Security in Future 5G Systems

Georg Sigl

Technical University of Munich

Faculty for Electrical and Computer Engineering

Institute for Security in Information Technology

Contents

- Applications for future 5G networks
- Security implications and research challenges
- Attacks on devices

Applications for future 5G networks

THE TACTILE INTERNET

Prof. Dr.-Ing. Thomas Wiegand, HHI

source: https://netzoekonom.de

Fraunhofer HHI

1

Presentation of T. Wiegand at Fraunhofer Institute Director‘s Meeting October 2015 in Hamburg

Security implications

- **IoT** → Every Thing needs an identity
  → Every Thing needs integrity, authenticity, (confidentiality)
  → Secure storage of identities and keys
- **Low latency** → Cryptography with low latency
- **Low power** → Cryptography with short block length
- **Safety** → Integrity and Authenticity of all involved components

Security implications

- **IoT** → Every Thing needs an identity
  → Every Thing needs integrity, authenticity, (confidentiality)
  → Secure storage of identities and keys
- **Low latency** → Cryptography with low latency
- **Low power** → Cryptography with short block length
- **Safety** → Integrity and Authenticity of all involved components

PUFs for identification and authentication

Classic

„Unique“
Physical Property

+

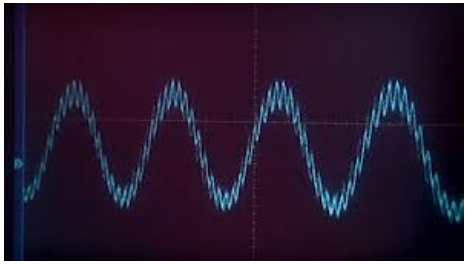
Measurement
Method

=

Authentication,
Key Generation

Silicon

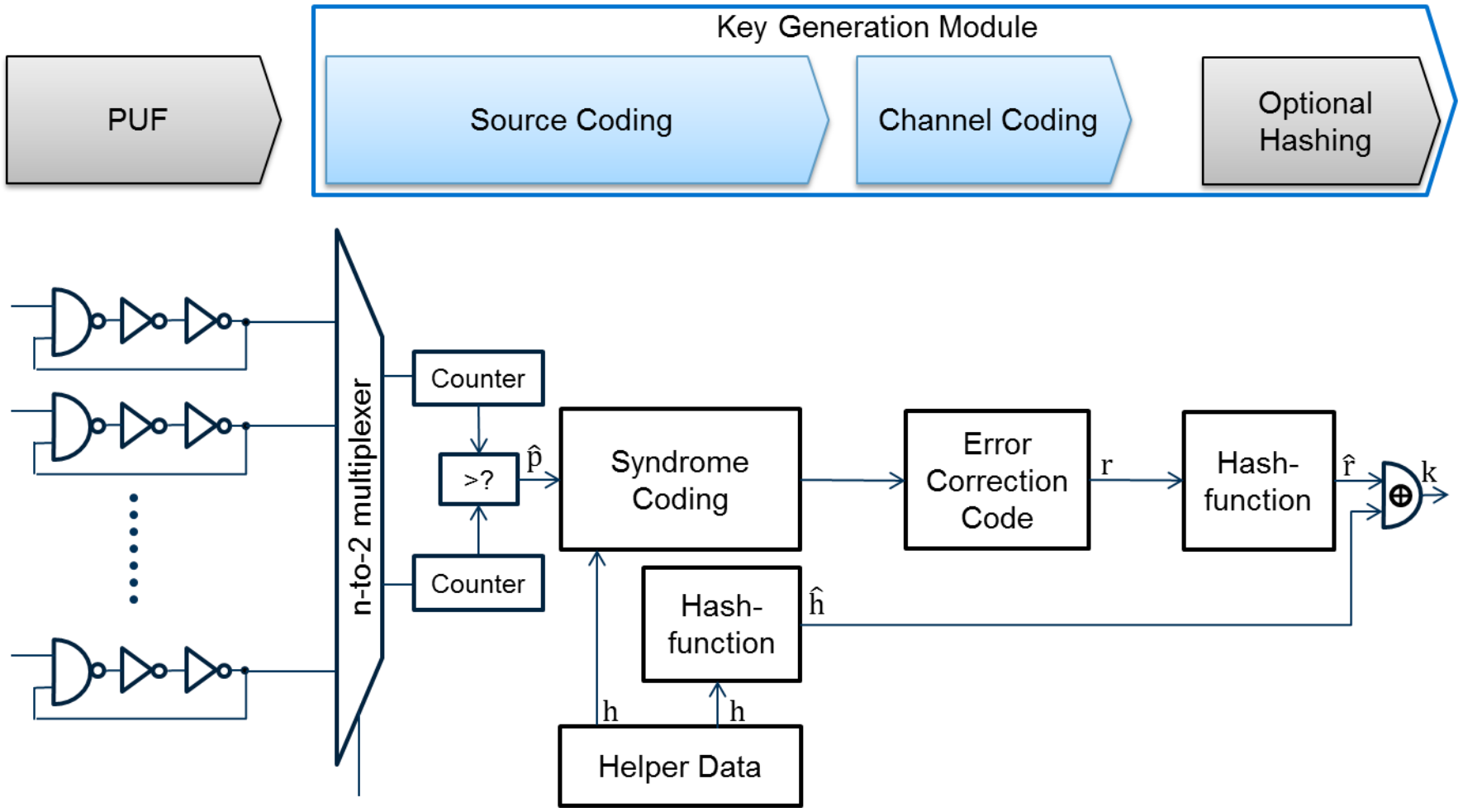
+



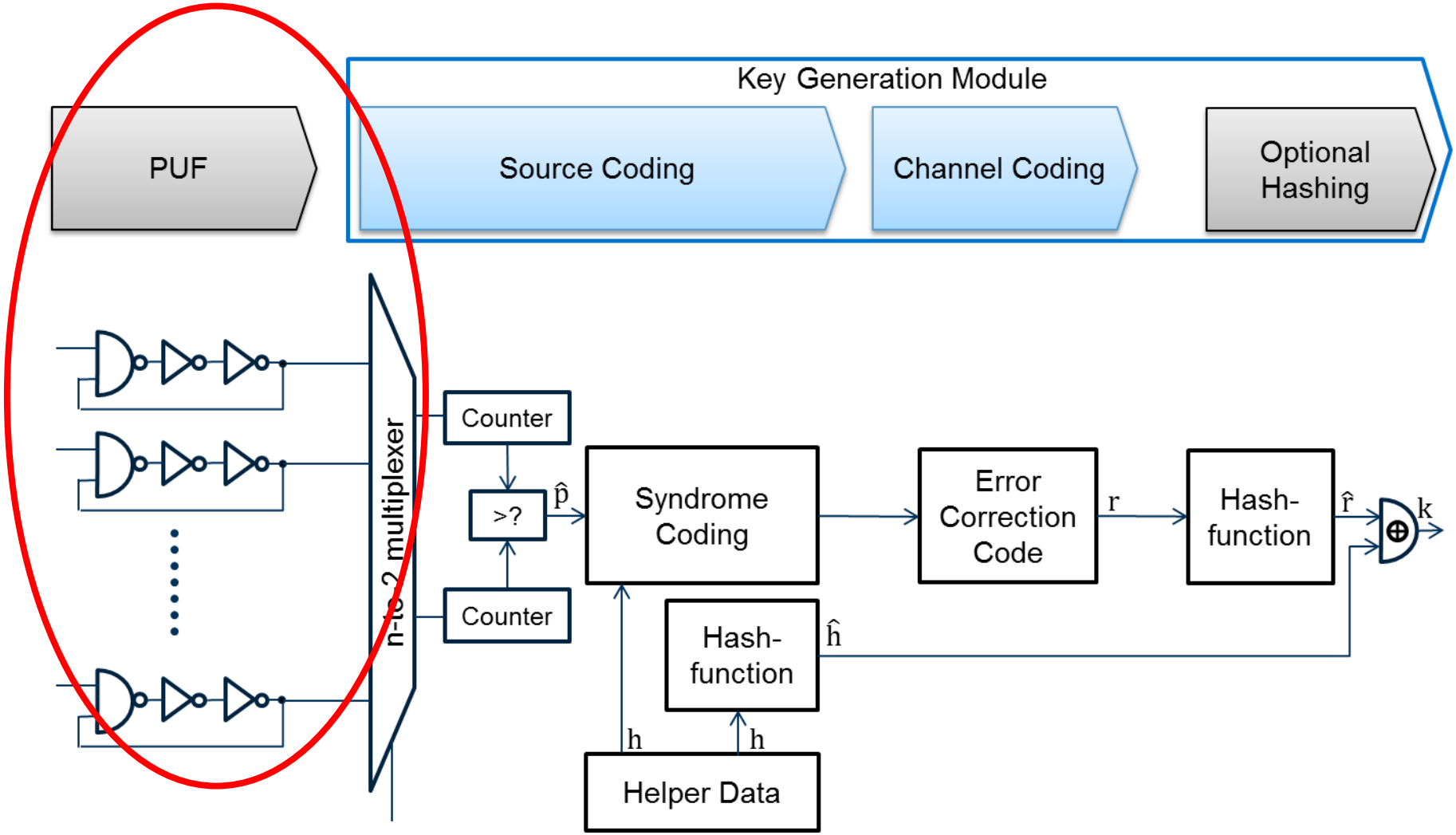
=

PUF
Physical
Unclonable
Function

Components of a PUF Key Generator



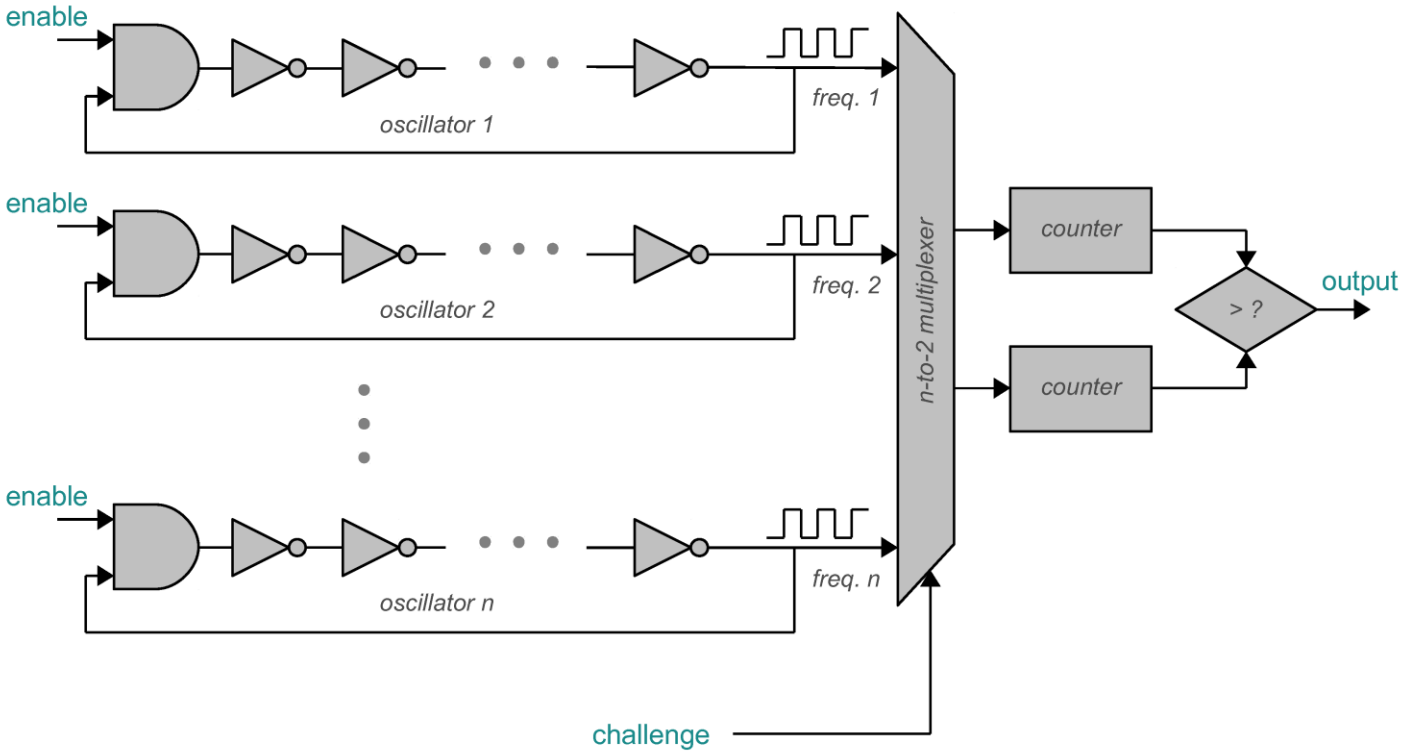
