# Cube-Attack-Like Cryptanalysis of Round-Reduced KECCAK Using MILP

**Ling Song**, Jian Guo

NANYANG TECHNOLOGICAL UNIVERSITY

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

FSE 2019 @ Paris, France

# Outlines

1. KECCAK and its Relatives
2. Cube-Attack-Like Crytanalysis
3. MILP Model for Searching Cubes
4. Main Results

# Outline

# Keccak

- Permutation-based primitive
  - Designed by Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche
  - Selected as SHA-3 standard
  - Underlying permutation: Keccak-$p[1600, 24]$
- Keccak under keyed modes: KMAC, Keccak-MAC
- Its relatives
  - Authenticated encrytion: Keyak, Ketje
  - Pseudorandom function: Kravatte

# Motivation

Cube attacks on Keyed Keccak:

- Cube-attak-like cryptanalysis (Dinur et al., EC'15)
- Conditional cube attacks (Huang et al., EC'17)

Mixed Integer Linear Programming (MILP) models greatly improved conditional cube attacks on keyed Keccak

- Li et al., AC'17
- Song et al., AC'18

How about cube-attack-like cryptanalysis using MILP?

# Our Work

- Propose an MILP model for cube-attack-like cryptanalysis of keyed KECCAK
- Apply the model to KETJE, KECCAK-MAC and XOODOO

| Target | $\|K\|$ | Rounds | T | M | Source |
|---|---|---|---|---|---|
| KETJE Jr V1 | 96 | 5/13 | $2^{56}$ | $2^{38}$ | [DLWQ17] |
| | 96 | 5/13 | $2^{36.86}$ | $2^{18}$ | this |
| | 72 | 6/13 | $2^{68.04}$ | $2^{34}$ | this |
| KETJE Jr V2 | 96 | 5/13 | $2^{50.32}$ | $2^{32}$ | [DLWQ17] |
| | 96 | 5/13 | $2^{34.91}$ | $2^{15}$ | this |
| | 80 | 6/13 | $2^{59.17}$ | $2^{25}$ | this |
| KETJE Sr V2 | 128 | 7/13 | $2^{113.58}$ | $2^{48}$ | [DLWQ17] |
| | 128 | 7/13 | $2^{99}$ | $2^{33}$ | this |
| XOODOO * | 128 | 6/- | $2^{89}$ | $2^{55}$ | this |
| KECCAK-MAC-512 | 128 | 7/24 | $2^{111}$ | $2^{46}$ | this |

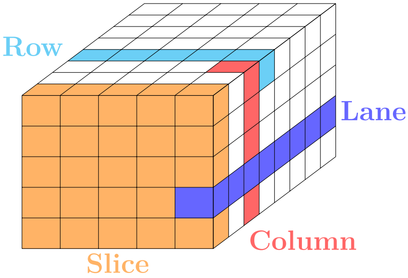
* In the KETJE mode.

# KECCAK-$p[b, n_r]$ Permutation

- $b$ bits: seen as a $5 \times 5$ array of $\frac{b}{25}$-bit lanes, $A[x, y]$
- $n_r$ rounds
- each round $R$ consists of five steps:

$$R = \iota \circ \chi \circ \pi \circ \rho \circ \theta$$

- $\chi$ : S-box on each row
- $\pi, \rho$: change the position of state bits




http://www.iacr.org/authors/tikz/

# KECCAK-$p$ Round Function

Internal state A: a $5 \times 5$ array of lanes

$\theta$ step $C[x] = A[x,0] \oplus A[x,1] \oplus A[x,2] \oplus A[x,3] \oplus A[x,4]$
$D[x] = C[x-1] \oplus (C[x+1] \lll 1)$
$A[x,y] = A[x,y] \oplus D[x]$

$\rho$ step $A[x,y] = A[x,y] \lll r[x,y]$
- The constants $r[x,y]$ are the rotation offsets.

$\pi$ step $A[y, 2*x+3*y] = A[x,y]$

$\chi$ step $A[x,y] = A[x,y] \oplus ((\ A[x+1,y])\&A[x+2,y])$

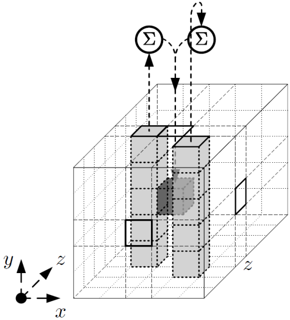
$\iota$ step $A[0,0] = A[0,0] \oplus RC[i]$
- $RC[i]$ are the round constants.

