Journal of The Korea Institute of Information Security & Cryptology
VOL.24, NO.3, Jun. 2014

ISSN 1598-3986(Print)
ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.3.453

오류주입공격에 대한 개선된 이중모드 레이저 프로빙 시스템*

이 영 실,[1†] Thiranant Non,[1] 이 훈 재[2‡]
[1]동서대학교 일반대학원, [2]동서대학교

An Improved Dual-mode Laser Probing System for Fault Injecton Attack*

Young Sil Lee,[1†] Thiranant Non,[1] HoonJae Lee[2‡]
[1]Dongseo University Graduate School, [2]Dongseo University

요 약

오류주입공격(Fault Injection Attack)은 하드웨어적 또는 소프트웨어적으로 구현된 암호칩에 인위적으로 오류를 주입 또는 발생시켜 암호 알고리즘 동작/수행을 방해함으로써 칩에 내장된 정보를 찾아내는 공격으로, 이 중 레이저를 이용한 오류주입공격은 특히 성공적인 것으로 입증된 바 있다. 본 논문에서는 기존의 플래쉬 펌프 방식의 레이저와 광섬유 레이저 모델을 병렬 결합한 이중모드 레이저 방식으로 개선된 레이저 프루빙 시스템을 제안하였다. 제안된 방법은 에너지 출력은 높으나 주파수 반복률이 낮아 오류주입공격 실험에 적합하지 않은 기존의 플래쉬 펌프 방식 레이저를 레이저 절단용으로 활용하고, 추가로 별도의 오류주입을 위한 고주파 반복률을 갖는 레이저를 단순 병렬 결합시키는 방법이다. 오류주입을 위해 결합된 제 2의 신규 레이저는 반도체 레이저와 광섬유 레이저를 선택하여 두 가지 시스템을 설계하였으며, 이에 따른 장·단점을 비교분석하였다.

ABSTRACT

Fault injection attack is the process of attempting to acquire the information on-chip through inject artificially generated error code into the cryptographic algorithms operation (or perform) which is implemented in hardware or software. From the details above, the laser-assisted failure injection attacks have been proven particularly successful. In this paper, we propose an improved laser probing system for fault injection attack which is called the Dual-Laser FA tool set, a hybrid approach of the Flash-pumping laser and fiber laser. The main concept of the idea is to improve the laser probe through utilizing existing equipment. The proposed laser probe can be divided into two parts, which are Laser-I for laser cutting, and Laser-II for fault injection. We study the advantages of existing equipment, and consider the significant parameters such as energy, repetition rate, wavelength, etc. In this approach, it solves the high energy problem caused by flash-pumping laser in higher repetition frequency from the fiber laser.

Keywords: Fault Injection Attack, Laser Probe, Side-Channel Attack, Fault Analysis Tools

접수일(2013년 12월 31일), 수정일(2014년 2월 25일), 게재확정일(2014년 4월 4일)

* 본 연구는 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었으며(과제번호: 2013-071188), 부산광역시에서 지원하는 BB21 과제에서 지원받았습니다.

† 주저자, youngsil.lee0113@gmail.com
‡ 교신저자, hjlee@dongseo.ac.kr (Corresponding author)

I. Introduction

The cryptographic algorithms that have been implemented are designed in the way such that they are difficult to be broken mathematically[1]. In order to obtain the secret key, which allows the decryption of encrypted information, an attacker must perform a brute force analysis that requires a prohibitively large number of experiments. There is no known methodology for the most commonly used cryptographic algorithms to significantly reduce the secret key search space. However, it is shown that secret information (such as the key of the encryption algorithm) can leak through side channel attacks.

Examples of such side channels are the time needed to perform the encryption or the power consumed by the device implementing the encryption algorithm. Timing and power side channel attacks are based on the fact that the individual computation steps that are needed during the encryption are dependent on the bits of the secret key and thus, the time needed for these steps and the power consumed by them are directly correlated to the secret key bits. These attacks have been proven to be effective and it incurs relatively at low cost. Furthermore, once a side-channel attack technique has been developed and made public, expensive equipment or high technical skills are not required to apply in practice.

A different type of side-channel attacks that were proved to be very effective is realized through the injection of deliberate (malicious) faults into a cryptographic device and the observation of the corresponding erroneous outputs[2-3]. Using this type of attack and analyzing the outputs of the cryptographic device, called differential fault analysis (DFA)[4], the number of experiments needed to obtain the bits of the secret key can be drastically reduced. This kind of active side-channel attacks (in contrast to the previously described passive ones) has been in the last decade the subject of intense and expanding research, as it has been demonstrated to be highly effective[5-7].

