Partial Sums Meet FFT: Improved Attack on 6-Round AES

Eurocrypt 2024

Orr Dunkelman Shibam Ghosh Nathan Keller
Gaëtan Leurent Avichai Marmor Victor Mollimard

29th May, 2024

Department of Computer Science, University of Haifa, Israel,
Department of Mathematics, Bar Ilan University, Ramat Gan, Israel,
Inria, Paris, France

אוניברסיטת חיפה
UNIVERSITY OF HAIFA
جامعة حيفا

Table of contents

Plan of this Section

Cryptanalysis Perspective

Distinguisher

Cryptanalysis Perspective

Distinguisher | Key Recovery

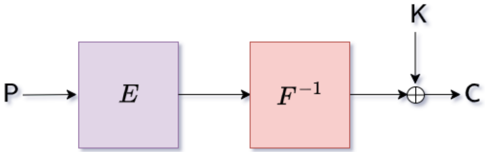
Cryptanalysis Perspective

Searching "Distinguisher" | Key Recovery

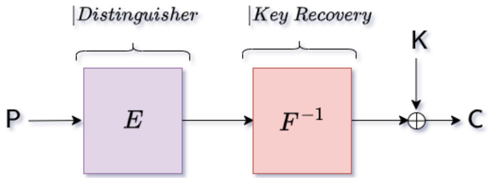
Cryptanalysis Perspective

Searching "Distinguisher" | Key Recovery

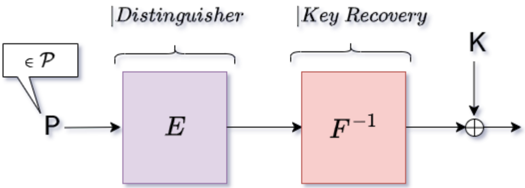
Cryptanalysis Perspective



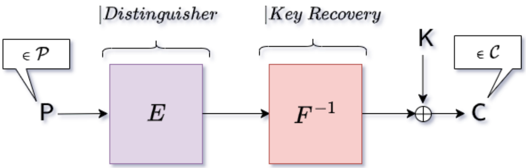
Cryptanalysis Perspective



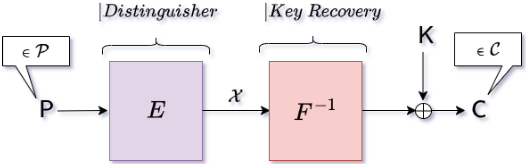
Key Recovery

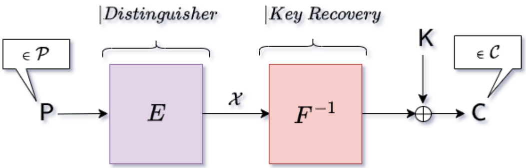


Key Recovery



Key Recovery

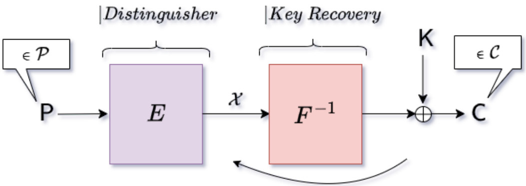




$$\bigoplus_{X \in \mathcal{X}} X = \bigoplus_{P \in \mathcal{P}} E(P) = 0$$

Integral/Zero-Sum Distinguisher

Key Recovery



$$\bigoplus_{X \in \mathcal{X}} X = \bigoplus_{P \in \mathcal{P}} E(P) = 0 = \bigoplus_{C \in \mathcal{C}} F(C \oplus K), \text{ For the right key } K$$

Integral/Zero-Sum Distinguisher

Key Recovery Programme

procedure FOO($\mathcal{C} \subseteq \{0,1\}^m$ of size 2^m)

for $\mathsf{K} \in \{0,1\}^m$ **do**

$\mathbf{S} = \mathbf{0}$

for $\mathsf{C} \in \mathcal{C}$ **do**

$\mathbf{S} = \mathbf{S} \oplus F(\mathsf{C} \oplus \mathsf{K})$

if $\mathbf{S} \neq \mathbf{0}$ **then**

Discard K

Key Recovery Programme

procedure $\text{FOO}(\mathcal{C} \subseteq \{0,1\}^m$ of size $2^m)$
    for $\mathsf{K} \in \{0,1\}^m$ **do**
        $\mathbf{S} = \mathbf{0}$
        for $\mathsf{C} \in \mathcal{C}$ **do**
            $\mathbf{S} = \mathbf{S} \oplus F(\mathsf{C} \oplus \mathsf{K})$
        if $\mathbf{S} \neq \mathbf{0}$ **then**
            Discard K

procedure $\text{BAR}(\mathcal{C} \subseteq \{0,1\}^m$ of size $2^m)$
    for $\mathsf{K} \in \{0,1\}^m$ **do**
        $\mathbf{S} = \mathbf{0}$
        for $\mathsf{C} \in \{0,1\}^m$ **do**
            $\mathbf{S} = \mathbf{S} \oplus F(\mathsf{C} \oplus \mathsf{K}) G_{\mathcal{C}}(\mathsf{C})$
        if $\mathbf{S} \neq \mathbf{0}$ **then**
            Discard K

Key Recovery Programme

procedure $\textsc{Foo}(\mathcal{C} \subseteq \{0,1\}^m$ of size $2^m)$
  for $K \in \{0,1\}^m$ **do**
    $\mathbf{S} = \mathbf{0}$
    for $C \in \mathcal{C}$ **do**
      $\mathbf{S} = \mathbf{S} \oplus F(C \oplus K)$
    if $\mathbf{S} \neq \mathbf{0}$ **then**
      Discard K

procedure $\textsc{Bar}(\mathcal{C} \subseteq \{0,1\}^m$ of size $2^m)$
  for $K \in \{0,1\}^m$ **do**
    $\mathbf{S} = \mathbf{0}$
    for $C \in \{0,1\}^m$ **do**
      $\mathbf{S} = \mathbf{S} \oplus F(C \oplus K) G_{\mathcal{C}}(C)$
    if $\mathbf{S} \neq \mathbf{0}$ **then**
      Discard K

$$G_{\mathcal{C}}(C) = \begin{cases} 1, & \text{if occurrences of } C \text{ is odd in } \mathcal{C} \\ 0, & \text{if occurrences of } C \text{ is even in } \mathcal{C} \end{cases}$$

