ulm university universität ulm

A New Error Correction Scheme for Physical Unclonable Functions

Sven Müelich, Martin Bossert

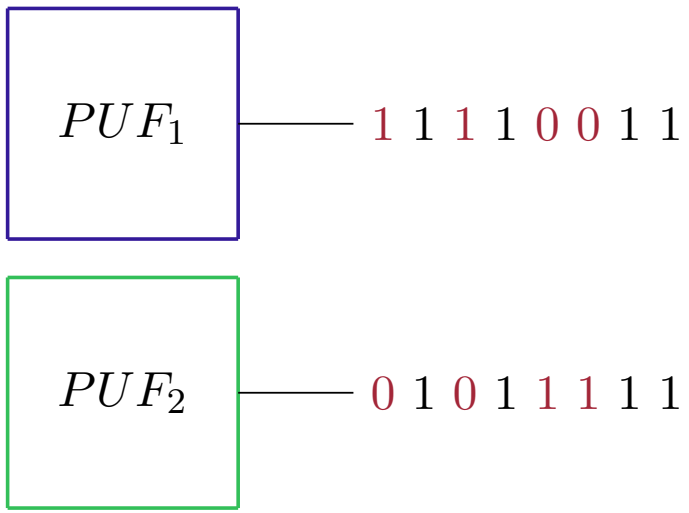
Institute of Communications Engineering, Ulm University, Germany

SCC 2017
Hamburg, February 6-9, 2017

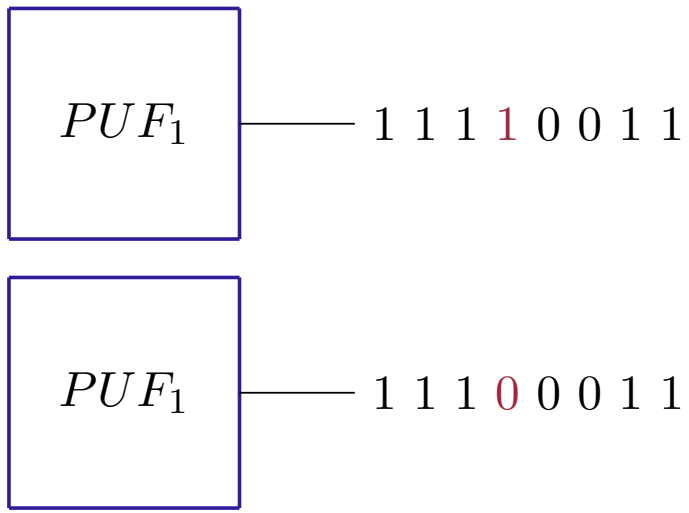
Outline

What is a PUF?

