Towards package opening detection at power-up by monitoring thermal dissipation

G. Chancel - J. Toulemont - F. Mailly - P. Maurine - P. Nouet

2025/04/04

INTRODUCTION

Context

Many hardware attacks either:

Context

Many hardware attacks either:

- Require a backside package opening:
  1. BBI, micro-probing
  2. LFI, photo-emission

Context

Many hardware attacks either:

- Require a backside package opening:
  1. BBI, micro-probing
  2. LFI, photo-emission
- Are more efficient after a frontside package opening:
  1. EMFI
  2. Side-channel attacks/analysis

Context

Many hardware attacks either:

- Require a backside package opening:
  1. BBI, micro-probing
  2. LFI, photo-emission
- Are more efficient after a frontside package opening:
  1. EMFI
  2. Side-channel attacks/analysis

Observations:

- Package removal is ont considered a significant problem
- May be a legacy of smart-cards where the package is limited

Context

Countermeasures:

Many countermeasureas exist against physical attacks:

Context

Countermeasures:

Many countermeasureas exist against physical attacks:

- Sensors to detect EMFI, BBI or LFI attempts

Context

Countermeasures:

Many countermeasureas exist against physical attacks:

- Sensors to detect EMFI, BBI or LFI attempts
- Nano-pyramids or TSV to detect substrate thinning/intrusion

Context

Countermeasures:

Many countermeasureas exist against physical attacks:

- Sensors to detect EMFI, BBI or LFI attempts
- Nano-pyramids or TSV to detect substrate thinning/intrusion
- Embedded coils to detect EM probes for SCA or EMFI

Context

Countermeasures:

Many countermeasureas exist against physical attacks:

- Sensors to detect EMFI, BBI or LFI attempts
- Nano-pyramids or TSV to detect substrate thinning/intrusion
- Embedded coils to detect EM probes for SCA or EMFI

Observations:

Context

Countermeasures:

Many countermeasureas exist against physical attacks:

- Sensors to detect EMFI, BBI or LFI attempts
- Nano-pyramids or TSV to detect substrate thinning/intrusion
- Embedded coils to detect EM probes for SCA or EMFI

Observations:

- Countermeasures focus on specific attacks

Context

Countermeasures:

Many countermeasureas exist against physical attacks:

- Sensors to detect EMFI, BBI or LFI attempts
- Nano-pyramids or TSV to detect substrate thinning/intrusion
- Embedded coils to detect EM probes for SCA or EMFI

Observations:

- Countermeasures focus on specific attacks
- Often, the attacks have already been carried out

Context

Trends:

Context

Trends:

- Security spreads to many applications

Context

Trends:

- Security spreads to many applications
- Not only smart-cards have to be secure

Context

Trends:

- Security spreads to many applications
- Not only smart-cards have to be secure
- Microcontrollers (IoT), SoCs (smartphones, laptopts), face physical threats

Context

Trends:

- Security spreads to many applications
- Not only smart-cards have to be secure
- Microcontrollers (IoT), SoCs (smartphones, laptopts), face physical threats
- SoC and microcontroller (µcu) packages ensure thermal dissipation

Context

Trends:

- Security spreads to many applications
- Not only smart-cards have to be secure
- Microcontrollers (IoT), SoCs (smartphones, laptopts), face physical threats
- SoC and microcontroller (µcu) packages ensure thermal dissipation
- Most SoCs and µcu embeds one or more temperature sensors

Context

Trends:

- Security spreads to many applications
- Not only smart-cards have to be secure
- Microcontrollers (IoT), SoCs (smartphones, laptopts), face physical threats
- SoC and microcontroller (µcu) packages ensure thermal dissipation
- Most SoCs and µcu embeds one or more temperature sensors

Idea:

- Are temperature sensors exploitable to check IC package integrity?