Key Recovery Programme

procedure $\text{FOO}(\mathcal{C} \subseteq \{0,1\}^m$ of size $2^m)$
  for K $\in \{0,1\}^m$ **do**
    S $=$ **0**
    for C $\in \mathcal{C}$ **do**
      S $=$ **S** $\oplus F(\mathsf{C} \oplus \mathsf{K})$
    if S $\neq$ 0 then
      Discard K

procedure $\text{BAR}(\mathcal{C} \subseteq \{0,1\}^m$ of size $2^m)$
  for K $\in \{0,1\}^m$ **do**
    S $=$ **0**
    for C $\in \{0,1\}^m$ **do**
      S $=$ **S** $\oplus F(\mathsf{C} \oplus \mathsf{K}) G_{\mathcal{C}}(\mathsf{C})$
    if S $\neq$ 0 then
      Discard K

BAR $\equiv$ Convolution for each K,

$$F * G(\mathsf{K}) = \bigoplus_{\mathsf{C} \in \{0,1\}^m} F(\mathsf{C} \oplus \mathsf{K}) G(\mathsf{C})$$

The BAR matrix

$$F * G(K) = \bigoplus_{C \in \{0,1\}^m} F(C \oplus K) G(C)$$

$$\begin{bmatrix} F(0\oplus 0) & F(0\oplus 1) & F(0\oplus 2) & F(0\oplus 3) & F(0\oplus 4) & F(0\oplus 5) & F(0\oplus 6) & F(0\oplus 7) \\ F(1\oplus 0) & F(1\oplus 1) & F(1\oplus 2) & F(1\oplus 3) & F(1\oplus 4) & F(1\oplus 5) & F(1\oplus 6) & F(1\oplus 7) \\ F(2\oplus 0) & F(2\oplus 1) & F(2\oplus 2) & F(2\oplus 3) & F(2\oplus 4) & F(2\oplus 5) & F(2\oplus 6) & F(2\oplus 7) \\ F(3\oplus 0) & F(3\oplus 1) & F(3\oplus 2) & F(3\oplus 3) & F(3\oplus 4) & F(3\oplus 5) & F(3\oplus 6) & F(3\oplus 7) \\ F(4\oplus 0) & F(4\oplus 1) & F(4\oplus 2) & F(4\oplus 3) & F(4\oplus 4) & F(4\oplus 5) & F(4\oplus 6) & F(4\oplus 7) \\ F(5\oplus 0) & F(5\oplus 1) & F(5\oplus 2) & F(5\oplus 3) & F(5\oplus 4) & F(5\oplus 5) & F(5\oplus 6) & F(5\oplus 7) \\ F(6\oplus 0) & F(6\oplus 1) & F(6\oplus 2) & F(6\oplus 3) & F(6\oplus 4) & F(6\oplus 5) & F(6\oplus 6) & F(6\oplus 7) \\ F(7\oplus 0) & F(7\oplus 1) & F(7\oplus 2) & F(7\oplus 3) & F(7\oplus 4) & F(7\oplus 5) & F(7\oplus 6) & F(7\oplus 7) \end{bmatrix} \times \begin{bmatrix} G(0) \\ G(1) \\ G(2) \\ G(3) \\ G(4) \\ G(5) \\ G(6) \\ G(7) \end{bmatrix}$$

The BAR matrix

$$F * G(K) = \bigoplus_{C \in \{0,1\}^m} F(C \oplus K) G(C)$$

$$\begin{bmatrix} F(0\oplus 0) & F(0\oplus 1) & F(0\oplus 2) & F(0\oplus 3) & F(0\oplus 4) & F(0\oplus 5) & F(0\oplus 6) & F(0\oplus 7) \\ F(1\oplus 0) & F(1\oplus 1) & F(1\oplus 2) & F(1\oplus 3) & F(1\oplus 4) & F(1\oplus 5) & F(1\oplus 6) & F(1\oplus 7) \\ F(2\oplus 0) & F(2\oplus 1) & F(2\oplus 2) & F(2\oplus 3) & F(2\oplus 4) & F(2\oplus 5) & F(2\oplus 6) & F(2\oplus 7) \\ F(3\oplus 0) & F(3\oplus 1) & F(3\oplus 2) & F(3\oplus 3) & F(3\oplus 4) & F(3\oplus 5) & F(3\oplus 6) & F(3\oplus 7) \\ F(4\oplus 0) & F(4\oplus 1) & F(4\oplus 2) & F(4\oplus 3) & F(4\oplus 4) & F(4\oplus 5) & F(4\oplus 6) & F(4\oplus 7) \\ F(5\oplus 0) & F(5\oplus 1) & F(5\oplus 2) & F(5\oplus 3) & F(5\oplus 4) & F(5\oplus 5) & F(5\oplus 6) & F(5\oplus 7) \\ F(6\oplus 0) & F(6\oplus 1) & F(6\oplus 2) & F(6\oplus 3) & F(6\oplus 4) & F(6\oplus 5) & F(6\oplus 6) & F(6\oplus 7) \\ F(7\oplus 0) & F(7\oplus 1) & F(7\oplus 2) & F(7\oplus 3) & F(7\oplus 4) & F(7\oplus 5) & F(7\oplus 6) & F(7\oplus 7) \end{bmatrix} \times \begin{bmatrix} G(0) \\ G(1) \\ G(2) \\ G(3) \\ G(4) \\ G(5) \\ G(6) \\ G(7) \end{bmatrix}$$

