Cube Analysis of KATAN Family of Block Ciphers

Speaker: Bingsheng Zhang
University of Tartu, Estonia

This talk covers partial results of the paper "Algebraic, AIDA/Cube and Side Channel Analysis of KATAN Family of Block Ciphers"
by Gregory V. Bard, Nicolas T. Courtois, Jorge Nakahara Jr, Pouyan Sepehrdad and Bingsheng Zhang

Outline

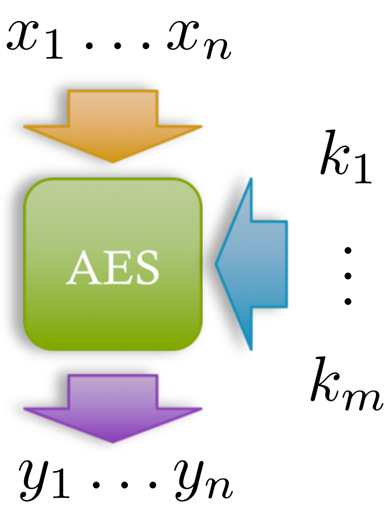
- Introduction to AIDA/Cube attacks
- KATAN family of block ciphers
- Cube attack on reduced-round KATAN family
- Side-channel attack against KATAN32
- Conclusion and further work

Introduction to Cube Attacks

- Cube attack (see eprint.iacr.org/2008/385) is also claimed to be a remake of AIDA (Algebraic IV Differential Attack, see eprint.iacr.org/2007/413)
- In this talk, we refer to Dinur and Shamir's version.
- Cube attack is generic key-recovery attack that can be applied to cryptosystems in a black-box setting, i.e. the internal structure of the target cipher is unknown.

Introduction to Cube Attacks

- A cryptosystem can be represented as multivariable polynomial over GF(2) in Algebraic Normal Form (ANF).



$$p_i(x_1, \dots, x_n, k_1, \dots, k_m) = y_i$$

However, the degrees of such polynomials are very high for a 'good' cryptosystem.

Introduction to Cube Attacks

- In chosen-plaintext/chosen-IV setting, the adversary can query $p_i(x_1, \ldots, x_n, k_1, \ldots, k_m) = y_i$ with arbitrary public variables x_i and fixed secret key variables, obtaining y_i.

- On the other hand, the polynomials can be decomposed as:

$$p(x_1, \ldots, x_n, k_1, \ldots, k_m) = t_I \cdot q_I + r(x_1, \ldots, x_n, k_1, \ldots, k_m)$$

where $t_I = \prod_i x_i, \;$ for $i \in I \subseteq [n]$

q_I does not contain x_i as they are factored out. $(x_i^2 = x_i)$

Introduction to Cube Attacks

- For example, let polynomial $p(x_1, x_2, x_3, k_1, k_2, k_3, k_4) =$
  $x_2 x_3 k_3 + x_1 x_2 k_1 + x_2 k_4 + x_1 x_3 k_2 k_3 + x_1 x_2 k_2 + 1$

- Let $I = \{1, 2\}$, so that $t_I = x_1 x_2$ and we have:
  $$p(x_1, x_2, x_3, k_1, k_2, k_3, k_4) = x_1 x_2 \cdot q_I + r$$
  where $q_I = k_1 + k_2$ and $r = x_2 x_3 k_3 + x_2 k_4 + x_1 x_3 k_2 k_3 + 1$

Introduction to Cube Attacks

- Main observation of cube attack: sum over GF(2) of all evaluations of p by assigning all possible binary values to the variables in I (and fixed value, usually 0, to all the public variables not in I) is exactly q_I.

$$
\begin{aligned}
\bigoplus_{x_i, i\in I} p(x_1, x_2, x_3, k_1, k_2, k_3, k_4) &= p(0,0,x_3,k_1,k_2,k_3,k_4)+ \\
& \quad p(0,1,x_3,k_1,k_2,k_3,k_4)+ \\
& \quad p(1,0,x_3,k_1,k_2,k_3,k_4)+ \\
& \quad p(1,1,x_3,k_1,k_2,k_3,k_4) \\
&= k_1 + k_2 = q_I
\end{aligned}
$$

Introduction to Cube Attacks

- Offline phase:
  - Gathering enough linear equations for key variables.
    - Linearity Test: $f(0) + f(a) + f(b) = f(a + b)$
    - Extract the equations.
- Online phase:
  - Query the gathered equations
  - Perform some cheap computations to recover the key.

