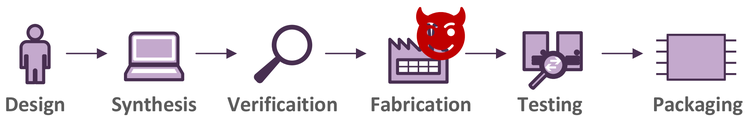
CLIC-A: Characterization of Locked Integrated Circuits via ATPG

Danielle Duvalsaint*, Shawn Blanton
Department of Electrical and Computer Engineering, Carnegie Mellon University
www.ece.cmu.edu/~actl

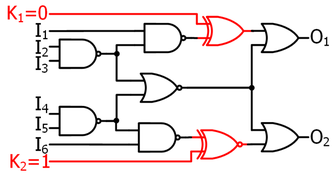
1. Hardware Security Threats

Possible threats in the IC design chain:
- IC piracy
- Reverse engineering
- Overproduction
- Malicious circuit insertion



2. Logic Locking

Logic locking aims to prevent threats by modifying a design such that it requires a correct key to function correctly



Security of logic locking methods often measured by ease of finding the correct key through an "attack"

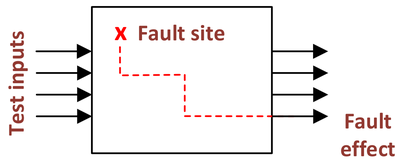
Attack Methods
- **Key sensitization** [Rajendran, DAC '12]
- **Hill climbing** [Plaza, TCAD '15]
- **SAT attack** [Subramanyan, HOST '15]
- **Key approximation** [Shamsi, HOST '17]
- **Bypass** [Xu, GLSVLSI '17]
- **Removal** [Yasin, TETC '17]
- **CycSAT** [Zhou, ICCAD'17]
- **SFLL-HD Attack** [Yang, TIFS '19]
- **Functional analysis attack** [Sirone, DATE '19]
- **CLIC-A** [Duvalsaint, ITC '20]

Locking Methods
- Random [DATE '08]
- Fault-based [DATE '12]
- Strong [DAC '12]
- SARLock [HOST '16]
- Anti-SAT [CHES '16]
- Cyclic [GLSVLSI '17]
- TTLock [GLSVLSI '17]
- SFLL-HD [CCS '17]

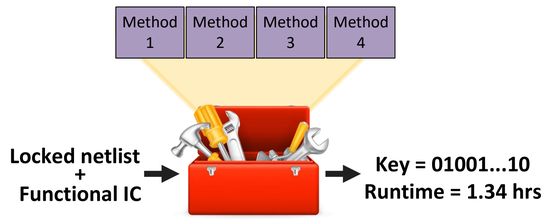
CLIC-A allows designers to **compare security of different locks**

3. CLIC-A

ATPG – Automatic test pattern generation
- Takes in a netlist and generates input patterns (tests) that propagate possible defects at signal lines to primary outputs
- Mature, well-developed tool able to handle large and complex designs



CLIC-A is an ATPG-based toolbox of methods for measuring the level of security of a locked circuit



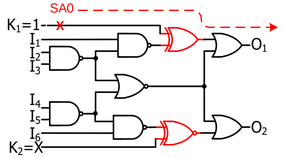
Security of lock measured in percentage of key solved and time to solve key

4. CLIC-A Methods

1: Key-input Sensitization [Rajendran et al., 2012]

Attack scenario: Locked netlist and a functional version of the circuit (i.e., oracle)

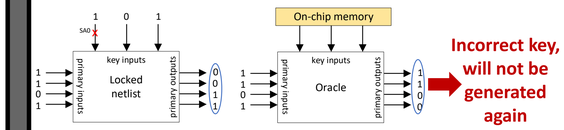
Input patterns are found that sensitize key values to primary outputs



2: Constraint-based ATPG

Attack scenario: Locked netlist and an oracle

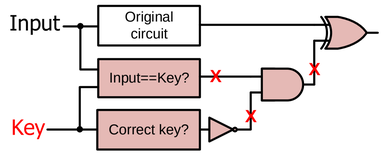
ATPG is used to generate a test for a fault at a key input, the test is then applied to the oracle



Incorrect key-input values are used as constraints on future ATPG rounds to guide ATPG towards correct key

3: Targeting Key-dependent Functionality

Attack scenario: Locked netlist (*i.e.,* oracle free)

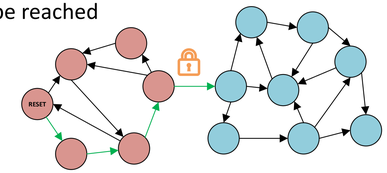


Tests generated for key-dependent functionality are analyzed to extract hard-coded key values

4: Sequential Key Derivation

Attack scenario: Locked netlist (*i.e.,* oracle free)

Functionality in the unlocked portion of the FSM require the key sequence to be reached

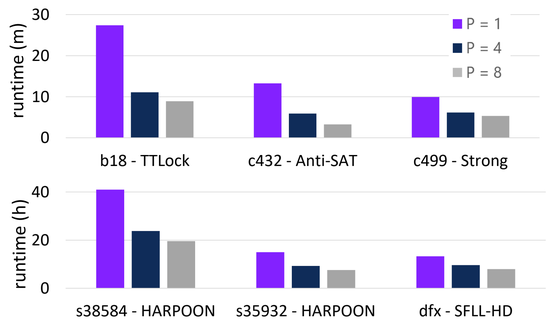


Analyzing functionality in each time frame reveals the correct key

5. Current Results

CLIC-A correctly solves key-input values for various lock types

Lock type	Circuit (gates, keys)	CLIC-A methods employed	CLIC-A performance % solved, runtime	Oracle required?
Random	c6288 (2406, 128)	1, 2	**100%**, 18 h	Y
Fault-based	c1908 (971, 91)	1, 2	**100%**, 6.61 m	Y
Strong	c499 (212, 10)	1, 2	**100%**, 13 m	Y
Cyclic	c7552 (1474, 50)	1, 2	**100%**, 8.4 m	Y
SARLock	apex2 (739, 71)	1, 2, 3	**100%**, 1.45 m	Y
Anti-SAT	c7552 (4337, 685)	1, 2, 3	**100%**, 13.5 m	Y
SFLL-HD	dfx (42404, 256)	3	**100%**, 13.3 h	N
Sequential locking	s38584 (5987, 32 cycles)	4	**100%**, 41.0 h	N



CLIC-A runtime decreases with the number of parallel ATPG runs (*P*)

*For more information, please contact dduvalsa@andrew.cmu.edu