The BAR matrix

$$\begin{bmatrix} F(0\oplus 0) & F(0\oplus 1) & F(0\oplus 2) & F(0\oplus 3) & F(0\oplus 4) & F(0\oplus 5) & F(0\oplus 6) & F(0\oplus 7) \\ F(1\oplus 0) & F(1\oplus 1) & F(1\oplus 2) & F(1\oplus 3) & F(1\oplus 4) & F(1\oplus 5) & F(1\oplus 6) & F(1\oplus 7) \\ F(2\oplus 0) & F(2\oplus 1) & F(2\oplus 2) & F(2\oplus 3) & F(2\oplus 4) & F(2\oplus 5) & F(2\oplus 6) & F(2\oplus 7) \\ F(3\oplus 0) & F(3\oplus 1) & F(3\oplus 2) & F(3\oplus 3) & F(3\oplus 4) & F(3\oplus 5) & F(3\oplus 6) & F(3\oplus 7) \\ F(4\oplus 0) & F(4\oplus 1) & F(4\oplus 2) & F(4\oplus 3) & F(4\oplus 4) & F(4\oplus 5) & F(4\oplus 6) & F(4\oplus 7) \\ F(5\oplus 0) & F(5\oplus 1) & F(5\oplus 2) & F(5\oplus 3) & F(5\oplus 4) & F(5\oplus 5) & F(5\oplus 6) & F(5\oplus 7) \\ F(6\oplus 0) & F(6\oplus 1) & F(6\oplus 2) & F(6\oplus 3) & F(6\oplus 4) & F(6\oplus 5) & F(6\oplus 6) & F(6\oplus 7) \\ F(7\oplus 0) & F(7\oplus 1) & F(7\oplus 2) & F(7\oplus 3) & F(7\oplus 4) & F(7\oplus 5) & F(7\oplus 6) & F(7\oplus 7) \end{bmatrix}_{8\times 8}$$

אוניברסיטת חיפה
UNIVERSITY OF HAIFA
جامعة حيفا

The BAR matrix

$$\begin{bmatrix} F(0\oplus 0) & F(0\oplus 1) & F(0\oplus 2) & F(0\oplus 3) & F(0\oplus 4) & F(0\oplus 5) & F(0\oplus 6) & F(0\oplus 7) \\ F(1\oplus 0) & F(1\oplus 1) & F(1\oplus 2) & F(1\oplus 3) & F(1\oplus 4) & F(1\oplus 5) & F(1\oplus 6) & F(1\oplus 7) \\ F(2\oplus 0) & F(2\oplus 1) & F(2\oplus 2) & F(2\oplus 3) & F(2\oplus 4) & F(2\oplus 5) & F(2\oplus 6) & F(2\oplus 7) \\ F(3\oplus 0) & F(3\oplus 1) & F(3\oplus 2) & F(3\oplus 3) & F(3\oplus 4) & F(3\oplus 5) & F(3\oplus 6) & F(3\oplus 7) \\ F(4\oplus 0) & F(4\oplus 1) & F(4\oplus 2) & F(4\oplus 3) & F(4\oplus 4) & F(4\oplus 5) & F(4\oplus 6) & F(4\oplus 7) \\ F(5\oplus 0) & F(5\oplus 1) & F(5\oplus 2) & F(5\oplus 3) & F(5\oplus 4) & F(5\oplus 5) & F(5\oplus 6) & F(5\oplus 7) \\ F(6\oplus 0) & F(6\oplus 1) & F(6\oplus 2) & F(6\oplus 3) & F(6\oplus 4) & F(6\oplus 5) & F(6\oplus 6) & F(6\oplus 7) \\ F(7\oplus 0) & F(7\oplus 1) & F(7\oplus 2) & F(7\oplus 3) & F(7\oplus 4) & F(7\oplus 5) & F(7\oplus 6) & F(7\oplus 7) \end{bmatrix}_{8\times 8}$$

The BAR matrix

$$\begin{bmatrix} F(0\oplus 0) & F(0\oplus 1) & F(0\oplus 2) & F(0\oplus 3) & F(0\oplus 4) & F(0\oplus 5) & F(0\oplus 6) & F(0\oplus 7) \\ F(1\oplus 0) & F(1\oplus 1) & F(1\oplus 2) & F(1\oplus 3) & F(1\oplus 4) & F(1\oplus 5) & F(1\oplus 6) & F(1\oplus 7) \\ F(2\oplus 0) & F(2\oplus 1) & F(2\oplus 2) & F(2\oplus 3) & F(2\oplus 4) & F(2\oplus 5) & F(2\oplus 6) & F(2\oplus 7) \\ F(3\oplus 0) & F(3\oplus 1) & F(3\oplus 2) & F(3\oplus 3) & F(3\oplus 4) & F(3\oplus 5) & F(3\oplus 6) & F(3\oplus 7) \\ F(4\oplus 0) & F(4\oplus 1) & F(4\oplus 2) & F(4\oplus 3) & F(4\oplus 4) & F(4\oplus 5) & F(4\oplus 6) & F(4\oplus 7) \\ F(5\oplus 0) & F(5\oplus 1) & F(5\oplus 2) & F(5\oplus 3) & F(5\oplus 4) & F(5\oplus 5) & F(5\oplus 6) & F(5\oplus 7) \\ F(6\oplus 0) & F(6\oplus 1) & F(6\oplus 2) & F(6\oplus 3) & F(6\oplus 4) & F(6\oplus 5) & F(6\oplus 6) & F(6\oplus 7) \\ F(7\oplus 0) & F(7\oplus 1) & F(7\oplus 2) & F(7\oplus 3) & F(7\oplus 4) & F(7\oplus 5) & F(7\oplus 6) & F(7\oplus 7) \end{bmatrix}_{8\times 8}$$

The BAR matrix

$$\begin{bmatrix} F(0\oplus 0) & F(0\oplus 1) & F(0\oplus 2) & F(0\oplus 3) & F(0\oplus 4) & F(0\oplus 5) & F(0\oplus 6) & F(0\oplus 7) \\ F(1\oplus 0) & F(1\oplus 1) & F(1\oplus 2) & F(1\oplus 3) & F(1\oplus 4) & F(1\oplus 5) & F(1\oplus 6) & F(1\oplus 7) \\ F(2\oplus 0) & F(2\oplus 1) & F(2\oplus 2) & F(2\oplus 3) & F(2\oplus 4) & F(2\oplus 5) & F(2\oplus 6) & F(2\oplus 7) \\ F(3\oplus 0) & F(3\oplus 1) & F(3\oplus 2) & F(3\oplus 3) & F(3\oplus 4) & F(3\oplus 5) & F(3\oplus 6) & F(3\oplus 7) \\ F(4\oplus 0) & F(4\oplus 1) & F(4\oplus 2) & F(4\oplus 3) & F(4\oplus 4) & F(4\oplus 5) & F(4\oplus 6) & F(4\oplus 7) \\ F(5\oplus 0) & F(5\oplus 1) & F(5\oplus 2) & F(5\oplus 3) & F(5\oplus 4) & F(5\oplus 5) & F(5\oplus 6) & F(5\oplus 7) \\ F(6\oplus 0) & F(6\oplus 1) & F(6\oplus 2) & F(6\oplus 3) & F(6\oplus 4) & F(6\oplus 5) & F(6\oplus 6) & F(6\oplus 7) \\ F(7\oplus 0) & F(7\oplus 1) & F(7\oplus 2) & F(7\oplus 3) & F(7\oplus 4) & F(7\oplus 5) & F(7\oplus 6) & F(7\oplus 7) \end{bmatrix}$$

