Cryptanalysis of QARMAv2

Hosein Hadipour Yosuke Todo

FSE 2024 - Leuven, Belgium

› hsn.hadipour@gmail.com

Motivation and Our Contributions

Motivation

- Sheding more light on the security of QARMAv2 against cryptanalysis.

Contributions

- Proposing a new CP-based tool to search for intergal distinguishers of tweakable block ciphers following the TWEAKEY framework.
- Providing the first concrete key recovery attack against three main variants of QARMAv2.

Motivation and Our Contributions

Motivation

- Sheding more light on the security of `QARMAv2` against cryptanalysis.

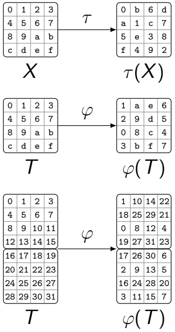
Contributions

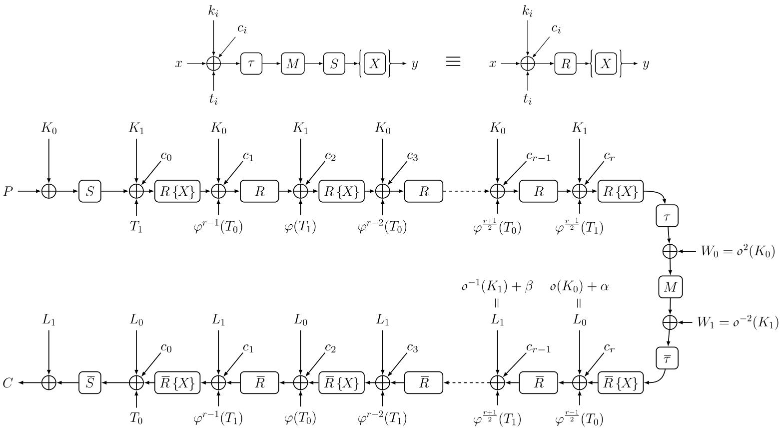
- Proposing a new CP-based tool to search for intergal distinguishers of tweakable block ciphers following the `TWEAKEY` framework.
- Providing the first concrete key recovery attack against three main variants of `QARMAv2`.

Outline

Background and Specification of QARMAv2

QARMAv2 Family of Tweakable Block Ciphers [Ava+23]





$$M := \begin{pmatrix} 0 & \rho & \rho^2 & \rho^3 \\ \rho^3 & 0 & \rho & \rho^2 \\ \rho^2 & \rho^3 & 0 & \rho \\ \rho & \rho^2 & \rho^3 & 0 \end{pmatrix}$$

$\rho \in \mathbb{F}_2^4$, $\rho^4 = 1$

Hosein Hadipour, Yosuke Todo

Security Parameters

Parameters of QARMAv2 with two tweak blocks ($\mathscr{T} = 2$).

Version	Block size (b)	Key Size (s)	r	#Rounds	Time	Data
QARMAv2-64-128	64	128	9	20	$2^{128-\varepsilon}$	2^{56}
QARMAv2-128-128	128	128	11	24	$2^{128-\varepsilon}$	2^{80}
QARMAv2-128-192	128	192	13	28	$2^{192-\varepsilon}$	2^{80}
QARMAv2-128-256	128	256	15	32	$2^{256-\varepsilon}$	2^{80}

Parameters of QARMAv2 with a single tweak block ($\mathscr{T} = 1$).

