Combining Partial Sums and FHT for the Fastest Known Attack on 6-Round AES

Shibam GHOSH

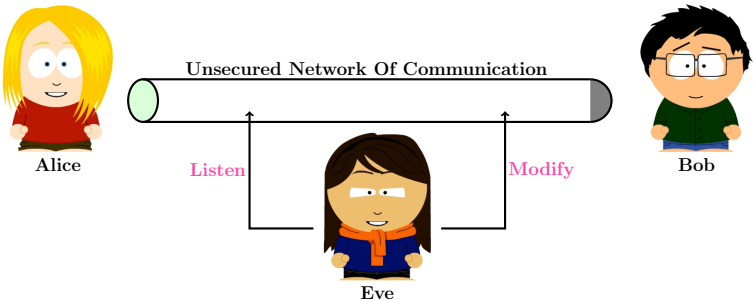
October 17, 2025

INRIA, Paris, France

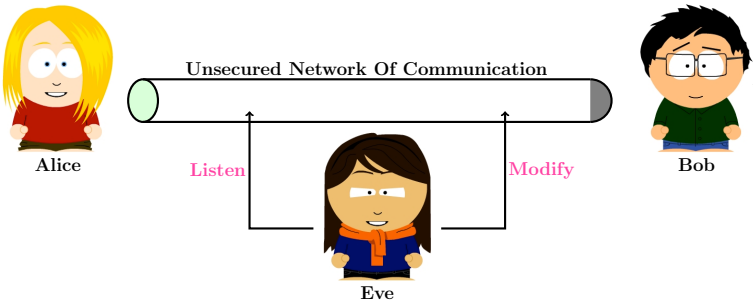
Table of contents

Plan of this Section

Why Cryptography?



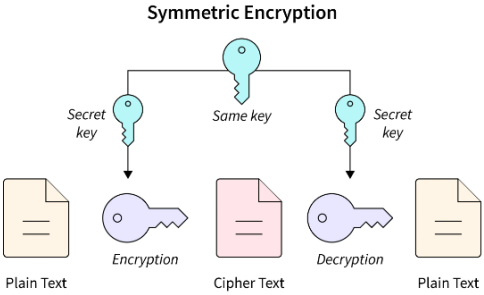
Why Cryptography?

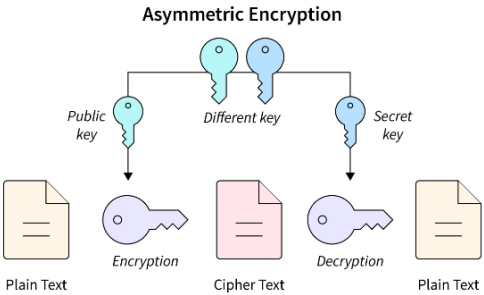


Goal: Efficient algorithms with the following functionalities:

Confidentiality Integrity Authenticity

Symmetric and Asymmetric Key Cryptography





Symmetric-Key Cryptography

Symmetric-Key Cryptosystem

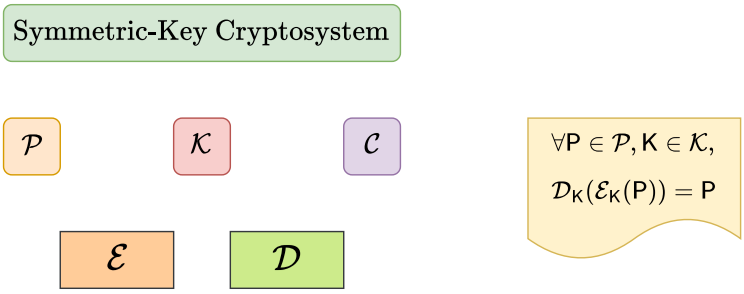
$\mathcal{P}$ $\mathcal{K}$ $\mathcal{C}$

$\mathcal{E}$ $\mathcal{D}$

$\forall \mathsf{P} \in \mathcal{P}, \mathsf{K} \in \mathcal{K},$

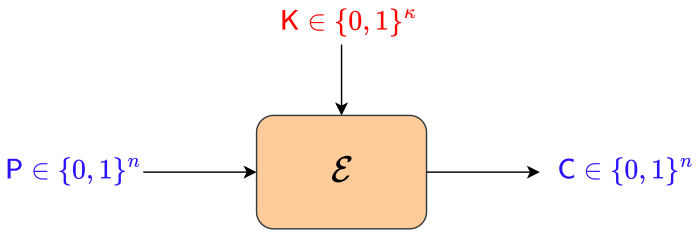
$\mathcal{D}_{\mathsf{K}}(\mathcal{E}_{\mathsf{K}}(\mathsf{P})) = \mathsf{P}$