Context

Trends:

- Security spreads to many applications
- Not only smart-cards have to be secure
- Microcontrollers (IoT), SoCs (smartphones, laptopts), face physical threats
- SoC and microcontroller (µcu) packages ensure thermal dissipation
- Most SoCs and µcu embeds one or more temperature sensors

Idea:

- Are temperature sensors exploitable to check IC package integrity?
- **Let us explore this with a common µcu**

THE DEVICE UNDER TEST

The device under test

DUT

The device under test

DUT

- STMicroelectronics STM32F439ZGT6
- Designed in a 90 nm bulk CMOS technology

The device under test

DUT

- STMicroelectronics STM32F439ZGT6
- Designed in a 90 nm bulk CMOS technology
- Embeds an ARM Cortex-M4 core and several cryptographic modules

The device under test

DUT

- STMicroelectronics STM32F439ZGT6
- Designed in a 90 nm bulk CMOS technology
- Embeds an ARM Cortex-M4 core and several cryptographic modules
- Embeds a temperature sensor: $\pm$ 1.5 °C between [-40 °C, 125 °C]

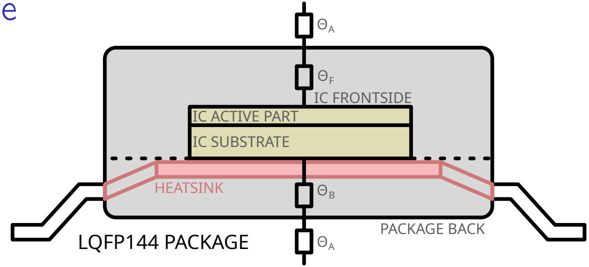
The device under test

DUT

- STMicroelectronics STM32F439ZGT6
- Designed in a 90 nm bulk CMOS technology
- Embeds an ARM Cortex-M4 core and several cryptographic modules
- Embeds a temperature sensor: ± 1.5 °C between [-40 °C, 125 °C]
- Embeds calibration values to mitigate process variation: TS_CAL1, TS_CAL2:

$$T = \frac{80}{TS_{CAL1} - TS_{CAL2}} \cdot (TS - TS_{CAL1}) + 30 \quad ^{\circ}C \qquad (1)$$

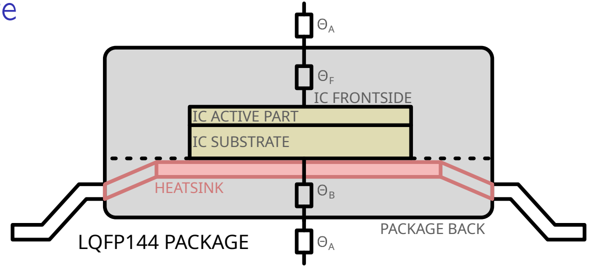
The device package



Package characteristics:

- LQFP144

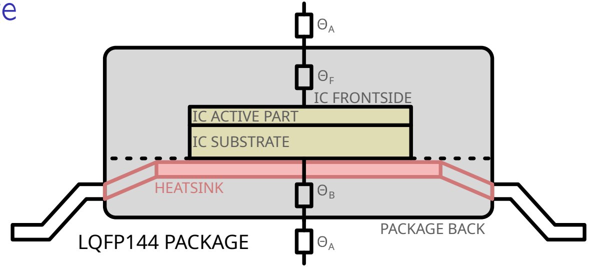
The device package



Package characteristics:

- LQFP144
- Embedded heatsink on the backside $\rightarrow \theta_F >> \theta_B$

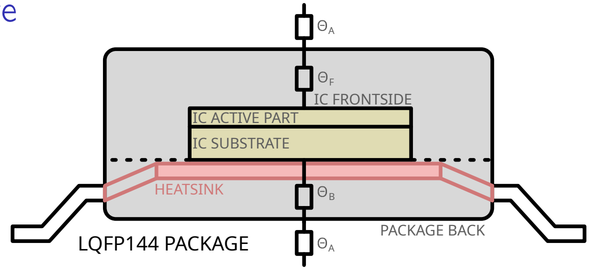
The device package



Package characteristics:

- LQFP144
- Embedded heatsink on the backside $\rightarrow \theta_F >> \theta_B$
- Removing either frontside or backside changes θ_F or θ_B

The device package



Package characteristics:

- LQFP144
- Embedded heatsink on the backside $\rightarrow \theta_F >> \theta_B$
- Removing either frontside or backside changes θ_F or θ_B
- **What are the effects of the package on thermal dissipation?**

IC thermal behavior

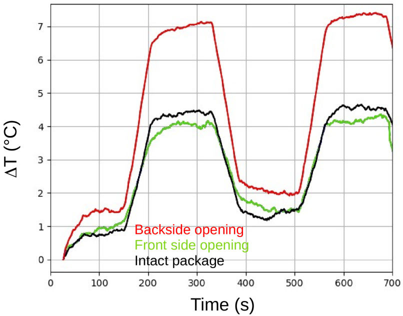
First experiment

- Compare an intact IC with frontside and backside opened ones
- Periodic FLASH memory write operation and idle state (180 s each)

