TOWARDS SECURE CRYPTOGRAPHIC SOFTWARE IMPLEMENTATION AGAINST SIDE-CHANNEL POWER ANALYSIS ATTACKS

Northeastern University Energy-Efficient and Secure Systems Lab

Northeastern University

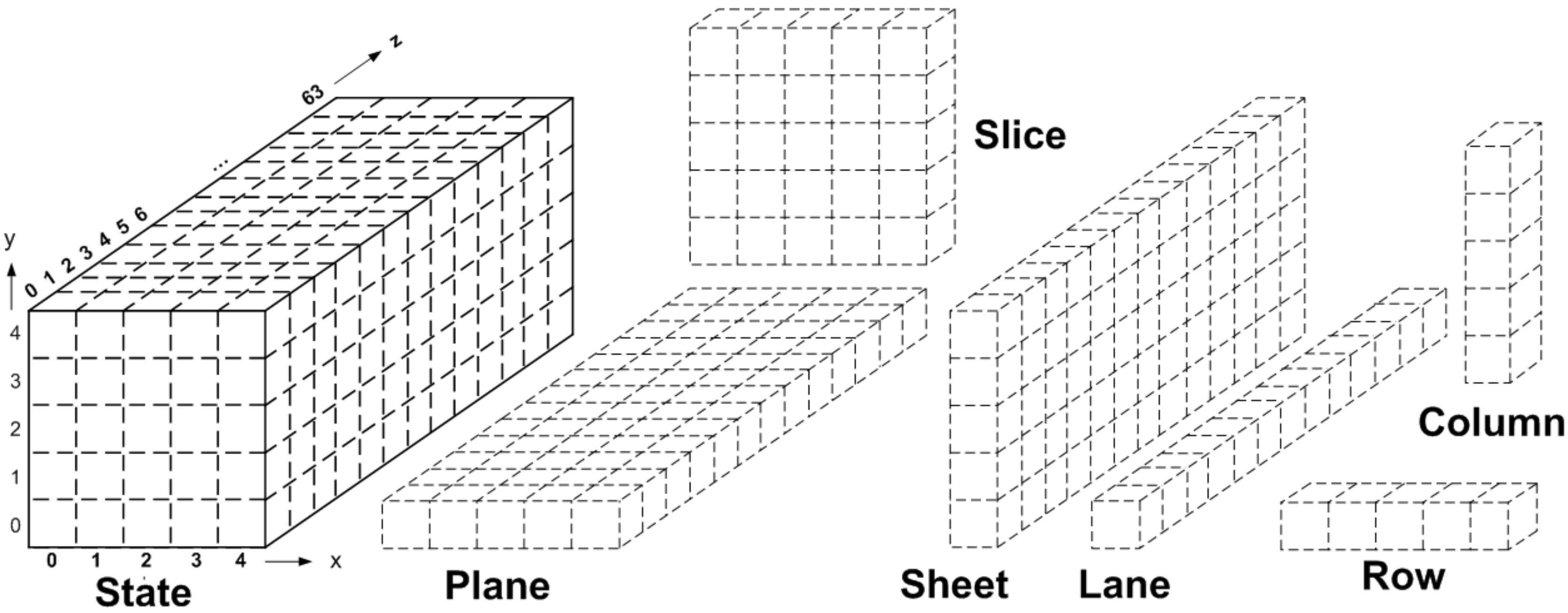
Outline

- **Details of Keccak**
- Previous attacks on Keccak
- Side-channel attacks on R_1
- Conclusion

Details of Keccak (1)

- Selected as the winner of the NIST hash function competition on October 2, 2012
- Draft FIPS PUB 202, May 2014
  - SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256
  - Internal state size: 1600 ($5 \times 5 \times 64$)
- In this paper:
  - 320 key bits, fill the first plane

Details of Keccak (2)