Version	Block size (b)	Key Size (s)	r	#Rounds	Time	Data
QARMAv2-64-128	64	128	7	16	$2^{128-\varepsilon}$	2^{56}
QARMAv2-128-128	128	128	9	20	$2^{128-\varepsilon}$	2^{80}
QARMAv2-128-192	128	192	11	24	$2^{192-\varepsilon}$	2^{80}
QARMAv2-128-256	128	256	13	28	$2^{256-\varepsilon}$	2^{80}

Designers' Analyses [Ava+23]

	QARMAv2-64		QARMAv2-128	
Attack	Parameter r	Rounds	Parameter r	Rounds
Differential	6 (5)	14 (12)	9 (8)	20 (18)
Boomerang (Sandwich)	7 (5)	16 (12)	10 (8)	22 (18)
Linear	5	12	7	16
Impossible-Differential	3	8	4	10
Zero-Correlation	3	8	4	10
Integral (Division Property)	–	5	–	–
Meet-in-the-Middle	–	10	–	12
Invariant Subspaces	–	5	–	6
Algebraic (Quadratic Equations)	–	6	–	7

Integral and Zero-Correlation (ZC) Distinguishers

- Integral attacks [Lai94; DKR97]
- ZC attacks [BR14]

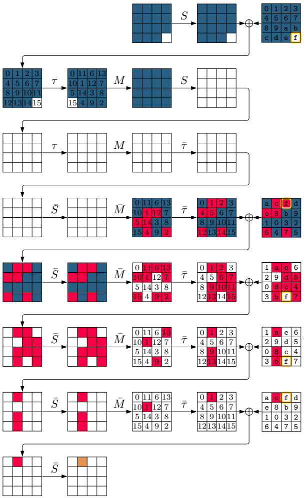
Link Between ZC and Integral Distinguishers [Sun+15]

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. Assume A is a subspace of $\mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^n \setminus \{0\}$ such that (α, β) is a ZC approximation for any $\alpha \in A$. Then, for any $\lambda \in \mathbb{F}_2^n$, $\langle \beta, F(x + \lambda) \rangle$ is balanced over the set

$$A^{\perp} = \{x \in \mathbb{F}_2^n \mid \forall\ \alpha \in A : \langle \alpha, x \rangle = 0\}.$$

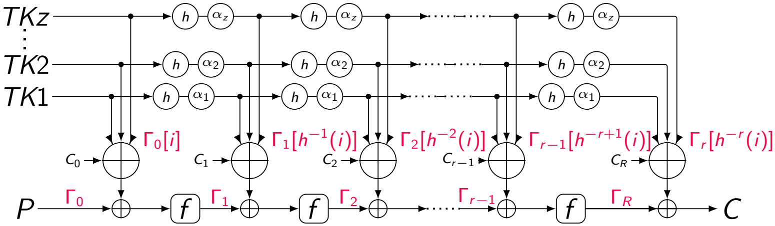
Example: Conversion of ZC Distinguisher to Integral Distinguisher

- ZC distinguisher:
  - ■/■/■: Fixed/Nonzero/Any value for linear mask
- Integral distinguisher:
  - $X_0[15] || T[15]$ takes all possible values and the remaining cells take a fixed value
  - $X_7[1]$ is balanced



Hosein Hadipour, Yosuke Todo

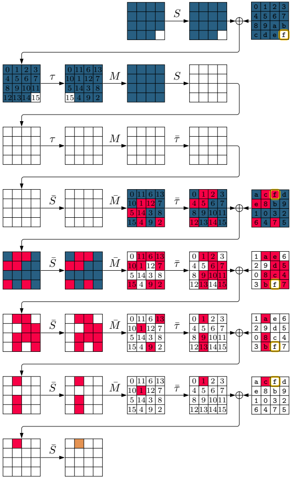
ZC Distinguishers for Ciphers Following the TWEAKEY Framework

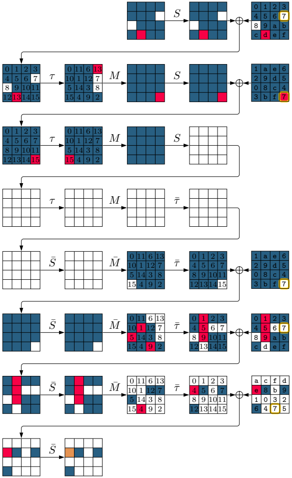


Ankele et al. [Ank+19]

