Building Trusted ICs using Split Fabrication

Kaushik Vaidyanathan, Bishnu P Das*, Ekin Sumbul, Renzhi Liu, Larry Pileggi
Carnegie Mellon University, Pittsburgh, PA 15213
kvaidya1@andrew.cmu.edu

***Abstract*—Due to escalating manufacturing costs the latest and most advanced semiconductor technologies are often available at off-shore foundries. Utilizing these facilities significantly limits the trustworthiness of the corresponding integrated circuits for mission critical applications. We address this challenge of cost-effective and trustworthy CMOS manufacturing for advanced technologies using split fabrication. Split fabrication, the process of splitting an IC into an untrusted and trusted component, enables the designer to exploit the most advanced semiconductor manufacturing capabilities available offshore without disclosing critical IP or system design intent. We show that split fabrication after the Metal1 layer is secure and has negligible performance and area overhead compared to complete IC manufacturing in the off-shore foundry. Measurements from split fabricated 130nm testchips demonstrate the feasibility and efficacy of the proposed approach.**

***Keywords*—Hardware security; Circuit obfuscation; Design for trust; Split fabrication.**

I. Introduction

The global IC supply chain makes integrated circuits (ICs) vulnerable to backdoor insertions and malicious circuit modifications [1]. Recent compromise of critical defense systems using targeted hardware attacks [2] has established the need to understand and counter such attacks. To secure military ICs from attacks, the US department of defense (DoD) had created the trusted access program [3] that restricts military grade chips to be designed, fabricated and packaged by accredited partners on-shore. However, with escalating cost and complexity of semiconductor manufacturing [4], some of the most advanced IC foundry technologies are available only at off-shore manufacturing facilities, thereby making the designs vulnerable to attacks. The mission critical ICs that will attempt to use these advanced off-shore technologies for defense and infrastructure require a trusted and state-of-the-art design flow, which we demonstrate is possible with a split fabrication approach.

Split fabrication, the process of splitting the IC into an untrusted and trusted component, enables the designer to exploit advanced semiconductor manufacturing capabilities available offshore without fully disclosing the system design intent [5] (Figure 1). A critical aspect of split fabrication which directly impacts the security, cost effectiveness and efficiency guaranteed by this technique is the metal layer after which the design is split between the untrusted and trusted foundries. Two embodiments of split fabrication have been previously proposed, namely split with 3D integration [7] and split after Metal3 (M3) [6], Figure 2(a) and 2(b) respectively. Imeson et al. [7] proposed split fabrication with 3D integration and computed the theoretic security provided by lifting certain wires to the trusted 3D tier using through silicon vias (TSV). Significant performance and area penalty of split with 3D clearly precludes such an approach from being adopted in high performance ASICs and SoCs. As for split fabrication after M3, Rajendran et al., in [6] proposed the proximity attack where the attacker in the untrusted foundry can potentially infer the hidden connections in the trusted tier using connections between gates in the untrusted tier, making it possible to perform a targeted attack. Therefore, clearly, both techniques do not achieve a good tradeoff between efficiency, security and cost. As a result, there is an overwhelming need for holistically evaluating different split fabrication options, bearing in mind all practical considerations.

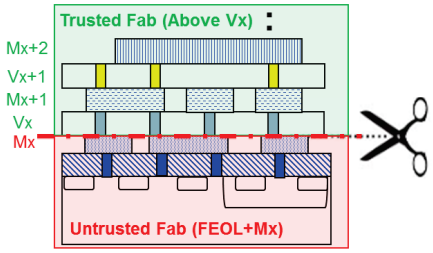


Figure 1. Split fabrication after Mx.

