Related-Tweak Statistical Saturation Cryptanalysis and Its Application on QARMA

Muzhou Li

Key Lab of Cryptologic Technology and Information Security
Ministry of Education, Shandong University, China

Joint work with Kai Hu, Meiqin Wang

March 27, 2019 @ Paris

Outline

Motivation and Contributions

Motivation

- Previous statistical saturation attacks are all implemented under single-key setting
- No public attack model under related-key/tweak setting

Contributions

- New cryptanalytic method: related-key/tweak statistical saturation attack
- New distinguishers are conditional equivalent with those utilized in the key/tweak difference invariant bias (KDIB/TDIB) technique
- Automatically search for KDIB/TDIB distinguishers for key-alternating ciphers
- Related-tweak statistical saturation and TDIB attacks on QARMA

Motivation and Contributions

Motivation

- Previous statistical saturation attacks are all implemented under single-key setting
- No public attack model under related-key/tweak setting

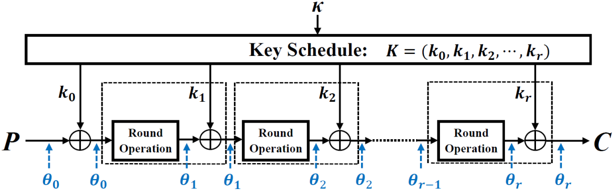
Contributions

- New cryptanalytic method: related-key/tweak statistical saturation attack
- New distinguishers are conditional equivalent with those utilized in the key/tweak difference invariant bias (KDIB/TDIB) technique
- Automatically search for KDIB/TDIB distinguishers for key-alternating ciphers
- Related-tweak statistical saturation and TDIB attacks on `QARMA`

Outline

KDIB Technique in Key-Alternating Ciphers

Key-Alternating Block Ciphers [Daemen & Rijmen]



- $\varepsilon_{\theta_{i-1},\theta_i}$: bias of round i
- Bias of θ under κ: $\varepsilon_\theta(\kappa) = 2^{r-1}(-1)^{\theta^t \cdot K} \prod_{i=1}^{r} \varepsilon_{\theta_{i-1},\theta_i}$
- Bias of linear hull (Γ, Λ) under κ:
  $\varepsilon(\kappa) = \sum_{\theta:\theta_0=\Gamma,\theta_r=\Lambda} (-1)^{\theta^t \cdot K} \varepsilon_\theta(0) = \sum_{\theta:\theta_0=\Gamma,\theta_r=\Lambda} (-1)^{d_\theta + \theta^t \cdot K} \varepsilon_\theta$
- $\theta^t \cdot K = \theta^t \cdot K'$ holds for all θ with $\varepsilon_\theta \neq 0$ in the linear hull (Γ, Λ) (*KDIB condition*) $\Rightarrow \varepsilon(\kappa) = \varepsilon(\kappa')$ [Bogdanov *et al.* @ ASIACRYPT'13]

KDIB Technique in Key-Alternating Ciphers

KDIB Distinguisher

- Many linear hulls (Γ, Λ) + a fixed $\Delta \Rightarrow$ KDIB distinguisher, if there exist κ and κ' with $K \oplus K' = \Delta$ satisfying the KDIB condition for each (Γ, Λ)

TDIB Distinguisher

- KDIB attack $\Rightarrow$ TDIB (tweak difference invariant bias) attack, if tweak is alternated
- Tweak has the same effect on the bias of linear hull with key
- $\theta^t \cdot T = \theta^t \cdot T'$ holds for all θ with $\varepsilon_\theta \neq 0$ in the linear hull (Γ, Λ) (*TDIB condition*) $\Rightarrow \varepsilon(t) = \varepsilon(t')$

KDIB Technique in Key-Alternating Ciphers

KDIB Distinguisher

- Many linear hulls (Γ, Λ) + a fixed $\Delta \Rightarrow$ KDIB distinguisher, if there exist κ and κ' with $K \oplus K' = \Delta$ satisfying the KDIB condition for each (Γ, Λ)

