Radboud University

Twin Column Parity Mixers and Gaston

A New Mixing Layer and Permutation

Solane El Hirch[1], Joan Daemen[1], Raghvendra Singh Rohit[2], Rusydi H. Makarim

CRYPTO

August 19-24, 2023

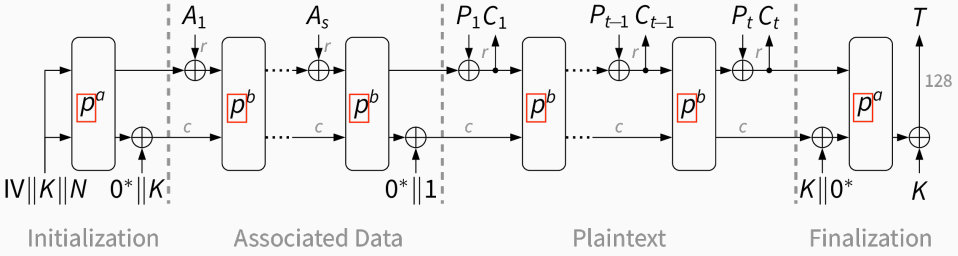
[1]Radboud University (The Netherlands)

[2]Technology Innovation Institute (United Arab Emirates)

Overview

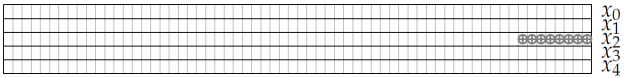
Ascon

- Family of cryptographic algorithms for authenticated encryption (AE) and hashing
- Winner of the NIST lightweight cryptography competition
- AE scheme based on the MonkeyDuplex mode
- Authenticated Encryption operation: with p^a and p^b the permutation ASCON-p with different number of rounds [Dobraunig et al.]

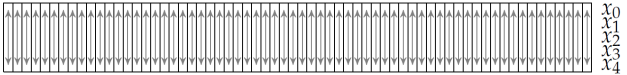


Ascon-p round transformation in [Dobraunig et al.]

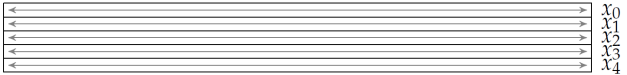
- 320-bit state: 5 rows $x_0, \ldots, x_4$ and 64 columns
- Round transformation $p = p_L \circ p_S \circ p_C$



(a) Round constant addition p_C

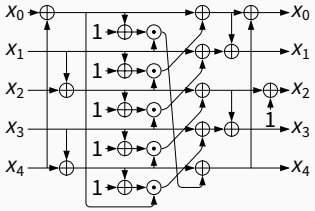


(b) Substitution layer p_S with 5-bit S-box $\mathcal{S}(x)$



(c) Linear layer with 64-bit diffusion functions $\Sigma_i(x_i)$

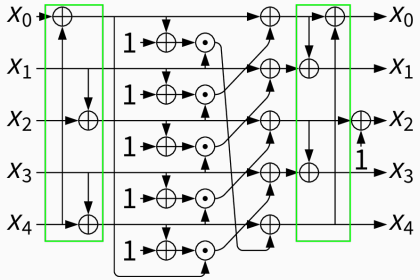
(a) Substitution layer p_S: χ_5 of KECCAK-f [BDPV11] and two mixing steps



(b) Linear layer p_L:

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

Operations dedicated to mixing in Ascon-p



6 bitwise XORs

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

10 bitwise XORs + 10 cyclic shifts

- Total computational cost: 16 bitwise XORs + 10 cyclic shifts
- Shift operations are often cheap, e.g. barrel shifter in the ARM Cortex-M family
- **Gate cost** of 3.2 binary XOR operations per bit

Can we get higher diffusion for the same gate cost?

Diffusion metrics

Difference and linear propagation

Differential cryptanalysis (DC)

- Pair of input and output difference referred as a *differential*
- DC exploits high-probability differentials
- Round differential: differential over a round function
- Differential *trail*: chain of round differentials

Linear cryptanalysis (LC)

- Combination of input mask and output mask is called a *linear approximation*
- LC exploits linear approximations with high correlation
- Round linear approximation: linear approximation over a round function
- Linear trail: chain of round linear approximations

Avoid differential trails with high probability and/or linear trails with high correlation contribution