Symmetric-Key Cryptography

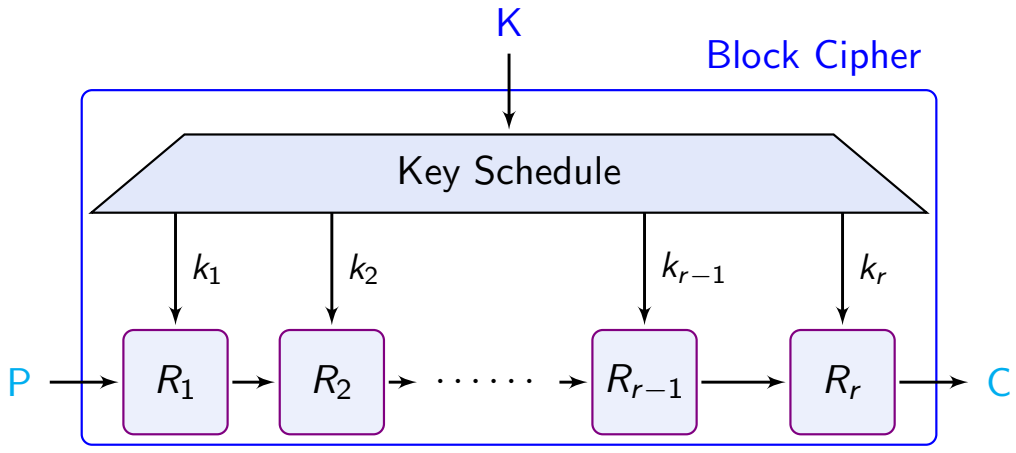


e.g., Block ciphers, stream ciphers, hash functions, MACs, ...

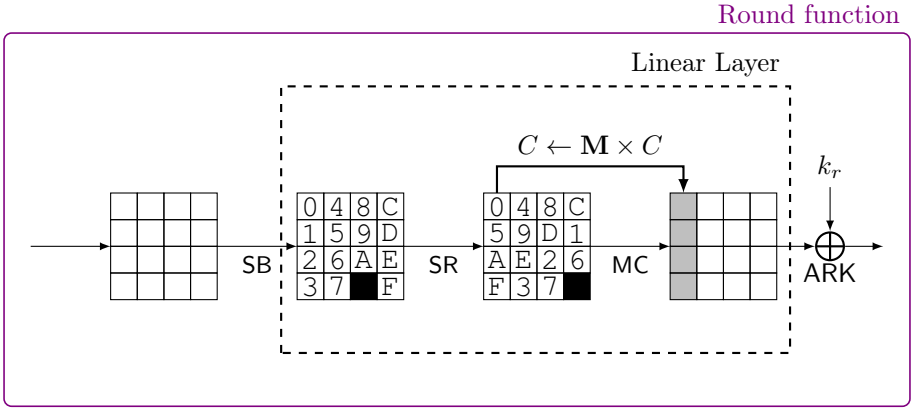
Block Cipher



Iterated Block Cipher



AES: The NIST Standard

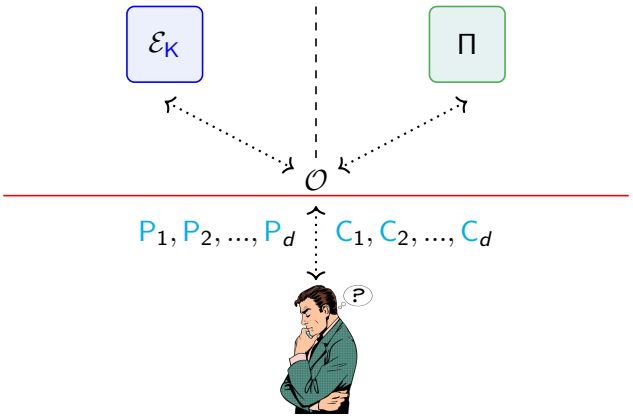


Motivation

Why Symmetric Key Cryptanalysis?

Cryptanalysis Perspective: Left-Right Distinguishing Game

$\mathcal{E}: \mathcal{P} \times \mathcal{K} \to \mathcal{C}$ is a block cipher and Π is a random permutation