IC thermal behavior

First experiment

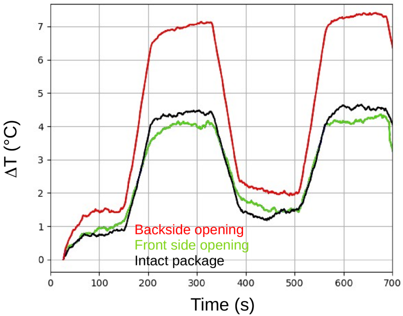
- Compare an intact IC with frontside and backside opened ones
- Periodic FLASH memory write operation and idle state (180 s each)



IC thermal behavior

First experiment

- Compare an intact IC with frontside and backside opened ones
- Periodic FLASH memory write operation and idle state (180 s each)

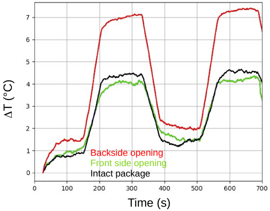


Conclusion:

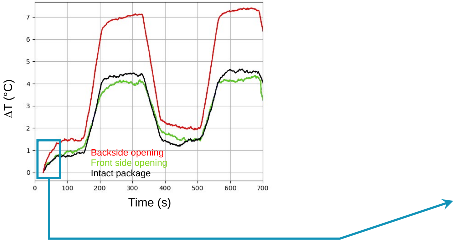
Temperature changes:

- Are fast whatever the package
- Are limited with an intact or frontside opened IC
- Are faster and stronger with a backside opened IC

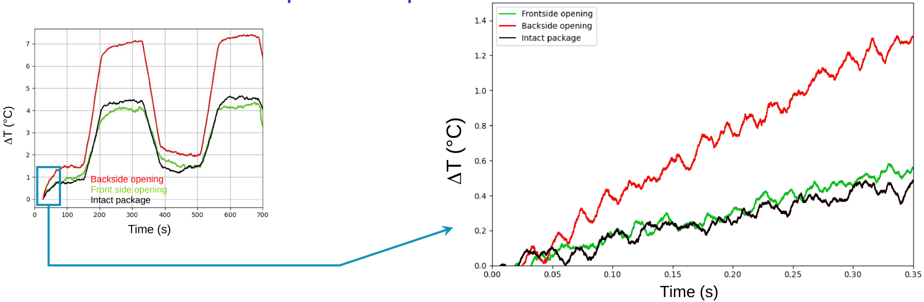
IC thermal behavior: power-up temperature transients



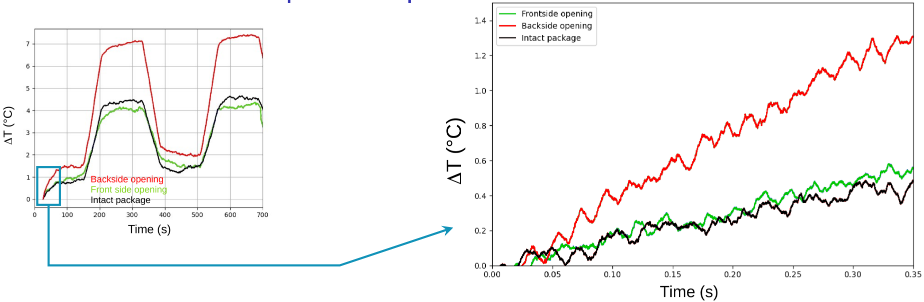
IC thermal behavior: power-up temperature transients



IC thermal behavior: power-up temperature transients

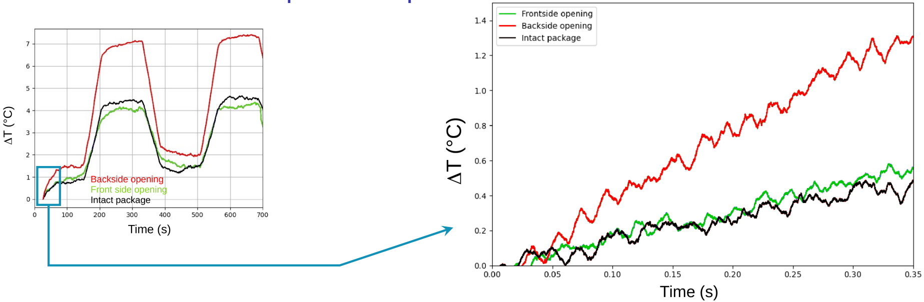


IC thermal behavior: power-up temperature transients



- Linear evolution over 350 ms: $T = \beta_1 \cdot t + \beta_0 + \varepsilon$
- Higher slope for the backside opened IC