Fig.1. shows fault injection techniques[8] that can be classified into three main categories: hardware fault injection, software fault injection and simulation-based fault injection. Hardware and software fault injections must be injected in the prototype or fully operational system, which can collectively be referred as physical-based fault injection.

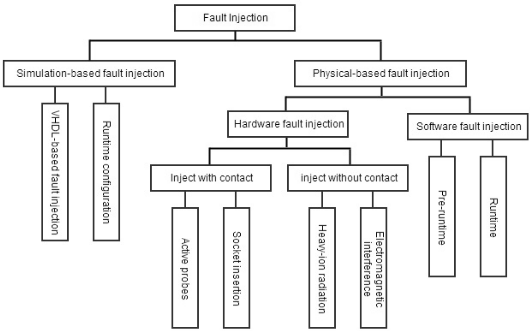


Fig.1. Classification of Fault Injection Techniques

Among them, hardware and software fault injection have been used for a long time. Over the past decade, with the development of fault injection technology, especially the increasing need of evaluating system early in the design cycle, simulation-based has attracted more attention of researchers.

To experiment fault injection attack, the failure analysis of many different products involve the use of the following tools and techniques[9]: Microscopes, Sample preparation, Radiography, Spectroscopic analysis, Device modification, Surface analysis, Scanning electron microscopy, Laser signal injection microscopy (LSIM), Semiconductor probing, Software-based fault location techniques. Especially, we are focusing on the laser signal injection microscopy (LSIM) which injects faults into the device.

In this paper, we propose an improved laser probe which can be used for the experiment of fault injection attack.

The rest of the paper is organized as follows. After introduction in section Ⅰ, we describe the related work in section Ⅱ. In section Ⅲ, we present the proposed improved laser probe and discussion in section Ⅳ. Finally, section Ⅴ concludes with a summary of our scheme and future work.

II. Laser Probe for Fault Injection Attack

A laser is a tool that produces light through a process called optical amplification based on the stimulated emission of electromagnetic radiation. Lasers are different from light sources due to their coherent emission. Spatial coherence refers to the output, which is a narrow beam, often called "pencil beam". Laser beams can be focused to very precise spots, giving high irradiance. They can be launched into beams of very low divergence in order to focus their power at a large distance. The light generated by stimulated emission is similar to the input signal in terms of wavelength, phase, and polarization. This makes the laser light coherent and able to maintain the uniform polarization and often established by the optical cavity design.

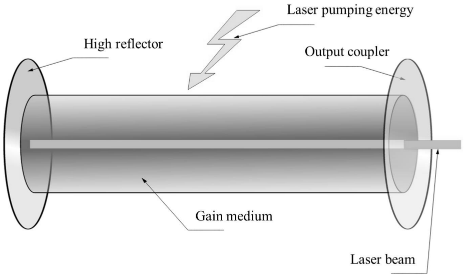


Fig.2. Components of a typical laser[10]

In Fig.2, a laser consists of a gain medium, which is a mechanism to supply energy and provide optical feedback. The gain medium is considered a material with properties that allow it to amplify light by stimulated emission. Light of a specific wavelength that passes through the gain medium will increase in power, known as amplification process. In order to amplify light, a gain medium needs to get supplied with energy. The process of supplying energy is called pumping. The energy is normally supplied as an electrical current, or as light at a different wavelength.

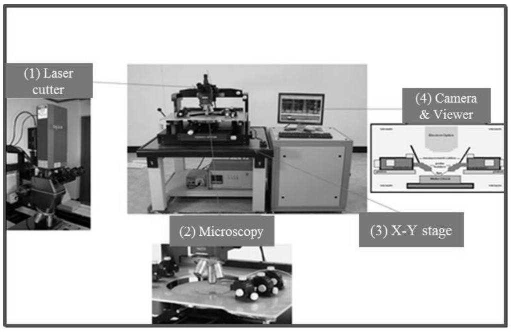


Fig.3. An example of FA tool set up

The Laser Fault Injection (LFI) technique has a good spatial and temporal precision to inject the faults. This laser used in fault injection tool will not result in permanent damage, because it allows adjusting by tuning the beam's energy level. However, an amount higher a destructive threshold can destroy the circuit. The parameters below should be considered when performing an attack: gain medium of laser, wavelength, repetition rate, spot size, output power and so on.

