Janusz Rajski • Maciej Trawka • Jerzy Tyszer • Bartosz Włodarczak

Hardware Root of Trust for SSN-based DFT Ecosystems

SIEMENS

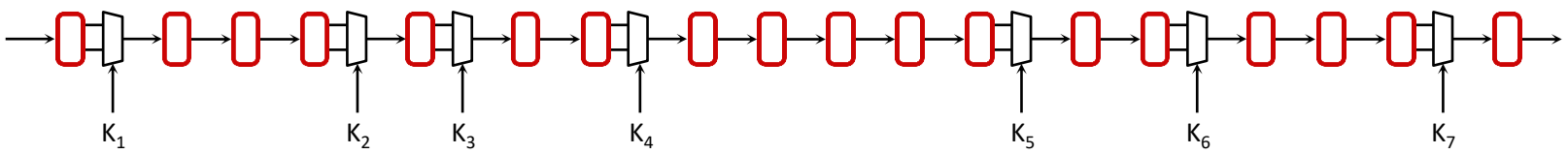
Motivation and Purpose

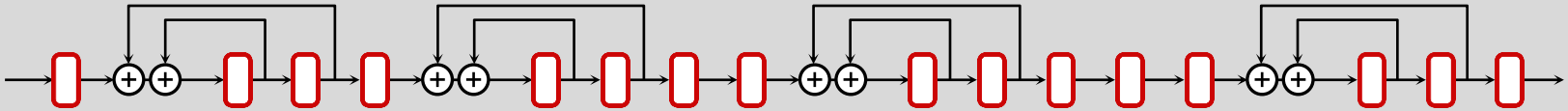
- Scan-based test – backdoor for security threats
- Hardware root of trust to defend against unauthorized access
- Compatible with DFT insertion flow
  - synthesizable
  - programmable and scalable
  - lightweight and die-centric
- Secure SSN technology with encrypted test patterns
- Synergistic with SSN’s central DFT entry
- Applicable to large SoC and 3D designs

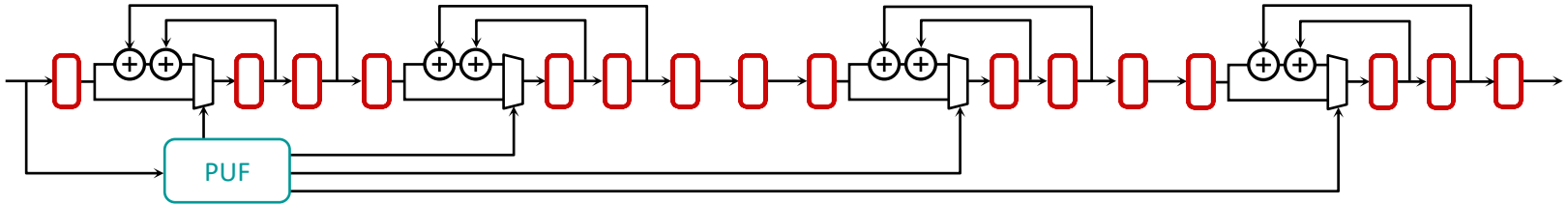
Outline

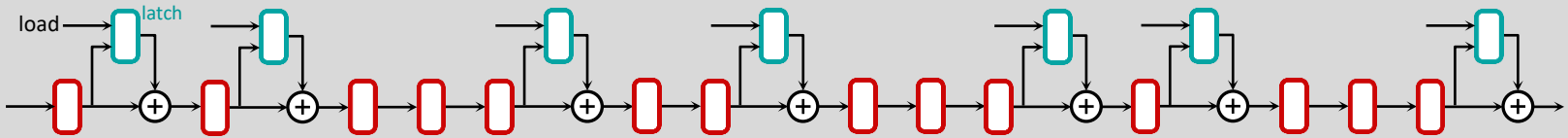
- Streaming scan network (SSN)
- Challenge-response authentication
- Hardware root of trust (RoT)
- Challenge generator
- Challenge hashing
- Test data encryption
- Conclusions

