Research Article

Sven Frohmann*, Enrico Dietz[a], Helmar Dittrich and Heinz-Wilhelm Hübers

Picosecond imaging of signal propagation in integrated circuits

DOI 10.1515/aot-2017-0001
Received January 4, 2017; accepted February 7, 2017; previously published online March 15, 2017

Abstract: Optical analysis of integrated circuits (IC) is a powerful tool for analyzing security functions that are implemented in an IC. We present a photon emission microscope for picosecond imaging of hot carrier luminescence in ICs in the near-infrared spectral range from 900 to 1700 nm. It allows for a semi-invasive signal tracking in fully operational ICs on the gate or transistor level with a timing precision of approximately 6 ps. The capabilities of the microscope are demonstrated by imaging the operation of two ICs made by 180 and 60 nm process technology.

Keywords: cybersecurity; hot carrier luminescence; imaging; microscopy; photon emission.

1 Introduction

Photon emission from pn-junctions has been known since 1955 [1]. However, it was not used as an analyzing method to investigate faults in integrated circuits (ICs) before the 1990s. The most dominant process for photon emission in modern CMOS ICs is hot carrier luminescence (HCL) [2]. It occurs when transistors operate in saturation mode, and charge carriers flow through the conduction channel. Due to the high electric field, the carriers are accelerated from source toward the drain. In a saturated MOSFET, the electrical field attains its maximum near the edge of the drain where some carriers gain enough energy to emit photons by direct and indirect transitions. As the mobility of electrons is three times higher than that of holes, the emission is much stronger in n-type transistors. The spectrum of HCL is given by the energy distribution of the carriers and hence ranges from the visible to the infrared with an intensity maximum ranging from 1000 to 1500 nm. The photon emission probability depends on the supply voltage and is about 10^{-4} to 10^{-6} photons per electron [3]. This and the extremely low electrical currents of modern ICs result in the generation of only about one HCL photon per switching cycle of a transistor. Besides the low emission rate, the epitaxial side of an IC is almost completely blocked for photon emission by multiple, densely packed metal layers that provide the electrical connection. Therefore, photon emission is observed from the backside through the silicon substrate [4]. Reabsorption in the silicon and total internal reflection at its air interface reduce the already low number of available photons further by a factor of about 100. Therefore, very sensitive near-infrared (NIR) single-photon detectors are required. Achieving spatial and temporal resolution at the same time typically involves complex imaging photomultiplier detectors [5], which are limited to wavelengths below 900 nm. To avoid these obstacles, different detector technologies need to be applied for high-resolution spatial and temporal measurements [6]. A commercially available system is TriPHEMOS from Hamamatsu [7]. It relies on a camera for spatial overview images and a single-photon detector for temporal analyses.

Besides the failure analysis of ICs, photon emission analysis is highly relevant for analyzing the logic functions of a security IC [8, 9], in particular, decoding cryptoalgorithms that are implemented in security applications such as smart cards [10]. One example are so-called physically unclonable functions (PUFs) that are implemented in certain ICs for security applications. Such PUFs are promising to overcome insecure data storage, hardware counterfeiting, and many other security problems. However, it has been shown recently that specific versions of PUFs can be completely characterized by means of photonic

[a]Present address: Bundesdruckerei GmbH, Kommandantenstraße 18, 10629 Berlin, Germany
***Corresponding author: Sven Frohmann,** Department of Optics and Atomic Physics, Technische Universität Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany, e-mail: sven.frohmann@tu-berlin.de
Enrico Dietz and Helmar Dittrich: Department of Optics and Atomic Physics, Technische Universität Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany
Heinz-Wilhelm Hübers: Department of Optics and Atomic Physics, Technische Universität Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany; and Deutsches Zentrum für Luft- und Raumfahrt e.V., Institute of Optical Sensor Systems, Rutherfordstr. 2, 12489 Berlin, Germany

emission analysis. This demonstrates the relevance of photon emission analysis for hardware security of ICs [11].

