On Determining Optimal Parameters for Testing Devices Against Laser Fault Attacks

Jakub Breier and Chien-Ning Chen
Physical Analysis and Cryptographic Engineering
Temasek Laboratories at Nanyang Technological University, Singapore
Email: {jbreier, chienning}@ntu.edu.sg

***Abstract*—Laser equipment has been used for a failure analysis for a long time. It is also becoming increasingly popular in fault injection attacks. Since it can be challenging to master this technique and get plausible results from experimental evaluations, in this paper we provide a set of guidelines and best practices that might help researchers to get the basic idea on this topic.**

First, we describe different decapsulation techniques with details on de-packaging steps. After that, we provide insights on choosing the right laser setup for laser fault injection. Finally, we provide hands-on experience on device profiling for making the attack successful.

I. Introduction

When it comes to breaking the ciphers, there is a huge gap between theory and real world. Currently used cryptographic algorithms have excellent security properties, enabling them to resist both linear and differential cryptanalysis. For example, the best known attack on AES-128, by Bogdanov et al. [1], can recover the full key with computational complexity $2^{126.1}$, therefore it is still considered infeasible for current computers. Unfortunately, in a real world, we cannot rely on theoretical security. Algorithms are executed on physical devices that have their properties. These properties can be observed and used in order to mount very efficient attacks, by measuring power consumption, electromagnetic emanation, execution time, or by injecting faults into algorithm execution. We call these attacks "physical attacks." For example, the most efficient power analysis attack is a single-trace template attack [2], therefore it requires only a single power trace after profiling the device. The situation is similar with the most efficient fault attack, it takes only one faulty encryption in order to recover the secret key [3].

But even with physical attacks, many published works propose attack models that are difficult to achieve in practice. When it comes to fault attacks, in theory we can disturb any step in algorithm execution at any specific bit. In a real world, there are many steps to be performed before we can start performing the attack itself and even then it is not guaranteed that we will achieve the desired result.

In this paper, we describe necessary steps for the laser fault injection, such as device decapsulation, with mechanical and chemical techniques, laser equipment setup, for determining optimal laser parameters and device profiling. We explain each step in detail, providing insights on advantages and disadvantages of different options. Our results can help researchers to make their experiments more effective and to avoid some problems associated with the process.

The rest of the paper is structured as follows. Section II provides an overview of related work in the field of laser fault injection. Section III describes different decapsulation techniques on various devices. Setting up the laser equipment is detailed in Section IV. Device profiling for fault attacks is explained in Section V, and finally, conclusion is given in Section VI.

II. Related Work

Optical attacks on cryptographic devices were proposed in 2003 by Skorobogatov and Anderson [4]. They used inexpensive equipment in order to set/reset individual bits of SRAM in a microcontroller. They also provided a simple countermeasure to thwart this attack.

Good overview of different fault attack methods and countermeasures is provided in the paper by Bar-El et al. [5]. It explains several techniques that can be used for disturbing integrated circuits and shows a few basic fault models on secret key and public key algorithms and on key transfer.

Van Woudenberg et al. [6] targeted secure microcontrollers deployed on smartcards. They showed how to overcome countermeasures on state-of-the-art secure devices and how to perform a successful attack.

Courbon et al. [7] showed that it could be beneficial to first obtain a chip image from a Scanning Electron Microscope, which can help to localize registers. Such method can save time needed for scanning the whole device with laser and help attackers to focus directly on important areas.

III. Device Decapsulation

The main condition for optical fault injection attacks is the visibility of the device. Therefore, it is necessary to depackage the chip, so that the laser beam could approach the surface. There are two main methods – *chemical decapsulation*, using acids to dissolve the epoxy layer covering the silicon die and *mechanical decapsulation*, using mechanical milling devices to reach the surface. This process depends on the chip package and also which side (front or back) of the silicon die surface the laser beam will approach. For example, epoxy plastic of DIP (dual in-line package) and also the smartcard package can be removed to reveal the front or backside of the silicon

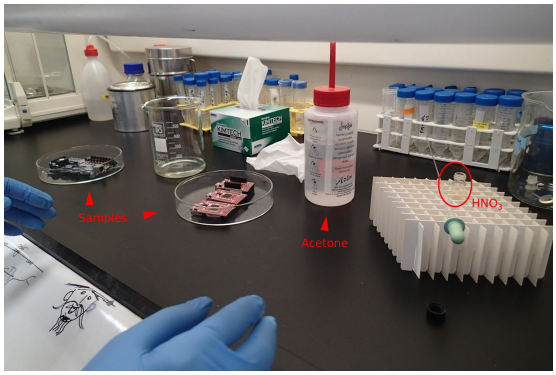


Fig. 1. Typical laboratory settings for chemical decapsulation.