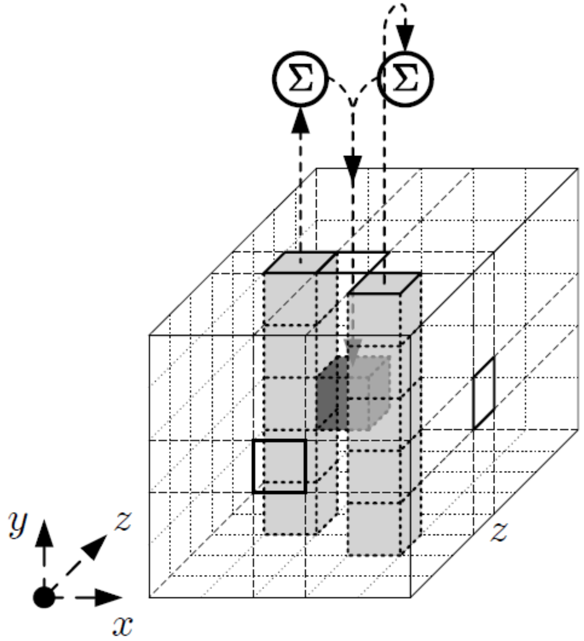


$$R_{i+1} = \iota \circ \chi \circ \pi \circ \rho \circ \theta(R_i), \quad i \in \{0,1\ldots\ 23\}$$

Details of Keccak (3)

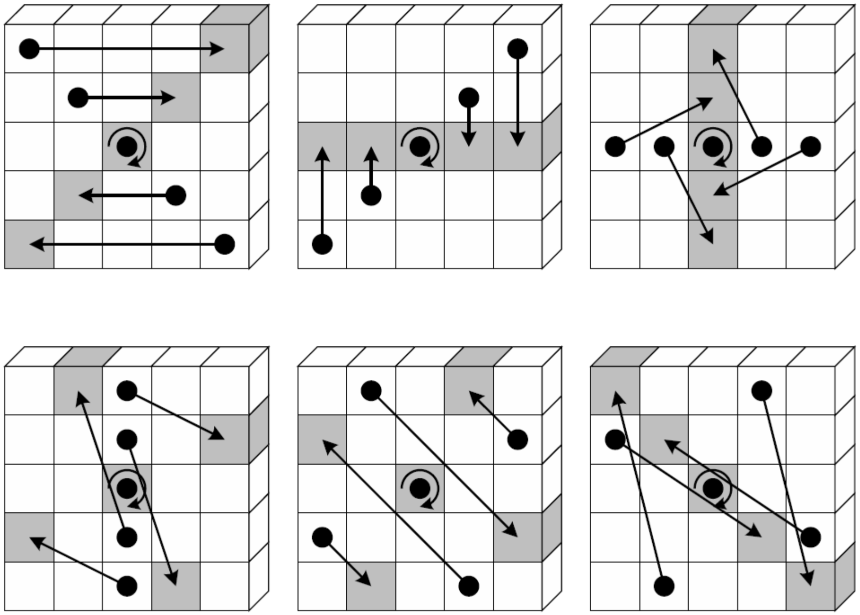
- θ is a linear operation which involves 11 input bits and outputs a single bit.

$$S'(x,y,z) = S(x,y,z) \oplus (\oplus^{4}_{i=0} S(x-1,i,z)) \oplus (\oplus^{4}_{i=0} S(x+1,i,z-1)).$$



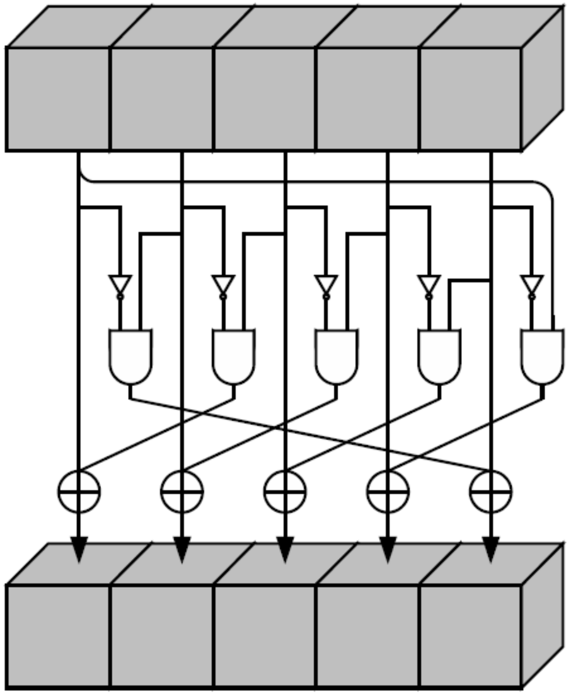
Details of Keccak (4)

