Low Cost BIST for Public Key Crypto Cores

Dusko Karaklajic, Miroslav Knezevic
and Ingrid Verbauwhede

K.U. Leuven, ESAT/COSIC
Belgium

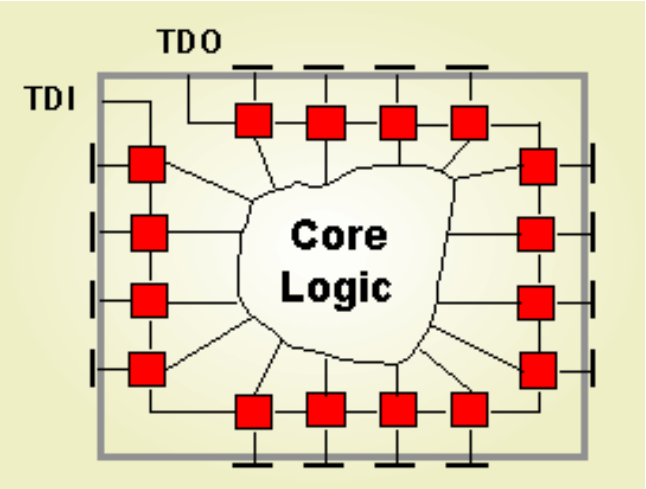
FDTC 2010.

Outline

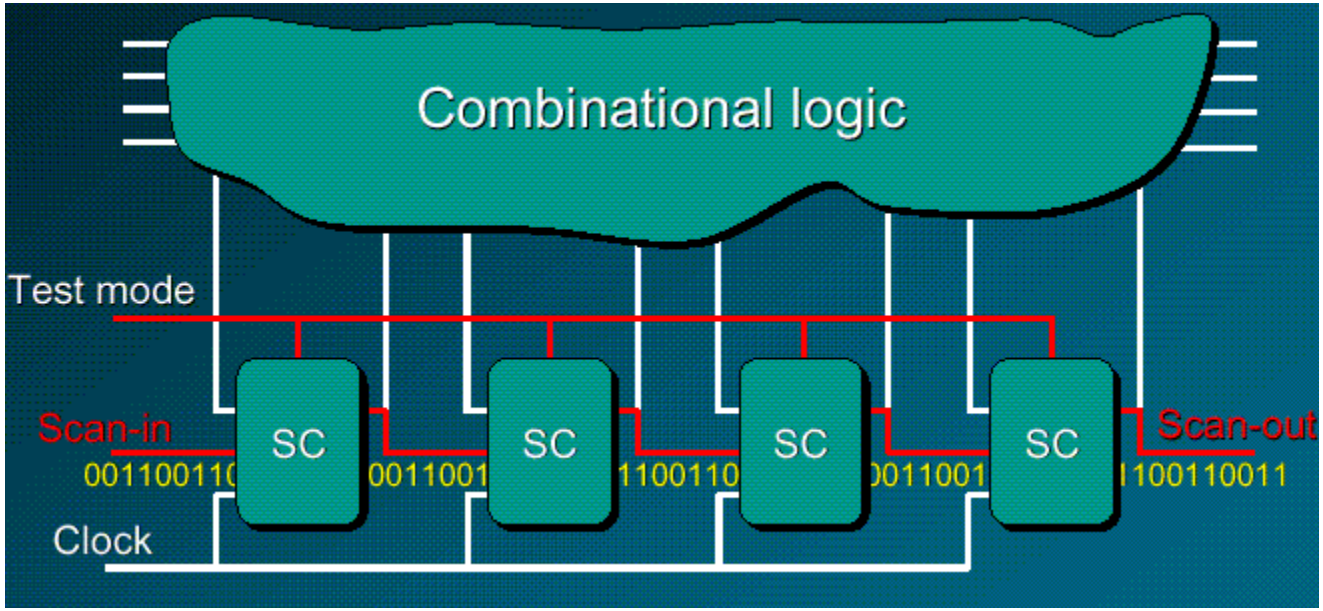
- Digital Testing
- Security Issues
- The Proposed Solution
- Evaluation
- Conclusion

