Split Manufacturing in Radio-Frequency Designs

Yu Bi, *Student Member, IEEE,* Jiann-Shiun Yuan, *Senior Member, IEEE,* and Yier Jin, *Member, IEEE*
Department of Electrical Engineering and Computer Science, University of Central Florida

***Abstract*—With the globalization of integrated circuit (IC) design flow and the outsourcing of chip fabrication service, intellectual property (IP) piracy and malicious logic insertion become main security threats to tamper hardware infrastructures. While most of the protection methods are dedicated for digital circuits, we try to protect radio-frequency (RF) designs which are more likely to be IP piracy victims. For the first time, we apply the split manufacturing method in RF circuit protection. Three different implementation cases are introduced for security and design overhead tradeoffs, i.e., the removal of the top metal layer, the removal of the top two metal layers, and the design obfuscation dedicated for RF circuits. We also develop a quantitative security evaluation method to measure the protection level of RF designs under split manufacturing. Finally, a class-AB power amplifier is used for demonstration through which we prove that: 1) the removal of top metal layer or top two metal layers can provide high-level protection for RF circuits with lower request to the domestic foundries; 2) design obfuscation method provides highest level of circuit protection, though at the cost of design overhead; 3) split manufacturing is more suitable to RF designs than to the digital circuits and it can effectively improve hardware tamper resistance and reduce IP piracy in the untrusted off-shore foundries.**

***Keywords*-Hardware Tamper Resistance, Hardware Trust, IP Piracy, Power Amplifier, RF Circuits, Split Manufacturing**

I. Introduction

The globalization of integrated circuits (IC) supply chain, especially the outsourcing of chip fabrication and the integration of third-party intellectual property (IP) cores, breeds security concerns and makes it easier to compromise the once trusted IC development process [1], [2]. Among all security threats, malicious logic insertions (aka hardware Trojan attacks) and IC piracy are of the most critical security threats that the US government is facing after more and more domestic IC companies go fabless. Following the trend of a growth of merchant foundry industry, fabless IC design houses can have access to reasonably-priced advanced-process capacity without the need for huge capital expenditure (the cost of developing a semiconductor foundry will be over $5.0 billion by 2015 [3]). The reduced fabrication cost, at the same time, sacrifices the design security and leaves all IC designs in the hands of foundry. The International Chamber of Commerce (ICC) stated in their 2011 report that the total global economic and social impacts of counterfeit and pirated products are as much as $775 billion every year.

For this reason, both governmental agencies and industrial companies are looking for a balance between fabrication cost and design security to prevent foundry from learning the design details of the submitted design layout. In order to address such threats, various hardware Trojan detection methods and hardware metering methods have been developed [4]–[7]. Among all these approaches, design obfuscation and camouflaging are candidates but both methods require the modification to the original circuits which may cause performance overhead. Intelligence Advanced Research Projects Activity (IARPA) proposed a new methodology, called split manufacturing, which only adds trivial efforts to IC designers but can effectively prevent IC piracy [8]. The key idea of split manufacturing is to protect circuit/system designs by dividing the manufacturing chips into Front-End-of-Line (FEOL) consisting of transistor layers to be fabricated by offshore foundries and Back-End-of-Line (BEOL) consisting of metallizations to be fabricated by trusted domestic facilities. Through this divided fabrication procedure, the design intention is not fully disclosed to the FEOL foundry. Even though the concept is straightforward, a successful implementation requires further research on various aspects, especially the balance between cost and security when the designer splits the layout into FEOL and BEOL. Analytical and experimental results have already been presented in digital circuits [9]–[13]. However, the analog/RF designs are rarely discussed using split manufacturing even though analog/RF circuits are more likely to be IP piracy victims than their digital counterparts.

In fact, the fundamental difference between digital design flow and RF design process has already raised the concern whether it is still applicable to apply split manufacturing in RF design. A deep look into both design flows proves us that it would be more suitable to apply split manufacturing in RF circuits than in digital circuits because of the unique functionality metal layers play in RF designs: 1) Metal layers are solely used as interconnections between gates and modules in digital circuits while in RF circuits, metal layers are also used to build functional blocks (e.g., inductors are often located on top metal layer; capacitors are built in upper level metal layers); 2) While metal layers are abstracted as wire connections in digital designs, wire length and wire direction are both functional parameters in RF designs. Therefore, a foundry fabricating the FEOL part of digital circuits may face a mathematical problem with finite solutions in order to recover the whole functionality of the design[1]. On the other hand, the foundry of RF FEOL needs to explore an infinite solution space to recover the RF design.