- ρ is the permutation over the bits along the z-axis.
- π changes *x* and y of the bits



Details of Keccak (5)

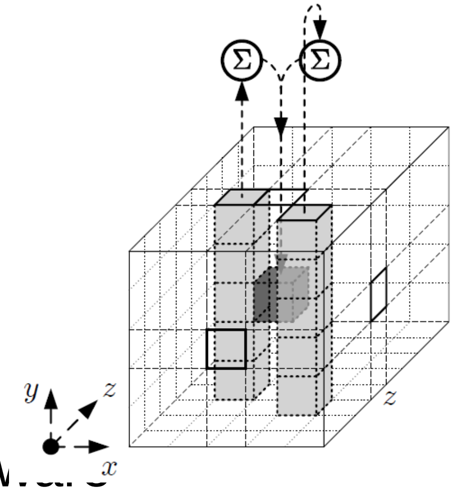
- χ is the only non-linear step
- ι is addition with a constant number



Outline

- The details of Keccak
- **Previous attacks on Keccak**
- Side-channel attacks on R_1
- Conclusion

Side-channel attacks on θ (1)



- Previous papers focus on θ
  - The first step of Keccak
  - Intermediate variables are stored in registers for software implementations
  - Hardware implementations also have leakage of θ because of Keccak properties

M. Taha and P. Schaumont. Dierential power analysis of MAC-keccak at any key-length. In International Workshop on Security, pages 68-82, Nov. 2013.

M. Taha and P. Schaumont. Side-channel analysis of MAC-Keccak. In IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pages 125{130, June 2013.

P. Luo, Y. Fei, X. Fang, A. Ding, M. Leeser, and D. Kaeli. Power analysis attack on hardware implementation of MAC-keccak on FPGAs. In ReConFigurable Computing and FPGAs (ReConFig), 2014 International Conference on, pages 1-7, Dec 2014.

Outline

- The details of Keccak
- Previous attacks on Keccak
- **Side-channel attacks on R_1**
- Conclusion

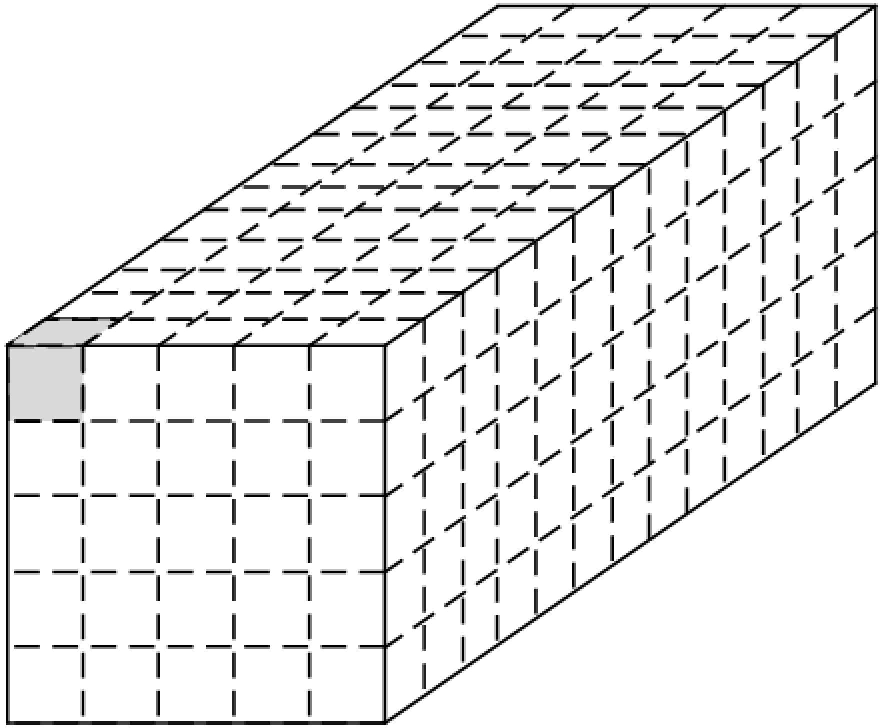
Side-channel attacks on R_1 (1)

- Each χ_{out} bit involves 3 bits of π_{out};
- Each π_{out} bit involves 2 key bits.

