University of Waterloo

Department of Electrical and Computer Engineering

Adaptive Recovery of Transient Errors in EC Scalar Multiplication

Abdulaziz Alkhoraidly

Anwar Hasan

Outline

- Elliptic curve cryptography
- Fault attacks on ECC and countermeasures
- Frequent validation for error recovery
- Adaptive error recovery
- Example and results

Elliptic Curve Cryptography

In a nutshell:

- An elliptic curve is a smooth curve defined over a field by
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
- The points on an EC form a group under point addition.
- This group has some interesting properties.
- The main operation in ECC is scalar multiplication:
$$Q = kP = \underbrace{P + P + \cdots + P}_{k \text{ times}}$$

Fault Attacks on ECC

Exploit faults to leak secret information.

Two classes:

- **Invalid curve attacks:** move to a weaker curve
  - invalid base point
  - invalid curve parameters
  - invalid computations
- **Same curve attacks:** stay on the same curve
  - sign-change attack

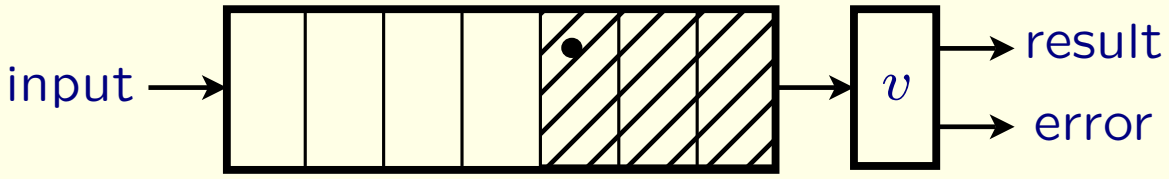
Fault Attacks on ECC

Countermeasures:

Countermeasure	Invalid curve	Sign-change
Point validation	yes	no
Montgomery's SM	no	yes^c
Combined curves	no	yes
Consistency checking	yes	yes
T/H redundancy	yes^c	yes^c
Rand. enc.	no	yes

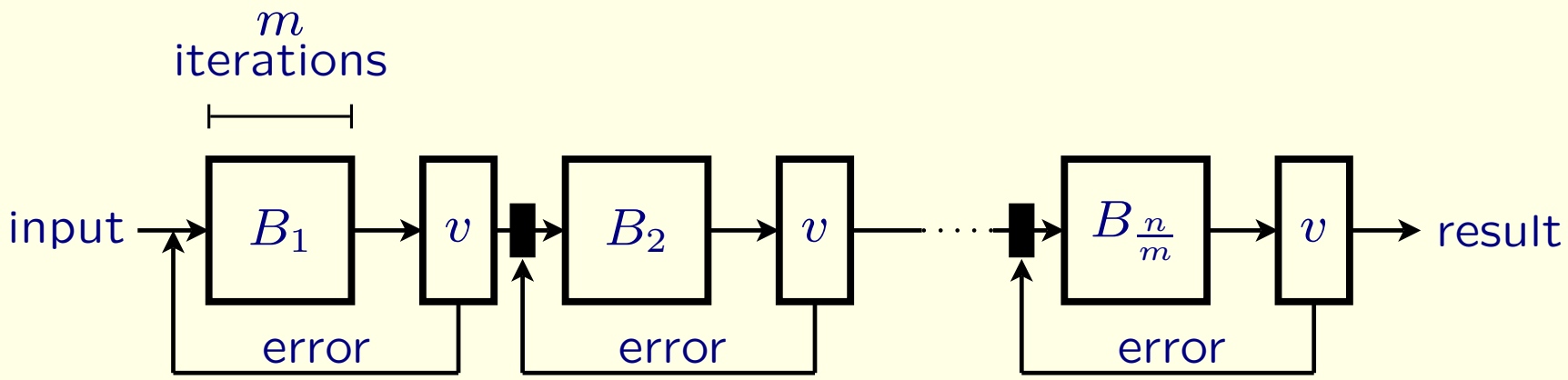
Note: Not all allow for error detection.

A Closer Look...



- Errors will propagate through iterations.
- Full recomputation is expensive.
- It makes sense to test frequently.

Error Recovery with Frequent Validation



- n: number of iterations.
- m: block size.
- B_i: i^{th} block.
- Limit error propagation with frequent validation.
- Reduce recomputation overhead.