IC thermal behavior: power-up temperature transients



- Linear evolution over 350 ms: $T = \beta_1 \cdot t + \beta_0 + \varepsilon$
- Higher slope for the backside opened IC

Question?

Is it possible to check the backside package integrity by checking the value of β_1

PACKAGE REMOVAL EXPERIMENTAL RESULTS

β_1 measurements across 13 circuits

Package integrity verification process → 13 devices (all units in °C/s)

IC n°	$\bar{\beta_1}$	σ_{β_1}	$\bar{R^2}$	σ_{R^2}	Backside
25	0.931	0.229	0.011	0.005	Closed
3	1.405	0.145	0.060	0.015	Closed
12	1.819	0.204	0.180	0.085	Closed
6	2.183	0.191	0.080	0.012	Closed
2	2.503	0.322	0.174	0.146	Closed
26	2.970	0.160	0.057	0.006	Closed
1	3.433	0.159	0.093	0.08	Opened
9	3.965	0.167	0.336	0.021	Opened
10	4.341	0.193	0.144	0.100	Opened
7	4.567	0.137	0.278	0.023	Opened
8	4.843	0.222	0.232	0.086	Opened
4	6.351	0.149	0.437	0.078	Opened
11	6.539	0.237	0.385	0.096	Opened

β_1 measurements across 13 circuits

Package integrity verification process → 13 devices (all units in °C/s)

IC n°	$\bar{\beta_1}$	σ_{β_1}	$\bar{R^2}$	σ_{R^2}	Backside
25	0.931	0.229	0.011	0.005	Closed
3	1.405	0.145	0.060	0.015	Closed
12	1.819	0.204	0.180	0.085	Closed
6	2.183	0.191	0.080	0.012	Closed
2	2.503	0.322	0.174	0.146	Closed
26	2.970	0.160	0.057	0.006	Closed
1	3.433	0.159	0.093	0.08	Opened
9	3.965	0.167	0.336	0.021	Opened
10	4.341	0.193	0.144	0.100	Opened
7	4.567	0.137	0.278	0.023	Opened
8	4.843	0.222	0.232	0.086	Opened
4	6.351	0.149	0.437	0.078	Opened
11	6.539	0.237	0.385	0.096	Opened

Conclusion

- Backside opened ICs show a higher average β_1 value, of around 2.89 °C/s

β_1 measurements across 13 circuits

Package integrity verification process → 13 devices (all units in °C/s)

IC n°	$\bar{\beta_1}$	σ_{β_1}	$\bar{R^2}$	σ_{R^2}	Backside
25	0.931	0.229	0.011	0.005	Closed
3	1.405	0.145	0.060	0.015	Closed
12	1.819	0.204	0.180	0.085	Closed
6	2.183	0.191	0.080	0.012	Closed
2	2.503	0.322	0.174	0.146	Closed
26	2.970	0.160	0.057	0.006	Closed
1	3.433	0.159	0.093	0.08	Opened
9	3.965	0.167	0.336	0.021	Opened
10	4.341	0.193	0.144	0.100	Opened
7	4.567	0.137	0.278	0.023	Opened
8	4.843	0.222	0.232	0.086	Opened
4	6.351	0.149	0.437	0.078	Opened
11	6.539	0.237	0.385	0.096	Opened

Conclusion

- Backside opened ICs show a higher average β_1 value, of around 2.89 °C/s
- σ_{β_1} ranges from 0.15 to 0.3 °C/s, with an average of 0.193 °C/s