Digital Testing

- Complex Digital Circuits
- Design for Testability
- Scan-chains

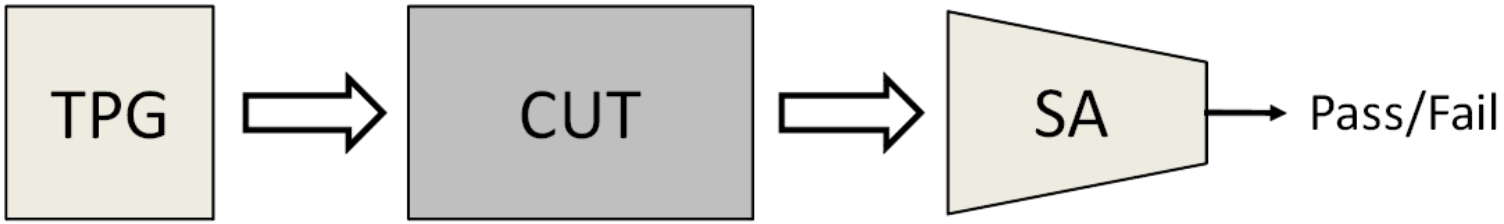


Security Issues



- Cryptographic circuits
- Scan-chain based attacks

Built In Self Test (BIST)

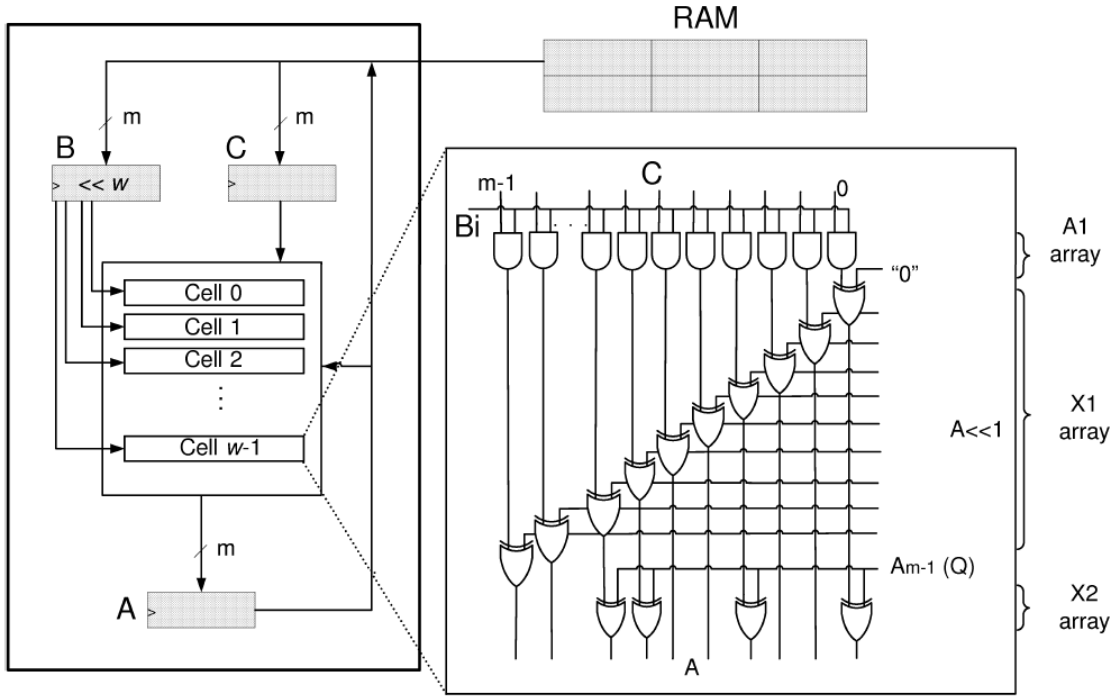


- 3 types:
  - Exhaustive
  - Deterministic
  - Pseudorandom
  - BIST Overhead

Pseudorandom BIST

- Pseudorandom Test Patterns
- Efficient Implementation
- Random Pattern Testability

