Challenges in the Design of Integrated Systems for IoT

Ricardo Reis

Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91501-970 – Porto Alegre – RS – Brazil
reis@inf.ufrgs.br

Abstract. The Internet of Things is moving fast to be the Internet of Everything. This brings several challenges in several areas of Computing Systems, as in Embedded Systems, Computer Architectures, Fault Tolerance and Integrated Circuits and Systems. One common point is the power optimisation, as the demanding energy is increasing year by year. Optimisation must be done in all levels of design abstraction, system, computer architecture till the physical design. Another issue is reliability and fault tolerance as systems at ground level can be affected by radiations reaching the ground. Also, as several devices in IoT are related to sensitive applications, security is also an important issue in different design levels, including the physical one. The talk will present an overview of all these issues, proposing also some solutions.

Keywords: Internet-of-things, Optimization, Physical Design, Fault Tolerance, Radiation Effects, Embedded. Systems, Computer Architectures, Fault Tolerance, VLSI, Nanoelectronics

1 Introduction

In [Reis 2018] is was shown that the Internet of Things (IoT) demands new challenges in the design of computing and electronics components. One of the major challenges is the power reduction of this expanding network of connected devices, where the majority is permanently connected. In a large set of applications, another significant issue is reliability, especially on critical areas as health and transport. It was presented an overview of design strategies that we have developed to reduce power consumption and to increase reliability in circuits that are components of the IoT, as the reduction of the number of transistors in IoT devices by using

optimisation techniques and the physical design of circuits tolerant to radiation effects.

In this paper the goal is to discuss challenges in several areas of Computing Systems, as in Embedded Systems, Computer Architectures, Fault Tolerance and Integrated Circuits and Systems. Power optimization is a major issue, as the demanding energy to run all electronics devices is increasing year by year. In [REIS 2018] is was shown a figure with the number of transistors fabricated each year till 2014. Figure 1 shows a new version, including data about the number of transistors produced in 2017. It is possible to see that in 3 years, the production of transistors in the world increased by 4 times, reaching the amount of 1 sextillions of transistors. How many power plants we will need to cope with increasing level of production of transistors?

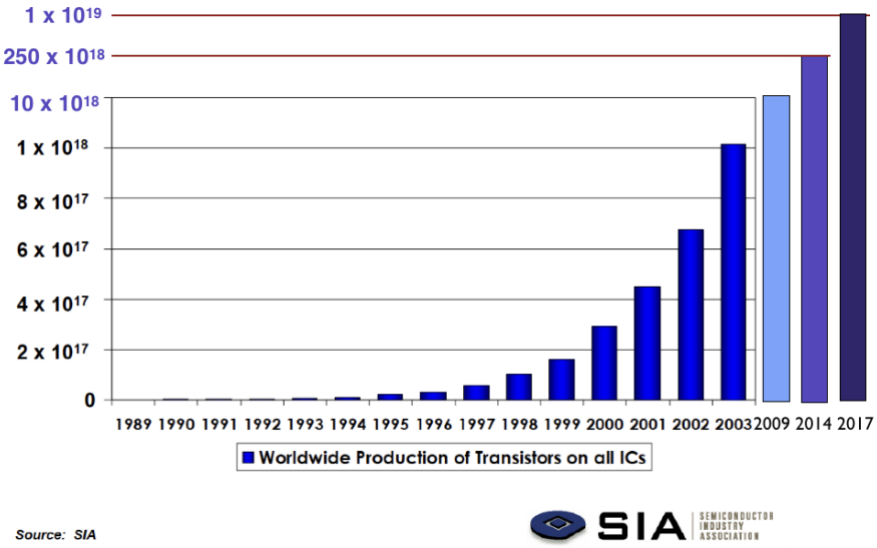

Fig. 1. Number of transistors produced annually in the world [adapted from SIA 2005]

An essential keyword on the Internet of Things is **optimisation**, especially the optimisation of power consumption, which must be addressed at all levels of abstraction in the design flow of a computer or electronic system. The total power optimisation is a summation of the optimisation done at each level of design abstraction. So, sustainable computing requires optimisation at all design levels of a computer or electronic system design.

So, it is needed, more and more, to reduce the transistor count in each application specific design, which means the design of dedicated chips for embedded systems and new computer architectures (that nowadays means the design of new systems on chip). In other words, the use of Application Specific

Integrated Circuits (ASICS). Also, due to reduction in voltages, the circuits are becoming more sensitive to radiation effects, even at ground level. Then, dedicated circuits to be used in critical applications, like in medicine and transport, must use fault tolerant techniques.

2 Internet of Things

Devices connected to the Internet of Things (or the Internet of Everything), can have many different complexities. If the complexity is considered by the number of components, the IoT includes small devices (with few transistors) and large devices (with billions of transistors). Large devices will consume much more power, but it should be considered that most devices on the Internet of Things are small ones with a low number of transistors. But, because they are found in large quantities, they can represent a total consumption more important than the consumption of the so-called large devices that, in general, are in a lower number. Therefore, consumption optimisation must be performed on both large and small devices that are present in large quantities. Another aspect to consider is that some devices require the application of reliability techniques (such as those related to transport or health systems), which can increase the number of components. Other devices are not critical, such as a camera or video, where an error in viewing a pixel of an image does not cause significant problems. Also, there is several cases where there is the need to consider security, as the protection of intellectual property.

It can be expected that many systems connected to the Internet of Everything (IoE) will be Cyber Physical Systems (CPS), that are systems composed by different classes of components like electronic elements, mechanical elements, optical elements, physical sensors, chemical sensors, organic components, and many others. So, it is needed to develop Electronic Design Automation (EDA) tools to cope with the design of CPS composed of all these classes of devices.

Figure 2 [The Connectivist 2014] shows an estimate of the number of devices connected to the Internet since 1992 when they were about 1 million devices. By 2020 it is estimated that there will be more than 50 billion devices connected in the network, and just two years ago it was around 35 billion devices connected to the IoT. That means a 50% increase in just two years. This significant growth in the number of connected devices to the Internet has naturally led to a considerable increase in the energy need to run the IoT.

