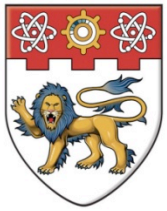


NANYANG TECHNOLOGICAL UNIVERSITY

Inaugural Youth Olympic Village

PRINTcipher: A Block Cipher for IC Printing

L. Knudsen, G. Leander, A. Poschmann, and M. Robshaw

Technical University of Denmark DTU

Axel Poschmann
Division of Mathematical Sciences,
School of Physical and Mathematical Sciences

18 August 2010

Outline

NANYANG TECHNOLOGICAL UNIVERSITY

- **Motivation**
- PRINTcipher
- Security Analysis
- Implementation Results
- Conclusions

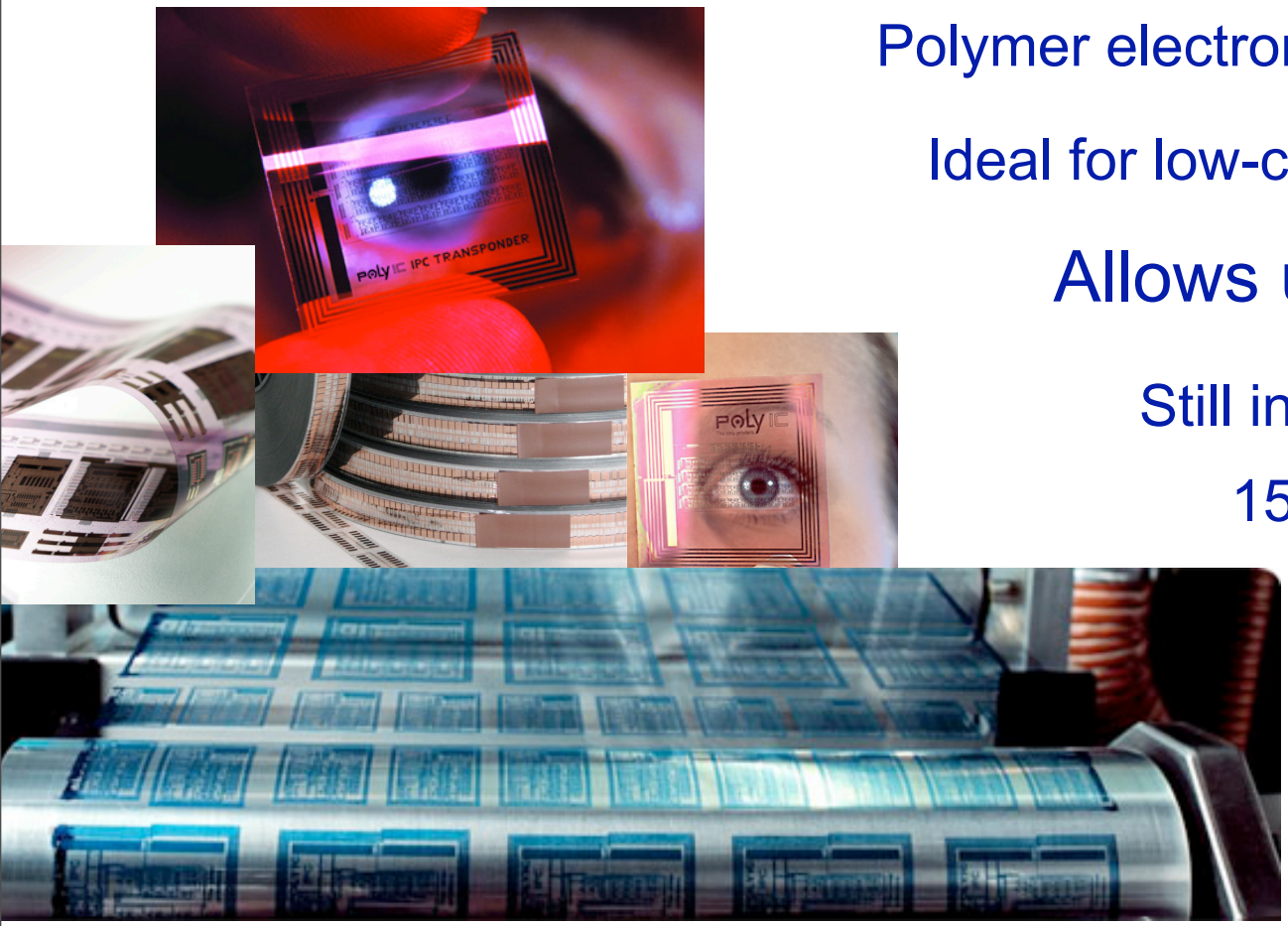
Acknowledgement

Project

Dr. Jasmin Wörle

Motivation

IC Printing **A.k.a.** Organic electronics,
Plastic electronics,
Polymer electronics



Ideal for low-cost RFID tags

Allows **unique** devices

Still in its infancy:

15**um** structure width

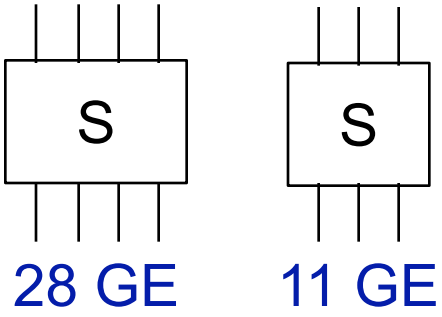
Ultra-constrained

Outline

- Motivation
- **PRINTcipher**
- Security Analysis
- Implementation Results
- Conclusions

Observations

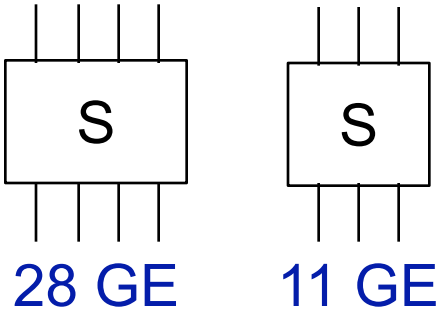
- Smaller S-box save GE
  (but need to increase rounds)



→ **- 50%**

Observations

- Smaller S-box save GE
  (but need to increase rounds)

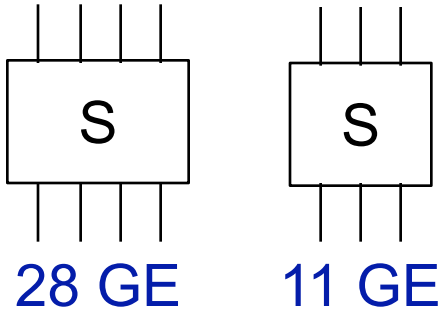


→ **- 50%**

- Storage is most expensive → minimize block size

Observations

- Smaller S-box save GE
  (but need to increase rounds)



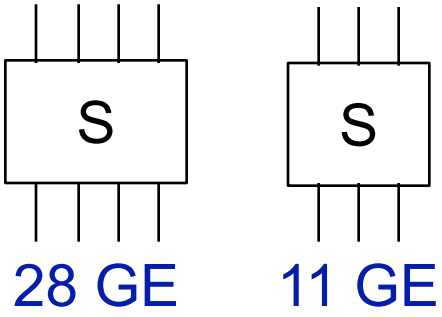
→ **- 50%**

- Storage is most expensive → minimize block size
- BUT! State size is lower bounded -> minimize key schedule

Observations

NANYANG TECHNOLOGICAL UNIVERSITY

- Smaller S-box save GE
  (but need to increase rounds)

