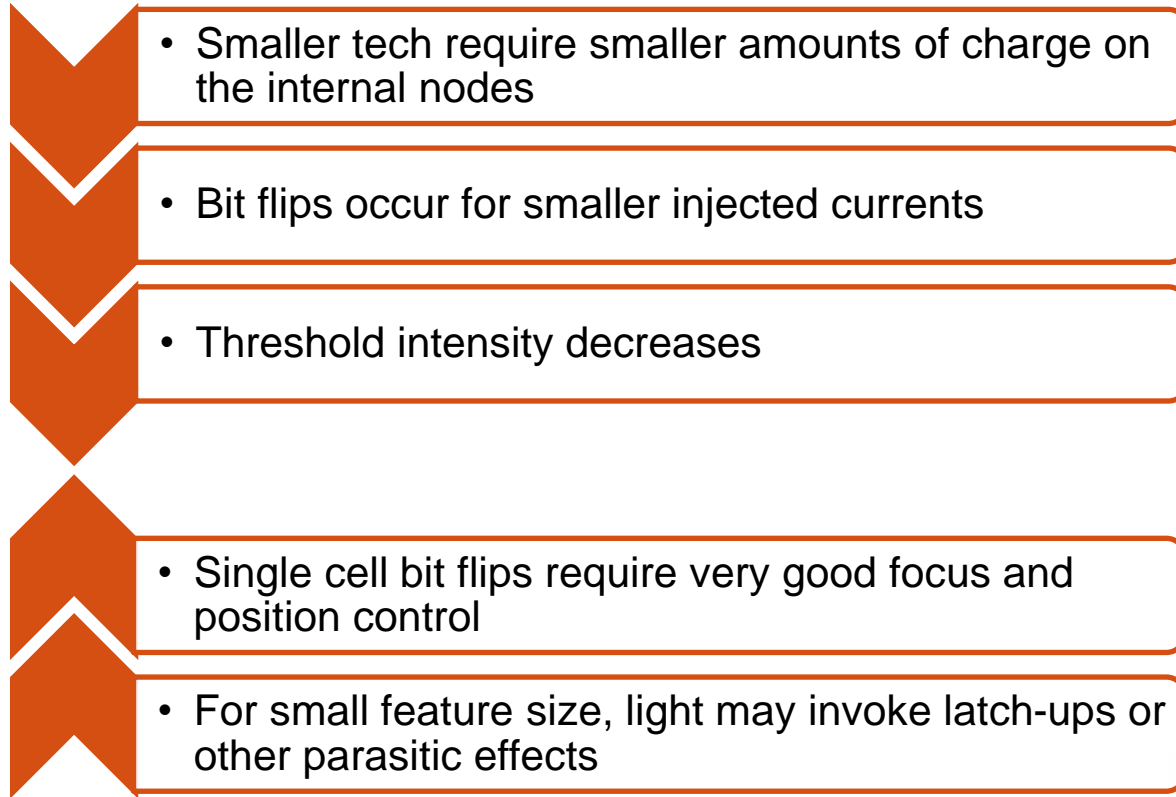
For each generation

- Charge spreads over the same area

For newer technologies

- Charge is collected by more digital cells
- LFI into a particular cell requires max. focusing

Impact on bit flips

- 
- Smaller tech require smaller amounts of charge on the internal nodes
 - Bit flips occur for smaller injected currents
 - Threshold intensity decreases
 - Single cell bit flips require very good focus and position control
 - For small feature size, light may invoke latch-ups or other parasitic effects