Components of a PUF Key Generator



Ring Oscillator PUF (Suh and Devadas, 2007) *

Ring oscillator frequencies depend on manufacturing variations

Two ROs are compared to obtain a response bit

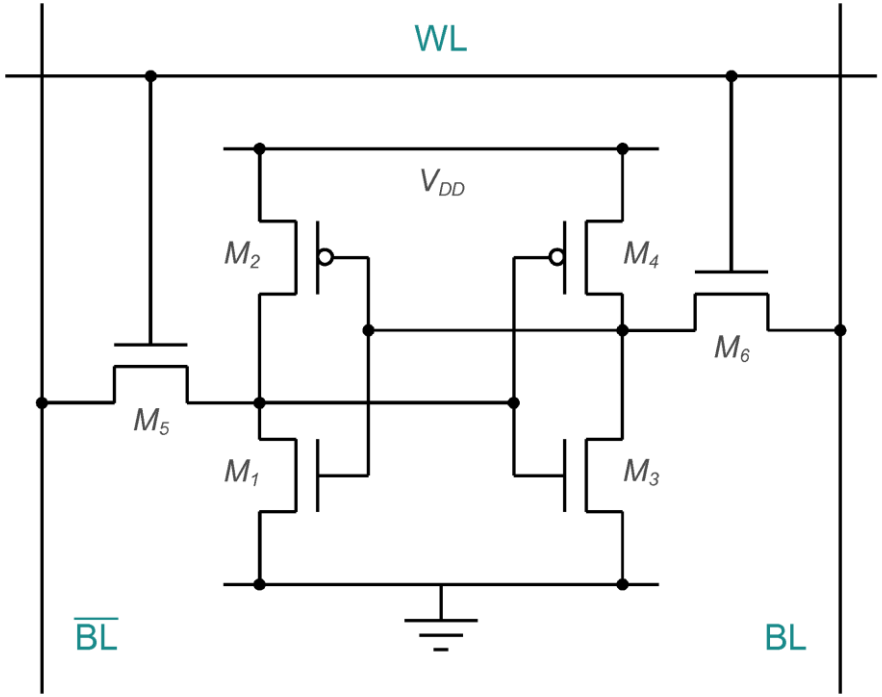


* G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. Design Automation Conference, 2007. DAC '07. 44th ACM/IEEE, pages 9–14, 2007.

SRAM PUF (Guajardo et al., 2007) *

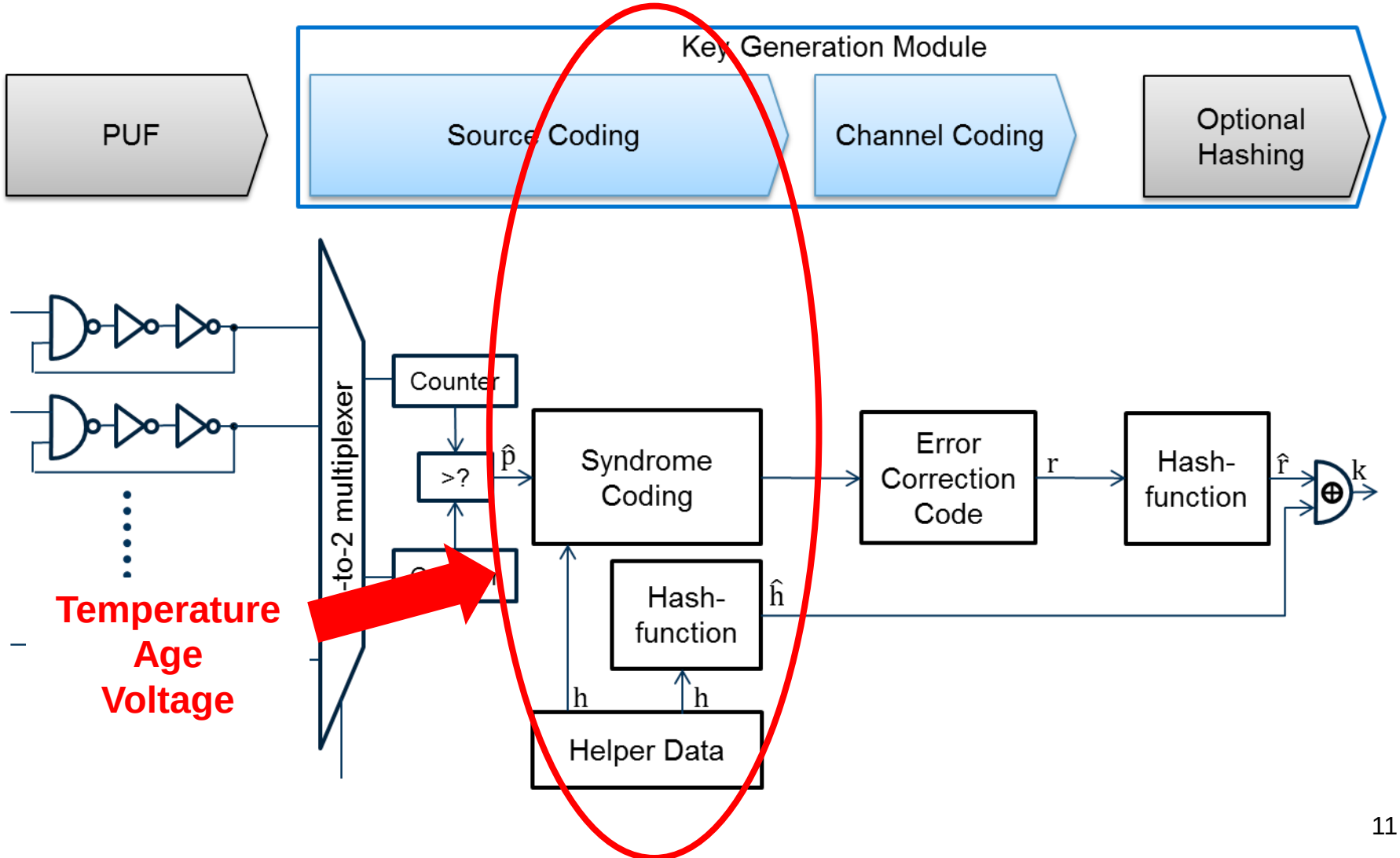
Symmetric circuit balance influenced by manufacturing variations