Attempts to secure scan chains

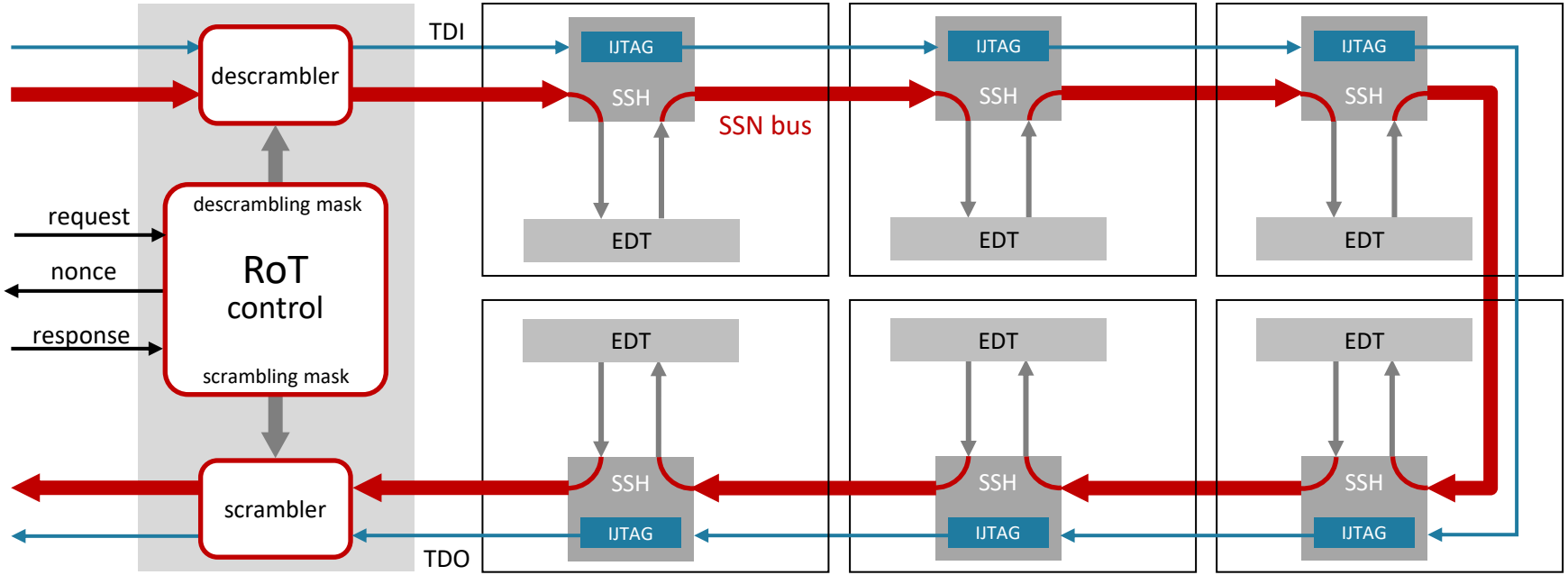






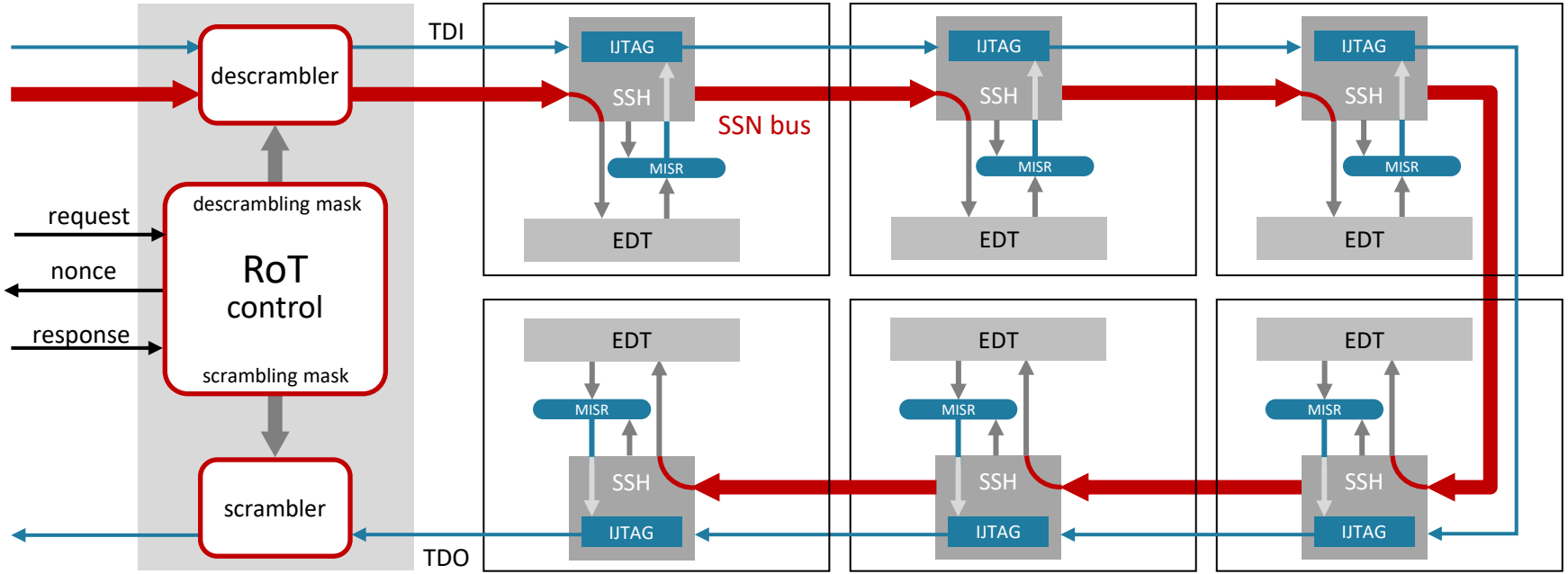


RoT and SSN-based SoC design



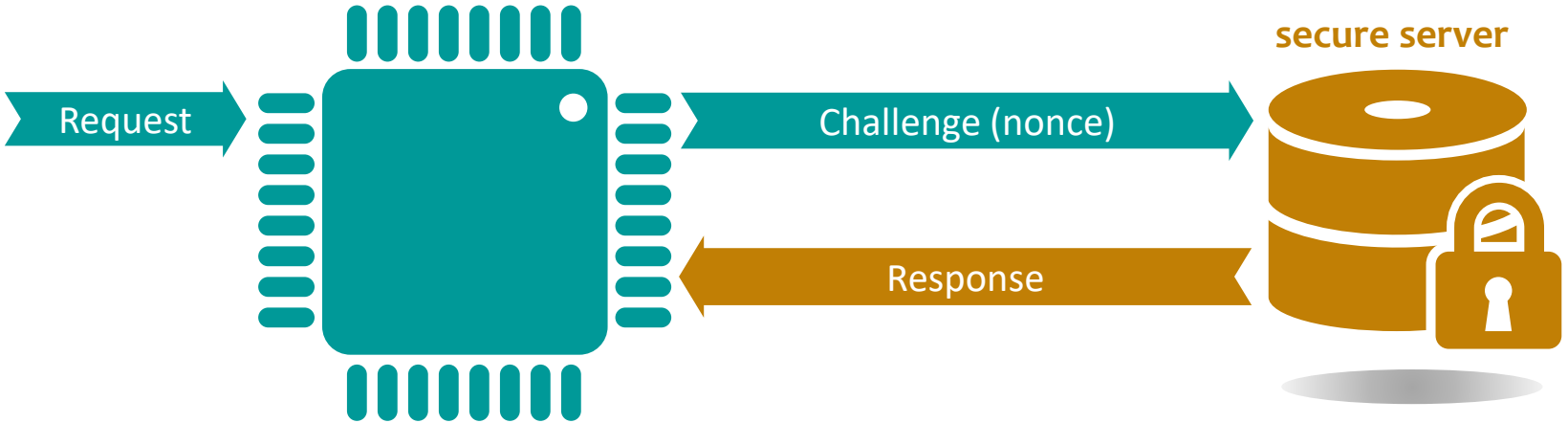
Full-duplex test data streaming

