In-house transistors’ layer reverse engineering characterization of a 45nm SoC

Dr. Franck Courbon
Department of Computer Science and Technology, University of Cambridge, UK
franck.courbon@cl.cam.ac.uk

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, similar standard cell recognition, as well as within and between die Standard Cell Statistical Analysis (SCSA). We develop the process to access the transistor’s drain/source area; image the full surface; develop a robust pattern recognition tool and analyze the standard cell size, local / global location and occurrences number. We present the inner workings of each step and results on 45–65nm FCBGA devices enabling to locate specific areas (core registers, hardware accelerator, and so on) within a die, and find similarities between dies. 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 integrated circuit design information can be retrieved with minimal costs and without outsourcing.

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. 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 µm³) of an IC [2], [3]. While some interesting FIB/SEM techniques [4] 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 I.

<table>
<thead>
<tr>
<th>Reverse Engineering</th>
<th>Output</th>
<th>Cost</th>
<th>Time</th>
<th>Operator</th>
<th>Dead sample</th>
<th>Applied on</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard [1]</td>
<td>Complete RE</td>
<td>High</td>
<td>Weeks</td>
<td>Expert</td>
<td>1+</td>
<td>Full volume possible</td>
<td>130nm</td>
</tr>
<tr>
<td>FIB/SEM destructive [4]</td>
<td>Complete RE</td>
<td>Very high</td>
<td>Weeks</td>
<td>Expert</td>
<td>1+</td>
<td>Hundred s µm³</td>
<td>65nm, 0.35µm</td>
</tr>
<tr>
<td>Xray, Synchrotron source [3]</td>
<td>Complete RE</td>
<td>Very high</td>
<td>Weeks</td>
<td>Expert</td>
<td>0</td>
<td>Few dozens µm³</td>
<td>32nm</td>
</tr>
<tr>
<td>Xray, ebeam(s) source [2]</td>
<td>Complete RE</td>
<td>Very high</td>
<td>Weeks</td>
<td>Expert</td>
<td>0</td>
<td>Few dozens µm³</td>
<td>NA</td>
</tr>
<tr>
<td>Drain/source SEM (this paper)</td>
<td>Partial RE</td>
<td>Very low</td>
<td>Hours</td>
<td>Anyone</td>
<td>1</td>
<td>Full single layer surface</td>
<td>45nm</td>
</tr>
</tbody>
</table>

Table I: Hardware reverse engineering techniques.

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 few side-channel techniques such as photon-emission analysis.

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 to bypass security mechanisms [5]. Multiphoton (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 7nm, 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 [6] reversed a ciphering circuit made of 400 NAND Gate Equivalent (GE) from optical images using normalized cross correlation. Also, Courbon [7] retrieved the location of a single type of standard cell (a flip-flop cell) on a 0.5mm² area device manufactured in a 130nm 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 45nm device (Mgates), while exploiting IC design requirements and investigating methodology limits and countermeasures.

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 I. Then, we introduce the device under investigation in Section II, and put into practice the methodology in Section III. Finally, we investigate partial reverse engineering applications in Section IV, present ways on how to extend this work in Section V, and analyze countermeasures in Section VI.

I. From integrated circuit design to standard cell physical extraction

IC design
An IC designer uses a certain number of off-the-shelf hard 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 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.

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 mm², 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 SiO₂ down to 32nm, 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.

Sample preparation
ICs running secure applications come in various formats – Smart Card, System-on-Chip (SoC), Package-on-Package (PoP) (the die thickness being 130µm 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., HNO₃), hot plates and protection equipment. 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 45nm process and packaged in a Flip-Chip Ball Grid Array (FCBGA).

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.

Sample 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. What is interesting is the capability to define multiple areas to acquire. It can allow the scanning of multiple ICs overnight/over the weekend, and a certain focus can be set for each of them. The only drawback is that we are not able to set a certain contrast/brightness per chip, and if the samples have different electron emission rates (that will occur if they are not coated), then images will be difficult to process. 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 and discuss the use of an offline artefact-free alignment tool.

Pattern recognition
In the past, Degate [8] was created to reverse engineer ICs. This written open source 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, and adjusting grid lines or loading large images. While we also implement a normalized cross correlation function 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.

The library can be used as it is or be the starting point for multi-samples analysis using machine learning techniques (based on Convolutional Neural Networks). This is undergoing investigation and the main concern is to be able to reach the main level of detection (while drastically reducing the recognition processing time)

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, latch, and so on. Having only drain and source remaining on our images, we can not 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 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. We place function hypothesis on cells/group of cells based on absolute/relative location, number of occurrences, width and shape of pattern within a single chip and between chips.

