Poster: DynUnlock: Unlocking Scan Chains Obfuscated using Dynamic Keys

Nimisha Limaye
New York University
nsl278@nyu.edu

Ozgur Sinanoglu
New York University Abu Dhabi
os22@nyu.edu

***Abstract*—Outsourcing in semiconductor industry opened up venues for faster and cost-effective chip manufacturing. However, this also introduced untrusted entities with malicious intent, to steal intellectual property (IP), overproduce the circuits, insert hardware Trojans, or counterfeit the chips. Recently, a defense is proposed to obfuscate the scan access based on a dynamic key that is initially generated from a secret key but changes in every clock cycle. This defense can be considered as the most rigorous defense among all the scan locking techniques. In this paper, we propose an attack that remodels this defense into one that can be broken by the SAT attack, while we also note that our attack can be adjusted to break other less rigorous (key that is updated less frequently) scan locking techniques as well.**

Poster: DynUnlock: Unlocking Scan Chains Obfuscated using Dynamic Keys

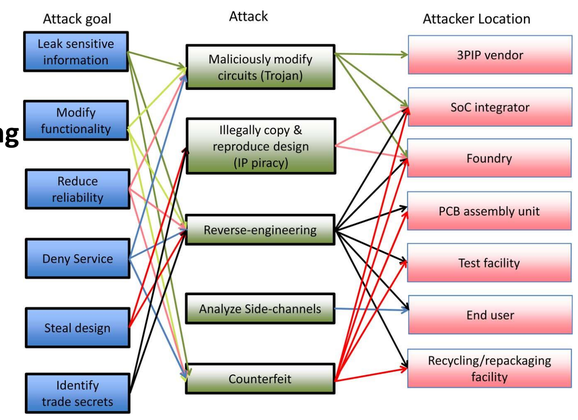
Nimisha Limaye [1] and Ozgur Sinanoglu [2]

Center for Cyber Security [1,2], New York University [1], New York University Abu Dhabi [2]

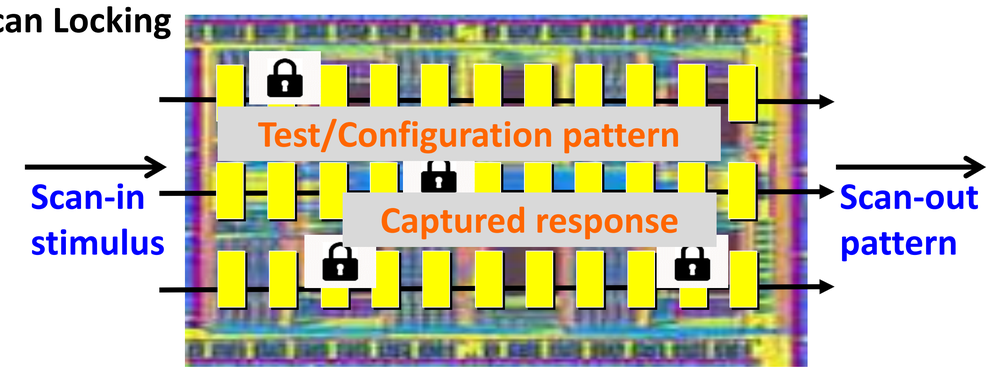
Motivation [1]

To thwart
- Intellectual Property piracy
- integrated circuit counterfeiting and overproduction,
- insertion of hardware Trojans