Metric for diffusion: the branch number

- **Branch number**: measure for the diffusion realized by a mapping popularized through AES
- Branch number of a state

$$\mathcal{B}_L(A) = w_h(A) + w_h(L(A))$$

  where w_h is the Hamming weight
- **High diffusion power:** there are few states with low branch number
- Branch number of linear layer L: for state A in the state space $\mathcal{A}$ w.r.t. L

$$\mathcal{B}(L) = \min_{A \in \mathcal{A} \setminus \{0\}} \mathcal{B}_L(A)$$

- Ascon-p mixing layer has branch number of 4

Circulant twin column parity mixers and row shifts

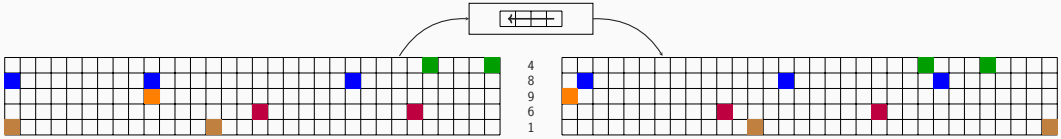
Use case

- Build a permutation with a round function
  - Non-linear layer as in ASCON-p: working on columns independently
  - Linear layer: mixlayer between two cyclic row shift steps
- State of m rows with n columns
- Suitable for software implementation: $n = 2^\ell$
- Mappings that are translation-invariant in the horizontal direction: **circulant**

Cyclic row shifts

Similar to ShiftRows in Rijndael [DR02]

$$\rho_{\text{east}}: \quad A_i \leftarrow (A_i \lll e_i), \text{ for } 0 \le i < m$$
$$\rho_{\text{west}}: \quad A_i \leftarrow (A_i \lll w_i), \text{ for } 0 \le i < m$$

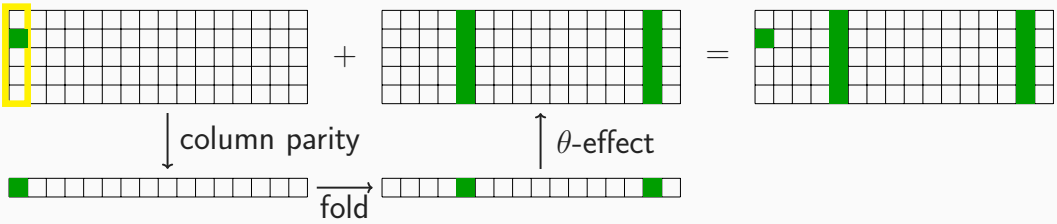


- e_i and w_i are offsets to specify
- Set $e_0 = 0$ and $w_0 = 0$

Specify $2(m-1)$ offsets

Circulant column parity mixer (CPM)

- Column parity mixers used in KECCAK-f and XOODOO
- Applied to our 2-dimensional state:

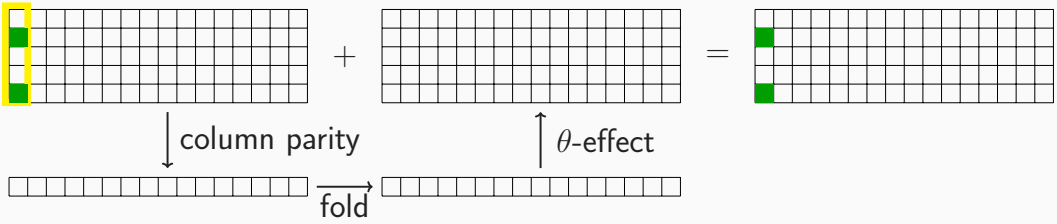


- Computational cost: $m-1$ per row for the CPM, 1 per row for the folding operation, m per row for the addition to the state totaling to $2m$ per row

CPM has computational cost of 2 XORs per bit

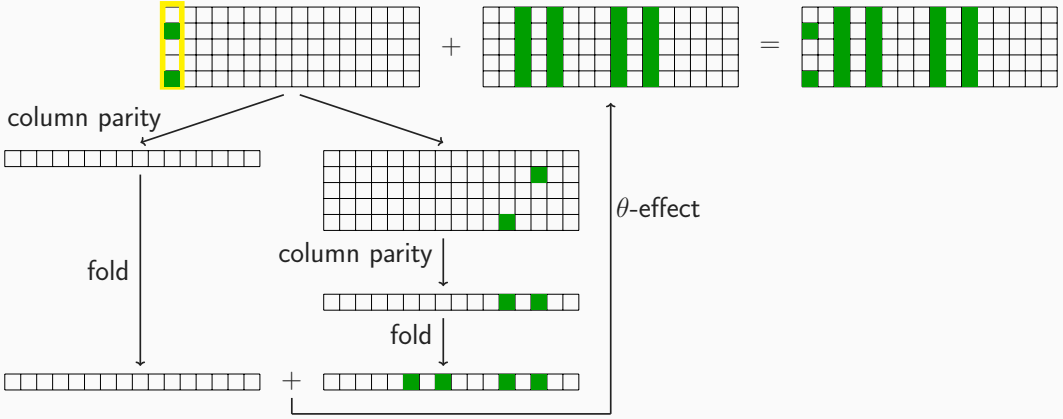
Circulant column parity mixer (CPM)