Based on the above discussion, it becomes obvious that the split manufacturing should be more effective to protect RF circuits from IP piracy. To assess our claim, analytical calculation and experimental demonstration are performed in this paper to solidify our findings and to push the territory of split manufacturing to cover all kinds of circuit designs.The rest of the paper is organized as follows: Section II introduces

[1]Note that the possible solution space could be large given large amount of standard cells in digital circuits. In fact, this is the key criterion to evaluate the security level of split manufacturing method in digital circuits.

the state-of-the-art split manufacturing practices. Section III presents the RF design flow. A detailed analytical analysis of applying split manufacturing in RF designs is presented in Section IV. Finally, the conclusions are drawn in Section V.

II. Split Manufacturing in Digital Domain

The concept of split manufacturing was officially proposed by IARPA through the Trusted Integrated Chips (TIC) program. The new program aims to develop and demonstrate new split manufacturing to chip fabrication where security and intellectual property protection can be assured [8]. Since then, a few embodiments of split manufacturing in digital circuits have been proposed. Imeson et al. proposed a method by applying 3D integration technology in split fabrication. Using a through silicon via (TSV), they came up with a security algorithm from graph problem to obfuscate the circuit by lifting certain wires to a trusted tier [10]. Rajendran et al. examined a split fabrication after metal3 layer, where digital benchmark circuits are separated into several partitions without interconnections [9]. Since the connections within each gate are mostly located in metal1 and metal2 layers which are known to the FEOL foundry, they further proposed a fault-analysis based pin swapping algorithm to defend the common proximity attacks. More recently, Vaidyanathan et al. investigated feasibility of split fabrication after metal1 layer so that untrusted foundries only have the information of basic gate-level blocks [11]. A similar technique is then applied to digital/analog IP designs [12]. A defense strategy against recognition attacks on IPs and an obfuscation method were both proposed as well as experimental demonstrations on a 1KB SRAM and a 14-bit current steering digital-to-analog converter (DAC). Hill et al. [13] described a comparative study of an asynchronous FPGA manufactured in both a standard process and a split manufacturing process. Compared to the standard process, split manufacturing process suffers penalties either on operating frequency or on the energy consumption.

III. RF Design Flow

Thanks to the advanced EDA tools for RF circuit designs and the development of RF design kits, RF engineers become more productive than ever before. Nevertheless, a typical RF design still involves heavy work of design fine-tuning and designers' experience plays a critical role here [14], [15]. Figure 1 shows the steps among a modern RF design flow.

From Figure 1 we can learn that steps I-III are the preparation of the RF circuit specification. Taking a power amplifier as an example, the defined specification will include design information such as the delivered output power, the amount of circuit stages, the operation class, etc. Different from digital designs where the specification will be strictly followed, however, the specification for RF circuits only serves as a guideline as it often happens that the performance of the final design deviates from the original settings (experienced RF engineers may be able to narrow the performance gap).

Guided by the specification, the circuit schematic will be designed, simulated and optimized. The optimized schematic will then guide the work of layout design and post-layout

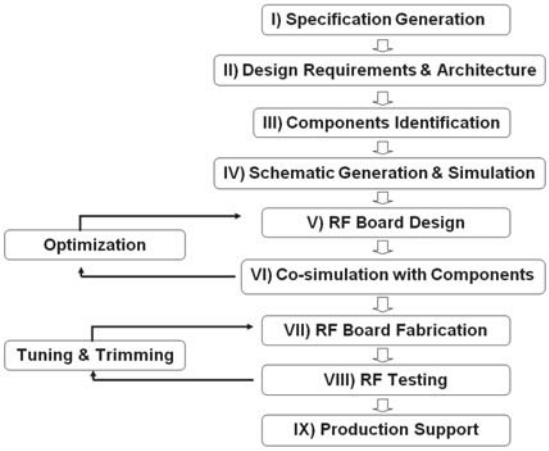


Fig. 1: Standard RF circuit design flow

simulation. All physical-level parameters come into the map during the layout design and post-layout simulation such as parasitic capacitors, wire resistance, etc. For RF circuits, the parasitic components can significantly affect the design performance and significantly deviate the circuit performance from the schematic level simulation. Therefore, the large portion of design time will be spent in layout optimization and circuit fine-tuning, even for experienced designers. If the circuit passes the post-layout simulation, it will be sent to foundry for fabrication and for post-fabrication testing. Even though current foundries embrace advanced technology and delicate equipments, the parasitics introduced by fabrication process remain a problem, i.e., unpredictable parasitic resistance and capacitance during the fabrication would both affect circuit functionality and performance. A fabricated RFIC circuit may not work properly which raises the demand of further tuning and trimming. To lower the fabrication cost and to increase the yield rate, techniques of post-fabrication calibration are used in modern RF designs, e.g., knob adjustments and Transverse Electro-Magnetic (TEM) cell.

