Practical cube-attack against nonce-misused Ascon

NIST Lightweight Cryptography Workshop 2022

Jules Baudrin
joint work with Anne Canteaut & Léo Perrin (Inria, Paris, France)

May 2022

Contact: jules.baudrin@inria.fr

In this talk

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

- Ascon design rationale
- The permutation
- The nonce-misuse scenario

Ascon specs. and attack setting

- Cube attack principle
- Recovery of the polynomial: main problems
- Highest-degree terms in theory
- Highest-degree terms in **practice**
- Conditional cubes

From theory to practice

- Choice of the cube: forcing some linear divisors
- The internal-state recovery

Main steps of the attack

- Conclusion

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

- **Authenticated encryption**: confidentiality/authenticity/integrity all-in-one in a single primitive

- Two main parts of the design:
  - The choice of a **mode of operation**: abstract construction with generic functions
  - The choice of an **instantiation** of the mode with carefully-chosen primitives

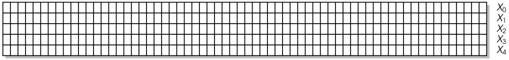
- In the case of Ascon [DEMS19]:
  - Duplex Sponge mode [BDPA11]
  - A carefully-chosen **permutation** $p : \mathbb{F}_2^{320} \to \mathbb{F}_2^{320}$.
  - ▶ **Ascon is permutation-based**.

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

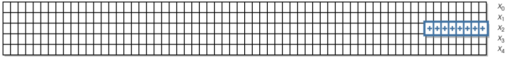
A confusion/diffusion structure…

The state

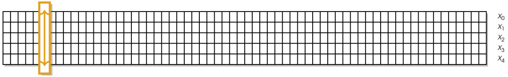


$$p = p_L \circ p_S \circ p_C$$

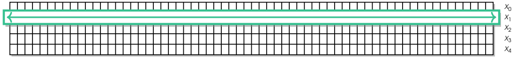
The constant addition p_C



The substitution layer p_S



The linear layer p_L



…studied algebraically

$$\begin{aligned}
y_0 &= \mathbf{x_4 x_1} + x_3 + \mathbf{x_2 x_1} + x_2 + \mathbf{x_1 x_0} + x_1 + x_0\\
y_1 &= x_4 + \mathbf{x_3 x_2} + \mathbf{x_3 x_1} + x_3 + \mathbf{x_2 x_1} + x_2 + x_1 + x_0\\
y_2 &= \mathbf{x_4 x_3} + x_4 + x_2 + x_1 + 1\\
y_3 &= \mathbf{x_4 x_0} + x_4 + \mathbf{x_3 x_0} + x_3 + x_2 + x_1 + x_0\\
y_4 &= \mathbf{x_4 x_1} + x_4 + x_3 + \mathbf{x_1 x_0} + x_1
\end{aligned}$$

Algebraic Normal Form (ANF) of the S-box

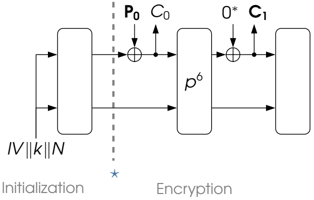
$$\begin{aligned}
X_0 &= X_0 \oplus (X_0 \ggg 19) \oplus (X_0 \ggg 28)\\
X_1 &= X_1 \oplus (X_1 \ggg 61) \oplus (X_1 \ggg 39)\\
X_2 &= X_2 \oplus (X_2 \ggg 1) \oplus (X_2 \ggg 6)\\
X_3 &= X_3 \oplus (X_3 \ggg 10) \oplus (X_3 \ggg 17)\\
X_4 &= X_4 \oplus (X_4 \ggg 7) \oplus (X_4 \ggg 41)
\end{aligned}$$

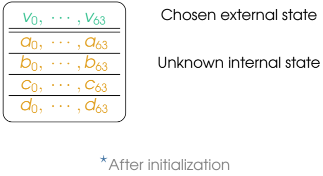
ANF of the linear layer p_L

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Simplified setting for Ascon -128





- Many reuse of the **same** (k, N) **pair**
- Chosen-plaintexts attack
- **If** the whole state is recovered, confidentiality is compromised, but not integrity nor authenticity in the case of Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

f_j: jth output coordinate. Instead of $f_j \in \mathbb{F}_2[v_0, \cdots, v_{63}, a_0, \cdots, d_{63}]$, we separate public variables from secret variables:

$$f_j \in \mathbb{F}_2[a_0, \cdots, d_{63}][v_0, \cdots, v_{63}] \quad f_j = \sum_{(u_0, \cdots, u_{63}) \in \mathbb{F}_2^{64}} \alpha_{u,\ j} \left(\prod_{i=0}^{63} {v_i}^{u_i} \right)$$

where $\alpha_{u,\ j} \in \mathbb{F}_2[a_0, \cdots, d_{63}]$.