II. Device under investigation
The circuit used for demonstration in this paper is a 9.3*10.4mm SoC manufactured in a 45nm 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 (650-850µm)
- Doped areas (transistors’ drain and source)
- Poly-Silicon (transistors’ gate)
- Stack of 7+ Metal layers and dielectrics (ascending about 0.2 to 0.9µm)
- Passivation: Si3N4/SiO2/Si3N4 (0.6/0.1/0.6µm)
- Polyimide (5µm)
- Die bumps
- PCB substrate
- Copper balls

III. Results

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).
In this work, we characterize the SEM image acquisition at the source/drain layer. We choose a magnification (2kX) covering the standard cell fixed height by 25–30 pixels. This choice gives enough pixels to then correctly characterize an inverter (the standard cell with the smallest width). The scanning speed choice is based on a signal-to-noise ratio (SNR) trade-off. It may also be interesting to integrate multiple ultra-fast images at the same location to increase the SNR. We use a standard 3072*2048 image resolution and a 1µs dwell time (time per pixel) without multiple image integration. Our overnight scan is a 87*52 images matrix (about 4,500 images), requiring 8.5 hours of automatic acquisition. Using a multi-beam SEM (up to 91 simultaneous beams) would have decreased the acquisition to less than 10 minutes. We used an additional proprietary SEM manufacturer software to acquire the full area that added a 10% overlay between each image. It individually saves images, but also provides a globally aligned image.

**Image alignment**

However, using the proprietary SEM tool, we found artefacts during image alignment. Artefacts were present at the images' junctions (Fig. 3), which negatively impact the subsequent methodology step (pattern recognition).

As images are also individually saved, we thus move to an offline alternative for alignment. We propose to find the offset between subsequent images using a Fast Fourier Transform (FFT) based technique. The same set of images has been aligned with this second approach resulting in a perfect alignment (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 processing**

1) **Standard cell properties**: It is important to understand what could go wrong in the previous preparation steps in order to adapt our 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, but can be detected as nothing should be located over the substrate polarization contact (or, in other words, between two transistors of the same type, no crossing element). If a large conductive stain blocks a complete standard cell, one can clean the sample again or use a second identical sample and gather images.

• Part of a shape can be missing (due to the sample preparation, as seen in Figure 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.

The following features, derived 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 but also to take this into account in the statistics.

• 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*10mm it results in a 22.7GB 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 analysing 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).

2) Proposed algorithm: We tune the pattern recognition process specifically to our task. The aim of the proposed algorithm is to ensure that no false positives are obtained with the tool.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Locate digital logic</td>
</tr>
<tr>
<td>2</td>
<td>Check for preparation/imaging artifacts</td>
</tr>
<tr>
<td>3</td>
<td>Rotate final image (feature extraction technique)</td>
</tr>
<tr>
<td>4</td>
<td>Pre-process image</td>
</tr>
<tr>
<td>5</td>
<td>All patterns selection (find out background area), ranked per size</td>
</tr>
<tr>
<td>6</td>
<td>Compute correlation for each pattern - along power rails only, and for the possible gate orientation only</td>
</tr>
<tr>
<td>7</td>
<td>Save recognized patterns localization with correlation coefficient higher than a high pre-determined threshold</td>
</tr>
</tbody>
</table>

8 Remove location from area to search (speed-up)  
9 Start again with next pattern  
10 Multiple iterations reducing the correlation threshold (5%) for each pattern  
11 Allow manual input for area with a missing pattern (i.e. partly under a stain)  
12 Standard Cell Statistical Analysis (shape, occurrences number...)  
13 Automated Text and graphical file report

Table II: Standard Cell Statistical Analysis flow

Fig. 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. Two cells with a partly missing transistor side are recognized. We expect this behaviour with the aforementioned parameters. In our case, we only analyze the transistor’s drain/source shape. We want to be independent of possible within-cells imaging fluctuations or missing substrate polarization contacts.

Standard Cell Statistical Analysis (SCSA)

It is, even visually, possible to spot a lot of chip-design information using our methodology. For instance, we applied the tool on a subset of the fully scanned IC (Fig. 6). The image is 21758*2381 pixels and corresponds to 0.23% of the IC (analog + digital + memory parts). The magnification used is 3kX. The original SEM image is fully covered with standard cells. After pattern recognition, we can notice that some instances are only present in specific locations of the component, while some areas do not include any of 6 selected patterns (Fig. 6).
Combining the number of occurrences (local or full area) of a pattern, their global position, their relative position to each other, the nearby presence of a memory/test block and their shape, it is possible to classify patterns and make a strong hypothesis on their function. For instance, a single shape is only located at specific locations (Fig. 7, 11840*7536 pixels).

In future work, it will be interesting to characterise IC camouflaging protection with our tool for multiple reasons. The first being that IC camouflaging is typically not applied on the entire die. Also, it would be interesting to investigate if the aforementioned statistics would enable extracting design information or reduce the attack surface.

For some circuits such as the processor under investigation, motherboards 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 bits 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 present in a certain voltage domain.

For some others, 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).

As an example, once identical shapes are obtained all over the circuit, 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).
- Occurrences (e.g., 32 spatially close occurrences for a specific 32 bits register or counter (analyzing the shape too), or 64 spatially close occurrences for a XOR based ciphering circuit).

For some circuits such as the processor under investigation, motherboards 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 bits 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 present in a certain voltage domain.

