T2 Symmetric Analysis

Maria Eichlseder Markus Schofnegger

Applied Cryptography 2 – ST 2020

Assignments (~~48~~ 32 points)

Assignment 1: Asymmetric Cryptanalysis and Multiparty Computation

- Release: 19 Mar 2020 (= team registration deadline!)
- Question time: 23 Apr 2020
- Submission: 30 Apr 2020

Assignment 2: Symmetric Cryptanalysis

- Release: 7 May 2020
- Question time: 4 Jun 2020
- Submission: 12 Jun 2020

A Related-Key Differential Analysis (AES)

Related-Key Differential Analysis (AES) 4 Points

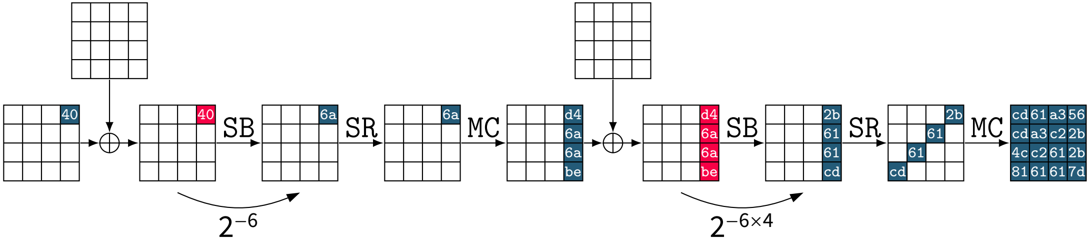
Analyze differential characteristics of AES (→ L7):

a Experimentally evaluate 2-round single-key differentials

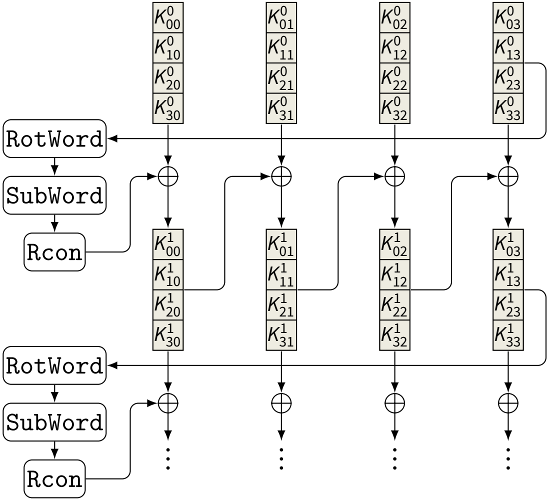
b Bound the number of active S-boxes under related keys using MILP

Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. **Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming.** Information Security and Cryptology – Inscrypt 2011. Vol. 7537. LNCS. Springer, 2011, pp. 57–76. DOI: 10.1007/978-3-642-34704-7_5.

A Related-Key Differential Analysis (AES) – Cheatsheet



A Related-Key Differential Analysis (AES) – Cheatsheet



- `RotWord`: rotate bytes (like in `ShiftRows`)
- `SubWord`: apply S-box (like in `SubBytes`)
- `Rcon`: add round constant

https://en.wikipedia.org/wiki/AES_key_schedule

B Linear Cryptanalysis (PRESENT)

Linear Cryptanalysis (PRESENT) 8 Points

Apply linear cryptanalysis to find the PRESENT key (→ L6):

a Compute the LAT and find a good linear approximation for 9 rounds

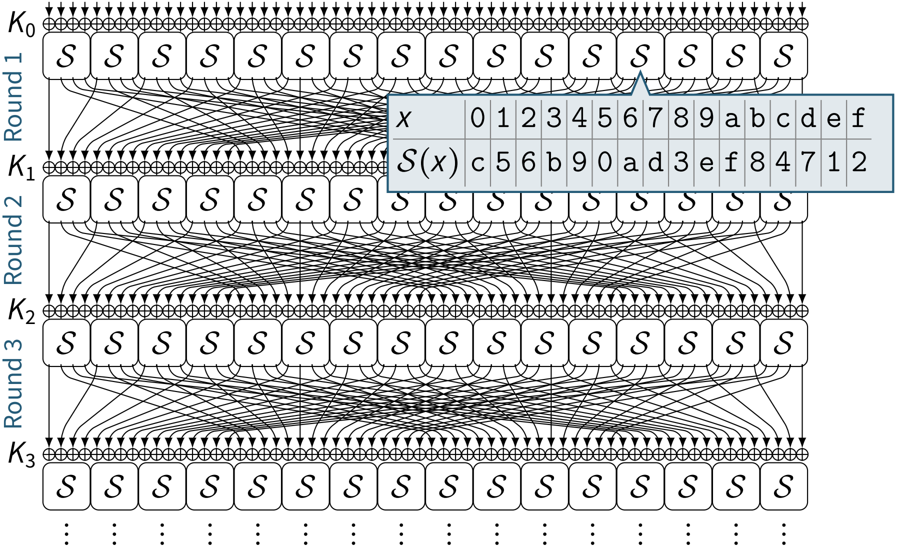
b Estimate the bias of the linear approximation and verify it experimentally

c Define and implement a key-recovery attack for 10-round PRESENT

Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. **PRESENT: An Ultra-Lightweight Block Cipher**. CHES 2007. Vol. 4727. LNCS. Springer, 2007, pp. 450–466. DOI: 10.1007/978-3-540-74735-2_31.