In this paper, we describe the design of a novel photon emission microscope for picosecond imaging of HCL. Its performance is evaluated by analyzing two ICs made by 180 and 60 nm process technology.

2 Photon emission microscope

A schematic drawing of the microscope is shown in Figure 1. It has been realized in a modular manner, allowing a flexible adaption to a variety of measurements and analysis schemes. Despite its modularity, everything fits on a small breadboard with an area < 0.25 m^2. It consists of the sample carrier module (1), the single-photon detector module (2), and the CCD camera module (3; see Figure 1).

The design of the sample carrier module provides the stable fastening of the IC board with its attached supply and control electronics and an accurate positioning with all 6 degrees of freedom. This enables the precise positioning of the IC with respect to the optical axis of the system. Large travel ranges of 50 mm of the motorized three-axis linear stage allows the usage of various ICs without particular requirements to their package or printed circuit board (PCB) layout.

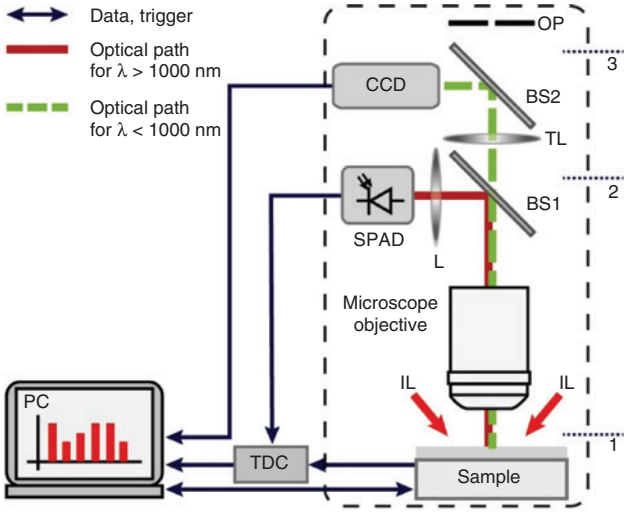

Figure 1: Schematic drawing of the photon emission microscope.

The photon emission from the IC under test is collected by interchangeable infrared-optimized Olympus microscope objectives with magnifications from 10 to 100. High numerical apertures of the objectives from 0.3 to 0.85 and adjustable spherical aberration compensation enable diffraction-limited resolution down to about 600 nm. As mentioned above for high-resolution emission imaging and picosecond temporal resolution, two dedicated detectors are used: a CCD camera and a single-photon avalanche detector (SPAD).

The CCD is used mainly to navigate on the IC to take overview images of large areas of the IC and acquire HCL images. Therefore, a CCD with high spatial resolution, low noise, and high dynamic range is preferred. Liquid nitrogen-cooled InGaAs cameras are generally a good choice. They are required if ICs are investigated, which are manufactured in processes smaller than 40 nm. In this case, HCL is spectrally shifted to wavelengths above 1000 nm [12]. However, ICs that are used in security applications are usually fabricated in larger-size process technology. Therefore, an NIR-optimized silicon CCD is the better choice due to the higher spatial resolution and higher dynamic range, which can be achieved with this CCD [13]. For temporal HCL analyses, however, silicon-based SPADs are not sufficient because of their limited sensitivity. As most of the spectrum of the HCL is in the NIR, two detector technologies are applicable: InGaAs SPADs and superconducting single-photon detectors (SSPDs). At first glance, SSPDs seem to be the better choice as they have quantum efficiencies of 70% and higher, high temporal resolution of <100 ps, and very low noise [14, 15]. However, SSPDs are difficult to handle: they require cooling with liquid helium, and their sensor areas are a few micrometers in diameter, making it difficult to collect all HCL photons. Accordingly, in our setup, an InGaAs SPAD is used for high temporal resolution measurements and an NIR-optimized CCD is used for overview images.