SRAM cells show a random, but stable value after power-up

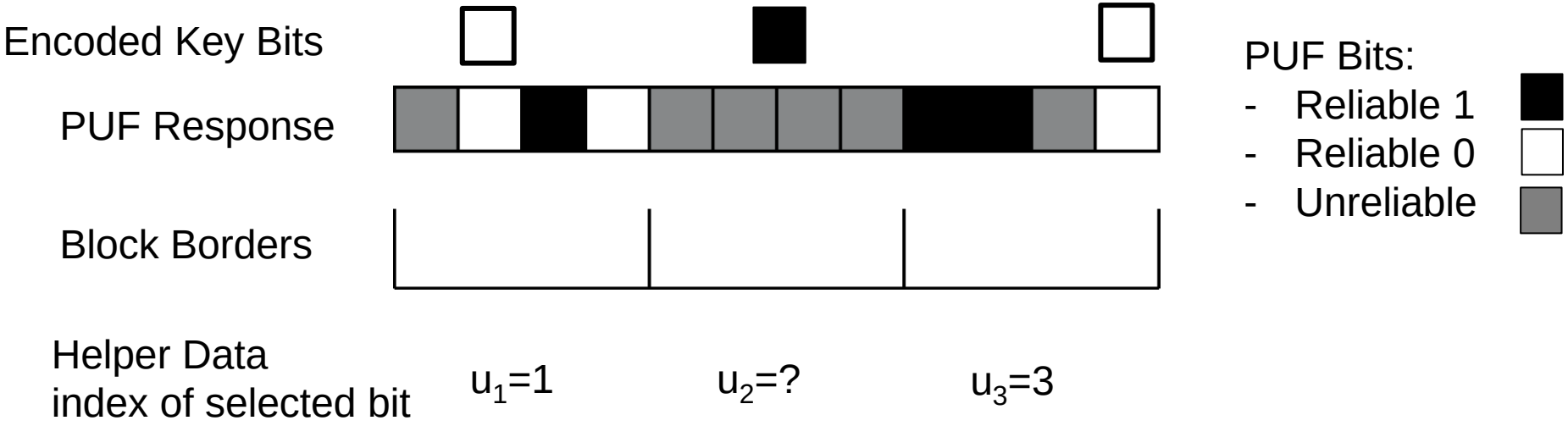


* J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls. FPGA intrinsic PUFs and their use for IP protection. In CHES 2007, volume 4727 of LNCS, pages 63–80. Springer, 2007