- Physical device from which a reproducible random bit sequence can be extracted

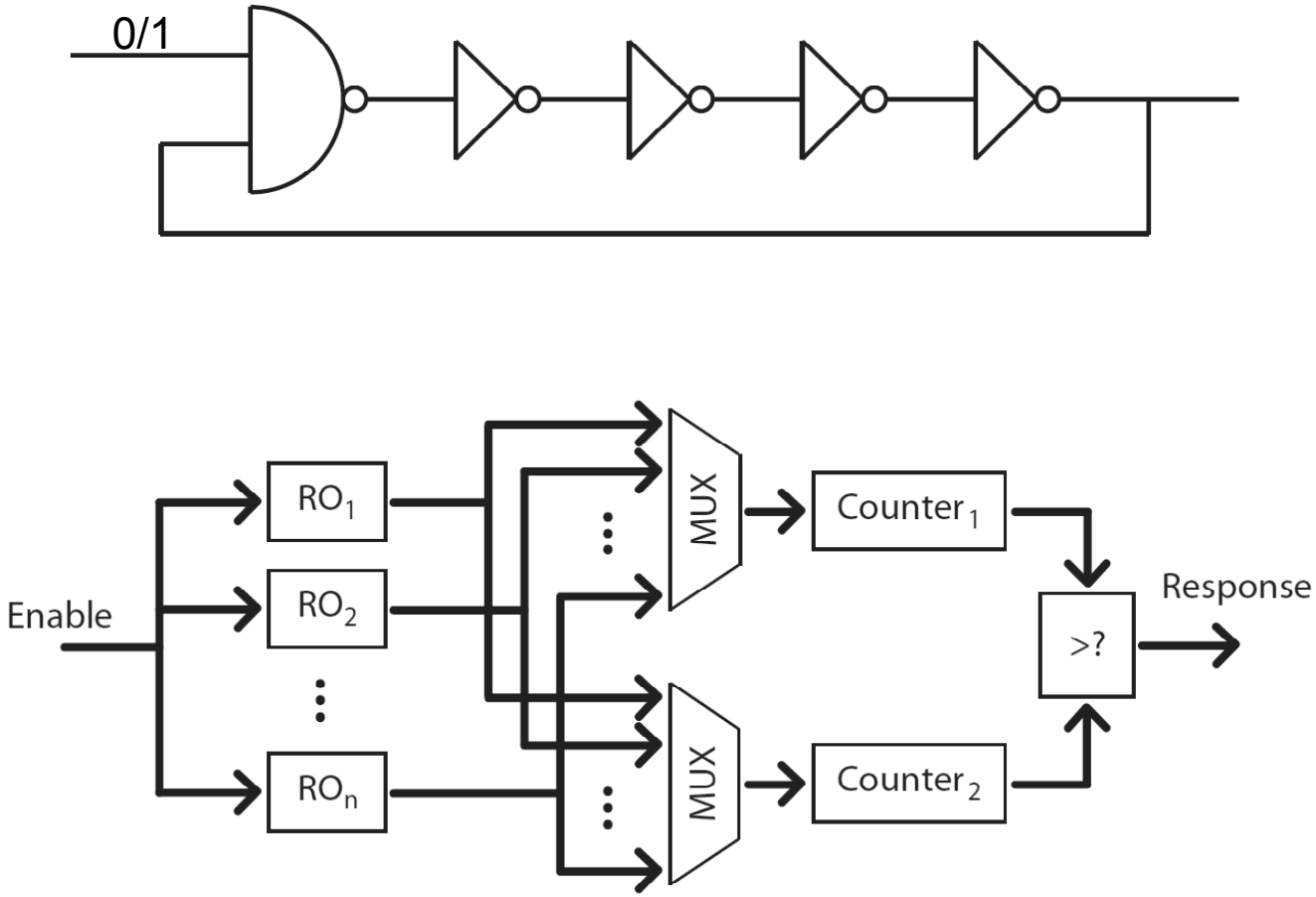