IV. Split Manufacturing in RF Circuits

As we mentioned earlier, the removal of metal layers in RF circuits will not just hide the interconnections between circuit components but also eliminate the passive components which are built in metal layers. Since a typical RF circuit only includes very few transistors and other passive components, the recovery of interconnections between these components will not be a difficult task. Rather, to derive the missing passive components and their sizes would be the main advantage to apply split manufacturing in RF designs. For the same reason, the difficulty level for attackers with the FEOL at hand to recover the passive components and to guess the sizes of these passive components will be the key criteria to assess the effectiveness of split manufacturing application in RF designs.

Compared to digital split fabrication [9] where the proximity attack dominates the security analysis, routing and mapping are no longer an issue for RF circuits. Furthermore, the recognition attack mechanism used in [12] cannot explain accurately the issue with RF split fabrication. To better guide

the implementation of split manufacturing in RF circuits and to balance between the security level and design efforts, we propose three approaches/scenarios to perform the RF split fabrication:

- Scenario I: Remove only the top metal layer from the layers to generate FEOL. Since the inductors are often located in the top layer, the FEOL foundry does not have the information of interconnections through top metal layer as well as the inductor locations and sizes.
- Scenario II: Remove the top and the second to the top metal layers. In this scenario, two upper metal layers are removed so that both inductors and capacitors are missing from the FEOL layout because the capacitors are often built through the top two metal layers.
- Scenario III: Design obfuscation. For RF designs, inductors are always located in metal rings and lower metal layers will be removed inside the rings for performance optimization. Therefore, the rings themselves, which contain multiple metal layers, would indicate positions and approximate sizes of inductors. Similarly, the lower metal layers will not be used where capacitors are located. Therefore, attackers in both scenarios I and II may learn the precise positions of the removed inductors/capacitors and may even further estimate their sizes. To further increase the security level but still to avoid performance overhead, we propose an obfuscation technique during the design phase to insert non-functional rings and to create empty zones in the original design. Using this method, it becomes more difficult for attackers to pin down the location, the count, and the sizes of passive components.

For the demonstration purpose, the TSMC 0.18 μm technology supporting six metal layers is used. In experimental demonstrations, the scenario I indicates the removal of metal6 layers. Similarly, scenario II means the removal of metal5 and metal6 layers. Scenario III follows the same rules that new rings and empty zones are removed from the metal layers metal1 to metal4. Note that the proposed three scenarios can be applied to any other process technology with the adjustment of available metal layers.

A. Split Manufacturing on Class-AB Power Amplifier

To demonstrate all three application scenarios as well as their security levels, an one-stage single-transistor class-AB power amplifier is investigated as our first example where we assume that the inductor is using metal6 layer and the capacitors are using metal5 and metal6 layers [16].

The class-AB power amplifier (see Figure 2 for detailed schematic) works at 5.8 GHz with a low supply voltage of 1.9 V. It is designed to deliver 19.8 dBm output power and 28.1% power-added efficiency.

1) Scenario I: Removal of Metal6 (Inductors): Since metal6 is removed from the FEOL, the schematic of the class-AB power amplifier, showed in Figure 3, is missing all inductor information. Although the attackers can easily recover the count and the locations of all inductors, they do not know the exact sizes and the values of the inductors. More precisely, the attackers can learn that 3 inductors are used in the design

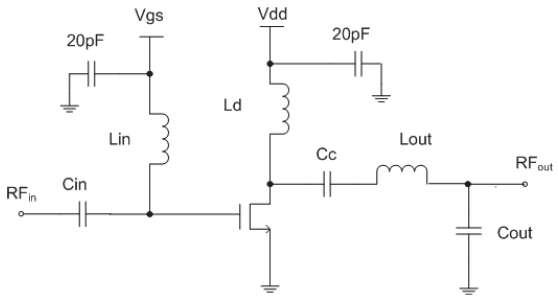


Fig. 2: Schematic of a class-AB power amplifier

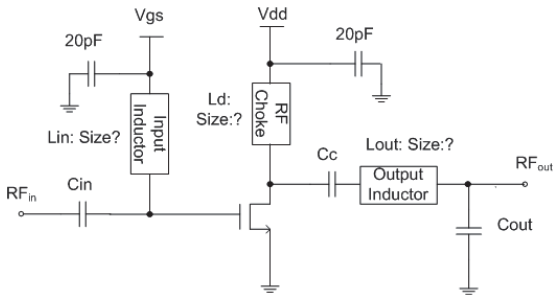
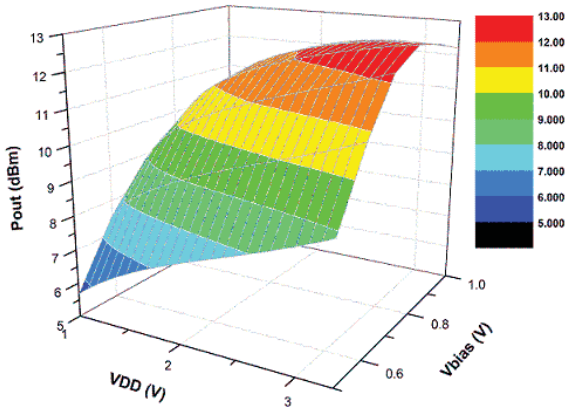


