Optical Fault Injections: a Setup Comparison

Dmytro Petryk, Zoya Dyka and Peter Langendoerfer
IHP
Im Technologiepark 25
Frankfurt (Oder), Germany
{petryk, dyka, langendoerfer}@ihp-microelectronics.com

Abstract— **Semi-conductor based devices are used everywhere in our daily lives. For many of them it is essential to protect the information they gather and communicate. Unfortunate cryptographic approaches can be successfully attacked if physical access to the devices is possible. One of the methods to retrieve important cryptographic data i.e. secret keys is to use fault injection. One approach is the optical fault injection. Nowadays many manufactures apply countermeasures against fault attacks, but adversaries invent and introduce new sophisticated approaches every year to bypass these countermeasures. This paper presents the essentials of optical injection attacks with a short description of experiments carried out. Most of them were published in recent years.**

Keywords — laser fault injection attacks

I. INTRODUCTION

The main goal of fault attacks is to induce an error which can disrupt the intended operation of the device under attack. Exploiting unintended functioning of the device can lead to access to sensitive information such as logins, passwords and other important security data. Fault injection attacks can be performed by impacting on clock, power, temperature, external electromagnetic pulses or by using laser sources. Optical (laser) fault injection (FI) attacks are semi-invasive attacks and were introduced by S. Skorobogatov in 2002 [18]. Experiments were performed using low-cost equipment such as focused camera flash and a laser pointer from a stock market. The attacked device was decapsulated to get access of its internal structure. Laser FI attacks can be performed with accurate timing and precise spatial location which leads to the intended influence only on a certain part of the device but it can also have an impact on contiguous components.

This paper presents a state-of-the-art of optical fault injection attacks, mainly focusing on the literature published in the last 3 years. Section II presents an overview of published experiments. Section III concludes this paper.

II. LASER FI ATTACKS: SHORT OVERVIEW

Most attacked circuits are implementations of cryptographic algorithms AES, RSA, PRESENT-80, ChaCha20, DES or different types of memory cells. The cryptographic algorithms are executed on a microcontroller or on an FPGA, for example: Atmel ATmega1284P, AVR ATmega328P, Xilinx Virtex 5, Xilinx Spartan-6, Xilinx Spartan 3, etc. The most attacked microcontroller is the Atmel AVR ATmega328P [1]-[5]. It is an 8-bit microcontroller produced in a 350 nm technology. It has 1 KB of EEPROM, 32 KB flash memory and 2 KB SRAM [38]. The second often attacked device is a Xilinx FPGA Virtex 5 VLX50T [6]-[9] manufactured in a 65 nm CMOS technology with a flip-chip package. It contains 7200 Virtex-5 FPGA slices and 2160 Kb of RAM. Each Virtex-5 FPGA slice contains four LUTs and four flip-flops [39].

Many laser FIs described in literature were performed with Riscure equipment [1]-[11]. Riscure is an independent worldwide laboratory that provides security testing of semi-conductor products such as smart card or embedded systems [40]. Plenty of attacks were done by backside injection using an infrared laser with 1064 nm wavelength. Frontside injections were performed using a green laser with 532 nm or a red laser with 808 nm wavelength. **Fig. 1** shows the Riscure Diode Laser Station that is a part of the laboratory equipment at the IHP [37].

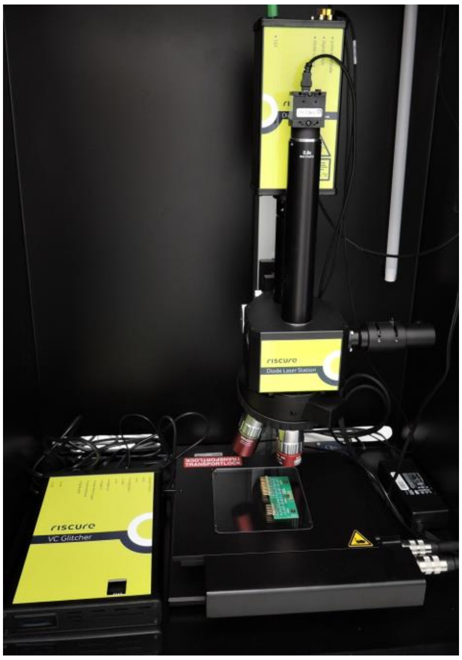

Fig. 1. Riscure Diode Laser Station as a part of the laboratory equipment at the IHP:

- maximum output power is 14 W for the red laser 808 nm and 20 W for the infrared laser 1064 nm;
- pulse duration in range of 20 ns – 100 µs;
- trigger delay 50 ns;
- elliptical spot sizes $60*14\ \mu m^2$, $15*3.5\ \mu m^2$ or $6*1.5\ \mu m^2$;
- X-Y-Z table with 3 µm accuracy and 0.05 µm step size;
- VC glitcher and icWaves.

Authors of [12] and [13] used the Alphanov equipment for their experiments. It is the Pulse-on-Demand module plus (PDM+) [41] that is a single mode laser with fiber output (fibre-optic light guide). This allows to achieve a smaller spot size than those of multimode lasers. Main features of the PDM are: single mode laser, maximum output power from 2 W up to 4.6 W depending on the wavelength, the pulse width can be set from 2 ns to continuous wave, 250 MHz repetition rate, laser wavelengths from 808 nm to 1075 nm, fiber output, spot size 1.5 μm^2 and 3.4 μm^2 with 50x and 20x magnification lens respectively.

Experiments in [14]-[20] were carried out with rare equipment or in specialized labours. In papers [21]-[36] the manufacturer of the used laser is not given.

Successful fault injections depend on a lot of parameters which must be considered when implementing a fault into the device under attack. Only an appropriate combination of these physical parameters can lead to valuable faults that can be exploited in practice. For the laser fault injection attacks these parameters are: wavelength, spot size, chip position (X, Y, Z), timing, pulse width and intensity [9], [12]. Table I gives a short overview of published experiments, attacked devices, applied lasers, etc. Dependent on the effect that can be reached in the behaviour of the attacked circuit, faults are classified into:

- Bit-set: logical state of the attacked cell will be changed from ‘0’ to ‘1’.
- Bit-reset: logical state of the attacked cell will be changed from ‘1’ to ‘0’.
- Bit-flip: logical state of the attacked cell will be changed into opposite logical state.
- Random value: the random change of the cell internal state to the logical ‘1’ or ‘0’.
- Stuck-at: the change of the cell internal state is no more possible.

Predicted behaviour of the attacked circuits was achieved in most conducted experiments (see Table I).

Table I. An overview of published optical fault injection experiments

Ref.	Applied laser	Attacked device (manufactured in technology)	Attacked algorithm	Results
[1]	• 808 nm (14 W) or 1064 nm (20 W) wavelength (multimode), • Pulse duration 20 ns – 100 μs, • 5x, 20x, 50x lenses, • Elliptical spot - 60*14, 15*3.5, 6*1.5 μm2	ATmega328P (350 nm)	ChaCha 20	Instruction skip
[2]			Present 80	Retrieve the key
[3]			-	Bit-flip, instruction skip, stuck-at faults
[4]			-	Stu stuck-at faults, change the address in the instruction
[5]			AES	Sensitive map, XOR skip
[6]		Xilinx Virtex-5 (65 nm)	Present 80	Faults detected. Sensor based on Phase Lock Loop (PLL)
[7]				Digital sensor. Higher detection rate than for PLL
[8]				Faults detected. Sensor used Ring Oscillator (RO) and PLL
[9]				Bit-flip
[10]		Flash (not mentioned)	none	Bit-set
[11]		Smartcard (not mentioned)	DES	Bypass PIN check. Possibility to retrieve a key
[12]	• 975 nm or 1064 nm wave-length (single-mode), • Pulse duration 2 ns, continuous wave • 10x, 20x lenses, • Spot 45, 3.4 μm^2	Cortex A9 (32 nm)	RSA, AES	Bit-flip, bit-reset
[13]		ATxmega16A4U (250 nm)	AES	Stable faults
[14]	• Hamamatsu PHEMOS-1000, • 1330 nm wave-length (C13193), • 5x, 20x lens	Xilinx Kintex 7 (28 nm)	AES	Defined logic location, plaintext output, AES core, bus width
[15]	• X-ray beamline ID16B in ESRF, • Beam 60*60 nm^2, • 10x lens	ATmega1284P (350 nm)	none	Semi-permanent stuck-at faults
[16]	• Gemplus station with 532 nm pulsed laser wavelength,	RTL version (130 nm)	RSA	Evaluated hardened and reference RTL versions against fault injection
[17]	• Gemalto platform with 532 nm laser, • 6 ns pulse, • Spot – 220 μm^2	Crypto processor (130 nm)	DES	Assessment of detection rate.
[18]	• probing station Wentworth Labs MP-901, • Laser pointer with 650 nm wave, • 1 μm^2 spot, • 10 mW power	PIC16F84 (1.2 μm)	-	Bit-set, bit-reset

