Entropy Sources – Practical Designs and Validation Challenges

Sonu Shankar and David McGrew

Agenda

- Background
- Ring Oscillators - Introduction
- RO-based Entropy Source Design Examples
- Sample Data
- Conditioners
- Design Observations, Sampling Challenges

Background

- Requirements span a wide range of applications, deployment scenarios and computational capabilities



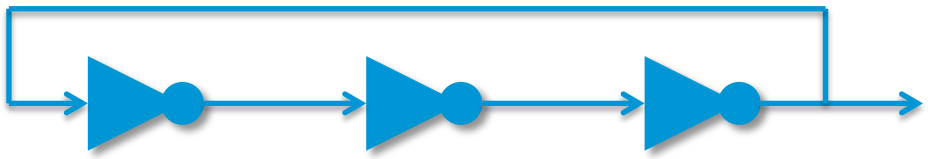




Background (continued)

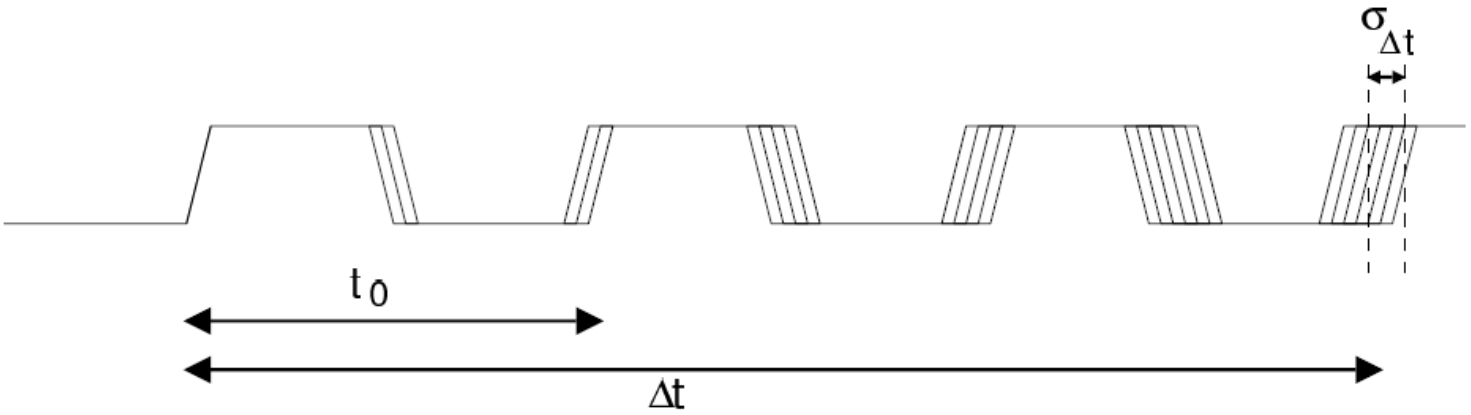
- Irrespective of application or deployment… quality of entropy sources must be consistently high across product portfolio
- Observations made –
  - Many entropy source designs exist in the industry
  - Quality of entropy sources and ability to assess entropy vary across designs
  - On-board hardware based entropy sources not always available
- Goal of this talk – Describe aspects of designs we encountered on entropy sources used across several embedded systems and challenges faced in preparation for assessment