TDIB Distinguisher

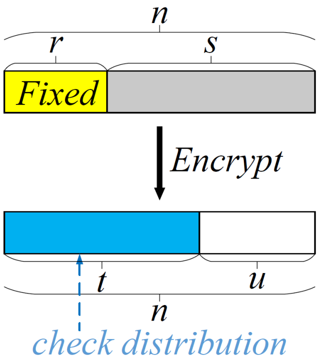
- KDIB attack $\Rightarrow$ TDIB (tweak difference invariant bias) attack, if tweak is alternated
- Tweak has the same effect on the bias of linear hull with key
- $\theta^t \cdot T = \theta^t \cdot T'$ holds for all θ with $\varepsilon_\theta \neq 0$ in the linear hull (Γ, Λ) (*TDIB condition*) $\Rightarrow \varepsilon(t) = \varepsilon(t')$

Outline

Related-Tweak Statistical Saturation Cryptanalysis

Statistical Saturation Cryptanalysis [Collard & Standaert @ CT-RSA'09]

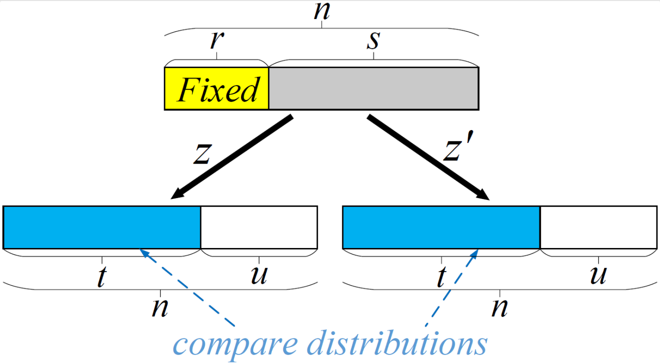
- Fix a part of plaintext bits and take all possible values for the other plaintext bits
- Consider the distribution of a part of the ciphertext value



Related-Tweak Statistical Saturation Cryptanalysis

Related-Key/Tweak Statistical Saturation Cryptanalysis

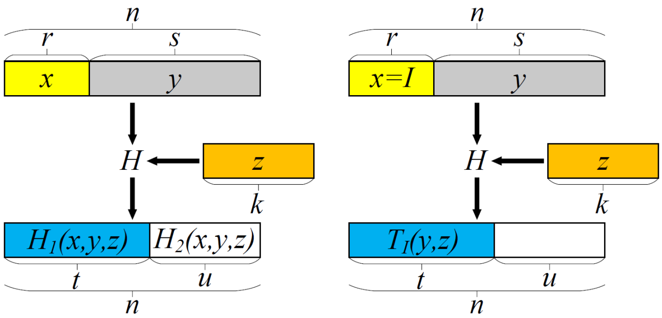
- Fix a part of plaintext bits and take all possible values for the other plaintext bits
- Consider distributions of a part of the ciphertext value under related-key/tweak pairs (z, z'), where $z' = z \oplus \Delta$ and Δ is a fixed value for all possible values of z



Conditional Equivalent Property

Decomposition of the Target Cipher

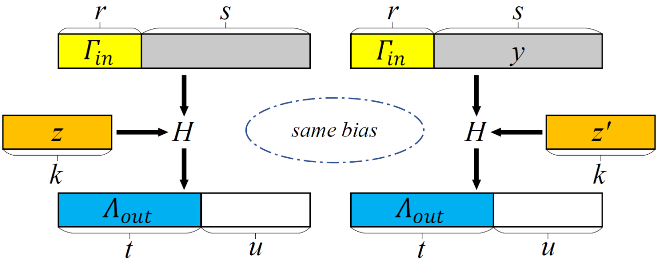
- $H : \mathbb{F}_2^n \times \mathbb{F}_2^k \to \mathbb{F}_2^n$: target cipher with n-bit block and k-bit tweak
- Split the input and output into two parts each:
  $H : \mathbb{F}_2^r \times \mathbb{F}_2^s \times \mathbb{F}_2^k \to \mathbb{F}_2^t \times \mathbb{F}_2^u$, $H(x, y, z) = (H_1(x, y, z), H_2(x, y, z))$
- Define $T_I : \mathbb{F}_2^s \times \mathbb{F}_2^k \to \mathbb{F}_2^t$, $T_I(y, z) = H_1(I, y, z)$