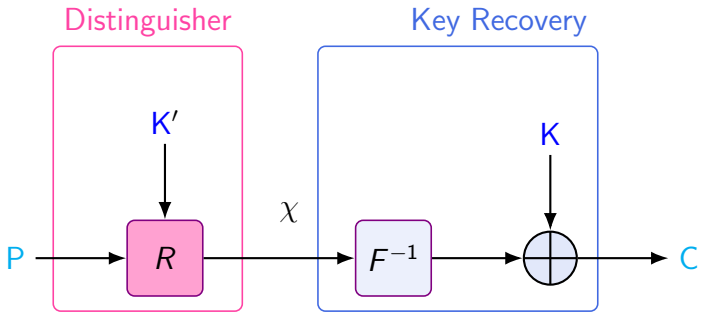
Cryptanalysis Perspective

"Searching 'Distinguisher'" | Key Recovery

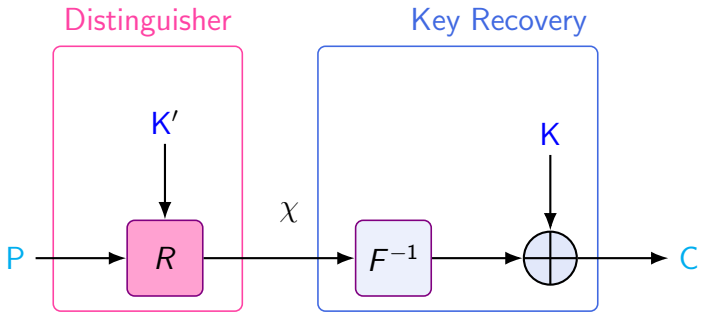
My Contributions in Cryptanalysis

Primitive	Distinguisher	Key Recovery	Venue
AES	Integral	✓	Eurocrypt 24
QARMA	Differential, Weak-Key	✓	FSE 25
ARADI	Integral	✓	Under Submission
PRESENT, GIFT, BAKSHEESH	Impossible Differential	✓	CHES 25
PRESENT, GIFT	Integral	✓	ACNS 23
TinyJambu-192/256	Differential	✓	FSE 23
TinyJambu-128	Integral		Indocrypt 22
KNOT, ASCON	Integral		Latincrypt 21
SHA-3, Xoodyak, Bash	Integral		DCC 25
QARMAv2	Known Attacks	✓	FSE 23
ChiLow	Known Attacks	✓	Eurocrypt 25
FRAST	Differential, Weak-key	✓	Under Submission

Cryptanalysis Perspective

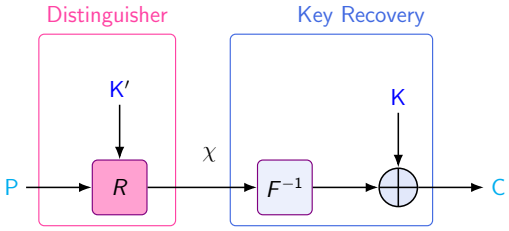


Cryptanalysis Perspective



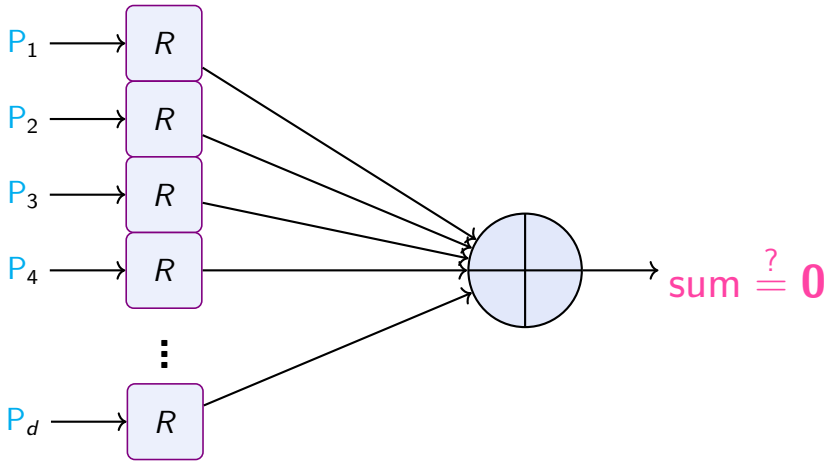
- $R(\cdot) = R_{r-1} \circ R_{r-2} \circ \cdots \circ R_1 \circ R_0(\cdot)$

Classic Distinguishers in Cryptanalysis

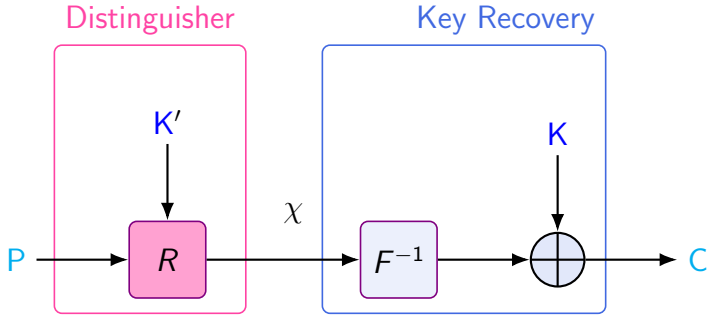


- Differential : $\Pr\left(R(\mathrm{P}) \oplus R(\mathrm{P} \oplus \Delta_{in}) = \Delta_{out}\right) = 2^{-a}, a \ll n$
- Integral : $\Pr\left(\bigoplus_{\mathrm{P}\in\mathcal{I}} R(\mathrm{P}) = \mathcal{S}\right) = 2^{-a}, a \ll n$
- Linear : $\left|\Pr\left(\alpha \cdot \mathrm{P} \oplus \beta \cdot R(\mathrm{P}) = 0\right) - \frac{1}{2}\right| = 2^{-a}, a \ll n$

Integral/Zero-Sum Distinguisher



Key Recovery Using Integral/Zero-Sum Distinguisher



$$\bigoplus_{\mathsf{X}\in\mathcal{X}} \mathsf{X} = \bigoplus_{\mathsf{P}\in\mathcal{P}} R(\mathsf{P}) = 0 = \bigoplus_{\mathsf{C}\in\mathcal{C}} F(\mathsf{C} \oplus \mathsf{K}), \text{ for the correct key } \mathsf{K}$$

Motivation

Algorithm For Key Recovery

Key Recovery Algorithm

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 Algorithm

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

procedure 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

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

Key Recovery Algorithm

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

procedure 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

BAR $\equiv$ Convolution for each K,

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

The BAR matrix

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

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

The BAR matrix

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

The BAR matrix

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

The BAR matrix

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

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 $\mathcal{M}_m$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Plan of this Section

