Hybrid STT-CMOS Designs for Reverse-engineering Prevention

Theodore Winograd
George Mason University

Hassan Salmani*
Howard University

Hamid Mahmoodi
San Francisco State University

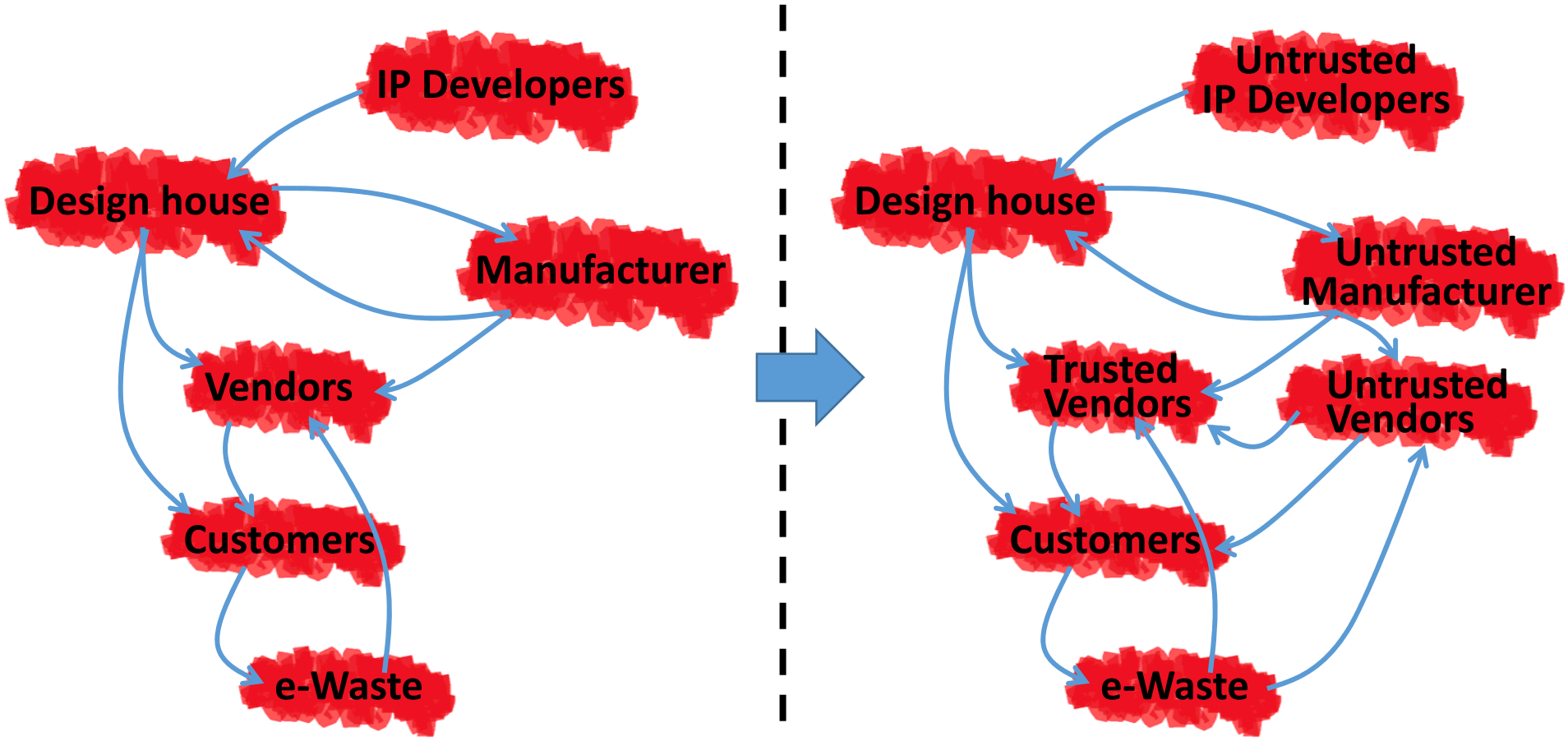
Kris Gaj
George Mason University

Houman Homayoun
George Mason University

Agenda

- Untrusted IC supply chain flow
- Previous work
- The security-driven design flow
- Results
  - Parametric Analyses
  - Security analyses
- Conclusions