Both detectors operate in different spectral regions and capture HCL light simultaneously, hence effectively caching nearly every available photon. To achieve this performance, collected emission is divided spectrally by a short-pass filter and beam splitter BS1 (Figure 1) and guided along two different paths to the two detectors. Wavelengths <1000 nm are transmitted through BS1 and are imaged onto the CCD camera (Andor iKon-M 934 BR-DD). The camera is equipped with a 1 MP backside illuminated deep depletion-type silicon CCD sensor with enhanced sensitivity in the NIR spectral region with a quantum efficiency of 30% at 1000 nm. Thermoelectrical cooling to –70°C minimizes dark current for long exposure

times up to many minutes to collect enough photons from the weak HCL of the operating IC.

Although the CCD collects light with wavelengths <1000 nm, the spectral part above 1000 nm is reflected by BS1 and imaged onto the SPAD (model ID220 from ID Quantique). It uses a cooled InGaAs diode in Geiger mode for time-resolved single-photon detection with quantum efficiency up to 20% in the NIR wavelength region between 1000 and 1700 nm. It is fiber coupled and detects photons from a region of the IC selected by the microscope objective. The size of the region, from where light is detected, can be adjusted by changing the focal length of the imaging lens L or using fibers with different diameters. The feasible adjustment range is from above 50 µm down to a diffraction-limited spot of approximately 0.8 µm. The latter typically enables single transistor or at least single logic gate measurements. Each signal from a single photon is time tagged by a field-programmable gate array (FPGA)-based time-to-digital converter (TDC) with 81 ps resolution. The signal is correlated to a time reference signal that is also registered by the TDC [16]. The source of the time reference signal depends on the analysis to be done and can, for example, originate from the IC. The complete timing precision of the detector and TDC is about 190 ps for a single photon. The total temporal resolution of the set-up is defined by the jitter of the detection electronics, including the SPAD, and by the temporal resolution of the TDC. This leads to a temporal resolution of about 200 ps. Thus, two events can be resolved only when they are at least 200 ps apart. This corresponds to a maximum transistor switching frequency of 2.5 GHz.

However, accumulating many photons from a periodic signal with a temporal super-resolution technique largely enhances the timing precision. This is done by repeating a measurement several times until the time of the observed single-photon event is represented by a Gaussian-like distribution in the timing histogram of photons from the same location on the chip (see Figure 2). By calculating the centroid of such distribution, photons emitted from different transistors or temporal events can be distinguished temporally with a timing precision better than the timing base of 81 ps of the TDC [11]. Using this technique, we achieved a precision of 6 ps in our measurements. The temporal precision is limited by two factors: the timing precision and temporal stability of the TDC's clock system and a thermal drift in the electronics of the sample IC and the electronics connected to it. The thermal drift limits the maximum time for a single measurement. To achieve a precision of 6 ps, the duration of a single temporal photon emission measurement is <1 min.

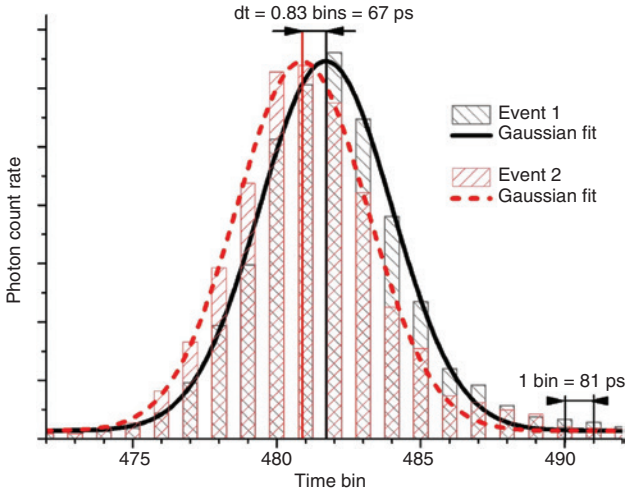

Figure 2: Illustration of the principle of the temporal super-resolution technique to increase the timing precision of temporal measurements.