[19]	• PIKO4 with 870 and 1080 nm lasers, • Spot – 10, 30 μm^2	IC (180 nm CMOS)	-	Assessment of impact of direction of the laser polarization.
[20]	• “Radon” laser simulators series, • 1064 nm wave, • 8-10 ns pulse	IC (250 nm CMOS & 1 μm BiCMOS)	-	Estimated the influence of polarization.
[21]	• 785 nm wave-length diode laser, • 100 mW power, • Fiber-optic 1 mm	8-bit Microcontroller (not mentioned)	RSA-CRT	Bit-set, skip program commands
[22]	• 532 and 1064 nm wavelength lasers, • 800 ps pulse, • 20x lens	Xilinx Spartan-6 (45 nm)	AES	Bit-set, bit-reset
[23]	• 532 and 1064 nm lasers, • 5 ns pulse, • Spot – 125*125 and 50*50 μm^2	IC (130 nm)	AES	Comparison of fault rate for frontside and backside
[24]	• Spot –1, 5, 20 μm^2	B18 design (ITC99) (not mentioned)	AES	Validated a fault model to predict laser attacks
[25]	• 1064 nm laser, • 3 W power, • 50 ns pulse, • Spot –1, 5, 20 μm^2	SRAM cell (250 nm CMOS)	-	Sensitive map, Obtain only two of four sensitive spots for bit-set, bit-reset
[26]	• 1030 nm laser with 3 W power, • 30 ps pulse, • Spot –1, 5, 20 μm^2		-	Sensitive map, Obtain all four sensitive spots for bit-set, bit-reset
[27]	• 1064 nm laser, • 800 mW power, • Tens of ns pulse, • 50x lens	Microcontroller (90 nm)	AES	Image of the smartcard, bit-set, bit-reset
[28]	• 1064 nm laser, • 3 W power, • 50 ns pulse, • 20x, 100x lenses	SRAM cell (CMOS 90 nm, FD-SOI 28 nm)	-	Comparison of sensitivity against optical attack for CMOS and FD-SOI
[29]	• 1064 nm laser, • 855 mW power, • 20 μs pulse, • Spot –5 μm^2	16-bit multiplier (28 nm)	-	Bit-set, bit-reset, bit-flip
[30]	• 590 and 1260 nm lasers, • 1 ps, 150 fs pulse, • Spot –0.9, 1.3 μm^2	SRAM cell (180 nm)	-	Sensitive areas for SEL
[31]	• 532 nm laser, • 5 ns pulse, • 125*125 μm^2 spot,	ASIC (130 nm)	AES	Bit-set, bit-flip
[32]	• 650 and 1065 nm lasers, • 25, 75 mW power, • 1 μm^2 spot with 20x lens	PIC16F84 (1.2 μm), PIC16F628 (0.9 nm), PIC16F628A (0.5 nm), MSP430F112 (0.35 nm)	-	Erase and write operations into the memory
[33]	• 254 nm UV lamp	CY27H010 (not mentioned), PIC16F54, (not mentioned) PIC16F84 (1.2 μm), AT89C205, (not mentioned) ATmega48 (not mentioned)	AES	Erase operations, possibility to retrieve a key
[34]	• 915 nm laser with 20 W power, • 15 ns pulse, • 100x lenses, spot – 2 μm^2	ASIC VA64_HDR9a (0.8 and 1.2 μm)	-	Sensitive map, SEL, bit-flip
[35]	• 930 nm laser, • 1 ps pulse, • 20x lens, spot – 2 μm^2	Operational Amplifier LM 124 (not mentioned)	-	SET sensitive map, energy comparison for front- and backside attack
[36]	• 1060 nm laser • 10-15 ns pulse	IC (180 nm)	-	Evaluation of diffraction coefficient

