Backside Polishing Detector: A New Protection Against Backside Attacks

S. Manich, D. Arumí, R. Rodríguez-Montañés
Quality in Electronics Group (QinE)
Universitat Politècnica de Catalunya-BarcelonaTech
Barcelona, Spain
{salvador.manich,daniel.arumi,rosa.rodriguez}@upc.edu

J. Mujal, D. Hernandez
Applus Laboratories - IT Labs
Campus UAB, Bellaterra, Barcelona, Spain
{jordi.mujal,david.hernandez}@applus.com

***Abstract*—Secure chips are in permanent risk of attacks. Physical attacks usually start removing part of the package and accessing the dice by different means: laser shots, electrical or electromagnetic probes, etc. Doing this from the backside of the chip gives some advantages since no metal layers interfere between the hacker and the signals of interest. The bulk silicon is thinned from hundreds to some tens of micrometers in order to improve the performance of the attack. In this paper a backside polishing detector is presented that is sensitive to the thickness of the bulk silicon existing below the transistors, a numerical signature is generated which is related to this. The detector implements built-in self-surveillance techniques which protect it from being tampered.**

***Index Terms*—Attack Detector, Security, TSV, Phase Detector, Built-in Self Surveillance.**

I. Introduction

In the world of security the protection of sensitive information is the cornerstone. In this objective, smart-cards and other specialized products embedded in integrated circuits play a key-role [1].

Integrated circuit technologies provide an implicit physical protection that motivated since late 90s their expansion as robust solutions for security products now. For example, at present nobody discusses the use of smart-cards in electronic payment [2]. Similarly, the new evolution of electronic payment with smart-phones involve the additions of cryptographic chips inside [3]. Alongside with this, the hacking technologies have also evolved. Very early, during development of space technologies in the 70s, it was discovered means to test failures in chips induced by particles in vacuum space [4]. Since this beginning now, these technologies have evolved as powerful tools available for hackers too.

One of the common attacks is the shot of laser beams onto chip [5]. The basic principle consists on the creation of free charges in the transistors and as a consequence to alter the right operation of the circuit. Depending on the case: light color, energy level and focus are tuned to improve the success of the attack. However, on the one hand circuit designers have learned how to mask the active parts against these shots and on the other hand the increase of metal layers in ICs have limited the success of this attack. One alternative to extend the power of laser attacks has been to direct the shots from the backside of the chip [6]. This approach has the advantage to circumvent all metals of the circuit allowing to reach transistors through the bulk glass. Nevertheless, the thickness is large, around 300 µm compared to the front thickness of 15 µm, and thus the laser has to use long wave lengths which limit its effectiveness. This inconvenient could be solved by thinning the backside of the wafer.

Another powerful tool is the optical imaging of the residual photon emission of transistors [7], [8]. In their saturation state, a low intensity photon emission in the band of infrared takes place. This allows mapping the activity of the circuit and locating sensitive parts of secure blocks. This tool does not allow conducting a full attack over a chip but it provides crucial information for the next steps of it. Images are captured from the backside of the chip but the large thickness absorbs most of the photons and thus it is thinned to increase the amount of signal arriving to the camera. Either in the works of [7] and [8] the chip is thinned to 20 µm and to 50 µm respectively.

The boldest backside attack is presented by Helfmeier in [9]. His objective is to remove individual transistors responsible of control signals, vital for the security. This operation has high risks and cannot be done from the front size of the chip unless the integrity of the chip is threatened. The approach is performed in several steps. First the entire chip is polished from 300 to 30 µm. Then, with a FIB machine, a trench is opened covering the area surrounding the targeted transistor. Finally, the transistor is precisely located and it is removed with the same FIB beam.

The reduction of chip thickness is used in standard chip production too. For example, in chip cards it is necessary to comply with card's dimensions. However, as formerly explain it may represent a direct via to access at important elements of the chip, despite the technology sophistication needed is high. One way to tackle with this problem would be to know how much bulk material does have the chip once it becomes active during production test.

In this paper a detector that reacts to the thickness of the bulk material is presented. Its core elements are TSVs [10]. TSVs are the present 3D technology massively used to stack chips, specially multifunction like CPUs and cache memories. Columns of conductive material pass through the silicon moving signals from the active side of the chip to the back-side.

