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

J. Toulemont, G. Chancel, F. Mailly, P. Maurine
and P. Nouet

University of Montpellier, CNRS, LIRMM
161 rue Ada
34095 Montpellier CEDEX 5, France

Abstract. Among the various threats to secure ICs, many are semi-invasive in the sense that their application requires the removal of the package to gain access to either the front or back of the target IC. Despite this stringent application requirements, little attention is paid to embedded techniques aiming at checking the package's integrity. This paper explores the feasibility of verifying the package integrity of microcontrollers by examining their thermal dissipation capability.

Keywords: Security, hardware, fault attacks, reverse-engineering, countermeasure, thermal dissipation monitoring

1 Introduction

During the design of secure integrated circuits, it is important to address numerous threats and potential attacks as early as possible in the standard design flow. These include side-channel attacks, fault attacks, reverse-engineering, and counterfeits, to name a few.

1.1 Context and related works

These threats and attacks are considered non-invasive if they do not require any contact with or modification of the target device. If their application involves modifying the device, they are considered invasive. Eventually, they are classified as semi-invasive if it is necessary to remove either the front or back part of the package using mechanical and chemical means before application.

Among semi-invasive attacks, one can identify some probing attacks [1, 3], laser fault injection (LFI) [5], Body Bias Injection (BBI) [14], electromagnetic (EM) side-channel or fault attacks [12] often performed , after package removal, with tiny probes really close to the IC surface for a better efficiency, etc.

Numerous embedded countermeasures have been proposed in the literature to increase resilience against semi-invasive attacks or reverse-engineering. While not exhaustive, some of these countermeasures aims:

- At detecting probing attacks, which consist in the direct measurement of some compromising signals by means of e-beams or a probing station directly in the target IC whose front panel has been removed. These countermeasures often consist of adding an active metal grid (called a shield) [7] in the top metal layers of ICs, grid whose electrical properties (e.g. its impedance or response to a specific stimulus) are monitored periodically or during IC boot-up.

- At detecting the presence of an EM probe in the close vicinity of the IC frontside. A possible solution to that aim has been proposed in [8] and consists in monitoring the resonance frequencies of some embedded loops which are modified by the proximity of a solenoid used by an adversary to perform an EM side-channel or fault attack. Again, the resonance frequencies are checked periodically or during the IC boot.

- At detecting the thinning of the substrate, a common practice to better concentrate the laser beam during LFI. According to [10], this can be achieved by adding etched holes into the substrate that weaken the substrate structure so that it breaks when mechanically polished. This can also be achieved by designing a shield penetrating the substrate thanks to the use of Through Silicon Vias (TSV) and metal wires [4]. Again, the electrical characteristics of the shield are checked during the boot.

- At reflecting as suggested in [13] the laser beam using micro-mirrors, with a random pyramidal shape, embedded in the substrate. These mirrors are called nano-pyramids.

- At integrating specialized embedded sensors detecting the occurrence of an EM pulse [6] in the vicinity of the chip, or a laser pulse [11], or an unexpected current in the substrate [2], or a voltage pulse on the power pads, etc.

All these embedded solutions require additional structures in ICs, resulting in significant area and cost overheads. It should be noted that solutions enabling the detection of intrusions by the backside of the IC are particularly expensive since they require the use of optional processing steps (such as TSV or nano-pyramids), which are only available in advanced CMOS technologies.

Eventually, up to the best of our knowledge, no solution has been proposed to check the integrity of the packaging instead of detecting a specific phenomenon (such as a parasitic current, a laser pulse, ...) induced by an intrusion attempt. This lack is perhaps a legacy of smart cards whose packaging is reduced to its strict minimum (a piece of plastic), or to the will of some manufacturers to protect their countermeasures by keeping them secret. As a reminder, the disclosure of a countermeasure has a direct impact on the Attack Potential score during an AVA_VAN (assurance vulnerability analysis) evaluation.

However, with the proliferation of secure applications in various domains, many ICs and especially microcontrollers are now exposed to hardware threats

and attacks. It is therefore conceivable that specific embedded solutions could be developed to verify the integrity of the package during the boot sequence of ICs, such as microcontrollers, or to verify the integrity of a system as a whole in the case of a package-on-package integration, which is very common in mobile applications. This is all the more justified as common or complex packages are designed for different purposes, one of those being to facilitate the dissipation of the heat generated by the circuit operation. For this purpose, common packages (QFP, QFN, ...) embed a heat sink that must be removed in order to gain access to the IC backside.

Objective and contributions

While temperature has been pointed out as a potential side-channel vulnerability [9], to the best of our knowledge, there has been no work aimed at exploiting the thermal behavior of ICs to thwart physical attacks, although modern microcontrollers often include a temperature sensor (STM32, Kinetics, etc). Within this context , this paper aims to determine if one can envision exploiting such a sensor to check the integrity of the package by monitoring heat dissipation during the IC boot. This study, which aims to establish a low-cost countermeasure against semi-invasive attacks, has been done on an STM32F439 microcontroller, considered as our case study for the rest of the paper.

Experimental results reported in this paper suggest that with such a temperature sensor (which has moderate performance and seems to be calibrated after fabrication), one can envisage verifying the integrity of the backside of the package by performing a procedure at the end of each boot that takes less than 0.3 second to complete.

In addition to this, the paper also reports data related to the efficiency of obvious solutions adversaries could use to bypass the proposed countermeasure.

Paper organization

Section 2 reports information related to the Device Under Test (DUT) that is necessary for the reading of the paper. Section 3 describes and justifies the embedded software procedure developed to monitor heat dissipation of the DUT. The latter procedure only uses the embedded temperature sensor and the RAM of the DUT. The effect of removing the frontside or the backside of the package are then reported and analyzed in section 4. Finally, natural solutions potentially allowing to bypass the package integrity check are tested in section 5 before concluding in section 6.