RoT and SSN-based SoC design

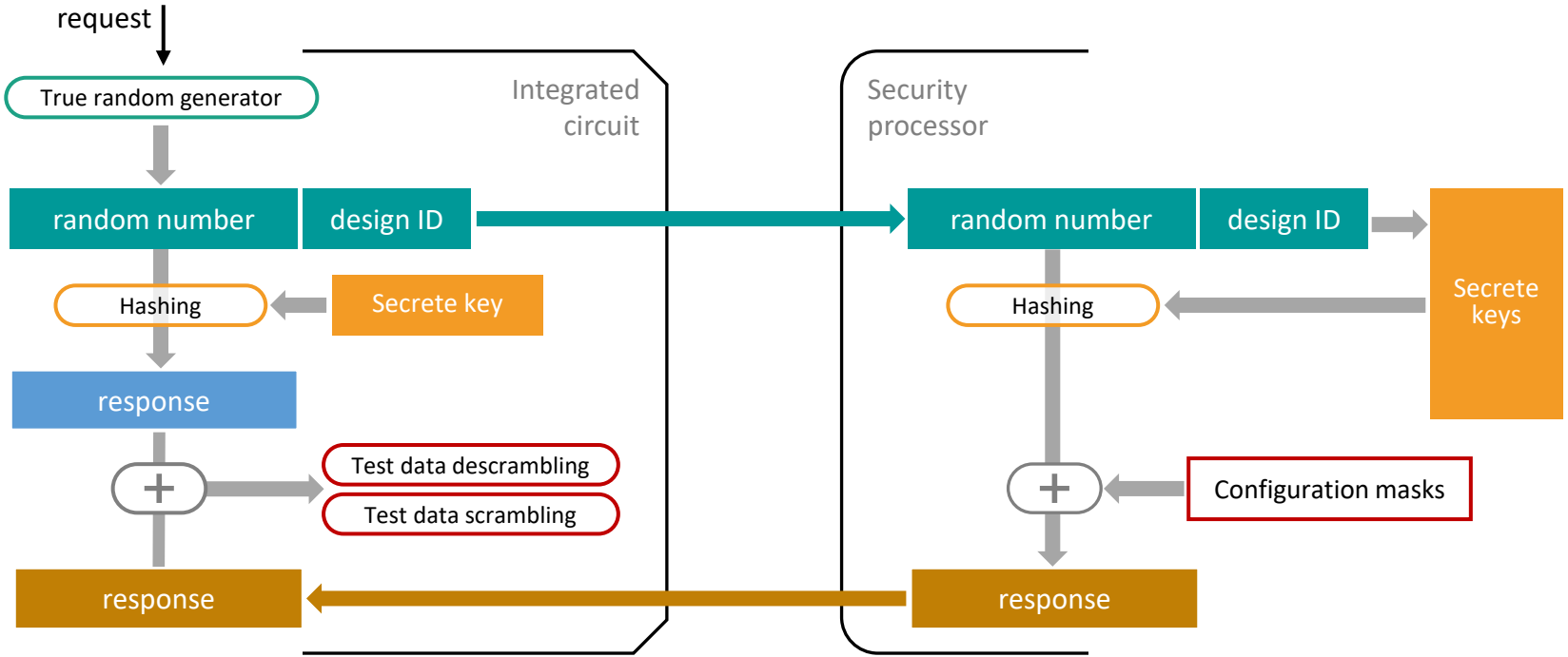


Input-only test data streaming with MISR or on-chip compare

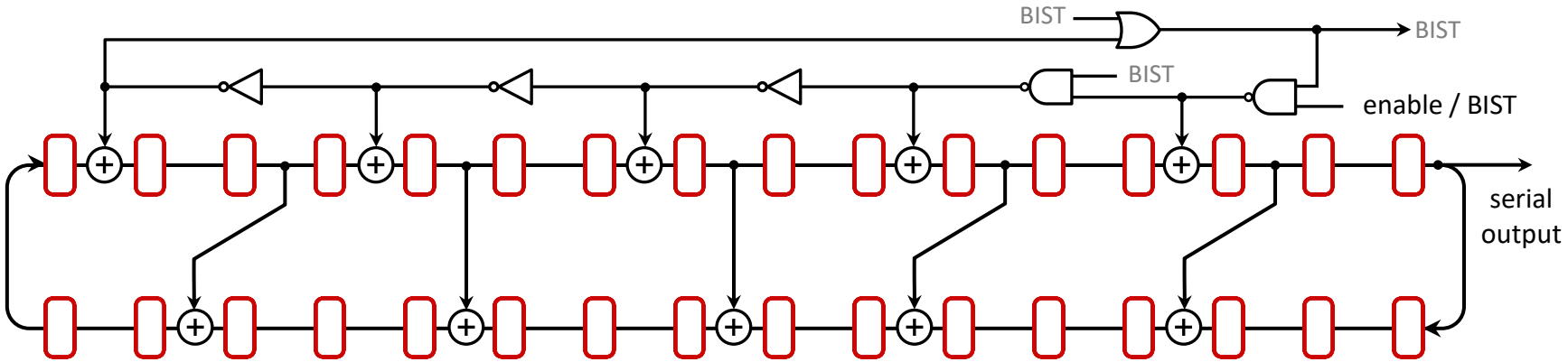
Challenge – response authentication



Challenge – response protocol



Challenge generator



Primitive characteristic polynomial: $x^{32} + x^{27} + x^{21} + x^{16} + x^{10} + x^5 + 1$

- Sampling many inverters to populate a long interval with the timing jitter
- Additional entropy due to setup and hold time violations