As the front end of line (FEOL) devices and Metal1 (M1) form the most complex and advanced aspects of a CMOS process [8], it is appropriate to use the untrusted foundry to manufacture the IC through completion of the M1 layer. The trusted foundry is then used to complete the remaining layers of the IC that establish the logic gate interconnections (Figure 2(c)), thereby obfuscating the system design intent to the untrusted foundry, hence enhancing hardware security. To illustrate the efficacy of split fabrication after M1 against reverse engineering at the untrusted foundry, we extract the circuit schematic from full layout (Figure 3(a)) and contrast that to a circuit schematic extracted from the same layout until M1 (Figure 3(b)). Note that for an advanced CMOS technology, M1 routing is used only to form leaf cells. Due to the critical and complex nature of the intra-cell M1 wiring patterns, the automated routing tools are generally not permitted to add inter-cell routing connections on that layer. It is clear, therefore, that with the FEOL and M1 layout, the attacker at the untrusted foundry only sees a sea of unconnected gates, thereby providing exceptional circuit obfuscation. To provide similar obfuscation, split after M3 or split after 3D would have to lift all gate interconnections to the metal layers above M3 or to the 3D layer, respectively. Lifting all wires to metal layers above M1 significantly increases design area as higher metal layers have relaxed wiring pitches.

* Currently with Indian Institute of Technology, Indore, India.

978-1-4799-4112-4/14/$31.00 ©2014 IEEE

Furthermore, increase in area and the number of additional vias in every wire owing to wire lifting would degrade performance and yield. Therefore, split fabrication after M1 incurs minimum design and cost overhead compared to split fabrication after M3 or split fabrication with 3D.

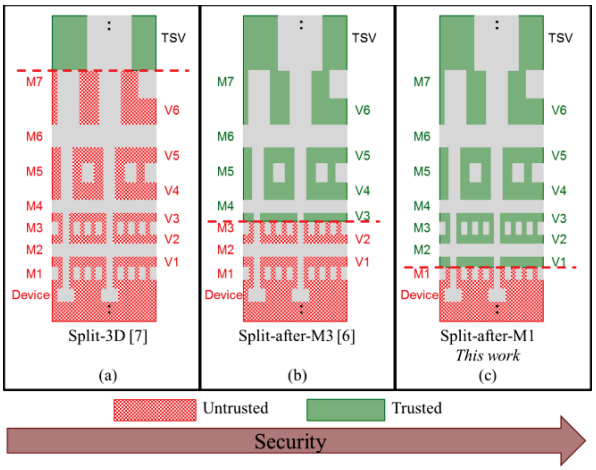


Figure 2. Split fabrication options, (a) Split with 3D [7], (b) Split after M3 [6], (c) Split after M1 (this work).

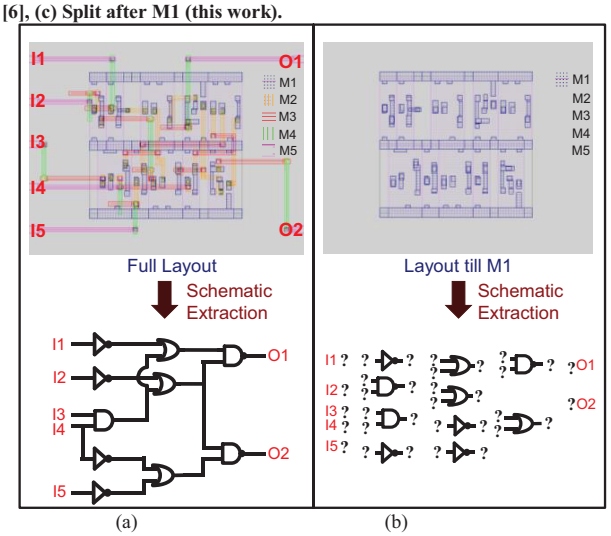


Figure 3. Tolerance to reverse engineering (a) Conventional fabrication: Full layout sent to untrusted foundry, extracted schematic is complete (b) Split fabrication after M1: Layout till M1 sent to untrusted foundry, extracted schematic is incomplete with sea of unconnected gates.