1. Motivation

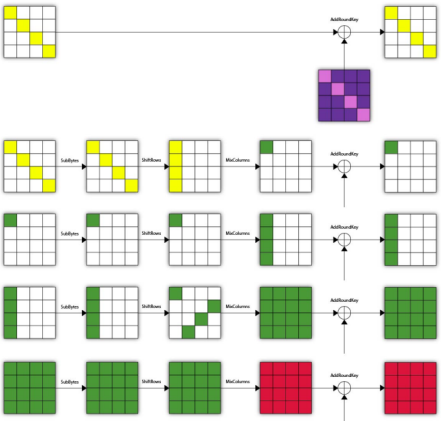
2. Integral Attack On AES

   FHT-based Integral Attack

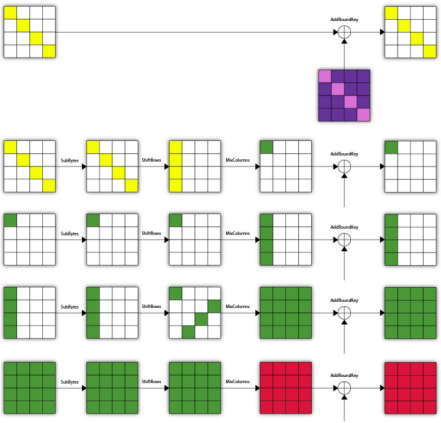
   Partial Sum Technique

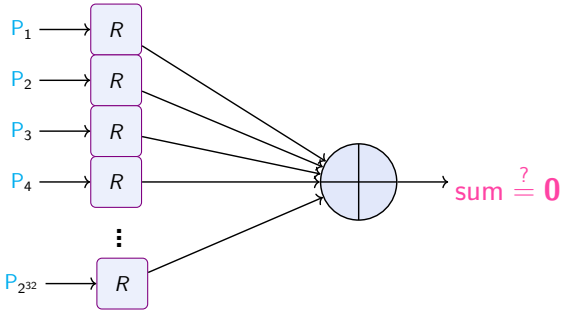
3. Partial Sums Meet FHT (Eurocrypt 2024)

Zero-Sum Property On AES

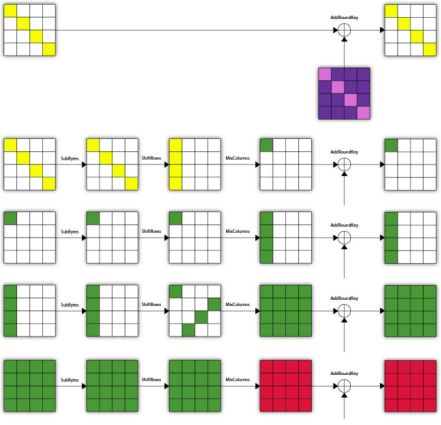


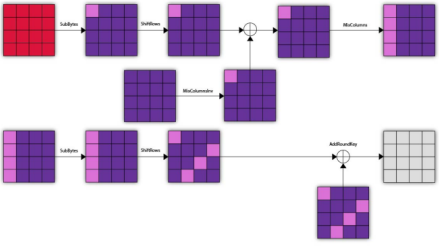
Zero-Sum Property On AES



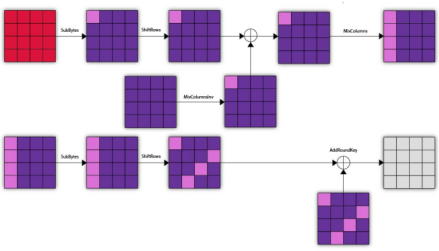


Zero-Sum Property On AES



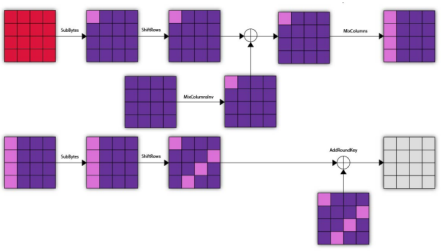


Integral Attack On AES



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

Integral Attack On AES



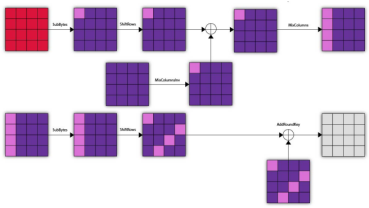
$$\chi(K, C) = S(K_4 \oplus S_3(K_3 \oplus C_3) \oplus S_2(K_2 \oplus C_2) \oplus S_1(K_1 \oplus C_1) \oplus S_0(K_0 \oplus C_0))$$

procedure FOO($\mathcal{C} \subseteq \{0,1\}^{32}$ of size 2^{32})
  for $K = (K_4K_3K_2K_1K_0) \in \{0,1\}^{40}$ **do**
    $\mathbf{S} = \mathbf{0}$
    for $C \in \mathcal{C}$ **do**
      $\mathbf{S} = \mathbf{S} \oplus \chi(K \oplus C)$
    if $\mathbf{S} \neq \mathbf{0}$ **then** Discard K