3 Sample preparation

As mentioned above, optical access to a modern IC is most efficient through the substrate. This allows obtaining an undisturbed and unshielded view to the transistor layer of the circuit, where HCL originates. However, it requires that the package of the IC must be opened and the rough backside surface of the silicon substrate must be polished to optical quality to achieve adequate imaging capabilities. To reduce the reabsorption of photons with energies above silicon's band-gap, a prior thinning of the substrate is advantageous.

The preparation of the ICs investigated in this study is done with a computerized numerical control (CNC) milling machine and the preferred IC package types are quad flat packages (QFP). They provide good access to the IC die from the bottom and can be easily mounted upside down on a PCB. The preparation steps are as follows: (1) grinding a hole in the bottom of the package material with a coarse diamond milling tool up to the copper chip carrier, (2) manually removing the chip carrier pad and adhesive, (3) grinding the silicon substrate with a fine diamond tool up to about 20–30 µm, (4) lapping with diamond paste to the target depth, and (5) polishing with very fine aluminum oxide powder.

The process steps come along with regular cleaning and measuring of the actual depth until the targeted depth is reached. Lapping and polishing steps are performed with self-made tool holder that provides uniform contact pressure. The tool path is a complex nonperiodic curve to minimize periodic tooling marks. The small tool diameter

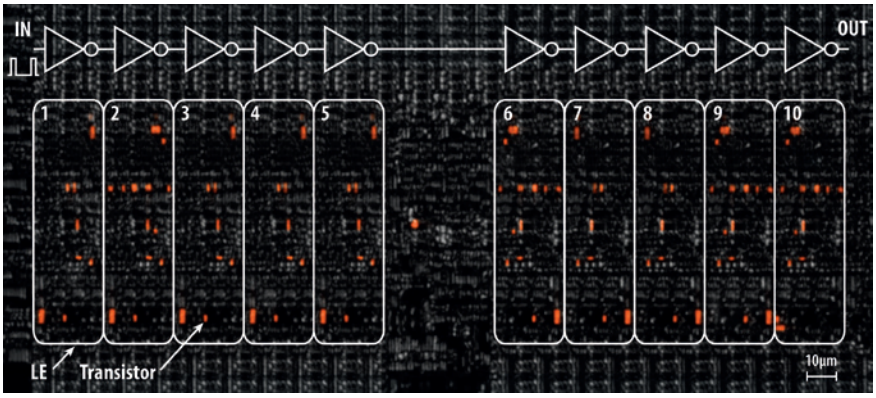

Figure 3: HCL overview image of an inverter chain with 10 elements realized in 10 LEs of an Altera Max V CPLD.

enables the perfect preparation of the IC die, including its borders and corners without harming the lead frame or bond wires.

4 Experiments

Combining the image data of the CCD with the time-resolved data of the SPAD enables picosecond imaging for circuit analysis (PICA) [17]. It allows for semi-invasive signal tracking in a fully operational IC on its gate or even single transistor level. A PICA is created from an HCL CCD image (Figure 3), where the emitting transistors in the image are temporally masked based on the temporal data obtained from measurements with the SPAD. For this at every transistor position in the HCL CCD image, a measurement with the SPAD is performed. A dedicated software has been developed. With this software, the HCL CCD image is pixel-precise temporally masked and processed to a video. The diameter of the SPAD's measuring point had been adapted to the size of the transistors. Its position was changed by moving the IC in lateral direction as described in Section 2.

With a timing precision of about 6 ps, we achieve an equivalent frame rate of more than 100 billion frames per second. Figure 4 shows the selected frames from a PICA video made with our microscope, where the signal propagation within a single logic element (LE) of an Altera Max V complex programmable logic device (CPLD; 180 nm process) is shown. The LE was programmed as inverter. The presented frames show distinctive moments of how the signal and hence the photon emission locations propagate through the logic gates of the LE. Image A in Figure 4 shows the time-integrated photon emission seen by the CCD camera when the LE is driven with a periodic input signal. All involved transistors become visible due to their photon emission while switching. Image B shows the moment when the input signal appears at the input transistors of the LE. Note that only a falling input edge creates an emission at the input and that rising and falling input edges propagate through different transistors that are color coded in the frames. The signal section corresponding to the rising input signal is red colored, whereas the successive signal section that corresponds to the falling input signal is green colored. The PICA video frames of both signal sections are overlaid in images B to E. Image C

