NOEKEON

CipherFreek

Department of EECS
Indian Institute of Technology Bhilai

November 27, 2020

Outline

- Block Cipher
  - 128-bit key
  - 128-bit block
- 16 rounds, Nr=16

- **Security**
  - resistance against cryptanalysis
  - no shortcut attacks
- **Efficiency**
  - Speed
- **Design**
  - Code/Circuit Compactness
  - Smart Cards

- Protection of Confidentiality , in our terms Privacy
- Data integrity and Authentication
- One-way function
- Self-Inverse Bit-Slice Cipher

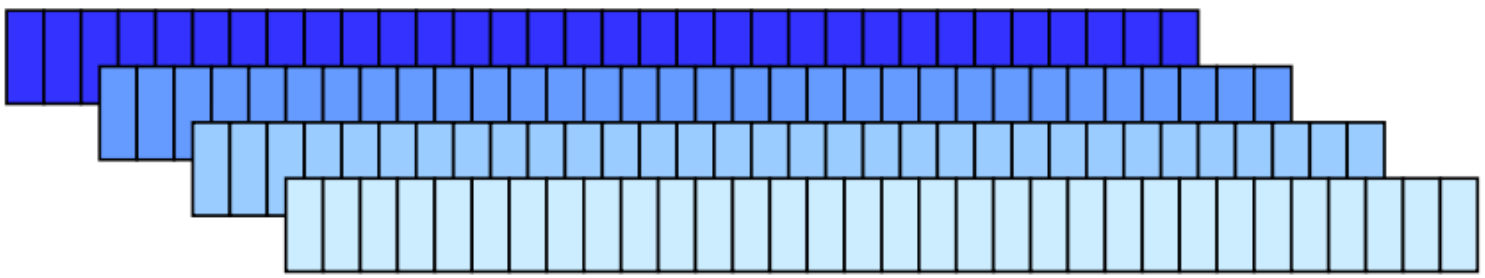
Outline

Round Transformation

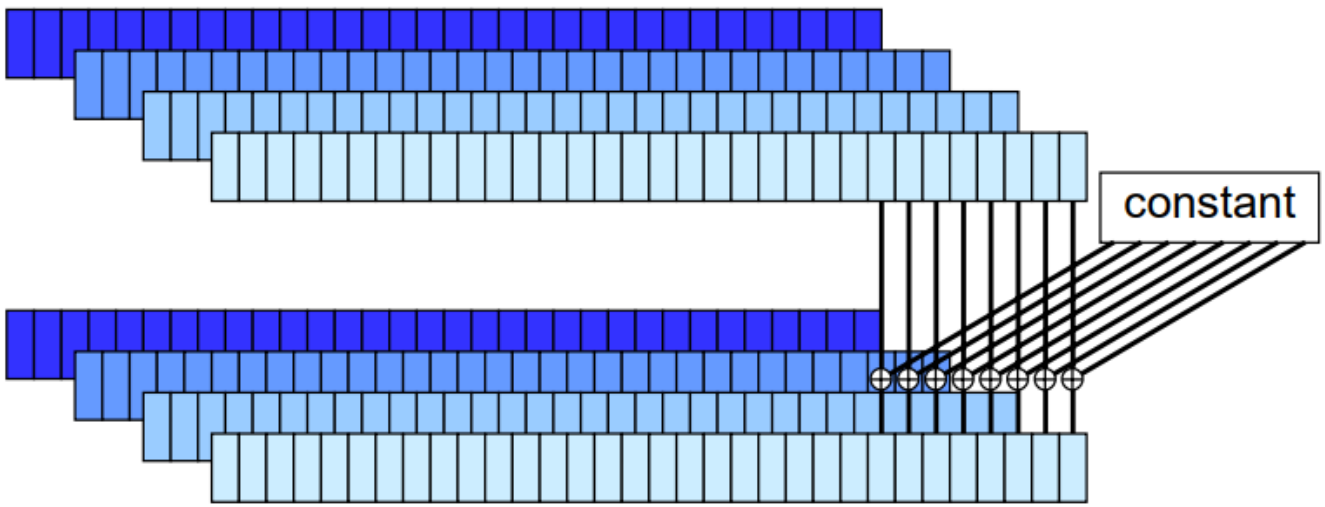
- Nr=16
- The Round Transformation is composed of different transformations
  - Round Constant Addition
  - Theta
  - Pi1
  - Gamma
  - Pi2

The State

- The different transformations operate on the intermediate result, called **the State**
- state consists of 4 32-bit words a_0, a_1, a_2, a_3