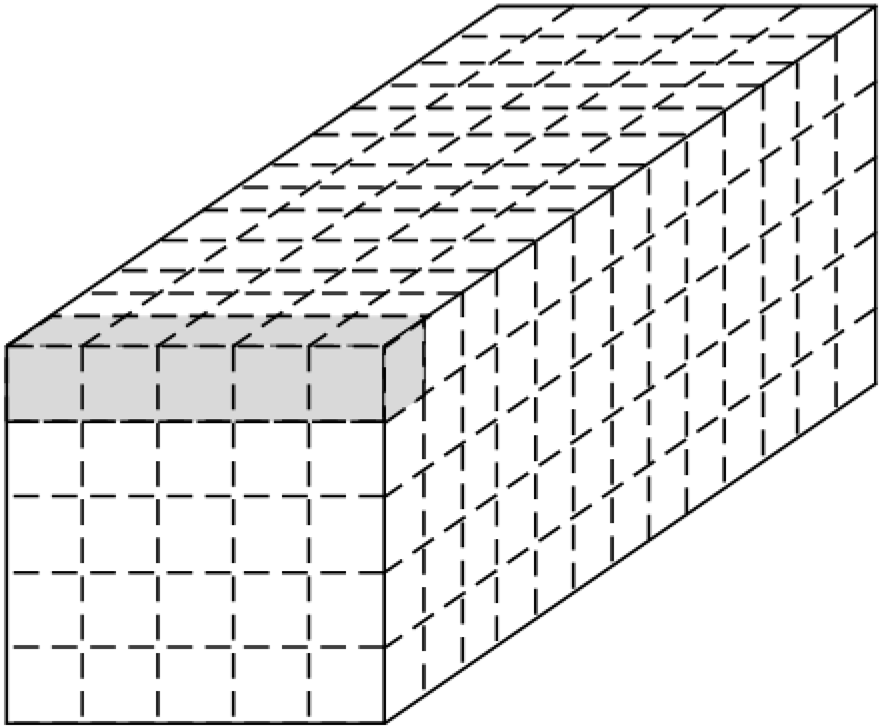
Conclusion :

(1) One bit SNR is too low;

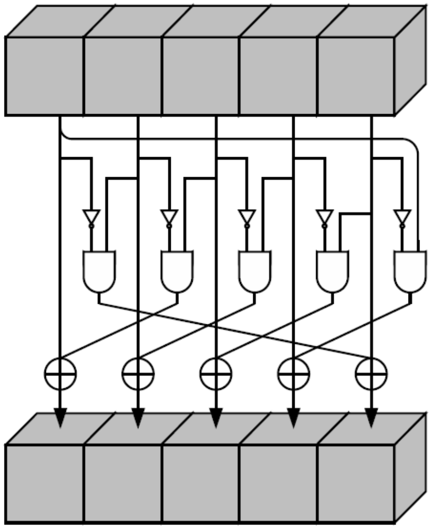
(2) One bits involves at least 6 key bits.



Side-channel attacks on R_1 (2)