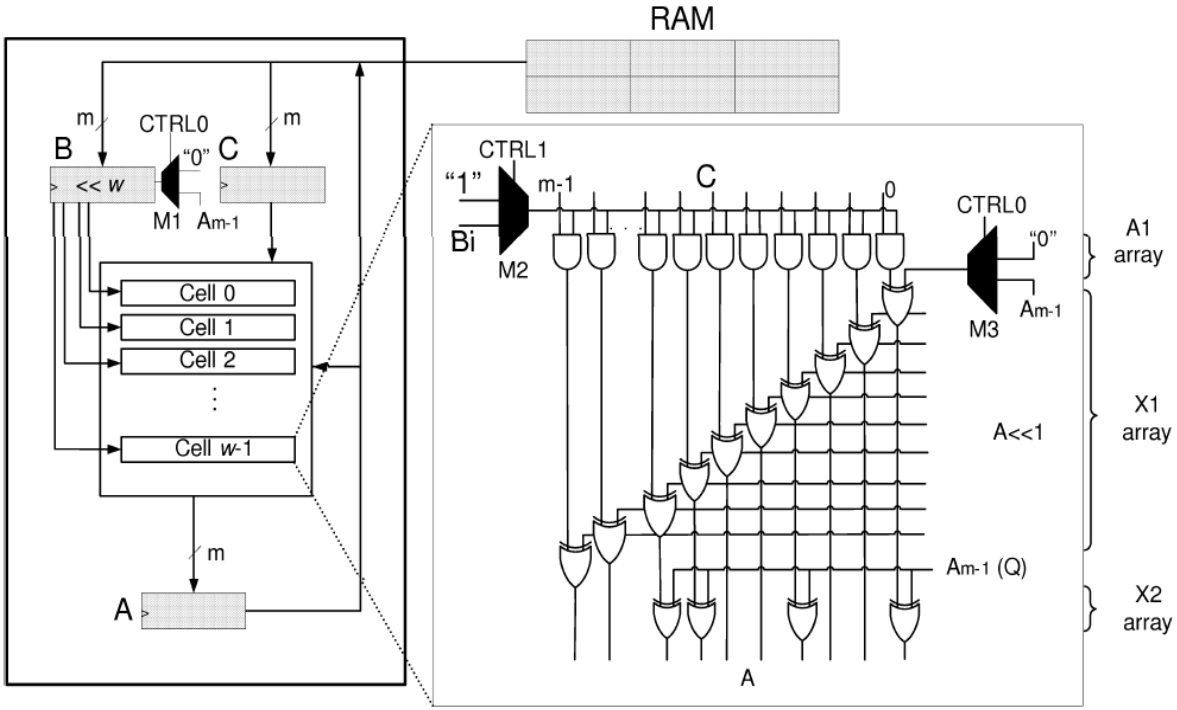
The Proposed Solution



$$A = BC \bmod P$$

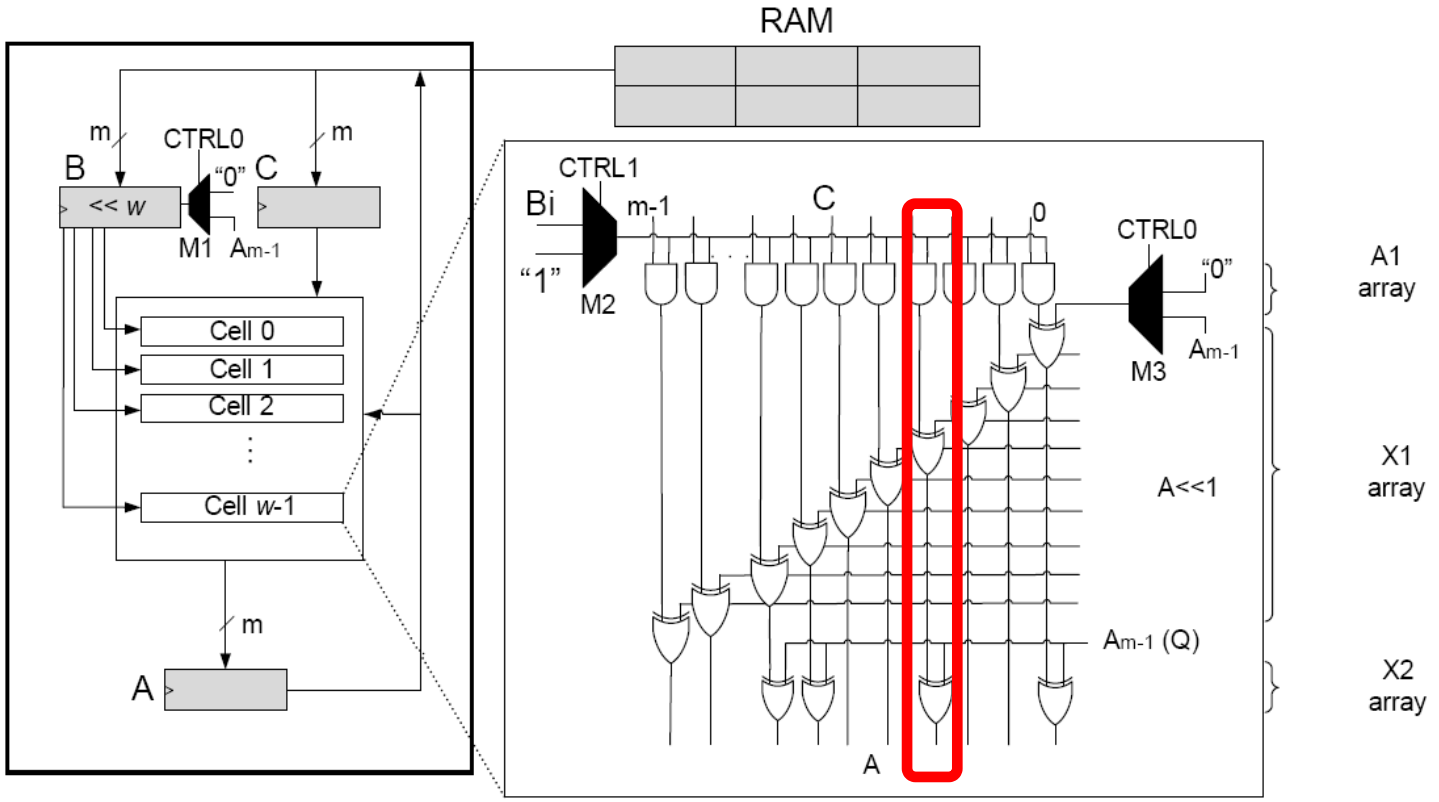
- Digit Serial Multiplier over GF(2^m)