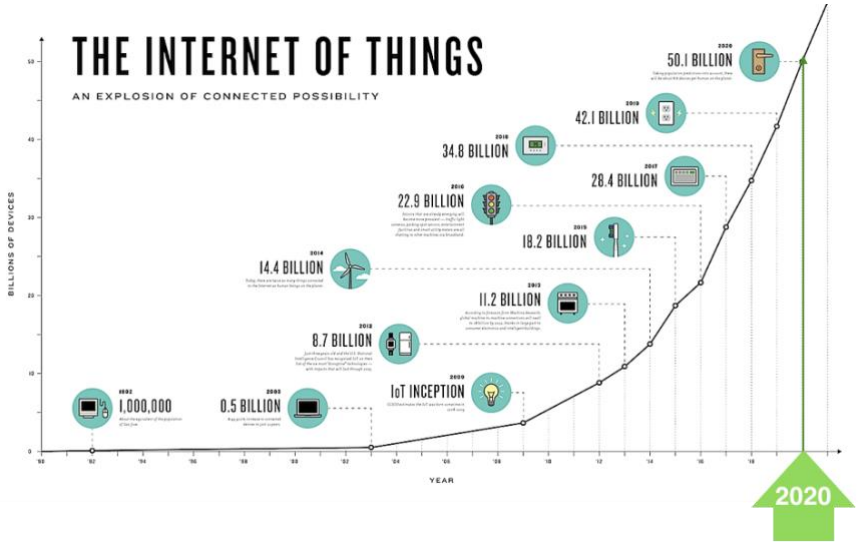

Fig. 2. Number of devices connected in the IoT
[adapted from The Connectivist 2014]

In critical areas such as the design of implanted devices (chips) in humans and chips to be used in transportation, the reliability of the implanted systems in humans and embedded systems in automobiles is obviously a critical issue. Some of the used techniques are based on the triplication of circuits and the temporal analysis of the propagation of a signal. Previously, the design of fault-tolerant circuits, to cope with radiation effects, was mainly in circuits that were sent to space. With the reduction of the value of the supply voltage of integrated circuits, nowadays the integrated circuits for use at ground level are also sensitive to errors caused by the radiation incident on the earth. Therefore, in critical applications it is necessary to implement radiation effects tolerance techniques [Velazco 2007]. Any critical systems used in the Internet of Health should be tolerant to any kind of noise (internal or external to the human body). They also must have a larger lifetime as possible, for obvious reasons and also should cope with environmental variability.

3 Power Consumption

The reduction of the power consumption of a System on a Chip (SoC) is a function of a sum of techniques and design strategies applied in different levels of abstraction in the design flow of an integrated system [Reis 2011A], [Reis 2011B]. The summation of the gains is that will define the total gain in power reduction. When we deal with the physical synthesis of a system on a chip, one technique is the optimisation of the number of components, that is, the transistor count. In Figure 3, it can be observed two solutions for the implementation of the same equation. The

first solution makes use of 4 basic logic gates (2 NOR 2-input ports and 2 NANDs), using a total of 16 transistors. We are not considering the possible inverters in the input as the inversion can be already available (as for example, if the variable is the output of a flipflop that has both values available in its output). The second solution makes use of only one logic gate (a supergate), which performs the same function but with only 10 transistors. That is, the second solution, having a reduction in the transistor count, will also have a proportionally smaller static power consumption. Furthermore, in the example of Figure 3, we can see that the first solution also has 3 connections between the basic gates (and therefore vias and contacts) that are eliminated in the second option, with only one larger logic gate.

This elimination of connections is increasingly important because it decreases the number of connections to be implemented in the routing step, using the different metal layers. The decrease in the number of connections decreases the density of connections and, therefore, increases the routability of the circuit. It also contributes to reduce the average length of the connections, which implies in a reduction of the delay. In modern technologies, the delay in connections is so or more significant than the delay in the switching of logic gates. A greater spacing between the connections also contributes to an increase of reliability, due, for example, to the reduction of the possibility of electromigration [Posser 2017].

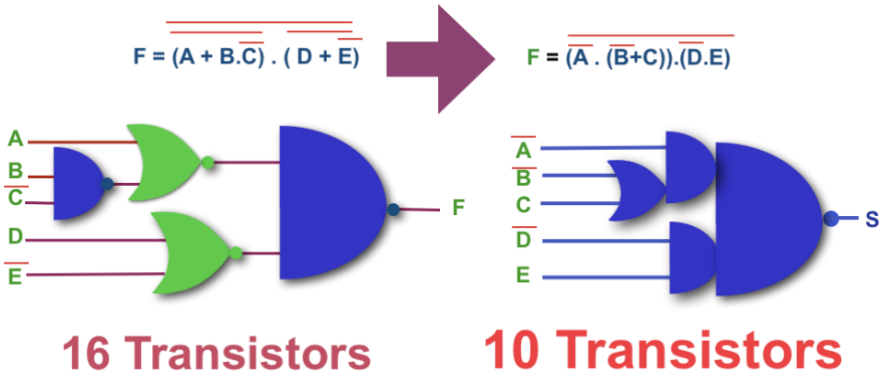

Fig. 3. Two options for the implementation of the same function [2011A Reis]

The reduction of the transistor count depends on the use of efficient EDA tools that transform the logical equations of a system so that in addition to mapping equations in CMOS gates, make optimal use of complex logic gates. In [Conceição 2019] we present a tool to reduce the number of transistors in a circuit through the fusion of networks of transistors that present fanout equal to 1. Also, it is fundamental the use of an automatic synthesis tool that can perform the automatic layout of any logical function. There is no way to achieve a logical optimisation when it should be used a technology mapping step to transform the equations according to the logic gates available in a traditional cell library [which have few

functions, in general, no more than 100 functions], as is done when using a traditional EDA system for standard cell-based designs. The technology mapping represents a step of deoptimization. With this aim, we have developed automatic layout synthesis tools such as ASTRAN [Ziesemer 2015] (Figure 4), which allows the automatic layout generation of any network of transistors [Reis 2011A].