Ring Oscillators



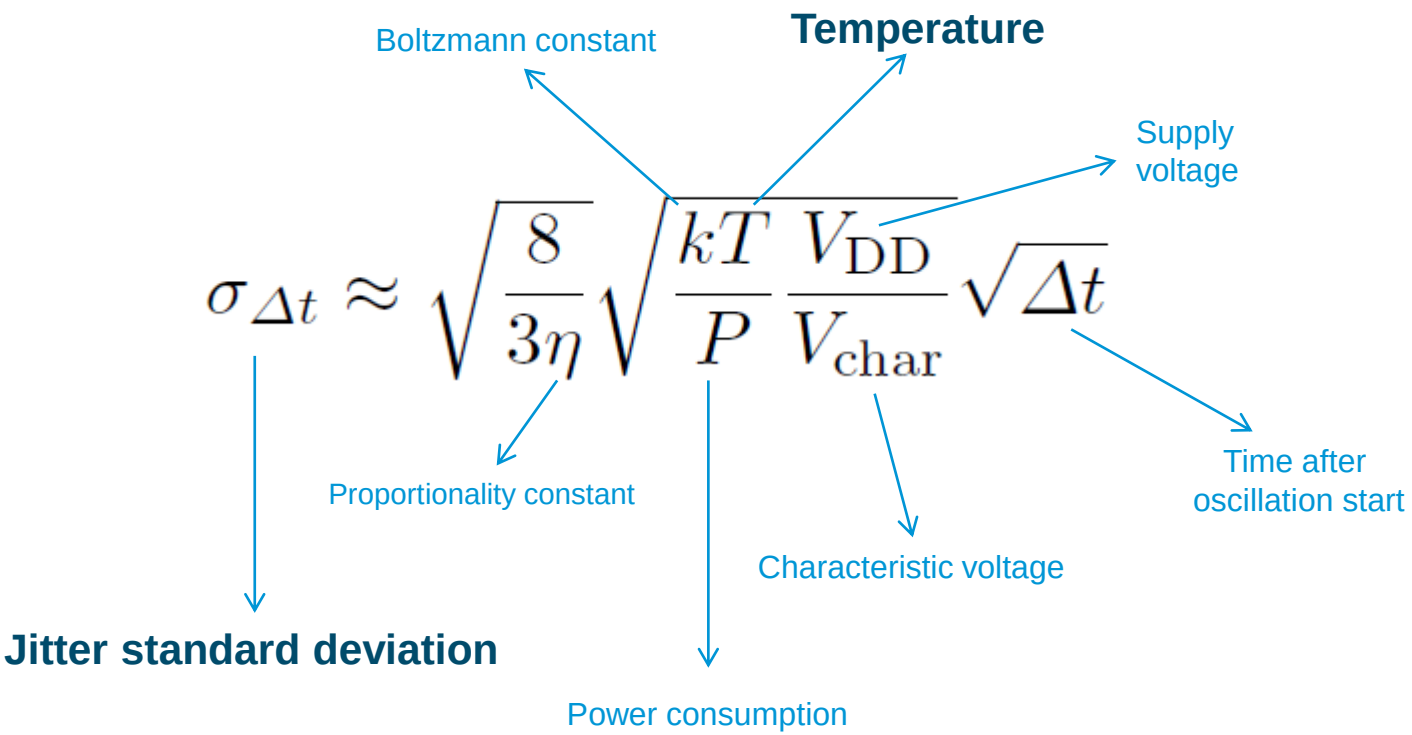
- Odd number of NOT gates connected in series with a wire inversion
- Output oscillates between two voltage levels
- Oscillations begin spontaneously above a threshold voltage

Ring Oscillators (continued)