Properties of BAR matrix $\mathcal{M}_m$

- $\mathcal{M}_m = \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m)$, $\mathcal{H}_m[i,j] = \frac{1}{2^{m/2}}(-1)^{i \cdot j}$

Properties of BAR matrix $\mathcal{M}_m$

- $\mathcal{M}_m = \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m)$, $\mathcal{H}_m[i,j] = \frac{1}{2^{m/2}}(-1)^{i \cdot j}$

$$\mathcal{H}_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \mathcal{H}_2 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Properties of BAR matrix $\mathcal{M}_m$

- $\mathcal{M}_m = \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m)$, $\mathcal{H}_m[i,j] = \frac{1}{2^{m/2}}(-1)^{i \cdot j}$

$$\mathcal{H}_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \mathcal{H}_2 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$\text{In General } \mathcal{H}_m = \frac{1}{2^{m/2}}\begin{bmatrix} \mathcal{H}_{m-1} & \mathcal{H}_{m-1} \\ \mathcal{H}_{m-1} & -\mathcal{H}_{m-1} \end{bmatrix}$$

Properties of BAR matrix $\mathcal{M}_m$

- $\mathcal{M}_m = \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m)$, $\mathcal{H}_m[i,j] = \frac{1}{2^{m/2}}(-1)^{i \cdot j}$

$$\mathcal{H}_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \mathcal{H}_2 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$\text{In General } \mathcal{H}_m = \frac{1}{2^{m/2}} \begin{bmatrix} \mathcal{H}_{m-1} & \mathcal{H}_{m-1} \\ \mathcal{H}_{m-1} & -\mathcal{H}_{m-1} \end{bmatrix}$$

- FHT: A divide-and-conquer algorithm, complexity $= \mathcal{O}(m2^m)$

Properties of BAR matrix $\mathcal{M}_m$

- $\mathcal{M}_m = \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m)$, $\mathcal{H}_m[i,j] = \frac{1}{2^{m/2}}(-1)^{i \cdot j}$

UNIVERSITY OF HAIFA אוניברסיטת חיפה جامعة حيفا

Properties of BAR matrix $\mathcal{M}_m$

- $\mathcal{M}_m = \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m)$, $\mathcal{H}_m[i,j] = \frac{1}{2^{m/2}}(-1)^{i \cdot j}$
- $\Delta = \mathcal{H}_m \times \mathcal{M}_m^0$, where $\mathcal{M}_m^0$ is the first column of $\mathcal{M}_m$

Properties of BAR matrix $\mathcal{M}_m$

- $\mathcal{M}_m = \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m)$, $\mathcal{H}_m[i,j] = \frac{1}{2^{m/2}}(-1)^{i \cdot j}$
- $\Delta = \mathcal{H}_m \times \mathcal{M}_m^0$, where $\mathcal{M}_m^0$ is the first column of $\mathcal{M}_m$

$$\begin{aligned}\mathcal{M}_m \times \mathcal{C} &= \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m) \times \mathcal{C} \\ &= \frac{1}{2^m}(\mathcal{H}_m \times ((\mathcal{H}_m \times \mathcal{M}_m^0) \star (\mathcal{H}_m \times \mathcal{C})))\end{aligned}$$

Properties of BAR matrix $\mathcal{M}_m$

- $\mathcal{M}_m = \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m)$, $\mathcal{H}_m[i,j] = \frac{1}{2^{m/2}}(-1)^{i \cdot j}$
- $\Delta = \mathcal{H}_m \times \mathcal{M}_m^0$, where $\mathcal{M}_m^0$ is the first column of $\mathcal{M}_m$

$$\begin{aligned}\mathcal{M}_m \times \mathcal{C} &= \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m) \times \mathcal{C} \\ &= \frac{1}{2^m}(\mathcal{H}_m \times ((\mathcal{H}_m \times \mathcal{M}_m^0) \star (\mathcal{H}_m \times \mathcal{C})))\end{aligned}$$

- Complexity: $2^{2m} \to 4m2^m$

Properties of BAR matrix $\mathcal{M}_m$

- $\mathcal{M}_m = \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m)$, $\mathcal{H}_m[i,j] = \frac{1}{2^{m/2}}(-1)^{i \cdot j}$
- $\Delta = \mathcal{H}_m \times \mathcal{M}_m^0$, where $\mathcal{M}_m^0$ is the first column of $\mathcal{M}_m$

$$\begin{aligned}\mathcal{M}_m \times \mathcal{C} &= \frac{1}{2^m}(\mathcal{H}_m \times \Delta \times \mathcal{H}_m) \times \mathcal{C} \\ &= \frac{1}{2^m}(\mathcal{H}_m \times ((\mathcal{H}_m \times \mathcal{M}_m^0) \star (\mathcal{H}_m \times \mathcal{C})))\end{aligned}$$

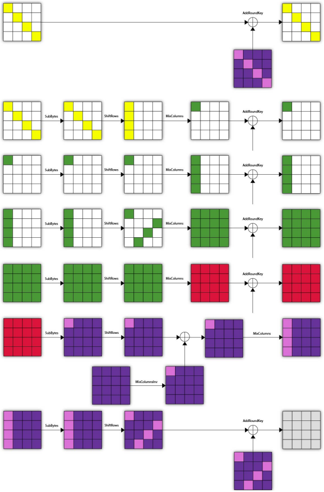
- Complexity: $2^{2m} \rightarrow 4m2^m$
- For $m = 32$: $2^{64} \rightarrow 2^{39}$