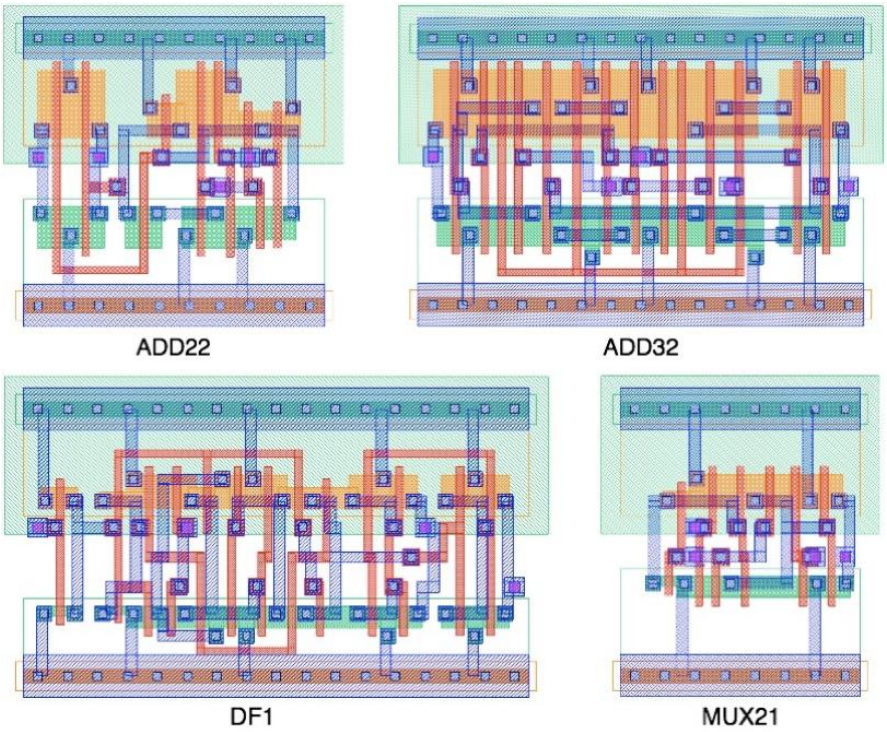

Fig. 4. Transistor Network Layouts Generated Automatically [Ziesemer 2015]

Another technique to reduce consumption is through the sizing of the transistors. Modern integrated circuit manufacturing technologies show a significant increase in static power consumption that is often greater than dynamic power consumption. One way to mitigate power consumption, especially the static one, is to carry out a sizing of transistors to optimise power consumption. In [Reimann 2016] significant decreases in consumption are obtained through the use of automatic transistor sizing tools. This method is also called cell selection, when the cells are selected from a cell library. In this case, cell selection means the selection of cells with a specific size and Vth (threshold voltage). In traditional cell libraries, one function has in general 3 sizings (one for smaller area, one for less power, and one for smaller delay) and 3 Vth (threshold voltage).

It is possible to investigate different strategies to do the automatic layout generation, one is ASTRAN that was referred above, another one is presented in

Figure 5, where transistors are placed and routed using some metal bricks and contacts/vias, to construct the layout of a transistor network.

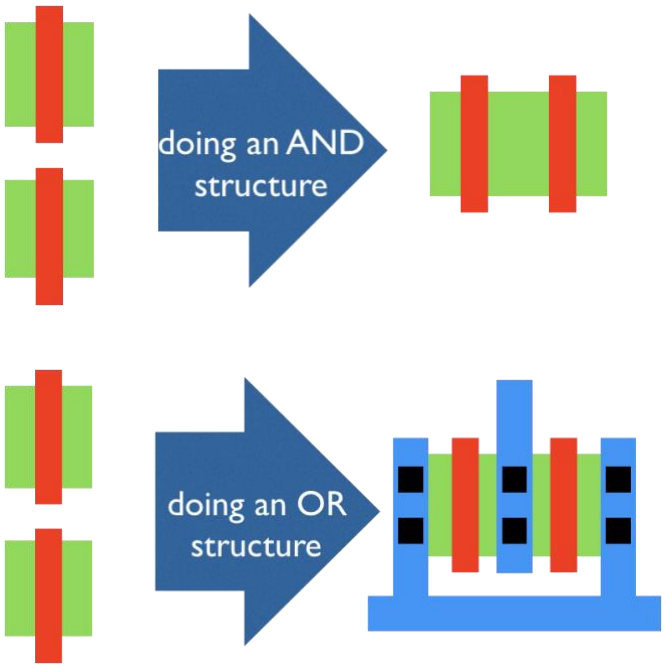

Fig. 5. Placement and routing of transistors to obtain the layout a transistor network

4 Reliability

The design of critical systems demands the use of techniques to increase reliability at different levels of design abstraction. At the architectural level, a traditional method is the redundancy of modules, especially triple module redundancy (TMR) [Kastensmidt 2006]. Another is the temporal redundancy [Nicolaidis 1999] where a signal traverses two paths, one with higher delay and another one with less delay. The difference of delay must be longer than the duration of a transient. Comparing the signal after traversing the two paths indicates if there was a transient propagation or not. At the physical level, we can apply different techniques to reduce or avoid problems such as electromigration [Posser 2017]. In [Velazco 2007] it is presented a series of works aimed at mitigating the effects of radiation on integrated circuits. In [Kastensmidt 2006] [Neuberger 2014] [Gennaro 2017] [Aguiar 2016] [Lazzari 2011] [Brendler 2018] [Brendler 2019] it is presented some of the results that our

research group has obtained in the development of techniques aiming the design tolerant to faults due to transients, as the ones due to radiation effects.

It was observed that there is an influence of the transistor arrangement in the sensitivity of gates to radiation effects [Brendler 2018] [Zimpeck 2018]. In Figure 6 it is presented an AOI21 gate designed using (a) close and (b) far topologies for a 7nm predictive Finfet technology. It was observed that for short pulse width the Far topology was less sensitive to radiation effects and more sensitive when the pulse width is above 1200 ps for a LET of 10MeV.cm2.mg-1. But for Linear Energy Transfer (LET) of 58MeV.cm2.mg-1, the Far topology is more sensitive from pulse width of 350 ps or more.