The Proposed Solution



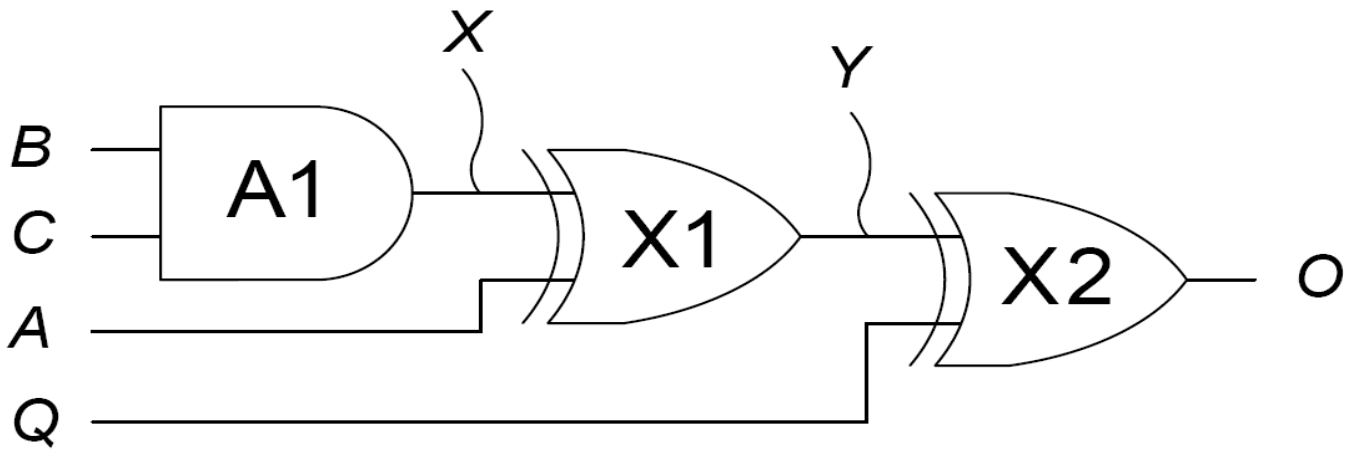
- Complete BIST Infrastructure
- Minimized hardware overhead