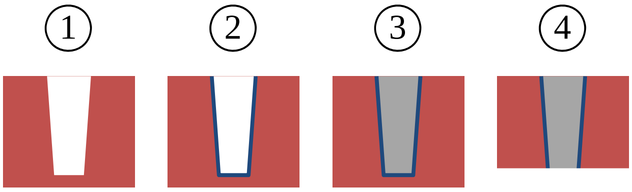

Fig. 1. Main steps of the TSV fabrication process: 1) etching, 2) oxidizing, 3) filling with conductive material and 4) wafer thinning.

They can be fabricated following patterns and, despite they are still expensive, their year production is increasing significantly and therefore their cost is being reduced progressively [11].

Many companies are currently using this technology for the integration of tiers. TSVs can be built before or after the fabrication of the devices and routing layers. Their creation follow these basic steps, see Fig. 1: 1) etching step to drill the holes, 2) oxide deposition to isolate the walls of the column from the substrate, 3) filling of the holes with conductive material (usually poly-silicon or cupper) and 4) thinning of the wafer because TSVs are initially blind and in this last step the tips are opened and made accessible. Presently, manufacturers can fabricate TSVs with the dimension ranges from $5-10$ µm of radius and $50-300$ µm of height.

The rest of the paper is distributed as follows. In Section II the principle of the Backside Polishing Detector (BPD) is presented. Next, in Section III the active part of the BPD is explained, the *delta meter*. Following, the model for the BPD is developed in Section IV and in Section V the results are presented. Finally, in Section VI conclusions are discussed.

II. Principle of the Backside Polishing Detector

As explained in the introduction, the core elements of the Backside Polishing Detector (BDP) are Through Silicon Vias (TSV). For our detector we exploit the parasitic capacitance effect that these structures have with the bulk silicon. Considering the thicknesses of the oxide, between $0.1-0.3$ µm the parasitic capacitances can range from 50 fF to 150 fF.

Different models have been proposed to model the electrical behavior of TSVs, [12]. Basically, they depend on the operating frequency and that for GHz they include the inductive, resistive and capacitive parasitic components. In our case, the BPD is designed to work at very low frequencies, in the range of MHz. As it is explained in [12], at these frequencies the only significant parasitic effect is the capacitive so we have assumed to work with a lumped model consisting of a capacitance connected to ground.

Let's consider the case for a single TSV shown in Fig. 2. A hacker polishes the wafer in order to get closer to the active region of the chip. At different degrees of polishing the value of the parasitic capacitance would become reduced close to a linear trend with the depth of the bulk material removed.

Owing to the cylindrical geometry we can approximate the parasitic capacitance as follows,

$$C_t = c_c \cdot x + C_b \approx c_c \cdot x \qquad (1)$$

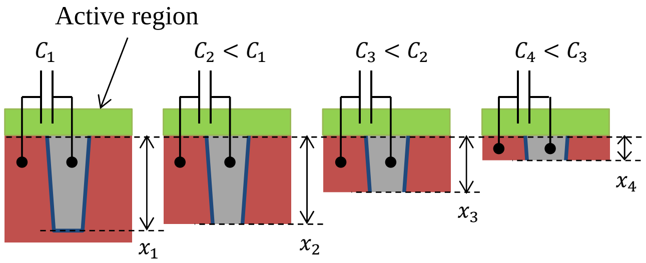

Fig. 2. TSVs present a parasitic capacitance that is proportional to the thickness of the bulk silicon.

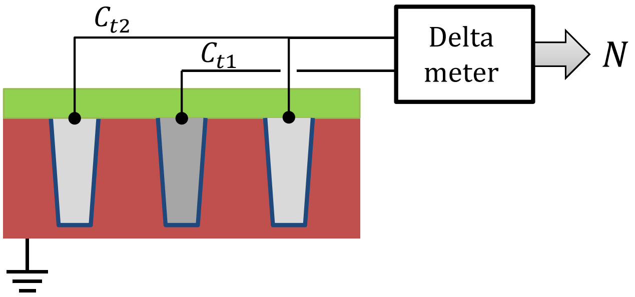

Fig. 3. Principle of the BPD.

where c_c is the unit length capacitance of the cylinder walls, x is the depth and C_b is the capacitance of the base that can be neglected, for its small contribution to the total parasitics and because is the first part to be wiped out during the attack.

In the next section, a circuit is presented that uses this parasitic effect to generate a signature for the depth of the bulk.