EM-SIDE-CHANNEL

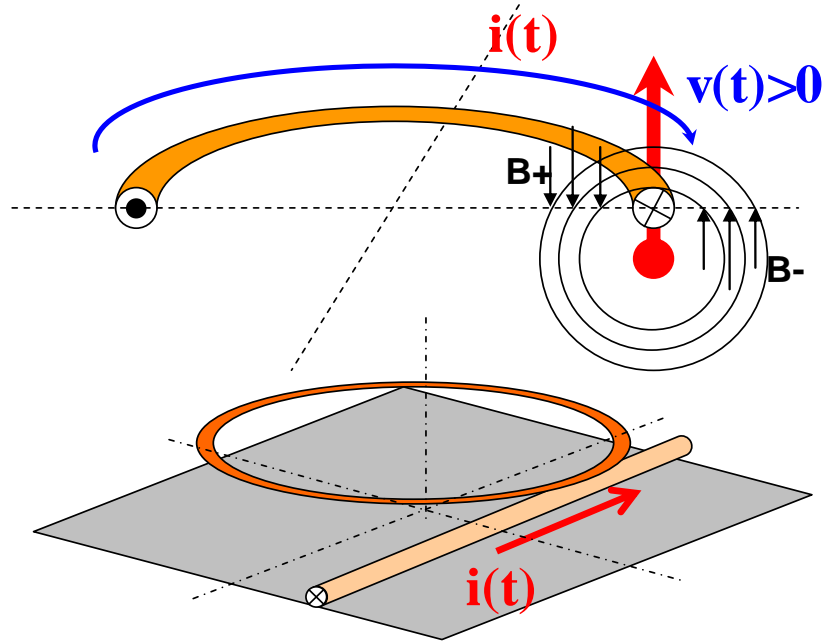


EM – Side-Channel

- **Question: Do small feature sizes affect EM-SCA?**
- Critical aspects
 - Raw signal strength through probe
 - Signal-to-noise-ratio through probe
 - Spatial resolution
 - Temporal resolution
 - Analysis stays mostly constant



Electromagnetic Emanation



EMA signal created by

- Current through metal line
- Coupled by magnetic field
- To a vertical or horizontal coil

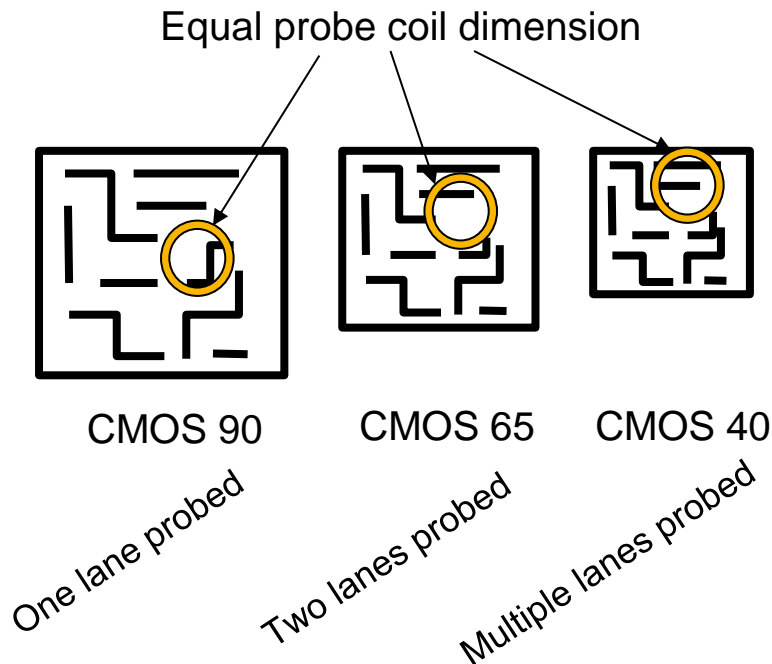
EMA detects

- **Changes** in current through the line

Leaks information on

- Internal power consumption
- Loading/unloading of internal capacities

SNR in EM probing



Determined by

- Absolute flux through probe
- Ratio of signal to noise

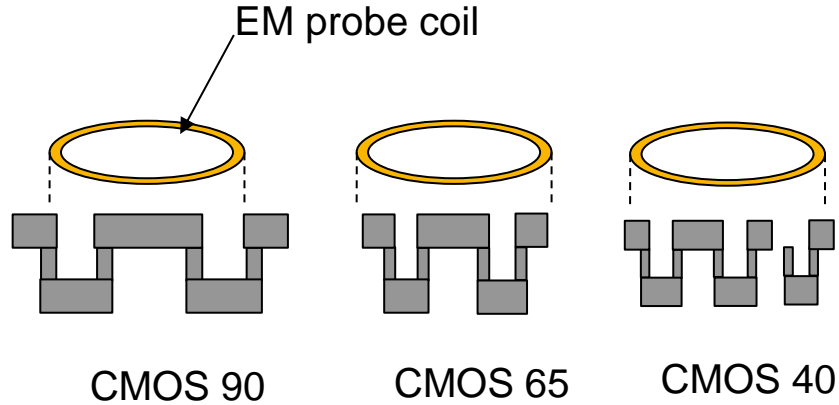
For each generation

- Core voltage changes but current stays about the same
- Absolute flux per line length constant