The only non-linear operation is $\chi$ step.

# KECCAK-$p$ Round Function: $\theta$

$\theta$ step: adding two columns to the current bit

$$
\begin{aligned}
C[x] =& A[x,0] \oplus A[x,1] \oplus A[x,2] \oplus \\
& A[x,3] \oplus A[x,4] \\
D[x] =& C[x-1] \oplus (C[x+1] \lll 1) \\
A[x,y] =& A[x,y] \oplus D[x]
\end{aligned}
$$

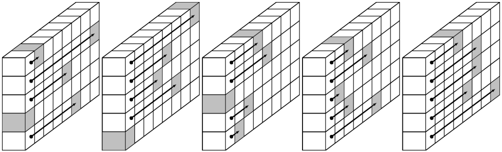



http://keccak.noekeon.org/

- The Column Parity kernel
  - If $C[x] = 0, 0 \leq x < 5$, then the state A is in the CP kernel.

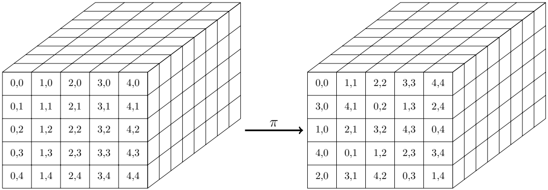
# KECCAK-$p$ Round Function: $\rho, \pi$

$\rho$ step: lane level rotations, $A[x, y] = A[x, y] \lll r[x, y]$



http://keccak.noekeon.org/

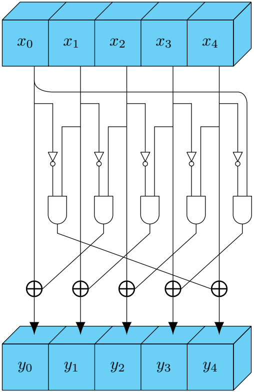
$\pi$ step: permutation on lanes, $A[y, 2*x+3*y] = A[x, y]$



# Keccak-$p$ Round Function: $\chi$

$\chi$ step: 5-bit S-boxes, nonlinear operation on rows

$$
\begin{aligned}
y_0 &= x_0 + (x_1 + 1) \cdot x_2, \\
y_1 &= x_1 + (x_2 + 1) \cdot x_3, \\
y_2 &= x_2 + (x_3 + 1) \cdot x_4, \\
y_3 &= x_3 + (x_4 + 1) \cdot x_0, \\
y_4 &= x_4 + (x_0 + 1) \cdot x_1.
\end{aligned}
$$

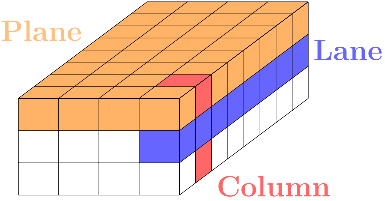



- Nonlinear term: product of two adjacent bits in a row.

# Xoodoo Permutation

- Sister of Keccak-$p$
- 384 bits: $4 \times 3 \times 32$
- Round function $R$:

$$R = \rho_{east} \circ \chi \circ \iota \circ \rho_{west} \circ \theta$$




- $\chi$ : S-box on each column
- $\rho_{west}, \rho_{east}$: change the position of bits in a plane

# Xoodoo Round Function

Internal state A: a $3 \times 4$ array of 32-bit lanes

$\theta$ step $C[x] = A[x,0] \oplus A[x,1] \oplus A[x,2]$
$D[x] = (C[x-1] \lll 5) \oplus (C[x+1] \lll 14)$
$B[x,y] = A[x,y] \oplus D[x]$

$\rho_{west}$ step $A[x,0] = B[x,0], A[x,1] = B[x-1,1], A[x,2] = B[x,2] \lll 11$

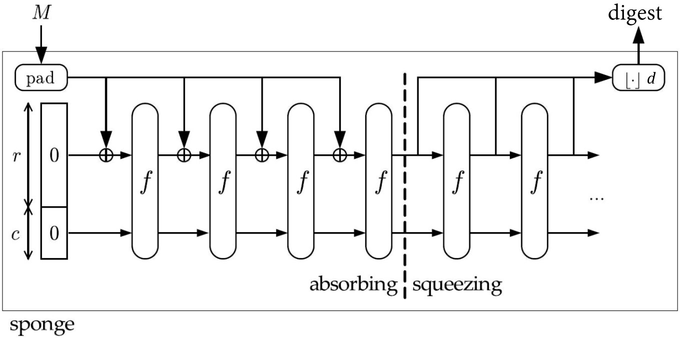
$\iota$ step $A[0,0] = A[0,0] \oplus RC[i]$