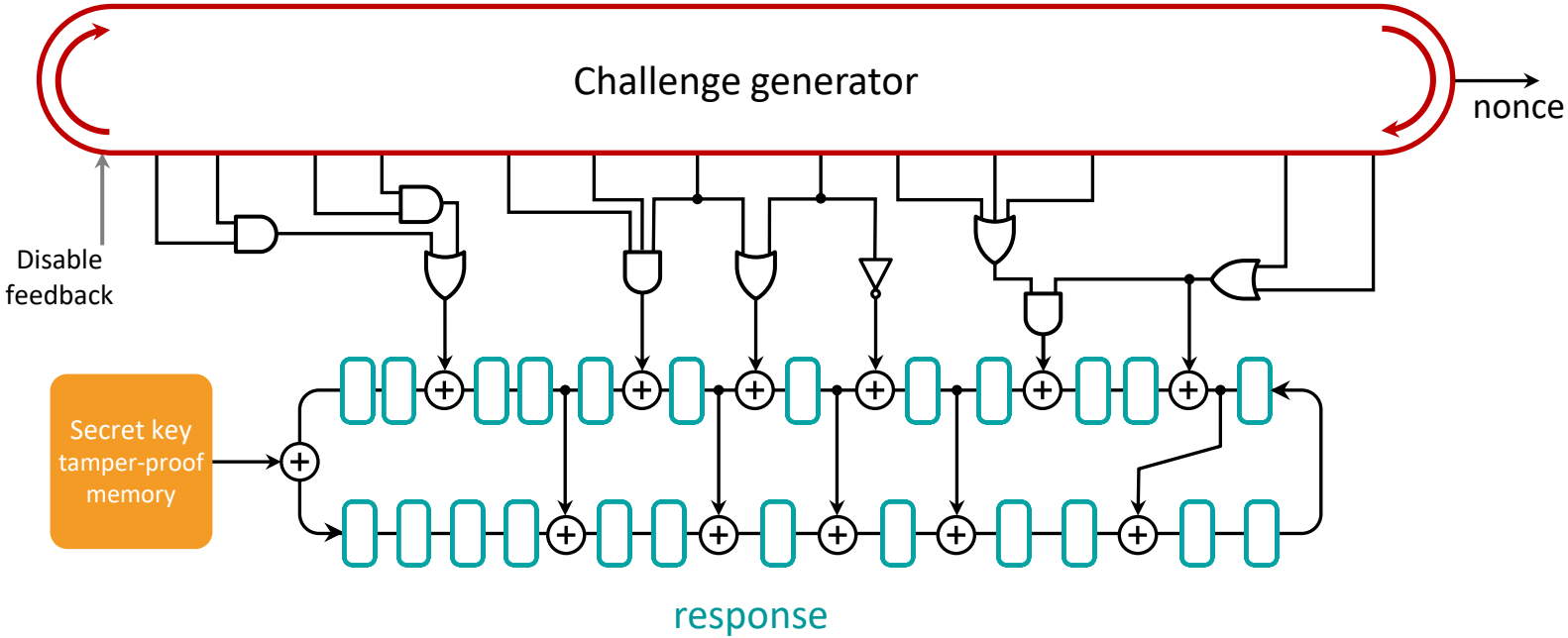
64-bit nonces




Testing challenge generators

- Hardware model
  - Xilinx Artix-7 FPGA
  - Digilent Arty Z7-200 board with a port to collect data
- Software event-driven simulator
- Statistical tests suites for 10^9-bit sequences
  - NIST SP800-22 (188 tests)
  - NIST SP800-90B (23 tests; permutation tests up to 10,000 times)
  - BSI AIS-31 (1290 tests)
- All tests passed by generators of different sizes
- Shannon entropy > 0.99999 (required 0.997)
- Min-entropy estimate based on collision counts > 0.99

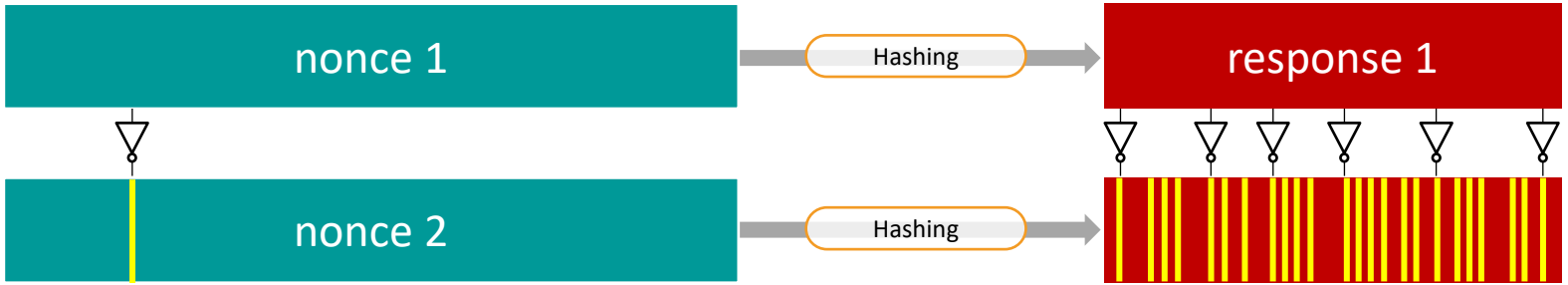
Hashing


Challenge generator