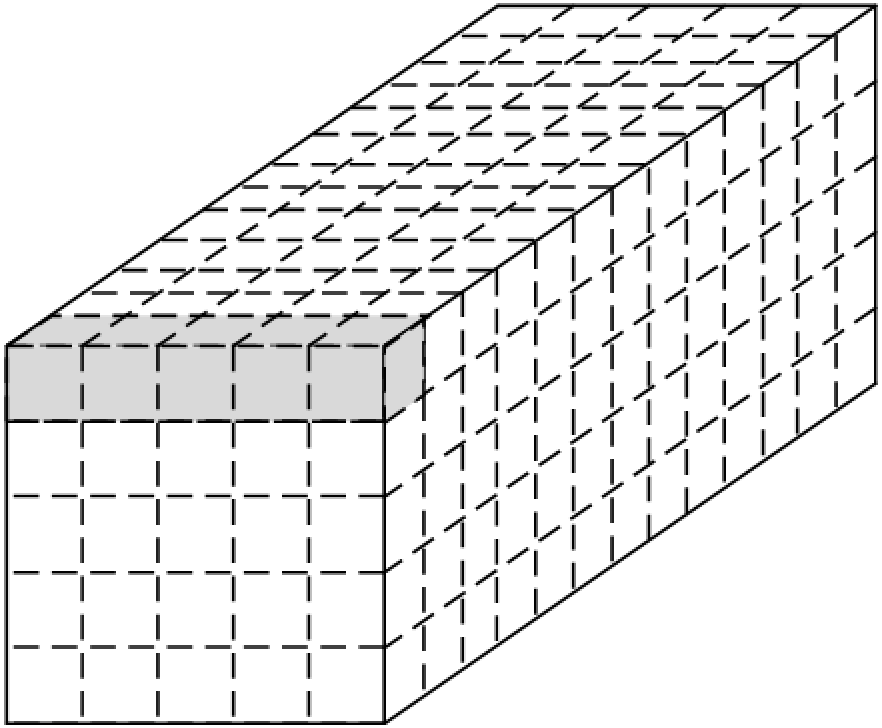


$R_1([0:4],4,0)$



5 bits of each row operate on each other, thus 11 key bits in total. Attackable?

Side-channel attacks on R_1 (3)



$R_1([0:4],4,0)$

Hamming distance :

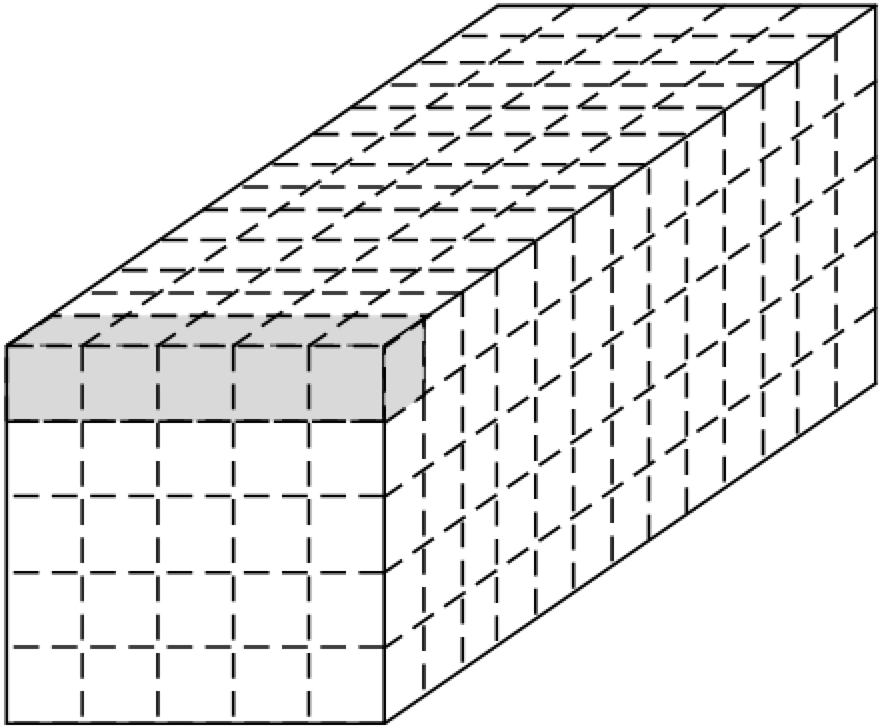
$HD(P([0:4],4,0), R_1([0:4],4,0))$

$P([0:4],4,0)$ is known, how to get R_1 :

$$R_1(0,4,0) \leftrightarrow \theta_{out}(2,0,2) \leftrightarrow P(2,0,2)$$
$$R_1(1,4,0) \leftrightarrow \theta_{out}(3,1,9) \leftrightarrow P(3,1,9)$$
$$R_1(2,4,0) \leftrightarrow \theta_{out}(4,2,25) \leftrightarrow P(4,2,25)$$
$$R_1(3,4,0) \leftrightarrow \theta_{out}(0,3,23) \leftrightarrow P(0,3,23)$$
$$R_1(4,4,0) \leftrightarrow \theta_{out}(1,4,62) \leftrightarrow P(1,4,62)$$

$P(2,0,2)$ is also a key bit, thus 11 key bits

Side-channel attacks on R_1 (4)