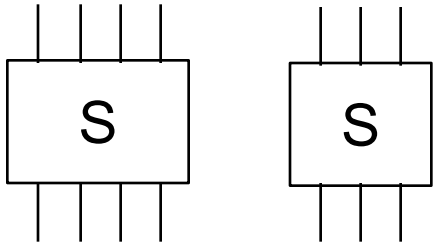


→ **- 50%**

- Storage is most expensive → minimize block size
- BUT! State size is lower bounded -> minimize key schedule
- In RFID scenarios key is most likely fixed

Observations

- Smaller S-box save GE
  (but need to increase rounds)



28 GE 11 GE

→ **- 50%**

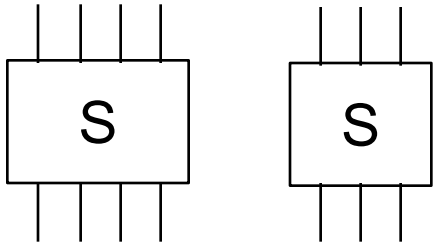
- Storage is most expensive → minimize block size
- BUT! State size is lower bounded -> minimize key schedule
- In RFID scenarios key is most likely fixed
- Addition: **non-fixed** vs. **fixed value** (*n* bits)

n x 2.67 GE *n/2* x 0.67 GE

→ **- 87.5%**

Observations

- Smaller S-box save GE
  (but need to increase rounds)



28 GE 11 GE

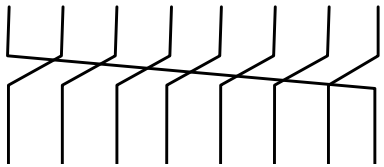
→ **- 50%**

- Storage is most expensive → minimize block size
- BUT! State size is lower bounded -> minimize key schedule
- In RFID scenarios key is most likely fixed
- Addition: **non-fixed** vs. **fixed value** (*n* bits)

n x 2.67 GE *n/2* x 0.67 GE

→ **- 87.5%**

- Bit permutations are for free



0 GE

S-Box

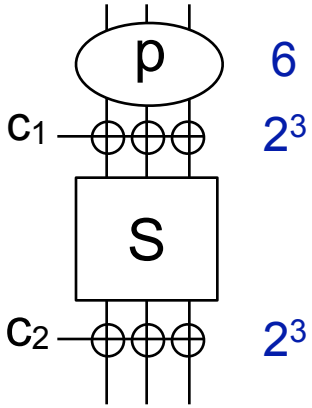
x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

- 3 x 3 S-box
- optimal wrt. LC and DC
- min occurrence of single-bit to single-bit differences/masks
- 384 optimal S-boxes in total

S-Box

x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

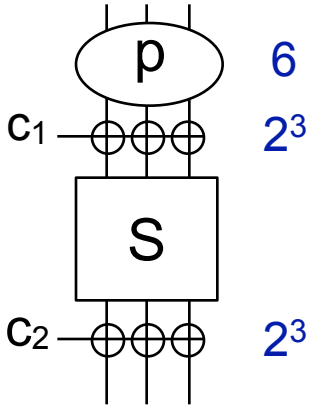
- 3 x 3 S-box
- optimal wrt. LC and DC
- min occurrence of single-bit to single-bit differences/masks
- 384 optimal S-boxes in total



S-Box

x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

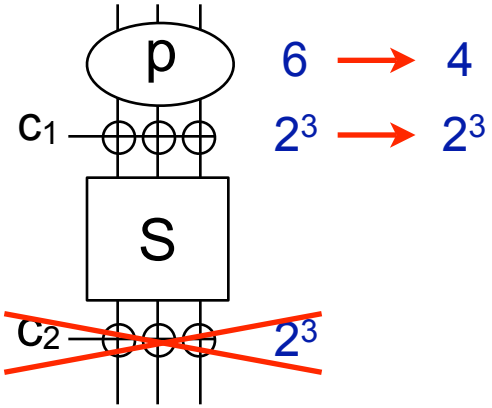
- 3 x 3 S-box
- optimal wrt. LC and DC
- min occurrence of single-bit to single-bit differences/masks
- ~~3~~1~~4~~ optimal S-boxes in total



S-Box

x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

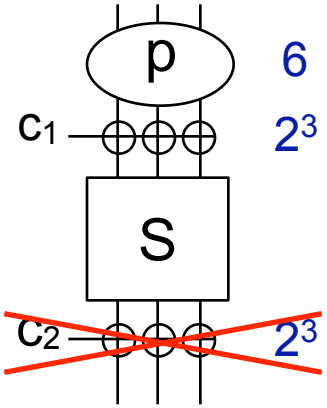
- 3 x 3 S-box
- optimal wrt. LC and DC
- min occurrence of single-bit to single-bit differences/masks
- ~~384~~ 1 optimal S-boxes in total



S-Box

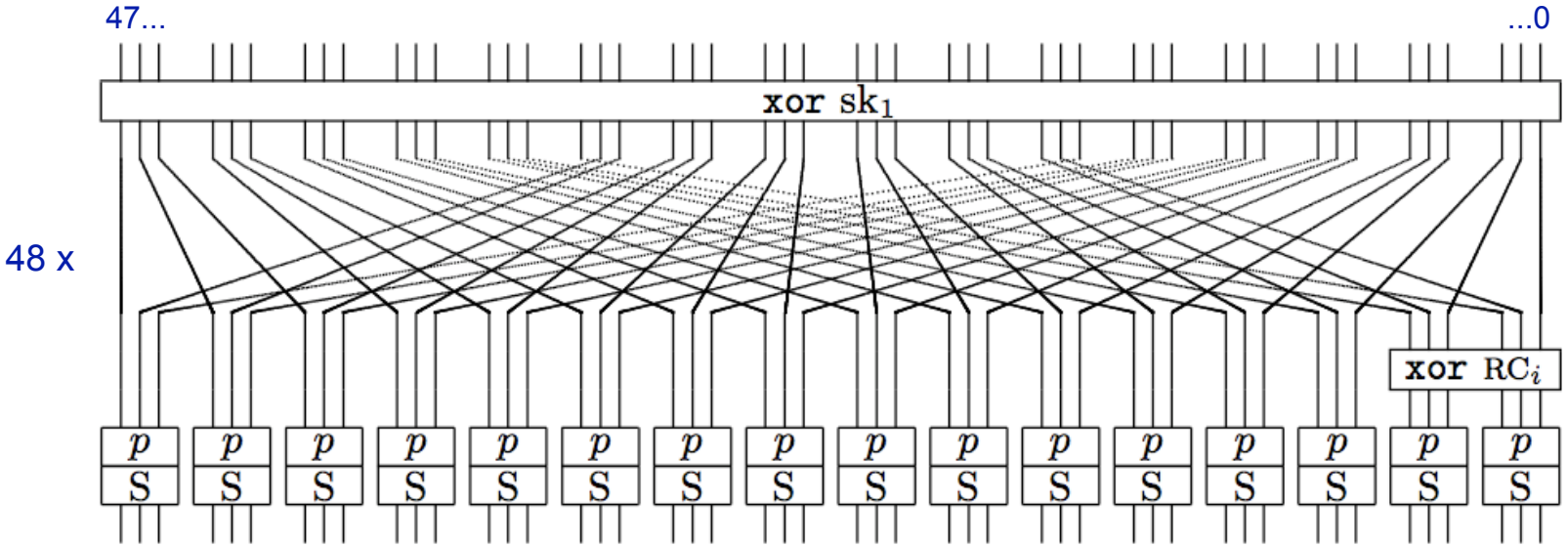
x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

- 3 x 3 S-box
- optimal wrt. LC and DC
- min occurrence of single-bit to single-bit differences/masks
- ~~384~~ 1 optimal S-boxes in total