nonce
Disable
feedback
Secret key
tamper-proof
memory
response

Testing hash function

- Speed test – the average time it takes to hash
- Avalanche effect
- Collision test – find two different nonces with the same hash
- Pre-image – find a nonce corresponding to a given hash value
- Second pre-image – given a nonce find another nonce such that $H_1 = H_2$

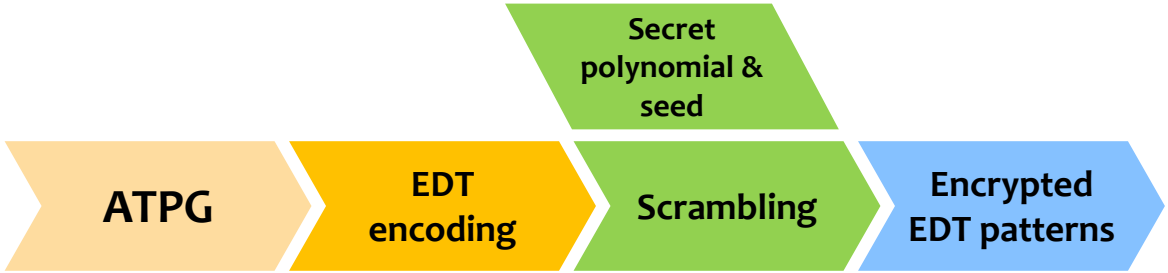
Avalanche effect



Nonce	Response	Cycles	Average	Deviation
64	47	300	23.5112	3.31815
	63	300	31.6007	3.8768
128	63	300	30.9967	4.00615
	127	500	63.0712	5.78218
256	127	500	63.3595	5.7497
	255	800	128.703	8.29533