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Cube attack principle

f_j: jth output coordinate. Instead of $f_j \in \mathbb{F}_2[v_0, \cdots, v_{63}, a_0, \cdots, d_{63}]$, we separate public variables from secret variables:

$$f_j \in \mathbb{F}_2[a_0, \cdots, d_{63}][v_0, \cdots, v_{63}] \quad f_j = \sum_{(u_0, \cdots, u_{63}) \in \mathbb{F}_2^{64}} \alpha_{u,j} \left(\prod_{i=0}^{63} {v_i}^{u_i} \right)$$

where $\alpha_{u,j} \in \mathbb{F}_2[a_0, \cdots, d_{63}]$.

Polynomial **expression** of $\alpha_{u,j}$ + **value** of $\alpha_{u,j}$ = equation in the unknown variables $\simeq$ recovery of some information

0. Select a monomial (**cube**) in f_j and target its coefficient: $\alpha_{u,j}$
1. **Offline phase**: recovery of the algebraic expression of $\alpha_{u,j}$
2. **Online phase**: recovery of the value of $\alpha_{u,j}$:
   $\alpha_{u,j} = \sum_{v \preccurlyeq u} f_j(v)$ (**chosen queries**).

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Problem 0: impossible access to the full ANF

$p \circ \cdots \circ p$: 6 iterations, 256 unknown variables.
S-box layer squares the number of terms. Linear layer triples it. **Impossible**.

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Problem 0: impossible access to the full ANF

$p \circ \cdots \circ p$: 6 iterations, 256 unknown variables.
S-box layer squares the number of terms. Linear layer triples it. **Impossible**.

Pb. 1: impossible access to a given $\alpha_{u,j}$ expression

Finding $\alpha_{u,j}$ for fixed u and j. **Too many combinatorial possibilities to track!**

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Problem 0: impossible access to the full ANF

$p \circ \cdots \circ p$: 6 iterations, 256 unknown variables.
S-box layer squares the number of terms. Linear layer triples it. **Impossible**.

Pb. 1: impossible access to a given $\alpha_{u,j}$ expression

Finding $\alpha_{u,j}$ for fixed u and j. **Too many combinatorial possibilities to track!**

$$v_0v_1 = v_0 \times v_1 = (v_0v_1) \times 1 = (v_0v_1) \times v_0 = (v_0v_1) \times v_1 = (v_0v_1) \times (v_0v_1)$$

Problem 0: impossible access to the full ANF

$p \circ \cdots \circ p$: 6 iterations, 256 unknown variables.
S-box layer squares the number of terms. Linear layer triples it. **Impossible**.

Pb. 1: impossible access to a given $\alpha_{u,\,j}$ expression

Finding $\alpha_{u,\,j}$ for fixed u and j. **Too many combinatorial possibilities to track!**

$$v_0v_1 = v_0 \times v_1 = (v_0v_1) \times 1 = (v_0v_1) \times v_0 = (v_0v_1) \times v_1 = (v_0v_1) \times (v_0v_1)$$

Pb. 2: Finding exploitable $\alpha_{u,\,j}$

We need to be able to solve the system!

Recovery of the polynomial: main problems

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Problem 0: impossible access to the full ANF

$p \circ \cdots \circ p$: 6 iterations, 256 unknown variables.
S-box layer squares the number of terms. Linear layer triples it. **Impossible**.

Pb. 1: impossible access to a given $\alpha_{u,\,j}$ expression

Finding $\alpha_{u,\,j}$ for fixed u and j. **Too many combinatorial possibilities to track!**

$$v_0 v_1 = v_0 \times v_1 = (v_0 v_1) \times 1 = (v_0 v_1) \times v_0 = (v_0 v_1) \times v_1 = (v_0 v_1) \times (v_0 v_1)$$

Pb. 2: Finding exploitable $\alpha_{u,\,j}$

We need to be able to solve the system!