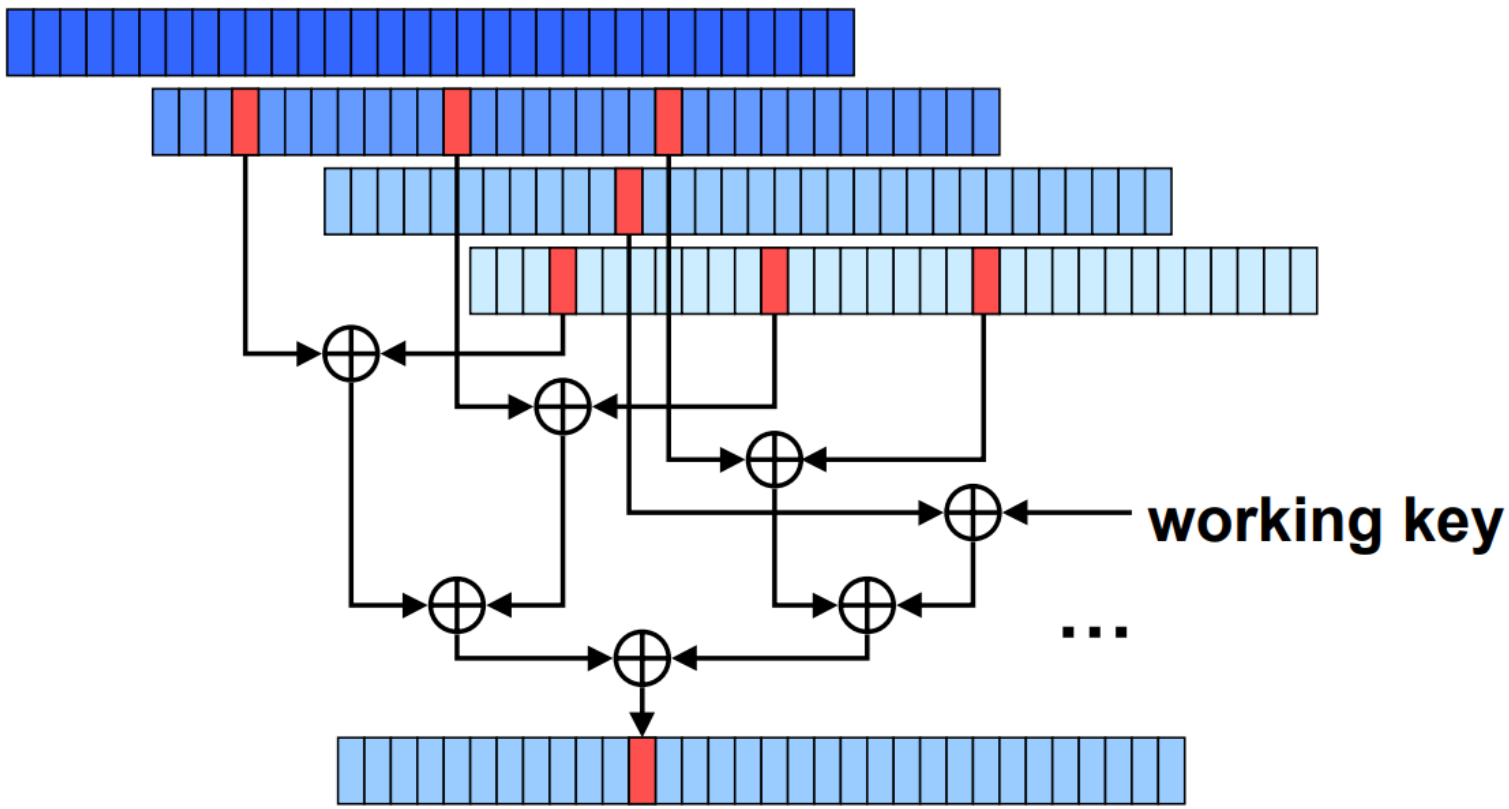


Round Constant Addition



Theta

Theta is a linear