Untrusted IC Supply Chain Flow

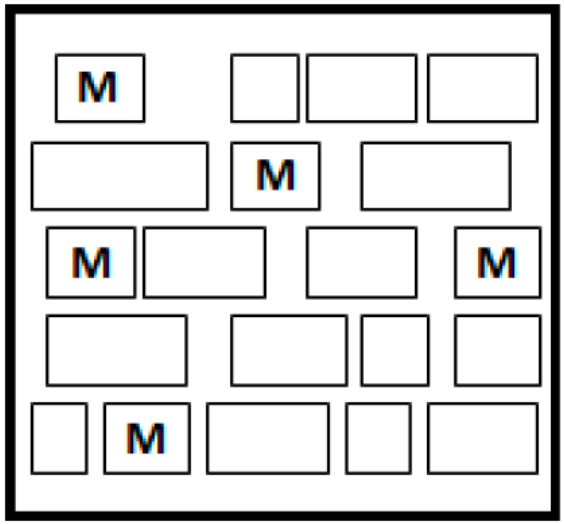


Previous Work

- Active and passive IC Metering
- Secure split-test
- Integrated Circuit Camouflaging
- SAFES architecture
- Shielding, obfuscation, self-modification (re-configuration), memory zeroization, and self-destruction, etc.

Our Solution: Hybrid STT-CMOS Designs

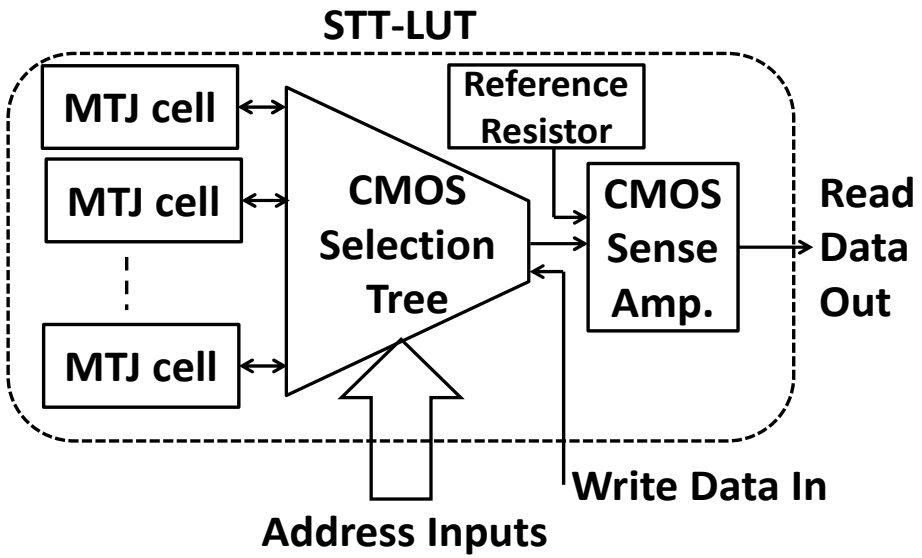
- Integration of custom and programmable cells
  - Hiding circuit functionality
- Security driven design flow
- Competitive with CMOS
  - Power, Performance, Area



M: STT-based LUT

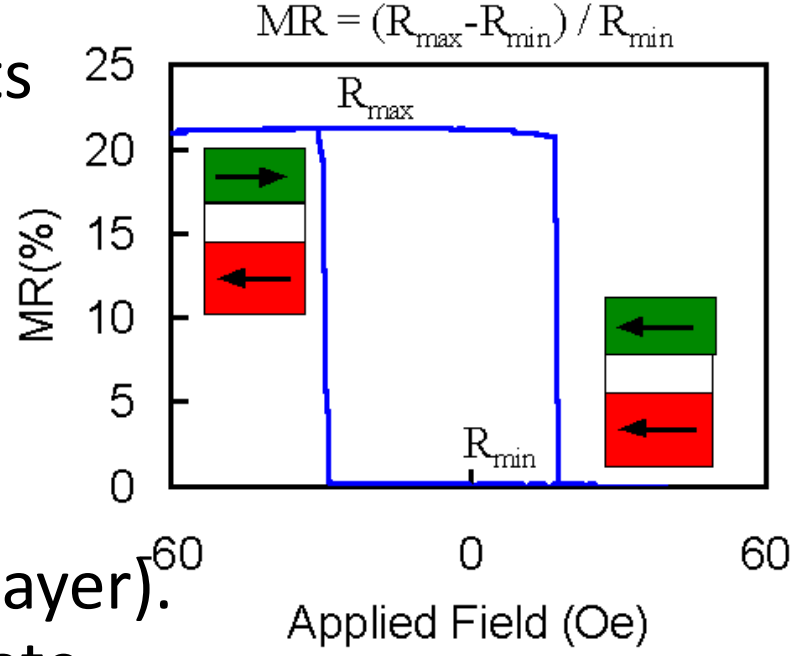
Spin Transfer Torque-based LUT

- STT advantages in terms of power, performance and security
- Non-volatile unlike SRAM (source of vulnerability)
  - MTJ offers non-volatile resistive storage
- Extreme low leakage
- Reliability against process variations
- Power and performance advantage over custom CMOS for complex circuits