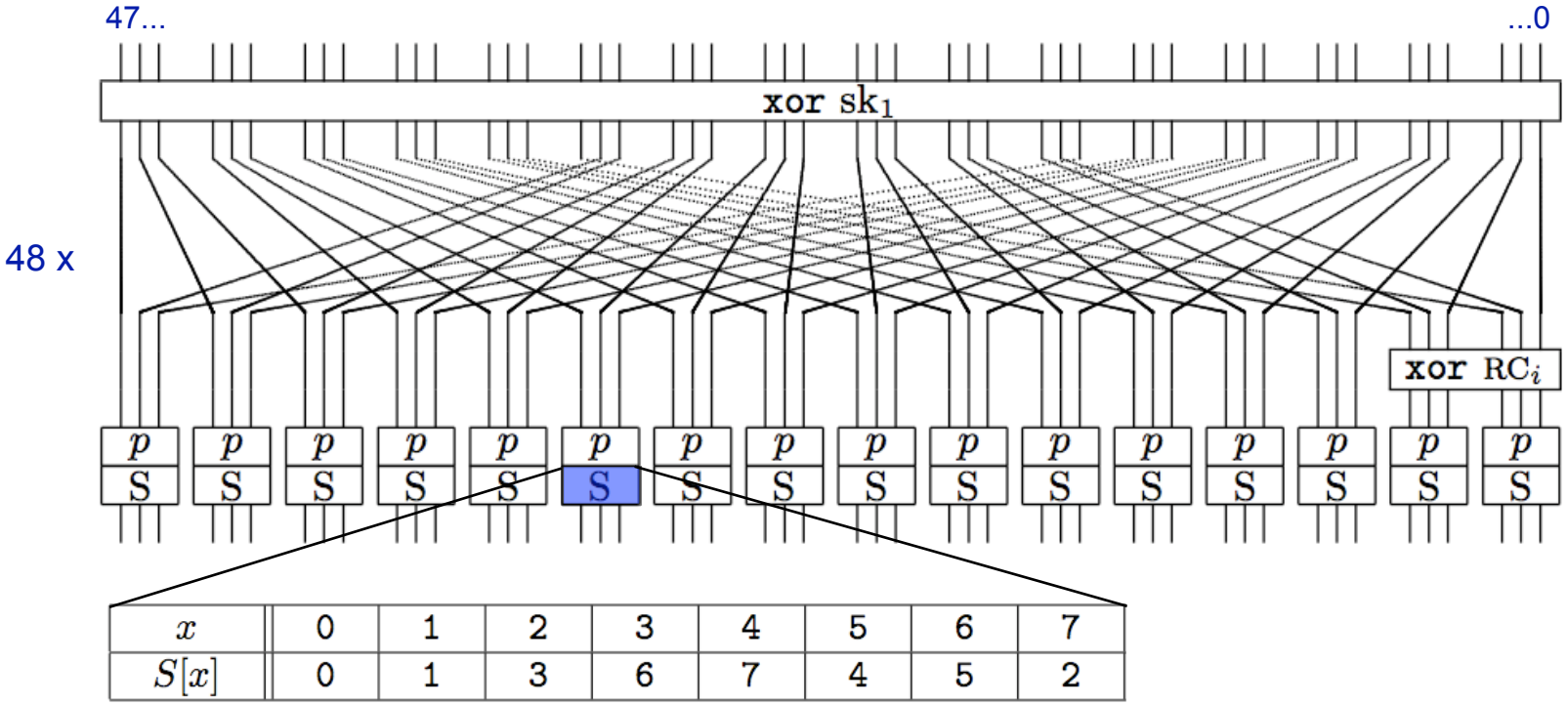


5 bit/S-box

PRINTcipher

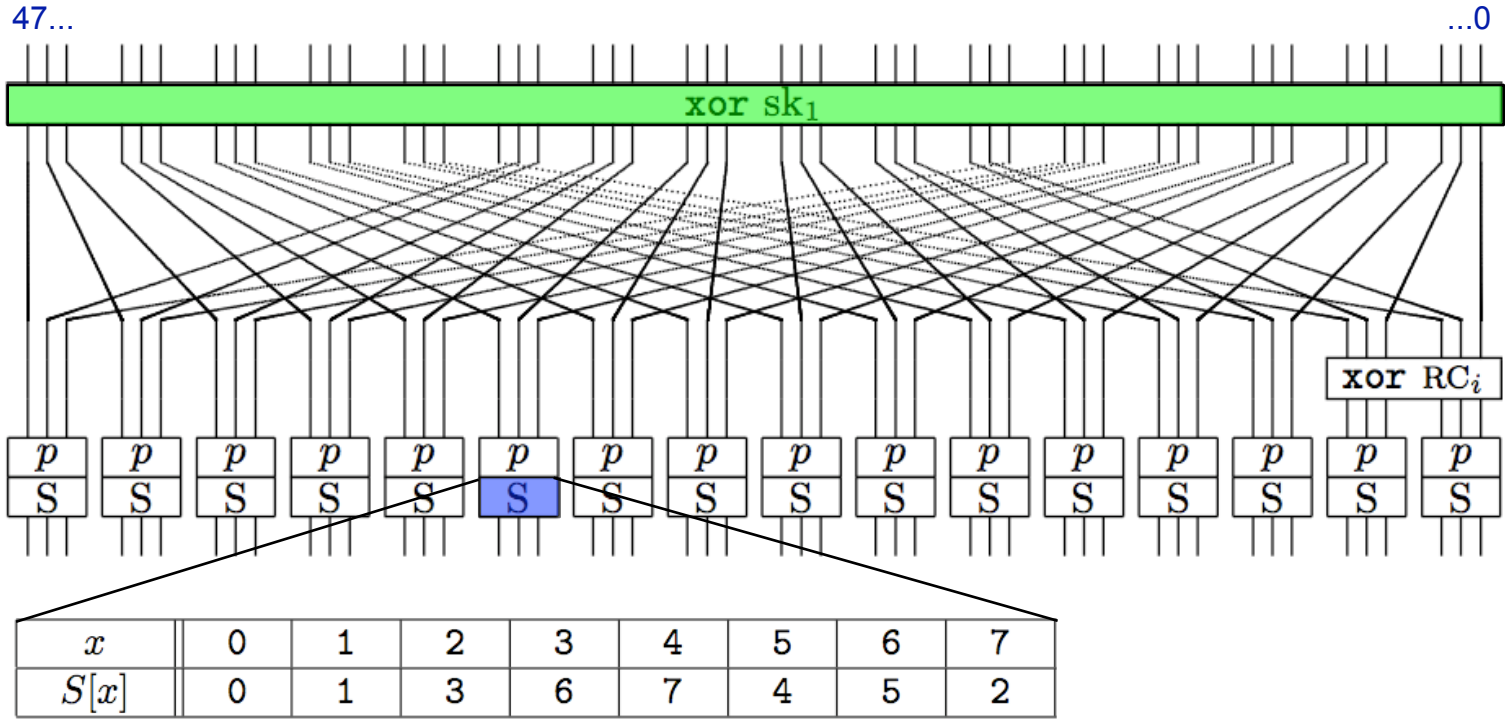


PRINTcipher



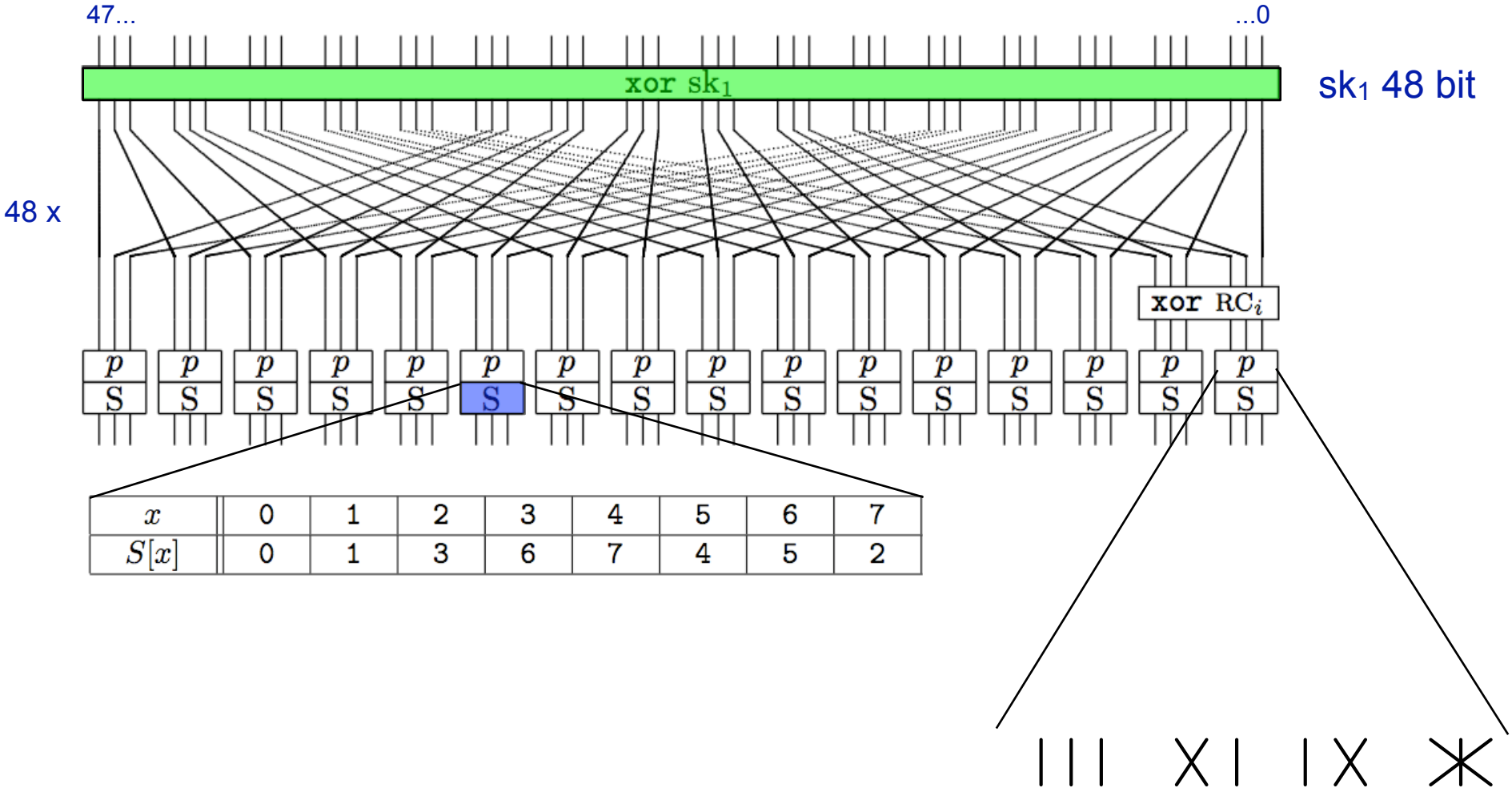
