Preparation of SCA Attacks: Successfully Decapsulating BGA Packages

Christian Wittke, Zoya Dyka, Oliver Skibitzki, and Peter Langendoerfer

IHP
Im Technologiepark 25
Frankfurt (Oder), Germany
{wittke, dyka, skibitzki, langendoerfer}@ihp-microelectronics.com

Abstract. In this paper we explain detailed how we successfully decapsulated a state of the art FPGA realized in a 45 nm technology and packaged in a BGA housing. For running SCA attacks it is important that the IC is still fully functional after decapsulation. The challenge here is the BGA package since the acid used to remove the plastic can easily destroy the substrate that is under the die. We achieved a success rate of 100%. The effect of the decapsulation for measuring EM traces is that the traces show an about 30% higher amplitude.

Keywords: Decapsulation, FPGA, Ball-Grid-Array (BGA), Package, EMA, Side Channel Analysis (SCA)

1 Introduction

Some types of physical attacks e.g. optical inspection, fault injections, etc. require the device under attack (DUA) to be decapsulated. But also more common attacks such as analysis of electromagnetic traces are benefiting from decapsulations since the amplitude of the measured signal is higher and by that allows simpler analysis. Ball-Grid-Array (BGA) packages are not really new but not as common as Quad-Flat-Packages (QFP). BGA packages are considered to be more challenging for an attacker when it comes to decapsulation. We report on how we opened BGA packaged FPGA already placed on a PCB with a success rate of 100%. We did a thorough but low cost preparation that consumed only one additional device to detect where the die is in the package, how thick the package is and how the plastic reacts on different types of acid. In order to prove that the decapsulation was successful i.e. that we could access the bare die and that the die was still working properly, we present EM traces of an elliptic curve kP operation recorded before and after the decapsulation. These traces show that after decapsulation the amplitude of the measured EM traces is about 30% higher.

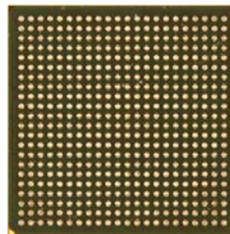
The rest of this paper is structured as follows. Section 2 summarizes typical packages and their structure. In section 3 the preparation for decapsulation is given and section 4 presents the decapsulation process and the impact for EM measurements. The paper finishes with short conclusions.

2 Packages

Integrated circuits (ICs) usually come in a package. The packages are standardized, e.g. by JEDEC Solid State Technology Association which is an organization for the standardization of semiconductors, including packages [1].

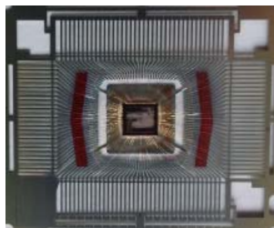
The package protects the die against damage and environmental influences. Furthermore the package bridges the different geometric connections from the die to the circuit board. An additional advantage is the better handling in terms of placement for component placement systems.

(a) QFP with pins on all sides

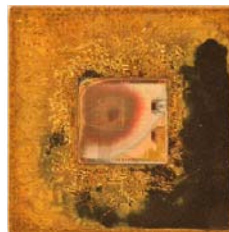


(b) BGA package with 484 solder balls (pins) on the back side

Fig. 1. Two different package types with their pins



(a) QFP leadframe



(b) BGA substrate

Fig. 2. (a) Leadframe as bridge in a QFP. The pads of the die are connected by bond wires. (b) Partially exposed substrate of a BGA package sample after etching attempts.

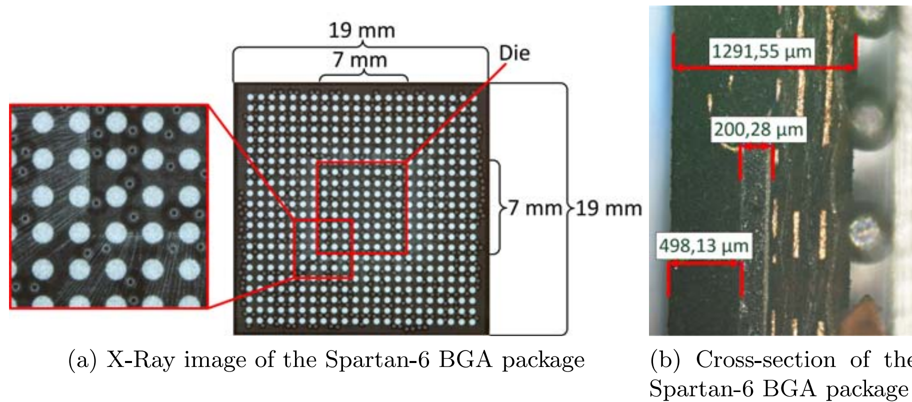
Common package types are e.g. the Quad-Flat-Package and the Ball-Grid-Array package. Both are surface mounted devices. The QFP has a rectangular form and pins on all four sides. An example QFP is shown in Fig. 1a. The connection from the pads of the die to the pins is realized by bond wires from

the pads to the lead frame (see Fig. 2a). Instead of pins on the sides the BGA package has balls of solder in a grid on the bottom. One benefit of BGAs is a higher density of pins, including a smaller pitch. Fig. 1b shows the under surface of a BGA with the grid of solder balls. The connections from the pads of the die to the pins of the package is realized through a substrate in the package (Fig. 2b).