mapping that takes the Working Key k and operates on the state

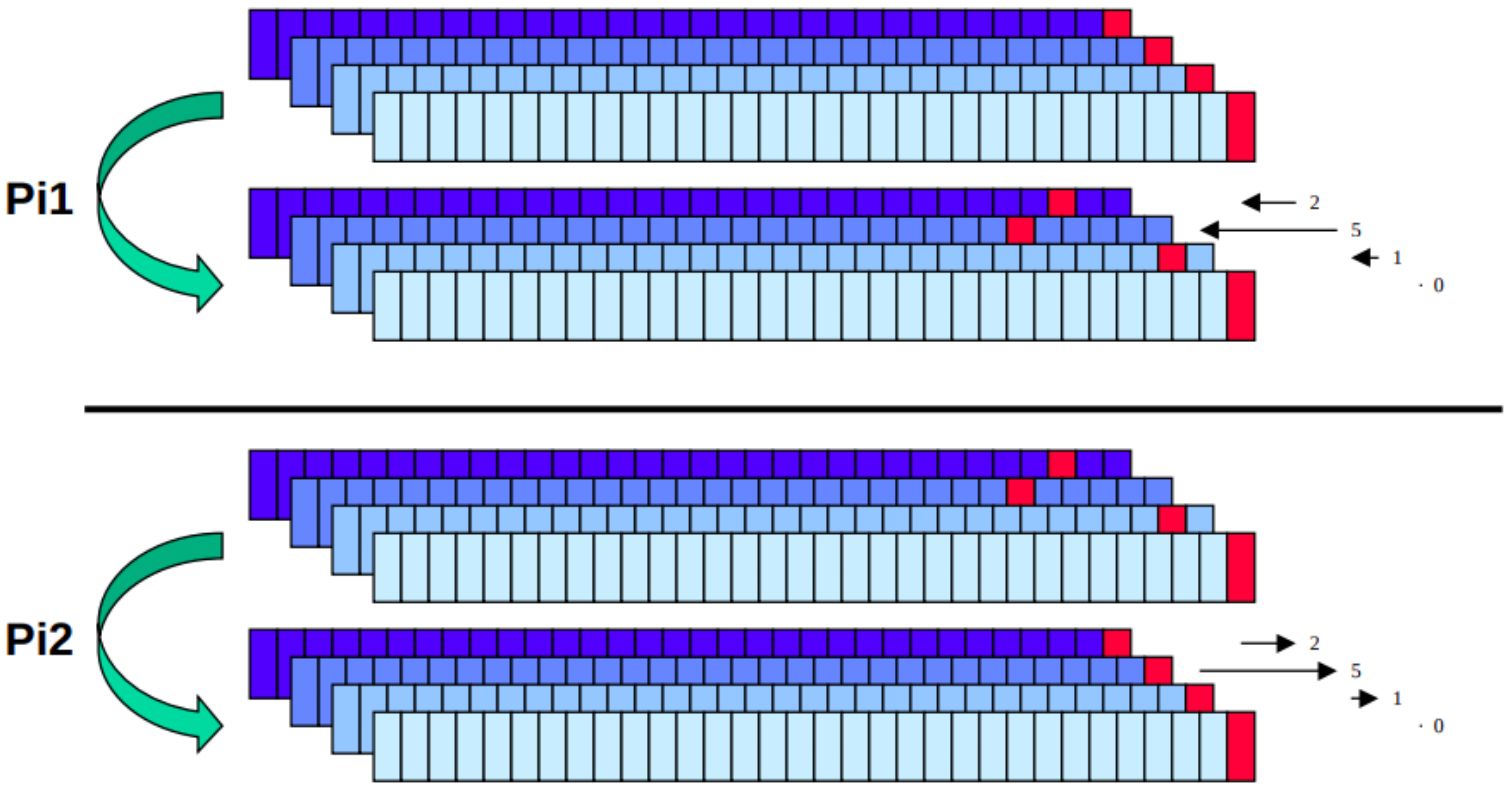


