山东大学密码技术与信息安全教育部重点实验室
Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University

Conditional Cube Attack on Round-Reduced ASCON

Zheng Li[1], Xiaoyang Dong[1,2], Xiaoyun Wang[1,2]

[1] Shandong University; [2] Tsinghua University

March 7, 2017

Outline

ASCON

- designed by Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer
- one of the 16 survivors of 3rd CAESAR competition
- specification of ASCON
  - permutation (12-round)
  - sponge-like construction
  - ASCON-128, ASCON-128a
- cryptanalysis of ASCON

Type	Attacked Rounds	Time	Source
Differential-Linear	4/12	2^{18}	[ASCON designers *at* CT-RSA 2015]
	5/12	2^{36}	
Cube-like Method	5/12	2^{35}	
	6/12	2^{66}	
	5/12	2^{24}	**Our result**
	6/12	2^{40}	
	7/12	$2^{103.9}$	

The Encryption of ASCON

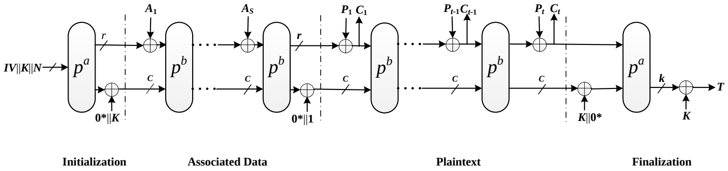

Figure: The Encryption of ASCON

Our target(omitted the associated data phase)

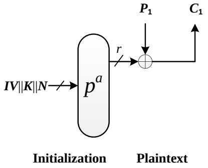

Figure: Objective Procedure of ASCON

The Permutation of Ascon's Initialization

state: 320-bit=5$\times$64-bit

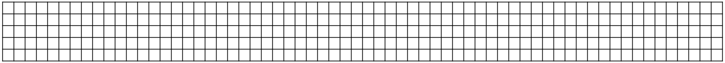

Figure: operating state

permutation: 12 iterations of round function

- round function
  - addition of constants
  - substitution layer (S-box)
  - linear diffusion layer

Outline

Cube Attack [Dinur and Shamir]

Theorem 1

$$f(k_0, ..., k_{n-1}, v_0, ..., v_{m-1}) = T \cdot P + Q(k_0, ..., k_{n-1}, v_0, ..., v_{m-1}) \quad (1)$$

T is a monomial which is actually the product of certain public variables, for example $(v_0, ..., v_{s-1})$, $1 \leq s \leq m$, denoted as cube C_T. None of the monomials in Q is divisible by T. P is called superpoly, which does not contain any variables of C_T. Then the sum of f over all values of the cube C_T (cube sum) is

$$\sum_{v'=(v_0,...,v_{s-1}) \in C_T} f(k_0, ..., k_{n-1}, v', v_s, ..., v_{m-1}) = P \quad (2)$$

where C_T contains all binary vectors of the length s, $v_s, ..., v_{m-1}$ are fixed to constant.

Conditional Cube Attack [Huang *et al.*]

Theorem 2

(simplified) For $(n+2)$-round Keccak sponge function $(n > 0)$, if there is one conditional cube variable v_0, and $q = 2^{n+1} - 1$ ordinary cube variables, $u_0, ..., u_{q-1}$, the term $v_0 u_0 ... u_{q-1}$ will not appear in the output polynomials of $(n+2)$-round Keccak sponge function.

Outline

Attack on 5-round Ascon

An Example to Determine $k_0(0) = 1$, i.e. $g = k_0(0)$.
Select a set of 16 cube variables $\{v_0, v_1 ... v_{15}\}$ satisfying:

- In the 1st round, any two of $\{v_0, v_1 ... v_{15}\}$ do not multiply.
- In the 2nd round: if $k_0(0)$=0, v_0 doesn't multiply with any of $\{v_1, v_2 ... v_{15}\}$; if $k_0(0)$=1, v_0 multiplies with some of $\{v_1, v_2 ... v_{15}\}$.

Thus,

- If $k_0(0)$=0, $v_0 v_1 ... v_{15}$ will not appear.
- If $k_0(0)$=1, $v_0 v_1 ... v_{15}$ will appear with high probability.

Therefore, we conclude the cube tester: If at least one nonzero cube sum occurs, we will determine that $k_0(0) = 1$. It is guaranteed to be right.
With similar testers for $k_0(t) = 0/1, k_0(t) + k_1(t) = 0/1$ with $t \in \{0, 1, ..., 63\}$, we can recover the whole key.

Attack on 6-round ASCON

Similar to 5-round attack, 32 variables are needed instead. An Example to Determine $k_0(0) = 1$, i.e. $g = k_0(0)$.
Select a set of 32 cube variables $\{v_0, v_1 ... v_{31}\}$ satisfying:

- Any two of $\{v_0, v_1 ... v_{31}\}$ do not multiply in the S-box operation of the first round.
- If $k_0(0)$=0, v_0 doesn't multiply with any of $\{v_1, v_2 ... v_{31}\}$ in the S-box operation of the second round.
- If $k_0(0)$=1, v_0 multiplies with some of $\{v_1, v_2 ... v_{31}\}$ in the S-box operation of the second round.