For running semi-invasive attacks or to improve measurements of EM radiation, the package of the attacked IC needs to be opened but the device has to be fully functional. We decided to open the BGA package of the Spartan-6 FPGA on the PCB. But we used a single FPGA to prepare the decapsulation.

3 Preparation

As preparation for opening the BGA package we decided to x-ray the Spartan-6 FPGA and also made a cross-section before decapsulation to learn about the dimensions of the die (see Fig. 3a) and the thickness of the package over the die (see Fig. 3b).



(a) X-Ray image of the Spartan-6 BGA package

(b) Cross-section of the Spartan-6 BGA package

Fig. 3. X-ray image and cross-section of the Spartan-6 package

For chemical opening of the package we examined various acids at room temperature for 24 hours at the center of the sample packages. We tested hydrofluoric acid (HF 50%), hydrochloric acid (HCl 37%), sulfuric acid (H_2SO_4 95-97%) and nitric acid (HNO_3 65% and 85-100%). Afterwards HCl (37%), HF (50%), H_2SO_4 (95-97%) and HNO_3 (65% and 85-100%) were heated at 50°C, 75°C to 100°C (or boiling temperature) and put at the center of sample packages again. In this second experiment we exposed the packages to the acids for 5 minutes and 2 hours respectively.

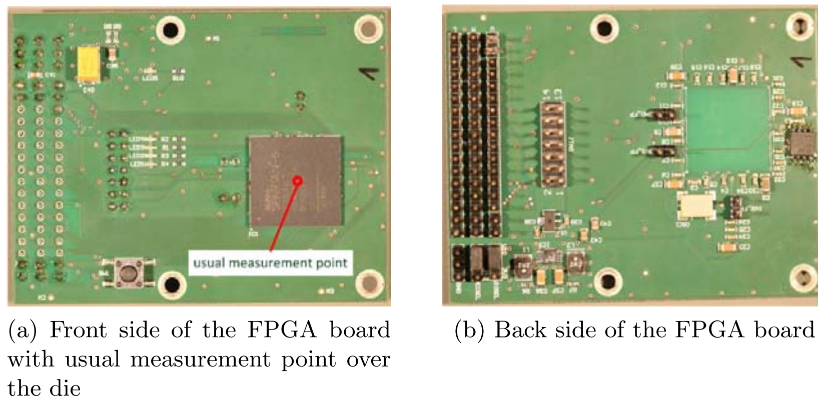
The best etching results were achieved with nitric acid (≥90%) [2] heated close to its boiling point of 84°C. But this highly depends on the compound of

the package, i.e. for different packages other acids may give better results. So we recommend to run similar tests on packages to be opened before trying to open the real target device.

4 Decapsulation of Spartan-6 in a BGA package

4.1 Preparation

The DUA is a Xilinx Spartan-6 FPGA. The board with the Spartan-6 was designed at IHP [3] based on the Fault Extension Board of the TU Graz. The board is shown in Fig. 4. The FPGA is placed on the front side of the board (see Fig. 4a) and most components are placed on the backside (see Fig. 4b). This improves measurements and ensures that all EM-probes can reach any measurement points on the FPGA board, without harming the probe. The board has several GPIOs to control and communicate with the FPGA, e. g. start an elliptic curve cryptography (ECC) computation, trigger the oscilloscope and provide input data. The FPGA is clocked with 4 MHz and has 1.2 V core and 3.3 V GPIO voltage.