III. CONCLUSION

Fault injection attacks are very dangerous nowadays for chip manufacturers. Induced current caused by light, laser beam, heavy ion irradiation, etc. can disrupt proper functioning of the device. Thus, performing optical injection can help the adversary to retrieve and/or modify the sensitive data stored in the attacked chip. This paper presented an overview of experiments described in literature as a table (see Table I). Using Table I the attacked devices, the used equipment and the attack results can be easily compared. 29 of 36 referenced papers reported backside attacks using an infrared laser with 1064 nm wavelength.

ACKNOWLEDGMENT

This project has received funding from the European Union’s Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 722325.

REFERENCES

[1] S.V. Dilip Kumar, Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, Shivam Bhasin, Anupam Chattopadhyay, and Anubhab Baksi, “A Practical Fault Attack on ARX-like Ciphers with a Case Study on ChaCha20”, Fault Diagnosis and Tolerance in Cryptography (FDTC), IEEE, Sept. 2017, pp. 33-40.

[2] Sikhar Patranabis, Debdeep Mukhopadhyay, Jakub Breier, Shivam Bhasin, “One Plus One is More than Two: A Practical Combination of Power and Fault Analysis Attacks on PRESENT and PRESENT-like Block Ciphers”, Fault Diagnosis and Tolerance in Cryptography (FDTC), IEEE, Sept. 2017, pp. 25-32.

[3] Jakub Breier, Dirmanto Jap and Shivam Bhasin, “The Other Side of The Coin: Analyzing Software Encoding Schemes Against Fault Injection Attacks”, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), May 2016, pp. 209-216.

[4] Jakub Breier and Dirmanto Jap, “Testing Feasibility of Back-Side Laser Fault Injection on a Microcontroller”, In Proceedings of the WESS'15: Workshop on Embedded Systems Security, WESS'15, New York, NY, USA, 2015. ACM, pp. 51-56.

[5] Jakub Breier, Dirmanto Jap and Chien-Ning Chen, “Laser profiling for the back-side fault attacks with a Practical Laser Skip Instruction Attack on AES”, In First Cyber-Physical System Security Workshop (CPSS 2015), ACM, Apr. 2015, pp. 99-103.

[6] Wei He, Jakub Breier and Shivam Bhasin, “An FPGA-compatible PLL-based sensor against fault injection attack”, In Proceedings of the 22nd Asia and South Pacific Design Automation Conference (ASP-DAC), Jan. 2017, pp. 39-40.

[7] Wei He, Jakub Breier and Shivam Bhasin “Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks”, In International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE'16), Dec. 2016, pp. 27-46.

[8] Wei He, Jakub Breier, Shivam Bhasin, Noriyuki Miura and Makoto Nagata, “Ring oscillator under laser: Potential of pll based countermeasure against laser fault injection”, In Fault Diagnosis and Tolerance in Cryptography (FDTC), IEEE, Aug. 2016, pp. 102-113.

[9] Jakub Breier, Wei He, Dirmanto Jap, Shivam Bhasin and Anupam Chattopadhyay, “Attacks in Reality: The Limits of Concurrent Error Detection Codes against Laser Fault Injection”, Journal of Hardware and Systems Security, Springer, 1 (4), 2017, pp. 298-310.

[10] Feifei Cai, Guoqiang Bai, Huizhi Liu and Xiaobo Hu, “Optical Fault Injection Attacks for Flash Memory of Smartcards”, 6th International Conference on Electronics Information and Emergency Communication (ICEIEC), June 2016, pp. 46-50.