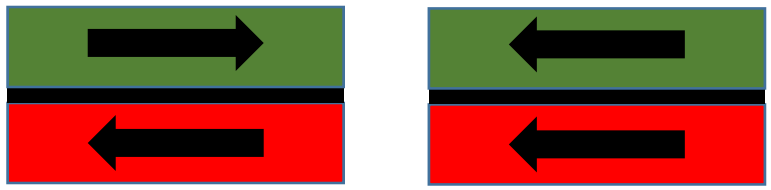


Magnetic Tunnel Junction (MTJ)

- Consisting of two Ferromagnets separated by a thin insulator (~ 1nm).
- Magnetization of one layer is fixed (reference layer) and other layer magnetization is switched accordingly (storage layer). Corresponding to “0” or “1” state.

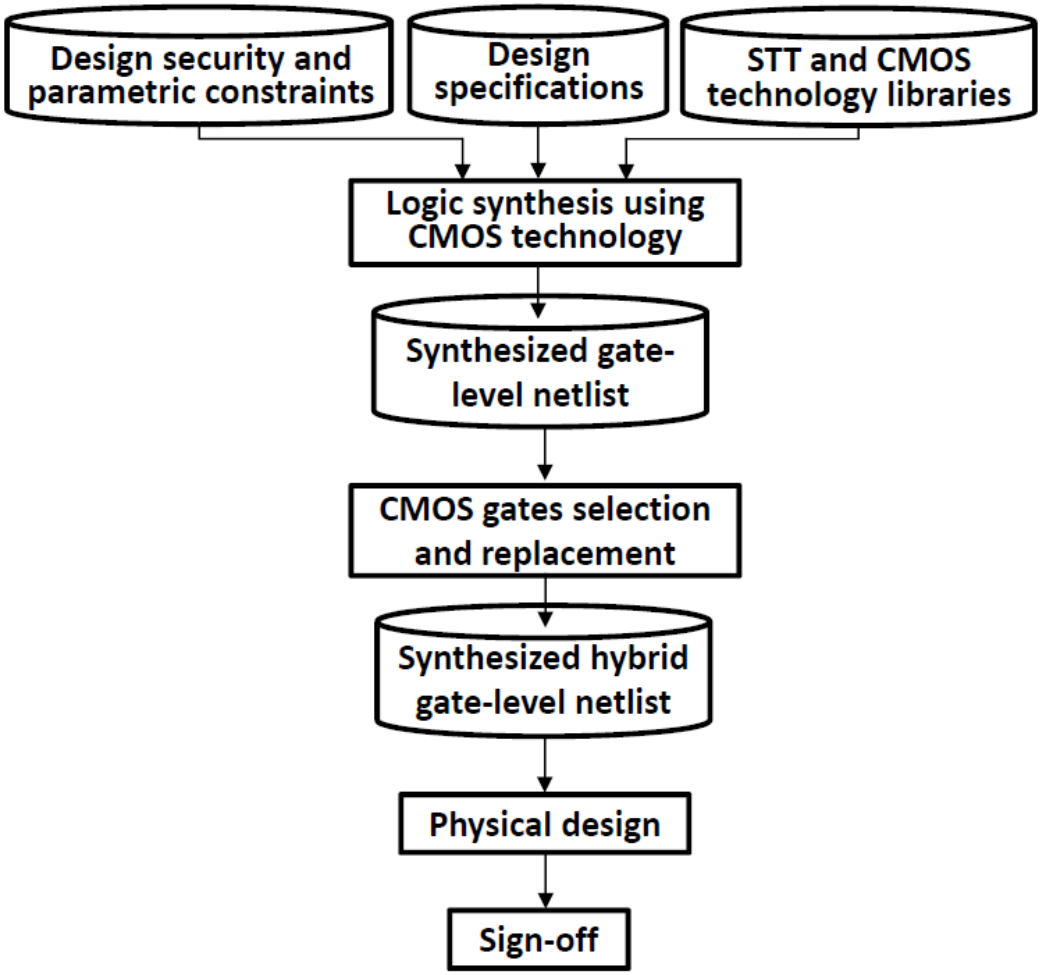


- The binary state is read by sensing the resistance



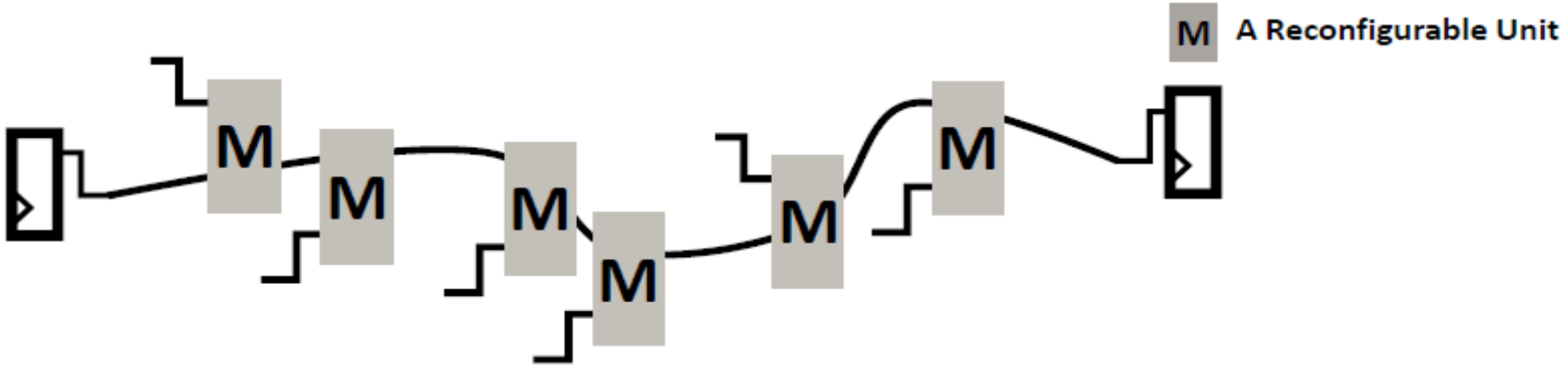
“1” State “0” State

Security-Driven STT-CMOS Design Flow