(a) Front side of the FPGA board with usual measurement point over the die

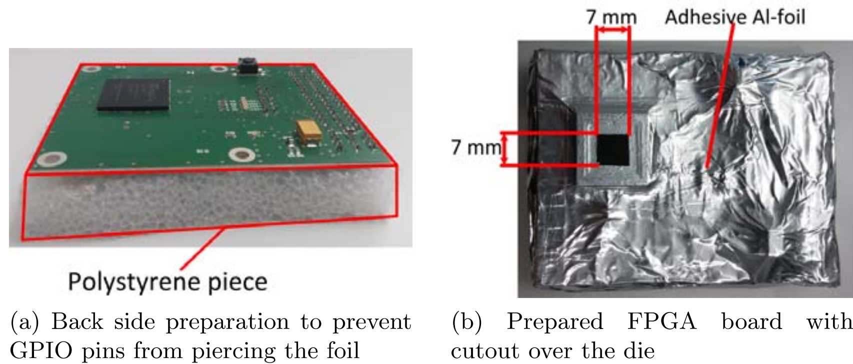
(b) Back side of the FPGA board

Fig. 4. Front and back side of the Spartan-6 Board

We decided to open the BGA package on the PCB. Therefore a good protection of the PCB and its components is needed. Otherwise the nitric acid could harm electrical components and the solder mask coating of the PCB. That would make the FPGA board inoperable.

To protect the PCB and its components against nitric acid we used adhesive aluminum foil similar to [4]. To prevent perforating the foil, we covered the whole back side of the board with a piece of polystyrene (see Fig. 5a) before covering the PCB with the aluminum foil. This shall prevent the acid passing through a hole in the foil. Furthermore, we have protected the cutout with multiple

overlapping layers of aluminum foil to avoid that the acid dissolves the glue (see Fig. 5b). The cutout was made at the end and the size was determined by the x-ray image of the chip.



(a) Back side preparation to prevent GPIO pins from piercing the foil

(b) Prepared FPGA board with cutout over the die

Fig. 5. Preparation of the Spartan-6 Boards for the decapsulation

4.2 Decapsulation

We prepared two FPGA boards for the decapsulation and opened the two BGA packages in parallel. The heated nitric acid ($\geq$90%) was dripped on the package for a minute and after that time the surface was cleaned with acetone spray. The cleaning with acetone spray removes remainings of the nitric acid and the package material. At the beginning the etch rate was low. We assume that the smooth surface is the reason behind this fact since the etch rate increased after the first etching steps. The decapsulation took 10 etching and cleaning periods.

Fig. 6 shows the opened BGA package. Nearly the whole die is visible. Only in the bottom corners some material of the package is left. We tried to remove these remainings with several additional etch and clean cycles. The result of these attempts can be seen in Fig. 7. There is still some material of the package behind the bond wires in Fig. 7a and a slight underetching of the die in Fig. 7b (marked with circle respectively). The optical inspection of both decapsulated FPGAs did not reveal any damage of the bond wires.

Next the aluminum foil was removed carefully. Intentionally the foil was left on the package and was cut with a scalpel to prevent the adhesive foil from damaging the bond wires while removing. Also the foil is some kind of shielding for EM measurements, which ensures that the EM radiation really stems from the die.

Fig. 8 shows the whole board with the decapsulated FPGA and the remaining foil. The functionality of the boards was successfully tested with our ECC design.

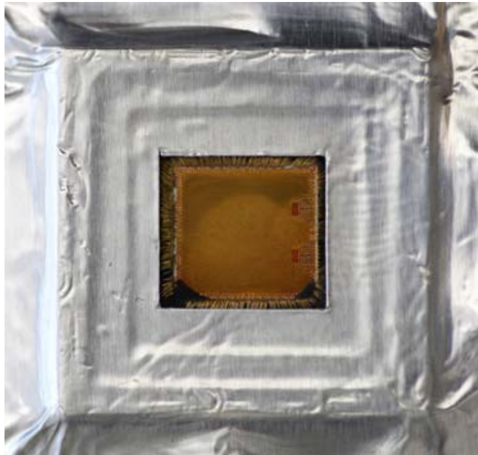
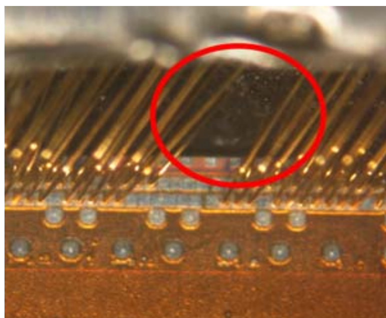
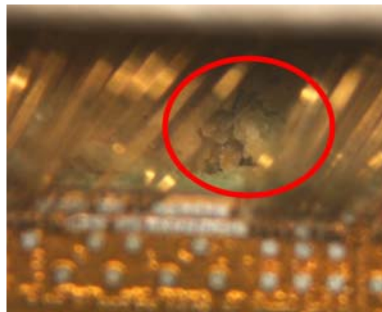


Fig. 6. Opened BGA package after cleaning with acetone spray



(a) Die from first FPGA board with still package material behind the bond wires (black material)



(b) Die from second FPGA board with underetching behind the die and bond wires (brighter material and deeper focus)

Fig. 7. Microscope images of the dies and bond wires after decapsulation

4.3 EM measurements

In order to determine the influence of the decapsulation on measured EM traces we measured the EM radiation over a non- and a decapsulated FPGA on our boards. The whole measurement setup (including probe, oscilloscope, power supply), ECC design, its input values and the position over the die were kept constant for fair comparison. Only the altitude of the probe over the die differs. We used the MFA-R-75 EM probe from Langer [5] to measure the traces. The probe was positioned at exactly the same position for both measurements using a high precision x-y-z table. The measured electromagnetic traces (EMT) are shown in Fig. 9 and Fig. 10.