x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

PRINTcipher



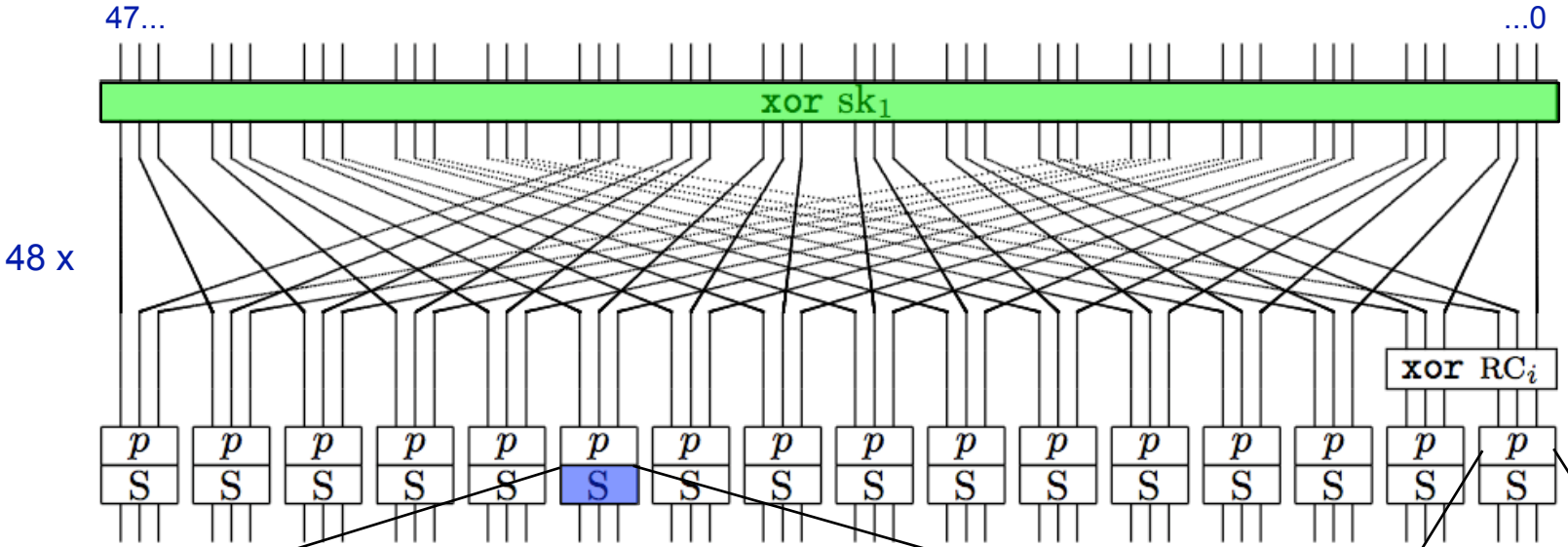
x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