Fault injection attack equipment can be divided into four parts as shown in Fig. 3. (1) Laser cutter for a laser beam fire and cutting on the target; (2) Optical microscopy (Microscope) to enlarge the size of the target; (3) X-Y stage (including anti-vibration enclosures) for moving target in the X-axis, Y-axis, R-rotation. Z-axis movement is generally achieved by an optical microscope; (4) Camera and Viewer.

III. An Improved Laser Probing System for Fault Injection Attack

Typically the laser probe is considered expensive equipment. Thus, enhancing the laser probe through utilizing existing equipment is recommended rather than buying a new product. The basic concept of the proposed idea is a dual-laser probe which is the combination between existing laser probe and extra laser head in parallel. Our improved laser probe can be divided into two parts: Laser-Ⅰ for laser cutting to remove the surface of the targeted device, before performing the fault injection attack and Laser-Ⅱ for fault injection. In this case, we needed a separate controller.

In our proposed idea on laser probe enhancement, we assume QuikLaze-II or EzLaze-3[11] of New Wave Research is used for laser I. The key of the motivation is from the first conceptual design of this research, experimented by research teams in Cambridge university and Gyeongbuk university.

Also, the combination of laser-Ⅱ methods is divided by the laser types as shown in Fig 4 and 5.

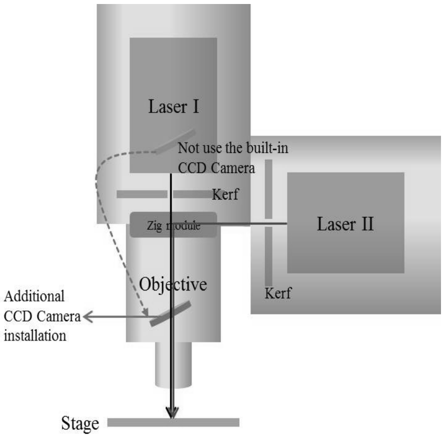

Laser I
Not use the built-in CCD Camera
Kerf
Zig module
Laser II
Objective
Kerf
Additional CCD Camera installation
Stage

Fig.4. An Improved laser probe—Case 1.

Fig.4. shows the design of improved laser probe—case 1 which used Diode laser for laser-Ⅱ. In this case, combined experiments auxiliary devices (zig module) are used together with the laser probe which enables the mode-switching between Laser-Ⅰ and Laser-Ⅱ. However, the extra-large size of the laser probe is the problem. In addition, an additional CCD camera installation is needed.

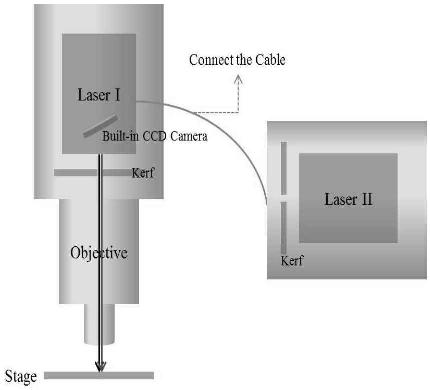


Fig.5. An Improved laser probe—Case 2.

Fig.5. shows the design of improved laser probe—case 2 which used Fiber laser for laser-Ⅱ. In this case, we can connect between the Laser-I and Laser-II through fiber cable. Thus, we can solve the problem occurring in the case 1 and a wider working space can be utilized. In addition, an additional installation of the CCD camera is no longer required. Mode-switching can be done by either operating the zig module or using additional software to control the operation.

Ⅳ. Discussion

In this section, we compare the advantages and disadvantages of our proposed improve laser probes.

Before making the comparison, we describe some notations to compare two proposed ideas.