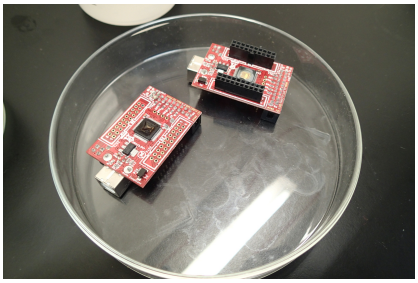


Fig. 2. Detail of the samples.

surface by using chemical or mechanical decapsulation, respectively. In some flip chip packages, the backside of silicon is uncovered or only with a metal cover, which can be removed easily, but the frontside of the silicon is unaccessible. In this section, we will describe both methods together with practical examples, successful and unsuccessful.

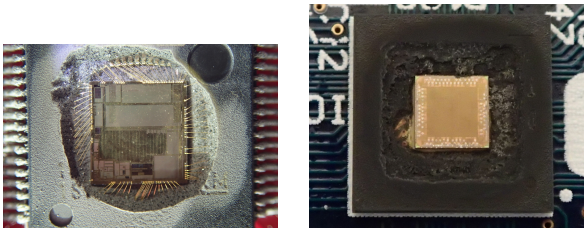
A. Chemical Techniques

Chemical decapsulation technique can be used both for the frontside and backside of the chip. Most of the time, either a fuming nitric acid (HNO_3 with concentration $\geq$90%), a concentrated sulphuric acid (H_2SO_4 with concentration $\geq$96%), or a combination of these acids is used. It was shown ([8]) that for ICs with copper wire bonds, a mixture of 80% HNO_3 and 20% H_2SO_4 is a good option in order to keep the wiring unharmed. Because of the corrosive nature of such acids, this technique needs to be performed in a chemical laboratory with a specific equipment needed, such as fume hood, preventing inhaling vapors from the acid. A typical laboratory setting for chemical depackaging can be seen in Fig. 1, detailed picture of the samples being processed (ARM Cortex-M3) is in Fig. 2.

The process consists of following steps:

1) Heating the acid to 30-60 degrees Celsius (optional step, makes the process faster).
2) Applying small portion of the acid on the epoxy surface.
3) Washing the acid with the acetone.
4) Repeating steps 2-3 until desired portion of the chip is visible.

The last step has to be detemined with respect to which part of the chip we want to aim at and we also need to consider what bonding wires are used and what will be the result after exposing them to the acid. The easiest situation is with the golden wires. In such case we do not have to worry about damaging them, unless we mechanically cut the contacts. Therefore we can expose the whole surface of the chip to the acid. Such a depackaged chip can be visible in Fig. 3 (a). If the wire material is copper, once the acid reaches the edge of the chip, it will dissolve all the wirings, as can be seen in Fig. 3 (b). In such cases we have to be careful and only depackage central region of the die.



(a) (b)

Fig. 3. Chemical decapsulation – successful (a), and unsuccessful (b).

To summarize, we provide a table stating advantages and disadvantages of using acids for chip decapsulation (Tab. I).

TABLE I
ADVANTAGES AND DISADVANTAGES OF CHEMICAL DECAPSULATION

Advantages	**Disadvantages**
• only technique for the frontside decapsulation	• need to perform in a laboratory
• does not require expensive equipment	• fuming acid is a health hazard
• does not leave mechanical damage on the surface	• acid can dissolve bonding wires on the edge of the chip, making it unusable
• relatively fast	• low precision • uneven delayering

B. Mechanical Techniques

Mechanical decapsulation can only be used for the backside of the chip (silicon substrate) since once the milling head reaches the IC components, it will destroy them. Also, excessive heat generated during the process can easily destroy the chip even before reaching the surface. Depending how precise is the milling equipment, it can be used not only for removing the epoxy package, but for delayering the silicon substrate as well. That is especially beneficial for laser fault injection, since effective penetration of light is $\approx$ 1.58 μm for 532 nm wavelength, $\approx$ 12.79 μm for 808 nm wavelength, and $\approx$ 1100 μm for 1064 nm wavelength [9]. Even if we use a laser with the last mentioned wavelength, results differ significantly if we have a silicon substrate with 300 μm thickness or with only 200 μm.