UNIVERSITY OF HAIFA

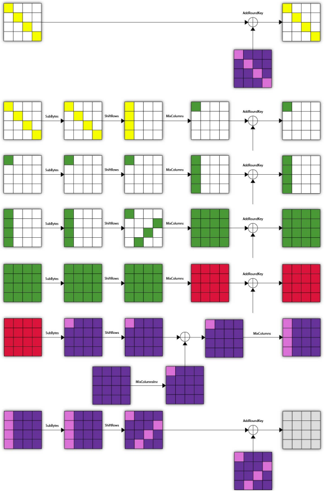
Plan of this Section

1. Motivation
2. Integral attack on AES
3. Partial Sums Meet FFT
4. Results and Conclusion

Integral Attack On AES



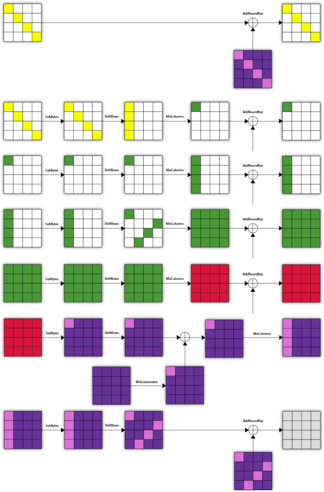
Integral Attack On AES



$$\chi(\mathrm{K}, \mathrm{C}) = S(\mathrm{K}_4 \oplus S_3(\mathrm{K}_3 \oplus \mathrm{C}_3) \oplus S_2(\mathrm{K}_2 \oplus \mathrm{C}_2)$$
$$\oplus S_1(\mathrm{K}_1 \oplus \mathrm{C}_1) \oplus S_0(\mathrm{K}_0 \oplus \mathrm{C}_0))$$

1. Naive Complexity: $c \times 2^{72}$

Integral Attack On AES



$$\chi(\mathrm{K}, \mathrm{C}) = S(\mathrm{K}_4 \oplus S_3(\mathrm{K}_3 \oplus \mathrm{C}_3) \oplus S_2(\mathrm{K}_2 \oplus \mathrm{C}_2) \oplus S_1(\mathrm{K}_1 \oplus \mathrm{C}_1) \oplus S_0(\mathrm{K}_0 \oplus \mathrm{C}_0))$$

1. Naive Complexity: $c \times 2^{72}$
2. FHT [Todo et al. [TA14]]: For each fixed K_4,

$$\chi(\mathrm{K}, \mathrm{C}) = S_{\mathrm{K}_4}(S_3(\mathrm{K}_3 \oplus \mathrm{C}_3) \oplus S_2(\mathrm{K}_2 \oplus \mathrm{C}_2) \oplus S_1(\mathrm{K}_1 \oplus \mathrm{C}_1) \oplus S_0(\mathrm{K}_0 \oplus \mathrm{C}_0))$$

The Problem with Finite Field Arithmetic

- $F * G(k) = \bigoplus_{x} F(x \oplus k)g(x)$ VS $F * G(k) = \sum_{x} F(x \oplus k)g(x)$
- We need functions whose output is an integer and not an element of $\mathbb{F}_2^8$

The Problem with Finite Field Arithmetic

- $F * G(k) = \bigoplus_{x} F(x \oplus k)g(x)$ VS $F * G(k) = \sum_{x} F(x \oplus k)g(x)$
- We need functions whose output is an integer and not an element of $\mathbb{F}_2^8$
- Todo et al. [TA14] proposed to consider 8 outputs separately
- $F(\mathsf{K} \oplus \mathsf{C}) = (F^0(\mathsf{K} \oplus \mathsf{C}), ..., F^7(\mathsf{K} \oplus \mathsf{C}))$
- and compute convolution for each F^i separately

אוניברסיטת חיפה
UNIVERSITY OF HAIFA
جامعة حيفا

The Problem with Finite Field Arithmetic

- $F * G(k) = \bigoplus_x F(x \oplus k)g(x)$ VS $F * G(k) = \sum_x F(x \oplus k)g(x)$
- We need functions whose output is an integer and not an element of $\mathbb{F}_2^8$
- Todo et al. [TA14] proposed to consider 8 outputs separately
- $F(\mathrm{K} \oplus \mathrm{C}) = (F^0(\mathrm{K} \oplus \mathrm{C}), \ldots, F^7(\mathrm{K} \oplus \mathrm{C}))$
- and compute convolution for each F^i separately
- So we need to run the algorithm for 8 times.

Complexity: Time $c \times 2^8 \times 8 \times 2^{39}$ and Memory $f \times 2^{32}$

אוניברסיטת חיפה
UNIVERSITY OF HAIFA
جامعة حيفا

Partial Sum Technique [FKL+00]

$$\chi(K \oplus C) = S(K_4 \oplus S_3(K_3 \oplus C_3) \oplus S_2(K_2 \oplus C_2) \oplus S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0)))$$

- Guess (K_1, K_0) and compute $S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0)$

Partial Sum Technique [FKL+00]

$$\chi(K \oplus C) = S(K_4 \oplus S_3(K_3 \oplus C_3) \oplus S_2(K_2 \oplus C_2) \oplus S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0)))$$

- Guess (K_1, K_0) and compute $S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0)$

Declare an empty bit-array A_1 of size 2^{24}

for $c_0, c_1, c_2, c_3 \in \{0,1\}^{32}$ **do**

$a_1 \leftarrow (S_0(C_0 \oplus K_0) \oplus S_1(C_1 \oplus K_1)) G_{\mathcal{C}}(C_0, C_1, C_2, C_3)$

$A_1[a_1, C_2, C_3] \leftarrow A_1[a_1, C_2, C_3] \oplus 1$

Partial Sum Technique [FKL+00]

$$\chi(K \oplus C) = S(K_4 \oplus S_3(K_3 \oplus C_3) \oplus S_2(K_2 \oplus C_2) \oplus S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0)))$$

- Guess (K_1, K_0) and compute $S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0)$

Declare an empty bit-array A_1 of size 2^{24}

for $c_0, c_1, c_2, c_3 \in \{0,1\}^{32}$ **do**

$a_1 \leftarrow (S_0(C_0 \oplus K_0) \oplus S_1(C_1 \oplus K_1)) G_{\mathcal{C}}(C_0, C_1, C_2, C_3)$

