Cube Attacks on Ascon

Internship - Symmetric cryptanalysis

ROUSSEAU Jules

Research team : CAPSULE
Univesité de Rennes - Irisa

July 17, 2024

Supervisors : André SCHROTTENLOHER, Patrick DERBEZ

Lightweight encryption

Why?

- Little memory
- Low power consumption
- High performance
- Security in IoT

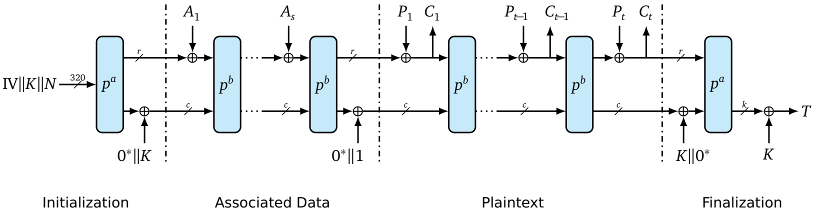
Ascon[1]

- ▷ Ascon is a family of lightweight ciphers
- ▷ Futur standard selected by NIST, 2023
- ▷ Design based on a sponge construction (AEAD cipher, hash function)

[1] Dobraunig, Eichlseder, Mendel, Schläffer. Ascon v1.2. Journal of Cryptology 2021

Ascon Specification

Duplex-Sponge mode in Ascon



- IV, A are public
- K, N are secret

Parameters

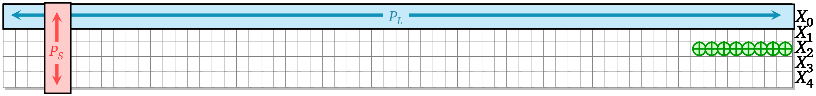
Bit size of					Rounds	
Key K	Nonce N	Tag T	Data block	State S	p^a	p^b
128	128	128	64	320	12	6

Ascon Specification

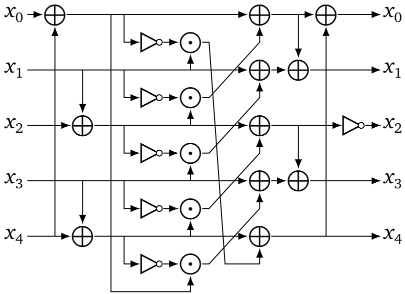
Permutation P in Ascon

$$P = P_L \circ P_S \circ P_C$$

- P_C 1-byte **constant addition**
- P_S Nonlinear Substitution layer : 5-bit **S-box** on each of the 64 columns
- P_L **Linear Diffusion Layer** on each of the 5 rows



Ascon Specification



Ascon's 5-bit S-box

$$
\begin{aligned}
x_0 &:= x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)\\
x_1 &:= x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)\\
x_2 &:= x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6)\\
x_3 &:= x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)\\
x_4 &:= x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)
\end{aligned}
$$

Ascon's linear diffusion layer

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathbf{S}(x)$	4	b	1f	14	1a	15	9	2	1b	5	8	12	1d	3	6	1c
x	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
$\mathbf{S}(x)$	1e	13	7	e	0	d	11	18	10	c	1	19	16	a	f	17

Sbox as a lookup table

Cube attacks

- **Algebraic Normal Form (ANF)**
  Let $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ be a Boolean function, its ANF is given by :

$$f(x) = \sum_{u \in \mathbb{F}_2^n} a_u x^u$$

$x = (x_0, \ldots, x_{n-1})$ the public variables

examples

ANF : $n = 4, f(x) = x_0x_1x_2x_3 + x_1x_3 + x_0x_2$

Monomial : $x_1x_3 = x^u$ with $u = (01010)$

$$x^u = (x_0, x_1, x_2, x_3)^{(0,1,0,1)} = x_0^0 x_1^1 x_2^0 x_3^1 = x_1x_3$$

- **Cube**

$x = (x_0, x_1, x_2, x_3)$, let's consider $I = (0, 2)$ so $x^I = \boldsymbol{x_0 x_2}$.