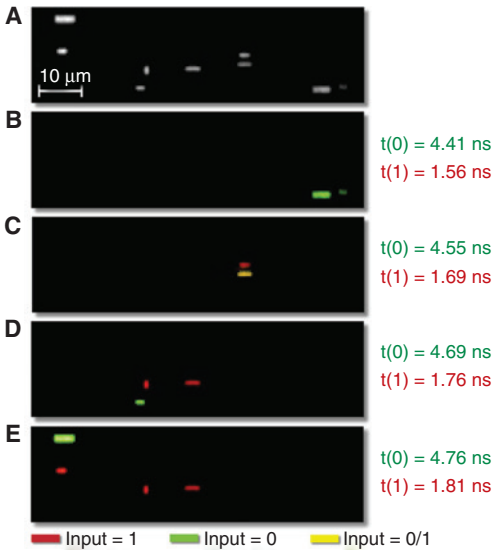

Figure 4: Time series of photon emission of the signal propagation in the third LE shown in Figure 3.
(A) Photon emission image integrated over the whole propagation time. (B–E) Overlaid emission images for both logical input states of the inverter (red, logical high; green, logical low) observed at the time given on the right. IC supply voltage was 2.2 V and its substrate was thinned to 30 µm and polished. Electrical input signal: 3 ns low-voltage TTL pulses with 50 MHz.

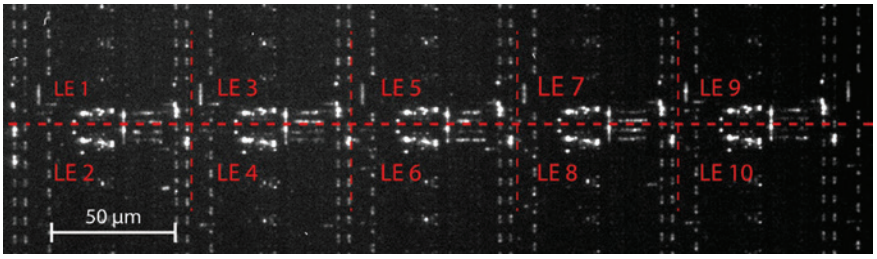

Figure 5: Photon emission image of several adjacent LEs in an Altera Cyclone IV FPGA with a feature size of 60 nm. IC supply voltage Vcc 1.4 V, clock rate 50 MHz, exposure time 5 min, and substrate thickness 15 µm.

shows a transistor (red) that switches only with rising input and another (yellow) that switches at both input edge directions (red and green). Finally, in image E, the inverted input signal is present on the output transistors of the LE, which are the leftmost two. The large green-colored area is the p-MOS transistor that drives the output to logical 1 and the smaller red one is the n-MOS transistor that drives the output to logical 0 at the given times. The observed propagation time from input to output is about 0.3 ns. This time depends on the programmed logic operation of the LE. The time series shown in Figure 4 is from the third inverter of the inverter chain shown in Figure 3. A periodic input signal with a pulse length of 3 ns and a frequency of 50 MHz was applied to the first inverter using an arbitrary waveform generator. The registered photon events were time correlated to that periodic input signal. In the measurement of Figure 4, the video's start point is arbitrary, because only relative time data are relevant. Therefore, the time differences caused by the propagation delay in the connected cables had not been matched, resulting in a temporal offset seen in Figure 4.

To demonstrate that photon emission analysis is feasible on more modern ICs than the Altera Max V of Figure 3, first experiments were done on an Altera Cyclone IV FPGA made in a 60 nm process. Figure 5 shows the photon emission from an Altera Cyclone IV. Although it needs about 10 times longer integration times and it gets more difficult to distinguish single transistors, single LEs and their inputs and outputs can still clearly be identified and addressed for time-resolved analysis.