Integral Attack On AES

FHT-based Integral Attack

Integral Attack On AES Using FHT [Todo et al. [TA14a]]



procedure $\mathrm{BAR}(\mathcal{C} \subseteq \{0,1\}^{32}$ of size $2^{32})$

  for $K_4 \in \{0,1\}^8$ **do**

    for $K = (K_3K_2K_1K_0) \in \{0,1\}^{32}$ **do**

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

      for $C \in \{0,1\}^{32}$ **do**

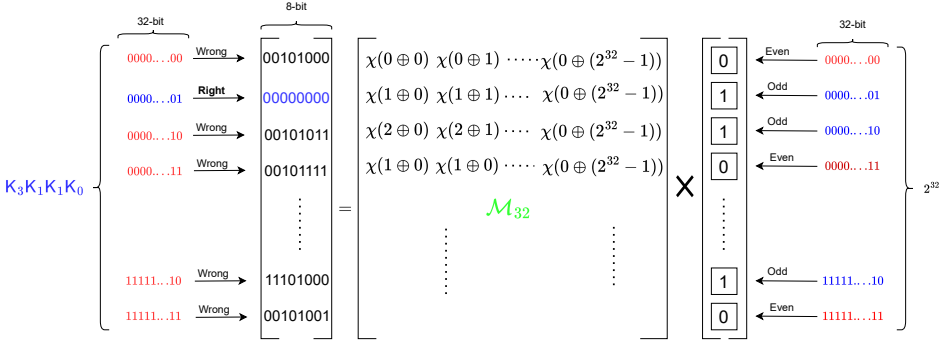
        $\mathbf{S} = \mathbf{S} \oplus \chi(K \oplus C)G_{\mathcal{C}}(C)$

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

        Discard K

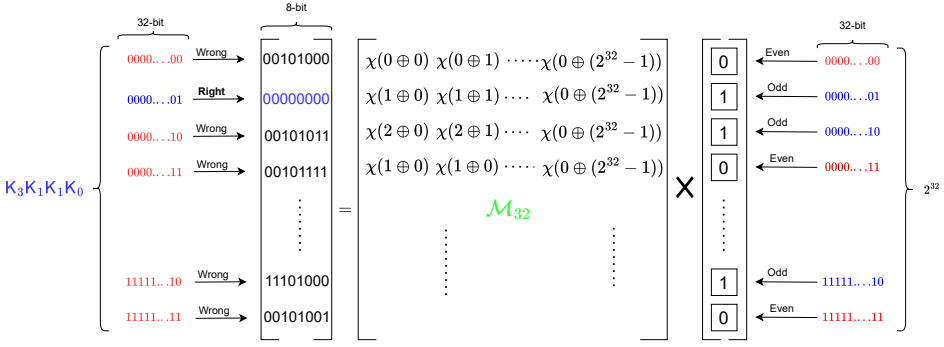
Integral Attack On AES Using FHT [Todo et al. [TA14a]]

For each $K_4 \in \{0,1\}^8$:



Integral Attack On AES Using FHT [Todo et al. [TA14a]]

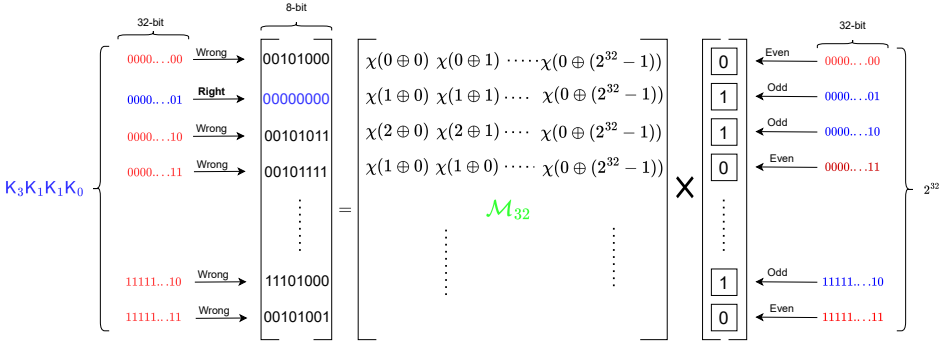
For each $K_4 \in \{0,1\}^8$:



Time: $2^8 \times 2^{39}$

Integral Attack On AES Using FHT [Todo et al. [TA14a]]

For each $K_4 \in \{0,1\}^8$:



Time: $2^8 \times 2^{39} \times 8$

The Problem with Finite Field Arithmetic

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

The Problem with Finite Field Arithmetic

- $\chi * G(K) = \sum_{C} \chi(C \oplus K) G(C)$ VS $\chi * G(K) = \bigoplus_{C} \chi(C \oplus K) G(C)$
- We need functions whose output is an integer and not an element of $\mathbb{F}_2^8$
- Todo et al. [TA14a] proposed to consider 8 outputs separately
- Complexity: Time $c \times 2^{50}$, Memory 2^{32}

The Problem with Finite Field Arithmetic

- $\chi * G(K) = \sum_{C} \chi(C \oplus K) G(C)$ VS $\chi * G(K) = \bigoplus_{C} \chi(C \oplus K) G(C)$
- We need functions whose output is an integer and not an element of $\mathbb{F}_2^8$
- Todo et al. [TA14a] proposed to consider 8 outputs separately
- Complexity: Time $c \times 2^{50}$, Memory 2^{32}