Properties of S-box

$$
\begin{aligned}
y_0 &= x_4x_1 + x_3 + x_2x_1 + x_2 + x_1x_0 + x_1 + x_0, \\
y_1 &= x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0, \\
y_2 &= x_4x_3 + x_4 + x_2 + x_1 + 1, \\
y_3 &= x_4x_0 + x_4 + x_3x_0 + x_3 + x_2 + x_1 + x_0, \\
y_4 &= x_4x_1 + x_4 + x_3 + x_1x_0 + x_1.
\end{aligned}
$$

- Among the 5-bit output of the S-box, x_4x_3 only exists in y_2.
- x_2 will only multiply with x_1 and x_3. Especially, quadratic terms containing x_2 exist only in y_0 with x_2x_1 and y_1 with $x_3x_2 + x_2x_1$.

Attack on 7-round Ascon

Main idea

divide the full key space into n subsets $\{Key_1, Key_2 ... Key_n\}$, their corresponding cube sets are $\{Cube_1, Cube_2 ... Cube_n\}$. If the cube sums over $Cube_i$ are zero, we determine $rightkey \in Key_i$.

Notations

S_i	the intermediate state after i-round, e.g. $S_{0.5}$ means the intermediate state after S-box in 1st round, esp. S_0 means the initial state of Ascon
$S_i[j]$	the jth word of S_i, $0 \leqslant j \leqslant 4$
$S_i[j][k]$	the kth bit of $S_i[j]$, $0 \leqslant j \leqslant 4$, $0 \leqslant k \leqslant 63$

Details of 7-round Attack

original cube set: set $S_0[3][j] = v_j$ for $j = 0, 1 \ldots 63$ and $S_0[4][i] = v_{64}$ where i could take a value from $\{0, 1 \ldots 63\}$.

0	1	.	.	.	.	i	.	.	.	.	j	.	.	.	.	63
IV(0)	IV(1)					IV(i)					IV(j)					IV(63)
k0(0)	k0(1)					k0(i)					k0(j)					k0(63)
k1(0)	k1(1)					k1(i)					k1(j)					k1(63)
v0	v1					vi					vj					v63
n(0)	n(1)					v64					n(j)					n(63)

Figure: Notations for State Bits

After the 1st round, $v_i v_{64}$ is the unique quadratic term. In detail, after the S-box in the 1st round, $v_i v_{64}$ just appears in $S_{0.5}[2][i]$; after the linear diffusion layer in the 1st round, ANF of $S_1[2][i]$, $S_1[2][i+1]$ and $S_1[2][i+6]$ contain $v_i v_{64}$.

Details of 7-round Attack

All the possible cubic terms in $S_{1.5}$ and their corresponding coefficients are listed below.

index of S-box	cubic terms	corresponding coefficients (*partial divisors*)
$i+1$	$v_i v_{64} v_{i+1}$	$k_0(i+1)+k_1(i+1)+1$
		$k_0(i+1)+k_1(i+1)+IV(i+1)$
	$v_i v_{64} v_{i+4}$	$k_0(i+4)+k_1(i+4)+1$
	$v_i v_{64} v_{i+26}$	$k_0(i+26)+k_1(i+26)+1$
	$v_i v_{64} v_{i+48}$	$IV(i+48)+1$
	$v_i v_{64} v_{i+55}$	$IV(i+55)+1$
i	$v_i v_{64} v_{i+3}$	$k_0(i+3)+k_1(i+3)+1$
	$v_i v_{64} v_{i+25}$	$k_0(i+25)+k_1(i+25)+1$
	$v_i v_{64} v_{i+47}$	$IV(i+47)+1$
	$v_i v_{64} v_{i+54}$	$IV(i+54)+1$
$i+6$	$v_i v_{64} v_{i+6}$	$k_0(i+6)+k_1(i+6)+1$
		$k_0(i+6)+k_1(i+6)+IV(i+6)$
	$v_i v_{64} v_{i+9}$	$k_0(i+9)+k_1(i+9)+1$
	$v_i v_{64} v_{i+31}$	$k_0(i+31)+k_1(i+31)+1$
	$v_i v_{64} v_{i+53}$	$IV(i+53)+1$
	$v_i v_{64} v_{i+61}$	$IV(i+60)+1$