Let $E_K(T, P) : \mathbb{F}_2^{t\times n} \to \mathbb{F}_2^n$ be a TBC following the STK construction. Suppose that the tweakey schedule of E_K has z parallel paths and applies a permutation h on the tweakey cells in each path. Let (Γ_0, Γ_r) be a pair of linear masks for r rounds of E_K, and $\Gamma_1, \ldots, \Gamma_{r-1}$ represents a possible sequence for the intermediate linear masks. If there is a cell position i such that any possible sequence $\Gamma_0[i], \Gamma_1[h^{-1}(i)], \Gamma_2[h^{-2}(i)], \ldots \Gamma_r[h^{-r}(i)]$ has at most z linearly active cells, then (Γ_0, Γ_r) yields a ZC linear hull for r rounds of E.

Example: ZC Distinguisher for Tweakable Block Ciphers



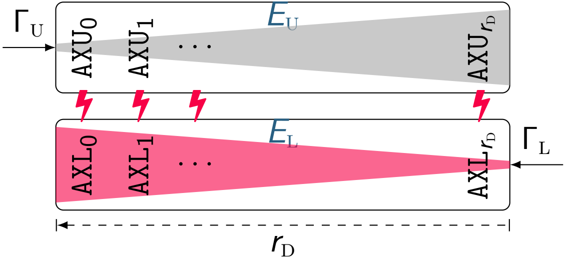


: Fixed nonzero, : Any nonzero, : Unknown

Hosein Hadipour, Yosuke Todo

CP Model to Search for ZC-based Integral Distinguishers [HSE23]

- $\mathcal{CSP}_{\mathrm{U}}(\Gamma_{\mathrm{U}})$
- $\mathcal{CSP}_{\mathrm{L}}(\Gamma_{\mathrm{L}})$
- $\mathcal{CSP}_{\mathtt{M}}(\Gamma_{\mathrm{U}}, \Gamma_{\mathrm{L}})$
- $\mathcal{CSP}_{\mathrm{D}} = \mathcal{CSP}_{\mathrm{U}} \wedge \mathcal{CSP}_{\mathrm{L}} \wedge \mathcal{CSP}_{\mathtt{M}}$



Properties of MixColumns of QARMAv2

Properties of MixColumns of QARMAv2

- MixColumns of QARMAv2 is defined as follows:

$$\begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = \begin{pmatrix} 0 & \rho & \rho^2 & \rho^3 \\ \rho^3 & 0 & \rho & \rho^2 \\ \rho^2 & \rho^3 & 0 & \rho \\ \rho & \rho^2 & \rho^3 & 0 \end{pmatrix} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix} = \begin{pmatrix} \rho X_1 + \rho^2 X_2 + \rho^3 X_3 \\ \rho^3 X_0 + \rho X_2 + \rho^2 X_3 \\ \rho^2 X_0 + \rho^3 X_1 + \rho X_3 \\ \rho X_0 + \rho^2 X_1 + \rho^3 X_2 \end{pmatrix}.$$

- ρ: rotation to the left by 1 bit, and $\rho^4 = 1$.

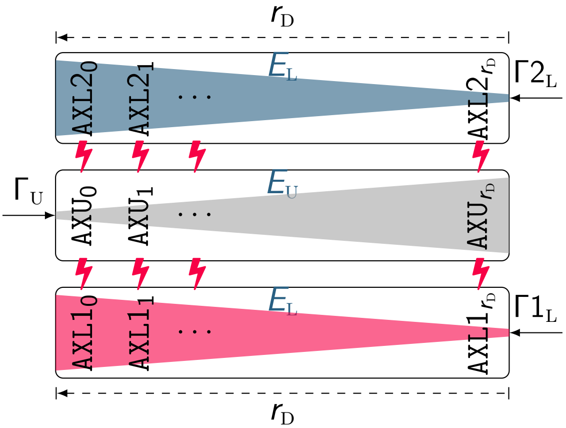
- If X_i and X_j have the zero-sum property simultaneously, then a linear combination of Y_i and Y_j also has the zero-sum property:

$$\bigoplus_{c \in \mathbb{C}} \left((\rho^{(i-j) \bmod 4} X_i(c)) \oplus X_j(c) \right) = \bigoplus_{c \in \mathbb{C}} \left((\rho^{(i-j) \bmod 4} Y_i(c)) \oplus Y_j(c) \right).$$