Uniqueness and Unclonability



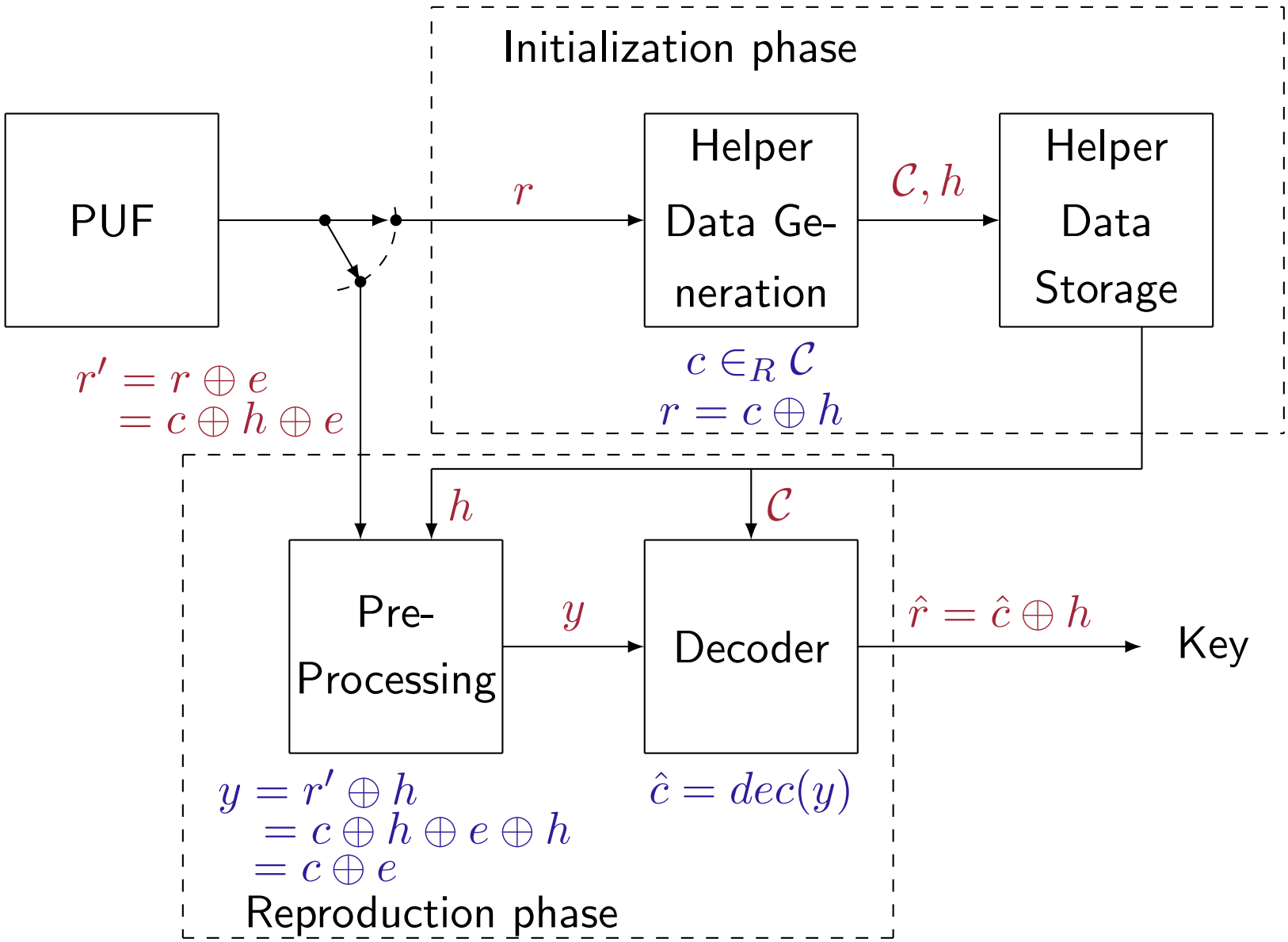
Reproducibility

Example: Ring-Oscillator PUF (ROPUF)