Milling/polishing equipment varies significantly. For basic decapsulation of standard microcontrollers in DIP, a micro mill with a price range less than hundred dollars is enough. Especially for lower-cost devices where it is not a problem to have several spare chips to learn the technique first. Such technique can be seen in Fig. 4. It is an AVR microcontroller decapsulated by using Proxxon precision drill/grinder. Milling has to be slow with several pauses in order to let the chip to cool down. After the epoxy layer is removed, copper substrate is carefully thinned until it can be peeled off easily. The final

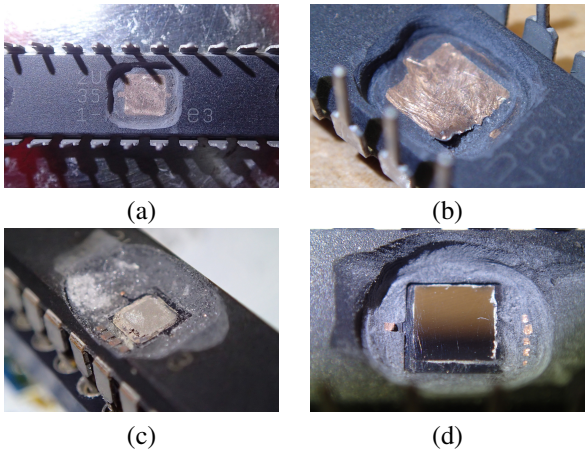


Fig. 4. Mechanical decapsulation steps: (a) grinding, (b) thinning the copper substrate, (c) removing the substrate, (d) removing the glue and polishing.

TABLE II
ADVANTAGES AND DISADVANTAGES OF MECHANICAL DECAPSULATION

Advantages	Disadvantages
• provides high precision • can be used for delayering of the silicon substrate • can be automated • does not have to be performed in a laboratory	• cannot be used for the frontside • excessive heat can damage the chip • precise equipment is expensive

layer is a glue which holds the silicon die, this can be removed by hard plastic tools by scratching off.

Many high-end devices encapsulated in a ball grid array (BGA) flip chip package and have a metal cover instead of an epoxy package. This cover can be easily removed by heating the glue that keeps it on the board. However, silicon substrate thickness in this case might pose a significant obstacle for the optical fault injection. Thinning the layer needs to be done carefully and a high precision equipment is necessary, such as Ultra Tec ASAP-1. Precision milling devices range in prices in tens of thousands dollars. Also, a special sample preparation is needed before.

In Tab. II we provide a summary of advantages and disadvantages of mechanical decapsulation techniques.

IV. Laser Setup

As it was already mentioned in the previous section, optical sources with different wavelengths have different penetration depths for silicon, therefore we have to select a laser that is appropriate for our purposes. For frontside attacks, where IC components are directly visible, a green (532 nm) or a red (808 nm) can be used, since there is no need of penetrating the silicon substrate. Shorter wavelengths correspond to more energy per photon, therefore are more effective in producing faults. For backside attacks, we have to use longer wavelengths, so a near-infrared laser (1064 nm) is a safe bet, with penetration capabilities more than 1100 μm.

Another important parameter is the laser spot size. Current manufacturing technologies allow very small transistor sizes. Spot size has to be small enough to allow precise fault injection, especially if we are targeting on a single bit set/reset attack models. In our experiments we have attacked several technologies, ranging from low-end microcontrollers manufactured by 250 nm process, to high-end FPGAs with transistor size 65 nm. Our laser spot size depends on the used lens, it varies between $\approx$ 10-800 μm^2. We were able to perform bit flip faults in all the devices under test with high success rates ($\geq$90%). Authors in [10] claim they were able to disturb particular bits even with a very large laser beam spot (125$\times$125 μm^2), although the success rate was lower.