Conditional Equivalent Property

Theorem 1

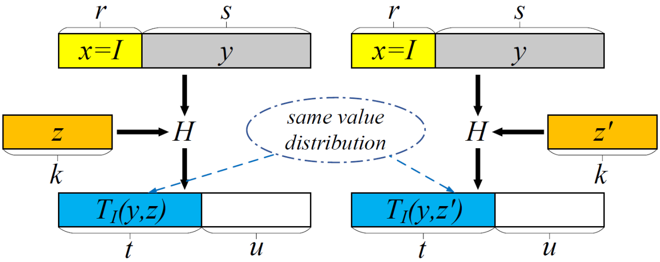
- (Γ, Λ): the linear hull of H with $\Gamma = (\Gamma_{in}, 0)$ and $\Lambda = (\Lambda_{out}, 0)$, where $\Gamma_{in} \in \mathbb{F}_2^r$ and $\Lambda_{out} \in \mathbb{F}_2^t \backslash \{0\}$
- Given a fixed Δ, we have: the bias is invariant under related-tweak pairs $(z, z' = z \oplus \Delta)$ for all possible mask pairs $(\Gamma_{in}, \Lambda_{out})$ $\Longleftrightarrow$ $T_I(y, z)$ has the same value distribution with $T_I(y, z')$



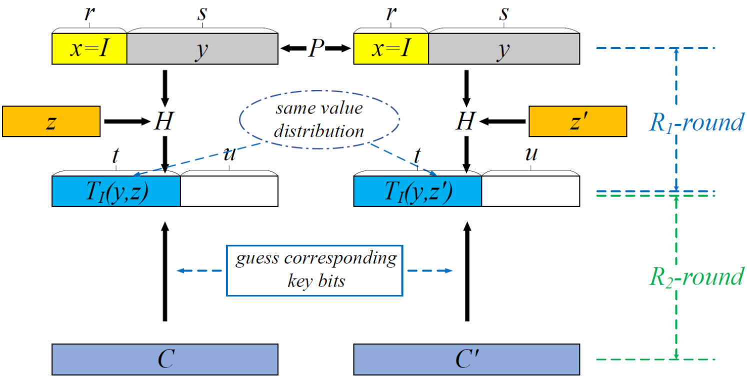
Conditional Equivalent Property

Theorem 1

- (Γ, Λ): the linear hull of H with $\Gamma = (\Gamma_{in}, 0)$ and $\Lambda = (\Lambda_{out}, 0)$, where $\Gamma_{in} \in \mathbb{F}_2^r$ and $\Lambda_{out} \in \mathbb{F}_2^t \backslash \{0\}$
- Given a fixed Δ, we have: the bias is invariant under related-tweak pairs $(z, z' = z \oplus \Delta)$ for all possible mask pairs $(\Gamma_{in}, \Lambda_{out})$ $\Longleftrightarrow$ $T_I(y, z)$ has the same value distribution with $T_I(y, z')$



Key Recovery Attack Using Proposed Method

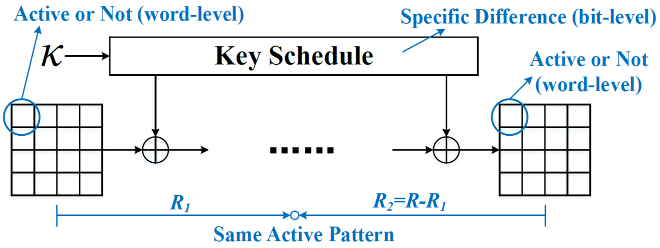


- Reject right key $\alpha_0 = 0$
- Accept wrong key α_1 fulfills
  $\log_2(\alpha_1) \leq (2^t - 1 - t)\, 2^{s+1} - 2^{s(2^t-1)/2}$