III. BPD's Delta Meter

Imagine that a structure consisting of two sets of TSVs is built. Set t1 have a capacitance of $C_{t1} = c_c \cdot x$ and set t2 a capacitance of $C_{t2} = (1+u)c_c \cdot x$, where u is the unbalancing ratio. These sets will present a capacitance difference equal to $C_N = (C_{t2} - C_{t1}) = u \cdot c_c \cdot x$. In Fig. 3 an example of two sets with capacitances $C_{t2} = 2C_{t1}$ is shown, the unbalancing ratio is then $u = 1$. A *delta meter* is designed such that it measures the capacitance difference and outputs a digital signature N proportional to this.

This difference is used to prevent a simple tampering tactic consisting of adding a metalization on the backside of the chip in order to compensate the amount of capacitance lost during the grinding. Owing to these two sets this tampering becomes less trivial, furthermore the geometry of the sets can be planned special such that it makes this tampering even uneasier.

A. Delta Meter

Delta meter is the circuit that implements the transformation $N = f(C_N)$, i.e. it generates a digital signature that is a function of the capacitance difference C_N. The circuit is designed following two main objectives: 1) to be as linear as possible and 2) to have a strong resilience to tampering.

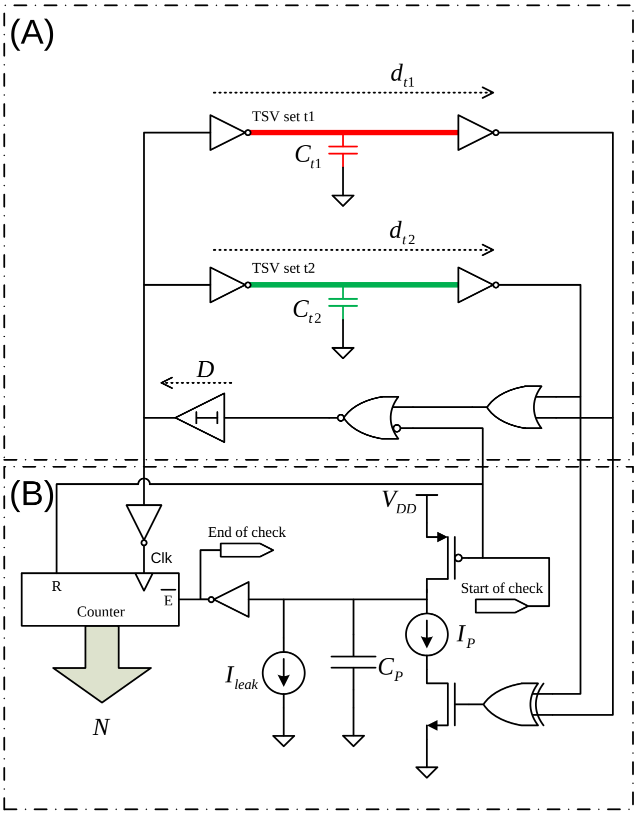

Fig. 4. Schematic of the *delta meter*.

In Fig. 4 the schematic of the *delta meter* is shown. It is composed by to modules (A) and (B). Module (A) is a ring oscillator that excites simultaneous oscillations in the two TSV sets, represented here by the two capacitors C_{t1} and C_{t2}. Module (B) is a phase detector that measures the delay difference of the signals coming from set t1 and set t2 lines and generates the digital signature N. The operation of these two modules is explained hereafter.

1) Module A: It is the core of the detector. It has two different parts: the single line part whose total delay is D and a split part that contains the set t1 line with a total delay of d_{t1} and the set t2 line with a total delay of d_{t2}. When the *start of check* input is ON, the loop of the ring is closed and the oscillation starts. The signal coming from D switches simultaneously the lines controling TSVs in set t1 and set t2.

The transitions coming from D split through both lines and due to the difference in the parasitic capacitances of the two sets, $u \cdot c_c$, the transition in set t2 will arrive later than in set t1, i.e. $d_{t2} > d_{t1}$. Once the transitions cross the output inverters and arrive to the OR gate, they will be combined in the following way: if they are rising, the one coming from the set t1 line (the fastest) will trigger the output of the OR, otherwise if they are falling transitions, the one coming from the set t2 line (the slowest) will trigger the output of the OR gate.