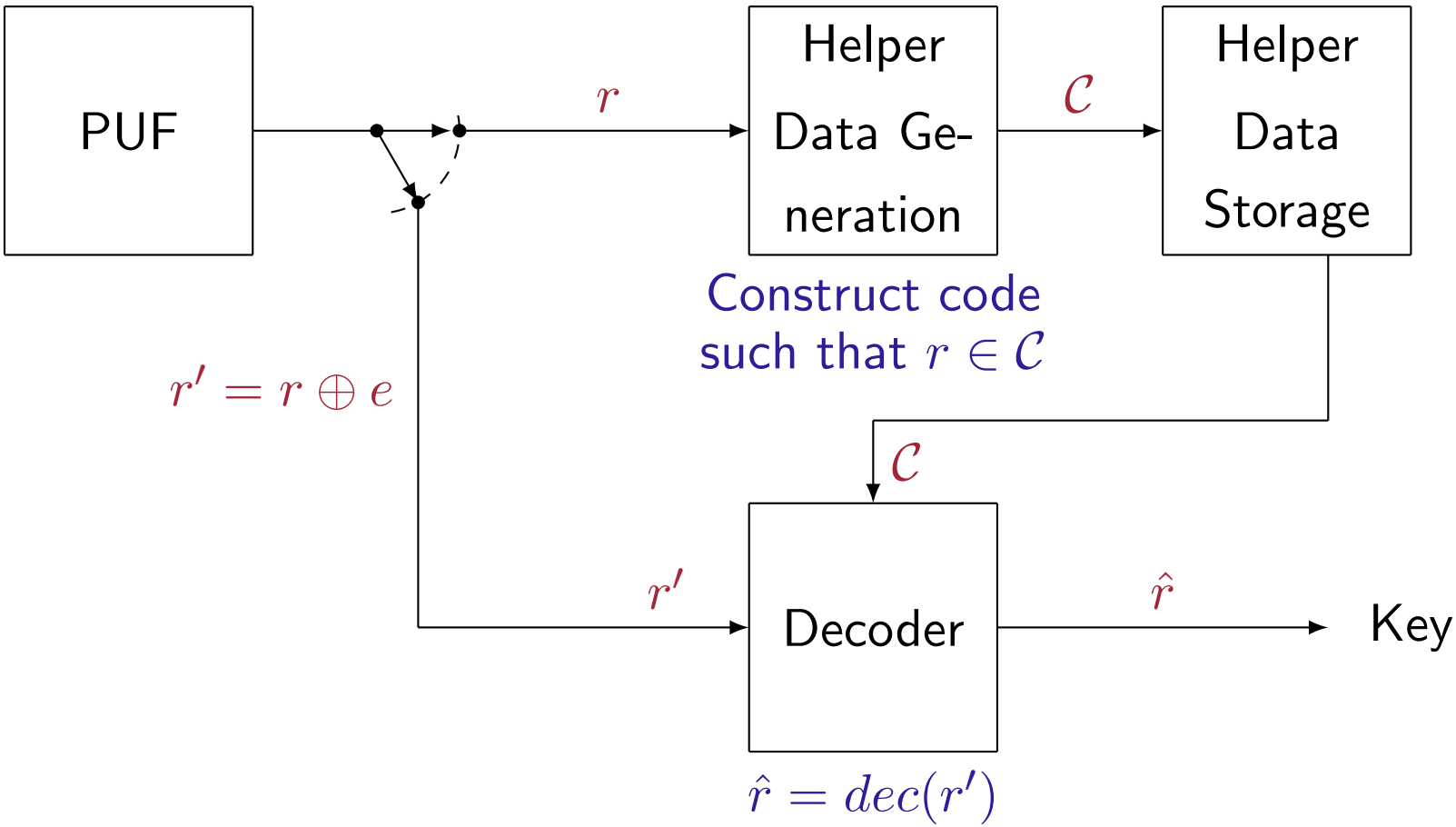


Matthias Hiller, Georg Sigl, and Michael Pehl: A New Model for Estimating Bit Error Probabilities of Ring-Oscillator PUFs