2 The Device Under Test

The chosen test case for our study is the STM32F439. The latter is designed in 90nm CMOS technology around an ARM Cortex M4. It occupies a silicon area of about $4.4mm \times 5.5mm$ and contains several cryptographic modules but also a

temperature sensor with a resolution of $\pm 1.5^oC$, operating between -40^oC and $+125^oC$. Its maximum sampling rate is about 100 kS/s, it can thus provide a measure each 10 µs, the time to convert its analog response into a 12 bits digital value.

Because of fabrication process variations, it is recommended to use it to monitor temperature changes rather than getting absolute temperature values. However, the effect of these variations can be partially mitigated thanks to calibration values, TS_CAL1 and TS_CAL2, which values are measured during post fabrication calibration and stored inside each device. They allow getting a better estimate of the current temperature with eq. 1, in which $valTS$ is the temperature measurement provided by the integrated sensor and T^o the actual temperature after correction.

$$T^o = \frac{80}{TS\_CAL2 - TS\_CAL1} \cdot (valTS - TS\_CAL1) + 30 \tag{1}$$

In our case study, the STM32F439 is encapsulated in a $20mm \times 20mm$ LQFP-144 package. The heat dissipation capabilities of this package are represented Fig. 1 in which θ_F, θ_B are the frontside and backside thermal resistances respectively.

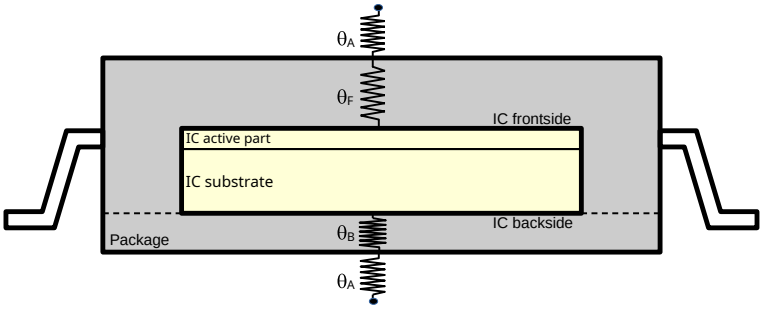

Fig. 1. Thermal dissipation of LQFP packages

The thermal resistance values (in $^\circ C \cdot W^{-1}$) of such packages typically follows the relation: $\theta_F >> \theta_B$, because of the presence of an embedded metal heat sink inside the package on the IC backside. Thus, an attacker aiming at removing the package to get access, either to the IC frontside or the backside, necessarily removes θ_F or θ_B, that is to say set θ_F or θ_B equals to zero.

3 Monitoring the thermal dissipation capability

The method to monitor the thermal dissipation capability of the DUT has been established after several experiments performed to better understand its thermal behavior assumed to be standard and shared with many ICs, at least those

encapsulated in the same package. This section describes the performed experiments and the results we obtained. Eventually, the monitoring method, that must be fast, is introduced. Indeed, it is not acceptable to notably extend the IC boot sequence to check for the package integrity.

3.1 Analysis of the thermal behavior

This section describes the successive experiments that have led us to the proposed embedded solution for checking the package integrity during the IC boot. The latter is described at the end of this section.

3.2 Preliminary tests

The first experiments aimed at observing differences between thermal behavior of ICs in non-tampered packages and in their counterpart with either frontside or backside removed. For this purpose, changes of temperature were monitored during a sequence which alternately wrote words into the flash memory for 180 seconds and remained idle for 180 seconds. It should be noted that the first phase of writing was set to start 180s after power on.

Measured temperature changes with respect to the initial temperature are reported in Fig. 2 for three DUTs :

- one in an non-tampered package (black),
- one in a package with a frontside opening (blue),
- and one in package with a backside opening (red).

For clarity, a moving average (with a window of 50 points) has been applied to the raw temperatures to reduce the effect of the sensor intrinsic noise and low accuracy. As one can observe, the IC temperature increases slowly after power-up and more sharply when flash memory writing starts. All chips demonstrate a similar periodic variation of their temperature which are representative of alternate writing and idle sequences. However, one can easily observe that the amplitude of temperature changes is significantly affected by the backside package removal. For an non-tampered package or a frontside opening of the package, amplitude of the temperature variations is about 3°C, while it is almost doubled for a backside opening of the package. In addition, it can also be observed that the waveforms of the temperature changes is close to a square wave, a clear indication that the temperature change is fast enough to allow a quick detection of package removal.

From this preliminary experiment, we may conclude that creating an opening on the backside of the package, and thus destroying the heat sink, has a significant impact on the thermal behavior of such ICs. On the contrary, the effect of opening the frontside is much more limited. In addition, it can also be observed that the waveform of temperature changes is close to a square wave, a clear indication that the temperature changes are fast. In fact, it takes less than 30 seconds for the temperature to reach 90% of the semi-permanent state,

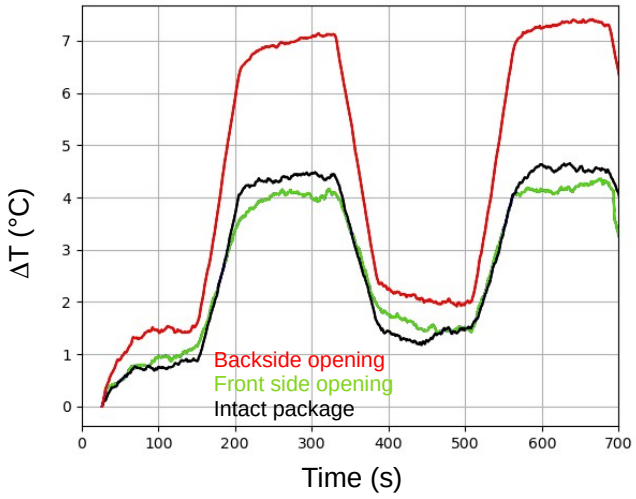

Fig. 2. Temperature changes, ΔT (^oC), for an IC in an intact package (black), in a package with a frontside opening (green) and with a backside opening (red).

depending on the state of the package. This encouraging observation led us to analyze the temperature transient that occurs just after IC power-up. Indeed, as shown in Fig. 2, the temperature of the IC with a backside opening rises much faster than the one of an IC in an non-tampered package or a frontside opened package.

