Conditional Cube Attack on Round-Reduced \textsc{Ascon}

Zheng Li$^1$, Xiaoyang Dong$^{1,2}$, Xiaoyun Wang$^{1,2}$

$^1$ Shandong University; $^2$ Tsinghua University

March 7, 2017
Outline

1. **Ascon** and Its Cryptanalysis Results
2. Related Works
3. Our works
Ascon and Its Cryptanalysis Results

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Attacked Rounds</th>
<th>Time</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Differential-Linear</td>
<td>4/12</td>
<td>$2^{18}$</td>
<td>[Ascon designers at CT-RSA 2015]</td>
</tr>
<tr>
<td></td>
<td>5/12</td>
<td>$2^{36}$</td>
<td></td>
</tr>
<tr>
<td>Cube-like Method</td>
<td>5/12</td>
<td>$2^{35}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6/12</td>
<td>$2^{66}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5/12</td>
<td>$2^{24}$</td>
<td>Our result</td>
</tr>
<tr>
<td></td>
<td>6/12</td>
<td>$2^{40}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7/12</td>
<td>$2^{103.9}$</td>
<td></td>
</tr>
</tbody>
</table>
The Encryption of \texttt{Ascon}

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure}
\caption{The Encryption of \texttt{Ascon}}
\end{figure}

Our target (omitted the associated data phase)

\begin{figure}
\centering
\includegraphics[width=0.5\textwidth]{figure}
\caption{Objective Procedure of \texttt{Ascon}}
\end{figure}
The Permutation of Ascon’s Initialization

state: 320-bit = 5 × 64-bit

Figure: operating state

permutation: 12 iterations of round function
- round function
  - addition of constants
  - substitution layer (S-box)
  - linear diffusion layer
Outline

1. Ascon and Its Cryptanalysis Results

2. Related Works

3. Our works
Cube Attack [Dinur and Shamir]

**Theorem 1**

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

\(T\) 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

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

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

1. ASCON and Its Cryptanalysis Results
2. Related Works
3. Our works
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 $k_0(0) = 0$, $v_0v_1...v_{15}$ will not appear.
- If $k_0(0) = 1$, $v_0v_1...v_{15}$ 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

\[ y_0 = x_4x_1 + x_3 + x_2x_1 + x_2 + x_1x_0 + x_1 + x_0, \]
\[ y_1 = x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0, \]
\[ y_2 = x_4x_3 + x_4 + x_2 + x_1 + 1, \]
\[ y_3 = x_4x_0 + x_4 + x_3x_0 + x_3 + x_2 + x_1 + x_0, \]
\[ y_4 = x_4x_1 + x_4 + x_3 + x_1x_0 + x_1. \]

- 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 \( j \)th word of \( S_i \), \( 0 \leq j \leq 4 \)
- \( S_i[j][k] \) the \( k \)th bit of \( S_i[j] \), \( 0 \leq j \leq 4, 0 \leq k \leq 63 \)
Our works

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 $\{0, 1 \ldots 63\}$.

![Figure: Notations for State Bits](image)

After the 1st round, $v_iv_{64}$ is the unique quadratic term. In detail, after the S-box in the 1st round, $v_iv_{64}$ 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 $v_iv_{64}$. 
Details of 7-round Attack