$A_1[a_1, C_2, C_3] \leftarrow A_1[a_1, C_2, C_3] \oplus 1$

$$\chi(K \oplus C) = S(K_4 \oplus S_3(K_3 \oplus C_3) \oplus S_2(K_2 \oplus C_2) \oplus a_1)$$

Complexity: $2^{16} * 2^{32}$

Partial Sum Technique [FKL+00] at a Glance

$$\mathsf{K}_4 \oplus S_3(\mathsf{K}_3 + \mathsf{C}_3) \oplus S_2(\mathsf{K}_2 + \mathsf{C}_2) \oplus \underbrace{S_1(\mathsf{K}_1 + \mathsf{C}_1) \oplus S_0(\mathsf{K}_0 + \mathsf{C}_0)}_{2^{48}}$$

$$\mathsf{K}_4 \oplus S_3(\mathsf{K}_3 + \mathsf{C}_3) \oplus \underbrace{S_2(\mathsf{K}_2 + \mathsf{C}_2) \oplus A_1}_{2^{48}}$$

$$\mathsf{K}_4 \oplus \underbrace{S_3(\mathsf{K}_3 + \mathsf{C}_3) \oplus A_2}_{2^{48}}$$

$$\underbrace{\mathsf{K}_4 \oplus A_3}_{2^{48}}$$

Partial Sum Technique [FKL+00] at a Glance

$$K_4 \oplus S_3(K_3 + C_3) \oplus S_2(K_2 + C_2) \oplus \underbrace{S_1(K_1 + C_1) \oplus S_0(K_0 + C_0)}_{2^{48}}$$

$$K_4 \oplus S_3(K_3 + C_3) \oplus \underbrace{S_2(K_2 + C_2) \oplus A_1}_{2^{48}}$$

$$K_4 \oplus \underbrace{S_3(K_3 + C_3) \oplus A_2}_{2^{48}}$$

$$\underbrace{K_4 \oplus A_3}_{2^{48}}$$

Complexity: Time $c \times 2^{50}$ and Memory 2^{24}

Plan of this Section

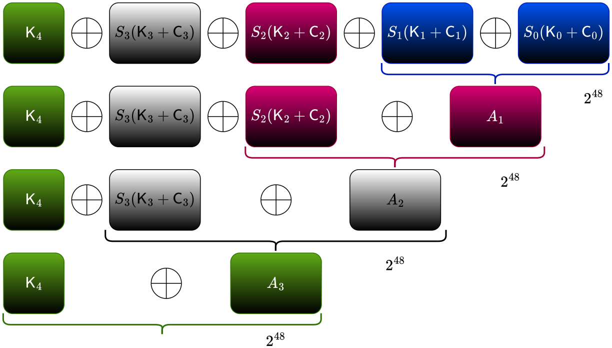
1. Motivation
2. Integral attack on AES
3. Partial Sums Meet FFT
4. Results and Conclusion

Basic Idea

- We follow the general structure of the partial sums attack
- Replace each partial sum with FFT
- However, rearrange the steps to make it FFT compatible
- Rearrange the steps again to reduce memory complexity

Partial Sums Meet FFT

$$\chi(K \oplus C) = S(K_4 \oplus S_3(K_3 \oplus C_3) \oplus S_2(K_2 \oplus C_2) \oplus S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0)))$$



Partial Sums Meet FFT

$$\chi(K \oplus C) = S(K_4 \oplus S_3(K_3 \oplus C_3) \oplus S_2(K_2 \oplus C_2) \oplus S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0)))$$

$$\underbrace{S_1(K_1 + C_1) \bigoplus S_0(K_0 + C_0)}_{A_1}$$

Partial Sums Meet FFT

$$\chi(K \oplus C) = S(K_4 \oplus S_3(K_3 \oplus C_3) \oplus S_2(K_2 \oplus C_2) \oplus S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0)))$$

$$\underbrace{\boxed{S_1(K_1 + C_1)} \bigoplus \boxed{S_0(K_0 + C_0)}}_{\boxed{A_1}}$$

$A_1 = [\,]$ of size $2^{16} \times 2^{24}$; ▷ 2^{40} memory

for all $(a_1, C_2, C_3) \in \{0,1\}^{24}$ **do**

  for all $(K_0, K_1) \in \{0,1\}^{16}$ **do**

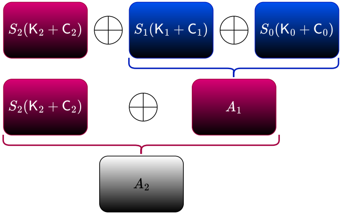
    $A_1[K_0, K_1][a_1, C_2, C_3] \leftarrow \bigoplus_{C_0, C_1} A[C_0, C_1, C_2, C_3] \cdot \mathbb{1}(S_0(C_0 \oplus K_0) \oplus S_1(C_1 \oplus K_1) = a_1)$

Partial Sums Meet FFT

$$S_2(\mathsf{K}_2+\mathsf{C}_2) \oplus \underbrace{S_1(\mathsf{K}_1+\mathsf{C}_1) \oplus S_0(\mathsf{K}_0+\mathsf{C}_0)}_{A_1}$$

$$\underbrace{S_2(\mathsf{K}_2+\mathsf{C}_2) \oplus A_1}_{A_2}$$

Partial Sums Meet FFT



for all $(K_0, K_1) \in \{0,1\}^{16}$ **do**

  $A_2 = [\,]$ of size $2^8 \times 2^{16}$;

  for all C_3 **do**

    for all $(K_2, a_2) \in \{0,1\}^{16}$ **do**

$$A_2[K_2][a_2, C_3] \leftarrow \bigoplus_{a_1, C_2} A_1[K_0, K_1][a_1, C_2, C_3] \cdot \mathbb{1}(a_1 \oplus S_2(C_2 \oplus K_2) = a_2)$$

Partial Sums Meet FFT

for all $(\mathrm{K}_0, \mathrm{K}_1) \in \{0,1\}^{16}$ **do**

$\quad \ldots$

$\quad$ **for all** $k_2 \in \{0,1\}^8$ **do**

$\quad\quad \ldots$

$\quad\quad$ **for all** $k_3 \in \{0,1\}^8$ **do**

$\quad\quad\quad A_4$ of size 2^8;