3.3 Temperature transients at power-up

To monitor the temperature transients at power-up, we sampled the latter at 83333 samples per second, i.e. with one measurement every 12 µs. Fig. 3 shows the observed linear temperature trends obtained for the same three ICs previously characterized in Fig. 2. However, the slope of the temperature variation with time is significantly greater (by about 3°C/s) for a DUT with a backside opening. As a result, whether the package is intact or not, the temperature at power up can be modeled as follows:

$$T^o = \beta_1 \cdot t + \beta_0 + \epsilon \tag{2}$$

with ϵ being a modeling error, β_1 the line slope, and β_0 the line constant coefficient.

3.4 Thermal dissipation metric at boot

From the results above, it appears that the slope β_1 of the temperature transient is a good metric for checking the integrity of the package. A simple way to obtain

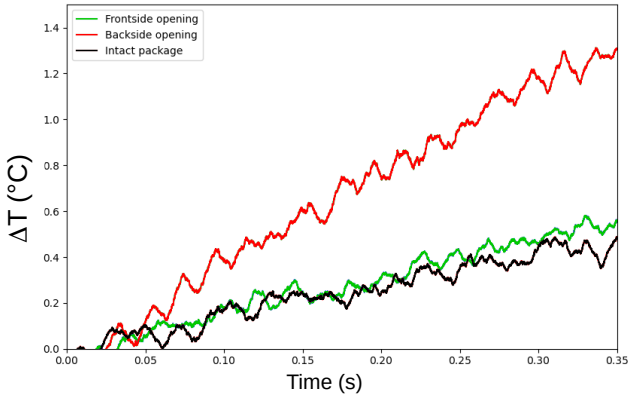

Fig. 3. Temperature changes during the first 0.35s after power-up for ICs in an intact package (black), a package with a frontside opening (green) and a package with a backside opening (blue).

this is to perform a linear regression of the temperature values provided by the embedded temperature sensor against time during IC boot. This results in the calculation of:

$$\beta_1 = \frac{cov(T^o, t)}{V(t)} \tag{3}$$

with V(t) being the variance of the temperature, and $cov(T^o, t)$ representing the covariance between temperature and time, which can be easily obtained on-chip using accumulators (registers) that store only the sums involved in the computation of means:

$$\beta_1 = \frac{\overline{T^o \cdot t} - \overline{T^o} \cdot \bar{t}}{\overline{t^2} - \bar{t}^2} \tag{4}$$

The soundness of the linear model can also be checked by computing the coefficient of determination, R^2. Its value ranges from 0 to 1 and is calculated using the following expression:

$$R^2 = \frac{cov(T^o, t)^2}{V(t)V(T^o)} = \frac{(\overline{T^o \cdot t} - \overline{T^o} \cdot \bar{t})^2}{(\overline{t^2} - \bar{t}^2) \cdot (\overline{T^{o\,2}} - \overline{T^o}^2)} \tag{5}$$

The closer the value is to 1, the better the linear model reflects temperature changes over time. However, in our case, since the variance of temperature measurements is part of the denominator, R^2 is thus necessarily limited by the accuracy of the temperature sensor. In fact, R^2 is the ratio of the variance (of the temperature) explained by the model to the total variance. It is also the square of the Pearson correlation $\rho(T^o, t)$. Therefore, if there is no linear increase or decrease in temperature (an unlikely scenario in our context), the value of R^2 should be close to 0.

An embedded code has been written and stored in each DUT. It provides both β_1 and R^2 measurements . For this purpose, after power-on and during 300 ms, the temperature values are measured every 25 µs by the embedded sensor and are then stored in RAM. The value of 300 ms was empirically found to be sufficient to make the heat dissipation caused by the processing and RAM storage measurable with a sensor of such accuracy. Of course, it is possible to write embedded code that calculates β_1 values more quickly, but the aim of this work is not to calculate quickly, but rather to measure the slope of the temperature rise at start-up. Therefore, the number of RAM write operations (and thus the duration of the measurement phase) should be adapted to the device and to the sensor accuracy.

4 Impact of package removal : experimental results

This section presents initial experimental evidence of the ability to verify the integrity of the backside of the package during IC boot thanks to thermal dissipation. This initial evidence is supported by additional experiments conducted at various ambient temperatures using a climatic chamber. Experiments were also conducted on overpowered and underpowered ICs operating at room temperature.

4.1 Experimental results at room temperature

We applied the embedded package integrity verification process to 13 devices, 7 of which have a backside opening. Table 1 shows the means and standard deviations of the β_1 and R^2 distributions obtained for each IC after 25 power-ups. Note that ICs were left in idle mode for 30s between each power-up to avoid any cumulative effect due to the small time constant of thermal transients that might have distorted the verification process.

The $\overline{\beta_1}$ values for ICs with a backside opening are significantly higher (by about $3^oC/s$ for the average value) than those for ICs without backside opening. This is clear evidence that ICs with a backside opening heat up more than the others during power-up. Standard deviations, σ_{β_1}, range from 0.15 to $0.3^oC/s$, a rather small value compared to the gap between the $\overline{\beta_1}$ values obtained for ICs with and without a backside opening. Consequently, $\overline{\beta_1}$ seems to be a reliable metric for checking the package integrity.