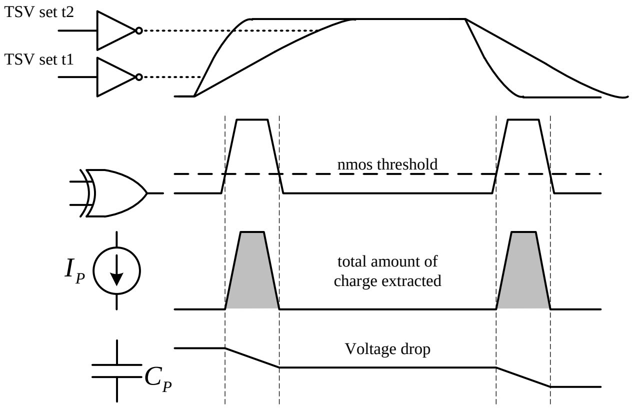

Fig. 5. The phase detector generates a voltage drop in the tank capacitor C_P that is proportional to the time delay existing between set t1 and set t2 lines.

According to this, the period of the ring oscillation is,

$$t = 2D + d_{t1} + d_{t2} \tag{2}$$

The parameters of the ring, i.e. delay D and buffers strength, must be dimensioned to make the signal switching to happen in the full voltage range. Otherwise, the linearity of the *delta meter* would become distorted.

2) Module B: Module B of Fig. 4 is the phase detector. Before starting, the *start of check* signal is at OFF and it closes the pmos transistor which will charge capacitor C_P at a maximum voltage V_{DD} and will also reset the counter to $N = (0...0)_2$. The rest of the elements are the current source I_P whose purpose is to discharge capacitor C_P at a constant current ratio when the nmos transistor is closed, the current source I_{leak} which models the leakage discharge of capacitor C_P and the inverter connected to the enabling signal of the counter, whose purpose is to stop the counter when the voltage level of the capacitor decreases below its threshold level.

When the *start of check* signal is set to ON, the pmos transitor opens and the capacitor is let to store the charge. At the same time, the ring starts oscillating and provides the clock signal to the counter which starts increasing its value N at the speed of the oscillation. Owing to the delay difference between d_{t1} and d_{t2} the XOR gate starts producing two pulses per period, as illustrated in Fig. 5. Once the voltage in the capacitor has decreased below the threshold of the inverter, the counter stops and stores the final value N which will be correlated to the total discharge of the capacitor and thus to the delay between the set t1 and set t2 lines.

In the next section the model of the *delta meter* is developed to justify its approximate linear behavior with respect to x.

IV. Model of the Delta Meter

Following the principle illustrated in Fig. 5 the number of ring periods registered in the counter can be estimated as,

$$N = (1 - h_t)\frac{C_P V_{DD}}{2I_P(d_{t2} - d_{t1}) + I_{leak}t_{min}} \tag{3}$$

where C_PV_{DD} is the total charge stored in the tank capacitor, $2I_D(d_{t2} - d_{t1})$ is the amount of charge drained in each period, $I_{leak}t_{min}$ is the leakage charge flowing per period and h_t is the normalized threshold level of the inverter gate (counter enabling), that senses the voltage at the tank capacitor. The leakage term would be important in case that the delay difference $(d_{t2} - d_{t1})$ would approach to zero, situation in which most of the bulk material would be removed and the parasitic capacitances of the TSVs would be the minimum possible. In this case the period of the ring oscillator would be the minimum possible, t_{min}, too.

A. *Modeling the Delay*

For the modeling of the delay we assume the α-power model for the transistors [13]. Using the approximation in [14] the delay is modeled as,

$$d = \tilde{k}\frac{CV_{DD}}{(V_{DD} - V_t)^\alpha} \tag{4}$$

where α is the velocity saturation coefficient of the carriers, V_t the threshold voltage of the transistors, $\tilde{k}$ is a trans-resistance which includes the rest of transistor parameters and C the parasitic capacitance in which the line propagates. All technological parameters are balanced between nmos and pmos transistors. Expression (4) approximates well if the signal swing is in the full voltage range and if the line is short enough so that no effects of transmission lines manifest. These conditions must be considered during the design of the BPD.

