Journal of Hardware and Systems Security (2020) 4:1–10
https://doi.org/10.1007/s41635-019-00068-8

Practical Partial Hardware Reverse Engineering Analysis

For Local Fault Injection and Authenticity Verification

Franck Courbon[1]

Received: 31 May 2018 / Accepted: 15 March 2019 / Published online: 6 April 2019

Abstract
Reverse engineering typically requires expensive equipment, skilled technicians, time, a cross section of the component to be sliced out and a dedicated reconstruction software. In this paper, we present a low-cost alternative, combining fast frontside sample preparation, electron microscopy imaging, error-free standard cell recognition and within and between-die standard cell statistical analysis (SCSA). Step-by-step, we depict the process to access the transistor's drain/source area, to acquire the full area of a single chip layer, to adapt pattern recognition for standard cells and to analyze the standard cell width, local/global location and occurrences number. The inner workings of each step are accompanied by results on 45–65-nm FCBGA devices enabling to locate specific areas (e.g. registers, hardware accelerator). We particularly point out the importance of such design information extraction for local fault injection and hardware assurance. The primary goal is to analyze how much design information of a complex integrated circuit can be retrieved with minimal costs and without outsourcing.

Keywords Standard cell · Partial reverse engineering · Pattern recognition · Statistical analysis · Countermeasures

1 Introduction

Hardware-based vulnerabilities of integrated circuits (ICs) running security applications allow an attacker to retrieve sensitive data or bypass security mechanisms. Reverse engineering [1], a specific kind of attack, is seen as an expansive approach compared to side-channel or even fault attack approaches. However, products include more and more countermeasures regarding side-channel and fault attacks at the development stage, thus reducing such attack schemes. On the other hand, reverse engineering, due to time and cost constraints, is not typically considered a standard solution. Indeed, typical reverse engineering involves perfectly accessing each layer of a circuit, acquiring images and processing them. It requires skills, expertise, expensive equipment, high precision and time [2]. Reverse engineering is utilized for circuit integrity verification or IP infringement detection and can be performed by analytical laboratories. X-ray-based reverse engineering (non-destructive) is widely under investigation but currently requires highly sophisticated equipment and has only been applied to a very small subset (some μm^3) of an IC [3, 4]. While some interesting FIB/SEM techniques [5] have so far been applied to parts of a circuit, they are quite demanding in terms of knowledge, time and equipment, as illustrated in Table 1. There are also ongoing multi-electron beam source and X-ray detector investigations to allow local X-ray analysis without synchrotron [6].

To counteract the difficulty of the standard reverse engineering process, we propose to retrieve sensitive information of a component (e.g. registers location and hardware accelerator) by only analyzing where the transistors' drain/source are located. Having such information is enough to reduce the area of interest for a subsequent localized attack (e.g. electromagnetic or laser attack); check the authenticity of the circuit (e.g. hardware trojan detection); or understand the underlying hardware layer after a side-channel technique such as photon-emission analysis.

Our goal is not to reverse engineer a complete chip but instead to gain partial design information for particular purposes. They lie in the area of malicious circuit modification detection but also in combined attacks where such technique

✉ Franck Courbon
franck.courbon@cl.cam.ac.uk

[1] Department of Computer Science and Technology,
University of Cambridge, William Gates building,
15 JJ Thomson Avenue, CB30FD, Cambridge, UK

Table 1 Hardware reverse engineering techniques comparison

RE technique	Cost/time/exp.	Applied on
Standard [1]	++	Full volume possible
FIB/SEM [5]	+ + +	Hundreds μm^3
X-ray [4]	+ + ++	Few dozens μm^3
Drain/source	–	Full single-layer surface

would decrease the number of samples and attack time needed. Thus, a complete attack could be applied thanks to some extracted spatial information combined with standard side-channel (e.g. power) extracted temporal information. Also, extracted spatial information can be analyzed once chip sub-functions have been roughly localized with a more global technique.

Most of the drawbacks of hardware reverse engineering disappear (cost, time, manual corrective action), and we retrieve the standard cells function or a specific group of standard cells by location (absolute and cell-to-cell), occurrences number, and width/shape analysis, which we refer to as standard cell statistical analysis (SCSA). The methodology herein is depicted from sample acquisition to a few recognition examples.

Utilizing such an approach, locating specific cells can be done regardless of the device technology node and package. For instance, it can reduce attack rating for the identification and exploitation phase and can be used in conjunction with laser fault attacks [8] to bypass security mechanisms [7]. Multi-spot (bypass/fault capability) and high-power (through the substrate capability) platforms are commercially available, increasing security threat (redundancy and software check can be defeated). While technology node approaches 7 nm, the size of the implemented transistor/single standard cell is larger, and laser energy (pulse duration/power) can be reduced enough to only perturb a single standard cell below the peak of the Gaussian shape beam.

In the past, Nohl [9] reversed a ciphering circuit made of 400 NAND gate equivalent (GE) from optical images using normalized cross-correlation. Also, Courbon [10] retrieved the location of a single type of standard cell (a flip-flop cell) on a 0.5-mm^2 area device manufactured in a 130-nm process. To the best of our knowledge, we are the first to develop, and explain step by step, a low-cost full area (single layer) standard cells extraction methodology on a 45-nm device (Mgates), while analyzing IC design requirements, methodology limits and countermeasures. The aforementioned methodology takes its sample preparation roots in the failure analysis world, its image processing roots in the cell (biology) analysis world.