$\chi * G(K) = \sum_{C} \chi(C \oplus K) G(C)$

$\chi * G(K) = \bigoplus_{C} \chi(C \oplus K) G(C)$

The Problem with Finite Field Arithmetic

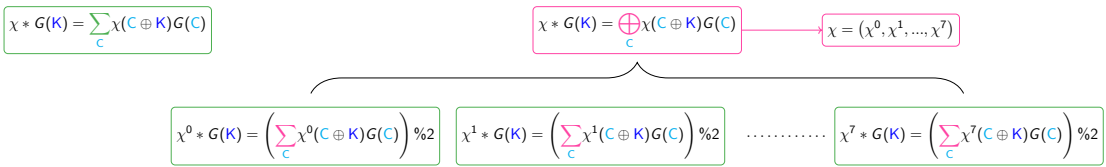
- $\chi * G(K) = \sum_C \chi(C \oplus K) G(C)$ VS $\chi * G(K) = \bigoplus_C \chi(C \oplus K) G(C)$
- We need functions whose output is an integer and not an element of $\mathbb{F}_2^8$
- Todo et al. [TA14a] proposed to consider 8 outputs separately
- Complexity: Time $c \times 2^{50}$, Memory 2^{32}

$\chi * G(K) = \sum_C \chi(C \oplus K) G(C)$

$\chi * G(K) = \bigoplus_C \chi(C \oplus K) G(C)$ → $\chi = (\chi^0, \chi^1, ..., \chi^7)$

The Problem with Finite Field Arithmetic

- $\chi * G(K) = \sum_C \chi(C \oplus K) G(C)$ VS $\chi * G(K) = \bigoplus_C \chi(C \oplus K) G(C)$
- We need functions whose output is an integer and not an element of $\mathbb{F}_2^8$
- Todo et al. [TA14a] proposed to consider 8 outputs separately
- Complexity: Time $c \times 2^{50}$, Memory 2^{32}



Integral Attack On AES

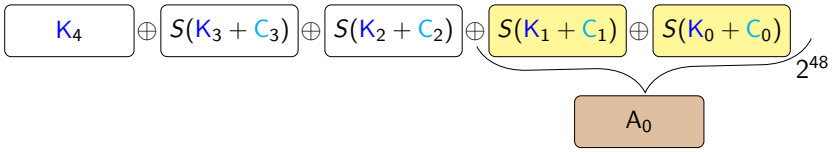
Partial Sum Technique

Partial Sum Technique [FKL+00]

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

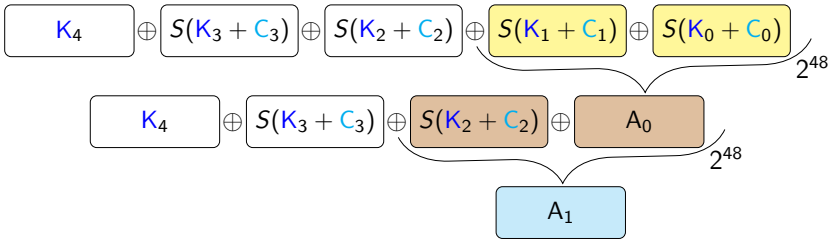
Partial Sum Technique [FKL+00]

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



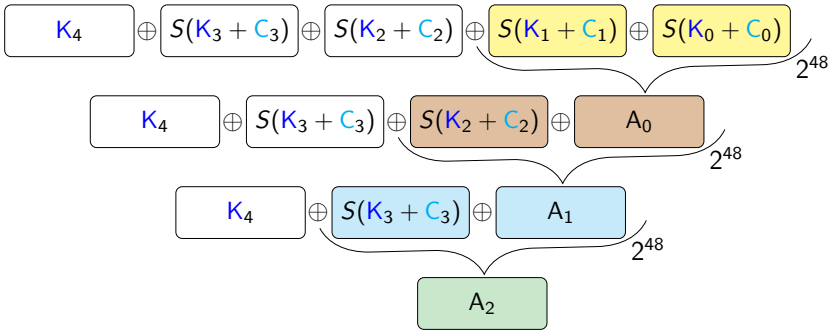
Partial Sum Technique [FKL+00]

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



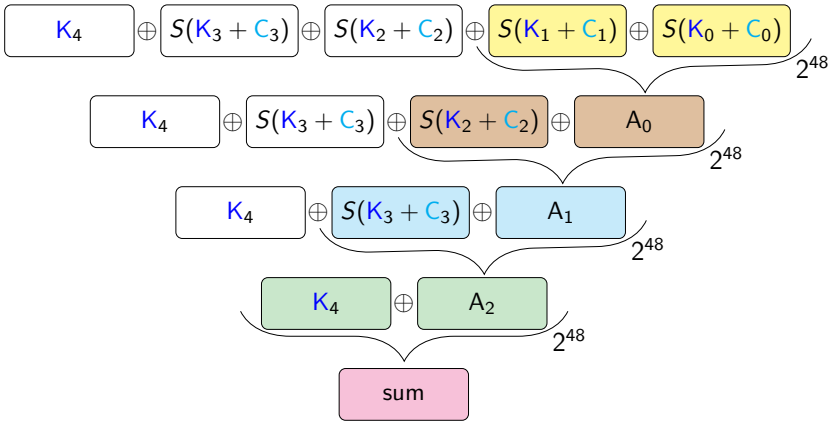
Partial Sum Technique [FKL+00]