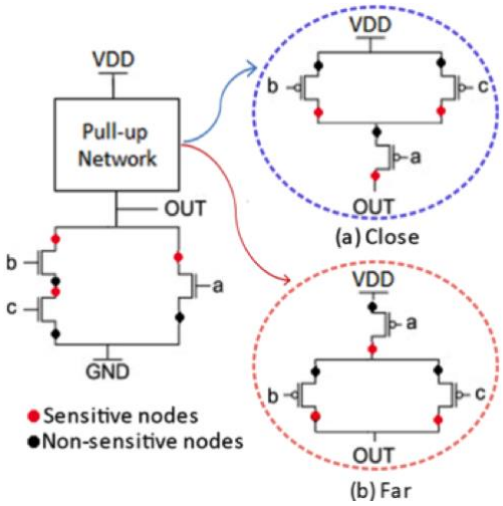

Fig. 6. Influence of transistor arrangement in the sensitivity of gates to radiation effects [Brendler 2018]

5 Security

Security is a critical issue in the design of many circuits and systems for IoT. Chip content security has increasingly become one of the significant issues for the Semiconductor (IC) Industry, and the reasons range from counterfeiting to the theft of core technologies and trade secrets. This concern is even more significant in the IoT context, that uses more and more embedded systems and embedded devices on a large scale. An extensive set of IoT circuits are small ones and typically using mature process technology, which implies in a circuit more accessible to suffer reverse engineering by delayering the set of layers. These characteristics make these embedded systems susceptible to intellectual property infringement using reverse

engineering attacks [El Massad 2015]. However, there are also more and more IoT devices using modern technologies using several layers and making the reverse engineering more complicated, but still possible.

Let's consider the design security in IoT from the perspective of the physical design. One action is to make reverse engineering more laborious by using camouflage techniques. Another way to make reverse engineering difficult is to use different transistor arrangements for the same function, or yet to use complex logic functions beyond the available ones in a standard cell library. Also, it can be considered the generation of different layout approaches for a same function. This task is more comfortable with the help of an EDA tool to generate several different layouts for a same function. Chip-level reverse engineering is an analysis of electronic circuits that focus on getting back the circuit functionality description from the layout view, by first identifying the transistors and how they are connected. Chip-level reverse engineering is a more and more complex task that demands advanced equipment like high-resolution optical and electronic microscopes, probe stations and logic analysers. It comprises several main steps, as illustrated in Figure 7.

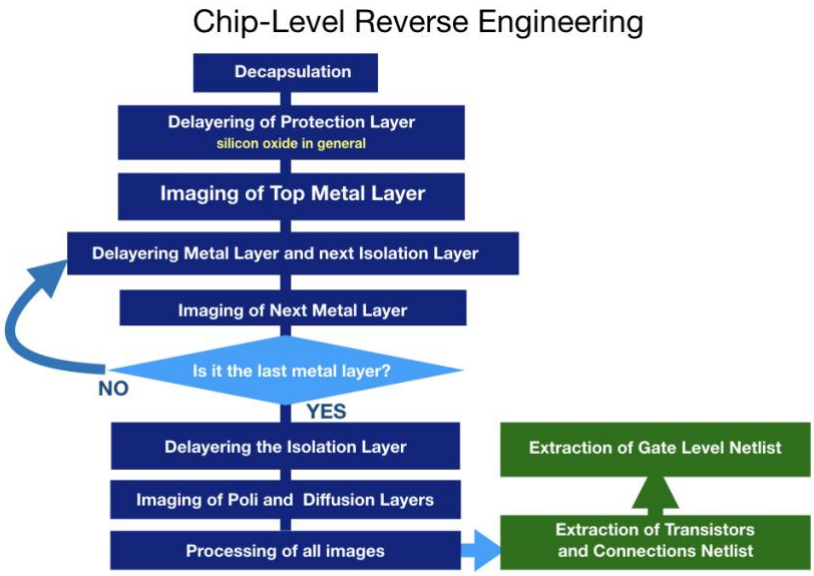

Fig. 7. Influence of transistor arrangement in the sensitivity of gates to radiation effects [Brendler 2018]

The decapsulation step exposes the IC internal components like the die and pad interconnections. Delayering consists in taking out the material of layer by layer. It is a destructive process done by using acids and allowing to see each metal

layer, polysilicon, active areas and substrate. In each imaging step, an image is taken of each layer using an ultra-high-resolution optical microscope. Each image related to each metal layers, via layers, polysilicon layer and diffusion layers are saved in a database. Then, it is done a post-processing to analyse the obtained images of each layer to build up first a transistors and connections netlist. Then, from this netlist it is obtained a gate level one. From a gate level netlist it is possible to go to higher abstraction levels and to discover the functionality of the chip. Let's present some alternative physical design approaches to prevent this kind of attack by making harder the reverse engineering steps.

Post-processing steps in chip-level reverse engineering cover the activities of annotation, gate-level schematic extraction, and schematic analysis and organization. These steps are partially automated by extraction tools and pattern recognition tools that are used to annotate wire names, identify connections, and recognize logic cells. Anti-reverse engineering strategies rely on reducing the power of such tools, making the activities more time consuming, complicated, and expensive willing to discourage most forms of attack.

The camouflage technique is a way to provide security for the circuit in the cell level. Instead of only using cells from a typical standard cell library, it works by selecting some gates from the original netlist to be camouflaged [Rajendran 2013]. It uses a look-alike technique where camouflaged gates share the same layout and include dummy lines, as well as dummy and true pins, as shown in Figure 8. The choice of which pins will be true or dummy defines the gate functionality. Therefore, some cells in the circuit layout will differ just by the contact layers, thus making a pattern recognition more difficult.