While split fabrication after M1 is an interesting concept, it is important to evaluate its effectiveness holistically, considering several practical challenges. A few practical challenges we have identified are: i) the notion of compatibility between the trusted and untrusted foundries, ii) impact of split fabrication after M1 on SoC design methodology, iii) additional process variation seen in split fabricated silicon iv) performance, power and area overhead of the split fabricated IC in comparison to a similar non-split fabricated IC. To tackle these issues and to identify any overhead arising from split fabrication after M1, it is essential to undertake a split fabrication exercise. We have designed, split fabricated and tested a high performance ASIC/SoC sub system in 130nm CMOS. Results indicate that split fabrication after M1 offers exceptional security while having negligible performance and area overhead compared to an unsecure IC that is manufactured completely in an off-shore foundry. Our key contributions are:

- propose and analyze security of split after M1.
- identify practical challenges in split fabrication and create a split fabrication compatible SoC design methodology.
- demonstrate design efficiency and security offered by split fabrication after M1 with 130nm CMOS testchips.

II. Security Analysis Of Split Fabrication After Metal1 (M1)

In this section we introduce an attack model and show that split fabrication after M1 is resilient to the previously proposed proximity attack [6].

A. Attack Model

Of the many hardware security attacks mentioned in [9], we cater to one of the most fundamental attacks, that is, the insertion of a hardware trojan at an untrusted foundry. Similar to [7] we assume that the attacker pursues a *targeted attack,* wherein the attacker is not interested in merely sabotaging the IC but wants to orchestrate a specific failure event(s) for a specific trigger input(s). For an attacker in the foundry to implant such a targeted attack, the attacker needs two things, a) Gate level netlist of the full design and b) Precise mapping of gates in the netlist to their physical location in the layout. In a conventional non-split fabrication scenario, since the untrusted foundry manufactures the entire IC, the attacker in the foundry has access to both these inputs and can undertake a targeted attack. The objective of split fabrication is to deny the attacker access to the complete gate level netlist and layout, thereby thwarting the attack.

The attack model is also shown in Figure 4 in the context of an SoC design flow, with the attacker in the untrusted foundry (in shaded red) having access only to the FEOL+M1 layout. Intellectual property (IP) blocks are typically considered a major source of hardware trojans [9]. Hence, hard IP blocks would need to be designed and qualified using split fabrication to guarantee security and performance [10]. Following manufacturing at the untrusted and trusted foundries, the wafer is diced into dies and packaged at a trusted facility as already enforced by the trusted access program, such as TAPO [3]. It is assumed that the attacker will not have access to the fully integrated IC thereby preventing any reverse engineering [11].

B. Security Analysis

Proximity Attack: Security analysis of split fabrication after M3 was done by [6]. They proposed the "proximity attack" wherein the attacker in the untrusted foundry leverages the existing connections in the untrusted tier, typically done within M3, to infer missing connections in the trusted tier above M3. They showed that it is possible to leverage the predictability associated with place and route tools to infer missing connections for small designs. For a simple place and route block as shown in Figure 5(a), it might be possible to

exactly identify the correct design connectivity by analyzing the proximity of gates and ports with missing connections. In contrast if we look at the same block in Figure 5(b), with all connections moved to the trusted tier in split after M1, it is extremely difficult, if not impossible, to correctly identify design connectivity with only the layout up to M1 available to the untrusted foundry. For instance, even for the simple example in Figure 5(b) a gate G is connected to K, L and H and not to its immediate neighbors I and J, illustrating the ineffectiveness of a proximity attack for split after M1.

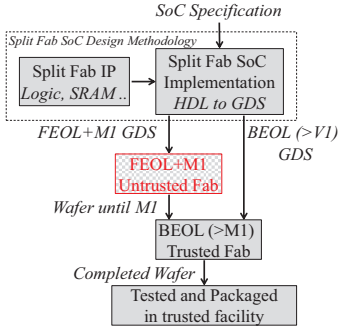
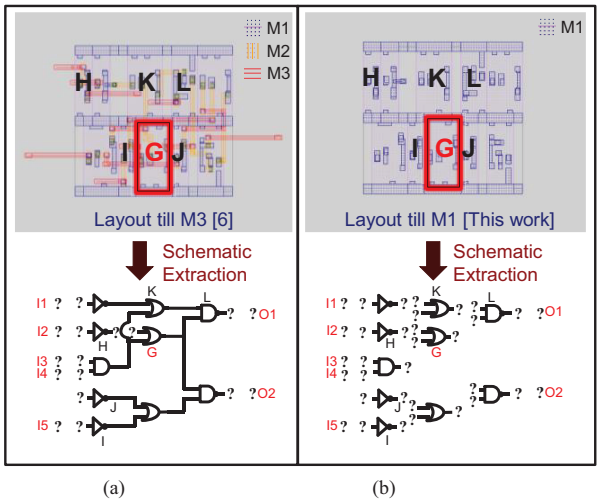