PRINTcipher



x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

PRINTcipher



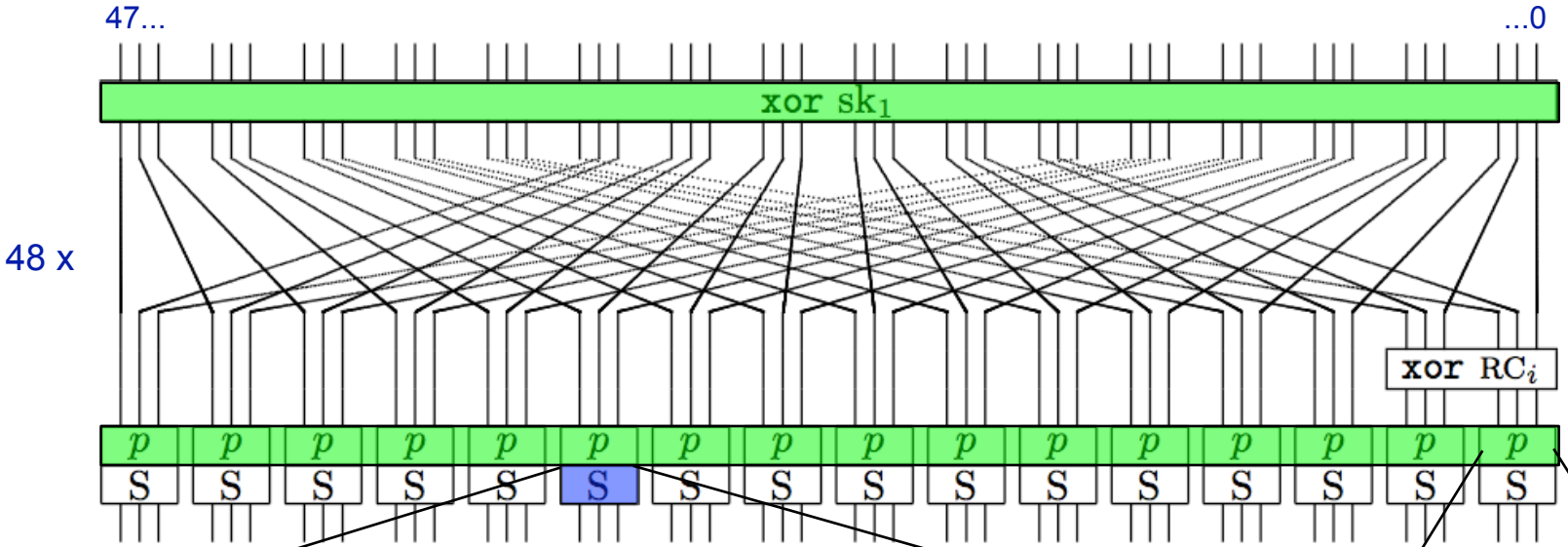
x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

x	0	1	2	3	4	5	6	7
$V_0[x]$	0	1	3	6	7	4	5	2
$V_1[x]$	0	1	7	4	3	6	5	2
$V_2[x]$	0	3	1	6	7	5	4	2
$V_3[x]$	0	7	3	5	1	4	6	2

PRINTcipher

NANYANG TECHNOLOGICAL UNIVERSITY

$k = sk_1 || sk_2 = 80$ bit

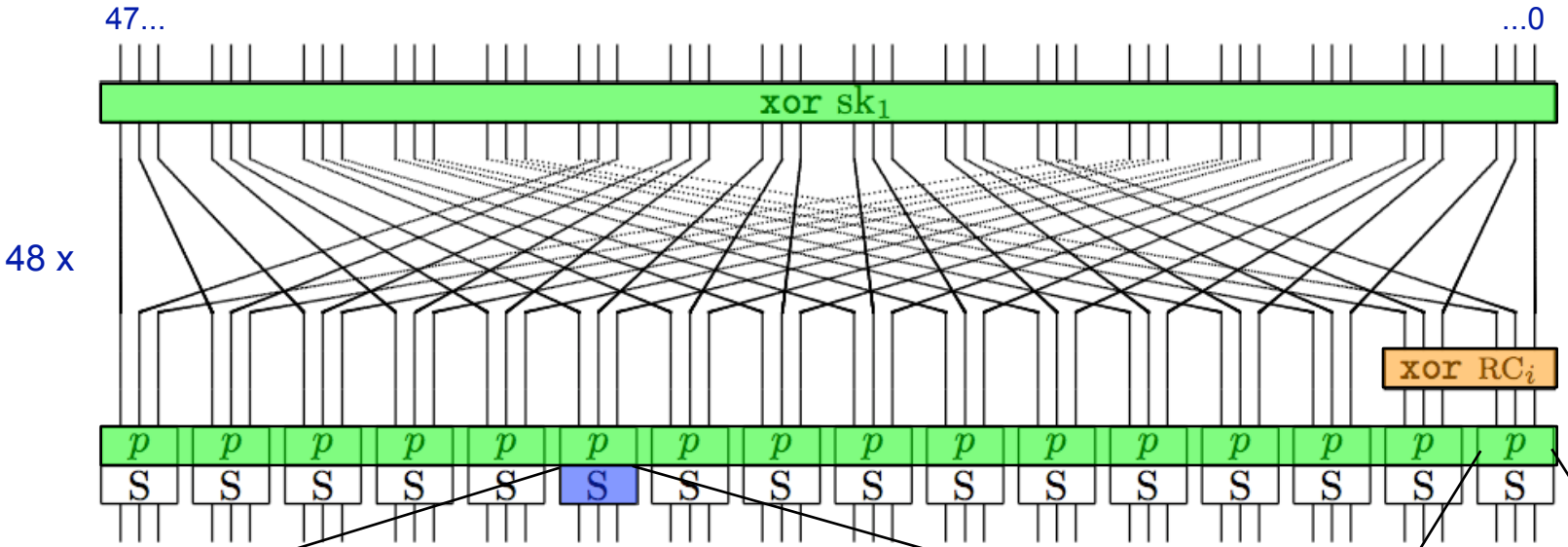


x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

x	0	1	2	3	4	5	6	7
$V_0[x]$	0	1	3	6	7	4	5	2
$V_1[x]$	0	1	7	4	3	6	5	2
$V_2[x]$	0	3	1	6	7	5	4	2
$V_3[x]$	0	7	3	5	1	4	6	2

PRINTcipher

PRINTcipher-48 k = $sk_1||sk_2$ = 80 bit



sk_1 48 bit

vs. slide attacks

sk_2 32 bit

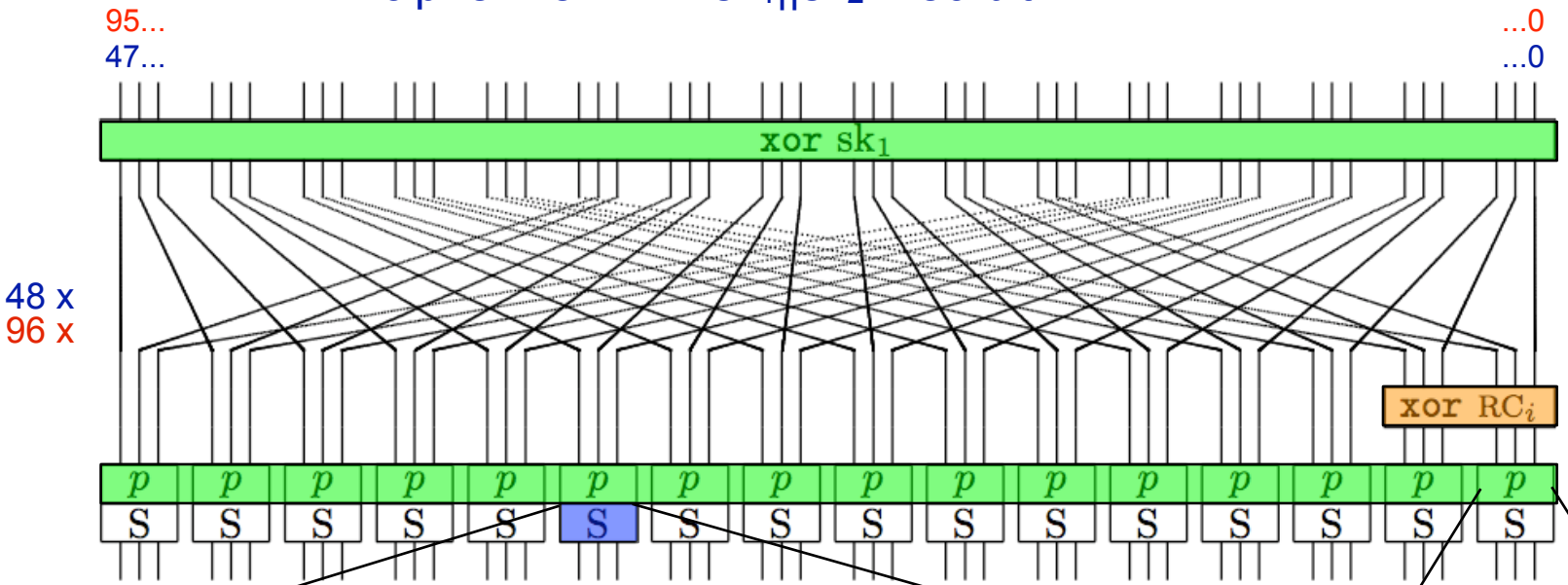
x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

x	0	1	2	3	4	5	6	7
$V_0[x]$	0	1	3	6	7	4	5	2
$V_1[x]$	0	1	7	4	3	6	5	2
$V_2[x]$	0	3	1	6	7	5	4	2
$V_3[x]$	0	7	3	5	1	4	6	2