The cube C_I associated to x^I is $C_I = \{\mathbf{0}0\mathbf{0}0, \mathbf{1}0\mathbf{0}0, \mathbf{0}0\mathbf{1}0, \mathbf{1}0\mathbf{1}0\}$

- **Cube**

$x = (x_0, x_1, x_2, x_3)$, let's consider $I = (0,2)$ so $x^I = \boldsymbol{x_0 x_2}$.
The cube C_I associated to x^I is $C_I = \{\mathbf{0}0\mathbf{0}0, \mathbf{1}0\mathbf{0}0, \mathbf{0}0\mathbf{1}0, \mathbf{1}0\mathbf{1}0\}$

- **Division Property**

	initial state $\cdots$ $\longrightarrow$	i^{th} intermediate state $\cdots$ $\longrightarrow$	final state
	x	$y = f^i(x)$	$z = f(y)$
$Ex:$	x_0, x_1, x_2, x_3	$y_0 = x_1x_2 + x_1$	$z_0 = y_0y_1 = x_1x_2x_0 + x_1x_0$
		$y_1 = x_0$	$z_1 = y_0 + y_1 = x_1x_2 + x_1 + x_0$

- **Cube**

$x = (x_0, x_1, x_2, x_3)$, let's consider $I = (0, 2)$ so $x^I = \boldsymbol{x_0 x_2}$.
The cube C_I associated to x^I is $C_I = \{\mathbf{0}0\mathbf{0}0, \mathbf{1}0\mathbf{0}0, \mathbf{0}0\mathbf{1}0, \mathbf{1}0\mathbf{1}0\}$

- **Division Property**

	initial state $\cdots$ $\longrightarrow$	i^{th} intermediate state $\cdots$ $\longrightarrow$	final state
	x	$y = f^i(x)$	$z = f(y)$
$Ex:$	x_0, x_1, x_2, x_3	$y_0 = x_1x_2 + x_1$	$z_0 = y_0y_1 = x_1x_2x_0 + x_1x_0$
		$y_1 = x_0$	$z_1 = y_0 + y_1 = x_1x_2 + x_1 + x_0$

$$f_k(x) = p_I(x[\bar{I}], k) \cdot x^I + q(x, k)$$

$$\bigoplus_{x[I]} f_k(x) = p_I(x[\bar{I}], k)$$

Cube attacks

- **Division trails**
  $u \xrightarrow{f} v$ is a trail from x^u to $y^v \iff$ x^u belongs to y^v

  In our case : $u \xrightarrow{f} v$ where $v = e_i \iff x^u$ appears in the ANF of y_i

Cube attacks

- **Division trails**

  $u \xrightarrow{f} v$ is a trail from x^u to y^v $\iff$ x^u belongs to y^v

  In our case : $u \xrightarrow{f} v$ where $v = e_i$ $\iff$ x^u appears in the ANF of y_i

- **3SBDP without unknown subset**

$$\bigoplus_{x \in \mathbb{X}} x^u = \begin{cases} 1 & \textit{if the number of trails is odd} \\ 0 & \textit{otherwise} \end{cases}$$

Cube attacks

- **Division trails**

  $u \xrightarrow{f} v$ is a trail from x^u to y^v $\iff$ x^u belongs to y^v

  In our case : $u \xrightarrow{f} v$ where $v = e_i$ $\iff$ x^u appears in the ANF of y_i

- **3SBDP without unknown subset**

$$\bigoplus_{x \in \mathbb{X}} x^u = \begin{cases} 1 & \textit{if the number of trails is odd} \\ 0 & \textit{otherwise} \end{cases}$$

Drawback

We need to count ALL the trails !

Cube attacks

Cube attacks usual purposes

Finding distinguishers

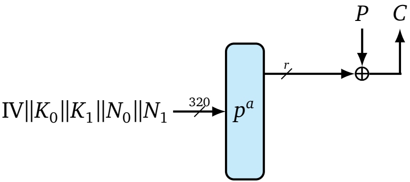
- distinguish a cryptographic function from a random one
- Bounds on the degree of monomials
- $\bigoplus_{x \in \chi} f(x) = 0$

Recover information on the key

- Result of the sum determined by the key bits
- $\bigoplus_{x \in \chi} f(x) \neq 0$

My work on Ascon

The attack model of Ascon[2]



- Modelization in MILP and SAT
- GOAL : Accelerating the trails calculation : fewer trails or making it more efficient

XOR	$a \xrightarrow{\oplus} b$	$b = a_1 + \cdots + a_n$
AND	$a \xrightarrow{\odot} b$	$b = a_i \quad \forall i \in \{1, \ldots, n\}$
COPY	$a \xrightarrow{copy} b$	$a \geq b_i \quad \forall i \in \{1, \ldots, n\}$, and $b_1 + \cdots + b_n \geq a$
NEGATION	$a \xrightarrow{\neg} b$	$b \geq a$

[2] Rohit, Hu, Sarkar, Sun. Misuse-free key-recovery and distinguishing attacks on 7-round ascon. IACR Trans. Symmetric Cryptol. 2021