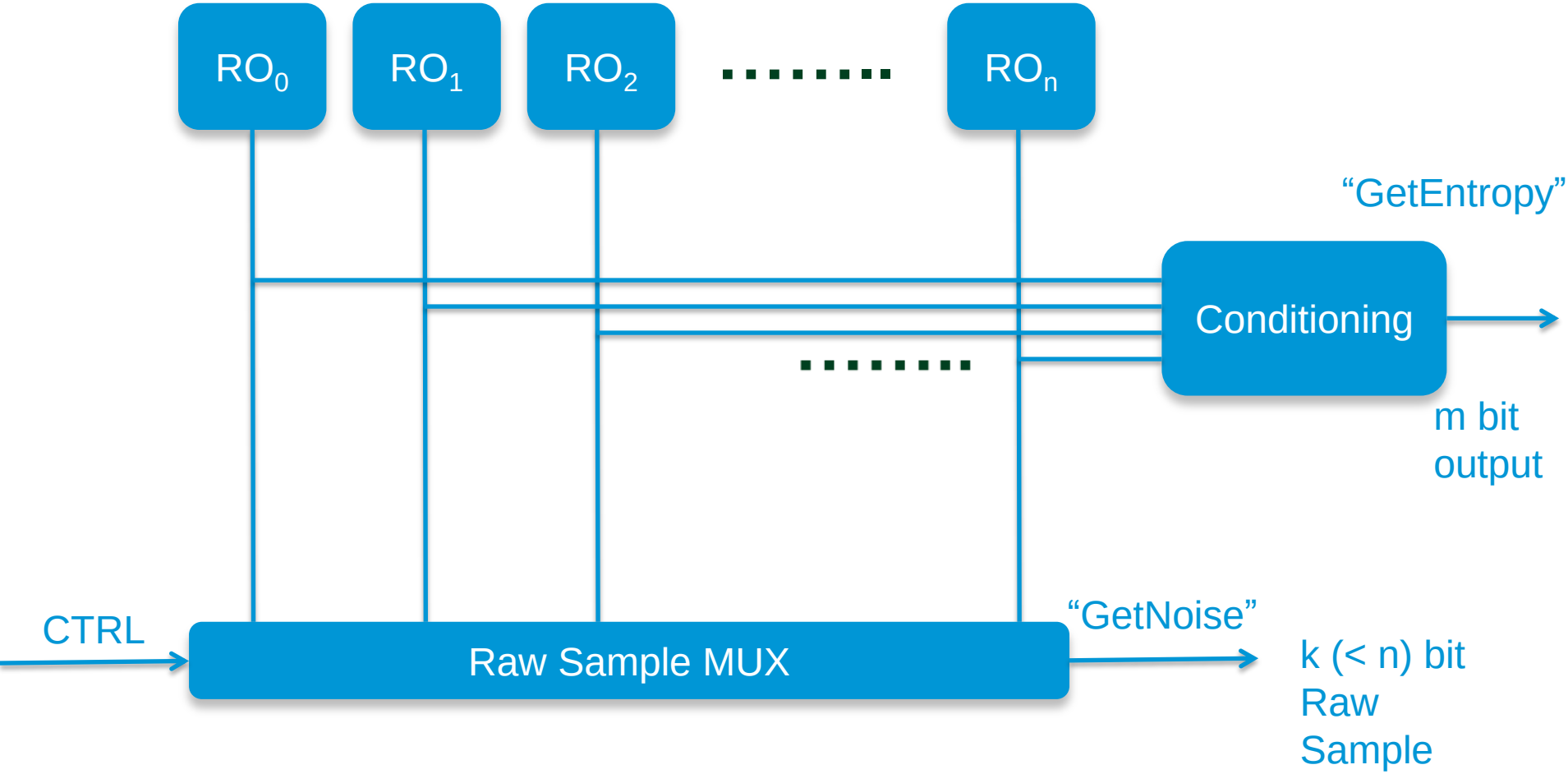
- Property exploited for entropy – Ring oscillator jitter (fluctuations in oscillator period due to electronic noise)
- Jitter causes increasing uncertainty in signal transition times