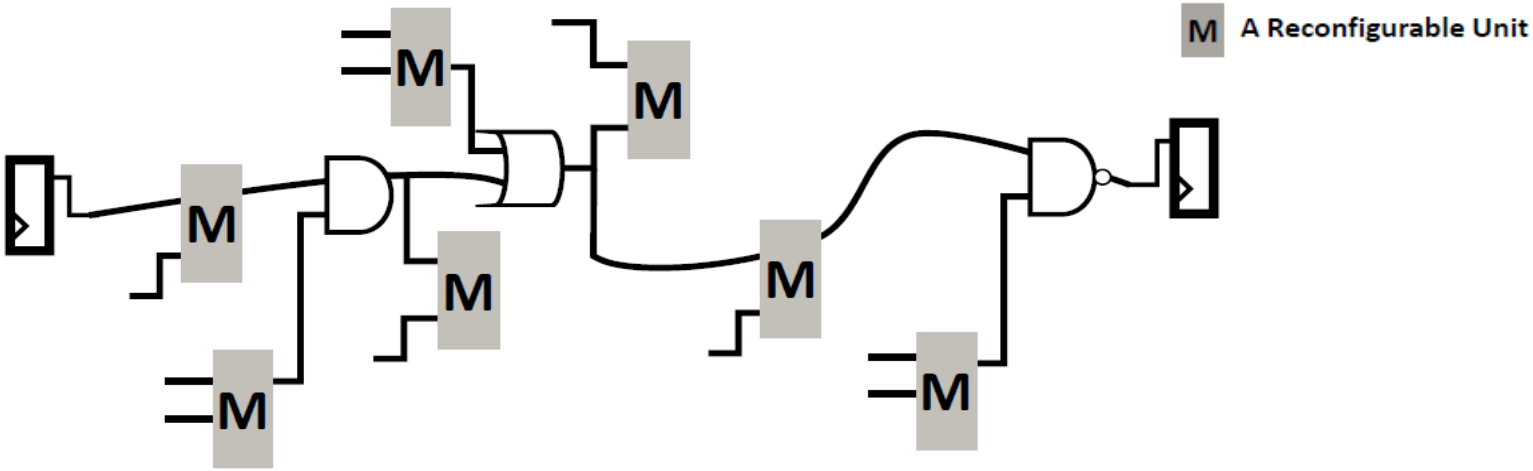
CMOS Gate Selection and Replacement

- Independent selection
  - Gates are randomly selected such that they are not necessarily reachable from each other.
- Dependent selection
  - All gates on selected timing paths are replaced with reconfigurable LUTs



CMOS Gate Selection and Replacement (Continued)

- Parametric-aware dependent selection (based on timing)
  - Selected gates on a timing path are replaced while their deriving gates are replaced with reconfigurable LUTs