Fig. 3: A class-AB power amplifier with metal6 removed (missing inductors)

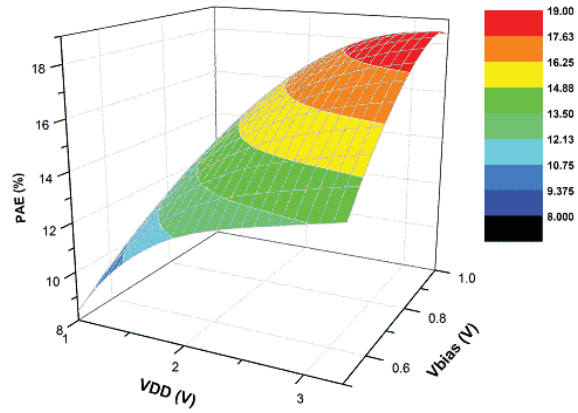
through the inductor rings. They can also extract the values for all other components. Therefore, the attackers with the FEOL of the power amplifier at hand can easily guess the general functionality of the entire design. But a detailed specification including the the supply voltage and the operating frequency remains unknown. As a result, the task for attackers to recover the entire circuit is not as simple as sweeping all possible inductor values. As we emphasized earlier, we assume that the attackers are also experienced RF designers so they would also apply the analytical calculation and other parameters from the known components in order to derive the inductor values. The procedure to recover the whole circuit from the known FEOL by attackers is described in the following steps (Note that the IP piracy cost is directly related to the complexity of the these steps):

Step 1: In the first step, the attackers will try to find out the operating conditions such as bias voltage, supply voltage and operating frequency, which can significantly shift the power amplifier performance. Since the untrusted foundry is also the provider of the fabrication process (in our case, we are using the 0.18 μm technology), the attackers should be aware of the available supply voltage for this technology (from 1 to 3.3 V). The attackers should at least try 23 different supply voltages if a step size of 0.1 V is chosen[2]. In terms of gate biasing, the reasonable range for a power amplifier varies from 0.4 to 1 V but it is not necessary that all designs follow this setting (e.g., an exception would be presented in the experimentation section). Hence, using 0.05 V as a voltage sweeping step, the gate biasing can have at least 13 different cases for attackers to choose. Meanwhile, the operating frequency still remains a puzzle to attackers, which acts as an imperative role in

[2]They may try more supply voltages with smaller voltage step size in order to get more accurate simulation results.

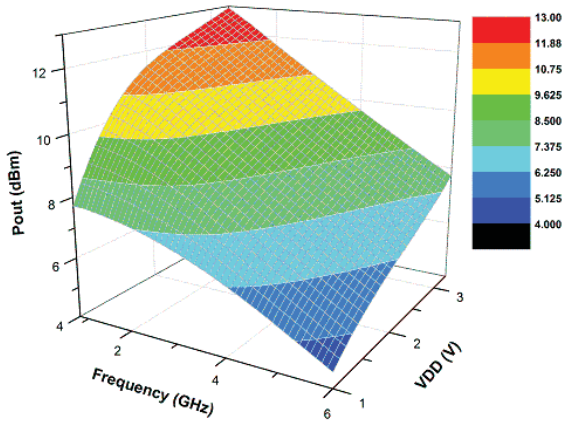


(a)

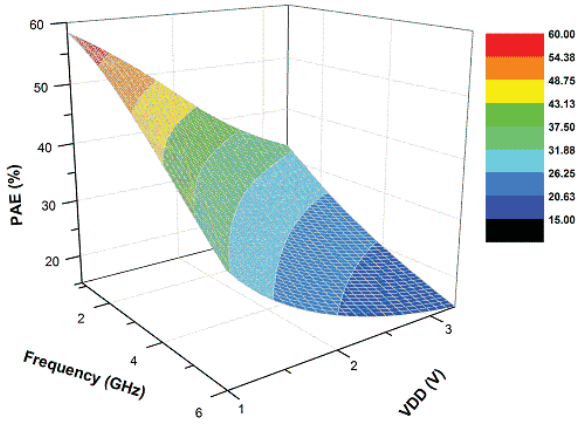


(b)

Fig. 4: (a) Supply voltage and gate biasing versus output power (b) Supply voltage and gate biasing versus power-added efficiency



(a)