Ring Oscillators Jitter

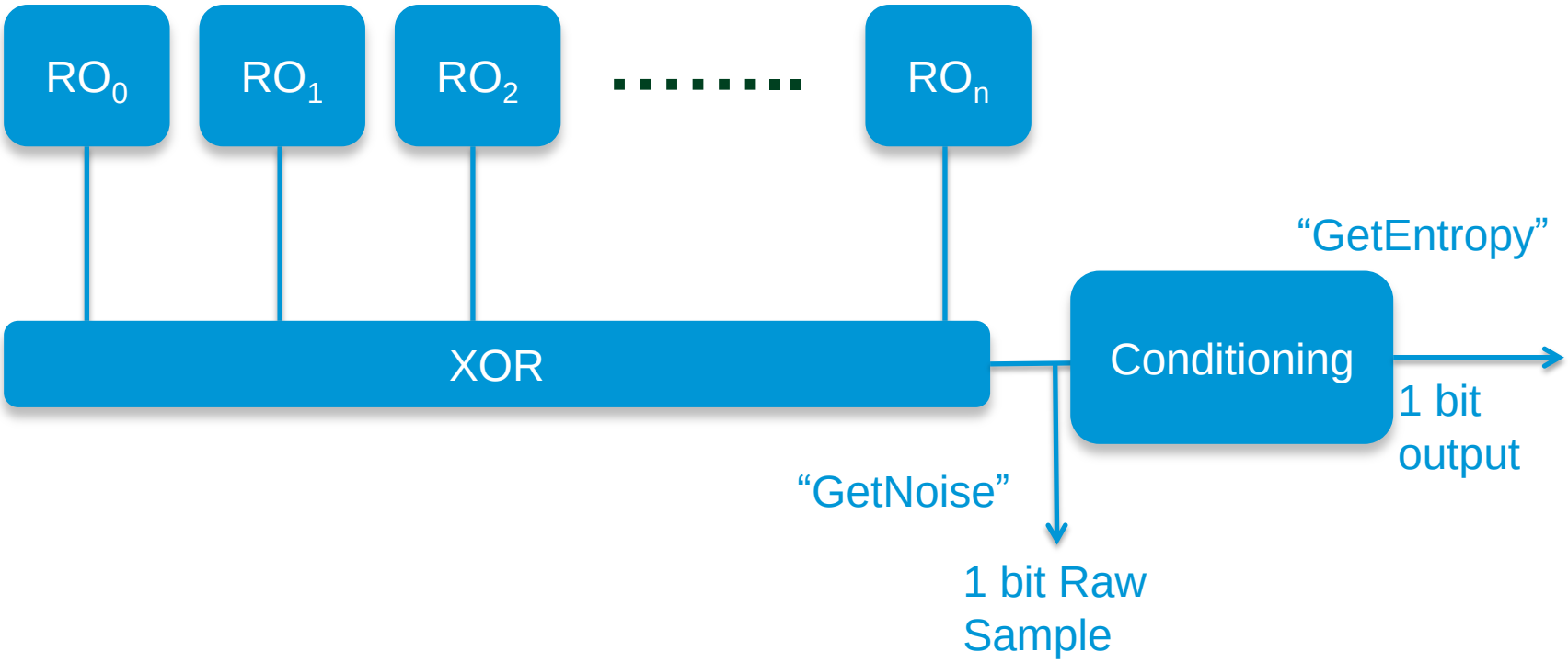


- Above is for a single-ended CMOS RO derived by Hajimiri et al. – "Jitter and Phase Noise in Ring Oscillators", *IEEE J. Solid-State Circuits 34(6) (1999) 790-804. (*Reference for equation and figure on prev slide*)*

Generic RO-based design



Generic RO-based design (continued)



Sample Data

```
5ca2 5d86 6996 6996 ac53 8d72 897e c13e
38c7 08b7 4cb2 4db2 5ea1 5ea1 5aa5 52ac
51a6 5927 9845 ba41 46b9 4678 8f50 bf40
7086 59a6 5d22 8d72 6e11 fb04 db24 9b64
e01f e817 2cd1 1ee1 08b7 4837 d823 dc0b
ce31 cc33 cc37 a857 d32c 9b64 0bd4 2bd0
10e9 36c8 3788 7718 f409 d22d 92fd 02fd
3b54 eb10 ef10 ef38 46b9 06f9 06f9 06d1
ab10 ef10 6f80 5fa2 759b 649b 4cb7 0af5
8c73 8c71 8a65 fa8d 4788 f708 f30c f304
3fc0 3ee5 1ae5 4ab5 27d8 25d2 2dc2 5da2
ce33 dc23 d42b 10cf 46e9 13e6 39c6 b946
a34c b34d f609 f68b 13ec 136c 936c a51b
9c68 9768 9768 d30c a05f 807b 857a c53a
b64d b24d b26d d22c 59a6 59a6 59a6 19e2
ed14 eb14 6b9c 43bc 00ff 827d 827d 8a65
```