Performance, Power, Area Overheads

	Performance degradation %			Power overhead %			Area overhead %			Number of STTs			
Circuit	Indep	Dep	Para	Indep	Dep	Para	Indep	Dep	Para	Indep	Dep	Para	size
s641	0	2	1	11.14	82.11	8.45	2.64	20.66	4.98	5	39	9	287
s820	10.82	14.77	2.37	11.45	18.72	5.08	3.02	5.63	1.34	5	9	2	289
s832	4.42	71.20	7.75	13.44	14.39	1.92	3.22	4.98	0.51	5	8	1	379
s953	0	28.42	4.55	11.02	33.49	8.03	2.32	7.14	2.38	5	15	5	395
s1196	0	0	0	7.83	12.54	7.95	1.97	3.94	2.64	5	10	7	508
s1238	0	8.76	4.45	8.32	14.39	8.13	2.02	4.38	2.73	5	11	7	529
s1488	0	45.45	6.7	4.43	15.49	8.18	1.60	6.83	3.47	5	21	11	657
s5378a	7.3	82.32	1.5	2.93	45.11	9.80	0.37	9.30	6.88	5	131	98	2779
s9234a	7.7	62.42	0	1.20	42.18	9.83	0.20	10.06	3.24	5	256	82	5597
s13207	2.07	0	0	0.73	9.82	8.21	0.12	2.19	2.60	5	92	111	7951
s15850a	0	25.39	0	0.70	9.41	6.04	0.10	1.88	1.78	5	89	85	9772
s38584	0	0	0	0.21	1.86	5.13	0.05	0.44	1.56	5	47	166	19253
Average	2.69	28.40	2.36	6.12	24.96	7.23	1.47	6.45	2.84	5.00	60.67	48.67	4033.00

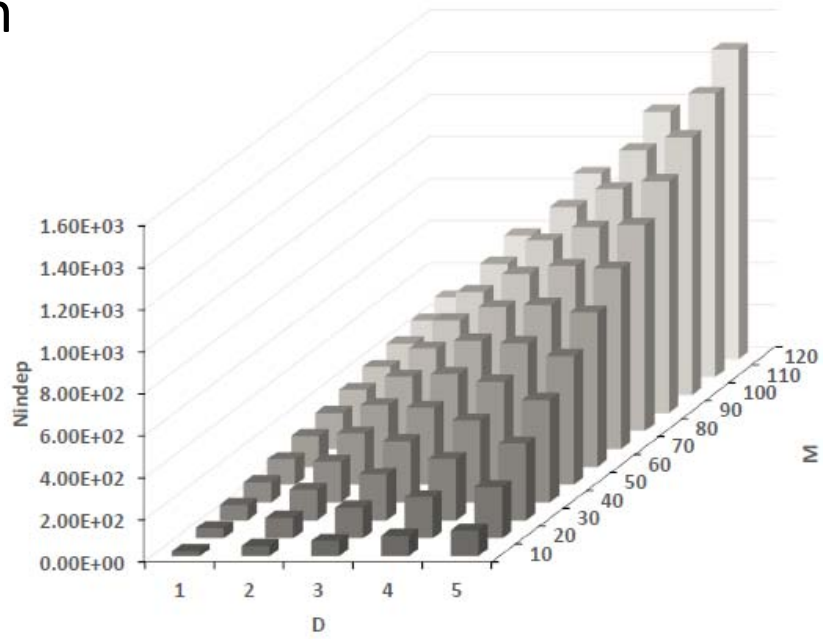
ATPG Attacks

- An attacker applies random inputs and observe circuit outputs to determine functionality of reconfigurable LUTs
- Attack Model
  - An untrusted manufacturer has the netlist of a STT-CMOS circuit containing known standard cells and unknown reconfigurable STT-based LUT (the unresolved circuit)
  - The untrusted manufacturer obtains a configured STT-CMOS circuit (the blackbox circuit)
  - The untrusted manufacturer develops a set of patterns by analyzing the unresolved circuit and applies it to the blackbox circuit to determine the functionality of STT-based LUTs

ATPG Attacks (Continued)

- Independent selection:
  - An attacker may use a testing technique to justify and propagate the output of missing gates to the observation points
  - With this effort, the attacker can develop a partial truth table for each missing gate and then guess the functionality of the missing gate