5 Summary

We developed a photon emission microscope for picosecond imaging of ICs with a spatial resolution of 600 nm and a temporal precision of 6 ps. It is realized by combining two cost-effective maintenance-free detector technologies that complement each other: a silicon NIR-optimized CCD camera for overview images and navigation on the IC and a single-photon InGaAs avalanche diode for time-resolved measurements. Compared to silicon SPAD or NIR-optimized photomultiplier solutions, this enables access to low-voltage ICs whose HCL is in the NIR above 1000 nm. From the results obtained with an FPGA fabricated in 60 nm process, we assume that this method is also feasible for 45 nm processes albeit CCD exposure and SPAD integration times will increase. For ICs manufactured in processes smaller than 45 nm, a liquid nitrogen-cooled InGaAs camera instead of the NIR-optimized silicon CCD is required because, with smaller process sizes, HCL spectra shift to wavelengths above 1000 nm. Peltier-cooled InGaAs cameras are generally insufficient for HCL analyses because of their relatively high dark currents [18]. The system presented here is a powerful tool for failure analysis and for benchmarking security ICs, which complements or replaces other tools.

Acknowledgments: H.D. acknowledges support from the Helmholtz Research School on Security Technologies.

Funding: German Federal Ministry of Education and Research (BMBF); The IKT2020 Program (16KIS0014).

References

[1] R. Newman, Phys. Rev. 100, 700–703 (1955).
[2] J. Bude, N. Sano and A. Yoshii, Phys. Rev. B 45, 5848 (1992).
[3] A. L. Lacaita, F. Zappa, S. Bigliardi and M. Manfredi, IEEE Trans. Electron Devices 40, 577–582 (1993).
[4] C. Boit, Microelectronics Failure Analysis Desk Reference, 6th ed. (ASM International, OH, USA, 2011) pp. 297–291.
[5] J. C. Tsang, J. A. Kash and D. P. Vallett, IBM J. Res. Dev. 44, 583–603 (2000).
[6] A. Schlösser, E. Dietz, S. Frohmann and S. Orlic, Meas. Sci. Technol. 24, 035102-5 (2013).
[7] http://www.hamamatsu.com/resources/pdf/sys/SSMS0005E_TriPHEMOS.pdf (2017).

[8] S. Skorobogatov, Workshop on Fault Diagnosis and Tolerance in Cryptography, (FDTC, 2009), pp. 111–119.
[9] A. Schlösser, D. Nedospasov, J. Krämer and J.-P. Seifert, J. Cryptogr. Eng. 3, 3–15 (2013).
[10] J. Krämer, D. Nedospasov, A. Schlösser and J.-P. Seifert, Construct. Side-Channel Anal. Secure Des. 7864, 1–16 (2013).
[11] S. Tajik, E. Dietz, S. Frohmann, H. Dittrich, D. Nedospasov, et al., J. Cryptol. 30, 550–571 (2017).
[12] J. A. Rowlette, E. B. Varner, S. Seidel and I. C. Bailon, 16th Annu. Meet. IEEE Lasers Electro-Opt. Soc. 2, 740–741 (2003).
[13] http://www.andor.com/scientific-cameras/ikon-xl-and-ikon-large-ccd-series/ikon-m-934 (2017).
[14] C. M. Natarajan, M. G. Tanner and R. H. Hadfield, Supercond. Sci. Technol. 25, 063001 (2012).
[15] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, et al., Nat. Photonics 7, 210–214 (2013).
[16] W. Becker, ISBN: 978-3-319-14928-8 (Springer International Publishing, 2015)
[17] D. Vallet, Microelectronics Failure Analysis Desk Reference, 6th ed. (ASM International, 2011), pp. 292–300.
[18] H. Nakyay, Y. Komiyama, N. Kashikawa, T. Uchida, T. Nagayama, et al., Proc. SPIE 9915, 99151O (2016).