The same conclusion could be drawn for $\overline{R^2}$. However, due to the limited accuracy of the embedded temperature sensor, the difference between the values obtained for ICs with and without a backside opening is very limited, especially regarding the values of σ_R. However, one can expect to get higher (smaller) values of $\overline{R^2}$ (σ_R) with a more accurate temperature sensor. As a result, $\overline{\beta_1}$ appears to be a good indicator to identify a missing backside of the package. If the sensor had a better accuracy, $\overline{R^2}$ could have been an alternative indicator.

Regarding values listed in Table 1, we might be tempted to compare the values obtained for the two sets of ICs (with and without a backside opening)

Table 1. Average values and standard deviation of 25 measurements of β_1 for the same IC batch before and after package opening. Units are expressed in °C·s^{-1}.

IC n°	$\overline{\beta_1}$	$\overline{\sigma_{\beta_1}}$	$\overline{R^2}$	$\overline{\sigma_{R^2}}$	Backside Opening
25	0.93	0.23	0.01	0.0	no
3	1.40	0.15	0.06	0.01	no
12	1.82	0.2	0.18	0.08	no
6	2.18	0.19	0.08	0.01	no
2	2.50	0.32	0.17	0.15	no
26	2.97	0.16	0.06	0.01	no
9	3.96	0.16	0.34	0.02	yes
7	4.56	0.14	0.28	0.02	yes
1	3.43	0.16	0.09	0.01	yes
10	4.34	0.19	0.14	0.1	yes
8	4.84	0.22	0.23	0.08	yes
11	6.53	0.24	0.39	0.09	yes
4	6.34	0.15	0.44	0.08	yes

and see if the $\overline{\beta_1} + 3\sigma_{\beta_1}$ of all ICs with an intact package are lower than all $\overline{\beta_1} - 3\sigma_{\beta_1}$ of all ICs with a backside opening. However, this would create an overlapping gray area that could be a source of false alarms due to process variations from one IC to another. This limitation can easily be overcome if a post-fabrication characterization of $\overline{\beta_1}$ is undertaken in a trusted environment for each IC with its non-tampered package. An opening in the backside of the package at a later moment will then affect thermal dissipation, thus increasing $\overline{\beta_1}$ in a deterministic way due to an increase of the thermal resistance between the silicon chip and the air surrounding the package. Finally, reported $\overline{\beta_1}$ variation in Table 1 are more evidence of the effect of process variations at the IC, package, and board levels. This point is supported by additional data in the next section.

This analysis has consequences on how IC package integrity check should be performed. In fact, it is necessary to measure for each IC the $\overline{\beta_1} \pm 3\sigma_{\beta_1}$ after manufacturing and to store these values in an embedded non-volatile memory, as it is done for the embedded temperature sensor (through TS_CAL1 and TS_CAL2 mentioned previously). These values will then be considered as the upper and lower acceptable bounds for any measurement of β_1 during further boots during IC life.

4.2 Experimental results at different ambient temperatures

To further support the idea that thermal monitoring could be a way to detect a backside opening of an IC package, the effect of ambient temperature on the embedded measures of β_1 was analyzed. The idea was to verify that β_1 is indeed a reliable metric for checking package integrity. Twenty β_1 values were therefore collected for two ICs placed in a climatic chamber with temperature set successively at 15°C and 45°C. Again, ICs were left in idle mode for 30s between each

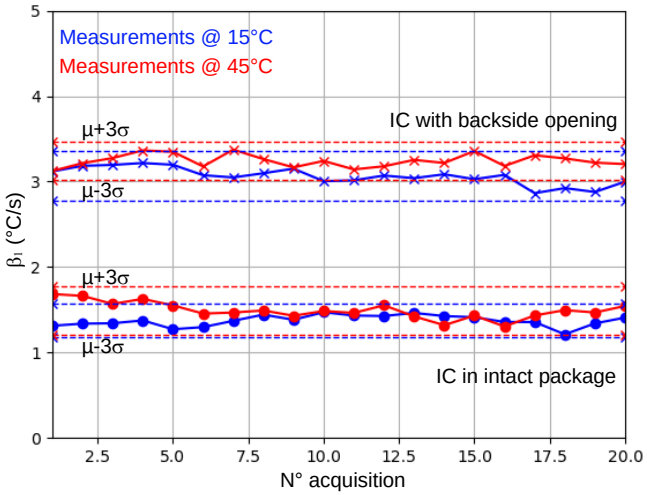

Fig. 4. Effect of ambient temperature on β_1 for two ICs : one had its package intact, the other had a backside opening.

power-up. One of them had its package intact, the other a backside opening. This range, that could be perceived as limited, has been chosen to prevent our ICs and PCBs from being damaged by heat and humidity, as we cannot control the latter with our piece of equipment.

Fig. 4 reports the values of β_1 obtained for these two ICs over 20 power-ups. The influence of the ambient temperature (at least a change of 30°C) seems to be very limited. The means and the standard deviations are in the same order of magnitude than the ones reported in Table 1. This is not too surprising. In fact, β_1 is an indirect measure of the thermal resistance of air and the material of which the package is made of, which are not expected to change much over this temperature range.

In support of this claim, we periodically measured β_1 for an IC in an non-tampered package over a period of 120 hours (five days). One measurement was taken every 120s. At the same time, the ambient temperature in the test room is recorded as well as the internal temperature of the device at the beginning and at the end of the β_1 measurement process. Figure 5 illustrates the results. As can be seen, room temperature varied between 21°C and 25°C during these five days, while the internal temperature varied jointly with the latter between 23°C and 28°C. Correlations between the room temperature and the internal temperature at the beginning and at the end of the β_1 measurements are indeed equal to 0.96 and 0.97. During the same experiment, β_1 varied almost completely incoherently with the room temperature around its mean (1.71), as supported by the value of the correlation between them: -0.22. A linear regression between the room temperature and β_1 showed that β_1 decreases by 0.01 for an increase of one degree Celsius in the room temperature, as illustrated in Fig. 6.