The paper is organized as follows: we start by talking about IC design and geometries, before introducing the multi-field steps to localize standard cells in Section 2. Then, we introduce the device under investigation in Section 3, and put into practice the methodology in Section 4. Finally, we investigate partial reverse engineering applications in Section 5 and present ways on how to extend this work in Section 6.

2 From Integrated Circuit Design to Standard Cell Physical Extraction

2.1 IC Design

An IC designer uses a certain number of off-the-shelf macros (IP royalty fees apply) combined with a certain number of standard cells (from a chosen process design kit (PDK)), a ratio that primarily depends on project cost and design (i.e. timing) constraints. For instance, ARM cores hard macros are widely present at the moment in embedded devices, such as mobile phones and smart cards. There are similarities between products, as standard cells and hard macros are re-used across a large variety of devices. Herein, we analyze standard cells and hard macros XY localizations. In the era of specialization (i.e. dedicated ASIC for machine learning/server) and open-source hardware (based on RISC V instruction set architecture (ISA)), investigating hardware implementation is paramount.

2.2 IC Geometries

Integrated circuit area (length and width expressed in mm) is wider compared to the thickness of each metal layer (few hundreds nm), hence the planarity problem when delayering. Adding to the high density of transistors per mm^2, this leads to long imaging time. The smallest feature (for not advanced process) is generally the transistor gate width, corresponding to the technology node. A transistor controls how much current flows through from source to drain, depending on the voltage applied on the gate. Such capability is used to obtain various Boolean functions (or to create a current amplifier). Drain and source are created by local doping (boron, phosphorus) of the semiconductor substrate which is silicon based. From bottom to top, following the substrate, we find poly-silicon that forms the transistors' gates (separated by a dielectric Si02 down to 32 nm, then replaced by Hafnium-based (higher permittivity) dielectric). Typically, a first metal layer is then used to interconnect transistors, thus forming standard cells (NAND, OR, FLIP-FLOP). Then, non-basic functions, such as a 32-bit counter, are formed by interconnecting multiple standard cells together, while power/clock are routed in top metal layers. Metal layers are separated by a dielectric

(SiO2 (glass)), and vias allow vertical connections between the subsequent layers.

2.3 Sample Preparation

ICs running secure applications come in various formats—smart card, system-on-chip (SoC), package-on-package (PoP) (the die thickness being 130 μm for smart cards and PoPs due to fitting requirements). However, we reckon that it is possible to extract the die of any circuit at almost no cost: a combination of sharp cutting tools, acids (i.e. HNO_3), hot plates and protection equipments [11]. Once the die is extracted, it is possible to easily reach the transistors' active region using HF acid. This has very interesting features in terms of cost, full area application, speed and required skills, while the technique allows several samples to be prepared at once. There is no need of cross-sectioning, and the technique is independent of the technology node. In this paper, we show how easily one can reach such layer of a circuit, manufactured with a 45-nm process and packaged in a flip-chip ball grid array (FCBGA).

2.4 Sample Imaging

Scanning electron microscopy (SEM) is a standard for imaging deep sub-micron integrated circuits as optical microscopy has a smaller depth of focus and is limited by light diffraction (coating techniques can limit the impact of the latter but requires an extra step and thus variable). Detector type, aperture size, probe current, accelerating voltage, magnification, scanning speed and image resolution can be easily tuned. Despite being less prompt to contrast changes compared to optical microscopy, it is worth ensuring that the prepared integrated circuit remains as flat as possible after attaching it with carbon tape, given the large area to be acquired. The SEM only gives a grayscale intensity for each pixel (a certain secondary or backscattered electrons detector count), and the image is thus saved in a single-channel format (saving memory space). There are many parameters to set (mainly accelerating voltage, probe current and time per pixel), impacting acquisition time and signal-to-noise ratio. Here, we particularly point out practical features and considerations, pros and cons of SEM imaging with respect to our application.

2.5 Images Alignment

Newer SEMs include proprietary tools (e.g. ZEISS ATLAS, FEI MAPS) dedicated to large-area acquisition; it is thus easy to scan a specified area with a specific magnification, image rotation, time per pixel (dwell) and image overlap and then have the tool performing the alignment task. Another option (if a SEM without large-area acquisition dedicated software is used) is to directly use SEM APIs to write an acquisition recipe and use offline tools for alignment. Herein, we demonstrate the use of an offline artefact-free alignment tool.

2.6 Pattern Recognition

There has been an attempt to automate or semi-automate integrated circuit reverse engineering in the open-source community, Degate [12]. This software is quite interesting as the user can load images and directly process them. However, we found some limitations in terms of pattern recognition rate, timing performance, adjusting grid lines or loading large images. While we also implement a normalized cross-correlation function [13] as a kernel to recognize patterns, we specifically create a lighter custom tool dedicated to single-layer analysis, fast and robust with respect to possible SEM images (sample preparation and foundry). We propose an algorithm taking into account the possible artefacts arising from previous methodology steps. A single missing pattern could ruin our statistics, and therefore we ensure that no false recognition is obtained with standard pattern recognition algorithms. We are thus able to automatically collect labelled data (error-free) and create a standard cell (single layer) library. This library can be used as it is or be the starting point for multi-sample analysis using machine learning techniques to speed up analysis.