Outline

Searching for KDIB Distinguishers with STP

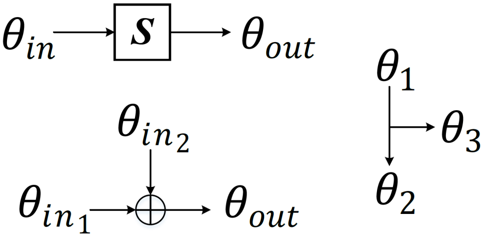
- STP: a decision procedure to confirm if there is a solution to a set of equations
- From previous KDIB attacks (Bogdanov *et al.* @ ASIACRYPT'13), distinguishers were derived at *word-level* for linear masks and *bit-level* for key difference
- Our searching algorithm: *word-level* mask propagation, *bit-level* difference propagation



Searching for KDIB Distinguishers with STP

Part 1. Word-Level Mask Propagation Properties

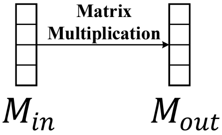
- Substitution: $\theta_{\text{out}} = \theta_{\text{in}}$
- XOR: $\theta_{\text{out}} = \theta_{\text{in}_1} = \theta_{\text{in}_2}$
- Three-Branch: $\theta_3 = 1$, if $\theta_1 = 1$ or $\theta_2 = 1$ holds



Searching for KDIB Distinguishers with STP

Part 1. Word-Level Mask Propagation Properties

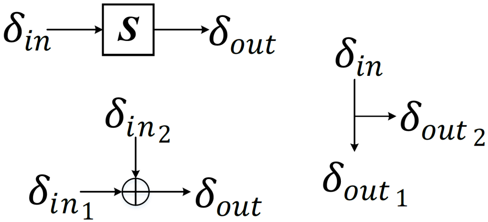
- Deterministic Pattern: M_{out} is unique given M_{in}



- $G = \{M_{in} \mid (M_{in}, M_{out}) \text{ is a deterministic pattern}\}$
- Matrix-Based Linear Layer:
  column-wise active state of input is θ_{in}, column-wise active state of output is θ_{out}. Then $\theta_{out} = M_{out}$ if $\theta_{in} \in G$. Otherwise, $\theta_{out} = (1, 1, 1, 1)^t$

Part 2. Bit-Level Difference Propagation Properties

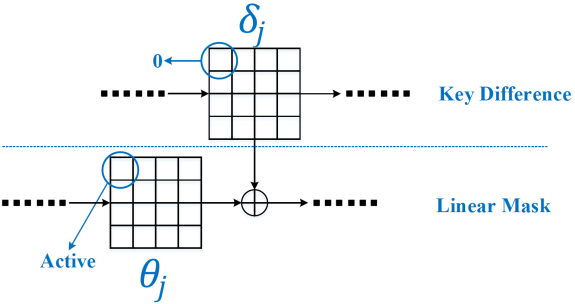
- Substitution: $p = \mathrm{DDT}(\delta_{in}, \delta_{out})$ and $p \neq 0$
- XOR: $\delta_{out} = \delta_{in_1} \oplus \delta_{in_2}$
- Three-Branch: $\delta_{out_1} = \delta_{out_2} = \delta_{in}$



Searching for KDIB Distinguishers with STP

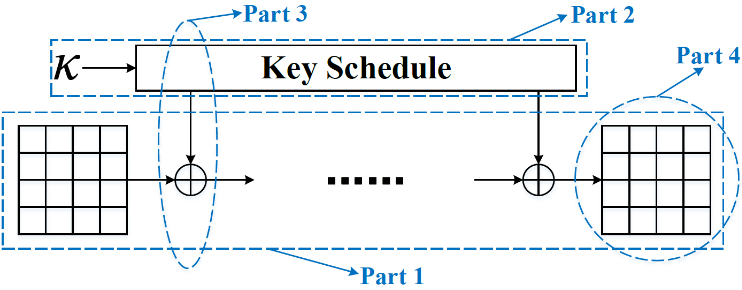
Part 3. Depicting the KDIB Condition

- An r-round linear hull (θ_0, θ_r) and the difference on key $\{\delta_0, \delta_1, \cdots, \delta_r\}$
- KDIB condition: $\oplus_{j=0}^{r} \theta_j \cdot \delta_j = 0$ holds for all possible linear trails $\{\theta_0, \theta_1, \ldots, \theta_r\}$ with $\varepsilon_\theta \neq 0$ in this linear hull
- word-level linear masks $\Rightarrow$ word-level KDIB condition