Error Recovery with Frequent Validation

Advantages:

- Reduced overhead.
- Significantly more reliable.

Disadvantage:

- Requires knowledge of error statistics for optimal performance.

Adaptive Error Recovery

Change block size during the computation to reflect the perceived error rate.

Issues

- Block size range:
  - avoid large blocks
- Adaptive policy:
  - avoid complicated functions
  - increase slowly and decrease quickly

Adaptive Error Recovery

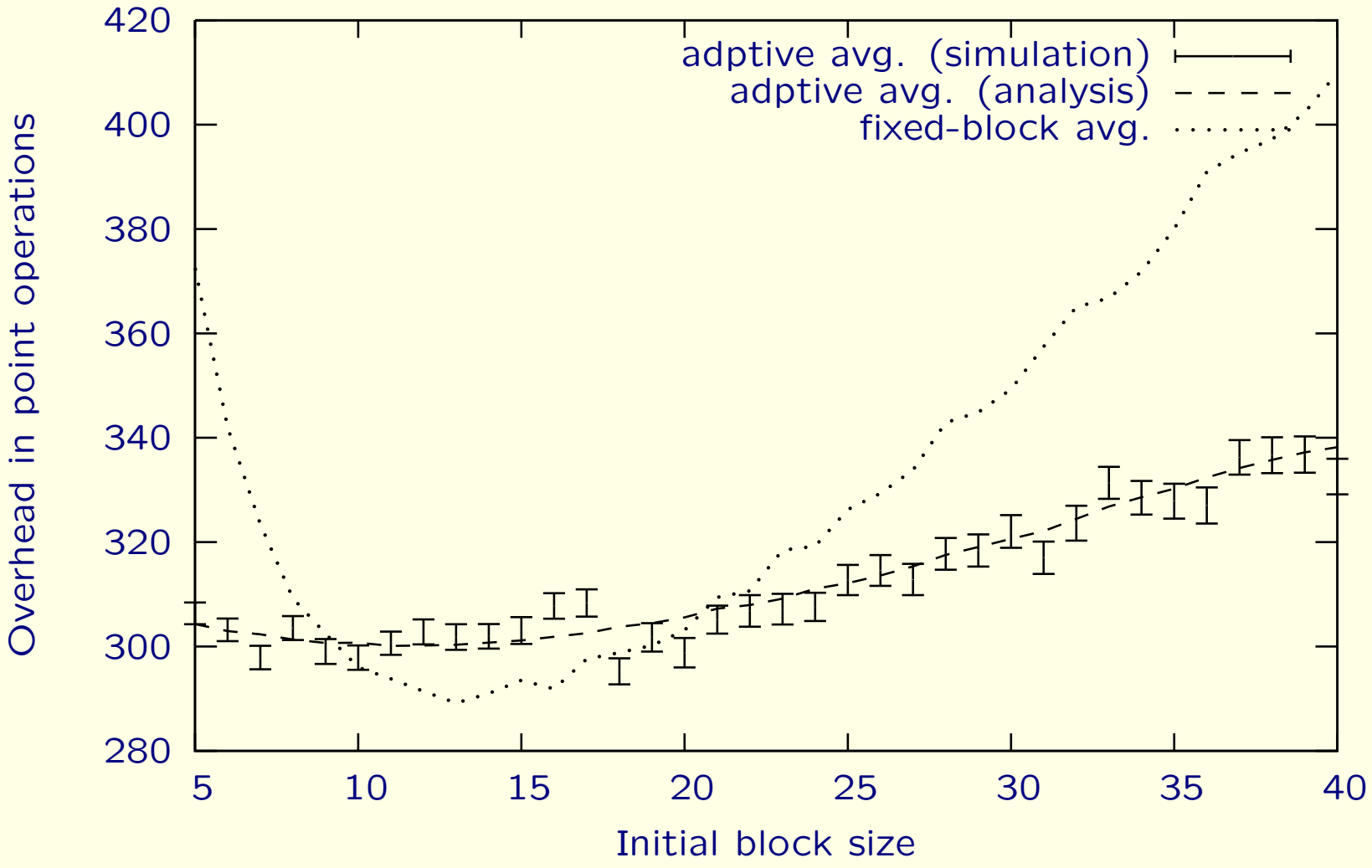
An example:

Parameters:

- Size: 256 iterations.
- Avg. basic iteration: 1.5 point operations
- Modified iteration: 2 po
- Validation test: 4 po
- Block size range: [5,40] iterations
- Adaptive policy: $m_{\uparrow} = m + 1$, $m_{\downarrow} = \mathrm{Floor}(m/2)$

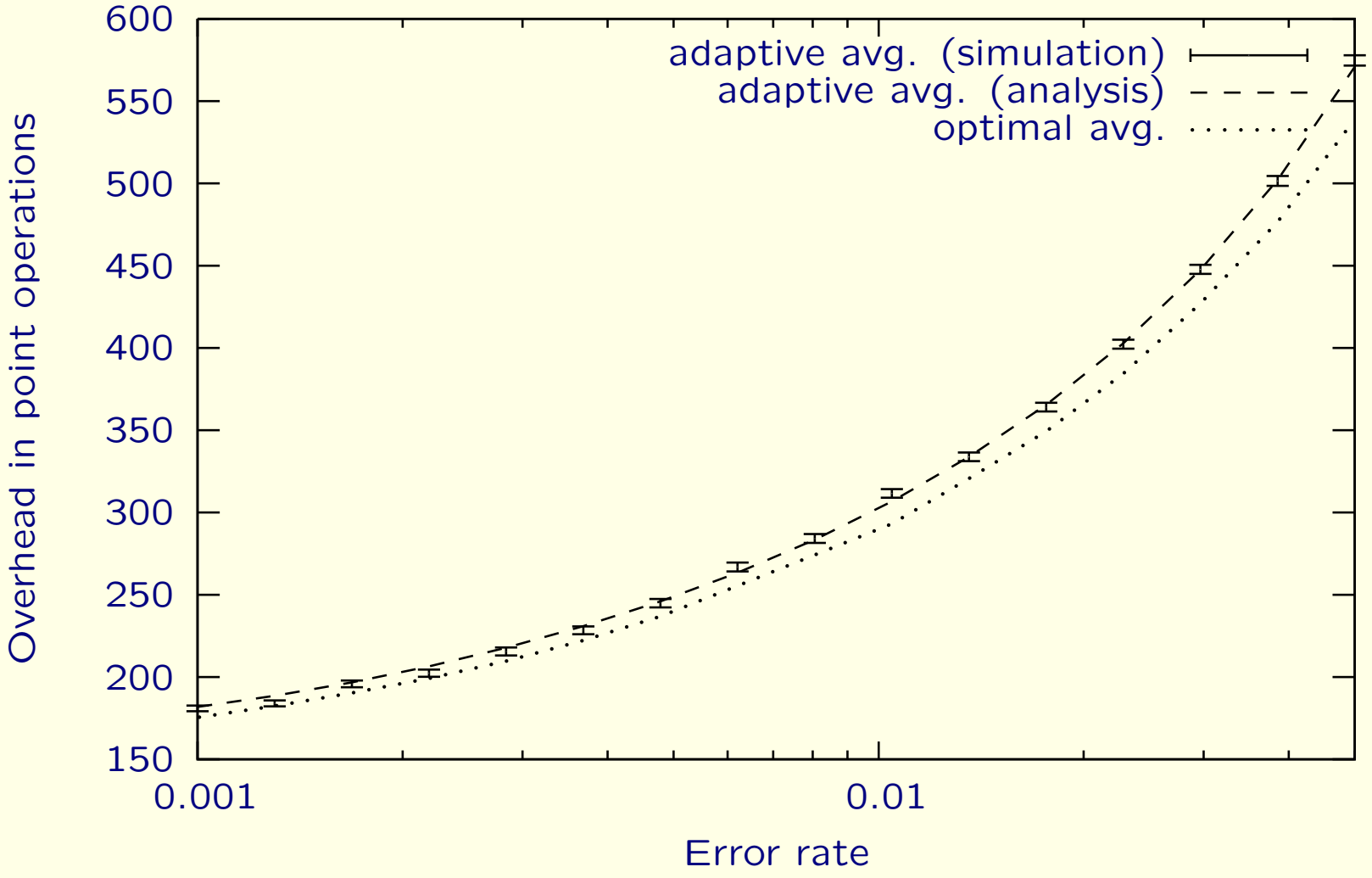
Adaptive Error Recovery