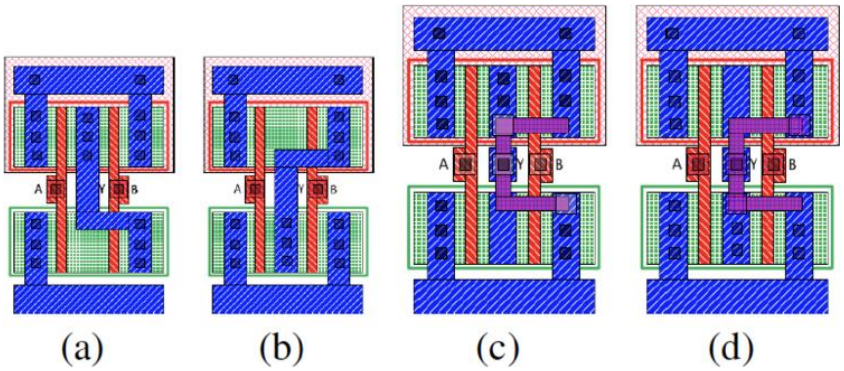

Fig. 8. Influence of transistor arrangement [Rajendran 2013]

The work of [Gomez 2019] proposes to use many different layouts for the same cell as an alternative to a look-alike method. Besides NOR and NAND gates, they propose to automate the layout of inverters, latches, and flip-flop cells to generate different layouts as a way to improve security. They argue that an imaging tool is trained with a database of regular optimal cells. So, it will not be able to

identify other gates that have a non-optimal geometry shape, and therefore they cannot extract a full netlist.

The use of more complex AOIs (And Or Inverters) is also a way to complicate a reverse engineering, mainly if a same AOI can have different layouts. Transistor reordering is a simple technique based on rearranged transistor networks keeping the same logic function. In the design of AOI gates, it is possible to consider different orderings of the transistors for the same function as shown in Figure 9. Different transistor combinations change the electrical and physical characteristics of logic cells, and consequently, it also alters the susceptibility to process variations and radiation-induced soft errors. However, it can also be used to complicate reverse engineering.

Figure 9 shows the layout of an AOI21 logic cell implemented using two different transistor ordering. The layouts are related to a FinFet technology using three fins per transistor. It is possible to see that the metal layer is different in both solutions. So, the use of different transistor ordering for the same function also helps to difficult reverse engineering. However, it is also known that a different transistor ordering means different sensitivity to radiation effects [Zimpeck 2019].

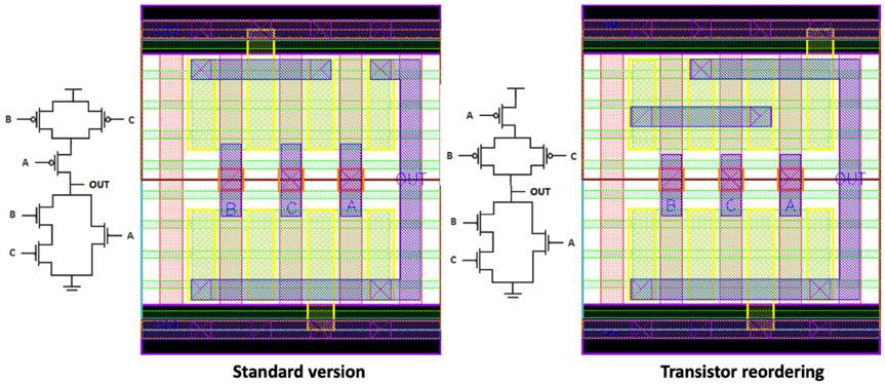

Fig. 9. An AOI using two different transistor reordering

As mentioned, instead of making similar layouts for different logic functions to make reverse engineering difficult, we can also use an opposite option, that is to have many different layouts for a same logic function. It is possible by generating transistor networks on the fly using a layout generator tool as ASTRAN [Ziesemer 2015]. Even better if the logic function is not a conventionally one found in a traditional cell library.

The use of complex cells composed by several transistors provides a more extensive set of layout options as well as a big design exploration with transistor reordering. As an example, Figure 10 shows four layout options for the same logic function, also using transistor reordering, that enables four different metal layer artworks. Other layout artworks are still possible for the same netlist varying the parameters of the cell layout generator.

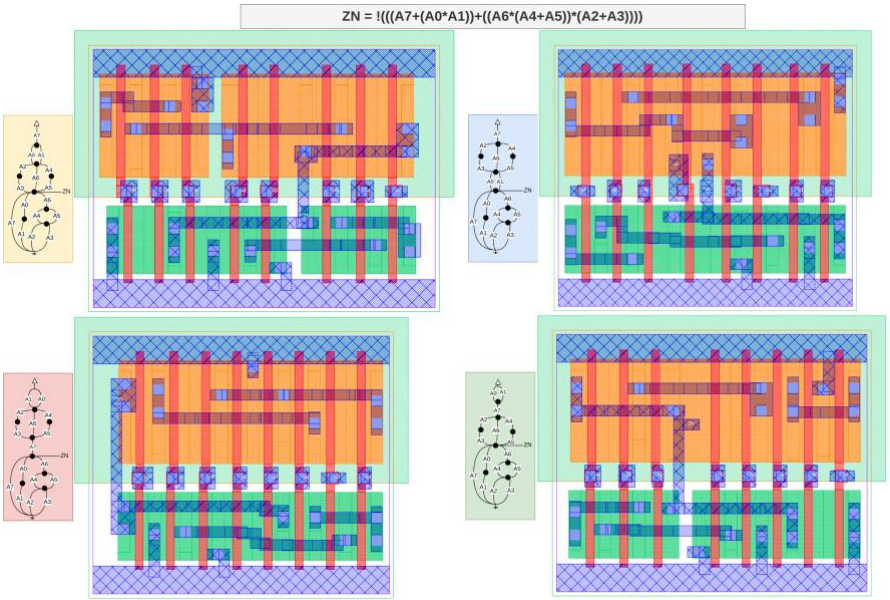

Fig. 10. The same AOI function using 4 different transistor arrangements

This approach does not show the limitations that we have when using a standard cell library, that contains a limited set of logic functions and a limited set of sizing. By using a layout generator tool, we overcome this limitation and extend the number of logic functions that a circuit can use, as well to generate cells with a large set of sizing options. This push reverse engineers to analyse circuit from a transistor level instead of a gate level, thus considerably increasing the complexity of a reverse engineering approach.

The tool we developed can be set to generate new complex cells (supercells) with up to a limiting number of transistors defined by the designer, as well as the limit of allowed serial transistors.