Figure 4. Attack model for split fabrication.



(a) (b)

Figure 5. Vulnerability to proximity attack (a) Split fabrication after M3 is vulnerable [6], (b) Split fabrication after M1 is not vulnerable.

As an SoC is physically partitioned into several blocks, we analyze security at the block level, not at the SoC level. If there are N gates in a block, and we were to make the simplistic assumption that every gate drives only one more gate (no fanout greater than 1) and there are no combinational loops, then there are at least N! configurations to interconnect these gates. In real designs, with fanout, the actual number of configurations N gates can be connected in is much higher than this lower bound. Conservatively, we use the lower bound (N!) as a security metric (W). For instance, for the simple example shown in Figure 5(b) where N is 10, W is 10!, i.e. 3.6e6. For a design with 1000 gates, W is 1e249. In a real block with thousands to millions of gates, it would be impractical for an attacker at the untrusted foundry, with no other additional information, to correctly identify all these connections. Therefore, security analysis of split fabrication after M1 reveals that this technique is tolerant to existing attacks and provides exceptional security for ASIC/SoC sub-blocks.

III. Split Fabrication After Metal1 (M1) Design

While there have been some investigations pertaining to the security offered by split fabrication [6-7], there has been little work on the practical challenges posed by split fabrication. In this section, we first formalize the notion of compatibility between the trusted and untrusted foundry, and then propose modifications to the commercial SoC design methodology to create efficient and secure split fabricated ICs.

A. Foundry Compatibility for Split Fabrication

In split fabrication literature it is implicitly assumed that the two foundries are compatible, without a clear definition of compatibility. We formalize the notion of foundry compatibility in split fabrication. Two foundries are split fabrication compatible if Mx, the last layer in the untrusted foundry and Vx, the first layer in the trusted foundry follow:

$$\mathbf{UT.Mx.W \geq T.Vx.LW + (2*Mx.EX.Vx)}$$

where, UT.Mx.W is the minimum width of Mx in the untrusted foundry, T.Vx.LW is the minimum size of Via Vx in the trusted foundry and Mx.EX.Vx is the minimum enclosure of untrusted foundry Mx on trusted foundry Vx (Figure 6). Mx.EX.Vx has to be agreed upon by the two foundries as this design rule arises from lithographic misalignment tolerances for Mx in untrusted foundry and Vx in trusted foundry.

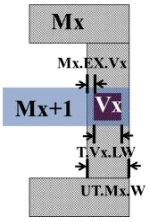


Table I. Comparison Table between Semi and Fully Compliant Split Fab

Semi-Compliant Split Fab	Fully Compliant Split Fab
Mismatch in BEOL stacks	Identical BEOL stacks
IPs containing beyond M1 need to split fab qualified	IP can be used as it is
Modify existing design flow to be split fab compatible	Physical synthesis flow can be used as it is
Ex. IBM and GF 130nm	Ex.: IBM Common Platform Alliance (<65nm)

Figure 6. Compatibility definition for foundries to split fabricate after Mx

If two foundries do not satisfy the inequality defined above, that foundry pair is deemed "incompatible" for split fabrication after Mx. Two foundries satisfying the inequality can further be classified as semi-compatible or fully compatible for split fabrication after Mx. Fully compatible foundries have same back-end-of-line (BEOL) stacks, as compared to semi-compatible foundries that have slightly different BEOL stacks. Table I summarizes the differences between the two methods. It is noteworthy that as most foundries are guided by scaling trends projected by International Technology Roadmap for Semiconductors (ITRS) [12], they end up being compatible. However, to differentiate themselves from competitors, foundries are often semi-compatible for split fabrication, unless, they co-develop the process, such as the IBM Common Platform [13], and end up being fully compatible foundries for split fabrication.