PRINTcipher

PRINTcipher-96 $k = sk_1 || sk_2 = 160$ bit

PRINTcipher-48 $k = sk_1 || sk_2 = 80$ bit



sk_1 48 bit

sk_1 96 bit

vs. slide attacks

sk_2 32 bit

sk_2 64 bit

x	0	1	2	3	4	5	6	7
$S[x]$	0	1	3	6	7	4	5	2

x	0	1	2	3	4	5	6	7
$V_0[x]$	0	1	3	6	7	4	5	2
$V_1[x]$	0	1	7	4	3	6	5	2
$V_2[x]$	0	3	1	6	7	5	4	2
$V_3[x]$	0	7	3	5	1	4	6	2

Outline

- Motivation
- PRINTcipher
- **Security Analysis**
- Implementation Results
- Conclusions

Security Analysis I

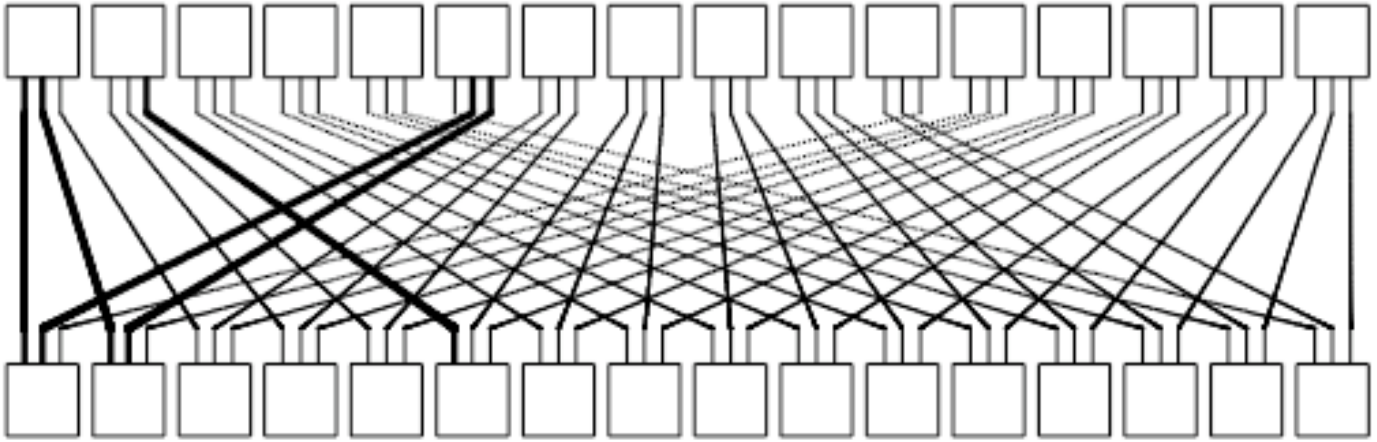
- **Differential and Linear Cryptanalysis**
  - let p denote the probability and
    $q = (2p-1)^2$ the correlation of a linear characteristic
  - max p = 1/4, max q = 1/4
  - same for any key-dependent permuted S-box
  - min 1 active S-box per round
  - *s* round characteristic $p_s = q_s = 2^{-2s}$

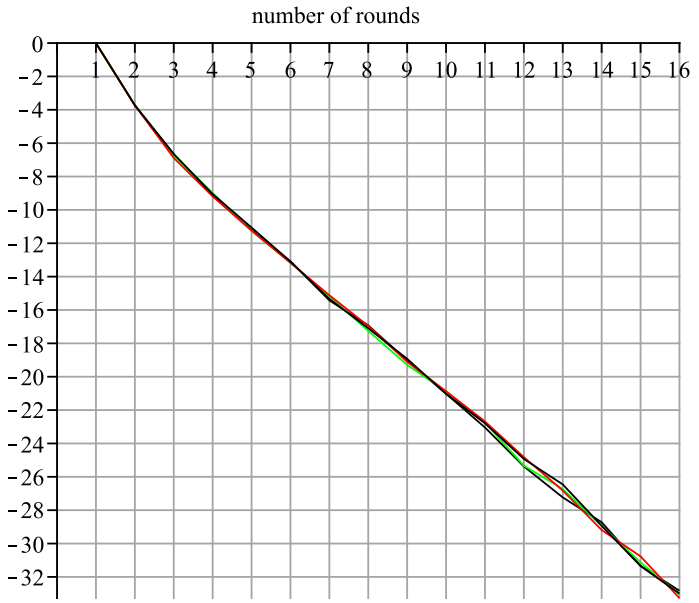
    ➡ **LC and DC impractical**

- **High order DC and Algebraic attacks**
  - S-box has deg 2, allows quadratic equation system
  - but 48 rounds -> expected deg close to max

    ➡ **not feasible**

Security Analysis II





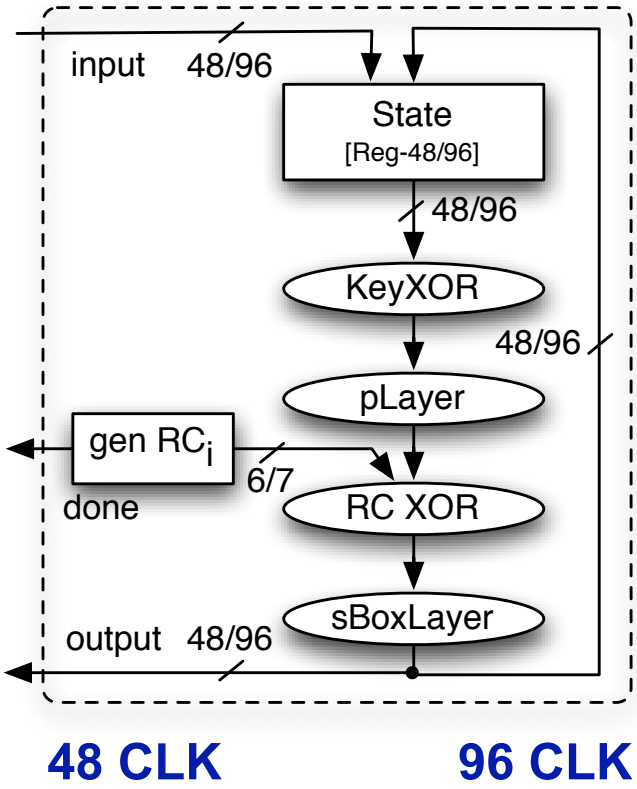
- **Statistical Saturation attacks**
  - upper bounded by **30 rounds**

Outline

- Motivation
- PRINTcipher
- Security Analysis
- **Implementation Results**
- Conclusions