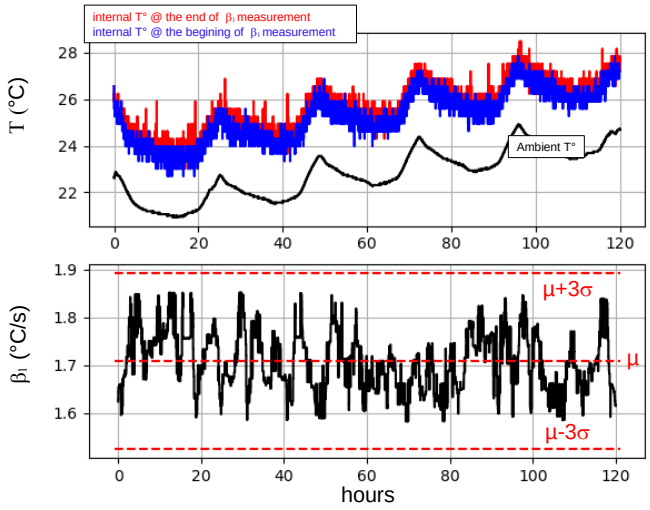

Fig. 5. Measurements of β_1 and of the ambient and internal temperatures over 120h for an IC in an intact package.

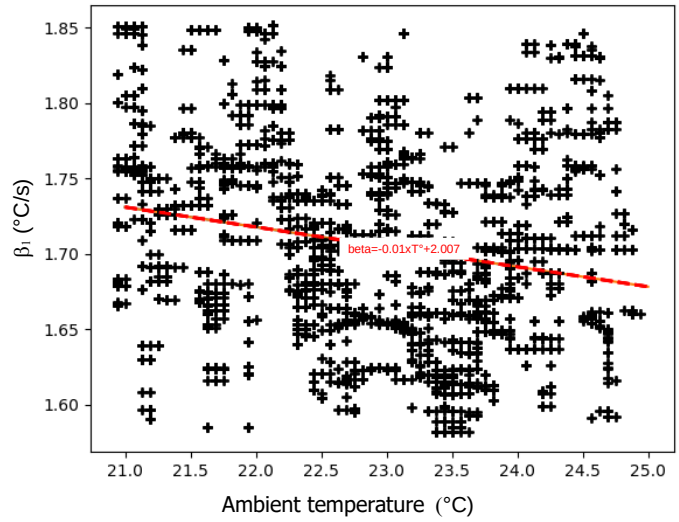

Fig. 6. The effect of the ambient temperature on β_1 measured during 120 hours.

Thus, for an increase of 30 °C, as it is the case in the preceding experiment, one can expect an increase of β_1 by 0.3 °C/s. This is what could be observed in Fig. 4. As a result, the reduced effect of room temperature on β_1 can be neglected unless:

– The device can experience large changes ($> 30°C$) of ambient temperature in its application context,
– The accuracy of the embedded temperature sensor used to verify package integrity is about 0.01°C.

In these extreme cases, the upper and lower acceptable values of β_1 that allow the package integrity check should be defined according to the internal temperature of the IC at the beginning of the verification process. This has an additional cost in terms of IC customization after its fabrication. In other cases, most of the variance of β_1 is due to (explained by) the measurement errors done by the embedded sensor.

4.3 Experimental results at different supply voltages

Similarly, we studied the impact of the supply voltage, V_{dd}, variations of which are expected to change the heat dissipated by ICs in a quadratic way, since the power dissipation of ICs is proportional to $f_{ck} \cdot V_{dd}^2$ where f_{ck} is the clock frequency. Two ICs were used in the experiment: one with an intact package and one with a backside opening. Ten measurements of β_1 were performed for each IC while the ICs were supplied by either 3V, 3.3V or 3.6V. Again, the idea was to verify that β_1 remains a reliable metric for checking package integrity over a range of supply voltage conditions.

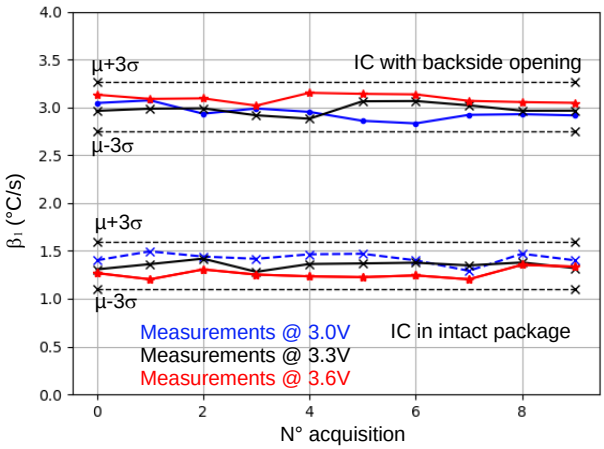

Fig. 7. Effect of supply voltage changes on β_1 : 10 measurements of β_1 for two ICs : one with an intact package, one with a backside opening of the package

Fig. 7 shows variations of β_1 during this experiment. For both circuits, variations of β_1 remain less than three times the standard deviations reported in the

previous section. This was not a surprising result due to an on-chip regulator which is incorporated inside the DUT as in most modern microcontrollers. As a matter of fact, whatever is the supply voltage, power dissipation remains almost constant except the thermal dissipation of the regulator. We could not confirm this hypothesis because the on-chip regulator on the STM32F439 in LQFP144 package cannot be disabled (there is no $BYPASS\_REG$ pin).