Test Pattern Generator



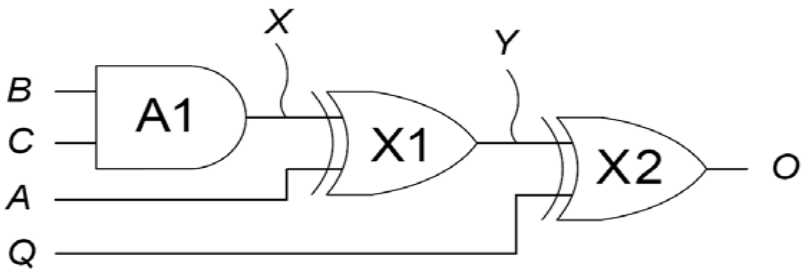
- CTRL0=1 and CTRL1=0
- Basic building blocks

Test Pattern Generator

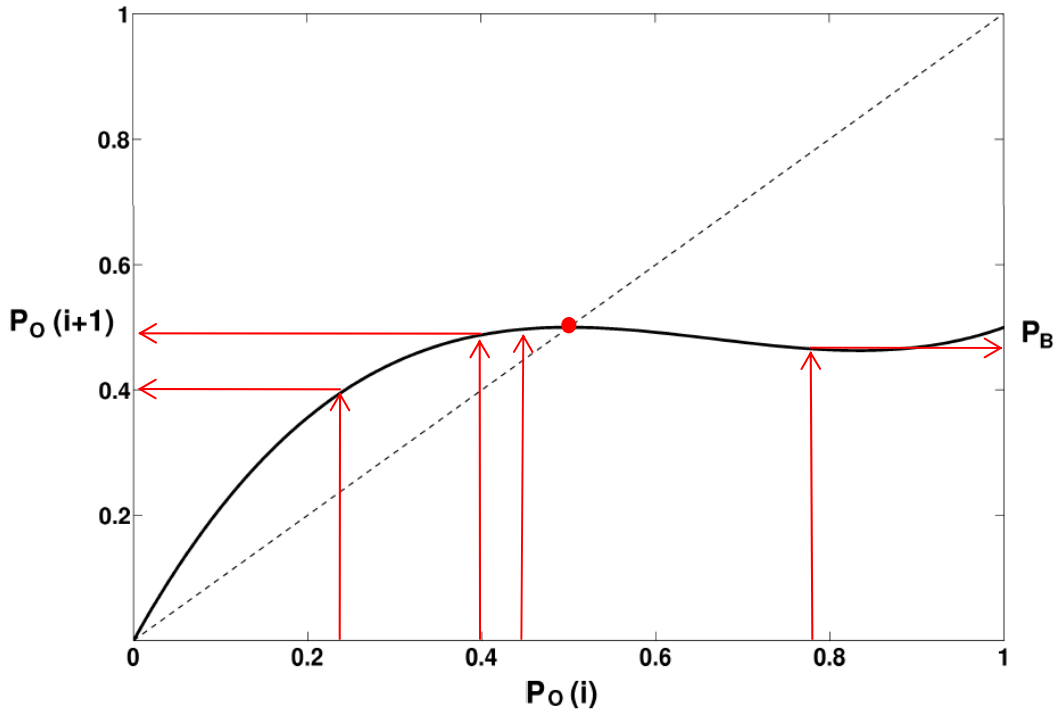


$$P_O(i+1) = 4P_B P_O(i)^3 - (4P_B+2)P_O(i)^2 + (2+P_B)P_O(i)$$