6 3D Circuits

There are two main types of 3D circuits. The basic 3D circuits are composed of several tiers (layers) of silicon fabricated separately and mounted one over the other and connected by using TSV (through-silicon vias) (see Figure 11). They are called TSV 3D Circuits or Stacked 3D Circuits.

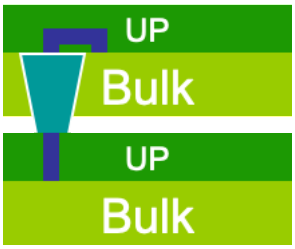

Fig. 11. Scheme of a TSV 3D circuit (Hentschke 2007)

Another type of 3D Circuits, shown in Figure 12, is the Monolithic ones (M3D), where the tiers of transistors are placed one over the others by deposition. The connections between tiers in a monolithic 3D Circuits (MIVs) are much smaller than the TSVs used in stacked 3D Circuits. Also, the layers of transistors in a monolithic 3D are separated by an isolation layer much thinner than in stacked 3D circuits. In one main type of monolithic circuits, one tier is used to do the NMOS transistors (the top one), and a next tier is used to do the PMOS transistors. The implementation of connections is divided into two set of connections, the interlayer one, that mainly does the connections inside a network of transistors (logic cell) and are located between P and N tiers. The longer connections use a back-end level of connections in the top of the NMOS layer (see Figure 12).

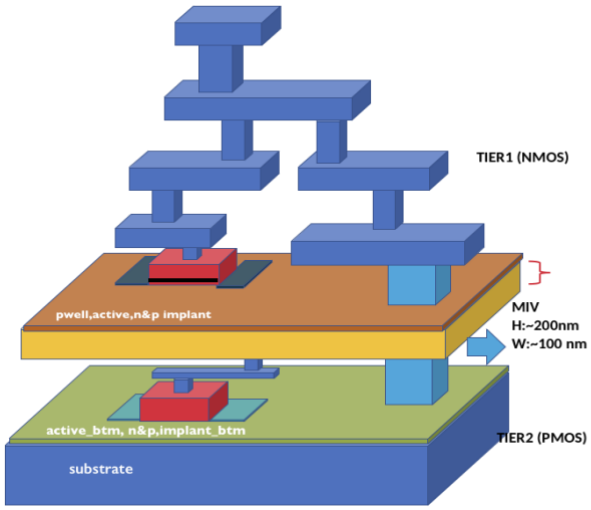

Fig. 12. Scheme of a Monolithic 3D circuit (source: Carolina Metzler)

It is also possible to conclude that 3D circuits are more protected to reverse engineering, mainly the monolithic ones, as they are more difficult and more

laborious to do delayering. The use of different tiers to do PMOS and NMOS transistors also help to improve security. It can also be concluded that 3D circuits are more tolerant to radiation effects as lower tiers will be less sensitive to radiation.

In Monolithic 3D, a gate is folded and implemented using two tiers (Figure 13). The use of more regular layout of transistor networks is important to allow an easier way to implement MIVs as a vertical one, connecting top and bottom layer elements.

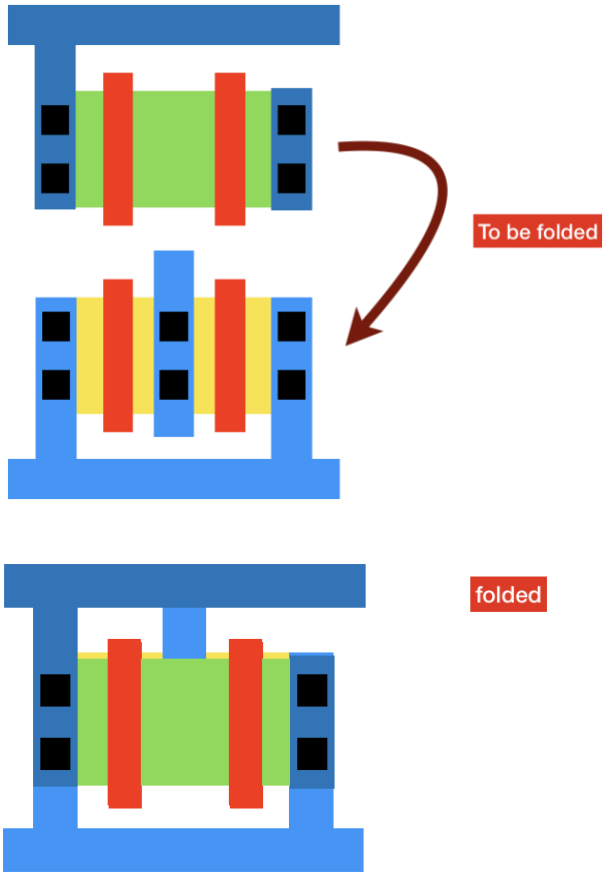

Fig. 13. In Monolithic 3D, a gate is folded and implemented using two tiers

The different tiers of a 3D circuit can correspond to different types of circuits as well to different technologies. The only concern is to well adjust the placement of TSVs or MIVs. Figure 14 shows an example.

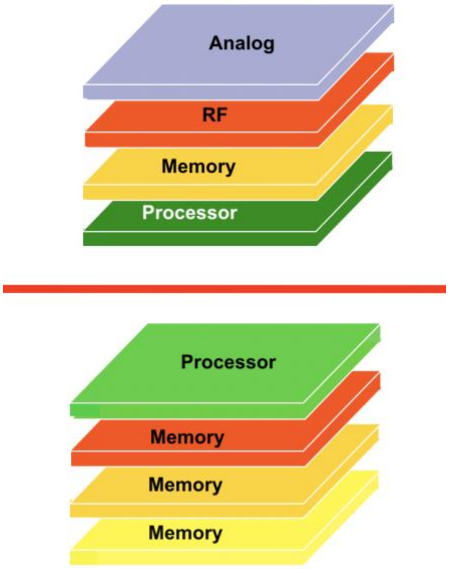

Fig. 14. The different tiers of a 3D circuit can correspond to different types of circuits

7 Hardware Accelerators

The evolution of computer architectures, which today means, the evolution of microprocessor architectures has been very significant. Nowadays, there are chips with multiple CPUs and several GPUs, as can be seen in Figure 15 [Techinsights, 2018] showing the floorplan of the A12 microprocessor (from Apple). In this same figure, it can be observed that about half of the area is occupied with hardware accelerators, which are modules dedicated to the execution of a specific function. For example, an encryption module placed next to the output/input pins and which will encode the output data and decode the received data. The execution of this function will be faster, because it is done by a dedicated module (that means a smaller one) and with only the needed number of transistors to perform that function. It also will consume less power.