Details of 7-round Attack

index of S-box	cubic terms	auxiliary cube variables	corresponding coefficients (*partial divisors*)
$i+1$	$v_i v_{64} v_{i+1}$	$S_0[4][i+1] = v_{i+1}$	$k_0(i+1) + k_1(i+1)$
	$v_i v_{64} v_{i+4}$		$k_0(i+4) + k_1(i+4) + 1$
	$v_i v_{64} v_{i+26}$		$k_0(i+26) + k_1(i+26) + 1$
	$v_i v_{64} v_{i+48}$	$S_0[4][i+48] = v_{i+48}$	0
	$v_i v_{64} v_{i+55}$	$S_0[4][i+55] = v_{i+55}$	0
i	$v_i v_{64} v_{i+3}$		$k_0(i+3) + k_1(i+3) + 1$
	$v_i v_{64} v_{i+25}$		$k_0(i+25) + k_1(i+25) + 1$
	$v_i v_{64} v_{i+47}$	$S_0[4][i+47] = v_{i+47}$	0
	$v_i v_{64} v_{i+54}$	$S_0[4][i+54] = v_{i+54}$	0
$i+6$	$v_i v_{64} v_{i+6}$	$S_0[4][i+6] = v_{i+6}$	$k_0(i+6) + k_1(i+6)$
	$v_i v_{64} v_{i+9}$		$k_0(i+9) + k_1(i+9) + 1$
	$v_i v_{64} v_{i+31}$		$k_0(i+31) + k_1(i+31) + 1$
	$v_i v_{64} v_{i+53}$	$S_0[4][i+53] = v_{i+53}$	0
	$v_i v_{64} v_{i+61}$	$S_0[4][i+60] = v_{i+60}$	0

Table: Coefficients of Cubic Terms with Auxiliary Cube Variables

Details of 7-round Attack

	cubic terms	control cube variable	corresponding coefficients
$i+1$	$v_i v_{64} v_{i+1}$		$k_0(i+1)+k_1(i+1)$
	$v_i v_{64} v_{i+4}$	$S_0[4][i+4]=v_{i+4}$	$k_0(i+4)+k_1(i+4)$
	$v_i v_{64} v_{i+26}$		$k_0(i+26)+k_1(i+26)+1$
	$v_i v_{64} v_{i+48}$		0
	$v_i v_{64} v_{i+55}$		0
i	$v_i v_{64} v_{i+3}$		$k_0(i+3)+k_1(i+3)+1$
	$v_i v_{64} v_{i+25}$		$k_0(i+25)+k_1(i+25)+1$
	$v_i v_{64} v_{i+47}$		0
	$v_i v_{64} v_{i+54}$		0
$i+6$	$v_i v_{64} v_{i+6}$		$k_0(i+6)+k_1(i+6)$
	$v_i v_{64} v_{i+9}$		$k_0(i+9)+k_1(i+9)+1$
	$v_i v_{64} v_{i+31}$		$k_0(i+31)+k_1(i+31)+1$
	$v_i v_{64} v_{i+53}$		0
	$v_i v_{64} v_{i+61}$		0

Table: Coefficients of Cubic Terms with Auxiliary and Control Cube Variable

Details of 7-round Attack

$$
\begin{cases}
k_0(i+1)+k_1(i+1)=0\\
k_0(i+4)+k_1(i+4)=a\\
k_0(i+26)+k_1(i+26)=b\\
k_0(i+3)+k_1(i+3)=c\\
k_0(i+25)+k_1(i+25)=d\\
k_0(i+6)+k_1(i+6)=0\\
k_0(i+9)+k_1(i+9)=e\\
k_0(i+31)+k_1(i+31)=f
\end{cases}
\tag{3}
$$

Similar control cube variable can change the corresponding coefficients. Therefore, there are $2^6 = 64$ kinds of control cube variable combinations corresponding to 64 groups of coefficients respectively. In Eq. (3), where $(a, b, c, d, e, f) \in F_2^6$ varies according to different control cube variable combination.

Details of 7-round Attack

$$\begin{cases} k_0(i+1)+k_1(i+1)=0 \\ k_0(i+4)+k_1(i+4)=a \\ k_0(i+26)+k_1(i+26)=b \\ k_0(i+3)+k_1(i+3)=c \\ k_0(i+25)+k_1(i+25)=d \\ k_0(i+6)+k_1(i+6)=0 \\ k_0(i+9)+k_1(i+9)=e \\ k_0(i+31)+k_1(i+31)=f \end{cases} \quad (3)$$

When key meets the corresponding conditions, there are no cubic terms in $S_{1.5}$. The highest degree of monomials in S_2 is 2. As the algebraic degree of S-box is 2, the algebraic degree of the 7-round ASCON's output is less than or equal to 64, which means that $v_0 v_1 \ldots v_{64}$ will not appear in the output.

Details of 7-round Attack

$$\begin{cases} k_0(i+1)+k_1(i+1)=0 \\ k_0(i+4)+k_1(i+4)=a \\ k_0(i+26)+k_1(i+26)=b \\ k_0(i+3)+k_1(i+3)=c \\ k_0(i+25)+k_1(i+25)=d \\ k_0(i+6)+k_1(i+6)=0 \\ k_0(i+9)+k_1(i+9)=e \\ k_0(i+31)+k_1(i+31)=f \end{cases} \tag{3}$$

When key does not meet the corresponding conditions, some cubic terms will appear in S_2. Therefore, $v_0 v_1 \dots v_{64}$ will appear in the output of 7-round.

Experimental Verification

Implementation of 5/6-round attacks on Ascon
Experimental verification for 7-round attack
source code: `https://github.com/lizhengcn/Ascon_test`

Thanks for Your Attention