Table 1. Notation

Parameters	Description
Frequency/ Repetition rate	The number of times of a repeating laser shots per unit time
Energy	The amount of the power used to perform the fault injection attack, measured in Watt
Diode lifetime	The period of time that laser diode can perform its task, measured in hour
Cooling	The process required to remove the heat produced by the device/machine
Floor space	The amount of area taken by that device/machine, measured in square meter
Spot size	The diameter of the circle formed by the cross section of the field of view of an optical instrument at a given distance

Table 2. shows the comparison between the existing laser probes, in this case it is EzLaze-3 and the proposed idea. The performance is shown in terms of energy, repetition rate, wavelength, spot size and so on. EzLaze-3 gives lower energy which ranges from 0.5mJ to 2.5mJ; whereby the proposed dual-mode laser probe gives 20mJ (20mW). The repetition rate of the proposed idea gives up to 5 times over EzLaze-3, and 2 times better in terms of wavelength, which is 1064nm. The spot size of EzLaze-3; in the sense how accurate the laser probe can focus, ranges from 2×2㎛ to 50×50㎛ and 1×1㎛ for the proposed idea. The main difference that makes the proposed idea advantageous is the laser switching function, controlled by auxiliary devices (zig module).

Table 2. Specification comparison between EzLaze-3[11] and propose idea for fault injection

Parameter	EzLaze-3	Estimated performance
Energy	min. 0.5mJ max. 2.2mJ	0~20mJ (0~20㎽)
Repetition rate	1~5Hz	≤ 25㎒
Wavelength	523nm Green	1064㎚ IR(Infrared)
Spot size	min.2×2㎛ max.50×50㎛	1㎛ × 1㎛
Synch board	None	Synchronization of start timing between signal and pulse
Manual override switch	None	Select laser switch by zig module

Table 3. shows the feature comparison between the proposed improves laser probes. In case 1, if we used Diode laser for Laser-Ⅱ, we can obtain high speed in terms of number of times in a given duration, and high energy. But the problem is that it is

not cost-effective and the overall size is large. In addition, microscope eyepiece is not made available, and an additional CCD camera installation is needed. In case 2, if we used fiber laser for Laser-Ⅱ, similarly, it can support the high speed but it produces low energy.

However, Fiber laser is cheaper than Diode laser and possible to use the microscope eyepiece. Moreover, the large size problem can be overcome in this case.

Table 3. Feature comparison between proposed improve laser probe ideas

	Case 1. Diode laser	Case 2. Fiber laser
Speed (frequency)	High speed/High frequency	High speed/High frequency
Energy	High energy	Low energy
Cost	High cost	Low cost
Monitoring	Available PC monitoring	Available PC monitoring
Microscope	Not available microscope eyepiece	Available microscope eyepiece
Auxiliary device	Zig module	None
Camera	Additional CCD camera	Built in CCD camera
Special feature	Provides high and efficient functionally but huge in size costly	Extremely compact, highly flexible cable delivery into scan head

On the other hand, Table 4. shows the feature comparison between three different types of lasers. We can see that fiber laser has more advantages (such as extremely compact design, maintenance free operation, allows for easy integration into production and minimal floor space requirements, etc.) over Nd:YAG laser and CO2 laser. The main advantages that make fiber laser superior to other lasers are as follows. 1) It has high optical efficiency which is up to 30% more power efficient than Nd:YAG which gives only 5% and 10% for CO_2. 2) It has better degree of integration into production with minimal floor space, and good air-cooling system (no water chiller required-cost and energy savings). 3) It gives a good quality of laser beam in terms of power with low mean time between failure. 4) It has a good reliability and maintenance free operation, which means there is no cleaning or optical alignment process required for optimum power output.

Table 4. Feature comparison between different lasers[12]

	Fiber laser	Nd:YAG	CO_2
Wall Plug Efficiency	30%	~5%	~10%
Output Powers	to 50㎾	to 6㎾	to 20㎾
BPP(4/5㎾)	〈 2.5	25	6
Diode Lifetimes	100,000	10,000	N.A.
Cooling	Air/Water	Deionized	Water
Floor Space (4/5㎾)	〈 1㎡	6㎡	3㎡
Operating Cost/hour	$21.31	$38.33	$24.27
Maintenance	Not required	Often	Required

V. Conclusion

In this paper, the research on different fault injection tools was studied. The main concept of the idea to improve the laser probe is through utilizing existing equipment. The proposed laser probe can be divided into two parts, which are Laser-I for laser cutting, and Laser-II for fault injection. We study the advantages of existing equipment, and consider the significant parameters such as energy, repetition rate, wavelength, etc. The features and advantages of proposed laser probes are compared. In case 1, Diode laser for Laser-II gives a high speed but it is not cost-effective, and the size is large. It is not made available to use the microscope eyepiece, and an additional CCD camera installation is needed. In case 2, fiber laser is used for Laser-II, which can support high speed and it is cost-effective. The common problem that both the cases are facing is low energy production. Lastly, three different types of lasers are compared and advantages are studied.