[11] Jasper G. J. van Woudenberg, Marc F. Witteman, Federico Menarini, “Practical optical fault injection on secure microcontrollers”, Workshop on Fault Diagnosis and Tolerance in Cryptography, Sept. 2011, pp. 91-99.

[12] Aurelien Vasselle, Hugues Thiebeauld, Quentin Maouhoub, Adele Morisset, Sebastien Ermeneux, “Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot”, Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Sept. 2017, pp. 41-48.

[13] Falk Schellenberg, Markus Finkeldey, Nils Gerhardt, Martin Hofmann, Amir Moradi and Christof Paar, “Large Laser Spots and Fault Sensitivity Analysis”, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), May 2016, pp. 203-208.

[14] Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert and Christian Boit, “On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs”, Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Nov. 2017, pp. 1661-1674.

[15] Stephanie Anceau, Pierre Bleuet, Jessy Clediere, Laurent Maingault, Jean-luc Rainard and Remi Tucoulou, “Nanofocused X-Ray Beam to Reprogram Secure Circuits”, Cryptographic Hardware and Embedded Systems (CHES), Aug. 2017, pp. 175-188.

[16] R. Leveugle, “Early Analysis of Fault-Based Attack Effects in Secure Circuits”, IEEE Transactions on Computers, Volume: 56, Issue: 10, Oct. 2007, pp. 1431-1434.

[17] Y. Monnet, M. Renaudin, R. Leveugle, N. Feyt, P. Moitrel, F. M'Buwa Nzenguet, “Practical Evaluation of Fault Counter-measures on an Asynchronous DES Crypto Processor”, 12th IEEE International On-Line Testing Symposium (IOLTS'06), July 2006, pp.125-130.

[18] Sergei P. Skorobogatov and Ross J. Anderson, “Optical Fault Induction Attacks”, Cryptographic Hardware and Embedded Systems (CHES), Feb 2002, pp. 2-12.

[19] P. K. Skorobogatov, A. V. Sogoyan, G. G. Davydov, A. N. Egorov, and D. V. Savchenkov, “The Impact of Laser Polarization Direction on Local Dose Rate Effects Simulation for Modern Integrated Circuits”, Russian Microelectronics, Volume 44, Issue 1, January 2015, pp. 22–26.

[20] P.K. Skorobogatov, G.G. Davydov, A.V. Sogoyan, A.Y. Nikiforov, A.N. Egorov, “The Impact Of Plane-Polarized Unfocused Laser Radiation On Bulk Ionization In Deep-Submicron Modern ICs”, 15th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Sept. 2015, pp. 1-4.

[21] Jörn-Marc Schmidt and Michael Hutter, “Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results”, In Karl C. Posch, J.W. (ed.) Proceedings of 15th Austrian Workhop on Microelectronics (Austrochip’07), Graz, 2007, pp. 61–67.

[22] Bodo Selmke, Johann Heyszl and Georg Sigl, “Attack on a DFA protected AES by Simultaneous Laser Fault Injections”, Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Aug. 2016, pp. 36-46.

[23] Stephan De Castro, Jean-Max Dutertre, Bruno Rouzeyre, Giorgio Di Natale and Marie-Lise Flottes, “Frontside Versus Backside Laser Injection: A Comparative Study”, Journal on Emerging Technologies in Computing Systems (JETC) - Special Issue on Secure and Trustworthy Computing, Volume 13 Issue 1, Article No. 7, Dec. 2016, pp. 1-15.

[24] Athanasios Papadimitriou, David Hély, Vincent Beroulle, Paolo Maistri, Regis Leveugle, “Analysis of laser-induced errors: RTL fault models versus layout locality characteristics”, Microprocessors and Microsystems, Volume 47, Part A, Nov 2016, pp. 64-73.

[25] Cyril Roscian, Alexandre Sarafianos, Jean-Max Dutertre and Assia Tria, “Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells”, Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Aug. 2013, pp. 89-98.