Test Pattern Generator



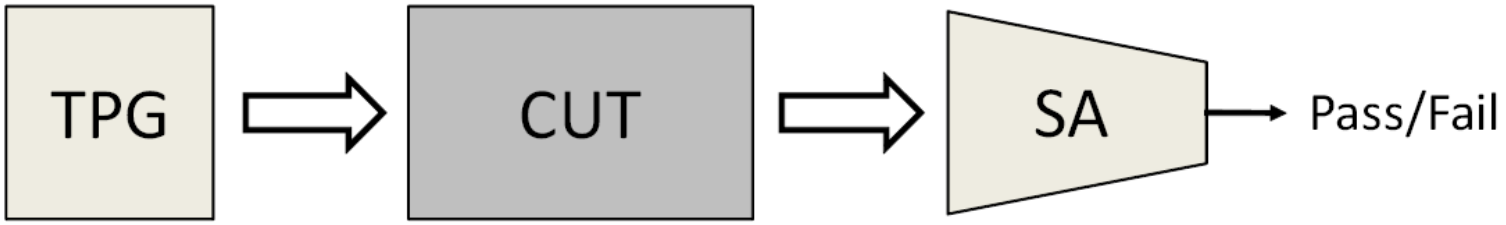
$$\lim_{i \to \infty} Po(i) = 0.5$$



TPG Randomness

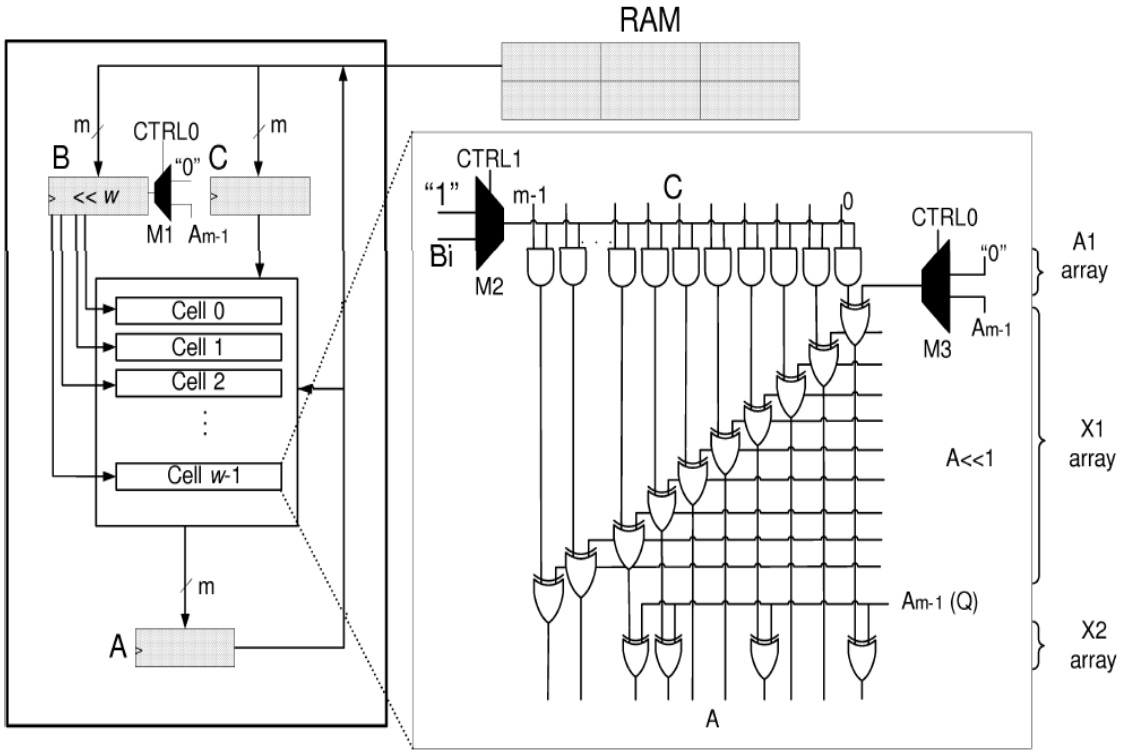
- NIST test
- Multiplier based TPG vs. LFSR
- Practical fault simulation