Sample Data

```
5ca2 5d86 6996 6996 ac53 8d72 897e c13e
38c7 08b7 4cb2 4db2 5ea1 5ea1 5aa5 52ac
51a6 5927 9845 ba41 46b9 4678 8f50 bf40
7086 59a6 5d22 8d72 6e11 fb04 db24 9b64
e01f e817 2cd1 1ee1 08b7 4837 d823 dc0b
ce31 cc33 cc37 a857 d32c 9b64 0bd4 2bd0
10e9 36c8 3788 7718 f409 d22d 92fd 02fd
3b54 eb10 ef10 ef38 46b9 06f9 06f9 06d1
ab10 ef10 6f80 5fa2 759b 649b 4cb7 0af5
8c73 8c71 8a65 fa8d 4788 f708 f30c f304
3fc0 3ee5 1ae5 4ab5 27d8 25d2 2dc2 5da2
ce33 dc23 d42b 10cf 46e9 13e6 39c6 b946
a34c b34d f609 f68b 13ec 136c 936c a51b
9c68 9768 9768 d30c a05f 807b 857a c53a
b64d b24d b26d d22c 59a6 59a6 59a6 19e2
ed14 eb14 6b9c 43bc 00ff 827d 827d 8a65
```

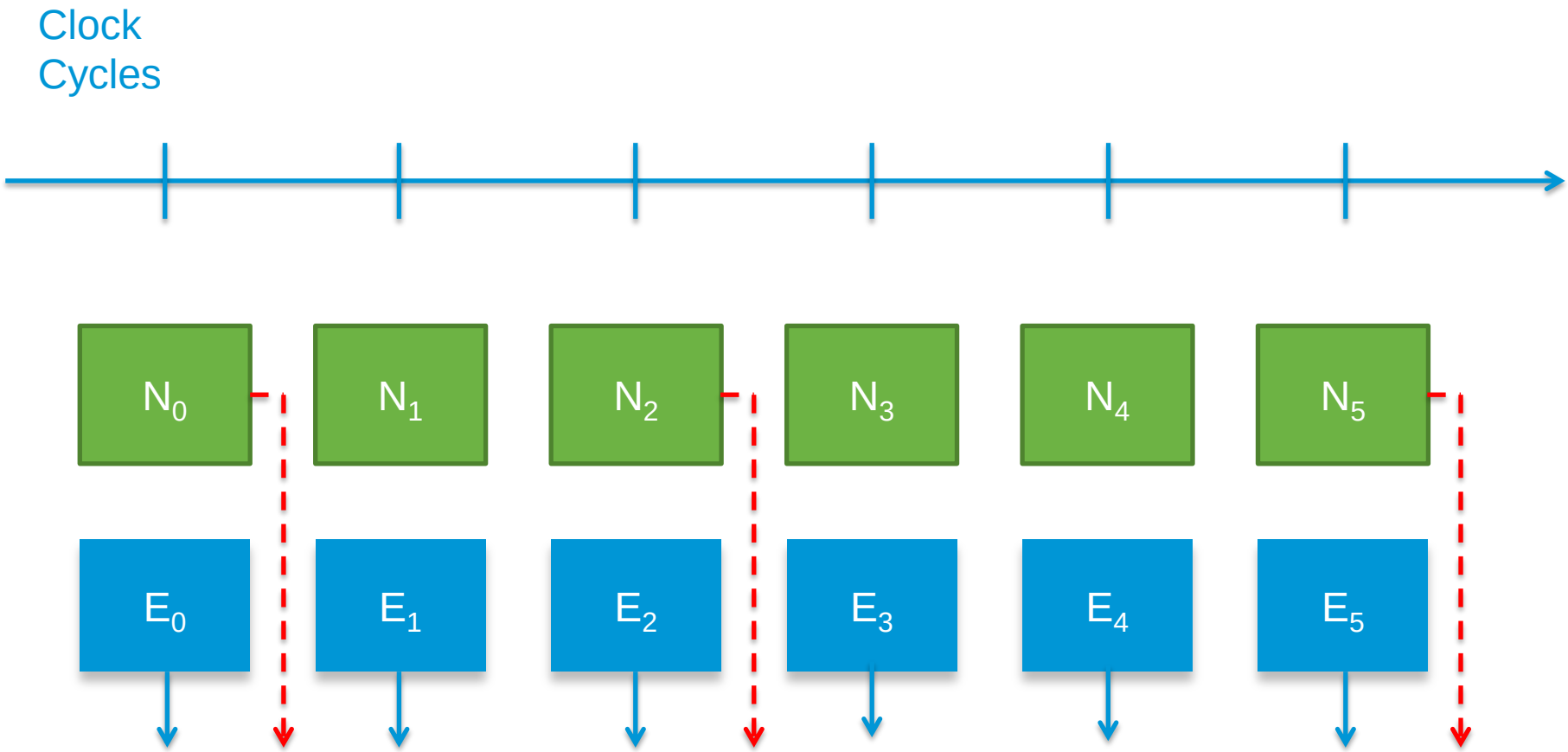
Conditioners

- Conditioners used to generate unbiased output
- SHA-1 engine
- LFSR (shift register w/ input linear function of previous state)
- Combination of SHA-1 and LFSR

Design Observations, Sampling Challenges

- Most entropy source designs are based on ring oscillators
- Access to raw noise samples is rare
- Consecutive raw noise sampling is non-trivial or impossible

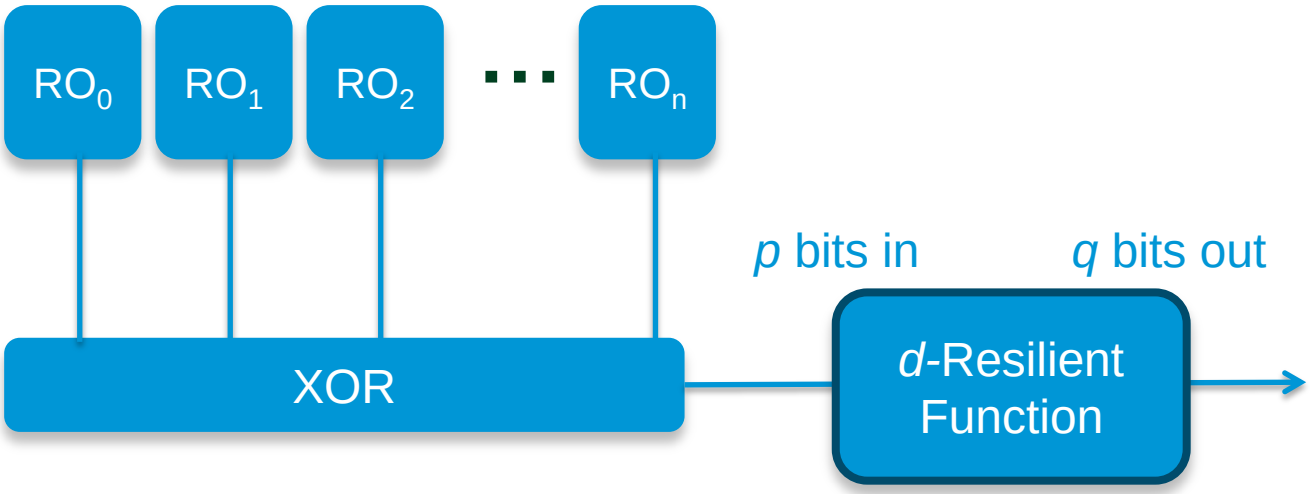
Intermittent access to raw noise samples