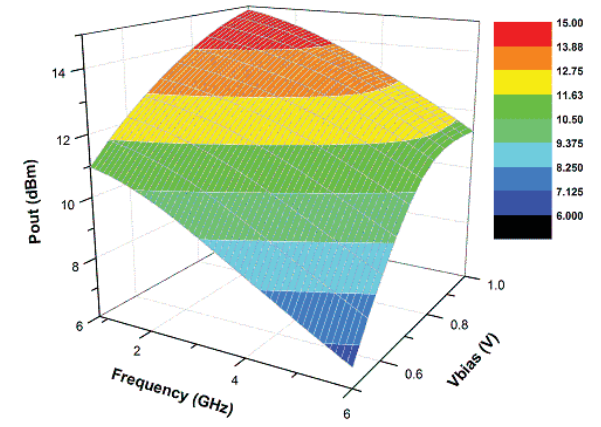
(b)

Fig. 5: (a) Supply voltage and frequency versus output power (b) Supply voltage and frequency versus power-added efficiency

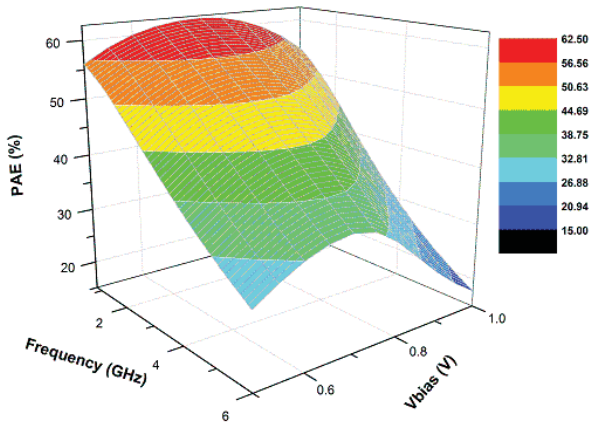
RF design. The attackers may narrow down the spectrum by assuming this example design works in the commercial communication protocol range, which is basically from 0.8 to 6 GHz. Again, the design may or may not take the communication frequency as its operating frequency, because the attackers are not aware if this layout works for some specific applications, either military or scientific confidentiality. Under this assumption, it comes to a group of 53 possible values if a step of 0.1 GHz is selected.

With all these possible cases available, the attackers will then run simulation to recover the original design by choosing the best performance of output power and power-added efficiency. For example, Figures 4 (a) and (b) show the case that the actual supply voltage and gate bias, namely 1.9 and 1 V, do not deliver the best output yields. Similarly, Figures 5 (a) and (b) show that the maximum output power is not coincident with the maximum power-added efficiency. Since this power amplifier is designed for the low-power application, the specification defines the operating frequency to be 5.8 GHz; however, Figure 5 shows that the defined operating frequency is located in the middle level of the overall performance. Clearly attackers cannot recover the original design if the optimized parameter settings are chosen. Figures 6 (a) and (b) reflects the relationship of circuit performance versus frequency and gate bias. As you can find from the figure, the actual values for frequency and gate bias, 5.8 GHz and 1 V, are located in the low performance area. Therefore, If the attackers follow any of the recovery process through Figures 4, 5 and 6, they cannot find the correct settings. Note that these sample testing process only represents a small fraction of the overall testing space meaning that it will take significant amount of time for attackers to fully simulate the design and collect the original design parameters even for a simple RF circuit.

Step 2: In the second step, we assume that the attackers have chosen the correct operating conditions for the power amplifier, they then need to set the biasing conditions to precisely recover the inductor values. Following a general RF design methodology, the experienced attackers will sweep the RF choke L_d and the input inductor L_{in} by a reasonable range,

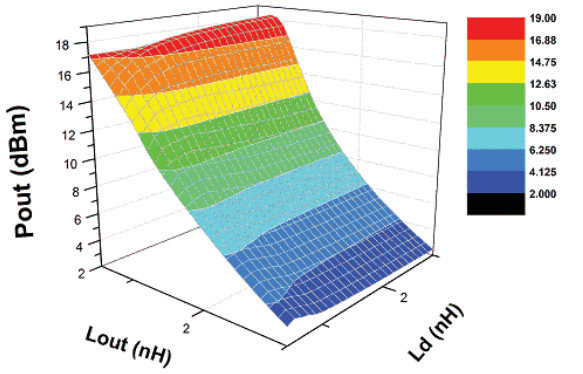


(a)