B. Design Methodology for Semi-Compliant Split Fabrication after Metal1 (M1)

In the most common, semi-compliant split fabrication scenario, the untrusted and trusted foundry can have slightly different BEOL stacks. Split fabrication after M1 can even allow for the integration of a state-of-the-art untrusted FEOL with a more relaxed but trusted BEOL. As conventional SoC design methodologies are developed for a specific foundry, there is a need to modify design flows to cater to split fabrication. The critical components of an ASIC/SoC design flow are IP blocks and high productivity physical implementation methodologies.

IP blocks. There are two forms of IP blocks, soft IP and hard IP. Soft IP is typically synthesizable as compared to hard IP which is designed and characterized on silicon. Soft IP is typically verifiable and can be modified to meet SoC specifications, thereby not presenting a challenge for split fabrication. In contrast, hard IP is designed by an external vendor and is disclosed to the customer as an "abstract." This enables the attacker in a conventional fabrication setting to collude with the hard IP designer or work by himself to implant trojans in the IP [9]. Consequently, this maliciously modified IP can trigger an IC failure. Hence, to completely secure an IC, it is imperative to secure the hard IP development process. Split fabrication after M1, by definition, forces the on-shore development of all critical hard IP in an SoC, as no hard IP, except standard cells (prior to 90 nm CMOS), can possibly be complete at the M1 layer. Details of designing efficient and obfuscated split fabrication compatible IP is presented in our previous work [10]. It is noteworthy that such on-shore split fabrication compatible hard IP development does not present any cost overhead as hard IP anyway is procured from an external vendor. However, it does require us to modify the custom IC design environment to support split fabricated IP design.

Physical implementation methodology. Physical synthesis design automation technology has been instrumental in dramatically reducing SoC time to market, thereby enabling more applications to be mapped from microprocessors to an efficient ASIC/SoC substrate. For split fabrication to be a practical alternative, it is essential to modify these high productivity physical synthesis methodologies to be split fabrication compatible.

As a first step, we assessed the compatibility of different foundries and converged on the semi-compatible foundry pair of Global Foundries (GF), Singapore as the untrusted foundry to manufacture FEOL devices and M1, and IBM, Burlington as the trusted foundry to complete the IC starting at V1. Table II summarizes the compatibility analysis. In this exercise our objective is not merely to demonstrate the feasibility of split fabrication but also to identify, a) any additional process variation arising from wafer handoff after M1, and, b) any performance, power or area overhead induced by split fabrication when compared to an IC completed fully in an untrusted off-shore foundry. To accomplish these goals we have created a custom and semi-custom split fabrication design flow, described next.

Table II. Compatibility analysis between GF and IBM 130nm.

Compatibility Analysis
Mismatch in M1 and V1 size (still compliant)
Identical 1X (>V1) metals and vias
Mismatch in BEOL stacks
Via array configurations were different
Different 2X metals and vias
Special feature support like MiM Caps differ

B.1. Custom IP Design Flow for Split Fabrication after Metal1 (M1)

For this demonstration we have created a design flow using GF and IBM process design kits (PDKs) to design and verify split fabrication compatible IP (Figure 7). The schematic entry and layout for the custom block are done in the untrusted (UT) PDK. The layout is done in such a manner that layout constructs above the M1 layer have to meet the superset of design rules defined by the trusted and untrusted PDKs. This is done to ensure the same layout can be used, with minimal modifications, to generate the GDS for full flow and split flow comparison. Design rule check (DRC) is run on the layout for layers below V1 in the untrusted PDK. Layout versus schematic (LVS) check is run on the untrusted PDK. After this, in the split GDS processing step, the layout for layers below V1 is exported as usual, forming the untrusted component of split fabrication. Layers above M1 are exported by remapping them to the trusted PDK layer numbers. This remapped layout containing layers above M1 is imported into the trusted PDK and DRC is run to check layout constructs above M1. This layout above M1 forms the trusted component of split fabrication. For the purpose of comparison, we export the full flow layout from the untrusted foundry PDK, after resizing layout shapes for all layers above M1 to pass DRC. Ideally, if split fabrication were to become commercial, this custom IP design could be done using a specific split fabrication PDK and it will not be necessary to create a full flow design.