From
- Untrusted foundry
- Untrusted test facility
- Untrusted end-user



Scan Locking

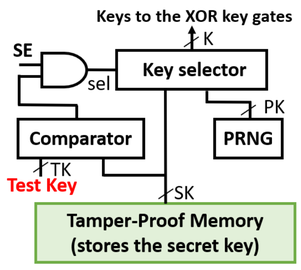


Scan-in stimulus ≠ Test/configuration pattern

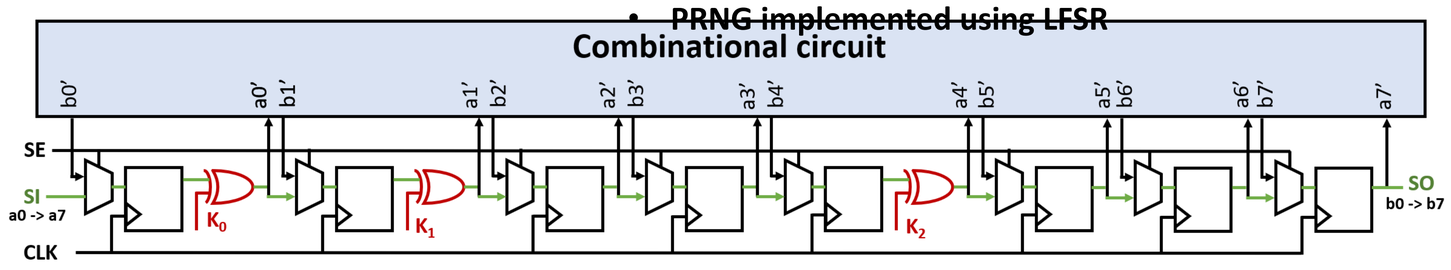
Scan-out pattern ≠ Captured response

Encrypt Flip Flop Dynamic (EFF-Dyn) [2]

- Key is updated every clock cycle
- Most dynamic case of scan locking
- Key from Key selector goes as input to the XOR gates
- PRNG implemented using LFSR



Input to the key-gates at different conditions (K)		
SE = 0	SE = 1	
SK	TK = SK	SK
	TK ≠ SK	PK

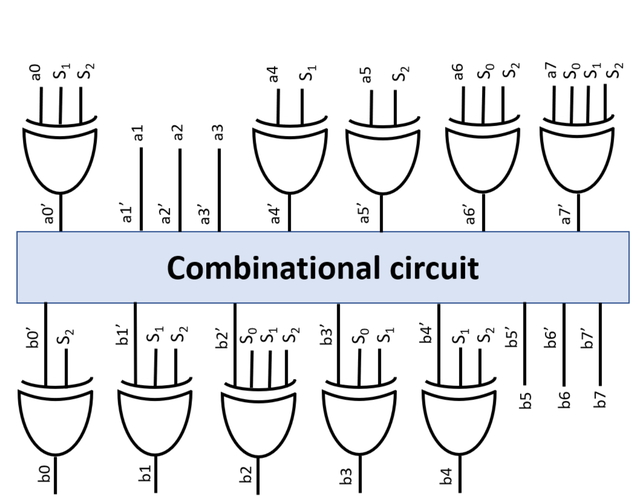


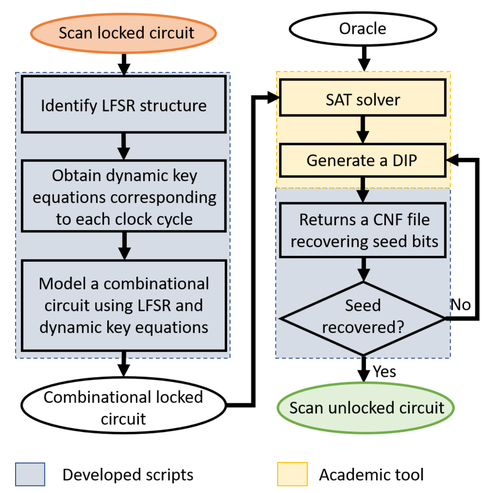
DynUnlock Attack

$$a7' = a7 \oplus k_0^1 \oplus k_1^2 \oplus k_2^5$$
$$\vdots$$
$$a3' = a3 \oplus k_0^5 \oplus k_1^6$$
$$\vdots$$
$$a0' = a0 \oplus k_0^8$$

$$b0 = b0' \oplus k_2^{14} \oplus k_1^{11} \oplus k_0^{10}$$
$$b1 = b1' \oplus k_2^{13} \oplus k_1^{10}$$
$$b2 = b2' \oplus k_2^{12}$$
$$\vdots$$
$$b5 = b5'$$
$$\vdots$$
$$b7 = b7'$$