KATAN Cipher Family

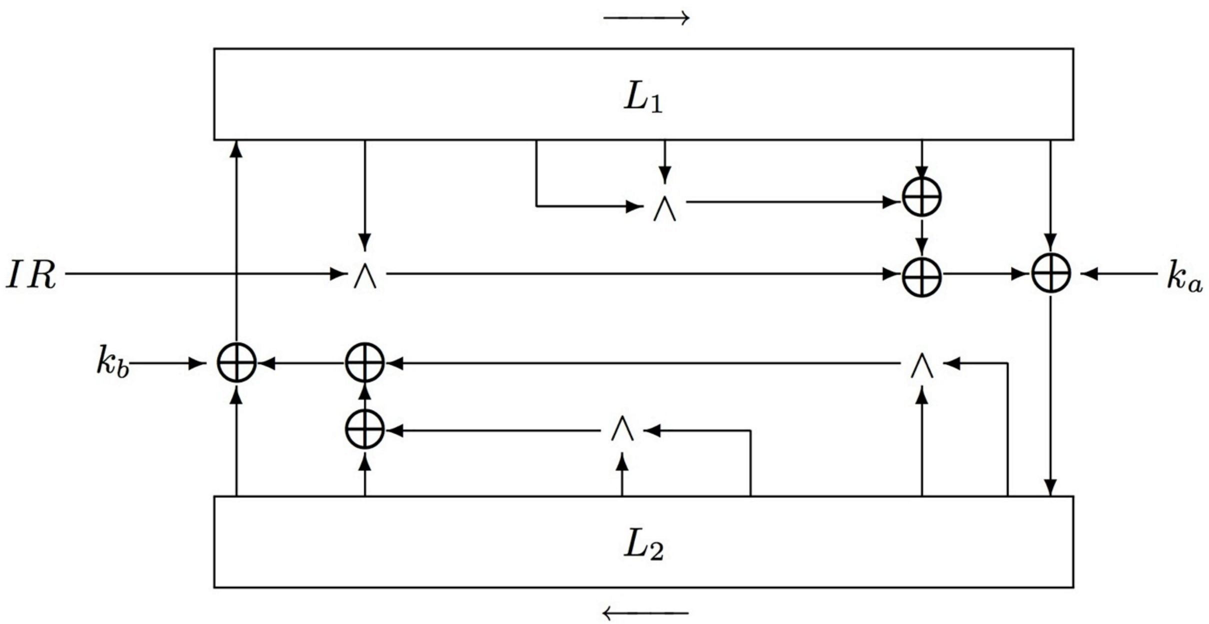
- KATAN is a family of lightweight, hardware-oriented block ciphers.
- Three variants: 32, 48, 64 (block size).
- 80-bit key and 254 rounds.
- The design was inspired by Trivium.

KATAN Cipher Family

- KATAN consists of two LFSR's, called L_1 and L_2.
- Two nonlinear Boolean functions, f_a and f_b.
- For KATAN48, f_a and f_b are applied twice per round, but the same pair of key bits are reused.
- For KATAN64, f_a and f_b are applied 3 times.

KATAN Cipher Family

$$f_a(L_1) = L_1[x_1] + L_1[x_2] + (L_1[x_3] \cdot L_1[x_4] + L_1[x_5] \cdot IR + k_a)$$
$$f_b(L_2) = L_2[y_1] + L_2[y_2] + (L_2[y_3] \cdot L_2[y_4] + L_2[y_5] \cdot L_2[y_6] + k_b)$$



KATAN Cipher Family

Cipher	$\|L_1\|$	$\|L_2\|$	x_1	x_2	x_3	x_4	x_5
KATAN32/KTANTAN32	13	19	12	7	8	5	3
KATAN48/KTANTAN48	19	29	18	12	15	7	6
KATAN64/KTANTAN64	25	39	24	15	20	11	9

Cipher	y_1	y_2	y_3	y_4	y_5	y_6
KATAN32/KTANTAN32	18	7	12	10	8	3
KATAN48/KTANTAN48	28	19	21	13	15	6
KATAN64/KTANTAN64	38	25	33	21	14	9

KATAN Cipher Family

- Key Schedule is a linear mapping that expands 80-bit key to 508 subkey bits according to

$$k_i = \begin{cases} K_i, & \text{for } 0 \leq i \leq 79 \\ k_{i-80} + k_{i-61} + k_{i-50} + k_{i-13}, & \text{otherwise} \end{cases}$$

- The subkey of i-th round is $k_a || k_b = K_{2i} || K_{2i+1}$
- At least 40 rounds is needed before complete key diffusion.