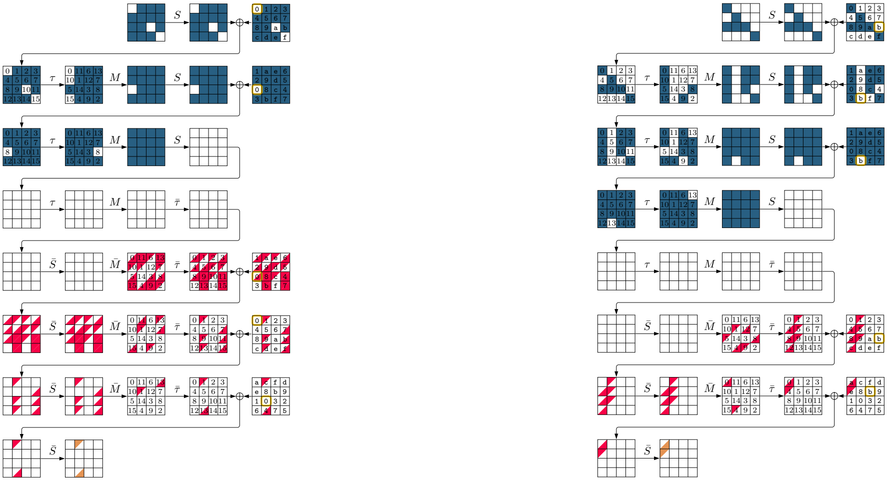
Our Method to Search for Distinguishers

Our Method to Search for ZC-based Integral Distinguishers

- $CSP_{\mathrm{U}}(\Gamma_{\mathrm{U}})$
- $CSP1_{\mathrm{L}}(\Gamma1_{\mathrm{L}})$
- $CSP2_{\mathrm{L}}(\Gamma2_{\mathrm{L}})$
- $CSP_{\mathtt{M}}(\Gamma_{\mathrm{U}}, \Gamma1_{\mathrm{L}}, \Gamma2_{\mathrm{L}})$
- $CSP_{\mathrm{U}} \wedge CSP1_{\mathrm{L}} \wedge CSP2_{\mathrm{L}} \wedge CSP_{\mathtt{M}}$



Example of Our Method to Search for Distinguishers



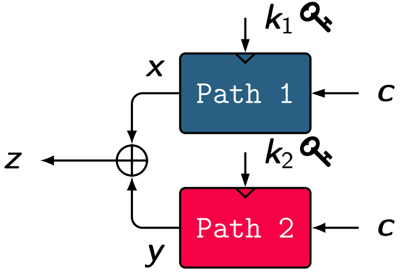
: Fixed nonzero, : Any nonzero, : Unknown

Hosein Hadipour, Yosuke Todo

Key Recovery Attack on QARMAv2

Naive Approach v.s. MitM [SW12]

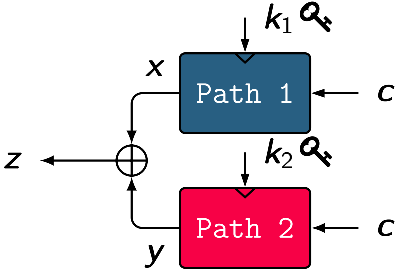
- Naive approach:
  - $x = F(\boldsymbol{k}_1, \boldsymbol{k}_2, \boldsymbol{c})$
  - $T = N \cdot 2^{|\boldsymbol{k}_1 \cup \boldsymbol{k}_2|}$
- MitM:
  - $x = g(\boldsymbol{k}_1, \boldsymbol{c}), \; y = h(\boldsymbol{k}_2, \boldsymbol{c})$
  - $T = N \cdot 2^{|\boldsymbol{k}_1|} + N \cdot 2^{|\boldsymbol{k}_2|}$



$$\sum_{c \in \boldsymbol{c}} z = 0$$

Naive Approach v.s. MitM [SW12]