Using (4) the delay difference is calculated as,

$$\begin{aligned}(d_{t2} - d_{t1}) &= \tilde{k}\frac{V_{DD}}{(V_{DD} - V_t)^\alpha}(C_{t2} - C_{t1}) = \\ &= \tilde{k}\frac{V_{DD}}{(V_{DD} - V_t)^\alpha}C_N = \tilde{k}\frac{V_{DD}}{(V_{DD} - V_t)^\alpha}u \cdot c_c \cdot x\end{aligned} \tag{5}$$

Combining (5) in (3) we have the following,

$$\begin{aligned}N = (1 - h_t)&\frac{C_PV_{DD}}{I_{leak}t_{min}} \cdot \\ &\frac{1}{1 + \dfrac{2I_P\tilde{k}}{I_{leak}t_{min}}\dfrac{V_{DD}}{(V_{DD} - V_t)^\alpha}u \cdot c_c \cdot x}\end{aligned} \tag{6}$$

If we use the first order approximation $(1 + x)^{-1} \approx (1 - x)$ of the Taylor's series we get,

$$\begin{aligned}N \approx (1 - h_t)&\frac{C_PV_{DD}}{I_{leak}t_{min}} \cdot \\ &\left(1 - \frac{2I_P\tilde{k}}{I_{leak}t_{min}}\frac{V_{DD}}{(V_{DD} - V_t)^\alpha}u \cdot c_c \cdot x\right)\end{aligned} \tag{7}$$

In this expression the term $I_{leak}t_{min}$ is the most sensitive to process variations. In order to minimize its effect, a minimum charge is drained per period of the ring oscillator and made independent of the TSVs lines, such that this leakage becomes $I_{leak}t_{min} + Q_{min} \approx Q_{min}$. Therefore, the final expression of the *delta meter* is,

$$\begin{aligned}N =& N_{max}\left(1 - \tilde{K} \cdot u \cdot x\right) \\ N_{max} &= (1 - h_t)\frac{C_PV_{DD}}{Q_{min}} \\ \tilde{K} &= \frac{2I_P\tilde{k}}{Q_{min}}\frac{V_{DD}}{(V_{DD} - V_t)^\alpha} \cdot c_c\end{aligned} \tag{8}$$

The parameter N_{max} is the maximum counting that the detector can reach in case that a hacker would polish all the bulk silicon. The product $\tilde{K} \cdot u$ is the conversion factor from thickness to the decimal fraction of the counted periods. In normal conditions these are subtracted from the maximum such that the counter will give an intermediate value (pass response), that can be tuned using the unbalancing ratio u of the TSV sets t1 and t2.

V. Results

TABLE I
Response of the BPD to different kind of attacks.

Attack	Thickness [µm]	Oscillator frequency [MHz] min : typ : max	Signature N min : typ : max
0	250	87 : 70 : 57	77 : 91 : 105
1	200	90 : 72 : 59	98 : 112 : 126
2	150	93 : 74 : 61	133 : 147 : 168
3	100	96 : 77 : 63	217 : 252 : 273
4	50	100 : 80 : 65	322 : 343 : 357
5	25	102 : 81 : 66	371 : 392 : 413
6	0	103 : 83 : 67	427 : 441 : 462

A BPD has been implemented in a 65 nm technology from ST-microelectronics. The two TSV sets have a nominal capacitance of $C_{t1} = 250$ fF and an unbalancing ratio of $u = 0.5$, being the largest capacitance $C_{t2} = 375$ fF. The maximum bulk depth of the simulated integrated circuit is 250 µm giving a ratio of $c_c = 1\ \mu\mathrm{F\,m^{-1}}$.

The simulated attack produces 7 different thicknesses and in each of them the BPD is run to obtain the signature N. In Table I the results are shown for the typical and the corner cases. These values are also plotted in Fig. 6.

The pass region is $N_{pass} = [77, 105]$ that owing to the global variability it produces a escape region of $[187\ \mu\mathrm{m}, 250\ \mu\mathrm{m}]$ and thus the thickness of the bulk silicon is protected from 187 µm down to 0.

We have also considered possible tampering actions. The hacker polishes the bulk of the chip down to 15 µm, point at which he can use a FIB for local editing. To cheat the detector he contacts one or the other TSV sets with a micro-probe following the objective to reinforce the capacitance unbalance and reach back the pass region. Assuming a 20 fF parasitic capacitance, the two signatures obtained are shown in red crosses (Tamper 1) and (Tamper 2) in Fig. 6. The tampering doesn't succeed since the signatures still stay far from the pass region. We could also think of the use of heavier micro-probes to additionally decrease signatures. This