Signature Analyzer

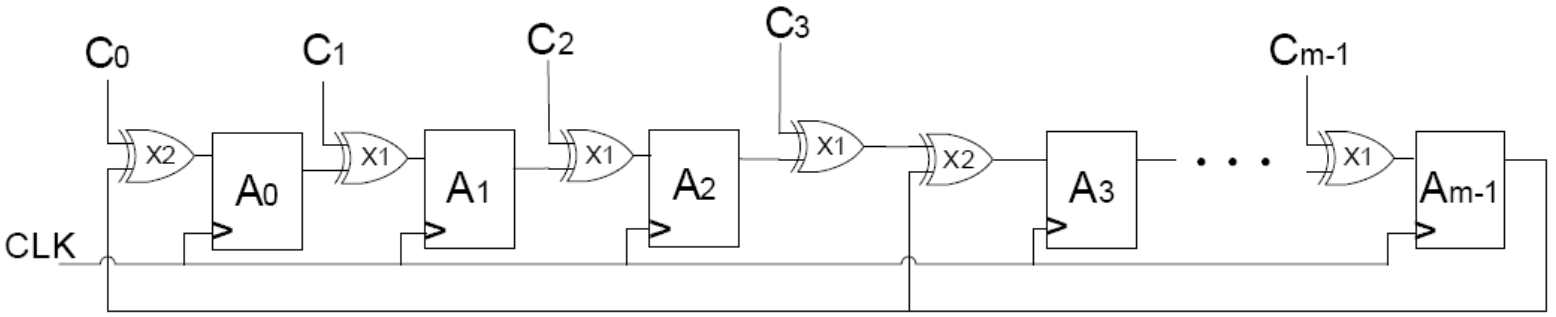


- CUT responses compactor
- Aliasing probability

Signature Analyzer



Signature Analyzer



- Multiple In Shift Register
- Aliasing probability 2^{-m}

Self Test

- Good random pattern testability properties
- N=43 patterns for 99% of Fault Coverage
- Simulation: N=52 patterns for 99% FC

Overhead

Design	Area (GE)	Overhead
Original Multiplier	4473	-
Proposed Multiplier	4488	0.33%

- GF(2^{163})
- UMC 0.13μm
- Additional overhead

Conclusion

- Efficient BIST solution
- Security
- Minimized hardware overhead
- Applications

Thank you!

NIST Randomness Test

Test	TPG	LFSR
Frequency	0.534146	0.779188
BlockFrequency	0.739918	0.494392
CumlativeSums	0.911413	0.595549
Runs	0.350485	0.145326
LongestRun	0.911413	0.616305
Rank	0.739918	0.534140
FFT	0.350480	0.037560
NonOverlappingTemplate	0.911413	0.883171
OverlappingTemplate	0.350485	0.304126
Universal	0.213309	0.262240
ApproximateEntropy	0.350485	0.816537
RandomExcursions	0.819544	0.816537
RandomExcursionsVariant	0.788728	0.995711
Serial	0.534146	0.574903
Linear	0.000000	0.000000

Modes of Operation

Configuration Mode	Setup Phase		Configuration Phase	
	CTRL0	CTRL1	CTRL0	CTRL1
Normal	0	0	0	0
TPG	1	1	1	0
SA	0	1	0	1
ST	1	1	1	0