4.4 Final validation

To further support the proposed package verification technique, we decided to perform experiments on different ICs before and after the opening of their backside. To that end, six ICs were selected: №2, 3, 6, 28, 26 and 25. For each of them, the experiment shown in Table 1 have been performed, first with the package intact and then with the backside removed. The results obtained are given in Table 2.

Table 2. Average values and standard deviation of 25 measurements of β_1 for the same IC batch before and after package opening. Units are expressed in °C·s^{-1}.

	Intact package		Backside opening		
IC n°	$\overline{\beta_1}$	$\overline{\sigma_{\beta_1}}$	$\overline{\beta_1'}$	$\overline{\sigma_{\beta_1'}}$	$\overline{\beta_1'} - \overline{\beta_1}$
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

Similar to the previous experiments, the β_1 values increase when the IC backside is removed. On average, they increase by 3.3 °C·s^{-1}, which is very similar to the previous observations and supports the proposed technique. Furthermore, it can now be seen that the β_1 distribution of an IC after backside opening does not overlap with the distribution obtained with its intact package. Therefore, the probability of not detecting the opening is limited.

4.5 Partial conclusion

At this stage, it seems possible to detect a backside opening of the package by monitoring the heat dissipation capability of ICs with β_1 as metric. This metric appears to be stable with room temperature variations (at least between 15°C and 45°C) and supply voltage variations (at least if the IC integrates an on-chip regulator). To overcome die to die variations due to process variations, we have proposed to store two additional values, $\overline{\beta_1} - 3 \cdot \sigma_{\beta_1}$ and $\overline{\beta_1} + 3 \cdot \sigma_{\beta_1}$, into a secure

non-volatile memory after manufacturing, and measuring β_1 at the end of each boot to verify that β_1 falls within the expected range. It is worth noting that the proposed add-on for backside package integrity testing is fully electrical and can be implemented by a few lines of code incorporated in the boot sequence that will store detection margins during first boot and secure backside of the package for the entire life of the microcontroller. Of course, such a countermeasure, as many others, could be still bypass using fault injection attack targeting the verification process or the thermal sensor. However, the presence of this countermeasure forces the adversary to successfully perform a preliminary fault attack before attacking cryptographic applications or other sensitive applications.

Of course, such countermeasure could still be bypassed using fault injection attacks targeting the thermal or the sensor verification process. However, the mere presence of this countermeasure forces the adversary to successfully perform a preliminary fault injection before attacking other sensitive ICs regions.

The response to the detection of an intrusion is not discussed in this work, as it could vary depending on the application. In fact, without being exhaustive, it could range from a total FLASH memory erasure, to a limitation of the user's privileges, or again to a halt in the boot process. In the latter case, a digital counter (in secure non-volatile memory), could be incremented so that if too many intrusion attempts are made, a FLASH erasure is performed.

Let us now switch our role from secure IC designers to that of malicious adversaries, fully aware of the presence of this embedded countermeasure in the target IC, that want to bypass it using tools commonly available in security characterization laboratories. Several methods come to mind. We have tested some of them and found three that can be sometimes successful. Those that sometimes gave positive results, i.e. bypassed the countermeasure, are presented in this section.

5 Bypassing the package integrity verification

5.1 Fast successive power-ups and power-downs

As previously explained, the verification is based on the measurement of the heat dissipation capability during the first 0.30 seconds after power-up. This verification procedure has been defined considering that the IC is at room temperature before being turned on. This explains why each measurement in previous sections was immediately followed by 30s in the idle mode to allow chip cool-down.

One may thus wonder what might happen if the target IC is not at room temperature when it is turned-on. In other words, is there a way to bypass the countermeasure by using successive power-ups, each one interrupted before the end of the package verification process?

For the purpose of verification, an IC in a package with a backside opening (with its $\overline{\beta_1}$ close to 3) was forced to undergo a rapid sequence of power-ups and power-downs. Figure 8 shows the first 10 β_1 values when the measurements are separated by $\Delta m = 1s,\ 3s,\ 10s$ instead of $\Delta m = 30s$ as previously. Experiments were repeated three times.

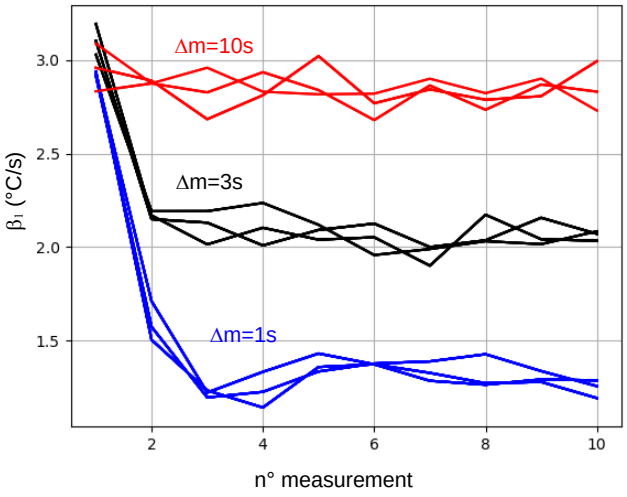

Fig. 8. Ten first measurements of β_1 provided by the IC when the measurements are separated by $\Delta m = 1s,\ 3s,\ 10s$ instead of $\Delta m = 30s$.

One can notice that the coefficient starts to drop as soon as the duration between each measurement is not long enough (i.e. is lower than 3s) and reaches a coefficient similar to the one of a circuit with an non-tampered package when measurements are separated by only 1s. However, the first two measures are not in the range of validity for a circuit with an non-tampered package. Thus, to bypass the countermeasure, the adversary has to stop at least the two first boot sequence before the end of the package integrity verification. This is not so easy to do even if the adversary is aware of the countermeasure. Thus the countermeasure still makes semi-invasive attacks more difficult to perform.