- Highest-degree terms (2^{t-1} at round t) are easier to study.

Strong constraint: products of two former highest-degree terms.

$$v_0 v_1 = v_0 \times v_1 = \cancel{(v_0 v_1) \times 1} = \cancel{(v_0 v_1) \times v_0} = \cancel{(v_0 v_1) \times v_1} = \cancel{(v_0 v_1) \times (v_0 v_1)}$$

Highest-degree terms in theory

Jules BAUDRIN, Anne CANTEAUT & Léo PERRIN (Inria, Paris, France)

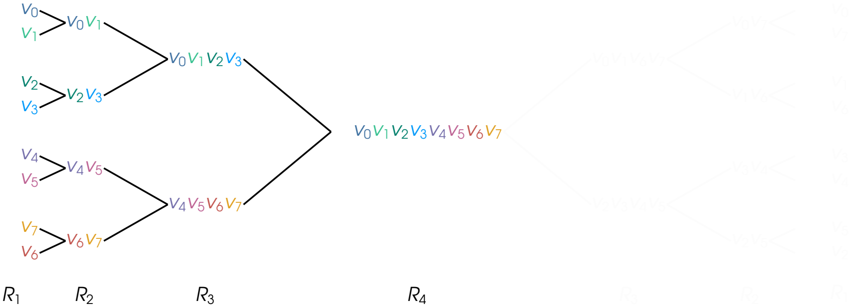
Strong constraint: products of two former highest-degree terms.

$$v_0v_1 = v_0 \times v_1 = \cancel{(v_0v_1) \times 1} = \cancel{(v_0v_1) \times v_0} = \cancel{(v_0v_1) \times v_1} = \cancel{(v_0v_1) \times (v_0v_1)}$$

Strong constraint: products of two former highest-degree terms.

$$V_0V_1 = V_0 \times V_1 = \cancel{(V_0V_1) \times 1} = \cancel{(V_0V_1) \times V_0} = \cancel{(V_0V_1) \times V_1} = \cancel{(V_0V_1) \times (V_0V_1)}$$

Trail t_0

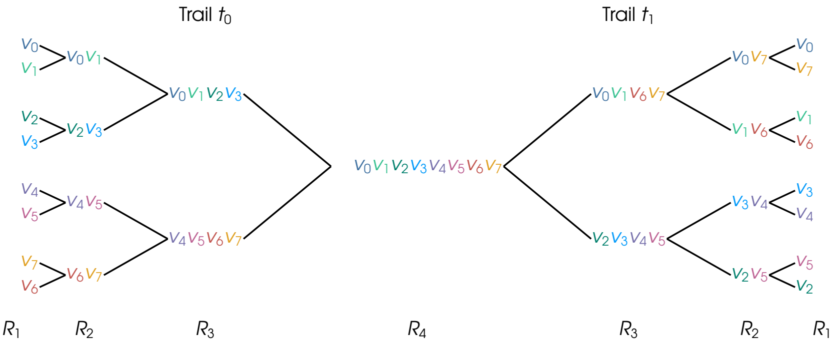


Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Strong constraint: products of two former highest-degree terms.

$$v_0v_1 = v_0 \times v_1 = \cancel{(v_0v_1) \times 1} = \cancel{(v_0v_1) \times v_0} = \cancel{(v_0v_1) \times v_1} = \cancel{(v_0v_1) \times (v_0v_1)}$$

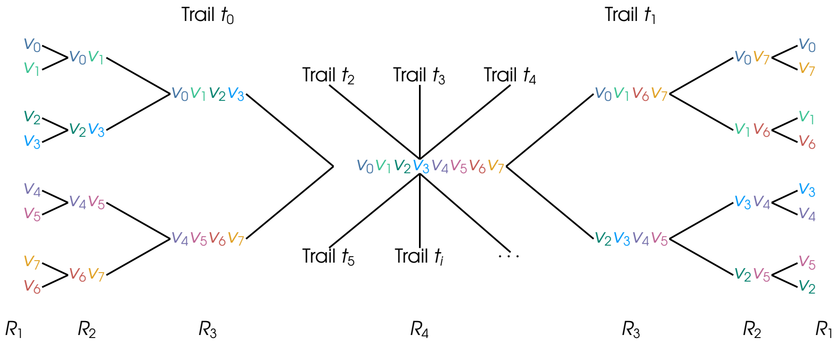


Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Strong constraint: products of two former highest-degree terms.