LFSR round	s_0	s_1	s_2
1	$s_1 \oplus s_2$	s_0	s_1
2	$s_0 \oplus s_1$	$s_1 \oplus s_2$	s_0
3	$s_0 \oplus s_1 \oplus s_2$	$s_0 \oplus s_1$	$s_1 \oplus s_2$
4	$s_0 \oplus s_2$	$s_0 \oplus s_1 \oplus s_2$	$s_0 \oplus s_1$
5	s_2	$s_0 \oplus s_2$	$s_0 \oplus s_1 \oplus s_2$
6	s_1	s_2	$s_0 \oplus s_2$
7	s_0	s_1	s_2
8	$s_1 \oplus s_2$	s_0	s_1
9	$s_0 \oplus s_1$	$s_1 \oplus s_2$	s_0
10	$s_0 \oplus s_1 \oplus s_2$	$s_0 \oplus s_1$	$s_1 \oplus s_2$
11	$s_0 \oplus s_2$	$s_0 \oplus s_1 \oplus s_2$	$s_0 \oplus s_1$
12	s_2	$s_0 \oplus s_2$	$s_0 \oplus s_1 \oplus s_2$
13	s_1	s_2	$s_0 \oplus s_2$
14	s_0	s_1	s_2





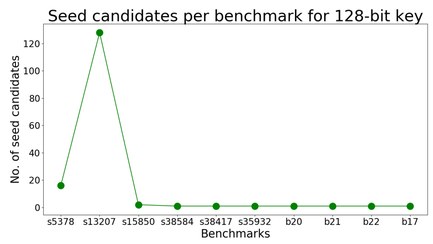
(a) Linear modeling of scan locked circuit.

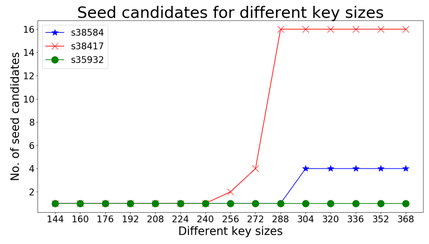
(b) Using this table, substitute k_y^x with s_0, s_1, and s_2. x denotes the row number and y denotes the column.

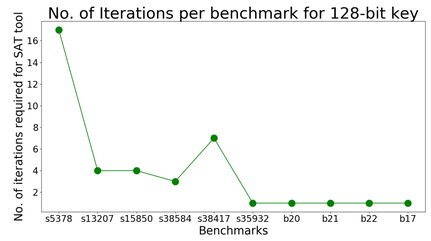
(c) Using (a) and (b), construct the combinational model of the scan locked circuit.

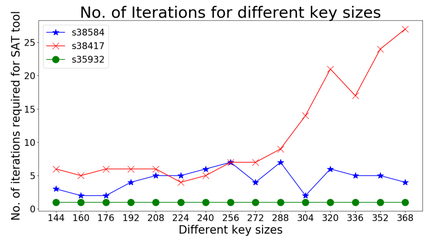
(d) Flowchart for DynUnlock attack using developed scripts and academic tools.

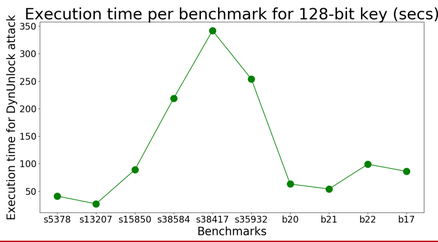
Experimental Results on ISCAS-89 & ITC-99 Suites

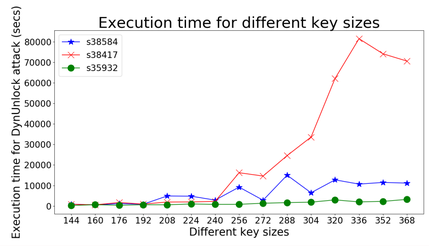












Conclusion

- DynUnlock is a **novel attack** which circumvents the **most dynamic case** of scan locking [2] and can **break any version** of dynamic scan locking.
- **Recovered** the complete LFSR seed within **seven minutes** for all the benchmarks under consideration for key size of **128-bits**.
- DynUnlock attack is **scalable** with **number of scan flops** as well as with **increasing key sizes.**
- With our attack process, we will never run out of iterations, as **the attack will always provide seed candidates,** if not the correct unique seed.
- Brute-forcing the seed candidates **recovers the correct key** (Maximum brute-force required -> 2^7 = 128 for s13207).

References

[1] M. Rostami et al., "A primer on hardware security: Models, methods, and metrics," Proc. of the IEEE, 2014.

[2] R. Karmakar et al., "A Scan Obfuscation Guided Design-for-Security Approach For Sequential Circuits," TCAS II: Express Briefs, 2019