[26] Marc Lacruche, Nicolas Borrel, Clément Champeix, C. Roscian, A. Sarafianos, Jean-Baptiste Rigaud, Jean-Max Dutertre, Edith Kussener, “Laser Fault Injection into SRAM cells: Picosecond versus Nanosecond pulses”, IEEE 21st International On-Line Testing Symposium (IOLTS), July 2015, pp 13-18.

[27] Franck Courbon, Jacques J.A. Fournier, Philippe Loubet-Moundi and Assia Tria, “Combining image processing and laser fault injections for characterizing a hardware AES”, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Volume: 34, Issue: 6, June 2015, pp. 928-936.

[28] Jean-Max Dutertre, Stephan De Castro, Alexandre Sarafianos, No´emie Boher, Bruno Rouzeyre, Mathieu Lisart, Joel Damiens, Philippe Candelier, Marie-Lise Flottes and Giorgio Di Natale, “Laser attacks on integrated circuits from CMOS to FD-SOI”, 9th IEEE International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS), May 2014, pp. 1-6.

[29] R. Leveugle, P. Maistri, P. Vanhauwaert, F. LuG. Di Natale, M.-L. Flottes, B. Rouzeyre, A. Papadimitriou, D. Hély, V. Beroulle, G. Hubert, S. De Castro, J.-M. Dutertre, A. Sarafianos, N. Boher, M. Lisart, J. Damiens, P. Candelier, C. Tavernier, “Laser-induced Fault Effects in Security-dedicated Circuits”, 22nd International Conference on Very Large Scale Integration (VLSI-SoC), Oct. 2014, pp. 1-6.

[30] N. A. Dodds, N. C. Hooten, R. A. Reed, R. D. Schrimpf, J. H. Warner, N. J.-H. Roche, D. McMorrow, S. Buchner, S. Jordan, J. A. Pellish, W. G. Bennett, N. J. Gaspard, and M. P. King, “SEL-Sensitive Area Mapping and the Effects of Reflection and Diffraction From Metal Lines on Laser SEE Testing”, IEEE Transactions on Nuclear Science, Volume: 60, Issue: 4, Aug. 2013, pp. 2550 – 2558.

[31] Cyril Roscian, Jean-Max Dutertre, Assia Tria, “Frontside Laser Fault Injection on cryptosystems. Appacation to the AES last round”, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), June 2013, pp. 119-124.

[32] Sergei Skorobogatov, “Optical Fault Masking Attacks”, Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Aug. 2010, pp. 23-29.

[33] Jörn-Marc Schmidt, Michael Hutter, Thomas Plos, “Optical Fault Attacks on AES: A Threat in Violet”, Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Sept. 2009, pp 13-22.

[34] B. Alpat, R. Battiston, M. Bizzarri, D. Caraffini, E. Fiori, A. Papi, M. Petasecca, A. Pontetti, “The radiation sensitivity mapping of ICs using an IR pulsed laser system”, Microelectronics Reliability, Volume 43, Issue 6, June 2003, pp. 981-984.

[35] Dean Lewis, Vincent Pouget, Felix Beaudoin, Philippe Perdu, Herve Lapuyade, Pascal Fouillat, and Andre Touboul, “Backside Laser Testing of ICs for SET Sensitivity Evaluation”, IEEE Transactions On Nuclear Science, Vol. 48, No. 6, Dec. 2001, pp. 2193-2201.

[36] P. K. Skorobogatov, “Laser Simulation of Volume Ionization Effects in Submicron VLSI circuits”, Russian Microelectronics, Volume 42, Issue 7, Dec. 2013, pp 420–423.

[37] IHP - Innovations for High Performance Microelectronics: https://www.ihp-microelectronics.com/en/start.html.

[38] Microchip Technology, ATmega328P datasheet: http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-42735-8-bit-AVR-Microcontroller-ATmega328-328P_Datasheet.pdf

[39] Xilinx Virtex-5 Family Overview: https://www.xilinx.com/support/documentation/data_sheets/ds100.pdf

[40] Riscure: https://www.riscure.com/about-riscure/

[41] Alphanov. Single-Mode Laser Source For Full Temporal Agility: http://www.alphanov.com/8-optoelectronics-systems-pulse-on-demand-modules.html#technical-specifications