$\chi$ step $B[x,y] = A[x,y] \oplus ((\ A[x,y+1])\&A[x,y+2])$

$\rho_{east}$ step $A[x,0] = B[x,0], A[x,1] = B[x,1] \lll 1, A[x,2] = B[x-2,2] \lll 8$

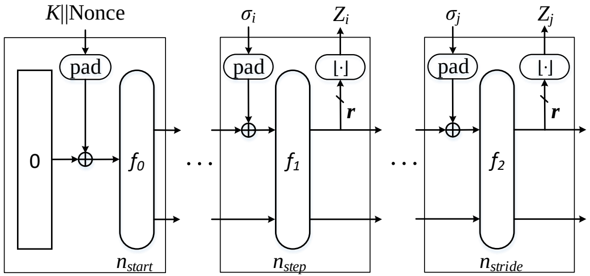
The only non-linear operation is $\chi$ step.

# KECCAK: KECCAK-$p[1600, 24]$ + Sponge




- Sponge construction [BDPV11]
  - $b$-bit permutation $f$
  - Two parameters: bitrate $r$, capacity $c$, and $b = r + c$.
- KECCAK-MAC
  - Take $K||M$ as input

# KETJE: KECCAK-$p^\star$ + MonkeyDuplex




- KECCAK-$p^\star[b, n_r] = \pi \circ$KECCAK-$p[b, n_r] \circ \pi^{-1}$
- $n_{start} = 12,\ n_{step} = 1,\ n_{stride} = 6$
- 4 variants

| | | | | | |
|---|---|---|---|---|---|
| Jr: | $b = 200$ | $r = 16$, | Minor: | $b = 800$ | $r = 128$ |
| Sr: | $b = 400$ | $r = 32$, | Major: | $b = 1600$ | $r = 256$ |

- XOODOO can be an alternative permutation.

# Outline

# Cube Attacks [DS09] (Higher Order Differential Cryptanalysis)

- Given a Boolean polynomial $f(k_0, \ldots, k_{n-1}, v_0, \ldots, v_{m-1})$ and a monomial $t_I = \wedge_{i_r \in I} v_{i_r}$, $I = (i_1, \ldots, i_d)$, $f$ can be written as

$$f(k_0, \ldots, k_{n-1}, v_0, \ldots, v_{m-1}) = t_I \cdot p_{S_I} + q(k_0, \ldots, k_{n-1}, v_0, \ldots, v_{m-1})$$

  - $q$ contains terms that are not divisible by $t_I$
  - $p_{S_I}$ is called the superpoly of $I$ in $f$
  - $v_{i_1}, \ldots, v_{i_d}$ are called cube variables. $d$ is the dimension.
- The the cube sum is exactly

$$\sum_{(v_{i_1}, \ldots, v_{i_d}) \in C_I} f(k_0, \ldots, k_{n-1}, v_0, \ldots, v_{m-1}) = p_{S_I}$$

- Cube attacks: $p_{S_I} = L(k_0, \ldots, k_{n-1})$ is a linear polynomial.
- Solve a set of linear equations and recover the key.

# Cube-Attack-Like Cryptanalysis [DMP+15]

Cube attack: $p_{S_I} = L(k_0, \ldots, k_{n-1})$
Cube-attack-like: using $n_a$ aux. vars, $p'_{S_I} = L'(k_{i_1}, \ldots, k_{i_{n_i}})$, $n_i < n$

Offline phase Build a lookup table. $T = 2^{n_i+d}, M = 2^{n_i}$.

| $k_{i_1} \ldots k_{i_{n_i}}$ | Cube sum |
|---|---|
| 00...00 | 01011... |
| 00...01 | 11010... |
| ... | ... |
| 11...11 | 10110... |

Online phase $T = 2^{n_a+d}$

1. Set the value of $n_a$ aux. vars.
2. Query the cipher to obtain the cube sum.
3. Look up the table to recover the $n_i$ key bits

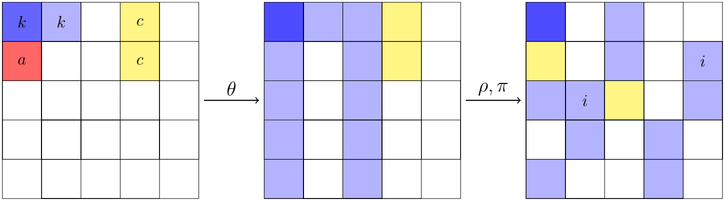
# Task of the MILP Model

The algebraic degree of $n$ rounds is $2^n$. The first round can be linearized by avoiding adjacent cube variables.