Components of a PUF Key Generator



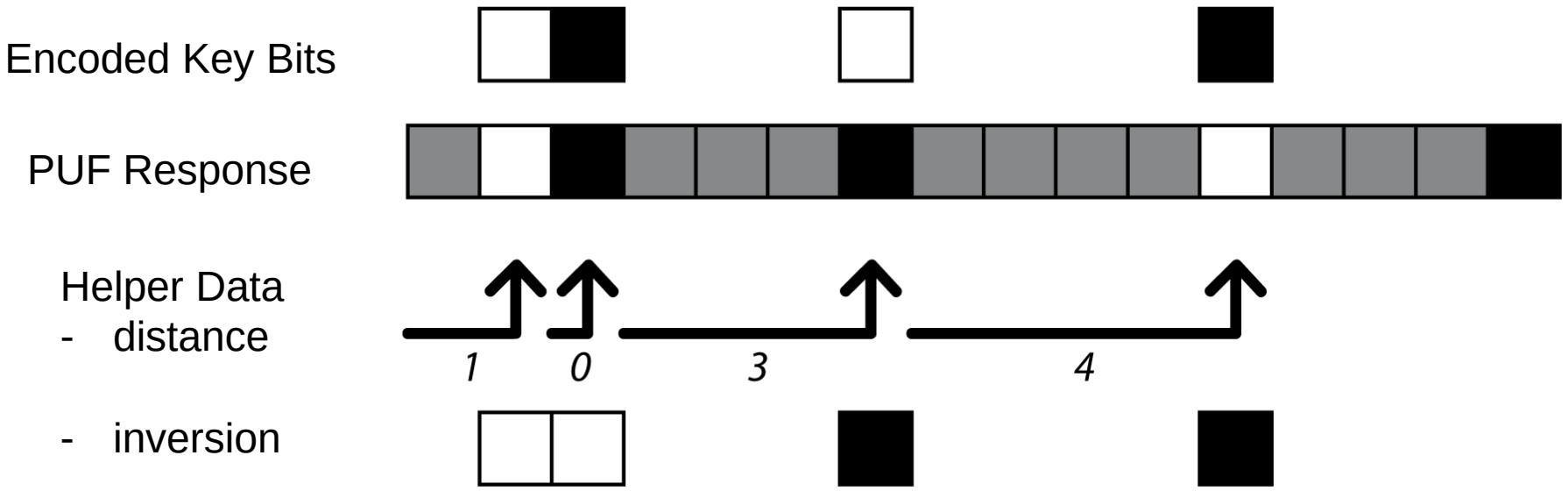
State of the Art in error correction



- All error correctors work on fixed block structure:
  e.g. IBS (Yu and Devadas, 2010 *)
- Goal: find one white and one black square in each block of four
- Helper data store the indices of selected bits

* M.-D. Yu and S. Devadas, Secure and robust error correction for physical unclonable functions, IEEE Design & Test of Computers, vol. 27, no. 1, pp. 48-65, 2010

Differential Sequence Coding *



- No fixed block borders
- Helper data store distance to next bit and an inversion indicator
- Larger blocks of unreliable bits can be skipped
- Very efficient error corrector scheme for high error rates

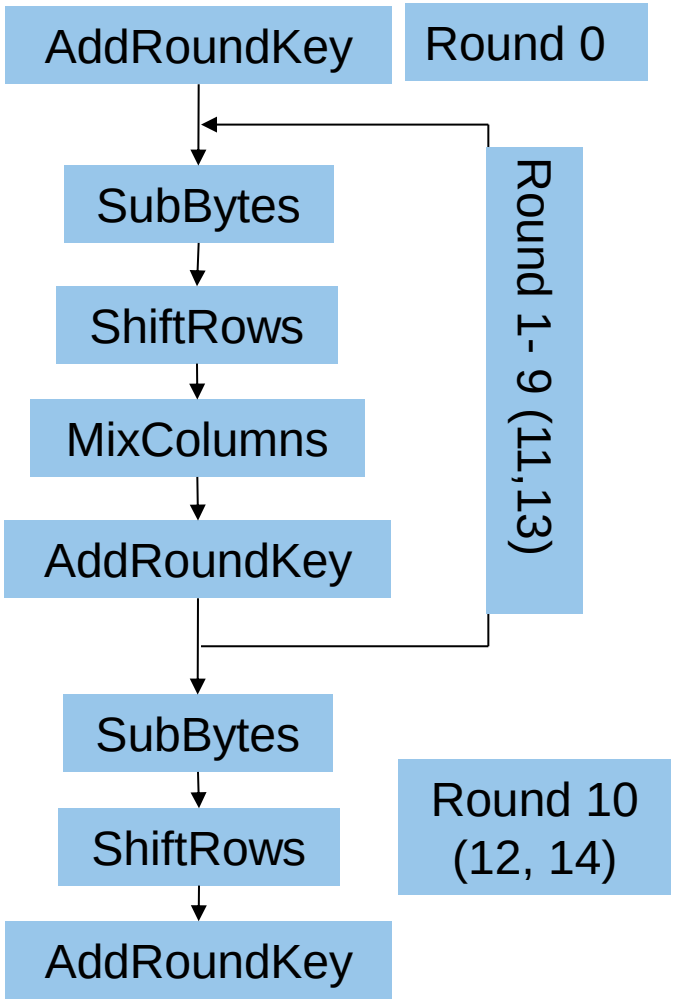
* M. Hiller, M. Weiner, L. Rodrigues Lima, M- Birkner and G. Sigl. Breaking through Fixed PUF Block Limitations with Differential Sequence Coding and Convolutional Codes, TrustED, 2013