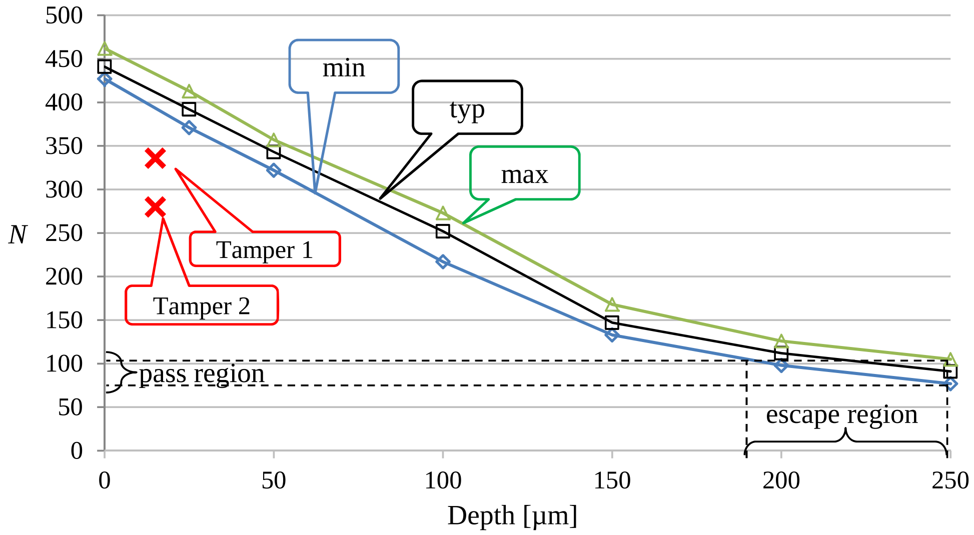

Fig. 6. Plot of the values in Table I. The limits of the simulated corners for maximum and minimum process parameters are shown.

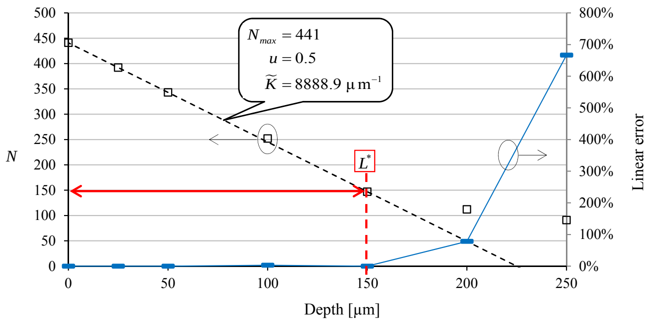

Fig. 7. Fitting of the linear approximation, error and BPD characteristic depth.

case of tunning presents much difficulties, but as a precaution the detector must be designed such that pass region is in the approximately middle range of the counting, above the point when the response bends. As a design criteria we propose to use the characteristic depth as is explained below.

In Fig. 7 the fitting of equation (8) with typical values is shown. From the adjustment the extracted parameters are: $N_{max} = 441$, $\tilde{K} = 8888.9\ \mu\mathrm{m}^{-1}$, being $u = 0.5$ by design. The error between the linear model and the simulated values is printed at the right axis. Notice that below $150\ \mu\mathrm{m}$ the error is negligible but above this depth it increases very quickly, tending to a linear growth with the depth.

We call characteristic depth L^* of BPD to the depth at which the error starts increasing, for our case this happens at approximately $L^* = 150\ \mu\mathrm{m}$. Notice that above this value the sensitivity of the BPD decreases quickly and therefore it doesn't make sense to extend the depth of the TSVs beyond this value. Therefore, for this detector we would use TSVs of a maximum depth of $150\ \mu\mathrm{m}$.

BPD is aimed to be used as a single unit per chip. Therefore the estimation of the area overhead presented in Table II assumes the impact of the detector area with respect to the areas of the present manufactured dies. For the BPD we assume that it works with an unbalancing ratio $u = 0.5$. This means that it needs 5 TSVs columns separated as 2 for set t1 and 3 for set t2. We suppose a diameter for the TSVs of 10 um and additional area equivalent to a TSV for the *delta meter*, giving a total area of 471 um^2 for a technology of 65 nm.

TABLE II

Estimated area overhead for current manufactured dies.