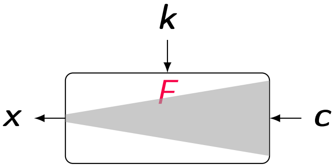
- Naive approach:
  - $\boldsymbol{x} = F(\boldsymbol{k}_1, \boldsymbol{k}_2, \boldsymbol{c})$
  - $T = N \cdot 2^{|\boldsymbol{k}_1 \cup \boldsymbol{k}_2|}$
- MitM:
  - $\boldsymbol{x} = g(\boldsymbol{k}_1, \boldsymbol{c}),\ \boldsymbol{y} = h(\boldsymbol{k}_2, \boldsymbol{c})$
  - $T = N \cdot 2^{|\boldsymbol{k}_1|} + N \cdot 2^{|\boldsymbol{k}_2|}$



$$\sum_{c \in \boldsymbol{c}} \boldsymbol{z} = 0 \iff \sum_{c \in \boldsymbol{c}} \boldsymbol{x} = \sum_{c \in \boldsymbol{c}} \boldsymbol{y}$$

Naive Approach v.s. Partial-Sum Technique [Fer+00]

- Naive approach:
  - $\boldsymbol{x} = F(\boldsymbol{k}, \boldsymbol{c})$
  - $T = N \cdot 2^{|\boldsymbol{k}|}$



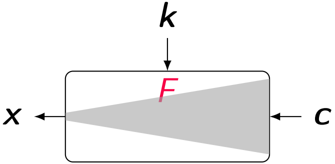
- Partial-sum technique:
  - $x_1 = f_1(k_1, x_0), x_2 = f_2(k_2, x_1), \cdots, \boldsymbol{x} = f_n(k_n, x_{n-1})$
  - $x_0 = \boldsymbol{c}, N_0 = N, N_i < N$
  - $T = \sum_{i=1}^{n} \frac{N_{i-1}}{n} \cdot 2^{|k_1| + \cdots + |k_i|} < \sum_{i=1}^{n} \frac{N}{n} \cdot 2^{|\boldsymbol{k}|}$
  - $T < N \cdot 2^{|\boldsymbol{k}|}$

Hosein Hadipour, Yosuke Todo

Naive Approach v.s. Partial-Sum Technique [Fer+00]

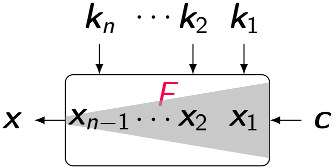
Naive approach:

- $x = F(\boldsymbol{k}, \boldsymbol{c})$
- $T = N \cdot 2^{|\boldsymbol{k}|}$



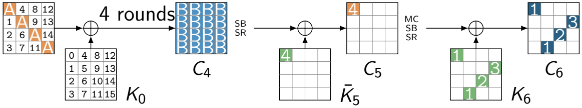
Partial-sum technique:

- $x_1 = f_1(\boldsymbol{k}_1, x_0), x_2 = f_2(\boldsymbol{k}_2, x_1), \cdots, x = f_n(\boldsymbol{k}_n, x_{n-1})$
- $x_0 = \boldsymbol{c}, N_0 = N, N_i < N$
- $T = \sum_{i=1}^{n} \frac{N_{i-1}}{n} \cdot 2^{|\boldsymbol{k}_1|+\cdots+|\boldsymbol{k}_i|} < \sum_{i=1}^{n} \frac{N}{n} \cdot 2^{|\boldsymbol{k}|}$
- $T < N \cdot 2^{|\boldsymbol{k}|}$