For newer technologies

- Smaller structures lead to overlapping and hence decreased SNR
- Higher clock frequency increases SNR via quicker changes in flux

Resolution of EM probing



Determined by

- Probe dimension
- Density of probed lines

Newer technologies

- Need smaller probes for the same spatial resolution

Smaller probes lead to

- Lower induction → worse SNR
- High complexity of setup


Impact on EM probing



- SNR decreases with smaller technologies



- Resolution decreases with smaller technologies



- Increased cost for smaller EM probes



- Absolute flux per line and per area stays constant



- Higher clocks lead to higher signal through $\Delta\phi/\Delta t$

Stories from behind the metal shield



SAFE ERROR



Safe Error Attack Analysis

- **Based on bit flip bias – Independent of technology node**
- Attacks runs in three phases



- Countermeasures



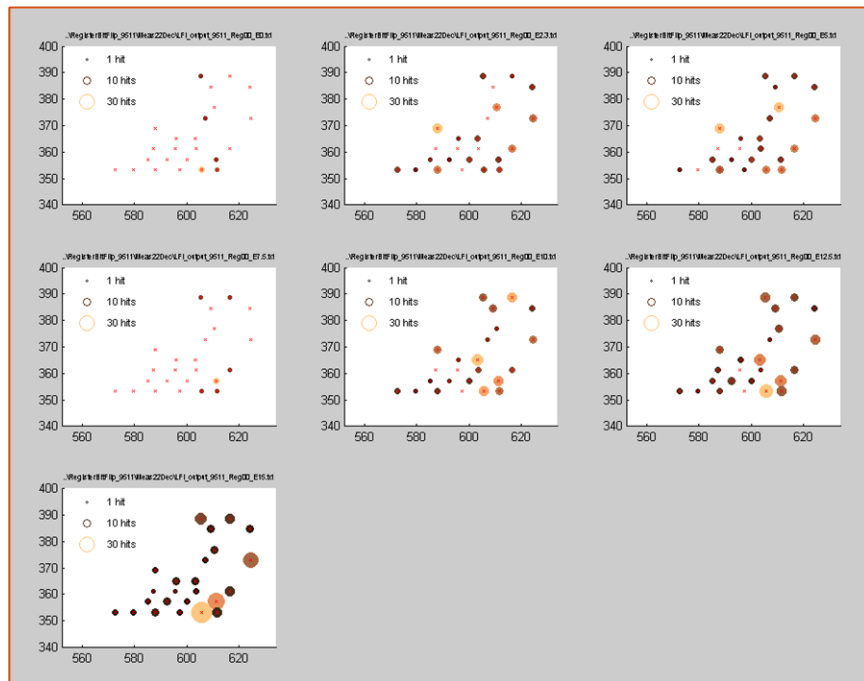
Physical Characterization

Determine bit flip bias

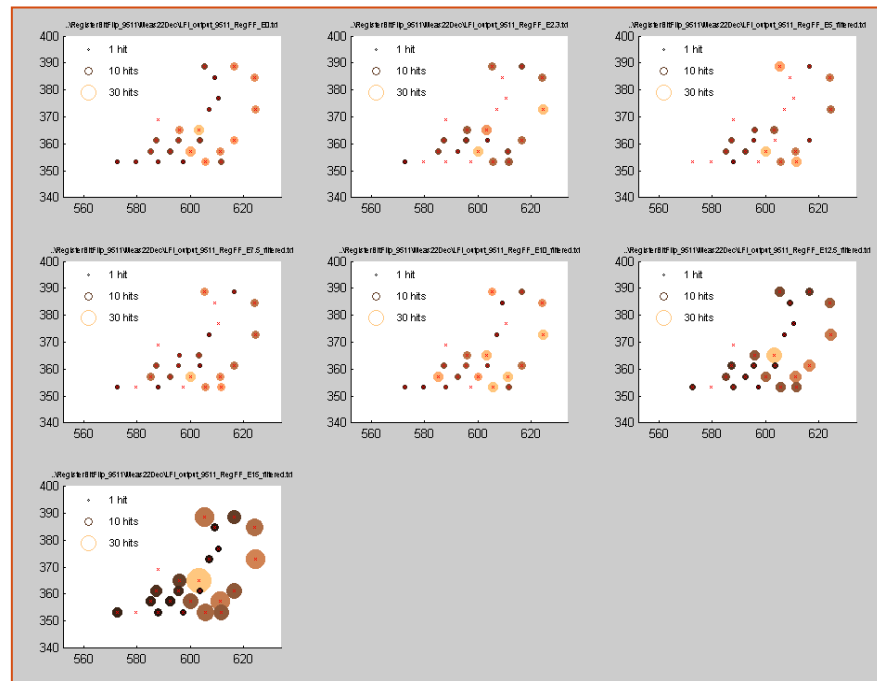
- Scan a set of standard registers with an LFI station
- Two Presets: 0x00, 0xFF



Physical Characterization



Preset 0x00



Preset 0xFF

Results over different laser pulse energies and position

Physical Characterization

Determine bit flip bias

- Scan a set of standard registers with an LFI station
- Two Presets: 0x00, 0xFF



Results

- Preferred flip direction for very low energy: 0 → 1
- Not a 100% bias, but enough for a safe-error attack

Effect of masking

Targeted pair could be

- Two mask bits
- Two masked key bits
- One mask, one masked key bit

Possible effects of hitting a pair

- Flip bias 0 → 1

Key	Mask	Masked Key	Mask'	Masked Key'	Key'
0	0	0	1	1	0 → 0
0	1	1	1	1	0 → 0
1	0	1	1	1	1 → 0
1	1	0	1	1	1 → 0

Excursion – Security Evaluation

Identification Phase:

- Perform the attack **once** to demonstrate its feasibility and / or achieve a one-time benefit (learning phase)

Exploitation Phase:

- Perform the attack **multiple times** for commercial exploitation

Information Flow between these Phases:

- One of the outcomes of the Identification Phase is a **virtual script** that tells the attacker of the Exploitation Phase how to perform the attack