In future work, it will be interesting to characterise IC camouflaging protection with our tool for multiple reasons. The first being that IC camouflaging is typically not applied on the entire die. Also, it would be interesting to investigate if the aforementioned statistics would enable extracting design information or reduce the attack surface.

In the following, we discuss how practical it is to use Standard Cell Statistical Analysis outputs (text or graph format) for the two main aspects of this paper: precise laser fault attacks and Hardware Trojan detection.

IV. From standard cells localization to applications

Spatial information for laser setup

The device used for chip design extraction is sacrificed for Standard Cell Statistical Analysis (SCSA) purposes. It allows localizing a specific area (various hardware accelerators, hard macros) or specific standard cells on the component (D flipflop). It is particularly interesting to combine such information with laser fault attacks on a second identical sample kept functional. Nowadays, due to the number of metal (light blocking) layers present on ICs, a backside approach through the substrate is taken. Thinning down the substrate for smart cards or PoP is not necessary as the substrate is already about 130µm thick. An IR camera (30k$) correlates the location on the second sample with the SEM image. A lower cost approach is to add a small resistor on the ground path of the device to measure its power consumption and use a constant high enough energy laser beam to find IC edges (laser scanning microscopy technique) or map with first local faults. Then, one can import the SEM image into the laser platform. Despite the main sample of the study being a 45nm technology node SoC, we note that a single standard cell (several µm²) 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 [9].

This single layer reverse engineering will help to place the laser spot at the area we are interested in [9]. 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).
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 dependent on the sample preparation/pattern recognition process. 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 not 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 the name of each gate is given with its XY position. A DEF file does not include proprietary inner standard cell information. It can therefore be easier to set such technique up. Additionally, minimal changes to sample preparation would allow detecting dopant-layer or contact-layer hardware malicious modification.

V. Perspectives and opening

Importantly, implementing the laser fault injection on specific registers found using the methodology proposed here on large SoCs can improve attacks efficiency [5]. Some other low cost sample preparation techniques could be used to access different chip layers. We particularly think about similarly obtaining poly/contact/metal1/metal2 layers. Regarding SEM, we note that having an individual contrast/brightness setup for each sample in a SEM chamber (no coating given different reemission rates) would be an interesting add-on. Also, fast acquisition (to decrease the amount of equipment renting time) images could be enhanced by signal processing techniques. Additionally, one could play with SEM parameters to extract subsurface information from multiple layers (with a backside approach) using some other signal processing techniques.

Many statistics can be drawn; for instance, between different versions of the same product, slightly different products of the same manufacturer, and versions of a product before and after the insertion of Silicon-based countermeasures (hardware obfuscation). Below are some 65nm devices, anterior to the version of the 45nm product used in this article.

The following presents a subset of a 90nm and 130nm digital logic from two other manufacturers, compared to the previous device under investigation. Those devices are coming from the smart card industry where the current state of the art technology node used is 65nm. Within the second circuit, standard cells look alike (at Si. level).

Fig. 9. Similar product (90nm, 130nm) of two different IC manufacturers.

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 cells 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)). Even if Silicon is transparent at infra-red wavelengths, IR cameras do not give fine information of each standard cell shape. A complete characterization of IR cameras imaging, resolution and autofocus capabilities depending on Si. doping level and Si. thickness followed by pattern recognition could be an interesting experiment to perform for comparison.

VI. Countermeasures

Even visually, it is possible to find a group of gates or individual gates of interest within the design without statistical analysis and large datasets. We understand that breaking cell distribution at design stage, location and occurrence-wise, can be used to avoid such statistical analysis. Such countermeasure has to be applied on non-critical path (no timing impact). Hardware redundancy (that would affect statistics but also impact a single fault attack for instance) or light sensors can be added to the circuit at a cost of area (will not protect against several laser beams attack or other local attacks respectively). Re-computation can be added in the software at the cost of time. Last but not least, after applying our methodology on different components, we actually found a single sample that is quite different, having regular patterns (See Fig. 8). We found out that this device is metal only programmable [10]. 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). Against reverse engineering (and partial) on CMOS based circuits, hardware obfuscation and logic locking are the main countermeasures (but have a cost, and may not cover the entire circuit). We are in the process of combining multiple circuit analysis (e.g., different versions with/without countermeasure) and performing different (but still low cost) sample preparation/SEM imaging to characterize hardware obfuscation at not only the drain/source level, but also at doping and Metal1/2 layers (e.g., backside preparation.
followed by successive acquisitions with variable microscopy parameters).

**Conclusion**

An alternative to high cost reverse engineering is presented and applied on a commercial 45nm SoC. The methodology includes die extraction from any package, drain/source layer SEM access and 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 for the complete process. Single layer reverse engineering addresses combined attacks and malicious hardware modification detection problematics. The technique proposed can be applied on various samples to extract standard cell information. Combined reverse engineering / fault attacks countermeasures are discussed, together with a countermeasure by its nature already implemented in the field (metal only programmable technology).

**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**