$$N_{indep} = \sum_{i=1}^{M} \alpha_i \times D_i$$

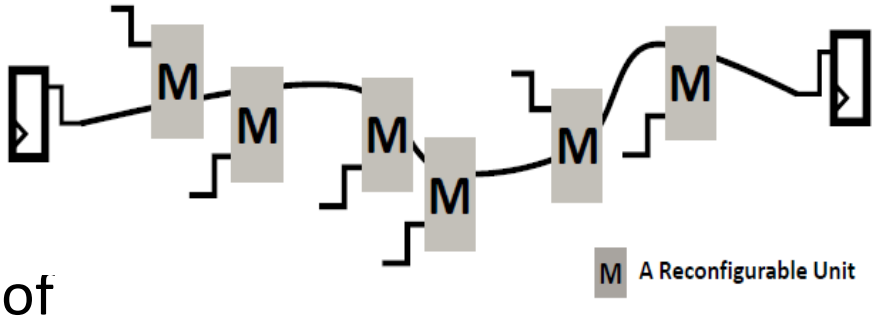


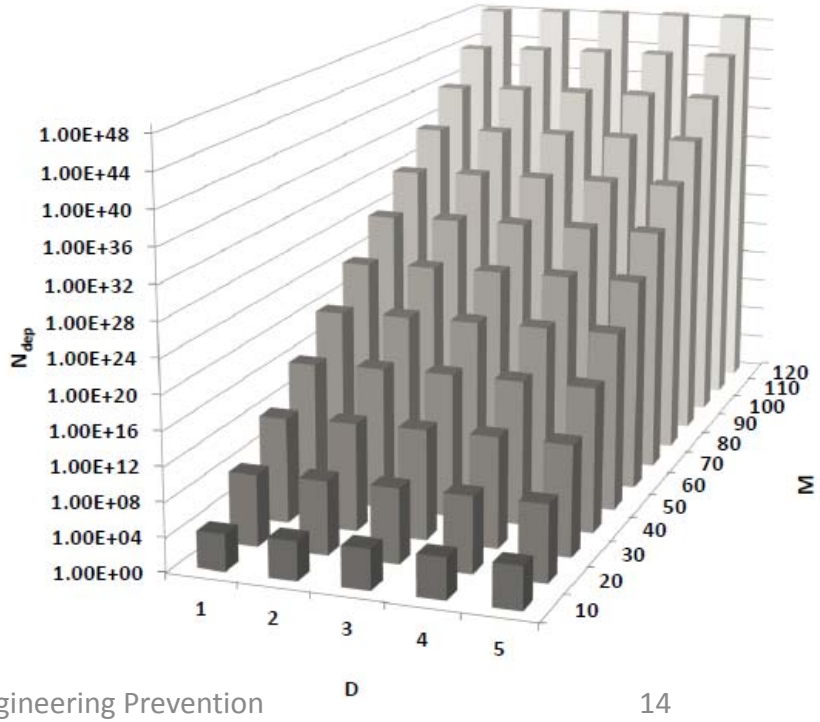
***M*: the number of reconfigurable LUTs**
***α*: gates similarity**
***D*: the depth of circuit**

ATPG Attacks (Continued)

- Dependent selection:
  - An attacker may try to study the impact of value change of off-path signal of the closest missing gate to an observation point to determine the missing gate.
  - The attacker can develop a partial truth table