Excursion – CC for Smart Cards

Range of values CC 3.x	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

We need to achieve 31 points for VAN.5
(part of EAL 4+, 5, 5+, 6, 6+) for each and every attack path!

“Application of Attack Potential to Smartcards”
(developed for JIL by JHAS group)

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Identification scenario

Assume an AES 256 case

Static bit flip approach

LFI Test

- Load chosen key and plain tex
- LFI to the IC before AES excecution
- Excecute AES
- Analyse result – get key

Exploitation scenario

Result from identification phase

- Physical location of bits
- Timing information on key loading

Additional conditions

- Known cipher text, known plain text
- Unlimited tries

Attack

- Pair of masked key and mask
- Between key loading and AES operation
- Either per spatial or temporal double shot
- Analyse result – get key

Identification phase

Identification of physical location of key bits

- Problem 1: Key bits are masked
- Problem 2: Mask bits are stored scrambled
- Problem 3: Any reset is creating a new mask and scrambling pattern

Assumptions

- Mask has on average a Hamming Weight of 0.5
- Mask bits are scrambled byte-wise and independently

Identification phase

Effects of mask

- Two laser attacks are needed for each key bit:
512

Effects of scrambling

- 32 possible locations for each mask bit:
 $1 - (33/64)^n = 0.99 \Rightarrow n = 6.95$ per bit
- So total is $512 \times 7 = 3584$

Excursion – CC for Smart Cards

Range of values CC 3.x	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

We need to achieve 31 points for VAN.5
(part of EAL 4+, 5, 5+, 6, 6+) for each and every attack path!

“Application of Attack Potential to Smartcards”
(developed for JIL by JHAS group)

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

$$14 + 13 = 27$$

Conclusion

Security Summary

- The question is, whether HW security offers sufficient advantages over SW security in an Online World, where a system view is required → We like to believe it does...
- Security will improve as technology shrinks, but not per se dramatically
- Security Analysts are here to stay...





SECURE CONNECTIONS
FOR A SMARTER WORLD