1. Find $2^{n-1}$-dimensional cubes where $n$ is as large as possible; (attack more rounds).
2. Find balanced attacks where $n_i$ and $n_a$ are close and as small as possible. (low complexity).

# Outline

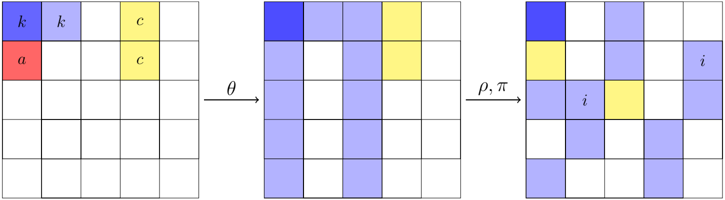
# An Example




$$d = 64,\ n_a = 64,\ n_i = 64,$$

the cube sum of up to 7 rounds depends on only 64 key bits

# An Example




$$d = 64,\ n_a = 64,\ n_i = 64,$$

the cube sum of up to 7 rounds depends on only 64 key bits

Core of the Model

1. Propagation of cube variables and the dimension $d$ (through $\theta$)
2. Propagation of key bits and $n_a$ (through $\theta$)
3. Interaction of key bits and cube variables, and $n_i$ (before $\chi$)

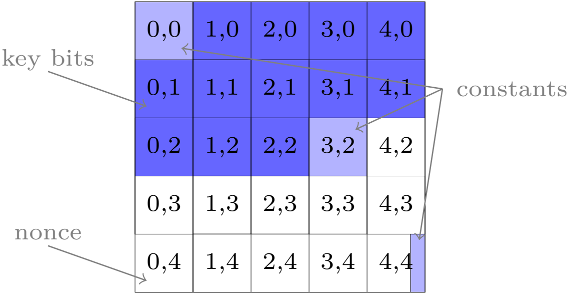
# Mixed Integer Linear Programming

- An MILP problem is of the form

$$
\begin{aligned}
\texttt{min} \quad & c^T x \\
& Ax \geq b \\
& x \geq 0 \\
& x \in \mathbb{Z}^n
\end{aligned}
\quad \rightarrow \quad
\begin{aligned}
\texttt{min} \quad & n_i, n_a \\
& d = 2^{n-1} \\
& Ax \geq b \\
& x \in \{0, 1\}^n
\end{aligned}
$$

- Solvers
  - Gurobi, CPLEX, SCIP, ...
- Application to cryptanalysis since Mouha et al.'s pioneering work [MWGP11]

# Model of KETJE as an Example



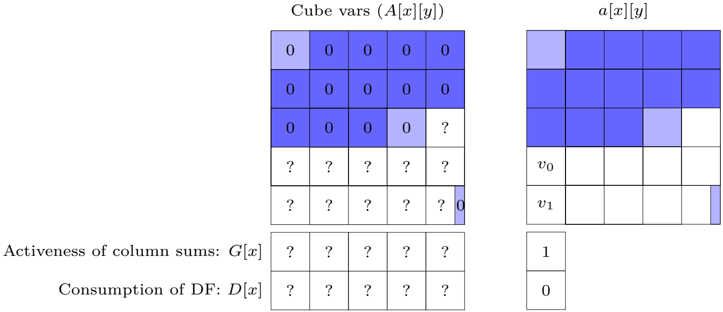

Initial state of Ketje Jr V1

## Notations

- State: $a \xrightarrow{\theta} b \xrightarrow{\pi \circ \rho} c$
- Activeness: $A \xrightarrow{\theta} B \xrightarrow{\pi \circ \rho} C$

$A[x][y][z] = 1$ if bit $(x, y, z)$ is a cube variable.