A more important fact is that the use of hardware accelerators leads to greater energy efficiency (allowing more sustainable computing), mainly due to the reduction in the number of components used to perform a function. At any given time, only the hardware accelerators in use at that time are being powered. So, the hardware accelerators that are not in use are disconnected from the power supply (shut down). This strategy is also known as "Dark Silicon". We can even predict

architectures consisting essentially of hardware accelerators, with only one or two small CPUs to manage these hardware accelerators.

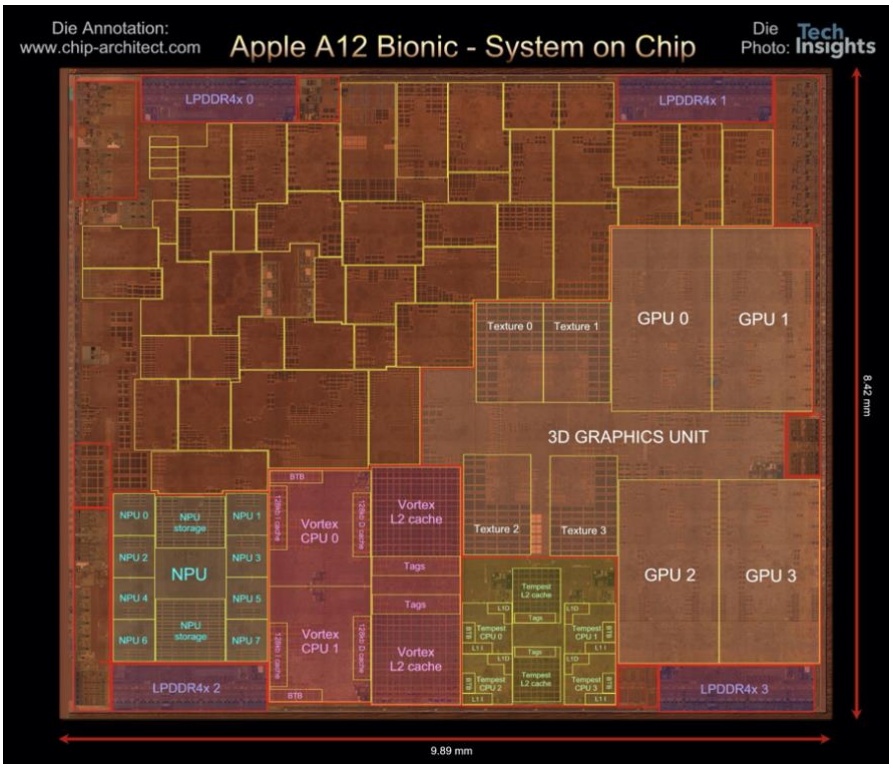

Fig. 15. Apple 12 Floorplan with an NPU [Techinsights, 2018]

The introduction of an Neural Processing Unit (NPU) in A11 is another element characterising the heterogeneity of the SoC. And we can expect increasingly heterogeneous architectures, with dedicated modules for different operations to be performed by a SoC. In Figure 15 [Techinsights, 2018] the floorplan of the Apple A12 microprocessor is presented, where one of the modules is an NPU. NPU is mostly dedicated to facial recognition [Techinsights, 2018], processing machine learning tasks more efficiently, consuming less energy than CPUs do. The 2 high performance CPUs plus the 4 lower power CPUs, occupy about 15% of the area of the chip and 4 GPUs occupy about 20% of the area. Most of the area is filled with the hardware accelerators. That is, it is increasing the use of hardware accelerators in the architecture of Apple microprocessors/systems on chip.

6 Conclusions

The main challenges in several areas of Computing Systems, as in Embedded Systems, Computer Architectures, Fault Tolerance and Integrated Circuits and Systems, are mainly power consumption, reliability and security. To have sustainable computing, it is fundamental that the design of the devices connected to the IoE, includes optimization in all abstraction levels of a design, mainly with the goal of reducing power consumption. At architectural level, the use of hardware accelerators is a great strategy, not only to reduce power consumption but also to speed up the execution of functions.

At physical level, it can be observed that most of the chips being designed nowadays use many more transistors than necessary to perform a function. There is a significant space for the optimisation of the transistor count at logical level. In devices related to critical applications, like medical and transport ones, it is needed the application of techniques for fault tolerance, as nowadays circuits at ground level can have faults due to radiation effects. The keyword in the IoT/IoE is **optimisation**.

7 Acknowledgements

We thank CNPq, FINEP, Fapergs, and CAPES for financial support for the development of our team's work, as well as the master's and doctoral students of PGMICRO and PPGC and students of Scientific Initiation who have contributed to the research works that served as the basis for this paper.

References

[Reis 2018] REIS, R., **Strategies for Reducing Power Consumption and Increasing Reliability in IoT,** First Cross-domain IFIP Internet of Things (IoT) Conference, Poznan, Poland. September 18-19, 2018. In: Internet of Things. Information Processing in an Increasingly Connected World, DOI: 10.1007/978-3-030-15651-0_8

[SIA 2015] Semiconductor Industry Association, **Rebooting the IT Revolution**, available at http://www.semiconductors.org/clientuploads/Resources/RITR%20WEB%20version%20FINAL.pdf

[The Connectivist 2014], available at: http://ow.ly/i/5vph6/original

[Velazco 2007] VELAZCO, R., FOUILLAT, P, REIS, R. 2007], **Radiation Effects on Embedded Systems**, Springer, June 2007. ISBN 978-1-4020-5645-1

[Reis 2011A] REIS, R., **Design Automation of Transistor Networks, a New Challenge**. IEEE International Symposium on Circuits and Systems, ISCAS2011, Rio de Janeiro, Brasil, May 15-19, 2011. IEEE Press. p. 2485-2488, DOI 10.1109/ISCAS.2011.5938108

[Reis 2011B] REIS, R., **Power Consumption & Reliability in NanoCMOS**, IEEE NANO, 11th International Conference on Nanotechnology, Portland, USA, August 15-19, 2011 (**invited talk**), p.711-714, DOI:10.1109/NANO.2011.6144656

[Posser 2017] POSSER, G., SAPATNEKAR, S., REIS, R., **Electromigration Inside Logic Cells**, Springer, 118 p., 2017, DOI 10.1007/978-3-319-48899-8

[Conceição 2019] CONCEIÇÃO, C., REIS, R., **Transistor Count Reduction by Gate Merging**, IEEE Transactions on Circuits and Systems I, Vol. 66, Issue 6, June 2019, DOI: 10.1109/TCSI.2019.2907722.