Design Observations, Sampling Challenges

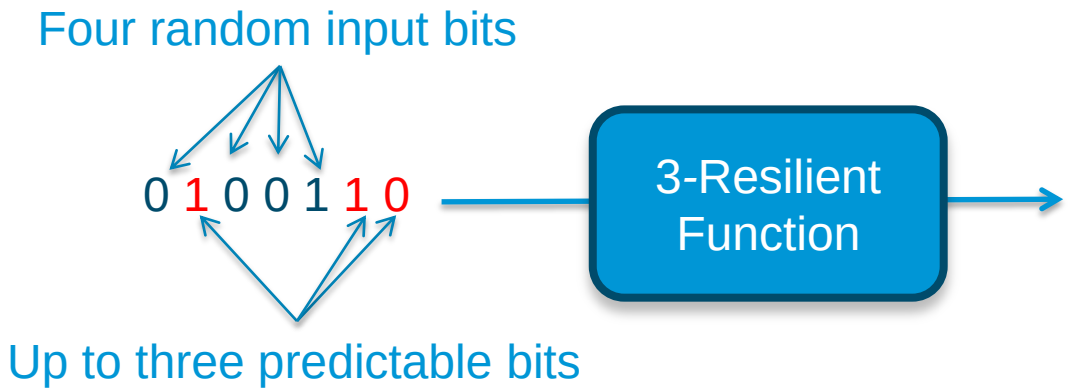
- Access to entire conditioner input unavailable in all cases
- Individual RO outputs not accessible in all cases
- Resilient functions as conditioners not used in practice

Resilient Functions as Conditioners

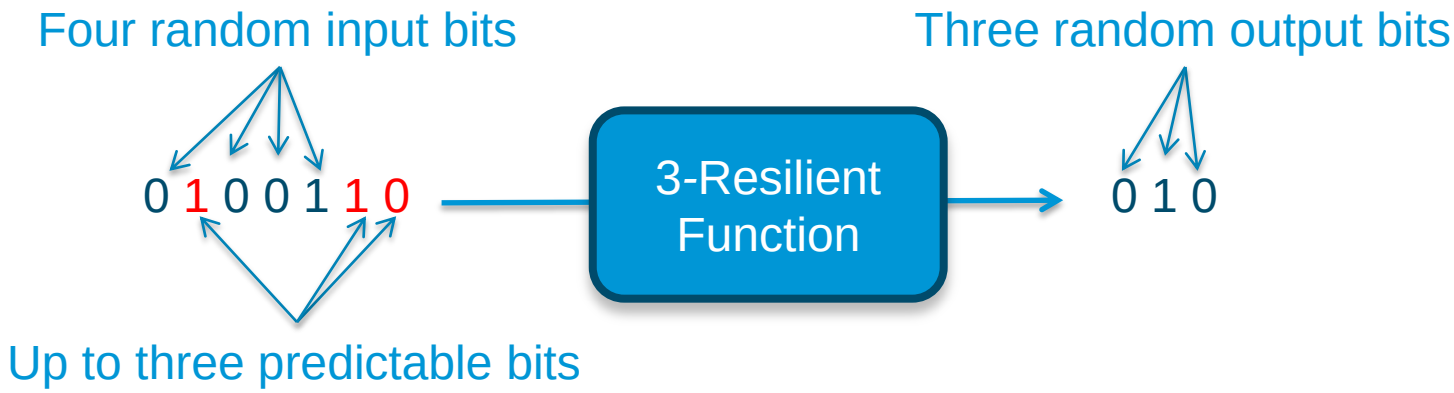


Sunar, Martin, and Stinson. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on Computers*, 58:109–119, 2007.

Resilient Functions as Conditioners



Resilient Functions as Conditioners



Thank you.