5.2 Pre-heating the IC before power-up

Like the previous bypass method, the one discussed in this section exploits the same major weakness of the proposed package integrity verification method, namely the need to stabilize at room temperature before powering up. The idea is to use a hot air station, a very common piece of equipment in electronics laboratories, to heat the circuit above room temperature before powering it up, so as to lower β_1 down to an acceptable range for an IC in an non-tampered package. The main difficulty for the adversary is, of course, to choose the duration and temperature of the hot air flow without any prior knowledge. Therefore, it is necessary to make several attempts. We were able to bypass the countermeasure after 10 to 15 attempts, depending on the target IC. Therefore, if an unlimited number of boots is possible, this method seems very easy to use. However, with a limited number of attempts, the game becomes more risky and difficult. One

can easily imagine that an alarm during package integrity verification will at least temporarily block IC operation.

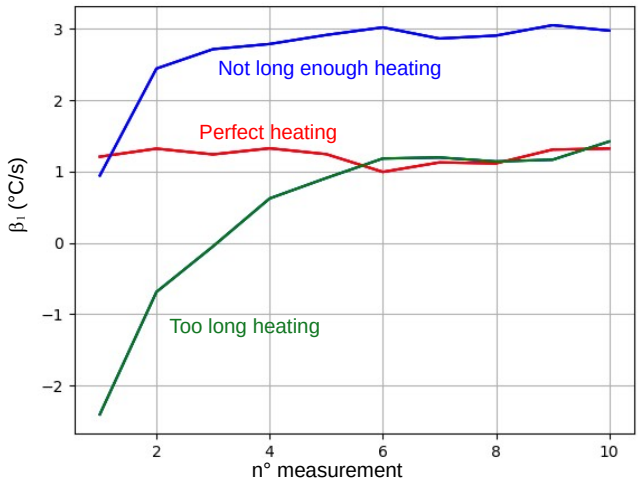

Fig. 9. Evolution of β_1 after an initial heating of the DUT with an hot air station.

In fact, if the circuit is too hot at power-up, it will cool down instead of heating up during the boot sequence. This results in forcing the first three measurements of β_1 to be negative, as shown in Fig. 9 (green curve), which shows the first 10 measurements of β_1 for an IC in package with a backside opening. Conversely, if the circuit is not enough heat up, most of β_1 measurements are likely to remain in the range of a circuit with a backside opening of the package (blue curve). Finally, if the heating conditions are perfect (both in duration and temperature), the countermeasure will be bypassed (red curve). Note also the increase of β_1 during the successive measurements. After 10 measurements, the junction temperature is not in its steady state, except for the red curve.

These results show that there is room for improvement in the package verification procedure to make it more robust against a hot air station bypass attempt. In fact, an initial on-chip temperature measurement can be easily used to detect the bypassing attempt using pre-heating.

5.3 Removable heatsink

A final way to bypass the package integrity verification countermeasure consists in placing a removable heatsink in contact with the IC backside (i.e. substrate), during power-up and β_1 verification. Then, one could remove it to perform fault injection attacks.

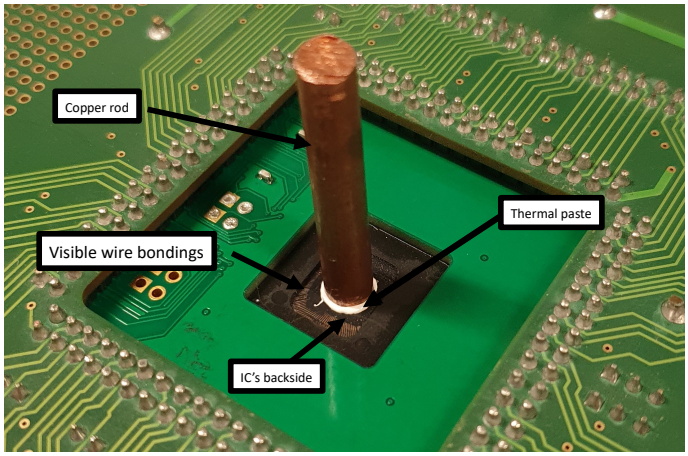

Fig. 10. The copper rod used as a removable heatsink.

As a demonstration, we placed a 32mm long and 3mm wide copper cylinder with some thermal interface material as shown in Fig. 10 to try to replicate approximately the heat sink suppressed by the opening operation. The copper rod was estimated to have a 3 °C·W^{-1} thermal resistance. Then, we performed β_1 measurements with the heatsink on the IC batch considered in section 4.4, i.e. ICs that were characterized before and after the backside opening procedure. Table 3 shows the results, where $\beta_1^{''}$ stands for the value of β_1 measured in presence of the copper rod.

Firstly, it should be observed that the discrepancies between $\overline{\beta_1}$, $\overline{\beta_1^{'}}$ and $\overline{\beta_1^{''}}$ for a small set of ICs are significant. This confirms that defining an acceptable range of β_1 to check package integrity must be done considering die to die variations. It is therefore imperative to define an unique acceptable range for each IC after manufacturing and packaging since, as mentioned previously, removing the backside is expected to have a significant and deterministic effect on the IC thermal dissipation. The related additional cost induced might seem prohibitive, but in fact, is not, as such customization process is already used to calibrate the embedded temperature sensor (TS_CAL1 and TS_CAL2 values).

Secondly, it should be noted that adding the copper rod and the thermal interface material reduces the average value of β_1 by about 5 °C·s^{-1}. This reduction is too important to bypass the proposed package detection technique. In fact, the distribution of $\beta_1^{''}$ of all ICs has a mean value too low to overlap with that of β_1, i.e. the one of ICs in their intact package. Therefore, the probability of obtaining a legitimate β_1 value during a boot is quite low.