Type of circuit	Area	Overhead
BPD $u = 0.5$ 5 TSVs (10 um$\varnothing$) + *delta meter*	471 um^2	
DRAM and Flash Production Product Generations	29 mm^2	16.25 ppm
MPU (High-volume microprocessors)	88 mm^2	5.35 ppm
High-performance MPU	164 mm^2	2.87 ppm
ASIC Product Generations	858 mm^2	0.55 ppm

As present die areas we have considered the data in the ITRS predictions for year 2015 in four different cases, [15]. As it can be observed in Table II the maximum area overhead is 16.25 ppm for DRAM and Flash Production Product Generations, which represents a very small impact.

VI. Conclusions

In this paper a Backside Polishing Detector has been presented. The objective is to detect the amount of material that is removed from the bulk of a chip. The detector generates a signature that is proportional to thickness of the chip. Its operation is fully autonomous and it only has a start signal to run the operation. Once it finishes it activates a stop signal and provides the signature in the output of a counter. In a clean chip the signature will be a number around the half run of the counter (pass margin) while in a tampered circuit the signature will provide a number far out of this pass margin. The BPD is robust in the sense that actions trying to cheat its operation will unbalance the signature forcing a higher or lower value away from the pass margin.

Results in a simulated BPD have been reported for the typical and the corner cases. They show the stability of the detector under process variations. Also, different tampering actions have been considered and the signature response has been shown resilient against them.

Acknowledgments

Authors wish to thank reviewers for their constructive comments and suggestions. This work has been funded by the Spanish research program TEC2013-41209-P.

References

[1] S. Zanero, “Smart card content security,” *Dipartimento di Elettronica e Informazione*, 2002. [Online]. Available: http://home.deib.polimi.it/zanero/papers/scsecurity.pdf

[2] T. Sloane, “The safety of end-to-end encryption continues to make inroads,” *Payments Journal*, 2015. [Online]. Available: http://www.paymentsjournal.com/Page.aspx?id=25215

[3] J. Gotzfried and T. Muller, “Armored: Cpu-bound encryption for android-driven arm devices,” in *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, Sept 2013, pp. 161–168.

[4] T. C. May and M. H. Woods, “A new physical mechanism for soft errors in dynamic memories,” in *Reliability Physics Symposium, 1978. 16th Annual*. IEEE, 1978, pp. 33–40.

[5] C. H. Kim and J.-J. Quisquater, “Faults, injection methods, and fault attacks,” *Design & Test of Computers, IEEE*, vol. 24, no. 6, pp. 544–545, 2007.

[6] J. G. van Woudenberg, M. F. Witteman, and F. Menarini, “Practical optical fault injection on secure microcontrollers,” in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on*. IEEE, 2011, pp. 91–99.

[7] J. Ferrigno and M. Hlavác, “When aes blinks: introducing optical side channel,” *Information Security, IET*, vol. 2, no. 3, pp. 94–98, 2008.

[8] J. Krämer, D. Nedospasov, A. Schlösser, and J.-P. Seifert, “Differential photonic emission analysis,” in *Constructive Side-Channel Analysis and Secure Design*. Springer, 2013, pp. 1–16.

[9] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. S. Krissler, C. Boit, and J.-P. Seifert, “Breaking and entering through the silicon,” in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 733–744.

[10] K. Salah, “Tsv-based 3d integration fabrication technologies: An overview,” in *Design Test Symposium (IDT), 2014 9th International*, Dec 2014, pp. 253–256.

[11] S. Hamdioui, “Yield improvement and test cost reduction for tsv based 3d stacked ics,” in *Design Technology of Integrated Systems in Nanoscale Era (DTIS), 2011 6th International Conference on*, April 2011, pp. 1–1.

[12] G. Katti, M. Stucchi, K. De Meyer, and W. Dehaene, “Electrical modeling and characterization of through silicon via for three-dimensional ics,” *Electron Devices, IEEE Transactions on*, vol. 57, no. 1, pp. 256–262, 2010.

[13] K. A. Bowman, B. L. Austin, J. C. Eble, X. Tang, and J. D. Meindl, “A physical alpha-power law mosfet model,” in *Proceedings of the 1999 international symposium on Low power electronics and design*. ACM, 1999, pp. 218–222.

[14] A. Balankutty, T. Chih, C. Chen, and P. R. Kinget, “Mismatch characterization of ring oscillators,” in *Custom Integrated Circuits Conference, 2007. CICC’07. IEEE*. IEEE, 2007, pp. 515–518.

[15] A. Allan, “International technology roadmap for semiconductors,” *Semiconduct. Ind. Assoc*, pp. 1–76, 2012 Update.