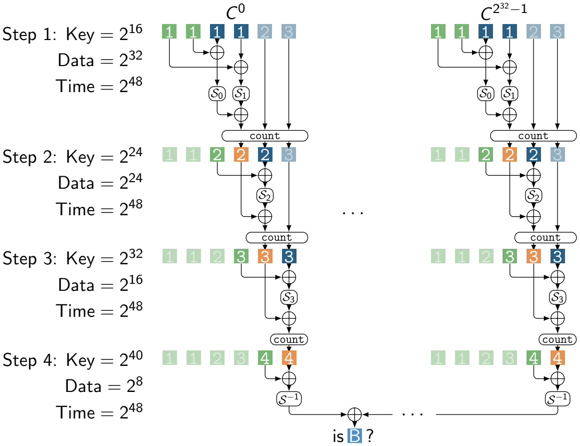


Hosein Hadipour, Yosuke Todo

Example: Partial-Sum Technique [Fer+00]

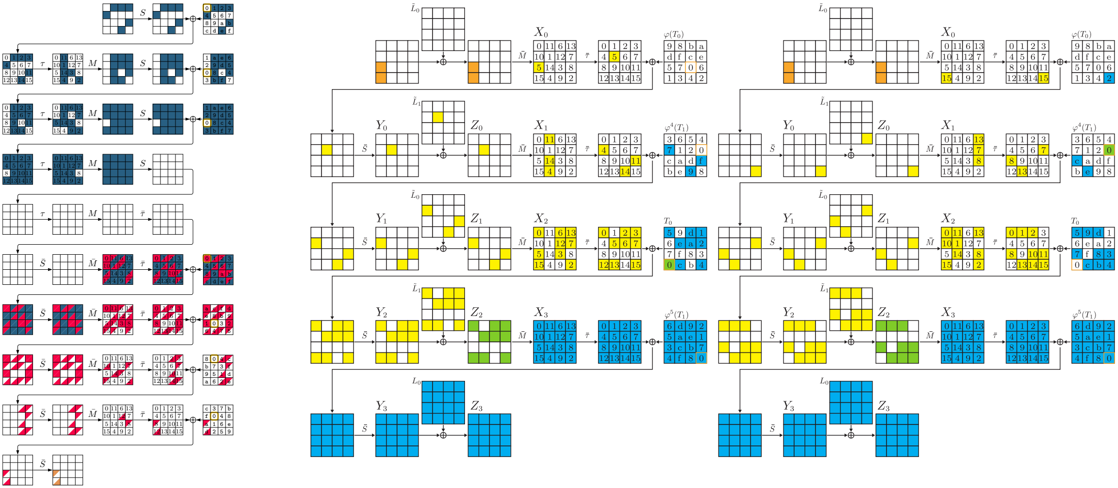


- Guess $K_6[0, 7]$ and derive $\mathcal{S}_0(C_6[0] \oplus K_6[0]) \oplus \mathcal{S}_1(C_6[7] \oplus K_6[7])$
- Guess $K_6[10]$ and derive $\mathcal{S}_2(C_6[10] \oplus K_6[10])$
- Guess $K_6[13]$ and derive $\mathcal{S}_3(C_6[13] \oplus K_6[13])$
- Guess $\bar{K}_5[0]$ and derive $C_4[0]$
- Time complexity: $6 \times 4 \times 2^{48} \approx 2^{52}$ S-box lookups



Hosein Hadipour, Yosuke Todo
FSE 2024 - Leuven, Belgium

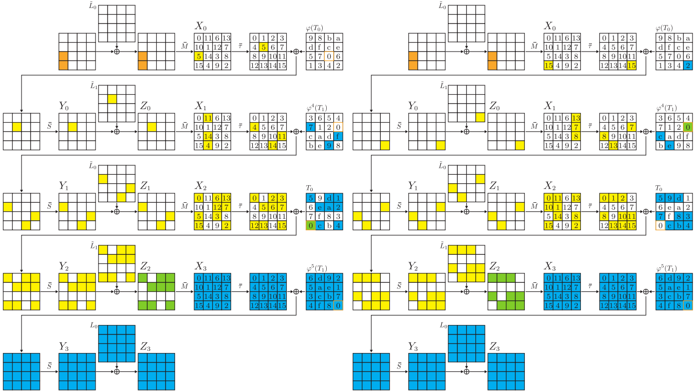
13-Round Integral Attack on QARMAv2-64-128 ($\mathscr{T} = 1$) I