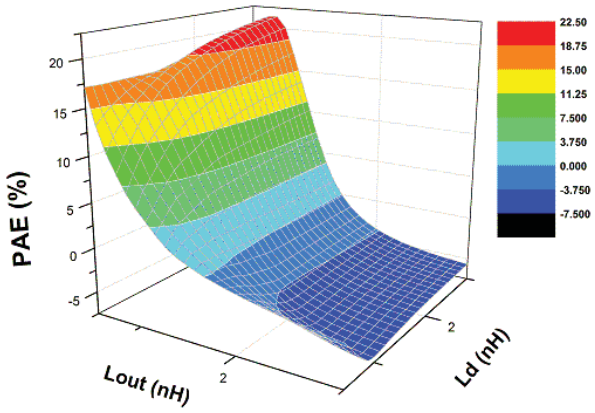


(b)

Fig. 6: (a) Gate biasing and frequency versus output power (b) Gate biasing and frequency versus power-added efficiency



(a)



(b)

Fig. 7: (a) Output inductor and RF choke versus output power (b) Output inductor and RF choke versus power-added efficiency

which is from 0.5 to 3 nH in the 0.18 μm technology, to check the input reflection coefficient S11 and to further guess the frequency range, rather than a random sweeping on different frequencies. Based on the simulation results, the attackers will probably learn the circuit working frequency between 4 and 7 GHz. The derived frequency range helps to narrow the possible range of the input inductor but, still, the attackers need to select the inductor value from 4 to 7 GHz for the overall performance simulation. The attackers will then sweep the RF choke L_d and the output inductor L_{out} to optimize the output performance and the matching network. The simulation results will be meaningless if a wrong input inductor value is chosen.

Figure 7 illustrates the output results that vary with respect to the RF choke and the output inductor. The actual values for the RF choke and the output inductor are 963 and 670 pH, respectively. However, from Figure 7 we can see that both values produce good but not the best performance. It is possible that the attackers only aim to the best performance so they may choose inductor values from the wrong rage.

2) Scenario II: Removal of Metal5 and Metal6 (Capacitors and Inductors): In this case, both inductors and capacitors are not available to the untrusted foundry because of the removal of metal5 and metal6 layers from the FEOL. The missing capacitors add additional uncertainty for attackers to recover the whole design. That is, the unknown capacitors add more freedom in the simulation though parameter sweepings and will produces large amounts of combinations of inductors and capacitors. In this case, it is much easier for an experienced attacker to follow the typical power amplifier design procedure to retrieve the missing components.

Step 1: The first step of circuit testing is exactly the same as that in Scenario I.

Step 2: After selecting the operating point, the attacker needs to decide the RF choke inductor and output coupling capacitor. The 0.18 μm technology indicates that the reasonable ranges for inductor and capacitor are 0.5 to 5 nH and 1 to 10 pF, respectively. Using a sweeping step of 0.1 nH and 0.1 pF for inductors and capacitors, respectively, the attackers will come up with a total of 45 possible values for inductors and

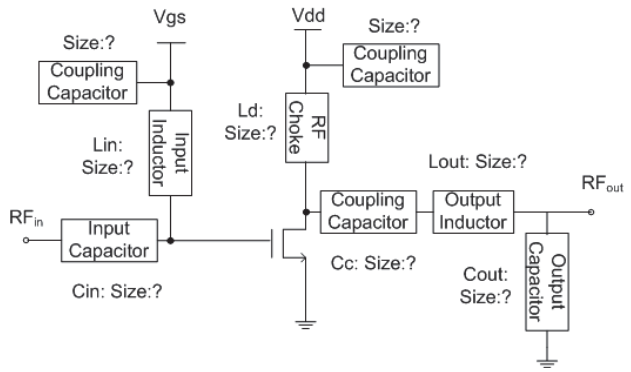


Fig. 8: Schematic of class-AB power amplifier without top two metal layers (missing inductors and capacitors)

90 possible values for capacitors[3]. Figure 9 shows the overall circuit performance when the values of the choke inductor and the output capacitor are changing. The figure helps attackers to recover the correct values of both components.

Step 3: After selecting the RF choke and coupling capacitor from various combinations, the attackers need to do the output matching to achieve a matched 50 Ω output. The RF designers often perform output matching through load pull simulation, which provides the designers a bunch of matching combinations to choose from. Advanced EDA tools can help synthesize the maximum output power and power-added efficiency as well as further reflect the impedance of the optimal points. After choosing the impedance, the designers can use the Smith chart to recover the output matching network. Because of the simple structure of the single transistor power amplifier, the output matching network only includes one inductor and one capacitor. Relying on the load pull simulation, the attackers can retrieve four possible matching networks as showed in Figure 10.

The possible topologies cover L-type (Figures 10(a) and (b)), Π-type (Figure 10(c)) and T-type (Figure 10(d)), which are all basic network topology in RF design. All component values for each topology are located in reasonable design ranges; however, only the first two networks are possible given the number of passive components.