β_1 measurements across 13 circuits

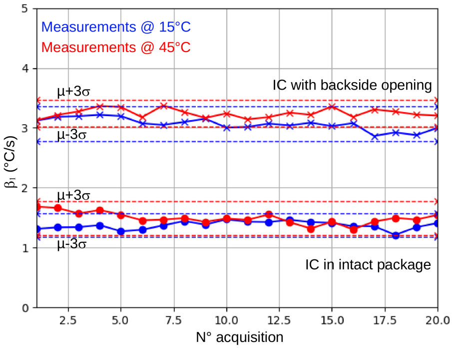
Package integrity verification process → 13 devices (all units in °C/s)

IC n°	$\bar{\beta_1}$	σ_{β_1}	$\bar{R^2}$	σ_{R^2}	Backside
25	0.931	0.229	0.011	0.005	Closed
3	1.405	0.145	0.060	0.015	Closed
12	1.819	0.204	0.180	0.085	Closed
6	2.183	0.191	0.080	0.012	Closed
2	2.503	0.322	0.174	0.146	Closed
26	2.970	0.160	0.057	0.006	Closed
1	3.433	0.159	0.093	0.08	Opened
9	3.965	0.167	0.336	0.021	Opened
10	4.341	0.193	0.144	0.100	Opened
7	4.567	0.137	0.278	0.023	Opened
8	4.843	0.222	0.232	0.086	Opened
4	6.351	0.149	0.437	0.078	Opened
11	6.539	0.237	0.385	0.096	Opened

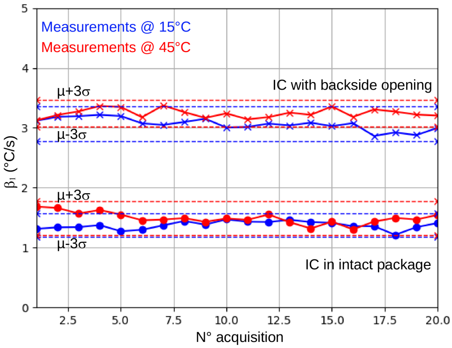
Conclusion

- Backside opened ICs show a higher average β_1 value, of around 2.89 °C/s
- σ_{β_1} ranges from 0.15 to 0.3 °C/s, with an average of 0.193 °C/s
- Is β_1 stable with room temperature and power supply voltage?

Experimental results at fixed temperatures

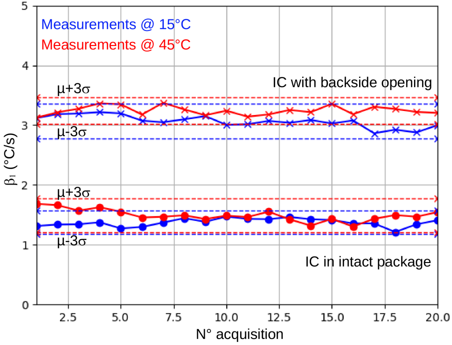


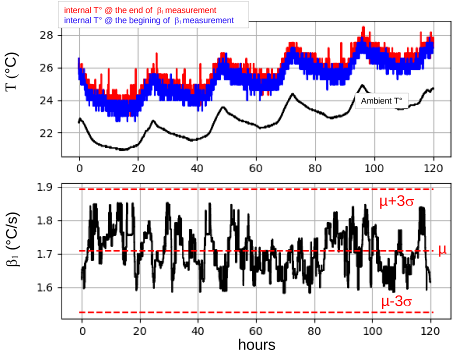
Experimental results at fixed temperatures



β_1 seems temperature independent

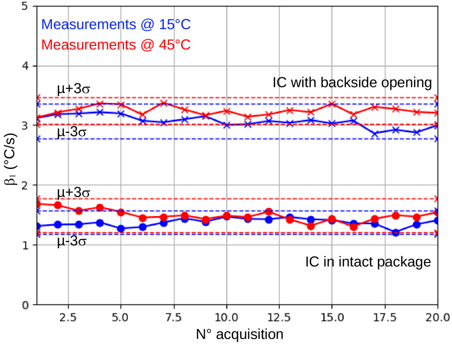
Experimental results at fixed temperatures



