Successfully Decapsulating BGA Packages: How To

Christian Wittke, Zoya Dyka, Oliver Skibitzki and Peter Langendoerfer

IHP
Im Technologiepark 25
Frankfurt (Oder), Germany

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 (EM) traces are benefiting from decapsulations since the amplitude of the measured signal is higher and by that allows simpler analysis and better local measurements in terms of side channel attacks.

In this work 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 [1]. The challenge here is that the device needs to be fully functional after dacapsulation. When decapsulating the BGA package the acid can easily destroy the substrate that is under the die. Moreover the PCB and the mounted components need a good protection to keep the device functional. But even though the decapsulation of BGA packages is more challenging than the one of QPF packages it is doable if prepared thoroughly. As preparation steps we made a x-ray image of the device and cut the FPGA in order to learn about the dimension and placement of the die in the package. Next we run a series of experiments with different acids at different temperatures to learn which acids are suitable and how fast the plastic reacts to the acids since the manufacturer of the chip often do not reveal the material of the package. The next step is the thorough protection of the whole device since we opened the BGA package on the PCB, i.e. in-situ. For protection we used adhesive aluminum foil similar to [2]. The removal of the package material and cleaning of the die is the last step for the decapsulation of the DUA.

We destroyed only one FPGA for the preparation and successfully opened four FPGAs on PCBs which was a success rate of 100 %. As a result we tested the DUAs and recorded EM traces of an elliptic curve decryption (EC point kP operation) with the MFA-R-75 EM probe from Langer [3] to show that the die and the PCB were still fully functional and that decapsulation improves the measurement results of the EM traces.

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.

References

[1] JEDEC - Global Standards for the Microelectronics Industry, `www.jedec.org`

[2] 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`

[3] LANGER EMV-Technik GmbH, MFA02 micro probe set, `http://www.langer-emv.com/produkte/stoeraussendung/nahfeldsonden/set-mfa02/`