Cube Attack Results

Cipher	# Rounds	Time	Data	Attack
KATAN32	50	2^{34}	$2^{25.42}$ CP	AIDA/Cube
	60	2^{39}	$2^{30.28}$ CP	AIDA/Cube
KATAN48	40	2^{49}	$2^{24.95}$ CP	AIDA/Cube
KATAN64	30	2^{35}	$2^{20.64}$ CP	AIDA/Cube

Table 1: AIDA / Cube attack complexities on KATAN family.

Cube Attack Results

Some equations for KATAN64:

Maxterm	Degree	Cube equation	Cipher bit
0CB0C29808C10001	16	k_5	c_{44}
2E2128800020305A	16	k_4	c_7
10E2002920014471	16	$k_1 + k_5 + k_{12}$	c_{47}
0A12042100446263	16	$k_8 + k_{10} + k_{19}$	c_{12}
029290CC02C10140	16	k_2	c_5
AE0C032002100492	16	k_9	c_9
4241092108534C00	16	k_1	c_{44}
0E0864A20828A800	16	k_0	c_{56}
4104901087403083	16	k_7	c_8
44010B12812A0124	16	k_3	c_{49}
0200A0D00305E08A	16	$k_3 + k_{10}$	c_{48}
041102168238A802	16	k_6	c_9
439C00A810940044	16	$k_3 + k_8 + k_{17}$	c_9
60910A0B93000802	16	$k_1 + k_8$	c_{47}
018C084049C98003	16	$k_0 + k_1 + k_2 + k_8 + k_{11}$	c_8
3C1500040080C097	16	$k_4 + k_{15}$	c_{48}
0800FD4900016180	16	$k_5 + k_9 + k_{18}$	c_{54}

Side-channel Attack Against KATAN32

- Side-channel model
  - We use the side-channel cube attack model of Shamir.
  - Internal cipher data leaks after r round, $r < 254$
  - The data is supposed to be captured by some side channel information, such as power, timing analysis or electromagnetic emanations (a strong assumption).
  - We need only one bit of intermediate state. (Bit 19 after 40 rounds of KATAN32)

Side-channel Attack Against KATAN32

Cipher	# Rounds	Time	Data	Attack
KATAN32	254	2^{51}	$2^{23.80}$ CP	Side-Channel

Table 1: Side-Channel attack on KATAN32

Side-channel Attack Against KATAN32

Maxterm	Degree	Cube equation	Cipher bit
41356548	12	k_4	c_{19}
2464E14C	12	k_{15}	c_{19}
1EA26848	12	$k_5 + 1$	c_{19}
E3516900	12	$k_1 + k_{16}$	c_{19}
4A8E6888	12	$k_0 + k_{17} + 1$	c_{19}
EBD02900	12	$k_3 + k_{10} + 1$	c_{19}
A0867A0C	12	$k_{14} + k_{17} + 1$	c_{19}
C0C34C43	12	$k_4 + k_{10} + k_{19}$	c_{19}
E2A54302	12	$k_{11} + k_{15} + k_{23}$	c_{19}
9C045983	12	$k_2 + k_7 + k_{11} + k_{16} + k_{24} + k_{26}$	c_{19}
bd30cb11	15	k_{13}	c_{19}
7c366259	16	k_{18}	c_{19}
2cd5f264	16	$k_6 + k_{15} + 1$	c_{19}
b7351759	18	$k_3 + k_{18} + k_{23}$	c_{19}

Strange Phenomena

- Breaking 77 rounds of KATAN32 is much easier than 76 rounds.
  - attack on 76 rounds: 5.64 times faster than brute force.
  - attack on 77 rounds: 67.87 times faster than brute force.
  - attack on 78 rounds: 3.49 times faster than brute force.

(Above results are from Algebraic Attacks using SAT solvers)

Conclusion and further work

- Cube attacks for reduced-round KATAN32, KATAN48 and KATAN64.
- Side-channel attack against full-round KATAN32.
- After the acceptance of our paper, we tried to similar attack methods against KTANTAN block ciphers.
- More rounds are broken since the key schedule is weaker.

Acknowledgement

- Thanks for useful comments from reviewers, e.g.

  "On page 3, you write 'close to be(ing) overdefined': that means, in fact, underdefined? It sounds to me like the girl who is 'a little bit' pregnant."

Thanks

Q & A