$$v_0v_1 = v_0 \times v_1 = \cancel{(v_0v_1) \times 1} = \cancel{(v_0v_1) \times v_0} = \cancel{(v_0v_1) \times v_1} = \cancel{(v_0v_1) \times (v_0v_1)}$$

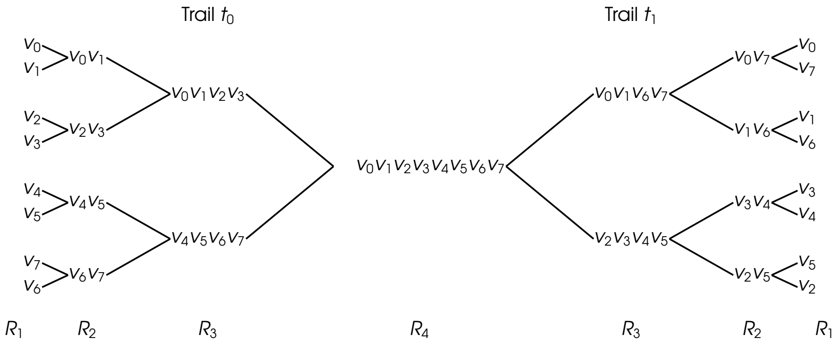


Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Strong constraint: products of two former highest-degree terms.

$$v_0v_1 = v_0 \times v_1 = \cancel{(v_0v_1) \times 1} = \cancel{(v_0v_1) \times v_0} = \cancel{(v_0v_1) \times v_1} = \cancel{(v_0v_1) \times (v_0v_1)}$$

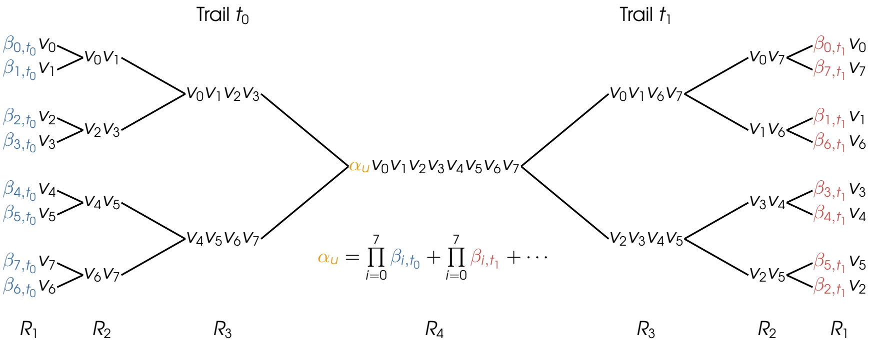


Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Strong constraint: products of two former highest-degree terms.

$$v_0v_1 = v_0 \times v_1 = \cancel{(v_0v_1) \times 1} = \cancel{(v_0v_1) \times v_0} = \cancel{(v_0v_1) \times v_1} = \cancel{(v_0v_1) \times (v_0v_1)}$$



- Fewer combinatorial choices
- Known structure of α_u: sum of products of former coefficients

For $r = 6$

- Still costly to recover the polynomial expressions: computations have to be done round after round.

- The polynomials look horrible!

▶ Need for a cheaper and easier recovery: **conditional cubes** [HWX+17, LDW17]

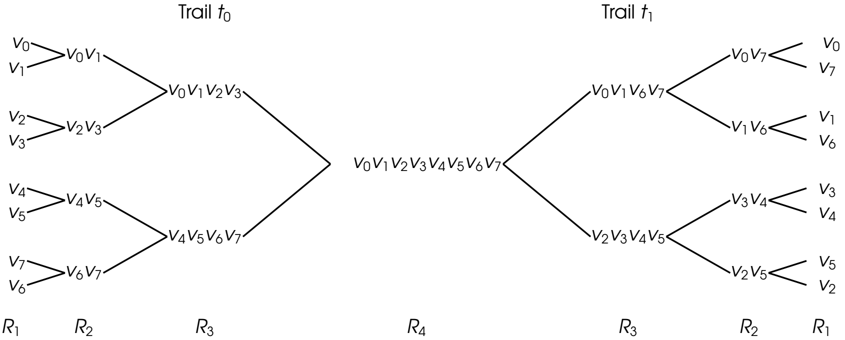
- We look for α_u with a simple divisor: β_0.
- **Without the full knowledge** of α_u, we can still deduce that: $\alpha_u = 1 \implies \beta_0 = 1$.
- If β_0 is linear, the **system** will be **linear**.