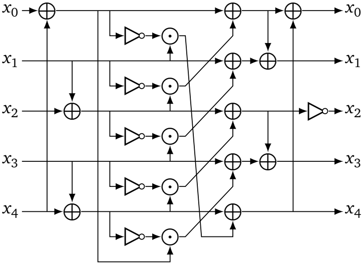
My work on Ascon

Equivalent modelizations

According to the ANF of the Sbox

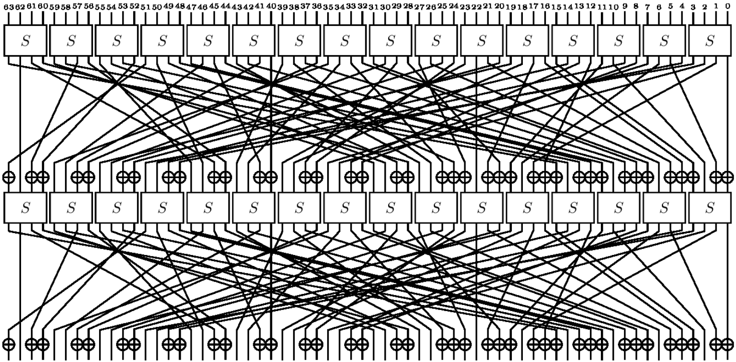
$$y_0 = x_4x_1 + x_3 + x_2x_1 + x_2 + x_1x_0 + x_1 + x_0$$
$$y_1 = x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0$$
$$y_2 = x_4x_3 + x_4 + x_2 + x_1 + 1$$
$$y_3 = x_4x_0 + x_4 + x_3x_0 + x_3 + x_2 + x_1 + x_0$$
$$y_4 = x_4x_1 + x_4 + x_3 + x_1x_0 + x_1$$

According to its Boolean circuit



GIFT-64

What's GIFT ?



SubCells: 4-bit SBox

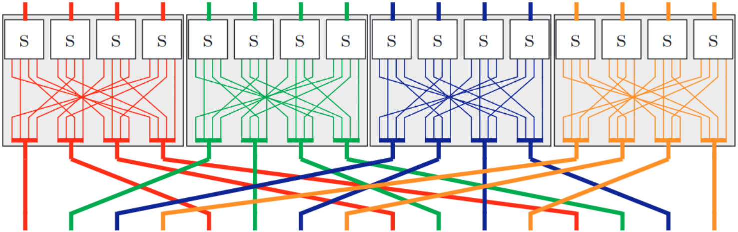
PermBits: Permutation of bits

AddRoundKey: XORing of key bits and round constants

28 rounds keys derived from the 128-bit master Key

GIFT Super Sbox

Discard inconsistent trails in middle rounds $\Longrightarrow$ fewer trails to compute?



Verify trail consistency through a Super Sbox (SSB)

Algorithm 1: trails_checking

Input: Truth table of Super Sbox

Output: Verification of $u \xrightarrow{f_{SSB}} v$

1 ▷ Calculate y, the ANF of SSB using the Moebius Transform

2 ▷ Calculate y^v

3 ▷ Check if $x^u \in y^v$ ANF

What did I do ?

Cipher	Known integral distinguisher	Integral-resistance property
SKINNY-64	12	13
CRAFT	13	14
GIFT-64	**10**	**12**
PRESENT	**9**	**13**
SIMON32	15	16
SIMON48	16	17
SIMON64	18	19
SIMON96	22	23
SIMON128	26	27
Simeck32	15	16
Simeck48	18	19
Simeck64	21	22

[HLLT21][3]

- Trying to fill the gap
- Finding the cause : The lower bound or the best distinguisher known ?
- Using fixed keys

[3] Hebborn, Lambin, Leander, Todo. Strong and tight security guarantees against integral distinguishers. ASIACRYPT 2021

Future work

- Obtain results on the lower bound for fixed-key GIFT
- Apply the implementation to key-independent GIFT
- Fill the gap between the lower bound and the known distinguisher

References

- Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer, *Ascon v1.2: Lightweight authenticated encryption and hashing*, Journal of Cryptology **34** (2021).
- Phil Hebborn, Baptiste Lambin, Gregor Leander, and Yosuke Todo, *Strong and tight security guarantees against integral distinguishers*, Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I (Mehdi Tibouchi and Huaxiong Wang, eds.), Lecture Notes in Computer Science, vol. 13090, Springer, 2021, pp. 362–391.
- Raghvendra Rohit, Kai Hu, Sumanta Sarkar, and Siwei Sun, *Misuse-free key-recovery and distinguishing attacks on 7-round ascon*, IACR Trans. Symmetric Cryptol. **2021** (2021), no. 1, 130–155.