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



Partial Sum Technique [FKL+00]

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



Plan of this Section

1. Motivation
2. Integral Attack On AES
3. Partial Sums Meet FHT (Eurocrypt 2024)
   - Packing Technique
   - Results

Basic Idea

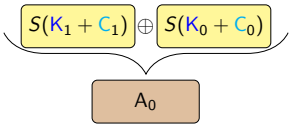
- We follow the general structure of the partial sums attack
- Replace each partial sum with FHT
- However, rearrange the steps to make it FHT compatible
- Rearrange the steps again to reduce memory complexity

Attacks 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 [TA14b]
		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

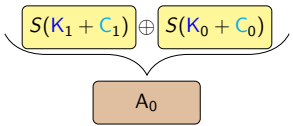
Partial Sums Meet FHT

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



Partial Sums Meet FHT

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



$\mathsf{A}_0 = [\,]$ of size $2^{16} \times 2^{24}$; ▷ 2^{40} memory

for all $(a_1, \mathsf{C}_2, \mathsf{C}_3) \in \{0,1\}^{24}$ **do**

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

$$\mathsf{A}_0[\mathsf{K}_0, \mathsf{K}_1][a_1, \mathsf{C}_2, \mathsf{C}_3] \leftarrow \bigoplus_{\mathsf{C}_0, \mathsf{C}_1} G_{\mathcal{C}}[\mathsf{C}_0, \mathsf{C}_1, \mathsf{C}_2, \mathsf{C}_3] \cdot \mathbb{1}(S_0(\mathsf{C}_0 \oplus \mathsf{K}_0) \oplus S_1(\mathsf{C}_1 \oplus \mathsf{K}_1) = a_1)$$

Partial Sums Meet FHT

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

$\cdots$

for all $K_2 \in \{0,1\}^8$ **do**

$\cdots$

for all $K_3 \in \{0,1\}^8$ **do**

$\cdots$

for all $K_4 \in \{0,1\}^8$ **do**

$$\mathrm{sum}[K_4] \leftarrow \bigoplus_{a_3} A_2[K_3][a_3] \cdot S(a_3 \oplus K_4)$$

for all $K_4 \in \{0,1\}^8$ **do**

if $\mathrm{sum}[K_4] \neq 0$ **then**

K_0, K_1, K_2, K_3, K_4 is not a valid key candidate

Complexities of Various Steps

Steps	Time (`uint64_t` Addition)	Memory (bits)
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 FHT's

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

$\cdots$

for all $\mathsf{K}_2 \in \{0,1\}^8$ **do**

$\cdots$

for all $\mathsf{K}_3 \in \{0,1\}^8$ **do**

$\cdots$

for all $\mathsf{K}_4 \in \{0,1\}^8$ **do**

$\cdots$

$$\mathsf{sum}[k_4] \leftarrow \bigoplus_{a_3} S(a_3 \oplus \mathsf{K}_4) \cdot \mathsf{A}_2[\mathsf{K}_3][a_3]$$

Partial Sums Meet FHT (Eurocrypt 2024)

Packing Technique

Packing Technique

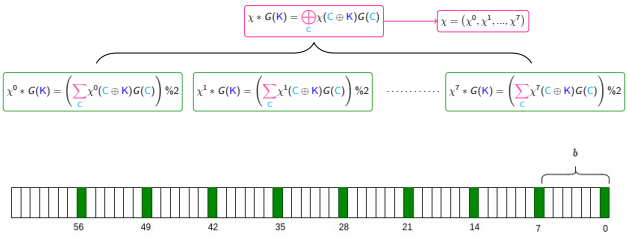
- We assume that the attack is implemented using 64-bit operations in software

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

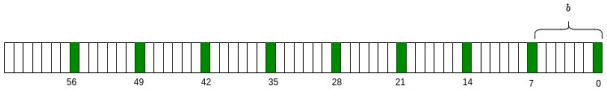
Packing Technique

- 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



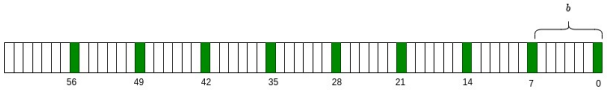
$$\bigoplus_{a_3} S(a_3 \oplus k_4) \cdot A_3[k_3][a_3] = \sum_{a_3} (2^{7b} S^7(K \oplus C) + \cdots + S^0(K \oplus C)) A_3[k_3][a_3]$$

How large should b be?



How Small should b be?

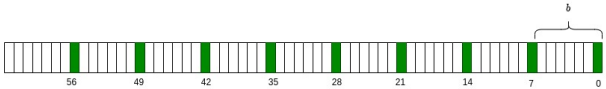
How large should b be?



How Small should b be?

- Ensure: $S^j(\mathsf{K} \oplus \mathsf{C}) < 2^b \ \forall j$?

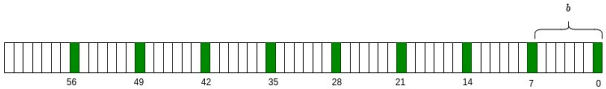
How large should b be?