Results: Constant error rate



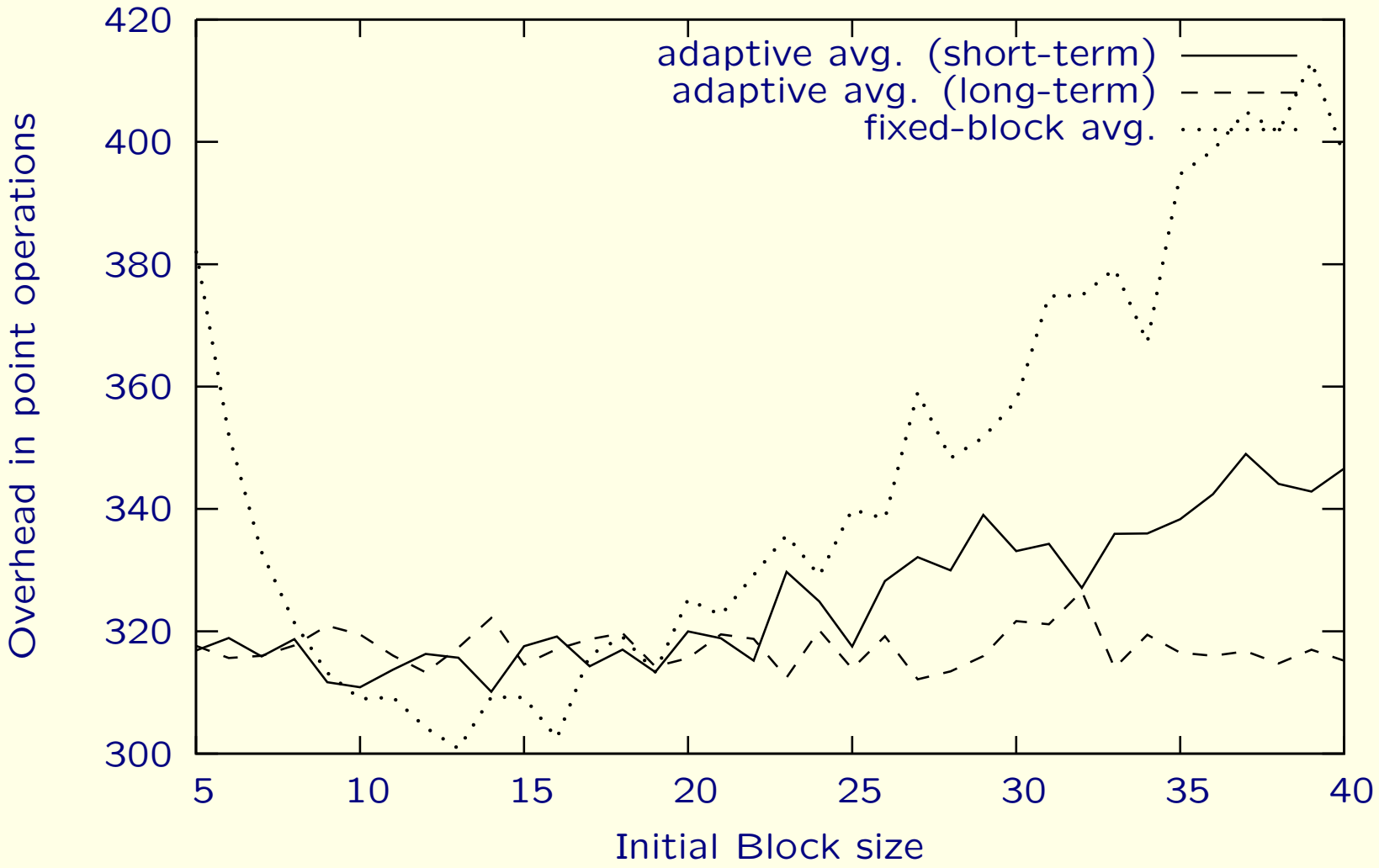
Adaptive Error Recovery

Results: Constant error rate



Adaptive Error Recovery

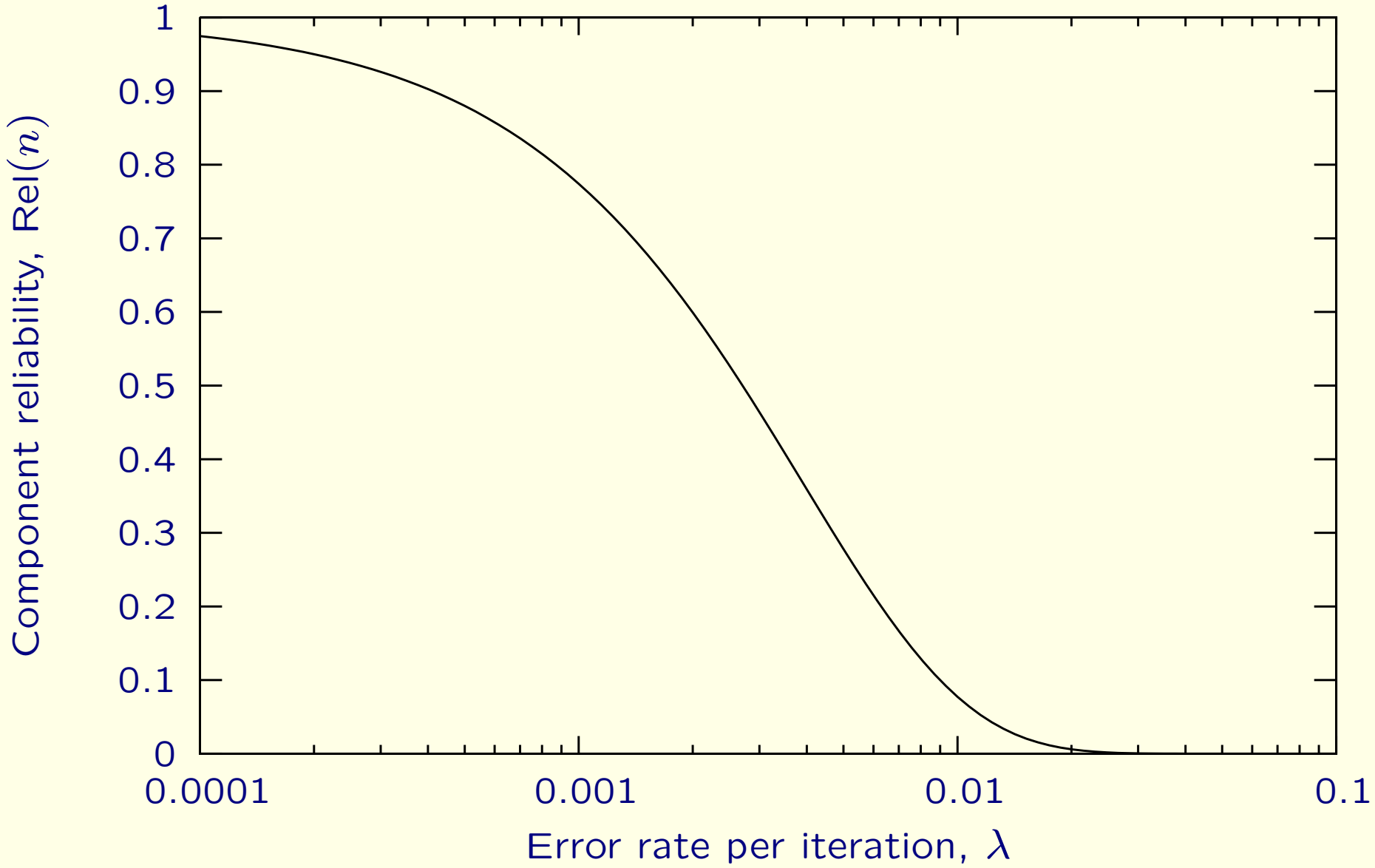
Results: Variable error rate, $\lambda \in [0.001, 0.05]$



Summary

- Fault-tolerance is essential when implementing cryptography.
- Frequent validation allows for efficient and reliable error recovery.
- Adaptive error recovery reduces the need to know error statistics and gives near-optimal performance.

Thank you...


Component reliability, Rel(n)
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0.0001
0.001
0.01
0.1
Error rate per iteration, λ