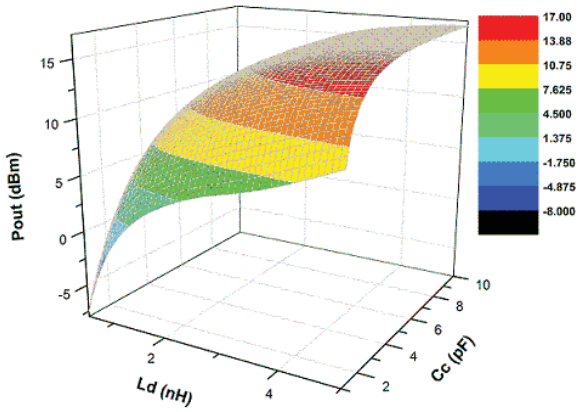
Step 4: After the load pull simulation, the attackers need to use the source pull simulation to recover the input matching network, which follows a similar procedure to the load pull simulation.

Step 5: The final tuning is necessary for attackers to adjust the performance before all circuit parameters are recovered.

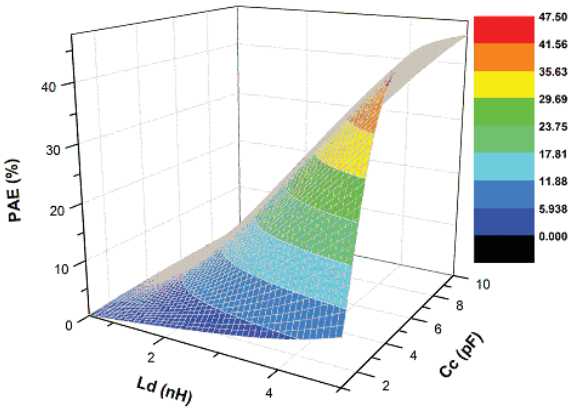
3) Scenario III: Obfuscation Techniques: Although various obfuscation techniques can be applied that increase the difficulty for attackers to recover the original circuit, in order to balance the performance impact and lower the design cost only two obfuscation methods are demonstrated in this paper. Those two methods add 1) extra block space where the capacitors/inductors are located and 2) dummy cells to mislead the attackers into incorrect simulations.

To avoid high frequency signals interfering with each

[3]Note that the range of inductor shifts from 0.5 to 5 nH rather than from 0.5 to 3 nH due to the fact that capacitor values are unknown in Scenario II.



(a)



(b)

Fig. 9: (a) RF choke and output coupling versus output power (b) RF choke and output coupling versus power-added efficiency

other, the lower level metals are not used where the inductors/capacitors are located. The existence of these empty areas may reveal to the attackers the approximate sizes of the inductors/capacitors which can lead to the recovery of the original design. To address this issue and to further increase the difficulty of RF IP piracy, we propose an obfuscation technique to deliberately increase passive component area. This will have the effect of lowering the correlation between the area of each inductor/capacitor and their value.

A second method will also be applied which includes unused empty blocks in the original design so that the attackers cannot find the correct circuit structure. Those extra blocks can be located either in the input or the output side. For example, the attackers will only select L-types output matching networks from Figures 10(a) and (b), but they will also consider other topologies if two empty blocks are inserted.

Different from the IP protection scenarios I and II, the obfuscation technique in scenario III requires modifying the original layout. The RF design performance will be affected due to the sensitivity of layout modifications. To address

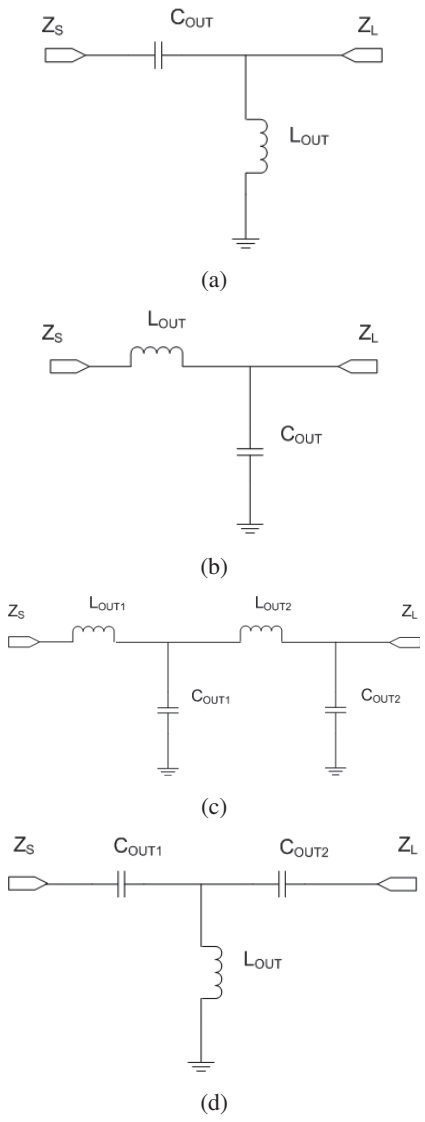


Fig. 10: Four possible output matching network for the class-AB power amplifier

this issue, we suggest a new RF design methodology, called security co-design, which considers security at the early stage of the RF designs by altering some design rules to integrate the obfuscation technique in the design flow.