Security implications

- **IoT** → Every Thing needs an identity
  → Every Thing needs integrity, authenticity, (confidentiality)
  → Secure storage of identities and keys
- **Low latency** → Cryptography with low latency
- **Low power** → Cryptography with short block length
- **Safety** → Integrity and Authenticity of all involved components

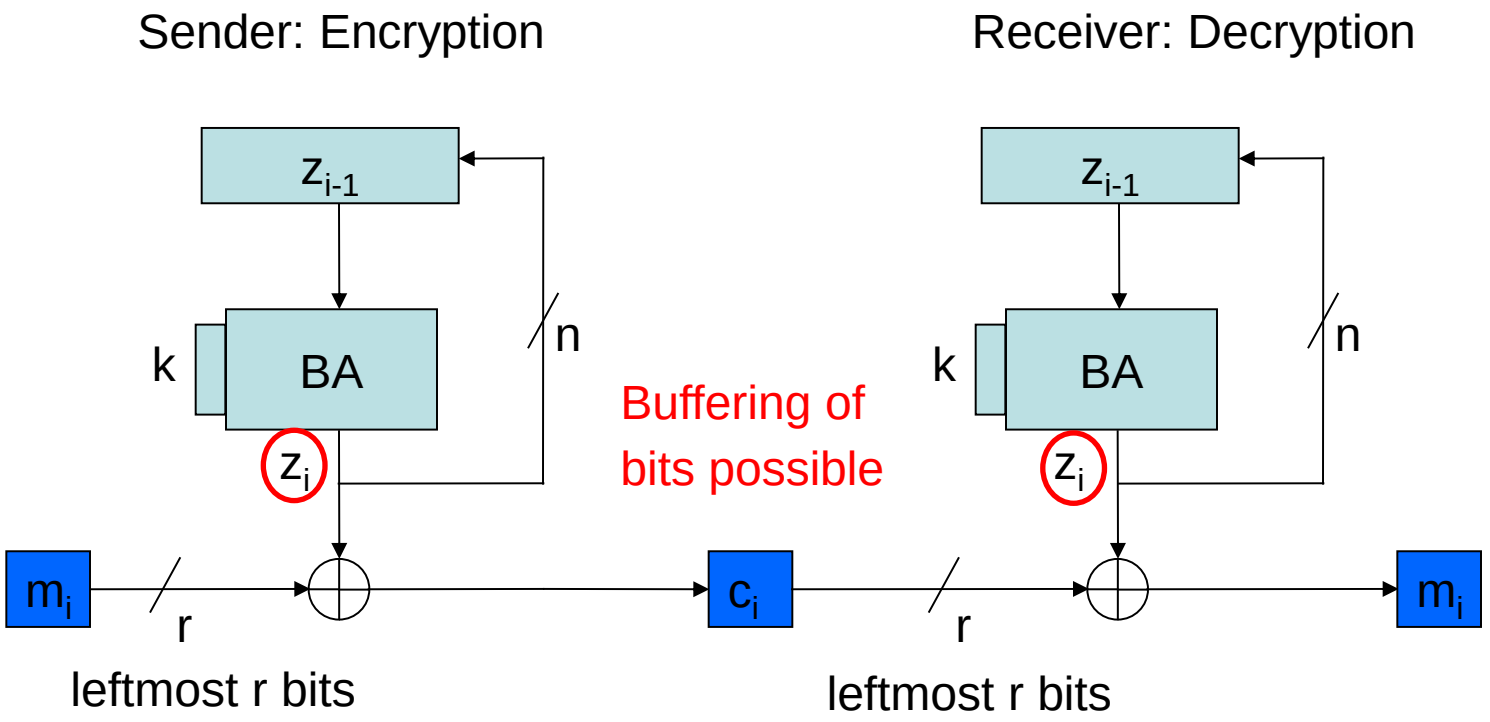
Typical symmetric cypher

- Diffusion and non-linearity required
- Usually several rounds
- All rounds could be combined in one cycle
  - Combinational path would be too long
- In AES we have a minimal latency of 10 clock cycles
- Implementations with 500 MHz to 2 GHz seem to be possible → 5 to 20ns latency added
- Low power implementations with ~10 MHz → 1µs latency
- Protected implementations need longer!