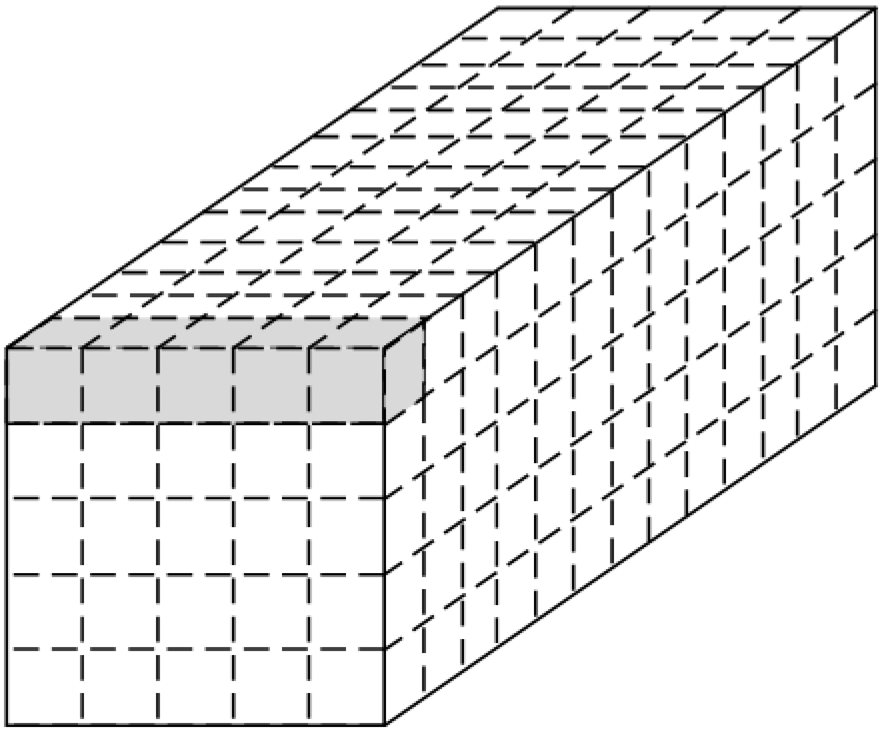


$R_1([0:4],4,0)$

π and ρ only change the position of bits, the values are not changed.

$$R_1(0,4,0) \leftrightarrow \theta_{out}(2,0,2) \leftrightarrow P(2,0,2)$$
$$R_1(1,4,0) \leftrightarrow \theta_{out}(3,1,9) \leftrightarrow P(3,1,9)$$
$$R_1(2,4,0) \leftrightarrow \theta_{out}(4,2,25) \leftrightarrow P(4,2,25)$$
$$R_1(3,4,0) \leftrightarrow \theta_{out}(0,3,23) \leftrightarrow P(0,3,23)$$
$$R_1(4,4,0) \leftrightarrow \theta_{out}(1,4,62) \leftrightarrow P(1,4,62)$$

Side-channel attacks on R_1 (5)