V. Conclusion

Split manufacturing has presented a new solution against reverse engineering and IP piracy when the IC design flow becomes more globalized. Different from all previous work to apply the split manufacturing in digital circuits, we introduced the first attempt to implement a similar method in RF designs. Quantitative analysis was presented to assess the security protection level for RF designs when the untrusted foundries would like to recover the circuit designs based on part of the circuit layout. To further guide the application of split manufacturing in RF circuits, three different FEOL and BEOL separation and obfuscation methods were introduced. All these methods were demonstrated on one RF circuit: a class-AB power amplifier. The simulation results confirm that the unknown passive components, either inductors or capacitors, along with the missing DC biasing conditions, can raise significant uncertainty for the attacker to recover the RF circuits. In conclusion, split manufacturing is more effective in RF IC trust than in digital circuit security.

References

[1] "Defense science board (dsb) study on high performance microchip supply," *http://www.cra.org/govaffairs/images/2005-02-HPMS_Report_Final.pdf*, 2005.

[2] S. Adee, "The hunt for the kill switch," *IEEE Spectrum*, vol. 45, no. 5, pp. 34–39, 2008.

[3] Age Yeh, *Trends in the global IC design service market*, DIGITIMES Research, 2012.

[4] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *IEEE Symposium on Security and Privacy*, 2007, pp. 296–310.

[5] Yousra Alkabani and Farinaz Koushanfar, "Active hardware metering for intellectual property protection and security," in *USENIX Security*, 2007, pp. 291–306.

[6] Yier Jin, Bo Yang, and Yiorgos Makris, "Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing," in *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 99–106.

[7] Yu Bi, P.-E. Gaillardon, X.S. Hu, M. Niemier, Jiann-Shiun Yuan, and Yier Jin, "Leveraging emerging technology for hardware security - case study on silicon nanowire fets and graphene symfets," in *Test Symposium (ATS), 2014 IEEE 23rd Asian*, Nov 2014, pp. 342–347.

[8] Intelligence Advanced Research Projects Activity, "Trusted integrated chips (TIC) program," 2011.

[9] Jeyavijayan Rajendran, Ozgur Sinanoglu, and Ramesh Karri, "Is split manufacturing secure?," in *Design, Automation Test in Europe Conference Exhibition (DATE), 2013*, March 2013, pp. 1259–1264.

[10] Frank Imeson, Ariq Emtenan, Siddharth Garg, and Mahesh Tripunitara, "Securing computer hardware using 3d integrated circuit (ic) technology and split manufacturing for obfuscation," in *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, Washington, D.C., 2013, pp. 495–510, USENIX.

[11] Kaushik Vaidyanathan, Bishnu P Das, Ekin Sumbul, Renzhi Liu, and Larry Pileggi, "Building trusted ics using split fabrication," in *Hardware-Oriented Security and Trust (HOST), 2014*, May 2014.

[12] Kaushik Vaidyanathan, Renzhi Liu, Ekin Sumbul, Qiuling Zhu, Franz Franchetti, and Larry Pileggi, "Efficient and secure intellectual property (ip) design with split fabrication," in *Hardware-Oriented Security and Trust (HOST), 2014*, May 2014.

[13] B. Hill, R. Karmazin, C.T.O. Otero, J. Tse, and R. Manohar, "A split-foundry asynchronous fpga," in *Custom Integrated Circuits Conference (CICC), 2013 IEEE*, Sept 2013, pp. 1–4.

[14] J.S. Yuan and Y. Bi, "Process and temperature robust voltage multiplier design for rf energy harvesting," *Microelectronics Reliability*, vol. 55, pp. 107–113, 2015.

[15] J.S. Yuan, Y. Xu, S.D. Yen, Y. Bi, and G.W. Hwang, "Hot carrier injection stress effect on a 65 nm lna at 70 ghz," *Device and Materials Reliability, IEEE Transactions on*, vol. 14, no. 3, pp. 931–934, Sept 2014.

[16] J. Carls, R. Eickhoff, P. Sakalas, S. von der Mark, and S. Wehrli, "Design of a c-band cmos class ab power amplifier for an ultra low supply voltage of 1.9 v," in *Microwave and Optoelectronics Conference, 2007. IMOC 2007. SBMO/IEEE MTT-S International*, Oct 2007, pp. 786–789.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.