$$N_{dep} = \prod_{i=1}^{M} \alpha_i \times P_i \times D_i$$

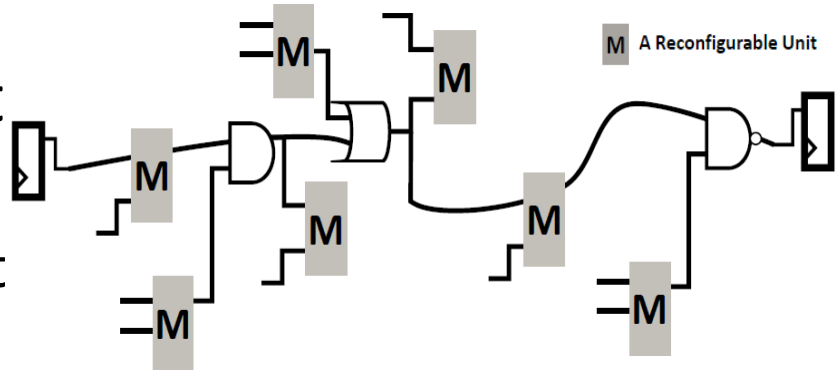


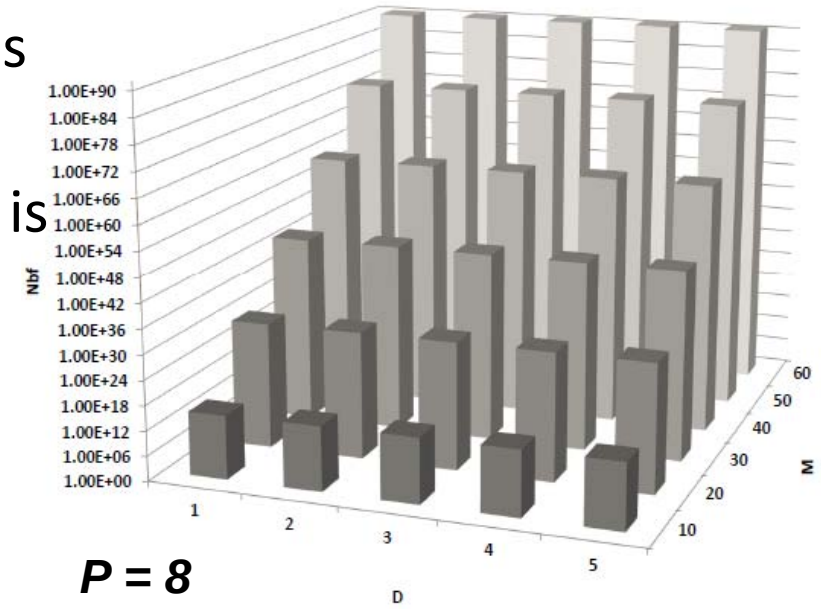


ATPG Attacks (Continued)

- Parametric-aware dependent selection (based on delay):
  - An attacker is not able to creat any partial truth tables for missing gates, as off-path signals are blocked.
  - The only option remains here is Brute force attack.