$\quad\quad\quad$ **for all** $k_4 \in \{0,1\}^8$ **do**

$$A_4[k_4] \leftarrow \bigoplus_{a_3} A_3[k_3][a_3] \cdot S(a_3 \oplus k_4)$$

$\quad\quad\quad$ **for all** $k_4 \in \{0,1\}^8$ **do**

$\quad\quad\quad\quad$ **if** $A_4[k_4] \neq 0$ **then**

$\quad\quad\quad\quad\quad k_0, k_1, k_2, k_3, k_4$ is not a valid key candidate

Complexities of Various Steps

Steps	Time	Memory
1	$2^{24} * (4 * 16 * 2^{16}) = 2^{46}$	2^{40}
2	$2^{16} * (2^{8} * (4 * 16 * 2^{16})) = 2^{46}$	2^{24}
3	$2^{16} * 2^{8} * (4 * 16 * 2^{16}) = 2^{46}$	2^{16}
4	$2^{16} * 2^{8} * 2^{8} * (8 * 4 * 8 * 2^{8}) = 2^{48}$	2^{8}
Total	$2^{48.5}$	2^{40}

Packing Multiple FFT's

for all $(\mathrm{K}_0, \mathrm{K}_1) \in \{0,1\}^{16}$ **do**

$\quad \ldots$

$\quad$ **for all** $k_2 \in \{0,1\}^8$ **do**

$\quad\quad \ldots$

$\quad\quad$ **for all** $k_3 \in \{0,1\}^8$ **do**

$\quad\quad\quad \ldots$

$\quad\quad\quad$ **for all** $k_4 \in \{0,1\}^8$ **do**

$\quad\quad\quad\quad \ldots$

$$A_4[k_4] \leftarrow \bigoplus_{a_3} S(a_3 \oplus k_4) \cdot A_3[k_3][a_3]$$

UNIVERSITY OF HAIFA אוניברסיטת חיפה جامعة حيفا

Packing Technique

- We assume that the attack is implemented using 64-bit operations in software

Packing Technique

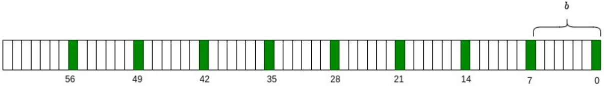
- We assume that the attack is implemented using 64-bit operations in software
- Computing one convolution (results one bit information) is a waste of resources

Packing Technique

- We assume that the attack is implemented using 64-bit operations in software
- Computing one convolution (results one bit information) is a waste of resources
- We compute several convolution in parallel and pack the results in 64-bit

Packing Technique

- We assume that the attack is implemented using 64-bit operations in software
- Computing one convolution (results one bit information) is a waste of resources
- We compute several convolution in parallel and pack the results in 64-bit



$$\bigoplus_{a_3} S(a_3 \oplus k_4) \cdot A_3[k_3][a_3] = \sum_{a_3} (2^{7b} S^7(\mathsf{K} \oplus \mathsf{C}) + \cdots + S^0(\mathsf{K} \oplus \mathsf{C}))A_3[k_3][a_3]$$

$$= \sum_{a_3} \sum_{j} 2^{jb} S^j(\mathsf{K} \oplus \mathsf{C}) \cdot A_3[k_3][a_3]$$

How large should b be?

- How large should b be so that $S^j(\mathsf{K} \oplus \mathsf{C}) < 2^b \; \forall j$?

How large should b be?

- How large should b be so that $S^j(\mathsf{K} \oplus \mathsf{C}) < 2^b \; \forall j$?
- Suppose S is a balanced function then each $S^j(\mathsf{K} \oplus \mathsf{C})$ is the sum 128 elements

How large should b be?

- How large should b be so that $S^j(\mathsf{K} \oplus \mathsf{C}) < 2^b \ \forall j$?
- Suppose S is a balanced function then each $S^j(\mathsf{K} \oplus \mathsf{C})$ is the sum 128 elements
- Thus each $S^j(\mathsf{K} \oplus \mathsf{C})$ is distributed as $Bin(128, 1/2)$
- Expectation is 64 and Standard deviation $4\sqrt{2}$
- If $b = 7$, Using Chernoff bound, $Pr(S^j(\mathsf{K} \oplus \mathsf{C}) > 2^7)$ is extremely small

How small should b be?

- If b is too large, this may cause an overflow

How small should b be?

- If b is too large, this may cause an overflow
- Obviously we ignore overflow beyond 64 bits

How small should b be?

- If b is too large, this may cause an overflow
- Obviously we ignore overflow beyond 64 bits
- Assuming each $s^j(\mathrm{K} \oplus \mathrm{C}) < 2^b$, there will be no overflow if $7b < (64 - n)$
- Thus, $b \leq 7$

How small should b be?

- If b is too large, this may cause an overflow
- Obviously we ignore overflow beyond 64 bits
- Assuming each $s^j(\mathrm{K} \oplus \mathrm{C}) < 2^b$, there will be no overflow if $7b < (64 - n)$
- Thus, $b \leq 7$

Using $b = 7$, we compute 8 convolutions in parallel

Complexity: 2^{45} VS 2^{48}

Complexities of Various Steps

Steps	Time	Memory
1	$2^{46}/7$	2^{40}
2	$2^{46}/7$	2^{24}
3	$2^{46}/7$	2^{16}
4	$2^{48}/8$	2^{8}
Total	$\approx 2^{44}$	2^{40}

Complexities of Various Steps

Steps	Time	Memory
1	$2^{46}/7$	2^{40}
2	$2^{46}/7$	2^{24}
3	$2^{46}/7$	2^{16}
4	$2^{48}/8$	2^{8}
Total	$\approx 2^{44}$	2^{40}

But still we need at least $128GB$ of memory

אוניברסיטת חיפה
UNIVERSITY OF HAIFA
جامعة حيفا

Low memory Variant

for all $K_0 \in \{0,1\}^8$ **do**

A_0 of size 2^{32}; $\triangleright$ 2^{32} memory

for all $(C_0, C_1, C_2, C_3) \in \{0,1\}^{32}$ **do**

$a_0 \leftarrow S_0(C_0 \oplus K_0)$

$A_0[a_0, C_1, C_2, C_3] \leftarrow A[C_0, C_1, C_2, C_3]$

A_1 of size $2^8 \times 2^{24}$; $\triangleright$ 2^{32} memory

for all $(C_2, C_3) \in \{0,1\}^{16}$ **do**

for all $(K_1, a_1) \in \{0,1\}^{16}$ **do**

$$A_1[K_1][a_1, C_2, C_3] \leftarrow \bigoplus_{a_0, C_1} A_0[a_0, C_1, C_2, C_3] \cdot \mathbb{1}(a_0 \oplus S_1(C_1 \oplus K_1) = a_1)$$