[Reimann 2016] REIMANN, T., SZE, C., REIS, R., **Challenges of Cell Selection Algorithms in Industrial High Performance Microprocessor Designs**, Integration, Elsevier, Vol. 52, January 2016, Pages 347-354, doi:10.1016/j.vlsi.2015.09.001, ISSN: 0167-9260

[Ziesemer 2015] ZIESEMER, A., REIS, R., **Physical Design Automation of Transistors Network**, Microelectronics Engineering, V. 148, p. 122-128, December 2015, Elsevier B.V., ISSN: 0167-9317, doi:10.1016/j.mee.2015.10.018

[Kastensmidt 2006] KASTENSMIDT, F., CARRO, L.; REIS, R., **Fault-Tolerance Techniques for SRAM-Based FPGA**, Springer. April 2006, 183 p., ISBN 0-387-31068-1

[Nicolaides 1999] NICOLAIDIS, M., **Time redundancy based soft-error tolerance to rescue nanometer technologies**. In: IEEE VLSI TEST SYMPOSIUM, 17., 1999. Proceedings... IEEE Computer Society, 1999. p. 86-94.

[Neuberger 2014] NEUBERGER, G., WIRTH, G., REIS, R., **Protecting Chips Against Hold Time Violations Due to Variability**, Springer, 107 p., 2014. ISBN 978-94-007-2426-6. DOI 10.1007/978-94-007-2427-3

[Gennaro 2017] GENNARO, R., ROSA, F., OLIVEIRA, A., KASTENSMIDT, F., OST, L., REIS, R. (2017), **Analyzing the Impact of Fault Tolerance Methods in ARM Processors under Soft Errors Running Linux and Parallelization APIs**, IEEE Transactions on Nuclear Science, Volume: 64, Issue: 8, August 2017, ISSN: 1558-1578, DOI: 10.1109/TNS.2017.2706519

[Aguiar 2016] AGUIAR, Y., ZIMPECK, A., MEINHARDT, C., REIS, R. (2016), **Permanent and Single Event Transient Faults Reliability Evaluation EDA Tool**, Microelectronics Reliability, Volume 64, September 2016, Pages 63-67, published by Elsevier B.V., 2016. ISSN: 0026-2714.

[Lazzari 2011] LAZZARI, C., WIRTH, G., KASTENSMIDT, F., ANGHEL, L., REIS, R. (2011), **Asymmetric Transistor Sizing Targeting Radiation-Hardened Circuits**, Journal on Electrical Engineering, Springer, DOI10.1007/s00202-011-0212-8, June 2011.

[Brendler 2018] BRENDLER, L. H.; ZIMPECK, A. L.; MEINHARDT, C.; REIS, R., **Evaluating the Impact of Process Variability and Radiation Effects on Different Transistor Arrangement**. In: VLSI-SOC - International Conference on Very Large Scale Integration (VLSI), 2018, Verona. VLSI-SOC - International Conference on Very Large Scale Integration, 2018. v. 1. p. 1-6.

[Brendler 2019] BRENDLER, L., ZIMPECK, A., MEINHARDT, C., REIS, R., **Multi-level Design Influences on Robustness Evaluation of 7nm FinFET Technology**, IEEE Transactions on Circuits and Systems I. DOI: 10.1109/TCSI.2019.2927374

[Zimpeck 2018] ZIMPECK, A., MEINHARDT, C., ARTOLA, L., HUBERT, G., KASTENSMIDT, F., REIS, R., **Impact of Different Transistor Arrangements on Gate Variability**, Microelectronics Reliability, Volume 88-90, September 2018, Pages 111-115, published by Elsevier B.V., ISSN: 0026-2714. doi.org/10.1016/j.microrel.2018.06.090

[El Massad 2015] EL MASSAD, M., GARG, S., TRIPUNITARA, M., **Integrated circuit (IC) decamouflaging: Reverse engineering camouflaged ICs within minutes**. Network and Distributed System Security Symposium (NDSS) (01,2015). https://doi.org/10.14722/ndss.2015.23218

[Rajendran 2013] RAJENDRAN, J., SAM, M., SINANOGLU, O., KARRI, R., **Security Analysis of Integrated Circuit Camouflaging**, CCS'13, November 4–8, 2013, Berlin, Germany

[Gomez 2019] GOMEZ, H., DURAN, C., ROA, E.: **Defeating silicon reverse engineering using a layout level standard cell camouflage**. IEEE Transactions on Consumer Electronics 65(1), 109{118 (Feb 2019). https://doi.org/10.1109/TCE.2018.2890616

[Hentschke 2007**]** HENTSCHKE, R., **Algorithms for Wire Length Improvement of VLSI Circuits with Concern to Critical Paths,** PhD. Thesis, PPGC/UFRGS, 2017**.**

[Zimpeck 2019] ZIMPECK, A., MEINHARDT, C., KASTENSMIDT, F., HUBERT, G., REIS, R., ARTOLA, L., **Mitigation of process variability effects using decoupling cells,** Microelectronics Reliability, Volume 100-101, September 2019, 6 pages, paper 113446, published by Elsevier B.V., ISSN: 0026-2714. DOI: 10.1016/j.microrel.2019.113446

[Techinsights 2018], http://techinsights.com/