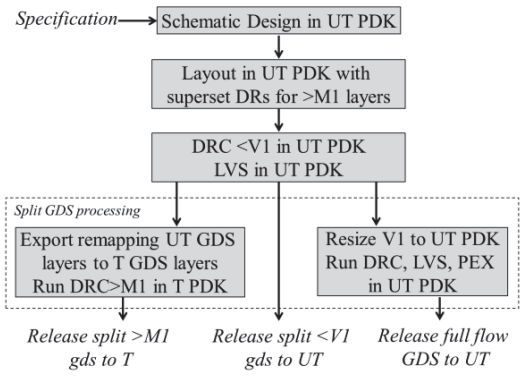


Figure 7. Custom IP split fabrication after Metal1 (M1) design flow.

B.2. ASIC/SoC Design Flow for Split Fabrication after Metal1 (M1)

Split fabrication physical implementation from HDL to GDS uses commercially available high productivity tools, while using split fabrication compatible IP and technology

files (Figure 8). Additional steps are added to the flow to improve obfuscation.

With split fabrication IP created based on the techniques in [10] using the custom design flow in the previous section, the functionally verified hardware description of the design is taken through a usual logic synthesis step to map HDL to logic gates. Physical synthesis, the process of mapping logic gates to layout, typically uses physical abstracts of the IP and a technology file to guide cell placement and auto-routing. The technology (tech) file contains the unit tile information that defines the standard cell placement grid, and design rules for all metal and via layers that will be used by the auto-router to do wiring. To create a split fabrication compatible tech file it might suffice to splice together contents of the tech files from two foundries for the respective layers they manufacture. However, to characterize the split fabrication process by comparing the full flow and split flow designs, we have to create a special BEOL tech file such that it contains a superset of design rules for the untrusted and trusted foundry. Such a tech file is required the creation of placed and routed design that is both full flow and split flow compatible, enabling split fabrication process characterization.

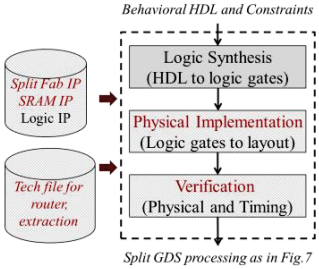


Figure 8. ASIC/SoC split fabrication after M1 design flow. Items in maroon (shaded) are adapted for split fabrication.

As logic gates use most of the M1 routing resources for intra-cell connections, we obfuscate all inter-cell connections from the untrusted foundry by blocking the M1 layer during inter-cell routing. To further improve circuit obfuscation, we add standard cells, instead of filler cells, to fill empty spaces in the physically synthesized layout [14]. This ensures that the attacker in the foundry cannot:

- distinguish between a real cell and a filler cell.
- gather any information about the design by looking at cell statistics.
- insert hardware trojan circuits as there is no empty space.

Finally, the layout from the physical synthesis tool is exported and the GDS splitting steps discussed in Section III.B.1 are carried out. While exporting layout GDS to the untrusted foundry, the designer has to ensure that:

- no text and label shapes are exported.
- no design names and library names get exported, as library names are encoded in the GDS stream [15].

These additional steps and changes to the conventional physical synthesis flow can be used to create secure and high performance ASIC/SoCs efficiently. Even though we illustrated the split fabrication design flow using a 130nm foundry pair, the approach is applicable to any technology node, with ongoing designs in 65nm and 28nm CMOS.