2.7 Statistical Analysis

At the layer of interest, various repetitive shapes are visualized. They correspond to basic functions such as INV, AND, OR, MUX, DEC, half adder, DFF and latch. Having only drain and source remaining on our images, we cannot directly retrieve the function of a standard cell (as poly and M1 layers are missing). Whatever the device type, the number of these base functions is very low (few tens only). Additionally, base functions are split [14] into different instances as the number of inputs, the presence of signal such as reset/clock, the drive strength and different voltage domains (for a SoC) differ. Those instances are each optimally designed depending on speed, power, area requirements and foundry capabilities. The chip designer uses such instances from the design kit to implement all his/her functions (or directly use other IPs), resulting in a chip with about 200kGE (gate equivalent) for a smart card digital logic, versus a SoC with several tens/hundreds millions standard cell occurrences for the logic only. In this paper, the goal is to give a first approach on recognizing cells based on absolute/relative location, number of occurrences, width and shape of pattern within a single chip and between chips.

3 Device Under Investigation

The circuit used for demonstration in this paper is a 9.3×10.4 mm SoC manufactured in a 45-nm technology node and packaged in a FCBGA, the standard for reducing size and increasing speed of a device compared to wire bonding. Within this case study, the main part of interest, the digital logic, is expected to include several millions of standard cells. For information, the typical layer stack (starting from bottom to top) of such devices is the following:

- Silicon substrate (650–850 μm)
- Doped areas (transistors' drain and source)
- Poly-Silicon (transistors' gate)
- Stack of 7+ metal layers and dielectrics (ascending about 0.2 to 0.9 μm)
- Passivation: $Si_3N_4/SiO_2/Si_3N_4$ (0.6/0.1/0.6 μm)
- Polyimide (5 μm)
- Die bumps
- PCB substrate
- Copper balls

4 Step by Step Practical Implementation

4.1 Frontside Sample Preparation

Under a fume cupboard, we first heat up the complete device on a 400 °C (command) hot plate for a few minutes. Placing a sharp knife under the die, we subsequently detach the die from its package. At this stage, the die comes with Copper balls—we use the same sharp knife to scratch the surface to remove all of them. We perform this until we reach the polyimide layer (Kapton). Due to the hardness of the Kapton material, we do not scratch inferior layers. We can perform some SEM imaging at this stage to visualize the top metal layer (Fig. 1).

If this layer is satisfactory for your reverse engineering application (chip identification, integrity verification), a quick manual polishing (not done in either Fig. 1 images) removes copper residues, while backscattered electrons SEM imaging prevents the visualization of surface scratches (SEM image in Fig. 1).

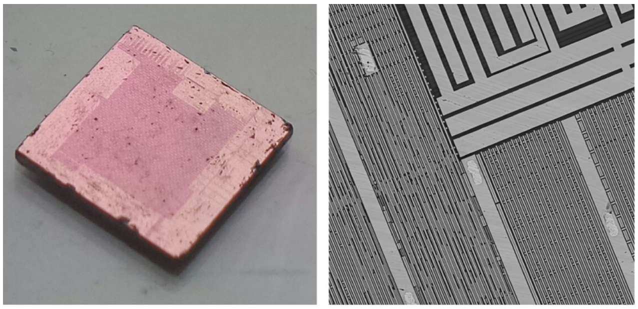

Fig. 1 At polyimide layer optical and SEM image at × 600

The Kapton film (polyimide) is now the top layer; it is detached, and dielectric/metal layers are etched away using a 50% hydrofluoric acid (HF) bath (less than 10 min). After the metal layers have been removed, only drain and source implants remain. Samples are first rinsed with acetone, before an ultrasonic bath with deionized water only is used. This perfectly cleans the die surface in less than 10 min. Last but not least, a nitrogen gun is used to avoid any water residues. The sample is, at this stage, ready for imaging. One can note the possibility to obtain the technology node (from 45 nm) with a high magnification SEM image, Fig. 2.

To sum up the whole sample preparation process, its main benefits are its speed (less than 40 min), cost per sample (few $), whole sample surface application (about 100 mm^2), technology node independence (45-65-90-130 nm in this paper), effectiveness (100% success rate) and accessibility (no required skills).

4.2 Frontside Image Acquisition

Regarding the sub-polyimide surface, imaging layer ICs' features are quite large at the top metal layers. However, using an optical microscope requires a nicely polished surface. Also, the lack of imaging depth of field is problematic for large areas. In fact, SEM remains the most interesting tool for direct imaging (without required signal processing), and this layer needs far less scans due to the top layer geometries. Unless a shield is present, the top metal layer can thus be directly imaged.

In this work, we perform SEM image acquisition at the source/drain layer. We choose a horizontal field width (200 μm) for this sample covering the standard cell fixed height (across the device) by 29 pixels. This choice gives enough pixels to then correctly characterize an inverter (the standard cell with the smallest width). The accelerating voltage is set low to improve image resolution (5keV). The scanning speed choice is based on a signal-to-noise ratio (SNR) trade-off. This trade-off depends on the subsequent image processing capabilities. We use a standard 3072×2048 image resolution and a 1-μs dwell time (time per pixel) without multiple image integration. Our overnight