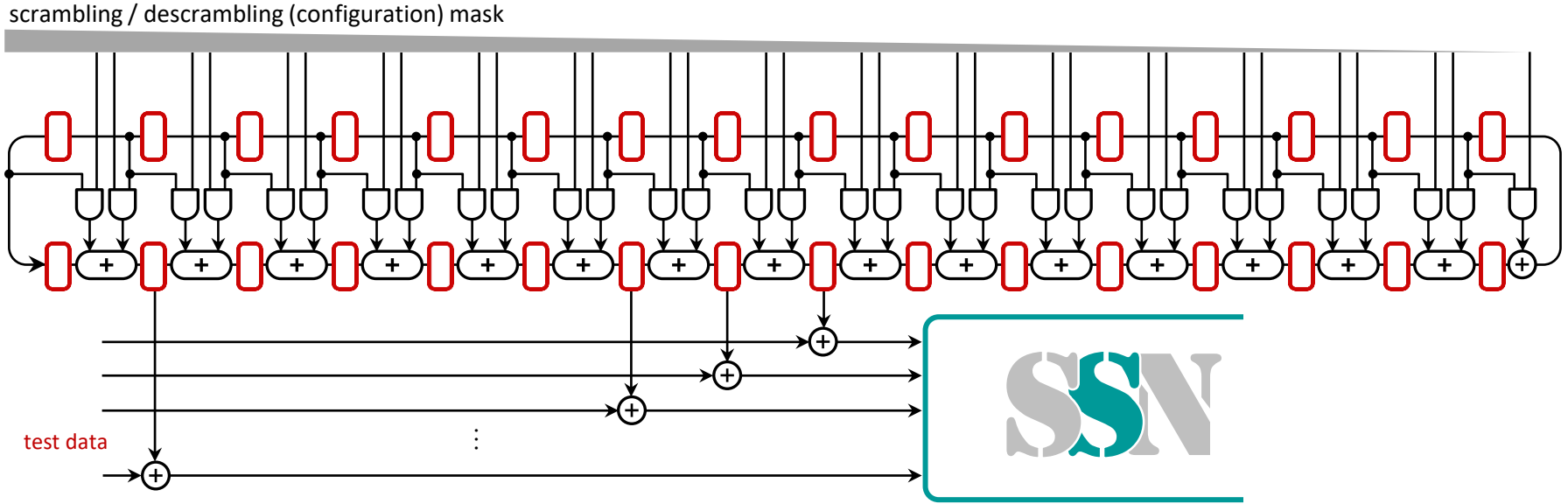
#samples: 500,000
#derivatives: 64 per nonce
1-Hamming distance from parent

ATPG encrypted patterns



Encrypting data going to and coming from a DUT makes eavesdropping ineffective

Scrambler / descrambler



- The Vernam stream cipher
- Very fast – has to match the SSN speed
- Can implement any polynomial
- Initial secret state applied during RoT reset

Security analysis

- EDT encoding
- SSN input-only streaming with MISR (no reference responses)
- SSN and IJTAG scrambling protocols
- Encrypted ATE test patterns
- On-chip decryption of stimuli, on-chip encryption of responses
- Authentication protocol
- Eavesdropping limited per device (electronic device ID)
- Unpredictable circuit behavior in unauthorized access

Conclusions

- Framework for secure access to DFT infrastructure
  - effective
  - efficient
  - synergistic
  - scalable
  - automatable
  - synthesizable
  - software model, not IP
- Validated key components in hardware and software