Practical cube-attack against nonce-misused Ascon

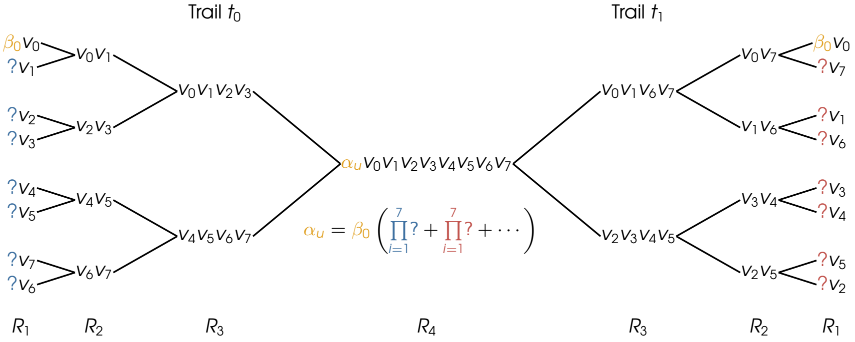
Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Conditional cubes

- We look for α_u with a simple divisor: β_0.
- **Without the full knowledge** of α_u, we can still deduce that: $\alpha_u = 1 \implies \beta_0 = 1$.
- If β_0 is linear, the **system** will be **linear**.



- We look for α_u with a simple divisor: β_0.
- **Without the full knowledge** of α_u, we can still deduce that: $\alpha_u = 1 \implies \beta_0 = 1$.
- If β_0 is linear, the **system** will be **linear**.

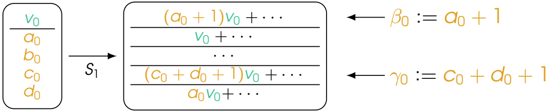


Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Choice of the cube: forcing some linear divisors

Study of the first rounds: Column C_0 after the first S-box layer

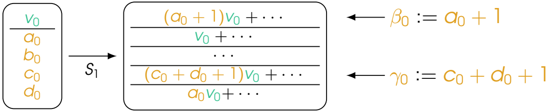


- After the second round, the coefficient of any v_0v_i, $i \neq 0$ can be decomposed as: $\beta_0 P + 1Q + \gamma_0 R + (\beta_0+1)S$.

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Study of the first rounds: Column C_0 after the first S-box layer



- After the second round, the coefficient of any v_0v_i, $i \neq 0$ can be decomposed as: $\beta_0 P + 1Q + \gamma_0 R + (\beta_0+1)S$.

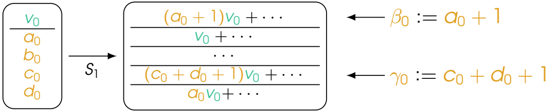
- It is possible to **select** the remaining 31 indices i such that all coefficients of v_0v_i at round 2 look like **either** $\beta_0 P$ **or** $\gamma_0 R$ instead.
- This ensures that: $\alpha_{u,j} = \beta_0(\dots) + \gamma_0(\dots)$ for all output coordinates after 6 rounds ($j \in [\![0, 63]\!]$).