Part 4. Extra Equations

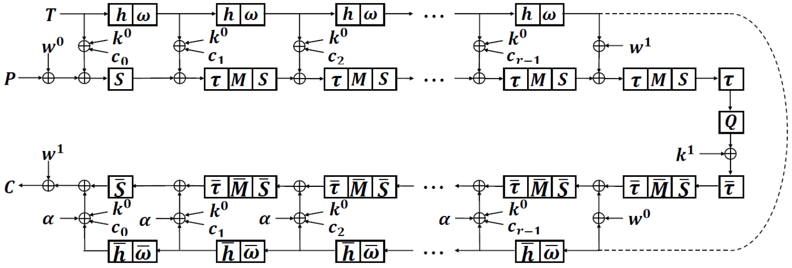
- At least one round key difference is non-zero $\Rightarrow$ exclude trivial solutions
- Describing the active state of input and output mask
- Restricting the total propagation probabilities, for ciphers containing S-box in their key schedule



Outline

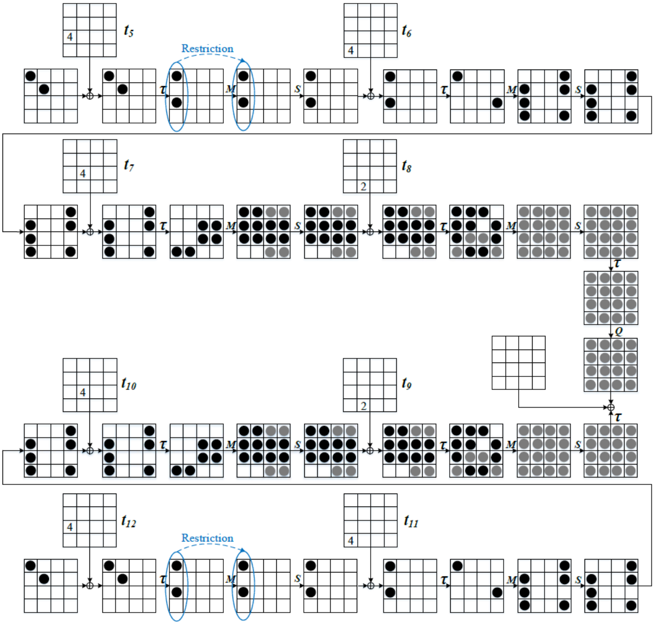
Brief Introduction to QARMA

The Structure of $(2r+2)$-Round QARMA [Avanzi @ ToSC'17]

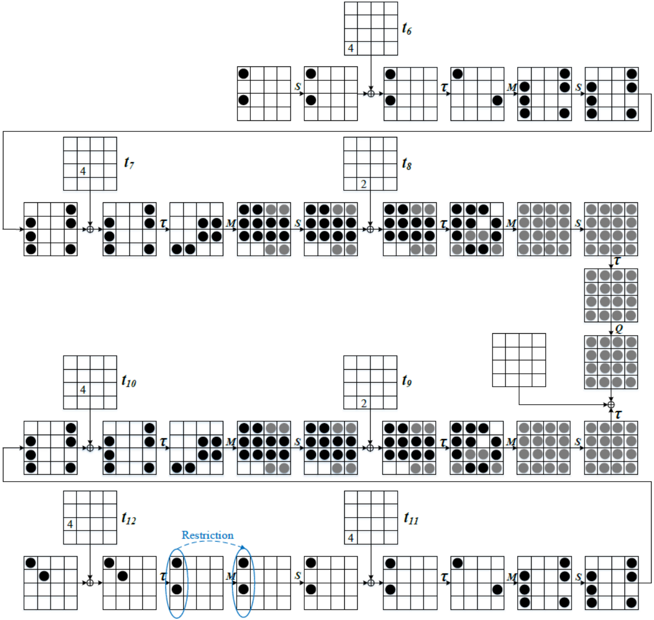


- Two kinds of block sizes: $n = 64$ (QARMA-64), 128 (QARMA-128)
- Key size: $2n$, separated into two parts $w^0 \| k^0$ with same length
- Tweak size: n
- 16 rounds (QARMA-64), 24 rounds (QARMA-128)