The last important parameter is the laser power. Every device has a different energy threshold until its behavior changes into faulty one. Since we do not want the beam to be activated for a long time because of losing the precision, a good choice is to increase power level while keeping the laser activation period short. Our near-infrared laser has a maximum output power of 20 W, further reduced by using objective lenses to 7-8 W. Surprisingly, our results show that we need higher energy for perturbating smaller size technologies. For 65 nm FPGA, the laser power had to be at least 80% in order to produce results. For old microcontrollers, laser powers between 10-20% are sufficient.

V. Device Profiling and Attack

After we have determined, what laser to use, we have to profile the device, so that we know what attack models are possible. As in previous cases, there is also a difference between frontside and backside approaches. When attacking from the frontside, it is possible to determine the position of some components by optical inspection. It is relatively easy to see memory blocks, for example, since they constitute a large regular area on the chip. However, some IC components might be covered by a metal layer or other metal components, which will reflect the laser beam. Figure 5 is an example that laser fault is possible only on uncovered parts (the small windows).

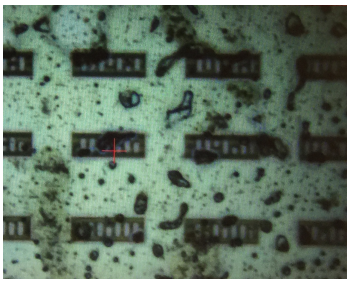
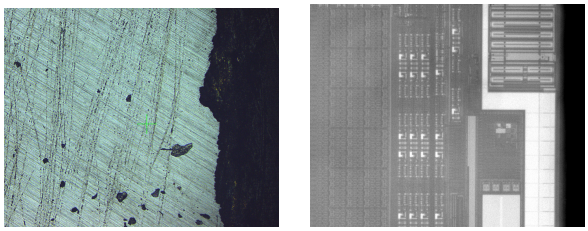


Fig. 5. Metal layer and small windows on the frontside of silicon die.

When trying to recognize components from the backside, it is impossible to use a standard imaging equipment, since we will only see the surface, as depicted in Fig. 6 (a). However, if the silicon substrate is thin enough, we can use infrared camera to capture the underlying layer, as shown in Fig. 6 (b). Another approach would be to use localized electromagnetic analysis to distinguish active areas of the chip. This technique might speed up the scanning process, although the areas obtained by measuring EM emanation might be still relatively large.

During the initial profiling we vary four parameters in order to get optimal settings for the actual attack:

- Location – if we do not have clear knowledge about location of different components on the chip, the best



(a) (b)

Fig. 6. Same area captured with standard (a), and infrared (b) imaging equipment.

option is to scan the whole chip area with step size small enough to localize components such as registers, memory blocks, etc. A precise X-Y positioning table is a necessity, we have used a table with 0.05 μm step size.

- Power – since every device acts differently under different power, the safest option is to start with the lowest power possible and increase in small steps to prevent destructive changes.
- Offset – offset is the time from the trigger. Trigger can be either manually set at the position in the algorithm where we want the fault to occur or we can use more advanced techniques, such as pattern recognition from communications and power traces. But even if we set the trigger very precisely, there is some delay after the laser gets activated (usually in tens of ns). Therefore, for initial scanning there has to be some variability in the offset.
- Glitch length – it is the period when laser is activated. This parameter determines the overall energy that affects the device and also number of operations affected that are executed in the device at that time. For example, in [11] authors managed to skip the whole last AddRoundKey of AES in order to retrieve the secret key used in the device. Such attack required a very long glitch length ($\approx$ 3 μs).

After determining the right parameters, we can perform a fine-grain scan on a smaller area. Result of such a scan is depicted in Fig. 7. It shows a faulty region of a microcontroller. Faulty area is $\approx$ 80$\times$1100 μm large, that is, $\approx$ 0.97% of the whole chip size. Summary of our results on different

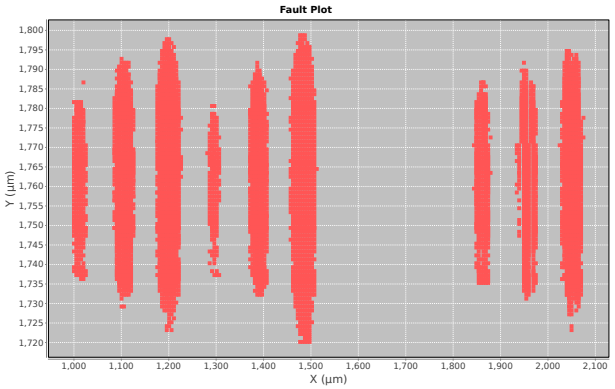


Fig. 7. Distribution of faults corresponding to a microcontroller area (zoomed).

architectures is stated in Tab. III. Please note that we were unable to get any results from the frontside decapsulated FPGA due to metallic upper layer.