Choice of the cube: forcing some linear divisors

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Study of the first rounds: Column C_0 after the first S-box layer



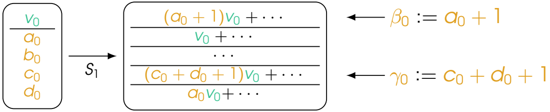
- After the second round, the coefficient of any $v_0 v_i$, $i \neq 0$ can be decomposed as: $\beta_0 P + 1Q + \gamma_0 R + (\beta_0 + 1)S$.
- It is possible to **select** the remaining 31 indices i such that all coefficients of $v_0 v_i$ at round 2 look like **either** $\beta_0 P$ **or** $\gamma_0 R$ instead.
- This ensures that: $\alpha_{u,j} = \beta_0(\dots) + \gamma_0(\dots)$ for all output coordinates after 6 rounds ($j \in [\![0, 63]\!]$).
- $(\alpha_{u,0}, \cdots, \alpha_{u,63}) \neq (0, \cdots, 0) \implies \beta_0 = 1$ or $\gamma_0 = 1$

Choice of the cube: forcing some linear divisors

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Study of the first rounds: Column C_0 after the first S-box layer



- After the second round, the coefficient of any $v_0 v_i$, $i \neq 0$ can be decomposed as: $\beta_0 P + 1Q + \gamma_0 R + (\beta_0 + 1)S$.
- It is possible to **select** the remaining 31 indices i such that all coefficients of $v_0 v_i$ at round 2 look like **either** $\beta_0 P$ **or** $\gamma_0 R$ instead.
- This ensures that: $\alpha_{u,j} = \beta_0(\dots) + \gamma_0(\dots)$ for all output coordinates after 6 rounds ($j \in [\![0, 63]\!]$).
- $(\alpha_{u,0}, \cdots, \alpha_{u,63}) \neq (0, \cdots, 0) \implies \beta_0 = 1$ or $\gamma_0 = 1$
- **In practice, reciprocal also true!** $\forall j,\ \alpha_{u,j} = 0 \implies \beta_0 = 0$ and $\gamma_0 = 0$

Practical cube-attack against nonce-misused Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

First step, non-adaptative: 32-degree conditional cubes

Recovery of all the bits $c_i + d_i + 1$, and about 32/64 a_i.

First step, non-adaptative: 32-degree conditional cubes

Recovery of all the bits $c_i + d_i + 1$, and about 32/64 a_i.

Second step, adaptative: 32-degree cubes

- 32-degree coefficients depend only on $c_i + d_i + 1$ and a_i.
- Inputting the recovered values **drastically simplifies** the expressions of some coefficients, and thus the computations.
- Simple-enough expressions to be **effectively-solved**.

▶ Recovery of the remaining a_i.

First step, non-adaptative: 32-degree conditional cubes

Recovery of all the bits $c_i + d_i + 1$, and about 32/64 a_i.

Second step, adaptative: 32-degree cubes

- 32-degree coefficients depend only on $c_i + d_i + 1$ and a_i.
- Inputting the recovered values **drastically simplifies** the expressions of some coefficients, and thus the computations.
- Simple-enough expressions to be **effectively-solved**.

▶ Recovery of the remaining a_i.

Third step, adaptative: **31-degree cubes**

- Cubes of lower size are needed to recover b_i and c_i.
- Same principle as second step

▶ Recovery of all b_i and c_i.

Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

- Full-state recovery on the full 6-round encryption: 2^{40} online time and data.
- Harder to study the complexity of the adaptative offline choices. The attack is however **effective**.
- Does not threaten Ascon directly.
- Good reminder that **a nonce is not a constant**!

Main questions/openings

- Misused-ciphers studies: academically interesting, is it "real-life" interesting ?
- Changing the input wire during encryption: a possible free counter-measure ?

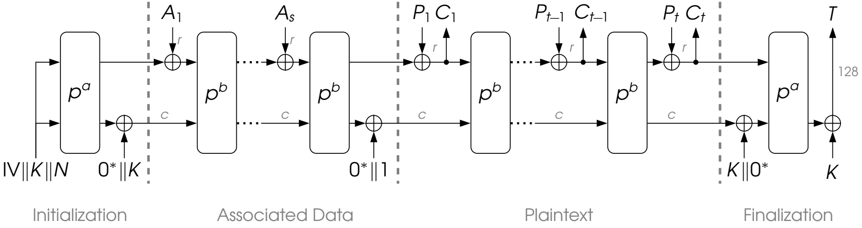
- Full-state recovery on the full 6-round encryption: 2^{40} online time and data.
- Harder to study the complexity of the adaptative offline choices. The attack is however **effective**.
- Does not threaten Ascon directly.
- Good reminder that **a nonce is not a constant**!