- Column parity mixers used in KECCAK-f and XOODOO
- Applied to our 2-dimensional state:



- Computational cost: CPM has computational cost of 2 XORs per bit
- Branch number of 4

Circulant twin CPM



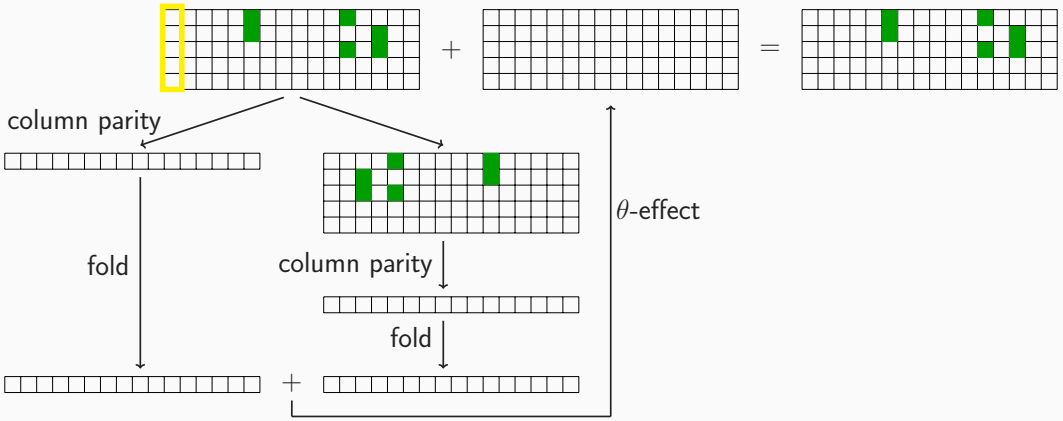
Twin CPM has a **computational cost** of 3.2 XORs per bit

Specify $m + 3$ offsets

Differential and linear propagation properties

Differential diffusion properties of twin CPMs

θ-effect kernel: subspace of states where the twin CPM acts like the identity



Differential diffusion properties of twin CPMs

θ-**effect kernel:** subspace of states where the twin CPM acts like the identity

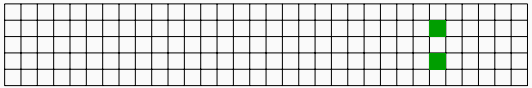
- Branch number is twice the number of active bits
- States in the kernel with less than 6 active bits have low branch number: undesirable

States with low branch number outside of the kernel: undesirable

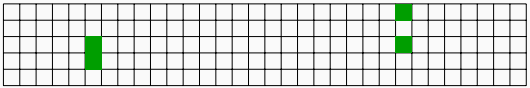
Conditions on the shift offsets to achieve differential branch number of 12

Undesirable in-kernel states

- States avoidable by conditions on shift offsets

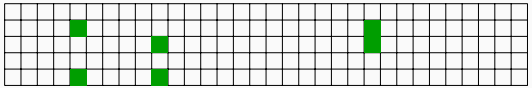


Orbital: Branch number of at most 4

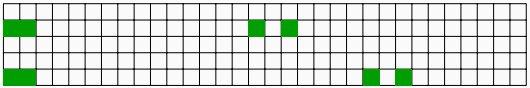


States with less than 6 active bits

- States unavoidable



Vortices: Branch number of at most 12



Row twins

Linear mask propagation properties

- Study linear propagation from the output to the input: a mask v at the output of θ maps to a mask $u = \theta^{\mathrm{T}}(v)$ before θ
- Branch number:

$$\mathcal{B}(L) = \min_{A \in \mathcal{A} \setminus \{0\}} (w_h(A) + w_h(\theta(A)))$$

corresponds to the differential branch number

Linear mask propagation properties

- Study linear propagation from the output to the input: a mask v at the output of θ maps to a mask $u = \theta^{\mathrm{T}}(v)$ before θ
- Linear branch number:

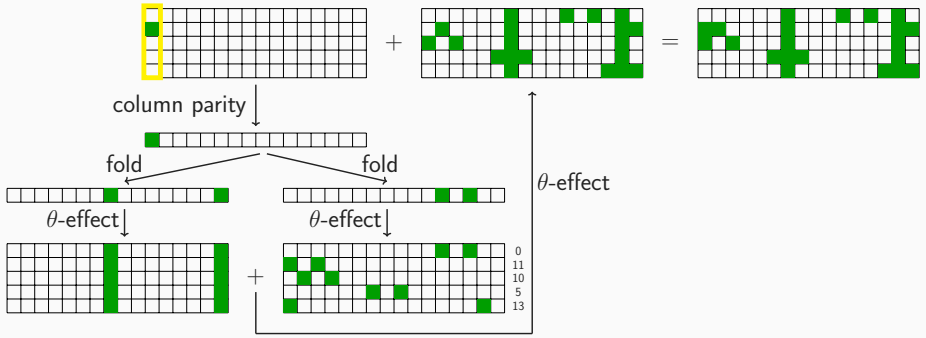
$$\mathcal{B}(\theta^{\mathrm{T}}) = \min_{A \in \mathcal{A} \setminus \{0\}} (w_h(A) + w_h(\theta^{\mathrm{T}}(A)))$$

Linear mask propagation properties

- Study linear propagation from the output to the input: a mask v at the output of θ maps to a mask $u = \theta^{\mathrm{T}}(v)$ before θ
- The inherent presence of orbitals in the kernel of θ^{T} leads to a **linear branch number of 4**
- Low-weight 3-round trails in the kernel of θ^{T} in two consecutive rounds
  - Avoid 3-round trails with weight 12 and 24
  - Cannot avoid 3-round trails with 6-bit states with weight at most 36

Transpose of a twin CPM

Twin CPM has differential branch number 12 and linear branch number 4: we **can build** a mixing layer with linear branch number 12 and differential branch number 4 by *transposing* the twin CPM



Same computational cost

Proof-of-concept: Gaston

Gaston round function and the state

- State of five 64-bit rows
- Linear layer
  - $\lambda = \rho_{\text{west}} \circ \theta \circ \rho_{\text{east}}$
  - θ is a twin CPM
  - Round constant addition ι
- Non-linear layer: χ mapping of KECCAK-f applied on 5-bit columns as in ASCON-p

Determining the shift offsets: search strategy

Shift offsets of λ gathered in

$$\mathrm{R}_\lambda = (\mathrm{R}_\theta, \mathrm{R}_\rho)$$

$$\mathrm{R}_\lambda = (s, t_0, t_1, t_2, t_3, t_4, u, w_0, w_1, w_2, w_3, w_4, e_0, e_1, e_2, e_3, e_4)$$

- Choose R_λ s.t λ has a branch number of 12

  $\rightarrow$ **Any 2-round trail has at least 12 active columns**

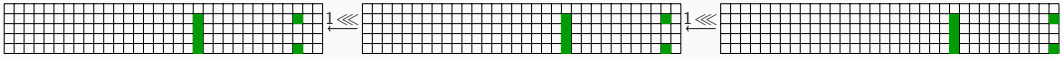
- Choose R_ρ to translate the bit-level diffusion to the column level for λ
  - The rows shuffles should move bits in same columns to different columns
  - Minimize number of bits in the same columns after ρ_{east}
  - Eliminate candidates that lead to low-weight 3-round linear trails
  - Maximize minimum squared correlation C^2 of 3-round trails

Differential and linear bounds of Gaston

Experiments

Selecting the offsets requires the generation of states: tree-based approach [HMMD22]

- Partitions the state space in classes
- Restrict investigations on propagation to one representative of each class: **canonical**



- Generate all states with branch number below a given target

Further investigation with a hybrid usage of SMT and MILP

- Differential and linear branch numbers
- Best 3-round differential and linear trails

Results

Differential		
	Gaston	ASCON-p
Branch number	12	4
Minimum weight of 2-round trail	24	8
Minimum weight of 3-round trail	≤ 106	40
Linear		
Branch number	4	4
Minimum weight of 2-round trail	8	8
Minimum weight of 3-round trail	34	28

Conclusion

Conclusion

Circulant twin CPMs are a generalization of CPMs used in KECCAK-f and XOODOO

- High local diffusion
- Optimization for differential or linear branch number
- Proof-of-concept: lightweight permutation Gaston
  - Same budget in terms of gate cost
  - Better differential and linear propagation properties than ASCON-p

Thank you for your attention!


G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche.
The KECCAK reference, January 2011.
https://keccak.team/papers.html.


J. Daemen and V. Rijmen.
The Design of Rijndael: AES - The Advanced Encryption Standard.
Information Security and Cryptography. Springer, 2002.


Solane El Hirch, Silvia Mella, Alireza Mehrdad, and Joan Daemen.
Improved differential and linear trail bounds for ASCON.
IACR Trans. Symmetric Cryptol., 2022(4):145–178, 2022.