Hosein Hadipour, Yosuke Todo
FSE 2024 - Leuven, Belgium

Our Key Recovery Attack on QARMAv2-64-128 ($\mathscr{T} = 1$) II

- Guess L_0:
  - Compute $X_0[5]$ by partial-sum technique.
  - Compute $X_0[15]$ by partial-sum technique.
  - Merge the results to derive 2^{64-4s} candidates for L_1.
  - Brute force the remaining 2^{64-4s} candidates for L_1 by 1 extra pair.
- Each partial-sum involves 36 bits of L_1.



$$T = 2^{64} \times \left(s \times 2^{44}\texttt{RF} + s \times 2^{50.15}\texttt{MA} + s \times 2^{50.67}\texttt{MA} + 2^{64-4s}\texttt{ENC}\right)$$

For $s = 5: \;\; T = 2^{110.47}, \;\; M = 2^{44}, \;\; D = 5 \times 2^{44}$

Hosein Hadipour, Yosuke Todo
FSE 2024 - Leuven, Belgium

Contributions and Future Works

Contributions and Future Works I

Summary of our attacks on QARMAv2. $\mathscr{T}$: No. of independent tweak blocks.

Version	$\mathscr{T}$	#Rounds	Time	Data	Memory
QARMAv2-64-128	1	**13**/16	$2^{110.47}$	$2^{46.32}$	$2^{46.32}$
QARMAv2-64-128	2	14/20	$2^{110.17}$	$2^{46.32}$	$2^{46.32}$
QARMAv2-128-256	2	16/32	$2^{234.11}$	$2^{46.58}$	$2^{46.58}$

Contributions and Future Works II

- Contributions
  - Introducing a new CP-based tool to search for integral distinguishers of tweakable block ciphers following the TWEAKEY framework.
  - Providing the longest concrete key recovery attack against QARMAv2.
- Future works
  - Whether there exists a 12-round integral distinguisher for QARMAv2-128 ($\mathscr{T} = 2$) with data complexity less than 2^{80}?
  - Can other cryptanalytic techniques, outperforme our integral attacks, especially for QARMAv2-64-128 ($\mathscr{T} = 1$)?

: https://github.com/hadipourh/QARMAnalysis

: https://ia.cr/2023/1833

Bibliography I

[Ank+19] Ralph Ankele et al. **Zero-Correlation Attacks on Tweakable Block Ciphers with Linear Tweakey Expansion**. *IACR Transactions on Symmetric Cryptology* 2019.1 (Mar. 2019), pp. 192–235. DOI: 10.13154/tosc.v2019.i1.192-235.

[Ava+23] Roberto Avanzi et al. **The QARMAv2 Family of Tweakable Block Ciphers**. *IACR Trans. Symmetric Cryptol.* 2023.3 (2023), pp. 25–73. DOI: 10.46586/TOSC.V2023.I3.25-73.

[BR14] Andrey Bogdanov and Vincent Rijmen. **Linear hulls with correlation zero and linear cryptanalysis of block ciphers**. *Des. Codes Cryptogr.* 70.3 (2014), pp. 369–383. DOI: 10.1007/s10623-012-9697-z.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. **The Block Cipher Square**. FSE 1997. Vol. 1267. LNCS. Springer, 1997, pp. 149–165. DOI: 10.1007/BFb0052343.

Bibliography II

[Fer+00] Niels Ferguson et al. **Improved Cryptanalysis of Rijndael**. FSE 2000. Vol. 1978. LNCS. Springer, 2000, pp. 213–230. DOI: 10.1007/3-540-44706-7_15.