Helper Data Algorithms: Code-Offset

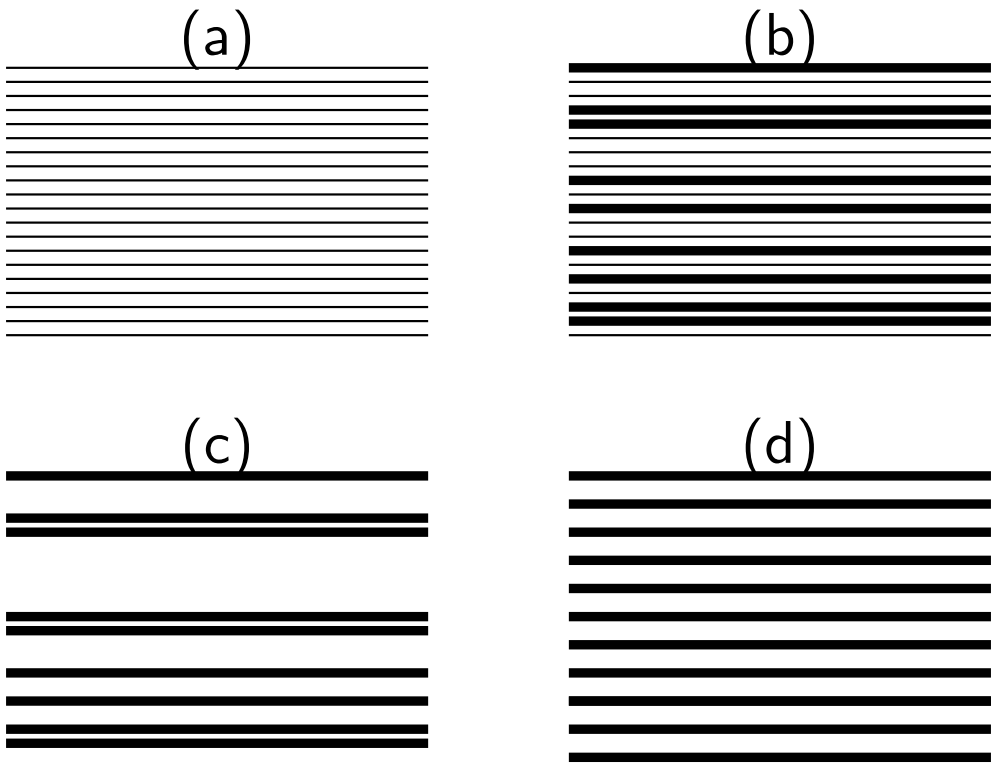


New Scheme


PUF
r
Helper Data Generation
$\mathcal{C}$
Helper Data Storage
Construct code such that $r \in \mathcal{C}$
$r' = r \oplus e$
$\mathcal{C}$
r'
Decoder
$\hat{r}$
Key
$\hat{r} = dec(r')$

New Scheme: Initialization Phase

Question: How to generate a code $\mathcal{C}$, such that $r \in \mathcal{C}$?



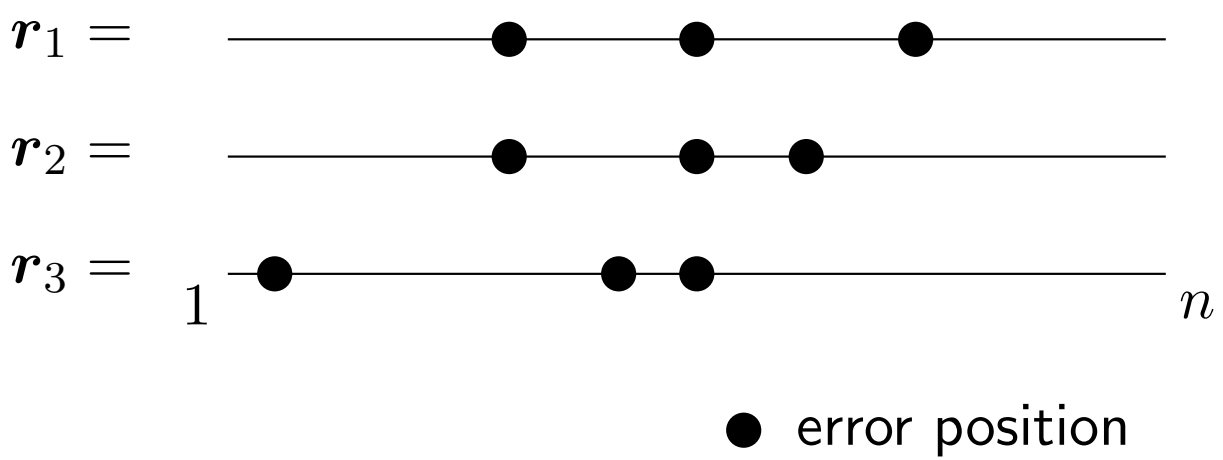
(a) Generate Code $\mathcal{C}$ based on Euclidean Geometry
(b) Choose parity check equations, s.t. $r \in \mathcal{C}$
(c) Delete rest of the parity check equations
(d) Generate more parity check equations, e.g. by using Projective Geometry or Reed-Solomon Code based construction

New Scheme: Reproduction Phase

Decoding:

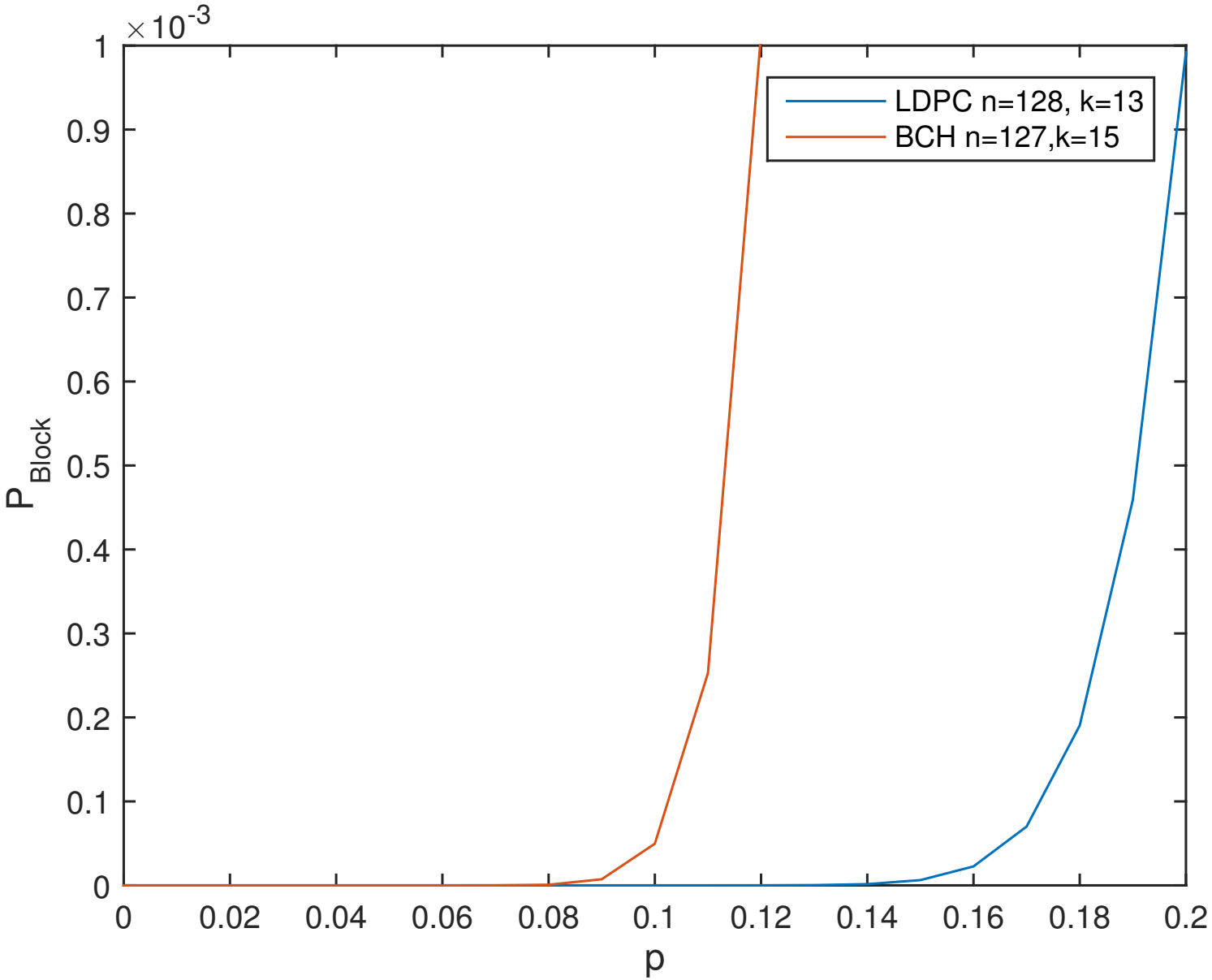
- Iterative bitflip procedure

Multiple readouts:

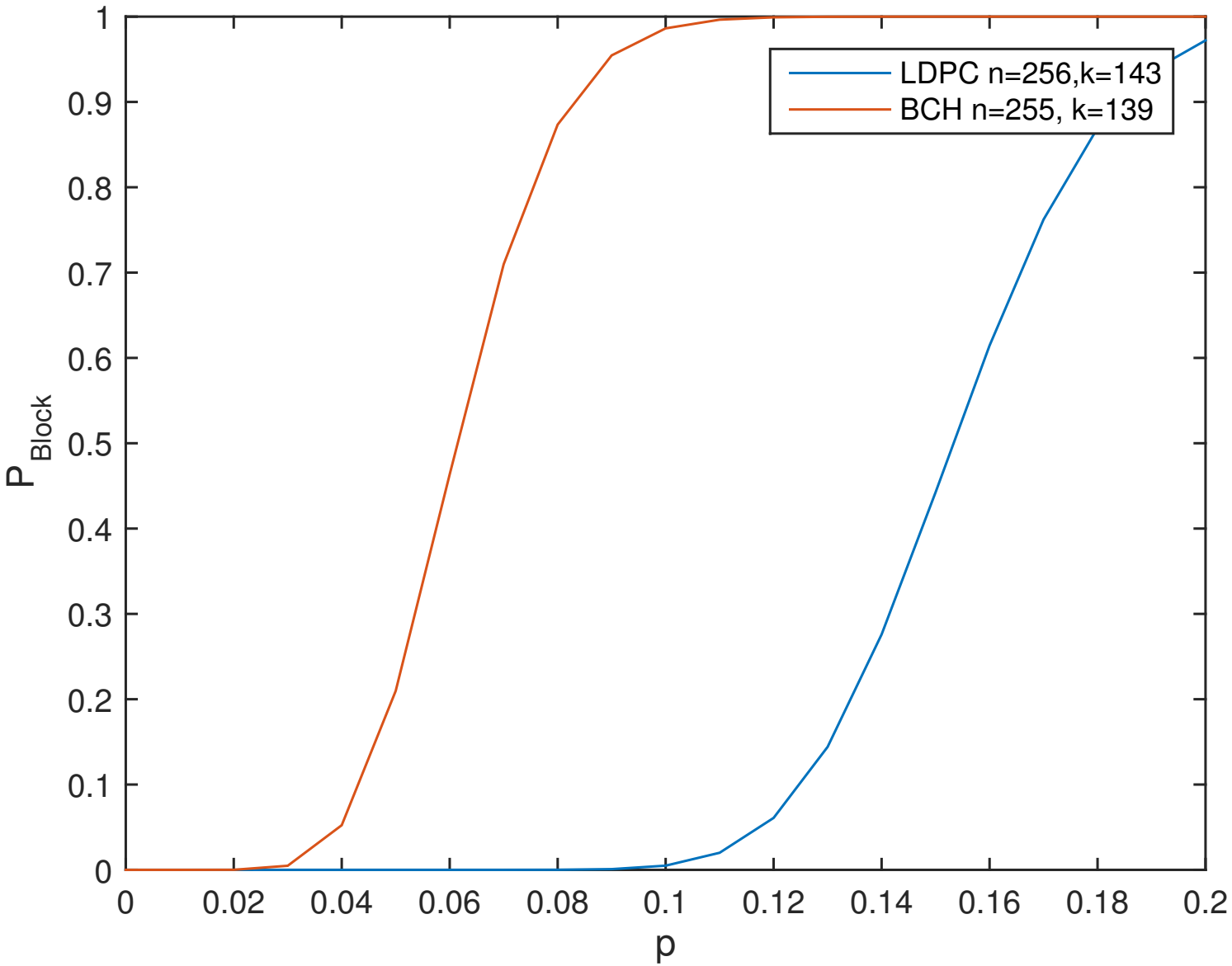


Obtaining soft information by using $m = 3$ readouts.

New Scheme: Examples (Code Rate ≈ 0.1)



New Scheme: Examples (Code Rate ≈ 0.55)



Conclusion

Advantages of the scheme:

- Needs only code, no additional helper data
- Scheme with very plain structure
- Memory efficiency
- Decoding in linear time
- Efficient hardware implementation possible

Drawback: Complexity of helper data generation

- happens only once per device
- not necessarily on chip (secure environment)

Future research:

- Construct codes with larger dimension for cryptographic security
- Investigate security issues
- Find additional code classes

Thank you for the attention!