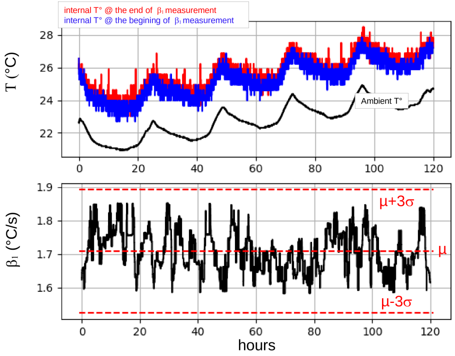


β_1 seems temperature independent

Experimental results at fixed temperatures

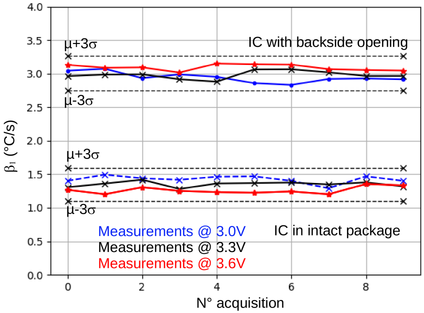


β_1 seems temperature independent

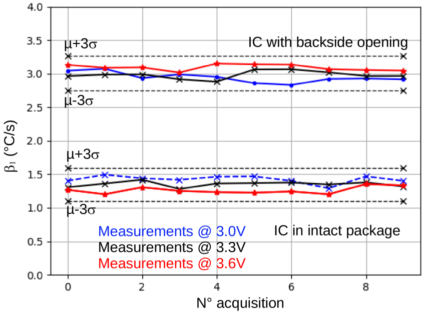


$$\rho_{T_{AMB},T_{IC}} = 96\ \%$$
$$\rho_{T_{AMB},\beta_1} = -22\ \%$$

Experimental results at different voltages

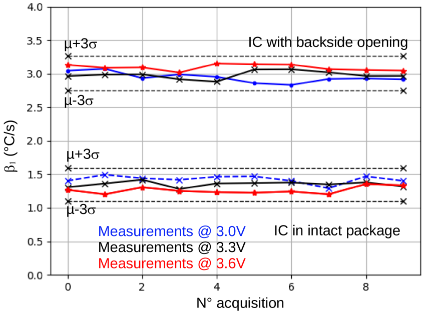


Experimental results at different voltages



β_1 seems voltage independent

Experimental results at different voltages

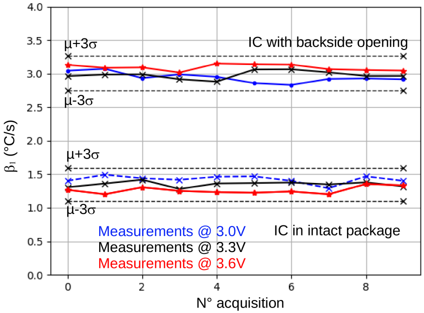


β_1 seems voltage independent

Conclusion:

- β_1 seems temperature independent

Experimental results at different voltages

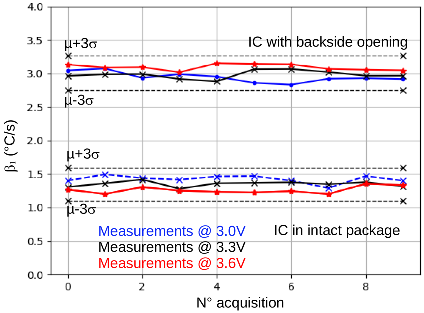


β_1 seems voltage independent

Conclusion:

- β_1 seems temperature independent
- β_1 seems supply voltage independent

Experimental results at different voltages



β_1 seems voltage independent

Conclusion:

- β_1 seems temperature independent
- β_1 seems supply voltage independent
- β_1 is stable over time

Package integrity verification

What we propose

Package integrity verification

What we propose

- Characterize the IC with the interval $\beta_1 \pm 3 \cdot \sigma_{\beta_1}$ after manufacturing

Package integrity verification

What we propose

- Characterize the IC with the interval $\beta_1 \pm 3 \cdot \sigma_{\beta_1}$ after manufacturing
- Store its calibration value like for TS_CAL1 and TS_CAL2

Package integrity verification

What we propose

- Characterize the IC with the interval $\beta_1 \pm 3 \cdot \sigma_{\beta_1}$ after manufacturing
- Store its calibration value like for TS_CAL1 and TS_CAL2
- Check at every boot that β_1 is conform to the calibration value, i.e. ↴

$$\beta_1 \in [\overline{\beta_1} - 3 \cdot \sigma_{\beta_1}, \overline{\beta_1} + 3 \cdot \sigma_{\beta_1}] \tag{2}$$

Further validation: comparing identical ICs

Further validation: comparing identical ICs (units in °C·s^{-1})