# Propagation of Cube Variables and $d$




Example:
(1) $a[x][3][z] = v_0, a[x][4][z] = v_0$, then $A[x][3][z] = A[x][4][z] = 1,\ G[x][z] = 0,\ D[x][z] = 1$
(2) $a[x][3][z] = v_1, a[x][4][z] = v_2$, then $A[x][3][z] = A[x][4][z] = 1,\ G[x][z] = 1,\ D[x][z] = 0$

**Dimension $d$** $\quad d = \sum A[x][y][z] - \sum D[x][z]$

# Propagation of Cube Variables and $d$

- Relation of $D$, $G$ and $A$

| $A[x][y_0][z]$ | $A[x][y_1][z]$ | $G[x][z]$ | $D[x][z]$ | Inequalities |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | $A[x][y_0][z] + A[x][y_1][z] - G[x][z] - 2D[x][z] \geq 0,$ |
| 0 | 1 | 1 | 0 | $-A[x][y_1][z] + G[x][z] + D[x][z] \geq 0,$ |
| 1 | 0 | 1 | 0 | $-A[x][y_0][z] + G[x][z] + D[x][z] \geq 0.$ |
| 1 | 1 | 1 | 0 | |
| 1 | 1 | 0 | 1 | |

# Propagation of Cube Variables and $d$

## Activness of $b$

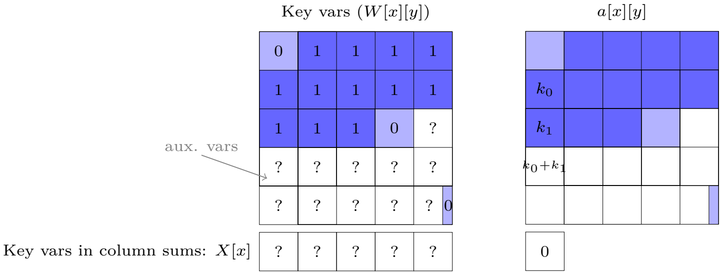
$B[x][y][z] = 1$ if any of $A[x][y][z]$, $G[x-1][z]$ or $G[x+1][z-1]$ is 1.

$$\begin{aligned} B[x][y][z] - A[x][y][z] &\geq 0, \\ B[x][y][z] - G[x+1][z-1] &\geq 0, \\ B[x][y][z] - G[x-1][z] &\geq 0, \\ A[x][y][z] + G[x-1][z] + G[x+1][z-1] - B[x][y][z] &\geq 0. \end{aligned}$$

## Activeness of $c$

$$C = \pi \circ \rho(B)$$

# Propagation of Key Bits and $n_a$




Example:

$a[x][1][z] = k_0$, $a[x][2][z] = k_1$, $a[x][3][z] = k_0 + k_1$,then $W[x][3][z] = 1$, $X[x][z] = 0$

Constraint: $X[x][z] + W[x][3][z] + W[x][4][z] = 1.$

$n_a$: $n_a = \sum_{x,z,3 \le y < 5} W[x][y][z] + \sum_z W[4][2][z].$

# Interaction of Key Bits and Cube Variables, and $n_i$

$$W \xrightarrow{\theta} Y \xrightarrow{\pi \circ \rho} Z$$

$$A \xrightarrow{\theta} B \xrightarrow{\pi \circ \rho} C$$

Collect key bits which are adjacent to cube vars.

$n_i = \#$bits $(x, y, z)$ where

$$Z[x][y][z] = 1 \wedge (C[x-1][y][z] = 1 \vee C[x+1][y][z])$$

# Outline

# Main Results

| Target | $\lvert K \rvert$ | Rounds | T | M | Source |
|---|---|---|---|---|---|
| KETJE Jr V1 | 96 | 5/13 | $2^{56}$ | $2^{38}$ | [DLWQ17] |
| | 96 | 5/13 | $2^{36.86}$ | $2^{18}$ | this |
| | 72 | 6/13 | $2^{68.04}$ | $2^{34}$ | this |
| KETJE Jr V2 | 96 | 5/13 | $2^{50.32}$ | $2^{32}$ | [DLWQ17] |
| | 96 | 5/13 | $2^{34.91}$ | $2^{15}$ | this |
| | 80 | 6/13 | $2^{59.17}$ | $2^{25}$ | this |
| KETJE Sr V2 | 128 | 7/13 | $2^{113.58}$ | $2^{48}$ | [DLWQ17] |
| | 128 | 7/13 | $2^{99}$ | $2^{33}$ | this |
| XOODOO * | 128 | 6/- | $2^{89}$ | $2^{55}$ | this |
| KECCAK-MAC-512 | 128 | 7/24 | $2^{111}$ | $2^{46}$ | this |

* In the KETJE mode.

In conclusion:

1. Cube-attack-like cryptanalysis with (vs. without) MILP
    - better attacks
    - easier to find cubes

2. This work does not threaten the security of any keyed KECCAK construction.

In conclusion:

1. Cube-attack-like cryptanalysis with (vs. without) MILP
    - better attacks
    - easier to find cubes

2. This work does not threaten the security of any keyed KECCAK construction.

Thank you for your attention!