[HSE23] Hosein Hadipour, Sadegh Sadeghi, and Maria Eichlseder. **Finding the Impossible: Automated Search for Full Impossible Differential, Zero-Correlation, and Integral Attacks**. EUROCRYPT 2023. Vol. 14007. LNCS. Springer, 2023, pp. 128–157. DOI: 10.1007/978-3-031-30634-1_5.

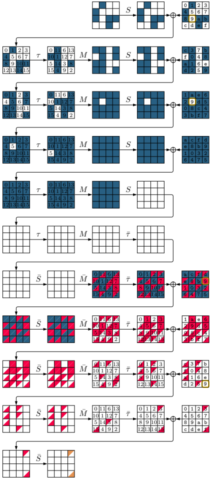
[Lai94] Xuejia Lai. **Higher order derivatives and differential cryptanalysis**. *Communications and cryptography*. Springer, 1994, pp. 227–233.

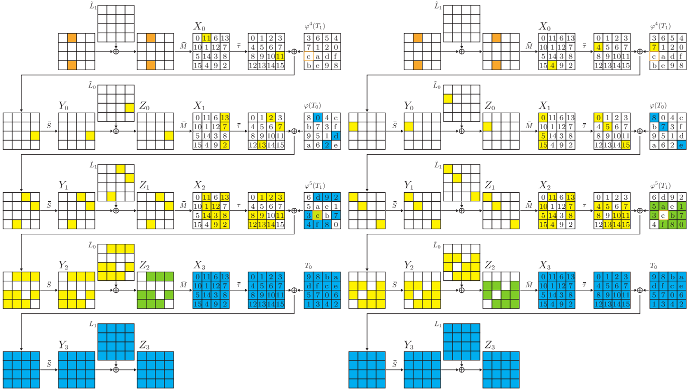
[Sun+15] Bing Sun et al. **Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis**. CRYPTO 2015. Vol. 9215. LNCS. Springer, 2015, pp. 95–115. DOI: 10.1007/978-3-662-47989-6_5.

Bibliography III

[SW12] Yu Sasaki and Lei Wang. **Meet-in-the-Middle Technique for Integral Attacks against Feistel Ciphers**. SAC 2012. Vol. 7707. LNCS. Springer, 2012, pp. 234–251. DOI: 10.1007/978-3-642-35999-6_16.

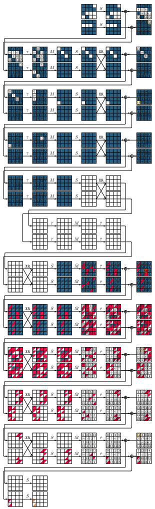
14-Round Integral Attack on QARMAv2-64-128 ($\mathscr{T} = 2$)

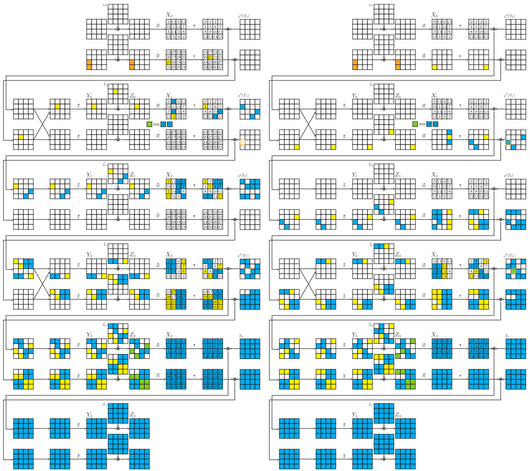




Hosein Hadipour, Yosuke Todo
FSE 2024 - Leuven, Belgium

16-Round Integral Attack on QARMAv2-128-256 ($\mathscr{T} = 2$)





Hosein Hadipour, Yosuke Todo
FSE 2024 - Leuven, Belgium