Main questions/openings

- Misused-ciphers studies: academically interesting, is it "real-life" interesting ?
- Changing the input wire during encryption: a possible free counter-measure ?

Thank you for your attention!

The whole Ascon AEAD mode



[DEMS, Jea16]

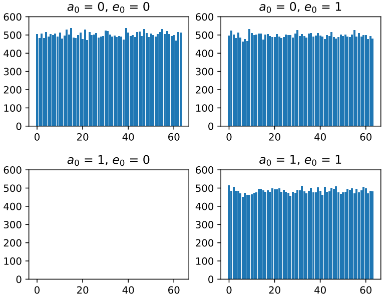
Jules Baudrin, Anne Canteaut & Léo Perrin (Inria, Paris, France)

Justifying the “in practice” reciprocal

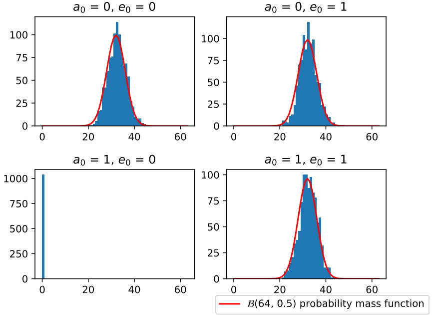
$$\alpha_{u,\,j} = (a_0 + 1)p_{j,1} + (c_0 + d_0 + 1)p_{j,2}\ \forall\, j \in [\![0, \cdots, 63]\!].$$

When $(a_0 + 1, c_0 + d_0 + 1) \neq (0, 0)$, $\alpha_{u,\,j}$ are not expected to be **all** canceled at the same time.

Whenever we observe that $\alpha_{u,\,j} = 0\ \forall\, j$, we guess that $(a_0, c_0 + d_0) = (1, 1)$.



Individual cancellations of each $\alpha_{u,j}$
(1000 random internal states)



Hamming weight of the cube-sum vectors
(1000 random internal states)

Second step, adaptative: 32-degree cubes

- 32-degree coefficients depend only on $c_i + d_i + 1$ and a_i.
- After step 1, all the $c_i + d_i + 1$ **are recovered** and about half of the a_i as well.
- We choose our 32 indices i in order to **minimize the number of unknowns**.
- Each α_u is a sum of products, each product being of the form: $\prod_{i, u_i = 1} \ell_i$ where $\ell_i \in \{a_i, 1, c_i + d_i + 1, a_i + 1\}$. Such a product is very often equal to 0 !
- Minimizing the number of unknowns = **Minimizing the degree and the density of the expressions**.
- Simple-enough expressions to be **effectively-computed** round after round, then **effectively-solved** (over-determined, small degree, sparse systems).

Third step, adaptative: **31-degree cubes**: $\mathrm{wt}(u) = 31$

Each α_u is a sum of products. Each product is either:

- the product of 32 coefficients of degree-1 terms after S_1, or
- the product of one constant term and 31 coefficients of degree-1 terms.

Each coefficient of degree-1 term is known (because all $c_i + d_i + 1$ and all a_i are known).

So α_u can be expressed as a sum of constant terms, that is, a quadratic polynomial in the remaining unknowns b_i, c_i. ($d_i = c_i + 1 + \varepsilon_i$ with known ε_i)

Again, the computations and the solving of the systems are practical.

Bibliography

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
Cryptographic sponge functions, 2011.
https://keccak.team/sponge_duplex.html.

Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer.
Ascon TikZ figures.
https://ascon.iaik.tugraz.at/resources.html.

Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer.
Ascon v1.2.
Technical report, National Institute of Standards and Technology, 2019.
https://csrc.nist.gov/Projects/lightweight-cryptography/finalists.

Senyang Huang, Xiaoyun Wang, Guangwu Xu, Meiqin Wang, and Jingyuan Zhao.
Conditional cube attack on reduced-round Keccak sponge function.
In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 259–288, Paris, France, April 30 – May 4, 2017. Springer, Heidelberg, Germany.

Jérémy Jean.
TikZ for Cryptographers.
https://www.iacr.org/authors/tikz/, 2016.

Zheng Li, Xiaoyang Dong, and Xiaoyun Wang.
Conditional cube attack on round-reduced ASCON.
IACR Trans. Symm. Cryptol., 2017(1):175–202, 2017.