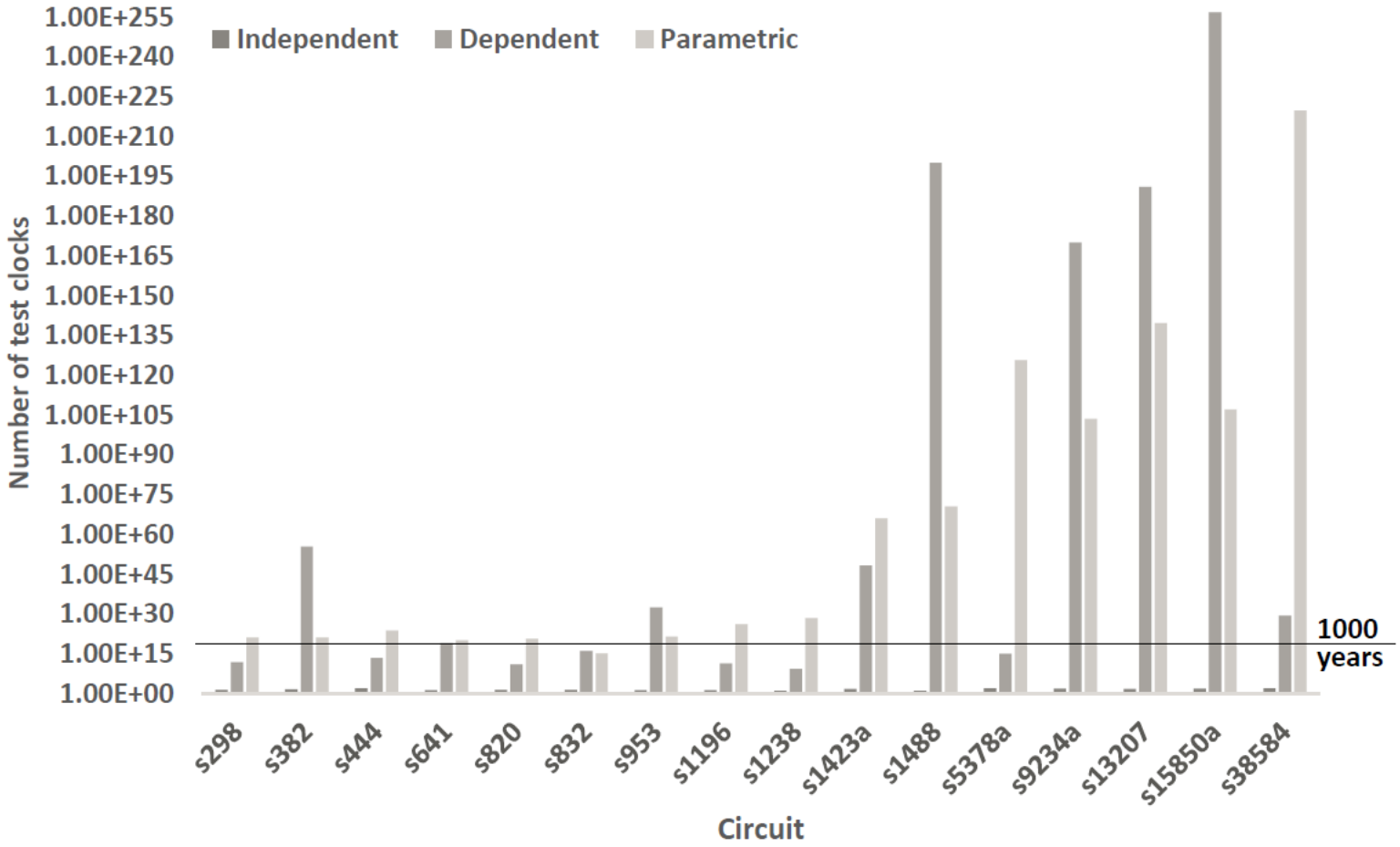
$$N_{bf} = 2^I \times P^M \times D.$$





P = 8

Brute force Attacks



SAT-based Attacks

- Time to decamouflaging

*This table is reproduced**

	Time (Sec)	$\|I\|$	Circuit Gates	Camouflaged Gates
c5315	300	25	2406	63
c7552	100	10	3512	65
s5378	150	19	2779	56
s9234	600	32	5597	79
s38584	2200	22	19234	128

  - Very strong correlation between time for decamouflaging and the number of circuit and camouflaged gates, 0.9898, and 0.9887, respectively.
  - On the other hand, the correlation between time for decamouflaging and $|I|$ is insignificant, 0.2324.
- These facts highlight time to identify camouflaged gates strongly depends on the size of circuit and the number camouflaged gates. While the possible types for camouflaged gates is limited to 3 in above analysis, it has been discussed increasing the number of possible identities far significantly increase time for decamouflaging.

**M. E. Massad and et al. Integrated circuit (IC) decamouaging: Reverse engineering camouflaged ICs within minutes, NDSS2015.*

SAT-based Attacks (Continued)

- Our empirical analysis reveals that time to determine the identity of an unknown gate for a same circuit has an exponential relationship with the number of possible identities and the number of unknown gates

$$Time \propto T^{\beta K}$$

  - where *T* is the number of possible identities and *K* the number of unknown gates.
- Empirically β depends on *T*. For small *T*, e.g. three for a camouflaged circuit, β is about 0.1, and for large *T*, e.g. 16 for STT-CMOS hybrid circuits, β is about 0.9.

SAT-based Attacks (Continued)

- For *T* = 16, time to determine the functionality of STT-based LUTs

	Time (Sec)	The number of missing gates (K)
c5315	1.87E+68	63
c7552	2.76E+70	65
s5378	4.87E+60	56
s9234	4.10E+85	79
s38584	5.18E+138	128

CPU Time for Gate Selection and Replacement

- Collected on 1.7 GHz Intel Core i7 with 8 GB of RAM (minute:second)

Circuit	Independent	Dependent	Parametric
s298	00:00.1	00:00.1	00:00.1
s382	00:00.4	00:00.4	00:00.6
s444	00:00.3	00:00.3	00:00.1
s641	00:00.7	00:01.0	00:00.8
s820	00:00.1	00:00.1	00:00.1
s832	00:00.1	00:00.1	00:00.1
s953	00:00.1	00:00.2	00:00.2
s1196	00:00.1	00:00.2	00:00.2
s1238	00:00.1	00:00.1	00:00.1
s1423a	00:01.2	00:00.8	00:00.7
s1488	00:00.1	00:00.1	00:00.1
s5378a	00:09.1	00:14.9	00:26.9
s9234a	01:15.5	01:07.4	01:30.2
s13207	00:25.4	00:25.4	00:27.1
s15850a	00:52.6	00:48.2	00:54.9
s38584	00:35.7	00:42.3	00:44.0

Conclusions

- Introducing a novel security-driven hybrid STT-CMOS design flow to prevent design reverse engineering.
- Presenting three novel selection and replacement algorithms, i.e. independent, dependent, and parametric-aware dependent selections
- Significant resiliency of hybrid STT-CMOS circuits against brute-force, ATPG, and SAT-based attacks
- Insignificant impact of STT-based LUTs on design parametric constraints including area, power, and performance
- Computationally inexpensive where selecting CMOS gates for replacement takes less than a minute even for large circuits.

Increasing STT-based LUTs

	# of STT-based LUTs		Security	
Circuit	Min	Max	Min	Max
s298	1	44	4.9	1.43E+29
s444	1	62	22.2	2.32E+51
s820	1	46	7.4	2.66E+30
s953	1	100	4.9	4.05E+56
s1238	1	29	2.45	5.63E+12
s1488	1	92	1	1.88E+45
s9234a	1	100	2	8.19E+84
s15850a	1	100	7.4	1.81E+85
s382	1	67	7.35	2.9E+56
s641	1	100	4	4.01E+53
s832	1	60	2.45	6.07E+41
s1196	1	21	2.45	1.38E+10
s1423a	1	100	14.7	1.38E+96
s5378a	1	100	24.5	9E+110
s13207	1	100	20	1.37E+82
s38584	1	100	4.9	1.65E+108

Increasing STT-based LUTs (Continued)