Low memory Variant

for all $K_0 \in \{0,1\}^8$ **do**

A_0 of size 2^{32}; $\triangleright$ 2^{32} memory

for all $(C_0, C_1, C_2, C_3) \in \{0,1\}^{32}$ **do**

$a_0 \leftarrow S_0(C_0 \oplus K_0)$

$A_0[a_0, C_1, C_2, C_3] \leftarrow A[C_0, C_1, C_2, C_3]$

A_1 of size $2^8 \times 2^{24}$; $\triangleright$ 2^{32} memory

for all $(C_2, C_3) \in \{0,1\}^{16}$ **do**

for all $(K_1, a_1) \in \{0,1\}^{16}$ **do**

$$A_1[K_1][a_1, C_2, C_3] \leftarrow \bigoplus_{a_0, C_1} A_0[a_0, C_1, C_2, C_3] \cdot \mathbb{1}(a_0 \oplus S_1(C_1 \oplus K_1) = a_1)$$

Time: $\approx c \times 2^{46}$ and Memory: $0.5\,GB$

Plan of this Section

1. Motivation
2. Integral attack on AES
3. Partial Sums Meet FFT
4. Results and Conclusion

אוניברסיטת חיפה
UNIVERSITY OF HAIFA
جامعة حيفا

Integral Attack on 6-Round AES

	FHT+Part. Sums	FHT	Part. Sums
AWS Instance	m6i.32xlarge	r6i.32xlarge	m6i.32xlarge
Running Time(m)	48	3120	4859
Total Cost (USD)	5	418	497

In Conclusion: Our attack is 65 times faster and 83 times cheaper

Integral Attack on 6-Round AES

Cipher	Rounds	Data	Time	Technique and Source
AES	6	2^{32} CP	2^{71} Enc.	Square [DKR97]
		$6 \cdot 2^{32}$ CP	2^{52} S-box Eval.	Square & Partial sums [FKL$^+$01]
		2^{71} ACPC	2^{71} Enc.	Boomerang [Bir04]
		2^{33} CP	2^{52} S-box Eval.	Square & Partial sums [Tun12]
		$6 \cdot 2^{32}$ CP	2^{52} Add.	Square & FHT [TA14]
		2^{26} CP	2^{80} Enc.	Mixture Differential [BDK$^+$20]
		2^{55} ACPC	2^{80} Enc.	Retracing Boomerang [DKRS20]
		$2^{79.7}$ ACPC	2^{78} Enc.	Boomeyong [RSP21]
		2^{59} ACPC	2^{61} Enc.	Truncated Boomerang [BL22]
		2^{33} CP	$2^{46.4}$ Add.	Square & Partial sums & FHT

The Improvement Matrix

	AES	Kuznyechik		MISTY1	CLEFIA
Rounds	6	6	7	8 (Full)	12
Improvement Factor	2^5	2^6	2^6	2^3	2^{30}

Thank You for your attention!

Any questions?

Our Attack Without Packing

- Factor of 6 improvement than Todo-Aoki's attack

Our Attack Without Packing

- Factor of 6 improvement than Todo-Aoki's attack
- 16/8 vs. 32 bit addition (Factor of 12 improvement)

Our Attack Without Packing

- Factor of 6 improvement than Todo-Aoki's attack
- 16/8 vs. 32 bit addition (Factor of 12 improvement)
- Factor of 8 improvement than Partial-sum attack

Other Attacks With Packing

- Factor of 20 improvement than Todo-Aoki's attack

Other Attacks With Packing

- Factor of 20 improvement than Todo-Aoki's attack
- Factor of 60 improvement than Partial-sum attack

Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir.
Improved key recovery attacks on reduced-round AES with practical data and memory complexities.
J. Cryptol., 33(3):1003–1043, 2020.

Alex Biryukov.
The boomerang attack on 5 and 6-round reduced AES.
In Hans Dobbertin, Vincent Rijmen, and Aleksandra Sowa, editors, *Advanced Encryption Standard - AES, 4th International Conference, AES 2004, Bonn, Germany, May 10-12, 2004, Revised Selected and Invited Papers*, volume 3373 of *Lecture Notes in Computer Science*, pages 11–15. Springer, 2004.

Augustin Bariant and Gaëtan Leurent.
Truncated boomerang attacks and application to AES-based ciphers.
Cryptology ePrint Archive, Report 2022/701, 2022.

https://eprint.iacr.org/2022/701.

Joan Daemen, Lars R. Knudsen, and Vincent Rijmen.
The block cipher square.
In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer, 1997.

Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir.
The retracing boomerang attack.
In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 280–309. Springer, 2020.

- Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David A. Wagner, and Doug Whiting.
  Improved cryptanalysis of rijndael.
  In *FSE*, volume 1978 of *Lecture Notes in Computer Science*, pages 213–230. Springer, 2000.
- Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting.
  Improved cryptanalysis of Rijndael.
  In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 213–230. Springer, Heidelberg, April 2001.
- Mostafizar Rahman, Dhiman Saha, and Goutam Paul.
  Boomeyong: Embedding yoyo within boomerang and its applications to key recovery attacks on AES and pholkos.

IACR Trans. Symmetric Cryptol., 2021(3):137–169, 2021.

Yosuke Todo and Kazumaro Aoki.
FFT key recovery for integral attack.
In Dimitris Gritzalis, Aggelos Kiayias, and Ioannis G. Askoxylakis, editors, *CANS 14*, volume 8813 of *LNCS*, pages 64–81. Springer, Heidelberg, October 2014.

Michael Tunstall.
Improved "partial sums"-based square attack on AES.
In *Proceedings of the International Conference on Security and Cryptography - SECRYPT, (ICETE 2012)*, pages 25–34. INSTICC, SciTePress, 2012.