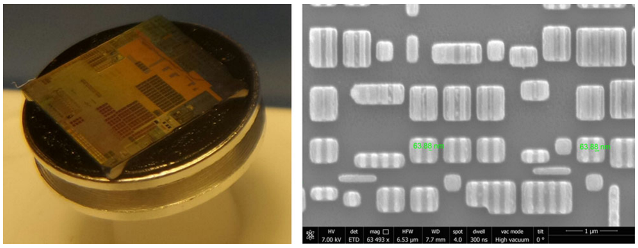

Fig. 2 At drain/source layer: optical and SEM image at × 63k

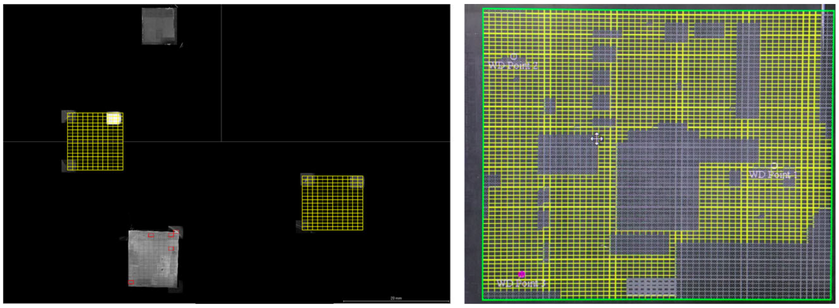

Fig. 3 Left, Multi-chip acquisition; right, logic area select

scan is a 87×52 image matrix (about 4,500 images), requiring 8.5h of automatic acquisition. With our practical approach, we noted the following observation:

- Astigmatism can be set at the centre of the device.
- Three focus points (for interpolation) can be taken at three chip sides.
- Contrast/luminosity is a tricky parameter, different secondary electrons re-emission rates (no coating, not uniform in SEM chamber) can be problematic.

Multi-chip acquisition is possible (weekend acqusition for instance), including the possibility to set a focus point for each integrated circuit. The only drawback is the impossibility to set a certain contrast/brightness per chip (against SEM chamber artefact/samples different electron emission rates), Fig. 3.

Also, using a multi-beam SEM (up to 91 simultaneous beams) would have decreased the acquisition time to less than 10 min. We used a proprietary SEM manufacturer software (additional) to acquire the full area that added a 10% overlay between each image. It individually saves images, but also provides a globally aligned image.

4.3 Image Alignment

The proprietary SEM tool provides a reconstructed whole chip image (142k×159k pixels). Artefacts are present at the images' junctions (example given with top image on Fig. 4), which negatively impact the subsequent methodology step (pattern recognition).

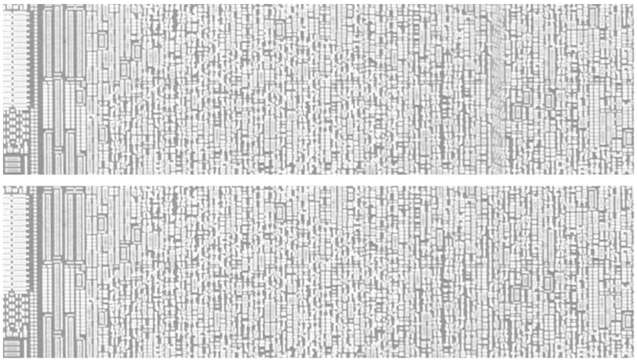

Fig. 4 Alignment example: SEM manufacturer tool (top) and offline non-proprietary technique (bottom)

As images are also individually saved, we thus move to an offline alternative for alignment. The same set of images has been aligned with this second approach (example image with bottom image on Fig. 4). We are able to align all images together, making compatible large image acquisition and pattern recognition. It only takes several minutes and is completely automated (matrix dimension detection, overlap calculation). Image alignment is still an area of research (mainly for speed concerns) but 2D image alignment problematics have been resolved time ago in other fields such as biology where electron microscopy is also used or standard optical acquisition.

4.4 Image Processing

4.4.1 Standard Cell Statistical Analysis Flow

Pattern recognition is then performed on obtained images. The former is specifically tuned for our task. After automatically checking for preparation/imaging artefacts, patterns are found on the chip along power lines and ranked per size. Standard correlation techniques with multiple iterations loops (with decreasing correlation coefficient) are used to avoid false detection. Information about pattern location, size and occurrences are saved. Then, co-location information combined with computer architecture and technology/tool-specific constraints allow making hypothesis on the retrieved standard cells. The main aim is to ensure that no false positives are obtained with the tool allowing on one side to have non-false positive for statistical purposes but also to obtain a dictionary of error-free patterns.

4.4.2 Enhanced Pattern Recognition Robustness via Artefacts Correction

It is important to understand what could go wrong in the previous preparation steps, in order to adapt the pattern recognition tool accordingly:

- If any tungsten remains on the surface, it will be adjacent to a NMOS/PMOS area, and therefore only affects the background of the image. Such artefact can thus be easily spotted (based on edge detection).

- Large stains can be present on a circuit (non-cleanroom environment) but can be detected as nothing should be located over the substrate polarization contact (or, in other words, no crossing element between two transistors of the same type).
- Part of a shape can be missing (over etching, as seen in Fig. 5); therefore, the tool checks the presence of NMOS and PMOS components (we cannot have one without the other). If missing, an analysis of the specified area is performed and some filtering enables the retrieval of the original missing shape (as would still let a trace in the silicon).