	Intact package		Backside opening		
IC №	$\overline{\beta_1}$	$\overline{\sigma_{\beta_1}}$	$\overline{\beta_1'}$	$\overline{\sigma_{\beta_1'}}$	$\overline{\beta_1'} - \overline{\beta_1}$
2	1.400	0.125	7.470	0.063	6.070
3	1.608	0.147	5.899	0.089	4.291
6	1.636	0.112	5.642	0.068	4.006
28	2.095	0.195	4.097	0.077	2.002
26	2.970	0.175	5.817	0.084	2.847
25	3.101	0.453	5.660	0.059	2.559

Further validation: comparing identical ICs (units in °C·s^{-1})

	Intact package		Backside opening		
IC №	$\overline{\beta_1}$	$\overline{\sigma_{\beta_1}}$	$\overline{\beta_1'}$	$\overline{\sigma_{\beta_1'}}$	$\overline{\beta_1'} - \overline{\beta_1}$
2	1.400	0.125	7.470	0.063	6.070
3	1.608	0.147	5.899	0.089	4.291
6	1.636	0.112	5.642	0.068	4.006
28	2.095	0.195	4.097	0.077	2.002
26	2.970	0.175	5.817	0.084	2.847
25	3.101	0.453	5.660	0.059	2.559

Observation:

- As before, β_1 increases with backside opening

Further validation: comparing identical ICs (units in °C·s^{-1})

	Intact package		Backside opening		
IC №	$\overline{\beta_1}$	$\overline{\sigma_{\beta_1}}$	$\overline{\beta'_1}$	$\overline{\sigma_{\beta'_1}}$	$\overline{\beta'_1} - \overline{\beta_1}$
2	1.400	0.125	7.470	0.063	6.070
3	1.608	0.147	5.899	0.089	4.291
6	1.636	0.112	5.642	0.068	4.006
28	2.095	0.195	4.097	0.077	2.002
26	2.970	0.175	5.817	0.084	2.847
25	3.101	0.453	5.660	0.059	2.559

Observation:

- As before, β_1 increases with backside opening
- In average $\rightarrow$ + 3.3 °C·s^{-1}

Further validation: comparing identical ICs (units in °C·s^{-1})

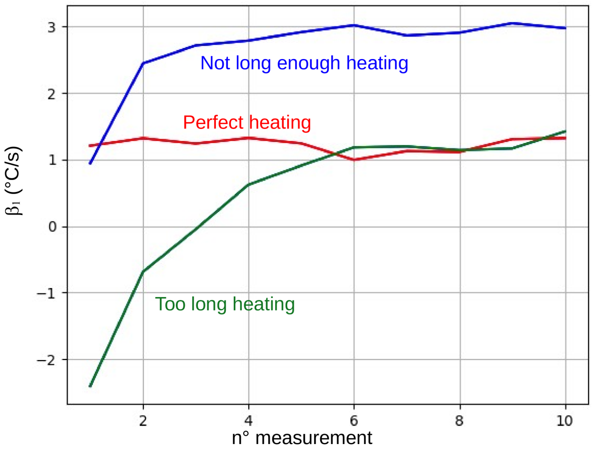
	Intact package		Backside opening		
IC №	$\overline{\beta_1}$	$\overline{\sigma_{\beta_1}}$	$\overline{\beta_1'}$	$\overline{\sigma_{\beta_1'}}$	$\overline{\beta_1'} - \overline{\beta_1}$
2	1.400	0.125	7.470	0.063	6.070
3	1.608	0.147	5.899	0.089	4.291
6	1.636	0.112	5.642	0.068	4.006
28	2.095	0.195	4.097	0.077	2.002
26	2.970	0.175	5.817	0.084	2.847
25	3.101	0.453	5.660	0.059	2.559

Observation:

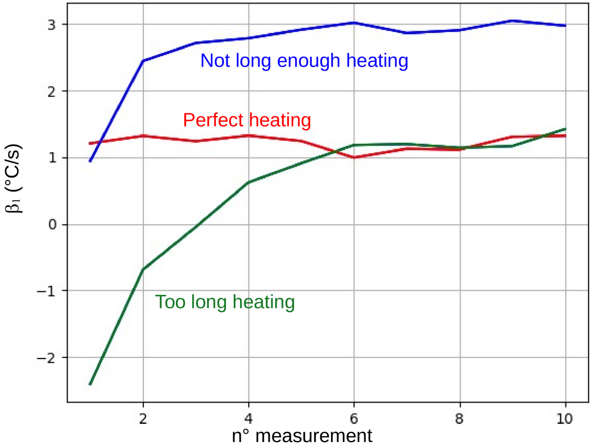
- As before, β_1 increases with backside opening
- In average $\rightarrow$ + 3.3 °C·s^{-1}
- β_1 distributions do not overlap