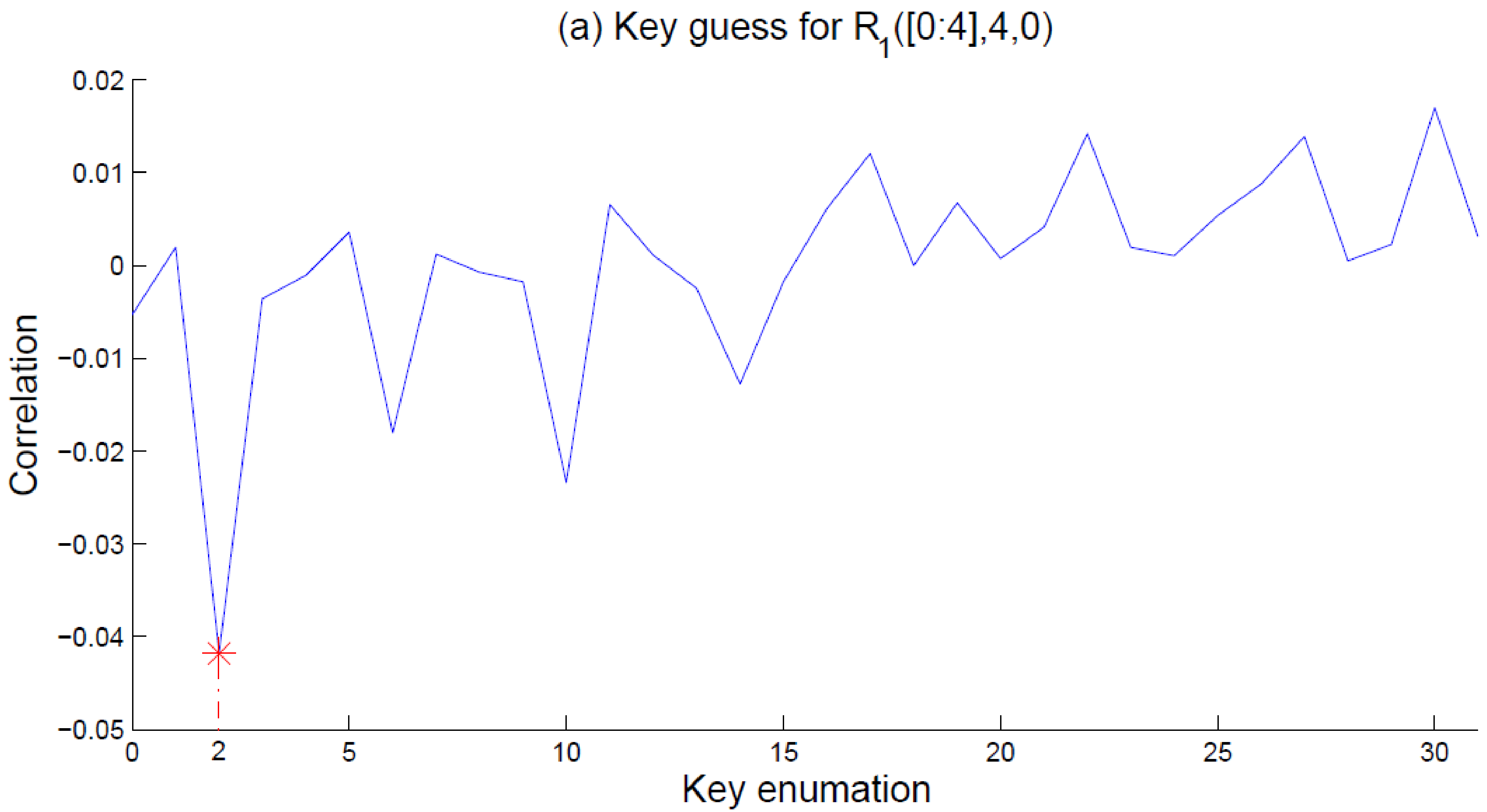


$$R_1(0,4,0) \leftrightarrow \theta_{out}(2,0,2) \leftrightarrow P(2,0,2)$$
$$R_1(1,4,0) \leftrightarrow \theta_{out}(3,1,9) \leftrightarrow P(3,1,9)$$
$$R_1(2,4,0) \leftrightarrow \theta_{out}(4,2,25) \leftrightarrow P(4,2,25)$$
$$R_1(3,4,0) \leftrightarrow \theta_{out}(0,3,23) \leftrightarrow P(0,3,23)$$
$$R_1(4,4,0) \leftrightarrow \theta_{out}(1,4,62) \leftrightarrow P(1,4,62)$$