Theta

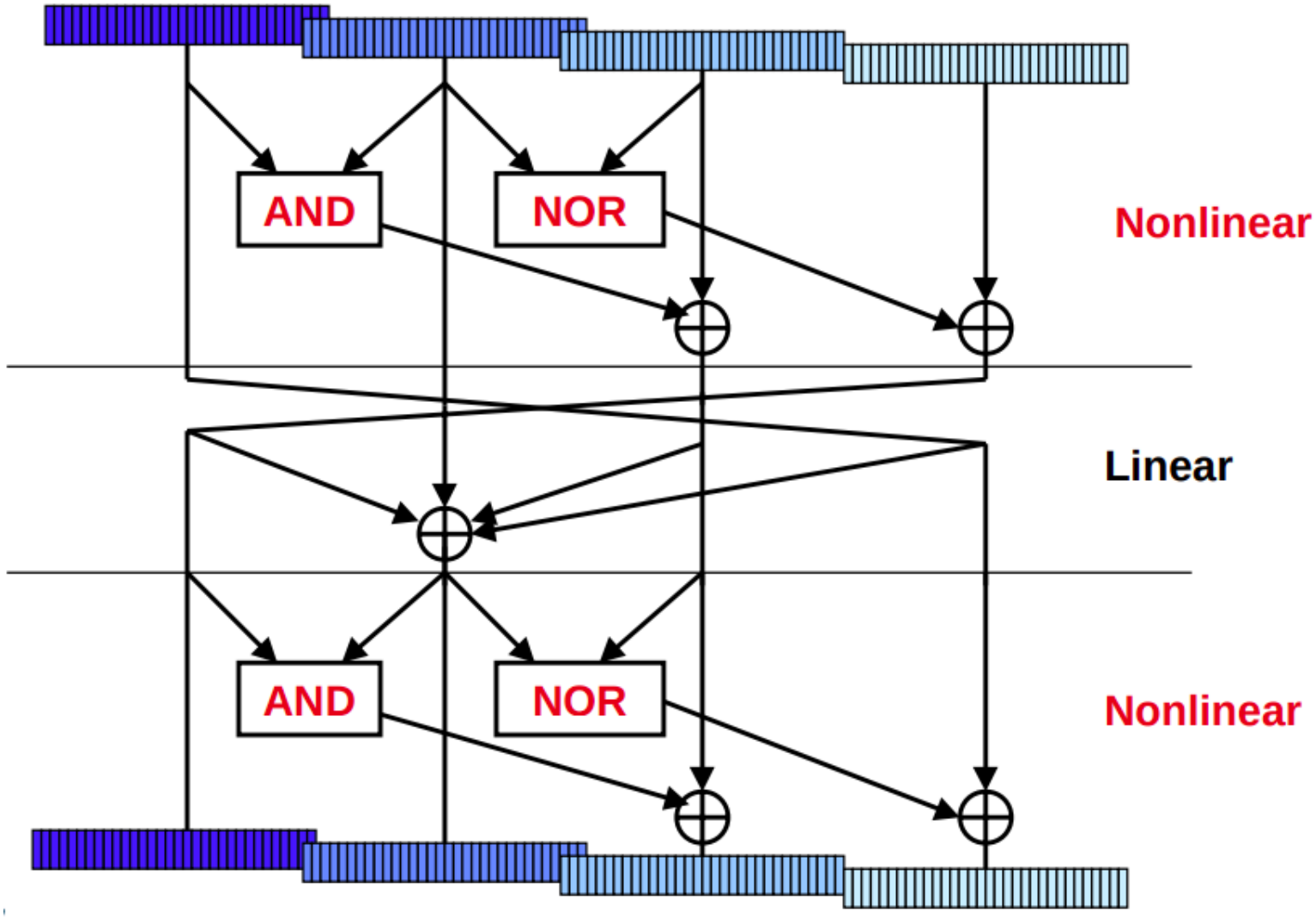
The design criteria for Theta:

- Involution
- Small number of operations
- Relevant diffusion
- Symmetry

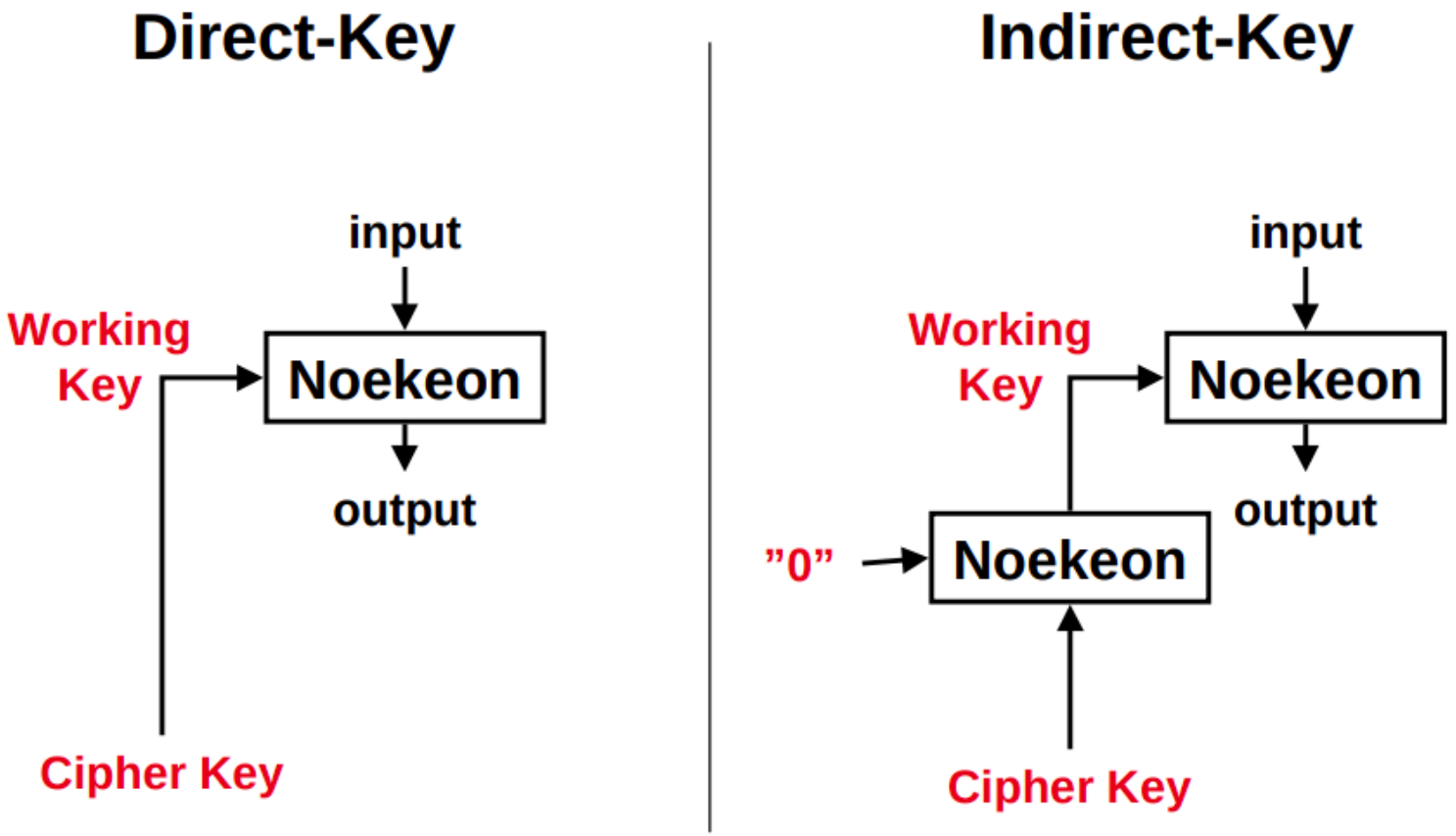
Pi1 and Pi2



Gamma Illustrated



Key Schedule Modes



Outline

Strength agaisnt known attacks

- Linear and differential cryptanalysis: propagation analysis
- Truncated differentials
- Symmetry properties and slide attacks
- Weak keys
- Related-key attacks
- Hidden weaknesses and Trapdoors

Implementation

Hardware Suitability

Implemented in small number of gates:

- 640 XOR gate
- 64 AND
- 64 NOR

High speed: small gate delay

- 7 XOR
- 1 AND
- 1 NOR

Software Performance

- Particulary suitable for 32-bit processors and a bit difficult for 8-bit processors.
- Pentium-II

NOEKEON	$NOEKEON^{-1}$	bit rate @ 200MHz
525 cycles	525cycles	49 Mbit/s

- ARM7

codesize	NOEKEON	$NOEKEON^{-1}$	bit rate @28.56MHz
332 bytes	712 cycles	712 cycles	5.1Mbit/s
3688 bytes	475 cycles	475 cycles	7.7Mbit/s

Protection agaisnt Implementation attacks

- Fixed set of instructions.
- State splitting which counters Differential power analysis at a low cpu cost because of few non-linear operations.
- Direct-key mode counters key schedule attacks.

Outline

Weakness of NOEKEON

- All round keys are same.
- The linear and non-linear part of the round has order 2!.
- If round constants are removed:
  - all rounds are equal.
  - there is symmetry within the words.
  - the cipher and its inverse are equal.
- Non-linearity is only provided by some binary ANDs.

Outline

Strength and advantages of NOEKEON

- In specialized hardware implementations, it is ultra compact and quick;
- Allows efficient DPA-resistant software implementations;
- a very low RAM requirement in software implementations.
- has a very small amount of code.
- efficient on wide range of platforms.
- It is very easy to memorize because of its simple design.

Thanks

Team Members

- Guntuku Sai Rishitha
- Ram Tiwari
- Saurav Raj

Implementation Info

- Github Link: `https://github.com/ramtw/CipherFreek`