Implementation Results I

round *UMCL18G212T3* library

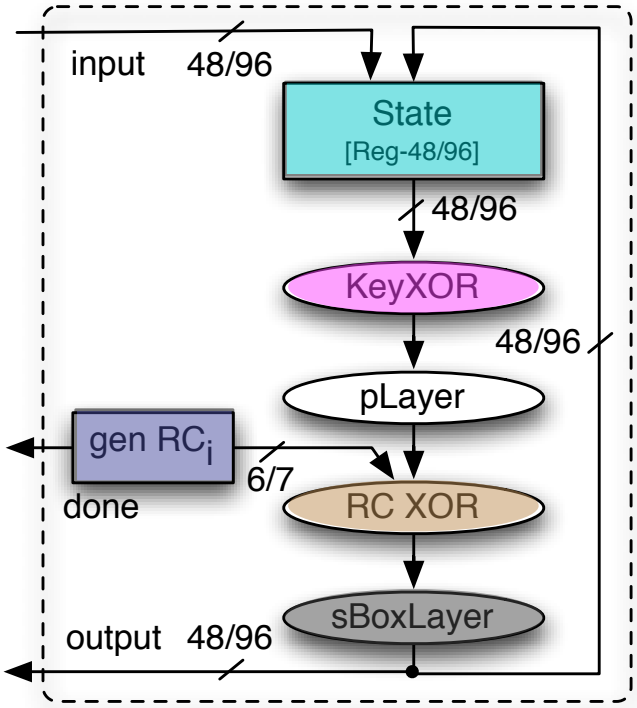


48 CLK **96 CLK**

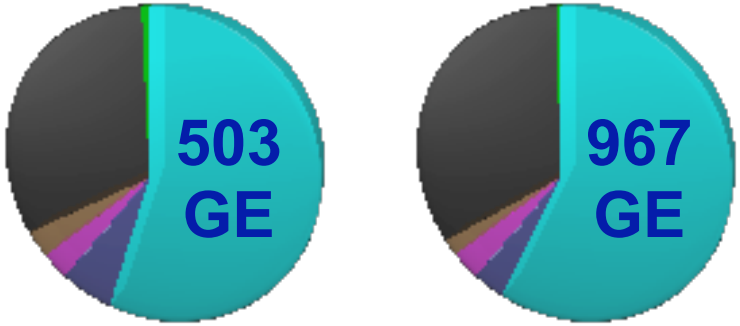
Implementation Results I

NANYANG TECHNOLOGICAL UNIVERSITY

round *UMCL18G212T3* library



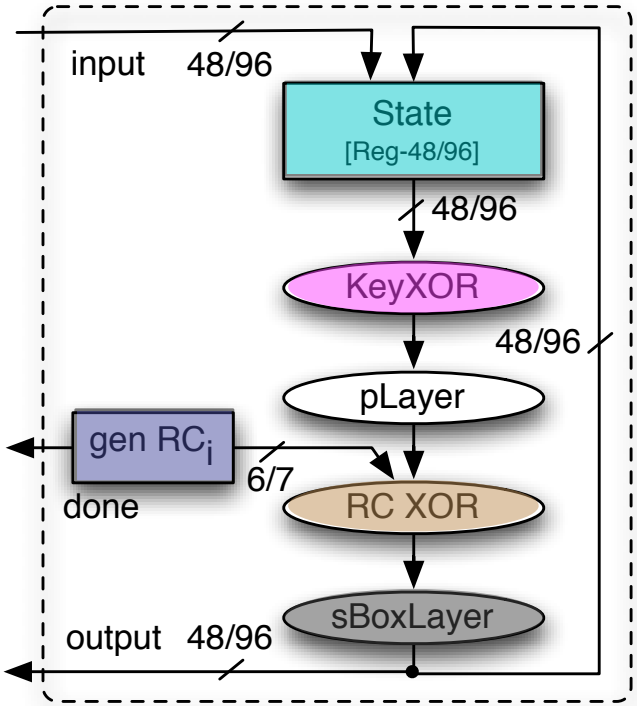
48 CLK **96 CLK**

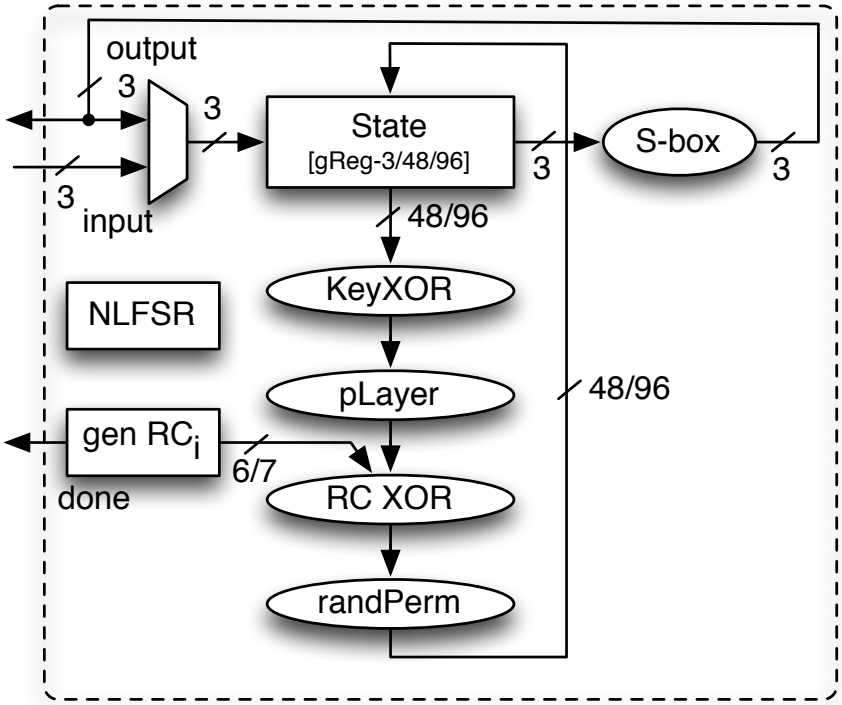


Implementation Results I

NANYANG TECHNOLOGICAL UNIVERSITY

round *UMCL18G212T3* library **serial**





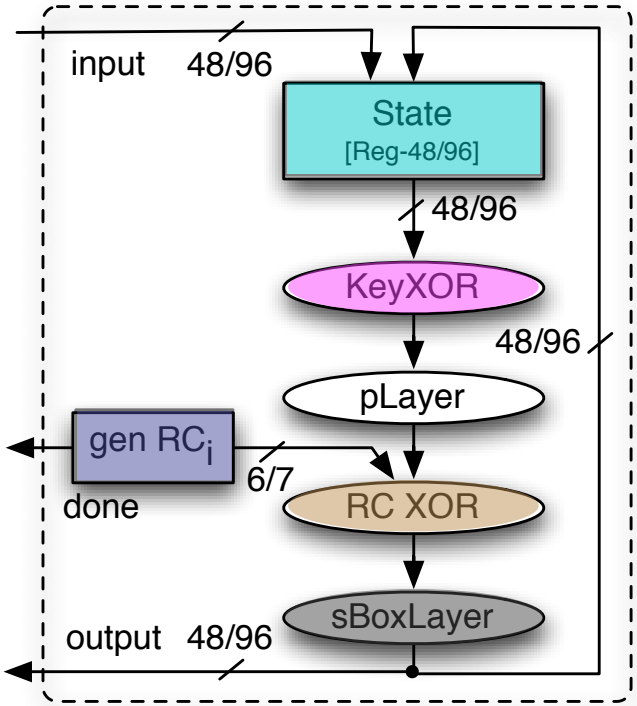
48 CLK **96 CLK**

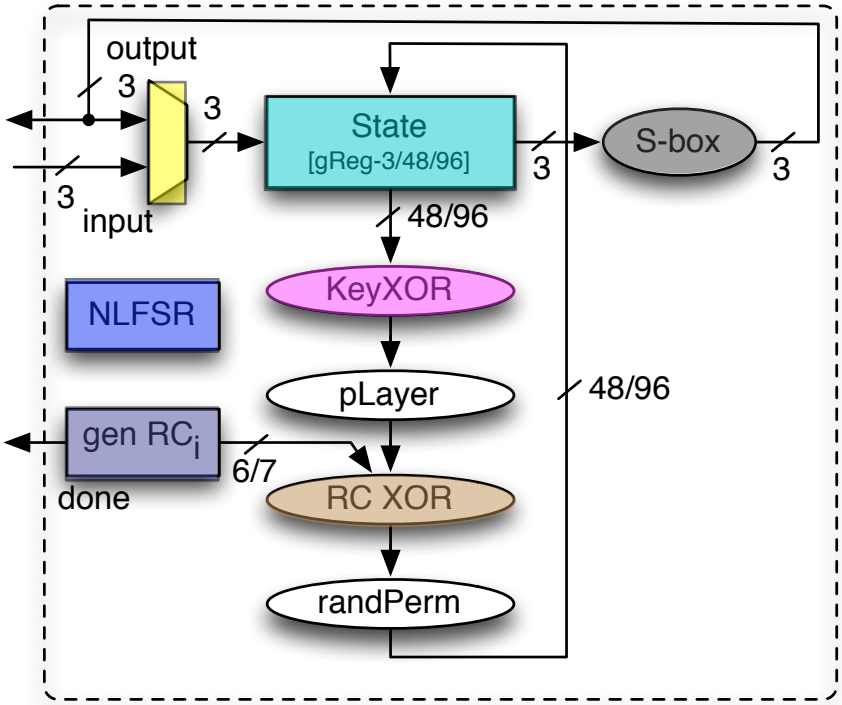
48*16 = 768 CLK **96*32 = 3072 CLK**

Implementation Results I

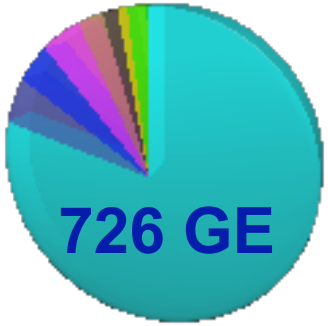
NANYANG TECHNOLOGICAL UNIVERSITY

round *UMCL18G212T3* library **serial**

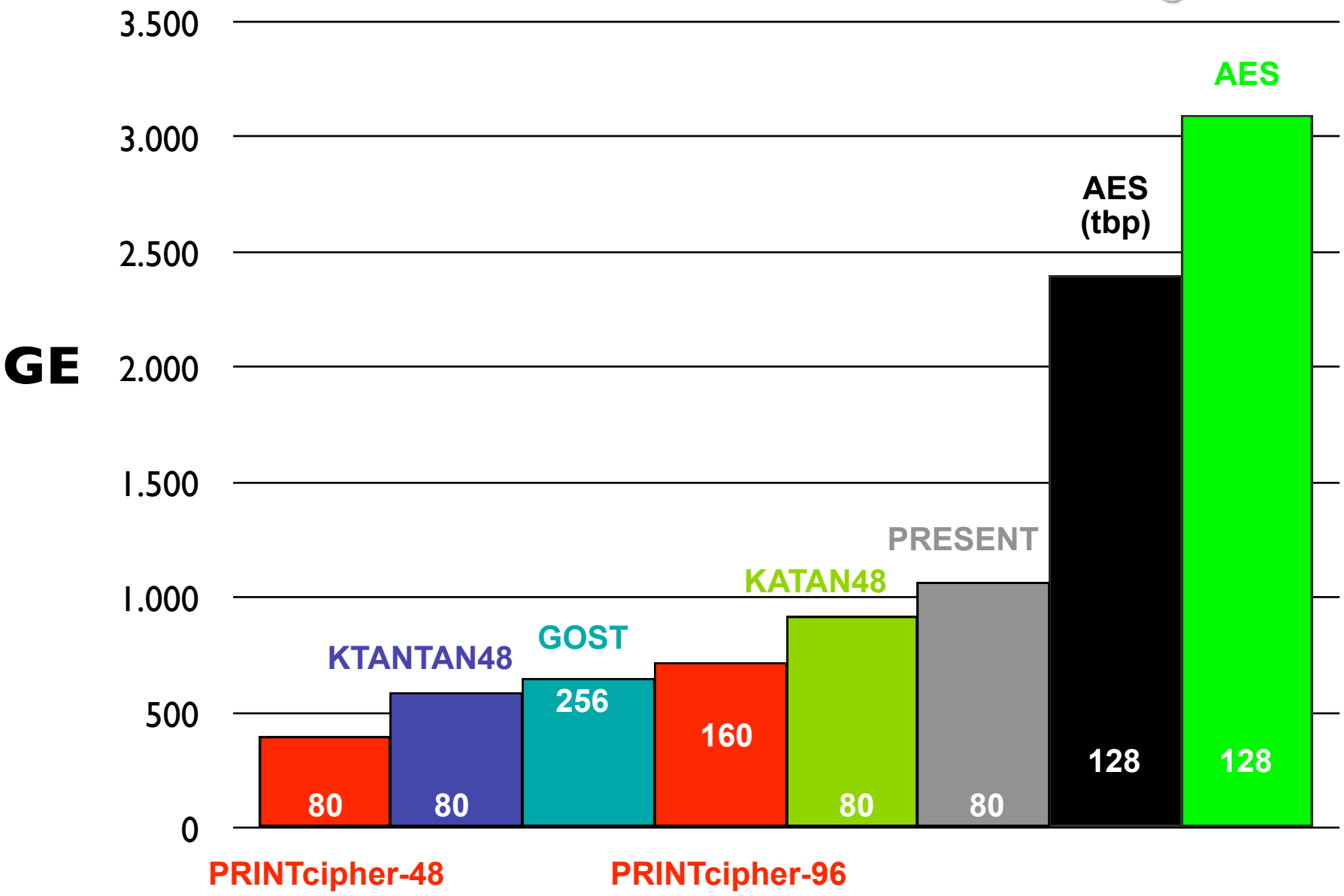




48 CLK **96 CLK** **48*16 = 768 CLK** **96*32 = 3072 CLK**



Implementation Results II



Outline

- Motivation
- PRINTcipher
- Security Analysis
- Implementation Results
- **Conclusions**

Conclusions

NANYANG TECHNOLOGICAL UNIVERSITY

- considered IC printing
- proposed PRINTcipher-48 and PRINTcipher-96
- PRINTcipher:
  - takes advantage of unique features of IC printing
  - requires only 402 GE
  - provides good scalability: +100 GE = 16x faster
  - object of study rather than being suitable for deployment

Conclusions

NANYANG TECHNOLOGICAL UNIVERSITY

- considered IC printing
- proposed PRINTcipher-48 and PRINTcipher-96
- PRINTcipher:
  - takes advantage of unique features of IC printing
  - requires only 402 GE
  - provides good scalability: +100 GE = 16x faster
  - object of study rather than being suitable for deployment

Please study PRINTcipher!

Thank you!

Questions?

Axel Poschmann
Division of Mathematical Sciences
Nanyang Technological University
SPMS-MAS-04-20, 50 Nanyang Avenue
Singapore 639798
T (65) 6513-7459 GMT+8h
E axel.poschmann@gmail.com
W www.ntu.edu.sg/home/aposchmann/