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

<table>
<thead>
<tr>
<th>index of S-box</th>
<th>cubic terms</th>
<th>corresponding coefficients (partial divisors)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i + 1$</td>
<td>$v_i v_{64} v_{i+1}$</td>
<td>$k_0(i + 1) + k_1(i + 1) + 1$</td>
</tr>
<tr>
<td>$i + 1$</td>
<td>$v_i v_{64} v_{i+4}$</td>
<td>$k_0(i + 4) + k_1(i + 4) + 1$</td>
</tr>
<tr>
<td>$i + 1$</td>
<td>$v_i v_{64} v_{i+26}$</td>
<td>$k_0(i + 26) + k_1(i + 26) + 1$</td>
</tr>
<tr>
<td>$i + 1$</td>
<td>$v_i v_{64} v_{i+48}$</td>
<td>$IV(i + 48) + 1$</td>
</tr>
<tr>
<td>$i + 1$</td>
<td>$v_i v_{64} v_{i+55}$</td>
<td>$IV(i + 55) + 1$</td>
</tr>
<tr>
<td>$i$</td>
<td>$v_i v_{64} v_{i+3}$</td>
<td>$k_0(i + 3) + k_1(i + 3) + 1$</td>
</tr>
<tr>
<td>$i$</td>
<td>$v_i v_{64} v_{i+25}$</td>
<td>$k_0(i + 25) + k_1(i + 25) + 1$</td>
</tr>
<tr>
<td>$i$</td>
<td>$v_i v_{64} v_{i+47}$</td>
<td>$IV(i + 47) + 1$</td>
</tr>
<tr>
<td>$i$</td>
<td>$v_i v_{64} v_{i+54}$</td>
<td>$IV(i + 54) + 1$</td>
</tr>
<tr>
<td>$i + 6$</td>
<td>$v_i v_{64} v_{i+6}$</td>
<td>$k_0(i + 6) + k_1(i + 6) + 1$</td>
</tr>
<tr>
<td>$i + 6$</td>
<td>$v_i v_{64} v_{i+9}$</td>
<td>$k_0(i + 9) + k_1(i + 9) + 1$</td>
</tr>
<tr>
<td>$i + 6$</td>
<td>$v_i v_{64} v_{i+31}$</td>
<td>$k_0(i + 31) + k_1(i + 31) + 1$</td>
</tr>
<tr>
<td>$i + 6$</td>
<td>$v_i v_{64} v_{i+53}$</td>
<td>$IV(i + 53) + 1$</td>
</tr>
<tr>
<td>$i + 6$</td>
<td>$v_i v_{64} v_{i+61}$</td>
<td>$IV(i + 60) + 1$</td>
</tr>
</tbody>
</table>
Our works

Details of 7-round Attack

Table: Coefficients of Cubic Terms with Auxiliary Cube Variables

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

Table: Coefficients of Cubic Terms with Auxiliary Cube Variables
### Details of 7-round Attack

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

**Table:** Coefficients of Cubic Terms with Auxiliary and Control Cube Variable
Details of 7-round Attack

\[
\begin{aligned}
&k_0(i + 1) + k_1(i + 1) = 0 \\
&k_0(i + 4) + k_1(i + 4) = a \\
&k_0(i + 26) + k_1(i + 26) = b \\
&k_0(i + 3) + k_1(i + 3) = c \\
&k_0(i + 25) + k_1(i + 25) = d \\
&k_0(i + 6) + k_1(i + 6) = 0 \\
&k_0(i + 9) + k_1(i + 9) = e \\
&k_0(i + 31) + k_1(i + 31) = f
\end{aligned}
\]

(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

\[
\begin{align*}
  k_0(i + 1) + k_1(i + 1) &= 0 \\
  k_0(i + 4) + k_1(i + 4) &= a \\
  k_0(i + 26) + k_1(i + 26) &= b \\
  k_0(i + 3) + k_1(i + 3) &= c \\
  k_0(i + 25) + k_1(i + 25) &= d \\
  k_0(i + 6) + k_1(i + 6) &= 0 \\
  k_0(i + 9) + k_1(i + 9) &= e \\
  k_0(i + 31) + k_1(i + 31) &= f
\end{align*}
\] (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 $v_0v_1\ldots v_{64}$ will not appear in the output.
Details of 7-round Attack

\[
\begin{align*}
  k_0(i + 1) + k_1(i + 1) &= 0 \\
  k_0(i + 4) + k_1(i + 4) &= a \\
  k_0(i + 26) + k_1(i + 26) &= b \\
  k_0(i + 3) + k_1(i + 3) &= c \\
  k_0(i + 25) + k_1(i + 25) &= d \\
  k_0(i + 6) + k_1(i + 6) &= 0 \\
  k_0(i + 9) + k_1(i + 9) &= e \\
  k_0(i + 31) + k_1(i + 31) &= f
\end{align*}
\]

When key does not meet the corresponding conditions, some cubic terms will appear in $S_2$. Therefore, $v_0v_1 \ldots v_{64}$ 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