4.4.3 Enhanced Statistical Analysis via Design Rule

The following features, derivated from computer architecture standards, need to be taken into account to ensure pattern recognition efficiency and reduce timing impact:

- A small pattern can be part of a larger pattern. One approach is to recognize larger patterns first.
- Patterns are present along power rails; therefore, possible rotations of the pattern are limited. For instance, the PMOS side (usually larger than NMOS) will be located on the positive rail side. Also, the highest correlation points will only be located at the same extremity of the patterns.
- The size of the complete layer has quite a large print, e.g. for this 10 × 10 mm die results in a 22.7-GB image (even if grayscale encoded only on 8bits (1byte)). We need a clever manipulation of the image (RAM constraint).
- The logic only can be acquired (or another part can be acquired with less resolution; SEMs do not provide this function yet).
- While substrate polarization contacts may not be present in all circuits, background can always be retrieved by analyzing intensity values across the pattern height. For instance, a pattern is found at a location if the intensity (gradient) is not continuous (a change of intensity is found between NMOS drain/source and Si and then between Si and PMOS drain/source).

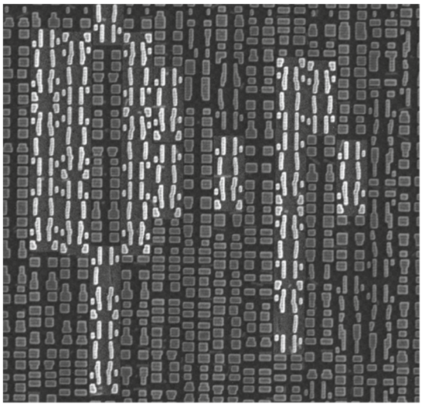

Fig. 5 A close-up on a pattern recognition example

Figure 5 shows a typical case where a standard cell with a different current drive strength (fan-out) (compared to the selected standard cell) has not been recognized. There are also two standard cells with a partly missing transistor side that are recognized. We expect this behaviour with the aforementioned parameters. We want to be independent of possible within-cells imaging fluctuations or missing substrate polarization contacts.

Combining the number of occurrences (local or full area) of a pattern, their global position, their relative position to each other and their shape, it is possible to classify patterns and make a strong hypothesis on their function. Typically, assumptions can be first made on the pattern width—patterns 1 and 3 are made of 4 to 8 transistors while pattern 2 is made of 20+ transistors. The main difficulties are to recognize the full standard cell and not a subset of it, and slight differences between gates due to the presence of an extra input (e.g. reset/clock/signal) or a different fan-out (larger current to drive) as highlighted on Fig. 6.

4.5 Single-Chip Information Extraction

In this section, we applied the methodology flow on a subset of the fully scanned IC. The image is 11840 × 7536 pixels that corresponds to 0.40% (1/250) of the IC (analog + digital + memory parts). The original SEM image is fully covered with standard cells (and memory blocs). From each initial pattern size and appearances, we can derive the hypothetic number of transistors and the number of inputs/outputs. Using standard image processing, each pattern is associated with a certain number of occurrences, Fig. 7 and co-location information regarding other pattern. The second image output highlights the presence of a given FF/latch design occurrence in a restricted location. Globally, one can make hypotheses on a shape's function based on:

- The area analysis (e.g. a flip-flop is usually the largest element)
- The number of transistors (e.g. a NAND cell has 4 transistors)
- Localization (e.g. a group of gates next to the memory could be used for deciphering)
- Co-localization (e.g. two groups of cells often linked)
- Occurrences (e.g. 32 spatially close occurrences for a specific 32-bit register or counter (analyzing the shape too), or 64 spatially close occurrences for a XOR-based ciphering circuit)
- Global number of occurrences in the chip

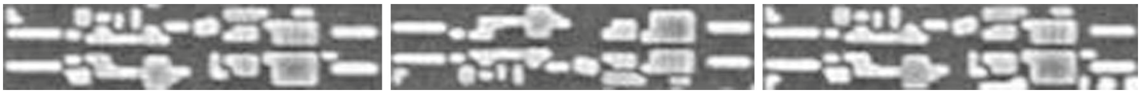

Fig. 6 Differences over similar 20+ transistors standard cells

Subsequently, an area with possible XOR gates, large quantities of possible NAND gates and possible DFF gates may be the hint for a crypto coprocessor location (e.g. DES). The presence of 'rare' occurrences standard cell in a limited area may indicate the presence of a crypto coprocessor too. Post pattern recognition, it is possible to display occurrences of pattern that appear everywhere before moving to an empty area to vizualize recognized pattern.

For some circuits such as the processor under investigation, motherboard manufacturers require information on the processor; a datasheet is thus made public. Using the latter, one can thus assume a certain number of 8-/16-/32-bit registers or a certain function being in a certain area (based on registers description and ballout definition respectively) or a certain number of expected core registers or specific function registers (each FF will be next to the other, timing constraint) present in a certain voltage domain (possible thick pwell). For some circuits, it is a complete black box approach despite knowing the general architecture of the device (e.g. ARM based) or accessing public documents (e.g. public parts of certification results). Unfortunately, the complexity of the circuit does not permit to continue further statistics on the chip.

In the following, we discuss how practical it is to use standard cell statistical analysis outputs (text, file or graph format) for the two main aspects of this paper: precise laser fault attacks and hardware trojan detection.