One of TDIB Distinguishers for 8-Round QARMA-64



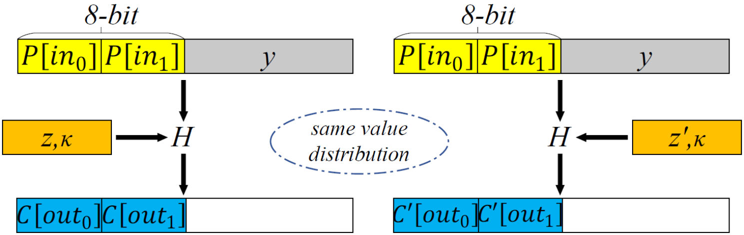
Related-Tweak SS Distinguishers for 8-Round QARMA-64



Convert TDIB into Related-Tweak SS for QARMA-64

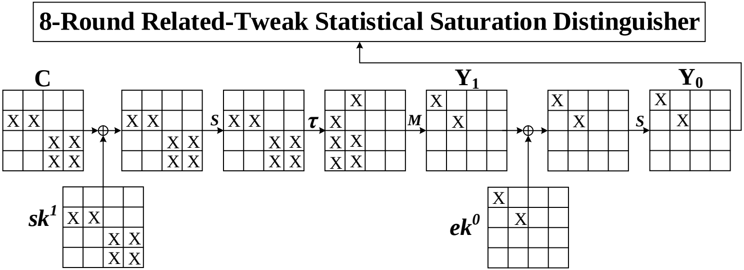
Theorem 3

- (Γ, Λ): linear hull contained in the TDIB distinguishers of the block cipher H
- $\Gamma = (\Gamma[\mathrm{in}_0]||\Gamma[\mathrm{in}_1], 0)$ and $\Lambda = (\Lambda[\mathrm{out}_0]||\Lambda[\mathrm{out}_1], 0)$, where $\Lambda[\mathrm{out}_0] = \Lambda[\mathrm{out}_1]$



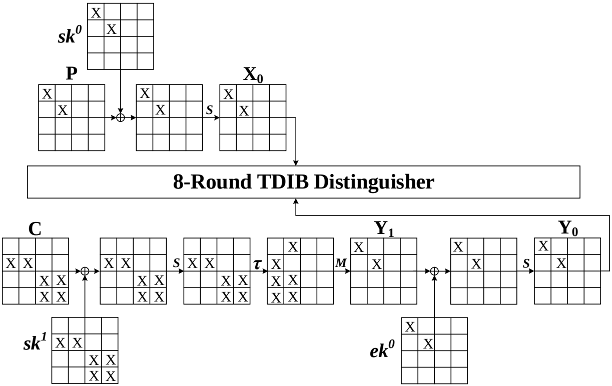
$C[\mathrm{out}_0] \oplus C[\mathrm{out}_1]$ and $C'[\mathrm{out}_0] \oplus C'[\mathrm{out}_1]$: same value distribution

Related-Tweak SS Attacks on 10-Round QARMA-64



Attacks	Rounds	Data	Time	Memory	#tks	Reference
MITM	8	2^{16} CPT	2^{33}	2^{89} 64-bit	1	Li & Jin @ 2018
MITM	9	2^{16} CPT	2^{48}	2^{89} 64-bit	1	Li & Jin @ 2018
RT SS	10	2^{59} CPT	2^{59}	$2^{29.6}$ bits	8	Our Result

TDIB Attacks on 11-Round QARMA-128



Attacks	Rounds	Data	Time	Memory	#tks	Reference
MITM	10	2^{88} CPT	2^{156}	2^{145} 128-bit	1	Li & Jin @ 2018
TDIB	11	$2^{126.1}$ KPT	$2^{126.1}$	2^{71} bits	4	Our Result

Thanks for Your Attention!