Through this research, we study the existing laser probes which are considered efficient enough presently. However, the evolution of the techniques and equipment is moving fast forward. The proposed technique is to utilize and enhance existing equipment, in order to acquire the most efficient tool for the fault injection purpose.

This research contributes to recent technology, trends, and understandings in fault-injection attack with FA tools accuracy and countermeasure. In addition, this research idea can be adapted according to the environment and industries. The development of countermeasures against invasive attack and non-invasive attack is concerned.

References

〔1〕 A.J. Meneze, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Oct. 1996.

〔2〕 R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices," Proceedings of the 5th International Workshop on Security Protocols, pp. 125-136, Apr. 1997.

〔3〕 D. Boneh, R. DeMillo, and R. Lipton, "On the importance of eliminating errors in cryptographic computations," Journal of Cryptology, vol. 14, no. 2, pp. 101-119, Nov. 2001.

〔4〕 E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," in proceedings of CRYPTO'97, LNCS 1294, pp. 513-525, Aug. 1997.

〔5〕 D. Boneh, R. DeMillo, and R. Lipton, "On the importance of checking cryptographic protocols for faults," in proceedings of EUROCRYPT'97, LNCS 1233, pp. 37-51, May, 1997.

〔6〕 F. Bao, R.H. Deng, Y. Han, A. Jeng, A.D. Narasimhalu, and T. Ngair, "Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults," Proceedings of the 5th International Workshop on Security Protocols, Springer-Verlag London, pp. 115-124, Apr, 1997.

〔7〕 A.K. Lenstra, "Memo on RSA signature generation in the presence of faults," Manuscript, September. 1996. Available from Author at arjen.lenstra@citicorp.com

〔8〕 Mei-Chen Hsueh, T.K. Tsai, and R.K. Iyer, "Fault Injection Techniques and Tools," IEEE Computer, Vol. 30, Issue. 4, pp. 75-82, Apr. 1997.

〔9〕 Wikipedia, Failure analysis, http://en.wikipedia.org/wiki/Failure_analysis

〔10〕 Wikipedia, Laser, http://en.wikipedia.org/wiki/Laser

〔11〕 New Wave Research, http://www.esi.com/Products/NewWaveResearch.aspx.

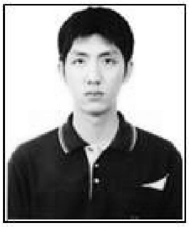
〔12〕 GNTECH, http://gn-tech.net

〔13〕 G.R. Gordon, "The LASER, Light Amplification by Stimulated Emission of Radiation," The Ann Arbor Conference on Optical Pumping, Jun. 1959.

〔14〕 HoonJae Lee, "A study on generalization of Fault-Injection Analysis tools," 2013-046, Dongseo University Industry-Academic Cooperation Foundation, 2013.

〈저자소개〉

이 영 실 (Young-Sil Lee) 정회원
2006년 2월: 동서대학교 정보네트워크학과 학사 졸업
2010년 8월: 동서대학교 디자인&IT전문대학원 유비쿼터스IT학과 석사 졸업
2011년 3월 ~ 현재: 동서대학교 일반대학원 유비쿼터스IT학과 박사과정
2012년 1월 ~ 현재: University of Oulu, Dept. of Electrical Engineering, 박사과정
〈관심분야〉 부채널분석, 암호 알고리즘, 헬스케어 시스템 보안, 센서 네트워크 보안



Thiranant Non 정회원
2013년 3월: Multimedia University (Malaysia), Information Technology 학사 졸업
2013년 3월 ~ 현재: 동서대학교 일반대학원 유비쿼터스IT학과 석사과정
〈관심분야〉 네트워크보안, 클라우드 컴퓨팅, e-Healthcare, 인증 프로토콜

이 훈 재 (HoonJae Lee) 정회원
1987년: 경북대학교 전자공학과 석사 졸업
1998년: 경북대학교 전자공학과 박사 졸업
1987년 ~ 1998년 국방과학연구소 선임연구원/ 팀장
1998년 ~ 2002년 경운대학교 조교수
2002년 ~ 현재: 동서대학교 컴퓨터정보공학부 교수
〈관심분야〉 암호이론, 네트워크보안, 부채널공격, 정보통신/정보네트워크