5 Single-Cell Localization Direct Applications

5.1 Spatial Information for Laser Setup

Despite the main sample of the study being a 45-nm technology node SoC, we note that a single standard cell (several μm^2) can be perturbed at once. Indeed, the laser beam has a Gaussian shape, a spot diameter of a μm and an easily controllable energy (duration by power) reaching the area of interest [16]. This single-layer reverse engineering will help to place the laser spot at the area we are interested in. Symmetrically, we can first launch a laser fault attack to then analyze the situation using the underlying hardware structure. However, if a secure device is attacked this way, detectors might detect the intrusion leading to extra consideration to be taken for the attack (e.g. remove power before sensitive data erase). One can also think about the potential of such an approach together with photon counting techniques (specifically without timing capabilities, e.g. only a CCD camera is used).

5.2 Spatial Information for Integrity Checking

Another use case is a fabless chip designer/manufacturer (or anyone with a design reference) that would like to analyze the integrity of its components at wafer reception. The success rate of such technique is only dependant on the

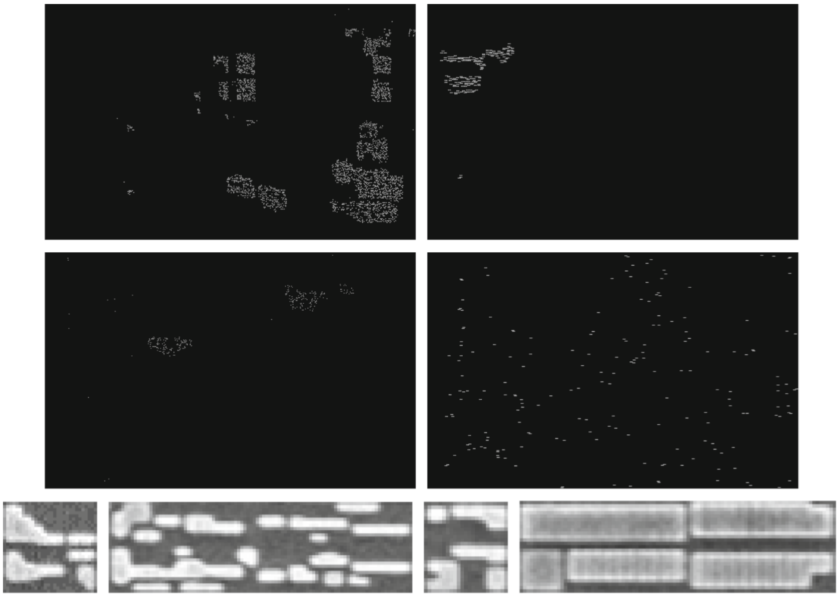

Fig. 7 Single round recognition of respective pattern (top left to bottom right)

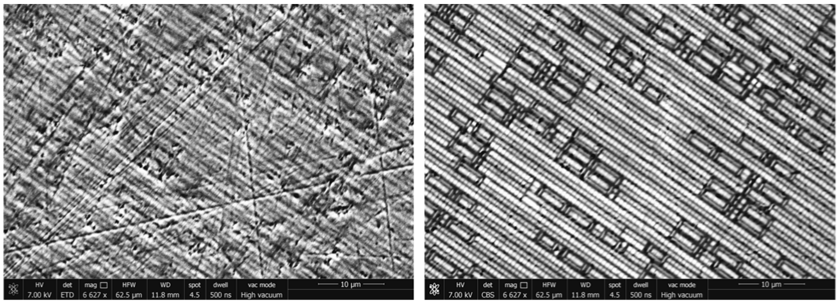
HV 7.00 kV det ETD mag 6 627 x HFW 62.5 µm WD 11.8 mm spot 4.5 dwell 500 ns vac mode High vacuum 10 µm
HV 7.00 kV det CBS mag 6 627 x HFW 62.5 µm WD 11.8 mm spot 4.5 dwell 500 ns vac mode High vacuum 10 µm

Fig. 8 Backside imaging of a 45-nm SoC active region through a thin remaining Si layer using secondary (left) and backscattered detectors (right)

sample preparation/pattern recognition process as there is no triggering element. The standard cell statistical analysis can be applied on a defective device coming from a lot (or a defective die taken from a wafer) to no affect cost and yield. The correlation is made by comparing the list of standard cells physically extracted using our methodology and a design output file. Specifically, this could be done with the Design Exchange Format (DEF) file, where each gate instance is listed with its XY position. A DEF file does not include proprietary inner standard cell information, hypothetically more compliant.

5.3 Extending Scanning Electron Microscopy Use

To complete investigations done at FPGA level [17], it is thus interesting today to look for low-cost approaches enabling to retrieve such layers over the complete area of a circuit. It can start with a frontside wet etching adaptation (change in HF formula for instance) to a backside information extraction with combined polishing/wet etching methods. Various imaging parameters (laser/ebeam) can actually be set to obtain an interesting beam/matter interaction. In Fig. 8, we show in practice that it is possible to look through a thinned Si substrate using backscattered electrons.

In Fig 9, we show in practice the capability to visualize various layers of a component backside prepared. The preparation is a mix of polishing (standard polishing) and wet etching (choline hydroxide) resulting in a fast and low technique. Long wet etching is also a possibility if edges are kept intact (protection needed). The sample preparation can also be modified to reveal dopant level or type (e.g. KOH).

Part of our approach and obtained data can be used as a starting point for machine learning–based (convolutional neural networks) fast pattern recognition, as our data is labelled with no false positives. In this paper, we choose a frontside destructive approach. It would be obviously more interesting to perform standard cell analysis from the backside of the device in a non-invasive way. Laser scanning microscopy has been used in the past and would be an interesting method to compare with (thinning required, setup, cells distinction (fan-out)).

