# Inspiring Trust in Outsourced Integrated Circuit Fabrication

Siddharth Garg
*Department of Electrical and Computer Engineering, New York University, Brooklyn, New York, 11201*
*Email: sg175@nyu.edu*

***Abstract*—The fabrication of integrated circuits (ICs) is typically outsourced to an external semiconductor foundry to reduce cost. However, this can come at the expense of trust. How can a designer ensure the integrity of the ICs fabricated by an external foundry? The talk will discuss a new approach for inspiring trust in outsourced IC fabrication by complementing the untrusted (outsourced) with an IC fabricated at a low-end but trusted foundry. This approach is referred to as split fabrication. We present two different ways in which split fabrication can be used to enhance security: logic obfuscation and verifiable ASICs.**

## 1. Introduction

Many semiconductor design companies have adopted the *fabless* model, i.e., they outsource integrated circuit (IC) fabrication to one of a few large commercial IC foundries, often located off-shore. However, this comes at the expense of trust. How can the design company trust that the off-shore (untrusted) foundry has not maliciously modified the IC by inserting a hardware backdoor, commonly referred to as a hardware Trojan, in the chip? Hardware Trojan insertion has been recognized as significant threats to the economic viability of outsourced IC fabrication, and to the security of ICs used in critical infrastructure.

One promising approach that addresses these security concerns is split fabrication. The idea is to integrate a trusted IC, fabricated separately at a low-end but secure facility, with the untrusted IC using 2.5D or 3D stacking. The integrity of the trusted chip is guaranteed; however, the transistors on this chip are slow and power hungry. (In fact, as we shall soon see, the trusted IC may only have passive metal wires.) The untrusted chip, on the other hand, is faster and lower power than the trusted chip but potentially modified by the external foundry. The goal is to ensure that the *combination* of the two chips is secure while retaining the speed and power benefits of advanced, outsourced fabrication.

We now discuss two orthogonal ways in which split fabrication can be used to guarantee security. The first is based on logic obfuscation [1] — obfuscating the design of the chip makes it harder for an adversary to modify it in a targeted manner, thus deterring hardware Trojan insertion. The second method aims to detect malicious modifications by verifying the integrity of each computation performed by the untrusted IC using the trusted IC. These so-called verifiable ASICs [2] use powerful cryptographic protocols to provide formal security guarantees under arbitrary misbehaviour of the untrusted IC. The two approaches are briefly described below.

### 1.1. Logic Obfuscation

In split fabrication based logic obfuscation, the IC netlist into multiple "parts", and each part is fabricated at a separate foundry. Intuitively, since no one foundry gets access to the full design of the IC, its ability to either pirate the design or to maliciously modify it in a targeted way is hindered. In its simplest instantiation, an IC is split into two parts. One part has of all the active components (transistors) and some of the interconnect (wires), while the other part has the remaining interconnections. Since the interconnect-only part does not have any active components, it can be fabricated at a low-end trusted foundry. Imeson et al. [1] have proposed a formal, quantitative notion of security for split fabrication based logic obfuscation, and algorithms to maximize security for a given number of "hidden" interconnections on the trusted tier.

### 1.2. Verifiable ASICs

Verifiable ASICs, first proposed by Wahby et al. [2], perform online (in-field) verification of an untrusted ICs computations using a second trusted IC fabricated at a low-end, secure foundry. Verification is performed using interactive proof systems, cryptographic protocols developed that *guarantee* that the likelihood of missed detection (i.e., not flagging an incorrect computation) is below a desired (infinitesimally small) value. Compared to prior work on hardware Trojan detection, the verifiable ASICs approach is the only one that provides formal (mathematical) security guarantees under arbitrary Trojan misbehaviour. Wahby et al. [2] have shown that, for certain types of computations, this approach can outperform the alternative — implementing the desired functionality at the low-end, secure foundry.

## References

[1] 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)*, pages 495–510, 2013.

[2] R. S. Wahby, M. Howald, S. Garg, A. Shelat, and M. Walfish. Verifiable asics. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 759–778, May 2016.

978-3-9815370-8-6/17/$31.00 