Possible solution: Output Feedback Mode

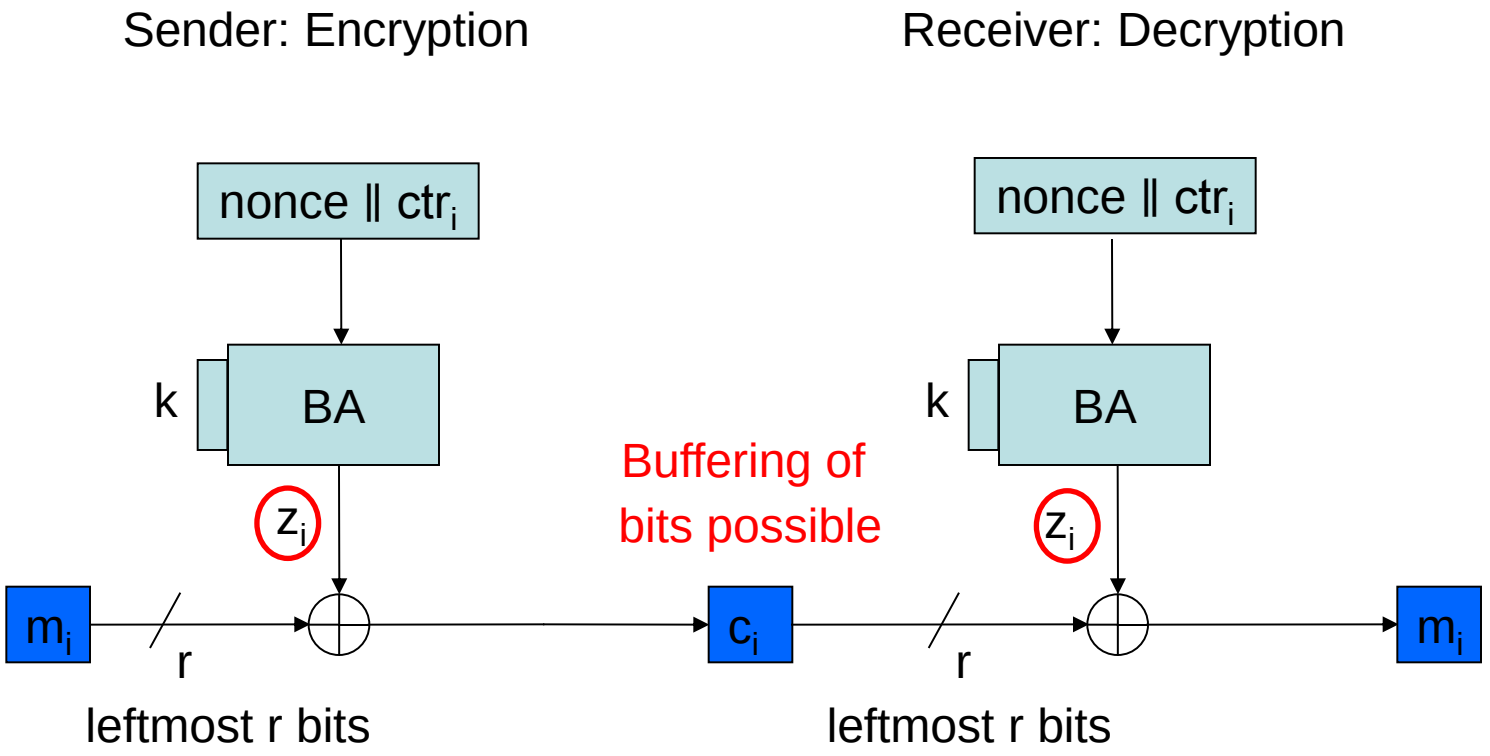
$z_i=BA(z_{i-1}),\quad c_i=z_i \oplus m_i,\quad m_i=z_i \oplus c_i,\quad z_0=IV$



Possible solution: Counter Mode

$z_i = BA(nonce \| ctr_i)$, $c_i = z_i \oplus m_i$, $m_i = z_i \oplus c_i$

IV = nonce := “number used once”



Security implications

- **IoT** → Every Thing needs an identity
  → Every Thing needs integrity, authenticity, (confidentiality)
  → Secure storage of identities and keys
- **Low latency** → Cryptography with low latency
- **Low power** → Cryptography with short block length
- **Safety** → Integrity and Authenticity of all involved components

Block length versus power

- Power for sending a bit dominates whole power consumption
  Around a factor of 10 more power for sending than calculation
- The block length is the minimum amount of bits, which can be encrypted
- Problem: if we want to transmit only one bit of information, we have to send a complete block?
- Stream ciphers (like OFB and CTR mode) can encrypt any number of bits → they are better for low bit counts
- Next problem: Brute force attacks!
- Information should be 64 bit or more to have sufficient security against brute force
- Questions:
  - Are there similar requirements for error correction?
  - Can we combine crypto and error correction?