One can of course choose a different heatsink provoking a smaller $\beta_1^{''}$ values reduction. However, this requires skill and knowledge about the DUT, so it is not straightforward. In addition to this, it is made all the more difficult by the fact that it seems impossible to select a heatsink that can be used for all ICs due to significant die-to-die variations.

Table 3. Average values and standard deviation of 25 measurements of β_1 for the same IC batch with the copper rod heatsink. Units are expressed 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

Despite these difficulties, it is still possible for an adversary to bypass the countermeasure, either thanks to luck or skill. In this case, it should be noted that the thermal interface material is mandatory to effectively make a significant physical contact between the IC backside and the copper rod. Therefore, it appears possible to bypass the countermeasure, but the thermal interface material must be removed, without powering down the IC, before attacks can be carried out.

6 Conclusion

The spread of secure applications from smart cards to microcontrollers (IoT), which are encapsulated in plastic packages, raises the issue of verifying package integrity to thwart semi-invasive attacks; a topic which has not, up to the best of our knowledge be addressed up to now. We investigated the possibility of checking the integrity of the packaging using an embedded temperature sensor, a very common block in modern microcontrollers, to monitor at power-up the thermal dissipation of ICs. Experimental results reported in this paper suggest that it is possible to detect the creation of a backside opening during the boot sequence of microcontrollers. This is all the more encouraging as the sensor in question has a limited accuracy (± 1.5 °C). Further work will consolidate these preliminary results and investigate the possibility of detecting the frontside opening of the package using a more accurate sensor, as well as the possibility of detecting fault injection attacks at runtime.

References

1. Ross Anderson and Markus Kuhn. Tamper resistance – a cautionary note new. In 2nd USENIX Workshop on Electronic Commerce (EC 96), Oakland, CA, 1996. USENIX Association.
2. R. Possamai Bastos, F. Sill Torres, J.-M. Dutertre, M.-L. Flottes, G. Di Natale, and B. Rouzeyre. A bulk built-in sensor for detection of fault attacks. In

2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pages 51–54, 2013.
3. Christian Boit, Rudolf Schlangen, Uwe Kerst, and Ted Lundquist. Physical techniques for chip-backside ic debug in nanotechnologies. IEEE Design & Test of Computers, 25, 2008.
4. S. Borel, L. Duperrex, E. Deschaseaux, J. Charbonnier, J. Clédière, R. Wacquez, J. Fournier, J. Souriau, Grégory Simon, and A. Merle. A Novel Structure for Backside Protection Against Physical Attacks on Secure Chips or SiP. In 2018 IEEE 68th Electronic Components and Technology Conference (ECTC), pages 515–520, San Diego, United States, May 2018. IEEE.
5. Jean-Max Dutertre, Vincent Beroulle, Philippe Candelier, Stephan De Castro, Louis-Barthelemy Faber, Marie-Lise Flottes, Philippe Gendrier, David Hély, Regis Leveugle, Paolo Maistri, Giorgio Di Natale, Athanasios Papadimitriou, and Bruno Rouzeyre. Laser fault injection at the cmos 28 nm technology node: an analysis of the fault model. In 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pages 1–6, 2018.
6. David El-Baze, Jean-Baptiste Rigaud, and Philippe Maurine. A fully-digital EM pulse detector. In Luca Fanucci and Jürgen Teich, editors, 2016 Design, Automation & Test in Europe Conference & Exhibition, DATE 2016, Dresden, Germany, March 14-18, 2016, pages 439–444. IEEE, 2016.
7. Ya Gao, Qizhi Zhang, Haocheng Ma, Jiaji He, and Yiqiang Zhao. Eo-shield: A multi-function protection scheme against side channel and focused ion beam attacks. In 2023 28th Asia and South Pacific Design Automation Conference (ASP-DAC), pages 670–675, 2023.
8. Naofumi Homma, Yu ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Makoto Nagata, and Takafumi Aoki. EM attack is non-invasive? - design methodology and validity verification of em attack sensor. In CHES, pages 1–16. Springer, 2014.
9. Michael Hutter and Jörn-Marc Schmidt. The temperature side channel and heating fault attacks. In Smart Card Research and Advanced Applications: 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers, page 219–235, Berlin, Heidelberg, 2014. Springer-Verlag.
10. S. Manich, D. Arumi, R. Rodriguez-Montanes, J. Mujal, and D. Hernandez. Backside polishing detector: a new protection against backside attacks. In Conference on Design of Circuits and Integrated Systems, page 1, 11 2015.
11. Kohei Matsuda, Sho Tada, Makoto Nagata, Yuichi Komano, Yang Li, Takeshi Sugawara, Mitsugu Iwamoto, Kazuo Ohta, Kazuo Sakiyama, and Noriyuki Miura. An ic-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density. Japanese Journal of Applied Physics, 59(SG):SGGL02, feb 2020.
12. Sébastien Ordas, Ludovic Guillaume-Sage, and Philippe Maurine. Electromagnetic fault injection: the curse of flip-flops. Journal of Cryptographic Engineering, 7(3):183–197, 2017.
13. Haoting Shen, Navid Asadizanjani, Mark Tehranipoor, and Domenic Forte. Nanopyramid: An optical scrambler against backside probing attacks. volume ISTFA 2018: Conference Proceedings from the 44th International Symposium for Testing and Failure Analysis of International Symposium for Testing and Failure Analysis, pages 280–289, 11 2018.
14. Karim Tobich, Philippe Maurine, Pierre-Yvan Liardet, Mathieu Lisart, and Thomas Ordas. Voltage spikes on the substrate to obtain timing faults. In 2013

Euromicro Conference on Digital System Design, DSD 2013, Los Alamitos, CA, USA, September 4-6, 2013, pages 483–486. IEEE Computer Society, 2013.

Acknowledgments

This work is supported by the "France 2030" government investment plan managed by the French National Research Agency (ANR), under the project ARSENE (ANR-22-PECY0004).