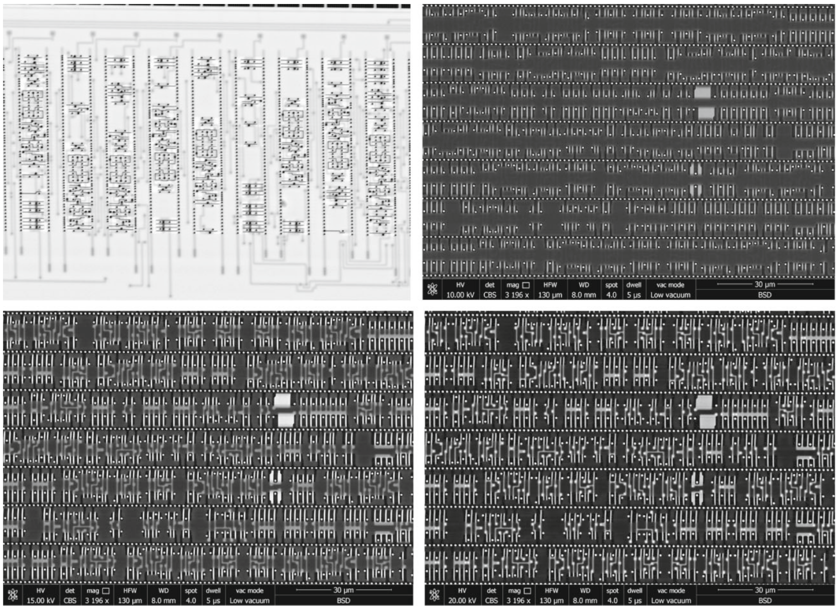
HV 10.00 kV det CBS mag 3 196 x HFW 130 µm WD 8.0 mm spot 4.0 dwell 5 µs vac mode Low vacuum BSD 30 µm
HV 15.00 kV det CBS mag 3 196 x HFW 130 µm WD 8.0 mm spot 4.0 dwell 5 µs vac mode Low vacuum BSD 30 µm
HV 20.00 kV det CBS mag 3 196 x HFW 130 µm WD 8.0 mm spot 4.0 dwell 5 µs vac mode Low vacuum BSD 30 µm

Fig. 9 0.35-μm circuit imaging using a backscattered electrons (BSE) detector

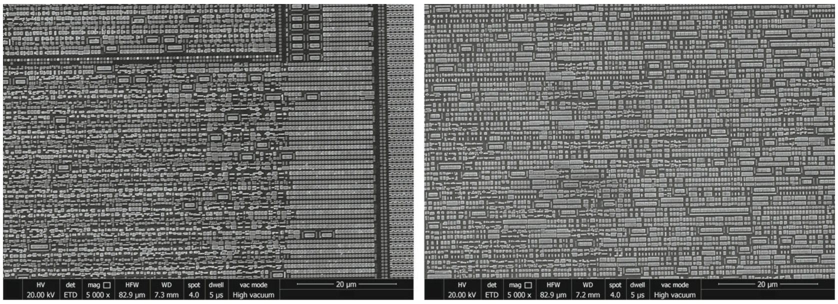
HV det mag □ HFW WD spot dwell vac mode 20 µm
20.00 kV ETD 5 000 x 82.9 µm 7.3 mm 4.0 5 µs High vacuum
HV det mag □ HFW WD spot dwell vac mode 20 µm
20.00 kV ETD 5 000 x 82.9 µm 7.2 mm 4.0 5 µs High vacuum

Fig. 10 Two different generations of a similar 65-nm SoC at active

6 Perspectives and Opening

6.1 Chip to Chip Analysis, Different Process Analysis

So far, we depict the different steps for standard cell statistical analysis with few examples on a 45-nm chip. The low cost and quick data extraction enable to perform reverse engineering at a different scale than previously seen in the literature. The idea is to compare multi-chip analysis to extract design information from new function implementation to countermeasure analysis. The best approach would be to begin with smaller and better known integrated circuit (less standard cells, more design information available, single core, single voltage, physically accessible chip on board). Figure 10 displays 65-nm devices, anterior version of the main product (45nm) used in this article. The general idea is to be able to retrieve direct information from an already analyzed integrated circuit.

6.2 Machine Learning Framework

Machine learning is ideally used for prediction and requires some training data. It particularly makes sense to use it for domain where time is the main criteria (speech recognition). The first concern is to be able to reach the same level of detection while drastically reducing the recognition processing time. Retrieved shapes with standard correlation technique are used as an error-free dictionary to build up the machine learning model. It would be interesting to evaluate such framework in terms of error rate but also for denoising microscopy images. The latter could resolve low-resolution images and further reduce methodology time (scanning). It would be interesting to propose and share a SEM image benchmark or an online tool where test images can be loaded and analyzed according to a specifically trained model.

6.3 Countermeasures

The partial reverse engineering main interest is its possible application on multiple circuits giving thus more data to be compared with even in a black box approach to assess countermeasures/extract design information. When designing a circuit for secure applications, countermeasures against reverse engineering first appeared in the set of required features, and so before fault attack countermeasures. Actually, it exists proprietary countermeasures at active/poly/via/metal1 layers to hide functionality of a component from non through vias to dummy cells and programmable logic using local oxide breakdown [18] and used by pay-TV, telecommuncations and smart card industries [19]. Most countermeasure techniques are based on principles such as logic-locking [20] and netlist/physical obfuscation (doping, dummy via/cell, oxide breakdown, electric charge) [21].