How Small should b be?

- Ensure: $S^j(\mathsf{K} \oplus \mathsf{C}) < 2^b \ \forall j$?
- $S^j(\mathsf{K} \oplus \mathsf{C}) \sim \mathit{Binomial}(128, 1/2)$
- $\mu = 64, \sigma = 4\sqrt{2}$

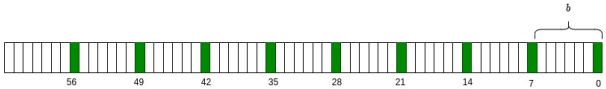
How large should b be?



How Small should b be?

- Ensure: $S^j(\mathsf{K} \oplus \mathsf{C}) < 2^b \ \forall j$?
- $S^j(\mathsf{K} \oplus \mathsf{C}) \sim Binomial(128, 1/2)$
- $\mu = 64, \sigma = 4\sqrt{2}$
- If $b = 7$, Using Chernoff bound,
  - $Pr(S^j(\mathsf{K} \oplus \mathsf{C}) > 2^7)$ is extremely small

How large should b be?



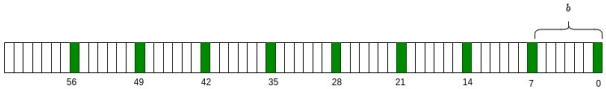
How Small should b be?

- Ensure: $S^j(\mathsf{K} \oplus \mathsf{C}) < 2^b \ \forall j$?
- $S^j(\mathsf{K} \oplus \mathsf{C}) \sim Binomial(128, 1/2)$
- $\mu = 64, \sigma = 4\sqrt{2}$
- If $b = 7$, Using Chernoff bound,
  - $Pr(S^j(\mathsf{K} \oplus \mathsf{C}) > 2^7)$ is extremely small

How Large should b be?

- Ensure: No Overflow

How large should b be?



How Small should b be?

- Ensure: $S^j(\mathsf{K} \oplus \mathsf{C}) < 2^b \ \forall j$?
- $S^j(\mathsf{K} \oplus \mathsf{C}) \sim Binomial(128, 1/2)$
- $\mu = 64, \sigma = 4\sqrt{2}$
- If $b = 7$, Using Chernoff bound,
  - $Pr(S^j(\mathsf{K} \oplus \mathsf{C}) > 2^7)$ is extremely small

How Large should b be?

- Ensure: No Overflow
- $7b \leq (64 - n) \implies b \leq 7$

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}

Complexity: Time 2^{44}, Memory 128GB

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}

Complexity: Time 2^{44}, Memory 128GB

Low Memory Variant: Time 2^{46}, Memory 0.5GB

Partial Sums Meet FHT (Eurocrypt 2024)

Results

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

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}

Conclusion

Partial Sum Meet FHT Without Packing VS Todo et al's FHT	Partial Sum Meet FHT Without Packing VS Partial Sum
6 or 12 times Improvement	8 times Improvement (One Sbox $\approx$ One 32-bit Addition)
20 times Improvement	60 times Improvement (16 parallel Sbox using AESNI)
Partial Sum Meet FHT With Packing VS Todo et al's FHT With Packing	Partial Sum Meet FHT With Packing VS Partial Sum With Parallel Sbox

Open Questions

- FFT-based techniques for ciphers over prime fields ($GF(p)$)

Open Questions

- FFT-based techniques for ciphers over prime fields ($GF(p)$)
  - Applications: Prime field masking, MPC, ZKP
  - AES-prime (Eurocrypt 2023):
    $GF(2^8)$ **vs.** $GF(2^7 - 1)$, $x \mapsto x^{-1}$ **vs.** $x \mapsto x^5$

Open Questions

- FFT-based techniques for ciphers over prime fields ($GF(p)$)
  - Applications: Prime field masking, MPC, ZKP
  - AES-prime (Eurocrypt 2023):
    $GF(2^8)$ **vs.** $GF(2^7 - 1)$, $x \mapsto x^{-1}$ **vs.** $x \mapsto x^5$
- Can similar packing techniques be applied in other contexts?

https://github.com/ShibamCrS/Partial_Sums_Meet_FFT.git

https://artifacts.iacr.org/eurocrypt/2024/a7/

[BDK+20] 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.

[Bir04] 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.

[BL22] 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.

[DKR97] 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.

[DKRS20] 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.

[FKL+00] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David A. Wagner, and Doug Whiting. Improved Cryptanalysis of Rijndael. In *Proceedings of Fast Software Encryption (FSE)*, volume 1978 of *Lecture Notes in Computer Science*, pages 213–230. Springer, 2000.

[FKL+01] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay,

David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. pages 213–230, 2001.

[RSP21] 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.

[TA14a] Yosuke Todo and Kazumaro Aoki. FFT Key Recovery for Integral Attack. In *Proceedings of Cryptology and Network Security (CANS)*, volume 8813 of *Lecture Notes in Computer Science*, pages 64–81. Springer, 2014.

[TA14b] Yosuke Todo and Kazumaro Aoki. FFT key recovery for integral attack. pages 64–81, 2014.

[Tun12] 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.