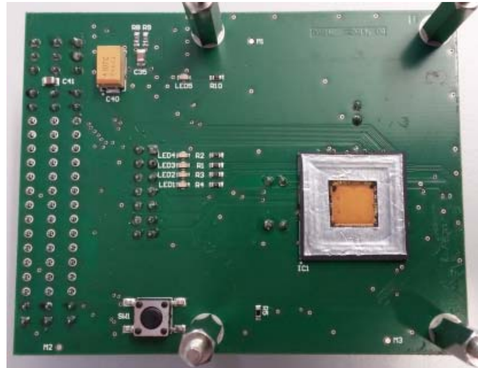


Fig. 8. FPGA on the board after decapsulating it

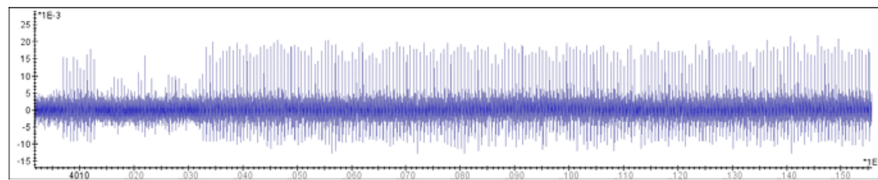


Fig. 9. EMT measured on top of a non decapsulated FPGA

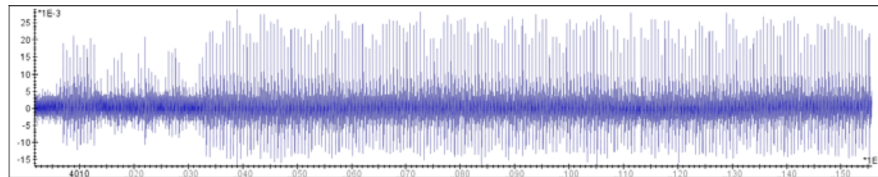


Fig. 10. EMT measured on top of a decapsulated FPGA

The amplitude of EMT measured on top of the decapsulated FPGA (see Fig. 10) is approximately 30% higher than the amplitude of EMT measured on the non decapsulated FPGA (see Fig. 9). This is due to the smaller distance of approximately 500 μm (see Fig. 3b) between the probe and die and the missing package material in the measurement of the decapsulated FPGA.

5 Conclusion

In this paper we have shown that decapsulation of BGA packages even though more challenging than the one of QFP packages is doable if prepared thoroughly. If the information about the package is not available, we propose to x-ray the device and to cut/break it in order to learn about the actual placement of the die in the package as preparation. We did this as a first step. The second step

was to run a series of experiments with different acids at different temperatures to learn how fast the plastic reacts to the acids. We consumed only one device for experiments and successfully opened two devices on boards which is a success rate of 100%.

In addition we recorded EM trace of an elliptic curve point kP multiplication to show that the die and the PCB were still fully functional and that decapsulation improves the quality of the measured EM traces, i.e. the amplitude of the traces, by 30%.

Acknowledgments

The work presented in this paper has been partially funded by the "Ministry of Sciences, Research and Cultural Affairs (MWFK)" from resources of the European Social Fund (ESF) and of the state Brandenburg.
We thank Dipl.-Stom. Nikolai Kljagin for x-raying of the FPGA in his dental clinic.

References

1. JEDEC - Global Standards for the Microelectronics Industry, www.jedec.org
2. Acros Organics - Data sheet Nitric acid fuming, 85-100%, http://www.acros.com/Ecommerce/msds.aspx?PrdNr=27062&Country=EN&Language=en
3. IHP - Innovations for High Performance Microelectronics, www.ihp-microelectronics.com/en/start.html
4. Loubet Moundi, P.: Cost effective techniques for chip delayering and in-situ depackaging. In: COSADE 2013 Short Talks Session, https://www.cosade.org/cosade13/presentations/session5b_a.pdf
5. LANGER EMV-Technik GmbH, "MFA02 micro probe set," http://www.langer-emv.com/produkte/stoeraussendung/nahfeldsonden/set-mfa02/.