The idea behind our technique is to analyze how standard cells distribution participate to design information extraction (and for authenticity verification too). In future work, it will be interesting to characterize IC camouflaging protection with our tool for multiple reasons. IC camouflaging is typically not applied on the entire die. Also, it would be interesting to combine in practice aforementioned statistics and local attacks. Common Criteria (CC) attack classification would be affected if less samples, expertise and time are required.

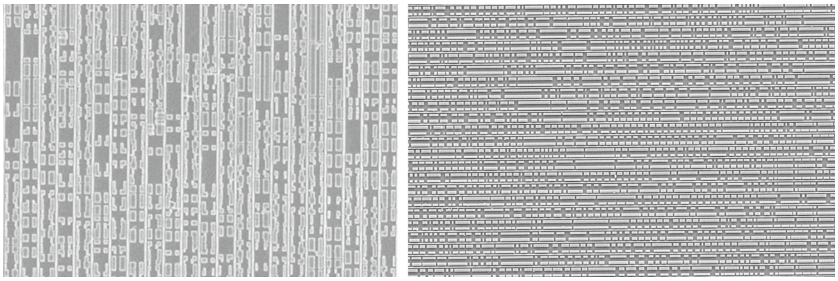

Fig. 11 Similar product (90nm, 130nm) from two different IC manufacturers

Last but not least, after applying our methodology on different components, we actually found a single sample (90nm, smart card industry) that is quite different, having regular patterns (Fig. 11). We found out that this device is metal-only programmable [22]. This would be a countermeasure by design to drain/source-based reverse engineering; it would, however, be interesting to characterize design capability (low power, high gate density) and robustness against other types of attacks (e.g. side channel).

7 Conclusion

An alternative to high-cost reverse engineering is presented and applied on a commercial 45-nm SoC. This is a first step towards automatic partial design information extraction. The methodology includes any package die extraction, drain/source layer access and SEM imaging, pattern recognition and a new approach called standard cells statistical analysis (SCSA). We particularly characterize each step of the methodology and point out the low cost and time resources needed to start partial reverse engineering investigations. Single-layer reverse engineering mainly addresses combined attacks (such as EM observation/perturbation and laser fault attacks) and malicious hardware modification detection problematics.

Acknowledgments Dr Franck Courbon is an Early Career Fellow jointly funded by The Isaac Newton Trust and The Leverhulme Trust under the agreement ECF-2017-606.

References

1. Randy T, Dick J (2009) The state-of-the-art in IC reverse engineering. CHES
2. Advanced IC reverse engineering techniques: in depth analysis of a modern smart card, Blackhat 2015
3. Harrod B (2016) Rapid analysis of various emerging nanoelectronics (RAVEN)
4. Holler M, Guizar-Sicairos M, Tsai EHR, Dinapoli R, Müller E, Bunk O, Raabe J, Aeppli G (2017) High-resolution non-destructive three-dimensional imaging of integrated circuits. Nature 543:402–406
5. Principe EL, Asadizanjani N, Forte D, Tehranipoor M, Chivas R, DiBattista M, Silverman S, Marsh M, Piche N, Mastovich J (2017) Steps toward automated deprocessing of integrated circuits. ISTFA
6. Nanoscale X-ray tomosynthesis for rapid assessment of IC dice, Richard Lanza AIDA-2020 meeting, 2018
7. Vasselle A., Thiebeauld H., Maouhoub Q, Morisset A, Ermeneux S (2017) Laser-induced fault injection on smartphone bypassing the secure boot FDTC
8. Champeix C, Borrel N, Dutertre JM, Robisson B, Lisart M, Sarafianos A SEU sensitivity and modeling using picosecond pulsed laser stimulation of a D Flip-Flop in 40 nm CMOS technology. In: 2015 IEEE international symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFTS)
9. Nohl K, Evans D, Starbug S, Plötz H (2008) Reverse-engineering a cryptographic RFID tag. Usenix
10. Courbon F, Loubet-Moundi P, Fournier JJA, Tria A (2014) Increasing the efficiency of laser fault injections using fast gate level reverse engineering. International Symposium on Hardware-Oriented Security and Trust, HOST
11. Beck F (1998) Integrated circuit failure analysis: a guide to preparation techniques
12. Schobert M (2009) http://www.degate.org/
13. Lewis JP (1995) Fast normalized cross-correlation
14. Faraday Technology Corporation, 90 nm Logic SP-RVT (Low-K) Process
15. Hatami N, Gavet Y, Debayle J (2017) Classification of time-series images using deep convolutional neural networks
16. Courbon F, Loubet-Moundi P, Fournier J, Tria A (2014) Adjusting laser injections for fully controlled faults
17. Rajendran J, Sam M, Karri R (2013) Security analysis of integrated circuit camouflaging, CCS
18. Cocchi R Camouflage circuitry and programmable cells to secure semiconductor designs during manufacturing. In: 2015 National Aerospace and Electronics Conference (NAECON)
19. Inside Secure accelerates strategy in Silicon IP business with SypherMedia acquisition, 7th November 2017
20. Yasin M, Sinanoglu O (2017) Evolution of logic locking, VLSI-SoC
21. Chakraborty RS, Bhunia S HARPOON: an obfuscation-based SoC design methodology for hardware protection
22. https://www.baysand.com/technology/mcsc-foundation-technology

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.