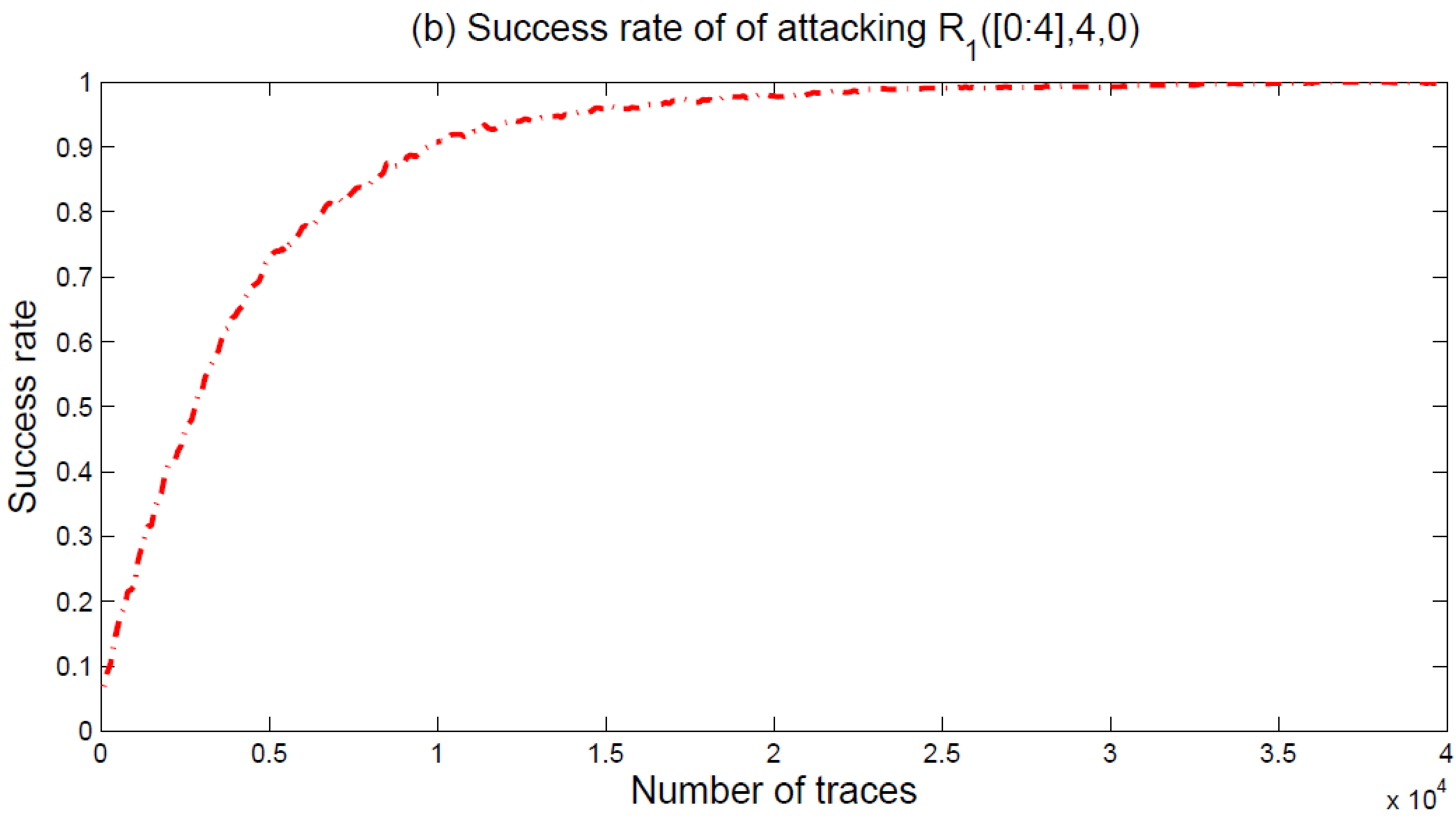
What can we recover:

$$kg_1 = P(2,0,2) \oplus P(1,0,2) \oplus P(3,0,1)$$
$$kg_2 = P(2,0,9) \oplus P(4,0,8)$$
$$kg_3 = P(3,0,25) \oplus P(0,0,24)$$
$$kg_4 = P(4,0,23) \oplus P(1,0,22)$$
$$kg_5 = P(1,0,62) \oplus P(2,0,61)$$

Side-channel attacks on R_1 (6)



Side-channel attacks on R_1 (7)



Side-channel attacks on R_1 (8)

$$
\begin{cases} KG_1 = \{S(x-1,0,z) \oplus S(x,0,z) \oplus S(x+1,0,z-1)\} \\ \qquad KG_2 = \{S(x-1,0,z) \oplus S(x+1,0,z-1)\} \end{cases}
$$

$$
x \in \{0,1\ldots\}, z \in \{0,1\ldots 63\}.
$$

- Combine 2-bit XORs and 3-bit XORs to recover key bits
- There are 320 identical 2-bit XORs and 3-bit XORs

Outline

- Details of Keccak
- Previous attacks on Keccak
- Side-channel attacks on R_1
- **Conclusion**

Conclusion

- The first round output of Keccak can be attacked
- Attacking methods are different for software/hardware implementations
- Countermeasures should be added

THANKS!

http://tescase.coe.neu.edu/

Northeastern University