Discussion. As it may be already apparent to a physical implementation expert, several physical synthesis transforms can be deployed to add more layers of circuit obfuscation, occasionally at the cost of performance, power or area. For instance, using an assorted set of standard cells, using non-conventional placement algorithms and intentional layout randomization are just a few techniques a designer can use during physical implementation to further obfuscate their design at a reasonable design cost.

IV. Results And Discussion

Results presented, unless mentioned otherwise, are from 130nm test chip measurements using Global foundries (GF), Singapore as the offshore foundry and IBM, Burlington as the on-shore trusted foundry. Manufacturing the split wafers does not require any additional, expensive process steps or mask-sets compared to full flow wafers, thereby incurring no significant cost overhead. To identify any performance, power or area overhead from split fabrication we analyze two aspects:

- overhead arising from the split fabrication process
- overhead arising from split fabrication design methodology

A. Split Fabrication after Metal1 (M1) Characterization

The objective of this ring oscillator (RO) testchip was to identify any degradation in performance and/or process variation owing to the split fabrication process. A synthesized 32 bit multiplier configured to behave as an RO was used as a design testcase. The design flow in Section III.B was used to ensure that the resulting full flow and split fabrication ROs are almost identical, except for the slightly different via sizes required by GF and IBM, enabling split fabrication after M1 characterization. Measurements from silicon, shown in Figure 9, indicate a negligible difference between full flow and split fabrication test chips. The differences are well within wafer-to-wafer process variation. While we have not tested thousands of instances to conclude on yield, all instances of chips we have tested were fully functional (Figure 9).

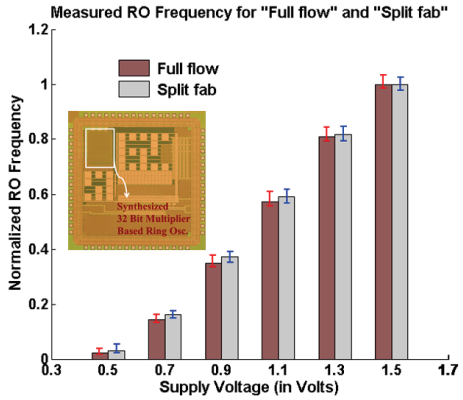


Figure 9. Measurements from RO-testchip in 130nm CMOS show no noticeable impact on performance or process variation owing to split fabrication after M1. Error bar shows minimum and maximum measured values from 10 chips.

We designed another Imaging-testchip containing an ASIC/SoC sub-block used in high performance imaging, built with standard cells and split fabrication compatible SRAMs. Measurement results from the block are similar to the RO-testchip as shown in Figure 10, illustrating the readiness of split fabrication after M1 for industrial scale SoC design with split fabrication compatible embedded memory and logic IP.

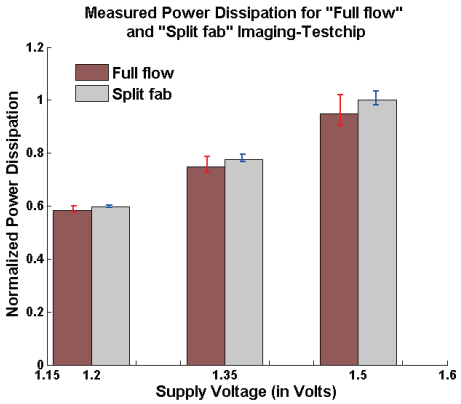


Figure 10. Measurements from Imaging-testchip (with SRAM and logic IP) illustrate the readiness of split fabrication after M1 to undertake SoC designs. Error bar shows minimum and maximum values from 4 chips.

B. Split Fabrication after Metal1 (M1) Overhead Evaluation

We next quantify any performance overhead arising from the split fabrication design methodology. We create a set of baseline designs using standard physical implementation reference flows in the GF 130nm process. These designs were created without consideration of split fabrication. Next, we compare the performance of the same designs created using the split fabrication after M1 design flow in 130nm CMOS. For the same physical area, we identify any performance overhead introduced by pursuing the split fabrication design methodology. Results shown in Table III indicate no appreciable design efficiency overhead to pursuing a split flow compared to full flow, for the chosen untrusted and trusted foundry pair at 130nm. It is worth noting that the exact design overhead depends on the specific untrusted and trusted foundry pair, which can be minimized by doing a compatibility analysis as described in Section III.

