# Live Demonstration: Securing Wireless ICs Against Supply Chain Attacks Using SyncLock

Alán Rodrigo Díaz Rizo, Hassan Aboushady, Haralampos-G. Stratigopoulos

# Live Demonstration: Securing Wireless ICs Against Supply Chain Attacks Using *SyncLock*

Alán Rodrigo Díaz-Rizo, Hassan Aboushady, Haralampos-G. Stratigopoulos
Sorbonne Université, CNRS, LIP6, Paris, France

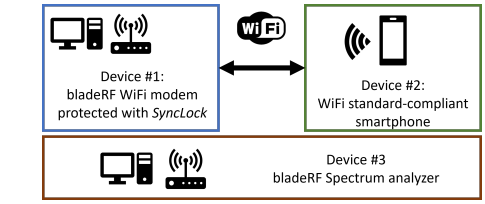
***Abstract*—The globalization of the Integrated Circuit (IC) supply chain has given rise to several hardware security and trust threats. Especially, IC piracy and counterfeiting are significant preoccupations for designers. This demonstration shows how to secure a wireless IC against such threats. The case study is an open-source IEEE 802.11 WiFi modem implemented on hardware using a Software Defined Radio (SDR) bladeRF board. The modem is secured with synchronization-based locking (*SyncLock*), a state-of-the-art locking scheme for RF transceivers. *SyncLock* disables the wireless communication between the modem and a WiFi-compliant receiver unless the correct secret key is loaded onto the modem.**

## I. Introduction

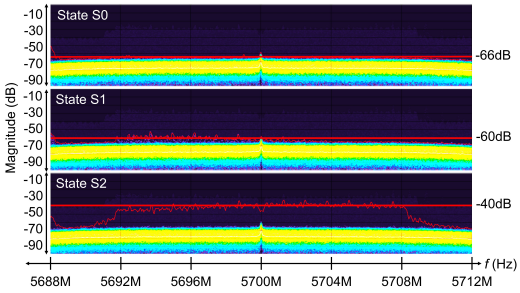
IC piracy and counterfeiting is a major preoccupation nowadays for designers. The ownership of the IC may be lost in seconds while the design is a multi-person effort spanning several months or years. Adversaries can be a third-party that purchases a licence to use the design as an IP block into a larger design, i.e., a system-on-chip (SoC), a foundry that receives the blueprint of the chip for fabrication or a reverse-engineer. IC ownership protection is typically a contractual confidentiality agreement between the two parties often reinforced by security audits. However, this approach does not offer strong security guarantees. A rigorous security approach is locking offering end-to-end protection against any adversary in the supply chain. Locking embeds and mingles into the original design a circuit, called lock mechanism, that is controlled by a secret key, which is typically a binary string. For the correct key, the lock mechanism is transparent and the intended functionality is restored, while for an incorrect key the functionality is corrupted. For wireless ICs comprising an RF transceiver, two approaches have been proposed, namely logic locking (LL) of the digital baseband Physical (PHY) layer [1] and synchronization-based locking (*SyncLock*) [2]. *SyncLock* is a state-of-the-art locking technique specific to RF transceivers. Unless the correct key is used, the receiver is not synchronized with the transmitter, thus the communication link crashes. The advantage of *SyncLock* compared to standard LL is that it is resilient to the various LL counterattacks aiming at extracting the secret key or removing the lock mechanism.

## II. Demonstration Setup

The demonstration employs the Software Defined Radio (SDR) bladeRF board and the open-source *bladeRF-wiphy* project from Nuand to create a WiFi modem. The *bladeRF-wiphy* project is modified to incorporate *SyncLock* into its PHY layer using the methodology described in [2]. The demonstration employs three devices, as illustrated in Fig. 1a. Device #1 is the SDR serving as the WiFi modem secured with *SyncLock*. Device #2 is a smartphone. The demonstration consists of Device #2 trying to establish a connection with Device #1 via WiFi. When the connection is established, Device #2 interacts with Device #1, downloading data from the host computer connected to Device #1. Device #3 is a second SDR that serves as a spectrum analyzer monitoring the central frequency band where Devices #1 and #2 exchange data. Fig. 1b shows the three different monitoring states by Device #3, namely Device #1 is turned off (State S0), Device #1 is turned on but has an incorrect key loaded (State S1), and Device #1 is turned on and has the correct key loaded (State S2).




(a) Demonstration setup.




(b) Device #3 output.

Fig. 1: *SyncLock* demonstration.

## III. Visitor Experience

Visitors will learn the inner workings of the *SyncLock* locking technique for RF transceivers and will interact with the WiFi modem with their smartphone to witness the effect of locking on the communication link. In essence, locking is demonstrated as a means to prevent unauthorized access to the WiFi modem.

## References

[1] A. R. Díaz-Rizo, J. Leonhard, H. Aboushady, and H. Stratigopoulos, "RF transceiver security against piracy attacks," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 69, no. 7, pp. 3169–3173, Jul. 2022.

[2] A. R. Díaz-Rizo, H. Aboushady, and H.-G. Stratigopoulos, "Anti-piracy design of RF transceivers," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 1, pp. 492–505, Jan. 2023.