BYPASSING THE PACKAGE INTEGRITY VERIFICATION

Pre-heating the IC before power-up

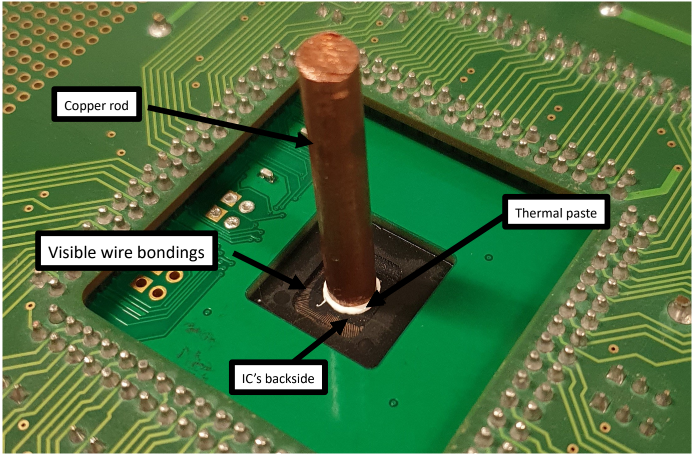


Pre-heating the IC before power-up



- Easy when unlimited boots are allowed
- Can be protected thanks to an initial temperature measurement

Removable heat-sink



Removable heat-sink results (units in °C·s^{-1})

	Intact package		Backside opening		32 mm long rod	
IC №	$\overline{\beta_1}$	$\overline{\sigma_{\beta_1}}$	$\overline{\beta_1'}$	$\overline{\sigma_{\beta_1'}}$	$\overline{\beta_1''}$	$\overline{\sigma_{\beta_1''}}$
26	2.970	0.453	5.660	0.059	0.709	0.047
3	1.608	0.147	5.899	0.089	0.735	0.047
6	1.636	0.112	5.642	0.068	0.708	0.109
28	2.095	0.195	4.097	0.077	0.516	0.073
2	1.400	0.125	7.470	0.063	0.816	0.142
25	3.101	0.453	5.660	0.059	0.714	0.095

Average β_1 reduction of 5 °C·s^{-1}

CONCLUSION

Conclusion

Conclusion

- Secure applications → From smart-cards to microcontrollers

Conclusion

- Secure applications → From smart-cards to microcontrollers
- µc → Often encapsulated in plastic packages

Conclusion

- Secure applications → From smart-cards to microcontrollers
- µc → Often encapsulated in plastic packages
- Check package integrity against semi-invasive attacks

Conclusion

- Secure applications → From smart-cards to microcontrollers
- µc → Often encapsulated in plastic packages
- Check package integrity against semi-invasive attacks
- By using the embedded temperature sensor:
  - Monitoring thermal dissipation during boot

Conclusion

- Secure applications $\rightarrow$ From smart-cards to microcontrollers
- µc $\rightarrow$ Often encapsulated in plastic packages
- Check package integrity against semi-invasive attacks
- By using the embedded temperature sensor:
  - Monitoring thermal dissipation during boot
- Experimental results suggest it is feasible

Conclusion

- Secure applications → From smart-cards to microcontrollers
- µc → Often encapsulated in plastic packages
- Check package integrity against semi-invasive attacks
- By using the embedded temperature sensor:
  - Monitoring thermal dissipation during boot
- Experimental results suggest it is feasible
- Heatsink bypass compensation is tricky

Conclusion

- Secure applications → From smart-cards to microcontrollers
- µc → Often encapsulated in plastic packages
- Check package integrity against semi-invasive attacks
- By using the embedded temperature sensor:
  - Monitoring thermal dissipation during boot
- Experimental results suggest it is feasible
- Heatsink bypass compensation is tricky
- All of this with a sensor with a limited accuracy (± 1.5 °C)