TABLE III. Security offered by split fabrication after Metal1 (M1) and its associated performance overhead

Design	#Gates	Split Fab Overhead	Security (W)
MULT32	3852	+10%	3852! → ∞
DES64	3975	-12%	3975! → ∞
S15850	1624	-2%	1624! → ∞
S35932	4397	-5%	4397! → ∞
S38584	5673	+3%	5673! → ∞

C. Split Fabrication after Metal1 (M1) Security

For a set of design blocks listed in Table III, we computed the number of possible connections (W) between logic gates using the expression described in Section II.B. It is clear that the attacker at the untrusted foundry, without additional information, cannot reverse engineer the functionality of the circuit. In the event that the attacker at the untrusted foundry, by illegal means, secures information about the complete design and succeeds in implanting a FEOL trojan, then we leverage split fabrication to exhaustively test and detect such trojans using a specialized test-only BEOL on select sacrificial dies [16].

V. Conclusion

Targeted hardware trojans can be more effective than software viruses, essentially crippling defense and infrastructure installations. The escalating cost of manufacturing that creates more advanced technologies off-shore results in significant hardware security concerns. To provide DoD designs with access to state-of-the-art semiconductor manufacturing offshore while simultaneously guaranteeing exceptional security, we proposed split fabrication after M1. We demonstrate that split fabrication after M1 obfuscates the underlying design intent by hiding all gate connections. To identify any overhead arising from split fabrication we have designed split fabrication testchips in 130nm CMOS using a split fabrication compatible design methodology. Measurements from testchips indicate that split fabricated ICs have negligible performance, power, area overhead or process variability when compared to ICs built entirely at the untrusted foundry, thereby, proving the efficacy of the split fabrication after M1 technique to obfuscate, and consequently secure mission critical ICs.

Acknowledgement

This work was supported in part by the Intelligence Advanced Research Program Agency and Space and Naval Warfare Systems Center Pacific under Contract No. N66001-12-C-2008, Program Manager Dennis Polla.

References

[1] M. Potkonjak et al., "Hardware Trojan horse detection using gate-level characterization," DAC, July 2009.
[2] S. Skorobogatov et al., "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip," CHES, Sep. 2012.
[3] "Trusted access program office", https://www.tapoffice.org/ .
[4] S. Heck et al., "Creating value in the semiconductor industry," McKinsey & Company, Autumn 2011.
[5] R. Jarvis et al., "Split manufacturing method for advanced semiconductor circuits," US Patent no. 7195931, 2004.
[6] J. Rajendran et al., "Is split manufacturing secure?," DATE, March 2013.
[7] F. Imeson et al., "Securing computer hardware using 3D integrated circuit (IC) technology and split manufacturing for obfuscation," USENIX SEC, August 2013.
[8] G. Northrop, "Design Technology Co-Optimization in Technology Definition for 22nm and Beyond," VLSI-Technology, June, 2011.
[9] M. Rostami et al., "Hardware Security: Threat Models and Metrics," ICCAD, Nov, 2013.
[10] K. Vaidyanathan et al., "Efficient and Secure Intellectual Property (IP) Design for Split Fabrication," HOST, May 2014.
[11] R. Torrance et al., "Reverse Engineering in the Semiconductor Industry," CICC, Sep, 2007.
[12] "International Roadmap of Semiconductors", http://www.itrs.net/ .
[13] "IBM Common Platform", http://www.commonplatform.com/ .
[14] L. Chow et al., "Camouflaging a standard based integrated circuit," US Patent no. 8151235, April 2012.
[15] S. DiBartolomeo et al., "All About Calma's GDSII Stream Format," http://www.artwork.com/gdsii/gdsii/index.htm
[16] K. Vaidyanathan et al., "Detecting Reliability Attacks during Split Fabrication using Test-only BEOL Stack," DAC, June 2014.