Mitsuru Matsui. **Linear Cryptanalysis Method for DES Cipher**. EUROCRYPT 1993. Vol. 765. LNCS. Springer, 1993, pp. 386–397. DOI: 10.1007/3-540-48285-7_33.

B Linear Cryptanalysis (PRESENT) – Cheatsheet



x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{S}(x)$	c	5	6	b	9	0	a	d	3	e	f	8	4	7	1	2

C Cube Attack (Keccak)

Cube Attack (Keccak) — 12 Points

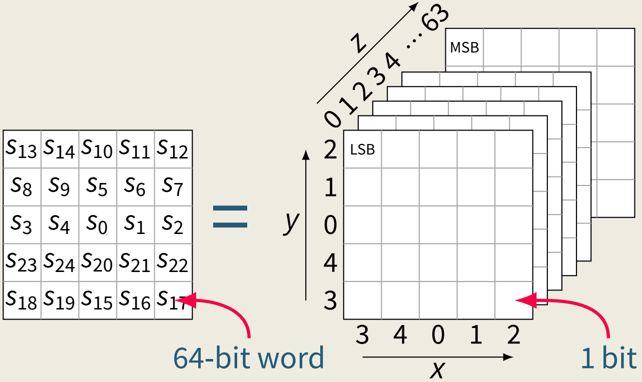
Implement the cube attack to find the Keccak-MAC key (→ L8):

- a Implement the cube-sum function for Keccak-MAC
- b Implement the offline phase (find suitable cubes)
- c Implement the online phase (equation-solving)
- d Demonstrate the cube attack for 4-round Keccak-MAC

Itai Dinur, Paweł Morawiecki, Josef Pieprzyk, Marian Srebrny, and Michał Straus. **Cube Attacks and Cube-Attack-Like Cryptanalysis on the Round-Reduced Keccak Sponge Function.** EUROCRYPT 2015. Vol. 9056. LNCS. Springer, 2015, pp. 733–761. DOI: 10.1007/978-3-662-46800-5_28. URL: http://ia.cr/2014/736.

C Cube Attack (Keccak) – Cheatsheet

State: 5 × 5 × 64 = 1600 bits



s_{13}	s_{14}	s_{10}	s_{11}	s_{12}
s_{8}	s_{9}	s_{5}	s_{6}	s_{7}
s_{3}	s_{4}	s_{0}	s_{1}	s_{2}
s_{23}	s_{24}	s_{20}	s_{21}	s_{22}
s_{18}	s_{19}	s_{15}	s_{16}	s_{17}

Operations

Register-oriented, but hardware-friendly:

$\oplus$ `xor`

$\odot$ `and`

$\lll_b$ `rotl` by b bits

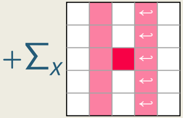
Steps in each Round

$\theta \to \rho \to \pi \to \chi \to \iota$

$S = s_0 \| s_1 \| \dots \| s_{24}$, $\quad s_0 = x_{63} \cdots x_0$, $\quad \dots \quad s_{24} = x_{1599} \cdots x_{1536}$

C Cube Attack (Keccak) – Cheatsheet

1 θ – Add neighbour column sums



$[x,y] \mathrel{+}= \Sigma_x$

$$\Sigma_x = \sum [x-1,\cdot] + \sum [x+1,\cdot] \lll 1$$

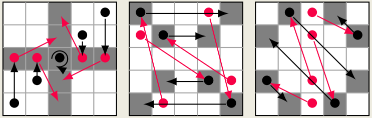
2 ρ – Rotate words by offset ρ_{xy}

$\xleftarrow[\rho_{xy}]{\text{ROTL}}$

25	39	3	10	43
55	20	36	44	6
28	27	0	1	62
56	14	18	2	61
21	8	41	45	15

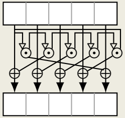
$[x,y] \lll= \rho_{xy}$

3 π – Permute words



4 χ – Apply 5-bit S-box to each row

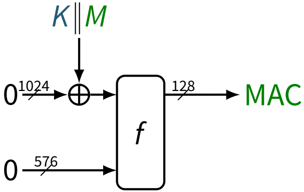
$\mathcal{S}$



$[\cdot,y] = \mathcal{S}([\cdot,y])$

5 ι – Add constant C_r to register s_0

C Cube Attack (KECCAK) – Cheatsheet



$K = s_0 \| s_1$ $\quad$ $M = s_2 \| s_3 \| \dots \| s_{15}$ $\quad$ $\mathrm{MAC} = s_0 \| s_1$

- 1-round cube for testing: cube variable $\{p_{128}\}$ → equations

$$\begin{aligned} y_{45} &= k_{66}, \\ y_{85} &= k_{106} + 1. \end{aligned}$$

Remaining Schedule

11 June		Holiday	(Friday) Deadline T2
18 June	👥	S3: Post-Quantum Crypto	
		S4: Fully Homomorphic Encryption	
25 June	👥	S5: Algebraic Attacks: Gröbner Bases etc.	
		Conclusion	
02 July	📝	VO Exam	