Dedicated programs running on the target are also employed during the profiling, instead of directly attacking the cryptographic algorithm. Explicit trigger signals will help to have a better timing (offset and glitch length). For microcontrollers, we need multiple profiling programs to identify faults in different components, e.g., memory scanning for memory faults; memory storing and loading for faults on address and data bus; outputting values of registers for faulty register values and incorrect instruction execution. Watch dog timer can help to restart the microcontrollers in case the target stops responding. For FPGAs, a customized placement can help to identify the target components quickly, instead of an exhaustive search.

TABLE III
SUMMARY OF RESULTS FOR DIFFERENT ARCHITECTURES.

Architecture	Side attacked	Fault types
AVR	frontside, backside	bit flips, instruction skips, instruction changes
ARM	frontside	instruction execution disturbance
FPGA	fronstide	no faults
	backside	bit flips in slice registers

VI. Conclusion

In this paper we provided a hands-on experience on laser fault injection on integrated circuits. Researchers can use it as guidelines when choosing the right laser equipment, decapsulation technique, and profiling method. There are many works describing results on laser fault attacks, however they do not focus on describing the process itself in the detail. We hope this paper fills this gap and brings more light into the experimental process.

References

[1] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique Cryptanalysis of the Full AES," in *ASIACRYPT 2011*, ser. LNCS, D. Lee and X. Wang, Eds. Springer, 2011, vol. 7073, pp. 344–371.

[2] M. S. E. Mohamed, S. Bulygin, M. Zohner, A. Heuser, and M. Walter, "Improved Algebraic Side-Channel Attack on AES," Cryptology ePrint Archive, Report 2012/084, 2012, http://eprint.iacr.org/.

[3] D. Saha, D. Mukhopadhyay, and D. RoyChowdhury, "A Diagonal Fault Attack on the Advanced Encryption Standard," Cryptology ePrint Archive, Report 2009/581, 2009, http://eprint.iacr.org/.

[4] S. Skorobogatov and R. Anderson, "Optical Fault Induction Attacks," in *Cryptographic Hardware and Embedded Systems - CHES 2002*, ser. LNCS. Springer, 2003, vol. 2523, pp. 2–12.

[5] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks," Cryptology ePrint Archive, Report 2004/100, 2004, http://eprint.iacr.org/.

[6] J. van Woudenberg, M. Witteman, and F. Menarini, "Practical Optical Fault Injection on Secure Microcontrollers," in *Fault Diagnosis and Tolerance in Cryptography, 2011 Workshop on*, Sept 2011, pp. 91–99.

[7] F. Courbon, P. Loubet-Moundi, J. J.-A. Fournier, and A. Tria, "Adjusting laser injections for fully controlled faults," in *Constructive Side-Channel Analysis and Secure Design 2014*, Paris, France, Apr. 2014.

[8] S. Murali and N. Srikanth, "Acid Decapsulation of Epoxy Molded IC Packages With Copper Wire Bonds," *Electronics Packaging Manufacturing, IEEE Transactions on*, vol. 29, no. 3, pp. 179–183, July 2006.

[9] M. A. Green, "Self-consistent optical parameters of intrinsic silicon at 300 k including temperature coefficients," *Solar Energy Materials and Solar Cells*, vol. 92, no. 11, pp. 1305 – 1310, 2008.

[10] C. Roscian, J.-M. Dutertre, and A. Tria, "Frontside laser fault injection on cryptosystems - Application to the AES' last round," in *Hardware-Oriented Security and Trust (HOST)*, June 2013, pp. 119–124.

[11] J. Breier, D. Jap, and C.-N. Chen, "Laser Profiling for the Back-Side Fault Attacks: With a Practical Laser Skip Instruction Attack on AES," in *1st ACM Workshop on Cyber-Physical System Security*. New York, NY, USA: ACM, 2015, pp. 99–103.